Cyklická podgrupa

$H = \{ \ldots x^{-2}, x^{-1}, 1, x, x^2, \ldots \}$

- toto je najmenšia podgrupa obsahujúca x

(v skutočnosti sa tu môžu členy opakovať)

→ ak sú všetky rôzne – nekonečná cyklická grupa
(vymyslieť na $\mathbb{Z}$)

→ ak sa niečo opakuje, t.j. $x^n = x^m$, potom $(m>n)$
$x^{n-m} = 1$. → teda existuje nejaká (nenulová) mocnina x rovná 1-ke.

Lemma Množina S celých čísel, pre ktoré $x^n = 1$ je podgrupou $\mathbb{Z}^+$.

Dôkaz Ak $x^m = 1$ a $x^n = 1$, potom aj $x^{m+n} = x^m x^n = 1$, teda $m+n \in S$ pre $m, n \in S$. podobne $x^0 = 1$ a ak $x^n = 1$ aj $x^{-n} = 1$, lebo $1 = x^0 = x^{n+(-n)} = x^n x^{-n} = x^{-n}$)

---

ako dôsledok máme $S = m\mathbb{Z}$

- m sa nazýva rád prvku x

Potom H pozostáva z $H = \{1, x, \ldots, x^{m-1}\}$ navzájom rôznych

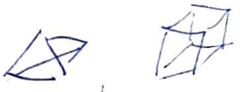
Cyklická grupa rádu m

Príklad $\begin{bmatrix}1&1\\-1&0\end{bmatrix}$ má rád 6 v $GL_2(\mathbb{R})$

cvič.

na druhej strane $\begin{bmatrix}1&1\\0&1\end{bmatrix}$ má nekonečný rád.

$$\begin{bmatrix}1&1\\0&1\end{bmatrix}^n = \begin{bmatrix}1&n\\0&1\end{bmatrix}.$$

(Cvič: Symetrie △, □,  (akcie na stenách, diagonálach, vrcholoch))

Def Rád grupy G je počet jej prvkov:

$$|G| = \text{počet prvkov } G.$$

Podobne sa dá hovoriť o grupe G generovanej nejakou podmnožinou U. ~~Hovoríme, že U generuje~~
Ide o najmenšiu podgrupu obsahujúcu U
- obsahuje reťazce prvkov z U a ich inverzov.

Špeciálne: množina U generuje G ak sa každý z prvkov G dá vyjadriť ako takýto súčin.

Príklady. V S_3 sme mali $U=\{\rho,\tau\}$, ($\rho^3=1$, $\tau^2=1$, $\rho\tau=\tau\rho^2$)

- v $GL_n(\mathbb{R})$ — ERO
- Kleinova grupa $\begin{bmatrix}\pm1&\\&\pm1\end{bmatrix}$ — nie je cyklická (prečo?)

Príklad: ~~K~~ quaterniónová grupa $H = \{\pm 1, \pm i, \pm j, \pm k\}$

Dá sa reprezentovať pomocou:

$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $i = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$, $j = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, $k = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$

~~generovaná~~ i, j a vzťahmi

platí $i^4 = 1$, $i^2 = j^2$, $ji = i^3 j$

(cvič. ukážať, že to je iné ako D_8)

Izomorfizmy

Ak G a G' sú dve grupy, chceli by sme povedať, že ~~sú~~ sú izomorfné, ak všetky vlastnosti grupovej štruktúry G platia aj v G' a naopak.

Príklad: Matice $\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \in GL_2(\mathbb{R})$ vzhľadom na násobenie

$$\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x+y \\ 0 & 1 \end{bmatrix}$$

sa správajú rovnako ako čísla $x, y \in \mathbb{R}$ vzhľadom na sčítanie.

Teda chceme nejaké párovanie medzi prvkami G a G'

$$\begin{matrix} a & & b \\ \updownarrow & & \updownarrow \\ a' & & b' \end{matrix}$$

také, aby súčin $a \cdot b \longleftrightarrow a'b'$.

Zápis: $\varphi : G \to G'$ bijektívne zobrazenie spĺňajúce $\varphi(ab) = \varphi(a)\varphi(b)$.

Def. grup. izomorfizmu

Vlastnosti: identita $1 \in G$ zodpovedá $\varepsilon' \in G'$

(nulový vektor → nul. vektor)

$\forall a: 1a = a \implies \varphi(1)\varphi(a) = \varphi(a)$

Rády prvkov sú rovnaké

$a^r = 1 \implies \varphi(a^r) = \varphi(a)^r = 1$

$\varphi(1) = 1'$

Príklady

$\mathbb{Z}^+$ a $C = \{\dots, a^{-2}, a^{-1}, 1, a, a^2, \dots\}$

$\varphi(n) = a^n$ / $\varphi(m+n) = \varphi(m)\varphi(n)$

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

$G = \{1, x, x^2, \dots, x^{n-1}\}$, $G' = \{1, y, y^2, \dots, y^{n-1}\}$

dve cyklické grupy rádu n.

Preto má zmysel hovoriť o triede izomorfných grúp.

($\mathbb{Z}/3\mathbb{Z}$)

Napr. $\exists$ iba jedna rádu 3

dve rádu 4

päť rádu 12 (a aj 8?) (tri komutatívne, dve nekomutatívne)

Špeciálny typ izomorfizmu — automorfizmus.

$1 \rightsquigarrow 1 = y^0$

$x \rightsquigarrow x^2 = y$

$x^2 \rightsquigarrow x = y^2$

keďže rád x^2 je tiež 3, máme dva rôzne popisy cyklickej grupy.

