Групе Силова (Силовљеве групе)

дефиниција

Нека је G група и p прост број. Ако је $|G| = p^{\alpha} m$, тако да $НЗД(p,m)=1$, онда се подгрупа $P \leq G$, реда p^{α} назива Силовљева p-група групе G.

Нотација:

$Syl_p(G) \equiv$ скуп свих Силовљевих p-група.

$n_p(G) \equiv$ број свих Силовљевих p-група, односно $n_p(G) = |Syl_p(G)|$

Теорема Силова

Нека је G група реда $p^{\alpha} m$, где је p прост број, $m \geq 1$ и $p \nmid m$. Онда:

(1) $Syl_p(G) \neq \emptyset$.

(2) Све Силовљеве p-групе су конјуговане међусобно, односно ако су P_1 и P_2 Силовљеве p-групе, онда постоји $g \in G$ тако да $P_1 = g P_2 g^{-1}$.
Посебно, $n_p(G) = |G : N_G(P)|$.

(3) Свака p-група у G је садржана у некој Силовљевој p-групи.

(4) $n_p(G) \equiv 1 \pmod{p}$.

<u>Доказ:</u>

(1) Доказујемо тврђење индукцијом по $|G|$.

$|G| = 1$ ✓

Претпоставимо да је тврђење тачно за све групе чији је ред мањи од n.

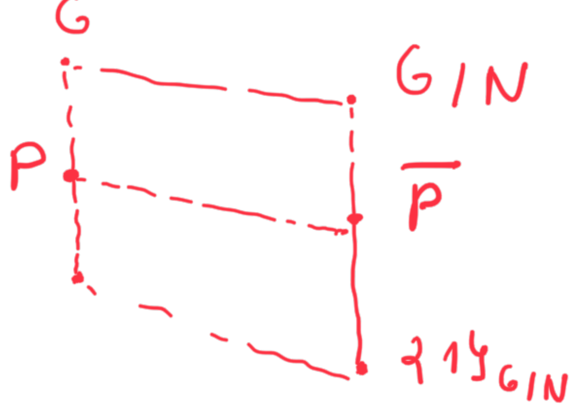
Нека је $|G| = n = p^{\alpha} \cdot m$, $p \nmid m$.

(а) $p \mid |Z(G)|$.

Нека је N подгрупа у $Z(G)$ реда p.

Јасно је $N \trianglelefteq G$.

$|G/N| = p^{\alpha-1} \cdot m < n$.



По индуктивној претпоставци, постоји $\overline{P}$, подгрупа у G/N, таква да $|\overline{P}| = p^{\alpha-1}$ односно $\overline{P}$ је Силовљева

p-група у G/N.

По теореми о кореспонденцији, постоји подгрупа $P \le G$, за коју вриједи

$$|G:P| = \underbrace{|\bar{G} : \bar{P}|}_{m}$$

$\Rightarrow |P| = p^{\alpha}$.

(б) Претпоставимо да $p \nmid |Z(G)|$.

Подсјетимо се једначине класа:

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

гдје су $g_1, g_2, \dots, g_r$ представници класа конјугације са више елемената.

$p \mid |G|$, али $p \nmid |Z(G)|$.

Закључујемо да постоји бар један $i \in \{1, 2, \dots, r\}$ тако да

$p \nmid |G : C_G(g_i)|$.

што значи да је $|C_G(g_i)| = p^{\alpha} \cdot m'$

при чему $m' < m$, јер у супротном

$|C_G(g_i)| = p^{\alpha} \cdot m \Rightarrow g_i \in Z(G)$,

супротно претпоставци да $g_i \notin Z(G)$,

за $i \in \{1, 2, \dots, r\}$.

Међутим $C_G(g_i)$ је подгрупа групе G и $|C_G(g_i)| < |G|$, па по индуктивној претпоставци, видимо да постоји Силовљева p-група у $C_G(g_i)$, реда p^α. Истовремено, то је Силовљева p-група и у G.

(2) Из (1) закључујемо да постоји бар једна Силовљева p-група. Нека је то P_1.

Нека је $S = \{P_1, P_2, \dots, P_k\}$ скуп свих конјугованих група групи P_1.

У ствари, $S = \{g P_1 g^{-1} : g \in G\}$.

Докажимо да $p \nmid k$.

