4 Struktura primitivne grupe

4.1 Minimalne edinke in podstavek grupe

Netrivialni edinki N grupe G, ki ne vsebuje nobene druge netrivialne edinke grupe G, rečemo *minimalna edinka*. V tem primeru pišemo $N \lhd_m G$. Grupo, generirano z vsemi minimalnimi edinkami grupe G, označimo s $\mathrm{soc}(G)$, in ji rečemo *podstavek grupe* G (angl. *socle*).

Dokažimo najprej preprosto, vendar velikokrat uporabljeno trditev.

LEMMA 4.1 *Naj bo N minimalna edinka in H poljubna edinka grupe G. Tedaj je bodisi $H \cap N = 1$, in zato $\langle N, H\rangle = N \times H$, bodisi $N \leq H$.*

PROOF. Ker je presek $H \cap N \leq N$ edinka grupe G, N pa minimalna edinka, je bodisi $H \cap N = 1$ bodisi $H \cap N = N$. V prvem primeru je $\langle N, H\rangle = N \times H$, v drugem pa $N \leq H$. ∎

Od tod hitro sledi naslednje zanimivo dejstvo.

PROPOSITION 4.2 *Če je K minimalna edinka grupe G in $C = C_G(K)$ njen centralizator v grupi G, tedaj je* $\mathrm{soc}(G) \leq \langle K, C\rangle$.

PROOF. Naj bo N poljubna minimalna edinka grupe G. Tedaj je po prejšnji lemi bodisi $N \leq K$ bodisi $N \cap K = 1$. V slednjem primeru N centralizira K, in je zato $N \leq C$. V obeh primerih je N vsebovana v grupi $\langle K, C\rangle$. Ker je bila N poljubna minimalna edinka, od tod sledi $\mathrm{soc}(G) \leq \langle K, C\rangle$. ∎

PROPOSITION 4.3 *Naj bo N minimalna edinka grupe G. Tedaj N premore takšne enostavne, v G med seboj konjugirane minimalne edinke $T_1, \ldots, T_k$, da je*

$$N = T_1 \times \ldots \times T_k.$$

Če N ne premore netrivialne abelove edinke, potem so $T_1, \ldots, T_k$ edine minimalne edinke grupe N.

PROOF. Izberimo poljubno minimalno edinko T grupe N in označimo s $\mathcal{T} = \{T^g : g \in G\}$ množico vseh njenih konjugirank v grupi G. Ni težko videti, da je vsak element množice $\mathcal{T}$ minimalna edinka grupe N, zato je grupa $S = \langle \mathcal{T} \rangle$ vsebovana v $\mathrm{soc}(N)$. Po drugi strani pa je edinka grupe G, zato iz minimalnosti N sledi, da je $S = \mathrm{soc}(N) = N$.

Naj bo $\mathcal{M}$ družina tistih podmnožic $\{T_1, \ldots, T_i\} \subseteq \mathcal{T}$, za katere velja $\langle T_1, \ldots, T_i \rangle = T_1 \times \ldots \times T_i$, in naj bo $\{T_1, \ldots, T_k\}$ kak izmed maksimalnih elementov (glede na vsebovanost) v družini $\mathcal{M}$.

Vzemimo poljuben element $T^g \in \mathcal{T}$. Ker je grupa $\langle T_1, \ldots, T_k \rangle$ edinka grupe N, po lemi 4.1 sledi, da je bodisi T^g vsebovan v $\langle T_1, \ldots, T_k \rangle$ bodisi je $\langle T_1, \ldots, T_k, T^g \rangle = T_1 \times \ldots \times T_k \times T^g$. Ker je slednje v protislovju z maksimalnostjo množice $\{T_1, \ldots, T_k\}$, sledi, da grupa $\langle T_1, \ldots, T_k \rangle$ vsebuje vse elemente množice $\mathcal{T}$, in zato tudi grupo $\langle \mathcal{T} \rangle = N$. Ker je obratna vsebovanost očitna, smo s tem dokazali formulo $N = T_1 \times \ldots \times T_k$. Med drugim to pomeni, da je vsaka edinka katerekoli od podgrup $T_i \leq N$ hkrati tudi edinka grupe N. Iz minimalnosti edink T_i tedaj sledi enostavnost grup T_i.

