Silovljeve teoreme

Def. 1. Za proizvoljnu grupu G, $H < G$ je p-podgrupa ako je H p-grupa, p je prost broj.

2. $H < G$ je Silovljeva p-podgrupa akko je H maksimalna p-podgrupa grupe G.

I Silovljeva teorema

Neka je G konačna grupa reda $p^n \cdot m$, $(p, m) = 1$. Tada postoji $H < G$ takva da je $|H| = p^n$.

Dalje, prema Prvoj Silovljevoj teoremi i Lagrangeovoj teoremi, ako je $|G| = p^n \cdot m$, $(p, m) = 1$, onda je Silovljeva podgrupa reda p^n. Silovljeve teoreme su strukturne teoreme teorije grupa i omogućavaju kombinatornu analizu strukture konačnih grupa, pre svega nekomutativnih.

Primer Neka je $|G| = 12 = 2^2 \cdot 3$. Tada G sadrži podgrupe H, K, $|H| = 2^2$, $|K| = 3$. Primetimo da je $H \cap K < H, K$ pa kako $(|H|, |K|) = 1$, prema Lagrangeovoj teoremi, $|H \cap K| = 1$. Otuda i prema jednakosti $|HK| \cdot |H \cap K| = |H| \cdot |K|$, sledi $|HK| = 12$, tj. $G = HK$.

Dokaz Prve Silovljeve teoreme Dokaz izvodimo potpunom indukcijom po broju elemenata grupe $|G|$ i pri tome koristimo klasovnu jednakost:

$$(KJ) \qquad |G| = |Z(G)| + \sum_{x \in T,\ x \notin Z(G)} |G : \mathbb{C}(x)|$$

Neka je $|G| = p^n \cdot m$, $(p, m) = 1$, $n \geq 1$, $p \in$ Prost i pretpostavimo

(IH) Silovljeva teorema važi za sve grupe $|H|$, $|H| < |G|$.

Razlikujemo dva slučaja:

(1) $p^n \mid |\mathbb{C}(x)|$ za neki $x \in T$, $x \notin Z(G)$.

Tada je $\mathbb{C}(x)$ prava podgrupa grupe G, dakle $|\mathbb{C}(x)| < |G|$, pa prema IH $\mathbb{C}(x)$ sadrži Silovljevu podgrupu H reda p^n. Naravno, tada je H Silovljeva podgrupa grupe G.

(2) Ni za jedno $x \in T$, $x \notin Z(G)$, $p^n \mid |G(x)|$ (negacija H.(4)).
Kako vazi $p^n \mid |G| = |C(x)| \cdot |G : C(x)|$, to u ovom slucaju, tj. za $x \in T$, $x \notin Z(G)$, $p \mid |G : C(x)|$, pa

$$p \mid \sum_{x \in T,\, x \notin Z(G)} |G : C(x)|$$

, te prema (KJ) sledi

$p^n m = |Z(G)| + \alpha p$ za neko $\alpha \in \mathbb{N}$.

Otuda $p \mid |Z(G)|$ pa, s obzirom da je $Z(G)$ Konačna Abelova grupa prema Kašijevoj lemi za Abelove grupe, postoji $a \in Z(G)$, $\text{red}(a) = p$.

Tada $\langle a \rangle < Z(G)$, pa $\langle a \rangle \lhd G$, te je $G/\langle a \rangle$ dobro definisana grupa i

$$\text{red}(G/\langle a \rangle) = |G| / |\langle a \rangle| = p^n \cdot m / p = p^{n-1} m.$$

Prema (IH), $G/\langle a \rangle$ ima Silovljevu podgrupu K reda p^{n-1}. Neka je $k : G \to G/\langle a \rangle$ kanonski homomorfizam i neka je $H = k^{-1}(K)$. Tada je H Silovljeva podgrupa reda p^n grupe G. Zaista, neka je $K = \{h_i \langle a \rangle \mid 1 \le i \le p^{n-1}\}$ gde su $h_i \langle a \rangle$ disjunktni kosetи podgrupe $\langle a \rangle < G$.

