UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN
INFORMACIJSKE TEHNOLOGIJE

Magistrsko delo

Simetrije cirkulantnih grafov

(Symmetry of circulant graphs)

Ime in priimek: Maruša Saksida
Študijski program: Matematične znanosti, 2. stopnja
Mentor: doc. dr. Primož Šparl

Koper, december 2014

Ključna dokumentacijska informacija

Ime in PRIIMEK: Maruša SAKSIDA

Naslov magistrskega dela: Simetrije cirkulantnih grafov

Kraj: Ljubljana

Leto: 2014

število listov: 77 število slik: 44 število tabel: 2

število referenc: 23

Mentor: doc. dr. Primož Šparl

UDK: 519.17(043.2)

Ključne besede: Cirkulantni graf, točkovna tranzitivnost, povezavna tranzitivnost, ločna tranzitivnost, izomorfizem, grupa avtomorfizmov, ciklični indeks, normalen cirkulant.

Math. Subj. Class. (2010): 05C25, 20B25

Izvleček: Magistrsko delo obravnava simetrije cirkulantnih grafov oziroma cirkulantov. Cirkulanti, $\mathrm{Circ}(n; S)$, so grafi, katerih množico točk predstavlja ciklična grupa $\mathbb{Z}_n$, množico povezav pa določa poljubna podmnožica S te grupe, ki je zaprta za inverze in ne vsebuje nevtralnega elementa. Pri tem velja, da sta dve točki, a in b, cirkulanta $\mathrm{Circ}(n; S)$ povezani natanko tedaj, ko obstaja tak element $s \in S$, da je $a + s = b$. Pogosto se zgodi, da dva na videz popolnoma različna grafa z matematičnega vidika predstavljata isti graf. Pravimo, da sta pripadajoča grafa izomorfna. Permutacijam množice točk danega grafa, ki ohranjajo sosednost, pravimo avtomorfizmi. Množica vseh avtomorfizmov grafa tvori grupo avtomorfizmov. Ta grupa naravno deluje na različne objekte grafa, kot so točke, povezave ali loki. Če na množici točk, povezav ali lokov grupa avtomorfizmov deluje tranzitivno, pravimo, da je graf točkovno, povezavno ali ločno tranzitiven. Ravno s temi tremi lastnostmi grafov, še posebej cirkulantov, se ukvarjamo v tem magistrskem delu. Tako najprej dokažemo, da so vsi točkovno tranzitivni grafi praštevilskega reda

cirkulantni grafi. Prav tako si ogledamo kaj lahko povemo o izomorfnosti takšnih grafov, o njihovi grupi avtomorfizmov ter določimo število paroma neizomorfnih cirkulantov praštevilskega reda za posamezno praštevilsko vrednost. Pri povezavni in ločni tranzitivnosti ugotovimo, da je cirkulant povezavno tranzitiven natanko tedaj, ko je ločno tranzitiven. Poiščemo vse ločno tranzitivne cirkulante do 30 točk in dobljeni seznam primerjamo s karakterizacijo ločno tranzitivnih cirkulantov I. Kovácsa. Na koncu obravnavamo še ločno tranzitivne cirkulante, ki so normalni. Natanko določimo kako izgledajo ločno tranzitivni cirkulanti praštevilskega reda ter kako izgledajo normalni ločno tranzitivni cirkulanti.

Key words documentation

Name and SURNAME: Maruša SAKSIDA

Title of final project paper: Symmetry of circulant graphs

Place: Ljubljana

Year: 2014

Number of pages: 77 Number of figures: 44 Number of tables: 2

Number of references: 23

Mentor: Assist. Prof. Primož Šparl, PhD

UDC: 519.17(043.2)

Keywords: Circulant graph, vertex-transitive, edge-transitive, arc-transitive, isomorphism, group of authomorphisms, cycle index, normal circulant.

Math. Subj. Class. (2010): 05C25, 20B25

Abstract: In this master's thesis we investigate symmetries of circulant graphs or circulants. Circulants $\mathrm{Circ}(n; S)$ are graphs where the set of vertices is represented by a cyclic group $\mathbb{Z}_n$ and the adjacency is determined by a subset S of $\mathbb{Z}_n$, which is closed under taking inverses and does not contain the identity element. Two vertices a and b of the circulant $\mathrm{Circ}(n; S)$ are adjacent if and only if there exists an element $s \in S$ such that $a+s = b$. It often happens that two graphs represent the same graph which at first glance appear to be entirely different from a mathematical point of view. We say that the corresponding graphs are isomorphic. We call the premutations of the vertices which preserve adjacency automorphisms. The set of all automorphisms of a graph forms a group called the group of automorphisms. This group acts naturally on different objects of the graph, such as vertices, edges and arcs. If the group of automorphisms acts transitively on the set of vertices, edges or arcs, we say that the graph is vertex-, edge- or arc-transitive, respectively. These properties of graphs, mainly of circulants, are the main topics of interest in this master's thesis. We first prove that all vertex-transitive graphs of prime

order are circulants. We then investigate the question of when two such graphs are isomorphic, we investigate their group of automorphisms and determine the number of pairwise non-isomorphic circulants of a fixed prime order. Regarding edge- and arc-transitivity we prove that a circulant is edge-transitive if and only if it is also arc-transitive. We find all arc-transitive circulants on up to 30 vertices and compare the obtained list with the characterization of arc-transitive circulants of I. Kovács. In the end we take a look at so-called normal arc-transitive circulants. We determine the structure of arc-transitive circulants of prime order and of normal arc-transitive circulants.

Zahvala

Prav posebna zahvala gre najprej Ivi Antončič, za vso pomoč, spodbude in napotke v času študija in pri pisanju tega magistrskega dela.

Nič manj ne gre zahvala mentorju dr. Primožu Šparlu, ki me je v času pisanja tega magistrskega dela ves čas usmerjal in ga potrpežljivo popravljal.

Mami, tebi hvala za neizmerno podporo na vsakem življenjskem koraku.

Hvala tudi Mariji, Nastji, Gabrielu in Hirokiju, za nepozaben čas na Famnitu.

Kazalo vsebine

Seznam tabel

Seznam slik

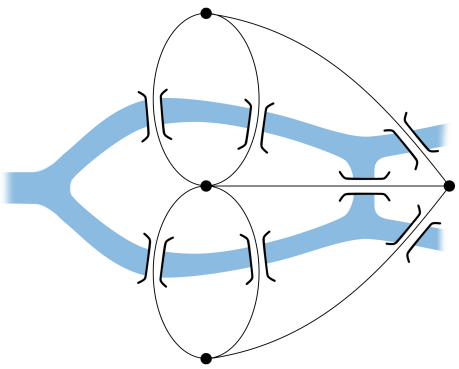
Seznam kratic

TTP točkovno tranzitiven graf praštevilskega reda
N-Circ normalen cirkulant

1 UVOD

Magistrsko delo, ki je pred vami, sodi na področje algebraične teorije grafov. Teorije grafov zato, ker so glavni predmet preučevanja grafi, algebraične pa zaradi pristopa, ki uporablja številna spoznanja iz (abstraktne) algebre.

Grafe si lahko najpreprosteje predstavljamo kot objekte, sestavljene iz točk in povezav med njimi. Tako kot večina drugih teorij v matematiki se je tudi ta razvila iz realnega problema. Leta 1735 se je švicarski matematik Leonhard Euler (1707 - 1783) lotil problema Königsberških mostov. Skozi tedanje mesto Königsberg (sedanji Kaliningrad v Rusiji) je tekla reka Pregel, ki je mesto razdelila na štiri dele, ti pa so bili med seboj povezani s sedmimi mostovi. Euler se je lotil vprašanja, ali je mogoče vsakega od mostov prečkati natanko enkrat in se vrniti na začetno mesto. Leta 1736 je v članku z naslovom "Solutio problematis ad geometriam situs pertinentis" dokazal, da to ni mogoče in sicer tako, da je namesto štirih območij kopnega in sedem mostov med njimi narisal štiri točke in sedem povezav med njimi. Nastal je (multi)graf s pomočjo katerega zlahka vidimo, da kaj takega res ni mogoče.



Slika 1: Shematični prikaz mesta Königsberg.

Kot nakazuje že slika 1, grafe običajno upodobimo kot diagrame, pri čemer lahko točke grafa poljubno razporedimo, pomembno pa je le to, katere točke so med seboj povezane. Še posebej zanimivi so grafi, v katerih je vsaka točka vsebovana na istem številu povezav. Gre za tako imenovane regularne grafe. Primer takih grafov so Cayleyjevi

grafi in tako tudi njihova poddružina cirkulantnih grafov, s katerimi se številni matematiki ukvarjajo že vrsto let. Ravno ti grafi so predmet preučevanja tega magistrskega dela. Zanimale nas bodo predvsem simetrije oziroma avtomorfizmi cirkulantnih grafov, ukvarjali pa se bomo tudi z vprašanjem kdaj sta dva cirkulantna grafa izomorfna in kolikšno je število njihovih izomorfnostnih razredov.

Magistrsko delo je razdeljeno na več poglavij. V drugem poglavju so opredeljeni in na primerih razloženi osnovni pojmi teorije grup in grafov, ki so bistveni za razumevanje nadaljnjega besedila. V naslednjem poglavju se bomo omejili zgolj na točkovno tranzitivne grafe praštevilskega reda. Pogledali si bomo kaj lahko povemo o izomorfnosti dveh takšnih grafov in o njihovi grupi avtomorfizmov ter določili število paroma neizomorfnih cirkulantov praštevilskega reda za posamezno praštevilsko vrednost. S sintezo znanj, pridobljenih skozi prva tri poglavja, se bomo v četrtem poglavju posvetili še lastnosti imenovani ločna tranzitivnost. Poiskali bomo vse ločno tranzitivne cirkulante do 30 točk in jih klasificirali. Srečali se bomo tudi s pojmom normalen cirkulant in za celotno družino ločno tranzitivnih grafov določili kdaj so normalni.

2 OSNOVNO O GRUPAH IN GRAFIH

Za kasnejše, nekoliko resnejše raziskovanje, se moramo najprej seznaniti z osnovnimi pojmi, zato si bomo v tem poglavju pogledali najpomembenjše definicije in rezultate iz teorije grup in teorije grafov.

2.1 Teorija grup

Grupa je v matematiki eden od osnovnih pojmov sodobne algebre. Po [21] je ta izraz prvi uporabil francoski matematik Evariste Galois (1811 - 1832). Kot pripoveduje legenda naj bi se Galois, zaradi neuslišane ljubezni, podal v dvoboj in umrl, noč pred tem pa naj bi zapisal vse, kar ve o teoriji grup. Grupe imajo ključno vlogo predvsem pri raziskovanju simetrij drugih abstraktnih in konkretnih struktur, poleg tega so pomembne tudi v fiziki, še posebej v kvantni mehaniki. Definicije in rezultati tega poglavja so povzeti po knjigi [6]. Večina rezultatov je navedenih brez dokazov, vendar si jih zainteresirani bralec lahko ogleda v knjigi [6].

2.1.1 Grupe in podgrupe

Definicija 2.1. Grupa $(G, *)$ je množica G skupaj z binarno operacijo $*$ na G, ki zadošča naslednjim aksiomom:

- Za vse $g_1, g_2, g_3 \in G$ velja $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$. Tej lastnosti operacije $*$ pravimo **asociativnost**.
- Obstaja tak element $e \in G$, da za vsak element $g \in G$ velja $e * g = g * e = g$. Elementu e pravimo **enota** oziroma **identiteta** grupe G.
- Za vsak element $g \in G$ obstaja $g^{-1} \in G$, za katerega velja $g * g^{-1} = g^{-1} * g = e$. Elementu g^{-1} pravimo **inverz** elementa g.

Če za binarno operacijo $*$ velja še, da je komutativna, to je, če za poljubna $g_1, g_2 \in G$ velja $g_1 * g_2 = g_2 * g_1$, pravimo, da je grupa **abelska** oziroma **komutativna**.

Opomba 2.2. V nadaljevanju bomo namesto o grupi $(G, *)$ govorili kar o grupi G in namesto $g_1 * g_2$ pisali kar $g_1 g_2$.

Primer 2.3. Ena izmed grup, ki jo spoznamo že v prvih letih osnovne šole, je množica celih števil skupaj z operacijo seštevanja, $(\mathbb{Z}, +)$. Prav tako so grupe $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$, pri čemer z * označimo multiplikativno grupo vseh obrnjivih elementov. Pravzaprav so vse omenjene grupe abelske. Pari $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$ in $(\mathbb{C}, \cdot)$ niso grupe, saj element 0 nima inverza.

Definicija 2.4. Grupa G je **končna**, če ima pripadajoča množica G končno število elementov. V tem primeru je **moč** oziroma **red grupe** kar število njenih elementov in ga označimo z $|G|$.

Primer 2.5. Do sedaj smo spoznali zgolj grupe neskončnega reda, primer končne grupe pa je grupa $(\mathbb{Z}_n, +)$, kjer je $n \in \mathbb{N}$. To je grupa katere elementi so števila med 0 in $n-1$, torej $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$, pri tem pa seštevamo po modulu n.

Definicija 2.6. Red elementa g grupe G je najmanjše naravno število n, tako da je $g^n = e$. Če tako število ne obstaja, pravimo, da je element g neskončnega reda. Red elementa g označimo z $|g|$.

Opomba 2.7. Kljub temu, da se termin red uporablja tako za same grupe kot za njene elemente, ni razloga za dvoumnost, saj je navadno iz konteksta razvidno, na kaj se nanaša.

Definicija 2.8. Če je podmnožica H grupe G za podedovano operacijo sama zase grupa, potem je H **podgrupa** grupe G. To označimo s $H \leq G$.

Primer 2.9. Grupa $(\mathbb{Z}, +)$ je podgrupa grupe $(\mathbb{R}, +)$, grupa $(\mathbb{Q}^*, \cdot)$ pa ni podgrupa grupe $(\mathbb{R}, +)$, čeprav je $\mathbb{Q}^* \subset \mathbb{R}$. Vsaka grupa G ima vsaj dve podgrupi, to sta **trivialna podgrupa** $\{e\}$ in **neprava podgrupa** G.

Naslednja trditev nam poda kriterij, s katerim lažje določimo ali je dana podmnožica grupe G tudi njena podgrupa.

Trditev 2.10. *Podmnožica H grupe G je za podedovano operacijo $*$ njena podgrupa natanko tedaj, ko je:*

1. *H zaprta za binarno operacijo $*$ grupe G, to je: $\forall\, g_1, g_2 \in H$ velja $g_1 * g_2 \in H$,*
2. *identiteta e grupe G je element H,*
3. *za vse $g \in H$ velja $g^{-1} \in H$.*

Pogosto se zgodi, da dve na videz popolnoma različni grupi z matematičnega vidika predstavljata isto grupo. Pravimo, da sta pripadajoči grupi izomorfni.

Definicija 2.11. Naj bosta $(G, *)$ in $(G', \circ)$ grupi. Grupi G in G' sta **izomorfni**, če obstaja bijektivna preslikava $\rho : G \to G'$, za katero velja $\rho(g_1) \circ \rho(g_2) = \rho(g_1 * g_2)$, za poljubna $g_1, g_2 \in G$. V temu primeru pišemo $G \cong G'$. Preslikavi ρ pravimo **izomorfizem grup** iz G v G'.

2.1.2 Nekatere družine grup

V tem podrazdelku si bomo pogledali dve najpomembnejši družini grup.

Ciklične grupe

Ena izmed najenostavnejših družin grup so ciklične grupe.

Trditev 2.12. *Naj bo G grupa in $g \in G$. Potem je $H = \{g^n \mid n \in \mathbb{Z}\}$ podgrupa grupe G. Pravzaprav je H najmanjša podgrupa grupe G, ki vsebuje g, to pomeni, da vsaka podgrupa, ki vsebuje g, vsebuje celotno podgrupo H.*

Definicija 2.13. Naj bosta G in H kot v trditvi 2.12. Potem podgrupi H pravimo **ciklična podgrupa** grupe G, generirana z elementom g. Elementu g pravimo **generator** te podgrupe, le to pa označimo z $\langle g \rangle$. Če obstaja element g grupe G, za katerega je $\langle g \rangle = G$, pravimo, da je grupa G **ciklična**.

Opomba 2.14. V primeru, ko je $G = \langle g \rangle$, je red elementa g kar red ciklične grupe G, torej $|g| = |G|$.

Definicija 2.15. Naj bo G grupa in M njena neprazna podmnožica. Tedaj je $\langle M \rangle$ **podgrupa grupe G, generirana z M**, ki je definirana kot najmanjša podgrupa grupe G, ki vsebuje podmnožico M.

Opomba 2.16. V primeru, ko je $G = \langle g_1, g_2 \rangle$, lahko vsak element grupe G zapišemo kot produkt elementov g_1, g_2, g_1^{-1} in g_2^{-1}.

Trditev 2.17. *Vsaka ciklična grupa je abelska.*

Grupa $(\mathbb{Z}, +)$ je ciklična grupa generirana z elementoma 1 in -1. Pravzaprav je ta grupa do izomorfizma grup natančno edina neskončna ciklična grupa. Naslednji izrek pa nam natančno določi vse končne ciklične grupe.

Trditev 2.18. *Naj bo G končna ciklična grupa reda n. Potem je G izomorfna grupi $(\mathbb{Z}_n, +)$.*

Dokaz. Naj bo G končna ciklična grupa, generirana z elementom g. Tedaj je seveda tudi element g reda n in tako je $G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\} = \{e, g, g^2, g^3, \ldots, g^{n-1}\}$ očitno izomorfna $\mathbb{Z}_n$, kjer ustrezni izomorfizem ρ iz G v $\mathbb{Z}_n$ definiramo s predpisom $\rho(g^i) = i$. □

Naslednji trditvi govorita o tem, kako izgleda in koliko elementov vsebuje posamezna podgrupa ciklične grupe.

Trditev 2.19. *Vsaka podgrupa ciklične grupe je ciklična.*

Trditev 2.20. *Naj bo $G = \langle g \rangle$ ciklična grupa reda n in naj bo $g^m \in G$ poljuben. Potem je $|\langle g^m \rangle| = \frac{n}{D(n,m)}$.*

Za vsako ciklično grupo znamo določiti tudi natančno število vseh njenih podgrup.

Trditev 2.21. *Naj bo G ciklična grupa reda n. Potem za vsak deljitelj d števila n obstaja natanko ena podgrupa grupe G, ki je reda d.*

Primer 2.22. Poiščimo podgrupe ciklične grupe $\mathbb{Z}_{15}$. Ker je $|\mathbb{Z}_{15}| = 15$, po trditvi 2.21 obstaja natanko po ena podgrupa moči $1, 3, 5$ in 15. Podgrupa moči 1 je trivialna grupa, podgrupa moči 15 pa je kar celotna grupa $\mathbb{Z}_{15}$. Podgrupa H_3 moči 3 je sestavljena iz enote in dveh paroma inverznih elementov reda 3. Edina elementa reda 3 sta 5 in 10, torej je $H_3 = \{0, 5, 10\} = \langle 5 \rangle$. Podgrupa H_5 moči 5 je sestavljena iz nevtralnega elementa in štirih elementov reda 5, torej je $H_5 = \{0, 3, 6, 9, 12\} = \langle 3 \rangle$. S tem smo našli vse podgrupe ciklične grupe $\mathbb{Z}_{15}$.

Permutacijske grupe

Navadno za nek ravninski objekt pravimo, da je simetričen, če obstaja premica, ki objekt razdeli na dva skladna in en drugemu zrcalna dela. Primer takšne simetričnosti je na primer velika tiskana črka A. Poznamo pa tudi druge vrste simetrij. Spomnimo se 5-krake zvezde pri kateri je očitno, da ima več kot le zrcalno simetrijo, saj vsak njen vrtež za 72° ne spremeni njene prvotne slike. V vseh doslej opisanih primerih gre za geometrijsko simetrijo, saj so nas zanimale simetrije nekih konkretnih upodobitev. V matematiki pa nas zanimajo tudi simetrije abstraktnih objektov in v ta namem so nam v pomoč simetrične grupe in njihove podgrupe.

Definicija 2.23. Permutacija neprazne množice A je bijektivna preslikava množice A nase, to je $\varphi : A \to A$. Naj bo S_A množica vseh permutacij množice A in naj bosta $\tau, \sigma \in S_A$ poljubna. Potem lahko na S_A definiramo operacijo kompozitum $\circ$ permutacij τ in σ kot $\tau \circ \sigma : A \xrightarrow{\sigma} A \xrightarrow{\tau} A$, ki je prav tako bijekcija množice A nase in zato permutacija množice A.

Primer 2.24. Naj bo množica A podana kot $A = \{1, 2, 3, 4, 5\}$ in naj bo σ permutacija množice A, ki slika $1 \mapsto 4$, $2 \mapsto 2$, $3 \mapsto 5$, $4 \mapsto 3$, $5 \mapsto 1$. Permutacijo σ v bolj standarni obliki zapišemo kot (1435).

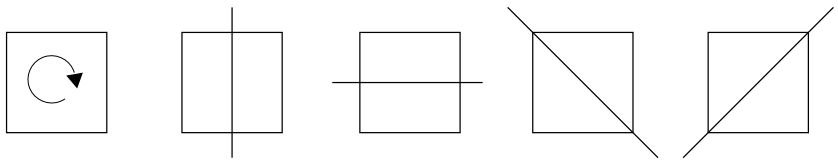
Opomba 2.25. Permutacije komponiramo iz desne proti levi, torej je $(12)(123) = (1)(23) = (23)$.

Trditev 2.26. *Naj bo A neprazna množica in naj bo S_A množica vseh permutacij množice A. Potem je par $(S_A, \circ)$ grupa.*

Definicija 2.27. Naj bo A končna množica $\{1, 2, \ldots, n\}$. Grupo vseh permutacij na množici A imenujemo **simetrična grupa** na n elementih in jo označimo s S_n. Vsako podgrupo simetrične grupe S_n imenujemo **permutacijska grupa** stopnje n.

Spomnimo, da je simetrična grupa S_n moči $n!$, kjer je $n! = n(n-1)(n-2)\ldots(2)(1)$.

Primer 2.28. Grupa $G = \{id, (1234), (1432), (13)(24), (12)(34), (14)(23), (13), (24)\}$ je primer podgrupe simetrične grupe S_4. Če oglišča kvadrata poimenujemo naravno z $1, 2, 3$ in 4 v smeri urinega kazalca, vidimo, da elementi grupe G določajo ravno vse simetrije tega kvadrata. Imamo štiri rotacije, prva je id, to je rotacija za $0°$, potem (1234), to je rotacija za $90°$ v smeri urinega kazalca, in (1432), kar je rotacija za $90°$ v nasprotni smeri urinega kazalca, ter rotacija za $180°$, to je element $(13)(24)$. Poleg tega kvadrat dopušča še štiri zrcaljenja preko osi simetrije in sicer $(12)(34), (14)(23), (13)$ in (24).



Slika 2: Simetrije kvadrata.

Posebne podgrupe simetričnih grup so diedrske grupe. Gre za grupe simetrij pravilnih večkotnikov. Ker ima pravilni večkotnik z n stranicami $2n$ različnih simetrij (n rotacij in n zrcaljenj), ima pripadajoča diedrska grupa natanko $2n$ elementov. Če je število stranic n pravilnega večkotnika liho, potem vsaka izmed n osi simetrije poteka skozi središče stranice in njeno nasprotno oglišče. Če pa je število stranic n sodo, potem $\frac{n}{2}$ osi simetrij poteka skozi središči nasprotnih stranic, ostalih $\frac{n}{2}$ osi simetrij pa skozi nasprotni si oglišči.

Definicija 2.29. Diedrska grupa $D_{2\cdot n}$ je podgrupa simetrične grupe S_n generirana z dvema elementoma ρ in τ, to je $D_{2\cdot n} = \langle \rho, \tau \rangle$, kjer je $n \geq 2$ in $\rho, \tau \in S_n$:

$$\rho : i \mapsto i+1, \text{ za } \forall i \in \{1, 2, \ldots, n-1\} \text{ in } \rho(n) = 1,$$

$$\tau : i \mapsto n-i, \text{ za } \forall i \in \{1, 2, \ldots, n-1\}.$$

Kot smo že omenili, ima $D_{2\cdot n}$ natanko $2n$ elementov in glede na definicijo so to ravno:

$$id, \rho, \rho^2, \ldots \rho^{n-1}, \tau, \tau\rho, \tau\rho^2, \ldots \tau\rho^{n-1}.$$

Torej je vsak element oblike $\tau^i\rho^j$, kje je $i \in \{0, 1\}$ in $j \in \{0, 1, \ldots, n-1\}$. Ker velja $\tau\rho\tau = \rho^{-1}$, v kar se bo bralec zlahka prepričal, je vsak element oblike $\tau\rho^j$ reda 2, saj je $\tau\rho^j\tau\rho^j = \tau\tau\rho^{-j}\rho^j = id$.

Z diedrsko grupo smo se pravzaprav že srečali pri zgledu grupe, ki predstavlja vse simetrije kvadrata. To je grupa z osmimi elementi, ki jo v obliki diedrske grupe zapišemo kot $D_{2\cdot 4} = \{id, \tau, \tau\rho, \tau\rho^2, \tau\rho^3, \rho, \rho^2, \rho^3\}$. Slika 3 prikazuje še primer delovanja diedrske grupe $D_{2\cdot 8}$ na stop znak.

Slika 3: Delovenje elementov diedrske grupe $D_{2\cdot 8}$ na stop znak [20].

2.1.3 Odseki

Definicija 2.30. Naj bo H podgrupa grupe G in $g \in G$. Podmnožica, definirana kot $gH = \{gh \mid h \in H\}$ grupe G, je **levi odsek** grupe G po podgrupi H, ki vsebuje element g. Podmnožica $Hg = \{hg \mid h \in H\}$ grupe G je **desni odsek** grupe G po podgrupi H, ki vsebuje element g.

Primer 2.31. Poiščimo vse leve odseke podgrupe $3\mathbb{Z}$ v grupi $\mathbb{Z}$.

$$0 + 3\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\},$$
$$1 + 3\mathbb{Z} = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\},$$
$$2 + 3\mathbb{Z} = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}.$$

Očitno je, da zgornji trije levi odseki pokrijejo celotno grupo $\mathbb{Z}$, torej tvorijo particijo grupe $\mathbb{Z}$.

Opomba 2.32. Podgrupa H abelske grupe G tvori isto particijo grupe G glede na leve in desne odseke, saj velja $gH = Hg$ za vsak $g \in G$.

Trditev 2.33. *Moč posameznih odsekov grupe G po končni podgrupi H je enaka moči podgrupe H, torej velja $|gH| = |H| = |Hg|$ za vsak $g \in G$.*

Definicija 2.34. Naj bo H podgrupa grupe G. Število različnih levih oziroma desnih odsekov grupe G po podgrupi H imenujemo **indeks** podgrupe H v grupi G in ga označimo z $[G : H]$.

Definicija 2.35. Podgrupa H grupe G je **edinka**, oznaka $H \lhd G$, če za poljuben $g \in G$ velja $gH = Hg$.

Opomba 2.36. Ker so v abelski grupi vsi levi in desni odseki enaki, sledi, da so vse podgrupe abelske grupe edinke.

