Tampereen yliopisto

Juuso Huhtivuo

CAYLEYN GRAAFIEN 1-FAKTOROINNISTA

Informaatioteknologian ja viestinnän tiedekunta
Pro gradu -tutkielma
Helmikuu 2024

Tiivistelmä

Juuso Huhtivuo: Cayleyn graafien 1-faktoroinnista
Pro gradu -tutkielma
Tampereen yliopisto
Matematiikan maisteriohjelma
Helmikuu 2024

Tässä pro gradu -tutkielmassa käsitellään Cayleyn graafeja ja niihin liittyvää avointa 1-faktorointikonjektuuria. Cayleyn graafit ovat graafeja, jotka havainnollistavat algebrallisten ryhmien rakennetta suhteessa johonkin ryhmän virittävään joukkoon. Cayleyn graafien 1-faktorointikonjektuurin mukaan parillisen kertaluvun ryhmän Cayleyn graafi voidaan virittävästä joukosta riippumatta 1-faktoroida eli jakaa 1-säännöllisiin, virittäviin ja särmien osalta pareittain erillisiin aligraafeihin.

Tutkielman ensimmäisessä varsinaisessa luvussa käsitellään yleisesti graafiteoriaa ja määritellään graafiteorian keskeisimmät käsitteet. Vastaavasti luvussa 3 käsitellään ryhmäteorian perusteita, kuten permutaatioita, ryhmiä, erilaisia aliryhmiä, ryhmien välisiä tuloja, symmetriaryhmiä sekä edellisiin liittyviä lauseita. Graafiteoriaa käsittelevästä luvusta 2 poiketen luvun 3 jälkimmäisellä puolikkaalla käsitellään monia sellaisia määritelmiä ja tuloksia, jotka eivät usein sisälly suoraan yliopiston maisteritason opetukseen, kuten Sylowin lauseita, nilpotentteja ryhmiä ja puolisuoria tuloja. Molempien lukujen sisältöä havainnollistetaan esimerkeillä.

Lukujen 2 ja 3 valmistelevat tarkastelut mahdollistavat Cayleyn graafien käsittelyn luvussa 4. Siinä todistetaan, että jokainen äärellisesti virittyvä ryhmä on isomorfinen yhtenäisen, suuntaamattoman ja paikallisesti äärellisen graafin symmetriaryhmän aliryhmän kanssa. Tämän jälkeen määritellään kyseisessä lauseessa esitetyn konstruktion pohjalta Cayleyn graafit ja käsitellään niiden vaihtoehtoisia määritelmiä, ominaisuuksia ja solmutransitiivisuutta, ja annetaan esimerkkejä.

Tutkielman 5. luku keskittyy Cayleyn graafien 1-faktorointikonjektuuriin. Luvussa määritellään konjektuurin esittämiseksi tarvittavat käsitteet, todistetaan eräissä konjektuurin osatulosten todistuksissa tarvittava Vizingin lause ja lopulta todistetaan konjektuuri Richard A. Stongin vuoden 1985 artikkeliin pohjautuen suurille perheille äärellisiä ryhmiä: ryhmille, joiden kertaluku on luvun 2 potenssi, Abelin ryhmille, diedriryhmille ja nilpotenteille ryhmille. Numeroituvasti äärettömien ryhmien osalta konjektuuri todistetaan äärettömästi virittyville ryhmille ja Abelin ryhmille. Viimeisessä luvussa esitetään yhteenveto tutkielman sisällöstä sekä pohditaan jatkotutkimusmahdollisuuksia.

Avainsanat: algebrallinen graafiteoria, Cayleyn graafi, virittävä joukko, 1-faktorointi

Sisällys

1 Johdanto

Algebrallinen graafiteoria on matematiikan osa-alue, jossa käytetään algebrallisia menetelmiä graafien tutkimuksessa ja yhdistetään graafeihin algebrallisia rakenteita. Eräs mielenkiintoinen algebrallisen graafiteorian tutkimuskohde on Cayleyn graafit, joiden tarkoitus on havainnollistaa ryhmiä – abstrakteja algebrallisia objekteja – geometrisesti graafeina. Yksi tapa tutkia Cayleyn graafeja, ja graafeja ylipäänsäkin, on tarkastella sitä, ovatko ne 1-faktoroituvia. 1-faktoroituvuus tarkoittaa graafin jakamista särmävieraisiin, 1-säännöllisiin virittäviin aligraafeihin.

1-faktoroituvuus on graafiteoreetikoille erityinen mielenkiinnon kohde, koska se kertoo paljon graafin rakenteesta. 1-faktoroituvuutta alettiin tiettävästi tutkia ensimmäisen kerran 1800-luvulla. Vertailukohtana mainittakoon, että graafiteoria itsessäänkin on suhteellisen nuori matematiikan osa-alue ja sai varsinaisesti alkunsa vasta 1700-luvulla. Vuonna 1859 M. Reiss osoitti, että graafi K_{2n} on 1-faktoroitavissa. Sen jälkeen 1-faktorointiin liittyen on todistettu monia mielenkiintoisia tuloksia. D. Köning osoitti vuonna 1931, että kaksijakoinen graafi on 1-faktoroitavissa, jos ja vain jos se on säännöllinen. Graafiteoriaa laajalti ja tuotteliaasti 1900-luvun lopulta alkaen tutkinut B. Alspach puolestaan osoitti vuonna 1982, että viivagraafi $L(K_n)$ on 1-faktoroitavissa, jos ja vain jos $n \equiv 0 \bmod 4$ tai $n \equiv 1 \bmod 4$. Lisäksi kuuluisa neliväriluause on ekvivalentti sen kanssa, että tietyntyyppiset graafit ovat 1-faktoroituvia. [19]

Cayleyn graafien ohella tämän tutkielman keskiössä on Cayleyn graafien 1-faktorointikonjektuuri, jonka mukaan mikä tahansa parillisen kertaluvun ryhmän Cayleyn graafi on 1-faktoroituva virittävästä joukosta riippumatta. Yleisesti ottaen matematiikassa konjektuuriksi kutsutaan sellaista väitettä, jonka arvellaan olevan tosi mutta jota ei ole pystytty ainakaan kokonaan todistamaan oikeaksi tai vääräksi. Graafiteoriassa tunnetaan myös muita 1-faktorointiin liittyviä konjektuureja, mutta tämän tutkielman puitteissa Cayleyn graafien 1-faktorointikonjektuurilla tarkoitetaan nimenomaan edellä määriteltyä konjektuuria.

1-faktorointikonjektuurin ensimmäiset osatulokset todistettiin tiettävästi vuonna 1980, kun G. Stern ja H. Lenz [22] todistivat konjektuurin parillisen kertaluvun syklisten ryhmien Cayleyn graafeille. Viisi vuotta myöhemmin vuonna 1985 Richard Stong [23] ilmeisesti Sternistä ja Lenzistä tietämättä todisti, että isot perheet Cayleyn graafeja – kertalukua 2^k, $k \in \mathbb{Z}_+$, olevien ryhmien, Abelin ryhmien, diedriryhmien sekä minimaalisilla virittävillä joukoilla myös mm. nilpotenttien ryhmien Cayleyn graafit – ovat 1-faktoroituvia, ja saavutti näin ollen Sternin ja Lenzin tulokseen verrattuna vahvempia tuloksia. 2000-luvulla Stongin työtä on suoraan jatkanut mm. Stongin nilpotentteihin ryhmiin liittynyttä todistusta yleistänyt Alireza Abdollahi [1].

Tutkielman näkökulmana aiheeseen ovat nimenomaan Stongin artikkelin tulokset, koska kyseinen artikkeli on myöhemmän 1-faktorointikonjektuurin tutkimuksen kulmakivi ja avasi konjektuurin tutkimusta huomattavasti: useissa myöhemmin julkaistuissa aiheeseen liittyvissä tutkimuksissa viitataan Stongin artikkeliin. Näkökulman valintaa perustelee lisäksi se, että ainakin yhteen Stongin tulokseen on olemassa

yleistys (Abdollahin [1] todistama tulos), jota tutkielmassa myös käsitellään.

1-faktorointikonjektuuria käsitellään tutkielman luvussa 5. Sitä ennen tarkasteluja pohjustetaan käymällä läpi graafiteoriasta ja ryhmäteorista tarvittavia esitietoja luvuissa 2 ja 3. Koska Stongin artikkelin lähestymistapa on hyvin ryhmäteoreettinen ja artikkeli kokonaisuudessaan on ilmaisultaan ja merkinnöiltään varsin vaikeaselkoinen ja tiivis, on luku 3 huomattavasti lukua 2 laajempi, ja siinä käsitellään myös sellaisia ryhmäteorian määritelmiä ja tuloksia, joihin ei usein yliopiston syventävilläkään kursseilla tutustuta. Myös koko tutkielman näkökulma on näistä seikoista johtuen painottunut ryhmäteoriaan. Toisaalta luku 4, jossa käsitellään Cayleyn graafeja yleisesti, on luonteeltaan hieman enemmän graafiteoreettinen.

Lukijalta edellytetään yliopiston kandidaatintutkinnon mukaisia esitietoja mm. kuvauksista ja joukoista. Varsinaisesti graafi- ja ryhmäteoriasta ei tarvita esitietoja, koska niitä käsitellään suhteellisen laajasti tutkielman ensimmäisellä puoliskolla, ja määritelmiä myös pyritään havainnollistamaan selventämällä intuitiota ja antamalla esimerkkejä määritelmien yksipuolisen esittämisen sijaan. Kaikki käytettävät määritelmät ja tulokset on pyritty kirjoittamaan eksplisiittisesti esille. Todistukset sen sijaan pääsääntöisesti sivuutetaan luvuissa 2 ja 3.

Luvun 2 päälähteenä on käytetty Reinhard Diestelin kirjaa [7]. Kyseinen teos on hieman vaikea ja sopii parhaiten sellaisille lukijoille, jotka tuntevat graafiteoriaa jo valmiiksi jonkin verran. Graafiteorian perusteisiin tutustumiseen oivallinen teos on Riikka Kangaslammen, Pertti Koiviston ja Riitta Niemistön opetusmoniste [14]. Luku 3 puolestaan pohjautuu Joseph J. Rotmanin kirjaan [20], jota voi suositella kaikille ryhmäteoriasta kiinnostuneille esitiedoista riippumatta. Luku 4 on koostettu useasta eri lähteestä, joista merkittävimpiä ovat John Meierin [17] ja Norman Biggsin [3] kirjat. Luvussa 5 puolestaan on hyödynnetty Stongin [23] ja Abdollahin [1] artikkelien ohella Dieter Jungnickelin kirjaa [13].

2 Graafiteoriaa

Tässä luvussa määritellään graafiteorian peruskäsitteet ja annetaan erityisesti vaikeimmista käsitteistä esimerkkejä. Esitys ei ole millään muotoa kattava graafiteorian perusteiden läpikäynti, vaan käsittely on rajattu vain niihin käsitteisiin, joita tullaan tarvitsemaan luvuissa 4 ja 5.

Koska graafiteorian merkinnöistä ja terminologiasta ei ole varsinkaan suomen kielellä isolta osin tieteellisessä yhteisössä konsensusta, on tärkeää sitoa tutkielman merkinnät ja määritelmät mahdollisimman perusteellisesti. Esimerkiksi jo graafin käsitteellekin on olemassa lukuisia keskenään vaihtoehtoisia ja ei-ekvivalentteja määritelmiä. Tästä syystä liikkeelle lähdetään itse graafin määritelmästä, josta edetään graafin ja solmun asteeseen, graafihomomorfismeihin ja -isomorfismeihin, graafien mahdollisiin ominaisuuksiin, erilaisiin aligraafeihin ja lopulta graafien välisiin tuloihin.

Luvun esitysjärjestys vastaa pääpiirteissään alan oppikirjallisuutta ja opetusmonisteita. Matemaattinen sisältö pohjautuu Diestelin kirjaan [7] lukuun ottamatta graafien välisten tulojen määritelmiä, jotka ovat peräisin Richard Hammackin ym. kirjasta [9]. Notaatioita on muutettu jonkin verran lähdemateriaalissa käytetyistä, jotta ne olisivat yhtenäisiä Stongin artikkelin [23] merkintöjen kanssa.

2.1 Graafiteorian peruskäsitteitä

Graafi määritellään tässä tutkielmassa kahden joukon (solmujoukon ja särmäjoukon) järjestettynä parina.

Määritelmä 2.1 (Graafi)**.** Graafi on järjestetty pari $\mathcal{G} = (V, E)$, jossa $V \neq \emptyset$, $E \subseteq \{\{u, v\} \mid u, v \in V\}$ ja $V \cap E = \emptyset$. Joukon V alkioita kutsutaan *solmuiksi* ja joukon E alkioita *särmiksi*. Vastaavasti joukkoa V itsessään kutsutaan *solmujoukoksi* ja joukkoa E *särmäjoukoksi*.

Muutama huomio edellä esitetystä määritelmästä on paikallaan. Ensinnäkin määritelmä ei rajoita solmu- tai särmäjoukon kokoa mitenkään, eli kyseiset joukot voivat olla numeroituvia tai ylinumeroituvia. Tässä tutkielmassa käsitellään kuitenkin vain sellaisia graafeja, joiden solmujoukko on numeroituva. Solmujoukon numeroituvuudesta seuraa, että myös särmäjoukko on numeroituva.

Toisaalta määritelmä 2.1 mahdollistaa sen, että jollakin graafin $\mathcal{G} = (V, E)$ solmulla $v \in V$ on voimassa $\{v, v\} \in E$, eli että graafissa $\mathcal{G}$ on silmukoita. Jos silmukoita ei ole, graafia kutsutaan *yksinkertaiseksi graafiksi* [17]. Useimmat tässä tutkielmassa käsiteltävät graafit ovat yksinkertaisia.

Graafin määritelmässä asetettiin hieman epätavanomaiselta vaikuttava ehto $V \cap E = \emptyset$. Tämä ehto ei kuitenkaan ole kriittinen. Olennaisesti ehto tarkoittaa sitä, että graafin särmät eivät voi olla myös solmuja eikä niihin voida viitata samoilla symboleilla, eli särmät ja solmut ovat aidosti erilaisia matemaattisia objekteja. Tämän rajoitteen tarkoitus on yksinkertaistaa tulevia tarkasteluja sekä selkeyttää intuitiota.

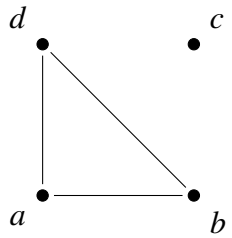
Määritelmän 2.1 mukaiset graafit ovat suuntaamattomia graafeja, joissa särmät ovat siis järjestämättömiä pareja. Vaihtoehtoisesti olisi voitu määritellä suunnattu graafi, jossa särmät ovat järjestettyjä solmupareja. Monesti graafit määritellään nimenomaan suunnattuina, koska suuntaamaton graafi voidaan sitten hyvin intuitiivisella tavalla määritellä suunnatun graafin erityistapauksena. Tässä tutkielmassa päädyttiin kuitenkin edellä kuvattuun ratkaisuun lähdemateriaalissa, erityisesti Diestelin kirjassa ja Stongin artikkelissa, tehtyjen valintojen vuoksi. Suunnattuun graafiin palataan luvun loppupuolella määritelmässä 2.25.

Graafi voidaan esittää geometrisesti piirtämällä piste jokaista solmua kohden ja viiva solmujen välille jokaista särmää kohden. Graafin muulla rakenteella kuin solmujen ja särmien nimillä ja solmujen välisillä suhteilla, eli särmien sijainneilla, ei kuitenkaan ole merkitystä, eli solmu- ja särmäjoukko määrittelevät graafin täysin. Täten ei ole merkitystä esimerkiksi sillä, mihin sijainteihin solmut piirretään, vaan ainoastaan sillä, että ne nimetään oikein ja että oikeiden solmujen välillä on särmä. Muutkin piirtotekniset yksityiskohdat ovat sinänsä epärelevantteja. Esimerkissä 2.2 havainnollistetaan tässä tutkielmassa käytettävää notaatiota.

Esimerkki 2.2. Kuvassa 2.1 on esitetty graafi

$$\mathcal{G} = (\{a, b, c, d\}, \{\{a, b\}, \{b, d\}, \{a, d\}\}),$$

jonka solmujoukko on $\{a, b, c, d\}$ ja särmäjoukko $\{\{a, b\}, \{b, d\}, \{a, d\}\}$.



Kuva 2.1. Graafi $\mathcal{G} = (\{a, b, c, d\}, \{\{a, b\}, \{b, d\}, \{a, d\}\})$.

Graafiteorian todistuksissa tarkastellaan usein mielivaltaista graafin solmua ja sen suhteita muihin solmuihin. On siis hyödyllistä ottaa käyttöön solmuun liittyvän särmän käsite.

Määritelmä 2.3 (Solmuun liittyvä särmä)**.** Särmä e liittyy solmuun v, jos $v \in e$.

Solmuun liittyvän särmän käsite antaa luonnollisella tavalla pohjan naapurisolmun käsitteelle.

Määritelmä 2.4 (Särmän päätesolmut ja solmun naapurisolmu)**.** Olkoon $\mathcal{G} = (V, E)$ graafi, $v_1, v_2 \in V$ ja $e \in E$. Jos $v_1 \in e, v_2 \in e$ ja $v_1 \neq v_2$, sanotaan, että solmut v_1 ja v_2 ovat särmän e päätesolmut. Lisäksi sanotaan, että solmut v_1 ja v_2 ovat naapurisolmuja. Mikäli solmut eivät ole naapurisolmuja, ne ovat *itsenäisiä* suhteessa toisiinsa.

Särmien osalta naapuruutta vastaava käsite on vierekkäisyys: kaksi eri särmää ovat vierekkäisiä, mikäli niillä on sama päätesolmu, ja itsenäisiä suhteessa toisiinsa, mikäli ne eivät ole vierekkäisiä.

Monesti on kiinnostavaa tai hyödyllistä tarkastella sitä, kuinka monta särmää solmuun liittyy. Seuraavat käsitteet tarjoavat formaalin tavan tehdä tällaisia tarkasteluja.

Määritelmä 2.5 (Graafin ja solmun aste)**.** Graafin $\mathcal{G} = (V, E)$ aste $|\mathcal{G}|$ on sen solmujen lukumäärä, eli $|\mathcal{G}| = |V|$. Graafin $\mathcal{G}$ solmun v aste $d_{\mathcal{G}}(v)$ on sen naapurisolmujen lukumäärä. Solmun v asteelle käytetään myös notaatiota $d(v)$, jos sekaannuksen vaaraa ei ole.

Määritelmä 2.6 (Graafin solmujen minimiaste ja maksimiaste)**.** Olkoon $\mathcal{G} = (V, E)$ graafi. Graafin $\mathcal{G}$ solmujen

1. minimiaste $\delta(\mathcal{G}) \coloneqq \min\{d(v) \mid v \in V\}$,
2. maksimiaste $\Delta(\mathcal{G}) \coloneqq \max\{d(v) \mid v \in V\}$.

Graafeille voidaan määritellä yhdiste, leikkaus ja erotus hyvin luonnollisella tavalla, koska graafit ovat kahden joukon järjestettyjä pareja. Myös graafien homomorfismit ja isomorfismit määritellään samaan tapaan kuin esimerkiksi ryhmäteoriassa.

Määritelmä 2.7 (Graafien yhdiste, leikkaus ja joukko-opillinen erotus)**.** Olkoot $\mathcal{G}_1 = (V_1, E_1)$ ja $\mathcal{G}_2 = (V_2, E_2)$ graafeja. Tällöin

$$\begin{aligned}\mathcal{G}_1 \cup \mathcal{G}_2 &= (V_1 \cup V_2, E_1 \cup E_2),\\ \mathcal{G}_1 \cap \mathcal{G}_2 &= (V_1 \cap V_2, E_1 \cap E_2) \text{ ja}\\ \mathcal{G}_1 \setminus \mathcal{G}_2 &= (V_1 \setminus V_2, E_1 \setminus E_2).\end{aligned}$$

Määritelmä 2.8 (Graafihomomorfismi ja -isomorfismi)**.** Olkoot $\mathcal{G}_1 = (V_1, E_1)$ ja $\mathcal{G}_2 = (V_2, E_2)$ graafeja (eivät välttämättä eri graafeja). Kuvaus $\varphi\colon V_1 \to V_2$ on graafihomomorfismi graafilta $\mathcal{G}_1$ graafille $\mathcal{G}_2$, jos se säilyttää solmujen naapuruuden, eli $\{\varphi(x), \varphi(y)\} \in E_2$, jos $\{x, y\} \in E_1$. Mikäli kuvaus φ on bijektio ja sen käänteiskuvaus on graafihomomorfismi, sanotaan, että kuvaus φ on graafi-isomorfismi. Tällöin sanotaan lisäksi, että graafit $\mathcal{G}_1$ ja $\mathcal{G}_2$ ovat isomorfiset, mitä merkitään $\mathcal{G}_1 \cong \mathcal{G}_2$.

Graafien välisten kuvausten yhteydessä on luontevaa puhua särmän $\{v_1, v_2\}$ kuvasta kuvauksessa f, vaikka f on graafien solmujoukkojen välinen kuvaus. Tällöin tarkoitetaan siis särmää $\{f(v_1), f(v_2)\}$. Vastaavasti voidaan puhua särmän $\{u_1, u_2\}$ alkukuvasta, mikäli solmuilla u_1 ja u_2 on alkukuvat.

Määritelmä 2.9 (Graafin symmetria)**.** Graafin $\mathcal{G}$ automorfismia eli isomorfismia $\varphi\colon \mathcal{G} \to \mathcal{G}$ kutsutaan graafin symmetriaksi.

Kuten yleensäkin matematiikassa, graafien isomorfisuus tarkoittaa, että graafit ovat solmujen ja särmien nimiä vaille samat. Yleensä ei ole merkityksellistä, ovatko graafit identtiset vai isomorfiset.

2.2 Graafien ominaisuuksia

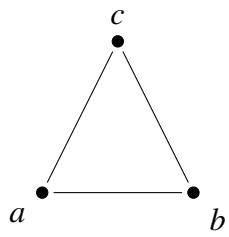
Tässä alaluvussa esitellään luettelomaisesti graafien tavanomaisia ominaisuuksia.

Määritelmä 2.10 (Triviaali graafi)**.** Jos graafin aste on 1 eikä siinä ole silmukkaa, graafia kutsutaan triviaaliksi graafiksi.

Huomautus. Triviaali graafi muodostaa usein graafin asteen mukaan etenevissä induktiotodistuksissa perustapauksen.

Määritelmä 2.11 (k-säännöllisyys)**.** Graafi $\mathcal{G}$ on k-säännöllinen, jos sen jokaisen solmun aste on k.

Esimerkki 2.12. Kuvan 2.2 graafi $\mathcal{G} = (\{a, b, c\}, \{\{a, b\}, \{b, c\}, \{a, c\}\})$ on pienin yksinkertainen 2-säännöllinen graafi.



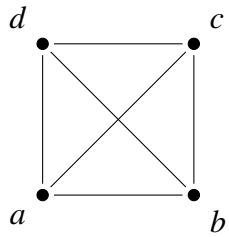
Kuva 2.2. Graafi $\mathcal{G} = (\{a, b, c\}, \{\{a, b\}, \{b, c\}, \{a, c\}\})$.

Määritelmä 2.13 (k-täydellisyys)**.** Yksinkertainen graafi $\mathcal{G} = (V, E)$ on k-täydellinen, mikäli $|V| = k$ ja kaikki solmut ovat pareittain naapureita keskenään, eli kaikilla $v_1, v_2 \in V, v_1 \neq v_2$, on voimassa $\{v_1, v_2\} \in E$.

Esimerkki 2.14. Kuvan 2.3 graafi

$$\mathcal{G} = (\{a, b, c, d\}, \{\{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}\})$$

on 3-säännöllinen ja 4-täydellinen.



Kuva 2.3. Graafi $\mathcal{G} = (\{a, b, c, d\}, \{\{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}\})$.

Graafit voivat olla selvällä tavalla äärellisiä tai äärettömiä solmujen lukumäärän mukaan. Äärettömätkin graafit voivat kuitenkin olla paikallisesti äärellisiä:

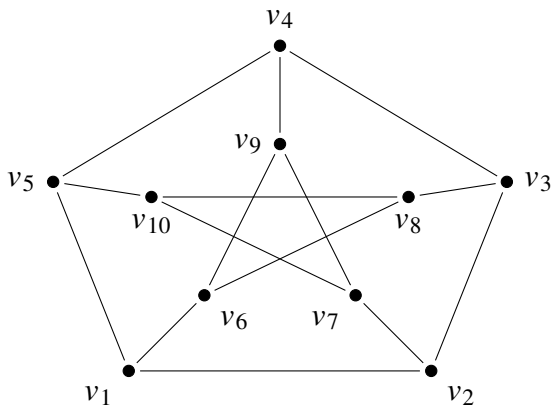
Määritelmä 2.15 (Paikallinen äärellisyys)**.** Graafi on paikallisesti äärellinen, jos sen jokaisen solmun aste on äärellinen.

Huomautus. Jos graafi ei ole paikallisesti äärellinen, se ei tietysti voi olla äärellinenkään.

Seuraavaksi esiteltävä solmutransitiivisuuden käsite lienee tämän luvun hankalimpia käsitteitä, ja sitä onkin erityisen perusteltua havainnollistaa esimerkillä.

Määritelmä 2.16 (Solmutransitiivisuus)**.** Graafi $\mathcal{G} = (V, E)$ on solmutransitiivinen, jos mille tahansa solmuille $v, w \in V$ on olemassa sellainen graafin $\mathcal{G}$ automorfismi α, että $\alpha(v) = w$.

Esimerkki 2.17 (Petersenin graafi)**.** Klassinen esimerkki solmutransitiivisesta graafista on kuvassa 2.4 esitetty Petersenin graafi.



Kuva 2.4. Petersenin graafi.

Täsmällinen Petersenin graafin solmutransitiivisuuden todistus sivuutetaan, sillä se vaatii ryhmäteoreettisia käsitteitä, joita ei tässä tutkielmassa vielä ole määritelty. Esimerkinomaisesti todettakoon, että vaikkapa solmuille v_1 ja v_2 solmutransitiivisuuden määritelmän mukaiseksi automorfismiksi kelpaa kuvaus α, jolla $\alpha(v_i) = v_{i+1}$, kun $i \in \{1, 2, 3, 4, 6, 7, 8, 9\}$, ja $\alpha(v_5) = v_1, \alpha(v_{10}) = v_6$. Kyseinen kuvaus vastaa intuitiivisesti graafin kiertämistä vastapäivään.

2.3 Aligraafit

Tämän alaluvun aiheena ovat erilaiset aligraafit. Samaan tapaan kuin yleensäkin matematiikassa, aligraafeja voidaan muodostaa mielivaltaisista graafeista tiettyjen ehtojen perusteella, ja niillä on täten mielivaltaisiin graafeihin verrattuna poikkeuksellisen mielenkiintoisia ominaisuuksia. Ensimmäisenä on tarpeen määritellä yleinen aligraafin käsite.

Määritelmä 2.18 (Aligraafi ja aito aligraafi)**.** Graafi $\mathcal{G}' = (V', E')$ on graafin $\mathcal{G} = (V, E)$ aligraafi, mitä merkitään $\mathcal{G}' \subseteq \mathcal{G}$, jos $V' \subseteq V$ ja $E' \subseteq E$. Mikäli $\mathcal{G}'$ on graafin $\mathcal{G}$ aligraafi ja $\mathcal{G}' \neq \mathcal{G}$, sanotaan, että graafi $\mathcal{G}'$ on graafin $\mathcal{G}$ aito aligraafi.

Virittävät ja indusoidut aligraafit ovat aligraafien erityistapauksia.

Määritelmä 2.19 (Virittävä aligraafi)**.** Graafi $\mathcal{G}' = (V', E')$ on graafin $\mathcal{G} = (V, E)$ virittävä aligraafi, jos $\mathcal{G}' \subseteq \mathcal{G}$ ja $V' = V$.

