UNIVERZA NA PRIMORSKEM
Fakulteta za matematiko, naravoslovje in informacijske tehnologije

Matematika – 1. stopnja

Vida Maksimović

Hamiltonski cikli v kubičnih Cayleyjevih grafih alternirajoče grupe A_5

Zaključna projektna naloga

Mentor: doc. dr. Klavdija Kutnar

Koper, 2011

UNIVERSITY OF PRIMORSKA
Faculty of Mathematics, Natural Sciences and Information Technologies

Mathematics – 1^{st} degree

Vida Maksimović

Hamilton cycles in cubic Cayley graphs on the alternating group A_5

Final Project Paper

Mentor: doc. dr. Klavdija Kutnar

Koper, 2011

Zahvala

Največja zahvala za nastanek zaključne projektne naloge gre mentorici doc. dr. Klavdiji Kutnar, ker mi je vzbudila zanimanje za algebraično teorijo grafov, ter potrpežljivo popravljala in pomagala pri samem nastajanju le-te.

Zahvalila bi se staršem, mlajšemu bratu in fantu, ker so mi stali ob strani v času študija, me podpirali v najhujših trenutkih in verjeli vame.

Najlepša hvala Nastji in Mariji, ki sta si vzeli čas za naše ure učenja, pomoči pri razumevanju dokazov in njuni raznolikosti, ki me je vedno spravila v dobro voljo.

Nazadnje pa se zahvaljujem vsem sošolkam, ker so poskrbele, da sem z veseljem obiskovala ure predavanj in vaj in vsem ostali, ki ste kakorkoli pripomogli k nastanku zaključne projektne naloge.

Hvala vsem!

Povzetek

Graf, katerega grupa avtomorfizmov deluje tranzitivno na njegovih točkah, pravimo, da je točkovno tranzitiven. Raziskovalna motivacija za pričujočo projektno nalogo izhaja iz že vrsto let odprtega problema v algebraični teoriji grafov. Gre za Lovászov problem, ki govori o obstoju hamiltonskih poti in ciklov v povezanih točkovno tranzitivnih grafih. To so poti oziroma cikli, ki vsebujejo vse točke grafa.

Če grupa avtomorfizmov točkovno tranzitivnega grafa premore podgrupo G, ki deluje regularno na množici točk grafa, pravimo, da je graf Cayleyjev graf grupe G. V nalogi bomo dokazali obstoj hamiltonskih ciklov v kubičnih Cayleyjevih grafih alternirajoče grupe A_5.

Abstract

Every graph whose group of automorphism acts transitive on its vertices is called vertex-transitive graph. Motivation for this project work derives from an open problem which is present for many years in algebraic graph theory. This is Lovász's problem about the existence of Hamilton paths and cycles, that is, paths and cycles that contain all the vertices of a graph, in connected vertex-transitive graphs.

If the automorphism group of a vertex-transitive graph has a subgroup G acting regularly on the vertex set then the graph is called a Cayley graph on G. In this work we will prove the existence of Hamilton cycles in cubic Cayley graphs on the alternating group A_5.

Math. Subj. Class. (2010): 47H09, 15A04

Ključne besede: alternirajoča grupa, hamiltonski cikel, Cayleyjev graf

Keywords: alternating group, Hamilton cycle, Cayley graph

Kazalo

Uvod

Leta 1969 je Lovász [34] postavil vprašanje, ali ima vsak končen povezan točkovno tranzitiven graf hamiltonsko pot. Vsi znani povezani točkovno tranzitivni grafi imajo hamiltonsko pot. Še več, znani so le štirje povezani točkovno tranzitivni grafi (z vsaj tremi točkami), ki nimajo hamiltonskega cikla. To so: Petersenov graf (slika 1), Coxeterjev graf (slika 2) ter grafa dobljena s trisekcijo točk teh dveh grafov (slika 3)(trisekcija je postopek, pri katerem vsako točko grafa zamenjamo s trikotnikom). Z malo premisleka pridemo do sklepa, da Petersenov graf nima hamiltonskega cikla, ima pa hamiltonsko pot (slika 4). Dokaz, da Coxeterjev graf nima hamiltonskega cikla, si lahko bralec prebere v članku [15]. Hamiltonsko pot v Coxeterjevem grafu pa si lahko ogledamo na sliki 5. Premislimo še, zakaj grafa dobljena s trisekcijo Petersenovega in Coxeterjevega grafa nimata hamiltonskega cikla: trisekcija pomeni, da vsako točko grafa zamenjamo s trikotnikom. Ko v trisekciji danega grafa iščemo hamiltonski cikel, moremo v vsakem trikotniku (ki je nadomestil točko) izbrati natanko dve povezavi. Če v dani trisekciji grafa dobimo hamiltonski cikel, potem posledično hamiltonski cikel obstaja tudi v prvotnem grafu. To pa zato, ker če vsak trikotnik stisnemo v eno samo točko, spet dobimo prvoten graf. Petersenov graf in Coxeterjev graf ne premoreta hamiltonskega cikla, torej hamiltonskega cikla nimata niti njuni trisekciji. Z nadaljnjo trisekcijo seveda dobimo nove kubične grafe brez hamiltonskega cikla, a nas ti grafi ne zanimajo, saj niso več točkovno tranzitivni.

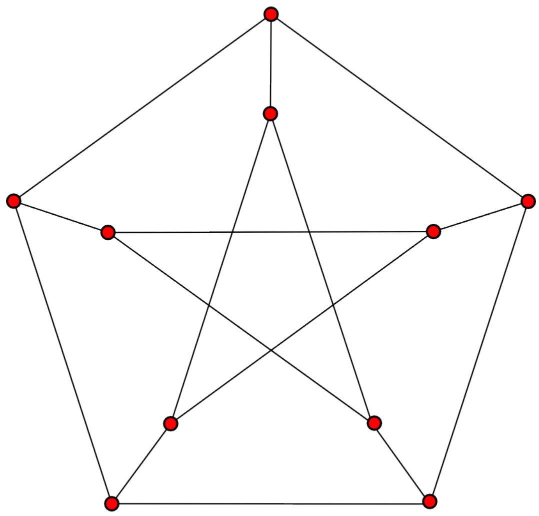
Cayleyjevi grafi so poseben primer točkovno tranzitivnih grafov [25]. Ker znani točkovno tranzitvni grafi brez hamiltonskega cikla (Petersenov, Coxeterjev in grafa dobljena s trisekcijo teh dveh) niso Cayleyjevi (glej primer 1.2.16), se je postavila domneva, da ima vsak povezan Cayleyjev graf na več kot dveh točkah hamiltonski cikel. Ta problem je spodbudil kar nekaj matematičnega zanimanja, postavile so se domneve in protidomneve glede njegove resničnosti. Tako je Thomassen [14], [42] domneval, da obstaja končno mnogo povezanih točkovno tranzitivnih grafov brez hamiltonskega cikla, Babai [11], [13], pa je postavil domnevo, da je takih grafov neskončno. Kljub temu, da so se v zadnjih 30 letih v literaturi pojavile številne publikacije, ki obravnavajo ta dva problema, a smo še vedno daleč od popolne rešitve (glej [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [17], [18], [20], [23], [26], [29],

[31], [33], [35], [36], [37], [38], [39], [40], [43], [44], [45]).

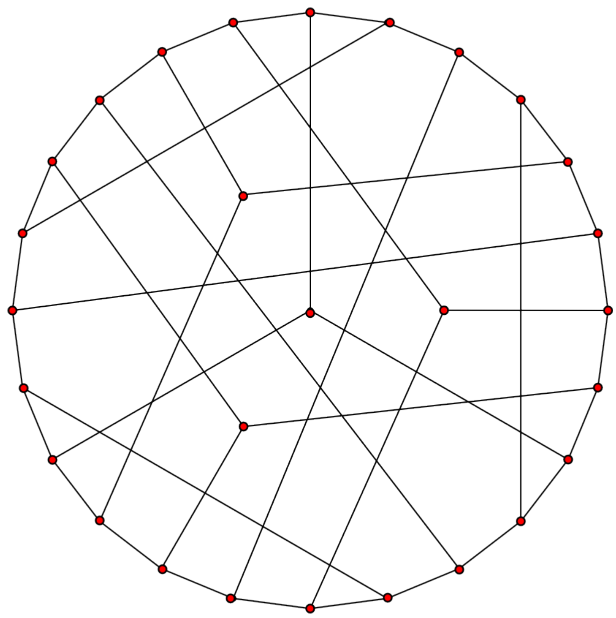
Znano je, da povezani točkovno tranzitivni grafi reda kp, kjer je $k < 4$ (z izjemo Petersonovega in Coxeterjevega grafa), reda p^j, kjer je $j < 4$, ter reda $2p^2$, kjer je p praštevilo, premorejo hamiltonski cikel. Obstoj hamiltonskih poti je dokazan tudi v povezanih točkovno tranzitivnih grafih reda $5p$ in $6p$. Najsplošnejši rezultat v tej smeri pa je Babaijev rezultat, ki pravi, da povezan točkovno tranzitiven graf na n točkah vsebuje cikel dolžine vsaj $\sqrt{3n}$ (glej [12]).

Poseben poudarek je bil dan tudi Cayleyjevim grafom. Največ do sedaj dokazanih rezultatov je odvisnih od različnih omejitev, kot so omejitve na različne tipe grup, na red grup, ali generatorske množice. Na primer v [35] je bilo dokazano, da imajo povezani Cayleyjevi grafi abelovih grup hamiltonski cikel. Na podlagi številnih člankov je znano tudi, da ima vsak povezan Cayleyjev graf grupe s ciklično komutatorsko podgrupo praštevilskega reda hamiltonski cikel (glej [20], [29], [35]).

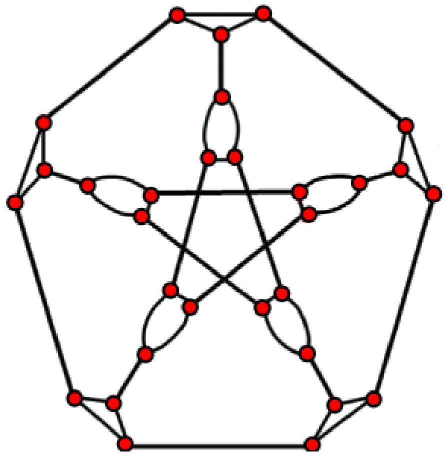
V tem delu se bomo osredotočili na problem obstoja hamiltonskih ciklov v kubičnih Cayleyjevih grafih alternirajoče grupe A_5. In sicer, da vas lažje vpeljemo, smo obsežen del namenili razlagi uvodnih pojmov algebrajične teorije grafov. V drugem poglevju je prikazan in obrazložen način, kako dobiti vse neizomorfne kubične Cayleyjeve grafe alternirajoče grupe A_5 in na kaj moramo biti pozorni pri samem računanju. V tretjem poglavju pa poiščemo hamiltonske cikle v vseh kubičnih Cayleyjevih grafih alternirajoče grupe A_5. Četrto poglavje pa je namenjemo Cayleyjevim grafom in prikazu znanih rezultatov na tem področju raziskovanja. Za podrobnejši vpogled vas vabimo, da si preberete naslednjih nekaj strani. Prijetno branje.



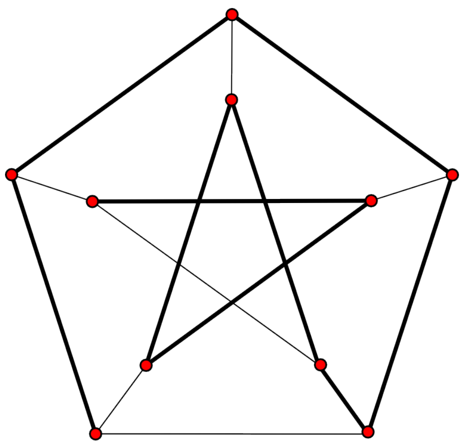
Slika 1: Petersenov graf.



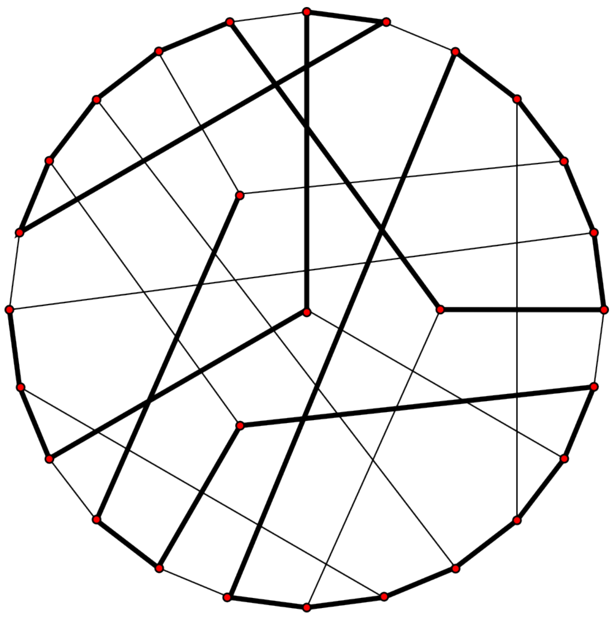
Slika 2: Coxeterjev graf.



Slika 3: Trisekcija Petersenovega grafa.