Успоставимо дејство групе G на скуп S путем конјугације.

Стабилизатори „тачака" скупа S, односно група P_i су заправо $N_G(P_i)$.

$G \,|\, S$, а све су групе P_i конјуговане са P_1, што значи да је S једна орбита.

Онда

$$|S| = |\text{орбита од } P_1| = |G : N_G(P_1)|$$

P_1 је Силовљева p-група и $|P_1| = p^\alpha$.

Такође $P_1 \trianglelefteq N_G(P_1)$, одакле

$$|N_G(P_1)| = p^\alpha \cdot m'$$

$\Rightarrow |S|$ не може бити дељиво са p,

тј. $p \nmid k$.

Нека је Q произвољна Силовљева p-група у G. Доказујемо да Q мора бити у S.

Посматрајмо дејство групе Q на S конјугацијом, $Q \mid S$

$$x \longrightarrow f_x$$

$$f_x(P_i) = x P x^{-1}, \quad x \in Q.$$

Овим дејством, скуп S се разбија на коначан број орбита

$$|S| = |\text{орбита } P_{i_1}| + |\text{орбита } P_{i_2}| + \dots$$

$$+ |\text{орбита } P_{i_e}|$$

Знамо, $|\text{орбита } P_{i_j}| = |Q : N_Q(P_{i_j})|$, па је $|\text{орбита } P_{i,j}| \in \{1, p^t\}$, $t \leq \alpha$.

Међутим, показали смо да $p \nmid |S|$,

што значи да је бар једна орбита реда 1.

Претпоставимо да је

$$|\text{орбита } P_n| = 1.$$

$$|\text{орбита } P_n| = \frac{|Q|}{|N_Q(P_n)|} = 1.$$

$$\left[\, N_Q(P_n) = Q \cap N_G(P_n) \,\right]$$

$P_n \trianglelefteq N_G(P_n)$.

$|\text{орбита } P_n|$ у дејству групе Q на S

је величине 1.

То значи да за свако $x \in Q$,

$$x P_n x^{-1} = P_n$$

$$\Rightarrow x \in N_G(P_n) \Rightarrow Q \leq N_G(P_n).$$

Скуп $P_n \cdot Q$, с обзиром да су у

питању групе, а $P_n \trianglelefteq N_G(P_n)$,

онда је $P_n \cdot Q$ подгрупа у $N_G(P_n)$,

$$|P_h \cdot Q| = \frac{\underbrace{|P_h|}_{p^\alpha} \cdot \underbrace{|Q|}_{p^\alpha}}{\underbrace{|P_h \cap Q|}_{p^3}}$$

$$P_h \cdot Q = \{ z \cdot s \mid z \in P_h,\ s \in Q \}$$

$$\supseteq P_h$$

$$|P_h \cdot Q| \geq |P_h|$$

С друге стране $|P_h \cdot Q|$ мора бити $p^{2\alpha-3}$.

Користећи чињеницу да је $P_h \cdot Q$ подгрупа у $N_G(P_h)$, што значи да је $|P_h \cdot Q| = p^\alpha$.

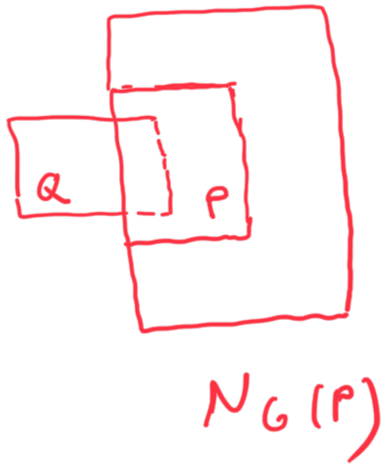
Закључујемо да је $|P_h \cap Q| = p^\alpha$, одакле закључујемо $P_h = Q$.

Прије него пређемо на доказивање (3), доказујемо следећу лему.

<u>Лема</u> Нека је P Силовљева p-група у G, а Q било које p-група.

$Q \cap P = Q \cap N_G(P)$.

Онда је $Q \cap P = Q \cap N_G(P)$.



доказ:

$$P \le N_G(P) \Rightarrow Q \cap P \le \underbrace{Q \cap N_G(P)}_{H}$$

H је подгрупа у G.

Докажимо да је $H \le Q \cap P$.

Јасно је да H мора бити или тривијална или p-група.

