UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN
INFORMACIJSKE TEHNOLOGIJE

Magistrsko delo

Normalni Cayleyjevi digrafi

(Normal Cayley digraphs)

Ime in priimek: Gresa Jakupi
Študijski program: Matematične znanosti, 2. stopnja
Mentor: izr. prof. dr. Ademir Hujdurović

Koper, september 2022

Ključna dokumentacijska informacija

Ime in PRIIMEK: Gresa JAKUPI

Naslov magistrske naloge: Normalni Cayleyjevi digrafi

Kraj: Koper

Leto: 2022

Število listov: 62 Število slik: 16 Število referenc: 24

Mentor: izr. prof. dr. Ademir Hujdurović

UDK: 519.17(043.2)

Ključne besede: normalni Cayleyjevi digrafi, teorija grafov, vozliščno tranzitivni digrafi

Math. Subj. Class. (2020):

Izvleček:
V magistrskem delu so predstavljeni normalni Cayleyjevi digrafi. V uvodnem poglavju so zapisane definicije in izreki iz področja toerije končnih grup, teorije permutacijskih števil in teorije grafov, ki služijo kot podlaga za nadaljnje vsebine. V naslednjem poglavju so predstavljeni Cayleyjevi (di)grafi skupaj s primeri. Osrednje poglavje tega dela je normalni Cayleyjevi (di)grafi, kjer smo podali zadostne pogoje za normalnost Cayleyjevih digrafov na abelovih grupah. Predstavili smo primere normalnih in nenormalnih Cayleyjevih (di)grafov, na koncu še primer grafa, ki je hkrati normalen in nenormalen Cayleyjev graf za isto grupo. V zadnjem poglavju je prikazana klasifikacija ločno tranzitivnih cirkulantov, ki dokaže, da so ločno tranzitivni cirkulanti bodisi normalni bodisi pripadajo družini grafov, ki jih dobimo z leksikografskimi produkti.

Key document information

Name and SURNAME: Gresa JAKUPI

Title of Master's thesis: Normal Cayley digraphs

Place: Koper

Year: 2022

Number of pages: 62 Number of figures: 16 Number of references: 24

Mentor: Assoc. Prof. Ademir Hujdurović, PhD

UDC: 519.17(043.2)

Keywords: normal Cayley digraphs, graph thoery, vertex transitive digraphs

Math. Subj. Class. (2020):

Abstract:
In the master's thesis are presented normal Cayley digraphs. The introductory chapter contains definitions and theorems from the fields of finite group theory, permutation number theory and graph theory, which serve as a basis for further content. In the next chapter, Cayley (di)graphs are presented with examples. The most important chapter of this work is normal Cayley (di)graphs, where we have given sufficient conditions for the normality of Cayley digraphs on abelian groups. We presented examples of normal and nonnormal Cayley (di)graphs and in the end an example of a graph that is at the same time a normal and an nonnormal Cayley graph for the same group. In the last chapter, the classification of arc-transitive circulants is shown, which proves that arc-transitive circulants are either normal or belong to the family of graphs obtained by lexicographic products.

Zahvala

Najprej bi se rada zahvalila svojemu mentorju, izr. prof. dr. Ademirju Hujduroviću, za hitro odzivnost, strokovno pomoč, nasvete ter usmerjanje pri pisanju magistrskega dela.

Iskreno sem hvaležna tudi vsem profesorjem, asistentom in zaposlenim na fakulteti. Zahvaljujem se za vso prijaznost, potrpežljivost in prijetno vzdušje, ki ga ustvarjate. Predvsem pa za veliko uporabnega znanja, ki ste nam predali.

Nazadnje bi se rada zahvalila tudi moji družini za vso podporo, spodbudo in potrpežljivost v vseh letih mojega študija.

Kazalo vsebine

Kazalo slik in grafikonov

Seznam kratic

gcd največji skupni delitelj
itn. in tako naprej
npr. na primer
oz. oziroma
tj. to je

1 UVOD

Osrednja tema mojega magistrskega dela so normalni Cayleyjevi digrafi. Cayleyjevi digrafi so najpogosteje preučevan in najpogosteje srečan razred vozliščno tranzitivnih digrafov. Na začetku predstavimo osnovne rezultate iz teorije končnih grup, permutacijskih grup in teorije grafov. Nato definiramo Cayleyjeve digrafe ter predstavimo osnovne lastnosti Cayleyjevih digrafov.

Naj bo G grupa in $S \subseteq G$, Cayleyjev digraf definiramo kot **Cayleyjev digraf** G in ga označimo s $Cay(G, S)$, z množico vozlišč $V(Cay(G, S)) = G$ in množico lokov $A(Cay(G, S)) = \{(g, gs) : g \in G, s \in S\}$. S je **generatorska množica** $Cay(G, S)$.

Med osnovnimi lastnostmi Cayleyjevih digrafov, ki smo jih predstavili, so naslednji rezultati.

- Digraf $Cay(G, S)$ je graf če in samo če je $S = S^{-1}$ (zapisano additivno $S = -S$).
- Naj bo G grupa in $S \subseteq G$. Cayleyev digraf $Cay(G, S)$ je krepko povezan če in samo če je $\langle S \rangle = G$.
- Digraf Γ je izomorfen Cayleyjevemu digrafu grupe G če in samo če $Aut(\Gamma)$ vsebuje regularno podgrupo, izomorfno G.

Glavni del magistrske naloge je obravnava normalnih Cayleyjevih digrafov, in sicer Cayleyjev digraf $Cay(G, S)$ je normalen Cayleyjev digraf grupe G, če je $G_L \trianglelefteq Aut(Cay(G, S))$.

Dokazali smo naslednjo karakterizacijo normalnih Cayleyjevih digrafov. Naj bo G grupa. Cayleyjev digraf $\Gamma = Cay(G, S)$ od G je normalen Cayleyjev digraf G, če in samo če je $Stab_{Aut(\Gamma)}(1_G) \leq Aut(G)$. Ekvivalentno $Stab_{Aut(\Gamma)}(1_G) = Aut(G, S)$.

V tem delu so podani zadostni pogoji za normalnost Cayleyjevih digrafov na abelovih grupah ter so s pomočjo tega rezultata določeni vsi nenormalni Cayleyjevi grafi na abelovih grupah valence največ 4. Predstavljeni so tudi primeri grafov, ki so hkrati normalni Cayleyjevi digrafi za eno grupo ter nenormalni Cayleyjevi digrafi za drugo grupo.

2 OSNOVNE DEFINICIJE

V tem poglavju so navedene osnovne definicije in izreki, ki jih potebujemo za razumevanje magistrske naloge, in ki so povzeti iz naslednjih virov: [22], [6] [8]

2.1 TEORIJA KONČNIH GRUP

Ker v nadaljevanju govorili o grupah, ki delujejo na grafe, začnemo z nekaterimi osnovnimi definicijami in rezultati teorije permutacijskih grup in teorije grafov. Poudarjamo, da je naše množenje permutacij na levi. To pomeni, da je $fg(x) = f(g(x))$. Zavedati se moramo, da včasih v literaturi množenje permutacij je zapisano na desni.

2.1.1 Množice in preslikave

V tem kratkem poglavju predstavljamo (ali v mnogih primerih spomnili) nekaj osnovnih konceptov, ki se uporabljajo v besedilu. Primerno jih bo navesti na začetku, da so vsi na istem mestu.

Množica je zbirka predmetov, imenovanih elementi X. Če je X množica, bo zapis $x \in X$ pomenil, da je x element X. Množice so pogosto definirane v smislu lastnosti. Na primer, če $\mathbb{R}$ označuje množico vseh realnih števil, potem je množica vseh pozitivnih realnih števil označena z izrazom $\{r \in \mathbb{R} \mid r > 0\}$. Množico lahko definiramo tudi tako, da naštejemo njene elemente. Primer je množica, sestavljena iz celih števil $1, 2$ in 3, ki jih lahko označimo bodisi

$$\{1, 2, 3\},$$

bodisi bolj nerodno,

$$\{r \in \mathbb{R} \mid r \text{ je celo število in } 1 \leq r \leq 3\}.$$

Unija dveh množic X in Y je množica

$$X \cup Y = \{a \mid a \in X \text{ ali } a \in Y\}$$

katerih elementi so elementi X skupaj z elementi Y .

Presek X in Y je množica

$$X \cap Y = \{a \mid a \in X \text{ in } a \in Y\}.$$

Razlika X in Y je množica

$$X \setminus Y = \{x \in X \mid x \notin Y\}.$$

Upoštevajmo, da ni treba, da je Y podmnožica X, da lahko govorimo o razliki $X \setminus Y$. Upoštevajmo, da sta unija in razlika množice analogni seštevanju in odštevanju. Presek je nekoliko podobno množenju. Na primer, za poljubne tri množice X, Y, Z velja

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z),$$

kar je analogno distribucijskemu zakonu $a(b + c) = ab + ac$ za realna števila a, b, c. **Produkt** X in Y je množica

$$X \times Y = \{(x, y) \mid x \in X \text{ in } y \in Y\}.$$

(x, y) imenujemo **urejen par**. To pomeni, da ko je $X = Y$, potem $(x, y) \neq (y, x)$, razen če je $x = y$. Produkt $X \times X$ lahko označimo z X^2. Na primer, $\mathbb{R} \times \mathbb{R}$ je kartezična ravnina, običajno označena z $\mathbb{R}^2$.

Preslikava iz X v Y je pravilo f, ki vsakemu elementu $x \in X$ dodeli edinstven element $f(x) \in Y$. Zapis $f : X \to Y$ bo uporabljen za označevanje preslikave iz X v Y; X imenujemo **domena** f, Y pa njegova **kodomena**. Slika f je

$$f(X) = \{y \in Y \mid y = f(x) \text{ za nekatere } x \in X\}.$$

Na primer, če je $f : \mathbb{R} \to \mathbb{R}$ preslikava $f(r) = r^2$, potem je $f(\mathbb{R})$ množica vseh nenegativnih realnih vrednosti. **Kompozitum** dveh preslikav $f : X \to Y$ in $G : W \to X$ je preslikava $f \circ G : W \to Y$, definirana z $G \to f(w) = f(G(w))$. Kompozitum $f \circ G$ je definirana vedno, ko je domena f vsebovana v sliki G.

2.1.2 Binarne operacije

Definicija 2.1. Binarna operacija na množici X je funkcija

$$f : X \times X \to X$$

.

Primer 2.2. Naj $\mathbb{Z}$ označuje množico celih števil. Na $\mathbb{Z}$ obstajata dve binarni operaciji, imenovani seštevanje in množenje. Definirana sta s $f_+(m, n) = m+n$ in $f_\cdot(m, n) = mn$. Upoštevajmo, da deljenje ni binarna operacija na $\mathbb{Z}$.

Potrebujemo tudi pojem podmnožice, ki je zaprta.

Definicija 2.3. Naj bo f binarna operacija na množici A. Podmnožica B množice A, taka da je $f(x, y) \in B$, kadar koli je $x, y \in B$, je **zaprta**.

Na primer, naj bo $A = \mathbb{Z}$ in naj bo B množica vseh nenegativnih celih števil. Potem je B zaprta tako glede seštevanja kot množenja. Liha cela števila so zaprta pri množenju, niso pa zaprta pri seštevanju, saj je na primer $1 + 1 = 2$.

Če je f preslikava iz X v Y in $y \in Y$, potem je **praslika** od y

$$f^{-1}(y) = \{x \in X \mid f(x) = y\}.$$

Seveda $f^{-1}(y)$ lahko nima nobenih elementov; to je lahko prazna množica. Na primer, če je $f : \mathbb{R} \to \mathbb{R}$ preslikava $f(r) = r^2$, potem je $f^{-1}(-1)$ prazen. Upoštevajmo, da če je $y \neq y'$, potem je $f^{-1}(y) \cap f^{-1}(y')$ prazna množica.

Pojem praslike elementa je uporaben pri definiranju nekaterih nadaljnjih lastnosti preslikav. Na primer, preslikava $f : X \to Y$ je **ena proti ena** ali **injektivna**, če in samo če je $f^{-1}(y)$ prazna ali ima en sam element X za vsak $y \in Y$. Z drugimi besedami, f je injektivna, če in samo če $f(x) = f(x')$ implicira $x = x'$. Podobno je f surjektiven, če $f^{-1}(y)$ ni prazen za vse $y \in Y$. Druga možnost je, da je f **surjektivna**, če in samo če je $f(X) = Y$. Preslikava $f : X \to Y$, ki je hkrati injektivna in surjektivna, imenujemo **bijektivna**. Preslikavo, ki je injektivna, surjektivna ali bijektivna, imenujemo injekcija, surjekcija ali bijekcija. Bijektivna preslikava $f : X \to Y$ ima **inverzno preslikavo** f^{-1}, ki je definirana tako, da je $f^{-1}(y) = x$, če in samo če je $f(x) = y$. Neposredno iz definicije sledi $f^{-1} \circ f(x) = x$ in $f \circ f^{-1}(y) = y$ za vsak $x \in X$ in $y \in Y$.

Naslednja trditev podaja merila za injektivnost in surjektivnost.

Trditev 2.4. *Predpostavimo, da je $f : X \to Y$ preslikava in predpostavimo, da obstaja preslikava $g : Y \to X$, taka da je $g \circ f(x) = x$ za vsak $x \in X$. Potem je f injektivna in g surjektivna. Poleg tega je f bijektivna, če in samo če sta $g \circ f$ in $f \circ g$ identitetni preslikavi na X oziroma Y.*

2.1.3 Grupe

Pojem grupe vključuje množico z binarno operacijo, ki zadošča trem naravnim lastnostim. Preden navedemo definicijo, omenimo nekaj osnovnih, vendar zelo različnih primerov, ki jih je treba upoštevati. Prva so cela števila pod operacijo seštevanja. Druga pa je množica vseh bijekcij množice glede na operacijo kompozituma. Sedaj navedemo definicijo.

Definicija 2.5. Grupa je množica G z binarno operacijo, zapisano $(x, y) \to xy$, tako da

(i) $(xy)z = x(yz)$ za vsak $x, y, z \in G$;

(ii) G vsebuje nevtralni element (identiteto) 1, tako da je $1x = x1 = x$ za vsak $x \in G$, in

(iii) za vsak $x \in G$, potem obstaja $y \in G$, tako da je $xy = 1$. V tem primeru pravimo, da ima vsak element G **desni inverz**.

Lastnost (i) imenujemo asociativni zakon. Z drugimi besedami, delovanje grupe je asociativno. V teoriji grup je običajna uporaba črke e za označevanje identitete. Upoštevajmo, da lastnost (iii) vključuje zmožnost reševanja enačbe, ki je poseben primer enačbe $ax = b$. Obstaja več dodatnih lastnosti, ki jih lahko vsilimo za definiranje posebnih razredov grup. Na primer, lahko zahtevamo, da je operacija grupe neodvisna od vrstnega reda, v katerem vzamemo elemente grupe. Natančneje podajamo naslednjo definicijo.

Definicija 2.6. Za grupo G pravimo, da je **komutativna** ali **abelova**, če in samo če za vsak $x, y \in G$ velja $xy = yx$. Za grupo, ki ni abelova, pravimo, da **ni komutativna**.

Primer 2.7. (Cela števila) Cela števila $\mathbb{Z}$ tvorijo grupo pri seštevanju. Dejstvo, da je seštevanje asociativno, je dobro znano. Ničla je aditivna identiteta. Pravzaprav je to edina dodatna identiteta. Aditivni inverz $m \in \mathbb{Z}$ je njegov negativni $-m : m+(-m) = 0$. Poleg tega je $\mathbb{Z}$ abelova: $m + n = n + m$ za vsak $m, n \in \mathbb{Z}$.

Grupa $G = \{1, -1\}$ pri množenju je še enostavnejši primer abelove grupe.

Definicija 2.8. Grupa G je **končna**, če je število $|G|$ elementov v množici G končna. Označili bomo z $|G|$ red grupe G.

Red $G = \{1, -1\}$ je dva, medtem ko je $\mathbb{Z}$ neskončna grupa.

Preden preidemo na več primerov grup, bomo dokazali trditev, ki daje nekaj osnovnih posledic definicije grup. Dokazali bomo, da obstaja samo en identitetni element 1, prav tako pa bomo dokazali, da ima vsak element x v grupi natanko določen obojestranski inverz x^{-1}. Preden navedemo trditev, se spomnimo, da smo ta dejstva opazili že pri $\mathbb{Z}$: obstaja samo ena aditivna identiteta, 0, in prav tako samo en desni inverz, $-m$, za vsak m. Poleg tega je $-m$ tudi levi inverz od m. Te lastnosti so običajno navedene kot del definicije grupe, vendar smo se odločili za uporabo minimalnega nabora aksiomov grupe.

Trditev 2.9. *V vsaki grupi je natanko en identitetni element,* 1*. Nadalje, če je* y *desni inverz od* x*, potem je* $xy = yx = 1$*. Zato je desni inverz tudi levi inverz. Zato ima vsak* $x \in G$ *obojestranski inverz* y*, za katerega je značilna lastnost, da je* $xy = 1$ *ali* $yx = 1$*. Poleg tega je vsak obojestranski inverz natanko določen.*

Dokaz. Da bi dokazali edinstvenost 1, predpostavimo, da sta 1 in $1'$ oba elementa identitete. Potem je $1 = 11' = 1'$. Tako je identiteta edinstvena.

Naj ima zdaj x desni inverz y in naj bo w desni inverz od y. Potem

$$w = 1w = (xy)w = x(yw) = x1 = x.$$

Ker je $w = x$, sledi, da če je $xy = 1$, potem je $yx = 1$. Tako je vsak desni inverz obojestranski inverz. □

Odslej bomo natanko določeni levi ali desni inverz od x imenovali **inverz od** x. Zapis za inverz od x je x^{-1}. Naslednji rezultat je formula za inverz produkta.

Trditev 2.10. *Za vsak* $x, y \in G$ *velja* $(xy)^{-1} = y^{-1}x^{-1}$.

Dokaz. Naj bo $w = y^{-1}x^{-1}$. Potem zadošča pokazati, da je $w(xy) = 1$. Toda

$$w(xy) = (wx)y = ((y^{-1}x^{-1})x)y = (y^{-1}(x^{-1}x))y = (y^{-1}1)y = y^{-1}y = 1.$$

□

Če so $x_1, x_2, \ldots, x_n$ poljubni elementi grupe G, potem bo izraz $x_1x_2 \cdots x_n$ stal za $x_1(x_2 \cdots x_n)$, kjer je $x_2 \cdots x_n = x_2(x_3 \cdots x_n)$ in tako naprej. To daje indukcijo produkta poljubnega končnega števila elementov G. Poleg tega lahko zaradi asociativnosti pare $(\cdots)$ oklepajev vstavimo ali odstranimo v izrazu $x_1x_2 \cdots x_n$, ne da bi pri tem spremenili izraz elementov grupe, če je novi izraz smiseln (na primer, ne moremo imeti praznega para oklepajev in število levih oklepajev mora biti enako številu desnih oklepajev). Tako lahko izračun v dokazu trditve 2.10 poenostavimo na

$$(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y^1 = y1y^{-1} = 1.$$

Simetrične grupe $\mathbf{S_n}$

Zdaj smo prišli do **simetričnih grup**, znanih tudi kot **permutacijske grupe**. Tvorijo najpomembnejši razred končnih grup. Vse simetrične grupe reda, večjega od dva, niso abelove. Simetrična grupa je nedvomno najpogostejša končna grupa v matematiki.

Naj X označuje množico. Bijektivno preslikavo $\sigma : X \to X$ bomo imenovali **permutacija** X. Množica vseh permutacij X je označena s $Sym(X)$ in se imenuje **simetrična grupa** X. Ko je $X = \{1, 2, \ldots, n\}$, $Sym(X)$ označimo s S_n in imenujemo **simetrična grupa na** n **črkah**.

Če ni navedeno drugače, bomo n črk, ki jih S_n permutira, šteli za elemente množice $\mathbb{Z}_n$, celih števil po modulu n.

Trditev 2.11. *Množica $Sym(X)$ permutacij X je grupa pod kompozicijo, katere identitetni element je identitetna preslikava $id_X : X \to X$. Če $|X| = n$, potem $|Sym(X)| = n!$.*

Definicija 2.12. Permutacija $\rho \in S_n$ je **soda**, če jo lahko zapišemo kot produkt sodega števila transpozicij, in **liha**, če jo lahko zapišemo kot produkt lihega števila transpozicij. Množica vseh sodih permutacij v S_n je podgrupa, ki se imenuje **alternirajoča grupa** na n črkah in jo označimo z A_n.

Spomnimo se, da lahko vsako permutacijo v S_n zapišemo kot **produkt transpozicij** in to število je vedno sodo ali vedno liho.

V naslednjem primeru obravnavamo shemo za zapis elementov S_3, ki se zlahka posploši na S_n za vsak $n > 0$. Videli bomo tudi, da S_3 ni abelova.

Primer 2.13. Za zapis šestih elementov σ od S_3 potrebujemo način za kodiranje σ_1, σ_2 in σ_3. Da bi to naredili, predstavimo σ s poljem

$$\begin{pmatrix} 1 & 2 & 3 \\ \sigma_1 & \sigma_2 & \sigma_3 \end{pmatrix}.$$

Na primer, če je $\sigma_1 = 2, \sigma_2 = 3$ in $\sigma_3 = 1$, potem

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Dopolnitev seznama elementov S_3 bomo prepustili bralcu. Če je $n > 2$, potem S_n ni abelov: vrstni red, v katerem sta uporabljeni dve permutaciji, je pomemben. Na primer, če je $n = 3$ in

$$\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

potem

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

medtem

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

Zato je $\sigma\tau \neq \tau\sigma$.

Ciklične grupe

Definicija 2.14. Naj bo G grupa in $x \in G$, tako da

$$\langle x \rangle = \{x^n : n \in \mathbb{Z}\}$$

je ciklična podgrupa od G, ki jo **generira** element x, in je najmanjša podgrupa grupe G, ki vsebuje element x.
G je **ciklična grupa**, če obstaja $x \in G$, tako da je $\langle x \rangle = G$. x je **generator** grupe G. Ciklično grupo reda n pa označimo z Z_n.

Še posebej je $\mathbb{Z}$ primer neskončne ciklične grupe, v kateri se z^m interpretira kot mz. Tudi multiplikativna grupa $G = \{1, -1\}$ je ciklična. Aditivne grupe $\mathbb{Z}_m$, sestavljene iz celih števil po modulu pozitivnega celega števila m, tvorijo pomemben razred cikličnih grup. $\mathbb{Z}_m$ je grupa ostankov pri deljenju z m. So gradniki končnih (pravzaprav končno generiranih) abelovih grup. Upoštevajmo, da so vse ciklične grupe abelove. Vendar pa ciklične grupe niso tako pogoste. Na primer, $S(3)$ ni ciklična, prav tako niti $\mathbb{Q}$, aditivna grupa racionalnih števil.

