Sylowljeva teorija

Ostopanj, Dragana

Sveučilište J.J.Strossmayera u Osijeku
Odjel za matematiku
Preddiplomski studij matematike

Dragana Ostopanj

Sylowljeva teorija

Završni rad

Osijek, 2015.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Preddiplomski studij matematike

Dragana Ostopanj

Sylowljeva teorija

Završni rad

Mentor: doc. dr. sc. Ivan Matić

Osijek, 2015.

Sažetak. Tema ovog završnog rada je objasniti što su to Sylowljevi teoremi, što su Sylowljeve podgrupe i koliko ih ima te koliki je njihov red. Započet ćemo definicijom Sylowljeve podgrupe, a nakon iskazivanja Sylowljevih teorema reći ćemo nešto o posljedicama istih. Zatim ćemo objasniti tranzitivno djelovanje podgrupe te tako doći do Frattinijevog teorema. Bitno pitanje u pogledu konačnih grupa je pitanje prostosti koje ćemo pojasniti u jednome od poglavlja kao i broj elemenata prostog reda. Rad ćemo završiti Schur-Zassenhausovim teoremom koji nam govori o komplementima normalnih podgrupa.

Ključne riječi: Sylowljevi teoremi, Sylowljeve podgrupe, broj podgrupa, Frattinijev teorem, grupe prostog reda, elementi prostog reda, Schur-Zassenhausov teorem

Abstract. The topic of this final paper is to explain what exactly are Sylow Theorems, what are Sylow subgroups and how many of them are there as well as which is their order. We will start with a definition of a Sylow subgroup and after state of Sylow Theorems we will say something about the consequences of such. Then, we will explain transitive action of a subgroup as well as how to reach to the Frattini Theorem. An important question with respect to final subgroups is the question of simplycity as well as the number of elements of a prime order which will be explained in one of the upcoming chapters. This paper will be concluded with Schur-Zassenhaus Theorem which gives us an insight in complements of normal subgroups.

Key words: Sylow Theorems, Sylow subgroups, number of subgroups, Frattini Theorem, groups of a prime order, elements of a prime order, Schur-Zassenhaus Theorem

Sadržaj

1. Uvod

Godine 1872. norveški matematičar Peter Ludwig Mejdell Sylow objavio je niz teorema koji su danas poznati kao Sylowljevi teoremi. Ovi važni teoremi opisuju prirodu maksimalnih p-podgrupa konačne grupe koje se danas zovu Sylowljeve p-podgrupe. (Kako bi bilo zgodnije, skupit ćemo Sylowljeve teoreme u jedan teorem).

2. Sylowljeve podgrupe

Počinjemo definicijom Sylowljeve podgrupe.

Definicija 2.1 *Neka je G grupa i p prost broj. Sylowljeva p-podgrupa grupe G je maksimalna podgrupa od G (u skupovnom smislu). Skup svih Sylowljevih p-podgrupa od G označavamo s $Syl_p(G)$. Broj Sylowljevih p-podgrupa od G označavamo s $n_p(G)$ ili samo n_p kada je iz konteksta jasno o kojoj grupi se radi.*

Naravno, ako prost broj p dijeli $|G|$ (red od G), tada G sadrži Sylowljevu p-podgrupu, štoviše, svaka p-podgrupa grupe G sadržana je u Sylowljevoj p-podgrupi. Isto tako, ako je G beskonačna grupa i H p-podgrupa od G, tada nam Zornova lema[1]govori da G sadrži Sylowljevu p-podgrupu koja sadrži H.

Budući da je konjugiranje izomorfizam i čuva red elemenata grupe, slijedi da ako je S Sylowljeva p-podgrupa od G, onda je to i svaki konjugat S^a od S, gdje je $S^a = aSa^{-1}$.

Valja primjetiti da ako je G konačna grupa i $|G| = p^n m$ gdje je $(p, m) = 1$, tada je svaka podgrupa reda p^n Sylowljeva p-podgrupa. Dokazat ćemo obrat ove tvrdnje nešto kasnije: Svaka Sylowljeva podgrupa grupe G je reda p^n.

[1]Zornova lema: Ako je P parcijalno uređen skup u kojem svaki lanac ima gornju među, tada P ima maksimalni element.

3. Normalizator Sylowljeve podgrupe

Neka je G konačna grupa. Ako je Sylowljeva p-podgrupa od G normalna podgrupa od G, tada G/S ne sadržava elemente reda p. U daljnjem ćemo takve elemente zvati p-elementima. Stoga, $p \nmid [G : S]$ te je zbog toga S skup svih p-elemenata u G.

Naravno, S je uvijek normalna podgrupa svog normalizatora $N_G(S)$.