Intuitiivisesti virittävä aligraafi on siis aligraafi, joka sisältää kaikki alkuperäisen graafin solmut mutta ei välttämättä kaikkia särmiä.

Määritelmä 2.20 (Indusoitu aligraafi)**.** Olkoon $\mathcal{G} = (V, E)$ graafi ja $\mathcal{G}' = (V', E')$ sen aligraafi. Jos kaikilla $\{x, y\} \in E$ on voimassa $\{x, y\} \in E'$, kun $x, y \in V'$, niin sanotaan, että graafi $\mathcal{G}'$ on graafin $\mathcal{G}$ indusoitu aligraafi ja että solmujoukko V' indusoi aligraafin $\mathcal{G}'$ graafissa $\mathcal{G}$.

Indusoitu aligraafi ei siis välttämättä sisällä kaikkia alkuperäisen graafin solmuja virittävän aligraafin tapaan, mutta sen sijaan säilyttää alkuperäisen graafin rakenteen eli sisältämiensä solmujen yhteydet.

Määritelmä 2.21 (Polku)**.** Polku on graafi $P = (V, E)$, jolle

$$V = \{v_0, v_1, \ldots, v_k\} \text{ ja } E = \{\{v_0, v_1\}, \{v_1, v_2\}, \ldots, \{v_{k-1}, v_k\}\},$$

missä kaikki solmut $v_i, i \in \{0, \ldots, k\}$ ovat eri solmuja mahdollisesti päätesolmuja lukuun ottamatta. Sanotaan, että polku P yhdistää solmuja v_0 ja v_k.

Määritelmä 2.22 (Polun pituus)**.** Olkoon $P = (V, E)$ polku. Polun pituus on sen sisältämien särmien lukumäärä eli $|E|$.

Polun käsite vastaa varsin tarkasti intuitiivista käsitystä polusta määritelmän teknisyydestä huolimatta. On kuitenkin huomattava, että graafiteoreettinen polku sisältää vain polun muodostamiseen osallistuvat särmät ja solmut. Mikäli jollakin graafilla on aligraafinaan polku, sanotaan, että graafi sisältää polun.

Polun käsite mahdollistaa edelleen syklin käsitteen määrittelyn. Sykli on polku, jossa alku- ja päätesolmun välillä on särmä.

Määritelmä 2.23 (Sykli)**.** Sykli C on polku (V, E), jolle on voimassa

$$V = \{v_0, v_1, \ldots, v_k\} \text{ ja } E = \{\{v_0, v_1\}, \ldots, \{v_k, v_0\}\},$$

missä $k \geq 2$.

Polun käsitteen avulla voidaan määritellä vielä eräs keskeinen graafien ominaisuus, nimittäin yhtenäisyys. Myös yhtenäisyyden käsitteen eksakti määritelmä vastaa varsin tarkasti käsitteestä syntyvää intuitiivista mielikuvaa.

Määritelmä 2.24 (Yhtenäisyys)**.** Graafi $\mathcal{G} = (V, E)$ on yhtenäinen, jos mille tahansa solmuille $v_1, v_2 \in V, v_1 \neq v_2$ voidaan muodostaa polku P siten, että P yhdistää solmuja v_1 ja v_2.

Viimeisenä määritellään suunnattu graafi, jota käsiteltiin epämuodollisesti jo alaluvussa 2.1. Tässä tutkielmassa suunnattuja graafeja ei myöhemmin juuri tarvita, joten asia jätetään pitkälti kuriositeetin tasolle.

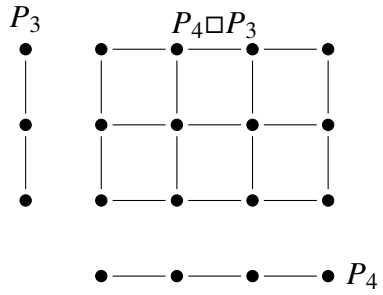
Määritelmä 2.25 (Suunnattu graafi)**.** Suunnattu graafi $\mathcal{G}$ on graafi (V, E), missä joukkoihin V ja E liittyy kaksi kuvausta, init: $E \to V$ ja ter: $E \to V$, jotka liittävät jokaiseen graafin särmään e alkusolmun $\text{init}(e)$ ja päätesolmun $\text{ter}(e)$.

2.4 Graafien tuloja

Tässä alaluvussa käsitellään erilaisia graafien välisiä tuloja, joilla muodostetaan kahdesta graafista uusi graafi. On olemassa lukuisia graafien välisiä ”laskutoimituksia”, mutta tässä alaluvussa määritellään loppututkielman kannalta relevanteimmat eli karteesinen ja suora tulo. Graafien tuloja ei välttämättä aina käsitellä graafiteorian peruskursseilla tai kaikissa alan oppikirjoissakaan, joten aihe saattaa olla graafiteoriaan vain pintapuolisesti tutustuneille ennestään tuntematon. Muista luvun 2 alaluvuista poiketen tämä alaluku pohjautuu Richard Hammackin ym. kirjaan [9], koska Diestelin kirjassa [7] graafien tuloja ei käsitellä. Huomautettakoon sekaannusten välttämiseksi, että tässä tutkielmassa merkinnällä $A \times B$, missä A ja B ovat algebrallisten alkioiden tai solmujen joukkoja, tarkoitetaan joukkojen A ja B tavanomaista karteesista tuloa.

Määritelmä 2.26 (Graafien karteesinen tulo)**.** Graafien $\mathcal{G} = (V_\mathcal{G}, E_\mathcal{G})$ ja $\mathcal{H} = (V_\mathcal{H}, E_\mathcal{H})$ karteesinen tulo $\mathcal{G}\square\mathcal{H}$ on graafi, jonka solmujoukko on $V_\mathcal{G} \times V_\mathcal{H}$ ja jossa kahden solmun $(g, h), (g', h') \in V_\mathcal{G} \times V_\mathcal{H}$ välillä on särmä täsmälleen silloin, kun $g = g'$ ja $\{h, h'\} \in E_\mathcal{H}$ tai kun $\{g, g'\} \in E_\mathcal{G}$ ja $h = h'$.

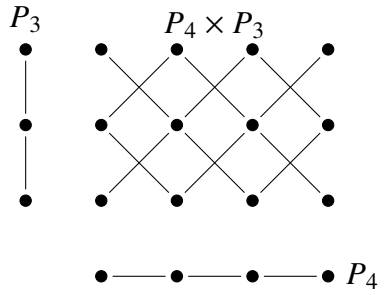
Esimerkki 2.27. Kuvassa 2.5 on esitetty polkugraafien P_4 ja P_3 karteesinen tulo $P_4\square P_3$. Polkugraafi P_n on polku, jossa on n solmua. Koska solmujen nimet ovat tässä esimerkissä yhdentekeviä, ei niitä ole piirretty näkyviin.



Kuva 2.5. Karteesinen tulo $P_4\square P_3$.

Määritelmä 2.28 (Graafien suora tulo)**.** Graafien $\mathcal{G} = (V_\mathcal{G}, E_\mathcal{G})$ ja $\mathcal{H} = (V_\mathcal{H}, E_\mathcal{H})$ suora tulo $\mathcal{G} \times \mathcal{H}$ on graafi, jonka solmujoukko on $V_\mathcal{G} \times V_\mathcal{H}$ ja jossa kahden solmun $(g, h), (g', h') \in V_\mathcal{G} \times V_\mathcal{H}$ välillä on särmä täsmälleen silloin, kun $\{g, g'\} \in E_\mathcal{G}$ ja $\{h, h'\} \in E_\mathcal{H}$.

Esimerkki 2.29. Kuvassa on esitetty polkugraafien P_4 ja P_3 suora tulo $P_4 \times P_3$.



Kuva 2.6. Suora tulo $P_4 \times P_3$.

Huomautus. Kirjallisuudessa suoraa tuloa kutsutaan toisinaan muiden muassa tensorituloksi, ristituloksi, kategoriseksi tuloksi tai hämäävästi jopa karteesiseksi tuloksi. Eri kirjoittajat käyttävät myös graafien eri tuloille keskenään ristiriitaisia merkintöjä ja merkitsevät esimerkiksi karteesista tuloa symbolilla $\times$, mikä saattaa sekoittua joukko-opilliseen karteesiseen tuloon, ellei käsitteitä ole eksplisiittisesti määritelty. Esimerkiksi Stong käyttää artikkelinsa [23] Lemman 2.1 todistuksessa graafien karteesiselle tulolle merkintää $\times$.

3 Ryhmäteoriaa

Luvun tavoitteena on käydä läpi ryhmäteoreettisia määritelmiä ja tuloksia, jotka pohjustavat Cayleyn graafien käsittelyä ja niihin liittyvien algebrallisen graafiteorian todistusten kirjoittamista luvuissa 4 ja 5. Ensin käsitellään ryhmäteorian ja kombinatoriikan perusteita – muun muassa permutaatioita, ryhmiä ja aliryhmiä – minkä jälkeen käsitellään ryhmien virittämistä, Lagrangen lausetta, tekijäryhmiä, Sylowin 1. lausetta, nilpotentteja ryhmiä ja ryhmien tuloja. Lopulta määritellään symmetriaryhmät, jotka luovat yhteyden graafi- ja ryhmäteorian välille ja ovat erityisesti luvussa 4 keskeisiä.

Edellisestä luvusta 2 poiketen tämä luku sisältää määritelmien ohella suuren määrän lauseita ja seurauksia. Todistukset kuitenkin sivuutetaan, koska useimmat tulokset esitellään yliopisto-opetuksessa. Lisäksi lukija pystyy tarkistamaan todistukset lähdekirjallisuudesta lauseiden yhteyteen lisättyjen viitteiden avulla. Erityisesti vaikeimpien määritelmien ja lauseiden kohdalla pyritään myös antamaan esimerkkejä sekä selostetaan intuitiota, mutta tämä on jouduttu jättämään varsin vähälle tutkielman laajuuden rajaustarpeen vuoksi.

Merkinnät ja määritelmät ovat pääosin standardinmukaisia, sillä ryhmäteoriassa merkinnät ja terminologia ovat vakiintuneet varsin hyvin. Matemaattinen sisältö on merkittävissä määrin peräisin Rotmanin kirjasta [20], joka on muodostunut erääksi alan merkkiteokseksi ja auktoriteetiksi. Poikkeavat lähteet on merkitty määritelmien ja todistusten yhteyteen. Osa esimerkeistä on lisäksi kirjoittajan omia.

3.1 Permutaatiot

Permutaatioita esitellään varsin laajasti, koska ensinnäkin niitä tarvitaan luvun 4 todistuksissa ja toiseksi permutaatioiden avulla saadaan muodostettua erinomaisia esimerkkejä Cayleyn graafeista.

Määritelmä 3.1 (Permutaatio ja joukon permutaatioiden joukko)**.** Olkoon X epätyhjä joukko. Joukon X permutaatio α on bijektio $\alpha\colon X \to X$. Joukon X kaikkien permutaatioiden joukkoa merkitään S_X.

Joukon X permutaatiot määritellään toisinaan joukon X alkioiden uudelleenjärjestämisenä. Tämä lähestymistapa oli käytössä erityisesti 1700- ja 1800-luvuilla, jolloin kuuluisa matemaatikko Joseph-Louis Lagrange kehitti permutaatiot [20]. Permutaatioiden määritteleminen alkioiden uudelleenjärjestämisenä on yhtäpitävää bijektiivisyyteen perustuvan määritelmän kanssa, ja tämä lähestymistapa saattaa myös helpottaa asian intuitiivista hahmottamista. Määritelmien yhteys muuttuu ilmeiseksi seuraavan esimerkin myötä.

Esimerkki 3.2 (Permutaatioiden matriisinotaatio)**.** Joukon $X = \{1, 2, 3\}$ eräs permutaatio on bijektio $\alpha\colon X \to X$, jolla $\alpha(1) = 3, \alpha(2) = 2$ ja $\alpha(3) = 1$. Tätä merkitään matriisimuodossa $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$. Joukon X muut permutaatiot ovat $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$,

$\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$, $\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$, $\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$ ja $\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$.

Esimerkki 3.3 (Permutaatioiden yhdistäminen)**.** Permutaatioiden yhdistäminen tarkoittaa yhdistetyn kuvauksen muodostamista permutaatioista. Olkoot $\alpha = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$ ja $\beta = \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$ joukon $\{1, 2, 3\}$ permutaatioita. Tällöin permutaatioiden α ja β yhdistetty permutaatio $\alpha\beta = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$, koska

$$\begin{aligned}\alpha\beta(1) &= \alpha(\beta(1)) = \alpha(3) = 1,\\ \alpha\beta(2) &= \alpha(\beta(2)) = \alpha(2) = 3 \text{ ja}\\ \alpha\beta(3) &= \alpha(\beta(3)) = \alpha(1) = 2.\end{aligned}$$

Määritellään sitten syklin käsite. Intuition tasolla sykli on sellainen permutaatio, joka uudelleenjärjestää joukon alkiot siirtämällä osaa niistä, kaikkia saman verran. Täsmällistä määritelmää varten täytyy ensin määritellä permutaation kiinnittämä ja siirtämä alkio.

Määritelmä 3.4 (Permutaation kiinnittämä ja siirtämä alkio)**.** Olkoon X jokin joukko, $x \in X$ ja $\alpha \in S_X$. Permutaatio α *kiinnittää* alkion x, jos $\alpha(x) = x$, ja *siirtää* alkiota x, jos $\alpha(x) \neq x$.

Määritelmä 3.5 (r-sykli ja sen pituus)**.** Olkoon X jokin joukko, ja olkoot $i_1, i_2, \ldots, i_r$ kyseisen joukon alkioita. Olkoon lisäksi $\alpha \in S_X$. Jos α kiinnittää kaikki alkiot $x \in X$, jotka eivät ole mitään alkioita $i_k, k \in \{1, \ldots, r\}$, ja

$$\alpha(i_1) = i_2, \ldots, \alpha(i_{r-1}) = i_r, \alpha(i_r) = i_1,$$

sanotaan, että permutaatio α on r-sykli. Lisäksi sanotaan, että r-syklin pituus on r.

Määritelmä 3.6 (Transpositio)**.** 2-sykliä, joka siis vaihtaa kahden alkion paikkaa, kutsutaan transpositioksi.

Syklit esitetään normaalista permutaationotaatiosta poiketen yhdellä rivillä, siis muodossa $\alpha = (i_1 i_2 \ldots i_r)$, jossa $i_k, k \in \{1, \ldots, r\}$, ovat määritelmän 3.5 mukaisia alkioita.

Esimerkki 3.7 (4-sykli)**.** Permutaatio $\alpha = \begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 4 & 2 & 1\end{pmatrix}$ on 4-sykli $\alpha = (1324)$, koska $\alpha(1) = 3, \alpha(3) = 2, \alpha(2) = 4$ ja $\alpha(4) = 1$.

Edellisestä esimerkistä havaitaan erinomaisesti syklin nimen luonnollisuus. Syklejä voidaankin intuitiivisesti hahmotella siten, että sykliin kuuluvat alkiot on kiinnitetty ympyrän kehälle, ja ympyrää kierretään keskipisteensä ympäri.

Esimerkki 3.8. Esimerkissä 3.2 muodostettiin kaikki joukon $X = \{1, 2, 3\}$ permutaatiot. Syklinotaatiota käyttäen joukon S_X esitys voidaan lyhentää muotoon

$$S_X = \{(1), (23), (12), (123), (132), (13)\}.$$

Määritelmä 3.9 (Erilliset permutaatiot)**.** Olkoon X joukko. Joukon X permutaatiot $\alpha, \beta \in S_X$ ovat erilliset, jos permutaatio α siirtää vain sellaisia alkioita $x \in X$, jotka β kiinnittää, ja jos β siirtää vain sellaisia alkioita, jotka α kiinnittää. Permutaatioiden perhe $\alpha_1, \alpha_2, \ldots, \alpha_m$ on erillinen, jos mitkä tahansa kaksi perheen permutaatiota ovat erillisiä.

Esimerkissä 3.8 havaittiin, että kaikki joukon $X = \{1, 2, 3\}$ permutaatiot ovat itse asiassa syklejä. Herää kysymys, ovatko kaikki permutaatiot syklejä. Vastaus on osittain myönteinen:

Lause 3.10. *Olkoon X äärellinen joukko. Tällöin jokainen permutaatio $\alpha \in S_X$ on joko sykli tai erillisten syklien yhdistetty permutaatio.*

Todistus. Ks. [20], s. 6. □

Jos permutaatio ei ole sykli vaan erillisten syklien yhdistetty permutaatio, kutsutaan permutaation esittämistä syklien yhdistettynä funktiona permutaation *faktoroinniksi*.

Määritelmä 3.11 (Permutaation parillisuus ja parittomuus)**.** Permutaatio α on parillinen, jos se voidaan esittää sellaisena transpositioiden yhdistettynä funktiona, jossa yhdistetään parillinen määrä transpositioita. Muussa tapauksessa permutaatio on pariton.

3.2 Ryhmät

Tässä alaluvussa määritellään ryhmän käsite sekä siihen liittyviä muita ryhmäteorian keskeisiä peruskäsitteitä. Olennainen osa ryhmäteoriaa ovat binäärioperaatiot eli laskutoimitukset, jotka tulee määritellä ennen itse ryhmän käsitettä.

Määritelmä 3.12 (Binäärioperaatio)**.** Epätyhjän joukon G binäärioperaatio $*$ on kuvaus $*\colon G \times G \to G$.

Binäärioperaatio on siis kuvaus, joka liittää kahteen joukon alkioon kolmannen kyseisen joukon alkion. Binäärioperaatioilla voi olla erilaisia ominaisuuksia:

Määritelmä 3.13 (Binäärioperaation ominaisuuksia)**.** Olkoon $*$ epätyhjän joukon G binäärioperaatio. Binäärioperaatio $*$ on

- liitännäinen, jos kaikilla $a, b, c \in G$ on voimassa $(a * b) * c = a * (b * c)$,
- vaihdannainen, jos kaikilla $a, b \in G$ on voimassa $a * b = b * a$.

Ryhmä itsessään määritellään tässä tutkielmassa ryhmäteoriassa vakiintuneella tavalla.

Määritelmä 3.14 (Ryhmä)**.** Olkoon G epätyhjä joukko ja $*$ sen liitännäinen binäärioperaatio. Pari $(G, *)$ on ryhmä, jos on olemassa sellainen $e \in G$, että

- kaikilla $a \in G$ on voimassa $a * e = a = e * a$
- jokaisella $a \in G$ on olemassa sellainen $b \in G$, että $a * b = e = b * a$.

Edellisen määritelmän merkintöjä käyttäen joukkoa G kutsutaan ryhmän $(G, *)$ perusjoukoksi, alkiota e ryhmän neutraali- tai identiteettialkioksi ja alkiota b alkion a vasta- tai käänteisalkioksi. Yksilöivien nimien antaminen alkioille e ja b on mielekästä, sillä kyseiset alkiot ovat yksikäsitteisiä:

Lause 3.15. *Olkoon $(G, *)$ ryhmä. Tällöin on olemassa sellainen yksikäsitteinen $e \in G$, että $a * e = a = e * a$ kaikilla $a \in G$. Lisäksi jokaisella $a \in G$ on olemassa sellainen yksikäsitteinen $b \in G$, että $a * b = e = b * a$.*

Todistus. Ks. [20], s. 13. □

Huomautus. Neutraalialkiota merkitään usein symboleilla 0 tai 1 ja alkion a käänteisalkiota notaatiolla a^{-1}, ja näin toimitaan jatkossa myös tässä tutkielmassa. On kuitenkin huomattava, että nämä ovat puhtaasti merkintöjä, eivätkä viittaa yleisesti lukuihin 0 ja 1 tai reaalilukujen potenssiin.

Monesti määritelmissä ja lauseissa ryhmä samaistetaan perusjoukkoonsa ja liitännäinen binäärioperaatio $*$ jätetään määrittämättä. Tällöin binäärioperaation oletetaan olevan yhteydestä selvä, tai sen tarkemmalla määritelmällä ei ole merkitystä. Mikäli binäärioperaatiota ei erikseen määritellä, sitä kutsutaan *tuloksi*. Alkioiden a ja b tulolle käytetään yksinkertaisesti merkintää ab.

Tärkein ryhmän erityistapaus on Abelin ryhmä. Abelin ryhmässä binäärioperaatio on paitsi liitännäinen myös vaihdannainen.

Määritelmä 3.16 (Abelin ryhmä)**.** Ryhmä $(G, *)$ on Abelin ryhmä, mikäli binäärioperaatio $*$ on vaihdannainen.

Ryhmistä on helppo keksiä esimerkkejä. Tarkemmat todistukset sille, että esimerkeissä esitellyt rakenteet todella ovat ryhmiä, sivuutetaan, vaikkakin ne ovat hyvin suoraviivaisia.

Esimerkki 3.17. Joukko S_X, missä $X = \{1, 2, 3\}$, muodostaa kuvausten yhdistämisen kanssa ryhmän $(S_X, \circ)$, jonka neutraalialkio on identtinen permutaatio (1).

Esimerkki 3.18. Kokonaislukujen joukko $\mathbb{Z}$ yhdessä tavanomaisen kokonaislukujen yhteenlaskuoperaation + kanssa muodostaa ryhmän $(\mathbb{Z}, +)$, jonka neutraalialkio on 0. Lisäksi ryhmä $(\mathbb{Z}, +)$ on Abelin ryhmä.

Käänteisalkion erityisen mielenkiintoinen ominaisuus, jota monesti todistuksissakin tarvitaan, on se, että alkion a käänteisalkion käänteisalkio on alkio a itse. Ominaisuus seuraa suoraan käänteisalkion määritelmästä.

Seuraus 3.19. *Olkoon G ryhmä ja $a \in G$. Tällöin $(a^{-1})^{-1} = a$.*

Todistus. Ks. [20], s. 14. □

Määritellään seuraavaksi potenssi ryhmissä tuttuun tapaan, ja käsitellään sen jälkeen joitakin suoraan määritelmästä seuraavia potenssin ominaisuuksia. Sitä ennen huomautetaan, että tässä tutkielmassa $\mathbb{N} = \{0, 1, \dots\}$, eli luonnollisten lukujen joukko sisältää nollan.

Määritelmä 3.20 (Potenssi)**.** Olkoon G ryhmä, $a \in G$, e ryhmän G neutraalialkio ja $n \in \mathbb{N}$. Tällöin

- $a^0 = e$,
- $a^1 = a$,
- $a^{n+1} = aa^n$, kun $n \geq 1$ ja
- $a^{-n} = (a^{-1})^n$ kaikilla n.

Seuraus 3.21. *Olkoon $(G, *)$ ryhmä, $a \in G$ ja $n, m \in \mathbb{Z}_+$. Tällöin on voimassa $a^m * a^n = a^{m+n}$ ja $(a^m)^n = a^{mn}$.*

Todistus. Ks. [20], s. 12. □

Eräs tapa jaotella ryhmiä on ryhmän perusjoukon koon eli ryhmän kertaluvun mukaan. Ryhmät jaotellaan kertaluvun perusteella äärellisiin ja äärettömiin ryhmiin. Tässä luvussa ei lähtökohtaisesti tätä jaottelua oleteta, vaan ryhmät voivat olla äärellisiä tai äärettömiä, ellei muuta mainita. Kuitenkin myöhemmin luvussa 5 iso osa tarkastelusta toteutetaan vain äärellisille ryhmille.

Määritelmä 3.22 (Ryhmän kertaluku)**.** Ryhmän G kertaluku $|G|$ on ryhmän perusjoukon alkioiden lukumäärä.

Huomautus. Ryhmää, jonka kertaluku on yksi, kutsutaan *triviaaliksi ryhmäksi*.

Määritellään vielä ryhmähomomorfismit ja -isomorfismit eli ryhmien väliset ryhmän rakenteen säilyttävät kuvaukset, sekä homomorfismin ydin ja kuva.

Määritelmä 3.23 (Ryhmähomomorfismi ja -isomorfismi)**.** Olkoot $(G, *)$ ja $(H, \circ)$ ryhmiä. Kuvaus $f\colon G \to H$ on ryhmähomomorfismi, jos kaikilla $a, b \in G$ on voimassa

$$f(a * b) = f(a) \circ f(b).$$

Kuvaus f on ryhmäisomorfismi, jos se on ryhmähomomorfismi ja bijektio. Jos on olemassa ryhmäisomorfismi $f\colon G \to H$, sanotaan, että ryhmät G ja H ovat isomorfiset, ja merkitään $G \cong H$.

Määritelmä 3.24 (Homomorfismin ydin ja kuva)**.** Olkoon $f\colon G \to H$ ryhmähomomorfismi. Homomorfismin f

- ydin $\ker(f) = \{a \in G \mid f(a) = 1\}$,
- kuva $\operatorname{im}(f) = \{h \in H \mid f(a) = h \text{ jollakin } a \in G\}$.

3.3 Aliryhmät

Määritelmä 3.25 (Aliryhmä)**.** Olkoon $(G, *)$ ryhmä ja $S \subseteq G$. Tällöin $(S, *)$ on ryhmän $(G, *)$ aliryhmä, jos

- $S \neq \emptyset$,
- $s^{-1} \in S$ kaikilla $s \in S$,
- $st \in S$ kaikilla $s, t \in S$.

Sitä, että ryhmä S on ryhmän G aliryhmä, merkitään $S \leq G$. Jos on voimassa $S \leq G$ ja $S \neq G$, sanotaan, että S on ryhmän G *aito aliryhmä*, mitä merkitään $S < G$.

Toisinaan aliryhmän vaihtoehtoisena määritelmänä esitetään, että S on ryhmän G aliryhmä, jos $1 \in S$, missä 1 on ryhmän G neutraalialkio, ja

$$st^{-1} \in S \text{ kaikilla } s, t \in S.$$

Toisaalta kyseinen ehto voidaan johtaa määritelmästä 3.25.

Lause 3.26. *Kaikki aliryhmät ovat ryhmiä.*

Todistus. Ks. [20], s. 20. □

Esimerkki 3.27. Olkoon $f : G \to H$ ryhmähomomorfismi. Tällöin on voimassa

$$\ker(f) \leq G \text{ ja } \operatorname{im}(f) \leq H.$$

Täsmällinen todistus löytyy esimerkiksi lähteestä [20], s. 22.

Määritelmä 3.28 (Maksimaalinen aliryhmä)**.** Olkoon G ryhmä ja H sen aliryhmä. Aliryhmä H on maksimaalinen aliryhmä, jos ryhmällä G ei ole sellaista aidosti aliryhmästä H eroavaa aliryhmää N, että $H < N < G$.

3.4 Ryhmien virittäminen

Tarkastellaan seuraavaksi ryhmien virittyvyyttä. Ensin määritellään yksittäisen alkion virittämä syklinen aliryhmä.

Määritelmä 3.29 (Alkion virittämä syklinen aliryhmä ja syklinen ryhmä)**.** Olkoon G ryhmä ja $a \in G$. Alkion a virittämä syklinen aliryhmä $\langle a \rangle$ on ryhmän G aliryhmä, joka koostuu kaikista alkion a potensseista. Ryhmä G on syklinen, jos on olemassa sellainen $a \in G$, että $G = \langle a \rangle$, eli syklinen ryhmä on yksiön virittämä ryhmä.

Suoraan edellisestä määritelmästä ja seurauksesta 3.21 seuraa, että kaikki sykliset ryhmät ovat Abelin ryhmiä.

Seuraus 3.30. *Kaikki sykliset ryhmät ovat Abelin ryhmiä.*

Todistus. Ks. [12], s. 34. □

Toisaalta syklisen ryhmän määritelmästä seuraa, että kaikki syklisen ryhmän aliryhmät ovat syklisiä.

Seuraus 3.31. *Kaikki syklisen ryhmän aliryhmät ovat syklisiä.*

Todistus. Ks. [12], s. 35. □

Alkion virittämän syklisen aliryhmän käsitteen avulla voidaan kertaluvun käsite määritellä myös yksittäiselle alkiolle. Määritelmä perustuu suoraan ryhmän kertaluvun määritelmään.

Määritelmä 3.32 (Alkion kertaluku)**.** Kun G on ryhmä ja $a \in G$, alkion a kertaluku $|a|$ on $|\langle a \rangle|$ eli syklisen aliryhmän $\langle a \rangle$ kertaluku.

Vaihtoehtoisesti alkion $a \in G$ kertaluku voitaisiin määritellä pienimmäksi sellaiseksi kokonaislukueksponentiksi n, jolla $a^n = 1$. Tämä ehto on kuitenkin johdettavissa edellisestä määritelmästä:

Lause 3.33. *Jos G on ryhmä ja alkion $a \in G$ kertaluku on $m \in \mathbb{Z}_+$, niin m on pienin sellainen kokonaislukueksponentti, että $a^m = 1$.*

Todistus. Ks. [20], s. 21. □

Alkion virittämän syklisen aliryhmän käsitettä voidaan yleistää tarkastelemalla joukon virittämää aliryhmää. Intuitiivisesti voidaan ajatella, että joukko S virittää ryhmän G, jos jokainen ryhmän alkio voidaan esittää joukon S alkioiden ja niiden käänteisalkioiden tulona.

Määritelmä 3.34 (Joukon virittämä aliryhmä)**.** Olkoon G ryhmä ja $S \subseteq G$. Joukon S virittämä aliryhmä $\langle S \rangle$ on pienin ryhmän G aliryhmä, joka sisältää joukon S. Sanotaan, että joukko S virittää aliryhmän $\langle S \rangle$ ja että joukon S alkiot ovat aliryhmän $\langle S \rangle$ virittäjiä. Joukkoa S kutsutaan aliryhmän $\langle S \rangle$ virittäväksi joukoksi.

Huomautus. On tietysti täysin mahdollista, että joukko S virittää myös koko ryhmän G eikä ainoastaan sen aliryhmää. Jos joukko S virittää ryhmän G, ryhmälle G käytetään toisinaan merkintää (G, S). Tässä tutkielmassa kyseistä notaatiota ei kuitenkaan käytetä myöhemmin ilmenevän sekaannusmahdollisuuden vuoksi.

Puhuttaessa joukon virittämästä aliryhmästä tarkastellaan, millainen aliryhmä saadaan tietyllä virittävällä joukolla. Tämä aliryhmä on määritelmänsä mukaan pienin mahdollinen eli yksikäsitteinen. Tutkielman 4. ja 5. luvussa esitetään useammin käänteinen kysymys, eli millaiset joukot virittävät annetun (ali-)ryhmän. Samalla ryhmällä voi luonnollisesti olla useita tällaisia joukkoja, kuten seuraava esimerkki osoittaa, eli ryhmän virittävä joukko ei ole yksikäsitteinen. Toisinaan kirjallisuudessa esitetään rajoite, että virittävän joukon tulisi olla minimaalinen, mutta tässä tutkielmassa kyseistä rajoitetta ei aseteta.

Esimerkki 3.35. Olkoon $X = \{1, 2, 3\}$. Ryhmän $(S_X, \circ)$ virittää esimerkiksi joukko $\{(12), (23), (13)\}$. Toisaalta myös joukko $\{(12), (123)\}$ virittää saman ryhmän. Triviaalisti ryhmän perusjoukko on aina eräs ryhmän virittävä joukko, eli myös joukko S_X virittää ryhmän $(S_X, \circ)$.

Jos joukko S on äärellinen ja se virittää ryhmän G, sanotaan, että ryhmä G on äärellisesti viritettävissä. Jokainen äärellinen ryhmä on äärellisesti viritettävissä. Toisaalta monesti äärettömät ryhmät eivät ole äärellisesti viritettävissä: esimerkiksi rationaalilukujen joukko varustettuna rationaalilukujen summalla ei ole äärellisesti viritettävissä. Kokonaislukujen joukko varustettuna summalla puolestaan on äärellisesti viritettävissä: itse asiassa ryhmä $(\mathbb{Z}, +)$ on luvun 1 virittämä syklinen ryhmä. Toisaalta myös joukko $\{2, 3\}$ virittää ryhmän $(\mathbb{Z}, +)$. Kokonaislukujen yhteenlaskuryhmään sekä seuraavaksi esitettävään neliön diedriryhmään palataan luvussa 4.

Esimerkki 3.36. Neliön diedriryhmän perusjoukko on

$$\{\mathrm{id}, r, r^2, r^3, t, tr, tr^2, tr^3\} = \{\mathrm{id}, r, r^2, r^3, t, rt, r^2t, r^3t\}$$

ja binäärioperaatio on kuvausten yhdistäminen. Ryhmän alkiot tulkitaan geometrisesti siten, että kuvaus r vastaa neliön 90° kiertoa ja t neliön peilausta x-akselin suhteen, kun neliön keskipiste on origossa ja sivut ovat koordinaattiakselien suuntaiset. Kuvaus id vastaa identtistä kiertoa, eli sitä, että mitään kiertoa ei tapahdu. Neliön diedriryhmää merkitään tässä tutkielmassa symbolilla D_4. On jo ryhmän alkioiden esityksen perusteella selvää, että ryhmän D_4 virittää esimerkiksi joukko $S_1 = \{r, t\}$. Toisaalta myös joukko $S_2 = \{t, tr^3\}$ virittää ryhmän D_4.

3.5 Lagrangen lause

Konstruoidaan tässä alaluvussa käsitteistö Lagrangen lauseen esittämiseksi. Lagrangen lauseen mukaan aliryhmän kertaluku jakaa ryhmän kertaluvun. Lauseella on monia helposti johdettavia seurauksia, joita tarvitaan myöhemmin algebrallisen graafiteorian todistuksissa. Määritellään kuitenkin ensin aliryhmän vasen ja oikea sivuluokka.

Määritelmä 3.37 (Aliryhmän oikea ja vasen sivuluokka)**.** Olkoon G ryhmä, $S \leq G$ ja $t \in G$. Alkion t määräämä aliryhmän S oikea sivuluokka ryhmässä G on joukko

$$St = \{st \mid s \in S\}.$$

Vastavaasti alkion t määräämä vasen sivuluokka on joukko

$$tS = \{ts \mid s \in S\}.$$

Alkiota t kutsutaan sivuluokan St tai tS edustajaksi.

Aliryhmän sivuluokat jakavat ryhmän erillisiin joukkoihin, joilla on keskenään samankaltaisia ominaisuuksia. Seuraava esimerkki havainnollistaa asiaa.

Esimerkki 3.38. Tarkastellaan ryhmää $(\mathbb{R}^2, +')$, eli ryhmää, jonka perusjoukon muodostavat kaikki reaalilukuparit ja jonka binäärioperaation muodostaa reaalilukuparien yhteenlasku. Binäärioperaatio on siis

$$(x_1, y_1) +' (x_2, y_2) = (x_1 + x_2, y_1 + y_2),$$

kun $x_1, x_2, y_1, y_2 \in \mathbb{R}$. Mikä tahansa origon kautta kulkeva suora l on ryhmän $(\mathbb{R}^2, +')$ aliryhmä. Kaikki suoran l kanssa yhdensuuntaiset suorat ovat kyseisen aliryhmän sivuluokkia. Tarkempien perustelujen osalta ks. [20], s. 24.

Määritelmä 3.39 (Aliryhmän indeksi)**.** Olkoon G ryhmä ja $S \leq G$. Aliryhmän S indeksi ryhmässä G on aliryhmän S oikeiden sivuluokkien lukumäärä ryhmässä G. Aliryhmän S indeksiä ryhmässä G merkitään $[G : S]$.

Nyt voidaan esittää Lagrangen lause. Todistetaan myös kaksi sen suoraa seurausta.

Lause 3.40 (Lagrangen lause)**.** *Jos G on äärellinen ryhmä ja $S \leq G$, niin aliryhmän S kertaluku jakaa ryhmän G kertaluvun, ja $[G : S] = |G|/|S|$.*

Todistus. Ks. [20], s. 26. □

Seuraus 3.41. *Jos G on äärellinen ryhmä ja $a \in G$, niin alkion a kertaluku jakaa ryhmän G kertaluvun.*

Todistus. Olkoon $a \in G$, missä G on äärellinen ryhmä. Määritelmän 3.32 mukaan alkion a kertaluku $|a| = |\langle a \rangle|$, ja koska $\langle a \rangle \leq G$, niin väite seuraa suoraan Lagrangen lauseesta 3.40. □

Seuraus 3.42. *Olkoon G äärellinen ryhmä ja $a \in G$. Jos $a^k = 1$ jollakin $k \in \mathbb{Z}_+$, niin $k = n|a|$ jollakin $n \in \mathbb{Z}_+$, eli alkion a kertaluku jakaa luvun k.*

Todistus. Olkoon G äärellinen ryhmä ja $a \in G$ sellainen alkio, että $a^k = 1$ jollakin $k \in \mathbb{Z}_+$. Jos luku k on alkion a kertaluku, väite seuraa. Muussa tapauksessa olkoon $|a| = m$. Täytyy olla $m < k$, koska m on lauseen 3.33 perusteella pienin kokonaislukueksponentti, jolle on voimassa $a^m = 1$. Jos nyt olisi $k = nm + r$ jollakin $n \in \mathbb{N}$ ja $0 < r < m$, saataisiin edelleen

$$a^k = a^{nm+r} = 1^n a^r = a^r \neq 1,$$

mikä on ristiriita. Siispä täytyy olla $k = nm$ eli $k = n|a|$, mikä todistaa väitteen. □

3.6 Tekijäryhmät

Tässä alaluvussa perehdytään tekijäryhmän käsitteeseen. Sitä varten tulee ensin määritellä normaali aliryhmä.

Määritelmä 3.43 (Normaali aliryhmä)**.** Ryhmän G aliryhmä N on normaali aliryhmä, mitä merkitään $N \lhd G$, jos $gNg^{-1} = N$ kaikilla $g \in G$.

Normaaleilla aliryhmillä on monia kiinnostavia ominaisuuksia. Todistuksetta mainittakoon, että jokainen normaali aliryhmä on jonkin ryhmähomomorfismin ydin, ja jokainen normaalin aliryhmän N vasen sivuluokka ryhmässä G on myös sen oikea sivuluokka ryhmässä G.

Siirrytään sitten itse tekijäryhmiin. Tekijäryhmää ei itse asiassa nosteta omaksi määritelmäkseen, vaan se johdetaan lauseena normaalin aliryhmän ja sivuluokkien määritelmistä. Luonnollisella kielellä ilmaistuna tekijäryhmällä tarkoitetaan normaalin aliryhmän sivuluokkien muodostamaa ryhmää.

Lause 3.44 (Tekijäryhmä)**.** *Jos G on ryhmä ja $N \lhd G$, niin normaalin aliryhmän N sivuluokat ryhmässä G muodostavat ryhmän, jonka kertaluku on $[G : N]$ ja jota merkitään G/N.*

Todistus. Olkoon G ryhmä ja $N \lhd G$. Konstruoidaan ryhmä G/N seuraavasti: Olkoon perusjoukkona kaikkien normaalin aliryhmän N sivuluokkien perhe. Koska N on normaali aliryhmä, ei ole merkitystä, käsitelläänkö vasemman- vai oikeanpuoleisia sivuluokkia. Binäärioperaatioksi valitaan ryhmän G perusjoukon epätyhjien osajoukkojen joukko-opillinen tulo:

$$AB = \{ab \mid a \in A, b \in B\},$$

kun $A, B \subseteq G$ ja $A \neq \emptyset, B \neq \emptyset$. Selvästi tämä binäärioperaatio on liitännäinen, koska G on ryhmä ja siis sen binäärioperaatio on liitännäinen.

Varmistetaan, että kahden sivuluokan tulo on sivuluokka. Olkoon Na alkion a määräämä normaalin aliryhmän N oikea sivuluokka ja Nb alkion b määräämä normaalin aliryhmän N oikea sivuluokka. Nyt

$$NaNb = Na(a^{-1}Na)b = N(aa^{-1})Nab = NNab = Nab.$$

Siispä sivuluokkien Na ja Nb tulo on todella sivuluokka.

Sivuluokkien tulon neutraalialkio on $N = N1$, missä 1 on ryhmän G neutraalialkio, ja sivuluokan Na käänteisalkio on $N(a^{-1})$. Näin ollen G/N on ryhmä. Lopulta aliryhmän indeksin määritelmän 3.39 nojalla $|G/N| = [G : N]$, mikä todistaa väitteen. □

Suoraan Lagrangen lausetta 3.40 soveltaen saadaan, että kun G on äärellinen ryhmä ja $N \lhd G$, niin tekijäryhmän G/N kertaluku on $|G|/|N|$.

Esimerkki 3.45 (Kokonaislukujen modulaariset ryhmät tekijäryhminä)**.** Olkoon $n \in \mathbb{Z}_+$. Tällöin ryhmä $\mathbb{Z}_n$, eli kaikki kokonaisluvut modulo n, on sama ryhmä kuin tekijäryhmä $\mathbb{Z}/\langle n \rangle$. Kyseistä ryhmää merkitään myös $\mathbb{Z}/n\mathbb{Z}$.

Tekijäryhmiin liittyy olennaisesti luonnollisen homomorfismin käsite.

Määritelmä 3.46 (Luonnollinen homomorfismi)**.** Olkoon G ryhmä ja $N \lhd G$. Luonnollinen homomorfismi on kuvaus

$$f : G \to G/N,$$

jolle $f(a) = Na$.

Seuraus 3.47. *Luonnollinen homomorfismi $f : G \to G/N$ on surjektio, joka on todella homomorfismi ja jolle on voimassa $Ker(f) = N$.*

Todistus. Ks. [20], s. 33. □

3.7 Sylowin 1. lause

Sylowin 1. lause on ryhmän kertalukuun liittyvä varsin tekninen tulos, jonka mukaan ryhmällä on tietyntyyppinen aliryhmä, jonka kertaluku riippuu alkuperäisen ryhmän kertaluvun alkutekijähajotelmasta. Sylowin lauseita ajatellaan perinteisesti olevan kolme, mutta tässä tutkielmassa tarvitaan vain niistä ensimmäistä, eikä muita lauseita näin ollen käsitellä. Lausetta sekä siihen liittyviä käsitteitä tarvitaan sekä nilpotenttien ryhmien käsittelyssä seuraavassa alaluvussa että alaluvun 5.4 todistuksissa.

Sylowin 1. lauseen idean pohjustamistarkoituksessa esitetään Cauchyn lause, joka on heikompi versio Sylowin 1. lauseesta ja joka on Sylowin 1. lausetta vanhempi tulos. Tulos muistuttaa hieman Lagrangen lauseesta johdettua seurausta 3.41.

Lause 3.48 (Cauchyn lause)**.** *Jokainen äärellinen ryhmä, jonka kertaluku on jaollinen alkuluvulla p, sisältää alkion, jonka kertaluku on p.*

Todistus. Ks. [20], s. 74. □

Sylowin 1. lause koskee Sylowin p-aliryhmiä, jotka on tarpeen määritellä ennen Sylowin 1. lauseen esittämistä.

Määritelmä 3.49 (p-ryhmä)**.** Olkoon p alkuluku. Ryhmä G on p-ryhmä, jos jokaiselle $g \in G \setminus \{1\}$ on voimassa $|g| = p^k$ jollakin $k \in \mathbb{Z}_+$.

Huomautus. Voidaan tietysti puhua myös p-aliryhmästä, joka määritellään vastaavasti kuin p-ryhmä.

Määritellään sitten Sylowin p-aliryhmä ja esitetään Sylowin 1. lause. Määritelmä ja lause noudattavat luvun muusta sisällöstä poiketen John Humphreysin kirjan [12] esitystä (s. 98–99).

Määritelmä 3.50 (Sylowin p-aliryhmä)**.** Olkoon p alkuluku, $n \in \mathbb{Z}_+$ ja k sellainen positiivinen kokonaisluku, joka ei ole jaollinen luvulla p. Olkoon lisäksi G äärellinen ryhmä, jonka kertaluku on kp^n. Sylowin p-aliryhmä on sellainen ryhmän G aliryhmä, jonka kertaluku on p^n.

Vaihtoehtoisesti Sylowin p-aliryhmä voitaisiin määritellä ryhmän G maksimaalisena p-aliryhmänä.

Lause 3.51 (Sylowin 1. lause)**.** *Olkoon p alkuluku, ja olkoon G äärellinen ryhmä, jonka kertaluku on kp^n, missä alkuluku p ei jaa lukua k. Tällöin ryhmällä G on ainakin yksi Sylowin p-aliryhmä.*

Todistus. Ks. [12], s. 99. □

3.8 Nilpotentit ryhmät

Tässä alaluvussa käsitellään nilpotentteja ryhmiä. Voidaan ajatella, että nilpotentit ryhmät yleistävät edellisessä alaluvussa käsiteltyjä p-ryhmiä. Nilpotentteja ryhmiä kutsutaan lisäksi ”melkein vaihdannaisiksi ryhmiksi”. Nilpotenttien ryhmien määrittely vaatii hieman taustatietoja kommutaattoreista ja kommutaattorialiryhmistä, jotka määritellään näin ollen ensimmäisenä.

Määritelmä 3.52 (Kommutaattori ja kommutaattorialiryhmä)**.** Olkoon G ryhmä. Jos $a, b \in G$, niin alkioiden a ja b kommutaattori on alkio

$$[a, b] = aba^{-1}b^{-1}.$$

Ryhmän G kommutaattorialiryhmä on kaikkien ryhmän G kommutaattorien virittämä ryhmän G aliryhmä.

Otetaan lisäksi käyttöön kommutaattoreihin liittyvä, merkintöjä yksinkertaistava määritelmä:

Määritelmä 3.53. Olkoon G ryhmä, ja olkoot $H, K \leq G$. Merkitään tällöin

$$[H, K] = \langle [h, k] \mid h \in H \text{ ja } k \in K \rangle.$$

Määritellään nyt edellisten käsitteiden avulla karakteristiset aliryhmät, joita edelleen tarvitaan nilpotenttien ryhmien määritelmässä.

Määritelmä 3.54 (Karakteristiset aliryhmät)**.** Ryhmän G karakteristiset aliryhmät $\gamma_i(G)$ määritellään induktiivisesti:

- $\gamma_1(G) = G$,
- $\gamma_{i+1}(G) = [\gamma_i(G), G]$, missä $i \in \mathbb{Z}_+$.

On tärkeää huomata, että

$$\gamma_2(G) = [\gamma_1(G), G] = [G, G]$$

on ryhmän G kommutaattorialiryhmä ja että $\gamma_{i+1}(G) \leq \gamma_i(G)$ kaikilla $i \in \mathbb{Z}_+$.

Viimein voidaan määritellä nilpotentti ryhmä.

Määritelmä 3.55 (Nilpotentti ryhmä)**.** Ryhmä G on nilpotentti, jos on on olemassa sellainen $c \in \mathbb{N}$ että $\gamma_{c+1}(G) = 1$. Pienintä tällaista lukua c kutsutaan nilpotentin ryhmän G luokaksi.

Nilpotenteilla ryhmillä, kuten monilla muillakin abstraktin algebran käsitteillä, on lukuisia keskenään ekvivalentteja määritelmiä. Näistä kiinnostuneille koottua tietoa löytyy esimerkiksi Matti Karppasen pro gradu -tutkielmasta [15].

Esitetään vielä todistuksetta kaksi mielenkiintoista nilpotentteihin ryhmiin liittyvää lausetta. Ensimmäinen lause liittää nilpotentit ryhmät p-ryhmiin ja jälkimmäinen Sylowin aliryhmiin.

Lause 3.56. *Jokainen äärellinen p-ryhmä on nilpotentti, kun p on alkuluku.*

Todistus. Ks. [20], s. 115. □

Lause 3.57. *Äärellinen ryhmä G on nilpotentti, jos ja vain jos se on Sylowin aliryhmiensä suora tulo (ks. määritelmä 3.58).*

Todistus. Ks. [20], s. 116. □

3.9 Ryhmien tuloja

Tässä alaluvussa määritellään ryhmien suora ja puolisuora tulo, joita käytetään luomaan kahdesta ryhmästä uusi ryhmä. Suoran tulon määritelmä palautuu suoraviivaisesti alkioiden väliseen binäärioperaatioon, kun taas puolisuora tulo on monimutkaisempi operaatio.

Määritelmä 3.58 (Suora tulo)**.** Ryhmien $(H, *_H)$ ja $(K, *_K)$ suora tulo $H \times K$ on ryhmä, jonka perusjoukko on $\{(h, k) \mid h \in H, k \in K\}$ ja binäärioperaatio

$$(h_1, k_1) \cdot' (h_2, k_2) = (h_1 *_H h_2, k_1 *_K k_2),$$

missä $h_1, h_2 \in H$ ja $k_1, k_2 \in K$.

Huomautus. Määritelmän 3.58 mukaista suoraa tuloa kutsutaan toisinaan kirjallisuudessa myös ulkoiseksi suoraksi tuloksi, sillä ryhmien suoralle tulolle on myös vaihtoehtoinen määritelmä, jota kutsutaan sisäiseksi suoraksi tuloksi. Tämän määritelmän mukaan suoran tulon perusjoukon alkiot ovat ryhmien H ja K perusjoukkojen alkioiden tuloja, eivät järjestettyjä pareja. Voidaan kuitenkin osoittaa, että määritelmät ovat ekvivalentit, joten tätä erottelua ei tehdä (ks. [20], s. 40–41). Pääsääntöisesti tässä tutkielmassa käytetään syntaksin osalta nimenomaan ulkoista suoraa tuloa, mutta esimerkiksi lauseen 5.25 todistuksessa suora tulo ymmärretään sisäisenä suorana tulona.

Voidaan helposti todentaa, että suora tulo todella on ryhmä ja itse asiassa jopa Abelin ryhmä, jos ryhmät H ja K ovat Abelin ryhmiä. Nimittäin $\cdot'$ on liitännäinen ja vaihdannainen binäärioperaatio, koska ryhmien H ja K binäärioperaatiot ovat liitännäisiä ja vaihdannaisia. Lisäksi ryhmän $H \times K$ neutraalialkio on $(1_H, 1_K)$, missä 1_H on ryhmän H neutraalialkio ja 1_K on ryhmän K neutraalialkio, ja alkion (h, k) käänteisalkio on (h^{-1}, k^{-1}).

Lause 3.59. *Olkoot G ja H ryhmiä. Tällöin $|G \times H| = |G||H|$.*

Todistus. Joukkojen karteesisen tulon mahtavuuden määritelmän perusteella mille tahansa joukoille A ja B on voimassa $|A \times B| = |A||B|$, mistä väite suoraan seuraa. □

Suoran tulon käsitettä voidaan yleistää, jolloin päädytään puolisuoraan tuloon.

Määritelmä 3.60 (Puolisuora tulo)**.** Ryhmä G on ryhmien H ja K puolisuora tulo, mitä merkitään $G = H \rtimes K$, jos

1. $H \lhd G$ ja $K \leq G$,
2. $HK = G$,
3. $H \cap K = \{1\}$.

Huomautus. Edellisessä määritelmässä merkintä HK tarkoittaa ryhmien H ja K perusjoukkojen joukko-opillista tuloa eli joukkoa $\{hk \mid h \in H, k \in K\}$.

Käydään puolisuoran tulon määritelmä läpi vielä luonnollisella kielellä. Ensimmäisenä havaitaan, että määritelmän mukaan puolisuora tulo itsessään on ryhmä, samaan tapaan kuin ryhmien suora tulokin on ryhmä. Määritelmän ehto 1 kertoo, että ryhmän H tulee olla puolisuoran tulon $H \rtimes K$ normaali aliryhmä ja ryhmän K sen aliryhmä – siis aliryhmien H ja K alkiot ovat oleellisesti samankaltaisia, esimerkiksi lukuja tai kuvauksia. Ehto 2 puolestaan kertoo puolisuoran tulon rakenteen: puolisuoran tulon alkiot ovat täsmälleen kaikki tulot $hk, h \in H, k \in K$. Ehto 3 rajoittaa ryhmien H ja K perusjoukkoja määrittämällä, että niiden ainoa yhteinen alkio on ryhmän G neutraalialkio 1.

Puolisuoralla tulolla on monia vaihtoehtoisia määritelmiä, joihin ei tässä tarkemmin perehdytä. Kiinnostunut lukija löytää näistä lisää tietoa Rotmanin kirjasta [20], s. 168. Määritelmä 3.60 lienee näistä selkein konstruktiivisen rakenteensa vuoksi.

Eräs syy siihen, miksi puolisuorat tulot ovat kiinnostavia, on se, että kaikki diedriryhmät ovat isomorfisia puolisuorien tulojen kanssa. Erityisesti neliön diedriryhmä on isomorfinen ryhmien $\mathbb{Z}_4$ ja $\mathbb{Z}_2$ puolisuoran tulon kanssa. Tämä erityistapaus todistetaan esimerkissä 3.62.

Lause 3.61. *Kaikilla diedriryhmillä D_m on voimassa $D_m \cong \mathbb{Z}_m \rtimes \mathbb{Z}_2$.*

Todistus. Ks. [20], s. 168. □

Esimerkki 3.62. Olkoon K ryhmä, jonka perusjoukko koostuu kierroista id, r, r^2 ja r^4 ja jonka binäärioperaatio on kuvausten yhdistäminen. Olkoon P ryhmä, jonka perusjoukko koostuu peilauksista id ja t ja jonka binäärioperaatio on kuvausten yhdistäminen (merkintöjen osalta ks. esimerkki 3.36). On suoraviivaista todentaa, että K ja P ovat todella ryhmiä. Selvästi myös $K \cong \mathbb{Z}_4$ ja $P \cong \mathbb{Z}_2$, joten $\mathbb{Z}_4 \rtimes \mathbb{Z}_2 \cong K \rtimes P$.

Todistetaan nyt suoraan määritelmän 3.60 perusteella, että

$$\mathbb{Z}_4 \rtimes \mathbb{Z}_2 \cong K \rtimes P \cong D_4.$$

Päättely perustuu esimerkissä 3.36 havaittuun ryhmän D_4 rakenteeseen.

1. Selvästi $K, P \leq D_4$. Esimerkiksi käymällä kaikki vaihtoehdot läpi havaitaan, että $kPk^{-1} = P$ kaikilla $k \in K$, joten $P \lhd D_4$.
2. Ryhmän D_4 rakenteen perusteella ryhmien perusjoukoille on voimassa $D_4 = KP$.

3. Ainoa aliryhmien K ja P yhteinen alkio on identtinen kierto (eli identtinen peilaus) id, joka on myös molempien aliryhmien neutraalialkio, joten $K \cap P = \{\mathrm{id}\}$.

Siispä määritelmän 3.60 perusteella $\mathbb{Z}_4 \rtimes \mathbb{Z}_2 \cong K \rtimes P \cong D_4$.

Käsitellään sitten kolmea suoriin tuloihin liittyvää lausetta. Tässä tutkielmassa läpikäytävät esitiedot eivät riitä lauseiden todistamiseen, mutta lauseet esitetään todistuksetta, koska niitä tullaan tarvitsemaan luvussa 5. Ensimmäinen tulos tunnetaan äärellisten Abelin ryhmien peruslauseena.

Lause 3.63 (Äärellisten Abelin ryhmien peruslause)**.** *Jokainen äärellinen Abelin ryhmä on isomorfinen äärellisen monen äärellisen syklisen ryhmän suoran tulon kanssa.*

Todistus. Ks. [20], s. 130. □

Esitetään sitten äärellisesti virittyvien Abelin ryhmien peruslause, joka yleistää äärellisten Abelin ryhmien peruslausetta. Käytetään sen esityksessä lyhennysmerkintää $\mathbb{Z}^r = \underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{r \text{ kertaa}}$.

Lause 3.64 (Äärellisesti virittyvien Abelin ryhmien peruslause)**.** *Olkoon G äärellisesti virittyvä Abelin ryhmä. Tällöin*

$$G \cong \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_s} \times \mathbb{Z}^r,$$

missä $r \geq 0$ ja p_i on alkuluku kaikilla $i \in \{1, \ldots, s\}$.

Todistus. Ks. [20], s. 319. □

Viimeisenä käsitellään Krull-Schmidtin lausetta, josta seuraa, että ryhmän esitys suorana tulona on isomorfiaa vaille yksikäsitteinen. Lauseen esittämistä varten tarvitaan liuta apukäsitteitä.

