Grupy a reprezentace 2

Zpracováno na základě poznámek J. Mareše a s jejich využitím

wiki-skripta

Podgrupy - proč ?

Pro studium vlastností a struktur grup je potřeba je rozdělit na "nedělitelné"grupy a podívat se jakým způsobem jsou z nich tyto grupy složené.

Je to vlastně komplikovaná analogie rozkladu čísla na prvočinitele.
Těmito prvočiniteli jsou grupy speciáního typu.

(Matematikům to trvalo 100 let, než v roce 1980 našli všechny tyto grupy)

A způsoby jejich skládání do složitějších celků se řeší dodnes.

Podgrupa

Neprázdná podmnožina H grupy G, tj. $\emptyset \neq H \subset G$, je ***podgrupa*** *grupy G (značíme $H \leq G$), pokud je grupou vůči násobení v G. (Tedy obsahuje jednotku z G a je uzavřená vůči násobení prvků z H a vůči jejich inverzi.)*

Example

- Množina $\{E, A\}$ je podgrupou v D_6 ($A^2 = E$, $A^{-1} = A$).
- Rotace kolem pevné osy je podgrupou v SU(2)
- Koplexní čísla jsou podgrupou v kveternionech
- jakákoliv permutace generuje podgrupu v symetrické grupě

Věta pro zjednodušení důkazu podgrup

Theorem

Podnožina $\emptyset \neq H \subset G$ *je podgrupa* $\Leftrightarrow (\forall x, y \in H)(xy^{-1} \in H)$.

Důkaz.

Implikace $\Rightarrow$ *plyne přímo z definice podgrupy.*

Dokážeme opačnou implikaci $\Leftarrow$, *tj. že* H *je grupa.*
Z definice je H *neprázdná, a tedy můžeme vzít* $g \in H$.
Pokud nyní položíme $x = g$ *a* $y = g$, *máme* $gg^{-1} \in H$, *tedy* H *obsahuje jednotku. Dále tedy volíme* $x = 1$ *a* $y = g$ *a dostáváme* $1g^{-1} \in H$, *tedy* H *obsahuje inverzi* g.
Nakonec pro libovolné prvky $f, g \in G$ *volíme* $x = f$ *a* $y = g^{-1}$, *dostáváme* $f(g^{-1})^{-1} \in H$, *tedy* H *obsahuje součin* fg. □

Pro konečnou podgrupu $H \leq G$ platí $(\forall x \in H)(|x| < \infty)$.

Důležité podgrupy - centralizátory

Buď $\emptyset \neq A \subset G$ libovolná podmnožina.

Definujeme ***centralizátor*** *množiny* A *v* G *jako:* $C_G(A) = \{g \in G | gag^{-1} = a \text{ pro } \forall a \in A\}$.

Jelikož $(gag^{-1} = a) \Leftrightarrow (ga = ag)$, je centralizátor množiny A množina všech prvků z G, které komutují se všemi prvky z A.
Nebo se dá říct, že jsou to všechny prvky $g \in G$, které po působení na každý prvek z A "akcí"$(gag^{-1} = a)$ ponechá tento prvek na místě.

Centralizátor -věta

Theorem

Množina $C_G(A)$ je podgrupa v G.

Důkaz.

Víme, že $C_G(A)$ je neprázdná, $e \in C_G(A)$ ($eae^{-1} = a$).
Dále mějme $x \in C_G(A)$. Pak pro $\forall a \in A$ platí:

$$x^{-1}| \quad xax^{-1} = a \quad |x$$
$$a = x^{-1}ax,$$

tedy $x^{-1} \in C_G(A)$.
Pro dva prvky $x, y \in C_G(A)$ pak máme:

$$(xy)a(xy)^{-1} = x(yay^{-1})x^{-1} = xax^{-1} = a,$$

a tedy centralizátor je uzavřený i vůči násobení. □

Centrum

Definujeme

> ***centrum*** *grupy* G *je množina* $Z(G) = \{g \in G | gfg^{-1} = f \text{ pro } \forall f \in G\}$.