Teorem 3.1 *Neka je G konačna grupa i neka je $S \in Syl_p(G)$.*

1. *S je skup svih p-elemenata od $N_G(S)$*
2. *Svaki p-element $a \in G \setminus S$ konjugacijom mijenja S, tj. $S^a \neq S$*
3. *S je jedina Sylowljeva p-podgrupa od $N_G(S)$*
4. *$p \nmid [N_G(S) : S]$*

Ako je $S \in \mathrm{Syl}_p(G)$, tada je

$$S^a \leq N_G(S)^a$$

za svaki $a \in G$. Stoga, ako a normalizira $N_G(S)$, tj. ako vrijedi $N_G(S)^a = aN_G(S)a^{-1}$, tada je

$$S^a \leq N_G(S),$$

a budući da je S^a također Sylowljeva p-podgrupa od $N_G(S)$, Teorem 3.1 povlači da je $S^a = S$. Drugim riječima, ako a normalizira $N_G(S)$, tada a također normalizira i S te je zbog toga

$$N_G(N_G(S)) = N_G(S).$$

Teorem 3.2 *Normalizator $N_G(S)$ Sylowljeve podgrupe grupe G jednak je svom normalizatoru, tj.*

$$N_G(N_G(S)) = N_G(S).$$

Uskoro ćemo biti u mogućnosti dokazati da ne samo da $N_G(S)$ normalizira samu sebe, nego da to vrijedi za svaku podgrupu grupe G koja sadrži $N_G(S)$.

4. Sylowljevi teoremi

Neka je G konačna grupa i neka je $S \in \mathrm{Syl}_p(G)$. Činjenica da svaki p-element $a \notin S$ konjugacijom mijenja S potiče nas da pogledamo djelovanje p-podgrupe K grupe G konjugacijom na skup

$$\mathrm{conj}_G(S) = \{S^a \mid a \in G\}$$

konjugata od S u G. Što se tiče stabilizatora od S^a, imamo

$$\mathrm{stab}(S^a) = N_G(S^a) \cap K = S^a \cap K,$$

pa je tako

$$|\mathrm{orb}_K(S^a)| = [K : S^a \cap K]$$

što je djeljivo s p osim ako je $K \leq S^a$, u kojem slučaju je orbita reda 1.
Stoga,

$$\mathrm{Fix}_{\mathrm{conj}_G(S)}(K) = \{S^a \mid K \leq S^a\}$$

pa je tako

$$|\mathrm{conj}_a(S)| \equiv |\{S^a \mid K \leq S^a\}| \pmod{p}.$$

Sada ako je K Sylowljeva p-podgrupa grupe G, tada je $K \leq S^a$ ako i samo ako je $K = S^a$ te je zbog toga

$$|\mathrm{conj}_G(S)| \equiv \begin{cases} 1 \pmod{p}, & K \in \mathrm{conj}_G(S) \\ 0 \pmod{p}, & K \notin \mathrm{conj}_G(S). \end{cases}$$

Slijedi da slučaj $K \notin \mathrm{conj}_G(S)$ nije moguć pa je tako $\mathrm{Syl}_p(G) = \mathrm{conj}_G(S)$ klasa konjugiranosti i

$$n_p \equiv 1 \pmod{p}.$$

Primjetimo također da

$$n_p = |\mathrm{conj}_G(S)| = [G : N_G(S)] \mid |G|.$$

Konačno, možemo odrediti red Sylowljeve p-podgrupe S, budući da je

$$[G : S] = [G : H_G(S)] \cdot [H_G(S) : S],$$

a ni jedan od faktora desno nije djeljiv s p. Stoga, red od S je najveća potencija od p koja dijeli $|G|$. Time smo dokazali Sylowljeve teoreme.

Teorem 4.1 *(Sylowljevi teoremi) Neka je G konačna grupa i neka je $|G| = p^n m$, gdje je p prost broj takav da $p \nmid m$.*

1. *Sylowljeve p-podgrupe grupe G su podgrupe od G reda p^n.*
2. *$Syl_p(G)$ je klasa konjugiranosti u $sub(G)$.*
3. *Broj n_p Sylowljevih p-podgrupa zadovoljava*

$$n_p \equiv 1 \pmod{p} \quad i \quad n_p = [G : H_G(S)] \mid |G|,$$

   gdje je $S \in Syl_p(G)$.

4. *Neka je $S \in Syl_p(G)$,*
   (a) *S je normalna ako i samo ako je $n_p = 1$.*
   (b) *S normalizira samu sebe ako i samo ako je $n_p = [G : S] = m$, u kojem slučaju sve Sylowljeve p-podgrupe od G normaliziraju same sebe.*
5. *Ako je K p-podgrupa od G, tada je*

$$|\{S \in Syl_p(G) \mid K \leq S\}| \equiv 1 \pmod{p}.$$

Dokazat ćemo kasnije u poglavlju da je svaka normalna Sylowljeva p-podgrupa konačne grupe komplementirana.

4.1. Neke posljedice Sylowljevih teorema

Promotrimo neke od manje ili više izravnih posljedica Sylowljevih teorema.

4.1.1. Djelomičan obrat Lagrangeovog teorema

Sylowljeva p-podgrupa S grupe G sadrži podgrupe svih redova koji dijele $|S|$. Ovo daje djelomičan obrat Lagrangeovog teorema.

