

ALGEBRA 7.5.

18.2 Burnside

G kon. působí na X (kon.)

$$|X/\sim| = \frac{1}{|G|} \sum_{g \in G} |X_g|$$

počet orbit = prům. počet per. b.

Pr.  2x2 barvy 2 barvy.
Zajímá nás počet obarvení až na otočení.

$X = \{\text{všechny obarvení}\} \dots |X| = 2^4 = 16$

$G = \{\text{otočení } 0, 90, 180, 270^\circ\}$. $|G| = 4$

Počet orbit = $\frac{1}{4} (|X_0| + |X_{90}| + |X_{180}| + |X_{270}|) = \frac{1}{4} (16 + 2 + 4 + 2)$

$X_0 = \text{všechno}$

$X_{180} = \text{diag. mají stejnou barvu} = 6$

$X_{90} = \text{všechny pol. stejné barvy}$

Def. Bud' G permutacím gr., t.j. $G \leq S_X$.

G je transitivní, pokud má jenom 1 orbitu ve svém působení na X . [t.j. $\forall x, y \in X \exists g \in G : g(x) = y$]

Věta 18.5 (Jordanova věta). Každá konečná transitivní grupa G , $|G| \geq 2$, obsahuje aspoň 1 permutaci bez pevného bodu.

Důk. Burnside: počet orbit = průměrný počet pevných bodů.

trans. \rightarrow $\frac{1}{1}$

$\exists g \in G$ má $n \geq 2$ pevných bodů ... Tedy nedprůměrný počet!

$\Rightarrow \exists g \in G$, st. má podprůměrný počet pevných bodů.

$\Rightarrow g$ má 0 pevných bodů. $\ddot{\smile}$



orbita = $\{g(x) \mid g \in G\}$

$$[x] = \{g(x) \mid g \in G\}$$

$$X_g = \{x \in X \mid g(x) = x\}$$

↑
pevný bod

$$G_x = \{g \in G \mid g(x) = x\} \leq G$$

$$|[x]| = [G : G_x]$$

$$|G| = |G_x| \cdot |[x]|$$

V.18.6 (Cauchyova věta) Bud' G konečná grupa a p prvočíslo t.j. $p \mid |G|$. Pak v G existuje prvek řádu p .

• Lagrange: $\text{ord } g \mid |G|$ pro každé $g \in G$.

• Opacně věta: Platí, že pokud $n \mid |G|$, pak $\exists g \in G$ t.j. $\text{ord } g = n$.

Obecně ne!

Dř. $X = \{ (a_1, a_2, \dots, a_p) \in G^p \mid a_1 a_2 \dots a_p = 1 \}$.

$|X|$: libovolně a_1, \dots, a_{p-1} , doplněním $a_p = a_{p-1}^{-1} \dots a_1^{-1}$.

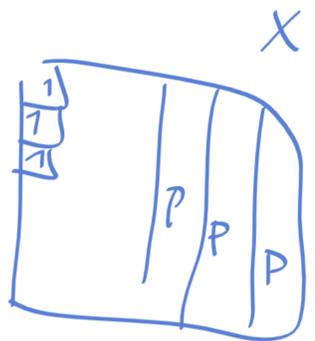
$\Rightarrow |X| = |G|^{p-1}$

\mathbb{Z}_p působí na X rotací sloček:

0. $(a_1, \dots, a_p) = (a_1, \dots, a_p)$

1. $(a_1, \dots, a_p) = (a_2, a_3, \dots, a_p, a_1) \in X$

2. $(a_1, \dots, a_p) = (a_3, a_4, \dots, a_p, a_1, a_2)$



$|[x]| \mid |\mathbb{Z}_p| = p \Rightarrow$ každá orbita má velikost 1 nebo p .

Existuje orbita velikosti 1, a sice $(1, 1, \dots, 1)$.

Zároveň X je disjunktivně sjednocením orbit,

p dílů $|X| = |G|^{p-1}$.

Tedy počet 1-prvkových orbit je $\frac{|X|}{p}$ pro nějaké $k \geq 1$

\Rightarrow existuje aspoň $p-1$ 1-prvkových orbit různých od $(1, 1, \dots, 1)$.

Bud' (a_1, a_2, \dots, a_p) jiné 1-prvkové orbita.

Pak $a_1 = a_2, a_2 = a_3, \dots \Rightarrow$ Prvek je tvaru $(a, a, a, \dots, a) \in X$

$\Rightarrow \underline{a^p = 1}$, zároveň $a \neq 1$. Tedy $\text{ord } a = p$.

