UPODOBITVE SIMETRIČNIH GRUP

MATEVŽ MIŠČIČ

Fakulteta za matematiko in fiziko
Univerza v Ljubljani

V članku so obravnavane upodobitve končnih grup. Definirane so nerazcepne upodobitve in dokazano je, da je vsaka upodobitev končne grupe direktna vsota nerazcepnih upodobitev. Klasificirane so vse nerazcepne upodobitve simetričnih grup.

REPRESENTATIONS OF SYMMETRIC GROUPS

In this paper representation theory of finite groups is presented. Irreducible representations are defined and it is shown that every representation of a finite group is a direct sum of irreducible representations. All irreducible representations of symmetric groups are classified.

1. Uvod

Upodobitev grupe G je homomorfizem grup iz G v neko splošno linearno grupo. S pomočjo upodobitev lahko vsak element grupe predstavimo z neko obrnljivo matriko. Na ta način si lahko pri problemih iz teorije grup pomagamo z linearno algebro, ki jo dobro poznamo.

Ta članek je razdeljen na dva dela. V prvem delu bomo spoznali osnove teorije upodobitev končnih grup. Naučili se bomo, kdaj je neka upodobitev nerazcepna in kaj je karakter upodobitve. Ko bomo seznanjeni z osnovami te teorije, se bomo posvetili upodobitvam simetrične grupe, ki bodo glavna tema drugega dela. Glavni cilj tega dela bo poiskati vse nerazcepne upodobitve simetrične grupe. Nazadnje pa bomo poiskali še baze vektorskih prostorov, v katere te upodobitve slikajo.

2. Upodobitve grup

V tem poglavju bomo spoznali nekaj osnovnih dejstev o upodobitvah grup.

Definicija 1. *Upodobitev grupe* G je homomorfizem grup $\rho : G \to \mathrm{GL}(V)$, kjer je $\mathrm{GL}(V)$ grupa avtomorfizmov končnorazsežnega kompleksnega vektorskega prostora V. Dimenziji $\dim V$ rečemo *stopnja upodobitve* ρ.

Načeloma upodobitev grupe lahko slika v poljuben (ne nujno končnorazsežen) vektorski prostor nad poljubnim obsegom, mi pa se bomo ukvarjali le s končnorazsežnimi kompleksnimi upodobitvami, zato smo se na take upodobitve omejili že v definiciji. V nadaljevanju bo torej vsak vektorski prostor končnorazsežen in kompleksen. Omejimo se tudi samo na končne grupe.

Če na d-dimenzionalnem prostoru V fiksiramo bazo, dobimo izomorfizem grup med $\mathrm{GL}(V)$ in $\mathrm{GL}_d(\mathbb{C})$, torej lahko vsako upodobitev obravnavamo kot homomorfizem v ustrezno splošno linearno grupo.

Naj bo $\rho : G \to \mathrm{GL}(V)$ upodobitev. Za $x \in G$ bomo avtomorfizem $\rho(x)$ prostora V pogosto označili kar z ρ_x.

Zgled 1. Oglejmo si nekaj primerov upodobitev.

1. Trivialni homomorfizem $\rho : G \to \mathrm{GL}(V)$ v enodimenzionalen vektorski prostor V je *trivialna upodobitev grupe G*.

2. Naj G deluje na končno množico X in naj bo V vektorski prostor z bazo $B = \{e_x \mid x \in X\}$. Za $g \in G$ bomo endomorfizem ρ_g prostora V definirali na bazi B: $\rho_g(e_x) = e_{g \cdot x}$. Ker ρ_g preslika B bijektivno na B, je avtomorfizem prostora V. Za vsaka $g, h \in G$ velja tudi $\rho_g \circ \rho_h = \rho_{gh}$, torej je $\rho : G \to \mathrm{GL}(V)$ upodobitev grupe G. Taki upodobitvi bomo rekli *permutacijska upodobitev delovanja G na X*.

3. Grupa G deluje nase z množenjem. Permutacijsko upodobitev tega delovanja imenujemo *regularna upodobitev grupe G*. To je upodobitev $\rho : G \to \mathrm{GL}(V)$ v prostoru V z bazo $\{e_s \mid s \in G\}$. Velja $\rho_g(e_s) = e_{gs}$.

4. Grupa S_n naravno deluje na množici $\{1, 2, \ldots, n\}$. Permutacijski upodobitvi tega delovanja pa rečemo *permutacijska upodobitev grupe S_n*.

5. Upodobitvi $\rho : S_n \to \mathrm{GL}(\mathbb{C})$ s predpisom $\rho_\sigma(z) = \mathrm{sgn}(\sigma) z$ pravimo *alternirajoča upodobitev S_n*.

V algebri pogosto obravnavamo algebrske strukture do izomorfizma natančno. Podobno bomo naredili pri upodobitvah.

Definicija 2. Upodobitvi $\rho^1 : G \to \mathrm{GL}(V_1)$ in $\rho^2 : G \to \mathrm{GL}(V_2)$ sta *ekvivalentni*, če obstaja izomorfizem vektorskih prostorov $f : V_1 \to V_2$, da za vsak $x \in G$ velja $\rho^2_x f = f \rho^1_x$.

$$\begin{array}{ccc} V_1 & \xrightarrow{f} & V_2 \\ \downarrow{\scriptstyle \rho^1_x} & & \downarrow{\scriptstyle \rho^2_x} \\ V_1 & \xrightarrow{f} & V_2 \end{array}$$

Oglejmo si še en način kako lako gledamo na upodobitve.

Definicija 3. Naj bo $\mathbb{F}$ polje in $G = \{x_1, \ldots, x_n\}$ grupa. Označimo z $\mathbb{F}[G]$ množico vseh $\mathbb{F}$-linearnih kombinacij elementov grupe G. Na tej množici definiramo seštevanje, množenje s skalarji in množenje s predpisi

$$\sum_{i=1}^{n} \alpha_i x_i + \sum_{i=1}^{n} \beta_i x_i = \sum_{i=1}^{n} (\alpha_i + \beta_i) x_i,$$

$$\lambda \left(\sum_{i=1}^{n} \alpha_i x_i \right) = \sum_{i=1}^{n} (\lambda \alpha_i) x_i,$$

$$\left(\sum_{i=1}^{n} \alpha_i x_i \right) \left(\sum_{i=1}^{n} \beta_i x_i \right) = \sum_{i=1}^{n} \left(\sum_{x_j x_k = x_i} \alpha_j \beta_k \right) x_i.$$

S temi operacijami množica $\mathbb{F}[G]$ postane algebra, ki ji pravimo *grupna algebra*.

Iz upodobitve $\rho : G \to \mathrm{GL}(V)$ dobimo linearno delovanje grupne algebre $\mathbb{C}[G]$ na vektorski prostor V:

$$\left(\sum_{i=1}^{n} \alpha_i x_i \right) \cdot v = \sum_{i=1}^{n} \alpha_i \rho(x_i) v.$$

S tem V postane $\mathbb{C}[G]$-modul. Včasih namesto o upodobitvah govorimo o modulih, še posebej pogosto je tako v primeru upodobitev simetričnih grup.

2.1 Nerazcepne upodobitve

Iz dveh upodobitev neke grupe lahko sestavimo novo upodobitev te grupe na naslednji način:

Definicija 4. Naj bosta $\rho^1 : G \to \mathrm{GL}(V_1)$ in $\rho^2 : G \to \mathrm{GL}(V_2)$ upodobitvi grupe G. Njuna *zunanja direktna vsota* je upodobitev $\rho^1 \oplus \rho^2 : G \to V_1 \oplus V_2$ s predpisom $(\rho^1 \oplus \rho^2)(u, v) = (\rho^1(u), \rho^2(v))$.

V tem razdelku pa se bomo ukvarjali predvsem s tem, kako v neki upodobitvi prepoznati direktno vsoto dveh preprostejših upodobitev.

Definicija 5. Naj bo $\rho : G \to \mathrm{GL}(V)$ upodobitev. Podprostor $W \leq V$ je *invarianten* za ρ, če za vsak $x \in G$ velja $\rho_x(W) \leq W$. Če V nima dimenzije 0 in sta edina invariantna podprostora upodobitve ρ trivialni podprostor 0 in cel prostor V, potem pravimo, da je ρ *nerazcepna upodobitev.*

Če je $W \leq V$ invarianten za ρ, potem je za vsak $x \in G$ zožitev ρ_x na W avtomorfizem prostora W, saj je W končnorazsežen. Poleg tega je kompozitum dveh zožitev enak zožitvi kompozituma, torej dobimo upodobitev grupe G na prostoru W, ki ji rečemo *podupodobitev upodobitve* ρ. Ponavadi kar podprostoru W pravimo podupodobitev, ampak imamo v takem primeru seveda v mislih prej opisano upodobitev na podprostoru W.