Izrek, ki sledi, nam pomaga pri iskanju podgrup dane grupe. Izrek je plod slavnega matematika Josepha-Louisa Lagrangea (1736 - 1813), katerega dela zasledimo skoraj na vseh področjih matematike. Kot navaja [22], se je Lagrange namreč ukvarjal tako z algebro, analizo in teorijo števil kot tudi z analitično in nebesno mehaniko. Med njegova pomembna dela sodi knjiga, v kateri je razvil teorijo, ki je danes poznana pod imenom Lagrangeva mehanika. Ta izjemna knjiga slovi tudi po tem, da v njej ni nobenih risb. Lagrange je bil namreč mnenja, da so njegove formule tako nazorne, da skice enostavno niso potrebne.

Izrek 2.37. ***(Lagrangev izrek)*** *Naj bo H podgrupa končne grupe G. Potem red podgrupe H deli red grupe G.*

Posledica 2.38. *Vsaka grupa praštevilske moči je ciklična.*

Dokaz. Naj bo G grupa praštevilske moči p in naj bo g element grupe G, ki ni enak identiteti. Naj bo sedaj $\langle g \rangle$ ciklična podgrupa grupe G, generirana z elementom g. Podgrupa $\langle g \rangle$ vsebuje vsaj dva elementa, g in e. Po Lagrangevem izreku moč podgrupe $\langle g \rangle$ deli moč grupe G. Torej sta edini možnosti $|\langle g \rangle| = 1$, kar ne drži, in $|\langle g \rangle| = p$, torej $\langle g \rangle = G$ in tako je grupa G ciklična. □

V tem razdelku si poglejmo še en pomemben izrek, katerega avtor je francoski matematik Avgustin Louis Cauchy (1789-1857). Glede na vir [4] je Cauchy že kot mladenič postal profesor na Politehnični šoli v Parizu. Njegovo glavno področje raziskovanja je bila sicer analiza in teorija permutacijskih grup, a kljub temu je pisal skoraj o vsem. Bil je tako plodovit pisec, da so uredniki večjih francoskih revij celo postavili omejitev števila člankov, ki jih je lahko objavil. Kot odgovor na to pa je Cauchy prepričal urednika, s katerim sta bila v sorodu, da je začel izdajati revijo, ki je vsebovala samo njegove članke.

Izrek 2.39. ***(Cauchyjev izrek)*** *Naj bo p praštevilo in naj bo G taka končna grupa, da p deli $|G|$. Potem ima G element reda p in posledično tudi podgrupo te moči.*

2.1.4 Delovanje grupe na množici

Do sedaj smo že videli kako lahko grupa na nek način deluje na različne objekte, na primer grupa simetrij kvadrata na ta kvadrat. V tem podrazdelku pa bomo spoznali formalno definicijo delovanja grupe na množici.

Definicija 2.40. Naj bo G grupa in X poljubna množica. **Delovanje grupe G na množici** X je preslikava $* : G \times X \to X$, za katero velja

- $e * x = x$ za vsak $x \in X$,
- $(g_1 g_2) * x = g_1 * (g_2 * x)$ za vse $x \in X$ in vse $g_1, g_2 \in G$.

Opomba 2.41. V nadaljevanju bomo namesto $g * x$ pisali kar gx.

Definicija 2.42. Delovanje grupe G na množici X je **tranzitivno**, če za poljubna $x_1, x_2 \in X$ obstaja tak $g \in G$, da je $gx_1 = x_2$.

Definicija 2.43. (povzeto po [**?**]) Delovanje grupe G na množici X je **k-tranzitivno**, če za poljubni k-terici $(x_1, x_2, \ldots, x_k), (y_1, y_2, \ldots, y_k)$ različnih elementov iz X obstaja tak $g \in G$, da je $gx_i = y_i$, za vse $1 \leq i \leq k$.

Definicija 2.44. Naj grupa G deluje na množici X in naj bo x poljuben element množice X. Množici $G_x = \{g \in G : gx = x\}$ vseh elementov grupe G, ki element x fiksirajo, rečemo **stabilizator** elementa x v grupi G.

Trditev 2.45. *Naj grupa G deluje na množici X. Potem je stabilizator G_x podgrupa grupe G.*

Primer 2.46. Poglejmo si grupo vseh simetrij kvadrata, s katero smo se že srečali, torej $G = \{id, (1234), (1432), (13)(24), (12)(34), (14)(23), (13), (24)\}$, ki deluje na oglišča kvadrata, katera označimo z $1, 2, 3$ in 4. Torej grupa G deluje na množici $X = \{1, 2, 3, 4\}$. Izberimo element $1 \in X$ in poglejmo kateri so tisti elementi iz grupe G, ki element 1 fiksirajo. To sta ravno elementa id in (24). Stabilizator elementa 1 v grupi G je torej $G_1 = \{id, (24)\}$.

Definicija 2.47. Naj grupa G deluje na množici X. Elementa x_1, x_2 sta v **relaciji** $x_1 \sim x_2$, če obstaja tak $g \in G$, da velja $gx_1 = x_2$. Ekvivalenčnim razredom relacije $\sim$, na katere razpade množica X, pravimo **orbite** delovanja grupe G na množici X in jih označimo z $\mathcal{O}_G(x) = \{y \in X; x \sim y\} = \{y \in X, \exists\, g \in G \ni: gx = y\} = \{gx;\, g \in G\}$.

Opomba 2.48. Da je relacija $\sim$ iz zgornje definicije res ekvivalenčna relacija se je lahko prepričati.

Opomba 2.49. Glede na definicijo je delovanje grupe G na množici X tranzitivno natanko tedaj, ko je $\mathcal{O}_G(x) = X$ za nek in posledično vsak $x \in X$.

Primer 2.50. Naj sedaj grupa $H = \{id, (12)(34)\}$ deluje na množici oglišč kvadrata $X = \{1, 2, 3, 4\}$. Množica X razpade na dve orbiti in sicer na $\mathcal{O}_H(1) = \{1, 2\}$ in na $\mathcal{O}_H(3) = \{3, 4\}$.

Nadaljnje pojme in rezultate tega podrazdelka povzemam po [7].

Lema 2.51. *Naj permutacijska grupa G deluje na množici X in naj bo $\mathcal{O}_G(x)$ orbita elementa x pri delovanju grupe G. Če sta $x_1, x_2 \in \mathcal{O}_G(x)$, je podmnožica permutacij iz G, ki preslikajo x_1 v x_2, levi odsek grupe G po podgrupi G_{x_1}. In obratno, za poljuben $g \in G$ vsi elementi levega odseka gG_x, preslikajo x v isto točko, namreč v gx.*

Dokaz. Ker grupa G deluje tranzitivno na množici $\mathcal{O}_G(x)$, vsebuje G tak element $g \in G$, da velja $gx_1 = x_2$. Naj bo sedaj $h \in G$ spet tak, da velja $hx_1 = x_2$. Sledi $hx_1 = gx_1$, oziroma $g^{-1}hx_1 = x_1$. To pomeni, da je $g^{-1}h \in G_{x_1}$ in tako je $h \in gG_{x_1}$. Posledično vsi elementi, ki preslikajo x_1 v x_2 ležijo v istem odseku gG_{x_1}.

Dokažimo še obrat. Dokazati moramo, da vsak element množice gG_x preslika x v isto točko. Vsak element množice gG_x ima obliko gh, kjer je $h \in G_x$. Ker je $(gh)x = g(hx) = gx$, sledi, da vsi elementi množice gG_x preslikajo x v gx. □

Lema 2.52. ***(Lema o orbiti in stabilizatorju)*** *Naj končna permutacijska grupa G deluje na množici X in naj bo $x \in X$ poljuben. Potem velja*

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

Dokaz. Glede na lemo 2.51 vemo, da natanko $|G_x|$ elementov grupe G preslika x v isto točko. Ker elementi grupe G preslikajo x v natanko $|\mathcal{O}_G(x)|$ različnih točk, res velja $|G| = |G_x||\mathcal{O}_G(x)|$. □

Definicija 2.53. Delovanje premutacijske grupe G na množici X je **semiregularno**, če zgolj identiteta fiksira kak element množice X.

Lema o orbiti in stabilizatorju nas pripelje do naslednje trditve.

Trditev 2.54. *Če je delovanje grupe G na množici X semiregularno, potem velja $|\mathcal{O}_G(x)| = |G|$.*

Definicija 2.55. Permutacijska grupa je **regularna**, če je semiregularna in tranzitivna.

Če grupa G deluje tranzitivno na množici X, potem je $\mathcal{O}_G(x) = X$. Če je delovanje grupe G še semiregularno, sledi $|X| = |G|$. Naslednji rezultat je torej na dlani.

Trditev 2.56. *Če grupa G deluje regularno na množici X, potem je $|G| = |X|$.*

2.2 Teorija grafov

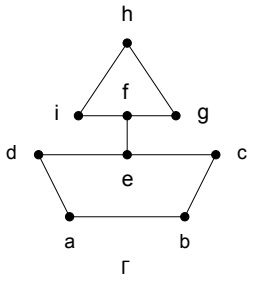
V vsakdanjem življenju naletimo na številne primere, kjer si lahko za predstavitev situacije pomagamo z grafi. Sociologi na primer uporabljajo grafe za ponazoritev družbenih odnosov, kemiki pa za predstavitev modelov molekul. Vsakokrat, ko vidimo zemljevid relacij avtobusov ali letalskih destinacij, gre v resnici za graf. Za preučevanje takšnih in podobnih primerov pa se moramo najprej seznaniti z osnovnimi pojmi, ki jih bomo spoznali v tem razdelku. Večina definicij in rezultatov je povzeta po [7] in [17]. Kadar temu ni tako, je ustrezen vir posebej naveden.

2.2.1 Graf in podgraf

Spoznali smo že, kako si grafe lahko predstavljamo. Sedaj si poglejmo še njihovo formalno definicijo.

Definicija 2.57. Naj bo V neprazna množica in E poljubna družina dvoelementnih podmnožic množice V. Paru $\Gamma = (V, E)$ pravimo **graf** na množici **točk** $V = V(\Gamma)$ in z množico **povezav** $E = E(\Gamma)$.

Grafi so torej abstraktni kombinatorični objekti, katere pa, kadar je to seveda mogoče, lahko predstavimo tako, da za vsako točko grafa narišemo točko v ravnini, povezave pa prikažemo s črtami, ki povezujejo povezane točke.



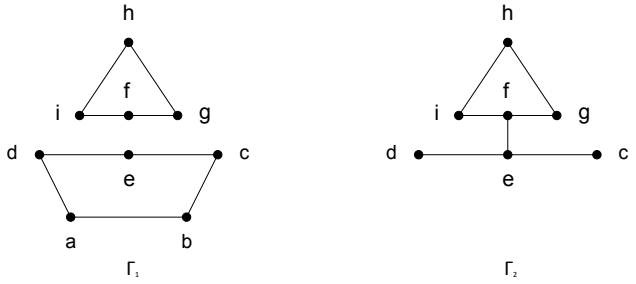
Slika 4: Primer predstavitve grafa.

Definicija 2.58. Elemente množice E običajno namesto z $\{u, v\}$ krajše označimo kar z uv. Kadar je par točk uv element množice E, pravimo da sta točki u in v **sosednji** v grafu Γ in pišemo $u \sim v$. Rečemo tudi, da sta točki u in v **krajišči** povezave uv.

Na sliki 4 je predstavljen graf $\Gamma = (V, E)$, ki ima devet točk in sicer $V(\Gamma) = \{a, b, c, d, e, f, g, h, i\}$, ter deset povezav, torej $E(\Gamma) = \{ab, ad, bc, ce, de, ef, fg, fi, gh, hi\}$.

Opomba 2.59. Naša definicija grafa ne dopušča, da isti par točk povezuje več povezav (vzporedne povezave) in možnosti, da je točka povezana sama s seboj (zanka). Grafom, ki tega ne dopuščajo, pravimo **enostavni grafi**. V nadaljevanju se bomo ukvarjali zgolj z enostavnimi grafi, ki jim bomo na kratko rekli kar grafi.

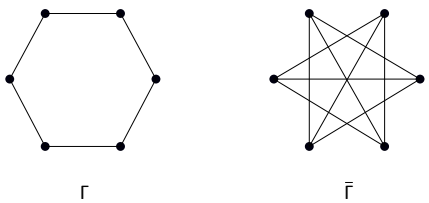
Definicija 2.60. Podgraf grafa Γ je graf Γ_1 za katerega velja $V(\Gamma_1) \subseteq V(\Gamma)$ in $E(\Gamma_1) \subseteq E(\Gamma)$. Kadar velja $V(\Gamma_1) = V(\Gamma)$, pravimo, da je podgraf Γ_1 **vpeti podgraf** grafa Γ. V primeru, ko sta dve točki grafa Γ_1 povezani natanko tedaj, ko sta povezani v grafu Γ, pa podgrafu Γ_1 pravimo **inducirani podgraf** grafa Γ.



Slika 5: Levo vpeti podgraf Γ_1 in desno inducirani podgraf Γ_2 grafa Γ iz slike 4.

Obstaja kar nekaj operacij, ki jih lahko delamo na grafih in tako dobimo nove grafe. Najenostavnejša operacija je **unija** grafov, ki jo dobimo tako, da naredimo graf, katerega komponente so posamezni grafi. Pogosta operacija pa je tudi komplement grafa.

Definicija 2.61. Komplement grafa Γ je graf $\overline{\Gamma}$, ki ga dobimo iz grafa Γ tako, da ohranimo vse točke, dve različni točki pa sta povezani v $\overline{\Gamma}$ natanko tedaj, ko nista povezani v Γ.



Slika 6: Levo graf Γ, desno njegov komplement $\overline{\Gamma}$.

2.2.2 Stopnja točk

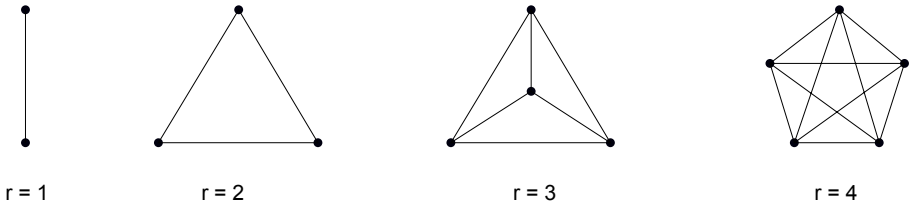
Definicija 2.62. Stopnja točke u v grafu Γ je število povezav, ki imajo točko u za svoje krajišče. Stopnjo točke označimo z $\deg(u)$ ali $d(u)$.

Točkam stopnje 0 pravimo **izolirane točke**, točkam stopnje 1 pa **listi**.

Graf na sliki 4 ima točke a, b, c, d, g, h in i stopnje 2, točki e in f pa sta stopnje 3.

Definicija 2.63. Graf je **regularen**, če imajo vse njegove točke isto stopnjo. Če imajo vse točke grafa stopnjo r, pravimo, da je graf **regularen stopnje r** ali **r-regularen**.

Grafom, ki so 3-regularni, pravimo **kubični grafi**.



Slika 7: Nekaj primerov regularnih grafov.

2.2.3 Sprehodi

Definicija 2.64. Sprehod dolžine k v grafu Γ je zaporedje k povezav grafa Γ oblike:

$$u_0u_1, u_1u_2, u_2u_3, \ldots, u_{k-1}u_k.$$

Ta sprehod krajše zapišemo kot $u_0u_1u_2 \ldots u_k$ in mu rečemo sprehod od u_0 do u_k. Če so vse točke sprehoda različne, potem ta sprehod imenujemo **pot**.

Definicija 2.65. Obhod je sklenjen sprehod, kar pomeni, da se sprehod začne in konča v isti točki, torej

$$u_0u_1, u_1u_2, u_2u_3, \ldots, u_ku_0.$$

Če so v obhodu vse povezave in vse točke, razen prve in zadnje, različne, potem pripadajoči obhod imenujemo **cikel** v grafu.

Na grafu na sliki 4 je $defghifec$ sprehod dolžine 8 od točke d do točke c, vendar to ni pot, saj se točki e in f ponovita dvakrat. Pot od točke d do točke c pa je na primer dec.

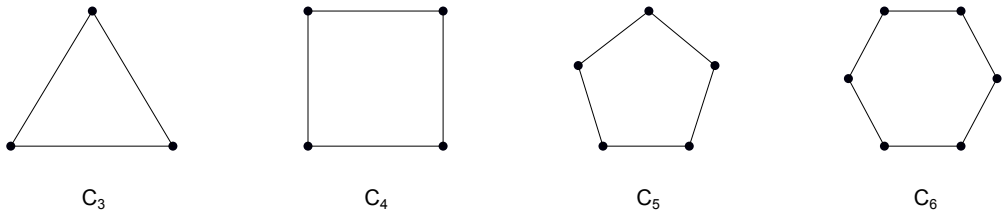
Definicija 2.66. Graf Γ je **povezan**, če obstaja pot med poljubnima dvema točkama grafa Γ. V nasprotnem primeru je graf **nepovezan**.

Spomnimo se sedaj grafov Γ_1 in Γ_2 s slike 5. Graf Γ_1 je nepovezan, medtem ko je graf Γ_2 povezan.

2.2.4 Osnovne družine grafov

V tem razdelku si bomo ogledali nekatere družine grafov, s katerimi se bomo v nadaljevanju večkrat srečali.

Definicija 2.67. Cikel na $n \geq 3$ točkah je graf C_n definiran z množico točk $V(C_n) = \mathbb{Z}_n$ in množico povezav $E(C_n) = \{u(u+1) \mid u \in \mathbb{Z}_n\}$. Graf C_n je 2-regularen z n povezavami.



Slika 8: Cikli C_3, C_4, C_5 in C_6.

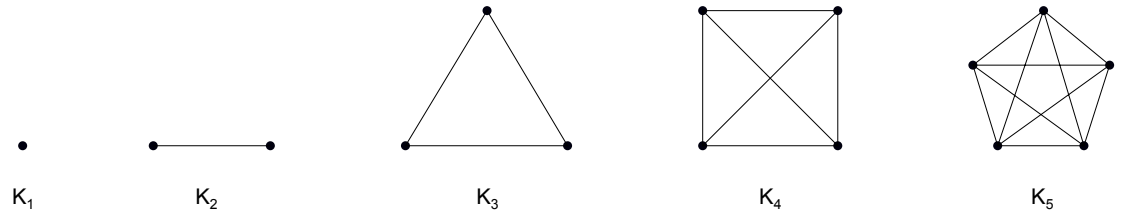
Definicija 2.68. Pot na n točkah je graf P_n, definiran z množico točk $V(P_n) = \mathbb{Z}_n$ in množico povezav $E(P_n) = \{u(u+1) \mid u \in \{0, 1, \ldots, n-2\}\}$. Graf P_n ima $n-1$ povezav in ga lahko dobimo iz cikla C_n z odstranitvijo katerekoli povezave.

Slika 9: Poti P_1, P_2, P_3, P_4 in P_5.

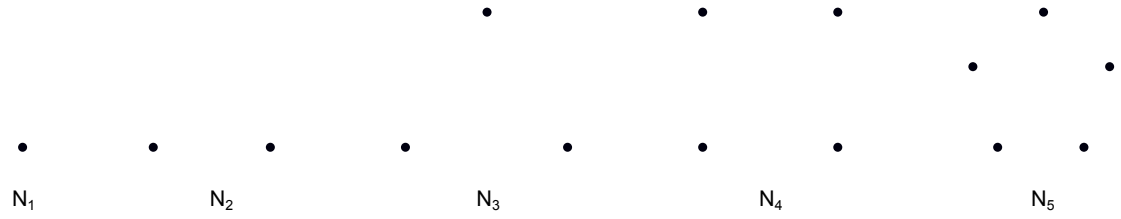
Definicija 2.69. Polni graf na n točkah je graf K_n, v katerem so vse točke paroma povezane, to je $V(K_n) = \mathbb{Z}_n$ in $E(K_n) = \{uv \mid u, v \in \mathbb{Z}_n, u \neq v\}$. Polni graf K_n je $(n-1)$-regularen in ima $\frac{1}{2} \cdot n \cdot (n-1)$ povezav.

Definicija 2.70. Prazni graf je graf brez povezav. Prazni graf na n točkah označimo z N_n in je 0-regularen. N_n je torej ravno komplement grafa K_n.

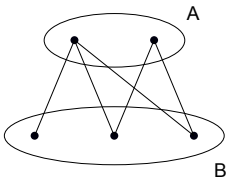
Definicija 2.71. Graf je **dvodelen**, če lahko množico točk $V(\Gamma)$ zapišemo kot disjunktno unijo dveh neprazih podmnožic $A, B \subseteq V(\Gamma)$, tako da za vsako povezavo $uv \in E(\Gamma)$ velja, da je ena od točk u, v vsebovana v množici A, druga pa v množici B. Množici A in B imenujemo **množici dvodelnega razbitja** grafa Γ.



Slika 10: Polni grafi K_1, K_2, K_3, K_4 in K_5.

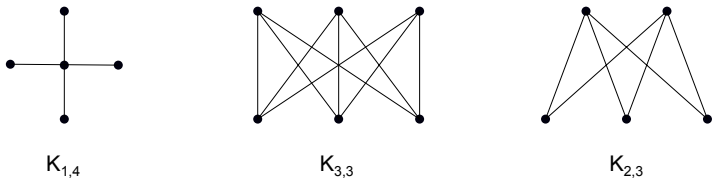


Slika 11: Prazni grafi N_1, N_2, N_3, N_4 in N_5.



Slika 12: Ponazoritev dvodelnega grafa.

Definicija 2.72. Polni dvodelni graf je dvodelni graf, kjer je vsaka točka iz prve množice dvodelnega razbitja povezana z vsemi točkami iz druge množice dvodelnega razbitja. Če je v prvi množici dvodelnega razbitja m točk, v drugi pa n, graf označimo s $K_{m,n}$. Polni dvodelni graf $K_{m,n}$ ima $m + n$ točk in $m \cdot n$ povezav. Grafom $K_{1,n}$ pravimo tudi **zvezde**.

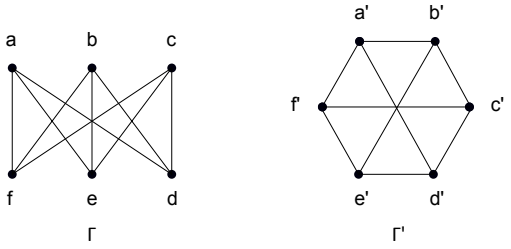


Slika 13: Polni dvodelni grafi $K_{1,4}$, $K_{3,3}$ in $K_{2,3}$.

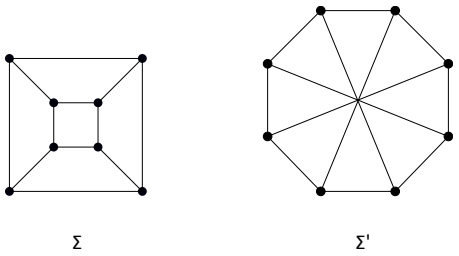
2.2.5 Izomorfizem grafa

Podobno kot pri grupah se tudi pri grafih zgodi, da dva na videz popolnoma različna grafa z matematičnega vidika predstavljata isti graf.

Definicija 2.73. Grafa Γ in Γ' sta **izomorfna**, če obstaja bijektivna preslikava $\varphi : V(\Gamma) \to V(\Gamma')$, za katero velja $uv \in E(\Gamma)$ natanko tedaj, ko je $\varphi(u)\varphi(v) \in E(\Gamma')$. V tem primeru pišemo $\Gamma \cong \Gamma'$. Preslikavi φ pravimo **izomorfizem grafov** iz Γ v Γ'.



Slika 14: Primer izomorfnih grafov.



Slika 15: Primer neizomorfnih grafov.

Grafa na sliki 14 sta izomorfna, saj obstaja bijektivna preslikava $\varphi : V(\Gamma) \to V(\Gamma')$, ki ohranja sosednost, namreč $\varphi(a) = a'$, $\varphi(b) = c'$, $\varphi(c) = e'$, $\varphi(d) = f'$, $\varphi(e) = d'$ in $\varphi(f) = b'$. Pri preprostih grafih, kot sta to grafa s slike 14, iskanje izomorfizma ni tako zahtevna naloga, v primerih, ko grafi niso tako enostavni, pa potrebujemo bolj izdelane metode za preverjanje ali sta dva grafa izomorfna. Zato je v splošnem lažje dokazati, kdaj dva grafa nista izomorfna. Ker izomorfna grafa pravzaprav predstavljata en in isti graf, se morata ujemati v vseh grafovskih lastnostih. Tako morata na primer imeti:

- Enako število točk in povezav,
- točke paroma istih stopenj,
- enako število ciklov določene dolžine,
- enako število povezanih komponent.

Primer neizomorfnih grafov je prikazan na sliki 15. Graf Σ' namreč vsebuje 5-cikel, graf Σ pa ne.

2.2.6 Matrika sosednosti in lastne vrednosti

Matrika sosednosti je eden izmed načinov podajanja grafa. Ta matrika nam namreč pove, koliko točk graf vsebuje in katere točke grafa so med seboj povezane. S tem nam graf natančno definira.

Definicija 2.74. Matrika sosednosti grafa Γ z množico točk $V(\Gamma) = \{0, 1, 2, \ldots, n-1\}$, je $n \times n$ matrika $A(\Gamma) = (a_{ij})$ z vrsticami in stolpci, ki jih indeksirajo točke grafa Γ in za katero velja:

$$a_{ij} = \begin{cases} 1, & \text{če sta točki grafa } i \text{ in } j \text{ povezani} \\ 0, & \text{sicer} \end{cases}$$

Ker imamo opraviti z enostavnimi grafi brez zank, ima matrika sosednosti na diagonali same ničle in je simetrična.

Opomba 2.75. Ker za množico točk grafa vzamemo točke od 0 do $n-1$ je posledično prvi element matrike sosednosti označen kot a_{00} in zato pravimo, da se matrika začne z vrstico oziroma stolpcem 0, zadnja vrstica oziroma stolpec matrike pa je $n-1$.

Definicija 2.76. Karakteristični polinom matrike A je polinom $\phi(A, \lambda) = det(\lambda I - A)$. Z $\phi(\Gamma, \lambda)$ označimo karakteristični polinom matrike sosednosti $A(\Gamma)$ grafa Γ. Število λ je **lastna vrednost** grafa Γ natanko tedaj, ko je λ ničla karakterističnega polinoma $\phi(\Gamma, \lambda)$. Množici lastnih vrednosti grafa Γ skupaj z njihovo kratnostjo pravimo **spekter grafa** in jo označimo s Spect(Γ).

V samo računanje determinant in razcepljanje pripadajočih polinomov se na tem mestu ne bomo spuščali, si pa bralec lahko o tem več prebere v knjigi [15].

Primer 2.77. Poglejmo si matriko sosednosti in spekter grafa C_4 s slike 8.

$$A(C_4) = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

$$\phi(C_4, \lambda) = det \begin{bmatrix} \lambda & -1 & 0 & -1 \\ -1 & \lambda & -1 & 0 \\ 0 & -1 & \lambda & -1 \\ -1 & 0 & -1 & \lambda \end{bmatrix} = \lambda^2(\lambda - 2)(\lambda + 2)$$

Sledi, da je spekter grafa Spect(C_4) = $\{0^2, 2^1, -2^1\}$.

