

ALGEBRA 5.5.

16.3

$G \cong \text{cycl. skupina } \langle a \rangle$

$$\exp: \mathbb{Z}_n \xrightarrow{\sim} G \\ g \mapsto a^g$$

$$\log: G \xrightarrow{\sim} \mathbb{Z}_n \\ a^g \mapsto g$$

typically non- \mathbb{Z} .

Mimulo: cyklické možnosti
"složitost" $O(\log n)$.
To je dobrý, že
"je v počtu v
lin. soust., a tedy
mejí delší log n".
Výrobek a^n je extrémně
pomalejší $O(e^{\log n})$
T expon.

Př. $G = \mathbb{Z}_n = \langle a \rangle$

$$\log_a b = g \in \mathbb{Z}, "b = a^g"$$

"adit.-grupé" tohle odpovídá

Výpočet diskr. log. "v \mathbb{Z}_n ... modu l" a, b, u, hledáme g.

Výsledek: a generuje \mathbb{Z}_n , tedy $\gcd(a, n) = 1$ Béz.

Par $bx \equiv ax \equiv g \pmod{n}$, Cyklické (Eukl.)

$$\text{tedy je em nejméně } g.$$

Např. diskr. log. pro \mathbb{Z}_p^* , kde $p \geq 2^{1000}$ prvočí,

je velmi pomalý.

Diffie-Hellman protocol Mezi Alice a Bobem, kteréji' sotva společný klíč, ale komunikují jenom bez bezpečnosti. Tedy mohou využít t. "Caesaraova zifra"

$$+ z_1 z_2 z_3 \dots \quad \leftarrow \mathbb{Z}_{p-1} \quad z_i, s_i \in \mathbb{Z}_2 \\ s_1 s_2 s_3 \dots \quad \leftarrow \text{klíč}$$

$$z_1 + s_1, z_2 + s_2, \dots \quad \leftarrow \text{zefifikace správ} \\ \text{na polohu.}$$

Tímto způsobem přijde klíč a dostane poslední správu.

Pokud dívce klíče = dívce správy \Rightarrow reprosto bezpečnost.

Výpočet v $G = \langle a \rangle$ (vezmějme)

Alice ... teď využije $i \in \{2, \dots, |G|-1\}$, spočte a^i ,
Bob ... $\frac{a}{a^i} \quad u \in \{2, \dots, |G|-1\}$.

A pošle a^i ; B pošle a^u .

A spočte $(a^i)^u = \underline{a^{iu}}$, B spočte $(a^u)^i = \underline{a^{iu}}$ \leftarrow spořečný klíč.