Teorem 4.2 *Neka je G konačna grupa i p prost broj. Ako $p^k \mid |G|$, tada G sadrži podgrupu reda p^k.*

4.1.2. Više o normalizatoru Sylowljevljeve podgrupe

Prisjetimo se da je normalizator $N_G(S)$ Sylowljeve podgrupe S grupe G sam sebi normalizator. Sada možemo reći više.

Teorem 4.3 *Neka je G konačna grupa i $S \in Syl_p(G)$. Ako je*

$$S \leq N_G(S) \leq H \leq G,$$

tada je H normalizator samome sebi. Posebno, ako je $H < G$, tada H nije normalna podgrupa od G.

Dokaz: Konjugiranjem bilo kojim $a \in N_G(H)$ dobivamo

$$S^a \leq N_G(S)^a \leq H \leq G$$

pa su tako S^a i S Sylowljeve p-podgrupe od H. Slijedi da su S i S^a konjugirane u H. Stoga, postoji $h \in H$ za kojeg je $S^{ha} = S$, tj. $ha \in N_G(S) \leq H$. Dakle, $a \in H$ i $N_G(H) = H$.

□

4.1.3. Broj podgrupa konačne grupe

U ranijem poglavlju dokazali smo da ako je G p-grupa i $p^k \mid |G|$, tada broj $n_{p,k}(G)$ podgrupa od G reda p^k zadovoljava

$$n_{p,k}(G) \equiv 1 \pmod{p} \tag{1}$$

Upravo smo dokazali da je za svaku konačnu grupu G za koju $p \mid |G|$

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

Kako bismo vidjeli da (1) vrijedi za sve konačne grupe, tražimo veličinu skupa

$$\mathcal{F}_k = \{(H, S) \mid H \leq S, S \in \mathrm{Syl}_p(G), |H| = p^k\}$$

modulo p. S jedne strane, za svaki $S \in \mathrm{Syl}_p(G)$ postoji $n_{p,k}(S) \equiv 1 \pmod{p}$ podgrupa od S reda p^k pa je tako

$$|\mathcal{F}_k| \equiv n_p(G) \cdot 1 \pmod{p} \equiv 1 \pmod{p}.$$

S druge strane, za svaku $H \leq G$ reda p^k, Teorem 4.1 povlači da je

$$|\{S \in \mathrm{Syl}_p(G) \mid H \leq S\}| \equiv 1 \pmod{p}$$

te je zbog toga

$$|\mathcal{F}_k| \equiv n_{p,k}(G) \cdot 1 \pmod{p} \equiv n_{p,k}(G) \pmod{p}.$$

Stoga, $n_{p,k}(G) \equiv 1 \pmod{p}$ i dokazali smo važni Frobeniusov teorem.

Teorem 4.4 *(Frobenius) Neka je G grupa reda $p^n m$, gdje je $(p, m) = 1$. Tada za svaki $1 \leq k \leq n$ broj $n_{p,k}(G)$ podgrupa grupe G reda p^k zadovoljava*

$$n_{p,k}(G) \equiv 1 \pmod{p}.$$

□

4.2. Tranzitivno djelovanje, Frattinijev argument

Frattinijev argument pokazuje da ako grupa G djeluje na nepraznom skupu X i ako je $H \leq G$ tranzitivna[2]na X, onda je

$$G = H\text{stab}_G(X)$$

i ako je H regularna[3]na X, onda je

$$G = H \cdot \text{stab}_G(X)$$

pa je tako $\text{stab}_G(X)$ komplement od H u G. Nadalje, neka je G konačna grupa i neka je

$$S \leq H \trianglelefteq G$$

gdje je $S \in \text{Syl}_p(G)$. Neka G djeluje na $\text{conj}_G(S)$ konjugiranjem. Budući da je $S^a \in \text{Syl}_p(H)$ za svaki $a \in G$, slijedi da H djeluje tranzitivno na $\text{conj}_G(S)$.
Stoga,

$$G = H\text{stab}_G(X) = HN_G(S).$$

Ovaj specifičan argument naziva se još i Frattinijev argument.

Teorem 4.5 *Neka je G konačna grupa i $H \leq G$. Ako je $S \in Syl_p(H)$, tada je*

$$G = HN_G(S)$$

i ako je djelovanje grupe H konjugiranjem na $conj_G(S)$ regularno, tada je

$$G = H \cdot N_G(S).$$

Ovaj teorem može se koristiti kako bi se pokazalo da Frattinijeva[4]podgrupa konačne grupe G ima svojstvo da je svaka njena Sylowljeva podgrupa normalna u G.

Teorem 4.6 *(Frattini) Ako je G konačna grupa, tada Frattinijeva podgrupa $\Phi(G)$ ima svojstvo da su sve njene Sylowljeve podgrupe normalne u G.*

Dokaz: Ako je $S \in \text{Syl}_p(\Phi)$, tada je $S \leq \Phi \trianglelefteq G$ te prema Frattinijevom argumentu slijedi da je

$$G = \Phi N_G(S).$$

Ali ako je $N_G(S) < G$, tada postoji maksimalna podgrupa M grupe G za koju je $N_G(S) \leq M$ pa je tako $G \leq M$, što je kontradikcija. Stoga, $N_G(S) = G$ i $S \trianglelefteq G$. □

[2]Grupa G djeluje tranzitivno na skupu X ako za svaki par x, y iz X postoji g iz G takav da je $gx = y$.

