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:

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

■

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. $(\mathbb{Z}_n, +_{\text{mod } n}) \not\leq (\mathbb{Z}, +)$, 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: