Ako sme videli:

Tvrdenie Jadro homomorfizmu je normálna podgrupa.

Sem 12.3.18

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

- v abelovskej grupe je každá podgrupa normálna

$bab^{-1} = a$, t.j. $a \in N \Rightarrow a \in N$.

Netriv. príklad T – horné trojuholníkové regulárne (invertibilné) matice nie sú.

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

$\cancel{A}$

T.

Centrum grupy $Z(G)$ 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

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

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

Relácie ekvivalencie a rozklady

- jeden zo základných matematických postupov je začať s množinou S, vyhlásiť niektoré prvky v S za rovnocenné (vzhľadom na nejaké pravidlo) a vytvoriť tzv. faktorovú množinu.

Napríklad: Celé čísla $\mathbb{Z}$ vieme rozdeliť na dve triedy – párne $\underline{0}$ a nepárne $\underline{1}$.

: Alebo trojuholníky v rovine – vzhľadom na podobnosť (jeden vieme dostať z druhého posunutím, otočením, reflexiou)

Čo je v pozadí: Majme množinu S, potom Rozklad $\mathcal{R}$ bude rozdelenie S na neprázdne časti s navzájom nulovým prienikom.

Napr. $\{0\}, \{1,4\}, \{2,3\}$, tvoria rozklad $\{0,1,2,3,4\}$.

Formálne:
- $\mathcal{R} = \{ S_i \mid S_i \text{ je podmnožina } S \}$
- $\bigcup S_i = S$
- $S_i \neq \emptyset$
- $S_i \cap S_j = \emptyset$.

Na druhej strane, máme relácia ekvivalencie:

i) reflexívna $a \sim a$ $\forall a \in S$

ii) symetrická $a \sim b \Rightarrow b \sim a$ $\forall a, b \in S$

iii) tranzitívna $a \sim b, b \sim c \Rightarrow a \sim c$ $\forall a, b, c \in S$.

Fajny rozkladu a ekvivalencie sú totožné – pre reláciu $\sim$ vieme vytvoriť triedy ekvivalencie:

$$C_a = \underline{a} = \{ b \in S : a \sim b \}.$$

(viac na prednáške M. Sleziaka (?))

asi nie

Potom faktorová množina $S/_\sim = \underline{S}$ – množina tried ekvivalencie.

Príklad $\mathbb{Z}/_\sim = \{\underline{0}, \underline{1}\}$, kde $\underline{0} = \{\dots, -4, -2, 0, 2, 4, \dots\}$

$\underline{1} = \{\dots, -3, -1, 1, 3, \dots\}$.

Potom máme prirodzené (surjektívne) priradenie

$$S \longrightarrow \underline{S}$$
$$a \longmapsto \underline{a}$$

Na rozklad sa dá pozerať dvoma spôsobmi

- rozdelí prvky S na neprázdne kôpky – prvky $\underline{S}$ a potom zobrazenie $S \to \underline{S}$ priradí prvku meno jeho kôpky.
- iný pohľad: $a \sim b$ v S interpretovať ako rovnosť obrazov $\underline{a} = \underline{b}$ v $\underline{S}$.

To vedie k takémuto všeobecnému menu:

Ak $\varphi: S \to T$ je ľubovoľné zobrazenie, definujme

$a \sim b$ ak $\varphi(a) = \varphi(b)$. (relácia ekvivalencie určená zobrazením)

Definícia vzor. $t \in T$ je:

$$\varphi^{-1}(t) = \{s \in S : \varphi(s) = t\}.$$

Ľahko preskúmame, že je trieda ekvivalencie.

Zaujímajú nás neprázdne vzory, teda t by malo patriť do $\operatorname{Im}\varphi$.

Potom $\bar{S} \approx \operatorname{Im}\varphi$, máme bijektívne zobrazenie $\bar{\varphi}: \bar{S} \to \operatorname{Im}\varphi$

$$\bar{s} \longmapsto \varphi(s)$$

Vybavení toudo teórion ~~tróčo~~ sa môžeme vrátiť
do grupovým homomorfizmom.

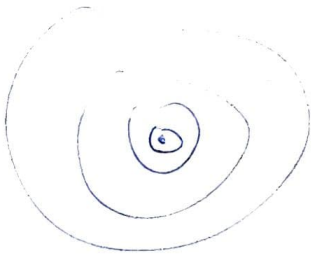
Nech $\varphi: G \to G'$ je homomorfizmus. Analyzujme
reláciu ekvivalencie danú φ. (označíme $\equiv$ – bude sa nazývať kongruencia)

$a \equiv b$ práve vtedy, keď $\varphi(a) = \varphi(b)$.