Määritelmä 3.65 (Hajottamaton ryhmä)**.** Ryhmä G on hajottamaton, jos $G \neq \{1\}$, ja mikäli $G = H \times K$ niin joko $H = \{1\}$ tai $K = \{1\}$.

Määritelmä 3.66 (Nouseva ketjuehto)**.** Ryhmä G toteuttaa nousevan ketjuehdon, jos jokainen kasvava ketju sen normaaleja aliryhmiä pysähtyy, eli jos

$$K_1 \leq K_2 \leq K_3 \leq \cdots$$

on ketju ryhmän G normaaleja aliryhmiä, niin on olemassa sellainen $t \in \mathbb{Z}_+$, että

$$K_t = K_{t+1} = K_{t+2} = \cdots .$$

Määritelmä 3.67 (Laskeva ketjuehto)**.** Ryhmä G toteuttaa laskevan ketjuehdon, jos jokainen laskeva ketju sen normaaleja aliryhmiä pysähtyy, eli jos

$$H_1 \geq H_2 \geq H_3 \geq \cdots$$

on ketju ryhmän G normaaleja aliryhmiä, niin on olemassa sellainen $s \in \mathbb{Z}_+$, että

$$H_s = H_{s+1} = H_{s+2} = \cdots .$$

Lause 3.68 (Krull-Schmidtin lause)**.** *Olkoon G ryhmä, joka toteuttaa sekä nousevan että laskevan ketjuehdon. Jos*

$$G = H_1 \times \cdots \times H_s \text{ ja } G = K_1 \times \cdots \times K_t$$

ovat kaksi ryhmän G jakoa hajottamattomiin tekijöihin, niin on voimassa $s = t$ ja ryhmät H_i ja K_j voidaan indeksoida uudelleen siten, että $H_k \cong K_k$ kaikilla indekseillä $k \in \{1, \ldots, s\}$. Lisäksi jos r on sellainen indeksi, että $1 < r < s$, niin indeksointi voidaan valita siten, että

$$G = H_1 \times \cdots \times H_r \times K_{r+1} \times \cdots \times K_s.$$

Todistus. Ks. [20], s. 149. □

3.10 Symmetriaryhmät

Ryhmäteoriaa käsittelevän luvun viimeisessä alaluvussa käsitellään symmetriaryhmiä. Symmetriaryhmä on ryhmä, jonka perusjoukon alkiot ovat kuvauksia ja jonka binäärioperaatio on kuvausten yhdistäminen. Symmetriaryhmiä on käsitelty jo aiemmin tutkielmassa – muun muassa permutaatioiden ryhmä $S_{\{1,2,3\}}$ ja neliön diedriryhmä D_4 ovat symmetriaryhmiä. Tässä alaluvussa symmetriaryhmiä käsitellään kuitenkin vielä kootusti, koska ne muodostavat tärkeän linkin graafiteorian ja ryhmäteorian välille ja pohjustavat täten lukuun 4 siirtymistä: nimittäin myös graafeista voidaan muodostaa symmetriaryhmiä, joiden alkiot ovat isomorfismeja graafilta itselleen eli graafiautomorfismeja.

Alaluvun luonne ja esitys eroaa hieman edellisistä alaluvuista, koska symmetriaryhmät eivät ole puhtaasti abstraktiin algebraan liittyviä rakenteita vaan niitä käytetään monilla muillakin matematiikan osa-alueilla, ja notaatiot on täten pyritty pitämään mahdollisimman yleisinä. Lisäksi tämän alaluvun sisältö on peräisin Meierin kirjasta [17].

Otetaan ensimmäisenä käyttöön määritelmiä selkeyttävä merkintä $\mathrm{Sym}(X)$. Määritellään sitten hyvin yleisellä tasolla symmetriaryhmä, ja tarkastellaan asiaa konkretisoivia esimerkkejä.

Määritelmä 3.69 (Joukko $\mathrm{Sym}(X)$)**.** Olkoon X joukko, säännöllinen ja origokeskinen monikulmio, graafi tai ryhmä. Merkinnällä $\mathrm{Sym}(X)$ tarkoitetaan joukkoa, jonka alkioita ovat kaikki ne bijektiot objektilta X itselleen, jotka säilyttävät objektin X matemaattisen rakenteen.

Huomautus. Useimmiten edellisessä määritelmässä mainitut objektin X matemaattisen rakenteen säilyttävät bijektiot ovat automorfismeja.

Määritelmä 3.70 (Symmetriaryhmä)**.** Olkoon X joukko, säännöllinen ja origokeskinen monikulmio, graafi tai ryhmä. Tällöin järjestettyä paria $(\mathrm{Sym}(X), \circ)$ kutsutaan objektin X symmetriaryhmäksi, mikäli kyseinen rakenne on ryhmä.

Samaistetaan jatkossa joukko $\mathrm{Sym}(X)$ ryhmään $(\mathrm{Sym}(X), \circ)$, kuten aiemmissakin alaluvuissa on tehty.

Esimerkki 3.71. Jos X on joukko, $\mathrm{Sym}(X)$ on kaikkien joukon X permutaatioiden ryhmä. Jos X on ryhmä G, puhutaan ryhmän G automorfismiryhmästä $\mathrm{Aut}(G)$, joka siis koostuu ryhmän G isomorfismeista itselleen. Myös jos X on graafi $\mathcal{G}$, $\mathrm{Sym}(\mathcal{G})$ on graafin automorfismien eli symmetrioiden ryhmä.

Symmetriaryhmien yhteydessä on jopa poikkeuksellisen tärkeää käyttää täsmällistä terminologiaa, sillä käsitteistö vaihtelee paljon kirjoittajasta riippuen ja samalle objektille saatetaan saman tekstinkin sisällä käyttää eri nimiä asiayhteydestä riippuen. Lisäksi aiheeseen liittyy paljon keskenään samanlaisia käsitteitä. Esimerkiksi symmetriaryhmä ja symmetrinen ryhmä eivät tarkoita samaa asiaa:

Määritelmä 3.72 (Symmetrinen ryhmä ja permutaatioryhmä)**.** Olkoon X joukko. Tällöin kaikkien joukon X permutaatioiden joukko S_X yhdessä permutaatioiden yhdistämisen kanssa muodostaa ryhmän, jota kutsutaan *symmetriseksi ryhmäksi*. Symmetrisen ryhmän aliryhmät puolestaan ovat *permutaatioryhmiä*.

Symmetrinen ryhmä on symmetriaryhmän erityistapaus. Täten kaikki symmetriset ryhmät ovat symmetriaryhmiä, mutta kaikki symmetriaryhmät eivät ole symmetrisiä ryhmiä.

4 Cayleyn graafit

Tässä luvussa perehdytään Cayleyn graafeihin. Cayleyn graafien konsepti on peräisin vuodelta 1878, jolloin englantilainen matemaatikko Arthur Cayley julkaisi artikkelin *The Theory of Groups: Graphical Representation* [4]. Artikkelin nimi on varsin osuva, sillä Cayleyn graafit ovat nimenomaan tapa visualisoida ryhmiä geometrisesti graafeilla. Lisäksi ne mahdollistavat ryhmien ominaisuuksien tarkastelun graafien avulla, vaikkakin kenties yleisempää on hyödyntää algebrallisia menetelmiä graafiteorian tuloksien todistamiseen. Viimeksi mainittua menetelmää hyödyntävää matematiikan osa-aluetta kutsutaan algebralliseksi graafiteoriaksi.

Tutkielman tavoitteiden kannalta tämä luku ensisijaisesti pohjustaa tutkielman viidettä lukua, jossa käsitellään Cayleyn graafeihin liittyvää 1-faktorointikonjektuuria. Toisaalta luku on myös itsessään tärkeä, sillä Cayleyn graafeja tai algebrallista graafiteoriaa ylipäänsä käsitellään yliopisto-opetuksessa harvoin.

Cayleyn graafien käsittely aloitetaan todistamalla Cayleyn lause, jonka mukaan jokainen ryhmä on isomorfinen jonkin permutaatioryhmän kanssa, sekä sen muokattu versio, jonka mukaan jokainen äärellisesti virittyvä ryhmä on isomorfinen yhtenäisen, suuntaamattoman ja paikallisesti äärellisen graafin symmetriaryhmän aliryhmän kanssa. Lauseen pohjalta määritellään Cayleyn graafit. Tämän jälkeen todistetaan joitakin Cayleyn graafien yleisiä ominaisuuksia ja annetaan esimerkkejä Cayleyn graafeista.

Luku perustuu isoilta osin Meierin kirjaan [17]. Muutamien lauseiden lähteenä on käytetty lisäksi Biggsin [3] kirjaa.

4.1 Cayleyn lause

Ennen Cayleyn graafien määrittelyä on tarpeen oikeuttaa määritelmä tarkastelemalla ryhmien ja graafien välistä yhteyttä. Aloitetaan todistamalla Cayleyn lause, jonka mukaan jokainen ryhmä on isomorfinen jonkin symmetrisen ryhmän aliryhmän eli permutaatioryhmän kanssa. Tulos itsessään pohjustaa Cayleyn graafien käsittelyä siinä mielessä, että monia symmetriaryhmiä (erityisesti monikulmioiden symmetriaryhmiä) voidaan helposti visualisoida graafimaisella esityksellä.

Lause 4.1 (Cayleyn lause)**.** *Jokainen ryhmä on isomorfinen jonkin permutaatioryhmän kanssa.*

Todistus. Väite todistetaan olennaisesti kahdessa eri vaiheessa. Ensin konstruoidaan kuvaus miltä tahansa ryhmältä jollekin permutaatioryhmälle ja osoitetaan, että jokaisen lähtöjoukon alkion kuva todella on permutaatio, minkä jälkeen konstruoitu kuvaus osoitetaan ryhmäisomorfismiksi.

Olkoon $(G, \cdot)$ ryhmä, ja olkoon S_G joukon G symmetrinen ryhmä, eli ryhmä, jonka alkioina ovat kaikki joukon G permutaatiot. Määritellään kuvaus

$$\pi \colon G \to S_G, \pi(g) = \alpha_g,$$

missä $\alpha_g \in S_G$ on sellainen kuvaus joukossa G, että $\alpha_g(h) = g \cdot h$ kaikilla $h \in G$. Osoitetaan, että α_g on todella permutaatio. Ensinnäkin se on selvästi kuvaus joukossa G. Toiseksi se on injektio, koska jos $\alpha_g(h_1) = \alpha_g(h_2)$ eli $gh_1 = gh_2$, niin $g^{-1}gh_1 = g^{-1}gh_2$, jolloin $h_1 = h_2$. Kolmanneksi kuvaus α_g on myös surjektio. Olkoon nimittäin $h \in G$. Tällöin

$$h = 1 \cdot h = (gg^{-1})h = g(g^{-1}h) = \alpha_g(g^{-1}h) \in \alpha_g[G]$$

ryhmän G binäärioperaation liitännäisyyden ja neutraalialkion 1 määritelmän nojalla, joten $G = \alpha_g[G]$. Täten α_g on bijektio ja siis joukon G permutaatio.

Siirrytään sitten todistuksen jälkimmäiseen vaiheeseen, eli osoitetaan, että kuvaus π on ryhmäisomorfismi. Aloitetaan todistamalla homomorfisuus. Riittävä ehto ryhmähomomorfisuudelle on, että $\pi(gh) = \pi(g) \circ \pi(h)$ eli että $\alpha_{gh} = \alpha_g \circ \alpha_h$. Olkoon $x \in G$ mikä tahansa ryhmän G alkio. Nyt

$$\alpha_{gh}(x) = (gh)x = g(hx)$$

ja edelleen permutaatioiden α_g ja α_h määritelmän nojalla

$$g(hx) = g \cdot \alpha_h(x) = \alpha_g(\alpha_h(x)) = (\alpha_g \circ \alpha_h)(x).$$

Siispä $\pi(gh) = \pi(g) \circ \pi(h)$, eli π on homomorfismi.

Osoitetaan sitten, että π on bijektio. Aloitetaan injektiivisyyden todistamisesta. Oletetaan argumentin vuoksi, että $\pi(g) = \pi(h)$ joillakin $g, h \in G$. Tällöin $\alpha_g = \alpha_h$, jolloin myös $\alpha_g(1) = \alpha_h(1)$. Siis $g \cdot 1 = h \cdot 1$ eli $g = h$, joten π on injektio. Selvästi π on myös bijektio $G \to \pi[G]$, missä

$$\pi[G] = \{\pi(g) \in S_G \mid g \in G\}.$$

Koska π on ryhmähomomorfismi ja G on ryhmä, $\pi[G]$ on ryhmä, ja erityisesti

$$\pi[G] = \{\pi(g) \in S_G \mid g \in G\} \leq S_G,$$

eli $\pi[G]$ on permutaatioryhmä. Lisäksi $G \cong \pi[G]$, mikä todistaa väitteen. □

Cayleyn lauseella on monta hieman toisistaan eroavaa muotoilua. Useissa lähteissä se todistetaan vain äärellisille ryhmille, mutta tässä tutkielmassa kyseistä rajoitetta ei ole asetettu, sillä todistus etenee sekä äärellisille että äärettömille ryhmille identtisesti surjektiivisuuden osoittamista lukuun ottamatta. Todistetaan seuraavana Cayleyn lauseen muokattu versio, jossa suoraan konstruoidaan Cayleyn graafit.

Lause 4.2. *Jokainen äärellisesti virittyvä ryhmä on isomorfinen yhtenäisen, suuntaamattoman ja paikallisesti äärellisen graafin symmetriaryhmän aliryhmän kanssa.*

Todistus. Olkoon G äärellisesti virittyvä ryhmä ja $S \subseteq G \setminus \{1\}$ sen virittävä joukko. Olkoon lisäksi $S^{-1} = \{s^{-1} \mid s \in S\}$. Konstruoidaan nyt ryhmästä G ja virittävästä joukosta S riippuva graafi $\mathcal{G}$ siten, että graafin $\mathcal{G}$ solmujoukko on G ja särmäjoukko

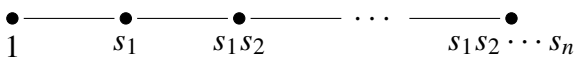
$$\{\{g, gs\} \mid g \in G, s \in S \cup S^{-1}\}.$$

On varmasti voimassa $gs \in G$ eli gs on todella graafin $\mathcal{G}$ solmu, sillä G on suljettu binäärioperaation suhteen, ja $s \in S \subseteq G \setminus \{1\}$.

Graafi $\mathcal{G}$ on suoraan määritelmän nojalla suuntaamaton. Todistetaan, että se on yhtenäinen. Itse asiassa riittää osoittaa, että ryhmän G neutraalialkiota vastaavan solmun ja minkä tahansa solmun välillä on polku. Olkoon siis g graafin $\mathcal{G}$ solmu. Koska S on ryhmän G äärellinen virittävä joukko, on voimassa $g = 1 \cdot s_1 \cdots s_n$, missä $s_i \in S$ kaikilla $i \in \{1, \ldots, n\}$, kun $n \in \mathbb{Z}_+$. Mutta tämähän tarkoittaa, että solmujen 1 ja g välillä on polku, jonka muodostavat särmät

$$\{1, s_1\}, \{s_1, s_1 s_2\}, \ldots, \{s_1 \ldots s_{n-1}, s_1 \cdots s_{n-1} s_n\}.$$

Kuva 4.1 havainnollistaa asiaa.



Kuva 4.1. Polku alkioiden 1 ja $s_1 s_2 \cdots s_n$ välillä graafissa $\mathcal{G}$.

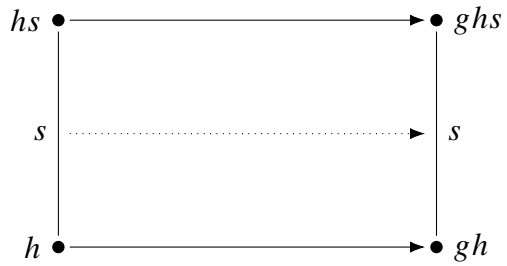
Jos $h \neq g$ on graafin $\mathcal{G}$ solmu, niin koska solmujen 1 ja h välillä on polku ja solmujen 1 ja g välillä on polku, on tietysti myös solmujen g ja h välillä polku. Täten graafi $\mathcal{G}$ on yhtenäinen.

Todistetaan sitten graafin $\mathcal{G}$ paikallinen äärellisyys. Tämä seuraa itse asiassa suoraan siitä, että virittävä joukko S on oletuksen mukaan äärellinen. Olkoon nimittäin g graafin $\mathcal{G}$ solmu. Tällöin jokaista $s \in S \cup S^{-1}$ kohden solmuun g liittyy särmä $\{g, gs\}$, joka on sama särmä kuin $\{gs, g\}$, koska $gss^{-1} = g$. Näitä solmuja on $|S \cup S^{-1}|$ kappaletta. Koska S on äärellinen ja täten myös S^{-1} on äärellinen, niin jokaisen graafin $\mathcal{G}$ solmun aste $|S \cup S^{-1}|$ on äärellinen. Siispä $\mathcal{G}$ on paikallisesti äärellinen.

Konstruoidaan sitten ryhmän G ja graafin $\mathcal{G}$ symmetriaryhmän $\mathrm{Sym}(\mathcal{G})$ aliryhmän välille kuvaus, joka osoitetaan ryhmäisomorfismiksi. Olkoon siis

$$\alpha \colon G \to \mathrm{Sym}(\mathcal{G})$$

sellainen kuvaus, että $\alpha(g)$ on graafin $\mathcal{G}$ automorfismi α_g, joka kuvaa solmun h solmulle gh. Kuvaus α_g on todella graafin $\mathcal{G}$ automorfismi kaikilla $g \in G$. Jos nimittäin $\{h, hs\}$ on graafin $\mathcal{G}$ särmä, kun $h \in G$ ja $s \in S \cup S^{-1}$, niin tietysti $gh \in G$, jolloin myös $\{gh, ghs\}$ on graafin $\mathcal{G}$ särmä. Toisaalta särmän $\{h, hs\}$ päätesolmujen kuvat kuvauksessa α_g ovat gh ja ghs, joiden välillä on graafin $\mathcal{G}$ määritelmän mukaan särmä. Täten kuvaus α_g säilyttää solmujen naapuruuden, minkä lisäksi se on selvästi bijektio ryhmän binäärioperaation ominaisuuksien nojalla, joten α_g on graafiautomorfismi. Tätä havainnollistetaan kuvalla 4.2.



Kuva 4.2. Särmän $\{h, hs\}$ kuva graafin $\mathcal{G}$ automorfismissa α_g.

Tarkistetaan sitten, että ryhmähomomorfismiehto on voimassa kuvaukselle α. Olkoon v graafin $\mathcal{G}$ solmu. Tällöin

$$\alpha(gh)(v) = \alpha_{gh}(v) = (gh)v = g(hv) = \alpha_g(hv) = (\alpha_g \circ \alpha_h)(v).$$

Täten $\alpha(gh) = \alpha_g \circ \alpha_h$, joten α on ryhmähomomorfismi.

Osoitetaan vielä, että α on bijektio. Jos $\alpha(g) = \alpha(g')$ eli $\alpha_g = \alpha_{g'}$, niin kaikilla $h \in G$ on voimassa $\alpha_g(h) = \alpha_{g'}(h)$ ja edelleen $gh = g'h$. Tällöin $g = g'$, joten α on injektio. Lisäksi muotoa $\alpha_g, g \in G$, olevat graafin $\mathcal{G}$ automorfismit muodostavat ryhmän $\mathrm{Sym}(\mathcal{G})$ aliryhmän $\mathrm{Sym}(\mathcal{G})_G$, koska

$$(\alpha_g \circ \alpha_h)(v) = g(hv) = (gh)v = \alpha_{gh}(v) \in \mathrm{Sym}(\mathcal{G})_G,$$

eli $\mathrm{Sym}(\mathcal{G})_G$ on suljettu kuvausten yhdistämisen suhteen. Täten α on suoraan määritelmän nojalla surjektio kuvauksena $G \to \mathrm{Sym}(\mathcal{G})_G$. Näin ollen α on ryhmäisomorfismi $G \to \mathrm{Sym}(\mathcal{G})_G$ ja siis ryhmät G ja $\mathrm{Sym}(\mathcal{G})_G$ ovat isomorfiset. □

Edellisessä lauseessa esitetty konstruktio voidaan nyt nostaa omaksi määritelmäkseen lähdettä [23] mukaillen.

Määritelmä 4.3 (Cayleyn graafi)**.** Olkoon G ryhmä, $S \subseteq G \setminus \{1\}$ ryhmän G virittävä joukko ja $S^{-1} = \{s^{-1} \mid s \in S\}$. Tällöin graafi $\Gamma(G, S)$ on ryhmän G Cayleyn graafi suhteessa virittävään joukkoon S, jos graafin $\Gamma(G, S)$

1. solmujoukko on G,
2. särmäjoukko on $\{\{g, sg\} \mid g \in G, s \in S \cup S^{-1}\}$.

Sanotaan, että alkio s virittää särmän $\{g, sg\}$ tai että särmä $\{g, sg\}$ liittyy alkioon s.

On huomattava, että lauseessa 4.2 konstruoidun graafin särmät ovat muotoa $\{g, gs\}, g \in G, s \in S \cup S^{-1}$, kun taas edellisen määritelmän mukaan ne ovat muotoa $\{g, sg\}$. Tässä ei ole ristiriitaa huolimatta siitä, että ryhmä G ei välttämättä ole Abelin ryhmä, vaan itse asiassa kyseiset graafit ovat keskenään isomorfiset:

Lause 4.4. *Olkoon $\Gamma_1(G,S)$ graafi, jonka solmujoukko on G ja särmäjoukko on $\{\{g,gs\} \mid g \in G, s \in S \cup S^{-1}\}$. Olkoon lisäksi $\Gamma_2(G,S)$ graafi, jonka solmujoukko on G ja särmäjoukko on $\{\{g,sg\} \mid g \in G, s \in S \cup S^{-1}\}$. Tällöin graafit $\Gamma_1(G,S)$ ja $\Gamma_2(G,S)$ ovat isomorfiset.*

Todistus. Olkoon $f\colon G \to G$ graafien $\Gamma_1(G,S)$ ja $\Gamma_2(G,S)$ solmujoukkojen välinen kuvaus, jolle on voimassa $f(g) = g^{-1}$, kun $g \in G$. Todistetaan, että kuvaus f on määritelmän 2.8 mukainen graafi-isomorfismi. Koska ryhmä G on suljettu käänteisalkioiden suhteen, $f(g) \in G$ kaikilla g. Lisäksi f on selvästi bijektio ryhmän määritelmän nojalla.

Oletetaan, että solmujen g ja h välillä on särmä graafissa $\Gamma_1(G,S)$. Tällöin $h = gs$ jollakin $s \in S \cup S^{-1}$. Koska $(gs)^{-1} = s^{-1}g^{-1}$, graafien solmujoukot ovat samat ja oletuksen perusteella $s^{-1} \in S \cup S^{-1}$, niin graafissa $\Gamma_2(G,S)$ solmujen g^{-1} ja $s^{-1}g^{-1}$ välillä on särmä. Nyt

$$g^{-1} = f(g) \text{ ja } s^{-1}g^{-1} = f(gs),$$

ja koska kuvauksella f on selvästi käänteiskuvaus, joka on homomorfismi, bijektio f on isomorfismi. Täten graafit $\Gamma_1(G,S)$ ja $\Gamma_2(G,S)$ ovat isomorfiset. □

Cayleyn graafien määritelmä vaihtelee lähteestä riippuen huomattavan paljon. Tähän tutkielmaan valittu määritelmä antaa eksplisiittisen kuvauksen graafista, mikä ei ole aina itsestäänselvyys (ks. esim. [13], s. 262). Määritelmän valintaan on tietysti vaikuttanut myös luvun 5 päälähteenä käytettävässä Stongin artikkelissa [23] tehty määritelmän valinta, jota määritelmä 4.3 mukailee. Käydään seuraavaksi läpi muutamia Cayleyn graafien vaihtoehtoisia määritelmiä. Kohdan 1 määritelmää käytti mm. Cayley itse, kohdan 2 määritelmää puolestaan käyttää Meier [17] ja kohdan 3 määritelmää Stong artikkelinsa [23] tietyissä todistuksissa.

1. Cayleyn graafi on määritelmän 4.3 mukainen muotoa $\Gamma(G,S)$ oleva graafi, missä G on äärellinen ryhmä.

   Toisinaan Cayleyn graafien määritelmässä asetetaan rajoitteeksi sen ryhmän, jonka Cayleyn graafeja muodostetaan, äärellisyys. Tällöin selvästi myös Cayleyn graafit ovat aina äärellisiä. Jos taas ryhmä G on ääretön, ovat selvästi kaikki siitä muodostetut Cayleyn graafitkin äärettömiä. Itse asiassa Cayley itse tarkasteli 1800-luvun lopulla vain äärellisten ryhmien Cayleyn graafeja, ja vasta vuonna 1912 Dehn [6] määritteli äärettömien ryhmien Cayleyn graafit. Tässä tutkielmassa käytetty määritelmä ei edellytä tällaista kategorista jaottelua.

2. Cayleyn graafi määritellään muuten samoin kuin määritelmässä 4.3, mutta särmäjoukko on $\{(g,sg) \mid g \in G, s \in S \cup S^{-1}\}$, eli Cayleyn graafit ovat suunnattuja graafeja.

   Tämä määritelmä on itse asiassa ekvivalentti tässä tutkielmassa käytettävän määritelmän kanssa. Nimittäin kun $\Gamma(G,S)$ on suunnattu Cayleyn graafi ja $g \in G, s \in S \cup S^{-1}$, niin alkoiden g ja sg välillä on särmä, mutta toisaalta myös alkioiden sg ja $s^{-1}sg = g$ välillä on särmä. Ekvivalenssi seuraa siis siitä, että

alkioiden s sallitaan olevan joukon S alkioita tai niiden käänteisalkioita, eli toisin sanoen virittävä joukko määriteltiin nimenomaan alaluvussa 3.4 kuvatulla tavalla.

3. Cayleyn graafi on muotoa $\Gamma(G, S)$ oleva graafi, jolle ovat voimassa määritelmän 4.3 ehdot 1 ja 2, mutta jossa $S \subseteq G \setminus \{1\}$ ei välttämättä ole ryhmän G virittävä joukko.

   Tämä määritelmä on huomattavasti edellä esitettyjä laajempi. Luvussa 5 tullaan laajentamaan merkintää $\Gamma(G, S)$ siten, että joukko S saa olla mikä tahansa joukon G osajoukko, jolloin syntyy tämän määritelmän mukaisia graafeja. Kyseisiä graafeja ei kuitenkaan selkeyden vuoksi kutsuta Cayleyn graafeiksi.

On tärkeää huomata, että kaikki Cayleyn graafien määritelmät eivät suinkaan ole keskenään ekvivalentteja, jolloin myös niistä seuraavat Cayleyn graafien ominaisuudet vaihtelevat. Seuraavaksi todistetaan muutamia suoraan määritelmästä 4.3 johdettavissa olevia Cayleyn graafien ominaisuuksia. Ominaisuus 1 on mainittu lähteessä [3]. Ominaisuudet 2 ja 3 eivät välttämättä ole voimassa erilaisilla Cayleyn graafin määritelmillä, eikä niitä täten usein esitetä kirjallisuudessa.

Lause 4.5 (Cayleyn graafien ominaisuuksia)**.** *Seuraavat ominaisuudet ovat voimassa kaikille määritelmän 4.3 mukaisille Cayleyn graafeille.*

1. *Cayleyn graafit ovat yhtenäisiä.*

2. *Cayleyn graafit ovat yksinkertaisia.*

3. *Cayleyn graafi $\Gamma(G, S)$ on k-säännöllinen, kun $k = |S \cup S^{-1}|$.*

Todistus. Olkoon $\mathcal{G} = \Gamma(G, S)$ Cayleyn graafi, missä G on ryhmä ja $S \subseteq G \setminus \{1\}$ sen virittävä joukko.