Definicija 2.15. Naj bo $\sigma \in S_n$. Če obstaja niz $x_1, x_2, \ldots, x_r \in \{1, 2, \ldots, n\}$, tak da je

$$\sigma(x_i) = x_{i+1} (i = 1, 2, \ldots, r-1)$$

$$\sigma(x_r) = x_1 (i = 1, 2, \ldots, r-1)$$

$$\sigma(x) = x (x \notin \{x_1, x_2, \ldots, x_r\})$$

tedaj permutacijo σ označimo z $(x_1 x_2 \ldots x_{r-1} x_r)$ in jo imenujemo **cikel dolžine** r. Cikel dolžine dva (2-cikel) se imenuje **transpozicija**.

Dva cikla $(a_1 a_2 \ldots a_r)$ in $(b_1 b_2 \ldots b_s)$ sta disjunktna, če in samo če sta množici $\{a_1, a_2, \ldots, a_r\}$ in $\{b_1, b_2, \ldots, b_s\}$ disjunktni.

Spomnimo se, da je permutacija $\sigma \in S_n$ **soda**, če se lahko napiše kot produkt sodo mnogih transpozicij. Permutacija $\sigma \in S_n$ je **liha**, če ni soda.

Definicija 2.16. Naj bo $n \in \mathbb{N}$,

$$\varphi(n) = \#(\{m \in \mathbb{Z} \mid 0 \leq m < n \text{ in } gcd(m, n) = 1\}).$$

Z drugimi besedami, $\varphi(n)$ šteje število nenegativnih celih števil, manjših od n, ki so relativno praštevila do n. To se imenuje **Eulerjeva φ funkcija**.

Primer 2.17. Naj bo $n \in \mathbb{N}$. Množica celih števil po modulu n je ciklična grupa, imenovana grupa pod operacijo seštevanja po modulu n.

Naj bo $G = \langle g \rangle$, kjer je $|G| = n$. Na splošno pišemo

$$G = \{1, g, \ldots, g^{n-1}\}$$

Opazimo, da je G abelova in vsaka podgrupa G je tudi ciklična. Če je d delitelj n, potem je število elementov v G, ki imajo red d $\varphi(d)$ (φ se imenuje Eulerjeva φ funkcija) in G vsebuje enolično določeno podgrupo reda d. Naj bo $x \in G$ in je torej $x = g^r$ za nek $0 \leq r \leq n-1$. Red x je $\frac{n}{gcd(n,r)}$. Znano je tudi, da je grupa praštevilskega reda ciklična.

Izrek 2.18. *Vsaka ciklična grupa reda n je izomorfna grupi $\mathbb{Z}_n$.*

Kadar je G končna ciklična grupa in je $x \in G$ generator G, pogosto pišemo $G = \langle x \rangle$. Izkaže pa se, da lahko ima končna ciklična grupa več generatorjev, zato izraz $G = \langle x \rangle$ ni nujno natanko določen. Če želimo videti primer tega, razmislimo o štiriindvajseturni uri kot končni ciklični grupi. To je predogled grupe $\mathbb{Z}_m$ celih števil po modulu m, kjer je $m = 24$.

Primer 2.19. Vzemimo uro s 24 urami, oštevilčenimi od 0 do 23. Operacija grupe na tej uri je časovni premik za neko celo število n ur. Časovni premik naprej se pojavi, ko je n pozitiven, časovni premik nazaj pa, ko je n negativen. Ko je $n = 0$, ne pride do premika, zato bo ura 0 identiteta. Enourni časovni premik pri 23 urah pošlje čas na 0 ur, medtem ko dvourni časovni premik pošlje 23 ur na 1 uro in tako naprej. Z drugimi besedami, operacija grupe je seštevanje po modulu 24. Inverz pa je, recimo, deveta ura je petnajsta ura. Dve uri sta inverz druga drugi, če premik eno za drugo postavi čas na 0 ur. Zaradi tega je 24-urna ura v grupi reda 24, ki je v resnici ciklična, saj nas lahko večkratni premik časa za eno uro, ki se začne pri 0 urah, postavi na katero koli uro. Vendar pa obstajajo tudi drugi generatorji, katere ne bomo iskali v tem delu.

Trditev 2.20. *Naj bo $G = \langle g \rangle$ ciklična grupa reda n. Potem*

1. *$G \cong \mathbb{Z}_n$;*
2. *$Z_n \cong \mathbb{Z}_{2^{k_0}} \times \mathbb{Z}_{{p_1}^{k_1}} \times \cdots \times \mathbb{Z}_{{p_t}^{k_t}}$, kjer je $2^{k_0} p_1^{k_1} \cdots p_t^{k_t}$ enolično določena faktorizacija števila n.*

Trditev 2.21. *Naj bo $G = Z_{p^k} = \langle g \rangle$, kjer je p praštevilo.*

- *Če je $p = 2$ in $k = 1$, potem $Aut(\mathbb{Z}_2) \cong \{1\}$*
- *Če je $p = 2$ in $k \geq 2$, potem je $Aut(G) \cong Z_2 \times Z_{2^{k-2}}$*
- *Če je p liho, potem je $Aut(G) \cong Z_{p^{k-1}(p-1)}$.*

Diedrske grupe

Diedrske grupe so permutacijske grupe pravilnih mnogokotnikov v ravnini.

Primer 2.22. (Diedrske grupe) Diedrske grupe so grupe, ki so definirane z določitvijo dveh generatorjev a in b ter z določitvijo relacij, ki jih generatorji izpolnjujejo. Ko definiramo grupo z generatorji in relacijami, upoštevamo vse besede v generatorjih, v tem primeru a in b: to so vsi nizi ali produkti $x_1x_2\cdots x_n$, kjer je vsak x_i bodisi a bodisi b, n pa poljubno pozitivno celo število. Na primer, $abbaabbaabba$ je beseda z $n = 16$. Dve besedi pomnožimo tako, da ju postavimo eno poleg druge, torej

$$(x_1x_2\cdots x_n)(y_1y_2\cdots y_p) = x_1x_2\cdots x_ny_1y_2\cdots y_p.$$

To ustvari asociativno binarno operacijo na nizu besed. Naslednji korak je vsiliti nekaj odnosov, ki jih izpolnjujeta a in b. Recimo, da je $m > 1$. Diedrska grupa $D(m)$ je definirana kot množica vseh besed v a in b z zgornjim množenjem, za katerega predpostavljamo, da je predmet naslednjih odnosov:

$$a^m = b^2 = 1, ab = ba^{m-1}. \tag{2.1}$$

Razume se, da imata ciklični grupi $\langle a\rangle$ in $\langle b\rangle$ red m oziroma dva. Po (2.72) je $a^{-1} = a^{m-1}$ in $b = b^{-1}$. Na primer, če je $m = 3$, potem $a^3 = b^2 = 1$, torej

$$aaababbbb = (aaa)(bab)(ab)(bb) = (a^2)(ab) = a^3b = b.$$

Primer 2.23. Preverimo zdaj, ali je $D(2)$ grupa. Ker je množenje besed asociativno, sledi iz zahteve $a^2 = b^2 = 1$ in $ab = ba$, da je mogoče vsako besedo strniti v eno od $1, a, b, ab, ba$. Toda $ab = ba$, torej $D(2) = \{1, a, b, ab\}$. Opazimo, da je $D(2)$ zaprta glede na množenje in da je $a(ab) = a^2b = b, b(ab) = (ba)b = ab^2 = a, (ab)a = (ba)a = ba^2 = bin(ab)(ab) = (ba)(ab) = ba^2b = b^2 = 1$. Zato je $D(2)$ zaprta glede množenja, zato sledi, da je $D(2)$ grupa. Upoštevajmo, da je red $D(2)$ enak 4.

Definicija 2.24. Diedrska grupa D_{2n} reda $2n$ je simetrija pravilnega n-kotnika in ima predstavitev $\langle \rho, \tau : \rho^n = \tau^2 = 1, \tau^{-1}\rho\tau = \rho^-1\rangle$.

2.1.4 Podgrupe

Sedaj izločimo najpomembnejše podmnožice grup: in sicer tiste, ki so tudi grupe.

Definicija 2.25. Neprazna podmnožica H grupe G se imenuje **podgrupa** G, če kadar koli je $x, y \in H$, imamo $xy^{-1} \in H$.

Ker je vsaka podgrupa neprazna, vsaka podgrupa H grupe G vsebuje identiteto grupe G, torej tudi inverze vseh njenih elementov. Poleg tega je H po definiciji zaprt glede na operacijo grupe G. Nazadnje, asociativnost operacije grupe na H izhaja iz njene asociativnosti v G. Posledično je vsaka podgrupa G tudi grupa. Tako smo dokazali naslednji rezultat.

Trditev 2.26. *Podmnožica H grupe G je podgrupa, če in samo če je H grupa pod operacijami grupe G. To pomeni, da je H zaprta glede na operacijo grupe in vsebuje identiteto G in inverz elementa H je njegov inverz v G.*

Primer 2.27. Recimo, da G označuje cela števila. Soda cela števila sestavljajo podgrupo G, saj je razlika dveh sodih celih števil soda. Po drugi strani pa liha cela števila ne, saj je razlika dveh lihih celih števil sodo število.

Trditev 2.28. *Naj bo G grupa in predpostavimo, da je H neprazna končna podmnožica G, tako da za vsak $a, b \in H$ velja $ab \in H$. Potem je H podgrupa grupe G.*

Naj bo G končna grupa in H podgrupa grupe G. Spomnimo se, da je 1 trivialna podgrupa grupe G in če je $H \leq G$ in $H \neq G$, potem je H **prava podgrupa grupe** G.

Naj bo $S = \{s_1, \ldots, s_t\}$ neprazna podmnožica G. (Pod)grupa H generirana z S je definirana kot:

$$H = \{x_1^{k_1} \ldots x_r^{k_r} \mid \text{ za vse } 1 \leq i \leq r, x_i \in S \text{ in } r, k_i \in \mathbb{N}\},$$

označimo s $H = \langle S \rangle$. Pravimo, da je S generatorska množica H in elementi od S so generatorji H.

Definicija 2.29. Red grupe G je **kardinalnost grupe** G, označena z $|G|$. Red elementa grupe g je red podgrupe $\langle g \rangle$, označen z $|g|$.

Če $|G|$ je končna, potem rečemo, da je G **končna grupa** (ali preprosto **končna**), sicer pa rečemo, da je G **neskončna grupa** (ali preprosto **neskončna**). V okviru te naloge se predpostavlja, da so vse grupe končne.

Lagrangeov izrek pravi, da red vsake podgrupe H grupe G deli red G in tako red vsakega elementa grupe $g \in G$ deli red G.

Naj bo H podgrupa grupe G in $g \in G$. Množica $gH = \{gh \mid h \in H\}$ pravimo, da je **levi odsek** od H, množica $Hg = \{hg \mid h \in H\}$ pravimo, da je **desni odsek** od H. Na splošno $gH \neq Hg$. Vendar je število levih odsekov H v G enako številu desnih odsekov H. Število različnih levih (desnih) odsekov H v G je **indeks** H v G, označen z $|G : H|$. Natančno, indeks H v G je enak kvocientu redov obeh grup, tj.

$$|G : H| = \frac{|G|}{|H|}.$$

Definicija 2.30. Naj sta g in h dva elementa G. Za element $h^g := g^{-1}hg$ pravimo, da je **konjugiran** h **z** g.

Rečemo, da sta elementa g in g' **konjugirana** v G, če obstaja element $x \in G$, tak da je g' konjugiran z elementom od g z x. Množica

$$g^G = \{g^x \mid x \in G\}$$

se imenuje **razred konjugiranosti** g **v** G. Upoštevajmo, da sta dva elementa g in g' v istem razredu konjugiranosti, če in samo če sta konjugirana v G, zato je G disjunktna unija njegovih razredov konjugiranosti.

Pravimo, da dva elementa g in h **komutirata**, če je $gh = hg$. Če g in h komutirajo v G, potem je konjugacija h z g enaka h, to je $h^g = h$. **Center** G je podmnožica vseh $x \in G$, tako da x komutira z g za vsak $g \in G$, označeno z

$$Z(G) = \{x \mid g^x = g \text{ za vse } g \in G\}.$$

Ni težko opaziti, da je nevtralni element 1 vsebovan v $Z(G)$. Če je G abelova, potem je $Z(G) = G$.

Definicija 2.31. Naj je G grupa in H podgrupa grupe G. **Centralizator** grupe H v G je podgrupa vseh $g \in G$, tako da g komutira z vsakim elementom iz H, označen s $C_G(H)$, in pravimo, da $C_G(H)$ centralizira H.

Opažamo, da G centralizira svoj center $Z(G)$.

Podobno kot pri definiciji 2.30 lahko definiramo 'konjugiranost' za podgrupe grupe G.

Naj bo H podgrupa grupe G. Za podgrupo $H^g := g^{-1}Hg$ pravimo, da je konjugirana podgrupa od H z g.

Definicija 2.32. Naj je G grupa in H podgrupa G. **Normalizator** podgrupe H v G je podgrupa vseh $g \in G$, tako da je $H^g = H$, označen z $N_G(H)$ in pravimo, da $N_G(H)$ normalizira H.

Definicija 2.33. Podgrupa H je **podgrupa edinka grupe** G, če G normalizira H. Pravimo, da je H podgrupa edinka v G, označena s $H \trianglelefteq G$.

Jasno je, da grupa G vsebuje vsaj dve podgrupi edinki, in sicer trivialno podgrupo in samo G. Center $Z(G)$ je tudi podgrupa edinka G. Če je G abelova, potem je vsaka podgrupa G podgrupa edinka v G. Naj bo H podgrupa G in N podgrupa edinka G. Potem je HN podgrupa od G in $H \cap N$ je podgrupa edinka grupe H.

Naj bo N podgrupa edinka grupe G. Potem je $gN = Ng$ za vse $g \in G$. Množico G/N definiramo kot množico vseh levih odsekov podgrupe N od G in definiramo binarno operacijo na G/N, kot je prikazano spodaj: za vse $gN, hN \in G/N$,

$$(gN)(hN) = ghN.$$

Preprosto je videti, da pri takšni binarni operaciji G/N tvori grupo in pravimo, da je G/N **kvocientna grupa** G po N. Red G/N je enak indeksu N v G.

Ta del zaključimo z uvedbo direktnega produkta grup.

Definicija 2.34. Naj bosta G in H dve grupi. **Direktni produkt** G in H je grupa z množico $\{(g,h) \mid g \in G, h \in H\}$ in binarna operacija:

$$(g,h)(g',h') = (gg',hh').$$

Direktni produkt G in H je označen z $G \times H$.

2.1.5 Homomorfizmi grup

Naj bosta G in H grupi.

Definicija 2.35. Preslikava $\phi : G \to H$ je **homomorfizem** iz G v H, če je za vsak $g,h \in G$,

$$\phi(gh) = \phi(g)\phi(h).$$

Definicija 2.36. Jedro homomorfizma $\phi : G \to H$ je množica vseh elementov $g \in G$, takih, da je $\phi(g) = 1$, in ga označujemo s $Ker(\phi)$.

Definicija 2.37. Slika homomorfizma $\phi : G \to H$ je množica vseh elementov $h \in H$, za katere obstaja $g \in G$, tako da je $\phi(g) = h$, in je označen z $Im(\phi)$.

Naj bo $\phi : G \to H$ homomorfizem. Potem je $Ker(\phi)$ podgrupa edinka grupe G in $Im(\phi)$ je podgrupa grupe H.

Definicija 2.38. Homomorfizem $\phi : G \to H$ je **izomorfizem**, če je ϕ bijekcija. Če tak izomorfizem obstaja, potem pravimo, da sta G in H izomorfni in zapišemo $G \cong H$. Izomorfizem iz G na samega sebe je **avtomorfizem** G.

Množica $Aut(G)$ vseh avtomorfizmov G, z množenjem kot spodaj: za vsak $g \in G$ in $\alpha, \beta \in Aut(G)$,

$$g^{\alpha\beta} = (g^{\alpha})^{\beta}$$

tvori grupo, ki se imenuje **grupa avtomorfizmov** od G.

Lema 2.39. *[[13], Izrek 1.6.2] Naj bo $G = G_1 \times \cdots \times G_t$, kjer sta $|G_i|$, $|G_j|$ **tuji števili** za vsak $1 \leq i \neq j \leq t$. Potem*

$$Aut(G) = Aut(G_1) \times \cdots \times Aut(G_t).$$

Izrek 2.40. ***(Prvi izrek o izomorfizmu)*** *Naj bo $\phi : G \to H$ homomorfizem. Potem je $G/Ker(\phi) \cong Im(G)$.*

Izrek 2.41. ***(Drugi izrek o izomorfizmu)*** *Naj bo G grupa, H podgrupa grupe G in N podgrupa edinka grupe G. Potem je $H/(H \cap N) \cong (HN)/N$.*

Primer 2.42. Naj bo G grupa in $g \in G$. Naj bo $\phi_g : G \to G$ definiran kot spodaj: za vsak $x \in G$

$$\phi_g : x \to x^g.$$

Preprosto je preveriti, da je ϕ_g avtomorfizem G, imenovan notranji avtomorfizem, induciran z g. Množico

$$\{\phi_g \mid g \in G\}$$

notranjih avtomorfizmov G imenujemo **grupa notranjih avtomorfizmov** G, označena z $Inn(G)$. Iz izreka 2.40 sledi, da

$$G/Z(G) \cong Inn(G).$$

Poleg tega je $Inn(G) \trianglelefteq Aut(G)$ in **grupa zunanjih avtomorfizmov** G definirana kot

$$Out(G) = Aut(G)/Inn(G).$$

Podgrupa H grupe G je karakteristična podgrupa grupe G, oz. je **karakteristična** za grupo G, če je za vsak $\pi \in Aut(G)$

$$H^\pi = H,$$

in pišemo H char G. Karakteristična podgrupa je podgrupa edinka v G. Na primer, trivialna podgrupa in G sta karakteristični podgrupi G, center $Z(G)$ pa je tudi karakterističen v G.

Definicija 2.43. Naj bosta G in H dve grupi, $\pi : H \to Aut(G)$ pa homomorfizem. **(Zunanji) poldirektni produkt** G in H je grupa z množico $\{(g, h) \mid g \in G, h \in H\}$ in binarno operacijo

$$(g, h)(g', h') = (g(g')^{(h^{-1})^\pi}, hh'),$$

in je označen z $G \rtimes_\pi H$ (ali preprosto $G \rtimes H$).

Primer 2.44. Naj bo G grupa s podgrupama H in N, tako da je $G = NH$. Predpostavimo, da je $H \cap N = 1$ in $N \lhd G$. Naj bosta $g, g' \in G$, kjer je $g = nh$ in $g' = n'h'$. Torej

$$gg' = (nh)(n'h') = n(hn'h^{-1})hh' = n(n')^{\phi_{h^{-1}}}hh'.$$

kjer je $\phi_{h^{-1}}$, kot je definirano v primeru 2.42. Ker je $N \lhd G$, potem $\phi_{h^{-1}}$ inducira avtomorfizem N. Tako obstaja homomorfizem $\pi : H \to Aut(N)$, tako da

$$gg' = n(n')^{\phi_{h^{-1}}}hh' = n(n')^{(h-1)^{\pi}}hh'.$$

Tako je $G = N \rtimes H$ in pravimo, da je G **notranji poldirektni produkt** N s H. Upoštevajmo, da če je H tudi podgrupa edinka v G, potem velja, da je $G = N \times H$.

Naj bo $\Omega = \{1, \ldots, n\}$ množica. Spomnimo se, da množica vseh permutacij Ω pod funkcijsko kompozicijo tvori grupo, imenovano simetrična grupa Ω, in jo označimo s S_n.

Definicija 2.45. Permutacijska grupa Ω je podgrupa S_n.

Upoštevajmo, da S_n deluje na Ω naravno, kjer je a^{σ} preslikava $a \in \Omega$ pod permutacijo σ. Množica vseh sodih permutacij σ tvori permutacijsko grupo, ki jo imenujemo alternirajoča grupa in jo označimo z A_n. Ko je $n \geq 5$, je A_n enostavna grupa in je enolično določena netrivialna podgrupa edinka grupe S_n.

Uvedli smo dve vrsti produktov grup: direktni produkt in poldirektni produkt. Tukaj predstavljamo drugo vrsto produkta grupe, ki se uporablja v tej nalogi.

Definicija 2.46. Naj bo G grupa in $H \leq S_n$. **Venčni produkt** $G \wr H$ je poldirektni produkt $G^n \rtimes H = \{(a_1, \ldots, a_n)\pi \mid a_i \in G, \pi \in H\}$ kjer je

$$(a_1, \ldots, a_n)\pi(a'_1, \ldots, a'_n)\pi' = (a_1, \ldots, a_n)\pi(a'_1, \ldots, a'_n)\pi^{-1}\pi\pi' = (a_1 a'_{1\pi}, \ldots, a_n a'_{n^{\pi}})\pi\pi'$$

Opomba 2.47. Naj bo $G \leq S_m$, ki deluje na Δ, in $H \leq S_n$. Venčni produkt $G \wr H$ ima dve naravni delovanji.

- **Neprimitivno delovanje**: Naj bo $\Omega = \Delta_1 \cup \cdots \cup \Delta_n$ disjunktna unija n kopij Δ, kjer je $\Delta_i = \{\delta_{i1}, \ldots, \delta_{im}\}$ za vsak $1 \leq i \leq n$. Potem za vsak $\delta_{ij} \in \Omega$ in $(a_1, \ldots, a_n)\pi \in G \wr H$ velja, da

$$(\delta_{ij})^{(a_1,\ldots,a_n)\pi} = (\delta_{ij}^{ai})^{\pi} = \delta_{i^{\pi} j^{a_i}}.$$

- **Primitivno delovanje**: Naj bo $\Omega = \Delta^n = \{(\delta_1, \ldots, \delta_n) \mid \delta_i \in \Delta\}$. Potem za vsak $(\delta_i, \ldots, \delta_n) \in \Omega$ in $(a_1, \ldots, a_n)\pi \in G \wr H$ velja, da

$$(\delta_i, \ldots, \delta_n)^{(a_1,\ldots,a_n)\pi} = (\delta_1^{a_1}, \ldots, \delta_n^{a_n})^{\pi} = (\delta_{1^{\pi^{-1}}}^{a_{1^{\pi^{-1}}}}, \ldots, \delta_{n^{\pi^{-1}}}^{a_{n^{\pi^{-1}}}}).$$

2.1.6 Posebi razredi grup

Tukaj navajamo nekaj razredov grup, ki so ključnega pomena v tej nalogi.

Definicija 2.48. Naj bo G grupa. Rečemo, da je G **enostavna**, če G nima netrivialne prave podgrupe edinke.

Ciklične grupe praštevilskega reda so enostavne grupe, saj nimajo netrivialnih pravilnih podgrup in so edine abelove enostavne grupe. Upoštevajmo, da je center $Z(G)$ grupe G podgrupa edinka, če je G neabelova enostavna, potem je $Z(G) = 1$ in je $Inn(G) \cong G$.

