UNIVERZA V LJUBLJANI
PEDAGOŠKA FAKULTETA

DEJAN KREJIĆ

DELOVANJA GRUP IN BLOKI NEPRIMITIVNOSTI

DIPLOMSKO DELO

Ljubljana, 2015

UNIVERZA V LJUBLJANI
PEDAGOŠKA FAKULTETA

Dvopredmetni učitelj: matematika - računalništvo

DEJAN KREJIĆ
Mentor: doc. dr. PRIMOŽ ŠPARL

DELOVANJA GRUP IN BLOKI NEPRIMITIVNOSTI

DIPLOMSKO DELO

Ljubljana, 2015

Zahvaljujem se svojemu mentorju doc. dr. Primožu Šparlu za kvalitetno mentorstvo, razumevanje in za ves trud, ki ga je prispeval pri nastanku mojega diplomskega dela.

Rad bi se zahvalil tudi svoji družini in prijateljem, ki so me podpirali in spodbujali skozi celoten študij.

Povzetek

Diplomsko delo spada na področje teorije grup. V njem obravnavamo delovanja grup, največ pozornosti pa posvetimo raziskovanju blokov neprimitivnosti in njihovih lastnosti. Gre za pomemben koncept v teoriji permutacijskih grup, saj obstoj tako imenovanega sistema blokov neprimitivnosti za dano delovanje pogosto omogoča, da obravnavo danega delovanja zreduciramo na delovanje na precej manjši množici, s čimer postane bolj obvladljivo.

V diplomskem delu zberemo temeljna znanja, ki so potrebna za razumevanje osrednje teme. Spoznamo delovanja grup ter z njimi povezane lastnosti in rezultate, predstavimo pa tudi nekaj konkretnih primerov. Vpeljemo pojem bloka neprimitivnosti, raziščemo kriterij za njihov obstoj in jih predstavimo na nekaj zgledih. Bloke neprimitivnosti povežemo s pojmom neprimitivnega delovanja in podamo potrebne ter zadostne pogoje za opredelitev primitivnosti in neprimitivnosti delovanja. Ogledamo si konkretne primere primitivnih in neprimitivnih delovanj grup. Raziščemo povezavo med netranzitivnimi edinkami in bloki neprimitivnosti.

Ključne besede: blok neprimitivnosti, delovanje grupe, primitivnost, sistem blokov neprimitivnosti

Klasifikacija MSC(2010): 20B15, 20B25, 20B35

Abstract

This BSc thesis deals with certain topics from group theory. We investigate group actions and in particular devote most of our attention to the research of blocks of imprimitivity and their characteristics. This is a very important concept in the theory of permutation groups, since the existence of the so-called imprimitivity block system for a given action, often enables us to reduce the action to a much smaller set, which makes it more manageable.

In the thesis, we collect the basic notions and results that are necessary for the understanding of the central theme. We review some basic facts about group actions and their properties and present some examples. We introduce the concept of a block of imprimitivity, we explore the criterion for their existence and we give some examples of them. We link the concept of blocks of imprimitivity with the concept of an imprimitive action and present necessary and sufficient conditions for the action to be primitive or imprimitive. We present examples of primitive and imprimitive group actions and explore the connection between intransitive normal subgroups and blocks of imprimitivity.

Keywords: block of imprimitivity, group action, primitivity, system of blocks of imprimitivity

MSC(2010) classification: 20B15, 20B25, 20B35

Kazalo

Poglavje 1

Uvod

Diplomsko delo spada v teorijo grup, ki predstavlja pomembno področje abstraktne algebre. Ta veja matematike se v splošnem ukvarja s proučevanjem strukturnih lastnosti grup. Med prve pomembnejše raziskovalce tega področja uvrščamo Leonharda Eulerja, Josepha Louisa Lagrangea, Carla Friedricha Gaussa, Nielsa Henrika Abela in Evarista Galoisa, ki so delovali v 18. in v začetku 19. stoletja [4]. To časovno obdobje uradno še ni del sodobne teorije grup, kot jo poznamo danes. Ta se prične šele leta 1882 z Dyckovo abstraktno definicijo grupe, ki je terjalo številna vprašanja in razvoj tega področja [3]. Danes ima teorija grup v splošnem veliko uporabno vrednost, saj se uporablja pri različnih vejah matematike in v drugih znanostih. Grupe na primer imajo pomembno vlogo pri algebrski topologiji, kjer jih uporabljamo za opis invariant topoloških prostorov. Pri študiju diferencialnih enačb so zelo pomembne tako imenovane Liejeve grupe, ki povežejo analizo in teorijo grup [4]. Lahko se ozremo tudi na uporabo grup izven matematike. Tako se pri kemiji grupa uporablja za opisovanje simetrij molekul in razvrstitev kristalnih struktur. Omenimo še področje fizike, kjer je znano, da upodobitve Liejevih grup pripomorejo pri iskanju možnih fizikalnih teorij, prav tako pa so pomembne pri opisovanju simetrij, ki naj bi jih upoštevali fizikalni zakoni [4].

Teorija grup je torej očitno zelo uporabna tudi na področju proučevanja simetrij. V praksi se grupe pogosto uporabljajo za opisovanje simetrij obravnavanih objektov, kar bo razvidno v nadaljevanju diplomskega dela. Pri tem govorimo o tako imenovanih avtomorfizmih danega objekta, ki v grobem predstavljajo preoblikovanje objekta tako, da se njegova struktura ohranja. Skupek vseh teh avtomorfizmov, skupaj z operacijo kompozituma preslikav, tvori grupo avtomorfizmov [3]. Pravimo, da ta grupa deluje na množici, oziroma na dani objekt. Ta pojem predstavlja temelj diplomskega dela. S proučevanjem teh delovanj spoznavamo simetrijske lastnosti objekta, kar lahko nudi uporabne informacije o samem objektu. Kot primer se navežimo na področje teorije grafov, ki se v grobem ukvarja z grafi in njihovimi lastnostmi. Z algebraičnega vidika se pri grafih v večji meri ukvarjamo s proučevanjem simetrij grafov, ali drugače povedano, z avtomorfizmi grafov. Tukaj so simetrije izrednega pomena, saj je v primeru, da je graf vozliščno tranzitiven, kar med drugim pomeni, da so vsa vozlišča na nek način enaka med seboj, nekatere grafovske lastnosti dovolj preveriti le na enem vozlišču.

Seveda velja opomniti, da je vozliščna tranzitivnost posledica velike simetričnosti grafa, kar pa ugotovimo s proučevanjem delovanja grupe avtomorfizmov grafa. To je le en primer uporabnosti delovanj grup, obstaja pa jih seveda še mnogo več [2]. Potrebno se je zavedati, da raziskovanje delovanja grup ni vedno preprosto. Pri delovanjih grup na manjših množicah je proučevanje enostavno, saj gre za manjša in posledično bolj obvladljiva delovanja. V takšnih primerih strukture delovanja ni težko opazovati. Pogosto pa se srečujemo z delovanji grup na velikih množicah, kjer hitro spoznamo, da je raziskovanje z običajnimi metodami precej zahtevno in neuspešno. Zato se je potem smiselno vprašati, ali obstaja bolj sistematičen način, ki bi omogočal enostavnješe raziskovanje. V tem diplomskem delu bomo v ta namen spoznali bloke neprimitivnosti, sisteme neprimitivnosti in primitivnost delovanj, ki predstavljajo ustrezno „orodje“ za enostavnejše in bolj sistematično preučevanje delovanj. Ker razumevanje osrednje teme diplomskega dela zahteva določeno mero poznavanja osnovnih znanj iz teorij grup, bomo zato naslednje poglavje diplomskega dela namenili spoznavanju potrebnih osnov.

Poglavje 2

Osnovna znanja

2.1 Teorija grup

Preden se lotimo obravnave osrednje tematike diplomskega dela, je zaradi razumevanja obravnave potrebno spoznati temeljna znanja s področja grup. Pri tem bomo privzeli, da bralec že pozna pojme kot so *grupa*, *podgrupa*, *red grupe*, *red elementa*, *generatorji grupe*, *cikličnost grupe* ipd. Bralec lahko te pojme obnovi v [8]. Iz tega razloga se bomo v tem poglavju posvetili le nekaterim manj znanim pojmom in pomembnejšim rezutatom, ki jih bomo potrebovali v nadaljevanju. Celoten razdelek z vsemi svojimi podrazdelki je povzet po [6] in [8].

2.1.1 Definicije, trditve in izreki

V tem podrazdelku bomo spoznali nekatere za nas pomembne definicije, trditve in izreke, s katerimi bralec mogoče še ni seznanjen. Za začetek najprej sklenimo sledeč dogovor.

Dogovor. V nadaljevanju bomo grupo $(G, \bullet)$ in produkt $x \bullet y$ pisali brez operacije, torej samo z G in xy, v primeru morebitnih nejasnosti pa bomo pri zapisu upoštevali tudi operacijo v grupi.

Trditev 2.1. *Naj bosta $H,K \leq G$. Tedaj je presek $H \cap K$ tudi podgrupa v G.*

Definicija. Naj bo G grupa in H njena prava podgrupa (oznaka $H < G$). Podgrupi H pravimo *maksimalna* podgrupa, če ne obstaja $K < G$, da velja $H < K < G$.

Definicija. Naj bo G grupa, H njena podgrupa in $g \in G$. Tedaj je *levi odsek* grupe G po podgrupi H, ki vsebuje g, enak množici $gH=\{gh : h \in H\}$. Podobno množica $Hg=\{hg : h \in H\}$ predstavlja *desni odsek* grupe G po podgrupi H, ki vsebuje g.

Trditev 2.2. *Naj bo G končna grupa in H njena podgrupa. Tedaj imajo vsi levi odseki grupe G po podgrupi H enako kardinalnost, ta pa je enaka redu podgrupe H. Enako velja tudi za desne odseke grupe G po podgrupi H.*

Definicija. Množico G/H vseh levih (desnih) odsekov grupe G po podgrupi H imenujemo *kvocientna množica*. Kardinalnosti *kvocientne množice* pravimo *indeks* podgrupe H v grupi G, označimo pa ga z $[G : H]$.

Izrek 2.3. *(Lagrangee) Naj bo G končna grupa in $H \leq G$. Potem je moč (kardinalnost) grupe G deljiva z močjo podgrupe H in velja naslednja enakost:*

$$|G| = [G : H] \cdot |H|.$$

Posledica 2.4. *Naj bo G končna grupa. Tedaj velja, da za vsak $g \in G$ red elementa g deli red grupe G.*

Definicija. Naj bo H pomnožica grupe G in $g \in G$. Tedaj množici

$$H^g = g^{-1}Hg = \{g^{-1}hg \mid h \in H\}$$

pravimo *konjugiranka* množice H z elementom g.

Definicija. Podgrupa H grupe G je *edinka* (oznaka $H \triangleleft G$), če je enaka vsaki svoji konjugiranki, to je

$$H^g = H$$

za vsak $g \in G$.

2.1.2 Znane družine grup

V tem podrazdelku bomo spoznali nekatere standardne družine grup, ki bodo omenjene skozi obravnavo osrednje teme diplomskega dela. Omenimo, da navedene družine grup predstavljajo le majhen delček vseh grup in obstaja še mnogo drugih, ki pa nas v nadaljevanju ne bodo zanimale.

Ciklična grupa $\mathbb{Z}_n$:
Grupa $\mathbb{Z}_n$ v resnici predstavlja komutativno grupo ($\mathbb{Z}_n$,+), pri čemer je $\mathbb{Z}_n$ množica ostankov pri deljenju z n, operacija v grupi pa je seštevanje po modulu n. Grupa $\mathbb{Z}_n$ je reda n.

