UNIVERZA V LJUBLJANI
FAKULTETA ZA MATEMATIKO IN FIZIKO

Matematika – 1. stopnja

Nina Vidmar

Schur–Zassenhausov izrek

Delo diplomskega seminarja

Mentor: doc. dr. Primož Moravec

Ljubljana, 2012

Kazalo

Schur–Zassenhausov izrek

Povzetek

Schur–Zassenhausov izrek je eden izmed pomembnejših izrekov v teoriji končnih grup. Pove nam, kdaj ima podgrupa edinka v dani grupi komplement, saj komplement v splošnem ne obstaja vedno. Uporabimo ga lahko kot orodje pri klasifikaciji končnih grup, saj nam pove nekaj o strukturi grupe.

Spoznali bomo tri sorodne izreke, ki vsi govorijo o komplementih podgrup edink. Zadnji in seveda najpomembnejši bo Schur–Zassenhausov izrek, tisti, ki nam bo povedal, kdaj za podgrupo edinko komplement obstaja in kaj za take komplemente velja. Dokaz izreka je zelo obsežen in poteka s pomočjo uporabe izrekov Sylowa, p-grup in rešljivih grup.

Theorem of Schur–Zassenhaus

Abstract

The Schur–Zassenhaus theorem is one of the most important theorems in the theory of finite groups. This result gives conditions, under which a normal subgroup of a given finite group admits a complement. Note that in general such complements do not exist. Therefore, the theorem tells us something about the structure of a group and it is a tool for the classification of finite groups.

We will introduce three related theorems about complements of normal subgroups. The last and the most important one is the theorem of Schur–Zassenhaus, which gives information on when complements of a normal subgroup exist and how they look like. This result has a very elaborate proof, which uses tools like Sylow theorem, the theory of p-groups and solvable groups.

Math. Subj. Class. (2010): 20D10, 20D15, 20D20, 20E22, 20E34

Ključne besede: grupa, Schur–Zassenhausov izrek, podgrupa edinka, komplement

Keywords: group, theorem of Schur–Zassenhaus, normal subgroup, complement

1. Uvod

Cilj matematikov, ki se ukvarjajo s teorijo končnih grup, je že od nekdaj klasifikacija le teh. Določitev strukture vseh končnih grup pa se je izkazala za zelo obsežen problem, saj v nekaterih primerih, kot so na primer p-grupe, število vseh možnih struktur postane preveliko. Kot primer navedimo, da obstaja 10494213 neizomorfnih tipov grup moči 512, kar naredi njihovo klasifikacijo praktično nemogočo.

Po drugi strani je bila eden od največjih dosežkov v matematiki nasploh klasifikacija vseh končnih enostavnih grup. To so grupe, v katerih sta edini podgrupi edinki trivialna grupa in pa celotna grupa. Klasifikacija je povzeta v izreku, ki pravi:

Vsaka končna enostavna grupa je izomorfna eni od grup naslednjih tipov:

- ciklični grupi praštevilskega reda,
- alternirajoči grupi stopnje vsaj 5,
- enostavni grupi Liejevega tipa,
- eni izmed 26 sporadičnih enostavnih grup.

Klasifikacija obsega približno 10000 strani, napisalo jo je približno 100 avtorjev, objavljena pa je bila v večini med letoma 1955 in 2004. Opomniti velja, da do danes še nikomur ni uspelo zbrati celotnega dokaza na enem mestu. Več zanimivosti o klasifikaciji si lahko preberete na [6].

S pomočjo klasifikacije enostavnih končnih grup pa lahko načeloma klasificiramo tudi vse končne. Eden izmed načinov je preko kompozicijske vrste, ta za dano grupo G izgleda takole:

$$\{1\} = N_1 \lhd N_2 \lhd \cdots \lhd N_k = G,$$

kjer so N_{i-1} maksimalne podgrupe edinke v N_i, kar je ekvivalentno temu, da so kvocienti N_i/N_{i-1} končne enostavne grupe za $i = 1, \ldots, k$, pri čemer je to vrsta maksimalne dolžine. Definicijo in več o kompozicijskih vrstah lahko najdete na spletni strani, navedeni v [7].

Klasifikacijo kvocientov N_i/N_{i-1} torej poznamo. Očitno poznamo tudi $N_1 = \{1\}$, $N_2/N_1 = N_2$ in N_3/N_2, zato N_3 poznamo, če znamo konstruirati razširitev N_2 z N_3/N_2 in tako naprej še za vse ostale edinke v vrsti, vse do G.

Na tem mestu je smiselno povedati, kaj za poljubni grupi N in H pomeni razširitev N s H. Neformalno rečeno je to grupa G, ki vsebuje tako podgrupo edinko M, da je $M \cong N$ in $G/M \cong H$. V grobem rečeno je cilj teorije razširitev pokazati, kako lahko konstruiramo grupo iz podgrupe edinke in njene kvocientne grupe. Formalna definicija pa pravi naslednje:

Definicija 1.1. Naj bosta N in H poljubni grupi. Grupna *razširitev* N s H je kratko eksaktno zaporedje grup in homomorfizmov

$$\{1\} \longrightarrow N \xrightarrow{\mu} G \xrightarrow{\varepsilon} H \longrightarrow \{1\},$$

kjer je μ injektiven, ε surjektiven in $\operatorname{im}\mu = \ker\varepsilon = M$.

Za homomorfizme velja, da so njihova jedra edinke v grupi, iz katere slikajo, torej je M edinka v G. Velja tudi, da je $N/\ker\mu = N/\{1\} = N \cong \operatorname{im}\mu = M$, torej je $M \cong N$. Prav tako je $G/\ker\varepsilon = G/M \cong \operatorname{im}\varepsilon = H$, zato je $G/M \cong H$ in G je razširitev N s H kot neformalno rečeno. Zgornji zaključki sledijo iz izrekov o homomorfizmih, ki jih lahko najdete v [4].

Strategija klasifikacije končnih grup torej zajema poznavanje vseh končnih enostavnih grup in hkrati postopek konstrukcije vseh razširitev dane grupe N z grupo H. Izkaže pa se, da je slednje zelo težak problem v splošnem.

Po drugi strani so nekatere razširitve grup odlikovane. Take so na primer razcepne razširitve, o katerih lahko izveste več v [3].

Definicija 1.2. Naj bosta N in H taki podgrupi grupe G, da velja $G = HN$ in $H \cap N = \{1\}$. Podgrupi H pravimo *komplement* podgrupe N v grupi G.

V primeru, ko je N edinka v G, komplementu pravimo *semidirektni produkt* in pišemo

$$G = H \ltimes N \quad \text{ali} \quad G = N \rtimes H.$$

Če sta N in H taki, da tvorita semidirektni produkt, torej njun produkt je neka grupa v kateri je N edinka in njun presek je trivialen, se izkaže, da je naš iskani G ravno $H \ltimes N$, oziroma natančneje, $G \cong H \ltimes N$. Taka razširitev je razcepna razširitev, še več, izkaže se, da je vsaka razcepna razširitev semidirektno-produktna razširitev (razširitev, ki je semidirektni produkt). Več o tem lahko najdete v [3].

Če se vrnemo nazaj h kompozicijski vrsti, vidimo, da so grupe v vrsti podane, kar pa nas zanima, je njihova struktura oziroma klasifikacija. Strukturo N_i/N_{i-1} za $i = 1, \ldots, k$ že poznamo in recimo, da poznamo strukturo N_j za $j = 1, \ldots, s$ kjer $s \leq k$. Če sta N_s in N_{s+1}/N_s taki, da skupaj tvorita semidirektni produkt, je N_{s+1} izomorfna temu semidirektnemu produktu. S tem smo ugotovili, da je N_{s+1} semidirektni produkt dveh grup, katerih klasifikacijo poznamo. Na to pa zdaj lahko pogledamo malce drugače. Ali ima N_s, ki je edinka v N_{s+1}, komplement v N_{s+1} in ali je morda enolično določen.

Seveda komplement ne obstaja vedno in tudi ni enoličen, se pa izkaže, da so komplementi, če obstajajo, povezani med seboj. Eden od rezultatov, ki zagotavlja obstoj komplementa in pove, kako so taki komplementi med seboj povezani, je Schur–Zassenhausov izrek:

Izrek 1.3 (Schur–Zassenhaus)**.** *Imejmo grupo G in K njeno podgrupo edinko, za kateri velja, da sta si $|K|$ in $|G/K|$ tuji si števili, oziroma krajše*

$$(|K|, |G/K|) = 1.$$

Potem ima K komplement v G. Če velja še, da je ena izmed K ali G/K rešljiva, potem so vsi komplementi konjugirani v G.

Izrek nam v resnici odgovori na vprašanje, kdaj lahko grupo G konstruiramo iz njene podgrupe edinke N in kvocientne grupe G/N. V članku, ki je naveden v [1], si lahko preberete več o tem.

Komplement pa je včasih koristno imeti iz povsem preprostega razloga. Izkaže se, kar bomo v nadaljevanju tudi pokazali, da se da v primeru, ko je grupa sestavljena iz edinke in njenega komplementa, vsak njen element enolično izraziti kot produkt elementov edinke in njenega komplementa, torej izvemo še nekaj dodatnega o strukturi elementov v grupi.

