Ryhmien kasvunopeus

LuK Tuuli Lankila

Pro gradu -tutkielma
2024

Tarkastajat:
Dos. Ilkka Törmä
Dos. Ville Salo

MATEMATIIKAN JA TILASTOTIETEEN LAITOS

TURUN YLIOPISTO
Matematiikan ja tilastotieteen laitos

Tuuli Lankila: Ryhmien kasvunopeus
Pro gradu -tutkielma, 32 s.
Matematiikka
2024

Tutkielma keskittyy ryhmien kasvunopeuden tarkasteluun. Erityisesti tarkastellaan kolmea päätyyppiä ryhmien kasvulle: polynomista, eksponentiaalista ja välimuotoista kasvua. Lisäksi tutkielmassa syvennytään eri ryhmien kasvutyyppien ominaisuuksiin ja tutkitaan, miten nämä ominaisuudet vaikuttavat ryhmien rakenteeseen. Erityisesti kiinnitetään huomiota nilpotenttien ja ratkeavien ryhmien kasvunopeuteen sekä esitellään Grigorchukin ryhmä, joka oli ensimmäinen esimerkki ryhmästä, jolla on välimuotoista kasvua. Tutkielman tavoitteena on syventää ymmärrystä ryhmien kasvunopeuden matemaattisista ominaisuuksista sekä niiden merkityksestä ryhmäteorian tutkimuksessa.

Asiasanat: ryhmä, kasvufunktio, kasvunopeus, Grigorchukin ryhmä

Sisällys

1 Johdanto

Ryhmien kasvunopeus kuvaa sitä, miten nopeasti äärellisen joukon generoima ryhmä kasvaa, kun sen alkioita kerrotaan keskenään. Jokainen ryhmän alkio voidaan kirjoittaa ryhmän generaattorien tulona ja kasvunopeus laskee, kuinka monta alkiota voidaan kirjoittaa sisältäen n kappaletta generaattoreita.

Ryhmien kasvunopeuden esitteli ensimmäisen kerran amerikkalainen matemaatikko John Milnor vuonna 1968 artikkelissaan *A Note on Curvature and Fundamental Group* [8]. Erityisesti huomion kiinnitti aikanaan Milnorin asettamat kaksi kysymystä:

1. Onko olemassa sellaisia äärellisen joukon generoimia ryhmiä, joilla on välimuotoista kasvua, eli kasvua polynomisen ja eksponentiaalisen kasvun välissä?

2. Millä ryhmillä on polynomista kasvua?

Toiseen kysymykseen saatiin ratkaisu vuonna 1981, kun Mikhael Gromov osoitti, että ryhmällä on polynomista kasvua jos ja vain jos se sisältää nilpontentin aliryhmän, jolla on äärellinen indeksi [10]. Venäläinen matemaatikko Rostislav Grigorchuk vastasi ensimmäiseen kysymykseen pari vuotta Gromovin jälkeen vuonna 1983 konstruoidessaan ensimmäisen esimerkin äärellisen joukon generoimasta ryhmästä, jolla on välimuotoista kasvua. Kyseinen ryhmä onkin nimetty hänen mukaansa Grigorchukin ryhmäksi [10]. Nykytutkimuksessa ryhmien kasvunopeus on merkittävä tutkimuksen kohde.

Tässä tutkielmassa syvennytään ryhmän kasvunopeuden kolmeen tyyppiin ja niiden ominaisuuksiin. Lisäksi tarkastellaan eri kasvutyyppejä olevia ryhmiä ja osoitetaan niille kasvunopeuteen liittyviä tuloksia. Erityisesti tutustutaan edellä mainittuun Grigorchukin ryhmään, joka oli merkittävä edistysaskel ryhmien kasvutyyppien tutkimuksessa. Luku 2 sisältää esitietoja, jotka ovat oleellisia, kun perehdytään tarkemmin erilaisten ryhmien kasvutyyppeihin. Luvuissa 2.1 ja 2.2 käsitellään nilpotentit, ratkeavat ja polysykliset ryhmät, joiden kasvun ominaisuuksia tarkastellaan myöhemmin tutkielmassa tarkemmin. Lisäksi määritellään sanametriikan määritelmä luvussa 3, jonka jälkeen voidaan siirtyä tutkielman varsinaiseen teemaan.

Luvussa 4 esitellään ensin ryhmän kasvufunktiot, joiden pohjalta määritellään kasvun kolme tyyppiä; polynominen, eksponentiaalinen ja välimuotoinen kasvu. Lisäksi todistetaan joitain oleellisia niihin liittyviä ominaisuuksia, kuten milloin kaksi ryhmää ovat samaa kasvun tyyppiä. Tästä siirrytään tutkimaan tarkemmin, mitä kasvu merkitsee nilpotenttien ryhmien kohdalla luvussa 6, jonka päätuloksena todistetaan, että nilpotenteilla ryhmillä on polynomista kasvua.

Nilpotenttien ryhmien jälkeen tarkastellaan ratkeavien ryhmien kasvun ominaisuuksia luvussa 7 ja todistetaan lopuksi tulos, jonka mukaan äärellisen joukon generoiman ratkeavan ryhmän kasvu on välttämättä joko eksponentiaalista tai polynomista.

Grigorchukin ryhmä konstruoidaan viimeisenä luvussa 8 kahdella tapaa: ensin samaan tapaan kuin Grigorchuk alun perin itse vuonna 1983, eli sovelletaan permutaatioita yksikkövälille ja toisena binääriaakkoston avulla. Luvussa todistetaan Grigorchukin ryhmälle monia mielenkiintoisia ominaisuuksia, joista merkittävin tut-

kielman kannalta on tietenkin se, että Grigorchukin ryhmällä on välimuotoista kasvua.

2 Ryhmäteoriaa

Tässä luvussa käsitellään tutkielman kannalta keskeisiä ryhmäteorian määritelmiä ja tuloksia.

Määritelmä 1. Olkoon G ryhmä, jonka generoi joukko X. Joukkoa X kutsutaan *symmetriseksi*, jos $X = X^{-1}$ eli jos $x \in X$, niin $x^{-1} \in X$.

Määritelmä 2. [4] Olkoon G ryhmä ja H sen aliryhmä. Aliryhmän H muodostamien vasempien sivuluokkien lukumäärää kutsutaan ryhmän H *indeksiksi* ryhmässä G ja sitä merkitään $[G : H]$. Jos G on äärellinen, niin $[G : H] = |G|/|H|$.

Lause 1. *[2] Olkoon G äärellisen joukon generoima ryhmä ja H sen aliryhmä, jolla on äärellinen indeksi. Tällöin myös H on äärellisen joukon generoima.*

Todistus. Olkoon $R \subset G$ ryhmän G oikeiden sivuluokkien edustajisto eli jokaista ekvivalenssiluokkaa edustaa yksi alkio joukosssa R ja $1_G \in R$. Tällöin $|R| = [G : R]$ on äärellinen. Olkoon S äärellinen ryhmän G generoiva joukko, jolle pätee, että jos $s \in S$, niin $s^{-1} \in S$. Osoitetaan, että

$$S' = RSR^{-1} \cap H$$

generoi ryhmän H. Olkoon $h \in H$. Merkitään $h = s_1 s_2 \cdots s_n$, $s_i \in S$. On olemassa sellaiset alkiot $h_1 \in H$ ja $r_1 \in R$, että $s_1 = h_1 r_1$. Tällöin $h_1 = 1_G s_1 r_1^{-1} \in S'$. Induktion avulla saadaan, että kaikilla $i = 2, 3, \ldots, n-1$ on olemassa sellaiset alkiot $h_i \in H$ ja $r_i \in R$ siten, että $r_{i-1} s_i = h_i r_i$ eli $h_i = r_{i-1} s_i r_i^{-1} \in S'$. Asettamalla $h_n = r_{n-1} s_n$, saadaan

$$\begin{aligned} h &= s_1 \cdots s_n \\ &= (1_G s_1 r_1^{-1})(r_1 s_2 r_2^{-1}) \cdots (r_{n-2} s_{n-1} r_{n-1}^{-1})(r_{n-1} s_n) \\ &= h_1 h_2 \cdots h_{n-1} h_n. \end{aligned}$$

Huomataan, että $h_n = h_{n-1}^{-1} \cdots h_2^{-1} h_1^{-1} \in H$ ja $h_n = r_{n-1} s_n = r_{n-1} s_n 1_G \in RSR^{-1}$, joten $h_n \in S'$. Eli joukko S' generoi ryhmän H. □

Lause 2. *[2] Olkoon G ryhmä ja N sen normaali aliryhmä. Oletetaan, että ryhmät N ja G/N ovat äärellisen joukon generoimia. Tällöin ryhmä G on äärellisen joukon generoima.*

Todistus. Merkitään tekijänryhmän homomorfismia $\pi : G \to G/N$. Olkoon $U \subseteq N$ ja $T \subseteq G/N$ kaksi symmetristä ryhmät N ja G/N generoivaa joukkoa. Olkoon $S \subseteq G$ äärellinen symmetrinen joukko, siten että $\pi(S) \supseteq T$ ja $U \subseteq S$. Olkoon $g \in G$. Nyt on olemassa sellaiset $h \geq 0$ ja $t_1, t_2, \ldots, t_H \in T$ siten, että $\pi(g) = t_1 t_2 \cdots t_h$. Olkoot $s_1, s_2, \ldots, s_h \in S$ sellaiset alkiot, että $\pi(s_i) = t_i$ kaikilla $i = 1, 2, \ldots, h$. Asettamalla $g' = s_1 s_2 \cdots s_h$, saadaan $\pi(g) = \pi(g')$. Tästä seuraa, että $n = (g')^{-1} g \in \mathrm{Ker}(\pi) = N$. Näin ollen on olemassa sellainen $k \geq 0$ ja $s_{h+1}, s_{h+2}, \ldots, s_{h+k} \in S$, että $n = s_{h+1} s_{h+2} \cdots s_{h+k}$. Nyt $g = g'n = s_1 s_2 \cdots s_h s_{h+1} s_{h+2} \cdots s_{h+k}$. Eli joukko S generoi ryhmän G. □

Määritelmä 3. [3] Oletetaan, että G on ryhmä ja $g, h \in G$ mielivaltaisia. Alkiota

$$[g, h] = ghg^{-1}h^{-1} \in G$$

kutsutaan alkioiden g ja h *kommutaattoriksi*.

Aliryhmästä, jonka generoi kaikki ryhmän G kommutaattorit eli *kommutaattorialiryhmästä*, käytetään merkintää G' tai $[G, G]$. Yleisesti, jos $H \leq G$ ja $K \leq G$, merkinnällä $[H, K]$ tarkoitetaan aliryhmää, jonka generoi kommutaattorit $[h, k]$, jossa $h \in H$ ja $k \in K$.

Merkitään $G^{(i)} = [G^{(i-1)}, G^{(i-1)}]$, jossa $G^{(0)} = G$. Tällöin $G^{(1)} = G' \trianglelefteq G$ ja seuraava lause osoittaa, että G/G' on Abelin ryhmä.

Lause 3. *[3] Olkoon G' ryhmän G kommutaattorialiryhmä. G/G' on Abelin ryhmä.*

Todistus. Olkoon $xG', yG' \in G/G'$, jolloin $x^{-1}y^{-1}xyG' = G'$, sillä $x^{-1}y^{-1}xy \in G'$. Tästä seuraa, että $xyG' = yxG'$, joten xG' ja yG' kommutoivat tekijäryhmässä G/G'. Tämä pätee kaikilla $x, y \in G$, joten G/G' on Abelin ryhmä. □

Määritelmä 4. Olkoon X mikä tahansa joukko, jossa on määritelty binäärioperaatio $*$. Joukkoa $(X, *)$ kutsutaan *monoidiksi*, jos se toteuttaa seuraavat ehdot:

1. $a * b \in X$,
2. $(a * b) * c = a * (b * c)$,
3. on olemassa sellainen $e \in X$, että $e * a = a * e = a$,

kaikilla $a, b, c \in X$.

Määritelmä 5. Olkoon G ryhmä ja $S \subseteq G$. Joukon S *normaali sulkeuma* $\mathrm{ncl}_G(S)$ on leikkaus kaikista ryhmän G normaaleista aliryhmistä, jotka sisältävät joukon S. Normaali sulkeuma $\mathrm{ncl}_G(S)$ on tällöin pienin joukon G normaali aliryhmä, joka sisältää joukon S.

Määritelmä 6. Ryhmä G on residuaalisesti äärellinen, jos jokaiselle alkiolle $g \in G$, $g \neq 1_G$ on olemassa äärellinen joukko S ja homomorfismi $h : G \to S$, että $h(g) \neq 1$.

Määritelmä 7. [1] Kaksi ryhmää, G ja H, ovat *yhteismitallisia*, jos on olemassa sellaiset aliryhmät $K < G$ ja $L < H$, että $[G : K]$ ja $[H : L]$ ovat äärellisiä ja $K \cong L$. Ryhmät G ja H ovat *kvasi-yhteismitallisia*, jos on olemassa sellaiset $M \trianglelefteq K \leq G$ ja $N \trianglelefteq L \leq H$ niin, että $[G : K]$, $[H : L]$, $|M|$ ja $|N|$ ovat äärellisiä ja $K/M \cong L/N$.

Määritelmä 8. [4] Olkoon G ryhmä. Kuvaus $\phi : G \to G$ on *automorfismi*, jos ϕ on isomorfismi. Ryhmän G automorfismien joukkoa merkitään $\mathrm{Aut}(G)$

Määritellään vielä ryhmien karakteristiset aliryhmät. Karakterististet aliryhmät pysyvät samoina, kun kuvataan ryhmää isomorfisesti itselleen.

Määritelmä 9. Olkoon G ryhmä ja H sen aliryhmä. H on *karakteristinen aliryhmä*, jos $\phi(H) = H$ kaikilla $\phi \in \mathrm{Aut}(G)$.

2.1 Ratkeavat ja polysykliset ryhmät

Luku perustuu lähteeseen [1].

Määritelmä 10. Ryhmä G on *ratkeava*, jos sillä on normaalisarja

$$1 = G_n \trianglelefteq G_{n-1} \trianglelefteq \cdots \trianglelefteq G_1 = G, \tag{1}$$

ja tekijäryhmät G_{i-1}/G_i ovat Abelin ryhmiä.

Määritelmä 11. Seuraavat yhtäpitävät ehdot toteuttavaa ryhmää kutsutaan *Noetherin ryhmäksi*:

(*i*) *Maksimaalisuusehto*: Millä tahansa joukolla ryhmän G aliryhmiä, on olemassa maksimaalinen alkio.

(*ii*) *Kasvavan ketjun ehto*: Aidosti kasvava ketju ryhmän G aliryhmiä

$$G_1 < G_2 < \cdots < G_n < \ldots$$

on äärellinen.

(*iii*) Jokainen ryhmän G aliryhmä on äärellisen joukon generoima.

Määritelmä 12. Olkoon p jokin alkuluku. Sanotaan, että äärellinen ryhmä G on p-ryhmä, jos p on sen kertaluvun ainoa tekijä. Tällöin $|G| = p^n$ jollekin kokonaisluvulle $n > 0$.

Lause 4. *Ratkeava ryhmä on Noetherin ryhmä jos ja vain jos sillä on normaalisarja, joka sisältää vain syklisiä tekijöitä.*

Todistus. Olkoon ryhmällä G normaalisarja, joka sisältää syklisiä tekijöitä. Olkoon $H \leq G$ aliryhmä. Osoitetaan, että se on äärellisen joukon generoima. Merkitään $H_i = H \cap G_i$. Todistetaan induktiolla i:n suhteen arvosta $i = n$, että H_i on äärellisen joukon generoima. Arvolla $i = n$ on $H_n = 1$, joten väite on selvä. Oletetaan sitten, että H_i on äärellisen joukon generoima. Nyt H_i on ryhmän H_{i-1} normaali aliryhmä ja $H_{i-1}/H_i = H_{i-1}/G_i \leq G_{i-1}/G_1$ on syklisen ryhmän aliryhmänä syklinen, siis äärellisen joukon generoima. Lauseen 2 mukaan H_{i-1} on siis äärellisen joukon generoima. Ryhmä G siis toteuttaa määritelmän 11 eli G on Noetherin ryhmä.

Olkoon G Noetherin ryhmä. Tällöin sarjassa (1) kaikki tekijät ovat äärellisen joukon generoimia Abelin ryhmiä, jotka ovat syklisten ryhmien suoria summia. Sarja (1) voidaan siis kehittää normaalisarjaksi, jossa on vain syklisiä tekijöitä. □

Edellisen lauseen takia ratkeavia Noetherin ryhmiä kutsutaan *polysyklisiksi ryhmiksi*. Tästä eteenpäin tutkielmassa käytetään tätä nimitystä.

Määritelmä 13. Olkoon G polysyklinen ryhmä ja olkoon (1) sen normaalisarja, joka koostuu syklisistä tekijöistä. Äärettömien tekijöiden määrää tässä sarjassa kutsutaan tällöin ryhmän G *Hirschin pituudeksi* ja siitä käytetään merkintää $h(G)$.

2.2 Nilpotentit ryhmät

Luku perustuu lähteisiin [1] ja [9].

Määritelmä 14. Ryhmän G keskus $Z(G)$ on joukko $\{x \in G \mid xy = yx \text{ kaikilla } y \in G\}$.

Määritelmä 15. Ryhmän G normaalisarja (1) on keskussarja, jos sen kaikille epätriviaaleille tekijöille G_{i-1}/G_i pätee keskussarjaehto eli $G_{i-1}/G_i \subseteq Z(G/G_i)$. Jos ryhmällä on keskussarja, niin silloin kyseistä ryhmä kutsutaan *nilpotentiksi.*

Esimerkki 1. Olkoon G ryhmä ja $G/Z(G)$ Abelin ryhmä. Tällöin ryhmällä G on normaalisarja $1 \subseteq Z(G) \subseteq G$. Keskussarjaehto on voimassa ensimmäiselle tekijälle $Z(G)/1$, koska $Z(G)/1 = Z(G) = Z(G/1)$. Toiselle tekijälle $G/Z(G) = Z(G/Z(G))$ eli keskussarjaehto on myös voimassa. Näin ollen ryhmä G on nilpotentti ja erityisesti voidaan todeta, että kaikki Abelin ryhmät ovat nilpotentteja.

Määritelmä 16. Ryhmän G *alempi keskussarja* $\gamma_i(G)$ määritellään olevan $\gamma_1(G) = G$ ja $\gamma_{i+1} = [\gamma_i(G), G]$.

Jos (1) on ryhmän G keskussarja, niin $\gamma_i(G) \leq G_i$. Tällöin G on nilpotentti jos ja vain jos $\gamma_{c+1}(G) = 1$ jollekin c. Jos c on ensimmäinen indeksi, jolle edellinen pätee, niin c on ryhmän G keskussarjan lyhin pituus ja voidaan sanoa ryhmän G kuuluvan *nilpotenssiluokkaan* c.

3 Sanametriikka

Luku pohjautuu lähteeseen [2].

Olkoon G äärellisen ja symmetrisen joukon X generoima ryhmä. Kaikilla alkioille $g \in G$ on siis olemassa luku $n \geq 0$, $x_1, \ldots, x_n \in X$ ja $\epsilon_1, \ldots, \epsilon_n \in \{-1, 1\}$ siten, että

$$g = x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_n^{\epsilon_n}. \tag{2}$$

Sanan pituus $l_X(g) = l_X^G(g)$ alkiolle $g \in G$ ryhmässä G määritellään olevan pienin lukumäärä generaattoreita $x_i \in X$, jolla $g \in G$ voidaan esittää muodossa (2). Eli

$$l_X(g) = \min\{n \geq 0 \ : \ x_1 x_2 \cdots x_n = g, x_i \in X, 1 \leq i \leq n\}.$$

Määritelmästä seuraa, että $l_X(g) = 0$ jos ja vain jos $g = 1_G$.

Lause 5. *Seuraavat yhtälöt ovat voimassa:*

$$l_X(g^{-1}) = l_X(g)$$

ja

$$l_X(gh) \leq l_X(g) + l_X(h)$$

kaikilla $g, h \in G$.

Todistus. Olkoon $g, h \in G$. Asetetaan $l_X(g) = m$ ja $l_X(h) = n$. Tällöin on olemassa sellaiset $x_1, \ldots, x_m \in X$ ja $y_1, \ldots, y_n \in X$, että $g = x_1 \cdots x_m$ ja $h = y_1 \cdots y_n$. Nyt $g^{-1} = x_m^{-1} \cdots x_1^{-1}$ ja $l_X(g^{-1}) \leq m = l_X(g)$. Toistamalla sama päättelyketju toisinpäin (eli aloittaen alkiosta g^{-1}), saadaan $l_X(g^{-1}) = l_X(g)$.

Koska $gh = x_1 \cdots x_m y_1, \ldots, y_n$, niin $l_X(gh) \leq m + n = l_X(g) + l_X(h)$. □

Tarkastellaan seuraavaksi kuvausta $d_X = d_X^G : G \times G \to \mathbb{N}$, jolle

$$d_X(g, h) = l_X(g^{-1}h)$$

kaikilla $g, h \in G$.

Lause 6. *Kuvaus d_X on metriikka joukossa G.*

Todistus. Olkoon $g, h, k \in G$. Koska $l_X(g) = 0$ jos ja vain jos $g = 1_G$, niin $d_X(g, h) = 0$ jos ja vain jos $h = g$. Lauseesta 5 seuraa, että $d_X(g, h) = d_X(h, g)$, sekä

$$\begin{aligned} d_X(g, k) + d_X(k, h) &= l_X(g^{-1}k) + l_X(k^{-1}h) \\ &\geq l_X((g^{-1}k)(k^{-1}h)) \\ &= l_X(g^{-1}h) \\ &= d_X(g, h). \end{aligned}$$

□

Metriikkaa d_X kutsutaan *sanametriikaksi* ryhmässä G suhteessa äärelliseen generoivaan joukkoon X.

Lause 7. *Metriikka d_X on invariantti vasemmalta kertomisen suhteen eli*

$$d_X(gg_1, gg_2) = d_X(g_1, g_2)$$

kaikilla $g, g_1, g_2 \in G$.

Todistus. Kaikilla $g, g_1, g_2 \in G$ pätee

$$d_X(gg_1, gg_2) = l_X(g_1^{-1}g^{-1}gg_2) = l_X(g_1^{-1}g_2) = d_X(g_1, g_2).$$

□

Olkoon $g \in G$ ja $n \in \mathbb{N}$. Merkintää

$$B_X^G(g, n) = \{h \in G \ : \ d_X(g, h) \leq n\}$$

kutsutaan *n-säteiseksi palloksi* joukossa G, jonka keskipiste on alkio $g \in G$. Kun $g = 1_G$, niin $B_X^G(1_G, n) = \{h \in G \ : \ l_X(h) \leq n\}$ ja voidaan lyhyemmin merkitä $B_X^G(1_G, n) = B_X^G(n)$. Kun ryhmä G on kontekstista selvä, voidaan kirjoittaa $B_X^G(g, n) = B_X(g, n)$ ja $B_X^G(n) = B_X(n)$.

Määritelmä 17. Olkoon $X \neq \emptyset$. Joukon X metriikat d_1 ja d_2 ovat *Lipschitz-ekvivalentit*, jos on olemassa sellaiset $h, k > 0$, että

$$hd_2(x, y) \leq d_1(x, y) \leq kd_2(x, y)$$

kaikilla $x, y \in X$.

4 Ryhmien kasvunopeus

Seuraavaksi määritellään kasvufunktiot, sekä niiden avulla kasvun tyypit ja kasvunopeus. Luvussa on käytetty lähteitä [1] ja [2].

4.1 Kasvufunktiot

Olkoon G ääretön ryhmä, jonka generoi joukko $X = \{x_1, \ldots, x_i\}$. Jokainen alkio $x \in G$ voidaan kirjoittaa sanana $x = y_1 \cdots y_n$, jossa $y_j \in X$ tai $y_j^{-1} \in X$. Olkoot $a_X^G(n)$ n:n mittaisten alkioiden lukumäärä ryhmässä G ja $s_S^G(n)$ niiden sanojen lukumäärä, joiden pituus on enintään n ryhmässä G. Tällöin s_X^G on funktio $s_X^G : \mathbb{N} \to \mathbb{N}$, jolle

$$s_X^G(n) = \sum_{i=0}^{n} a_X^G(i).$$

Funktio voidaan myös esittää seuraavassa ekvivalentissa muodossa:

$$s_X^G(n) = |B_X^G(n)| = |\{g \in G : l_X(g) \leq n\}|.$$

Funktioita $a(n)$ ja $s(n)$ kutsutaan ryhmän G *kasvufunktioiksi.* Funktio $a(n)$ on ryhmän G *tiukka kasvufunktio* ja funktio $s(n)$ on ryhmän G *kumulatiivinen kasvufunktio.* Kumulatiivisesta kasvufunktiosta voidaan käyttää myös merkintää s_X (tai s_X^G), jos ryhmän G generoivaa joukkoa halutaan tarkentaa. Tästä eteenpäin kutsutaan kaikkia kasvavia funktioita $f : \mathbb{N} \to [0, \infty)$ kasvufunktioiksi.

Huomataan, että $s_X(0) = |B_X(0)| = |\{1_G\}| = 1$ ja $s_X(n) \leq s_X(n+1)$ kaikilla $n \in \mathbb{N}$. Lisäksi, koska kuvaus $(x_1, x_2, \ldots, x_n) \mapsto x_1 x_2 \cdots x_n$ on surjektio joukosta $(X \cup \{1_G\})^n$ joukkoon $B_X(n)$, niin

$$s_X(n) \leq |X \cup \{1_G\}|^n \tag{3}$$

kaikilla $n \in \mathbb{N}$.

Lause 8. *Seuraavat väitteet ovat keskenään ekvivalentit:*

(i) Ryhmä G on äärellinen.

(ii) $a(n) \to 0$, kun $n \to \infty$.

(iii) $s(n) \to c$, kun $n \to \infty$ ja c on vakio.

Todistus. Osoitetaan ensin, että väitteestä (i) seuraa väite (ii). Koska ryhmä G on äärellinen, on sen alkioilla maksimaalinen pituus. On siis olemassa sellainen n_ϵ, että $a(n) = 0$, kun $n > n_\epsilon$.

Osoitetaan sitten, että väitteestä (ii) seuraa väite (iii). Koska $a(n) = 0$, kun $n > n_\epsilon$, niin $s(n) = \sum_{i=0}^{n} a(i) = \sum_{i=0}^{n_\epsilon} a(i) + \sum_{n_\epsilon}^{n} a(i) = \sum_{i=0}^{n_\epsilon} a(i) + 0 = c$.

Väitteestä (iii) seuraa väite (i) suoraan funktion $s(n)$ määritelmän perusteella. □

Lause 9. *Olkoon G äärellisen joukon generoima ryhmä. Olkoot joukot X ja X' eräät äärelliset, symmetriset joukot, jotka generoivat ryhmän G. Merkitään $c = \max\{l_{X'}(x) : x \in X\}$. Seuraavat väitteet ovat voimassa:*

(i) $l_{X'}(g) \leq cl_X(g)$ *kaikilla* $g \in G$,

(ii) $d_{X'}(g,h) \leq cd_X(g,h)$,

(iii) $B_X(n) \subseteq B_{S'}(cn)$ *kaikilla* $n \in \mathbb{N}$,

(iv) $s_X(n) \leq s_{X'}(cn)$ *kaikilla* $n \in \mathbb{N}$.

Todistus. Olkoon $g \in G$. Oletetaan, että $l_X(g) = n$. Tällöin on olemassa sellaiset $x_1, x_2, \ldots, x_n \in X$, että $g = x_1x_2\cdots x_n$. Nyt

$$g = l_X(x_1x_2\cdots x_n) \leq \sum_{i=1}^{n} l_X(x_i) \leq cn,$$

eli kohta (i) on voimassa.

Kohdan (i) nojalla kaikilla $g, h \in G$ pätee

$$d_{X'}(g,h) = l_{X'}(g^{-1}h) \leq cl_S(g^{-1}h) = cd_X(g,h),$$

joten kohta (ii) on voimassa. Tästä seuraa myös, että $d_{X'}(g, 1_G) \leq cn$, kun $d_X(g, 1_G) \leq n$ kaikilla $g \in G$, joten väite (iii) on voimassa. Tällöin

$$s_X(n) = |B_X(n)| \leq |B_{X'}(cn)| = s_{X'}(cn)$$

kaikilla $n \in \mathbb{N}$, josta saadaan väite (iv). □

Kaksi metriikkaa. d ja d', ovat *Lipschitz-ekvivalentit*, jos on olemassa sellaiset $c_1, c_2 > 0$, että

$$c_1d_X(x,y) \leq d'_X(x,y) \leq c_2d_X(x,y)$$

kaikilla $x, y \in X$.

Seuraus 1. *Olkoon G äärellisen joukon generoima ryhmä ja olkoot X ja X' eräät ryhmän G generoivat äärelliset, symmetriset joukot. Tällöin metriikat d_X ja $d_{X'}$ ovat Lipchitz-ekvivalentit.*

Seuraavaksi muotoillaan kahden kasvufunktion välinen suhde.

Määritelmä 18. Olkoon $f, g : \mathbb{N} \to \mathbb{N}$ (tai $f, g : \mathbb{N} \to \mathbb{R}$ tai $f, g : \mathbb{R} \to \mathbb{R}$) kasvufunktioita. Sanotaan, että g *dominoi* funkiota f, jos on olemassa sellainen kokonaisluku $c \geq 1$, että $f(n) \leq cg(cn)$ kaikilla $n \geq 1$. Tällöin merkitään $f \preceq g$. Funktiot f ja g ovat *ekvivalentit*, jos $f \preceq g$ ja $g \preceq f$ ja siitä käytetään merkintää $f \sim g$.

Lause 10.

(i) $\preceq$ *on refleksiivinen ja transitiivinen relaatio.*

(ii) $\sim$ *on ekvivalenssirelaatio.*

(iii) Olkoon $f, f', g, g' : \mathbb{N} \to [0, \infty)$ *kasvufunktioita. Oletetaan, että* $f \sim f'$, $g \sim g'$ *ja* $f \preceq g$. *Tällöin* $f' \preceq g'$.

Todistus. Selvästi $\preceq$ on refleksiivinen. Olkoon $s_1, s_2, s_3 : \mathbb{N} \to [0, \infty)$ kasvufunktioita. Oletetaan, että $s_1 \preceq s_2$ ja $s_2 \preceq s_3$. Olkoon c_1, c_2 sellaisia positiivisia kokonaislukuja, että $s_1(n) \leq c_1 s_2(c_1 n)$ ja $s_2(n) \leq c_2 s_3(c_2 n)$ kaikilla $c \geq 1$. Valitaan $c = c_1 c_2$, jolloin

$$s_1(n) \leq c_1 s_2(c_1 n) \leq c_1 c_2 s_3(c_1 c_2 n) = c s_3(cn)$$

kaikilla $n \geq 1$ eli $\preceq$ on transitiivinen. Kohta (ii) seuraa suoraan kohdasta (i) ja relaation $\sim$ määritelmästä.

Oletetaan, että f, f', g, g' toteuttavat kohdan (iii) alkuoletukset. Tällöin on voimassa $f' \preceq f$, $f \preceq g$ ja $g \preceq g'$. Relaation $\preceq$ transitiivisuudesta seuraa, että $f' \preceq g'$. □

Olkoon $s : \mathbb{N} \to [0, \infty)$ kasvufunktio. Merkitään sen $\sim$-ekvivalenssiluokkaa merkinnällä $[s]$.

Jos s_X ja s_Y ovat kasvufunktioita ja $s_X \preceq s_Y$, kirjoitetaan $[s_X] \preceq [s_Y]$. Tällöin $\preceq$ merkitsee *osittaista järjestystä* kasvufunktioiden ekvivalenssiluokkien joukolla.

Esimerkki 2. Olkoon $s : \mathbb{N} \to [0, \infty)$ kasvufunktio. Oletetaan, että s on polynomi, jonka aste on d. Tällöin $s \sim n^d$.

Esimerkki 3. Olkoon $a, b \in (1, \infty)$. Oletetaan, että $a \leq b$. Tällöin $a^n \leq b^n$ kaikilla $n \geq 1$, joten $a^n \preceq b^n$. Toisaalta, jos asetetaan $c = [\log_a b] + 1 > 1$ (missä $[\cdot]$ tarkoittaa logaritmin kokonaislukuosaa), niin saadaan

$$b^n = (a^{\log_a b})^n = a^{(\log_a b)n} \leq a^{cn} \leq c a^{cn},$$

kaikilla $n \geq 1$. Eli $a^n \sim b^n$. Erityisesti $a^n \sim e^n$ kaikilla $a \in (1, \infty)$.