[3]Grupa G djeluje regularno na skupu X ako za svaki par x, y iz X postoji jedinstveni g iz G takav da je $gx = y$.

[4]Frattinijeva podgrupa $\Phi(G)$ konačne grupe G je presjek svih maksimalnih podgrupa grupe G.

4.3. Potraga za "prostošću"

Sylowljevi teoremi pružaju snažne "alate" za analizu konačnih grupa. Ključan problem u pogledu konačnih grupa je pitanje prostosti. Kako ćemo objasniti u predstojećem poglavlju, pitanje glede toga koje su konačne grupe proste čini se da je riješeno, ali je rješenje toliko kompleksno da neki matematičari još uvijek imaju pitanja vezana uz njegovu potpunu točnost.

Vidjeli smo da grupa reda potencije prostog broja ima normalnu podgrupu svakog reda $p^k \mid p^n$. Shodno tome, nećemo voditi nikakve daljnje izravne analize p-grupa u ovom poglavlju.

Tijekom naše rasprave, p će označavati prost broj, Y_p proizvoljnu Sylowljevu podgrupu, kao i obično, n_p označava broj Sylowljevih p-podgrupa od G. Prisjetimo se da je:

1. $n_p = 1 + kp$, za neki cijeli broj $k \geq 0$
2. $n_p = [G : H_G(Y_p)] \mid |G|$.

Primijetimo da ako je $|G| = p^n m$, pri čemu $p \nmid m$, tada $n_p \mid |G|$ ako i samo ako $n_p \mid m$.

Sljedeće činjenice (među ostalima) su korisne u pokazivanju da grupa nije prosta:

1. Y_p je normalna ako i samo ako je $n_p = 1$.
2. Ako je $[G : H]$ jednak najmanjem prostom broju koji dijeli $|G|$, tada je $H \triangleleft G$.
3. Jezgra svakog djelovanja $\lambda : G \to S_x$ je normalna podgrupa od G.
4. Ako je $H < G$, tada $[G : H^0] \mid [G : H]!$. Stoga, ako $|G| \nmid [G : H]!$, tada je H^0[5]netrivijalna prava normalna podgrupa od G.

Imat ćemo koristi i od činjenice da ako je p prost broj i $1 \leq e < p$, onda je ep najmanji cijeli broj za kojeg $p^e \mid (ep)!$.

4.3.1. n_p-argument

Često se dogodi da za neki neparan prost broj $p \mid |G|$, cijeli broj $1 + kp$ ne dijeli $|G|$ osim ako je $k = 0$, u kom je slučaju $n_p = 1$ i $Y_p \trianglelefteq G$. Nazovimo argument

$$n_p = 1 + kp \mid |G| \Rightarrow k = 0$$

n_p-argument. Primijetimo da n_p-argument ne vrijedi ako je $p = 2$ osim ako je $|G|$ potencija broja 2, budući da $1 + 2k \mid |G|$ za neki $k > 1$.

[5] $H^0 = \bigcap_{a \in G} H^a$

Primjer 4.1 *Ako je* $|G| = 9982 = 2 \cdot 7 \cdot 23 \cdot 31$*, onda nam rutinski izračun pokazuje da za* n_7 *argument vrijedi*

$$1 + 7k \mid |G| \Rightarrow k = 0$$

pa je tako $Y_7 \triangleleft G$ *i* G *nije prosta.*

Primjer 4.2 *Ako je* $|G| = p^n m$*, za* $n \geq 1$*,* $m > 1$ *i* $p \nmid m$*, onda* $n_p = (1 + kp) \mid m$ *pa tako ako je* $m < p$*, onda je* $k = 0$ *odakle je i* $Y_p \triangleleft G$*.*

Dakle, grupe reda

$$p^n, 2p^n, \ldots, (p-1)p^n$$

za p prost broj i $n \geq 1$ sadrže podgrupu $Y_p \triangleleft G$ i stoga nisu proste.

Malo programiranja pokazuje da među redovima do 10000 (ne uključujući proste potencije) postoji samo 569 redova (manje od 6%) koji nisu podložni n_p-argumentu za neki p. Dakle, velika većina redova do 10000 su ili potencije prostih brojeva ili imaju svojstvo da grupe toga reda sadrže normalnu Sylowljevu podgrupu.

4.3.2. Broj elemenata prostog reda

Ako je p prost broj i $p \mid |G|$, ali $p^2 \nmid |G|$, tada je svaka od n_p različitih Sylowljevih podgrupa grupe G reda p te su zato podgrupe međusobno disjunktne. Stoga, G sadrži točno $n_p \cdot (p-1)$ različitih elemenata reda p. Ponekad je ovo jednostavno brojanje elemenata (za različite proste brojeve p) dovoljno da bi se pokazalo da je jedna od Sylowljevih podgrupa normalna.

