Tampereen yliopisto

Jonne Karru

ÄÄRELLISTEN ABELIN RYHMIEN RAKENTEESTA

Informaatioteknologian ja viestinnän tiedekunta
Kandidaattitutkielma
Helmikuu 2020

Tiivistelmä

Jonne Karru: Äärellisten Abelin ryhmien rakenteesta
Kandidaattitutkielma
Tampereen yliopisto
Matematiikan ja tilastotieteen tutkinto-ohjelma
Helmikuu 2020

Tässä tutkielmassa luokitellaan kaikki äärelliset Abelin ryhmät isomorfiaa vaille ja tarkastellaan tietyn kertaluvun omaavien ei-isomorfisten Abelin ryhmien määrittämistä.

Luvussa 3 tarkastellaan äärellisiä Abelin ryhmiä. Näille ryhmille esitetään ja todistetaan erilaisia ominaisuuksia sekä pykälän päätuloksena esitetään ja todistetaan äärellisten Abelin ryhmien peruslause. Peruslauseen nojalla saadaan luokiteltua kaikki äärelliset Abelin ryhmät ja sen avulla johdettuja ominaisuuksia käytetään määrittämään saman kertaluvun kaikki eri Abelin ryhmät isomorfiaa vaille. Luvussa 2 esitetään luettelomaisesti luvussa 3 tarvittavia ryhmäteorian määritelmiä ja lauseita.

Avainsanat: ryhmä, ryhmäteoria, Abelin ryhmä, äärellinen Abelin ryhmä, p-ryhmä

Sisältö

1 Johdanto

Tässä tutkielmassa luokitellaan kaikki äärelliset Abelin ryhmät isomorfiaa vaille ja tarkastellaan tietyn kertaluvun omaavien ei-isomorfisten Abelin ryhmien määrittämistä.

Tutkielman edetessä huomataan, että eräät lukuteorian perustulokset ovat isossa roolissa äärellisten Abelin ryhmien rakennetta tarkasteltaessa. Historiallisesti lukuteorian käsitteiden tutkimus yhdessä ryhmäteorian käsitteiden kanssa johtikin erityisesti sekä äärellisten että äärettömien Abelin ryhmien teorian kehitykseen.

Luvussa 3 tarkastellaan äärellisiä Abelin ryhmiä. Näille ryhmille esitetään ja todistetaan erilaisia ominaisuuksia sekä pykälän päätuloksena esitetään ja todistetaan äärellisten Abelin ryhmien peruslause. Peruslauseen nojalla saadaan luokiteltua kaikki äärelliset Abelin ryhmät ja sen avulla johdettuja ominaisuuksia käytetään määrittämään saman kertaluvun kaikki eri Abelin ryhmät isomorfiaa vaille.

Luvussa 2 esitetään luettelomaisesti luvussa 3 tarvittavia ryhmäteorian määritelmiä ja lauseita. Lukijalta edellytetään ryhmäteorian peruskäsitteiden hyvää tuntemista, vaikka luvussa 2 onkin esitetty iso osa tarvittavista käsitteistä. Lähdeteoksena tutkielmassa on käytetty Mordesonin ja Senin teosta Fundamentals of Abstract Algebra. Vaihtoehtoisia tutkielman aihetta käsitteleviä teoksia löytyy lähteistä [2] ja [3].

2 Valmistelevia tarkasteluja

2.1 Peruskäsitteitä

Tässä luvun 2 pykälässä 2.1 esitetään ryhmän, Abelin ryhmän ja aliryhmän määritelmät sekä ryhmien neutraalialkioon ja vasta-alkioihin liittyvä lause. Määritelmät sekä lauseet todistuksineen ovat lähteestä [1] sivuilta 58–59 ja sivulta 99.

Määritelmä 2.1. *Ryhmä* on järjestetty pari $(G, *)$, missä G on epätyhjä joukko ja $*$ on joukon G sellainen laskutoimitus, että seuraavat ehdot pätevät:

(i) Laskutoimitus $*$ on *liitännäinen* joukossa G eli $a * (b * c) = (a * b) * c$ aina, kun $a, b, c \in G$.

(ii) On olemassa sellainen $e \in G$, että $a * e = a = e * a$ aina, kun $a \in G$. Alkiota e kutsutaan *neutraalialkioksi*.

(iii) Jokaista alkiota $a \in G$ kohti on olemassa sellainen $b \in G$, että $a * b = e = b * a$. Alkiota b kutsutaan alkion a *vasta-alkioksi*.

Määritelmä 2.2. Jos ryhmälle $(G, *)$ pätee lisäksi, että $a * b = b * a$ jokaisella $a, b \in G$ eli laskutoimitus $*$ on *vaihdannainen*, niin ryhmää kutsutaan *Abelin ryhmäksi*.

Lause 2.3. *Olkoon $(G, *)$ ryhmä. Tällöin neutraalialkio $e \in G$ on yksikäsitteinen ja jokaisella $a \in G$ on yksikäsitteinen vasta-alkio $b \in G$.*

Todistus. Ks. [1, ss. 58–59]. □

Pari $(\{e\}, *)$ eli neutraalialkion omaava joukko varustettuna laskutoimituksella on ryhmä ja sitä kutsutaan *triviaaliksi ryhmäksi*. Alkion a vasta-alkiota voidaan kutsua *käänteisalkioksi* ja siitä käytetään myös merkintää a^{-1}.

Määritelmä 2.4. Olkoon $(G, *)$ ryhmä ja H joukon G epätyhjä osajoukko. Tällöin pari $(H, *)$ on ryhmän $(G, *)$ *aliryhmä*, jos $(H, *)$ on ryhmä.

2.2 Erilaisia ryhmiä ja niiden ominaisuuksia

Tässä pykälässä esitetään syklisen ryhmän ja normaalin aliryhmän määritelmät sekä niihin liittyviä lauseita. Lisäksi esitetään Lagrangen lause sekä eräs sen seuraus ja ensimmäinen isomorfialause. Määritelmät sekä lauseet todistuksineen lukuunottamatta lausetta 2.11 ovat lähteestä [1] sivuilta 110–154.

Määritelmä 2.5. Ryhmä $(G, *)$ on *syklinen ryhmä*, jos on olemassa sellainen $a \in G$, että $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.

Lause 2.6. *Jokainen syklinen ryhmä on Abelin ryhmä.*

Todistus. Ks. [1, s. 110]. □

Lause 2.7. *Jokainen äärellinen syklinen ryhmä, jonka kertaluku on n, on isomorfinen ryhmän $(\mathbb{Z}_n, +_n)$ kanssa, ja jokainen ääretön syklinen ryhmä on isomorfinen ryhmän $(\mathbb{Z}, +)$ kanssa.*

Todistus. Ks. [1, s. 110]. □

Tästä lähtien käytetään merkinnällistä lyhennettä G ryhmälle $(G, *)$ eli ryhmään viitataan merkitsemällä sitä siihen liitettävällä joukolla. Myös laskutoimitus $*$ voidaan jättää merkitsemättä, eli esimerkiksi alkioiden a ja b laskutoimitusta $a * b$ merkitään ab.

Lause 2.8. *Syklisen ryhmän jokainen aliryhmä on syklinen.*

Todistus. Ks. [1, s. 112]. □

Lause 2.9. *Olkoon G äärellinen syklinen ryhmä, jonka kertaluku on m. Tällöin jokaista kertaluvun m positiivista jakajaa d kohti on olemassa yksikäsitteinen ryhmän G aliryhmä, jonka kertaluku on d.*

Todistus. Ks. [1, s. 113]. □

Määritelmä 2.10. Olkoon G ryhmä. Ryhmän G aliryhmää H kutsutaan ryhmän G *normaaliksi aliryhmäksi*, jos $aH = Ha$ jokaisella $a \in G$.

