Grupy a reprezentace 7

Zpracováno s pomocí poznámek J. Mareše

wiki-skripta

Použití Sylowovy věty: Grupa řádu pq

Example

Nechť p, q jsou prvočísla $p < q$ $|G| = pq$ a nechť $P \in Syl_p(G)$ a $Q \in Syl_q(G)$, potom

1. $Q \trianglelefteq G$
2. Pokud také $P \trianglelefteq G$, pak G je cyklická

Ad 1) $n_q = 1 + kq,\ n_q | p \ \Rightarrow n_q = 1 \Rightarrow Q \trianglelefteq G$

Ad 2) Jelikož $n_p | q$ prvočíslo, potom $n_p = 1$, nebo q. Pokud $n_p = 1$ pak $P \trianglelefteq G,\ G = PQ \simeq P \times Q \simeq \mathbb{Z}_p \times \mathbb{Z}_q \simeq \mathbb{Z}_{pq}$.

Použití Sylowovy věty: Grupa řádu 30

Example

Předpokládejme $|G| = 30$. Ukážeme, že má normální podgrupu izomorfní grupě $\mathbb{Z}_{15}$.
Každá podgrupa řádu 15 je normální a podle předchozího příkladu je abelovská, stačí dokázat, že vždy existuje taková podgrupa.
Nechť $P \in Syl_5(G)$ a $Q \in Syl_3(G)$. Je-li jedna z nich normální, pak PQ je podgrupa řádu 15. Pokud není ani jedna z nich normální, pak $n_5 = 6$ a $n_3 = 10$.
Průnik různých Sylowovych podgrup řádu 5 i řádu 3 (jsou cyklické) je jednotkový element (Lagrangeova věta).
Z toho plyne že máme v tomto případě bychom potřebovali $(6.4) + (10.2) = 44$ různých prvků v grupě. Nesmysl $\Rightarrow n_p \vee n_q = 1$, ale protože $PQ \trianglelefteq G$ musí být obě jsou normální, tj $n_p = n_q = 1$.

Použití Sylowovy věty:Grupa řádu $p^2 q$

Example

Grupa řádu $p^2 q$ má normální Sylowovu podgrupu. Nechť $P \in Syl_p(G)$ a $Q \in Syl_q(G)$.

1. $p > q,\ n_p = 1 + kp,\ n_p | q \ \Rightarrow n_p = 1$ a $P \trianglelefteq G$.
2. $p < q,\ \ n_q = 1 + lq$. Pokud $n_q = 1$ je $Q \trianglelefteq G$. Pokud $n_q > 1,\ n_q | p^2$, tj. $n_q = p^2$ nebo $n_q = p$. Ale $q > p,\ \Rightarrow q = p^2$, tedy

$$lp = p^2 - 1 = (p - 1)(p + 1).$$

Jelikož $q > p$ tak $q = p + 1$ a to je možné pro $p = 2,\ \ q = 3$, tj. grupa řádu 12, u ostatních je $n_q = 1$ a $Q \trianglelefteq G$.
Grupa řádu $12 = 2^2.3$ má $n_3 = 1$ nebo $n_3 = 4$. Je-li $n_3 = 4$ je to $4 \times 2 = 8$ prvků řádu 3. V tom případě Syl_2 podgrupa řádu 4 obsahuje všechny zbylé prvky a je právě jedna.

Použití Sylowovy věty: Grupa řádu 12

Example

Nechť$|G| = 12$. Ukážeme, že buď má normální Sylowovu 3–podgrupu nebo je izomorfní grupě A_4.
Pro $n_3 = 1$ je podgrupa normální. Nechť $n_3 = 4$. Průnik Syl podgrup je e a obsahují $2.4 = 8$ různých prvků řádu 3, $|G : N_G(P)| = n_3 = 4$. A protožr P normalizuje sama sebe $N_G(P) = P$.
Vezměme akci grupy G na podmnožině $Syl_3(G)$, té odpovídá permutační reprezentace

$$\varphi : G \to S_4,$$

jádro akce nepřehazuje P_i, tudíž musí být podgrupou normalizátorů všech P_i a to je jenom e.Takže φ je injektivní.

$$G \simeq \varphi(G) \leq S_4.$$

Podgrupa řádu 12 v S_4, která obsahuje 8 prvků řádu 3 je A_4,

$$\varphi(G) = A_4, \quad G \simeq A_4.$$

Použití Sylowovy věty: Grupa řádu 60

Corollary

Mějme grupu $|G| = 60$. Má–li více jak jednu Sylowovu 5–podgrupu, potom G je prostá.