$k : x \longmapsto \dot{x}\langle a \rangle$, $\dot{x} \in G$

Dalje,

$$\begin{aligned} x \in H &\iff x \in k^{-1}(K) \\ &\iff k(x) \in K \\ &\iff x\langle a \rangle = h_i \langle a \rangle \text{ za neko } i \\ &\iff h_i^{-1} x \in \langle a \rangle \text{ za neko } i \\ &\iff h_i^{-1} x = a^j \text{ za neke } i, j \\ &\iff x = h_i a^j \text{ za neke } i, j, \end{aligned}$$

tj.

$$H = \bigcup_{1 \le i \le p^{n-1}} h_i \langle a \rangle$$

i to je disjunktna unija, pa

$$|H| = \sum_{1 \le i \le p^{n-1}} |h_i \langle a \rangle| = \sum_{1 \le i \le p^{n-1}} |\langle a \rangle| = p^{n-1} \cdot |\langle a \rangle| = p^{n-1} p = p^n,$$

budući smo koristili činjenicu da svaki kaset $h_i \langle a \rangle$ ima isti broj elemenata kao i podgrupa $\langle a \rangle$, tj. p.
Dakle, H je Silovljeva p-podgrupa grupe G reda p^n ▨

Primer 1. Opisati grupe reda 6.

Rešenje: Pastoje bar dve međusobno neizomorfne grupe reda 6, to su $\mathbb{C}_6 = \mathbb{C}_2 \times \mathbb{C}_3$ i $\mathbb{S}_3 = \mathbb{D}_3$.

Dokazujemo da je svaka grupa reda 6 izomorfna jednoj od ove dve grupe. Neka je G grupa reda 6. Prema Kozi-Silovljevoj teoremi, postoje $a, b \in G$, $red(a) = 2$, $red(b) = 3$. Kako je $|G : \langle b \rangle| = 6 : 3 = 2$, to je $\langle b \rangle \lhd G$, pa

$ab = b^i a$, $i \in \{0, 1, 2\}$. Tada $i \neq 0$ (jer inače $b = 1$, $\#$), pa (1) $ab = ba$ ili (2) $ab = b^2 a$.

Dalje $|\langle a \rangle \langle b \rangle| \cdot |\langle a \rangle \cap \langle b \rangle| = |\langle a \rangle| \cdot |\langle b \rangle|$, pa $|\langle a \rangle \langle b \rangle| = 6$, odakle $G = \langle a \rangle \langle b \rangle$ tj. G je generisana elementima a, b. Otuda u slučaju (1), G je Abelova, dok je u slučaju (2) $G \cong \mathbb{S}_3$ (videti zadatak na ovu temu).

Primer 2. Opisati sve grupe reda $2p$, p je prost broj.

Rešenje (1) $p = 2$, tada $G \cong \mathbb{C}_4$ ili $G \cong \mathbb{C}_2^2$.

(2) Neka je $p > 2$. Tada imamo bar dve međusobno neizomorfne grupe reda $2p$, to su $\mathbb{C}_{2p} = \mathbb{C}_2 \times \mathbb{C}_p$ i $\mathbb{D}_p$.

Svaka grupa reda $2p$ izomorfna je jednoj od ovih dveju grupa. Zaista, neka je G grupa reda $2p$ i neka su $a, b \in G$, $red(a) = 2$, $red(b) = p$. Tada

(a) $G = \langle a \rangle \langle b \rangle$ jer je $|\langle a \rangle \langle b \rangle| \cdot |\langle a \rangle \cap \langle b \rangle| = |\langle a \rangle| \cdot |\langle b \rangle|$

(b) $\langle b \rangle \lhd G$ jer $|G : \langle b \rangle| = 2$.

Otuda $ab = b^i a$ za neko $i \in \{1, 2, \ldots, p-1\}$, tj. $\sigma_a(b) = b^i$, pa $b = i(b) = \sigma_{a^2}(b) = \sigma_a^2(b) = \sigma_a(b^i) = (b^i)^i = b^{i^2}$, tj. $i^2 = 1 \mod p$, odakle je $i \in \{1, -1\}$ (jer je $\mathbb{Z}_p$ polje!).

Slučaj $i = 1$ $ab = ba$, tj. G je Abelova te $G \cong \mathbb{C}_{2p}$.