Iskanja komplementov oziroma iskanja odgovora o njihovem obstoju se bomo lotili postopoma. V prvem razdelku se bomo omejili na primer, ko je podgrupa edinka Abelova podgrupa in dokazali Schur–Zassenhausov izrek za Abelove edinke. Ta dokaz nam bo v pomoč pri dokazu naslednjega pomembnega izreka in pa tudi malo pri dokazu zadnjega izreka, izreka za edinke, ki niso nujno Abelove.

V drugem razdelku bomo pogledali izrek, ki je posplošitev Schur–Zassenhausovega izreka za edinke. To bo Gaschützov izrek, ki pravi:

Izrek 1.4 (Gaschützov izrek)**.** *Naj bosta K Abelova podgrupa edinka grupe G in U podgrupa G taki, da velja*

$$K \leq U \quad in \quad (|K|, |G/U|) = 1.$$

(a) *Recimo, da ima K komplement v U. Potem ima K komplement tudi v G.*
(b) *Recimo, da sta H_0 in H_1 dva taka komplementa K v G, da velja*

$$H_0 \cap U = H_1 \cap U.$$

Potem sta H_0 in H_1 konjugirana v G.

In končno, v tretjem razdelku, se bomo lotili Schur–Zassenhausovega izreka, tistega splošnega, ki govori o komplementih podgrup edink, ki niso nujno Abelove. Zanj bomo porabili največ časa, saj bomo morali prej spoznati kar nekaj novih pojmov, izrekov in trditev, ki nam bodo pomagali pri dokazu.

2. Schur–Zassenhausov izrek za Abelove edinke

V tem razdelku bomo spoznali in dokazali različico Schur-Zassenhausovega izreka, ki nam pove, kaj mora veljati, da ima podgrupa edinka, ki je Abelova, v dani grupi komplement.

2.1. Osnovne definicije in rezultat.

Za začetek si poglejmo nekaj osnovnih pojmov, ki nas bodo spremljali do konca.

Definicija 2.1. Naj bo G grupa in N taka njena podgrupa, da velja $xNx^{-1} = N$ za vsak $x \in G$, oziroma ekvivalentno, $xN = Nx$ za vsak $x \in G$. Potem podgrupi N pravimo *podgrupa edinka* grupe G in označimo $N \lhd G$.

Primer 2.2. Če je G poljubna grupa, je njen *center*

$$Z(G) = \{c \in G \mid cx = xc, \text{ za vse } x \in G\}$$

edinka.

V nadaljevanju bomo večkrat uporabili dejstvo, da je NH podgrupa v G za $N \lhd G$ in $H \leq G$. Prepričajmo se, da je to res. Vzemimo $a, b \in NH$ in preverimo, da je $ab^{-1} \in NH$. Če pišemo $a = nh$ in $b = n'h'$ za $n, n' \in N$ in $h, h' \in H$, dobimo

$$ab^{-1} = nh(n'h')^{-1} = nhh'^{-1}n'^{-1} = nh''n'^{-1} \overset{N \text{ edinka}}{=} n''h'',$$

kjer je $n'' \in N$ in $h'' \in H$, torej je $ab^{-1} \in NH$.

Definicija 2.3. Naj bosta H in U taki podgrupi grupe G, da velja $G = HU$ in $U \cap H = \{1\}$. Podgrupi H pravimo *komplement* podgrupe U v grupi G.

V primeru, ko je U edinka (tedaj velja tudi $G = HU = UH$), pravimo, da je G *semidirektni* produkt U in H in pišemo

$$G = H \ltimes U.$$

Trditev 2.4. *Naj bo G grupa, $N \lhd G$ in $H \leq G$. Če je G semidirektni produkt N in H, potem se da vsak $g \in G$ enolično izraziti kot $g = nh$, kjer je $n \in N$ in $h \in H$.*

Dokaz. Pa recimo, da lahko neki $g \in G$ zapišemo na dva načina, $g = n_1h_1 = n_2h_2$. Iz tega sledi, da je $n_2^{-1}n_1 = h_2h_1^{-1} \in N \cap H = \{1\}$. Kar pa pomeni, da je $n_1 = n_2$ in $h_1 = h_2$. □

Definicija 2.5. Naj bo G poljubna grupa, $U \leq G$ in $x \in G$. Potem je

- $Ux = \{ux \mid u \in U\}$ *desni odsek* (grupe G po podgrupi U),

- $xU = \{xu \mid u \in U\}$ *levi odsek.*

Če je U edinka, sta Ux in xU enaka. Ker bomo v nadaljevanju obravnavali samo primere, kjer bomo imeli podgrupo edinko, bomo od sedaj naprej govorili le o odsekih.

Definicija 2.6. Naj bo G grupa in $H \leq G$. Množici

$$G/H = \{gH \mid g \in G\}$$

vseh odsekov grupe G po podgrupi H pravimo *kvocientna* ali *faktorska množica.*

Če je H edinka, je kvocientna množica grupa.

Definicija 2.7. Moč množice vseh odsekov $|G/H|$ imenujemo *indeks* podgrupe H v grupi G in označimo z $|G : H|$.

- Če je množica desnih/levih odsekov grupe G po podgrupi U končna, potem je število desnih/levih odsekov enako $|G : U|$ (indeks podgrupe U v grupi G ali moč kvocientne množice).
- Dva odseka sta bodisi enaka, bodisi disjunktna.

Dokaze osnovne rezultatov o kvocientnih množicah in odsekih, ki smo jih zapisali zgoraj, lahko najdete v [2].

Sedaj si oglejmo dva primera, da se že na začetku prepričamo, da komplement v splošnem ne obstaja vedno.

Primer 2.8.

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$$

je kvaternionska grupa moči 8, sestavljena iz elementov, za katere velja

$$i^2 = j^2 = k^2 = -1 \quad \text{in} \quad ij = k = -ji.$$

$$Z(Q_8) = \{\pm 1\}$$

je center kvaternionske grupe (množica elementov, ki komutirajo z vsemi ostalimi elementi, očitno je edinka).

Njegov komplement bi moral vsebovati elemente i, j, in k do predznaka natančno, ampak potem pa bi vseboval tudi -1, torej ta edinka nima komplementa.

Primer 2.9.

$$D_4 = \langle \sigma, \tau | \sigma^4 = id, \tau^2 = id, \tau\sigma\tau = \sigma^{-1} \rangle$$

je diedrska grupa moči 8. Vzemimo

$$U = \langle \sigma \rangle.$$

Vidimo, da je $|U| = 4$, torej je $|D_4 : U| = \frac{|D_4|}{|U|} = 2$ in iz tega sledi, da je U edinka v D_4. Res, saj velja izrek, ki pravi, da če je $H \leq G$ in $|G : H| = 2$, potem je $H \lhd G$. Velja pa tudi Lagrangeev izrek, ki nam pove, da za končne grupe velja $|G| = |G : H||H|$, oziroma $|G : H| = \frac{|G|}{|H|}$. Oba izreka lahko najdete na primer v [4]. Sedaj pa si poglejmo

$$S = \langle \tau \rangle.$$

Očitno je, da je $D_4 = US$, saj sta generatorja teh dveh podgrup ravno generatorja grupe D_4 in v njunem preseku je samo enota, torej je S komplement U v D_4.

Poglejmo sedaj, kaj pravi glavni izrek tega razdelka.

Izrek 2.10 (Schur–Zassenhaus)**.** *Naj bo K taka Abelova podgrupa edinka grupe G, da sta $|K|$ in $|G:K|$ tuji si števili, oziroma krajše, $(|K|, |G:K|) = 1$. Potem ima K komplement v G in vsi komplementi so med seboj konjugirani v G.*

Izrek nam pove, kdaj zagotovo imamo komplement, lahko pa edinka ne zadošča pogojem izreka, pa vseeno ima komplement. To lahko vidimo v primeru 2.9, kjer si števili 4 in 2 očitno nista tuji.

Izrek za splošne edinke se zelo malo razlikuje od zgornjega izreka, le za konjugiranost komplementov je treba predpostaviti, da je ena izmed K ali G/K rešljiva. V resnici pa se izkaže, da je to vedno res, več o tem v tretjem razdelku.

Kot ponavadi ima izrek več dokazov. Na primer, izredno lepa in pa tudi zahtevna je povezava tega izreka s teorijo razširitev grup.

Naš dokaz bo razmeroma elementaren, metodi, s katero se ga bomo lotili, pravimo metoda Wielandta in je opisana v [2]. Še preden se direktno lotimo dokaza, si moramo pripraviti teren, spoznati nekaj pojmov in narediti nekaj izpeljav.

2.2. **Metoda Wielandta.**

Definicija 2.11. Naj bosta $U \leq G$ in $S \subseteq G$. Potem je S *desna transverzala* podgrupe U v grupi G (ali množica predstavnikov desnih odsekov), če S vsebuje natanko en element iz vsakega desnega odseka Ux, $x \in G$.

Podobno definiramo levo transverzalo. V primeru, ko je U edinka, so desni odseki enaki levim in lahko govorimo samo o transverzali.

Definicija 2.12. G grupa, $\Omega = \{\alpha, \beta, \dots\}$ neprazna končna množica. Grupa G *deluje* na Ω, če za vsak par $(\alpha, g) \in \Omega \times G$ element $\alpha^g \in \Omega$ zadošča:

$\mathcal{O}_1$ $\alpha^1 = \alpha$ za $1 = 1_G$ in vsak $\alpha \in \Omega$,

$\mathcal{O}_2$ $(\alpha^x)^y = \alpha^{xy}$ za vsak $x, y \in G$ in vsak $\alpha \in \Omega$.

