Sylowljevi teoremi i primjene

Olujević Lujić, Ana

Sveučilište J.J. Storssmayera u Osijeku
Fakultet primijenjene matematike i informatike
Sveučilišni prijediplomski studij Matematika

Ana Olujević

Sylowljevi teoremi i primjene

Završni rad

Osijek 2023.

Sveučilište J.J. Strossmayera u Osijeku
Fakultet primijenjene matematike i informatike
Prijediplomski studij Matematika

Ana Olujević

Sylowljevi teoremi i primjene

Završni rad

Voditelj: prof.dr.sc. Ivan Matić

Osijek 2023.

Sažetak. U ovom završnom radu ćemo se baviti Sylowljevim teoremima i njihovom primjenom. U prvom dijelu rada ćemo iskazati Sylowljeve teorem, a zatim ih i dokazati. U drugom dijelu rada ćemo navesti nekoliko primjera u kojima se primjenjuju iskazani teoremi. Prije nego krenemo s primjerima definirati ćemo nekoliko pojmova koji se koriste u primjerima.

Ključne riječi: Konačne grupe, Sylowljeve p–podgrupe, prost broj, red grupe.

The Sylow theorems and their applications

Abstract. This final paper will discuss Sylow's theorems and their application. In the first part of the paper, we will state Sylow's theorems and then prove them. In the second part of the paper, we will give several examples in which the stated theorems are applied. Before we start with the examples, we will define a couple of terms that are used in the examples.

Key words: Finite groups, Sylow's p-subgroups, prime number, group order.

Sadržaj

1 Uvod

U ovom ćemo radu proučavati isključivo konačne grupe. Neka je G grupa čiji je red djeljiv prostim brojem p. Kažemo da je podgrupa grupe G **Sylowljeva p–podgrupa** ako je njen red najveća potencija od p. Drugim riječima, H je Sylowljeva p–podgrupa od G ako je p–podgrupa i ako njen indeks u G nije djeljiv s p.

Sylowljevi teoremi tvrde da postoje Sylowljeve p–podgrupe za proste brojeve p koji dijele red od G, da su Sylowljeve p–podgrupe za fiksni p konjugirane i da je svaka p–podgrupa sadržana u takvoj podgrupi. Štoviše, teoremi daju ograničenja na mogući broj Sylowljevih p–podgrupa od G.

Definicija 1.1. *([2], Chapter 1) Neka je p prost broj. Ako je G konačna grupa reda p^n za neki prirodan broj n, kažemo da je G p–grupa. Kažemo da je podgrupa H konačne grupe G p–podgrupa ako je H p–grupa.*

Definicija 1.2. *([1], Chapter 1) Red grupe G je broj elemenata skupa G, odnosno $|G|$. Kažemo da je grupa G konačna ukoliko je skup G konačan, te da je grupa beskonačna ukoliko nije konačna.*

Definicija 1.3. *([2], Chapter 1) Kažemo da je podgrupa N od G normalna i označavamo je s $N \trianglelefteq G$, ako $gNg^{-1} = N$ za sve $g \in G$.*

Definicija 1.4. *([2], Example 1.6) Za grupu G kažemo da je ciklička ukoliko je generirana jednim elementom, tj. ako je $G = (r)$ za neki $r \in G$.*

Definicija 1.5. *([2]), Definition 1.20) Kažemo da je homomorfizam iz grupe G u grupu G' preslikavanje $\alpha : G \to G'$ takvo da je $\alpha(ab) = \alpha(a)\alpha(b)$ za sve $a, b \in G$.*

Izomorfizam je bijektivni homomorfizam.

Automorfizam grupe G je izomorfizam grupe na samu sebe, skup svih automorfizama grupe G označavamo s $Aut(G)$.

Definicija 1.6. *([2], Example 1.12) Neka je G grupa. Podskup*

$$Z(G) = \{x \in G : ax = xa, \forall a \in G\}$$

nazivamo centar grupe G. Centar grupe G sadrži upravo one elemente koji komutiraju sa svim elementima iz G.

