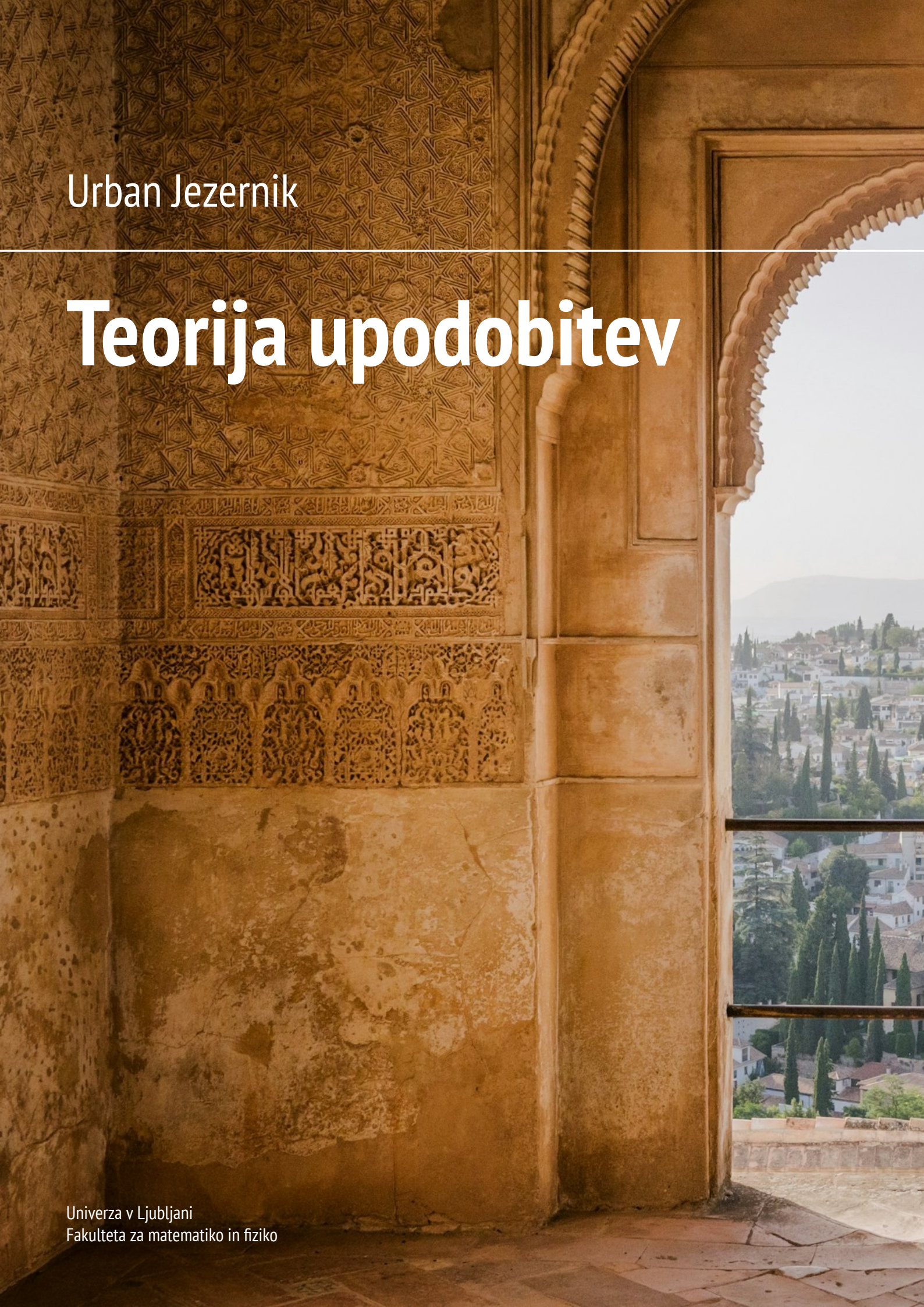


Urban Jezernik

# Teorija upodobitev

Univerza v Ljubljani
Fakulteta za matematiko in fiziko

Urban Jezernik

# TEORIJA UPODOBITEV



FMF | UNIVERZA V LJUBLJANI
Fakulteta za matematiko in fiziko

Ljubljana 2026

Izdaja: Univerza v Ljubljani, Fakulteta za matematiko in fiziko

Urban Jezernik

**TEORIJA UPODOBITEV**

Strokovni pregled: Primož Moravec
Jezikovni pregled: Grega Rihtar
Tehnični urednik: Matjaž Zaveršnik
Odgovorni urednik: Matej Brešar

Elektronska izdaja je dostopna pod pogoji licence CC BY 4.0 na:
https://www.fmf.uni-lj.si/pub/upodobitve/

Kataložni zapis o publikaciji (CIP) pripravili v Narodni in univerzitetni knjižnici v Ljubljani
COBISS.SI-ID 279114499
ISBN 978-961-6619-59-2 (PDF)

# Kazalo


**1 Temelji teorije upodobitev** **9**
1.1 Osnovni pojmi . . . 9
1.2 Fundamentalne konstrukcije . . . 12

**2 Upodobitev pod mikroskopom** **23**
2.1 Razstavljanje upodobitve . . . 23
2.2 Matrični koeficienti . . . 30

**3 Upodobitve končnih grup** **35**
3.1 Polenostavnost . . . 35
3.2 Karakterji . . . 38

**4 Razširjeni zgledi – končni** **53**
4.1 Simetrične grupe . . . 53
4.2 Splošne linearne grupe . . . 62

**5 Uporabe** **71**
5.1 Aritmetična zaporedja . . . 71
5.2 Podmnožice brez produktov . . . 75
5.3 Prepoznavanje komutatorjev . . . 79
5.4 Slučajni sprehodi . . . 82

**6 Razširjeni zgledi – neskončni** **91**
6.1 Kompaktne grupe . . . 92
6.2 Zvezne linearne grupe . . . 95
6.3 Diskretne linearne grupe . . . 105

**Kratek opis vsebine**

Teorija upodobitev se ukvarja z *linearizacijo* abstraktnih objektov, predvsem grup in njihovih delovanj. Gre za klasično in dobro raziskano vejo matematike, ki ima številne uporabe tudi v drugih znanostih. Dva pomembna cilja, ki ju doseže ta teorija, sta naslednja.

1. Namesto abstraktne obravnave dano grupo na različne načine uresničimo z obrnljivimi matrikami, kar nam z močnimi orodji linearne algebre omogoča bolj transparenten študij njihovih lastnosti. Tukaj nas zanimajo predvsem najenostavnejši načini predstavitev grup z matrikami.

   **Zgled 0.0.1.** Opazujmo diedrsko grupo $D_{2n} = \langle s, r \rangle$, v kateri je $s^2 = 1$, $r^n = 1$ in $srs = r^{-1}$. Ta abstraktna grupa izhaja iz simetrij pravilnega $n$-kotnika v ravnini, s čimer lahko uresničimo njena generatorja $s, r$ kot matriki

   $$s \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad r \mapsto \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix}$$

   in torej poljuben element $D_{2n}$ kot matriko v $\mathrm{GL}_2(\mathbf{R})$.

2. Številne situacije, kjer se pojavljajo grupe prek svojih delovanj, lahko lineariziramo in to linearno strukturo razstavimo na enostavne komponente, ki jih razumemo s pomočjo prejšnje točke.

   **Zgled 0.0.2.** Opazujmo simetrično grupo $S_n$, ki naravno deluje na množici $\{1, 2, \ldots, n\}$ s permutacijami. Temu delovanju lahko priredimo vektorski prostor z bazo $\{e_1, e_2, \ldots, e_n\}$. Permutaciji $\sigma \in S_n$ lahko v tej bazi priredimo permutacijsko matriko v $\mathrm{GL}_n(\mathbf{C})$, ki vektor $e_i$ preslika v $e_{\sigma(i)}$. Na ta način lahko uresničimo naravno delovanje simetrične grupe $S_n$ znotraj matrične grupe $\mathrm{GL}_n(\mathbf{C})$.

Najprej bomo vzpostavili temelje teorije upodobitev (osnovne definicije in zgledi, fundamentalne konstrukcije upodobitev). Pokazali bomo, kako se lahko približamo vsaki konkretni upodobitvi, kot da bi jo pogledali pod mikroskopom (videli bomo, da je vsaka sestavljena iz *celic*, vsaka celica pa iz *organelov*). Za tem si bomo ogledali dobro razvito teorijo upodobitev končnih grup (tu bomo pod mikroskopom videli in razumeli čudovito strukturo s pomočjo Fourierove transformacije), podrobneje bomo raziskali upodobitve dveh temeljnih družin končnih grup (simetrične grupe in splošne linearne grupe nad končnim poljem). Ta teorija ima številne uporabe, od katerih bomo izpostavili nekaj sodobnejših (v teoriji števil, kombinatoriki, slučajnih procesih na grupah). Nazadnje bomo obravnavali še nekaj zgledov upodobitev pomembnih družin neskončnih grup (kompaktne grupe ter linearne grupe, zvezne in diskretne).

**Literatura**

Pri predstavitvi temeljev teorije upodobitev uporabljamo jezik homomorfizmov grup (in ne modulov), tako da porabimo več časa za osnove, a je snov predstavljena bolj konkretno. To pride prav predvsem pri razstavljanju dane upodobitve na nerazcepne podupodobitve, pri čemer sledimo pristopu Kowalskega in opazujemo matrične koeficiente. Karakterje obdelamo v jeziku nekomutativne Fourierove transformacije kot Diaconis. S tem tudi pripravimo teren za kasnejše uporabe teorije upodobitev. Omenimo kolobar virtualnih karakterjev in kot Serre dokažemo Artinov izrek. Razširjena zgleda upodobitev simetričnih grup in splošnih linearnih grup nad končnim poljem pretežno izvedemo s pomočjo monografije Fultona in Harrisa. Pri upodobitvah simetrične grupe določene aspekte izrazimo s Fourierovo transformacijo, pri linearnih grupah pa sledeč Bushnell in Henniart nekoliko bolj naravno predstavimo ostne upodobitve. V uporabah teorije upodobitev predstavimo Rothov izrek po Gowersovo in raziščemo soroden problem za nekomutativne grupe, kjer analitične argumente napravimo kot Eberhard. Pri prepoznavanju komutatorjev nam prav pridejo razvita Fourierova orodja, slučajne sprehode pa raziščemo podobno kot Diaconis. Kompaktne grupe in povezavo s klasično Fourierovo analizo črpamo iz Kowalskega, upodobitve Liejevih grup pa prikažemo kot Fulton in Harris, pri čemer se za integriranje Liejevih homomorfizmov naslonimo na Hallovo knjigo. Diskretne grupe obdelamo sledeč Conradu in Putmanu, razliko med klasičnimi in $p$-adičnimi Liejevimi grupami prikažemo kot Choiy.


- E. Kowalski, *An Introduction to the Representation Theory of Groups*, American Mathematical Society, 2014.
- P. Diaconis, *Group representations in probability and statistics*, Lecture notes - monograph series 11, i-192, 1988.
- J. P. Serre, *Linear Representations of Finite Groups*, Springer GTM 42, 1977.
- W. Fulton, J. Harris, *Representation Theory: A First Course*, Springer GTM 129, 2004.
- C. J. Bushnell, G. Henniart, *The Local Langlands Conjecture for* $\mathrm{GL}(2)$, Springer Grundlehren der mathematischen Wissenschaften **335**, 2006.
- W. T. Gowers, *Generalizations of Fourier analysis, and how to apply them*, Bulletin of the American Mathematical Society **54**, 1-44 (2017).
- S. Eberhard, *Product mixing in the alternating group*, Discrete Analysis, 2-18 (2016).
- B. C. Hall, *Lie groups, Lie algebras, and representations*, Quantum Theory for Mathematicians, Springer, New York, NY, 2013.
- K. Conrad, $\mathrm{SL}_2(\mathbf{Z})$.
- A. Putman, *The representation theory of* $\mathrm{SL}_n(\mathbf{Z})$.
- K. Choiy, *A note on the image of continuous homomorphisms of locally profinite groups*.

### Oblika zapiskov

Zapiski so pripravljeni predvsem v elektronski obliki, ki omogoča neposreden dostop do povezanih virov in kratkih kvizov za hitro ponavljanje po poglavjih. Za tiste, ki so raje odklopljeni ali želijo tiskano različico, je na voljo tudi v formatu PDF.

### Zahvala

Zapiske sem v največji meri pripravil med izvajanjem predmeta na magistrskem študiju matematike na Fakulteti za matematiko in fiziko Univerze v Ljubljani v letu 2022/23. Zahvaljujem se študentom, ki so obiskovali predavanja in med spremljanjem opozarjali na vsebinske pomanjkljivosti. Zapiske sta še posebej podrobno pregledala študenta Hana Ibrahimpašić in Daniel Vitas. Zahvaljujem se jima za številne koristne pripombe. Za Založbo FMF je zapiske strokovno pregledal Primož Moravec. Njegovi predlogi so naredili delo bolj dostopno študentom, za kar sem mu, kot mu bodo tudi bralci, hvaležen.

# Poglavje 1

# Temelji teorije upodobitev

V tem poglavju bomo vzpostavili temelje teorije upodobitev. Spoznali bomo koncept upodobitve in si ogledali številne primere. Premislili bomo, kako upodobitve med seboj primerjamo in kako iz danih upodobitev sestavimo nove.

## 1.1 Osnovni pojmi

### Upodobitve grup

Naj bo $G$ grupa in $V$ vektorski prostor nad poljem $F$. Upodobitev grupe $G$ na prostoru $V$ je delovanje $G$ na množici $V$, ki upošteva dodatno strukturo množice $V$, namreč to, da je vektorski prostor. Natančneje, **upodobitev** (rekli bomo tudi **linearno delovanje**) grupe $G$ na prostoru $V$ je homomorfizem grup

$$\rho : G \to \mathrm{GL}(V).$$

Pri tem je $\mathrm{GL}(V)$ grupa vseh obrnljivih linearnih preslikav iz prostora $V$ vase. Razsežnosti prostora $V$ rečemo **stopnja upodobitve** in jo označimo z $\deg(\rho)$.

Ko v prostoru $V$ izberemo bazo in torej izomorfizem $V \cong F^{\deg(\rho)}$, lahko upodobitev $\rho$ enakovredno zapišemo kot homomorfizem

$$\rho : G \to \mathrm{GL}_{\deg(\rho)}(F)$$

iz grupe $G$ v obrnljive matrike razsežnosti $\deg(\rho)$ nad $F$.

Nad poljem kompleksnih števil $F = \mathbf{C}$ upodobitvam rečemo **kompleksne**, nad polji karakteristike $p > 0$, na primer $F = \mathbf{F}_p$,[1] pa upodobitvam rečemo **modularne**.

Za element $g \in G$ in vektor $v \in V$ rezultat delovanja elementa $g$ na vektorju $v$, se pravi $\rho(g)(v)$, včasih pišemo krajše kot $g \cdot v$ ali kar $gv$.[2]

**Zgled 1.1.1.**

- Opazujmo matrično grupo $\mathrm{GL}_2(\mathbf{C})$ in vektorski prostor $\mathbf{C}^2$. Množenje matrik z vektorji podaja upodobitev
$$\rho : \mathrm{GL}_2(\mathbf{C}) \to \mathrm{GL}(\mathbf{C}^2) \equiv \mathrm{GL}_2(\mathbf{C}), \quad A \mapsto (v \mapsto A \cdot v) \equiv A.$$
- Opazujmo grupo realnih števil $\mathbf{R}^*$ za množenje in vektorski prostor $\mathbf{C}$. Absolutna vrednost podaja upodobitev
$$|\cdot| : \mathbf{R}^* \to \mathrm{GL}(\mathbf{C}) = \mathbf{C}^*, \quad x \mapsto |x|.$$

[1] Končno polje ostankov celih števil pri deljenju s $p$ bomo označili s $\mathbf{F}_p$.

[2] Ta zapis odraža dejstvo, da je upodobitev pravzaprav delovanje grupe $G$ na množici $V$ z dodatnimi lastnostmi. Za vse $g, h \in G$ in $v \in V$ velja $g \cdot (h \cdot v) = (gh) \cdot v$, ker gre za delovanje grupe. Po drugi strani pa za vse $g, h \in G$, $v, w \in V$ in $\alpha \in F$ velja še $g \cdot (v + w) = g \cdot v + g \cdot w$ in $g \cdot (\alpha v) = \alpha (g \cdot v)$, ker je delovanje linearno.

- Opazujmo grupo celih števil $\mathbf{Z}$ in vektorski prostor $\mathbf{C}$. Eksponentna funkcija podaja upodobitev

$$\chi\colon \mathbf{Z} \to \mathrm{GL}(\mathbf{C}) = \mathbf{C}^*, \quad x \mapsto e^x.$$

  Splošneje imamo za vsak parameter $\alpha \in \mathbf{C}$ upodobitev

$$\chi_\alpha\colon \mathbf{Z} \to \mathrm{GL}(\mathbf{C}) = \mathbf{C}^*, \quad x \mapsto e^{\alpha x}.$$

- Opazujmo grupo ostankov $\mathbf{Z}/q\mathbf{Z}$ za poljubno naravno število $q$. Za vsak parameter $m \in \mathbf{Z}/q\mathbf{Z}$ imamo upodobitev

$$\chi_m\colon \mathbf{Z}/q\mathbf{Z} \to \mathrm{GL}(\mathbf{C}) = \mathbf{C}^*, \quad x + q\mathbf{Z} \mapsto e^{2\pi i m x/q}.$$

- Opazujmo diedrsko grupo $D_{2n} = \langle s, r \rangle$, v kateri je $s^2 = 1$, $r^n = 1$ in $srs = r^{-1}$. Ta grupa izhaja iz simetrij pravilnega $n$-kotnika v ravnini, s čimer nam ponuja svojo naravno upodobitev $\rho\colon D_{2n} \to \mathrm{GL}(\mathbf{R}^2) = \mathrm{GL}_2(\mathbf{R})$, ki preslika generatorja kot

$$s \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad r \mapsto \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix}.$$

  Splošneje imamo za vsak parameter $k \in \mathbf{Z}$ upodobitev $\rho_k\colon D_{2n} \to \mathrm{GL}(\mathbf{R}^2) = \mathrm{GL}_2(\mathbf{R})$, ki preslika generatorja kot

$$s \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad r \mapsto \begin{pmatrix} \cos(2\pi k/n) & -\sin(2\pi k/n) \\ \sin(2\pi k/n) & \cos(2\pi k/n) \end{pmatrix}.$$

- Opazujmo grupo ostankov $\mathbf{Z}/6\mathbf{Z}$ in racionalni vektorski prostor $\mathbf{Q}^2$. Preslikava

$$\rho\colon \mathbf{Z}/6\mathbf{Z} \to \mathrm{GL}(\mathbf{Q}^2) = \mathrm{GL}_2(\mathbf{Q}), \quad x + 6\mathbf{Z} \mapsto \begin{pmatrix} 1/2 & 1/8 \\ -6 & 1/2 \end{pmatrix}^x$$

  je upodobitev grupe $\mathbf{Z}/6\mathbf{Z}$. Relevantna matrika je namreč reda 6.

- Opazujmo ciklično grupo $\mathbf{Z}/p\mathbf{Z}$ za praštevilo $p$ nad končnim poljem $\mathbf{F}_p$. Preslikava

$$\rho\colon \mathbf{Z}/p\mathbf{Z} \to \mathrm{GL}(\mathbf{F}_p^2) = \mathrm{GL}_2(\mathbf{F}_p), \quad x \mapsto \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

  podaja modularno upodobitev grupe $\mathbf{Z}/p\mathbf{Z}$. Relevantna matrika je namreč reda $p$.

- Naj bo $G$ grupa in $V$ vektorski prostor nad poljem $F$. **Trivialna upodobitev** grupe $G$ je homomorfizem

$$\rho\colon G \to \mathrm{GL}(V), \quad g \mapsto \mathrm{id}_V.$$

  Kadar je vektorski prostor $V$ razsežnosti 1, trivialno upodobitev in vektorski prostor sam označimo kot $\mathbf{1}$, v primerih višje razsežnosti pa ju označimo kot $\mathbf{1}^{\dim V}$.

- Naj bo $V$ vektorski prostor in naj bo $G$ poljubna podgrupa grupe $\mathrm{GL}(V)$. Tedaj je naravna vložitev $G \to \mathrm{GL}(V)$ upodobitev grupe $G$ na prostoru $V$.

  Za konkreten zgled lahko vzamemo $V = \mathbf{C}^2$ in $G = \left\langle \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \right\rangle \leq \mathrm{GL}(\mathbf{C}^2)$. Na ta način dobimo upodobitev grupe $G \cong \mathbf{Z}$ na prostoru $\mathbf{C}^2$.

- Naj bo $G$ poljubna grupa, opremljena z delovanjem na neki množici $X$. Naj bo $F[X]$ vektorski prostor z bazo $\{e_x\}_{x \in X}$. Grupa $G$ deluje na $F[X]$ s homomorfizmom

$$\pi\colon G \to \mathrm{GL}(F[X]), \quad g \mapsto (e_x \mapsto e_{g \cdot x}),$$

  kjer je $x \in X$. To delovanje imenujemo **permutacijska upodobitev** grupe $G$ na $F[X]$.

  Za konkreten zgled lahko vzamemo $G = S_n$, ki naravno deluje na množici $X = \{1, 2, \ldots, n\}$. Na ta način dobimo permutacijsko upodobitev grupe $S_n$ na prostoru $F[\{1, 2, \ldots, n\}]$ razsežnosti $n$.

- Naj bo $G$ grupa in $F$ polje. Grupa $G$ vselej deluje na sebi s Cayleyjevim delovanjem. Prirejeni permutacijski upodobitvi grupe $G$ na $F[G]$[3] rečemo **Cayleyjeva upodobitev** grupe $G$ nad $F$. To delovanje označimo z $\pi_{\mathrm{Cay}}$.
- Naj bo $G$ grupa in $F$ polje. Naj bo $\mathrm{fun}(G,F)$ množica vseh funkcij iz množice $G$ v $F$. Te funkcije lahko po točkah seštevamo in množimo s skalarji, na ta način je $\mathrm{fun}(G,F)$ vektorski prostor. Grupa $G$ deluje na $\mathrm{fun}(G,F)$ s homomorfizmom

$$\rho_{\mathrm{fun}}\colon G \to \mathrm{GL}(\mathrm{fun}(G,F)), \quad g \mapsto (f \mapsto (x \mapsto f(xg))),$$

  kjer je $f \in \mathrm{fun}(G,F)$, $x \in G$. To delovanje izhaja iz (desnega) Cayleyjevega delovanja grupe $G$ na sebi in ga zato imenujemo **(desna) regularna upodobitev** grupe $G$ nad $F$.

Upodobitev $\rho$ grupe $G$ pohvalimo s pridevnikom **zvesta**, kadar je injektivna, torej ker $\rho = 1$. Trivialna upodobitev netrivialne grupe ni zvesta, sta pa vselej zvesti Cayleyjeva in desna regularna upodobitev.

## Kategorija upodobitev

Naj bo $G$ grupa. Opazujmo neki njeni upodobitvi $\rho_1$ in $\rho_2$ nad vektorskima prostoroma $V_1$ in $V_2$, obema nad poljem $F$. Ti dve upodobitvi lahko *primerjamo* med seboj, in sicer tako, da hkrati primerjamo vektorska prostora in delovanji grupe $G$ na teh dveh prostorih.

Natančneje, **spletična**[4] med upodobitvama $\rho_1$ in $\rho_2$ je linearna preslikava $\Phi\colon V_1 \to V_2$, za katero za vsak $g \in G$ in $v \in V_1$ velja[5]

$$\Phi(\rho_1(g)\cdot v) = \rho_2(g)\cdot\Phi(v).$$

**Zgled 1.1.2.** Opazujmo grupo $\mathbf{Z}$ in dve njeni upodobitvi, ki smo ju že videli. Prva naj bo upodobitev

$$\rho\colon \mathbf{Z} \to \mathrm{GL}(\mathbf{C}^2), \quad x \mapsto \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix},$$

druga pa naj bo kar trivialna upodobitev $\mathbf{1}$ na prostoru $\mathbf{C}$. Predpišimo linearno preslikavo $\Phi\colon \mathbf{C} \to \mathbf{C}^2$ v standardni bazi z matriko $\binom{1}{0}$. Tedaj za vsak vektor $v \in \mathbf{C}$ in vsako število $x \in \mathbf{Z}$ velja

$$\Phi(x\cdot v) = \begin{pmatrix} v \\ 0 \end{pmatrix} = x\cdot\begin{pmatrix} v \\ 0 \end{pmatrix} = x\cdot\Phi(v),$$

zato je $\Phi$ spletična med $\mathbf{1}$ in $\rho$.

Množica vseh spletičen med $\rho_1$ in $\rho_2$ je podmnožica množice linearnih preslikav $\hom(V_1,V_2)$, za katero uporabimo oznako $\hom_G(\rho_1,\rho_2)$ ali kar $\hom_G(V_1,V_2)$.

Za dano upodobitev $\rho$ grupe $G$ na vektorskem prostoru $V$ je identična preslikava $\mathrm{id}_V$ seveda spletična med $\rho$ in $\rho$. Prav tako lahko vsaki dve spletični $\Phi_1$ med $\rho_1$ in $\rho_2$ ter $\Phi_2$ med $\rho_2$ in $\rho_3$ skomponiramo do spletične $\Phi_2 \circ \Phi_1$ med $\rho_1$ in $\rho_3$. Množica vseh upodobitev dane grupe $G$ nad poljem $F$ torej tvori **kategorijo upodobitev**, katere objekti so upodobitve grupe $G$ nad $F$, morfizmi pa so spletične med upodobitvami. To kategorijo označimo z $\mathrm{Rep}_G$.

## Izomorfnost upodobitev

**Domača naloga 1.1.3.** Naj bo $\Phi\colon V_1 \to V_2$ spletična med upodobitvama $\rho_1$ in $\rho_2$, ki je obrnljiva kot linearna preslikava. Prepričaj se, da je tudi njen inverz $\Phi^{-1}\colon V_2 \to V_1$ spletična med $\rho_2$ in $\rho_1$.

Spletični $\Phi$, ki je obrnljiva kot linearna preslikava, rečemo **izomorfizem** upodobitev $\rho_1$ in $\rho_2$.

[3] Prostor $F[G]$ je vektorski prostor nad $F$, generiran z množico $G$. Običajno mu pravimo **grupna algebra**, saj ta prostor na naraven način podeduje operacijo množenja iz grupe $G$.

[4] Angleško *intertwiner*. Simpatičen prevod je po Francetu Križaniču.

[5] Z opustitvijo eksplicitnih oznak za delovanja lahko ta pogoj pišemo krajše kot $\Phi(gv) = g\Phi(v)$.

**Zgled 1.1.4.** Opazujmo ciklično grupo $\mathbf{Z}/n\mathbf{Z}$ za poljuben $n > 1$. Ta grupa naravno deluje na množici $\Omega = \{1, 2, \ldots, n\}$,[6] od koder izhaja permutacijska upodobitev

$$\pi: \mathbf{Z}/n\mathbf{Z} \to \mathrm{GL}(\mathbf{C}[\Omega]).$$

Grupa $\mathbf{Z}/n\mathbf{Z}$ ima tudi Cayleyjevo upodobitev,

$$\pi_{\mathrm{Cay}}: \mathbf{Z}/n\mathbf{Z} \to \mathrm{GL}(\mathbf{C}[\mathbf{Z}/n\mathbf{Z}]).$$

Ti dve upodobitvi sta izomorfni. Vektorska prostora lahko namreč naravno primerjamo z bijektivno linearno preslikavo

$$\Phi: \mathbf{C}[\Omega] \to \mathbf{C}[\mathbf{Z}/n\mathbf{Z}], \quad e_i \mapsto e_{\bar{i}},$$

kjer je $i \in \Omega$. Preslikava $\Phi$ je spletična, saj za vsak $\bar{x} \in \mathbf{Z}/n\mathbf{Z}$ in $i \in \Omega$ velja

$$\Phi(\bar{x} \cdot e_i) = \Phi(e_{x+i}) = e_{\overline{x+i}} = \bar{x} \cdot e_{\bar{i}} = \bar{x} \cdot \Phi(e_i).$$

V to kratko zgodbo lahko vključimo še desno regularno upodobitev

$$\rho_{\mathrm{fun}}: \mathbf{Z}/n\mathbf{Z} \to \mathrm{GL}(\mathrm{fun}(\mathbf{Z}/n\mathbf{Z}, \mathbf{C})).$$

Vektorski prostor $\mathrm{fun}(\mathbf{Z}/n\mathbf{Z}, \mathbf{C})$ lahko na naraven način opremimo z bazo iz karakterističnih funkcij

$$1_{\bar{x}}: \mathbf{Z}/n\mathbf{Z} \to \mathbf{C}, \quad \bar{y} \mapsto \begin{cases} 1 & \bar{y} = \bar{x}, \\ 0 & \text{sicer} \end{cases}$$

za $\bar{x} \in \mathbf{Z}/n\mathbf{Z}$. Predpišimo linearno preslikavo[7]

$$\Phi': \mathbf{C}[\mathbf{Z}/n\mathbf{Z}] \to \mathrm{fun}(\mathbf{Z}/n\mathbf{Z}, \mathbf{C}), \quad e_{\bar{x}} \mapsto 1_{-\bar{x}}.$$

Jasno je $\Phi'$ bijektivna. Preverimo še, da je res spletična. Za vsaka $\bar{x}, \bar{y} \in \mathbf{Z}/n\mathbf{Z}$ velja

$$\Phi'(\bar{x} \cdot e_{\bar{y}}) = \Phi'(e_{\overline{x+y}}) = 1_{-\overline{x+y}}.$$

Po drugi strani za vsak $\bar{z} \in \mathbf{Z}/n\mathbf{Z}$ velja

$$(\bar{x} \cdot \Phi'(e_{\bar{y}}))(\bar{z}) = (\bar{x} \cdot 1_{-\bar{y}})(\bar{z}) = 1_{-\bar{y}}(\bar{z} + \bar{x}) = \begin{cases} 1 & \bar{z} = -\overline{x+y}, \\ 0 & \text{sicer}. \end{cases}$$

Torej je res $\Phi'(\bar{x} \cdot e_{\bar{y}}) = \bar{x} \cdot \Phi'(e_{\bar{y}})$. S tem je $\Phi'$ izomorfizem med Cayleyjevo upodobitvijo in desno regularno upodobitvijo.

Eden pomembnih ciljev teorije upodobitev je razumeti vse upodobitve dane grupe do izomorfizma natančno. Kasneje bomo spoznali, kako lahko to v določenih[8] primerih *precej dobro* uresničimo.

## 1.2 Fundamentalne konstrukcije

Naj bo $\rho$ upodobitev grupe $G$ na prostoru $V$ nad poljem $F$. Premislili bomo, kako lahko prostor, grupo ali polje modificiramo na različne načine in tako dobimo neko drugo, novo upodobitev, oziroma kako lahko dano upodobitev vidimo kot rezultat kakšne od teh fundamentalnih konstrukcij.

[6] Generator $\bar{1} = 1 + n\mathbf{Z} \in \mathbf{Z}/n\mathbf{Z}$ deluje kot cikel $(1\ 2\ \cdots\ n)$.

[7] Pozor, karakteristična funkcija je zasidrana pri *inverzu* elementa $\bar{x}$ v $\mathbf{Z}/n\mathbf{Z}$.

[8] Na primer, *precej dobro* bomo opisali upodobitve poljubne končne grupe nad poljem kompleksnih števil.

## Podupodobitve

Naj bo $G$ grupa z upodobitvijo $\rho: G \to \mathrm{GL}(V)$. Denimo, da obstaja vektorski podprostor $W \leq V$, ki je *invarianten* za delovanje grupe $G$, se pravi $g \cdot w \in W$ za vsak $g \in G$, $w \in W$. V tem primeru upodobitev $\rho$ inducira upodobitev $\tilde{\rho}: G \to \mathrm{GL}(W)$ in vložitev vektorskih prostorov $\iota: W \to V$ je spletična. Upodobitvi $\tilde{\rho}$ rečemo **podupodobitev** upodobitve $\rho$.

**Zgled 1.2.1.**

- Naj bo $n$ naravno število. Opazujmo permutacijsko delovanje grupe $\mathbf{Z}/n\mathbf{Z}$ na množici $\Omega = \{1, 2, \ldots, n\}$, ki porodi permutacijsko upodobitev na prostoru $\mathbf{C}[\Omega]$ z baznimi vektorji $e_i$ za $i \in \Omega$. Naj bo še $e_0 = e_n$.

  Naj bo $\zeta \in \mathbf{C}$ primitiven $n$-ti koren enote. Za $j \in \Omega$ naj bo

  $$f_j = \sum_{i \in \Omega} \zeta^{ij} e_i \in \mathbf{C}[\Omega].$$

  Za vsak $\bar{x} \in \mathbf{Z}/n\mathbf{Z}$ velja

  $$\bar{x} \cdot f_j = \sum_{i \in \Omega} \zeta^{ij} e_{\overline{x+i}} = \sum_{i \in \Omega} \zeta^{(i-\bar{x})j} e_i = \zeta^{-\bar{x}j} \cdot f_j,$$

  zato je vsak podprostor $\mathbf{C} \cdot f_j \leq \mathbf{C}[\Omega]$ invarianten za delovanje grupe $\mathbf{Z}/n\mathbf{Z}$ in podupodobitev na tem podprostoru $\mathbf{C} \cdot f_j$ je očividno izomorfna upodobitvi $\chi_{-j}$ grupe $\mathbf{Z}/n\mathbf{Z}$. Na ta način smo sestavili $n$ podupodobitev permutacijske in s tem regularne upodobitve ciklične grupe moči $n$.

- Naj bo $G$ grupa in $\rho$ njena upodobitev na prostoru $V$. Opazujmo množico vseh fiksnih vektorjev te upodobitve,

  $$V^G = \{v \in V \mid \forall g \in G\colon\ g \cdot v = v\}.$$

  Množica $V^G$ je vektorski podprostor prostora $V$, ki je invarianten za delovanje grupe $G$. Torej je $\tilde{\rho}: G \to \mathrm{GL}(V^G)$ podupodobitev upodobitve $\rho$. Na prostoru $V^G$ po definiciji grupa $G$ deluje trivialno, torej je $\tilde{\rho}$ izomorfna trivialni upodobitvi $\mathbf{1}^{\dim V^G}$.

  **Domača naloga 1.2.2.** Naj bo $G$ grupa in $F$ polje. Določi upodobitvi $F[G]^G$ in $\mathrm{fun}(G,F)^G$.

  Prostor $V^G$ lahko razumemo še na naslednji alternativen način, ki nam bo prišel zelo prav v nadaljevanju. Iz vsakega vektorja $v \in V^G$ izhaja spletična

  $$\Phi_v: \mathbf{1} \to V, \quad x \mapsto xv$$

  med $\mathbf{1}$ in $\rho$. S tem je določena preslikava $V^G \to \hom_G(\mathbf{1}, V)$. Ta preslikava ima jasen inverz, ki spletični $\Phi \in \hom_G(\mathbf{1}, V)$ priredi $\Phi(1)$. Na ta način lahko identificiramo prostor $V^G$ z množico spletičen $\hom_G(\mathbf{1}, V)$.

- Naj bo $G$ grupa in $\rho$ njena upodobitev na prostoru $V$. Predpostavimo, da obstaja vektor $v \in V$, ki je lastni vektor vsake linearne preslikave $\rho(g)$ za $g \in G$.

  Torej za vsak $g \in G$ obstaja $\chi(g) \in F$, da je $\rho(g) \cdot v = \chi(g)v$. Na ta način dobimo funkcijo $\chi: G \to F$, se pravi element prostora $\mathrm{fun}(G,F)$. Ta funkcija ni čisto poljubna; ker je $\rho$ upodobitev, je $\chi$ nujno *homomorfizem* iz grupe $G$ v grupo $F^*$. Torej je $\chi$ pravzaprav upodobitev grupe $G$ na prostoru $F$ razsežnosti 1.[9]

  Zdaj kot v zadnjem zgledu s predpisom

  $$\Phi: F \to V, \quad x \mapsto xv$$

[9] Kadar je $\chi(g) = 1$ za vsak $g \in G$, je ta upodobitev izomorfna $\mathbf{1}$. Kadar je $\chi(g) \neq 1$ za vsaj kak $g \in G$, pa ta upodobitev *ni* trivialna.

dobimo injektivno spletično med $\chi$ in $\rho$, torej lahko vidimo $\chi$ kot enorazsežno podupodobitev upodobitve $\rho$. Hkrati lahko iz te spletične obnovimo podatek o skupnem lastnem vektorju $v$ in upodobitvi $\chi$.[10]

Vzpostavili smo torej bijektivno korespondenco med množico enorazsežnih podupodobitev upodobitve $\rho$ in skupnimi lastnimi vektorji vseh preslikav $\rho(g)$ za $g \in G$.

Poseben primer te korespondence je zadnji zgled. Množico enorazsežnih trivialnih podupodobitev upodobitve $\rho$ lahko identificiramo z množico neničelnih spletičen $\hom_G(\mathbf{1}, V)\setminus\{x \mapsto 0\}$, ta pa ustreza skupnim lastnim vektorjem $\rho(g)$ za $g \in G$ z lastno vrednostjo 1, kar je ravno množica $V^G\setminus\{0\}$.

- Naj bo $G$ grupa in $F$ polje. Opazujmo Cayleyjevo upodobitev $\pi_{\text{Cay}}$ na $F[G]$ in desno regularno upodobitev $\rho_{\text{fun}}$ na $\text{fun}(G,F)$. Trdimo, da je $\pi_{\text{Cay}}$ podupodobitev upodobitve $\rho_{\text{fun}}$.

  V ta namen predpišimo linearno preslikavo[11]

  $$\Phi\colon F[G] \to \text{fun}(G,F), \quad e_g \mapsto 1_{g^{-1}}$$

  za $g \in G$. Jasno je $\Phi$ injektivna preslikava. Hkrati za vse $g,h,x \in G$ velja

  $$\Phi(\pi_{\text{Cay}}(g)\cdot e_h) = \Phi(e_{gh}) = 1_{h^{-1}g^{-1}}$$

  in

  $$(\rho_{\text{fun}}(g)\cdot\Phi(e_h))(x) = 1_{h^{-1}}(xg) = 1_{h^{-1}g^{-1}}(x),$$

  zato je $\Phi$ tudi spletična.

  Kadar je grupa $G$ *končna*, sta prostora $F[G]$ in $\text{fun}(G,F)$ enake razsežnosti, zato sta v tem primeru upodobitvi $\pi_{\text{Cay}}$ in $\rho_{\text{fun}}$ izomorfni. Kadar je grupa $G$ *neskončna*, pa preslikava $\Phi$ vsekakor ni bijektivna.[12] V tem primeru upodobitvi nista izomorfni.[13]

**Domača naloga 1.2.3.** Naj bo $G$ grupa z upodobitvijo $\rho$ na prostoru $V$. Naj bo $N$ podgrupa edinka v $G$. Premisli, da množica fiksnih točk

$$V^N = \{v \in V \mid \forall n \in N\colon\ \rho(n)\cdot v = v\}$$

tvori podupodobitev upodobitve $\rho$, ki jo lahko identificiraš z množico $\hom_N(\mathbf{1}, V)$.

## Jedro, slika, kvocient

Naj bo $G$ grupa z upodobitvijo $\rho$ na prostoru $V$. Ogledali smo si že, kako za vsak $G$-invarianten podprostor $W \leq V$ dobimo podupodobitev upodobitve $\rho$. Sorodno lahko za vsak $G$-invarianten podprostor $W \leq V$ tvorimo **kvocient** $V/W$, na njem linearno deluje grupa $G$ s predpisom

$$G \to \text{GL}(V/W), \quad g \mapsto (v + W \mapsto \rho(g)\cdot v + W)$$

za $v \in V$.

Na vse do zdaj omenjene konstrukcije lahko gledamo na skupen način, in sicer s pomočjo spletične $\Phi$, ki vlaga prostor $W$ v $V$. Ni težko preveriti, da so standardne konstrukcije, ki jih lahko uporabimo na spletičnah vektorskih prostorov, na naraven način opremljene z linearnim delovanjem grupe $G$.

**Trditev 1.2.4.** *Naj bo $\Phi$ spletična upodobitev grupe $G$. Tedaj prostori* $\ker\Phi$, $\text{im}\,\Phi$, $\text{coker}\,\Phi$ *podedujejo linearno delovanje grupe $G$.*

[10] Namreč, $v = \Phi(1)$ in $\chi(g)v = \Phi(\chi(g)\cdot 1) = \rho(g)\cdot\Phi(1)$.

[11] Poseben primer te preslikave smo videli za grupo $\mathbf{Z}/n\mathbf{Z}$, kjer smo premislili, da je celo bijektivna.

[12] Slika $\text{im}\,\Phi$ namreč sestoji iz funkcij, ki so neničelne le v končno mnogo elementih grupe $G$.

[13] To sledi na primer iz dejstva, da prostora $F[G]^G$ in $\text{fun}(G,F)^G$ nista izomorfna.

**Zgled 1.2.5.** Naj bo $G$ grupa in $\rho$ njena upodobitev na prostoru $V$. Podprostor prostora $V$, na katerem grupa $G$ deluje trivialno, je vselej $G$-invarianten. Največji tak podprostor je ravno prostor vseh fiksnih vektorjev $V^G$. Videli smo že, da lahko ta prostor identificiramo z množico spletičen $\hom_G(\mathbf{1}, V)$.

Oglejmo si sedaj še dual zgodnje konstrukcije. Naj bo $V_1 = \langle \rho(g)\cdot v - v \mid v \in V,\ g \in G\rangle$. Prostor $V_1$ je $G$-invarianten podprostor prostora $V$, zato kvocient $V/V_1$ podeduje linearno delovanje grupe $G$. Po konstrukciji je to delovanje trivialno in prostor $V/V_1$ je največji kvocient prostora $V$, na katerem grupa $G$ deluje trivialno. Kvocient $V/V_1$ označimo z $V_G$ in mu pravimo **prostor koinvariant** upodobitve $\rho$.

**Domača naloga 1.2.6.** Izračunaj prostor koinvariant regularne upodobitve ciklične grupe $\mathbf{Z}/n\mathbf{Z}$.

Prostor koinvariant je po konstrukciji dualen prostoru fiksnih vektorjev, zato lahko nanj prenesemo tudi interpretacijo s spletičnami. Opazujmo množico $\hom_G(V, \mathbf{1})$. Spletične iz te množice so ravno linearne preslikave $\lambda: V \to F$ z lastnostjo $\lambda(\rho(g)\cdot v) = \lambda(v)$ za vsaka $v \in V$, $g \in G$, kar je ekvivalentno pogoju $\lambda(V_1) = 0$. Vsako tako spletično lahko zato interpretiramo kot linearno preslikavo iz $V/V_1 = V_G$ v $F$. Na ta način je vzpostavljena bijektivna korespondenca med množico spletičen $\hom_G(V, \mathbf{1})$ in množico linearnih preslikav $\hom_F(V_G, F)$, slednja množica pa je ravno dual $V_G^*$ prostora koinvariant $V_G$.

## Direktna vsota

Naj ima grupa $G$ družino upodobitev $\{\rho_i\}_{i\in I}$ na vektorskih prostorih $\{V_i\}_{i\in I}$. Tedaj lahko tvorimo direktno vsoto vektorskih prostorov $\bigoplus_{i\in I} V_i$, ki je opremljena z linearnim delovanjem

$$\bigoplus_{i\in I} \rho_i : G \to \mathrm{GL}\Big(\bigoplus_{i\in I} V_i\Big), \quad g \mapsto \left(\sum_{i\in I} v_i \mapsto \sum_{i\in I} \rho_i(g)\cdot v_i\right).$$

Na ta način dobimo **direktno vsoto** upodobitev $\bigoplus_{i\in I} \rho_i$. Pri tem je vsaka od upodobitev $\rho_i$ podupodobitev te direktne vsote.

**Zgled 1.2.7.**

- Opazujmo permutacijsko upodobitev $\pi$ grupe $\mathbf{Z}/n\mathbf{Z}$ na prostoru $\mathbf{C}[\Omega]$, kjer je $\Omega = \{1, 2, \ldots, n\}$. Premislili smo že, da ima ta upodobitev $n$ podupodobitev. Za vsak $j \in \Omega$ imamo upodobitev na podprostoru $\mathbf{C}\cdot f_j$, ki je izomorfna upodobitvi $\chi_{-j}$. Ker je množica vektorjev $\{f_j \mid j \in \Omega\}$ linearno neodvisna,[14] lahko permutacijsko upodobitev torej zapišemo kot direktno vsoto $\pi = \bigoplus_{j\in\Omega} \chi_j$.

  **Domača naloga 1.2.8.** Prepričaj se, da so upodobitve $\chi_j$ za $j \in \Omega$ grupe $\mathbf{Z}/n\mathbf{Z}$ med seboj paroma neizomorfne.

- Opazujmo permutacijsko upodobitev simetrične grupe $S_3$ na prostoru $\mathbf{R}[\{1,2,3\}] = \mathbf{R}^3$. Delovanje grupe $S_3$ ohranja vektor $e_1 + e_2 + e_3$, zato ima ta upodobitev trivialno enorazsežno podupodobitev, dano s podprostorom $\langle e_1 + e_2 + e_3\rangle$. Eden od komplementov tega podprostora je $\langle e_1 - e_2, e_2 - e_3\rangle$, ki je hkrati $S_3$-invariaten podprostor.[15] Če označimo $u_1 = e_1 - e_2$ in $u_2 = e_2 - e_3$, lahko slednjo upodobitev opišemo s homomorfizmom

  $$\rho: S_3 \to \mathrm{GL}(\langle u_1, u_2\rangle), \quad (1\ 2) \mapsto \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \quad (1\ 2\ 3) \mapsto \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

  Permutacijska upodobitev $S_3$ je zato direktna vsota enorazsežne podupodobitve $\mathbf{1}$ in dvorazsežne podupodobitve $\rho$.

  Premislimo, da upodobitve $\rho$ *ne* moremo zapisati kot direktne vsote svojih pravih podupodobitev. V ta namen opazujmo njene morebitne enorazsežne podupodobitve. Premislili smo že, da te ustrezajo skupnim lastnim vektorjem vseh preslikav $\rho(x)$ za $x \in S_3$. Lastna vektorja $\rho((1\ 2))$ sta $u_1$ in $u_1 + 2u_2$. Noben od teh dveh vektorjev ni hkrati lastni vektor $\rho((1\ 2\ 3))$. Torej je upodobitev $\rho$ stopnje 2, hkrati pa nima enorazsežnih podupodobitev in je torej ne moremo razstaviti nadalje.

[14] Prehodna matrika iz baze $e_i$ v bazo $f_j$ je ravno Vandermondova matrika.

[15] Na primer, generator $(1\ 3\ 2)$ preslika vektor $e_1 - e_2$ v $e_3 - e_1$, kar lahko zapišemo kot $-(e_1 - e_2) - (e_2 - e_3)$.

Direktna vsota je najbolj preprost način, kako lahko iz danih upodobitev sestavimo novo upodobitev. V nadaljevanju bomo zato veliko časa posvetili obratnemu problemu: dano upodobitev bomo kot v zadnjem zgledu skušali razstaviti na direktno vsoto čim bolj enostavnih podupodobitev.

## Tenzorski produkt

Naj ima grupa $G$ upodobitvi $\rho_1$ in $\rho_2$ na prostorih $V_1$ in $V_2$. Tedaj lahko tvorimo **tenzorski produkt** vektorskih prostorov $V_1 \otimes V_2$, ki je naravno opremljen z linearnim delovanjem

$$\rho_1 \otimes \rho_2 : G \to \mathrm{GL}(V_1 \otimes V_2), \quad g \mapsto (v_1 \otimes v_2 \mapsto \rho_1(g)v_1 \otimes \rho_2(g)v_2).$$

**Domača naloga 1.2.9.** Izberimo bazi prostorov $V_1$ in $V_2$. Tenzorski produkti baznih elementov tvorijo bazo prostora $V_1 \otimes V_2$. Kako je videti matrika $(\rho_1 \otimes \rho_2)(g)$ v odvisnosti od matrik $\rho_1(g)$ in $\rho_2(g)$?

**Zgled 1.2.10.** Opazujmo simetrično grupo $S_3$. Ogledali smo si že njeno permutacijsko upodobitev na prostoru $\mathbf{R}^3$, ki smo jo razstavili na direktno vsoto trivialne upodobitve $\mathbf{1}$ in dvorazsežne upodobitve $\rho$. Poleg teh dveh ima grupa $S_3$ še eno zanimivo upodobitev, ki izračuna predznak dane permutacije, se pravi

$$\mathrm{sgn} : S_3 \to \mathrm{GL}(\mathbf{R}) = \mathbf{R}^*, \quad \sigma \mapsto \mathrm{sgn}(\sigma).$$

To je netrivialna enorazsežna upodobitev.

Tvorimo tenzorski produkt upodobitev $\rho$ in sgn. Dobimo upodobitev na vektorskem prostoru $\mathbf{R} \otimes \mathbf{R}^2$, ki ga lahko naravno identificiramo s prostorom $\mathbf{R}^2$. V tem smislu je upodobitev $\mathrm{sgn} \otimes \rho$ izomorfna dvorazsežni upodobitvi

$$S_3 \to \mathrm{GL}(\mathbf{R}^2), \quad \sigma \mapsto (v \mapsto \mathrm{sgn}(\sigma) \cdot \rho(\sigma) \cdot v).$$

**Domača naloga 1.2.11.** Dokaži, da sta upodobitvi $\rho$ in $\mathrm{sgn} \otimes \rho$ izomorfni.

Naj ima grupa $G$ upodobitev na prostoru $V$. Tedaj lahko tvorimo **tenzorske potence** $V^{\otimes n}$ za $n \in \mathbf{N}_0$. Vsaka od teh tvori upodobitev grupe $G$. Na prostoru $V^{\otimes n}$ deluje simetrična grupa $S_n$, in sicer na dva načina. Prvi način izhaja iz permutacijske upodobitve grupe $S_n$, in sicer dobimo delovanje

$$\pi : S_n \to \mathrm{GL}(V^{\otimes n}), \quad \sigma \mapsto \left(v_1 \otimes v_2 \otimes \cdots \otimes v_n \mapsto v_{\sigma(1)} \otimes v_{\sigma(2)} \otimes \cdots \otimes v_{\sigma(n)}\right).$$

Drugi način delovanja grupe $S_n$ na tenzorski potenci pa je $\mathrm{sgn} \otimes \pi$, pri katerem delovanje $\pi$ še utežimo s predznakom delujoče permutacije. Prostor koinvariant upodobitve $\pi$ je

$$\mathrm{Sym}^n(V) = \frac{V^{\otimes n}}{\left\langle v_1 \otimes v_2 \otimes \cdots \otimes v_n - v_{\sigma(1)} \otimes v_{\sigma(2)} \otimes \cdots \otimes v_{\sigma(n)} \mid v_i \in V,\ \sigma \in S_n \right\rangle},$$

imenujemo ga **simetrična potenca** upodobitve $G$ na $V$. Analogno prostor koinvariant upodobitve $\mathrm{sgn} \otimes \pi$ označimo z $\bigwedge^n(V)$ in imenujemo **alternirajoča potenca**. Obe potenci sta seveda upodobitvi grupe $G$. Vse potence hkrati zajamemo z direktnima vsotama

$$\mathrm{Sym}(V) = \oplus_{n \in \mathbf{N}_0} \mathrm{Sym}^n(V) \quad \text{in} \quad \bigwedge V = \oplus_{n \in \mathbf{N}_0} \bigwedge^n(V).$$

**Domača naloga 1.2.12.** Naj bo $G$ grupa s kompleksno upodobitvijo $\rho$ na prostoru $V$ razsežnosti $\deg(\rho) < \infty$. Dokaži, da je upodobitev $G$ na alternirajoči potenci $\bigwedge^{\deg(\rho)} V$ izomorfna enorazsežni upodobitvi $G \to \mathbf{C}^*$, $g \mapsto \det(\rho(g))$.

## Dual

Naj bo $G$ grupa z upodobitvijo $\rho$ na prostoru $V$ nad poljem $F$. Tvorimo lahko **dualen prostor** $V^* = \hom(V,F)$, ki je naravno opremljen z linearnim delovanjem

$$\rho^*: G \to \mathrm{GL}(V^*), \quad g \mapsto \big(\lambda \mapsto \big(v \mapsto \lambda(\rho(g^{-1})\cdot v)\big)\big)$$

za $\lambda \in V^*$, $v \in V$. Na ta način dobimo **dualno upodobitev** $\rho^*$ upodobitve $\rho$.

Za funkcional $\lambda \in V^*$ in vektor $v \in V$ včasih uporabimo oznako $\langle \lambda, v\rangle$ za uporabo $\lambda(v)$. S to oznako lahko zapišemo definicijo dualne upodobitve kot

$$\langle \rho^*(g)\cdot\lambda, v\rangle = \langle \lambda, \rho(g^{-1})\cdot v\rangle.$$

**Zgled 1.2.13.** Opazujmo grupo $\mathbf{Z}$ in za parameter $a \in \mathbf{C}$ njeno upodobitev

$$\chi_a: \mathbf{Z} \to \mathrm{GL}(\mathbf{C}), \quad x \mapsto e^{ax}.$$

Za dualno upodobitev $\chi_a^*$, funkcional $\lambda \in \mathbf{C}^*$ in vektor $z \in \mathbf{C}$ velja

$$\langle \chi_a^*(x)\cdot\lambda, z\rangle = \langle \lambda, \chi_a(-x)\cdot z\rangle = \lambda(e^{-ax}\cdot z).$$

Funkcionali v dualnem prostoru $\mathbf{C}^*$ so skalarna množenja s kompleksnimi števili. Če funkcionalu $\lambda$ ustreza število $l \in \mathbf{C}$, dobimo torej

$$\chi_a^*(x)\cdot l = e^{-ax}\cdot l.$$

Dualna upodobitev $\chi_a^*$ je torej enorazsežna upodobitev, ki je izomorfna upodobitvi $\chi_{-a}$.

**Domača naloga 1.2.14.** Naj bo $G$ grupa.

- Naj bosta $\rho_1, \rho_2$ upodobitvi grupe $G$ in predpostavimo, da je vsaj ena končne stopnje. Dokaži, da je

$$(\rho_1 \oplus \rho_2)^* \cong \rho_1^* \oplus \rho_2^* \quad \text{in} \quad (\rho_1 \otimes \rho_2)^* \cong \rho_1^* \otimes \rho_2^*.$$

- Naj bo $\rho$ upodobitev grupe $G$ končne stopnje. Tedaj je $(\rho^*)^* \cong \rho$.

Naj bo zdaj $G$ grupa z dvema upodobitvama $\rho$ in $\sigma$ na prostorih $V$ in $W$. **Prostor linearnih preslikav** $\hom(V,W)$ je naravno opremljen z linearnim delovanjem

$$\hom(\rho,\sigma): G \to \mathrm{GL}(\hom(V,W)), \quad g \mapsto \big(\Phi \mapsto \big(v \mapsto \sigma(g)\cdot\Phi\cdot\rho(g^{-1})\cdot v\big)\big).$$

Invariante tega delovanja sestojijo iz linearnih preslikav, ki so invariantne glede na predpisano delovanje grupe $G$, se pravi ravno iz spletičen med $\rho$ in $\sigma$. S simboli je torej $\hom(V,W)^G = \hom_G(V,W)$.

**Trditev 1.2.15.** *Naj bo $G$ grupa z upodobitvama $\rho$ in $\sigma$. Predpostavimo, da je $\deg(\sigma) < \infty$. Tedaj je $\hom(\rho,\sigma) \cong \rho^* \otimes \sigma$.*

*Dokaz.* Naj bo $\rho$ upodobitev na prostoru $V$ in $\sigma$ upodobitev na prostoru $W$. Izomorfizem med vektorskima prostoroma $V^* \otimes W$ in $\hom(V,W)$ podaja linearna preslikava

$$V^* \otimes W \to \hom(V,W), \quad \lambda \otimes w \mapsto (v \mapsto \lambda(v)\cdot w).$$

Ni težko preveriti, da je ta preslikava spletična. □

## Skalarji

Naj bo $G$ grupa z upodobitvijo $\rho$ na prostoru $V$ nad poljem $F$. Naj bo $E$ razširitev polja $F$. Tedaj je prostor $E \otimes V$ naravno opremljen z linearnim delovanjem

$$E \otimes \rho : G \to \mathrm{GL}(E \otimes V), \quad g \mapsto (e \otimes v \mapsto e \otimes \rho(g) \cdot v).$$

Ta postopek konstrukcije prostora $E \otimes V$ imenujemo **razširitev skalarjev**. Dano upodobitev lahko razširimo do ugodnejših skalarjev[16], lahko pa tudi dano upodobitev nad velikim poljem $E$ gledamo kot razširitev skalarjev neke upodobitve nad preprostejšim poljem $F$.[17] V tem primeru rečemo, da je dana upodobitev **definirana nad poljem** $F$. Včasih nam uspe najti celo preprost *podkolobar* polja $F$, nad katerim je definirana dana upodobitev.

**Zgled 1.2.16.** Opazujmo grupo $S_3$ in njeno permutacijsko upodobitev na realnem prostoru $\mathbf{R}[\{1,2,3\}]$. Poznamo že njeno dvorazsežno upodobitev $\rho$ na podprostoru $\langle e_1 - e_2, e_2 - e_3 \rangle$, ki *nima* enorazsežnih podupodobitev. Ta je definirana z matrikami, ki imajo zgolj celoštevilske koeficiente. Upodobitev $\rho$ je zato definirana nad *kolobarjem* $\mathbf{Z}$. To upodobitev lahko zato *projiciramo* s homomorfizmom kolobarjev $\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$ za poljubno praštevilo $p$ do upodobitve

$$S_3 \to \mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z}), \quad (1\ 2) \mapsto \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \quad (1\ 2\ 3) \mapsto \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix},$$

ki je definirana nad *končnim* poljem $\mathbf{Z}/p\mathbf{Z}$. Pri $p = 3$ ima ta projicirana upodobitev enorazsežen invarianten podprostor $\langle e_1 + e_2 + e_3 \rangle$. Projekcije nam lahko torej dano upodobitev dodatno razstavijo.

Kadar imamo opravka s konkretnim poljem $F$, lahko dano upodobitev modificiramo tudi z **avtomorfizmi polja**. Te si najlažje predstavljamo po izbiri baze vektorskega prostora. Če je $\sigma \in \mathrm{Aut}(F)$, dobimo iz dane upodobitve $\rho : G \to \mathrm{GL}_n(F)$ modificirano upodobitev

$$\rho^\sigma : G \to \mathrm{GL}_n(F), \quad g \mapsto \rho(g)^\sigma,$$

pri kateri vsak člen matrike $\rho(g)$ preslikamo z avtomorfizmom $\sigma$.

**Zgled 1.2.17.** Naj bo $G$ grupa s kompleksno upodobitvijo $\rho$. Kompleksno konjugiranje je avtomorfizem polja $\mathbf{C}$, zato lahko s konjugiranjem členov matrik tvorimo **konjugirano upodobitev** $\overline{\rho}$.

## Restrikcija

Naj bo $G$ grupa z upodobitvijo $\rho : G \to \mathrm{GL}(V)$. Kadar je na voljo še ena grupa $H$ s homomorfizmom $\phi : H \to G$, lahko upodobitev $\rho$ sklopimo s $\phi$ in dobimo upodobitev $\rho \circ \phi$ grupe $H$ na prostoru $V$. Temu postopku pridobivanja upodobitev grupe $H$ iz upodobitev grupe $G$ pravimo **restrikcija**, pri tem pa novo upodobitev $\rho \circ \phi$ označimo kot $\mathrm{Res}^G_H(\rho)$. Predstavljamo si, da smo upodobitev $\rho$ *potegnili nazaj* vzdolž homomorfizma $\phi$. Restrikcija je funktor iz kategorije $\mathrm{Rep}_G$ v kategorijo $\mathrm{Rep}_H$.

**Zgled 1.2.18.** Naj bo $G$ grupa s podgrupo edinko $N$. Tvorimo kvocientni homomorfizem $\phi : G \to G/N$. Vsaki upodobitvi grupe $G/N$ lahko z restrikcijo priredimo upodobitev grupe $G$. Vsaka taka pridobljena upodobitev grupe $G$ vsebuje podgrupo $N$ v svojem jedru. Na ta način dobimo bijektivno korespondenco med upodobitvami grupe $G/N$ in upodobitvami grupe $G$, ki so trivialne na $N$.

Običajno ni res, da je vsaka upodobitev grupe $G$ trivialna na $N$, se pa to lahko zgodi v kakšnih posebnih primerih. Na primer, *enorazsežne* upodobitve grupe $G$ nad poljem $F$ so homomorfizmi iz $G$ v $F^*$, kar ravno ustreza homomorfizmom iz abelove grupe $G/[G,G]$ v $F^*$. Vsaka enorazsežna upodobitev grupe $G$ je torej trivialna na $[G,G]$.

Za konkreten primer si oglejmo simetrično grupo $S_n$. Njene kompleksne enorazsežne upodobitve ustrezajo homomorfizmom $S_n \to \mathbf{C}^*$. Ker je $[S_n, S_n] = A_n$, opazujemo torej homomorfizme $S_n/A_n \cong \mathbf{Z}/2\mathbf{Z} \to \mathbf{C}^*$. Na voljo sta le dva taka homomorfizma: trivialen in netrivialen (ki preslika generator grupe $\mathbf{Z}/2\mathbf{Z}$ v $-1 \in \mathbf{C}^*$). Prvi ustreza trivialni upodobitvi $\mathbf{1}$, drugi pa ustreza predznačni upodobitvi sgn.

[16] Na primer polja kompleksnih števil.

[17] Na primer $E = \mathbf{C}$ in $F = \mathbf{Q}$.

Kadar imamo na voljo tri grupe, povezane s homomorfizmoma $\phi_2 : H_2 \to H_1$ in $\phi_1 : H_1 \to G$, lahko restrikcijo izvedemo dvakrat zaporedoma. Upodobitvi $\rho$ v $\mathrm{Rep}_G$ tako priredimo upodobitev $\mathrm{Res}^{H_1}_{H_2}(\mathrm{Res}^{G}_{H_1}(\rho))$ v $\mathrm{Rep}_{H_2}$. Od grupe $H_2$ do $G$ imamo neposredno povezavo prek homomorfizma $\phi_1 \circ \phi_2$, s čimer dobimo upodobitev $\mathrm{Res}^{G}_{H_2}(\rho)$. Ni težko preveriti, da sta dobljeni upodobitvi izomorfni. Tej lastnosti restrikcije pravimo **tranzitivnost**.

## Indukcija

Naj bo kot zgoraj $G$ grupa in $H$ še ena grupa s homomorfizmom $\phi : H \to G$. **Indukcija** je postopek, ki s pomočjo homomorfizma $\phi$ upodobitvi $\rho$ grupe $H$ priredi upodobitev grupe $G$. Indukcija torej deluje ravno v obratno smer kot restrikcija in nam omogoča, da upodobitev $\rho$ *potisnemo naprej* vzdolž homomorfizma $\phi$. Ta postopek je nekoliko bolj zapleten kot restrikcija.

