Grupy a reprezentace 6

Zpracováno na základě poznámek J. Mareše a s jejich využitím

wiki-skripta

p–grupa a Sylowova podgrupa

Definice: Buďte G grupa a p prvočíslo.

1. *Grupu řádu p^α pro nějaké $\alpha \geq 1$ se nazývá* ***p-grupa****. Podgrupy G řádu p^α nazýváme* ***p-podgrupy*** *G.*
2. *Je-li G řádu $p^\alpha m$ a $p \nmid m$, pak podgrupu řádu p^α nazýváme* ***Sylowova p-podgrupa*** *G.*
3. *Množinu všech Sylowových p-podgrup značíme $Syl_p(G)$ a počet těchto podgrup $n_p(G)$ (nebo jen n_p, je-li grupa jasná z kontextu).*

Lemma

Nechť $P \in Syl_p(G)$ a Q libovolná p-podgrupa G, pak $N_G(P) \cap Q = P \cap Q$.

Důkaz.

$\supset$) *Nechť $H = N_G(P) \cap Q$. Protože $P \leq N_G(P)$, je jasné že $P \cap Q \leq H$, musíme tedy ukázat opačnou inkluzi.*
$\subset$) *Z definice je $H \leq Q$, stačí proto ukázat, že $H \leq P$. Protože $H \leq N_G(P)$, je PH podgrupa a platí*

$$|PH| = \frac{|P||H|}{|P \cap H|}.$$

Všechny členy na pravé straně jsou mocniny p, proto PH je p-podgrupa a protože $P \leq PH$ je p-podgrupa maximálního řádu, musí platit $|PH| = |P| = p^\alpha$, tedy $PH = P$ a $H \leq P$. □

Sylowowa věta

Theorem (Sylow)

Buď G grupa řádu $p^\alpha m$, kde p je prvočíslo a $p \nmid m$. Pak:

1. *Existuje Sylowova p-podgrupa, tedy $Syl_p(G) \neq \emptyset$.*
2. *Je-li P Sylowova p-podgrupa G a Q libovolná p-podgrupa G, pak existuje $g \in G$ takové, že $Q \leq gPg^{-1}$, tedy Q je obsažena v nějakékonjugované k P. Speciálně každé dvě Sylowovy p-podgrupy G jsou vzájemně konjugované v G.*
3. *Počet Sylowových p-podgrup je tvaru $1 + kp$, tedy $n_p \equiv 1 \mod p$. Dále n_p je index grupy $N_G(P)$ v G pro každou Sylowovu p-podgrupu P, a tedy $n_p | m$.*

Důkaz 1

Důkaz provedeme úplnou indukcí na $|G|$, přičemž pro $|G| = 1$ není co dokazovat. Nechť tedy existuje Sylowova p-podgrupa pro všechny grupy menšího řádu než $|G|$.
Když $p \mid |Z(G)|$, pak podle Cauchyho věty existuje $N \trianglelefteq Z(G)$ řádu p. Pak $|\overline{G}| = |G/N| = p^{\alpha-1}m$ a z indukčního předpokladu existuje $\overline{P} \leq \overline{G}$ řádu $p^{\alpha-1}$. Takže pro P podgrupu G obsahující N takovou, že $P/N = \overline{P}$, platí $|P| = |P/N||N| = p^{\alpha}$ a P je Sylowova p-podgrupa G. Omezíme se proto na případ $p \nmid |Z(G)|$.

Pokračování

$p \nmid |Z(G)|$
Nechť $g_1, g_2, \ldots, g_r$ jsou reprezentanti různých tříd neobsažených v centru G, pak platí rovnice tříd

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|. \tag{1}$$

Pokud by platilo $p \mid |G : C_G(g_i)|, \forall i$, pak by platilo taky $p \mid |Z(G)|$, protože $p \mid |G|$. Proto pro nějaké i musí platit $p \nmid |G : C_G(g_i)|$. Označíme $H = C_G(g_i)$ pro dané i a máme

$$|G : C_G(g_i)| = \frac{p^\alpha m}{p^\alpha k}, \ |H| = p^\alpha k, \quad \text{kde } p \nmid k, \tag{2}$$

a jelikož $g_i \notin Z(G), |H| < |G|$. Z indukčního předpokladu má H Sylowovu p-podgrupu P, která je taky podgrupou G. Navíc $|P| = p^\alpha$, takže P je Sylovova p-podgrupa G.