Trditev 1 (Maschkejev izrek). *Če je W invarianten podprostor za upodobitev $\rho : G \to \mathrm{GL}(V)$, potem obstaja komplement W' od W v V, ki je tudi invarianten za ρ.*

Dokaz. Naj bo $\langle \cdot, \cdot \rangle$ nek skalarni produkt na prostoru V. Definirajmo preslikavo $\langle \cdot, \cdot \rangle_2 : V \times V \to \mathbb{C}$ s predpisom $\langle u, v \rangle_2 = \sum_{x \in G} \langle \rho_x(u), \rho_x(v) \rangle$. Lahko je preveriti, da je tudi $\langle \cdot, \cdot \rangle_2$ skalarni produkt na V. Za poljubne $u, v \in V$ in $x \in G$ velja $\langle \rho_x(u), \rho_x(v) \rangle_2 = \sum_{y \in G} \langle \rho_{yx}(u), \rho_{yx}(v) \rangle = \langle u, v \rangle_2$, saj tudi yx preteče celo grupo G, ko jo preteče y. Tej lasnosti bomo rekli invariantnost skalarnega produkta $\langle \cdot, \cdot \rangle_2$ za ρ. Naj bo $W' = W^\perp$ ortogonalni komplement od W glede na $\langle \cdot, \cdot \rangle_2$. Izberimo poljubna $u \in W'$ in $x \in G$. Za vsak $v \in W$ velja $\langle \rho_x(u), v \rangle_2 = \langle u, \rho_{x^{-1}}(v) \rangle_2 = 0$, kjer smo v prvi enakosti upoštevali invariantnost skalarnega produkta v drugi pa invariantnost podprostora W. Torej je $\rho_x(u) \in W^\perp = W'$. S tem je trditev dokazana.

Pripomnimo, da smo v definiciji skalarnega produkta $\langle \cdot, \cdot \rangle_2$ potrebovali končnost grupe G. Lahko je poiskati primer kakšne upodobitve neskončne grupe za katero trditev ne velja.

Naj bo W invarianten podprostor upodobitve $\rho : G \to \mathrm{GL}(V)$. Zgornja trditev nam zagotavlja obstoj komplementa W' podprostora W v V, ki je tudi invarianten za ρ. Velja $V = W \oplus W'$ in ρ je določena s tem, kako slika elemente podprostorov W in W'. Pravimo, da je ρ *notranja direktna vsota* svojih podupodobitev na invariantnih podprostorih W in W'. V takem primeru je ρ ekvivalentna zunanji direktni vsoti obeh podupodobitev.

Posledica 2. *Vsaka upodobitev je direktna vsota nerazcepnih upodobitev.*

Dokaz. Dokaz poteka z indukcijo na stopnjo upodobitve. Vsaka upodobitev stopnje 1 je že kar sama nerazcepna. Naj bo $\rho : G \to \mathrm{GL}(V)$ neka upodobitev in denimo, da trditev velja za vse upodobitve nižje stopnje. Če je ρ nerazcepna, ni kaj dokazati, sicer pa obstaja pravi netrivialen invarianten podprostor $W \leq V$. Po trditvi 1 obstaja tak invarianten podprostor W', ki je komplement od W, da je ρ direktna vsota podupodobitev na W in W', ki sta obe nižje stopnje kot ρ. Podupodobitvi sta po indukcijski prepostavki direktni vsoti nerazcepnih upodobitev, zato enako velja za ρ.

Zgled 2. Oglejmo si permutacijsko upodobitev grupe S_n na vektorskem prostoru $\mathbb{C}^n$ z bazo $\{e_1, \ldots, e_n\}$. Spomnimo se, da avtomorfizem ρ_σ preslika bazni vektor e_k v $e_{\sigma(k)}$. Enorazsežen vektorski podprostor W, ki ga razpenja $e_1 + \cdots + e_n$, je očitno invarianten podprostor. Opazimo lahko, da je že standardni skalarni produkt invarianten za to upodobitev. Iz dokaza trditve 1 lahko sklepamo, da je ortogonalni komplement $W' = \{(x_1, \ldots, x_n) \in \mathbb{C}^n \mid x_1 + \cdots + x_n = 0\}$ prostora W invarianten. To je seveda lahko videti tudi direktno. Podupodobitev na W je trivialna upodobitev in je kot enorazsežna upodobitev seveda nerazcepna. Podupodobitev na W' je $(n-1)$-dimenzionalna upodobitev. Pokažimo, da je tudi ta nerazcepna. Naj bo $V \leq W'$ neničeln invarianten podprostor. V njem obstaja nek neničeln vektor $(x_1, \ldots, x_n)$. Vse komponente tega vektorja ne morejo biti enake, saj bi bile v takem primeru vse enake 0. Zaradi invariantnosti lahko predpostavimo, da je $x_1 \neq x_2$. Invarianten prostor V potem vsebuje vektorja $(x_1, x_2, \ldots, x_n)$ in $(x_2, x_1, \ldots, x_n)$, torej vsebuje tudi njuno razliko $(x_1 - x_2, x_2 - x_1, 0, \ldots, 0)$ in vektor $e_1 - e_2$. Potem pa mora vsebovati tudi $e_2 - e_3, \ldots, e_{n-1} - e_n$, zato velja $V = W'$.

Naslednji cilj je pokazati Schurovo lemo, ki nam bo večkrat prišla prav.

Trditev 3 (Schurova lema). *Naj bosta $\rho^1 : G \to \mathrm{GL}(V_1)$ in $\rho^2 : G \to \mathrm{GL}(V_2)$ nerazcepni upodobitvi G in $f : V_1 \to V_2$ taka linearna preslikava, da za vse $x \in G$ velja $\rho^2_x f = f \rho^1_x$.*

1. *Če ρ^1 in ρ^2 nista ekvivalentni, potem je $f = 0$.*

2. *Če je $V_1 = V_2$ in $\rho^1 = \rho^2$, je $f = \lambda\,\mathrm{id}$ za nek $\lambda \in \mathbb{C}$.*

Dokaz. 1. Pokažimo, da je $\ker f$ invarianten za ρ^1 in $\operatorname{im} f$ invarianten za ρ^2. Naj bo $x \in G$ poljuben. Če je $v \in \ker f$, je $f\rho^1_x(v) = \rho^2_x f(v) = 0$, torej je tudi $\rho^1_x(v) \in \ker f$. Podobno, če je $v = f(u) \in \operatorname{im} f$, je $\rho^2_x(v) = \rho^2_x f(u) = f\rho^1_x(u) \in \operatorname{im} f$. Denimo, da je $f \neq 0$. Zaradi nerazcepnosti ρ^1 mora potem biti $\ker f = 0$, zaradi nerazcepnosti ρ^2 pa mora biti $\operatorname{im} f = V_2$. Potem pa je f izomorfizem vektorskih prostorov V_1 in V_2, zato sta ρ^1 in ρ^2 ekvivalentni.

2. Linearna preslikava f ima neko kompleksno lastno vrednost λ. Ker za vsak $x \in G$ velja $\rho^2_x(f - \lambda\,\mathrm{id}) = (f - \lambda\,\mathrm{id})\rho^1_x$, je $\ker(f - \lambda\,\mathrm{id})$ netrivialen podprostor prostora V_1, ki je invarianten za ρ^1. Upodobitev ρ^1 pa je nerazcepna, zato je $\ker(f - \lambda\,\mathrm{id}) = V_1$ in posledično $f = \lambda\,\mathrm{id}$.

2.2 Karakterji upodobitev

Definicija 6. *Karakter upodobitve $\rho : G \to \mathrm{GL}(V)$* je preslikava $\chi_\rho : G \to \mathbb{C}$, definirana s predpisom $\chi_\rho(x) = \mathrm{tr}(\rho(x))$.

V neslednji trditvi bomo pokazali nekaj osnovnih lastnosti karakterjev.

Lema 4. *Naj bo χ karakter upodobitve $\rho : G \to \mathrm{GL}(V)$ stopnje d. Potem velja:*

1. *$\chi(1) = d$,*

2. *za vse $x \in G$ velja $\chi(x^{-1}) = \overline{\chi(x)}$,*

3. *za vse $x, y \in G$ velja $\chi(yxy^{-1}) = \chi(x)$.*

Dokaz.

1. $\chi(1) = \mathrm{tr}(\rho(1)) = \mathrm{tr}(\mathrm{id}_d) = d$.

2. Naj bo G reda n. Velja $\rho^n_x = \rho_{x^n} = \rho_1 = \mathrm{id}$, torej so lastne vrednosti $\lambda_1, \ldots, \lambda_d$ preslikave ρ_x enotska kompleksna števila. Sledi $\mathrm{tr}(\rho_{x^{-1}}) = \sum_{j=1}^d \lambda_j^{-1} = \sum_{j=1}^d \overline{\lambda_j} = \overline{\mathrm{tr}(\rho_x)}$.

3. Linearne preslikave lahko znotraj sledi ciklično permutiramo, zato velja
$$\chi(yxy^{-1}) = \mathrm{tr}(\rho_y \rho_x \rho_y^{-1}) = \mathrm{tr}(\rho_y^{-1} \rho_y \rho_x) = \chi(x).$$

Tretja točka nam pove, da je karakter χ konstanten na konjugiranostnih razredih. Funkciji, za katero to velja, rečemo *razredna funkcija.* Pokazali bomo, da karakterji nerazcepnih upodobitev grupe tvorijo bazo razrednih funkcij.

Naj bo $\mathbb{C}^G$ vektorski prostor vseh funkcij iz G v $\mathbb{C}$. Preslikava $(\cdot,\cdot) : \mathbb{C}^G \times \mathbb{C}^G \to \mathbb{C}$ s predpisom $(f,g) = \frac{1}{|G|}\sum_{x\in G} f(x^{-1})g(x)$ je simetrična bilinearna forma na $\mathbb{C}^G$.