• El Gramelinov protocol - variace ve RSA - viz script

• jednosměrné funkce, zdejší verze

— 4 —

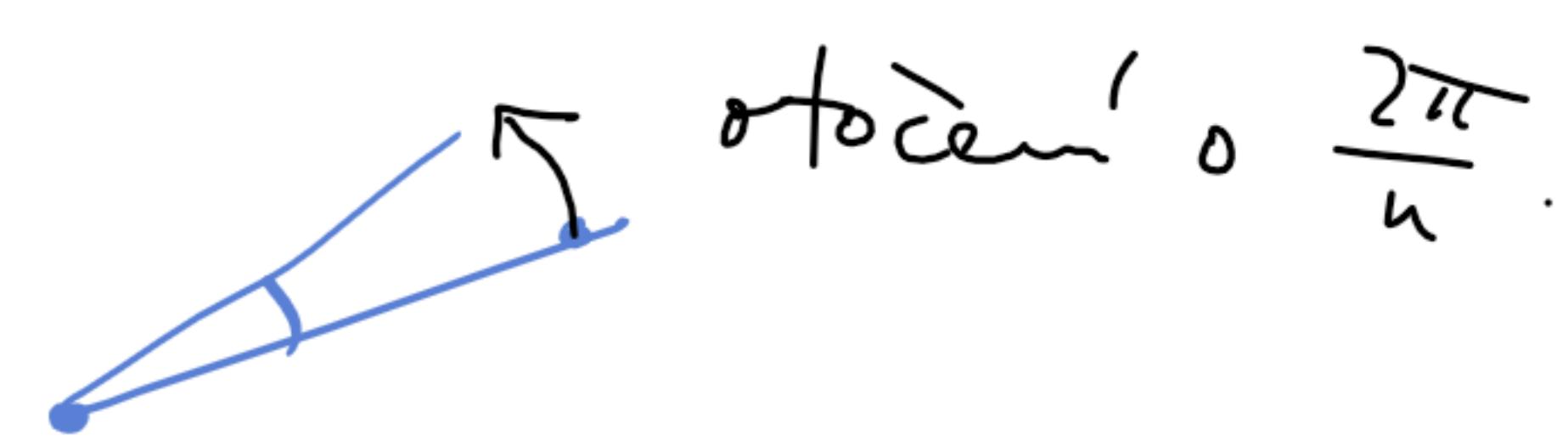
18. Přirobení grupy na množinu

18.1 Abstraktní grupa jako grupa permutací

17. Grupy sym.
viz scripta
pro kontext+

Př. Zn. množinu interpretující jako grupu násobek rotací v řadě $\theta \cdot \frac{2\pi}{n}$ pro $\theta \in \mathbb{R}$.

Dále v prostoru hom. $\mathbb{Z}_n \rightarrow S_{R^2}$



Def. Přirobený grupa G na množinu X je liborohy' homom.

$\pi: G \rightarrow S_X$. Hodnotu permutace $\pi(g)$ ve proku $x \in X$ často označuje $g(x)$.

• π je hom., tedy $\pi(1) = \text{id}$

$$\pi(g^{-1}) = \pi(g)^{-1} \dots \text{inverzí}$$

$(g \cdot h)(x) = g(h(x))$ vztahem k G odpovídá
zdejší permutaci

Př. Trivialní příp. $\pi(g) = \text{id} \quad \forall g \in G$.

Př. $GL_n(T)$ pro těleso T

| invert. transf. ne r. p. Tⁿ

| přirobené příslušné X=Tⁿ: pro $A \in GL_n(T)$ máme

$$\pi(A)(v) = Av$$

To zdejší můžeme i pro podgrupy $G \leq GL_n(T)$: zdejší příslušné ne Tⁿ.

Vita 15.10 (Cayleyova reprezentace). Ke žádoucímu funkci jde množit
do nějaké symetrické grupy,

tj. \exists hom. $\varphi: G \hookrightarrow S_X$.

Dl. Doložit vztahme $X=G$. [tedy pokud G lze vložit do $S_G \cong S_{|G|}$]

Pro $a \in G$ máme levou translací $La: G \rightarrow G$

$$x \mapsto ax$$

Soudno: La je permutace na G (to můžu zkontrolovat a)

• zobrazení $G \xrightarrow{\varphi} S_G$ je hom. (tj. tedy G přísluší k $X=G$)

$$a \mapsto La$$

$$La(x) = (ax)$$

OK.

