Dodatna poglavja iz matematike za fizike

Skripta

Jože Zobec,

Miha Čančula

Povzeto po predavanjih

Izred. prof. dr. Sašo Strle

Uvod

Predmet je sestavljen iz dveh delov:

1. Teorija (diskretnih) grup in njih upodobitve,
   - grupe, podgrupe, homomorfizmi, kvocientne grupe (strukturni izreki)
   - reprezentacije končnih grup in kompaktnih grup
2. Gladke mnogoterosti in tenzorji
   - tangentni sveženj $\rightarrow$ kovariantni in kontravariantni tenzorji,
   - diferencialne forme $\in$ multilinearna algebra
   - integracija na mnogoterosti
   - krovni prostori, fundamentalna grupa

To skripto sem se odločil napisati, ker v je do sedaj nihče se ni poizkusil, in ker je dobro imeti tako gradivo na računalniku. Matematiki operirajo z mnogimi, nam fizikom nenavadnimi pojmi in težko jim je slediti. Dobro je, če lahko na računalniku enostavno uporabiš iskalnik besed ter se tako lažje navigiraš preko tako zajetnega gradiva. To je meni glavna motivacija.

Odločil sem se, da bom poleg tega dodal tudi neke vrste cheat-sheet za fizike, ki vsebuje pojme, ki so fizikom grozljivi, pa vendar niso (npr. *homomorfizem, endomorfizem, algebra...*). Tam je vse na enem mestu.

Jože Zobec,

Ribnica, 26. oktober 2013

Del I

Grupe

Poglavje 1

Osnovni pojmi

Definicija:

Grupa G je neprazna množica z binarno operacijo μ, ki jo imenujemo množenje: $\mu : G \times G \to G$, za katero velja $(a, b, c \in G)$:

1. operacija μ je asociativna: $\mu(\mu(a, b), c) = \mu(a, \mu(b, c))$.
2. množica G vsebuje element, ki je za operacijo μ identiteta – e: $\mu(e, a) = a$.
3. $\forall a \in G,\ \exists\, a^{-1} \in G$, ki je inverzni element za operacijo μ: $\mu(a, a^{-1}) = e$.

Z drugimi besedami, imamo množico, ki je zaprta za neko asociativno operacijo μ. Po navadi enačimo $\mu(a, b) \equiv ab$ in pišemo skrajšano.

Definicija:

Grupa G je *komutativna* ali *abelova*, če za $\forall a, b \in G$ velja $ab = ba$. V tem primeru operacijo μ imenujemo seštevanje in zapišemo $a + b = b + a$.

Opombe:

- Množica z asociativno operacijo je *polgrupa* (tj. nima nujno vseh inverzov ali identitete).
- Polgrupa z enoto (identiteto) je *monoid*.
- Identiteto, e, običajno označimo z 1.
- V primeru abelove grupe včasih operacijo označimo z znakom '+' in identiteto z '0'.

Primeri iz znanih množic števil:

- $(\mathbb{N}, +)$, $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ je asociativna, vendar nima identitete (število 0 ni naravno število) – torej je polgrupa.
- $(\mathbb{N} \cup \{0\}, +)$ je monoid, saj nimamo inverzov. Do grupe dopolnimo tako: $(\mathbb{Z}, +)$.
- $(\mathbb{N}, \cdot)$ je spet monoid. Do grupe manjkajo ulomki. Grupa je torej $(\mathbb{Q}, \cdot)$.

Opazimo, da imamo nad množico $\mathbb{Q}$ v resnici dve asociativni operaciji: množenje in seštevanje.

Definicija:

Obseg je (neprazna) množica O, ki ima med svojimi elementi dve asociativni operaciji: množenje, za katero je O grupa; in seštevanje, za katero je O abelova grupa, med operacijama pa velja distributivnostni zakon. Tj. $\forall a, b, c \in O,\ a(b+c) = ab + ac$.

Kadar imamo opravka z množico, ki je abelova grupa za operacijo seštevanja, za operacijo množenja pa le polgrupa, govorimo o *kolobarju*.

Ostali primeri grup:

- Za $\forall n \in \mathbb{N}$ je množica ostankov pri deljenju z n končna grupa z n elementi, operacija je '+', po modulu n. Ta grupa je $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$; $(a, b) \mapsto a + b \pmod n$:
  - identiteta: 0,
  - inverz: $a^{-1} = n - a$
- $S^1 = \mathbb{T}$ – krožnica. $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ je grupa za operacijo množenja kompleksnih števil, to je gladka krivulja. Enotsko krožnico lahko parametrično zapišemo tudi kot $\{e^{i\phi} \mid \phi \in \mathbb{R}\}$.
- $C_n = \{e^{2i\pi k/n} \mid k \in 0, 1, 2, \ldots, n-1\}$, oz. ciklična grupa z n elementi. Grupna operacija je množenje kompleksnih števil. Dobimo jo kot grupo n-tih korenov. C_n in $\mathbb{Z}_n$ sta algebrajično ekvivalentna.

Definicija:

Če sta G in H grupi, je preslikava $f : G \to H$ *homomorfizem*, če velja $f(g_1 \cdot g_2) = f(g_1)f(g_2)$. Bijektivni homomorfizem imenujemo *izomorfizem*. G in H sta *izomorfni*, če med njima obstaja kak tak izomorfizem.

Zgled:

Trdimo, da sta $\mathbb{Z}_n$ in C_n izomorfni. Poiskati moramo $f : \mathbb{Z}_n \to C_n$. Uganemo

$$f(k) \equiv e^{2i\pi k/n},$$

kar je očitno bijekcija. Pokazati moramo, da je še homomorfizem. V grupi $\mathbb{Z}_n$ je naša operacija grupnega množenja seštevanje po modulu n. Torej

$$f(k_1 \cdot k_2) = f\big(k_1 + k_2 \pmod n\big) = e^{2i\pi(k_1+k_2)/n} = e^{2i\pi k_1/n} e^{2i\pi k_2/n} = f(k_1)f(k_2).$$

■

1.1 Grupe linearnih transformacij

Definicija:

Množica V je *vektorski prostor* nad obsegom $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}, \mathbb{H}\}$, kadar imamo elementi operaciji seštevanja:

$$\begin{aligned} + : V \times V &\to V, \\ (v, w) &\mapsto v + w, \end{aligned}$$

za katero je abelova grupa; in množenje s skalarji,

$$\begin{aligned} \cdot : \mathbb{F} \times V &\to V, \\ (\lambda, v) &\mapsto \lambda v, \end{aligned}$$

za katero je asociativna in velja distributivnostni zakon. Pri množenju s skalarjem ponavadi ne pišmo pike.

Algebra je vektorski prostor nad kolobarjem.

Naj bo V vektorski prostor nad obsegom $\mathbb{F}$ in naj bo $L_{\mathbb{F}}(V)$ množica linearnih preslikav (veljata *asociativnost* in *homogenost*):

$$\begin{aligned} T &: V \to V, \\ T(\lambda v + \mu w) &= \lambda T(v) + \mu T(w). \end{aligned}$$

Linearne preslikave lahko množimo s skalarji:

$$\begin{aligned} (S + T)v &= Sv + Tv, \\ (\lambda S)v &= \lambda(Sv). \end{aligned}$$

Opazimo, da je $L_{\mathbb{F}}(V)$ vektorski prostor nad $\mathbb{F}$. Poleg tega, pa lahko preslikave v $L_{\mathbb{F}}(V)$ še komponiramo, čemur rečemo produkt:

$$(ST)(v) = S(T(v)).$$

Poraja se nam vprašanje: ali je $L_{\mathbb{F}}(V)$ za množenje (komponiranje) grupa? Ničelna linearna preslikava gotovo ni obrnljiva, $0 : V \to V,\ v \mapsto 0$. Kaj pa ostale? Preslikava $T : \mathbb{R}^2 \to \mathbb{R}^2,\ (x, y) \mapsto (x, 0)$ ni obrnljiva.

Obrnljive so natanko *bijektivne linearne preslikave*. Množico vseh teh označimo z

$$GL_{\mathbb{F}}(V) = \{T \in L_{\mathbb{F}}(V) \mid T \text{ ima inverz}\}.$$

$GL_{\mathbb{F}}(V)$ imenujemo *splošna linearna grupa* – grupa za komponiranje linearnih preslikav. Naj bo $\{v_1, v_2, \ldots, v_n\}$ baza v prostoru V, nad obsegom $\mathbb{F}$. Potem lahko linearne preslikave predstavimo z matrikami

$$M_n(\mathbb{F}) = \{\text{matrike dimenzije } n \times n, \text{ s koeficienti v } \mathbb{F}\}.$$

Potem $GL_{\mathbb{F}}(V)$ ustrezajo obrnljive matrike dimenzije $n \times n$ s koeficienti v $\mathbb{F}$, ki jih označimo z

$$GL_{\mathbb{F}}(V) = \{A \in M_n(\mathbb{F}) \mid \det A \neq 0\}.$$

V definiciji grupe nismo trdili dnoličnosti inverzov in enote, pa te kljub temu velja. Še več, za grupo potrebujemo le „polovico“ lastnosti.

Trditev:

Naj bo G množica z asociativno operacijo, za katero velja:
- $\exists e \in G$, tako da $a \cdot e = a,\ \forall a \in G$,
- $\forall a \in G$, $\exists b \in G$, tako da $a \cdot b = e$.

Potem velja:

(1) Če je $a \cdot a = a \ \Rightarrow a = e$.

(2) G je grupa (zgoraj velja še $ae = a$ in $ab = e$).

(3) e je en sam in b je za a enolično določen.

Dokaz: Dokazali bomo ciklično: (1) $\Rightarrow$ (3) $\Rightarrow$ (2) $\Rightarrow$ (1) $\Rightarrow$ (3).
(1) Recimo, da je $a \cdot a = a$. Velja $\forall a\ \exists b$, tako da $a \cdot b = e$.

$$\begin{aligned} aa &= a \ / \cdot b \\ (aa)b &= \underbrace{ab}_{e} \\ a(ab) &= e \\ \Rightarrow ae &= e \end{aligned}$$

To je očitno res lahko samo, kadar $a = e$.
(3) e je en sam: recimo, da obstaja še e' z istimi lastnostmi: $\Rightarrow ae' = a, \forall a \in G$. Ker velja $\forall a \in G$, si za a izberemo $a = e'$

$$\Rightarrow\ a = e' : e' \cdot e' = e' \Rightarrow e' = e, \text{ po točki (1).}$$

Za dani a je b en sam: pa recimo, da je $ab = e$ in $ab' = e$.
(2) Naj za a in b velja $ab = e$. Videti želimo

$$ba = e :\ (ba) \cdot (ba) = b \underbrace{(ab)}_{e} a = \underbrace{(be)}_{b} a = ba.$$

Po točki (1) sledi, da je $(ba) = e$. Preveriti moramo še, da je $ea = a,\ \forall a \in G$:

$$\underbrace{e}_{ab} a = (ab)a = a(ba) = ae = a.$$

(3) Vrnimo se še nazaj k točki (3) in pokažimo enoličnost b:

$$\begin{aligned} & ab = e, \quad ab' = e, \\ & \qquad ab' = e \ /b \cdot \text{ (množimo z leve)} \\ & \Rightarrow \underbrace{(ba)}_{e} b' = b \\ & \qquad eb' \Rightarrow b \end{aligned}$$

■

Definicija:

Naj bo G grupa. Podmnožica $H \subseteq G$ je *podgrupa*, če je H skupaj z operacijo v G grupa. To označimo s $H \leq G$.

Očitno za H velja:

1. $e \in H$, identiteta,
2. $a \in H$, potem je tudi $a^{-1} \in H$,
3. $\forall a, b \in H$ je $ab \in H$.

Trditev:

Neprazna podmnožica $H \subseteq G$ je podgrupa, če in samo če:
(i) $e \in H$

(ii) $\forall a \in H$ je $a^{-1} \in H$

(iii) $\forall a, b \in H$ je $ab \in H$

Dokaz: Res iz privzetkov in lastnosti množenja v G. ■

Trditev:

Neprazna podmnožica $H \subseteq G$ je podgrupa $\iff \forall a, b \in H$ velja $ab^{-1} \in H$.

Dokaz:

($\Rightarrow$) Očitno.

($\Leftarrow$) Tu si bomo pomagali s prejšnjim izrekom:

- za $b = a$ dobimo $a \cdot a^{-1} \in H$, kar zadosti pogoju (i).
- če vzamemo $a = e$ in $b = a \Rightarrow ab^{-1} = ea^{-1} = a^{-1} \in H$, kar zadosti pogoju (ii).
- $ab = a \cdot (b^{-1})^{-1} \in H$, kar zadosti pogoju (iii).

■

Posledica:

Naj bo G grupa; $\forall a \in G$ je množica

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$$

podgrupa v G, ki jo imenujemo *ciklična grupa*, generirana z a. Pri tem a^n pomeni:

$$\begin{aligned} a^0 &\equiv e, \\ a^1 &\equiv a, \\ a^2 &\equiv a \cdot a, \\ &\dots \\ a^n &\equiv a \cdot a^{n-1} = \underbrace{a \cdot a \cdot \ldots \cdot a}_{n\text{-krat}}, \ n \in \mathbb{N}. \end{aligned}$$

Element a^{-1} imenujemo inverz a. Velja $a^{-n} \equiv (a^{-1})^n$.

Dokaz: Preveriti moramo, da je za $a^n, a^m \in \langle a \rangle \in$, tudi $a^n \cdot a^{-m} \in \langle a \rangle$.

$$a^n \cdot a^{-m} = a^{n-m}$$

Recimo, da je $n, m > 0$. Za $n \geq m$ velja:

$$a^n a^{-m} = a^n (a^{-1})^m = a^{n-m+m} (a^{-1})^m = a^{n-m} \underbrace{a^m \cdot (a^{-1})^m}_{e} = a^{n-m}.$$

Za $n < m$ velja:

$$a^n a^{-m} = a^n (a^{-1})^m = \ldots = a^{n-m} = (a^{-1})^{m-n}.$$

■

Primeri podgrup:

1. $(S^1, \cdot) \leq (\mathbb{C}\backslash\{0\}, \cdot)$,
2. $(C_n, \cdot) \leq (S^1, \cdot)$,
3. $(\mathbb{Z}_n, +_{\bmod n}) \not\leq (\mathbb{Z}, +)$, ker operaciji nista isti,
4. $(n\mathbb{Z}, +) \leq (\mathbb{Z}, +)$, kjer $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$, torej množica celih večkratnikov števila n. Opazimo lahko, da je $n\mathbb{Z}$ ciklična grupa, generirana z n: kn pomeni

   $$\underbrace{n + n + n \ldots + n}_{k\text{-krat}},$$

   v multiplikativnem smislu, je to n^k. Aditivni inverz je $(-1)n$, kar multiplikativno pišemo n^{-1}.
5. $\underbrace{SL_n(\mathbb{F})}_{\leq GL_n(\mathbb{F})} = \{A \in GL_n(\mathbb{F}) \mid \det A = 1\}$. Enostavno se lahko prepričamo, da je res podgrupa:
   - $I \in SL_n(\mathbb{F})$, $\det I = 1$
   - $A \in SL_n(\mathbb{F})$, A^{-1} : $\det(A^{-1}) = 1/\det A = 1 \Rightarrow A^{-1} \in SL_n(\mathbb{F})$
   - $A, B \in SL_n(\mathbb{F})$, $\det(AB) = \det A \det B = 1 \Rightarrow AB \in SL_n(\mathbb{F})$
6. $O_n = \{A \in GL_n(\mathbb{R}) \mid A^T A = I\} \leq GL_n(\mathbb{R})$
7. $U_n = \{A \in GL_n(\mathbb{C}) \mid A^* A = I\} \leq GL_n(\mathbb{C})$, v fiziki bi A^* pisali kot $A^\dagger$.
8. $SO_n = SL_n(\mathbb{R}) \cap O_n$
9. $SU_n = SL_n(\mathbb{C}) \cap U_n$
10. $Sp_n = \{A \in GL_n(\mathbb{H}) \mid A^* A = I\} \leq GL_n(\mathbb{H})$, *simplektična* grupa – ohranja neko količino (v fiziki bi to bila energija). Množica $\mathbb{H}$ je prostor kvaternionov.

Trditev:

Naj bodo $H_i \leq G$, za $i \in I$ (I je indeksna množica in se bo še velikokrat pojavljala). Potem je tudi

$$\bigcap_{i \in I} H_i \leq G$$

Dokaz: Sledi iz trditve o ab^{-1}... Očitno res. ■

Posledica:

$\forall X \subseteq G$ obstaja najmanjša podgrupa v G, ki vsebuje X. Tej grupi rečemo podgrupa, generirana z X in jo označimo z $\langle X \rangle$.

1.2 Homomorfizmi in izomorfizmi

Definicija:

G, H grupi. Preslikava $f : G \to H$ je *homomorfizem*, če je $f(ab) = f(a)f(b)$ $\forall a, b \in G$. Bijektivni homomorfizem imenujemo *izomorfizem*:

Opomba: Če je $f : G \to H$ homomorfizem, potem je $f(e) = e$ in $f(a^{-1}) = \big(f(a)\big)^{-1}$ (torej enoto preslika v enoto in inverze preslika v inverze).

Definicija:

Endomorfizem je homomorfizem, ki slika sam nase.
Avtomorfizem je bijektivni endomorfizem, tj. izomorfizem, ki slika sam nase.

Primeri:

- H, G grupi, $H \leq G$. *Inkluzijska preslikava* $i : H \to G,\ h \mapsto h$ je homomorfizem.
- G grupa, $a \in G$.
  - *Leva translacija* za a je $L_a : G \to G,\ g \mapsto ag$.
  - *Desna translacija* za a je $R_a : G \to G,\ g \mapsto ga$.

  L_a in R_a sta homomorfizma le za $a = e$, tedaj je $L_a = R_a$, tj. identiteta. Za $a \neq e$ pa velja $L_a(e) \neq e$, $R_a(e) = a \neq e$. Ampak: L_a in R_a sta bijekciji, inverza sta $L_{a^{-1}}$ in $R_{a^{-1}}$.
- $f_a : G \to G,\ g \mapsto aga^{-1}$ je *konjugacija* ali *notranji avtomorfizem*.

  Dokaz:
  - $f_a(gh) = agha^{-1} = ag\underbrace{a^{-1}a}_{e}ha^{-1} = f_a(g) \cdot f_a(h)$ – res endomorfizem.
  - $f_a = L_a \circ R_{a^{-1}}$, obe sta bijektivni, tj. je tudi njun kompozitum, f_a bijektivna – res avtomorfizem. ■
- $\exp : (\mathbb{R}, +) \to \big((0, \infty), \cdot\big)$ je izomorizem (inverz je ln, oz. log).

  Dokaz:
  - Očitno bijektivna funkcija.
  - Dokazati moramo, da je homomorfizem:

    $$\exp(x + y) = \exp(x) \cdot \exp(y) \quad \blacksquare$$
- Za $d, n \in \mathbb{N}$ je $f_d : C_n \to C_{nd},\ z \mapsto z^d$ (spomnimo se, da je $C_n = \{z \in \mathbb{C} \mid z^n = 1\}$ grupa n-tih korenov) homomorfizem.

Dokaz: Res slika v C_{nd}:

$$z^n = 1;\ f(z) = z^d \ \Rightarrow\ z^{nd} = (z^n)^d = 1^d = 1.$$

To je očitno homomorizem, ki slika v C_{nd}, vendar f_d ni surjektivna. ■

- Matrična homomorfizma nad obsegom $\mathbb{F}$:
  - Determinanta za množenje matrik: $\det : (GL_n(\mathbb{F}, \cdot) \to (\mathbb{F}, +),\ A \mapsto \det A$ obseg.

    Dokaz: $\det(AB) = \det A \det B$. ■
  - Sled za seštevanje matrik: $\mathrm{tr} : \big(M_n(\mathbb{F}), +\big),\ A = \big[a_{ij}\big]_{i,j=1}^n \mapsto \mathrm{tr}(A) = \sum_{i=1}^n a_{ii}$

    Dokaz: $\mathrm{tr}(A+B) = \mathrm{tr}(A) + \mathrm{tr}(B)$. ■

Za lažjo pisavo bomo uvedli nekaj oznak.

Oznaka: G grupa, $A, B \subseteq G$ podmnožici.

- $AB \equiv \{ab \mid a \in A, b \in B\}$
- $Ab \equiv \{ab \mid a \in A\}$
- $aB \equiv \{ab \mid b \in B\}$

Definicija:

G, H grupi, $H \leq G$. H je *edinka* v G (*normalna podgrupa*), če $\forall a \in G$ velja

$$aHa^{-1} \subseteq H.$$

Oznaka je $H \lhd G$.

Lema:

$H \leq G$ je edinka $\iff aHa^{-1} = H\ \forall a \in G$.