Lause 2.11. *Olkoon G Abelin ryhmä. Tällöin jokainen ryhmän G aliryhmä on normaali aliryhmä.*

Todistus. Olkoon G Abelin ryhmä ja H sen aliryhmä. Oletetaan, että $a \in G$. Tällöin $ah = ha$ jokaisella $h \in H$, koska $H \subseteq G$ ja G on Abelin ryhmä. Näin ollen $aH = Ha$. Koska a oli mielivaltainen, niin $aH = Ha$ jokaisella $a \in G$, joten H on ryhmän G normaali aliryhmä. □

Lause 2.12 (Lagrangen lause)**.** *Olkoon H äärellisen ryhmän G aliryhmä. Tällöin ryhmän H kertaluku jakaa ryhmän G kertaluvun.*

Todistus. Ks. [1, s. 120]. □

Seuraus 2.13. *Olkoon G äärellinen ryhmä, jonka kertaluku on n. Tällöin ryhmän G jokaisen alkion a kertaluku jakaa ryhmän G kertaluvun n ja $a^n = e$.*

Todistus. Ks. [1, s. 121]. □

Lause 2.14 (Ensimmäinen isomorfialause)**.** *Olkoon f homomorfismi ryhmältä G ryhmälle G_1. Tällöin $f(G)$ on ryhmän G_1 aliryhmä ja $G/\mathrm{Ker}\, f \simeq f(G)$.*

Todistus. Ks. [1, s. 154]. □

2.3 p-ryhmistä

Kun tarkastellaan äärellisten Abelin ryhmien rakennetta, p-ryhmät ja Sylowin p-aliryhmät ovat merkittävässä roolissa. Tässä pykälässä esitellään ensin Cauchyn lause, minkä jälkeen määritellään p-ryhmä ja esitetään riittävä ja välttämätön ehto sille, että ryhmä on äärellinen p-ryhmä. Tämän jälkeen määritellään Sylowin p-aliryhmä sekä todistetaan Sylowin p-aliryhmille kaksi ominaisuutta. Määritelmät sekä lauseet todistuksineen ovat lähteestä [1] sivuilta 196–205.

Lause 2.15 (Cauchyn lause)**.** *Olkoon G äärellinen ryhmä, jonka kertaluku n on jaollinen alkuluvulla p. Tällöin ryhmä G sisältää alkion, jonka kertaluku on p ja täten aliryhmän, jonka kertaluku on p.*

Todistus. Ks. [1, ss. 196-197]. □

Määritelmä 2.16. Olkoon p alkuluku. Ryhmä G on *p-ryhmä*, jos ryhmän G jokaisen alkion kertaluku on muotoa p^n, missä n on jokin positiivinen kokonaisluku.

Lause 2.17. *Olkoon G epätriviaali p-ryhmä. Ryhmä G on äärellinen p-ryhmä, jos ja vain jos $|G| = p^k$ jollakin positiivisella kokonaisluvulla k.*

Todistus. Ks. [1, s. 198]. □

Määritelmä 2.18. Olkoon G äärellinen ryhmä ja p alkuluku. Ryhmän G aliryhmää P kutsutaan ryhmän G *Sylowin p-aliryhmäksi*, jos P on p-aliryhmä ja se ei sisälly aidosti mihinkään muuhun ryhmän G p-aliryhmään. Toisin sanoen P on ryhmän G maksimaalinen p-aliryhmä.

Lause 2.19. *Äärellisellä ryhmällä G on Sylowin p-aliryhmä jokaisella alkuluvulla p.*

Todistus. Ks. [1, ss. 202-203]. □

Lause 2.20. *Olkoon G äärellinen ryhmä ja olkoon lisäksi H ryhmän G Sylowin p-aliryhmä. Tällöin H on ryhmän G yksikäsitteinen Sylowin p-aliryhmä, jos ja vain jos H on ryhmän G normaali aliryhmä.*

Todistus. Ks. [1, s. 205]. □

2.4 Ryhmien suorat tulot

Tässä pykälässä määritellään ryhmien suora tulo (myöhemmin Abelin ryhmistä puhuttaessa suora summa) ja esitetään eräitä ryhmien suoriin tuloihin liittyviä lauseita. Määritelmät sekä lauseet todistuksineen ovat lähteestä [1] sivuilta 181–184.

Määritelmä 2.21. Olkoon $I_n = \{1, 2, \ldots, n\}$ indeksijoukko ja $\{(G_i, *_i) \mid i \in I_n\}$ joukko ryhmiä. Olkoon lisäksi

$$G = G_1 \times G_2 \times \cdots \times G_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in G_i, i \in I_n\}.$$

Asetetaan vielä joukolle G laskutoimitus $*$ siten, että jokaisella $(a_1, a_2, \ldots, a_n)$, $(b_1, b_2, \ldots, b_n) \in G$ pätee

$$(a_1, a_2, \ldots, a_n) * (b_1, b_2, \ldots, b_n) = (a_1 *_1 b_1, a_2 *_2 b_2, \ldots, a_n *_n b_n).$$

Määritelmässä 2.21 suoran tulon ryhmien laskutoimituksia $*_i$ ei merkitä tästä eteenpäin tässä pykälässä vaan käytetään yleisen kertolaskun merkintätapaa eli $a *_i b$ merkitään ab.

Lause 2.22. *Olkoon $\{G_i \mid i \in I_n\}$ joukko ryhmiä ja $G = G_1 \times G_2 \times \cdots \times G_n$. Olkoon lisäksi e_i ryhmän G_i neutraalialkio jokaisella $i \in G$. Tällöin $(G, *)$, missä $*$ on määritelmän 2.21 mukainen laskutoimitus, on ryhmä, jonka neutraalialkio on $e = (e_1, e_2, \ldots, e_n)$ ja jokaisella $(a_1, a_2, \ldots, a_n) \in G$ on vasta-alkio $(a_1, a_2, \ldots, a_n)^{-1} = (a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1})$.*
Edelleen, olkoon $H_i = \{(e_1, e_2, \ldots, e_{i-1}, a_i, e_{i+1}, \ldots, e_n) \mid a_i \in G_i\}$ jokaisella $i \in I_n$. Tällöin seuraavat ehdot pätevät.

(i) H_i on ryhmän G normaali aliryhmä jokaisella $i \in I_n$.

(ii) Jokainen $a \in G$ voidaan ilmaista yksikäsitteisesti muodossa $a = h_1 h_2 \cdots h_n$, missä $h_i \in H_i$ ja $i \in I_n$.

(iii) $H_i \cap (H_1 H_2 \cdots H_{i-1} H_{i+1} \cdots H_n) = \{e\}$ *jokaisella* $i \in I_n$.

(iv) $G = H_1 H_2 \cdots H_n$.

Todistus. Ks. [1, ss. 182-183]. □

Määritelmä 2.23. Lauseen 2.22 mukainen ryhmä G on ryhmien G_i, $i \in I_n$ *suora ulkotulo*.

Määritelmä 2.24. Olkoon G ryhmä ja $\{ N_i \mid i \in I_n \}$ joukko ryhmän G normaaleja alirymiä. Tällöin ryhmä G on ryhmien $N_1, N_2, \ldots, N_n$ *suora sisätulo*, jos jokainen $a \in G$ voidaan ilmaista yksikäsitteisesti muodossa $a = a_1 a_2 \cdots a_n$, missä $a_i \in N_i$ jokaisella $i \in I_n$.

Lause 2.25. *Olkoon* G *ryhmä ja* $\{ N_i \mid i \in I_n \}$ *joukko ryhmän* G *normaaleja alirymiä. Tällöin ryhmä* G *on joukon* $\{ N_i \mid i \in I_n \}$ *suora sisätulo, jos ja vain jos* $G = N_1 N_2 \cdots N_n$ *ja* $N_i \cap (N_1 N_2 \cdots N_{i-1} N_{i+1} \cdots N_n) = \{e\}$ *jokaisella* $i \in I_n$.

Todistus. Ks. [1, s. 184]. □

3 Äärelliset Abelin ryhmät

3.1 Äärellisten Abelin ryhmien rakenne

Tässä pykälässä tarkastellaan äärellisten Abelin ryhmien rakenteellisia ominaisuuksia. Lauseen 2.7 nojalla kaikki äärelliset sykliset ryhmät on määritetty isomorfiaa vaille ja tästä eteenpäin äärelliseksi sykliseksi ryhmäksi, jonka kertaluku on n, voidaan yleisyyttä menettämättä valita additiivinen ryhmä $\mathbb{Z}_n$.