Trditev 5. *Naj bosta $\rho^1 : G \to \mathrm{GL}(V_1)$ in $\rho^2 : G \to \mathrm{GL}(V_2)$ nerazcepni upodobitvi grupe G stopenj d_1 in d_2. Na prostorih V_1 in V_2 izberemo bazi. Naj bosta $[r^1_{ij}(x)]$ in $[r^2_{ij}(x)]$ matriki, ki pripadata ρ^1_x in ρ^2_x glede na izbrani bazi. Tu so r^1_{ij} in r^2_{ij} funkcije iz grupe G v $\mathbb{C}$ za vse ustrezne i,j. Velja:*

1. *Če sta ρ^1 in ρ^2 neekvivalentni, je $(r^1_{ik}, r^2_{lj}) = 0$ za vse i,j,k,l.*
2. *Če je $V_1 = V_2 = V$ in $\rho^1 = \rho^2 = \rho$, potem za vse i,j,k,l velja $(r_{ik}, r_{lj}) = \frac{1}{d}\delta_{ij}\delta_{kl}$, kjer je $d = d_1 = d_2$ in $[r_{ij}(x)]$ matrika od ρ_x.*

Dokaz. Naj bo $f : V_1 \to V_2$ poljubna linearna preslikava. Definirajmo novo linearno preslikavo $f' = \frac{1}{|G|}\sum_{x\in G}(\rho^2_x)^{-1} f \rho^1_x$. Za vsak $y \in G$ velja $(\rho^2_y)^{-1} f' \rho^1_y = \frac{1}{|G|}\sum_{x\in G}(\rho^2_{xy})^{-1} f \rho^1_{xy} = f'$ oziroma $\rho^2_y f' = f' \rho^1_y$, zato lahko uporabimo Schurovo lemo. Naj bosta $[a_{ij}]$ in $[a'_{ij}]$ matriki, ki pripadata f in f'. Iz definicije f' sledi

$$a'_{ij} = \frac{1}{|G|}\sum_{x\in G}\sum_{k=1}^{d_2}\sum_{l=1}^{d_1} r^2_{ik}(x^{-1})\, a_{kl}\, r^1_{lj}(x).$$

1. Če sta ρ^1 in ρ^2 neekvivalentni, po Schurovi lemi velja $f' = 0$, zato mora za vse i in j veljati

   $$0 = \sum_{k=1}^{d_2}\sum_{l=1}^{d_1}\left(\frac{1}{|G|}\sum_{x\in G} r^2_{ik}(x^{-1}) r^1_{lj}(x)\right) a_{kl}.$$

   Ker to velja za vsako linearno preslikavo f' oziroma za vse a_{kl}, dobimo

   $$(r^1_{ik}, r^2_{lj}) = \frac{1}{|G|}\sum_{x\in G} r^2_{ik}(x^{-1}) r^1_{lj}(x) = 0$$

   za vse i,j,k,l.

2. V drugem primeru iz Schurove leme sledi $f' = \lambda\,\mathrm{id}$. Če primerjamo sledi linearnih preslikav na obeh straneh, dobimo

   $$\lambda d = \frac{1}{|G|}\sum_{x\in G}\mathrm{tr}\left((\rho_x)^{-1} f \rho_x\right) = \frac{1}{|G|}\sum_{x\in G}\mathrm{tr}(f) = \mathrm{tr}(f).$$

   Sledi $f' = \frac{\mathrm{tr}(f)}{d}\,\mathrm{id}$. V matrični obliki lahko to zapišemo kot

   $$a'_{ij} = \frac{1}{d}\mathrm{tr}(f)\delta_{ij} = \frac{1}{d}\left(\sum_{k,l=1}^{d}\delta_{kl}a_{kl}\right)\delta_{ij} = \frac{1}{d}\sum_{k,l=1}^{d}\delta_{ij}\delta_{kl}a_{kl}$$

   za vsaka i,j. Dobimo enakost

   $$\sum_{k,l=1}^{d}\left(\frac{1}{|G|}\sum_{x\in G} r^2_{ik}(x^{-1}) r^1_{lj}(x)\right) a_{kl} = \sum_{k,l=1}^{d}\left(\frac{1}{d}\delta_{ij}\delta_{kl}\right) a_{kl},$$

   ki velja za vse i,j in za vse izbire a_{kl}. Torej mora veljati $(r^2_{ik}, r^1_{lj}) = \frac{1}{d}\delta_{ij}\delta_{kl}$.

Za $f, g \in \mathbb{C}^G$ definirajmo $\langle f, g\rangle = \frac{1}{|G|}\sum_{x\in G} f(x)\overline{g(x)}$. Preslikava $\langle\cdot,\cdot\rangle$ je očitno skalarni produkt na $\mathbb{C}^G$. Če je χ karakter neke upodobitve grupe G, iz druge točke leme 4 sledi

$$(f,\chi) = \frac{1}{|G|}\sum_{x\in G} f(x^{-1})\chi(x) = \frac{1}{|G|}\sum_{x\in G} f(x)\chi(x^{-1}) = \frac{1}{|G|}\sum_{x\in G} f(x)\overline{\chi(x)} = \langle f,\chi\rangle,$$

torej se $(\cdot,\cdot)$ in $\langle\cdot,\cdot\rangle$ v takem primeru ujemata. Sedaj lahko pokažemo, da so karakterji nerazcepnih upodobitev ortonormirani glede na $\langle\cdot,\cdot\rangle$.

Trditev 6. *Naj bosta χ in ψ karakterja dveh neekvivalentnih nerazcepnih upodobitev grupe G. Potem velja:*

1. $\langle\chi,\chi\rangle = 1$

2. $\langle\chi,\psi\rangle = 0$

Dokaz.

1. Naj bo d stopnja karakterja χ. Velja

$$\langle\chi,\chi\rangle = (\chi,\chi) = (\sum_{i=1}^{d} r_{ii}, \sum_{j=1}^{d} r_{jj}) = \sum_{i,j=1}^{d}(r_{ii}, r_{jj}) = \sum_{i,j=1}^{d}\frac{1}{d}\delta_{ij} = 1.$$

2. $\langle\chi,\psi\rangle = (\chi,\psi) = (\sum_i r^1_{ii}, \sum_j r^2_{jj}) = \sum_{i,j}(r^1_{ii}, r^2_{jj}) = 0.$

Trditev 7. *Naj bo ρ upodobitev v prostoru V, ki je direktna vsota podupodobitev τ in τ' na podprostorih W in W'. Označimo s χ karakter od ρ, s ψ in ψ' pa karakterja podupodobitev τ in τ'. Potem velja $\chi = \psi + \psi'$.*

Dokaz. Ker je $V = W \oplus W'$, lahko bazi podprostorov W in W' združimo in dobimo bazo prostora V. Matrika, ki pripada ρ_x v tej bazi, je bločno diagonalna, bloka na diagonali pa sta ravno matriki, ki pripadata τ_x in τ'_x v izbranih bazah. Iz tega sledi $\mathrm{tr}(\rho_x) = \mathrm{tr}(\tau_x) + \mathrm{tr}(\tau'_x)$.

Trditev 8. *Naj bo $V = W_1 \oplus \cdots \oplus W_n$ razcep upodobitve $\rho : G \to \mathrm{GL}(V)$ na nerazcepne podupodobitve. Naj bo ρ' neka nerazcepna upodobitev grupe G. Označimo s χ in χ' karakterja od ρ in ρ'. Število podupodobitev iz razcepa, ki so ekvivalentne ρ', je enako $\langle\chi,\chi'\rangle$.*

Dokaz. Naj bodo $\psi_1, \ldots, \psi_n$ karakterji ustreznih podupodobitev. Potem je $\chi = \psi_1 + \cdots + \psi_n$ in iz linearnosti skalarnega produkta v prvem faktorju sledi $\langle\chi,\chi'\rangle = \langle\psi_1,\chi'\rangle + \cdots + \langle\psi_n,\chi'\rangle$. Vsak od sumandov $\langle\psi_j,\chi'\rangle$ pa je enak 1, če je podupodobitev na prostoru W_j ekvivalentna ρ', in 0 sicer.

Številu podupodobitev iz razcepa ρ, ki so ekvivalentne ρ', rečemo *večkratnost* upodobitve ρ' v ρ.

Posledica zgornje trditve je, da so dobljene nerazcepne podupodobitve pri razcepu $V = W_1 \oplus \cdots \oplus W_n$ do ekvivalence in vrstnega reda natančno določene. Podprostori pa seveda niso nujno enolično določeni, saj lahko na primer upodobitev, ki vsak element grupe preslika v identiteto na $\mathbb{C}^2$, razcepimo kot direktno vsoto trivialnih podupodobitev na poljubnih dveh enodimenzionalnih podprostorih W_1 in W_2, za katera velja $W_1 \oplus W_2 = \mathbb{C}^2$.

Razcep upodobitve na nerazcepne podupodobitve je do ekvivalence določen s karakterjem upodobitve, zato sta dve upodobitvi z enakim karakterjem ekvivalentni.

Označimo s χ_G karakter regularne upodobitve grupe G. Stopnja regularne upodobitve je enaka $|G|$, zato velja $\chi_G(1) = |G|$. Za $x \neq 1$ pa je $\rho_x(e_y) = e_{xy}$, kar je bazni vektor različen od e_y. Matrika od ρ_x ima torej po diagonali same ničle, zato je $\chi_G(x) = 0$. Dokazali smo naslednjo trditev.

Trditev 9. *Za karakter regularne upodobitve grupe G velja $\chi_G(1) = |G|$ in $\chi_G(x) = 0$ za $x \neq 1$.*

Trditev 10. *V razcepu regularne upodobitve na nerazcepne podupodobitve se pojavi vsaka nerazcepna upodobitev z večkratnostjo, ki je enaka stopnji te upodobitve.*

Dokaz. Naj bo ρ nerazcepna upodobitev stopnje d s karakterjem χ. Večkratnost ρ v regularni upodobitvi je enaka $\langle \chi, \chi_G \rangle = \frac{1}{|G|} \sum_{x \in G} \chi(x)\overline{\chi_G(x)} = \frac{1}{|G|}\chi(1)|G| = d$.