Simetrična grupa S_n:
Gre za grupo, kjer je S_n množica vseh permutacij množice {1,2, ... ,n}, operacija v grupi pa je komponiranje preslikav (levi ali desni kompozitum). Za nas bo pomemben levi kompozitum preslikav, ki je opisan v [6]. Simetrične grupe za $n \geq 3$ niso *komutativne*, njihov *red* pa je enak $n!$.

Alternirajoča grupa A_n:
Grupo sestavljajo vse sode permutacije množice {1,2, ... ,n}, operacija pa je komponiranje preslikav. Ker je grupa sestavljena iz samih sodih permutacij množice {1,2, ... ,n}, je red grupe $\frac{n!}{2}$.

Diedrska grupa D_n:
V tem primeru gre za množico vseh togih simetrij pravilnega n-kotnika. Elemente grupe si lahko predstavljamo kot rotacije in zrcaljena pravilnega n-kotnika. Množica D_n je seveda podmnožica S_n, *red* grupe D_n pa je $2n$. Diedrsko grupo lahko predstavimo tudi kot tako imenovano končno prezentirano grupo na sledeč način

$$D_n = \langle\ r,z \mid r^n = z^2 = e,\ zrz^{-1} = r^{-1}\ \rangle.$$

2.1.3 Homorfizmi grup

Za konec tega razdelka se posvetimo še *homomorfizmom* grup, ki predstavljajo pomembne elemente v obravnavi osrednje tematike diplomskega dela. *Homomorfizmi* v splošnem predstavljajo preslikave med matematičnimi strukturami, ki ohranjajo njihovo strukturo.

Definicija. Bijektivno preslikavo množice same nase imenujemo *permutacija.*

Definicija. Naj bosta $(G, \bullet)$ in $(H, \circ)$ grupi. Preslikavo $\varphi : G \to H$, za katero velja:

$$\varphi(x \bullet y) = \varphi(x) \circ \varphi(y) \text{ za } \forall x, y \in G,$$

imenujemo *homomorfizem* grup.

Opomba. Ko operacija v grupah G in H ni navedena in jo torej v skladu z našim dogovorom izpuščamo, se pogoj za homomorfizem prepiše v $\varphi(xy) = \varphi(x)\varphi(y)$. Pri tem je potrebno vedeti, da xy na levi strani predstavlja produkt v grupi G, $\varphi(x)\varphi(y)$ pa produkt v grupi H.

Definicija. Preslikava $\varphi : G \to H$ je *izomorfizem*, če veljata naslednja pogoja:

1. φ je homomorfizem grup.
2. φ je bijektivna preslikava.

V primeru, ko je $H = G$, takšnemu izomorfizmu pravimo *avtomorfizem* grupe G. Ni se težko prepričati, da množica vseh *avtomorfizmov* grupe G za operacijo kompozitum predstavlja grupo. Označimo jo z $Aut(G)$.

V teoriji grup pravimo, da sta dve grupi *izomorfni* (oznaka $\cong$), če med njima obstaja kakšen izomorfizem grup. V tem primeru sta grupi strukturno enaki, ločita se le po konkretnem zapisu elementov in operacije v grupi.

2.2 Teorija grafov

Ker bomo v nadaljevanju omenjali tudi nekatere osnovne pojme iz teorije grafov, je smiselno, da bralca v tem kratkem razdelku seznanimo z osnovami tega področja. Osredotočili se bomo le na pojme, ki so pomembni v okviru tega diplomskega dela. Razdelek je povzet po [9].

Definicija. (*Enostaven neusmerjen*) *graf* je urejeni par $\Gamma = (V(\Gamma), E(\Gamma))$, kjer je $V(\Gamma)$ neprazna množica vozlišč grafa Γ, $E(\Gamma)$ pa množica povezav grafa Γ, pri čemer je $E(\Gamma)$ podmnožica množice neurejenih parov različnih vozlišč iz $V(\Gamma)$. V primeru, ko ni nevarnosti za nesporazum, množici $V(\Gamma)$ in $E(\Gamma)$ označimo kar z V in E. Za dve vozlišči u in v v grafu Γ pravimo, da sta *sosednji* (oznaka $u \sim v$), če je $\{u, v\} \in E(\Gamma)$. Kardinalnost množice $V(\Gamma)$ imenujemo *red* grafa Γ.

Dogovor. Dogovorimo se, da bo v nadaljevanju beseda *graf* označevala enostaven neusmerjen graf.

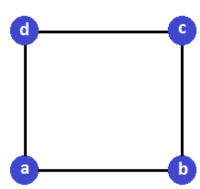
V predhodnem razdelku smo avtomorfizme omenili pri grupah, enako pa o avtomorfizmih lahko govorimo tudi pri grafih, kjer gre tokrat za primerne permutacije množice vozlišč grafa. Za nas bo v nadaljevanju *avtomorfizem grafa* prav tako pomemben pojem, zato je smiselno, da ga bralcu posebej predstavimo.

Definicija. Naj bo $\Gamma = (V, E)$ graf. Vsako bijektivno preslikavo $\varphi : V \to V$, ki ohranja sosednost, imenujemo *avtomorfizem grafa* Γ. Pri tem mora za poljuben par vozlišč $u, v \in V$ veljati sledeče:

$$\varphi(u) \sim \varphi(v) \iff u \sim v.$$

Tudi tokrat se ni težko prepričati, da množica vseh avtomorfizmov grafa Γ (oznaka $Aut(\Gamma)$) za operacijo kompozitum tvori grupo.

Zgled. Dan je graf $\Gamma = (V, E)$, kjer je $V = \{a, b, c, d\}$ in $E = \{\{a, b\}, \{b, c\}, \{c, d\}, \{d, a\}\}$. Poiščimo kak avtomorfizem tega grafa.



Slika 2.1: Upodobitev grafa Γ.

Torej, vozlišča grafa želimo premešati tako, da se bo sosednost vsakega vozišča ohranila (pri premešanju vozlišč bo na primer slika vozlišča a še vedno povezana s slikama vozlišč b in d). To lahko na primer storimo s ciklično rotacijo (predstavljamo si, da graf, upodobljen na sliki 2.1., rotiramo). Ta avtomorfizem je tako na primer podan s predpisom: $\varphi(a) = b$, $\varphi(b) = c$, $\varphi(c) = d$ in $\varphi(d) = a$.

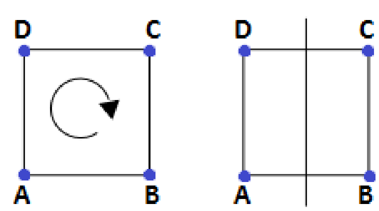
Poglavje 3

Delovanja grup

V tem poglavju se bomo posvetili *delovanjem grup*, ki predstavljajo temeljni pojem tega diplomskega dela. Skozi celotno poglavje bomo izhajali iz [8] in delno tudi iz [2] in [3].

S pomočjo grup v matematiki pogostokrat opisujemo simetrije konkretnih ali abstraktnih objektov. Kot primer vzemimo družino diedrskih grup, ki si jih lahko predstavljamo kot grupe simetrij pravilnih n-kotnikov. Elementi diedrske grupe tedaj na n-kotnik „delujejo“ kot rotacije in zrcaljenja. Za uvod in konkretno predstavitev pojma *delovanje* grupe, si oglejmo naslednji zgled.

Zgled. Oglejmo si grupo simetrij pravilnega štirikotnika, torej kvadrata. Premislimo, da gre za grupo D_4. V ta namen si oglejmo spodnjo sliko.

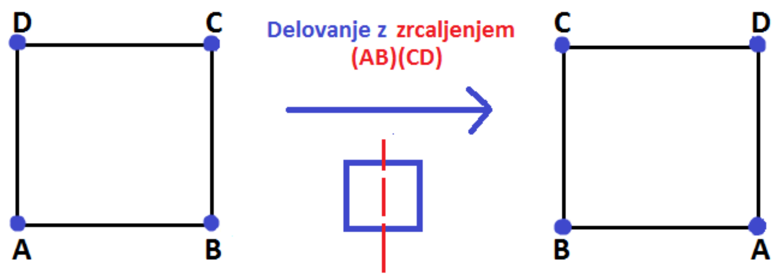


Slika 3.1: Simetriji kvadrata.

Na zgornji sliki sta prikazani rotacija kvadrata za 90 stopinj in eno izmed zrcaljenj tega kvadrata. Bralec se je verjetno z lahkoto prepričal v to, da oboje predstavlja simetrijo kvadrata. Namreč, če kvadrat rotiramo za 90 stopinj ali pa ga zrcalimo, kot je prikazano na zgornji sliki, je očitno, da se bo struktura kvadrata ohranila. To pomeni, da bo oglišče A še vedno povezano z ogliščema B in D. Enak razmislek velja tudi za preostala oglišča. Vemo pa, da sta prav rotacija in zrcaljenje generatorja grupe D_4, ki premore osem elementov. Iz tega jasno sledi, da potem vsak element grupe D_4 porodi eno izmed simetrij tega kvadrata. Ni se težko prepričati, da drugih simetrij kvadrat ne dopušča, tako da grupa njegovih simetrij res kar sovpada z grupo D_4.

Vsak element grupe D_4 permutira oglišča kvadrata, hkrati pa recimo tudi njegove robove. Na nek način si torej lahko predstavljamo, da grupa D_4 „deluje“ na razne objekte, povezane s kvadratom.

Za občutek, kako posamezen element grupe D_4 deluje na oglišča lika, si poglejmo naslednji dve sliki.



Slika 3.2: Delovanje zrcaljenja $(AB)(CD)$ na množici oglišč štirikotnika.

V zgornjem zgledu smo si ogledali primer *delovanja* grupe na manj abstraktni množici, saj si oglišč ali pa robov določenega lika ni težko predstavljati. Seveda pa delovanje grup ni omejeno zgolj na množice oglišč n-kotnikov in kot bomo spoznali v nadaljevanju, lahko govorimo celo o povsem abstraktnih delovanjih.

Skratka, pri delovanju grupe na množici elementi grupe permutirajo elemente dane množice, pri čemer pa morata veljati še dva dodatna pogoja, kar bo razvidno iz spodnje formalne definicije.

Definicija. Naj bo X neprazna množica in G grupa. *Delovanje* grupe G na množici X je preslikava $\star : G \times X \to X$ tako, da:

1. $\star(e, x) = x$ za $\forall x \in X$.
2. $\star(g_1 g_2, x) = \star(g_1, \star(g_2, x))$ za $\forall x \in X$ in za $\forall g_1, g_2 \in G$.

V tem primeru množici X pravimo G-množica.

Opomba. Omeniti velja dejstvo, da gre pri zgornji definiciji v resnici za tako imenovano *levo delovanje* grupe. Obstaja namreč tudi *desno delovanje* grupe, ki je definirano na zelo podoben način, vendar mu v tem diplomskem delu ne bomo posvečali posebne pozornosti. Zato se dogovorimo, da bo za nas beseda delovanje vedno pomenila zgoraj definirano levo delovanje.

Dogovor. Naj grupa G deluje na množici X in naj bo $\Delta \subseteq X$. Množico $g \star \Delta = \{g \star x : x \in \Delta\}$ bomo krajše označevali z $g \star \Delta$.

Dogovor. Dogovorimo se, da bomo pri delovanjih grup, namesto $\star(g,x)$ pisali $g \star x$, ali pa celo gx, če le ne bo nevarnosti za zmedo.

Omenimo, da je pri delovanju grupe na neko množico ta množica načeloma lahko poljubna, torej je lahko tudi kar pripadajoča množica elementov grupe, ki deluje. V tem primeru grupa deluje sama nase. Oglejmo si nekaj konkretenih zgledov.

Zgled. Naj bo G grupa in $\star : G \times G \to G$ preslikava, ki je definirana kot levo množenje v grupi, to je, $g \star x = gx$. Zlahka se prepričamo, da gre res za delovanje.

