# Luku 5

# Äärellisviritteisistä Abelin ryhmistä

Palautetaan mieleen, että $R$-moduli $M$ on äärellisviritteinen, jos sillä on äärellinen virittäjä joukko eli alkiot $m_1, \ldots, m_k \in M$ siten, että $M = \mathrm{Span}(m_, \ldots, m_k)$. Kun $R = K$ on kunta, äärellisviritteiset $R$-modulit (eli $K$-vektoriavaruudet) on helppoa luokitella ainakin isomorfiaa vaille - ne ovat tällöin vapaat ja äärellisulotteiset. Jokaisella äärelliviritteisellä $K$-vektoriavaruudella on hyvinmääritelty dimensio $\dim K \in \mathbb{N}$ ja kaksi tällaista vektoriavaruutta ovat isomorfisia jos ja vain jos niillä on sama dimensio. Dimensio on siis *invariantti* joka *luokittele* äärellisviritteiset vektoriavaruudet isomorfiaa vaille täydellisesti.

Kun $R$ ei ole kunta asiat ovat tunnetusti paljon monimutkaisempia. Kuntien jälkeen "yksinkertaisin" rengas on kokonaislukujen rengas $\mathbb{Z}$, joten tässä osiossa tutkimme äärellisviritteisiä $\mathbb{Z}$-moduleita, eli siis äärellisviritteisiä Abelin ryhmiä. Kaikki tässä luvussa tarkasteltavat tulokset ovat (ainakin sopivasti yleistettynä ja tulkittuna) voimassa itse asiassa myös kun $R$ on niin sanottu *pääideaalirengas* eli sellainen vaihdannainen rengas, jonka jokainen ideaali on yhden alkion virittämä. $\mathbb{Z}$ on pääideaalirengas. Toinen tuttu meille esimerkki pääideaalirenkaasta, joka ei ole kunta, on polynomirengas $K[X]$, missä $K$ on kunta. Olisimme periaatteessa voineet tutkia yleisesti äärellisviritteisiä moduleita pääideaalirenkaan yli, mutta sen sijaan pidäytymme tärkeässätapauksessa $R = \mathbb{Z}$, jolloin todistuksetkin ovat paljon konkrettisimpia ja helpommin ymmärrettäviä.

Yksinkertaisin epätriviaali virittäjäjoukko sisältää yhden alkion, joten aloitetaan yhden alkion virittämistä Abelin ryhmistä. Tällaisia ryhmiä sanotaan *syklisiksi*. Olkoon $A$ syklinen ryhmä ja olkoon $x$ sen virittäjä. Määritel-

lään kuvauksen $f\colon \mathbb{Z} \to Z$ kaavalla $f(n) = nx$. Helposti nähdään, että tämä kuvaus on ryhmien välinen homomorfismi. Lisäksi, koska $x$ virittää $A$:n, se on tässä tapauksessa surjektiivinen. $f$:n ydin on jokin $\mathbb{Z}$:n aliryhmä, eli muotoa $m\mathbb{Z}$ jollakin $m \in \mathbb{N}$. Isomorfialauseesta seuraa nyt, että $A \cong \mathbb{Z}/mZ = \mathbb{Z}_m$. Näin olleen jokainen syklinen ryhmä on isomorfinen $\mathbb{Z}_m$:n kanssa jollakin $m \in \mathbb{N}$. Kun $m = 0$, $A$ on ääretön ja isomorfinen $\mathbb{Z}$:n kanssa. Kun $m > 0$, $A$:ssä on tasan $m$ alkiota.

Yleisemmin olkoon $A$ jokin Abelin ryhmä ja olkoon $a \in A$. Tällöin aliryhmä $A' = \mathrm{Span}(a)$ on syklinen ryhmä. Merkitsemme myös $A' = \mathbb{Z}[a]$. Tämä merkintä on luonnollinen, sillä

$$A' = \{na \mid n \in \mathbb{Z}\}.$$

Yllä olevan mukaan on olemassa kaksi mahdollisuutta. Jos $A'$ on ääretön, se on isomorfinen $\mathbb{Z}$:n kanssa. Tällöin kaikilla $n \in \mathbb{Z}, \neq 0$ myös $na \neq 0$. Sanomme tällöin, että $a$:n *kertaluku* on ääretön.