Iz zgornje trditve lahko sklepamo, da je nerazcepnih upodobitev grupe G le končno mnogo.

Posledica 11. *Naj bodo $\rho_1, \ldots, \rho_n$ vse nerazcepne upodobitve grupe G. Za $i = 1, \ldots, n$ naj bo d_i stopnja, χ_i pa karakter upodobitve ρ_i. Potem velja:*

1. $\sum_{i=1}^{n} d_i^2 = |G|$,
2. $\sum_{i=1}^{n} d_i \chi_i(x) = 0$ *za* $x \neq 1$.

Dokaz. Ker je karakter direktne vsote upodobitev enak vsoti karakterjev, velja

$$\chi_G(x) = \sum_{i=1}^{n} d_i \chi_i(x).$$

Če vstavimo $x = 1$ in upoštevamo še enakost $\chi_i(1) = d_i$ dobimo ravno prvo točko. Za $x \neq 1$ dobimo drugo točko.

2.3 Nekomutativna Fourierova transformacija

V tem razdelku bomo spoznali nekaj lastnosti nekomutativne Fourierove transformacije.

Definicija 7. Naj bo $f : G \to \mathbb{C}$ funkcija. *Fourierova transformiranka funkcije* f je preslikava $\widehat{f}$, ki upodobitev $\rho : G \to \mathrm{GL}(V)$ grupe G preslika v endomorfizem $\widehat{f}(\rho) = \sum_{x \in G} f(x)\rho(x)$ vektorskega prostora V.

Iz definicije takoj sledi, da je Fourierova transformacija linearna, torej da za funkciji $f, g : G \to \mathbb{C}$ in skalarja $\alpha, \beta \in \mathbb{C}$ velja $\widehat{\alpha f + \beta g} = \alpha \widehat{f} + \beta \widehat{g}$.

Naslednja trditev pove, da je funkcija na G natanko določena z vrednostmi svoje Fourierove transformiranke v nerazcepnih upodobitvah.

Trditev 12 (Inverzna formula). *Naj bo f funkcija na G. Velja*

$$f(x) = \frac{1}{|G|} \sum d_\rho \operatorname{tr}(\rho_{x^{-1}} \widehat{f}(\rho)),$$

kjer vsota teče po vseh nerazcepnih upodobitvah ρ grupe G.

Dokaz. Obe strani sta linearni v f. Ker funkcije oblike $f(x) = \delta_{xy}$ razpenjajo prostor vseh funcij iz G v $\mathbb{C}$, je dovolj preveriti, da formula velja za takšne funkcije. Za tako funkcijo f je $\widehat{f}(\rho) = \rho_y$, zato je desna stran enaka

$$\frac{1}{|G|} \sum d_\rho \operatorname{tr}(\rho_{x^{-1}} \rho_y) = \frac{1}{|G|} \sum d_\rho \chi_\rho(x^{-1}y) = \frac{1}{|G|} \chi_G(x^{-1}y).$$

To pa je po trditvi 9 enako δ_{xy}.

Trditev 13 (Plancherelov izrek). *Naj bosta f, g funkciji na G. Velja*

$$\sum_{x \in G} f(x^{-1}) g(x) = \frac{1}{|G|} \sum d_\rho \operatorname{tr}(\widehat{f}(\rho)\widehat{g}(\rho)),$$

kjer vsota teče po vseh nerazcepnih upodobitvah ρ grupe G.

Dokaz. Spet je zaradi linearnosti dovolj preveriti trditev le za funkcije oblike $f(x) = \delta_{xy}$. V tem primeru leva stran postane $g(y^{-1})$, desna pa $\frac{1}{|G|} \sum d_\rho \operatorname{tr}(\rho_y \widehat{g}(\rho))$. Po inverzni formuli sta torej obe strani res enaki.

Spomnimo se, da je funcija na G razredna, če je konstantna na konjugiranostnih razredih grupe G. Naš zadnji cilj v tem razdelku je pokazati, da karakterji nerazcepnih upodobitev tvorijo bazo razrednih funkcij. Iz tega takoj sledi, da je nerazcepnih upodobitev toliko, kolikor je konjugiranostnih rezredov.

Trditev 14. *Naj bo f razredna funkcija na G. Potem za nerazcepno upodobitev ρ od G velja $\widehat{f}(\rho) = \lambda \operatorname{id}$, kjer je $\lambda = \frac{|G|}{d_\rho} \langle \overline{f}, \chi_\rho \rangle$.*

Dokaz. Za vsak $x \in G$ velja

$$\rho_x \widehat{f}(\rho) \rho_x^{-1} = \sum_{y \in G} f(y) \rho_{xyx^{-1}} = \sum_{y \in G} f(xyx^{-1}) \rho_{xyx^{-1}} = \widehat{f}(\rho).$$

Po Schurovi lemi je potem $\widehat{f}(\rho) = \lambda \operatorname{id}$ za nek $\lambda \in \mathbb{C}$. Če vzamemo sled endomorfizmov na obeh straneh, dobimo $d_\rho \lambda = \operatorname{tr}\left(\sum_{x \in G} f(x) \rho_x\right) = \sum_{x \in G} f(x) \chi_\rho(x) = |G| \langle \overline{f}, \chi_\rho \rangle$.

Trditev 15. *Karakterji nerazcepnih upodobitev tvorijo ortonormirano bazo razrednih funkcij na G.*

Dokaz. Po lemi 4 so karaterji nerazcepnih upodobitev razredne funkcije, po trditvi 6 pa so ortonormirani. Pokazati moramo še, da razpenjajo vektorski prostor vseh razrednih funkcij na G. Če ga ne razpenjajo, potem obstaja neničelna razredna funkcija f, da je $\overline{f}$ pravokotna na vse te karakterje. Po prejšnji trditvi potem za vsako nerazcepno upodobitev ρ velja $\widehat{f}(\rho) = \frac{|G|}{d_\rho} \langle \overline{f}, \chi_\rho \rangle \operatorname{id} = 0$. Z uporabo inverzne formule potem dobimo $f = 0$, kar je v nasprotju z neničelnostjo f. Torej nerazcepni karakterji res razpenjajo prostor razrednih funkcij na G.

Posledica 16. *Število nerazcepnih upodobitev G je enako številu konjugiranostnih razredov G.*

Dokaz. Bazo prostora razrednih funkcij na G tvorijo tudi funkcije, ki so ne enem razredu konstantno enake 1, na ostalih pa so enake 0. Takih funkcij je seveda toliko, kolikor je konjugiranostnih razredov grupe G. Ker imata vsaki bazi enako moč, smo s tem že dokazali posledico.

Recimo, da nam uspe poiskati toliko nerazcepnih upodobitev grupe G, kot ima G konjugiranostnih razredov. Če so vse te upodobitve paroma neekvivalentne, lahko iz zgornje posledice sklepamo, da smo že našli vse nerazcepne upodobitve G.

3. Upodobitve simetrične grupe

Vsako permutacijo lahko razcepimo na produkt disjunktnih ciklov. Ta razcep je enoličen do vrstnega reda ciklov natančno. Recimo, da sta $\sigma, \pi \in S_n$ permutaciji in naj bo

$$\sigma = (a_1^1, a_2^1, \ldots, a_{\lambda_1}^1) \cdots (a_1^k, a_2^k, \ldots, a_{\lambda_k}^k)$$

razcep σ na produkt disjunknih ciklov, kjer je $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k$. Potem je

$$\pi\sigma\pi^{-1} = (\pi(a_1^1), \ldots, \pi(a_{\lambda_1}^1)) \cdots (\pi(a_1^k), \ldots, \pi(a_{\lambda_1}^k))$$

razcep $\pi\sigma\pi^{-1}$ na disjunktne cikle. Sledi, da sta dve permutaciji konjugirani natanko tedaj, ko imata za vsak $l \in \mathbb{N}$ enako število ciklov dolžine l. V tem primeru pravimo, da imata enako ciklično strukturo. Dobili smo tudi bijekcijo med konjugiranostnimi razredi grupe S_n in razčlenitvami števila n. Konjugiranostnemu razredu premutacije σ na primer ustreza razčlenitev $(\lambda_1, \cdots, \lambda_k)$.

Vemo že, da so nerazcepne upodobitve poljubne grupe v bijekciji s konjugiranostnimi razredi. V primeru simetrične grupe S_n pa so ti razredi v bijekciji z razčlenitvami števila n. V tem razdelku si bomo ogledali, kako lahko vsaki razčlenitvi števila n priredimo nerazcepno upodobitev grupe S_n.

Definicija 8. *Youngov diagram razčlenitve* $\lambda = (\lambda_1, \ldots, \lambda_k)$ je množica $\{(i, j) \in \mathbb{N}^2 \mid i \leq k \text{ in } j \leq \lambda_i\}$. Bijektivno preslikavo t iz Youngovega diagrama v $\{1, 2, \ldots, n\}$ imenujemo *tablo oblike* λ ali λ-*tablo*.

Youngov diagram razčlenitve λ si bomo predstavljali kot skupino n kvadratov, ki so razporejeni v k vrstic tako, da je v i-ti vrstici λ_i kvadratov. Tablo pa si bomo predstavljali kot Youngov diagram, v katerem so v kvadratih napisana različna števila od 1 do n. Element tabloja t, ki se nahaja v i-ti vrstici in j-tem stolpcu, bomo namesto s $t(i, j)$ označili kar s $t_{i,j}$.