Slika 4: Petersenov graf premore hamiltonsko pot.



Slika 5: Coxeterjev graf premore hamiltonsko pot.

Poglavje 1

Razlaga pojmov

1.1 Osnovne lastnosti grup

Definicija 1.1.1. *Binarna operacija* $\star$ *na neprazni množici* G *je poljubna preslikava* $\star\colon G \times G \to G$*. Urejenemu paru* $(G, \star)$ *pravimo grupoid.*

Definicija 1.1.2. *Urejenemu paru* $(G, \star)$ *pravimo grupa, če velja:*

i) asociativnost: za vsak $a, b, c \in G$ *velja*

$$(a \star b) \star c = a \star (b \star c),$$

ii) obstoj nevtralnega elementa: obstaja tak $e \in G$*, da velja*

$$a \star e = e \star a = a,$$

iii) obstoj inverznega elementa: za vsak $a \in G$ *obstaja tak* $a' \in G$*, da je*

$$a \star a' = e = a' \star a.$$

Naj bo $(G, \star)$ grupa. Če velja:

$$a \star b = b \star a, \text{za vse } a, b \in G,$$

pravimo, da je grupa $(G, \star)$ komutativna ali abelova.

Red $o(G)$ grupe G je kardinalnost mnžice G. Grupa je končna, če je $o(G) < 1$. V nadeljevanju bomo red grupe G označevali z oznako $|G|$.

Definicija 1.1.3. *Naj bo* G *grupa in* $H \subseteq G$*. Če je* $(H, \star)$ *grupa, pravimo, da je* H *podgrupa grupe* G*. Oznaka:* $(H, \star) \leq (G, \star)$*.*

Od sedaj bomo operacijo $\star$ imenovali kar množenje, in grupo $(G, \star)$ označevali krajše le z G. Nevtralni element bomo označevali z id_G ali id ali 1. Inverz danega elementa a, pa bomo označevali z a^{-1}.

Definicija 1.1.4. *Naj bo G grupa ter x in y elementa grupe G. Elementa x in y sta konjugirana, če obstaja takšen element a iz G, da velja:*

$$y = a^{-1}xa. \tag{1.1}$$

Element $a^{-1}xa$ pišemo krajše kot x^a.

Naj bo G grupa in $S \subseteq G$. Potem z S^a označimo množico:

$$S^a = a^{-1}Sa = \{a^{-1}sa \mid s \in S\}.$$

V dokazu izreka 1.1.6, ki pove, da je v primeru, ko je H podgrupa dane grupe G, za vsak element $a \in G$ tudi H^a podgrupa, bomo uporabili naslednjo trditev.

Trditev 1.1.5. *Podmnožica H v grupi G je podgrupa, če za vse $x, y \in H$ velja:*

i) $id_G \in H$,

ii) $xy \in H$,

iii) $x^{-1} \in H$.

Dokaz trditve 1.1.5 si bralec lahko prebere v knjigi [21].

Izrek 1.1.6. *Naj bo G grupa, $H \leq G$ in a element grupe G. Potem je $H^a \leq G$, kjer je $H^a = \{a^{-1}ha \mid h \in H\}$ konjugiranka podgrupe H v grupi G.*

Dokaz. i) Vemo, da je id_G element H, saj je H podgrupa grupe G. Torej vzemimo elementa $id_G \in H$ in $a \in G$. Po definiciji grupe H^a sledi:

$$a^{-1}id_G a = a^{-1}a = id_G$$

S tem smo dokazali, da je $id_G \in H^a$.

ii) Vzemimo dva poljubna elementa $x, y \in H^a$. Ker je H podgrupa grupe G, sledi da sta elementa $x^a, y^a \in H$, torej je tudi njun produkt $x^a y^a \in H$. Če pa njun produkt poenostavimo dobimo sledeče:

$$x^a y^a = axa^{-1}aya^{-1} = axid_G ya^{-1} = axya^{-1} \in H,$$

iz tega sledi, da je $xy \in H^a$.

iii) Podobno, $x \in H^a$ implicira $axa^{-1} \in H$ in zato imamo $(axa^{-1})^{-1} = ax^{-1}a^{-1} \in H$ in $x^{-1} \in H^a$.

Po trditvi 1.1.5 sledi H^a je podgrupa v grupi G. □

Izrek 1.1.7. *(Lagrangev izrek) Naj bo G končna grupa in H podgrupa grupe G. Potem je $[G:H] = |G|/|H|$, kjer je $[G:H]$ označuje indeks podgrupe H v grupi G, t.j. število levih odsekov po podgrupi H v grupi G.*

Dokaz izreka 1.1.7 si bralec lahko prebere v knjigi [21].

Definicija 1.1.8. *Naj bo g element grupe G in H podgrupa grupe G. Pravimo, da element g normalizira H, če je $H^g = H$.*

Definicija 1.1.9. *Podgrupa H v grupi G je edinka, če je enaka vsem svojim konjugirankam (t.j. vsi elementi grupe G normalizirajo H). Oznaka: $H \triangleleft G$.*

Definicija 1.1.10. *Naj bo G grupa in S podmnožica grupe G. Potem obstaja najmanjša podgrupa grupe G, ki vsebuje S. Oznaka: $\langle S \rangle$. Pravimo, da S generira podgrupo $\langle S \rangle$. Če je $S = \{a\}$ za nek $a \in G$, grupo G imenujemo ciklična grupa.*

Primer 1.1.11. *Naj bo $G = \mathbb{Z}_{20}$ in $S = \{5\}$. Potem je $\langle S \rangle = \{0, 5, 10, 15\}$. Če je $S = \{1\}$, pa je $\langle S \rangle = \mathbb{Z}_{20}$.*

Trditev 1.1.12. *Naj bo $G = \langle a, b \rangle$ končna grupa generirana z dvema elementoma. Če a normalizira $\langle b \rangle$, je $\langle b \rangle \triangleleft G$.*

Dokaz. Naj bo G grupa generirana z elementoma a in b. Vemo, da je $\langle b \rangle^b = \langle b \rangle$ in $\langle b \rangle^a = \langle b \rangle$, saj a normalizira grupo generirano z elementom b. Vsak element grupe G je oblike:

$$x = \prod_i a^{l_i} b^{t_i}.$$

Iz tega sledi, da je $\langle b \rangle^x = \langle b \rangle$. Torej je $\langle b \rangle$ edinka v G. □

Definicija 1.1.13. *Naj bosta $(G, *)$ in $(H, \circ)$ grupi. Potem je preslikava $f : G \to H$ homomorfizem grup, če za vse $x, y \in G$ velja:*

$$f(x * y) = f(x) \circ f(y). \tag{1.2}$$

Definicija 1.1.14. *Naj bo $f : G \to H$ homomorfizem grup.*

i) Če je f injektivna preslikava, f imenujemo monomorfizem.

ii) Če je f surjektivna preslikava, f imenujemo epimorfizem.

iii) Če je f monomorfizem in epimorfizem, f imenujemo izomorfizem.

iv) Če je $G = H$, f imenujemo enodomorfizem.

v) Če je f izomorfizem in endomorfizem, f imenujemo avtomorfizem.

Definicija 1.1.15. *Simetrična grupa S_X neprazne množice X je grupa vseh permutacij (bijektivnih preslikav) množice X z operacijo sestavljanja preslikav.*

Simetrično grupo S_X na množici $X = I_n = \{1, 2, \ldots, n\}$ označujemo z oznako S_n in njen nevtralni element, ki ga imenujemo tudi identiteta, označujemo z oznako id_n.

Definicija 1.1.16. *Grupa G deluje na množici X z desne, če za vsak urejeni par $(x, g) \in X \times G$ obstaja tak element x^g iz množice X, da velja:*

i) $x^1 = x$ *za vsak* $x \in X$, *kjer je 1 nevtralni element grupe* G.

ii) $(x^g)^h = x^{(gh)}$ *za vsak* $x \in X$ *in vsak* $g, h \in G$.

Podobno lahko definiramo levo delovanje (glej [21]).

Definicija 1.1.17. *Relacija R na množici X je ekvivalenčna relacija, če veljajo naslednje lastnosti:*

i) (refleksivnost) $\forall x \in X : xRx$,

ii) (simetričnost) $\forall x, y \in X : xRy \Longrightarrow yRx$,

iii) (tranzitivnost) $\forall x, y, z \in X : xRy$ *in* $yRz \Longrightarrow xRz$.

Naj bo R ekvivalenčna relacija na množici X. Potem je ekvivalenčni razred $[x]_R$ elementa $x \in X$ glede na relacijo R množica vseh tistih elementov množice X, ki so z elementom x v relaciji R, tj. $[x]_R = \{y \in X \mid xRy\}$.

Definicija 1.1.18. *Naj grupa G deluje na množici X z desne strani. Na množico X vpeljemo relacijo $\sim$ s predpisom: $x \sim y \iff$ obstaja tak element $g \in G$, da je $y = x^g$.*

Trditev 1.1.19. *Relacija $\sim$ na množici X s predpisom: $x \sim y \iff$ obstaja tak element $g \in G$, da je $y = x^g$, je ekvivalenčna relacija.*

Dokaz. i) Vzemimo poljuben element x iz množice X. Ker je G grupa vemo, da premore id. Iz tega sledi:

$$x = x^{id} \Rightarrow x \sim x.$$

ii) Vzemimo poljubna elementa $x, y \in X$ in $g \in G$. Če je $x \sim y$ sledi:

$$\begin{aligned} x \sim y \Rightarrow \quad y &= x^g \text{ (pomnožimo z desne z } g^{-1}) \\ y^{g^{-1}} &= x^{gg^{-1}} \\ y^{g^{-1}} &= x \quad \Rightarrow y \sim x. \end{aligned}$$

iii) Vzemimo poljubne elemente $x, y, z \in X$ in $g, g' \in G$. Če je $x \sim y$ in $y \sim z$ vemo, da je $y = x^g$ in $z = y^{g'}$ iz tega sledi:

$$z = (x^g)^{g'} \Rightarrow x \sim z.$$

Po definiciji 1.1.17 sledi relacija $\sim$ je ekvivalenčna relacija. $\square$

Definicija 1.1.20. *Orbita elementa $x \in X$ pri delovanju grupe G na množici X, je množica:*

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

Trditev 1.1.21. *Za orbiti $Orb(x_1)$ in $Orb(x_2)$ pri delovanju grupe G na množici X, velja:*

$$Orb(x_1) \cap Orb(x_2) = \emptyset \quad ali \quad Orb(x_1) = Orb(x_2).$$

Dokaz. Naj imata orbiti $Orb(x_1)$ in $Orb(x_2)$ skupen element x'. To pomeni, da je $x' = x_i^{g_i}$ za nek $g_i \in G$, kjer je $i \in \{1, 2\}$. Zato je

$$\begin{aligned} Orb(x_i) &= \{x_i^g \mid g \in G\} \\ &= \{x_i^{g_i g_i^{-1} g} \mid g \in G\} \\ &= \{x'^{g_i^{-1} g} \mid g \in G\} \\ &= \{x'^g \mid g \in G\} = Orb(x'). \end{aligned}$$

Lastnosti iz trditve 1.1.21 sledijo iz tega, da so $Orb(x)$ ekvivalenčni razredi relacije $\sim$, definirane v definiciji 1.1.18. □

Definicija 1.1.22. *Stabilizator elementa $x \in X$, pri delovanju grupe G na množici X, je množica:*

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

Trditev 1.1.23. *Stabilizator G_x, pri delovanju grupe G na množici X, je podgrupa grupe G.*

Dokaz.

i) Naj bo id_G nevtralni element grupe G. Po definiciji delovanja stabilizatorja G_x sledi, da je $x^{id_G} = x$.

ii) Naj bosta $g_1, g_2 \in G_x$ in $x \in X$. Torej velja $x^{g_1} = x$ in $x^{g_2} = x$, in posledično:

$$x^{g_1 g_2} = (x^{g_1})^{g_2} = x^{g_2} = x \text{ oz. } g_1 g_2 \in G_x.$$

iii) Naj bo $g \in G_x$ in $x \in X$. Potem velja:

$$\begin{aligned} x &= x^g \\ x^{g^{-1}} &= x^{g g^{-1}} \\ x^{g^{-1}} &= x \end{aligned}$$

Torej je g^{-1} vsebovan v stabilizatorju G_x.

Po trditvi 1.1.5 smo dokazali, da je stabilizator G_x podgrupa grupe G. □

Izrek 1.1.24. *(Lema orbita - stabilizator) Za delovanje končne grupe G na množici X velja, da je $|Orb(x)| \cdot |G_x| = |G|$, kjer je $x \in X$.*

Dokaz. Definirajmo

$$\omega = \{(g, x') \in G \times Orb(x) \mid x^g = x'\}.$$

Izračunajmo moč množice ω na dva načina. Najprej dobimo, da je

$$|\omega| \;=\; \sum_{g \in G} |\{x' \in Orb(x) \mid x^g = x'\}| \;= \sum_{g \in G} 1 = |G|. \tag{1.3}$$

Drugič pa, da je

$$|\omega| \;=\; \sum_{x' \in Orb(x)} |\{g \in G \mid x^g = x'\}|.$$

Opazimo, da tisti elementi $g \in G$, ki preslikajo x v x', tvorijo desni odsek podgrupe G_x v G. Zato je število takih elementov enako $|G_x|$. Iz tega sledi, da se zgornja enakost piše kot

$$\sum_{x' \in Orb(x)} |\{g \in G \mid x^g = x'\}| \;=\; \sum_{x' \in Orb(x)} |G_x| \;= |Orb(X)| \cdot |G_x|. \tag{1.4}$$

Dokaz izreka sledi iz točk (1.3) in (1.4). □

Definicija 1.1.25. *Grupa G deluje na množici X tranzitivno, če za vsak par elementov $x, y \in X$ obstaja element $g \in G$, ki preslika x v y (tj. $x^g = y$).*

Definicija 1.1.26. *Grupa G deluje na množici X polregularno, če je $G_x = \langle id \rangle$ za vsak $x \in X$.*

Delovanje imenujemo regularno, če je hkrati tranzitivno in polregularno.