Důkaz 2 a 3

Nechť Q je libovolná p-podgrupa G a nechť

$$\mathcal{S} = \{gPg^{-1} | g \in G\} \overset{ozn.}{=} \{P_1, P_2, \ldots, P_r\} = \mathcal{S}. \tag{3}$$

Z definice $\mathcal{S}$ může G, tedy taky Q, působit na $\mathcal{S}$ konjugací. $\mathcal{S}$ lze proto zapsat jako sjednocení orbit akce Q:

$$\mathcal{S} = O_1 \cup O_2 \cup \cdots \cup O_s \tag{4}$$

kde $r = |O_1| + |O_2| + \cdots + |O_s|$. Je potřeba si uvědomit, že r nezávisí na Q, ale počet orbit s ano (G má z definice jenom jednu orbitu na $\mathcal{S}$, ale Q jich může mít víc). Přeuspořádáme prvky $\mathcal{S}$ tak, aby prvních s bylo reprezentanty Q-orbit: $P_i \in O_i, 1 \leq i \leq s$. Pak z věty o počtu tříd ekvivalence plyne $|O_i| = |Q : N_Q(P_i)|$. Z definice platí $N_Q(P_i) = N_G(P_i) \cap Q$ a podle předchozího lemmatu, $N_G(P_i) \cap Q = P_i \cap Q$. Celkem tedy máme

$$|O_i| = |Q : P_i \cap Q|, \quad 1 \leq i \leq s. \tag{5}$$

Pokračování

Teď můžeme ukázat, že $r \equiv 1 \mod p$. Díky libovolnosti Q můžeme položit $Q = P_1$, takže

$$|O_1| = 1, \tag{6}$$

a $\forall i > 1, P_1 \neq P_i$, tedy $P_1 \cap P_i < P_1$, proto

$$|O_i| = |P_1 : P_1 \cap P_i| > 1, \quad 2 \leq i \leq s. \tag{7}$$

Protože P_1 je p-grupa, $|P_1 : P_1 \cap P_i|$ musí být mocnina p, tedy

$$p \mid |O_i|, \quad 2 \leq i \leq s. \tag{8}$$

Odtud

$$r = |O_1| + (|O_2| + \cdots + |O_s|) \equiv 1 (mod\ p) \tag{9}$$

Nyní buď Q libovolná p-podgrupa G. Kdyby $Q \notin P_i, \forall i \in \hat{r}$, pak $Q \cap P_i < Q, \forall i$, tedy

$$|O_i| = |Q : Q \cap P_i| > 1, \quad 1 \leq i \leq s. \tag{10}$$

Tudíž $p \mid |O_i|, \forall i$ a $p \mid r$, což je spor s $r \equiv 1 \mod p$. Proto $Q \leq gPg^{-1}$, pro nějaké $g \in G$.

Pokračování

Pro důkaz ekvivalence Sylowových p-podgrup stačí za Q volit libovolnou Sylowovu p-podgrupu. Pak $Q \leq gPg^{-1}$ a zároveň $|gPg^{-1}| = |Q| = p^{\alpha}$, proto $gPg^{-1} = Q$.
Stačí si uvědomit že $\mathcal{S} = Syl_p(G)$ protože každá Sylowova p-podgrupa je konjugovaná k P, tedy $n_p = r \equiv 1 \mod p$. Nakonec díky počtu trid ekvivalence a tomu, že všechny Sylowovy p-podgrupy jsou konjugované, dostáváme

$$n_p = |G : N_G(P)|, \quad \forall P \in Syl_p(G). \tag{11}$$

Corollary

Buď P Sylowova p-podgrupa grupy G. Potom následující tvrzení jsou ekvivalentní:

1. *P je jediná Sylowova p-podgrupa v G, tedy $n_p = 1$,*
2. *$P \trianglelefteq G$.*

Důkaz.