3 TOČKOVNA TRANZITIVNOST

V tem poglavju pričenjamo s študijem simetrij grafov, pri čemer se bomo omejili predvsem na grafe, ki imajo množico točk praštevilske moči. Ugotovili bomo, da so v primeru, ko grupa simetrij na točkah grafa deluje tranzitivno, ti grafi precej simetrični in da jim lahko določimo marsikatero lastnost. Ugotovitve tega poglavja so povzete po člankih [2] in [13].

3.1 Avtomorfizem grafa

S pojmom izomorfizma grafa smo se že srečali v 2. poglavju. Kadar izomorfizem slika dani graf samega vase, izomorfizmu pravimo avtomorfizem grafa.

Definicija 3.1. Permutacijam množice točk danega grafa, ki ohranjajo sosednost, torej izomorfizmom iz danega grafa vase, pravimo **avtomorfizmi**.

Trditev 3.2. *Množica vseh avtomorfizmov grafa* Γ *tvori skupaj z operacijo kompozituma preslikav grupo.*

Dokaz. Naj bosta α, β avtomorfizma grafa Γ, to je $\alpha, \beta : V(\Gamma) \to V(\Gamma)$ sta bijektivni preslikavi, ki ohranjata sosednost. Ker je kompozitum bijektivnih preslikav prav tako bijektivna preslikava, je kompozitum dveh avtomorfizmov, $\alpha \circ \beta : V(\Gamma) \to V(\Gamma)$, bijektivna preslikava. Naj bosta u in v poljubni sosedni točki grafa Γ. Ker je β avtomorfizem grafa Γ, sta sosedni tudi točki $\beta(u)$ in $\beta(v)$, ker pa je tudi α avtomorfizem grafa Γ, sta potem sosedni tudi točki $\alpha(\beta(u)) = (\alpha \circ \beta)(u)$ in $\alpha(\beta(v)) = (\alpha \circ \beta)(v)$. Torej tudi kompozitum $\alpha \circ \beta$ ohranja sosednost v grafu Γ. To pomeni, da je kompozitum dveh avtomorfizmov ponovno avtomorfizem. Ker je avtomorfizem bijekcija, za vsak avtomorfizem α obstaja tudi enolično določen inverz, to je $\alpha^{-1} : V(\Gamma) \to V(\Gamma)$, ki je prav tako bijekcija. Naj bosta u in v poljubni točki in označimo $x = \alpha^{-1}(u)$ in $y = \alpha^{-1}(v)$. Ker je α avtomorfizem, sta x in y sosedni natanko tedaj, ko sta sosedni $\alpha(x) = u$ in $\alpha(y) = v$. Torej sta u in v sosedni natanko tedaj, ko sta sosedni $\alpha^{-1}(u)$ in $\alpha^{-1}(v)$ in tako je tudi α^{-1} avtomorfizem grafa Γ. Seveda je množica avtomorfizmov grafa Γ neprazna, saj vsebuje vsaj identiteto. Od tod sledi, da množica vseh avtomorfizmov

grafa tvori podgrupo simetrične grupe S_n, kjer je $n = |V(\Gamma)|$. Torej je množica vseh avtomorfizmov grafa Γ skupaj z operacijo kompozituma preslikav res grupa. □

Definicija 3.3. Grupo iz zgornje trditve imenujemo **grupa avtomorfizmov** grafa Γ in jo označimo z $\mathrm{Aut}(\Gamma)$.

Spomnimo se grupe vseh simetrij kvadrata, to je $G = \{id, (13), (24), (12)(34), (13)(24), (14)(23), (1234), (1432)\}$, za katero smo že ugotovili, da je pravzaprav diedrska grupa $D_{2\cdot 4}$. Namesto kvadrata lahko govorimo o grafu C_4 in z nekaj razmisleka lahko ugotovimo, da je grupa $D_{2\cdot 4}$ ravno njegova grupa avtomorfizmov. Očitno je, da imajo pravzaprav vsi grafi cikli C_n za grupo avtomorfizmov diedrsko grupo $D_{2\cdot n}$. Prav tako je enostavno določiti grupo avtomorfizmov polnega grafa K_n in praznega grafa N_n. Ker grafa K_n in N_n vsebujeta vse oziroma nobene povezave, grupo avtomorfizmov sestavljajo kar vse permutacije množice točk $V(K_n)$ oziroma $V(N_n)$, kar je ravno permutacijska grupa S_n. To, da imata grafa K_n in N_n isto grupo avtomorfizmov pa ni naključje, saj sta si grafa komplementarna. Ker avtomorfizem grafa ohranja sosednost, namreč pare povezanih točk preslika v pare povezanih točk, pare nepovezanih točk pa v pare nepovezanih točk. Očitno torej velja naslednja trditev.

Trditev 3.4. *Naj bo Γ graf z grupo avtomorfizmov $Aut(\Gamma)$. Potem velja $Aut(\overline{\Gamma}) = Aut(\Gamma)$.*

V splošnem iskanje grupe avtomorfizmov grafa ni enostavna naloga in je običajno ne znamo rešiti kar za celotno obravnavano družino grafov. Zato se pri iskanju grupe avtomorfizmov omejimo na prav posebne skupine grafov. Mi se bomo omejili na tako imenovane točkovno tranzitivne grafe, ki so praštevilskega reda.

3.2 Točkovno tranzitivni grafi

S pojmom tranzitivno delovanje smo se srečali že v drugem poglavju. Prav tako pa smo ugotovili, da je množica vseh avtomorfizmov grafa za operacijo komponiranja preslikav grupa. Kadar ta deluje tranzitivno na množici točk grafa, pravimo, da je graf točkovno tranzitiven. V nadaljevanju bomo razmislili kaj lahko povemo o točkovni tranzitivnosti posameznih družin grafov, predvsem pa nas bo ta lastnost zanimala pri prav posebni družini grafov, ki jo bomo spoznali v tem razdelku in sicer pri Cayleyjevih grafih, predvsem pri posebni poddružini Cayleyevih grafov, imenovanih cirkulanti.

Definicija 3.5. Graf Γ je **točkovno tranzitiven**, če njegova grupa avtomorfizmov deluje tranzitivno na množici točk $V(\Gamma)$, to je, če za vsak par točk $u, v \in V(\Gamma)$ obstaja avtomorfizem φ grafa Γ, za katerega velja $\varphi(u) = v$.

Osnovni pogoj za točkovno tranzitivnost grafa je regularnost grafa, o čemer govori tudi naslednja trditev.

Trditev 3.6. *Vsak točkovno tranzitiven graf je regularen.*

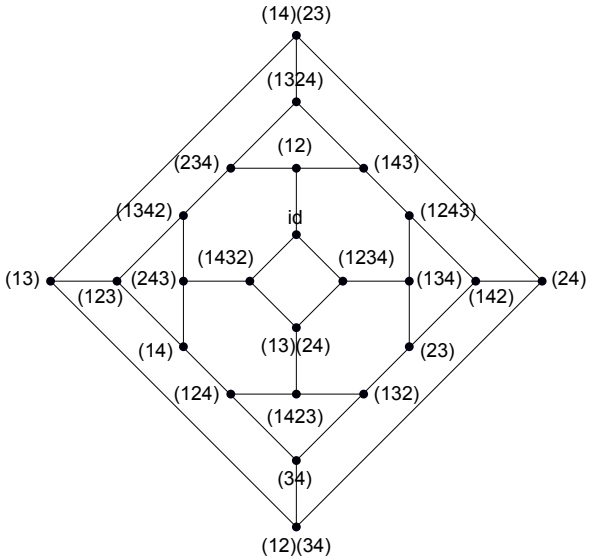
Dokaz. Avtomorfizem grafa Γ ohranja sosednost in zato lahko preslika točko $u \in \Gamma$ v točko $v \in \Gamma$ le, če imata točki isto stopnjo. Ker je graf točkovno tranzitiven, lahko poljubno točko tega grafa z avtomorfizmi preslikamo v poljubno drugo točko, torej imajo vse točke grafa isto stopnjo, kar pomeni, da je graf res regularen. □

Razmislimo sedaj o točkovni tranzitivnosti posameznih družin grafov, ki smo jih spoznali v 2. poglavju. Za začetek ponovno vzemimo graf C_4. Ta je točkovno tranzitiven, saj z uporabo permutacije $(0123)^i$, za $1 \leq i \leq 3$, poljubno točko slej ko prej preslikamo v katerokoli drugo točko. Pravzaprav je enostavno videti, da so vsi grafi C_n točkovno tranzitivni, saj za ustrezni avtomorfizem vedno lahko uporabimo kar permutacijo $(0123\ldots(n-1))^i$, za $1 \leq i \leq n-1$. Prav tako je očitno, da so vsi polni grafi K_n in prazni grafi N_n točkovno tranzitivni, saj je njihova grupa avtomorfizmov celotna simetrična grupa S_n. Graf P_n, razen grafov P_1 in P_2, ni točkovno tranzitiven, saj ni niti regularen. Pri obravnavanju točkovne tranzitivnosti polnih dvodelnih grafov $K_{m,n}$ moramo te najprej razdeliti na dve množici in sicer na polne dvodelne grafe $K_{m,n}$, kjer je $m \neq n$, in na polne dvodelne grafe $K_{m,n}$, kjer je $m = n$, torej na grafe $K_{n,n}$. Grafi $K_{m,n}$, kjer je $m \neq n$, niso regularni in tako glede na trditev 3.6 tudi ne točkovno tranzitivni. Ravno obratno velja za grafe $K_{n,n}$, ki so točkovno tranzitivni. Če točke prve množice dvodelnega razbitja grafa $K_{n,n}$ označimo naravno od 0 do $n-1$, točke druge množice dvodelnega razbitja pa naravno od $0'$ do $(n-1)'$, hitro vidimo, da tudi v tem primeru z uporabo avtomorfizmov $(012\ldots n-1)^i(0'1'2'\ldots(n-1)')^i$, za $1 \leq i \leq n-1$ in $(00')(11')\ldots((n-1)(n-1)')$, slej ko prej poljubno točko preslikamo v katerokoli drugo točko.

Spoznajmo sedaj še eno veliko družino grafov, ki jo bomo preučevali v nadaljevanju. Ta družina je dobila ime po angleškem odvetniku in matematiku Arthurju Cayleyju (1821 - 1895). Kot navaja [18] je Cayley kar 14 let preživel kot odvetnik, a je bil ves ta čas dejaven tudi v matematiki. Še v času, ko je opravljal odvetniški poklic, je objavil okoli 250 matematičnih člankov. Po njem se imenujejo tudi Cayleyjeva števila in Cayleyjevi oktonioni.

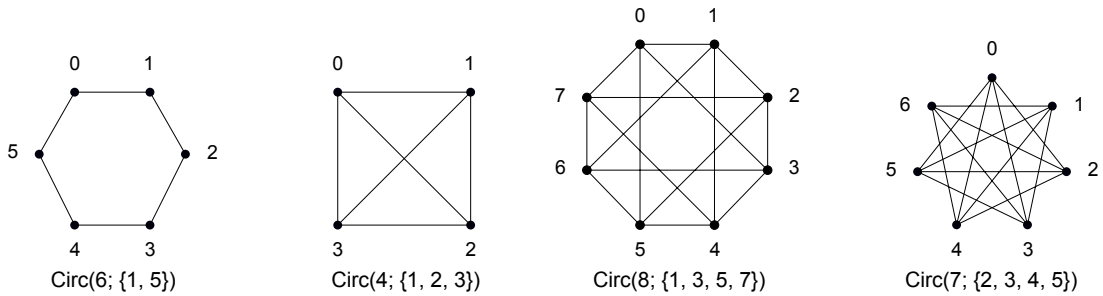
Definicija 3.7. Naj bo G končna grupa in $S \subseteq G \setminus \{e\}$ poljubna podmnožica grupe G, ki je zaprta za inverze. **Cayleyev graf** $\Gamma = Cay(G; S)$ je graf, definiran z množico točk $V(\Gamma) = G$ in množico povezav $E(\Gamma) = \{uv \mid u^{-1}v \in S\}$.

Definicija 3.8. Vzemimo ciklično grupo $\mathbb{Z}_n$. Naj bo $S \subseteq \mathbb{Z}_n \setminus \{0\}$ poljubna podmnožica, zaprta za (aditivne) inverze. Tedaj Cayleyev graf $\mathrm{Cay}(\mathbb{Z}_n; S)$ označimo s $\mathrm{Circ}(n; S)$ in ga imenujemo **cirkulant**. Množici S pravimo **povezavna množica**.



Slika 16: Cayleyev graf Cay(S_4; $\{(12), (1234), (1432)\}$).

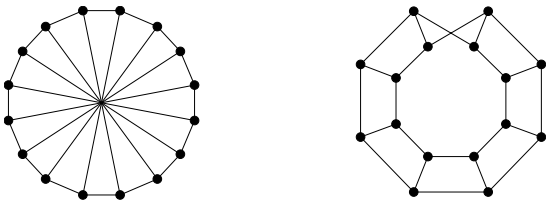
Poglejmo si, če lahko grafe, ki smo jih spoznali doslej, predstavimo kot cirkulante. Cikel C_n je cirkulant reda n s povezavno množico $S = \{1, n-1\}$, $C_n = \mathrm{Circ}(n; \{1, n-1\})$ (primer je graf $\mathrm{Circ}(6; \{1, 5\})$ na sliki 17). Prav tako sta polni graf K_n in prazni graf N_n cirkulanta na n točkah, ki imata povezavni množici oblike $S = \{1, 2, \ldots, n-1\}$ oziroma $S = \emptyset$, torej $K_n = \mathrm{Circ}(n; \{1, 2, \ldots, n-1\})$ in $N_n = \mathrm{Circ}(n; \emptyset)$ (primer je graf $\mathrm{Circ}(4; \{1, 2, 3\})$ na sliki 17). V družino cirkulantnih grafov spadajo tudi polni dvodelni grafi, katerih množici dvodelnega razbitja imata enako moč, torej polni dvodelni grafi oblike $K_{n,n}$. S pravilnim poimenovanjem točk ugotovimo, da so $K_{n,n}$ cirkulantni grafi reda $2n$ s povezavno množico oblike $S = \{1, 3, 5, \ldots, 2n-1\}$, torej $K_{n,n} = \mathrm{Circ}(2n; \{1, 3, 5, \ldots, 2n-1\})$ (primer je graf $\mathrm{Circ}(8; \{1, 3, 5, 7\})$ na sliki 17).



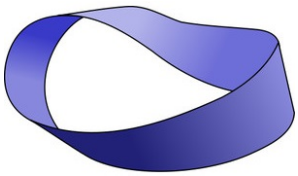
Slika 17: Primeri cirkulantov.

Zgolj kot zanimivost omenimo še Möbiusov graf M_n =Circ($2n; \{1, n, 2n-1\}$), ki je prav tako primer cirkulantnega grafa (primer je prikazan na sliki 18). Möbiusov graf izhaja

iz posebne ploskve imenovane Möbiusov trak (slika 19). Kot navaja [11] ima ta ploskev nenavadne topološke lastnosti, saj ima na primer le eno "stran" in en rob. Möbiusov trak preprosto naredimo tako, da iz lista papirja izrežemo dolg trak. Vzamemo oba konca, enega od njiju zavrtimo za 180°, nato ju zlepimo skupaj. Če gremo s prstom vzdolž traku bomo ugotovili, da prepotujemo ves trak in se ponovno vrnemo na začetno mesto. Če sledimo robu, se nam zgodi enako.



Slika 18: Dve predstavitvi Möbiusovega grafa M_8.



Slika 19: Möbiusov trak [23].

Za vse te osnovne družine grafov je bilo precej lahko videti, da so oziroma niso točkovno tranzitivni. Nekoliko manj trivialen, a še vedno dokaj preprost, je dokaz, da so pravzaprav tudi vsi Cayleyevi grafi, posledično pa tudi cirkulanti, točkovno tranzitivni.

Izrek 3.9. *Vsak Cayleyev graf Cay$(G; S)$ je točkovno tranzitiven.*

Dokaz. Za vsak $g \in G$ je preslikava $\alpha_g : u \mapsto gu$ avtomorfizem grafa Cay$(G; S)$, saj velja

$$u \sim v \;\Leftrightarrow\; \exists s \in S : v = us \;\Leftrightarrow\; \exists s \in S : gv = gus \;\Leftrightarrow\; gu \sim gv.$$

Avtomorfizmi α_g že zadoščajo za točkovno tranzitivnost grafa Cay$(G; S)$, saj za katerikoli točki $u, v \in G$ avtomorfizem $\alpha_{vu^{-1}} \in G$ preslika u v v. □

Da so grafi C_n, K_n, N_n in $K_{n,n}$ točkovno tranzitivni, torej sledi tudi iz dejstva, da so to pravzaprav cirkulantni grafi.

V dokazu izreka 3.9 smo v resnici dokazali več kot trdi sam izrek. Množica vseh preslikav α_g tvori grupo $\tilde{G}$, ki je podgrupa grupe Aut(Cay$(G; S)$). Iz dejstva, da grupa

$\tilde{G}$ deluje tranzitivno na množico točk grafa $\mathrm{Cay}(G;S)$ in, da le element $e \in \tilde{G}$ fiksira kakšno točko, sledi naslednja lema.

Lema 3.10. *Če je $\Gamma = Cay(G;S)$ Cayleyev graf, potem grupa Aut(Cay(G; S)) vsebuje podgrupo, ki deluje regularno na točke grafa Γ in je izomorfna grupi G.*

Velja tudi obrat leme 3.10. Avstrijski matematik Gert Sabidussi (1929 -) je bil s člankom [12] prvi, ki je opozoril na dejstvo, da je v primeru, ko grupa G deluje regularno na točke grafa Γ, graf Γ Cayleyjev graf $Cay(G;S)$ za primerno množico S.

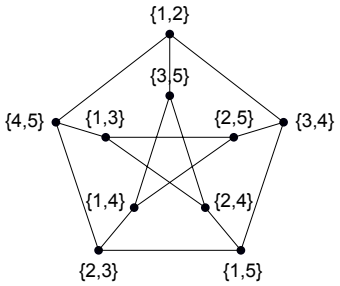
Izrek 3.11. *Če grupa G deluje regularno na točke grafa Γ, potem je Γ izomorfen Cayleyjevemu grafu grupe G za primerno povezavno množico S.*

Dokaz. Naj $\mathrm{Aut}(\Gamma)$ vsebuje regularno podgrupo G in izberimo poljubno točko $u \in V(\Gamma)$. Ker grupa G na $V(\Gamma)$ deluje regularno, za katerokoli točko $v \in V(\Gamma)$ obstaja enolično določen element $g_v \in G$, tako da je $v = g_v u$. Točke grafa Γ lahko brez škode za splošnost preimenujemo tako, da vsako točko v preimenujemo v g_v, kjer je $v = g_v u$. Naj bo S množica vseh točk grafa Γ, ki so povezane s točko e. Ker je graf Γ enostaven, je očitno, da $e \notin S$. Dokazati moramo še, da je množica S zaprta za inverze in da je $\Gamma \cong Cay(G;S)$.

Naj bo $s \in S$ tak, da velja $e \sim s$. Ker je $G \leq Aut(\Gamma)$, je $s^{-1} \in G$, in zato je $s^{-1}e \sim s^{-1}s$, torej $s^{-1} \sim e$, od tod sledi, da je tudi $s^{-1} \in S$, in tako je S res zaprta za inverze. Naj bo sedaj $g_w \sim g_v$. Ker je $g_w \in G$ in s tem tudi $g_w^{-1} \in G$, sledi, da je $e \sim g_w^{-1} g_v$ in zato $g_w^{-1} g_v \in S$. Obratno, naj bo $s \in S$ in naj bo g_w poljubna točka v Γ. Ker je $e \sim s$, je $g_w \sim g_w s$ in tako je Γ res Cayleyjev graf $\mathrm{Cay}(G;S)$. □

V tem razdelku smo spoznali nekatere družine točkovno tranzitivnih grafov, ki pa predstavljajo le majhen delež v celotni družini točkovno tranzitivnih grafov, saj je le ta zelo obširna. Spoznali smo, da so vsi Cayleyevi grafi točkovno tranzitivni, a še zdaleč ne drži obrat te trditve, torej, da je vsak točkovno tranzitiven graf Cayleyjev. Primer takšnega grafa je Petersenov graf $P_{5,2}$, ki je prikazan na sliki 20. Pravzaprav se izkaže, da je to najmanjši točkovno tranzitiven graf, ki ni Cayleyjev. Točke Petersenovega grafa $P_{5,2}$ lahko označimo z 2-podmnožicami $\{i,j\}$ množice $\{1,2,3,4,5\}$, pri čemer sta dve točki povezani, če sta pripadajoči 2-podmnožici disjunktni. Za poljubni točki $\{i,j\}$ in $\{k,l\}$ obstaja premutacija $(ik)(jl) \in S_5$, ki točko $\{i,j\}$ preslika v točko $\{k,l\}$, če $i,j \notin \{k,l\}$. Na ta način lahko slej ko prej poljubno točko preslikamo v katerokoli drugo, kar pomeni, da je Petersenov graf $P_{5,2}$ res točkovno tranzitiven.

Prepričajmo se še, da Petersenov graf ni Cayleyev. Dokažimo to s protislovjem. Torej naj bo Petersenov graf Cayleyev graf $\mathrm{Cay}(G;S)$. Ker ima Petersenov graf 10 točk in



Slika 20: Petersenov graf $P_{5,2}$.

je 3-regularen, sledi, da je $|G| = 10$ in $|S| = 3$. Edini grupi reda 10 sta ciklična grupa $\mathbb{Z}_{10}$ in diedrska grupa $D_{2\cdot 5}$.

1. Naj bo najprej $G \cong \mathbb{Z}_{10}$. Ker je $|S| = 3$ in velja $-S = S$, je $S = \{\pm s, 5\}$ za nek $s \in \{1, 2, 3, 4\}$. Sledi, da je $0 \sim s, s \sim s+5, s+5 \sim 5, 5 \sim 0$ in tako dobimo 4-cikel v tem Cayleyjevem grafu. Najmanjši cikel Petersenovega grafa pa je 5-cikel, kar pomeni, da $G \ncong \mathbb{Z}_{10}$.

2. Naj bo torej $G \cong D_{2\cdot 5}$. Podobno kot prej ugotovimo, da S vsebuje ali en element reda 2 in dva, en drugemu inverzna, elementa reda 5, torej $S = \{\tau\rho^i, \rho^j, \rho^{-j}\}$, za $i \in \{0, 1, 2, 3, 4\}$ in $j \in \{1, 2\}$, ali pa S vsebuje 3 elemente reda 2, to je $S = \{\tau\rho^i, \tau\rho^j, \tau\rho^k\}$, kjer so $i, j, k \in \{0, 1, 2, 3, 4\}$ paroma različni.

   2.1 Če je $S = \{\tau\rho^i, \rho^j, \rho^{-j}\}$, sledi, da je $id \sim \rho^j, \rho^j \sim \tau\rho^{i-j}, \tau\rho^{i-j} \sim \tau\rho^i, \tau\rho^i \sim id$, torej tudi v tem primeru dobimo 4-cikel, kar pomeni, da ta Cayleyjev graf ni Petersenov.

   2.2 Edina možnost, ki še ostane je, da je $S = \{\tau\rho^i, \tau\rho^j, \tau\rho^k\}$. V tem primeru lahko naredimo razbitje elementov iz $D_{2\cdot 5}$ na sledeč način $\{id, \rho, \rho^2, \rho^3, \rho^4\}$ in $\{\tau, \tau\rho, \tau\rho^2, \tau\rho^3, \tau\rho^4\}$. Hitro se lahko prepričamo, da je dobljeni graf dvodelen, vendar Petersenov graf ni dvodelen, saj vsebuje cikel dolžine 5.

Od tod sledi, da tudi $G \ncong D_{2\cdot 5}$, kar pomeni, da Petersenov graf res ni Cayleyev.

Opomba 3.12. Grupa avtomorfizmov grafa Γ lahko deluje tudi 2-tranzitivno na množico točk $V(\Gamma)$. To pomeni, da lahko katerikoli urejen par različnih točk preslikamo v katerikoli drug urejen par različnih točk. To je mogoče zgolj v primeru, ko ima graf ali vse možne povezave ali nobene, torej je graf poln ali prazen. To ugotovitev strnimo v trditev, ki sledi.

Trditev 3.13. *Naj bo Γ graf reda n. Njegova grupa avtomorfizmov $Aut(\Gamma)$ je 2-tranzitivna natanko tedaj, ko je $\Gamma \cong K_n$ ali $\Gamma \cong N_n$.*

3.3 Točkovno tranzitivni grafi praštevilskega reda

V prejšnjem razdelku smo spoznali, da je vsak Cayleyjev graf točkovno tranzitiven in da ne velja, da je vsak točkovno tranzitiven graf Cayleyjev. To dejstvo se spremeni, če množico točk omejimo na praštevilsko moč.

Opomba 3.14. V nadaljevanju nas bo večinoma zanimalo delovanje grupe avtomorfizmov $\mathrm{Aut}(\Gamma)$ grafa Γ na množici točk $V(\Gamma)$. V tem primeru bomo zaradi lažjega poimenovanja orbite $\mathcal{O}_{Aut(\Gamma)}(v)$ označevali zgolj z $\mathcal{O}$.

Izrek 3.15. *Povezan graf $\Gamma = (V, E)$ z množico točk praštevilske moči p je točkovno tranzitiven natanko tedaj, ko je Γ cirkulant.*

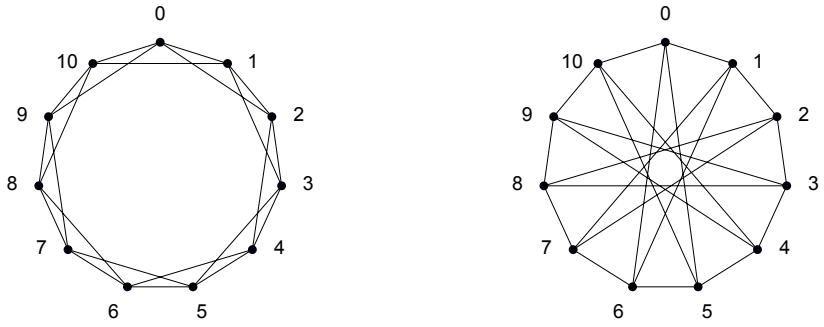
Dokaz.
($\Leftarrow$) Če je graf Γ cirkulant je po izreku 3.9 točkovno tranzitiven.
($\Rightarrow$) Če je graf $\Gamma = (V, E)$ točkovno tranzitiven, grupa avtomorfizmov $\mathrm{Aut}(\Gamma)$ na množici točk $V(\Gamma)$ deluje tranzitivno in zato je dolžina edine orbite $\mathcal{O}$ enaka $|V(\Gamma)| = p$. Po lemi o orbiti in stabilizatorju velja, da je $|\mathrm{Aut}(\Gamma)| = |\mathrm{Aut}(\Gamma)_0||\mathcal{O}| = |\mathrm{Aut}(\Gamma)_0| \cdot p$, torej p deli $|\mathrm{Aut}(\Gamma)|$. Po Cauchyjevem izreku grupa $\mathrm{Aut}(\Gamma)$ premore podgrupo moči p, ki pa je vedno ciklična. Torej obstaja nek $a \in \mathrm{Aut}(\Gamma)$ reda p, to je $\langle a \rangle \cong \mathbb{Z}_p$. Ker a ni identiteta in ker je praštevilskega reda, ima na množici moči p le eno orbito, ki je reda p. Torej grupa $\langle a \rangle$ deluje tranzitivno na množici točk grafa Γ in ker zgolj enota $0 \in \mathbb{Z}_p$ fiksira točke grafa Γ, grupa $\langle a \rangle$ deluje regularno na točke grafa Γ. Od tod sledi, da je graf Γ Cayleyjev graf z množico točk $\mathbb{Z}_p$, torej cirkulant. □

Opomba 3.16. V nadaljevanju bomo točkovno tranzitivnim grafom praštevilskega reda na kratko rekli kar TTP grafi.