Preslikavi

$$G \times \Omega \to \Omega$$
$$(g, \alpha) \mapsto \alpha^g$$

v tem primeru pravimo delovanje grupe G na množici Ω.

Primer 2.13. Grupa G deluje sama nase s konjugiranjem: $g, h \in G$, $h^g = g^{-1}hg$.

Definicija 2.14. Za $\alpha \in \Omega$ je

$$G_\alpha = \{x \in G \mid \alpha^x = \alpha\}$$

stabilizator α v G.

Stabilizator je torej množica tistih elementov iz G, ki s svojim delovanjem ne spremenijo elementa $\alpha \in \Omega$, lahko tudi rečemo, da fiksirajo α.

Lema 2.15. *G_α je podgrupa v G.*

Dokaz. Očitno je G_α podmnožica v G. Naj bosta $g, h \in G_\alpha$.

$$\alpha^{gh^{-1}} = (\alpha^g)^{h^{-1}} = \alpha^{h^{-1}} = \alpha.$$

Slednja enakost sledi iz

$$\alpha = (\alpha^h)^{h^{-1}} = \alpha^{h-1}.$$

□

Lema 2.16. *$(G_\alpha)^g = G_{\alpha^g}$ za $g \in G$, $\alpha \in \Omega$.*

Dokaz. Naj bo $x \in G_{\alpha^g}$. Potem velja

$$(\alpha^g)^x = \alpha^g \Leftrightarrow \alpha^{gxg^{-1}} = \alpha \Leftrightarrow gxg^{-1} \in G_\alpha \Leftrightarrow x \in g^{-1}G_\alpha g,$$

kar pomeni $x \in (G_\alpha)^g$. □

Definicija 2.17. Pravimo, da G deluje *tranzitivno* na Ω, če za vsak $\alpha, \beta \in \Omega$ obstaja tak $x \in G$, da velja $\alpha^x = \beta$.

Izrek 2.18 (Frattinijev argument)**.** *Naj G vsebuje podgrupo edinko N in naj N deluje tranzitivno na Ω. Potem je $G = G_\alpha N$ za vsak $\alpha \in \Omega$ in G_α je komplement N, če je $N_\alpha = \{1\}$.*

Dokaz. Očitno velja $G_\alpha N \subseteq G$. Pokažimo še obratno vsebovanost. Vzemimo $\alpha \in \Omega$ in $y \in G$ (vemo, da je $\alpha^y \in \Omega$). Sedaj uporabimo tranzitivnost N na Ω. Obstaja tak $x \in N$, da je

$$\alpha^y = \alpha^x \Leftrightarrow \alpha^{yx^{-1}} = \alpha,$$

torej je $yx^{-1} \in G_\alpha$, kar pomeni $y \in G_\alpha x \subseteq G_\alpha N$. Dokazali smo še obratno vsebovanost in s tem dobili $G = G_\alpha N$.

Naj bo $N_\alpha = \{1\}$ in dokažimo še, da velja $G_\alpha \cap N = \{1\}$. To pa je očitno, saj je $G_\alpha \cap N = N_\alpha = \{1\}$. □

Sedaj imamo vse, kar smo potrebovali, da se lahko lotimo metode Wielandta.

Definicija 2.19. Naj bo K Abelova podgrupa v G in $\mathcal{S}$ množica vseh transverzal podgrupe K v grupi G. Za $R, S \in \mathcal{S}$ definiramo:

$$R|S := \prod_{\substack{(r,s)\in R\times S \\ Kr=Ks}} (rs^{-1}) \qquad (\in K)$$

$$(Kr = Ks \Leftrightarrow rs^{-1} \in K).$$

Iz zgornje definicije sledi šest trditev, ki jih bomo uporabili pri dokazu izreka.

(1) $$(R|S)^{-1} = (S|R).$$

Dokaz.

$$(R|S)^{-1} = \left(\prod_{\substack{(r,s)\in R\times S \\ Kr=Ks}} (rs^{-1}) \right)^{-1} \overset{K \text{ Abelova}}{=} \prod_{\substack{(r,s)\in R\times S \\ Kr=Ks}} (rs^{-1})^{-1} =$$

$$= \prod_{\substack{(r,s)\in R\times S \\ Kr=Ks}} (sr^{-1}) = (S|R).$$

□

(2) $$(R|S)(S|T) = (R|T).$$

Dokaz.

$$(R|S)(S|T) = \prod_{\substack{(r,s_1)\in R\times S \\ Kr=Ks_1}} (rs_1^{-1}) \prod_{\substack{(s_2,t)\in S\times T \\ Ks_2=Kt}} (s_2t^{-1}).$$

$Kr = Ks_1$ in $Ks_2 = Kt$ pomenita $rs_1^{-1},\ s_2t^{-1} \in K$, K je Abelova, torej vsi elementi med seboj komutirajo, zato dobimo:

$$(R|S)(S|T) = \prod_{\substack{(r,s_1)\in R\times S\\(s_2,t)\in S\times T\\Kr=Ks_1\\Ks_2=Kt}} (rs_1^{-1})(s_2t^{-1}) = \prod_{\substack{(r,t)\in R\times T\\Kr=Kt}} (rt^{-1}) = (R|T).$$

Na tem mestu se pojavi vprašanje, ali se s_1^{-1} in s_2 res lahko pokrajšata, oziroma ali pare lahko uredimo tako, da $s_1 = s_2$. Odgovor je pritrdilen, saj gremo v obeh produktih po prav vseh $s \in S$, ker pare $(r, s_1) \in R \times S$ in $(s_2, t) \in S \times T$ lahko vedno uredimo tako, da zadoščajo zahtevi (predstavnike istih odsekov damo skupaj) in da so v njih zastopani vsi predstavniki transverzale. Pogoja $Kr = Ks_1$ in $Ks_2 = Kt$ iz prvega produkta lahko prepišemo v pogoj $Kr = Kt$ v drugem produktu, saj smo pare, ki so zadoščali prvima dvema pogojema, preuredili tako, da je veljalo $s_1 = s_2 =: s$, in s tem dobili pogoja $Kr = Ks$ in $Ks = Kt$, to pa nam da pogoj $Kr = Kt$. □

Kot dodatek zdaj privzamemo, da je K podgrupa edinka v G. Potem je vsak $S \in \mathcal{S}$ tudi leva transverzala K in G deluje z levim množenjem na $\mathcal{S}$. Če vzamemo $x \in G$ in $S \in \mathcal{S}$, lahko S zapišemo kot $S = \{k_1, x_1k_2, \ldots, x_{n-1}k_n\}$, kjer je $G = \{1, x_1, \ldots, x_{n-1}\}$ in so k_i med seboj ne nujno različni elementi iz K. Potem je $xS = \{xk_1, xx_1k_2, \ldots, xx_{n-1}k_n\}$ tudi element $\mathcal{S}$, saj je preslikava $g \mapsto xg$, kjer sta $x, g \in G$ očitno avtomorfizem G.

Za $k \in K$ dobimo:

$$(kR)|S = k^{|G:K|}(R|S), \quad k \in K. \tag{3}$$

Dokaz.

$$(kR)|S = \prod_{\substack{(r,s)\in R\times S\\Kr=Ks}} (krs^{-1}).$$

Vprašanje je, kolikokrat lahko iz produkta izpostavimo k, oziroma, koliko parov (r, s) imamo. Parov je ravno toliko, kolikor je elementov v transverzali, teh je toliko, kot je odsekov, kar pa je ravno $|G : K|$. Torej $(kR)|S = k^{|G:K|}(R|S)$.

□

Vidimo tudi:

$$(xR)|(xS) = \prod_{\substack{(r,s)\in R\times S\\Kr=Ks}} (xr(xs)^{-1}) =$$

$$= \prod_{\substack{(r,s)\in R\times S\\Kr=Ks}} (xrs^{-1}x^{-1}) = x\left(\prod_{(r,s)\in R\times S} (rs^{-1})\right)x^{-1} = x(R|S)x^{-1}.$$

Pogoj v prvem produktu, ki se po definiciji glasi $Kxr = Kxs$, kjer je x fiksen element iz G, lahko zamenjamo s pogojem $Kr = Ks$. Ker je K edinka, lahko $Kxr = Kxs$ zapišemo kot $xKr = xKs$, iz česar sledi, da $Kr = Ks$.

To nam da:

$$R|S = 1 \Rightarrow (xR)|(xS) = 1. \tag{4}$$

Zdaj pa privzemimo še, da sta $|K|$ in $|G:K|$ tuji si števili. Potem je preslikava

$$\alpha : K \to K$$
$$k \mapsto k^{|G:K|}$$

avtomorfizem K. Ker je K končna Abelova podgrupa, torej direktni produkt cikličnih grup, je preslikava α endomorfizem K. Za vsak $k \in K$ vemo, da njegov red deli $|K|$. Ker sta si $|K|$ in $|G:K|$ tuji, je $k^{|G:K|} = 1$ samo za $k = 1$, torej je jedro preslikave trivialno, zato je α avtomorfizem K.

V tem primeru iz (3) sledita še dve trditvi:

$$(kR)|S = 1 \quad \text{za} \quad k := (R|S)^{-\alpha^{-1}} \tag{5}$$

(tj. $k^{|G:K|} = (R|S)^{-1}$)

$$R|S = 1 = (kR)|S \Rightarrow k = 1. \tag{6}$$

Trditve (1) - (6) so ključnega pomena pri dokazu izreka. Zdaj, ko jih imamo, se lahko lotimo dokaza.