Začnimo z upodobitvijo $\rho : H \to \mathrm{GL}(V)$. Konstruirali bomo prostor, na katerem deluje grupa $G$. Odskočna deska za to bo regularna upodobitev grupe $G$, katere vektorski prostor je prostor funkcij $\mathrm{fun}(G,F)$. Ta prostor razširimo s prostorom $V$ do prostora funkcij

$$\mathrm{fun}(G,V) = \{f \mid f : G \to V\},$$

na katerem linearno deluje grupa $G$ z analogom regularne upodobitve, in sicer kot

$$g \cdot f = (x \mapsto f(xg))$$

za $g \in G$, $f \in \mathrm{fun}(G,V)$. Po drugi strani na tej množici deluje tudi grupa $H$, in sicer na dva načina: prvič prek homomorfizma $\phi$ in pravkar opisanega delovanja grupe $G$, drugič pa prek svojega delovanja $\rho$ na prostoru $V$. Ko ti dve delovanji združimo, dobimo delovanje grupe $H$ na prostoru funkcij $\mathrm{fun}(G,V)$ s predpisom

$$h \cdot f = \left(x \mapsto \rho(h) \cdot f\left(\phi(h^{-1}) \cdot x\right)\right)$$

za $h \in H$, $f \in \mathrm{fun}(G,V)$.[18] Opazujmo invariantni podprostor

$$\mathrm{fun}(G,V)^H = \{f \in \mathrm{fun}(G,V) \mid \forall h \in H, x \in G.\ \rho(h) \cdot f(x) = f(\phi(h) \cdot x)\}.$$

Ker grupa $G$ deluje na $\mathrm{fun}(G,V)$ prek množenja z *desne*, pogoj pripadnosti invariantam $\mathrm{fun}(G,V)^H$ pa je izražen prek množenja z *leve*, je podprostor $\mathrm{fun}(G,V)^H$ avtomatično $G$-invarianten. S tem smo dobili upodobitev grupe $G$ na prostoru $\mathrm{fun}(G,V)^H$. To je želena **inducirana upodobitev**. Zanjo uporabimo oznako $\mathrm{Ind}^G_H(\rho)$.

**Zgled 1.2.19.** Naj bo $G$ grupa z vložitvijo $\phi : 1 \to G$ trivialne podgrupe. Vsaka upodobitev trivialne grupe nad poljem $F$ je trivialna. Iz enorazsežne trivialne upodobitve $\mathbf{1}$ dobimo prostor funkcij $\mathrm{fun}(G,F)$, na katerem grupa $G$ deluje z regularno upodobitvijo. Inducirana upodobitev je v tem primeru torej kar regularna, se pravi $\mathrm{Ind}^G_1(\mathbf{1}) = \rho_{\mathrm{fun}}$.

Inducirano upodobitev $\mathrm{Ind}^G_H(\rho) = \mathrm{fun}(G,V)^H$ smo konstruirali z invariantami grupe $H$. To pomeni, da vektorji v tem prostoru niso poljubne funkcije v $\mathrm{fun}(G,V)$, temveč zadoščajo določenim restriktivnim pogojem. Te funkcije so določene z vrednostmi, ki jih zavzamejo na predstavnikih desnih odsekov $\mathrm{im}\,\phi \backslash G$,[19] in te vrednosti pripadajo podprostoru $V^{\ker\phi}$.[20]

**Zgled 1.2.20.** Naj bo $G$ grupa z upodobitvijo $\rho$ in naj bo $\phi = \mathrm{id}_G$. Tedaj je vsaka funkcija $f \in \mathrm{fun}(G,V)^G$ določena že z vrednostjo $f(1)$. Dodatnih restrikcij za to vrednost ni, zato dobimo izomorfizem vektorskih prostorov

$$\mathrm{fun}(G,V)^G \to V, \quad f \mapsto f(1),$$

ki je spletična glede na regularno delovanje $G$ na $\mathrm{fun}(G,V)$. S tem imamo torej izomorfizem upodobitev $\mathrm{Ind}^G_G(\rho) \cong \rho$.

[18] Delovanje $H$ na $\mathrm{fun}(G,V)$ je konstruirano analogno delovanju grupe na prostoru linearnih preslikav.

[19] Če je $R$ množica predstavnikov desnih odsekov $\mathrm{im}\,\phi$ v $G$ in če že poznamo vrednosti $f \in \mathrm{fun}(G,V)$ na množici $R$, potem lahko vsako drugo vrednost $f$ izračunamo kot $f(x \cdot r) = \rho(y) \cdot f(r)$ za $x = \phi(y) \in \mathrm{im}\,\phi$.

[20] Če je $f \in \mathrm{fun}(G,V)^H$, potem pogoj $H$-invariantnosti uporabimo z elementi $h \in \ker\phi$ in dobimo $\rho(h) \cdot f(x) = f(x)$, torej je $f \in V^h$.

**Domača naloga 1.2.21.** Naj bo $G$ grupa z upodobitvijo $\rho$ na prostoru $V$ in naj bo $\phi\colon G \to G/N$ kvocientna projekcija za neko podgrupo edinko $N$ v $G$. Dokaži, da je $\mathrm{Ind}_G^{G/N}(\rho)$ izomorfna upodobitvi $G/N$ na prostoru $V^N$, ki izhaja iz upodobitve $\rho$.

Najpomembnejši primer indukcije, čeravno ne tudi najbolj preprost, je **indukcija iz podgrupe končnega indeksa**. Naj bo $G$ grupa s podgrupo $H$ in naj bo $\phi$ vložitev $H$ v $G$. Predpostavimo, da je $|G:H| < \infty$. Naj bo $\rho$ upodobitev grupe $H$ na prostoru $V$. Premislimo, kako je videti upodobitev $\mathrm{Ind}_H^G(\rho)$.

Naj bo $R$ neka izbrana množica predstavnikov desnih odsekov $H$ v $G$. Vsaka funkcija $f \in \mathrm{fun}(G,V)^H$ je določena z vrednostmi $f(r)$ za $r \in R$ in dodatnih restrikcij za te vrednosti ni, zato dobimo izomorfizem vektorskih prostorov[21]

$$\Phi\colon \mathrm{fun}(G,V)^H \to \mathrm{fun}(R,V), \quad f \mapsto (r \mapsto f(r)).$$

Da dobimo spletično, moramo posplošitev regularnega delovanja $G$ na $\mathrm{fun}(G,V)$ prenesti prek linearnega izomorfizma $\Phi$ na desno stran. V ta namen naj bo $v \in V$ in $f \in \mathrm{fun}(G,V)^H$ z lastnostjo $f(r_0) = v$ in $f(r) = 0$ za $r \in R \setminus \{r_0\}$. Za vsak $g \in G$ mora tako veljati

$$g \cdot \left( r \mapsto \begin{cases} v & r = r_0, \\ 0 & r \neq r_0 \end{cases} \right) = \Phi(g \cdot f) = \Phi(x \mapsto f(xg)).$$

Za $x \in R$ z lastnostjo $xg \in Hr_0$, se pravi $x = hr_0g^{-1}$ za nek $h \in H$, velja $f(xg) = f(hr_0) = \rho(h) \cdot v$. Seveda je $|R \cap Hr_0g^{-1}| = 1$, torej obstaja natanko en tak $x$. Za $x \in R$ z lastnostjo $xg \notin Hr_0$ pa velja $f(xg) = 0$. S tem je

$$g \cdot \left( r \mapsto \begin{cases} v & r = r_0, \\ 0 & r \neq r_0 \end{cases} \right) = \left( r \mapsto \begin{cases} \rho(h) \cdot v & r = hr_0g^{-1} \text{ za nek } h \in H, \\ 0 & r \notin Hr_0g^{-1} \end{cases} \right).$$

Da bo preslikava $\Phi$ spletična, moramo na $\mathrm{fun}(R,V)$ torej uvesti tako delovanje grupe $G$, ki dani vektor $v$ pri vnosu $r_0 \in R$ preslika tako, da najprej izračuna odsek elementa $r_0g^{-1}$ po $H$, ta element zapiše kot $r_0g^{-1} = h^{-1}r$ za $h \in H$, $r \in R$, nato pa na vektor $v$ deluje z $\rho(h)$ in ga hkrati prestavi k vnosu $r$.

Opisan postopek si lahko nekoliko lažje predstavljamo tako, da množico $\mathrm{fun}(R,V)$ identificiramo z direktno vsoto $\bigoplus_{r \in R} Vr$, kjer je $Vr$ kopija vektorskega prostora $V$ pri komponenti $r$. Element $g \in G$ deluje na vektorju $vr_0 \in Vr_0$ kot $g^{-1}$ z desne. V teh domačih oznakah izračunamo

$$g \cdot vr_0 = vr_0g^{-1} = vh^{-1}r = (h \cdot v)r = (\rho(h) \cdot v)r,$$

kar ravno ustreza bolj zakompliciranemu zapisu zgoraj.

Poseben primer opisane indukcije dobimo z enorazsežnimi upodobitvami grupe $H$. Vsak homomorfizem $\rho\colon H \to F^*$ porodi prostor $\mathrm{fun}(G,F)^H$ razsežnosti $|G:H|$, ki je podprostor prostora funkcij $\mathrm{fun}(G,F)$ in na katerem torej grupa $G$ deluje z regularno upodobitvijo. Inducirana upodobitev je v tem primeru podupodobitev regularne upodobitve $\rho_{\mathrm{fun}}$. Na ta način lahko dobimo mnogo različnih upodobitev grupe $G$.

**Zgled 1.2.22.** Opazujmo grupo $S_n$ in njeno podgrupo $A_n$ indeksa 2. Za $n \geq 5$ je grupa $A_n$ enostavna, zato je $A_n = [A_n, A_n]$ in ni netrivialnih enorazsežnih upodobitev. Oglejmo si inducirano upodobitev $\mathrm{Ind}_{A_n}^{S_n}(\mathbf{1})$. A priori vemo, da je to dvorazsežna upodobitev. Za množico predstavnikov odsekov vzamemo $R = \{(), (1\,2)\}$. V domačih oznakah je vektorski prostor upodobitve enak $F() \oplus F(1\,2)$, na katerem deluje grupa $S_n$ s predpisom

$$g \cdot x\sigma = x\sigma g^{-1} = \begin{cases} x\sigma & g \in A_n, \\ x((1\,2)\sigma) & g \notin A_n \end{cases}$$

za $g \in S_n$, $x \in F$, $\sigma \in R$. To delovanje lahko zapišemo še enostavneje. Vektorski prostor identificiramo z dvorazsežnim prostorom $F^2$, delovanje pa opišemo kot

$$g \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{cases} \begin{pmatrix} x \\ y \end{pmatrix} & g \in A_n, \\ \begin{pmatrix} y \\ x \end{pmatrix} & g \notin A_n \end{cases}$$

[21] Množico funkcij $\mathrm{fun}(R,V)$ lahko vidimo kot direktno vsoto prostorov $V$, indeksirano z množico $R$.

za $x,y \in F$, $g \in S_n$. Alternirajoča grupa $A_n$ je v jedru te upodobitve, ki zato izhaja iz kvocienta $S_n/A_n \cong \mathbf{Z}/2\mathbf{Z}$. Opisana upodobitev je natanko permutacijska upodobitev grupe $\mathbf{Z}/2\mathbf{Z}$ na prostoru $F[\{1,2\}]$, inducirana upodobitev pa je ravno restrikcija te upodobitve vzdolž kvocientne projekcije $S_n \to S_n/A_n$. Inducirano upodobitev lahko zapišemo kot vsoto dveh enorazsežnih podupodobitev. Prva je podupodobitev z diagonalnim prostorom $\{(x,x) \mid x \in F\} \leq F^2$, ta je izomorfna trivialni upodobitvi $\mathbf{1}$. Druga pa je podupodobitev z antidiagonalnim prostorom $\{(x,-x) \mid x \in F\} \leq F^2$. Ta ni trivialna, saj element $(1\ 2)$ deluje na $(1,-1)$ kot množenje z $-1 \in F$. Ta podupodobitev je zato izomorfna predznačni upodobitvi sgn. Nazadnje je torej $\mathrm{Ind}_{A_n}^{S_n}(\mathbf{1}) \cong \mathbf{1} \oplus \mathrm{sgn}$.

Naj bosta $G,H$ grupi s homomorfizmom $\phi\colon H \to G$. Ni težko preveriti, da indukcija naravno prenese spletično med dvema upodobitvama grupe $H$ v spletično med induciranima upodobitvama. Indukcija je torej funktor iz kategorije $\mathrm{Rep}_H$ v kategorijo $\mathrm{Rep}_G$.

Kadar imamo na voljo tri grupe, povezane s homomorfizmoma $\phi_2\colon H_2 \to H_1$ in $\phi_1\colon H_1 \to G$, lahko indukcijo izvedemo dvakrat zaporedoma. Upodobitvi $\rho$ v $\mathrm{Rep}_{H_2}$ tako priredimo upodobitev $\mathrm{Ind}_{H_1}^{G}(\mathrm{Ind}_{H_2}^{H_1}(\rho))$ v $\mathrm{Rep}_G$. Od grupe $H_2$ do $G$ imamo neposredno povezavo prek homomorfizma $\phi_1 \circ \phi_2$, s čimer dobimo upodobitev $\mathrm{Ind}_{H_2}^{G}(\rho)$. Ni težko preveriti, da sta dobljeni upodobitvi izomorfni. Tej lastnosti indukcije pravimo **tranzitivnost**.

**Domača naloga 1.2.23.** Dokaži tranzitivnost indukcije.

S tranzitivnostjo indukcije lahko vsako indukcijo vzdolž homomorfizma $\phi\colon H \to G$ razdelimo na tri korake: najprej induciramo vzdolž kvocientne projekcije $H \to H/\ker\phi$, nato vzdolž izomorfizma $H/\ker\phi \to \mathrm{im}\,\phi$ in nazadnje vzdolž vložitve $\mathrm{im}\,\phi \to G$. Vsako od teh posameznih indukcij razumemo precej dobro in zato lahko to znanje uporabimo pri razumevanju indukcije vzdolž $\phi$. Na primer, iz povedanega in razmislekov o preprostejših indukcijah, ki smo jih že naredili, sledi, da je razsežnost inducirane upodobitve $\rho$ grupe $H$ na prostoru $V$ enaka

$$\deg(\mathrm{Ind}_H^G(\rho)) = |G : \mathrm{im}\,\phi| \cdot \dim(V^{\ker\phi}).$$

## Adjunkcija restrikcije in indukcije

Indukcija in restrikcija vsekakor nista inverzna funktorja. Na primer, če je $H \leq G$ in $\phi$ vložitev, potem za upodobitev $\rho$ v $\mathrm{Rep}_G$ velja $\deg(\mathrm{Res}_H^G(\rho)) = \deg(\rho)$ in zato $\deg(\mathrm{Ind}_H^G(\mathrm{Res}_H^G(\rho))) = |G:H| \cdot \deg(\rho)$, kar je lahko mnogo večje od $\deg(\rho)$. Sta pa funktorja restrikcije in indukcije vendarle tesno povezana. Tvorita namreč **adjungiran par** funktorjev.[22]

**Trditev 1.2.24.** *Naj bosta $G,H$ grupi s homomorfizmom $\phi\colon H \to G$. Za vsako upodobitev $\rho$ v $\mathrm{Rep}_G$ in upodobitev $\sigma$ v $\mathrm{Rep}_H$ velja*

$$\hom_H(\mathrm{Res}_H^G(\rho), \sigma) \cong \hom_G(\rho, \mathrm{Ind}_H^G(\sigma)).$$

*Dokaz.* Naj bo $\rho$ upodobitev na prostoru $V$ in $\sigma$ upodobitev na prostoru $W$. Naj bo

$$\Phi \in \hom_H(\mathrm{Res}_H^G(\rho), \sigma) = \hom_H(V, W).$$

Sestavimo pripadajočo spletično

$$\Psi \in \hom_G(\rho, \mathrm{Ind}_H^G(\sigma)) = \hom_G(V, \mathrm{fun}(G,W)^H).$$

Za vektor $v \in V$ definirajmo

$$\Psi(v) = (x \mapsto \Phi(\rho(x) \cdot v)) \in \mathrm{fun}(G,W).$$

**Domača naloga 1.2.25.** Preveri, da prirejanje $\Phi \mapsto \Psi$ vzpostavi izomorfizem med prostoroma spletičen $\hom_H(V,W)$ in $\hom_G(V, \mathrm{fun}(G,W)^H)$.

[22] V nadaljevanju bomo spoznali presenetljivo uporabnost tega navidez naključnega dejstva.

□

**Zgled 1.2.26.** Naj bo $G$ grupa s podgrupo $H$ končnega indeksa. Grupa $G$ deluje na množici desnih odsekov $H\backslash G$ s homomorfizmom

$$G \to \mathrm{Sym}(H\backslash G), \quad g \mapsto \left(Hx \mapsto Hxg^{-1}\right).$$

Iz tega delovanja izhaja permutacijska upodobitev $\pi$ grupe $G$ na prostoru $F[H\backslash G]$. Po konstrukciji je $\pi \cong \mathrm{Ind}_H^G(\mathbf{1})$. Iz adjunkcije med restrikcijo in indukcijo za trivialni upodobitvi grup $G$ in $H$ od tod izpeljemo izomorfizem

$$\hom_H(\mathbf{1},\mathbf{1}) \cong \hom_G(\mathbf{1},\pi) \cong F[H\backslash G]^G.$$

Prostor $\hom_H(\mathbf{1},\mathbf{1}) = \hom(F,F)$ sestoji zgolj iz skalarnih množenj in je torej enorazsežen. Zato je enorazsežen tudi prostor invariant $F[H\backslash G]^G$. Vektor, ki ga razpenja, lahko dobimo kot sliko $\mathrm{id}_F \in \hom_H(\mathbf{1},\mathbf{1})$. Tej spletični po adjunkciji ustreza spletična

$$\Psi: F \to F[H\backslash G], \quad 1 \mapsto \sum_{Hx \in H\backslash G} e_{Hx},$$

od koder sledi

$$F[H\backslash G]^G = \left\langle \sum_{Hx \in H\backslash G} e_{Hx} \right\rangle.$$

**Domača naloga 1.2.27.** Naj bosta $G,H$ grupi s homomorfizmom $\phi: H \to G$. Za vsako upodobitev $\rho$ v $\mathrm{Rep}_G$ in upodobitev $\sigma$ v $\mathrm{Rep}_H$ velja

$$\mathrm{Ind}_H^G(\mathrm{Res}_H^G(\rho) \otimes \sigma) \cong \rho \otimes \mathrm{Ind}_H^G(\sigma).$$

**Domača naloga 1.2.28.** Premisli, kako se restrikcija in indukcija ujameta z dualom, direktno vsoto in tenzorskim produktom.

# Poglavje 2

# Upodobitev pod mikroskopom

V tem poglavju bomo pribili upodobitev dane grupe in se ji tesno približali, kot da bi jo pogledali pod mikroskopom. Pri tem bomo najprej uzrli osnovne kose, iz katerih je sestavljena upodobitev. Ti osnovni kosi ustrezajo celicam, ki jih vidimo pod mikroskopom. Za tem se bomo približali še sestavi teh osnovnih kosov: vsak je dan s homomorfizmom v matrike, zato bomo raziskali koeficiente te matrike. Ti ustrezajo organelom, ki jih v celici vidimo pod mikroskopom. Nazadnje bomo premislili, da so te upodobitvene celice dovolj diferencirane med seboj, da za njihovo identifikacijo zadošča poznavanje le nekaterih njihovih organelov.

## 2.1 Razstavljanje upodobitve

Pogosto nas zanima, ali lahko dano upodobitev $\rho$ grupe $G$ na prostoru $V$ zapišemo kot direktno vsoto nekih podupodobitev in na ta način upodobitev $\rho$ *razstavimo* na preprostejše upodobitve, podobno kot razstavimo števila na manjše faktorje.

### Nerazcepnost

Naj bo $G$ grupa z upodobitvijo $\rho$ na prostoru $V \neq 0$. Kadar *ne* obstaja noben $G$-invarianten podprostor prostora $V$ (razen prostorov 0 in $V$), tedaj rečemo, da je upodobitev $\rho$ **nerazcepna**.[1] V tem primeru upodobitve seveda ne moremo razstaviti na enostavnejše v smislu direktne vsote.

**Zgled 2.1.1.**

- Opazujmo permutacijsko upodobitev simetrične grupe $S_3$ na prostoru $\mathbf{R}[\{1,2,3\}] = \mathbf{R}^3$. Premislili smo že, da je ta upodobitev direktna vsota enorazsežne podupodobitve $\mathbf{1}$ in dvorazsežne podupodobitve $\rho$, pri čemer slednja nima nobene enorazsežne podupodobitve. S tem je permutacijska upodobitev razstavljena kot direktna vsota dveh nerazcepnih upodobitev.

- Opazujmo diedrsko grupo $D_{2n}$ z dvorazsežno upodobitvijo $\rho_k$ za $k \in \mathbf{Z}$, ki jo obravnavajmo kot kompleksno upodobitev. Matrika $\rho_k(r)$ ima lastni vrednosti $e^{\pm 2\pi i k/n}$. Ti dve vrednosti sta različni, če in samo če $k$ *ni* deljiv z $n/2$. Za vsak $0 < k < n/2$ ima $\rho_k(r)$ torej različni lastni vrednosti z lastnima vektorjema $\binom{1}{\mp i}$. Matrika $\rho_k(s)$ zamenja ta dva lastna podprostora med seboj. Upodobitev $\rho_k$ za $0 < k < n/2$ torej nima nobene enorazsežne kompleksne podupodobitve in je zato nerazcepna.

Preverimo, da so nerazcepne upodobitve dane grupe med seboj *neprimerljive*, tudi če so enake razsežnosti. Zatorej si jih lahko predstavljamo kot neodvisne osnovne kose kategorije upodobitev dane grupe.[2]

[1] Rečemo tudi, da je $V$ **enostavna** upodobitev. Ta terminologija izhaja iz alternativne obravnave upodobitev kot *modulov nad grupnimi algebrami*.

[2] Po analogiji s faktorizacijo števil si nerazcepne upodobitve lahko predstavljamo kot praštevila.

**Lema 2.1.2** (Schurova lema)**.** *Naj bo $G$ grupa z upodobitvijo $\rho$ in nerazcepno upodobitvijo $\pi$. Tedaj je vsaka spletična $v$ $\hom_G(\pi,\rho)$ bodisi injektivna bodisi ničelna in vsaka spletična $v$ $\hom_G(\rho,\pi)$ je bodisi surjektivna bodisi ničelna. V posebnem je vsaka spletična med dvema nerazcepnima upodobitvama grupe $G$ bodisi izomorfizem bodisi ničelna.*

*Dokaz.* Naj bo $\Phi \in \hom_G(\pi,\rho)$. Tedaj je $\ker\Phi$ podupodobitev $\pi$, zato je po nerazcepnosti bodisi $\ker\Phi = 0$ bodisi $\Phi = 0$. Prvi primer ustreza možnosti, da je $\Phi$ injektivna, v drugem primeru pa je $\Phi$ ničelna. Soroden razmislek dokaže trditev o spletičnah v $\hom_G(\rho,\pi)$. □

Nad algebraično zaprtimi polji lahko to neprimerljivost raztegnemo do ene same upodobitve: osnovni kosi nimajo netrivialnih simetrij.

**Posledica 2.1.3.** *Naj bo $G$ grupa z nerazcepno upodobitvijo $\pi$ končne razsežnosti nad* algebraično zaprtim poljem*. Tedaj je* $\dim\hom_G(\pi,\pi) = 1$*. Povedano še drugače: množica* $\hom_G(\pi,\pi)$ *sestoji le iz skalarnih večkratnikov identitete.*

*Dokaz.* Naj bo $0 \neq \Phi \in \hom_G(\pi,\pi)$. Ker je polje algebraično zaprto, ima linearna preslikava $\Phi$ vsaj kakšno lastno vrednost, recimo $\lambda$. Preslikava $\Phi - \lambda\cdot\mathrm{id} \in \hom_G(\pi,\pi)$ zato ni injektivna, s čimer mora biti po Schurovi lemi ničelna, se pravi $\Phi = \lambda\cdot\mathrm{id}$. □

Množico vseh izomorfnostnih razredov nerazcepnih upodobitev dane grupe $G$ označimo z $\mathrm{Irr}(G)$.

**Zgled 2.1.4.** Naj bo $G$ grupa z nerazcepno upodobitvijo $\pi$ končne razsežnosti nad poljem kompleksnih števil. Spletične $\hom_G(\pi,\pi) = \hom(\pi,\pi)^G$ so endomorfizmi vektorskega prostora, ki so $G$-invariantni, se pravi komutirajo z delovanjem grupe $G$. Zglede takih endomorfizmov lahko dobimo iz delovanj centralnih elementov grupe $G$; za vsak $z \in Z(G)$ je $\pi(z) \in \hom_G(\pi,\pi)$. Po Schurovi lemi je zato $\pi(z) = \omega(z)\cdot\mathrm{id}$ za nek skalar $\omega(z)$. Ker je $\pi$ homomorfizem, je $\omega\colon Z(G) \to \mathbf{C}^*$ enorazsežna upodobitev centra grupe $G$. Tej upodobitvi rečemo **centralni karakter** upodobitve $\pi$.

Še posebej zanimiv je primer, ko je $G$ *abelova* grupa. Takrat za vsako nerazcepno upodobitev $\pi$ končne razsežnosti nad poljem $\mathbf{C}$ velja $\pi(g) = \omega(g)\cdot\mathrm{id}$ za *vsak* $g \in G$. Vsak enorazsežen podprostor je zato avtomatično podupodobitev. Ker je $\pi$ nerazcepna, od tod sklepamo $\deg(\pi) = 1$ in s tem $\pi = \omega$. Upodobitev $\pi$ je tako *enorazsežna*. Na primer, vsaka končno razsežna nerazcepna kompleksna upodobitev grupe $\mathbf{R}$ je nujno enorazsežna.

**Domača naloga 2.1.5.** Poišči kakšno nerazcepno upodobitev ciklične grupe $\mathbf{Z}/3\mathbf{Z}$ nad poljem $\mathbf{Q}$, ki *ni* enorazsežna.

## Komplementarna podupodobitev

Predpostavimo zdaj, da ima dana upodobitev $\rho$ grupe $G$ na prostoru $V$ neko podupodobitev $\tilde\rho$ na podprostoru $W \leq V$. Seveda lahko vselej najdemo vektorski prostor $U \leq V$, za katerega je $V = U \oplus W$, vsekakor pa ni jasno, če lahko najdemo tak podprostor $U$, ki je celo $G$-invarianten. Kadar je temu tako, rečemo, da smo našli **komplementarno podupodobitev** podupodobitve $\tilde\rho$.[3] Ni vsaka podupodobitev komplementirana.

**Zgled 2.1.6.** Naj grupa $\mathbf{R}$ deluje na realnem prostoru $\mathbf{R}^2$ s homomorfizmom

$$\rho\colon \mathbf{R} \to \mathrm{GL}_2(\mathbf{R}), \quad x \mapsto \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}.$$

Oglejmo si enorazsežne podupodobitve. Premislili smo že, da te ustrezajo skupnim lastnim vektorjem vseh preslikav $\rho(x)$ za $x \in \mathbf{R}$. Pri $x = 1$ imamo linearno preslikavo $\rho(1)$ z enim samim lastnim vektorjem,

[3] Če komplementarna podupodobitev obstaja, potem je enolično določena (do izomorfizma upodobitev), saj je izomorfna kvocientu $\rho/\tilde\rho$.

in sicer $e_1 \in \mathbf{R}^2$. Hkrati je $e_1$ lastni vektor vseh preslikav $\rho(x)$ za $x \in \mathbf{R}$. Torej ima $\rho$ *eno samo* enorazsežno podupodobitev, in sicer je to $\mathbf{R} \cdot e_1 \leq \mathbf{R}^2$. Ta vektorski podprostor ima mnogo komplementov v $\mathbf{R}^2$, noben od teh pa ni hkrati enorazsežna podupodobitev $\rho$.

Ni težko preveriti, da obstoj komplementarne podupodobitve vselej izhaja iz **projekcijskih spletičen**.[4]

**Trditev 2.1.7.** *Naj bo $G$ grupa z upodobitvijo $\rho$ na prostoru $V$ in naj bo $\tilde{\rho}$ njena podupodobitev na prostoru $W \leq V$. Tedaj ima $\tilde{\rho}$ komplementarno podupodobitev, če in samo če obstaja spletična $\Phi \in \hom_G(V,V)$, ki je projekcija na $W$. V tem primeru je* $\ker\Phi$ *komplementarna upodobitev.*

## Polenostavnost

Vrnimo se k začetni ideji o *razstavljanju* dane upodobitve. Kadar lahko dano upodobitev $\rho$ zapišemo kot direktno vsoto *nerazcepnih* upodobitev $\bigoplus_{i\in I} \rho_i$, tedaj rečemo, da je $\rho$ **polenostavna** upodobitev. Če so pri tem vse podupodobitve $\rho_i$ izomorfne med seboj, upodobitev $\rho$ imenujemo **izotipična** upodobitev.

**Zgled 2.1.8.**

- Permutacijska upodobitev grupe $S_3$ na $\mathbf{R}^3$ je polenostavna.
- Regularna upodobitev ciklične grupe $\mathbf{Z}/n\mathbf{Z}$ nad $\mathbf{C}$ je polenostavna.

Vseh upodobitev žal ne moremo razstaviti na direktno vsoto nerazcepnih.[5] Polenostavnost dane upodobitve je namreč tesno povezana z obstojem komplementarnih podupodobitev.

**Trditev 2.1.9.** *Upodobitev grupe $G$ je polenostavna, če in samo če ima vsaka njena podupodobitev komplementarno podupodobitev.*

*Dokaz.* ($\Rightarrow$): Naj bo najprej $\rho{:}G \to \mathrm{GL}(V)$ polenostavna upodobitev, pri kateri je $V = \bigoplus_{i\in I} V_i$ in upodobitve $G$ na podprostorih $V_i$ so nerazcepne. Naj bo $W \leq V$ poljuben $G$-invarianten podprostor. Po Zornovi lemi obstaja maksimalen $G$-invarianten podprostor $U \leq V$ z lastnostjo $U \cap W = 0$. Izberimo poljuben $i \in I$. Presek $(U \oplus W) \cap V_i$ je $G$-invarianten podprostor prostora $V_i$, zato je po nerazcepnosti bodisi trivialen bodisi enak $V_i$. Če bi bil trivialen, bi lahko $U$ povečali do prostora $U \oplus V_i$, kar je v nasprotju z maksimalnostjo izbire $U$. Zatorej je $(U \oplus W) \cap V_i = V_i$ in tako $(U \oplus W) \geq V_i$. Ker je bil $i$ poljuben, od tod sledi $U \oplus W = V$. Podupodobitev $W$ ima torej komplementarno podupodobitev $U$. ✓

($\Leftarrow$): Naj bo $\rho{:}G \to \mathrm{GL}(V)$ upodobitev, v kateri je vsaka podupodobitev komplementirana. Dokazati želimo, da je $\rho$ polenostavna. Uporabili bomo naslednjo pomožno trditev, ki je ni težko preveriti.

**Domača naloga 2.1.10.** Naj bo $\rho$ upodobitev, v kateri je vsaka podupodobitev komplementirana. Tedaj ima $\rho$ nerazcepno podupodobitev.

Naj bo $W$ vsota vseh $G$-invariantnih podprostorov v $V$, ki so nerazcepne upodobitve, se pravi $W = \sum_{i\in I} V_i$, a ta vsota ni nujno direktna. Po pomožni trditvi je $W \neq 0$. Po predpostavki je $W$ komplementirana z $G$-invariantnim podprostorom $U$. Po pomožni trditvi ima tudi $U$ nerazcepno podupodobitev, zato je ta vsebovana v $W$, kar implicira $W = V$. Dokažimo zdaj še, da je $W$ *direktna* vsota podprostorov $V_i$. V ta namen naj bo $J$ maksimalna podmnožica indeksne množice $I$, za katero je $\sum_{j\in J} V_j$ direktna vsota. Taka podmnožica obstaja po Zornovi lemi. Označimo $\tilde{V} = \bigoplus_{j\in J} V_j$. Če velja $\tilde{V} \neq V$, potem mora za nek $i \in I\backslash J$ po nerazcepnosti veljati $V_i \cap \tilde{V} = 0$, kar pa je v nasprotju z maksimalnostjo množice $J$. Tako je res $\tilde{V} = V$ in upodobitev $V$ je polenostavna. ✓ □

[4] Linearna preslikava $A{:}X \to X$ je projekcija na podprostor $Y \leq X$, če je $A^2 = A$ in $\mathrm{im}\, A = Y$. Projekcijska spletična je torej spletična, ki je hkrati projekcija na nek podprostor.

[5] V nadaljevanju bomo pokazali, da so upodobitve *končnih* grup nad poljem karakteristike 0 vselej polenostavne.

**Zgled 2.1.11.** Eničnozgornjetrikotna upodobitev grupe $\mathbf{R}$ na $\mathbf{R}^2$ *ni* nerazcepna, hkrati pa njena podupodobitev $\mathbf{R}\cdot e_1 \cong \mathbf{1}$ *ni* komplementirana. Ta upodobitev zatorej *ni* polenostavna.

Z uporabo zadnjega kriterija lahko dokažemo, da je polenostavnost zaprta za osnovne konstrukcije z upodobitvami.

**Posledica 2.1.12.** *Podupodobitve, kvocienti in direktne vsote polenostavnih upodobitev dane grupe so polenostavne.*

*Dokaz.* Preverimo le zaprtost za podupodobitve. Naj bo $\rho$ polenostavna upodobitev grupe $G$ na prostoru $V$ in naj bo $W \leq V$ podupodobitev. Naj bo $U \leq W$ poljubna podupodobitev upodobitve na $W$. Po polenostavnosti obstaja komplementarna podupodobitev $\tilde{U} \leq V$ upodobitve $U \leq V$. Tedaj je $\tilde{U} \cap W$ podupodobitev, ki je komplementirana podupodobitvi $U$ v $W$. □

Nazadnje lahko s pomočjo projekcijskih spletičen naredimo še en korak naprej pri razumevanju simetrij upodobitev. Premislili smo že, da so osnovni kosi brez netrivialnih simetrij. V primeru polenostavnih upodobitev drži tudi obratno.

**Posledica 2.1.13.** *Naj bo $G$ grupa s* polenostavno *upodobitvijo $\rho$ končne razsežnosti. Če je* $\dim \hom_G(\rho,\rho) = 1$*, potem je $\rho$ nerazcepna.*

*Dokaz.* Naj $\rho$ upodablja grupo $G$ na prostoru $V$. Naj bo $W \leq V$ nerazcepna podupodobitev in naj bo $U$ njena komplementarna podupodobitev. Naj bo $\Phi\colon V \to V$ pripadajoča projekcija na podprostor $W$ z jedrom $U$. Ker je $\Phi \in \hom_G(\rho,\rho)$, iz predpostavke sledi, da je $\Phi$ skalarni večkratnik identitete. To je mogoče le v primeru, ko je $V = W$ in $U = 0$, torej je $\rho$ nerazcepna. □

## Kompozicijska vrsta

Vsake upodobitve ne moremo razstaviti kot direktno vsoto nerazcepnih upodobitev. Kljub temu pa je res, da lahko vsako upodobitev (na končno razsežnem prostoru) razstavimo na nerazcepne upodobitve, le da moramo pri tem poseči po nekoliko zahtevnejšem načinu razstavljanja.

Naj bo $G$ grupa z upodobitvijo na prostoru $V$. Predpostavimo, da obstaja zaporedje $G$-invariantnih podprostorov

$$0 = V_0 \leq V_1 \leq V_2 \leq \cdots \leq V_n = V,$$

pri čemer so vsi zaporedni kvocienti $V_i/V_{i-1}$ za $1 \leq i \leq n$, gledani kot upodobitve grupe $G$, *nerazcepni*. Tako zaporedje imenujemo **kompozicijska vrsta** upodobitve na prostoru $V$. Kvocienti $V_i/V_{i-1}$ se pri tem imenujejo **kompozicijski faktorji**.

**Zgled 2.1.14.** Naj bo $\rho$ eničnozgornjetrikotna upodobitev grupe $\mathbf{R}$ na $V = \mathbf{R}^2$. Ta upodobitev ima podupodobitev $V_1 = \mathbf{R}\cdot e_1$. Kvocient $V/V_1$ je enorazsežen in na njem grupa $\mathbf{R}$ deluje trivialno. Dobimo torej kompozicijsko vrsto

$$0 = V_0 \leq V_1 \leq V,$$

katere kompozicijska faktorja sta kot upodobitvi izomorfna $\mathbf{1}$. Sama upodobitev grupe $\mathbf{R}$ na $V$ pa seveda ni trivialna.

**Izrek 2.1.15** (Jordan-Hölder-Noether)**.** *Vsaka upodobitev na končno razsežnem prostoru ima kompozicijsko vrsto. Vsaki dve kompozicijski vrsti imata enako število členov in do permutacije ter izomorfizma natančno enake kompozicijske faktorje.*

*Dokaz.* Naj grupa deluje linearno na končno razsežnem prostoru $V$. Da kompozicijska vrsta res obstaja, ni težko preveriti. Najprej izberemo neko nerazcepno podupodobitev $V_1$. Če je $V_1 < V$, potem izberemo podupodobitev $V_2$, ki vsebuje $V_1$ in je med vsemi takimi minimalne razsežnosti. S tem je $V_2/V_1$ nerazcepna. Induktivno nadaljujemo z grajenjem kompozicijske vrste. Ker je $V$ končno razsežen, se ta postopek ustavi.

Premislimo še, kako lahko vsaki dve kompozicijski vrsti povežemo med seboj. Opazujmo dve taki vrsti,

$$0 = V_0 \leq V_1 \leq \cdots \leq V_n = V \quad \text{in} \quad 0 = W_0 \leq W_1 \leq \cdots \leq W_m = V.$$

S pomočjo druge vrste bomo skušali najti *finejšo* vrsto, ki je bliže prvi, ter obratno.[6] Za $0 \leq i < n$ in $0 \leq j \leq m$ naj bo

$$V_{i,j} = V_i + (V_{i+1} \cap W_j),$$

S tem dobimo verigo

$$V_i = V_{i,0} \leq V_{i,1} \leq \cdots \leq V_{i,m} = V_{i+1}$$

med $V_i$ in $V_{i+1}$. Ker je kvocient $V_{i+1}/V_i$ nerazcepen in je vsak $V_{i,j}$ podupodobitev, mora za natanko en indeks $j$ veljati $V_i = V_{i,j}$ in $V_{i+1} = V_{i,j+1}$. Kompozicijski faktor $V_{i+1}/V_i$ je tedaj izomorfen kvocientu

$$\frac{V_i + (V_{i+1} \cap W_{j+1})}{V_i + (V_{i+1} \cap W_j)}.$$

Zgodbo zdaj ponovimo še za drugo verigo. S pomočjo prve poiščimo finejšo. Definiramo $W_{j,i} = W_j + (W_{j+1} \cap V_i)$. Kvocient $W_{j+1}/W_j$ je enak

$$\frac{W_j + (W_{j+1} \cap V_{i+1})}{W_j + (W_{j+1} \cap V_i)}.$$

**Domača naloga 2.1.16.** Prepričaj se, da velja

$$\frac{V_i + (V_{i+1} \cap W_{j+1})}{V_i + (V_{i+1} \cap W_j)} \cong \frac{W_j + (W_{j+1} \cap V_{i+1})}{W_j + (W_{j+1} \cap V_i)}.$$

S tem smo za vsak $0 \leq i < n$ našli natanko določen $j$, da je $V_{i+1}/V_i \cong W_{j+1}/W_j$. Premislimo še, da je to prirejanje injektivno. Indeks $j$ je enolično določen s pogojem, da je $V_{i,j+1}/V_{i,j} \neq 0$, kar je po gornjem izomorfizmu enakovredno pogoju $W_{j,i+1}/W_{j,i} \neq 0$. Ker je $W_{j+1}/W_j$ nerazcepen, je slednji pogoj lahko izpolnjen le za *en* indeks $i$. □

Iz izreka sledi, da lahko za vsako upodobitev $\rho$ grupe $G$ na končno razsežnem prostoru najdemo bazo prostora, v kateri imajo vse matrike $\rho(g)$ za $g \in G$ *bločno zgornjetrikotno* obliko (pri čemer je število blokov enako dolžini kompozicijske vrste). Po drugi strani lahko za *polenostavno* upodobitev najdemo bazo prostora, v kateri imajo vse matrike *bločno diagonalno* obliko.

## Izotipične komponente

Po zadnjem izreku je za dano upodobitev $\rho$ na končno razsežnem prostoru in nerazcepno upodobitev $\pi$ število kompozicijskih faktorjev, ki so izomorfni $\pi$, neodvisno od kompozicijske vrste. Temu številu pravimo **večkratnost** $\pi$ v $\rho$ in ga označimo z $\mathrm{mult}_\rho(\pi)$.

Kadar je dana upodobitev *polenostavna*, je do izomorfizma natančno enolično določena s svojimi večkratnostmi. Če je $\rho = \bigoplus_{i \in I} \rho_i$, potem je

$$\hom_G(\pi, \rho) = \bigoplus_{i \in I} \hom_G(\pi, \rho_i).$$

Po Schurovi lemi je (nad algebraično zaprtim poljem) vsak od zadnjih prostorov spletičen bodisi trivialen bodisi enorazsežen. Večkratnost $\pi$ v $\rho$ lahko zatorej izračunamo kot

$$\mathrm{mult}_\rho(\pi) = \dim \hom_G(\pi, \rho).$$

[6] Ta argument je soroden premisleku o obstoju Hirschove dolžine v policikličnih grupah iz Teorije grup.

**Zgled 2.1.17.**

- Za eničnozgornjetrikotno upodobitev $\rho$ grupe $\mathbf{R}$ na $\mathbf{R}^2$ je $\mathrm{mult}_\rho(\mathbf{1}) = 2$. Ker ta upodobitev ni trivialna, ne more biti polenostavna, saj bi sicer bila izomorfna $\mathbf{1}^2$.
- Opazujmo permutacijsko upodobitev $\pi$ grupe $S_3$ na $\mathbf{R}^3$. To upodobitev smo že razstavili na direktno vsoto $\mathbf{1} \oplus \rho$, kjer je $\rho$ dvorazsežna nerazcepna upodobitev na podprostoru $\langle u_1 = e_1 - e_2, u_2 = e_2 - e_3 \rangle$. Premislili smo, kako lahko to upodobitev projiciramo do upodobitve $\tilde{\rho}$ grupe $S_3$ na prostoru $(\mathbf{Z}/3\mathbf{Z})^2$ nad končnim poljem $\mathbf{Z}/3\mathbf{Z}$.

  Upodobitev $\tilde{\rho}$ *ni* nerazcepna, saj ima invarianten podprostor $\langle u_1 - u_2 = e_1 + e_2 + e_3 \rangle$. Na tem podprostoru grupa $S_3$ deluje trivialno. V kvocientu $(\mathbf{Z}/3\mathbf{Z})^2/\langle u_1 - u_2 \rangle \cong \mathbf{Z}/3\mathbf{Z}$ generatorja $(1\ 2)$ in $(1\ 2\ 3)$ grupe $S_3$ preslikata odsek vektorja $u_1$ v odsek $-u_1$ oziroma $u_1$. V tem prepoznamo predznačno upodobitev, interpretirano kot homomorfizem $\mathrm{sgn}: S_3 \to \mathrm{GL}_1(\mathbf{Z}/3\mathbf{Z}) \cong \{1, -1\}$. Nad poljem $\mathbf{Z}/3\mathbf{Z}$ za permutacijsko upodobitev $\pi$ tako velja $\mathrm{mult}_\pi(\mathbf{1}) = 2$ in $\mathrm{mult}_\pi(\mathrm{sgn}) = 1$.

  Premislimo, da upodobitev $\pi$ nad $\mathbf{Z}/3\mathbf{Z}$ *ni* polenostavna. Če bi namreč bila, bi po zgornjem morala biti izomorfna direktni vsoti $\mathbf{1} \oplus \mathbf{1} \oplus \mathrm{sgn}$. Prostor $(\mathbf{Z}/3\mathbf{Z})^3$ bi zatorej imel bazo, v kateri bi matriki za $\pi((1\ 2))$ in $\pi((1\ 2\ 3))$ bili hkrati diagonalni. Ti dve matriki bi zato komutirali, kar pomeni, da bi morali komutirati tudi linearni preslikavi $\pi((1\ 2))$ in $\pi((1\ 2\ 3))$. Vendar pa to ne drži, saj na primer velja $\pi((1\ 2\ 3)(1\ 2))e_1 = e_3$ in $\pi((1\ 2)(1\ 2\ 3))e_1 = e_1$.

Čeravno so kompozicijski faktorji upodobitve enolično določeni do permutacije natančno, pa *ni* res, da so enolično določeni tudi členi kompozicijske vrste, niti kadar je dana upodobitev polenostavna. Lahko se namreč zgodi, da neka nerazcepna podupodobitev nastopa z večkratnostjo vsaj 2.[7]

Oglejmo si tako situacijo še podrobneje. Naj bo $G$ grupa z upodobitvijo $\rho$ na prostoru $V$. Naj bo $\pi$ neka *nerazcepna* upodobitev grupe $G$. Opazujmo vse $G$-invariantne (glede na upodobitev $\rho$) podprostore v $V$, ki so kot upodobitve izomorfni $\pi$. Vsota (ne nujno direktna) vseh teh podprostorov

$$\mathrm{Izotip}_\rho(\pi) = \textstyle\sum_{W \le V,\ W \cong \pi} W$$

je **$\pi$-izotipična komponenta** upodobitve $\rho$. Ta je sicer definirana za vsako upodobitev, a jo je za polenostavne upodobitve še posebej lahko določiti.

**Trditev 2.1.18.** *Naj bo $G$ grupa s polenostavno upodobitvijo $\rho = \bigoplus_{i \in I} \rho_i$ na prostoru $V = \bigoplus_{i \in I} V_i$, kjer je vsak $\rho_i$ nerazcepna podupodobitev. Za vsako nerazcepno upodobitev $\pi$ grupe $G$ je*

$$\mathrm{Izotip}_\rho(\pi) = \textstyle\bigoplus_{i \in I:\ \rho_i \cong \pi} V_i.$$

*Dokaz.* Naj bo $W$ direktna vsota podprostorov $V_i$, ki so kot upodobitev izomorfni $\pi$. Seveda je $W \le \mathrm{Izotip}_\rho(\pi)$. Dokažimo, da velja tudi obratna neenakost. Naj bo $U$ direktna vsota tistih prostorov $V_i$, ki kot upodobitev *niso* izomorfni $\pi$. Velja $V = W \oplus U$. Opazujmo projekcijo $p: V \to U$ z jedrom $W$. Naj bo $Z \le \mathrm{Izotip}_\rho(\pi)$ podprostor, ki je kot upodobitev izomorfen $\pi$. Zožitev $p|_Z$ je spletična v $\hom_G(Z, U)$, ki je po Schurovi lemi ničeln prostor. Torej je $p(Z) = 0$ in s tem $Z \le W$. Ker je bil $Z$ poljuben, smo s tem dokazali $\mathrm{Izotip}_\rho(\pi) \le W$. □

Naj bo $G$ grupa z upodobitvijo $\rho$ na prostoru $V$ in nerazcepno upodobitvijo $\pi$ na prostoru $W$. Vsak $G$-invarianten (glede na upodobitev $\rho$) podprostor v $V$, ki je kot upodobitev izomorfen $\pi$, lahko dobimo kot sliko prostora $W$ z neko spletično v $\hom_G(\pi, \rho)$.[8] Vsoto vseh takih $G$-invariantnih podprostorov lahko torej zajamemo kot sliko linearne preslikave

$$\Sigma_{\pi,\rho}: \hom_G(\pi, \rho) \otimes W \to V, \quad \Phi \otimes w \mapsto \Phi(w).$$

S tem je $\mathrm{im}\,\Sigma_{\pi,\rho} = \mathrm{Izotip}_\rho(\pi)$. Grupa $G$ deluje na $\hom_G(\pi, \rho) = \hom(W, V)^G$ trivialno, na $W$ pa prek $\pi$. Na ta način je $\Sigma_{\pi,\rho}$ celo spletična upodobitev.

[7] Na primer, kadar je upodobitev trivialna, se pravi $V = \mathbf{1}^k$ za nek $k > 1$, lahko izberemo poljubno bazo prostora $V$ in prek nje dobimo nek drug izomorfizem $V \cong \mathbf{1}^k$.

[8] Vsaka neničelna spletična v $\hom_G(\pi, \rho)$ je namreč injektivna.

**Trditev 2.1.19.** *Naj bo $G$ grupa z upodobitvijo $\rho$ in nerazcepno upodobitvijo $\pi$ nad algebraično zaprtim poljem. Predpostavimo, da je* $\dim \hom_G(\pi,\rho) < \infty$. *Tedaj je $\Sigma_{\pi,\rho}$ injektivna.*

*Dokaz.* Naj bo $\{\Phi_i\}_{i\in I}$ baza prostora $\hom_G(\pi,\rho)$. Premislimo, da prostori $\operatorname{im}\Phi_i$ tvorijo notranjo direktno vsoto v $V$. Injektivnost $\Sigma_{\pi,\rho}$ od tod neposredno sledi.

Dokazujemo s protislovjem. Naj bo $J \subseteq I$ množica najmanjše moči, za katero prostori $\operatorname{im}\Phi_j$ za $j \in J$ *ne* tvorijo direktne vsote. Obstaja torej $k \in J$, da je

$$\operatorname{im}\Phi_k \cap \sum_{j\in J\setminus\{k\}} \operatorname{im}\Phi_j \neq 0.$$

Po nerazcepnosti $\pi$ je spletična $\Phi_k$ injektivna, zato je $\operatorname{im}\Phi_k$ nujno vsebovana v vsoti $\sum_{j\in J\setminus\{k\}} \operatorname{im}\Phi_j$. Po minimalnosti $J$ je zadnja vsota direktna, zato je

$$\Phi_k \in \hom_G(W, \bigoplus_{j\in J\setminus\{k\}} \operatorname{im}\Phi_j).$$

Slednji prostor je direktna vsota prostorov $\hom_G(W, \operatorname{im}\Phi_j)$. Po Schurovi lemi je vsak od teh enorazsežen, zato je $\hom_G(W, \operatorname{im}\Phi_j)$ generiran s spletično $\Phi_j$. Od tod sledi, da je $\Phi_k$ linearna kombinacija spletičen $\Phi_j$ za $j \in J\setminus\{k\}$. To je protislovno z dejstvom, da je $\{\Phi_i\}_{i\in I}$ baza prostora $\hom_G(\pi,\rho)$. □

**Posledica 2.1.20.** *Naj bo $G$ grupa z upodobitvijo $\rho$ in nerazcepno upodobitvijo $\pi$ nad algebraično zaprtim poljem. Predpostavimo, da je* $\hom_G(\pi,\rho) < \infty$. *Izotipična komponenta* $\operatorname{Izotip}_\rho(\pi)$ *je polenostavna, $\pi$-izotipična in vsebuje $\pi$ z večkratnostjo* $\dim \hom_G(\pi,\rho)$.

*Dokaz.* Iz injektivnosti $\Sigma_{\pi,\rho}$ sledi $\operatorname{Izotip}_\rho(\pi) \cong \hom_G(\pi,\rho) \otimes W$. Ker grupa $G$ deluje trivialno na $\hom_G(\pi,\rho)$, je prostor $\hom_G(\pi,\rho) \otimes W$ kot upodobitev izomorfen direktni vsoti $\dim \hom_G(\pi,\rho)$ kopij prostora $W$, na katerem $G$ deluje s $\pi$. □

**Domača naloga 2.1.21.** Naj bo $G$ grupa s končno razsežno upodobitvijo $\rho$ na prostoru $V$ nad algebraično zaprtim poljem. Premisli, da se izotipične komponente, ki pripadajo paroma neizomorfnim nerazcepnim upodobitvam, sekajo trivialno.

**Zgled 2.1.22.**

- Naj bo $G$ grupa s polenostavno upodobitvijo $\rho = \bigoplus_{i\in I} \rho_i$ na prostoru $V = \bigoplus_{i\in I} V_i$, v kateri vsaka nerazcepna podupodobitev nastopa z večkratnostjo 1. Upodobitve $\rho_i$ so torej paroma neizomorfne. Izotipične komponente so torej kar enake podprostorom $V_i$. Ker so te komponente neodvisne od izbire dekompozicije, so torej podprostori $V_i$ polenostavne dekompozicije enolično določeni.

  Naj bo $W \leq V$ nek $G$-invarianten podprostor. Upodobitev $G$ na tem podprostoru je tudi polenostavna. Vsaka njena nerazcepna podupodobitev je hkrati podupodobitev $\rho$, zato po enoličnosti podprostorov $V_i$ sestoji iz nekaterih teh podprostorov. Prostor $W$ je zato enak $\bigoplus_{i\in J} V_i$ za neko podmnožico $J \subseteq I$.

  Za konkreten zgled lahko vzamemo ciklično grupo $\mathbf{Z}/n\mathbf{Z}$ in njeno regularno upodobitev, ki smo jo razcepili na direktno vsoto upodobitev $\bigoplus_{j\in\{1,2,\ldots,n\}} \chi_j$. Po zadnjem komentarju je vsaka podupodobitev regularne upodobitve torej enaka direktni vsoti nekaterih od upodobitev $\chi_j$.

- Naj bo $G$ grupa z upodobitvijo $\rho$ na prostoru $V$ in naj bo $\pi$ neka njena enorazsežna upodobitev. Taka upodobitev je seveda nerazcepna. Vektor $v \in V$ pripada izotipični komponenti $\operatorname{Izotip}_\rho(\pi)$, če in samo če grupa $G$ na prostoru $\langle v\rangle$ deluje kot s $\pi$, se pravi

  $$\operatorname{Izotip}_\rho(\pi) = \{v \in V \mid \forall g \in G\colon\ \rho(g)\cdot v = \pi(g)v\},$$

  pri čemer $\pi$ interpretiramo kot preslikavo v polje.

  Kadar je grupa $G$ abelova, je vsaka njena nerazcepna upodobitev nad algebraično zaprtim poljem enorazsežna. Vsaka polenostavna upodobitev take grupe je zato direktna vsota podprostorov, na katerih grupa deluje s skalarnimi množenji prek svojih enorazsežnih upodobitev.

## 2.2 Matrični koeficienti

Vsaka upodobitev dane grupe je homomorfizem v grupo obrnljivih matrik $\mathrm{GL}(V)$. Do sedaj smo na upodobitve gledali z bolj konceptualnega stališča: govorili smo o strukturi prostora $V$ in o njegovi morebitni dekompoziciji na nerazcepne upodobitve. Zdaj si bomo z vsako od teh umazali roke in si jo ogledali še podrobneje.

Predpostavimo, da je prostor $V$ končno razsežen. Izberimo bazo prostora $V$ in s tem izomorfizem $V \cong F^n$ za nek $n$, tako da je upodobitev dana s homomorfizmom $\rho: G \to \mathrm{GL}_n(F)$. Vsak tak homomorfizem je *po komponentah* podan s svojimi **matričnimi koeficienti**; to so funkcije

$$f_{i,j}: G \to F, \quad g \mapsto \langle e_i^*, \rho(g) \cdot e_j \rangle = \rho(g)_{i,j}$$

za $i, j \in \{1, 2, \ldots, n\}$.

O matričnih koeficientih upodobitve $\rho$ lahko abstraktneje govorimo tudi brez izbire baze prostora. Za vsak vektor $v \in V$ in kovektor $\lambda \in V^*$ definiramo $f_{v,\lambda}: G \to F$, $g \mapsto \langle \lambda, \rho(g) \cdot v \rangle$. To so **posplošeni matrični koeficienti**. Kadar je prostor $V$ končno razsežen, lahko vsak vektor razvijemo po izbrani bazi in vsak kovektor po dualni bazi, s čimer posplošeni matrični koeficient razvijemo po običajnih matričnih koeficientih.

### Matrični koeficienti in regularna upodobitev

Matrične koeficiente lahko vidimo kot elemente vektorskega prostora funkcij $\mathrm{fun}(G, F)$ iz $G$ v $F$. Na tem prostoru deluje grupa $G$ z regularno upodobitvijo $\rho_{\mathrm{fun}}$. Naj bo $\mathrm{MK}(\pi) \leq \mathrm{fun}(G, F)$ podprostor, ki ga razpenjajo matrični koeficienti neke končno razsežne nerazcepne upodobitve $\pi$.[9]

**Trditev 2.2.1.** $\mathrm{MK}(\pi)$ *je $G$-invarianten podprostor.*

*Dokaz.* Naj bo $g \in G$ in $f_{v,\lambda}$ posplošen matrični koeficient. Velja

$$(g \cdot f_{v,\lambda}): x \mapsto f_{v,\lambda}(xg) = \langle \lambda, \pi(xg) \cdot v \rangle = f_{\pi(g)\cdot v, \lambda}(x),$$

zato je $g \cdot f_{v,\lambda} = f_{\pi(g)\cdot v,\lambda} \in \mathrm{MK}(\pi)$. □

Matrični koeficienti upodobitve $\pi$ nam torej dajejo podupodobitev na prostoru $\mathrm{MK}(\pi)$ znotraj regularne upodobitve $\rho_{\mathrm{fun}}$ na $\mathrm{fun}(G, F)$. Ni presenetljivo, da je ta podupodobitev v resnici tesno povezana s $\pi$.

**Izrek 2.2.2.** *Naj bo $G$ grupa s končno razsežno nerazcepno upodobitvijo $\pi$. Tedaj je*

$$\mathrm{MK}(\pi) = \mathrm{Izotip}_{\rho_{\mathrm{fun}}}(\pi)$$

*Nad algebraično zaprtim poljem je večkratnost $\pi$ v slednji upodobitvi enaka* $\deg(\pi)$.

*Dokaz.* Naj bo $\pi$ upodobitev na prostoru $W$. Spomnimo se, da je $\pi$-izotipična komponenta v $\rho_{\mathrm{fun}}$ napeta na vektorje oblike $\Phi(w)$ za $\Phi \in \hom_G(\pi, \rho_{\mathrm{fun}})$ in $w \in W$. Regularno upodobitev predstavimo kot inducirano upodobitev $\rho_{\mathrm{fun}} = \mathrm{Ind}_1^G(\mathbf{1})$. Po adjunkciji med restrikcijo in indukcijo je

$$\hom_G(\pi, \rho_{\mathrm{fun}}) \cong \hom_1(\mathrm{Res}_1^G(\pi), \mathbf{1}) \cong \hom(\mathbf{1}^{\deg(\pi)}, \mathbf{1}).$$

Naj bo $\{e_i \mid 1 \leq i \leq \deg(\pi)\}$ neka izbrana baza prostora $W$. Po zgornji adjunkciji s tem dobimo bazo

$$\Phi_i: W \to \mathrm{fun}(G, F), \quad w \mapsto (g \mapsto \langle e_i^*, \pi(g) \cdot w \rangle) = f_{e_i^*, w}$$

[9] Prostor $\mathrm{MK}(\pi)$ je enak prostoru, ki ga razpenjajo posplošeni matrični koeficienti upodobitve $\pi$, zato je neodvisen od izbire baze.

prostora spletičen $\hom_G(\pi, \rho_{\text{fun}})$ za $1 \le i \le \deg(\pi)$. Ko te bazne spletične evalviramo na izbrani bazi prostora $W$, dobimo torej ravno prostor $\mathrm{MK}(\pi)$. Nad algebraično zaprtim poljem te evalvacije tvorijo celo bazo[10]

$$\Phi_i(f_j) = f_{i,j}$$

prostora $\mathrm{Izotip}_{\rho_{\text{fun}}}(\pi)$. V izbranih bazah torej matrični koeficienti tvorijo bazo za $\pi$-izotipično komponento regularne upodobitve. Večkratnost $\pi$ v njej je enaka $\dim \hom_G(\pi, \rho_{\text{fun}}) = \deg(\pi)$. □

Izpostavimo pomembno posledico, ki nam pove, da lahko vse nerazcepne upodobitve najdemo v regularni.

**Posledica 2.2.3.** *Vsaka končno razsežna nerazcepna upodobitev dane grupe je uresničljiva kot podupodobitev regularne.*

V posebnem smo z zadnjim dokazom izpeljali, da so po izbiri baze matrični koeficienti končno razsežne nerazcepne upodobitve nad algebraično zaprtim poljem $\pi$ vselej linearno neodvisni.[11] Vseh je ravno $\deg(\pi)^2$ in znotraj regularne upodobitve tvorijo podupodobitev $\mathrm{MK}(\pi)$, ki sestoji iz $\deg(\pi)$ mnogo kopij upodobitve $\pi$.

Vse podobno velja, kadar imamo namesto ene same nerazcepne upodobitve *končno mnogo* paroma neizomorfnih nerazcepnih upodobitev $\{\pi_i\}_{i \in I}$ dane grupe $G$. Vsaka od njih nam po izbiri baze podari svoje matrične koeficiente. Ti razpenjajo prostore, ki so enaki izotipičnim komponentam v regularni upodobitvi in te komponente tvorijo notranjo direktno vsoto. Matrični koeficienti vseh teh upodobitev so torej linearno neodvisni med seboj. Vseh skupaj je $\sum_{i \in I} \deg(\pi_i)^2$.

Matrični koeficienti so elementi prostora funkcij $\mathrm{fun}(G, F)$. V primeru, ko je grupa končna, lahko po primerjanju dimenzij zato izpeljemo neenakost

$$\sum_{i \in I} \deg(\pi_i)^2 \le \dim \mathrm{fun}(G, F) = |G|.$$

**Posledica 2.2.4.** *Končna grupa ima le končno mnogo končno razsežnih nerazcepnih upodobitev. Nad algebraično zaprtim poljem je vsaka od njih stopnje kvečjemu* $\sqrt{|G|}$.

*Dokaz.* Vsaka končno razsežna nerazcepna upodobitev je vsebovana v regularni in se zatorej pojavi kot njen kompozicijski faktor. Vseh možnih kompozicijskih faktorjev je končno mnogo, ker je prostor $\mathrm{fun}(G, F)$ končno razsežen. Drugi del posledice sledi neposredno iz neenakosti pred njo. □

**Zgled 2.2.5.** Opazujmo grupo $S_3$ nad poljem $\mathbf{C}$. Njeno regularno upodobitev smo že razstavili na direktno vsoto $\mathbf{1} \oplus \rho$, kjer je $\rho$ dvorazsežna nerazcepna upodobitev. Poleg tega poznamo še enorazsežno predznačno upodobitev sgn. Vsota kvadratov stopenj teh treh upodobitev je $1^2 + 1^2 + 2^2 = 6$, kar je ravno enako moči grupe $S_3$. Od tod sledi, da so te tri *vse* končno razsežne nerazcepne upodobitve grupe $S_3$.

Več o upodobitvah končnih grup si bomo ogledali nekoliko kasneje.