Merkinnällisesti tässä luvussa käytetään yhteenlaskun merkintätapaa eli ab on $a+b$ ja a^n on na, missä $n \in \mathbb{Z}$. Lisäksi käytetään alkiota 0 ryhmän neutraalialkiona, alkion a vasta-alkiolle käytetään merkintää $-a$ ja alkion a kertaluvulle käytetään merkintää $\circ(a)$. Indeksijoukosta lukuun n asti, kuten edellisessä luvussa, käytetään merkintää $I_n = \{1, 2, 3, \ldots, n\}$. Lisäksi ryhmien tai aliryhmien suorasta ulko- tai sisätulosta $G \times H$ käytetään merkintää $G \oplus H$ ja sitä kutsutaan ryhmien G ja H *suoraksi summaksi*.

Luvun päätuloksena esitetään ja todistetaan äärellisten Abelin ryhmien peruslause lauseessa 3.8. Lauseen nojalla kaikilla äärellisillä Abelin ryhmillä on yksikäsitteinen esitys syklisten p-ryhmien suorana summana. Täten suoran summan käsite on olennainen osa äärellisten Abelin ryhmien luokittelua ja alla esitetään riittävä ja välttämätön ehto, jotta Abelin ryhmä on aliryhmiensä suora summa.

Lause 3.1. *(Vrt. [1, s. 247]) Olkoon G Abelin ryhmä. Ryhmä G on aliryhmiensä $G_1, G_2, \ldots, G_n$ suora summa, jos ja vain jos*

(i) $G = G_1 + G_2 + \cdots + G_n$ *(toisin sanoen jokainen $g \in G$ voidaan esittää muodossa $g = g_1 + g_2 + \cdots + g_n$ jollakin $g_i \in G_i$, $i \in I_n$) ja*

(ii) $G_i \cap (G_1 + G_2 + \cdots + G_{i-1} + G_{i+1} + \cdots + G_n) = \{0\}$ *jokaisella $i \in I_n$.*

Todistus. Lauseen 2.11 nojalla jokainen ryhmän G aliryhmä on normaali aliryhmä, joten lauseen todistus seuraa suoraan lauseesta 2.25. □

Jos ryhmä G on aliryhmien $G_1, G_2, \ldots, G_n$ suora summa, niin merkitään

$$G = G_1 \oplus G_2 \oplus \cdots \oplus G_n.$$

Osoitetaan vielä, että jos ryhmä on aliryhmiensä suora summa, niin se on isomorfinen aliryhmiensä kanssa isomorfisten ryhmien suoran summan kanssa.

Lause 3.2. *(Vrt. [1, s. 247]) Olkoon G Abelin ryhmä. Jos $G = G_1 \oplus G_2 \oplus \cdots \oplus G_n$ ja $G_i \simeq H_i$, missä H_i on ryhmä ja $i \in I_n$, niin*

$$G \simeq H_1 \oplus H_2 \oplus \cdots H_n.$$

Todistus. Oletetaan, että $G = G_1 \oplus G_2 \oplus \cdots \oplus G_n$ ja $G_i \simeq H_i$, missä H_i on ryhmä ja $i \in I_n$. Tällöin on olemassa isomorfismit $f_i \colon G_i \to H_i$, kun $i \in I_n$. Lauseen 3.1 nojalla $g = g_1 + \cdots + g_n$, kun $g \in G$ ja $g_i \in G_i$. Asetetaan nyt $f \colon G \to H_1 \oplus H_2 \oplus \cdots H_n$, $f(g) = (f_1(g_1), \ldots, f_n(g_n))$. Selvästi f on kuvaus, sillä f_i on kuvaus jokaisella $i \in I_n$. Edelleen, koska f_i on bijektio, kun $i \in I_n$, niin myös f on bijektio.

Olkoot $a, b \in G$. Tällöin $a = a_1 + \cdots + a_n$ ja $b = b_1 + \cdots + b_n$, missä $a_i, b_i \in G_i$ jokaisella $i \in I_n$. Nyt koska G on Abelin ryhmä ja G_i sen aliryhmä, kun $i \in I_n$, niin $a + b = a_1 + \cdots + a_n + b_1 + \cdots + b_n = a_1 + b_1 + \cdots + b_n + a_n$. Täten, koska f_i on homomorfismi jokaisella $i \in I_n$, niin $f(a + b) = (f_1(a_1 + b_1), \ldots, f_n(a_n + b_n)) = (f_1(a_1) + f_1(b_1), \ldots, f_n(a_n) + f_n(b_n)) = (f_1(a_1), \ldots, f_n(a_n)) + (f_1(b_1), \ldots, f_n(b_n)) = f(a) + f(b)$. Näin ollen f on homomorfismi ja täten isomorfismi, joten $G \simeq H_1 \oplus H_2 \oplus \cdots \oplus H_n$. □

Aloitetaan äärellisten Abelin ryhmien luokittelu määrittelemällä ryhmän suoraan summaesitykseen liittyvä käsite.

Määritelmä 3.3. Olkoon G Abelin ryhmä ja A sen aliryhmä. Tällöin A on ryhmän G *suora summattava*, jos on olemassa ryhmän G sellainen aliryhmä B, että $G = A \oplus B$.

Seuraavassa lauseessa esitellään erilaisia äärellisen Abelin ryhmän G alkioista muodostettavia ryhmiä ja osoitetaan niille tiettyjä ominaisuuksia.

Lause 3.4. *(Vrt. [1, s. 248]) Olkoon G Abelin ryhmä. Olkoon lisäksi $r \in \mathbb{Z}$ ja p alkuluku.*

(i) *Olkoon $G[r] = \{ g \in G \mid rg = 0 \}$. Tällöin $G[r]$ on ryhmän G aliryhmä.*

(ii) *Olkoon $rG = \{ rg \mid g \in G \}$. Tällöin rG on ryhmän G aliryhmä.*

(iii) *Olkoon $G(p) = \{ g \in G \mid$ alkion g kertaluku on p^s missä $s \geq 0 \}$. Tällöin $G(p)$ on ryhmän G aliryhmä.*

(iv) $G/G[r] \simeq rG$.

Todistus. (i), (ii) ja (iv) Asetetaan $f\colon G \to G$, $f(x) = rx$. Nyt, koska G on Abelin ryhmä, niin $f(x+y) = r(x+y) = rx+ry = f(x)+f(y)$, joten f on homomorfismi. Täten ensimmäisen isomorfialauseen nojalla $f(G) = \{\, rg \mid g \in G \,\} = rG$ on ryhmän G aliryhmä. Edelleen, koska $\operatorname{Ker} f = \{\, g \in G \mid f(g) = rg = 0 \,\} = G[r]$ ja $G[r]$ on ryhmän G aliryhmä, niin ensimmäisen isomorfialauseen nojalla $G/G[r] \simeq rG$.

(iii) Koska $\circ(0) = 1 = p^0$, niin $0 \in G(p)$. Siis $G(p)$ on epätyhjä. Olkoot $a, b \in G(p)$. Tällöin $p^k a = 0$ ja $p^l b = 0$ joillakin $k \geq 0$ ja $l \geq 0$. Nyt, koska G on Abelin ryhmä, niin $p^{k+l}(a+(-b)) = p^{k+l}a+p^{k+l}b = p^l p^k a+p^k p^l b = p^l 0+p^k 0 = 0$, joten $(a+(-b)) \in G(p)$. Siis $G(p)$ on ryhmän G aliryhmä. □

Seuraavaksi asetetaan ensin lauseessa 3.4 esiintyvälle ryhmälle $G(p)$ nimi. Tämän jälkeen esitetään ja todistetaan lause liittyen äärellisen Abelin ryhmän esitykseen suorana summana.

Määritelmä 3.5. Lauseen 3.4 mukainen aliryhmä $G(p)$ on ryhmän G *p-primäärikomponentti*.