2 Sylowljevi teoremi

Neka grupa H djeluje na skup X te neka je O orbita elementa x_0. Često ćemo koristiti preslikavanje $H \to X, h \mapsto hx_0$ koje inducira bijekciju

$$H/Stab(x_0) \to O;$$

stoga

$$(H : Stab(x_0)) = |O|.$$

Konkretno kada je H p–podgrupa, $|O|$ je potencija od p, pa se ili O sastoji od jednog elementa ili je $|O|$ djeljiv s p. Kako je X disjunktna unija orbita, možemo zaključiti:

Lema 2.1. *([2], Lemma 5.1)*
Neka je H p–podgrupa koja djeluje na konačnome skupu X, i neka je X^H skup fiksnih točaka od H, tada

$$|X| \equiv |X^H| \pmod{p}.$$

Kada lemu primjenimo na p–grupu H koja djeluje na samu sebe konjugiranjem, vidimo da vrijedi

$$(Z(H) : 1) = (H : 1) \pmod{p}$$

pa i $p \mid (Z(H) : 1)$.

Teorem. 2.2 (Prvi Sylowljev teorem). *([1],Theorem 5.2) Neka je G konačna grupa i neka je p prost broj. Ako $p^r|(G : 1)$, tada G ima podgrupu reda p^r.*

Dokaz. Kako vrijedi da grupa reda p^n ima normalnu podgrupu reda p^m za sve $m \leq n$, dovoljno je dokazati da tvrdnja vrijedi za p^r pri čemu je p^r najveća potencija od p koji dijeli $(G : 1)$, pa stoga pretpostavimo da je $(G : 1) = p^r m$, gdje m nije djeljiv s p.
Neka je

$$X = \{\text{podskupovi od } G \text{ s } p^r \text{ elemenata}\},$$

s djelovanjem od G definiranim s

$$G \times X \to X, \qquad (g, A) \mapsto gA \stackrel{def}{=} \{ga | a \in A\}.$$

Neka je $A \in X$, i neka

$$H = Stab(A) \stackrel{def}{=} \{g \in G | gA = A\}.$$

Za bilo koji $a \in A$, $h \mapsto ha_0 : H \to A$ je injektivno, stoga je $(H : 1) \leq |A| = p^r$. U jednakosti

$$(G : 1) = (G : H)(H : 1)$$

znamo da je $(G : 1) = p^r m$, $(H : 1) \leq p^r$, i da je $(G : H)$ broj elemenata u orbiti od A. Ako možemo pronaći A takav da p ne dijeli broj elemenata u njegovoj orbiti, onda možemo

zaključiti da za takav A, $H = Stab(A)$ ima red p^r. Broj elemenata u X je

$$|X| = \binom{p^r m}{p^r} = \frac{(p^r m)(p^r m - 1)\cdots(p^r m - i)\cdots(p^r m - p^r + 1)}{p^r(p^r - 1)\cdots(p^r - i)\cdots(p^r - p^r + 1)}.$$

Primjetimo, jer je $i < p^r$, potencija od p koja dijeli $p^r m - i$ je potencija od p koja dijeli i. Isto vrijedi i za $p^r - i$. Stoga su odgovarajući članovi u brojniku i nazivniku djeljivi s istim potencijama od p, pa p ne dijeli $|X|$. Budući da orbite tvore particiju od X,

$$|X| = \sum |O_i|, \qquad O_i$$

gdje su O_i različite orbite,i tako barem jedan od O_i nije djeljiv s p. □

Primjer 2.3. *([2], Example 5.3) Neka je $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ polje s p elemenata, i neka je $G = GL_n(\mathbb{F}_p)$. Matrice $n \times n$ u G su upravo one čiji stupci tvore bazu za $\mathbb{F}_p^n$. Prema tome, prvi stupac može biti bilo koji nenulvektor u $\mathbb{F}_p^n$, kojih ima $p-1$; drugi stupac može biti bilo koji vektor koji nije u rasponu prvog stupca, kojih ima $p^n - p$, i tako redom. Prema tome, red od G je*

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

pa je potencija od p koji dijeli $(G:1)$ jednaka $p^{1+2+\ldots+(n-1)}$.