## Karakterji

Naj bo $G$ grupa in $\rho$ njena končno razsežna upodobitev. Po izbiri baze dobimo matrične koeficiente $f_{i,j}$. Te lahko kombiniramo na različne načine, da dobimo funkcije v $\mathrm{fun}(G, F)$, ki so *neodvisne* od izbire baze. Najosnovnejša[12] taka funkcija je sled linearnega operatorja, se pravi

$$\chi_\rho : G \to F, \quad g \mapsto \mathrm{tr}(\rho(g)) = \textstyle\sum_{i=1}^{\deg(\rho)} f_{i,i}(g).$$

[10] Preslikava $\Sigma_{\pi, \rho_{\text{fun}}}$ je injektivna, ker je $\dim \hom_G(\pi, \rho_{\text{fun}}) = \deg(\pi) < \infty$.

[11] Temu dejstvu včasih pravimo *Burnsideov izrek o nerazcepnosti*.

[12] V resnici je sled do skalarja natančno *edina* taka funkcija.

| | $()$ | $(1\,2)$ | $(1\,2\,3)$ |
|---|---|---|---|
| $\chi_{\mathbf{1}}$ | 1 | 1 | 1 |
| $\chi_{\mathrm{sgn}}$ | 1 | $-1$ | 1 |
| $\chi_\rho$ | 2 | 0 | $-1$ |

Tabela 2.1: Tabela karakterjev $S_3$

To funkcijo imenujemo **karakter** upodobitve $\rho$. Kadar je upodobitev $\rho$ nerazcepna, tudi njenemu karakterju dodamo pridevnik *nerazcepen*.

Karakter je neodvisen od izbire baze, zato za vsaka $x,g \in G$ velja $\chi_\rho(xgx^{-1}) = \chi_\rho(g)$. Karakterji so torej funkcije na $G$, ki so konstantne na konjugiranostnih razredih.[13] Takim funkcijam pravimo **razredne funkcije** in jih označimo s

$$\mathrm{fun}_{\mathrm{cl}}(G,F) = \{f \in \mathrm{fun}(G,F) \mid \forall x,g \in G\colon f(xgx^{-1}) = f(g)\}.$$

Za dan konjugiranostni razred $\mathcal{C}$ v grupi $G$ bomo pisali $\chi_\rho(\mathcal{C})$ za vrednost karakterja v poljubnem predstavniku tega razreda.

**Zgled 2.2.6.** Opazujmo grupo $S_3$ nad poljem $\mathbf{C}$. Poznamo že vse tri njene končno razsežne nerazcepne upodobitve. Določimo karakterje teh nerazcepnih upodobitev. Karakterji enorazsežnih upodobitev so kot funkcije kar enaki upodobitvam. Za karakter $\chi_\rho$ velja

$$() \mapsto \mathrm{tr}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = 2, \quad (1\,2) \mapsto \mathrm{tr}\begin{pmatrix}-1 & 1\\ 0 & 1\end{pmatrix} = 0, \quad (1\,2\,3) \mapsto \mathrm{tr}\begin{pmatrix}0 & -1\\ 1 & -1\end{pmatrix} = -1.$$

V grupi $S_3$ je vsak element konjugiran enemu od $()$, $(1\,2)$ ali $(1\,2\,3)$. S tem so torej vse vrednosti karakterja $\chi_\rho$ določene.

Vse podatke o vrednostih karakterjev dane grupe po navadi zložimo v **tabelo karakterjev**. Stolpce indeksiramo s predstavniki konjugiranostnih razredov, vrstice pa z nerazcepnimi karakterji. Vrednosti v tabeli so vrednosti karakterjev v konjugiranostnih razredih.

Že samo imenovanje karakterjev odzvanja, da to niso poljubne funkcije v $\mathrm{fun}(G,F)$, temveč da v nekem smislu zajemajo srž upodobitve.

**Trditev 2.2.7.** *Naj bo $G$ grupa s končno razsežnima nerazcepnima upodobitvama nad algebraično zaprtim poljem. Ti dve upodobitvi sta izomorfni, če in samo če imata enaka karakterja.*

*Dokaz.* Ker so matrični koeficienti različnih nerazcepnih upodobitev linearno neodvisni med seboj, so tudi njihovi karakterji linearno neodvisni kot elementi prostora $\mathrm{fun}(G,F)$. □

Karakterjev fundamentalnih konstrukcij različnih upodobitev ni težko izračunati.

**Trditev 2.2.8.** *Naj bo $G$ grupa s končno razsežnimi upodobitvami $\rho$, $\rho_1$, $\rho_2$. Tedaj za vse $g \in G$ velja*

$$\chi_\rho(1) = \deg(\rho), \quad \chi_{\rho_1\oplus\rho_2} = \chi_{\rho_1} + \chi_{\rho_2}, \quad \chi_{\rho_1\otimes\rho_2} = \chi_{\rho_1}\cdot\chi_{\rho_2}, \quad \chi_{\rho^*}(g) = \chi_\rho(g^{-1}).$$

*Za podgrupo $H \leq G$ in poljuben $h \in H$ velja*

$$\chi_{\mathrm{Res}^G_H(\rho)}(h) = \chi_\rho(h).$$

*Kadar je $H \leq G$ končnega indeksa in $\rho$ upodobitev grupe $H$, za poljubno izbiro predstavnikov desnih odsekov $R$ grupe $H$ v $G$ velja*

$$\chi_{\mathrm{Ind}^G_H(\rho)}(g) = \sum_{r\in R:\, rgr^{-1}\in H} \chi_\rho(rgr^{-1}).$$

[13] **Konjugiranostni razred** elementa $g \in G$ je množica $\{xgx^{-1} \mid x \in G\}$. Grupa $G$ je disjunktna unija konjugiranostnih razredov svojih elementov. Včasih uporabljamo oznako $g^x = x^{-1}gx$ in s tem oznako $g^G$ za konjugiranostni razred elementa $g$ v $G$.

*Dokaz.* Netrivialna je le zadnja enakost o indukciji. Naj $H$ deluje na prostoru $V$ prek $\rho$. Spomnimo se, da lahko induciran prostor identificiramo z direktno vsoto $\bigoplus_{r\in R} Vr$, kjer je $Vr$ kopija prostora $V$ pri komponenti $r$. Element $g \in G$ deluje na $vr_0 \in Vr_0$ kot

$$g \cdot vr_0 = (\rho(h)\cdot v)r,$$

pri čemer je $r = hr_0g^{-1}$ za enolično določena $r \in R$, $h \in H$. Prostori $Vr$ se torej pri delovanju med seboj permutirajo, poleg tega pa grupa deluje netrivialno še na vsaki komponenti posebej. Za izračun sledi so zato relevantne samo komponente, ki so fiksne pri tej permutaciji. To so komponente $Vr_0$, za katere je $r = r_0$, se pravi komponente z lastnostjo $Hr_0g^{-1} = Hr_0$. To je enakovredno pogoju $r_0gr_0^{-1} \in H$. Za tako komponento $Vr_0$ element $g$ deluje na vektorju $vr_0$ kot

$$g \cdot vr_0 = \left(\rho(r_0gr_0^{-1})\cdot v\right)r_0,$$

zato je sled induciranega delovanja $g$ na $Vr_0$ enaka $\chi_\rho(r_0gr_0^{-1})$. Ko seštejemo prispevke po vseh relevantnih predstavnikih $r_0 \in R$, dobimo želeno formulo za induciran karakter. □

**Zgled 2.2.9.** Naj bo $G$ končna grupa. V tem primeru je regularna upodobitev $\rho_{\text{fun}}$ končno razsežna. Določimo njen karakter najprej na roke. V regularni upodobitvi imamo naravno bazo iz karakterističnih funkcij

$$1_x : G \to F, \quad y \mapsto \begin{cases} 1 & y = x, \\ 0 & \text{sicer.} \end{cases}$$

Na vsaki od teh element grupe $g \in G$ deluje kot $\rho_{\text{fun}}(g)\cdot 1_x = 1_{xg^{-1}}$. Grupa $G$ torej permutira karakteristične funkcije. Sled preslikave $\rho_{\text{fun}}(g)$ je zato enaka številu karakterističnih funkcij, ki jih ta preslikava fiksira. To je mogoče le, če je $x = xg^{-1}$, kar pa se zgodi zgolj pri $g = 1$, ko je $\rho_{\text{fun}}(1) = \mathrm{id}$ s sledjo $\dim \mathrm{fun}(G,F) = |G|$. Torej je karakter regularne upodobitve končne grupe enak

$$\chi_{\rho_{\text{fun}}} : G \to F, \quad g \mapsto \begin{cases} |G| & g = 1, \\ 0 & \text{sicer.} \end{cases}$$

Ta karakter bi lahko hitreje izračunali s pomočjo znane identifikacije $\rho_{\text{fun}} \cong \mathrm{Ind}_1^G(\mathbf{1})$. V tem primeru je $R = G$ in za $g \neq 1$ je vsota v formuli za induciran karakter prazna, torej se evalvira v 0, za $g = 1$ pa dobimo $\sum_{r\in G} \chi_{\mathbf{1}}(1) = |G|$.

Lastnost karakterjev kot srža upodobitve se prenese na končno razsežne polenostavne upodobitve, *če je le polje ničelne karakteristike*. Karakter dane polenostavne upodobitve $\rho$ namreč lahko razvijemo kot

$$\chi_\rho = \textstyle\sum_{\pi\in \mathrm{Irr}(G)} \mathrm{mult}_\rho(\pi)\cdot\chi_\pi.$$

Polenostavna upodobitev je enolično določena s svojimi nerazcepnimi komponentami in njihovimi večkratnostmi. Če je torej $\chi_{\rho_1} = \chi_{\rho_2}$ za polenostavni upodobitvi $\rho_1$, $\rho_2$, potem od tod iz neodvisnosti nerazcepnih karakterjev sledi enakost $\mathrm{mult}_{\rho_1}(\pi) = \mathrm{mult}_{\rho_2}(\pi)$ za vsako nerazcepno upodobitev $\pi$. To je enakost v polju $F$, od koder po predpostavki o ničelni karakteristiki sledi, da ta enakost velja tudi v kolobarju celih števil. S tem je $\rho_1 \cong \rho_2$.

**Posledica 2.2.10.** *Nad algebraično zaprtim poljem ničelne karakteristike je polenostavna upodobitev do izomorfizma natančno določena s svojim karakterjem.*

Karakterji so torej funkcije na grupi, s katerimi so v številnih primerih upodobitve, ki so sicer veliko bolj kompleksni objekti kot le funkcije na grupi, natančno določene. V nadaljevanju bomo videli, da lahko včasih eksplicitno izračunamo vse nerazcepne karakterje, ne da bi sploh poznali same nerazcepne upodobitve. Na ta način lahko dodobra razumemo kategorijo upodobitev dane grupe zgolj z uporabo karakterjev.

# Poglavje 3

# Upodobitve končnih grup

V tem poglavju bomo raziskali kategorijo upodobitev končne grupe s posebnim poudarkom na situaciji, ko je karakteristika polja tuja moči grupe. V tem primeru je, kot bomo videli, vsaka upodobitev polenostavna, zato lahko vprežemo karakterje za razumevanje kategorije upodobitev.

## 3.1 Polenostavnost

### Nerazcepne upodobitve

Prepričajmo se najprej, da končne grupe nimajo *prevelikih* nerazcepnih upodobitev.

**Trditev 3.1.1.** *Vsaka nerazcepna upodobitev končne grupe je končno razsežna.*

*Dokaz.* Naj bo $G$ končna grupa z upodobitvijo $\rho$ na prostoru $V$. Izberimo poljuben neničeln vektor $v \in V$. Opazujmo podprostor

$$W = \langle \rho(g) \cdot v \mid g \in G \rangle$$

prostora $V$. Ker je $G$ končna, je $W$ končno razsežen. Hkrati je po konstrukciji ta podprostor $G$-invarianten. Vsaka upodobitev končne grupe ima torej končno razsežno podupodobitev. V posebnem to pomeni, da ni neskončno razsežne nerazcepne upodobitve. □

Iz trditve in razmislekov v prejšnjem poglavju sledi, da je vsaka nerazcepna upodobitev končne grupe vsebovana v regularni upodobitvi. Nad algebraično zaprtim poljem dodatno velja, da je razsežnosti kvečjemu $\sqrt{|G|}$.

### Maschkejev izrek

Spoznali smo že, da niso vse upodobitve polenostavne, niti kadar je grupa končna. Videli smo primer grupe $S_3$ z dvorazsežno upodobitvijo $\rho$, ki je bila definirana nad kolobarjem $\mathbf{Z}$ in katere projekcija po modulu 3 *ni* bila polenostavna. Naslednji izrek razkrije, da je to mogoče le v primeru, ko karakteristika polja deli moč grupe.

**Izrek 3.1.2** (Maschke)**.** *Naj bo $G$ končna grupa in $F$ polje. Tedaj je vsaka upodobitev $G$ nad poljem $F$ polenostavna, če in samo če* $\operatorname{char}(F) \nmid |G|$.

Preden dokažemo izrek, pojasnimo, kako in zakaj nam prideta prav končnost grupe $G$ in ustrezna karakteristika polja $F$. Ti dve predpostavki namreč odpirata vrata orodju **povprečenja po grupi**. Za dano funkcijo $f \in \operatorname{fun}(G, F)$ lahko v tej ugodni situaciji izračunamo njeno povprečno vrednost[1]

$$\mathbf{E}(f) = \frac{1}{|G|} \sum_{g \in G} f(g) \in F.$$

[1] Tukaj uporabljamo verjetnostno oznako za povprečno vrednost. Mislimo si, da enakomerno naključno izberemo element $X$ iz grupe $G$ in v njem izračunamo vrednost $f$. Število $\mathbf{E}(f)$ je pričakovana vrednost slučajne spremenljivke $f(X)$.

Te račune povprečij lahko razširimo na izračun povprečne linearne preslikave upodobitve. Za dano upodobitev $\rho$ grupe $G$ na prostoru $V$ lahko v tej ugodni situaciji izračunamo njeno povprečno vrednost

$$\mathbf{E}(\rho) = \frac{1}{|G|}\sum_{g\in G}\rho(g) \in \hom(V,V).$$

**Domača naloga 3.1.3.** Preveri, da je $\mathbf{E}(\rho) \in \hom_G(V,V)$ projekcijska spletična na podprostor fiksnih vektorjev $V^G$.

*Dokaz.* (dokaz Maschkejevega izreka) ($\Leftarrow$) : Predpostavimo $\mathrm{char}(F) \nmid |G|$. Naj bo $\rho$ upodobitev grupe $G$ na prostoru $V$ in naj bo $W$ poljuben $G$-invarianten podprostor. Naj bo $P \in \hom(V,V)$ projektor na $W$. Grupa $G$ deluje na prostoru linearnih preslikav $\hom(V,V)$.[2] Povprečna vrednost tega delovanja je projekcijska spletična na podprostor spletičen $\hom(V,V)^G = \hom_G(V,V)$. Ko to povprečno vrednost uporabimo na projektorju $P$, dobimo torej linearno preslikavo

$$Q = \frac{1}{|G|}\sum_{g\in G} g\cdot P \in \hom_G(V,V),$$

za katero velja $Q|_W = \mathrm{id}_W$ in $\mathrm{im}\,Q = W$. Torej je $Q$ projekcijska spletična na $W$. Njeno jedro je zato $G$-invarianten komplement prostora $W$ v $V$. ✓

($\Rightarrow$) : Predpostavimo, da $\mathrm{char}(F) \mid |G|$.[3] Opazujmo regularno upodobitev $\rho_{\mathrm{fun}}$ na prostoru $\mathrm{fun}(G,F)$. Ta prostor ima vselej $G$-invarianten podprostor

$$\mathrm{fun}_0(G,F) = \left\{f \in \mathrm{fun}(G,F) \mid \textstyle\sum_{g\in G} f(g) = 0\right\}$$

korazsežnosti 1 v $\mathrm{fun}(G,F)$. Dokažimo, da upodobitev na tem podprostoru *ni* komplementirana in da torej vsaka upodobitev ni polenostavna.

Zavoljo protislovja predpostavimo, da komplement obstaja. Imamo torej funkcijo $0 \neq \phi \in \mathrm{fun}(G,F)$, za katero velja $\sum_{g\in G}\phi(g) \neq 0$ in prostor $F\cdot\phi$ je $G$-invarianten. Torej obstaja enorazsežna upodobitev $\chi : G \to F^*$, da pri vsakem $g \in G$ velja $g\cdot\phi = \chi(g)\cdot\phi$, se pravi $\phi(g) = \chi(g)\cdot\phi(1)$. Od tod sledi

$$\sum_{g\in G}\phi(g) = \phi(1)\cdot\sum_{g\in G}\chi(g).$$

Trdimo, da je zadnja vsota vselej ničelna, kar nas privede v protislovje s predpostavko $\sum_{g\in G}\phi(g) \neq 0$. Če je namreč $\chi$ trivialna upodobitev, potem iz predpostavke o karakteristiki izpeljemo

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

Če pa $\chi$ ni trivialna, potem za nek $x \in G$ velja $\chi(x) \neq 1$ in v tem primeru izračunamo

$$(\chi(x)-1)\cdot\sum_{g\in G}\chi(g) = \sum_{g\in G}\chi(xg) - \sum_{g\in G}\chi(g) = 0,$$

kar zopet implicira $\sum_{g\in G}\chi(g) = 0$. ✓ □

**Zgled 3.1.4.** V ekstremni situaciji, ko je $\mathrm{char}(F) = p > 0$ in $|G| = p^n$ za nek $n \in \mathbf{N}$, je kategorija upodobitev videti precej nenavadno. V takih neugodnih razmerah *netrivialnih nerazcepnih upodobitev ni*. Poglejmo si, zakaj je tako v primeru $F = \mathbf{F}_p$ za neko praštevilo $p$.

Imejmo nerazcepno upodobitev $p$-grupe $G$ na prostoru $V$ nad poljem $\mathbf{F}_p$. Vemo že, da je $V$ nujno končno razsežen, zato je $|V| = p^k$ za neki $k \in \mathbf{N}$. Grupa $G$ permutacijsko deluje na množici neničelnih vektorjev $V\setminus\{0\}$. Po lemi o orbiti in stabilizatorju je velikost orbite vsakega neničelnega vektorja enaka indeksu stabilizatorja, ki je po predpostavki o moči grupe nujno potenca praštevila $p$. Ker pa moč $|V\setminus\{0\}|$ ni deljiva s $p$, mora obstajati vektor $0 \neq v \in V$ z orbito moči 1. Ta vektor je torej fiksen za delovanje grupe $G$ in zato razpenja enorazsežen podprostor $\mathbf{F}_p\cdot v$, ki je kot upodobitev izomorfen $\mathbf{1}$. Torej je $V = \mathbf{1}$ in upodobitev je res trivialna.

[2] Spomnimo se, da je delovanje $G$ na $\hom(V,V)$ dano kot $g\cdot\Phi = \rho(g)\Phi\rho(g)^{-1}$ za $g \in G$, $\Phi \in \hom(V,V)$.

[3] V tem primeru sicer nimamo dostopa do povprečenja v celoti, lahko pa uporabimo *delno* povprečenje, ki izračuna le vsoto po grupi.

## Dekompozicija regularne upodobitve

Naj bo $G$ končna grupa in $F$ algebraično zaprto polje karakteristike tuje $|G|$. Vsaka nerazcepna upodobitev $\pi$ grupe $G$ nad $F$ je uresničljiva kot podupodobitev regularne $\rho_{\text{fun}}$. Slednja je po Maschkejevem izreku polenostavna, zato jo lahko zapišemo kot direktno vsoto izotipičnih komponent nerazcepnih upodobitev. Vsaka $\pi$-komponenta pri tem sestoji iz $\deg(\pi)$ mnogo kopij upodobitve $\pi$. Izpostavimo in povzemimo.

**Izrek 3.1.5.** *Naj bo $G$ končna grupa in $F$ algebraično zaprto polje karakteristike tuje $|G|$. Velja*

$$\rho_{\text{fun}} \cong \bigoplus_{\pi \in \text{Irr}(G)} \underbrace{\pi \oplus \pi \oplus \cdots \oplus \pi}_{\deg(\pi)}.$$

V posebnem iz izreka po primerjavi razsežnosti izpeljemo

$$\sum_{\pi \in \text{Irr}(G)} \deg(\pi)^2 = |G|.$$

**Zgled 3.1.6.**

- Opazujmo permutacijsko upodobitev $\pi$ grupe $\mathbf{Z}/n\mathbf{Z}$ na prostoru $\mathbf{C}[\Omega]$, kjer je $\Omega = \{1, 2, \ldots, n\}$. Premislili smo že, da je $\pi$ izomorfna regularni upodobitvi in da jo lahko razstavimo kot direktno vsoto $\pi = \bigoplus_{j \in \Omega} \chi_j$, kjer je $\chi_j : \mathbf{Z}/n\mathbf{Z} \to \mathbf{C}^*$, $x \mapsto e^{2\pi i j x/n}$, enorazsežna upodobitev. V posebnem od tod sledi, da so $\{\chi_j \mid j \in \Omega\}$ *vse* neizomorfne nerazcepne upodobitve ciklične grupe $\mathbf{Z}/n\mathbf{Z}$.
- Naj bo $A$ poljubna končna abelova grupa. Strukturni izrek o abelovih grupah nam pove, da $A$ lahko zapišemo kot direktni produkt določenih cikličnih grup, se pravi $A = C_1 \times C_2 \times \cdots \times C_k$. Kategorijo upodobitev vsake od cikličnih kosov nad $\mathbf{C}$ že poznamo. Naj bodo $\{\chi^i_j \mid j \in \Omega_i\}$ nerazcepne upodobitve grupe $C_i$. Tvorimo lahko **produkt upodobitev**

  $$\chi^1_{j_1} \times \chi^2_{j_2} \times \cdots \times \chi^k_{j_k} : \prod_{i=1}^k C_i = A \to \mathbf{C}^*, \quad (c_1, c_2, \ldots, c_k) \mapsto \prod_{i=1}^k \chi^i_{j_i}(c_i).$$

  Na ta način dobimo $\prod_{i=1}^k |\Omega_i| = \prod_{i=1}^k |C_i| = |A|$ enorazsežnih upodobitev. Vsaki dve od teh sta različni med seboj. Na ta način smo torej našli *vse* nerazcepne upodobitve abelove grupe $A$.

**Domača naloga 3.1.7.** Naj bosta $G_1, G_2$ grupi z nerazcepnima končno razsežnima upodobitvama $\rho_1, \rho_2$ nad algebraično zaprtim poljem. Tedaj je produkt $\rho_1 \times \rho_2$ nerazcepna upodobitev grupe $G_1 \times G_2$. Premisli, da velja tudi obratno; vsaka končno razsežna kompleksna nerazcepna upodobitev grupe $G_1 \times G_2$ je oblike $\rho_1 \times \rho_2$ za neki nerazcepni upodobitvi $\rho_1, \rho_2$.

## Ortogonalnost matričnih koeficientov

Na prostor funkcij $\text{fun}(G, F)$ uvedimo **skalarni produkt** s predpisom

$$[f_1, f_2] = \frac{1}{|G|} \sum_{g \in G} f_1(g) f_2(g^{-1})$$

za $f_1, f_2 \in \text{fun}(G, F)$. Ker je polje $F$ v splošnem abstraktno, to sicer ni običajen skalarni produkt, je pa to vendarle nedegenerirana simetrična bilinearna forma na $\text{fun}(G, F)$, zato zanjo uporabljamo vso standardno terminologijo iz običajnih skalarnih produktov.

Z uporabo povprečenja na prostoru linearnih preslikav (podobno kot pri dokazu Maschkejevega izreka) bomo nadgradili dekompozicijo regularne upodobitve na *ortogonalno* direktno vsoto.

**Trditev 3.1.8.** *Naj bo $G$ končna grupa z neizomorfnima nerazcepnima upodobitvama $\pi_1$, $\pi_2$ nad algebraično zaprtim poljem karakteristike tuje $|G|$. Tedaj sta prostora $\text{MK}(\pi_1)$ in $\text{MK}(\pi_2)$ ortogonalna.*

*Dokaz.* Naj upodobitvi $\pi_1$, $\pi_2$ delujeta na prostorih $V_1$, $V_2$. Grupa $G$ deluje na prostoru linearnih preslikav $\hom(V_1,V_2)$. Povprečje tega delovanja je projekcijska spletična na podprostor $\hom(V_1,V_2)^G = \hom_G(V_1,V_2)$, ki je po Schurovi lemi trivialen. Za poljubno linearno preslikavo $A \in \hom(V_1,V_2)$ je torej

$$\frac{1}{|G|}\sum_{g\in G} g\cdot A = 0.$$

Izberimo zdaj posebno preslikavo $A$. Naj bo $\{e_i\}_i$ baza prostora $V_1$ in $\{f_j\}_j$ baza prostora $V_2$. Vzemimo

$$A_{i,l}: V_1 \to V_2, \quad v \mapsto \langle e_i^*, v\rangle f_l.$$

S to izbiro dosežemo enakost

$$0 = \frac{1}{|G|}\sum_{g\in G}(g\cdot A_{i,l})(e_j) = \frac{1}{|G|}\sum_{g\in G}\langle e_i^*, g^{-1}\cdot e_j\rangle g\cdot f_l = \frac{1}{|G|}\sum_{g\in G} f_{i,j}^{\pi_1}(g^{-1})g\cdot f_l.$$

Na zadnjem uporabimo še $f_k^*$ in dobimo

$$0 = \frac{1}{|G|}\sum_{g\in G} f_{i,j}^{\pi_1}(g^{-1})\langle f_k^*, g\cdot f_l\rangle = \frac{1}{|G|}\sum_{g\in G} f_{i,j}^{\pi_1}(g^{-1})f_{k,l}^{\pi_2}(g),$$

kar je enakovredno $[f_{i,j}^{\pi_1}, f_{k,l}^{\pi_2}] = 0$, se pravi ortogonalnosti matričnih koeficientov. □

Na soroden način lahko analiziramo skalarne produkte znotraj matričnih koeficientov ene same nerazcepne upodobitve.

**Trditev 3.1.9.** *Naj bo $G$ končna grupa z nerazcepno upodobitvijo $\pi$ nad algebraično zaprtim poljem karakteristike tuje $|G|$. Po izbiri poljubne baze za matrične koeficiente velja*

$$[f_{i,j}, f_{k,l}] = \begin{cases} 1/\deg(\pi) & (i,j) = (l,k) \\ 0 & \textit{sicer.} \end{cases}$$

*Dokaz.* Pristopimo kot pri zadnjem dokazu, pri čemer prostor spletičen $\hom_G(V,V)$ po Schurovi lemi zdaj sestoji le iz skalarnih večkratnikov identitete. Za linearno preslikavo $A \in \hom(V,V)$ je zato

$$\frac{1}{|G|}\sum_{g\in G} g\cdot A = \lambda_A \cdot \mathrm{id}_V$$

za neki $\lambda_A \in F$. Velja $g\cdot A = \pi(g)A\pi(g)^{-1}$, zato je $\mathrm{tr}(g\cdot A) = \mathrm{tr}(A)$, od koder izpeljemo

$$\lambda_A = \frac{\mathrm{tr}(A)}{\deg(\pi)}.$$

Kot v zadnjem dokazu dobljeno uporabimo s preslikavo $A_{i,l}(v) = \langle e_i^*, v\rangle e_l$ za neko izbrano bazo $\{e_i\}_i$ prostora $V$. Velja $\mathrm{tr}(A_{i,l}) = \langle e_i^*, e_l\rangle = 1_{i=l}$, od koder kot v zadnjem dokazu izpeljemo

$$[f_{i,j}, f_{k,l}] = \langle e_k^*, e_j\rangle \frac{1_{i=l}}{\deg(\pi)} = \frac{1_{i=l,j=k}}{\deg(\pi)},$$

kar je natanko želeno. □

## 3.2 Karakterji

Iz rezultatov zadnjega razdelka sledi, da je nad algebraično zaprtim poljem ničelne karakteristike (na primer zelo ugodnim poljem $\mathbf{C}$) kategorija upodobitev dane končne grupe popolnoma določena z nerazcepnimi upodobitvami, ki jih lahko razumemo s pomočjo karakterjev. V tem razdelku bomo podrobneje razvili to teorijo.

## Ortonormiranost karakterjev

Iz ortogonalnosti matričnih koeficientov z lahkoto izpeljemo ortonormiranost karakterjev.

**Posledica 3.2.1.** *Naj bo $G$ končna grupa z nerazcepnima upodobitvama $\pi_1$, $\pi_2$ nad algebraično zaprtim poljem karakteristike tuje $|G|$. Velja*

$$[\chi_{\pi_1}, \chi_{\pi_2}] = \begin{cases} 1 & \pi_1 \cong \pi_2, \\ 0 & \textit{sicer.} \end{cases}$$

*Dokaz.* Izberemo bazo, izrazimo $\chi_\pi = \sum_i f^\pi_{i,i}$ in uporabimo zadnji dve trditvi o skalarnih produktih matričnih koeficientov. □

V skladu z običajno terminologijo za funkcijo $f \in \mathrm{fun}(G,F)$ označimo $\|f\| = \sqrt{[f,f]}$, to je **norma** funkcije $f$. Nerazcepni karakterji tvorijo ortonormiran sistem vektorjev v $\mathrm{fun}(G,F)$.

## Razredne funkcije

Karakterji niso poljubne funkcije v $\mathrm{fun}(G,F)$, temveč vselej pripadajo prostoru $\mathrm{fun}_{\mathrm{cl}}(G,F)$ razrednih funkcij. Vemo že tudi, da so karakterji nerazcepnih upodobitev tudi linearno neodvisni. S pomočjo ortonormiranosti karakterjev bomo sedaj dokazali, da tvorijo celo *bazo* prostora razrednih funkcij.

**Izrek 3.2.2** (o bazi razrednih funkcij)**.** *Naj bo $G$ grupa in $F$ algebraično zaprto polje karakteristike tuje $|G|$. Tedaj karakterji nerazcepnih upodobitev tvorijo ortonormirano bazo prostora* $\mathrm{fun}_{\mathrm{cl}}(G,F)$.

Zopet bomo za dokaz uporabili metodo povprečenja po grupi, a bomo to povprečenje še *utežili*. Za dano funkcijo $f \in \mathrm{fun}(G,F)$ definiramo njeno **nekomutativno Fourierovo transformacijo** $\hat{f}$ kot funkcijo, ki poljubni upodobitvi $\rho$ grupe $G$ na prostoru $V$ priredi

$$\hat{f}(\rho) = \sum_{g \in G} f(g)\rho(g^{-1}) \in \hom(V,V).$$

Fourierova transformacija funkciji $f$ torej priredi njeno uteženo povprečje poljubne upodobitve vzdolž $f$, pri čemer se zgleduje po skalarnem produktu na prostoru funkcij $\mathrm{fun}(G,F)$. V primeru, ko je $f$ konstantna funkcija $1/|G|$, z njeno Fourierovo transformacijo najdemo običajno povprečno vrednost upodobitve $\mathbf{E}(\rho)$.

**Zgled 3.2.3.**

- Naj bo $f$ poljubna periodična funkcija na množici $\mathbf{Z}$ s periodo $n > 1$ in vrednostmi v $\mathbf{C}$. Funkcijo $f$ lahko torej obravnavamo kot funkcijo na ciklični grupi $\mathbf{Z}/n\mathbf{Z}$. Nerazcepne kompleksne upodobitve slednje grupe so ravno enorazsežne upodobitve $\chi_j(x) = e^{2\pi i j x/n}$ za $j \in \Omega = \{1,2,\ldots,n\}$. Nekomutativna Fourierova transformacija funkcije $f$ v teh upodobitvah je

  $$\hat{f}(\chi_j) = \sum_{x \in \mathbf{Z}/n\mathbf{Z}} f(x)e^{-2\pi i j x/n}.$$

  Vektorju števil $(f(1), f(2), \ldots, f(n)) \in \mathbf{C}^n$ na ta način priredimo vektor $(\hat{f}(\chi_1), \hat{f}(\chi_2), \ldots, \hat{f}(\chi_n)) \in \mathbf{C}^n$. To prirejanje je v numerični matematiki znano pod imenom **diskretna Fourierova transformacija** in je fundamentalno v digitalnem procesiranju signalov.

- Naj bo $f \in \mathrm{fun}(G,F)$ funkcija na $G$ in $\rho_{\mathrm{fun}}$ regularna upodobitev grupe $G$. Vrednost $\hat{f}(\rho_{\mathrm{fun}})$ je linearni endomorfizem prostora funkcij $\mathrm{fun}(G,F)$. Pri tem se karakteristična funkcija $1_x$ za $x \in G$ preslika v

  $$\hat{f}(\rho_{\mathrm{fun}}) \cdot 1_x = \sum_{g \in G} f(g)\rho_{\mathrm{fun}}(g^{-1}) \cdot 1_x = \sum_{g \in G} f(g) 1_{xg} = \sum_{g \in G} f(x^{-1}g) 1_g.$$

  V posebnem pri $x = 1$ dobimo $\hat{f}(\rho_{\mathrm{fun}}) \cdot 1_1 = f$. Funkcijo $f$ lahko torej rekonstruiramo iz vrednosti njene Fourierove transformacije v regularni upodobitvi.

Regularna upodobitev končne grupe nad ugodnim poljem je direktna vsota nerazcepnih upodobitev grupe, zato je tudi Fourierova transformacija v regularni upodobitvi direktna vsota Fourierovih transformacij v nerazcepnih upodobitvah. Iz zgornjega premisleka sledi, da je vsaka funkcija zatorej enolično določena z vrednostmi svoje Fourierove transformacije v vseh nerazcepnih upodobitvah.

**Lema 3.2.4** (o Fourierovi transformaciji razredne funkcije)**.** *Naj bo $G$ končna grupa in $F$ algebraično zaprto polje karakteristike tuje $|G|$. Za vsako* razredno *funkcijo $f$ in nerazcepno upodobitev $\pi$ na prostoru $V$ je*

$$\hat{f}(\pi) = \frac{|G|}{\deg(\pi)} \cdot [f, \chi_\pi] \cdot \mathrm{id}_V.$$

*Dokaz.* Za vsak $h \in G$ velja

$$\hat{f}(\pi) \cdot \pi(h) = \sum_{g \in G} f(g)\pi(g^{-1}h) = \sum_{g \in G} f(g)\pi(h)\pi(h^{-1}g^{-1}h).$$

Izpostavimo $\pi(h)$ in na grupi $G$ uporabimo avtomorfizem $g \mapsto hgh^{-1}$, pa lahko zadnjo vsoto zapišemo kot

$$\pi(h) \sum_{g \in G} f(hgh^{-1})\pi(g^{-1}).$$

Ker je $f$ razredna funkcija, je dobljeno ravno enako $\pi(h) \cdot \hat{f}(\pi)$. Vrednost Fourierove transformacije v $\pi$ je torej spletična v $\hom_G(\pi, \pi)$. Po Schurovi lemi sklepamo, da je $\hat{f}(\pi)$ skalarni večkratnik identitete. Njegova sled je enaka

$$\mathrm{tr}\left(\hat{f}(\pi)\right) = \sum_{g \in G} f(g)\chi_\pi(g^{-1}) = |G| \cdot [f, \chi_\pi].$$

Od tod izračunamo relevantni skalar kot $|G| \cdot [f, \chi_\pi] / \deg(\pi)$. □

Opremljeni lahko z lahkoto izpeljemo izrek.

*Dokaz.* (dokaz izreka o bazi razrednih funkcij) Predpostavimo, da nerazcepni karakterji *ne* razpenjajo prostora razrednih funkcij. Torej obstaja funkcija $f \in \mathrm{fun}_{\mathrm{cl}}(G, F)$, ki je vsebovana v ortogonalnem komplementu vseh nerazcepnih karakterjev. Za vsak $\pi \in \mathrm{Irr}(G)$ velja torej $[f, \chi_\pi] = 0$. Preslikava $\hat{f}(\pi)$ je po lemi zato ničelna. Ker to velja za vsako nerazcepno upodobitev, mora veljati tudi za regularno upodobitev, se pravi $\hat{f}(\rho_{\mathrm{fun}}) = 0$. Po zadnjem zgledu to implicira $f = 0$. □

Vsaka razredna funkcija je enolično določena s svojimi vrednostmi v predstavnikih konjugiranostnih razredov. Če **število konjugiranostnih razredov** označimo s $\mathrm{k}(G)$, velja torej $\dim \mathrm{fun}_{\mathrm{cl}}(G, F) = \mathrm{k}(G)$. Ker karakterji tvorijo bazo prostora razrednih funkcij, lahko *število* nerazcepnih upodobitev torej izračunamo neposredno iz algebraične strukture grupe.

**Posledica 3.2.5.** *Za končno grupo $G$ nad algebraično zaprtim poljem karakteristike tuje $|G|$ velja $|\mathrm{Irr}(G)| = \mathrm{k}(G)$.*

V splošnem *ne* poznamo eksplicitne korespondence[4] med konjugiranostnimi razredi in nerazcepnimi upodobitvami. Vemo le, da njuni števili sovpadata.

**Zgled 3.2.6.**

- Opazujmo diedrsko grupo $D_{2n}$ nad poljem $\mathbf{C}$. Vsak element te grupe lahko zapišemo v obliki $r^i$ ali $sr^i$ za nek $0 \leq i < n$. Izračunajmo konjugiranostne razrede. Velja

$$\left(r^i\right)^{r^j} = r^i, \quad \left(r^i\right)^{sr^j} = r^{-i},$$

[4] In najverjetneje taka korespondenca v splošnem *ne* obstaja. Je pa na voljo za kakšne posebne družine grup, kot bomo spoznali kasneje.

| | $1$ | $r^i$ | $s$ |
|---|---|---|---|
| $\chi_\epsilon$ | $1$ | $1$ | $\epsilon$ |
| $\chi_{\rho_k}$ | $2$ | $2\cos(2\pi ik/n)$ | $0$ |

Tabela 3.1: Tabela karakterjev $D_{2n}$ za lih $n$

zato je konjugiranostni razred $r^i$ enak $\{r^i, r^{-i}\}$. Za $i \neq 0, n/2$ ima vsak razred 2 elementa. Vseh teh konjugiranostnih razredov je torej $\lfloor (n+2)/2 \rfloor$. Velja tudi

$$\left(sr^i\right)^{r^j} = sr^{2j+i}, \quad \left(sr^i\right)^{sr^j} = sr^{2j-i},$$

zato je konjugiranostni razred $s$ enak $\{sr^{2j} \mid j \in \mathbf{Z}\}$ in konjugiranostni razred $sr$ je enak $\{sr^{2j+1} \mid j \in \mathbf{Z}\}$. Če je $n$ sod, sta ta dva razreda disjunktna, če je $n$ lih, pa sovpadata. Skupaj torej dobimo

$$\mathrm{k}(D_{2n}) = \begin{cases} n/2+3 & n \equiv 0 \pmod 2, \\ (n+3)/2 & n \equiv 1 \pmod 2. \end{cases}$$

Določimo zdaj še nerazcepne upodobitve. Poznamo že dvorazsežne nerazcepne upodobitve $\rho_k$ za $0 < k < n/2$, vseh teh je $\lceil n/2 \rceil - 1$. Za karakter take upodobitve velja $\chi_{\rho_k}(r) = 2\cos(2\pi k/n)$, zato so vsi ti karakterji različni med seboj in s tem so upodobitve $\rho_k$ neizomorfne. Poleg teh dvorazsežnih upodobitev imamo še linearne upodobitve. Število teh je enako velikosti abelacije $D_{2n}/[D_{2n}, D_{2n}]$.[5] Velja

$$[r^i, sr^j] = r^{-i}\left(r^i\right)^{sr^j} = r^{-2i}, \quad [sr^i, sr^j] = r^{-i}s\left(sr^i\right)^{sr^j} = r^{2j-2i},$$

zato je $[D_{2n}, D_{2n}] = \langle r^2 \rangle$. S tem je

$$D_{2n}/[D_{2n}, D_{2n}] \cong \begin{cases} (\mathbf{Z}/2\mathbf{Z})^2 & n \equiv 0 \pmod 2, \\ \mathbf{Z}/2\mathbf{Z} & n \equiv 1 \pmod 2. \end{cases}$$

Linearne upodobitve so torej oblike

$$\chi_{\epsilon,\delta} : D_{2n} \to \mathbf{C}^*, \quad s \mapsto \epsilon, \quad r \mapsto \delta$$

za $\epsilon, \delta \in \{1, -1\}$. Ko je $n$ lih, je nujno $\delta = 1$.

Skupaj smo torej našli ravno $\mathrm{k}(D_{2n})$ nerazcepnih upodobitev, zato so to *vse* nerazcepne upodobitve grupe $D_{2n}$.

**Domača naloga 3.2.7.** Izračunaj tabelo kompleksnih karakterjev kvaternionske grupe $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, v kateri velja $i^2 = j^2 = k^2 = ijk = -1$. Primerjaj jo s tabelo karakterjev grupe $D_8$.

- Opazujmo simetrično grupo $S_n$ nad poljem $\mathbf{C}$. Vsako njeno permutacijo $\sigma \in S_n$ lahko zapišemo kot produkt disjunktnih ciklov.[6] Recimo, da so dolžine teh ciklov enake $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k$. Seveda velja $\sum_{i=1}^k \lambda_i = n$. Zaporedju $(\lambda_1, \lambda_2, \ldots, \lambda_k)$ pravimo **cikličnі tip** permutacije $\sigma$. Kadar so kateri od členov cikličnega tipa enaki, ciklični tip pišemo tudi kot $1^{i_1}2^{i_2}\cdots n^{i_n}$, kjer je $i_m$ število ciklov dolžine $m$ v $\sigma$.

  **Domača naloga 3.2.8.** Konjugiranostni razredi v $S_n$ so določeni s cikličnim tipom. Natančneje, če je $(\lambda_1, \lambda_2, \ldots, \lambda_k)$ ciklični tip permutacije $\sigma$, potem konjugiranostni razred $\sigma^{S_n}$ sestoji natanko iz vseh permutacij s tem cikličnim tipom. Ta konjugiranostni razred po navadi označimo kot $\mathcal{C}_{(\lambda_1, \lambda_2, \ldots, \lambda_k)}$.

[5] **Komutator** elementov $x, y \in G$ je element $[x, y] = x^{-1}y^{-1}xy$. **Komutatorska podgrupa** grupe $G$ je $[G, G] = \langle [x, y] \mid x, y \in G \rangle$.

[6] Pri tem fiksne točke permutacije obravnavamo kot cikle dolžine 1.

V teoriji števil in kombinatoriki cikličnim tipom rečemo tudi **razčlenitve** števila $n$. Število vseh razčlenitev označimo s $p(n)$. Velja torej $p(n) = \mathrm{k}(S_n) = |\mathrm{Irr}(S_n)|$. Splošna eksplicitna formula za to število *ne* obstaja, poznamo pa njeno asimptotsko oceno

$$p(n) \sim \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{\frac{2n}{3}}}$$

za $n \to \infty$ (Hardy-Ramanujan 1918).

V konkretnem primeru $n = 3$ velja $p(3) = 3$, namreč $3 = 3 = 2+1 = 1+1+1$. Res smo našli natanko 3 nerazcepne upodobitve grupe $S_3$. V primeru $n = 4$ pa velja $p(4) = 5$. Temu ustrezajo konjugiranostni razredi identične permutacije $()$ $(4 = 1+1+1+1)$, transpozicije $(1\ 2)$ $(4 = 2+1+1)$, tricikla $(1\ 2\ 3)$ $(4 = 3+1)$, štiricikla $(1\ 2\ 3\ 4)$ $(4 = 4)$ in produkta dveh tranzpozicij $(1\ 2)(3\ 4)$ $(4 = 2+2)$. Ti konjugiranostni razredi so zaporedoma velikosti 1, 6, 8, 6, 3. Kmalu bomo s tem podatkom določili tabelo karakterjev grupe $S_4$.

Ker nerazcepni karakterji tvorijo ortonormirano bazo prostora razrednih funkcij, lahko vsako razredno funkcijo $f \in \mathrm{fun}_{\mathrm{cl}}(G,F)$ razvijemo po tej bazi kot

$$f = \sum_{\pi \in \mathrm{Irr}(G)} [f, \chi_\pi]\chi_\pi.$$

Alternativna baza prostora razrednih funkcij sestoji iz karakterističnih funkcij konjugiranostnih razredov v $G$. Razvoj te baze po karakterjih nam podaja še eno relacijo med karakterji, ki je ortogonalna[7] ortonormiranosti.

**Posledica 3.2.9.** *Naj bo $G$ končna grupa nad algebraično zaprtim poljem karakteristike tuje $|G|$. Za vsaka elementa $g, h \in G$ velja*

$$\sum_{\pi \in \mathrm{Irr}(G)} \chi_\pi(g)\chi_\pi(h^{-1}) = \begin{cases} |G|/|g^G| & g^G = h^G, \\ 0 & \textit{sicer.} \end{cases}$$

*Dokaz.* Karakteristično funkcijo $1_{h^G}$ razvijemo po nerazcepnih karakterjih kot

$$1_{h^G} = \sum_{\pi \in \mathrm{Irr}(G)} [1_{h^G}, \chi_\pi]\chi_\pi = \sum_{\pi \in \mathrm{Irr}(G)} \frac{|h^G|}{|G|} \chi_\pi(h^{-1})\chi_\pi$$

in dobljeno evalviramo v elementu $g$. □

## Razstavljanje upodobitve

S pomočjo ortonormirane baze karakterjev z lahkoto razumemo vsako končno razsežno upodobitev končne grupe nad ugodnim poljem.

**Posledica 3.2.10.** *Naj bo $G$ končna grupa s končno razsežno upodobitvijo $\rho$ nad algebraično zaprtim poljem karakteristike 0.*

1. *Za vsako nerazcepno upodobitev $\pi$ velja* $\mathrm{mult}_\rho(\pi) = [\chi_\rho, \chi_\pi]$.
2. $||\chi_\rho||^2 = \sum_{\pi \in \mathrm{Irr}(G)} \mathrm{mult}_\rho(\pi)^2$.
3. *Upodobitev $\rho$ je nerazcepna, če in samo če* $||\chi_\rho|| = 1$.

[7] Relaciji sta ortogonalni v smislu tabele karakterjev. Ortonormiranost karakterjev preberemo tako, da fiksiramo vrstice. To drugo relacijo pa preberemo tako, da fiksiramo stolpce. Tej relaciji včasih rečemo **druga ortogonalnostna relacija**.

| | () | (1 2) | (1 2 3) | (1 2 3 4) | (1 2)(3 4) |
|---|---|---|---|---|---|
| $\chi_{\mathbf{1}}$ | 1 | 1 | 1 | 1 | 1 |
| $\chi_{\mathrm{sgn}}$ | 1 | −1 | 1 | −1 | 1 |
| $\chi_\tau$ | 2 | 0 | −1 | 0 | 2 |
| $\chi_\rho$ | 3 | 1 | 0 | −1 | −1 |
| $\chi_{\mathrm{sgn}\otimes\rho}$ | 3 | −1 | 0 | 1 | −1 |

Tabela 3.2: Tabela karakterjev $S_4$

*Dokaz.* Upodobitev $\rho$ je polenostavna, zato lahko njen karakter zapišemo kot

$$\chi_\rho = \sum_{\pi\in\mathrm{Irr}(G)} \mathrm{mult}_\rho(\pi)\cdot\chi_\pi.$$

Skalarno pomnožimo s $\chi_\pi$ in uporabimo ortonormiranost, pa dobimo $\mathrm{mult}_\rho(\pi) = [\chi_\rho, \chi_\pi]$. Od tod izračunamo

$$\|\chi_\rho\|^2 = [\chi_\rho,\chi_\rho] = \sum_{\pi\in\mathrm{Irr}(G)} \mathrm{mult}_\rho(\pi)\cdot[\chi_\rho,\chi_\pi] = \sum_{\pi\in\mathrm{Irr}(G)} \mathrm{mult}_\rho(\pi)^2.$$

Nazadnje je $\|\chi_\rho\| = 1$, če in samo če je za natanko eno nerazcepno upodobitev $\pi$ njena večkratnost v $\rho$ enaka 1, se pravi, če je $\rho$ nerazcepna. □

**Zgled 3.2.11.** Opazujmo grupo $S_4$ nad poljem $\mathbf{C}$. Vemo že, da za predstavnike konjugiranostnih razredov lahko izberemo elemente $1 = ()$, $(1\ 2)$, $(1\ 2\ 3)$, $(1\ 2\ 3\ 4)$ in $(1\ 2)(3\ 4)$. S tem je število nerazcepnih upodobitev enako 5. Določimo jih.

Vemo že, da imamo natanko dve enorazsežni upodobitvi, in sicer $\mathbf{1}$ in sgn. Naj bo $\pi$ permutacijska upodobitev na prostoru $\mathbf{C}[\Omega]$, kjer je $\Omega = \{1,2,3,4\}$. V standardni bazi je vsaka matrika te upodobitve permutacijska, zato je vrednost karakterja $\chi_\pi$ v permutaciji $\sigma$ ravno število fiksnih točk $\sigma$. V izbranih predstavnikih konjugiranostnih razredov ima torej $\chi_\pi$ vrednosti $4,2,1,0,0$. Od tod izračunamo normo

$$\|\chi_\pi\|^2 = \frac{1}{4!}\left(1\cdot 4^2 + 6\cdot 2^2 + 8\cdot 1^2\right) = 2.$$

Upodobitev $\pi$ torej *ni* nerazcepna. Velja

$$[\chi_\pi,\chi_{\mathbf{1}}] = \frac{1}{4!}(1\cdot 4 + 6\cdot 2 + 8\cdot 1) = 1,$$

torej $\pi$ vsebuje $\mathbf{1}$ z večkratnostjo 1, kar je povsem analogno temu, kar smo videli pri grupi $S_3$. Zapišemo lahko torej $\pi = \mathbf{1}\oplus\rho$ za neko upodobitev $\rho$. Njen karakter ima vrednosti $3,1,0,-1,-1$ in s tem normo

$$\|\chi_\rho\|^2 = \frac{1}{4!}\left(1\cdot 3^2 + 6\cdot 1^2 + 6\cdot(-1)^2 + 3\cdot(-1)^2\right) = 1,$$

zato je upodobitev $\rho$ nerazcepna.

Za zdaj imamo tri nerazcepne upodobitve stopenj $1,1,3$. Iščemo torej še dve nerazcepni upodobitvi, katerih vsote kvadratov stopenj so enake $24 - (1^2+1^2+3^2) = 13$. Stopnji teh dveh neznanih upodobitev sta zato nujno enaki 2 in 3. Ker že imamo eno nerazcepno upodobitev stopnje 3, lahko iz nje pridelamo novo s tenzoriranjem z upodobitvijo stopnje 1. Dobimo upodobitev $\mathrm{sgn}\otimes\rho$. Njen karakter ima vrednosti $3,-1,0,1,-1$ in s tem normo 1, zato je upodobitev $\mathrm{sgn}\otimes\rho$ res nerazcepna. Nazadnje nam torej manjka le še ena upodobitev stopnje 2. Imenujmo jo $\tau$. Čeprav je ne poznamo, lahko iz ortonormiranosti karakterjev določimo njen karakter $\chi_\tau$ kot natanko tisto razredno funkcijo, ki je ortogonalna na vse poznane neracepne karakterje in je norme 1 ter pozitivne stopnje. Na ta način dobimo vrednosti $2,0,-1,0,2$. S tem smo nazadnje določili celotno tabelo karakterjev grupe $S_4$ nad $\mathbf{C}$.[8]

Upodobitve $\tau$ ni težko eksplicitno določiti. Vemo, da je stopnje 2. Njena vrednost $\tau((1\ 2)(3\ 4))$ je matrika v $\mathrm{GL}_2(\mathbf{C})$ reda 2 s sledjo 2. Taka matrika je lahko le identiteta. Torej je $\tau$ trivialna v

[8] Zanimivo je, da nam je uspelo določiti tabelo karakterjev, ne da bi eksplicitno poznali vse upodobitve.

konjugiranostnem razredu elementa $(1\,2)(3\,4)$ in je zato pravzaprav restrikcija upodobitve kvocientne grupe $S_4$ po edinki, generirani s tem konjugiranostnim razredom. Slednjo kvocientno grupo identificiramo kot $S_3$ prek epimorfizma

$$\psi{:}S_4 \to S_3, \quad (1\,2) \mapsto (1\,2),\ (1\,2\,3\,4) \mapsto (1\,3)$$

z jedrom $\{(), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$. Upodobitev $\tau$ torej prepoznamo kot restrikcijo dvorazsežne nerazcepne upodobitve grupe $S_3$ vzdolž homomorfizma $\psi$.

## Projekcije na izotipične komponente

Dekompozicijo regularne upodobitve smo dobili iz matričnih koeficientov nerazcepnih upodobitev, torej gre za nekakšno *notranjo* dekompozicijo. Obstaja pa tudi *zunanja* dekompozicija, pri kateri iz upodobitve same s pomočjo ustreznih projekcijskih spletičen najdemo izotipične komponente upodobitve.

Naj bo $G$ končna grupa in $F$ algebraično zaprto polje karakteristike tuje $|G|$. Naj bo $\rho$ podupodobitev regularne upodobitve $\rho_{\text{fun}}$ na prostoru $V \leq \text{fun}(G,F)$. Ta prostor lahko predstavimo kot sliko neke projekcijske spletične $\Phi \in \hom_G(\rho_{\text{fun}}, \rho)$. Res je tudi obratno, vsaka spletična $\Phi \in \hom_G(\rho_{\text{fun}}, \rho_{\text{fun}})$ podaja prek svoje slike podupodobitev regularne upodobitve. Podupodobitve so torej parametrizirane s spletičnami. Izkaže se, da te vselej izhajajo iz Fourierovih transformacij.

**Trditev 3.2.12.** *Naj bo $G$ končna grupa in $F$ algebraično zaprto polje karakteristike tuje $|G|$. Preslikava*

$$\mathcal{F}{:}\text{fun}(G,F) \to \hom_G(\rho_{\text{fun}}, \rho_{\text{fun}}), \quad f \mapsto \left(h \mapsto \hat{h}(\rho_{\text{fun}}) \cdot f\right)$$

*je izomorfizem vektorskih prostorov.*

*Dokaz.* Ni težko preveriti, da je $\mathcal{F}$ dobro definirana preslikava. Očitno je linearna. Za $f \in \text{fun}(G,F)$ je $\mathcal{F}(f) \cdot 1_1 = \widehat{1_1}(\rho_{\text{fun}}) \cdot f = f$, zato je $\mathcal{F}$ injektivna. Oba prostora sta enake razsežnosti, namreč $|G|$, zato je $\mathcal{F}$ izomorfizem. □

V posebnem je vsaka endospletična regularne upodobitve enaka evalvaciji Fourierove transformacije v neki fiksni funkciji.[9] Nekoliko natančneje si oglejmo, kaj je ta evalvacija. Za funkciji $f, h \in \text{fun}(G,F)$ je

$$\hat{h}(\rho_{\text{fun}}) \cdot f = \sum_{g \in G} h(g)\rho_{\text{fun}}(g^{-1}) \cdot f = \left(x \mapsto \sum_{g \in G} h(g) f(xg^{-1})\right).$$

Zadnjo vsoto prepoznamo kot **konvolucijo** funkcij $f$ in $h$, se pravi

$$(f * h)(x) = \sum_{g \in G} f(xg^{-1})h(g).$$

Velja torej $\hat{h}(\rho_{\text{fun}}) \cdot f = f * h$. Če dodatno predpostavimo, da je $f$ razredna funkcija, potem se ni težko prepričati, da velja $f * h = h * f$, torej je v tem primeru

$$\mathcal{F}(f) \cdot h = \hat{h}(\rho_{\text{fun}}) \cdot f = \hat{f}(\rho_{\text{fun}}) \cdot h$$

in zato preslikava $\mathcal{F}$ ni nič drugega kot običajna Fourierova transformacija razredne funkcije. V posebnem so torej Fourierove transformacije karakterjev endospletične regularne upodobitve. Izkaže se, da so te vselej tesno povezane s projekcijami na izotipične komponente.

**Trditev 3.2.13.** *Naj bo $G$ končna grupa in $F$ algebraično zaprto polje karakteristike tuje $|G|$. Za vsako končno razsežno upodobitev $\rho$ in nerazcepno upodobitev $\pi$ je*

$$\frac{\deg(\pi)}{|G|} \cdot \widehat{\chi_\pi}(\rho)$$

*projektor na $\pi$-izotipično komponento v $\rho$.*

[9] V asociativni algebri to izrečemo po navadi takole: vsak levi ideal v polenostavni algebri je glavni.

*Dokaz.* Iz leme o Fourierovi transformaciji razredne funkcije izpeljemo, da za vsaki nerazcepni upodobitvi $\pi_1$, $\pi_2$ na prostorih $V_1$, $V_2$ velja

$$\frac{\deg(\pi_1)}{|G|} \cdot \widehat{\chi_{\pi_1}}(\pi_2) = \begin{cases} \mathrm{id}_{V_2} & \pi_1 \cong \pi_2, \\ 0 & \text{sicer.} \end{cases}$$

Ko upodobitev $\rho$ razstavimo na direktno vsoto nerazcepnih podupodobitev, je linearni endomorfizem $\deg(\pi)/|G| \cdot \widehat{\chi_\pi}(\rho)$ torej ničeln na podupodobitvah, ki niso izomorfne $\pi$, in identiteta na podupodobitvah, ki so izomorfne $\pi$. Ta endomorfizem je torej projektor na direktno vsoto podupodobitev, ki so izomorfne $\pi$, torej ravno na $\pi$-izotipično komponento. □

**Zgled 3.2.14.** Naj bo $\rho_{\mathrm{fun}}$ regularna upodobitev grupe $G$. Vemo že, da za vsako funkcijo $f \in \mathrm{fun}(G,F)$ velja $\hat{f}(\rho_{\mathrm{fun}}) \cdot 1_1 = f$. Torej je projekcija funkcije $1_1$ na $\pi$-izotipično komponento enaka

$$\frac{\deg(\pi)}{|G|} \cdot \widehat{\chi_\pi}(\rho_{\mathrm{fun}}) \cdot 1_1 = \frac{\deg(\pi)}{|G|} \cdot \chi_\pi.$$

S tem dobimo razvoj

$$1_1 = \frac{1}{|G|} \sum_{\pi \in \mathrm{Irr}(G)} \chi_\pi(1) \cdot \chi_\pi,$$

ki je le poseben primer druge ortogonalnostne relacije.

Oglejmo si še karakteristično funkcijo $1_x$ za $x \in G$. Njena projekcija na $\pi$-izotipično komponento je

$$\frac{\deg(\pi)}{|G|} \cdot \widehat{\chi_\pi}(\rho_{\mathrm{fun}}) \cdot 1_x = \frac{\deg(\pi)}{|G|} \cdot \left(g \mapsto \chi_\pi(x^{-1}g)\right),$$

s čimer dobimo razvoj

$$1_x(g) = \frac{1}{|G|} \sum_{\pi \in \mathrm{Irr}(G)} \chi_\pi(1)\chi_\pi(x^{-1}g).$$

Vsako funkcijo $f \in \mathrm{fun}(G,F)$ lahko razvijemo po karakterističnih funkcijah kot $f = \sum_{x \in G} f(x)1_x$. Ker že poznamo razvoj vsake od karakterističnih funkcij po $\pi$-izotipičnih komponentah, od tod izpeljemo

$$f(g) = \frac{1}{|G|} \sum_{\pi \in \mathrm{Irr}(G)} \sum_{x \in G} f(x)\chi_\pi(1) \operatorname{tr}\left(\pi(x^{-1}) \cdot \pi(g)\right),$$

kar lahko po upoštevanju linearnosti sledi izrazimo kot

$$f(g) = \frac{1}{|G|} \sum_{\pi \in \mathrm{Irr}(G)} \chi_\pi(1) \operatorname{tr}\left(\hat{f}(\pi) \cdot \pi(g)\right).$$

Temu razvoju funkcije $f$ po $\pi$-izotipičnih komponentah rečemo **Fourierova inverzija**, saj nam eksplicitno pove, kako lahko $f$ izračunamo iz njenih Fourierovih transformacij v nerazcepnih upodobitvah.

**Zgled 3.2.15.** Naj bo $A$ končna abelova grupa. Vemo že, da so vse njene kompleksne nerazcepne upodobitve enorazsežne. V tem primeru so upodobitve kar enake svojim karakterjem. Za dano funkcijo $f \in \mathrm{fun}(A, \mathbf{C})$ lahko Fourierovo inverzijo zapišemo kot

$$f = \frac{1}{|A|} \sum_{\chi \in \mathrm{Irr}(A)} \hat{f}(\chi) \cdot \chi,$$

kar je le posledica dejstva $\hat{f}(\chi) = |A| \cdot [f, \chi]$.

## Izračunljivost tabele karakterjev

Naj bo $G$ končna grupa in $F$ algebraično zaprto polje karakteristike tuje $|G|$. Kategorijo $\mathrm{Rep}_G$ v tem primeru razumemo zelo dobro, če le poznamo tabelo karakterjev. Za zdaj smo si ogledali nekaj zgledov, kako to tabelo izračunati za posebne primere grupe. Pri tem smo si sicer res pomagali z razvito teorijo, a je bil večji del izračuna tabele opravljen z metodo ostrega pogleda. V splošnem se temu lahko izognemo; obstaja namreč več algoritmov, ki le z uporabo linearne algebre izračunajo tabelo karakterjev.

Ogledali si bomo enega takih algoritmov, ki uporablja projekcije na izotipične komponente iz zadnjega razdelka. Algoritem temelji na Fourierovi transformaciji karakteristične funkcije $1_{\mathcal{C}}$ konjugiranostnega razreda $\mathcal{C}$ grupe $G$ v regularni upodobitvi $\rho_{\mathrm{fun}}$. Po lemi o Fourierovi transformaciji razredne funkcije je namreč zožitev $\widehat{1_{\mathcal{C}}}(\rho_{\mathrm{fun}})$ na $\pi$-izotipično komponento skalarno množenje s številom

$$\frac{|G|}{\deg(\pi)} \cdot [1_{\mathcal{C}}, \chi_\pi] = |\mathcal{C}| \cdot \frac{\chi_\pi(\mathcal{C}^{-1})}{\chi_\pi(1)}.$$

Vektorji v $\pi$-izotipični komponenti so zato hkratni lastni vektorji preslikav $\widehat{1_{\mathcal{C}}}(\rho_{\mathrm{fun}})$, ko $\mathcal{C}$ preteče vse konjugiranostne razrede grupe $G$. Pokažimo, da je ta opis v resnici karakterizacija $\pi$-izotipičnih komponent.