Definicija 1.1.27. *Permutacija $g \in S_X$ je cikel dolžine k, če v množici X obstajajo taki različni elementi $x_1, ..., x_k$, da veljajo naslednje enakosti:*

i) ${x_i}^g = x_{i+1}$ *za vsak* $i \in \{1, ..., k-1\}$,

ii) ${x_k}^g = x_1$,

iii) $x^g = x$ *za vsak* $x \in \{x_1, ..., x_k\}$.

Ciklu dolžine 2 pravimo transpozicija, ciklu dolžine $m \geq 2$ pa m-cikel.

Pravimo, da sta cikla $\alpha, \beta \in S_n$ ločena, če permutirata različne elemente množice I_n. Vsako permutacijo lahko zapišemo kot produkt ločenih ciklov. In vsako permutacijo lahko zapišemo kot produkt transpozicij. Le-ta ni enoličen, je pa enoličen do sodosti/lihosti števila transpozicij natančno (glej [30]).

Primer 1.1.28. *Naj bo* (12453) *permutacija iz S_5. Potem jo lahko zapišemo kot* (12)(14)(15)(13) *in kot* (53)(45)(24)(12).

Definicija 1.1.29. *Permutacija $\alpha \in S_n$ je soda, če jo lahko zapišemo kot produkt sodo mnogo transpozicij. Permutacija $\alpha \in S_n$ je liha, če jo lahko zapišemo kot produkt liho mnogo transpozicij.*

Izrek 1.1.30. *Množica vseh sodih permutacij v simetrični grupi S_n tvori podgrupo v S_n, ki jo imenujemo alternirajoča grupa A_n.*

Dokaz. V dokazu uporabimo trditev 1.1.5.

i) Očitno je id_{S_n} soda permutacija in zato vsebovana v A_n.

ii) Naj bosta $x, y \in A_n$ poljubni sodi permutaciji. Potem lahko tako x kot y zapišemo kot produkt sodo mnogo transpozicij. Naj bo t_x (t_y) število transpozicij v zapisu permutacije x (permutacije y) kot produkt transpozicij. Potem lahko produkt xy zapišemo s $t_x + t_y$ transpozicijami. Ker sta t_x in t_y sodi števili, je tudi $t_x + t_y$ sodo število in zato $xy \in A_n$.

iii) Naj bo $x \in A_n$. Potem obstaja taka permutacija $x^{-1} \in S_n$, da je $xx^{-1} = id_{S_n}$. Ker sta $x, id_{S_n} \in A_n$, ju lahko zapišemo kot produkt sodo mnogo transpozicij in zato se mora tudi permutacija x^{-1} zapisati kot produkt sodo mnogo transpozicij oziroma $x^{-1} \in A_n$.

□

Trditev 1.1.31. *Vsaka soda permutacija na množici $I_n = \{1, \ldots, n\}$, $n \geq 3$, je produkt samih 3-ciklov v S_n. Torej 3-cikli generirajo alternirajočo grupo A_n.*

Dokaz. Za $n = 3$ je stvar jasna. Naprej gre z indukcijo. Predpostavimo, da je bila trditev dokazana za vse sode permutacije na manj kot n točkah. Bodi $\pi \in A_n$. Permutacija $\sigma = \pi(a\ b\ c)$, kjer je $\pi(c) = a$, zadošča

$$\sigma(b) = \pi(c)(a\ b\ c) = b$$

in je seveda soda permutacija. Ker σ ohranja točko b, jo lahko razumemo kot sodo permutacijo na $n-1$ točkah. Po indukcijski prepostavki je σ produkt 3-ciklov, npr. $\sigma = \alpha_1\alpha_2 \ldots \alpha_s$. Postavimo $\alpha_0 = (a\ c\ b)$ in dobimo $\alpha_1 \ldots \alpha_s\alpha_0 = \pi$. □

Naj bo G grupa z nevtralnim elementom 1. Potem je očitno, da sta $\langle 1 \rangle$ in G vedno edinki v G. Imenujemo ju nepravi edinki grupe G. Če je edinka H grupe G različna od $\langle 1 \rangle$, jo imenujemo netrivialna edinka grupe G. Če sta $\langle 1 \rangle$ in G edini podgrupi edinki v grupi G pravimo, da je grupa G *enostavna.* Naslednji izrek, ki pove, da je alternirajoča grupa A_5 enostavna, bomo potrebovali v nadaljevanju pri določitvi vseh možnih generatorskih množic grupe A_5.

Definicija 1.1.32. *Enostavna grupa je grupa, ki nima pravih podgrup edink.*

Primer 1.1.33. *Naj bo $\mathbb{Z}_p$ aditivna grupa reda p, kjer je p praštevilo. Po Lagrangevem izreku 1.1.7 vemo, da mora red podgrupe $H \leq \mathbb{Z}_p$ deliti red grupe $\mathbb{Z}_p$. Ker pa je p praševilo vemo, da sta edina deljitelja števila p število 1 in p. Torej $\mathbb{Z}_p$ nima netrivialne podgrupe, torej nima netrivialne edinke in zato je $\mathbb{Z}_p$ enostavna grupa.*

Izrek 1.1.34. *Alternirajoča grupa A_n, $n \neq 4$, je enostavna.*

Dokaz. Za $n \leq 3$ je stvar jasna. Za $n = 4$ je grupa $\{id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ edinka v A_4. Recimo, da je $n > 4$ in bodi N netrivialna edinka v A_n. Pokazati želimo, da je $N = A_n$. V prvem koraku pokažimo, da ima N 3-cikel.

Naj bo $\alpha \neq id$ nek element v N, ki ohranja največje možno število elementov v $\{1, 2, \ldots, n\}$. Pa razcepimo sedaj α na produkt samih ciklov

$$\alpha = \alpha_1 \alpha_2 \ldots \alpha_s.$$

S ponovnim preštevilčenjem lahko dosežemo, da je $\alpha_1 = (1\ 2 \ldots k)$. Razlikujemo več možnosti:

a) α premakne vsako od števil 1, 2, 3, 4, 5. Postavimo $\beta = (3\ 4\ 5)$, potem $\beta^{-1}\alpha^{-1}\beta \in N$ in zato $\beta^{-1}\alpha^{-1}\beta\alpha \in N$. Toda lahko je pokazati, da permutacija $\beta^{-1}\alpha^{-1}\beta\alpha$ fiksira 1, obenem pa fiksira vse točke, ki jih fiksira permutacija α, protislovje z izborom permutacije α.

b) α premakne 1, 2, 3, 4 in nič drugega. V tem primeru mora biti $\alpha = (1\ 2)(3\ 4)$. Potem je za $\beta = (3 4 5)$, $\beta^{-1}\alpha^{-1}\beta\alpha \in N$. Ker je $\beta^{-1}\alpha^{-1}\beta\alpha = \beta$, sledi, da $\beta \in N$ in β premakne manj elementov kot α. To pa je v protislovju s predpostavko, da α premakne najmanj elementov.

c) $\alpha = (1 2 3)$ in N torej vsebuje 3-cikel.

Pokazati moramo še, da N vsebuje vsak 3-cikel. V ta namen izberimo sodo permutacijo

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \\ i & j & k & \cdots \end{pmatrix}$$

Potem je $\sigma(1 2 3)\sigma^{-1} = (i\, j\, k)$ element grupe N (saj je namreč N edinka). Ker so bile i, j, k poljubne točke, so vsi 3-cikli v N. Po trditvi 1.1.31 je zato $N = A_n$.

$\square$

Definicija 1.1.35. *Naj bo G grupa in $a, b \in G$. Potem je $[a, b] = a^{-1}b^{-1}ab$ komutator elementov a in b. Podgrupo $G' = [G, G] = \langle [a, b] \mid a, b \in G \rangle$ imenujemo komutatorska podgrupa grupe G.*

Definicija 1.1.36. *Naj bo G grupa in N_i njene podgrupe. Potem zaporedju*

$$1 = N_0 \leq N_1 \leq N_2 \leq \cdots \leq N_{k-1} \leq N_k = G$$

pravimo komutatorska vrsta, če velja, da je $N_i \trianglelefteq N_{i+1}$ in da je kvocientna grupa N_{i+1}/N_i enostavna grupa, kjer $0 \leq i \leq k-1$.

Naj bo n pozitivno celo število. Potem je n-ta komutatorska podgrupa grupe G definirana kot

$$G^{(0)} = G, G^{(n)} = [G^{(n-1)}, G^{(n-1)}] \text{ ko je } n \geq 1.$$

Definicija 1.1.37. *Grupa G je rešljiva, če obstaja tako zaporedje podgrup*

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_s = G$$

tako, da je kvocientna grupa G_{i+1}/G_i abelska za vsak $i = 0, 1, \ldots, s-1$.

Definicija 1.1.38. *Naj bo G grupa. Če obstaja tako naravno število n, da je $G^{(n)} = \langle id \rangle$, pravimo da je G rešljiva grupa.*

Primer 1.1.39. *Vsaka abelova grupa je rešljiva.*

Ker je v abelovi grupi G za poljubna elementa $a, b \in G$ njun komutator $[a, b] = a^{-1}b^{-1}ab = a^{-1}ab^{-1}b = 1$, je $G^{(1)} = [G, G]$ in zato je grupa G rešljiva.

Izrek 1.1.40. *Če sta H in G/H rešljivi grupi, kjer je $H \triangleleft G$, je rešljiva tudi grupa G. Še več, velja tudi:*

$$H \text{ in } G/H \text{ sta rešljivi} \Leftrightarrow G \text{ rešljiva.}$$

Dokaz izreka 1.1.40 si bralec lahko prebere v knjigi [28].

Definicija 1.1.41. *Grupa reda p^k, kjer je p praštevilo, imenujemo p-grupa.*

Definicija 1.1.42. *Center $Z(G)$ grupe G je množica elementov grupe G, ki komutirajo z vsemi elementi grupe G,*

$$Z(G) = \{x \in G \mid xa = ax \text{ za vsak } a \in G\}.$$

Izrek 1.1.43. *Vsaka p-grupa (p je praštevilo) je rešljiva.*

Dokaz. Naj bo G p-grupa za neko praštevilo p. Potem je $|G| = p^n$ za nek $n \in \mathbb{N}$.

Za $n = 1$ je grupa G reda p in zato izomorfna ciklični grupi $\mathbb{Z}_p$, ki je rešljiva, kot smo videli v primeru 1.1.39.

Recimo, da izrek velja za vse $n < n_0$ in naj bo G grupa reda p^{n_0}. Vemo, da ima vsaka p-grupa netrivialni center [28]. V primeru, da je $G = Z(G)$, sledi da je G abelova. Torej je $[G, G] = \langle id \rangle$ in je G rešljiva. Če pa je $Z(G) \subset G$, je $|Z(G)| = p^l$, kjer je $p^l < n_0$ in je $|G/Z(G)| = p^t$, kjer je $t < n_0$. Po indukcijski predpostavki sta $Z(G)$ in $G/Z(G)$ rešljivi, po izreku 1.1.40 pa sledi, da je tudi grupa G rešljiva. $\square$

Izrek 1.1.44. *Če je G grupa reda pqr, kjer so p, q, r praštevila, je grupa G rešljiva.*

Izrek 1.1.45. *(Burnsidov $p^a q^b$ izrek) Vsaka grupa reda $p^a q^b$, kjer sta p, q praštevili in a, b naravni števili, je rešljiva.*

Dokaza izreka 1.1.45 in izreka 1.1.44 si bralec lahko prebere v knjigi [19].

Trditev 1.1.46. *Alternirajoča grupa A_5 je najmanjša nerešljiva grupa.*

Dokaz. Prepričajmo se, da je alternirajoča grupa A_5 res nerešljiva. Po izreku 1.1.34 vemo, da sta edini edinki v A_5 nepravi edinki $\{id\}$ in A_5. Spomnimo se, da je komutatoska podgrupa $[G, G]$ grupe G najmanjša podgrupa edinka grupe G, za katero je kvocientna grupa $G/[G, G]$ abelova [28]. Ker A_5 ni abelova grupa in je $[A_5, A_5] = A_5$ oziroma $A_5^{(n)} = A_5$. Torej A_5 ni rešljiva.