19. FAKTOR GRUPY

19.1 Normální podgrupy

T.19.1 G grupa, $H \leq G$, NTJE

1) $aH = Ha$ pro $\forall a \in G$
 (čili levé a pravé rozkladové třídy komají)

2) $aha^{-1} \in H$ pro každé $h \in H, a \in G$
 (čili H je uzavřené ve konjugaci libovolným prvkem)

Def. Podgrupa H je normální v grupě G , pokud splňuje obiv. podmínky z T.19.1. Značíme $H \trianglelefteq G$.

Dl. (\Rightarrow) Bud' $h \in H, a \in G$. Víme $aH = Ha \Rightarrow$ existuje $h' \in H$
 $t. \rightarrow a h = h' a \Rightarrow a h a^{-1} = h' \in H \checkmark$

(\Leftarrow) Dokažeme $aH \subseteq Ha$ (a tedy $Ha \subseteq aH$). Bud' $ah \in aH$.
 Pak $h' = a h a^{-1} \in H$, a tedy $ah = h' a \in Ha \checkmark$
 Podobně $Ha \subseteq aH$.

Komentář ke konjugaci (viz 17.2) \rightarrow vnitřní

G grupa. $\text{Aut}(G) =$ grupa všech automorfismů G ,
 čili izomorfismů $G \rightarrow G$.

$\text{Inn}(G) =$ „vnitřní autom.“
 = automorfismy $\varphi_a: G \rightarrow G$ pro dané $a \in G$.

$$g \mapsto a g a^{-1}$$

konjugace
 Viz podobnost matice
 v LA

Tvrdím: φ_a je autom.
 • hom., čili $\varphi_a(gh) = \varphi_a(g) \cdot \varphi_a(h)$
 $a g h a^{-1} = a g a^{-1} \cdot a h a^{-1}$

• bijekce • prostě: $a g a^{-1} = a h a^{-1} \Rightarrow g = h$
 • ne: $g \in \text{Im } \varphi_a$? $\varphi_a(a^{-1} g a) = a a^{-1} g a a^{-1} = g \checkmark$

Snadno: $\text{Inn}(G) \leq \text{Aut}(G)$

$H \trianglelefteq G$ pokud $aha^{-1} \in H \quad \forall h \in H, a \in G.$

- $\{1\} \trianglelefteq G$, bo $a1a^{-1} = 1 \in \{1\}$
- $G \trianglelefteq G$
- G abelovské, pak $aha^{-1} = h \in H$ pro $\forall h$.
Tedy každá podgrupa je normální.
- $SL_n(T) \trianglelefteq GL_n(T)$, bo: $H \in SL_n(T), A \in GL_n(T)$
 $\det(AHA^{-1}) = \det(A) \det(H) \det(A)^{-1} = \det(H) = 1$
 $\Rightarrow AHA^{-1} \in SL_n(T)$.
- $H = \{id, (12)\} \not\trianglelefteq S_3$, bo $(13) = (23)(12)(23)^{-1} \notin H$.
- $A_n \trianglelefteq S_n$, bo $sgn(aha^{-1}) = sgn(a)sgn(h)sgn(a)^{-1} = sgn(h)$.
- $D_{2n} \not\trianglelefteq S_n$.
- $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, kvat. gr. ... každá podgr. je normální.
- A_n ($n \neq 4$) ... jediné normální podgr. krom $\{1\}, A_n$
... Jednoduchá grupa

T. 15.2 Jádro homomorfismu je normální podgrupa. ↖ 15.2

DŮ. Hom. $\varphi: G \rightarrow H$. $\ker \varphi = \{g \in G \mid \varphi(g) = 1_H\} \leq G$
Bud' $a \in G, k \in \ker \varphi$. $aka^{-1} \in \ker \varphi$.

$$\varphi(aka^{-1}) = \varphi(a) \varphi(k) \varphi(a)^{-1} = \varphi(a) \varphi(a)^{-1} = 1 \quad \checkmark$$

15.2 Konstrukce faktorgrupy

Def. G grupa, $N \trianglelefteq G$.

Definuje relaci na G : $a \sim b \Leftrightarrow ab^{-1} \in N$.

• T. 14.10: $ab^{-1} \in N \Leftrightarrow Na = Nb$
 N normální $\Leftrightarrow aN = bN$

• Tedy dvo. $[a] = aN = Na$

• Faktorgrupa G podle podgrupy N
= množina těchto bloků
= $\{aN \mid a \in G\}$

Faktorprůh. $m \in T[x]$
 $\deg m = d$.

$T[x]/(m(x)) = \{f \in T[x] \mid \deg f < d\}$
 $f+g$ nom.
 $f \odot g = f \cdot g \pmod m$.