Definicija 2.49. Naj je G grupa reda n. Če je $n = p^k$, kjer je p praštevilo, potem pravimo, da je G p-grupa. Če je $n = p^k m$, kjer je p praštevilo in $(p, m) = 1$, potem je p-**podgrupa Sylowka grupe** G podgrupa, ki ima red p^k.

Naslednji rezultat je znan kot Izrek Sylowa.

Izrek 2.50. *Naj bo G grupa z redom n, kjer je $n = p^k m$, kjer je p praštevilo in $(p, m) = 1$. Potem*

- *G vsebuje podgrupo reda p^k;*
- *katerikoli dve p-podgrupi Sylowki grupe G sta med seboj konjugirani;*
- *vsaka podgrupa grupe G, katere red je potenca p, je podgrupa neke p-podgrupe Sylowke grupe G.*

Definicija 2.51. Elementarna abelova p-grupa ranga k je **direktni produkt** k cikličnih grup reda p ($k \geq 1$) in jo označimo z Z_p^k.

Upoštevajmo, da ima vsak netrivialni element elementarne abelove p-grupe red p.

2.2 TEORIJA PERMUTACIJSKIH GRUP

2.2.1 Delovanje grup, sistem blokov in primitivnost

Grupo enot v $\mathbb{Z}_n$ glede na množenje označimo z $\mathbb{Z}_n^*$ in opazimo, da je $Aut(\mathbb{Z}_n) = \{x \mapsto ax : a \in \mathbb{Z}_n^*\}$.

Naj bo G grupa in X neprazna množica. Pravimo, da G deluje na X, če obstaja funkcija $f : G \times X \to G$, pri čemer je $f(g, x)$ zapisano gx, tako da je $g(hx) = (gh)x$ in $1x = x$ za vsak $g, h \in G$ in $x \in X$ (seveda je 1 identitetni element v G). Rekli bomo, da G deluje na X na levi. V tem besedilu so vse grupe in množice končne, v tem primeru je stopnja delovanja $|X|$, število elementov v X. Pravimo, da je **kardinalnost** X

stopnja G, ki deluje na X, in pravimo, da G deluje zvesto na X, če samo 1 fiksira vse točke X. Na primer, grupa G **deluje zvesto** sama sebi s konjugacijo, če in samo če je $Z(G) = \{1\}$.

S tem povezan pojem je permutacijska predstavitev grupe G, ki je homomorfizem $\phi : G \to S_n$ za nek n. Standardni rezultat teorije grup je, da vsako delovanje G na X inducira homomorfizem $\phi : G \to S_X$. Torej vsako delovanje G na X povzroči ustrezno permutacijsko predstavitev G. Občasno bomo zlorabili terminologijo in $\phi(G)$ označili kot permutacijsko predstavitev, če je delovanje jasno. Delovanje G na X se imenuje **zvesto**, če je $Ker(\phi) = 1$. **Jedro** delovanja ϕ od G na X označimo s $Ker(\phi)$.

Primer 2.52. Naj bo n pozitivno celo število in $f : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ definiramo z $f(g, x) = g+x$. Za $g, h \in \mathbb{Z}_n$ in $x \in \mathbb{Z}_n$ je $g+(h+x) = (g+h)+x$ in $0+x = x$, tako da je f delovanje $\mathbb{Z}_n$ na sebe. Stopnja tega delovanja je $|\mathbb{Z}_n| = n$ in delovanje je zvesto, namreč če je $f(g, x) = x$ za vse $x \in \mathbb{Z}_n$, potem je $g = 0$. Ustrezna permutacijska predstavitev $\mathbb{Z}_n$ je $\phi : \mathbb{Z}_n \to S_n$, podana z $\phi(g)$, je funkcija definirana z $x \mapsto x + g \pmod n$. Opazimo, da je $\phi(\mathbb{Z}_n)$ podgrupa S_n, ki jo generira n-cikel $(0, 1, 2, ..., n-1)$ in je običajno označena z $(\mathbb{Z}_n)_L$ (glej definicijo 3.11). Podobno, če je $H \leq \mathbb{Z}_n$ podgrupa reda m, potem podobni argumenti kažejo, da je tudi $k : \mathbb{Z}_n \times (\mathbb{Z}_n/H)$, podano s $k(g, x + H) = g + (x + H)$. Če je $m > 1$, to delovanje ni zvesto, saj je $k(h, x + \mathbb{Z}_n/H) = x + \mathbb{Z}_n/H$ za vsakega $h \in H$. Stopnja tega delovanja je nato n/m, kjer $|H| = m$. Ustrezna permutacijska predstavitev $\mathbb{Z}_n$ je $\delta : \mathbb{Z}_n \to S_{n/m}$, podana z $\delta(g)$, je funkcija, definirana z $x \mapsto x + g \pmod{n/m}$, in je tudi izomorfna za $(\mathbb{Z}_{n/m})_L$.

Definicija 2.53. Pravimo, da je G **tranzitivna** na X (ali G je **tranzitivna**), če za katera koli dva $x, y \in X$, potem obstaja $g \in G$, tako da je $g(x) = y$; drugače pravimo, da G ni tranzitivna X.

Običajno pri razpravi o permutacijskih grupah začnemo s podgrupo S_n ali pa določimo grupo in delovanje te grupe na množici X, ki nato inducira naravno podgrupo S_X. Podobno se koncept o permutacijski grupi prevede v koncept o delovanjih in obratno in ponavadi se vzdržimo določanja analognih konceptov v vsakem kontekstu. Torej je delovanje G na X tranzitivno, če za vsak $x, y \in X$ obstaja $g \in G$ takšen, da je $gx = y$, in stopnja tranzitivne permutacijske grupe $G \leq S_n$ je n.

Definicija 2.54. Naj bo $G \leq S_n$ tranzitivna in $x \in \mathbb{Z}_n$. **Stabilizator** x v G, označen s $Stab_G(x)$, je opredeljen s $Stab_G(x) = \{g \in G : g(x) = x\}$. To pomeni, da je $Stab_G(x)$ množica vseh permutacij v G, ki preslikajo x na x.
Stabilizator x v G je pogosto označen z G_x in je podgrupa G.

Izrek 2.55. *Naj bodo $G \leq S_n$, $x \in \mathbb{Z}_n$ in $h \in G$. Potem je $hStab_G(x)h^{-1} = Stab_G(h(x))$. Če je G tranzitivna, je $Stab_G(x)$ konjugiran v G na $Stab_G(y)$ za vsak $y \in \mathbb{Z}_n$.*

Dokaz. Opazimo, da

$$\begin{aligned} Stab_G(h(x)) &= \{g \in G : g(h(x)) = h(x)\} \\ &= \{g \in G : h^{-1}gh(x) = x\} \\ &= \{g \in G : h^{-1}gh \in Stab_G(x)\} \\ &= \{g \in G : g \in hStab_G(x)h^{-1}\} \\ &= hStab_G(x)h^{-1}. \end{aligned}$$

Za drugo trditev, ker je G tranzitivna, obstaja $h \in G$, tako da je $h(x) = y$. Potem je $Stab_G(y) = Stab_G(h(x)) = hStab_G(x)h^{-1}$. □

Definicija 2.56. Naj G deluje na X in naj bo $x \in X$. **Orbita** x pod G je množica preslikav od x in je označena z

$$G(x) = \{g(x) \mid g \in G\}.$$

Naj bo $y \in X$ tako, da je $x \neq y$. Upoštevajmo, da je $G(x) = G(y)$, če in samo če obstaja nek $g \in G$, tako da je $g(x) = y$. Orbite dveh različnih elementov iz X so bodisi enake bodisi disjunktne, zato je X disjunktna unija orbit iz G.

Če je G tranzitivna na X, potem ima G samo eno orbito, to je X. Naj bo H podgrupa G in $x \in X$. Znano je, da je $G = Stab_G(x)H = HStab_G(x)$, če in samo če je H tranzitivna.

Naslednji rezultat je zelo koristen in se včasih imenuje tudi **Orbita-Stabilizator izrek**.

Izrek 2.57. *Naj bodo $G \leq S_n$ in $x \in \mathbb{Z}_n$. Množica $G(x)$, je orbita x v G. Potem*

$$|G| = |G(x)| \cdot |Stab_G(x)|$$

ali ekvivalntno

$$|G(x)| = [G : Stab_G(x)].$$

Dokaz. Definirajmo $\phi : G \to G(x)$ z $\phi(g) = g(x)$. Iz definicije od ϕ sledi, da je $|\phi(G)| = |G(x)|$. Tudi

$$\begin{aligned} \phi(g) = \phi(h) &\iff g(x)) = h(x) \\ &\iff h^{-1}g(x) = x \\ &\iff h^{-1}g \in Stab_G(x)\} \\ &\iff h^{-1}gStab_G(x) = 1 \cdot Stab_g(x) \text{(kot levi odsek)} \\ &\iff \text{h in g sta v istem levem odseku } Stab_G(x). \end{aligned}$$

To pomeni $|\phi(G)|$, je število levih odsekov $Stab_G(x)$ in tako $|G(x)| = [G : StabG(x)]$. Ker so tukaj vse grupe končne, je $[G : Stab_G(x)] = |G|/|Stab_G(x)|$ □

Naslednja uporaba izreka stabilizatorja orbite je prvotno posledica G. A. Millerja [14].

Izrek 2.58. *Naj bo G tranzitivna grupe reda n in p praštevilo. Najvišja stopnja p^k od p, ki deli n, deli tudi dolžino vsake orbite p-Sylowovke podgrupe G.*

Dokaz. Naj je P p-sylowka podgrupe G in x točka. Po izreku stabilizatorja orbite je $n = [G : Stab_G(x)]$ in $[P : Stab_P(x)] = |P(x)|$. Potem

$$\begin{aligned} n \cdot [Stab_G(x) : Stab_P(x)] &= [G : Stab_G(x)] \cdot [Stab_G(x) : Stab_P(x)] \\ &= [G : Stab_P(x)] \\ &= [G : P] \cdot [P : Stab_P(x)] \\ &= [G : P] \cdot |P(x)|. \end{aligned}$$

Ker je $gcd([G : P], p) = 1$ in p^k deli n, vidimo p^k deli $|P(x)|$ □

Naslednja posledica je oblika prejšnjega rezultata, ki se najpogosteje uporablja (za naše namene) in je tudi posledica Mullerja [14].

Posledica 2.59. *Naj bo p praštevilo in $k \geq 1$. P-sylowovka tranzitivne grupe stopnje p^k je tranzitivna.*

Definicija 2.60. Permutacijska grupa $G \leq S_n$ je **polregularna**, če je $Stab_G(x) = 1$ za vsak $x \in \mathbb{Z}_n$, G pa **regularna**, če je G hkarti polregularna in tranzitivna.

Naslednji rezultat sledi neposredno iz izreka stabilizatorja orbite, če je $G \leq S_n$ tranzitiven, potem ima G samo eno orbito.

Iz izreka 2.57 sledi, da je G regularna na X, če in samo če je G tranzitivna na X in $|X| = |G|$ in ta lastnost omogoča lažji način za ugotavljanje, ali je grupa regularna. Upoštevajmo, da če G ni tranzitivna na X in je $Stab_G(x) = 1$ za vsak $x \in X$, potem pravimo, da je G polregularna na Ω. Naj bo $g \in G$. Pravimo, da je g polregularen element (ali g je polregularen), če je $\langle g \rangle$ polregularna na X.

Particija $B = \{B_1, \ldots, B_t\}$ od X je dekompozicija podmnožice X, tako da je $X = \cup_{i=1}^{t} B_i$ z $B_i \subseteq \Omega$ in $B_i \cap B_j = \emptyset$ za vsak $1 \leq i \neq j \leq t$.

Posledica 2.61. *Tranzitivna grupa je regularna, če in samo, če sta njen red in stopnja enaki.*

Primer 2.62. Grupa S_n je regularna, če in samo če je $n \leq 2$, A_n pa regularna, če in samo če je $n = 1$ ali 3, vendar je polregularna za $n = 2$. Grupa $(\mathbb{Z}_n)_L$ je regularna za vsa pozitivna cela števila n.

Rešitev. Grupa S_n je po posledici 2.61 regularna, če in samo če je $n! = n$ katera velja, če in samo če $n \leq 2$.Tudi, $A_1 = 1$ je regularna , $A_2 = 1$ ni regularna, pri $n \geq 3$ pa je grupa A_n tranzitivna in tako regularna, če in samo če je $n!/2 = n$, kar velja, če in samo, če je $n = 3$. Končno je $(\mathbb{Z}_n)_L$ tranzitivna reda n in tako regularna. □

Definicija 2.63. Naj bo G grupa, ki deluje tranzitivno na X. Za neprazno podmnožico B v X pravimo, da je **blok** za G, če je za vsak $g \in G$ $g(B) = B$ ali $g(B) \cap B = \emptyset$.

Če je G tranzitivna na X, potem sta X in kateri koli $\{B\}$ za $B \in X$ bloka za G, ki jih imenujemo trivialni bloki. Če je B blok za G, potem množica

$$B = \{g(B) \mid g \in G\}$$

tvori particijo X in vsaka množica $g(B)$ je tudi blok za G. Pravimo, da je particija B **sistem blokov** za G.

Definicija 2.64. Naj bo G grupa, ki deluje tranzitivno na X. Če G nima netrivialnih blokov na X, potem pravimo, da je G **primitivna** na X; sicer G imenujemo **neprimitivna**.

2.3 TEORIJA GRAFOV

2.3.1 Osnovne definicije

Definicija 2.65. Graf Γ je trojica, ki jo sestavljajo **množica vozlišč** $V(\Gamma)$, **množica povezav** $E(\Gamma)$ in relacija, ki povezuje vsak rob z dvema vozliščema, imenovanima njegovi **končni točki**.

Red grafa je kardinalnost njegove množice vozlišč, **velikost** grafa pa je kardinalnost njegove množice povezav. Za graf pravimo, da je **končen** graf, če sta njegova množica vozlišč in povezav končna. **Izolirano vozlišče** je graf reda 1 s prazno množico povezav. Graf narišemo tako, da vsako vozlišče predstavimo s točko, vsako povezavo pa s krivuljo, ki povezuje njegove končne točke. Na splošno ni nujno, da so končne točke povezav v grafu različne. **Zanka** je povezava, kjer sta končni točki enaki, **večkratne povezave** pa so povezave z enakim parom končnih točk.

Definicija 2.66. Enostaven graf je graf brez zank ali večkratnih povezav.

Naj bo Γ graf. Če je Γ enostaven, potem je $E(\Gamma)$ množica neurejenih parov različnih vozlišč in lahko vsako povezavo poimenujemo z njegovimi končnimi točkami, kar pomeni, da lahko zapišemo $\{u, v\}$ za povezavo s končnima točkama u in v. Pravimo, da sta u in v **sosednja** v Γ. Pravimo, da je urejen par (u, v) lok od Γ. Očitno vsaka povezava $\{u, v\}$ od Γ ustreza dvema lokoma, ki sta (u, v) in (v, u).

Predpostavlja se, da so grafi, omenjeni v tej nalogi, enostavni in končni.

Če sta u in v končni točki povezav v Γ, potem pravimo, da sta u in v **sosednja** in je u **sosed** v. Naj bo $N_\Gamma(u) = \{v | \{u, v\} \in E(\Gamma)\}$ in za $N_\Gamma(u)$ pravimo, da je **soseska** u v Γ. Stopnja u je $|N_\Gamma(u)|$ in je označena z $d_\Gamma(u)$.

Definicija 2.67. Graf Γ je **regularen**, če imajo vsa njegova vozlišča enako stopnjo. Stopnja vozlišč je **valenca** Γ, označena z $val(\Gamma)$.

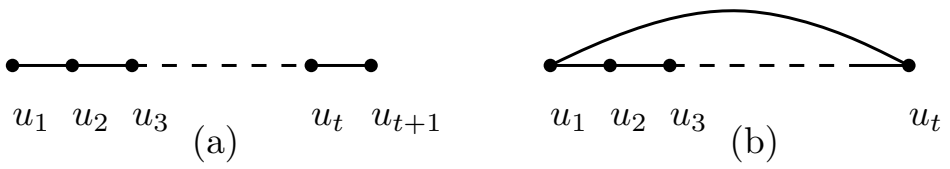
Definicija 2.68. Podgraf grafa Γ je graf Σ z $V(\Sigma) \subseteq V(\Gamma)$ in $E(\Sigma) \subseteq E(\Gamma)$ in dodelitev končnih točk v Σ je enaka kot v Γ.

Če je Σ podgraf Γ, potem pravimo, da je Σ vsebovan v Γ in zapišemo $\Sigma \subseteq \Gamma$. Naj bo U podmnožica $V(\Gamma)$. **Inducirani podgraf** Γ_U je podgraf, kjer je množica vozlišč U in množica povezav vsebuje vse povezave iz Γ, katerih obe končni točki sta vsebovani v U.

Pot P_t je graf s seznamom vozlišč $\{u_1, \ldots, u_{t+1}\}$ in u_i, u_j sta sosednji, če in samo če je $j = i + 1$, kjer je $1 \leq i \leq t$ (glej sliko 1(a)). Pravimo, da je P_t pot dolžine t ali preprosto t-pot. Ena sama povezava je na primer 1-pot. Cikel C_t ima t vozlišč $u_1, \ldots, u_t$ in

$$E(C_t) = \{\{u_i, u_{i+1}\} \mid 1 \leq i \leq t - 1\} \cup \{u_1, u_t\}$$

(glej sliko 1(b)). Pravimo, da je C_t cikel dolžine t ali preprosto t-cikel. Upoštevajmo, da t-cikel vsebuje t različnih $(t-1)$-poti. Cikel sode (lihe) dolžine imenujemo sodi (lihi) cikel.



Slika 1: t-pot in t-cikel

Definicija 2.69. Graf Γ je **povezan**, če vsaki dve različni vozlišči Γ ležita na poti; sicer je Γ **nepovezan**.

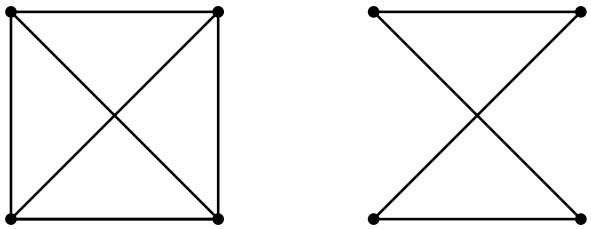
Za inducirani podgraf Γ_U od Γ pravimo, da je komponenta od Γ, če je povezan, vendar ne obstaja $U' \subseteq V(\Gamma)$ z $U \subset U'$ tako, da je $\Gamma_{U'}$ povezan. Tako je enostavno videti, da nepovezani graf vsebuje vsaj dve povezani komponenti. Ker grafične lastnosti nepovezanega grafa izhajajo iz njegovih povezanih komponent, je na splošno bolj zanimivo obravnavati povezane grafe. V tem delu obravnavamo le povezane grafe.

Definicija 2.70. Graf Γ je **dvodelni** graf, če je $V(\Gamma) = U \cup V$ disjuntkna unija dveh podmnožic U in V, tako da vsaka povezava Γ povezuje vozlišče v U z enim iz V, množici vozlišč U in V se imenujeta dva dela Γ.

Iz definicije 2.70 sledi, da dvodelni graf ne vsebuje lihih ciklov, kar vodi do ekvivalntne definicije, to je, da je graf dvodelen, če in samo če ne vsebuje lihih ciklov (glej [19]). Dva inducirana podgrafa Γ_U in Γ_V sta grafa s praznimi množicami povezav.

Definicija 2.71. Polni graf K_n je graf reda n, kjer sta vsaki dve disjunktni vozlišči sosednji. **Polni dvodelni** graf $K_{n,m}$ je dvodelni graf, kjer imata oba dela red n in m, dve vozlišči pa sta sosednji, če in samo če sta v različnih delih.

Izolirano vozlišče je graf reda 1, ki ga označimo s K_1, enojna povezava pa je polni graf in tudi polni dvodelni graf, označimo ga s K_2. Lahko opazimo, da je vsak inducirani podgraf polnega grafa še vedno poln, zato je vsak poln graf K_n z $n \geq 3$ nebipartiten graf.



K_4 $C_4 \cong K_{2,2}$

Slika 2: Polni graf in polni dvodelni graf

2.3.2 Izomorfizmi grafov

Grafa $X_1 = (V_1, E_1)$ in $X_2 = (V_2, E_2)$ sta enaka, če je $V_1 = V_2$ in $E_1 = E_2$. Čeprav je to razumna definicija, se za večino primerov model odnosa ne spremeni, če preimenujemo vozlišča grafa. To seveda vodi do definicije **izomorfnih grafov**.

Definicija 2.72. Za grafa X in Y se funkcija $\varphi : V(X) \to V(Y)$ imenuje **izomorfizem** iz X v Y , če

1. φ je bijekcija;

2. $\forall u, v \in V(X)\{u, v\} \in E(X) \iff \{\varphi(u), \varphi(v)\} \in E(Y)$.

Grafa X in Y imenujemo izomorfna, če obstaja izomorfizem iz X v Y, kar označimo z $X \cong Y$.

Lema 2.73. *Naj bosta X in Y končna grafa in $\varphi : V(X) \to V(Y)$ bijektivna funkcija. če*

$$\forall u, v \in V(X)\{u, v\} \in E(X) \implies \{\varphi(u), \varphi(v)\} \in E(Y)$$

potem je φ izomorfizem.

Za funkcijo $\varphi : A \to B$ in za podmnožico $S \subseteq A$ definiramo $\varphi(S) = \{\varphi(s) : s \in S\}$.

Lema 2.74. *Naj bo φ izomorfizem iz X v Y . Potem za vsak $v \in V(X)$ velja $\varphi(X(v)) = Y(\varphi(v))$.*

Posledica 2.75. *Izomorfizmi ohranjajo stopnjo vozlišč, to pomeni za izomorfizem φ iz X v Y velja $d_X(v) = d_Y(\varphi(v)), \forall v \in V$.*

Upoštevajmo lahko tudi izomorfizem grafa Γ na samega sebe. V tem primeru namesto "izomorfizem" uporabljamo besedo "avtomorfizem". Ponavljamo definicijo, da poudarimo njeno pomembnost.

Definicija 2.76. Naj bo Γ graf. **Avtomorfizem** Γ je bijektivna funkcija $\varphi : V(X) \to V(X)$, tako da $\forall u, v \in V(X)$ imamo $\{u, v\} \in E(\Gamma) \iff \{\varphi(u), \varphi(v)\} \in E(\Gamma)$. Množico vseh avtomorfizmov grafa Γ označimo z $Aut(\Gamma)$.

Iz definicije sledi, da če je φ avtomorfizem Γ, potem ohranja sosednost vozlišč Γ, tako da imamo $d_\Gamma(u) = d_\Gamma(\varphi(u))$ za vsak $u \in V(\Gamma)$. Naj bo $f : V(\Gamma) \to V(\Gamma)$ definiran kot $f : u \to u$ za vsak $u \in V(\Gamma)$, in tako je f avtomorfizem Γ, za katerega pravimo, da je trivialni avtomorfizem Γ. Jasno je, da ima vsak graf trivialni avtomorfizem.