Toinen mahdollisuus on, että $A'$ on äärellinen joten ylläolevan mukaan isomorfinen $\mathbb{Z}_m$:n kanssa jollakin $m > 0$. Lisäksi on olemassa isomorfismi $\mathbb{Z} - m \to A'$, jolle $f(\bar{1}) = a$. Tällöin $A'$:ssä $ma = 0$, mutta alkiot $a, 2a, \ldots, (m-1)a$ eroavat nolla-alkiosta. Sanomme tässä tapauksessa kokonaisluku $m$ alkion $a$ *kertaluvuksi*. Tässä tapauksessa kertaluku on siis pienin positiivinen kokonaisluku $n$ jolle $na = 0$.

**Lemma 5.1.** *Olkoon $b \neq 0$ syklisen äärellisen ryhmän $\mathbb{Z}_m$ alkio, $m \geq 1$. Olkoon $n$ sen kertaluku. Tällöin*
*(i) $n$ on äärellinen ja on $m$:n tekijä.*
*(ii) Olkoon $k \in \mathbb{N}$. Tällöin $kb = 0$ jos ja vain jos $k = qn$ jollakin $q \in \mathbb{Z}$ eli jos ja vain jos $k$ on jaollinen $n$:llä.*

*Todistus.* (i) Olkoon $b \neq 0$ syklisen äärellisen ryhmän $\mathbb{Z}_m$ alkio. Tällöin $mb = 0$ (tämähän pätee kaikille $\mathbb{Z}_m$:n alkioille. Olkoon $n$ $b$:n kertaluku Abelin ryhmässä $\mathbb{Z}_m$. Osoitetaan, että $n$ on $m$:n tekijä. Nimittäin jakoyhtälön nojalla $m = qn + r$, missä $0 \leq r < n$. Nyt

$$rb = (m - qn)b = mb - q(nb) = 0 - 0 = 0.$$

Koska $n$ on minimaalinen positiivinen kokonaisluku jolle $nb = 0$ ja $0 \leq r < n$, tästä seuraa, että pakosti $r = 0$. Siis $m = qn$ ja $n$ on $m$:n tekijä.

(ii) Kuvaus $\mathbb{Z}_n \to \mathbb{Z}[b]$, $\bar{k} \to kb$ on isomorfismi. Koska $\mathbb{Z}_n$:ssä $\bar{k} = 0$ jos ja vai jos $k$ on jaollinen $n$:llä, (ii) seuraa. □

Yllä löydettiin jo kokonainen perhe erilaisia äärellivirittеisiä Abelin ryhmiä, nimittäin sykliset ryhmät $\mathbb{Z}_m$. Äärellinen suora summa äärellisvirittеistä ryhmistä on selvästi äärellisvirittеinen, joten jokainen muotoa

$$\mathbb{Z}^n \oplus \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \ldots \oplus \mathbb{Z}_{m_k} \tag{5.2}$$

oleva ryhmä on äärellisvirittеinen. Tässä luvussa todistamme käänteisen väitteen - jokainen äärellisvirittеinen Abelin ryhmä on isomorfiaa vaille muotoa 5.2 eli äärellinen suora summa syklisistä ryhmistä.
Tällainen esitys ei ole yksikäsitteinen. Esimerkiksi voidaan näyttää, että $\mathbb{Z}_2 \oplus \mathbb{Z}_{15} \cong \mathbb{Z}_{30} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_{10}$. Tämä on suora sovellus Lemmasta 5.7, jonka todistamme myöhemmin.
Jos esityksessä 5.2 kuitenkin vaaditaan, että $m_1|m_2|\ldots|m_{k-1}|m_k$, niin siitä tulee yksikäsitteinen. Tässä merkintä $p|q$ tarkoittaa, että $p$ on $q$:n tekijä eli $q$ on jaollinen $p$:llä.
Voimassa on siis seuraava äärellisvirittеisten Abelin ryhmien struktuurilause.