Slučaj $i = 2$ $ab = b^{-1}a = b^{p-1}a$, tj. $G \cong \mathbb{D}_p = \langle \rho, \sigma \rangle$ ∎

Dakle, grupe reda 10: $\mathbb{C}_{10}$, $\mathbb{D}_5$; grupe reda 14: $\mathbb{C}_{14}$, $\mathbb{D}_7$.

U daljem izlaganju Silovljevih teorema koristićemo sledeću notaciju i terminologiju.

Neka je σ_x unutrašnji automorfizam grupe G, za $a \in G$ i $H \subseteq G$ umesto $\sigma_x(a)$ i $\sigma_x(H)$ koristićemo oznake a^x, odnosno H^x. Dakle, $a^x = x^{-1}ax$, $H^x = x^{-1}Hx$. Primetimo da je, s obzirom da je $\sigma_x \in Aut(G)$, za $H < G$ tada $H^x < G$ i $|H^x| = |H|$.

Ako je $H \subseteq G$, $N(H) \overset{def}{=} \{x \in G \mid H^x = H\}$ i $N(H)$ nazivamo <u>normalizatorom</u> skupa H. Lako se proverava da je

<u>lema 1.</u> $N(H) < G$.

Ako je H Silovljeva p-podgrupa grupe G, pisaćemo kraće da je H S_p-podgrupa grupe G. Tada s_p označava broj svih S_p-podgrupa grupe G. Ako je $Q < G$ i $red(Q)$ je stepen prostog broja p, reći ćemo da je Q p-podgrupa grupe G. Do daljeg pretpostavljamo da je G konačna grupa.

<u>lema 2</u> Neka Q p-podgrupa grupe G i P S_p-podgrupa grupe G, p je prost broj. Ako $Q < N(P)$ tada $Q < P$.

<u>Dokaz</u> Prema poznatoj jednakosti

$$|QP| \cdot |Q \cap P| = |P| \cdot |Q|$$

i kako su $|Q \cap P|, |P|, |Q|$ stepeni prostog broja p (jer $Q \cap P < P$) to je $|QP| = p^\alpha$ za neki $\alpha \in N$. Dokažimo da je $QP < G$.

Kako je $Q < N(P)$, to $QP = \bigcup_{x \in Q} xP = \bigcup_{x \in Q} Px = PQ$, pa

- $(QP)^{-1} = P^{-1}Q^{-1} = PQ = QP$
- $(QP)(QP) = Q(PQ)P = Q(QP)P = (QQ)(PP) = QP$

pa $QP < G$. Primetimo da je $P < QP$. Dakle QP je p-podgrupa koja sadrži S_p-podgrupu P. Zbog maksimalnosti S_p podgrupe u skupu p-podgrupa grupe G, sledi $QP = P$, odakle $Q < P$ ∎

Neka je G konačna grupa, $|G| = mp^a$, $(m,p)=1$, p je prost.

II Silovljeva teorema 1. Ako je Q p-podgrupa grupe G, onda je Q sadržana u nekoj S_p-podgrupi grupe G.

2. Svake dve S_p-podgrupe su konjugovane, tj. ako su P, Q S_p-podgrupe grupe G, onda postoji $x \in G$ tako da $Q = P^x$.

III Silovljeva teorema 1. $s_p \equiv 1 \pmod p$

2. $s_p = |G : N(P)|$, P je S_p-podgrupa grupe G.

3. $s_p \mid |G|$.

Dokaz Odjednom dokazujemo obe teoreme. Neka je $\mathcal{O} \subseteq G$

$S = \{P^x \mid x \in G\}$ gde je P neka S_p-podgrupa grupe G.

Primetimo da je P^x S_p-pgra grupe G.

Neka je $\theta : G \longrightarrow Sym(S)$, gde je $\theta(g)(s) = s^x$, $g \in G$, $s \in S$, tj.: $\theta(g)(P^x) = P^{xg}$. Tada je θ dejstvo grupe G na S. Zaista,

$\theta(e)(s) = s^e = s$; $\theta(g_1 g_2)(s) = s^{g_1 g_2} = (s^{g_1})^{g_2} = \theta(g_2)(\theta(g_1)(s))$

$= (\theta(g_1)\theta(g_2))(s)$, tj.:

$\theta(e) = i_S$, $\theta(g_1 g_2) = \theta(g_1)\theta(g_2)$; pa je θ homomorfizam grupe G na skup S. Dalje za $s \in S$, orbita elementa s je

$s^G = \{s^g \mid g \in G\} = \{P^{xg} \mid g \in G\} = \{P^x \mid x \in G\} = S$, tj.:

(1) $s^G = S$.