Lause 3.6. *Olkoon G äärellinen Abelin ryhmä, jonka kertaluku on p^l, missä l on positiivinen kokonaisluku ja p on alkuluku. Olkoon $a \in G$ sellainen, että sen kertaluku $\circ(a) = p^k$ on maksimaalinen ryhmässä G eli $\circ(a) \geq \circ(b)$ jokaisella $b \in G$. Tällöin $\langle a \rangle$ on ryhmän G suora summattava. Toisin sanoen on olemassa sellainen ryhmän G aliryhmä B, että $G = \langle a \rangle \oplus B$.*

Todistus. (Vrt. [1, ss. 248–249]) Olkoon $0 \neq x \in G$. Koska $|G| = p^l$, niin seurauksen 2.13 nojalla $\circ(x) = p^t$ jollakin positiivisella kokonaisluvulla t. Koska alkion a kertaluku p^k on maksimaalinen ryhmässä G, niin $\circ(a) \geq \circ(x)$, joten $t \leq k$. Täten $p^k x = 0$ jokaisella $x \in G$. Asetetaan

$$C = \{\, B \mid B \text{ on ryhmän } G \text{ aliryhmä ja } \langle a \rangle \cap B = \{0\} \,\}.$$

Nyt, koska $\langle a \rangle \cap \{0\} = \{0\}$, niin $\{0\} \in C$, joten C on epätyhjä. Koska G on äärellinen ryhmä, niin sillä on äärellisesti aliryhmiä, joten C sisältää äärellisen määrän ryhmän G aliryhmiä. Joukolla C on siis maksimaalinen alkio ryhmän kertaluvun suhteen. Merkitään tätä maksimaalista alkiota kirjaimella B. Näytetään nyt, että $G = \langle a \rangle \oplus B$.

Tehdään vastaoletus, että on olemassa sellainen $g \in G$, että $g \notin \langle a \rangle \oplus B$. Koska $p^k g = 0 \in \langle a \rangle \oplus B$, niin on olemassa sellainen positiivinen kokonaisluku s, että $p^s g \in \langle a \rangle \oplus B$. Olkoon n pienin sellainen positiivinen kokonaisluku, että $p^n g \in \langle a \rangle \oplus B$, joten $p^n g \in \langle a \rangle \oplus B$ mutta $p^{n-1} g \notin \langle a \rangle \oplus B$. Merkitään $d = p^{n-1} g$,

jolloin $d \notin \langle a \rangle \oplus B$ ja $pd \in \langle a \rangle \oplus B$. Nyt suoran summan nojalla $pd = ta + b$ jollakin kokonaisluvulla t ja ryhmän B alkiolla b. Täten, koska G on Abelin ryhmä, niin $0 = p^{k-1}pd = p^{k-1}ta + p^{k-1}b$. Näin ollen $p^{k-1}ta = -p^{k-1}b \in \langle a \rangle \cap B$, sillä $p^{k-1}ta \in \langle a \rangle$ eli $-p^{k-1}b \in \langle a \rangle$ ja samoin $-p^{k-1}b \in B$ eli $p^{k-1}ta \in B$. Edelleen, koska $\langle a \rangle \cap B = \{0\}$, niin $-p^{k-1}b = 0$. Tällöin alkion a kertaluvun $\circ(a) = p^k$ täytyy jakaa $p^{k-1}t$ ja täten $p \mid t$. Olkoot $t = pr$ ja $a' = ra \in \langle a \rangle$. Nyt $pd = pa' + b$ ja koska G on Abelin ryhmä, niin $p(d - a') = b \in B$. Merkitään $x = d - a'$. Tällöin $x = d - a' = d - ra \notin B$, sillä $ra \in \langle a \rangle$. Tämän nojalla $\langle a \rangle \cap \langle B, x \rangle \neq \{0\}$. Täten on olemassa sellaiset $m, s \in \mathbb{Z}$ ja $b_1 \in B$, että $0 \neq ma = b_1 + sx \in \langle a \rangle \cap \langle B, x \rangle$. Jos $\operatorname{syt}(p, s) \neq 1$, niin $s = pq$ jollakin $q \in \mathbb{Z}$. Koska $px \in B$, niin $ma = b_1 + q(px) \in B$, missä on ristiriita, sillä $0 \neq ma \in \langle a \rangle$, $0 \neq ma \in B$ ja $\langle a \rangle \cap B = \{0\}$. Tämän nojalla $\operatorname{syt}(p, s) = 1$. Täten on olemassa sellaiset $u, v \in \mathbb{Z}$, että $1 = us + vp$. Tällöin $x = u(sx) + v(px) = u(ma - b_1) + v(px) = uma + (-ub_1 + v(px)) \in \langle a \rangle \oplus B$. Siis $d - a' = x \in \langle a \rangle \oplus B$. Tällöin $d = d - a' + a' \in \langle a \rangle \oplus B$, missä on ristiriita, sillä $d \notin \langle a \rangle \oplus B$, joten vastaoletus on väärä ja $G = \langle a \rangle \oplus B$. □

Alkuluvullisen tai alkulukujen tulon omaavan kertaluvun Abelin ryhmät eli Abelin p-ryhmät ovat isossa roolissa äärellisten Abelin ryhmien luokittelussa. Seuraavassa lauseessa osoitetaan, että määritelmän 2.16 mukainen ryhmä rajoitettuna Abelin ryhmiin voidaan ilmaista syklisten p-ryhmien suorana summana.

Lause 3.7. *Olkoon p alkuluku ja G äärellinen Abelin p-ryhmä. Tällöin ryhmä G on syklisten p-ryhmien suora summa. Edelleen, jos $G = G_1 \oplus G_2 \oplus \cdots \oplus G_r = H_1 \oplus H_2 \oplus \cdots \oplus H_s$, missä G_i ja H_j ovat syklisiä p-ryhmiä sekä $|G_1| \geq |G_2| \geq \cdots \geq |G_r| > 1$ ja $|H_1| \geq |H_2| \geq \cdots \geq |H_r| > 1$, niin $r = s$ ja $G_i \simeq H_i$, kun $1 \leq i \leq r$.*

Todistus. (Vrt. [1, ss. 249–250]) Olkoon G sellainen äärellinen Abelin p-ryhmä, että $|G| = p^n$. Todistetaan väite, että ryhmä G on syklisten p-ryhmien suora summa, induktiolla luvun n suhteen. Jos $n = 1$, niin G on ryhmä, jonka kertaluku on p. Tällöin lauseen 2.15 nojalla on olemassa sellainen $a \in G$, että $\circ(a) = p$. Koska $\circ(a) = p$, niin a generoi ryhmän G, joten $G = \langle a \rangle$ ja ryhmä on syklinen p-ryhmä. Edelleen, koska $\{0\}$ on syklinen p-ryhmä, niin $G = \langle a \rangle \oplus \{0\}$. Siis G on syklisten p-ryhmien suora summa, kun $n = 1$.

Oletetaan sitten, että väite pätee kaikilla p-ryhmillä, joiden kertaluku on pienempi kuin $|G|$. Olkoon $a \in G$ sellainen, että $\circ(a)$ on maksimaalinen ryhmässä G. Tällöin lauseen 3.6 nojalla on olemassa sellainen ryhmän G aliryhmä B, että $G = \langle a \rangle \oplus B$. Nyt B on p-ryhmä, koska $B \subseteq G$, ja $|B| < |G|$. Täten induktio-oletuksen nojalla

B on syklisten p-ryhmien suora summa, joten edelleen G on syklisten p-ryhmien suora summa.