Promotrimo gornje trokutaste matrice s jedinicama na glavnoj dijagonali:

$$\begin{pmatrix} 1 & * & * & \ldots & * \\ 0 & 1 & * & \ldots & * \\ 0 & 0 & 1 & \ldots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix}.$$

One tvore podgrupu U reda $p^{n-1}p^{n-2}\cdots p$, dakle Sylowljevu p–podgrupu od G.

Teorem. 2.4. ***Drugi Sylowljev teorem*** *([2],Theorem 5.6) Neka je G konačna grupa i neka je $|G| = p^r m$ gdje m nije djeljiv s p.*

1. *Svake dvije Sylowljeve p–podgrupe su konjugirane.*
2. *Neka je s_p broj Sylowljevih p–podgrupa u G; tada je $s_p \equiv 1 \pmod p$ i $s_p | m$.*
3. *Svaka p–podgrupa od G sadržana je u Sylowljevoj p–podgrupi.*

Neka je H podgrupa od G. Normalizator od H u G je

$$N_G = \left\{ g \in G \mid gHg^{-1} = H \right\};$$

broj konjugiranih elemenata od H u G je $(G : N_G(H))$.

Lema 2.5. *([2],Lemma 5.7) Neka je P Sylowljeva p–podgrupa od G i H p–podgrupa. Ako H normalizira P, tj. ako $H \subset N_G(P)$ tada je $H \subset P$. Posebno, nijedna Sylowljeva P–podgrupa od G osim P ne normalizira P.*

Dokaz. (**Drugi Sylowljev teorem**)

1. Neka je X skup Sylowljevih p–podgrupa u G, i neka G djeluje na X konjugacijom

$$(g, P) \mapsto gPg^{-1} : G \times X \to X.$$

Neka O bude jedna od G–orbita: trebamo pokazati da je O cijeli X. Neka je $P \in O$ i neka P djeluje na O djelovanjem od G. Jedna G–orbita može se raspasti u nekoliko P–orbita, od kojih će jedna biti $\{P\}$. Zapravo to je jedina jednočlana orbita jer

$$\{Q) \text{ je } P\text{-orbita} \iff P \text{ normalizira } Q,$$

a znamo da to vrijedi samo za $Q = P$. Stoga je broj elemenata u svakoj P–orbiti različitoj od $\{P\}$ djeljiv s p i imamo da je $|O| \equiv 1 \pmod{p}$.
Pretpostavimo da postoji $P \notin O$. Ponovno dopuštamo da P djeluje na O, ali ovaj puta argumentiramo da ne postoje jednočlane orbite, pa je broj elmenata u svakoj P–orbiti djeljiv s p. To implicira da je $|O|$ djeljivo s p, što je u suprotnom s ranije dokazanom kongruencijom. Ne može postojati takav P , pa je O cijeli X.

2. Neka je s_p broj elemenata u O, pokazali smo da je $s_p \equiv 1 \pmod{p}$ i neka je P Sylowljeva p–podgrupa od G. Prema 1., s_p je broj konjugata od P koji je jednak

$$(G : N_G(P)) = \frac{(G:1)}{(N_G:1)} = \frac{(G:1)}{(N_G(P):P)(P:1)} = \frac{m}{(N_G(P):P)},$$

što je djelitelj od m.

3. Neka je H p–podgrupa od G, i neka H djeluje konjugiranjem na skup X, gdje je X skup Sylowljevih p–podgrupa. Budući da $|X| = s_p$ nije djeljivo s p , X^H mora biti neprazan, tj. barem jedna H–orbita sastoji se od jedne Sylowljeve p–podgrupe. Tada H normalizira P i prema Lema 2.5 vrijedi $H \subseteq P$. □

Korolar 2.6. *([2], Corollary 5.8) Sylowljeva p–podgrupa je normalna ako i samo ako je jedina Sylowljeva p–podgrupa.*

Definicija 2.7. *([2], Chapter 1) Neka je G grupa i neka su $H_1, \ldots, H_k$ njene podgrupe. Kažemo da je G direktan produkt svojih podgrupa H_i ako je preslikavanje*

$$(h_1, h_2, \ldots, h_k) \mapsto h_1 h_2 \cdots h_k : H_1 \times H_2 \times \cdots \times H_k \to G$$

izomorfizam grupa.