Dokaz:

($\Leftarrow$) Očitno, saj je $aHa^{-1} = H \leq H$.

($\Rightarrow$) Vemo: $aHa^{-1} \subseteq H$, $\forall a \in G$. Za poljubno izbrani $a \in G$ velja $aHa^{-1} \subseteq H$. Za svoj „a“ izberem njegov inverz, tj. ‘a^{-1}’, kar nam da $a^{-1}Ha \subseteq H$. To pomeni, $\forall h \in H, a^{-1}ha \in H$, torej $a^{-1}ha = k \in H \Rightarrow h = aka^{-1} \in aHa^{-1} \Rightarrow \forall h \in H$ je $h \in aHa^{-1} \Rightarrow H \subseteq aHa^{-1}$. Vemo, da če $A \subseteq B$ in $B \subseteq A \Rightarrow A = B$, tj.

$$aHa^{-1} = H.$$

■

Trditev:

Naj bo $f : G \to H$ homomorfizem grup. Potem velja:
(1) Slika f: $\operatorname{im} f = \{f(g) \mid g \in G\} \leq H$.

(2) Jedro f: $\ker f = \{g \in G \mid f(g) = e\} \lhd G$.

Dokaz:

(1) Pokažimo, da je $\operatorname{im} f$ res podgrupa v H:

Za $f(g_1), f(g_2) \in \operatorname{im} f$ moramo preveriti, da je $f(g_1)\big(f(g_2)\big)^{-1} \in \operatorname{im} f$.

$$f(g_1)\big(f(g_2)\big)^{-1} = f(\underbrace{g_1 g_2^{-1}}_{\in G}) \in \operatorname{im} f \Rightarrow \text{ je res grupa.}$$

(2) Pokažimo, da je $\ker f$ res edinka v G:

- Res grupa:
  - $e \in \ker f$, ker je homomorfizem (identiteto slika v identiteto, tj. $e \in \ker f$).
  - $a \in \ker f \ \Rightarrow f(a) = e \Rightarrow f(a^{-1}) = e^{-1} = e \Rightarrow a^{-1} \in \ker f$,
  - $a, b \in \ker f \ \Rightarrow \ f(a) = e = f(b) \Rightarrow f(ab) = f(a)f(b) = ee = e \ \Rightarrow \ ab \in \ker f$.
- Res edinka:

$$g \in \ker f \text{ in } a \in G : \ f(aga^{-1}) = f(a)f(g)f(a^{-1}) = f(a)ef(a^{-1}))e \ \Rightarrow aga^{-1} \in \ker f.$$

■

Na osnovi tega dobimo kanonično dekompozicijo homomorfizma $f : G \to H$ tako, da ga predstavimo kot kompozitum surjektivnega homomorfizma, izomorfizma in injektivnega homomorfizma.
To znamo narediti pri linearni algebri:

Trditev:

Če sta V, W vektorska prostora nad obsegom $\mathbb{F}$ in je $T : V \to W$ linearna preslikava, označimo s $\ker T = \{v \in V \mid T(v) = 0\}$; in $\operatorname{im} T = \{T(v) \mid v \in V\}$, velja

$$V \ \to V/_{\ker T} \xrightarrow{\overline{T}} \ \operatorname{im} T \hookrightarrow W$$

To „klobaso“ interpretiramo kot

- $V \to V/_{\ker T}$ je kvocientna projekcija: $v_1 \sim v_2$, če je $(v_1 - v_2) \in \ker T$. Simbol '$\sim$' predstavlja ekvivalenčno relacijo.
- $V/_{\ker T} \xrightarrow{\overline{T}} \operatorname{im} T$ je preslikava inducirana s T, tj. slika enako, kot T.
- $\operatorname{im} T \hookrightarrow W$ je inkluzija (oz. inkluzijska preslikava, glej str. 13).

Podobno bi radi naredili za grupe (tj. dobili kanonično dekompozicijo homomorfizma grup).

Definicija:

Naj bo $H \leq G$. *Levi odsek* H v G je aH, $a \in H$, *desni odsek* pa Ha, $a \in G$. Element a je *predstavnik* odseka.

Opomba: Odsek ima več predstavnikov. Kdaj je $aH = bH$ (kdaj je levi odsek za dva predstavnika enak)?

- Če na desni v H izberemo e, sledi $b \cdot e \in bH = aH$ ($\Rightarrow b \in aH$).

  $$\Rightarrow b = ah \text{ za nek } h \in H \Rightarrow a^{-1}b = h \in H.$$

  Če a in b predstavljata isti odsek, potem je $ab^{-1} \in H$ (in ekvivalentno $b^{-1}a \in H$ $\Rightarrow$ v eno smer velja).

- Če je $a^{-1}b = h \in H$, potem $b = ah$, zato je $bH = ahH$. Ker je H grupa, je $hH \in H \Rightarrow \overbrace{ah}^{b} H \subseteq aH$. Lahko tudi zamenjamo vlogi a in $b \Rightarrow$ $aH = bH$.

- $a \sim b \overset{\text{def}}{\iff} a^{-1}b \in H$ je ekvivalenčna relacija. $a \sim b$ v tem primeru pomeni $aH = bH$.

Trditev:

Naj bo $H \leq G$. Potem sta odseka aH in bH bodisi disjunktna (presek je prazna množica), bodisi enaka. Slednje velja $\iff a^{-1}b \in H$.

Dokaz: Če aH in bH nista disjunktna obstaja $c \in aH \cap bH \Rightarrow c = ah = bk$; $h, k \in H$. Ker $H \ni hk^{-1} = a^{-1}b \Rightarrow a^{-1}b \in H \Rightarrow$ sta enaka.

$$\Rightarrow a^{-1}b \in H \Rightarrow aH = bH \text{ (dokazali v opombi)}^{1}.$$

■

Posledica:

Po zadnji trditvi grupa G razpade na disjunktne odseke po podgrupi H:

$$G = a_1H \cup a_2H \cup \ldots \cup a_nH = \bigcup_{i \in I} a_iH,$$

izberemo tako, da iz vsakega ekvivalenčnega razreda vzamemo enega predstavnika. Podobno lahko naredimo z desnimi odseki:

$$G = Hb_1 \cup Hb_2 \cup \ldots \cup Hb_n = \bigcup_{i \in I} Hb_i$$

Ali je število (medsebojno disjunktnih) levih odsekov enako številu (medsebojno disjunktnih) desnih odsekov? Ustrezajoči levi in desni odseki *niso nujno enaki*!

Definicija:

- če je G končna grupa, in $H \leq G$, označimo št. odsekov H v G kot $[G : H]$. Isto oznako uporabimo tudi, če je G neskončna, $[G : H]$ pa je še vedno končno. To število imenujemo *indeks* grupe H v G.
- Število elementov grupe G označimo z $|G| \in \mathbb{N} \cup \{\infty\}$. To imenujemo *moč* ali *red* grupe.
- Naj bo $a \in G$. Najmanše število $n \in \mathbb{N}$, za katerega je $a^n = e$, imenujemo *red elementa* a. Če tak n ne obstaja, je red ∞ (neskončno).

Trditev:

Lagrangejev izrek: G končna grupa, $H \leq G$. Potem

$$[G : H] = \frac{|G|}{|H|}.$$

Posebej sledi, da moč podgrupe deli moč grupe.

Dokaz: Odseki H v G določajo (razcep) za G: $G = a_1H \cup a_2H \cup \ldots \cup a_nH$, vsi navedeni odseki so disjunktni.

- Da unija odsekov zastopa ves G, saj je poljuben $a \in G$ v odseku aH (ker $e \in H$).
- V a_iH je ravno $|H|$ elementov ($\forall i \in I$), saj je L_{a_i} bijekcija.

$$|G| = |a_1H| + \ldots + |a_nH| = n \cdot |H| = [G : H] \cdot |H|.$$

■

Trditev:

G, H grupi, $H \leq G$. Levi odseki H v G so v bijektivni korsespondenci z desnimi odseki.

Dokaz:

- Iščemo preslikavo, za katero bi radi pozneje pokazali, da je bijekcija:

$$F : \{\text{levi odseki}\} \to \{\text{desni odseki}\},$$
$$aH \to Ha^{-1}.$$

  Zakaj je dobro $F(aH) = Ha^{-1}$ vidimo, če preverimo, kdaj sta desna odseka enaka: $Hb = Hc \iff b = hc \iff bc^{-1} \in H$, za leve je pa $a^{-1}b \in H \Rightarrow$ na eni strani moramo dobiti inverz, da bosta pogoja enaka.

- Preverimo, da je F dobro definirana (tj. da je relacija F res preslikava): če sta aH in bH enaka leva odseka, jih mora F preslikati v enaka desna,

$$aH = bH \iff a^{-1}b \in H,$$
$$Ha^{-1} = Hb^{-1} \iff a^{-1}(b^{-1})^{-1} = a^{-1}b \in H,$$

  to pa pomeni

- Dva enaka slika v dva enaka $\Rightarrow$ je funkcija.
- Dva različna slika v 2 različna – $a^{-1}b \notin H \Rightarrow a^{-1}(b^{-1})^{-1} = (b^{-1}a)^{-1} \notin H \Rightarrow$ injekcija.
- Vsi so slike: vsak ima a^{-1} inverz.

- Očitno je bijekcija.

■

Posledica:

Če je G končna grupa in $a \in G$, potem

$$\mathrm{red}(a) \mid |G|$$

(red a deli moč grupe G). Še več, $\mathrm{red}(a)$ je moč ciklične podgrupe, generirane z a:

$$\mathrm{red}(a) = |\langle a \rangle|$$

Dokaz: Naj bo $H = \langle a \rangle \leq G$, po Langrangejevem izreku sledi $|H|$ deli $|G|$. Dokazati moramo le še $\mathrm{red}(a) = |\langle a \rangle|$. Elementi H so

$$\langle a \rangle = \{e, a^{\pm 1}, a^{\pm 2}, a^{\pm 3} \ldots\}.$$

Ker je G končna, se bodo začeli ponavljati. Naj bo $k \in \mathbb{N}$ najmanjše število, da za nek $m \in \mathbb{Z}$ velja $a^{m+k} = a^m$. Od tod z množenjem z a^{-m} dobimo $a^k = e$. Ker je k najmanjši možni, je to ravno $\mathrm{red}(a)$. Potem $\forall m \in \mathbb{Z}$ velja

$$m = qk + r, \quad q \in \mathbb{Z}, \quad 0 \leq r < k,$$
$$a^m = a^{qk} \cdot a^r = (a^k)^q a^r = e^q a^r = a^r.$$

$\Rightarrow$ v ciklični grupi so natanko elementi $e, a, \ldots, a^{k-1}$.

$\Rightarrow$ $|\langle a \rangle| = k = \mathrm{red}(a)$.

■

Zgled:

Če je $[G : H] = 2$, je $H \lhd G$.

Rešitev:

- G razpade na dva odseka (vemo).
- Radi bi pokazali: $\forall a \in G$ je $aHa^{-1} \subseteq H$.
  - če je $a \in H \Rightarrow aHa^{-1} \subseteq H$, ker je H grupa.
  - izberimo poljuben $a \notin H$ ($\Rightarrow a^{-1} \notin H$) – spet želimo $aHa^{-1} \subseteq H$. Opazimo: $aH \neq H = eH \Rightarrow$ sta disjunktna $\Rightarrow G = eH \cup aH$.
  - Podobno velja, da sta H in Ha dva različna desna odseka $\Rightarrow aH = Ha \neq H$. Ta izraz lahko z desne množimo z a^{-1} dobimo

$$aHa^{-1} = H.$$

■

Zgled:

G, H grupi, $H \leq G$. Velja $H \lhd G \iff \forall$ levi odsek, je tudi desni odsek.

Rešitev:
($\Rightarrow$): $aHa^{-1} = Ha \;\Rightarrow\; aH = Ha,\ \forall a \in G$. $\square$

($\Leftarrow$): $\forall a\ \exists b$, tako da: $aH = Hb$. želimo $b = a$. Ali smemo?
Za $e \in H$ na desni dobimo $eb = b \in aH; b = ah, h \in H$. $a^{-1}b \in H$.

$$\begin{aligned} aH &= Hb, \\ aHb^{-1} &= H, \\ aH(ah)^{-1} &= a\underbrace{Hh^{-1}}_{H}a^{-1} = aHa^{-1}. \square \end{aligned}$$

■

Trditev:

G grupa, $H \lhd G$. Potem je množica levih odsekov H v G grupa za operacijo

$$aH \cdot bH \overset{\text{def}}{=} abH,$$

kar nakazuje, da je to natanko tedaj, ko so levi odseki enaki desnim.

- Oznaka za to grupo je $G/H = \{aH \mid a \in G\}$. Imenujemo jo *faktorska*, ali *kvocientna* grupa grupe G po edinki H (z operacijo ...).
- Enota za G/H je $eH = eH$, inverz pa $(aH)^{-1} = a^{-1}H$.

Dokaz

- Asociativnost sledi iz asociativnosti množenja v G.
- Notranja: $aH \cdot bH \in G/H$.

$$aH \cdot bH = abb^{-1}HbH = abHH = abH \in G/H.$$

■

Zgornji izrek nam da tole zaporedje grup in homomorfizmov:

$$\begin{aligned} p : a &\longrightarrow aH, \\ \{e\} \to H \overset{i}{\hookrightarrow} G \overset{p}{\longrightarrow}\ & G/H \to \{e\}. \end{aligned} \tag{1.1}$$

Tu se moramo spomniti

- inkluzija i je injektivna,
- inducirana preslikava $G \xrightarrow{p} G/H$ je surjektivna,
- $\ker p = H$, $\mathrm{im}(i) = H$.

Vse preslikave tu so homomorfizmi. To zaporedje je *eksaktno*: pri vski grupi je jedro izhodnega homomorfizma enako sliki vhodnega.

- pri H: slika je $\{e\}$; jedro je $\{e\}$, ker je inkluzija injektivna.
- pri G: slika je H; jedro je $\{a \in G \mid p(a) = aH = eH = H\}$. Pogoj $aH = H \iff a \in H$.
- pri G/H: slika od p je G/H; jedro je G/H, ker se vse slika v e.

Trditev:

$H \lhd G$, $f : G \to K$ homomorfizem, za katerega velja $H \subseteq \ker f$ ($f : \{H\} \to \{e\}$).
Potem f določa homomorfizem $\overline{f} : G/H \to K$ s predpisom

$$\begin{array}{ccc} G & \xrightarrow{f} & K \\ & \searrow^{p} \; G/H \; \nearrow_{\overline{f}} & \end{array}$$

se pravi

$$G \xrightarrow{f} K$$

in hkrati

$$G \underset{p}{\to} G/H \underset{\overline{f}}{\to} K$$

za katerega velja $f = \overline{f} \circ p$.

Dokaz:

- Preveriti moramo, da je $\overline{f}$, da je $\overline{f}$ dobro definiran in homomorfizem. Težava je v tem, da odsek nima samo enega predstavnika. ($aH = bH$, $a \neq b$), $\overline{f}$ pa je določena predstavnikom. $aH = bH \Rightarrow$ želimo vedeti $f(a) = \overline{f}(ab)) = \overline{f}(bH) = f(b)$.

$$\begin{aligned} \Rightarrow a^{-1}b \in & H \subseteq \ker f \\ f(a^{-1}b) = f(a)^{-1} & f(b) = e. \quad \square \end{aligned}$$

- Da je $\overline{f}$ homomorfizem takoj sledi: $\overline{f}(aH \cdot bH) = \overline{f}(abH) = f(ab) = f(a) \cdot f(b) = \overline{f}(aH) \cdot \overline{f}(bH)$.

■

Od tod takoj sledi kanonična dekompozicija homomorfizma.

Trditev:

Prvi izrek o izomorfizmu: Naj bo $f : G \to H$ homomorfizem (kot že vemo, je jedro edinka). Potem je

$$\overline{f} : G/\ker f \to \operatorname{im} f$$

izomorfizem in zaporedje

$$\{e\} \to \ker f \hookrightarrow G \xrightarrow{P} G/\ker f \xrightarrow{f} \operatorname{im} f \hookrightarrow H$$

je *kanonična dekompozicija homomorfizma grup* f, kar lahko zapišemo tudi

$$f = i \circ \overline{f} \circ P$$

Dokaz: Jedro homomorfizma, $\ker f$, je edinka v G, zato sledi, da obstaja inducirani homomorfizem $\overline{f} : G/\ker f \to H$. Trdimo: $\overline{f}$ je injektiven in zato bijektiven na $\operatorname{im} f$. Če je $a \cdot \ker f$ v jedru $\overline{f}$, torej $\overline{f}(a \cdot \ker f) = e$, je $f(a) = e$ in $a \in \ker f \Rightarrow a \cdot \ker f = \ker f$, ki je identiteta v $G/\ker f$. Edini odsek, ki se s $\overline{f}$ preslika v e je identiteta .

■

Zgled:

$(\mathbb{Z}, +)$; $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ je podgrupa v $\mathbb{Z}$. Potem je $n\mathbb{Z} \lhd \mathbb{Z}$ (edinka).

Bolj na splošno: Če je G abelova in $H \leq G$, je H edinka, tj. $aHa^{-1} = \{aha^{-1} \mid h \in H\} = \{aa^{-1}h \mid h \in H\} = H$.

Kaj je kvocientna grupa po edinki $n\mathbb{Z}$? Grupa $\mathbb{Z}/n\mathbb{Z}$ je množica odsekov $n\mathbb{Z}$ v $\mathbb{Z}$. Hitro vidimo, da je $\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, n - 1 + n\mathbb{Z}\}$ je izomorfna grupi ostankov pri deljenju z n, tj.

$$\begin{aligned} f : \mathbb{Z} &\to \mathbb{Z}_n \\ k &\mapsto k \pmod{n} \end{aligned}$$

Dokaži: f je surjetkivni homomorfizem in $\ker f = n\mathbb{Z}$, zato je $\overline{f} : \mathbb{Z}/n\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}_n$.

Ponovitev: G, H grupi, $H \leq G \iff \forall a, b \in H : ab^{-1} \in H$.

(1) H je *edinka*, če jo ohranjajo konjugacije, $aHa^{-1} \subseteq H \ \forall a \in G$ ($\iff aHa^{-1} = H$).

(2) *Kvocientna grupa*: $G/H = \{aH \mid a \in G\}$ je grupa, če je H edinka (tedaj so levi odseki enaki desnim in velja $aH \cdot bH = aHHb = aHb = abH$).

(3) $f : G \to H$ homomorfizem grup $\Rightarrow \ker f \lhd G$.

(4) $\operatorname{im} f$ inducira izomorfizem $\overline{f} : G/\ker f \xrightarrow{\cong} \operatorname{im} f$

(5) To da dekompozicijo kot $f : G \xrightarrow{p} G/\ker f \xrightarrow{\overline{f}} \operatorname{im} f \hookrightarrow H$

Točki (4) in (5) sta *prvi izrek o izomorfizmu*. Grupa $G/\ker f$ ima za elemente množico $\{a \cdot \ker f \mid a \in G\}$.

Zgled:

Pokaži, da je $SL_n(\mathbb{F})$ edinka v $GL_n(\mathbb{F})$ in „izračunaj“ pripadujočo kvocientno grupo (tj. poišči znano grupo, ki ji je kvocientna grupa izomorfna).

Ideja: Poiščemo homomorfizem $f : GL_n(\mathbb{F}) \to H$ v primeru grupe H tako, da je $\ker f = SL_n(\mathbb{F})$. Potem bo prvi izrek o izomorfizmu

$$\overline{f} : GL_n(\mathbb{F})/SL_n(\mathbb{F}) \xrightarrow{\cong} \operatorname{im} f \subseteq H$$

Rešitev: Ta homomorfizem je očitno determinanta (vse matrike iz $SL_n(\mathbb{F})$ so v jedru), za $\mathbb{F}$ pa vzamemo $\mathbb{F}^* \equiv \mathbb{F}\backslash\{0\}$.

$$\begin{aligned} \det : GL_n(\mathbb{F}) &\to \mathbb{F}^* \\ A &\mapsto \det A \end{aligned}$$

Velja tudi, da je $SL_n(\mathbb{F})$ edinka:

Dokaz: Naj bosta $A, A^{-1} \in GL_n(\mathbb{F})$ in $S \in SL_n(\mathbb{F})$, $SL_n(\mathbb{F}) = \{S \mid \det S = 1\}$.

$$\begin{aligned} \det(A^{-1}) &= (\det A)^{-1}, \text{ lastnost homomorfizma,} \\ \det(ASA^{-1}) &= \det(A)\det(S)\big(\det(A)\big)^{-1} = \det S = 1, \\ &\Rightarrow ASA^{-1} \in SL_n(\mathbb{F}),\ \forall A \in GL_n(\mathbb{F}), \\ &\Rightarrow A\big(SL_n(\mathbb{F})\big)A^{-1} = SL_n(\mathbb{F}), \end{aligned}$$

Kar pa pomeni $SL_n(\mathbb{F}) \lhd GL_n(\mathbb{F})$. ■
Kaj pa je im(det)? Determinanta je surjektivna, saj za poljuben $a \in \mathbb{F}^*$ velja

$$\det \begin{bmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & \ddots & & & & & \\ & & & 1 & & & & \\ & & & & a & & & \\ & & & & & 1 & & \\ & & & & & & \ddots & \\ & & & & & & & 1 \end{bmatrix} = a.$$

Potem to pomeni

$$\overline{\det} : {}^{GL_n(\mathbb{F})}\!/_{SL_n(\mathbb{F})} \xrightarrow{\cong} \mathbb{F}^*,$$

torej je kvocientna grupa ${}^{GL_n(\mathbb{F})}\!/_{SL_n(\mathbb{F})} \cong \mathbb{F}^*$, kar pa pomeni, da je kvocientna grupa kar $\mathbb{F}^*$.