Primer 2.77. Naj bo Γ n-cikel z $V(\Gamma) = \{u_1, \ldots, u_n\}$. Naj bosta ρ in τ definirana kot spodaj, za vsak $1 \leq i \leq n - 1$

$$\rho : u_i \mapsto u_{i+1},$$

$$\tau : u_i \mapsto u_{n-i},$$

in

$$\rho : u_n \mapsto u_1,$$

$$\tau : u_n \mapsto u_n.$$

Tako sta ρ in τ avtomorfizma Γ in pravimo, da je ρ rotacija Γ in τ zrcaljenje Γ. Dobro je znano, da ρ in τ generirata grupo avtomorfizmov Γ in $Aut(\Gamma) \cong D_{2_n}$.

Izrek 2.78. *Za graf* Γ *je množica* $Aut(\Gamma)$ *grupa glede na operacijo kompozituma funkcij, to je za* $f, g \in Aut(\Gamma)$, $fg = f \circ g$ *ali ekvivalentno* $(fg)(v) = f(g(v))$ *za vsak* $v \in V(\Gamma)$.

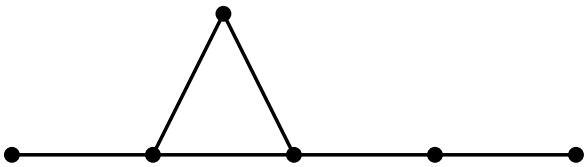
Definicija 2.79. Komplement $\bar{\Gamma}$ grafa Γ je graf z $V(\bar{\Gamma}) = V(\Gamma)$ in za vsaki dve različni točki $u, v \in V(\Gamma)$ velja $\{u, v\} \in E(\bar{\Gamma}) \iff \{u, v\} \neq E(\Gamma)$.

Lema 2.80. *Za vsak graf* Γ *velja* $Aut(\Gamma) = Aut(\bar{\Gamma})$.

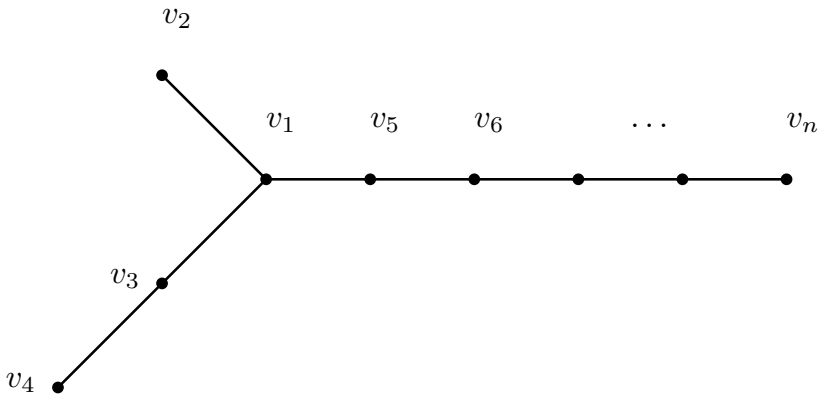
Graf Γ imenujemo **asimetričen**, če je $Aut(\Gamma) = \{id\}$.

Primer 2.81. Za vsako pozitivno celo število $n \geq 6$ obstaja asimetričen graf z n vozlišči.

Rešitev. Če je $n = 6$, potem upoštevajmo graf na sliki 3. Zlahka je videti, da je ta graf asimetričen, zato izpuščamo podrobnosti. Recimo, da je $n \geq 7$, in razmislimo o grafu na sliki 4, ter naj bo φ njegov avtomorfizem. Upoštevajmo, da je v_1 natanko določeno vozlišče stopnje 3, zato mora biti določeno s φ. Jasno je tudi, da mora biti v_2 fiksen, saj je natanko določen sosed v_1 stopnje 1. Recimo, da je $\varphi(v_3) = v_5$. Potem sledi $\varphi(v_4) = v_6$. Vendar je to nemogoče, saj ima v_4 stopnjo 1 in v_6 stopnjo 2. Zato φ fiksira v_3, v_4 in v_5. Zdaj lahko vidimo (z indukcijo), da φ fiksira tudi oglišča $v_6, \ldots, v_n$. To dokazuje, da je graf asimetričen. [11] □



Slika 3: Asimetrični graf reda 6



Slika 4: Asimetrični graf reda $n \geq 7$

Izrek 2.82. *Skoraj vsi grafi so asimetrični.*

Cayleyjevi grafi

Naj bo Γ graf z množico vozlišč $V(\Gamma)$ in množico povezav $E(\Gamma)$. Naj bo $A = Aut(\Gamma)$ grupa avtomorfizmov Γ. Jasno je, da vsak avtomorfizem Γ naravno inducira permutacijo množice vozlišč Γ. Ker A ohranja sosednost vozlišč Γ, vsak avtomorfizem Γ inducira tudi permutacijo množice povezav. Tako lahko grupo avtomorfizmov A obravnavamo kot permutacijsko grupo $V(\Gamma)$ in permutacijsko grupo $E(\Gamma)$. Recimo, da je red Γ n in velikost Γ m. Tako imamo naslednje $A \lesssim S_n$ in $A \lesssim S_m$.

Definicija 2.83. Pravimo, da

- Γ je **vozliščno tranzitiven** graf (ali Γ je vozliščno tranzitiven), če je A tranzitiven na $V(\Gamma)$ (uporablja se tudi termin **točkovno tranzitiven** graf);
- Γ je **povezavno tranzitiven** graf (ali Γ je povezavno tranzitiven), če je A tranzitiven na $E(\Gamma)$;
- Γ je **ločno tranzitiven** graf (ali Γ je ločno tranzitiven), če je A tranzitiven na množici lokov od Γ.

Naj bo na primer $\Gamma = C_n$ cikel. Iz primera 2.77 je grupa avtomorfizmov Γ tranzitivna na $V(\Gamma)$, $E(\Gamma)$ in množici lokov Γ. Zato je cikel vozliščno tranzitiven, povezavno tranzitiven in ločno tranzitiven. Lahko vidimo, da ločna tranzitivnost povezanega grafa Γ implicira vozliščno tranzitivnost in povezavno tranzitivnost, vendar tranzitivnost povezav ne implicira tranzitivnosti vozlišč. Na primer, naj bo $\Gamma = K_{n,m}(n \neq m)$ poln dvodelni graf z dvema deloma U in V . Ker je $Aut(\Gamma) = S_n \times S_m$, je Γ povezavno tranzitiven. Ker je $n \neq m$, ne obstaja avtomorfizem Γ, ki preslika vozlišča U v vozlišča V , zato Γ ni vozliščno tranzitiven.

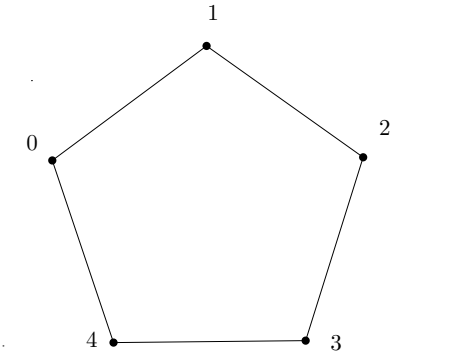
Definicija 2.84. Naj bo G grupa in S neprazna podmnožica G, kjer je $1 \notin S$ in $S^{-1} = S$. **Cayleyjev graf** $\Gamma = Cay(G, S)$ za G je graf z $V(\Gamma) = G$ in

$$E(\Gamma) = \{\{x, y\} \mid x^{-1}y \in S\}.$$

Pravimo, da je G definirajoča grupa Γ in S **generatorska množica** Γ.

Naj bo Γ Cayleyjev graf z definirajočo grupo G in generatorsko množico S ter naj bo $g \in G$ vozlišče Γ . Iz definicije sledi $N_\Gamma(g) = \{gs \mid s \in S\}$ in torej $d_\Gamma(g) = |S|$. Tako je Γ regularen graf z $val(\Gamma) = |S|$. Ker je $1 \notin S$, velja, da Γ ne vsebuje zank, zato je Γ enostaven graf.

Primer 2.85. Naj bo $G = \mathbb{Z}_5$ in $S = \{1, 4\}$. Potem je $Cay(G, S)$ 5-cikel.



Slika 5: 5-cikel

Trditev 2.86. *Cayleyjev graf $Cay(G, S)$ je **povezan**, če in samo če je $G = \langle S \rangle$.*

Za vsak $g \in G$ lahko definiramo permutacijo $g_R : G \to G$ z desnim množenjem z g na G in lahko definiramo permutacijo $g_L : G \to G$ z levim množenjem z g^{-1} na G kot spodaj:

- **desno množenje**: $g_R : x \mapsto xg$, za $x \in G$;
- **levo množenje**: $g_L : x \mapsto g^{-1}x$, za $x \in G$.

Opazimo lahko, da je g_L avtomorfizem Γ in grupa $G_L = \{g_L \mid g \in G\}$ je podgrupa $Aut(\Gamma)$, izomorfna G. Tako je vsak Cayleyjev graf vozliščno tranzitiven graf. Vendar ni vsak vozliščno tranzitivni graf Cayleyjev graf za neko grupo, najmanjši primer je dobro znani Petersenov graf (glej [[4], stran 124]).

Pravzaprav je G_L **polregularen** tudi na $V(\Gamma)$, saj je $(G_L)_x = 1$ za vsak $x \in G$. Tako G_L deluje **regularno** na $V(\Gamma)$. Naslednji rezultat je merilo za določitev, ali je dani graf Cayleyjev graf ali ne (glej [[4], lema 16.3] ali [17]).

Izrek 2.87. ***(Karakterizacija Cayleyjevega grafa)*** *Graf Γ je Cayleyjev graf za grupo G, če in samo če $Aut(\Gamma)$ vsebuje regularno podgrupo, izomorfno G.*

Upoštevajte, da je lahko graf Cayleyjev graf za različne grupe. Na primer, polni graf K_n je Cayleyjev graf za katero koli končno grupo G reda n, zlasti $K_n \cong Cay(G, G\backslash\{1\})$.

Definicija 2.88. Cayleyjev graf je **holomorfni Cayleyjev graf**, če je njegova generatorska množica sestavljena iz unije razredov konjugiranosti elementov definirajoče grupe grafa.

Naj bo $G_R = \{g_R \mid g \in G\}$. Ni težko videti, da je G_R podgrupa $Aut(\Gamma)$, če in samo če je S sestavljena iz unije konjugacijskih razredov elementov iz G, to je $G_R \leq Aut(\Gamma)$, če in samo če je Γ holomorfni graf.

Naj bo $Aut(G, S) = \{\rho \in Aut(G) \mid S^\rho = S\}$ in $Aut(\Gamma)_1 = \{\sigma \in Aut(\Gamma) \mid 1^\sigma = 1\}$. Očitno je $Aut(G, S) \leq Aut(\Gamma)_1$. Ker je Γ vozliščno tranzitiven in je G_L regularen na $V(\Gamma)$, velja $Aut(\Gamma) = G_L Aut(\Gamma)_1$.

Trditev 2.89. *[[15], posledica 4.2B]* $N_{Aut(\Gamma)}(G_L) = G_L \rtimes Aut(G, S)$.

Definicija 2.90. Cayleyjev graf $\Gamma = Cay(G, S)$ je normalen za G, če je G_L podgrupa edinka $Aut(\Gamma)$; drugače je Γ nenormalen za G.

Iz trditve 2.89 in definicije 2.90 sledi, da je Γ normalen Cayleyjev graf za G, če in samo če je $Aut(\Gamma) = G_L \rtimes Aut(G, S)$.

Primer 2.91. Naj bo Γ polni graf K_n z $n \geq 2$. Spomnimo se, da je K_n Cayleyjev graf za katero koli končno grupo G reda n, grupa avtomorfizmov K_n pa je simetrična grupa S_n. Za $n \geq 5$ vsebuje S_n samo dve pravi podgrupi edinki, in sicer trivialno podgrupo in A_n. Tako iz izreka 2.87 velja, da Γ ni normalen za katero koli končno grupo G reda n z $n \geq 5$.

Primer 2.91 predlaga naravno vprašanje: katere končne grupe dopuščajo normalen Cayleyjev graf? V [20] je Xu pokazal, da ima vsaka končna grupa vsaj en normalen Cayleyjev graf, razen za $Z_4 \times Z_2$ in $Q_8 \times Z_2^m$ z $m \geq 0$. Nadalje je domneval, da so "skoraj vsi" Cayleyjevi grafi normalni. Ta domneva še vedno ostaja nerešena. Vendar nam naslednji primer pove, da obstajajo Cayleyjevi grafi, ki so normalni in nenormalni za različne regularne grupe.

Primer 2.92. Naj bo $\Gamma = K_4$ in torej $A = Aut(\Gamma) = S_4$. Razmislimo o dveh različnih Cayleyjevih predstavitvah Γ, podanih z $(Z_2 \times Z_2, (Z_2 \times Z_2) \backslash \{1\})$ in $(Z_4, Z_4 \backslash \{1\})$. Znano je, da je regularna podgrupa A, izomorfna Z_2^2, normalna v A, vendar nobena podgrupa A, izomorfna Z_4, ni normalna. Tako je Γ nenormalen Cayleyjev graf za Z_4 in normalen Cayleyjev graf za Z_2^2.

Digraf Γ je urejeni par (V, A), kjer je V neprazna množica, **množica vozlišč** od Γ in $A \subseteq \{(u, v) : u, v \in V\}$ urejenega para V, **množica lokov** od Γ. Za lok (u, v) digrafa se običajno misli, da je **usmerjen** od u do v, lok pa včasih imenujemo tudi **usmerjena povezava**. Če sta $(u, v) \in A(\Gamma)$ in $(v, u) \in A(\Gamma)$, lahko ta dva loka prepoznamo in štejemo kot **povezavo**. Graf Γ je digraf, v katerem je $(u, v) \in A(\Gamma)$, če in samo če je $(v, u) \in A(\Gamma)$, v tem primeru pa mislimo, da so robovi neurejeni par točk, označeni uv. Množico lokov grafa običajno imenujemo **množica povezav** in označujemo z E namesto A. Po tej definiciji več povezav (različne povezave z enakimi končnimi točkami) ni dovoljenih. To se ne naredi zaradi kakršne koli nenaklonjenosti do več povezav, ampak bolj iz želje, da začnemo z najpreprostejšo definicijo grafa, v večini primerov, ki zadevajo simetrijo v digrafih, večkratne povezave niso pomembne (so irelevantne). Ta opredelitev sicer omogoča zanke, vendar v tem delu zanke večino časa niso pomembne. V tem besedilu so vsi grafi končni (torej tudi končne množice vozlišč). Osnovni izrazi digrafov in grafov ter operacije, kot so sprehodi, preseki digrafov itd., so definirani kot običajno. Glej na primer [5].

Kot je v navadi, za graf Γ z $N_\Gamma(u)$ označimo množico sosedov v Γ vozlišča u. Za digraf Γ zunanje sosedje u označimo z $N_\Gamma^+(u)$, vhodne sosednje pa z $N_\Gamma^-(u)$. To pomeni, da je $N_\Gamma^+(u) = \{v : (u, v) \in A(\Gamma)\}$ in $N_\Gamma^-(u) = \{v : (v, u) \in A(\Gamma)\}$. Če je graf ali digraf Γ **jasen**, lahko preprosto napišemo $N^+(u)$ itd.

Definicija 2.93. Izomorfizem med dvema digrafoma Γ_1 in Γ_2 je bijekcija $\phi : V(\Gamma_1) \to V(\Gamma_2)$, tako da je $\phi(u, v) \in A(\Gamma_2)$, če in samo če $(u, v) \in A(\Gamma_1)$.

Tako je izomorfizem ena na ena preslikava množice vozlišč na množico vozlišč, ki ohranja loke.

Vsak izomorfizem ϕ med dvema digrafoma Γ_1 in Γ_2 povzroča naravno bijekcijo med $A(\Gamma_1)$ in $A(\Gamma_2)$, podano z $(u, v) \mapsto (\phi(u), \phi(v))$. Pogosto bomo za preslikavo loka (u, v) pod ϕ preprosto zapisali $\phi(u, v)$ namesto $(\phi(u), \phi(v))$.

Definicija 2.94. Vsaka bijekcija ϕ od $V(\Gamma_1)$ do množice X povzroči digraf na X, izomorfen Γ_1. Določimo namreč Γ_2 z $V(\Gamma_2) = X$ in $A(\Gamma_2) = \{\phi(u, v)) : (u, v) \in A(\Gamma_1)\}$. Sprejeli bomo notacijsko konvencijo množice $\phi(\Gamma_1) = \Gamma_2$.

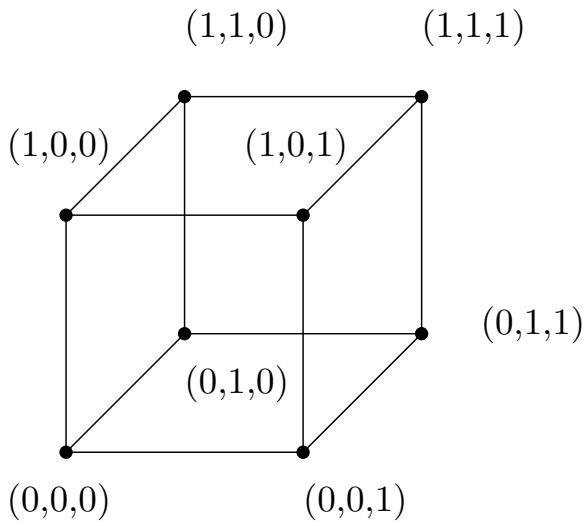
Avtomorfizem digrafa je izomorfizem digrafa s samim seboj. Množica vseh avtomorfizmov digrafa Γ je grupa pod funkcijo kompozituma in se imenuje **grupa avtomorfizmov** Γ, označena z $Aut(\Gamma)$. Seveda $Aut(\Gamma)$ deluje tudi na loke digrafa in povezave grafa.

Definicija 2.95. Digraf, katerega grupa avtomorfizmov je tranzitivna na svoji množici vozlišč, se imenuje **vozliščno tranzitiven digraf**. (Di) graf, katerega avtomorfizem je tranzitiven na svoji množici lokov, se imenuje **ločno tranzitiven (di)graf**. Graf Γ je **povezavno tranzitiven**, če je $Aut(\Gamma)$ tranzitiven na svoji množici povezav $E(\Gamma)$.

Primer 2.96. Poln graf K_n reda $n \geq 1$ je vozliščno tranzitiven, ločno tranzitiven in $Aut(\Gamma) = S_n$.

Rešitev. Ker ima K_n vsak lok, če je $\sigma \in S_n$, potem je $\sigma(u, v) \in A(K_n)$ za vsak par različnih vozlišč u in v. Tako je $Aut(K_n) = S_n$ (saj je S_n "največja" permutacijska grupa na n vozliščih). Grupa S_n je zagotovo tranzitivna in tudi če $(u_1, v_1), (u_2, v_2) \in A(S_n)$, potem obstaja $\sigma \in S_n$ z $\sigma(u_1, v_1) = (u_2, v_2)$. Tako je K_n vozliščno tranzitiven in ločno tranzitiven. □

Primer 2.97. Za $n \geq 1$ definirajte graf $\mathbb{Q}_n$ z $V(\mathbb{Q}_n) = \mathbb{Z}_2^n$ in dve vozlišči sta sosednji če in samo, če se razlikujeta natančno v eni koordinati. Graf Q_n je **n-dimenzionalna hiperkocka** ali **n-kocka** in je vozliščno tranzitivna. 3-kocka je prikazana na sliki 6.



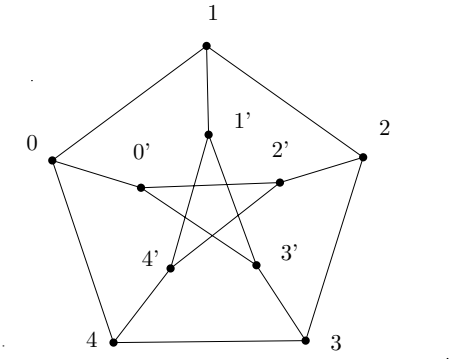
Slika 6: 3-kocka

Rešitev. Določimo $\tau_i : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ z $\tau_i(x)$ dodamo 1 modul 2 v i-to koordinato x in je identiteta ostalih koordinat. Če je $e \in E(Q_n)$, potem $\tau_i(e) \in E(Q_n)$, tako kot v kateri koli koordinati, dodajanje konstante (bodisi 0 bodisi 1) ne spremeni, ali so koordinate enake ali različne. Tako je $\tau_i \in Aut(Q_n)$ za vsak $1 \leq i \leq n$. Poleg tega je lahko ugotoviti ali kateri koli element $\mathbb{Z}_2^n$ je lahko spremenjen s katerim koli drugim elementom $\mathbb{Z}_2^n$ s spreminjanjem (ali dodajanjem 1) koordinat prvega, ki se razlikuje od drugega. Tako je $\langle \tau_i : 1 \leq i \leq n \rangle$ tranzitiven, Q_n pa vozliščno tranzitiven. □

$(n+1)$ dimenzionalno kocko lahko sestavimo iz n-kocke tako, da vzamemo dve kopiji n-kocke in ju združimo s popolnim ujemanjem. Ena n-kocka ima dodatno koordinato, dodano z 1 v dodatni koordinati, druga pa ima dodatno koordinato, dodano z 0 v dodatni koordinati. Ujemajoči se robovi so nato med ustreznima točkama v dveh kopijah. To pomeni, da se ujemajoči vozlišči razlikujejo le v dodatni koordinati. To je razvidno iz slike 6, kjer sta dve kopiji 2-kocke zgornja in spodnja stran kocke, dodatna koordinata pa prva koordinata. Ta konstrukcija za $(n+1)$-kocko iz n kocke je pogosto koristna za indukcijske argumente.

Primer 2.98. Petersenov graf, prikazan na sliki 7, je vozliščno tranzitiven.

Rešitev. Preprosto je videti, da vrtenje 72° pusti Petersenov graf nespremenjen, zato lahko katero koli točko "zunanjega" 5-cikla $0, 1, 2, 3, 4$ preslikamo v katero koli drugo točko "zunaj" 5-cikla in podobno je mogoče katero koli točk "znotraj" 5-cikla $0', 1', 2', 3', 4'$ preslikati v katero koli drugo točko v "notranjem" 5-ciklu. Tako je le še treba pokazati, da obstaja avtomorrfizem Petersenovega grafa, ki preslika zunanji 5-cikel v notranji 5-cikel in obratno. Razmislimo o preslikavi $i \mapsto i'$ in $i' \mapsto -i$. Neposredni izračuni (kar bi morali storiti!) potrjujejo, da je ta preslikava avtorfizem Petersenovega grafa in je zato Petersenov graf vozliščno tranzitiven. □



Slika 7: Petersonov graf

Opomba o našem zapisu ciklov. Običajno je cikel označen z zaporedjem vozlišč, recimo $v_0v_1 \dots v_{n-1}v_0$. V prejšnjem odstavku opazimo, da smo uporabili nekoliko nestandardni zapis $v_0, v_1, \dots, v_{n-1}, v_0$, saj pri uporabi števil za oznake vozlišč pogosto lahko pride do dvoumnosti, zlasti če ima graf veliko vozlišč. Na primer, graf z množico vozlišč $\mathbb{Z}_{25}$ je lahko cikel 01230 cikel dolžine 4 ali dva različna cikla dolžine 3! Tako lahko uporabljamo vejice med vozlišči pri označevanju ciklov ali ne, če to ne povzroča dvoumnosti. Podoben komentar velja za zapis ciklov permutacij.