3.3.1 Izomorfnost TTP grafov

O izomorfizmu grafov smo nekaj spregovorili že v drugem poglavju, ko smo spoznali osnovne pojme teorije grafov. Ugotavljanje izomorfnosti grafov sicer ni enostavna naloga, a obstajajo družine grafov, kjer je to vprašanje precej preprosto. Sem spadajo tudi TTP grafi.

Poglejmo si dva cirkulanta in sicer $\mathrm{Circ}(11; \{\pm 1, \pm 2\})$ in $\mathrm{Circ}(11; \{\pm 1, \pm 5\})$, prikazana na sliki 21. Sprva se zdi, da gre za dva bistveno različna grafa, a hitro ugotovimo, da sta omenjena grafa izomorfna. Naj bodo $i \in \{0, 1, 2, \ldots, 10\}$ točke grafa $\mathrm{Circ}(11; \{\pm 1, \pm 5\})$. Če te preimenujemo tako, da vsako točko i preslikamo v $2i$, torej $i \mapsto 2i$, dobimo ravno graf $\mathrm{Circ}(11; \{\pm 1, \pm 2\})$.



Slika 21: Izomorfna cirkulanta $\mathrm{Circ}(11;\{\pm 1,\pm 2\})$ in $\mathrm{Circ}(11;\{\pm 1,\pm 5\})$.

O tem ali sta dva grafa izomorfna, veliko pove tudi matrika sosednosti in njene lastne vrednosti. Lahko je videti, da dva grafa, ki imata različne lastne vrednosti, nista izomorfma. Obrat pa v splošnem ne velja. To pomeni, da obstajajo grafi, ki niso izomorfni, vendar imajo iste lastne vrednosti, tak primer grafov je prikazan na sliki 22. V primeru TTP grafov pa bomo ugotovili, da drži tudi obrat.

Slika 22: Neizomorfna grafa z istim spektrom $\{0^3,-2,2\}$.

V skladu s člankom [13] matriko sosednosti cirkulantnih grafov imenujemo kar cirkulantna matrika. V tej matriki je vsaka vrstica po prvi zgolj ciklična rotacija vrstice nad njo. Takšna matrika ima obliko

$$A=\begin{bmatrix} a_{00} & a_{01} & a_{02} & \dots & a_{0(n-1)} \\ a_{0(n-1)} & a_{00} & a_{01} & \dots & a_{0(n-2)} \\ a_{0(n-2)} & a_{0(n-1)} & a_{00} & \dots & a_{0(n-3)} \\ \vdots & \vdots & & \ddots & \vdots \\ a_{01} & a_{02} & a_{03} & \dots & a_{00} \end{bmatrix}.$$

Če točke cirkulanta uredimo kar naravno od 0 do $n-1$, je cirkulant natanko določen že s povezavami, ki gredo iz točke 0 (povezave iz ostalih točk pa dobimo zgolj s ciklično rotacijo povezav iz točke 0). Torej je očitno res, da imajo cirkulanti za matriko sosednosti kar cirkulantno matriko. Podajmo definicijo cirkulantne matrike še formalno.

Definicija 3.17. (povzeto po [19]) Matrika A je **cirkulantna matrika**, če velja $a_{ij} = a_{0(j-i)}$, za vse i, j, pri čemer indekse računamo po modulu n.

Takšne matrike sta v članku [1] preučevala Ablow in Brenner in dokazala, da so lastne vrednosti cirkulantnih matrik natanko

$$\lambda_k = a_{00} + a_{01}\omega^k + \ldots + a_{0n-1}\omega^{k(n-1)},$$

kjer je ω primitivni n-ti koren enote, kar pomeni, da je $\omega^n = 1$, pri čemer je $\omega^i \neq 1$ za $i = \{1, 2, 3, \ldots, n-1\}$.

Izomorfnost grafov in njihove matrike sosednosti povezuje lema, ki sledi. Za razumevanje le te si poglejmo še definicijo prav posebne matrike.

Definicija 3.18. Naj bo $\pi \in S_n$ poljubna permutacija. **Permutacijska matrika** P_π je $n \times n$ matrika, ki jo iz identitete dimenzije $n \times n$ dobimo tako, da stolpce permutiramo v skladu s permutacijo π. Gre torej za matriko, katere element v i-ti vrstici in j-tem stolpcu ima vrednost $\delta_{\pi(i)j}$, kjer je δ Kroneckerjeva funkcija.

Spomnimo, da za Kroneckerjev δ velja

$$\delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}.$$

Tako je na primer za permutacijo $\pi = (032) \in S_4$ ustrezna permutacijska matrika enaka

$$P_{(032)} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Vidimo, da so se stolpci enotske matrike v permutacijski matriki $P_{(032)}$ zamenjali tako, da je stolpec 0 enotske matrike postal stolpec 3 v matriki $P_{(032)}$, stolpec 2 je postal stolpec 3, stolpec 3 je postal 0, stolpec 1 pa se je ohranil.

Premislimo, da oba opisa v zgornji definiciji res sovpadata. Edina enica v i-ti vrstici enotske matrike je v i-tem stolpcu. Če je P_π matrika, ki jo iz identitete dobimo s permutiranjem stolpcev glede na π, potem je edina enica v i-ti vrstici matrike P_π po definiciji v $\pi(i)$-tem stolpcu, torej je $(P_\pi)_{ij} = 1$ natanko tedaj, ko je $j = \pi(i)$. Torej res velja

$$(P_\pi)_{ij} = \begin{cases} 1, & \text{če } \pi(i) = j \\ 0, & \text{sicer} \end{cases}.$$

Primer 3.19. Permutacijske matrike velikosti 3×3 so

$$\underset{P_{id}}{\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}}, \underset{P_{(12)}}{\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}}, \underset{P_{(01)}}{\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}}, \underset{P_{(012)}}{\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}}, \underset{P_{(021)}}{\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}}, \underset{P_{(02)}}{\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}}.$$

Ker očitno velja $P_\pi P_\pi^T = I$, je $P_\pi^{-1} = P_\pi^T$. Iz tega sledi, da je:

$$(P_\pi^{-1})_{ij} = (P_\pi^T)_{ij} = (P_\pi)_{ji} = \begin{cases} 1, & \text{če } \pi(j) = i \\ 0, & \text{sicer} \end{cases}$$

Poglejmo si sedaj lemo, ki povezuje izomorfnost grafov z določeno lastnostjo pripadajočih sosednostnih matrik.

Lema 3.20. *Naj bosta Γ in Γ' izomorfna grafa. Tedaj obstaja taka permutacijska matrika P_π, da velja $A(\Gamma) = P_\pi A(\Gamma') P_\pi^{-1}$.*

Dokaz. Označimo tako točke grafa Γ kot točke grafa Γ' z elementi množice $\mathbb{Z}_n$, kjer je n red obeh grafov. Ker sta grafa Γ in Γ' izomorfna, obstaja nek izomorfizem $\pi : \Gamma \to \Gamma'$, ki ga lahko zapišemo kot permutacijsko matriko P_π. Naj bo $A = (a_{ij})$ matrika sosednosti grafa Γ in $A' = (a'_{ij})$ matrika sosednosti grafa Γ'. Dokažimo, da velja $P_\pi A' P_\pi^{-1} = A$.

Iz zgornjih razmislekov sledi, da je $P_\pi A' P_\pi^{-1} = (a'_{\pi(i)\pi(j)})$. Naprej za poljubna i in j velja, da je

$$a'_{\pi(i)\pi(j)} = 1 \iff$$
$$\pi(i) \sim \pi(j) \text{ v grafu } \Gamma' \iff$$
$$i \sim j \text{ v grafu } \Gamma \iff$$
$$a_{ij} = 1.$$

Torej res velja $P_\pi A' P_\pi^{-1} = A$. □

Nekoliko bolj posplošeno zvezo, kot v lemi 3.20, srečamo tudi v naslednji definiciji.

Definicija 3.21. Dve $n \times n$ matriki A in B sta si podobni, če obstaja taka obrnljiva matrika P, da velja $A = PBP^{-1}$.

Opomba 3.22. Po lemi 3.20 sledi, da sta si matriki sosednosti dveh izomorfnih grafov podobni.

Trditev 3.23. *Če sta si matriki A in B podobni, potem imata enaka karakteristična polinoma.*

Dokaz. S P označimo obrnljivo matriko, za katero je $A = PBP^{-1}$. Od tod z uporabo lastnosti determinante sledi

$$\begin{aligned}\phi(A,\lambda) &= det(\lambda I - A) = det(\lambda I - PBP^{-1}) \\ &= det(P(\lambda I - B)P^{-1}) = detPdet(\lambda I - B)det(P^{-1}) \\ &= det(\lambda I - B) = \phi(B,\lambda).\end{aligned}$$

□

Opomba 3.24. Po trditvi 3.23 imata izomorfna grafa enaka karakteristična polinoma.

Direktno iz trditve 3.23 sledi posledica, katero bomo nekoliko kasneje uporabili pri dokazovanju.

Posledica 3.25. *Če sta matriki A in B podobni, potem imata iste lastne vrednosti, pri čemer imajo posamezne lastne vrednosti v obeh matrikah tudi isto kratnost.*

Opomba 3.26. Glede na posledico 3.25 imata izomorfna grafa iste lastne vrednosti.

Izreka, ki sledita, nam natanko določita, kdaj sta dva cirkulanta praštevilske moči izomorfna.

Izrek 3.27. *Dva TTP grafa $\Gamma = (V, E)$ in $\Gamma' = (V', E')$ sta izomorfna natanko tedaj, ko imata isti spekter.*

Dokaz.
($\Rightarrow$) Če sta grafa Γ in Γ' izomorfna, po posledici 3.25 sledi, da imata njuni pripadajoči matriki sosednosti A in A' iste lastne vrednosti, pri čemer se ujemajo tudi kratnosti posameznih lastnih vrednosti.
($\Leftarrow$) Predpostavimo sedaj, da imata matriki sosednosti A in A' TTP grafov Γ in Γ' iste lastne vrednosti z ujemajočimi se kratnostmi. Radi bi dokazali, da sta grafa Γ in Γ' izomorfna. Po izreku 3.15 sta grafa Γ in Γ' cirkulanta. Torej sta njuni matriki sosednosti pravzaprav cirkulantni matriki z lastnimi vrednostmi $\lambda_k = a_{00} + a_{01}\omega^k + \ldots + a_{0n-1}\omega^{k(n-1)}$ in $\lambda'_k = a'_{00} + a'_{01}\omega^k + \ldots + a'_{0n-1}\omega^{k(n-1)}$ za $0 \leq k < n$. V našem primeru je $n = |V(\Gamma)| = p$, in $a_{ii} = 0$ za $0 \leq i \leq p-1$. V splošnem torej velja

$$\lambda_0 = a_{01} + a_{02} + \ldots + a_{0p-1}$$

$$\lambda_1 = a_{01}\omega + a_{02}\omega^2 + \ldots + a_{0p-1}\omega^{p-1}$$

$$\vdots$$

$$\lambda_{p-1} = a_{01}\omega^{p-1} + a_{02}\omega^{2(p-1)} + \ldots + a_{0p-1}\omega^{(p-1)(p-1)}.$$

Ker je $\lambda_1 = a_{01}\omega + a_{02}\omega^2 + \ldots + a_{0p-1}\omega^{p-1}$ lastna vrednost tako matrike A kot matrike A' obstaja nek k, $1 \leq k \leq p-1$, tako da velja

$$\lambda'_k = a'_{01}\omega^k + a'_{02}\omega^{2k} + \ldots + a_{0p-1}\omega^{k(p-1)} = \lambda_1.$$

Zapišimo lastno vrednost λ_1 kot $\lambda_1 = \sum_{j=1}^{p-1} a_{0j}\omega^j$ in lastno vrednost λ'_k kot $\lambda'_k = \sum_{j=1}^{p-1} a'_{0j}\omega^{jk}$. Ker so, glede na [16], primitivni p-ti koreni enote linearno neodvisni nad poljem racionalnih števil, za koeficiente enačb velja $a'_{0j} = a_{0(jk)}$, kjer indekse računamo po modulu p. Radi bi videli, da je bijektivna preslikava $\varphi : V' \to V$, podana kot $\varphi(j') = jk$, izomorfizem grafov Γ' in Γ. Ker sta grafa Γ in Γ' cirkulanta, je za dokaz, da je φ izomorfizem, dovolj preveriti, da je $(0', j') \in E'$ natanko tedaj, ko je $(0, jk) \in E$. Velja, da je $(0', j') \in E'$ natanko tedaj, ko je $a'_{0j} = 1$, kar pa je po zgornjem res natanko tedaj, ko je $a_{0(jk)} = 1$, torej natanko tedaj, ko je $(0, jk) \in E$. □

Na tem mestu vpeljimo še definicijo ekvivalence povezavnih množic cirkulantov, ki nam bo pomagala pri naslednjih ugotovitvah.

Definicija 3.28. Naj bosta Γ in Γ' cirkulanta reda n, S in S' pa naj bosta njuni pripadajoči povezavni množici. Pravimo, da je povezavna množica S **ekvivalenta** povezavni množici S', oznaka $S \sim S'$, če obstaja tak element $q \in \mathbb{Z}_n^*$, da je $qS = S'$.

Naslednji izrek velja za celotno družino cirkulantnih grafov. Pove nam, da sta cirkulanta, ki imata ekvivalentni povezavni množici, izomorfna. Kot bomo kmalu videli, obrat izreka v splošnem ne velja.

Izrek 3.29. *Naj bosta Γ in Γ' cirkulanta istega reda. Če sta njuni povezavni množici S in S' ekvivalentni, sta cirkulanta Γ in Γ' izomorfna.*

Dokaz. Naj velja $S \sim S'$. Potem obstaja tak element $q \in \mathbb{Z}_n^*$, da je $qS = S'$. Označimo točke cirkulantov z 0 do $p-1$ na običajen način in pokažimo, da je preslikava $\varphi : i \mapsto qi$ izomorfizem grafa Γ v graf Γ'. Preslikava φ je bijekcija iz $\mathbb{Z}_n$ sama vase, saj je $q \in \mathbb{Z}_n^*$ obrnljiv. Naj bo $(u, v) \in E(\Gamma)$. Po definiciji cirkulantnega grafa sledi, da je $v - u \in S$. Preslikava φ preslika točki u in v v qu in qv in res velja $(qu, qv) \in E(\Gamma')$, saj je $qv - qu = q(v - u) \in qS = S'$. Torej res velja $\Gamma \cong \Gamma'$. □

Pokažimo sedaj, da v primeru, ko se omejimo na cirkulante praštevilskega reda, velja tudi obrat izreka 3.29.

Izrek 3.30. *Naj bosta Γ in Γ' cirkulanta istega praštevilskega reda. Cirkulanta Γ in Γ' sta izomorfna natanko tedaj, ko sta pripadajoči povezavni množici S in S' ekvivalentni.*

Dokaz.
($\Leftarrow$) Ta implikacija sledi po izreku 3.29.
($\Rightarrow$) Dokažimo sedaj, da v primeru, ko množici S in S' nista ekvivalentni, tudi grafa Γ in Γ' nista izomorfna. Po izreku 3.27 je dovolj dokazati, da so lastne vrednosti pripadajočih matrik sosednosti $A(\Gamma)$ in $A(\Gamma')$ različne. Naj bo $a_0 = (0, a_{01}, \ldots, a_{0(p-1)})$

prva vrstica matrike $A(\Gamma)$ in naj bo $a'_0 = (0, a'_{01}, \ldots, a'_{0(p-1)})$ prva vrstica matrike $A(\Gamma')$. Naj bo

$$\lambda_1 = a_{01}\omega + a_{02}\omega^2 + \ldots + a_{0p-1}\omega^{p-1}$$

lastna vrednost matrike $A(\Gamma)$. Lastne vrednosti matrike $A(\Gamma')$ so

$$\lambda'_k = a'_{01}\omega^k + a'_{02}\omega^{2k} + \ldots + a'_{0p-1}\omega^{k(p-1)}, \text{ za } 0 \leq k \leq p-1.$$

Ker so ω^k primitivni p-ti koreni enote, ki pa so linearno neodvisni nad poljem racionalnih števil, je, kot v dokazu izreka 3.27, lastna vrednost λ'_k matrike $A(\Gamma')$ enaka lastni vrednosti λ_1 matrike $A(\Gamma)$ samo, če je

$$a'_{0j} = a_{0(jk)} \text{ za vse } 0 \leq j \leq p-1.$$

Ker je $S = \{j \in \mathbb{Z}_n \;\; a_{0j} = 1\}$ in $S' = \{j \in \mathbb{Z}_n \;:\; a'_{0j} = 1\}$ sledi, da je $\lambda'_k = \lambda_1$ natanko tedaj, ko je $S' = kS$. Ker pa smo predpostavili, da S in S' nista ekvivalentni, pomeni da je $\lambda_1 \neq \lambda'_k$ za vsak k. Torej Γ in Γ' res nista izomorfna. □

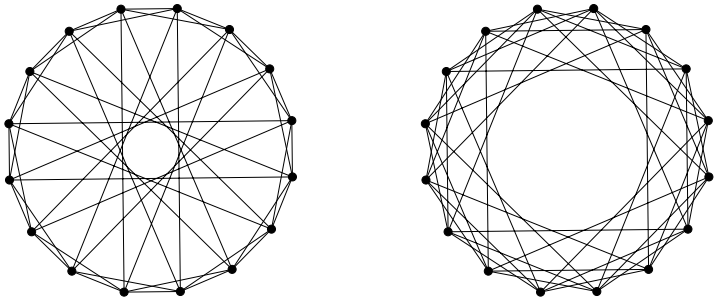
Problem izomorfizma cirkulantov je leta 1967 sprožil madžarski matematik András Ádám, ki je domneval, da izrek 3.30 drži kar za celotno družino cirkulantnih grafov. Dokazali smo, da sta v splošnem dva cirkulanta Γ in Γ', ki imata pripadajoči povezavni množici S in S' ekvivalentni, izomorfna, vendar obrat te trditve ne velja. Na sliki 23 je primer dveh cirkulantov $\mathrm{Circ}(16; \{\pm 1, \pm 2, \pm 7\})$ in $\mathrm{Circ}(16; \{\pm 2, \pm 3, \pm 5\})$, katerih povezavni množici nista ekvivalentni, vendar med njima obstaja izomorfizem $\varphi : \mathbb{Z}_{16} \to \mathbb{Z}_{16}$, ki slika

$$\varphi(i) = \begin{cases} i, & \text{če } i \text{ sod} \\ i+4, & \text{če } i \text{ lih} \end{cases}$$

S tako imenovano Ádámovo domnevo se je več desetletij ukvarjalo mnogo matematikov. Danes vemo, da domneva drži le za cirkulante točno določenih redov. Tako na primer izrek 3.30 velja celo za cirkulante, katerih red ni deljiv s kvadratom nobenega praštevila. Vendar pa je dokaz tega dejstva precej zapleten in presega okvire tega magistrskega dela.

3.3.2 Preštevanje TTP grafov

V prejšnjem razdelku smo ugotovili, da si lahko pri štetju izomorfnostnih razredov TTP grafov pomagamo s štetjem povezavnih množic, ki niso ekvivalentne. S tako imenovanim preštevanjem se je kar nekaj časa ukvarjal tudi Arthur Cayley. Kot pravi [17] je Cayley leta 1875 Britanski zvezi predstavil članek, v katerem je opisal metodo, s katero lahko, vsaj načeloma, določimo število alkanov z danim številom ogljikovih atomov. Cayleyjeve metode pa so bile precej okorne in nepraktične, in skoraj 50 let je



Slika 23: Izomorfna cirkulanta Circ(16; $\{\pm1, \pm2, \pm7\}$) levo in Circ(16; $\{\pm2, \pm3, \pm5\}$) desno.

minilo, preden je prišlo do pomembnih novih dosežkov, ko je madžarski matematik George Pólya (1887 - 1985) podal učinkovit postopek, ki ga lahko uporabimo za naloge preštevanja, pri katerih je potrebno upoštevati kakšne simetrije. Ta pristop je bil še posebno uspešen pri nalogah v zvezi s preštevanjem grafov in molekul. Definicije in rezultati tega poglavja so povzeti po [13] in [14].

Najprej si poglejmo definicijo tako imenovanega cikličnega indeksa, s pomočjo katerega bomo kasneje ugotovili natančno število neizomorfnostnih razredov cirkulantov določenega reda.

Definicija 3.31. Naj grupa G deluje na množici N moči n. Vzemimo poljuben element $g \in G$ in s $k_i(g)$, $i \in \{1, \dots n\}$, označimo število orbit grupe $\langle g \rangle$ dolžine i. Če je $\bar{g}$ permutacija množice N, porojena z delovanjem elementa g, tedaj $k_i(g)$ ustreza številu ciklov dolžine i v cikličnem zapisu permutacije $\bar{g}$. Zato n-terici $(k_1(g), k_2(g), \dots, k_n(g))$ rečemo **ciklična struktura** elementa g. Elementu $g \in G$ s ciklično strukturo $(k_1, k_2, \dots, k_n)$ lahko priredimo element $z_g(x_1, \dots, x_n) = x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$, ki mu pravimo **ciklični indeks permutacije** ali **monom** z_g. Polinomu

$$Z_G(x_1, \dots, x_n) = \frac{1}{|G|} \sum_{g \in G} z_g$$

pa pravimo **ciklični indeks** delovanja grupe G.

Trditev 3.32. *Ciklični indeks, ciklične grupe G reda n, je polinom*

$$Z_G(x_1, \dots, x_n) = \frac{1}{n} \sum_{d|n} \varphi(d)(x_d)^{n/d},$$

kjer je $\varphi(d)$ Eulerjeva φ funkcija, ki nam pove število generatorjev grupe $\mathbb{Z}_d$.

Dokaz. Ciklična grupa G reda n je generirana s permutacijo $(01 \dots n-1)$. Po trditvi 2.21 za vsak deljitelj d števila n obstaja natanko ena pogrupa grupe G, ki je reda d,

ta je po trditvi 2.19 prav tako ciklična in zato generirana z elementom reda d, katerih je ravno $\varphi(d)$. To pomeni, da vsota cikličnega indeksa ciklične grupe teče ravno čez vse deljitelje d števila n. Element reda d ciklične grupe reda n v obliki permutacije zapišemo kot kompozitum n/d disjunktnih ciklov dolžine d. Od tod sledi, da imamo v grupi reda n točno $\varphi(d)$ elementov sestavljenih iz n/d ciklov dolžine d, kar torej k cikličnemu indeksu prispeva ravno $\varphi(d)(x_d)^{n/d}$. □

Naslednji izrek nam poda zvezo med cikličnim indeksom in številom neekvivalentnih barvanj s predpisanim številom objektov dane barve. Pri tem so z izrazom neekvivalentna barvanja mišljena bistveno različna barvanja glede na delovanje pripadajoče grupe.

Izrek 3.33. *(**izrek Redfielda in Pólya**) Naj grupa G deluje na množici N moči n in naj bo $B = \{c_1, \ldots, c_b\}$ poljubna množica moči b. Definirajmo polinom*

$$\mathcal{P}(t_1, \ldots, t_b) = Z_G(\textstyle\sum_{i=1}^{b} t_i, \sum_{i=1}^{b} t_i^2, \ldots, \sum_{i=1}^{b} t_i^n).$$

Tedaj je koeficient v polinomu $\mathcal{P}$ pri monomu $t_1^{\alpha_1} t_2^{\alpha_2} \cdots t_b^{\alpha_b}$ enak številu paroma neekvivalentnih barvanj množice N z barvami iz B, pri katerih je α_i elementov barve c_i za vse $1 \leq i \leq b$.

Če v polinomu $\mathcal{P}(t_1, \ldots, t_b)$ vsak $t_1, \ldots, t_b$ zamenjamo z vrednostjo 1, dobimo spodnjo posledico izreka Redfielda in Pólya. Ta nam poda točno število izomorfnostnih razredov barvanj množice N z b barvami.

Posledica 3.34. *Število barvanj množice N z b barvami, do ekvivalence glede na delovanje grupe G, je enako vrednosti cikličnega indeksa $Z_G(x_1, \ldots, x_n)$ pri $x_1 = \ldots = x_n = b$.*

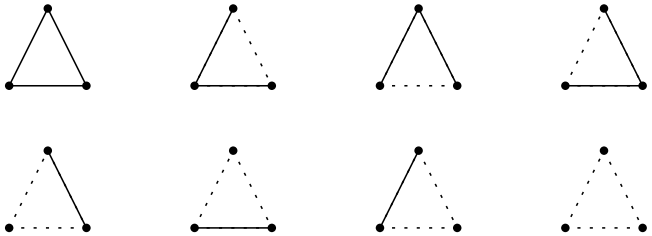
Ugotovitve tega razdelka prenesimo sedaj na našo nalogo o preštevanju neizomorfnostnih razredov cirkulantov praštevilskega reda.

Graf na n točkah dobimo na tak način, da pobarvamo povezave grafa K_n z dvema barvama, recimo črno in belo. Pri tem to barvanje interpretiramo tako, da je dobljeni graf določen s črnimi povezavami. Število vseh barvanj, brez upoštevanja izomorfizmov, je torej enako številu 2^n. Na sliki 24 so prikazana vsa možna barvanja povezav za grafe reda 3. Vendar vidimo, da nam vsa barvanja, ki vsebujejo natanko eno belo povezavo, dajo paroma izomorfne grafe, saj vse dobimo zgolj z rotacijo enega. Prav tako so paroma izomorfni vsi grafi, ki jih dobimo iz barvanj z natanko eno črno povezavo. To pomeni, da z upoštevanjem izomorfizmov, dobimo natanko štiri bistveno različna barvanja polnega grafa K_3, prikazana na sliki 25, in zato lahko govorimo o štirih različnih izomorfnostnih razredih grafov reda 3. Kot smo že ugotovili, število izomorfnostnih razredov dobimo s pomočjo cikličnega indeksa in posledice izreka Redfielda in Pólya. Ker

je tokrat dovolj upoštevati zgolj rotacijske simetrije, moramo določiti ciklični indeks ciklične grupe $\mathbb{Z}_3$. Ta je po trditvi 3.32 enak

$$Z_{\mathbb{Z}_3}(x_1, x_2, x_3) = \frac{1}{3}\sum_{d|3}\varphi(d)(x_d)^{\frac{3}{d}} = \frac{1}{3}\cdot(\varphi(1)\cdot x_1^3 + \varphi(3)\cdot x_3^1) = \frac{1}{3}(x_1^3 + 2x_3^1).$$

Po posledici izreka Redfielda in Pólya moramo v ciklični indeks namesto vrednosti x_1, x_2, x_3 vstaviti število barv, kar je v našem primeru 2. Dobljena vrednost nam pri tem pove točno število izomorfnostnih razredov. Ker je torej $Z_{\mathbb{Z}_3}(2,2,2) = 4$, imamo res ravno štiri različne izomorfnostne razrede grafov reda 3.