Zgled. Naj bo G grupa in $\star : G \times G \to G$ preslikava, podana s predpisom $g \star x = gxg^{-1}$ za $\forall g, x \in G$. Prepričajmo se, da gre res za delovanje.

Ker je $e \star x = exe^{-1} = exe = x$ za vsak $x \in G$, velja prvi pogoj delovanja. Za preverbo drugega pogoja delovanja se vprašamo, ali za poljubne $g, h, x \in G$ velja enakost $(gh) \star x = g \star (h \star x)$.

$$\begin{aligned}
(gh) \star x &= ghx(gh)^{-1} \\
&= ghxh^{-1}g^{-1} \\
&= g \star (hxh^{-1}) \\
&= g \star (h \star x).
\end{aligned}$$

Zgled. Če se ozremo na simetrično grupo S_n in vse njene podgrupe, ni težko ugotoviti, da vse omenjene grupe naravno delujejo na množici $X = \{1, 2, \ldots, n\}$. Za $\alpha \in S_n$ in $i \in X$ definiramo $\alpha \star i = \alpha(i)$. Jasno je, da gre za delovanje.

Zgled. Kot smo videli v uvodnem primeru tega poglavja, lahko govorimo tudi o grupah simetrij geometrijskih objektov. S tem mislimo na geometrijske like in telesa. V uvodnem primeru smo se pogovarjali le o delovanju grupe simetrij na množici oglišč in robov, v resnici pa grupa simetrij porodi še vrsto drugih delovanj. Na primer, grupe simetrij geometrijskih likov delujejo tudi na množici diagonal, pri geometrijskih telesih pa lahko govorimo o delovanju na množici robov, ploskev, telesnih diagonal, ploskovnih diagonal in podobno.

Zgled. Delovanje grup se velikokrat omenja tudi pri teoriji grafov, kjer govorimo o delovanju grupe avtomorfizmov grafa na množici vozlišč, povezav, lokov grafa, itd.

Zgled. Za konec omenimo še naslednje zglede delovanj grup. Splošna linearna grupa $GL(n, \mathbb{R})$ in njene podgrupe, posebna linearna grupa $SL(n, \mathbb{R})$, ortogonalna grupa $O(n, \mathbb{R})$ in posebna ortogonalna grupa $SO(n, \mathbb{R})$, so primeri tako imenovanih *Liejevih* grup. Vse te grupe naravno delujejo na vektorskem prostoru $\mathbb{R}^n$.

Oglejmo si sedaj nekaj dobro znanih osnovnih rezultatov o delovanjih. Dokaze si lahko zainteresirani bralec ogleda v [8].

Trditev 3.1. *Naj grupa G deluje na neprazni množici X. Za poljuben $g \in G$ definirajmo preslikavo $\sigma_g : X \to X$ s predpisom $\sigma_g(x) = gx$. Potem velja:*

1. *σ_g predstavlja permutacijo množice X.*
2. *Preslikava $\phi : G \to S_X$, s predpisom $\phi(g) = \sigma_g$, je homomorfizem grup.*

Iz te trditve sledi naslednji izrek, ki pove, da lahko na vsako končno grupo gledamo kot na podgrupo dovolj velike simetrične grupe.

Izrek 3.2. *(Cayley) Naj bo G končna grupa. V tem primeru je G izomorfna neki podgrupi grupe S_n, kjer je $n = |G|$.*

Sedaj pa se posvetimo dvema pojmoma, ki sta na področju delovanja grup zelo pomembna in s katerima se bomo v nadaljevanju pogostokrat srečevali.

Definicija. Naj grupa G deluje na neprazni množici X in naj bo x poljuben element množice X. Tedaj množici

$$G_x = \{g \in G : gx = x\}$$

elementov, ki element x fiksirajo, pravimo *stabilizator* točke x v grupi G. Množici slik,

$$\mathcal{O}_G(x) = \{gx : g \in G\},$$

pa pravimo *orbita* točke x pri delovanju grupe G.

Stabilizator točke x si lahko predstavljamo kot skupek elementov grupe delovanja, za katere velja, da točke x ne premikajo, oziroma jo „pribijejo“. Orbito točke x si na bolj preprost način lahko predstavljamo kot vse elemente v množici X, kamor lahko element x pri delovanju grupe G „premaknemo“.

Na tem mestu spomnimo na dobro znano in uporabno trditev.

Trditev 3.3. *Naj grupa G deluje na množici X in naj bo $x \in X$. Tedaj je G_x podgrupa grupe G.*

Definicija. Naj grupa G deluje na množici X. To delovanje je *tranzitivno*, če za poljubna $x, y \in X$ obstaja $g \in G$ tako, da velja $gx = y$.

Bolj preprosto povedano gre za delovanje grupe, ki ima eno samo orbito.

Sedaj pa se seznanimo z najpomembnejšim rezultatom tega poglavja, ki ima veliko uporabno vrednost, zato si bomo ogledali tudi njegov dokaz.

Izrek 3.4. *(O orbiti in stabilizatorju) Naj končna grupa G deluje na neprazni množici X. Tedaj za poljuben $x \in X$ velja enakost*

$$|G| = |\mathcal{O}_G(x)| \cdot |G_x|.$$

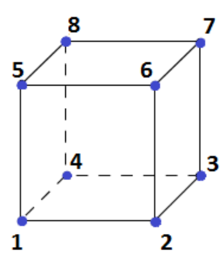
Dokaz. Pri dokazu izreka o orbiti in stabilizatorju lahko razmišljamo na sledeč način. Spomnimo se enakosti $|G| = [G : H] \cdot |H|$ iz Lagrangeevega izreka. Glede na to enakost torej lahko trdimo, da je dovolj najti bijektivno preslikavo med orbito poljubne točke $x \in X$ in množico levih odsekov grupe G po stabilizatorju G_x.

Definirajmo preslikavo $\phi : \mathcal{O}_G(x) \to G/G_x$. Naj bo $x_1 \in \mathcal{O}_G(x)$. Torej $\exists g_1 \in G$ tako, da velja $x_1 = g_1 x$. Definirajmo tedaj $\phi(x_1) = g_1 G_x$. Definirajmo preslikavo $\phi : \mathcal{O}_G(x) \to G/G_x$. Najprej je potrebno preveriti, ali je preslikava dobro definirana. Lahko bi se načeloma zgodilo, da velja $x_1 = g_1 x = g_1^{'} x$, zato je potrebno pokazati, da je vrednost $\phi(x_1)$ neodvisna od izbire $g_1 \in G$, za katerega velja $x_1 = g_1 x$. Torej, naj bo še $x_1 = g_1^{'} x$. Potem je $g_1 x = g_1^{'} x$ in seveda $g_1^{-1}(g_1 x) = g_1^{-1}(g_1^{'} x)$. Glede na definicijo delovanja lahko oklepaje premaknemo in dobimo $x = (g_1^{-1} g_1)x = (g_1^{-1} g_1^{'})x$. Torej očitno velja $g_1^{-1} g_1^{'} \in G_x$ in zato je $g_1^{'} \in g_1 G_x$ ter $g_1 G_x = g_1^{'} G_x$. Torej je ϕ dobro definirana.

Preveriti je potrebno še injektivnost in surjektivnost preslikave ϕ. Predpostavimo, da obstajata $x_1, x_2 \in \mathcal{O}_G(x)$, da velja $\phi(x_1) = \phi(x_2)$. V tem primeru zagotovo obstajata $g_1, g_2 \in G$ tako, da velja $x_1 = g_1 x$ in $x_2 = g_2 x$. Ker smo predpostavili $\phi(x_1) = \phi(x_2)$, sledi $g_2 \in g_1 G_x$ in zato je $g_2 = g_1 g$ za nek $g \in G_x$. Torej $x_2 = g_2 x = g_1(gx) = g_1 x = x_1$. Ker je $\phi(x_1) = \phi(x_2)$ le v primeru, ko je $x_1 = x_2$, sledi, da je ϕ injektivna. Za konec le še pokažimo, da je vsak levi odsek grupe G po stabilizatorju G_x slika nekega elementa iz $\mathcal{O}_G(x)$. Naj bo $g_1 G_x$ poljuben levi odsek. V tem primeru je kar $\phi(g_1 x) = g_1 G_x$, iz česar sledi, da je res vsak levi odsek slika nekega elementa iz $\mathcal{O}_G(x)$. Torej je ϕ surjektivna in posledično bijektivna. S tem je dokaz končan. ■

Za konec tega poglavja si oglejmo še konkreten primer, kjer bomo združili večji del teorije tega poglavja.

Zgled. Določimo red grupe vseh simetrij kocke.

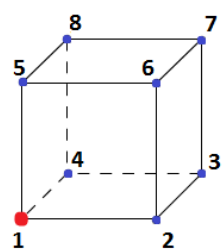


Slika 3.3: Kocka z označenimi oglišči.

Kot že vemo, grupe simetrij geometrijskih teles naravno delujejo na množici oglišč telesa. Pri tem vsak element grupe (t.j. simetrija) na nek način premeša oglišča danega telesa. Tako lahko vsako simetrijo kocke enolično zapišemo s permutacijo, ki je vsebovana v simetrični grupi S_8. Pomembno pa je vedeti, da obstajajo omejitve glede „premešanja“ množice oglišč, saj se mora pri delovanju grupe simetrij struktura kocke ohraniti. To pomeni, da mora pri vsakem premešanju oglišč na primer slika oglišča 1 še vedno ležati na skupnem robu s sliko vsakega od oglišč 2, 4 in 5. Enako velja seveda tudi za preostala oglišča. Iz tega razloga grupa simetrij kocke zagotovo ne bo izomorfna kar celi grupi S_8.

Iskano grupo simetrij označimo z G. Pri iskanju grupe nam bo v veliko pomoč izrek o orbiti in stabilizatorju. V ta namen poskusimo določiti velikost orbite oglišča 1. Hitro ugotovimo, da rotacija kocke $\pi = (1234)(5678)$ predstavlja eno izmed simetrij kocke, prav tako pa je simetrija kocke tudi $\theta = (15)(26)(37)(48)$, ki predstavlja zrcaljenje preko ravnine skozi razpolovišča robov 15, 26, 37 in 48.

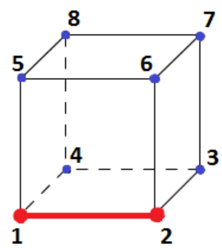
Na tem mestu lahko uporabimo izrek o orbiti in stabilizatorju, saj sedaj vemo, kakšna je velikost orbite oglišča 1. S permutacijo π lahko oglišče 1 premaknemo v oglišča 1, 2, 3 in 4, s permutacijo θ pa ga lahko spravimo v oglišče 5 na „zgornjem nivoju“. Torej lahko s kombinacijo obeh permutacij oglišče 1 spravimo v vsa oglišča kocke in zato je $|\mathcal{O}_G(1)| = 8$. Torej velja $|G| = 8 \cdot |G_1|$.



Slika 3.4: Kocka s fiksiranim ogliščem 1.

Tudi velikost stabilizatorja G_1 bomo določili s pomočjo izreka o orbiti in stabilizatorju, zato razmislimo, kako G_1 deluje na preostalih ogliščih. Razmislimo, kam lahko „premaknemo“ oglišče 2, da se bo struktura kocke ohranila (njegova slika bo torej še vedno na skupnem robu z ogliščem 1). Potencialni možnosti sta (poleg tega, da oglišče 2 pustimo na mestu) le dve: oglišči 4 in 5. Hitro ugotovimo, da s permutacijo $\sigma = (24)(68)$ strukturo kocke ohranimo, oglišče 2 pa premaknemo v oglišče 4. Kaj pa oglišče 5? Tudi tu ni nobenih težav, saj na primer s permutacijo $\rho = (25)(38)$ oglišče 2 spravimo v oglišče 5. Torej je orbita oglišča 2 pri delovanju grupe G_1 velikosti 3. Potem velja $|G_1| = |\mathcal{O}_{G_1}(2)| \cdot |G_{1,2}| = 3 \cdot |G_{1,2}|$, pri čemer $G_{1,2}$ predstavlja podgrupo simetrij kocke, ki fiksira vsako izmed oglišč 1 in 2 (posledično tudi rob, ki ju povezuje).