Pred naslednjo razpravo potrebujemo nekaj dodatnih definicij.

Definicija 2.99. Naj bo Γ regularen graf. **Valenca** Γ je število povezav, katere so incidentne s katero koli vozliščem. Pravimo, da je Γ kubičen, če je regularen valence 3. Končno je Γ simetričen, če je njegova grupa avtomorfizmov tranzitivna pri svojem delovanju na množici vozlišč in na množici lokov.

3 CAYELYJEVI (DI)GRAFI

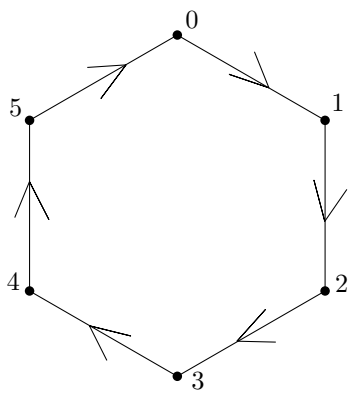
Naš glavni cilj za naslednje razdelke je pridobiti knjižnico primerov in videti, kako zgraditi vozliščno tranzitivne digrafe. Začnemo s Cayleyjevimi digrafi, saj so daleč najpogosteje preučevan in najpogosteje srečan razred vozliščno tranzitivnih digrafov. Po ogledu nekaterih njihovih osnovnih lastnosti bomo podali Sabidussijevo karakterizacijo Cayleyjevih digrafov (3.21) in pokazali, da Petersenov graf ni Cayleyjev graf (3.25).

Definicija 3.1. Naj bo G grupa in $S \subseteq G$. Definirajmo **Cayleyjev digraf** G, označen s $Cay(G, S)$, ki bo digraf z množico vozlišč $V(Cay(G, S)) = G$ in množico lokov $A(Cay(G, S)) = \{(g, gs) : g \in G, s \in S\}$. S je **generatorska množica** $Cay(G, S)$.

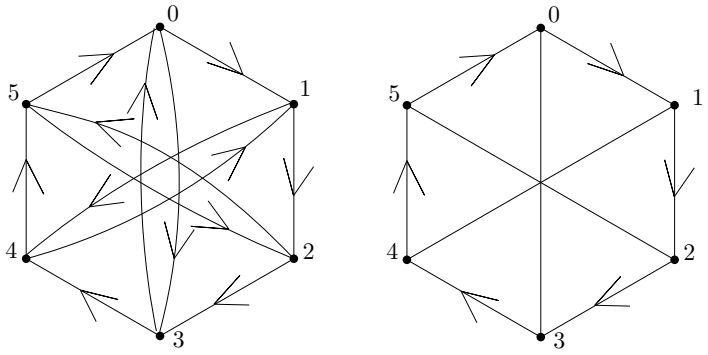
Upoštevajte, da je $(x, y) \in A(Cay(G, S))$, če in samo če je $x^{-1}y \in S$, kot potem $x = g$ in $y = gs$, tako da je $xy^{-1} = s$ (slednji pogoj se pogosto uporablja namesto prejšnjega pogoja v definiciji Cayleyjevega digrafa).

Primer 3.2. Naj bo $Cay(G, S)$ (di)graf z množico vozlišč $V(Cay(G, S)) = G$ in množico lokov $A(Cay(G, S)) = \{(g, gs) : s \in S\}$.

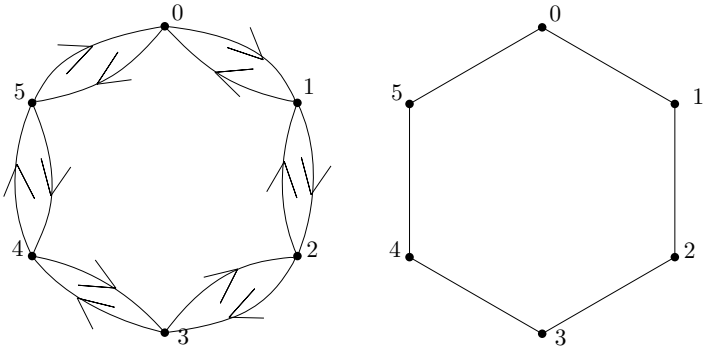
- če je $G = \mathbb{Z}_6$ in $S = \{1\}$. Potem $Cay(\mathbb{Z}_6, \{1\})$ na sliki 8 je digraf.
- če je $G = \mathbb{Z}_6$ in $S = \{1, 3\}$. Potem $Cay(\mathbb{Z}_6, \{1, 3\})$ na sliki 9 je digraf.
- če je $G = \mathbb{Z}_6$ in $S = \{1, 5\}$. Potem $Cay(\mathbb{Z}_6, \{1, 5\})$ na sliki 10 je graf.



Slika 8: Cayleyjev digraf $Cay(\mathbb{Z}_6, \{1\})$

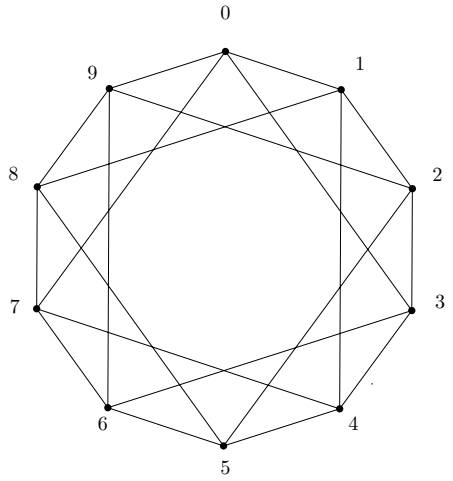


Slika 9: Cayleyjev digraf $Cay(\mathbb{Z}_6, \{1, 3\})$



Slika 10: Cayleyjev graf $Cay(\mathbb{Z}_6, \{1, 5\})$

Primer 3.3. Graf na sliki 11 je $Cay(\mathbb{Z}_{10}, \{1, 3, 7, 9\})$. Upoštevajmo, da ker je binarna operacija na $\mathbb{Z}_{10}$ seštevanje, obstaja povezava med dvemi vozlišči, če in samo če je razlika med oznakami na vozliščih vsebovana v množici $\{1, 3, 7, 9\}$. Upoštevajmo, da obračanje grafa v smeri urnega kazalca za 36°, ga ne spremeni.



Slika 11: Cayleyjev graf $Cay(\mathbb{Z}_{10}, \{1, 3, 7, 9\})$

Lema 3.4. *Digraf $Cay(G, S)$ je **graf**, če in samo če je $S = S^{-1}$ (ali, zapisano aditivno, da je $S = -S$).*

Dokaz. Recimo, da $Cay(G, S)$ je graf. Potem $(g, gs) \in A(Cay(G, S))$, če in samo če $(gs, g) \in A(Cay(G, S))$, če in samo če $(gs)^{-1}g = s^{-1} \in S$. Recimo, da je $S = S^{-1}$. Če je $(g, gs) \in A(Cay(G, S))$, potem je $(gs, gs(s^{-1)}) = (gs, s) \in A(Cay(G, S))$. □

V mnogih primerih, ima ali nima Cayleyjev digraf zanke, nima nobenega učinka. V teh primerih je ponavadi privzeto izključiti zanke, tako da vztrajamo tudi, da je $1_G \notin S$ (ali $0 \notin S$, če je G abelova grupa in operacija je seštevanje). Številni običajni grafi so izomorfni Cayleyjevim grafom.

Primer 3.5. 3-kocka, kot je narisana na sliki 6, je $Cay(\mathbb{Z}_2^3, S)$, kjer je $S = \{(0, 0, 1), (0, 1, 0), (1, 0, 0)\}$). Upoštevajmo, da za $\mathbb{Z}_2^n$ je vsak element svoj inverz in tako so Cayleyjevi digrafi od $\mathbb{Z}_2^n$ vedno grafi.

Primer 3.6. Naj bo $n \geq 3$ pozitivno celo število. Cikel dolžine n je izomorfen $Cay(\mathbb{Z}_n, \{1, n-1\})$.

Primer 3.7. Naj bo G grupa, $n = |G|$ in $S = G\backslash\{1_G\}$. Potem je $Cay(G, S)$ izomorfen K_n.

Primer 3.8. Naj bo $n \geq 1$, S pa podmnožica $\mathbb{Z}_{2n}$, sestavljena iz vseh n lihih števil. Potem je $Cay(\mathbb{Z}_n, S)$ izomorfen $K_{n,n}$.

Cayleyjev digraf brez zank, čigar generatorska množica ima d elementov, je regularen glede na izstopno in vhodno valenco d.
Morda najpogostejši Cayleyjevi digrafi, s katerimi se srečujemo, so Cayleyjevi digrafi cikličnih grup $\mathbb{Z}_n$ reda n, kot v primeru 3.3.

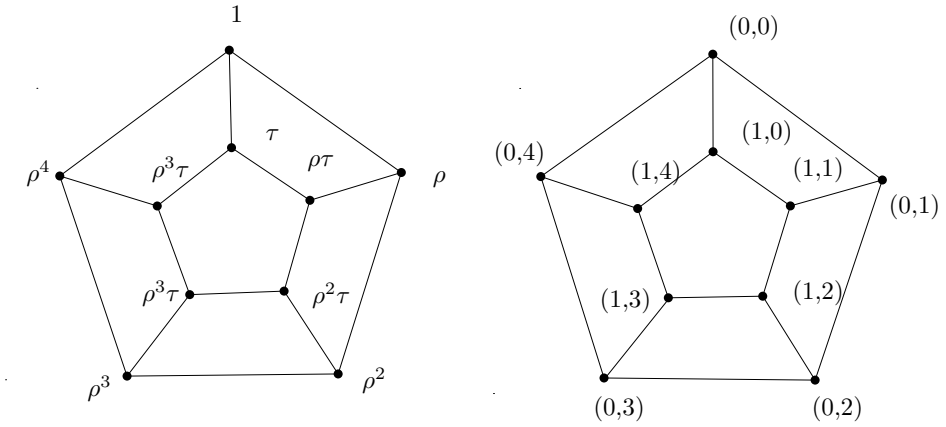
Definicija 3.9. Cayleyjev (di) graf $\mathbb{Z}_n$ se imenuje **cirkulantski (di)graf** reda n.

V naslednjem primeru preučujemo Cayleyjev graf diedrske grupe.

Spomnimo se, diedrska grupa D_{2n} reda $2n$ je simetrija pravilnega n-kotnika in ima predstavitev $\langle \rho, \tau : \rho^n = \tau^2 = 1, \tau^{-1}\rho\tau = \rho^-1\rangle$.

Primer 3.10. Cayleyjeva grafa $Cay(\mathbb{Z}_2 \times \mathbb{Z}_5, \{(0, 1), (0, 4), (1, 0)\})$ in $Cay(D_{10}, \{\rho, \rho^4, \tau\})$ sta izomorfna.

Rešitev. Graf na levi na sliki 12 je $Cay(D_{10}, \{\rho, \rho^4, \tau\})$, medtem ko je graf na desni na sliki 12 $Cay(\mathbb{Z}_2 \times \mathbb{Z}_5, \{(0, 1), (0, 4), (1, 0)\})$ in so na videz izomorfni. Tako je možno, da je graf izomorfen Cayleyjevim grafom različnih grup, in ker je Cayleyjev graf G, ni invarianten pri izomorfizmu. Lahko je videti, da obračanje za 72° ne spremeni ničesar pri zgornjih grafih. Poleg tega ni težko videti, da lahko preslikamo "notranji" 5-cikel na "zunanji" 5-cikel in obratno. □



Slika 12: $Cay(D_{10}, \{\rho, \rho^4, \tau\})$ in $Cay(\mathbb{Z}_2 \times \mathbb{Z}_5, \{(0,1), (0,4), (1,0)\})$

Definicija 3.11. Naj bo G grupa in $g \in G$. Definirajmo $g_L : G \mapsto G$ z $g_L(x) = gx$. Preslikava g_L je **levi premik** G. **Leva regularna predstavitev** G, označena z G_L, je $G_L = \{g_L : g \in G\}$. To pomeni, da G_L sestavljajo vsi levi premiki G. Preprosto je preveriti, da je G_L grupa, ki je izomorfna G.

Naj bo $x, y \in G$ in $g = yx^{-1}$. Potem je $g_L(x) = yx^{-1}x = y$, tako da je G_L tranzitivna na G. Upoštevajmo tudi, da $g_L(x) = x$ nam da $gx = x$ ali $g = 1$. Edini element G_L, ki fiksira točko, je identiteta. Zato je G_L regularna.

Permutacije, omenjene na koncu primera 3.3, generira $G_L = (\mathbb{Z}_{10})_L$, medtem ko permutacije, omenjene na koncu primera 3.10, generirajo $(\mathbb{Z}_{10})_L$ (ne pa $(D_{10})_L$). Če si želimo ogledati generatorje $(D_{10})_L$ iz primera 3.10, opazimo, da obstaja preslikava, katera tudi pusti grafe nespremenjene (najbolj očiten je dobljen s preslikavo okoli navpične črte skozi sredino grafa - ostale preslikave lahko dobimo z obračanjem te črte za 72°). Nato dobimo grupo $(D_{10})_L$ z obračanjem za 72° in nato preslikava notranji 5-cikel na zunanji 5-cikel.

Na splošno so za abelovo grup G premiki G sestavljeni iz preslikave $x \mapsto g+x = x+g$, $g \in G$. Tj., $G_L = \{x \mapsto x + g : g \in G\}$. Natančneje, za ciklično grupo $\mathbb{Z}_n$ imamo $\mathbb{Z}_n$, ki jo generira preslikava $x \mapsto x + 1$ (ali seveda bi namesto 1 lahko postavili kateri koli generator $\mathbb{Z}_n$).

Lema 3.12. *Če je G grupa in $S \subseteq G$, potem je $G_L \leq Aut(Cay(G, S))$. Še posebej Cayleyjev digraf grupe G je vozliščno tranzitiven digraf.*

Dokaz. Naj bo $g \in G$ in $s \in S$, torej $(g, gs) \in A(Cay(G, S))$. Naj bo $h \in G$. Potem je $h_L(g, gs) = (hg, hgs) = (g', g's) \in A(Cay(G, S))$ kjer je $g' = hg$. Potem je $h_L \in Aut(Cay(G, S))$ torej $G_L \leq Aut(Cay(G, S))$. Kot smo že ugotovili, je G_L tranzitiven, $Aut(Cay(G, S))$ je tranzitven in torej je $Cay(G, S)$ vozliščno tranzitiven digraf. □

Nekateri avtorji bodo Cayleyjeve digrafe definirali na desni, tako da bo **desna regularna predstavitev** G_R vsebovana v grupi avtomorfizmov.

Tako kot večina avtorjev tudi tu počnemo stvari "za nazaj". Določili smo namreč Cayleyjev digraf G glede na vozlišča in povezave (kot je običajno pri definiranju grafa!), Nato pa pokazali, da je grupa G_L vsebovana v njeni grupi avtomorfizmov. To pa ni pravi način, kako bi morali razmišljati o tem, kako zgraditi Cayleyjev digraf. Namesto tega pomislimo na S kot na zunanjega soseda identitete (kar v resnici tudi sta), nato pa uporabimo grupo G_L, da "izpolnimo" preostale loke v digrafu z uporabo elementov G_L na lokih med identiteto in njenimi sosedi. Upoštevajmo, da je pri tej metodi konstrukcije Cayleyjevega digrafa G_L avtomatsko podgrupa grupe avtomorfizmov.

Nekateri avtorji bodo pri opredeljevanju Cayleyjevega digrafa vztrajali predvsem iz zgodovinskih razlogov, da je $\langle S\rangle = G$ (čeprav očitno, to ni potreben pogoj, da bi lahko definirali Cayleyjeve digrafe). Naslednji rezultat kaže, da je $\langle S\rangle = G$ enakovredno vztrajanju, da so vsi Cayleyjevi digrafi povezani. Opažamo, da je naša predstava o povezanem digrafu Γ ta, da obstaja usmerjena pot med katerima kolima dvema vozliščema. To pomeni, da če je $u, v \in V(\Gamma)$ obstaja pot $w_1 \dots w_r$ v Γ z $u = w_1, v = w_r$ in $(w_i, w_{i+1}) \in A(\Gamma)$. Mnogi avtorji se na to sklicujejo, da je Γ **krepko povezan**, pri čemer je šibkejši pogoj, da obstaja pot med katerimi koli vozlišči v spodnjem preprostem grafu Γ, kot **šibko povezan** digraf.

Lema 3.13. *Naj bo G grupa in $S \subseteq G$. Cayleyjev digraf $Cay(G, S)$ je krepko povezan, če in samo če je $\langle S\rangle = G$.*

Dokaz. Predpostavimo, da je $\langle S\rangle = G$. Naj bo $x, y \in G$ in $g = x^{-1}y$. Potem obstajajo $s_1, \dots, s_r \in S$ tako, da $s_1 s_2 \cdots s_r = g$. Za $1 \leq i \leq r$, naj bo $v_i = s_1 s_2 \cdots s_i$. Upoštevajmo, da je $(v_i, v_i s_{i+1}) = (v_i, v_{i+1})$, tako da je v G lok od v_i do v_{i+1}. Potem je $W = 1_G v_1 \cdots v_r$ sprehod po $Cay(G, S)$ od 1_G do g. Upoštevajmo, da je $x_L(1_G) = x$ in $x_L(g) = y$, zato je $x_L(W)$ sprehod v G od x do y. Tako je G krepko povezan. Predpostavimo, da je $Cay(G, S)$ krepko povezan. Potem za vsak $g \in G$ obstaja pot $P_g = v_0 v_1 \dots v_r$ v $Cay(G, S)$ od 1_G do g, kjer je $v_0 = 1_G$ in $v_r = g$. Kot $(v_i, v_{i+1}) \in A(Cay(G, S))$ je $v_{i+1} = v_i s_i$ za nekatere $s_i \in S$. Potem je $g = s_0 \dots s_r$ in $g \in \langle S\rangle$. Ker je g poljuben, $\langle S\rangle = G$. □

Zdaj se obrnemo na razmerje med Cayleyjevim digrafom grupe G in $Aut(G)$, **grupo avtomorfizmov** G.

Lema 3.14. *Naj bosta G in H izomorfni grupi z izomorfizmom $\alpha : G \mapsto H$. Naj bo $S \subseteq G$. Potem je $\alpha(Cay(G, S)) \cong Cay(H, \alpha(S))$. Še posebej, če je $H = G$, potem je $\alpha(Cay(G, S))$ Cayleyjev digraf G z generatorsko množico $\alpha(S)$ ali ekvivalentno $\alpha(Cay(G, S)) = Cay(G, \alpha(S))$.*

Dokaz. Jasno $\alpha : G \to H$, tako da je $V(\alpha(Cay(G,S))) = H$. Naj je $a = (g, gs) \in A(Cay(G,S))$, kjer sta $g \in G$ in $s \in S$. Potem $\alpha(a) = \alpha(g, gs) = (\alpha(g), \alpha(gs)) = (\alpha(g), \alpha(g)\alpha(s)) = (h, hs')$ kjer je $h = \alpha(g)$ in $s' = \alpha(s) \in \alpha(S)$. Nato α preslika loke od $Cay(G,S)$ na loke $Cay(H, \alpha(S))$ bijektivno kot $|S| = |\alpha(S)|$. Torej $\alpha(Cay(G,S)) = Cay(H, \alpha(S))$, kot je zahtevano. Rezultat sledi z nastavitvijo $H = G$. □

Na splošno je precej netrivialno preverjati, ali je permutacija v grupi avtomorfizmov grafa ali ne. Za Cayleyjeve digrafe grupe G in avtomorfizme G je to enostavno preveriti!

Posledica 3.15. *Naj bo G grupa, $S \subseteq G$ in $\alpha \in Aut(G)$. Potem je $\alpha \in Aut(Cay(G,S))$ če in samo če je $\alpha(S) = S$.*

Primer 3.16. Kateri avtomorfizmi $\mathbb{Z}_{15}$ so vsebovani v grupi avtomorfizmov $\Gamma = Cay(\mathbb{Z}_{15}, \{1,3,4,12\})$?

Rešitev. Avtomorfizmi $\mathbb{Z}_{15}$ so sestavljeni iz množenja z enotami v $\mathbb{Z}_{15}$. To pomeni, da so avtomorfizmi $\mathbb{Z}_{15}$ preslikave $x \mapsto ax$, kjer je $a \in Z_{15}^*$. Ker je $1 \in S = \{1,3,4,12\}$, moramo samo preveriti, katera cela števila 3,4,12 povzročajo avtomorfizme Γ. Ker je 4 edina enota med $\{3,4,12\}$, moramo samo preveriti, ali je $x \mapsto 4x$ avtomorfizem Γ, saj je $x \mapsto 1x$ identiteta in je vedno v $Aut(\Gamma)$. Ker je $4 \cdot \{1,3,4,12\} = \{4,12,1,3\}$, vidimo, da je $x \mapsto 4x$ res avtomorfizem Γ, zato so avtomorfizmi $\mathbb{Z}_{15}$, ki jih vsebuje Γ, $x \mapsto ax$, kjer je $a = 1$ ali 4. □

Posledica 3.17. *Naj bo G abelova grupa, $G \neq \mathbb{Z}_2^k$ za nekaj $k \geq 1$ in $S \subseteq G$ takšna, da je $S = -S$. Potem je $Aut(Cay(G,S)) \neq G_L$, še posebej pa je preslikava $\iota : G \mapsto G$, podana z $\iota(g) = -g$, v $Aut(Cay(G,S))$ in $\iota \neq 1$.*

Dokaz. Za grupo G je preslikava $x \mapsto x^{-1}$ avtomorfizem grupe, če in samo če je G abelova (v tem primeru je bolj primerno preslikavo zapisati $x \mapsto -x$ in tudi ι). Če je torej $Cay(G,S)$ Cayleyjev graf, tako da je $S = -S$, potem je $\iota \in Aut(Cay(G,S))$ po posledici 3.15. Opažamo edino abelovo grupo, tako da je vsak element lastni inverz (in za katero je $\iota = 1_G$) grupe $\mathbb{Z}_2^k$, $k \geq 1$. Če je G abelova, je $G \neq \mathbb{Z}_2^k$, $k \geq 1$ in $Cay(G,S)$ je Cayleyjev graf G, nato $Aut(Cay(G,S)) \neq G_L$. □

Eden prvih večjih problemov, ki smo ga obravnavali v zvezi s simetrijami v grafih, je bilo vprašanje, ali obstaja Cayleyjev (di) graf G, katerega grupa avtomorfizmov je G.