**Lause 5.3.** *Olkoon $A$ äärellisvirittеinen Abelin ryhmä. Tällöin on olemassa tasan yksi kokoelma luonnollisia lukuja $n, k \in \mathbb{N}$, $m_1, \ldots, m_k$, siten että $m_i > 1$ kaikilla $i = 1, \ldots, k$, $m_1|m_2|\ldots|m_{k-1}|m_k$ ja*

$$A \cong \mathbb{Z}^n \oplus \mathbb{Z}_{m_1} \oplus \ldots \mathbb{Z}_{m_k}. \tag{5.4}$$

Lauseen todistus on pitkä ja sisältää lukuisia yksityiskohtia. Osoitetaan ensin hajotelman (5.4) olemassaolo. Ennen sitä takastellaan kuitenkin vapaita äärellisulotteisia ryhmiä ja todistetaan niille väiteittä, joiden vastineet äärellisulotteisille vektoriavaruuksille olemme osoittaneet todeksi jo Luvussa 2.

**Lemma 5.5.** *Olkoot $n, m \in \mathbb{N}$. Jos $\mathbb{Z}^n \cong \mathbb{Z}^m$, niin $n = m$. Erityisesti vapaan äärellisulotteisen Abelin ryhmän dimensio on hyvinmääritelty.*

*Todistus.* Yksi tapa olisi käyttää $\mathbb{Z}$:n upotusta rationaalilukujen kuntaan $\mathbb{Q}$, jolle väite tiedetään olevan tosi vektoriavaruuksien teoriasta.
Jos $\mathbb{Z}^n \cong \mathbb{Z}^m$, niin on olemassa $(m \times n)$-kokoinen matriisi $A$ joka on kääntyvä $\mathbb{Z}$-kertoimisena matriisina - otetaan sellaiseksi isomorfismin $\mathbb{Z}^n \cong \mathbb{Z}^m$ matriisi. Tämä tarkoittaa siis sitä, että on olemassa $\mathbb{Z}$-kertoiminen $(n \times m)$-kokoinen matriisi $B$ jolle $AB = I_m, BA = I_n$. Mutta tällöin samanlaiset ominaisuudet pätevät $A$:lle ja $B$:lle jos ne oletetaan $\mathbb{Q}$-kertoimisina matriisina. Tällöin kuitenkin on pakko olla $m = n$, sillä $\mathbb{Q}$ on kunta (ja $A$ määrittelee tällöin isomorfismin $\mathbb{Q}^n \to \mathbb{Q}^m$).
Toinen hauska tapa on huomata, että jos $\mathbb{Z}^n = A = \mathbb{Z}^m$, niin $2\mathbb{Z}_n = 2A = 2\mathbb{Z}_m$, mistä seuraa, että

$$\mathbb{Z}_2^n = (\mathbb{Z}_n)/(2\mathbb{Z}_n) = A/2A = (\mathbb{Z}_m)/(2\mathbb{Z}_m) = \mathbb{Z}_2^m.$$

Ryhmässä vasemmalla on $2^n$ alkiota ja ryhmässä oikealla $2^m$ alkiota. Näin ollen $n = m$. □

Seuraava tulos on Proposition 2.18 paras mahdollinen yleistys $\mathbb{Z}$-modulille.

**Propositio 5.6.** *Olkoon $A \cong \mathbb{Z}^n$ $n$-ulotteinen vapaa Abelin ryhmä ja olkoon $B \subset A$ aliryhmä. Tällöin on olemassa $A$:n kanta $(a_1, \ldots, a_n)$, $k \leq n$ ja positiiviset kokonaisluvut $m_1, \ldots, m_k$ siten, että jono $(m_1 a_1, m_2 a_2, \ldots, m_k a_k)$ on $B$:n kanta ja lisäksi $m_i | m_{i+1}$, $i = 1, \ldots, k-1$.*
*Erityisesti jokaisen vapaan äärellisulotteisen vapaan ryhmän aliryhmä on myös vapaa.*

*Todistus.* Väite osoitetaan induktiolla $n = \dim A$:n suhteen. Jos $n = 0$ väite on triviaalisti selvä. Jos $n = 1$ väite on algebrasta tunnettu tosiasia, että $\mathbb{Z}$:n jokainen aliryhmä on muotoa $m\mathbb{Z}$, $m \in \mathbb{N}$.
Oletetaan siis, että väite on tosi $n-1$:lle.
Jos $B = \{0\}$ on triviaali, asia on selvä. Muuten $B$:ssä on olemassa ainakin yksi alkio $b \neq 0$ ja jos se esitetään jossakin $A$:n kannassa $(v_1, \ldots, v_n)$ lineaarisena kombinaationa