Definicija 2.8. *([2], Definition 3.8) Kažemo da je grupa G semidirektan produkt svojih podgrupa N i Q ako je N normalna i ako homomorfizam $G \to G/N$ inducira izomorfizam $Q \to G/N$. Pišemo $G = N \rtimes Q$ (ili $G = N \rtimes_\Theta Q$, kada je $\Theta : Q \to Aut(N)$).*

Korolar 2.9. *([2], Corollary 5.9) Pretpostavimo da grupa G ima samo jednu Sylowljevu p–podgrupu za svaki prost broj p koji dijeli njezin red. Tada je G direktan produkt svojih Sylowljevih p–podgrupa.*

Prethodna dva korolara nećemo dokazivati, a dokaz se može naći u ([2], Corollary 5.8, Corollary 5.9)

3 Primjene Sylowljevih teorema

Primjer 3.1 (Grupe reda 99). *([2], Example 5.13) Neka grupa G ima red 99. Sylowljevi teoremi impliciraju da grupa G ima barem jednu podgrupu H reda 11, i vrijedi $s_{11} \mid \frac{99}{11}$ i $s_{11} \equiv 1 \pmod{11}$. Slijedi da je $s_{11} = 1$ i H je normalna. Slično, $s_9 \mid 11$ i $s_9 \equiv 1 \pmod{3}$, pa je i Sylowljeva 3–podgrupa također normalna. Stoga je G izomorfna direktonom produktu svojih Sylowljevih podgrupa koje su obje komutativne, pa je stoga i G komutativna.*
Navedimo i alternativni dokaz. Prvo na isti način kao i prije provjerimo da je Sylowljeva 11–podgrupa N od G normalna. Sylowljeva 3–podgrupa Q bijektivno se preslikava na G/N, pa je $G = N \times Q$. Ostaje odrediti djelovanje Q na N konjugiranjem. Kako je N grupa reda 11, N je ciklička grupa, te prema [1, 3.5a)] vrijedi da je $Aut(N)$ ciklička grupa reda 10, pa postoji samo trivijalni homomorfizam $Q \to Aut(N)$, iz čega slijedi da je G direktan produkt od N i Q.

Primjer 3.2 (Grupe reda pq, gdje su p i q prosti , $p < q$). *([2], Example 5.14) Neka je G takva grupa i neka su P i Q Sylowljeve p i q podgrupe. Tada je $(G : Q) = p$ što je najmanji prosti broj koji dijeli $(G : 1)$, pa je Q normalna. Jer se P bijektivno preslikava na G/Q imamo*

$$G = Q \times P,$$

te još ostaje odrediti djelovanje P na Q konjugiranjem.
Grupa $Aut(Q)$ je ciklička reda $q - 1$, pa je $G = Q \times P$, osim ako $p \mid q - 1$. Ako $p \mid q - 1$, tada $Aut(Q)$ ima jedinstvenu podgrupu P' reda p. Zapravo se P' sastoji od preslikavanja

$$x \mapsto x^i,\ \{i \in \mathbb{Z}/q\mathbb{Z} \mid i^p = 1\}.$$

Neka su a i b generatori za P odnosno Q i pretpostavimo da je djelovanje od a na Q dano s $x \mapsto x^{i_0}$, $i_0 \neq 1$ (u $\mathbb{Z}/q\mathbb{Z}$). Tada je G zadana generatorima a i b relacijama

$$a^p,\ b^q,\ aba^{-1} = b^{i_0}.$$

Ukratko: ako $p \nmid q - 1$, tada je jedina grupa reda pq ciklička grupa C_{pq}; ako $p \mid q - 1$, tada postoji i nekomutativna grupa dana gornjim generatorima i relacijama.