Definicija 3.18. Naj bo $\Gamma = Cay(G,S)$ digraf in $Aut(\Gamma) = G_L$, potem Γ je **usmerjena regularna predstavitev**, oziroma **DRR**, medtem ko naj bo $\Gamma = Cay(G,S)$ graf in $Aut(\Gamma) = G_L$, potem je **grafična regularna predstavitev** G, oziroma **GRR**.

Prejšnji rezultat pokaže, da Cayleyjevi grafi abelovih grup, ki niso elementarno abelove 2-grupe niso GRR.

Primer 3.19. Kateri avtomorfizmi $\mathbb{Z}_8$ so vključeni v grupo avtomorfizmov $\Gamma = Cay(\mathbb{Z}_8, \{2, 6\})$?

Rešitev. Najprej opazimo, da je $S = -S$, tako da je Γ graf in je po posledici 3.17 preslikava $x \mapsto -x$ vsebovana v $Aut(\Gamma)$. Avtomorfizmi $\mathbb{Z}_8$ so sestavljeni iz množenja z enotami v $\mathbb{Z}_8$. Upoštevajmo, da če je $x \mapsto ax$ v $Aut(\Gamma)$, potem je tudi $x\ x \mapsto -ax$ v $Aut(\Gamma)$. Torej moramo samo preveriti, katere enote v $\mathbb{Z}_8$ med 1 in 4 inducirajo avtomorfizme Γ, saj avtomorfizmi, ki jih inducirajo enote med 1 in 4, sestavljene z $x \mapsto -x$, dajejo avtomorfizme $\mathbb{Z}_{16}$, inducirane z enotami med 5 in 7. Z računanjem $3 \cdot \{2, 6\} = \{6, 2\}$ vidimo, da $Aut(\Gamma)$ vsebuje $x \mapsto ax$ za $a = 1, 3, 5, 7$. □

Primer 3.20. Kateri avtomorfizmi $\mathbb{Z}_{16}$ so vključeni v grupo avtomorfizmov $\Gamma = Cay(\mathbb{Z}_{16}, \{1, 2, 5, 6, 10, 11, 14, 15\})$?

Rešitev. Najprej opazimo, da je $S = -S$, tako da je Γ graf in je po posledici 3.17 preslikava $x \mapsto -x$ vsebovana v $Aut(\Gamma)$. Avtomorfizmi $\mathbb{Z}_{16}$ so sestavljeni iz množenja z enotami v $\mathbb{Z}_{15}$. Upoštevajmo, da če je $x \mapsto ax$ v $Aut(\Gamma)$, potem je tudi $x\ x \mapsto -ax$ v $Aut(\Gamma)$. Torej moramo samo preveriti, katere enote v $\mathbb{Z}_{16}$ med 1 in 8 inducirajo avtomorfizme Γ. Torej moramo samo preveriti, ali je $x \mapsto 5x$ avtomorfizem Γ. Upoštevajmo, da je $5 \cdot \{1, 2, 5, 6, 10, 11, 14, 15\} = \{5, 10, 9, 14, 2, 7, 6, 11\} \neq S$, torej edini avtomorfizem $\mathbb{Z}_{16}$ v $Aut(\Gamma)$ je identiteta in $x \mapsto -x$. □

Naslednji pomemben rezultat Sabidussija [17] karakterizira Cayleyjeve digrafe.

Izrek 3.21. *Digraf Γ je izomorfen Cayleyjevemu digrafu grupe G, če in samo če $Aut(\Gamma)$ vsebuje regularno podgrupo, izomorfno G.*

Dokaz. Če je $\Gamma \cong Cay(G, S)$ z $\phi : \Gamma \to Cay(G, S)$ izomorfizem, potem po lemi 3.12, $Aut(Cay(G, S))$ vsebuje regularno podgrupo $G_L \cong G$, in sicer $\phi^{-1} G_L \phi$.

Za nasprotno domnevamo, da $Aut(\Gamma)$ vsebuje regularno podgrupo $H \cong G$, z $\omega : H \to G$ izomorfizem. Fiksirajmo $v \in V(\Gamma)$. Ker je H regularen, za vsak $u \in V(\Gamma)$ po [[8] Vaja 1.1.2] obstaja enolično določen $h_u \in H$, takšen, da je $h_u(v) = u$. Definirajmo $\phi : V(\Gamma) \to G$ z $\phi(u) = \omega(h_u)$. Preslikava ϕ je naš izomorfizem iz Γ v Cayleyjev digraf G. V bistvu izberemo vozlišče v, ki ga bomo identificirali (preko ϕ) z identiteto v G. Potem je vozlišče $u \in V(\Gamma)$ identificirano z $\omega(h_u)$. Preostale so nam tehnične podrobnosti, ki dokazujejo, da to deluje.

Najprej upoštevajmo, da je vsak h_u enolično določen, ϕ je dobro definiran in je tudi bijekcija, saj je ω bijekcija. Naj je $U = \{u \in V(\Gamma) : (v, u) \in A(\Gamma)\}$. Trdimo, da je $\phi(\Gamma) = Cay(G, \phi(U))$, kjer je $\phi(\Gamma)$ digraf z $V(\phi(\Gamma)) = \{\phi(v) : v \in V(\Gamma)\}$, in

$A(\phi(\Gamma)) = \{(\phi(u), \phi(v)) : (u, v) \in A(\Gamma)\}$. Ker je $\phi(V(\Gamma)) = G$, imamo $V(\phi(\Gamma)) = G$. Naj je $a \in A(\phi(\Gamma))$. Pokazati moramo, da je $a = (g, gs)$ za nekatere $g \in G$ in $s \in \phi(U)$. Kot $a \in A(\phi(\Gamma))$ je $\phi^{-1}(a) = (u_1, u_2) \in A(\Gamma)$ z [[8] Vaja 1.1.12]. Naj bo $w \in V(\Gamma)$ tak, da je $h(w) = u$. Potem je $h^{-1}(u_1, u_2) = (v, w) \in A(\Gamma)$, tako da je $w = h_w(v) \in U$. Tudi $h_{u_2} = h_{u_1}h_w$ kot $h_{u_1}h_w(v) = h_{u_1}(w) = u_2$. Nastavimo $g = \omega(h_{u_1})$ in $s = \omega(hw) \in \phi(U)$. Potem,

$$a = \phi(u_1, u_2) = (\omega(h_{u_1}), \omega(h_{u_2})) = (\omega(h_{u_1}), \omega(h_{u_1}h_w)) = (\omega(h_{u_1}), \omega(h_{u_1})\omega(h_w)) = (g, gs)$$

kot smo zahtevali. □

Ta odsek končamo z navedbo primera vozliščno tranzitivnega grafa, ki ni izomorfen Cayleyjevemu grafu. Naš primer je Petersenov graf (glej sliko 7), ki sta skupaj s komplementom najmanjša (glede na število vozlišč) ne-Cayleyjevi vozliščno tranzitivni grafi. Pred nadaljevanjem dokažemo teoretični rezultat grupe, ki bo poenostavil dokazovanje (in tudi rezultat ali njegove posplošitve se uporabljajo za poenostavitev številnih dokazov).

Lema 3.22. *Naj bo* $G = \langle \rho, \tau : \rho^m = \tau^n = 1, \tau^{-1}\rho\tau = \rho^a, 1 \leq a \leq m \rangle$. *Če je* $\rho_1, \tau_1 \in \langle \rho, \tau \rangle$ *tako, da je* $\rho_1^m = \tau_1^n = 1, \tau_1^{-1}\rho_1\tau_1 = \rho_1^a$ *in* $\langle \rho_1, \tau_1 \rangle = \langle \rho, \tau \rangle$, *potem obstaja* $\alpha \in Aut(G)$, *tako da je* $\alpha(\tau) = \tau_1$ *in* $\alpha(\rho) = \rho_1$.

Dokaz. Ker $\rho_1\tau_1 = \tau_1\rho_1^a$ lahko vsak element G zapišemo enolično kot $\tau_1^x\rho_1^y$ za $0 \leq x \leq n-1$ in $0 \leq y \leq m-1$. Določimo $\alpha : G \mapsto G$ z $\alpha(\tau^x\rho^y) = \tau_1^x\rho_1^y$. Ker je $\rho\tau = \tau\rho^a$, lahko vsak element G zapišemo tudi enolično kot $\tau^x\rho^y$, $0 \leq x \leq n-1$ in $0 \leq y \leq m-1$. To pomeni, da je α bijekcija kot $\langle \rho_1, \tau_1 \rangle = \langle \rho, \tau \rangle$. Potem

$$\tau^x\rho^y\tau^u\rho^v = \tau^x\tau\rho^{ay}\tau^{u-1}\rho^v = \tau^x\tau^2\rho^{a^2y}\tau^{u-2}\rho^v = \ldots = \tau^x\tau^u\rho^{a^uy}\rho^v = \tau^{x+u}\rho^{a^uy+v}$$

n analogno temu $\tau_1^{x+u}\rho_1^{a^uy+v} = \tau_1^x\rho_1^y\tau_1^u\rho_1^v$. Potem

$$\alpha(\tau^x\rho^y\tau^u\rho^v) = \alpha(\tau^{x+u}\rho^{a^uy+v}) = \tau_1^{x+u}\rho_1^{a^uy+v} = \tau_1^x\rho_1^y\tau_1^u\rho_1^v = \alpha(\tau^x\rho^y)\alpha(\tau^u\rho^v)$$

in $\alpha \in Aut(G)$. □

Podoben rezultat velja za katero koli grupo, ki jo ustvari končni seznam elementov skupaj s končnim seznamom definirajočih razmerij. Glej [[7], str. 5].

Definicija 3.23. Ožina je najmanjša dolžina cikla v grafu.

Trditev 3.24. *Povezan Cayleyjev graf abelove grupe z valenco vsaj* 3 *ima ožino največ* 4.

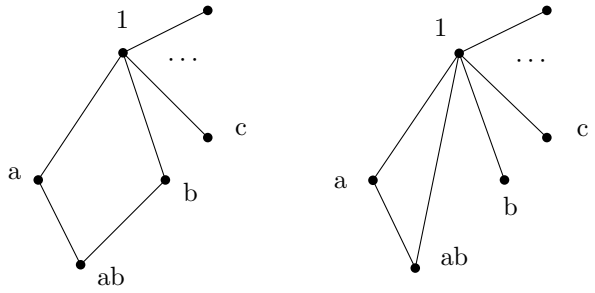
Dokaz. Naj bo $Cay(G, S)$ povezan Cayleyjev graf na abelovi grupi z valenco vsaj 3. Naj bo $|S| \geq 3$, $S = \{a, b, c, \ldots\}$.
Opazimo, da

$$a \sim a \cdot b$$

$$b \sim b \cdot a,$$

ker imamo abelovo grupo velja $b \cdot a = a \cdot b$.
Predpostavimo, da $ab \neq 1$:

- Če $ab \notin S$ imamo cikel dolžine 4, in sicer $1, a, ab, b, 1$.
- Če je $ab \in S$, potem imamo cikel dolžine 3, namreč, $1, a, ab, 1$.



Slika 13: Cikel dolžine 4 in cikel dolžine 3

Predpostavimo, da je $ab = 1 \Rightarrow b = a^{-1}$. Lahko ponovimo zgornji argument za a in c, namesto a in b, ker je $ac \neq 1$. □

Izrek 3.25. *Petersenov graf ni Cayleyjev graf.*

Dokaz. Dokazali bomo s protislovjem in predpostavljamo, da je Petersenov graf P Cayleyjev graf Cay (G, S), kjer $|G| = 10$ in $|S| = 3$. Ker je $|G| = 10, G = \mathbb{Z}_{10}$ ali D_{10}, saj so to edine grupe reda 10. Če je $G = \mathbb{Z}_{10}$, je ožina P največ 4. Vendar ima P ožino 5. Tako je $P = Cay(D_{10}, S)$.

Pred nadaljevanjem bo koristno pregledati nekatere lastnosti D_{10}. $D_{10} = \langle \rho, \tau \rangle$ nastavimo kot v definiciji D_{2n} in se spomnimo, da je $\langle \rho \rangle \trianglelefteq D_{10}$. Poleg tega ima $\langle \rho \rangle$ v D_{10} dva leva odseka, in sicer $\langle \rho \rangle$ in $\tau\langle \rho \rangle = \{\tau, \tau\rho, \tau\rho^2, \tau\rho^3, \tau\rho^4\}$. D_{10} ima kot simetrije pravilnega petkotnika 5 rotacij, od katerih je vsaka vsebovana v $\langle \rho \rangle$, od katerih imajo štirje elementi red 5, ostali pa 1. Ker ima D_{10} 5 elementov reda 2,so ti elementi levega odseka $\tau\langle \rho \rangle$.

Zdaj razmislimo o dveh možnostih za S, in sicer, da je S sestavljen iz treh involucij (elementi reda 2), ali pa je S involucija skupaj z elementom, ki ni sam svoj inverz skupaj s svojim inverzom. V slednjem primeru je element, ki ni involucija, vsebovan v $\langle \rho \rangle$. Če je S sestavljen izključno iz involucij, potem v $\langle \rho \rangle$ (to je podgrupa reda 5)

ne more biti noben element S, zato je vsak element S vsebovan v levem odseku $\tau\langle\rho\rangle$. Nato ima vsaka povezava P eno končno točko v $\langle\rho\rangle$, ostali pa v levem odseku $\tau\langle\rho\rangle$. Torej je P dvodelna, kar ni res, saj vsebuje lihe cikle. Potem mora biti S sestavljen iz dveh elementov reda 5, ki sta medsebojno inverzna, recimo ρ_1 in ρ_1^{-1}, in involucije, recimo τ_1, ker je P graf. Potem $\rho_1 = \rho^b$ za nek $1 \leq b \leq 4$ in $\tau_1 = \tau\rho^c$, za nek c. Zato je $\rho_1^5 = \tau_1^2 = 1$ in

$$\tau_1^{-1}\rho_1\tau_1 = (\tau\rho^c)^{-1}\rho^b\tau\rho^c = \rho^{-c}\tau^{-1}\rho^b\tau\rho^c = \rho^{-c}\rho^{-b}\rho^c = \rho^{-b} = (\rho_1)^{-1}.$$

Po lemi 3.22 obstaja $\alpha \in Aut(D_{10})$ tako, da je $\alpha(\rho_1) = \rho$ in $\alpha(\tau_1) = \tau$. Potem je $P \cong Cay(D_{10}, \{\rho, \rho^4, \tau\})$ po lemi 3.14. Vendar je v primeru 3.10 $Cay(D_{10}, \{\rho, \rho^4, \tau\})$ izomorfen Cayleyjevemu grafu $\mathbb{Z}_{10}$, kar je protislovje. □

Za dokazovanje izrekov v drugem poglavju najprej potrebujemo naslednje izreke.

Izrek 3.26. *Tranzitivna grupa praštevilske stopnje p vsebuje regularno ciklično podgrupo. Posledično je vsak vozliščno tranzitivni digraf praštevilskega reda p izomorfen Cayleyjevemu digrafu $\mathbb{Z}_p$.*

Dokaz. Naj je G tranzitivna grupa praštevilske stopnje p. Po izreku o stabilizatorju orbite velikost orbite grupe deli vrstni red grupe. Ker je G tranzitiven, ima eno orbito velikosti p, zato p deli $|G|$. Potem G vsebuje element reda p po Cauchyjevem izreku. Ker je $G \leq S_p$, mora biti kateri koli element reda p p-cikel ρ. Potem je $\langle\rho\rangle$ regularna ciklična podgrupa, rezultat pa sledi po izreku 3.21 □

Definicija 3.27. Permutacijska grupa $G \leq S_n$ je **2-tranzitivna**, če kadar koli

$$(x_1, y_1), (x_2, y_2) \in \mathbb{Z}_n \times \mathbb{Z}_n$$

tako, da $x_1 \neq y_1$ in $x_2 \neq y_2$, potem obstaja $g \in G$, tako da $g(x_1, y_1) = (x_2, y_2)$. To pomeni, da je grupa 2-tranzitivna pod pogojem, da za katera koli dva nediagonalno urejena para obstaja element grupe, ki preslika enega v drugega.

Izrek 3.28. *Naj bo $G \leq S_p$, p praštevilo, tranzitivna, tako da je preslikava $x \mapsto x+1$ v G. Potem je bodisi G 2-tranzitivna bodisi $G < AGL(1,p) = \{x \mapsto ax + b : a \in \mathbb{Z}_p^*, b \in \mathbb{Z}p\} \cong \mathbb{Z}_p^* \cdot \mathbb{Z}_p$.*

Center grupe G, označeno z $Z(G)$, je množica vseh elementov G, ki komutirajo z vsakim elementom G. To pomeni, da je $Z(G) = \{g \in G : gx = xg \text{ za vse } x \in G\}$. Preprosto je preveriti, da je $Z(G)$ podgrupa edinka, dejansko karakteristična podgrupa G.

Lema 3.29. *Center $Z(G)$ tranzitivne grupe $G \leq S_n$ je polregularen.*

Dokaz. Recimo, da je $\alpha \in Z(G)$ in $\alpha(x) = x$. Ker je G tranzitiven, za vsak $y \in \mathbb{Z}_n$ obstaja $g_y \in G$, tako da je $g_y(x) = y$. Potem je $\alpha g_y = g_y \alpha$ in tako

$$y = g_y(x) = g_y\alpha(x) = \alpha g_y(x) = \alpha(y)$$

in tako $\alpha(y) = y$ za vse $y \in \mathbb{Z}_n$. □

Lema 3.30. *Naj bo G grupa, $H \leq G$ in $\alpha \in Aut(G)$. Naj bo $K = \alpha(H)$. Potem je $\bar{\alpha} : G/H \to G/K$ z $\bar{\alpha}(gH) = \alpha(g)K$ dobro definirana bijekcija.*

Dokaz. Da pokažemo, da je $\bar{\alpha}$ dobro definirana, predpostavimo, da $g_1, g_2 \in G$ in $g_1H = g_2H$. Ker je $\alpha(H) = K$ in $\alpha \in Aut(G)$, je $\alpha(g_iH) = \alpha(g_i)K$ za $i = 1, 2$ in $\bar{\alpha}$ preslika G/H v G/K. Potem je $\alpha(g_1)K = \alpha(g_1H) = \alpha(g_2H) = \alpha(g_2)K$ in je $\bar{\alpha}$ dobro definirana. Da je $\bar{\alpha}$ znotraj, sledi, ker je α znotraj. Končno, če je $\bar{\alpha}(g_1H) = \bar{\alpha}(g_2H)$, potem je $\alpha(g_1)K = \alpha(g_2)K$, torej $\alpha(g_2^{-1}g_1)K = K$ in $\alpha(g_2^{-1}g_1) \in K$. Ker je $\alpha(H) = K$, $g_2^{-1}g_1 \in H$ in $g_1H = g_2H$. Tako je $\bar{\alpha}$ ena proti ena in je torej bijekcija od G/K. □

Definicija 3.31. Naj bo G grupa s podgrupo $H \leq G$ in $\alpha \in Aut(G)$, tako da je $\alpha(H) = H$. Definirajmo $\bar{\alpha} : G/H \to G/H$ z $\bar{\alpha}(gH) = \alpha(g)H$.

Spomnimo se, da je $\bar{\alpha}$ dobro definirana permutacija G/H po lemi 3.30.

Lema 3.32. *Naj bo G grupa in $H \leq G$ brez jedra v G. Naj bo $\bar{A} = \{\bar{\alpha} : \alpha \in Aut(G)$ in $\alpha(H) = H\}$. Potem je $N_{S_{G/H}}(G, G/H) = \bar{A}(G, G/H)$.*

Dokaz. Ker je H brez jedra v G, je levo delovanje G na G/H zvesto. Naj bo $\delta \in N_{S_{G/H}}(G, G/H)$. Ker je $(G, G/H)$ tranzitivna na množici levih odsekov H v G, obstaja $\hat{\ell}_1 \in (G, G/H)$ tako, da je $\hat{\ell}_1\delta(H) = H$. Ker je $\delta^{-1}\hat{\ell}_1\delta \in (G, G/H)$, obstaja $\hat{\ell} \in (G, G/H)$ z $\delta^{-1}\hat{\ell}_1\delta = \hat{\ell}$, zato je $\delta\hat{\ell}(H) = H$. Naj bo $\beta = \delta\hat{\ell}$. Ko se $\hat{\ell}$ in δ normalizirata $(G, G/H)$, se normalizira tudi β. Določite $\alpha : G \to G$ z $\alpha(g) = k$, če in samo če $\beta^{-1}\hat{g}\beta = \hat{k}$. Naj bo $h \in H$. Ker je $\beta(H) = H, \beta^{-1}\hat{h}\beta(H) = H$, zato je $\beta^{-1}\hat{h}\beta$ vsebovano v $(G, G/H)$ in popravi H. Zato je $\beta^{-1}\hat{h}\beta = \hat{h}_1$ za nekatere $h_1 \in H$. Potem je $\alpha(H) = H$. Ker je $\beta^{-1}\hat{g}\hat{h}\beta = \beta^{-1}\hat{g}\beta \cdot \beta^{-1}\hat{h}\beta$, imamo $\alpha(gh) = \alpha(g)\alpha(h)$, zato je α homomorfizem. Jasno je, da je α, inducirano s konjugacijo, injektivno, zato je $\alpha \in Aut(G)$. Upoštevajmo, da je $\beta^{-1}\hat{g}\beta = \hat{\alpha(g)}$ za vse $g \in G$ in da je za $x, g \in G$, $\bar{\alpha}^{-1}\hat{g}\bar{\alpha}(xH) = \bar{\alpha}^{-1}(g\alpha(x)H) = \alpha^{-1}(g)(xH)$, tako da je $\bar{\alpha}^{-1}\hat{g}\bar{\alpha} = \hat{\alpha^{-1}(g)}$. Tako je $\beta^{-1}\bar{\alpha}^{-1}\hat{g}\bar{\alpha}\beta = \beta^{-1}\hat{\alpha^{-1}(g)}\beta = \hat{g}$, tako da $\bar{\alpha}\beta$ komutira z $\hat{g}$ za vsak $g \in G$. Tako se $\bar{\alpha}\beta$ centralizira $(G, G/H)$, tako da po lemi 3.29 imamo $\bar{\alpha}\beta$ je polregularen. Končno, ker je $\beta(H) = \delta\hat{\ell}(H) = H$ in $\alpha(H) = H$, imamo $\bar{\alpha}\beta(H) = H$. Ker je $\bar{\alpha}\beta$ polregularen, imamo $\bar{\alpha}\beta = 1$, zato je $\beta = \bar{\alpha}^{-1}$. Od kod je $\delta = \beta\hat{\ell}^{-1} = \bar{\alpha}^{-1}\hat{\ell}^{-1}$. Tako je $N_{S_{G/H}}(G, G/H) \leq \bar{A}(G, G/H)$. □

Lema 3.33. *Avtomorfizem $\bar{\alpha}$ v $\bar{A}$ je v $(G, G/H)$, če in samo če je $\bar{\alpha}$ notranji avtomorfizem G, induciran s $h \in H$.*

Dokaz. Naj je $g \in G$. Najprej, če je $\bar{\alpha}(gH) = hgh^{-1}H$ za nekaj $h \in H$, potem je $\bar{\alpha}(g) = hgH = \hat{h}_L(gH)$ in $\bar{\alpha} = \hat{h}_L$. Predpostavimo zdaj $\hat{g}_L \in \bar{A}$. Potem je $\hat{g}_L(H) = gH = H$, torej $g \in H$.Tako $\bar{A} \cap (G, G/H) = \{\hat{h}_L : h \in H\}$. □

Če je $H = 1$, potem je G pravilen in imamo naslednji rezultat.