1) $\Leftarrow$ 2): $n_p = 1$, znamená že pro všechna $g \in G$ platí $|gPg^{-1}| = |P|$, tudíž $gPg^{-1} = P$, tj. $P \trianglelefteq G$.
2)$\Leftarrow$1): $\forall g \in G, gPg^{-1} = P$. Nechť $\tilde{P} \in Syl_p(G)$. Pak $\tilde{P} = gPg^{-1} = P$. □

Použití

- $|G| < \infty$ a abelovská, pak má právě jednu Sylowovu p–podgrupu pro každé $p \mid |G|$.
- S_3 má 3 Syl_2 podgrupy ($\langle(1,2)\rangle$, $\langle(2,3)\rangle$, $\langle(1,3)\rangle$) $n_2 = (1 + k2)$ a právě jednu Syl_3 $\langle(1,2,3)\rangle$ $n_3 = (1 + k3)$ – 4 nedělí 3.
- S_4 má $n_2 = (1 + k2) = 1, 3, 5$ a $n_3 = (1 + k3) = 1, 4, 7$

.

Přímý součin grup

Jedná se o způsob konstrukce větších grup z menších.
Přímý (direktní) součin definujeme pro konečné a spočetně nekonečné množiny grup (rozdíl definice je jen formální).

1. **Přímým součinem** konečné množiny grup $(G_1, *_1)$, $(G_2, *_2)$, $\ldots (G_n, *_n)$ je grupa jejíž prvky je množina n-tic $(g_1, g_2, \ldots, g_n)$, $(h_1, h_2, \ldots, h_n)$ $(g_i, h_j \in G_i)$ s násobením definovaným po složkách.

$$(g_1, g_2, \ldots, g_n) * (h_1, h_2, \ldots, h_n) = (g_1 *_1 h_1, g_2 *_2 h_2, \ldots, g_n *_n h_n). \tag{12}$$

   Označení: $G = G_1 \times G_2 \times \ldots \times G_n$
2. **Přímým součinem** spočetné množiny grup $(G_1, *_1)$, $(G_2, *_2)$, $\ldots (G_n, *_n)$ je grupa jejíž prvky je sočetná množina $(g_1, g_2, \ldots)$, $(h_1, h_2, \ldots)$ $(g_i, h_j \in G_i)$ s násobením definovaným po složkách.

$$(g_1, g_2, \ldots) * (h_1, h_2, \ldots) = (g_1 *_1 h_1, g_2 *_2 h_2, \ldots). \tag{13}$$

Každá podgrupa $(1, 1, \ldots, g_i, 1, 1, \ldots)$ je normální. (Lze faktorizovat)
Je zřejmé, že výsledkem přímého součinu grup je opět grupa a to řádu $|G| = |G_1||G_2| \ldots |G_n|$ nebo nekonečného.

Klasifikace Abelovských grup

1. *Grupa G je **konečně generovaná**, pokud existuje konečná množina $A \subset G$ taková, že $G =< A >$.*
2. *Pro každé $r \in \mathbb{Z}$, $r \geq 0$, buď $\mathbb{Z}^r = \mathbb{Z} \times \mathbb{Z} \times \ldots \times \mathbb{Z}$ direktní součet r kopií grupy $\mathbb{Z}$, kde $\mathbb{Z}^0 = e$. Grupa $\mathbb{Z}^r$ se nazývá **volná Abelovská grupa řádu** r.*

Theorem (základní věta Abelovských grup)

Buď G konečně generovaná Abelovská grupa. Pak:

1. *$G \cong \mathbb{Z}^r \times Z_{n_1} \times Z_{n_2} \times \ldots \times Z_{n_s}$ pro nějaká celá čísla splňující následující podmínky:*
   1. *$r \geq 0$ a $n_j \geq 2$ pro všechna j,*
   2. *$n_{i+1} | n_i$ pro $1 \leq i \leq s-1$,*
2. *tento rozklad je jednoznačný.*

Důkaz.

Bude zřejmé později. □

$\Rightarrow$ Každý prvočíselný dělitel $|G|$ musí dělit n_1.

Důsledek:
Je–li $n = p_1 p_2 p_3 \dots p_k$ součin k různých prvočísel, potom keždá abelovská grupa řádu n je izomorfní Z_n

Example

Nechť $n = 180 = 2^2 \cdot 3^2 \cdot 5$, potom máme možnosti:

1. $n_1 = 180$ – grupa Z_{180}
2. $n_1 = 2^2 \cdot 3 \cdot 5,\ n_2 = 3$ – grupa $Z_{60} \times Z_3$
3. $n_1 = 2 \cdot 3^2 \cdot 5\ n_2 = 2$ – grupa $Z_{90} \times Z_2$
4. $n_1 = 2 \cdot 3 \cdot 5\ n_2 = 6$ – grupa $Z_{30} \times Z_6$

A toto jsou všechny možnosti neizomorfních abelovských grup řádu 180.