Zadnji stavek trditve bo sledil iz izreka 4.4, ki ga bomo dokazali v nadaljevanju. ∎

THEOREM 4.4 *Za poljubno grupo G obstajajo takšne minimalne edinke $K_1, \ldots, K_n$, da je*

$$\mathrm{soc}(G) = K_1 \times \ldots \times K_n.$$

Če grupa G ne premore netrivialne abelove edinke, tedaj so $K_1, \ldots, K_n$ edine minimalne edinke grupe G.

PROOF. Dokaz je na las podoben dokazu trditve 4.3. Naj bo $\{K_1, \ldots, K_n\}$ takšna množica minimalnih edink grupe G, da je $\langle K_1, \ldots, K_n \rangle = K_1 \times \ldots \times K_n$, vendar $\langle K_1, \ldots, K_n, K \rangle \neq K_1 \times \ldots \times K_n \times K$ za vsako drugo minimalno edinko K grupe G.

Vzemimo poljubni minimalno edinko grupe G. Ker je $K_1 \times \ldots \times K_n$ edinka grupe G, je, upoštevajoč maksimalnost družine $\{K_1, \ldots, K_n\}$ in lemo 4.1, grupa K vsebovana v produktu $K_1 \times \ldots \times K_n$. S tem smo dokazali, da je $\mathrm{soc}(G) \leq K_1 \times \ldots \times K_n$. Ker pa so K_i minimalne edinke grupe G, velja tudi obratna vsebovanost in s tem enakost $\mathrm{soc}(G) = K_1 \times \ldots \times K_n$.

Pa denimo, da grupa G premore še kako drugo minimalno edinko K, različno od edink $K_1, \ldots, K_n$. Tedaj po lemi 4.1 za vsako od grup K_i velja $\langle K_i, K \rangle = K \times K_i$. Od tod sledi, da grupa K centralizira podstavek $\mathrm{soc}(G)$, in ker je v njem vsebovan, je K vsebovana v centru $Z(G)$. Ker pa je center $Z(G)$ abelova edinka grupe G, od tod sledi, da grupa G ni polenostavna. ∎

REMARK. Grupam, ki ne premorejo netrivialnih abelovih edink, pravimo tudi *polenostavne grupe*. Po zgornjem izreku je podstavek polenostavne grupe enak direktnemu produktu *vseh* svojih minimalnih edink, le-te pa so enostavne neabelove grupe.

Obratno, denimo, da so vse grupe K_i neabelove in predpostavimo, da grupa G ni polenostavna. Tedaj G vsebuje kako abelovo minimalno edinko A. Kot minimalna edinka je A vsebovana v podstavku $\mathrm{soc}(G)$, zato lahko opazujemo njeno projekcijo A_i na posamezni faktor K_i direktnega produkta $\mathrm{soc}(G) = K_1 \times \ldots \times K_n$. Tedaj je A_i abelova edinka grupe K_i, ki pa je po trditvi 4.3 izomorfna potenci T^k neabelove enostavne grupe T. Če A_i nadalje projiciramo na posamezni faktor T v potenci T^k, dobimo abelovo edinko grupe T, ki je zaradi enostavnosti grupe T seveda trivialna. Od tod sledi, da je trivialna tudi grupa A_i. Ker to velja za vsak $i \in \{1, \ldots, n\}$, pa je trivialna tudi grupa A, kar je v protislovju z našimi predpostavkami. S tem smo dokazali, da podstavek grupe, ki ni polenostavna, ni enak direktnemu produktu neabelovih minimalnih edink.

Vidimo torej, da lahko pogoj o polenostavnosti grupe G iz zgornjega izreka nadomestimo s pogojem, da so vse grupe K_i v razcepu podstavka $\mathrm{soc}(G)$ neabelove.

4.2 Podstavek primitivne permutacijske grupe

V tem razdelku se bomo osredotočili na podstavek primitivne permutacijske grupe. Gradili bomo na izreku 4.4. Pričnimo z naslednjo preprosto, a zanimivo trditvijo.

Lemma 4.5 *Naj bosta $H, G \leq Sym(\Omega)$ takšni permutacijski grupi, da za poljubna $h \in H$ in $g \in G$ velja $hg = gh$. Če je grupa G tranzitivna, je H semiregularna. Če sta tranzitivni obe grupi G in H, sta obe regularni njuni delovanji pa sta simultano izomorfni desnemu in levemu regularnemu delovanju grupe G na sami sebi.*

Remark. Zadnji stavek leme formalno povemo takole: Obstajata bijekcija $\varphi\colon \Omega \to G$ in izomorfizem grup $f\colon \mathrm{Sym}(\Omega) \to \mathrm{Sym}(G)$, ki preslika grupo G v grupo $G_\rho = \{\rho_g : g \in G\}$ desnih množenj $\rho_g\colon x \mapsto xg$, grupo H pa v grupo $G_\lambda = \{\lambda_g : g \in G\}$ levih množenj $\lambda_g\colon x \to g^{-1}x$. Par $(f|_G, \varphi)$ je izomorfizem delovanj grup G na Ω in G_ρ na G, par $(f|_H, \varphi)$ pa izomorfizem delovanj grup H na Ω in G_λ na G.