1. Osana lauseen 4.2 todistusta todistettiin, että lauseessa 4.2 konstruoidut graafit ovat yhtenäisiä, ja lauseessa 4.4 todistettiin, että lauseen 4.2 konstruktio on ekvivalentti määritelmän 4.3 kanssa. Tämä todistaa väitteen.

2. Olkoon g Cayleyn graafin $\mathcal{G}$ solmu, jolloin $g \in G$. Koska $1 \notin S \cup S^{-1}$, ei millään $s \in S \cup S^{-1}$ ole voimassa $sg = g$. Täten graafissa $\mathcal{G}$ ei ole silmukoita. Lisäksi määritelmän 4.3 perusteella graafin $\mathcal{G}$ minkä tahansa kahden solmun välillä on korkeintaan yksi särmä, koska ryhmän G binäärioperaatio on hyvin määritelty. Täten graafi $\mathcal{G}$ on yksinkertainen.

3. Lauseen 4.2 todistuksen yhteydessä todistettiin, että ryhmään G ja kyseisen ryhmän virittävään joukkoon S liittyvässä lauseen 4.2 mukaisessa graafissa jokaisen solmun aste on $|S \cup S^{-1}|$, ja lauseessa 4.4, että lauseen 4.2 mukaiset graafit ovat isomorfisia määritelmän 4.3 mukaisten graafien kanssa. Tämä todistaa väitteen.

□

4.2 Esimerkkejä

Käydään sitten läpi esimerkkejä Cayleyn graafeista intuition selkeyttämiseksi ja ominaisuuksien tutkimiseksi. Esimerkit on järjestetty luonnollisella tavalla vaikeuden perusteella suunnilleen nousevaan järjestykseen. Esimerkkien 4.6 ja 4.7 ideat ovat peräisin Biggsin kirjasta [3]. Muut esimerkit perustuvat Meierin kirjaan [17]. Aloitetaan tarkastelemalla symmetristen ryhmien Cayleyn graafeja.

Esimerkki 4.6 (Symmetrisen ryhmän Cayleyn graafeja)**.** Esimerkissä 3.17 todettiin, että joukon $X = \{1, 2, 3\}$ permutaatiot muodostavat ryhmän S_X ja että esimerkiksi joukot $P_1 = \{(12), (23), (13)\}$ ja $P_2 = \{(12), (123)\}$ virittävät sen (esimerkki 3.35). Voidaan siis muodostaa Cayleyn graafit $\mathcal{G}_1 = \Gamma(S_X, P_1)$ ja $\mathcal{G}_2 = \Gamma(S_X, P_2)$.

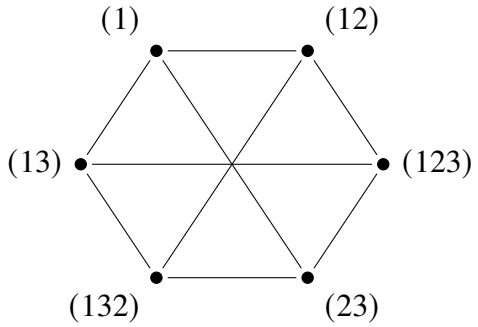
Aloitetaan graafista $\mathcal{G}_1$. Koska

$$(12) \circ (12) = (1), (23) \circ (23) = (1) \text{ ja } (13) \circ (13) = (1),$$

jokainen joukon P_1 alkio on oma käänteisalkionsa, eli $P_1^{-1} = P_1$. Täten riittää tarkastella graafin $\mathcal{G}_1$ särmien konstruoinnissa yksinomaan joukon P_1 alkioita. Nyt

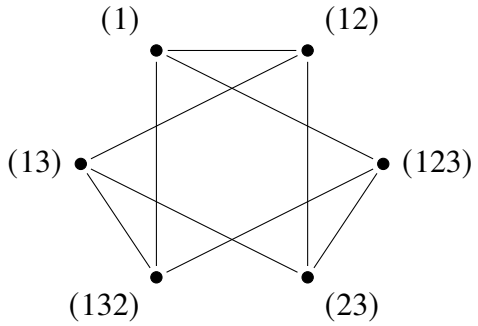
$$(12) \circ (1) = (12), (23) \circ (1) = (23) \text{ ja } (13) \circ (1) = (13),$$

joten solmuun (1) liittyvät särmät ovat tismalleen $\{(1), (12)\}$, $\{(1), (23)\}$ ja $\{(1), (13)\}$. Vastaavasti selvitetään muihin solmuihin liittyvät särmät. Lopputuloksena saadaan seuraava kuvan 4.3 mukainen graafi.

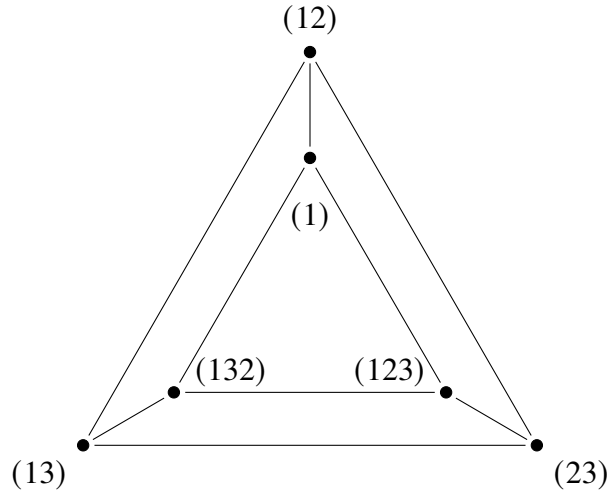


Kuva 4.3. Cayleyn graafi $\Gamma(S_X, P_1)$.

Vastaavasti muodostetaan graafi $\mathcal{G}_2$ suhteessa virittävään joukkoon $P_2 = \{(12), (123)\}$. Konstruoinnissa tulee huomioida, että syklin (123) käänteisalkio on (132), joten graafissa $\mathcal{G}_2$ tulee olemaan myös alkion (132) virittämiä särmiä. Muilta osin särmäjoukko selvitetään mekaanisesti samaan tapaan kuin edellä, joten tämä vaihe sivuutetaan. Järjestelmällä graafin $\mathcal{G}_2$ solmut uudelleen se saadaan kuvassa 4.5 esitettyyn muotoon, joka havainnollistaa ryhmän S_X rakennetta huomattavasti paremmin kuin kuva 4.4, minkä lisäksi graafin ulkoasu on uudessa muodossa huomattavasti edellistä elegantimpi. Sekä graafista $\mathcal{G}_1$ että graafista $\mathcal{G}_2$ havaitaan suoraan, että ne noudattavat lauseessa 4.5 esitettyjä Cayleyn graafien ominaisuuksia.



Kuva 4.4. Cayleyn graafi $\Gamma(S_X, P_2)$.

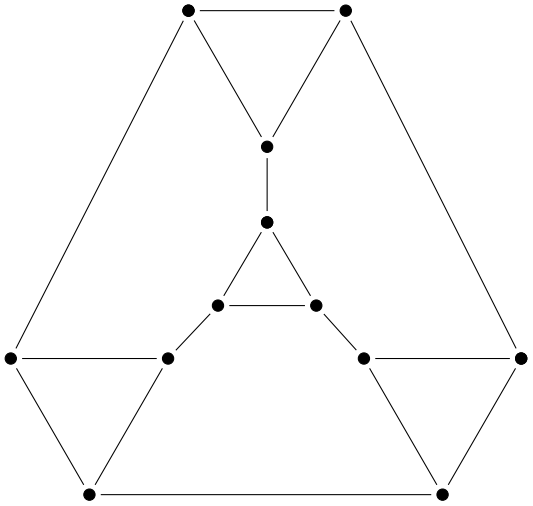


Kuva 4.5. Kuvan 4.4 Cayleyn graafi $\Gamma(S_X, P_2)$ uudelleen piirrettynä.

Edellinen esimerkki osoittaa, että Cayleyn graafit riippuvat aina paitsi siitä ryhmästä, jonka Cayleyn graafi muodostetaan, myös valitusta virittävästä joukosta. Samasta ryhmästä voidaan siis erilaisilla virittävän joukon valinnoilla muodostaa Cayleyn graafeja, joiden särmäjoukot eroavat toisistaan. Täten Cayleyn graafeja käsiteltäessä tulee aina mainita kyseessä olevaan Cayleyn graafiin liittyvä ryhmä ja virittävä joukko, eli esimerkiksi graafin $\Gamma(G, S)$ tapauksessa puhua ryhmän G Cayleyn graafista suhteessa virittävään joukkoon S. Toisaalta kirjoitetussa tekstissä yksinkertaisesti ilmaisu "Cayleyn graafi $\Gamma(G, S)$" on riittävä. Mikäli G ja S ovat kontekstissa selviä tai merkityksettömiä, voidaan puhua yleisesti Cayleyn graafeista.

Käydään läpi lisää esimerkkejä Cayleyn graafeista. Tästä eteenpäin Cayleyn graafien solmujen nimiä ei piirtoteknisistä syistä aina merkitä näkyviin, vaan tietyissä esimerkeissä käsitellään *merkitsemättömiä* Cayleyn graafeja.

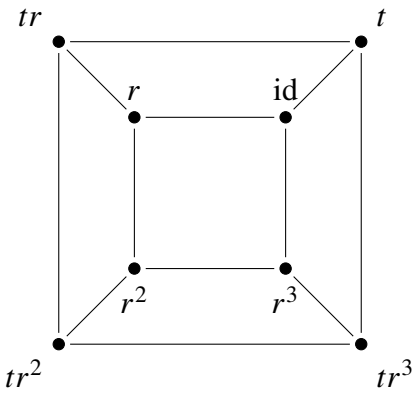
Esimerkki 4.7. Ryhmä A_4 on ryhmän $S_{\{1,2,3,4\}}$ aliryhmä, joka sisältää kaikki joukon $\{1, 2, 3, 4\}$ parilliset permutaatiot. Ryhmän A_4 alkiot ovat näin ollen syklinotaatiota käyttäen (1), (234), (243), $(12)(34)$, (123), (124), (132), (134), $(13)(24)$, (142), (143) ja $(14)(23)$. Kuva 4.6 esittää ryhmän A_4 Cayleyn graafia suhteessa virittävään joukkoon $S = \{(123), (12)(34)\}$.



Kuva 4.6. Cayleyn graafi $\Gamma(A_4, \{(123), (12)(34)\})$.

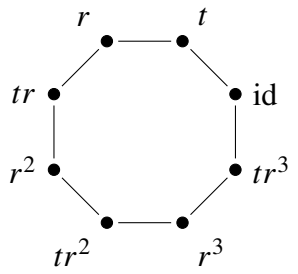
Vastaavasti ryhmälle A_5 voitaisiin muodostaa Cayleyn graafeja suhteessa erilaisiin virittäviin joukkoihin. Tämä kuitenkin sivuutetaan solmujen ja särmien suuresta lukumäärästä johtuvan piirtoteknisen monimutkaisuuden vuoksi. Ryhmän A_5 Cayleyn graafi suhteessa tiettyihin virittäviin joukkoihin esittää kolmiulotteisesti piirrettynä kuuluisan hiili-60-molekyylin eli fullereenimolekyylin pallomaista rakennetta (ks. [3], s. 127), minkä vuoksi kyseinen graafi on varsin elegantti.

Esimerkki 4.8 (Neliön symmetriaryhmän D_4 Cayleyn graafeja)**.** Edellisessä luvussa käsiteltiin neliön symmetriaryhmää D_4, ja esimerkissä 3.36 todettiin, että joukko $S_1 = \{r, t\}$ virittää ryhmän D_4. Kuvassa 4.7 on esitetty Cayleyn graafi $\Gamma(D_4, S_1)$. Graafi havainnollistaa erinomaisesti ryhmän D_4 rakennetta – erityisesti sitä, että ryhmä D_4 on isomorfinen puolisuoran tulon $\mathbb{Z}_4 \rtimes \mathbb{Z}_2$ kanssa (ks. esimerkki 3.62).



Kuva 4.7. Cayleyn graafi $\Gamma(D_4, \{r, t\})$.

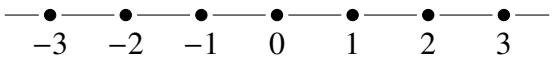
Toisaalta esimerkin 3.36 perusteella myös joukko $S_2 = \{t, tr^3\}$ virittää ryhmän D_4. Koska alkio tr^3 vastaa geometrisesti tulkittuna peilusta y-akselin suhteen, joukon S_2 voidaan ajatella koostuvan kahdesta vierekkäisestä peilauksesta. Virittävällä joukolla S_2 saadaan muodostettua kuvassa 4.8 esitetty Cayleyn graafi $\Gamma(D_4, S_2)$.



Kuva 4.8. Cayleyn graafi $\Gamma(D_4, \{t, tr^3\})$.

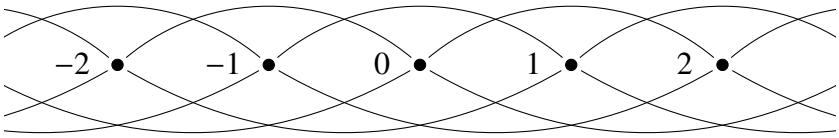
Toistaiseksi on tarkasteltu vain äärellisten ryhmien Cayleyn graafeja. Esitetään tästä syystä vielä kaksi havainnollistavaa esimerkkiä äärettömien ryhmien Cayleyn graafeista. Ensimmäisenä tarkastellaan kokonaislukujen yhteenlaskuryhmän $(\mathbb{Z}, +)$ Cayleyn graafeja.

Esimerkki 4.9. Minimaalinen kokonaislukujen yhteenlaskuryhmän virittävä joukko on $\{1\}$. Muodostetaan nyt Cayleyn graafi $\Gamma(\mathbb{Z}, \{1\})$. Kuvasta 4.9 huomataan, että se vastaa luonnollisella tavalla kokonaislukujen lukusuoraa.



Kuva 4.9. Cayleyn graafi $\Gamma(\mathbb{Z}, \{1\})$.

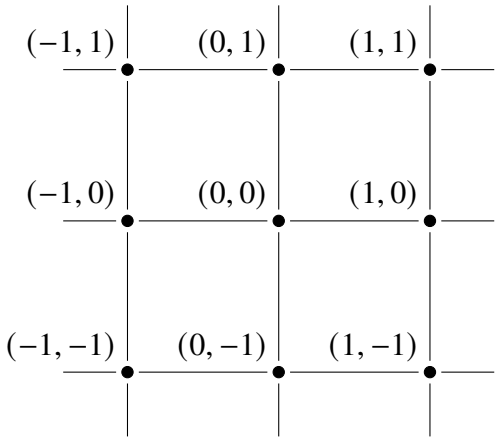
Virittävällä joukolla $\{2, 3\}$ samasta ryhmästä muodostuu hieman erilainen Cayleyn graafi, joka on esitetty kuvassa 4.10. Siinä havaitaan samantyyppistä rakennetta kuin edellisessä graafissa, ja lisääntyneestä monimutkaisuudesta huolimatta se säilyttää kokonaislukujen yhteenlaskuryhmän horisontaalisesti orientoituneen geometrisen muodon.



Kuva 4.10. Cayleyn graafi $\Gamma(\mathbb{Z}, \{2, 3\})$.

Muodostetaan vielä eräs suoran tulon $\mathbb{Z} \times \mathbb{Z}$ Cayleyn graafi.

Esimerkki 4.10. Määritelmän 3.58 mukaan kahden ryhmän $(\mathbb{Z}, +)$ suora tulo $\mathbb{Z} \times \mathbb{Z}$ on ryhmä. Selvästi esimerkiksi joukko $\{(1, 0), (0, 1)\}$ virittää sen – itse asiassa kyseinen virittävä joukko on myös minimaalinen – joten voidaan muodostaa Cayleyn graafi $\Gamma(\mathbb{Z} \times \mathbb{Z}, \{(1, 0), (0, 1)\})$. Kyseinen graafi on esitetty kuvassa 4.11.



Kuva 4.11. Cayleyn graafi $\Gamma(\mathbb{Z} \times \mathbb{Z}, \{(1,0),(0,1)\})$

4.3 Cayleyn graafien solmutransitiivisuudesta

Kirjallisuudessa (esim. [13], s. 262) esitetään toisinaan Cayleyn graafille seuraava määritelmä: graafi $\mathcal{G} = (V, E)$ on Cayleyn graafi, jos sillä on sellainen symmetriaryhmä H, että mille tahansa graafin $\mathcal{G}$ solmuille v ja w on olemassa täsmälleen yksi sellainen automorfismi $h \in H$ että $h(v) = w$. Tässä havaitaan selvä yhteys solmutransitiivisuuden määritelmään 2.16. Voitaisiinkin epämuodollisesti sanoa, että tämän määritelmän mukaan graafi $\mathcal{G}$ on Cayleyn graafi, jos ja vain jos se on ”yksikäsitteisesti” solmutransitiivinen. Kyseinen määritelmä voidaan todistaa yhtäpitäväksi perinteisemmän määritelmän 4.3 kanssa (ks. [13], s. 263). Tässä tutkielmassa tyydytään todistamaan, että määritelmän 4.3 mukaiset Cayleyn graafit ovat solmutransitiivisia. Todistus on peräisin Biggsin kirjasta [3], s. 123.

Lause 4.11. *Cayleyn graafit ovat solmutransitiivisia.*

Todistus. Olkoon $\mathcal{G} = \Gamma(G, S)$ Cayleyn graafi, olkoot v, w mitä tahansa graafin $\mathcal{G}$ solmuja ja olkoon $g \in G$. Tällöin g on myös graafin $\Gamma(G, S)$ solmu. Määritellään graafin $\Gamma(G, S)$ automorfismi π seuraavasti:

$$\pi_g(h) = gh \text{ kaikilla } h \in G.$$

Lauseen 4.2 todistuksessa havaittiin, että tämä kuvaus todella on graafin $\Gamma(G, S)$ automorfismi.

Koska v ja w ovat Cayleyn graafin $\mathcal{G}$ solmuja, on voimassa $v, w \in G$, ja koska G on ryhmä, on lisäksi voimassa $wv^{-1} \in G$. Edelleen

$$\pi_{wv^{-1}}(v) = (wv^{-1})v = w(v^{-1}v) = w \cdot 1 = w,$$

mistä seuraa määritelmän 2.16 nojalla, että Cayleyn graafi $\mathcal{G}$ on solmutransitiivinen. □

Vaikka kaikki Cayleyn graafit ovat solmutransitiivisia, ja ”yksikäsitteisesti” solmutransitiiviset graafit ovat Cayleyn graafeja, yleisesti kaikki solmutransitiiviset graafit eivät suinkaan ole Cayleyn graafeja. Tämä havaitaan seuraavasta esimerkistä, joka on jatkoa esimerkille 2.17.

Esimerkki 4.12. Esimerkissä 2.17 piirrettiin Petersenin graafi ja todettiin, että se on solmutransitiivinen. Lisäksi Petersenin graafi toteuttaa kaikki lauseen 4.5 mukaiset Cayleyn graafien ominaisuudet. Petersenin graafi ei kuitenkaan ole Cayleyn graafi. Väitteen todentaminen ei ole tässä vaiheessa käytössä olevien määritelmien ja tulosten avulla mahdollista, joten yksityiskohdat sivuutetaan. Biggsin kirjaan [3] (s. 124) pohjautuvan päättelyn idea on seuraava:

Oletetaan, että Petersenin graafi on Cayleyn graafi, eli että se on muotoa $\Gamma(G, S)$ jollakin ryhmällä G ja ryhmän G virittävällä joukolla $S \subseteq G \setminus \{1\}$. Petersenin graafissa on 10 solmua, joten ryhmän G kertaluvun tulee olla 10. Kertalukua 10 olevia ryhmiä on itse asiassa vain kaksi, nimittäin säännöllisen viisikulmion diedriryhmä ja kertalukua 10 oleva syklinen ryhmä [18]. Koska Petersenin graafi on 3-säännöllinen, täytyy olla $|S \cup S^{-1}| = 3$. Käymällä molempien ryhmien osalta kaikki tällaiset virittävät joukot läpi havaitaan, ettei niistä yhdelläkään muodostu Petersenin graafia. Täten oletuksen siitä, että Petersenin graafi on Cayleyn graafi, täytyy olla väärä.

Edellisessä esimerkissä jouduttiin käymään läpi kaikki vaihtoehdot, jotta saatiin todistettua, ettei Petersenin graafi ole Cayleyn graafi. Myös yleisesti ottaen kysymys siitä, milloin graafi ei ole Cayleyn graafi, on varsin hankala, sillä graafi voi hyvin toteuttaa lauseessa 4.5 todistetut Cayleyn graafien ominaisuudet ja olla solmutransitiivinen, vaikka se ei silti ole Cayleyn graafi. Graafin koon kasvaessa myös kaikkien tapausten läpikäynti hankaloituu. Käänteiseen kysymykseen siitä, milloin graafi on Cayleyn graafi, sen sijaan on selkeä, vaikkakaan ei kovin yksinkertainen, vastaus, joka tunnetaan Sabidussin lauseena. Lauseen esitti ja todisti tiettävästi ensimmäisenä itävaltalainen matemaatikko Gert Sabidussi vuoden 1958 artikkelissaan [21].

5 Cayleyn graafien 1-faktorointikonjektuuri

Tässä luvussa tarkastellaan Cayleyn graafien 1-faktorointikonjektuuria, jonka mukaan jokainen Cayleyn graafi $\Gamma(G, S)$, missä ryhmän G kertaluku on parillinen, on 1-faktoroituva. Luvun ensimmäisessä alaluvussa 5.1 määritellään, mitä tarkoitetaan j-faktorilla ja 1-faktoroituvuudella, ja annetaan näistä käsitteistä esimerkkejä. Lisäksi esitetään konjektuuri täsmällisessä muodossa. Alaluvussa 5.2 puolestaan todistetaan konjektuurin osatulosten todistuksissa tarvittava Vizingin lause. Alaluvun 5.1 päälähteenä on käytetty Stongin artikkelia [23], kun taas alaluku 5.2 pohjautuu Jungnickelin kirjaan [13]. Alaluvussa 5.3 todistetaan Stongin [23] ja Abdollahin [1] artikkeleihin perustuen eräitä konjektuurin osatuloksia äärellisille ryhmille. Lopulta alaluvussa 5.4 yleistetään muutamia alaluvun 5.3 todistuksia numeroituvasti äärettömille ryhmille Stongin artikkelin perusteella.

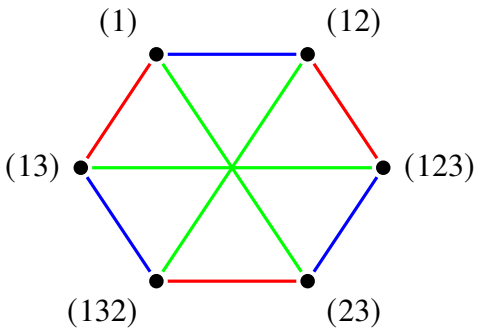
5.1 1-faktoroituvuus

Aloitetaan Cayleyn graafien 1-faktorointikonjektuurin tarkastelussa tarvittavien käsitteiden määrittely esittämällä yleisen j-faktorin määritelmä. 1-faktori määritellään j-faktorin erityistapauksena.

Määritelmä 5.1 (j-faktori)**.** Graafin $\mathcal{G}$ j-faktori on graafin $\mathcal{G}$ virittävä aligraafi, joka on j-säännöllinen, $j \in \mathbb{Z}_+$.

Määritelmän 5.1 mukaan j-faktori on ensinnäkin graafi. Toiseksi se sisältää kaikki samat solmut kuin alkuperäinen graafi, mutta särmiä on poistettu siten, että jokaisen solmun aste on j. On ilmeistä, että jos $\delta(\mathcal{G}) = k$, missä $\delta(\mathcal{G})$ on graafin $\mathcal{G}$ solmujen minimiaste (ks. määritelmä 2.6), niin graafilla $\mathcal{G}$ ei voi olla j-faktoria, jos $j > k$.

Esimerkki 5.2 (1-faktori)**.** Määritelmän 5.1 mielenkiintoinen erityistapaus saadaan valinnalla $j = 1$. Tällöin päädytään 1-faktoriin eli sellaiseen graafin $\mathcal{G}$ virittävään aligraafiin, jossa jokaiseen solmuun liittyy täsmälleen 1 särmä. Kuvassa 5.1 on esitetty esimerkistä 4.6 tutun Cayleyn graafin $\Gamma(S_X, \{(12), (23), (13)\})$, $X = \{1, 2, 3\}$, erilliset 1-faktorit eri väreillä korostettuina.



Kuva 5.1. Cayleyn graafin $\Gamma(S_X, \{(12), (23), (13)\})$ 1-faktorit.

Huomautus. Osittain vaihtoehtoinen nimi kirjallisuudessa 1-faktorille on *täydellinen sovitus* (englanniksi *perfect matching*). Sovitus tarkoittaa suuntaamattoman graafin särmäjoukon osajoukkoa, jossa mitkään kaksi särmää eivät liity samaan solmuun. Täydellinen sovitus puolestaan on sovitus, jossa jonkin särmän päätesolmuna kukin alkuperäisen graafin solmu on täsmälleen kerran. Täydellisen sovituksen käsitteen johtoajatus vastaa siis 1-faktorin käsitettä, mutta koska sovitukset ovat särmäjoukkoja eivätkä graafeja, ei täydellisen sovituksen käsite ole ekvivalentti 1-faktorin määritelmän kanssa. [16]

Edellisessä esimerkissä muodostettiin itse asiassa tarkastellun Cayleyn graafin 1-faktorointi. Määritellään tämä käsite vielä täsmällisesti.

Määritelmä 5.3 (1-faktorointi)**.** Graafin $\mathcal{G} = (V, E)$ 1-faktorointi on sen särmäjoukon E sellainen ositus, että jokainen ositukseen kuuluva osajoukko muodostaa yhdessä solmujoukon V kanssa graafin $\mathcal{G}$ 1-faktorin. Jos graafilla on 1-faktorointi, sanotaan, että se on 1-faktoroituva.

1-faktorointi (tai yleisemmin j-faktorointi) ei välttämättä ole yksikäsitteinen, eli samalla graafilla voi olla useita 1-faktorointeja. Yleisesti ottaen ei kuitenkaan ole järin kiinnostavaa, kuinka monta 1-faktorointia graafilla on, vaan se, onko 1-faktorointia ylipäänsä olemassa. Loppututkielmassa keskitytäänkin nimenomaan jälkimmäiseen kysymykseen.

Tutkielmassa ei ole vielä esitetty Cayleyn graafien 1-faktorointikonjektuurin täsmällistä muotoilua, mikä on välttämätöntä sen osatulosten todistamiseksi. Perustellaan konjektuurin mielekkyyttä kuitenkin hieman ennen sen varsinaista esittämistä. 1-faktoroituvuuteen liittyy nimittäin seuraava lause, joka antaa riittävän ehdon 1-faktorin olemassaololle.

Lause 5.4. *Jos $\mathcal{G}$ on yhtenäinen ja solmutransitiivinen graafi, jossa on parillinen määrä solmuja, niin graafilla $\mathcal{G}$ on 1-faktori.*

Todistus. Sivuutetaan tarvittavien esitietojen laajuuden vuoksi. Tulos on esitetty Diestelin kirjassa [7] sivulla 55 harjoitustehtävänä. □

Edellisen lauseen havainto perustelee Cayleyn graafien 1-faktorointikonjektuurin esittämistä, vaikkakaan se ei suoraan koske Cayleyn graafeja. Tuntuisi nimittäin

luontevalta, että jos yhtenäisillä solmutransitiivisilla graafeilla, joissa on parillinen määrä solmuja, on 1-faktori, niin kertaluvultaan parillisiin ryhmiin liittyvillä Cayleyn graafeilla, jotka ovat lauseen 4.5 perusteella solmutransitiivisia ja yhtenäisiä, olisi 1-faktorointi. Esitetään tämän havainnon pohjustamana konjektuurin täsmällinen muotoilu lähdettä [13] mukaillen.

Konjektuuri 5.5. Olkoon G ryhmä, jonka kertaluku on parillinen, $S \subseteq G \setminus \{1\}$ ja $G = \langle S \rangle$. Tällöin Cayleyn graafi $\Gamma(G, S)$ on 1-faktoroituva.