Slika 24: Vsa možna barvanja povezav polnega grafa K_3 z dvema barvama.

Slika 25: Vsa možna barvanja povezav grafa K_3 z upoštevanjem izomorfizmov.

Ker nas zanima število izomorfnostnih razredov cirkulantov praštevilskega reda p, je pri tem potrebno upoštevati tudi to, da je povezavna množica S zaprta za inverze, torej za vsak $s \in S$, sledi, da je tudi $-s \in S$. To pomeni, da je graf natanko določen že s $\frac{p-1}{2}$ elementi množice S. Iz slike 25 vidimo, da sta edini možni barvanji povezav cirkulantov reda 3 prvo in zadnje barvanje, kateri predstavljata ravno polni oziroma prazni graf. Pri določanju cikličnega indeksa cirkulantov reda p je torej treba določiti število ekvivalenčnih razredov za podmnožice $S \subset \mathbb{Z}_p^*$, za katere je $S = -S$. V resnici nas torej zanimajo podmnožice kvocientne grupe $\mathbb{Z}_p^*/\{-1\}$ reda $\frac{p-1}{2}$, katero označimo s H_p. Grupo simetrij nam v tem primeru določa kar grupa H_p sama, saj sta dve takšni podmnožici ekvivalentni ravno, ko je $S = hS$, za nek $h \in H_p$. Ciklični indeks cirkulantov reda p je torej enak

$$Z_{H_p}(x_1, \ldots, x_m) = \frac{1}{m}\sum_{d|m}\varphi(d)(x_d)^{m/d}, \text{ kjer je } m = \frac{p-1}{2}.$$

V primeru določanja izomorfnostnih razredov cirkulantov praštevilskega reda p, je torej polinom iz izreka Redfielda in Pólya definiran kot

$$\mathcal{P}(t_1, t_2) = Z_G(\sum_{i=1}^{2} t_i, \sum_{i=1}^{2} t_i^2, \ldots, \sum_{i=1}^{2} t_i^m) = Z_G(t_1 + t_2, t_1^2 + t_2^2, \ldots, t_1^m + t_2^m),$$

pri čemer so s t_1 mišljene bele povezave (ki pomeni, da pripadajoče povezave ni), s t_2 pa črne povezave (oziroma povezava je). Kot pravi izrek, nam koeficient v polinomu $\mathcal{P}$ pri monomu $t_1^{\alpha_1} t_2^{\alpha_2}$ pove število neekvivalenih barvanj množice povezav z dvema barvama, pri čemer nam stopnja α_1 poda polovico števila povezav bele barve, α_2 pa polovico števila povezav črne barve iz posamezne točke danega cirkulanta reda p. To pomeni, da je cirkulant reda p ravno stopnje $2\alpha_2$ oziroma, da povezavna množica S vsebuje $2\alpha_2$ različnih elementov. Torej nam koeficient pri monomu $t_1^{\alpha_1} t_2^{\alpha_2}$ pove število izomorfnostnih razredov cirkulantov reda p, ki so stopnje $2\alpha_2$. Pa si napisano poglejmo kar na konkretnem primeru. Ker je ciklični indeks cirkulantov reda 3 enak $Z_{H_3}(x_1) = x_1$, je polinom iz izreka Redfielda in Pólya enak $\mathcal{P}(t_1, t_2) = Z_{H_3}(t_1 + t_2) = t_1 + t_2 = 1 \cdot t_1^1 \cdot t_2^0 + 1 \cdot t_1^0 \cdot t_2^1$. Člen $1 \cdot t_1^1 \cdot t_2^0$ nam pove, da imamo en izomorfnostni razred cirkulantov le s povezavami bele barve oziroma brez povezav, to je ravno prazen graf N_3, člen $1 \cdot t_1^0 \cdot t_2^1$ pa nam pove, da imamo en izomorfnosti razred cirkulantov le s povezavami črne barve, katerih je iz posamezne točke ravno $2 \cdot 1 = 2$, kar pomeni, da v tem primeru dobimo ravno polni graf K_3. Ker t_1 predstavlja "nepovezave", nas torej v resnici zanima le potenca pri t_2, torej lahko v polinomu $\mathcal{P}(t_1, t_2)$ namesto t_1 pišemo 1, namesto t_2 pa x in tako nam bo koeficient pred x^k podal ravno število izomorfnostnih razredov cirkulantov reda p in stopnje $2k$. Za cirkulante reda 3 tako dobimo, da je $\mathcal{P}(1, x) = 1 + x$ in na tak način lažje razberemo število izomorfnostnih razredov za posamezno stopnjo. Tudi s slike 25 je očitno, da sta možni barvanji povezav cirkulantov reda 3 le prvo in zadnje barvanje in, da pri tem dobimo ravno prazni oziroma polni graf. V splošnem nas torej za cirkulantne grafe reda p zanima polinom

$$\mathcal{P}(1, x) = Z_{H_p}(1 + x, 1 + x^2, \ldots, 1 + x^m).$$

Opomba 3.35. Polinom $\mathcal{P}(1, x)$ imenujemo **rodovna funkcija** za število izomorfnostnih razredov cirkulantov reda p.

Določimo sedaj ciklični indeks, število izomorfnostnih razredov cirkulantov in pripadajočo rodovno funkcijo za prvih nekaj praštevilskih redov p. Ker smo za praštevilsko vrednost 3 že razmislili, bomo zgled začeli s praštevilsko vrednostjo 5. Na koncu podrazdelka bomo podali še tabelo, v kateri je zapisano število izomorfnostnih razredov cirkulantov še za nekaj nadaljnjih praštevilskih redov.

Za cirkulante praštevilskega reda $\boldsymbol{p = 5}$, Circ$(5; S)$, je pripadajoči ciklični indeks enak

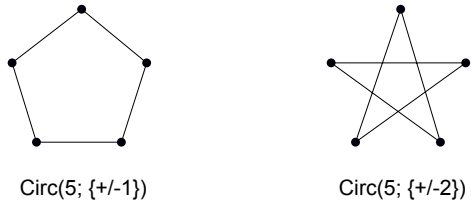
$$Z_{H_5}(x_1, x_2) = \frac{1}{2} \sum_{d|2} \varphi(d)(x_d)^{\frac{2}{d}} = \frac{1}{2} \cdot (\varphi(1) \cdot x_1^2 + \varphi(2) \cdot x_2^1) = \frac{1}{2}(x_1^2 + x_2^1).$$

Ker je $Z_{H_5}(2,2) = \frac{1}{2}(2^2+2) = 3$, imamo tri različne izomorfnostne razrede cirkulantov reda 5. Kako je s posameznimi izomorfnostnimi razredi, nam poda rodovna funkcija

$$Z_{H_5}(1+x, 1+x^2) = \frac{1}{2}((1+x)^2 + (1+x^2)) = 1 + x + x^2.$$

Ta pravi, da imamo en izomorfnostni razred cirkulantov stopnje 0, torej $S = \emptyset$ (to je prazen graf N_5), en izomorfnostni razred cirkulantov stopnje $2 \cdot 1$, torej $|S| = 2$, in en izomorfnostni razred cirkulantov stopnje $2 \cdot 2$, torej $|S| = 4$ (to je polni graf K_5).

Cirkulant reda 5 in stopnje 2 je cikel C_5, ki se lahko predstavi kot $\mathrm{Circ}(5; \{\pm 1\})$ ali kot $\mathrm{Circ}(5; \{\pm 2\})$ (slika 26). Povezavni množici teh dveh cirkulantov sta po izreku 3.30 ekvivalentni in od tod sledi, da sta $\mathrm{Circ}(5; \{\pm 1\})$ in $\mathrm{Circ}(5; \{\pm 2\})$ izomorfna, kar se ujema z dejstvom, da je v rodovni funkciji koeficient pred x enak 1.



Slika 26: Izomorfnostni razred cirkulantov reda 5 in stopnje 2.

Podobno imamo za cirkulante praštevilskega reda $\boldsymbol{p = 7}$, $\mathrm{Circ}(7; S)$, pripadajoči ciklični indeks enak

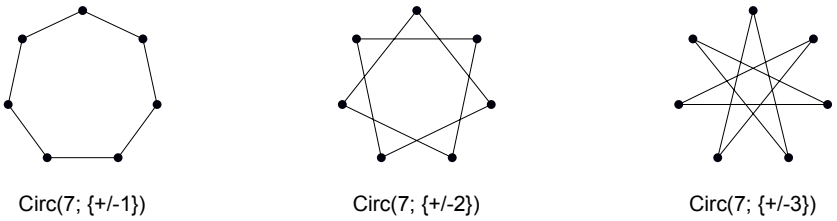
$$Z_{H_7}(x_1, x_2, x_3) = \frac{1}{3}\sum_{d|3} \varphi(d)(x_d)^{\frac{3}{d}} = \frac{1}{3} \cdot (\varphi(1) \cdot x_1^3 + \varphi(3) \cdot x_3^1) = \frac{1}{3}(x_1^3 + 2x_3^1).$$

Ker je $Z_{H_7}(2,2,2) = \frac{1}{3}(2^3+4) = 4$, imamo štiri različne izomorfnostne razrede cirkulantov reda 7. Funkcija

$$Z_{H_7}(1+x, 1+x^2, 1+x^3) = \frac{1}{3}((1+x)^3 + 2(1+x^2)) = 1 + x + x^2 + x^3,$$

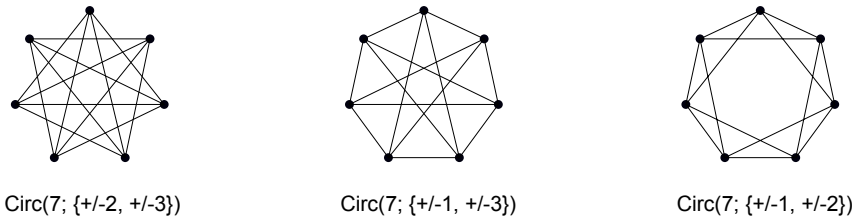
nam pove, da imamo en izomorfnostni razred cirkulantov stopnje 0, torej $S = \emptyset$ (to je prazen graf N_7), en izomorfnostni razred cirkulantov stopnje $2 \cdot 1$, torej $|S| = 2$ (to je cikel C_7, ki se ga lahko predstavi kot $\mathrm{Circ}(7; \{\pm 1\})$ ali $\mathrm{Circ}(7; \{\pm 2\})$ ali $\mathrm{Circ}(7; \{\pm 3\})$, glej sliko 27), en izomorfnostni razred cirkulantov stopnje $2 \cdot 2$, torej $|S| = 4$, in en izomorfnostni razred cirkulantov stopnje $2 \cdot 3$, torej $|S| = 6$ (to je polni graf K_7).

Cirkulant reda 7 in stopnje 4 dobimo tako, da poiščemo vse možne povezavne množice moči 4. Število različnih povezavnih množic moči 4 je $\binom{3}{2} = 3$. Brez škode za splošnost



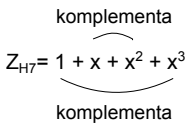
Slika 27: Izomorfnostni razred cirkulantov reda 7 in stopnje 2.

si za začetek izberimo cirkulant Circ$(7; \{\pm 1, \pm 2\})$. Po izreku 3.30 bo ta izomorfen tudi cirkulantoma s povezavno množico $2 \cdot \{\pm 1, \pm 2\} = \{\pm 2, \pm 3\}$ in $3 \cdot \{\pm 1, \pm 2\} = \{\pm 3, \pm 1\}$. S tem dobimo natanko tri različne možnosti cirkulantov reda 7 in stopnje 4, ti pa so paroma izomorfni. Torej imamo do izomorfizma natančno res le en cirkulant reda 7 in stopnje 4 (slika 28).



Slika 28: Izomorfnostni razred cirkulantov reda 7 in stopnje 4.

Preden nadaljujemo razmislimo o posameznih izomorfnostnih razredih cirkulantov praštevilskega reda. Vedno imamo prazen in poln graf, in ta dva grafa sta med seboj komplementarna. Cirkulant s stopnjo točk 2 je vedno cikel (spomnimo, da tu obravnavamo le cirkulante praštevilskega reda), ne glede na izbrano povezavno množico, torej tudi cirkulanti s stopnjo točk 2 spadajo v en izomorfnostni razred. Komplementi cirkulantov s stopnjo točk 2 so cirkulanti s stopnjo točk $p - 3$, kar pomeni, da prav tako ti cirkulanti spadajo v en izomorfnostni razred. Če pogledamo izomorfnostne razrede cirkulantov reda 7, res vidimo, da se komplementno dopolnjujejo (slika 29).



Slika 29: Komplementno dopolnjevanje izomorfnostnih razredov.

Preverimo ugotovitve še za cirkulante reda $\boldsymbol{p = 11}$, Circ$(11; S)$. Tu je pripadajoči

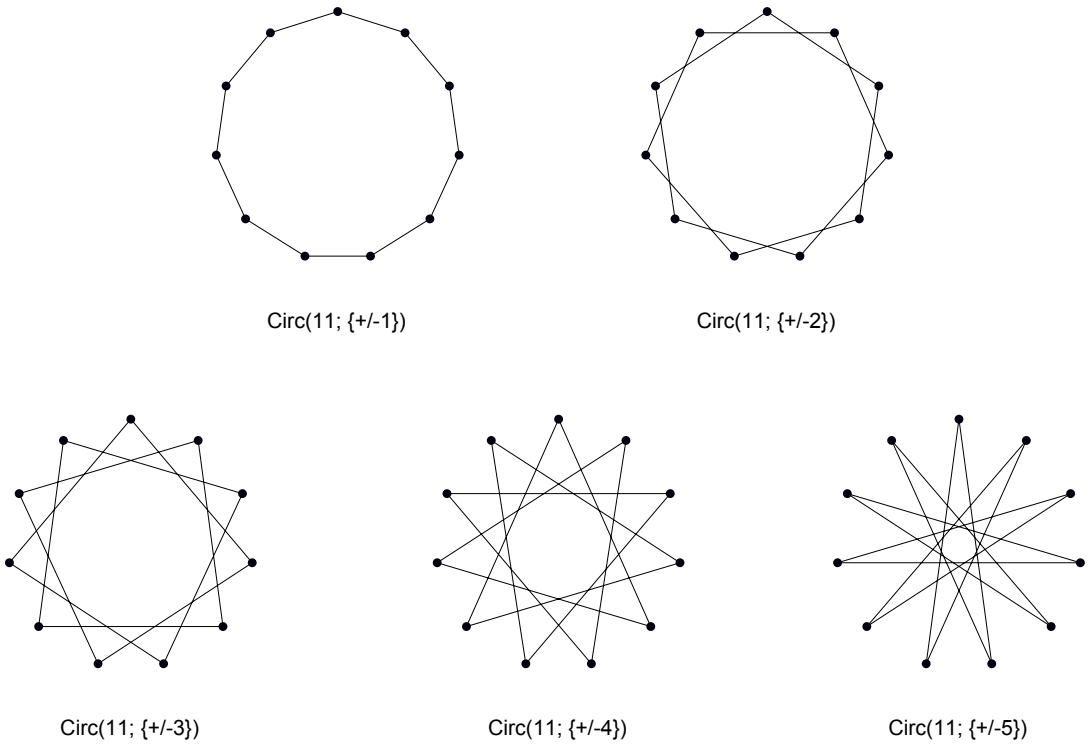
ciklični indeks enak

$$Z_{H_{11}}(x_1,\ldots,x_5)=\frac{1}{5}\sum_{d|5}\varphi(d)(x_d)^{\frac{5}{d}}=\frac{1}{5}\cdot(\varphi(1)\cdot x_1^5+\varphi(5)\cdot x_5^1)=\frac{1}{5}(x_1^5+4x_5^1),$$

torej imamo $Z_{H_{11}}(2,\ldots,2)=\frac{1}{5}(2^5+8)=8$ različnih izomorfnostnih razredov. Funkcija

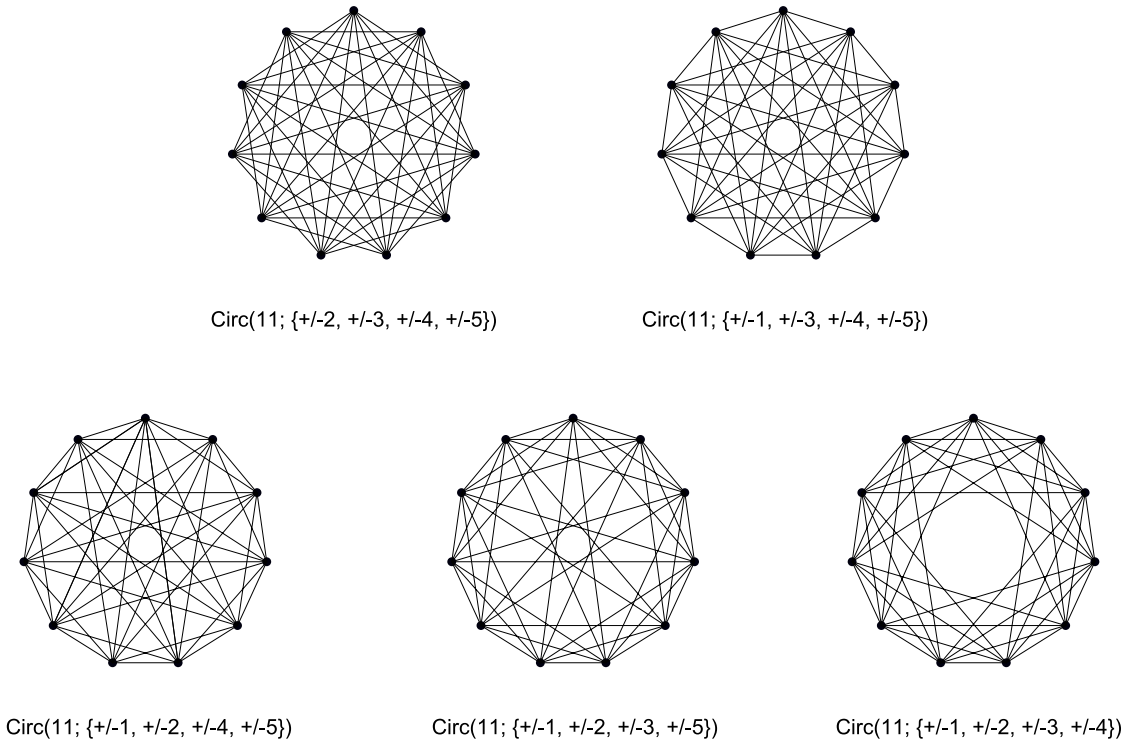
$$Z_{H_{11}}(1+x,1+x^2,\ldots,1+x^5)=\frac{1}{5}((1+x)^5+4(1+x^5))=1+x+2x^2+2x^3+x^4+x^5$$

pravi, da imamo en izomorfnostni razred cirkulantov stopnje 0, torej prazen graf N_{11}, in en izomorfnostni razred cirkulantov stopnje 10, kar je komplement praznega grafa, torej poln graf K_{11}. Kot smo že ugotovili imamo vedno tudi en izomorfnostni razred cirkulantov stopnje 2, to je cikel C_{11}, prikazan na sliki 30, njegov komplement pa je cirkulant stopnje 8. Vsi cirkulanti stopnje 8 prav tako spadajo v en izomorfnostni razred, prikazan na sliki 31.



Slika 30: Izomorfnostni razred cirkulantov reda 11 in stopnje 2.

Za cirkulante stopnje 4 imamo dva izomorfnostna razreda, prav tako za cirkulante stopnje 6, saj so ti cirkulanti zgolj komplementi cirkulantov stopnje 4. Poiščimo torej le dva izomorfnostna razreda cirkulantov stopnje 4. Ti cirkulanti imajo torej povezavno množico moči 4. Število različnih kombinacij za povezavno množico je $\binom{5}{2}=10$.

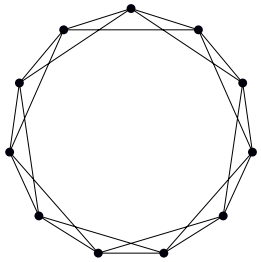


Slika 31: Izomorfnostni razred cirkulantov reda 11 in stopnje 8.

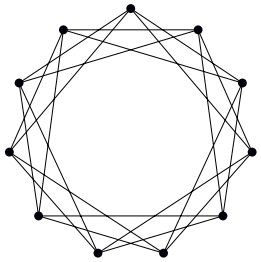
Izberimo najprej cirkulant $\mathrm{Circ}(11;\{\pm1,\pm2\})$. Ta je po izreku 3.30 izomorfen cirkulantom $\mathrm{Circ}(11;\{\pm2,\pm4\})$, $\mathrm{Circ}(11;\{\pm3,\pm5\})$, $\mathrm{Circ}(11;\{\pm3,\pm4\})$ in $\mathrm{Circ}(11;\{\pm1,\pm5\})$. Torej teh pet cirkulantov spada v en izomorfnostni razred. Ostane nam še pet cirkulanov iz drugega izomorfnostnega razreda. Brez škode za splošnost vzemimo poljuben cirkulant, ki ga ni v prvem razredu, na primer $\mathrm{Circ}(11;\{\pm2,\pm3\})$. Ta cirkulant je izomorfen cirkulantom $\mathrm{Circ}(11;\{\pm4,\pm5\})$, $\mathrm{Circ}(11;\{\pm2,\pm5\})$, $\mathrm{Circ}(11;\{\pm1,\pm3\})$ in $\mathrm{Circ}(11;\{\pm1,\pm4\})$ in teh pet cirkulantov spada v drug izomorfnostni razred. Na sliki 32 je prikazan po en cirkulant iz vsakega izomorfnostnega razreda. Zlahka se prepričamo, da cirkulanta na sliki 32 nista izomorfna. Cirkulant $\mathrm{Circ}(11;\{\pm1,\pm2\})$ namreč vsebuje 3-cikel, cirkulant $\mathrm{Circ}(11;\{\pm2,\pm3\})$ pa ne.

S komplementom teh dveh izomorfnostnih razredov dobimo ravno dva izomorfnostna razreda cirkulanov stopnje 6 (slika 33).

Na slikah 34 in 35 imamo predstavljene izomorfnostne razrede cirkulantov reda $\boldsymbol{p = 13}$, za posamezno stopnjo (ustrezna rodovna funkcija je zapisana v spodnji tabeli 1). Poleg prikazanih razredov imamo še razred s polnim grafom K_{13}, razred s praznim grafom N_{13}, razred s cikli C_{13}, ter razred s komplementi ciklov C_{13} in tri razrede s komplementi cirkulantov prikazanih na sliki 34.

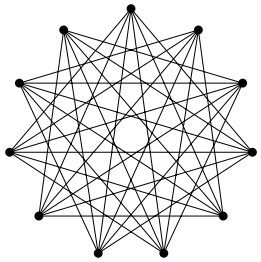


Circ(11; {+/-1, +/-2})=
Circ(11; {+/-2, +/-4})=
Circ(11; {+/-3, +/-5})=
Circ(11; {+/-3, +/-4})=
Circ(11; {+/-1, +/-5})

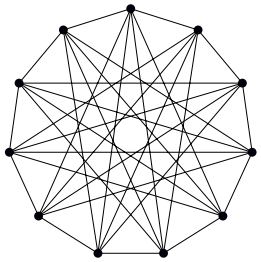


Circ(11; {+/-2, +/-3})=
Circ(11; {+/-4, +/-5})=
Circ(11; {+/-2, +/-5})=
Circ(11; {+/-1, +/-3})=
Circ(11; {+/-1, +/-4})

Slika 32: Dva izomorfnostna razreda cirkulantov reda 11 in stopnje 4.

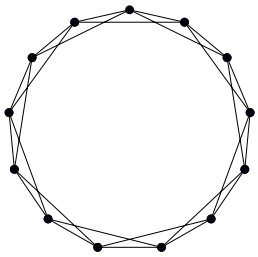


Circ(11; {+/-3, +/-4, +/-5})=
Circ(11; {+/-1, +/-3, +/-5})=
Circ(11; {+/-1, +/-2, +/-4})=
Circ(11; {+/-1, +/-2, +/-5})=
Circ(11; {+/-2, +/-3, +/-4})

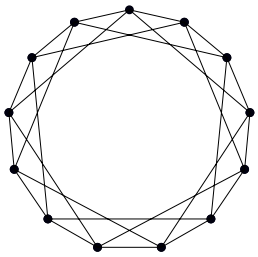


Circ(11; {+/-1, +/-4, +/-5})=
Circ(11; {+/-1, +/-2, +/-3})=
Circ(11; {+/-1, +/-2, +/-4})=
Circ(11; {+/-2, +/-3, +/-5})=
Circ(11; {+/-2, +/-3, +/-5})

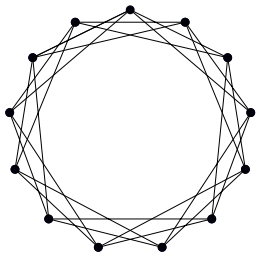
Slika 33: Dva izomorfnostna razreda cirkulantov reda 11 in stopnje 6.



Circ(13; {+/-1,+/-2})
Circ(13; {+/-2,+/-4})
Circ(13; {+/-3,+/-6})
Circ(13; {+/-4,+/-5})
Circ(13; {+/-3,+/-5})
Circ(13; {+/-1,+/-6})

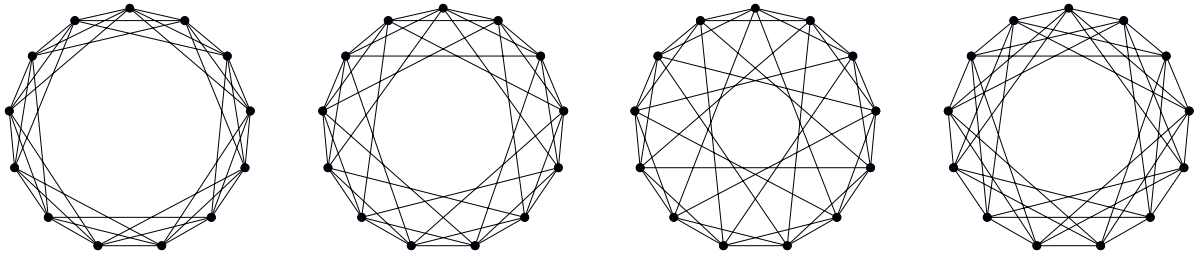


Circ(13; {+/-1,+/-3})
Circ(13; {+/-2,+/-6})
Circ(13; {+/-3,+/-4})
Circ(13; {+/-1,+/-4})
Circ(13; {+/-2,+/-5})
Circ(13; {+/-5,+/-6})



Circ(13; {+/-2,+/-3})
Circ(13; {+/-4,+/-6})
Circ(13; {+/-1,+/-5})

Slika 34: Trije izomorfnostni razredi cirkulantov reda 13 in stopnje 4.