Trditev:

Drugi in tretji izrek o izomorfizmu: Naj bo G grupa in $H, K \leq G$. Potem velja:

(2) Če je $K \lhd G$, potem je $H \cap K \lhd H$ in ${}^{H}\!/_{K \cap H} \cong {}^{HK}\!/_{K}$

(3) Če je $K \leq H$ in sta obe edinki v G, potem je

$${}^{H}\!/_{K} \lhd {}^{G}\!/_{K}$$
in
$${}^{G}\!/_{K}\Big/{}^{H}\!/_{K} \cong {}^{G}\!/_{H}$$

Dokaz:

(3) Naj bo $f : {}^{G}\!/_{K} \to {}^{G}\!/_{H}$ homomorfizem s predpisom $f(aK) = aH$. Relacija f je res homomorfizem, saj je

$$f(aK \cdot bK) = f(abK) = abH = aH \cdot bH = f(aK)f(bK).$$

f je očitno surjektiven, saj dobimo v sliki vse odseke, zato moramo izračunati le $\ker f$, pa dobimo

izomorfizem

$$\overline{f} : {}^{G}\!/_{K}\!/_{\ker f} \to {}^{G}\!/_{H}.$$

V $\ker(f)$ so vsi odseki aK, ki se s f preslikajo v identični odsek $eH \equiv H$, v ${}^{G}\!/_{H}$,

$$aK \overset{f}{\longmapsto} aH = H \iff a \in H.$$

Torej so v jedru ravno tisti odseki, ki imajo predstavnike v H:

$$\{aK \mid a \in H\} \equiv {}^{H}\!/_{K} \cong \ker f.$$

■

(2) Naj bo $p : G \to {}^{G}\!/_{K}$ kvocientni homomorfizem in $q \equiv {}^{p}\!/_{H}$,

$$q : H \to {}^{G}\!/_{K}.$$

Trdimo, da je jedro q: $\ker q = H \cap K$; in slika q: $\operatorname{im} q = {}^{HK}\!/_{K}$. Velja

$$q(a) = \text{identiteta} \iff p(a) = \text{identiteta} \iff a \in K.$$

Vendar $a \in H$. Torej velja $a \in K \cap H \Rightarrow K \cap H \lhd H$.

Po prvem izreku o izomorfizmu sledi $q : {}^{H}\!/_{K \cap H} \overset{\cong}{\longrightarrow} \operatorname{im} q$. V sliki so vsi odseki oblike aK, $a \in H$. Kot množica elementov v G to ustreza produktu množic $HK = \{ab \mid a \in H,\ b \in K\}$. Ta množica je podgrupa v G, ker je K edinka.

$$a_1b_1 \cdot a_2b_2 = \underbrace{a_1a_2}_{\in H}\underbrace{(\ \underbrace{a_2^{-1}b_1a_2}_{\in K\ (\text{edinka})}\ )}_{\in K}b_2 \in HK.$$

Torej so $\operatorname{im} q$ odseki HK po K, to je ${}^{HK}\!/_{K}$.

■

1.2.1 Komutatorska podgrupa

Grupa je *abelova*, če produkt komutira: $ab = ba$, $\forall a, b \in G$.

$$\begin{aligned} ab &= ba \quad / \cdot a^{-1} \\ aba^{-1} &= b \quad / \cdot b^{-1} \\ aba^{-1}b^{-1} &= e \ \overset{(!)}{\longleftarrow} \end{aligned}$$

Definicija:

Za $a, b \in G$ je $[a, b] \equiv aba^{-1}b^{-1}$ *komutator* elementov a in b. *Komutatorska podgrupa*, $[G, G]$, je najmanjša podgrupa, ki vsebuje vse komutatorje v G.

Opomba: $[G, G]$ očitno vsebuje produkte komutatorjev in vsi elementi so take oblike: $e[a, a]$.

$$[a, b]^{-1} = (aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1} = [b, a].$$

Trditev:

Naj bo G poljubna grupa. Velja:

(1) $[G,G] \lhd G$,

(2) $G/[G,G]$ je abelova in jo imenujemo *abelacija* ali *abelianizacija* grupe G.

(3) Če je H poljubna abelova grupa in $f : G \to H$ homomorfizem, potem $[G,G] \leq \ker f$

Dokaz:

(1) Ker je vsak element iz $[G,G]$ produkt komutatorjev za poljuben $a \in G$, tudi $c[a,b]c^{-1}$ nek komutator, saj za produkt

$$[a_1,b_1]\cdot[a_2,b_2]\cdot\ldots\cdot[a_k,b_k]$$

velja

$$c[a_1,b_1]\cdot\ldots\cdot[a_k,b_k]c^{-1} = c[a_1,b_1]c^{-1}c[a_2,b_2]c^{-1}\ldots c[a_k,b_k]c^{-1}$$

Izračunajmo konjugacijo:

$$\begin{aligned} c[a,b]c^{-1} &= caba^{-1}b^{-1}c^{-1} = cac^{-1}cbc^{-1}ca^{-1}c^{-1}cb^{-1}c^{-1} \\ &= (cac^{-1})(cbc^{-1})(cac^{-1})^{-1}(cbc^{-1})^{-1} = [cac^{-1},cbc^{-1}] \in [G,G]. \blacksquare \end{aligned}$$

(2) Pokazati moramo, da odseki v $G/[G,G]$ komutirajo (tj. ta kvocientna grupa je abelova):

$$a[G,G]\cdot b[G,G] \stackrel{?}{=} b[G,G]\cdot a[G,G]$$

Pokazati moramo, da ab in ba predstavljati isti odsek, to pa je $\iff (ba)^{-1}ab \in [G,G]$:

$$(ba)^{-1}ab = a^{-1}b^{-1}ab = [a^{-1},b^{-1}] \in [G,G]. \blacksquare$$

(3) Če je $f : G \to H$ homomorfizem v abelovo grupo, čelimo videti, da je $[G,G] \leq \ker f$. Dovolj je, če

$$f\big([a,b]\big) = e,$$

če pokažemo za enega, to je

$$f\big(aba^{-1}b^{-1}\big) = \overbrace{f(a)f(b)f(a^{-1})f(b^{-1})}^{\text{elementi v } H \text{ komutirajo}} = f(a)f(a^{-1})f(b)f(b^{-1}) \stackrel{\text{homo.}}{=} f(a)f(a)^{-1}f(b)f(b)^{-1} = e$$

$\blacksquare$

Vsebina: Komutatorska podgrupa je najmanjša edinka v G, po kateri je kvocient abelov.

Poglavje 2

Simetrije in upodobitve

Definicija:

Naj bo X poljubna množica. *Simetrična* ali *permutacijska množica* X je množica vseh bijekcij $X \to X$.

To imenujemo *permutacije* ali *simetrije* na X, oznaka za grupo je $S(X)$. Posebej če je X končna in $|X| = n$, označimo $S(X)$ z S_n in elemente X označimo z $\{1, 2, \ldots, n\}$. V tem primeru permutacije opišemo

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \alpha(1) & \alpha(2) & \alpha(3) & \ldots & \alpha(n) \end{pmatrix},$$

če je α permutacija.

Posebne permutacije so cikli:

Definicija:

$\alpha \in S_n$ je r-cikel, če $\exists \overbrace{i_1, i_2, \ldots, i_r}^{\text{vsi različni}} \in \{1, 2, \ldots, n\}$, ki jih α premakne, ostale elemente pa pusti pri miru (oz. jih fiksira) in velja:

$$\alpha(i_1) = i_2,\ \alpha(i_2) = i_3, \ldots,\ \alpha(i_{r-1}) = i_r,\ \alpha(i_r) = i_1.$$

Tak α ponavadi zapišemo kot $\alpha = (i_1, i_2, i_3, \ldots, i_r)$.

Definicija:

Dva cikla, α in β sta *disjunktna*, če premakneta različne elemente – tj. β lahko premika kvečjemu elemente, ki jih α fiksira in obratno.

Vaja:

1. $|S_n| = n!$ (očitno).
2. Če je α r-cikel, je $\text{red}(\alpha) = r$:

Dokaz: $\text{red}(\alpha) = k$, če $\alpha^k = e$ in k najmanjše tako število. Jasno je, da je $\alpha^r = e$. Tak r je najmanjši: za $k < r$, α^k preslika i_1 v i_{1+k}, kjer je $1 + k \in \{2, \ldots, r\}$, zato $i_{i+k} \neq i_1$. ■

3. Naj bo α r-cikel in $d \in \mathbb{N}$. Potem α^d produkt (d, r) disjunktnih ciklov dolžine $r/(d, r)$ (oznaka (d, r) naj bi predstavljala največji skupni delitelj števil d in r).

   Dokaz:

   - $G = \langle a \rangle$ je ciklična grupa reda r.
   - $H = \langle a^d \rangle$ je podgrupa v G

   $x = e^{2i\pi/12}$ generira C_{12}, x^d generira podgrupo: $\langle x^d \rangle = \{x^{dk} \mid k \in \mathbb{Z}\}$

   - ◇ $\underline{d = 5:}$ $\langle x^5 \rangle = \{e, x^5, (x^5)^2, \ldots, (x^5)^1 2\}$ – imamo 12 različnih elementov – seveda, največji skupni delitelj grup je 1, ker sta si 5 in 12 tuji števili $\Rightarrow \langle x^5 \rangle = \langle x \rangle = C_{12} \leq C_{12}$, saj je $12/(12, 5) = 12/1 = 12$.
   - ◇ $\underline{d = 3:}$ $\langle x^3 \rangle = \{e, x^3, (x^3)^2, (x^3)^3\} \cong C_4$, ker je $12/(12, 3) = 12/3 = 4$.

   Odtod sklepamo, da če $k = (d, r)$, potem je H ciklična podgrupa moči (reda) r/k. Dobiti moramo najmnanjši n, da je $(\alpha^d)^n = e$. Očitno je $(\alpha^d)^{r/k}$, $\alpha^{dr/k} = (\alpha^r)^{d/k} = e$. To število je najmanjše s to lastnostjo:

   $$\alpha^{dn} = e, \quad \text{upoštevamo, da je } \alpha \text{ reda } r$$

   $\Rightarrow r | dn$ (r najmanjše število, pri katerem $\alpha^r = e$). Ker je $k = (d, r) \Rightarrow (r/k) | n \Rightarrow n \geq r/k$.

   Sklep: Če je največja skupna mera števil d in r enaka 1 $\big(\text{tj. } (d, r) = 1\big)$, α^d določa isto grupo moči r in je zato r-cikel. V primeru, da $k \neq 1$ trdimo, da α razpade na produkt k disjunktnih ciklov.

   ■

Opomba: disjunktni permutaciji (cikla) komutirata.

Trditev:

Vsaka permutacija v $S_n \backslash \{e\}$ je produkt disjunktnih ciklov dolžine ≥ 2. Ta produkt je do vrstnega reda faktorjev enoličen.

Posledica:

Vsaka permutacija je produkt *transpozicij*, tj. ciklov dolžine (reda) 2: (a, b), $a \neq b$.

Opomba: Ta izrazitev *ni* enolična. Enolična je le parnost števila transpozicij).

Definicija:

Predznak ali *parnost* permutacije, je število, ki ga dobimo kot $(-1)^{\#\text{transpozicij}}$ v poljubni izrazitvi permutacije s transpozicijami.

Oznaka: α permutacija $\Rightarrow$ predznak α ... $\text{sign}(\alpha) \in \{\pm 1\}$.

Trditev:

sign : $S_n \to C_2 = \{\pm 1\}$, je homomorfizem in jedro tega imenujemo *alternirajoča grupa*, A_n.

Sledi: $A_n \lhd S_n$, indeksa 2.

Dokaz: α r-cikel, β p-cikel $\Rightarrow \operatorname{sign}(\alpha\beta) = (-1)^{r+p} = (-1)^r(-1)^p = \operatorname{sign}(\alpha)\operatorname{sign}(\beta)$. sign torej res homomorfizem in je hkrati surjektiven, saj je znak $\forall$ transpozicije -1. $A_n = \ker(\text{sign})$ je edinka,

$$S_n/A_n = \{\pm 1\},$$

kar pa pomeni $[S_n : A_n] = 2$.

■

Ponovitev:

- X množica, $S(X) = \{\text{bijekcije} X \to X\}$
- $X = \{1, 2, \ldots, n\} \to S(X) = S_n$

Trditev:

Caylejev izrek:
- G poljubna grupa. Potem je G izomorfna podgrupi simetrične grupe $S(G)$.
- Če je G končna in $|G| = n$, potem je G izomorna podgrupi v S_n.

Dokaz: Za dano G želimo poiskati ...

- $S(G) = \{f : G \to G \mid f \text{ bijekcija}\}$
- G je grupa z operacijo $G \times G \to G$ in potem injektivni homomorfizem $G \to S(G)$.

Naj bo $L : G \to S(G)$, $g \mapsto L_g$ (leva translacija). Za levo translacijo velja (str. 13):

- L_g je bijekcija, njen inverz je $L_{g^{-1}}$
- L je homomorfizem: $L(gh) = L_g \circ L_h$ (kompozitum v $S(G)$).
- L je injektivna: če je L_g identiteta, je $L_g(e) = ge = e \Rightarrow g = e \;\Rightarrow\; \ker L = e$.

Slika $L(G) \in S(G)$ je torej izomorfna G.

■

Posledica:

Naj bo G končna grupa, $|G| = n$, in $\mathbb{F}$ poljuben obseg. Tedaj je G *izomorfna podgrupi v* $GL_n(\mathbb{F})$ in $\exists$ homomorfizem $\varphi : G \to GL_n(\mathbb{F})$ ki je injektiven.

Dokaz: Bolj na splošno: naj bo X poljubna končna množica in $\varphi : G \to S(X)$ homomorfizem. Ta homomorfizem lahko „dvignemo“ do homomorfizma v neko splošno linearno grupo,

- Naj bo V vektorski prostor nad $\mathbb{F}$ za bazo X, torej

$$X = \{x_1, x2, \ldots, x_m\},$$
$$V = \left\{ \sum_{i=1}^{m} \lambda_i x_i \;\middle|\; \lambda_i \in \mathbb{F} \right\}.$$

- Grupo $S(X)$ lahko vložimo v $GL_{\mathbb{F}}(V)$, tako da vsakemu elementu $\sigma \in S(X)$ priredimo linearno preslikavo, ki permutira vektorje v bazi

$$\begin{aligned} \sigma &\mapsto A_\sigma; \\ A_\sigma : V &\to V \\ x_i &\mapsto \sigma(x_i) = x_{\sigma(i)} \end{aligned}$$

- Matrika takšne preslikave je *permutacijska matrika*, ki je obrnljiva ($\det A_\sigma = \pm 1$) in jo dobimo z zamenjavo matrike identitete. Na ta način $S(X)$ postane podgrupa v $GL_{\mathbb{F}}(V)$ in φ porodi

$$\begin{array}{rccc} \hat{\varphi}: & G & \longrightarrow & GL_{\mathbb{F}}(V) \\ & \searrow & & \nearrow \\ & & S(X) & \\ & {\scriptstyle \varphi} & & \end{array}$$

Posebej: Če je $\varphi : G \to S(X)$ injektiven, dobimo injektiven $\hat{\varphi}$. Za $X = G$ je $|X| = |G| = n$, zato je V vektorski prostor nad $\mathbb{F}$ dimenzije n in je $GL_{\mathbb{F}}(V) \equiv GL_n(\mathbb{F})$.

■

2.1 Teorija upodobitev in pridruženih delovanj

Definicija:

Naj bo G grupa in X množica. Potem homomorfizem $\varphi : G \to S(X)$ imenujemo *upodobitev* (*reprezentacija*).

Definicija:

Naj bo V vektorski prostor nad obsegom $\mathbb{F}$. Homomorfizem $\varphi : G \to GL_{\mathbb{F}}(V)$ imenujemo *linearna upodobitev* G na V.

Opomba:

- Iz dokaza zadnje posledice sledi, da poljubna upodobitev $G \to S(X)$ porodi linearno upodobitev $G \to GL_{\mathbb{F}}(V)$, kjer je V vektorski prostor z bazo X nad obsegom $\mathbb{F}$.

- Upodobitvi $G \to S(G)$, oz. $G \to GL_{\mathbb{F}}(V)$, kjer je V vektorski prostor z bazo G, rečemo *regularna upodobitev* (tj. $X = G$).

Glavni rezultat teorije upodobitev končnih grup je, da **linearna regularna upodobitev vsebuje vse linearne upodobitve**.

Poljubna upodobitev $\varphi : G \to S(X),\ g \mapsto \sigma$ porodi *delovanje* grupe G na množico X, tj. preslikavo

$$\begin{aligned} \tilde{\varphi} : G \times X &\to X, \\ (g, x) &\mapsto \varphi(g)(x) = \sigma(x), \end{aligned}$$

z lastnostima:

- $\tilde{\varphi}(e, x) = \varphi(e)(x) = x$, ker je φ homomorfizem, je $\varphi(e)$ spet identiteta.
- $\tilde{\varphi}\big(g, \tilde{\varphi}(h, x)\big) = \big[\varphi(g) \circ \varphi(h)\big](x) = \varphi(gh)(x) = \tilde{\varphi}(gh, x)$

Dogovor: Kjer imamo opraviti le z enim delovanjem, izpustimo ime preslikave in pišemo kar

$$\tilde{\varphi}(g, x) = gx.$$

V tem zapisu sta zgornji lastnosti

$$\begin{aligned} \varphi(e) = \mathrm{id} \Rightarrow ex &= x \\ (gh)x &= g(hx) \end{aligned}$$

izgledata kot definicija identitete in asociativnost.
Velja tudi obratno: vsako delovanje G na X določa upodobitev G na X:

$$\left.\begin{array}{r} \underline{\text{Upodobitve}} \\ G \to S(X) \\ \text{homomorfizmi} \end{array}\right\} \longleftrightarrow \left\{\begin{array}{r} \underline{\text{Delovanja}} \\ G \times X \to X \\ ex = x \\ (gh)x = g(hx) \end{array}\right.$$

Analogno za linearne upodobitve dobimo korespondenco z delovanji, ki so pri fiksnem g linearni.

$$\left.\begin{array}{r} G \to GL_{\mathbb{F}}(V) \\ V \text{ vekt. prostor} \\ \text{homo.} \end{array}\right\} \longleftrightarrow \left\{\begin{array}{rl} G \times V & \to V \\ ex & = x \\ (gh)x & = g(hx) \\ x & \mapsto gx \text{ je linearna} \end{array}\right.$$

Definicija:

Naj G deluje na X (imamo delovanje $G \times X \to X$).

- *Orbita* elementa $x \in X$ je $Gx = \{gx \mid g \in G\}$.
- *Stabilizatorska podgrupa* elementa $x \in X$ je $G_x = \{g \in G \mid gx = x\}$.

Trditev:

Naj G deluje na X.

1. Potem je $G_x \leq G, \forall x \in X$.
2. Stabilizator poljubne druge točke na orbiti Gx je konjugiran stabilizatorju x.
3. Če je X končen, je $|Gx| = [G : G_x]$

Dokaz: [*Vaja*]

1. G_x je res podgrupa:

   - $e \in G_x: \ ex = e \Rightarrow e \in G_x$ po definiciji
   - $g \in G_x \Rightarrow g^{-1} \in G_x$:

   $$\begin{aligned} gx &= x, \quad / \cdot g^{-1}, \text{ asociatovnost} \\ x &= g^{-1}gx = g^{-1}x \Rightarrow g^{-1} \in G_x \end{aligned}$$

   - produkt: $ghx = gx = gx = x$ (očitno, ker $gx = x$ in $hx = x$). ■

2. Izberimo poljuben $y \in Gx$. Dokazujemo, da je G_y konjugiran G_x, tj. $\exists a$, tako da: $G_y = aG_xa^{-1}$. Vemo: $y = gx$ za nek $g \in G$. Naj bo $h \in G_y : hy = y$,

   $$\left.\begin{aligned} hgx &= gx \\ g^{-1}hgx &= x \\ g^{-1}hg &\in G_x \end{aligned}\right\} G_y \subseteq gG_xg^{-1}$$

   Sedaj enako naredimo za $g^{-1}: \ x = g^{-1}y$, ostalo je enako. Od tam sledi, da je tudi $G_x \subseteq g^{-1}G_yg$. To je res natanko tedaj, ko $G_y = gG_xg^{-1}$. ■

3. X končna, $Y = G_x \subseteq X$ tudi končna. $Y \subseteq X$ je invariantna za delovanje G, v smislu, da je $\forall g \in G$ in $\forall y \in Y : gy \in Y$.