5.2 Vizingin lause

Iso osa tunnetuista Cayleyn graafien 1-faktorointikonjektuurin osatulosten todistuksista pohjautuu enemmän tai vähemmän Vizingin lauseeseen, jonka mukaan minkä tahansa graafin $\mathcal{G}$ särmät ovat särmäväritettävissä joko k:lla tai $k+1$:llä värillä, missä k on graafin $\mathcal{G}$ solmujen maksimiaste. Tämän alaluvun tavoitteena on todistaa Vizingin lause. Tarkastellaan ennen sitä graafien särmävärityksiä yleisesti. Määritellään ensin, mitä graafin särmävärityksellä tarkoitetaan.

Määritelmä 5.6 (Graafin särmäväritys)**.** Graafin $\mathcal{G} = (V, E)$ särmäväritys on sellainen kuvaus $\alpha\colon E \to C$, missä C on joukko värejä, että jokainen samaan solmuun liittyvä särmä kuvautuu eri värille.

Yleensä graafien särmävärityksissä ollaan kiinnostuneita siitä, kuinka monta väriä graafin värittämiseen vähintään tarvitaan. Aiheen käsittelyä helpottaa seuraavaksi määriteltävä kromaattisen indeksin käsite.

Määritelmä 5.7 (Kromaattinen indeksi)**.** Graafin $\mathcal{G}$ kromaattinen indeksi $\chi'(\mathcal{G})$ on pienin värien lukumäärä, joka tarvitaan graafin $\mathcal{G}$ särmäväritykseen.

Toisinaan kirjallisuudessa Cayleyn graafit määritellään särmävärityksien avulla. Itse asiassa Cayley itsekin teki näin vuoden 1878 artikkelissaan [4]. Kyseisen määritelmän mukaan Cayleyn graafi on suunnattu ja väritetty graafi, jonka solmu- ja särmäjoukot ovat määritelmän 4.3 mukaiset, mutta jokainen särmä $\{g, sg\}, g \in G$, $s \in S \cup S^{-1}$, on lisäksi väritetty alkiota s vastaavalla värillä, kun jokaiseen $s \in S \cup S^{-1}$ liittyy täsmälleen yksi väri. Väritykset liittyvät siis olennaisesti Cayleyn graafien historiaan, minkä lisäksi graafin piirtämisen yhteydessä ne korostavat käsiteltävän ryhmän geometrista luonnetta ja rakennetta. Täten osa konkreettisuudesta menetetään, kun värityksistä luovutaan.

Todistetaan seuraavaksi aiemmin mainittu Vizingin lause. Muistutettakoon lukijaa, että määritelmän 2.6 mukaan merkinnällä $\Delta(\mathcal{G})$ tarkoitetaan graafin $\mathcal{G}$ solmujen maksimiastetta. Otetaan lisäksi käyttöön uusi merkintä: kun α ja β ovat mitä tahansa värejä ja $\mathcal{G}$ on graafi, $\mathcal{G}(\alpha, \beta)$ on se graafin $\mathcal{G}$ virittävä aligraafi, jonka särmät ovat tismalleen ne graafin $\mathcal{G}$ särmät, jotka on väritetty joko värillä α tai värillä β. Selvästi särmävärityksen määritelmän nojalla graafin $\mathcal{G}(\alpha, \beta)$ yhtenäiset komponentit ovat polkuja, joiden pituus on yksi tai parillinen ja joiden särmät on vuorotellen väritetty värillä α ja värillä β. Lisäksi värien α ja β vaihtaminen päittäin missä tahansa graafin $\mathcal{G}(\alpha, \beta)$ yhtenäisessä komponentissa tuottaa aidosti alkuperäisestä eroavan värityksen.

Lause 5.8 (Vizingin lause)**.** *Mille tahansa graafille* $\mathcal{G} = (V, E)$ *on voimassa joko* $\chi'(\mathcal{G}) = \Delta(\mathcal{G})$ *tai* $\chi'(\mathcal{G}) = \Delta(\mathcal{G}) + 1$.

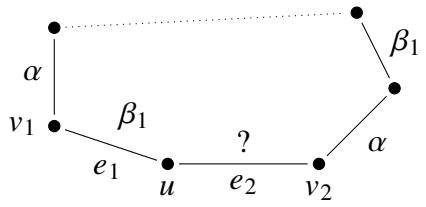
Todistus. Olkoon $\mathcal{G}$ graafi. Voidaan olettaa, että $\mathcal{G}$ on yhtenäinen, sillä mikäli näin ei ole, graafi $\mathcal{G}$ koostuu yhtenäisistä komponenteista, ja väite voidaan todistaa mielivaltaiselle komponentille. Selvästi $\chi'(G) \geq \Delta(G)$ särmävärityksen määritelmän nojalla. Todistetaan induktiolla luvun $m = |E|$ suhteen, että $\chi'(\mathcal{G}) \leq \Delta(\mathcal{G}) + 1$. Yhdessä näistä epäyhtälöistä seuraa, että joko $\chi'(\mathcal{G}) = \Delta(\mathcal{G})$ tai $\chi'(\mathcal{G}) = \Delta(\mathcal{G}) + 1$.

Induktioväite on triviaalisti voimassa perustapauksessa $m = 1$, jolloin siis graafissa $\mathcal{G}$ on yksi särmä, joka voidaan värittää täsmälleen yhdellä värillä. Valitaan nyt jokin graafin $\mathcal{G}$ särmä $e_1 = \{u, v_1\}, u, v_1 \in V$, ja tehdään induktio-oletus: graafi $\mathcal{G}' = (V, E \setminus \{e_1\})$ on väritetty käyttäen korkeintaan $\Delta(\mathcal{G}') + 1$ väriä. Induktioväitteen todistuksen idea on käyttää tätä väritystä graafin $\mathcal{G}$ särmävärityksen konstruoimiseen.

Tehdään ensin yleinen induktio-oletuksesta seuraava graafin $\mathcal{G}'$ särmäväritystä koskeva havainto. Koska graafin solmujen maksimiasteen määritelmän perusteella solmun v aste graafissa $\mathcal{G}'$ on korkeintaan $\Delta(\mathcal{G}')$ ja induktio-oletuksen mukaan graafi $\mathcal{G}'$ voidaan värittää käyttäen korkeintaan $\Delta(\mathcal{G}') + 1$ väriä, on olemassa ainakin yksi väri γ, jolla ei ole väritetty mitään solmuun v liittyvää särmää graafin $\mathcal{G}'$ särmävärityksessä.

Siirrytään sitten varsinaiseen induktioväitteen todistukseen. Jos graafissa $\mathcal{G}$ missään solmuihin u tai v_1 liittyvissä särmissä ei ole käytetty jotakin samaa väriä, voidaan särmä $e_1 = \{u, v_1\}$ värittää kyseisellä värillä. Kyseisellä särmällä ei tietenkään valmiiksi ollut väriä, koska sitä ei ole graafissa $\mathcal{G}'$. Oletetaan nyt toisaalta, että solmuun u liittyvissä särmissä ei ole käytetty väriä α ja että solmuun v_1 liittyvissä särmissä ei ole käytetty väriä $\beta_1 \neq \alpha$. Voidaan lisäksi olettaa, että jokin solmuun v_1 liittyvä särmä on väritetty värillä α ja jokin solmuun u liittyvä särmä on väritetty värillä β_1. Olkoon jälkimmäinen särmä $e_2 = \{u, v_2\}$. Muutetaan vielä edellä konstruoitua väritystä seuraavasti: annetaan särmälle e_1 väri β_1 ja poistetaan särmältä e_2 väri kokonaan.

Tarkastellaan nyt tilannetta sen perusteella, mikä väri puuttuu solmuun v_2 liittyvien särmien värien joukosta. Jos kyseinen väri on α, voidaan särmä e_2 värittää värillä α, mikä takaa halutun lopputuloksen. Oletetaan siis, että värillä α on väritetty jokin solmuun v_2 liittyvä särmä. Mikäli solmu v_2 ei sijaitse samassa graafin $\mathcal{G}(\alpha, \beta_1)$ yhtenäisessä komponentissa kuin solmut u ja v_1, voidaan värit α ja β_1 vaihtaa solmun v_2 sisältävässä komponentissa siten, että väri α ei liity mihinkään solmuun v_2 liittyvään särmään, ja edelleen kyseinen väri ei liity myöskään mihinkään solmuun u liittyvään särmään. Tällöin asetetaan graafissa $\mathcal{G}$ väri α särmälle e_2. Muussa tapauksessa solmut u, v_1 ja v_2 sijaitsevat samassa graafin $\mathcal{G}(\alpha, \beta_1)$ komponentissa, mikä edelleen tarkoittaa graafin $\mathcal{G}(\alpha, \beta_1)$ ominaisuuksien nojalla, että solmujen u ja v_2 välillä on polku, jossa joka toinen särmä on väritetty värillä α ja joka toinen värillä β_1, eli värit α ja β_1 vuorottelevat. Tämä polku yhdessä värittämättömän särmän e_2 kanssa muodostaa syklin, joka on esitetty kuvassa 5.2.



Kuva 5.2. Solmut u, v_1 ja v_2 sisältävä sykli graafissa $\mathcal{G}$.

Oletetaan sitten, että se väri, joka puuttuu solmuun v_2 liittyvistä särmistä, on väri $\beta_2 \neq \beta_1$. Voidaan lisäksi olettaa, että tällä värillä on väritetty jokin solmuun u liittyvä särmä – muussa tapauksessa voitaisiin nimittäin antaa särmälle e_2 väri β_2, jolloin saavutettaisiin haluttu väritys. Olkoon nyt $e_3 = \{u, v_3\}$ se särmä, joka on väritetty värillä β_2. Muutetaan edellä konstruoitua väritystä seuraavasti: annetaan särmälle e_2 väri β_2 ja poistetaan särmältä e_3 väri toistaiseksi kokonaan. Vastaavasti kuten edellä voidaan olettaa, että värillä α on väritetty jokin solmuun v_3 liittyvä särmä ja että solmut u, v_2 ja v_3 sijaitsevat samassa graafin $\mathcal{G}(\alpha, \beta_2)$ yhtenäisessä komponentissa, sillä muuten voitaisiin etsiä särmälle e_2 jokin sopiva väri, jolloin saataisiin haluttu väritys. Näin ollen solmujen u ja v_3 välillä on polku graafissa $\mathcal{G}(\alpha, \beta_2)$, jonka särmissä vuorottelevat värit α ja β_2. Tämä polku muodostaa yhdessä toistaiseksi värittämättömän särmän e_3 kanssa syklin. Näin ollen on löydetty kaksi sykliä, joissa särmien värit vaihtelevat.

Jatketaan edelleen graafin $\mathcal{G}$ särmävärityksen konstruoimista edellä kuvatulla tavalla, kunnes löydetään sellainen solmun u naapurisolmu v_k, että särmää $e_k = \{u, v_k\}$ ei ole vielä väritetty millään värillä ja jompikumpi seuraavista ehdoista on voimassa:

1. Jokin väri $\beta_k \neq \beta_{k-1}$ puuttuu solmuun v_k liittyvien särmien värien joukosta, ja tällä värillä ei ole väritetty myöskään mitään solmuun u liittyvää särmää.

2. Jokin väri $\beta_i, i \leq k-2$, puuttuu solmuun v_k liittyvien särmien värien joukosta.

Toinen edellisistä ehdoista väistämättä toteutuu jollakin k, koska solmulla u on korkeintaan $d(u) \leq \Delta(\mathcal{G})$ naapurisolmua.

Tapauksessa 1 särmälle e_k voidaan antaa puuttuva väri, jolloin on saatu muodostettua haluttu väritys. Tapauksessa 2 päätellään seuraavasti: Kuten aiemminkin, voidaan olettaa, että solmut u, v_i ja v_{i+1} sijaitsevat samassa graafin $\mathcal{G}(\alpha, \beta_i)$ yhtenäisessä komponentissa. Tämä komponentti on solmujen u ja v_{i+1} välinen polku, jossa värit α ja β_i vuorottelevat. Merkitään tätä polkua symbolilla P. Polku P ei sisällä solmua v_k, koska värillä β_i ei ole väritetty yhtään solmuun v_k liittyvää särmää. Täten se graafin $\mathcal{G}(\alpha, \beta_i)$ komponentti C, joka sisältää solmun v_k, ja polku P ovat graafin $\mathcal{G}(\alpha, \beta_i)$ ominaisuuksien nojalla erillisiä. Vaihdetaan nyt värit α ja β_i päittäin komponentissa C ja annetaan särmälle e_k väri α, jolloin on viimein saatu muodostettua haluttu väritys.

Graafille $\mathcal{G}$ on voimassa $\Delta(\mathcal{G}) = \Delta(\mathcal{G}')$ tai $\Delta(\mathcal{G}) = \Delta(\mathcal{G}') + 1$. Ensimmäisessä tapauksessa on voimassa $\chi'(\mathcal{G}) = \chi'(\mathcal{G}')$ ja jälkimmäisessä tapauksessa $\chi'(\mathcal{G}) = \chi'(\mathcal{G}') + 1$ edellä esitetyn graafin $\mathcal{G}$ särmävärityksen konstruktion nojalla. Induktio-oletuksen mukaan $\chi'(\mathcal{G}') \leq \Delta(\mathcal{G}') + 1$, joten kummassakin tapauksessa

$\chi'(\mathcal{G}) \leq \Delta(\mathcal{G})+1$. Siispä induktioväite on todistettu, mistä päätellään ensimmäisessä kappaleessa kuvatulla tavalla, että $\chi'(\mathcal{G}) = \Delta(\mathcal{G})$ tai $\chi'(\mathcal{G}) = \Delta(\mathcal{G}) + 1$. □

Vizingin lause ei ole suoraan järin hyödyllinen Cayleyn graafien 1-faktorointikonjektuurin osatulosten todistamisessa. Sen sijaan seuraavaksi todistettava Vizingin lauseen seuraus on tietyissä todistuksissa hyvin keskeinen. Seurauksen mukaan se, että k-säännöllinen Cayleyn graafi $\Gamma(G, S)$, missä ryhmän G kertaluku on parillinen, on 1-faktoroituva, on yhtäpitävää sen kanssa, että kyseisen graafin särmien värittämiseen tarvitaan vähintään k eri väriä. Koska $k = |S \cup S^{-1}|$, tämä merkitsee edelleen sitä, että särmävärityksessä käytetään yhtä monta väriä kuin joukossa $S \cup S^{-1}$ on alkioita.

Seuraus 5.9. *Olkoon $\mathcal{G}$ k-säännöllinen yksinkertainen graafi, jossa on n solmua. Tällöin $\chi'(\mathcal{G}) = k + 1$, jos n on pariton. Jos n on parillinen, niin on voimassa $\chi'(\mathcal{G}) = k$, jos ja vain jos graafi $\mathcal{G}$ on 1-faktoroituva.*

Todistus. Oletetaan ensin, että n on pariton, eli $n = 2m + 1$ jollakin $m \in \mathbb{N}$. Olkoon α jokin väri. Koska graafi $\mathcal{G}$ on yksinkertainen, kuhunkin solmuun liittyy enintään $2m$ särmää. Jos nyt jokin särmä väritetään värillä α, muita sen päätesolmuihin liittyviä särmiä ei voida enää värittää värillä α graafin $\mathcal{G}$ särmävärityksessä. Koska graafissa $\mathcal{G}$ on $n = 2m + 1$ solmua, väri α voidaan täten liittää enintään $\left\lfloor \frac{2m+1}{2} \right\rfloor = m$ särmään. Koska graafissa $\mathcal{G}$ on yhteensä

$$\frac{k(2m + 1)}{2} > mk$$

särmää, ei voi olla $\chi'(\mathcal{G}) = k$. Tällöin Vizingin lauseen (lause 5.8) nojalla täytyy olla $\chi'(\mathcal{G}) = k + 1$.

Oletetaan sitten, että n on parillinen, eli $n = 2m$ jollakin $m \in \mathbb{N}$. Samaan tapaan kuin edellä päätellään, että $\chi'(\mathcal{G}) = k$, jos ja vain jos jokainen väri liitetään tismalleen m särmään. Tämä on yhtäpitävää sen kanssa, että graafin $\mathcal{G}$ särmäväritys muodostaa kyseisen graafin 1-faktoroinnin, koska tietyllä värillä väritetyt särmät muodostavat graafin $\mathcal{G}$ 1-faktorin särmävärityksen määritelmän nojalla. □

5.3 Äärelliset ryhmät

Tässä alaluvussa todistetaan Cayleyn graafien 1-faktorointikonjektuurin osatuloksia Stongin [23] ja Abdollahin [1] artikkeleihin pohjautuen. Luvun päälähteenä on käytetty Stongin artikkelia. Abdollahin artikkelia käytetään toissijaisena lähteenä, koska siinä todistetaan vahvempi muoto eräästä Stongin esittämästä tuloksesta. Apulause 5.24, lause 5.25 ja seuraus 5.26 ovat peräisin Abdollahilta, muuten sisältö on peräisin Stongilta ja muutamissa kohdin tutkielman kirjoittajalta. Jungnickelin kirjassa [13] on yksinkertaistetut versiot lauseen 5.10 kohtien 1 ja 2 todistuksista, ja vaikka kyseisiä todistuksia ei ole tässä tutkielmassa hyödynnetty, lukija voi tarpeen mukaan käyttää Jungnickelin kirjaa tämän alaluvun oheislukemistona.

Tässä alaluvussa oletetaan, että kaikki käsiteltävät ryhmät ja täten niihin liittyvät Cayleyn graafit ovat äärellisiä. Useimmat todistettavat tulokset yleistyvät lähes sellaisinaan äärettömille ryhmille, mutta esimerkiksi ryhmän ja sen alkioiden kertaluvun

yhteyttä käsiteltäessä oletus ryhmien äärellisyydestä on tärkeä. Äärettömiä ryhmiä käsitellään lyhyesti seuraavassa alaluvussa 5.4.

Seuraavat kaksi lausetta esittävät koostetusti Stongin artikkelin päätulokset. Lauseiden todistamisessa käytetään hieman standardista poikkeavaa esitystapaa, eli itse lauseet esitetään todistuksetta nyt alaluvun alussa, ja vasta myöhemmin lauseet todistetaan kohta kohdalta. Lauseen 5.10 kohta 1 on seuraus 5.16, kohta 2 on seuraus 5.21, ja kohta 3 diedriryhmiin rajattuna on seuraus 5.22. Lauseen 5.11 kohta 1 laajennettuna kaikille virittäville joukoille on seuraus 5.26. Lauseen 5.11 kohtien 2 ja 3 todistuksia ei tutkielman laajuuden rajaustarpeen vuoksi esitetä lainkaan. Lisäksi lauseen 5.10 kohta 3 todistetaan vain diedriryhmille, sillä disyklisiä ryhmiä ei tässä tutkielmassa määritellä.

Lause 5.10. *Olkoon G ryhmä. Cayleyn graafi $\Gamma(G, S)$ on 1-faktoroituva kaikilla ryhmän G virittävillä joukoilla $S \subseteq G \setminus \{1\}$, jos jokin seuraavista ehdoista on voimassa.*

1. *Ryhmän G kertaluku on 2^k, missä $k \in \mathbb{Z}_+$.*
2. *Ryhmä G on Abelin ryhmä, jonka kertaluku on parillinen.*
3. *Ryhmä G on diedriryhmä tai disyklinen ryhmä.*

Lause 5.11. *Olkoon G ryhmä. Cayleyn graafi $\Gamma(G, S)$ on 1-faktoroituva kaikilla ryhmän G minimaalisilla virittävillä joukoilla $S \subseteq G \setminus \{1\}$, jos jokin seuraavista ehdoista on voimassa.*

1. *Ryhmä G on parillista kertalukua oleva nilpotentti ryhmä.*
2. *Ryhmällä G on aito normaali aliryhmä, joka on Abelin ryhmä ja jonka indeksi ryhmässä G on 2^k.*
3. *Ryhmän G kertaluku on $2^m p^n$, missä m ja n ovat luonnollisia lukuja ja p on sellainen alkuluku, että $p > 2^m$.*

Ennen edellä mainittujen tulosten todistamista yleistetään merkintää $\Gamma(G, S)$ apulauseen 5.14 todistuksen syntaktisten yksityiskohtien selkeyttämiseksi. Vastedes merkinnällä $\Gamma(G, S)$ tarkoitetaan graafia, jonka solmujoukko on G ja särmäjoukko on $\{\{g, sg\} \mid g \in G, s \in S \cup S^{-1}\}$, missä $S \subseteq G \setminus \{1\}$. Tässä joukon S ei siis tarvitse olla ryhmän G virittävä joukko, vaikka käytetään määritelmän 4.3 mukaista notaatiota $\Gamma(G, S)$. Tällaisista graafeista ei kuitenkaan puhuta Cayleyn graafeina vaan yksinkertaisesti muotoa $\Gamma(G, S)$ olevina graafeina. Mikäli joukko S on ryhmän G virittävä joukko, tämä mainitaan erikseen ja puhutaan ryhmän G Cayleyn graafista suhteessa virittävään joukkoon S.

Monet luvussa 4 todistetut ominaisuudet ovat voimassa vain sellaisille graafeille $\Gamma(G, S)$, jotka ovat määritelmän 4.3 mukaisesti Cayleyn graafeja. Esimerkkinä todettakoon, että kaikki Cayleyn graafit $\Gamma(G, S)$ ovat yhtenäisiä, mutta jos S ei ole ryhmän G virittävä joukko, graafi $\Gamma(G, S)$ ei ole yhtenäinen vaan koostuu erillisistä graafin $\Gamma(G, S)$ aligraafeista, joista jokaisen indusoi jokin ryhmän $\langle S \rangle$ sivuluokka. Koska

ryhmän sivuluokat ovat mahtavuudeltaan yhtäsuuria ja matemaattiselta rakenteeltaan samanlaisia, seuraa kyseisestä tuloksesta edelleen, että muotoa $\Gamma(G, S)$ olevan graafin yhtenäiset komponentit ovat erillisiä ja keskenään isomorfisia graafeja. Tulosta tullaan itse asiassa tarvitsemaan myöhemmin, joten todistetaan se.

Apulause 5.12. Olkoon G ryhmä, $S \subseteq G \setminus \{1\}$ ja $\Gamma(G, S)$ graafi, jonka solmujoukko on G ja särmäjoukko on $\{\{g, sg\} \mid g \in G, s \in S \cup S^{-1}\}$. Jos S ei ole ryhmän G virittävä joukko, graafi $\Gamma(G, S)$ koostuu yhtenäisistä, keskenään erillisistä graafin $\Gamma(G, S)$ aligraafeista, joista jokaisen indusoi jokin ryhmän $\langle S \rangle$ sivuluokka.

Todistus. Olkoon G ryhmä. Oletetaan, että $S \subseteq G \setminus \{1\}$, mutta $G \neq \langle S \rangle$. Graafin $\Gamma(G, S)$ särmäjoukon määritelmän nojalla $\{g_i, g_{i+1}\}$ on graafin särmä, jos ja vain jos $g_{i+1} = sg_i$ jollakin $s \in S \cup S^{-1}$, $i \in \{1, \ldots m-1\}$, missä $m \in \mathbb{Z}_+$. Tällöin solmujen g_1 ja g_m välillä on polku graafissa $\Gamma(G, S)$, jos ja vain jos $g_m = s_1 s_2 \ldots s_{m-1} g_1$, missä $s_1 s_2 \ldots s_{m-1} \in \langle S \rangle$. Siispä on voimassa $g_m \in \langle S \rangle g_1$. Koska edellinen on voimassa kaikille ryhmän G alkioille, väite seuraa. □

Lähdemateriaalin [23] iästä ja yleisestä korkeasta vaikeusasteesta johtuen tämän alaluvun todistuksissa käytetään implisiittisesti todistuksetta joitakin aputuloksia, joita myös lähdemateriaalissa on samaan tapaan käytetty. Seuraavassa apulauseessa 5.13 todistetaan apulauseen 5.14 todistuksessa tarvitut tällaiset aputulokset. Vastaisuudessa näin ei toimita, vaan vastaavan kaltaisia helpohkosti verifioitavia ”aputulosten aputuloksia” ei erikseen esitetä tai todisteta vedoten tarpeeseen rajata tutkielman laajuutta. Todistukset etenisivät suurilta osin vastaavasti kuin apulauseessa 5.13, esimerkiksi induktiolla graafin tai ryhmän koon suhteen. Useimmat näistä tuloksista ovat lisäksi intuition tasolla suhteellisen selkeitä.

Apulause 5.13. Olkoon $\Gamma(G, S)$ graafi, missä G on ryhmä ja $S \subseteq G \setminus \{1\}$. Tällöin

1. jokainen graafin $\Gamma(G, S)$ 2-faktori koostuu sykleistä,
2. jos alkion $s \in S \cup S^{-1}$ kertaluku on parillinen ja suurempi kuin 2, alkion s virittämien särmien muodostaman 2-faktorin muodostavat syklit ovat parillisen pituisia,
3. kaikki graafin $\Gamma(G, S)$ parillisen pituiset syklit voidaan 1-faktoroida.

Todistus.

1. Oletetaan, että graafilla $\Gamma(G, S)$ on ainakin yksi 2-faktori – muussa tapauksessa väite pitää triviaalisti paikkansa. Olkoon $\mathcal{G}$ jokin graafin $\Gamma(G, S)$ 2-faktori. Jokaisen 2-faktorin $\mathcal{G}$ solmun v_i, $i \in \{1, 2, \ldots n\}$, aste on 2, eli jokainen solmu on kahden muun solmun naapurisolmu. Koska G on äärellinen ryhmä ja täten 2-faktori $\mathcal{G}$ on äärellinen, voidaan 2-faktorin särmät luetella: jos 2-faktori $\mathcal{G}$ on yhtenäinen, särmät ovat

   $$\{v_1, v_2\}, \{v_2, v_3\}, \ldots, \{v_{n-1}, v_n\} \text{ ja } \{v_n, v_1\}.$$

   Täten 2-faktori $\mathcal{G}$ on sykli. Vastaavasti jos 2-faktori ei ole yhtenäinen, sen erillisille komponenteille voidaan kullekin tehdä vastaava päättely. Täten 2-faktori $\mathcal{G}$ koostuu kaikissa tapauksissa sykleistä.

2. Olkoon $s \in S \cup S^{-1}$. Oletetaan, että alkion s kertaluku on parillinen ja suurempi kuin 2, eli $|s| = 2n$ jollakin $n \in \mathbb{Z}_+, n \geq 2$. Tällöin $s^{2n} = 1$. Olkoon v graafin $\Gamma(G, S)$ solmu, jolloin on voimassa $v \in G$. Solmuun v liittyy täsmälleen kaksi alkion s virittämää särmää, nimittäin $\{v, sv\}$ ja $\{s^{-1}v, v\}$, joten alkion s virittämät särmät muodostavat graafin $\Gamma(G, S)$ 2-faktorin $\mathcal{G}$. Kohdan 1 perusteella kaikki graafin $\Gamma(G, S)$ 2-faktorit koostuvat sykleistä. Olkoon $\mathcal{G}'$ jokin tällainen sykli. Koska 2-faktori $\mathcal{G}$ muodostuu alkion s virittämistä särmistä, on syklin $\mathcal{G}'$ särmäjoukko muotoa

$$\{\{v, sv\}, \{sv, ssv\}, \ldots, \{s^{2n-1}v, v\}\}.$$

Selvästi siis syklissä $\mathcal{G}'$ on $2n$ särmää, eli särmiä on parillinen määrä.