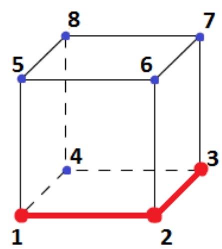
Oglejmo si sedaj delovanje grupe $G_{1,2}$ na preostalih ogliščih. Kam lahko premaknemo oglišče 3? Potencialna možnost je samo oglišče 6. Če z elementom grupe $G_{1,2}$ premaknemo oglišče 3 na mesto oglišča 6, moramo zaradi ohranitve strukture kocke oglišče 6 nujno premakniti na mesto oglišča 3. V tem primeru je potem potrebno zamenjati tudi oglišči 4 in 5. Tako smo dobili novo ustrezno permutacijo $\lambda = (36)(45)$,



Slika 3.5: Kocka s fiksiranima ogliščema 1 in 2.

ki je očitno simetrija kocke. Pri delovanju grupe $G_{1,2}$ je torej orbita oglišča 3 velikosti 2 in sledi $|G_{1,2}| = |\mathcal{O}_{G_{1,2}}(3)| \cdot |G_{1,2,3}| = 2 \cdot |G_{1,2,3}|$.

Oglejmo si sedaj grupo $G_{1,2,3}$.



Slika 3.6: Kocka s fiksiranimi oglišči 1, 2 in 3.

Vprašamo se, kakšna je orbita oglišča 4 pri delovanju grupe $G_{1,2,3}$. V primeru, ko oglišča 1, 2 in 3 fiksiramo, oglišča 4 ne moremo nikamor premakniti, saj se sosednost oglišč kocke nebi ohranila. Torej je pri delovanju grupe $G_{1,2,3}$ velikost orbite oglišča 4 enaka 1. Razmislimo, ali velja enako tudi za oglišča 5, 6, 7 in 8. Kakšna je orbita oglišča 5 pri delovanju grupe $G_{1,2,3}$? Očitno, ker je „spodnji nivo“ kocke fiksiran, oglišča 5 ni mogoče premakniti na drugo mesto, saj potem ne bi ležalo na skupnem robu z ogliščem 1. S tem bi se „porušila“ struktura kocke. Torej bo pri delovanju grupe $G_{1,2,3}$ velikost orbite oglišča 5 prav tako enaka 1. Enak razmislek velja tudi za preostala oglišča. S tem smo ugotovili, da delovanje grupe $G_{1,2,3}$ vsa oglišča kocke fiksira, in sledi

$$\begin{aligned} |G_{1,2,3}| &= 1, \\ |G_{1,2}| &= 2 \cdot |G_{1,2,3}| = 2 \cdot 1 = 2, \\ |G_1| &= 3 \cdot |G_{1,2}| = 3 \cdot 2 = 6, \\ |G| &= 8 \cdot |G_1| = 8 \cdot 6 = 48. \end{aligned}$$

Torej, red grupe G je 48.

Poglavje 4

Primitivnost in neprimitivnost delovanja grup

Delovanja grup na majhnih množicah so načeloma obvladljiva in zato je njihovo raziskovanje precej preprosto. Ko pa raziskujemo delovanja grup na velikih množicah, kmalu ugotovimo, da je proučevanje z običajnimi metodami zahtevno in neuspešno. Zato se je potem smiselno vprašati, ali obstaja način, ki bi omogočal bolj enostavno in sistematično pot pri odkrivanju strukturnih lastnosti delovanj. Tu igra pomembno vlogo tako imenovano neprimitivno delovanje grup, ki predstavlja osrednjo temo tega diplomskega dela. V tem poglavju izhajamo predvsem iz [2].

Najprej se bomo posvetili tako imenovanim *blokom neprimitivnosti*, ki predstavljajo ključen element neprimitivnih delovanj. Bloki neprimitivnosti, ohlapno povedano, predstavljajo „kose“ množice, za katere velja, da jih delovanje ne more „raztrgati“. Obstoj tovrstnih blokov omogoča reduciranje delovanja na manjše množice, pri čemer pa se strukturne lastnosti prvotnega delovanja običajno prenesejo na to inducirano delovanje, s čimer raziskovanje postane bolj enostavno.

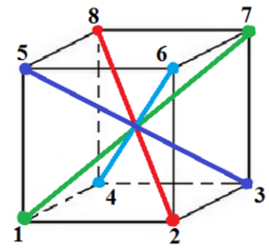
4.1 Bloki neprimitivnosti

Definicija. Naj grupa G tranzitivno deluje na množici X. Neprazno množico $\Delta \subseteq X$ imenujemo *blok* za to delovanje, če za vsak $g \in G$ velja $g \star \Delta = \Delta$ ali $(g \star \Delta) \cap \Delta = \emptyset$.

Opomba. Glede na zapisano definicijo lahko bralec hitro ugotovi, da celotna G-množica in vsak posamezen element G-množice predstavlja blok delovanja. Tovrstni bloki nimajo uporabne vrednosti, zato jim pravimo *trivialni bloki.* Netrivialnemu bloku z najmanjšo kardinalnostjo pravimo *minimalen* blok, tistemu z največjo kardinalnostjo pa *maksimalen* blok.

Oglejmo si nekaj zgledov.

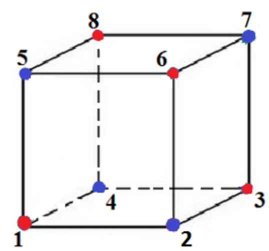
Zgled. Spomnimo se zadnjega zgleda iz prejšnjega poglavja, kjer smo določili red grupe simetrij kocke. Pri tem smo si pomagali z naravnim delovanjem te grupe na množici osmih oglišč kocke. Na tem mestu se vprašajmo, ali obstajajo znotraj množice oglišč kocke neke manjše podmnožice, ki bi ustrezale definiciji bloka. Oglejmo si na primer krajišča telesnih diagonal.



Slika 4.1: Krajišča telesnih diagonal.

Razmislimo, ali res za vsako telesno diagonalo kocke velja, da množica, ki sestoji iz njenih krajišč, ustreza definiciji bloka. Pod drobnogled vzemimo na primer par $\{2, 8\}$ (krajišči rdeče telesne diagonale). Zanimivo je opaziti, da krajišči poljubne telesne diagonale nimata skupnega soseda, torej oglišča, ki bi ležalo na skupnem robu z vsakim izmed njiju. Ni se težko prepričati, da sta krajišči poljubne telesne diagonale tudi edini tip para oglišč kocke, ki so v takšnem odnosu. Iz tega sledi, da se pri delovanju katerekoli simetrije na oglišča kocke krajišči poljubne telesne diagonale lahko premakneta v krajišči preostalih telesnih diagonal ali pa se ne premakneta, torej ostaneta znotraj svoje diagonale. V nasprotnem primeru bi se sturktura kocke „porušila“.

Poskusimo poiskati še kakšen netrivialen blok delovanja. Oglejmo si na primer množico $\{1, 3, 6, 8\}$.

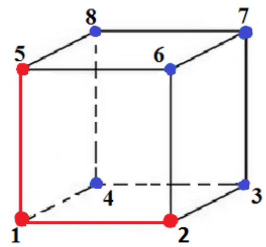


Slika 4.2: Kocka z označenim blokom delovanja.

Tudi v tem primeru se ni težko prepričati, da izbrana množica predstavlja blok delovanja. Vemo namreč, da grupa simetrij kocke pri delovanju na oglišča kocke ohranja sosednost oglišč, posledično pa tudi razdalje (razdaljo razumemo kot najmanjše število robov, ki povezujejo izbrani oglišči) med njimi.

Če se ozremo na zgornjo sliko, opazimo, da so od vsakega „rdečega“ oglišča preostala „rdeča“ oglišča oddaljena za 2, „modra”pa za 1 ali 3. To pomeni, da se v primeru, da se pri delovanju nekega elementa grupe simetrij kocke na oglišča neko „rdeče“ oglišče premakne v „modro“, sledi, da se bodo posledično vsa „rdeča“ oglišča premaknila v „modra“ oglišča. V nasprotnem se sosednost med oglišči kocke nujno spremeni, saj bi v tem primeru neki oglišči, ki sta oddaljeni za 2, bili po novem oddaljeni za 1 ali 3. V primeru, ko se pri delovanju neko „rdeče“ oglišče premakne v „rdeče“ oglišče, iz enakega razloga kot prej, opazimo, da se potem tudi vsa preostala „rdeča“ oglišča nujno premaknejo v „rdeča“ oglišča. Torej je množica $\{1, 3, 6, 8\}$ res blok delovanja.

Sedaj pa poskusimo poiskati primer podmnožice oglišč, ki ni blok. Vzamemo na primer krajišča robov kocke.



Slika 4.3: Kocka z označenima robovoma.

Na primer, če na množici oglišč kocke delujemo s simetrijo $\lambda = (25)(38)$, se množica $\{1, 2\}$ preslika v množico $\{1, 5\}$ od koder sledi, da $\{1, 2\}$ ni blok.

Zgled. Oglejmo si delovanje ciklične grupe $G = \langle(123456)\rangle$ na množici $X = \{1, 2, 3, 4, 5, 6\}$ in določimo vse netrivialne bloke tega delovanja.

Ker je grupa G ciklična in je red elementa (123456) enak 6, je seveda G reda 6. Konkretno je $G = \{id, (14)(25)(36), (135)(246), (153)(264), (165432), (123456)\}$.

Ker nas zanimajo le netrivialni bloki delovanja, so lahko možni kandidati le podmnožice $\Delta \subseteq X$, za katere velja $1 < |\Delta| < 6$.

$|\Delta| = 2$:
Hitro opazimo, da dvoelementne množice, ki vsebujejo zaporedne številke (števili 6 in 1 prav tako razumemo kot zaporedni števili), ne ustrezajo definiciji bloka, saj če na njih delujemo z elementom (123456), dobimo množico, ki vsebuje le en element iz prvotne množice in nek nov element (na primer za $\Delta = \{1, 2\}$ in $\lambda = (123456)$ je $\lambda \star \Delta = \{2, 3\}$, od koder sledi, da Δ ni blok). Podoben razmislek sledi tudi za vse takšne množice Δ, ki vsebujejo števili, med katerima se nahaja natanko eno vmesno število (to so množice $\{1, 3\}, \{2, 4\}, \{3, 5\}, \{4, 6\}, \{1, 5\}$ in $\{2, 6\}$). Za vsako izmed naštetih množic se v dejstvo, da to ni blok, prepričamo z delovanjem z elementom (135)(246). Ostanejo le še podmnožice, katerih elementa se razlikujeta za 3, torej $\{1, 4\}, \{2, 5\}$ in $\{3, 6\}$. V tem primeru hitro uvidimo, da vse tri množice predstavljajo bloke, saj element (123456) permutira te tri množice, posledično pa tudi vsaka njegova potenca. S tem smo preverili vse možnosti dvoelementnih množic (vse ostale so že zajete). Torej, bloki kardinalnosti dve so trije in sicer: $\Delta_1 = \{1, 4\}, \Delta_2 = \{2, 5\}$ in $\Delta_3 = \{3, 6\}$.

$|\Delta| = 3$:
Glede na to, da obstaja 20 različnih troelementnih podmnožic, bo bolje, če morebitne bloke poiščemo s premislekom. Enako kot prej opazimo, da blok velikosti 3 ne sme

vsebovati dveh zaporednih števil, saj bi delovanje elementa (123456), „blok“ „raztrgalo“. Torej edini možnosti sta: $\Delta_4 = \{1,3,5\}$ in $\Delta_5 = \{2,4,6\}$, ki pa sta očitno res bloka, saj element (123456) ravno izmenjuje ti dve množici.