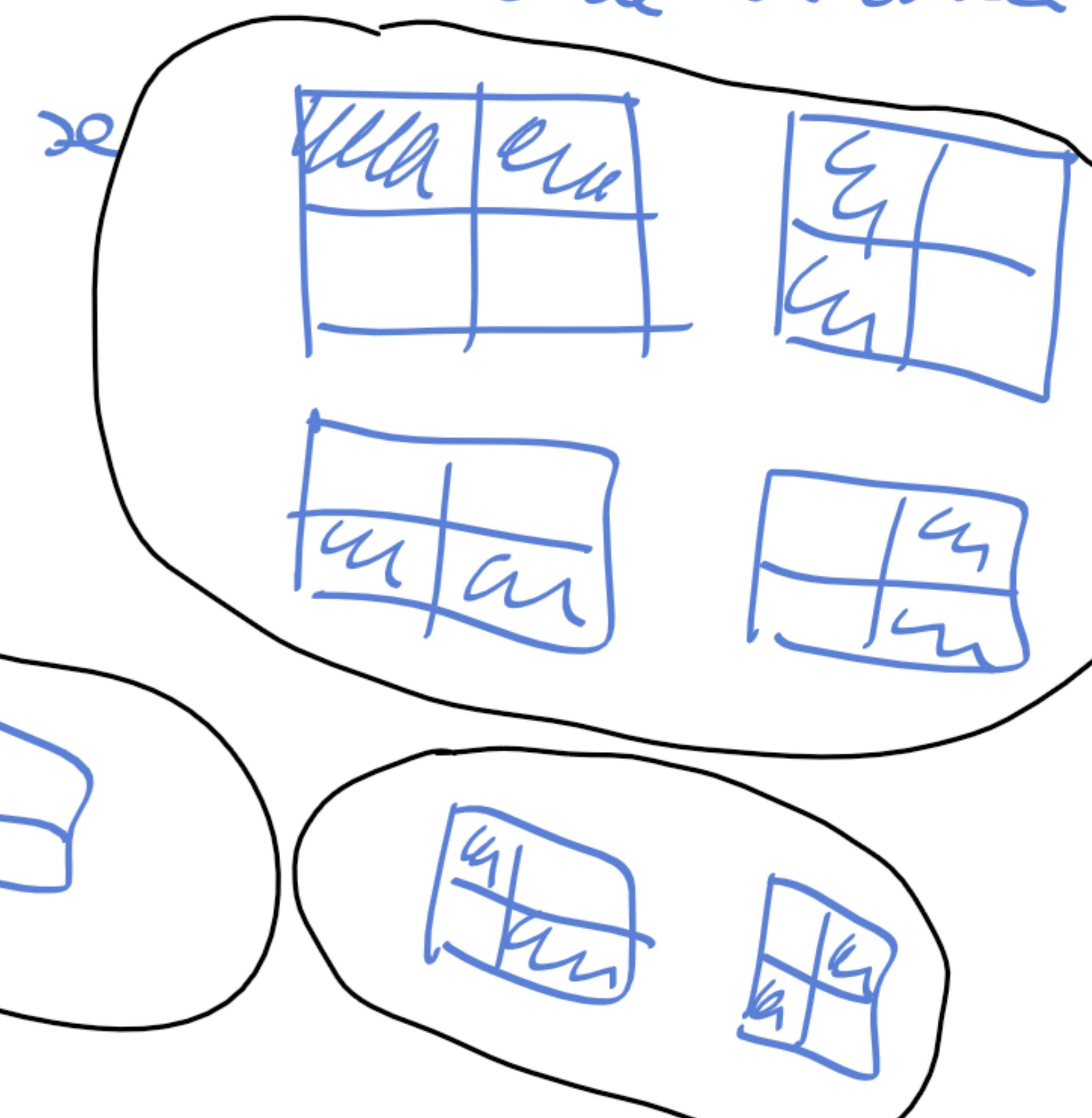
• Snadne' ověření:

$$La \circ Lb = LaLb: \begin{cases} LaLb(x) = (ax) \\ LaLb(x) = La(bx) = a(bx) \end{cases}$$

[národe 15.5 obecnější o reprez. grup]