**Lema 3.2.16.** *Naj bo $G$ končna grupa in $F$ algebraično zaprto polje karakteristike tuje $|G|$. Izotipične komponente regularne upodobitve so natanko netrivialni preseki lastnih podprostorov $\widehat{1_{\mathcal{C}}}(\rho_{\mathrm{fun}})$, ko $\mathcal{C}$ preteče vse konjugiranostne razrede grupe $G$.*

*Dokaz.* Naj bo

$$W = \bigcap_{\mathcal{C}} \mathrm{LP}_{\lambda_{\mathcal{C}}}\left(\widehat{1_{\mathcal{C}}}(\rho_{\mathrm{fun}})\right) \leq \mathrm{fun}(G,F)$$

presek lastnih podprostorov[10] za neke skalarje $\lambda_{\mathcal{C}}$, kjer presek teče po vseh konjugiranostnih razredih grupe $G$. Predpostavimo, da je $W \neq 0$. Naj bo $w \in W$. Za $\pi \in \mathrm{Irr}(G)$ naj bo $P_\pi$ projekcija na $\pi$-izotipično komponento. Velja

$$P_\pi \cdot w = \frac{\chi_\pi(1)}{|G|} \widehat{\chi_\pi}(\rho_{\mathrm{fun}}) \cdot w = \frac{\chi_\pi(1)}{|G|} \sum_{g \in G} \chi_\pi(g) \rho_{\mathrm{fun}}(g^{-1}) \cdot w.$$

Vsoto lahko razvijemo po vsakem konjugiranostnem razredu posebej in dobimo

$$\frac{\chi_\pi(1)}{|G|} \sum_{\mathcal{C}} \chi_\pi(\mathcal{C}) \sum_{g \in \mathcal{C}} \rho_{\mathrm{fun}}(g^{-1}) \cdot w = \left( \frac{\chi_\pi(1)}{|G|} \sum_{\mathcal{C}} \chi_\pi(\mathcal{C}) \lambda_{\mathcal{C}} \right) w$$

pri čemer smo v enakosti upoštevali, da je $w \in W$. Od tod sledi

$$W \leq \mathrm{LP}_{\frac{\chi_\pi(1)}{|G|} \sum_{\mathcal{C}} \chi_\pi(\mathcal{C}) \lambda_{\mathcal{C}}}(P_\pi).$$

Projektor $P_\pi$ ima seveda le dve možni lastni vrednosti: 0 in 1. Ker je po predpostavki $W \neq 0$, ne more biti za vse $\pi \in \mathrm{Irr}(G)$ projekcija na $\pi$-izotipično komponento ničelna na $W$. Torej je za nek $\pi$ nujno

$$W \leq \mathrm{LP}_1(P_\pi) = \mathrm{Izotip}_{\rho_{\mathrm{fun}}}(\pi).$$

Vemo že, kako deluje $\widehat{1_{\mathcal{C}}}(\rho_{\mathrm{fun}})$ na $\pi$-izotipični komponenti, od koder določimo skalarje kot $\lambda_{\mathcal{C}} = |\mathcal{C}| \cdot \chi_\pi(\mathcal{C}^{-1})/\chi_\pi(1)$. Iz definicije $W$ zdaj sledi, da je $\pi$-izotipična komponenta vsebovana v $W$, s čimer smo nazadnje izpeljali $W = \mathrm{Izotip}_{\rho_{\mathrm{fun}}}(\pi)$. □

S to karakterizacijo izotipičnih komponent lahko opišemo algoritem za izračun tabele karakterjev.[11] Najprej oštevilčimo elemente grupe $G$ kot $g_1, g_2, \ldots, g_{|G|}$ in pripravimo vektorski prostor $F^{|G|} \cong \mathrm{fun}(G,F)$ s standardno bazo $e_i$, ki ustreza karakteristični funkciji $1_{g_i}$. Izračunamo še konjugiranostne razrede grupe $G$ in iz vsakega izberemo predstavnika. Pripravimo funkcijo, ki izračuna matriko regularne

[10] Za endomorfizem $A$ je $\mathrm{LP}_\lambda(A)$ lastni podprostor $A$ za lastno vrednost $\lambda$.

[11] Na podoben način lahko določimo tudi upodobitve same, ne le karakterje.

| | $()$ | $(1\,2)(3\,4)$ | $(1\,2\,3)$ | $(1\,2\,3\,4\,5)$ | $(1\,2\,3\,5\,4)$ |
|---|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 5 | 1 | $-1$ | 0 | 0 |
| $\chi_3$ | 4 | 0 | 1 | $-1$ | $-1$ |
| $\chi_4$ | 3 | $-1$ | 0 | $-\zeta^2-\zeta^3$ | $-\zeta-\zeta^4$ |
| $\chi_5$ | 3 | $-1$ | 0 | $-\zeta-\zeta^4$ | $-\zeta^2-\zeta^3$ |

Tabela 3.3: Tabela karakterjev $A_5$, kjer je $\zeta = e^{2\pi i/5}$

upodobitve $\rho_{\text{fun}}$ v poljubnem elementu $x \in G$, in za tem še funkcijo, ki izračuna matriko Fourierove transformacije $\widehat{1_{\mathcal{C}}}(\rho_{\text{fun}})$ za konjugiranostni razred $\mathcal{C}$. Izračunamo lastne podprostore vseh teh matrik in za tem vse njihove netrivialne preseke. Te so ravno izotipične komponente. V vsaki komponenti $W$ izberemo bazo, v kateri izračunamo sled zožitve matrike $\rho_{\text{fun}}(x)$ na $W$. Ker je $W$ kot upodobitev izomorfen direktni vsoti $\deg(\pi)$ kopij neke nerazcepne upodobitve $\pi$, velja $\dim(W) = \deg(\pi)^2$ in zato

$$\operatorname{tr}(\rho_{\text{fun}}(x)|_W) = \sqrt{\dim(W)} \cdot \chi_\pi(x).$$

Iz izračunane sledi torej lahko določimo vrednost pripadajočega karakterja v predstavnikih konjugiranostnih razredov. Implementacija predstavljenega algoritma za izračun tabele karakterjev nad $\mathbf{C}$ v programskem jeziku GAP[12] je dostopna tukaj.

**Zgled 3.2.17.** Opazujmo alternirajočo grupo $A_5$ nad poljem $\mathbf{C}$. Z opisanim algoritmom hitro izračunamo njeno tabelo karakterjev.

Iz tabele lahko razberemo kar nekaj lastnosti grupe. Oglejmo si, kako hitro premislimo, da je $A_5$ *enostavna* grupa. Če bi namreč $A_5$ imela kakšno pravo netrivialno edinko $N$, potem bi kvocient $A_5/N$ imel kakšno netrivialno nerazcepno upodobitev $\rho$. Restrikcija $\operatorname{Res}^{A_5/N}_{A_5}(\rho)$ je zato netrivialna nerazcepna upodobitev grupe $A_5$ z netrivialnim jedrom. Vrednost karakterja $\chi_\rho$ v poljubnem elementu $N$ je torej enaka $\chi_\rho(1)$. Iz tabele karakterjev grupe $A_5$ pa je jasno, da takega karakterja ni.[13]

Predstavljeni algoritem ima številne pomanjkljivosti. V programskem jeziku GAP je za izračun tabele karakterjev implementiran algoritem (Dixon 1967, Schneider 1990), ki izboljša predstavljenega na naslednja dva načina.

1. S predstavljenim algoritmom bomo težko izračunali tabelo karakterjev kakšne zelo velike grupe, saj moramo v postopku diagonalizirati matrike velikosti $|G| \times |G|$. Algoritem v GAP sicer temelji na enaki ideji iskanja skupnih lastnih podprostorov, a pri tem ne opazuje regularne upodobitve, temveč upošteva abstraktne formule med karakterji in iz njih izpelje matrike velikosti $\mathrm{k}(G) \times \mathrm{k}(G)$, katerih skupni lastni vektorji so (bolj ali manj) karakterji. Ker je število $\mathrm{k}(G)$ bistveno manjše od $|G|$, je ta izračun veliko lažji in hitrejši.

2. Za izračun natančnih vrednosti karakterjev moramo vse račune izvajati eksaktno in brez približkov. Numerične metode, ki jih sicer lahko uporabimo za hitro računanje lastnih vrednosti velikih matrik, torej odpadejo. Programski jezik GAP zna računati simbolično, a je to lahko precej zamudno. Algoritem v GAP se temu izogne tako, da večino računov opravi nad poljem $\mathbf{F}_p$ za ustrezno izbrano dovolj veliko praštevilo $p$, potem pa te rezultate prenese nazaj nad $\mathbf{C}$. Vsi računi so zato hitri in eksaktni.

## Kolobar virtualnih karakterjev

Pogosto nas ne zanima le računski aspekt upodobitev, temveč konceptualno razumevanje, od kod prihajajo nerazcepne upodobitve dane grupe. Kot bomo videli, ima tukaj glavno vlogo indukcija.

[12] GAP je programski jezik, ki pride zelo prav pri delu z grupami, saj ima implementiranih veliko standardnih konstrukcij grup in funkcij za delo z njimi. Dostopen je prosto na naslovu https://www.gap-system.org. Osnovna načela za delo z upodobitvami končnih grup lahko najdeš v Moravčevi skripti.

[13] Iz argumenta vidimo, da velja celo naslednje. Končna grupa $G$ je enostavna, če in samo če je vsaka njena netrivialna nerazcepna upodobitev zvesta.

Naj bo $G$ grupa in $F$ polje karakteristike tuje $|G|$. Karakterji upodobitev grupe $G$ so celoštevilske kombinacije nerazcepnih karakterjev. Tvorimo množico vseh takih kombinacij, se pravi

$$R(G) = \bigoplus_{\pi \in \mathrm{Irr}(G)} \mathbf{Z} \cdot \chi_\pi \subseteq \mathrm{fun}_{\mathrm{cl}}(G,F).$$

Množica $R(G)$ je najprej očitno abelova podgrupa razrednih funkcij. Za tem je opremljena z množenjem, ki izhaja iz tenzorskega produkta upodobitev. Množica $R(G)$ na ta način postane komutativen podkolobar v $\mathrm{fun}_{\mathrm{cl}}(G,F)$, ki ga imenujemo **kolobar virtualnih karakterjev**.[14]

Naj bo $H$ podgrupa v $G$. Restrikcija vzdolž vložitve $H$ v $G$ porodi *homomorfizem kolobarjev*

$$\mathrm{Res}: R(G) \to R(H), \quad \chi_\pi \mapsto \chi_{\mathrm{Res}^G_H(\pi)}.$$

Sorodno dobimo z indukcijo preslikavo

$$\mathrm{Ind}: R(H) \to R(G), \quad \chi_\pi \mapsto \chi_{\mathrm{Ind}^G_H(\pi)},$$

ki pa je le *homomorfizem abelovih grup*. Ob koncu razdelka o indukciji smo za upodobitvi $\rho$ v $\mathrm{Rep}_G$ in $\sigma$ v $\mathrm{Rep}_H$ zapisali izomorfizem

$$\mathrm{Ind}^G_H(\mathrm{Res}^G_H(\rho) \otimes \sigma) \cong \rho \otimes \mathrm{Ind}^G_H(\sigma),$$

ki ga zdaj lahko interpretiramo s karakterji teh upodobitev in sklenemo, da je slika $\mathrm{Ind}(R(H))$ *ideal* v $R(G)$.

**Zgled 3.2.18.** Naj bo $H$ ciklična grupa. Definirajmo indikatorsko funkcijo generatorjev grupe $H$ kot

$$c_H: H \to F, \quad h \mapsto \begin{cases} |H| & \langle h \rangle = H, \\ 0 & \text{sicer.} \end{cases}$$

Ker je $H$ abelova grupa, je seveda $c_H \in \mathrm{fun}_{\mathrm{cl}}(H,F)$.

Premislimo, da velja celo $c_H \in R(H)$. Dokazujmo z indukcijo na $|H|$. Vsaka prava podgrupa $K \leq H$ je tudi ciklična, zato zanjo po indukcijski predpostavki velja $c_K \in R(K)$. Naj bo $R$ množica predstavnikov odsekov $K$ v $H$. S formulo za indukcijo karakterja za $h \in H$ izračunamo

$$\mathrm{Ind}^H_K(c_K)(h) = \sum_{r \in R : h \in K} c_K(h) = \begin{cases} |H:K| c_K(h) & h \in K, \\ 0 & \text{sicer} \end{cases} = \begin{cases} |H| & \langle h \rangle = K, \\ 0 & \text{sicer.} \end{cases}$$

Vsak element $h \in H$ generira neko podgrupo $H$, bodisi pravo bodisi kar $H$. Torej lahko zapišemo

$$c_H = |H| - \sum_{K < H} \mathrm{Ind}^H_K(c_K).$$

Konstanta $|H|$ je karakter trivialne upodobitve $\mathbf{1}^{|H|}$ grupe $H$, torej iz zadnje enakosti sledi želeno $c_H \in R(H)$.

Naj bo $C$ množica vseh cikličnih pogrup grupe $G$ in izberimo $H \in C$. Naj bo $R$ množica predstavnikov desnih odsekov $H$ v $G$. Zadnji zgled nam pove $c_H \in R(H)$. Ta virtualni karakter lahko induciramo na grupo $G$ in za $g \in G$ dobimo

$$\mathrm{Ind}^G_H(c_H)(g) = \sum_{r \in R : rgr^{-1} \in H} c_H(rgr^{-1}) = \sum_{r \in R : \langle rgr^{-1} \rangle = H} |H| = \sum_{x \in G : \langle xgx^{-1} \rangle = H} 1.$$

Ko torej seštejemo prispevke po vseh cikličnih podgrupah, dobimo

$$\sum_{H \in C} \mathrm{Ind}^G_H(c_H)(g) = \sum_{x \in G} \sum_{H \in C} 1_{\langle xgx^{-1} \rangle = H} = \sum_{x \in G} 1 = |G|.$$

[14] Virtualnih, ker vsebuje tudi negativne kombinacije nerazcepnih kolobarjev, ki ne ustrezajo karakterjem upodobitev.

Konstantna funkcija $|G|$ je torej element ideala $\sum_{H\in C} \mathrm{Ind}(R(H))$ v $R(G)$. Od tod seveda sledi vsebovanost

$$|G|\cdot R(G) \leq \sum_{H\in C} \mathrm{Ind}(R(H)).$$

Vsak virtualni karakter v $R(G)$ je zato linearna kombinacija induciranih virtualnih karakterjev cikličnih podgrup, pri čemer so koeficienti racionalna števila z imenovalcem kvečjemu $|G|$. Povzemimo to presenetljivo ugotovitev.

**Izrek 3.2.19** (Artinov izrek)**.** *Naj bo $G$ končna grupa in $\rho$ njena končno razsežna upodobitev nad poljem karakteristike tuje $|G|$. Tedaj je $\chi_\rho$* racionalna *linearna kombinacija indukcij nerazcepnih karakterjev cikličnih podgrup grupe $G$.*

Racionalnim kombinacijam se lahko izognemo, če razširimo razred podgrup. Namesto cikličnih podgrup opazujemo **$p$-elementarne podgrupe** grupe $G$. To so podgrupe, ki so izomorfne direktnemu produktu ciklične grupe in $p$-grupe.

**Izrek 3.2.20** (Brauerjev izrek)**.** *Naj bo $G$ končna grupa in $\rho$ njena končno razsežna upodobitev nad algebraično zaprtim poljem karakteristike* 0*. Tedaj je $\chi_\rho$* celoštevilska *linearna kombinacija indukcij nerazcepnih karakterjev $p$-elementarnih podgrup grupe $G$, ko $p$ preteče vse praštevilske delitelje moči $G$.*

Dokaz Brauerjevega izreka je nekoliko bolj zapleten kot preprost argument, ki nas je pripeljal do Artinovega izreka. Bralec ga lahko najde v (Serre 1977).

Ne spreglejmo ključne lekcije tega razdelka: nerazcepne upodobitve dane končne grupe iščemo s pomočjo indukcije iz preprostih podgrup.

## Kompleksne upodobitve

Splošno teorijo upodobitev končnih grup zaključimo z upodobitvami nad najugodnejšim poljem $\mathbf{C}$. To polje je daleč od abstraktnega in je opremljeno z mnogo dodatne strukture, ki jo lahko izkoristimo pri upodobitvah.

### Vrednosti karakterjev

Najprej si oglejmo nekaj dodatnih lastnosti, ki jih imajo karakterji kompleksnih upodobitev. Njihove vrednosti namreč niso čisto poljubna kompleksna števila, temveč so algebraična cela števila[15] omejene absolutne vrednosti.

**Trditev 3.2.21.** *Naj bo $G$ končna grupa. Za vsako končno razsežno kompleksno upodobitev $\rho$ in vsak $g \in G$ je*

$$|\chi_\rho(g)| \leq \deg(\rho), \quad \chi_\rho(g) \in \bar{\mathbf{Z}}, \quad \chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}.$$

*Dokaz.* Velja $\rho(g^{|G|}) = \rho(1) = \mathrm{id}$, zato je $\rho(g)$ linearna preslikava končnega reda. Take preslikave so diagonalizabilne.[16] Naj bo $\mathrm{Spec}(\rho(g)) \subseteq \mathbf{C}^*$ množica lastnih vrednosti $\rho(g)$. Vsaka lastna vrednost $\lambda \in \mathrm{Spec}(\rho(g))$ je končnega reda v $\mathbf{C}^*$. S tem je seveda

$$\chi_\rho(g) = \sum_{\lambda\in\mathrm{Spec}(\rho(g))} \lambda \in \bar{\mathbf{Z}}, \quad |\chi_\rho(g)| \leq \sum_{\lambda\in\mathrm{Spec}(\rho(g))} |\lambda| = \deg(\rho)$$

in hkrati

$$\chi_\rho(g^{-1}) = \sum_{\lambda\in\mathrm{Spec}(\rho(g))} \lambda^{-1} = \sum_{\lambda\in\mathrm{Spec}(\rho(g))} \overline{\lambda} = \overline{\chi_\rho(g)}.$$

□

[15] **Algebraično celo število** je kompleksno število, ki je ničla moničnega polinoma s celoštevilskimi koeficienti. Množico algebraičnih celih števil označimo z $\bar{\mathbf{Z}}$. Ni se težko prepričati, da $\bar{\mathbf{Z}}$ tvori kolobar in da velja $\mathbf{Q}\cap\bar{\mathbf{Z}} = \mathbf{Z}$.

[16] Diagonalizabilnost sledi iz obravnave Jordanove normalne forme preslikave $\rho(g)$.

S pomočjo te restriktivne lastnosti vrednosti karakterjev lahko izpeljemo pomembno lastnost stopenj nerazcepnih kompleksnih upodobitev.

**Izrek 3.2.22** (o stopnjah upodobitev)**.** *Stopnja vsake nerazcepne kompleksne upodobitve končne grupe deli moč grupe.*

Dokaz bomo navezali na edino mesto, kjer smo že videli ulomek $|G|/\deg(\pi)$, in sicer je to lema o Fourierovi transformaciji razredne funkcije. Ko funkcija, vzdolž katere izvedemo transformacijo, slika v kolobar algebraičnih celih števil, lahko lemo o Fourierovi transformaciji razredne funkcije zaostrimo na naslednji način.

**Lema 3.2.23.** *Naj bo $G$ končna grupa. Za vsako funkcijo $f \in \mathrm{fun}_{\mathrm{cl}}(G, \bar{\mathbf{Z}})$ in nerazcepno kompleksno upodobitev $\pi$ je $\hat{f}(\pi)$ skalarno množenje z algebraičnim celim številom.*

*Dokaz.* Vemo že, da je $\hat{f}(\pi)$ skalarno množenje s številom

$$\frac{|G|}{\deg(\pi)} \cdot [f, \chi_\pi].$$

Preveriti moramo torej, da je to algebraično celo število. Funkcijo $f$ lahko razvijemo kot vsoto karakterističnih funkcij konjugiranostnih razredov s koeficienti v $\bar{\mathbf{Z}}$. Ker $\bar{\mathbf{Z}}$ tvori kolobar, bo torej trditev dovolj preveriti za primer, ko je $f = 1_{\mathcal{C}}$ za nek konjugiranostni razred $\mathcal{C}$ v $G$.

Vse nerazcepne upodobitve lahko obravnavamo v enem zamahu, in sicer tako, da opazujemo regularno upodobitev in s tem linearno preslikavo $\widehat{1_{\mathcal{C}}}(\rho_{\mathrm{fun}})$. Na vsaki od podupodobitev, ki je izomorfna $\pi$, ta preslikava deluje kot $\widehat{1_{\mathcal{C}}}(\pi)$, torej kot skalarno množenje z gornjim številom. To število je zato lastna vrednost preslikave $\widehat{1_{\mathcal{C}}}(\rho_{\mathrm{fun}})$.

Vemo že, da $\widehat{1_{\mathcal{C}}}(\rho_{\mathrm{fun}})$ deluje na naravni bazi iz karakterističnih funkcij $1_x$ za $x \in G$ kot

$$\widehat{1_{\mathcal{C}}}(\rho_{\mathrm{fun}}) \cdot 1_x = \sum_{g \in G} 1_{\mathcal{C}}(x^{-1}g) 1_g \in \mathrm{fun}(G, \{0,1\}).$$

V tej bazi ima torej $\widehat{1_{\mathcal{C}}}(\rho_{\mathrm{fun}})$ matriko s koeficienti v množici $\{0,1\}$. Karakteristični polinom te matrike ima zato celoštevilske koeficiente, torej so lastne vrednosti preslikave $\widehat{1_{\mathcal{C}}}(\rho_{\mathrm{fun}})$ algebraična cela števila. □

*Dokaz.* (dokaz izreka o stopnjah upodobitev) Naj bo $\pi \in \mathrm{Irr}(G)$. Uporabimo lemo s funkcijo $f = \chi_\pi$, ki nam pove, da je

$$\frac{|G|}{\deg(\pi)} \cdot [\chi_\pi, \chi_\pi] = \frac{|G|}{\deg(\pi)} \in \bar{\mathbf{Z}}.$$

Ker je zadnje število hkrati v $\mathbf{Q}$, je torej v $\mathbf{Q} \cap \bar{\mathbf{Z}} = \mathbf{Z}$. □

### Skalarni produkti in unitarnost

Polje $\mathbf{C}$ je opremljeno s standardnim skalarnim produktom $\langle z, w \rangle = z \cdot \overline{w}$. Ta produkt lahko razširimo na vsak končno razsežen kompleksen vektorski prostor. Obravnavali bomo dve taki razširitvi, in sicer na prostor funkcij $\mathrm{fun}(G, \mathbf{C})$ ter na vektorski prostor, na katerem upodabljamo grupo $G$.

Opazujmo najprej prostor funkcij $\mathrm{fun}(G, \mathbf{C})$. Vemo že, da ga lahko opremimo s skalarnim produktom $[\cdot, \cdot]$. Ker pa je ta prostor kompleksen, lahko nanj vpeljemo še **standarden kompleksni skalarni produkt**,

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

za $f, h \in \mathrm{fun}(G, \mathbf{C})$. Za vsako končno razsežno kompleksno upodobitev $\rho$ po zadnji trditvi velja

$$[f, \chi_\rho] = \langle f, \chi_\rho \rangle,$$

zato se večina rezultatov, ki smo jih izpeljali za skalarni produkt $[\cdot, \cdot]$, prenese na skalarni produkt $\langle \cdot, \cdot \rangle$. V posebnem karakterji še vedno tvorijo ortonormiran sistem vektorjev v $\mathrm{fun}(G, \mathbf{C})$ in koeficienti razvoja razrednih funkcij po karakterjih se ne spremenijo.

**Domača naloga 3.2.24.** Oglejmo si še eno uporabo restriktivnih vrednosti kompleksnih karakterjev. Naj bo $G$ končna grupa in $\rho$ njena poljubna *zvesta* končno razsežna kompleksna upodobitev. Tedaj obstaja $N$, tako da je vsaka nerazcepna kompleksna upodobitev grupe $G$ podupodobitev $\rho^{\otimes N}$.

Dokaza se lahko lotiš tako, da fiksiraš nerazcepno upodobitev $\pi \in \mathrm{Irr}(G)$ in opazuješ *rodovno funkcijo* večkratnosti, se pravi formalno vsoto $F(X) = \sum_{k=0}^{\infty} \mathrm{mult}_{\rho^{\otimes k}}(\pi) X^k$. Dovolj bo premisliti, da je ta rodovna funkcija neničelna. Izrazi vsak koeficient $\mathrm{mult}_{\rho^{\otimes k}}(\pi)$ s pomočjo skalarnega produkta in se na ta način prepričaj, da ima $F(X)$ pol pri $X = 1/\deg \rho$, zato je res neničelna.

Osredotočimo se sedaj še na upodobitveni prostor. Naj bo $\rho$ kompleksna upodobitev grupe $G$ na končno razsežnem prostoru $V$. Izberimo bazo prostora $\{v_i\}_i$ in z njo kompleksen skalarni produkt

$$\left\langle \sum_i \alpha_i v_i, \sum_i \beta_i v_i \right\rangle = \sum_i \alpha_i \overline{\beta_i}.$$

Prostor $V$ je opremljen z linearnim delovanjem grupe $G$. Zdaj smo na ta prostor dodali strukturo skalarnega produkta in ni jasno, ali je grupa $G$ kompatibilna s to dodatno strukturo. Kadar je tako, se pravi

$$\forall g \in G.\ \forall v, w \in V.\quad \langle \rho(g) \cdot v, \rho(g) \cdot w \rangle = \langle v, w \rangle,$$

tedaj rečemo, da je $\rho$ **unitarna upodobitev**. V tem primeru $\rho$ slika iz $G$ v grupo unitarnih transformacij $\mathrm{U}(V)$ prostora $V$ s skalarnim produktom $\langle \cdot, \cdot \rangle$. Seveda ni vsaka upodobitev končne grupe unitarna,[17] je pa vsaka upodobitev *unitarizabilna*.

**Trditev 3.2.25.** *Naj bo $G$ končna grupa in $\rho$ njena končno razsežna kompleksna upodobitev na prostoru $V$. Tedaj na $V$ obstaja skalarni produkt, glede na katerega je $\rho$ unitarna.*

*Dokaz.* Izberimo poljuben skalarni produkt $\langle \cdot, \cdot \rangle$ na $V$ in ga povprečimo do

$$\langle \cdot, \cdot \rangle_0 \colon V \times V \to \mathbf{C}, \quad \langle v, w \rangle_0 = \frac{1}{|G|} \sum_{g \in G} \langle \rho(g) \cdot v, \rho(g) \cdot w \rangle.$$

Ni težko preveriti, da je $\langle \cdot, \cdot \rangle_0$ skalarni produkt na $V$, glede na katerega je $\rho$ unitarna upodobitev. □

V kontekstu kompleksnih upodobitev končnih grup lahko torej brez škode predpostavimo, da je prostor opremljen s skalarnim produktom, glede na katerega je dana upodobitev unitarna.

**Zgled 3.2.26.** Končna grupa deluje z regularno upodobitvijo $\rho_{\mathrm{fun}}$ na prostoru funkcij $\mathrm{fun}(G, \mathbf{C})$. Ta prostor je opremljen s standardnim kompleksnim skalarnim produktom. Glede na ta skalarni produkt je $\rho_{\mathrm{fun}}$ unitarna upodobitev, saj za vsaka $f, h \in \mathrm{fun}(G, \mathbf{C})$ in $x \in G$ velja

$$\langle \rho_{\mathrm{fun}}(x) \cdot f, \rho_{\mathrm{fun}}(x) \cdot h \rangle = \frac{1}{|G|} \sum_{g \in G} f(gx) \overline{h(gx)} = \langle f, h \rangle.$$

Unitarnost upodobitev končne grupe $G$ lahko izkoristimo pri Fourierovi transformaciji. Za unitarno upodobitev $\rho$ je namreč $\rho(g^{-1}) = \rho(g)^*$ za vsak $g \in G$ in s tem

$$\hat{f}(\rho) = \sum_{g \in G} f(g) \rho(g)^*.$$

Opremljeni s tem komentarjem se obrnimo k Fourierovi inverziji. Formula za razvoj funkcije $f \in \mathrm{fun}(G, \mathbf{C})$ po $\pi$-izotipičnih komponentah je nekoliko asimetrična. To lahko popravimo tako, da jo uteženo povprečimo z neko drugo funkcijo $h \in \mathrm{fun}(G, \mathbf{C})$. Dobimo

$$\sum_{g \in G} f(g) \overline{h(g)} = \frac{1}{|G|} \sum_{\pi \in \mathrm{Irr}(G)} \sum_{g \in G} \overline{h(g)} \chi_\pi(1) \operatorname{tr}\left(\hat{f}(\pi) \cdot \pi(g)\right),$$

[17] Skalarni produkt na danem prostoru lahko izberemo na veliko različnih načinov.

kar lahko po upoštevanju linearnosti sledi in gornjega komentarja glede unitarnosti upodobitve $\pi$ zapišemo kot

$$\langle f,h\rangle = \frac{1}{|G|^2}\sum_{\pi\in\mathrm{Irr}(G)}\chi_\pi(1)\,\mathrm{tr}(\hat{f}(\pi)\cdot\hat{h}(\pi)^*).$$

Tej enakosti rečemo **Parsevalov izrek**. Nekoliko pregledneje ga lahko zapišemo z uporabo še enega skalarnega produkta, tokrat na prostoru endomorfizmov danega vektorskega prostora $V$. Za linearni preslikavi $A,B\in\hom(V,V)$ definiramo

$$\langle A,B\rangle_{\mathrm{HS}} = \mathrm{tr}(A\cdot B^*),$$

to je **Hilbert-Schmidtov skalarni produkt**. Parsevalov izrek nam torej povezuje standarden kompleksni skalarni produkt funkcij s Hilbert-Schmidtovim skalarnim produktom Fourierovih transformacij v nerazcepnih upodobitvah,

$$\langle f,h\rangle = \frac{1}{|G|^2}\sum_{\pi\in\mathrm{Irr}(G)}\chi_\pi(1)\left\langle\hat{f}(\pi),\hat{h}(\pi)\right\rangle_{\mathrm{HS}}.$$

# Poglavje 4

# Razširjeni zgledi – končni

Kategorijo upodobitev dane končne grupe nad ugodnim poljem razumemo, če imamo na voljo tabelo karakterjev, izračun te pa je končen problem. S tem smo za konkretne končne grupe dosegli ultimativen cilj teorije upodobitev. Biti pa moramo previdni, da zaradi vseh teh čudovitih dreves ne spregledamo gozda. Grupe namreč praviloma ne nastopajo posamično, temveč kot del večjih družin.[1] V tem poglavju si bomo podrobneje ogledali dve temeljni družini grup, in sicer simetrične grupe ter splošne linearne grupe nad končnim poljem.[2] Njuno teorijo upodobitev bomo obravnavali celostno.

## 4.1 Simetrične grupe

Opazujmo simetrično grupo $S_n$ za $n \in \mathbf{N}$ nad poljem $\mathbf{C}$. Ogledali smo si že tabele karakterjev za $n \leq 4$ in razložili, da je število nerazcepnih upodobitev enako številu konjugiranostnih razredov, to pa je enako številu razčlenitev $p(n)$. Družina simetričnih grup je posebna, saj zanjo presenetljivo obstaja eksplicitna korespondenca med konjugiranostnimi razredi in nerazcepnimi upodobitvami. Iz dane razčlenitve $(\lambda_1, \lambda_2, \ldots, \lambda_k)$ števila $n$ lahko torej konstruiramo nerazcepno upodobitev grupe $S_n$ in za tem z nekoliko več truda določimo vrednosti karakterjev.

### Nerazcepne upodobitve

Naj bo $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$ razčlenitev $n$. Nerazcepno upodobitev grupe $S_n$, prirejeno $\lambda$, kot po navadi iščemo z indukcijo iz podgrup. Razčlenitev $\lambda$ lahko interpretiramo kot ciklični tip permutacij, zato se naravno ponuja **Youngova grupa**

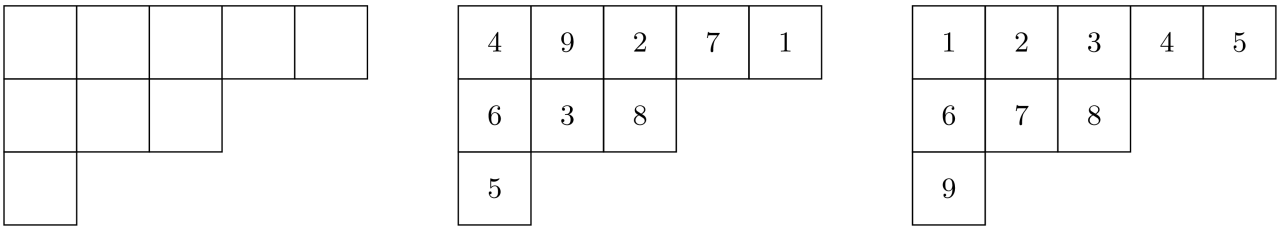
$$P = S_{\lambda_1} \times S_{\lambda_2} \times \cdots \times S_{\lambda_k}.$$

Razčlenitev $\lambda$ si lahko predstavljamo kot zaporedje vrstic diagrama, v katerem je $\lambda_1$ škatlic v 1. vrstici, $\lambda_2$ škatlic v 2. vrstici, …, $\lambda_k$ škatlic v $k$. vrstici. Pri tem so vrstice poravnane na levo. Takemu shematičnemu prikazu razčlenitve pravimo **Youngov diagram**. Diagram ima $n$ škatlic, v katere poljubno vpišemo števila od 1 do $n$. Tako izpolnjenemu diagramu pravimo **Youngova tabela**. Vsaka Youngova tabela nam pravzaprav ponuja vložitev grupe $P$ v $S_n$. Fiksirajmo standardno vložitev, ki ustreza temu, da v škatlice vpišemo po vrsti števila od 1 do $n$, začenši zgoraj levo in hodeč po 1. vrstici, nato po 2. vrstici in tako naprej. Grupa $P$, standardno vložena v $S_n$, predstavlja ravno vse permutacije, ki ohranjajo *vrstice* tabele.

Inducirajmo trivialno upodobitev iz $P$ na $S_n$. V razdelku o indukciji smo spoznali, da lahko $\mathrm{Ind}_P^{S_n}(\mathbf{1})$ interpretiramo kot permutacijsko upodobitev $S_n$ na desnih odsekih podgrupe $P$. To interpretacijo lahko vložimo v prostor funkcij $\mathrm{fun}(S_n, \mathbf{C})$. Namesto množice $P$ lahko namreč opazujemo indikatorsko funkcijo

[1] Na primer abelove grupe, simetrične grupe, diedrske grupe, splošne linearne grupe, končne enostavne grupe …

[2] Vsaka končna grupa je zgrajena iz končnih enostavnih grup, te pa sestojijo iz, grobo rečeno, treh neskončnih družin, in sicer cikličnih grup praštevilske moči $\mathbf{Z}/p\mathbf{Z}$, alternirajočih grup $A_n$ in različnih matričnih grup nad končnimi polji, na primer $\mathrm{SL}_n(\mathbf{F}_p)/Z(\mathrm{SL}_n(\mathbf{F}_p))$. Zgleda družin, ki si jih bomo ogledali, sta torej do neke mere reprezentativna za razumevanje upodobitev nekomutativnih končnih enostavnih grup. Podrobnejši opis končnih enostavnih grup je na voljo tukaj.




Slika 4.1: Youngov diagram razčlenitve $\lambda = (5,3,1)$ in dve Youngovi tabeli. Druga tabela je standardna.

$1_P$. Element $g \in S_n$ na njej deluje kot $\rho_{\text{fun}}(g) \cdot 1_P = 1_{Pg^{-1}}$, se pravi kot permutacija desnih odsekov. Na ta način upodobitveni prostor upodobitve $\text{Ind}_P^{S_n}(\mathbf{1})$ vidimo kot

$$\langle \rho_{\text{fun}}(g) \cdot 1_P \mid g \in S_n \rangle.$$

Ta prostor lahko izrazimo s pomočjo Fourierove transformacije kot

$$\langle \hat{f}(\rho_{\text{fun}}) \cdot 1_P \mid f \in \text{fun}(S_n, \mathbf{C}) \rangle = \text{im}\, \mathcal{F}(1_P) = \langle 1_P * f \mid f \in \text{fun}(S_n, \mathbf{C}) \rangle.$$

Upodobitev $S_n$ na tem prostoru gotovo *ni* nerazcepna, saj na primer vsebuje trivialno z večkratnostjo $\langle \chi_{\mathbf{1}}, \text{Ind}_P^{S_n}(\chi_{\mathbf{1}}) \rangle = \langle \chi_{\mathbf{1}}, \chi_{\mathbf{1}} \rangle = 1$. Ta prostor bomo zato še dodatno projicirali na neki podprostor.

Do zdaj smo upoštevali le grupo $P$ permutacij, ki ohranjajo *vrstice* izbrane Youngove tabele. Iz tega gledišča je naravno, da obravnavamo tudi grupo permutacij, ki ohranjajo *stolpce* tabele. Označimo jo s $Q$. Ravno ta podgrupa je dodatek, ki nam bo dodatno reduciral zgoraj opisano inducirano upodobitev. Pri tem bomo upoštevali, da je $Q$ sestavljena dualno $P$, zato jo bomo utežili s predznačno upodobitvijo sgn.

Definirajmo funkcijo

$$\sigma_\lambda = (\text{sgn} \cdot 1_Q) * 1_P \in \text{fun}(S_n, \mathbf{C}),$$

ki ji pravimo **Youngov simetrizator**. Njene vrednosti so

$$\sigma_\lambda(x) = \sum_{p \in P, q \in Q : qp = x} \text{sgn}(q).$$

Ker velja $P \cap Q = 1$, ima vsak element $x \in S_n$ *kvečjemu en* zapis v obliki $x = qp$ za $p \in P, q \in Q$,[3] torej ima zadnja vsota kvečjemu en neničeln člen in je torej enaka karakteristični funkciji množice $QP = \{qp \mid q \in Q, p \in P\}$, uteženi s predznakom člena v $Q$.

Vzdolž Youngovega simetrizatorja dobimo endospletično $\mathcal{F}(\sigma_\lambda)$ regularne upodobitve, katere slika je vektorski prostor

$$V_\lambda = \text{im}\, \mathcal{F}(\sigma_\lambda) = \langle \sigma_\lambda * f \mid f \in \text{fun}(S_n, \mathbf{C}) \rangle,$$

ki ga imenujemo **Spechtov modul**. Na tem prostoru naravno deluje grupa $S_n$[4], dobljeno upodobitev označimo z $\rho_\lambda$. Velja $V_\lambda \neq 0$, saj je $\sigma_\lambda = \sigma_\lambda * 1_1 \in V_\lambda$.

**Izrek 4.1.1.** *(o nerazcepnih upodobitvah simetrične grupe)*

1. *Za vsako razčlenitev $\lambda$ je $\rho_\lambda$ nerazcepna.*
2. *Za različni razčlenitvi $\lambda, \mu$ je $\rho_\lambda \not\cong \rho_\mu$.*
3. *Vsaka nerazcepna upodobitev simetrične grupe je izomorfna $\rho_\lambda$ za neko razčlenitev $\lambda$.*

Zadnja točka seveda sledi iz prvih dveh, saj je število nerazcepnih upodobitev ravno enako številu razčlenitev $n$. Pred dokazom izreka si oglejmo nekaj zgledov.

**Zgled 4.1.2.**

[3] Res, če je $x = q_1 p_1 = q_2 p_2$, potem je $q_2^{-1} q_1 = p_2 p_1^{-1} \in P \cap Q = 1$, zato je $q_1 = q_2$ in $p_1 = p_2$.

[4] Ker je $\mathcal{F}(\sigma_\lambda)$ spletična, je to res invarianten podprostor. Ni pa težko videti, kako elementi grupe zares delujejo; za $g \in S_n$ element $\rho_{\text{fun}}(g)$ preslika $\sigma_\lambda * f$ v $\sigma_\lambda * (\rho_{\text{fun}}(g) \cdot f)$.

- Naj bo $\lambda = (n)$. Tedaj je $P = S_n$ in $Q = 1$, zato je $\sigma_\lambda = 1$. Za funkcijo $f \in \mathrm{fun}(S_n, \mathbf{C})$ je $\mathcal{F}(1) \cdot f = 1 * f = |G| \cdot \mathbf{E}(f)$ in grupa $S_n$ deluje trivialno na tej funkciji. S tem je

$$V_\lambda = \mathrm{im}\,\mathcal{F}(1) = \mathbf{C}$$

in dobimo trivialno upodobitev.

- Naj bo $\lambda = (1,1,\ldots,1)$. Tedaj je $P = 1$ in $Q = S_n$, zato je $\sigma_\lambda = \mathrm{sgn}$. Za funkcijo $f \in \mathrm{fun}(S_n, \mathbf{C})$ je

$$\mathcal{F}(\mathrm{sgn}) \cdot f = \mathrm{sgn} * f = \left( x \mapsto \sum_{g \in G} \mathrm{sgn}(xg^{-1}) f(g) \right) = (\mathrm{sgn} * f)(1) \cdot \mathrm{sgn},$$

zato je

$$V_\lambda = \mathrm{im}\,\mathcal{F}(\mathrm{sgn}) = \langle \mathrm{sgn} \rangle.$$

Na funkciji sgn grupa $S_n$ deluje kot $\rho_{\mathrm{fun}}(g) \cdot \mathrm{sgn} = \mathrm{sgn}(g) \cdot \mathrm{sgn}$, torej je $\rho_\lambda$ predznačna upodobitev.

- Naj bo $\lambda = (n-1,1)$. Tedaj je $P = S_{n-1}$ in $Q = \{(), (1\ n)\}$. Za funkcijo $f \in \mathrm{fun}(S_n, \mathbf{C})$ velja najprej

$$(1_P * f)(x) = \sum_{p \in P} f(p^{-1}x) = \sum_{g \in Px} f(g),$$

torej $1_P * f$ izračuna vsoto funkcije $f$ po odseku $Px$. Prostor $\mathrm{im}\,\mathcal{F}(1_P)$ lahko zato identificiramo s podprostorom funkcij $\mathrm{fun}_{P\backslash S_n}(S_n, \mathbf{C})$, ki so konstantne na desnih odsekih $P\backslash S_n$. Delovanje $S_n$ na tem prostoru ni nič drugega kot $\mathrm{Ind}_P^{S_n}(\mathbf{1})$, kar prepoznamo kot standardno permutacijsko upodobitev grupe $S_n$ njenega delovanja na $\{1,2,\ldots,n\}$. Uporabimo zdaj še konvolucijo s funkcijo $\mathrm{sgn} \cdot 1_Q$. Dobimo linearno preslikavo

$$\mathrm{fun}_{P\backslash S_n}(S_n, \mathbf{C}) \to \mathrm{fun}_{P\backslash S_n}(S_n, \mathbf{C}), \quad \psi \mapsto (x \mapsto \psi(x) - \psi((1\ n) \cdot x)).$$

Njeno jedro sestoji iz funkcij $\psi$, ki so konstantne na odsekih $P\backslash S_n$ in povrhu zadoščajo še enakosti $\psi(x) = \psi((1\ n) \cdot x)$ za vsak $x \in S_n$. Ko ta pogoj uporabimo s transpozicijami $(i\ n)$ za $1 \le i < n$, sklenemo, da je vsaka taka funkcija $\psi$ nujno konstantna. Nazadnje je torej

$$V_\lambda = \mathrm{im}\,\mathcal{F}(\sigma_\lambda) \cong \frac{\mathrm{fun}_{P\backslash S_n}(S_n, \mathbf{C})}{\mathbf{C}}.$$

Ta prostor je razsežnosti $n-1$. Prirejeno upodobitev imenujemo **standardna upodobitev** simetrične grupe $S_n$. Kot smo videli, jo lahko dobimo tako, da iz standardne permutacijske upodobitve odstranimo trivialno upodobitev.

**Domača naloga 4.1.3.** Naj bo $\lambda$ razčlenitev $n$ in $\lambda'$ razčlenitev, ki jo iz $\lambda$ dobimo tako, da transponiramo Youngov diagram. Preveri, da velja $\mathrm{sgn} \otimes \rho_\lambda \cong \rho_{\lambda'}$.

Dokaz izreka bomo izpeljali s pomočjo naslednje leme, v kateri igra ključno vlogo delovanje Fourierove transformacije Youngovega simetrizatorja $\widehat{\sigma_\lambda}(\rho_{\mathrm{fun}})$ na prostoru $V_\lambda$. V lemi uporabljamo leksikografsko delno urejenost $<$ na množici vseh razčlenitev.

**Lema 4.1.4.** *Opazujmo simetrično grupo $S_n$.*

1. *Za vsako razčlenitev $\lambda$ je $\widehat{\sigma_\lambda}(\rho_{\mathrm{fun}}) \cdot V_\lambda \subseteq \mathbf{C} \cdot \sigma_\lambda$.*
2. *Za razčlenitvi $\lambda > \mu$ je $\widehat{\sigma_\lambda}(\rho_{\mathrm{fun}}) \cdot V_\mu = 0$.*

*Dokaz.* (dokaz izreka o nerazcepnih upodobitvah simetrične grupe)

1. Naj bo $W \leq V_\lambda$ podupodobitev. Po lemi je $\widehat{\sigma_\lambda}(\rho_{\text{fun}}) \cdot W$ bodisi $\mathbf{C} \cdot \sigma_\lambda$ bodisi 0.

   V prvem primeru sledi, da je $\sigma_\lambda \in W$, od koder sklenemo $W \geq \langle \rho_{\text{fun}}(g) \cdot \sigma_\lambda \mid g \in S_n \rangle$, kar je ravno enako $\operatorname{im} \mathcal{F}(\sigma_\lambda) = V_\lambda$. ✓

   Privzemimo zdaj, da je $\widehat{\sigma_\lambda}(\rho_{\text{fun}}) \cdot W = 0$, kar lahko zapišemo kot $W * \sigma_\lambda = 0$. Od tod sledi $W * V_\lambda = 0$ in zato $W * W = 0$. Naj bo $W = \operatorname{im} P$ za neko projektorsko endospletično $P$ regularne upodobitve. Vemo že, da so vse take preslikave oblike $P = \mathcal{F}(w)$ za neko funkcijo $w \in \operatorname{fun}(S_n, \mathbf{C})$. Ker je $P \cdot 1_1 = \widehat{1_1}(\rho_{\text{fun}}) \cdot w = w$, sledi $w \in W$. Še več, ker je $P^2 = P$, izračunamo $w = P \cdot w = \widehat{w}(\rho_{\text{fun}}) \cdot w = w * w$. Ker je $W * W = 0$, sledi $w = 0$ in s tem $W = 0$. ✓

2. Za različni razčlenitvi $\lambda$, $\mu$ lahko brez škode predpostavimo $\lambda > \mu$, saj je $<$ linearna urejenost. Po lemi je $\widehat{\sigma_\lambda}(\rho_{\text{fun}}) \cdot V_\mu = 0$. Hkrati je $\widehat{\sigma_\lambda}(\rho_{\text{fun}}) \cdot V_\lambda$ bodisi $\mathbf{C} \cdot \sigma_\lambda$ bodisi 0. V slednjem primeru pristopimo kot zgoraj: velja $V_\lambda * V_\lambda = 0$ in projektorska endospletična regularne upodobitve na $V_\lambda$ je oblike $\mathcal{F}(v)$ za neki $v \in V_\lambda$ z lastnostjo $v = v * v$, kar implicira $v = 0$ in s tem $V_\lambda = 0$, protislovje. Torej je $\widehat{\sigma_\lambda}(\rho_{\text{fun}}) \cdot V_\lambda \neq 0$ in zato $V_\lambda \not\subseteq V_\mu$.

□

Preostane nam še dokaz leme.

*Dokaz.* (dokaz leme)

1. Za vsaka $p \in P$, $q \in Q$ je $\operatorname{sgn} \cdot 1_q * \sigma_\lambda * 1_p = \sigma_\lambda$. Dokažimo najprej, da je Youngov simetrizator do skalarja natančno *edina* funkcija s to lastnostjo.

   Res, naj funkcija $f \in \hom(S_n, \mathbf{C})$ zadošča $\operatorname{sgn} \cdot 1_q * f * 1_p = f$. To pomeni, da za vsak $g \in G$ velja

   $$f(g) = \sum_{x \in S_n : qxp = g} \operatorname{sgn}(q) \cdot f(g) = \operatorname{sgn}(q) \cdot f(q^{-1} g p^{-1}),$$

   kar lahko prepišemo v $f(qgp) = \operatorname{sgn}(q) \cdot f(g)$. Od tod sledi $f(qp) = \operatorname{sgn}(q) \cdot f(1)$. Na množici $QP$ se torej do skalarja $f(1)$ natančno funkcija $f$ ujema z Youngovim simetrizatorjem $\sigma_\lambda$.

   Preverimo še, da je zunaj množice $QP$ funkcija $f$ ničelna. V ta namen se spomnimo, da $P$ in $Q$ izhajata iz Youngove tabele $T$. Elementi $S_n$ naravno delujejo s permutacijami na množici tabel. Za $g \in S_n$ naj bo $g \cdot T$ rezultat tega delovanja z elementom $g$.

   **Domača naloga 4.1.5.** Za vsak $g \in S_n \setminus QP$ obstajata števili, ki sta zapisani v istem stolpcu $T$ in isti vrstici $g \cdot T$.

   Naj bo $t$ transpozicija, ki zamenja števili iz predhodne naloge. Zanjo torej velja $t \in Q$ in $g^{-1} t g \in P$. S tem je

   $$f(g) = f(t \cdot g \cdot g^{-1} t g) = \operatorname{sgn}(t) \cdot f(g) = -f(g),$$

   zato je $f(g) = 0$. ✓

   Dokazano uporabimo z elementom $\sigma_\lambda * f * \sigma_\lambda$, kjer je $f$ poljubna funkcija. Vrednost $\operatorname{sgn} \cdot 1_q * (\sigma_\lambda * f * \sigma_\lambda) * 1_p$ izračunamo kot

   $$(\operatorname{sgn} \cdot 1_q * \operatorname{sgn} \cdot 1_Q * 1_P) * f * (\operatorname{sgn} \cdot 1_Q * 1_P * 1_p) = \sigma_\lambda * f * \sigma_\lambda,$$

   od koder sledi želeno

   $$\widehat{\sigma_\lambda}(\rho_{\text{fun}}) \cdot (\sigma_\lambda * f) = \sigma_\lambda * f * \sigma_\lambda \in \mathbf{C} \cdot \sigma_\lambda.$$

2. Trdimo, da za vsako funkcijo $f \in \operatorname{fun}(S_n, \mathbf{C})$ velja enakost

   $$1_{P_\mu} * f * (\operatorname{sgn} \cdot 1_{Q_\lambda}) = 0.$$

   Ker je ta enakost linearna v $f$, lahko predpostavimo, da je $f = 1_g$ za nek $g \in G$.

Naj bosta $T_\lambda$, $T_\mu$ Youngovi tabeli razčlenitev $\lambda$, $\mu$, s katerima smo dobili grupi $P$ in $Q$. Tabelo $T_\lambda$ zamenjajmo s tabelo $g^{-1} \cdot T_\lambda$; ob tem se $Q_\lambda$ zamenja s $g^{-1} Q_\lambda g$. Z novimi tabelami je

$$1_{P_\mu} * (\operatorname{sgn} \cdot 1_{g^{-1} Q_\lambda g}) = 1_{P_\mu} * 1_{g^{-1}} * (\operatorname{sgn} \cdot 1_{Q_\lambda}) * 1_g.$$

Če nam uspe dokazati, da je leva stran ničelna, bo taka tudi desna, od koder po dodatni konvoluciji z $1_{g^{-1}}$ z desne sledi želena enakost.

Predpostavimo torej lahko, da je $g = 1$. Kot v dokazu prejšnje točke najdemo transpozicijo $t \in Q_\lambda \cap P_\mu$. Z njo velja

$$1_{P_\mu} * (\operatorname{sgn} \cdot 1_{Q_\lambda}) = \left(1_{P_\mu} * 1_t\right) * \left(1_{t^{-1}} * (\operatorname{sgn} \cdot 1_{Q_\lambda})\right).$$

Ker je $1_{P_\mu} * 1_t = 1_{P_\mu}$ in $1_{t^{-1}} * (\operatorname{sgn} \cdot 1_{Q_\lambda}) = -(\operatorname{sgn} \cdot 1_{Q_\lambda})$, je zadnja konvolucija enaka svoji negativni vrednosti, torej je ničelna.

□

Ob izpeljavi dokaza izreka smo premislili, da je $\sigma_\lambda * \sigma_\lambda = n_\lambda \cdot \sigma_\lambda$ za neki skalar $n_\lambda \in \mathbf{C}$. Linearna preslikava $\mathcal{F}(\sigma_\lambda)$ slika v vektorski podprostor $V_\lambda$, na tem podprostoru pa deluje kot

$$\mathcal{F}(\sigma_\lambda) \cdot (\sigma_\lambda * f) = \sigma_\lambda * \sigma_\lambda * f = n_\lambda \cdot (\sigma_\lambda * f),$$

torej kot skalarno množenje z $n_\lambda$. Ta skalar lahko izračunamo iz sledi preslikave $\mathcal{F}(\sigma_\lambda)$. V standardni bazi iz karakterističnih funkcij namreč velja

$$\mathcal{F}(\sigma_\lambda) \cdot 1_g = \sigma_\lambda * 1_g = \left(x \mapsto \sigma_\lambda(xg^{-1})\right) = \sum_{x \in S_n} \sigma_\lambda(xg^{-1}) \cdot 1_x$$

za vsak $g \in S_n$, torej so diagonalni členi prirejene matrike $\mathcal{F}(\sigma_\lambda)$ enaki $\sigma_\lambda(1) = 1$. Od tod izračunamo sled preslikave $\mathcal{F}(\sigma_\lambda)$ kot

$$n_\lambda \cdot \dim V_\lambda = \operatorname{tr} \mathcal{F}(\sigma_\lambda) = \sum_{g \in S_n} 1 = n!,$$

zato v posebnem velja $n_\lambda = n! / \dim V_\lambda$. Skalar $n_\lambda$ je torej neničelno racionalno število.

V posebnem lahko tvorimo endospletično $\mathcal{F}(\sigma_\lambda / n_\lambda)$ regularne upodobitve, ki je *projektorska spletična*[5] na prostor $V_\lambda$. V tej posebni situaciji dobimo torej eksplicitno projekcijo z regularne na nerazcepno upodobitev $V_\lambda$. V standardni bazi ima matrika preslikave $\mathcal{F}(\sigma_\lambda / n_\lambda)$ racionalne koeficiente. Ker njeni stolpci razpenjajo prostor $V_\lambda$, lahko torej izberemo ortogonalno[6] bazo $B_\lambda = \{b_1, b_2, \ldots, b_r\}$ prostora $V_\lambda$, v kateri ima vsak vektor $b_i$ racionalne koeficiente v standardni bazi. Ker grupa $S_n$ regularno deluje s permutacijami na standardni bazi, imajo torej tudi slike $\rho_{\text{fun}}(g) \cdot b_i$ racionalne koeficiente v standardni bazi za vsak $g \in S_n$. Vsako od teh slik pa lahko razvijemo tudi po bazi $B_\lambda$ kot

$$\rho_{\text{fun}}(g) \cdot b_i = \sum_{b_j \in B_\lambda} \frac{\langle \rho_{\text{fun}}(g) \cdot b_i, b_j \rangle}{\langle b_j, b_j \rangle} b_j,$$

in pri tem so koeficienti razvoja racionalni. V bazi $B_\lambda$ ima torej vsaka matrika $\rho_{\text{fun}}(g)$ za $g \in S_n$ racionalne koeficiente. Upodobitev $\rho_\lambda$ je torej definirana nad poljem $\mathbf{Q}$.

**Domača naloga 4.1.6.** Naj bo $G$ končna grupa z upodobitvijo nad $\mathbf{Q}$. Dokaži, da obstaja baza vektorskega prostora, v kateri je dana upodobitev definirana nad $\mathbf{Z}$. Nasvet: izberi neko bazo prostora in vsak njen element povpreči po grupi $G$.

**Posledica 4.1.7.** *Vsaka nerazcepna upodobitev simetrične grupe je definirana nad* $\mathbf{Z}$.

[5] Velja namreč $\sigma_\lambda / n_\lambda * \sigma_\lambda / n_\lambda * f = \sigma_\lambda / n_\lambda * f$.

[6] Če izbrana baza ni ortogonalna, na njej uporabimo Gram-Schmidtovo ortogonalizacijo.

Vsak Spechtov modul $V_\lambda$ lahko z redukcijo po modulu $p$ za poljubno praštevilo $p$ reduciramo do vektorskega prostora nad končnim poljem $\mathbf{F}_p$. Na ta način dobimo modularno upodobitev $\rho_{\lambda,p}$ simetrične grupe. Kot smo videli že v primeru $p = 3$, te upodobitve niso nujno nerazcepne. Izkaže se, da pa ima taka modularna upodobitev *enoličen nerazcepen kvocient* $D_\lambda$, če za razčlenitev $\lambda = 1^{i_1}2^{i_2}\cdots n^{i_n}$ velja $i_j < p$ za vsak $j$. Takim ugodnim razčlenitvam pravimo **$p$-regularne razčlenitve**. Izkaže se, da je število $p$-regularnih razčlenitev ravno enako številu konjugiranostnih razredov elementov v $S_n$, katerih red je *tuj* $p$. Na ta način dobimo vse modularne upodobitve simetrične grupe, a tega ne bomo dokazali (glej (Curtis-Reiner 1962) in krajši povzetek tukaj).

**Izrek 4.1.8.** *Vsaka nerazcepna upodobitev $S_n$ nad $\mathbf{F}_p$ je izomorfna $D_\lambda$ za neko $p$-regularno razčlenitev $\lambda$ števila $n$. Pri tem za različni razčlenitvi $\lambda, \mu$ velja $D_\lambda \ncong D_\mu$.*

**Zgled 4.1.9.** Opazujmo grupo $S_3$. Njene nerazcepne upodobitve nad $\mathbf{C}$ dobimo iz razčlenitev $3^1$, $2^1 1^1$ in $1^3$, in sicer zaporedoma $\mathbf{1}$, $\rho$ in sgn. Opazujmo praštevilo $p = 3$. Prvi dve od teh razčlenitev sta 3-regularni, tretja pa ni. Iz prve dobimo nerazcepno upodobitev $\mathbf{1}$ nad $\mathbf{F}_3$, druga upodobitev $\rho$ pa, kot smo videli, ni nerazcepna nad $\mathbf{F}_3$, temveč ima podupodobitev $\mathbf{1}$ s kvocientom $\rho/\mathbf{1} \cong \mathrm{sgn}$. Dobimo torej dve nerazcepni upodobitvi nad $\mathbf{F}_3$, in sicer $\mathbf{1}$ in sgn. Nekoliko nenavadno je, da smo predznačno upodobitev nad $\mathbf{F}_3$ pri tem dobili iz standardne upodobitve $S_3$ in *ne* iz predznačne upodobitve.

Modularni svet je veliko bolj mističen od kompleksnega. Sodobna teorija upodobitev se povečini ukvarja s tem, kako *regularna* je kategorija upodobitev v odvisnosti od praštevila $p$.[7] V zvezi s tem obstajajo številni odprti problemi.

**Odprt problem 4.1.10.** Naj bo $p \le n$ in naj bo $\lambda$ $p$-regularna razčlenitev $n$. Izračunaj večkratnosti $\mathrm{mult}_{\rho_{\lambda,p}}(\pi)$ nerazcepnih upodobitev $\pi$ nad $\mathbf{F}_p$.

Ta problem je razrešen le za razčlenitve $\lambda$ z največ dvema deloma, torej s $k \le 2$. Za $k = 3$ sodobna bilijardna domneva (Lusztig-Williamson 2018) predvideva, da se te večkratnosti obnašajo po zakonu nekega zakompliciranega dinamičnega sistema.

## Vrednosti karakterjev

Premislili smo že, da so vsi Spechtovi moduli definirani nad $\mathbf{Z}$, zato so vrednosti karakterjev simetrične grupe vselej cela števila. Poznamo pa celo dokaj preprost način, kako lahko eksplicitno določimo vse vrednosti karakterjev nerazcepnih upodobitev. Izrekli ga bomo v jeziku polinomskega kolobarja $\mathbf{C}[\mathbf{x}] = \mathbf{C}[x_1, x_2, \ldots, x_k]$. Potrebovali bomo nekaj posebnih polinomov iz tega kolobarja, in sicer **diskriminanto**

$$\Delta(\mathbf{x}) = \prod_{1 \le i < j \le k} (x_i - x_j)$$

ter **potenčne vsote**

$$P_j(\mathbf{x}) = x_1^j + x_2^j + \cdots + x_k^j$$

za $j \in \mathbf{N}$. Za dan polinom $P(\mathbf{x}) \in \mathbf{C}[\mathbf{x}]$ označimo s

$$[P(\mathbf{x})]_{(\ell_1, \ell_2, \ldots, \ell_k)}$$

njegov koeficient pred monomom $x_1^{\ell_1} x_2^{\ell_2} \cdots x_k^{\ell_k}$.

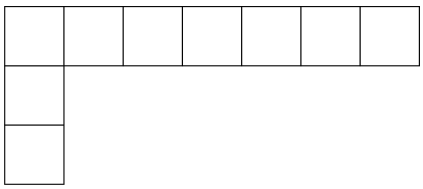
**Izrek 4.1.11** (Frobeniusova formula)**.** *Naj bo $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$ razčlenitev $n$ in $\chi_\lambda$ pripadajoči karakter. Naj bo $C_{1^{i_1}2^{i_2}\ldots n^{i_n}}$ konjugiranostni razred. Tedaj je*

$$\chi_\lambda\left(C_{1^{i_1}2^{i_2}\ldots n^{i_n}}\right) = \left[\Delta(\mathbf{x}) \cdot P_1(\mathbf{x})^{i_1} P_2(\mathbf{x})^{i_2} \cdots P_n(\mathbf{x})^{i_n}\right]_{(\ell_1, \ell_2, \ldots, \ell_k)},$$

*pri čemer je*

$$\ell_1 = \lambda_1 + k - 1, \quad \ell_2 = \lambda_2 + k - 2, \quad \ldots, \quad \ell_k = \lambda_k.$$

[7] Na primer, mnogo dela je osredotočenega na Lusztigovo in Jamesovo domnevo.



Slika 4.2: Kljuka $\lambda = (7,1,1)$.

Dokaz temelji na poznavanju osnov teorije simetričnih funkcij, ki jih po navadi spoznamo pri kombinatoričnih predmetih, zato ga brez prehude žalosti izpustimo. Poglejmo pa si nekaj primerov uporabe izreka.