Circ(13; {+/-1,+/-2, +/-3})
Circ(13; {+/-1,+/-4, +/-5})
Circ(13; {+/-1,+/-5, +/-6})
Circ(13; {+/-2,+/-4, +/-6})
Circ(13; {+/-2,+/-3, +/-5})
Circ(13; {+/-3,+/-4, +/-6})

Circ(13; {+/-1,+/-2, +/-4})
Circ(13; {+/-1,+/-2, +/-6})
Circ(13; {+/-1,+/-3, +/-6})
Circ(13; {+/-2,+/-4, +/-5})
Circ(13; {+/-3,+/-4, +/-5})
Circ(13; {+/-3,+/-5, +/-6})

Circ(13; {+/-1,+/-2, +/-5})
Circ(13; {+/-1,+/-3, +/-5})
Circ(13; {+/-1,+/-4, +/-6})
Circ(13; {+/-2,+/-3, +/-4})
Circ(13; {+/-2,+/-3, +/-6})
Circ(13; {+/-4,+/-5, +/-6})

Circ(13; {+/-1,+/-3, +/-4})
Circ(13; {+/-2,+/-5, +/-6})

Slika 35: Štirje izomorfnostni razredi cirkulantov reda 13 in stopnje 6.

Kot smo ugotovili, iskanje izomorfnostnih razredov cirkulantov praštevilskega reda ni zahtevna naloga. Čim najdemo rodovno funkcijo, nam ta pravzaprav pove vse o obliki in številu posameznih izomorfnostnih razredov. Z izrekom 3.30 pa najdemo vse cirkulante v posameznem razredu. V tabeli 1 je povzeto število izomorfnostnih razredov, zapisane pa so tudi pripadajoče rodovne funkcije, za prvih nekaj praštevilskih redov.

Tabela 1: Število izomorfnostnih razredov cirkulantov in pripadajoče rodovne funkcije za prvih nekaj praštevilskih redov.

Praštevilo	**Št. izomorfnostnih razredov**	**Rodovna funkcija**
3	2	$1+x$
5	3	$1+x+x^2$
7	4	$1+x+x^2+x^3$
11	8	$1+x+2x^2+2x^3+x^4+x^5$
13	14	$1+x+3x^2+4x^3+3x^4+x^5+x^6$
17	36	$1+x+4x^2+7x^3+10x^4+7x^5+4x^6+x^7+x^8$
19	60	$1+x+4x^2+10x^3+14x^4+14x^5+10x^6+4x^7+x^8+x^9$
23	188	$1+x+5x^2+15x^3+30x^4+42x^5+42x^6+30x^7+15x^8+5x^9+x^{10}+x^{11}$
29	1182	$1+x+7x^2+26x^3+73x^4+143x^5+217x^6+246x^7+217x^8+143x^9+73x^{10}+26x^{11}+7x^{12}+x^{13}+x^{14}$
31	2192	$1+x+7x^2+31x^3+91x^4+201x^5+335x^6+429x^7+429x^8+335x^9+201x^{10}+91x^{11}+31x^{12}+7x^{13}+x^{14}+x^{15}$

3.3.3 Grupa avtomorfizmov TTP grafov

Poleg tega, da znamo za cirkulante praštevilskega reda natančno poiskati njihove razrede izomorfnosti, znamo natančno določiti tudi njihovo grupo avtomorfizmov. V tem podrazdelku si bomo pogledali pomemben izrek in njegovi dve posledici. Dejstva so povzeta po članku [2].

Definirajmo najprej preslikave, ki jih bomo v nadaljevanju večkrat omenjali.

Naj bosta $a \in \mathbb{Z}_p^*$ in $b \in \mathbb{Z}_p$. Tedaj je preslikava $T_{a,b} : \mathbb{Z}_p \to \mathbb{Z}_p$, definirana s predpisom

$$x \mapsto ax + b, \text{ za vsak } x \in \mathbb{Z}_p.$$

Definicija 3.36. Preslikavi $T_{a,b}$ pravimo **afina linearna transformacija**.

Z AGL(1,p) pa označimo množico vseh afinih linearnih transformacij na $\mathbb{Z}_p$, to je AGL(1,p)=$\{T_{a,b} : a \in \mathbb{Z}_p^*, b \in \mathbb{Z}_p\}$. Pokažimo, da je množica AGL(1,p) grupa za operacijo komponiranja preslikav.

Trditev 3.37. *Množica AGL(1,p) je za operacijo komponiranja preslikav grupa.*

Dokaz. Najprej preverimo zaprtost operacije. Vzemimo dve preslikavi $T_{a,b} : x \mapsto ax+b$ in $T_{c,d} : x \mapsto cx + d$, kjer sta $a, c \in \mathbb{Z}_p^*$ in $b, d \in \mathbb{Z}_p$. Kompozitum preslikav slika po predpisu $(T_{a,b} \circ T_{c,d})(x) = T_{a,b}(T_{c,d}(x)) = a(T_{c,d}(x)) + b = a(cx + d) + b = acx + ad + b$, torej $T_{a,b} \circ T_{c,d} : x \mapsto acx + (ad + b)$. Ker je $ac \in \mathbb{Z}_p^*$ in $ad + b \in \mathbb{Z}_p$, sledi $T_{a,b} \circ T_{c,d} = T_{ac,ad+b} \in$ AGL(1,p), torej je operacija res notranja. Asociativnost sledi iz dejstva, da je komponiranje preslikav asociativna operacija. Identiteta je očitno $T_{1,0}$, kar pa nas po zgornjem računu pripelje do tega, da je inverz $T_{a,b}^{-1} = T_{a^{-1},-a^{-1}b} \in$ AGL(1,p). Torej je AGL(1,p) res grupa. □

Definicija 3.38. Grupi AGL(1,p) pravimo **afina linearna grupa**.

Izrek 3.39. ***(Burnside-ov izrek**, povzeto po [5]) Če grupa G deluje tranzitivno na množici praštevilskega reda p, potem je G 2-tranzitivna ali pa obstaja podgrupa $H \leq \mathbb{Z}_p^*$, da je*

$$G \cong \{T_{a,b} : a \in H, b \in \mathbb{Z}_p\} \leq AGL(1,p).$$

Zaradi obsežnosti in kompleksnosti dokaza Burnside-ovega izreka dokaza tu ne bomo navajali. Vseeno pa preverimo, da je $K = \{T_{a,b} : a \in H < \mathbb{Z}_p^*, b \in \mathbb{Z}_p\}$ res podgrupa grupe AGL(1,p). Po izreku 2.10 je dovolj preveriti sledeče:

1. Zaprtost: $T_{a,b} \circ T_{c,d} = T_{ac,ad+b} \in K$, saj zaradi $a, c \in H$, velja tudi $ac \in H$.
2. Ker je $1 \in H$, je nevtralni element grupe AGL(1,p), torej $T_{1,0}$, vsebovan v K.

3. Ker za vsak $T_{a,b} \in \mathrm{AGL}(1,\mathrm{p})$ velja $T_{a,b}^{-1} = T_{a^{-1},-a^{-1}b}$ in ker za vsak $a \in H$ velja, da je tudi $a^{-1} \in H$, sledi, da za vsak $T_{a,b} \in K$ velja, da je tudi $T_{a,b}^{-1} \in K$.

Izrek 3.40. *Naj bo* Γ *cirkulant reda* p *s povezavno množico* S.

1. *Če je* $S = \emptyset$ *ali* $S = \mathbb{Z}_p^*$, *potem je* $Aut(\Gamma) = S_p$.
2. *Sicer je* $Aut(\Gamma) = \{T_{a,b} : a \in H, b \in \mathbb{Z}_p\}$, *kjer je* H *največja podgrupa grupe* $\mathbb{Z}_p^*$, *tako da je* S *unija odsekov grupe* $\mathbb{Z}_p^*$ *po podgrupi* H.

Dokaz. Če je $S = \emptyset$ ali $S = \mathbb{Z}_p^*$, potem je Γ prazni oziroma polni graf in je grupa avtomorfizmov $\mathrm{Aut}(\Gamma)$ res kar S_p. Naj bo torej $\emptyset \subset S \subset \mathbb{Z}_p^*$. Ker Γ ni polni oziroma prazni graf, grupa avtomorfizmov $\mathrm{Aut}(\Gamma)$ ni 2-tranzitivna in zato je po Burnside-ovem izreku izomorfna grupi $\{T_{a,b} : a \in H, b \in \mathbb{Z}_p\}$ za ustrezno podgrupo $H \leq \mathbb{Z}_p^*$. Po definiciji velja, da je $0 \sim s$ za vse $s \in S$. Stabilizator točke 0 je $\mathrm{Aut}(\Gamma)_0 = \{T_{a,0} : a \in H\}$, kar pomeni, da za vsak $s \in S$ velja, da je $\mathrm{Aut}(\Gamma)_0(s) = Hs \subseteq S$ in tako je S unija odsekov grupe $\mathbb{Z}_p^*$ po podgrupi H, torej $S = \bigcup_{s \in S} Hs$. Naj bo sedaj $K \leq \mathbb{Z}_p^*$ poljubna taka podgrupa, da velja $S = \bigcup_{s \in S} Ks$. Radi bi dokazali, da je za vsak $k \in K$ res $T_{k,0} \in \mathrm{Aut}(\Gamma)$. Ker je $S = \bigcup_{s \in S} Ks$ in ker je $k \in K$, sledi, da je $ks \in S$ za vse $s \in S$. Ker je $x \sim x + s$ $\forall s \in S$ sledi, da je tudi $kx \sim kx + ks$, torej je res $T_{k,0} \in \mathrm{Aut}(\Gamma)$. Od tod sledi, da je $K \leq H$ in izrek je dokazan. □

Posledica 3.41. *Naj bo* Γ *cirkulant reda* p *s povezavno množico* S. *Če je* $D(p-1, |S|) = 2$, *potem je* $Aut(\Gamma)$ *diedrska grupa* $D_{2\cdot p}$ *reda* $2p$.

Dokaz. Ker velja $D(p-1, |S|) = 2$ mora biti $\emptyset \subset S \subset \mathbb{Z}_p^*$ (razen v primeru, ko je $p = 3$ in $S = \{\pm 1\}$, takrat je $\mathrm{Aut}(\Gamma) = S_3 = D_{2\cdot 3}$). Po izreku 3.40 sledi, da je $\mathrm{Aut}(\Gamma) = \{T_{a,b} : a \in H, b \in \mathbb{Z}_p\}$, kjer je H največja podgrupa grupe $\mathbb{Z}_p^*$, tako da je S unija odsekov po H. Ker je $D(p-1, |S|) = 2$ in ker je S unija odsekov po H, pomeni, da je $|H| = 2$. Podgrupa reda 2 grupe $\mathbb{Z}_p^*$ je $H = \{1, -1\}$ in od tod sledi, da je $\mathrm{Aut}(\Gamma) = \{T_{a,b} : a \in \{1, -1\}, b \in \mathbb{Z}_p\}$. Očitno gre v tem primeru ravno za diedrsko grupo $D_{2\cdot p}$, pri čemer elementi oblike $T_{1,b}$ predstavljajo rotacije, elementi $T_{-1,b}$ pa zrcaljenja. □

Primer 3.42. Naj bo $\Gamma = Circ(13; \{\pm 1, \pm 5\})$. Ker velja $D(12, 4) = 4$, ne moremo uporabiti posledice 3.41, ampak moramo po izreku 3.40 poiskati tako največjo podgrupo H grupe $\mathbb{Z}_{13}^*$, da lahko povezavno množico zapišemo kot unijo odsekov po podgrupi H. Ker je grupa $\mathbb{Z}_{13}^* = \langle 2 \rangle$ ciklična in ker je $|\mathbb{Z}_{13}^*| = 12$, po trditvi 2.21 obstaja natanko po ena podgrupa vsakega izmed redov $1, 2, 3, 4, 6$ in 12. Ker je $|S| = 4$ so edine možnosti moči podgrupe H 2 ali 4. Podgrupa reda 2 je $\{1, 12\}$, podgrupa reda 4 je $\{1, 5, 8, 12\}$. Vidimo, da se množico S da zapisati kar kot podgrupo reda 4. Torej je naša iskana podgrupa H enaka $\{1, 5, 8, 12\}$, grupa avtomorfizmov pa je enaka $\mathrm{Aut}(\Gamma) = \{T_{a,b} : a \in \{1, 5, 8, 12\}, b \in \mathbb{Z}_{13}\}$.

Primer 3.43. Naj bo sedaj $\Gamma = Circ(13; \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5\}$. Ker je $D(12, 10) = 2$, sledi, da je grupa avtomorfizmov tega cirkulanta kar diedrska grupa $D_{2\cdot 13}$.

Določimo sedaj grupe avtomorfizmov cirkulantov majhnega praštevilskega reda za vsak izomorfnostni razred. Ker imajo vsi izomorfni grafi isto grupo avtomorfizmov, bomo za vsak razred vzeli po enega predstavnika. Ker pa ima po trditvi 3.4 komplement grafa isto grupo avtomorfizmov kot dani graf, je dovolj pogledati le grafe stopnje največ $\frac{p-1}{2}$.

Za praštevilsko vrednost $p = 3$ obstajata zgolj prazni in polni graf in oba imata za grupo avtomorfizmov kar simetrično grupo S_3. V nadaljevanju bomo spustili primere, kjer je $|S| = 0$ ali $|S| = p - 1$, saj je grupa avtomorfizmov vedno S_p.

Pri $p = 5$ je za $|S| = 2$ po posledici 3.41 grupa avtomorfizmov $D_{2\cdot 5}$ (kar je sicer precej očitno, saj gre za cikel C_5). Prav tako bomo v nadaljevanju spustili primere, kjer je $|S| = 2$ oziroma $|S| = p - 3$ (cirkulanta s povezavno množico 2 in $p - 3$ sta med seboj komplementarna), saj je v tem primeru grupa avtomorfizmov vedno $D_{2\cdot p}$.

Za praštevilsko vrednost $p = 7$ imamo zgolj primere, ki smo jih navedli zgoraj.

Za $p = 11$ je v primeru, ko je $|S| = 4$, oziroma za komplemente pri $|S| = 6$, grupa avtomorfizmov, zaradi posledice 3.41, enaka $D_{2\cdot 11}$.

Na nekoliko bolj zanimive primere prvič naletimo pri praštevilski vrednosti $p = 13$. Pri $|S| = 4$ je $D(12, 4) = 4$ in ne moremo kar privzeti, da je grupa avtomorfizmov diedrska grupa. Kot smo pokazali v prejšnjem podrazdelku, imamo v tem primeru tri izomorfnostne razrede cirkulantov. Iz vsakega od razredov vzemimo po enega predstavnika in preverimo kakšna je grupa avtomorfizmov. Glede na to, da smo v zgornjem primeru že določili vse podgrupe grupe $\mathbb{Z}_{13}^*$, po izreku 3.39 sledi, da je $Aut(Circ(13; \{\pm 1, \pm 2\})) = Aut(Circ(13; \{\pm 1, \pm 3\})) = \{T_{a,b} : a \in \{1, 12\}, b \in \mathbb{Z}_{13}\} = D_{2\cdot 13}$ in $Aut(Circ(13; \{\pm 1, \pm 5\})) = \{T_{a,b} : a \in \{1, 5, 8, 12\}, b \in \mathbb{Z}_{13}\}$. V primeru, ko je $|S| = 8$, gre zgolj za komplemente grafov z $|S| = 4$, zato imajo isto grupo avtomorfizmov. Preverimo še grupo avtomorfizmov cirkulantov s povezavno množico moči 6. Ker imamo v tem primeru 4 izomorfnostne razrede, ponovno iz vsakega razreda vzemimo zgolj po enega predstavnika in dobimo, da je $Aut(Circ(13; \{\pm 1, \pm 2, \pm 3\})) = Aut(Circ(13; \{\pm 1, \pm 2, \pm 4\})) = Aut(Circ(13; \{\pm 1, \pm 2, \pm 5\})) = \{T_{a,b} : a \in \{1, 12\}, b \in \mathbb{Z}_{13}\} = D_{2\cdot 13}$ in $Aut(Circ(13; \{\pm 1, \pm 3, \pm 4\})) = \{T_{a,b} : a \in \{1, 3, 4, 9, 10, 12\}, b \in \mathbb{Z}_{13}\}$.

V tem poglavju smo se natančneje spoznali s cirkulanti praštevilskega reda. Ugotovili smo kdaj sta dva taka grafa izomorfna in kakšna je njihova grupa avtomorfizmov. Prav

tako smo dokazali, da so vsi cirkulanti točkovno tranzitivni. V naslednjem poglavju se bomo posvetili še vprašanju tako imenovane ločne tranzitivnosti cirkulantov.

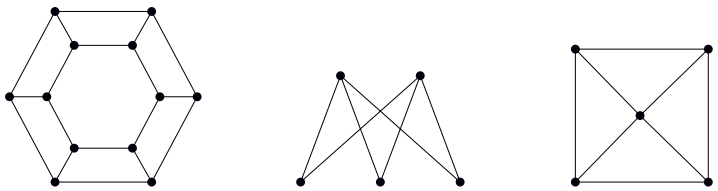
4 LOČNA IN POVEZAVNA TRANZITIVNOST

V prejšnjem poglavju smo se srečali s točkovno tranzitivnostjo. Spoznali smo, da je graf točkovno tranzitiven, če grupa avtomorfizmov deluje tranzitivno na množici točk grafa. Množica točk grafa pa ni edini objekt na katerem lahko opazujemo delovanje grupe avtomorfizmov. Le ta lahko deluje tudi na množici povezav in na množici lokov, pri čemer lok predstavlja urejeni par povezanih točk. Kadar je katero od teh dveh delovanj grupe avtomorfizmov tranzitivno pravimo, da je graf povezavno oziroma ločno tranzitiven. Vprašanje tovrstne tranzitivnosti pri cirkulantnih grafih bo glavna tema tega poglavja. Definicije in rezultati tega poglavja so povzeti po [7], zadnji podrazdelek pa po članku [9].

4.1 Povezavno tranzitivni grafi

Podajmo najprej formalno definicijo povezavne tranzitivnosti.

Definicija 4.1. Graf Γ je **povezavno tranzitiven**, če njegova grupa avtomorfizmov deluje tranzitivno na povezave grafa $E(\Gamma)$. To pomeni, da za katerikoli dve povezavi $e_1, e_2 \in E(\Gamma)$ grafa Γ obstaja avtomorfizem grafa Γ, ki preslika e_1 v e_2.



Slika 36: Primeri različnih vrst tranzitivnosti.

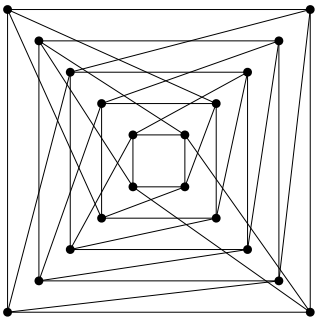
Za cikle C_n smo že ugotovili, da so točkovno tranzitivni, zlahka pa se tudi prepričamo, da so povezavno tranzitivni, saj z avtomorfizmom $(01 \dots (n-1))$ poljubno povezavo slej, ko prej preslikamo v poljubno drugo povezavo. Sicer pa v splošnem ne drži, da so kar vsi točkovno tranzitivni grafi tudi povezavno tranzitivni. Graf je namreč lahko

le točkovno tranzitiven ali le povezavno tranzitiven, lahko je oboje ali pa ni ne eno ne drugo.

Na sliki 36 imamo primere treh grafov z različnimi vrstami tranzitivnosti.

Prvi graf je točkovno tranzitiven. Če točke, ki ležijo na zunanjem ciklu grafa, naravno označimo od 0 do 5, točke, ki ležijo na notranjem ciklu grafa, pa naravno od $0'$ do $5'$, vidimo, da lahko z avtomorfizmoma $(012345)^i(0'1'2'3'4'5')^i$, za $1 \leq i \leq 5$, in $(00')(11')(22')(33')(44')(55')$, slej, ko prej poljubno točko preslikamo v katerokoli drugo točko. Omenjeni graf pa ni povezavno tranzitiven, saj zunanja in notranja povezava 6-cikla ležita na enem 4-ciklu, prečna povezava pa na dveh 4-ciklih. To pomeni, da ne moremo zamenjati zunanje oziroma notranje povezave s prečno.

Drugi graf je primer grafa, ki ni točkovno tranzitiven, je pa povezavno tranzitiven. Graf $K_{2,3}$ ni regularen, kar že takoj pomeni, da ni točkovno tranzitiven. Je pa povezavno tranzitiven. Vsaka povezava ima eno točko v prvi množici dvodelnega razbitja, drugo pa v drugi. Vsaka premutacija, ki ohranja ti dve množici točk in s tem tudi množico povezav, je simetrija grafa $K_{2,3}$. Pravzaprav so vsi polni dvodelni grafi $K_{m,n}$, za katere je $m \neq n$, povezavno tranzitivni in niso točkovno tranzitivni. Grupa avtomorfizmov ima na množici točk natanko dve orbiti, ki sovpadata z množicama dvodelnega razbitja. Iz tega primera tudi vidimo, da regularnost ni potreben pogoj za povezavno tranzitivnost, kot je to za točkovno. Je pa veliko težje najti regularne grafe, ki so povezavno tranzitivni in niso točkovno tranzitivni. Takim grafom pravimo **semisimetrični grafi**. Glede na [10] je najmanjši tak graf reda 20 in se imenuje Folkmanov graf (slika 37).



Slika 37: Folkmanov graf.

Tretji graf s slike 36 je primer grafa, ki ni niti točkovno niti povezavno tranzitiven. Graf ni regularen, torej ni točkovno tranzitiven. Povezave tega grafa, ki imajo za krajišče sredinsko točko se razlikujejo od povezav, ki za krajišče te točke nimajo, saj prve ležijo

na dveh 3-ciklih, druge pa le na enem 3-ciklu. To pomeni, da ta graf ni niti povezavno tranzitiven.

Ugotovili smo, da sta točkovna in povezavna tranzitivnost na nek način neodvisni ena od druge. Nekoliko drugače je z naslednjo vrsto tranzitivnosti imenovano ločna tranzitivnost.

4.2 Ločno tranzitivni grafi

Ponovno najprej podajmo kar formalno definicijo ločne tranzitivnosti.

Definicija 4.2. Graf Γ je **ločno tranzitiven**, če njegova grupa avtomorfizmov deluje tranzitivno na loke grafa. To pomeni, da za katerakoli para povezanih točk $u_1 \sim v_1, u_2 \sim v_2$, za $u_1, u_2, v_1, v_2 \in V(\Gamma)$, obstaja avtomorfizem $\alpha \in Aut(\Gamma)$, za katerega velja $\alpha(u_1) = u_2$ in $\alpha(v_1) = v_2$, in obstaja avtomorfizem $\beta \in Aut(\Gamma)$, za katerega velja $\beta(u_1) = v_2$ in $\beta(v_1) = u_2$.

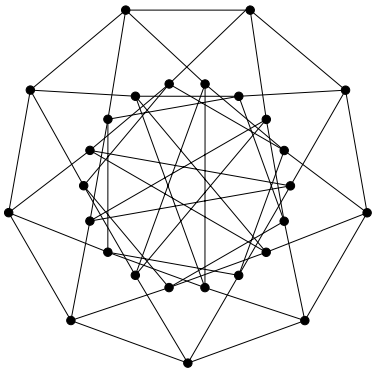
Primer ločno tranzitivnega grafa je cikel C_4, saj lahko z avtomorfizmoma (0123) in (01)(24) slej ko prej poljuben lok preslikamo v katerikoli drug lok. Pravzaprav so vsi cikli C_n ločno tranzitivni. Grupa avtomorfizmov ciklov C_n je diedrska grupa $D_{2\cdot n} = \langle \rho, \tau \rangle$ in ravno avtomorfizma ρ in τ nam poljuben lok preslikata v katerikoli drug lok. Avtomorfizem ρ poljubno povezavo preslika v poljubno drugo povezavo, avtomorfizem τ pa poljubno povezavo obrne. Očitno je tudi, da so vsi polni grafi K_n in prazni grafi N_n ločno tranzitivni, saj je njihova grupa avtomorfizmov simetrična grupa S_n.

Izkaže se, da je ločna tranzitivnost strožja lastnost od točkovne in povezavne tranzitivnosti, saj pri povezanih grafih ta ostali dve vrsti tranzitivnosti implicira. To pomeni, da graf, ki ni točkovno ali povezavno tranzitiven, ni niti ločno tranzitiven. To dejstvo nam pove, da pravzaprav nobeden izmed grafov na sliki 36 ni ločno tranzitiven.

Trditev 4.3. *Vsak povezan ločno tranzitiven graf je tudi točkovno in tudi povezavno tranzitiven.*

Dokaz. Naj bo povezan graf Γ ločno tranzitiven. Da iz ločne tranzitivnosti sledi povezavna tranzitivnost je očitno, zato dokažimo le, da iz ločne tranzitivnosti sledi tudi točkovna tranzitivnost. Naj bosta u, v poljubni točki grafa Γ, to je $u, v \in V(\Gamma)$. Naj bo sedaj (u, z), za $z \in V(\Gamma)$, poljuben lok s krajiščem v točki u in (v, w), za $w \in V(\Gamma)$, poljuben lok s krajiščem v točki v. Ker je graf Γ ločno tranzitiven, obstaja $\alpha \in \mathrm{Aut}(\Gamma)$, ki preslika lok (u, z) v lok (v, w). Od tod sledi, da α preslika tudi točko u v točko v in ker sta bili u in v poljubni točki grafa Γ, je le ta res točkovno tranzitiven. □

Obrat trditve 4.3 v splošnem ne velja. Obstajajo namreč povezani grafi, ki so točkovno in povezavno tranzitivni, a niso ločno tranzitivni. Takim grafom pravimo **poltranzitivni grafi**. Glede na [8] je najmanjši primer poltranzitivnega grafa Doyle-Holtov graf, ki je reda 27 (slika 38).



Slika 38: Doyle-Holtov graf.

Za grafe, ki jim znamo določiti njihovo grupo avtomorfizmov, znamo seveda določiti tudi ali so ločno tranzitivni. V splošnem pa je določitev grupe avtomorfizmov danega grafa in določitev ali je graf ločno tranzitiven izjemno zahtevna naloga. Lema, ki sledi, v primeru točkovno tranzitivnih grafov povezuje ločno tranzitivnost in delovanje stabilizatorja točke na njene sosede.