Primjer 3.3 (Grupa reda 30). *([2], Example 5.15) Neka je G grupa reda 30. Tada*

$$s_3 = 1, 4, 7, \ldots \text{ i dijeli } 10;$$

$$s_5 = 1, 6, 11, \ldots \text{ i dijeli } 6.$$

Stoga je $s_3 = 1$ ili 10, $s_5 = 1$ ili 6. Zapravo, barem je jedan od brojeva s_3 i s_4 jednak 1, jer bi inače postojali 20 elemenata reda 3 i 24 elementa reda 5, što je nemoguće. Prema tome, Sylowljeva 3–podgrupa P ili Sylowljeva 5–podgrupa je normalna, pa je $H = PQ$ podgrupa od G. Kako 3 ne dijeli $5 - 1 = 4$, vrijedi da je H komutativna, $H \cong C_3 \times C_5$. Stoga

$$G = (C_3 \times C_5) \times_\Theta C_2,$$

te preostaje odrediti moguće homomorfizme $\Theta : C_2 \to Aut(C_3 \times C_5)$. Ali takav homomorfizam Θ je određen slikom elementa od C_2 različitog od identitete, koji mora biti element reda 2. Neka a, b, c generiraju C_3, C_5, C_2. Tada

$$Aut\,(C_3 \times C_5) = Aut\,(C_3) \times Aut\,(C_5)\,,$$

a jedini elementi od $Aut(C_3)$ i $Aut(C_5)$ reda 2 su $a \mapsto a^{-1}$ i $b \mapsto b^{-1}$. Dakle postoje točno četiri homomorfizma Θ, a $\Theta(c)$ je jedan od sljedećih elemenata:

$$\begin{cases} a \mapsto a \\ b \mapsto b \end{cases} \quad \begin{cases} a \mapsto a \\ b \mapsto b^{-1} \end{cases} \quad \begin{cases} a \mapsto a^{-1} \\ b \mapsto b \end{cases} \quad \begin{cases} a \mapsto a^{-1} \\ b \mapsto b^{-1} \end{cases} .$$

Grupe koje odgovaraju tim homomorfizmima imaju centre reda 30, 3 *(generirane s a),* 5 *(generirane s b) i* 1 *redom, te su prema tome neizomorfne. Pokazali smo (do izomorfizma) da postoje točno* 4 *grupe reda* 30. *Primjer, treća na našem popisu ima generatore a,b i c i relacije*

$$a^3, \quad b^5, \quad c^2, \quad ab = ba, \quad cac^{-1} = a^{-1}, \quad cbc^{-1} = b.$$

Primjer 3.4 (Grupe reda 12)**.** *([2], Example 5.16) Neka je G grupa reda* 12 *i neka je P njena Sylowljeva* 3*–podgrupa. Ako P nije normalna, tada P ne sadrži netrivijalnu normalnu podgrupu od G, te je preslikavanje*

$$\varphi : G \to Sym\,(G/P) \approx S_4$$

injekcija, a njegova slika je podgrupa od S_4 *reda* 12. *Prema Drugom Sylowljevom teoremu vidimo da G ima točno* 4 *Sylowljeve* 3*–podgrupe, te stoga imamo točno* 8 *elemenata reda* 3. *Ali svi elementi od* S_4 *reda* 3 *su u* A_4, *pa* $\varphi(G)$ *siječe* A_4 *u podgrupama s najmanje* 8 *elemenata. Prema Lagrangeovom teoremu* $\varphi(G) = A_4$ *pa vrijedi* $G \approx A_4$.
Sada pretpostavimo da je P normalna. Tada $G = P \rtimes Q$, *gdje je Q Sylowljeva* 4*–podgrupa. Ako je Q ciklička reda* 4 *tada postoji jedinstveno netrivijano preslikavanje* $Q(= C_4) \to Aut(P)(= C_2)$, *pa stoga dobivamo jednu nekomutativnu grupu* $C_3 \rtimes C_4$. *Ako je* $Q = C_2 \times C_2$, *tada postoje točno tri netrivijalna homomorfizma* $\Theta : Q \to Aut(P)$ *ali sve tri dobivene grupe su izomorfne s* $S_3 \times C_2$ *gdje je* $C_2 = Ker(\Theta)$.
Konačno, postoje 3 *nekomutativne grupe reda* 12 *i* 2 *komutativne grupe reda* 12.