$$b = m_1 v_1 + \ldots + m_n v_n,$$

ainakin yksi kerroin $m_i$ eroaa nollasta. Voimme aina olettaa (järjestelemällä kanta uudella tavalla), että $m_1 = 0$.
Positiivisten luonnollisten lukujen joukko on "hyvinjärjestetty". Se tarkoittaa sitä, että jokaisessa sen epätyhjässä osajoukossa on pienin alkio. Voimme siis valita sellainen $A$:n kanta $(v_1, \ldots, v_n)$, että $B$ sisältää alkion

$$b_1 = m_1 v_1 + \ldots + m_n v_n,$$

jossa $m = m_1 \neq 0$ on pienin sellainen positiivinen kokonaisluku jolla on tällainen ominaisuus, eli jos $b \in B$,$(v_1', \ldots, v_n')$ on jokin toinen $A$:n kanta ja

$$b = m_1' v_1' + \ldots + m_n' v_n',$$

niin joko $m_1' = 0$ tai $|m_1'| \geq m$. Itse asiassa, koska aina voimme permutoida missä tahansa kannassa mikä tahansa alkio sen ensimmäiseksi alkioksi, yllä jokainen kerroin $m_i'$ on joko 0 tai itseisarvoltaan $\geq m$.
Yhtälössä

$$b_1 = m_1 v_1 + \ldots + m_n v_n,$$

kirjoitetaan jokainen $m_i$, $i \geq 2$ muodossa $m_i = qm + r_i$, missä $0 \leq r_i < m$ ja $q_i, r_i \in \mathbb{Z}$. Tämä on mahdollista kokonaislukujen jakoyhtälön nojalla. Tällöin

$$b_1 = ma_1 + r_2 v_2 + \ldots + r_n v_n,$$

missä $a_1 = v_1 + q_2v_2 + \ldots + q_nv_n$. Helposti nähdään, että $(a_1, v_2, \ldots, v_n)$ on edellenkin $A$:n kanta. Luvun $m$ minimaalisuudesta seuraa tällöin, että $r_2 = \ldots = r_n = 0$. Olemme siis todistaneet, että $A$:llä on olemassa kanta $(a_1, v_2, \ldots, v_n)$ siten, että $b_1 = m_1a_1$.
Koska $(a_1, v_2, \ldots, v_n)$ on kanta, pätee

$$A = \mathbb{Z}[a_1] \oplus A',$$

missä $\mathbb{Z}[a_1] = \{ma_1 \mid m \in \mathbb{Z}\}$ on $a_1$:n virittämä aliryhmä ja $A'$ on jonon $(v_2, \ldots, v_n)$ virittämä aliryhmä.
Seuraavaksi todistamme, että itse asiassa

$$B = \mathbb{Z}[b_1] \oplus B',$$

missä $B' = A' \cap B$. Tässä $\mathbb{Z}[b_1] = \{mb_1 \mid m \in \mathbb{Z}\}$ on $b$:n virittämä ($B$:n) aliryhmä.
Nimittäin olkoon $b \in B$. Esitetään se kannassa $(a_1, v_2, \ldots, v_n)$ lineaarisena kombinaationa

$$b = m_1'a_1 + m_2'v_2 + \ldots + m_n'v_n.$$

Jakoyhtälön nojalla voimme taas kirjoittaa $m_1' = qm + r$, $0 \leq r < m$. Nyt

$$b = ra_1 + m_2'v_2 + \ldots + m_n'v_n + qma_1 = ra_1 + m_2'v_2 + \ldots + m_n'v_n - qb_1,$$