Důkaz sporem.

Nechť $n_5 > 1$ a existuje netriviální $H \trianglelefteq G$. Pak $n_p = 6$ a $|N_G(P)| = 10$ Protože index normalizátoru je počet konjugovaných.
Pokud $5 \mid |H|$ pak H musí obsahovat všech 6 Syl_5 podgrup $|H| \geq 1 + 6.4 = 25$ a $|H| \mid 60$, takže $|H| = 30$, ale grupa řádu 30 má pouze jednu normální Syl_5 podgrupu a to je spor, tzn. $5 \nmid |H|$.
Pokud $5 \nmid |H|$.
Nechť $|H| = 6$ nebo 12, pak H má charakteristickou (normální) právě jednu Syl podgrupu, která je normální i v G. Vezměme jednu z char podgrup H, $K \trianglelefteq H$, $|K| = 2, 3, 4$ a faktor grupu $\overline{G} = G/K$, $|\overline{G}| = 30, 20, 15$. $\overline{G}$ má normální podgrupu $\overline{L} \trianglelefteq \overline{G}$ řádu 5 dle předchozího.$L/K \trianglelefteq G/K$, 4.VOI $L \trianglelefteq G$ a $5 \mid |L|$. Spor $L \trianglelefteq H$. □

Závěr: A_5 je prostá. (12345) a (13425) jsou generátory různých Syl_5 podgrup.

Polopřímý součin

Polopřímý součin je další způsob, jak nebo studovat strukturu grupy nebo jak z menších grup vyrobit grupu větší jejich složením. Ve výsledku dostaneme z grup H a K grupu G, ve které bude platit $H \trianglelefteq G$, ale $K \leq G$ nemusí být normální.
Jako motivaci si vezměme přímý součin. Předpokládejme, že už máme G a platí $H \cap K = e$. Dále $HK \leq G$ a existuje bijekce mezi prvky HK a dvojicemi (h, k), kde $h \in H$ a $k \in K$. Chceme-li součin dvou prvků z HK opět napsat ve tvaru hk, postupujeme takto:

$$(h_1 k_1)(h_2 k_2) = h_1 k_1 h_2 (k_1^{-1} k_1) k_2 = h_1 (k_1 h_2 k_1^{-1}) k_1 k_2 = h_1 h_3 k_3 = h_4 k_3,$$

kde jsme využili toho, že H je normální podgrupa. **Důležité je, že výraz** $(k_1 h_2 k_1^{-1})$ **vyjadřuje zobrazení prvku** h_2 **automorfismem podgrupy** H.
Cílem polopřímého součinu je zavést grupu s obdobným násobením bez „zastřešující“ grupy, která nám umožňuje násobit mezi sebou prvky z K a H.

Theorem

Buďte H a K grupy a $\varphi : K \to \mathrm{Aut}\, H$ je homomorfismus (každému prvku $k \in K$ přiřadí nějakou permutaci H). Dále buď $\cdot$ akce grupy K na H daná vztahem $\varphi(k)h = k \cdot h$. Buď G množina dvojic (h, k), $h \in H$ a $k \in K$ a definuje násobení těchto dvojic jako:

$$(h_1, k_1)(h_2, k_2) = (h_1 k_1 \cdot h_2, k_1 k_2).$$

1. *G s takto definovanou operací je grupa řádu $|G| = |K||H|$.*
2. *Množiny $\{(h, 1) | h \in H\}$ a $\{(1, k) | k \in K\}$ jsou podgrupy G isomorfní grupám H a K. (Dále mezi nimi nerozlišujeme.)*
3. *$H \trianglelefteq G$.*
4. *$H \cap K = e$.*
5. *$(\forall h \in H, k \in K)(khk^{-1} = k \cdot h)$.*

Důkaz.