Lause 11. *Kaksi saman ryhmän kasvufunktiota ovat ekvivalentit.*

Todistus. Olkoon G ryhmä ja $s = s_X^G$ ja $t = s_Y^G$ sen kasvufunktiot. Ilmaistaan jokainen joukon Y alkio sanana joukossa X ja jokainen joukon X alkio sanana joukossa Y. Olkoon näin saatujen sanojen maksimipituus c. Jokaiselle $x \in G$ pätee $l_X(x) \leq c l_Y(x)$ ja tästä seuraa, että $t(n) \leq s(cn)$ kaikilla n. Vastaavasti voidaan johtaa $s(n) \leq t(cn)$, joten määritelmän nojalla kasvufunktiot s ja t ovat ekvivalentit. □

Edellinen lause seuraisi myös suoraan lauseen 9 kohdasta (iii) sekä epäyhtälöstä (3). Näistä seuraa myös, että $s_X(n) \preceq e^n$.

Olkoon G äärellisen ja symmetrisen joukon X generoima ryhmä. Kasvufunktioiden ekvivalenssiluokkia $[s_X]$ kutsutaan ryhmän G *kasvun tyypiksi* ja sitä merkitään $s(G)$.

Lause 12. *Olkoon* $s : \mathbb{N} \to [0, \infty)$ *kasvufunktio, jolle* $s(0) > 0$. *Tällöin* $s \sim 1$ *jos ja vain jos* s *on rajoitettu.*

Todistus. Oletetaan, että s on rajoitettu. Merkitään vakiofunktiota $g(n) = 1$. Tällöin on olemassa sellainen kokonaisluku $c \geq 1$, jolle $s(n) \leq c$ kaikilla $n \in \mathbb{N}$. Tästä seuraa, että $s(n) \leq cg(n) \leq cg(cn)$ kaikilla $n \in \mathbb{N}$ eli $s(n) \preceq 1$. Asettamalla $c = \left[\frac{1}{s(0)}\right] + 1$, saadaan $g(n) = 1 \leq cs(0) \leq cs(n) \leq cs(cn)$ kaikilla $n \in \mathbb{N}$ eli $1 \preceq s(n)$.

Oletetaan, että $s \sim 1$. Tällöin $s \preceq 1$, joten on olemassa sellainen kokonaisluku $c \geq 1$, että $s(n) \leq c$ kaikilla $n \in \mathbb{N}$, joten s on rajoitettu. □

Seuraus 2. *Olkoon G äärellisen joukon generoima ryhmä. Tällöin $s(G) \sim 1$ jos ja vain jos G on äärellinen. Tästä seuraa, että kaikilla äärellisillä ryhmillä on sama kasvun tyyppi.*

Todistus. Olkoon X ryhmän G generoiva äärellinen ja symmetrinen joukko. Oletetaan, että $s(G) \sim s_X(n) \sim 1$. Lauseen 12 mukaan s_X on rajoitettu eli on olemassa sellainen kokonaisluku $c \geq 1$, että $s_X(n) \leq c$ kaikilla $n \in \mathbb{N}$. Tästä seuraa, että $|G| \leq c$, joten G on äärellinen. Vastaavasti, jos G on äärellinen, niin $s(G) = |B_X(n)| \leq |G|$ kaikilla $n \in \mathbb{N}$. Lauseen 12 mukaan $s(G) \sim s_X(n) \sim 1$. □

Lause 13. *Olkoon G ääretön äärellisen joukon generoima ryhmä. Tällöin $n \preceq s(G)$.*

Todistus. Olkoon X äärellinen ja symmetrinen joukko, joka generoi ryhmän G. Ryhmässä G on voimassa

$$\{1_G\} = B_X(0) \subseteq B_X(1) \subseteq B_X(2) \subseteq \cdots \subseteq B_X(n) \subseteq B_X(n+1) \subseteq \cdots . \qquad (4)$$

Osoitetaan, että jos $B_X(n) = B_X(n+1)$ jollakin $n \in \mathbb{N}$, niin $B_X(n) = B_X(m)$ kaikilla $m \geq n$. Todistetaan väite induktiolla. Oletetaan, että $B_X(n) = B_X(m)$ jollakin $m \geq n+1$. Kaikilla $g \in B_X(n+1)$ on olemassa $g' \in B_X(m)$ ja $x \in X$ siten, että $g = g'x$. Induktio-oletuksen nojalla $g' \in B_X(m-1)$, joten $g = g'x \in B_X(m-1)X \subseteq B_X(m)$. Koska $B_X(m) \subseteq B_X(m+1)$, niin $B_X(m+1) = B_X(m) = B_X(n)$.

Tästä seuraa, että jos $B_X(n) = B_X(n+1)$ jollakin $n \in \mathbb{N}$, niin $G = B_X(n)$. Koska G on ääretön, niin kaikki sisältymiset yhtälössä (4) ovat aitoja. Eli kaikilla $n \in \mathbb{N}$ $n \leq |B_X(n)| = s_X(n)$. Tällöin $n \preceq s_X(n)$ ja näin ollen $n \preceq s(G)$. □

4.2 Kasvun tyypit

Kasvufunktioiden ekvivalenssiluokkia voidaan lajitella sen mukaan, miten nopeasti ryhmän koko suhteessa sen generoivaan joukkoon. Vaikka kasvufunktio riippuu ryhmän generoivasta joukosta, kuitenkin kasvun tyyppi on ryhmälle sama riippumatta sen generoivasta joukosta. Määritellään seuraavaksi kolme kasvun tyyppiä: polynominen, eksponentiaalinen ja välimuotoinen kasvu.

Olkoon G äärellisen joukon generoima ryhmä.

Määritelmä 19. Ryhmällä G on *polynomista kasvua*, jos on olemassa luku $d \geq 0$ siten, että $s(G) \preceq n^d$. Kun valitaan infimum yli tällaisten lukujen d, niin kyseistä lukua kutsutaan kasvun *asteeksi* ja sitä voidaan merkitä $d(G)$. Jos $d = 1$, sanotaan, että ryhmän G kasvu on *lineaarista*.

Määritelmä 20. Ryhmällä G on *eksponentiaalista kasvua*, jos $s(G) \sim e^n$ ja *subeksponentiaalista kasvua*, jos $s(G) \not\sim e^n$.

Seuraavassa alaluvussa osoitetaan, että kaikilla ryhmillä, joilla on polynomista kasvua, on myös subeksponentiaalista kasvua.

Määritelmä 21. Ryhmällä G on *välimuotoista kasvua*, jos sen kasvu ei ole eksponentiaalista eikä polynomista.

Lause 14. *Jokaisella äärellisen joukon generoimalla ryhmällä, jolla on polynomista kasvua, on myös subeksponentiaalista kasvua.*

Todistus. Osoitetaan ensin, että jos $n^d \preceq e^n$ jollakin kokonaisluvulla $d \geq 0$, niin $n^d \not\sim e^n$. Koska $\lim_{n\to\infty} \frac{n^d}{e^n} = 0$, niin lukujono $\left(\frac{n^d}{e^n}\right)_{n\geq 1}$ on rajoitettu. Tällöin on olemassa sellainen $c > 1$, että $\frac{n^d}{e^d} < c$ kaikilla $n \geq 1$. Tästä seuraa, että

$$n^d \leq ce^n \leq ce^{cn}$$

kaikilla $n \geq 1$, joten $n^d \preceq e^n$.

Oletetaan, että $e^n \preceq n^d$, jolloin on olemassa sellainen $c > 0$, että $e^n \leq c(cn)^d$ kaikilla $n \geq 1$. Tällöin $\frac{e^n}{n^d} \leq c^{d+1}$ kaikilla $n \geq 1$, mikä on ristiriita, koska $\lim_{n\to\infty} \frac{e^n}{n^d} = \infty$. Eli $e^n \not\preceq n^d$, joten $n^d \not\sim e^n$.

Olkoon G äärellisen joukon generoima ryhmä. Edellisestä seuraa relaation $\preceq$ transitiivisuuden ja relaation $\sim$ symmetrisyyden nojalla, että jos $s(G) \preceq n^d$, niin $s(G) \not\sim e^n$. Eli ryhmällä G on subeksponentiaalista kasvua. □

Lause 15. *Jos $[G : H]$ on äärellinen, niin ryhmilllä G ja H on ekvivalentit kasvufunktiot ja näin ollen ovat myös samaa kasvun tyyppiä.*

Todistus. Olkoon r maksimaalinen pituus alkioille ryhmän H sivuluokkien edustajistossa X. Tällainen on olemassa, sillä ryhmän H indeksi ryhmässä G on äärellinen. Olkoon $xu \in G$ jokin alkio, jonka pituus on korkeintaan n ja jossa $x \in H$ ja $u \in X$. Tällöin $k := l(x) \leq n + r$. Alkio x voidaan kirjoittaa muodossa $x = y_1 \cdots y_k$, jossa y_j on ryhmän H generaattori tai generaattorin käänteisalkio. Nyt

$$x = y_1 u_1^{-1} \cdot u_1 y_2 u_2^{-1} \cdot u_2 y_3 \cdots y_k u_k^{-1}$$

jollakin $u_j \in S$. Tämä osoittaa, että suhteessa generaattoreihin, jotka ovat muotoa $u_i^{-1} y_j u_m \in H$, saadaan $l_H(x) \leq k$. Näin ollen

$$s_G(n) \leq |G : H| s_H(n + r) \leq |G : H| s_H((r + 1)n).$$

□

Esimerkki 4.

(a) Olkoon $G = \mathbb{Z}$. Valitaan $X = \{-1, 1\}$ sen generoivaksi joukoksi, jolloin pallo, jonka keskipiste on alkio $g \in G$ ja säde on r, on väli $[g-r, g+r] = \{n \in \mathbb{Z} \mid g - r \leq n \leq g+r\}$. Saadaan $s_X(n) = 2n+1$, josta seuraa, että $s(\mathbb{Z}) \sim s_X(n) \sim n$. Ryhmällä $\mathbb{Z}$ on siis polynomista kasvua.

(b) Olkoon $G = \mathbb{Z}^2$ ja $X = \{(-1,0),(0,-1),(1,0),(0,1)\}$. Tällöin pallo, jonka keskipiste on $g = (n,m) \in G$ ja säde r, on nelikulmio, jonka kärkipisteet ovat $(n,m+r)$,$(n+r,m)$, $(n,m-r)$ ja $(n-r,m)$. Kasvufunktioksi saadaan $s_X(n) = 1 + \sum_{k=1}^{n} 4k = 2n^2 + 2n + 1$, josta seuraa, että $s(G) \sim s_X(n) \sim n^2$. Ryhmällä $\mathbb{Z}^2$ on siis polynomista kasvua.

(c) Olkoot $G = \mathbb{Z}^2$ ja

$$Y = \{(1,0),(-1,0),(0,1),(0,-1),(1,1),(-1,1),(1,-1),(-1,-1)\}$$

sen generoiva joukko. Nyt pallo, jonka keskipiste on $g = (n,m) \in G$ ja säde r, on neliö $[n-r,n+r]\times[m-r,m+r]$. Kasvufunktio on tällöin $s_Y^{\mathbb{Z}^2}(n) = 4n^2+4n+1 = (2n+1)^2 = (s_Y^{\mathbb{Z}}(n))^2$. Saadaan $s(\mathbb{Z}^2) \sim s_Y(n) \sim n^2$, kuten edellisessäkin kohdassa ja voidaan uudelleen todeta ryhmällä $\mathbb{Z}^2$ olevan polynomista kasvua.

4.3 Kasvunopeus

Tässä luvussa määritellään ryhmän kasvunopeus suhteessa sen generoivaan joukkoon, sekä yhdistetään se kasvutyyppien käsitteisiin.

Lemma 1. *Olkoon $a : \mathbb{N} \to \mathbb{R}$ submultiplikatiivinen funktio eli $a(n+m) \leq a(n)a(m)$ kaikilla $n,m \geq 1$. Tällöin raja-arvo*

$$\lim_{n\to\infty} \sqrt[n]{a(n)}$$

on olemassa ja sen arvo on $\inf_{n\geq 1} \sqrt[n]{a(n)}$.

Ennen kuin todistamme kyseisen lemman, johdetaan ensin seuraava aputulos, jota kutsutaan Feketen lemmaksi:

Lemma 2 (Feketen lemma)**.** *Oletetaan, että funktiolle $a(n)$ pätee $a(n+m) \leq a(n)+a(m)$ kaikilla $n,m \in \mathbb{N}$ eli $a(n)$ on subadditiivinen. Tällöin*

$$\lim_{n\to\infty} \frac{a(n)}{n} = \inf_{n\in\mathbb{N}} \frac{a(n)}{n}.$$

Todistus. Riittää osoittaa, että pätee $\limsup_{n\to\infty} \frac{a(n)}{n} \leq \frac{a(m)}{m}$ kaikilla $m \in \mathbb{N}$. Olkoon $n,m \in \mathbb{N}$. Merkitään $n = b_n m + r_n$, jossa $0 \leq r \leq m-1$. Subadditiivisuudesta seuraa, että

$$\frac{a(n)}{n} = \frac{a(b_n m + r_n)}{b_n m + r_n} \leq \frac{a(m)}{m} + \frac{a(r_n)}{b_n m}.$$

$\lim_{n\to\infty} \frac{a(r_n)}{b_n m} = 0$, sillä $0 \leq a(r_n) \leq a(m-1)$ on rajoitettu ja $\lim_{n\to\infty} b_n = \infty$. Näin ollen saadaan haluttu tulos:

$$\limsup_{n\to\infty} \frac{a(n)}{n} \leq \frac{a(m)}{m}.$$

□

Lemman 1 todistus: Olkoot $a(n)$ submultiplikatiivinen funktio ja $b(n)$ subadditiivinen funktio, jolle $b(n) := \ln a(n)$ kaikilla $n \in \mathbb{N}$. Nyt

$$\frac{b(n)}{n} = \frac{\ln a(n)}{n} = \ln\left(\sqrt[n]{a(n)}\right)$$

ja koska logaritmifunktio on jatkuva ja kasvava, niin lemman 2 nojalla

$$\lim_{n\to\infty} \ln\left(\sqrt[n]{a(n)}\right) = \inf_{n\in\mathbb{N}} \ln\left(\sqrt[n]{a(n)}\right).$$

Erityisesti raja-arvo $\lim_{n\to\infty} \sqrt[n]{a(n)}$ on olemassa. □

Seuraus 3. *Olkoon G äärellisen joukon generoima ryhmä ja olkoon X äärellinen ja symmetrinen ryhmän G generoiva aliryhmä. Tällöin raja-arvo*

$$\omega_X = \lim_{n\to\infty} \sqrt[n]{s(n)}$$

on olemassa ja $\omega_X \in [0, \infty)$.

Määritelmä 22. Lukua $\omega_X = \omega_X^G$ kutsutaan ryhmän G *kasvunopeudeksi* suhteessa generoivaan joukkoon X.

Lause 16. *Olkoon G äärellisen joukon generoima ryhmä ja olkoon X äärellinen ja symmetrinen ryhmän G generoiva aliryhmä. Ryhmällä G on eksponentiaalista kasvua jos ja vain jos $\omega_X > 1$.*

Todistus. Oletetaan, että $s(G) \sim e^n$. Koska $e^n \preceq s_X$, niin on olemassa sellainen kokonaisluku $c \geq 1$, että $e^n \leq cs_x(cn)$ kaikilla $n \in \mathbb{N}$. Nyt

$$1 < \sqrt[c]{e} = \lim_{n\to\infty} \sqrt[cn]{e^n} \leq \lim_{n\to\infty} \sqrt[cn]{cs_X(cn)} = \left(\lim_{n\to\infty} \sqrt[cn]{c}\right) \cdot \left(\lim_{n\to\infty} \sqrt[cn]{s_X(cn)}\right) = \omega_X.$$

Oletetaan nyt, että $\omega_X > 1$. Lemmasta 1 seuraa, että $\sqrt[n]{s_X(n)} \geq \omega_X$ eli

$$\omega_X^n \leq s_X(n).$$

Tästä saadaan, että $e^n \sim \omega_X^n \preceq s_X(n)$. Lauseesta 11 seuraa, että $s_X(n) \preceq e^n$ ja näin ollen $s(G) \sim s_X \sim e^n$. □

Seuraus 4. *Olkoon G äärellisen joukon generoima ryhmä ja olkoon X äärellinen ja symmetrinen ryhmän G generoiva aliryhmä. Ryhmällä G on subeksponentiaalista kasvua jos ja vain jos $\omega_X = 1$.*

Koska $\sim$ on ekvivalenssirelaatio, niin seurauksena lauseen 16 kanssa saadaan suoraan seuraava tulos:

Seuraus 5. *Olkoon G äärellisen joukon generoima ryhmä. Olkoot X ja X' kaksi äärellistä ja syymetristä ryhmän G generoivaa joukkoa. Nyt $\omega_X = 1$ (tai $\omega_X > 1$) jos ja vain jos $\omega_{X'} = 1$ (tai $\omega'_X > 1$).*

5 Kasvun ominaisuuksia

Seuraavaksi tarkastellaan, millaisia kasvun ominaisuuksia on erilaisilla ryhmillä. Luku perustuu lähteisiin [1] ja [2].