2.3. **Dokaz Schur–Zassenhausovega izreka za Abelove edinke.** Spomnimo se: dokazali bomo, da pri predpostavki, da sta $|K|$ in $|G:K|$ tuji, Abelova podgrupa edinka K v G ima komplement in da so vsi komplementi med seboj konjugirani v G.

Dokaz. Zaradi (1) in (2) za relacijo $R \sim S \iff R|S = 1$ velja:

- $R|R = 1$ refleksivnost (sledi neposredno iz definicije),
- $R|S = 1 \Rightarrow S|R = (R|S)^{-1} = 1$ simetričnost,
- $R|S = 1$ in $S|T = 1 \Rightarrow R|T = (R|S)(S|T) = 1$ tranzitivnost.

Torej je to ekvivalenčna relacija na $\mathcal{S}$. Naj bo $\widetilde{R}$ ekvivalenčni razred, ki vsebuje R,

$$\widetilde{R} = \{T \in \mathcal{S},\ T|R = 1\}.$$

Radi bi, da

$$\widetilde{S}^x = \widetilde{x^{-1}S} = \{T,\ T|(x^{-1}S) = 1\}$$

definira delovanje G na $\mathcal{S}/\!\sim$. Lastnosti $\mathcal{O}_1$ in $\mathcal{O}_2$ sta očitni iz definicije, veljati mora še:

$$R \sim S \Rightarrow (x^{-1}R) \sim (x^{-1}S),$$

oziroma

$$R|S = 1 \Rightarrow (x^{-1}R)|(x^{-1}S) = 1,$$

to pa sledi neposredno iz (4).

Vzemimo sedaj $R,\ S \in \mathcal{S}$ in k kot v (5). Oglejmo si

$$\widetilde{S}^k = \{T \in \mathcal{S},\ T|(k^{-1}S) = 1\}.$$

Ker velja

$$T|(k^{-1}S) \overset{K \text{ Abelova}}{=} (kT)|S \overset{(3)}{=} k^{|G:K|}(T|S) \overset{(5)}{=} (R|S)^{-1}(T|S) \overset{(1)}{=}$$
$$\overset{(1)}{=} (S|R)(T|S) \overset{K \text{ Abelova}}{=} (T|S)(S|R) \overset{(2)}{=} (T|R),$$

velja torej

$$\widetilde{S}^k = \widetilde{R},$$

kar pomeni, da K deluje tranzitivno na $\mathcal{S}/\!\sim$.

Stabilizator $\widetilde{R}$ v K, $K_{\widetilde{R}} = \{k \in K,\ \widetilde{R}^k = \widetilde{R}\}$, je zaradi (6) trivialen. V stabilizatorju so namreč taki k, za katere velja

$$T|R = 1 = T|(k^{-1}R) \overset{K \text{ Abelova}}{=} (kT)|R \overset{(6)}{\Longrightarrow} k = 1.$$

Zdaj nam Frattinijev argument 2.18 pove, da je stabilizator $G_{\widetilde{R}} = \{x \in G,\ \widetilde{R}^x = \widetilde{R}\}$ komplement K v G. Za elemente iz stabilizatorja velja

$$T|R = 1 = T|(x^{-1}R),$$

torej je tudi $R|T = 1$, od koder sledi

$$R|(x^{-1}R) = 1 \Longleftrightarrow x(R|(x^{-1}R))x^{-1} = 1 \Longleftrightarrow (xR)|(xx^{-1}R) = (xR)|R = 1,$$

zato je komplement oblike

$$G_{\widetilde{R}} = \{x \in G,\ (xR)|R = 1\}.$$

Zdaj pa bi radi videli, da v primeru, ko je X komplement, velja $X = G_{\widetilde{R}}$ za neki R. Če je X komplement, potem velja $xX = X$ za $x \in X$. To je res, saj je očitno $xX \subseteq X$. Prav tako pa velja tudi $X \subseteq xX$, saj vsak $a \in X$ lahko zapišemo kot $a = xx^{-1}a = x(x^{-1}a) \in xX$. Zato za vsak $x \in X$ velja $(xX)|X = 1$, torej $x \in G_{\widetilde{X}}$, oziroma

$$X \subseteq G_{\widetilde{X}}.$$

Vzemimo sedaj $a \in G_{\widetilde{X}}$. Potem velja $(aX)|X = 1$. Recimo, da velja $a \notin X$. Ker je $G = KX$ in $K \cap X = \{1\}$, je $a = kx$ za $k \in K$ in $x \in X$. Zato je $aX = kX$ in $(kX)|X = 1$, to pa je mogoče samo, če je $k = 1$, potem pa je $a = x$ in pridemo v protislovje. Dobili smo

$$G_{\widetilde{X}} \subseteq X.$$

Torej je $X = G_{\widetilde{X}}$ oziroma $X = G_{\widetilde{R}}$ za $X = R$. Zaradi tranzitivnosti delovanja in leme 2.16 velja:

$$(G_{\widetilde{R}})^k = G_{\widetilde{R}^k} = G_{\widetilde{S}},$$

za $k \in K$ in $\widetilde{R}, \widetilde{S} \in \mathcal{S}/\!\sim$, torej so vsi komplementi med seboj konjugirani.

□

3. Gaschützov izrek

V tem razdelku si bomo ogledali Gaschützov izrek, ki je posplošitev Schur–Zassenhausovega izreka za Abelove edinke.

Imejmo sedaj

$$K \leq U \leq G \quad \text{in} \quad K \lhd G.$$

Če je H komplement K v G, potem je $H \cap U$ komplement K v U. To sledi iz Dedekindove identitete, ki je ne bomo dokazovali (dokaz lahko najdete v [2]), pravi pa:

Trditev 3.1 (Dedekindova identiteta)**.** *Naj bo $G = UV$, kjer sta U in V podgrupi grupe G. Potem vsaka podgrupa H, ki zadošča $U \leq H \leq G$, porodi faktorizacijo $H = U(V \cap H)$.*

Nasprotna implikacija pa je obravnavana v Gaschützovem izreku. Za $K = U$ ta izrek ravno sovpada s Schur–Zassenhausovim izrekom, ki smo ga ravno dokazali.

Izrek 3.2 (Gaschützov izrek)**.** *Naj bosta K Abelova podgrupa edinka grupe G in U podgrupa G taki, da velja*

$$K \leq U \quad in \quad (|K|, |G : U|) = 1.$$

(a) *Recimo, da ima K komplement v U. Potem ima K komplement tudi v G.*
(b) *Recimo, da sta H_0 in H_1 dva taka komplementa K v G, da velja*

$$H_0 \cap U = H_1 \cap U.$$

Potem sta H_0 in H_1 konjugirana v G.

Dokaz. Naj bo A komplement K v U, tj.

$$\text{(i)} \quad U = KA \quad \text{in} \quad K \cap A = \{1\}.$$

Naj bo $\mathcal{L}$ množica levih transverzal podgrupe U v grupi G (ker U ni edinka v G, leve transverzale niso enake desnim). Naj bo S_0 neka izbrana transverzala iz $\mathcal{L}$. Vemo, da je G disjunktna unija odsekov, vsaka transverzala pa vsebuje po enega predstavnika iz vsakega odseka. Naj bo $S_0 = \{s_1, s_2, \ldots, s_n\}$. Potem so $s_1U, s_2U, \ldots, s_nU$ vsi levi odseki, ki so različni in pokrijejo cel G. Torej za vsak $x \in G$ obstaja $s_i \in S_0$, da velja $x \in s_iU$, torej $x = s_iu$, $u \in U$. Potem lahko za vsako levo transverzalo $L \in \mathcal{L}$ in $l \in L$ pišemo:

$$l = xu \text{ za } x \in G, u \in U,$$

$$xu = (s_l u_l)u, \text{ kjer je } s_l \in S_0 \text{ in } u_l \in U,$$

$$(s_l u_l)u = s_l(u_l u) = s_l u' = s_l k_l a_l,$$

kjer je $u' \in U = KA$, zato je $u' = k_l a_l$ za $k_l \in K$ in $a_l \in A$. Dobimo torej

$$\text{(ii)} \quad l = s_l k_l a_l, \text{ za } s_l \in S_0, \ k_l \in K, \ a_l \in A \text{ in } s_l U = lU.$$

Še več, zaradi (i) je po trditvi 2.4 zapis l v (ii) enoličen . V posebnem, za vsak $l \in L$ obstaja natanko en tak $l_0 \in S_0K$, da je $lU = l_0U$,

$$l_0 := s_l k_l,$$

torej $l \in L$ lahko zapišemo $l = l_0 a_l$. Iz tega sledi, da je vsak $L \in \mathcal{L}$ povezan s takim elementom $L_0 := \{l_0 \mid l \in L\}$, ki je prav tako leva transverzala in leži znotraj

$$\mathcal{S} := \{L \in \mathcal{L} \mid L \subseteq S_0K\},$$

da velja $LA = L_0A$. Res, saj za $la \in LA$ velja $la = s_l k_l a_l a = l_0(a_l a) \in L_0A$. Za $l_0a \in L_0A$ pa velja $l_0a = s_l k_l (a_l {a_l}^{-1})a = s_l k_l a_l ({a_l}^{-1} a) \in LA$. Enoličnost zapisa v (ii) nam da:

$$\text{(iii)} \quad L_0 \text{ je edini element iz } \mathcal{S}, \text{ za katerega velja } LA = L_0A.$$