Primjer 4.3 *Neka je* $|G| = 30 = 2 \cdot 3 \cdot 5$*. Onda s obzirom na činjenicu da* $np = 1 + kp \mid |G|$ *možemo samo zaključiti da je* $n_3 \in \{1, 10\}$ *i* $n_5 \in \{1, 6\}$*. Međutim, ako je* $n_3 = 10$ *i* $n_5 = 6$*, tada* G *sadrži barem* $n_3 \cdot (3-1) = 20$ *elemenata reda 3 i 24 elementa reda 5, što je ukupno 44 elementa. Stoga, jedna od* Y_3 *ili* Y_5 *mora biti normalna u* G*.*

4.3.3. Indeks jednak najmanjem prostom djelitelju

Ako je $|G| = pq^k$ gdje je $p < q$, p i q prosti, onda je $Y_q \triangleleft G$ jer je $[G : Y_q] = p$ najmanji prost broj koji dijeli $|G|$. Štoviše, jasno je da je

$$G = Y_q \rtimes {}^6Y_p.$$

[6]Neka je G grupa i $H, K \leq G$. Ako je $G = H \cdot K$, $H \trianglelefteq G$, tada G nazivamo semidirektnim produktom podgrupa H i K. To označavamo s $G = H \rtimes K$.

Primjer 4.4 *Ako je* $|G| = 3 \cdot 5^2 = 75$*, onda je* $Y_5 \triangleleft G$ *i*

$$G = Y_3 \rtimes Y_5.$$

Također, $1 + 3k \mid 25$ *vrijedi samo za* $k = 0$ *ili* $k = 8$ *pa je zato* $n_3 = 1$ *ili* $n_3 = 25$*. Primijetimo da je za* $n_3 = 1$*,* $G = Y_3 \bowtie {}^7Y_5$ *Abelova.*

Kada je $|G| = pq$, možemo dati poprilično potpunu analizu kako slijedi.

Teorem 4.7 *Neka je* $|G| = pq$*, gdje su* p *i* q *prosti brojevi,* $p < q$*. Tada je*

$$G = C_q(b) \rtimes C_p(a)$$

gdje je

$$b^a = b^k$$

za neki $1 \leq k < q$ *i* $k^p \equiv 1 \pmod{q}$*. Štoviše, G je ciklička ako i samo ako* $p \nmid q - 1$*.*

Dokaz: Vidjeli smo da je

$$G = Y_q \rtimes Y_p = C_q(b) \rtimes C_p(a).$$

Dakle, $aba^{-1} = b^k$ za neki $1 \leq k < q$ i ponovljeno konjugiranje s a nam daje

$$b = a^p b a^{-p} = b^{k^p}$$

što povlači da je $k^p \equiv 1 \pmod{q}$. Štoviše, $n_p \mid q$ pa je tako $n_p = 1$ ili $n_p = q$. Ali $n_p = 1$ ako i samo ako je $Y_p \trianglelefteq G$, tj. ako i samo ako je G ciklička i $n_p = q$ ako i samo je $1 + kp = q$, tj. ako i samo $p \nmid q - 1$. □

Primjer 4.5 *Vratimo se na slučaj kada je* $|G| = 30 = 2 \cdot 3 \cdot 5$*. Vidjeli smo u Primjeru 4.3 jedna od* Y_3 *i* Y_5 *mora biti normalna u G. Slijedi da je* $Y_3Y_5 \trianglelefteq G$ *reda 15 pa je zato i ciklička. Stoga,* $Y_3, Y_5 \sqsubseteq Y_3Y_5 \trianglelefteq G$ *pa su obje* Y_3 *i* Y_5 *normalne u G.*

4.3.4. Upotreba/korištenje jezgre djelovanja

Jezgra djelovanja $\lambda : G \to S_x$ je normalna u G i ovo može biti korisna tehnika za pronalaženje normalnih podgrupa, iako sve ne moraju biti Sylowljeve podgrupe.

Na primjer, ako G djeluje na $\mathrm{Syl}_p(G)$ konjugiranjem, tada je jezgra od $\lambda : G \to S_{kp+1}$

$$K = \bigcap_{S \in \mathrm{Syl}_p(G)} N_G(Y)$$

[7] Grupa G se naziva (unutarnji) direktan produkt dvije normalne podgrupe H i K ako je $G = H \cdot K$. To označavamo s $G = H \bowtie K$.

koja je normalna podgrupa od G. Problem je što bi mogla biti trivijalna ili jednaka grupi G.