1. Asociativita platí, protože pro libovolné $(a, x), (b, y), (c, z) \in G$ platí

$$\begin{aligned} ((a,x)(b,y))(c,z) &= (ax \cdot b, xy)(c,z) &&= (ax \cdot b(xy) \cdot c, xyz) \\ &= (ax \cdot bx \cdot (y \cdot c), xyz) &&= (ax \cdot (by \cdot c), xyz) \\ &= (a,x)(by \cdot c, yz) &&= (a,x)((b,y)(c,z)). \end{aligned}$$

   Platnost 3. rovnosti mezi odpovídá axiomu homomorfismu $\varphi(b)\varphi(y \cdot c) = \varphi(b(y \cdot c))$. Dále je z definice vidět, že $(1, 1)$ je jednotkový prvek, $(h, k)^{-1} = (k^{-1} \cdot h^{-1}, k^{-1})$ je inverzní prvek pro libovolné $(h, k) \in G$ a $|G| = |H||K|$.

2. Nechť $\tilde{H} = \{(h, 1) | h \in H\}$ a $\tilde{K} = \{(1, k) | k \in K\}$. Máme

$$(a, 1)(b, 1) = (a1 \cdot b, 1) = (ab, 1), \qquad \forall a, b \in H.$$

   Analogicky,

$$(1, x)(1, y) = (1, xy), \qquad \forall x, y \in K,$$

   takže $\tilde{H}, \tilde{K} \leq G$ isomorfní H, K.

Důkaz.

4. Je jasné, že $\tilde{H} \cap \tilde{K} = e$.
5. Dále platí

$$\begin{aligned}(1,k)(h,1)(1,k)^{-1} &= ((1,k)(h,1))(1,k^{-1}) \\ &= (k \cdot h, k)(1,k^{-1}) \\ &= (k \cdot hk \cdot 1, kk^{-1}) \\ &= (k \cdot h, 1),\end{aligned}$$

tedy přiřazením $h \leftrightarrow (h,1)$ a $k \leftrightarrow (1,k)$ z bodu (2.) dostáváme $khk^{-1} = k \cdot h$.

3. Nakonec, protože $K \leq N_G(H)$, platí $G = HK$ a zároveň $H \leq N_G(H)$, dostáváme $N_G(H) = G$, tedy $H \trianglelefteq G$.

□

Definice polopřímého součinu

*Grupu G z předchozí věty nazýváme **polopřímý součin** grup H a K vzhledem k homohorfismu φ a značíme $H \rtimes_\varphi K$.*

Theorem

Nechť $H, K \leq G$ tak, že

1. $H \trianglelefteq G$
2. $H \cap K = e$
3. $\varphi : K \to Aut(H)$ *je homomorfismus levou konjugací v* H, $\varphi \mapsto k \sqcup k^{=1}$

Potom $HK \simeq H \rtimes_\varphi K$
Speciálně : je-li $G = HK$ *a jsou-li splněny podmínky 1) a 2) potom* $G = H \rtimes_\varphi K$

Důkaz.

$H \trianglelefteq G \Rightarrow HK \leq G$, *každé* $x \in HK$ *může být zapsáno právě jedním způsobem* $x = hk$; *tj. existuje bijekce*

$$(hk) \mapsto (h, k),\ HK \mapsto H \rtimes_\varphi K$$

$\square$

Použití ke klasifikaci grup řádu n

1. najít $G = HK$, $H \cap K = 1$ a $H \trianglelefteq K$
2. pro různé páry H a K najít všechny izomorfismy
3. pro každý pár H, K najít homomorfismus $\varphi : K \to Aut(H)$ (homomorfismů může být více)
4. pro každou trojici K, K, φ vytvořit $H \rtimes_\varphi K$ a vybrat neizomorfní.

Example

- Dihedrální grupa $D_n \simeq \mathbb{Z}_n \rtimes_\varphi \mathbb{Z}_2$.
  $\varphi_s(r) = srs^{-1} = r^{-1}$, $\varphi_{s^2}(r) = \varphi_e(r) = r$
- Grupa řádu pq, $p < q$
  Měli jsme $P \in Syl_p(G)$ a $Q \in Syl_q(G)$, potom $Q \trianglelefteq G$ a P a Q jsou cyklické. $Aut(Q)$ je cyklická řádu $q-1$, tj. všechny automorfismy jsou $q^i \mapsto q^{ik}$ $k = 1, 2, \dots, q-1$. (pro $k = 0$ není automorfismus) Pokud $p \nmid q-1$, potom φ je pouze identita a neexituje polopřímý součin (obraz homomorfismu do grupy $Aut(Q)$ je podgrupa), G je abelovská. Nechť $p \mid q-1$, a $P = \langle y \rangle$ potom $Aut(Q)$ obsahuje podgrupu řádu p generovanou $\langle \gamma \rangle$ a máme množinu p homomorfismů $\varphi_k(y) = \gamma^k$, $k = 0, 1, \dots p-1$, přičemž $\varphi_0(y)$ je triviální a ostatní jsou izomorfní.