Za $x \in G$ in levo transverzalo $xL \in \mathcal{L}$ dobimo

$$(xL)_0 A = xLA = xL_0A = (xL_0)_0 A,$$

in zato po (iii)

$$\text{(iv)} \quad (xL)_0 = (xL_0)_0 \text{ za vsak } L \in \mathcal{L}.$$

Zdaj pa definiramo

$$\text{(v)} \quad S^x := (x^{-1}S)_0 \text{ za } S \in \mathcal{S} \text{ in } x \in G.$$

Ker velja

$$(S^x)^y = (y^{-1}(x^{-1}S)_0)_0 \overset{\text{(iv)}}{=} (y^{-1}(x^{-1}S))_0 = ((xy)^{-1}S)_0 = S^{xy},$$

(v) definira delovanje G na $\mathcal{S}$. V nadaljevanju bomo pisali $(xS)_0$ namesto $S^{x^{-1}}$, ker želimo uporabiti zapis

$$R|S := \prod_{\substack{(r,s)\in R\times S\\ Kr=Ks}} (rs^{-1}) \qquad (R,S\in\mathcal{S}),$$

ki je sedaj malo drugačen kot tisti, ki je bil predstavljen v podrazdelku 2.2 o metodi Wielandta. Zaradi tega moramo preveriti, če trditve (1)-(6) še vedno držijo. (1) in (2) sledita kot prej. Za $k^{-1}\in K$ in $S\in\mathcal{S}$ velja

$$kS \subseteq kS_0K \overset{K\text{edinka}}{=} S_0K,$$

saj je za $S_0 = \{s_1,\dots,s_n\}$

$$kS_0K = \{ks_1,\dots,ks_n\}K = \{s_1k_1,\dots,s_nk_n\}K = S_0K,$$

kjer so $k_i\in K$ za $i=1,\dots,n$ in zato po (iii) sledi $kS = (kS)_0\in\mathcal{S}$. Zato kot prej v razdelku 2.2 sledi (3):

$$(kS)_0|R = k^{|G:U|}(S|R) \text{ za } k\in K \text{ in } S,R\in\mathcal{S}.$$

Za dokaz (4) naj bo $x\in G$ in $(r,s)\in R\times S$ tako, da je $Kr=Ks$ (potem velja tudi $rK=sK$, saj je K edinka) in $R,S\in\mathcal{S}$. Sedaj uporabimo zapis iz (ii) in dobimo

$$xr = s_{xr}k_{xr}a_{xr} \quad \text{in} \quad xs = s_{xs}k_{xs}a_{xs},$$

potem pa iz

$$xrK = xsK$$

sledi (in ker je K edinka)

$$s_{xr}Ka_{xr} = s_{xs}Ka_{xs}.$$

Iz tega sledi $s_{xr}=s_{xs}$ in prav tako $a_{xr}=a_{xs}$, ker je $K\cap A=\{1\}$. Dobimo

$$(xr)_0(xs)_0^{-1} = xra_{xr}^{-1}(xsa_{xs}^{-1})^{-1} = xrs^{-1}x^{-1}$$

in zato

$$(xR)_0|(xS)_0 = \prod_{\substack{(r,s)\in R\times S\\ Kr=Ks}} ((xr)_0(xs)_0^{-1}) = x(R|S)x^{-1} \text{ za vse } x\in G \text{ in } R,S\in\mathcal{S}.$$

Sedaj pa trditve (4)-(6) sledijo kot prej v podrazdelku 2.2. Kot v dokazu Schur–Zassenhausovega izreka za Abelove edinke

$$R\sim S \iff R|S = 1$$

definira ekvivalenčno relacijo na $\mathcal{S}$ in obstoj komplementa sledi kot prej, z uporabo delovanja G in K na $\mathcal{S}/\!\sim$.

Naj bosta H_0,H_1 kot v (b). Potem je

$$A := U\cap H_0 = U\cap H_1$$

komplement K v U ter leva transverzala A v H_i (i=0,1) je tudi leva transverzala U v G. Naj bo S_0 neka izbrana leva transverzala A v H_0 in $\mathcal{S}$ naj bo definirana glede na S_0 kot prej. Potem za vsak $s\in S_0$ obstaja tak $k_s\in K$, da $sk_s\in H_1$ ($k_s=1$, če $s\in H_0\cap H_1$). Sedaj je

$$S_1 := \{sk_s \mid s\in S_0\}$$

leva transverzala A v H_1, kjer velja $S_1 \subseteq S_0K$, tj. $S_1 \in \mathcal{S}$.

Po (ii) imamo

$$(L_i)_0 = S_i$$

za vsako L_i, levo transverzalo U v G, ki je vsebovana v H_i. $(L_0)_0$ mora biti tak, da bo veljalo $(L_0)_0 \subseteq S_0K$, kjer vemo, da je $S_0 \subseteq H_0$. Ker je $G = KH_0$ in $L_0 \subseteq H_0$, velja $L_0 \not\subset K$, zato bo $(L_0)_0$ ravno S_0. Podobno vidimo za $(L_1)_0 = S_1$. Velja še

$$(xS_i)_0 = S_i \text{ za vse } x \in H_i,$$

iz podobnega razloga kot zgoraj.

Torej H_i fiksira ekvivalenčni razred $\mathcal{S}/\sim$, ki vsebuje S_i (i=0,1).

Zdaj pa kot prej v dokazu Schur–Zassenhausovega izreka iz tranzitivnosti delovanja G na $\mathcal{S}/\sim$ sledi, da sta H_0 in H_1 konjugirana v G.

□

4. Schur–Zassenhausov izrek

V tem razdelku bomo spoznali in dokazali splošni Schur–Zassenhausov izrek, ki govori o obstoju komplementov edink, ki niso Abelove. Pravzaprav se izrek glasi skoraj enako kot izrek iz 2. razdelka, le da je za konjugiranost komplementov treba še dodatno nekaj privzeti. V resnici se izkaže, da so komplementi v vsakem primeru konjugirani, ampak ta privzetek bistveno skrajša dokaz. Več o tem pa po dokazu.

Za začetek si oglejmo lep primer podgrupe edinke, ki ima komplement.

Primer 4.1. Imejmo grupo G in K njeno podgrupo edinko, za katero velja:

- G/K je p-grupa,
- $p \nmid |K|$,

pri čemer definiramo:

Definicija 4.2. *p-grupa* je grupa, katere red vsakega elementa je potenca števila p, kjer je p praštevilo. Če je G končna grupa, je to ekvivalentno temu, da je $|G| = p^n$ za neki $n \in \mathbb{N}$.

Torej je $|G/K| = p^n$, p je praštevilo in $n \in \mathbb{N}$. Ker velja

$$|G/K| = \frac{|G|}{|K|} = p^n \quad \text{in} \quad p \nmid |K|,$$

iz tega sledi

$$|G| = p^n m, \ |K| = m \quad \text{in} \quad p \nmid m.$$

Če za naše potrebe povzamemo izreke Sylowa, dobimo izrek, ki pravi:

Izrek 4.3. *Naj bo G končna grupa, za katero velja $|G| = p^n m$, kjer je p praštevilo in $p \nmid m$. Potem G vsebuje podgrupo reda p^n, ki ji pravimo* p-podgrupa Sylowa *grupe G. Še več, vse p-podgrupe Sylowa so med seboj konjugirane v G.*

Zdaj vemo, da naša grupa G vsebuje p-podgrupe Sylowa in da so te med seboj konjugirane. Ostane le še vprašanje, ali so ravno p-podgrupe Sylowa komplementi K. Obstaja

$$H \leq G, \ |H| = p^n \quad \text{in} \quad KH \leq G, \quad \text{saj je} \quad K \lhd G.$$

Velja tudi

$$K \cap H = \{1\},$$

saj velja, da red elementa deli moč grupe, moči teh dveh podgrup pa sta si tuji, zato lahko pišemo

$$|KH| = |K||H| = mp^n = |G|,$$

torej je

$$G = KH.$$

p-podgrupe Sylowa grupe G so torej res komplementi K in vse so med seboj konjugirane v G.

Poglejmo sedaj, kaj pravi izrek.

Izrek 4.4 (Schur–Zassenhaus)**.** *Imejmo grupo G in K njeno podgrupo edinko, za kateri velja:*

$$(|K|, |G/K|) = 1.$$

Potem ima K komplement v G. Če velja še, da je ena izmed K ali G/K rešljiva, potem so vsi komplementi konjugirani v G.

4.1. **Priprava na dokaz.** Preden se lotimo dokaza izreka, nas čaka še kar nekaj dela. Na začetku dokaza izreka bomo potrebovali dva znana izreka o homomorfizmih.

Izrek 4.5. *Če sta $N \subseteq H$ podgrupi edinki grupe G, potem velja:*

$$G/H \cong (G/N)/(H/N).$$

Izrek 4.6. *Če je $N \lhd G$ in $H \leq G$ potem je $N \cap H \lhd H$ in velja:*

$$H/N \cap H \cong HN/N.$$

V primeru 4.1 smo se srečali s p-podgrupami Sylowa. Na tem mestu ponovimo definicijo, pri dokazu izreka si bomo namreč pomagali s temi podgrupami.

Definicija 4.7. Podgrupa H grupe G se imenuje *p-podgrupa Sylowa* (kjer je p praštevilo), če velja:

$$|H| = p^n \quad in \quad p^{n+1} \nmid |G|.$$

Množico vseh p-podgrup Sylowa grupe G označimo s $\mathrm{Syl}_p G$.