Neka je $|G| = p^m u$ i $|K| = p^s v$, gdje su $m \geq 1$, $u > 1$ i $p \nmid u$. Također, neka je $n_p = kp + 1$. Tada je $K = G$ ako i samo ako je $n_p = 1$ i to povlači da je $s = m$. Obratno, ako je $s = m$ tada K sadrži Sylowljevu p-podgrupu S od G. Jedina Sylowljeva p-podgrupa od G u $N_G(Y)$ je sama grupa Y i tada je $n_p = 1$ i $K = G$. Dakle,

$$K = G \Leftrightarrow Y_p \triangleleft G \Leftrightarrow s = m$$

slijedi

$$p^{m-s}\frac{u}{v} \mid (kp+1)!$$

i $p^{m-s} \mid (kp)!$. Stoga, ako je $k < p$, tada je $m - k \leq s$. Iz toga slijedi da ako je $k < m$, tada je $s > 0$ i K je netrivijalna. Dakle

$$k < \min\{m, p\} \Rightarrow K \neq \{1\}.$$

Konačno napominjemo da K ima nešto jednostavniji oblik ako je $n_p = u$ jer tada svaka grupa normalizira samu sebe i

$$K = \bigcap_{Y \in \mathrm{Syl}_p(G)} Y$$

Teorem 4.8 *Neka je $|G| = p^m u$, gdje je p prost broj, $m \geq 1, u > 1$ i $p \nmid u$. Neka je $n_p = 1 + kp$.*

1. *Ako je $k = 0$, tada je $Y \triangleleft G$.*

2. *Ako je $0 < k < \min\{m, p\}$, tada je*

$$K = \bigcap_{Y \in Syl_p(G)} N_G(Y)$$

netrivijalna prava normalna podgrupa od G reda $p^s v$, gdje je $m - k \leq s \leq m - 1$ i $v \mid u$. Posebno, ako je $k = (u-1)/p$ tada je

$$K = \bigcap_{Y \in Syl_p(G)} Y$$

reda p^s.

Primjer 4.6 *Ako je $|G| = 108 = 3^3 \cdot 4$, tada $1 + 3k \mid 4$ te je $k = 0$ ili $k = 1$ Dakle ovaj slučaj nije podložan n_p-argumentu. Međutim, ako je $k = 1$ tada Teorem 4.8 povlači da je*

$$K = \bigcap_{Y \in Syl_3(G)} Y$$

prava netrivijalna podgrupa od G reda 9. Dakle, G nije prosta.
Ako je $|G| = 189 = 3^3 \cdot 7$, tada $1 + 3k \mid 7$ te je $k = 0$ ili $k = 2$. Ako je $k = 2$, tada Teorem 4.8 povlači da je

$$K = \bigcap_{Y \in Syl_3(G)} Y$$

prava netrivijalna normalna podgrupa od G reda 3 ili reda 9.
Ako je $|G| = 300 = 2^2 \cdot 3 \cdot 5^2$, tada $n_5 = 1 + 5k \mid 12$ te je $k = 0$ ili $k = 1$ (i $n_5 = 6$). No, ako je $k = 1$, tada Teorem 4.8 povlači da G nije prosta.

4.3.5. Upotreba/primjena normalizatora Sylowljevih podgrupa

Neka su p i q prosti, $p \neq q$ takvi da $p \mid |G|$ i $q \mid |G|$ i neka je $Y_q \in \mathrm{Syl}_q(G)$. Pod pretpostavkom da je $n_q > 1$ i $N_G(Y_q) < G$ pretpostavimo $p \nmid n_q$ što znači da $p \mid |N_G(Y_q)|$ i $P \in \mathrm{Syl}_p(N_G(Y_q))$. Pogledajmo što možemo reći o $|N_G(P)|$.
Prvo, ako je $P \lhd N_G(Y_q)$, tada je $N_G(Y_q) \leq N_G(P)$ iz čega slijedi da

$$|N_G(Y_q)| \mid |N_G(P)|.$$

S druge strane, ako P nije normalna podgrupa od $N_G(Y_q)$, činjenica da je $Y_q \trianglelefteq N_G(Y_q)$ povlači da je PY_q podgrupa grupe G. K tome, ako je PY_q Abelova, tada $Y_q \leq N_G(P)$ i tada

$$|Y_q| \mid |N_G(P)|.$$

U oba slučaja, ako P nije Sylowljeva p-podgrupa od G, ali $P \lhd P^*$[8] $\in \mathrm{Syl}_P(G)$, tada je $P^* \leq N_G(P)$ te

$$|P^*| \mid |N_G(P)|.$$

Primjer 4.7 *Ako je $|G| = 3675 = 3 \cdot 5^2 \cdot 7^2$, tada je lako pokazati da je $n_7 \in \{1, 15\}$. Ako je $n_7 = 15$, tada je $|N_G(Y_7)| = 5 \cdot 7^2$. Neka je P Sylowljeva 5-podgrupa grupe $N_G(Y_7)$. Broj takvih grupa je $1 + 5k \mid 7^2$ te je $P \lhd N_G(Y_7)$. Stoga,*

$$5 \cdot 7^2 \mid |N_G(P)|.$$

Također, P je indeksa 5 u $P^* \in Syl_5(G)$ i tada je $P \lhd P^*$ iz čega slijedi da

$$5^2 \mid |N_G(P)|$$

te

$$5^2 \cdot 7^2 \mid |N_G(P)|.$$

Dakle, ili je $N_G(P) = G$ iz čega slijedi da je $P \lhd G$ ili je $N_G(P)$ indeksa 3 u G te je $N_G(P)$ normalna u G.