Sedaj, ko smo se prepričali, da je alternirajoča grupa A_5 nerešljiva, se prepričajmo, da ne obstaja grupa G reda $n < 60$, ki je nerešljiva. POljubno manjše število lahko zapišemo kot produkt $p^{t_1} q^{t_2} r^{t_3}$, kjer so p, q in r praštevila. Če je $n = p^t$, je G rešljiva po izreku 1.1.43. Če je $n = p^t q^s$, je G rešljiva po Burnsidovem izreku 1.1.45. Če je $n = p^{t_1} q^{t_2} r^{t_3}$, dejstvo da je $n < 60 = 2^2 \cdot 3 \cdot 5$, pove, da je $n = 2 \cdot 3 \cdot 5$ in zato je po izreku 1.1.44 G rešljiva. □

V dokazu naslednje trditve bomo potrebovali naslednje dejstvo. Ker za poljuben par elementov $i, j \in I_n$, $n \leq 2$, obstaja taka permutacija $\alpha \in A_n$, da je $\alpha(i) = j$, lahko sklepamo, da alternirajoča grupa A_n deluje tranzitivno na množici I_n.

Trditev 1.1.47. *Naj bodo a, b in c taki elementi alternirajoče grupe A_5, da je $a^2 = b^2 = c^2 = id$, kjer je id nevtralni element v A_5. Če noben par $\{x, y\}$, ki je vsebovan v $\{a, b, c\}$, ne generira tranzitivne grupe na množici $\{1, 2, 3, 4, 5\}$, potem $\{a, b, c\}$ ne generira alternirajoče grupe A_5.*

Dokaz. Naj bo $\{a, b, c\} \subseteq A_5$ množica treh takih involucij iz alternirajoče grupe A_5, da noben par involucij iz $\{a, b, c\}$ ne generira tranzitivne grupe na množici $I_5 = \{1, 2, 3, 4, 5\}$.

Naj bo $\{x, y\} \subseteq \{a, b, c\}$ poljuben par involucij iz $\{a, b, c\}$. Potem je produkt xy reda 2, 3 ali 5 (saj produkt dveh sodih permutacij soda permutacija, torej ker se nahajamo v A_5 so te možnosti involucija ali 3-cikel ali 5-cikel). V slednjem primeru je $\langle x, y \rangle \cong D_{2 \cdot 5}$ tranzitivna grupa na I_5, kar je v nasprotju z našo predpostavko.

Recimo, da je xy reda 2. Potem je $\langle x, y \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ in brez škode za splošnost lahko rečemo, da je $x = (1\ 2)(3\ 4)(5)$ in $y = (1\ 3)(2\ 4)(5)$. Torej ima $\langle x \rangle$ na I_5 tri orbite: $\{1, 2\}$, $\{3, 4\}$ in $\{5\}$, grupa $\langle y \rangle$ ima orbite $\{1, 3\}$, $\{2, 4\}$ in $\{5\}$ in grupa $\langle x, y \rangle$ ima orbiti $\{1, 2, 3, 4\}$ in $\{5\}$. Če tretja involucija z v $\{a, b, c\}$ fiksira $5 \in I_5$, potem očitno tudi $\langle a, b, c \rangle$ fiksira 5 in zato ima grupa $\langle a,b,c\rangle$ na I_5 dve orbiti, torej $\langle a,b,c\rangle \neq A_5$. Če tretja involucija z v $\{a,b,c\}$ ne fiksira $5 \in I_5$, potem lahko, ker $\langle x,z\rangle$ ni tranzitivna na I_5, brez škode za splošnost predpostavimo, da ima $\langle z\rangle$ na I_5 naslednje tri orbite $\{1,5\}$, $\{3,4\}$ in $\{2\}$. Vendar potem je pa $\langle y,z\rangle$ tranzitivna na I_5, protislovje.

Recimo, da je xy reda 3. Potem je $\langle x,y\rangle \cong S_3$ in brez škode za splošnost lahko rečemo, da je $x = (12)(34)(5)$ in $y = (12)(45)(3)$. Torej ima $\langle x\rangle$ na I_5 tri orbite: $\{1,2\}$, $\{3,4\}$ in $\{5\}$, grupa $\langle y\rangle$ ima orbite $\{1,2\}$, $\{4,5\}$ in $\{3\}$ in grupa $\langle x,y\rangle$ ima orbiti $\{1,2\}$ in $\{3,4,5\}$. Če je tretja involucija z v $\{a,b,c\}$ oblike $(12)(ij)$, kjer sta i in j elementa iz orbite $\{3,4,5\}$, potem ima tudi grupa $\langle a,b,c\rangle$ na I_5 dve orbiti, torej $\langle a,b,c\rangle \neq A_5$. Če tretja involucija z v $\{a,b,c\}$ ne ohranja množice $\{1,2\}$, potem lahko brez škode za splošnost vzamemo $(14)(25)$. Ker $\langle y,z\rangle$ ni tranzitivna na I_5, brez škode za splošnost lahko predpostavimo, da ima $\langle z\rangle$ na I_5 naslednje tri orbite $\{1,4\}$, $\{2,5\}$ in $\{3\}$. Vendar potem je pa $\langle x,z\rangle$ tranzitivna na I_5, protislovje.

□

Trditev 1.1.48. *Naj bo G grupa s prezentacijo $\langle a,x \mid a^2 = x^3 = (ax)^3 = id\rangle$. Potem je G izomorfna alternirajoči grupi A_4.*

Dokaz. Iz relacij $a^2 = x^3 = id$ sklepamo, da vsak element grupe G lahko zapišemo kot x^i ali $x^i a x^{\pm1} a \cdots x^{\pm1} a x^j$, kjer sta $i,j \in \{0,\pm1\}$. Po relaciji $(xa)^3 = id$ oziroma $xaxaxa = id$, ki implicira $axa = (xax)^{-1} = x^{-1}ax^{-1}$ in $xax = (axa)^{-1} = ax^{-1}a$, sledi, da je $ax^{\pm1}a = x^{\mp1}ax^{\mp1}$. Po uporabi te enakosti, izraz $x^i a x^{\pm1} a \ldots x^{\pm1} a x^j$ preoblikujemo v izraz oblike $x^i a x^j$ z enim samim elementom a v izrazu. Zato je

$$G = \{x^i, x^i a x^j \mid i,j \in \{0,\pm1\}\}.$$

Iz tega sledi, da je $|G| \leq 3 + 3 \times 3 = 12$. Po drugi strani, če v alternirajoči grupi A_4 vzamemo elementa $b = (123)$ in $c = (12)(34)$, je njun produkt enak $bc = (243)$ in zato $c^2 = b^3 = (bc)^3 = id$. Očitno elementa b in c generirata alternirajočo grupo A_4 in obstaja homomorfizem, ki grupo G preslika v alternirajočo grupo A_4.

Tabela 1.1: Homomorfizem, ki grupo G preslika v alternirajočo grupo A_4.

$x^0 \to id$	$x \to (123)$	$a \to (12)(34)$	$xa \to (243)$
$x^{-1} \to (132)$	$x^{-1}a \to (143)$	$xax \to (124)$	$xax^{-1} \to (13)(24)$
$x^{-1}ax \to (14)(23)$	$x^{-1}ax^{-1} \to (142)$	$ax \to (134)$	$ax^{-1} \to (234)$

Ker je red alternirajoče grupe A_4 enak $|A_4| = 12$ in $|G| \leq 12$, iz tega sledi, da je $|G| = 12$ in $G \cong A_4$. □

Trditev 1.1.49. *Naj bo G grupa s prezentacijo*

$$\langle a,b \mid a^2 = x^5 = (ax)^3 = id\rangle \tag{1.5}$$

ali

$$\langle a, b \mid a^2 = x^3 = (ax)^5 = id\rangle. \tag{1.6}$$

Potem je G izomorfna alternirajoči grupi A_5.

Dokaz. Naj bo G grupa s prezentacijo (1.5). Potem iz relacij v (1.5) dobimo:

$$\begin{gathered} axa = x^{-1}ax^{-1}, ax^{-1}a = xax, \\ ax^2a = x^{-1}(ax^{-2}a)x^{-1}, ax^{-2}a = x(ax^2a)x, \\ ax^2ax^2a = x^{-1}(ax^2a)x^{-1}, ax^{-2}ax^{-2}a = x(ax^{-2}a)x \\ ax^{-2}ax^2a = x(ax^2ax^{-2}a) = (ax^2ax^{-2}a)x^{-1}. \end{gathered}$$

Torej lahko vsak element iz grupe G zapišemo v sledeči obliki:

$$x^i, x^iax^j, x^i(ax^2a)x^j, x^i(ax^2ax^{-2})a,$$

kjer sta $i, j \in \{0,1,2,3,4\}$. Zato je red grupe G enak $|G| \leq 60$. Ko v alternirajoči grupi A_5 definiramo $x = (12345)$ in $a = (12)(34)$, dobimo $xa = (245)$, torej izbrana elementa izpolnjujeta pogoj $a^2 = x^5 = (ax)^3 = id$.

Ko ima G prezentacijo (1.6), pa si pomagamo s tem dejstvom, da je grupa G s prezentacijo (1.5) izomorfna alternirajoči grupi A_5. Recimo, da je $G = \langle a, x | a^2 = x^3 = (ax)^5 = id\rangle$. Naj bo $z = ax$. Potem je $az = aax = x$ reda 3 in $G = \langle a, z\rangle$ (a imamo, x pa dobimo kot produkt elementov a in z in zato je grupa generirana z elementoma za in z kar enaka grupi G). Torej $G = \langle a, z | a^2 = z^5 = (az)^3 = id\rangle$. In po prvem delu trditve, sledi da je grupa G izomorfna alternirajoči grupi A_5. □

1.2 Osnovne lastnosti grafov

Definicija 1.2.1. *Digraf je urejeni par $\Gamma = (V, E)$, kjer je V neprazna množica. Elemente te množice imenujemo točke ali vozlišča. E je podmnožica množice $V \times V$. Elemente te množice imenujemo loki.*

Definicija 1.2.2. *Graf (V, E) je digraf, za katerega velja:*

i) za vsak $\alpha \in V$ velja, da $(\alpha, \alpha) \notin E$ (nima zank).

ii) za vse $\alpha, \beta \in V$ velja: če $(\alpha, \beta) \in E \Rightarrow (\beta, \alpha) \in E$.

Točke digrafa Γ označujemo tudi z $V(\Gamma)$, ter loke z $E(\Gamma)$. V grafu Γ je za vsak lok (α, β) tudi (β, α) lok. Zato par takšnih dveh lokov nadomestimo z neusmerjeno povezavo $\{\alpha, \beta\}$, ki jo krajše označujemo tudi z $\alpha\beta$.

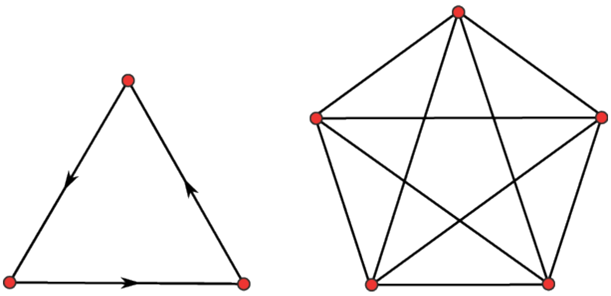
Definicija 1.2.3. *Stopnja točke u v grafu Γ, označimo jo z $deg_\Gamma(u)$ ali $d_\Gamma(u)$, je število povezav v grafu Γ, ki imajo točko u za svoje krajišče.*

Točkam stopnje 0 pravimo *izolirane točke*, točkam stopnje 1 pa *listi*. Najmanjšo stopnjo točke grafa Γ označimo z $\delta(\Gamma)$, največjo pa z $\Delta(\Gamma)$.

Definicija 1.2.4. *Graf Γ je regularen, če velja $\delta(\Gamma) = \Delta(\Gamma)$, in $d-$regularen, če velja $d = \delta(\Gamma) = \Delta(\Gamma)$.*

Kubični graf je 3-regularen graf. To pomeni, da je stopnja vsake točke enaka 3.

Primer 1.2.5. *Na sliki 1.1 vidimo digraf na treh točkah in 4-regularen graf na petih točkah.*



Slika 1.1: digraf in 4-regularen graf

Definicija 1.2.6. *Naj bo Γ graf in u točka grafa Γ. Množici točk, s katerimi je u povezana, pravimo množica sosedov točke u.*

Definicija 1.2.7. *Sprehod (dolžine k) je niz k povezav v grafu*

$$(u, x)(x, y) \dots (t, z)(z, w)$$

Temu sprehodu lahko rečemo tudi sprehod med točkama u in w. Povezave niso usmerjene, zato predstavlja niz

$$(w, z)(z, t) \dots (y, x)(x, u)$$

isti sprehod. Pogosto sprehod pišemo samo z zaporedjem točk na danem nizu povezav.

$$uxy \dots tzw$$

Sprehod je *enostaven*, ko so vse vsebovane povezave v sprehodu različne. Enostaven sprehod je *pot*, kadar so vse točke $v_0, v_1, \dots, v_k$ med seboj različne. Enostavni sprehod je *cikel*, ko so vse točke $v_0, v_1, \dots, v_{k-1}$ med seboj različne in je $v_0 = v_k$.

