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, 5. 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:

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

■

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. $(\mathbb{Z}_n, +_{\text{mod } n}) \nleq (\mathbb{Z}, +)$, 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, $a \in G$.
  - <u>*Leva translacija* za a</u> je $L_a : G \to G,\ g \mapsto ag$.
  - <u>*Desna translacija* za a</u> 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:

  $$\exp(x + y) = \exp(x) \cdot \exp(y) \quad ■$$
- 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 $a \in G$. Najmanjše 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.

$\blacksquare$

Posledica:

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

$$\mathrm{red}(a) \;\Big|\; |G|$$

(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 $e, a, \ldots, a^{k-1}$.

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

$\blacksquare$

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

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

$\blacksquare$

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: $aH = Hb$. želiko $b = a$. 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

$$aH \cdot bH \stackrel{\text{def}}{=} abH.$$

- 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 tolde zaporedje grup in homomorfizmov:

$$p : a \longrightarrow aH,$$
$$\{e\} \to H \xhookrightarrow{i} G \xrightarrow{p} {}^{G}/_{H} \to \{e\}.$$

Tu se moramo spomniti

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

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 $aH = H \iff a \in H$.