*Buďte G grupa a V vektorový prostor nad tělesem T. Potom **lineární reprezentací** grupy G na prostoru V nazýváme každý homomorfismus $T : G \to GL(V)$, který každému prvku $g \in G$ přiřazuje lineární zobrazení $T(g)$ takové, že $(\forall g, h \in G)(T(g)T(h) = T(gh))$.*

- *Prostor V nazýváme **reprezentativní prostor** a jeho dimenzi **rozměr** reprezentace.*
- *Je-li navíc T injektivní, nazýváme takovou reprezentaci **věrnou**.*
- *Je-li $\dim V < \infty$ (existuje tedy konečná báze V), mluvíme o **maticové** reprezentaci.*

Unitární reprezentace

- *T je vždy věrnou reprezentací faktor grupy $G/\mathrm{Ker}\ T$.*
- *Prostá grupa má jen věrné reprezentace (kromě triviální).*

Je-li $\mathcal{H}$ Hilbertův prostor a T homomorfismus grupy G do množiny unitárních operátorů na $\mathcal{H}$, nazýváme T ***unitární*** *reprezentací G na $\mathcal{H}$.*

Dvě reprezentace $T : G \to V$ a $T' : G \to V'$ nazýváme ***ekvivalentní****, pokud existuje lineární isometrie $A : V \to V'$ taková, že $\forall g \in G$ platí $T'(g) = AT(g)A^{-1}$ a je-li navíc A unitární, říkáme, že reprezentace jsou* ***unitárně ekvivalentní****. (izometrie : $\|A\varphi\| = \|\varphi\|, \forall \varphi \in V$)*

Pro maticové reprezentace jde o změnu báze.

Lemma (Hilbert)

Každá maticová reprezentace grupy je ekvivalentní unitární reprezentaci.

Důkaz.

Konstrukcí: Buď A_i matice reprezentující prvek $g_i \in G$. Sestrojíme nejprve hermitovskou matici $H = \sum_{i=1}^{r} A_i A_i^{\dagger}$. Hermitovské matice můžeme diagonalizovat pomocí unitární matice U. Nechť tato diagonalizované matice je:

$$D = U^{-1} H U = \sum_i U^{-1} A_i A_i^{\dagger} U = \sum_i U^{-1} A_i U U^{-1} A_i^{\dagger} U = \sum_i A_i' A_i'^{\dagger},$$

kde jsme označili $A_i' = U^{-1} A_i U$. Rozpisem poslední sumy

$$\sum_i A_i' A_i'^{\dagger} = \sum_i \sum_j (A_i')_{kj} (A_i'^{\dagger})_{jk} = \sum_i \sum_j |(A_i')_{kj}|^2$$

zjišťujeme, že diagonální členy D jsou kladné, protože jednou z matic A_i' je identita (člen $j = k$). $\square$

Důkaz.

Proto můžeme vytvořit matice $D^{\frac{1}{2}}$ a $D^{-\frac{1}{2}}$. Potom z definice zřejmě platí:

$$I = D^{-\frac{1}{2}} \sum_i A'_i A'^{\dagger}_i D^{-\frac{1}{2}}.$$

Nyní již definujeme matice finální reprezentace $A''_i = D^{-\frac{1}{2}} A'_i D^{\frac{1}{2}}$, o kterých ukážeme, že jsou unitární:

$$\begin{aligned} A''_j A''^{\dagger}_j &= D^{-\frac{1}{2}} A'_j D^{\frac{1}{2}} I D^{\frac{1}{2}} A'^{\dagger}_j D^{-\frac{1}{2}} = \\ &= D^{-\frac{1}{2}} A'_j D^{\frac{1}{2}} D^{-\frac{1}{2}} \sum_i A'_i A'^{\dagger}_i D^{-\frac{1}{2}} D^{\frac{1}{2}} A'^{\dagger}_j D^{-\frac{1}{2}} = \\ &= D^{-\frac{1}{2}} \sum_i A'_j A'_i (A'_j A'_i)^{\dagger} D^{-\frac{1}{2}} = \\ &= D^{-\frac{1}{2}} \sum_k A'_k A'^{\dagger}_k D^{-\frac{1}{2}} = I. \end{aligned}$$