Lause 17. *Olkoon G äärellisen joukon generoima ryhmä ja $H \leq G$ äärellisen joukon generoima aliryhmä. Tällöin $s(H) \preceq s(G)$.*

Todistus. Olkoon X_G äärellinen, symmetrinen joukko, joka generoi ryhmän G ja X_H äärellinen, symmetrinen joukko, joka generoi ryhmän H. Nyt $X = X_G \cup X_H$ on äärellinen ja symmetrinen ryhmän G osajoukko. Koska $X_H \subseteq X$, niin $B^H_{X_H}(n) \subseteq B^G_X(n)$. Tästä seuraa, että kaikilla $n \in \mathbb{N}$ pätee $s^H_{X_H}(n) \leq s^G_X(n)$. Joten $s(H) \preceq s(G)$. □

Seuraus 6. *Jokaisella äärellisen joukon generoimalla ryhmällä, joka sisältää äärellisen joukon generoiman aliryhmän, jolla on eksponentiaalista kasvua, on eksponentiaalista kasvua.*

Seuraava lause osoittaa, että ryhmällä G ja sen aliryhmillä, joilla on äärellinen indeksi ryhmässä G, ovat samaa kasvun tyyppiä.

Lause 18. *Olkoon G äärellisen joukon generoima ryhmä ja $H \leq G$ sen aliryhmä, jolle $[G : H] < \infty$. Tällöin H on äärellisen joukon generoima ja $s(G) = s(H)$.*

Todistus. Koska $[G : H] < \infty$, niin lauseesta 1 seuraa, että H on äärellisen joukon generoima. Lauseesta 17 seuraa, että $s(H) \preceq s(G)$.

Olkoon X äärellinen ja symmetrinen ryhmän G generoiva joukko. Tarkastellaan äärellistä symmetristä joukkoa $X' = RXR^{-1} \cap H$. Lauseen 1 nojalla joukko X' generoi ryhmän H. Olkoon $g \in B^G_X(n)$ ja merkitään $g = x_1 x_2 \cdots x_n$, $x_i \in X$. Kuten lauseen 1 todistuksessa, voidaan löytää sellaiset $r_0 = 1_G, r_1, r_2, \ldots, r_n \in R$, että

$$\begin{aligned} g &= x_1 x_2 \cdots x_n \\ &= (1_G x_1 r_1^{-1})(r_1 x_2 r_2^{-1}) \cdots (r_{n-2} x_{n-1} r_{n-1}^{-1})(r_{n-1} x_n r_n^{-1}) r_n \\ &= h_1 h_2 \cdots h_{n-1} h_n r_n, \end{aligned}$$

jossa $h_i = r_{i-1} x_i r_i^{-1}$. Koska $B^G_X(n) \subseteq B^H_{X'}(n)R$, niin

$$s^G_X(n) = |B^G_X(n)| \leq |B^H_{X'}(n)||R| = [G : H] s^H_{X'}(n) \leq [G : H] s^H_{X'}([G : H]n).$$

Eli $s(G) \preceq s(H)$ ja saadaan $s(G) = s(H)$. □

Edellisestä lauseesta seuraa suoraan tulos:

Seuraus 7. *Jos G_1 ja G_2 ovat yhteismitallisia ryhmiä ja G_2 on äärellisen joukon generoima, niin G_1 on myös äärellisen joukon generoima ja $s(G_1) = s(G_2)$.*

Lemma 3. *Olkoon $s_1, s_2, s_1', s_2' : \mathbb{N} \to [0, \infty)$ kasvufunktioita. Oletetaan, että $s_1 \preceq s_1'$ ja $s_2 \preceq s_2'$. Tällöin niiden tulot $s_1 s_2, s_1' s_2' : \mathbb{N} \to [0, \infty)$ ovat kasvavia funktioita ja $s_1 s_2 \preceq s_1' s_2'$.*

Todistus. Koska kasvavien funktioiden tulo on kasvava, on selvää, että $s_1 s_2$ ja $s_1' s_2'$ ovat myös kasvufunktioita. Olkoot c_1 ja c_2 sellaisia positiivisia kokonaislukuja, että $s_1(n) \leq c_1 s_1'(c_1 n)$ ja $s_2(n) \leq c_2 s_2(c_2 n)$ kaikilla $n \in \mathbb{N}$. Merkitään $c = c_1 c_2$. Nyt

$$\begin{aligned}(s_1 s_2)(n) &= s_1(n) s_2(n) \\ &\leq c_1 s_1'(c_1 n) c_2 s_2'(c_2 n) \\ &\leq c_1 c_2 s_1'(c_1 c_2 n) s_2'(c_1 c_2 n) \\ &= c s_1'(cn) s_2'(cn) \\ &= c(s_1' s_2')(cn)\end{aligned}$$

kaikilla $n \in \mathbb{N}$. □

Lause 19. *Olkoot G_1 ja G_2 kaksi äärellisen joukon generoimaa ryhmää. Tällöin niiden suora tulo $G_1 \times G_2$ on myös äärellisen joukon generoima ja $s(G_1 \times G_2) = s(G_1)s(G_2)$.*

Todistus. Olkoot X_1 ja X_2 äärelliset ja symmetriset joukot, jotka generoivat ryhmät G_1 ja G_2. Tällöin ryhmän $G_1 \times G_2$ generoiva äärellinen ja symmetrinen joukko on

$$X = (X_1 \times \{1_{G_2}\}) \cup (\{1_{G_1}\} \times X_2).$$

Olkoon $(g_1, g_2) \in B_X^{G_1 \times G_2}(n)$. On olemassa sellaiset alkiot $y_1, \ldots, y_k \in X_1$ ja $x_1, \ldots, x_m \in X_2$, että $k + m = n$ ja

$$\begin{aligned}(g_1 g_2) &= (y_1, 1_{G_2})(y_2, 1_{G_2}) \cdots (y_k, 1_{G_2}) \cdot (1_{G_1}, x_1)(1_{G_1}, x_2) \cdots (1_{G_1}, x_m) \\ &= (y_1 \cdots y_k, x_1 \cdots x_m).\end{aligned}$$

Tästä seuraa, että $B_X^{G_1 \times G_2}(n) \subseteq B_{X_1}^{G_1}(n) \times B_{X_2}^{G_2}(n)$ ja $s_X^{G_1 \times G_2}(n) \leq s_{X_1}^{G_1}(n) s_{X_2}^{G_2}(n)$. Näin ollen $s(G_1 \times G_2) \preceq s(G_1)s(G_2)$.

Jos $g_1 \in B_{X_1}^{G_1}(n)$ ja $g_2 \in B_{X_2}^{G_2}(n)$, niin $(g_1, g_2) \in B_X^{G_1 \times G_2}(2n)$. Tästä seuraa, että $s_{X_1}^{G_1}(n) s_{X_2}^{G_2}(n) \leq s_X^{G_1 \times G_2}(2n) \leq 2 s_X^{G_1 \times G_2}(2n)$, joten $s(G_1)s(G_2) \preceq s(G_1 \times G_2)$. □

Lause 20. *Olkoot G ryhmä, $H \leq G$ ja $N \trianglelefteq G$. Jos ryhmällä G on polynomista kasvua, $|G : H|$ on ääretön ja H on äärellisen joukon generoima, niin $d(H) \leq d(G) - 1$. Jos taas N on ääretön ja äärellisen joukon generoima, niin $d(G/N) \leq d(G) - 1$.*

Todistus. Olkoon ryhmällä G polynomista kasvua. Oletetaan, että $|G : H| = \infty$. Olkoon $X = \{x_1, \ldots, x_m\}$ ryhmän G generoivien alkioiden joukko. Oletetaan lisäksi, että joukko X sisältää myös ryhmän H generoivat alkiot. Olkoon $Hu_1, \ldots, Hu_n$ ryhmän H erillisiä sivuluokkia, jossa alkiot u_j kuuluvat ryhmän H sivuluokkien edustajistoon. Tällöin joukko $K := Hu_1 \cup \cdots \cup Hu_n$ ei ole suljettu oikealta kertomisen suhteen kerrottaessa ryhmän G generaattoreilla tai niiden käänteisalkioilla. Muutoin olisi $K = G$. Täten yksi alkioista $u_i x_j^{\pm}$ edustaa uutta sivuluokkaa. Aloittaen alkiosta $u_1 = x_1$, niin jokaiselle n voidaan löytää n kappaletta erillisiä ryhmän H sivuluokkia, joita edustaa alkiot, joiden pituus on enintään n. Voidaan siis olettaa, että $l(u_i) \leq i$. Jos alkiot, joiden pituus on enintään n ryhmässä H ovat $z_1, \ldots, z_k$, niin muotoa

$z_i u_j$ olevien alkioiden joukossa ei esiinny samaa alkiota kahdesti. Tällöin $s_G(2n) \geq ns_H(n)$, joten koska ryhmän G kasvu on polynomista, $d(G) \geq d(H) + 1$.

Olkoon N ääretön, äärellisen joukon generoima ryhmän G normaali aliryhmä. Olkoon X äärellinen joukko ryhmän G generoivia alkioita, joka sisältää lisäksi ryhmän N generoivien alkioiden joukon Y. Tällöin

$$s_{G,X}(2n) \geq s_{G/N,XN/N}(n) s_{N,Y}(n) \geq n s_{G/N}(n),$$

mistä seuraa $d(G) \geq d(G/N) + 1$. □

6 Nilpotenttien ryhmien kasvu

Tässä kappaleessa osoitetaan, että jokaisella äärellisen joukon generoimalla nilpotnetilla ryhmällä on polynomista kasvua [1].

Lemma 4. *Olkoon G ryhmä. Olkoon H ja K kaksi normaalia ryhmän G aliryhmää. Oletetaan, että $S \subseteq H$ ja $T \subseteq K$ generoivat ryhmät H ja K. Tällöin $[H, K]$ on normaali sulkeuma joukosta $\{[s, t] : s \in S, t \in T\}$ ryhmässä G.*

Todistus. Merkitään, että N on joukon $\{[s, t] : s \in S, t \in T\}$ normaalia sulkeumaa ryhmässä G. Koska $\{[s, t] : s \in S, t \in T\} \subset [H, K]$ ja $[H, K]$ on normaali aliryhmä, saadaan

$$N \subset [H, K]. \tag{5}$$

Olkoon $\pi : G \to G/N$ homomorfismi. Kaikilla $s \in S$ ja $t \in T$ saadaan

$$[\pi(s), \pi(t)] = \pi([s, t]) = 1_{G/N},$$

eli $\pi(s)$ ja $\pi(t)$ kommutoivat. Tästä seuraa, että kaikki alkiot ryhmästä $\pi(H)$ kommutoi kaikkien ryhmän $\pi(K)$ alkioiden kanssa, sillä S generoi ryhmän H ja T generoi ryhmän K. Toisin sanoen $\pi([h, k]) = [\pi(h), \pi(k)] = 1_{G/N}$ kaikilla $h \in H$ ja $k \in K$. Eli $[h, k] \in N$ kaikilla $h \in H$ ja $k \in K$ ja näin ollen $[H, K] \subset N$. Yhdessä kohdan (5) kanssa saadaan $[H, K] = N$. □

Olkoon G ryhmä. Sen alempi keskussarja on jono $(C^i(G))_{i \geq 0}$ normaaleja G:n aliryhmiä, joille pätee $C^0(G) = G$ ja $C^{i+1}(G) = [C^i(G), G]$ kaikilla $i \geq 0$. Alkioille $g_1, g_2, \ldots, g_i \in G$, $i \geq 3$ asetetaan induktiivisesti

$$[g_1, g_2, \ldots, g_i] = [[g_1, g_2, \ldots, g_{i-1}], g_i] \in C^{i-1}(G)$$

Jos $S \subset G$ ja $i \geq 2$, merkitään joukkoa, joka koostuu alkioista

$$[s_1, s_2, \ldots, s_i],\ s_1, s_2, \ldots, s_i \in S$$

notaatiolla $S_G^{(i)}$. Tämän joukon alkioita kutsutaan S-kommutaattoreiksi, joiden paino on i. Nyt siis $S_G^{(i)} \subset C^{i-1}(G)$.

Lemma 5. *Olkoon G ryhmä. Olkoon $S_G \subset G$ ryhmän G generoiva joukko. Tällöin aliryhmä $C^i(G)$ on joukon $S_G^{(i+1)}$ normaali sulkeuma ryhmässä G kaikilla $i \geq 1$.*

Todistus. Todistetaan väite induktiolla. Lemmasta 4 seuraa asettamalla $H = K = G$ ja $S = T = S_G$, että $C^1(G) = [G, G]$ on joukon $S_G^{(2)} = \{[s_1, s_2] : s_1, s_2 \in S_G\}$ normaali sulkeuma ryhmässä G. Eli väite pätee, kun $i = 1$.

Oletetaan, että $C^{i-1}(G)$ on joukon $S_G^{(i)}$ normaali sulkeuma ryhmässä G. Merkitään, että joukon $S_G^{(i+1)}$ normaali sulkeuma ryhmässä G on N. Koska $S_G^{(i+1)} \subseteq C^i(G)$ ja $C^i(G)$ on normaali aliryhmä, voidaan päätellä, että

$$N \subseteq C^i(G). \tag{6}$$

Merkitään tekijäkuvausta $\pi : G \to G/N$. Olkoon $w \in S_G^{(i)}$ ja $s \in S_G$. Tällöin $[w, s] \in S_G^{(i+1)}$ ja näin ollen $[w, s] \in N$. Tästä seuraa, että $[\pi(w), \pi(s)] = \pi([w, s]) = 1_{G/N}$, sillä $\pi(w)$ ja $\pi(s)$ kommutoivat. Koska S_G generoi ryhmän G, niin $\pi(S_G)$ generoi ryhmän G/N ja $\pi(w) \in Z(G/N)$. Tästä seuraa, että $\pi(hwh^{-1}) = \pi(h)\pi(w)\pi(h)^{-1} = \pi(w)$ kaikilla $h \in G$, joten $\pi([hwh^{-1}, s]) = [\pi(hwh^{-1}), \pi(s)] = [\pi(w), \pi(s)] = 1_{G/N}$. Joten

$$[hwh^{-1}, s] \in N. \tag{7}$$

Induktio-oletuksen nojalla jokainen ryhmän $C^{i-1}(G)$ alkio voidaan esittää muodossa $(h_1 w_1 h_1^{-1})(h_2 w_2 h_2^{-1}) \cdots (h_m w_m h_m^{-1})$, jossa $w_k \in S_G^{(i)}$ ja $h_k \in G$ kaikilla $k = 1, 2, \ldots, m$, $m \in \mathbb{N}$. Lemmasta 4 saadaan valitsemalla $H = C^{i-1}(G)$, $K = G$, $S = \{hwh^{-1} : w \in S_G^{(i)}, h \in G\}$ ja $T = S_G$, että $C^i(G) = [C^{i-1}(G), G]$ on joukon $\{[hwh^{-1}, s] : w \in S_G^{(i)}, h \in G, s \in S_G\}$ normaali sulkeuma ryhmässä G. Eli kohdasta (7) seuraa, että

$$C^i(G) \subseteq N.$$

Joten yhdessä kohdan (6) kanssa saadaan, että $C^i(G) = N$. □

Lemma 6. *Olkoon G äärellisen joukon generoima nilpotentti ryhmä, joka on nilpotenssiastetta $q \geq 1$. Tällöin aliryhmät $C^i(G)$, $i = 1, 2, \ldots, q-1$ ovat äärellisen joukon generoimia.*

Todistus. Olkoon S_G ryhmän G generoiva äärellinen joukko. Näytetään ensin, että tekijäryhmät $C^i(G)/C^{i+1}(G)$ ovat äärellisen joukon generoimia kaikilla $i = 1, 2, \ldots, q-1$. Lemmasta 5 seuraa, että $C^i(G)$ on joukon $S_G^{(i+1)}$ normaali sulkeuma ryhmässä G. Olkoon $\pi : G \to G/C^{i+1}(G)$ homomorfismi. Tällöin $C^i(G)/C^{i+1}(G) = \pi(C^i(G))$ on joukon $\pi(S_G^{(i+1)})$ normaali sulkeuma ryhmässä $G/C^{i+1}(G)$. Koska $\pi(S_G^{(i+1)}) = (\pi(S_G))^{(i+1)} \subseteq Z(C^i(G)/C^{i+1}(G))$ niin $\pi(S_G^{(i+1)})$ generoi ryhmän $C^i(G)/C^{i+1}(G)$.