Prav tako bomo potrebovali definicijo, ki pravi:

Definicija 4.8. Naj bo $\mathbb{P}$ množica vseh pozitivnih praštevil, za $n \in \mathbb{N}$ definiramo množico

$$\pi(n) := \{p \in \mathbb{P} \mid p \text{ deli } n\}.$$

Za končno grupo G definiramo množico $\pi(G)$ kot

$$\pi(G) := \pi(|G|).$$

Sedaj pa se vrnimo nazaj k delovanju in definirajmo nekaj pojmov ter si poglejmo nekaj trditev, ki jih bomo potrebovali v dokazu. Na tem mestu še enkrat ponovimo, kaj je stabilizator.

Definicija 4.9. Za $\alpha \in \Omega$ je $G_\alpha = \{x \in G \mid \alpha^x = \alpha\}$ *stabilizator* α v G.

Stabilizator je torej množica tistih elementov iz G, ki s svojim delovanjem ne spremenijo elementa $\alpha \in \Omega$, lahko tudi rečemo, da fiksirajo α.

Pravimo, da sta dva elementa $\alpha, \beta \in \Omega$ *ekvivalentna*, če obstaja $x \in G$, za katerega velja $\alpha^x = \beta$. Lastnosti $\mathcal{O}_1$ in $\mathcal{O}_2$ pokažeta, da ta pojem ekvivalence definira ekvivalenčno relacijo na Ω. Pripadajoči ekvivalenčni razredi (ki razbijejo Ω na disjunktne dele) se imenujejo *orbite* grupe G (ali *G-orbite*) na Ω. Za $\alpha \in \Omega$ je

$$\alpha^G := \{\alpha^x \mid x \in G\}$$

orbita, ki vsebuje α.

Trditev 4.10. *$|\alpha^G| = |G : G_\alpha|$ za $\alpha \in \Omega$. Sledi, da je dolžina $|\alpha^G|$ orbite α^G delitelj $|G|$.*

Dokaz. Za $y, x \in G$

$$\alpha^y = \alpha^x \iff \alpha^{yx^{-1}} = \alpha \iff yx^{-1} \in G_\alpha \iff G_\alpha yx^{-1} = G_\alpha \iff G_\alpha y = G_\alpha x.$$

Dva enaka elementa v orbiti α^G torej pomenita dva enaka odseka v G/G_α. Zato je različnih elementov v α^G ravno toliko, kot je različnih odsekov v G/G_α. □

Ker je Ω disjunktna unija orbit grupe G, dobimo:

Posledica 4.11. *Če število n deli $|G : G_\alpha|$ za vse $\alpha \in \Omega$, potem n deli tudi $|\Omega|$.*

Definicija 4.12. Za $U \subseteq G$ je

$$C_\Omega(U) := \{\alpha \in \Omega \mid U \subseteq G_\alpha\}$$

množica fiksnih točk množice U v Ω.

$\Omega \backslash C_\Omega(G)$ je unija vseh G-orbit dolžine > 1. Res, saj je

$$C_\Omega(G) = \{\alpha \in \Omega \mid G = G_\alpha\} = \{\alpha \in \Omega \mid \alpha^x = \alpha \text{ za vsak } x \in G\},$$

torej $C_\Omega(G)$ vsebuje ravno vse orbite dolžine 1.

Trditev 4.13. *Naj bo G p-grupa. Potem je*

$$|\Omega| \equiv |C_\Omega(G)| \pmod{p}.$$

Dokaz. Za $\alpha \in \Omega' := \Omega \backslash C_\Omega(G)$ velja, da je $G_\alpha \neq G$. Torej p deli $|G : G_\alpha|$ (Lagrangeev izrek) in ker G deluje tudi na Ω' (res, saj je $\Omega = \Omega' \cup C_\Omega(G)$ in zato za $\alpha \in \Omega'$ velja, da $\alpha \neq \alpha^x \notin C_\Omega(G)$, zato je $\alpha^x \in \Omega$) iz posledice 4.11 sledi

$$|\Omega'| \equiv 0 \pmod{p},$$

oziroma

$$|\Omega| \equiv |C_\Omega(G)| \pmod{p}.$$

□

Definicija 4.14. Naj bo Ω množica samih neprazniih podmnožic grupe G in $H \leq G$. Potem H deluje s konjugiranjem na Ω. Za $A \in \Omega$ je množica, ki sestoji iz podmnožic

$$A^x = x^{-1}Ax \quad (x \in H),$$

orbita H. Stabilizator

$$N_H(A) := \{x \in H \mid A^x = A\}$$

podmnožice A v H je *normalizator* A v H.

Trditev 4.15. *Naj bo P p-grupa in $N \neq \{1\}$ podgrupa edinka grupe P. Potem $Z(P) \cap N \neq \{1\}$. Torej tudi $Z(P) \neq \{1\}$.*

Dokaz. Naj bo P p-grupa, N njena podgrupa edinka in naj P deluje na $\Omega := N$ s konjugiranjem. Potem je

$$\begin{aligned} C_\Omega(P) &= \{n \in N \mid P \subseteq P_n\} = \\ &= \{n \in N \mid x^{-1}nx = n, \text{ za vse } x \in P\} = \\ &= \{n \in N \mid nx = xn, \text{ za vse } x \in P\} = \\ &= Z(P) \cap N. \end{aligned}$$

Ker je $\Omega = N$ p-grupa (če je $|P| = p^n$, je $|N| = p^m$ za $m \leq n$) iz trditve 4.13 dobimo

$$|C_\Omega(P)| \equiv |\Omega| \equiv 0 \pmod{p}.$$

Ker je očitno $1 \in C_\Omega(P)$, sledi, da je $|C_\Omega(P)| \geq p$, torej $Z(P) \cap N \neq \{1\}$. □

Za potrebe dokaza spoznajmo še karakteristične podgrupe.

Definicija 4.16. Podgrupi U grupe G pravimo *karakteristična podgrupa* grupe G (ali karakteristična v G), če zanjo velja:

$$U^\alpha = U \quad \text{za vsak } \alpha \in \operatorname{Aut} G.$$

V tem primeru pišemo U char G.

Očitno je, da so karakteristične podgrupe podgrupe edinke v G.

Trditev 4.17. *$Z(G)$ je karakteristična podgrupa grupe G.*

Dokaz. Za $x \in Z(G),\ g \in G,\ \alpha \in \operatorname{Aut} G$ velja

$$x^\alpha g^\alpha = (xg)^\alpha = g^\alpha x^\alpha$$

in ker je $G = \{g^\alpha \mid g \in G\}$, dobimo $x^\alpha \in Z(G)$. □

Izrek 4.18. *Naj bo N podgrupa edinka grupe G in A karakteristična podgrupa v N. Potem je A edinka v G.*

Dokaz. Naj bo $a \in G$ in φ_a notranji avtomorfizem G,

$$\varphi_a :\ G \to G, \qquad x \mapsto x^a\ (= a^{-1}xa).$$

Potem je predpis φ_a avtomorfizem N, saj je N edinka v G. Ker je A karakteristična v N, je invariantna na φ_a za vsak $a \in G$, torej je A edinka v G. □

Posledica 4.19. *Če je N edinka v G, je $Z(N)$ prav tako edinka v G.*

Prav tako bomo morali vedeti, kaj pomeni pojem minimalna podgrupa edinka.

Definicija 4.20. Naj bo G grupa. Podgrupa edinka $N \neq \{1\}$ grupe G je *minimalna podgrupa edinka* grupe G, če sta trivialna grupa in N edini podgrupi edinki grupe G, ki sta vsebovani v N.

Pri dokazu si bomo pomagali tudi z rešljivimi grupami.

Definicija 4.21. Grupa G je *rešljiva*, če ima tako zaporedje podgrup

$$\{1\} = G_0 \leq G_1 \leq \cdots \leq G_k = G,$$

da je $G_{i-1} \trianglelefteq G_i$ in G_i/G_{i-1} je Abelova za $i = 1, 2, \ldots, k$.

Posledica 4.22. *Podgrupe in homomorfne slike rešljive grupe so rešljive grupe.*

Dokaz izpustimo, saj sledi direktno iz definicije, najdete ga lahko na primer v [5].

Definicija 4.23. *Komutator* elementov $x, y \in G$ je element

$$[x, y] = x^{-1}y^{-1}xy.$$

Definicija 4.24.

$$G' = \langle [x, y] :\ x, y \in G \rangle,$$

je *komutatorska podgrupa* grupe G.

Izrek 4.25. *Vsaka rešljiva minimalna podgrupa edinka N grupe G je Abelova podgrupa v G.*

Dokaz. Ker je N rešljiva, obstaja zaporedje podgrup

$$\{1\} = N_0 \subsetneqq N_1 \subsetneqq \cdots \subsetneqq N_k = N,$$

da je $N_{i-1} \lhd N_i$ in N_i/N_{i-1} Abelova za $i = 1, \ldots, k$.

Dokaza se lotimo s protislovjem. Recimo, da N ni Abelova.

- $k = 0 \Longrightarrow N = N_0 = \{1\}$,
- $k = 1 \Longrightarrow \{1\} = N_0 \leq N_1 = N \Longrightarrow N$ Abelova.

Torej je $k > 1$.