3. Oletetaan argumentin vuoksi, että graafi $\Gamma(G, S)$ sisältää ainakin yhden parillisen pituisen syklin. Olkoon $\mathcal{G}$ jokin tällainen parillisen pituinen sykli. Olkoon sen solmujoukko

$$V = \{v_1, v_2, \ldots, v_n\}$$

ja särmäjoukko

$$E = \{\{v_1, v_2\}, \{v_2, v_3\}, \ldots, \{v_{n-1}, v_n\}, \{v_n, v_1\}\}$$

Jaetaan syklin $\mathcal{G}$ särmäjoukko E kahteen erilliseen osaan E_1 ja E_2 seuraavasti:

$$E_1 = \{\{v_1, v_2\}, \{v_3, v_4\}, \ldots, \{v_{n-1}, v_n\}\}$$
$$E_2 = \{\{v_2, v_3\}, \ldots, \{v_n, v_1\}\}$$

Selvästi $E = E_1 \cup E_2$, ja graafeissa (V, E_1) ja (V, E_2) jokaisen solmun aste on 1. Täten kyseiset graafit ovat syklin $\mathcal{G}$ 1-faktoreita, ja on muodostettu syklin $\mathcal{G}$ 1-faktorointi. Näin voidaan menetellä kaikkien graafin $\Gamma(G, S)$ syklien kohdalla, mikä todistaa väitteen.

□

Nyt on mahdollista siirtyä luvun varsinaisten päätulosten todistamiseen. Johdetaan ensin hyödyllinen apulause, jonka erityistapauksina saadaan todistettua, että jos ryhmän G kertaluku on luvun 2 potenssi tai jos kaikkien virittävän joukon S alkioiden kertaluku on parillinen, niin graafi $\Gamma(G, S)$ on 1-faktoroituva.

Apulause 5.14. Olkoon G ryhmä, ja olkoot $S_1, S_2 \subseteq G \setminus \{1\}$ joukkoja, jotka eivät välttämättä viritä ryhmää G. Oletetaan, että graafi $\Gamma(G, S_2)$ on 1-faktoroituva ja että $S_2 \subset S_1$. Tällöin jos joukon $S_1 \setminus S_2$ jokaisen alkion kertaluku on parillinen, niin graafi $\Gamma(G, S_1)$ on 1-faktoroituva.

Todistus. Olkoon $s \in S_1 \setminus S_2$. Oletetaan ensin, että alkion s kertaluku $|s| = 2$. Tämä tarkoittaa sitä, että $s = s^{-1}$, eli alkio s on oma vasta-alkionsa. Tällöin jokaiseen graafin $\Gamma(G, S_1 \setminus S_2)$ solmuun v liittyy tismalleen yksi alkion s virittämä särmä, nimittäin $\{v, sv\}$, koska ryhmän binäärioperaatio on hyvin määritelty. Siispä alkion s virittämien särmien joukko muodostaa 1-faktorin. Koska edellinen on voimassa

jokaiselle joukon $S_1 \setminus S_2$ alkiolle ja kyseisen joukon alkioiden virittämät särmät ovat tismalleen graafin $\Gamma(G, S_1 \setminus S_2)$ särmät, on graafi $\Gamma(G, S_1 \setminus S_2)$ 1-faktoroituva tapauksessa $|s| = 2$.

Oletetaan sitten, että $|s| > 2$. Tällöin $ss \neq 1$, joten $v \neq ssv$, missä v on mikä tahansa graafin $\Gamma(G, S_1 \setminus S_2)$ solmu. Täten solmuun v liittyy täsmälleen kaksi alkion s virittämää särmää, nimittäin $\{v, sv\}$ ja $\{s^{-1}v, v\}$. Alkion s virittämät särmät muodostavat siis graafin $\Gamma(G, S_1 \setminus S_2)$ 2-faktorin $\mathcal{G}$. Apulauseen 5.13 kohdan 1 nojalla 2-faktori $\mathcal{G}$ koostuu sykleistä. Syklit ovat apulauseen 5.13 kohdan 2 perusteella parillisen pituisia, koska oletuksen perusteella joukon $S_1 \setminus S_2$ jokaisen alkion kertaluku on parillinen. Lopulta apulauseen 5.13 kohdan 3 perusteella nämä parillisen pituiset syklit voidaan 1-faktoroida, joten myös koko 2-faktori $\mathcal{G}$ voidaan 1-faktoroida. Koska edellinen on voimassa kaikille joukon $S_1 \setminus S_2$ alkioille, graafi $\Gamma(G, S_1 \setminus S_2)$ on 1-faktoroituva. Lisäksi koska $(S_1 \setminus S_2) \cap S_2 = \emptyset$, niin graafien $\Gamma(G, S_1 \setminus S_2)$ ja $\Gamma(G, S_2)$ särmäjoukot ovat erilliset, jolloin

$$\Gamma(G, S_1 \setminus S_2) \cup \Gamma(G, S_2) = \Gamma(G, S_1).$$

Oletuksen perusteella $\Gamma(G, S_2)$ on 1-faktoroituva, joten myös graafi $\Gamma(G, S_1)$ on 1-faktoroituva. Tämä todistaa väitteen. □

Apulauseesta 5.14 saadaan johdettua kaksi seurausta, joista ensimmäistä tarvitaan jälkimmäisen todistuksessa. Seuraus 5.16 todistaa lauseen 5.10 kohdan 1.

Seuraus 5.15. *Olkoon G ryhmä. Jos joukon $S \subseteq G \setminus \{1\}$ kaikkien alkioiden kertaluku on parillinen, graafi $\Gamma(G, S)$ on 1-faktoroituva.*

Todistus. Valitaan $S_1 = S$ ja $S_2 = \emptyset$. Nyt triviaalisti graafi $\Gamma(G, S_2)$ on 1-faktoroituva, minkä lisäksi $S_2 \subset S_1$ ja $S_1, S_2 \subseteq G \setminus \{1\}$. Lisäksi oletuksen perusteella jokaisen joukon $S = S_1 \setminus S_2$ alkion kertaluku on parillinen, joten apulauseen 5.14 perusteella graafi $\Gamma(G, S_1 \setminus S_2) = \Gamma(G, S)$ on 1-faktoroituva. □

Seuraus 5.16. *Jos ryhmän G kertaluku on 2^k, $k \in \mathbb{Z}_+$, ja $S \subseteq G \setminus \{1\}$, graafi $\Gamma(G, S)$ on 1-faktoroituva.*

Todistus. Oletetaan, että ryhmän G kertaluku on 2^k, $k \in \mathbb{Z}_+$. Olkoon nyt $a \in G$. Lagrangen lauseen seurauksen 3.41 perusteella $|a|$ jakaa luvun 2^k, eli $2^k = n|a|$, missä $n \in \mathbb{Z}_+$. Jos nyt $k = 1$, niin graafissa $\Gamma(G, S)$ on vain kaksi solmua ja niiden välillä on särmä, joten graafi on selvästi 1-faktoroituva. Jos taas $k > 1$, on voimassa $2 \mid |a|$, eli alkion a kertaluku on parillinen. Koska tämä on voimassa kaikille ryhmän G alkioille ja $S \subseteq G \setminus \{1\}$, tästä seuraa seurauksen 5.15 nojalla, että graafi $\Gamma(G, S)$ on 1-faktoroituva. □

Pyritään seuraavaksi todistamaan lauseen 5.10 kohta 2, eli että jos G on Abelin ryhmä, jonka kertaluku on parillinen, niin Cayleyn graafi $\Gamma(G, S)$ on 1-faktoroituva. Tätä varten tarvitaan apulause, joka osoittautuu erittäin hyödylliseksi myös muissa todistuksissa.

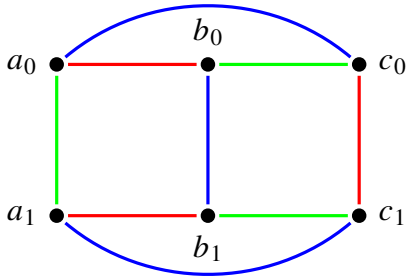
Apulause 5.17. Jos $\mathcal{G}$ on yksinkertainen, säännöllinen graafi, niin graafi $\mathcal{G}\Box\Gamma(\mathbb{Z}_2, \{1\})$ on 1-faktoroituva. Erityisesti graafi $\Gamma(G, S)\Box\Gamma(\mathbb{Z}_2, \{1\})$ on 1-faktoroituva millä tahansa ryhmällä G ja sen virittävällä joukolla $S \subseteq G \setminus \{1\}$.

Todistus. Pyritään näyttämään, että graafi $\mathcal{G}\Box\Gamma(\mathbb{Z}_2, \{1\})$ on yksinkertainen, säännöllinen ja särmäväritettävissä $k+1$:llä värillä. Tällöin väite seuraa suoraan seurauksesta 5.9. Oletetaan siis, että $\mathcal{G}$ on yksinkertainen ja k-säännöllinen graafi, jossa on n solmua. Koska Cayleyn graafissa $\Gamma(\mathbb{Z}_2, \{1\})$ on 2 solmua, karteesisessa tulossa $\mathcal{G}\Box\Gamma(\mathbb{Z}_2, \{1\})$ solmuja on määritelmän 2.26 perusteella $2n$ kappaletta eli parillinen määrä. Lisäksi karteesinen tulo $\mathcal{G}\Box\Gamma(\mathbb{Z}_2, \{1\})$ on säännöllinen graafi, koska $\mathcal{G}$ ja $\Gamma(\mathbb{Z}_2, \{1\})$ ovat säännöllisiä. Itse asiassa määritelmästä 2.26 seuraa, että karteesinen tulo $\mathcal{G}\Box\Gamma(\mathbb{Z}_2, \{1\})$ on $k+1$ -säännöllinen. Lisäksi kyseinen graafi on selvästi yksinkertainen.

Jaetaan nyt graafin $\mathcal{G}\Box\Gamma(\mathbb{Z}_2, \{1\})$ särmäväritettävyyden todistus kahteen osaan suhteessa graafin $\mathcal{G}$ särmäväritettävyyteen. Olkoon v mikä tahansa graafin $\mathcal{G}$ solmu. Vizingin lauseen (lause 5.8) perusteella graafin $\mathcal{G}$ särmien värittämiseen riittää joko k tai $k+1$ väriä. Molemmissa tapauksissa graafin $\mathcal{G}$ missä tahansa särmävärityksessä solmuun v liittyvät särmät voidaan värittää k:lla eri värillä. Konstruoitaessa graafin $\mathcal{G}\Box\Gamma(\mathbb{Z}_2, \{1\})$ särmäväritystä kaikki kyseisen graafin solmuihin $(v, 0)$ ja $(v, 1)$ liittyvät särmät on edellisen perusteella väritetty käyttäen joko k tai $k+1$ väriä lukuun ottamatta kyseisten solmujen välissä olevaa särmää, jollainen graafissa väistämättä on määritelmän 2.26 perusteella. Jos graafi $\mathcal{G}$ on särmäväritettävissä k:lla värillä, särmän $\{(v, 0), (v, 1)\}$ värittämiseen tarvitaan yksi väri lisää, jolloin graafi $\mathcal{G}\Box\Gamma(\mathbb{Z}_2, \{1\})$ on väritettävissä $k+1$:llä värillä. Toisaalta jos $\mathcal{G}$ on väritettävissä $k+1$:llä värillä, voidaan särmän $\{(v, 0), (v, 1)\}$ värittämiseen käyttää väriä, jolla mitään solmuun v liittyvää särmää ei graafissa $\mathcal{G}$ ole väritetty – eli käytetään ns. yli jäänyttä väriä – jolloin siis myös graafi $\mathcal{G}\Box\Gamma(\mathbb{Z}_2, \{1\})$ on väritettävissä $k+1$:llä värillä. Joka tapauksessa yksinkertainen ja $k+1$ -säännöllinen graafi $\mathcal{G}\Box\Gamma(\mathbb{Z}_2, \{1\})$, jossa on parillinen määrä solmuja, on särmäväritettävissä $k+1$:llä värillä, jolloin seurauksen 5.9 perusteella se on 1-faktoroituva. □

Piirretään vielä esimerkkinä astetta 3 olevan 2-säännöllisen graafin (ks. esimerkki 2.12) ja Cayleyn graafin $\Gamma(\mathbb{Z}_2, \{1\})$ karteesisen tulon 1-faktorointi, mikä havainnollistaa todistuksen ideaa.

Esimerkki 5.18. Kuvassa 5.3 on esitetty esimerkin 2.12 graafin ja Cayleyn graafin $\Gamma(\mathbb{Z}_2, \{1\})$ karteesisen tulon 1-faktorointi. Kuhunkin 1-faktoriin kuuluvat särmät on merkitty selkeyden vuoksi omalla värillään. Kuvassa on käytetty piirtoteknisistä syistä seuraavankaltaisia lyhennysmerkintöjä: $(x, i) \coloneqq x_i, x \in \{a, b, c\}, i \in \{0, 1\}$.



Kuva 5.3. Karteesisen tulon $(\{a, b, c\}, \{\{a, b\}, \{b, c\}, \{a, c\}\}) \square \Gamma(\mathbb{Z}_2, \{1\})$ 1-faktorointi.

Todistetaan seuraavaksi lause, jonka seurauksina todistetaan edelleen lauseen 5.10 kohdat 2 ja 3. Lauseen todistuksessa tarvitaan seuraavaa tietynlaisen joukon alkioiden kertalukua koskevaa apulausetta.

Apulause 5.19. Olkoon $K = H \rtimes G$, missä H ja G ovat ryhmiä ja ryhmän G kertaluku on 2^k jollakin $k \in \mathbb{Z}_+$. Tällöin joukon $K \setminus H$ kaikkien alkioiden kertaluku on parillinen.

Todistus. Olkoon $K = H \rtimes G$, missä H ja G ovat ryhmiä ja ryhmän G kertaluku on 2^k jollakin $k \in \mathbb{Z}_+$. Tällöin määritelmän 3.60 nojalla on voimassa

$$H \lhd K, G \leq K, H \cap G = \{1\} \text{ ja } K = HG.$$

Olkoon $x \in K \setminus H$. Tällöin on olemassa sellaiset $h \in H$ ja $g \in G$, että $x = hg$. Koska $x \notin H$, on voimassa $x \neq h$ ja siis $g \neq 1$. Olkoon $n \in \mathbb{Z}_+$ alkion x kertaluku. Tällöin $1 = x^n = (hg)^n$. Koska $H \lhd K$, määritelmän 3.43 nojalla $gNg^{-1} = N$, mikä tarkoittaa, että $ghg^{-1} = h_1$ jollakin $h_1 \in H$, eli $gh = h_1 g$ jollakin $h_1 \in H$. Niinpä

$$(hg)(hg) = h(gh)g = h(h_1 g)g = hh_1 g^2$$

jollakin $h_1 \in H$, ja edelleen

$$1 = x^n = (hg)^n = hh_1 \cdots h_{n-1} g^n$$

joillakin $h_1, \ldots, h_{n-1} \in H$. Ryhmässä K on siis voimassa $(hh_1 \cdots h_{n-1})^{-1} = g^n$. Koska $hh_1 \cdots h_{n-1} \in H, g^n \in G$ ja $H \cap G = \{1\}$, täytyy olla $hh_1 \cdots h_{n-1} = 1$ ja $g^n = 1$.

Koska $g \in G$, Lagrangen lauseen seurauksen 3.41 nojalla ryhmän G kertaluku on jaollinen alkion g kertaluvulla. Ryhmän G kertaluku on 2^k jollakin $k \in \mathbb{Z}_+$, joten alkion $g \neq 1$ kertaluku on 2^m jollakin $m \in \mathbb{Z}_+, m \leq k$. Edelleen koska $g^n = 1$, jakaa alkion g kertaluku seurauksen 3.42 mukaan luvun n. Täten luku n on parillinen. Tämä todistaa väitteen, koska alkion $x \in K \setminus H$ kertaluku on oletuksen mukaan n. $\square$

Lause 5.20. *Olkoon G ryhmä, jonka kertaluku on $2^k, k \in \mathbb{Z}_+$, ja olkoon S ryhmän $H \rtimes G$ virittävä joukko, missä H on mikä tahansa ryhmä. Oletetaan, että on olemassa sellainen $s \in S$, että $s \notin H$ ja että kaikilla $h \in S \cap H$ on voimassa $shs^{-1} = h^{\pm 1}$ (eli $shs^{-1} = h$ tai $shs^{-1} = h^{-1}$). Tällöin Cayleyn graafi $\Gamma(H \rtimes G, S)$ on 1-faktoroituva.*

Todistus. Olkoon G kertalukua $2^k, k \in \mathbb{Z}_+$, oleva ryhmä, olkoon H mikä tahansa ryhmä ja olkoon $S \subseteq H \rtimes G \setminus \{1\}$ ryhmän $H \rtimes G$ virittävä joukko. Merkitään $S' = S \cap H$. Oletetaan, että on olemassa sellainen $s \in S$ että $s \notin H$ ja että kaikilla $h \in S'$ on voimassa $shs^{-1} = h^{\pm 1}$. Selvästi on voimassa $S' \cup \{s\} \subseteq S$. Mikäli $S' \cup \{s\} = S$,

$$\Gamma(H \rtimes G, S) \cong \Gamma(\langle S' \cup \{s\}\rangle, S' \cup \{s\}).$$

Mikäli taas $S' \cup \{s\} \subset S$, väitteen todistamiseksi riittää apulauseen 5.14 nojalla osoittaa, että Cayleyn graafi $\Gamma(\langle S' \cup \{s\}\rangle, S' \cup \{s\})$ on 1-faktoroituva. Nimittäin $S \setminus (S' \cup \{s\}) \subseteq H \rtimes G \setminus H$, joten joukon $S \setminus (S' \cup \{s\})$ kaikkien alkioiden kertaluku on apulauseen 5.19 nojalla parillinen. Kummassakin edellä mainitussa tapauksessa riittää siis osoittaa, että Cayleyn graafi $\Gamma(\langle S' \cup \{s\}\rangle, S' \cup \{s\})$ on 1-faktoroituva.

Jaetaan nyt todistus kahteen osaan alkion s kertaluvun perusteella. Koska $s \neq 1$, täytyy olla $|s| > 1$. Jos $|s| = 2$, niin graafi $\Gamma(\langle S' \cup \{s\}\rangle, S' \cup \{s\})$ on isomorfinen graafin $\Gamma(\langle S'\rangle, S') \times \Gamma(\mathbb{Z}_2, \{1\})$ kanssa. Nimittäin jokaista graafin $\Gamma(\langle S'\rangle, S')$ solmua s' kohden on graafissa $\Gamma(\langle S' \cup \{s\}\rangle, S' \cup \{s\})$ solmun s' lisäksi solmu ss', ja koska $|s| = 2$, niin solmujen s' ja ss' välillä on suuntaamaton särmä. Kyseinen graafi jakautuu siis luonnollisella tavalla kahteen isomorfiseen osaan, mikä vastaa Cayleyn graafin $\Gamma(\langle S'\rangle, S') \times \Gamma(\mathbb{Z}_2, \{1\})$ "tikapuurakennetta". Tämä graafi puolestaan on 1-faktoroituva apulauseen 5.17 nojalla, joten myös Cayleyn graafi $\Gamma(\langle S' \cup \{s\}\rangle, S' \cup \{s\})$ on 1-faktoroituva.

Jos $|s| > 2$, olkoon

$$f \colon H \rtimes G \to G$$

ryhmähomomorfismi. Tällöin on voimassa $f(s) = g$ jollakin $g \in G$, ja edelleen $|g| = 2^n$ jollakin $n \in \mathbb{Z}_+$. Seurauksen 5.16 nojalla graafi $\Gamma(G, \{g\})$ on 1-faktoroituva. Olkoon $\mathcal{G}$ jokin graafin $\Gamma(G, \{g\})$ 1-faktori. Yleistetään 1-faktori $\mathcal{G}$ graafiin $\Gamma(\langle S' \cup \{s\}\rangle, S' \cup \{s\})$ siten, että otetaan graafin $\Gamma(\langle S' \cup \{s\}\rangle, S' \cup \{s\})$ 1-faktoriin kaikki alkion s 1-faktorissa $\mathcal{G}$ virittämät särmät, joiden päätesolmut kuvautuvat homomorfismissa f ryhmän G sellaisiksi alkioiksi, joiden välillä on särmä graafin $\Gamma(G, \{g\})$ 1-faktorissa $\mathcal{G}$. Loput graafin $\Gamma(\langle S' \cup \{s\}\rangle, S' \cup \{s\})$ särmät muodostavat 2^{k-1} erillistä graafin $\Gamma(\langle S'\rangle, S') \times \Gamma(\mathbb{Z}_2, \{1\})$ keskenään isomorfista kopiota. Nämä kopiot ovat 1-faktoroituvia apulauseen 5.17 nojalla, joten Cayleyn graafi $\Gamma(\langle S' \cup \{s\}\rangle, S' \cup \{s\})$ on 1-faktoroituva, ja väite seuraa. □

Ensimmäisenä lauseen 5.20 seurauksena todistetaan, että Abelin ryhmistä muodostetut Cayleyn graafit ovat 1-faktoroituvia. Todistus on teknisyydestään huolimatta suoraviivainen: Abelin ryhmälle konstruoidaan äärellisesti virittyvien Abelin ryhmien peruslauseen avulla esitys suorana tulona, ja edelleen isomorfiaa hyödyntämällä yleistetään suora tulo puolisuoraksi tuloksi, jolloin päästään hyödyntämään lausetta 5.20.

Seuraus 5.21. *Jos G on Abelin ryhmä, jonka kertaluku on parillinen, ja $S \subseteq G \setminus \{1\}$ on ryhmän G virittävä joukko, niin Cayleyn graafi $\Gamma(G, S)$ on 1-faktoroituva.*

Todistus. Olkoon G Abelin ryhmä, jonka kertaluku on parillinen. Koska ryhmä G on sivulla 48 esitetyn oletuksen perusteella äärellinen, se on myös äärellisesti virittyvä, jolloin äärellisesti virittyvien Abelin ryhmien peruslauseen 3.64 nojalla

$$G \cong \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_n},$$

missä p_i on alkuluku kaikilla $i \in \{1, \ldots, n\}$. Koska ryhmän G kertaluku on parillinen, täytyy olla $p_j = 2$ jollakin $j \in \{1, \ldots, n\}$. Voidaan olettaa, että $j = 1$, jolloin siis $p_1 = 2$. Merkitään nyt $H = \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_n}$, jolloin $G \cong \mathbb{Z}_2 \times H$. Olkoot edelleen

$$\mathbb{Z}_2' = \mathbb{Z}_2 \times \{1_H\} \text{ ja } H' = \{0\} \times H,$$

missä 1_H on ryhmän H neutraalialkio ja 0 on ryhmän $\mathbb{Z}_2$ neutraalialkio. Tällöin selvästi $\mathbb{Z}_2' \cong \mathbb{Z}_2$ ja $H' \cong H$. Edelleen on voimassa $G \cong \mathbb{Z}_2' \rtimes H'$, koska

$$\mathbb{Z}_2' \lhd \mathbb{Z}_2' \rtimes H', H' \leq \mathbb{Z}_2' \rtimes H', \mathbb{Z}_2' \cap H' = \{(0, 1_H)\} \text{ ja } \mathbb{Z}_2' H' \cong G,$$

missä $(0, 1_H)$ on ryhmän $\mathbb{Z}_2' \rtimes H'$ neutraalialkio.

Olkoon nyt $S \subseteq \mathbb{Z}_2' \rtimes H' \setminus \{(0, 1_H)\}$ ryhmän $\mathbb{Z}_2' \rtimes H'$ virittävä joukko. Ryhmien $\mathbb{Z}_2'$ ja H' rakenteen vuoksi joukossa $S \setminus H'$ on ainakin yksi alkio, ja Abelin ryhmän binäärioperaation vaihdannaisuuden nojalla kaikilla $s \in S \setminus H'$ ja $h \in S \cap H'$ on voimassa $shs^{-1} = h$. Lisäksi ryhmän $\mathbb{Z}_2'$ kertaluku on $2 = 2^1$, joten lauseen 5.20 nojalla Cayleyn graafi $\Gamma(\mathbb{Z}_2' \rtimes H', S)$ on 1-faktoroituva. Tämä todistaa väitteen, koska $\mathbb{Z}_2' \rtimes H' \cong G$ ja joukko S on mikä tahansa ryhmän $\mathbb{Z}_2' \rtimes H'$ virittävä joukko. □

Koska seurauksen 3.30 perusteella kaikki sykliset ryhmät ovat Abelin ryhmiä, edellisestä seurauksesta seuraa edelleen, että kaikki sellaiset Cayleyn graafit $\Gamma(G, S)$, missä G on parillista kertalukua oleva syklinen ryhmä ja S on ryhmän G virittävä joukko, ovat 1-faktoroituvia.

Todistetaan seuravaavaksi diedriryhmistä muodostettujen Cayleyn graafien 1-faktoroituvuus. Tulos seuraa suoraviivaisesti alaluvussa 3.9 tehdyistä havainnoista ja lauseesta 5.20.

Seuraus 5.22. *Jos G on ryhmä, jonka kertaluku on 2^k, $k \in \mathbb{Z}_+$, H on Abelin ryhmä ja $ghg^{-1} = h^{\pm 1}$ kaikilla $g \in G$ ja $h \in H$, niin Cayleyn graafi $\Gamma(H \rtimes G, S)$ on 1-faktoroituva kaikilla ryhmän $H \rtimes G$ virittävillä joukoilla S. Erityisesti jos D_m on kertalukua $2m, m \in \mathbb{Z}_+$, oleva diedriryhmä, niin Cayleyn graafi $\Gamma(D_m, S)$ on 1-faktoroituva kaikilla virittävillä joukoilla $S \subseteq D_m \setminus \{id\}$.*

Todistus. Yleisessä muodossa väite seuraa suoraan lauseesta 5.20. Diedriryhmien osalta päätellään seuraavasti: Olkoon D_m kertalukua $2m, m \in \mathbb{Z}_+$, oleva diedriryhmä. Lauseen 3.61 perusteella ryhmä D_m on isomorfinen puolisuoran tulon $\mathbb{Z}_m \rtimes \mathbb{Z}_2$ kanssa. Tässä ryhmän $\mathbb{Z}_2$ kertaluku on 2, $\mathbb{Z}_m$ on Abelin ryhmä ja $ghg^{-1} = h^{\pm 1}$ kaikilla $g \in \mathbb{Z}_2$ ja $h \in \mathbb{Z}_m$. Tällöin lauseen 5.20 perusteella Cayleyn graafi $\Gamma(D_m, S)$ on 1-faktoroituva kaikilla ryhmän D_m virittävillä joukoilla $S \subseteq D_m \setminus \{\text{id}\}$. □

Seuraukset 5.21 ja 5.22 tarjoavat vaihtoehtoisen tavan todentaa esimerkin 4.12 havainto siitä, että Petersenin graafi ei ole Cayleyn graafi. Nimittäin Petersenin graafi ei ole 1-faktoroituva (ks. [13], harjoitus 7.2.7), mutta toisaalta ainoat kertaluvun 10 ryhmät ovat syklinen ryhmä ja viisikulmion diedriryhmä [18]. Koska kaikki syklisistä ryhmistä tai diedriryhmistä muodostetut Cayleyn graafit ovat 1-faktoroituvia, seuraisi siitä, että Petersenin graafi on Cayleyn graafi, ristiriita, eikä Petersenin graafi täten voi olla Cayleyn graafi.

Osoitetaan lopuksi, että Cayleyn graafien 1-faktorointikonjektuuri on voimassa nilpotenteille ryhmille. Ensin todistetaan tietynlaisia tekijäryhmiä koskeva varsin tekninen aputulos, jota tarvitaan edelleen yhdessä apulauseen 5.24 kanssa lauseen 5.25 todistuksessa. Perimmäisenä tavoitteena apulauseiden 5.23 ja 5.24 ja lauseen 5.25 esittämisessä on mahdollistaa nilpotenttien ryhmien Sylowin aliryhmärakenteen hyödyntäminen sen todistamisessa, että nilpotenttien ryhmien Cayleyn graafit ovat 1-faktoroituvia.

Apulause 5.23. Olkoon N ryhmän G normaali aliryhmä ja $S \subseteq G \setminus \{1\}$ ryhmän G sellainen virittävä joukko, että $S \cap N = \emptyset$. Oletetaan, että kun $s_i, s_j \in S$ ja $s_i \neq s_j^{\pm 1}$, niin $s_i s_j, s_i s_j^{-1} \notin N$. Tällöin jos Cayleyn graafi $\Gamma(G/N, (SN)/N)$ on 1-faktoroituva, niin myös Cayleyn graafi $\Gamma(G, S)$ on 1-faktoroituva.