[8] P^* je oznaka za Sylowljevu podgrupu od G reda p.

Pretpostavimo da je $|G| = pqu$, gdje su p i q prosti, $p \neq q$ te $p \nmid u$ i $q \nmid u$. Ako $p \nmid n_q$, tj. ako $p \mid |N(Y_q)|$, tada je $Y_p \leq N(Y_q)$ te je $Y_pY_q \leq G$ reda pq. Dakle, ako $p \nmid (q-1)$, tada je Y_pY_q Abelova (ciklička) grupa te je $Y_q \leq N(Y_q)$. Dakle, $q \mid |N(Y_q)|$ pa stoga $n_p \mid \frac{|G|}{pq}$.

Teorem 4.9 *Ako je $|G| = pqu$, gdje je $p < q$, p, q prosti brojevi takvi da $p \nmid u$ i $q \nmid u$, tada*

$$p \nmid (q-1) \quad i \quad p \nmid n_q \quad \Rightarrow \quad n_p \mid \frac{|G|}{pq}.$$

Primjer 4.8 *Ako je $|G| = 1785 = 3{\cdot}5{\cdot}7{\cdot}17$, tada je $n_3 \in \{1, 7, 85, 595\}$ i $n_{17} \in \{1, 35\}$. No,*

$$3 < 17, \quad 3 \nmid (17-1), \quad 3 \nmid n_{17} \quad \Rightarrow \quad n_3 \mid \frac{|G|}{3 \cdot 17} = 35$$

te je zbog toga $n_3 = 1$ ili $n_3 = 7$.

5. O postojanju komplementa: Schur-Zassenhausov teorem

U ovome poglavlju koristimo djelovanje grupe kako bi dokazali Schur-Zassenhausov teorem koji nam daje dovoljan (ali ne nužan) uvjet prema kojemu normalna podgrupa H grupe G ima komplement K i tako daje poluizravnu dekompoziciju $G = H \rtimes K$.

Definicija 5.1 *Neka je G konačna grupa. Hallova podgrupa H od G je podgrupa sa svojstvom da su $|H|$ i indeks $[G : H]$ relativno prosti.*

Schur-Zassenhausov teorem tvrdi da normalna Hallova podgrupa H ima komplement. Kako bi ga dokazali koristit ćemo Frattinijev argument.

Posebno, razmatramo djelovanje grupe G lijevom translacijom na skup $\mathcal{R}$ svih lijevih transverzala od H i pokazat ćemo da je to djelovanje regularno, dakle

$$G = H \rtimes \mathrm{stab}_G(R)$$

$\forall R \in \mathcal{R}$. Stoga pogledajmo pobliže transverzale i njihovo djelovanje.

5.1. Transverzale i njihovo djelovanje

Neka je G konačna grupa i H normalna Hallova podgrupa od G s desnim podskupovima

$$H \setminus G = \{H = H_1, \ldots, H_m\}.$$

Neka je $\mathcal{R}$ skup svih desnih transverzala od H. Ako je $R = \{r_1, \ldots, r_m\} \in \mathcal{R}$ gdje je $r_i \in H_i, \forall i$ i ako je $a \in G$, tada vrijedi

$$Har_i = aHr_i,$$

te su podskupovi Har_i međusobno različiti. Dakle,

$$aR = \{ar_1, \ldots, ar_m\} \in \mathcal{R}$$

te vidimo da G djeluje na skupu $\mathcal{R}$ lijevom translacijom.

Iako H ne mora djelovati tranzitivno na $\mathcal{R}$ možemo podići djelovanje grupe G do na djelovanja na kongruentne klase pripadne G-kongruencije na $\mathcal{R}$ tako da H djeluje tranzitivno. Uvjet G-kongruencije je

$$R \equiv S \quad \Rightarrow \quad aR \equiv aS$$

za svaki $a \in G$, tj.

$$\{r_1, \ldots, r_m\} \equiv \{s_1, \ldots, s_m\} \quad \Rightarrow \quad \{ar_1, \ldots ar_m\} \equiv \{as_1, \ldots, as_m\}.$$

To nas navodi da probamo sljedeće. Pod pretpostavkom da su R i S indeksirani tako da su r_i i s_i u istom desnom podskupu M_i, definiramo binarnu relaciju $\equiv$ tako da

$$R \equiv S \quad \text{ako je} \quad \prod_{i=1}^{m} r_i s_i^{-1} = 1.$$

Neka je

$$R \,|\, S = \prod_{i=1}^{m} r_i s_i^{-1}.$$

Tada definicija glasi

$$R \equiv S \quad \text{ako je} \quad R \,|\, S = 1.$$

Ova relacija je očito refleksivna. Također, kako je $r_i s_i^{-1} \in H, \forall i$, ako je H Abelova grupa, tada $\forall R, S, T \in \mathcal{R}$ vrijedi

$$(R \,|\, S)^{-1} = S \,|\, R \quad \text{i} \quad (R \,|\, S)(S \,|\, T) = R \,|\, T$$

te je zbog toga $\equiv$ relacija ekvivalencije na $\mathcal{R}$. Označimo s $\mathcal{R} \,|\, \equiv$ skup svih klasa ekvivalencije na $\mathcal{R}$, a s $[R]$ klasu ekvivalencije koja sadrži R.