**Zgled 4.1.12.**

- Naj bo $n = 7$ in $\lambda = (4,3)$. Izračunajmo vrednost karakterja v permutaciji $(1\ 2)(3\ 4)$. Velja $i_1 = 3$, $i_2 = 2$, $\ell_1 = 5$, $\ell_2 = 3$ in s tem

$$\chi_{(4,3)}(\mathcal{C}_{1^3 2^2}) = \left[(x_1 - x_2)\cdot(x_1 + x_2)^3 (x_1^2 + x_2^2)^2\right]_{(5,3)} = 2.$$

- Izračunajmo vrednost poljubnega karakterja $\chi_\lambda$ v dolgem ciklu $(1\ 2 \cdots n) \in S_n$. Konjugiranostni razred je torej $\mathcal{C}_{n^1}$ in izračunati moramo koeficient

$$\left[\Delta(\mathbf{x})\cdot(x_1^n + x_2^n + \cdots + x_k^n)\right]_{(\ell_1,\ell_2,\ldots,\ell_k)}.$$

  Diskriminanta $\Delta(\mathbf{x})$ je enaka Vandermondovi determinanti

$$\Delta(\mathbf{x}) = \sum_{\sigma\in S_k} \operatorname{sgn}(\sigma)\cdot x_1^{\sigma(k)-1} x_2^{\sigma(k-1)-1}\cdots x_k^{\sigma(1)-1}.$$

  Opazujmo potence spremenljivke $x_1$. Opazimo, da velja $\ell_1 = \lambda_1 + k - 1 \geq k$, zato iščemo monome, katerih potenca pri $x_1$ je vsaj $k$. Edina možnost je, da ta monom izhaja iz produkta diskriminante in člena $x_1^n$. Iščemo torej člen

$$\left[\sum_{\sigma\in S_k} \operatorname{sgn}(\sigma)\cdot x_1^{\sigma(k)-1+n} x_2^{\sigma(k-1)-1}\cdots x_k^{\sigma(1)-1}\right]_{(\ell_1,\ell_2,\ldots,\ell_k)}.$$

  Oglejmo si zdaj spremenljivko $x_2$. Da bo obstajal kak relevanten monom, mora veljati $\ell_2 = \sigma(k-1) - 1$. Ker je $\sigma(k-1) \leq k$, sledi $\ell_2 \leq k-1$ in od tod $\lambda_2 \leq 1$. Edina možnost, da je $\chi_\lambda(\mathcal{C}_{n^1}) \neq 0$, je torej, da ima razčlenitev $\lambda$ vse člene od drugega dalje enake 1 in je zato oblike

$$\lambda = (n-s, 1, 1, \ldots, 1)$$

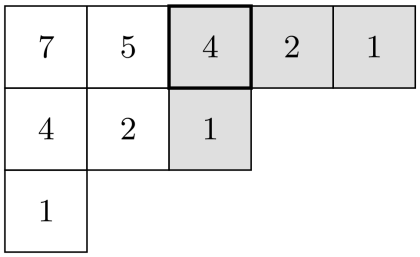
  za neki $0 \leq s \leq n-1$. Takšni razčlenitvi pravimo **kljuka**.

  Za kljuko je $k = s+1$ in $(\ell_1,\ell_2,\ldots,\ell_k) = (n, k-1, k-2, \ldots, 1)$, od koder ni težko izračunati, da edini relevanten monom izhaja iz permutacije $\sigma = (1\ 2 \cdots k)$, zato je nazadnje

$$\chi_\lambda(C_{n^1}) = \operatorname{sgn}(\sigma) = (-1)^s.$$

  Vrednost karakterja v dolgem ciklu je torej neničelna le za kljuke, v katerih pa ima vrednost $\pm 1$.

**Domača naloga 4.1.13.** Izračunaj vrednost poljubnega karakterja $\chi_\lambda$ v konjugiranostnem razredu transpozicij.




Slika 4.3: V celicah Youngovega diagrama razčlenitve $\lambda = (5,3,1)$ so zapisane dolžine kljuk. Označena je kljuka $H_\lambda(1,3)$.

S Frobeniusovo formulo lahko določimo stopnje nerazcepnih upodobitev simetrične grupe. Za to bomo potrebovali koncept kljuke, ki je malo splošnejši od tiste, ki smo jo videli v zadnjem zgledu. Opazujmo Youngov diagram razčlenitve $\lambda$. Za vsako celico $(i,j)$ diagrama, pri čemer $i$ predstavlja vrstico in $j$ stopec, je **kljuka** $H_\lambda(i,j)$ množica tistih celic, ki so desno ali pod celico $(i,j)$, vključivši celico $(i,j)$.[8] **Dolžina kljuke** $H_\lambda(i,j)$ je enaka številu celic v kljuki, se pravi $|H_\lambda(i,j)|$.

**Posledica 4.1.14** (formula o dolžinah kljuk)**.** *Naj bo $\lambda$ razčlenitev $n$. Tedaj je*

$$\dim V_\lambda = \frac{n!}{\prod_{i,j} |H_\lambda(i,j)|}.$$

*Dokaz.* Velja

$$\dim V_\lambda = \chi_\lambda(C_{1^n}) = \left[\Delta(\mathbf{x}) \cdot (x_1 + x_2 + \cdots + x_k)^n\right]_{(\ell_1,\ell_2,\ldots,\ell_k)}.$$

Diskriminanto razvijemo kot v zadnjem zgledu, drugi člen pa po multinomski formuli kot

$$(x_1 + x_2 + \cdots + x_k)^n = \sum_{j_1+j_2+\cdots+j_k=n} \frac{n!}{j_1!j_2!\cdots j_k!} x_1^{j_1} x_2^{j_2} \cdots x_k^{j_k}.$$

Ko razviti vsoti zmnožimo, dobimo člen $x_1^{\ell_1} x_2^{\ell_2} \cdots x_k^{\ell_k}$, če in samo če za neko permutacijo $\sigma \in S_n$ in nabor $j_1, j_2, \ldots, j_k$ velja $\sigma(k-i+1) - 1 + j_i = \ell_i$. Iskani koeficient je torej enak

$$\sum_\sigma \operatorname{sgn}(\sigma) \cdot \frac{n!}{(\ell_1 - \sigma(k) + 1)!(\ell_2 - \sigma(k-1) + 1)! \cdots (\ell_k - \sigma(1) + 1)!},$$

pri čemer seštevamo po tistih $\sigma \in S_k$, za katere velja $\ell_i - \sigma(k-i+1) + 1 \geq 0$ za vsak $i$. To vsoto lahko prepišemo v

$$\frac{n!}{\ell_1!\ell_2!\cdots\ell_k!} \cdot \sum_\sigma \operatorname{sgn}(\sigma) \cdot \prod_{j=1}^{k} \ell_j(\ell_j - 1)\cdots(\ell_j - \sigma(k-j+1) + 2).$$

Zadnjo vsoto lahko seštevamo po vseh $\sigma \in S_k$, saj so členi, v katerih je $\ell_i - \sigma(k-i+1) + 1 < 0$, ničelni. To vsoto zato prepoznamo kot determinanto matrike razsežnosti $k \times k$ z $j$-tim stolpcem

$$1,\ \ell_j,\ \ell_j(\ell_j-1),\ \ldots,\ell_j(\ell_j-1)\cdots(\ell_j-k+2).$$

Ta determinanta je enaka Vandermondovi determinanti, zato je iskani koeficient enak

$$\frac{n!}{\ell_1!\ell_2!\cdots\ell_k!} \cdot \prod_{1\leq i<j\leq n} (\ell_i - \ell_j).$$

Če ima $\lambda$ en sam stolpec in je torej $\lambda = (1,1,\ldots,1)$, potem je $k = n$ in $\ell_i = n - i + 1$, zato je zadnje število enako

$$\frac{n!}{n!(n-1)!\cdots 1!} \cdot \prod_{1\leq i<j\leq n} (j-i) = \frac{n!}{n!(n-1)!\cdots 1!} \cdot \prod_{1<j\leq n} (j-1)! = 1,$$

[8] $H_\lambda(i,j)$ torej sestoji iz tistih celic $(a,b)$, za katere je $a = i$ in $b \geq j$ ali $b = j$ in $a \geq i$.

kot mora biti, saj že vemo, da je v tem primeru $V_\lambda \cong \mathrm{sgn}$. Dolžine kljuk so $|H_\lambda(i,1)| = n-i+1$, zato formula o kljukah za ta trivialen primer drži. Splošnega primera ni težko izpeljati z indukcijo (glej nalogo spodaj). S tem je formula o kljukah dokazana. □

**Domača naloga 4.1.15.** Z indukcijo na število stolpcev Youngovega diagrama $\lambda$ dokaži, da je

$$\frac{n!}{\ell_1!\ell_2!\cdots\ell_k!}\cdot\prod_{i<j}(\ell_i-\ell_j) = \frac{n!}{\prod_{i,j}|H_\lambda(i,j)|}.$$

**Zgled 4.1.16.** Iz formule o dolžinah kljuk takoj izračunamo stopnjo standardne upodobitve. Ustreza ji razčlenitev $(n-1,1)$, torej je njena stopnja enaka

$$\frac{n!}{1\cdot 2\cdot\cdots\cdot(n-2)\cdot n\cdot 1} = n-1.$$

V zvezi s tabelo karakterjev simetrične grupe omenimo še sodobnejši presenetljiv rezultat (Miller 2014), v katerem avtor dokaže, da so vrednosti skoraj vseh karakterjev v skoraj vseh grupnih elementih ničelne. Natančneje, če enakomerno naključno izberemo $g \in S_n$ in $\pi \in \mathrm{Irr}(S_n)$, potem je

$$\lim_{n\to\infty} \mathbf{P}_{g,\pi}\left(\chi_\pi(g) = 0\right) = 1.$$

Avtor omeni analogno vprašanje glede same tabele karakterjev.

**Odprt problem 4.1.17.** Enakomerno naključno izberimo konjugiranostni razred $\mathcal{C}$ v $S_n$ in $\pi \in \mathrm{Irr}(S_n)$. Kaj lahko povemo o obnašanju zaporedja $\mathbf{P}_{\mathcal{C},\pi}\left(\chi_\pi(\mathcal{C}) = 0\right)$, ko gre $n$ čez vse meje?

Na podlagi ekstenzivnih Monte Carlo simulacij (Miller-Scheinerman 2025) ponujata nekaj domnev v tej smeri.

## Alternirajoče grupe

Oglejmo si, kako lahko iz tabele karakterjev simetrične grupe skoraj popolnoma določimo tabelo karakterjev alternirajoče grupe $A_n$.

Določimo najprej konjugiranostne razrede. Naj bo $\mathcal{C} = \sigma^{A_n} \subseteq A_n$ konjugiranostni razred. Ta množica je torej zaprta za konjugiranje z vsemi sodimi permutacijami. Če velja tudi $\sigma^{(1\,2)} \in \mathcal{C}$, potem je $\mathcal{C}$ celo konjugiranostni razred v $S_n$ in torej ustreza neki razčlenitvi števila $n$. Prav lahko pa se zgodi, da $\mathcal{C}$ ni zaprt za konjugiranje z $(1\,2)$. V tem primeru je množica $\mathcal{C}\cup\mathcal{C}^{(1\,2)}$ konjugiranostni razred permutacije $\sigma$ v $S_n$ in zato ustreza neki razčlenitvi števila $n$. Konjugiranostne razrede grupe $A_n$ dobimo torej iz konjugiranostnih razredov sodih permutacij v $S_n$, in sicer določeni razredi v $S_n$ ostanejo konjugiranostni razredi v $A_n$, drugi pa se razcepijo na dva konjugiranostna razreda v $A_n$ enake velikosti. Ni težko prepoznati, kateri razredi se razcepijo.

**Domača naloga 4.1.18.** Naj bo $\mathcal{C}$ konjugiranostni razred sode permutacije v $S_n$, ki ustreza razčlenitvi $\lambda = (\lambda_1,\lambda_2,\ldots,\lambda_k)$. Dokaži, da se $\mathcal{C}$ razcepi v dva konjugiranostna razreda v $A_n$, če in samo če so vsi $\lambda_i$ lihi in različni med seboj.

Poskusimo zdaj na podoben način razumeti še nerazcepne upodobitve grupe $A_n$. Naj bo $\lambda$ razčlenitev $n$, ki ji pritiče nerazcepna upodobitev $\rho_\lambda$ na prostoru $V_\lambda$ s karakterjem $\chi_\lambda$. Opazujmo zožitev karakterja $\chi_\lambda|_{A_n}$ na $A_n$. Po ortonormiranosti karakterjev v $S_n$ velja

$$\langle \chi_\lambda|_{A_n}, \chi_\lambda|_{A_n}\rangle + \frac{1}{|A_n|}\sum_{\sigma\in S_n\setminus A_n}|\chi_\lambda(\sigma)|^2 = \frac{1}{|A_n|}\cdot|S_n|\langle\chi_\lambda,\chi_\lambda\rangle = 2.$$

Torej je $\langle \chi_\lambda|_{A_n}, \chi_\lambda|_{A_n}\rangle \in \{1,2\}$, zato je $\rho_\lambda|_{A_n}$ bodisi nerazcepna upodobitev bodisi vsota dveh neizomorfnih nerazcepnih upodobitev. Drugi primer nastopi, če in samo če je $\chi_\lambda|_{S_n\setminus A_n} = 0$, kar je ekvivalentno izomorfizmu $\rho_\lambda \cong \mathrm{sgn}\otimes\rho_\lambda$. Zadnja upodobitev je izomorfna $\rho_{\lambda'}$, zato se upodobitev $\rho_\lambda$ razcepi na $A_n$, če

in samo če je $\lambda = \lambda'$, se pravi, da je $\lambda$ simetrična razčlenitev. V tem primeru lahko zapišemo $\chi_\lambda|_{A_n} = \alpha + \beta$, kjer sta $\alpha, \beta$ nerazcepna karakterja $A_n$. Ni se težko prepričati, da zanju velja $\beta(\sigma) = \alpha(\sigma^{(1\,2)})$ za vsak $\sigma \in A_n$, torej sta v posebnem upodobitvi, na katere razpade $\rho_\lambda$, enake razsežnosti. Konkretne vrednosti karakterjev $\alpha$ in $\beta$ lahko izračunamo s pomočjo ortogonalnosti karakterjev.

S štetjem konjugiranostnih razredov v $A_n$ se ni težko prepričati, da na opisan način dobimo vse nerazcepne upodobitve alternirajoče grupe. Podrobnosti so podrobno prikazane v (Fulton-Harris 2004).

## 4.2 Splošne linearne grupe

Opazujmo **splošno linearno grupo**

$$G_p = \mathrm{GL}_2(\mathbf{F}_p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbf{F}_p,\ ad - bc \neq 0 \right\}$$

obrnljivih matrik razsežnosti $2 \times 2$ nad končnim poljem $\mathbf{F}_p$, pri čemer je $p$ praštevilo. Njeno kategorijo upodobitev bomo obravnavali nad $\mathbf{C}$. Še pred tem pa moramo bolje spoznati to grupo.[9]

### Osnovne poteze

Grupo $G_p$ lahko razumemo s pomočjo njenih podgrup

$$B_p = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a,d \in \mathbf{F}_p^*,\ b \in \mathbf{F}_p \right\},$$
$$D_p = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a,d \in \mathbf{F}_p^* \right\},$$
$$U_p = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbf{F}_p \right\}.$$

Grupa $B_p$ je **Borelova podgrupa**, grupa $U_p$ pa **unipotentna podgrupa**. Seveda je $B_p/U_p = D_p$. Grupa $G_p$ ima torej vrsto podgrup

$$G_p \geq B_p \geq U_p \geq 1.$$

Borelova podgrupa *ni* edinka v $G_p$, ima pa kvocientna množica $G_p/B_p$ odsekov vsekakor pomembno vlogo. Grupa $G_p$ namreč deluje na ravnini $\mathbf{F}_p^2$ z matričnim množenjem in za tem na množici premic v tej ravnini, se pravi

$$\mathbf{P}^1(\mathbf{F}_p) = \{\ell \leq \mathbf{F}_p^2 \mid \dim \ell = 1\},$$

čemur pravimo **projektivna premica** nad $\mathbf{F}_p$. Grupa $G_p$ deluje na tej premici tranzitivno in stabilizator premice $e_1$ je ravno Borelova podgrupa $B_p$. Projektivno premico lahko zato enačimo z množico $G_p/B_p$. V posebnem tako dobimo homomorfizem

$$\Pi: G_p \to \mathrm{Sym}(\mathbf{P}^1(\mathbf{F}_p)) = S_{p+1},$$

o katerem bomo več povedali nekoliko kasneje. Za zdaj ne spreglejmo, da od tod takoj izračunamo $|G_p/B_p| = p+1$ in s tem

$$|G_p| = |G_p/B_p| \cdot |B_p| = (p+1) \cdot (p-1)^2 p.$$

Grupa $G_p$ je opremljena tudi z determinantnim homomorfizmom

$$\det: G_p \to \mathbf{F}_p^*.$$

Jedro tega homomorfizma je **specialna linearna grupa**

$$\mathrm{SL}_2(\mathbf{F}_p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbf{F}_p,\ ad - bc = 1 \right\}.$$

[9] Lastnosti, ki jih bomo navedli v tem razdelku, ni težko preveriti in jih prepuščamo bralcu v razmislek.

Velja $|\mathrm{SL}_2(\mathbf{F}_p)| = |G_p|/(p-1) = (p+1)p(p-1)$. Izpostavimo dva posebna elementa te grupe,

$$S_+ = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad S_- = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Levo množenje s tema dvema elementoma ustreza izvajanju vrstičnih operacij na dani matriki,

$$S_+ \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix}, \quad S_- \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c+a & d+b \end{pmatrix}$$

Ker lahko vsako matriko v $\mathrm{SL}_2(\mathbf{F}_p)$ z vrstičnimi operacijami pripeljemo do identitete, sklenemo, da elementa $S_+$, $S_-$ *generirata* grupo $\mathrm{SL}_2(\mathbf{F}_p)$.

**Zgled 4.2.1.** Naj bo $p = 2$. Grupa $G_2$ v tem primeru enaka $\mathrm{SL}_2(\mathbf{F}_2)$ in je moči 6. Naravno deluje z matričnim množenjem na množici treh neničelnih vektorjev $\mathbf{F}_2^2 \setminus \{0\} = \{e_1, e_2, e_1+e_2\}$. Na ta način dobimo homomorfizem

$$G_2 \to S_3, \quad S_+ \mapsto (2\ 3),\ S_- \mapsto (1\ 3).$$

ki je surjektiven, ker zapisani transpoziciji generirata grupo $S_3$. Ker imata obe grupi enako moč, je celo izomorfizem, torej je $G_2 \cong S_3$.

**Trditev 4.2.2.** *Za $p > 2$ je $[G_p, G_p] = \mathrm{SL}_2(\mathbf{F}_p)$.*

*Dokaz.* Ker je $G_p/\mathrm{SL}_2(\mathbf{F}_p)$ komutativna, je $[G_p, G_p] \leq \mathrm{SL}_2(\mathbf{F}_p)$. Za obratno neenakost upoštevamo račun

$$\left[S_+^{-2^{-1}}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right] = S_+^{2^{-1}} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot S_+^{-2^{-1}} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = S_+$$

in sklenemo $S_+ \in [G_p, G_p]$. Sorodno dobimo $S_- \in [G_p, G_p]$. Ker $S_+, S_-$ generirata $\mathrm{SL}_2(\mathbf{F}_p)$, dobimo še drugo vsebovanost. □

Nazadnje upoštevajmo oba posebna homomorfizma, $\Pi$ in det. Presek njunih jeder sestoji iz skalarnih matrik z determinanto 1, torej je enak $\{I, -I\}$. Ta podgrupa je edinka v $\mathrm{SL}_2(\mathbf{F}_p)$, zato lahko tvorimo kvocient

$$\mathrm{PSL}_2(\mathbf{F}_p) = \frac{\mathrm{SL}_2(\mathbf{F}_p)}{\{I, -I\}}.$$

**Zgled 4.2.3.** Za $p = 2$ je $\mathrm{PSL}_2(\mathbf{F}_2) = \mathrm{SL}_2(\mathbf{F}_2) \cong S_3$. Za $p = 3$ se grupa $\mathrm{PSL}_2(\mathbf{F}_3)$ prek delovanja $\Pi$ vloži v simetrično grupo $S_4$. Ker je $|\mathrm{PSL}_2(\mathbf{F}_3)| = 12$, je slika te vložitve podgrupa indeksa 2 v $S_4$, kar pomeni, da gre za alternirajočo podgrupo. Sledi $\mathrm{PSL}_2(\mathbf{F}_3) \cong A_4$.

**Domača naloga 4.2.4.** Naj bo $p = 5$. Grupa $\mathrm{PSL}_2(\mathbf{F}_5)$ je moči 60. Poišči njene 2-podgrupe Sylowa. Na množici teh podgrup grupa $\mathrm{PSL}_2(\mathbf{F}_5)$ deluje tranzitivno. Iz tega delovanja izpelji, da je $\mathrm{PSL}_2(\mathbf{F}_5) \cong A_5$.

**Izrek 4.2.5.** *Za $p > 3$ je grupa $\mathrm{PSL}_2(\mathbf{F}_p)$ enostavna.*

*Dokaz.* Izrek je prvi izrekel Galois leta 1831, ni pa podal dokaza. Prvi objavljen dokaz najdemo v (Jordan 1870). Nekoliko bolj sodobna različica dokaza je v Conradovih zapiskih. □

Družina grup $G_p$ za praštevila $p$ je torej dobra prijateljica ene od fundamentalnih družin končnih enostavnih grup.

## Konjugiranostni razredi

Predpostavimo, da je $p > 2$. Konjugiranostni razredi v $G_p$ so enaki podobnostnim razredom matrik. Te najlažje sistematično obravnavamo prek lastnosti njihovih karakterističnih polinomov, ki so stopnje 2. Bodisi je ta polinom razcepen (z eno dvojno ničlo ali dvema različnima v $\mathbf{F}_p$) bodisi je nerazcepen. V primeru dvojnih ničel obravnavamo še možnost, da matrika morda ni diagonalizabilna. Na ta način dobimo naslednje konjugiranostne razrede.

1. **Skalarji**. Naj ima element $g \in G_p$ karakteristični polinom z dvojno ničlo $a \in \mathbf{F}_p^*$ in je hkrati diagonalizabilen. Tedaj je $g$ skalarna matrika

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}.$$

   Vsak tak element je centralen v $G_p$, zato je njegov konjugiranostni razred velikosti 1. Vseh takih razredov je $p-1$.

2. **Nediagonalizabilni elementi**. Naj ima element $g \in G_p$ karakteristični polinom z dvojno ničlo $a \in \mathbf{F}_p^*$ in hkrati *ni* diagonalizabilen. Tedaj je po Jordanovi formi $g$ podoben matriki

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

   Centralizator vsakega takega elementa je enak

$$C_p = \left\{ \begin{pmatrix} x & t \\ 0 & x \end{pmatrix} \mid x \in \mathbf{F}_p^*,\ t \in \mathbf{F}_p \right\} = S_p \times U_p,$$

   pri čemer je $S_p$ množica skalarnih matrik. Velja $|C_p| = (p-1)p$. Konjugiranostni razred je torej velikosti $p^2 - 1$. Vseh takih razredov je $p-1$.

3. **Razcepni polenostavni elementi**. Naj ima element $g \in G_p$ karakteristični polinom z dvema različnima ničlama $a, b \in \mathbf{F}_p^*$. Tak element je diagonalizabilen in zato podoben

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}.$$

   Centralizator vsakega takega elementa je enak

$$T_r = D_p = \left\{ \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} \mid x, y \in \mathbf{F}_p^* \right\}.$$

   in je zato moči $(p-1)^2$. Konjugiranostni razred je torej velikosti $p(p+1)$. Vseh takih razredov je $\binom{p-1}{2} = (p-1)(p-2)/2$.

4. **Nerazcepni polenostavni elementi**. Naj ima element $g \in G_p$ *nerazcepen* karakteristični polinom. Ta polinom torej nima ničel v $\mathbf{F}_p$, ima pa ničle v razširitvi $F$ tega polja z ničlama karakterističnega polinoma. Ker je $p > 2$, sta ti dve ničli različni.[10] Razširitev $F/\mathbf{F}_p$ je stopnje 2, zato jo lahko predstavimo kot

$$F \cong \frac{\mathbf{F}_p[X]}{(X^2 - \epsilon)} = \mathbf{F}_p(\sqrt{\epsilon}),$$

   kjer $\epsilon \in \mathbf{F}_p^*$ *ni* kvadrat v $\mathbf{F}_p$. To polje je opremljeno z Galoisjevim avtomorfizmom $\sigma\colon \sqrt{\epsilon} \mapsto -\sqrt{\epsilon}$ reda 2. Če je $\lambda$ lastna vrednost $g$, je torej tudi $\lambda^\sigma$ lastna vrednost in pripadajoča lastna vektorja sta

[10] Ponovljena ničla bi bila ničla odvoda karakterističnega polinoma, ki pa je linearen in ima vse ničle v $\mathbf{F}_p$.

$v$ in $v^\sigma$. Zamenjajmo bazo v $w_2 = v + v^\sigma$ in $w_1 = (v - v^\sigma)/\sqrt{\epsilon}$. Ta dva vektorja sta invariantna za avtomorfizem $\sigma$, zato imata obe komponenti v $\mathbf{F}_p$. V tej bazi ima element $g$ matriko

$$\begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix},$$

kjer je $a = (\lambda + \lambda^\sigma)/2 \in \mathbf{F}_p$ in $b = (\lambda - \lambda^\sigma)/(2\sqrt{\epsilon}) \in \mathbf{F}_p^*$. Centralizator vsakega takega elementa je enak

$$T_{nr} = \left\{ \begin{pmatrix} x & \epsilon y \\ y & x \end{pmatrix} \mid x, y \in \mathbf{F}_p,\ (x,y) \neq (0,0) \right\}.$$

Konjugiranostni razred je torej velikosti $p(p-1)$. Vseh takih razredov je $p(p-1)/2$.[11]

| | $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ | $\left(\begin{smallmatrix} a & 1 \\ 0 & a \end{smallmatrix}\right)$ | $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$ | $\left(\begin{smallmatrix} a & \epsilon b \\ b & a \end{smallmatrix}\right)$ |
|---|---|---|---|---|
| število razredov | $p-1$ | $p-1$ | $(p-1)(p-2)/2$ | $p(p-1)/2$ |
| velikost razreda | 1 | $p^2-1$ | $p(p+1)$ | $p(p-1)$ |

Tabela 4.1: Konjugiranostni razredi v $G_p$: njihov tip, število razredov določenega tipa in velikost razreda

Za velika praštevila $p$ velja $|G_p| \sim p^4$.[12] Hkrati iz izračunov števila razredov in njihovih velikosti vidimo, da je število polenostavnih elementov asimptotsko primerljivo s $p^4$, razdeljeno približno na polovico med razcepnimi in nerazcepnimi elementi. Generični elementi v $G_p$ so za velika praštevila torej polenostavni.

Seštejemo število vseh konjugiranostnih razredov in dobimo

$$\mathrm{k}(G_p) = p^2 - 1.$$

Grupa $G_p$ ima torej $p^2-1$ nerazcepnih kompleksnih upodobitev.

Preden nadaljujemo z natančnim določanjem teh upodobitev, se še enkrat ozrimo na klasifikacijo konjugiranostnih razredov. Med določanjem velikosti razredov smo naleteli na dva posebna centralizatorja polenostavnih elementov, in sicer $T_r$ in $T_{nr}$. Ta dva centralizatorja bosta imela pomembno vlogo v teoriji upodobitev grupe $G_p$. Prvemu pravimo **razcepni torus**, drugemu pa **nerazcepni torus**. Za razcepni torus velja

$$T_r \cong \mathbf{F}_p^* \times \mathbf{F}_p^*,$$

nerazcepni torus pa identificiramo kot[13]

$$T_{nr} \cong \mathbf{F}_p(\sqrt{\epsilon})^*, \quad \begin{pmatrix} x & \epsilon y \\ y & x \end{pmatrix} \mapsto x + \sqrt{\epsilon} y.$$

Obe grupi, $\mathbf{F}_p^*$ in $\mathbf{F}_p(\sqrt{\epsilon})^*$, sta ciklični grupi. Prva je moči $p-1$, druga pa moči $p^2-1$.

## Tabela karakterjev, 1. del

Predpostavimo, da je $p > 2$. Določimo najprej enorazsežne upodobitve grupe $G_p$. Ker je $[G_p, G_p] = \mathrm{SL}_2(\mathbf{F}_p) = \ker(\det)$, vse enorazsežne upodobitve dobimo tako, da najprej uporabimo determinanto $\det: G_p \to \mathbf{F}_p^*$, za tem pa poljubno upodobitev abelove grupe $\mathbf{F}_p^*$. Za vsak homomorfizem $\chi: \mathbf{F}_p^* \to \mathbf{C}^*$ dobimo torej enorazsežno upodobitev $\chi \circ \det$ grupe $G_p$ in vse enorazsežne upodobitve so take oblike. Vseh teh upodobitev je $|\mathbf{F}_p^*| = p-1$.

Nadaljujmo s pomočjo homomorfizma $\Pi: G_p \to S_{p+1}$, ki opisuje permutacijsko delovanje $G_p$ na projektivni premici. Od tod dobimo permutacijsko upodobitev $G_p$ na $\mathbf{C}[\mathbf{P}^1(\mathbf{F}_p)]$. Kot smo videli že v primeru

[11] Če zamenjamo v zgornji matriki $b$ z $-b$, dobimo podobno matriko. To ravno ustreza delovanju $\sigma$.

[12] Za funkciji $f, g: \mathbf{N} \to \mathbf{R}$ pišemo $f \sim g$, če velja $\lim_{n\to\infty} f(n)/g(n) = 1$.

[13] Element $x + \sqrt{\epsilon} y$ deluje na $\mathbf{F}_p(\sqrt{\epsilon})$ z množenjem z leve. Če to grupo obravnavamo kot vektorski prostor nad $\mathbf{F}_p$, potem je matrika tega delovanja v bazi $\{1, \sqrt{\epsilon}\}$ ravno ta, ki je prikazana.

| | $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ | $\left(\begin{smallmatrix} a & 1 \\ 0 & a \end{smallmatrix}\right)$ | $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$ | $\left(\begin{smallmatrix} a & \epsilon b \\ b & a \end{smallmatrix}\right)$ |
|---|---|---|---|---|
| $\chi \circ \det$ | $\chi(a)^2$ | $\chi(a)^2$ | $\chi(a)\chi(b)$ | $\chi(a^2 - \epsilon b^2)$ |

Tabela 4.2: Enorazsežni karakterji $G_p$

simetrične grupe, ta upodobitev *ni* nerazcepna, saj vedno vsebuje $\mathbf{1}$. Naj bo St komplement $\mathbf{1}$ v tej permutacijski upodobitvi. Ta komplement je do izomorfizma natako enolično določen in mu pravimo **Steinbergova upodobitev**.[14] Vrednosti karakterjev St ni težko izračunati. Račun pokaže $\langle \mathrm{St}, \mathrm{St} \rangle = 1$, zato je St nerazcepna upodobitev.

| | $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ | $\left(\begin{smallmatrix} a & 1 \\ 0 & a \end{smallmatrix}\right)$ | $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$ | $\left(\begin{smallmatrix} a & \epsilon b \\ b & a \end{smallmatrix}\right)$ |
|---|---|---|---|---|
| St | $p$ | $0$ | $1$ | $-1$ |

Tabela 4.3: Steinbergov karakter $G_p$

Steinbergovo upodobitev lahko tenzoriramo s poljubno enorazsežno in dobimo $\mathrm{St} \otimes (\chi \circ \det)$, kar označimo krajše kot $\mathrm{St}(\chi)$. Za $\chi = \mathbf{1}$ dobimo običajno Steinbergovo upodobitev. Vse te upodobitve so tudi nerazcepne.

| | $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ | $\left(\begin{smallmatrix} a & 1 \\ 0 & a \end{smallmatrix}\right)$ | $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$ | $\left(\begin{smallmatrix} a & \epsilon b \\ b & a \end{smallmatrix}\right)$ |
|---|---|---|---|---|
| $\mathrm{St}(\chi)$ | $p\chi(a)^2$ | $0$ | $\chi(a)\chi(b)$ | $-\chi(a^2 - \epsilon b^2)$ |

Tabela 4.4: Posplošeni Steinbergov karakter $G_p$

Do zdaj smo našteli $2(p-1)$ nerazcepnih upodobitev, iščemo pa jih $p^2 - 1$. Še veliko jih manjka! Sledeč filozofiji Artina in Brauerja nadaljnje nerazcepne upodobitve iščemo z indukcijo iz podgrup $G_p$. Opazujmo Borelovo podgrupo $B_p$. Ta grupa je opremljena s projekcijo na razcepni torus

$$B_p \to B_p/U_p = D_p = T_r = \mathbf{F}_p^* \times \mathbf{F}_p^*.$$

Nerazcepne upodobitve razcepnega torusa so ravno produkti $\chi_1 \times \chi_2$, kjer sta $\chi_1$, $\chi_2$ nerazcepni upodobitvi prvega oziroma drugega faktorja torusa. Na ta način dobimo nerazcepne upodobitve Borelove podgrupe,

$$\rho(\chi_1, \chi_2) : B_p \to \mathbf{C}^*, \quad \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mapsto \chi_1(a)\chi_2(d).$$

Vsako od teh upodobitev induciramo na grupo $G_p$ in dobimo upodobitev

$$\pi(\chi_1, \chi_2) = \mathrm{Ind}_{B_p}^{G_p}(\rho(\chi_1, \chi_2))$$

razsežnosti $|G_p/B_p| = p + 1$. Karakter take upodobitve lahko izračunamo s formulo za vrednosti karakterjev inducirane upodobitve.

**Domača naloga 4.2.6.** Izračunaj vrednosti karakterjev upodobitve $\pi(\chi_1, \chi_2)$.

Od tod po preprostem računu določimo normo karakterja kot

$$\|\chi_{\pi(\chi_1,\chi_2)}\|^2 = \begin{cases} 2 & \chi_1 = \chi_2, \\ 1 & \chi_1 \neq \chi_2. \end{cases}$$

Za $\chi_1 \neq \chi_2$ je upodobitev $\pi(\chi_1, \chi_2)$ torej nerazcepna. Iz karakterja opazimo, da je $\rho$ simetrična v svojih argumentih, se pravi $\pi(\chi_1, \chi_2) \cong \pi(\chi_2, \chi_1)$. Na ta način torej dobimo $\binom{p-1}{2} = (p-1)(p-2)/2$ nerazcepnih upodobitev grupe $G_p$. Tem upodobitvam pravimo **upodobitve glavne vrste**.[15] V primeru, ko je $\chi_1 = \chi_2$, iz vrednosti karakterjev opazimo izomorfizem $\pi(\chi, \chi) \cong \mathrm{St}(\chi) \oplus (\chi \circ \det)$, torej tukaj ne najdemo nobenih novih nerazcepnih upodobitev.

[14] Steinbergovo upodobitev dobimo torej tako, da $\Pi$ podaljšamo s standardno upodobitvijo simetrične grupe $S_{p+1}$.

[15] Angleško *principal series representations*.

| | $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ | $\left(\begin{smallmatrix} a & 1 \\ 0 & a \end{smallmatrix}\right)$ | $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$ | $\left(\begin{smallmatrix} a & \epsilon b \\ b & a \end{smallmatrix}\right)$ |
|---|---|---|---|---|
| $\pi(\chi_1,\chi_2)$ | $(p+1)\chi_1(a)\chi_2(a)$ | $\chi_1(a)\chi_2(a)$ | $\chi_1(a)\chi_2(b)+\chi_2(a)\chi_1(b)$ | 0 |

Tabela 4.5: Karakter upodobitve $\pi(\chi_1,\chi_2)$ grupe $G_p$

## Tabela karakterjev, 2. del

Opazujmo zdaj še upodobitve, ki jih dobimo z indukcijo iz nerazcepnega torusa. Te so nekoliko bolj zapletene, zato bomo pristopili bolj previdno. Naj bo

$$\theta: T_{nr} \cong \mathbf{F}_p(\sqrt{\epsilon})^* \to \mathbf{C}^*$$

poljubna enorazsežna upodobitev. Izračunajmo karakter indukcije upodobitve $\theta$ nerazcepnega torusa. Uporabimo formulo za karakter inducirane upodobitve. Naj bo $R$ množica predstavnikov desnih odsekov $T_{nr}$ v $G_p$. Za $g \in G_p$ je $rgr^{-1} \in T_{nr}$ za neki $r \in R$, če in samo če je $rgr^{-1}$ bodisi skalar bodisi nerazcepen polenostaven element, kar je enakovredno temu, da je $g$ bodisi skalar bodisi nerazcepen polenostaven element. Za skalarje, ki jih interpretiramo kot elemente $g = a \in \mathbf{F}_p^* \subseteq \mathbf{F}_p(\sqrt{\epsilon})^*$, velja

$$\mathrm{Ind}_{T_{nr}}^{G_p}(\theta)(a) = |G_p : T_{nr}| \cdot \theta(a) = p(p-1)\theta(a).$$

Za nerazcepne polenostavne elemente, ki jih interpretiramo kot elemente $g = a + \sqrt{\epsilon}b \in \mathbf{F}_p(\sqrt{\epsilon})^*$, pa velja $g^{G_p} \cap T_{nr} = \{g, g^\sigma\}$. V formuli za izračun induciranega karakterja sta zato relevantna le dva člena in dobimo

$$\mathrm{Ind}_{T_{nr}}^{G_p}(\theta)(a+\sqrt{\epsilon}b) = \theta(a+\sqrt{\epsilon}b) + \theta(a-\sqrt{\epsilon}b).$$

Z avtomorfizmom $\sigma \in \mathrm{Gal}(\mathbf{F}_p(\sqrt{\epsilon})/\mathbf{F}_p)$ lahko delujemo na upodobitvi s predpisom $\theta^\sigma(x) = \theta(x^\sigma) = \theta(x^p)$. Torej je zadnja vrednost karakterja enaka $\theta(g) + \theta^\sigma(g)$.

| | $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ | $\left(\begin{smallmatrix} a & 1 \\ 0 & a \end{smallmatrix}\right)$ | $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$ | $\left(\begin{smallmatrix} a & \epsilon b \\ b & a \end{smallmatrix}\right)$ |
|---|---|---|---|---|
| $\mathrm{Ind}_{T_{nr}}^{G_p}(\theta)$ | $p(p-1)\theta(a)$ | 0 | 0 | $\theta(a+\sqrt{\epsilon}b)+\theta(a-\sqrt{\epsilon}b)$ |

Tabela 4.6: Karakter upodobitve $\mathrm{Ind}_{T_{nr}}^{G_p}(\theta)$ grupe $G_p$

Iz vrednosti karakterjev lahko izračunamo normo induciranega karakterja. Vrednost $\|\mathrm{Ind}_{T_{nr}}^{G_p}(\theta)\|^2$ je enaka

$$\frac{1}{|G_p|}\left(\sum_{g\in\mathbf{F}_p^*}(p(p-1)|\theta(g)|)^2 + \sum_{g\in\mathbf{F}_p(\sqrt{\epsilon})^*\setminus\mathbf{F}_p^*}\frac{p(p-1)}{2}\cdot|\theta(g)+\theta^\sigma(g)|^2\right).$$

Zadnjo vsoto lahko po razvoju kvadrata zapišemo kot

$$\frac{p(p-1)}{2}\cdot\left(2(p^2-p)+2\mathrm{Re}\left(\sum_{g\in\mathbf{F}_p(\sqrt{\epsilon})^*}\theta(g)\overline{\theta^\sigma(g)} - \sum_{g\in\mathbf{F}_p^*}|\theta(g)|^2\right)\right).$$

Prvo notranjo vsoto prepoznamo kot skalarni produkt upodobitev $\theta$ in $\theta^\sigma$ v grupi $\mathbf{F}_p(\sqrt{\epsilon})$, ki je enak bodisi 0 bodisi 1 po ortogonalnosti nerazcepnih karakterjev. S tem je norma $\|\mathrm{Ind}_{T_{nr}}^{G_p}(\theta)\|^2$ enaka

$$\frac{1}{|G_p|}\left(p^2(p-1)^3 + p^2(p-1)^2 + p(p-1)\cdot\left((p^2-1)\langle\theta,\theta^\sigma\rangle - (p-1)\right)\right),$$

kar se poenostavi do

$$\|\mathrm{Ind}_{T_{nr}}^{G_p}(\theta)\|^2 = p - 1 + \langle\theta,\theta^\sigma\rangle = \begin{cases} p & \theta = \theta^\sigma, \\ p-1 & \theta \neq \theta^\sigma. \end{cases}$$

Upodobitev $\mathrm{Ind}_{T_{nr}}^{G_p}(\theta)$ je torej daleč od nerazcepne.

Pred nadaljevanjem postojmo pri pogoju $\theta = \theta^\sigma$, ki razdeli inducirane upodobitve na dva naravna razreda. Ta pogoj lahko enakovredno zapišemo kot $\theta(x) = \theta(x^p)$ za vsak $x \in \mathbf{F}_p(\sqrt{\epsilon})^*$, kar je, ker je $\mathbf{F}_p(\sqrt{\epsilon})^*$ ciklična grupa, enako kot $\theta(x^{p-1}) = 1$. Vrednost $\theta$ je torej trivialna na množici $\{x^{p-1} \mid x \in \mathbf{F}_p(\sqrt{\epsilon})^*\}$, ki jo prepoznamo ravno kot jedro determinante $\ker(\det) = \{x \in \mathbf{F}_p(\sqrt{\epsilon})^* \mid x^{p+1} = 1\}$. Pogoj $\theta = \theta^\sigma$ je torej enakovreden temu, da se $\theta$ *faktorizira prek determinante*, se pravi, da je oblike $\theta = \chi \circ \det$ za nek karakter $\chi: \mathbf{F}_p^* \to \mathbf{C}^*$. Vseh takih upodobitev je $p-1$. Upodobitve $\theta$, ki se *ne* faktorizirajo prek determinante, torej za katere velja $\theta \neq \theta^\sigma$, se imenujejo **regularne**. Regularne upodobitve prihajajo torej v parih $(\theta, \theta^\sigma)$. Število Galoisjevih orbit regularnih upodobitev je zato enako $((p^2-1)-(p-1))/2 = p(p-1)/2$.

Glede na to, da inducirana upodobitev iz nerazcepnega torusa ni nerazcepna, lahko poskusimo inducirati še iz kakšne druge podgrupe. Naravni kandidat, ki nam še preostane, je centralizator nediagonalizabilnega elementa, se pravi grupa $C_p = S_p \times U_p$. Izberimo upodobitvi

$$\chi: S_p \cong \mathbf{F}_p^* \to \mathbf{C}^*, \quad \psi: U_p \cong \mathbf{F}_p \to \mathbf{C}^*$$

in tvorimo produktno upodobitev $\chi \times \psi$ grupe $C_p$. To upodobitev induciramo na grupo $G_p$. S formulo za izračun karakterjev inducirane upodobitve ni težko določiti njenega karakterja. Naj bo $R$ množica predstavnikov desnih odsekov $C_p$ v $G_p$. Za $g \in G_p$ je $rgr^{-1} \in C_p$ za nek $r \in R$, če in samo če je $g$ bodisi skalar bodisi nediagonalizabilen element. Za skalarje velja

$$\mathrm{Ind}_{C_p}^{G_p}(\chi \times \psi)\left(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\right) = |G_p : C_p| \cdot \chi(a) = (p^2-1)\chi(a).$$

Za nediagonalizabilen element $g$ pa velja $g^{G_p} \cap C_p = gU_p \backslash S_p$, zato je v formuli za induciran karakter relevantnih le $p-1$ členov in dobimo

$$\mathrm{Ind}_{C_p}^{G_p}(\chi \times \psi)\left(\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}\right) = \sum_{t \in \mathbf{F}_p^*} (\chi \times \psi)\left(\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix} \cdot \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}\right) = \sum_{t \in \mathbf{F}_p^*} \chi(a)\psi(t).$$

Zadnjo vsoto lahko prepišemo kot

$$\chi(a) \cdot \left(\sum_{t \in \mathbf{F}_p} \psi(t) - 1\right) = \chi(a) \cdot (p \cdot \langle \psi, \mathbf{1} \rangle - 1) = \begin{cases} (p-1)\chi(a) & \psi = \mathbf{1}, \\ -\chi(a) & \psi \neq \mathbf{1}. \end{cases}$$

Inducirani karakter je torej odvisen od $\psi$ le preko veljavnosti enakosti $\psi = \mathbf{1}$.

| | $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ | $\left(\begin{smallmatrix} a & 1 \\ 0 & a \end{smallmatrix}\right)$ | $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$ | $\left(\begin{smallmatrix} a & \epsilon b \\ b & a \end{smallmatrix}\right)$ |
|---|---|---|---|---|
| $\mathrm{Ind}_{C_p}^{G_p}(\chi \times \psi)$ | $(p^2-1)\chi(a)$ | $(p \cdot 1_{\psi=\mathbf{1}} - 1)\chi(a)$ | $0$ | $0$ |

Tabela 4.7: Karakter upodobitve $\mathrm{Ind}_{C_p}^{G_p}(\chi \times \psi)$ grupe $G_p$

Iz vrednosti karakterjev izračunamo normo

$$\|\mathrm{Ind}_{C_p}^{G_p}(\chi \times \psi)\|^2 = \begin{cases} 2(p-1) & \psi = \mathbf{1}, \\ p & \psi \neq \mathbf{1}. \end{cases}$$

Upodobitev $\mathrm{Ind}_{C_p}^{G_p}(\chi \times \psi)$ je torej spet daleč od nerazcepne.

Primerjajmo obe inducirani upodobitvi. Skalarni produkt njunih karakterjev lahko izračunamo tako, da seštejemo le prispevke po skalarnih elementih, saj so vsi drugi členi ničelni. Dobimo

$$\langle \mathrm{Ind}_{T_{nr}}^{G_p}(\theta), \mathrm{Ind}_{C_p}^{G_p}(\chi \times \psi) \rangle = \frac{1}{|G_p|} \sum_{a \in \mathbf{F}_p^*} p(p-1)\theta(a) \cdot (p^2-1)\overline{\chi(a)},$$

kar prepoznamo kot

$$(p-1) \cdot \langle \theta|_{S_p}, \chi \rangle = \begin{cases} 0 & \chi \neq \theta|_{S_p}, \\ p-1 & \chi = \theta|_{S_p}. \end{cases}$$

Če torej izberemo $\chi = \theta|_{S_p}$, je skalarni produkt med obema upodobitvama enak $p-1$. Izračunali smo tudi že normi obeh upodobitev, obe sta blizu $\sqrt{p}$. V luči Cauchy-Schwartzove neenakosti sta karakterja obeh induciranih upodobitev kot vektorja torej zelo blizu temu, da bi bila *vzporedna* in s tem *enaka*. Najtesnejšo zvezo med njima dobimo, če minimiziramo normi obeh, torej če vzamemo za $\theta$ regularen karakter in za $\psi$ poljuben netrivialen karakter. S to izbiro opazujmo *virtualen* karakter

$$\zeta_\theta = \mathrm{Ind}_{C_p}^{G_p}(\theta|_{S_p} \times \psi) - \mathrm{Ind}_{T_{nr}}^{G_p}(\theta) \in R(G_p).$$

Po že opravljenih računih je norma tega virtualnega karakterja res minimalna,

$$\langle \zeta_\theta, \zeta_\theta \rangle = \|\mathrm{Ind}_{C_p}^{G_p}(\theta|_{S_p} \times \psi)\|^2 + \|\mathrm{Ind}_{T_{nr}}^{G_p}(\theta)\|^2 - 2\langle \mathrm{Ind}_{T_{nr}}^{G_p}(\theta), \mathrm{Ind}_{C_p}^{G_p}(\theta|_{S_p} \times \psi)\rangle = 1.$$

Torej je bodisi $\zeta_\theta$ bodisi $-\zeta_\theta$ nerazcepen karakter. Ker velja $\zeta_\theta(1) = p-1$, je $\zeta_\theta$ nerazcepen karakter.

| | $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ | $\left(\begin{smallmatrix} a & 1 \\ 0 & a \end{smallmatrix}\right)$ | $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$ | $\left(\begin{smallmatrix} a & \epsilon b \\ b & a \end{smallmatrix}\right)$ |
|---|---|---|---|---|
| $\zeta_\theta$ | $(p-1)\theta(a)$ | $-\theta(a)$ | $0$ | $-\theta(a+\sqrt{\epsilon}b) - \theta(a-\sqrt{\epsilon}b)$ |

Tabela 4.8: Karakter $\zeta_\theta$ grupe $G_p$

Na ta način za vsak regularen karakter $\theta$ nerazcepnega torusa dobimo nerazcepno upodobitev s karakterjem $\zeta_\theta$. Taki upodobitvi pravimo **ostna upodobitev**.[16] Z izračunom skalarnih produktov se ni težko prepričati, da sta dve taki upodobitvi izomorfni, če in samo če sta regularna karakterja v isti orbiti Galoisove grupe. Število ostnih upodobitev je zato enako $p(p-1)/2$. Poudarimo, da smo ostne upodobitve konstruirali le implicitno prek indukcij. Z nekaj truda bi lahko izpeljali eksplicitno konstrukcijo teh upodobitev. Izkaže se, da ostnih upodobitev *ni* mogoče opisati kot neposredno induciranih iz podgrup $G_p$.[17]

Povzemimo. Skupaj smo našli naslednje upodobitve:

- linearne: $p-1$ upodobitev stopnje 1,
- Steinbergove: $p-1$ upodobitev stopnje $p$,
- glavne vrste: $(p-1)(p-2)/2$ upodobitev stopnje $p+1$,
- ostne: $p(p-1)/2$ upodobitev stopnje $p-1$.

S tem smo našteli $p^2-1$ nerazcepnih upodobitev in zatorej vse nerazcepne upodobitve grupe $G_p$.

| | $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ | $\left(\begin{smallmatrix} a & 1 \\ 0 & a \end{smallmatrix}\right)$ | $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$ | $\left(\begin{smallmatrix} a & \epsilon b \\ b & a \end{smallmatrix}\right)$ |
|---|---|---|---|---|
| $\chi \circ \det$ | $\chi(a)^2$ | $\chi(a)^2$ | $\chi(a)\chi(b)$ | $\chi(a^2-\epsilon b^2)$ |
| $\mathrm{St}(\chi)$ | $p\chi(a)^2$ | $0$ | $\chi(a)\chi(b)$ | $-\chi(a^2-\epsilon b^2)$ |
| $\pi(\chi_1,\chi_2)$ | $(p+1)\chi_1(a)\chi_2(a)$ | $\chi_1(a)\chi_2(a)$ | $\chi_1(a)\chi_2(b) + \chi_2(a)\chi_1(b)$ | $0$ |
| $\zeta_\theta$ | $(p-1)\theta(a)$ | $-\theta(a)$ | $0$ | $-\theta(a+\sqrt{\epsilon}b) - \theta(a-\sqrt{\epsilon}b)$ |

Tabela 4.9: Tabela karakterjev $G_p$

Izračunano tabelo karakterjev grupe $G_p$ lahko uporabimo, da z njo določimo še tabelo karakterjev grupe $\mathrm{PSL}_2(\mathbf{F}_p)$.

**Domača naloga 4.2.7.** Izračunaj tabelo karakterjev grupe $\mathrm{SL}_2(\mathbf{F}_p)$ in grupe $\mathrm{PSL}_2(\mathbf{F}_p)$. S tabelo se prepričaj, da je grupa $\mathrm{PSL}_2(\mathbf{F}_p)$ enostavna za $p > 3$. V pomoč ti je lahko obravnava v (Fulton-Harris 2004).

[16] Angleško *cuspidal representation*.

[17] Najpreprostejši znan opis je preko Weilove upodobitve (Bushnell-Henniart 2006), ki ostne upodobitve uresniči na določenih podprostorih v $\mathrm{fun}(\mathbf{F}_p(\sqrt{\epsilon}), \mathbf{C})$.

## Matrike višjih razsežnosti

Argumente, ki smo jih videli v tem razdelku, bi lahko posplošili na matrike večjih razsežnosti in tako (s precej več truda) izračunali generično tabelo karakterjev grupe $\mathrm{GL}_n(\mathbf{F}_q)$, kot je storil (Green 1955). Zopet dobimo glavno vrsto upodobitev, tokrat inducirano induktivno iz podgrup $\mathrm{GL}_m(\mathbf{F}_q)$ za $m < n$. Pri tem je relevantno, da to lahko naredimo na več načinov, na primer za vsako razčlenitev števila $n = m_1 + m_2 + \cdots + m_k$ lahko v $\mathrm{GL}_n(\mathbf{F}_q)$ vidimo bločno diagonalni direktni produkt grup

$$\mathrm{GL}_{m_1}(\mathbf{F}_q) \times \mathrm{GL}_{m_2}(\mathbf{F}_q) \times \cdots \times \mathrm{GL}_{m_k}(\mathbf{F}_q).$$

Teorija upodobitev $\mathrm{GL}_n(\mathbf{F}_q)$ zato vključuje nekaj kompleksnosti teorije upodobitev simetrične grupe $S_n$. Tudi v splošnem primeru dobimo ostne upodobitve, in sicer s pomočjo indukcije iz Galoisjevih razredov regularnih upodobitev nerazcepnega torusa, ki ga lahko predstavimo kot končno polje $\mathbf{F}_{q^n}$.

Ni pa tako enostavno pridobiti tudi tabele karakterjev družine enostavnih grup $\mathrm{PSL}_n(\mathbf{F}_q)$ ali njene prijateljice $E_8(\mathbf{F}_q)$. Seveda lahko posamezne tabele za specifične vrednosti $n$ in $q$ izračunamo,[18] ampak končni cilj je imeti generične tabele karakterjev, kot smo to dosegli za $G_p = \mathrm{GL}_2(\mathbf{F}_p)$. Za razumevanje teorije upodobitev teh grup imamo na voljo matematično zahtevno Deligne-Lusztigovo teorijo, ki upodobitve končnih grup sestavlja s pomočjo upodobitev prirejenih algebraičnih grup nad algebraično zaprtim poljem, na primer $\mathrm{SL}_n(\overline{\mathbf{F}_p})$, in sicer te upodobitve izhajajo iz delovanja na $\ell$-adičnih kohomoloških grupah prirejenih raznoterosti. Iz te teorije lahko razumemo *del* generične tabele karakterjev, na primer poznamo vse stopnje nerazcepnih upodobitev, ne poznamo pa vseh vrednosti vseh karakterjev.

[18] Računanje teh tabel specifičnih končnih enostavnih grup je zbrano v ATLAS. Ti izračuni so močno pripomogli k dokazu izreka o klasifikaciji končnih enostavnih grup.

# Poglavje 5

# Uporabe

Avstralski matematik Geordie Williamson je na svojem plenarnem predavanju na Mednarodnem matematičnem kongresu leta 2018 opisal teorijo upodobitev na naslednji način.

*The idea is that groups in mathematics are everywhere, but groups are nonlinear objects and are rather complicated. We attempt to linearize in some way by taking, for example, actions on a space of functions. We understand what can happen in the linear world by representation theory. Then we hope to go back to our original problem.*

V tem poglavju si bomo pogledali nekaj konkretnih uporab teorije upodobitev, ki na prvi pogled nimajo nobene povezave z upodobitvami, nazadnje pa je za njihovo razumevanje ključna. Začeli bomo z abelovimi grupami. V tem primeru uporabam teorije upodobitev po navadi rečemo **harmonična analiza**. To zgodbo bomo potem razširili še v nekomutativen svet.

## 5.1 Aritmetična zaporedja

### Aritmetična zaporedja v gostih množicah

Za poljuben $n \in \mathbf{N}$ opazujmo množico celih števil $\{1,2,\ldots,n\}$ . Vsaki njeni podmnožici $A$ lahko priredimo gostoto $\delta = |A|/n$. Kadar je $A$ visoke gostote, pričakujemo, da bomo v njej lahko našli veliko vzorcev različnih vrst, ki upoštevajo strukturo seštevanja ali množenja v množici celih števil. Eden od temeljnih takih vzorcev v množici celih števil so **aritmetična zaporedja**, se pravi zaporedja oblike

$$x,\ x+y,\ x+2y,\ldots,\ x+(k-1)y$$

za $x,y \in \mathbf{Z}$, $k \in \mathbf{N}$. Število $k$ je dolžina tega zaporedja in opazujemo seveda le zaporedja dolžine vsaj 3. Izkaže se, da je ta struktura vselej prisotna, neodvisno od izbire konkretne množice $A$, če je le $n$ dovolj velik in gostota $\delta$ pozitivna.

**Izrek 5.1.1** (Szemerédi 1974)**.** *Naj bosta $k \geq 3$ in $\delta > 0$. Tedaj za vse dovolj velike $n \in \mathbf{N}$ velja, da vsaka podmnožica $A \subseteq \{1,2,\ldots,n\}$ gostote vsaj $\delta$ vsebuje aritmetično zaporedje dolžine $k$.*

Dokaz tega izreka je kombinatoričen in tehnično precej zahteven. Mi si bomo ogledali poseben primer za $k = 3$, torej za obstoj 3-članih aritmetičnih zaporedij. Za ta primer bomo izpeljali celo nekoliko močnejšo izjavo, katere dokaz bo slonel na teoriji upodobitev.

**Izrek 5.1.2** (Roth 1953)**.** *Za neko konstanto $C$ in za vse dovolj velike $n \in \mathbf{N}$ velja, da vsaka podmnožica $A \subseteq \{1,2,\ldots,n\}$ gostote vsaj $C/\log\log n$ vsebuje aritmetično zaporedje dolžine 3.*

### Harmonična analiza

#### Projekcija v $\mathbf{F}_p$

Rothov izrek se sicer tiče podmnožice celih števil, ampak ker to množico filtriramo s podmnožicami $\{1,2,\ldots,n\}$, lahko izberemo neko praštevilo $p \geq n$ in dogajanje opazujemo v projekciji na kvocient

$\mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$. Pri tem moramo biti nekoliko previdni, saj so aritmetična zaporedja v $\mathbf{F}_p$ lahko nekoliko nenavadna.

**Zgled 5.1.3.** Naj bo $p > 2$. V $\mathbf{F}_p$ tvori množica $\{0, 1, (p+1)/2\}$ aritmetično zaporedje. Res, če vzamemo $x = 0$, $y = (p+1)/2$, potem dobimo zaporedje z razliko $y$ kot

$$x = 0,\ x + y = \frac{p+1}{2},\ x + 2y = p + 1 = 1.$$

Če torej rešimo Rothov problem za podmnožice $\mathbf{F}_p$ namesto za podmnožice $\{1, 2, \ldots, n\}$, moramo biti previdni, saj dobljenega aritmetičnega zaporedja morda ne bomo mogli dvigniti iz $\mathbf{F}_p$ v $\mathbf{Z}$. Tej težavi se lahko izognemo tako, da izberemo praštevilo $p$ z lastnostjo $p > 2n$. Ni se težko prepričati, da v tem primeru vsako aritmetično zaporedje s 3 členi v $\{1, 2, \ldots, n\} \subseteq \mathbf{F}_p$ lahko dvignemo do aritmetičnega zaporedja v $\{1, 2, \ldots, n\}$. Poleg tega želimo, da se gostota množice $A$ pri projekciji iz $\{1, 2, \ldots, n\}$ v $\mathbf{F}_p$ ne spremeni preveč, zato praštevilo $p$ ne sme biti preveliko. Optimalna izbira bo torej praštevilo $p$ z lastnostjo $2n < p < 4n$, taka izbira pa tudi vselej obstaja po Bertrandovem postulatu.

Dogajanje smo na ta način prestavili v končno abelovo grupo $\mathbf{F}_p$. V njej opazujemo množico $A \subseteq \mathbf{F}_p$, ki je gostote $\delta$. Dokazati želimo, da za dovolj velik $p$ obstajajo v $A$ aritmetična zaporedja dolžine 3, če je le $\delta > C/\log\log p$ za neko konstanto $C$.

### Izražanje problema v jeziku upodobitev

Rothov izrek v $\mathbf{F}_p$ napadimo z močnimi orodji teorije upodobitev grupe $\mathbf{F}_p$. Problem bomo najprej izrazili v prostoru funkcij $\mathrm{fun}(\mathbf{F}_p, \mathbf{C})$. Naj bo $1_A$ karakteristična funkcija množice $A$. Vsako aritmetično zaporedje dolžine 3 je oblike $x, z, y$, pri čemer je $z - x = y - z$, kar je enakovredno $x + y = 2z$. Števila $x$, $y$ in $(x+y)/2$ morajo torej pripadati množici $A$. Število aritmetičnih zaporedij dolžine 3 v $A$ lahko zato izrazimo kot

$$\sum_{x,y,z \in \mathbf{F}_p : x+y=2z} 1_A(x) 1_A(y) 1_A(z) = \sum_{z \in \mathbf{F}_p} (1_A * 1_A)(z) 1_A(z/2)$$

Naj bo $1_{2A}(z) = 1_A(z/2)$. Zadnjo vsoto prepoznamo kot skalarni produkt

$$p \cdot \langle 1_A * 1_A, 1_{2A} \rangle,$$

kar lahko s Parsevalovim izrekom razvijemo kot

$$\frac{1}{p} \sum_{\chi \in \mathrm{Irr}(\mathbf{F}_p)} \widehat{1_A * 1_A}(\chi) \overline{\widehat{1_{2A}}(\chi)}.$$

Trikrat globoko vdihnimo in premislimo vsako zadevo posebej.

1. Nerazcepne upodobitve oziroma karakterje grupe $\mathbf{F}_p$ eksplicitno poznamo, enaki so

   $$\chi_j : \mathbf{F}_p \to \mathbf{C}^*, \quad x \mapsto \zeta^{jx}$$

   za $j \in \mathbf{F}_p$, kjer je $\zeta = e^{2\pi i/p}$.

2. Povezavo med konvolucijo in Fourierovo transformacijo smo videli že pri spletičnah. Dokazali smo, da vse endospletične regularne upodobitve izhajajo iz uporabe Fourierove transformacije. Te lastnosti smo kasneje uporabili tudi pri simetrični grupi. Naj bo zdaj $G$ poljubna grupa in $F$ polje. Naj bosta $f_1, f_2 \in \mathrm{fun}(G, F)$ funkciji in $\rho$ upodobitev grupe $G$. Kompozicija Fourierovih transformacij $\widehat{f_1}(\rho) \cdot \widehat{f_2}(\rho)$ je enaka

   $$\sum_{g_1, g_2 \in G} f_1(g_1) f_2(g_2) \rho(g_1^{-1} g_2^{-1}) = \sum_{g \in G} (f_2 * f_1)(g) \rho(g^{-1}).$$

   Torej velja

   $$\widehat{f_1}(\rho) \cdot \widehat{f_2}(\rho) = \widehat{f_2 * f_1}(\rho)$$

   in Fourierova transformacija pretvarja konvolucijo funkcij v produkt linearnih preslikav, pri čemer moramo biti pozorni na vrstni red operacij zaradi morebitne nekomutativnosti grupe.

3. Velja

$$\widehat{1_{2A}}(\chi) = \sum_{g\in\mathbf{F}_p} 1_{2A}(g)\chi(-g) = \sum_{x\in\mathbf{F}_p} 1_A(x)\chi(-2x) = \widehat{1_A}(\chi^2).$$

Število iskanih aritmetičnih zaporedij je zato enako

$$\frac{1}{p}\sum_{j\in\mathbf{F}_p} \widehat{1_A}(\chi_j)^2\overline{\widehat{1_A}(\chi_j^2)} = \frac{1}{p}\sum_{j\in\mathbf{F}_p} \widehat{1_A}(\chi_j)^2\widehat{1_A}(\chi_{-2j}).$$

**Glavni del in prispevki netrivialnih karakterjev**

Izolirajmo prispevek trivialne upodobitve. Velja $\widehat{1_A}(\chi_0) = \widehat{1_A}(\mathbf{1}) = |A|$, zato je število aritmetičnih zaporedij dolžine 3 v $A$ enako

$$\frac{|A|^3}{p} + \frac{1}{p}\sum_{j\in\mathbf{F}_p^*} \widehat{1_A}(\chi_j)^2\widehat{1_A}(\chi_{-2j}).$$

Glavni del rezultata je nekoliko nehomogen. To lahko popravimo z dodatno normalizacijo s $p^2$, ki ima pravzaprav zelo smiselno interpretacijo. Če namreč izberemo $x,y,z\in\mathbf{F}_p$ enakomerno naključno, a pogojno na veljavnost $x+y=2z$,[1] potem je verjetnost, da so $x,y,z$ vsi v $A$, enaka

$$\mathbf{P}_{x,y,z\in\mathbf{F}_p}(x,y,z\in A \mid x+y=2z) = \delta^3 + \frac{1}{p^3}\sum_{j\in\mathbf{F}_p^*} \widehat{1_A(\chi_j)}^2\widehat{1_A}(\chi_{-2j}).$$

Brez pogojne omejitve bi bila zgornja verjetnost seveda enaka $\delta^3$. Srčika pogoja aritmetičnega zaporedja dolžine 3 se torej skriva v prispevkih netrivialnih karakterjev. Splošna strategija harmonične analize je, da ti prispevki nikdar ne uspejo izničiti glavnega delta $\delta^3$ in da v $A$ torej res obstaja aritmetično zaporedje dolžine 3.