Naj bo $G \leq \mathrm{Sym}(\Omega)$ primitivna permutacijska grupa, K njena minimalna edinka in $C = C_G(K)$ centralizator grupe K v G. Tedaj je C tudi edinka grupe G. Naj bo N še kaka minimalna edinka grupe G. Če $N \neq K$, tedaj N seka K trivialno, in zato N centralizira K. To pa pomeni $N \leq C$. Od tod sledi, da je $\mathrm{soc}(G) \leq \langle N, C\rangle$.

Če je $C \neq 1$, tedaj je C tranzitivna, in po prejšnji lemi sta tako K kot C regularni edinki grupe G, in sta zato izomorfni. Regularna edinka primitivne grupe je nujno minimalna edinka, zato je tudi C minimalna edinka grupe

K. Od tod sledi, da je je $\langle C, K\rangle \leq \mathrm{soc}(G)$, in zato $\mathrm{soc}(G) = \langle K, C\rangle$. Še več, ker je vsaka minimalna edinka G bodisi enaka K bodisi vsebovana v C, sta K in C edini minimalni edinki.

V primeru, da je $K = C$, tedaj je K abelova, in kot vemo je tedaj G permutacijsko izomorfna kaki podgrupi grupe $\mathrm{AGL}(d, \mathbb{Z}_p)$. V tem primeru je K edina minimalna edinka grupe G.

Če pa je $K \neq C$, tedaj je $\langle K, C\rangle = K \times C$, in zato $\mathrm{soc}(G) = K \times C$. Spomnimo se se, da je vsaka minimalna edinka produkt med seboj izomorfnih enostavnih grup, grupi K in C pa sta izomorfni. Zato je $\mathrm{soc}(G) \cong T_1 \times T_2 \times \ldots \times T_k$ za nek $k \geq 2$ in $T_i \cong T$ za neko neabelovo enostavno grupo T. Ker so T_i neabelove, so to vse enostavne edinke grup K in C, in jih zato grupa G s konjugacijo permutira med seboj (in to z dvema orbitama – ena orbita sestabljajoča K, druga pa C).

Ostane nam še primer, ko je $C = 1$. Tedaj se G zvesto vloži v $\mathrm{Aut}(K)$, grupa K je edina minimalna edinka v G, in zato $\mathrm{soc}(G) = K = \mathrm{soc}(G) \cong T_1 \times T_2 \times \ldots \times T_k$ za nek $k \geq 1$, kjer je $T_i \cong T$ za neko neabelovo enostavno grupo T. Podobno kot zgoraj, so T_i edine enostavne edinke grupe K, in zato jih G med seboj permutira (tokrat tranzitivno).

Tako smo dokazali naslednje:

THEOREM 4.6 *Naj bo $G \leq Sym(\Omega)$ primitivna permutacijska grupa, K njena minimalna edinka in $C = C_G(K)$ centralizator grupe K v G. Tedaj sta C in K edini minimalni edinki grupe G in velja ena od naslednjih trditev:*

(i) $C = K$, $\mathrm{soc}(G) = K \cong \mathbb{Z}_p^d$ *in G je permutacijsko izomorfna kaki podgrupi* $\mathrm{AGL}(d, \mathbb{Z}_p)$*;*

(ii) $C = 1$, $\mathrm{soc}(G) = K \cong T$ *za kako enostavno neabelovo grupo T in $G \cong \tilde{G}$, kjer $T \leq \tilde{G} \leq Aut(T)$;*

(iii) $\mathrm{soc}(G) =\cong T_1 \times T_2 \times \ldots \times T_k$ *za nek $k \geq 2$, kjer je $T_i \cong T$ za neko neabelovo enostavno grupo T. Pri tem so T_i edine enostavne edinke grupe* $\mathrm{soc}(G)$ *in grupa G s konjugacijo permutira množico $\{T_1, \ldots, T_k\}$.*