Zgled 3. Naj bo $\lambda = (4, 3, 1)$ razčlenitev števila 8. Youngov diagram te razčlenitve je

$$\begin{array}{|c|c|c|c|}\hline & & & \\ \hline & & \\ \cline{1-3} \\ \cline{1-1}\end{array},$$

primer λ-tabloja pa je

$$t = \begin{array}{|c|c|c|c|}\hline 7 & 4 & 2 & 6 \\ \hline 3 & 1 & 8 \\ \cline{1-3} 5 \\ \cline{1-1}\end{array}.$$

Velja tudi $t_{1,2} = 4$.

Na množici vseh λ tablojev bomo definirali relacijo. Za tabloja t in s naj velja $t \sim s$, če imata za vsak i tabloja t in s v i-ti vrstici enaka števila. Tako definirana relacija $\sim$ je ekvivalenčna relacija.

Definicija 9. Ekvivalenčni razred λ tabloja po relaciji $\sim$ imenujemo λ-*tabloid*. Tabloid, ki mu pripada tablo t, označimo s $\{t\}$.

Tabloide bomo risali na enak način kot tabloje, le da bomo izpustili navpične črte med stolpci. To nakazuje, da je vrstni red elementov znotraj vsake vrstice nepomemben, pomembno je le to, v kateri vrstici se nahaja kateri element. Zaradi istega razloga bomo pri tabloidih elemente v vsaki vrstici ponavadi napisali kar v vrstnem redu od najmanjšega do največjega.

Grupa S_n na naraven način deluje na množico vseh λ-tablojev. Permutacija $\pi \in S_n$ deluje na tablo t tako, da velja $(\pi \cdot t)_{i,j} = \pi(t_{i,j})$. To delovanje je usklajeno z relacijo $\sim$, saj velja $t \sim s$ natanko tedaj, ko je $\pi \cdot t \sim \pi \cdot s$. S tem torej dobimo delovanje grupe S_n na množico λ-tabloidov.

Zgled 4. Naj bo $\lambda = (2, 2)$ razčlenitev števila 4 in

$$t = \begin{array}{|c|c|}\hline 2 & 4 \\ \hline 3 & 1 \\ \hline\end{array}$$

λ-tablo. Potem velja

$$\{t\} = \begin{array}{c}\hline 2 \;\; 4 \\ \hline 1 \;\; 3 \\ \hline\end{array} = \left\{ \begin{array}{|c|c|}\hline 2 & 4 \\ \hline 1 & 3 \\ \hline\end{array}, \begin{array}{|c|c|}\hline 4 & 2 \\ \hline 1 & 3 \\ \hline\end{array}, \begin{array}{|c|c|}\hline 2 & 4 \\ \hline 3 & 1 \\ \hline\end{array}, \begin{array}{|c|c|}\hline 4 & 2 \\ \hline 3 & 1 \\ \hline\end{array} \right\}.$$

Permutacija $(1\,4\,3)$ pošlje tabloid $\{t\}$ v tabloid

$$(1\,4\,3)\cdot\{t\} = \begin{array}{cc}\hline 2 & 3\\ \hline 1 & 4\\ \hline\end{array}.$$

Definicija 10. Naj bo λ razčlenitev števila n. Kompleksni vektorski prostor, ki ima za bazo množico vseh λ-tabloidov, označimo z M^λ. Imamo tudi upodobitev $\rho : S_n \to \mathrm{GL}(M^\lambda)$, kjer je $\rho(\pi)$ definiran na bazi s predpisom $\rho(\pi)\{t\} = \{\pi t\}$.

Če je $\lambda = (\lambda_1, \ldots, \lambda_k)$ razčlenitev n, potem obstaja $n!$ različnih λ-tablojev. V vsakem ekvivalčnem razredu relacije $\sim$ je natanko $\lambda_1!\,\lambda_2!\cdots\lambda_k!$ tablojev, zato obstaja natanko $\frac{n!}{\lambda_1!\,\lambda_2!\cdots\lambda_k!}$ različnih tabloidov. To je torej dimenzija prostora M^λ.

Zgled 5. Naj bo $\lambda = (n)$. Potem obstaja samo en λ-tabloid, delovanje grupe S_n pa je trivialno. V tem primeru gre za trivialno upodobitev.

Naj bo zdaj $\lambda = (1^n)$ razčlenitev iz n enk. Če je več zaporednih členov razčlenitve enakih, bomo zapisali le enega in njihovo število označili v eksponentu. V tem primeru je $n!$ tabloidov, ki jih lahko identificiramo s permutacijami iz S_n. Če s permutacijo π delujemo na tabloid, ki ustreza permutaciji σ, dobimo tabloid, ki ustreza permutaciji $\pi\sigma$. Upodobitev S_n na prostoru $M^{(1^n)}$ je torej regularna upodobitev grupe S_n.

Če pa je $\lambda = (n-1, 1)$, imamo n tabloidov, ki jih lahko enačimo s števili od 1 do n, glede na to katero število se nahaja v drugi vrstici. Permutacija π pošlje tabloid, ki ima v drugi vrstici a, v tabloid, ki ima v drugi vrstici $\pi(a)$. Gre torej za permutacijsko upodobitev.

Kot smo videli, M^λ ni vedno nerazcepna upodobitev, poiskali pa bomo ustrezno nerazcepno podupodobitev, tako da bosta nerazcepni podupodobitvi za različni razčlenitvi neekvivalentni.

Definicija 11. *Stabilizator stolpcev* λ-tabloja t je množica C_t vseh tistih permutacij $\pi \in S_n$, za katere imata tabloja $\pi \cdot t$ in t za vsak i v i-tem stolpcu ista števila.

Definicija 12. Za podmnožico $A \subset S_n$ vpeljimo oznako $\kappa(A) = \sum_{\sigma\in A} \mathrm{sgn}(\sigma)\sigma$ za element grupne algebre $\mathbb{C}[S_n]$. Za λ-tablo t naj bo $\kappa_t = \kappa(C_t) = \sum_{\sigma\in C_t} \mathrm{sgn}(\sigma)\sigma$. Element $e_t = \kappa_t\{t\}$ vektorskega prostora M^λ imenujemo λ-*politabloid*.

Produkt dveh permutacij, ki ohranjata stolpce nekega tabloja, tudi ohranja stolpce tega tabloja. Prav tako tudi inverz vsake take permutacije ohranja stolpce. Sledi, da je C_t podgrupa grupe S_n.

Zgled 6. Oglejmo si primer za tablo

$$t = \begin{array}{|c|c|c|}\hline 4 & 1 & 3\\ \hline 2 & 5 & \multicolumn{1}{c}{}\\ \cline{1-2}\end{array}.$$

Stabilizator stolpcev je v tem primeru enak $C_t = \{\mathrm{id}, (2\,4), (1\,5), (2\,4)(1\,5)\}$.
Velja še $\kappa_t = \mathrm{id} - (2\,4) - (1\,5) + (2\,4)(1\,5)$ in

$$e_t = \begin{array}{ccc}\hline 4 & 1 & 3\\ \hline 2 & 5 & \\ \cline{1-2}\end{array} + \begin{array}{ccc}\hline 2 & 1 & 3\\ \hline 4 & 5 & \\ \cline{1-2}\end{array} - \begin{array}{ccc}\hline 4 & 5 & 3\\ \hline 2 & 1 & \\ \cline{1-2}\end{array} - \begin{array}{ccc}\hline 2 & 5 & 3\\ \hline 4 & 1 & \\ \cline{1-2}\end{array}.$$

Lema 17. *Za λ-tablo t in permutacijo $\pi \in S_n$ velja:*

1. $C_{\pi t} = \pi C_t \pi^{-1}$,
2. $\pi \cdot e_t = e_{\pi t}$.

Dokaz.

1. Za permutacijo σ velja $\sigma \in C_{\pi t}$ natanko tedaj, ko imata tabloja πt in $\sigma\pi t$ v istoležnih stolpcih ista števila, oziroma ko to velja za t in $\pi^{-1}\sigma\pi t$. To pa velja natanko tedaj, ko je $\pi^{-1}\sigma\pi \in C_t$ oziroma $\sigma \in \pi C_t \pi^{-1}$.

2. Upoštevamo, da sta znaka permutacij σ in $\pi\sigma\pi^{-1}$ enaka, in dobimo:

$$\begin{aligned}\pi e_t = \pi \sum_{\sigma \in \mathbb{C}_t} \operatorname{sgn}(\sigma)\sigma\{t\} &= \sum_{\sigma \in \mathbb{C}_t} \operatorname{sgn}(\pi\sigma\pi^{-1})\pi\sigma\pi^{-1}\{\pi t\} = \\ = \sum_{\sigma \in \pi\mathbb{C}_t\pi^{-1}} \operatorname{sgn}(\sigma)\sigma\{\pi t\} &= e_{\pi t}.\end{aligned}$$

Naj bo S_λ vektorski podprostor M^λ, ki ga razpenjajo vsi λ-politabloidi. Po drugi točki prejšnje leme je S_λ invarianten za delovanje S_n, zato imamo podupodobitev $\rho : S_n \to \mathrm{GL}(S_\lambda)$. Prostor S_λ je $\mathbb{C}[S_n]$ modul, imenuje se *Spechtov modul*. Pokazali bomo, da je ta upodobitev nerazcepna, še pred tem pa si oglejmo nekaj primerov Spechtovih modulov.

Zgled 7. Naj bo $\lambda = (n)$. Vemo, da obstaja samo en λ-tabloid. Za vsak tablo t velja $C_t = \{\mathrm{id}\}$, zato je politabloid e_t kar enak edinemu tabloidu za to razčlenitev. Prostor S_λ je torej enorazsežen. Ker vsaka permutacija deluje trivialno, gre za trivialno upodobitev.