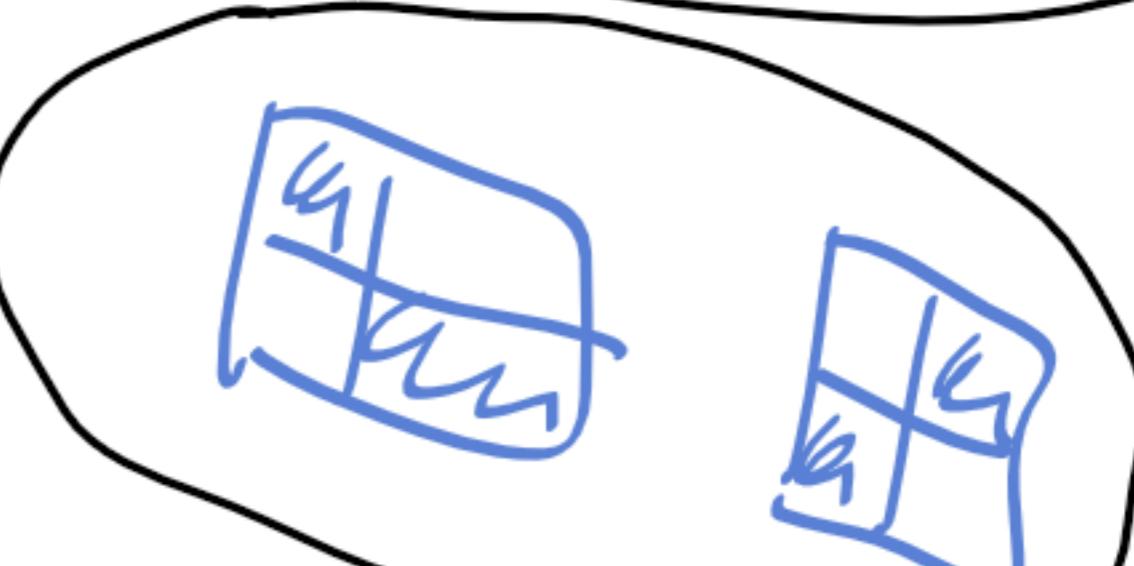
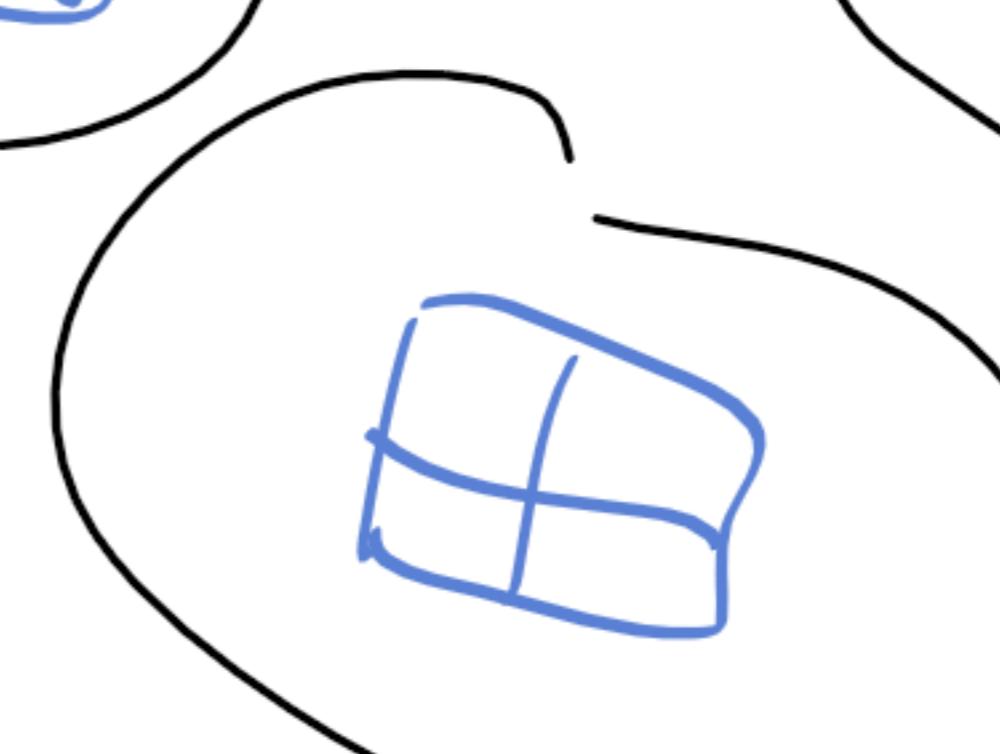
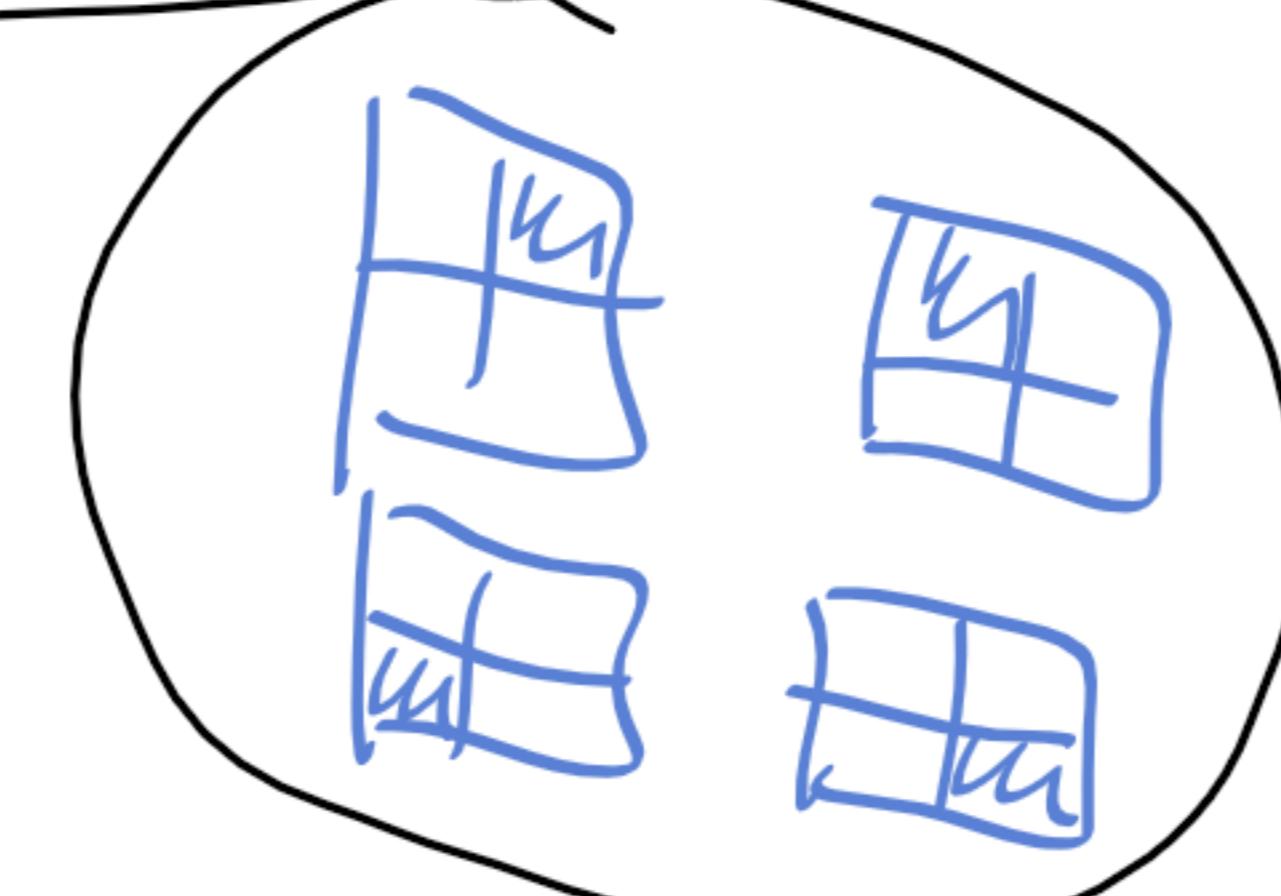
Příklad kolika způsoby jde obrnit poličkové tabule 2×2 dvěma barvami až neotocenými, tříšmějí, zobrazeny považuju se stejnou, pokud se listí otocením.