Primijetimo da ako je $h \in H$, tada $r_i s_i^{-1} \in H$ povlači da je

$$(hR) \,|\, S = \prod_{i=1}^{m} h r_i s_i^{-1} = h^m (R \,|\, S).$$

Povrh toga, kako su r_i i s_i iz istog desnog podskupa od H (što vrijedi i za ar_i i as_i) slijedi da je za svaki $a \in G$

$$aR \,|\, aS = \prod_{i=1}^{m} (ar_i)(as_i)^{-1} = a \left(\prod_{i=1}^{m} r_i s_i^{-1} \right) a^{-1} = (R \,|\, S)^a.$$

Stoga, $aR \equiv aS$ ako i samo ako je $R \equiv S$. Dakle, $\equiv$ je G-kongruencija na $\mathcal{R}$ i vrijedi

$$a[R] = [aR].$$

Sada H djeluje tranzitivno ako i samo ako za svaki $R, S \in \mathcal{R}$ postoji $h \in H$ za kojeg je $[hR] = [S]$, tj. za kojeg je

$$1 = (hR) \,|\, S = h^m (R \,|\, S) \quad \Leftrightarrow \quad h^{-m} = R \,|\, S.$$

No ova jednadžba uvijek ima rješenje u H ako su $m = [G : H]$ i $|H|$ relativno prosti.

Djelovanje grupe H na $\mathcal{R}\,|\equiv$ je također regularno kada je $[hR] = [R]$ ako i samo ako je

$$1 = (hR)\,|\,R = h^m(R\,|\,R) = h^m$$

što povlači da je $h = 1$. Stoga, ako je H normalna Abelova podgrupa grupe G, Frattinijev argument povlači da je

$$G = H \rtimes \mathrm{stab}_G([R])$$

za svaki $R \in \mathcal{R}$. Prema tvrdnji konjugacije, svaki konjugat komplementa od H je također komplement od H. S druge strane, ako je

$$G = H \rtimes K$$

tada je $K \in \mathcal{R}$ te je zbog toga

$$H \rtimes K = G = H \rtimes \mathrm{stab}_G([K]).$$

No $K \leq \mathrm{stab}_G([K])$ te je zbog toga

$$K = \mathrm{stab}_G([K]).$$

Dakle, skup komplemenata od H u G je skup

$$\{\mathrm{stab}_G([R]) \mid R \in \mathcal{R}\}.$$

Također, budući da G djeluje tranzitivno na $\mathcal{R}\,|\equiv$, svi stabilizatori su konjugati te su zbog toga svi komplementi od H konjugati.

Teorem 5.1 *(Schur-Zassenhaus - za Abelove podgrupe) Ako je G konačna grupa, tada svaka Abelova normalna Hallova podgrupa od G ima komplement u G. Povrh toga, komplementi od H u G tvore klasu konjugacije od sub(G).*

5.2. Schur-Zassenhausov teorem

Uvjet Abelove podgrupe možemo izostaviti iz Schur-Zassenhausovog teorema.

Teorem 5.2 *(Schur-Zassenhaus) Svaka normalna Hallova podgrupa H konačne grupe G ima komplement u G. Povrh toga, komplementi od H u G tvore klasu konjugiranosti u G. Posebno, svaka normalna Sylowljeva podgrupa od G je komplementirana.*

Dokaz ovog teorema možete potražiti na [1]

Schur-Zassenhausov teorem dovodi nas do sljedećeg vrlo važnog korolara.

Korolar 5.1 *Neka je* $|G| = n\omega$ *gdje je* $(n, \omega) = 1$. *Ako* G *sadrži normalnu (Hallovu) podgrupu* N *reda* n, *tada je svaka podgrupa* N *grupe* G *reda* ω' *koji dijeli* ω *sadržana u nekom komplementu od* N.

Dokaz: Schur-Zassenhausov teorem povlači da postoji $K \leq G$ za koju vrijedi $G = N \rtimes K$. Tada je $|NH \cap K| = \omega'$ i

$$N \rtimes H = N \rtimes (NH \cap K).$$

Stoga, prema Schur-Zassenhausovom teoremu postoji $a \in G$ takav da je

$$H = (NH \cap K)^a \leq K^a.$$

No K^a je također komplement od N u G. □

Literatura

[1] S. Roman, Fundamentals of group theory : An advanced approach, Springer science & Business media, Boston, 2012.

[2] Frattini subgroup, dostupno na:
https://en.m.wikipedia.org/wiki/Frattini_subgroup

[3] Hall subgroup, dostupno na: https://en.m.wikipedia.org/wiki/Hall_subgroup