Platí, že $Z(G) = C_G(G)$, tedy je to množina prvků G, které komutují se všemi ostatními. Jako speciální případ předchozí věty platí, že je podgrupou $Z(G) \leq G$.

Centrum je centralizátor celé grupy

> *Pro* $A \subset G$ *a* $g \in G$ *zavádíme značení:* $gA = \{ga | a \in A\}$. *Obdobně pro* Ag, *a tedy konkrétně* $gAg^{-1} = \{gag^{-1} | a \in A\}$.

Normalizátor

Buď $\emptyset \neq A \subset G$. *Definujeme* ***normalizátor*** A *v* G *jako:* $N_G(A) = \{g \in G | gAg^{-1} = A\}$.

Normalizátor se od centralizátoru liší tím, že může prvky A zpermutovat (množina A se tím nezmění). Grupové vlastnosti $N_G(A)$ se ukáží podobně jako u $C_G(A)$. Tady je opět A libovolná množina. Později zavedeme

normální podgrupu, kterých může být v grupě mnoho. Jsou to takové **podgrupy**, které normalizuje celá grupa.

Věta - normalizátor

Corollary

Platí, že $C_G(A) \leq N_G(A) \leq G$.

Důkaz.

$N_G(A) \leq G$: Použijeme značení z předchozího.

1. $N_G(A) \neq \emptyset$, protože $e \in N_G(A)$.
2. Nechť $x, y \in N_G(A)$, tj. $xAx^{-1} = A$ a $yAy^{-1} = A$. Pak platí $(xy)A(xy)^{-1} = x\underbrace{(yAy^{-1})}_{A}x^{-1} = xAx^{-1} = A$. (Asociativita platí z vlastností grupového násobení v G.) To ale znamená, že $(xy) \in N_G(A)$.
3. Nechť $x \in N_G(A)$. Pak zřejmě platí $xAx^{-1} = A \rightarrow x^{-1}Ax = A$, tj. $x^{-1} \in N_G(A)$, čímž je $N_G(A) \leq G$ dokázáno.

$C_G(A) \leq G$ již bylo dokázáno a $C_G(A) \leq N_G(A)$ je pak zřejmé z definice podgrupy. □

Grupu nazýváme **cyklická**, *pokud je generována jen jedním prvkem* a *a značíme* $H =< a >= \{a^n | n \in \mathbb{Z}, a^0 = e\}$.

U končných grup je jednotkový prvek vždy nějakou nenulovou mocninou generátoru.

Cyklická grupa má rank=1. Může být generována i různými prvky -např. $\mathbb{Z}_p$

Cyklická grupa je vždy abelovská (komutativní).

Theorem

Dvě cyklické grupy $< x >$ *a* $< \xi >$ *stejného řádu jsou isomorfní.*

Důkaz.

Pro konečné grupy máme izomorfismus: $\varphi(x) = \xi, \ \varphi(x^n) = \xi^n$
Pro nekonečnou grupu $< x >$*:* $\varphi : G \to \mathbb{Z}$

$$\varphi(e) = 0, \ \varphi(x) = 1, \ \varphi(x^n) = n, \ n \in \mathbb{N},$$

Theorem

Pro grupu $G =< x >$ *platí* $|G| = |x|$.

Důkaz.

1. *Pro* $|x| = \infty$ *jsou všechny prvky* x^α *různé pro* $\forall\alpha \in \mathbb{N}$, *tedy jich je nekonečně mnoho.*
2. *Nechť* $|x| = n$. *Platí* $(\forall\alpha \in \mathbb{Z})(\alpha = kn + m)$, *pro nějaké* $n \in \mathbb{Z}$ *a* $(m \in \mathbb{Z}^+)(m \leq n)$. *Potom* $s^\alpha = x^{kn}x^m = ex^m$. *Máme tedy právě* n *prvků v* G.