Lema 4.4. *Točkovno tranzitiven graf* Γ *je ločno tranzitiven natanko tedaj, ko stabilizator* $Aut(\Gamma)_v$ *poljubne točke* $v \in \Gamma$ *deluje tranzitivno na množico sosedov točke* v*.*

Dokaz.
($\Rightarrow$) Naj bo graf Γ ločno tranzitiven. To med drugim pomeni, da za katerakoli dva soseda v_1 in v_2 točke v obstaja avtomorfizem $\alpha \in \mathrm{Aut}(\Gamma)$, ki preslika lok (v, v_1) v lok (v, v_2). Ker α točko v fiksira je $\alpha \in \mathrm{Aut}(\Gamma)_v$. Ker sta v_1 in v_2 poljubni sosedi točke v, $\mathrm{Aut}(\Gamma)_v$ res deluje tranzitivno na množico sosedov točke v.
($\Leftarrow$) Naj sedaj $\mathrm{Aut}(\Gamma)_v$ deluje tranzitivno na množici sosedov točke v in naj bosta (u_1, v_1) in (u_2, v_2) poljubna loka grafa Γ. Ker je graf Γ točkovno tranzitiven obstaja nek $\alpha_1 \in Aut(\Gamma)$, ki preslika u_1 v v, torej $\alpha_1(u_1) = v$ in nek $\alpha_2 \in Aut(\Gamma)$, ki preslika u_2 v v, torej $\alpha_2(u_2) = v$. To pa pomeni, da sta točki $\alpha_1(v_1)$ in $\alpha_2(v_2)$ sosedi točke v. Ker po predpostavki $\mathrm{Aut}(\Gamma)_v$ deluje tranzitivno na množici sosedov točke v, obstaja nek $\alpha' \in \mathrm{Aut}(\Gamma)_v$, ki preslika točko $\alpha_1(v_1)$ v točko $\alpha_2(v_2)$, točko v pa fiksira, torej $\alpha'(\alpha_1(v_1)) = \alpha_2(v_2)$ in $\alpha'(v) = v$. Od tod sledi, da je $\alpha_2^{-1}\alpha'\alpha_1(u_1, v_1) = \alpha_2^{-1}(\alpha'(\alpha_1(u_1, v_1))) = \alpha_2^{-1}(\alpha'(v, \alpha_1(v_1))) = \alpha_2^{-1}(v, \alpha'(\alpha_1(v_1))) = \alpha_2^{-1}(v, \alpha_2(v_2)) = (u_2, v_2)$, kar pomeni, da je Γ res ločno tranzitiven graf. □

Pri ločni tranzitivnosti nas zanima tranzitivnost delovanja grupe avtomorfizmov na množico urejenih parov povezanih točk, ta pojem pa zlahka posplošimo na tranzitivnost delovanja grupe avtomorfizmov na zaporedja zaporedno povezanih točk. Tako tranzitivnost imenujemo s-ločna tranzitivnost.

Definicija 4.5. Graf Γ je **s-ločno tranzitiven**, kjer je $s \geq 0$, če njegova grupa avtomorfizmov deluje tranzitivno na množici vseh s-lokov grafa Γ. Pri tem je s-lok zaporedje točk $(v_0, v_1, \ldots, v_s)$, kjer sta poljubni zaporedni točki povezani in $v_{i-1} \neq v_{i+1}$, za $0 < i < s$.

Opomba 4.6. Bralec bo opazil, da so 0-ločno tranzitivni grafi ravno točkovno tranzitivni, 1-ločno tranzitivni pa ločno tranzitivni.

Cikli C_n so s-ločno tranzitivni grafi za vse $s \geq 0$. Polni grafi K_n, za $n \geq 4$, so 2-ločno tranzitivni, niso pa 3-ločno tranzitivni. Ti grafi vsebujejo vse možne povezave med točkami, zato lahko poljuben 2-lok preslikamo v katerikoli drug 2-lok, graf pa se pri tem ohrani. Ker polni graf vsebuje 3-cikle, ne moremo preslikati poljuben 3-lok v katerikoli drug 3-lok, kot je to razvidno iz slike 39.

Slika 39: Polni grafi K_n so 2-ločno tranzitivni in niso 3-ločno tranzitivni.

Podoben razmislek nas pripelje do tega, da so polni dvodelni grafi $K_{n,n}$ 3-ločno tranzitivni, niso pa 4-ločno tranzitivni. Ti grafi namreč vsebujejo 4-cikle in zato ne morejo biti 4-ločno tranzitivni (razen seveda v trivialnih primerih $K_{1,1}$ in $K_{2,2}$).

4.2.1 Ločno tranzitivni cirkulanti

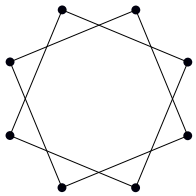
Kot smo že omenili, v splošnem povezavna in točkovna tranzitivnost ne zadoščata za ločno tranzitivnost, tu pa bomo dokazali, da v primeru cirkulantnih grafov vendarle zadoščata.

Izrek 4.7. *Cirkulant je ločno tranzitiven natanko tedaj, ko je povezavno tranzitiven.*

Dokaz. Če je graf ločno tranzitiven, smo že v trditvi 4.3 dokazali, da je tudi povezavno tranzitiven. Torej moramo za cirkulante dokazati le obrat te trditve. Naj bo $\mathrm{Circ}(n; S)$ povezavno tranzitiven cirkulant, kar pomeni, da lahko z grupo avtomorfizmov preslikamo katerokoli povezavo v katerokoli drugo povezavo. Cirkulant bo tako očitno ločno

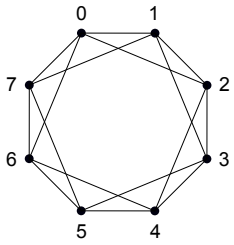
tranzitiven, če lahko nek lok (u, v) preslikamo v lok (v, u). Kot že vemo je preslikava $\alpha : \mathbb{Z}_n \to \mathbb{Z}_n$, podana s predpisom $\alpha(g) = g + s$, avtomorfizem cirkulantnega grafa. Prav tako je tudi preslikava $\beta : \mathbb{Z}_n \to \mathbb{Z}_n$, podana s predpisom $\beta(g) = -g$, avtomorfizma cirkulantnega grafa, saj $u \sim v \Leftrightarrow \exists s \in S : v = u + s \Leftrightarrow \exists s \in S : -v = -(u+s) = -u+(-s) \Leftrightarrow -u \sim -v$. Oglejmo si kaj avtomorfizem $\alpha \circ \beta$ naredi s parom povezanih točk 0 in s. Torej $\alpha(\beta(0)) = \alpha(0) = s$ in $\alpha(\beta(s)) = \alpha(-s) = -s + s = 0$. Tako smo našli avtomorfizem, ki lok $(0, s)$ preslika v lok $(s, 0)$, kar pomeni, da je res vsak povezavno tranzitiven cirkulant tudi ločno tranzitiven. □

Prav tako je pri obravnavi ločne tranzitivnosti cirkulantov smiselno obravnavati le povezane cirkulante, saj tisti, ki to niso, razpadejo na več izomorfnih komponent povezanosti, ki so že same po sebi cirkulanti. Na sliki 40 je prikazan nepovezan cirkulant $\mathrm{Circ}(8; \{\pm 2\})$ in res vidimo, da je sestavljen iz dveh komponent povezanosti, natančneje dveh 4-ciklov C_4, ki sta sama po sebi cirkulanta. Ker je graf C_4 ločno tranzitiven in ker je $\mathrm{Circ}(8; \{\pm 2\})$ unija dveh kopij grafa C_4, je tudi cirkulant $\mathrm{Circ}(8; \{\pm 2\})$ ločno tranzitiven.

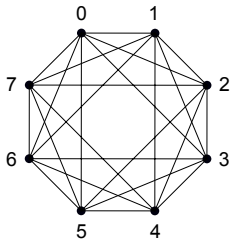


Slika 40: Nepovezan cirkulant $\mathrm{Circ}(8; \{\pm 2\})$.

Na sliki 41 je primer cirkulanta $\mathrm{Circ}(8; \{\pm 1, \pm 2\})$, ki ni ločno tranzitiven. Lok $(0, 7)$ leži na dveh 3-ciklih, medtem ko lok $(0, 6)$ leži zgolj na enem 3-ciklu, kar pomeni, da loka $(0, 7)$ ne moremo preslikati v lok $(0, 6)$. Cirkulant $\mathrm{Circ}(8; \{\pm 1, \pm 2 \pm 3\})$ s slike 42 pa je ločno tranzitiven, saj lahko z avtomorfizmi $\rho, \tau, (13)(26)(57), (12)(56)$, kjer sta $\rho, \tau \in D_{2\cdot 8}$, poljuben lok preslikamo v poljuben drugi lok.



Slika 41: Cirkulant $\mathrm{Circ}(8; \{\pm 1, \pm 2\})$, ki ni ločno tranzitiven.



Slika 42: Ločno tranzitiven cirkulant Circ(8; {±1, ±2, ±3}).

Madžarski matematik István Kovács je v članku [9] klasificiral ločno tranzitivne cirkulante. Zaradi kompleksnosti dokaza njegovega izreka ne bomo dokazovali, bomo pa z njegovo pomočjo klasificirali ločno tranzitivne cirkulante do 30 točk. Za razumevanje izreka še prej definirajmo prav posebno družino cirkulantov, imenovano normalni cirkulanti in dve operaciji na grafih, to sta leksikografski produkt in izbrisani leksikografski produkt.

Definicija 4.8. Cirkulant Γ=Circ$(n; S)$ je **normalen cirkulant** natanko tedaj, ko je naravna regularna podgrupa grupe avtomorfizmov, izomorfna ciklični grupi $\mathbb{Z}_n$, edinka v grupi Aut(Γ).

Opomba 4.9. Permutacijska grupa, izomorfna ciklični grupi $\mathbb{Z}_n$, je generirana z elementom $g = (01 \dots (n-1))$. Včasih jo označimo kar z $\langle g \rangle$.

S pomočjo trditve, ki sledi, dokažemo, da v primeru, ko stabilizator $\mathrm{Aut}(\Gamma)_0$ normalizira grupo $\langle g \rangle$, je $\langle g \rangle$ edinka v grupi Aut(Γ).

Trditev 4.10. *Naj bo* Γ=*Circ*$(n; S)$ *cirkulant reda* n *in naj bo* $\langle g \rangle$ *naravna regularna podgrupa grupe Aut*(Γ)*, izomorfna ciklični grupi* $\mathbb{Z}_n$*. Potem velja Aut*(Γ) =*Aut*$(\Gamma)_0 \cdot \langle g \rangle$*.*

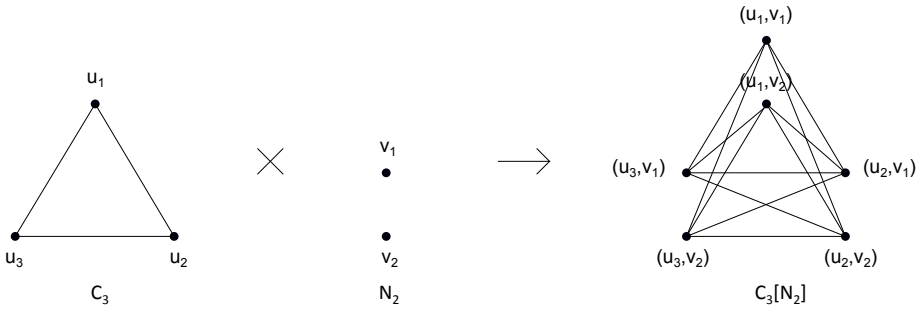
Dokaz. Po izreku 3.9 je graf Γ točkovno tranzitiven. Zato njegova grupa avtomorfizmov Aut(Γ) deluje tranzitivno na točke grafa Γ, kar pomeni, da je orbita $\mathcal{O}$ ena sama in ta je velikosti n. Po izreku o orbiti in stabilizatorju velja $|\mathrm{Aut}(\Gamma)| = |\mathrm{Aut}(\Gamma)_0| \cdot |\mathcal{O}| = |\mathrm{Aut}(\Gamma)_0| \cdot n$. Ker je $|\langle g \rangle| = n$, v primeru, ko pri produktu elementov iz $\langle g \rangle$ in $\mathrm{Aut}(\Gamma)_0$ dobimo same različne elemente, pokrijemo celotno grupo Aut(Γ). Vprašanje je torej, ali je lahko $g_1\alpha_1 = g_2\alpha_2$ za neke paroma različne $g_1, g_2 \in \langle g \rangle$ in $\alpha_1, \alpha_2 \in \mathrm{Aut}(\Gamma)_0$. Privzemimo, da to drži, kar pomeni, da je $g_2^{-1}g_1 = \alpha_2\alpha_1^{-1}$. Ker elementi stabilizatorja $\mathrm{Aut}(\Gamma)_0$ točko 0 fiksirajo, jo mora fiksirati tudi produkt $\alpha_2\alpha_1^{-1}$. Od tod sledi, da točko 0 fiksira tudi produkt $g_2^{-1}g_1$, kar je možno le v primeru, ko je $g_2^{-1}g_1 =$id, torej $g_1 = g_2$ in s tem tudi $\alpha_1 = \alpha_2$, to pa je v protislovju z našo predpostavko. Ugotovili smo, da je produkt grup $\langle g \rangle$ in $\mathrm{Aut}(\Gamma)_0$ velikosti $|\mathrm{Aut}_0| \cdot n$ in ker $\langle g \rangle \leq \mathrm{Aut}(\Gamma)$ in $\mathrm{Aut}(\Gamma)_0 \leq \mathrm{Aut}(\Gamma)$, je produkt res kar grupa Aut(Γ). □

Dve operaciji na grafih smo spoznali že v 2. poglavju, to sta unija in komplement. Spoznajmo sedaj še operacijo produkta dveh grafov. Produkt dveh grafov je običajno graf, katerega množica točk je kartezični produkt množice točk posameznih grafov. Pravilo, ki določa povezave v produktnem grafu, je mogoče izbrati na več načinov. Mi si bomo pogledali dva produkta grafov in sicer leksikografski produkt in izbrisani leksikografski produkt.

Definicija 4.11. Leksikografski produkt grafov Γ in Σ je graf $\Gamma[\Sigma]$, ki je definiran na množici točk $V(\Gamma[\Sigma]) = V(\Gamma) \times V(\Sigma)$, dve različni točki (u_1, v_1) in (u_2, v_2), za $u_1, u_2 \in V(\Gamma)$ in $v_1, v_2 \in V(\Sigma)$, pa sta povezani, kadar velja

- $u_1u_2 \in E(\Gamma)$ ali
- $u_1 = u_2$ in $v_1v_2 \in E(\Sigma)$.

Leksikogrfaski produkt grafov Γ in Σ pravzaprav dobimo tako, da vzamemo graf Γ in vsako njegovo točko razširimo v graf Σ. Sedaj vsaki dve "povezani" kopiji grafa Σ povežemo še z vsemi možnimi vmesnimi povezavami.



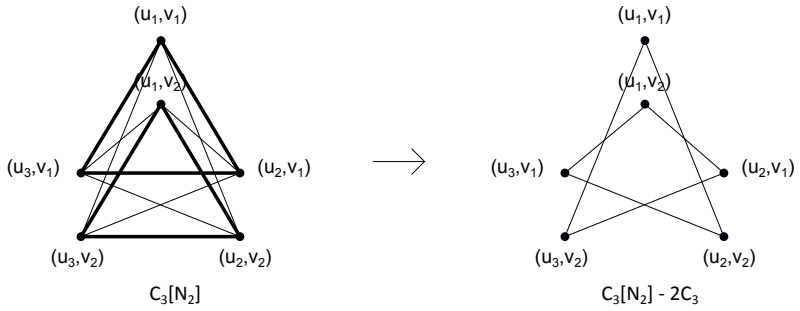
Slika 43: Leksikografski produkt grafov C_3 in N_2.

Definicija 4.12. Izbrisani leksikografski produkt grafov Γ in Σ je graf $\Gamma[\Sigma] - n\Gamma$, kjer je $n = |V(\Sigma)|$, ki je definiran na množici točk $V(\Gamma[\Sigma]) = V(\Gamma) \times V(\Sigma)$, dve različni točki (u_1, v_1) in (u_2, v_2), za $u_1, u_2 \in V(\Gamma)$ in $v_1, v_2 \in V(\Sigma)$, pa sta povezani, kadar velja

- $u_1u_2 \in E(\Gamma)$ in $v_1 \neq v_2$ ali
- $u_1 = u_2$ in $v_1v_2 \in E(\Sigma)$.

Izbrisani leksikografski produkt grafov Γ in Σ torej dobimo iz leksikografskega produkta $\Gamma[\Sigma]$ tako, da iz grafa $\Gamma[\Sigma]$ odstranimo $|V(\Sigma)|$ kopij grafa Γ.

Navedimo sedaj Kovácsev izrek.



Slika 44: Leksikografski produkt $C_3[N_2]$ in izbrisani leksikografski produkt $C_3[N_2] - 2C_3$.

Izrek 4.13. *Če je povezan graf* Γ *ločno tranzitiven cirkulant reda* n*, potem spada v eno izmed naslednjih družin grafov:*
(i) $\Gamma = K_n$*;*
(ii) Γ *je normalen cirkulant;*
(iii) $\Gamma = \Sigma[N_d]$*, kjer je* $n = md$ *in je* Σ *povezan ločno tranzitiven cirkulant reda* m*;*
(iv) $\Gamma = \Sigma[N_d] - d\Sigma$*, kjer je* $n = md$*,* $d > 3$*,* $D(d, m) = 1$ *in je* Σ *povezan ločno tranzitiven cirkulant reda* m*.*

S pomočjo programa MAGMA smo poiskali povezane ločno tranzitivne cirkulante do 30 točk ter jih predstavili v tabeli, ki sledi. Tabela 2 je razdeljena na 3 stolpce. Prvi stolpec predstavlja red cirkulanta $\mathrm{Circ}(n; S)$, drugi stolpec povezavno množico S, v tretjem pa je napisana družina v katero spada dani cirkulant. Če v tem stolpcu piše N-Circ pomeni, da gre za normalen cirkulant. V primeru izomorfnih cirkulantov je v stolpcu S predstavljena zgolj povezavna množica enega predstavnika tega izomorfnostnega razreda, zraven povezavne množice pa je dodan nabor vseh $q \in \mathbb{Z}_n^*$, za katere povezavna množica qS da izomorfen cirkulant.

Tabela 2: Povezani ločno tranzitivni cirkulanti.

n	**S**	**Družina**
3	$\{\pm 1\}$	K_3
4	$\{\pm 1\}$	N-Circ
	$\{\pm 1, 2\}$	K_4
5	$\{\pm 1\}$, $q \in \{2\}$	N-Circ
	$\{\pm 1, \pm 2\}$	K_5
6	$\{\pm 1\}$	N-Circ
	$\{\pm 1, 3\}$	$K_2[N_3]$
	$\{\pm 1, \pm 2\}$	$C_3[N_2]$
	$\{\pm 1, \pm 2, 3\}$	K_6
7	$\{\pm 1\}$, $q \in \{2, 3\}$	N-Circ
	$\{\pm 1, \pm 2, \pm 3\}$	K_7

n	**S**	**Družina**
8	$\{\pm 1\},\ q \in \{3\}$	N-Circ
	$\{\pm 1, \pm 3\}$	$C_4[N_2]$
	$\{\pm 1, \pm 2, \pm 3\}$	$K_4[N_2]$
	$\{\pm 1, \pm 2, \pm 3, 4\}$	K_8
9	$\{\pm 1\},\ q \in \{2, 4\}$	N-Circ
	$\{\pm 1, \pm 2, \pm 4\}$	$C_3[N_3]$
	$\{\pm 1, \pm 2, \pm 3, \pm 4\}$	K_9
10	$\{\pm 1\}, \{\pm 3\}$	N-Circ
	$\{\pm 1, \pm 3\}$	$K_2[N_5] - 5K_2$
	$\{\pm 1, \pm 4\},\ q \in \{3\}$	$C_5[N_2]$
	$\{\pm 1, \pm 3, 5\}$	$K_2[N_5]$
	$\{\pm 1, \pm 2, \pm 3, \pm 4\}$	$K_5[N_2]$
	$\{\pm 1, \pm 2, \pm 3, \pm 4, 5\}$	K_{10}
11	$\{\pm 1\},\ q \in \{2, 3, 4, 5\}$	N-Circ
	$\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5\}$	K_{11}
12	$\{\pm 1\},\ q \in \{5\}$	N-Circ
	$\{\pm 1, \pm 5\}$	$C_6[N_2]$
	$\{\pm 1, \pm 3, \pm 5\}$	$C_4[N_3]$
	$\{\pm 1, \pm 2, \pm 5\}$	$C_3[N_4] - 4C_3$
	$\{\pm 1, \pm 2, \pm 4, \pm 5\}$	$C_3[N_4]$
	$\{\pm 1, \pm 2, \pm 3, \pm 5, 6\}$	$K_4[N_3]$
	$\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5\}$	$K_6[N_2]$
	$\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5, 6\}$	K_{12}
13	$\{\pm 1\},\ q \in \{2, 3, 4, 5, 6\}$	N-Circ
	$\{\pm 1, \pm 5\},\ q \in \{2, 4\}$	N-Circ
	$\{\pm 1, \pm 3, \pm 4\},\ q \in \{2\}$	N-Circ
	$\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6\}$	K_{13}
14	$\{\pm 1\},\ q \in \{3, 5\}$	N-Circ
	$\{\pm 1, \pm 6\},\ q \in \{3, 5\}$	$C_7[N_2]$
	$\{\pm 1, \pm 3, \pm 5\}$	$K_2[N_7] - 7K_2$
	$\{\pm 1, \pm 3, \pm 5, 7\}$	$K_2[N_7]$
	$\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6\}$	$K_7[N_2]$
	$\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, 7\}$	K_{14}
15	$\{\pm 1\},\ q \in \{2, 4, 7\}$	N-Circ
	$\{\pm 1, \pm 4\},\ q \in \{2\}$	N-Circ
	$\{\pm 1, \pm 4, \pm 6\},\ q \in \{2\}$	$C_5[N_3]$
	$\{\pm 1, \pm 2, \pm 4, \pm 7\}$	$C_3[N_5] - 5C_3$
	$\{\pm 1, \pm 2, \pm 4, \pm 5, \pm 7\}$	$C_3[N_5]$
	$\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 7\}$	$K_5[N_3]$
	$\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 7\}$	K_{15}
	$\{\pm 1\},\ q \in \{3, 5, 7\}$	N-Circ
	$\{\pm 1, \pm 7\},\ q \in \{3\}$	$C_8[N_2]$

n	**S**	**Družina**
	$\{\pm1, \pm3, \pm5, \pm7\}$	$K_2[N_8]$
	$\{\pm1, \pm2, \pm3, \pm5, \pm6, \pm7\}$	$K_4[N_4]$
	$\{\pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \pm7\}$	$K_8[N_2]$
	$\{\pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \pm7, 8\}$	K_{16}
17	$\{\pm1\}$, $q \in \{2, 3, 4, 5, 6, 7, 8\}$	N-Circ
	$\{\pm1, \pm4\}$, $q \in \{2, 3, 6\}$	N-Circ
	$\{\pm1, \pm2, \pm4, \pm8\}$, $q \in \{3\}$	N-Circ
	$\{\pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \pm7, \pm8\}$	K_{17}
18	$\{\pm1\}$, $q \in \{5, 7\}$	N-Circ
	$\{\pm1, \pm8\}$ $q \in \{5, 7\}$	$C_9[N_2]$
	$\{\pm1, \pm5, \pm7\}$	$C_6[N_3]$
	$\{\pm1, \pm3, \pm5, \pm7\}$	$K_2[N_9] - 9K_2$
	$\{\pm1, \pm3, \pm5, \pm7, 9\}$	$K_2[N_9]$
	$\{\pm1, \pm2, \pm4, \pm5, \pm7, \pm8\}$	$\mathrm{Circ}(9, \{\pm1, \pm2, \pm4\})[N_2]$
	$\{\pm1, \pm2, \pm3, \pm4, \pm5, \pm7, \pm8, 9\}$	$K_6[N_3]$
	$\{\pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \pm7, \pm8\}$	$K_9[N_2]$
	$\{\pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \pm7, \pm8, 9\}$	K_{18}
19	$\{\pm1\}$, $q \in \{2, 3, 4, 5, 6, 7, 8, 9\}$	N-Circ
	$\{\pm1, \pm7, \pm8\}$, $q \in \{2, 4\}$	N-Circ
	$\{\pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \pm7, \pm8, \pm9\}$	K_{19}
20	$\{\pm1\}$, $q \in \{3, 7, 9\}$	N-Circ
	$\{\pm1, \pm9\}$, $q \in \{3\}$	$C_{10}[N_2]$
	$\{\pm1, \pm6, \pm9\}$, $q \in \{3\}$	$C_5[N_4] - 5C_4$
	$\{\pm1, \pm3, \pm7, \pm9\}$	$\mathrm{Circ}(10, \{\pm1, \pm3\})[N_2]$
	$\{\pm1, \pm4, \pm6, \pm9\}$, $q \in \{3\}$	$\mathrm{Circ}(10, \{\pm1, \pm4\})[N_2]$
	$\{\pm1, \pm3, \pm5, \pm7, \pm9\}$	$K_2[N_{10}]$
	$\{\pm1, \pm2, \pm3, \pm6, \pm7, \pm9\}$	$K_4[N_5] - 5K_4$
	$\{\pm1, \pm2, \pm3, \pm5, \pm6, \pm7, \pm9, 10\}$	$K_4[N_5]$
	$\{\pm1, \pm2, \pm3, \pm4, \pm6, \pm7, \pm8, \pm9\}$	$K_5[N_4]$
	$\{\pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \pm7, \pm8, \pm9\}$	$K_{10}[N_2]$
	$\{\pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \pm7, \pm8, \pm9, 10\}$	K_{20}
21	$\{\pm1\}$, $q \in \{2, 4, 5, 8, 10\}$	N-Circ
	$\{\pm1, \pm8\}$, $q \in \{2, 4\}$	N-Circ
	$\{\pm1, \pm4, \pm5\}$, $q \in \{2\}$	N-Circ
	$\{\pm1, \pm6, \pm8\}$, $q \in \{2, 4\}$	$C_7[N_3]$
	$\{\pm1, \pm2, \pm4, \pm5, \pm8, \pm10\}$	$C_3[N_7] - 7C_3$
	$\{\pm1, \pm2, \pm4, \pm5, \pm7, \pm8, \pm10\}$	$C_3[N_7]$
	$\{\pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \pm8, \pm9, \pm10\}$	$K_7[N_3]$
	$\{\pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \pm7, \pm8, \pm9, \pm10\}$	K_{21}
22	$\{\pm1\}$, $q \in \{3, 5, 7, 9\}$	N-Circ
	$\{\pm1, \pm10\}$, $q \in \{3, 5, 7, 9\}$	$C_{11}[N_2]$
	$\{\pm1, \pm3, \pm5, \pm7, \pm9\}$	$K_2[N_{11}] - 11K_2$
	$\{\pm1, \pm3, \pm5, \pm7, \pm9, 11\}$	$K_2[N_{11}]$