Todistetaan nyt suoran summaesityksen yksikäsitteisyys. Oletetaan, että $G = G_1 \oplus G_2 \oplus \cdots \oplus G_r = H_1 \oplus H_2 \oplus \cdots \oplus H_s$. Lauseen 3.4 nojalla $G[p]$ on ryhmän G aliryhmä ja $G_i[p]$ on ryhmän G_i aliryhmä. Olkoon $a \in G[p]$. Tällöin a voidaan esittää muodossa $a = a_1 + a_2 + \cdots + a_r$ joillakin $a_i \in G_i$, missä $1 \leq i \leq r$. Edelleen lauseen 3.4 nojalla $pa = 0$, joten koska G on Abelin ryhmä, niin $pa_1 + pa_2 + \cdots + pa_r = pa = 0$. Täten $pa_i = 0$ jokaisella $1 \leq i \leq r$, joten $a_i \in G_i[p]$ jokaisella $1 \leq i \leq r$ eli $G[p] = G_1[p] + G_2[p] + \cdots + G_r[p]$ ja $G_i[p] \cap (G_1[p]G_2[p] \cdots G_{i-1}[p]G_{i+1}[p] \cdots G_r[p]) = \{0\}$, koska $G_i \cap (G_1 G_2 \cdots G_{i-1} G_{i+1} \cdots G_r) = \{0\}$. Täten lauseen 3.1 nojalla $G[p] = G_1[p] \oplus G_2[p] \oplus \cdots \oplus G_r[p]$. Koska $G_i[p] \subseteq G_i$ ja G_i on syklinen p-ryhmä, niin $G_i[p]$ on syklinen p-ryhmä. Tällöin jokaisen ryhmän $G_i[p]$ alkion, neutraalialkiota lukuunottamatta, kertaluku on p eli $|G_i[p]| = p$ jokaisella $1 \leq i \leq r$. Täten $|G[p]| = |G_1[p]||G_2[p]| \cdots |G_r[p]| = p^r$. Vastaavasti voidaan osoittaa, että $|G[p]| = p^s$, koska $G = H_1 \oplus H_2 \oplus \cdots \oplus H_s$. Täten $p^r = p^s$ eli $r = s$.

Koska saman kertaluvun omaavat sykliset ryhmät ovat isomorfisia, niin väitteen $G_i \simeq H_i$, kun $1 \leq i \leq r$, todistamiseksi riittää näyttää, että $|G_i| = |H_i|$, kun $1 \leq i \leq r$. Todistetaan tämä induktiolla luvun n suhteen. Jos $n = 1$, niin lauseen 3.6 nojalla $G_1 \oplus G_2 \oplus \cdots \oplus G_r = H_1 \oplus H_2 \oplus \cdots \oplus H_s = \langle a \rangle \oplus B$, joten selvästi väite pätee. Oletetaan, että väite pätee kaikille p-ryhmille, joiden kertaluku on pienempi kuin p^n, missä $n > 1$. Lauseen 3.4 nojalla $G_i/G_i[p] \simeq pG_i$. Koska G_i on syklinen ja $G_i[p] \subseteq G_i$, niin $G_i[p]$ on syklinen. Lisäksi jokainen ryhmän $G_i[p]$ alkio poislukien neutraalialkio on kertaluvultaan p eli $|G_i[p]| = p$. Täten Lagrangen lauseen nojalla $|pG_i| = |G_i/G_i[p]| = \frac{|G_i|}{|G_i[p]|} = \frac{|G_i|}{p} < |G_i|$. Ryhmän pG_i määrittelyn ja sen nojalla, että ryhmän pG_i kertaluku on aidosti pienempi kuin ryhmän G_i seuraa, että $pG_i = \{0\}$, jos ja vain jos $|G_i| = p$. Nyt, jos $pG_i = \{0\}$, niin $pG_l = \{0\}$, kun $i \leq l \leq r$. Täten $pG = pG_1 \oplus \cdots \oplus pG_m$, missä $m \leq r$ sekä $pG_i \neq \{0\}$, kun $1 \leq i \leq m$, ja $pG_l = \{0\}$, kun $m + 1 \leq l \leq r$. Täysin vastaavasti voidaan näyttää, että $pG = pH_1 \oplus \cdots \oplus pH_t$, missä $t \leq r$, $pH_l \neq \{0\}$, kun $1 \leq l \leq t$, ja $pH_l = \{0\}$, kun $t + 1 \leq l \leq r$. Koska $|pG| < |G|$, niin induktio-oletuksen nojalla $m = t$ ja $|pG_i| = |pH_i|$, kun $1 \leq l \leq m$. Täten $|G_i| = |H_i|$, kun $1 \leq l \leq m$. Koska $|G_i| = p = |H_i|$, kun $m + 1 \leq i \leq r$, niin $|G_i| = |H_i|$, kun $1 \leq l \leq r$. □

Seuraavaa tämän pykälän päätulosta kutsutaan *äärellisten Abelin ryhmien peruslauseeksi*. Lauseessa osoitetaan, että jokainen äärellinen Abelin ryhmä voidaan esit-

tää yksikäsitteisesti syklisten p-ryhmien suorana summana. Lauseen nojalla saadaan siis luokiteltua kaikki äärelliset Abelin ryhmät yksikäsitteisesti.

Lause 3.8. *Olkoon G äärellinen Abelin ryhmä. Tällöin G on syklisten p-ryhmien suora summa. Edelleen, mitkä tahansa kaksi ryhmän G hajotelmaa epätriviaalien syklisten p-ryhmien suorana summana ovat samat summattavien järjestystä lukuun ottamatta.*

Todistus. (Vrt. [1, ss. 251–252]) Jos $|G| = 1$, niin G on triviaali ryhmä ja täten syklisten p-ryhmien, tässä tapauksessa triviaalien ryhmien, suora summa. Oletetaan nyt, että $|G| > 1$. Olkoon $|G| = p_1^{n_1} p_2^{n_2} \cdots p_l^{n_l}$ aritmetiikan peruslauseen mukainen, missä luvut p_i ovat erisuuria alkulukuja ja luvut n_i positiivisia kokonaislukuja. Lauseen 2.19 nojalla ryhmällä G on Sylowin p_i-aliryhmä G_i, kun $1 \leq i \leq l$. Koska G on Abelin ryhmä, niin lauseen 2.11 nojalla ryhmä G_i on ryhmän G normaali aliryhmä ja täten lauseen 2.20 nojalla yksikäsitteinen, kun $1 \leq i \leq l$.

Nyt $|G_i| = p_i^{n_i}$, kun $1 \leq i \leq l$, joten $G_i \cap G_j = \{0\}$, kun $i \neq j$. Näytetään, että

$$G_i \cap (G_1 + G_2 + \cdots + G_{i-1} + G_{i+1} + \cdots + G_l) = \{0\},$$

kun $1 \leq i \leq l$. Oletetaan, että $a \in G_i \cap (G_1 + G_2 + \cdots + G_{i-1} + G_{i+1} + \cdots + G_l)$. Tällöin $a \in G_i$ ja $a \in G_1 + G_2 + \cdots + G_{i-1} + G_{i+1} + \cdots + G_l$. Täten

$$a = a_1 + \cdots + a_{i-1} + a_{i+1} + \cdots + a_l,$$

missä $a_j \in G_j$. Nyt Lagrangen lauseen nojalla jokaisella $j \neq i$ pätee, että $\circ(a_j) = p^{r_j}$ jollakin eksponentin r_j arvolla, missä $0 \leq r_j \leq n_j$. Olkoon

$$r = p_1^{r_1} \cdots p_{i-1}^{r_{i-1}} p_{i+1}^{r_{i+1}} \cdots p_l^{r_l},$$

jolloin $ra = 0$, sillä G on Abelin ryhmä ja G_i sen aliryhmä, kun $1 \leq i \leq l$. Täten $\circ(a)$ jakaa luvun r, ja koska $a \in G_i$, niin $\circ(a)$ jakaa luvun $p_i^{n_i}$. Mutta koska $p_i^{n_i}$ ei esiinny luvun r alkulukutekijähajotelmassa, niin $p_i^{n_i}$ ja r ovat keskenään jaottomia. Täten on oltava $\circ(a) = 1$, joten $a = 0$. Siis

$$G_i \cap (G_1 + G_2 + \cdots + G_{i-1} + G_{i+1} + \cdots + G_l) = \{0\},$$

mistä seuraa, että

$$|G_1 + \cdots + G_l| = |G_1| \cdots |G_l| = p_1^{n_1} p_2^{n_2} \cdots p_l^{n_l} = |G|.$$

Täten lauseen 3.1 nojalla

$$G = G_1 \oplus G_2 \oplus \cdots \oplus G_l.$$

Koska jokainen G_i on Abelin p-ryhmä, niin lauseen 3.7 nojalla jokainen G_i on syklisten p-ryhmien suora summa. Täten, koska $G = G_1 \oplus G_2 \oplus \cdots \oplus G_l$, niin G on syklisten p-ryhmien suora summa. Lauseen ensimmäinen osa on siis todistettu.