Primjer 3.5 (Grupe reda $2p^n$, $4p^n$ i $8p^n$, za n neparan)**.** *([2], Example 5.18) Neka je G grupa reda* $2^m p^n$, $1 \leqslant m \leqslant 3$, *p neparan prost broj,* $1 \leqslant n$. *Pokazati ćemo da G nije prosta. Neka je P Sylowljeva p–podgrupa i neka je* $N = N_G(P)$ *tako je da je* $s_p = (G : N)$.
Prema Drugom Sylowljevom teoremu znamo da $s_p \mid 2^m$, $s_p = 1, p+1, 2p+1, \ldots$. *Ako je* $s_p = 1$, *P je normalna.*
Ako nije, postoje dva slučaja koja ćemo razmotriti:

(i) $s_p = 4$ *i* $p = 3$, *ili*

(i) $s_p = 8$ *i* $p = 7$.

U prvom slučaju, djelovanje G konjugiranjem na skup Sylowljevih 3*–podgrupa definira homomorfizam* $G \to S_4$, *koji , ako je G prosta, mora biti injektivan. Prema tome* $(G : 1) \mid 4!$, *a kako je* $n = 1$, *imamo* $(G : 1) = 2^m 3$. *Sada Sylowljeva* 2*–podgrupa ima red* 3, *pa imamo homomorfizam* $G \to S_3$, *čija je jezgra netrivijalna normalna podgrupa od G.*
U drugom slučaju, isti argument pokazuje da $(G : 1) \mid 8!$ *pa je opet* $n = 1$. *Prema tome* $(G : 1) = 56$ *i* $s_7 = 8$. *Stoga G ima* 48 *elemenata reda* 7, *pa može postojati samo jedna Sylowljeva* 2*–podgrupa koja mora biti normalna.*

Primjer 3.6 (Grupe reda 60)**.** *([2], Example 5.19) Neka je G prosta grupa reda* 60. *Pokazati ćemo da je G izomorfna s* A_5. *Neka je P Sylowljeva* 2*–podgrupa i* $N = N_G(P)$, *tako da je* $s_2 = (G : N)$. *Prema Sylowljevim teoremima,* $s_2 = 1, 3, 5$ *ili* 15.
(a) Slučaj $s_2 = 1$ *je nemoguć, jer bi P bila normalna.*
(b)Slučaj $s_2 = 3$ *je nemoguć, jer bi jezgra od* $G \to Sym(G/N)$ *bila netrivijalna normalna podgrupa od G.*

(c) U slučaju da je $s_2 = 5$*, dobivamo inkluziju* $G \hookrightarrow Sym(G/N) = S_5$*, koja realizira* G *kao podgrupu indeksa* 2 *od* S_5*, a mi znamo da je za* $n \geq 5$*,* A_n *je jedina podgrupa indeksa* 2 *od* S_n*.*
(d) U slučaju da je $s_2 = 15$*, uzmemo li da je* $s_5 = 6$ *prebrojavanjem dobivamo da postoje* 2 *Sylowljeve* 2*–podgrupe* P *i* Q *koje se sijeku u grupi reda* 2*. Normalizator* N *od* $P \cap Q$ *sadrži* P *i* Q*, pa ima indeks* $1, 3$ *ili* 5 *u* G*. Prva dva slučaja su nemoguća iz istih razloga kao u (a) i (b). Ako je* $(G : N) = 5$*, argument u (c) daje izomorfizam* $G \approx A_5$*; ali to je nemoguće jer je* $s_2(A_5) = 5$*.*

Literatura

[1] T.W. Hungerfotd, Algebra, Springer-Verlag, New York, 1974.

[2] J. S. Milne, Group Theory, Version 4.00, 2021., dostupno na: `http://www.jmilne.org/math/CourseNotes/GT.pdf`