Za omejitev netrivialnih prispevkov najprej uporabimo trikotniško neenakost,

$$\left|\sum_{j\in\mathbf{F}_p^*} \widehat{1_A}^2(\chi_j)\widehat{1_A}(\chi_{-2j})\right| \le \max_{j\in\mathbf{F}_p^*}|\widehat{1_A}(\chi_j)|\cdot\sum_{j\in\mathbf{F}_p^*}|\widehat{1_A}(\chi_j)||\widehat{1_A}(\chi_{-2j})|.$$

Zadnjo vsoto ocenimo s Cauchy-Schwartzovo neenakostjo, tako da dobimo zgornjo mejo

$$\max_{j\in\mathbf{F}_p^*}|\widehat{1_A}(\chi_j)|\cdot\sqrt{\sum_{j\in\mathbf{F}_p}|\widehat{1_A}(\chi_j)|^2}\cdot\sqrt{\sum_{j\in\mathbf{F}_p}|\widehat{1_A}(\chi_{-2j})|^2}.$$

Vsota pod korenoma je v obeh primerih enaka, in sicer jo po Parsevalu lahko izrazimo kot

$$\sum_{j\in\mathbf{F}_p}|\widehat{1_A}(\chi_j)|^2 = \sum_{j\in\mathbf{F}_p}\langle\widehat{1_A}(\chi_j),\widehat{1_A}(\chi_j)\rangle_{\mathrm{HS}} = p^2\langle 1_A,1_A\rangle = p|A|.$$

Od tod torej sklenemo

$$\mathbf{P}_{x,y,z\in\mathbf{F}_p}(x,y,z\in A \mid x+y=2z) \ge \delta^3 - \delta\cdot\frac{1}{p}\max_{j\in\mathbf{F}_p^*}|\widehat{1_A}(\chi_j)|.$$

Kadar je Fourierova transformacija $1_A$ v vseh netrivialnih karakterjih strogo manjša od $p\delta^2$, je verjetnost na levi strani strogo pozitivna, zato res najdemo aritmetično zaporedje dolžine 3 v $A$. Ko pa ima po drugi strani $\widehat{1_A}$ kakšen velik netrivialen Fourierov koeficient, se pravi, ko za nek $j\in\mathbf{F}_p^*$ velja

$$|\widehat{1_A}(\chi_j)| \ge p\delta^2,$$

pa harmonična analiza odpove. V tem primeru moramo podrobneje raziskati pomen velikega Fourierovega koeficienta.

[1] Na ta način torej izbiramo aritmetična zaporedja v $\mathbf{F}_p$ dolžine 3.

**Večanje gostote**

Predpostavimo, da je $|\widehat{1_A}(\chi_j)| \geq p\delta^2$ za nek $j \in \mathbf{F}_p^*$. Preden nadaljujemo, bomo funkcijo $1_A$ projicirali na podprostor funkcij z ničelnim povprečjem. Naj bo $f = 1_A - \delta \in \mathrm{fun}(\mathbf{F}_p, \mathbf{C})$. Velja

$$\widehat{f}(\chi_j) = \widehat{1_A}(\chi_j) - \delta\widehat{1}(\chi_j) = \widehat{1_A}(\chi_j) - \delta p\langle \mathbf{1}, \chi_j\rangle = \widehat{1_A}(\chi_j),$$

zato je

$$\left|\sum_{x\in\mathbf{F}_p} f(x)\zeta^{-jx}\right| = |\widehat{f}(\chi_j)| \geq p\delta^2.$$

Funkcija $x \mapsto \zeta^{-jx}$ precej oscilira, ko $x$ preteče ves $\mathbf{F}_p$. Če bi bila ta funkcija približno konstanta, bi lahko sklepali, da je vsota vrednosti $f$ precej velika. Približno konstantnost te funkcije lahko dosežemo tako, da preidemo na neko podmnožico $\mathbf{F}_p$.

**Domača naloga 5.1.4.** Obstaja konstanta $c \in (0, \frac{1}{2})$, za katero velja naslednje. Množico $\mathbf{F}_p$ lahko razčlenimo kot disjunktno unijo množice podmnožic $P_1, P_2, \ldots, P_m$, tako da je vsaka množica $P_i$ aritmetično zaporedje dolžine med $c\sqrt{p}$ in $(1-c)\sqrt{p}$, hkrati pa je $|\zeta^{-jx} - \zeta^{-jy}| < c\delta^2$ za vsaka $x, y \in P_i$.

S pomočjo razčlenitve množice $\mathbf{F}_p$ torej sklepamo

$$\left|\sum_{x\in\mathbf{F}_p} f(x)\zeta^{-jx}\right| \leq \sum_{i=1}^{m}\left|\sum_{x\in P_i} f(x)\zeta^{-jx}\right| = \sum_{i=1}^{m}\left|\sum_{x\in P_i} f(x)\left(\zeta^{-jx_0} + (\zeta^{-jx} - \zeta^{-jx_0})\right)\right|,$$

pri čemer smo v vsakem $P_i$ izbrali nek element $x_0$. Po trikotniški neenakosti in upoštevanju približne konstantnosti funkcije $x \mapsto \zeta^{-jx}$ na $P_i$ lahko zadnjo vsoto omejimo navzgor kot

$$\sum_{i=1}^{m}\left|\sum_{x\in P_i} f(x)\right| + \sum_{i=1}^{m}\sum_{x\in P_i}|f(x)|c\delta^2 \leq \sum_{i=1}^{m}\left|\sum_{x\in P_i} f(x)\right| + cp\delta^2.$$

S tem nazadnje dobimo neenakost

$$\sum_{i=1}^{m}\left|\sum_{x\in P_i} f(x)\right| \geq (1-c)p\delta^2.$$

Po konstrukciji je povprečje funkcije $f$ po $\mathbf{F}_p$ enako 0. Vsote po zaporedjih $P_i$ se torej seštejejo v 0, po absolutni vrednosti pa se seštejejo v vsaj $(1-c)p\delta^2$. Torej obstaja neki $i$, za katerega velja

$$\sum_{x\in P_i} f(x) + \left|\sum_{x\in P_i} f(x)\right| \geq \frac{1}{m}(1-c)p\delta^2.$$

Ker je $|\mathbf{F}_p| = \sum_{i=1}^{m}|P_i|$, dobimo neenakost $p \geq mc\sqrt{p}$. Hkrati za vsako realno število $r$ velja $r + |r| = 2\max(r, 0)$, zato je

$$\max\left(\sum_{x\in P_i} f(x), 0\right) \geq \frac{c(1-c)}{2}\sqrt{p}\delta^2 \geq \frac{c}{2}|P_i|\delta^2.$$

Leva stran je zato strogo pozitivna in enaka vsoti $f$ po $P_i$. Upoštevamo še $f = 1_A - \delta$ in sklenemo

$$|A \cap P_i| \geq \frac{c}{2}|P_i|\delta^2 + |P_i|\delta$$

oziroma ekvivalentno

$$\frac{|A \cap P_i|}{|P_i|} \geq \delta + \frac{c}{2}\delta^2.$$

Množica $A$ ima torej v aritmetičnem zaporedju $P_i$ gostoto za $\frac{c}{2}\delta^2$ večjo kot v $\mathbf{F}_p$.

**Iteracija**

Povzemimo. Če množica $A$ gostote $\delta$ nima aritmetičnih zaporedij dolžine 3, potem smo našli aritmetično zaporedje $P_i$, v katerem ima $A$ gostoto vsaj $\delta + \frac{c}{2}\delta^2$. Ta postopek zdaj iteriramo.[2] Če množica $A \cap P_i$ nima aritmetičnih zaporedij dolžine 3, potem najdemo aritmetično zaporedje dolžine med $c\sqrt{|P_i|}$ in $(1-c)\sqrt{|P_i|}$, v katerem ima $A$ gostoto vsaj $\delta + 2\frac{c}{2}\delta^2$, in tako dalje. Ker gostota na nobeni točki ne more preseči vrednosti 1, se ta postopek gotovo ustavi po končno mnogo korakih. Na tej točki najdemo aritmetično zaporedje dolžine 3 v $A$, če je le velikost množice $P_i$ do te točke dovolj velika. Iz podrobne analize večanja gostote in spreminjaja velikosti množic $P_i$ se da izpeljati,[3] da ta argument res deluje, če je le $\delta \geq C/\log\log p$ za neko konstanto $C$. S tem je Rothov izrek dokazan.

### Onkraj Rothovega izreka

Veliko dela po Rothovem izreku je bilo posvečenega izboljšanju meje o gostoti, ki še zagotovi obstoj aritmetičnih zaporedij dolžine 3. Večina izboljšav spodnje meje je s seboj prinesla nove ideje, uporabne tudi za reševanje kakšnih drugih problemov. Najsodobnejši rezultat v zvezi s tem je prebojen članek (Bloom-Sisask 2020), v katerem avtorja dokažeta, da obstajata konstanti $C, c$, tako da ima vsaka množica $A \subseteq \{1,2,\ldots,n\}$ gostote vsaj $C/(\log n)^{1+c}$ aritmetično zaporedje dolžine 3. Ta meja se torej znebi dvojnega logaritma in uvede minimalen eksponent k logaritmu, zato je bistveno manjša restrikcija na gostoto.[4]

Ta rezultat lahko uporabimo, na primer, z množico praštevil. Po izreku Čebiševa je število praštevil do $n$ vsaj $Cn/\log n$, zato imajo praštevila v $\{1,2,\ldots,n\}$ gostoto vsaj $C/\log n$ in na njih lahko uporabimo posplošeni Rothov izrek. Ker lahko vselej tudi izpustimo prvih nekaj praštevil, torej sklepamo, da množica praštevil vsebuje neskončno mnogo aritmetičnih zaporedij dolžine 3. Poudarimo konceptualno pomembno dejstvo, da smo ta rezultat izpeljali zgolj zaradi same gostote praštevil in ne zaradi kakršne koli druge njihove lastnosti. Ne nazadnje je slogan izvirnega Rothovega izreka ta, da lahko najdemo v vsaki dovolj gosti množici strukturo.

**Odprt problem 5.1.5.** Ali je mogoče z ustrezno posplošitvijo Rothovega izreka dokazati, da praštevila vsebujejo aritmetična zaporedja dolžine $k$ za vsak $k \geq 3$? Obstoj takih zaporedij je sicer znan iz (Green-Tao 2004), ki temelji na razširitvi Szemerédijevega izreka, a ne v smeri nižanja meje gostote, temveč v uporabi izreka na specifičnih redkih podmnožicah.

**Domača naloga 5.1.6.** S harmonično analizo dokaži, da ima za vsak $n \geq 3$ Fermatova enačba $x^n + y^n = z^n$ netrivialno ($xyz \neq 0$) rešitev v $\mathbf{F}_p$ za vsako dovolj veliko (v odvisnosti od $n$) praštevilo $p$. Eden izmed pristopov je, da število rešitev enačbe izraziš s Fourierovo inverzijo funkcije $1_0$ v aditivni grupi $\mathbf{F}_p$ kot

$$\sum_{x,y,z\in\mathbf{F}_p} 1_0(x^n+y^n-z^n) = \frac{1}{p}\sum_{x,y,z,j\in\mathbf{F}_p} \zeta^{j(x^n+y^n-z^n)} = \frac{1}{p}\sum_{j\in\mathbf{F}_p} S_j \cdot S_j \cdot \overline{S_j},$$

kjer je $S_j = \sum_{a\in\mathbf{F}_p} \zeta^{ja^n}$. Določi glavni del ter omeji prispevke netrivialnih karakterjev.

## 5.2 Podmnožice brez produktov

### Antipodgrupe

Naj bo $G$ končna grupa in $A \subseteq G$ njena podmnožica. Množica $A$ je podgrupa, če in samo če je zaprta za množenje, se pravi $A \cdot A \subseteq A$. Skrajno diametralno tej strukturi se znajdemo, če predpostavimo, da produkt *nobenih* dveh elementov iz množice $A$ ne pripada $A$, se pravi $A \cdot A \cap A = \varnothing$. Z drugimi besedami,

[2] Ne bomo preveč natančni glede iteracije. V grobem lahko iz aritmetičnega zaporedja $P_i$ preidemo na ciklično grupo enake moči (morda ne več praštevilske) in potem ponovimo argument v tej ciklični grupi.

[3] Glej (Peluse 2022).

[4] Iskanje optimalnih restrikcij na gostoto je predstavljeno v (Bone 2024).

enačba $xy = z$ v množici $A$ nima rešitev. V tem primeru rečemo, da je množica $A$ **brez produktov**. Če smo v teoriji grup malodane obsedeni s strukturiranimi množicami, nas mora vsaj malo zanimati tudi druga skrajnost.

Kadar množica $A$ vsebuje kakšno podgrupo, seveda *ni* brez produktov, zato se morajo take množice čim bolj izogniti podgrupam. Osnovno vprašanje v zvezi z množicami brez produktov je, kako velike podmnožice brez produktov dana grupa vsebuje. Za začetek si oglejmo nekaj preprostih zgledov.

**Zgled 5.2.1.**

- Naj bo $G = \mathbf{Z}/n\mathbf{Z}$ in $A$ neka njena podmnožica. Množica $A$ je brez produktov, če in samo če enačba $x + y = z$ nima rešitve v $A$. To vprašanje je ravno obratno sorodni lastnosti, ki smo jo opazovali v prejšnjem razdelku. Tam smo reševali le malo drugačno enačbo $x + y = 2z$ in dokazali, da ima vselej rešitve v podmnožicah pozitivne gostote. Zanimivo je, da je situacija precej drugačna za enačbo $x + y = z$.[5] Za množico $A$ lahko vzamemo na primer vsa števila v $\mathbf{Z}/n\mathbf{Z}$, ki so strogo med $\frac{1}{3}n$ in $\frac{2}{3}n$. Ta množica je jasno brez produktov in je gostote približno $\frac{1}{3}$ v $\mathbf{Z}/n\mathbf{Z}$ za velike vrednosti $n$.

  To konstrukcijo lahko posplošimo na poljubno končno abelovo grupo.

  **Domača naloga 5.2.2.** Naj bo $A$ končna abelova grupa. Prepričaj se, da vselej obstaja podmnožica v $A$, ki je brez produktov in gostote vsaj $\frac{2}{7}$.

- Simetrična grupa $S_n$ vsebuje ogromno množico brez produktov, in sicer množico vseh lihih permutacij $S_n \setminus A_n$. Produkt dveh lihih permutacij je soda permutacija, zato je ta množica res brez produktov. Njena gostota je $\frac{1}{2}$.

- Naj bo $G$ končna grupa s podgrupo $H \leq G$. Naj bo $A = Hg$ za nek $g \in G \setminus H$. Tedaj za $x = h_1 g$ in $y = h_2 g$ velja $Hxy = Hh_1 g h_2 g = Hgh_2 g$. Pri tem velja $xy \in A$, če in samo če je $Hgh_2 g = Hg$, kar se poenostavi do $gh_2 \in H$, se pravi $g \in H$, kar je sprto s predpostavko. Množica $A$ je zato brez produktov. Njena gostota v $G$ je $1/|G : H|$. Ta primer posploši zadnjega, kjer smo obravnavali $A_n \leq S_n$.

Veliko težje je najti podmnožice brez produktov pozitivne gostote v alternirajoči grupi $A_n$ (ko gre $n$ proti neskončnosti) ali linearni grupi $\mathrm{PSL}_2(\mathbf{F}_p)$ (ko gre $p$ proti neskončnosti). Dokazali bomo, da to težavo lahko pojasnimo s teorijo upodobitev.

**Izrek 5.2.3** (Gowers 2008)**.** *Naj bo $G$ končna grupa in naj bo $m$ najmanjša stopnja netrivialne nerazcepne kompleksne upodobitve $G$. Tedaj je vsaka podmnožica brez produktov v $G$ gostote kvečjemu $m^{-1/3}$.*

**Zgled 5.2.4.**

- Iz rezultatov o upodobitvah simetričnih grup (natančneje, formule o kljukah) sledi, do ima $S_n$ dve nerazcepni upodobitvi stopnje 1 (to sta $\mathbf{1}$ in sgn) in dve nerazcepni upodobitvi stopnje $n-1$ (to sta $\rho$ in $\rho \otimes \mathrm{sgn}$), vse druge nerazcepne upodobitve pa so višje stopnje (za $n \geq 7$). Velja torej $m = \Theta(n)$.[6] Po izreku v $A_n$ zatorej *ni* podmnožic brez produktov pozitivne gostote, ko gre $n$ čez vse meje. Še več, največja dovoljena gostota je velikostnega reda $m^{-1/3} = \Theta(n^{-1/3})$.

- Opazujmo grupo $\mathrm{PSL}_2(\mathbf{F}_p)$. Iz njene tabele karakterjev razberemo, da zanjo velja $m = (p-1)/2$. Po izreku tudi ta grupa nima podmnožic brez produktov pozitivne gostote, ko gre $p$ čez vse meje. Še več, največja gostota, ki jo dopušča izrek, je velikostnega reda $m^{-1/3} = \Theta(p^{-1/3}) = \Theta(|\mathrm{PSL}_2(\mathbf{F}_p)|^{-1/9})$, kar je celo veliko manjše (relativno glede na velikost grupe) od zgornje meje, ki smo jo videli v primeru alternirajoče grupe.

[5] Lahko bi naredili sicer enak razmislek kot v dokazu Rothovega izreka, a nam od tiste točke, ko harmonična analiza odpove, obstoj aritmetičnih zaporedij $P_i$ ne bi koristil za reševanje enačbe $x + y = z$.

[6] Za funkciji $f, g : \mathbf{N} \to \mathbf{R}$ pišemo $f \ll g$, če obstaja konstanta $C$, da je $f(n) \leq Cg(n)$ za vse $n$. V primeru, ko za funkciji $f, g$ velja hkrati $f \ll g$ in $g \ll f$, pišemo $f = \Theta(g)$. Funkciji $f$ in $g$ sta torej asimptotsko do konstante natančno enaki.

## Harmonična analiza

Gowersov izrek bomo dokazali s pomočjo nekoliko močnejše trditve.

**Trditev 5.2.5.** *Naj bo $G$ končna grupa in naj bo $m$ najmanjša stopnja netrivialne nerazcepne kompleksne upodobitve $G$. Naj bosta $A, B \subseteq G$ podmnožici gostote $\alpha, \beta$. Tedaj velja*

$$\left|\mathbf{P}_{x,y,z\in G}(x,y\in A,\ z\in B \mid xy=z) - \alpha^2\beta\right| \leq m^{-1/2}\alpha\beta^{1/2}.$$

Iz trditve hitro izpeljemo Gowersov izrek. Uporabimo jo z $A = B$. Če je $A$ brez produktov in gostote $\alpha$, potem velja $\alpha^3 \leq m^{-1/2}\alpha^{3/2}$, kar je enakovredno $\alpha \leq m^{-1/3}$.

*Dokaz.* (dokaz trditve) Verjetnost v trditvi je enaka

$$\frac{|\{(x,y,z)\in A\times A\times B \mid xy=z\}|}{|G|^2}.$$

Število rešitev enačbe $xy = z$ za $x, y \in A, z \in B$ lahko izrazimo kot

$$\sum_{x,y,z\in G: xy=z} 1_A(x)1_A(y)1_B(z) = \sum_{z\in G}(1_A * 1_A)(z)1_B(z) = |G|\cdot\langle 1_A * 1_A, 1_B\rangle.$$

Skalarni produkt razvijemo s Parsevalovo formulo in dobimo

$$\frac{1}{|G|}\sum_{\pi\in\mathrm{Irr}(G)} \chi_\pi(1)\cdot\langle\widehat{1_A}(\pi)^2, \widehat{1_B}(\pi)\rangle_{\mathrm{HS}}.$$

Prispevek trivialne upodobitve je enak

$$\langle\widehat{1_A}(\mathbf{1})^2, \widehat{1_B}(\mathbf{1})\rangle_{\mathrm{HS}}/|G| = |A|^2|B|/|G| = \alpha^2\beta|G|^2.$$

Prispevke netrivialnih upodobitev lahko s trikotniško neenakostjo po absolutni vrednosti omejimo navzgor kot

$$\frac{1}{|G|}\sum_{\mathbf{1}\neq\pi\in\mathrm{Irr}(G)} \chi_\pi(1)\left|\langle\widehat{1_A}(\pi)^2, \widehat{1_B}(\pi)\rangle_{\mathrm{HS}}\right|,$$

kar je po Cauchy-Schwartzovi neenakosti kvečjemu

$$\frac{1}{|G|}\sum_{\mathbf{1}\neq\pi\in\mathrm{Irr}(G)} \chi_\pi(1)\|\widehat{1_A}(\pi)\|_{\mathrm{HS}}^2\|\widehat{1_B}(\pi)\|_{\mathrm{HS}}.$$

V zadnji vsoti zadnjo normo omejimo z maksimumom, da dobimo zgornjo mejo

$$\max_{\mathbf{1}\neq\pi\in\mathrm{Irr}(G)}\|\widehat{1_B}(\pi)\|_{\mathrm{HS}}\cdot\frac{1}{|G|}\sum_{\mathbf{1}\neq\pi\in\mathrm{Irr}(G)}\chi_\pi(1)\|\widehat{1_A}(\pi)\|_{\mathrm{HS}}^2,$$

Prvi člen lahko omejimo z neenakostjo

$$m\cdot\max_{\mathbf{1}\neq\pi\in\mathrm{Irr}(G)}\|\widehat{1_B}(\pi)\|_{\mathrm{HS}}^2 \leq \sum_{\mathbf{1}\neq\pi\in\mathrm{Irr}(G)}\chi_\pi(1)\|\widehat{1_B}(\pi)\|_{\mathrm{HS}}^2 \leq |G|^2\|1_B\|^2 = |B||G|$$

in zadnjo neenakost lahko uporabimo tudi za omejitev drugega člena. S tem dobimo zgornjo mejo

$$\sqrt{\frac{|B||G|}{m}}\cdot|A| = m^{-1/2}\alpha\beta^{1/2}|G|^2$$

za prispevke netrivialnih upodobitev. Trditev je s tem dokazana. □

Iz Gowersovega izreka sledi nekoliko presenetljiva lastnost dovolj velikih podmnožic.

**Posledica 5.2.6** (Nikolov-Pyber 2011)**.** *Naj bo $G$ končna grupa in naj bo $m$ najmanjša stopnja netrivialne neracepne kompleksne upodobitve $G$. Če je $A$ podmnožica $G$ gostote strogo večje od $m^{-1/3}$, potem je $A \cdot A \cdot A = G$.*

*Dokaz.* Naj bo $g \in G$ in naj bo $B = gA^{-1} \subseteq G$. Množici $A$ in $B$ sta obe enake gostote, recimo $\alpha$. Velja $\alpha^3 > m^{-1}$, kar je enakovredno $m^{-1/2}\alpha^{3/2} < \alpha^3$. Iz trditve od tod sledi $A \cdot A \cap B \neq \emptyset$, zato je $g \in A \cdot A \cdot A$. Ker je bil $g$ poljuben, je $A \cdot A \cdot A = G$. □

Ta lastnost velikih množic ima veliko zelo relevantnih uporab v teoriji grup, na primer pri dokazovanju Babaijeve domneve o premerih končnih enostavnih grup prek teorije približnih podgrup in pri raziskovanju slučajnih sprehodov,[7] kot je razloženo v (Breuillard 2013).

## Največja možna gostota

Z Gowersovo zgornjo mejo za dovoljeno gostoto množice brez produktov se seveda lahko vprašamo, kako optimalna je ta meja. Z drugimi besedami, konstruirati želimo čim večje podmnožice brez produktov. V grupah $A_n$ in $\mathrm{PSL}_2(\mathbf{F}_p)$ te gotovo ne bodo pozitivne gostote, ko gredo moči grup čez vse meje.

**Zgled 5.2.7** (Kedlaya 1997)**.** Opazujmo alternirajočo grupo $A_n$, ki deluje na množici točk $\{1,2,\ldots,n\}$. Naj bo $T \subseteq \{2,3,\ldots,n\}$ poljubna podmnožica velikosti $t$. Definirajmo množico permutacij

$$S = \{\sigma \in A_n \mid \sigma(1) \in T,\ \sigma(T) \cap T = \emptyset\}.$$

Vsaka permutacija v $S \cdot S$ preslika 1 v $T^c$, zato je $S \cap S \cdot S = \emptyset$ in množica $S$ je brez produktov. Njena gostota v $A_n$ je enaka

$$\frac{1}{n!/2} \cdot t \cdot \binom{n-t}{t} t! \cdot (n-t-1)! \cdot \frac{1}{2} = \frac{t(n-t)!(n-t-1)!}{n!(n-2t)!} = \frac{t}{n} \cdot \frac{\binom{n-t}{t}}{\binom{n-1}{t}}.$$

Z aproksimacijo $\binom{n}{t} \sim (\frac{ne}{t})^t e^{O(-t^2/2n)}$[8] za $t = o(n)$ lahko zadnji izraz poenostavimo do

$$\frac{t}{n} e^{O(t^2/n)}.$$

Optimalno vrednost dosežemo z izbiro $t \sim n^{1/2}$, takrat je gostota množice $S$ v $A_n$ enaka $\sim n^{-1/2}$.

Gowersov izrek zagotavlja, da gostota množice brez produktov v $A_n$ ne more biti večja od $\Theta(n^{-1/3})$. Po drugi strani pa imamo zgled podmnožice brez produktov gostote $\sim n^{-1/2}$. Katera od teh mej je bližje resnični največji možni gostoti podmnožice brez produktov v $A_n$? To vprašanje je bilo razrešeno nedavno v (Keevash-Lifschitz-Minzer 2022), kjer avtorji dokažejo, da je konstrukcija v zadnjem zgledu v resnici optimalna: če je $A \subseteq A_n$ brez produktov največje možne moči, potem je $A$ ali $A^{-1}$ enaka eni od množic iz zadnjega zgleda. Njihov dokaz temelji na ideji, ki smo jo videli v dokazu Rothovega izreka, in sicer bodisi s harmonično analizo dokažemo želeno bodisi ima indikatorska funkcija visoko korelacijo z določenimi nelinearnimi karakterji in je zaradi tega prisotna neka struktura.

Konstrukcija Kedlaya, ki smo jo prikazali, je z nekoliko dodatnega truda[9] posplošljiva na vse podgrupe $G \leq S_n$, ki delujejo tranzitivno na množici $\{1,2,\ldots,n\}$. Vsaka grupa, ki tranzitivno deluje na množici $n$ točk, ima torej podmnožico brez produktov gostote $\sim n^{-1/2}$. V posebnem to velja za grupo $\mathrm{PSL}_2(\mathbf{F}_p)$, ki deluje tranzitivno na projektivni premici $\mathbf{P}^1(\mathbf{F}_p)$ s $p+1$ točkami. Na ta način dobimo podmnožico v $\mathrm{PSL}_2(\mathbf{F}_p)$ brez produktov gostote $\Theta(p^{-1/2})$. Gowersov izrek nam tukaj daje zgornjo mejo $\Theta(p^{-1/3})$ za gostoto množice brez produktov. V tem primeru optimalna ocena za gostoto ni znana.

**Odprt problem 5.2.8.** Kolikšna je gostota največje množice brez produktov v $\mathrm{PSL}_2(\mathbf{F}_p)$, ko gre $p$ čez vse meje?

[7] Del tega si bomo ogledali nekoliko kasneje.

[8] Za funkciji $f, g: \mathbf{N} \to \mathbf{R}$ pišemo $f = O(g)$, če velja $f \ll g$, ter $f = o(g)$, če velja $\lim_{n\to\infty} f(n)/g(n) = 0$.

[9] Definicija množice $S$ je enaka kot za primer $A_n$, dodaten trud je potreben le za oceno njene gostote.

## 5.3 Prepoznavanje komutatorjev

Oglejmo si še en čisto nekomutativen problem, ki na prvi pogled nima veliko skupnega s teorijo upodobitev, nazadnje pa se izkaže, da ga lahko popolnoma razrešimo, če le poznamo tabelo karakterjev grupe.

### Množica komutatorjev

Naj bo $G$ končna grupa in $K(G)$ njena podmnožica, ki sestoji iz elementov, ki so komutatorji v $G$, se pravi

$$K(G) = \{[x,y] \mid x,y \in G\}.$$

Ta množica v splošnem *ni* podgrupa.

**Zgled 5.3.1.** V programskem okolju GAP se ni težko prepričati, da je najmanjša[10] grupa $G$, v kateri $K(G)$ ne sovpada komutatorsko podgrupo $[G,G] = \langle K(G)\rangle$, moči 96. V GAP je ta grupa dostopna pod imenom `SmallGroup(96, 3)`. Podamo jo lahko v njeni permutacijski obliki kot podgrupo $S_{12}$, generirano s permutacijama

$$x = (1\ 3\ 5)(2\ 4\ 6)(7\ 11\ 9)(8\ 12\ 10), \quad y = (3\ 9\ 4\ 10)(5\ 7)(6\ 8)(11\ 12).$$

Hitro izračunamo, da je $|K(G)| = 29$, torej $K(G)$ vsekakor ni podgrupa $G$. Komutatorska podgrupa je le nekoliko večja, $|[G,G]| = 32$. Primer elementa v $[G,G]$, ki ni hkrati v $K(G)$, je permutacija $(5\ 6)(7\ 8)$.

V luči zgleda je teoriji grup vsekakor v interesu, da bi razumela, kdaj dani element $g \in G$ pripada množici $K(G)$. Lahko smo celo bolj natančni in se vprašamo, na koliko načinov lahko $g$ zapišemo kot komutator. V ta namen predpišimo funkcijo

$$N\colon G \to \mathbf{N}_0, \quad g \mapsto |\{(x,y) \in G \times G \mid g = [x,y]\}|.$$

Dokazali bomo naslednjo formulo za izračun funkcije $N$ s pomočjo teorije upodobitev.

**Izrek 5.3.2** (Frobenius)**.** *Naj bo $G$ končna grupa. Za vsak $g \in G$ velja*

$$N(g) = |G| \cdot \sum_{\pi \in \mathrm{Irr}(G)} \frac{\chi_\pi(g)}{\chi_\pi(1)}.$$

### Harmonična analiza

Funkcijo $N$ obravnavajmo kot element prostora $\mathrm{fun}(G,\mathbf{C})$. Ni se težko prepričati, da je $N$ razredna funkcija. Za vsak $z \in G$ namreč velja

$$[zxz^{-1}, zyz^{-1}] = z[x,y]z^{-1},$$

torej vsak par $(x,y)$ z lastnostjo $[x,y] = g$ porodi par $(zxz^{-1}, zyz^{-1})$ z lastnostjo $[zxz^{-1}, zyz^{-1}] = zgz^{-1}$. S tem je $N(g) = N(zgz^{-1})$.

Funkcijo $N$ bomo prepisali v malo bolj nenavadno obliko, ki pa nam bo dobro služila v nadaljevanju. Recimo, da za elementa $x,y \in G$ velja $[x,y] = g$. To enakost interpretiramo kot $x^{-1} \cdot y^{-1}xy = g$, torej je $g$ zapisan kot produkt elementa $x^{-1}$ in elementa, ki je konjugiran $x$. Vsakemu takemu paru $(x,y)$ lahko zato priredimo konjugiranostni razred $\mathcal{C} = x^G$ in elementa $a = x^{-1} \in \mathcal{C}^{-1}$ ter $b = y^{-1}xy \in \mathcal{C}$, za katera velja $a \cdot b = g$. S tem smo opisali prirejanje

$$\psi\colon \{(x,y) \in G \times G \mid g = [x,y]\} \to \{(\mathcal{C},a,b) \mid \mathcal{C} = (a^{-1})^G,\ b \in \mathcal{C},\ a \cdot b = g\}.$$

[10] Natančneje, obstajata dve taki neizomorfni grupi.

To prirejanje *ni* injektivno, saj s trojico $(\mathcal{C}, a, b)$ element $y$ ni enolično določen, pač pa le do odseka po centralizatorju $C_G(a^{-1}) = C_G(a)$ natančno.[11] Torej je $|\psi^{-1}(\mathcal{C}, a, b)| = |C_G(a)| = |G|/|\mathcal{C}|$. S tem lahko izrazimo

$$N(g) = \sum_{\mathcal{C}} \frac{|G|}{|\mathcal{C}|} \cdot |\{(a,b) \in G \times G \mid a \in \mathcal{C}^{-1},\ b \in \mathcal{C},\ a \cdot b = g\}|,$$

pri čemer vsota teče po vseh konjugiranostnih razredih grupe $G$.

Dobljeni zapis funkcije $N$ je priročen, ker je izražen le s konjugiranostnimi razredi in je neodvisen od izbire njihovih konkretnih predstavnikov. S tem je primeren za gnetenje s Fourierovo transformacijo. Najprej opazimo, da lahko drugi faktor zadnje vsote zapišemo kot

$$\sum_{a,b \in G,\ a \cdot b = g} 1_{\mathcal{C}^{-1}}(a) \cdot 1_{\mathcal{C}}(b) = (1_{\mathcal{C}^{-1}} * 1_{\mathcal{C}})(g),$$

zato je

$$N(g) = \sum_{\mathcal{C}} \frac{|G|}{|\mathcal{C}|} \cdot (1_{\mathcal{C}^{-1}} * 1_{\mathcal{C}})(g).$$

Konvolucijo lahko po Fourierovi inverziji razvijemo po karakterjih. Ker gre za karakteristične funkcije konjugiranostnih razredov, je ta razvoj še posebej preprost.

**Trditev 5.3.3.** *Naj bo $G$ končna grupa in $\mathcal{C}_1$, $\mathcal{C}_2$ konjugiranostna razreda v $G$. Velja*

$$1_{\mathcal{C}_1} * 1_{\mathcal{C}_2} = \frac{|\mathcal{C}_1| \cdot |\mathcal{C}_2|}{|G|} \sum_{\pi \in \mathrm{Irr}(G)} \frac{\overline{\chi_\pi(\mathcal{C}_1)} \cdot \overline{\chi_\pi(\mathcal{C}_2)}}{\chi_\pi(1)} \chi_\pi.$$

*Dokaz.* Uporabimo Fourierovo inverzijo za funkcijo $1_{\mathcal{C}_1} * 1_{\mathcal{C}_2}$. Za vsak $g \in G$ dobimo

$$(1_{\mathcal{C}_1} * 1_{\mathcal{C}_2})(g) = \frac{1}{|G|} \sum_{\pi \in \mathrm{Irr}(G)} \chi_\pi(1) \operatorname{tr}\left(\widehat{1_{\mathcal{C}_1} * 1_{\mathcal{C}_2}}(\pi) \cdot \pi(g)\right).$$

Fourierova transformacija konvolucije je produkt Fourierovih transformacij, ki jih za dani karakteristični funkciji ni težko izračunati po lemi o Fourierovi transformaciji razredne funkcije. Za vsako nerazcepno kompleksno upodobitev $\pi$ na prostoru $V$ velja

$$\widehat{1_{\mathcal{C}_1} * 1_{\mathcal{C}_2}}(\pi) = |\mathcal{C}_1| \cdot |\mathcal{C}_2| \cdot \frac{\overline{\chi_\pi(\mathcal{C}_1)} \cdot \overline{\chi_\pi(\mathcal{C}_2)}}{\chi_\pi(1)^2} \cdot \mathrm{id}_V.$$

Trditev je s tem dokazana. □

Trditev uporabimo za razvoj funkcije $N$ kot

$$N(g) = \sum_{\mathcal{C}} \frac{|G|}{|\mathcal{C}|} \cdot \frac{|\mathcal{C}|^2}{|G|} \sum_{\pi \in \mathrm{Irr}(G)} \frac{|\chi_\pi(\mathcal{C})|^2}{\chi_\pi(1)} \chi_\pi(g) = \sum_{\pi \in \mathrm{Irr}(G)} \frac{\chi_\pi(g)}{\chi_\pi(1)} \sum_{\mathcal{C}} |\mathcal{C}| \cdot |\chi_\pi(\mathcal{C})|^2.$$

Zadnja vsota je ravno enaka $|G| \cdot \langle \chi_\pi, \chi_\pi \rangle = |G|$, zato nazadnje sklenemo

$$N(g) = |G| \cdot \sum_{\pi \in \mathrm{Irr}(G)} \frac{\chi_\pi(g)}{\chi_\pi(1)}.$$

S tem smo izpeljali Frobeniusov izrek.

[11] Velja namreč zveza $b = y^{-1} a^{-1} y$.

| | () | (5,6)(7,8) | $y$ | $[x,y]$ | $x$ |
|---|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | 1 | 1 | 1 | $\zeta$ |
| $\chi_3$ | 1 | 1 | 1 | 1 | $\zeta^2$ |
| $\chi_4$ | 3 | 3 | $-1$ | $-1$ | 0 |
| $\chi_5$ | 6 | 2 | 0 | 0 | 0 |
| $\chi_6$ | 3 | $-1$ | 1 | $-1+2i$ | 0 |
| $\chi_7$ | 3 | $-1$ | 1 | $-1-2i$ | 0 |
| $\chi_8$ | 3 | $-1$ | $-1+2i$ | 1 | 0 |
| $\chi_9$ | 3 | $-1$ | $-1-2i$ | 1 | 0 |
| $\chi_{10}$ | 2 | $-2$ | 0 | 0 | $-1$ |
| $\chi_{11}$ | 2 | $-2$ | 0 | 0 | $-\zeta^2$ |
| $\chi_{12}$ | 2 | $-2$ | 0 | 0 | $-\zeta$ |

Tabela 5.1: Del tabele karakterjev `SmallGroup(96, 3)`, kjer je $\zeta = e^{2\pi i/3}$

## Prepoznavanje komutatorjev

S Frobeniusovim izrekom lahko komutatorje v grupi prepoznavamo neposredno iz tabele karakterjev grupe.

**Posledica 5.3.4.** *Naj bo $G$ končna grupa. Za vsak $g \in G$ velja*

$$g \in K(G) \iff \sum_{\pi \in \mathrm{Irr}(G)} \frac{\chi_\pi(g)}{\chi_\pi(1)} \neq 0.$$

**Zgled 5.3.5.** Naj bo $G = \langle x, y \rangle$ grupa moči 96 iz zadnjega zgleda. S predstavljenim algoritmom lahko hitro izračunamo njeno tabelo karakterjev. Grupa ima sicer 12 razredov za konjugiranje, zato je njena tabela karakterjev kar velika.

Iz tabele lahko razberemo, da je element $[x,y]$ res komutator, saj je

$$\sum_{i=1}^{12} \frac{\chi_i([x,y])}{\chi_i(1)} = 3 - \frac{1}{3} - 2 \cdot \frac{1}{3} + 2 \cdot \frac{1}{3} = \frac{8}{3} \neq 0.$$

Po drugi strani je element $(5\ 6)(7\ 8)$ v jedru vseh linearnih upodobitev, zato pripada komutatorski podgrupi $[G,G]$. Hkrati pa ta element *ne* pripada $K(G)$, saj je

$$\sum_{i=1}^{12} \frac{\chi_i((5\ 6)(7\ 8))}{\chi_i(1)} = 3 + 1 + \frac{1}{3} - 4 \cdot \frac{1}{3} - 3 = 0.$$

Njegov konjugiranostni razred v $G$ sestoji iz treh elementov. Ko te elemente dodamo množici $K(G)$, dobimo ravno $[G,G]$.

**Domača naloga 5.3.6.** Iz tabele karakterjev grupe $\mathrm{GL}_2(\mathbf{F}_p)$ razberi, da za $p > 2$ velja

$$K(\mathrm{GL}_2(\mathbf{F}_p)) = \mathrm{SL}_2(\mathbf{F}_p).$$

Iz tabele karakterjev grupe $\mathrm{SL}_2(\mathbf{F}_p)$ razberi, da za $p > 3$ množica komutatorjev v $\mathrm{SL}_2(\mathbf{F}_p)$ vsebuje vse neskalarne elemente. Sklepaj, da je za $p > 3$ vsak element grupe $\mathrm{PSL}_2(\mathbf{F}_p)$ komutator.

Nedavno razrešena Orejeva domneva iz leta 1951 je predvidevala, da je vsak element nekomutativne končne enostavne grupe komutator. Ta domneva je bila potrjena v (Liebeck-O'Brien-Shalev-Tiep 2010). Dokaz sloni na Frobeniusovi formuli za prepoznavanje komutatorjev. Avtorji z uporabo generičnih tabel karakterjev, Deligne-Lusztigove teorije in kar nekaj surove računske moči dokažejo, da prispevki nelinearnih karakterjev v Frobeniusovi formuli nikdar ne uspejo izničiti prispevka trivialnega karakterja.

Velika sestra Orejeve domneve je Thompsonova domneva.

**Odprt problem 5.3.7** (Thompsonova domneva)**.** V vsaki nekomutativni končni enostavni grupi $G$ obstaja konjugiranostni razred $\mathcal{C}$, da je $G = \mathcal{C} \cdot \mathcal{C}$.

Thompsonova domneva implicira Orejevo domnevo. Če namreč najdemo tak konjugiranostni razred $\mathcal{C}$, potem je v posebnem $1 \in \mathcal{C} \cdot \mathcal{C}$, zato je $\mathcal{C} = \mathcal{C}^{-1}$. Torej lahko vsak element $g \in G$ zapišemo kot $g = x^{-1}x^{g_2}$ za nek $x \in \mathcal{C}$, s čimer je $g = [x, g_2]$. Ker je bil $g$ poljuben, je torej vsak element v $G$ komutator, kar je ravno trditev Orejeve domneve.

Ta močnejša domneva je še vedno nerazrešena, je pa v zadnjih letih bilo kar nekaj aktivnosti v zvezi z njeno asimptotsko veljavnostjo. Ti rezultati večinoma temeljijo na teoriji karakterjev na naslednji način. Element $g \in G$ pripada $\mathcal{C} \cdot \mathcal{C}$, če in samo če velja $(1_{\mathcal{C}} * 1_{\mathcal{C}})(g) \neq 0$, kar lahko s pomočjo Fourierove inverzije, kot smo videli v zadnji trditvi, zapišemo kot

$$\sum_{\pi \in \mathrm{Irr}(G)} \frac{\overline{\chi_\pi(\mathcal{C})}^2}{\chi_\pi(1)} \chi_\pi(g) \neq 0.$$

S pomočjo poznavanja karakterjev končnih enostavnih grup je domneva znana za veliko primerov, odprtih pa je še nekaj neskončnih družin matričnih grup nad majhnimi polji, kot je zelo prijazno razloženo v Larsenovem predavanju tukaj.

## 5.4 Slučajni sprehodi

Naj bo $G$ končna grupa in $S$ neka njena podmnožica, ki generira $G$. Vsak element v $G$ lahko torej zapišemo kot produkt elementov iz množice $S$. V tem razdelku bomo raziskali, kaj se zgodi, če elementov iz množice $S$ ne množimo s ciljem, da bi zapisali nek konkreten element, ampak jih namesto tega množimo kar naključno.

### Slučajni sprehod

Naj bo $G$ grupa z generirajočo množico $S$. Enakomerno naključno izberimo element $X_1 = s_1 \in S$. Za tem še enkrat neodvisno izberimo $s_2 \in S$ in izračunajmo $X_2 = s_1 s_2 \in G$. Ta postopek ponavljamo. Ko že imamo $X_i \in G$, enakomerno naključno izberemo element $s_{i+1} \in S$ in izračunamo $X_{i+1} = X_i s_{i+1}$. Če smo torej po nekaj korakih že prišli do elementa $g \in G$, potem je verjetnost, da bomo po naslednjem koraku v elementu $h \in G$, enaka

$$p_S(g,h) = \begin{cases} 1/|S| & \exists s \in S : h = gs, \\ 0 & \text{sicer} \end{cases}$$

Po $n$ korakih tega postopka dobimo element $X_n \in G$, ki je seveda odvisen od izbire vmesnih elementov $s_i \in S$ na vsakem koraku. Temu procesu pravimo **slučajni sprehod** na grupi $G$ z generirajočo množico $S$.

**Zgled 5.4.1.** Naj bo $G = S_n$ in $S$ množica transpozicij v $S_n$. Predstavljajmo si, da imamo pred seboj urejen kup kart. Enakomerno naključno izberemo dve različni karti v tem kupu, eno z levo roko in eno z desno, in ju zamenjamo. Ta postopek ponovimo $n$-krat. Menjava na vsakem koraku ustreza izbiri naključne transpozicije $\sigma \in S$, s katero pomnožimo trenutno permutacijo, ki opisuje stanje, v katerem je kup kart. Slučajni sprehod v tem primeru torej opisuje slučajno mešanje kupa kart.

Nekoliko bolj abstraktno bi lahko na slučajni sprehod gledali kot na zaporedje slučajnih spremenljivk $X_1, X_2, \ldots$ z vrednostmi v $G$, ki pa niso porazdeljene neodvisno, temveč zanje velja **lastnost Markova**, to je

$$\mathbf{P}(X_{i+1} = y \mid X_1 = x_1, \ldots, X_i = x_i) = p_S(x_i, y)$$

za vsak $i \geq 0$ in za vse $x_1, x_2, \ldots, x_i \in G$. Ta lastnost je jasno izpolnjena za slučajni sprehod, kot smo ga opisali zgoraj. Po drugi strani je vsako zaporedje slučajnih spremenljivk z vrednostmi v $G$, ki zadošča lastnosti Markova, *uresničljivo* kot slučajni sprehod. Definiciji sta torej ekvivalentni.

Slučajna spremenljivka $X_n$ nam pove, v katerem elementu se nahajamo po $n$ korakih slučajnega sprehoda. Naš cilj je analizirati porazdelitev te slučajne spremenljivke v odvisnosti od $n$ in še posebej v limiti, ko gre $n$ čez vse meje. Kot bomo videli, je tudi ta problem izrazljiv v jeziku teorije upodobitev.

## Operator Markova

Po $n$ korakih slučajnega sprehoda se znajdemo v nedoločenem elementu grupe $G$. Uvedimo funkcijo

$$\mu_n : G \to \mathbf{C}, \quad g \mapsto \mathbf{P}(X_n = g),$$

ki meri verjetnost, da smo v danem elementu. Ta funkcija torej ni nič drugega kot porazdelitvena funkcija slučajne spremenljivke $X_n$. Slučajni sprehod se začne v 1, zato je $\mu_0 = 1_1$.

Vrednosti funkcije $\mu_n$ lahko izračunamo induktivno na $n$, upoštevajoč lastnost Markova. Velja

$$\mu_n(g) = \sum_{h \in G} \mathbf{P}(X_n = g \mid X_{n-1} = h)\mathbf{P}(X_{n-1} = h) = \sum_{h \in G} p_S(h,g) \cdot \mu_{n-1}(h).$$

Vrednosti $p_S(h,g)$ so neničelne le, kadar je $g \in hS$. Dobimo torej

$$\mu_n(g) = \frac{1}{|S|} \sum_{h \in gS^{-1}} \mu_{n-1}(h) = \frac{1}{|S|} \sum_{x \in G} \mu_{n-1}(gx^{-1}) 1_S(x).$$

Zadnjo vsoto prepoznamo kot konvolucijo

$$\left(\mu_{n-1} * \frac{1_S}{|S|}\right)(g),$$

ki jo lahko zapišemo s pomočjo Fourierove transformacije in nazadnje dobimo

$$\mu_n = \widehat{\frac{1_S}{|S|}}(\rho_{\mathrm{fun}}) \cdot \mu_{n-1}.$$

Rekurzivna zveza za izračun porazdelitvene funkcije $\mu_n$ iz $\mu_{n-1}$ se torej izrazi s pomočjo Fourierove transformacije normalizirane karakteristične funkcije generirajoče množice $S$ v regularni upodobitvi. Tej linearni preslikavi pravimo **operator Markova** in jo označimo kot

$$M = \widehat{\frac{1_S}{|S|}}(\rho_{\mathrm{fun}}) = \frac{1}{|S|} \sum_{x \in S} \rho_{\mathrm{fun}}(x)^*.$$

Za poljubno funkcijo $f \in \mathrm{fun}(G, \mathbf{C})$ je

$$(M \cdot f)(g) = \frac{1}{|S|} \sum_{x \in S} f(gx^{-1}),$$

torej $Mf$ v točki $g \in G$ izračuna povprečje funkcije $f$ po vseh elementih, ki v slučajnem sprehodu lahko vodijo v $g$.

**Trditev 5.4.2.** *Za slučajni sprehod na grupi z operatorjem Markova $M$ je*

$$\mu_n = M^n \cdot 1_1.$$

Operator Markova lahko zapišemo v naravni bazi karakterističnih funkcij in s tem dobimo matriko razsežnosti $|G| \times |G|$, ki ima v vsakem stolpcu $|S|$ neničelnih vrednosti, vsaka od njih je enaka $1/|S|$. Ob dodatnih predpostavkah na množico $S$ dobimo dodatne lastnosti te matrike. Če je na primer množica $S$ simetrična, kar pomeni, da je za vsak $s \in S$ tudi $s^{-1} \in S$, potem je opisana matrika za $M$ *simetrična* in zato nujno *diagonalizabilna* v ortonormirani bazi nad realnimi števili. V tem primeru ni težko izračunati visokih potenc $M$ in s tem $\mu_n$.

**Zgled 5.4.3.** Opazujmo simetrično grupo $S_3$ z generirajočo množico transpozicij $S = \{(1\,2), (1\,3), (2\,3)\}$. Ta množica je simetrična. Elemente grupe $S_3$ uredimo po vrsti kot

$$(), (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2).$$

Operator Markova je v standardni bazi karakterističnih funkcij elementov grupe enak

$$M = \frac{1}{3}\begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

Ta matrika je simetrična. Njen karakteristični polinom je enak $\lambda^6 - \lambda^4$, zato dobimo lastne vrednosti $(1,0,0,0,0,-1)$. Lastni vektor lastne vrednosti 1 je konstantni vektor 1, ki ustreza konstantni funkciji na $S_3$. Lastni vektor lastne vrednosti $-1$ je vektor sgn. Funkcijo $1_1$ razvijemo po lastnih vektorjih kot

$$1_1 = \langle 1_1, 1\rangle + \langle 1_1, \mathrm{sgn}\rangle \,\mathrm{sgn} + k,$$

pri čemer je $k \in \ker M$. Velja torej

$$1_1 = \frac{1}{6} + \frac{1}{6}\,\mathrm{sgn} + k.$$

Za vsak $n$ s tem dobimo

$$\mu_n = M^n \cdot 1_1 = \frac{1}{6} + \frac{(-1)^n}{6} \cdot \mathrm{sgn} = \begin{cases} \frac{1}{3} \cdot 1_{A_3} & n \equiv 0 \pmod 2, \\ \frac{1}{3} \cdot 1_{S_3 \setminus A_3} & n \equiv 1 \pmod 2. \end{cases}$$

Porazdelitev po sodo mnogo korakih je torej enakomerna na sodih permutacijah $A_3$, po liho mnogo korakih pa enakomerna na lihih permutacijah $S_3 \setminus A_3$.

Enakomerno porazdelitev na množici $A \subseteq G$ označimo z $U_A$. Velja $U_A = 1/|A| \cdot 1_A$. Enakomerna porazdelitev $U_G$ je vselej lastni vektor operatorja Markova z lastno vrednostjo 1. Preostalih lastnih vrednosti pa v splošnem ni lahko določiti.

**Domača naloga 5.4.4.** Naj bo $G$ končna grupa z generirajočo množico $S$ in operatorjem Markova $M$. Dokaži, da za vsako funkcijo $f \in \mathrm{fun}(G, \mathbf{C})$ velja $\|Mf\| \leq \|f\|$. Sklepaj, da so vse lastne vrednosti $M$ po absolutni vrednosti kvečjemu 1. Kaj je lastni vektor za lastno vrednost 1? Kdaj je $-1$ lastna vrednost in kaj je pripadajoči lastni vektor?

**Domača naloga 5.4.5.** Naj bo $p$ praštevilo in $S \subseteq \mathbf{F}_p$. Za vsak $i \in \mathbf{F}_p$ naj bo $R_i$ število rešitev enačbe $x_1 + x_2 + \cdots + x_p = i$, kjer so vse spremenljivke v $S$. Dokaži, da je $R_i/|S|^p = \mu_p(i)$, kjer je $\mu_p$ porazdelitvena funkcija slučajnega sprehoda v grupi $\mathbf{F}_p$ z množico $S$. Sklepaj, da je $R_0 \equiv |S| \pmod p$ in $R_i \equiv 0 \pmod p$ za $i \neq 0$.[12]

## Slučajni sprehod s konjugiranostnim razredom

Zelo dobro razumemo primer, ko je $S$ konjugiranostni razred v $G$, saj lahko Fourierovo transformacijo razredne funkcije eksplicitno izračunamo v odvisnosti od karakterjev. V tem primeru lahko eksplicitno določimo tudi vse lastne vektorje, ki jih dobimo kot generatorje izotipičnih komponent nerazcepnih upodobitev, ko smo videli v predstavljenem algoritmu za izračun tabele karakterjev.

**Trditev 5.4.6.** *Za slučajni sprehod na grupi $G$ z generirajočo množico $C$, kjer je $C$ konjugiranostni razred v $G$, je operator Markova diagonalizabilen z lastnimi vrednostmi*

$$r_\pi(C) = \frac{\overline{\chi_\pi(C)}}{\chi_\pi(1)}$$

*za vsako nerazcepno kompleksno upodobitev $\pi \in \mathrm{Irr}(G)$, pri čemer je večkratnost vsake lastne vrednosti enaka $\chi_\pi(1)^2$.*

[12] S tem si le slučajni korak stran od rešitve naloge I/3 s tekmovanja IMC 2022.

Operator Markova $M$ slučajnega sprehoda na $G$ z generirajočo množico $\mathcal{C}$, pri čemer je $\mathcal{C}$ konjugiranostni razred v $G$, deluje na vsaki od izotipičnih komponent regularne upodobitve kot skalarni večkratnik identitete z znamimi skalarji. Da lahko razumemo $\mu_n = M^n \cdot 1_1$, moramo najprej razviti funkcijo $1_1$ po izotipičnih komponentah. To naredimo, kot smo že, s pomočjo Fourierovih transformacij nerazcepnih karakterjev. Projekcija $1_1$ na $\pi$-izotipično komponento je enaka

$$v_\pi = \frac{\chi_\pi(1)}{|G|} \cdot \chi_\pi,$$

zato dobimo $1_1 = \sum_{\pi \in \mathrm{Irr}(G)} v_\pi$. Vektor $v_\pi$ je lastni vektor za $M$ z lastno vrednostjo $r_\pi(\mathcal{C})$. V tej množici lastnih vektorjev lahko torej funkcijo $\mu_n$ razvijemo kot

$$\mu_n = M^n \cdot 1_1 = \sum_{\pi \in \mathrm{Irr}(G)} r_\pi(\mathcal{C})^n \cdot v_\pi.$$

Za razumevanje asimptotskega obnašanja $\mu_n$ je pomembno poznati $|r_\pi(\mathcal{C})|$. Če je namreč $|r_\pi(\mathcal{C})| < 1$, potem vrednosti $r_\pi(\mathcal{C})^n$ konvergirajo k 0, ko gre $n$ čez vse meje.

**Lema 5.4.7.** *Za $\pi \in \mathrm{Irr}(G)$ drži $|r_\pi(\mathcal{C})| \leq 1$, pri čemer velja enakost natanko tedaj, ko je*

$$\{[g,c] \mid g \in G, c \in \mathcal{C}\} \subseteq \ker \pi.$$

*Dokaz.* Naj bo $x \in \mathcal{C}$. Enakost $|r_\pi(x)| = 1$ velja natanko tedaj, ko je $\pi(x)$ skalarna matrika. Taka matrika komutira z vsemi elementi $\pi(g)$ za $g \in G$. Velja torej $\pi([g,\mathcal{C}]) = 1$ za vsak $g \in G$. To pomeni, da je $[G,\mathcal{C}] \subseteq \ker \pi$, kar je enakovredno vsebovanosti v trditvi. Premislimo še, da za matriko $A$ velja $[A,\pi(g)] = 1$ za vse $g \in G$, če in samo če je $A$ skalarna matrika. Vektorski prostor, ki ga razpenjajo matrike $\pi(g)$ za $g \in G$, je enak prostoru matrik $M_{\deg(\pi)}(\mathbf{C})$,[13] v tej algebri pa so centralne matrike ravno skalarne matrike. Dokaz je s tem zaključen. □

Zberimo prispevke z maksimalno vrednostjo $r_\pi(\mathcal{C})$ v množico

$$X_\mathcal{C} = \{\pi \in \mathrm{Irr}(G) \mid |r_\pi(\mathcal{C})| = 1\}.$$

Velja torej

$$\mu_n - \sum_{\pi \in X_\mathcal{C}} r_\pi(\mathcal{C})^n \cdot v_\pi = \sum_{\pi \in \mathrm{Irr}(G) \setminus X_\mathcal{C}} r_\pi(\mathcal{C})^n \cdot v_\pi.$$

Prispevki $r_\pi(\mathcal{C})^n$ za $\pi$ zunaj $X_\mathcal{C}$ konvergirajo k 0 za velike vrednosti $n$ in zatorej dobimo

$$\lim_{n\to\infty} \left( \mu_n - \sum_{\pi \in X_\mathcal{C}} r_\pi(\mathcal{C})^n \cdot v_\pi \right) = 0.$$

Za konkretne grupe lahko s tabelo karakterjev ali upoštevanjem kakšnih dodatnih lastnosti eksplicitno izračunamo zadnjo vsoto in s tem določimo limitno porazdelitev $\mu_n$, če ta sploh obstaja.

**Domača naloga 5.4.8.** Naj bo $G$ nekomutativna končna enostavna grupa. Dokaži, da vsak netrivialen konjugiranostni razred $\mathcal{C}$ generira $G$ in da velja $X_\mathcal{C} = \{\mathbf{1}\}$. Sklepaj, da je $\lim_{n\to\infty} \mu_n = U_G$.

Napako pri aproksimaciji porazdelitev $\mu_n$ in vsoto prispevkov po $X_\mathcal{C}$ izrazimo s pomočjo norme $\|f\|_1 = \sum_{g \in G} |f(g)|$ za funkcijo $f \in \mathrm{fun}(G,\mathbf{C})$.[14] Naj bo $0 < \theta < 1$ konstanta. **Čas mešanja**[15] $t_{mix}(\theta)$ je najmanjše število $n$, pri katerem je

$$\|\mu_n - \sum_{\pi \in X_\mathcal{C}} r_\pi(\mathcal{C})^n \cdot v_\pi\|_1 \leq \theta.$$

[13] Če namreč ne razpenjajo celotnega prostora matrik, potem obstaja neka netrivialna linearna kombinacija matričnih koeficientov $\{f_{i,j} \mid 1 \leq i,j \leq \deg(\pi)\}$, ki je v vseh elementih $g \in G$ ničelna. To je protislovje z linearno neodvisnostjo matričnih koeficientov nerazcepne upodobitve $\pi$.

[14] Za primerjavo porazdelitev ne uporabljamo standardne norme $\|f\| = \langle f,f\rangle^{1/2}$, ampak normo $\|f\|_1$. Razlog za to je naslednji. Opazujmo družino simetričnih grup $S_n$. Potem je $\|U_{A_n} - U_{S_n}\|^2 = 1/|S_n|$, kar konvergira k 0 za $n \to \infty$, čeprav sta porazdelitvi očitno različni. Norma $\|\cdot\|_1$ nima te pomanjkljivosti; velja $\|U_{A_n} - U_{S_n}\|_1 = 1$.

[15] Rečemo tudi, da se slučajni sprehod **dobro premeša** po času $t_{mix}(\theta)$. Ta koncept je seveda odvisen od izbire konstante $\theta$, a po navadi za $\theta$ vzamemo kar neko majhno konstanto, na primer $\theta = 10^{-2}$.

Čas mešanja in s tem hitrost konvergence k limitni porazdelitvi lahko kvantitativno nadziramo, če dobro poznamo vrednosti $r_\pi(\mathcal{C})$ za $\pi$ zunaj $X_\mathcal{C}$, saj velja

$$||\mu_n - \sum_{\pi \in X_\mathcal{C}} r_\pi(\mathcal{C})^n \cdot v_\pi||_1 \leq \sum_{\pi \in \mathrm{Irr}(G) \setminus X_\mathcal{C}} |r_\pi(\mathcal{C})|^n \cdot ||v_\pi||_1.$$

Normo baznih vektorjev $v_\pi$ lahko omejimo s Cauchy-Schwartzovo neenakostjo kot

$$||v_\pi||_1 = \frac{\chi_\pi(1)}{|G|} \sum_{g \in G} |\chi_\pi(g)| \leq \frac{\chi_\pi(1)}{|G|} \sqrt{|G| \cdot \sum_{g \in G} |\chi_\pi(g)|^2} = \chi_\pi(1).$$

S tem velja

$$||\mu_n - \sum_{\pi \in X_\mathcal{C}} r_\pi(\mathcal{C})^n \cdot v_\pi||_1 \leq \left( \max_{\pi \in \mathrm{Irr}(G) \setminus X_\mathcal{C}} |r_\pi(\mathcal{C})| \right)^n \cdot \sum_{\pi \in \mathrm{Irr}(G) \setminus X_\mathcal{C}} \chi_\pi(1).$$

Če vsoto karakterjev zelo grobo navzgor ocenimo z $|G|$ in upoštevamo, da je

$$\max_{\pi \in \mathrm{Irr}(G) \setminus X_\mathcal{C}} |r_\pi(\mathcal{C})| \leq 1 - \epsilon < 1$$

za nek $\epsilon > 0$, potem velja

$$||\mu_n - \sum_{\pi \in X_\mathcal{C}} r_\pi(\mathcal{C})^n \cdot v_\pi||_1 \leq (1-\epsilon)^n \cdot |G|.$$

Napaka med porazdelitvama pade pod konstanto $\theta$, če je le

$$n \sim (\log|G| - \log\theta)/(-\log(1-\epsilon)) = O_{\epsilon,\theta}(\log|G|).$$

Takrat bo za majhno konstanto $\theta$ slučajni sprehod zelo blizu svoje limitne porazdelitve, če ta sploh obstaja. Čas mešanja je torej logaritmičen v velikosti grupe.