Príklady $\varphi: \mathbb{C}^\times \to \mathbb{R}^\times$ daná $\varphi(a) = |a|$.

→ (je to homomorfizmus, lebo $|z_1 z_2| = |z_1||z_2|$)

Čo sú triedy ekvivalencie? (prvky s rovnakou abs. hodnotou)



← Kružnice so stredom v nule, parametrizované sú polomerom – kl. $\mathbb{R}$ číslom.

($\operatorname{Im}\varphi = \mathbb{R}^+$)

Skúsme nájsť nejaké iné vhodné popisy tried ekvivalencie:

Tvrdenie Nech $\varphi: G \to G'$ je grupový homomorfizmus s jadrom N, a, b sú prvky G. Potom $\varphi(a) = \varphi(b) \Leftrightarrow b = an$ pre nejaké $n \in N$, resp. $a^{-1}b \in N$

Dôkaz Nech $\varphi(a) = \varphi(b)$, potom $\varphi(a)^{-1}\varphi(b) = 1$. φ je homomorfizmus $\varphi(a^{-1}b) = 1 \Leftrightarrow a^{-1}b \in N$, teda $a^{-1}b = n$ pre nejaké $n \in N$. Z toho $b = an$. ∎

~~Def~~ Množina prvkov tvaru an sa označuje aN a nazýva sa (ľavá) trieda ~~rozkladu~~ G podľa N (G modulo N)

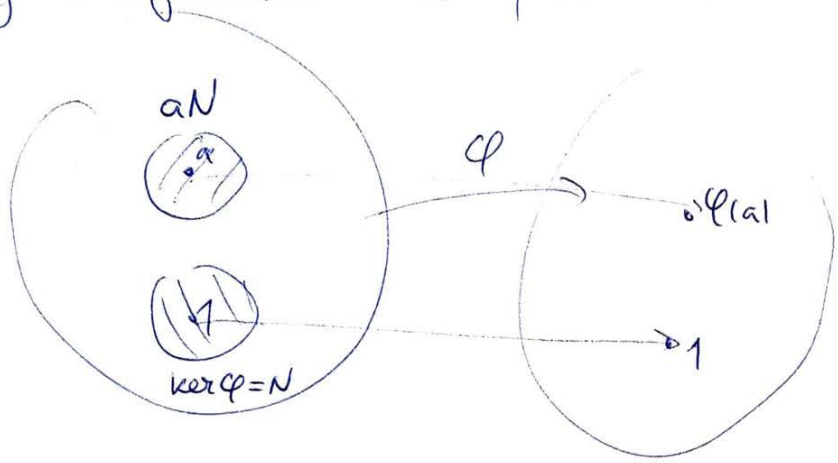
(po anglicky coset)

$$aN = \{g \in G : g = an \text{ pre nejaké } n \in N\}.$$

→ ~~Podľa~~ kongruencie

aN teda ~~obsahuje~~ obsahuje všetky prvky kongruentné a, t.j. triedy kongruencie sú práve (ľavé) triedy G podľa N.

Príklad



Špeciálny prípad $\ker(\varphi) = \{1\}$ – vtedy je jadro triviálne a homomorfizmus je injektívny – lebo všetky triedy majú 1 prvok.

(T.j. injektívnosť stačí overiť pre 1, $\varphi^{-1}(1) = \ker(\varphi)$)

Triedy G podľa H

(asi sem 19.3.2018 zdržanie kvôli praxi)

rozklad G podľa H sa dá urobiť pre ľubovoľnú podgrupu: ľavá trieda

$$aH = \{ah : h \in H\}$$

pravá trieda

$$Ha = \{ha : h \in H\}$$

Špeciálne: ak $a = 1$, $1H = H = H1$ – teda podgrupa je jedna z tried.