Osoitetaan väite käänteisellä induktiolla indeksistä $i = q - 1$ lähtien. Nyt tiedetään, että $C^{q-1}(G) \cong C^{q-1}(G)/\{1_G\} = C^{q-1}(G)/C^q(G)$ on äärellisen joukon generoima. Induktio-oletuksen mukaan aliryhmä $C^{i+1}(G)$ on äärellisen joukon generoima jollakin $i \leq q - 2$. Todistuksen ensimmäisestä osasta seuraa, että $C^i(G)/C^{i+1}(G)$ on myös äärellisen joukon generoima. Nyt lauseen 2 perusteella voidaan sanoa, että $C^i(G)$ on äärellisen joukon generoima. □

Nyt voidaan osoittaa tämän luvun päätulos:

Lause 21. *Olkoon G äärellisen joukon generoima nilpotentti ryhmä. Tällöin ryhmällä G on polynomista kasvua.*

Todistus. Olkoon ryhmä G äärellisen joukon generoima nilpotentti ryhmä, jonka nilpotenssiluokka on q. Osoitetaan väite induktiolla: kun $q = 0$, niin $G = \{1_G\}$, joten sillä on polynomista kasvua. Oletetaan, että $q \geq 1$ ja että kaikilla äärellisillä nilpotenteilla ryhmillä, joiden luokka on $\leq q-1$, on polynomista kasvua.

Aliryhmä $H = C^1(G)$ on nilpotentti ja sen nilpotenssiluokka on $\leq q-1$. Nyt $C^i(H) \subseteq C^{i+1}(G)$ kaikilla $i = 1, 2, \ldots, q-1$, joten $C^{q-1}(H) \subseteq C^q(G) = \{1_G\}$. Lemman 6 nojalla ryhmä H on äärellisen joukon generoima, joten ryhmällä H on polynomista kasvua. Olkoon $T \subseteq H$ äärellinen ja symmetrinen ryhmän H generoiva joukko. On siis olemassa sellaiset $c_1 > 0$ ja $p \geq 0$, että

$$s_T^H(n) \leq c_1(c_1 n)^p,$$

kaikilla $n \geq 1$.

Olkoon $X = \{x_1, x_2, \ldots, x_k\} \subseteq G$ äärellinen ja symmetrinen joukko, joka generoi ryhmän G. Olkoon $g \in G$. Oletetaan, että $m = l_X^G(g) \leq n$. Tällöin on olemassa sellaiset $1 \leq i_1, i_2, \ldots, i_m \leq k$ siten, että

$$g = x_{i_1} x_{i_2} \cdots x_{i_m}.$$

Koska $g_2 g_1 = g_1 g_2 [g_2^{-1}, g_1^{-1}]$ ja $[g_2^{-1}, g_1^{-1}] \in H$ kaikilla $g_1, g_2 \in H$, voidaan alkio g ilmaista nyt muodossa

$$g = x_{j_1} x_{j_2} \cdots x_{j_m} h,$$

jossa $1 \leq j_1 \leq j_2 \leq \cdots \leq j_m \leq k$ ja $h \in H$. Asetetaan

$$L = \max\{l_T^H(w) : w \in X^{(i)}, 2 \leq i \leq q\}$$

Kuten yllä todettiin, vaihtamalla kahden peräkkäisen generaattorin paikkaa keskenään, saadaan kommutaattori, jonka paino on kaksi. Jos näitä vaihdoksia tehdään niin kauan, että x_{j_1} (jossa $j_1 = i_{b_1} = \min\{i_b : b = 1, 2, \ldots, m\}$) on viimeinen alkio oikealta vasemmalle luettuna, tulee tehdä enintään n vaihdosta. Jos vastaavasti halutaan tehdä alkiolle x_{j_2} (jossa $j_2 = \min\{i_b : b = 1, 2, \ldots, m; b \neq b_1\}$), tarvitaan jälleen enintään n vaihdosta. Yhteensä on olemassa enintään $mn \leq n^2$ tällaista vaihdosta. Näin ollen saadaan korkeintaan n^2 kappaletta kommutaattoreita, joiden paino on kaksi. Jokaisella askeleella, kun siirretään generaattoria x_{j_l} vasemmalle, täytyy myös vaihtaa se kaikkien yksinkertaisten X-kommutaattorien kanssa, jotka esiintyivät ennen sitä. Joten saadaan korkeintaan n^3 kappaletta yksinkertaisia X-kommutaattoreita, joiden paino on kolme, n^4 kappaletta X-kommutaattoreita, joiden paino on neljä ja niin edelleen. Jatkamalla tällä tapaa, kaikki X-kommutaattorit, joiden paino on $q+1$ ovat ykkösalkioita 1_G, sillä G:n nilpotenssiluokka on q. Yksinkertaisten X-kommutaattorien kokonaislukumäärä, jotka saadaan tällä tavoin, on siis enintään $n^2 + n^3 + \cdots + n^q \leq qn^q$. Luvun L määritelmästä seuraa, että

$$l_T^H(h) \leq Lqn^q.$$

Toisaalt ryhmän G alkioiden lukumäärää, jotka ovat muotoa $x_{j_1}x_{j_2}\cdots x_{j_m}$, $1 \leq j_1 \leq j_2 \leq \cdots \leq j_m \leq k$, voidaan rajoittaa luvulla $c_2 n^k$, jossa $c_2 > 0$ on n:stä riippumaton vakio. Jokainen näistä ryhmän alkioista voidaankin kirjoittaa muodossa $x_1^{n_1}x_2^{n_2}\cdots x_k^{n_k}$, jossa $0 \leq n_i \leq n$ kaikilla $i = 1, 2, \ldots, k$.

Nyt

$$s_X^G(n) \leq c_2 n^k c_1 (Lqn^q)^r = Cn^\delta \leq C(Cn)^\delta$$

kaikilla $n \geq 1$, jossa $\delta = k + rq$ ja $C = c_1 c_2 (Lq)^r$. Nyt $C > 0$ on vakio ja riippumaton n:stä. Seuraa, että ryhmällä G on polynomista kasvua. □

7 Ratkeavien ryhmien kasvu

Tässä luvussa tutkitaan äärellisen joukon generoimia ratkeavia ryhmiä niiden kasvun näkökulmasta ja osoitetaan, että niiden kasvu on joko eksponentiaalista tai polynomista [1].

Lause 22. *Olkoon G äärellisen joukon generoima ryhmä, jolla on subekponentiaalista kasvua. Tällöin ryhmän G kommutaattorialiryhmä G' on äärellisen joukon generoima.*

Todistus. Koska G/G' on äärellisen joukon generoima Abelin ryhmä, se on äärellisen monen syklisen ryhmän tulo. Todistetaan ensin seuraava apulause:

Apulause 1. *Olkoon $N \triangleleft G$. Oletetaan, että tekijäryhmä G/N on ääretön syklinen ryhmä. Tällöin N on äärellisen joukon generoima.*

Todistus. Koska kaikki ryhmän G aliryhmät, joilla on äärellinen indeksi, ovat äärellisen joukon generoimia, voidaan olettaa, että tekijäryhmä G/N on ääretön ja syklinen. Olkoon $G/N = \langle xN \rangle$. Kirjoitetaan jokainen ryhmän G generaattoreista $\{x_1, \ldots, x_d\}$ muodossa $x_i = x^{e_i} y_i$, jossa $y_i \in N$. Nyt alkiot $\{x, y_1, \ldots, y_d\}$ generoivat ryhmän G. Tällöin ryhmä N sisältää generaattorien $y_1, \ldots, y_d$ normaalin sulkeuman K. Koska ryhmän G/K generoi ryhmän G generaattoreiden kuvat, eli sivuluokat xK, niin G/K ääretön ja syklinen. Ryhmä G/N on ääretön syklinen tekijäryhmä ja se on ryhmän G/K homomorfinen kuva, mikä on mahdollista vain, jos $K = N$.

Olkoon K_i ryhmän K aliryhmä, jonka generoi kaikki konjugaatit $x^{-n} y_i x^n$, jolloin $N \geq \langle K_1, \ldots, K_d \rangle$. Aliryhmä $\langle K_1, \ldots, K_d \rangle$ sisältää alkiot $y_1, \ldots, y_d$ ja on invariantti konjugoinnin suhteen kaikilla ryhmän G generaattoreilla, joten se on yhtäsuuri ryhmän N kanssa. Riittää siis todistaa, että jokainen K_i on äärellisen joukon genroima. Tarkastellaan tuloa $xy_i^{e_1}xy_i^{e_2}x\cdots y_i^{e_n}$, jossa $e_i \in \{0, 1\}$. Tätä muotoa olevia sanoja on olemassa 2^n kappaletta ja jokaisen pituus on korkeintaan $2n$. Subeksponentiaalisuudesta seuraa, että, jos n on tarpeeksi suuri, kaksi näistä sanoista ovat yhtäsuuret. Olkoon n pienin indeksi, jolloin edellinen tapahtuu eli joillain potensseilla f_i pätee

$$xy_i^{e_1}xy_i^{e_2}x\cdots y_i^{e_n} = xy_i^{f_1}xy_i^{f_2}x\cdots y_i^{f_n}. \tag{8}$$

Indeksin n minimaalisuuden nojalla $e_n \neq f_n$. Merkitään $y(k) = x^k y_i y^{-k}$, jolloin yhtälö (8) voidaan kirjoittaa muodossa

$$y(1)^{e_1} y(2)^{e_2} \cdots y(n)^{e_n} x^n = y(1)^{f_1} y(2)^{f_2} \cdots y(n)^{f_n} x^n.$$

Koska $e_n \neq f_n$, voidaan $y(n)$ kirjoittaa alkioiden $y(1), \ldots, y(n-1)$ tulona. Näin ollen $y(n+1) = xy(n)x^{-1}$ voidaan ilmaista alkioiden $y(2), \ldots, y(n)$ tulona

$$xy(k_1)y(k_2)\cdots y(k_p)x^{-1} = xy(k_1)x^{-1}xy(k_2)x^{-1}\cdots xy(k_p)x^{-1},$$

jossa jokainen $xy(k_i)x^{-1} = y(k_{k_i+1})$. Kun tähän sijoitetaan alkion $y(n)$ lauseke, nähdään, että $y(n+1)$ kuuluu myös aliryhmään $\langle y(1), \ldots, y(n-1)\rangle$. Induktion nojalla kaikki alkiot $y(n)$, $n > 0$, kuuluvat samaan aliryhmään. Kun korvataan x sen käänteisalkiolla, aliryhmä, jonka generoi alkiot $y(n)$, joissa $n < 0$, on myöskin äärellisen joukon generoima. Täten ryhmä K_i on äärellisen joukon generoima, mikä osoittaa väitteen. □

Tiedetään, että tekijäryhmä G/G' on muotoa $C_1 \times \cdots \times C_n$, jossa ryhmät C_i ovat syklisiä kaikilla i. Merkitään $G_i = \pi^{-1}(1 \times 1 \times \cdots \times C_i \times 1 \times \cdots \times 1)$. Silloin $G_i/(G' \cap G_i) = C_i$ on syklinen. Apulauseesta seuraa, että $G' \cap G_i$ on äärellisen joukon generoima. Tällöin $G' = \langle G_1 \cup \cdots \cup G_n \rangle$ on äärellisen joukon generoima.

□

Seuraus 8. *Äärellisen joukon generoima ratkeava ryhmä, jolla on subeksponentiaalista kasvua, on polysyklinen.*

Todistus. Olkoon G äärellisen joukon generoima ryhmä, jolla on subeksponentiaalista kasvua. Lauseen 22 mukaan kaikki ryhmän G kommutaattoriryhmät ovat äärellisen joukon generoimia, joten myöskin tekijäryhmät $G^{(i)}/G^{(i+1)}$ ovat äärellisen joukon generoimia. Koska nämä tekijäryhmät ovat polysyklisiä ja niistä vain äärellisen moni on epätriviaaleja, niin G on polysyklinen. □

Lause 23. *Olkoon G polysyklinen ryhmä, jolla on subekponentiaalista kasvua. Tällöin sillä on nilpotentti normaali aliryhmä N, jolla G/N on äärellinen.*

Todistus. Todistusta ei käydä läpi tässä tutkielmassa, sillä se vaatisi syvempää ymmärrystä lukuteoriasta. Se kuitenkin löytyy lähteestä [1] lauseesta 5.3. □

Yhdessä lauseen 21 kanssa, edellisestä seuraa tulos:

Seuraus 9. *Olkoon G äärellisen joukon generoima ratkeava ryhmä. Tällöin ryhmän G kasvu on joko eksponentiaalista tai polynomista.*

8 Grigorchukin ryhmä

Grigorchukin ryhmän ensimmäisen kerran esitteli Rostislav Grigorchuk vuonna 1980. Se oli samanaikaisesti myös ensimmäinen esimerkki äärellisen joukon generoimasta välimuotoisen kasvutyypin ryhmästä. Tässä luvussa konstruoidaan kyseinen ryhmä kahdella tavalla ja todistetaan siihen liittyviä ominaisuuksia. Luku on pääosin kirjoitettu käyttäen lähdettä [2].

8.1 Ryhmän konstruointi

Esitellään ensin se tapa, jolla Grigorchuk itse konstruoi ryhmän vuonna 1983 [1]. Grigorchukin ryhmän konstruoimiseen käytetään avoimen välin $(0,1)$ transformaatioita. Selvyyden vuoksi väliltä poistetaan kaikki pisteet, jotka ovat muotoa $1/2^n$. Olkoot E identiteettitransformaatio ja P transformaatio, joka vaihtaa keskenään välit $(0,1/2)$ ja $(1/2,1)$. Tällöin siis piste x kuvautuu joko pisteeksi $x+1/2$ tai $x-1/2$. Hajotetaan yksikköväli $(0,1)$ osaväleiksi $(1-\frac{1}{2^{n-1}}, 1-\frac{1}{2^n})$, jossa $n = 1,2,\ldots$. Olkoon ryhmä Γ neljän transformaation, a, b, c ja d, generoima. Generaattori a vastaa transformaatiota P sovellettuna koko välille. Muut kolme generaattoria suorittavat osaväleille $(1-\frac{1}{2^{n-1}}, 1-\frac{1}{2^n})$ joko tranformaation E tai P seuraavasti:

(*i*) b suorittaa kahdelle ensimmäiselle osavälille transformaation P ja kolmannelle osavälille transformaation E, minkä jälkeen sama toistetaan seuraaville osaväleille uudelleen eli PPE

(*ii*) c suorittaa samaan tapaan osaväleille transformaation PEP

(*iii*) d vastaa osavälien transformaatiota EPP.

Tästä seuraa $a^2 = b^2 = c^2 = d^2 = 1$ ja $bc = cb = d$, $cd = dc = b$, $db = bd = c$. Nämä ominaisuudet todistetaan tarkemmin toisen konstruointitavan yhteydessä.

Seuraavaksi käydään läpi vielä toinen tapa konstruoida Grigorchukin ryhmä, jonka merkintöjä käytetään tästä eteenpäin [2]. Olkoon $\Sigma = \{0,1\}$ aakkosto ja $\Sigma^* = \cup_{n\in\mathbb{N}}\Sigma^n$ kaikkien aakkoston Σ sanojen muodostama joukko. Merkitään tyhjää sanaa merkinnällä ϵ. Jokainen sana $w \in \Sigma^*$ voidaan kirjoittaa yksiselitteisesti muodossa $w = \sigma_1\sigma_2\cdots\sigma_n$, jossa $\sigma_i \in \Sigma$.

Olkoon $\mathrm{Sym}(\Sigma^*)$ joukon Σ^* symmetrinen ryhmä. Määritellään joukossa Σ^* osittainen järjestys $\preceq$: jos alkioille $u, v \in \Sigma^*$ on olemassa sellainen $w \in \Sigma^*$, että $uw = v$, niin $u \preceq v$. Määritellään nyt

$$\mathrm{Sym}(\Sigma^*, \preceq) = \{g \in \mathrm{Sym}(\Sigma^*) : g(u) \preceq g(v), \text{kaikilla } u, v \in \Sigma^*, \text{joilla } u \preceq v\}.$$

Tällöin $\mathrm{Sym}(\Sigma^*, \preceq) \leq \mathrm{Sym}(\Sigma^*)$. Sanan $w \in \Sigma^*$ pituus $l(w)$ on maksimi luvuista $n \in \mathbb{N}$, joille on olemassa sellaiset jonot toisistaan eroavia sanoja $(w_k)_{0\leq k\leq n}$ joukosta Σ^*, siten, että $\epsilon \preceq w_1 \preceq w_2 \preceq \cdots \preceq w_n = w$. Tästä seuraa, että jos$g \in \mathrm{Sym}(\Sigma^*, \preceq)$, niin $l(g(w)) = l(w)$ kaikille $w \in \Sigma^*$.