Věta se dá ekvivalentně napsat násedujícím způsobem.

Rozklad abelovské grupy podle Sylowových podgrup

Podgrupy abelovské grupy jsou normální, každá Sylowova daného řádu je právě jedna .

Theorem

Buď G abelovská grupa řádu $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, kde p_k jsou různá prvočísla. Potom

1. $G \cong A_1 \times A_2 \times \ldots \times A_k$, *kde* $|A_i| = p_i^{\alpha_i}$,
2. *pro každé* $A_i \in A_1, A_2, \ldots, A_k$, *kde* $|A_i| = p^{\alpha_i}$ *je* $A \simeq Z_{p^{\beta_1}} \times Z_{p^{\beta_2}} \times \ldots \times Z_{p^{\beta_t}}$, *kde* $\beta_1 \geq \beta_2 \geq \ldots \geq \beta_t \geq 1$ *a* $\beta_1 + \beta_2 + \ldots + \beta_t = \alpha$ *(t a* β_j *závisí na i)*
3. *a rozklad v 1) a 2) je jednoznačný až na pořadí* A_i.

Všimněte si, že $p_i^{\beta_{t+1}}$ dělí $p_i^{\beta_t}$.

Example

Nechť $n = 180 = 2^2 \cdot 3^2 \cdot 5$, potom máme dle této věty možnosti:

1. $p^\beta = 2^2$, β má rozklad 2 nebo 1,1 a tomu odpovídají abelovské grupy $\mathbb{Z}_4$ a $\mathbb{Z}_2 \times \mathbb{Z}_2$
2. $p^\beta = 3^2$, β má rozklad 2 nebo 1,1 a tomu odpovídají abelovské grupy $\mathbb{Z}_9$ a $\mathbb{Z}_3 \times \mathbb{Z}_3$
3. $p^\beta = 5^1$ β má rozklad 5 a tomu odpovídá abelovská grupa $\mathbb{Z}_5$.

Možné abelovské grupy potom dostaneme tak, že z každého bodu vezmeme jednu možnost.

1. $\mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{180}$
2. $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{60} \times \mathbb{Z}_3$
3. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{90} \times \mathbb{Z}_2$
4. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{30} \times \mathbb{Z}_6$

Theorem

Nechť $m, n \in \mathbb{Z}^+$, *pak* $\mathbb{Z}_m \times \mathbb{Z}_n \simeq \mathbb{Z}_{mn} \Leftrightarrow \gcd(m, n) = 1$ *(tj. m a n jsou nesoudělná).*

Důkaz.

⇒) *Nechť* $\mathbb{Z}_m =< x >$, $\mathbb{Z}_n = y$ *a* l *nejmenší společný násobek l.c.m.* (m, n) . *Všimneme si, že* $l = mn$, *právě když g.c.d* $(m, n) = 1$. *Dále nechť* $x^a y^b \in \mathbb{Z}_m \times \mathbb{Z}_n$ *libovolné, pak*

$$(x^a y^b)^l = x^{la} y^{lb} = e^a e^b = e,$$

protože $m \mid l$ *a taky* $n \mid l$. *Pokud g.c.d* $(m, n) \neq 1$, *každý element* $\mathbb{Z}_m \times \mathbb{Z}_n$ *je řádu nanejvýš* l, *tedy ostře menšího než mn, tedy* $\mathbb{Z}_m \times \mathbb{Z}_n$ *nemůže být isomorfní* $\mathbb{Z}_{mn}$.

⇐) *Naopak, pokud g.c.d.* $(m, n) = 1$, *pak* $|xy| = (|x|, |y|) = mn$. *Tudíž* $\mathbb{Z}_m \times \mathbb{Z}_n =< xy >$.

□

Theorem

Nechť $H, K \leq G$. Počet různých způsobů, jak napsat libovolný element z HK ve tvaru hk pro nějaké $h \in H$ a $k \in K$, je $|H \cap K|$. Speciálně když $H \cap K = e$, pak pro každý element existuje pouze jeden způsob.

Důkaz.