$|\Delta| = 4$ in $|\Delta| = 5$:
Izmed šestih elementov nikakor ne moremo izbrati štiri ali pet elementov tako, da bi se izognili zaporednosti števil v množici. Če na katerokoli množico kardinalnosti štiri ali pet delujemo z elementom (123456), je očitno, da potem ta množica ni blok. Zato lahko zaključimo, da bloki kardinalnosti štiri ali pet ne obstajajo.

Torej, ugotovili smo, da je res pet netrivialnih blokov. To so: $\Delta_1 = \{1,4\}, \Delta_2 = \{2,5\}, \Delta_3 = \{3,6\}$, $\Delta_4 = \{1,3,5\}$ in $\Delta_5 = \{2,4,6\}$.

Opomba. Bralec bo v nadaljevanju videl, da lahko tovrstno nalogo v resnici rešimo še hitreje s poznavanjem lastnosti blokov neprimitivnosti.

Pri raziskovanju blokov neprimitivnosti se lahko pojavi vrsta zanimivih vprašanj. Med njimi sta na primer: Kako je s presekom blokov? Kako je s sliko bloka? Odgovore na ti vprašanji bomo med drugimi raziskali v nadaljevanju. Najprej si oglejmo naslednjo trditev.

Trditev 4.1. *Naj grupa G tranzitivno deluje na množici X in naj bosta Δ_1 ter Δ_2 bloka za to delovanje z nepraznim presekom. Tedaj $\Delta_1 \cap \Delta_2$ prav tako predstavlja blok delovanja G na X.*

Dokaz. V primeru, ko je presek množic Δ_1 in Δ_2 enoelementna množica, je $\Delta_1 \cap \Delta_2$ spet blok, saj je vsak element množice X (trivialen) blok. Denimo torej, da množica $\Delta_1 \cap \Delta_2$ ni blok in vsebuje vsaj dva elementa. Potem vemo, da za neka različna elementa $\alpha, \beta \in \Delta_1 \cap \Delta_2$ obstaja $g \in G$ tako, da velja $g \star \alpha \in X \setminus (\Delta_1 \cap \Delta_2)$ in $g \star \beta \in \Delta_1 \cap \Delta_2$. Velja $\alpha, \beta \in \Delta_1 \cap \Delta_2$, to je $\alpha, \beta \in \Delta_1$ in $\alpha, \beta \in \Delta_2$. Ker je Δ_1 blok, bo $g \star \alpha, g \star \beta \in \Delta_1$. Tako sklepamo, saj vemo, da se pri delovanju na blok celoten blok ohrani (kot množica), ali pa se preslika v neko disjunktno množico. Torej zaradi $g \star \beta \in \Delta_1$ sledi $g \star \alpha \in \Delta_1$. Enak razmislek velja tudi za množico Δ_2. Ker je Δ_2 blok, zaradi $g \star \beta \in \Delta_2$ sledi še $g \star \alpha \in \Delta_2$. Torej je $g \star \alpha \in \Delta_1 \cap \Delta_2$, kar je protislovje, ki pove, da $\Delta_1 \cap \Delta_2$ res predstavlja blok. ■

Preden spoznamo novo lastnost blokov, se spomnimo pojma particije množice.

Definicija. *Particija* ali *razbitje* množice X je družina podmnožic $\{X_1, X_2, X_3, ..., X_k\}$ tako, da velja:

1. Če je i$\neq$j, potem je $X_i \cap X_j = \emptyset$.
2. $X = X_1 \cup X_2 \cup ... \cup X_k$.

Bolj preprosto povedano gre za razdelitev množice na „kose“. Na primer, naj bo dana množica $X = \{1,2,3,4,5,6\}$. Primer particije množice X bi lahko opisali kot skupek množic $X_1 = \{1,2\}, X_2 = \{3,4\}$ in $X_3 = \{5,6\}$. To seveda ni edina paritcija množice

X. Množici $X_4 = \{1, 3, 6\}$ in $X_5 = \{2, 4, 5\}$ prav tako tvorita particijo množice X. Opomnimo pa tudi, da particijo množice ne tvorijo nujno enaki „kosi“ množice. Na primer $X_6 = \{1, 3\}$ in $X_7 = \{2, 4, 5, 6\}$ prav tako tvorita particijo množice X.

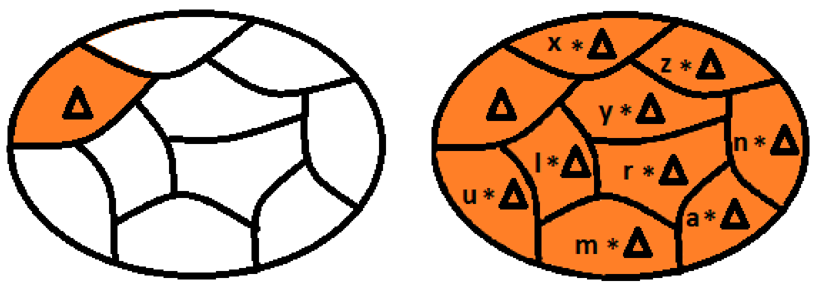
Bralec je verjetno opazil, da je za poljubno delovanje množica orbit delovanja particija množice, na kateri imamo definirano delovanje. Na tem mestu se spomnimo uvodnega primera tega poglavja, kjer smo pri delovanju grupe simetrij kocke na množici oglišč ugotovili, da krajišča telesnih diagnonal $\{1, 8\}, \{2, 7\}, \{3, 6\}$ in $\{4, 5\}$ predstavljajo bloke delovanja. Vidimo, da vsi ti bloki tvorijo particijo množice oglišč kocke.

Tako se je smiselno vprašati, ali tudi v splošnem velja, da iz bloka delovanja dobimo particijo množice delovanja.

Trditev 4.2. *Naj grupa G tranzitivno deluje na neprazni množici X, množica Δ pa naj bo blok za delovanje grupe G. V tem primeru množica $\Sigma = \{g \star \Delta \mid g \in G\}$ tvori particijo množice X in tedaj vsak element Σ predstavlja blok delovanja grupe G.*

Dokaz. Najprej pokažimo, da je $\bigcup_{g \in G}(g \star \Delta) = X$. Očitno je, da velja $\bigcup_{g \in G}(g \star \Delta) \subseteq X$, saj X predstavlja G-množico. Sedaj pa pokažimo še, da velja $\bigcup_{g \in G}(g \star \Delta) \supseteq X$. Naj bo $x \in X$ in vzemimo poljuben $y \in \Delta$. Ker G deluje tranzitivno na množici X, obstaja $g \in G$, da velja $g \star y = x$. Iz tega sledi $x \in g \star \Delta$. Ker je bil $x \in X$ poljuben, velja $\bigcup_{g \in G}(g \star \Delta) \supseteq X$, kar posledično pomeni, da je $\bigcup_{g \in G}(g \star \Delta) = X$. Pokažimo še prvo točko definicije particije množice. Naj bo $g_1, g_2 \in G$ in predpostavimo, da je $(g_1 \star \Delta) \cap (g_2 \star \Delta) \neq \emptyset$. Potem obstajata $x, y \in \Delta$, za katera velja $g_1 \star x = g_2 \star y$. Iz tega sledi enakost $x = (g_1^{-1} g_2) \star y$. Torej očitno velja $((g_1^{-1} g_2) \star \Delta) \cap \Delta \neq \emptyset$ in ker je Δ blok, sledi $g_1^{-1} \star (g_2 \star \Delta) = \Delta$. Po delovanju z elementom g_1 sledi $g_2 \star \Delta = g_1 \star \Delta$. S tem smo pokazali, da so elementi množice Σ paroma disjunktni in dokazali, da Σ tvori particijo množice X.
Prav tako se ni težko prepričati, da vsak element množice Σ predstavlja blok delovanja. Denimo namreč nasprotno, da obstaja nek $g_1 \in G$, da $g_1 \star \Delta$ ni blok. Tedaj zagotovo obstajata $x, y \in g_1 \star \Delta$ in nek $g_2 \in G$, da velja $g_2 \star x \in g_1 \star \Delta$ in $g_2 \star y \in X \setminus (g_1 \star \Delta)$. To pa vodi v protislovje. Zakaj? Ker je $x, y \in g_1 \star \Delta$, sledi $g_2 \star x, g_2 \star y \in (g_2 g_1) \star \Delta$, in zaradi predpostavke $g_2 \star x \in g_1 \star \Delta$ sledi $(g_2 g_1) \star \Delta = g_1 \star \Delta$. Tedaj pa iz $g_2 \star y \in (g_2 g_1) \star \Delta$ sledi še $g_2 \star y \in g_1 \star \Delta$, kar je v nasprotju s predpostavko. Torej vsak element množice Σ res predstavlja blok. ■

Opomba. Bralec je pri obravnavi zgornjega dokaza verjetno opazil, da se v tem primeru delovanje grupe G lahko prenese tudi na manjšo množico Σ, saj nevtralni element grupe vsak element Σ (t.j. blok) ohranja, velja pa tudi drugi pogoj delovanja, saj za poljubna $g_1, g_2 \in G$ velja $g_1 \star (g_2 \star \Delta) = (g_1 g_2) \star \Delta$. Prav ta možnost zmanjševanja velikosti množice, na kateri deluje dana grupa, omogoča enostavnejše odkrivanje strukturnih lastnosti delovanj, ki dopuščajo bloke neprimitivnosti.



Slika 4.4: Ilustrativni prikaz delovanja grupe G na blok Δ.

Definicija. Naj grupa G tranzitivno deluje na množici X in naj bo Δ netrivialen blok tega delovanja. Tedaj množica $\Sigma = \{g \star \Delta \mid g \in G\}$ tvori particijo množice X, ki jo imenujemo *sistem blokov neprimitivnosti*, ki vsebuje blok Δ.

Opomba. V literaturi zasledimo različna poimenovanja sistema blokov neprimitivnosti. Včasih mu pravimo tudi *G-invariantna particija*.

Bralec bo na podlagi zgornjih zgledov verjetno ugotovil, da na primer pari krajišč telesnih diagonal v kocki predstavljajo sistem blokov neprimitivnosti za delovanje grupe simetrij kocke.

V predhodnem poglavju smo spoznali pojem stabilizatorja točke, ki se nanaša na posamezen element množice delovanja. Izkaže se, da sta pri proučevanju blokov pomembna tudi tako imenovana *točkovni stabilizator množice* in *stabilizator množice*, zato si oglejmo njuni definiciji.

Definicija. Naj grupa G deluje na množici X in naj bo $\Delta \subseteq X$. Tedaj množici $G_{(\Delta)} = \{g \in G \mid g \star x = \alpha \text{ ; } za \ \forall x \in \Delta\}$ pravimo *točkovni stabilizator* množice Δ pri delovanju grupe G, množici $G_{\{\Delta\}} = \{g \in G \mid g \star \Delta = \Delta\}$ pa *stabilizator množice* Δ pri delovanju grupe G.

Trditev 4.3. *Naj grupa G deluje na množici X in naj bo $\Delta \subseteq X$. Tedaj sta $G_{(\Delta)}$ in $G_{\{\Delta\}}$ podgrupi grupe G, velja pa tudi, da je $G_{(\Delta)} \lhd G_{\{\Delta\}}$.*

Dokaz. Dokažimo najprej, da je $G_{(\Delta)} \leq G$. Očitno je $e \in G_{(\Delta)}$ in tako je $G_{(\Delta)}$ neprazna množica. Če je $g \in G_{(\Delta)}$, potem za vsak $x \in \Delta$ velja $g^{-1} \star x = g^{-1} \star (g \star x) = (g^{-1} g) \star x = x$, od koder sledi $g^{-1} \in G_{(\Delta)}$. Naj bosta še $g_1, g_2 \in G_{(\Delta)}$. Potem za $x \in \Delta$

velja $(g_1 g_2) \star x = g_1 \star (g_2 \star x) = g_1 \star x = x$ in sledi $G_{(\Delta)} \leq G$.