Naj bo zdaj $\lambda = (1^n)$. Spomnimo se, da imamo $n!$ tabloidov, ki jih lahko enačimo s permutacijami iz S_n. Stabilizator stolpcev vsakega tabloja je kar cela grupa S_n. Tabloid, ki ustreza id, označimo s t. Potem velja $\pi \cdot e_t = e_{\pi t} = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma)\sigma\{\pi t\} = \operatorname{sgn}(\pi) \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma\pi)\sigma\pi\{t\} = \operatorname{sgn}(\pi) e_t$. Politabloidi različnih tablojev se torej razlikujejo kvečjemu za predznak, zato je prostor S_λ tudi v tem primeru enodimenzionalen. Sode permutacije na ta prostor delujejo kot id, lihe pa kot $-\mathrm{id}$, torej smo dobili alternirajočo upodobitev.

Oglejmo si še primer, ko je $\lambda = (n-1, 1)$. Imamo n tabloidov, ki jih enačimo s števili od 1 do n, glede na to katero število se nahaja v drugi vrstici. Označimo s T_i tabloid, ki ima v drugi vrstici število i. Stabilizator stolpcev tabloja, ki ima v prvem stolpcu zgoraj število a in spodaj b, je $\{\mathrm{id}, (a, b)\}$, njegov politabloid pa je enak $T_a - T_b$. Ti politabloidi razpenjajo prostor S_λ, torej je $S_\lambda = \{\sum_{i=1}^n \alpha_i T_i \mid \sum_{i=1}^n \alpha_i = 1\}$. Za permutacijo $\pi \in S_n$ in tabloid T_i pa je $\pi T_i = T_{\pi(i)}$. V tem lahko prepoznamo $(n-1)$-dimenzionalno upodobitev grupe S_n.

Najprej definirajmo relacijo $\lhd$ na množici vseh razčlenitev števila n, kjer za razčlenitvi λ in μ velja $\lambda \lhd \mu$, če za vsak j velja $\sum_{i=1}^j \lambda_i \leq \sum_{i=1}^j \mu_i$. Če je i večji, kot je dolžina razčlenitve λ, potem naj bo $\lambda_i = 0$, podobno pa naj velja seveda tudi za μ. Ta relacija je seveda refleksivna, antisimetrična in tranzitivna, torej je delna urejenost. Rekli ji bomo *majorizacija.* Prav nam bosta prišli naslednji lemi.

Lema 18. *Naj bosta λ in μ razčlenitvi n, t naj bo λ-tablo, s pa μ-tablo. Če sta vsaka elementa iz iste vrstice tabloja s v različnih stolpcih tabloja t, potem velja $\mu \lhd \lambda$.*

Dokaz. Naj bo j poljuben. Oglejmo si elemente iz prvih j vrstic tabloja s. V vsakem stolpcu tabloja t se nahaja največ j od teh števil, največ eno iz vsake od prvih j vrstic s. Torej je že v zgornjih j vrsticah tabloja t dovolj prostora za vsa ta števila, zato velja $\sum_{i=1}^j \lambda_i \geq \sum_{i=1}^j \mu_i$.

Lema 19. *Naj bosta λ in μ razčlenitvi n, t naj bo λ-tablo, s pa μ-tablo. Če je $\kappa_t\{s\} \neq 0$, potem velja $\lambda \rhd \mu$. Če je poleg tega še $\lambda = \mu$, potem je $\kappa_t\{s\} = \alpha e_t$ za nek $\alpha \in \{-1, 1\}$.*

Dokaz. Recimo, da sta a in b v isti vrstici s in v istem stolpcu t. Potem je $\tau := (a\,b) \in C_t$ in $\tau \cdot s = s$. Naj bodo $\sigma_1, \ldots, \sigma_k$ predstavniki odsekov grupe C_t po $\langle\tau\rangle$. Potem velja $\kappa_t\{s\} = \sum_{\sigma\in\mathbb{C}_t} \operatorname{sgn}(\sigma)\sigma\{s\} = \sum_{j=1}^{k}(\operatorname{sgn}(\sigma)\sigma\{s\} + \operatorname{sgn}(\sigma\tau)\sigma\tau\{s\}) = \sum_{j=1}^{k}(\operatorname{sgn}(\sigma)\sigma\{s\} - \operatorname{sgn}(\sigma)\sigma\{s\}) = 0$. Če sta a in b v isti vrstici, morata torej biti v različnih stolpcih t, zato po prejšnji lemi velja $\lambda \trianglerighteq \mu$.

Naj bo $\lambda = \mu$. Elementi iz prve vrstice s so v različnih stolpcih t, zato jih lahko z neko permutacijo iz C_t spravimo v prvo vrstico. Podobno potem naredimo še z elementi iz ostalih vrstic. Torej obstaja permutacija $\pi \in S_n$, da je $\pi \cdot \{t\} = \{s\}$, in velja $\kappa_t\{s\} = \kappa_t\{\pi t\} = \sum_{\sigma\in\mathbb{C}_t} \operatorname{sgn}(\sigma)\sigma\{\pi t\} = \operatorname{sgn}(\pi)\sum_{\sigma\in\mathbb{C}_t} \operatorname{sgn}(\sigma\pi)\sigma\pi\{t\} = \operatorname{sgn}(\pi)e_t$.

Posledica 20. *Za λ-tablo t in $u \in M^\lambda$ velja $\kappa_t(u) = \alpha e_t$ za nek $\alpha \in \mathbb{C}$.*

Dokaz. Po prejšnji lemi za vsak λ-tabloid $\{s\}$ velja $\kappa_t\{s\} = \alpha e_t$ za nek $\alpha \in \{-1, 0, 1\}$. Ker je u linearna kombinacija takih tabloidov, je $\kappa_t(u)$ res skalarni večkratnik e_t.

V naslednjem izreku bomo potrebovali skalarni produkt na prostoru M^λ, ki je invarianten za delovanje S_n. Tak je na primer skalarni produkt, v katerem tabloidi tvorijo ortonormirano bazo prostora M^λ. Sedaj smo pripravili vse potrebno za dokaz podmodulskega izreka.

Izrek 21 (Podmodulski izrek). *Naj bo U podprostor M^λ, ki je invarianten za delovanje S_n. Potem je $S_\lambda \leq U$ ali pa je $U \leq S_\lambda^\perp$.*

Dokaz. Za vsaka $u \in U$ in λ-tablo t velja $\kappa_t(u) = \alpha e_t$. Če obstajata taka u in t, da je $\alpha \neq 0$, potem je $e_t = \frac{1}{\alpha}\kappa_t(u) \in U$, saj je U invarianten podprostor. Ker lahko tudi vse ostale politabloide dobimo iz e_t z delovanjem, mora v tem primeru veljati $S_\lambda \leq U$. Če pa za vsaka u in t velja $\kappa_t(u) = 0$, potem je $\langle u, e_t\rangle = \langle u, \kappa_t\{t\}\rangle = \sum_{\sigma\in\mathbb{C}_t} \operatorname{sgn}(\sigma)\langle u, \sigma\{t\}\rangle = \sum_{\sigma\in\mathbb{C}_t} \operatorname{sgn}(\sigma^{-1})\langle\sigma^{-1}u, \{t\}\rangle = \langle\kappa_t(u), \{t\}\rangle = 0$, torej je $U \leq S_\lambda^\perp$.

Če je U torej invarianten podprostor S_λ, je lahko U trivialen ali pa je $U = S_\lambda$. Torej smo pokazali, da je S_λ nerazcepna upodobitev grupe S_n. Vemo, da je nerazcepnih upodobitev S_n toliko, kolikor je razčlenitev števila n, zdaj pa smo uspeli vsaki razčlenitvi prirediti eno tako upodobitev. Če pokažemo še, da so vse te upodobitve neekvivalentne, bomo lahko sklepali, da so to tudi vse nerazcepne upodobitve S_n.

Trditev 22. *Če sta upodobitvi $\rho^\lambda : S_n \to S_\lambda$ in $\rho^\mu : S_n \to S_\mu$ ekvivalentni, velja $\lambda = \mu$.*

Dokaz. Naj bo $f : S_\lambda \to S_\mu$ ekvivalenca upodobitev, torej tak izomorfizem vektorskih prostorov, da za vsak $\sigma \in S_n$ velja $\rho^\mu_\sigma f = f\rho^\lambda_\sigma$. Izomorfizem f lahko razširimo do linearne preslikave $F : M^\lambda \to S_\mu$ tako, da F preslika $S^{\lambda\perp}$ v 0. Za tako definirani F še vedno velja $\rho^\mu_\sigma F = F\rho^\lambda_\sigma$, kjer je zdaj ρ^λ upodobitev na M^λ. Kot pri dokazu Schurove leme lahko vidimo, da je $\ker F$ invarianten podprostor M^λ, zato je po podmodulskem izreku $S_\lambda \subseteq \ker F$ ali pa je $\ker F \subseteq S^{\lambda\perp}$. Ker je f kot izomorfizem netrivialen, mora veljati druga možnost. Torej za vsak λ-politabloid e_t velja $0 \neq Fe_t = F\kappa_t\{t\} = \kappa_t F\{t\}$, kjer smo upoštevali, da F komutira z delovanjem grupe S_n. Torej v linearni kombinaciji μ-tabloidov $F\{t\}$ obstaja vsaj en tak μ-tabloid, ki ga κ_t ne preslika v 0. Iz tega po lemi 19 sledi, da je $\lambda \trianglerighteq \mu$. S simetričnim razmilekom lahko pokažemo še, da velja tudi $\lambda \trianglelefteq \mu$, zato je $\lambda = \mu$.