K tomuto rozkladu máme reláciu kongruencie:

pravá $a \equiv b \iff b = ah$ pre $h \in H$

$[a^{-1}b \in H]$

(ľavá) $(b = ha) \to ba^{-1} \in H$]

Overme, že to je naozaj relácia ekvivalencie:

i) reflexívnosť $a \equiv a$ lebo $a = a \cdot e$

ii) symetria $a \equiv b \Rightarrow b \equiv a$

$b = ah$ $a = bh'$ (zvolíť $h' = h^{-1}$)

iii) tranzitívnosť $a \equiv b$, $b \equiv c$ $\to$ $c = bh' = (ah)h' = a(hh')$

$b = ah$ $c = bh'$ ↑ patrí do H.

príklad $S_3 = \{1, \rho, \rho^2, \tau, \rho\tau, \rho^2\tau\}$ $\rho\tau$ je tiež symetria, generuje podgrupu rádu 2

$\{1, \rho\tau\} = H = \rho\tau H$ / $\{\rho, \rho^2\tau\} = \rho H = \rho^2 \tau H$ / $\{\rho^2, \tau\} = \rho^2 H = \tau H$.

počet ľavých tried ~~podgr~~ G podľa H sa nazýva **indexom** H v G., značí sa $[G : H]$.

Treba si všimnúť, že každá z tried má rovnako veľa prvkov: zobrazenie $a \longmapsto ah$

$H \longrightarrow aH$ je bijektívne.

preto dostaneme $|G| = |H| \cdot [G : H]$.

Dôsledok (Lagrangeova veta)

Nech G je konečná grupa, H je podgrupa G, potom rád H delí rád G.

Dôsledok Rád prvku a delí rád G.

Dôsledok Nech má grupa G p prvkov, kde p je prvočíslo. Nech $a \in G$, $a \neq 1$. Potom G je cyklická grupa $\{1, a, \dots, a^{p-1}\}$.

D: keďže $a \neq 1$, rád $(a) > 1$. Lenže rád (a) | delí $p = |G|$. a jediné také je p. Preto a má rád p a $\{1, a, \dots, a^{p-1}\}$ je celé G.

Niečo podobné dostaneme, keď sa pozrieme na homomorfizmus $\varphi : G \to G'$.

videli sme, že triedy podľa $\ker \varphi$ zodpovedajú prvkom v obraze $\operatorname{Im} \varphi$. Teda index $\ker \varphi$ v G je $|\operatorname{Im} \varphi|$:

$$[G : \ker \varphi] = |\operatorname{Im} \varphi|$$

Dôsledok Pre $\varphi : G \to G'$ homomorfizmus konečných grúp máme $|G| = |\ker \varphi| \cdot |\operatorname{Im} \varphi|$.

Potom $|\ker \varphi| \mid |G|$ ← zo vzorca

a $|\operatorname{Im} \varphi| \mid |G|$ aj $|G'|$)

← lebo $|\operatorname{Im} \varphi|$ je podgrupa G'.

---

prečo pravé / ľavé triedy?

pre S_3 a $\{1, \rho\tau\}$ máme pravé triedy:

$$\{1, \rho\tau\} = H = H\rho\tau, \quad \{\rho, \tau\} = H\rho = H\tau, \quad \{\rho^2, \rho^2\tau\} = H\rho^2 = H\rho\tau$$

→ čiže sú iné ako ľavé triedy.

Ale pre normálnu podgrupu dostaneme lomdrí triedy

Tvrdenie Podgrupa H grupy G je normálna vtedy a len vtedy ak každá ľavá trieda G podľa H je aj pravá trieda a podľa H. $\rightarrow$ t.j. $aH = Ha$. pre $\forall a \in G$.

Dôkaz Nech H je normálna. Potom pre $\forall h \in H$ a $\forall a \in G$ máme $ah = (aha^{-1})a$ ale z definície normálnosti $k = aha^{-1} \in H$, t.j. $ah = ka$.

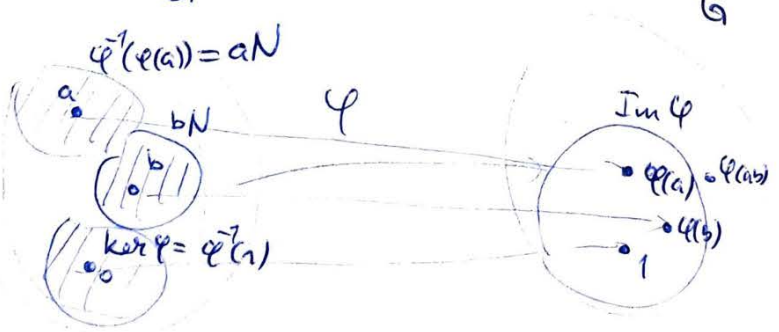
Preto $aH \subset Ha$. podobne dostaneme $Ha \subset aH$

(dalo by sa argumentovať počtom prvkov, ale chceme to všeobecne, aj pre nekonečné grupy)

Obrátene, nech H nie je normálna. Potom $\exists a \in G$, $h \in H$ také, že $aha^{-1} \notin H$. Preto $ah \in aH$ ale $ah \notin Ha$.