Sedaj dokažimo, da je $G_{\{\Delta\}} \leq G$. Kot prej bo $e \in G_{\{\Delta\}}$ in tako je $G_{\{\Delta\}}$ neprazna množica. Za $g \in G_{\{\Delta\}}$ je $g^{-1} \star \Delta = g^{-1} \star (g \star \Delta) = (g^{-1} g) \star \Delta = e \star \Delta = \Delta$ in sledi $g^{-1} \in G_{\{\Delta\}}$. Naj bosta še $g_1, g_2 \in G_{\{\Delta\}}$. Potem je $(g_1 g_2) \star \Delta = g_1 \star (g_2 \star \Delta) = g_1 \star \Delta = \Delta$. Torej res velja $G_{\{\Delta\}} \leq G$.

Potrebno je dokazati še, da je $G_{(\Delta)} \lhd G_{\{\Delta\}}$. Naj bo $g_1 \in G_{\{\Delta\}}$, $g_2 \in G_{(\Delta)}$ in $x \in \Delta$. Da je $G_{(\Delta)} \leq G_{\{\Delta\}}$, sledi iz definicije. Dovolj je torej pokazati, da je $(g_1 g_2 g_1^{-1}) \star x = x$. Naj bo $y = g_1^{-1} \star x$. Ker je $g_1 \in G_{\{\Delta\}}$, sledi $g_1^{-1} \in G_{\{\Delta\}}$, zato je posledično $y \in \Delta$. Potem je $(g_1 g_2 g_1^{-1}) \star x = (g_1 g_2) \star (g_1^{-1} \star x) = (g_1 g_2) \star y = g_1 \star (g_2 \star y)$. Ker je $g_2 \in G_{(\Delta)}$, sledi $g_1 \star (g_2 \star y) = g_1 \star y = g_1 \star (g_1^{-1} \star x) = (g_1 g_1^{-1}) \star x = x$. Torej je res $g_1 g_2 g_1^{-1} \in G_{(\Delta)}$. Tako smo dokazali, da je $G_{(\Delta)} \lhd G_{\{\Delta\}}$. ■

Bralec verjetno opaža zanimivo dejstvo, da je $G_{(\Delta)} = \bigcap_{\alpha \in \Delta} G_\alpha$.

Trditev 4.4. *Naj grupa G tranzitivno deluje na množici X in naj bo Δ blok tega delovanja. Tedaj grupa $G_{\{\Delta\}}$ tranzitivno deluje na množici Δ.*

Dokaz. Naj bo $x \in \Delta$. Ker grupa G na množici X deluje tranzitivno, sledi, da za vsak $\beta \in \Omega$ obstaja $g_1 \in G$, da je $g_1 \star x = y$. Posledično tudi za poljuben $z \in \Delta$ obstaja nek $g_2 \in G$, da je $g_2 \star x = z$. Vsak tak g_2 pa bo zagotovo element $G_{\{\Delta\}}$, saj je Δ blok. Namreč, ker je $g_2 \star x \in \Delta$, je $(g_2 \star \Delta) \cap \Delta \neq \emptyset$ in tako sledi $g_2 \star \Delta = \Delta$. Torej je g_2 element $G_{\{\Delta\}}$. S tem je dokaz končan. ■

Zadnji trditvi nam ponujata močno orodje za razumevanje in enostavnejše dokazovanje nekaterih lastnosti blokov neprimitivnosti. Njuna uporabnost se kaže tudi pri dokazovanju naslednje lastnosti blokov, ki nam omogoča lažje iskanje blokov.

Trditev 4.5. *Naj končna grupa G tranzitivno deluje na množici X in naj bo Δ blok tega delovanja. Tedaj velikost bloka Δ deli red grupe G.*

Dokaz. Ker po trditvi 4.3 velja $G_{\{\Delta\}} \leq G$, po Lagrangeevem izreku sledi, da red podgrupe $G_{\{\Delta\}}$ deli red grupe G. Če dokažemo, da velikost bloka Δ deli red grupe $G_{\{\Delta\}}$, je s tem dokaz končan. Po predhodni trditvi sledi, da grupa $G_{\{\Delta\}}$ tranzitivno deluje na množici Δ. Zaradi boljše preglednosti naj bo $H = G_{\{\Delta\}}$. Potem po izreku o orbiti in stabilizatorju sledi, da je $|H| = |\Delta| \cdot |H_x|$, kjer je $x \in \Delta$. Torej, ker $|\Delta|$ deli $|G_{\{\Delta\}}|$, sledi, da deli tudi red grupe G. ■

Za konec tega razdelka si oglejmo še naslednjo trditev, ki je prav tako pomembna pri iskanju blokov.

Trditev 4.6. *Naj grupa G tranzitivno deluje na končni množici X in naj bo Δ blok tega delovanja. Tedaj za vsak $g \in G$ velja $|g \star \Delta| = |\Delta|$, poleg tega pa $|\Delta|$ deli $|X|$.*

Dokaz. Prvi del trditve je očiten, saj po trditvi 3.1 vsak $g \in G$ pri delovanju na množici X porodi bijektivno preslikavo na X. Za poljubna različna $x, y \in \Delta$ tako velja $g \star x \neq g \star y$ in zato sledi $|g \star \Delta| = |\Delta|$. Da $|\Delta|$ deli kardinalnost množice X, je sedaj enostavno opaziti, saj po trditvi 4.2 orbita bloka Δ tvori particijo množice X. Ker imajo vsi elementi (bloki) te particije isto kardinalnost, je kardinalnost množice X večkratnik velikosti bloka Δ. Torej sledi, da $|\Delta|$ deli $|X|$. ■

Uporabnost zgornjih trditev bomo prikazali na primerih v nadaljevanju.

4.2 Primitivnost

V tem razdelku se bomo posvetili tako imenovani primitivnosti delovanj grup. Pri obravnavi primitivnosti delovanj ima obstoj blokov neprimitivnosti ključno vlogo.

Definicija. Naj grupa G tranzitivno deluje na množici X. V primeru, da ima to delovanje le trivialne bloke, pravimo, da grupa G *primitivno* deluje na množici X. Tranzitivnemu delovanju grupe G na množici X, ki ni primitivno, pravimo *neprimitivno* delovanje.

Če se ozremo na prej obravnavana delovanja grup, bo bralec verjetno brez težav opazil, da so bila vsa delovanja neprimitivna, saj so povsod nastopali neki bloki neprimitivnosti. Kaj pa primitivna delovanja? Oglejmo si konkreten zgled.

Zgled. Pokažimo, da je naravno delovanje grupe S_4 na množici $X = \{1, 2, 3, 4\}$ primitivno.

Po trditvi 4.6 so lahko netrivialni bloki le velikosti 2, a če bi bil recimo $\{i, j\}$ blok, kjer sta $i, j \in \{1, 2, 3, 4\}$ različna, bi $\alpha = (jk)$, kjer je $k \in \{1, 2, 3, 4\} \setminus \{i, j\}$, „blok“ $\{i, j\}$ „raztrgal“. Element i bo fiksiral, j pa poslal izven „bloka“. Torej pri naravnem delovanju S_4 na množici $X = \{1, 2, 3, 4\}$ ni netrivialnih blokov, kar pomeni, da je delovanje res primitivno.

Kot bomo pokazali v naslednjem zgledu, je šlo tu le za poseben primer bolj splošnega pojava.

Zgled. Obrazložimo, zakaj grupe S_n in A_n, pri čemer je $n > 2$, primitivno delujeta na množici $X = \{1, 2, \ldots, n\}$.

V primeru, da bi pri delovanju grupe S_n oziroma A_n na množici X obstajal netrivialen blok, bi potem lahko našli nek $i \notin X \setminus \Delta$. Ker so v grupi S_n vsebovane vse možne transpozicije elementov iz množice X in ker je $|\Delta|$ vsaj 2, je očitno, da z ustrezno transpozicijo (ij), pri čemer je $j \in \Delta$, po principu prejšnjega zgleda „blok“ Δ „raztrgamo“. V primeru, ko je $n = 3$, je po trditvi 4.6 očitno, da pri delovanju grupe A_3 na množici X ni netrivialnih blokov, ker je 3 praštevilo. V vseh ostalih primerih pa lahko najdemo ustrezno permutacijo $(ij)(kl)$, pri čemer je $j \in \Delta$, s katero po principu prejšnjega zgleda množico Δ „raztrgamo“.

Sedaj pa spoznajmo enega najpomembnejših rezultatov tega razdelka.

Trditev 4.7. *Naj grupa G tranzitivno deluje na množici X in naj bo $x \in X$. Množica Σ naj predstavlja množico vseh blokov Δ za G, ki vsebujejo element x, množica Π pa naj vsebuje vse $H \leq G$, pri čemer je $G_x \leq H$. Tedaj obstaja bijektivna preslikava $\Psi : \Sigma \to \Pi$, podana s predpisom $\Psi(\Delta) = G_{\{\Delta\}}$, katere inverzna preslikava je podana s predpisom $\Theta(H) = H \star \alpha = \{h \star \alpha : h \in H\}$. Preslikava Ψ ohranja urejenost v smislu, da če sta $\Delta_1, \Delta_2 \in \Sigma$, potem je $\Delta_1 \subseteq \Delta_2 \iff \Psi(\Delta_1) \leq \Psi(\Delta_2)$.*

Dokaz. Za začetek najprej pokažimo, da preslikava Ψ s predpisom $\Psi(\Delta) = G_{\{\Delta\}}$ res slika iz množice Σ v množico Π. Naj bo $\Delta \in \Sigma$. Potem za vsak $g \in G_x$ velja $x \in \Delta \cap (g \star \Delta)$ in sledi $\Delta = g \star \Delta$, saj je Δ blok. To dokazuje, da je vsak $g \in G_x$ vsebovan tudi v $G_{\{\Delta\}}$. Torej, ker je $G_x \subseteq G_{\{\Delta\}}$ za vsak $\Delta \in \Sigma$ in ker sta G_x ter $G_{\{\Delta\}}$ grupi, sledi $G_x \leq G_{\{\Delta\}}$. To pomeni, da Ψ res slika iz Σ v Π.

Sedaj pa pokažimo, da preslikava Θ res slika iz množice Π v množico Σ. Naj bo H podgrupa grupe G, pri čemer je $G_x \leq H$ in označimo $\Delta = H \star x$. V resnici nas zanima, ali je Δ res blok, ki vsebuje x. Naj bo $g \in G$. Če je $g \in H$, je očitno, da bo $\Delta = g \star \Delta$, saj je $g \star \Delta = g \star (H \star x) = (gH) \star x = \Delta$. V primeru, ko $g \notin H$, pa trdimo, da velja $(g \star \Delta) \cap \Delta = \emptyset$. Predpostavimo, da velja nasprotno, in sicer $(g \star \Delta) \cap \Delta \neq \emptyset$. Tedaj obstajata $h_1, h_2 \in H$ tako, da $g \star (h_1 \star x) = h_2 \star x$. Ker je torej $x = h_2^{-1} \star (g \star (h_1 \star x))$, posledično sledi $h_2^{-1} g h_1 \in G_x$ in tako velja $g \in h_2 G_x h_1^{-1}$ (množimo s h_2 na levi in s h_1^{-1} na desni). Jasno, ker sta $h_2, h_1^{-1} \in H$ in je $G_x \leq H$, sledi $h_2 G_x h_1^{-1} \subseteq H$. Torej je $g \in H$, s čimer smo prišli v protislovje s predpostavko in zato Δ predstavlja blok, ki pa očitno vsebuje x, saj $e \in H$. Iz tega sledi, da preslikava Θ res slika iz množice Π v množico Σ.