16 zobrazení, ale
číslo neotocenými jenom 6



$$X = \{16\text{ zobrazení}\}$$

$$G = \{g \text{ rotace o } 0^\circ, 90^\circ, 180^\circ, 270^\circ\}$$



- G grupa pohybů ne množině X (fixuje).

Def. Relace transitivity \sim na X : $x \sim y$ pokud $\exists g \in G: g(x) = y$.

Lemma 18.1 \sim je ekvivalence na X .

Dle. CV / skripta. Např. $x \sim y \Leftrightarrow y \sim x$: $g(x) = y \Leftrightarrow x = g^{-1}(y)$.
čili větší permutace považuje x ne y .

Def. Tedy ekvivalence \sim jsou orbity (ORBITA)

Orbita obsahující $x \in X$ nazívame $[x] = \{y \in X \mid y \sim x\} = \{g(x) \mid g \in G\}$

- Řečený příkladu \uparrow je počet orbit \sim tomu působení.

Def. Bod $x \in X$ je pevný bod pokud $g \in G$, pokud $g(x) = x$
Možností všechny pevné body pro každou $g \in G$ nazívame $X_g = \{x \in X \mid g(x) = x\}$

Stabilizátor pokud $x \in X$ je možnost $G_x = \{g \in G \mid g(x) = x\}$

Příklad Stabilizátor $\boxed{\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}} = G$.

Stab. $\boxed{\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}} = \{ \text{id}, \text{ otoc. o } 180^\circ \}$

Stab. $\boxed{\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}} = \{ \text{id} \}$

Lemma 18.2 Stabilizátor G_x je podgrupa G .

Dle. • $1 \in G_x$, bo $1(x) = x$ (vždy pohyb jde id.)

• $g, h \in G_x$, čili $g(x) = x, h(x) = x$.

Tak $(g \cdot h)x = g(h(x)) = g(x) = x \Rightarrow g \cdot h \in G_x$

$g^{-1}(x) = x \Rightarrow g^{-1} \in G_x$.

Tedy např. méně logické větu.

T. 18.3 (velkost orbity vs. index stabilizátoru). $\forall x \in X$ máme

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

Připomíme: index podgrupy = počet rozděloujících říd $g G_x$.

Dl. Najdu bijekci mezi $[x]$ a množinou $\{g G_x \mid g \in G\}$.

Využijme $\varphi: \{g G_x \mid g \in G\} \rightarrow [x]$

$$g G_x \mapsto g(x)$$

$g(x) \in [x]$. Je φ vůbec dobré def.? $g G_x = h G_x \Rightarrow ?$ $g(x) = h(x)$

T. 14.10: $g G_x = h G_x \Leftrightarrow h^{-1}g \in G_x \Leftrightarrow h^{-1}g(x) = x \Leftrightarrow g(x) = h(x)$

p dobré def. ✓

φ ještě (dilky \Leftarrow)

φ je, to je $g(x) \in [x]$ méně $g(x) = \varphi(g G_x)$

Druh. leh. věty: $|G| = |G_x| \cdot [G : G_x] = |G_x| \cdot |[x]| = \underline{\underline{\underline{O}}}$

18.2 Burnside

X/\sim ... množina všech říd ekvivalence \sim na množ. X

Pro nás $|X/\sim| =$ počet orbit daného působení

Věta 18.4 (BURNSIDEova věta). Ať boučková grupa G působí na kon. m. X .

Pal

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

↑ počet pravých bodů g .

• Problém = počet pravých bodů pro každé $g \in G$

Dl. $M = \{(g, x) \in G \times X \mid g(x) = x\}$. Soubor velikost M je správný.

$$|M| = \sum_{g \in G} |X_g| = \sum_{x \in X} |G_x|. \quad [x] = 0$$

$$\frac{1}{|G|} \sum_g |X_g| = \frac{1}{|G|} \cdot \sum_{x \in X} |G_x| \stackrel{?}{=} \sum_{x \in X} \frac{1}{|[x]|} = \sum_{o \in X/\sim} \sum_{x \in o} \frac{1}{|o|} =$$

$$= \sum_{o \in X/\sim} |o| \cdot \frac{1}{|o|} = \sum_{o \in X/\sim} 1 = |X/\sim|. \quad \therefore$$

Předběžné: pátek 4.6. ve předu. [včetně cv. na stř. 2.6.]

- Dohud nebrude opakovat přehled, můžete se s ním seznámit.
(tj. předtermín + termín v 1. týdnu slousťování)