Konjugácia

Definujme zobrazenie

$$\varphi(x) = bxb^{-1}$$

Je to automorfizmus: – zachováva násobenie

$$\varphi(xy) = bxyb^{-1} = (bxb^{-1})(byb^{-1}) = \varphi(x)\varphi(y).$$

– je to bijekcia, lebo k φ existuje inverzné zobrazenie (konjugácia b^{-1})

$$b^{-1}(bxb^{-1})b \rightsquigarrow x.$$

V prípade abelovskej (komutatívnej) grupy je konjugácia identita: $a \mapsto b^{-1}ab^{-1} = abb^{-1} = a.$

ale v prípade nekomutatívnych grúp sú aspoň niektoré konjugácie netriviálne

(cvič – ak je konj. vzhľadom na $\forall a = id$ $\Rightarrow$ kom.)

Vlast.

konjugovaný prvok má rovnaký rád

Význam: označiac $a' = bab^{-1}$

máme: $ba = a'b$

t.j. zodpovedá zmene a, ak prejdeme b-čkom na opačnú stranu.

Homomorfizmy

Def Pre grupy G, G' je zobrazenie spĺňajúce
$\varphi(ab) = \varphi(a)\varphi(b)$ homomorfizmus.

(Nepožadujeme bijekciu) na rozdiel od izomorfizmu)

Príklady:
- Determinant: $\det: GL_n(\mathbb{R}) \to \mathbb{R}^\times$
- Znamienko permutácie $\mathrm{sign}: S_n \to \{\pm 1\}$
- zobrazenie $\varphi: \mathbb{Z}^+ \to G$ dané $\varphi(n) = a^n$ pre fixný prvok $a \in G$.
- vloženie $i: \cancel{H} \to G$ $i(x) = x$.

Tvrdenie Grupový homomorfizmus zobrazuje identitu na identitu a inverz. na inverz.

D: $1 = 1 \cdot 1$ v G, teda $\varphi(1) = \varphi(1)\varphi(1) = \varphi(1)\varphi(1)$.
pre $1_{G'}$ platí: $1_{G'} \cdot \varphi(1) = \varphi(1)$, teda
máme $1_{G'}\varphi(1) = \varphi(1)\varphi(1)$ + krátenie sprava.

Tiež $\varphi(a^{-1})\varphi(a) = \varphi(a^{-1}a) = \varphi(1) = 1_{G'}$, podobne
$\varphi(a)\varphi(a^{-1}) = 1_{G'}$. t.j. $\varphi(a)^{-1} = \varphi(a^{-1})$. ∎

---

každý homomorfizmus definuje dve dôležité podgrupy
- obraz a jadro.

11

$\mathrm{Im}(\varphi) = \{ x \in G' \mid x = \varphi(a) \text{ pre } a \in G \}$,

resp. $\varphi(G)$ (v príkladoch ..)

$\ker \varphi = \{ a \in G \mid \varphi(a) = 1 \}$,

čo sa dá popísať aj ako vzor 1 ~~v~~ $\varphi^{-1}(1)$.

Im

Obe sú podgrupy, lebo $\varphi(ab) = \varphi(a)\varphi(b)$ (súčin prvkov z obrazu patrí do obrazu

+ $\varphi(a)^{-1} = \varphi(a^{-1})$, $\varphi(1) = 1$ + inverz + neut.

---

ker

$a, b \in \ker$ $\varphi(a) = \varphi(b) = 1$. Potom aj $\varphi(ab) = \varphi(a)\varphi(b) = 1 \cdot 1 = 1$

V príkladoch:

① Jadro homomorfizmu determinantu sú matice s $\det = 1$

– špeciálna lineárna grupa

$SL_n(\mathbb{R}) = \{ \text{reálne } n \times n \text{ matice } A \mid \det A = 1 \}$

② jadro znamienkového homomorfizmu: – alternujúca grupa

$A_n = \{ \text{párne permutácie} \}$.

Súvis s konjugáciou:

$a \in \ker \varphi$, $b \in G$ potom aj $bab^{-1} \in \ker \varphi$:

$$\varphi(bab^{-1}) = \varphi(b)\varphi(a)\varphi(b^{-1}) = \varphi(b)\, 1\, \varphi(b^{-1}) = 1.$$

t.j. $bab^{-1} \in \ker \varphi$ tiež.

Def Podgrupa N grupy G sa nazýva <u>normálnou</u> podgrupou ak je uzavretá na konjugáciu:

t.j. $a \in N \Rightarrow bab^{-1} \in N$ pre $\forall b \in G$

Ako sme videli:

<u>Tvrdenie</u> Jadro homomorfizmu je normálna podgrupa.

$\boxed{\text{sem } 12.3.18}$

<u>Príklady:</u> $SL_n(\mathbb{R})$ a A_n sú normálne podgrupy.

- v abelovskej grupe je každá podgrupa normálne
  $bab^{-1} = a$, t.j. $a \in N \Rightarrow a \in N$.

<u>Netriv. príklad</u> T – horné trojuholníkové regulárne (invertibilné) matice nie sú.

$$A = \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}, \quad B = \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}, \text{ dá } \quad BAB^{-1} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \notin T.$$

<u>Centrum grupy</u> $Z(G)$ je množina prvkov grupy, ktoré komutujú s každým prvkom G:

$$Z = \{ z \in G \mid zx = xz \text{ pre } \forall x \in G \}.$$

Fakt: centrum každej grupy je normálna podgrupa

$$(gzg^{-1} = zgg^{-1} = z)$$

<u>Príklad</u> pre $GL_n(\mathbb{R})$ sú centrom matice tvaru cI (skalárne matice).