   Trdimo, da je $|Y|$ enaka št. odsekov G_x v G. Glejmo preslikavo $f : G \to Y$, $g \mapsto gx$. f je surjektivna (po definiciji Y) in

   $$f(g) = f(h) \iff gx = hx \iff h^{-1}gx = x, \ h^{-1}g \in G_x,$$

   to pa je natanko tedaj, ko h in g določata isti odsek $\Rightarrow$ št. različnih točk v Y je enako št. različnih odsekov G_x v G. $|Y| = [G : G_x]$.

■

2.2 Operacije na grupah in strukturni izreki

Definicija:

Direktni produkt grup G in H je grupa $G \times H$ z operacijo množenja po komponentah:

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1g_2, h_1h_2).$$

Identiteta je (e, e), inverz elementa (g, h) je $(g, h)^{-1} = (g^{-1}, h^{-1})$, asociativnost pa sledi iz asociativnosti v G in H.

Opombe:

- V grupi $G \times H$ lahko gledamo G in H kot podgrupi, $G \equiv G \times \{e\}$ in $H \equiv \{e\} \times H$. Pri tej identifikaciji elementi podgrup G in H med seboj komutirajo.
- $(g, e) \cdot (e, h) = (ge, eh) = (g, h)$
- $(e, h) \cdot (g, e) = (eg, he) = (g, h)$
- Poleg tega sta G in H edinki v $G \times H$, njun presek je $G \cap H = \{e\} = (e, e)$.

Iz teh opažanj dobimo

Trditev:

G, H, K grupe, $H, K \lhd G$, $H \cap K = \{e\}$ in $HK = G$. Potem je $G = H \times K$.

Dokaz: [*Ideja*] Najprej vidimo, da elementi iz H komutirajo z elementi iz K (saj $H \cap K = \{e\}$). Upoštevamo **lemo:** G, H abelovi $\Rightarrow G \times H$ abelova.

Primer:

1. $G = C_2 \times C_3 =$? Najprej lahko kar zapišemo grupne elemente:

$$C_2 = \{1, -1\},$$
$$C_3 = \{1, \exp(2i\pi/3), \exp(-2i\pi/3\}$$
$$G = \left\{(1,1), \left(1, e^{2i\pi/3}\right), \left(1, e^{-2i\pi/3}\right), (-1,1), \left(-1, e^{2i\pi/3}\right), \left(-1, e^{-2i\pi/3}\right)\right\}$$

   Opazimo, da je $|G| = 6$. A je G izomorfna kakšni znani grupi moči 6, npr. C_6 (v tem primeru, moramo najti element reda 6). Če je G ciklična ima generator reda 6 in preslikava, ki preslika generator v $\exp(2i\pi/6)$ bo izomorfizem $G \to C_6$. Uganemo:

$$\left(-1, e^{2i\pi/3}\right)^1 = \left(-1, e^{2i\pi/3}\right),$$
$$\left(-1, e^{2i\pi/3}\right)^2 = \left((-1)\cdot(-1), e^{2i\pi/3}e^{2i\pi/3}\right) = \left(1, e^{-2i\pi/3}\right),$$
$$\left(-1, e^{2i\pi/3}\right)^3 = (-1, 1),$$
$$\left(-1, e^{2i\pi/3}\right)^4 = \left(1, e^{2i\pi/3}\right),$$
$$\left(-1, e^{2i\pi/3}\right)^5 = \left(-1, e^{-2i\pi/3}\right),$$
$$\left(-1, e^{2i\pi/3}\right)^6 = (1, 1)$$

   Vidimo: element $\left(1, \exp(-2i\pi/3)\right)$ generira celotno grupo G, in je reda 6 – tj. $G \cong C_6$, z izomorfizmom:

$$f : G \to C_6,$$
$$f\left(\left(-1, e^{2i\pi/3}\right)\right) = e^{2i\pi/6}, \text{ homomorfizem, torej,}$$
$$f\left(\left(-1, e^{2i\pi/3}\right)^k\right) = e^{2i\pi k/6}.$$

2. $G = C_2 \times C_4$, ali je izomorfna kakšni znani grupi (npr. C_8, sodeč po prejšnjem primeru)?

$$G = \{(1,1), (1,i), (1,-1), (1,-i), (-1,1), (-1,i), (-1,-1), (-1,-i)\}$$

   Ne glede na to, s katerim elementom bomo poskušali, največji red elementa je 4. Vendar pa ta grupa ni izomorfna C_4, saj nimamo bijektivnega homomorfizma, ki bi 8 elementov preslikal v 4. Imamo pač abelovo grupo, ki je bolj kompliciran.

3. $G = C_m \times C_n$, kjer sta m, n tuji si števili (njun največji skupni delitelj je 1).

   Vaja: Pokaži $G \cong C_{m\cdot n}$. Bolj splošno: za poljubni ciklični grupi redov m in n

$$G = \langle a \rangle \times \langle b \rangle$$

   Trdimo, da ima par $(a, b) \in G$ red $m \cdot n$. Velja $(a, b)^k = \left(a^k, b^k\right)$.

- $(a,b)^{mn} = (e,e)$ je očitno.
- mn je najmanjši tak eksponent v $\mathbb{N}$. Vemo $|G| = mn$. Red vsakega elementa deli mn. Če je (a,b) manjšega reda, kot mn, $\exists\ k \mid mn$ ∍: $(a,b)^k = (a^k, b^k) = (e,e)$.

$$\left.\begin{array}{ll} a^k = e & \Rightarrow m \mid k \\ b^k = e & \Rightarrow n \mid k \end{array}\right\} = k = mn$$

Če m in n nista tuja, je največji red enak najmanjšemu skupnemu večkratniku, kar je manj od $|G| = mn \Rightarrow$ ni ciklična.

■

Definicija:

- G grupa, X je podmnožica v G, tj. $X \subseteq G$. X *generira* G, če je $G = \langle X \rangle$ najmanjša podgrupa v G, ki vsebuje $\langle X \rangle$.
- G je *končno generirana*, če $\exists$ končna $X \subseteq G$ ∍: $G = \langle X \rangle$ (tj. število generatorjev v X je končno).
- G je *torzijska*, če je $\forall$ element v G končnega reda.
- Za praštevilo $p \in \mathbb{P}$ je G *p-grupa*, če je red vsakega elemnta v G neka potenca p-ja.
- G je *prosta abelova grupa* ranga $n \in \mathbb{N}$, če je $G \cong \underbrace{\mathbb{Z} \times \mathbb{Z} \times \ldots \times \mathbb{Z}}_{n\text{-krat}} = \mathbb{Z}^n$.

Trditev:

[*Brez dokaza.*] Naj bo A abelova grupa. Potem je množica vseh elementov končnega reda v A torzijska podgrupa T. Če je A končno generirana, je A/T prosta abelova grupa končnega ranga in

$$A \cong T \times A/T$$

Trditev:

[*Brez dokaza.*] Naj bo T končna abelova grupa. Potem $\exists$ zaporedje naravnih števil n_1, n_2, …, n_k, kjer

$$n_k \mid n_{k-1} \mid n_{k-2} \mid \ \ldots\ \mid n_2 \mid n_1$$

in velja

$$T \cong C_{n_1} \times C_{n_2} \times \ldots \times C_{n_k}.$$

Opomba: V primeru $C_2 \times C_4$ smo imeli primer takšnega zapisa končne abelove grupe $n_1 = 4$, $n_2 = 2$.

Posledica:

Če je T končna abelova grupa in $n = |T|$ nima kvadratnih faktorjev, je T ciklična moči n.

Dokaz: Po prejšnjem je $T = C_{n_1} \times \ldots \times C_{n_k}$ Če je $n_2 > 1$, potem je $n_2 \mid n_1$ in $n_1 \cdot n_2 \mid n$, potem $n_2^2 \mid n$, kar je v nasprotju s predpostavko. ■

Posledica:

Če je A končno generirana prosta abelova grupa in $B \leq A$ (podgrupa), je tudi B prosta.

Iz vsega tega dobimo metodo za predstavitev poljubne končno generirane abelove grupe A:

- Naj bo $X = \{x_1, x_2, \ldots, x_n\}$ končna množica generatorjev in $\mathbb{Z}^n$ prosta abelova grupa ranga n.

$$\{e\} \to \underbrace{\ker f}_{\cong \mathbb{Z}^m} \longrightarrow \mathbb{Z}^n \xrightarrow{f} A \to \{e\}$$

$$\mathbb{Z}^m \in (k_1, k_2, \ldots, k_n) \overset{f}{\mapsto} x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n} \ni A,$$

homomorfizem f je surjektiven, ker so x_i generatorji. Dobimo zgornje eksaktno zaporedje, ki pomeni $A \cong \mathbb{Z}^n / \ker f$. To da opis A z generatorji in relacijami:

$$A = \big[\underbrace{x_1, x_2, \ldots, x_n}_{\text{generatorji } A} \mid \underbrace{r_1, r_2, \ldots, r_m}_{\text{generatorji } \ker f}\big] \tag{2.1}$$

Opomba: Abelove grupe večinoma pišemo aditivno, v tem primeru direktni produkt zamenjamo z direktno vsoto, '$\oplus$'.

Zgled:

1. Ostanki po modulu n:

$$C_n \cong \mathbb{Z}_n = \{0, 1, \ldots, n-1\},$$

$\mathbb{Z}_n$ je ciklična z generatorjem 1.

$$\left.\begin{array}{rcl} \underbrace{\ker f}_{=n\mathbb{Z}} \to \mathbb{Z} & \xrightarrow{f} & \mathbb{Z}_n \\ 1 & \mapsto & 1 \end{array}\right\} \mathbb{Z}_n = \big[1 \mid n\big],$$

saj je '1' generator, in $n \cdot 1 = 0 \in \ker f$. Če generator označimo z x, potem je $\mathbb{Z}_n = \langle x \rangle$, relacija pa je $nx = 0$, $\Rightarrow \mathbb{Z}_n = \big[x \mid nx\big]$.

2. Naj bo $A = [x, y \mid 2x + y,\ x - 2y]$. Zapiši A kot vsoto (produkt) proste grupe in cikličnih končnih grup. To pomeni nekako tole

$$A = \mathbb{Z}_x \oplus \mathbb{Z}_y / \langle 2x + y,\ x - 2y \rangle$$

Ideja je ta, da generatorja (bazo) tako zamenjamo, da bo imenovalec lepši. Potem bosta relaciji preprostejši, $\Rightarrow$ relaciji oblike au, bv. Potem delamo linearno algebro nad $\mathbb{Z}$.

$$\begin{array}{ll} r_1 & = 2x + y \\ r_2 & = x - 2 \end{array} \quad \Big| \quad \text{Ideja:} \quad \begin{bmatrix} u \\ v \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix}, \text{ tj. } u, v \text{ lin. komb. } x \text{ in } y.$$

Matrika $A \in SL(2, \mathbb{Z})$, tj. mora biti obrnljiva, z '$\det A = 1$' (sicer so dobre tudi matrike, ki imajo '$\det A = -1$', vendar ugibamo, da zadošča $\det A = 1$) in celimi koeficienti. Gotovo je ta matrika oblike

$$\begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \quad \text{ali} \quad \begin{bmatrix} 1 & 0 \\ * & 1 \end{bmatrix}.$$

To nam te ti dve možnosti:

$$\begin{bmatrix}1 & n\\ 0 & 1\end{bmatrix}\begin{bmatrix}x\\ y\end{bmatrix}=\begin{bmatrix}x+ny\\ y\end{bmatrix};\quad \begin{bmatrix}1 & 0\\ n & 1\end{bmatrix}\begin{bmatrix}x\\ y\end{bmatrix}=\begin{bmatrix}x\\ y+nx\end{bmatrix}.$$

Dovoljeni operaciji sta:

$$(x,y)\mapsto(x+ny,y),$$
$$(x,y)\mapsto(x,y+nx).$$

Uporabimo lahko $(x,y)\to(x-2y,y)=(u_1,v_1)$. Relaciji tedaj izgledata

$$r_2=u_1,$$
$$r_1=2(2y+u_1)+y=5y+2u_1=5v_1+2u_1.$$

(u_1,v_1) ne moremo pretvoriti na nič lepšega.

Ampak: r_1 in r_2 generirata podgrupo relacij, na teh operatorjih lahko uporabimo isti princip.

$$(r_1,r_2)\to(r_1-2r_2,r_2),$$
$$\left.\begin{array}{ll} r_2 & =u_1\\ r_1' & =5v_1\end{array}\right\}A=\mathbb{Z}_{u_1}\oplus\mathbb{Z}_{u_2}/\langle u_1,5v_1\rangle$$

Ostanejo le ostanki po modulu 5: generator u_1 smo čisto „ubili“, generator v_1 pa nam da le tiste, ki so deljivi s 5. To pomeni

$$A=[u_1,v_1\mid u_1,5v_1]=\mathbb{Z}_1\oplus\mathbb{Z}_5\cong\mathbb{Z}_5$$

2.3 Struktura končno generiranih abelovih grup

A abelova grupa. Potem

$$A\cong\overbrace{\mathbb{Z}^n}^{\text{prosti del}}\oplus\overbrace{\mathbb{Z}_{c_1}\oplus\mathbb{Z}_{c_2}\oplus\ldots\oplus\mathbb{Z}_{c_k}}^{\text{torzijska podgrupa } T},$$

$n=$ rang grupe A, c_i so torzijski koeficienti in

$$c_i\geq 1,\forall i\in I,\quad c_1\mid c_2\mid\ \ldots\ \mid c_k,$$

kanonična dekompozicija.
Če je A generirana z $x_1,\ldots,x_m$.

$$\{0\}\to\underbrace{K}_{\ker f}\to\mathbb{Z}^m\underset{e_i\ \mapsto x_i}{\to}A\to\{0\},$$

$$e_i=(0,\ldots,0,\overbrace{1}^{i},0,\ldots,0).$$

Če generatorje v $\mathbb{Z}^m$ poimenujemo $y_i=e_i$, potem je K kot podgrupa v $\mathbb{Z}^m$ generirana z nekimi r_j, ki so linearne kombinacije y_i

$$r_j=\sum_{i=1}^{m}a_{ji}y_i$$

Relacije lahko zapišemo v matriko relacij R

$$R=[a_{ji}]=\begin{bmatrix}a_{11} & a_{12} & \ldots & a_{1m}\\ a_{21} & a_{22} & \ldots & a_{2m}\\ \vdots & & \ddots & \end{bmatrix}$$

Ideja za izračuna kanonične dekompozicije A je, da s spremembami nabora generatorjev matriko R preoblikujemo tako, da iz nje lahko odčitamo torzijske koeficiente.

Trditev:

Naj bo A abelova in $X = \{x_1, x_2, \dots x_m\}$ nabor generatorjev za A. Potem je množica $Y = \{y_1, \dots, y_m\}$ tudi nabor generatorjev za A, če Y dobimo iz X z zaporedjem operacij iz tegale nabora:

1. Zamenjamo lahko dva generatorja:

$$y_j = x_i,\ y_i = x_j, \quad y_k = x_k\ \forall k \neq i, j.$$

2. En generator pomnožimo z (-1):

$$y_i = -x_i, \quad y_k = x_k \forall k \neq i.$$

3. Poljubnemu generatorju prištejemo linearno kombinacijo ostalih:

$$y_i = x_i + \sum_{j \neq i} n_j x_j; \quad n_j \in \mathbb{Z}.$$

Dokaz: Očitno ima vsaka od zgornjih operacij inverz iste vrste, torej res sistem generatorjev preslika v sistem generatorjev (*opomba*: to je Gaussova eliminacija nad $\mathbb{Z}$).

■

Algoritem: za izračun KD (kanonične dekompozicije): Dani R preoblikujemo v „diagonalno“ matriko,

$$\underbrace{\begin{bmatrix} c_1 & & & & & & \\ & c_2 & & & & & \\ & & \ddots & & & & \\ & & & c_\ell & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{bmatrix}}_{\text{Smithova normalna oblika}}, \quad c_1 \mid c_2 \mid \dots \mid c_\ell, \quad c_i \geq 1, \quad m - \ell = \operatorname{rang} A.$$

Matrika R je dimenzije $m \times m$, vendar je njen rang manjši za rang matrike A. Če je $c_1 = 1$: za generator x_1 velja, da je tudi v podgrupi relacij K – v kvocuentu dobimo $\mathbb{Z}_{x_1}/\mathbb{Z}_{x_1}$ trivialno grupo.

Postopek: Na mesto $(1,1)$ postavimo največji skupni delitelj elementov matrike R. Ta postane naš c_1. Z njim potem najprej uničimo preostale elemente v prvi vrstici (s prištevanjem prvega stolpca), nato z novo prvo vrstico uničimo preostale elemente v prvem stolpcu:

$$R \to \left[\begin{array}{c|ccc} c_1 & * & * & * \\ \hline * & & & \\ * & & R' & \\ * & & & \end{array}\right] \to \left[\begin{array}{c|ccc} c_1 & 0 & 0 & 0 \\ \hline 0 & & & \\ 0 & & R'' & \\ 0 & & & \end{array}\right]$$

Nadaljujemo na matriki R''.

Opomba: Delovanje algoritma da dokaz obstoja kanonične dekompozicije.

Primeri:

- Izračunaj KD grupe, ki je kvocient $\mathbb{Z}^3$ po podgrupi, generirani z generatorji $(3,6,-3)$, $(3,3,-6)$, $(3,3,3)$:

$$R = \begin{bmatrix} 3 & 6 & -3 \\ 3 & 3 & -6 \\ 3 & 3 & 3 \end{bmatrix} \to \begin{bmatrix} 3 & 0 & 0 \\ 3 & -3 & -3 \\ 3 & -3 & 6 \end{bmatrix} \to \left[\begin{array}{c|cc} 3 & 0 & 0 \\ \hline 0 & -3 & -3 \\ 0 & -3 & 6 \end{array}\right] \to \begin{bmatrix} 3 & 0 & 0 \\ 0 & 3 & -3 \\ 0 & 3 & 6 \end{bmatrix} \to \begin{bmatrix} 3 & & \\ & 3 & \\ & & 9 \end{bmatrix};$$

$$\Rightarrow \begin{array}{rl} c_1 & = 3 \\ c_2 & = 3 \\ c_3 & = 9 \end{array}, \quad \operatorname{rang} A = 0,$$

  R je matrika relacij za grupo $A = \mathbb{Z}^3/K = \mathbb{Z}_x \oplus \mathbb{Z}_y \oplus \mathbb{Z}_z/\langle 3x, 3y, 9z\rangle = [x, y, z \mid 3x, 3y, 9z] = \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9$.

  Opomba: Operacije iz trditve delamo na vrsticah in s tem spreminjamo generatorje podgrupe relacij ter na stolpcih in s tem spreminjamo generatorje proste grupe.

- Določi KD kvocienta $\mathbb{Z}^3$ po podgrupi, generirani z $(2,4,2)$ in $(4,3,1)$:

$$R = \begin{bmatrix} 2 & 4 & 2 \\ 4 & 3 & 1 \end{bmatrix} \to \begin{bmatrix} 1 & 3 & 4 \\ 2 & 4 & 2 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 0 \\ 0 & -2 & -6 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix},$$

$$A \cong \mathbb{Z} \oplus \mathbb{Z}_1 \oplus \mathbb{Z}_2 \cong \mathbb{Z} \oplus \mathbb{Z}_2 = [x_1, x_2, x_3 \mid x_1, 2x_2]$$

  V tem primeru x_3 generira prosti del, x_1 ne nastopa v kvocientu, x_2 je reda 2, tj. generira $\mathbb{Z}_2$.

2.4 Proste grupe, prosti produkti in predstavitve grup

V prosti abelovi grupi med generatorji velja komutativnost. Vendar, pa ni vsaka prosta grupa abelova. Razčistimo pojem, kaj pomeni prosta grupa:

Definicija:

Prosta grupa je taka, v kateri poleg osnovnih zahtev za grupo ni nobene druge relacije. Elemente take grupe predstavljamo kot besede.

Če so $x_1, \ldots, x_n$ v prosti grupi, potem je tudi $x_1 x_2 \ldots x_n$ element te grupe in ta se ne da poenostaviti v noben drug element, če $x_i \neq e \forall i$ in če v x_i in x_{i+1} ne nastopajo elementi skupaj z inverzom.