□

Největší společný dělitel čísel n a m značíme $\gcd(n, m)$.

Lemma

Mějme grupu $G =< x >$. Potom platí:

1. Pokud $x^n = 1$ a $x^m = 1$, $(m, n \in \mathbb{Z} \setminus \{0\})$, potom $x^d = 1$, kde $d = \gcd(m, n)$
2. Navíc pokud $x^m = 1$, pak $|x|$ dělí m.

Důkaz:
1)
$d = mr + ns$ - Euclidův algoritmus

$$x^d = x^{mr+ns} = x^{mr}x^{ns} = 1$$

2)
$x^m = 1$, nechť $|x| = n$. Pak nechť $d = \gcd(m, n)$ a $x^d = 1$, d je menší rovno než n, n jeřád -nejmenší takové číslo $\Rightarrow d = n$ a $d|m$. Symbol $|$ znamená první číslo dělí druhé

Theorem

Mějme grupu $G =< x >$. *Potom platí:*

1. $|G| = \infty \Rightarrow |x^\alpha| = \infty$ *a navíc* $(x^\alpha \neq x^\beta)(\forall \alpha, \beta \in \mathbb{Z} \setminus \{0\})$,
2. $|G| = n \Rightarrow |x^\alpha| = \frac{n}{\gcd(n,\alpha)}$ *pro* $\alpha \in \mathbb{Z} \setminus \{0\}$.

Důkaz.

1) Sporem
$|G| = \infty$ znamená, že $|x| = \infty$. Nechť $(\exists n \in \mathbb{N})$ tak, že $|x^\alpha| = n$, tj. $((x^\alpha)^n = x^{n\alpha} = e)$ - spor. Dále nechť $x^\alpha = x^\beta$. Potom $x^{\alpha-\beta} = x^0 = 1$ (tedy $|x| = \alpha - \beta$), což je též spor. □

Pokud je $n\alpha$ záporné, $-n\alpha$ je kladné číslo - řád prvku.

Důkaz.

2) Víme tedy, že $|x| = n$. Označme si $d = \gcd(n, \alpha)$. Musí existovat celá čísla c a d taková, že $\alpha = cd$ a $n = bd$, $\gcd(b, c) = 1$. Platí:

$$(x^{\alpha})^{b} = x^{\alpha b} = x^{d\,c\,b} = x^{n\,c} = e.$$

Nyní ukážeme sporem, že $b \in \mathbb{N}$ je nejmenší takové číslo: Nechť $|x^{\alpha}|\ |b$ (dělí b). Potom

$$\exists k < b,\ x^{\alpha k} = e,\ n|ak,\ db|dck,\ b|ck.$$

Ale protože $\gcd(b, c) = 1$, b musí dělit k a to je spor.
(Doporučuji si to vyzkoušet na konkrétních číslech, třeba $n = 4$ a $\alpha = 6$.)

□

Důsledek

Theorem

Nechť $H < x >$, *potom*

1. $|x| = \infty \Rightarrow \{H =< x^{\alpha} > \Leftrightarrow \alpha = \pm 1\}$
2. $|x| = n < \infty \Rightarrow \{H =< x^{\alpha} > \Leftrightarrow \gcd(\alpha, n) = 1\}$
3. *Každá podgrupa grupy* $< x >$ *je cyklická.*

Podgrupy generované podmnožinou grupy

Máme-li nějakou podmnožinu M prvků z grupy, potom můžeme definovat podgrupu generovanou touto podmnožinou - pozor pro nekomutativní grupy. Je to minimální podgrupa, který obsahuje všechny prvky z M. Snadno se ukáže, že průnik podgrup je opět podgrupa - např. napřed pro dvě a potom indukcí.

$$K = G \cap H.$$

Pro $\forall x, y \in K$ platí $xy^{-1} \in K$. Vše leží v G i H.