Todistetaan nyt hajotelmien eli suorien summattavien yksikäsitteisyys induktiolla luvun $|G|$ alkulukutekijähajotelman erisuurten alkulukujen määrän l suhteen. Jos $l = 1$, niin G on Abelin p-ryhmä ja suorien summattavien yksikäsitteisyys pätee lauseen 3.7 nojalla. Tehdään induktio-oletus, että suorien summattavien yksikäsitteisyys pätee kaikilla epätriviaaleilla äärellisillä Abelin ryhmillä H, joiden kertaluvun $|H|$ alkulukutekijähajotelmissa on vähemmän erisuuria alkulukuja kuin l.

Olkoot

$$G = G_1 \oplus G_2 \oplus \cdots \oplus G_r$$

ja

$$G = H_1 \oplus H_2 \oplus \cdots \oplus H_t$$

kaksi ryhmän G hajotelmaa suoriksi summiksi epätriviaaleja syklisiä p-ryhmiä. Abelin ryhmille A ja B pätee, että $A \oplus B \simeq B \oplus A$. Täten voidaan olettaa, että tarvittaessa uudelleenjärjestelemällä suorat summattavat $G_1, G_2, \ldots, G_m$, missä $m \leq r$, ja suorat summattavat $H_1, H_2, \ldots, H_s$, missä $s \leq t$, ovat alkulukua p_1 vastaavat sykliset p-ryhmät. Samoin voidaan olettaa, että tarvittaessa uudelleenjärjestelemällä ryhmät $G_{m+1}, \ldots, G_r$ ja $H_{s+1}, \ldots, H_t$ ovat alkulukuja p, missä $p \neq p_1$, vastaavia syklisiä p-ryhmiä. Edelleen voidaan olettaa, että tarvittaessa uudelleenjärjestelemällä suorat summattavat, pätee $|G_1| \geq |G_2| \geq \cdots \geq |G_m|$ ja $|H_1| \geq |H_2| \geq \cdots \geq |H_s|$. Olkoot $A = G_1 \oplus G_2 \oplus \cdots \oplus G_m$, $B = H_1 \oplus H_2 \oplus \cdots \oplus H_s$, $C = G_{m+1} \oplus \cdots \oplus G_r$ ja $D = H_{s+1} \oplus \cdots \oplus H_t$. Tällöin

$$G = A \oplus C = B \oplus D.$$

Osoitetaan nyt, että $A = B$. Ensimmäiseksi huomioidaan, että edellä mainitun oletuksen mukaisesti ja siksi, että kyseessä on p-ryhmiä, jokaisen ryhmän A neutraalialkiosta poikkeavan alkion kertaluku on keskenään jaoton jokaisen ryhmän C neutraalialkiosta poikkeavan alkion kertaluvun kanssa. Samoin jokaisen ryhmän B neutraalialkiosta poikkeavan alkion kertaluku on keskenään jaoton jokaisen ryhmän D neutraalialkiosta poikkeavan alkion kertaluvun kanssa.

Osoitetaan nyt, että $A \subseteq B$. Olkoon $a \in A$ sellainen alkio, että $a \neq 0$. Tällöin $a \in G = B \oplus D$, joten $a = b + d$ joillakin $b \in B$ ja $d \in D$. Osoitetaan, että $a = b$. Tehdään vastaoletus, että $a - b \neq 0$. Tällöin alkion $a - b$ kertaluku on jokin luvun p_1 positiivinen monikerta, kun taas alkion d kertaluku eroaa jokaisesta luvun p_1 positiivisesta monikerrasta. Tämä on ristiriitaista, sillä $a - b = d$, joten vastaoletus on väärä eli $a - b = 0$ ja täten $a = b \in B$. Siis $A \subseteq B$.

Vastavaasti voidaan osoittaa, että $B \subseteq A$, joten $A = B$. Edelleen vastaavasti voidaan osoittaa, että $C = D$. Nyt $A = B$ on p-ryhmä ja täten lauseen 3.7 nojalla $m = s$ ja $G_i \simeq H_i$ jokaisella $1 \leq i \leq m$. Lisäksi $C = D$ on Abelin ryhmä, jonka kertaluku on $p_2^{n_2} \cdots p_l^{n_l}$. Induktio-oletuksen nojalla ryhmän $C = D$ hajotelmat $G_{m+1} \oplus \cdots \oplus G_r$ ja $H_{s+1} \oplus \cdots \oplus H_t$ ovat samat summattavien järjestystä lukuun ottamatta. Täten ryhmän G molemmat hajotelmat $G_1 \oplus G_2 \oplus \cdots \oplus G_r = A \oplus C$ ja $H_1 \oplus H_2 \oplus \cdots \oplus H_t = B \oplus D$ ovat samat summattavien järjestystä lukuun ottamatta. □

3.2 Äärellisten Abelin ryhmien ominaisuuksia

Lauseesta 3.8 seuraa, että jokaista äärellistä epätriviaalia Abelin ryhmää vastaa positiiviset kokonaisluvut $p_1^{n_1}, p_2^{n_2}, \ldots, p_k^{n_k}$, jotka ovat yksikäsitteisiä järjestystä lukuun ottamatta. Luvut $p_1, p_2, \ldots, p_k$ ovat alkulukuja, mutta eivät välttämättä erisuuria, ja $n_1, n_2, \ldots, n_k$ ovat positiivisia kokonaislukuja. Lisäksi lauseiden 2.7 ja 3.2 nojalla saadaan nyt äärelliselle Abelin ryhmälle G, että

$$G \simeq \mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}.$$

Lukuja $p_1^{n_1}, p_2^{n_2}, \ldots, p_k^{n_k}$ sanotaan ryhmän G *alkeellisiksi jakajiksi*. [1]

Käytetään nyt edellisessä pykälässä osoitettua äärellisten Abelin ryhmien peruslausetta äärellisten Abelin ryhmien ominaisuuksien todistamiseen. Seuraava tulos voitaisiin osoittaa myös käyttämällä Cauchyn lausetta 2.15, mutta tässä esitetään todistus nojaten lauseeseen 3.8.

Seuraus 3.9. *Olkoon G äärellinen Abelin ryhmä, jonka kertaluku on n, ja olkoon m luvun n positiivinen jakaja. Tällöin ryhmällä G on aliryhmä, jonka kertaluku on m.*

Todistus. (Vrt. [1, s. 253]) Jos $n = 1$, niin myös $m = 1$ ja $\{0\}$ on ryhmän G aliryhmä, jonka kertaluku on m. Oletetaan täten, että $n > 1$. Lauseen 3.8 ja pykälän alussa esitetyn lauseen seurauksen nojalla on olemassa sellaiset alkuluvut $p_1, p_2, \ldots, p_k$ ja sellaiset positiiviset kokonaisluvut $n_1, n_2, \ldots, n_k$, että $G \simeq \mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}$.

Tällöin $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$. Koska $m \mid n$, niin on olemassa sellaiset kokonaisluvut $0 \leq m_i \leq n_i$, missä $1 \leq i \leq k$, että $m = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$. Edelleen, koska $p_1^{m_1} \mid p_1^{n_1}$ jokaisella $1 \leq i \leq k$, niin lauseen 2.9 nojalla ryhmällä $\mathbb{Z}_{p_i^{n_i}}$ on yksikäsitteinen aliryhmä G_i, jonka kertaluku on $p_i^{m_i}$, kun $1 \leq i \leq k$. Täten voidaan osoittaa kuten lauseen 3.8 todistuksessa, että $G_1 + G_2 + \cdots + G_k = G_1 \oplus G_2 \oplus \cdots \oplus G_k$. Lisäksi $G_1 \oplus G_2 \oplus \cdots \oplus G_k$ on ryhmän $\mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}$ aliryhmä, jonka kertaluku on $p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k} = m$. Siis ryhmällä G on aliryhmä, jonka kertaluku on m. □

Osoitetaan sitten, että äärelliset Abelin ryhmät ovat p-primäärikomponenttiensa suoria summia. Tämän jälkeen käytetään tulosta esimerkissä, jossa tarkastellaan äärellisiä syklisiä ryhmiä.