Nechť $x \in HK$ a $y \in H \cap K$ libovolné, pak $x = yy^{-1}x = yz$, kde $z = y^{-1}x$ je element H nebo K. Takže existuje alespoň $|H \cap K|$ možností, jak zvolit y. Kdyby existovalo $x \in HK$, které lze zapsat více různými způsoby než $H \cap K$, pak celkový počet způsobů, jak zapsat všechny prvky, by byl větší než

$$|HK||H \cap K| = \frac{|H||K|}{|H \cap K|}|H \cap K| = |H||K|,$$

což je spor s růzností zápisu. □

Theorem

Nechť $H, K \trianglelefteq G$ a $H \cap K = e$, pak $HK \simeq H \times K$.

Důkaz.

Protože $H, K \trianglelefteq G$, je $HK \leq G$. Nechť $h \in H$, $k \in K$. Protože $H \trianglelefteq G$, platí $k^{-1}hk \in H$, tedy taky $h^{-1}(k^{-1}hk) \in H$. Analogicky, $(h^{-1}k^{-1}h)k \in K$. Dále díky tomu, že $H \cap K = e$, máme $h^{-1}k^{-1}hk = e$, tedy $hk = kh$, takže prvky H komutují s prvky K. Podle předcházející věty lze každý prvek HK zapsat právě jedním způsobem ve tvaru hk, kde $h \in H$ a $k \in K$. Zobrazení

$$\varphi : HK \to H \times K : hk \mapsto (h, k)$$

je proto dobře definované. Že φ je homomorfismus: $h_1, h_2 \in H$ a $k_1, k_2 \in K$. Pak díky tomu, že prvky H a K spolu komutují, platí $(h_1k_1)(h_2k_2) = (h_1h_2)(k_1k_2)$ a tento tvar je jednoznačně zapsán ve tvaru hk, kde $h \in H$, $k \in K$. Takže

$$\varphi(h_1k_1h_2k_2) = \varphi(h_1h_2k_1k_2) = (h_1h_2, k_1k_2) = (h_1, k_1)(h_2, k_2) = \\ = \varphi(h_1k_1)\varphi(h_2k_2),$$

tedy φ je homomorfismus a protože stejného řádu φ je isomorfizmus. □

Nalezení direktního součinu podgrup v grupě

V G najdeme $H, K \trianglelefteq G$ tak, že $H \cap K = e$. Potom $HK \simeq H \times K$
V abelovských grupách je ukázáno.

Jak u nekomutativních grup?
Nechť $x, y \in G,\ A, B \subseteq G,\ A, B \neq \emptyset$
Definice:

1. Komutátor prvků x, y je $[x, y] = x^{-1}y^{-1}xy$
2. Podgrupa generovaná komutátory prvků z A a B je $[A, B] = \{< [a, b] > | \forall a \in A, b \in B\}$
3. Komutátorová podgrupa $G' = \{< [x, y] > | \forall x, y \in G\}$

Theorem

Nechť $x, y \in G,\ H \leq G$, *potom*

1. $xy = yx[x, y]$
2. $H \trianglelefteq G \Leftrightarrow [H, G] \leq H$
3. $\sigma([x, y]) = [\sigma(x), \sigma(y)]$ *pro všechny automorfismy* $\sigma \in Aut\,(G)$, G' *je charakteristické v* G *a* G/G' *je abelovská*
4. G/G' *je největší abelovská faktor grupa, tj. pokud* $H \trianglelefteq G$ *a* G/H *je abelovská, potom* $G' \leq H$.
5. *Pokud* $\varphi : G \to A$ *je libovolný homohorfismus do abelovská grupy* A, *potom* $G' \leq Ker\ \varphi$

Důkaz

1. Z definice
2. $H \trianglelefteq G \Leftrightarrow ghg^{-1} \in H \Leftrightarrow \exists \overline{g} = g^{-1},\ \overline{g}^{-1} h \overline{g} \in H \Leftrightarrow h^{-1}\overline{g}^{-1} h \overline{g} \in H$
3. Že je abelovská

$$(xG')(yG') = (xyG') = (yxx^{-1}y^{-1}G') = (yxG') = (yG')(xG')$$

4. $(xH)(yH) = yHxH$ dále
   $H = (xH)^{-1}(yH)^{-1}(xH)(yH) = x^{-1}y^{-1}xyH = [x,y]H$ pro všechna $x, y \in G \Rightarrow G' \leq H$. Platí i obráceně.
5. Protože je maximální abelovská a z předchozího důkazu.