n	S	Družina
	$\{\pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \pm7 \pm 8, \pm9, \pm10\}$	$K_{11}[N_2]$
	$\{\pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \pm7, \pm8, \pm9, \pm10, 11\}$	K_{22}
23	$\{\pm1\},\ q \in \{2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$	N-Circ
	$\{\pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \pm7, \pm8, \pm9, \pm10, \pm11\}$	K_{23}
24	$\{\pm1\},\ q \in \{5, 7, 11\}$	N-Circ
	$\{\pm1, \pm5\},\ q \in \{7\}$	N-Circ
	$\{\pm1, \pm7\},\ q \in \{5\}$	N-Circ
	$\{\pm1, \pm11\},\ q \in \{5\}$	$C_{12}[N_2]$
	$\{\pm1, \pm7, \pm9\},\ q \in \{5\}$	$C_8[N_3]$
	$\{\pm1, \pm5, \pm7, \pm11\}$	$C_6[N_4]$
	$\{\pm1, \pm3, \pm5, \pm7, \pm9, \pm11\}$	$K_2[N_{12}]$
	$\{\pm1, \pm2, \pm5, \pm7, \pm10, \pm11\}$	$\mathrm{Circ}(12, \{\pm1, \pm2, \pm5\})[N_2]$
	$\{\pm1, \pm2, \pm4, \pm5, \pm7, \pm10, \pm11\}$	$K_3[N_8] - 8K_3$
	$\{\pm1, \pm2, \pm4, \pm5, \pm7, \pm8, \pm10, \pm11\}$	$K_3[N_8]$
	$\{\pm1, \pm2, \pm3, \pm5, \pm6, \pm7, \pm9, \pm10, \pm11\}$	$K_4[N_6]$
	$\{\pm1, \pm2, \pm3, \pm4, \pm5, \pm7, \pm8, \pm9, \pm10, \pm11\}$	$K_6[N_4]$
	$\{\pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \pm7, \pm9, \pm10, \pm11, 12\}$	$K_8[N_3]$
	$\{\pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \pm7, \pm8, \pm9, \pm10, \pm11\}$	$K_{12}[N_2]$
	$\{\pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \pm7, \pm8, \pm9, \pm10, \pm11, 12\}$	K_{24}
25	$\{\pm1\},\ q \in \{2, 3, 4, 6, 7, 8, 9, 11, 12\}$	N-Circ
	$\{\pm1, \pm7\},\ q \in \{2, 3, 6, 9\}$	N-Circ
	$\{\pm1, \pm4, \pm6, \pm9, \pm11\},\ q \in \{2\}$	$C_5[N_5]$
	$\{\pm1, \pm2, \pm3, \pm4, \pm6, \pm7, \pm8, \pm9, \pm11, \pm12\}$	$K_5[N_5]$
	$\{\pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \pm7, \pm8, \pm9, \pm10, \pm11, \pm12\}$	K_{25}
26	$\{\pm1\},\ q \in \{3, 5, 7, 9, 11\}$	N-Circ
	$\{\pm1, \pm5\},\ q \in \{3, 7\}$	N-Circ
	$\{\pm1, \pm12\},\ q \in \{3, 5, 7, 9, 11\}$	$C_{13}[N_2]$
	$\{\pm1, \pm3, \pm9\},\ q \in \{5\}$	N-Circ
	$\{\pm1, \pm5, \pm8, \pm12\},\ q \in \{3, 7\}$	$\mathrm{Circ}(13, \{\pm1, \pm5\})[N_2]$
	$\{\pm1, \pm3, \pm5, \pm7, \pm9, \pm11\}$	$K_{13}[N_2] - 2K_{13}$
	$\{\pm1, \pm3, \pm4, \pm9, \pm10, \pm12\},\ q \in \{5\}$	$\mathrm{Circ}(13, \{\pm1, \pm3, \pm4\})[N_2]$
	$\{\pm1, \pm3, \pm5, \pm7, \pm9, \pm11, \pm13\}$	$K_2[N_{13}]$
	$\{\pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \pm7, \pm8, \pm9, \pm10 \pm 11, \pm12\}$	$K_{13}[N_2]$
	$\{\pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \pm7, \pm8, \pm9, \pm10, \pm11, \pm12, 13\}$	K_{26}
27	$\{\pm1\},\ q \in \{2, 4, 5, 7, 8, 10, 11, 13\}$	N-Circ
	$\{\pm1, \pm8, \pm10\},\ q \in \{2, 4\}$	$C_9[N_3]$
	$\{\pm1, \pm2, \pm4, \pm5, \pm7, \pm8, \pm10, \pm11, \pm13\}$	$\mathrm{Circ}(13, \{\pm1, \pm3, \pm4\})[N_2]$
	$\{\pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \pm7, \pm8, \pm10 \pm 11, \pm12, \pm13\}$	$K_9[N_3]$
	$\{\pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \pm7, \pm8, \pm9, \pm10, \pm11, \pm12, \pm13\}$	K_{27}
	$\{\pm1\},\ q \in \{3, 5, 9, 11, 13\}$	N-Circ
	$\{\pm1, \pm13\},\ q \in \{3, 5\}$	$C_{14}[N_2]$
	$\{\pm1, \pm3, \pm9\},\ q \in \{5\}$	N-Circ
	$\{\pm1, \pm6, \pm13\},\ q \in \{3, 5\}$	$C_7[N_4] - 4C_7$

n	**S**	**Družina**
	$\{\pm1, \pm6, \pm8, \pm13\},\ q \in \{3, 5\}$	$C_7[N_4]$
	$\{\pm1, \pm3, \pm5, \pm9, \pm11, \pm13\}$	$\mathrm{Circ}(14, \{\pm1, \pm3, \pm5\})[N_2]$
	$\{\pm1, \pm3, \pm5, \pm7, \pm9, \pm11, \pm13\}$	$K_2[N_{14}]$
	$\{\pm1, \pm2, \pm3, \pm5, \pm6, \pm9, \pm10, \pm11, \pm13\}$	$K_4[N_7] - 7K_4$
	$\{\pm1, \pm2, \pm3, \pm5, \pm6, \pm7, \pm9, \pm10, \pm11, \pm13, 14\}$	$K_4[N_7]$
	$\{\pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \pm8, \pm9, \pm10 \pm 11, \pm12, \pm13\}$	$K_7[N_4]$
	$\{\pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \ldots, \pm13, 14\}$	K_{28}
29	$\{\pm1\},\ q \in \{2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$	N-Circ
	$\{\pm1, \pm12\},\ q \in \{2, 3, 4, 6, 8, 11\}$	N-Circ
	$\{\pm1, \pm4, \pm5, \pm6, \pm7, \pm9, \pm13\},\ q \in \{2\}$	N-Circ
	$\{\pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \ldots, \pm14\}$	K_{29}
30	$\{\pm1\},\ q \in \{7, 11, 13\}$	N-Circ
	$\{\pm1, \pm11\},\ q \in \{7\}$	N-Circ
	$\{\pm1, \pm14\},\ q \in \{7, 11, 13\}$	$C_{15}[N_2]$
	$\{\pm1, \pm9, \pm11\},\ q \in \{7\}$	$C_{10}[N_3]$
	$\{\pm1, \pm7, \pm11, \pm13\}$	$C_6[N_5] - 5C_6$
	$\{\pm1, \pm4, \pm11, \pm14\},\ q \in \{7\}$	$\mathrm{Circ}(15, \{\pm1, \pm4\})[N_2]$
	$\{\pm1, \pm5, \pm7, \pm11, \pm13\}$	$C_6[N_5]$
	$\{\pm1, \pm4, \pm9, \pm11, \pm14\},\ q \in \{7\}$	$C_5[N_6] - 6C_5$
	$\{\pm1, \pm3, \pm7, \pm9, \pm11, \pm13\}$	$\mathrm{Circ}(10, \{\pm1, \pm3\})[N_3]$
	$\{\pm1, \pm4, \pm6, \pm9, \pm11, \pm14\},\ q \in \{7\}$	$C_5[N_6]$
	$\{\pm1, \pm3, \pm5, \pm7, \pm9, \pm11, \pm13\}$	$K_2[N_{15}] - 15K_2$
	$\{\pm1, \pm3, \pm5, \pm7, \pm9, \pm11, \pm13, 15\}$	$K_2[N_{15}]$
	$\{\pm1, \pm2, \pm4, \pm7, \pm8, \pm11, \pm13, \pm14\}$	$\mathrm{Circ}(15, \{\pm1, \pm2, \pm4, \pm7\})[N_2]$
	$\{\pm1, \pm2, \pm4, \pm5, \pm7, \pm8, \pm11, \pm13, \pm14\}$	$C_3[N_{10}] - 10C_3$
	$\{\pm1, \pm2, \pm4, \pm5, \pm7, \pm8, \pm10, \pm11, \pm13, \pm14\}$	$C_3[N_{10}]$
	$\{\pm1, \pm2, \pm3, \pm4, \pm7, \pm8, \pm9, \pm11, \pm13, \pm14\}$	$K_6[N_5] - 5K_6$
	$\{\pm1, \pm2, \pm3, \pm4, \pm6, \pm7, \pm8, \pm9, \pm11, \pm12, \pm13, \pm14\}$	$K_5[N_6]$
	$\{\pm1, \pm2, \pm3, \pm4, \pm5, \pm7, \pm8, \pm9, \pm10, \pm11, \pm13, \pm14, 15\}$	$K_6[N_5]$
	$\{\pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \pm7, \pm8, \pm9, \pm11, \pm12, \pm13, \pm14, 15\}$	$K_{10}[N_3]$
	$\{\pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \ldots, \pm14\}$	$K_{15}[N_2]$
	$\{\pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \ldots, \pm14, 15\}$	K_{30}

Glede na tabelo 2 res vidimo, da vsi ločno tranzitivni cirkulanti spadajo v eno izmed družin, ki jih navaja Kovács v izreku 4.13. Razmislimo sedaj ali lahko o ločno tranzitivnih cirkulantih in družini, v katero spadajo, sklepamo še kaj več.

Najprej si poglejmo kaj lahko povemo o ločni tranzitivnosti grafov, ki spadajo v družino leksikografski produkt grafov oziroma izbrisani leksikografski produkt grafov. Naj bosta Γ_1 in Γ_2 grafa in naj bo Γ leksikografski produkt grafov Γ_1 in Γ_2, Γ' pa naj bo izbrisani leksikografski produkt grafov Γ_1 in Γ_2, torej $\Gamma = \Gamma_1[\Gamma_2]$ in $\Gamma' = \Gamma_1[\Gamma_2] - n\Gamma_1$, za $n = |V(\Gamma_2)|$. Iz definicije leksikografskega produkta in izbrisanega leksikografskega

produkta vidimo, da je za poljuben $\alpha \in S_{V(\Gamma_2)}$ preslikava $(u_i, v_j) \mapsto (u_i, \alpha(v_j))$ avtomorfizem grafa Γ, prav tako pa je za vsak $\beta \in \mathrm{Aut}(\Gamma_1)$ preslikava $(u_i, v_j) \mapsto (\beta(u_i), v_j))$ tudi avtomorfizem grafa Γ. To pomeni, da je v primeru, ko je Γ_1 ločno tranzitiven graf, Γ_2 pa prazen graf, tudi graf Γ', ločno tranzitiven. Brez večjih težav se prepričamo, da je v tem primeru ločno tranzitiven tudi graf Γ, saj lahko zgoraj opisani avtomorfizem, ki izhaja iz α spremenimo do te mere, da α deluje samo na vozliščih (u_i, v_j) za nek fiksen i, na vseh ostalih pa ne. Še več, ko je $\Gamma_1 = \mathrm{Circ}(m; S)$ in je Γ_2 prazen graf N_d, je Γ cirkulant in sicer $\Gamma = \Gamma_1[N_d] = \mathrm{Circ}(md; \{km + s : s \in S, k \in \{0, 1, \ldots, d-1\}\}$. Če velja še $D(m, d) = 1$, je cirkulant tudi graf Γ', saj je avtomorfizem, ki ga dobimo kot kompozitum zgoraj opisanega avtomorfizma z $\beta = (01 \ldots (m-1))$ in zgoraj opisanega avtomorfizma z $\alpha = (01 \ldots (d-1))$ očitno reda md, torej generira regularno ciklično podgrupo grupe avtomorfizimov grafa Γ', ki je zato po izreku 3.11 cirkulant, torej $\Gamma' = \Gamma_1[N_d] - n\Gamma_2 = \mathrm{Circ}(md; \{km + s : s \in S, k \in \{1, 2, \ldots, d-1\}\}$. Od tod sledita spodnji dve trditvi.

Trditev 4.14. *Naj bo Γ leksikografski produkt $\Gamma = \Sigma[N_d]$, kjer je Σ povezan ločno tranzitiven cirkulant. Potem je Γ ločno tranzitiven cirkulant.*

Trditev 4.15. *Naj bo Γ izbrisani leksikografski produkt $\Gamma = \Sigma[N_d] - d\Sigma$, kjer je Σ povezan ločno tranzitiven cirkulant reda m in velja $d > 3$ ter $D(m, d) = 1$. Potem je Γ ločno tranzitiven cirkulant.*

Osredotočimo se sedaj na ločno tranzitivne cirkulante praštevilskega reda. S pomočjo tabele 2 opazimo, da imajo vsi taki cirkulanti povezavno množico S oblike Hq, kjer je $H \leq \mathbb{Z}_p^*$ in $q \in \mathbb{Z}_p^*$. Dokažimo to ugotovitev še teoretično.

Trditev 4.16. *Cirkulant $Circ(p; S)$ praštevilskega reda p je ločno tranzitiven natanko tedaj, ko obstaja $q \in \mathbb{Z}_p^*$ in $H \leq \mathbb{Z}_p^*$, da je $S = Hq$.*

Dokaz.
V primeru, ko je $\mathrm{Circ}(p; S)$ poln graf K_p je $\mathrm{Circ}(p; S)$ ločno tranzitiven in S je grupa $\mathbb{Z}_p^*$. Torej naj bo $\Gamma = Circ(p; S)$, za $|S| < p - 1$. Po izreku 3.40 je $\mathrm{Aut}(\Gamma) = \{T_{a,b} : a \in K, b \in \mathbb{Z}_p\}$, kjer je K največja podgrupa grupe $\mathbb{Z}_p^*$, tako da je S unija odsekov grupe $\mathbb{Z}_p^*$ po podgrupi K.
($\Rightarrow$) Naj bo graf Γ ločno tranzitiven. Po lemi 4.4 stabilizator točke 0, to je $\mathrm{Aut}(\Gamma)_0$, deluje tranzitivno na sosedih točke 0, kar je ravno povezavna množica S. Naj bo $q \in S$ poljuben. Potem je $S = \mathcal{O}_{Aut(\Gamma)_0}(q) = \{T_{a,0}(q) : a \in K\} = \{aq : a \in K\} = Kq$, torej lahko vzamemo kar $H = K$.
($\Leftarrow$) Naj bo sedaj $S = Kq$ za nek $K \leq \mathbb{Z}_p^*$ in $q \in \mathbb{Z}_p^*$. Ker je $K \leq \mathbb{Z}_p^*$ največja podgrupa, da je S unija odsekov grupe $\mathbb{Z}_p^*$ po podgrupi K in je $S = Hq$, sledi $H = K$. Po lemi 4.4 je dovolj videti, da $\mathrm{Aut}(\Gamma)_0$ deluje tranzitivno na množici sosedov točke 0, torej na S.

Ker je $q \in S$ in za vsak $s \in S$ velja, da je $s = hq = T_{h,0}(q)$ za nek $h \in H$, stabilizator $\mathrm{Aut}(\Gamma)_0$ res deluje tranzitivno na S in zato je graf Γ res ločno tranzitiven. □

Ugotovili smo natanko kako izgledajo ločno tranzitivni cirkulanti $\mathrm{Circ}(p; S)$ praštevilskega reda p. Spomnimo se sedaj izreka 4.13 in razmislimo v katero družino spadajo. V primeru, ko je $|S| = p-1$, je $\mathrm{Circ}(p; S)$ kar poln graf K_p. Ker je grupa avtomorfizmov polnih grafov K_p simetrična grupa S_p in ker $\langle(01\dots(p-1))\rangle$ ni edinka v grupi S_p, saj $(p-2\ \ p-1)(01\dots(p-1))(p-2\ \ p-1) \notin \langle(01\dots(p-1))\rangle$, polni grafi K_p niso normalni cikulanti (z izjemo polnega grafa K_3). Isti razmislek velja za vse polne grafe K_n poljubnega reda $n > 3$. Vsi ostali ločno tranzitivni cirkulanti $\mathrm{Circ}(p; S)$ praštevilskega reda p, za $|S| < p-1$, pa spadajo med normalne cirkulante, saj praštevilo p nima pravih deljiteljev, kar pomeni, da graf $\mathrm{Circ}(p; S)$ ne moremo sestaviti kot leksikografski produkt dveh grafov. Ta razmislek nas pripelje do naslednjega izreka.

Izrek 4.17. *Vsak ločno tranzitiven cirkulant $Circ(p; S)$ praštevilskega reda $p \geq 5$, ki ni poln graf K_p, je normalen cirkulant.*

Razmislimo sedaj o ločni tranzitivnosti cirkulantov poljubnega reda. Trditve 4.16 ne moremo kar posplošiti na vse cirkulante, saj implikacija v $\Rightarrow$ smer v splošnem ne drži. Na primer, cirkulant $\mathrm{Circ}(6; \{\pm 1, 3\})$ je ločno tranzitiven, čeprav množica $\{\pm 1, 3\}$ ni podgrupa grupe $\mathbb{Z}_6^*$. V splošnem pa velja implikacija trditve 4.16 v $\Leftarrow$ smer, dokaz le te ostaja enak. Torej velja, da so vsi cirkulanti s povezavno množico S oblike Hq, kjer je $H \leq \mathbb{Z}_n^*$ in $q \in \mathbb{Z}_n^*$, ločno tranzitivni.

Trditev 4.18. *Naj bo $Circ(n; S)$ tak cirkulant, da je $S = Hq$, za $H \leq \mathbb{Z}_n^*$ in $q \in \mathbb{Z}_n^*$. Potem je cirkulant $Circ(n; S)$ ločno tranzitiven.*

Sedaj se nam zastavi vprašanje ali je vsak ločno tranzitiven cirkulant $\mathrm{Circ}(n; S)$, kjer je $S = Hq$ za nek $q \in \mathbb{Z}_n^*$ in $H \leq \mathbb{Z}_n^*$ in $|S| < n-1$, normalen cirkulant. A temu ni tako. S pomočjo MAGME smo ugotovili, da ločno tranzitiven cirkulant $\mathrm{Circ}(8; \{\pm 1, \pm 3\})$ ni normalen, čeprav je $\{\pm 1, \pm 3\} \leq \mathbb{Z}_8^*$. Velja pa obrat zastavljenega vprašanja.

Trditev 4.19. *Naj bo ločno tranzitiven cirkulant $Circ(n; S)$ normalen. Potem je $S = Hq$, kjer je $H \leq \mathbb{Z}_n^*$ in $q \in \mathbb{Z}_n^*$.*

Dokaz. Naj bo ločno tranzitiven cirkulant $\Gamma = Circ(n; S)$ normalen. Potem velja $\alpha K \alpha^{-1} = K$ za $\forall\, \alpha \in \mathrm{Aut}(\Gamma)_0$, kjer je $K = \langle g \rangle$, za $g = (01\dots(n-1))$. Ker je grupa $\langle g \rangle$ ciklična, velja $g^i \in \langle g \rangle$ za $i \in \{0, 1, \dots, n-1\}$. To pomeni, da je za normalnost dovolj preveriti le, da velja

$$\alpha g \alpha^{-1} \in \langle g \rangle \ \text{ za } \forall\, \alpha \in Aut(\Gamma)_0,$$

saj v tem primeru velja tudi $\alpha g^i \alpha^{-1} \in \langle g \rangle$, saj je

$$\alpha g^i \alpha^{-1} = \underbrace{\underbrace{\alpha g \alpha^{-1}}_{\in\langle g\rangle}\underbrace{\alpha g \alpha^{-1}}_{\in\langle g\rangle}\dots\underbrace{\alpha g \alpha^{-1}}_{\in\langle g\rangle}}_{i \text{ krat}}, \langle g\rangle \text{ pa je grupa.}$$

Naprej velja

$$\alpha(01\dots(n-1))\alpha^{-1} = (\alpha(0)\,\alpha(1)\dots\alpha(n-1)).$$

Ker je $\alpha \in \mathrm{Aut}(\Gamma)_0$, sledi, da je $\alpha(0) = 0$, torej je

$$(\alpha(0)\,\alpha(1)\dots\alpha(n-1)) = (0\ \alpha(1)\dots\alpha(n-1)).$$

Ker je $(0\ \alpha(1)\dots\alpha(n-1)) \in \langle(01\dots n-1)\rangle$ sledi, da je

$$\alpha(j) = j\cdot\alpha(1) \pmod n \text{ za vse } j \in \{1,\dots,n-1\}.$$

Vsak $\alpha \in \mathrm{Aut}(\Gamma)_0$ je torej oblike

$$\alpha = \begin{pmatrix} 0 & 1 & 2 & \dots & (n-1) \\ 0 & z & 2z & \dots & (n-1)z \end{pmatrix}, \text{ za nek } z \in \mathbb{Z}_n^*.$$

Naj bo $H = \{z_\alpha : \alpha \in \mathrm{Aut}(\Gamma)_0\} \leq \mathbb{Z}_n^*$, pri čemer je $\alpha(q) = z_\alpha q$. Po lemi 4.4 stabilizator točke 0, torej $\mathrm{Aut}(\Gamma)_0$, deluje tranzitivno na sosedih točke 0, kar je ravno povezavna množica S. Torej je $S = \mathcal{O}_{Aut(\Gamma)_0}(q) = \{z_\alpha q : \alpha \in \mathrm{Aut}(\Gamma)_0\} = Hq$. □

Opomba 4.20. Paziti moramo, da v trditvi 4.19 govorimo le o normalnih cirkulantih, ki so hkrati tudi ločno tranzitivni in da trditve 4.19 ne moremo posplošiti kar na celotno družino normalnih cirkulantov. Na primer, ne-ločno tranzitiven cirkulant $\mathrm{Circ}(7;\{\pm1,\pm2\})$ je normalen, vendar $\{\pm1,\pm2\}) \not\leq \mathbb{Z}_7^*$.

Rezultati tega razdelka nas pripeljejo do ugotovitve, da pri iskanju ločno tranzitivnih cirkulantov programa MAGMA pravzaprav sploh ne potrebujemo. Če združimo Kovácsev izrek, trditvi 4.14 in 4.15 ter izreka 4.18 in 4.19, znamo med vsemi cirkulanti poljubnega reda ugotoviti kateri so ločno tranzitivni. To storimo na sledeč način. Med cirkulanti poljubnega reda n najprej poiščemo take, ki imajo za povezavno množico $S \leq \mathbb{Z}_n^*$. Torej najprej poiščemo vse podgrupe grupe $\mathbb{Z}_n^*$, med njimi pa izberemo vse take, ki so zaprte tudi za aditivne inverze. Vsem tako najdenim cirkulantom določimo še njihove izomorfne grafe, ki so, po izreku 3.29, ravno cirkulanti s povezavno množico oblike qS, kjer je $q \in \mathbb{Z}_n^*$. Nato poiščemo cirkulante reda n, ki jih lahko zapišemo kot leksikografski produkt oziroma izbrisani leksikografski produkt manjšega ločno tranzitivnega cirkulanta in praznega grafa. Če dodamo še polni graf reda n, res dobimo vse ločno tranzitivne cirkulante reda n.

5 ZAKLJUČEK

V tem magistrskem delu smo obravnavali simetrije cirkulantnih grafov. Najprej smo se omejili na točkovno tranzitivne grafe praštevilskega reda in ugotovili, da so to pravzaprav cirkulantni grafi. Določili smo jim grupo avtomorfizmov, natanko določili, kdaj sta dva cirkulanta praštevilskega reda izomorfna, ter za posamezno praštevilsko vrednost določili število paroma neizomorfnih cirkulantov tega reda. Točkovno tranzitivni grafi praštevilskega reda pa seveda predstavljajo le majhno množico med točkovno tranzitivnimi grafi. Kot nadaljevanje študije o točkovno tranzitivnih grafih bi se tako lahko lotili preučevanja točkovno tranzitivnih grafov reda $2p$, p^k ali pq.

V zadnjem poglavju smo se lotili še vprašanja o povezavni in ločni tranzitivnosti cirkulantov. Ugotovili smo, da je cirkulant povezavno tranzitiven natanko tedaj, ko je ločno tranzitiven. S pomočjo programa MAGMA smo poiskali vse ločno tranzitivne cirkulante reda največ 30 in jih predstavili v tabeli. Preko tabele smo nato ugotovili in kasneje tudi dokazali, da so cirkulanti $\mathrm{Circ}(p; S)$ praštevilskega reda p ločno tranzitivni natanko tedaj, ko je $S = Hq$, za nek $q \in \mathbb{Z}_n^*$ in $H \leq \mathbb{Z}_n^*$. Ugotovili smo tudi, da vsi ločno tranzitivni cirkulanti praštevilskega reda p, ki imajo $|S| < p - 1$, spadajo v družino normalnih cirkulantov. Na koncu smo se osredotočili še na normalne ločno tranzitivne cirkulante poljubnega reda. Prišli smo do zaključka, da za vsak normalen ločno tranzitiven cirkulant $\mathrm{Circ}(n; S)$, velja, da je $S = Hq$, za nek $q \in \mathbb{Z}_n^*$ in $H \leq \mathbb{Z}_n^*$.

Literatura

[1] C.M. Ablow in J.L. Brenner, Roots and Canonical Forms for Circulant Matrices, *Trans. Amer. Math. Soc.* 107 (1963), 360–376.

[2] B. Alspach, Point-Symmetric Graphs and Digraphs of Prime Order and Transitive Permutation Groups of Prime Degree, *Journal of Combinatorial Theory* 15 (1973), 12–17.

[3] N. Biggs, *Algebraic graph theory*, Cambridge: Cambridge University Press, 1979.

[4] P.J. Bentley, *Knjiga o številih*, Tehniška založba Slovenije, 2010.

[5] J.D. Dixon in B. Mortimer, *Permutation groups*, New York: Springer, 1996.

[6] J.B. Fraleigh, *A first course in abstract algebra*, Addison-Wesley, 2003.

[7] C. Godsil in G. Royle, *Algebraic graph theory*, Springer, 2001.

[8] D.F. Holt, A Graph Which Is Edge Transitive But Not Arc Transitive, *Journal of Graph Theory* 5 (1981), 201–204.

[9] I. Kovács, Classifying Arc-Transitive Circulants, *Journal of Algebraic Combinatorics* 20 (2004), 353–358.

[10] D. Marušič in P. Potočnik, Semisymmetry of Generalized Folkman Graphs, *Europ. J. Combinatorics* 22 (2001), 333–349.

[11] M. Strnad, Möbiusov trak, *Presek* vol. 16, št. 6 (1988/1989), 321–327.

[12] G. Sabidussi, On a class of fixed-point-free graphs, *Proc. Amer. Math. Soc.* 9 (1958), 800–804.

[13] J. Turner, Point-Symmetric Graphs with a Prime Number of Points, *Journal of Combinatorial Theory* 3 (1967), 136–145.

[14] P. Potočnik, *Zapiski predavanj iz Diskretne Matematike 1*, Ljubljana, samozaložba, 2011.

[15] I. Vidav, *Višja matematika 1*, Ljubljana, DMFA - založništvo, 2008.

[16] B.L. van der Waerden, *Modern Algebra*, Ungar, New York, 1953.

[17] R.J. Wilson in J.J. Watkins, *Uvod v teorijo grafov*, Ljubljana, Društvo matematikov, fizikov in astronomov Slovenije, 1997.

[18] Arthur Cayley.
URL: http://www-groups.dcs.st-and.ac.uk/history/Biographies/Cayley.html (15.4.2013)

[19] Circulants. URL: http://www.circulants.org/circ/Chapter01.pdf (17.4.2013)

[20] Dihedral.
URL: http://upload.wikimedia.org/wikipedia/commons/9/96/Dihedral8.png (24.4.2013)

[21] Evariste Galois.
URL: http://www-groups.dcs.st-and.ac.uk/history/Mathematicians/Galois.html (12.4.2013)

[22] J. L. Lagrange.
URL: http://www-groups.dcs.st-and.ac.uk/∼history/Mathematicians/Lagrange.html (5.1.2014)

[23] Mobius strip.
URL: http://www.wpclipart.com/signs_symbol/optical_illusions/illusions_2/Mobius_Strip.png.html (17.4.2013)