Lause 3.10. *Olkoon G äärellinen Abelin ryhmä. Tällöin G on määritelmän 3.5 mukaisten p-primäärikomponenttiensa suora summa.*

Todistus. (Vrt. [1, s. 253]) Olkoon $|G| = n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, missä alkuluvut p_i ovat erisuuria ja luvut n_i ovat epänegatiivisia kokonaislukuja. Kuten lauseen 3.8 todistuksessa, nyt ryhmällä G on Sylowin p_i-aliryhmä G_i, kun $1 \leq i \leq k$, jolle pätee $|G_i| = p_i^{n_i}$. Tästä seuraa, että $G_i \subseteq G(p_i)$, joten $|G(p_i)| \geq p_i^{n_i}$. Koska $G(p_i)$ on p_i-ryhmä, niin lauseen 2.17 nojalla $|G(p_i)| = p_i^t$ jollakin kokonaisluvulla t. Täten $t \geq n_i$. Osoitetaan, että $t = n_i$. Oletetaan, että $t > n_i$. Lauseen 2.12 nojalla luku $|G(p_i)|$ jakaa luvun $|G|$. Täten $p_i^t \mid p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, joten $p_i^{t-n_i} \mid p_1^{n_1} p_2^{n_2} \cdots p_{i-1}^{n_{i-q}} p_{i+1}^{n_{i+1}} \cdots p_k^{n_k}$, mikä on ristiriitaista, sillä alkuluvut p_i ovat erisuuria. Tällöin on oltava $t = n_i$. Täten $G_i = G(p_i)$, kun $1 \leq i \leq k$, sillä lauseen 2.20 nojalla Sylowin aliryhmät ovat nyt yksikäsitteisiä. Ryhmä G on siis p-primäärikomponenttiensa suora summa. □

Esimerkki 3.11. (Vrt. [1, s. 253]) Tarkastellaan syklistä ryhmää $\mathbb{Z}_n$. Aritmetiikan peruslauseen nojalla on olemassa alkuluvut $p_1, p_2, \ldots, p_k$ ja sellaiset positiiviset kokonaisluvut $n_1, n_2, \ldots, n_k$, että $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$. Alkuluvulle $p = p_i$ ryhmän $\mathbb{Z}_n$ p-primäärikomponentti on $\mathbb{Z}_{p_i^{n_i}}$, joten lauseiden 3.8, 3.2 ja 3.10 nojalla

$$\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}.$$

Kaikki äärelliset Abelin ryhmät on nyt lauseen 3.8 nojalla luokiteltu rakenteeltaan isomorfiaa vaille. Tarkastellaan vielä lopuksi peruslauseen myötä kaikkien ei-isomorfisten saman kertaluvun Abelin ryhmien määrittämistä. Määrittäminen aloitetaan määrittelemällä ei-isomorfiset ryhmät yksilöivä ominaisuus, minkä jälkeen esitetään ja todistetaan kaksi lausetta, joiden avulla pystytään määrittämään kaikki tietyn kertaluvun ei-isomorfiset äärelliset Abelin ryhmät.

Määritelmä 3.12. (Vrt. [1, s. 254]) Olkoon G äärellinen Abelin p-ryhmä, jonka kertaluku on p^n, missä $n > 0$. Olkoon $G = G_1 \oplus G_2 \oplus \cdots \oplus G_k$, missä jokainen G_i on syklinen ryhmä, jonka kertaluku on p^{n_i} ja $n_1 \geq n_2 \geq \cdots \geq n_k > 0$. Silloin kokonaislukuja $n_1, n_2, \ldots, n_k$ kutsutaan ryhmän G *invarianteiksi* ja k-monikkoa $(n_1, n_2, \ldots, n_k)$ kutsutaan ryhmän G *tyypiksi*.

Lause 3.13. *Kaksi Abelin p-ryhmää, joiden kertaluku on p^n, ovat isomorfiset, jos ja vain jos niillä on samat invariantit.*

Todistus. (Vrt. [1, s. 254]) Olkoot G ja H kaksi Abelin p-ryhmää, joiden kertaluku on p^n ja $n > 0$. Oletetaan, että ryhmillä G ja H on samat invariantit $n_1, n_2, \ldots, n_k$, missä $n_1 \geq n_2 \geq \cdots \geq n_k > 0$. Tällöin äärellisten Abelin ryhmien peruslauseen nojalla $G = G_1 \oplus G_2 \oplus \cdots \oplus G_k$, missä jokainen G_i, kun $1 \leq i \leq k$, on syklinen ryhmä, jonka kertaluku on p^{n_i}. Samoin $H = H_1 \oplus H_2 \oplus \cdots \oplus H_k$, missä jokainen H_i, kun $1 \leq i \leq k$, on syklinen ryhmä, jonka kertaluku on p^{n_i}. Koska saman kertaluvun omaavat sykliset ryhmät ovat isomorfisia, niin $G_i \simeq H_i$, missä $1 \leq i \leq k$. Täten lauseen 3.2 nojalla $G \simeq H$.

Oletetaan sitten, että $G \simeq H$. Olkoon $G = G_1 \oplus G_2 \oplus \cdots \oplus G_k$, missä jokainen G_i, kun $1 \leq i \leq k$, on syklinen ryhmä, jonka kertaluku on p^{n_i} sekä $n_1 \geq n_2 \geq \cdots \geq n_k > 0$. Olkoon samoin $H = H_1 \oplus H_2 \oplus \cdots \oplus H_t$, missä jokainen H_j, kun $1 \leq j \leq t$ on syklinen ryhmä, jonka kertaluku on p^{r_j} sekä $r_1 \geq r_2 \geq \cdots \geq r_t > 0$. Olkoon edelleen $f\colon G \to H$ ryhmien G ja H välinen isomorfismi.

Näytetään nyt nojaten isomorfismin $f^{-1}\colon H \to G$ ominaisuuksiin, että $f^{-1}(H_i)$ on ryhmän G syklinen aliryhmä, jonka kertaluku on p^{r_i}, kun $1 \leq i \leq t$. Koska H_i on ryhmän H aliryhmä, kun $1 \leq i \leq t$, niin $f^{-1}(H_i)$ on ryhmän G aliryhmä, kun $1 \leq i \leq t$. Nyt H_i on syklinen ryhmä, kun $1 \leq i \leq t$. Täten $H_i = \langle a \rangle$ jollakin $a \in H_i$. Olkoon nyt $b \in f^{-1}(H_i)$. Tällöin on olemassa sellainen $c \in H_i$, että $b = f^{-1}(c)$. Koska H_i on syklinen ryhmä, niin $c = na$ jollakin kokonaisluvulla n, joten $b = f^{-1}(c) = f^{-1}(na) = nf^{-1}(a)$. Näin ollen $f^{-1}(H_i)$ on ryhmän G syklinen aliryhmä.

Näytetään sitten, että $G = f^{-1}(H_1) \oplus f^{-1}(H_2) \oplus \cdots \oplus f^{-1}(H_t)$. Koska $f^{-1}(H_i)$ on ryhmän G aliryhmä, kun $1 \leq i \leq t$, niin $f^{-1}(H_1) + \cdots + f^{-1}(H_t) \subseteq G$. Olkoon sitten $a \in H$. Tällöin $f^{-1}(a) \in G$ ja a on muotoa $a_1 + \cdots + a_t$, missä $a_i \in H_i$, kun $1 \leq i \leq t$. Täten

$$f^{-1}(a) = f^{-1}(a_1) + \cdots + f^{-1}(a_t) \in f^{-1}(H_1) + \cdots + f^{-1}(H_t),$$

joten $G \subseteq f^{-1}(H_1) + \cdots + f^{-1}(H_t)$. Siis $G = f^{-1}(H_1) + \cdots + f^{-1}(H_t)$.