To idejo lahko uporabimo za konstrukcijo proste grupe na dani množici generatorjev:

- Naj bo $X = (x_i)_{i \in I}$ množica generatorjev grupe G. Prosto grupo nad X označimo s F_X (*free*), in dobimo takole: tvorimo besede nad abecedo s simboli x_i, x_i^{-1}, '_' (s '_' sem označil presledek).
- Besede so končni nabori črk abecede: $x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2} \ldots x_{i_k}^{\epsilon_k}$, kjer je $\epsilon_i = \pm 1$. Npr.

$$x_1 x_1 x_3 x_2^{-1} x_7 x_{11}^{-1} x_{12} x_{12}^{-1} x_{12} x_{12}$$

- Težave z grupno strukturo: $x_i x_i^{-1} \neq$ '_'. Te bi lahko izločili, ampak se naravno pojavijo pri množenju, ki je stikanje besed. Iz množice besed za opisano operacijo dobimo grupo tako, da vpeljemo relacijo na besedah, ki $x_i x_i^{-1} = x_i^{-1} x_i = e =$ '_' enači z identiteto.
- Ta kvocient imenujemo *prosta grupa nad X*.

Opomba: Preveriti je treba, če ta konstrukt res ustreza definiciji grupe:

- ima identiteto: prazna beseda (presledek),
- vsaka beseda ima inverz: $\left(x_{i_1}^{\epsilon_1} \dots x_{i_k}^{\epsilon_k}\right)^{-1} = x_{i_k}^{-\epsilon_k} \dots\ x_{i_1}^{-\epsilon_1}$
- Pokazati jo je sitno, zaradi krajšanja, vendar drži (*verjamemo na besedo* – „pun intended“).

Pomen: Analogno kot pri abelovih je vsaka grupa kvocient neke proste grupe. To izkoristimo za predstavitev poljubne grupe z generatorji in relacijami.

Lema:

Naj bo G grupa in X množica njenih generatorjev. Potem je G kvocient proste grupe nad X, tj. imamo eksaktno zaporedje

$$\{e\} \to \underset{=\ker f}{K} \to F_X \overset{f \text{ (homo.)}}{\longrightarrow} G \to \{e\},$$

ali $G \cong {}^{F_X}\!/_K$.

Dokaz: Vzamemo prosto grupo F_X in

$$\left.\begin{array}{rl} f : F_X & \to G \\ x_i & \mapsto x_i \end{array}\right\} \text{očitno surjektivna – v } \operatorname{im} f \text{ so vsi generatorji } G, \text{ in } \operatorname{im} f \leq G, \text{ je to cel } G.$$

Ta f je homomorfizem, $K = \ker f$. Potem imamo po standardnih izrekih (izreki o izmomorfizmu) $G \cong {}^{F_X}\!/_K$ oz. to zaporedje je eksaktno.

■

Posledica:

Naj bo G poljubna grupa, X množica in $f : X \to G$ preslikava.

Potem f določa enolično homomorfizem iz $\hat{f}$ iz proste grupe z generatorji X na G

$$\begin{array}{rl} \hat{f} : F_X & \to G \\ \hat{f}\big|_X & = f \end{array} \qquad \text{in} \qquad \begin{array}{ccc} X & \xrightarrow{f} & G \\ \searrow & & \nearrow_{\hat{f}} \\ & F_X & \end{array}$$

f določa homomorfizem $\hat{f}$ tako, da diagram komutira.

Dokaz: Definiramo $\hat{f}\left(x_{i_1}^{\epsilon_1} \dots x_{i_k}^{\epsilon_k}\right) = f(x_{i_1})^{\epsilon_1} \dots f(x_{i_k})^{\epsilon_k}$, kar velja po asociativnosti v G. ■

Trditev:

[*Brez dokaza*]Vsaka podgrupa proste grupe je prosta.

Pozor: pri abelovih je rang prodgrupe $\leq$ rangu grupe, pri prostih grupah pa ima lahko podgrupa več generatorjev, kot grupa (prosta grua na dveh generatorjih vsebuje proste grupe na več generatorjih, kot podgrupe).

Definicija:

Prosti produkt grup: G, H grupi, njun *prosti produkt* je $G * H$, množica besed in abecede $G \cup H$, kjer je operacija stikanja besed, edine relacije pa so tiste, ki veljajo v G in v H. Vsak element lahko zapišemo v obliki

$$g_1 h_1 g_2 h_2 \dots g_k h_k; \quad g_i \in G,\ h_i \in H,$$

saj upoštevamo množenje v G in H. Če je kakšen h_i ali g_j identiteta, lahko sosednja elementa zmnožimo v grupi. Kot pri prosti grupi preverimo, da je $G * H$ res grupa (tj. da je prosti produkt grup spet grupa).

Primer: Prosta grupa na dveh generatorjih $F_{\{x,y\}}$ je izomorfna prostemu produktu dveh kopij $\mathbb{Z}$. V grupi $F_{\{x,y\}}$ so besede $x^{n_1} y^{n_2} x^{n_3} y^{n_4} \dots$ kjer $n_i \in \mathbb{Z}$. V $\mathbb{Z} \times \mathbb{Z}$ z generatorjema x za prvi faktor in y za drugi faktor pa so besede $(n_1 x)(n_2 y)(n_3 x)(n_4 y) \dots$ kjer so faktorji pisani aditivno. Multiplikativno bi zapisali tako kot prej, $x^{n_1} y^{n_2} x^{n_3} y^{n_4} \dots$

$$\Rightarrow F_{\{x,y\}} \cong \mathbb{Z} * \mathbb{Z}$$
$$F_{\{x_1,\dots,x_n\}} \cong \underbrace{\mathbb{Z} * \mathbb{Z} * \dots * \mathbb{Z}}_{n \text{ faktorjev}}$$

Glavna uporaba je predstavitev grupe.

Definicija:

Predstavitev ali *prezentacija* grupe. Če je G poljubna grupa in $X = \{x_i, i \in I\}$ množica njenih generatorjev, potem je $G \cong {}^{F_X}\!/_{K}$, kjer je K edinka v F_X, določena kot jedro naravnega homomorfizma

$$f : F_X \to G$$
$$x_i \mapsto x_i$$

(za K vzamemo najmanjšo tako edinko). Če je R množica generatorjev za edinko K, je predstavitev grupe G z generatorji in relacijami dana z

$$G = \langle X \mid R \rangle. \tag{2.2}$$

Opomba: elementi v R so besede v X in $G = {}^{F_X}\!/_{\text{edinka, gen. z besedami v } R}$.

Zgled:

Poišči predstavietv za abelovo grupo $\mathbb{Z} = \mathbb{Z} \times \mathbb{Z}$ kot kvocient proste grupe $\mathbb{Z} * \mathbb{Z}$.

- $G = \mathbb{Z}^2$ z generatorjema $x = (1, 0)$ in $y = (0, 1)$ (aditiven zapis)

  $$\mathbb{Z}^2 \cong \langle \tilde{x}, \tilde{y} \mid [\tilde{x}, \tilde{y}] \rangle = \langle \tilde{x}, \tilde{y} \mid \tilde{x}\tilde{y} = \tilde{y}\tilde{x} \rangle,$$

  da smo dobili $\mathbb{Z}^2$ smo morali generatorjema $\tilde{x}$ in $\tilde{y}$ dodati relacijo komutativnosti.

- Je to res abelova grupa? $F_{\{\tilde{x},\tilde{y}\}}$ ima za komutatorsko grupo podgrupo, generirano s komuta-

torjem $[\tilde{x}, \tilde{y}]$:

$$\begin{aligned} F_{\{\tilde{x},\tilde{y}\}} &\xrightarrow{f} \mathbb{Z} \times \mathbb{Z} \\ \tilde{x}^n &\mapsto nx \\ \tilde{y}^n &\mapsto ny \end{aligned}$$

Ker je $\mathbb{Z}\times\mathbb{Z}$ abelova, jedro f vsebuje komutatorsko podgrupo, ki je generirana s komutatorjem $[\tilde{x}, \tilde{y}]$.

Zgled:

Poišči predstavitev S_3 (množica permutacij treh elementov).

Rešitev: Moč grupe je $|S_3| = 3! = 6$ in sicer

$$S_3 = \{e, (12), (13), (23), (123), (132)\}$$

Cilj nam je poiskati čim manjšo množico generatorjev in pripadajoče relacije:

$$\left.\begin{array}{ll} x & = (12), \quad \text{transpozicija} \\ y & = (123), \quad \text{tri-cikel} \end{array}\right\} \text{generatorja (ugibamo)}$$

$$x^2 = e, y^3 = e$$

Potrebujemo še eno zvezo, ker imamo ∞ elementov, S_3 pa jih ima samo 6. Uganemo $xyx = y^2$, tj.

$$S_3 = \langle x, y \mid x^2, y^3, xyx = y^2 \rangle.$$

Zgled:

Izračunaj predstavitev grupe simetrij pravilnega petkotnika G (v tem primeru $G = D_5$ – diederska grupa reda 5). To so togi premiki ravnine, ki petkotnik preslikajo nase – translacije in linearne preslikave. Velja $|D_n| = 2n$.

$$\vec{x} \mapsto \vec{a} + A\vec{x}, \quad \vec{a} = \text{konst. in } \det A \neq 0.$$

- $G \leq S_5$ ($|G| = 10$, $|S_5| = 120$).
- Uganemo generatorje:
  - rotacija: $(12345) = x = \exp(2i\pi/5)$, $x^5 = e$.
  - zrcaljenje: $y =$ čez simetralo daljice $\overline{3,4}$; $y^2 = e$:

$$y = (25)(34)$$

- $G = \{e, x, x^2, x^3, x^4, y, yx, yx^2, yx^3, yx^4\}$ – res jih je 10.
- So to res vsi (oz. če obrnemo naokrog – to so res vsi, ker moramo poiskati med njimi še eno relacijo). To relacijo lahko najdemo z nekaj sreče:

$$xy = yx^4 = yx^{-1}.$$

  Dobili smo relacijo, ki obrne $x^{n_1}y^{n_2} \leftrightarrow y^{m_1}x^{m_2}$. Vse elemente lahko spravimo v obliko $y^k x^\ell$.

$$G = \langle x, y \mid x^5, y^2, xy = yx^{-1} \rangle$$

Opomba: [*K zgledu*] D_5 ni komutativna ($xy \neq yx$), ima pa ciklični podgrupi reda 2 in 5 – $\langle x \rangle \cong \mathbb{Z}_5$ in $\langle y \rangle \cong \mathbb{Z}_2$, ampak še vedno tako, da $D_5 \ncong \mathbb{Z}_2 \times \mathbb{Z}_5$.

Opomba: V prejšnjem zgledu smo spoznali še eno pomembno družino grup – to so diederske grupe D_n, z $2n$ elementi in predstavitvijo

$$D_n = \langle x, y \mid x^n, y^2, xy = yx^{n-1} \rangle = \langle x, y \mid x^n, x^2, xy = yx^{-1} \rangle.$$

Grupa D_n je grupa *izometrij* pravilnega n-kotnika (tj. bijekcij, ki n-kotnik slikajo samega nase).

Poglavje 3

Linearne upodobitve končnih grup

Omejili se bomo na $\mathbb{F} = \mathbb{C}$, čeprav lahko vse izreke in trditve zlahka posplošimo na splošen $\mathbb{F}$.

Definicija:

Naj bo V vektorski prostor nad $\mathbb{C}$.

- Če je G grupa, je *linearna upodobitev* G na V (nad $\mathbb{C}$) homomorfizem
$$G \to GL_{\mathbb{C}}(V)$$
- $\dim_{\mathbb{C}} V = n \in \mathbb{N}$ imenujemo *stopnja upodobitve*.

Zgled:

Upodobitve stopnje 1 so homomorfizmi

$$G \to GL_1(\mathbb{C}) = \big\{[a] \mid \det[a] = a \neq 0\big\}, \quad GL_1(\mathbb{C}) = \mathbb{C}\backslash\{0\} = \mathbb{C}^*.$$

Če je G končna, je slika upodobitve G v $\mathbb{C}^*$ tudi končna podgrupa, vsebovana v krožnici S^1 (ker imajo elementi v G končen red), vsak element je nek koren enote.

- G končna grupa – potem so vse (končno dimenzionalne) linearne upodobitve $G \to GL_{\mathbb{C}}(V)$, V končno dimenzionalen vektorski prostor nad $\mathbb{C}$.
- *Regularna upodobitev*, kjer za V vzamemo vektorski prostor z bazo G, delovanje G pa permutira bazne vektorje ($g \cdot v_h = v_{(gh)}$, kjer $g, h \in G$), na nek način vsebuje vse upodobitve.
- Glavna ideja je ta, da vsaki upodobitvi priredimo *karakter*, ki je funkcija $G \to \mathbb{C}$. Za začetek zelimo primerjati različne upodobitve.
- Naj bosta $G \to GL_{\mathbb{C}}(V)$ in $G \to GL_{\mathbb{C}}(W)$ dve linearni upodobitvi grupe G. *Homomorfizem upodobitev* (ekvivariantni homomorfizem) je linearna preslikava $T : V \to W$, ki komutira z delovanjem
$$\begin{aligned} &v \in V, \;\; g \in G \\ &T(gv) = gT(v) \end{aligned}$$
- Če je T linearni izomorfizem, ki je ekvivarienten, sta upodobitvi *izomorfni*. Takšne upodobitve enačimo.

- Če je V končno dimenzionalen vektorski prostor nad $\mathbb{C}$, potem $\exists n \in \mathbb{N}$ in linearen izomorfizem $T : \mathbb{C}^n \to V$. Ta T lahko naredimo za izomorfizem upodobitev tako, da s pogojem ekvivariantnosti definiramo delovanje G na $\mathbb{C}^n$ na osnovi delovanja na V: za $x \in \mathbb{C}^n$ in $g \in G$ mora veljati

$$T(gx) = g \cdot T(x),$$

T izomorfizem $\Rightarrow gx = T^{-1}\big(g \cdot T(x)\big)$:

$$\begin{array}{ccc} \mathbb{C}^n & \xrightarrow[\cong]{T} & V \\ \text{(da diagram komutira)} \quad \vdots & & \downarrow \quad \text{(delovanje } G\text{)} \\ \mathbb{C}^n & \xrightarrow[\cong]{T} & V \end{array}$$

g na $\mathbb{C}^n$ je kompozitum izomorfizmov $\Rightarrow$ je izomorfizem.

Zgled:

Vsaka upodobitev ranga 1 ($\dim_{\mathbb{C}} V = 1$) določa upodobitev abelacije grupe.

Rešitev: to je homomorfizem $\varphi : G \to GL_1(\mathbb{C}) = \mathbb{C}^*$. Grupa $\mathbb{C}^*$ je abelova. Vsak homomorfizem iz G v abelovo grupo vsebuje v jedru komutatorsko podgrupo $K = [G, G]$ in φ inducira homomorfizem $\bar{\varphi}$:

$$\bar{\varphi} : G/K \to \mathbb{C}^*, \quad p : G \to G/K,$$

kjer je $G/K = G/[G,G] \overset{\text{def.}}{=}$ abelacija, in velja $\varphi = \bar{\varphi} \circ p$.

Vsi homomorfizmi iz G pridejo iz $G/K \to \mathbb{C}^*$.

■

Zgled:

Poišči vse upodobitve ranga 1 za diederske grupe D_n.

Rešitev:

- Najprej se spomnimo predstavitve D_n:

$$D_n = \langle x, y \mid x^n, y^2, xy = yx^{-1} \rangle$$

- Iz tega hočemo abelacijo, tj. bomo vsilili še relacijo $xy = yx$. Isto predstavitev potem lahko zapišemo aditivno (namesto multiplikativno) – tako je komutativnost že vsebovana:

$$\mathrm{ab}(D_n) = \langle x, y \mid x^n, y^2, xy = yx^{-1}, xy = yx \rangle = [x, y \mid nx, 2y, x + y = y - x]$$

Zadnja relacija pomeni $2x = 0$, kar v kombinaciji z nx pomeni

$$\begin{aligned} n = \mathrm{sod} = 2m \Rightarrow 2mx = 0 = m\overbrace{(2x)}^{=0} \Rightarrow 2x = 0, \\ n = \mathrm{lih} = 2m + 1 \Rightarrow (2m+1)x = 0 = m\underbrace{(2x)}_{=0} + x = 0 \Rightarrow x = 0. \end{aligned}$$

- Vidimo za $n = 2m$ dobimo relacijo, ki pomeni, da sta x in y dvoštevni osi:

$$\mathrm{ab}(D_{2m}) = [x, y \mid 2x, 2y] \cong \mathbb{Z}_2 \times \mathbb{Z}_2,$$

v primeru, ko je $n =$ lih pa dobimo, da je x enoštevna os, tj.

$$\mathrm{ab}(D_{2m+1}) = [x, y \mid x, 2y] \cong \mathbb{Z}_1 \times \mathbb{Z}_2 \cong \mathbb{Z}_2.$$

- Po prejšnjem zgledu drži, da so vse upodobitve ranga 1 določene z abelacijo. Torej zadošča, da poiščemo upodobitve abelacije. Iščemo vse možne homomorfizme $\mathrm{ab}(D_n) \to \mathbb{C}^*$:
  - n je lih: $\mathrm{ab}(D_n) \cong \mathbb{Z}_2 = \{\pm 1\}$. Imamo dva taka homomorfizma:
    1. $\varphi(a) = 1$, trivialna upodobitev – vse slikamo v identiteto:
    $$\varphi(1) = 1,$$
    $$\varphi(-1) = 1.$$
    2. $\varphi(a) = a$, identična upodobitev – nič ne spremenimo:
    $$\varphi(1) = 1,$$
    $$\varphi(-1) = -1.$$
  - n je sod: $\mathrm{ab}(D_n) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 = \big\{(1,1), (1,-1), (-1,1), (-1,-1)\big\}$. Izberemo si dva generatorja: $x = (-1, 1)$ in $y = (1, -1)$, potem $xy = (-1, -1)$. Dovolj je povedati, kam se preslikata x in y. Sklepamo: x in y sta reda $2 \Rightarrow \varphi(x) = \pm 1$ in $\varphi(y) = \pm 1$ ter bo $\varphi(xy) = \pm 1 \Rightarrow$ imamo 4 možnosti (vedno gresta dva elementa v '-1', dva pa v 1. Identiteta mora vedno ostati identiteta.

Definicija:

Naj bo $G \to GL_{\mathbb{C}}(V)$ upodobitev in $W \subseteq V$ vektorski prostor. W je *G-invarianten*, če je $g \cdot W = \{gw \mid w \in W\}$ vsebovan v W $\forall g \in G$. V tem primeru lahko zgornjo upodobitev zožimo na W in dobimo *podupodobitev* $G \to GL_{\mathbb{C}}(W)$.

Opomba: Premisliti moramo, da delovanje z porodi izomorfizem (avtomorfizem?) $W \to W$ (zahtevali smo le $gW \subseteq W$). Ker je $g : V \to V$ linearni izomorfizem, je injektiven, zato je tudi zožitev injektivna. Upoštevamo $\dim(\ker) + \dim(\mathrm{im}) = \dim(\text{prostora})$ in delovanje je injektivno

$$\dim(\ker) = 0 \Rightarrow \dim(gW) = \dim W \Rightarrow gW = W.$$

Cilj: Razcepiti upodobitev na podupodobitve, dokler je to mogoče. Ker je $\dim_{\mathbb{C}}(V) < \infty$, se bo proces iskanja podupodobitev končal.

Definicija:

Upodobitev $G \to GL_{\mathbb{C}}(V)$ je *nerazcepna* (*ireducibilna*), če sta edini podupodobitvi $\{0\}$ in V.

Lema:

Naj bo $G \to GL_{\mathbb{C}}(V)$ upodobitev končne grupe G. Potem ima V G-invarianten skalarni produkt, tj.

$$\langle \bullet, \bullet \rangle_G : V \times V \to \mathbb{C},$$
$$\langle gv, gw \rangle_G = \langle v, w \rangle_G.$$

Dokaz:

- Naj bo $\langle \bullet, \bullet \rangle : V \times V \to \mathbb{C}$ poljubni skalarni produkt. Za invarianten skalarni produkt zgornjega povprečimo po delovanju grupe:

$$\langle v, w \rangle_G = \frac{1}{|G|} \sum_{g \in G} \langle gv, gw \rangle.$$

- Tole je res skalarni produkt (*potrditev zgornjega izraza*):

$$\langle v, w \rangle_G = \frac{1}{|G|} \sum_{g \in G} \overbrace{\langle gv, gw \rangle}^{\geq 0},$$

  - je res večje ali enako 0,
  - je enako 0 samo, kadar je $v = 0$.
  - linearnost in antisimetričnost sta enostavni.