Dakle pri ovom dejstvu postoji samo jedna orbita, neka je to orbita za P. Stabilizator el. $s \in S$ je

$G_s = \{x \in G \mid s^x = s\} = N(S)$, tj.:

(2) $G_s = N(s)$.

Klasična jednačina dejstva glasi $|S| = \sum_{s \in T} |G : G_s|$, ali s obzirom da postoji samo jedna orbita i zbog (2), sledi

(3) $|S| = |G : N(P)|$.

Cilj nam je da dokažemo da je $S = \{Q \mid Q$ je S_p-podgrupa grupe $G\}$.

Neka je Q podgrupa grupe G i neka je $\theta_0 = \theta|_Q$, tj. θ_0 je restrikcija djelstva θ na $Q < G$. Odmah vidimo da je θ_0 djelstvo grupe Q na skupu S. Tada za $s \in S$

(4) θ_0-orbita elementa s : $s^Q = \{s^g \mid g \in Q\}$

(5) θ_0-stabilizator elementa s : $Q_s = \{g \in Q \mid s^g = s\}$

Kada je θ_0-orbita s^Q jednočlan skup? Kako $s \in s^Q$, to

$$s^Q = \{s\} \iff \{s^g \mid g \in Q\} = \{s\}$$
$$\iff \text{za sve } g \in Q,\ s^g = s$$
$$\iff Q < N(s).$$

Specijalno,

(6) $P^Q = \{P\} \iff Q < N(P)$ (P je neka S_p-pgra grupe G).

Iz prethodne Leme 2 (17-4) sledi

(7) $P^Q = \{P\} \iff Q < P$.

Prema klasičnoj jednakosti za djelstvo θ_0 imamo

(8) $|S| = \sum_{s \in T} |s^Q| = \sum_{\substack{s \in T \\ |s^Q| = 1}} 1 + \sum_{\substack{s \in T \\ |s^Q| \neq 1}} |Q : Q_s|$

Setimo se da je $|s^Q| = |Q : Q_s|$

Kako $|Q : Q_s|$ deli $|Q|$ i $|Q|$ je stepen broja p, i za $|s^Q| \neq 1$, $Q_s \subsetneq Q$, to prema (7) i (8) imamo

(9) $|S| = \sum_{\substack{s \in T \\ Q < s}} 1 + \alpha \cdot p$ za neki $\alpha \in \mathbb{N}$.

Ako je $Q = P$, onda, naravno, jedine S_p-podgrupe koje sadrže Q je ona sama, tj. P, dakle $\sum_{\substack{s \in T \\ Q < s}} 1 = 1$, pa prema (9)

(10) $|S| = 1 + \lambda p$ za neki $\lambda \in \mathbb{N}$, tj. iz (9) i (10), ali za proizvoljnu p-podgrupu Q grupe G imamo

(11) $\sum_{s \in T,\, Q < s} 1 = 1 \mod p$.

Iz (11) sledi

(a) Postoji $1 \in S$ takvo da je $Q < 1$, tj.
postoji $x \in G$ t.d. $Q < P^x$, tj. Q je sadržana u nekoj S_p-podgrupi grupe G.

(b) Ako je Q S_p-grupa grupe G onda $Q < P^x$ za neko $x \in G$ ali tada $|Q| = |P^x| = p^n$, pa $Q = P^x$, tj: svake dve S_p-grupe grupe G su konjugovane, pa

(c) $S = \{ P \mid P$ je S_p-grupa grupe $G \}$, tj: $s_p = |S|$.
Prema (3) onda

(d) $s_p = |G : N(P)|$, dalje i

(e) $s_p \mid |G|$.