Naj bo

$$N' = \langle [x, y] : \ x, y \in N \rangle,$$

komutatorska podgrupa grupe N. Vzemimo $[x, y]$ generator N', $x, y \in N$ in $g \in G$. Potem velja

$$[x, y]^g = g^{-1}(x^{-1}y^{-1}xy)g$$

in

$$[x^g, y^g] = (g^{-1}xg)^{-1}(g^{-1}yg)^{-1}(g^{-1}xg)(g^{-1}yg) = (g^{-1}x^{-1}g)(g^{-1}y^{-1}g)(g^{-1}x)(yg) =$$
$$= g^{-1}(x^{-1}y^{-1}xy)g = [x, y]^g,$$

torej velja

$$[x, y]^g = [x^g, y^g] \in N', \text{ saj } x^g, y^g \in N, \text{ ker je } N \text{ edinka.}$$

Iz tega sledi, da je $N' \lhd G$. Ker je $N' \leq N$ in je N minimalna edinka v G, sledi, da je $N' = \{1\}$ ali $N' = N$.

Če je $N' = \{1\}$, potem velja

$$[x, y] = 1 \text{ za vsak } x, y \in N,$$

kar pomeni

$$x^{-1}y^{-1}xy = 1 \iff xy = yx \text{ za vsak } x, y \in N,$$

torej je N Abelova, kar je v nasprotju z našo predpostavko.

Torej je $N' = N$. Ker je N rešljiva in je $k > 1$, obstaja

$$\{1\} \neq N_{k-1} \subsetneqq N_k = N, \text{ kjer je } N/N_{k-1} \text{ Abelova.}$$

Torej za vsak $x, y \in N$ velja

$$xN_{k-1}yN_{k-1} = yN_{k-1}xN_{k-1},$$
$$xyN_{k-1} = yxN_{k-1},$$
$$x^{-1}y^{-1}xyN_{k-1} = N_{k-1},$$
$$[x, y]N_{k-1} = N_{k-1} \Longrightarrow [x, y] \in N_{k-1}.$$

Dobili smo:

$$N' = N \leq N_{k-1} \subsetneqq N,$$

kar pa seveda ni mogoče, torej je N Abelova in izrek je dokazan. □

Izrek 4.26. *Če je grupa G rešljiva, potem ima tako zaporedje*

$$\{1\} = G_0 \leq G_1 \leq \cdots \leq G_s = G,$$

da je $G_{i-1} \trianglelefteq G_i$ in je G_i/G_{i-1} ciklična p-grupa za $i = 1, \ldots, s$.

V izreku sicer velja ekvivalenca, a je mi v dokazu našega glavnega izreka ne potrebujemo.

Dokaz. Ker je G rešljiva, vsebuje

$$\{1\} = G_0 \leq G_1 \leq \cdots \leq G_k = G,$$

da je $G_{i-1} \trianglelefteq G_i$ in G_i/G_{i-1} je Abelova za $i = 1, 2, \ldots, k$. Ker je G_i/G_{i-1} Abelova in končna, sledi, da je direktni produkt cikličnih p-grup. Torej jo lahko zapišemo kot

$$G_i/G_{i-1} = P_1 \times P_2 \times \cdots \times P_r = \langle x_1 G_{i-1}\rangle \times \langle x_2 G_{i-1}\rangle \times \cdots \times \langle x_r G_{i-1}\rangle,$$

kjer so $P_j = \langle x_j G_{i-1}\rangle$ ciklične p-grupe za $j = 1, \ldots, r$. Sedaj $G_{i-1} \leq G_i$ razširimo do vrste

$$G_{i-1} \leq \langle G_{i-1}, x_1\rangle \leq \langle G_{i-1}, x_1, x_2\rangle \leq \cdots \leq \langle G_{i-1}, x_1, \ldots, x_r\rangle = G_i$$

kjer so faktorji

$$\langle G_{i-1}, x_j\rangle/G_{i-1} = G_{i-1}\langle x_j\rangle/G_{i-1} \overset{4.6}{\cong} \langle x_j\rangle/G_{i-1} \cap \langle x_j\rangle$$

p-grupe (saj so homomorfne slike $\langle x_j\rangle$) in podobno tudi vsi ostali faktorji.

Očitno je, da še vedno velja $G_{i-1} \trianglelefteq G_i$ za $i = 1, \ldots, s$. □

4.2. **Dokaz Schur–Zassenhausovega izreka.** Prišli smo do mesta, kjer bomo končno dokazali glavni izrek tega diplomskega seminarja.

Dokazati želimo, da če imamo grupo G in K njeno podgrupo edinko, za kateri velja $(|K|, |G/K|) = 1$, potem ima K komplement v G. Če še dodatno velja, da je ena izmed K ali G/K rešljiva, potem so vsi komplementi med seboj konjugirani v G.

Dokaz. Naj bo $U \leq G$ in $N \trianglelefteq G$. Potem po izrekih 4.5 in 4.6 velja:

$$UK/K \cong U/U \cap K \quad \text{in} \quad (G/N)/(KN/N) \cong G/KN.$$

Torej je

$$U \cap K \text{ taka podgrupa edinka v } U,$$

da velja

$$(|U \cap K|, |U/U \cap K|) = 1.$$

Res, saj je $U \cap K$ podgrupa v K, $U/U \cap K \cong UK/K$ pa je podgrupa v G/K. $|K|$ in $|G/K|$ sta si tuji, zato sta si tudi $|U \cap K|$ in $|U/U \cap K|$. Prav tako je

$$KN/N \text{ podgrupa edinka v } G/N,$$

za katero velja

$$(|KN/N|, |G/KN|) = 1.$$

Res, saj je $(|K|, |G/K|) = 1$, in ker mora moč podgrupe deliti moč grupe, lahko $|G|$ in $|K|$ zapišemo kot:

$$|G| = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r} p_{r+1}^{n_{r+1}} \cdots p_s^{n_s} \quad \text{in} \quad |K| = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r},$$

kjer

$$p_i \in \mathbb{P} \text{ in } n_i \in \mathbb{N} \text{ za } i = 1, \ldots, s \text{ ter } p_i \neq p_j \text{ za } i \neq j.$$

Zapišimo sedaj $|N|$ kot $|N| = p_k^{m_k} \cdots p_{k'}^{m_{k'}} p_l^{m_l} \cdots p_{l'}^{m_{l'}}$ kjer $m_i \leq n_i$, $\{k, \ldots, k'\} \subseteq \{1, \ldots, r\}$ in $\{l, \ldots, l'\} \subseteq \{r+1, \ldots, s\}$. Dobimo:

$$|KN| = \frac{|K||N|}{|K \cap N|} = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r} p_l^{m_l} \cdots p_{l'}^{m_{l'}},$$

zato

$$|KN/N| = \frac{|KN|}{|N|} = \frac{p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}}{p_k^{m_k} \cdots p_{k'}^{m_{k'}}}$$

in

$$|G/KN| = \frac{|G|}{|KN|} = \frac{p_{r+1}^{n_{r+1}} \cdots p_s^{n_s}}{p_l^{m_l} \cdots p_{l'}^{m_{l'}}}.$$

Zaradi izbire oznak in paroma različnih praštevil v tem primeru prav tako sledi, da je $(|KN/N|, |G/KN|) = 1$.

Iz tega sledi, da hipotezo iz izreka podedujejo podgrupe in faktorske grupe grupe G. Prav tako, če je ena izmed K ali G/K rešljiva, se po posledici 4.22 tudi ta lastnost podeduje.

Sedaj se bomo s pomočjo indukcije na $|G|$ lotili obstoja komplementa. Za $|G| = 1$ izrek očitno velja. Predpostavimo sedaj, da v vsaki grupi, katere moč je manjša od $|G|$, tak komplement obstaja. Izrek očitno velja za $K = \{1\}$, saj je v tem primeru komplement kar grupa G. Torej lahko predpostavimo, da je $\{1\} \neq K < G$.

Naj bo $p \in \pi(K),\ P \in \mathrm{Syl}_p K$, kjer je p praštevilo, in

$$U := N_G(P).$$

Najprej predpostavimo, da $U \neq G$. Potem po indukciji sledi, da ima $U \cap K$ komplement H v U. Ker je K podgrupa edinka v G, $\Omega = \mathrm{Syl}_p K$, $P \in \Omega$, $G_\alpha = G_P = N_G(P) = U$ in K deluje tranzitivno na Ω s konjugiranjem (po izreku 4.3 vemo, da so si vse p-podgrupe Sylowa grupe K konjugirane v K), zato iz Frattinijevega argumenta sledi

$$G = KU = K(U \cap K)H = KH.$$

Ker je $H \leq U$, velja tudi

$$H \cap K = H \cap (U \cap K) = \{1\},$$

zato je H prav tako komplement K v G.

