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

$\longrightarrow$

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 $aH a^{-1}H \stackrel{?}{=} aa^{-1}H$?

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

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

Čiže vidíme podmienku toho, aby H bola normálna.

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

Potom máme zobrazenie

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

<u>Veta</u> S operáciou násobenia tried je $\overline{G} = G/N$ 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)

<u>Dôkaz</u> overme, že π súhlasí s grupovou operáciou.

$$\underset{\pi(a)\cdot\pi(b)}{aN \cdot bN} = a(bN)N = \underset{\pi(ab)}{abN}$$

Potom do jadra ~~platia~~ patria tie $a \in G$: $\pi(a) = \underset{\overset{\shortparallel}{\overline{1}}}{\pi(1)} = N$

t.j. $a \in N$.

Overiť, že operácia na $\overline{G}$ ~~je~~ naozaj ~~g~~ spĺňa asociatívnosť, 1-prvok, inverzy:

asoc $\quad \overline{a_1}(\overline{a_2}\,\overline{a_3}) = \varphi(a_1)\big(\varphi(a_2)\varphi(a_3)\big) = \varphi\big(a_1 \overset{\varphi}{(}a_2a_3)\big) = \varphi(a_1(a_2a_3)) =$

$= \varphi((a_1a_2)a_3) = \varphi(a_1a_2)\,\varphi(a_3) = \big(\varphi(a_1)\varphi(a_2)\big)\varphi(a_3) = (\overline{a_1}\,\overline{a_2})\overline{a_3}$

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

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

$\overline{\varphi} : \underset{\underset{aN}{\shortparallel}}{\overline{a}} \longmapsto \varphi(a)$, 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:

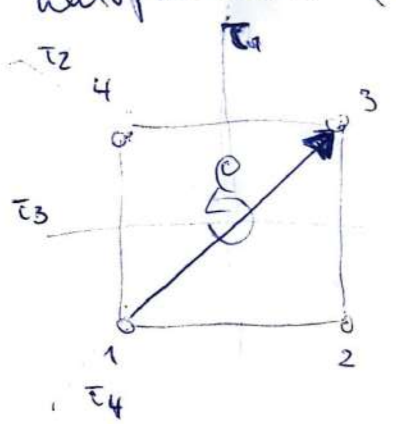
$\overline{\varphi}(\overline{a}\,\overline{b}) = \varphi(ab) = \varphi(a)\varphi(b) = \overline{\varphi}(\overline{a})\overline{\varphi}(\overline{b})$. ✓

Akcie grúp, orbity, ...

Príklady grúp, s ktorými sme začali, boli grupy symetrií geometrických objektov. Napr. S_3 a D_8. (trojuholník, štvorec).

Okrem celého objektu (máme (troj., štvorec) máme v ňom aj jeho časti – vrcholy, uhlopriečky.

Takže sa môžeme pozrieť, čo robí (napr. D_8) s uhlopriečkami: (orient. uhlopriečkami) 4-prvková, dvojprvková



$id(\overrightarrow{13}) = \overrightarrow{13}$	$\overline{13}$	$\tau_1 =$
$\rho(\overrightarrow{13}) = \overrightarrow{24}$	$\overline{24}$	$\rho\tau = \tau\rho^3$
$\rho^2(\overrightarrow{13}) = \overrightarrow{31}$	$\overline{13}$	$\rho^2\tau = \tau\rho^2$
$\rho^3(\overrightarrow{13}) = \overrightarrow{42}$	$\overline{24}$	$\rho^3\tau = \tau\rho$

$$\rho\tau = \tau\rho^3$$

1	2	3	4	1	2	3	4
↓	↓	↓	↓	↓	↓	↓	↓
2	3	4	1	2	1	4	3
↓	↓	↓	↓	ρ^3 ↓	↓	↓	↓
1	4	3	2	1	4	3	2

Akcia (operácia) grupy G na množine S je pravidlo, ako majú prvky $g \in G$ násobiť s prvkami $s \in S$, t.j.
(výsledok gs)
operácia skladania $G \times S \longrightarrow S$,
spravidla zapisovaná ako (ľavé) násobenie

$$g, s \longmapsto gs$$

Chceme tieto axiómy.

a) $1 \cdot s = s$ pre $\forall s \in S$ (1 je identita v G)

b) asociatívnosť $(gg')s = g(g's)$ pre $g, g' \in G$ a $s \in S$.

Množina S s akciou G sa nazýva G-množina.

Príklady:

- G – grupa (afinných transformácií roviny
  – má akciu na bodoch roviny
  (ale aj úsečkách, trojuholníkoch, ...)

- $G = \mathbb{Z}_2$ s $r^2 = 1$ má akciu na komplexných číslach: $r z \overset{r}{\longmapsto} \bar{z}$
  $1 z \longmapsto z$

- grupa matíc $GL_n(\mathbb{R})$ má akciu na vektoroch z $\mathbb{R}^n$. Ax, pravidlo $A(Bx) = (AB)x$ ...

Pre fixný prvok $g \in G$ je ~~akcia~~ násobenie g zobrazenie

$$m_g : S \longrightarrow S$$
$$m_g(s) = g(s)$$

Toto je permutácia S, lebo zložením $m_g, m_{g^{-1}}$

dostávame $m_{e} = id$, teda obe zobrazenia

$m_{g^{-1}} m_g = m_g m_{g^{-1}}$

$m_g, m_{g^{-1}}$ sú bijektívne.