- Preveriti moramo še, če je tak skalarni produkt (G-)invarianten: naj bo $h \in G$, $v, w \in V$.

$$\langle hv, hw \rangle_G = \frac{1}{|G|} \sum_{g \in G} \langle ghv, ghw \rangle.$$

  Ko g preteče G, tudi gh preteče cel G – označimo $g' = gh$:

$$\langle hv, hw \rangle_G = \frac{1}{|G|} \sum_{g' \in G} \langle g'v, g'w \rangle = \langle v, w \rangle_G. \blacksquare$$

- Ta skalarni produkt res obstaja, sami smo ga definirali in našli.

$\blacksquare$

Posledica:

Naj bo $G \to GL_{\mathbb{C}}(V)$ linearna upodobitev končne grupe. Izberimo nek G-invarianten skalarni produkt na V. Če elementu $g \in G$ pripadajoči linearni izomorfizem (avtomorfizem?) $g : V \to V$ predstavimo z matriko A glede na neko ortonormalno bazo (ONB) za V, potem je ta matrika *unitarna*, tj. $A^*A = I$ (oz. $A^* = A^{-1}$).

Opomba: V fiziki bi unitarnost označili kot $A^\dagger A = I$, vendar te notacije ne bomo uporabljali.

Dokaz: Element $g \in G$ je predstavljen z matriko A glede na neko ONB $(v_1, \ldots, v_n)$ za V. Pogoj invariantnosti skalarnega produkta da:

$$\langle A^*Av, w \rangle = \langle Av, Aw \rangle = \langle v, w \rangle, \quad \forall v, w \;\Rightarrow\; A^*A = I.$$

$\blacksquare$

Trditev:

Vsak invarianten podprostor ($gW \subseteq W$, $\forall g$) ima invarianten komplement. Naj bo $G \to GL_{\mathbb{C}}(V)$ upodobitev in $W \subseteq V$ invarianten podprostor. Potem $\exists$ komplementaren invarianten podprostor W' za W, tj. $V = W \oplus W'$. Za W' lahko vzamemo kar ortognonalni komplement $W^\perp$ glede na nek invarianten skalarni produkt.

Dokaz: Naj bo $\langle \bullet, \bullet \rangle$ nek G-invarianten skalarni produkt na V in $W^\perp = \{v \in V \mid \langle v, w \rangle = 0,\ \forall w \in W\}$. Trdimo, da je $W^\perp$ tudi G-invarianten:

- Naj bo $v \in W^\perp$, $g \in G$, potem za gv in $W \in W$ velja

$$\langle gv, w \rangle = \langle g^{-1}gv, g^{-1}w \rangle = \langle \overbrace{v}^{\in W^\perp}, \overbrace{g^{-1}w}^{\in W} \rangle = 0,$$

  od koder sledi $gv \in W^\perp$.

- Pokazati moramo še, da $W \oplus W^\perp = V$, kar smo pokazali že pri drugih kurzih tekom našega šolanja (Matematika I, II).

■

Posledica:

[*Komentar*] Če to ponavljamo, bomo V razcepili na nerazcepne podprostore.

Trditev:

Naj bo $G \to GL_{\mathbb{C}}(V)$ upodobitev končne grupe G na končno dimenzionalnem vektorskem prostoru V. Potem lahko V zapišemo kot direktno vsoto nerazcepnih upodobitev.

3.1 Konstrukcije upodobitev

Gre za konstrukcije vektorskih prostorov, na katere lahko „razširimo“ še upodobitve.

3.1.1 Direktna vsota

Direktna vsota: $G \to GL_{\mathbb{C}}(V)$ in $G \to GL_{\mathbb{C}}(W)$ sta dve upodobitvi. Tedaj je $G \to GL_{\mathbb{C}}(V \oplus W)$, s predpisom $g(v, w) = (gv, gw)$, spet upodobitev, dobljena iz direktne vsote. Če izberemo bazi za V in W ter glede na ti bazi delovanje $g \in G$ predstavimo z matrikama A na V in B na W, je delovanje g na $V \oplus W$ dano z direktno vsoto:

$$A \oplus B = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}.$$

3.1.2 Tenzorski produkt

$G \to GL_{\mathbb{C}}(V)$ in $G \to GL_{\mathbb{C}}(W)$ upodobitvi. Tenzorski produkt $V \otimes W$ je kvocient vektorskega prostora z bazo $V \times W$ po najmanjši ekvivalenčni relaciji, ki zadošča:

$$\left.\begin{array}{rl} (v_1 + v_2, w) & \sim (v_1, w) + (v_2, w) \\ (v, w_1 + w_2) & \sim (v, w_1) + (v, 2_2) \end{array}\right\} \text{aditivnost},$$
$$(\lambda v, w) \sim \lambda(v, w) \sim (v, \lambda w) \text{ homogenost},$$

$\forall v_i \in V$, $\forall w_i \in W$ in $\lambda \in \mathbb{C}$.

- To pomeni: vektorski prostor $V \times W$ je množica vseh končnih linearnih kombinacij $\sum_{i=1}^{n} \lambda_i (v_i, w_i)$, ekvivalenčna relacija pa dovoli, da operacije iz V in W prenesemo na $V \otimes W$.

- Element v $V \otimes W$, ki pripada paru (v, w) označimo $v \otimes w$ in imenujemo *elementarni tenzor*.
- Poljuben element v $V \otimes W$ je torej oblike

$$\sum_{i=1}^{n} \lambda_i v_i \otimes w_i$$

in pri tem velja

$$\lambda(v \otimes w) = (\lambda v \otimes w) = (v \otimes \lambda w) = \lambda v \otimes w.$$

Trditev:

Če je $v_1, \ldots, v_k$ baza za V in $w_1, \ldots, w_\ell$ baza za W, je $\left\{v_i \otimes w_j|_{j=1,\ldots,\ell}^{i=1,\ldots,k}\right\}$ baza za $V \otimes W$.

Dokaz:

- Za poljuben element v $V \otimes W$ imamo

$$\begin{aligned}
&\underbrace{\sum_m \lambda_m x_m \otimes y_m, \qquad \begin{matrix} x_m = & \sum_i a_{mi} v_i, \\ y_m = & \sum_j b_{mj} w_j \end{matrix}}_{} \\
&= \sum_m \lambda_m \Big(\sum_i a_{mi} v_i \Big) \otimes \Big(\sum_j b_{mj} w_j \Big) \\
&= \sum_{m,i,j} \lambda_m a_{mi} b_{mj} (v_i \otimes w_j).
\end{aligned}$$

- Še linearna neodvisnost: recimo

$$\begin{aligned}
\sum_{i,j} \lambda_{ij} v_i \otimes w_j &= 0 \\
\sum_j \Big(\sum_i \lambda_{ij} v_i \Big) \otimes w_j &= 0 \\
= \Big(\sum_i \lambda_{i1} v_i, w_1 \Big) + \ldots + \Big(\sum_i \lambda_{i\ell} v_i, w_\ell \Big) &= (0, 0).
\end{aligned}$$

(v prostoru z bazo $V \times W$) lahko seštevamo in množimo s skalarjem, osredotočimo se na drugo komponento. Ker so w_j baza, se to ne da, razen če so vsi koeficienti enaki 0. Ker so tudi v_i baza, morajo biti $\lambda_{ij} = 0$.

■

Primer: Poišči izražavo $\overbrace{\text{linearnih preslikav iz } V \cup W}^{L(V,W)}$ s tenzorskim produktom.

Rešitev: Poljuben $T \in L(V, W)$ vsakemu $v \in V$ priredi $T(v) \in W$, to lahko gledamo kot na takle elementi tenzorskega produkta:

$$T \in V^* \otimes W,$$

kjer je $V* = \big\{L(V, \mathbb{C})\big\}$ *dualni prostor* linearnih funkcionalov na V. Predpis pa deluje takole:

$$w \in W, \quad f \otimes w \in V^* \otimes W,$$

na poljuben $v \in V$ deluje s predpisom

$$\big(f \otimes w\big)(v) \equiv f(v) w \in W.$$

Da poljubno linearno preslikavo T zapišemo kot vsoto elementarnih tenzorjev, si pomagamo z bazami: $(v_1, \ldots, v_n)$ baza za V, tej priredimo dualno bazo $(f_1, \ldots, f_n)$ baza za V^* s predpisom $f_i(v_j) = \delta_{ij}$. Baza $(w_1, \ldots, w_m)$ za W da matriko $A = [a_{ij}]$ za T

$$T = \sum_{ij} a_{ji} f_i \otimes w_j. \blacksquare$$

Tvorimo lahko večkratne tenzorske produkte. Posebej zanimivi so tenzorji oblike

$$\underbrace{V \otimes V \otimes \ldots \otimes V}_{r\text{-krat } (kovariantni \text{ del})} \otimes \underbrace{V^* \otimes V^* \otimes \ldots \otimes V^*}_{s\text{-krat } (kontravariantni \text{ del})} = V^{r,s}.$$

Definicija:

Tenzorska algebra, prirejena prostoru V nad $\mathbb{C}$ je

$$T(V) = \bigoplus_{i=0}^{\infty} \underbrace{V^{\otimes_i}}_{V^i} = \underbrace{(\mathbb{C})}_{V^{\otimes_0}} \oplus \underbrace{(V)}_{V^{\otimes_1}} \oplus \underbrace{(V \otimes V)}_{V^{\otimes_2}} \oplus \underbrace{(V \otimes V \otimes V)}_{V^{\otimes_3}} \oplus \ldots$$

To je vektorski prostor, ki ga lahko opremimo še z množenjem vektorjev, analogno konstrukciji proste grupe oz. prostega produkta:

$$V^i \times V^j \to V^{i+j}$$
$$(v_1 \otimes \ldots \otimes v_i, w_1 \otimes \ldots \otimes w_j) \mapsto v_1 \otimes \ldots \otimes v_i \otimes w_1 \otimes \ldots \otimes w_j$$

3.1.3 Simetrični in alternirajoči produkt

Definicija:

Simetrični produkt dobimo iz tenzorskega tako, da zahtevamo komutatuvnost faktorjev:

$$v_1 \otimes v_2 \neq v_2 \otimes v_1, \text{ v splošnem.}$$

Na $V \otimes V$ vpeljemo najmanjšo ekvivalenčno relacijo, pri kateri velja

$$v_1 \otimes v_2 = v_2 \otimes v_1, \quad \forall v_1, v_2 \in V.$$

Kvocientu rečemo *simetrični produkt* in označimo s $S^2(V)$ (druga simetrična potenca).
Elemente pišemo kar z množenjem:

$$v_1 \otimes v_2 \in V \otimes V \rightsquigarrow v_1 v_2 \in S^2(V).$$

Podobno v višjih potencah. $S^n(V)$ je kvocient V^n, kjer zahtevamo, da faktorji komutirajo. Vsota vseh simetričnih potenc tvori *simetrično algebro*:

$$S(V) = \bigoplus_{i=0}^{\infty} S^i(V).$$

To lahko enačimo s polinomi v k spremenljivkah, kjer je $k = \dim_{\mathbb{C}} V$. Vsak simetrični tenzor reda n lahko zapišemo kot vsoto baznih $v_{i_1} v_{i_2} \ldots v_{i_n}$, kjer so v_{i_j} iz neke baze V. Če bazni element v_i enačimo s spremenljivko x_i, so zgornje monomi.

Definicija:

V *alternirajoči potenci* vektorskega prostora V zahtevamo, da je produkt tenzorjev antikomutativen, tj. dodamo relacijo

$$v_1 \otimes v_2 = -v_2 \otimes v_1.$$

Kvocient $V \otimes V$ pri tem poimenujemo druga *vnanja* (*exterior*) ali *alternirajoča* potenca V. Oznaka je $\Lambda^2(V)$, element pa je $v_1 \wedge v_2$.

Spet definiramo višje potence in algebro. *Vnanja algebra* nad V je

$$\Lambda(V) = \bigoplus_{i=0}^{\infty} \Lambda^i(V) = \bigoplus_{i=0}^{n} \Lambda^i(V),$$

kjer je $n = \dim_{\mathbb{C}} V$. Še več, $\dim_{\mathbb{C}} \Lambda(V) = 2^n$. To se zgodi, ker $v_1 \wedge v_1 = 0$, zato se bazni vektorji ne morejo ponavljati $\Rightarrow$

$$\dim_{\mathbb{C}} \Lambda^i(V) = \binom{n}{i}.$$

V vektorski prostor. Tenzorska algebra $T(V) = \bigoplus_i V^{\otimes_i} = \bigoplus_i V^i$. Če je $\{v_1, \ldots, v_n\}$ baza za V, je $\{v_{j_1} \otimes \ldots \otimes v_{j_n}\}$; $1 \leq j_i \leq n$ baza za $V^{\otimes_k}$. Tenzorski produkt je lineren v vsakem faktorju. Dve kvocientni konstrukciji:

- Simetrična algebra, kjer vsilimo komutativnost vektorskega prostora.
- Vnanja algebra, kjer vsilimo antikomutativnost, baza za $\Lambda^k(V)$ je $\{v_{j_1} \wedge \ldots \wedge v_{j_k}\}$, kjer je $1 \leq j_1 \leq j_2 \leq \ldots \leq j_k \leq n$.

Simetrično algebro in vnanjo algebro lahko gledamo tudi kot podmnožici v tenzorski algebri. Pomagamo si s projekcijama, ki vsakemu tenzorju priredita simetrični oz. alternirajoči tenzor.

- V $T^2(V) = V \otimes V$ imamo elementarne tenzorje $v \otimes w$ in takemu lahko priredimo simetrizirani tenzor

  $$v \cdot w = \frac{1}{2}(v \otimes w + w \otimes v),$$

  izraz na desni je simetričen na zamenjavo v in w. Podobno lahko dobimo anti-simetričeni tenzor

  $$v \wedge w = \frac{1}{2}(v \otimes w - w \otimes v).$$

- V splošnem definiramo projekciji
  - Simetrična projekcija, S^k:

    $$S^k : T^k(V) \to S^k(V),$$
    $$v_1 \otimes v_2 \otimes \ldots \otimes v_k \mapsto \frac{1}{k!} \sum_{\sigma \in S_k} v_{\sigma(1)} \otimes \ldots \otimes v_{\sigma(k)},$$

  - Alternirajoča projekcija, A^k:

    $$A^k : T^k(V) \to \Lambda^k(V),$$
    $$v_1 \otimes v_2 \otimes \ldots \otimes v_k \mapsto \frac{1}{k!} \sum_{\sigma \in S_k} \operatorname{sign}(\sigma) v_{\sigma(1)} \otimes \ldots \otimes v_{\sigma(k)}.$$

Če je $G \to GL_{\mathbb{C}}(V)$ linearna upodobitev grupe G, jo lahko razširimo do upodobitve po tenzorskih potencah z delovanjem po faktorjih

$$G \to GL_{\mathbb{C}}(V^{\otimes_k})$$
$$g(v_1 \otimes \ldots \otimes v_k) = gv_1 \otimes \ldots \otimes gv_k.$$

To inducira delovanje na simetrične in anti-simetrične potence.

Zgled:

Pokaži, da je $T^2(V)$ direktna vsota $S^2(V) \oplus \Lambda^2(V)$.

Rešitev:

- Hitro vidimo $v \otimes w = v \cdot w + v \wedge w$, torej je res vsota.
- Pokazati moramo še, da je $S^2(V) \cap \Lambda^2(V) = \{0\}$: če je $x \in S^2(V) \cap \Lambda^2(V)$, mora biti $x = 0$. Pa naj bo $x \in V \otimes V$, $\{v_1, \dots v_n\}$ baza za V, $\{v_i \otimes v_j\}$ baza za $V \otimes V$. Potem

$$\left.\begin{aligned} x = \sum_{i,j=1}^{n} \lambda_{ij} v_i \otimes v_j \quad & \overset{\text{sim.}}{=} \sum_{i,j=1}^{n} \lambda_{ij} v_j \otimes v_i \Rightarrow \lambda_{ij} = \lambda_{ji} \\ & \overset{\text{asim.}}{=} -\sum_{i,j=1}^{n} \lambda_{ij} v_j \otimes v_i \Rightarrow \lambda_{ij} = -\lambda_{ji} \end{aligned}\right\} \Rightarrow \lambda_{ij} = -\lambda_{ij} \Rightarrow \lambda_{ij} \equiv 0 \quad \forall i, j.$$

■

3.2 Karakterji upodobitev

Definicija:

Naj bo $\varphi : G \to GL_{\mathbb{C}}(V)$ linearna upodobitev grue G. Potem je *karakter* te upodobitve funkcija

$$\begin{aligned} \chi : G &\to \mathbb{C} \\ g &\mapsto \operatorname{tr}(g : V \to V) \\ \chi(g) &= \operatorname{tr}\big(\varphi(g)\big). \end{aligned}$$

Primer: Če je $\varphi : G \to GL_n(\mathbb{C}^*)$ upodobitev stopnje 1, potem je njen karakter kar φ.

Pomen: Pomagajo pri razumevanju nekomutativnih grup, ki imajo upodobitve višjih stopenj.

Trditev:

Naj bo G končna grupa in $\varphi : G \to GL_{\mathbb{C}}(V)$ upodobitev stopnje n ($n = \dim_{\mathbb{C}} V$). Potem velja

(1) $\chi(e) = n$,

(2) $\chi(g^{-1}) = \overline{\chi(g)}$ $\forall g \in G$.

(3) $\chi(hgh^{-1}) = \chi(g)$ $\forall g, h \in G$.

Dokaz:

(1) $\varphi(e) = \operatorname{tr}(I_{n\times n}) = n$, I je matrika identitete. ■

(3) Uporabimo cikličnost sledi:

$$\chi(hg^{-1}h) = \operatorname{tr}(hgh^{-1} : V \to V) = \operatorname{tr}(gh^{-1}h) = \operatorname{tr}(g : V \to V) = \chi(g). \blacksquare$$

(2) Naj bo $D : \chi(g^{-1}) = \overline{\chi(g)}$. Če V opremimo z G-invariantnim skalarnim produktom, vsakemu $g \in G$ pri upodobitvi glede na ONB pripada unitarna matrika A. To pomeni, da je $A^{-1} = A^* = \bar{A}^T$. Potem $\mathrm{tr}(A^{-1}) = \overline{\mathrm{tr}(A)}$. ■

Opomba:

- Lastnost **(3)** pomeni, da so karakterji kot funkcije $G \to \mathbb{C}$ konstantni na konjugiranostnih razredih elementov v G.
- Na G imamo avtomorfizem konjugiranja: $\forall h \in G$ imamo avtomorfizem $G \to G$, $g \to hgh^{-1}$.
- Množico $C_g = \{hgh^{-1} \mid h \in G\}$ imenujemo (*konjugiranostni*) *razred* elementa g, in ti razredi sestavljajo kompozicijo G (G je disjunktna unija različnih C_g, dva razreda C_{g_1} in C_{g_2} sta bodisi enaka, bodisi bodisi disjunktna).

Trditev:

Naj bosta $\varphi : G \to GL_{\mathbb{C}}(V)$ in $\psi : G \to GL_{\mathbb{C}}(W)$ upodobitvi, naj bosta χ_φ in χ_ψ njuna karakterja. Potem velja:

1. $\chi_{\varphi\oplus\psi} = \chi_\varphi + \chi_\psi$,
2. $\chi_{\varphi\otimes\psi} = \chi_\varphi \cdot \chi_\psi$.

Dokaz:

1. Če je $\varphi = A(g) : V \to V$ in $\psi(g) = B(g) : W \to W$, potem je $(\varphi \oplus \psi)(g) = A(g) \oplus B(g) : V \oplus W \to V \oplus W$ in ima sled
$$\mathrm{tr}(A \oplus B) = \mathrm{tr}\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix} = \mathrm{tr}(A) + \mathrm{tr}(B). \blacksquare$$

2. Naj bo $\{v_1, \ldots, v_n\}$ baza za V, $\{w_1, \ldots, w_n\}$ baza za W. Potem je baza $V \otimes W$ seveda
$$\{v_i \otimes w_j \mid i = 1, \ldots, n,\ j = 1, \ldots, m\}$$
kjer smo implicirali $\dim_{\mathbb{C}} V = n$ in $\dim_{\mathbb{C}} W = m$. Če element $A(g) : V \to V$ predstavlja matrično obliko za delovanje $\varphi(g)$, potem je $\mathrm{tr}\big(A(g)\big) = \sum_{i=1}^{n} A(g)_{ii}$ in podobno velja za $B(g)$. Po definiciji delovanja $g \in G$ na $V \otimes W$ je
$$\begin{aligned} g(v_i \otimes w_j) &= \big(A(g)v_i\big) \otimes \big(B(g)w_j\big) = \Big(\sum_k \big(A(g)\big)_{ki} v_k\Big) \otimes \Big(\sum_\ell \big(B(g)\big)_{\ell j} w_\ell\Big) \\ &= \sum_{k,\ell} \big(A(g)\big)_{ki} \big(B(g)\big)_{\ell j} v_k \otimes w_\ell \end{aligned}$$
Kako $g : V \otimes W \to V \otimes W$ priredimo matriko? Izračunamo g na baznih vektorjih $v_i \otimes w_j$ in te slike razvijemo po isti bazi. Diagonalni elementi ustrezajo komponentam $v_i \otimes w_j$ pri razvoju $g(v_i \otimes w_j)$ po bazi. Ta koeficient je $\big(A(g)\big)_{ii}\big(B(g)\big)_{jj}$,
$$\mathrm{tr}\big(A(g) \otimes B(g)\big) = \sum_{i,j} A_{ii}B_{jj} = \Big(\sum_i \big(A(g)\big)_{ii}\Big)\Big(\sum_j \big(B(g)\big)_{jj}\Big) = \mathrm{tr}(A) \cdot \mathrm{tr}(B) = \chi_\varphi(g) \cdot \chi_\psi(g). \blacksquare$$

Zgled:

$G \to GL_{\mathbb{C}}(V)$ upodobitev s karakterjem χ. Izrazi karakterja upodobitev $S^2(V)$ in $\Lambda^2(V)$ s tem χ.