Definicija 1.2.8. *Graf Γ je hamiltonski, če obstaja cikel, na katerem so vse točke grafa Γ. Tak cikel imenujemo hamiltonski cikel.*

Definicija 1.2.9. *Graf* Γ *je dvodelen, če je njegove točke mogoče razdeliti v dve podmnožici tako, da sta poljubni točki znotraj vsake od teh podmnožic nesosednji.*

Definicija 1.2.10. *Homomorfizem iz digrafa* Γ *v digraf* Γ' *je preslikava*

$$f : V(\Gamma) \to V(\Gamma'),$$

za katero velja: če $uv \in E(\Gamma)$, *potem* $f(u)f(v) \in E(\Gamma')$. *Homomorfizmi so torej preslikave vozlišč, ki ohranjajo sosednost.*

i) Če je f *injektivna preslikava,* f *imenujemo monomorfizem.*

ii) Če je f *surjektivna preslikava,* f *imenujemo epimorfizem.*

iii) Če je f *monomorfizem in epimorfizem,* f *imenujemo izomorfizem.*

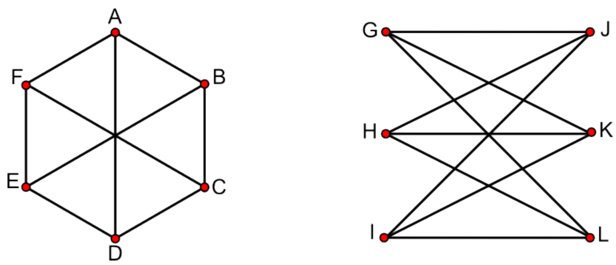
iv) Če je $X = Y$, f *imenujemo enodomorfizem.*

v) Če je f *izomorfizem in endomorfizem,* f *imenujemo avtomorfizem.*

Primer 1.2.11. *Definirajmo preslikavo*

$$\rho : \{A, B, C, D, E, F\} \to \{G, H, I, J, K, L\},$$

tako da je $\rho(A) = G$, $\rho(B) = J$, $\rho(C) = H$, $\rho(D) = K$, $\rho(E) = I$, $\rho(F) = L$. *Hitro se prepričamo, da je* ρ *izomorfizem grafov na spodnji sliki.*



Slika 1.2: Izomorfna si grafa.

Naj bo Γ graf. Potem množica vseh avtomorfizmov grafa Γ tvori grupo za običajno komponiranje preslikav, imenujemo jo *grupa avtomorfizmov* grafa Γ. Oznaka $Aut(\Gamma)$.

Definicija 1.2.12. *Digraf* $\Gamma = (V, E)$ *je točkovno tranzitiven, če grupa avtomorfizmov* $Aut(\Gamma)$ *deluje tranzitivno na množico točk digrafa.*

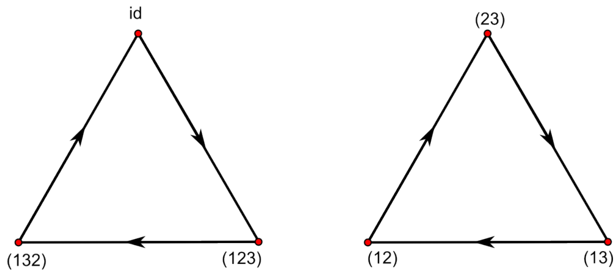
Definicija 1.2.13. *Cayleyjev digraf* $\Gamma = Cay(G, S)$ *grupe* G *glede na množico* S *je digraf, za katerega velja:*

i) $V(\Gamma) = G$,

ii) $(u,v) \in E(\Gamma) \Longleftrightarrow \exists s \in S : v = su$.

Za poljubno točko $u \in V(\Gamma)$ je število lokov, ki se začnejo v točki u enako $|S|$.

Primer 1.2.14. *Naj bo grupa $G = S_3$ in $S = \{(123)\}$. Slika 1.3 prikazuje Cayleyjev digraf $Cay(G,S)$.*



Slika 1.3: Cayleyjev graf $Cay(S_3,(123))$.

Trditev 1.2.15. *Naj bo G grupa in S njena podmnožica. Potem je Cayleyjev digraf $Cay(G,S)$ graf natanko tedaj, ko velja:*

$$1 \notin S \ \ (nima\ zank) \tag{1.7}$$

$$S = S^{-1} \ \ oz.\ če\ s \in S,\ potem\ tudi\ s^{-1} \in S. \tag{1.8}$$

Dokaz. Najprej predpostavimo, da je $\Gamma = \mathrm{Cay}(G,S)$ Cayleyjev graf. Potem Γ nima zank in zato za vsak $x \in G$ in vsak $s \in S$ velja, da je $x \neq sx$. Torej $1 \notin S$.

Naj bo (x,y) poljuben lok grafa Γ. Ker je Γ graf, je tudi (y,x) lok grafa Γ. Torej $(x,y),(y,x) \in E(\Gamma)$ in zato obstajata taka $s,s' \in S$, da je $y = sx$ in $x = s'y$. Odtod sledi, da je $y = sx = ss'y$. Če obe strani enačbe z leve pomnožimo z y^{-1} (z inverzom elementa y v grupi G), sledi da je $s' = s^{-1} \in S$.

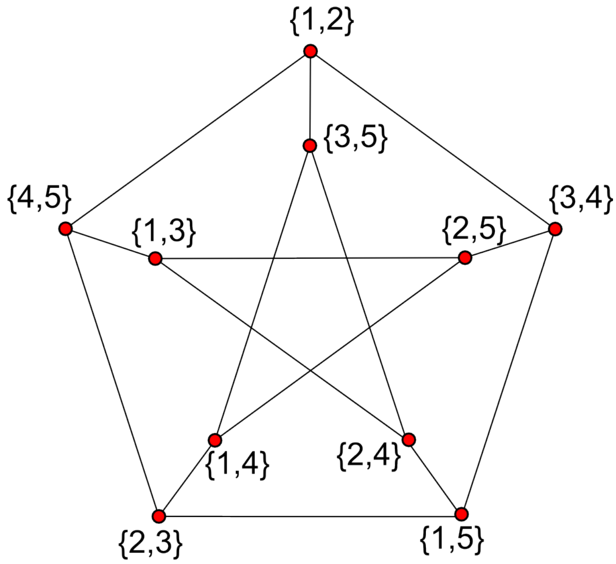
Za dokaz obratne smeri predpostavimo, da za Cayleyjev digraf $\Gamma = \mathrm{Cay}(G,S)$ veljata (1.7) in (1.8). Ker $1 \notin S$, $(x, 1 \cdot x) \notin E(\Gamma)$. Torej digraf Γ nima zank. Naj bo $(x,y) \in E(\Gamma)$ poljuben lok grafa Γ. Potem obstaja tak $s \in S$, da je $y = sx$. Če to enakost z desne pomnožimo z elementom s^{-1} dobimo $x = s^{-1}y$. Ker je po predpostavki $s^{-1} \in S$, odtod sledi, da je $(y,x) \in E(\Gamma)$. □

Sabiddusi je leta 1956 dokazal, da je digraf Γ Cayleyjev graf natanko tedaj, ko njegova grupa avtomorfizmov $Aut(\Gamma)$ vsebuje podgrupo, ki deluje regularno na množici točk grafa Γ. Torej je vsak Cayleyjev graf $Cay(G,S)$ točkovno tranzitiven [25], obrat pa ne drži. Petersenov graf je točkovno tranzitiven ni pa Cayleyjev graf.

Primer 1.2.16. *Graf na sliki 1.4, poznan kot Petersenov graf* $GP(5,2)$*, je točkovno tranzitiven. O tem se prepričamo takole: točke Petersenovega grafa označimo z 2-podmnožicami* $\{i,j\}$*, kjer sta* i *in* j*,* $i \neq j$*, elementa množice* I_5*, kot kaže spodnja slika. Dve točki sta povezani, če sta pripadajoči 2-podmnožici disjunktni. Za poljubni točki* $\{i,j\}$ *in* $\{k,l\}$*, kjer* $i \neq j$ *in* $k \neq l$*, obstaja premutacija iz simetrične grupe* S_5*, ki prvo preslika v drugo*

$$\{i,j\}^{(ik)(jl)} = \{k,l\},$$

če $i \notin \{l,k\}$ *in* $j \notin \{k,l\}$*. Sicer moramo biti nekoliko bolj pazljivi. A kljub temu lahko najdemo permutacijo, ki slika en par v drugega. Ker vse permutacije iz simetrične grupe* S_5 *disjunktne 2-podmnožice slikajo v disjunktne 2-podmnožice, je vsaka permutacija iz* S_5 *tudi avtomorfizem grafa* $GP(5,2)$ *in zato je* $G(5,2)$ *točkovno tranzitiven.*



Slika 1.4: Petersenov graf

Preverimo še dejstvo, da Petersenov graf ni Cayleyjev graf $Cay(G,S)$*. Pri dokazu bomo potrebovali dejstvo, da Petersenov graf ne vsebuje cikla dolžine* 4 *in da Petersenov graf ni dvodelen. Recimo nasprotno, da je Petersenov graf Cayleyjev graf* $Cay(G,S)$ *grupe* G *glede na množico* S*. Ker je Petersenov graf kubični graf na* 10*-ih točkah je* $|G| = 10$ *in* $|S| = 3$*. Ker sta ciklična grupa* $\mathbb{Z}_{10}$ *in diederska grupa* $D_{2\cdot 5}$ *edini grupi reda* 10 *(glej [21]), je grupa* G *izomorfna grupi* $\mathbb{Z}_{10}$ *ali diederski grupi* $D_{2\cdot 5}$*. Po povedi iz definicije 1.2.13, ki pravi, da je izhodna valenca Cayleyjevega digrafa* $Cay(G,S)$ *enaka* $|S|$ *in enačbi (1.8) iz trditve 1.2.15, množica* S *sestoji iz treh elementov reda* 2 *ali enega elementa reda* 2*, elementa reda več kot* 2 *in njegovega inverza.*

1) Naj bo grupa $G = \mathbb{Z}_{10}$.

Ker grupa $\mathbb{Z}_{10}$ vsebuje le en element reda 2 (to je element 5), je $S = \{5, x, -x\}$, kjer $x \notin \{0, 5\}$. Vendar potem pa je $(0, 5, x+5, 5, 0)$ 4-cikel v Petersenovem grafu. Protislovje, saj je najmanjši cikel v Petersenovem grafu dolžine 5.

2) Naj bo $G = D_{2\cdot 5} = \langle \tau, \rho \mid \tau^2 = \rho^5 = id, \tau\rho\tau = \rho^{-1} \rangle$.

Potem so elementi reda 2 v G natanko elementi iz množice $\{\tau, \tau\rho, \tau\rho^2, \tau\rho^3, \tau\rho^4\}$. Ker ima S en ali tri elemente reda 2, imamo dve možnosti:

2.1) $S = \{\tau\rho^a, \rho^b, \rho^{-b}\}$, kjer $a \in \{0, 1, 2, 3, 4\}$ in $b \in \{1, 2\}$.

Vendar potem je $(id, \rho^a\tau, \rho^{a-b}\tau, \rho^{-b}, id)$ 4-cikel v Petersenovem grafu. Protislovje, s tem, da je najmanjši cikel v Petersenovem grafu dolžine 5.

2.2) $S = \{\tau\rho^a, \tau\rho^b, \tau\rho^c, \}$, kjer $a, b, c \in \{0, 1, 2, 3, 4\}$.

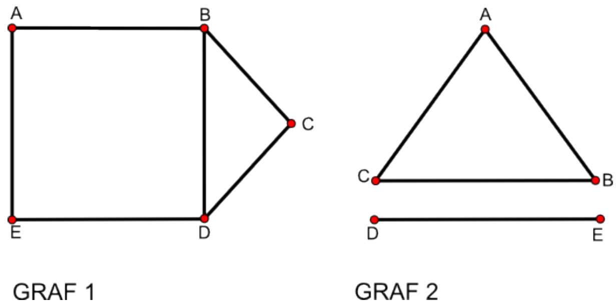
Če naredimo particijo elementov iz $D_{2\cdot 5}$ na sledeči način: $\{id, \rho, \rho^2, \rho^3, \rho^4\}$ in $\{\tau, \tau\rho, \tau\rho^2, \tau\rho^3, \tau\rho^4\}$, lahko hitro preverimo, da je dobljeni graf dvodelen. Lahko sklepamo, da Cayleyjev graf $Cay(G, S)$ ni Petersenov graf, saj Petersenov graf ni dvodelen (vsebuje namreč cikel dolžine 5).

Ker smo prišli do protislovja, sledi da Petersenov graf ni Cayleyjev graf.

Definicija 1.2.17. *Graf Γ je povezan, če obstaja pot poljubne točke v poljubno točko grafa Γ. Sicer je graf nepovezan.*

Primer 1.2.18. *Na sliki 1.5 sta predstavljena primera povezanega in nepovezanega grafa. Graf 1 je primer povezanega grafa, medtem ko je graf 2 nepovezan graf, saj ne obstaja pot od točke A do točke D.*

Trditev 1.2.19. *Cayleyjev graf $Cay(G, S)$ na grupi G glede na množico S je povezan $\Longleftrightarrow G = \langle S \rangle$ (množica S generira grupo G).*



Slika 1.5: Povezan in nepovezan graf.