Olkoon vielä $a \in f^{-1}(H_i)$ ja $a \in f^{-1}(H_1) + \cdots + f^{-1}(H_{i-1}) + f^{-1}(H_{i+1}) + \cdots + f^{-1}(H_t)$. Tällöin

$$\begin{aligned} a = f^{-1}(a_i) &= f^{-1}(a_1) + \cdots + f^{-1}(a_{i-1}) + f^{-1}(a_{i+1}) + \cdots + f^{-1}(a_t) \\ &= f^{-1}(a_1 + \cdots + a_{i-1} + a_{i+1} + \cdots + a_t), \end{aligned}$$

joten $a_i = a_1 + \cdots + a_{i-1} + a_{i+1} + \cdots + a_t$ eli $0 = (-a_i) + a_1 + \cdots + a_{i-1} + a_{i+1} + \cdots + a_t$. Tällöin esityksen yksikäsitteisyyden perusteella $a_j = 0$, kun $1 \leq j \leq t$. Siis $a = 0$ ja $f^{-1}(H_1) \cap f^{-1}(H_1) + \cdots + f^{-1}(H_{i-1}) + f^{-1}(H_{i+1}) + \cdots + f^{-1}(H_t) = \{0\}$, kun $1 \leq i \leq t$, joten lauseen 3.1 nojalla $G = f^{-1}(H_1) \oplus f^{-1}(H_2) \oplus \cdots \oplus f^{-1}(H_t)$. Edelleen, koska $f^{-1}(H_i)$ on syklinen, kun $1 \leq i \leq t$, eli $f^{-1}(H_i) = \langle f^{-1}(a_i) \rangle$, niin $\circ(f^{-1}(H_i)) = \circ(f^{-1}(a_i)) = \circ(a_i) = p^{r_i}$. Nyt lauseen 3.7 nojalla $t = k$ ja $p^{r_i} = |f^{-1}(H_i)| = p^{n_i}$, missä $1 \leq i \leq k$. Näin ollen ryhmillä G ja H on samat invariantit. □

Määritelmä 3.14. (Vrt. [1, s. 254]) Olkoon n positiivinen kokonaisluku. Luvun n *ositus* on s-monikko $(n_1, n_2, \ldots, n_s)$, missä $n_1, n_2, \ldots, n_s$ ovat positiivisia kokonaislukuja, $n = n_1 + n_2 + \cdots + n_s$ ja $n_1 \geq n_2 \geq \cdots \geq n_s$.

Lause 3.15. *Olkoon G Abelin p-ryhmä, jonka kertaluku on p^n. Tällöin ei-isomorfisten Abelin p-ryhmien määrä, joiden kertaluku on p^n on yhtä suuri kuin luvun n ositusten määrä.*

Todistus. (Vrt. [1, s. 254]) Jokaisella Abelin p-ryhmällä G, jonka kertaluku on p^n, on yksikäsitteinen hajotelma $G = G_1 \oplus G_2 \oplus \cdots \oplus G_k$, missä jokainen G_i $(1 \leq i \leq k)$ on syklinen ryhmä, jonka kertaluku on p^{n_i}, missä $n_1 \geq n_2 \geq \cdots \geq n_k > 0$. Tällöin $n = n_1 + n_2 + \cdots + n_k$, joten $n_1, n_2, \ldots, n_k$ on luvun n ositus.

Olkoon nyt, että $n = n_1 + n_2 + \cdots + n_k$, missä $n_1 \geq n_2 \geq \cdots \geq n_k > 0$. Tällöin $G = \mathbb{Z}_{p^{n_1}} \oplus \mathbb{Z}_{p^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_k}}$ on Abelin p-ryhmä, jonka kertaluku on $p^{n_1+n_2+\cdots+n_k} = p^n$, ja ryhmän G invariantit ovat $n_1, n_2, \ldots, n_k$. Tällöin lauseen 3.13 nojalla ei-isomorfisten Abelin p-ryhmien määrä, joiden kertaluku on p^n on yhtä suuri kuin luvun n ositusten määrä. □

Ei-isomorfiset saman kertaluvun Abelin ryhmät voidaan siis määrittää tarkastelemalla ryhmän kertaluvun alkulukuhajotelman alkulukujen eksponenttien osituksia. Alla esitetään esimerkit kaikkien tietyn kertaluvun ei-isomorfisten Abelin ryhmien määrittämisestä tarkastelemalla osituksia.

Esimerkki 3.16. (Vrt. [1, s. 255]) Määritetään lauseen 3.15 avulla isomorfiaa vaille kaikki Abelin ryhmät, joiden kertaluku on 2^4. Nyt luvulle 4 saadaan ositukset 4, 3+1, 2+2, 2+1+1 ja 1+1+1+1. Täten ei-isomorfisiksi Abelin ryhmiksi, joiden kertaluku on 2^4, saadaan

$$\mathbb{Z}_{16},$$
$$\mathbb{Z}_8 \oplus \mathbb{Z}_2,$$
$$\mathbb{Z}_4 \oplus \mathbb{Z}_4,$$
$$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \text{ ja}$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

Esimerkki 3.17. (Vrt. [1, s. 256]) Määritetään vielä pykälässä luokiteltujen äärellisten Abelin ryhmien ominaisuuksien avulla isomorfiaa vaille kaikki Abelin ryhmät, joiden kertaluku on 360. Olkoon siis G Abelin ryhmä, jonka kertaluku on 360. Nyt $360 = 2^3 3^2 5$. Lauseen 2.19 nojalla ryhmällä G on Sylowin 2-aliryhmä $G(2)$, Sylowin 3-aliryhmä $G(3)$ ja Sylowin 5-aliryhmä $G(5)$. Koska G on Abelin ryhmä, niin $G(2)$, $G(3)$ ja $G(5)$ ovat ryhmän G normaaleja aliryhmiä ja täten yksikäsitteisiä. Tällöin $G(2) \cap G(3) = \{0\}$, $G(2) \cap G(5) = \{0\}$ ja $G(3) \cap G(5) = \{0\}$, joten $|G(2)+G(3)+G(5)| = |G(2)| \cdot |G(3)| \cdot |G(5)| = 8 \cdot 9 \cdot 5$. Täten $G = G(2)+G(3)+G(5)$ ja edelleen saadaan siis $G = G(2) \oplus G(3) \oplus G(5)$. Nyt $3 = 2+1 = 1+1+1$, joten luvulle 3 on kolme eri ositusta. Täten lauseen 3.15 nojalla ryhmää $G(2)$ vastaa kolme ei-isomorfista Abelin ryhmää, joiden kertaluku on 2^3. Tällöin

$$G(2) \simeq \mathbb{Z}_8 \text{ tai } G(2) \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_2 \text{ tai } G(2) \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

Samoin saadaan $2 = 1+1$, joten ryhmää $G(3)$ vastaa kaksi ei-isomorfista ryhmää. Saadaan siis

$$\text{joko } G(3) \simeq \mathbb{Z}_9 \text{ tai } G(3) \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_3.$$

Koska $|G(5)| = 5$, niin

$$G(5) \simeq \mathbb{Z}_5.$$

Täten ei-isomorfisiksi Abelin ryhmiksi, joiden kertaluku on $360 = 2^3 3^2 5$, saadaan

$$\mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5,$$
$$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5,$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5,$$
$$\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5,$$

$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$ ja

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$.

Lähteet

[1] Malik, D. S., Mordeson, J. N. & Sen, M. K. *Fundamentals of Abstract Algebra*. McGraw-Hill, 1997.

[2] Papantonopoulou, A. *Algebra: Pure & Applied*. Prentice Hall, 2002.

[3] Redfield, R. H. *Abstract Algebra: A Concrete Introduction*. Addison Wesley Longman Inc., 2001.