## Naključno množenje podobnih matrik

Oglejmo si konkreten primer slučajnega sprehoda. Obravnavajmo grupo $G_p = \mathrm{GL}_2(\mathbf{F}_p)$ za $p > 3$, ki smo jo že dodobra spoznali. V njej za generirajočo množico izberimo konjugiranostni razred $\mathcal{C}$ regularnih polenostavnih elementov, ki so podobni matriki

$$A = \begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix},$$

kjer je $\delta$ generator ciklične grupe obrnljivih elementov končnega polja $\mathbf{F}_p^*$. Generirajoča množica sestoji torej iz vseh matrik, ki so v $G_p$ podobne $A$.

### Generiranje grupe

Preverimo najprej, da množica $\mathcal{C}$ res generira $G_p$. Ker je $G_p$ končna grupa, velja $A^{-1} \in \langle \mathcal{C} \rangle$ in zato je vsaka matrika, ki je podobna $A^{-1}$, tudi v $\langle \mathcal{C} \rangle$. S tem velja

$$[S_+, A] = (S_+^{-1} A^{-1} S_+) A = S_+^{\delta^{-1}-1} \in \langle \mathcal{C} \rangle.$$

Ker je $p > 3$, je $\delta \neq \pm 1$, zato dobimo $S_+ \in \langle \mathcal{C} \rangle$. Sorodno sklepamo za matriko $S_-$. S tem dobimo

$$\langle \mathcal{C} \rangle \geq \langle S_+, S_- \rangle = \mathrm{SL}_2(\mathbf{F}_p).$$

Ker je $\delta$ generator $\mathbf{F}_p^*$, grupa $\langle \mathcal{C} \rangle$ vsebuje matrike z vsemi možnimi determinantami. Od tod sledi, da $\mathcal{C}$ res generira grupo $G_p$.

| | $\chi_\pi(1)$ | $\overline{\chi_\pi(\mathcal{C})}$ | $r_\pi(\mathcal{C})$ | $\lvert r_\pi(\mathcal{C})\rvert$ |
|---|---|---|---|---|
| $\chi\circ\det$ | 1 | $\overline{\chi(\delta)}$ | $\overline{\chi(\delta)}$ | 1 |
| $\mathrm{St}(\chi)$ | $p$ | $\overline{\chi(\delta)}$ | $\overline{\chi(\delta)}/p$ | $1/p$ |
| $\pi(\chi_1,\chi_2)$ | $p+1$ | $\overline{\chi_1(\delta)}+\overline{\chi_2(\delta)}$ | $(\overline{\chi_1(\delta)}+\overline{\chi_2(\delta)})/(p+1)$ | $<2/(p+1)$ |
| $\zeta_\theta$ | $p-1$ | 0 | 0 | 0 |

Tabela 5.2: Lastne vrednosti operatorja Markova grupe $G_p$ z generirajočo množico $\mathcal{C}$

### Limitna porazdelitev sprehoda

Za razumevanje limitnega obnašanja porazdelitve $\mu_n$ moramo najprej določiti vrednosti $r_\pi(\mathcal{C})$. Tabelo karakterjev grupe $G_p$ v celoti poznamo.

Množica $X_\mathcal{C}$ v tem primeru sestoji iz linearnih upodobitev. Vsota prispevkov porazdelitev po $X_\mathcal{C}$ je zato enaka

$$\sum_{\pi\in X_\mathcal{C}} r_\pi(\mathcal{C})^n\cdot v_\pi = \sum_{\chi\in\mathrm{Irr}(\mathbf{F}_p^*)} \overline{\chi(\delta^n)}\cdot\frac{1}{|G_p|}\chi\circ\det.$$

Upoštevamo drugo ortogonalnostno relacijo in dobimo

$$\frac{1}{|G_p|}\cdot\left(g\mapsto\begin{cases}|\mathbf{F}_p^*| & \det g=\delta^n\\ 0 & \text{sicer.}\end{cases}\right)=\frac{1}{|\mathrm{SL}_2(\mathbf{F}_p)|}\cdot 1_{\det^{-1}(\delta^n)}=U_{\det^{-1}(\delta^n)}.$$

V tem primeru kandidat za limitno porazdelitev v resnici ne konvergira, saj za različne vrednosti $n$ po modulu $p-1$ dobimo bistveno različne porazdelitve. Ko je $n$ deljiv s $p-1$, dobimo enakomerno porazdelitev na $\mathrm{SL}_2(\mathbf{F}_p)$.

### Hitrost konvergence

Pogovorimo se še o oceni napake pri aproksimaciji $\mu_n$ s kandidatom za limitno porazdelitev. Za $\pi$ zunaj $X_\mathcal{C}$ ocenimo

$$\max_{\pi\in\mathrm{Irr}(G_p)\setminus X_\mathcal{C}}|r_\pi(\mathcal{C})|<\frac{2}{p},\qquad\sum_{\pi\in\mathrm{Irr}(G_p)\setminus X_\mathcal{C}}\chi_\pi(1)<p^3.$$

Velja torej

$$\|\mu_n-U_{\det^{-1}(\rho^n)}\|_1\le\frac{2^n}{p^{n-3}}.$$

Napaka zelo hitro upade, pod $\theta$ je že pri $n=(3\log p-\log\theta)/(\log p-\log 2)\sim 3$.[16] Težava je le ta, da $\mu_n$ v resnici ne konvergira. Da to popravimo, moramo opazovati obnašanje po aritmetičnih zaporedjih z razliko $p-1$. Za vse dovolj velike $p$ tako dobimo zelo dobro aproksimacijo

$$\mu_{p-1}\approx U_{\mathrm{SL}_2(\mathbf{F}_p)}.$$

Če torej v $G_p$ naključno zmnožimo $p-1$ matrik v $\mathcal{C}$ za dovolj velik $p$, dobimo (skoraj) naključno matriko v $\mathrm{SL}_2(\mathbf{F}_p)$. Napaka sicer pade ekstremno hitro, a linearni karakterji obremenijo sprehod do te mere, da ne moremo izkoristiti majhne napake že po 3 korakih, niti ne po $\log|G_p|\sim\log p$ korakih, temveč šele po $p-1\sim|G_p|^{1/4}$ korakih.

**Domača naloga 5.4.9.** Obravnavaj slučajni sprehod v $\mathrm{PSL}_2(\mathbf{F}_p)$ glede na neki konjugiranostni razred $\mathcal{C}$. V tem primeru bo $\lim_{n\to\infty}\mu_n$ enakomerna porazdelitev na $\mathrm{PSL}_2(\mathbf{F}_p)$. S pomočjo tabele karakterjev oceni hitrost konvergence in pokaži, da dosežemo približno naključno matriko v $\mathrm{PSL}_2(\mathbf{F}_p)$ veliko hitreje kot po $p-1$ korakih.

**Domača naloga 5.4.10** (Diaconis-Shashahani 1981)**.** Obravnavaj slučajni sprehod v $S_n$ glede na generirajočo množico $S$, ki sestoji iz transpozicij in enote $()$. To ni konjugiranostni razred, je pa unija dveh razredov. Premisli, kako lahko argumente posplošiš na to situacijo. Določi limitno porazdelitev. Ocena hitrosti konvergence bo zahtevala kar nekaj truda. Pomagaš si lahko z (Miščič 2022).

[16] Tako hitra konvergenca je posledica dejstva, da je konjugiranostni razred $\mathcal{C}$ v $G_p$ zelo velik, $\log|\mathcal{C}|\sim\log|G_p|$, in da imamo zelo dobre ocene za $r_\pi(\mathcal{C})$.

## Konvergenca v družinah

Za vsako konkretno nekomutativno končno enostavno grupo $G$ jasno velja, da so vse lastne vrednosti operatorja $M$, razen 1, po absolutni vrednosti kvečjemu $1-\epsilon$ za nek $\epsilon = \epsilon(G) > 0$. V tem primeru rečemo, da je grupa $G$ **$\epsilon$-ekspanzivna** glede na generirajočo množico $S$. Slučajni sprehod v taki grupi se dobro premeša po $O_\epsilon(\log|G|)$ korakih. Težave nastopijo, ko skušamo ta argument uporabiti za celo družino grup, saj se lahko zgodi, da z večanjem parametra $n$ vrednost ekspanzivnosti $\epsilon = \epsilon_n$ nujno konvergira k 0. Ta fenomen vidimo v primeru družine $A_n$ in konjugiranostnega razreda 3-ciklov.

**Domača naloga 5.4.11** (Helfgott-Seress-Zuk 2015)**.** Obravnavaj slučajni sprehod v $A_n$ glede na konjugiranostni razred 3-ciklov $\mathcal{C}$. Premisli, da je $\max_{\mathbf{1}\neq\pi\in\mathrm{Irr}(A_n)} |r_\pi(\mathcal{C})| = 1 - 3/(n-1)$ in s tem oceni hitrost konvergence.

V taki situaciji se slučajni sprehodi zmešajo dobro po $O_\epsilon(\log|G|)$ korakih, kar je lahko bistveno večje od $O(\log|G|)$ in torej asimptotsko gledano v resnici ni logaritmično v velikosti grupe.

Družini grup $(G_i, S_i)_{i\in\mathbf{N}}$, kjer je $G_i = \langle S_i\rangle$, pravimo **ekspanzivna družina**,[17] kadar obstaja konstanta $\epsilon > 0$, za katero je vsaka grupa $G_i$ $\epsilon$-ekspanzivna glede na $S_i$. V ekspanzivnih družinah se slučajni sprehodi enakomerno zelo hitro dobro premešajo.

Vsaka družina je ekspanzivna, če za generatorsko množico vzamemo kar $S_i = G_i$ za vsak $i$. V tem primeru je namreč operator Markova enak povprečju $\mathbf{E}(\rho_{\mathrm{fun}})$, ki je projektor na trivialno podupodobitev regularne, zato so vse njegove netrivialne lastne vrednosti ničelne. Želimo si ekspanzivnih družin, v katerih je množica $S_i$ čim manjša, po možnosti celo omejene velikosti v vseh članicah družine, na primer $|S_i| \leq 100$ za vsak $i$. V takih ekspanzivnih družinah lahko enakomerno zelo hitro z zaporednim vzorčenjem v množici omejene velikosti dobimo približno enakomerno naključne elemente ogromnih grup.

S pomočjo teorije upodobitev in poznavanja določenih lastnosti karakterjev končnih enostavnih grup $\mathrm{PSL}_n(\mathbf{F}_p)$ ni pretežko posplošiti zgleda iz zadnjega razdelka.[18] Zanimivo je, da isti rezultat ne deluje za družino alternirajočih grup.

**Izrek 5.4.12.** *Naj bo $n \geq 2$ fiksno naravno število. Za vsak $p \in \mathbf{P}$ naj bo $\mathcal{C}_{n,p}$ netrivialen konjugiranostni razred v $\mathrm{PSL}_n(\mathbf{F}_p)$. Tedaj je družina grup $(\mathrm{PSL}_n(\mathbf{F}_p), \mathcal{C}_{n,p})_{p\in\mathbf{P}}$ ekspanzivna.*

Bistveno bolj netrivialen pa je dokaz naslednjega izreka, po katerem lahko vse nekomutativne končne enostavne grupe napravimo za ekspanzivne z generatorskimi množicami omejene velikosti.

**Izrek 5.4.13** (Kassabov 2007, Kassabov-Lubotzky-Nikolov 2006, Breuillard-Green-Tao 2011)**.** *Obstaja konstanta $C > 0$, tako da je družina nekomutativnih končnih enostavnih grup ekspanzivna družina glede na generatorske množice velikosti kvečjemu $C$.*

Izrek nam zagotavlja obstoj neke ne prevelike generirajoče množice v končnih enostavnih grupah, glede na katere se slučajni sprehodi enakomerno zelo hitro dobro premešajo. Še težje pa je povedati kaj bolj konkretnega o teh generirajočih množicah. Za primer $A_n$ so te množice konstruirane v (Kassabov 2007) s pomočjo neke naključne metode. Dokaz omejitev absolutnih vrednosti lastnih vrednosti operatorja Markova sloni na teoriji upodobitev, a je precej bolj zahteven od tega, ki smo si ga ogledali mi, saj so te generatorske množice daleč od konjugiranostnih razredov. Pred nedavnim so se našle celo eksplicitne konstrukcije generirajočih množic $A_n$, glede na katere dobimo ekspanzivno družino (Caprace-Kassabov 2022). Tudi tukaj je ključna teorija upodobitev, a v igro vstopijo neskončne grupe avtomorfizmov polinomskih kolobarjev nad končnim poljem.

Dokazi ekspanzivnosti za generatorske množice, ki niso konjugiranostni razredi, po navadi potekajo na obraten način, kot bi pričakovali. Omejenost absolutnih vrednosti netrivialnih lastnih vrednosti operatorja Markova namreč lahko dokažemo, če premislimo, da se slučajni sprehodi enakomerno zelo

[17] Angleško *expander family*. Ime izhaja iz alternativne karakterizacije teh družin v teoriji grafov.
[18] Glej pregledni članek (Liebeck 2017).

hitro premešajo.[19] Primer uporabe te tehnike par excellence je naslednji rezultat, ki med drugim presenetljivo sloni na Gowersovem rezultatu o zgornji meji gostote množic brez produktov.

**Izrek 5.4.14** (Bourgain-Gamburd 2008, Breuillard-Green-Guralnick-Tao 2015)**.** *Naj bo $n$* fiksno *naravno število. Za vsak $p \in \mathbf{P}$ naj bo enakomerno naključno izberemo dva elementa $x, y \in \mathrm{PSL}_n(\mathbf{F}_p)$ in tvorimo množico $S_{n,p,x,y} = \{x, x^{-1}, y, y^{-1}\}$. Tedaj obstaja $\epsilon = \epsilon(n)$, da je*

$$\lim_{p\to\infty} \mathbf{P}_{x,y}(\mathrm{PSL}_n(\mathbf{F}_p) \textit{ je } \epsilon\textit{-ekspanzivna glede na } S_{n,p,x,y}) = 1.$$

Če sprostimo $n$ in opazujemo matrike velikih razsežnosti, cel kup tehnik v dokazu propade. Za te matrike ni znano in med strokovnjaki niti ni jasnega konsenza, ali so asimptotsko gledano skoraj gotovo ekspanzivne. Preprost primer, ki bi verjetno odprl vrata v velike matrike, je družina alternirajočih grup.

**Odprt problem 5.4.15.** V vsaki alternirajoči grupi $A_n$ enakomerno naključno izberemo dva elementa $x, y \in A_n$ in tvorimo množico $S_{n,x,y} = \{x, x^{-1}, y, y^{-1}\}$. Ali obstaja absolutna konstanta $\epsilon > 0$, da je

$$\lim_{n\to\infty} \mathbf{P}_{x,y}(A_n \text{ je } \epsilon\text{-ekspanzivna glede na } S_{n,x,y}) = 1?$$

Vzpodbuden delni rezultat je, da asimptotska visoko verjetna ekspanzivnost drži za družino določenih *kvocientov Cayleyjevih grafov* simetričnih grup, kot je predstavljeno v (Milanez 2022). Ti rezultati so bili nedavno posplošeni do *precej velikih* kvocientov Cayleyjevih grafov v (Cassidy 2025).

[19] Ni težko premisliti, da sta ta dva koncepta ekvivalentna. Čas mešanja v vsaki članici družine $G_i$ je $O(\log|G_i|)$, če in samo če je družina ekspanzivna.

# Poglavje 6

# Razširjeni zgledi – neskončni

V tem zaključnem poglavju si bomo ogledali nekaj zgledov iz teorije upodobitev neskončnih grup. Tukaj ni enotne teorije, s katero bi lahko obravnavali vsako grupo, obstajajo pa družine grup, znotraj katerih lahko razumemo upodobitve na enoten način. Ne bomo razvijali splošne teorije, temveč si bomo ogledali le konkretne, a reprezentativne predstavnike nekaterih izmed pomembnih družin neskončnih grup.

## Ozaljšane upodobitve

V svetu neskončih grup po navadi ne obravnavamo čisto vseh abstraktnih upodobitev, ker na ta način dobimo preprosto *preveč* upodobitev, ki niti niso *smiselne*.

**Zgled 6.0.1.** Opazujmo grupo $\mathbf{R}$. Vemo že, da je vsaka njena končno razsežna nerazcepna kompleksna upodobitev enorazsežna, torej oblike $\chi\colon \mathbf{R} \to \mathbf{C}^*$ za nek homomorfizem $\chi$. Premislimo, da je takih homomorfizmov *ogromno*. Grupa $\mathbf{R}$ je kot abelova grupa izomorfna neskončni direktni vsoti kopij $\mathbf{Z}$. Za vsak nabor realnih števil $x_1, x_2, \ldots, x_k$, ki so $\mathbf{Z}$-linearno neodvisna, lahko izberemo poljuben nabor kompleksnih števil $z_1, z_2, \ldots, z_k$ in dobimo homomorfizem abelovih grup $\chi\colon \mathbf{R} \to \mathbf{C}^*$ z lastnostjo $\chi(x_i) = z_i$ za vsak $i$.

To težavo zaobidemo tako, da ne opazujemo poljubnih upodobitev, temveč jih ozaljšamo z dodatnimi restrikcijami v odvisnosti od grupe, ki jo opazujemo.

### Zveznost

Grupa $\mathbf{R}$ ni le abstraktna grupa, temveč je opremljena s topologijo. Abstraktneje je **topološka grupa** množica, ki je hkrati grupa in topološki prostor, obe strukturi pa sta uglašeni s pogojem, da sta operaciji množenja in invertiranja zvezni.

**Zgled 6.0.2.** Grupe $\mathbf{R}$, $\mathbf{R}^3$, $\mathbf{R}^*$, $\mathrm{U}_1(\mathbf{C}) = S^1$, $\mathrm{SU}_2(\mathbf{C})$, $\mathrm{SO}_3(\mathbf{R})$, $\mathrm{GL}_3(\mathbf{C})$, $\mathrm{SL}_2(\mathbf{R})$, $\mathrm{SL}_2(\mathbf{Z})$ so topološke grupe. Vsaka od njih je opremljena z naravno topologijo, ki jo podeduje iz ambientalnega evklidskega prostora. Grupa $\mathrm{SL}_2(\mathbf{Z})$ sicer podeduje le *diskretno* topologijo.

Končno razsežna[1] kompleksna upodobitev $\rho\colon G \to \mathrm{GL}_n(\mathbf{C})$ topološke grupe $G$ je **zvezna**, kadar je zvezna kot preslikava, pri čemer prostor $\mathrm{GL}_n(\mathbf{C}) \subseteq \mathbf{C}^{n^2}$ opremimo z inducirano topologijo.

**Zgled 6.0.3.** Nore upodobitve grupe $\mathbf{R}$, ki smo jih konstruirali v zadnjem zgledu, povečini niso zvezne. So pa za vsak parameter $\zeta \in \mathbf{C}$ zvezne upodobitve oblike

$$\chi_\zeta\colon \mathbf{R} \to \mathbf{C}^*, \quad x \mapsto e^{\zeta x}.$$

[1] Če bi želeli obravnavati tudi neskončno razsežne upodobitve na prostoru $V$, bi morali to definicijo nekoliko popraviti. Najprej bi morali zahtevati, da vsak element grupe $G$ deluje kot zvezen linearen operator na $V$, kar ni avtomatično v neskončno razsežnih vektorskih prostorih. Za tem bi morali namesto zveznosti preslikave $\rho$ zahtevati, da je le *šibko zvezna*, kar pomeni, da je preslikava $G \times V \to V$, $(g, v) \mapsto \rho(g) \cdot v$ zvezna.

Kadar je dana topološka grupa $G$ opremljena z znano topologijo, ki izhaja iz evklidskega prostora, kot se zgodi na primer v grupah $\mathrm{SO}_3(\mathbf{R})$ ali $\mathrm{SL}_2(\mathbf{C})$, ima smisel govoriti o številnih dodatnih lastnostih matričnih koeficientov upodobitev. Lahko na primer zahtevamo, da so ti koeficienti gladki, analitični ali preprosto polinomi. V teh primerih rečemo, da imamo gladko, analitično oziroma polinomsko upodobitev.

### Unitarnost

Pri raziskovanju teorije upodobitev končnih grup nam je marsikje prav prišlo dejstvo, da smo vektorske prostore opremili s skalarnim produktom, ki je bil invarianten glede na upodobitev. Z drugimi besedami, opazovali smo **unitarne** upodobitve, ki slikajo v grupo $\mathrm{U}(V) \leq \mathrm{GL}(V)$. Z metodo povprečenja smo dokazali, da je vsaka upodobitev končne grupe unitarizabilna in torej po ustrezni zamenjavi baze lahko predpostavimo, da je oblike $\rho: G \to U_n(\mathbf{C})$. Za neskončne grupe tega sklepa ne moremo napraviti in tudi zaključek na splošno ne drži.

**Zgled 6.0.4.** Opazujmo grupo $\mathbf{R}$ in njene upodobitve $\chi_\zeta$. Ta upodobitev je unitarna, če in samo če za neki skalarni produkt na $\mathbf{C}$ velja

$$\langle u, v \rangle = \langle e^{\zeta x} u, e^{\zeta x} v \rangle$$

za vsak $x \in \mathbf{R}$ in vse $u, v \in \mathbf{C}$. Ta pogoj je enakovreden $|e^{\zeta x}| = 1$, se pravi $\zeta \in \mathbf{R} \cdot i$. V tem primeru upodobitev $\chi_\zeta$ nujno slika v enotsko krožnico $\mathrm{U}(\mathbf{C}) = S^1 = \{z \in \mathbf{C} \,|\, |z| = 1\}$.

Za neskončne topološke grupe najraje opazujemo zvezne unitarne upodobitve. O teh po navadi lahko povemo največ, kot bomo videli v nadaljevanju.

## 6.1 Kompaktne grupe

Večino rezultatov iz končnih grup lahko prenesemo v svet kompaktnih topoloških grup in njihovih zveznih unitarnih upodobitev.

### $\mathrm{U}_1(\mathbf{C})$

Najenostavnejši primer neskončne kompaktne grupe je unitarna grupa $\mathrm{U}_1(\mathbf{C}) = S^1$ kompleksnih števil absolutne vrednosti 1. To topološko grupo lahko alternativno vidimo kot $\mathbf{R}/\mathbf{Z}$ s kvocientno topologijo iz grupe $\mathbf{R}$.

### Nerazcepne upodobitve

Poznamo že nekaj upodobitev grupe $\mathbf{R}/\mathbf{Z}$, ki jih ponuja grupa $\mathbf{R}$, in sicer za vsak parameter $k \in \mathbf{Z}$ dobimo upodobitev

$$\chi_k: \mathbf{R}/\mathbf{Z} \to \mathbf{C}^*, \quad x \mapsto e^{2\pi i k x}.$$

Velja pa tudi obratno, iz vsake upodobitve $\chi: \mathbf{R}/\mathbf{Z} \to \mathrm{U}_1(\mathbf{C})$ z restrikcijo vzdolž $\mathbf{R} \to \mathbf{R}/\mathbf{Z}$ dobimo upodobitev $\mathbf{R}$. Te upodobitve lahko popolnoma opišemo s pomočjo elementarne analize.

**Trditev 6.1.1.** *Vsaka zvezna upodobitev $\mathbf{R} \to \mathbf{C}^*$ je oblike $\chi_\zeta$ za neki $\zeta \in \mathbf{C}$.*

*Dokaz.* Naj bo $\chi: \mathbf{R} \to \mathbf{C}^*$ zvezna. Če je $\chi$ celo *odvedljiva*, potem za vsak $x \in \mathbf{R}$ velja

$$\chi'(x) = \lim_{t \to 0} \frac{\chi(x+t) - \chi(x)}{t} = \chi(x)\chi'(0).$$

Funkcija $\chi$ torej reši diferencialno enačbo $\chi' = \zeta\chi$, kjer smo označili $\zeta = \chi'(0)$. Od tod sledi, da je $\chi(x) = A \cdot e^{\zeta x}$ za neko konstanto $A$. Vstavimo $x = 0$ in sklenemo $A = 1$, torej je res $\chi = \chi_\zeta$.

Prepričajmo se, da je $\chi$ *vselej* odvedljiva, s čimer bo trditev dokazana. V ta namen jo najprej integrirajmo do odvedljive funkcije

$$X\colon \mathbf{R} \to \mathbf{C}, \quad x \mapsto \int_0^x \chi(t)dt.$$

Funkcija $X$ sicer ni nujno homomorfizem, velja pa

$$X(x+y) = X(x) + \int_x^{x+y} \chi(t)dt = X(x) + \int_0^y \chi(t+x)dt = X(x) + \chi(x)X(y)$$

za vsaka $x, y \in \mathbf{R}$. Ker je $X' = \chi$, seveda obstaja $y_0 \in \mathbf{R}$, za katerega je $X(y_0) \neq 0$. Od tod lahko izrazimo $\chi(x)$ kot

$$\chi(x) = \frac{X(x+y_0) - X(x)}{X(y_0)}.$$

Ker je funkcija na desni odvedljiva, velja enako tudi za funkcijo na levi. □

Iz trditve izpeljemo, da vsaka zvezna upodobitev $\mathbf{R}/\mathbf{Z} \to \mathbf{C}^*$ izhaja iz upodobitve $\chi_\zeta$ za neki $\zeta$. Pri tem mora biti $\mathbf{Z} \leq \ker \chi_\zeta$, od koder sledi $\zeta = 2\pi i k$ za nek $k \in \mathbf{Z}$. Upodobitve $\chi_k$ torej izčrpajo vse končno razsežne zvezne kompleksne upodobitve grupe $\mathbf{R}/\mathbf{Z}$. Te upodobitve so vse tudi unitarne, kar ni naključje, kot bomo pojasnili nekoliko kasneje.

### Fourierova analiza

Klasična Fourierova analiza periodičnih funkcij se tesno prepleta s teorijo upodobitev grupe $\mathbf{R}/\mathbf{Z}$. Kot vemo, lahko z upodobitvami $\chi_k$ za $k \in \mathbf{Z}$ aproksimiramo poljubno zvezno funkcijo na $\mathbf{R}/\mathbf{Z}$. To naredimo na naslednji način. Prostor funkcij na grupi $\mathbf{R}/\mathbf{Z}$ opremimo s skalarnim produktom

$$\langle f, h \rangle = \int_0^1 f(t)\overline{h(t)}dt.$$

Fourierovi koeficienti funkcije $f$ so

$$\langle f, \chi_k \rangle = \int_0^1 f(t)e^{-2\pi i k t}dt$$

za $k \in \mathbf{Z}$. Z njimi definiramo delne Fourierove vsote

$$f_N = \sum_{k \in \mathbf{Z} : |k| \leq N} \langle f, \chi_k \rangle \chi_k$$

za $N \in \mathbf{N}$. V splošnem delne vsote $f_N$ ne konvergirajo po točkah,[2] je pa tako, če dodatno predpostavimo, da obravnavamo le kvadratno integrabilne funkcije $f$, se pravi

$$\int_0^1 |f(t)|^2 dt < \infty.$$

Za te funkcije po osnovnem izreku Fourierove analize velja konvergenca

$$\lim_{N \to \infty} \|f - f_N\| = 0,$$

torej lahko $f$ razvijemo v Fourierovo vrsto. Pri tem moramo biti nekoliko previdni, saj opisana konvergenca *ne* implicira, da vrsta $f_N$ v vseh točkah konvergira k $f$, temveč le *skoraj povsod*. Hkrati drži varianta Parsevalove formule

$$\|f\|^2 = \sum_{k \in \mathbf{Z}} |\langle f, \chi_k \rangle|^2.$$

Upodobitve $\chi_k$ za $k \in \mathbf{Z}$ torej tvorijo ortonormiran sistem funkcij, ki je *gost* v prostoru vseh dovolj lepih funkcij na $\mathbf{R}/\mathbf{Z}$.

[2] Lahko se celo zgodi, da $f_N$ ne konvergira v *nobeni* točki. Take primere je prvi konstruiral Kolmogorov; glej povzetek (Chen 1962).

**Zgled 6.1.2.** Opazujmo funkcijo $f:\mathbf{R}/\mathbf{Z}\to\mathbf{R}$, definirano kot

$$f(x) = -2\log|2\sin(\pi x)|$$

z vrednostjo $f(0) = 0$ v singularni točki. Pišimo $z = e^{2\pi i x}$. Potem je $\Re(2\log(1-z)) = 2\log|1-z| = \log|\sin(\pi x)|$. Uporabimo razvoj $-\log(1-z) = \sum_{k\geq 1} z^k/k$,[3] da dobimo

$$f(x) = 2\sum_{k\geq 1}\frac{\cos(2\pi k x)}{k} = \sum_{k\neq 1}\frac{1}{|k|}\chi_k(x)$$

za $0 < x < 1$. Fourierovi koeficienti funkcije $f$ so torej $\langle f,\chi_k\rangle = 1/|k|$ za $k\neq 0$ in $\langle f,\chi_0\rangle = 0$. Vsota kvadratov teh koeficientov konvergira, zato je po Riesz-Fischerjevem izreku $f$ kvadratno integrabilna funkcija na $\mathbf{R}/\mathbf{Z}$. Delne Fourierove vsote $f_N$ so v točki $x = 0$ enake

$$f_N(0) = 2\sum_{1\leq k\leq N}\frac{1}{k},$$

kar divergira za $N\to\infty$.

Fourierovo analizo lahko torej vidimo kot analog dekompozicije regularne upodobitve v primeru končnih grup za neskončno grupo $\mathbf{R}/\mathbf{Z}$.

## Poljubne kompaktne grupe

Izkaže se, da ima vse, kar smo videli za primer $\mathrm{U}_1(\mathbf{C})$, ustrezno posplošitev za poljubno kompaktno grupo $G$, na primer $\mathrm{SU}_2(\mathbf{C})$ ali $\mathrm{SO}_3(\mathbf{R})$. Za natančno obravnavo potrebujemo nekaj *teorije mere*, ki jo bomo prosto uporabili v tem podrazdelku.[4]

V primeru grupe $\mathbf{R}/\mathbf{Z}$ smo skalarni produkt na prostoru funkcij izrazili s pomočjo integrala. Izkaže se, da ima vsaka kompaktna grupa enolično verjetnostno mero $\mu$, ki zadošča pogoju invariantnosti $\mu(U) = \mu(g\cdot U) = \mu(U\cdot g)$ za vsako merljivo množico $U$ in element $g\in G$. To mero imenujemo **Haarova mera**.[5]

**Zgled 6.1.3.** Multiplikativna grupa $\mathrm{U}_1(\mathbf{C}) = S^1$ je izomorfna aditivni grupi $\mathbf{R}/\mathbf{Z}$ preko preslikave $\chi_1:\mathbf{R}/\mathbf{Z}\to S^1$, $x\mapsto e^{2\pi i x}$. Naj bo $\lambda$ standardna Lebesgueova mera na $\mathbf{R}$. To mero lahko preko kanonične projekcije $\mathbf{R}\to\mathbf{R}/\mathbf{Z}$ prenesemo na $\mathbf{R}/\mathbf{Z}$, pri čemer definiramo mero na podmnožici $U\subseteq\mathbf{R}/\mathbf{Z}$ kot $\lambda(\pi^{-1}(U)\cap[0,1))$. Za pripadajočo podmnožico $U\subseteq S^1$ potem definiramo njeno mero kot $\mu(U) = \lambda(\chi_1^{-1}(U))$. Ta mera je Haarova mera na $\mathrm{U}_1(\mathbf{C})$ in ima ključno vlogo v klasični Fourierovi analizi, kot smo se spomnili zgoraj.

**Zgled 6.1.4.** Nekoliko bolj zapleten opis ima Haarova mera na grupi $\mathrm{SU}_2(\mathbf{C})$. Elementi te grupe so matrike oblike

$$\begin{pmatrix} a & b\\ -\overline{b} & \overline{a}\end{pmatrix},\quad |a|^2+|b|^2 = 1.$$

Grupo $\mathrm{SU}_2(\mathbf{C})$ lahko torej identificiramo s sfero $S^3\subseteq\mathbf{R}^4$ preko vložitve $\iota(a,b) = (\Re(a),\Im(a),\Re(b),\Im(b))$. Mero na $\mathrm{SU}_2(\mathbf{C})$ potem definiramo preko Lebesgueove mere na $S^3$.

Oglejmo si, kako to deluje v koordinatah. Parametrizirajmo $a,b$ in s tem vložitev $\iota$ kot $a = e^{\frac{i}{2}(\phi+\psi)}\cos(\theta/2)$ in $b = e^{\frac{i}{2}(\phi-\psi)}\sin(\theta/2)$ za realna števila $\phi\in[0,2\pi)$, $\theta\in[0,\pi]$, $\psi\in[0,4\pi)$. Naj bodo $v_1,v_2,v_3$ tangentni vektorji na $S^3$, dobljeni z odvajanjem vložitve $\iota$ po parametrih $\phi,\psi,\theta$. Ti vektorji napenjajo paralelepiped z volumnom $\sqrt{\det(G)}$, kjer je $G$ Gramova matrika z elementi $G_{ij} = \langle v_i,v_j\rangle$. Izračunamo

$$G = \begin{pmatrix} 1/4 & 0 & \cos(\theta)/4\\ 0 & 1/4 & 0\\ \cos(\theta)/4 & 0 & 1/4\end{pmatrix},\quad \det(G) = \frac{\sin^2(\theta)}{64}.$$

[3] Vrsta konvergira le za $|z|<1$, zato v resnici uporabimo razvoj za $rz$ z $r<1$, nato pa izlimitiramo $r\to 1$ in vzamemo realni del.

[4] Za uvodno seznanitev s teorijo mere se lahko obrneš na (Magajna 2011).

[5] Dokaz obstoja Haarove mere lahko najdeš v prvem poglavju zapiskov (Hladnik 2006).

Diferencialen volumen na $S^3$ glede na izbrano parametrizacijo je torej $\frac{\sin(\theta)}{8} d\phi d\theta d\psi$. Ko to pointegriramo po celotni domeni parametrov, dobimo volumen sfere $2\pi^2$. Haarova mera je verjetnostna, zato moramo diferencialen volumen še normalizirati s faktorjem $1/(2\pi^2)$. Končno dobimo Haarovo mero na $\mathrm{SU}_2(\mathbf{C})$ z gostoto $\frac{\sin(\theta)}{16\pi^2}$ v parametrih $\phi, \theta, \psi$.

S Haarovo mero lahko definiramo integral merljive funkcije. S pomočjo tega se nam odprejo vrata orodju povprečenja po grupi, ki ga lahko izkoristimo za različne namene.

**Trditev 6.1.5.** *Vsaka zvezna končno razsežna kompleksna upodobitev kompaktne grupe je unitarizabilna.*

*Dokaz.* Naj bo $\rho: G \to \mathrm{GL}(V)$ upodobitev. Izberemo poljuben skalarni produkt $\langle \cdot, \cdot \rangle$ na $V$ in ga povprečimo do

$$\langle \cdot, \cdot \rangle_0 : V \times V \to \mathbf{C}, \quad \langle v, w \rangle_0 = \int_G \langle \rho(g) \cdot v, \rho(g) \cdot w \rangle d\mu(g).$$

Ni težko preveriti, da je $\langle \cdot, \cdot \rangle_0$ skalarni produkt na $V$, glede na katerega je $\rho$ unitarna upodobitev. □

Kot v primeru $\mathbf{R}/\mathbf{Z}$ lahko vse upodobitve najdemo v ustreznem modelu regularne upodobitve. Opazujemo funkcije na kompaktni grupi $G$, pri čemer se omejimo na prostor kvadratno integrabilnih merljivih funkcij in še te opazujemo le do ekvivalence *skoraj povsod* natančno. Prostor ekvivalenčnih razredov takih funkcij je $L^2(G)$. Na tem prostoru deluje grupa $G$ kot regularna upodobitev,

$$\rho(g) \cdot f = x \mapsto f(xg).$$

Ta prostor je seveda neskončno razsežen. Znameniti Peter-Weylov izrek razkrije dekompozicijo te upodobitve, ki je popolnoma analogna tisti iz sveta končnih grup.[6]

**Izrek 6.1.6** (Peter-Weyl)**.** *Naj bo $G$ kompaktna grupa s Haarovo mero $\mu$. Regularna upodobitev $G$ na $L^2(G)$ je izomorfna ortogonalni direktni vsoti Hilbertovih prostorov*

$$L^2(G) \cong \bigoplus_{\pi} \underbrace{\pi \oplus \pi \oplus \cdots \oplus \pi}_{\deg(\pi)},$$

*ko $\pi$ preteče vse končno razsežne nerazcepne zvezne unitarne upodobitve grupe $G$.*

Kot v končnih grupah se s pomočjo matričnih koeficientov prepričamo, da je vsaka nerazcepna zvezna unitarna upodobitev vsebovana v regularni. V posebnem je zato vsaka zvezna unitarna upodobitev kompaktne grupe nujno *končno razsežna*.

## 6.2 Zvezne linearne grupe

V tem razdelku si bomo ogledali, kako lahko razumemo teorijo upodobitev linearnih topoloških grup, ki lokalno izgledajo kot $\mathbf{R}^n$ ali $\mathbf{C}^n$. To so na primer grupe $\mathrm{GL}_n(\mathbf{C})$, $\mathrm{SL}_2(\mathbf{C})$, $\mathrm{SL}_2(\mathbf{R})$, $\mathrm{SO}_3(\mathbf{R})$, $\mathrm{SU}_2(\mathbf{C})$. Zadnji dve grupi sta sicer kompaktni, tako da ju lahko razumemo tudi z orodji zadnjega razdelka. Tu se bomo zato osredotočili na nekompaktne zglede.

### $\mathrm{SL}_2(\mathbf{C})$

Grupa $\mathrm{SL}_2(\mathbf{C})$ je zaprta podmnožica kompleksnega prostora $\mathbf{C}^4$, dana z enačbo $ad - bc = 1$. Ker je odvod determinantne preslikave v vsaki točki neničeln, je $\mathrm{SL}_2(\mathbf{C})$ podmnogoterost kompleksne razsežnosti 3. Pri opazovanju upodobitev grupe $\mathrm{SL}_2(\mathbf{C})$ bomo seveda upoštevali to strukturo, saj sicer dobimo *preveč*

[6] Za dokaz glej na primer zadnje poglavje zapiskov (Hladnik 2006). Tam najdeš tudi ekspliciten opis nerazcepnih zveznih unitarnih upodobitev grupe $\mathrm{SU}_2(\mathbf{C})$. V naslednjem razdelku si bomo ogledali še en drug (bolj geometrijski) način, kako lahko pridemo do teh upodobitev.

upodobitev.[7] Smiselno bo opazovati upodobitve, pri katerih so matrični koeficienti zvezne ali celo gladke funkcije matrike, ki deluje. Glede na to, da je $\mathrm{SL}_2(\mathbf{C})$ kompleksna mnogoterost, lahko opazujemo tudi kompleksno analitične upodobitve. Na grupo $\mathrm{SL}_2(\mathbf{C})$ lahko gledamo tudi kot na algebraično grupo,[8] zato ima smisel opazovati tudi le polinomske upodobitve. Kot bomo videli, so si nazadnje vse te različne oblike upodobitev grupe $\mathrm{SL}_2(\mathbf{C})$ med seboj zelo podobne.

### Standardna upodobitev in njene potence

Grupa $\mathrm{SL}_2(\mathbf{C})$ naravno deluje na vektorskem prostoru $\mathbf{C}^2$ z množenjem matrik z vektorji. Označimo bazna vektorja kot $X = e_1$ in $Y = e_2$. Na ta način dobimo **standardno upodobitev**

$$\rho_1 : \mathrm{SL}_2(\mathbf{C}) \to \mathrm{GL}_2(\mathbf{C}), \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \left( (X,Y) \mapsto (X,Y) \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right).$$

To upodobitev lahko vidimo kot upodobitev na prostoru linearnih polinomov v $X,Y$. V tej luči jo lahko naravno razširimo na prostor homogenih polinomov $\mathbf{C}[X,Y]_k$ stopnje $k \geq 1$.[9] Baza tega prostora so monomi $e_i = X^i Y^{k-i}$ za $0 \leq i \leq k$, torej je $\mathbf{C}[X,Y]_k$ razsežnosti $k+1$. Formalno za razširitev $\rho_1$ uporabimo simetrično potenco in dobimo

$$\rho_k = \mathrm{Sym}^k(\rho_1) : \mathrm{SL}_2(\mathbf{C}) \to \mathrm{GL}(\mathbf{C}[X,Y]_k), \quad g \mapsto (f(X,Y) \mapsto f((X,Y) \cdot g)).$$

Eksplicitno se bazni monom $e_i = X^i Y^{k-i}$ z upodobitvijo $\rho_k$ preslika v

$$\rho_k \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot X^i Y^{k-i} = (aX + cY)^i (bX + dY)^{k-i},$$

kar brez težave razvijemo po monomih v $\mathbf{C}[X,Y]_k$. Pri tem dobimo koeficiente, ki so polinomi v spremenljivkah $a,b,c,d$, zato je upodobitev $\rho_k$ polinomska.

**Trditev 6.2.1.** *Polinomske upodobitve $\rho_k : \mathrm{SL}_2(\mathbf{C}) \to \mathrm{GL}_{k+1}(\mathbf{C})$ so nerazcepne.*

*Dokaz.* Kot v obravnavi upodobitev splošne linearne grupe nad končnim poljem si oglejmo torus[10]

$$T = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \mid \lambda \in \mathbf{C}^* \right\} \cong \mathbf{C}^*.$$

Upodobitev $\rho_k$ zožimo na $T$. Velja

$$\rho_k \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \cdot e_i = \lambda^{2i-k} e_i.$$

Naj bo $\chi_i$ upodobitev $T \cong \mathbf{C}^* \to \mathbf{C}^*$, $\lambda \mapsto \lambda^i$. Imamo torej zelo preprosto dekompozicijo

$$\mathrm{Res}_T^{\mathrm{SL}_2(\mathbf{C})}(\rho_k) = \chi_{-k} \oplus \chi_{-k+2} \oplus \cdots \oplus \chi_k.$$

S pomočjo tega bomo dokazali, da je $\rho_k$ nerazcepna upodobitev. Res, naj bo $0 \neq W \leq \mathbf{C}[X,Y]_k$ poljuben $\mathrm{SL}_2(\mathbf{C})$-invarianten podprostor. Ker je $\mathrm{Res}_T^{\mathrm{SL}_2(\mathbf{C})}(\rho_k)$ polenostavna upodobitev, v kateri vsaka nerazcepna podupodobitev nastopa z večkratnostjo 1, podprostor $W$ nujno sestoji iz nekaterih od teh podupodobitev. Za neko množico $I \subseteq \{0,1,\ldots,k\}$ torej velja

$$W = \bigoplus_{i \in I} \mathbf{C} \cdot e_i.$$

[7] Podobno, kot smo že videli v primeru upodobitev grupe $\mathbf{R}$. Konkretno za vsak avtomorfizem polja $\mathbf{C}$ dobimo upodobitev $\mathrm{SL}_2(\mathbf{C}) \to \mathrm{SL}_2(\mathbf{C})$, ki aplicira avtomorfizem po členih matrike. Polje $\mathbf{C}$ ima *mnogo* divjih avtomorfizmov.

[8] **Linearna algebraična grupa** je grupa, ki je hkrati množica skupnih ničel nekih polinomov v prostoru $\mathbf{C}^n$.

[9] Pri $k = 0$ dobimo trivialno upodobitev.

[10] Ker je polje $\mathbf{C}$ algebraično zaprto, tukaj obstaja le en torus.

Upoštevajmo zdaj, da je $W$ invarianten še glede na vse druge elemente v $\mathrm{SL}_2(\mathbf{C})$. Velja

$$\rho_k \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot e_i = X^i (X+Y)^{k-i} = \sum_{j=i}^{k} \binom{k-i}{j-i} e_j.$$

Če je $e_{i_0} \in W$, je torej $e_i \in W$ za vsak $i \geq i_0$, saj je $W$ razpet z nekaterimi standardnimi baznimi vektorji. Podoben argument s spodnjetrikotno matriko pokaže, da je $e_i \in W$ za vsak $i \leq i_0$. Sklepamo torej $W = \mathbf{C}[X,Y]_k$ in $\rho_k$ je res nerazcepna upodobitev. □

Na ta način smo torej konstruirali neskončno mnogo nerazcepnih polinomskih upodobitev grupe $\mathrm{SL}_2(\mathbf{C})$ poljubne visoke stopnje. Zanimivo je, da te upodobitve *niso* unitarne. Lastne vrednosti unitarnih matrik so namreč nujno absolutne vrednosti 1, čemur upodobitve $\rho_k$ ne zadoščajo. Kasneje bomo videli preprost argument, da niti njena podgrupa $\mathrm{SL}_2(\mathbf{R})$ nima netrivialnih končno razsežnih unitarnih upodobitev. Upodobitve teh grup so torej bistveno drugačne od upodobitev kompaktnih grup, kjer so *vse* končno razsežne nerazcepne upodobitve unitarne.

**Domača naloga 6.2.2.** Grupa $\mathrm{SU}_2(\mathbf{C})$ je kompaktna podgrupa $\mathrm{SL}_2(\mathbf{C})$. Dokaži, da so zožitve upodobitev $\rho_k$ na $\mathrm{SU}_2(\mathbf{C})$ nerazcepne in unitarne. Izračunaj karakter vsake od teh upodobitev in dokaži, da te funkcije tvorijo gosto bazo prostora $L^2(\mathrm{SU}_2(\mathbf{C}))$. To so torej vse zvezne nerazcepne unitarne upodobitve grupe $\mathrm{SU}_2(\mathbf{C})$.

### Linearizacija upodobitve

Princip za dokazovanje, da smo z upodobitvami $\rho_k$ izčrpali vse dovolj lepe upodobitve grupe $\mathrm{SL}_2(\mathbf{C})$, temelji na *linearizaciji*. Vsako odvedljivo upodobitev $\rho\colon \mathrm{SL}_2(\mathbf{C}) \to \mathrm{GL}_n(\mathbf{C})$ lahko namreč obravnavamo kot preslikavo med mnogoterostmi, zato z njenim **odvodom** dobimo inducirano linearno preslikavo

$$D_I\rho\colon T_I \mathrm{SL}_2(\mathbf{C}) \to T_I \mathrm{GL}_n(\mathbf{C})$$

med tangentnima prostoroma v identični matriki. Oglejmo si podrobneje, kako sta videti ta dva tangentna prostora in kaj točno je $D_I\rho$.[11]

Opazujmo najprej grupo $\mathrm{GL}_n(\mathbf{C})$, ki je odprta podmnožica $\mathbf{C}^{n^2}$. Njen tangentni prostor v $I$ zato lahko identificiramo z vektorskim prostorom $\mathbf{C}^{n^2}$, ki ga predstavimo v matrični obliki kot

$$\mathfrak{gl}_n(\mathbf{C}) = \{X \mid X \in \mathrm{Mat}_n(\mathbf{C})\}.$$

Ta opis je prikladen, ker omogoča jasen opis majhne okolice $I$ v $\mathrm{GL}_n(\mathbf{C})$. Za vsak tangentni vektor $X \in \mathfrak{gl}_n(\mathbf{C})$ imamo preslikavo $\mathbf{R} \to \mathfrak{gl}_n(\mathbf{C})$, $t \mapsto tX$, ki jo lahko potisnemo v $\mathrm{GL}_n(\mathbf{C})$ z **eksponentno preslikavo** in dobimo gladko pot

$$\gamma\colon \mathbf{R} \to \mathrm{GL}_n(\mathbf{C}), \quad t \mapsto e^{tX} = \sum_{i=0}^{\infty} t^i X^i / i!$$

v grupi $\mathrm{GL}_n(\mathbf{C})$. Res, velja enakost $\det(\gamma(t)) = \det e^{tX} = e^{\mathrm{tr}(tX)}$,[12] zato je $\gamma(t)$ obrnljiva matrika. Tangentni vektor poti $\gamma$ v točki 0 izračunamo kot

$$D_0\gamma = \lim_{t\to 0} \frac{e^{tX} - I}{t} = \lim_{t\to 0} \frac{I + tX + O(t^2) - I}{t} = X.$$

Pot $\gamma$ je torej gladka pot v $\mathrm{GL}_n(\mathbf{C})$ z začetno vrednostjo $\gamma(0) = I$ in tangentnim vektorjem $X$. Vsak tangentni vektor smo torej s pomočjo eksponentne preslikave uresničili kot tangentni vektor neke gladke poti skozi $I$. Vsaj lokalno pa je res tudi obratno: vsaka gladka pot v $\mathrm{GL}_n(\mathbf{C})$ v neki okolici $I$ izhaja iz gladke poti v $\mathfrak{gl}_n(\mathbf{C})$, potisnjene v $\mathrm{GL}_n(\mathbf{C})$ z eksponentno preslikavo. To sledi neposredno iz naslednje lastnosti eksponentne preslikave.

[11] Za splošnejšo obravnavo tangentnih prostorov in odvodov med mnogoterostmi glej zapiske (Forstnerič 2023).

[12] Ta enakost je jasna, če matriko $X$ predstavimo v Jordanovi normalni obliki.

**Trditev 6.2.3.** *Eksponentna preslikava* $e\colon \mathfrak{gl}_n(\mathbf{C}) \to \mathrm{GL}_n(\mathbf{C})$ *je difeomorfizem v neki okolici* 0.

*Dokaz.* Na vsaki kompaktni podmnožici $\Omega \subseteq \mathfrak{gl}_n(\mathbf{C})$ je vsak člen matrike $X$ absolutno omejen, recimo z $\alpha$, zato je tudi vsak člen matrike $X^k$ omejen z $n^{k-1}\alpha^k$. Po Weierstrassovem M-testu zato vrsta, ki definira eksponentno preslikavo, enakomerno konvergentna po kompaktih v $\mathfrak{gl}_n(\mathbf{C})$. Delne vsote te vrste $\sum_{i=0}^{k} X^i/i!$ so polinomske funkcije, zato so odvedljive. Iz povedanega sledi, da je eksponentna preslikava diferenciabilna v okolici 0. Po izreku o inverzni preslikavi bo zdaj dovolj preveriti, da je linearna preslikava $D_0 e$ polnega ranga. Za poljuben $X \in \mathfrak{gl}_n(\mathbf{C})$ naj bo $\lambda\colon \mathbf{R} \to \mathfrak{gl}_n(\mathbf{C})$, $t \mapsto tX$ in naj bo $\gamma = e \circ \lambda$. Po verižnem pravilu velja

$$D_0 e \cdot X = D_0 e \cdot D_0 \lambda = D_0 \gamma = X.$$

Torej je $D_0 e$ kar identična preslikava. □

Eksponentna preslikava ima torej lokalno inverz, ki ga označimo z log. Za vsako gladko pot $\gamma\colon \mathbf{R} \to \mathrm{GL}_n(\mathbf{C})$ z $\gamma(0) = I$ lahko torej najdemo $\epsilon > 0$, da je pot $\gamma|_{(-\epsilon,\epsilon)}$ oblike $e^{\lambda}$, kjer je $\lambda = \log\gamma\colon (-\epsilon,\epsilon) \to \mathfrak{gl}_n(\mathbf{C})$ gladka pot v tangentnem prostoru.

S pomočjo eksponentne preslikave lahko dobro razumemo tudi tangentni prostor $T_I \mathrm{SL}_2(\mathbf{C})$ in njegovo lokalno povezavo z grupo $\mathrm{SL}_2(\mathbf{C})$. Izberimo poljuben tangentni vektor $X \in T_I \mathrm{SL}_2(\mathbf{C}) \leq \mathfrak{gl}_2(\mathbf{C})$. Obstaja torej gladka pot $\gamma\colon (-\epsilon,\epsilon) \to \mathrm{SL}_2(\mathbf{C})$ z odvodom $D_0\gamma = X$. Po potrebi $\epsilon$ še zmanjšamo in s tem po zadnji trditvi dosežemo, da je $\gamma(t) = e^{\lambda(t)}$, kjer je $\lambda\colon (-\epsilon,\epsilon) \to T_I \mathrm{SL}_2(\mathbf{C})$ gladka pot. Pri tem velja

$$X = D_0\gamma = D_0 e \cdot D_0\lambda = D_0\lambda.$$

Ker $\gamma$ slika v $\mathrm{SL}_2(\mathbf{C})$, za vsak $t \in (-\epsilon,\epsilon)$ velja

$$1 = \det(\gamma(t)) = e^{\mathrm{tr}(\lambda(t))},$$

zato je $\mathrm{tr}(\lambda(t)) = 0$ za vsak dovolj majhen $t$. To enakost odvedemo v točki 0 in dobimo $\mathrm{tr}(X) = 0$. Vsak vektor v $T_I \mathrm{SL}_2(\mathbf{C})$ zato pripada vektorskemu prostoru

$$\mathfrak{sl}_2(\mathbf{C}) = \{X \in \mathfrak{gl}_2(\mathbf{C}) \mid \mathrm{tr}(X) = 0\}.$$

Res pa je tudi obratno. Vsak vektor $X$ s sledjo 0 namreč določa pot $\gamma\colon \mathbf{R} \to \mathrm{SL}_2(\mathbf{C})$, $t \mapsto e^{tX}$. Velja $\gamma(0) = I$ in $D_0\gamma = X$, torej je $X \in T_I \mathrm{SL}_2(\mathbf{C})$.

**Posledica 6.2.4.** *Velja* $T_I \mathrm{SL}_2(\mathbf{C}) = \mathfrak{sl}_2(\mathbf{C})$. *Ta vektorski prostor je* 3*-razsežen z bazo*

$$e = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad f = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Pod vsem povedanim lahko **odvod upodobitve** $\rho\colon \mathrm{SL}_2(\mathbf{C}) \to \mathrm{GL}_n(\mathbf{C})$ torej razumemo kot linearno preslikavo

$$D_I\rho\colon \mathfrak{sl}_2(\mathbf{C}) \to \mathfrak{gl}_n(\mathbf{C}), \quad X \mapsto D_0\rho(e^{tX}),$$

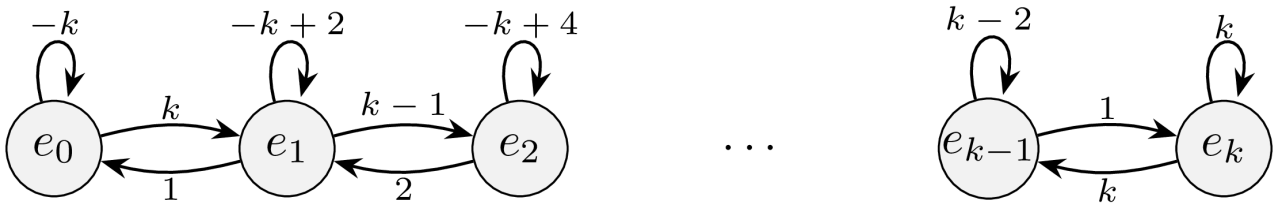
ki tangentni vektor $X \in \mathfrak{sl}_2(\mathbf{C})$ najprej pointegrira v pot $\gamma(t) = e^{tX}$ v $\mathrm{SL}_2(\mathbf{C})$ za vrednosti $t$ blizu 0, to pot preslika z upodobitvijo $\rho$ v pot v $\mathrm{GL}_n(\mathbf{C})$ in izračuna odvod slednje poti, ki je tangentni vektor v $\mathfrak{gl}_n(\mathbf{C})$.

**Zgled 6.2.5.** Linearizirajmo upodobitve $\rho_k\colon \mathrm{SL}_2(\mathbf{C}) \to \mathrm{GL}(\mathbf{C}[X,Y]_k)$. Najprej določimo slike generatorjev $e,h,f \in \mathfrak{sl}_2(\mathbf{C})$ z eksponentno preslikavo. Za vsak $t \in \mathbf{R}$ velja

$$e^{te} = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}, \quad e^{th} = \begin{pmatrix} e^t & 0 \\ 0 & e^{-t} \end{pmatrix}, \quad e^{tf} = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}.$$

Naj bodo $E_k, H_k, F_k$ slike $e,h,f$ s preslikavo $D_I\rho_k$. Tangentni prostor $\mathfrak{gl}_{k+1}(\mathbf{C})$ naravno deluje na prostoru $\mathbf{C}[X,Y]_k$ z bazo $e_i = X^i Y^{k-i}$ za $0 \leq i \leq k$. Velja

$$H_k \cdot e_i = D_0\left(\rho_k(e^{th}) \cdot e_i\right) = D_0\left((e^t X)^i (e^{-t} Y)^{k-i}\right) = (2i-k)e_i,$$




Slika 6.1: Prikaz delovanja elementov $E_k, H_k, F_k$ v upodobitvi $\rho_k$.

na enak način izračunamo

$$E_k \cdot e_i = (k-i)e_{i+1}, \quad F_k \cdot e_i = ie_{i-1}.$$

Element $H_k$ torej deluje diagonalno na $\mathbf{C}[X,Y]_k$, pri čemer ima vektor $e_k = X^k$ največjo lastno vrednost, in sicer $k$. Ta vektor je v jedru preslikave $E_k$, z zaporednimi uporabami preslikave $F_k$ pa iz njega po vrsti dobimo vse druge bazne vektorje $e_i$ za $0 \leq i \leq k$.

### Liejeva algebra

Preslikava $D_I\rho$ ni čisto poljubna linearna preslikava med vektorskimi prostori, temveč v sebi skriva še nekaj dodatne informacije glede grup $\mathrm{SL}_2(\mathbf{C})$ in $\mathrm{GL}_n(\mathbf{C})$.

Grupa $\mathrm{GL}_n(\mathbf{C})$ deluje s konjugiranjem na svojem tangentnem prostoru,

$$\mathrm{Ad}\colon \mathrm{GL}_n(\mathbf{C}) \to \mathrm{End}(\mathfrak{gl}_n(\mathbf{C})), \quad A \mapsto \left(X \mapsto AXA^{-1}\right).$$

To delovanje imamo tudi z grupo $\mathrm{SL}_2(\mathbf{C})$ in njenim tangentnim prostorom, saj za vsak $X \in \mathfrak{sl}_2(\mathbf{C})$ velja $\mathrm{tr}(AXA^{-1}) = \mathrm{tr}(X) = 0$.

Ni se težko prepričati, da je za vsak $A \in \mathrm{SL}_2(\mathbf{C})$ preslikava $D_I\rho$ *spletična* glede na to delovanje. Za vsak $Y \in \mathfrak{sl}_2(\mathbf{C})$ velja namreč

$$D_I\rho \cdot \mathrm{Ad}(A) \cdot Y = D_0\left(\rho(e^{tAYA^{-1}})\right) = \mathrm{Ad}(\rho(A)) \cdot D_I\rho \cdot Y.$$

V posebnem za vsak tangentni vektor $X \in \mathfrak{sl}_2(\mathbf{C})$ velja ta formula za $A = e^{tX}$. Izračunajmo odvod leve in desne strani v točki $t = 0$. Z uporabo verižnega pravila leva stran postane

$$D_I\rho \cdot D_0\left(e^{tX} Y e^{-tX}\right) = D_I\rho \cdot (XY - YX),$$

desna stran pa postane

$$D_0\left(\rho(e^{tX})(D_I\rho \cdot Y)\rho(e^{-tX})\right) = (D_I\rho \cdot X)(D_I\rho \cdot Y) - (D_I\rho \cdot Y)(D_I\rho \cdot X).$$

Označimo $[X,Y] = XY - YX$. Velja torej

$$D_I\rho \cdot [X,Y] = [D_I\rho \cdot X, D_I\rho \cdot Y],$$

kar pomeni, da preslikava $D_I\rho$ *spoštuje* operaciji $[\cdot,\cdot]$ na $\mathfrak{sl}_2(\mathbf{C})$ in $\mathfrak{gl}_n(\mathbf{C})$.

**Zgled 6.2.6.** V vektorskem prostoru $\mathfrak{sl}_2(\mathbf{C})$ veljajo računi

$$[h,e] = 2e, \quad [h,f] = -2f, \quad [e,f] = h.$$

Iz vrednosti $E_k$ in $F_k$ lahko zato izračunamo vrednost

$$H_k \cdot e_i = D_I\rho_k(h) \cdot e_i = [E_k, F_k] \cdot e_i = i(k-(i-1))e_i - (k-i)(i+1)e_i = (-k+2i)e_i$$

za $0 \leq i \leq k$, kar se ujema z izračunom iz prejšnjega zgleda.

Na oba tangentna prostora zato gledamo kot na vektorska prostora, ozaljšana z binarno operacijo $[\cdot,\cdot]$. Ta operacija je bilinearna in kratek račun pokaže, da zadošča enakostima

$$[X,Y]=-[Y,X],\quad [[X,Y],Z]+[[Y,Z],X]+[[Z,X],Y]=0$$

za vse tangentne vektorje $X,Y,Z$. Abstraktnim vektorskim prostorom s tako binarno operacijo pravimo **Liejeve algebre**. Te algebre tvorijo kategorijo: morfizmi med dvema algebrama so preslikave, ki spoštujejo vso strukturo, in jim zato upravičeno pravimo **Liejevi homomorfizmi**.[13] Kadar Liejev homomorfizem slika iz dane Liejeve algebre $L$ v $\mathfrak{gl}_n(\mathbf{C})$, po analogiji z grupami rečemo, da imamo **Liejevo upodobitev**. Te upodobitve lahko primerjamo med seboj s spletičnami in zato govorimo o izomorfnostnih razredih Liejevih upodobitev.[14] Prav tako na smiseln način posplošimo pojem nerazcepne upodobitve.[15]

Tangentna prostora $\mathfrak{sl}_2(\mathbf{C})$ in $\mathfrak{gl}_2(\mathbf{C})$ sta torej Liejevi algebri in odvod upodobitve $D_I\rho$ je Liejev homomorfizem, na katerega lahko gledamo kot na Liejevo upodobitev Liejeve algebre $\mathfrak{sl}_2(\mathbf{C})$. Vsaka upodobitev grupe $\mathrm{SL}_2(\mathbf{C})$ nam torej da Liejevo upodobitev njene Liejeve algebre. Kadar ima upodobitev grupe kakšen netrivialen invarianten podprostor, je ta invarianten tudi za delovanje Liejeve algebre. Razcepne upodobitve grupe dajo torej razcepne upodobitve Liejeve algebre. Z drugimi besedami, nerazcepne upodobitve Liejeve algebre, ki izhajajo iz upodobitve grupe, lahko izhajajo le iz nerazcepnih upodobitev grupe. Zaradi tega je še posebej pomembno, da opišemo vse nerazcepne upodobitve Liejeve algebre.

**Zgled 6.2.7.** Liejeve upodobitve $D_I\rho_k$ so nerazcepne. Argument za to je podoben tistemu iz grup, a je še lažji. Res, če je $W\leq \mathbf{C}[X,Y]_k$ netrivialen invarianten $\mathfrak{sl}_2(\mathbf{C})$-podprostor, potem vsebuje vektor $0\neq w=\sum_{i=0}^k a_ie_i$. Naj bo $i_0$ največji indeks, za katerega je $a_{i_0}\neq 0$. Potem je $F_k^{i_0}\cdot w=a_{i_0}i_0!e_0\in W$. Torej je $e_0\in W$. Po zaporednih uporabah $E_k$ sklenemo $e_i\in W$ za vsak $0\leq i\leq k$. Torej je res $W=\mathbf{C}[X,Y]_k$.