Keďže $a \in aH \cap Ha$, teda majú neprázdny prienik, ale sa nerovnajú – rozklady na pravé a ľavé triedy sú rôzne.

Ako príklad normálnych grúp sme videli jadrá homomorfizmov.



t.j. $aN \rightarrow \varphi(a)$
$bN \rightarrow \varphi(b)$
$abN \rightarrow \varphi(ab)$

keďže ak $x \in aN$, $y \in bN$ $\Rightarrow$ $\varphi(xy) = \varphi(x)\cdot\varphi(y) = ab$

t.j. $xy \in abN$

mohli by sme písať $(aN)(bN) \overset{?}{=} (abN)$?

~~• mohli by sme tieto predpoklady~~, že vidíme, že grupová štruktúra G' (presnejšie $\mathrm{Im}\,\varphi$) sa v istom zmysle prejavuje aj v G.

→

Povedali sme si, že rozklad na ľavé triedy vieme spraviť pre ľubovoľnú $H < G$.

Otázka: Za akých podmienok dostaneme $aH\,bH = abH$?

(zvoľme $b = a^{-1}$.)

potom $aH\,a^{-1}H \overset{?}{=} aa^{-1}H$?

→ ak zoberieme $e \in H$, tak platí $a e a^{-1} e = aa^{-1} e$ ✓

ale pre $h \in H$, $e \in H$ by sme mali mať $a h a^{-1} e = k \in H$.

Čiže vidíme podmienku toho, aby H bola normálna.

Pre normálnu podgrupu N grupy G označujeme množinu jej (ľavých/pravých) tried ako G/N (= $\bar{G}$)

Ďalej máme zobrazenie

$$\pi : G \longrightarrow G/N \quad (\bar{G})$$
$$a \longmapsto aN \quad (\bar{a}).$$

Veta S operáciou násobenia tried je $\bar{G} = G/N$ grupa a zobrazenie π je homomorfizmus s jadrom N.

Rád grupy G/N je index $[G:N]$ podgrupy N v G.

(Dôsledok: každá normálna podgrupa G je jadrom nejakého homomorfizmu)

Dôkaz overme, že π súhlasí s grupovou operáciou.

$$aN \cdot bN = a(bN)N = abN$$
$$\pi(a) \cdot \pi(b) \qquad\qquad \pi(ab)$$

Potom do jadra patria tie $a \in G$: $\pi(a) = \pi(1) = N$, t.j. $a \in N$.

Overíť, že operácia na $\overline{G}$ je naozaj grupa

asociatívnosť, 1. prvok, inverzy:

asoc $\overline{a_1}(\overline{a_2}\,\overline{a_3}) = \varphi(a_1)(\varphi(a_2)\varphi(a_3)) = \varphi(a_1 \overset{\varphi}{(}a_2 a_3)) = \varphi(a_1(a_2 a_3)) =$

$= \varphi((a_1 a_2)a_3) = \varphi(a_1 a_2)\varphi(a_3) = (\varphi(a_1)\varphi(a_2))\varphi(a_3) = (\overline{a_1}\overline{a_2})\overline{a_3}$

jedn. $\overline{1}\,\overline{a} = \varphi(1)\varphi(a) = \varphi(1a) = \varphi(a) = \varphi(a1) = \varphi(a)\varphi(1)$

$= \overline{a}\,\overline{1}$

inv. cvič.

Veta (o faktorovom izomorfizme)

Nech $\varphi : G \to G'$ je surjektívny grupový homomorfizmus a $N = \ker\varphi$. Potom G/N je izomorfné s G', cez $\overline{\varphi} : \underset{\text{t.j. } aN}{\overline{a}} \longmapsto \varphi(a)$, t.j. $\overline{\varphi}(\overline{a}) = \varphi(a)$.

Variant. $G/\ker(\varphi) \cong \mathrm{Im}(\varphi)$.

Dôkaz: Triedy rozkladu G/N (aN) sú dané jednak ako $a = aN$, ale aj pomocou obrazov $\varphi(a)$. Teda máme bijekciu z G/N do $\mathrm{Im}(\varphi)$.

Z konštrukcie, táto bijekcia je kompatibilná s násobením:

$$\overline{\varphi}(\overline{a}\,\overline{b}) = \varphi(ab) = \varphi(a)\varphi(b) = \overline{\varphi}(\overline{a})\,\overline{\varphi}(\overline{b}). \quad \checkmark$$