Dokažimo, da sta preslikavi Ψ in Θ inverzni. Po trditvi 4.4 vemo, da $G_{\{\Delta\}}$ na množici Δ deluje tranzitivno. To posledično pomeni, da bo kompozitum preslikav $\Theta \circ \Psi$ enak identiteti na množici Σ. Zakaj? Naj bo $H = G_{\{\Delta\}}$. Zaradi tranzitivnosti delovanja grupe H na množici Δ je $H \star x$ blok, ki vsebuje Δ in ker za vsak $g \in G_{\{\Delta\}}$ zaradi $x \in \Delta$ velja $g \star x \in \Delta$, je $H \star x = \Delta$. Sedaj pa dokažimo še, da je kompozitum $\Psi \circ \Theta$ identiteta na množici Π. Naj bo $H \in \Pi$ in $\Delta = \Theta(H) = H \star \alpha$. Potrebno je dokazati, da je $H = G_{\{\Delta\}}$. Ker je $hH = H$ za vsak $h \in H$, je jasno, da je $H \leq G_\Delta$. Obratno, če je $g \in G_\Delta$, je $g \star (H \star x) = H \star x$, torej obstaja $h \in H$, da je $gh \in G_x$, posledično pa je $g \in G_x h^{-1} \subseteq H$, saj $G_x \leq H$. Torej je $H = G_{\{\Delta\}}$ in s tem smo dokazali, da sta Θ in Ψ inverzni preslikavi.

Za konec pa pokažimo še, da Ψ ohranja urejenost. Naj bosta Δ_1 in Δ_2 bloka, ki vsebujeta x. Če je $G_{\{\Delta_1\}} \leq G_{\{\Delta_2\}}$, potem po trditvi 4.4 sledi, da je $\Delta_1 \subseteq \Delta_2$. Za implikacijo v nasprotno smer pa privzemimo, da je $\Delta_1 \subseteq \Delta_2$. Za $g \in G_{\{\Delta_1\}}$ tedaj velja, da je $(g \star \Delta_2) \cap \Delta_2 \neq \emptyset$, saj so vsi elementi množice Δ_1 vsebovani v množici Δ_2. Ker je Δ_2 blok, sledi $g \star \Delta_2 = \Delta_2$. Torej je vsak $g \in G_{\{\Delta_1\}}$ vsebovan v $G_{\{\Delta_2\}}$ in zato res velja $G_{\{\Delta_1\}} \leq G_{\{\Delta_2\}}$. S tem smo dokazali, da preslikava Ψ ohranja urejenost in tako je trditev dokazana. ■

Na tem mestu se spomnimo zgleda, kjer smo poiskali vse netrivialne bloke pri naravnem delovanju grupe $G = \langle(123456)\rangle$ na množici $X = \{1, 2, 3, 4, 5, 6\}$. Stabilizator točke 1 je tu trivialen, torej nam, glede na trditev 4.7, vsaka podgrupa grupe G da en blok, ki vsebuje 1. Seveda enako velja tudi za preostale elemente množice, saj so stabilizatorji preostalih točk prav tako trivialni. Ker obstajata natanko dve pravi netrivialni podgrupi grupe G, to sta $H_1 = \{id, (14)(25)(36)\}$ in $H_2 = \{id, (135)(246), (153)(264)\}$, iz tega sledi, da pri tem delovanju obstaja natanko 5 netrivialnih blokov. To so $\Delta_1 = \{1, 4\}, \Delta_2 = \{2, 5\}$, $\Delta_3 = \{3, 6\}$, $\Delta_4 = \{1, 3, 5\}$ in $\Delta_5 = \{2, 4, 6\}$, kot smo ugotovili že prej.

Posledica 4.8. *Naj grupa G tranzitivno deluje na množici X, ki vsebuje najmanj dva elementa. To delovanje je primitivno natanko tedaj, ko je za vsak $x \in X$ točkovni stabilizator G_x maksimalna podgrupa grupe G.*

Zgornja posledica nam omogoča bolj sistematično, enostavno in predvsem hitrejše raziskovanje strukturnih lastnosti delovanj grup. Preden si ogledamo konkreten zgled, kjer bomo prikazali uporabnost zadnje posledice, bomo prej spoznali še naslednjo trditev, ki je za nas prav tako pomembna.

Trditev 4.9. *Naj grupa G deluje na množici X in naj bosta $x, y \in X$ taka, da obstaja $g \in G$, za katerega je $y = g \star x$. Tedaj velja enakost $G_y = gG_xg^{-1}$.*

Dokaz. Najprej dokažimo, da velja $G_y \subseteq gG_xg^{-1}$. Naj bo $h \in G_y$. Potem velja $(g^{-1}hg) \star x = (g^{-1}h) \star y = g^{-1} \star y = x$. Torej je $g^{-1}hg \in G_x$ in posledično $h \in gG_xg^{-1}$. Sedaj pa dokažimo še, da je $G_y \supseteq gG_xg^{-1}$. Naj bo $h \in G_x$. Potem je $(ghg^{-1}) \star y = (gh) \star x = g \star x = y$. Sledi $ghg^{-1} \in G_y$ in s tem je dokaz končan. ■

Posledica 4.10. *Naj grupa G tranzitivno deluje na množici X. Tedaj so vsi stabilizatorji točk med seboj konjugirani.*

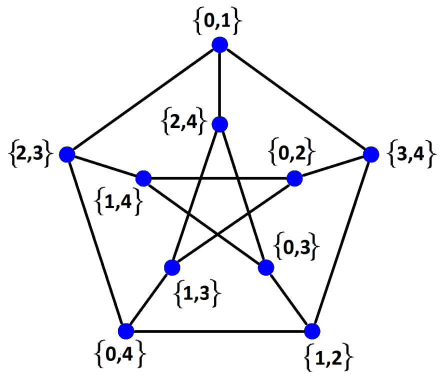
Bralec verjetno opaža, da ima zadnja posledica v kombinaciji s posledico 4.8 precejšnjo uporabno vrednost. Za ugotovitev, ali grupa primitivno deluje (pri tranzitivnem delovanju) na neki množici, je dovolj preveriti, ali je točkovni stabilizator poljubnega izbranega elementa množice res maksimalna podgrupa grupe delovanja.

Zgled. Pokažimo, da je grupa avtomorfizmov dobro znanega Petersenovega grafa $GP(5, 2)$ izomorfna grupi S_5 in da ta grupa primitivno deluje na množici vozlišč grafa.

Najprej pokažimo, da je $Aut(GP(5, 2)) \cong S_5$. Petersenov graf si lahko predstavljamo tudi na malce drugačen način, kot smo ga sicer vajeni. Predstavljajmo si, da vozlišča grafa tvorijo vse dvoelementne množice z elementi iz grupe $\mathbb{Z}_5$. Bralca opomnimo, da je $Sym(\mathbb{Z}_5)$ izomorfna grupi S_5. Dve vozlišči sta med seboj povezani natanko tedaj, ko je presek pripadajočih množic prazen. Če definiramo bolj formalno, velja:

$V(GP(5, 2)) = \{\{i, j\} : i, j \in \mathbb{Z}_5, i \neq j\}$ in velja $\{i, j\} \sim \{s, t\} \iff \{i, j\} \cap \{s, t\} = \emptyset$.

Pripadajoči graf je upodobljen na sliki 4.5.



Slika 4.5: Petersenov graf $GP(5, 2)$ z označenimi vozlišči.

Iz definicije očitno sledi, da vsaka permutacija $\sigma \in Sym(\mathbb{Z}_5)$ porodi avtomorfizem grafa, ki je definiran s predpisom $\sigma\star\{i,j\} = \{\sigma\star i, \sigma\star j\}$. Kako vemo, da tak predpis res predstavlja avtomorfizem grafa? Ker so permutacije iz $Sym(\mathbb{Z}_5)$ bijekcije na $\mathbb{Z}_5$, so bijekcije tudi na množici povezav iz $\mathbb{Z}_5$. Izberimo neko poljubno povezavo grafa in primerjajmo množici, ki označujeta vozlišči na tej povezavi. Ker so vsi štirje pripadajoči elementi iz $\mathbb{Z}_5$ različni (dva elementa v prvi in dva elementa v drugi množici) in je vsaka permutacija bijektivna preslikava, bosta pri delovanju σ na ti dve množici rezultat disjunktni množici, ki torej po definiciji grafa ustrezata paru povezanih vozlišč. Za nesosednji vozlišči velja zelo podoben premislek.

S tem smo spoznali, da grupa avtomorfizmov Petersenovega grafa vsebuje podgrupo, izomorfno S_5 in je tako reda vsaj 120. Če dokažemo, da je grupa avtomorfizmov grafa reda natanko 120, tako je prvi del trditve dokazan.

Zaradi boljše preglednosti naj bodo vozlišča označena na naslednji način: $a = \{0,1\}, b = \{2,3\}, c = \{0,4\}, d = \{1,2\}, e = \{3,4\}, f = \{2,4\}, g = \{1,4\}, h = \{1,3\}, i = \{0,3\}$ in $j = \{0,2\}$. Naj bo $G = Sym(\mathbb{Z}_5)$. Ker G očitno tranzitivno deluje na množici vozlišč grafa, po lemi o orbiti in stabilizatorju velja

$$|G| \;=\; 10 \cdot |G_a|.$$

Če fiksiramo vozlišče a, ni težko opaziti, da je pri delovanju grupe G_a orbita vozlišča b velikosti 3, saj z delovanjem permutacije $\alpha_1 = (01)(24) \in Sym(\mathbb{Z}_5)$ oglišče b premaknemo na mesto vozlišča e, z delovanjem permutacije $\alpha_2 = (01)(34) \in Sym(\mathbb{Z}_5)$, pa na mesto vozlišča f. Ker je stopnja grafa enaka 3, posledično ni možno, da bi bila orbita vozlišča b pri delovanju z G_a večja od 3. Torej velja

$$|G_a| \;=\; 3 \cdot |G_{a,b}|.$$

Sedaj pa dodatno fiksirajmo še vozlišče b. Razmislimo, kakšna je orbita vozliča c pri delovanju grupe $G_{a,b}$. Zaradi zahtev glede ohranitve povezav grafa (na primer vozlišče

a bo vedno povezano samo z vozlišči b, e, f) se vozlišče c lahko ohrani na istem mestu, ali pa mogoče premakne na mesto vozlišča g. Seveda je slednja možnost tudi ustrezna, saj z delovanjem permutacije $\alpha_3 = (01) \in Sym(\mathbb{Z}_5)$ vozlišči a in b fiksiramo, vozlišče c pa premaknemo na mesto vozlišča g. Torej potemtakem velja

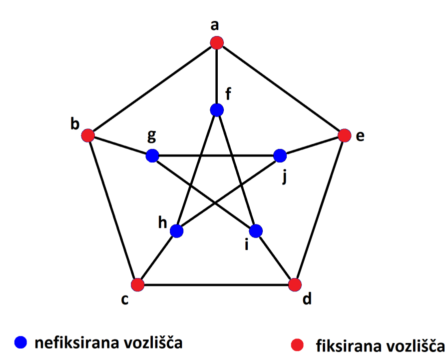
$$|G_{a,b}| \;=\; 2 \cdot |G_{a,b,c}|.$$

Fiksirajmo še vozlišče c in razmislimo, kam se lahko vozlišče d premakne pri delovanju grupe $G_{a,b,c}$. Lahko se ohrani na svojem mestu, ali pa mogoče premakne na mesto vozlišča h. Hitro ugotovimo, da z delovanjem permutacije $\alpha_4 = (23) \in Sym(\mathbb{Z}_5)$ fiksiramo vozlišča a, b in c, vozlišče d pa premaknemo na mesto vozlišča h in zato velja

$$|G_{a,b,c}| \;=\; 2 \cdot |G_{a,b,c,d}|.$$

Fiksirajmo nazadnje še vozlišče d in poglejmo, kam se lahko vozlišče e premakne pri delovanju grupe $G_{a,b,c,d}$. Bralec najbrž opaža, da vozlišča e ni mogoče premakniti v vozlišča „notranje zvezde“, saj v tem primeru vozlišče e ne bi bilo več povezano z vozliščema a in d. Torej je orbita elementa e pri delovanju grupe $G_{a,b,c,d}$ enoelementna.