Podgrupa ***generovaná podmnožinou*** $M \subset G$ *je nejmenší podgrupa* G *obsahující všechny prvky* M*. Tedy*

$$< M >= \bigcap_{\substack{H_i \leq G \\ M \subset H_i}} H_i.$$

Pro konečný počet prvků $A = \{a_1, a_2, \ldots, a_k\}$ píšeme:

$$< A >=< a_1, a_2, \ldots, a_k > .$$

Nechť $\overline{A} = \{a_{i_1}^{\epsilon_{i_1}} a_{i_2}^{\epsilon_{i_2}} a_{i_3}^{\epsilon_{i_3}} a_{i_4}^{\epsilon_{i_4}} \ldots, \epsilon_{i_1} = \pm 1, k \in \mathbb{N} \cup \{0\}\}$ a $\overline{A} = 1$ pro $A = \emptyset$, potom

$$\overline{A} =< A >, \ A \subseteq G.$$

Grafy grup - svazy podgrup

Nyní zavedeme relaci uspořádání, abychom mohli zavést svazy podgrup a kreslit tzv. Hasseho diagramy.(binární relace)

*Relaci $\preceq$ na množině M nazýváme **částečné uspořádání**, pokud platí:*

1. *reflexivita:* $(\forall x \in M)(x \preceq x)$,
2. *tranzitivita:* $(\forall x, y, z \in M)(x \preceq y \wedge y \preceq z \rightarrow x \preceq z)$,
3. *slabá antisymetrie:* $(\forall x, y \in M)(x \preceq y \wedge y \preceq x \rightarrow x = y)$.

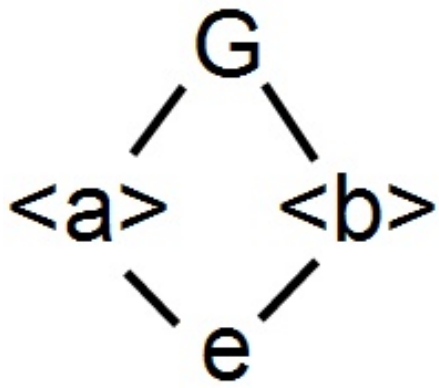
Example

Mějme libovolnou množinu A a její potenční množinu $\mathcal{P}(A) = 2^A$.
Zavedeme uspořádání $(\forall M, N \in 2^A)(M \preceq N \Leftrightarrow M \subset N)$.

Example

Grupa $G = \{e, a, b | a^2 = e, b^2 = e\}$ má podgrupy $\{e\}$, $< a >$, $< b >$ a G.
Můžeme zavést uspořádání pomocí relace "být podgrupou", tedy způsobem: $G_1 \preceq G_2 \Leftrightarrow G_1 \leq G_2$.

Sup, inf



Obrázek: Uspořádání na $G = \{e, a, b | a^2 = e, b^2 = e\}$ podle relace „být podgrupou“.

Buď $\{M, \preceq\}$ množina s částečným uspořádáním a $A \subset M$ její podmnožina. Prvek $x \in M$ nazveme

- ***horní závora*** *množiny A, pokud $(\forall a \in A)(a \preceq x)$,*
- ***dolní závora*** *množiny A, pokud $(\forall a \in A)(x \preceq a)$,*
- ***supremum*** *množiny A ($x = \sup_{\preceq} A$), je-li x nejmenší prvek množiny horních závor A,*
- ***infimum*** *množiny A ($x = \inf_{\preceq} A$), je-li x největší prvek množiny dolních závor A.*

Svaz a modulární svaz

Buď $\{M, \preceq\}$ množina s částečným uspořádáním. Pak $\forall x, y \in M$ definujeme operace

- ***spojení*** $x \vee y = \sup_{\preceq}\{x, y\}$.
- ***průsek*** $x \wedge y = \inf_{\preceq}\{x, y\}$,

Neplést spojení a průsek $(\vee, \wedge)$ s operacemi sjednocení a průnik $(\cup, \cap)$.