Rešitev: Vemo, da je $\chi_{T^2(V)} = \chi(g)^2$ in da je $T^2(V) = S^2(V) \oplus \Lambda^2(V)$. Potem

$$\chi_{T^2(V)} = \chi_{S^2(V)} + \chi_{\Lambda^2(V)} = \chi^2.$$

Za $S^2(V) \subseteq T^2(V)$ dobimo, da so baza $S^2(V)$ torej tenzorji oblike $(v_i \otimes v_j + v_j \otimes v_i)$. Za vsak $g \in G$ računamo sled matrike, s katero g deluje na $S^2(V)$. Na V deluje g za matriko A:

$$Av_i = \sum_k a_{ki} v_k;\ 1 \leq i \leq j \leq n.$$

$$\begin{aligned} g(v_i \otimes v_j + v_j \otimes v_i) &= Av_i \otimes Av_j + Av_j \otimes Av_i \\ &= \Big(\sum_k a_{ki} v_k\Big) \otimes \Big(\sum_\ell a_{\ell j} v_\ell\Big) + \Big(\sum_\ell a_{\ell j} v_j\Big) \otimes \Big(\sum_k a_{ki} v_k\Big) \\ &= \sum_{k,\ell} a_{ki} a_{\ell j} (v_k \otimes v_\ell + v_\ell \otimes v_k) \\ &= \sum_{k \leq \ell} (v_k \otimes v_\ell + v_\ell \otimes v_k) \begin{cases} a_{ki}a_{\ell j} + a_{\ell i}a_{kj}; & k \neq \ell \\ a_{ki}a_{kj}; & k = \ell \end{cases} \end{aligned}$$

Prispevek k sledi je koeficient pri $v_i \otimes v_j + v_j \otimes v_i$ in je enak $(a_{ii}a_{jj} + a_{ji}a_{ij})$, če je $i \neq j$, če sta enaka, je pa $(a_{ii}a_{ii})$.

$$\begin{aligned} \operatorname{tr}(A) &= \sum_{i=1}^n a_{ii}^2 + \sum_{1 \leq i \leq j \leq n} (a_{ii}a_{jj} + a_{ij}a_{ji}) \\ &= \frac{1}{2}\sum_i a_{ii}^2 + \frac{1}{2}\sum_i a_{ii}^2 + \frac{1}{2}\sum_{i \neq j} (a_{ii}a_{jj} + a_{ji}a_{ij}) \\ &= \frac{1}{2}\sum_{i,j} (a_{ii}a_{jj} + a_{ij}a_{ji}) \\ &= \frac{1}{2}\big(\chi(g^2) + \chi(g)^2\big) \end{aligned}$$

Ugotovimo:

$$\begin{aligned} \chi_{S^2(V)} &= \frac{1}{2}\big(\chi(g)^2 + \chi(g^2)\big), \\ \chi_{\Lambda^2(V)} &= \frac{1}{2}\big(\chi(g)^2 - \chi(g^2)\big). \end{aligned}$$

Trditev:

Schurova lema: Naj bosta dani nerazcepni upodobitvi $\varphi : G \to GL_{\mathbb{C}}(V)$ in $\psi : G \to GL_{\mathbb{C}}(W)$ in naj bo $T : V \to W$ linearna G-ekvivariantna preslikava $(T(gv) = g(T(v)) = gT(v))$. Potem velja:

1. Če φ in ψ nista izomorfni, je $T = 0$.
2. Če je $\varphi = \psi$, potem je $T = \lambda I$, $\lambda \in \mathbb{C}$.

Dokaz: Nerazcepna upodobitev ima le dva invariantna podprostora: $\{0\}$ in cel prostor. Za G-ekvivariantno T, sta $\ker(T)$ in $\operatorname{im}(T)$ invariantna podprostora

$$\left.\begin{array}{rl} \text{za } v \in \ker(T) : T(v) & = 0 \\ \text{poljuben } g \in G : T(gv) & = gT(v) = 0 \end{array}\right\} gv \in \ker T,$$

$$\text{če je } w \in \operatorname{im} T : w = T(v) \text{za nek } v \in V \text{ za nek } v \in V$$
$$\text{za poljuben } g \in G : gw = gT(v) = T(gv) \in \operatorname{im} T$$

1. Če je $T = 0$ je v redu, sicer uporabimo zgornje: $\ker(T)$ je invarianten podprostor in $\ker(T) \neq 0$, to ni ves prostor $\Rightarrow \ker(T) = \{0\} \Rightarrow$ T injektivna. $T \neq 0 \Rightarrow \operatorname{im}(T) \neq 0$, invarianten podprostor, ni $\{0\} \Rightarrow \operatorname{im}(T) = W \Rightarrow T$ surjektivna in nijenktivna, tj. izomorfizem. T je linearen ekvivariantni izmorfizem $\Rightarrow$ je izomorfizem upodobitev.
2. $T : V \to V$ je linearna preslikava med $\mathbb{C}$ vektorskimi prostori. Potem ima neko lastno vrednost $\lambda \in \mathbb{C}$. Zato $\ker(T - \lambda I) \neq 0$, iz ekvivariantnosti T sledi tudi ekvivariantnost '$T - \lambda I$', zato je $\ker(T - \lambda I) = V \Rightarrow T - \lambda I = 0$.

■

Opomba: Če je $T : V \to W$ poljubna preslikava, lahko T „povprečimo“ tako, da dobimo G-ekvivariantno preslikavo $\hat{T} : V \to W$,

$$\hat{T}(v) \equiv \frac{1}{|G|} \sum_{g \in G} g^{-1} T(gv).$$

Res:

$$\begin{aligned}
\hat{T}(hv) &= \frac{1}{|G|} \sum_{g \in G} hh^{-1} g^{-1} T(ghv) \\
&= \frac{1}{|G|} \sum_{g \in G} h\big(gh^{-1}\big) T(ghv) = \frac{h}{|G|} \sum_{k \in G} k^{-1} T(kv) \\
&= h \cdot \hat{T}(v). \ \blacksquare
\end{aligned}$$

- Iz zgornje trditve sledi: če sta V in W neizomorfni upodobitvi, T poljuben, potem je $\hat{T} = 0$.
- Če je $T : V \to V$ poljuben, je $\hat{T} = \lambda I$ za nek $\lambda \in \mathbb{C}$.

Ali lahko iz tega določimo vrednost λ?

$$\hat{T} = \frac{1}{|G|} \sum_{g \in G} g^{-1} T g.$$

Poskusimo sled:

$$\operatorname{tr}(\hat{T}) = \frac{1}{|G|} \sum_{g \in G} \operatorname{tr}\left(g^{-1} T g\right) = \frac{1}{|G|} \sum_{g \in G} \operatorname{tr}(T) = \operatorname{tr}(T)$$
$$\operatorname{tr}(\hat{T}) = \operatorname{tr}(\lambda I) = \lambda n; \ n = \dim_{\mathbb{C}} V$$
$$\lambda = \frac{1}{n} \operatorname{tr}(T), \text{ oz. } \hat{T} = \frac{1}{n} \operatorname{tr}(T) I$$

Posledica:

Ortogonalnist matričnih koeficientov: Naj bosta $\varphi : G \to GL_{\mathbb{C}}(V)$ in $\psi : G \to GL_{\mathbb{C}}(W)$ nerazcepni upodobitvi. Izberimo ONB $\{v_1, \ldots, v_n\}$ in $\{w_1, \ldots, w_m\}$ za vektorka prostora V in W. Poljubnemu elementu $g \in G$ glede na ti bazi pripadata matriki $A^g = A \in GL_n(\mathbb{C})$ in $B^g = B \in GL_m(\mathbb{C})$.

1. Če V in W nista izomorfni upodobitvi je

$$\sum_{g \in G} A^g_{k\ell} \overline{B^g}_{ji} = 0, \ \forall i, j, k, \ell$$

2. Če $V = W$: (mislimo si lahko tudi $\varphi = \psi$)

$$\frac{1}{|G|}\sum_{g\in G} A^g_{k\ell}\overline{A^g}_{ji} = \frac{1}{n}\delta_{i\ell}\delta_{jk}.$$

Dokaz:

1. Naj bo $T : V \to W$ linerna preslikava, da

$$\begin{array}{ll} T : v_k & \mapsto w_j \\ T : v_i & \mapsto 0, \forall i \neq k \end{array} \quad \Bigg| \quad T = \begin{bmatrix} 0 & & & & & & \\ & \ddots & & & & & \\ & & 0 & & & & \\ & & & 1_{jk} & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{bmatrix} = E_{jk}$$

   Vemo: $\hat{T} = 0$ (po Schurovi lemi). Če $\hat{T}$ napišemo v matriki C glede na izbrani bazi so vsi njeni elementi enaki 0:

$$\begin{aligned} 0 = C_{i\ell} &= \frac{1}{|G|}\sum_{g\in G}\left(B^{-1}E_{jk}A\right)_{i\ell} \\ &= \frac{1}{|G|}\sum_{g\in G} B^{-1}_{ij}A_{k\ell} = \frac{1}{|G|}\sum_{g\in G}\overline{B}_{ji}A_{k\ell} = 0. \ \blacksquare \end{aligned}$$

2. Tu bomo kar takoj pričeli z enačno

$$\left.\begin{array}{ll} T : V & \to V \\ v_k & \mapsto v_j \end{array}\right\} \hat{T} = \frac{1}{n}\operatorname{tr}(T)\cdot I = \frac{1}{n}\delta_{kj}\cdot I.$$

$$C_{i\ell} = \frac{1}{n}\delta_{i\ell}\delta_{jk}, \text{ napišemo kot prej}$$

$$C_{i\ell} = \frac{1}{|G|}\sum_{g\in G}\left(A^{-1}E_{jk}A\right)_{i\ell} = \frac{1}{|G|}\sum_{g\in G}\overline{A}_{ji}A_{k\ell}. \ \blacksquare$$

Opomba: Zgornji matrični koeficienti A^g_{ij} sestavljajo funkcije $G \to \mathbb{C}$ in formule v posledici motivirajo definicijo skalarnih produktov na takih funkcijah.

Definicija:

Naj bosta $\alpha, \beta : G \to \mathbb{C}$. Njun skalarni produkt je

$$\langle \alpha, \beta \rangle = \frac{1}{|G|}\sum_{g\in G}\alpha(g)\overline{\beta(g)}.$$

Trditev:

Naj bosta χ in χ' neizomorna karakterja nerazcepnih upodobitev. Potem

1. $\|\chi\|^2 = \langle \chi, \chi \rangle = 1 = \|\chi'\|^2$,
2. $\langle \chi, \chi' \rangle = 0$.

Dokaz:

2. Naj bosta $\varphi : G \to GL_{\mathbb{C}}(V)$ in $\psi : G \to GL_{\mathbb{C}}(W)$ neizomorfni upodobitvi, s karakterjema χ_φ in χ_ψ. Izberimo dve ONB. Potem sta $\varphi(g)$ in $\psi(g)$ predstavljena z matrikama A^g in B^g,

$$\chi_\varphi(g) = \operatorname{tr}(A^g) = \sum_i A^g_{ii},$$
$$\chi_\psi(g) = \operatorname{tr}(B^g) = \sum_j B^g_{jj}.$$

Njun skalarni produkt je

$$\langle \chi_\varphi, \chi_\psi \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_\varphi(g) \overline{\chi_\psi(g)} = \frac{1}{|G|} \sum_{g \in G} \sum_i A^g_{ii} \sum_j \overline{B^g_{jj}}$$
$$= \frac{1}{|G|} \sum_{i,j} \Big(\underbrace{\sum_{g \in G} A^g_{ii} \overline{B^g_{jj}}}_{=0} \Big) = 0. \blacksquare$$

1. Normo $\|\chi\|^2$ lahko zapišemo kot

$$\langle \chi_\varphi, \chi_\psi \rangle = \sum_{i,j} \underbrace{\frac{1}{|G|} \sum_{g \in G} A^g_{ii} \overline{A^g_{jj}}}_{= \frac{1}{n} \delta_{ij} \delta_{ij}} = \frac{1}{n} \sum_{i=1}^{n} 1 = 1. \blacksquare$$

Povzetek: Karakterji nerazcepnih upodobitev tvorijo ortonormiran sistem funkcij $G \to \mathbb{C}$.

Opomba: Te funkcije ne tvorijo baze vseh funkcij $G \to \mathbb{C}$ (je končno razsežen vektorski prostor za končno grupo G) za splošno grupo G, saj so konstantne na konjugiranostnih razredih.

Vemo: V poljubna upodobitev $\Rightarrow$ V zapišemo kot (direktno) vsoto nerazcepnih

$$V = W_1 \oplus W_2 \oplus \ldots \oplus W_k,$$

kjer so W_i nerazcepne upodobitve (ne nujno neizomorfne).

Posledica:

Če je V poljubna upodobitev in W nerazcepna upodobitev, je

$$\langle \chi_V, \chi_W \rangle = \text{število } W_i \text{ v dekompoziciji } V \text{ na nerazcepne, ki so izomorfni } W$$

(tj. kolikokrat se W ponovi v V).

Dokaz: Če je $W_i \ncong W$, je $\langle \chi_{W_i}, \chi_W \rangle = 0$, če $W_i \cong W$ je $\langle \chi_{W_i}, \chi_W \rangle = 1$. V je razcepna upodobitev, tj. $V = W_1 \oplus \ldots \oplus W_k$, torej tudi $\chi_V = \chi_{W_1} + \ldots + \chi_{W_k}$. Od tu takoj vidimo

$$\langle \chi_V, \chi_W \rangle = \sum_{i=1}^{k} \langle \chi_{W_i}, \chi_W \rangle = \underbrace{\sum_{i \in I} \langle \chi_{W_i}, \chi_W \rangle}_{\neq 0} + \underbrace{\sum_{j \in J} \langle \chi_{W_j}, \chi_W \rangle}_{=0} = \sum_{i \in I} 1 + 0 = 1 \cdot |I|,$$

kjer smo v indeksni množici vzeli tiste indekse, za katere je skalarni produkt neničeln. Po prvotni ugotovitvi, je teh ravno toliko, kolikor je $W_i \ni: W_i \cong W$, tj. smo dokazali posledico.

■

Sklep: Karakter določa upodobitev do izomorfizma natančno. Vemo, da je karakterjev nerazcepnih upodobitev le končno mnogo (ker so ortogonalni v končno dimenzionalnem vektorskem prostoru), zato je tudi nerazcepnih neizomorfnih upodobitev le končno mnogo. Če so $W_1, \ldots, W_s$ vse neizomorfne nerazcepne upodobitve za G, je poljubna upodobitev V

$$V \cong \bigoplus_{i=1}^{s} m_i W_i,$$

kjer W_i nastopa m_i-krat, zato $m_i \geq 0$ in

$$m_i = \langle \chi_V, \chi_{W_i} \rangle.$$

To da kanonično dekompozicijo na sumande, posebej je

$$\chi_V = \sum_{i=1}^{s} m_i \chi_{W_i}$$

in

$$\langle \chi_V, \chi_V \rangle = \sum_{i=1}^{s} m_i^2.$$

Trditev:

Dekompozicija regularne upodobitve: Za končno G naj bo V_G vektorski prostor z bazo G, kjer bazne vektorje pišemo $\{V_g \mid g \in G\}$. Na V_G deluje G s permutacijami baznih vektorjev: $gv_h = v_{gh}$. Potem velja:

1. Če je χ_G karakter te upodobitve, je $\chi_G(e) = |G|$ in $\chi_G(g) = 0$, $\forall g \neq e$.
2. Če je W_i poljubna nerazcepna upodobitev s karakterjem χ_i, je $\langle \chi_G, \chi_i \rangle = n_i = \dim_{\mathbb{C}} W_i$.
3. Če so $W_1, \ldots, W_s$ vse nerazcepne upodobitve, je
$$\sum_{i=1}^{s} n_i^2 = |G|.$$
4. $\sum_{i=1}^{n} n_i \chi_i = 0$, $\forall g \neq e$.

Dokaz:

1. $\chi_G(e) = \dim V_G = |G|$ (očitno – ■). Ker je $gv_h = v_{gh} \neq v_h \forall h$, če $g \neq e$, ima matrika delovanja z g na diagonali same ničle (glede na bazo $\{v_g\}$) $\Rightarrow \chi(g) = \mathrm{tr} = 0$. ■

2. Samo račun:
$$\langle \chi_G, \chi_i \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_G(g) \overline{\chi_i(g)},$$
kar je enako nič $\forall g \neq e$, tj. vsota odpade in dobimo
$$\langle \chi_G, \chi_i \rangle = \frac{1}{|G|} \cdot |G| \underbrace{\overline{\chi_i(e)}}_{\dim W_i} = n_i.$$

3. Iz druge točke vemo, da je
$$V_G = \bigoplus_{i=1}^{s} n_i W_i$$
in zato je
$$\chi_G = \sum_{i=1}^{s} n_i \chi_i.$$
Za $g = e$ dobimo $\chi_G(e) = |G| = \sum_i n_i \chi_i(e) = \sum_i n_i^2$, saj $\chi_i(e) = n_i$.

4. $g \neq e$ naredimo analogno in dobimo $\chi_G(g) = 0 = \sum_i n_i \chi_i(g)$.

■

Zgled:

Poišči vse nerazcepne upodobitve grupe $C_2 = \{1, -1\}$.

Rešitev: Poznamo že dve 1D upodobitvi $C_2 \to \mathbb{C}^*$:

$\varphi_1 : 1$	$\mapsto 1$	$\varphi_2 : 1$	$\mapsto 1$
$\varphi_1 : -1$	$\mapsto 1$	$\varphi_2 : -1$	$\mapsto -1$
(trivialna)		(identična)	

Po tretji izjavi o dekompoziciji regularne upodobitve je $|C_2| = 2 = \sum_i n_i^2 \Rightarrow$ to sta edini nerazcepni upodobitvi. Poljubna upodobitev v $GL_{\mathbb{C}}(V)$, $\dim_{\mathbb{C}} V = n$, obstaja dekompozicija V na 1-D podprostore, na katere C_2 deluje s φ_1 ali φ_2. Obstaja taka baza z V, v kateri je matrika, ki pripada $\varphi(-1)$ enaka (je direktna vsota $\pm$ 1-D matrik)
$$\begin{bmatrix} \pm 1 & & & \\ & \pm 1 & & \\ & & \ddots & \\ & & & \pm 1 \end{bmatrix}$$

Zgled:

Poišči vse nerazcepne upodobitve za C_n!

Rešitev: Možne 1-D: $\varphi : C_n \to \mathbb{C}^* = GL_1(\mathbb{C})$. Dovolj je povedati, kam gre $\exp(2i\pi/n)$ (recimo, da ga izberemo za generator):
$$\varphi_\ell : e^{2i\pi/n} \mapsto e^{pi\pi\ell/n}, \quad \ell = 0, 1, \ldots, n-1$$

Ali so vse te upodobitve neizomorfne? Dve upodobitvi sta izomorfni, če obstaja ekvivariantni izomorfizem vektorskih prostorov, na katere delujeta. V tem primeru, bi bila to preslikava

$$T : \underset{\varphi_\ell}{\mathbb{C}} \to \underset{\varphi_m}{\mathbb{C}},$$

za katero bi veljalo $T \circ \varphi_\ell = \varphi_m \circ T$. Ampak v $\mathbb{C}^*$ je T lahko le množenje s skalarjem, tj.

$$\lambda\varphi_\ell = \varphi_m\lambda \Rightarrow \varphi_\ell = \varphi_m,$$

kar pomeni, da so izomorfne lahko le enake upodobitve. Kot prej lahko tudi sedaj preštejemo in ugotovimo, da so to res vse:

$$|C_n| = n = \sum_{\ell=0}^{n-1} 1^2 = n.$$

Nadalje želimo iz strukture grupe G določiti število *neizomorfnih nerazcepnih upodobitev* (NNU) grupe. Pomagamo si z lastnostmi karakterjev kot funkcije $G \to \mathbb{C}$. Vemo že, da so elementi karakterji konstantni na konjugiranostnih razredih elementov grupe G, saj $\chi(hgh^{-1}) = \chi(g), \forall g, h \in G$.