3.1 Baza Spechtovega modula

V tem razdelku bomo poiskali baze prostorov S_λ.

Definicija 13. Tablo t je *standarden*, če njegovi elementi naraščajo po vrsticah v desno in po stolpcih navzdol. Politabloid e_t je *standarden*, če je t standarden tablo.

V tem razdelku bomo pokazali naslednji izrek.

Izrek 23. *Množica vseh standardnih politabloidov je baza prostora* S_λ.

Spomnimo se na pojem kompozicje števila. *Kompozicija števila* n *dolžine* k je urejena k-terica $\lambda = (\lambda_1, \ldots, \lambda_k)$, za katro velja $\sum_{i=1}^{k} \lambda_i = n$. Za razliko od razčlenitve pri kompoziciji ne velja nujno $\lambda_1 \geq \cdots \geq \lambda_k$.

Na enak način kot smo definirali relacijo majorizacije na razčlenitvah, jo lahko definiramo tudi na kompozicijah števila n. Pravimo, da kompozicija μ *majorizira* λ, če za vsak j velja $\sum_{i=1}^{j} \lambda_i \leq \sum_{i=1}^{j} \mu_i$. V tem primeru pišemo $\lambda \triangleleft \mu$.

Definicija 14. Za tabloid T in $i \leq n$ definirajmo T*-kompozicijo števila* i kot $T^i = (t_1^i, t_2^i, \ldots)$, kjer je t_j^i število elementov tabloida T manjših ali enakih i, ki se nahajajo v j-ti vrstici.

Ne glede na to, katerega predstavnika tabloida vzamemo, se bo izbrani element vedno nahajal v isti vrstici, zato je zgornja definicija dobra.

Definicija 15. Za λ-tabloida T in S pišimo $T \triangleleft S$, če za vsak i kompozicija S^i majorizira T^i.

Tako definirana relacija je očitno delna urejenost na množici tabloidov.

Zgled 8. Oglejmo si tabloide

$$T = \begin{array}{c}\hline 2\ 3\ 5 \\ \hline 1\ 4 \\ \hline\end{array}, \quad S = \begin{array}{c}\hline 1\ 4\ 5 \\ \hline 2\ 3 \\ \hline\end{array} \quad \text{in} \quad R = \begin{array}{c}\hline 2\ 4\ 5 \\ \hline 1\ 3 \\ \hline\end{array}.$$

Njihove kompozicije so

$$\begin{aligned}
&T^1 = (0,1),\ T^2 = (1,1),\ T^3 = (2,1),\ T^4 = (2,2),\ T^5 = (3,2),\\
&S^1 = (1,0),\ S^2 = (1,1),\ S^3 = (1,2),\ S^4 = (2,2),\ S^5 = (3,2)\ \text{ in}\\
&R^1 = (0,1),\ R^2 = (1,1),\ R^3 = (1,2),\ R^4 = (2,2),\ R^5 = (3,2).
\end{aligned}$$

Ker S^1 majorizira T^1 in T^3 majorizira S^3, tabloida T in S nista primerljiva. Velja pa $R \triangleleft T$ in $R \triangleleft S$.

Lema 24. *Če je* $a < b$ *in se* a *pojavi v nižji vrstici tabloida* T *kot* b*, potem je* $T \triangleleft (a\,b)T$.

Dokaz. Vpeljimo oznako $S = (a\,b)T$ in naj bosta p in q vrstici, v katerih se nahajata a in b. Če je $i < a$ ali $i \geq b$, velja $T^i = S^i$. Če pa je $a \leq i < b$, je $s_q^i = t_q^i + 1$, $s_p^i = t_p^i - 1$ in $t_j^i = s_j^i$ za $j \neq p, q$. Ker je po predpostavki $p > q$, tudi v tem primeru velja $T^i \triangleleft S^i$, torej je res $T \triangleleft S$.

Naj bo $u = \sum_{i=0}^{m} \alpha_i T_i$ element M^λ, kjer so T_i vsi različni λ-tabloidi. Rečemo, da se tabloid T_i *pojavi* v u, če je $\alpha_i \neq 0$.

Paru (a, b) elementov tabloja t rečemo inverzija tabloja t, če a in b ležita v istem stolpcu tabloja t, je a v nižji vrstici kot b in velja $a < b$.

Trditev 25. *Če je* t *standardni tablo, je* $\{t\}$ *največji tabloid glede na delno urejenost* $\triangleleft$*, ki se pojavi v politabloidu* e_t.

Dokaz. Vsak tabloid v e_t je oblike $\sigma\{t\}$ za nek $\sigma \in \mathbb{C}_t$. Z indukcijo na število inverzij tabloja σt bomo pokazali, da velja $\sigma\{t\} \triangleleft \{t\}$. Če tablo σt nima inverzij, potem velja $\sigma = \mathrm{id}$ in zato $\sigma\{t\} = \{t\}$. Recimo torej, da je (a, b) inverzija tabloja σt. Potem ima $(a\,b)\sigma t$ strogo manj inverzij, zato po indukcijski predpostavki velja $(a\,b)\sigma\{t\} \triangleleft \{t\}$. Po prejšnji lemi pa velja $\sigma\{t\} \triangleleft (a\,b)\sigma\{t\}$. Zaradi tranzitivnosti je potem $\sigma\{t\} \triangleleft \{t\}$, torej je $\{t\}$ res največji tabloid, ki se pojavi v e_t.

Trditev 26. *Standardni politabloidi so linearno neodvisni.*

Dokaz. Naj bodo $t_1, t_2, \ldots, t_m$ vsi različni standardni tabloji in recimo, da velja $\{t_1\} \triangleleft \{t_2\} \triangleleft \cdots \triangleleft \{t_m\}$. Naj za neke skalarje α_i velja $\sum_{i=1}^m \alpha_i e_{t_i} = 0$. Ker je $\{t_i\}$ največji tabloid, ki se pojavi v e_{t_i}, in je $\{t_i\} \triangleleft \{t_m\}$, se $\{t_m\}$ pojavi samo v politabloidu e_{t_m} in sicer s koeficientom 1. Če torej vsoto $\sum_{i=1}^m \alpha_i e_{t_i}$ razpišemo po bazi prostora M^λ sestavljeni iz vseh tabloidov, je koeficient pred tabloidom $\{t_m\}$ enak α_m. Zato mora veljati $\alpha_m = 0$. Z indukcijo na število neničelnih koeficientov dobimo, da mora za vsak i veljati $\alpha_i = 0$. Sledi, da so politabloidi e_{t_i} linearno neodvisni.

Sedaj bomo pokazali še, da standardni politabloidi razpenjajo prostor S_λ, torej da lahko vsak politabloid zapišemo kot linearno kombinacijo standardnih. Naj bo t poljuben tablo. Obstaja $\pi \in C_t$, da elementi v vsakem stolpcu tabloja πt naraščajo. Ker velja $e_{\pi t} = \pi e_t = \sum_{\sigma \in C_t} \mathrm{sgn}(\sigma)\pi\sigma t = \mathrm{sgn}(\pi) e_t$, je e_t linearna kombinacija standardnih politabloidov natanko tedaj, ko to velja za $e_{\pi t}$. Torej smemo predpostaviti, da elementi v stolpcih t naraščajo. Takemu tabloju bomo rekli *polstandardni tablo*, pripadajočemu politabloidu pa *polstandardni politabloid*.

Ideja dokaza je, da bomo vsak polstandardni politabloid zapisali kot linearno kombinacijo politabloidov, ki so bližje standardnim. Za te pa bomo po indukcijski predpostavki že vedeli, da ležijo v prostoru, ki ga razpenjajo standardni politabloidi. Potrebujemo torej neko merilo za to, kako blizu je nek politabloid standardnemu.

Definicija 16. Naj bosta $\lambda = (\lambda_1, \ldots, \lambda_k)$ in $\mu = (\mu_1, \ldots, \mu_k)$ dve kompoziciji nekega števila. Kompozicija λ je *manjša od μ v leksikografski urejenosti*, če obstaja $i \in \mathbb{N}$, da je $\lambda_i < \mu_i$ in za vse $j < i$ velja $\lambda_j = \mu_j$.

Ta relacija linearno uredi množico vseh kompozicij dolžine k nekega števila. Ker je ta množica končna, je ta relacija seveda tudi dobra urejenost.

Naj bo $\lambda = (\lambda_1, \ldots, \lambda_k)$ razčlenitev n. Vsakemu λ-tabloju bomo priredili kompozicijo $(s_1, \ldots, s_{\lambda_1})$ števila $\frac{n(n-1)}{2}$ dolžine λ_1, kjer je s_j vsota elementov v j-tem sptolcu tabloja t. Pravimo, da ta kompozicija *pripada* tabloju t in politabloidu e_t. Polstandardni tablo z najmanjšo kompozicijo glede na leksikografsko urejenost je tisti tablo, ki ima v prvem stolpcu začetnih nekaj naravnih števil, v drugem naslednjih nekaj naravnih števil in tako naprej do zadnjega stolpca. Tak tablo je seveda celo standarden. Lahko si mislimo, da je tablo bližje standardnemu, če mu pripada manjša kompozicija. To je zgolj intuicija, saj ima lahko na primer standardni tablo večjo kompozicijo kot kakšen tablo, ki ni standarden. Pokazali pa bomo, da lahko vsak politabloid, ki ni standarden, zapišemo kot linearno kombinacijo politabloidov, ki imajo manjšo kompozicijo. To lahko nato ponavljamo, dokler ne dobimo linearne kombinacije samih standardnih politabloidov. Pri dokazu si bomo pomagali z Garnirjevimi elementi.