Definice:
Buď $\{M, \preceq\}$ množina s částečným uspořádáním a operacemi $\wedge, \vee$. Potom $\{M, \wedge, \vee\}$ nazýváme svaz, pokud $(\forall x, y \in M)((x \vee y \in M)$ **a zároveň** $(x \wedge y \in M))$.

Example

Nechť je relace uspořádání $a \preceq b$ vlastnost, že a dělí b, potom $\{4, 6, 8\}$ není svaz - sup $= 24$, inf $= 2$. Zatímco $\{2, 4, 6, 8, 24\}$ s daným uspořádáním svaz je.

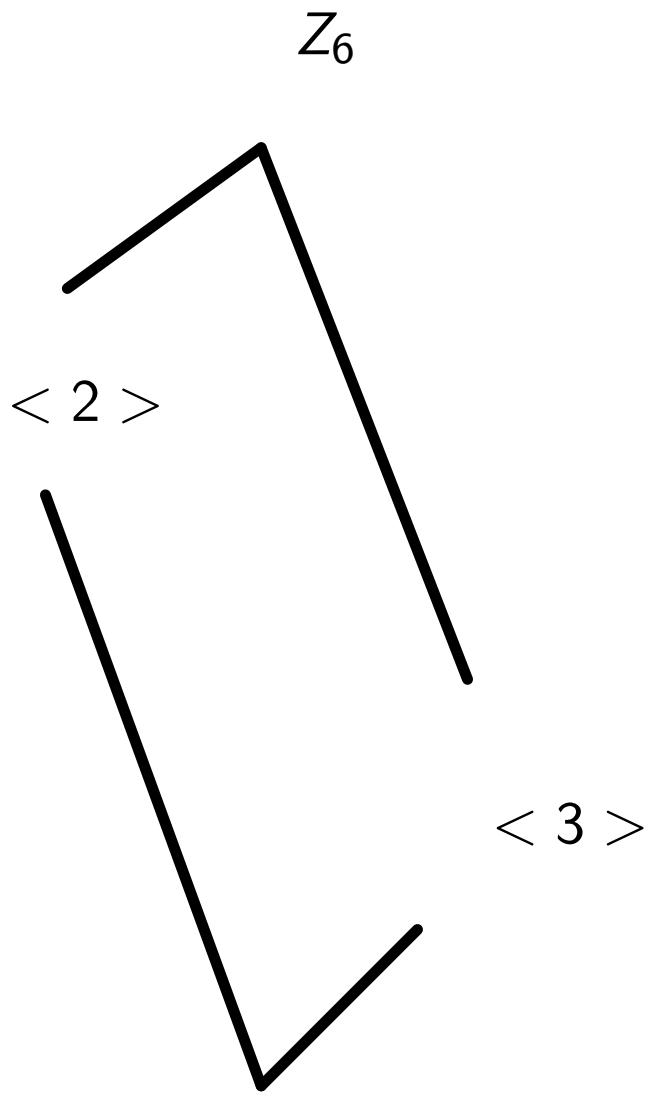
*Svaz $\{M, \wedge, \vee\}$ nazýváme **modulární**, pokud* $(\forall a, b, c \in M)((a \preceq c) \Rightarrow a \wedge (b \vee c) = (a \wedge b) \vee c)$.

Hasseovy diagramy

Konstrukce **Hasseova diagramu** konečné grupy G přes podgrupy:

- Najdeme všechny podgrupy G a seřadíme je podle jejich řádu. Grupu G umístíme nejvýše a grupu 1 nejníže. Zbytek podgrup rozmístíme podle jejich řádu a čarami spojíme všechny grupy A a B, pro něž $A \leq B$ a neexistuje podgrupa C, pro kterou $C < B$ (vlastní podgrupa) a zároveň $A < C$. (Tedy spojujeme jen „nejbližší“ podgrupy.)
- Mezi každými dvěma podgrupami $A \leq B$ existuje spojnice, ale může vést přes celý řetězec podgrup a těchto spojnic může být i více. Příklad je na obrázku.

Graf $\mathbb{Z}_6$



D_6