Posledica 3.34. $N_{S_G}(G_L) = G_L \rtimes Aut(G)$.

Dokaz. Po lemi 3.32 $G_L \trianglelefteq Aut(G)G_L$ in $G_L \cap Aut(G) = 1$ po lemi 3.33. Rezultat sledi. □

Definicija 3.35. Za grupo G je **podstavek** G, z oznako $soc(G)$, podgrupa G, generirana iz vseh minimalnih podgrup edink G.

Definicija 3.36. Grupa G je elementarna abelova, če je G $\cong \mathbb{Z}_p^k$ za nekatera praštevila p in $k \geq 1$.

Izrek 3.37. *Naj bo G tranzitivna permutacijska grupa praštevilske stopnje p. Potem je bodisi G 2-tranzitivna z neregularnim neabelovim enostavnim podstavkom bodisi je v G p-Sylowka podgrupa edinka.*

Dokaz. Kot v izreku 3.26 ponovno permutiramo množico G tako, da je preslikava $x \mapsto x + 1$ vsebovana v G. Potem je po izreku 3.28 bodisi je G 2-tranzitivna bodisi $G < AGL(1, p)$. Ker je $AGL(1, p) = N_{S_p}((\mathbb{Z}_p)_L)$ po posledici 3.34, imamo bodisi G 2-tranzitivna bodisi je v G p-Sylowka podgrupa edinka. V slednjem primeru smo dokazali. Če je G 2-tranzitivna, potem še en Burnsideov izrek [[15], teorem 4.1A] navaja, da je podstavek 2-tranzitivne grupe bodisi regularna elementarna abelova p-grupa P je bodisi neregularna neabelova preprosta grupa. V slednjem primeru sledi rezultat. V prejšnjem primeru sta $G \leq S_p$ in $|S_p| = p!$, kjer P je cikličen reda p. Nato G normalizira v S_p ciklično grupo reda p in rezultat tudi sledi. □

Definicija 3.38. Naj $G \leq S_n$ deluje na $\mathbb{Z}_n \times \mathbb{Z}_n$ na kanoničen način, to je $g(x, y) = (g(x), g(y))$. Orbite tega delovanja imenujemo **orbitale**. Ena orbitala je diagonala ali $\{(x, x) : x \in \mathbb{Z}_n\}$ in se imenuje trivialna orbitala. Predpostavljamo, da so $O_1, \ldots, O_r$ netrivialne orbitale. Definirajmo digrafe $\Gamma_1, \ldots, \Gamma_r$ z $V(\Gamma_i) = \mathbb{Z}_n$ in $A(\Gamma_i) = O_i$. Γ_i so **orbitalni digrafi** G.

Trditev 3.39. *Naj bo $G \leq S_n$ tranzitiven. Vsak digraf Γ reda n z $G \leq Aut(\Gamma)$ je posplošen orbitalni digraf od G.*

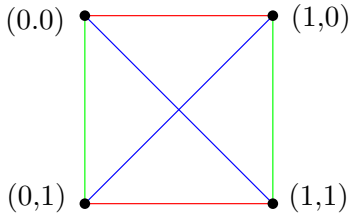
Definicija 3.40. Barvni digraf je digraf, v katerem je vsakemu loku dodeljena barva - običajno je barva samo celo število.

Definicija 3.41. Naj bo X množica in $G \leq S_X$. 2-**zaprtje** grupe G, z oznako $G^{(2)}$, je največja podgrupa grupe S_X, katere orbite na $X \times X$ so enake orbitam grupe G. Če je $G^{(2)} = G$, pravimo, da je G 2-**zaprta**.

Trditev 3.42. *Naj bo* Γ *vozliščno tranzitiven digraf. Potem je* $Aut(\Gamma)$ 2*-zaprt.*

Dokaz. Naj bodo $\Gamma_1, \ldots, \Gamma_r$ orbitalni digrafi od $Aut(\Gamma)$. Če je $\gamma \in Aut(\Gamma)^{(2)}$, potem je $\gamma \in Aut(\Gamma_i), 1 \leq i \leq r$, ker je $Aut(\Gamma)^{(2)} = \cap_{i=1}^{r} Aut(\Gamma_i)$. Po trditvi 3.39 je Γ posplošen orbitalni digraf od $Aut(\Gamma)$, z recimo, $\cup_{i=1}^{s} \Gamma_i = \Gamma$ za nek $1 \leq s \leq r$. Toda potem je $\gamma \in Aut(\Gamma)$, ker je $\gamma \in Aut(\Gamma_i), 1 \leq i \leq s$. □

Čeprav je $G^{(2)}$ grupa avtomorfizmov barvnega digrafa, ni nujno, da je grupa avtomorfizmov digrafa ali grafa.



Slika 14: Barvni Cayleyjev digraf $\mathbb{Z}_2 \times \mathbb{Z}_2$ z grupo avtomorfizmov $\mathbb{Z}_2 \times \mathbb{Z}_2$

Primer 3.43. Grupa $(\mathbb{Z}_2 \times \mathbb{Z}_2)_L$ je 2-zaprta, vendar ni grupa avtomorfizmov digrafa ali grafa.

Rešitev. Ker je vsak element $\mathbb{Z}_2 \times \mathbb{Z}_2$ sam svoj inverz, je vsak Cayleyjev digraf $\mathbb{Z}_2 \times \mathbb{Z}_2$ graf. Če preverimo, obstajajo štirje pari neizomorfnih Cayleyjevih grafov $\mathbb{Z}_2 \times \mathbb{Z}_2$, in sicer $K_4, \bar{K}_4$, je ujemanje in cikel dolžine 4. Prva dva grafa imata grupo avtomorfizmov S_4, medtem ko imata ostala dva grafa grupo avtomorfizmov $Z_2 \wr Z_2$.

Če želimo videti, da je $(\mathbb{Z}_2 \times \mathbb{Z}_2)_L$ 2-zaprt, upoštevajmo barvni digraf Γ, ki je podan na sliki 14. Barvni digraf Γ je unija treh orbitalnih digrafov $(\mathbb{Z}_2 \times \mathbb{Z}_2)_L$, pri čemer je vsak orbitalni digraf $((\mathbb{Z}_2 \times \mathbb{Z}_2)_L$ obarvan z drugo barvo na sliki 14. Zato je $(\mathbb{Z}_2 \times \mathbb{Z}_2)_L \leq Aut(\Gamma)$. Razmislimo o orbitalnem digrafu Γ_1 od $(\mathbb{Z}_2 \times \mathbb{Z}_2)_L$, podanem v zeleni barvi na sliki 14. Transpozicija $\gamma = ((1,0),(1,1)) \in Aut(\Gamma_1)$ s pregledom, vendar $\gamma \notin Aut(\Gamma_2)$, kjer je Γ_2 orbitalni digraf $(\mathbb{Z}_2 \times \mathbb{Z}_2)_L$, podan z rdečo barvo na sliki 14. Ker je $Aut(\Gamma_1) \cong \mathbb{Z}_2 \wr \mathbb{Z}_2 \cong \langle (\mathbb{Z}_2 \times \mathbb{Z}_2)_L, \gamma \rangle$ je reda 8, vidimo da $Aut(\Gamma_1) \cap Aut(\Gamma_2) = (\mathbb{Z}_2 \times \mathbb{Z}_2)_L$. Zato je $Aut(\Gamma) = (\mathbb{Z}_2 \times \mathbb{Z}_2)_L$ 2-zaprt. □

4 NORMALNI CAYELYJEVI (DI)GRAFI

Spomnimo se, če je $\Gamma = Cay(G, S)$ digraf in $Aut(\Gamma) = G_L$, potem je Γ **usmerjena regularna predstavitev** ali **DRR** od G, če pa je Γ graf in $Aut(\Gamma) = G_L$, potem je Γ **grafična regularna predstavitev** G ali **GRR**.

Definicija 4.1. Cayleyjev digraf $Cay(G, S)$ G je **normalen Cayleyjev digraf** G, če je $G_L \trianglelefteq Aut(Cay(G, S))$.

Jasno je, da je vsak GRR ali DRR za G normalen Cayleyjev graf ali digraf.

Definicija 4.2. Naj bo G grupa. Dva Cayleyjeva (di)grafa $Cay(G, S)$ in $Cay(G, T)$ od G imenujemo **Cayleyjeva izomorfna**, če je $\sigma(S) = T$ za nek $\sigma \in Aut(G)$. Lahko vidimo, da so Cayleyjevi izomorfni Cayleyjevi (di)grafi izomorfni kot (di)grafi.

Vendar pa obratno ne drži in obstajajo izomorfni Cayleyjevi (di)grafi, ki niso Cayleyjevi izomorfni.

Definicija 4.3. Cayleyjeva podmnožica S od G se imenuje **CI-podmnožica**, če za katerikoli $T \subseteq G$,$Cay(G, S) \cong Cay(G, T)$ pomeni, da so Cayleyjevi izomorfni, to je $T = \sigma(S)$ za nek $\sigma \in Aut(G)$ in v tem primeru imenujemo $Cay(G, S)$ **CI-graf**, kjer CI predstavlja Cayleyjev izomorfni.

Definicija 4.4. Pravimo, da je grupa G **DCI-grupa** ali **CI-grupa**, če so vsi Cayleyjevi digrafi ali grafi grupe G CI-grafi.

Primer 4.5. Polni graf K_n je normalen Cayleyjev graf grupe G če in samo če je $n = 2, 3$ ali 4 in $G = \mathbb{Z}_2, \mathbb{Z}_3$ ali $\mathbb{Z}_2^2$.

Rešitev. Seveda je, $Aut(K_n) = S_n$. Če je $n \geq 5$, potem je A_n preprost [[9], Izrek 4.6.24], zato je edina pravilna netrivialna normalna podgrupa S_n A_n. Ker A_n ni pravilen, K_n ni normalen Cayleyjev graf katere koli grupe in ker $Aut(K_n) = Aut(\overline{K}_n)$ tudi ni njegov komplement. Če je $n = 4$, je $|AGL(2, 2)| = 4(4 - 1)(4 - 2) = |S_4|$ in $AGL(2, 2) = S_4$. Potem je K_4 normalen Cayleyjev graf za $\mathbb{Z}_2$, ne pa tudi za $\mathbb{Z}_4$, saj je $Aut(\mathbb{Z}_4)$ reda 2. Končno, če je $n = 3$, potem ima A_3 normalno podgrupo reda 3 in K_3 je normalen, medtem ko je $Aut(K_2) = \mathbb{Z}_2$ regularen. Tako sta K_2 in K_3 normalna Cayleyjeva grafa $\mathbb{Z}_2$ oziroma $\mathbb{Z}_3$. □

Izrek 4.6. *Vsak circulantski digraf reda praštevil $p \geq 5$ z izjemo K_p in njegovega komplementa je normalen Cayleyjev digraf $\mathbb{Z}_p$.*

Primer 4.7. Heawoodov graf ni normalen Cayleyev digraf diedrske grupe reda 14.

Rešitev. Po [[8] Vaja 4.5.2] je Heawoodov graf Cayleyjev graf D_{14}, po [[8] Posledica 4.5.8] pa ima grupo avtorfizmov $G = PGL(3,2) \rtimes \mathbb{Z}_2$. Prav tako ima G blokovni sistem $\mathcal{B}$ z bloki velikosti 7 s $fix_G(\mathcal{B}) \cong PGL(3,2)$. Inducirano delovanje $PGL(3,2)$ na $B \in \mathcal{B}$ je 2-tranzitivna neabelova skoraj enostavna grupa, zato po izreku 3.37 nima normalne podgupe 7-Sylowke. Tako G nima normalne podgrupe Sylowke. Vendar je značilna podgrupa 7-Sylowke P iz D_{14}, zato je $P \trianglelefteq (D_{14})_L \rtimes Aut(D_{14}) = N_{S_{14}}((D_{14})_L)$ po posledici 3.34. □

Naslednji rezultat je značilen za normalne Cayleyjeve digrafe.

Izrek 4.8. *Naj bo G grupa, $S \subset G$, in $\Gamma = Cay(G,S)$. Naslednje trditve so ekvivalentne:*

(i) Γ *je normalen Cayleyjev digraf* G,

(ii) $Stab_{Aut(\Gamma)}(1_G) \leq Aut(G)$,

(iii) $Stab_{Aut(\Gamma)}(1_G) = Aut(G,S)$ *in*

(iv) $Aut(\Gamma) = G_L \rtimes Aut(G,S)$.

Dokaz. Upoštevajmo, da je $G_L \trianglelefteq Aut(\Gamma)$, če in samo če je $Aut(\Gamma) \leq N_{S_G}(G_L) = G_L \rtimes Aut(G)$ po posledici 3.34. Ker je G_L regularen, se to zgodi če in samo če je $Stab_{Aut(\Gamma)}(1_G) \leq Aut(G)$. Zadnja trditev velja če in samo če $Stab_{Aut(\Gamma)}(1_G) = Aut(G,S)$, kar je res če in samo če $Aut(\Gamma) = G_L \rtimes Aut(G,S)$. □

Torej, če je $Cay(G,S)$ normalni Cayleyjev digraf G, potem je $Aut(Cay(G,S)) = \{g_L\alpha : \alpha \in Aut(G,S), g \in G\}$.

Izrek 4.9. *[18]Naj bo G končna grupa. Potem ima G normalen Cayleyjev graf, razen če je $G \cong \mathbb{Z}_2 \times \mathbb{Z}_4$ ali $G \cong Q_8 \times \mathbb{Z}_2^r, r \geq 0$. Poleg tega ima vsaka končna grupa G normalen Cayleyjev digraf.*

4.1 NORMALNI CAYELYJEVI DIGRAFI ABELOVIH GRUP

V tem poglavju je predstavljen rezultat, ki pove zadostne pogoje, da je povezan Cayleyjev digraf abelove grupe normalen, ter se nato ta rezultat uporabi za določitev vseh povezanih grafov abelovih grup valence največ 4 ki niso normalni.

Lema 4.10. *Naj bo $\Gamma = Cay(A, S)$ povezan Cayleyjev digraf abelove grupe A. Recimo, da S izpolnjuje pogoj, da če je $x, y, z, u \in S$ z $1 \neq xy = zu$, potem $\{x, y\} = \{z, u\}$. Potem je $Cay(A, S)$ normalen Cayleyjev digraf A.*

Dokaz. Naj bo $\phi \in Stab_{Aut(\Gamma)}(1_A)$. Ko je Γ povezan z lemo 3.13, je $\langle S \rangle = A$. Zadostuje, da pokažemo, da je $\phi(s_1 \cdots s_r) = \phi(s_1)\phi(s_2) \cdots \phi(s_r)$ za kateri koli končni zmnožek elementov $s_1, \ldots, s_r$ v S. To pokažemo z indukcijo na r. Če je $r = 1$, je to trivialno, torej predvidevamo, da rezultat drži za $r \geq 1$, in naj bo $s_1, \ldots, s_{r+1} \in S$, tako da je $r + 1 \geq 2$. Nastavimo $w = s_1 \cdots s_{r-1}$ in opazimo, da je $\phi(S) = S$.

Denimo, da sta $s_r s_{r+1} \neq 1$ in $s_r \neq s_{r+1}$. Potem je $C = w, ws_r, ws_r s_{r+1}, ws_{r+1}, w$ 4-cikel v Γ, saj je A abelov. Recimo, da je $w, y, ws_r s_{r+1}, z, w$ 4-cikel v Γ.
Potem $w^{-1}y, y^{-1}ws_r s_{r+1} \in S$ in $w^{-1}yy^{-1}ws_r s_{r+1} = s_r s_{r+1} \neq 1$, in tako po hipotezi $\{w^{-1}y, y^{-1}ws_r s_{r+1}\} = \{s_r, s_{r+1}\}$. Sklepamo, da v Γ obstaja enolično določen 4-cikel, ki vsebuje w in $ws_r s_{r+1}$. Če je w, ws_r, x, ws_{r+1}, w 4-cikel v Γ, potem obstaja $t_1, t_2 \in S$ z $x = ws_r t_1 = ws_{r+1}t_2$. Zato je $w^{-1}x = s_r t_1 = s_{r+1}t_2$. Opomba $w^{-1}x \neq 1$, sicer je $w = x$ in w, ws_r, x, ws_{r+1}, w ni 4-ciklični. Torej po hipotezi $\{s_r, t_1\} = \{s_{r+1}, t_2\}$. Kot $s_r \neq s_{r+1}$ je $t_1 = s_{r+1}$ in $x = ws_r s_{r+1}$. Zato Γ vsebuje tudi enolično določen 4-cikel, ki vsebuje w, ws_r in ws_{r+1}.

Sedaj nastavimo $w = s_1 \cdots s_{r-1}$ if $r + 1 \geq 3$ in $w = 1$ if $r + 1 = 2$ in upoštevajmo

$$\phi(C) = \phi(w), \phi(ws_r), \phi(ws_r s_{r+1}), \phi(ws_{r+1}), \phi(w).$$

Z indukcijsko hipotezo in izbiro w imamo $\phi(ws_r) = \phi(w)\phi(s_r)$ in $\phi(ws_{r+1}) = \phi(w)\phi(s_{r+1})$. Potem

$$\phi(C) = \phi(w), \phi(w)\phi(s_r), \phi(ws_r s_{r+1}), \phi(w)\phi(s_{r+1}), \phi(w)$$

in tako $\phi(s_r), \phi(s_{r+1}) \in S$. Kot enolično določen 4-cikel v Γ^u, ki vsebuje $\phi(w), \phi(w)\phi(s_r)$ in $\phi(w)\phi(s_{r+1})$ je,

$$\phi(w), \phi(w)\phi(s_r), \phi(w)\phi(s_r)\phi(s_{r+1}), \phi(w)\phi(s_{r+1}), \phi(w)$$

vidimo $\phi(ws_r s_{r+1}) = \phi(w)\phi(s_r)\phi(s_{r+1})$. Z indukcijo je $\phi(w) = \phi(s_1) \cdots \phi(s_{r-1})$ in tako $\phi(s_1 \cdots s_{r+1}) = \phi(s_1) \cdots \phi(s_{r+1})$, kot je zahtevano.

Zdaj predpostavimo $s_r s_{r+1} \neq 1$, vendar $s_r = s_{r+1}$. Ker $s_r s_{r+1} \neq 1$ sprehod w, ws_r, ws_r^2 je pot P v Γ. Recimo, da je P vsebovan v 4-ciklu C v Γ. Potem obstaja $x \in A$ tako da $C = P, x, w$ in torej obstaja $t_1, t_2 \in S$ z $x = wt_1 = ws_r^2 t_2$. Ekvivalentno je $s_r^{-1}t_1 = s_r t_2$. If $s_t^{-1} = s_r t_2 = 1$, potem $t_1 = s_r$ in $t_2 = s_r^{-1}$. Ampak potem $x = ws_r$ in C ni 4-cikel. Torej $s_r^{-1}t_1 = s_r t_2 \neq 1$. Po hipotezi $\{s_r^{-1}, t_1\} = \{s_r, t_2\}$ in ker $s_r \neq s_r^{-1}$ (ker $s_r s_{r+1} \neq 1$) sledi: $t_2 = s_r^{-1}$ in $x = ws_r$. Ampak potem C ni 4-cikel, to je protislovje. V kombinaciji z argumenti v prejšnjem odstavku vidimo, da pot P dolžine 2 ni vsebovana v 4-ciklu, če in samo če, je $P = w, ws_r, ws_r^2$ za nekaj $s_r \in S$. Zdaj nastavimo

$w = s_1 \cdots s_{r-1}$. Potem je $\phi(P) = \phi(w), \phi(ws_r), \phi(ws_r^2) = \phi(w), \phi(w)\phi(s_r), \phi(ws_r^2)$ pot dolžine 2, ki ni v 4-ciklu. Sklepamo, da je $\phi(ws_r^2) = \phi(w)\phi(s_r)\phi(s_r)$ in tako $\phi(s_1 \cdots s_{r+1}) = \phi(s_1) \cdots \phi(s_{r+1})$, kot je zahtevano.

Končno, predpostavimo $s_r s_{r+1} = 1$. Potem $1, s_r, s_{r+1}$ je sprehod v Γ dolžine 2 od 1 do 1 in $\phi(1), \phi(s_r), \phi(s_{r+1})$ je tudi sprehod dolžine 2 od 1 do 1, ker $\phi(1) = 1$. Torej $\phi(s_r)\phi(s_{r+1}) = 1$. Zato je $\phi(s_r s_{r+1}) = \phi(1) = 1 = \phi(s_r)\phi(s_{r+1})$. Potem

$$\phi(s_1 \cdots s_{r+1}) = \phi(s_1 \cdots s_{r-1}) = \phi(s_1) \cdots \phi(s_{r-1}) = \phi(s_1) \cdots \phi(s_{r-1})\phi(s_r)\phi(s_{r+1})$$

in rezultat sledi z indukcijo. □

Primer 4.11. N-dimenzionalna hiperkocka Q_n je normalni Cayleyjev graf $\mathbb{Z}_2^n$.

Rešitev. Q_n je izomorfna za $Cay(\mathbb{Z}_2^n, S)$, kjer je S množica n vektorjev, ki so 0 v vseh koordinatah, razen v eni. Naj bo $x, y, z, u \in S$ z $(0, \ldots, 0) \neq x + y = z + u$. Potem $x + y$ ni nič v natančno dveh koordinatah, recimo i-ti in j-ti. Tudi x in y ter z in u sta 0 v vsaki koordinati, razen bodisi i-ti in j-ti bodisi j-ti in i-ti. Zato je $\{x, y\} = \{u, z\}$ in Q_n normalen Cayleyjev graf $\mathbb{Z}_2^n$ po lemi 4.10. □

Izrek 4.12. *Naj bo Γ povezan Cayleyjev graf abelove grupe A, ki ima valenco največ 3. Potem je Γ normalen Cayleyjev graf A razen, če velja eno od naslednjega:*

(i) $\Gamma = K_4$ *ali* K_5 *in* $A = \mathbb{Z}_4$ *oziroma* $\mathbb{Z}_5$,

(ii) $\Gamma = Q_3$ *in* $A = \mathbb{Z}_2 \times \mathbb{Z}_4$,

(iii) $\Gamma = K_{3,3}$ *in* $A = \mathbb{Z}_6$,

Dokaz. Če ima Γ valenco 1 potem je $\Gamma = K_2$, ki je GRR. Če Γ ima valenco 2, potem je Γ cikel, katerega grupa avtomorfizmov je diedrska grupa. Potem je Γ normalni Cayleyjev graf ciklične grupe, diedrska grupa pa ne vsebuje drugih tranzitivnih abelovih podgrup. Tako domnevamo, da ima Γ valenco 3.