Definicija:

Naj bo $\mathcal{H}_G \equiv \{f : G \to \mathbb{C} \mid f(hgh^{-1}) = f(g)\ \forall g, h \in G\}$ prostor funkcij na G, ki so konstantne na konjugiranostnih razredih. Elemente $\mathcal{H}_G$ imenujemo *razredne funkcije*.

Vemo: Karakterji nerazcepnih upodobitev grupe G tvorijo ortonormiran sistem v $\mathcal{H}_G$.

Trditev:

Karakterji nerazcepnih upodobitev grupe G tvorijo ortonormirano *bazo* v $\mathcal{H}_G$. Posebej je število nerazcepnih upodobitev za G enako številu konjugiranostnih razredov v G.

Dokaz: Dovolj je pokazati, da je razredna funkcija, ki je ortogonalna na vse karakterje NNU ničelna.

Ideja: Uporabimo regularno upodobitev (ki vsebuje vse nerazcepne) in na tej konstruiramo linearno preslikavo, ki je ekvivariantna in določena z izbrano razredno funkcijo. Za to preslikavo uporabimo Schurovo lemo (to je vse kar imamo).

Naj bo f razredna funkcija, $\langle f, \chi_i \rangle = 0$ za vsako NNU W_i, s karakterjem χ_i. Naj bo V_G regularna upodobitev, tj. baza za $V_G = \{v_g \mid g \in G\}$ in delovanje je $hv_g = v_{hg}$. Definirajmo

$$F : V_G \to V_G;\ F = \sum_{g \in G} \overline{f(g)} g,$$

kjer smo povprečili po g, da dobimo ekvivariantnost. Res:

$$\begin{aligned}
\forall h \in G : F \circ h &= h \circ F \\
F \circ h &= \sum_{g \in G} \overline{f(g)} gh = \sum_{g' \in G} \overline{f(g'h^{-1})} (hh^{-1}) g' \\
&= h \sum_{g' \in G} \overline{f(g'h^{-1})} h^{-1} g' = h \sum_{g'' \in G} \overline{f(hg''h^{-1})} g'' \\
&= h \sum_{g \in G} \overline{f(g)} g = h \circ F.
\end{aligned}$$

$F : V_G \to V_G$ je invariantna linearna preslikava. Po Schurovi lemi je $F = \lambda I$, $\lambda \in \mathbb{C}$. Potem je

$$\operatorname{tr}(F) = \lambda |G|,$$

kjer pa sedaj upoštevamo linearnost sledi

$$\lambda |G| = \sum_{g \in G} \overline{f(g)} \operatorname{tr}(g),$$

sled pa lahko zapišemo kot $\chi_G(g) = \sum_{i=1}^{n} n_i \chi_i(g)$, kar je karakter regularne upodobitve. Ta je skalar, kar pomeni

$$\operatorname{tr}(F) = \sum_{i=1}^{n} n_i \overbrace{\sum_{g \in G} \overline{f(g)} \chi_i(g)}^{|G|\langle \chi \rangle = 0},$$

to pa pomeni, da je $\lambda = 0$ in s tem tudi $F = 0$. Zato je za v_e, $e \in G$ identiteta:

$$0 = F(e) = \sum_{g \in G} \overline{f(g)} g v_e = \sum_{g \in G} \overline{f(g)} v_g,$$

kjer v_g po definiciji sestavljajo bazo $\Rightarrow$ so linearno neodvisni, vsota pa je $0 \Rightarrow f(g) = 0 \ \forall g$.

■

Zgled:

Poišči vse nerazcepne upodobitve S_3.

Rešitev: Moč grupe je $|S_3| = 3! = 6$, tj. ima največ 6 NNU. Elementi so (izkaže se sicer $S_3 \cong D_3$, vendar samo za diedersko grupo reda 3, za druge to ne velja)

$$S_3 = \{e, (12), (13), (23), (123), (132)\} = \langle x, y \mid x^3, y^2, xy = yx^2 \rangle = \{e, x, x^2, y, yx, yx^2\}.$$

Imamo največ 6 NNU, ki so 1-D. Dve že poznamo, kot upodobitve abelacije:

$$\operatorname{ab}(S_3) = \operatorname{ab}(D_3) = [x, y \mid x = 0, 2y = 0] = [y \mid 2y = 0] \cong C_2,$$

torej sta to identična in trivialna upodobitev, kot pri C_2. Dimenzije preostalih lahko napovemo:

$$6 = 1 + 1 + \sum_{i=3}^{m} n_i^2 \Rightarrow \begin{cases} 4 \times \text{1-D upodobitve} \\ 1 \times \text{2-D upodobitev} \end{cases}$$

Sicer smo v resnici z abelacjo zajeli vse 1-D upodobitve, vendar lahko to preverimo še na en način: iz števila konjugiranostnih razredov lahko preberemo število NNU. Razredi so: $\{e\}$, $\{x, x^2\}$, $\{y, yx, yx^2\}$. Zaradi posledice ortogonalnosti v Schurovi lemi, je število konjugiranostnih razredov enako številu NNU. Torej imamo največ 3 NNU. Preostane nam torej še ena 2-D,

$$\varphi_3 : S_3 \mapsto GL_2(\mathbb{C}), \quad \dim_{\mathbb{C}} \mathbb{C}^2 = n_3 = 2.$$

Lahko izračunamo njen karakter (glej tabelo karakterjev 3.2

Tabela 3.1: Tabela karakterjev grupe S_3. χ_3 je neznan, zato manjka. Števila v oklepaju so moči elementov v posameznem razredu, saj dajo iste karakterje.

	$e(1)$	$x(2)$	$y(3)$	n_i
χ_1	1	1	1	1
χ_2	1	1	-1	1
χ_3	2	*	*	2
χ_{S_3}	6	0	0	6

Iz dimenzij NNU in po definiciji regularne upodobitve vemo $V_{S_3} = V_1 \oplus V_2 \oplus 2V_3$, tj $\chi_{S_3} = \chi_1 + \chi_2 + 2\chi_3$, od koder lahko izračunamo

$$\chi_3 = \frac{1}{2}\big(\chi_{S_3} - \chi_1 - \chi_2\big),$$

s čimer dopolnimo tabelo do

	$e(1)$	$x(2)$	$y(3)$	n_i
χ_3	2	-1	0	2

Poskusimo uganiti upodobitev φ_3, $\varphi_3 : S_3 \to GL_{\mathbb{C}}(\mathbb{C}^2) \subseteq \mathbb{C}^{2\times 2}$. Ker je $\varphi 3$ homomorfizem grup, ga je dovolj opisati na generatorjih, pri tem morajo biti za slike izpolnjene relacije v grupi

$$x^3 = e, \quad y^2 = e, \quad yx = x^2y,$$

iz karakterja poznamo še sledi teh matrik:

$$x : \chi_3(x) = -1 = \operatorname{tr}\big(\varphi_3(x)\big),$$
$$y : \chi_3(y) = 0 = \operatorname{tr}\big(\varphi_3(y)\big).$$

Uganemo:

$$\varphi_3(x) = \begin{bmatrix} e^{2i\pi/3} & 0 \\ 0 & e^{-2i\pi/3} \end{bmatrix}, \qquad \varphi_3(y) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Kontrola: $\operatorname{tr}(\varphi(x)) = 2\cos(2i\pi/3) = -1$. Preveriti moramo še tretjo relacijo:

$$\varphi_3(yx) = \varphi_3(y)\varphi_3(x) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} e^{2i\pi/3} & 0 \\ 0 & e^{-2i\pi/3} \end{bmatrix} = \begin{bmatrix} 0 & e^{-2i\pi/3} \\ e^{2i\pi/3} & 0 \end{bmatrix}$$
$$\varphi_3(x^2y) = \varphi(x^2)\varphi(y) = \begin{bmatrix} e^{-2i\pi/3} & 0 \\ 0 & e^{2i\pi/3} \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & e^{-2i\pi/3} \\ e^{2i\pi/3} & 0 \end{bmatrix},$$

torej je res $yx = x^2y$.

Zgled:

Naj bo V_G regularna upodobitev grupe G. Poišči bazo za trivialno podupodobitev. [*Trivialna upodobitev je tista, kjer g deluje kot identiteta:* $\varphi_1 : G \to \mathbb{C}^*,\ g \mapsto 1$.]

Rešitev: Ker je ta dimenzije 1, je njena večkratnost 1. Baza za $V_G = \{v_g \mid g \in G\}$. Poiskati moramo tak $0 \neq w = \sum_{g\in G} \lambda_g v_g$, da je $hw = w, \forall h \in G$. Vzamemo lahko

$$w = \frac{1}{|G|}\sum_{g\in G} g,$$

ta zadošča in je do skalarnega večkratnika edina možnost (ker je to 1-D podprostor).

3.3 Lastnosti upodobitev

Trditev:

Grupa G je abelova $\iff$ vse nerazcepne upodobitve so 1-D.

Dokaz: Naj bo m število nerazcepnih upodobitev za G,

$$|G| = \sum_{i=1}^{m} n_i^2;\ n_i = \dim W_i,$$

kjer je W_i i-ta NNU.

($\Rightarrow$) Če je $|G|$ abelova, je vsak element svoj konjugiranostni razred: $C_g = \{hgh^{-1}\} = \{ghh^{-1}\} = \{g\}$ $\Rightarrow$ število nerazcepnih upodobitev = število elementov (število konj. razredov) = $|G|$. Od tod sledi

$$|G| = \sum_{i=1}^{|G|} n_i^2 \Rightarrow n_1 = 1 \quad \forall i.$$

($\Leftarrow$) Če je $n_i = 1\ \forall i$, je $m = |G|$ in m = št. konj. razr. elementov v G, torej j $C_g = g\ \forall g \in G$, kar pomeni, da je $hgh^{-1} = g\ \forall g, h \in G$. Potem velja $hg = gh\ \forall g, h \in G \Rightarrow$ je abelova.

■

Posledica:

Naj bo $A \leq G$ abelova podgrupa. Potem je dimenzija vsake nerazcepne upodobitve grupe

$$G \leq [G : A] = \frac{|G|}{|A|}.$$

Dokaz: Naj bo V nerazcepna upodobitev za G, torej je dan $\varphi : G \to GL_{\mathbb{C}}(V)$. Če φ zožimo na A dobimo upodobitev $\varphi_A : A \to GL_{\mathbb{C}}(V)$. Sedaj je φ_A upodobitev abelove grupe, zato V razpade na nerazcepne 1-D upodobitve grupe A.

Naj bo $W \leq V$ nerazcepna podupodobitev za A, $\dim_{\mathbb{C}} W = 1$.

- Oglejmo si vektorski prostor $V' \leq V$, ki ga razpenjajo vektorji v, $GW = \{gw \mid g \in G, w \in W\}$. V' je torej množica vseh linearnih kombinacij

$$\sum_{g \in G} \lambda_g g w_0,$$

kjer je $w_0 \in W$ baza, $\lambda_g \in \mathbb{C}$. V' je G-invarianten podprostor, saj $\forall h \in G$ velja:

$$h \sum_{g \in G} \lambda_g g w_0 = \sum_{g \in G} \lambda_g hg w_0 = \ldots \sum_{g' \in G} \lambda_{h^{-1}g'} g' w_0 \in V.$$

Ker je V nerazcepna za G, je $V' = V$, saj ne more biti manjši.

- Preštejmo linearno neodvisne vektorje v $V' = V$: ker je $A \leq G$ indeksa $k = [G : A]$, je $G = g_1A \cup g_2A \cup \ldots \cup g_kA$ za neke $g_1, g_2, \ldots, g_k \in G$. Poljuben $g \in G$ je oblike $g = g_ia$, za nek i in nek $a \in A$. Ker je W 1-D upodobitev za A, je $aw_0 = \mu_a w_0 \ \forall a \in A$. Zato je $gw_0 = g_iaw_0 = \mu_a g_i w_0$, torej iz vektorjev gw_0 dobimo kot različne kvečjemu vektorje $g_1w_0, g_2w_0, \ldots, g_kw_0$: število linearnih neodvisnih vektorjev je torej največ $k = [G : A] \Rightarrow \dim V \leq k = [G : A]$.

■

Zgled:

Določi možne dimenzije upodobitev diederske grupe D_n.

Rešitev: $|D_n| = 2n$, $D_n = \langle x, y \mid x^n, y^2, yx = x^{n-1}y \rangle$.

- Ni abelova $\Rightarrow$ vsaj ena nerazcepna upodobitev dimenzije > 1.
- Po posledici je zgornja meja za dimenzijo NNU indeks abelove podgrupe v D_n. V D_n imamo ciklično podgrupo C_n moči n, njen indeks je očitno 2 ($[D_n : C_n] = 2n/n = 2$). Potem je največja dimenzija nerazcepne upodobitve 2.

Vaja: [*Domača naloga*] Napišimo vse te upodobitve.

Trditev:

Naj bosta $\varphi : G \to GL(V)$ in $\psi : H \to GL(W)$ upodobitvi za njun tenzorski produkt, definiran kot

$$\varphi \otimes \psi : G \times H \to GL(V \otimes W),$$
$$(\varphi \otimes \psi)(g, h)(v \otimes w) \mapsto \varphi(g)v \otimes \psi(h)w,$$

velja:

1. Če sta φ in ψ nerazcepni, je tudi $\varphi \otimes \psi$ nerazcepna upodobitev $G \times H$.
2. Vsaka NNU za $G \times H$ je zgornje oblike.

Dokaz:

1. Karakter upodobitve ima normo 1 $\iff$ upodobitev je nerazcepna (drugače je $\chi = \sum_{i=1}^n m_i\chi_i$; $\|\chi\|^2 = \sum_{i=1}^n m_i^2 \geq 1$).

$$\chi_\varphi : G \to \mathbb{C},$$
$$g \mapsto \operatorname{tr}(g : V \to V),$$

za χ_ψ velja podobno. Za njun tenzorski produkt pa lahko zapišemo

$$\chi_{\varphi\otimes\psi} : G \times H \to \mathbb{C},$$
$$g, h \mapsto \operatorname{tr}(g \otimes h : V \otimes W \to V \otimes W),$$

Če je $\{v_i\}$ baza za V in $\{w_j\}$ baza za W, je $\{v_i \otimes w_j\}$ baza za $V \otimes W$. Zanima nas koeficient pri $\{v_i \otimes w_j\}$ v $gv_i \otimes hw_j$, ta pa je produkt diagonalnih elementov $g_{ii}h_{jj}$,

$$\chi(g, h) = \sum_{i,j} g_{ii}h_{jj} = \sum_i g_{ii} \sum_j h_{jj} = \chi_\varphi(g) \cdot \chi_\psi(h),$$

$$\begin{aligned}\|\chi\|^2 &= \frac{1}{|G\times H|}\sum_{g,h}|\chi(g,h)|^2\\ &= \frac{1}{|G||H|}\sum_{g,h}|\chi_\varphi(g)|^2\cdot|\chi_\psi(h)|^2\\ &= \left(\frac{1}{|G|}\sum_g|\chi_\varphi(g)|^2\right)\left(\frac{1}{|H|}\sum_h|\chi_\psi(h)|^2\right) = \|\chi_\varphi\|^2\cdot\|\chi_\psi\|^2 = 1.\end{aligned}$$

Norma karakterja te upodobitve je 1, torej je ta upodobitev nerazcepna.

2. Vemo:

$$|G| = \sum_{i=1}^{k} n_i^2,\ n_i = \dim V_i,\ i = 1,\dots,k, \{V_i\} \text{ vse NNU za } G,$$
$$|H| = \sum_{j=1}^{\ell} m_j^2, \text{ analogno temu zgoraj.}$$

$V_i \otimes W_j$ so nerazcepne za $G\times H$ dimenzije $n_i \times m_j$,

$$\sum_{i,j}(n_i m_j)^2 = \sum_i n_i^2 \sum_j m_j^2 = |G|\cdot|H| = |G\times H|.$$

$\Rightarrow$ to so vse nerazcepne upodobitve.

■

Zgled:

Tenzorski produkt nerazcepnih upodobitev grupe G ni nujno nerazcepna upodobitev grupe G (nujno je nerazcepna za $G\times G$). $G \equiv G\times\{e\}$.

Rešitev: $G = S_3$, V_3 = 2-D nerazcepna upodobitev za S_3. $W = V_3\otimes V_3$, ki je upodobitev za diagonalno delovanje g, $g(v\otimes w) = gv\otimes gw$, $\dim W = 2\cdot 2 = 4$, edine nerazcepne upodobitve za S_3 pa so dimenzij 1 in 2. Glej tab. 3.2.

Tabela 3.2: Tabela karakterjev s χ_W vred, kjer $\chi_W = V_3\otimes V_3$, tj. $\chi_W = \chi_3^2$. Števila v oklepaju so moči posameznih konj. razr.

	e (1)	x (2)	y (3)
χ_1	1	1	1
χ_2	1	1	-1
χ_3	2	-1	0
χ_W	4	1	0

Dekompozicijo W na nerazcepne dobimo z $\langle\chi_W,\chi\rangle$ za $i = 1,2,3$.

$$\langle\chi_W,\chi_1\rangle = \frac{1}{6}(1\cdot 4 + 2\cdot 1 + 3\cdot 0) = \frac{1}{6}\begin{bmatrix}4 & 1 & 0\end{bmatrix}\begin{bmatrix}1 & & \\ & 2 & \\ & & 3\end{bmatrix}\begin{bmatrix}1\\1\\1\end{bmatrix} = 1.$$

To je navaden skalarni produkt, normiran s številom elementov grupe, matrika vmes je pa matrika

uteži, ki so enake moči posameznih konj. razredov, saj se vsak karakter tolikokrat ponovi.

$$\langle \chi_W, \chi_2 \rangle = \frac{1}{6} \begin{bmatrix} 4 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & & \\ & 2 & \\ & & 3 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ -1 \end{bmatrix} = 1,$$

$$\langle \chi_W, \chi_3 \rangle = \frac{1}{6} \begin{bmatrix} 4 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & & \\ & 2 & \\ & & 3 \end{bmatrix} \begin{bmatrix} 2 \\ -1 \\ 0 \end{bmatrix} = 1.$$

Vidimo $W = V_3 \otimes V_3 = V_1 \oplus V_2 \oplus V_3$.

Zgled:

Naj bo G abelova grupa in naj bo $\hat{G}$ množica karakterjev NNU za G. Pokaži, da je $\hat{G}$ grupa za množenje funkcij po točkah in določi $|\hat{G}|$ (komentar: $\hat{G}$ je dualna grupa).

Rešitev:

- G ima $|G|$ 1-D upodobitev,
- produkt karakterjev je karakter tenzorskega produkta,
- tenzorski produkt 1-D prostorov je spet 1-D prostor.
- $\chi_1,\ \chi_2 \in \hat{G} \Rightarrow \chi_1\chi_2 \in \hat{G}$. Vemo: $\chi_1 \cdot \chi_2$ je karakter tenzorskega produkta upodobitev V_1 in V_2. Ker sta V_1 in V_2 nerazcepni z dimenzijo 1, je tudi $V_1 \otimes V_2$ 1-D vektorski prostor in zato je upodobitev nerazcepna.
- Identiteta: $\chi = 1$ je karakter trivialne upodobitve.
- Inverz: za dani $\chi \in \hat{G}$ ke inverz z operacijo množenja po točkah funkcija

$$\psi : \chi(g)\psi(g) = 1 \quad \forall g \in G$$
$$\psi(g) = \frac{1}{\chi(g)} \quad \forall g \in G.$$

  Ali je to dobro definirano? Da, $\chi(g) = \operatorname{tr}\left(\lambda \in GL(\mathbb{C}) = \mathbb{C}^*\right) \neq 0$. Je ψ res karakter upodobitve? Velja še več, slika φ oz. χ leži na enotski krožnici

$$\frac{1}{\chi(g)} \text{ spet na enotski krožnici,}$$

  $1/\chi(g) = \overline{\chi(g)} = \psi(g)$. Za upodobitev vzamemo $\overline{\varphi}$ Če je $\varphi : G \to \mathbb{C}^*$ homomorfizem, je tudi $\overline{\varphi} : G \to \mathbb{C}^*$, ker je

$$\overline{\varphi(gh)} = \overline{\varphi(g)\varphi(h)} = \overline{\varphi(g)} \cdot \overline{\varphi(h)}.$$

  Moč $|\hat{G}| = |G|$, ker je ravno toliko 1-D NNU.

Zgled:

Pokaži $\hat{G} \cong G$ (to je res samo za končne grupe).