Todistus. Oletetaan, että Cayleyn graafi $\Gamma(G/N, (SN)/N)$ on 1-faktoroituva ja että muut edellä mainitut oletukset ovat voimassa. Olkoon nyt $\mathcal{G}$ jokin graafin $\Gamma(G/N, (SN)/N)$ 1-faktori. Laajennetaan 1-faktori $\mathcal{G}$ graafin $\Gamma(G, S)$ 1-faktoriksi $\mathcal{G}'$ seuraavalla tavalla.

Olkoon

$$f \colon G \to G/N$$

luonnollinen homomorfismi. Otetaan 1-faktoriin $\mathcal{G}'$ kaikkien 1-faktorin $\mathcal{G}$ särmien alkukuvat luonnollisen homomorfismin f suhteen. Lagrangen lauseen 3.40 nojalla on voimassa $|G/N| = |G|/|N|$, ja tekijäryhmän määritelmän nojalla on olemassa tismalleen $|N|$ kappaletta sellaisia $g \in G$, että jollakin $g' \in G$ on voimassa $f(g) \in g'N$. Koska f on homomorfismi, tämä tarkoittaa, että yhdellä särmällä on $|N|$ alkukuvaa. Koska S ja N ovat erillisiä eikä millään $s_i, s_j \in S, s_i \neq s_j^{\pm 1}$ ole voimassa $s_i s_j \in N$ tai $s_i s_j^{-1} \in N$, niin Lagrangen lauseen 3.40 nojalla

$$|(SN)/N| = \frac{|SN|}{|N|} = \frac{|S||N|}{|N|} = |S|.$$

Edellä päätellyn nojalla tehtäessä laajennos graafin $\Gamma(G, S)$ 1-faktoriksi kaikille graafin $\Gamma(G/N, (SN)/N)$ 1-faktoreille saadaan katettua kaikki paitsi ne särmät, jotka virittää mikä tahansa sellainen alkio $s \in S$, jolla $s^2 \neq 1$, eli $s \neq s^{-1}$, mutta $s^2 \in N$. Koska $s^2 \neq 1$, tällaisen alkion s virittämät särmät, jotka eivät ole mukana 1-faktorien laajennuksissa, muodostavat kuitenkin itsessään kaksi 1-faktoria, mikä päätellään kuten apulauseen 5.14 todistuksen 2. kappaleessa. Koska tämä on voimassa kaikille sellaisille $s \in S$, joilla $s^2 \neq 1$ mutta $s^2 \in N$, on saatu muodostettua Cayleyn graafin $\Gamma(G, S)$ 1-faktorointi. □

Apulause 5.24. Olkoon G ryhmä, jonka kertaluku on pariton. Tällöin Cayleyn graafi $\Gamma(\mathbb{Z}_2 \times G, S)$ on 1-faktoroituva kaikilla ryhmän $\mathbb{Z}_2 \times G$ virittävillä joukoilla S, jotka sisältävät täsmälleen yhden alkion, jonka kertaluku on parillinen.

Todistus. Sivuutetaan. Todistus on muutamia muutoksia lukuun ottamatta olennaisesti sama kuin apulauseen 5.17 todistus. Ks. [1], s. 1–2. □

Apulauseiden 5.23 ja 5.24 avulla voidaan todistaa Abdollahin artikkelin päätulos, jonka seurauksena edelleen todistetaan nilpotenttien ryhmien Cayleyn graafien 1-faktoroituvuus.

Lause 5.25. *Olkoon H ryhmä, jonka kertaluku on pariton, ja olkoon Q ryhmä, jonka kertaluku on 2^k jollakin $k \in \mathbb{Z}_+$. Tällöin Cayleyn graafi $\Gamma(Q \times H, S)$ on 1-faktoroituva kaikilla ryhmän $Q \times H$ virittävillä joukoilla S.*

Todistus. Merkitään $G = Q \times H$. Olkoon S mikä tahansa ryhmän G virittävä joukko. Todistetaan väite induktiolla joukon S kertaluvun suhteen. Jos $|S| = 1$, niin G on syklinen ryhmä ja siis lauseen 3.30 nojalla Abelin ryhmä. Lauseen 3.59 perusteella $|G| = |Q||H|$, ja koska $|Q| = 2^k$ jollakin $k \in \mathbb{Z}_+$, niin $|G|$ on parillinen. Tällöin apulauseen 5.21 perusteella Cayleyn graafi $\Gamma(G, S)$ on 1-faktoroituva.

Oletetaan sitten, että väite on voimassa, kun $|S| = n - 1, n > 2$, eli että Cayleyn graafi $\Gamma(Q' \times H', S)$ on 1-faktoroituva, missä ryhmän Q' kertaluku on 2^k, H' on parittoman kertaluvun ryhmä ja S on mikä tahansa ryhmän $Q' \times H'$ virittävä joukko, jolle on voimassa $|S| = n - 1$. Pyritään tämän oletuksen avulla todistamaan väite tapauksessa $|S| = n$, eli että Cayleyn graafi $\Gamma(Q \times H, S)$ on 1-faktoroituva, kun ryhmän Q kertaluku on 2^k, H on parittoman kertaluvun ryhmä ja joukko S, jolle $|S| = n$, virittää ryhmän $Q \times H$.

Koska ryhmän Q kertaluku on 2^k, sen kaikkien alkioiden paitsi neutraalialkion kertaluku on parillinen, ja toisaalta koska ryhmän H kertaluku on pariton, kaikkien sen alkioiden kertaluku on pariton. Koska $G = \langle S \rangle$ ja ryhmän G parittoman kertaluvun alkioiden joukko on ryhmän H aliryhmä, täytyy joukossa S olla ainakin yksi alkio a, jonka kertaluku on parillinen.

Jaetaan tarkastelu kahteen osaan sen perusteella, onko joukossa S alkion a ohella muita alkioita, joiden kertaluku on parillinen. Oletetaan ensin, että on olemassa sellainen $a' \in S, a' \neq a$, että alkion a' kertaluku on parillinen. Tarkastellaan joukon $S \setminus \{a\}$ virittämää ryhmän G aliryhmää G'. Ryhmän G määritelmän nojalla on voimassa $G' = Q' \times H'$ joillakin $Q' \leq Q, Q' \neq \{1\}$, ja $H' \leq H$. Koska $|S \setminus \{a\}| = n - 1$, induktio-oletuksen mukaan Cayleyn graafi $\Gamma(G', S \setminus \{a\})$ on 1-faktoroituva. Apulauseen 5.12 perusteella Cayleyn graafi $\Gamma(G, S \setminus \{a\})$ koostuu erillisistä 1-faktoroituvan Cayleyn graafin $\Gamma(G', S \setminus \{a\})$ keskenään isomorfisista kopioista, joten myös Cayleyn graafi $\Gamma(G, S \setminus \{a\})$ on 1-faktoroituva. Koska

$$S \setminus (S \setminus \{a\}) = \{a\}$$

ja alkion a kertaluku on parillinen, apulauseen 5.14 nojalla Cayleyn graafi $\Gamma(G, S)$ on 1-faktoroituva.

Oletetaan sitten, että alkio a on joukon S ainoa alkio, jonka kertaluku on parillinen. Suoran tulon määritelmän nojalla a on muotoa a_1a_2 joillakin $a_1 \in Q$ ja $a_2 \in H$, joten

$$G = \langle S \rangle = \langle (S \setminus \{a\}) \cup \{a_1a_2\} \rangle = \langle a_1 \rangle \times \langle (S \setminus \{a\}) \cup \{a_2\} \rangle.$$

Viimeinen yhtäsuuruus seuraa siitä, että koska alkion a_1 kertaluku on parillinen, alkion a_2 kertaluku on pariton, ja koska H ja Q ovat isomorfisia ryhmän G normaalien aliryhmien kanssa, niin $(a_1a_2)^{k_1} = a_1$ jollakin $k_1 \in \mathbb{Z}_+$ ja $(a_1a_2)^{k_2} = a_2$ jollakin $k_2 \in \mathbb{Z}_+$. Täten $a_1, a_2 \in \langle S \rangle$. Yhtäsuuruudesta $Q \times H = G = \langle a_1 \rangle \times \langle (S \setminus \{a\}) \cup \{a_2\} \rangle$ seuraa edelleen, että $Q = \langle a_1 \rangle$. Nimittäin äärellisen ryhmän esitys suorana tulona on isomorfiaa vaille yksikäsitteinen Krull-Schmidtin lauseen 3.68 nojalla, ja $a_1 \notin H$, sillä alkion a_1 kertaluku on parillinen ja kaikkien ryhmän H alkioiden kertaluku on pariton.

Tarkastellaan sitten aliryhmää $N = \langle a_1^2 \rangle$. Selvästi N on ryhmän G normaali aliryhmä ja $N \cap S = \emptyset$. Jälkimmäinen ehto seuraa siitä, että koska ryhmän N kaikkien alkioiden kertaluku on parillinen ja joukossa S on vain yksi alkio $a = a_1a_2$, jonka kertaluku on parillinen, eikä millään $n \in \mathbb{Z}_+$ ole voimassa $a_1^{2n} = a_1a_2$, niin $a_1^{2n} \notin S$ kaikilla $n \in \mathbb{Z}_+$. Tällöin on tietenkin voimassa, että kun $s, t \in S$ ja $s \neq t^{\pm 1}$, niin $st \notin S$ ja $st^{-1} \notin S$, koska $s \neq a_1$ ja $t \neq a_1$. Nyt koska $G/N \cong \mathbb{Z}_2 \times H$, niin apulauseen 5.24 nojalla Cayleyn graafi $\Gamma(G/N, (SN)/N)$ on 1-faktoroituva. Edelleen tällöin apulauseen 5.23 nojalla Cayleyn graafi $\Gamma(G, S)$ on 1-faktoroituva, mikä päättää todistuksen. □

Seuraus 5.26. *Jos G on nilpotentti ryhmä, jonka kertaluku on parillinen, niin Cayleyn graafi $\Gamma(G, S)$ on 1-faktoroituva kaikilla ryhmän G virittävillä joukoilla S.*

Todistus. Olkoon G nilpotentti ryhmä, jonka kertaluku on parillinen. Tällöin ryhmän G kertaluvun alkutekijähajotelma on muotoa

$$|G| = a_1^{k_1}a_2^{k_2} \cdots a_n^{k_n} \cdot 2^m,$$

missä $a_i \neq 2$ ovat alkulukuja ja $k_i, m \in \mathbb{Z}_+, i \in \{1, \ldots n\}$. Täten lauseen 3.51 perusteella ryhmällä G on aliryhminään ainakin kertalukua $a_i^{k_i}$ olevat Sylowin a_i-aliryhmät, joita merkittäköön symboleilla $S_1, \ldots, S_n$, ja kertalukua 2^m oleva Sylowin 2-aliryhmä, jota merkittäköön symbolilla Q. Lauseen 3.57 mukaan jokainen äärellinen nilpotentti ryhmä on Sylowin aliryhmiensä suora tulo, joten

$$G \cong S_1 \times \cdots \times S_n \times Q.$$

Ryhmä $H = S_1 \times \cdots \times S_n$ on ryhmän G aliryhmä, jonka kertaluku on $a_1^{k_1} \cdots a_n^{k_n}$. Koska luvut a_i ovat parittomia, on niiden tulokin pariton. Täten $G \cong H \times Q$, missä Q on 2-ryhmä ja ryhmän H kertaluku on pariton. Siispä lauseen 5.25 mukaan Cayleyn graafi $\Gamma(G, S)$ on 1-faktoroituva. □

5.4 Äärettömät ryhmät

Yleistetään tässä alaluvussa muutamia edellisen alaluvun tuloksia numeroituvasti äärettömille Cayleyn graafeille eli numeroituvasti äärettömille ryhmille. 1-faktoroituvuus määriteltiin luvussa 5.1 kaikille graafeille, joten sitä tai muitakaan tarvittavia käsitteitä ei tarvitse erikseen yleistää äärettömille graafeille.

Ensimmäinen numeroituvasti äärettömiä Cayleyn graafeja koskeva 1-faktorointitulos kertoo, että kaikki numeroituvasti äärettömästi virittyvien ryhmien Cayleyn graafit ovat 1-faktoroituvia. Todistuksessa tarvitaan joukko-opin hyvinjärjestysperiaatetta, joten esitetään se vielä ennen varsinaista todistusta lähteeseen [8] perustuen. Hyvinjärjestysperiaatteen mukaan mikä tahansa luonnollisten lukujen joukon osajoukko voidaan hyvinjärjestää, eli missä tahansa luonnollisten lukujen joukon osajoukossa on pienin alkio.

Lause 5.27 (Hyvinjärjestysperiaate)**.** *Olkoon $A \subseteq \mathbb{N}, A \neq \emptyset$. Tällöin on olemassa sellainen $m \in A$, että $m \leq n$ kaikilla $n \in A$.*

Todistus. Ks. [8], s. 86. □

Varsinainen todistus on luonteeltaan algoritminen:

Lause 5.28. *Olkoon G numeroituvasti ääretön ryhmä. Jos $G = \langle S \rangle$ ja S on numeroituvasti ääretön, niin Cayleyn graafi $\Gamma(G, S)$ on 1-faktoroituva.*

Todistus. Olkoon G numeroituvasti ääretön ryhmä ja $G = \langle S \rangle$, missä S on numeroituvasti ääretön joukko. Indeksoidaan ryhmän G alkiot indeksein $i \in \mathbb{N}$ ja hyvinjärjestetään alkiot indeksin perusteella. Näin voidaan menetellä hyvinjärjestysperiaatteen (lause 5.27) nojalla. Koska ryhmän G alkiot vastaavat Cayleyn graafin $\Gamma(G, S)$ solmuja määritelmän 4.3 mukaisesti, voidaan yhtäpitävästi puhua solmujoukon indeksoinnista ja hyvinjärjestämisestä. Olkoon $\{v_0, v_1, \dots\}$ graafin $\Gamma(G, S)$ hyvinjärjestetty solmujoukko. Muodostetaan nyt graafin 1-faktorointi seuraavasti:

1. Olkoon $\mathcal{G}$ sellainen graafin $\Gamma(G, S)$ virittävä aligraafi, jossa ei ole yhtään särmää.

2. Lisätään graafiin $\mathcal{G}$ graafin $\Gamma(G, S)$ särmä $\{v_0, v_i\}$, jossa v_i on hyvinjärjestetyn solmujoukon ensimmäinen sellainen solmu, että $\{v_0, v_i\}$ on graafin $\Gamma(G, S)$ särmä.

3. Lisätään graafiin $\mathcal{G}$ graafin $\Gamma(G, S)$ särmä $\{v_j, v_k\}$, jossa v_j on hyvinjärjestetyn solmujoukon ensimmäinen ei-valittu solmu ja v_k ensimmäinen sellainen ei-valittu solmu, että $\{v_j, v_k\}$ on graafin $\Gamma(G, S)$ särmä.

4. Toistetaan edellistä kohtaa, jolloin graafista $\mathcal{G}$ muodostuu graafin $\Gamma(G, S)$ 1-faktori, koska jokaista solmua käytetään prosessissa tismalleen yhden kerran.

5. Poistetaan edellä muodostettuun 1-faktoriin $\mathcal{G}$ kuuluvat särmät graafista $\Gamma(G, S)$.

6. Iteroidaan kohtia 1–5, jolloin saadaan muodostettua graafin $\Gamma(G, S)$ 1-faktorointi.

Edellä kuvatulla algoritmilla saadaan muodostettua Cayleyn graafille $\Gamma(G, S)$ eräs 1-faktorointi, joten kyseinen graafi on 1-faktoroituva. □

Seuraava tulos yleistää seurauksen 5.21 eli Abelin ryhmistä muodostettujen Cayleyn graafien 1-faktoroituvuuden numeroituvasti äärettömille ryhmille.

Lause 5.29. *Jos G on numeroituvasti ääretön Abelin ryhmä ja S on sen numeroituva virittävä joukko, niin Cayleyn graafi $\Gamma(G, S)$ on 1-faktoroituva.*

Todistus. Jos S on numeroituvasti ääretön, suoraan lauseen 5.28 perusteella Cayleyn graafi $\Gamma(G, S)$ on 1-faktoroituva. Oletetaan siis, että joukko S on äärellinen. Tällöin G on äärellisesti virittyvä Abelin ryhmä, joka on lauseen 3.64 perusteella isomorfinen muotoa

$$\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s} \times \mathbb{Z}^r$$

olevan ryhmän kanssa, missä $r \geq 0$ ja n_i on alkuluku kaikilla $i \in \{1, \ldots, s\}$. Merkitään nyt $H = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$, jolloin

$$G \cong H \times \mathbb{Z}^r.$$

Selvästi H on äärellinen ryhmä. Merkitään edelleen $S' = S \cap H$, ja olkoon $s \in S$, $s \notin H$, sellainen alkio, jonka kertaluku on ääretön. Tällöin lause 5.20 yleistyy tilanteeseen suoraan, sillä suora tulo $\times$ on puolisuoran tulon $\rtimes$ erityistapaus ja sekä H että $\mathbb{Z}^r$ ovat Abelin ryhmiä, eli kaikilla $h \in S'$ on voimassa $shs^{-1} = h$. Siispä Cayleyn graafi $\Gamma(G, S)$ on 1-faktoroituva. □

Edellisten lauseiden lisäksi ainakin apulauseet 5.14 ja 5.17 sekä niiden seuraukset voitaisiin yleistää numeroituvasti äärettömille ryhmille. Tässä tutkielmassa todistuksia ei kuitenkaan esitetä aiheen rajaustarpeeseen vedoten.

6 Yhteenveto ja jatkotutkimusmahdollisuuksista

Tässä pro gradu -tutkielmassa tarkasteltiin Cayleyn graafeja ja niihin liittyvää Cayleyn graafien 1-faktorointikonjektuuria, jonka mukaan kaikki parillisen kertaluvun ryhmien Cayleyn graafit ovat 1-faktoroituvia. Konjektuuri todistettiin Stongin artikkeliin [23] perustuen kertalukua 2^k oleville äärellisille ryhmille, äärellisille parillisen kertaluvun Abelin ryhmille ja äärellisille diedriryhmille. Abdollahin artikkeliin [1] perustuen todistettiin, että konjektuuri on voimassa äärellisille parillisen kertaluvun nilpotenteille ryhmille. Numeroituvasti äärettömien ryhmien osalta käytiin läpi Stongin artikkelin tulokset, joiden mukaan konjektuuri on voimassa äärettömästi virittyville numeroituvasti äärettömille ryhmille ja numeroituvasti äärettömille Abelin ryhmille.

Päätulosten ohella tutkielmassa käsiteltiin varsin laajasti graafi- ja ryhmäteoreettisia esitietoja. Todistettiin, että jokainen äärellisesti virittyvä ryhmä on isomorfinen yhtenäisen, suuntaamattoman ja paikallisesti äärellisen graafin symmetriaryhmän aliryhmän kanssa, ja samalla konstruoitiin Cayleyn graafit. Cayleyn graafien käsittelyä syvennettiin tarkastelemalla niiden vaihtoehtoisia määritelmiä, ominaisuuksia sekä esimerkkejä Cayleyn graafeista. Merkittävänä todistettuna tuloksena mainittakoon myös graafien särmävärityksiin liittyvä Vizingin lause, jota hyödynnettiin Cayleyn graafien 1-faktorointikonjektuurin osatulosten todistamisessa.

Tutkielman aihe on vaativa ja edellytti runsaasti esitietojen käsittelyä, minkä vuoksi paljon mielenkiintoisia tuloksia ja näkökulmia jouduttiin rajaamaan tarkastelun ulkopuolelle tai jättämään maininnan tasolle. Käydään seuraavaksi läpi merkittävimpiä tällaisia aiheita.

Selkein mahdollisen jatkotutkimuksen aihe on ne Stongin artikkelin tulokset, joita ei tässä tutkielmassa pystytty käymään läpi. Näitä ovat lauseen 5.11 kohdat 2 ja 3. Lisäksi Stong todisti numeroituvasti äärettömille ryhmille, että kun $G * H$ on eitriviaalien ryhmien G ja H vapaa tulo ja joukko S virittää ryhmän $G * H$, niin Cayleyn graafi $\Gamma(G*H, S)$ on 1-faktoroituva. Toisena merkittävänä mutta pitkälti tutkielmassa sivuutettuna aiheena tässä ansaitsee tulla mainituksi alaluvussa 4.3 lyhyesti käsitelty Sabidussin lause (ks. [21]).

Graafiteorian ja algebrallisen graafiteorian tutkimiseen voidaan erinomaisesti soveltaa tietokoneita, ja monesti graafiteoreetikoilla onkin tietojenkäsittelyteoreettista taustaa. Laskennallisia menetelmiä Cayleyn graafien 1-faktorointikonjektuurin tutkimisessa ovat hyödyntäneet mm. Herke ja Maenhaut ([10] ja [11]), jotka ovat myös pystyneet tekemään havaintojensa perusteella uuden konjektuurin artikkelissaan [10].

Muista graafiteoriaa, erityisesti algebrallista graafiteoriaa ja Cayleyn graafeja, tutkineista matemaatikoista tässä mainittakoon Alspach, joka on tutkinut paitsi Cayleyn graafien 1-faktoroituvuutta (esim. [2]) myös muita algebrallisen graafiteorian aiheita, sekä Lovász, jonka tutkimus on keskittynyt erityisesti kombinatoriikkaan. Graafiteoriassa Lovász tunnetaan erityisesti esittämästään Lovászin konjektuurista, jonka mukaan jokainen yhtenäinen solmutransitiivinen graafi (jollaisia myös Cay-

leyn graafit ovat) sisältää Hamiltonin syklin [19]. Hamiltonin sykli on sykli, joka käy jokaisessa graafin solmussa tismalleen kerran [7].

Cayleyn graafien 1-faktorointikonjektuurin tarkastelu rajattiin tässä tutkielmassa tietoisesti sellaisiin tuloksiin, jotka koskevat suoraan nimenomaan Cayleyn graafeja, eikä kartoitettu laajamittaisesti, millaisia tuloksia 1-faktoroituvuuteen liittyen on Stongin artikkelin julkaisemisen jälkeen todistettu yleisesti graafeille. Merkittävä tällainen tulos on Csaban ym. teoksessa [5], jossa löydettiin graafin säännöllisyyteen liittyvä riittävä ehto 1-faktoroituvuudelle: nimittäin jos n on parillinen ja $D \geq 2\lceil n/4 \rceil - 1$, niin jokainen D-säännöllinen graafi, jossa on n solmua, voidaan jakaa täydellisiin sovituksiin (sovituksien osalta ks. alaluvun 5.1 huomautus). Tulos on samanhenkinen kuin Cayleyn graafien 1-faktorointikonjektuuri, sillä se koskee graafeja, joissa on parillinen määrä solmuja, ja toisaalta Cayleyn graafit ovat säännöllisiä graafeja. Lisäksi täydelliset sovitukset ja 1-faktorit vastaavat osittain toisiaan. Koska Cayleyn graafissa solmun aste riippuu yksinomaan virittävästä joukosta, ei tulos ole voimassa kaikilla virittävillä joukoilla eikä täten kaikilla Cayleyn graafeilla, vaikkakin tulos kattaa valtavan perheen Cayleyn graafeja.

Eräs merkittävä Cayleyn graafien matemaattinen anti on se, että ne haastavat perinteistä ajattelua, jossa ryhmät mielletään puhtaasti algebrallisiksi, abstrakteiksi objekteiksi, liittämällä ryhmiin geometrisen rakenteen ja täten mahdollistamalla täysin uusien tulosten käytön ryhmien tutkimisessa. Geometrinen esitys myös vahvistaa intuitiivista ymmärrystä ryhmän algebrallisesta rakenteesta. Tällainen ajatus ei kuitenkaan rajaudu pelkästään graafiteoriaan, vaan samanlaista metodia voidaan soveltaa muillakin matematiikan osa-alueilla. Näin ollen ryhmiin voidaan liittää mm. topologisen avaruuden rakenne, jolloin päädytään tarkastelemaan topologisia ryhmiä, tai moniston rakenne, jolloin ryhmää kutsutaan Lien ryhmäksi [24]. Sekä topologiset ryhmät että Lien ryhmät ovat mahdollisia jatkotutkimuksen aiheita.

Lähteet

[1] Abdollahi, A. 1-Factorizations of Cayley graphs. Ars Combinatoria 86 (2008), 129–131. Ennakkojulkaisu saatavilla osoitteessa https://doi.org/10.48550/arXiv.0705.0193.

[2] Alspach, B., Morton, M. & Qin, Y. 1-factorizations of Cayley graphs on solvable groups. Verkkoartikkeli, 1998. URL https://researchspace.auckland.ac.nz/bitstream/handle/2292/5039/393.pdf.

[3] Biggs, N. Algebraic Graph Theory, 2. painos. Cambridge University Press, Cambridge, 1993.

[4] Cayley, A. Desiderata and Suggestions: No. 2. The Theory of Groups: Graphical Representation. American Journal of Mathematics 1 (1878).

[5] Csaba, B., Kühn, D., Lo, A., Osthus, D. & Treglown, A. Proof of the 1-factorization and Hamilton decomposition conjectures. Memoirs of the American Mathematical Society 244, 3 (2013).

[6] Dehn, M. Über unendliche diskontinuierliche Gruppen. Math. Ann. 71 (1912), 116–144.

[7] Diestel, R. Graph Theory, 5. painos. Springer, Heidelberg, 2017.

[8] Enderton, H. Elements of Set Theory, 1. painos. Academic Press, New York, 1977.

[9] Hammack, R., Imrich, W. & Klavžar, S. Handbook of Product Graphs, 2. painos. CRC Press, Boca Raton, 2011.

[10] Herke, S. & Maenhaut, B. Perfect 1-Factorisations of Circulants with Small Degree. The Electronic Journal of Combinatorics 20, 1 (2013).

[11] Herke, S. & Maenhaut, B. Perfect 1-Factorizations of a Family of Cayley Graphs. Journal of Combinatorial Designs 23, 9 (2014), 369–399.

[12] Humphreys, J. A Course in Group Theory, 1. painos. Oxford University Press, Oxford, 1996.

[13] Jungnickel, D. Graphs, Networks and Algorithms, 2. painos. Springer, Heidelberg, 2005.

[14] Kangaslampi, R., Koivisto, P. & Niemistö, R. Graafiteoriaa. Opetusmoniste. Tampereen yliopisto, Tampere, 2022.

[15] Karppanen, M. Nilpotentin ryhmän ekvivalentit määritelmät. Pro gradu -tutkielma. Helsingin yliopisto, Helsinki, 2014.

[16] Lovász, L. & Plummer, M. Matching Theory, 1. painos. AMS Chelsea Publishing, Providence, 2009.

[17] Meier, J. Groups, Graphs and Trees: An Introduction to the Geometry of Infinite Groups, 1. painos. Cambridge University Press, Cambridge, 2008.

[18] Parattu, K. & Wingerter, A. Finite Groups of Order Less Than or Equal to 100. Lisämateriaalia ennakkojulkaisuun Tribimaximal Mixing From Small Groups. arXiv.org, 2011. URL https://doi.org/10.48550/arXiv.1012.2842.

[19] Qin, Y. On Subgraphs of Vertex-transitive Graphs. Väitöskirja. Simon Fraser University, Burnaby, 1998.

[20] Rotman, J. An Introduction to the Theory of Groups, 4. painos. Springer, New York, 1995.

[21] Sabidussi, G. On a Class of Fixed-point-free Graphs. Proceedings of the American Mathematical Society 9, 5 (1958), 800–804.

[22] Stern, G. & Lenz, H. Steiner Triple Systems with Given Subspaces: Another Proof of the Doyen-Wilson Theorem. Bolletino dell Unione Matematica Italiana 17 (1980), 109–114.

[23] Stong, R. On 1-Factorizability of Cayley Graphs. Journal of Combinatorial Theory, Series B 39, 3 (1985), 298–307.

[24] Tao, T. Cayley graphs and the geometry of groups. Blogiteksti. terrytao.wordpress.com, 2010. URL https://terrytao.wordpress.com/2010/07/10/cayley-graphs-and-the-geometry-of-groups.