Dokaz. ($\Leftarrow$) Naj množica S generira grupo G. Potem lahko vsak element $x \in G$ zapišemo kot produkt elementov iz množice S, to je: $x = s_0 s_1 \dots s_k$, kjer je $s_i \in S$ za vsak i. Temu pa v $Cay(G,S)$ ustreza pot od točke 1 do točke x. Iz tega sledi, da je Cayleyjev graf $Cay(G,S)$ povezan.

($\Rightarrow$) Naj bo $Cay(G,S)$ povezan. Potem obstaja pot v $Cay(G,S)$ med točko 1 in poljubno drugo točko x iz grupe G. Torej obstaja zaporedje $g_0 = 1, g_1, g_2, \dots, g_k = x$, za katero velja, da je $(g_i, g_{(i+1)})$ element množice povezav v Cayleyjevem grafu $Cay(G,S)$, za vsak $i \in \{0, \dots, k-1\}$. Sledi, da za vsak $i \in \{0, \dots, k-1\}$ velja: $g_{(i+1)} = sg_i$ za nek poljuben element s iz množice S. Dokaz gre z indukcijo. Očitno je $1 \in \langle S \rangle$. Recimo, da je za nek i produkt $g_0 g_1 \dots g_i$ element grupe $\langle S \rangle$. Potem velja: $g_{(i+1)} = sg_i$ za nek element s iz množice $\langle S \rangle$. Dejstvo, da je $g_i \in S$ in $s \in S$, pove, da $g_{(i+1)} \in \langle S \rangle$. Torej vsak grupni element pripada grupi $\langle S \rangle$. Iz tega pa sledi, da je grupa G generirana z množico S. $\square$

Poglavje 2

Kubični Cayleyjevi grafi alternirajoče grupe A_5

V nadaljevanju se bomo osredotočili na iskanje kubičnih Cayleyjevih grafov alternirajoče grupe A_5 in hamiltonskih ciklov. Prvi razdelek je namenjen obrazložitvi, kako lahko pridobimo 9 neizomorfnih grafov. V drugem razdelku, pa dokažemo, da ima vsak povezan kubični Cayleyjev graf grupe A_5 hamiltonski cikel.

2.1 Iskanje kubičnih Cayleyjevih grafov alternirajoče grupe A_5.

Za lažje razumevanje podrobneje opišimo alternirajočo grupo A_5. Alternirajoča grupa A_5 je reda $5!/2 = 60$. Njeni elementi so: identiteta, petnajst involucij, dvajset 3-ciklov in štriindvajset 5-ciklov:

$$\begin{aligned} A_5 = \{&id, (123), (132), (124), (142), (125), (152), (134), (143),\\ &(135), (153), (145), (154), (234), (243), (235), (253), (245),\\ &(254), (345), (354), (12)(34), (13)(24), (14)(23), (12)(35),\\ &(13)(25), (15)(23), (12)(45), (14)(25), (15)(24), (13)(45),\\ &(14)(35), (15)(34), (23)(45), (24)(35), (25)(34), (12345), (12453),\\ &(12354), (12435), (12534), (12543), (13245), (13254), (13524),\\ &(13542), (13425), (13452), (14235), (14253), (14532), (14523), (14325),\\ &(14352), (15234), (15243), (15423), (15432), (15324), (15342)\}.\end{aligned}$$

V tem poglavju se bomo osredotočili na kubične Cayleyjeve grafe. Če je Cayleyjev graf $Cay(G, S)$ kubični graf, po definiciji 1.2.13 in 1.2.15 vemo, da je red množice S enak $|S| = 3$ in velja $S = S^{-1}$. Zato se množica S sestoji iz enega elementa reda dva, enega elementa reda več kot dva in njegovega inverza ali pa iz treh elementov reda dva.

Torej imamo tri možnosti:

i) $S = \{a, x, x^{-1}\}$, kjer je a involucija in x 5-cikel,

ii) $S = \{a, x, x^{-1}\}$, kjer je a involucija in x 3-cikel,

iii) $S = \{a, b, c\}$, kjer je $a^2 = b^2 = c^2 = id$.

Sedaj, ko smo ugotovili kakšne oblike je lahko množica S, pregledamo katere od teh možnosti nam porodijo Cayleyjev graf.

Brez škode za splošnost lahko predpostavimo, da je $a = (12)(34)(5)$ (sicer preštevilčimo elemente množice I_5).

i) Naj bo $S = \{(12)(34), x, x^{-1}\}$, kjer je element x 5-cikel.

Za vsak 5-cikel y v A_5 pogledamo, ali involucija a normalizira grupo $\langle y \rangle$ generirano z y, ki je podgrupa grupe A_5. Če je $\langle y \rangle^a = \langle y \rangle$, potem je $\langle y \rangle \triangleleft \langle a, y \rangle$ in zato po trditvi 1.1.12 in izreku 1.1.34 sledi, da je $\langle a, y \rangle$ prava podgrupa grupe A_5.

Torej, da bi dobili povezan Cayleyjev graf moramo izbrati tak 5-cikel y, da velja $\langle y \rangle^a \neq \langle y \rangle$, saj le v tem primeru $\langle a, y \rangle$ generira celo grupo A_5 (glej trditev 1.1.49). Torej lahko predpostavimo, da je x tak 5-cikel, da $\langle x \rangle^a \neq \langle x \rangle$.

Sedaj pa poglejmo še produkte elementov ax. Ločimo tri podprimere:

a) Element ax je reda 2.

Če je ax reda 2, potem velja:

$$\begin{aligned}
(ax)^2 &= id \\
axax &= id \qquad | \, x^{-1} \text{ z desne} \\
axa &= x^{-1} \qquad (\text{ker } a^2 = id) \\
axa^{-1} &= x^{-1} \\
x^a &= x^{-1}.
\end{aligned}$$

Torej involucija a normalizira $\langle x \rangle$, kar je protislovje s prejšnim sklepom, da smo vzeli tak 5-cikel x, da $\langle x \rangle^a \neq \langle x \rangle$. Torej se ne more zgoditi, da bi bil element ax reda 2.

b) Element ax je reda 3.

Če preverimo vseh štiriindvajset 5-ciklov v A_5, ugotovimo, da je ax reda 3 natanko tedaj, ko x pripada naslednji množici 5-ciklov

$$\begin{aligned}
P = \{&(12345), (12435), (12534), (12543), \\
&(13452), (14352), (15432), (15342)\}
\end{aligned}$$

Še več, za vsak x iz množice P, po trditvi 1.1.49, $\langle a, x\rangle$ dejansko generira celo grupo A_5. Pripadajoči Cayleyjevi grafi so vsi izomorfni grafu na sliki 2.1.

c) Element ax je reda 5.

Če preverimo vseh štiriindvajset 5-ciklov v A_5 ugotovimo, da je ax reda 5 natanko tedaj, ko x pripada naslednji množici 5-ciklov

$$\begin{aligned} P &= \{(13245), (13254), (13524), (14235), \\ &\quad (14253), (14523), (15423), (15324)\}. \end{aligned}$$

Še več, za vsak x iz množice P, $\langle a, x\rangle$ dejansko generira celo grupo A_5. Pripadajoči Cayleyjevi grafi so vsi izomorfni grafu na sliki 2.2.

ii) Naj bo $S = \{(12)(34), x, x^{-1}\}$, kjer je element x 3-cikel,

Kot pri primeru i) preverimo za vsak 3-cikel y v alternirajoči grupi A_5 ali involucija a normalizira podgrupo $\langle y\rangle$ grupe A_5 generirano z izbranim 3-ciklom. Če je $\langle y\rangle^a = \langle y\rangle$, potem je $\langle y\rangle \triangleleft \langle a, y\rangle$ in zato po trditvi 1.1.12 in izreku 1.1.34 $\langle a, y\rangle$ prava podgrupa grupe A_5. Torej lahko predpostavimo, da je x tak 3-cikel, da $\langle x\rangle^a \neq \langle x\rangle$.

Sedaj pa poglejmo še produkte elementov ax. Ločimo tri podprimere:

a) Element ax je reda 2.

Po enakem razmisleku kot v primeru i) pridemo do sklepa, da se ne more zgoditi, da bi bil element ax reda 2.

b) Element ax je reda 3.

Po trditvi 1.1.48 vemo, da je $\langle a, x\rangle$ izomorfna alternirajoči grupi A_4. Torej $S = \{a, x\}$ ne generira grupe A_5.

c) Element ax je reda 5.

Če preverimo vseh dvajset 3-ciklov v A_5, ugotovimo, da je ax reda 5 natanko tedaj, ko x pripada naslednji množici 3-ciklov

$$P = \{(135), (153), (145), (154), (235), (253), (245), (254)\}.$$

Še več, za vsak x iz množice P, po trditvi 1.1.49, grupa $\langle a, x\rangle$ generira celo alternirajočo grupo A_5. Pripadajoči Cayleyjevi grafi so vsi izomorfni grafu na sliki 2.3.

iii) Primer, ko je $S = \{(12)(34), b, c\}$, kjer je element $a^2 = b^2 = c^2 = id$.

Vemo, da če noben par $\{x, y\} \subseteq \{a, b, c\}$ ne generira tranzitivne grupe na množici $\{1, 2, 3, 4, 5\}$, potem $\{a, b, c\}$ po trditvi 1.1.47, zagotovo ne generira alternirajoče grupe A_5. Torej lahko predpostavimo, da vsaj en par $\{x, y\}$ involucij iz $\{a, b, c\}$ generira tranzitivno grupo na $\{1, 2, 3, 4, 5\}$, recimo, da je to par $\{a, b\}$. Potem lahko brez škode za splošnost s preštevilčevanjem elementov iz grupe A_5 dosežemo, da je $a = (12)(34)(5)$ in $b = (15)(23)(4)$. Prepričajmo se še, da a in b res generirata tranzitivno grupo na $\{1, 2, 3, 4, 5\}$.

$$
\begin{aligned}
a &= (12)(34)(5) \quad b = (15)(23)(4) \quad ab = (13425) \quad (ab)^2 = (14532) \\
ba &= (15243) \quad (ba)^2 = (12354).
\end{aligned}
$$

$$
\begin{array}{llll}
1^a = 2 & 1^b = 5 & 1^{ab} = 3 & 1^{(ab)^2} = 4 \\
2^a = 1 & 2^b = 3 & 2^{ab} = 4 & 2^{(ab)^2} = 5 \\
3^a = 1 & 3^b = 2 & 3^{ab} = 4 & 3^{(ab)^2} = 5 \\
4^a = 1 & 4^b = 2 & 4^{ab} = 3 & 4^{(ab)^2} = 5 \\
5^a = 1 & 5^b = 2 & 5^{ab} = 3 & 5^{(ab)^2} = 4.
\end{array}
$$

Sedaj je potrebno še pogledati vse možnosti za tretjo involucijo iz množice S. Ker se v involucijah a in b elementi 1 in 3 ter 4 in 5 pojavljajo simetrično, zadostuje pogledati involucije c, ki fiksirajo 1,2 ali 3. Torej je potrebno pogledati 9 možnosti in za vsak izbor sklepati, ali $\{a, b, c\}$ generira alternirajočo grupo A_5 ali ne. Na primer če za elementa a in b iz alternirajoče grupe A_5 vzamemo $a = (12)(34)(5)$ in $b = (15)(23)(4)$, potem a fiksira 5 in b fiksira 4. Torej moramo najti še elemente, ki fiksirajo 1, 2 in 3. Do tega pridemo tako, da ročno izračunamo vse produkte z novo nastalimi elementi in to ponavlajamo dokler ne dobimo vseh 3-ciklov alternirajoče grupe A_5, saj če dobimo vse 3-cikle iz grupe A_5 , po trditvi 1.1.31 sledi, da S generira grupo A_5. Dobljene možnosti za tretjo involucijo so sledeče: (23)(45), (25)(34), (14)(35), (15)(34), (12)(35), (13)(25).

Vsaka od teh involucij skupaj z involucijama $(12)(34)(5), (15)(23)(4)$ porodi Cayleyjev graf. Pripadajoči grafi so predstavljeni na slikah 2.4, 2.5, 2.6, 2.7, 2.8, 2.9.

Rezultate tega poglavja lahko združimo v naslednjo trditev.

Trditev 2.1.1. *Do izomorfizma natančno obstaja devet kubičnih Cayleyjevih grafov alternirajoče grupe A_5. To so:*

- $Cay(A_5, \{(12)(34)(5), (12345), (15432)\})$,
- $Cay(A_5, \{(12)(34)(5), (135), (153)\})$,
- $Cay(A_5, \{(13)(24)(5), (13245), (15423)\})$,
- $Cay(A_5, \{(12)(34)(5), (15)(23)(4), (23)(45)(1)\})$,

- $Cay(A_5, \{(12)(34)(5), (15)(23)(4), (25)(34)(1)\})$,
- $Cay(A_5, \{(12)(34)(5), (15)(23)(4), (14)(35)(2)\})$,
- $Cay(A_5, \{(12)(34)(5), (15)(23)(4), (15)(34)(2)\})$,
- $Cay(A_5, \{(12)(34)(5), (15)(23)(4), (12)(35)(4)\})$,
- $Cay(A_5, \{(12)(34)(5), (15)(23)(4), (13)(25)(4)\})$.