$P \trianglelefteq N_G(P)$

$H \cdot P$ је подгрупа у $N_G(P)$

$|H \cdot P| = p^r$ и $H \cdot P \geq P$,

а како је P Силовљева p-група,

онда $H \cdot P = P$.

$H \le H \cdot P = P$ (*)

Подсјетимо се, $H = Q \cap N_G(P)$.

$H \le P$ из (*) а јасно је $H \le Q$.

$H \leq P$ из (*), ...

што значи $H \leq P \cap Q$.

(3) Нека је H произвољна p-подгрупа у G. Докажимо да $H \leq P_i$, за $P_i \in S$.

Посматрамо дејство групе H на $S = \{P_1, \dots, P_k\}$ конјугацијом.
Тиме се S разбија на орбите

$$|S| = |\text{орбита } P_{i_1}| + |\text{орбита } P_{i_2}| + \dots + |\text{орбита } P_{i_j}|.$$

Величине сваке од орбита је дјелитељ $|H|$, што значи да су у скупу $\{1, p^t\}$, $t \geq 1$.

Међутим, из (2) следи $p \nmid |S|$, што значи да постоји бар једна орбита величине 1.

Без умањења општости, нека је $|\text{орбита } P_{i_1}| = 1$.

$$|\text{орбита } P_{i_1}| = \frac{|H|}{|N_H(P_{i_1})|} = \frac{|H|}{|H \cap N_G(P_{i_1})|}$$

Доказали смо у леми да

$$|H \cap N_G(P_{i_1})| = |H \cap P_{i_1}|,$$

одакле

$$|\text{орбита } P_{12}| = 1 = \frac{|H|}{|H \cap P_{12}|}$$

$$\Rightarrow |H| = |H \cap P_{12}| \Rightarrow H \subseteq P_{12}.$$

(4) Покажемо да $|S| \equiv 1 \pmod{p}$.

$S = \{P_1, P_2, \ldots, P_k\}$.

Посматрајмо $P_1 \mid S$ конјугацијом.

Јасно је да у овом случају

$|\text{орбита } P_1| = 1.$

За $P_i \neq P_1$,

$$|\text{орбита } P_i| = \frac{|P_1|}{|P_1 \cap N_G(P_i)|}$$

$$\overset{\text{лема}}{=} \frac{|P_1|}{|P_1 \cap P_i|} = p^d, \quad d \geq 1, \; d < \alpha.$$

$$|S| = |\text{орбита } P_1| + \sum \underbrace{|\text{орбита } P_{i_j}|}_{\text{дељиво са } p.}$$

$$|S| = 1 + p \cdot f$$

$$\Rightarrow |S| \equiv 1 \pmod{p}.$$

<u>Последице:</u>

- $n_p = |Syl_p(G)|$

Нека је P произвољна Силовљева p-група.

$$n_p = \frac{|G|}{|N_G(P)|}$$

$P \le N_G(P)$ (*)

$n_p \mid |G|$, али због (*) $n_p \mid \frac{|G|}{p^\alpha}$

Закључак:

$$\boxed{n_p \equiv 1 \pmod{p} \text{ и } n_p \mid \frac{|G|}{p^\alpha}}$$

- Ако је Силовљева p-група нормална у G, онда $n_p = 1$.

- Ако је G Абелова, онда јасно за свако p, прост број, $p \mid |G|$, постоји јединствена Силовљева p-група.

- Ако су p_1, p_2 прости бројеви, $p_1 \neq p_2$, $p_1 \mid |G|$, $p_2 \mid |G|$, онда за $P_1 \in Syl_{p_1}(G)$ и $P_2 \in Syl_{p_2}(G)$, $P_1 \cap P_2 = \{1\}$.

<u>Пример</u>

Нека је G група реда pq, где су p и q прости бројеви, $p < q$.
Онда G има тачно једну подгрупу реда q, која је зато нормална у G.

<u>Доказ</u>:

Посматрамо n_q.

$$n_q \equiv 1 \pmod q, \quad n_q \mid \frac{|G|}{q} = p$$

$$\Rightarrow n_q \in \{1, p\}.$$

Ако n_q није 1, онда $n_q = 1 + qt$, $t > 0$.

Пошто је $q > p \Rightarrow n_q > p$.

Контрадикција.

Дакле, $n_q = 1$.