Olkoon $a, b, c, d \in \mathrm{Sym}(\Sigma^*)$. Määritellään nämä alkiot seuraavasti: tyhjälle sanalle

$$a(\epsilon) = b(\epsilon) = c(\epsilon) = d(\epsilon) = \epsilon.$$

Alkiolle a

$$a(0w) = 1w \text{ ja } (1w) = 0w$$

kaikilla $w \in \Sigma^*$. Määritellään alkiot $b(w)$, $c(w)$ ja $d(w)$ induktion avulla sanan pituudelle $l(w)$:

$$b(0w) = 0a(w),\ b(1w) = 1c(w)$$
$$c(0w) = 0a(w),\ c(1w) = 1d(w)$$
$$d(0w) = 0w,\ d(1w) = 1b(w)$$

kaikilla $w \in \Sigma^*$. Saadaan $a, b, c, d \in \mathrm{Sym}(\Sigma^*, \preceq)$.

Esimerkki 5. Olkoon $w = (00110) \in \Sigma^*$.

$$\begin{aligned} a(w) &= a(00110) = 10110, \\ b(w) &= b(00110) = 0a(0110) = 01110, \\ c(w) &= c(00110) = 0a(0110) = 01110, \\ d(w) &= d(00110) = 00110. \end{aligned}$$

Määritelmä 23. *Grigorchukin ryhmä* on symmetrisen ryhmän $\mathrm{Sym}(\Sigma^*)$ aliryhmä Γ, jonka generoi edellä määritetyt alkiot $a, b, c, d \in \Sigma^*$.

Koska $a, b, c, d \in \mathrm{Sym}(\Sigma^*, \preceq)$, niin $\Gamma \subset \mathrm{Sym}(\Sigma^*, \preceq)$.

Lause 24. *Seuraavat väitteet ovat voimassa ryhmässä* Γ*:*

(i) $a^2 = b^2 = c^2 = d^2 = 1_\Gamma$,

(ii) $bc = cb = d$, $dc = cd = b$ *ja* $db = bd = c$.

Todistus.

(*i*) Osoitetaan, että $g^2(w) = w$ kaikilla $w \in \Sigma^*$ ja $g \in \{a, b, c, d\}$. Kun $w = \epsilon$, väite on selvä. Alkion a määritelmästä seuraa

$$a^2(0w) = a(1w) = 0w \text{ ja } a^2(1w) = a(0w) = 1w$$

kaikilla $w \in \Sigma^*$ eli $a^2 = 1_\Gamma$. Osoitetaan väite käyttäen induktiota. Kun $l(w) = 0$, niin $w = \epsilon$, joka toteuttaa väitteen. Oletetaan, että väite on voimassa, kun $l(w) = n$. Alkioiden määritelmistä seuraa

$$\begin{aligned} &b^2(0w) = b(0a(w)) = 0a^2(w) = 0w,\ b^2(1w) = b(1c(w) = 1c^2(w) = 1w, \\ &c^2(0w) = c(0a(w)) = 0a^2(w) = 0w,\ c^2(1w) = c(1d(w) = 1d^2(w) = 1w, \\ &d^2(0w) = d(0w) = 0w,\ d^2(1w) = d(1c(w)) = 1c^2(w) = 1w, \end{aligned}$$

kaikilla $w \in \Sigma^*$. Eli induktioväite on voimassa, kun $l(w) = n + 1$, mistä väite seuraa.

(*ii*) Osoitetaan, että $ij(w) = k(w)$ kaikilla $w \in \Sigma^*$ ja $i, j, k \in \{b, c, d\}$, $i \neq j \neq k$. TOdistetaan väite induktiolla. Jos $l(w) = 0$, väite on voimassa. Oletetaan, että väite on voimassa, kun $l(w) = n$. Nyt

$$\begin{aligned} bc(0w) &= b(0a(w)) = 0a^2(w) = 0w = d(0w), \\ bc(1w) &= b(1d(w)) = 1cd(w) = 1b(w) = d(1w), \\ cd(0w) &= c(0w) = 0a(w) = b(0w), \\ cd(1w) &= c(1b(w)) = 1db(w) = 1c(w) = b(1w), \\ db(0w) &= d(0a(w)) = 0a(w) = c(0w), \\ db(1w) &= d(1c(w)) = 1bc(w) = 1d(w) = c(1w), \end{aligned}$$

kaikilla $w \in \Sigma^*$ eli väite pätee, kun $l(w) = n + 1$. Väite seuraa.

□

8.2 Grigorchukin ryhmän ominaisuuksia

Lauseesta 24 seuraa, että ryhmän Γ generoiva joukko $S = \{a, b, c, d\}$ on symmetrinen. Merkitään sanan pituutta funktiolla $l_S : \Gamma \to \mathbb{N}$. Jokainen ryhmän Γ alkio voidaan esittää muodossa

$$g = s_1 s_2 \cdots s_n, \tag{9}$$

jossa $s_i \in S$. Sanotaan, että 9 on alkion g *redusoitu muoto*, jos kaikilla $i, j = 1, 2, \ldots, n-1$ pätee, että kun $s_i = a$, niin $s_{i+1} \in \{b, c, d\}$ ja kun $s_j \in \{b, c, d\}$, niin $s_{j+1} = a$. Lauseesta 24 seuraa, että kaikki ryhmän Γ alkiot voidaan esittää redusoidussa muodossa.

Määritellään kaikilla $n \in \mathbb{N}$

$$H_n = \{g \in \Gamma : g(w) = w \text{ kaikilla } w \in \Sigma^n\}.$$

Osoitetaan, että H_n on ryhmän Γ normaali aliryhmä ja sen indeksi on äärellinen ryhmässä Γ kaikilla $n \in \mathbb{N}$

Lause 25. *Joukko H_n on ryhmän Γ normaali aliryhmä ja*

$$[\Gamma : H_n] < \infty,$$

kaikilla $n \in \mathbb{N}$. Lisäksi

$$\Gamma = H_0 \supset H_1 \supset H_2 \supset \cdots \supset H_n \supset H_{n+1} \supset \cdots .$$

Todistus. Koska $\Gamma \subset \mathrm{Sym}(\Sigma^*, \preceq)$, niin $g(\Sigma^*) \subset \Sigma^n$ kaikilla $g \in \Gamma$. Tarkastellaan kuvausta $\theta_n : \Gamma \to \mathrm{Sym}(\Sigma^n)$, jolle $\theta_n(g)(w) = g(w)$ kaikilla $g \in \Gamma$ ja $w \in \Sigma^n$. Selvästi θ on homomorfismi ja sen ydin $\ker(\theta_n) = H_n$. Eli H_n on ryhmän Γ normaali aliryhmä ja $[\Gamma : H_n] = |\Gamma / H_n| = |\theta_n(\Gamma)| \leq |\mathrm{Sym}(\Sigma^n)| < \infty$.

Olkoon $n \in \mathbb{N}$, $u \in \mathrm{Sym}(\Sigma^n)$ ja $g \in H_{n+1}$. Olkoon $\sigma \in \Sigma$ ja asetetaan $w = \sigma u \in \Sigma^{n+1}$, jolle $u \preceq w$. Koska $\Gamma \subset \mathrm{Sym}(\Sigma^*, \preceq)$, niin $g(u) \preceq g(w) = u\sigma$, josta seuraa, että $g(u) = u$. Tällöin $g \in H_n$ eli $H_n \supset H_{n+1}$. □

Seuraus 10. *Grigorchukin ryhmä Γ on residuaalisesti äärellinen.*

Todistus. Olkoon $h \in \cap_{n \in \mathbb{N}} H_n$. Kaikilla $w \in \Sigma^*$ on voimassa $h(w) = w$, joten $h = 1_\Gamma$. Tästä seuraa $\cap_{n \in \mathbb{N}} H_n = \{1_\Gamma\}$. Koska $[\Gamma : H_n] < \infty$ kaikilla $n \in \mathbb{N}$, niin kaikkien aliryhmien, joilla on äärellinen indeksi ryhmässä Γ, leikkaus on triviaali, mistä väite seuraa. □

Lause 26. *Seuraavat väitteet ovat voimassa ryhmälle H_1:*

(i) *H_1 koostuu kaikista ryhmän Γ alkioista, jotka voidaan ilmaista muodossa $g = s_1 s_2 \cdots s_n$, $s_i \in S$, jossa on parillinen määrä alkioita a,*

(ii) $[\Gamma : H_1] = 2$,

(iii) $H_1 = \langle b, c, d, aba, aca, ada \rangle$,

(iv) H_1 on alkioiden b, c ja d normaali sulkeuma ryhmässä Γ.

Todistus. Alkioiden a, b, c ja d määritelmistä seuraa, että $s(\sigma) = \sigma$ kaikilla $\sigma \in \Sigma$ jos ja vain jos $s \in \{b, c, d\}$. Olkoon $g = s_1 s_2 \cdots s_n$, $s_i \in S$. Nyt $g \in H_1$ jos ja vain jos $|i : s_i = a|$ on parillinen eli väite (i) on voimassa. Tästä seuraa myös väite (ii).

Olkoon $g \in H_1$. Se voidaan ilmaista yhdellä seuraavista redusoiduista muodoista:

$$\begin{aligned}
g &= t_0 a t_1 a t_2 a t_3 a t_4 \cdots a t_{2k-1} a t_{2k} = t_0(a t_1 a) t_2 (a t_3 a) t_4 \cdots (a t_{2k-1} a) t_{2k}, \\
g &= a t_1 a t_2 a t_3 a t_4 \cdots a t_{2k-1} a t_{2k} = (a t_1 a) t_2 (a t_3 a) t_4 \cdots (a t_{2k-1} a) t_{2k}, \\
g &= t_0 a t_1 a t_2 a t_3 a t_4 \cdots a t_{2k-1} a = t_0(a t_1 a) t_2 (a t_3 a) t_4 \cdots (a t_{2k-1} a), \\
g &= a t_1 a t_2 a t_3 a t_4 \cdots a t_{2k-1} a = (a t_1 a) t_2 (a t_3 a) t_4 \cdots (a t_{2k-1} a),
\end{aligned}$$

joissa $t_0, t_1, \ldots, t_{2k-1}, t_{2k} \in \{b, c, d\}$ ja $k \in \mathbb{N}$. Näin ollen väite (iii) on voimassa.

Nyt alkioiden b, c, d normaali sulkeuma ryhmässä Γ on aliryhmä $H \subset \Gamma$, jonka generoi kaikki konjugaatit gtg^{-1}, $g \in \Gamma$ ja $t \in \{b, c, d\}$. Kun valitaan alkion g arvoiksi 1_Γ ja a, niin voidaan todeta, että $H_1 \subset H$. Toisaalta $b, c, d \in H_1$, joten $H \subset H_1$. Väite (iv) seuraa. □

Olkoon $h_1 \in H_1$. Kaikilla $w \in \Sigma^*$ on olemassa sellaiset $w_0, w_1 \in \Sigma^*$, $l(w_0) = l(w_1) = l(w)$, että $h(0w) = 0w_0$ ja $h(1w) = 1w_1$. Merkitään $h_0, h_1 \in \mathrm{Sym}(\Sigma^*, \preceq)$ kuvauksia, joille $h_0(w) = w_0$ ja $h_1(w) = w_1$. Tällöin

$$h(0w) = 0h_0(w) \text{ ja } h(1w) = 1h_1(w),$$

kaikilla $w \in \Sigma^*$. Merkitään $\phi_0 : H_1 \to \mathrm{Sym}(\Sigma^*, \preceq)$ (vastaavasti $\phi_1 : H_1 \to \mathrm{Sym}(\Sigma^*, \preceq$)) kuvausta, jolle $\phi_0(h) = h_0$ (vastaavasti $\phi_1(h) = h_1$). Määritellään vielä tulokuvaus $\phi : H_1 \to \mathrm{Sym}(\Sigma^*, \preceq) \times \mathrm{Sym}(\Sigma^*, \preceq)$, $\phi(h) = (h_0, h_1)$. Nyt voidaan päätellä alkioiden määritelmien avulla, että

$$\begin{aligned}
&\phi(b) = (a, c),\ \phi(aba) = (c, a) \\
&\phi(c) = (a, d),\ \phi(aca) = (d, a) \\
&\phi(d) = (1_\Gamma, b),\ \phi(ada) = (b, 1_\Gamma).
\end{aligned} \tag{10}$$

Lause 27.

(i) Kuvaukset $\phi_0, \phi_1 : H_1 \to \Gamma$ ovat surjektiivisia homomorfismeja.

(ii) Kuvaus $\phi : H_1 \to \Gamma \times \Gamma$ on injektiivinen homomorfismi.

Todistus. Olkoon $\sigma \in \{0, 1\}$. Kaikille $h, h' \in H_1$ ja $w \in \Sigma^*$ saadaan

$$\sigma\phi_\sigma(hh')(w) = hh'(\sigma w) = h(\sigma\phi_\sigma(h')(w)) = \sigma\phi_\sigma(h)\phi_\sigma(h')(w).$$

Eli $\phi_\sigma(hh')(w) = \phi_\sigma(h)\phi_\sigma(h')(w)$, joten ϕ_0 ja ϕ_1 ovat homomorfismeja. Yhtälöistä (10) ja lauseen 26 kohdasta (iii) seuraa, että $\phi_0(H_1) = \phi_1(H_1) = \Gamma$. Eli kuvaukset ϕ_0 ja ϕ_1 ovat surjektiivisia.

Olkoon $h \in H_1$. Oletetaan, että $\phi(h) = 1_{\Gamma\times\Gamma} = (1_\Gamma, 1_\Gamma)$. Saadaan $h(\epsilon) = \epsilon$ ja $h(\sigma w) = \sigma h_\sigma(w) = \sigma w$ kaikilla $\sigma \in \{0, 1\}$ ja $w \in \Sigma^*$. Tällöin $h = 1_\Gamma = 1_H$ eli ϕ on injektiivinen kuvaus. □

Koska ϕ on injektiivinen kuvaus, voidaan jokainen alkio $h \in H_1$ samaistaa sen kuvan $\phi(h) \in \Gamma \times \Gamma$ kanssa. Eli merkitään $h = (h_0, h_1)$, jos $h \in H_1$ ja $\phi(h) = (h_0, h_1)$.

Seuraavassa lauseessa osoitetaan myös, että Grigorchukin ryhmä on 2-ryhmä eli jokaisen alkion kertaluku on muotoa 2^n, $n \in \mathbb{N}$.

Lause 28. *Grigorchukin ryhmä Γ on ääretön ryhmä, jonka generoi äärellinen joukko ja se ei sisällä yhtään alkiota, jonka kertaluku on ääretön.*

Todistus. Koska H_1 on aito ryhmän Γ osajoukko ja kuvaus ϕ_0 on surjektiivinen, Γ on ääretön.

Olkoon $X = \{a, b, c, d\}$ ryhmän Γ generoiva äärellinen ja symmetrinen joukko. Osoitetaan seuraavaksi, että jokaisen alkion $g \in \Gamma$ kertaluku on muotoa 2^n, $n \in \mathbb{N}$ eli että Γ on 2-ryhmä. Todistetaan väite induktiolla pituudelle $l_X(g)$. Väite on tosi, kun $l_X(g) = 1$, sillä $a^2 = b^2 = c^2 = d^2 = 1$.

Näytetään ensin, että jokainen alkio $g \in \Gamma \backslash \{1_\Gamma\}$ on konjugaatti joko joukon X alkiolle tai alkiolle g', joka voidaan esittää redusoidussa muodossa

$$g' = at_1at_2 \cdots at_k, \tag{11}$$

jossa $t_1, t_2, \ldots, t_k \in \{b, c, d\}$, $k \geq 1$ ja $l_X(g') \leq l_X(g)$. Jos g ei ole konjugaatti millekään joukon X alkiolle, niin millä tahansa alkiolla g:n konjugaattiluokasta on joku seuraavista muodoista (11) lisäksi:

$$t_1at_2 \cdots at_ka \text{ ja } t_0at_1 \cdots at_k,$$

jossa $t_0 \neq t_k$, $k \geq 1$. Konjugoimalla alkioilla a ja t_0 näitä esityksiä sekä korvaamalla alkion t_kt_0 alkiolla $t \in \{b, c, d\}$, päädytään tällöin esitykseen (11). Selvästi $l_X(g') \leq l_X(g)$.

Oletetaan, että $g \in H_1$ ja $l(g) > 1$. Koska alkion kertaluku on sama kuin sen konjugaattien kertaluku, voidaan olettaa, että g tai sen konjugaatti voidaan esittää muodossa (11) (jossa $k \geq 2$, koska $k \in H_1$). Nyt jokaisen nelikon $at_{2i-1}at_{2i}$, $i = 1, 2, \ldots, k/2$ kuvat $\phi_0(at_{2i-1}at_{2i})$ tai $\phi_1(at_{2i-1}at_{2i})$ ovat pituudeltaan ≤ 2. Näin ollen $l_X(g_0), l_X(g_1) \leq l_X(g)/2 < l_X(g)$. Induktion nojalla alkioiden g_0 ja g_1 kertaluku on 2^n, $n \in \mathbb{N}$ ja siksi $g = (g_0, g_1)$ on kertaluvultaan myös 2^n.