2.2 Hamiltonski cikli v kubičnih Cayleyjevih grafih alternirajoče grupe A_5

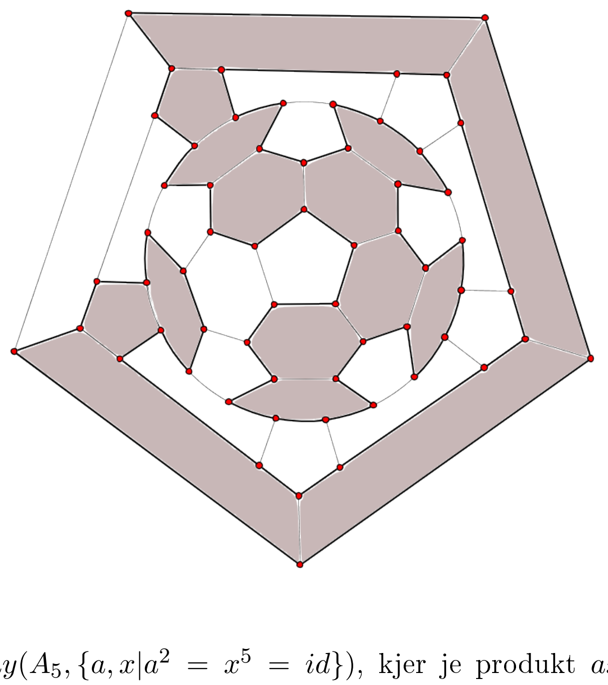
Kot smo omenili v uvodu, je cilj našega raziskovanja najti hamiltonske cikle v kubičnih Cayleyjevih grafih alternirajoče grupe A_5.

V tem poglavju bomo pokazali, da prav vseh devet grafov iz trditve 2.1.1 vsebuje hamiltonski cikel. Do takega cikla lahko pridemo na več načinov. Ena izmed metod, ki se izkaže za uporabno, je metoda, ki sloni na vložitvi grafov na ploskve: poiščemo hamiltonsko drevo lic, to je, drevo lic, katerega rob je hamiltonski cikel grafa Γ [22]. Ker niso vsi grafi planarni, bomo na vseh preostalih grafih poiskali hamiltonske cikle brez uporabe kakršne koli metode.

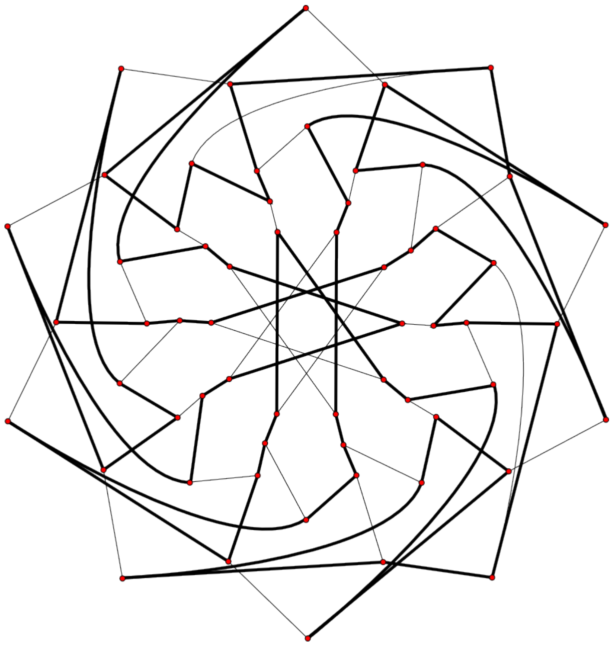
Izrek 2.2.1. *Vsak povezan kubični Cayleyjev graf alternirajoče grupe A_5 ima hamiltonski cikel.*

Dokaz. Po trditvi 2.1.1 obstaja devet neizomorfnih kubičnih grafov alternirajoče grupe A_5. Prikazani so na slikah 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9. Na vsaki sliki je prikazan tudi hamiltonski cikel. □

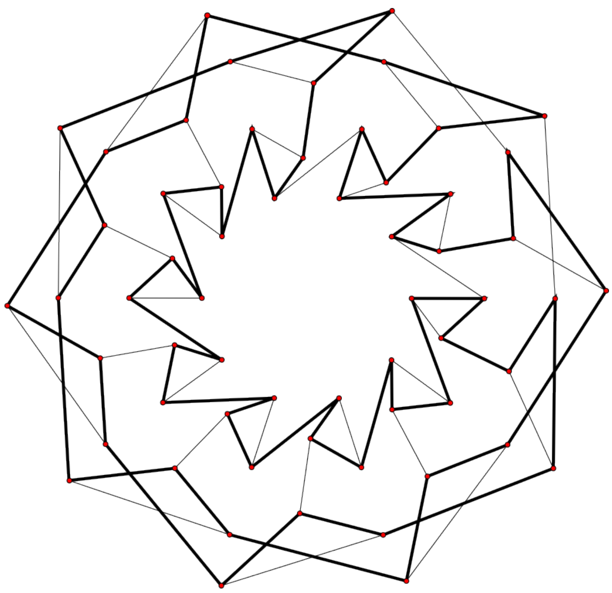
Primer 2.2.2. *Na Cayleyjevem grafu $Cay(A_5, \{a, x | a^2 = x^5 = id\})$ bolj znanem kot nogometna žoga, je predstavljen način, kako se uporablja zgoraj omenjena metoda iskanja hamiltonskih ciklov.*



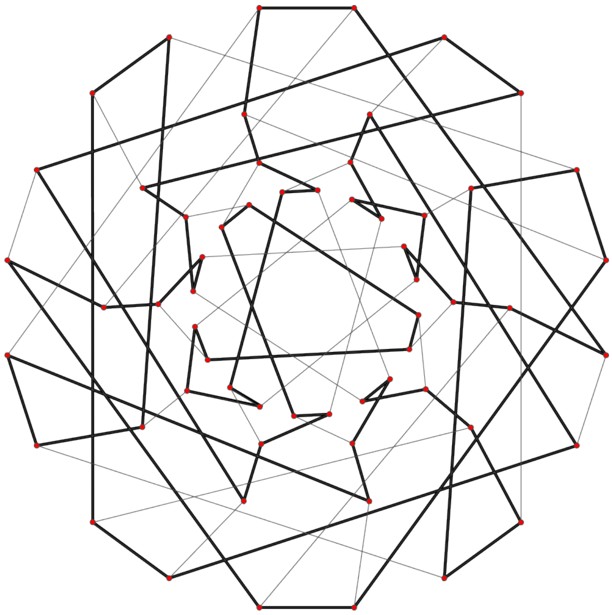
Slika 2.1: $Cay(A_5, \{a, x | a^2 = x^5 = id\})$, kjer je produkt ax 3-cikel, ima hamiltonski cikel.



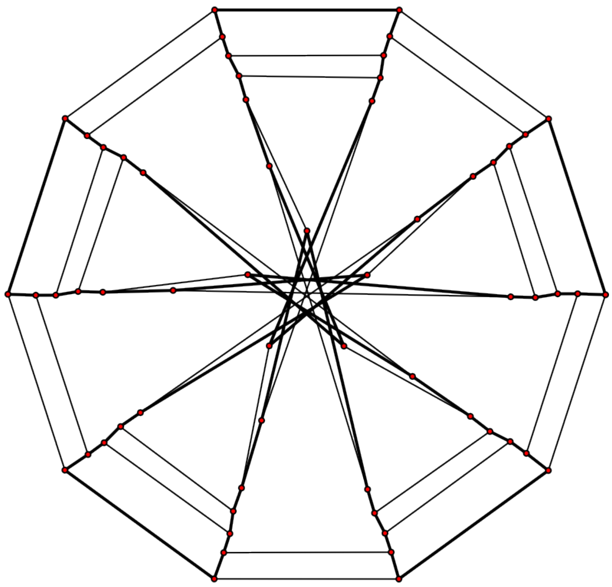
Slika 2.2: $Cay(A_5, \{a, x | a^2 = x^5 = id\})$, kjer je produkt ax 5-cikel, ima hamiltonski cikel.



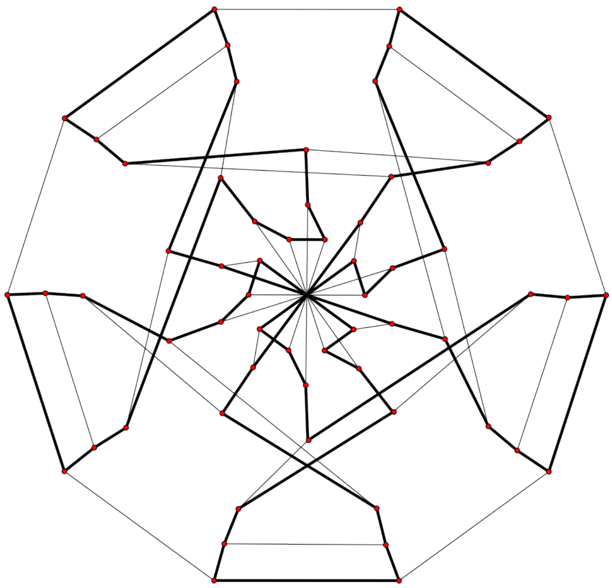
Slika 2.3: $Cay(A_5, \{a, x | a^2 = x^3 = id\})$, kjer je produkt ax 5-cikel, ima hamiltonski cikel.



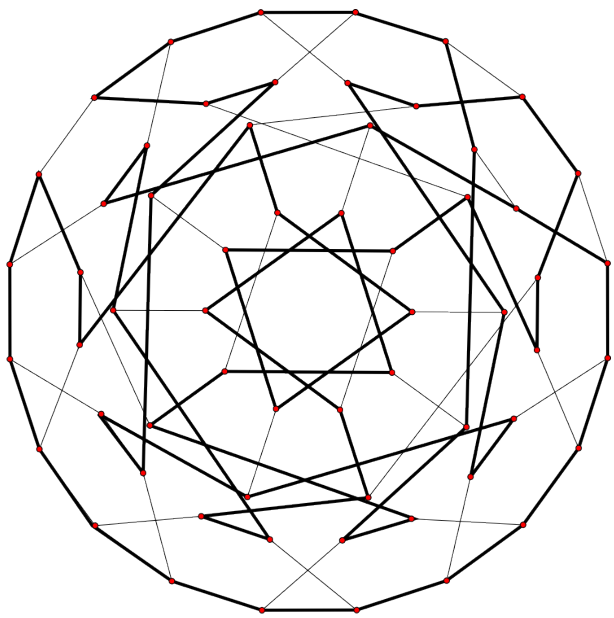
Slika 2.4: $Cay(A_5, \{(12)(34)(5), (15)(23)(4), (23)(45)(1)\})$ ima hamiltonski cikel.



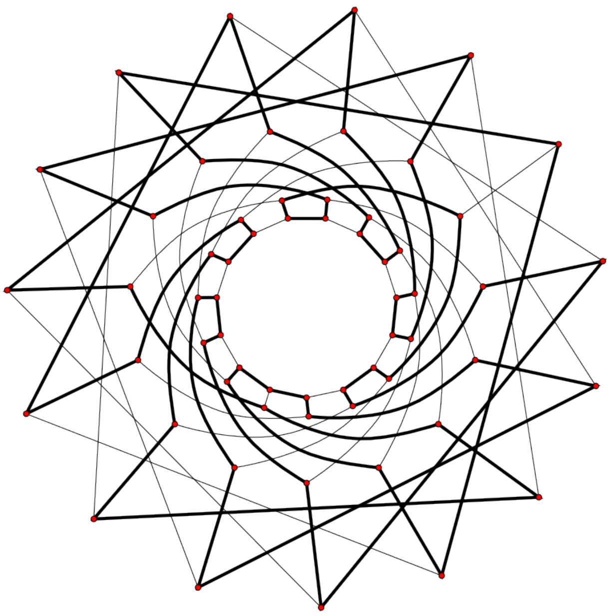
Slika 2.5: $Cay(A_5, \{(12)(34)(5), (15)(23)(4), (12)(35)(4)\})$ ima hamiltonski cikel.



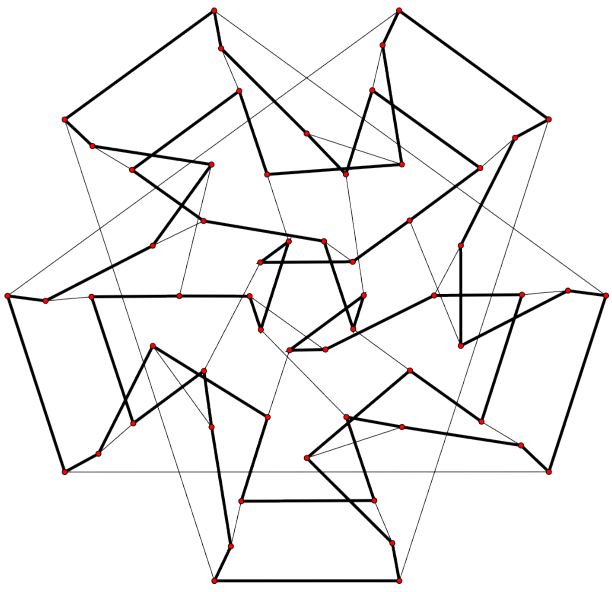
Slika 2.6: $Cay(A_5, \{(12)(34)(5), (15)(23)(4), (13)(25)(4)\})$ ima hamiltonski cikel.