Privzemimo sedaj, da je $U = G$. Potem je P podgrupa edinka v G (sledi direktno iz definicije $G = N_G(P) = \{x \mid x^{-1}Px = P\}$) in po posledici 4.19 je $N := Z(P)$ edinka v G. Velja tudi:

$$N = Z(P) \overset{4.15}{\neq} \{1\}.$$

Naj bo $\widehat{G} := G/N$. Po indukciji obstaja tak $N \leq V \leq G$, da je $\widehat{V} = V/N$ (podgrupe faktorske grupe G/N so oblike V/N, kjer je $N \leq V \leq G$) komplement $\widehat{K} = KN/N$ v $\widehat{G}$. Ker je $KN/N \cap V/N = \{N\}$, velja, da je $kN \neq vN$ za $k, v \notin N$, torej je $k \neq v$ za $k \in K, v \in V, \quad k, v \notin N$, kar pomeni

$$K \cap V = N.$$

Ker je $(KN/N)(V/N) = (G/N)$, za $k \in K$, $n \in N$, $v \in V$ in $g \in G$ velja $(knN)(vN) = (kN)(vN) \overset{N \lhd G}{=} kvN = gN$. Torej $g = kv$ ali $g, kv \in N$, kar nam da

$$G = KV.$$

Če je $V \neq G$, po indukciji obstaja komplement N v V,

$$V = NX, \quad N \cap X = \{1\},$$

zato velja

$$G = KNX \overset{N \leq K}{=} KX.$$

Ker velja še $K \cap NX = N$ in ker je $N \cap X = \{1\}$, dobimo

$$K \cap X = \{1\}.$$

Če je $V = G$, potem je

$$G/N = (KN/N)(G/N), \quad \text{zato je} \quad \widehat{K} = KN/N = N,$$

torej je $K \leq N$ in ker velja $N = Z(P) \leq P \leq K$, je K Abelova in po Schur–Zassenhausovem izreku za Abelove edinke 2.10 iz prvega razdelka ima komplement. Dokazali smo obstoj komplementa.

Dokazati moramo še, da če je ena izmed K ali G/K rešljiva, tedaj so vsi komplementi med seboj konjugirani. Tudi tega se bomo lotili s pomočjo indukcije na $|G|$.

Naj bosta H in H_1 dva komplementa K v G in naj bo N minimalna podgrupa edinka v G, ki je vsebovana v K. Označimo $\widehat{G} := G/N$. Potem sta $\widehat{H} = HN/N$ in $\widehat{H_1} = H_1N/N$ komplementa $\widehat{K}$ v $\widehat{G}$ in po indukciji obstaja tak $gN \in G/N$, da je

$$HN/N = (H_1N/N)^{gN}.$$

Iz tega pa sledi, da za vsak $hnN = hN \in HN/N$ obstaja tak $h_1 \in H_1$, da velja

$$hN = (h_1N)^{gN} = (gN)^{-1}h_1N(gN) = g^{-1}h_1gN = {h_1}^gN.$$

Želeli bi, da velja

$$HN = (H_1N)^g = {H_1}^gN.$$

Pokazali bomo obe vsebovanosti.

Vzemimo $hn \in HN,\ h \in H,\ n \in N$. Ker velja $hN = {h_1}^gN$, obstajata taka $n, n_1 \in N$, da velja

$$hn = {h_1}^g n_1 = (h_1 {n_1}^{g^{-1}})^g \in (H_1N)^g.$$

Sedaj vzemimo $h_1n \in H_1N,\ h_1 \in H_1,\ n \in N$.

$$(h_1n)^g = {h_1}^g n_1, \text{ kjer je } n_1 \in N.$$

Ker je $hN = {h_1}^gN$, obstaja $n_2 \in N$, da je ${h_1}^g n_1 = hn_2$, torej imamo še drugo vsebovanost, zato res velja

$$HN = (H_1N)^g = {H_1}^gN.$$

Torej sta H in ${H_1}^g$ komplementa N v NH.

Če $N \neq K$, potem $HN \neq G$ in po indukciji sta komplementa H in ${H_1}^g$ konjugirana v HN, torej obstaja $hn \in HN$, da velja $H^{hn} = {H_1}^g$. Ker velja

$$H^{hn} = H^n = {H_1}^g,$$

$$n^{-1}Hn = g^{-1}H_1g,$$

$$H = ng^{-1}H_1gn^{-1} = (gn^{-1})^{-1}H_1(gn^{-1}) = g'^{-1}H_1g',$$

končno dobimo

$$H = {H_1}^{g'}, \quad \text{za} \quad g' \in G,$$

torej sta H in H_1 konjugirana v G.

Privzemimo sedaj, da je $N = K$. Če je K rešljiva, je N rešljiva minimalna podgrupa edinka in zato po izreku 4.25 Abelova. Potem željeno sledi iz izreka 2.10.

Recimo sedaj, da K ni rešljiva, torej je rešljiva $\widehat{G} = G/K$. Potem obstaja podgrupa edinka $\widehat{A}$ v $\widehat{G}$, torej za $a_1, a_2 \in A$ in vsak $g \in G$ velja

$$(a_1K)^{gK} = a_2K$$

in ker velja

$$(a_1K)^{gK} = (gK)^{-1}(a_1K)(gK) \overset{K \lhd G}{=} g^{-1}a_1gK = {a_1}^gK,$$

dobimo

$$a_1{}^g K = a_2 K \text{ za } a_1, a_2 \in A \text{ in vsak } g \in G,$$

kar pomeni $a_1{}^g, a_2 \in K$ ali $a_1{}^g = a_2$, torej $A \trianglelefteq G$.

Zato velja $K \leq A \trianglelefteq G$ in po izreku 4.26 velja še, da smo $\widehat{A}$ lahko izbrali tako, da je $\widehat{G}/\widehat{A}$ netrivialna p-grupa. Ker po izreku 4.5 velja

$$\widehat{G}/\widehat{A} = (G/K)/(A/K) \cong G/A,$$

je tudi G/A p-grupa.

Iz Dedekindove identitete 3.1 sledi, da sta $H \cap A$ in $H_1 \cap A$ komplementa K v A in po indukciji konjugirana v A. Zato lahko privzamemo, da velja (po primernem konjugiranju)

$$H \cap A = H_1 \cap A := D \trianglelefteq \langle H, H_1 \rangle.$$

Ker je $H/D = H/(H \cap A)$ in je po izreku 4.6 $H/(H \cap A) \cong HA/A$ in ker velja $HK = G$, $K \leq A$, dobimo

$$H/D \cong G/A \cong H_1/D.$$

Ker so to p-grupe, obstajata (po izreku Sylowa) taka $P \in \mathrm{Syl}_p H$ in $P_1 \in \mathrm{Syl}_p H_1$, da velja

$$H = DP \quad \text{in} \quad H_1 = DP_1.$$

Ker velja $(|K|, |H|) = 1$, sta P in P_1 p-podgrupi Sylowa grupe

$$N_G(D) = \{g \in G \mid D^g = D\}.$$

Res, saj je $D \trianglelefteq H$, zato je očitno $H \leq N_G(D)$. Velja torej

$$P \leq H \leq N_G(D) \leq G = HK.$$

Če zapišemo

$$|H| = p_1^{\alpha_1} p_1^{\alpha_2} \cdots p_k^{\alpha_k}, \quad \text{kjer} \quad p_1 = p,$$
$$|K| = q_1^{\beta_1} q_1^{\beta_2} \cdots q_l^{\beta_l}, \quad q_i \neq p_j,$$

potem lahko $|G|$ zapišemo kot

$$|G| = \frac{|H||K|}{|H \cap K|} = p^{\alpha_1} b, \quad \text{kjer} \quad p \nmid b$$

in P je res p-podgrupa Sylowa $N_G(D)$. Povsem ekvivalentno to pokažemo za P_1. Sedaj pa po izreku Sylowa 4.3 obstaja tak $g \in N_G(D)$, da je $P_1{}^g = P$ in zato je

$$H_1{}^g = D^g P_1{}^g = DP = H,$$

torej sta H in H_1 konjugirana v G.

□

Morda se zdi, da zaradi zahteve, da mora biti za konjugiranost komplementov ena od grup K ali G/K rešljiva, Schur–Zassenhausov izrek izgubi na splošnosti. Vendar v resnici temu ni tako. To namreč vedno velja, saj obstaja zelo znan izrek, Feit-Thompsonov izrek, ki pravi, da je vsaka grupa lihega reda rešljiva. Mi v izreku zahtevamo da sta si moči $|G|$ in $|G/K|$ tuji, zato mora biti ena izmed njiju liha, torej je vedno ena izmed teh dveh grup rešljiva. Najbrž se potem pojavi vprašanje, zakaj smo sploh zahtevali rešljivost. To smo morali narediti zaradi dokaza izreka, saj smo si ga s to zahtevo mnogo skrajšali. Dokaz Feit-Thompsonovega izreka namreč obsega približno 300 strani. Zanj sta Walter Feit in John G. Thompson leta 1965 prejela Coleovo nagrado za izjemen prispevek k algebri.

Literatura

[1] K. Conrad, *The Schur-Zassenhaus theorem*, verzija 21.5.2008, [ogled 24. 8. 2012], dostopno na `www.math.uconn.edu/~kconrad/blurbs/grouptheory/schurzass.pdf`.

[2] H. Kurzweil in B. Stellmacher, *The theory of finite groups : an introduction*, Universitext, Springer, New York, 2004.

[3] D. J. S. Robinson, *A course in the theory of groups*, Graduate texts in mathematics **80**, 2nd ed., Springer, New York, 1996.

[4] J. J. Rotman, *An introduction to the theory of groups*, Graduate texts in mathematics **148**, 4th ed., Springer, New York, 1995.

[5] I. Vidav, *Algebra*, Matematika – fizika **4**, DMFA Slovenije, Ljubljana, 1987.

[6] *Classification of finite simple groups*, [ogled 26. 8. 2012], dostopno na `http://en.wikipedia.org/wiki/Classification_of_finite_simple_groups`.

[7] *Composition series*, [ogled 26. 8. 2012], dostopno na `http://en.wikipedia.org/wiki/Composition_series`.