Oletetaan nyt, että $g \notin H_1$. Kuten edellä, voidaan olettaa, että g tai sen konjugaatti voidaan esittää muodossa (11) (jossa k on pariton, sillä $g \notin H_1$). Käydään läpi kolme tapausta.

Tapaus 1. Alkio d esiintyy alkion g esityksessä. Olkoon $d = t_i$ jollekin $1 \leq i \leq k$. Alkiota (11) tai sen konjugaattia konjugoimalla $t_{i-1}at_{i-2}a \cdots at_1a$, voidaan olettaa, että $d = t_1$.

Nyt $g^2 = (adat_2)(at_3at_4) \cdots (at_kad)(at_2at_3) \cdots (at_{k-1}at_k) \in H_1$. Jokaisen näiden nelikon kuva $\phi_0(at_iat_j)$ on pituudeltaan 2, paitsi niiden, jotka ovat muotoa $at_jad = (at_ja)d$, sillä $\phi_0(d) = 1_\Gamma$. Vähintään yksi näistä nelikoista esiintyy alkiossa g^2, esimerkiksi asettamalla $j = k$, $l_X(\phi_0(g^2)) \leq 2k - 1 < 2k = l_X(g)$. Induktiolla saadaan, että $\phi_0(g^2)$ on myös kertaluvultaan 2^n, $n \in \mathbb{N}$. Vastaava tulos voidaan myös johtaa kuvauksella ϕ_1: jokaisen nelikon kuva tällä kuvauksella on pituudeltaan 2 paitsi alkiot muotoa $adat_j = (ada)t_j$, sillä $\phi(ada) = 1_\Gamma$. Jälleen asettamalla $j = k$, voidaan todeta, että $l_X(\phi(g^2)) < l_X(g)$. Joten myös $\phi(g^2)$ on kertaluvultaan 2^n ja näin ollen $g^2 = (\phi_0(g^2), \phi_1(g^2)$ on kertaluvultaan 2^n.

Tapaus 2. Oletetaan, että alkio d ei esiinny g:ssä, mutta alkio c esiintyy. Kuten aiemmin, g:lle tai sen konjugaatille voidaan olettaa $t_1 = c$. Tällöin

$$\begin{aligned}\phi_0(abat') &= ca,\\ \phi_0(acat') &= da,\\ \phi_1(abat') &= ac \text{ ja}\\ \phi_1(acat') &= ad\end{aligned}$$

kaikilla $t' \in \{b, c\}$. Tästä seuraa, että $l_X(\phi_0(g^2)) = 2k = l_X(g)$. Nyt $\phi_0(g^2) = da \dots a$, joten konjugoimalla alkiolla a päästään tapaukseen 1. Vastaavasti $\phi_1(g^2) = a \cdots ad$, jolloin konjugoimalla alkiolla ad päästään myös tapaukseen 1. Eli $\phi_0(g^2)$ ja $\phi_1(g^2)$ ovat kertaluvultaan 2^n, $n \in \mathbb{N}$. Tällöin $g^2 = (\phi_0(g^2), \phi_1(g^2))$, joten alkio g on kertaluvultaan 2^n.

Tapaus 3. Viimeiseksi oletetaan, että kumpikaan alkioista d tai c ei esiinny esityksessä (11). Nyt välttämättä $g = (ab)^{2h+1}$ jollakin $h \geq 0$. Saadaan $g^2 = (ab)^{4h+2} = ((aba)b)^{2h+1} \in H_1$, joten $\phi_0(g^2) = (ca)^{2h+1}$ ja $\phi_1(g^2) = (ac)^{2h+1}$. Koska $l_X(\phi_0(g^2)) = l_X(\phi_1(g^2)) = 4h + 2 = l_X(g)$, joten päädymme tapaukseen 2 eli $\phi_0(g^2)$ ja $\phi_1(g^2)$ ovat kertaluvultaan 2^n, $n \in \mathbb{N}$. Joten $g^2 = (\phi_0(g^2), \phi_1(g^2))$ ja g ovat kertaluvultaan myös 2^n. □

Jotta voidaan osoittaa, että ryhmällä Γ ei ole polynomista kasvua, tulee ensin osoittaa muutamia tuloksia.

Lemma 7. *Ryhmä $D := \langle a, d\rangle \leq \Gamma$ on diedriryhmä, jonka kertaluku on 8.*

Todistus. Diedriryhmällä D_8, jonka kertaluku on 8, on presentaatio $D_8 = \langle x, y \mid x^2 = 1, y^2 = 1, (xy)^4 = 1\rangle$. Lauseessa 24 todettiin, että $a^2 = d^2 = 1$, joten riittää osoittaa, että alkion ad kertaluku on 4. Koska $(ad)^2 = (ada)d$, niin $(ad)^2 = (b, 1)(1, b) = (b, b) \neq 1_\Gamma$ ja $(ad)^4 = (ad^2)^2 = (b, b)^2 = (b^2, b^2) = (1_\Gamma, 1_\Gamma) = 1_\Gamma$. Eli alkion ad kertaluku on 4. □

Palautetaan mieleen, että kaksi ryhmää G_1 ja G_2 ovat yhteismitallisia, jos on olemassa kaksi aliryhmää, $K_1 \subset G_1$ ja $K_2 \subset G_2$, joilla on äärellinen indeksi, siten, että K_1 ja K_2 ovat isomorfisia.

Lause 29. *Γ ja $\Gamma \times \Gamma$ ovat yhteismitallisia.*

Todistus. Osoitetaan ensin, että ryhmän $\phi(H_1)$ indeksi ryhmässä Γ on äärellinen. Koska $H_1 = \langle b, c, d, aba, aca, ada\rangle$, niin voidaan päätellä, että

$$\begin{aligned}\phi(H_1) &= \langle \phi(b), \phi(c), \phi(d), \phi(aba), \phi(aca), \phi(ada)\rangle\\ &= \langle (a, c), (a, d), (1_\Gamma, b), (c, a), (d, a), (b, 1_\Gamma)\rangle.\end{aligned}$$

Olkoon $B \subset \Gamma$ alkion b normaali sulkeuma joukossa Γ. Tekijäjoukon Γ/B generoi ryhmän Γ generaattorien kuvat. Koska $cd = b \in B$, niin joukon B generoi alkioiden a ja d kuvat. Lemmasta 7 saadaan, että

$$[\Gamma : B] = |\Gamma|/|B| \leq 8.$$

Olkoon $g \in \Gamma$. Tarkastellaan alkiota gbg^{-1}. Koska ϕ_0 on surjektiivinen, niin on olemassa alkio $h \in H_1$ siten, että $\phi_0(h) = g$. Tästä seuraa, että $(gbg^{-1}, 1_\Gamma) = \phi(hadah^{-1}) \in \phi(H_1)$. Nämä alkiot generoivat aliryhmän $B_0 = B \times \{1_\Gamma\} \subset \phi(H_1)$. Vastaavasti voidaan johtaa kuvauksen ϕ_1 avulla aliryhmä $B_1 = \{1_\Gamma\} \times B \subset \phi(H_1)$. Huomataan, että $B_0 \simeq B_1 \simeq B$ ja että B_0 ja B_1 ovat ryhmän $\Gamma \times \Gamma$ normaaleja aliryhmiä. Lisäksi $B_0 \cap B_1 = \{1_{\Gamma\times\Gamma}\}$, joten $(\Gamma \times \Gamma)/B_0B_1 \simeq \Gamma/B \times \Gamma/B$. Koska todettiin, että $[\Gamma : B] \leq 8$ ja $B_0B_1 \subset \phi(H_1)$, niin

$$[\Gamma \times \Gamma : \phi(H_1)] \leq [\Gamma \times \Gamma : B_0B_1] = [\Gamma : B]^2 = 64.$$

Eli ryhmän $\phi(H_1)$ indeksi ryhmässä $\Gamma \times \Gamma$ on äärellinen.

Toisaalta $[\Gamma : H_1] = 2$ ja koska ϕ on injektiivinen homomorfismi, niin H_1 ja $\phi(H_1)$ ovat isomorfisia. Tästä seuraa, että Γ ja $\Gamma \times \Gamma$ ovat yhteismitallisia. □

Seuraus 11. *Ryhmällä Γ ei ole polynomista kasvua.*

Todistus. Koska Γ on lauseen 28 mukaan ääretön, niin $n \preceq s(\Gamma)$ (lause 13). Ryhmien Γ ja $\Gamma \times \Gamma$ yhteismitallisuudesta seuraa yhdessä korollaarin 7 kanssa, että $s(\Gamma) = s(\Gamma \times \Gamma)$. Toisaalta lauseesta 19 seuraa, että $s(\Gamma \times \Gamma) = s(\Gamma)^2$. Nyt lemmasta 3 saadaan, että $n^2 \preceq s(G)^2 = s(G)$. Induktion avulla voidaan todeta, että $n^{2h} \preceq s(G)$ kaikilla $h \in \mathbb{N}$, joten ryhmällä Γ ei voi olla polynomista kasvua. □

Jäljelle jää osoittaa, että Grigorchukin ryhmällä on subeksponentiaalista kasvua, jolloin edellisen korollaarin kanssa saadaan seurauksena, että Grigorchukin ryhmällä on välimuotoista kasvua.

Aloitetaan määrittelemällä eräs kriteeri sille, milloin äärellisen joukon generoimalle ryhmällä on subeksponentiaalista kasvua.

Lemma 8. *Olkoon G äärellisen joukon generoima ryhmä. Olkoon $X \subset G$ äärellinen ja symmetrinen ryhmän G generoiva joukko. Oletetaan, että on olemassa kokonaisluku $M \geq 2$, vakiot $0 < k < 1$ ja $K \geq 0$ sekä injektiivinen homomorfismi*

$$\begin{aligned} \psi : & H \to G^M \\ & g \mapsto (g_i)_{i=1}^M, \end{aligned}$$

jossa aliryhmällä $H \leq G$ on äärellinen indeksi ryhmässä G, siten että

$$\sum_{i=1}^{M} l_X(g_i) \leq k l_X(g) + K \tag{12}$$

kaikilla $g \in H$. Tällöin ryhmällä G on subeksponentiaalista kasvua.

Todistus. Näytetään, että $\omega_X = \lim_{n\to\infty} s_X^G(n)^{\frac{1}{n}} = 1$. Olkoon $\epsilon > 0$. Tällöin on olemassa sellainen luonnollinen luku $n_0 \geq 1$, että $s_X^G(n) < (\omega_X + \epsilon)^n$ kaikilla $n \geq n_0$. Koska $\omega_X \geq 1$, saadaan

$$s_X^G(n) \leq s_X^G(n_0)(\omega_X + \epsilon)^n \tag{13}$$

kaikilla $n \in \mathbb{N}$.

Olkoon

$$s_X^H(n) = |\{h \in H : l_X(h) \leq n\}|.$$

Olkoon T ryhmän H vasempien sivuluokkien edustajisto ryhmässä G. Asetetaan $C = \max_{t \in T} l_X(t)$. Nyt, kaikilla $g \in G$ on olemassa sellaiset yksikäsitteiset $h \in H$ ja $t \in T$, että $g = th$. Näin ollen $l_X(h) \leq l_X(t) + l_X(g) \leq C + l(g)$, joten $B_X^G(n) \subseteq TB_X^H(n + C)$. Voidaan päätellä, että

$$s_X^G(n) \leq [G : H] s_X^H(n + C). \tag{14}$$

Toisaalta, kohdasta (12) saadaan

$$s_X^H(n) \leq \sum s_X^G(n_1) s_X^G(n_2) \cdots s_X^G(n_M),$$

jossa summa otetaan yli M-monikkojen $n_1, n_2, \ldots, n_M$, joille pätee $\sum_{i=1}^M n_i \leq kn+K$.

Nyt kohdasta (13) saadaan, että

$$\begin{aligned} s_X^H(n) \leq & s_X^G(n_0)^M \sum (\omega_X + \epsilon)^{n_1} (\omega_X + \epsilon)^{n_2} \cdots (\omega_X + \epsilon)^{n_M} \\ = & s_X^G(n_0)^M \sum (\omega_X + \epsilon)^{n_1 + n_2 + \cdots + n_M} \\ \leq & (s_X^G(n_0)(kn + K))^M (\omega_X + \epsilon)^{kn+K}. \end{aligned}$$

Yhtälöstä (14) saadaan vielä

$$s_X^G(n) \leq [G : H] s_X^H(n + C) \leq [G : H] (s_X^G(n_0)(kn + K'))^M (\omega_X + \epsilon)^{kn+K'},$$

jossa $K' = K + kC$. Ottamalla nyt n:n juuren puolittain, epäyhtälön vasen puoli lähestyy nyt kasvufunktiota ω_X, kun $n \to \infty$. Epäyhtälön oikea puoli taas lähestyy arvoa $(\omega_X + \epsilon)^k$, kun $n \to \infty$. Eli $\omega_X \leq (\omega_X + \epsilon)^k$. Koska ϵ on mielivaltainen, voidaan päätellä, että $\omega_X \leq \omega_X^k$. Koska oletuksen nojalla $0 < k < 1$, saadaan $\omega_X = 1$.

Korollaarista 4 seuraa, että ryhmällä G on subeksponentiaalista kasvua. □

Lemma 9. *Olkoon $n \geq 1$. Tällöin $\phi_\sigma(H_{n+1}) \subseteq H_n$, kun $\sigma = 0, 1$.*

Todistus. Todistetaan väite induktiolla. Koska kuvaukset ϕ_0 ja ϕ_1 ovat surjektiivisia homomorfismeja, niin $\phi_\sigma(H_1) \subseteq \Gamma = H_0$. Oletetaan, että $\phi_\sigma(H_n) \subseteq H_{n-1}$ ja osoitetaan, että $\phi_\sigma(H_{n+1}) \subseteq H_n$. Olkoot $g \in H_{n+1}$ ja $w = \sigma u$, $u \in \Sigma^n$ ja $\sigma \in \{0, 1\}$. Nyt

$$\sigma u = w = g(w) = \sigma \phi_\sigma(g)(u),$$

eli $\phi_\sigma(g)(u) = u$. Tämä osoittaa, että $\phi_\sigma(g) \in H_n$. Näin ollen $\phi_\sigma(H_{n+1}) \subseteq H_n$. □

Äskeisen lemman seurauksena homomorfismit $\phi_w : H_n \to \Gamma$, jotka määritellään

$$\phi_w = \phi_{\sigma_1} \circ \phi_{\sigma_2} \circ \cdots \circ \phi_{\sigma_n}$$

ovat hyvin määriteltyjä kaikilla $n \geq 1$ ja $w = \sigma_1 \sigma_2 \cdots \sigma_n \in \Sigma^n$. Määritellään nyt homomorfismi $\psi_n : H_n \to \Pi_{w \in \Sigma^n} \Gamma$ asettamalla $\psi_n(g) = (\phi_w(g))_{w \in \Sigma^n}$ kaikilla $g \in \Gamma$.

Koska kuvaus ϕ on injektiivinen homomorfismi, niin kuvaus ψ_n on myös injektiivinen. Samaistamalla ryhmä H_n sen kuvan $\psi_n(H_n) \subseteq \Pi_{w\in\Sigma^n}\Gamma$ kanssa, merkitään $g = (g_w)_{w\in\Sigma^n}$ kaikilla $g \in H_n$.

Tästä eteenpäin tarkastellaan aakkostoa $\Lambda = \{\alpha, \beta, \gamma, \delta\}$ sekä monoidia Λ^*. Määritellään kuvaus $\Lambda \to X$ seuraavasti: $\alpha \mapsto a$, $\beta \mapsto b$, $\gamma \mapsto c$ ja $\delta \mapsto d$. Tämä kuvaus laajenee yksikäsitteisesti surjektiiviseksi homomorfismiksi $\pi : \Lambda^* \to \Gamma$. Sanotaan, että sana $w = \lambda_1\lambda_2\cdots\lambda_n \in \Lambda^*$ on *redusoitu*, jos kaikilla $i, j = 1, 2, \ldots, n$ pätee, että, jos $\lambda_i = \alpha$, niin $\lambda_{i+1} \in \{\beta, \gamma, \delta\}$ ja jos $\lambda_j \in \{\beta, \gamma, \delta\}$, niin $\lambda_{j+1} = \alpha$.