Významné objekty, ktoré sa pri akcii G na S dajú študovať sú tzv. <u>orbity</u>.

Pre prvok $s \in S$ je jeho <u>orbita</u>:

$$O_s = \{ s' \in S : s' = gs \text{ pre nejaké } g \in G \},$$

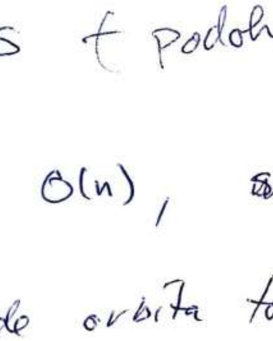
- ide o podmnožinu S + orbitu môžeme značiť aj ako Gs + podobne ako ľavú triedu v podgrupe.

---

príklad $G = O(n)$, $S = \mathbb{R}^n$, $s = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$

→ čo bude orbita tohto vektora?

(n-1)-rozmerná sféra...



Orbity opäť môžeme chápať ako triedu ekvivalencie

$s \sim s' \Leftrightarrow s' = gs$ pre nejaké $g \in G$. (dôkaz, že + je rel. ekv. → cvič.)

- ? tak dostaneme rozklad S na orbity.

uvedomiť si: Grupa G má akciu na každej orbite zvlášť.

- t.j. každý prvok $g \in G$ permutuje prvky z danej orbity, ale neprevádza ich z jednej na druhú.

(pri
Ak S má iba jednu orbitu, hovoríme, že akcia G je
na S <u>tranzitívna</u> – t.j. každý prvok z S sa dá
nejakým násobením dostať do ľubovoľného iného $s' \in S$.

<u>Stabilizátor</u> prvku $s \in S$ bude podgrupa G_s prvkov G,
ktoré nechávajú s namieste.

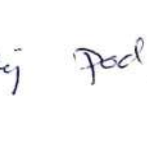
$$G_s = \{g \in G : gs = s\},$$

Je to naozaj podgrupa: ~~$xs = ys \iff s = x^{-1}ys$~~
+ uzavreté na operáciu $(g_1(g_2)s) = g_1(g_2 s) = g_1 s = s$
+ inverzy.

Potom máme popis:

$$xs = ys \iff s = x^{-1}ys \iff x^{-1}y \in G_s$$

t.j. dva prvky x, y majú rovnakú akciu na s, ak ich "rozdiel" $x^{-1}y$ je $stab_s$.

Príklad  D_8 – dihedrálna grupa – grupa symetrií štvorca
má (~~pri pohľade na vrch~~ akciu na vrcholoch.
-> stabilizátor 1 je dvojprvkový –
– orbita je celé S (všetky 4)

+ spraviť príklad?

(improvizácia... $\rho^4 = 1, \tau^2 = 1, \tau\rho = \rho^3\tau$)

Tvrdenie: Nech S je má na sebe G-akciu (je to G-množina) a s je prvkom S. Nech H je stabilizátor s a O_s je orbita s.
Potom máme prirodzené bijektívne zobrazenie

$$G/H \xrightarrow{\varphi} O_s$$

dané

$$aH \longmapsto as.$$

D: Táto definícia je dobrá: ~~Nahliadnime, že zobrazenie φ je kompatibilné s grupovou operáciou:~~ $b \in aH \Leftrightarrow b = ah,\ h \in H$

teda $bs = a\underbrace{hs}_{} = as$, teda naozaj každej triede $aH \in G/H$ priradí prvok tvaru $as \in O_s$.

Je to surjektívne: $O_s = \{gs \mid g \in G\}$, teda zjavne $\varphi(gH) = gs$, každý prvok z orbity trafíme.

Injektívnosť: Nech aH a bH sa zobrazia na ten istý prvok, t.j. $as = bs$. Lenže potom $a^{-1}bs = s$, teda $a^{-1}b \in H = G_s$ (stabilizátor s), teda a, b patria do tej istej triedy.

Navyše: φ je kompatibilné s grupovou operáciou (násobenie zľava):

$$\varphi(abH) = a\,\varphi(bH)$$

$$\begin{array}{ccc} \| & & \| \\ abs & & a(bs) \end{array}$$

20) Tvrdenie: Nech S je G-množina, s' je prvok orbity s ($s' = as$). Potom:

a) prvky $g \in G$ také, že $gs = s'$ tvoria ľavú triedu

$$aG_s = \{ g \in G \mid g = ah \text{ pre } h \in G_s \}$$

b) stabilizátor s' je konjugovaná podgrupa stabilizátora s

$$G_{s'} = aG_s a^{-1} = \{ g \in G \mid g = aha^{-1} \text{ pre } h \in G_s \}$$

Dôkaz: a) je jasné

b) Nech $gs' = s'$, potom $s = a^{-1}s' = \cancel{a^{-1}bs'} = s$ (t.j. $b \in G_{s'}$)

$a^{-1}gs' = a^{-1}gas$, $a^{-1}ga \in G_s$

teda aj $\cancel{h a^{-1} s'} =$

$h = a^{-1}ga \leftrightarrow g = aha^{-1}$.

Počítacia formula

Tvrdenie: Nech $s \in S$ a S je množina akcie grupou G. Potom

(rád G) = (rád stab)(veľkosť orbity)

$$|G| = |G_s||O_s|.$$

Resp. index stabilizátora G_s je $|O_s| = [G : O_s]$. (veľkosť orbity)

---

pre každý prvok $s \in S$ máme jednu takúto formulku...

→ veľkosť každej orbity delí počet prvkov grupy.