Slika 2.7: $Cay(A_5, \{(12)(34)(5), (15)(23)(4), (15)(34)(2)\})$ ima hamiltonski cikel.



Slika 2.8: $Cay(A_5, \{(12)(34)(5), (15)(23)(4), (14)(35)(2)\})$ ima hamiltonski cikel.



Slika 2.9: $Cay(A_5, \{(12)(34)(5), (15)(23)(4), (25)(34)(1)\})$ ima hamiltonski cikel.

Poglavje 3

Cayleyjevi grafi in hamiltonski cikli

Leta 1969 je Lovászovo vprašanje [34] povzročilo val zanimanja med raziskovalci in od takrat naprej se intenzivno raziskuje na tem področju algebraične teorije grafov. Danes vemo, da vsi znani povezani točkovno tranzitivni grafi imajo hamiltonsko pot. Oziroma, znani so le štirje povezani točkovno tranzitivni grafi (z vsaj tremi točkami), ki nimajo hamiltonskega cikla.

Ker so Cayleyjevi grafi poseben primer točkovno tranzitivnih grafov [25] in ker znani točkovno tranzitvni grafi brez hamiltonskega cikla (Petersenov, Coxeterjev in grafa dobljena s trisekcijo teh dveh) niso Cayleyjevi, se je postavila domneva, da ima vsak povezan Cayleyjev graf na več kot dveh točkah hamiltonski cikel. Ta problem je spodbudil kar nekaj matematičnega zanimanja, postavile so se domneve in protidomneve glede njegove resničnosti. Zato bomo to poglavje namenili temu, da navedemo nekaj pomembnih rezultatov, ki kažejo na resničnost te domneve.

Izrek 3.0.1. *(Holsztyński in Strube [27]) V vsakem povezanem Cayleyjevem grafu abelove grupe obstaja hamiltonski cikel.*

Izrek 3.0.2. *(Witte [45]) Vsak povezan Cayleyjev graf p-grupe ima hamiltonski cikel.*

Izrek 3.0.3. *(Alspach in Zhang [10]) Vsak povezan kubični Cayleyjev graf diederske grupe premore hamiltonski cikel.*

Izrek 3.0.4. *(Keating in Witte [29]) Naj bo N komutatorska podgrupa grupe G. Če je podgrupa N ciklična grupa praštevilskega reda, potem vsak povezan Cayleyjev graf grupe G premore hamiltonski cikel.*

Rezultate izreka 3.0.4 so kasneje posplošili tudi na točkovno tranzitivne grafe in sicer velja, da če je graf povezan in točkovno tranzitiven in premore podgrupo grupe automorfizmov s ciklično komutatorsko podgrupo reda praštevilske potence, potem premore hamiltonski cikel. V kolikor graf ni Petersenov graf [18].

Izrek 3.0.5. *(Pak in Radoičić [41]) Vsak povezan Cayleyjev graf $Cay(G,S)$, kjer je $S = \{a, b, a^b\}$ in je a involucija, premore hamiltonski cikel.*

Izrek 3.0.6. *(Cherkassoff in Sjerve [16]) Vsak povezan kubični Cayleyjev graf $Cay(G,S)$, kjer množica $S = \{a, b, c\}$ sestoji iz treh involucije a,b in c in velja $ab = ba$, premore hamiltonski cikel.*

Izrek 3.0.7. *(Glover in Marušič [24]) Vsak povezan kubični Cayleyjev graf $Cay(G,S)$, kjer je $S = \{a, x, x^{-1}\}$, $a^2 = id$, $x^s = id$ in $(ax)^3 = id$, premore hamiltonsko pot.*

Izrek 3.0.8. *(Kutnar, Marušič, Morris, Šparl [32]) Vsak povezan Cayleyjev graf $Cay(G,S)$ grupe, katere red ima majhno praštevilsko faktorizacijo, premore hamiltonski cikel.*

Rezultati iz [32] skupaj z drugimi rezultati na tem področju povedo naslednje. Naj bodo p, q, r različna si praštevila, potem ima vsak povezan Cayleyjev graf reda :

- kp, kjer $24 \neq k < 32$,
- kpq, kjer $k \leq 5$,
- pqr,
- kp^2, kjer je $k \leq 2$,

hamiltonski cikel.

In poleg tega ti rezultati dokažejo še obstoj hamiltonskih ciklov v vseh povezanih Cayleyjevih grafih reda $n < 120$ za $n \notin \{48, 72, 80, 96, 108, 112\}$.

Zaključek

V zaključni projektni nalogi smo raziskovali kubične Cayleyjeve grafe alternirajoče grupe A_5.

V prvem poglavju smo spoznali potrebne definicije, trditve in izreke, ki smo jih potrebovali za razumevanje poglavij, ki so sledili. Le-te so se nanašale na grupe, grafe ter medsebojno delovanje.

V drugem poglavju smo poiskali vse neizomorfne kubične Cayleyjeve grafe alternirajoče grupe A_5. Pri izračunih smo si pomagali s programom MAGMA.

V drugem podpoglavju, pa smo dokazali temeljno trditev projektne naloge, da vsak kubični Cayleyjevi graf alternirajoče grupe A_5 premore hamiltonski cikel.

Za konec, smo v tretjem poglavju predstavili nekaj pomembnejših rezultatov, ki kažejo na resničnost domneve, da ima vsak povezan Cayleyjev graf hamiltonski cikel.

Literatura

[1] B. Alspach, Hamiltonian cycles in vertex-transitive graphs of order $2p$, Proceedings of the Tenth Southeastern Conference on Combinatorics, Graph Theory and Computing (Florida Atlantic Univ., Boca Raton, Fla., 1979), pp. 131-139, Congress. Numer., XXIII-XX, Utilitas Math., Winnipeg, Man., 1979.

[2] B. Alspach, The classification of hamiltonian generalized Petersen graphs, J. Combin. Theory Ser. B 34 (1983), 293-312.

[3] B. Alspach, Lifting Hamilton cycles of quotient graphs, Discrete Math. 78 (1989), 25-36.

[4] B. Alspach, Hamilton cycles in metacirculant graphs with prime power cardinal blocks, Graph theory in memory of G. A. Dirac (Sandbjerg, 1985), 7-16, Ann. Discrete Math. 41, North-Holland, Amsterdam, 1989.

[5] B. Alspach, C. C. Chen and K. McAvaney, On a class of Hamiltonian laceable 3-regular graphs, Discrete Math. 151 (1996), 19-38.

[6] B. Alspach , E. Durnberger and B. Parsons, Hamilton cycles in metacirculant graphs with prime cardinality blocks, Cycles in graphs (Burnaby, B.C., 1982), 27-34, Ann. Discrete Math. 27, North-Holland, Amsterdam, 1985.

[7] B. Alspach, S. Locke and D. Witte, The Hamilton spaces of Cayley graphs on abelian groups, Discrete Math. 82 (1990), 113-126.

[8] B. Alspach and B. Parsons, On Hamiltonian cycles in metacirculant graphs, Algebraic and geometric combinatorics, $1-7$, Ann. Discrete Math. 15 (1982), North-Holland, Amsterdam, 1982.

[9] B. Alspach and Y. S. Qin, Hamilton-connected Cayley graphs on Hamiltonian groups, Europ. J. Combin. 22 (2001), 777-787.

[10] B. Alspach and C. Q. Zhang, Hamilton cycles in cubic Cayley graphs on dihedral groups, Ars Combin. 28 (1989), 101-108.

[11] L. Babai, Problem 17, Unsolved problems, in: Summer Research Workshop in Algebraic Combinatorics, Simon Fraser University, July, 1979.

[12] L. Babai, Long cycles in vertex-transitive graphs, J. Graph Theory 3 (1979), 301-304.

[13] L. Babai, Automorphism Groups, Isomorphism, Reconstruction, in: R.L. Graham, M. Grotschel, L. Lovász (Eds.), Handbook of Combinatorics, North-Holland, 1995, pp. 1447-1540 (Chapter 27).

[14] J.-C. Bermond, Hamiltonian graphs, in: L.W. Beinke, R.J. Wilson (Eds.), Selected Topics in Graph Theory, Academic Press, London, 1978, pp. 127-167.

[15] N. Biggs, Three remarkable graphs, Can. J. Math. 25 (1973), 397-411.

[16] Guido Mislin (editor), The Hilton Symposium 1993, Topics in Topology and Group Theory, On Groups Generated by three involution, two of which commute, 169-186.

[17] Y. Q. Chen, On Hamiltonicity of vertex-transitive graphs and digraphs of order p^4, J. Combin. Theory Ser. B 72 (1998), 110-121.

[18] E. Dobson, H. Gavlas, J. Morris and D. Witte, Automorphism groups with cyclic commutator subgroup and Hamilton cycles, Discrete Math. 189 (1998), 69-78.

[19] D.S. Dummit and R. M. Foote, Abstract algebra, 3th edition (2004), 886-888.

[20] E. Durnberger, Connected Cayley graphs of semi-direct products of cyclic groups of prime order by abelian groups are hamiltonian, Discrete Math. 46 (1983), 55-68.

[21] J. B. Fraleigh, A first course in abstract algebra, Addison-Wesley, 7th edition (2002), 93-94.

[22] H.H. Glover, K. Kutnar and D. Marušič, Hamiltonicity of cubic Cayley graphs: the $(2, 4k, 3)$ case, J. Algebraic Combin. 30(2009), 447-475.

[23] H. H. Glover and T. Y. Yang, A Hamilton cycle in the Cayley graph of the $(2, p, 3)$-presentation of $PSl_2(p)$, Discrete Math. 160 (1996), 149-163.

[24] H.H. Glover and D. Marušič, Hamiltonicity of cubic Cayley graphs, 2005

[25] C. D. Godsil and G. Royle, Algebraic graph theory, Springer Verlag (New York), 2001.

[26] R. J. Gould and R. L. Roth, A recursive algorithm for Hamiltonian cycles in the $(1, j, n)$-Cayley graph of the alternating group, Graph theory with applications to algorithms and computer science (Kalamazoo, Mich., 1984), 351-369, Wiley-Intersci. Publ., Wiley, New York, 1985.

[27] W. Holsztyński and R.F.E. Strube, Paths and circuits in finite groups, Discrete Math. 22 (1978), 263-272.

[28] S. Lang, Algebra, Revised Third Edition Department of Mathematics Yale University (2005), 19-20.

[29] K. Keating and D. Witte, On Hamilton cycles in Cayley graphs in groups with cyclic commutator subgroup. Cycles in graphs (Burnaby, B.C., 1982), 89-102, Ann. Discrete Math. 27, North-Holland, Amsterdam, 1985.

[30] K. Kutnar, A. Malnič, D. Marušič in P. Šparl, Uvod v teorijo grup, 4. oktober 2009.

[31] K. Kutnar and D. Marušič, Hamiltonicity of vertex-transitive graphs of order $4p$, Europ. J. Combin. 29 (2008), 423-438.

[32] K. Kutnar, D. Marušič, D.W. Morris, J. Morris, P. Šparl, Hamiltonian cycles in Cayley graphs whose order has few prime factors, Combinatorics, Combin., 2011.

[33] K. Kutnar and P. Šparl, Hamilton cycles and paths in vertex-transitive graphs of order $6p$, Discrete Math. 309 (2009), 5491-5500.

[34] L. Lovász, Combinatorial structures and their applications, in: Proc. Calgary Internat. Conf. Calgary, Alberta, 1969, Gordon and Breach, New York, 1970, pp. 243-246, Problem 11.

[35] D. Marušič, Hamilonian circuits in Cayley graphs, Discrete Math. 46 (1983), 49-54.

[36] D. Marušič, Vertex transitive graphs and digraphs of order p^k. Cycles in graphs (Burnaby, B.C., 1982), 115-128, Ann. Discrete Math. 27, North-Holland, Amsterdam, 1985.

[37] D. Marušič, Hamiltonian cycles in vertex symmetric graphs of order $2p^2$, Discrete Math. 66 (1987), 169-174.

[38] D. Marušič, On vertex-transitive graphs of order qp, J. Combin. Math. Combin. Comput. 4 (1988), 97-114.

[39] D. Marušič and T. D. Parsons, Hamiltonian paths in vertex-symmetric graphs of order $5p$, Discrete Math. 42 (1982), 227-242.

[40] D. Marušič and T. D. Parsons, Hamiltonian paths in vertex-symmetric graphs of order $4p$, Discrete Math. 43 (1983), 91-96.

[41] I. Pak and R. Radoičić, Hamiltonian Paths in Cayley graphs , Discrete Math., Volume 309, 6 September 2009, 5501-5508.

[42] C. Thomassen, Tilings of the torus and the Klein bottle and vertex-transitive graphs on a fixed surface, Trans. Amer. Math. Soc. 323 (1991), 605-635.

[43] D. Witte, On Hamiltonian circuits in Cayley diagrams, Discrete Math. 38 (1982), 99-108.

[44] D. Witte, On Hamilton cycles in Cayley graphs in groups with cyclic commutator subgroup, Discrete Math. 27 (1985), 89-102.

[45] D. Witte, Cayley digraphs of prime-power order are Hamiltonian, J. Combin. Theory Ser. B 40 (1986), 107-112.