Määritellään transformaatio $p : \Lambda^2 \to \Lambda^*$ asettamalla

$$p(\lambda\lambda') = \begin{cases} \epsilon, \text{ jos } \lambda = \lambda' \\ \delta, \text{ jos } \lambda = \beta, \lambda' = \gamma \text{ tai } \lambda = \gamma, \lambda' = \beta \\ \gamma, \text{ jos } \lambda = \beta, \lambda' = \delta \text{ tai } \lambda = \delta, \lambda' = \beta \\ \beta, \text{ jos } \lambda = \gamma, \lambda' = \delta \text{ tai } \lambda = \delta, \lambda' = \gamma \\ \lambda\lambda', \text{ muulloin .} \end{cases} \tag{15}$$

Olkoon sana $u = \lambda_1\lambda_2\cdots\lambda_n \in \Lambda^*$ ja $1 \le i \le n$. Asetetaan

$$u_{(i)} = \lambda_1\lambda_2\cdots\lambda_{i-1}p(\lambda_i\lambda_{i+1})\lambda_{i+2}\cdots\lambda_n \in \Lambda^*.$$

Sana u on tällöin redusoitu jos ja vain jos $u = u_{(i)}$ kaikilla $i = 1, 2, \ldots, n-1$. Induktion avulla määritellään $u_{(i_1,i_2,\ldots,i_k)} = (u_{(i_1,i_2,\ldots,i_{k-1})})_{i_k}$ kaikilla $1 \le i_k \le l(u_{(i_1,i_2,\ldots,i_{k-1})}) - 1$.

Olkoon $w = \lambda_1\lambda_2\cdots\lambda_n \in \Lambda^*$. Jos sana w on redusoitu, merkitään $\overline{w} = w$. Jos taas w ei ole redusoitu, olkoon i_1 pienin kokonaisluku, jolla $w \neq w_{(i_1)}$. Jos $w_{(i_1)}$ on redusoitu, merkitään $\overline{w} = w_{(i_1)}$. Muulloin, olkoon i_1 pienin kokonaisluku, jolla $w_{(i_1)} \neq w_{(i_1,i_2)}$. Jos $w_{(i_1,i_2)}$ on redusoitu, merkitään $\overline{w} = w_{(i_1,i_2)}$. Samaan tapaan jatketaan, jos $w_{(i_1,i_2)}$ ei ole redusoitu. Koska $l(w) > l(w_{(i_1)}) > w_{(i_1,i_2)} > \cdots > w_{(i_1,i_2,\ldots,i_{k-1})} > w_{(i_1,i_2,\ldots,i_k)} > \ldots$, on olemassa sellainen $k \in N$, että $w_{(i_1,i_2,\ldots,i_k)}$ on redusoitu. Asetetaan nyt $\overline{w} = w_{(i_1,i_2,\ldots,i_k)}$. Transformaatiota $w_{(i_1,i_2,\ldots,i_{j-1})} \mapsto w_{(i_1,i_2,\ldots,i_j)}$ kutsutaan vasemmalta kumoamiseksi. Tästä seuraa, että jokainen sana $w \in \Lambda^*$ voidaan muuttaa redusoisuksi sanaksi äärellisellä jonolla vasemmalta kumoamisia.

Merkitään $\Theta_1 \subseteq \Lambda^*$ sellaista osajoukkoa, joka sisältää kaikki redusoidut sanat w joukossa Λ, jotka sisältävät parillisen määrän alkiota α ja merkitään tätä lukumäärää $l_\alpha(w)$. Eli sana $w \in \Theta_1$ on tulo, jossa vuorottelevat alkiot $(\alpha\lambda\alpha)$ ja λ', joissa $\lambda, \lambda' \in \{\beta, \gamma, \delta\}$. Tarkastellaan kuvauksia $\Phi_0 : \Theta_1 \to \Lambda^*$ ja $\Phi_1 : \Theta_1 \to \Lambda^*$, jotka määritellään seuraavasti: $\Phi_\sigma((\alpha\lambda_1\alpha)\lambda_2\cdots) = \Phi_\sigma(\alpha\lambda_1\alpha)\Phi_\sigma(\lambda_2)\cdots$ ja $\Phi_\sigma(\lambda_1(\alpha\lambda_2\alpha)\cdots) = \Phi_\sigma(\lambda_1)\Phi_\sigma(\alpha\lambda_2\alpha)\cdots$ kaikilla $\lambda_1, \lambda_2, ... \in \{\beta, \gamma, \delta\}$, $\sigma \in \{0, 1\}$, jossa

$$\begin{aligned} &\Phi_0(\beta) = \alpha,\ \Phi_0(\alpha\beta\alpha) = \gamma,\ \Phi_1(\beta) = \gamma,\ \Phi_1(\alpha\beta\alpha) = \alpha, \\ &\Phi_0(\gamma) = \alpha,\ \Phi_0(\alpha\gamma\alpha) = \delta,\ \Phi_1(\gamma) = \delta,\ \Phi_1(\alpha\gamma\alpha) = \alpha \\ &\Phi_0(\delta) = \epsilon,\ \Phi_0(\alpha\delta\alpha) = \beta,\ \Phi_1(\delta) = \beta,\ \Phi_1(\alpha\delta\alpha) = \epsilon. \end{aligned}$$

Nämä määritelmät seuraavat kaavasta (10).

Määritellään induktiivisesti $\Theta_{n+1} \subseteq \Lambda^*$, $n \geq 1$, osajoukoksi, joka sisältää kaikki redusoidut sanat $w \in \Theta_n$ siten, että redusoidut sanat $\Phi_0(w), \Phi_1(w) \in \Theta_n$. Asetetaan rekursiivisesti sanalle $w_{\sigma_0\sigma_1\cdots\sigma_{n-1}\sigma} = \overline{\Phi_\sigma(w_{\sigma_0\sigma_1\cdots\sigma_{n-1}})}$ kaikilla $\sigma, \sigma_1, \sigma_2, \ldots, \sigma_{n-1} \in \{0,1\}$.

Lemma 10. *Kaikilla $w \in \Theta_1$ pätee*

$$l(w_0) + l(w_1) \leq l(w) + 1.$$

Todistus. Olkoon $w \in \Theta_1$. Käsittelemme kolme tapausta.

Tapaus 1. Oletetaan, että sana on muotoa $w = (\alpha\lambda_1\alpha)\lambda_2\cdots\lambda_{k-1}(\alpha\lambda_k\alpha)$, $\lambda_i \in \{\beta, \gamma, \delta\}$. Huomataan, että $l(w) = 2k+1$. Nyt

$$\begin{aligned} w_\sigma &= \overline{\Phi_\sigma(w)} \text{ ja} \\ \Phi_\sigma(w) &= \Phi_\sigma(\alpha\lambda_1\alpha)\Phi_\sigma(\lambda_2)\cdots\Phi_\sigma(\lambda_{k-1})\Phi_\sigma(\alpha\lambda_k\alpha), \end{aligned}$$

joten

$$\begin{aligned} l(w_\sigma) = l(\overline{\Phi_\sigma(w)}) &\leq l(\Phi_\sigma(w)) \\ &\leq l(\Phi_\sigma(\alpha\lambda_1\alpha)) + l(\Phi_\sigma(\lambda_2)) + \cdots + l(\Phi(\lambda_{k-1})) + l(\Phi_\sigma(\alpha\lambda_k\alpha)) \\ &\leq k = \frac{(2k+1)-1}{2} \\ &= \frac{l(w)-1}{2}. \end{aligned}$$

Eli

$$l(w_0) + l(w_1) \leq 2 \cdot \frac{l(w)-1}{2} = l(w) - 1 \leq l(w) + 1.$$

Tapaus 2. Oletetaan, että $w = \lambda_1(\alpha\lambda_2\alpha)\cdots(\alpha\lambda_{k-1}\alpha)\lambda_k$, jossa $\lambda_i \in \{\beta, \gamma, \delta\}$. Huomataan, että $l(w) = 2k-1$. Nyt

$$\begin{aligned} w_\sigma &= \overline{\Phi_\sigma(w)} \text{ ja} \\ \Phi_\sigma(w) &= \phi_\sigma(\lambda_1)\Phi_\sigma(\alpha\lambda_2\alpha)\cdots\Phi_\sigma(\alpha\lambda_{k-1}\alpha)\Phi_\sigma(\lambda_k), \end{aligned}$$

joten

$$\begin{aligned} l(w_\sigma) = l(\overline{\Phi_\sigma(w)}) &\leq l(\Phi_\sigma(w)) \\ &\leq l(\Phi_\sigma(\lambda_1) + l(\Phi_\sigma(\alpha\lambda_2\alpha)) + \cdots + l(\Phi(\alpha\lambda_{k-1}\alpha)) + l(\Phi_\sigma(\lambda_k) \\ &\leq k = \frac{(2k-1)+1}{2} \\ &= \frac{l(w)+1}{2}. \end{aligned}$$

Eli

$$l(w_0) + l(w_1) \leq 2 \cdot \frac{l(w)+1}{2} = l(w) + 1.$$

Tapaus 3. Viimeisenä oletetaan, että $w = (\alpha\lambda_1\alpha)\lambda_2 \cdots (\alpha\lambda_{k-1}\alpha)\lambda_k$, $\alpha_i \in \{\beta, \gamma, \delta\}$. Huomataan, että $l(w) = 2k$. Nyt

$$\begin{aligned} w_\sigma &= \overline{\Phi_\sigma(w)} \text{ ja} \\ \Phi_\sigma(w) &= \Phi_\sigma(\alpha\lambda_1\alpha)\Phi_\sigma(\lambda_2)\cdots\Phi_\sigma(\lambda_{k-1})\Phi_\sigma(\alpha\lambda_k\alpha), \end{aligned}$$

joten

$$\begin{aligned} l(w_\sigma) = l(\overline{\Phi_\sigma(w)}) &\leq l(\Phi_\sigma(w)) \\ &\leq l(\Phi_\sigma(\alpha\lambda_1\alpha)) + l(\Phi_\sigma(\lambda_2)) + \cdots + l(\Phi(\alpha\lambda_{k-1}\alpha)) + l(\Phi_\sigma(\lambda_k)) \\ &\leq k = \frac{(2k)}{2} \\ &= \frac{l(w)}{2}. \end{aligned}$$

Eli

$$l(w_0) + l(w_1) \leq 2 \cdot \frac{l(w)}{2} = l(w) \leq l(w) + 1.$$

□

Lemma 11. *Kaikilla $g \in H_3$ pätee*

$$\sum_{i,j,k=0}^{1} l_X(g_{ijk}) \leq \frac{5}{6} l_X(g) + 8$$

Todistus. Olkoot $g \in H_3$ ja $w \in \Theta_3$ sellaisia alkioita, että $g = \pi(w)$ ja $l_X(g) = l(w)$. Käytetään lemmaa 10 kolme kertaa:

$$\begin{aligned} \sum_{i,j=0}^{1} l(w_{ij}) &\leq \sum_{i=0}^{1} (l(w_i) + 1) \\ &= \sum_{i=0}^{1} l(w_i) + 2 \\ &\leq l(w) + 3, \end{aligned} \tag{16}$$

josta saadaan, että

$$\begin{aligned} \sum_{i,j,k=0}^{1} l(w_{ijk}) &\leq \sum_{i,j=0}^{1} (l(w_{ij}) + 1) \\ &\leq \sum_{i,j=0}^{1} l(w_{ij}) + 4 \\ &\leq \left(\sum_{i=0}^{1} l(w_i) + 2 \right) + 4 = \sum_{i=0}^{1} l(w_i) + 6 \\ &\leq l(w) + 1 + 6 = l(w) + 7. \end{aligned} \tag{17}$$

Huomataan, että kuvausten Φ_0 ja Φ_1 määritelmien nojalla saadaan, että

$$l(w_0) + l(w_1) \leq l(w) + 1 - l_\delta(w), \tag{18}$$

jossa $l_\delta(w)$ on alkion δ lukumäärä sanassa w. Jokainen alkio δ esiintyy sanassa joko itsekseen δ, jolle $\Phi_0(\delta) = \epsilon$ tai kolmikossa $(\alpha\delta\alpha)$, jolle $\Phi_1(\alpha\delta\alpha) = \epsilon$.

Toiseksi, jos alkio γ esiintyy sanassa w, niin $\Phi_0(\alpha\gamma\alpha) = \delta$ tai $\Phi_1(\gamma) = \delta$, jolloin alkion δ lukumäärä kasvaa joko sanassa w_0 tai w_1. Eli,

$$l(w_{00}) + l(w_{01}) + l(w_{10}) + l(w_{11}) \leq l(w) + 3 - l_\gamma(w), \tag{19}$$

jossa $l_\gamma(w)$ on alkion γ lukumäärä sanassa w.

Viimeisenä, jos alkio β esiintyy sanassa w, niin $\Phi_0(\alpha\beta\alpha) = \gamma$ ja $\Phi_1(\beta) = \gamma$, jolloin alkion γ lukumäärä kasvaa joko sanassa w_0 tai w_1. Näin ollen alkion δ lukumäärä kasvaa jossakin sanoista w_{00}, w_{01}, w_{10} ja w_{11}, joten

$$\sum_{i,j,k=0}^{1} l(w_{ijk}) \leq l(w) + 7 - l_\beta(w), \tag{20}$$

jossa $l_\beta(w)$ on alkion β lukumäärä sanassa w.

Koska $l(w) = l_\alpha(w) + l_\beta(w) + l_\gamma(w) + l_\delta(w)$ ja w on redusoitu, saadaan

$$l_\beta(w) + l_\gamma(w) + l_\delta(w) \geq \frac{l(w) - 1}{2}, \tag{21}$$

joten

$$\max_{\lambda \in \{\beta,\gamma,\delta\}} l_\lambda(w) > \frac{l(w)}{6} - 1. \tag{22}$$

Nyt epäyhtälöiden (17) avulla saadaan, että

$$\sum_{i,j,k=0}^{1} l(w_{ijk}) \leq \min\{\sum_{i=0}^{1} l(w_i) + 6, \sum_{i,j=0}^{1} l(w_{ij}) + 4\}. \tag{23}$$

Huomataan, että $\pi(w_{ijk}) = g_{ijk}$, jolloin $l_X(g_{ijk}) \leq l(w_{ijk})$ kaikilla $i, j, k = 0, 1$. Nyt käyttäen ensin yhtälöitä (23), (18), (19) ja (20) sekä sitten yhtälöä (21), saadaan

$$\begin{aligned}
\sum_{i,j,k=0}^{1} l_X(g_{ijk}) &\leq \sum_{i,j,k=0}^{1} l(w_{ijk}) \\
&\leq \min\{l(w) + 7 - l_\beta(w), l(w) + 7 - l_\gamma(w), l(w) + 7 - l_\delta(w)\} \\
&\leq l(w) + 7 - \max\{l_\beta(w), l_\gamma(w), l_\delta(w)\} \\
&\leq l(w) + 7 - \left(\frac{l(w)}{6} - 1\right) \\
&\leq \frac{5}{6} l(w) + 8 \\
&= \frac{5}{6} l(g) + 8.
\end{aligned}$$

□

Nyt voidaan osoittaa, että Grigorchukin ryhmällä on subeksponentiaalista kasvua.

Lause 30. *Grigorchukin ryhmällä* Γ *on subeksponentiaalista kasvua.*

Todistus. Olkoon $H = H_3$. Lauseen 25 nojalla $[G : H] < \infty$. Lemman 11 nojalla voidaan valita $\psi = \psi_3$, $M = 8$, $k = \frac{5}{6}$ ja $K = 8$, jolloin lemmasta 8 seuraa väite. $\square$

Lauseista 11 ja 30 seuraa yhdessä tämän luvun päätulos:

Seuraus 12. *Grigorchukin ryhmällä on välimuotoista kasvua.*

Viitteet

[1] *How Groups Grow*, Mann, Avinoam, 2012, Cambridge University Press, New York

[2] *Cellular Automata and Groups*, Ceccherini-Silberstein, Tullio, Coornaert, Michel, 2010, Springer, Berlin, Heidelberg

[3] *Ryhmäteoria, Lahtonen*, Jyrki, 2023, Turun yliopisto

[4] *Algebran peruskurssi I*, Koppinen, Markku, Turun yliopisto, 2006

[5] *Algebran peruskurssi II*, Koppinen, Markku, Turun yliopisto

[6] *Hausdorffin ja affiinin ulottuvuuden yhtäsuuruus*, Kössö, Valtteri, Pro Gradu -tutkielma, Oulun yliopisto, 2020

[7] *Growth Rate of Groups*, Lim Han, Cong, 2009

[8] *A Note On Curvature and Fundamental Group*, J. Milnor, Journal of Differential Geometry. 2, 1968

[9] *Nilpotentin ryhmän ekvivalentit määritelmät*, Karppanen, Matti, Pro Gradu -tutkielma, Helsingin yliopisto, 2014

[10] *Some properties of the growth and of the algebraic entropy of group endomorphisms*, Bruno, Spiga, Journal of Group Theory, Vol. 20 Is. 4, De Gruyter, 2016