Predpostavimo najprej, da so vsi elementi S involucije G. Potem je $A = \mathbb{Z}_n^2$ za nekaj $n \geq 3$. Če je S minimalna generirana množica $\mathbb{Z}_n^2$, potem gledamo vsak element S kot vektor v $\mathbb{Z}_n^2$, vidimo, da je S linearno neodvisen in osnova za $\mathbb{Z}_n^2$. Ker je Γ kubična, je $n = 3$. Potem obstaja $A \in Aut(\mathbb{Z}_n^2) = GL(n, 2)$, tako da je $A(S)$ kanonična osnova za $\mathbb{Z}_n^2$, in tako je $A(\Gamma)$ n-kocka. V primeru 4.11 je Γ normalen Cayleyjev graf $\mathbb{Z}_2^3$. Če torej S vsebuje samo involucije, je S linearno odvisen in je tako $n = 2$ kot $|S| = 3$. Torej $\Gamma = K_4$, kar je v primeru 4.5 normalen Cayleyjev graf $\mathbb{Z}_2$ in rezultat sledi.

Edina druga možnost je, da je $S = \{a, a^{-1}, s\}$, kjer je s involucija, a pa ne. S preučevanjem vseh možnih izbir dveh elementov $S^2 \backslash \{1\} = \{a^2, as, a^{-2}, a^{-1}s\}$, je edini

način, na katerega sta lahko dva elementa $S^2\backslash\{1\}$ enaka, če $s = a \pm 3$ ali $a^2 = a^{-2}$. V nasprotnem primeru imamo po izreku 4.10 Γ normalen Cayleyjev graf A. Če je $s = a^{\pm 3}$, potem je s s involucija $|a| = 6$ in $A = \mathbb{Z}_6$. Potem $\Gamma = Cay(\mathbb{Z}_6, \{1, 3, 5\}) \cong K_{3,3} \cong K_2 \wr \overline{K}_3$. As $N_{S_6}((\mathbb{Z}_6)_L)$ ima vrstni red 12 in $\mathbb{Z}_2 \wr S_3$ ima vrstni red 72, vidimo, da Γ ni normalen Cayleyjev graf $\mathbb{Z}_6$ in (iii) sledi. Če $a^2 = a^{-2}$, potem $|a| = 4$. Če je $\langle a \rangle$, potem $A = \mathbb{Z}_4$ in $\Gamma = K_4$. Ker ima $N_{S_4}((\mathbb{Z}_4)_L)$ red 8, Γ ni normalen Cayleyjev graf $\mathbb{Z}_4$ in (i) sledi. Če je $s \neq \langle a \rangle$, potem je $A \cong \mathbb{Z}_2 \times \mathbb{Z}_4, S = \{(0, 1), (0, 3), (1, 0)\}$ in $\Gamma \cong Q_3$. Potem $S_2 \times S_4 \leq Aut(\Gamma)$ in $S_2 \times S_4$ ne normalizira $(\mathbb{Z}_2 \times \mathbb{Z}_4)_L$. Potem sledi Γ ni normalen Cayleyjev graf $\mathbb{Z}_2 \times \mathbb{Z}_4$ in smo dokazali (ii). □

Dokaz za valenco 4 je podoben, vendar z več primeri. Večina primerov se obravnava z uporabo leme 4.10, le da obstaja več družin Cayleyjevih grafov abelovih grup, ki jih je treba neposredno prikazati kot normalne. Za ostale podrobnosti glej [2]. Podobno so Baik, Feng in Sim [1] določili vse nenormalne Cayleyjeve grafe abelovih grup valenc 5.

Izrek 4.13. *[2] Naj bo $X = Cay(G, S)$ povezan neusmerjen Cayleyjev graf abelove grupe G na S z valenco X največ 4. Potem je X normalen, razen v enem od naslednjih primerov :*

(i) $G = Z_2^3 = \langle u \rangle \times \langle v \rangle \times \langle w \rangle$, $S = \{w, wu, wv, wuv\}$ *in* $X = K_{4,4}$.

(ii) $G = Z_4 \times Z_2 = \langle a \rangle \times \langle b \rangle$, $S = \{a, a^2, a^3, b\}$ *in* $X = Q_3^c$ *(komplement kocke).*

(iii) $G = Z_4 \times Z_2 = \langle a \rangle \times \langle b \rangle$, $S = \{a, a^{-1}, a^2b, b\}$ *in* $X = K_{4,4}$.

(iv) $G = Z_4 \times Z_2^2 = \langle a \rangle \times \langle b \rangle \times \langle c \rangle$, $S = \{a, a^{-1}, b, c\}$ *in* $X = Q_4$ *(4-dimenzionalna kocka).*

(v) $G = Z_6 \times Z_2 = \langle a \rangle \times \langle b \rangle$, $S = \{a, a^{-1}, a^3, b\}$ *in* $X = K_{3,3} \times K_2$.

(vi) $G = Z_4 \times Z_4 = \langle a \rangle \times \langle b \rangle$, $S = \{a, a^{-1}, b, b^{-1}\}$ *in* $X = C_4 \times C_4$.

(vii) $G = Z_m \times Z_2 = \langle a \rangle \times \langle b \rangle$ *z* $m \geq 3$, $S = \{a, ab, a^{-1}, a^{-1}b\}$ *in* $X = C_m[2K_1]$.

(viii) $G = Z_{4m} = \langle a \rangle$ *z* $m \geq 2$, $S = \{a, a^{2m+1}, a^{-1}, a^{2m-1}b\}$ *in* $X = C_{2m}[2K_1]$.

(ix) $G = Z_5, S = G \setminus \{1\}$ *in* $X = K_5$.

(x) $G = Z_{10} = \langle a \rangle$, $S = \{a, a^3, a^7, a^9\}$ *in* $X = K_{5,5} - 5K_2$.

Takoj imamo naslednjo posledico.

Posledica 4.14.

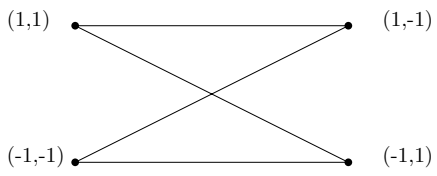
(i) Vsi povezani Cayleyjevi grafi z valenco največ 4, končne abelove grupe lihega reda so normalni razen za $G = Z_5$ *in* $X = K_5$.

(ii) Vsi povezani Cayleyjevi grafi z valenco največ 4, končne ciklične grupe so normalni razen za $G = Z_4$ *in* $X = K_4$ *ali* $G = Z_6$ *in* $X = K_{3,3}$ *ali* $G = Z_5$ *in* $X = K_5$ *ali* $G = Z_{2m}$ *in* $X = C_m[2K_1](m \geq 3)$ *ali* $G = Z_{10}$ *in* $X = K_2[5K_1] - 5K_2$.

Enoličen primer nenormalnega povezanega Caylejevega grafa z valenco 4 končne abelove grupe lihega reda je primer, ko $G = Z_5$ in $X = K_5$. Feng in Dong [24] sta dokazala analogno za grupe reda p^3 (p liho praštevilo). Vendar na splošno to ne drži za grupe lihega reda. V resnici sta Feng in Xu [23] podala nenormalen povezan Cayleyjev graf reda 81 in valence 4.

V primeru 2.92 podajamo primer Cayleyjevega grafa Γ grupe G, ki je normalen Cayleyjev graf grupe G, za katerega obstaja regularna podgrupa avtomorfizmov H, neizomorfna z G, in ki ni podgrupa edinka grupe avtomorfizmov od Γ. Dejansko obstajajo izomorfne regularne grupe G in H, za katere obstaja graf Γ, katerega grupa avtomorfizmov vsebuje tako G kot H z G normalno v $Aut(\Gamma)$, H pa ni normalno v $Aut(\Gamma)$. Povedano drugače, Γ je izomorfno za Cayleyjeve grafe Γ_1 in Γ_2 od G in H in Γ_1 je normalen Cayleyjev graf G, medtem ko Γ_2 ni normalen Cayleyjev graf H. Prvi primer tega pojava sta našla Giudici in Smith leta [10] za grupo $\mathbb{Z}_6^2$, medtem ko je Royle našel drugega za grupo $\mathbb{Z}_2^6$ že leta 2008 [16]. Prvo neskončno družino sta našla Bamberg in Giudici [3]. Za dodatne konstrukcije glej [21].

Zdaj bomo predstavili en primer grafa, ki je istočasno normalen in nenormalen Cayleyev graf za isto grupo $\mathbb{Z}_2^6$. Ta graf je skonstruiral Gordon Royle v [16]. Najprej bomo definirali Hadamardov graf $H(n)$. Za celo število n, naj bo Hadamardov graf $H(n)$, graf katerega vozlišča so vsi vektorji dolžine n, z vrednostimi 1 ali -1 (z drugimi besedami, množica vozlišč grafa $H(n)$ je $\{-1, 1\}^n$), dva različna vektorja $x = (x_1, \ldots, x_n)$ in $y = (y_1, \ldots, y_n)$ sta povezani natanko takrat, ko sta ortogonalni, oz je $x \cdot y = x_1y_1 + \ldots + x_ny_n = 0$. Na sliki 15 je prikazan Hadamardov graf $H(2)$.



Slika 15: Hadamardov graf $H(2)$.

Se bomo osredotočili na Hadamardov graf $H(8)$. Opazimo, da graf $H(8)$ ima 256 vozlišč oblike $(x_1, \ldots, x_8)$ kjer so $x_i \in \{-1, 1\}$. Opazimo, da graf $H(8)$ ima dve povezani

komponenti, namreč vsi vektorji s sodim številom znakov -1 pripadejo eni komponenti ter vsi vektorji z lihim številom znakov -1 pripadejo drugi komponenti povezanosti. Opazimo tudi, da je $x \cdot y = 0$ ekvivalentno z $x \cdot (-y) = (-x) \cdot y = (-x) \cdot (-y) = 0$. To pomeni, da vozlišče $x = (x_1, \ldots, x_8)$ ima enako množico sosedov kot vozlišče $-x = (-x_1, \ldots, -x_8)$. Iz tega sledi, da je vsaka povezana komponenta grafa $H(8)$ izomorfna leksikografskemu produktu $X[2K_1]$, kjer je X povezan graf na 64 vozlišč. Royle je dokazal naslednje lastnosti grafa X.

Izrek 4.15. *Naj bo X graf definiran kot zgoraj. Potem je X $(64, 35, 18, 20)$-krepko-regularen graf, $Aut(X) \cong \mathbb{Z}_2^6 \rtimes S_8$ ter premore dve regularni podgrupi izomorfni $\mathbb{Z}_2^6$, ena izmed teh je edinka, druga ni edinka v $Aut(X)$. Posledično je X normalen Cayleyjev graf za grupo $\mathbb{Z}_2^6$ ter X istočasno ni normalen Cayleyjev graf za grupo $\mathbb{Z}_2^6$.*

Opazimo, da graf X lahko definiramo na naslednji način.
Naj bo $G = \langle e_1, e_2, e_3, e_4, e_5, e_6 \rangle \cong \mathbb{Z}_2^6$, ter naj bo $S = \{e_i e_j e_k \mid 1 \leq i < j < k \leq 6\} \cup \{e_i e_j e_k e_l \mid 1 \leq i < j < k < l \leq 6\}$. Potem je $X = Cay(G, S)$, ter je X normalen Cayleyjev graf. Lahko pa definiramo isti graf s pomočjo množice $S_2 \subset \mathbb{Z}_2^6$

$$\begin{aligned} S_2 := \{&(0,0,0,1,0,0), (0,1,1,0,0,0), (1,0,1,0,1,0), (0,1,1,1,1,1), (0,1,1,0,1,1),\\ &(1,0,1,0,1,1), (1,1,1,0,1,1), (1,0,0,0,1,1), (0,0,1,1,0,1), (1,0,1,1,0,0),\\ &(0,0,0,0,1,1), (0,0,0,0,0,1), (0,1,0,1,1,0), (0,0,0,0,1,0), (1,0,0,0,0,0),\\ &(1,0,0,1,0,1), (1,1,0,0,1,0), (0,0,0,1,1,1), (0,0,0,1,0,1), (0,1,0,0,1,0),\\ &(1,1,0,1,1,1), (1,1,1,0,1,0), (0,0,1,0,0,1), (0,0,1,1,1,1), (1,0,1,1,0,1),\\ &(0,0,0,1,1,0), (0,1,1,1,0,0), (1,0,0,1,1,0), (1,1,0,1,0,1), (0,1,0,0,1,1),\\ &(1,1,0,0,0,0), (1,1,1,0,0,0), (0,1,0,1,1,1), (1,1,1,0,0,1), (0,0,1,0,1,1)\}. \end{aligned}$$

Potem je $X \cong Cay(\mathbb{Z}_2^6, S_2)$, pri čemer $Cay(\mathbb{Z}_2^6, S_2)$ ni normalen Cayleyjev graf.

5 LOČNO TRANZITIVNI CIRKUALNTI

Cirkulant je Cayleyjev digraf nad končno ciklično grupo. V nadaljevanju je prikazana klasifikacija ločno tranzitivnih cirkulantov. Ta rezultat dokaže, da so ločno tranzitivni cirkulanti bodisi normalni ali pa pripradejo družini grafov, ki jih dobimo z leksikografskimi produkti [12].

Naj bo G končna grupa z nevtralnim elementom 1. Za dano množico $S \subseteq G\backslash\{1\}$ definirajmo usmerjen graf

$$V(\Gamma) := G,\ E(\Gamma) := \{(g, gs) \in G \times G \mid g \in G, s \in S\}.$$

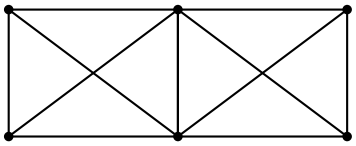
V primeru, ko je S simetričen, tj. $S = S^{-1} = \{g^{-1} \mid g \in S\}$ z Γ, mislimo na neusmerjen graf. Γ imenujemo Cayleyjev digraf nad G in ga bomo označili s $Cay(G, S)$. S naj bo množica povezav v Γ. Iz definicije sledi, da leva regularna predstavitev G inducira regularno podgrupo $Aut(\Gamma)$. To podgrupo označimo kot G_L. Cirkulant reda n je Cayleyjev digraf nad ciklično grupo reda n.

Naj H označuje ciklično grupo reda n in $\Gamma = Cay(H, S)$. V tem delu obravnavamo ločno tranzitivne cirkulante, tj. za katere $Aut(\Gamma)$ deluje tranzitivno na množici svojih lokov. Če Γ ni povezan, je zlahka razvidno, da je vsaka komponenta povezanosti izomorfna istemu ločno tranzitivnemu cirkulantu reda m, kjer je m deljitelj od n. Zaradi tega zadostuje, da med ločno tranzitivnimi cirkulanti upoštevamo povezane.

V tem delu klasificiramo vse povezane ločno tranzitivne cirkulante.

Preden navedemo naše glavne rezultate, je treba navesti nekaj pojmov.

Definicija 5.1. Za (di)grafe Γ in Σ označimo z $\Gamma[\Sigma]$ **leksikografski produkt** z Σ, tj. (di)graf z množico vozlišč $V(\Gamma) \times V(\Sigma)$; in za $u_1, u_2 \in V(\Gamma)$ in $v_1, v_2 \in V(\Sigma)$ je par $((u_1, u_2), (v_1, v_2))$ lok, če in samo če $(u_1, u_2) \in E(\Gamma)$ ali $u_1 = u_2$ in $(v_1, v_2) \in E(\Sigma)$.



Slika 16: Leksikografski produkt $P_3[K_2]$

Če je $V(\Gamma) = V(\Sigma)$, potem označimo z $\Gamma - \Sigma$ (di)graf z množico vozlišč $V(\Gamma)$ in množico lokov $E(\Gamma)\backslash E(\Sigma)$. Poleg tega naj bo $\bar{\Gamma}$ uporabljen za komplement Γ, $m\Gamma$ naj označi (di)graf, sestavljen iz m nepovezanih kopij Γ. K_n naj bo poln graf z n vozlišči.

Definicija 5.2. Cirkulant, definiran nad ciklično grupo H, se imenuje normalen, če je H_L podgrupa edinka v $Aut(\Gamma)$.

Izrek 5.3. *Naj bo Γ povezan ločno tranzitivni cirkulantni digraf reda n. Potem velja ena od naslednjih:*

- $\Gamma = K_n$*;*
- Γ *je normalen cirkulantni digraf;*
- $\Gamma = \Sigma[\bar{K}_d]$*, kjer je $n = md$ in Σ je povezan ločno tranzitivni cirkulantni digraf reda m;*
- $\Gamma = \Sigma[\bar{K}_d] - d\Sigma$*, kjer je $n = md$, $d > 3, gcd(d, m) = 1$ in Σ je povezan ločno tranzitivni cirkulantni digraf reda m.*

Iskanje normalnega cirkulanta, ki bi bil hkrati tudi nenormalen cirkulant, je odprto vprašanje. Vendarle, v nekaterih primerih je znano, da se to ne more zgoditi. Tako imamo naslednji izrek.

Izrek 5.4. *Naj bo n celo število, ki ni deljivo z 8. Naj bo $\Gamma = Cay(\mathbb{Z}_n, S)$ normalen Cayleyjev graf. Potem $Aut(\Gamma)$ ne premore ciklično regularno podgrupo, ki ni edinka.*

6 ZAKLJUČEK

V magistrskem delu smo si natančneje pogledali normalne Cayleyjeve digrafe. Caylejev digraf je vozliščno tranzitiven digraf.

V tretjem poglavju so predstavljeni Cayleyjevi (di)grafi, pogledali smo si razliko med Cayleyjevimi grafi in Cayleyjevimi digrafi. Digraf $Cay(G, S)$ je graf, če in samo če je $S = S^{-1}$. Dokazali smo tudi izrek, da Petersenov graf ni Cayleyjev graf.

Osrednja tema magistrskega dela je četrto poglavje, in sicer normalni Cayleyjevi (di)grafi. Pokazali smo primere grafov, ki so normalni Cayleyjevi (di)grafi in tudi tiste, ki niso normalni. Naslednje podpoglavje je normalni Cayleyjevi digrafi abelovih grup, kjer smo podali potrebne in zadostne pogoje za normalnost Cayleyjevih digrafov na abelovih grupah. S pomočjo tega rezultata smo določili vse nenormalne Cayleyjeve grafe na abelovih grupah valence največ 4. Na koncu poglavja smo tudi predstavili primer grafa, ki je hkrati normalen in nenormalen Cayleyjev graf za isto grupo $\mathbb{Z}_2^6$.

V zadnjem poglavju je prikazana klasifikacija ločno tranzitivnih cirkulantov. Ta rezultat dokaže, da so ločno tranzitivni cirkulanti bodisi normalni bodisi pripadajo družini grafov, ki jih dobimo z leksikografskimi produkti. Iskanje normalnega cirkulanta, ki bi bil istočasno tudi nenormalen, je odprto vprašanje, vendar je znano, da se to ne more zgoditi, ko število točk ni deljivo z 8.

7 LITERATURA IN VIRI

[1] Baik, Y. G., FENG, Y. Q. in Sim, H.-S. *The Normality of Cayley graphs of finite abelian groups with valency 5*, vol. 13. Journal of Systems Science and Complexity, 2000, pp. 425 – 431.

[2] Baik, Y. G., Feng, Y.-Q., Sim, H.-S. in Xu, M. *On the Normality of Cayley Graphs of Abelian Groups.* Algebra Colloquium, 1998, p. 297–304.

[3] Bamberg, J. in Giudici, M. *Point regular groups of automorphisms of generalised quadrangles*, vol. 118. Journal of Combinatorial Theory, Series A, 2011, pp. 1114–1128.

[4] Biggs, N. *Algebraic Graph Theory*, 2 ed. Cambridge Mathematical Library. Cambridge University Press, 1993.

[5] Bollobás, B. in Bollobas, B. *Modern graph theory*, vol. 184. Springer Science & Business Media, 1998.

[6] Carrell, J. *Groups, Matrices, and Vector Spaces: A Group Theoretic Approach to Linear Algebra.* Springer New York, 2017.

[7] Coxeter, H. S. M. in Moser, W. O. J. *Generators and Relations for Discrete Groups, Second Edition*, vol. 7. Society for Industrial and Applied Mathematics, USA, oct 1965, p. 588.

[8] Dobson, T., Malnič, A. in Marušič, D. *Symmetry in Graphs.* Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2022.

[9] Dummit, D. S. in Foote, R. M. *Abstract algebra*, 3rd ed ed. Wiley, New York, 2004.

[10] Giudici, M. in Smith, M. *A note on quotients of strongly regular graphs*, vol. 3. Ars Mathematica Contemporanea, 2010, pp. 147–150.

[11] Hujdurović, A. *Algebraic graph theory: drugo učno gradivo.* Fakulteta za matematiko, naravoslovje in informacijske tehnologije, 2018.

[12] Kovács, I. *Classifying Arc-Transitive Circulants*, vol. 20. Kluwer Academic Publishers, USA, nov 2004, p. 353–358.

[13] Kurzweil, H. in Stellmacher, B. *The Theory of Finite Groups.* Universitext, 2004.

[14] Miller, G. A. *A fundamental theorem with respect to transitive substitution groups*, vol. 9. American Mathematical Society, 1903, pp. 543 – 544.

[15] Mortimer, B. in Dixon, J. D. *Permutation Groups.* Springer Verlag, 1996.

[16] ROYLE, G. F. *A normal non-Cayley-invariant graph for the elementary abelian group of order 64*, vol. 85. Cambridge University Press, 2008, p. 347–351.

[17] Sabidussi, G. *On a Class of Fixed-Point-Free Graphs*, vol. 9. American Mathematical Society, 1958, pp. 800–804.

[18] Wang, C. Q., Wang, D. in Xu, M. *Normal Cayley graphs of finite groups*, vol. 41. Science in China Series A: Mathematics, 1998, pp. 242–251.

[19] West, D. B. *Introduction to Graph Theory.* Prentice Hall, 1996.

[20] Xu, M. Y. *Automorphism groups and isomorphisms of Cayley digraphs.* Graph theory (Lake Bled, 1995), 1998.

[21] Xu, Y. *On constructing normal and non-normal Cayley graphs*, vol. 340. Discrete Mathematics, 2017, pp. 2972–2977.

[22] Xu, Y. *Normal and non-normal cayley graphs.* PhD thesis, The University of Western Australia, 2018.

[23] Y.Q.Feng in M.Y.Xu. *The normality on a family of Cayley digraphs*, vol. 1. preprint, 1997, p. 1.

[24] Y.Q.Feng in Y.Z.Dong. *A note on Normal Cayley graphs of prime-cube order*, vol. 33. Graph Theory Notes of New York, 1997, pp. 20–23.