Naj bosta $A, B \subset \{1, \ldots, n\}$ disjunktni. Oglejmo si nek odsek $\pi(S_A \times S_B)$ podgrupe $S_A \times S_B$ v grupi $S_{A \cup B}$. Za $\sigma \in S_{A \cup B}$ velja $\sigma \in \pi(S_A \times S_B)$ natanko tedaj, ko je $\sigma(A) = \pi(A)$ oziroma natanko tedaj, ko je $\sigma(B) = \pi(B)$. Torej lahko izberemo tako permutacijo $\sigma \in \pi(S_A \times S_B)$, da za vsaka $a, a' \in A$ iz $a < a'$ sledi $\sigma(a) < \sigma(a')$ in za vsaka $b, b' \in B$ iz $b < b'$ sledi $\sigma(b) < \sigma(b')$. To je namreč tista permutacija, ki najmanjši element iz A preslika v najmanjši element iz $\pi(A)$, drugi najmanjši element iz A preslika v drugi najmanjši element iz $\pi(A)$ in tako naprej, podobno pa tudi slika elemente iz B v $\pi(B)$. Taka permutacija σ je z odsekom enolično določena in jo bomo zato imenovali *odlikovani predstavnik odseka* $\pi(S_A \times S_B)$.

Definicija 17. Za množici A in B kot zgoraj naj bo $T_{A,B}$ množica odlikovanih predstavnikov vseh odsekov podgrupe $S_A \times S_B$ v grupi $S_{A \cup B}$. Element $g_{A,B} = \sum_{\pi \in T_{A,B}} \mathrm{sgn}(\pi)\pi$ grupne algebre $\mathbb{C}[S_n]$ se imenuje *Garnirjev element, ki pripada množicama A in B*.

Zgled 9. Naj bo $A = \{2,3\}$ in $B = \{1,4\}$. Potem je $S_{A\cup B} = S_4$ in

$$S_A \times S_B = \{\mathrm{id}, (2\,3), (1\,4), (2\,3)(1\,4)\}.$$

Odsek permutacije $\pi = (1\,4\,2\,3)$ je $\pi(S_A \times S_B) = \{(1\,4\,2\,3), (1\,4\,2), (1\,2\,3), (1\,2)\}$. Množici A in B se s π preslikata v $\pi(A) = \{1,3\}$ in $\pi(B) = \{2,4\}$. Odlikovani predstavnik tega odseka je torej

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = (1\,2).$$

Vsi odlikovani predstavniki so id, $(1\,2)$, $(3\,4)$, $(1\,2)(3\,4)$, $(1\,3\,2)$ in $(2\,3\,4)$, zato je Garnirjev element enak $g_{A,B} = \mathrm{id} - (1\,2) - (3\,4) + (1\,2)(3\,4) + (1\,3\,2) + (2\,3\,4)$.

Trditev 27. *Naj bo e_t politabloid, A podmnožica elementov v stolpcu j tabloja t in B podmnožica elementov v stolpcu $j+1$ tabloja t, da je $|A| + |B|$ večje kot število elementov v j-tem stolpcu t. Potem velja $g_{A,B}(e_t) = 0$.*

Dokaz. Najprej bomo pokazali, da velja $\kappa(S_{A\cup B})e_t = 0$. Vsak tabloid, ki se pojavi v e_t, lahko zapišemo v obliki $\{\sigma t\}$ za nek $\sigma \in C_t$. Fiksirajmo nek tak tabloid $\{\sigma t\}$. Obstajata elementa $a \in A$ in $b \in B$, ki sta v isti vrstici tabloida $\{\sigma t\}$, saj je $|A| + |B|$ večje kot število elementov v j-tem in kot število elementov v $(j+1)$-vem stolpcu σt. Ker velja $(a\ b) \in S_{A\cup B}$ in je $(a\ b)\{\sigma t\} = \{\sigma t\}$, bomo podobno kot v dokazu leme 19 pokazali, da je $\kappa(S_{A\cup B})\{\sigma t\} = 0$. Naj bodo $\sigma_1, \ldots, \sigma_m$ predstavniki vseh odsekov grupe $S_{A\cup B}$ po podgrupi $\langle (ab) \rangle$. Potem je $\kappa(S_{A\cup B})\{\sigma t\} = \sum_{i=1}^{m}(\sigma_i\{\sigma t\} - \sigma_i(ab)\{\sigma t\}) = 0$. Iz tega že sledi $\kappa(S_{A\cup B})e_t = 0$.

Velja $S_{A\cup B} = \bigcup_{\pi \in T_{A,B}} \pi(S_A \times S_B)$, zato je

$$\kappa(S_{A\cup B}) = \sum_{\pi \in T_{A,B}} \mathrm{sgn}(\pi)\pi\, \kappa(S_A \times S_B) = g_{A,B}\, \kappa(S_A \times S_B).$$

Ker pa je $S_A \times S_B \subset C_t$, za vsak $\sigma \in S_A \times S_B$ velja $\mathrm{sgn}(\sigma)\sigma e_t = e_t$, torej je $\kappa(S_A \times S_B)e_t = |S_A \times S_B|\, e_t$.

Dobili smo

$$0 = \kappa(S_{A\cup B})e_t = g_{A,B}\, \kappa(S_A \times S_B)\, e_t = g_{A,B}\, |S_A \times S_B|\, e_t,$$

iz česar sledi $g_{A,B}(e_t) = 0$.

Enakost $g_{A,B}(e_t) = 0$ pomeni, da velja $\sum_{\pi \in T_{A,B}} \mathrm{sgn}(\pi)e_{\pi t} = 0$. Ker je tudi id odlikovan predstavnik, velja $e_t = -\sum_{\mathrm{id} \neq \pi \in T_{A,B}} \mathrm{sgn}(\pi)e_{\pi t}$, torej smo uspeli e_t zapisati kot linerano kombinacijo drugih politabloidov. Sedaj moramo le še izbrati A in B tako, da bodo $e_{\pi t}$ bližje standardnim politabloidom.

Trditev 28. *Standardni politabloidi razpenjajo S_λ.*

Dokaz. Vemo že, da zadošča dokazati, da je vsak polstandarden politabloid linearna kombinacija standarnih. Naj bo torej e_t poljuben polstandardni politabloid. Dokaz poteka z indukcijo na kompozicijo tabloja t. Polstandardni politabloid z najmanjšo kompozicijo je že kar sam standarden. Baza indukcije je s tem dokazana. Denimo, da politabloid e_t ni standarden in da vsak politabloid e_s z manjšo kompozicijo kot e_t leži v linearni ogrinjači standradnih politabloidov. Ker t ni standarden tablo in elementi v solpcih t naraščajo, obstajata indeksa i in j, da je $t_{i,j} > t_{i,j+1}$. Naj bo A množica elementov v t, ki vsebuje $t_{i,j}$ in vse elemente v stolpcu j pod njim, in B množica elementov v t, ki vsebuje $t_{i,j+1}$ in vse elemente v stolpcu $j+1$ nad njim. Vse predpostavke za zgornjo trditev so izpolnjene, zato velja $g_{A,B}(e_t) = 0$ oziroma $e_t = -\sum_{\mathrm{id} \neq \pi \in T_{A,B}} \mathrm{sgn}(\pi)e_{\pi t}$. Naj bo $e_{\pi t}$ poljuben politabloid z desne strani enakosti. Politabloida e_t in $e_{\pi t}$ imata enake vsote elementov v prvih $j-1$

stolpcih. Ker pa je t polstandarden in velja $t_{i,j} > t_{i,j+1}$, je vsak element iz množice A večji od vsakega elementa iz množice B, zato je vsota elementov v j-tem stolpcu za t večja kot za πt. Torej ima $e_{\pi t}$ manjšo kompozicijo kot e_t, zato se $e_{\pi t}$ po indukcijski predpostavki da zapisati kot linearno kombinacijo standardnih politabloidov. Enako potem velja za e_t.

Trditvi 26 in 28 skupaj dokazujeta izrek 23. Več o upodobitvah simetričnih grup lahko bralec poišče v [3].

4. Zaključek

V prejšnjem poglavju smo poiskali vse nerazcepne upodobitve simetričnih grup oziroma Spechtovih modulov. Poiskali smo tudi njihove baze. Ena od uporab upodobitev simetričnih grup je analiza mešanja kart z naključnimi transpozicijami. Recimo, da imamo n kart urejenih po velikosti. Na vsakem koraku naključno izberemo dve karti in ju zamenjamo. Koliko korakov potrebujemo, da bodo karte dobro premešane? Diaconis in Shahshahani sta s pomočjo upodobitev simetrične grupe S_n pokazala, da je zadosti narediti približno $\frac{1}{2}n \log n$ korakov, da bodo karte dobro premešane. Več o tem lahko bralec najde v [1]. Torej so upodobitve grup uporabne tudi na drugih področjih matematike, ne le v teoriji grup.

LITERATURA

[1] P. Diaconis, *Group representations in probability and statistics*, Lecture Notes–Monograph Series **11**, Institute of Mathematical Statistics, Hayward, 1988.

[2] J. P. Serre, *Linear representations of finite groups*, Graduate texts in mathematics **43**, Springer, New York, 1977.

[3] B. Sagan, *The symmetric group - representations, combinatorial algorithms, and symmetric functions*, Graduate texts in mathematics **203**, Springer, Belmont, 1991.