Tím je důkaz dokončen. □

Reducibilní a ireducibilní reprezentace

*$V_1 \subset V$ se nazývá **invariantní** podprostor příslušný operátoru A, když $(\forall \varphi \in V_1)(A\varphi \in V_1)$, tedy $A(V_1) \subset V_1$. Pokud se nejedná o triviální invariantní podprostor, nazývá se takový podprostor **vlastní**.*

*Říkáme, že T je **ireducibilní** reprezentace grupy G na prostoru V, pokud neexistuje vlastní invariantní podprostor V příslušný všem operátorům $T(g)$ pro všechna $g \in G$. Tedy $(\forall g \in G)(T(g)(V_1) \subset V_1) \Rightarrow (V_1 = 0 \vee V_1 = V)$. V opačném případě se reprezentace nazývá **reducibilní**.*

Reprezentace je ireducibilní, pokud neexistuje taková podobnostní transformace, která by převedla současně všechny $T(g)$ na blokově diagonální tvar.

*Reducibilní reprezentace, kterou je možné napsat jako direktní součet ireducibilních reprezentací se nazývá **úplně reducibilní**.*

Theorem

Buď T unitární reprezentace grupy G na Hilbertově prostoru $\mathcal{H}$. Potom:

1. *Ortogonální doplněk k $\mathcal{H}_1$ (označme $\mathcal{H}_2$) je invariantní podprostor $\Leftrightarrow$ $\mathcal{H}_1$ je invariantní podprostor.*
2. *$\mathcal{H}_1 \subset \mathcal{H}$ je invariantní podprostor $\Leftrightarrow$ projektor E_1 na $\mathcal{H}_1$ splňuje podmínku: $(T(g)E_1 = E_1 T(g))(\forall g \in G)$.*

Důkaz.

1. *Nechť $\psi_1 \in \mathcal{H}_1$ a $\psi_2 \in \mathcal{H}_2$, pak z předpokladu máme $T(g)|\psi_1\rangle \in \mathcal{H}_1 = \mathcal{H}_2^\perp$ a platí*

$$\langle\psi_2|T(g)\psi_1\rangle = 0 = \langle T^\dagger(g)\psi_2|\psi_1\rangle. \tag{1}$$

2. *Můžeme psát $\mathcal{H} = \mathcal{H}_1 \oplus \mathcal{H}_2$, tedy $\forall|\psi\rangle \in \mathcal{H}$ platí $|\psi\rangle = |\psi_1\rangle + |\psi_2\rangle$, kde $|\psi_1\rangle \in \mathcal{H}_1$ a $|\psi_2\rangle \in \mathcal{H}_2$.*

$\Rightarrow$) *Předpokládáme, že $\mathcal{H}_1$, a z předchozího bodu též $\mathcal{H}_2$, jsou invariantní.*

$$E_1 T(g)|\psi\rangle = E_1 T(g)|\psi_1\rangle + E_1 T(g)|\psi_2\rangle = E_1 T(g)E_1|\psi\rangle = T(g)E_1|\psi\rangle. \tag{2}$$

$\Leftarrow$) *Z rovnosti $E_1 T(g)|\psi\rangle = T(g)E_1|\psi\rangle$ plyne že $T(g)\mathcal{H}_1 \subset \mathcal{H}_1$.*

Corollary (Maschke)

Reducibilní unitární reprezentace je úplně reducibilní.

Theorem

Každá unitární ireducibilní reprezentace konečné grupy má konečnou dimenzi $n \leq |G|$. Span$\{T(g_i)|\psi_1\rangle\}, \; i = 1, \ldots, n$ je invariantní díky homomorfismu.

Důkaz.

$\psi_1 \in \mathcal{H}, \; \psi_\infty \neq \emptyset$ $\square$