Alternativní pohled:

Bral bych všechny $f \in T[x]$
někdy bych, že $f \sim g$, pokud
 $f \equiv g \pmod m$

$T[x]/(m(x))$ odpovídá třídě
Vezm $f \pmod m$

$$N \trianglelefteq G, \quad a \sim b \Leftrightarrow a b^{-1} \in N \Leftrightarrow N a = N b = a N = b N$$

$$[a] = a N = N a.$$

$$G/N = \{ [a] \mid a \in G \}.$$

Definujeme operace: $[a] \cdot [b] = [ab]$

$$[a]^{-1} = [a^{-1}]$$

neutrální prvek = $[1]$.

L. 19.3 $N \trianglelefteq G$. 1) Operace na třídách jsou dobře definované,
2) Faktorgrupa G/N je skutečná grupa.

Ds. 1) $A \vdash [a] = [c], [b] = [d]$.

Chci: $[ab] = [cd] \ \& \ [a^{-1}] = [c^{-1}]$

Plám: $a \sim c$, čili $ac^{-1} \in N$. $bd^{-1} \in N$.

Chci: $ab \sim cd$, čili $ab(cd)^{-1} \in N$

$$ab(cd)^{-1} = ab d^{-1} c^{-1} = \underbrace{a c^{-1}}_{\in N} \underbrace{c b d^{-1} c^{-1}}_{\text{konjugace} \in N} \in N \quad \checkmark$$

Podobně pro $^{-1}$.

2) Ověříme as. grupy pro G/N .

$$[a] \cdot ([b] \cdot [c]) \stackrel{?}{=} ([a] \cdot [b]) \cdot [c] \quad \checkmark$$

$$[a] \cdot [bc] = [abc] = [ab] \cdot [c]$$

Podobně: $[a] \cdot [1] = [a] = [1] \cdot [a]$

$\bullet [a] \cdot [a]^{-1} = [1] = [a]^{-1} [a]$.

$$\boxed{ab^{-1} \in H \Leftrightarrow a \sim b}$$

Př. $G = \mathbb{Z}$. $H = u\mathbb{Z}$. $a \sim b \Leftrightarrow a - b \in H \Leftrightarrow u \mid a - b$

$(\Leftrightarrow) a \equiv b \pmod{u}$.

$$[a] = \{ x \in \mathbb{Z} \mid x \equiv a \pmod{u} \} = a + u\mathbb{Z}, \quad a = 0, 1, \dots, u-1$$

$\bullet [a] + [b] = [a + b \pmod{u}]$; $-[a] = [-a] = [u - a]$

Vidíme: $\mathbb{Z}_u \xrightarrow{\cong} \mathbb{Z}/u\mathbb{Z}$
 $a \mapsto a + u\mathbb{Z}$.

CV. Uvězte to stejně pro faktoroid
 $(T[x]/u(x), +)$. $G = T[x]$
 $H = u(x)T[x]$

Pr. $G = S_n \supseteq N = A_n$.

$\pi \sim \sigma \Leftrightarrow \pi \sigma^{-1} \in A_n \Leftrightarrow \text{sgn } \pi = \text{sgn } \sigma$.

Tedy ~ me! 2 bloky, a nice $S = \{\text{sudé perm.}\}, L = \{\text{liché perm.}\}$.

Operace $S \cdot S = S, SL = LS = L, LL = S$

Vidim, že S_n/A_n je 2-prvková, $S_n/A_n \cong \mathbb{Z}_2$.

$$S \mapsto 0$$

$$L \mapsto 1$$

V. 19.4 $\varphi: G \rightarrow H$ hom. grp.

1) (věta o hom.) Je-li $N \subseteq \ker \varphi$ a $N \trianglelefteq G$, pak zobrazení

$\psi: G/N \rightarrow H$ je dobře definované a

$[a] \mapsto \varphi(a)$ je to grupový hom.

Dk. 1) Dobře def. ? $[a] = [b] \stackrel{?}{\implies} \varphi(a) = \varphi(b)$

$[a] = [b] \Rightarrow ab^{-1} \in N \Rightarrow ab^{-1} \in \ker \varphi \Rightarrow \varphi(ab^{-1}) = 1$
 $\Rightarrow \varphi(a) = \varphi(b) \quad \checkmark$

Hom. ?

$$\psi([a]) \cdot \psi([b]) \stackrel{?}{=} \psi([a] \cdot [b])$$

$$\parallel$$

$$\varphi(a) \cdot \varphi(b)$$

$$\parallel$$

$$\psi([ab])$$

$$\parallel$$

$$\varphi(ab)$$