Prema (10)

(f) $s_p \equiv 1 \pmod p$. ∎

Primer 1. Opis svih grupa reda 15. Postoji bar jedna grupa reda 15, to je $C_{15} = C_5 \times C_3$. Dovoljno je dokazati nešto. Neka je $|G| = 15 = 3 \cdot 5$ i neka su P, Q redom S_3, S_5-grupe grupe G. Tada $|P| = 3$ i $|Q| = 5$, pa su one obe grupe ciklične, tj. postoje $a \in P$, $b \in Q$ t.d. $P = \langle a \rangle$, $Q = \langle b \rangle$, $\text{red}(a) = 3$, $\text{red}(b) = 5$. Dalje $P \cap Q < P, Q$ pa $|P \cap Q| \mid 3, 5$ tj. $|P \cap Q| = 1$, pa $P \cap Q = \langle 1 \rangle$.
Otuda $|PQ| = |P| \cdot |Q| / |P \cap Q| = 3 \cdot 5 / 1 = 15$ pa

(1) $G = PQ$, $P \cap Q = \langle 1 \rangle$
Dalje, $s_3 = 1 \pmod 3$, $s_5 = 1 \pmod 5$ i $s_3, s_5 \mid 15$ odakle

(2) $s_3 = 1$, $s_5 = 1$.
Otuda za sve $x \in G$ $P^x = P$, $Q^x = Q$ tj:

(3) $P, Q \trianglelefteq G$.
Iz (1) i (3) sledi da je G unutrašnji direktni proizvod podgrupa $P \cong C_3$, $Q \cong C_5$ pa $G \cong P \times Q \cong C_3 \times C_5 \cong C_{15}$. ∎

Zadatak Neka je θ dejstvo iz dokaza II. i III. Silowljeve teoreme. Dokazati da je $\ker\theta = \text{core}(N(P))$, gde je P bilo koja S_p-grupa grupe G.

Zadatak Neka je $Q \lhd G$ p-podgrupa grupe G. Tada je Q sadržana u svakoj S_p-podgrupi grupe G.

Opis grupa reda $2p$, p je prost broj:

$p=2$ Tada postoje tačno dve grupe: C_4, C_2^2

$p \geq 3$ Tada postoje tačno dve grupe $C_{2p} = C_2 \times C_p$ i D_p.

Jedinstv.: Ako je $|G| = 2p$ neka su $P = \langle a \rangle$, $Q = \langle b \rangle$ redom S_2, S_p podgrupe grupe G. Tada $|Q| = p$ pa $|G:Q| = 2$ dj: $Q \lhd G$. Stoga $b^a \in \langle b \rangle$ dj: $b^a = b^i$ za neki i, $1 \leq i \leq p-1$. Tada $b = b^e = b^{a^2} = (b^a)^a = (b^i)^a = (b^a)^i = (b^i)^i = b^{i^2}$ pa $i^2 \equiv 1 \bmod p$, odakle $i \in \{1, -1\}$, pa imamo dva slučaja:

a) $i = 1$, i tada $G \cong C_2 \times C_p$ jer $ab = ba$

b) $i = -1$, i tada $G \cong D_p$ jer $ab = b^{-1}a$

Primetimo da je $G = \langle a, b \rangle = PQ$ (vidi opis grupa reda 15).

Dakle, postoje grupe reda 10 kao C_{10} i D_5, i grupe reda 14 kao C_{14} i D_7.

Zadatak Opisati grupe reda 1001. Postoji tačno pet grupa reda 1001.

Jedinstv.: Neka je $|G| = 1001 = 7 \cdot 11 \cdot 13$ i neka su P, Q, R redom S_7, S_{11}, S_{13} podgrupe grupe G. Tada $s_7 = 1 \pmod 7$, $s_{11} = 1 \pmod{11}$ i $s_{13} = 1 \bmod 13$ i $s_7, s_{11}, s_{13} \mid 1001$. Neka $a \mid 1001$. Tada za $a < 1001$ $a-1 \in \{0, 6, 10, 12, 76, 90, 1425\}$ i $7, 11, 13$ jedino dele 0 iz ovog skupa, pa $s_7 = 1$, $s_{11} = 1$, $s_{13} = 1$, pa $P, Q, R \lhd G$, te je G unutrašnji poludirekt podgrupa P, Q, R, dj: $G \cong P \times Q \times R \cong C_7 \times C_{11} \times C_{13} = C_{1001}$.