Pokažimo, da je grupa $G_{a,b,c,d}$ v resnici trivialna. Ker sedaj vemo, da fiksiramo tudi vozlišče e, bi potem vozlišča na „notranji zvezdi“ predstavljala tista vozlišča, ki bi se mogoče lahko še kam premaknila.



Slika 4.6: Prikaz fiksiranih vozlišč na grafu.

Iz zgornje slike je očitno, da je v primeru, ko je fiksiran celoten zunanji cikel grafa (rdeča vozlišča), potem posledično fiksirana tudi „notranja zvezda“ („modra“ vozlišča), saj je vsako „modro vozlišče“ povezano z natanko enim fiksiranim „rdečim vozliščem“.
Grupa $G_{a,b,c,d}$ je tako trivialna in zato je red iskane grupe avtomorfizmov enak $10 \cdot 3 \cdot 2 \cdot 2 = 120$, kar pomeni, da je $Aut(GP(5, 2)) \cong S_5$.

Sedaj pa dokažimo še drugi del.

Če želimo ugotoviti, ali grupa avtomorfizmov grafa deluje primitivno na množici vozlišč, potem zadostuje, da za neko poljubno vozlišče določimo točkovni stabilizator in preverimo, ali je maksimalna podgrupa v S_5.

Izberimo na primer vozlišče a. Iz enakosti

$$\begin{aligned} |G| &= 10 \cdot |G_a| \\ 120 &= 10 \cdot |G_a| \\ 12 &= |G_a| \end{aligned}$$

sledi, da iščemo neko grupo H, ki je reda 12. Ker so v H očitno elementi (01), (23) in (24), posledično H vsebuje $\langle(01),(23),(24)\rangle$. Ni se težko prepričati, da gre za grupo reda 12. Torej je $H = \langle(01),(23),(24)\rangle$, oziroma kar $H = \langle(01)(23),(01)(234)\rangle$.

Če po viru [1] privzamemo, da so v grupi S_5 vse podgrupe, ki so izomorfne D_6, maksimalne, je torej dovolj pokazati, da sta grupi H in D_6 izomorfni. Generatorja (01)(23) in (01)(234) grupe H sta reda 2 in 6 poleg tega pa je $(01)(23)(01)(234)(01)(23) = (01)(243) = ((01)(234))^{-1}$. Ker sta generatorja z in r grupe D_6 prav tako reda 2 in 6, je zato izomorfizem med grupama lahko definiran kot:

$$\Psi(((01)(234))^i((01)(23))^j) = r^i z^j.$$

Podrobnosti prepuščamo bralcu.
S tem smo pokazali, da sta grupi H in D_6 izomorfni, kar posledično pomeni, da je stabilizator poljubnega vozlišča maksimalna podgrupa v grupi G. Iz tega sledi, da grupa G primitivno deluje na množici vozlišč Petersenovega grafa $GP(5,2)$.

4.3 Orbite edinke

Za konec se posvetimo še edinkam, ki predstavljajo pomemben pojem pri obravnavi blokov neprimitivnosti. V splošnem vemo, da ko grupa G tranzitivno deluje na množici X, potem na množici X naravno deluje tudi vsaka njena podgrupa H. Izkaže se, da so pri obravnavi primitivnosti delovanja celotne grupe pomembne njene edinke.

Trditev 4.11. *Naj grupa G tranzitivno deluje na množici X in naj bo N njena edinka. Tedaj so orbite edinke N bloki za delovanje G na množici X.*

Dokaz. Naj bo x nek poljuben element množice X in g nek element grupe G. Tedaj $N \star x$ predstavlja orbito grupe N na množici X, ki vsebuje α. V resnici se torej sprašujemo, ali je pri delovanju nekega poljubnega elementa iz grupe G na orbito $N \star \alpha$ rezultat spet neka orbita grupe N. Da je temu res tako, se brž prepričamo:

$$\begin{aligned} g \star (N \star x) &= (gN) \star x = \\ &= (Ng) \star x = \\ &= N \star (g \star x). \end{aligned}$$

■

Opomba. Tu velja omeniti, da trditev v primeru, ko je N tranzitivna edinka, nima uporabne vrednosti, saj je potem $g \star (N \star x) = N \star x = X$ in tako je orbita edinke le ena sama. Tedaj orbita edinke tvori trivialni blok. V primeru ko je N netranzitivna netrivialna edinka, je uporabnost trditve očitna, saj vsaka orbita predstavlja blok neprimitivnosti.

Posledica 4.12. Naj grupa G primitivno deluje na množici X. Tedaj njena vsaka netrivialna podgrupa edinka tranzitivno deluje na množici X.

Dokaz. Grupa G deluje tranzitivno na množici X, torej po trditvi 4.11 sledi, da vsaka edinka grupe G tvori sistem blokov, kar pa pomeni, da je v primeru primitivnega delovanja ta sistem lahko le celotna množica X, ali pa unija vseh posameznih elementov množice. Ker pa gre za netrivialne edinke, je edina možnost, da bločni sistem sestavlja kar sama množica X, kar posledično pomeni, da vsaka netrivialna edinka na množici X deluje tranzitivno. ■

Oglejmo si dva preprosta zgleda.

Zgled. Naj grupa S_3 deluje na množici $X = \{1, 2, 3\}$. Ker vemo, da S_3 primitivno deluje na množici X in grupa A_3 predstavlja netrivialno edinko, mora po zgornji posledici grupa A_3 tranzitivno delovati na množici X. To je seveda očitno res. Po drugi strani, ker podgrupa $\langle(12)\rangle$ očitno ne deluje tranzitivno, po zgornji trditvi 4.11 sledi, da ni edinka v S_3.

Zgled. Naj grupa $\mathbb{Z}_8$ deluje sama nase s seštevanjem po modulu $\mathbb{Z}_8$. Na podlagi podgrup edink poiščimo kakšen sistem blokov.
Ker je grupa $\mathbb{Z}_8$ komutativna grupa, sledi, da je vsaka njena podgrupa edinka. Na primer, grupa $\langle 2\rangle = \{0, 2, 4, 6\}$ predstavlja edinko reda 4 in po trditvi 4.11 orbite te edinke tvorijo sistem blokov. Torej delovanje te grupe tvori bloka $\Delta_1 = \{1, 3, 5, 7\}$ in $\Delta_2 = \{0, 2, 4, 6\}$. Podobno podgrupa $\langle 4\rangle = \{0, 4\}$ pri delovanju tvori bloke $\Delta_1 = \{0, 4\}$, $\Delta_2 = \{1, 5\}$, $\Delta_3 = \{2, 6\}$ in $\Delta_4 = \{3, 7\}$.

Poglavje 5

Zaključek

V diplomskem delu smo se ukvarjali z delovanji grup, ki v splošnem predstavljajo pomembno področje v teoriji grup. Osrednja tema diplomskega dela sloni na obravnavi blokov neprimitivnosti, kjer je imel bralec možnost spoznati veliko definicij, lastnosti, rezultatov in konkretnih primerov, na katerih je lahko spoznal uporabnost tega koncepta, poleg tega pa preverjal svoje razumevanje obravnavane snovi.

Zaključimo lahko, da obravnava blokov neprimitivnosti in z njimi povezane primitivnosti delovanj zahteva določeno mero predznanja iz področja teorije grup, saj gre v resnici za nadgradnjo delovanja grup na množicah. S študijem vsebine diplomskega dela je bralec lahko spoznal, da je obstoj blokov neprimitivnosti odvisen od različnih dejavnikov, kot so na primer velikost G-množice, velikost grupe delovanja itd. Obstoj blokov neprimitivnosti ponuja možnost prenosa delovanja grupe s celotne množice na manjše množice, pri čemer se nekatere strukturne lastnosti delovanja ohranijo. Na tak način obsežna in posledično težje obvladljiva delovanja postanejo enostavnejša za raziskovanje.

V tem diplomskem delu si je bralec lahko med drugim ogledal tudi primer delovanja grupe avtomorfizmov znanega, vozliščno tranzitivnega, Petersenovega grafa $GP(5,2)$, kjer se je izkazalo, da ta grupa primitivno deluje na množici vozlišč tega grafa. Torej to delovanje ne dopušča netrivialnih blokov neprimitivnosti, kar je posledica zelo velike simetričnosti grafa. V tem primeru si pri raziskovanju strukturnih lastnosti tega delovanja, z uporabo koncepta blokov neprimitivnosti, ne moremo prav nič pomagati. Seveda to ne drži za vse vozliščno tranzitivne grafe, zato bi bilo v nadaljevanju smiselno raziskati tiste vozliščno tranzitivne grafe, ki pa bloke neprimitivnosti omogočajo. Še posebej zanimivi so grafi, katerih grupa avtomorfizmov vsebuje kakšno netrivialno edinko, ki velja za pomemben vir blokov. Tovrstni bloki nam ponavadi nudijo veliko uporabnih informacij o strukturnih lastnostih obravnavanega grafa. Ena izmed njih je gotovo hamiltonskost vozliščno tranzitivnih grafov, ki še vedno predstavlja odprt problem. Pri vsem tem bi bilo seveda ključnega pomena obravnavano snov najprej poglobiti, saj kot je bralec verjetno že opazil, ima vsaka blokovska lastnost veliko uporabno vrednost, ki nam omogoča enostavnejše raziskovanje delovanj.

Literatura

[1] Čakš, Branka, 2011: Podgrupe simetrične grupe S_5. Diplomsko delo. Maribor: Univerza v Mariboru. Fakulteta za naravoslovje in matematiko.

[2] Dixon, J. D., Mortimer, Brian, 1996: Permutation Groups. New York: Springer.

[3] Dummit, David S., Foote, Richard M., 2004: Abstract Algebra. 3rd ed. Hoboken: Wiley and sons.

[4] Fraleigh, John B., 2002: A First Course in Abstract Algebra. 6th ed. Massachusetts: Addison Weseley.

[5] Grafi in njihovi avtomorfizmi. Pridobljeno 15.07.2015 s svetovnega spleta: http://ucilnica1213.fmf.uni-lj.si/pluginfile.php/6990/mod_resource/content/0/SimetrijeOktNov.pdf

[6] Malnič, Aleksander, 2012: Zapiski pri predmetu algebrske strukture. Ljubljana: Pedagoška fakulteta.

[7] Primitivnost in neprimitivnost. Pridobljeno 15.07.2015 s svetovnega spleta: http://studentski.net/gradivo/ulj_fmf_mf3_peg_sno_primitivnost_in_neprimitivnost_01?r=1

[8] Šparl, Primož, 2013: Zapiski pri predmetu abstraktna algebra. Ljubljana: Pedagoška fakulteta.

[9] Šparl, Primož, 2014: Zapiski pri predmetu teorija grafov. Ljubljana: Pedagoška fakulteta.

Izjava o avtorstvu

Spodaj podpisani Dejan Krejić, z vpisno številko 01011318, izjavljam, da je diplomsko delo z naslovom

DELOVANJE GRUP IN BLOKI NEPRIMITIVNOSTI,

ki sem ga napisal pod mentorstvom doc. dr. Primoža Šparla, avtorsko delo in da so uporabljeni viri ter literatura korektno navedeni.

Podpis študenta:

____

Ljubljana, september 2015