**Trditev 6.2.8.** *Vsaka nerazcepna Liejeva upodobitev Liejeve algebre $\mathfrak{sl}_2(\mathbf{C})$ je izomorfna $D_I\rho_k$ za neki $k\geq 0$.*

*Dokaz.* Naj bo $\phi\colon\mathfrak{sl}_2(\mathbf{C})\to\mathfrak{gl}_m(\mathbf{C})=\mathrm{End}(V)$ nerazcepna Liejeva upodobitev, kjer je $V=\mathbf{C}^m$. Naj bodo $E,H,F$ slike $e,h,f$ s preslikavo $\phi$.

Naj bo $\lambda$ lastna vrednost $H$ in $v$ pripadajoči lastni vektor. Velja

$$HEv=[H,E]v+EHv=2Ev+\lambda Ev=(\lambda+2)Ev,$$

zato je $E\cdot\mathrm{LP}_\lambda(H)\subseteq\mathrm{LP}_{\lambda+2}(H)$. Podobno velja $F\cdot\mathrm{LP}_\lambda(H)\subseteq\mathrm{LP}_{\lambda-2}(H)$.

Izberimo lastno vrednost $\lambda$ preslikave $H$ z največjo možno realno komponento. Iz maksimalnosti $\lambda$ sledi $Ev\in\mathrm{LP}_{\lambda+2}(H)=0$. Naj bo $v_i=F^iv$ za $i\geq 0$.[16] Velja $v_i\in\mathrm{LP}_{\lambda-2i}(H)$. Za neki $n\geq 0$ velja torej $v_n\neq 0$ in $v_{n+1}=0$. Vektorji $v_0,v_1,\ldots,v_n$ so v različnih lastnih podprostorih $H$, zato so linearno neodvisni. Naj bo $W\leq V$ podprostor, ki ga generirajo.

Naj bo $w_i=Ev_i$ za $i\geq 0$.[17] Velja $w_0=Ev_0=Ev=0$, za $i\geq 1$ pa izračunamo

$$w_i=EFv_{i-1}=[E,F]v_{i-1}+FEv_{i-1}=Hv_{i-1}+Fw_{i-1}=(\lambda-2i+2)v_{i-1}+Fw_{i-1}.$$

Velja torej $w_1=\lambda v_0$. Od tod dobimo

$$w_2=(\lambda-2)v_1+Fw_1=(\lambda-2)v_1+\lambda v_1=(2\lambda-2)v_1,$$

[13] Liejev homomorfizem je torej linearna preslikava $\phi\colon L_1\to L_2$, za katero velja $\phi([x,y])=[\phi(x),\phi(y)]$ za vsaka $x,y\in L_1$.

[14] **Liejeva spletična** med Liejevima upodobitvama $\phi_1,\phi_2$ Liejeve algebre $L$ na prostoru $V$ je linearna preslikava $\alpha\in\mathrm{End}(V)$ z lastnostjo $\alpha(\phi_1(x)\cdot v)=\phi_2(x)\cdot\alpha(v)$ za vsaka $x\in L$, $v\in V$. Kadar najdemo obrnljivo Liejevo spletično, sta upodobitvi **izomorfni**.

[15] Liejeva upodobitev $\phi\colon L\to\mathfrak{gl}_n(\mathbf{C})$ je **nerazcepna**, če prostor $\mathbf{C}^n$ nima nobenih netrivialnih $L$-invariantnih podprostorov.

[16] Vektor $v$ torej *potisnemo navzdol* s $F$.

[17] Vektor $v_n$ torej *potisnemo navzgor* z $E$.

za tem

$$w_3 = (\lambda-4)v_2 + Fw_2 = (\lambda-4)v_2 + (2\lambda-2)v_2 = (3\lambda-6)v_2$$

in induktivno

$$w_i = i(\lambda - i + 1)v_{i-1}$$

za vsak $i \geq 1$. Prostor $W$ je torej invarianten za delovanje $\mathfrak{sl}_2(\mathbf{C})$, zato po nerazcepnosti velja $V = W$.

Lastna vrednost $\lambda$ ni čisto poljubna. Velja namreč $\operatorname{tr}(H) = \operatorname{tr}([E,F]) = 0$, zato je vsota vseh lastnih vrednosti $H$ enaka 0. Ta vsota je ravno

$$\sum_{i=0}^{n}(\lambda - 2i) = (n+1)\lambda - 2(n+1)n/2 = (n+1)(\lambda - n),$$

zato je $\lambda = n$. Od tod dobimo Liejevo spletično

$$\alpha: V \to \mathbf{C}[X,Y]_n, \quad v_i \mapsto \frac{n!}{(n-i)!}e_{n-i},$$

ki je izomorfizem Liejevih upodobitev $\phi$ in $D_I\rho_n$. □

### Integracija upodobitve

Vsaka upodobitev grupe $\mathrm{SL}_2(\mathbf{C})$ se odvede v Liejevo upodobitev Liejeve algebre $\mathfrak{sl}_2(\mathbf{C})$. Neverjetno je, da velja tudi obratno: vsaka Liejeva upodobitev se pointegrira do upodobitve grupe.

**Trditev 6.2.9.** *Naj bo $\phi: \mathfrak{sl}_2(\mathbf{C}) \to \mathfrak{gl}_n(\mathbf{C})$ Liejeva upodobitev. Tedaj obstaja analitična upodobitev $\rho: \mathrm{SL}_2(\mathbf{C}) \to \mathrm{GL}_n(\mathbf{C})$, za katero velja $D_I\rho = \phi$.*

Dokaz te trditve sloni na uporabi eksponentne preslikave in njenega inverza log. Naj bo $U \subseteq \mathrm{SL}_2(\mathbf{C})$ dovolj majhna okolica $I$, da je na njej log difeomorfizem v neko okolico enote $\mathfrak{sl}_2(\mathbf{C})$. Po potrebi $U$ še zmanjšamo, da je $U^{-1} = U$ in da je $\log|_{U\cdot U}$ še vedno difeomorfizem. Vsaki matriki $A \in U$ lahko priredimo $\log A$, ki jo s $\phi$ preslikamo v $\mathfrak{gl}_n(\mathbf{C})$ in nazadnje dvignemo nazaj do grupe z eksponentno preslikavo. Na ta način dobimo gladko funkcijo

$$\rho: U \subseteq \mathrm{SL}_2(\mathbf{C}) \to \mathrm{GL}_n(\mathbf{C}), \quad A \mapsto e^{\phi(\log A)}.$$

Odvod te funkcije v $I$ je na tangentnem vektorju $X \in \mathfrak{sl}_2(\mathbf{C})$ enak

$$D_I\rho \cdot X = D_0\rho(e^{tX}) = D_0 e^{\phi(\log e^{tX})} = D_0 e^{\phi(tX)} = D_0 e^{t\phi(X)} = \phi(X),$$

torej je $D_I\rho = \phi$ in smo $\phi$ pointegrirali na neko dovolj majhno okolico $I$.

Prepričajmo se, da je $\rho$ blizu tega, da bi bila homomorfizem. Naj bosta $A, B \in U$ poljubni matriki. Velja

$$\rho(A)\rho(B) = e^{\phi(\log A)}e^{\phi(\log B)}, \quad \rho(AB) = e^{\phi(\log(AB))}.$$

Če bi logaritem pretvoril produkt v vsoto in eksponentna funkcija vsoto v produkt, potem bi iz linearnosti $\phi$ takoj sledilo, da sta oba izraza enaka. Na splošno žal matrični logaritem in eksponentna funkcija nimata te lastnosti. Za vsaka $X, Y \in \mathfrak{gl}_n(\mathbf{C})$ lahko z nekaj truda z uporabo razvoja v Taylorjevo vrsto izračunamo vrednost

$$\log(e^X e^Y) = X + Y + \frac{1}{2}[X,Y] - \frac{1}{12}[[X,Y],X] + \frac{1}{12}[[X,Y],Y] + \cdots,$$

ki ji pravimo **Baker-Campbell-Hausdorffova formula**. Res torej na splošno ne velja $\log(e^X e^Y) = X+Y$, tolažilna lastnost razvoja pa je, da so vsi členi izrazljivi z Liejevim produktom $[\cdot,\cdot]$ v $\mathfrak{gl}_n(\mathbf{C})$. To pomeni, da za $A = e^X$, $B = e^Y$ velja

$$\begin{aligned}\phi(\log(AB)) &= \phi\left(X + Y + \frac{1}{2}[X,Y] + \cdots\right)\\ &= \phi(X) + \phi(Y) + \frac{1}{2}[\phi(X),\phi(Y)] + \cdots\\ &= \log(e^{\phi(\log A)}e^{\phi(\log B)}),\end{aligned}$$

kjer smo v srednji enakosti upoštevali, da je $\phi$ Liejev homomorfizem. Od tod sklepamo, da res velja $\rho(A)\rho(B) = \rho(AB)$ za vsaka $A, B \in U$. Preslikava $\rho$ je torej vsaj lokalno homomorfizem.

Pogovorimo se še o tem, kako lahko razširimo $\rho$ na celo grupo $\mathrm{SL}_2(\mathbf{C})$. Prepričajmo se najprej, da množica $U$ generira grupo $\mathrm{SL}_2(\mathbf{C})$. Upodobitev bo torej enolično določena s svojimi vrednostmi na $U$. Izberimo poljuben $A \in \mathrm{SL}_2(\mathbf{C})$. Ker je $\mathrm{SL}_2(\mathbf{C})$ povezan topološki prostor, najdemo gladko pot $\gamma\colon [0,1] \to \mathrm{SL}_2(\mathbf{C})$ z $\gamma(0) = I$, $\gamma(1) = A$. Ta pot je na kompaktne intervalu enakomerno zvezna, zato obstajajo indeksi $0 = t_0 < t_1 < \cdots < t_m = 1$, tako da za vsaka $t_i \le s < t \le t_{i+1}$ velja $\gamma(t)\gamma(s)^{-1} \in U$. S tem lahko zapišemo

$$A = \gamma(t_m) = \prod_{i=m}^{1} \left(\gamma(t_i)\gamma(t_{i-1})^{-1}\right).$$

Ker je $\gamma(t_i)\gamma(t_{i-1})^{-1} \in U$, kjer že imamo definiran $\rho$, lahko definicijo razširimo na $A$ s predpisom

$$\rho(A) = \prod_{i=m}^{1} \rho\left(\gamma(t_i)\gamma(t_{i-1})^{-1}\right).$$

Seveda moramo preveriti, da je ta definicija neodvisna od izbire delilnih točk $t_0, t_1, \ldots, t_m$ in od izbire poti $\gamma$.

Prepričajmo se najprej, da z isto potjo $\gamma$ drugačna izbira delilnih točk privede do enakega rezultata, če je le zadoščeno pogoju $\gamma(t)\gamma(s)^{-1} \in U$ za vsaka $t_i \le s < t \le t_{i+1}$. V ta namen bo dovolj premisliti, da se definicija $\rho(A)$ ne spremeni, če fineje izberemo delilne točke, se pravi, če dodamo še nekaj dodatnih točk.[18] Za to pa bo dovolj preveriti, da se definicija $\rho(A)$ ne spremeni, če dodamo eno samo dodatno delilno točko, na primer med $t_i$ in $t_{i-1}$ vrinemo nek $s$. V tem primeru se v definiciji $\rho(A)$ spremeni le faktor $\rho(\gamma(t_i)\gamma(t_{i-1})^{-1})$, in sicer ga zamenjamo s produktom

$$\rho(\gamma(t_i)\gamma(s)^{-1})\rho(\gamma(s)\gamma(t_{i-1})^{-1}).$$

Ker je $\rho$ homomorfizem na $U$, je zadnji člen enak $\rho(\gamma(t_i)\gamma(t_{i-1})^{-1})$, torej se vrednost $\rho(A)$ res ohrani pri dodajanju ene delilne točke. Definicija $\rho(A)$ je zato neodvisna od izbire delilnih točk.

Za neodvisnost od izbire poti potrebujemo nekaj *algebraične topologije*.

**Domača naloga 6.2.10.** Dokaži najprej, da je $\mathrm{SL}_2(\mathbf{C})$ *enostavno povezan* topološki prostor. To lahko narediš tako, da Gram-Schmidtovo ortogonalizacijo izvedeš postopoma in na ta način *deformacijsko retraktiraš* $\mathrm{SL}_2(\mathbf{C})$ na $\mathrm{SU}_2(\mathbf{C})$. Slednja grupa je homeomorfna sferi $S^3$, ki je enostavno povezana.

Za neodvisnost definicije $\rho$ od izbire poti opazujmo dve poti v $\mathrm{SL}_2(\mathbf{C})$, imenujmo ju $\gamma_1$ in $\gamma_2$, ki povezujeta $I$ z $A$. Ker je $\mathrm{SL}_2(\mathbf{C})$ enostavno povezan topološki prostor, obstaja *homotopija* $H\colon [0,1]\times[0,1] \to \mathrm{SL}_2(\mathbf{C})$ z lastnostmi $H(0,t) = \gamma_1(t)$, $H(1,t) = \gamma_2(t)$, $H(s,0) = 1$, $H(s,1) = A$. Po enakomerni zveznosti obstaja $N > 0$, da za vse $|s - s'| < 2/N$ in $|t - t'| < 2/N$ velja $H(s,t)H(s',t')^{-1} \in U$. Pokaži, da lahko s pomočjo homotopije $H$ pot $H(0,t) = \gamma_1(t)$ z zaporedjem majhnih perturbacij, ki ne vplivajo na vrednost $\rho(A)$, spremeniš v pot $H(1/N, t)$. Za tem slednjo pot z enakim argumentom spremeniš v pot $H(2/N, t)$ in tako naprej do poti $H(1,t) = \gamma_2(t)$. Vrednost $\rho(A)$ je torej res neodvisna od izbire poti $\gamma$.

S tem je dokaz trditve o integriranju Liejevih upodobitev $\mathfrak{sl}_2(\mathbf{C})$ zaključen.

### Nerazcepne upodobitve $\mathrm{SL}_2(\mathbf{C})$

Vzpostavili smo bijekcijo med analitičnimi upodobitvami grupe $\mathrm{SL}_2(\mathbf{C})$ in Liejevimi upodobitvami njene Liejeve algebre, ki ohranja nerazcepnost. Ker že poznamo nerazcepne upodobitve $\mathfrak{sl}_2(\mathbf{C})$, dobimo vse nerazcepne analitične upodobitve grupe.

**Posledica 6.2.11.** *Vsaka analitična nerazcepna končno razsežna kompleksna upodobitev grupe* $\mathrm{SL}_2(\mathbf{C})$ *je izomorfna* $\rho_k$ *za nek* $k \ge 0$.

[18] Za vsaki dve izbiri delilnih točk lahko namreč najdemo tretjo izbiro, ki je finejša od obeh. Ta sklep je podoben kot pri definiciji Riemannovega integrala.

Na grupo $\mathrm{SL}_2(\mathbf{C})$ bi lahko gledali kot na *realno* grupo.[19] V tem primeru bi njene *gladke* upodobitve dobili iz Liejevih upodobitev njene Liejeve algebre $\mathfrak{sl}_2(\mathbf{C})$, na katero bi gledali kot na *realno* Liejevo algebro.[20] Teh upodobitev je nekoliko več. Vsako od upodobitev $\rho_k$ lahko namreč še konjugiramo. Izkaže se, ni presenetljivo in ni težko, da vse nerazcepne realne Liejeve upodobitve dobimo kot tenzorske produkte teh.

**Posledica 6.2.12.** *Vsaka gladka nerazcepna končno razsežna kompleksna upodobitev grupe* $\mathrm{SL}_2(\mathbf{C})$ *je izomorfna* $\rho_k \otimes \overline{\rho_\ell}$ *za neka* $k, \ell \geq 0$.

Večino od povedanega v tem razdelku je razširljivo na poljubne topološke grupe, ki imajo strukturo realne ali kompleksne mnogoterosti, pri čemer sta množenje in invertiranje zvezni, gladki ali analitični operaciji. Takim grupam pravimo **Liejeve grupe**.[21] Eksaktno korespondenco med upodobitvami Liejeve grupe in njene prirejene Liejeve algebre izgubimo, če grupa ni enostavno povezana.

**Zgled 6.2.13.** Spomnimo se grupe $\mathrm{U}_1(\mathbf{C}) \cong \mathbf{R}/\mathbf{Z}$. Njena Liejeva algebra je $\mathbf{R}$ s trivialnim Liejevim produktom in njene enorazsežne Liejeve upodobitve so linearne preslikave $\mathbf{R} \to \mathbf{C}$, torej so oblike $X \mapsto \zeta X$ za neki $\zeta \in \mathbf{C}$. To upodobitev integriramo do lokalnega homomorfizma $x \mapsto e^{\zeta x}$, ki ga obravnavamo na majhni okolici enote v $\mathbf{R}/\mathbf{Z}$. Ta preslikava se na splošno *ne* razširi do homomorfizma na celotni grupi $\mathbf{R}/\mathbf{Z}$. Se pa razširi do homomorfizma na *univerzalnem krovu* grupe $\mathbf{R}/\mathbf{Z}$, ki je ravno $\mathbf{R}$.

**Zgled 6.2.14.** Opazujmo grupo $\mathrm{SU}_2(\mathbf{C})$. Videli smo že, da je ta grupa homeomorfna sferi $S^3$. Grupa $\mathrm{SU}_2(\mathbf{C})$ je torej enostavno povezana realna Liejeva grupa. Podobno kot za grupo $\mathrm{SL}_2(\mathbf{C})$ se lahko prepričamo, da je Liejeva algebra $\mathfrak{su}_2(\mathbf{C})$ Liejeve grupe $\mathrm{SU}_2(\mathbf{C})$ enaka

$$\mathfrak{su}_2(\mathbf{C}) = \left\{ \begin{pmatrix} ib & -c+id \\ c+id & -ib \end{pmatrix} \mid b,c,d \in \mathbf{R} \right\}.$$

Kot vektorski prostor je to 3-razsežen realni vektorski prostor z bazo

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Grupa $\mathrm{SU}_2(\mathbf{C})$ deluje s konjugiranjem na $\mathfrak{su}_2(\mathbf{C})$. Na ta način dobimo upodobitev

$$\mathrm{Ad}\colon \mathrm{SU}_2(\mathbf{C}) \to \mathrm{GL}(\mathfrak{su}_2(\mathbf{C})) \cong \mathrm{GL}_3(\mathbf{R}).$$

**Domača naloga 6.2.15.** Prepričaj se, da je $\ker \mathrm{Ad} = \{I, -I\}$ in da je $\operatorname{im} \mathrm{Ad} \cong \mathrm{SO}_3(\mathbf{R})$. Upodobitve grupe $\mathrm{SO}_3(\mathbf{R})$[22] so torej ravno upodobitve enostavno povezane grupe $\mathrm{SU}_2(\mathbf{C})$, ki imajo v jedru $-I$.

## $\mathrm{SL}_2(\mathbf{R})$

Grupa $\mathrm{SL}_2(\mathbf{R})$ se pojavlja vsepočez matematike, predvsem prek svojih delovanj na različnih prostorih. Njene različne plasti odstira knjiga (Lang 1985). Zelo na kratko si bomo ogledali njeno bogato teorijo upodobitev.

[19] To je analogno temu, da na kompleksna števila $\mathbf{C}$ gledamo kot na $\mathbf{R}^2$.
[20] Opazovali bi torej Liejeve homomorfizme $\mathfrak{sl}_2(\mathbf{C}) \to \mathfrak{gl}_n(\mathbf{C})$, ki so le $\mathbf{R}$-linearni.
[21] Za celovito obravnavo Liejevih grup se lahko obrneš na zapiske (Mrčun 2024).
[22] Grupa $\mathrm{SO}_3(\mathbf{R})$ *ni* enostavno povezana. Homeomorfna je projektivnemu prostoru $\mathbf{R}P^3$.

### Gladke upodobitve

Upodobitve $\rho_k$ grupe $\mathrm{SL}_2(\mathbf{C})$ lahko zožimo na podgrupo realnih matrik $\mathrm{SL}_2(\mathbf{R})$. Na ta način z analognim razmislekom kot v prejšnjem razdelku dobimo vse dovolj lepe upodobitve.

**Posledica 6.2.16.** *Vsaka gladka nerazcepna končno razsežna kompleksna upodobitev grupe* $\mathrm{SL}_2(\mathbf{R})$ *je izomorfna* $\rho_k$ *za nek* $k \geq 0$.

V kontekstu realnih Liejevih grup se sicer izkaže, da je vsaka zvezna končno razsežna upodobitev avtomatično gladka.[23] To seveda ne velja za kompleksne Liejeve grupe, kjer lahko vsako analitično upodobitev konjugiramo in dobimo upodobitev, ki je sicer gladka, a ne nujno analitična. Upodobitve $\rho_k$ torej podajajo vse zvezne končno razsežne upodobitve grupe $\mathrm{SL}_2(\mathbf{R})$.

### Unitarne upodobitve

Nobena od upodobitev $\rho_k$ ni unitarna. Če želimo konstruirati unitarne upodobitve, moramo poseči po neskončno razsežnih vektorskih prostorih. Te upodobitve lahko konstruiramo s pomočjo delovanj grupe $\mathrm{SL}_2(\mathbf{R})$. Ogledali si bomo en primer take konstrukcije.

Grupa $\mathrm{SL}_2(\mathbf{R})$ deluje na **hiperbolični ravnini**

$$\mathbf{H} = \{z \in \mathbf{C} \mid \mathrm{Im}(z) > 0\}$$

s predpisom

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}.$$

To delovanje je tranzitivno. Ni se težko prepričati, da stabilizator točke $i \in \mathbf{H}$ sestoji iz kompaktne množice matrik

$$\mathrm{SO}_2(\mathbf{R}) = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a^2+b^2 = 1 \right\} \cong \mathrm{U}_1(\mathbf{C}) = S^1.$$

Delovanje $\mathrm{SL}_2(\mathbf{R})$ na $\mathbf{H}$ je torej ekvivalentno delovanju $\mathrm{SL}_2(\mathbf{R})$ na množici svojih desnih odsekov po kompaktni podgrupi $\mathrm{SO}_2(\mathbf{R})$. To permutacijsko delovanje na prostoru $\mathbf{C}[\mathrm{SL}_2(\mathbf{R})/\mathrm{SO}_2(\mathbf{R})]$ lahko pretvorimo v upodobitev $\rho_k$ za vsak $k \geq 2$ z delovanjem na prostorih holomorfnih integrabilnih funkcij

$$D_k = \left\{ f : \mathbf{H} \to \mathbf{C} \mid f \text{ holomorfna}, \int_{\mathbf{H}} |f(z)|^2 y^k \frac{dxdy}{y^2} < \infty \right\},$$

in sicer definiramo

$$\rho_k : \mathrm{SL}_2(\mathbf{R}) \to \mathrm{GL}(D_k), \quad \rho_k \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot f(z) = (-cz+a)^{-k} \cdot f\left( \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \cdot z \right).$$

Izkaže se, da je $\rho_k$ nerazcepna unitarna upodobitev grupe $\mathrm{SL}_2(\mathbf{R})$ na neskončno razsežnem Hilbertovem prostoru $D_k$ in da so te upodobitve med seboj neizomorfne. Na ta način dobimo celo vrsto nerazcepnih unitarnih upodobitev grupe $\mathrm{SL}_2(\mathbf{R})$, ki jim pravimo **upodobitve diskretne vrste**.

Z opazovanjem drugih zanimivih podgrup v $\mathrm{SL}_2(\mathbf{R})$ najdemo še kakšne druge unitarne upodobitve. Še posebej zanimiva je diskretna podgrupa $\mathrm{SL}_2(\mathbf{Z})$. Z njo dobimo kvocientno množico $Y = \mathrm{SL}_2(\mathbf{Z}) \backslash \mathrm{SL}_2(\mathbf{R})$. Na grupo $\mathrm{SL}_2(\mathbf{R})$ lahko s pomočjo projekcije $\mathrm{SL}_2(\mathbf{R}) \to \mathrm{SL}_2(\mathbf{R})/\mathrm{SO}_2(\mathbf{R}) = \mathbf{H}$ prenesemo mero, ki jo nato potisnemo na $Y$, tako da lahko opazujemo prostor funkcij $L^2(Y)$, na katerem deluje grupa $\mathrm{SL}_2(\mathbf{R})$. V tem prostoru lahko najdemo veliko nerazcepnih unitarnih podupodobitev. Še posebej zanimive so upodobitve, ki so konstruirane s pomočjo indukcije unitarnih upodobitev Borelove podgrupe zgornjetrikotnih matrik. Te imenujemo **upodobitve glavne vrste** in jih lahko vidimo kot posplošitev upodobitev glavne vrste iz teorije upodobitev grupe $\mathrm{GL}_2(\mathbf{F}_p)$.

[23] Poseben primer tega fenomena smo videli v razdelku o upodobitvah grupe $\mathbf{R}/\mathbf{Z}$, kjer smo dokazali, da je vsaka zvezna upodobitev grupe $\mathbf{R}$ odvedljiva.

Poleg teh dveh družin upodobitev ima grupa $\mathrm{SL}_2(\mathbf{R})$ še eno nekoliko bolj nenavadno družino unitarnih nerazcepnih upodobitev, ki jih dobimo z indukcijo določenih *neunitarnih* upodobitev Borelove podgrupe. Te upodobitve tvorijo družino **upodobitev komplementarne vrste**.

Izkaže se, da vse netrivialne nerazcepne unitarne upodobitve grupe $\mathrm{SL}_2(\mathbf{R})$ lahko dobimo iz ene od opisanih družin upodobitev.

Razumevanje neskončno razsežnih nerazcepnih unitarnih upodobitev poljubnih Liejevih grup je eden od pomembnih nedoseženih ciljev teorije upodobitev. Nekaj znanih rezultatov skupaj z vizijo o tem, kako naprej, je predstavljenih v zelo dostopnem članku (Vogan 2007).

## 6.3 Diskretne linearne grupe

Nazadnje si bomo pogledali še nekaj zgledov upodobitev diskretnih neskončnih grup, in sicer $\mathrm{SL}_m(\mathbf{Z})$. V zadnjem zgledu smo videli, da te igrajo vlogo pri opisovanju unitarnih upodobitev Liejevih grup. Te grupe niso ozaljšane z uporabno topologijo, zato bomo opazovali kar običajne abstraktne končno razsežne kompleksne upodobitve. Kot bomo videli, se te grupe obnašajo bistveno različno za $m = 2$ oziroma za $m \geq 3$.

### $\mathrm{SL}_2(\mathbf{Z})$

#### Osnovne poteze

Grupa $\mathrm{SL}_2(\mathbf{Z})$ je diskretna podgrupa Liejeve grupe $\mathrm{SL}_2(\mathbf{C})$. Ta grupa je opremljena z naravnim **kongruenčnim homomorfizmom**

$$\pi_N : \mathrm{SL}_2(\mathbf{Z}) \to \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$$

za vsako naravno število $N$, ki vnose matrike reducira po modulu $N$.

**Domača naloga 6.3.1.** Preveri, da je $\pi_N$ surjektivna za vsak $N \in \mathbf{N}$.

V posebnem za vsako praštevilo $p$ dobimo homomorfizem v grupo $\mathrm{SL}_2(\mathbf{F}_p)$, ki jo že dobro poznamo. Z analognim argumentom kot v primeru tega končnega kvocienta se prepričamo, da matriki

$$S_+ = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad S_- = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

generirata grupo $\mathrm{SL}_2(\mathbf{Z})$. V tej neskončni grupi se sicer izkaže, da nam bolj prav prideta matriki

$$A = S_+^{-1} S_- S_+^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad B = S_+^{-1} S_- = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix},$$

ki prav tako generirata $\mathrm{SL}_2(\mathbf{Z})$. Za ti dve matriki velja $A^2 = B^3 = -I$. Kot v končnem primeru lahko tvorimo **modularno grupo**

$$\mathrm{PSL}_2(\mathbf{Z}) = \frac{\mathrm{SL}_2(\mathbf{Z})}{\{I, -I\}}.$$

Naj bosta $a, b$ sliki matrik $A, B$ v $\mathrm{PSL}_2(\mathbf{Z})$. Velja torej $a^2 = b^3 = 1$. Ker matriki $a, b$ generirata grupo $\mathrm{PSL}_2(\mathbf{Z})$, lahko vsak njen element zapišemo kot besedo s črkama $a$ in $b$. Glavna prednost alternativne izbire generatorjev izhaja iz dejstva, da ima vsak element *enoličen* tak zapis.[24]

**Trditev 6.3.2.** *Vsak element $v$ $\mathrm{PSL}_2(\mathbf{Z})$ lahko enolično zapišemo v obliki*

$$b^{i_0} a b^{i_1} a \cdots b^{i_{n-1}} a b^{i_n}$$

*za nek $n \in \mathbf{N}_0$ in $i_j \in \{0, 1, 2\}$, pri čemer je $i_j \neq 0$ za vsak $j \neq 0, n$.*

[24] Rečemo, da je grupa $\mathrm{PSL}_2(\mathbf{Z})$ **prosti produkt** podgrup $\langle a \rangle = \mathbf{Z}/2\mathbf{Z}$ in $\langle b \rangle = \mathbf{Z}/3\mathbf{Z}$.

*Dokaz.* Jasno ima vsak element tak zapis, saj $a, b$ generirata $\mathrm{PSL}_2(\mathbf{Z})$ in velja $a^2 = b^3 = 1$. Preverimo še enoličnost. Predpostavimo, da je $n$ najmanjše število, za katero je izraz kot zgoraj enak 1.[25] Seveda je tedaj $n \neq 0$ in kratek račun pokaže tudi, da je $n \neq 1$. Za $n \geq 2$ konjugiramo izraz iz trditve in dobimo

$$1 = ab^{i_1}ab^{i_2}\cdots ab^{i_{n-1}}ab^{i_n+i_0}.$$

Če je $i_n + i_0$ deljivo s 3, potem je zadnji člen trivialen in po krajšanju $a$ dobimo krajši izraz enake oblike, ki je enak 1, kar je protislovno z minimalnostjo $n$. Torej $i_n + i_0$ ni deljivo s 3. To pomeni, da smo 1 zapisali kot produkt elementov $ab$ in $ab^2$. Dvignimo ta zapis v grupo $\mathrm{SL}_2(\mathbf{Z})$. Izračunamo

$$AB = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix} = -S_+, \quad AB^2 = \begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix} = -S_-,$$

zato je v $\mathrm{SL}_2(\mathbf{Z})$ neka beseda v $S_+, S_-$ dolžine $n \geq 2$ enaka $\pm I$. To pa je protislovje, saj se pri množenju matrik $S_+, S_-$ vsota vseh koeficientov matrike povečuje, torej zagotovo ne moremo dobiti matrike $\pm I$. □

### Upodobitve

Namesto upodobitev grupe $\mathrm{SL}_2(\mathbf{Z})$ opazujmo upodobitve nekoliko enostavnejše grupe $\mathrm{PSL}_2(\mathbf{Z})$. Vsak homomorfizem te grupe v katerokoli grupo $G$ je določen s sliko generatorjev $a, b$. Glede na enolično predstavitev elementov grupe $\mathrm{PSL}_2(\mathbf{Z})$ pa je res tudi obratno: za vsako izbiro elementov $X, Y \in G$ z lastnostjo $X^2 = Y^3 = 1$ lahko na enoličen način predpišemo homomorfizem[26]

$$\rho\colon \mathrm{PSL}_2(\mathbf{Z}) \to G, \quad a \mapsto X,\ b \mapsto Y.$$

Na ta način dobimo mnogo homomorfizmov v različne grupe $G$.

**Zgled 6.3.3.** Z GAP se lahko prepričamo, da je alternirajoča grupa $A_9$ generirana s permutacijama

$$(1\,4)(2\,9)(3\,7)(5\,6), \quad (1\,2\,3)(4\,5\,6)(7\,8\,9).$$

Če torej $a$ preslikamo v prvo permutacijo, $b$ pa v drugo, dobimo surjektivni homomorfizem $\alpha_9\colon \mathrm{SL}_2(\mathbf{Z}) \to A_9$. Splošneje lahko na podoben način konstruiramo surjektivni homomorfizem $\alpha_n$ v grupo $A_n$ za vsak $n \geq 9$.

**Domača naloga 6.3.4.** Prepričaj se, da za *nobeno* število $N \geq 2$ ne velja, da se homomorfizem $\alpha_9$ faktorizira prek kongruenčnega homomorfizma $\pi_N$. Natančneje, ne obstaja homomorfizem $h\colon \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z}) \to A_9$, da bi veljalo $h \circ \pi_N = \alpha_9$. V pomoč ti bo Kitajski izrek o ostankih. Kvocient $A_9$ grupe $\mathrm{SL}_2(\mathbf{Z})$ je v tem smislu *nekongruenčen*.

Grupa $\mathrm{SL}_2(\mathbf{Z})$ ima torej končne kvociente $\mathrm{PSL}_2(\mathbf{F}_p)$ in $A_n$, ki tvorijo standardne predstavnike končnih enostavnih grup. Vsaka od teh končnih grup nam da svoje nerazcepne upodobitve, s čimer po restrikciji dobimo veliko različnih nerazcepnih upodobitev grupe $\mathrm{SL}_2(\mathbf{Z})$. Teorija upodobitev grupe $\mathrm{SL}_2(\mathbf{Z})$ bo torej zajemala bolj ali manj vso kompleksnost teorije upodobitev končnih enostavnih grup. Težko si je predstavljati, kako vse te spraviti pod eno streho.

Obravnave vseh upodobitev se lotimo sistematično po razsežnostih. Vsaka $n$-razsežna kompleksna upodobitev je določena z izbiro matrik $X, Y \in \mathrm{GL}_n(\mathbf{C})$ z lastnostjo $X^2 = Y^3 = I$. Upodobitve nas zanimajo le do izomorfizma natančno, kar pomeni, da moramo za razumevanje izomorfnostnih razredov upodobitev razumeti kvocientno množico

$$\mathrm{Rep}_n = \frac{\{(X, Y) \in \mathrm{GL}_n(\mathbf{C}) \times \mathrm{GL}_n(\mathbf{C}) \mid X^2 = Y^3 = I\}}{\mathrm{GL}_n(\mathbf{C})},$$

[25] Če nek element lahko zapišemo v želeni obliki na dva načina, potem vse črke prenesemo na eno stran enakosti in s tem tudi 1 zapišemo na netrivialen način v želeni obliki.

[26] To je analog razširjanja lokalnega homomorfizma, ki smo ga videli pri grupi $\mathrm{SL}_2(\mathbf{C})$. Tam nismo imeli enoličnosti zapisa kot tukaj, zato smo se morali potruditi z dokazovanjem dobre definiranosti razširitve homomorfizma z $U$ na ves $\mathrm{SL}_2(\mathbf{C})$. Tukaj to dobimo zastonj.

pri čemer grupa $\mathrm{GL}_n(\mathbf{C})$ deluje s hkratnim konjugiranjem na parih matrik, se pravi $A\cdot(X,Y) = (AXA^{-1},AYA^{-1})$ za $A\in\mathrm{GL}_n(\mathbf{C})$.[27] Elementi množice $\mathrm{Rep}_n$ predstavljajo ravno vse predstavnike izomorfnostnih razredov $n$-razsežnih upodobitev grupe $\mathrm{PSL}_2(\mathbf{Z})$.

Opišimo najprej enorazsežne upodobitve $\mathrm{Rep}_1$. Za števili $X,Y\in\mathbf{C}^*$ mora veljati $X\in\{1,-1\}$ in $Y\in\{1,\zeta,\zeta^2\}$, kjer je $\zeta = e^{2\pi i/3}$. Delovanje grupe $\mathbf{C}^*$ na parih je v tem primeru kar trivialno. Velja torej

$$\mathrm{Rep}_1 = \{1,-1\}\times\{1,\zeta,\zeta^2\}$$

in imamo 6 enorazsežnih upodobitev grupe $\mathrm{PSL}_2(\mathbf{Z})$.

Oglejmo si sedaj še dvorazsežne upodobitve $\mathrm{Rep}_2$. Kot bomo videli, je teh *neštevno mnogo*. Sistematično obravnavajmo vse možnosti za matriki $X,Y$.

1. Če je $X$ ali $Y$ skalarna matrika, potem lahko s konjugiranjem dosežemo, da sta obe matriki hkrati diagonalni. Predpostavimo najprej, da je $X$ skalarna. Zaradi pogoja $X^2 = I$ to pomeni, da je $X = \alpha I$ za $\alpha\in\{1,-1\}$. Po konjugiranju lahko dosežemo, da je $Y$ diagonalna matrika z diagonalnima členoma $a,b\in\{1,\zeta,\zeta^2\}$ (upoštevajoč $Y^3 = I$). Imamo torej dve možnosti za $X$ in šest možnosti za $Y$. Oglejmo si zdaj še možnost, ko je $Y$ skalarna, $X$ pa ni skalarna. To pomeni $Y = \beta I$ za $\beta\in\{1,\zeta,\zeta^2\}$. Po konjugiranju lahko dosežemo, da je $X$ diagonalna matrika z diagonalnima členoma $1,-1$ ($X$ ni skalarna in $X^2 = I$). Imamo torej tri možnosti za $Y$ in eno samo za $X$. Skupaj dobimo 15 upodobitev. Vse te upodobitve so seveda razcepne.

2. Če niti $X$ niti $Y$ nista skalarni matriki, potem imata obe dve različni lastni vrednosti. Po konjugiranju lahko matriki $X$, $Y$ zato zapišemo v obliki

$$X = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},\quad Y = \begin{pmatrix}a & b\\ c & d\end{pmatrix}$$

za neke $a,b,c,d\in\mathbf{C}$. Centralizator matrike $X$ v $\mathrm{GL}_2(\mathbf{C})$ je enak torusu diagonalnih matrik. S temi matrikami lahko torej še dodatno konjugiramo in poenostavimo matriko $Y$. Ločimo več možnosti.[28]

   (a) Če je $c = 0$ in $b = 0$, potem je $Y$ diagonalna matrika. Njeni lastni vrednosti sta različna tretja korena enote, zato je $Y$ oblike

$$Y = \begin{pmatrix}a & 0\\ 0 & d\end{pmatrix}$$

   za $a,d\in\{1,\zeta,\zeta^2\}$, $a\neq d$. Vse te upodobitve so seveda razcepne. Število vseh je 6.

   (b) Če je $c = 0$ in $b\neq 0$, potem je $Y$ zgornjetrikotna matrika. Njeni lastni vrednosti sta različna tretja korena enote in z dodatnim konjugiranjem z diagonalno matriko dosežemo, da je $b = 1$, zato je $Y$ oblike

$$Y = \begin{pmatrix}a & 1\\ 0 & d\end{pmatrix}$$

   za $a,d\in\{1,\zeta,\zeta^2\}$, $a\neq d$. Vse te upodobitve so seveda razcepne. Število vseh je 6.

   Analogno dobimo 6 razcepnih upodobitev, ko je $c\neq 0$ in $b = 0$.

   (c) Če je $c\neq 0$ in $b\neq 0$, potem z dodatnim konjugiranjem z diagonalno matriko dosežemo, da je $Y$ oblike

$$Y = \begin{pmatrix}a & b\\ 1 & d\end{pmatrix}$$

   za $b\in\mathbf{C}^*$. Pri tem je determinanta te matrike enaka $\delta = ad - b$, sled pa je enaka $\tau = a + d$. Ker sta lastni vrednosti $Y$ različna tretja korena enota, so edine možnosti

$$(\tau,\delta)\in\{(\zeta+\zeta^2,1),(1+\zeta,\zeta),(1+\zeta^2,\zeta^2)\}.$$

[27] Para matrik $(X,Y)$ in $(X',Y')$ sta torej ekvivalentna, če in samo če za neko matriko $A\in\mathrm{GL}_n(\mathbf{C})$ velja $(X,Y) = A\cdot(X',Y')$.

[28] Obravnava je analogna razumevanju konjugiranostnih razredov v končni grupi $\mathrm{GL}_2(\mathbf{F}_p)$, le da je tu nekoliko preprostejša, ker ni nerazcepnega torusa.

Za vsako od teh možnosti števili $a, d$ določimo kot rešitvi enačbe $\lambda^2 - \tau\lambda + \delta + b = 0$. Če je $b = (\tau^2 - 4\delta)/4$, dobimo eno samo matriko $Y$, sicer pa imamo dve različni možnosti. Vse te upodobitve so nerazcepne, saj $Y$ v nobenem primeru ne ohranja nobenega od standardnih baznih podprostorov. Vseh teh upodobitev je neštevno mnogo.

Sorodno obravnavo bi lahko izvedli v poljubni razsežnosti.

**Posledica 6.3.5.** *Grupa* $\mathrm{SL}_2(\mathbf{Z})$ *ima neštevno mnogo kompleksnih nerazcepnih upodobitev poljubne stopnje, večje od* 1.

## $\mathrm{SL}_3(\mathbf{Z})$

Oglejmo si še grupo $\mathrm{SL}_3(\mathbf{Z})$ kot zgled *aritmetične mreže višjega ranga*.

### Prezentacija

Upodobitve $\mathrm{SL}_3(\mathbf{Z})$ bi lahko skušali razumeti na podoben način kot $\mathrm{SL}_2(\mathbf{Z})$. Standardna generatorska množica sestoji iz matrik oblike $T_{ij} = I + E_{ij}$ za $1 \leq i, j \leq 3$, $i \neq j$, pri čemer je $E_{ij}$ matrika z vnosom 1 na mestu $(i, j)$ in 0 sicer. Kot v prejšnjem razdelku pa se zadeve poenostavijo z nestandardno izbiro generatorjev

$$x = \begin{pmatrix} 1 & 0 & 1 \\ 0 & -1 & -1 \\ 0 & 1 & 0 \end{pmatrix}, \quad y = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad z = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ -1 & -1 & -1 \end{pmatrix}.$$

Na ta način lahko dobimo precej preprosto **prezentacijo** te grupe, ki je podobna zelo uporabnemu opisu grupe $\mathrm{PSL}_2(\mathbf{Z})$ z generatorjema $a, b$ iz prejšnjega razdelka. Bistvena razlika je, da ta prezentacija vsebuje nekaj pogojev med generatorji $x, y, z$, ki niso tako zelo enostavne oblike kot v grupi $\mathrm{PSL}_2(\mathbf{Z})$. Izkaže se (Conder-Robertson-Williams 1992), da vse te pogoje lahko zajamemo z naslednjimi enakostmi:[29]

$$x^3 = y^3 = z^2 = (xz)^3 = (yz)^3 = (x^{-1}zxy)^2 = (y^{-1}zyx)^2 = (xy)^6 = I.$$

Z drugimi besedami, če želimo podati upodobitev $\mathrm{SL}_3(\mathbf{Z})$ v $\mathrm{GL}_n(\mathbf{C})$, potem moramo izbrati matrike $X, Y, Z \in \mathrm{GL}_n(\mathbf{C})$, ki zadoščajo vsem tem enakostim. Vsaka taka izbira se enolično razširi do upodobitve, ki preslika $x, y, z$ v $X, Y, Z$.

Če naivno skušamo poiskati matrike v $\mathrm{GL}_2(\mathbf{C})$ ali $\mathrm{GL}_3(\mathbf{C})$, ki zadoščajo tem enakostim, odkrijemo, da zaradi teh dodatnih restriktivnih pogojev dobimo *bistveno manj* rešitev kot v primeru grupe $\mathrm{PSL}_2(\mathbf{Z})$. Teorija upodobitev grupe $\mathrm{SL}_3(\mathbf{Z})$ je, kot bomo videli, precej bolj strukturirana.

### Končni kvocienti

Razliko med grupo $\mathrm{SL}_2(\mathbf{Z})$ in $\mathrm{SL}_3(\mathbf{Z})$ lahko jasno vidimo v njunih končnih kvocientih. Kot v dvorazsežnem primeru imamo surjektivne **kongruenčne homomorfizme**

$$\pi_N : \mathrm{SL}_3(\mathbf{Z}) \to \mathrm{SL}_3(\mathbf{Z}/N\mathbf{Z}).$$

Jedra teh homomorfizmov so **kongruenčne podgrupe**. Izkaže se (Bass-Lazard-Serre 1964), da pa tukaj (in v vseh $\mathrm{SL}_m(\mathbf{Z})$ za $m \geq 3$) *ni* nobenih bistveno drugačnih homomorfizmov v končne grupe. Natančneje, vsak homomorfizem $\alpha : \mathrm{SL}_3(\mathbf{Z}) \to G$ v končno grupo $G$ se faktorizira prek nekega kongruenčnega homomorfizma $\pi_N$. Povedano še drugače, vsaka podgrupa $H \leq \mathrm{SL}_3(\mathbf{Z})$ končnega indeksa vsebuje neko kongruenčno podgrupo. Tej lastnosti grupe $\mathrm{SL}_3(\mathbf{Z})$ rečemo **lastnost kongruenčnih podgrup**.[30]

Vsak končni kvocient $G$ grupe $\mathrm{SL}_3(\mathbf{Z})$ ima svoje nerazcepne upodobitve, ki jih z restrikcijo potegnemo do nerazcepnih upodobitev grupe $\mathrm{SL}_3(\mathbf{Z})$. Po lastnosti kongruenčnih podgrupe je tak $G$ nujno kvocient

[29] Rečemo, da je grupa $\mathrm{SL}_3(\mathbf{Z})$ dana s prezentacijo z *generatorji* $x, y, z$ in *relacijami*, ki jih podajajo te enakosti. Glej Teorijo grup za podrobnosti glede te konstrukcije in več zgledov.

[30] Angleško *congruence subgroup property*.

$\mathrm{SL}_3(\mathbf{Z}/N\mathbf{Z})$ za neki $N$, zato bo dovolj opazovati nerazcepne upodobitve kongruenčnih kvocientov. Če je $N$ praštevilo, te zelo dobro razumemo s tehnikami upodobitev končnih grup. Na splošno iz praštevilske faktorizacije $N = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ z uporabo Kitajskega izreka o ostankih dobimo

$$\mathrm{SL}_3(\mathbf{Z}/N\mathbf{Z}) \cong \mathrm{SL}_3(\mathbf{Z}/p_1^{k_1}\mathbf{Z}) \times \mathrm{SL}_3(\mathbf{Z}/p_2^{k_2}\mathbf{Z}) \times \cdots \times \mathrm{SL}_3(\mathbf{Z}/p_m^{k_m}\mathbf{Z}).$$

Razumeti moramo torej upodobitve grup $\mathrm{SL}_3(\mathbf{Z}/p^k\mathbf{Z})$ za praštevilo $p$ in vse potence $k \geq 1$.

### $p$-adične grupe

Vse kolobarje $\mathbf{Z}/p^k\mathbf{Z}$ za $k \geq 1$ lahko opazujemo hkrati, in sicer tako, da jih zložimo v ravno vrsto

$$\cdots \to \mathbf{Z}/p^k\mathbf{Z} \to \cdots \to \mathbf{Z}/p^2\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z},$$

pri čemer so homomorfizmi $r_k : \mathbf{Z}/p^k\mathbf{Z} \to \mathbf{Z}/p^{k-1}\mathbf{Z}$ redukcije po modulu $p^{k-1}$. Tvorimo **inverzno limito** te vrste,

$$\varprojlim_{k\in\mathbf{N}} \mathbf{Z}/p^k\mathbf{Z} = \left\{(\ldots, x_k, \ldots, x_2, x_1) \in \textstyle\prod_{k\in\mathbf{N}} \mathbf{Z}/p^k\mathbf{Z} \mid \forall k \in \mathbf{N}\colon\ r_k(x_k) = x_{k-1}\right\}.$$

Ker je vsak $\mathbf{Z}/p^k\mathbf{Z}$ kolobar, je tudi ta limita kolobar. Pravimo mu kolobar **$p$-adičnih celih števil** in ga označimo z $\mathbf{Z}_p$. Kolobar celih števil $\mathbf{Z}$ se naravno vloži v $\mathbf{Z}_p$ s preslikavo $n \mapsto (n)_{k\in\mathbf{N}}$.

Vse končne kolobarje $\mathbf{Z}/p^k\mathbf{Z}$ opremimo z diskretno topologijo in njihov produkt s produktno topologijo, tako da je $\mathbf{Z}_p$ tudi topološki prostor. Po izreku Tihonova je produkt vseh $\mathbf{Z}/p^k\mathbf{Z}$ kompakten, $\mathbf{Z}_p$ pa tvori zaprto množico v tem produktu, zato je tudi $\mathbf{Z}_p$ kompakten topološki prostor.[31]

Na enak način lahko opazujemo vse grupe $\mathrm{SL}_3(\mathbf{Z}/p^k\mathbf{Z})$ hkrati. Zložimo jih v ravno vrsto

$$\cdots \to \mathrm{SL}_3(\mathbf{Z}/p^k\mathbf{Z}) \to \cdots \to \mathrm{SL}_3(\mathbf{Z}/p^2\mathbf{Z}) \to \mathrm{SL}_3(\mathbf{Z}/p\mathbf{Z})$$

s prehodnimi homomorfizmi $r_k : \mathrm{SL}_3(\mathbf{Z}/p^k\mathbf{Z}) \to \mathrm{SL}_3(\mathbf{Z}/p^{k-1}\mathbf{Z})$ in tvorimo inverzno limito

$$\varprojlim_{k\in\mathbf{N}} \mathrm{SL}_3(\mathbf{Z}/p^k\mathbf{Z}) = \mathrm{SL}_3(\varprojlim_{k\in\mathbf{N}} \mathbf{Z}/p^k\mathbf{Z}) = \mathrm{SL}_3(\mathbf{Z}_p).$$

Grupa $\mathrm{SL}_3(\mathbf{Z}_p)$ podeduje topologijo iz prostora $\mathbf{Z}_p^9$, zato je kompaktna topološka grupa. Ta grupa naravno vsebuje $\mathrm{SL}_3(\mathbf{Z})$ in po definiciji je opremljena z zveznimi projekcijami v kongruenčne kvociente

$$\widetilde{\pi_{p^k}} : \mathrm{SL}_3(\mathbf{Z}_p) \to \mathrm{SL}_3(\mathbf{Z}/p^k\mathbf{Z})$$

za vsak $k \in \mathbf{N}$. Ker so končni kvocienti opremljeni z diskretno topologijo, so jedra teh homomorfizmov odprte podgrupe v $\mathrm{SL}_3(\mathbf{Z}_p)$. Ko $k$ raste, te podgrupe postajajo vedno manjše.

**Trditev 6.3.6.** *Podgrupe* $\ker \widetilde{\pi_{p^k}}$ *za* $k \in \mathbf{N}$ *tvorijo bazo okolic enote v* $\mathrm{SL}_3(\mathbf{Z}_p)$.

*Dokaz.* Naj bo $U$ odprta okolica enote v $\mathrm{SL}_3(\mathbf{Z}_p)$. Velja torej $U = \mathrm{SL}_3(\mathbf{Z}_p) \cap V$ za neko odprto množico $V$ v produktu vseh $\mathrm{SL}_3(\mathbf{Z}/p^k\mathbf{Z})$. Po definiciji produktne topologije množica $V$ vsebuje odprto množico oblike

$$\prod_{k\leq K} 1 \times \prod_{k>K} \mathrm{SL}_3(\mathbf{Z}/p^k\mathbf{Z}).$$

Torej $U$ vsebuje presek te množice z $\mathrm{SL}_3(\mathbf{Z}_p)$, kar je natanko $\ker \widetilde{\pi_{p^K}}$. □

Iz te lastnosti je razvidno, da se grupa $\mathrm{SL}_3(\mathbf{Z}_p)$ obnaša zelo drugače kot Liejeva grupa $\mathrm{SL}_3(\mathbf{C})$.

**Domača naloga 6.3.7.** S pomočjo eksponentne preslikave dokaži, da v grupi $\mathrm{GL}_n(\mathbf{C})$ obstaja odprta okolica enote $U$, ki ne vsebuje nobene netrivialne podgrupe.[32]

[31] Topologija na $\mathbf{Z}_p$ je nekoliko neobičajna. Dobimo namreč popolnoma nepovezan topološki prostor. Predstavljamo si ga lahko kot Cantorjevo množico, kot je prikazano tukaj.

[32] Tej lastnosti pravimo **brez majhnih podgrup**, angleško *no small subgroups*.

Kljub tej razliki pa je vendarle zelo plodno gledati na $\mathrm{SL}_3(\mathbf{Z}_p)$ kot na podgrupo splošne linearne grupe $\mathrm{GL}_3(\mathbf{Q}_p)$ poljem kvocientov $\mathbf{Q}_p$ kolobarja $\mathbf{Z}_p$ in jo v tej luči obravnavati kot neke vrste Liejevo grupo nad sicer nenavadnim poljem $\mathbf{Q}_p$. Grupa $\mathrm{SL}_3(\mathbf{Z}_p)$ je na ta način poseben primer **$p$-adične analitične grupe**. Razviti je mogoče analogno teorijo Liejevih grup nad $p$-adičnimi števili, ki omogoča, da njihove upodobitve razumemo s pomočjo njihovih prirejenih Liejevih algeber. Na ta način je mogoče izpeljati veliko zanimivih rezultatov o upodobitvah teh grup. Na primer (Aizenbud-Avni 2015), obstaja konstanta $C$, da je število nerazcepnih kompleksnih $n$-razsežnih upodobitev grupe $\mathrm{SL}_m(\mathbf{Z}_p)$ kvečjemu $Cn^{22}$ za vsak $m \geq 3$.

Vse upodobitve kongruenčnih kvocientov grupe $\mathrm{SL}_3(\mathbf{Z})$ lahko torej zajamemo tako, da opazujemo le upodobitve $p$-adične kompaktne grupe $\mathrm{SL}_3(\mathbf{Z}_p)$. Prepričajmo se še, da na ta način ne bomo zajeli nič drugih upodobitev.

**Trditev 6.3.8.** *Vsaka zvezna končno razsežna kompleksna upodobitev grupe $\mathrm{SL}_3(\mathbf{Z}_p)$ se faktorizira prek $\widetilde{\pi_{p^k}}$ za nek $k \in \mathbf{N}$.*

*Dokaz.* Naj bo $\rho\colon \mathrm{SL}_3(\mathbf{Z}_p) \to \mathrm{GL}_n(\mathbf{C})$ zvezna upodobitev. Naj bo $U$ odprta okolica enote v $\mathrm{GL}_n(\mathbf{C})$, ki ne vsebuje netrivialnih podgrup. Praslika $\rho^{-1}(U)$ je odprta okolica enote v $\mathrm{SL}_3(\mathbf{Z}_p)$, zato vsebuje neko kongruenčno jedro $\ker \widetilde{\pi_{p^k}}$. Slika $\rho(\ker \widetilde{\pi_{p^k}})$ je podgrupa v $U$, zato je trivialna. Jedro $\ker \rho$ torej vsebuje to kongruenčno jedro. □

Nazadnje lahko torej vse upodobitve grupe $\mathrm{SL}_3(\mathbf{Z})$, ki se faktorizirajo prek upodobitev končnih grup, razumemo kot zožitve zveznih upodobitev produktov $p$-adičnih grup po vseh praštevilih $p$, se pravi zveznih upodobitev grupe

$$\prod_{p \in \mathbf{P}} \mathrm{SL}_3(\mathbf{Z}_p),$$

ki jo označimo kot $\mathrm{SL}_3(\widehat{\mathbf{Z}})$.

**Domača naloga 6.3.9.** Postojmo pri skrivnostnem objektu $\widehat{\mathbf{Z}}$. Za vsako praštevilo $p$ smo definirali kolobar $\mathbf{Z}_p$ kot inverzno limito kolobarjev $\mathbf{Z}/p^k\mathbf{Z}$ glede na naravne prehodne homomorfizme med temi končnimi kolobarji. Na soroden način definiramo kolobar $\widehat{\mathbf{Z}}$ kot inverzno limito končnih kolobarjev $\mathbf{Z}/n\mathbf{Z}$ za vse $n \in \mathbf{N}$ glede na naravno prehodne homomorfizme med temi končnimi kolobarji (zdaj ti končni kolobarji niso več zloženi v vrsto, ampak v neko mrežo). Kolobar $\widehat{\mathbf{Z}}$ lahko gledamo kot podkolobar produkta $\prod_{n \in \mathbf{N}} \mathbf{Z}/n\mathbf{Z}$, opremljenega s produktno topologijo. Kolobar celih števil $\mathbf{Z}$ se na naraven način vloži v $\widehat{\mathbf{Z}}$.

S pomočjo Kitajskega izreka o ostankih se prepričaj, da imamo izomorfizem kolobarjev $\widehat{\mathbf{Z}} \cong \prod_{p \in \mathbf{P}} \mathbf{Z}_p$, ki je hkrati homeomorfizem topoloških prostorov (pri čemer na desni uporabimo produktno topologijo).

Premisli, da so obrnljivi elementi v $\widehat{\mathbf{Z}}$ ravno množica $\overline{\mathbf{P}} \setminus \mathbf{P}$, kjer smo s simbolom $\overline{\mathbf{P}}$ označili topološko zaprtje množice vseh praštevil v $\widehat{\mathbf{Z}}$.

### Nerazcepne upodobitve

Nerazcepne upodobitve grupe $\mathrm{SL}_3(\mathbf{Z})$ lahko konstruiramo s pomočjo nerazcepnih upodobitev grupe $\mathrm{SL}_3(\widehat{\mathbf{Z}})$ ali pa kot restrikcijo nerazcepnih upodobitev običajne Liejeve grupe $\mathrm{SL}_3(\mathbf{C})$. Te upodobitve lahko tenzorsko množimo med seboj. Neverjetno je, da na ta način dobimo *vse* nerazcepne upodobitve grupe $\mathrm{SL}_3(\mathbf{Z})$. Konceptualno lahko to pojasnimo z naslednjo lastnostjo *dviganja* upodobitev.

**Izrek 6.3.10** (Lubotzky 1980)**.** *Naj bo $\rho\colon \mathrm{SL}_3(\mathbf{Z}) \to \mathrm{GL}_n(\mathbf{C})$ upodobitev. Tedaj obstaja upodobitev*

$$\tilde{\rho}\colon \mathrm{SL}_3(\mathbf{C}) \times \mathrm{SL}_3(\widehat{\mathbf{Z}}) \to \mathrm{GL}_n(\mathbf{C}),$$

*katere zožitev na diagonalno vloženo podgrupo $\mathrm{SL}_3(\mathbf{Z})$ je ravno $\rho$, zožitev na $\mathrm{SL}_3(\mathbf{C})$ je polinomska upodobitev, zožitev na $\mathrm{SL}_3(\widehat{\mathbf{Z}})$ pa je zvezna upodobitev.*

Izrek sloni na **Margulisovi superrigidnosti** diskretnih podgrup v Liejevih grupah. Za grupo $\mathrm{SL}_3(\mathbf{Z})$ jo lahko izrazimo na naslednji način.

**Izrek 6.3.11** (Margulis 1991)**.** *Naj bo* $\rho\colon \mathrm{SL}_3(\mathbf{Z}) \to \mathrm{GL}_n(\mathbf{C})$ *upodobitev. Tedaj obstaja polinomska upodobitev* $\tilde{\rho}\colon \mathrm{SL}_3(\mathbf{C}) \to \mathrm{GL}_n(\mathbf{C})$*, ki se na nekem kongruenčnem jedru* $\ker \pi_N$ *ujema z* $\rho$*.*

*Dokaz.* (ideja dokaza iz (Steinberg 1985)) Grupa $\mathrm{SL}_3(\mathbf{Z})$ je generirana z matrikami $T_{ij} = I + E_{ij}$ za $i \neq j$. Te matrike niso zelo blizu identitete v $\mathrm{SL}_3(\mathbf{C})$, zato jih ne moremo potisniti v Liejevo algebro $\mathfrak{sl}_3(\mathbf{C})$ z logaritmom. Lahko pa vseeno formalno izračunamo njihov logaritem. Ker je $E_{ij}^2 = 0$, je $\log T_{ij} = E_{ij} \in \mathfrak{sl}_3(\mathbf{C})$. Z nekaj računanja se prepričamo, da matrike $E_{ij}$ generirajo Liejevo algebro $\mathfrak{sl}_3(\mathbf{C})$.

Nekaj podobnega lahko naredimo v sliki upodobitve $\rho$. Matrike $\rho(T_{ij})$ so daleč od identitete v $\mathrm{GL}_n(\mathbf{C})$. Vsako lahko zapišemo v Jordanski obliki kot produkt diagonalne matrike $\rho(T_{ij})_s$ (*polenostavni del*) in matrike z enicami po diagonali $\rho(T_{ij})_u$ (*unipotentni del*). Za unipotentni del velja $(\rho(T_{ij})_u - I)^n = 0$, zato lahko izračunamo logaritem $\log \rho(T_{ij})_u \in \mathfrak{gl}_n(\mathbf{C})$ z razvojem v končno Taylorjevo vrsto. Z nekaj računanja se prepričamo, da matrike $\log \rho(T_{ij})_u$ generirajo Liejevo algebro $\mathfrak{sl}_3(\mathbf{C})$ znotraj $\mathfrak{gl}_n(\mathbf{C})$.

Obe Liejevi algebri lahko povežemo z Liejevo upodobitvijo $\phi\colon \mathfrak{sl}_3(\mathbf{C}) \to \mathfrak{gl}_n(\mathbf{C})$, ki jo definiramo kot $E_{ij} \mapsto \log \rho(T_{ij})_u$. To upodobitev pointegriramo do upodobitve grup $\tilde{\rho}\colon \mathrm{SL}_3(\mathbf{C}) \to \mathrm{GL}_n(\mathbf{C})$.

Konstrukcija $\tilde{\rho}$ sloni le na uporabi unipotenih delov $\rho(T_{ij})$. Z nekaj računanja se prepričamo, da za število $N = n!$ velja $\rho(T_{ij})_s^N = I$. Od tod hitro sledi, da na kongruenčnem jedru $\ker \pi_N$ polenostavni del nima vpliva, zato se $\rho$ in $\tilde{\rho}$ na tem jedru ujemata. □

**Domača naloga 6.3.12.** Oglej si videoposnetek predavanja, kjer Lubotzky z uporabo nekaj osnovnih lastnosti $p$-adičnih analitičnih grup skicira, kako lastnost kongruenčnih podgrup implicira Margulisovo superrigidnost.

Vsaka upodobitev $\mathrm{SL}_3(\mathbf{Z})$ torej do končnega kvocienta natančno izhaja iz upodobitve $\mathrm{SL}_3(\mathbf{C})$. Da pokrijemo še vse možne končne kvociente, upoštevamo še zvezne upodobitve $\mathrm{SL}_3(\widehat{\mathbf{Z}})$. Z nekaj truda se da s to intuicijo hitro izpeljati Lubotzkyjev izrek.

**Domača naloga 6.3.13.** Preberi dokaz Lubotzkyjevega izreka v (Putman).

**Posledica 6.3.14.** *Nerazcepne končno razsežne kompleksne upodobitve grupe* $\mathrm{SL}_3(\mathbf{Z})$ *so zožitve tenzorskih produktov nerazcepnih polinomskih upodobitev grupe* $\mathrm{SL}_3(\mathbf{C})$ *in nerazcepnih zveznih upodobitev grupe* $\mathrm{SL}_3(\widehat{\mathbf{Z}})$*.*

V posebnem je vseh nerazcepnih upodobitev $\mathrm{SL}_3(\mathbf{Z})$ le števno mnogo, kar je v ostrem nasprotju z neštevno mnogo upodobitvami $\mathrm{SL}_2(\mathbf{Z})$. Vse povedano se da razširiti na grupe $\mathrm{SL}_m(\mathbf{Z})$ za $m \geq 3$.