# 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, 6. oktober 2013

# Del I

# Grupe

# Poglavje 1

# Osnovni pojmi

**Definicija:**

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

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

Z drugimi besedami, imamo množico, ki je zaprta za neko asociativno operacijo $\mu$. 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 $\mu$ 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 $f(a,b) = f(a)f(b)\ \forall a, b \in G$. 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 $\infty$ (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 $\alpha$ 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 $\alpha$ 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 $\alpha$ ponavadi zapišemo kot $\alpha = (i_1, i_2, i_3, \ldots, i_r)$.

**Definicija:**

Dva cikla, $\alpha$ in $\beta$ sta *disjunktna*, če premakneta različne elemente – tj. $\beta$ lahko premika kvečjemu elemente, ki jih $\alpha$ fiksira in obratno.

**Vaja:**

1. $|S_n| = n!$ (očitno).
2. Če je $\alpha$ $r$-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 $k < r$, $\alpha^k$ 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 $\alpha$ $r$-cikel in $d \in \mathbb{N}$. Potem $\alpha^d$ 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 $\big(\text{tj. } (d, r) = 1\big)$, $\alpha^d$ določa isto grupo moči $r$ in je zato $r$-cikel. V primeru, da $k \neq 1$ trdimo, da $\alpha$ razpade na produkt $k$ disjunktnih ciklov.

   ■

**Opomba:** disjunktni permutaciji (cikla) komutirata.

**Trditev:**

Vsaka permutacija v $S_n \backslash \{e\}$ je produkt disjunktnih ciklov dolžine $\geq 2$. 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:** $\alpha$ permutacija $\Rightarrow$ predznak $\alpha$ ... $\text{sign}(\alpha) \in \{\pm 1\}$.

**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:** $\alpha$ $r$-cikel, $\beta$ $p$-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 $\varphi$ porodi

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

**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 na $\mathbb{F}$ 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 $\varphi$ 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 $X$:

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

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

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

**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 $H$.