joten

$$ra_1 + m_2'v_2 + \ldots + m_n'v_n = b - qb_1 \in B,$$

joten minimaalisuuden nojalla $r = 0$. Siis $b - qb_1 \in A' \cap B = B'$. Olemme näyttäneet, että $B = \mathbb{Z}[b_1] + B'$. Koska $\mathbb{Z}_{[}b_1] \subset \mathbb{Z}_{[}a_1]$ ja $B' \subset A'$, ja $\mathbb{Z}_{[}a_1] \cap A' = \{0\}$, sama pätee aliryhmille $\mathbb{Z}_{[}b_1]$ ja $B'$. Summa $B = \mathbb{Z}[b_1] \oplus B'$ on siis suora.
Ryhmä $A' = \mathrm{Span}(v_2, \ldots, v_n$ on selvästi vapaa ja $(n-1)$-ulotteinen. Näin ollen induktio-oletuksen nojalla $A'$:ssä voidaan valita kanta $(a_2, \ldots, a_n)$ siten, että $(b_2, \ldots, b_k) = (m_2a_2, \ldots, m_ka_k)$ on $B$:n kanta jollakin $k \leq n$ ja positiivisilla kokonaisluvuilla $m_2, \ldots, m_k$. Lisäksi $m_2|m_3| \ldots |m_{k-1}|m_k$.
Olemme valmiit, kun vielä näytetään, että $m_1|m_2$. Olkoon $m_2 = qm_1 + r$ (jakoyhtälö), missä $q, r \in \mathbb{Z}$, $0 \leq r < m_1$. Nyt

$$b_1 + b_2 = m_1a_1 + m_2a_2 = m_1(a_1 + qa_2) + ra_2 = m_1a' + ra_2.$$

Tässä $a' = a_1 + qa_2$. Helposti nähdään, että $(a', a_2, \ldots, a_n)$ on $A$:n kanta. $m$:n minimaalisuuden nojalla $r = 0$. Väite on todistettu. □

Strukuurilauseen 5.3 olemassolo-väite on nyt syhteellisen helppo seuraus edellisestä tuloksesta.

*Todistus.* Olkoon $(v_1, \ldots, v_n)$ jokin $A$:n virittäjäjoukko. Proposition 2.22 nojalla on olemassa tasan yksi $\mathbb{Z}$-lineaarinen (eli ryhmähomomorfismi) kuvaus $f\colon \mathbb{Z}^n \to A$, jolle $f(e_i) = v_i$. Tässä $(e_1, \ldots, e_n)$ on $\mathbb{Z}^n$:n standardikanta. Konstuktion perusteella $f$ on surjektio, joten määrittelee isomorfismin

$$(\mathbb{Z}^n)/\operatorname{Ker} f \cong A.$$

Koska $\mathbb{Z}^n$ on vapaa äärellisulotteinen ryhmä edellisen tuloksen nojalla siinä voidaan valita kanta $(a_1, \ldots, a_n)$, siten, että joillakin positiivisilla kokonaisluvuilla $m_1, \ldots, m_k$ jono $(m_1a_1, m_2a_2, \ldots, m_ka_k)$ on $B = \operatorname{Ker} f$:n kanta. Lisäksi $m_i | m_{i+1}$, $i = 1, \ldots, k-1$. Helposti nähdään, että

$$\mathbb{Z}^n/B = (\oplus\mathbb{Z}[a_i])/(\oplus\mathbb{Z}[m_ia_i]) = \oplus(\mathbb{Z}[a_i]/Z[m_ia_i]) \cong$$

$$\cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m-2} \oplus \ldots \oplus \mathbb{Z}_{m_k} \oplus \mathbb{Z}_{m_{k+1}} \oplus \ldots \oplus \mathbb{Z}_{m_n},$$

missä $m_{k+1} = \ldots = m_n = 0$, joten vastaavat ryhmät $\mathbb{Z}_{m_i} = \mathbb{Z}$. Hajotelman (5.4) olemassaolo on näytetty.

□

Yksikäsitteisyyden osoittaminen on sotkuisempi. Aloitetaan määritelemällä niin sanottu $A$:n *torsioaliryhmä* $\operatorname{Tor} A$,

$$\operatorname{Tor} A = \{x \in A \mid \text{ on olemassa } n \in \mathbb{N}, n > 0 \text{ siten, että } nx = 0\}.$$

Helposti nähdään, että $\operatorname{Tor} A$ on todellakin aliryhmä. Jokainen sen alkio sanotaan ryhmän $A$ *torsioalkioksi*. Nyt, jos $A$ on äärellisviritteinen, ja esitetty muodossa

$$A = \mathbb{Z}^n \oplus \mathbb{Z}_{m_1} \oplus \ldots \mathbb{Z}_{m_k},$$

niin helposti nähdään, että

$$\operatorname{Tor} A = \mathbb{Z}_{m_1} \oplus \ldots \mathbb{Z}_{m_k}.$$

Tästä puolestaan seuraa, että $A/\operatorname{Tor}(A) \cong \mathbb{Z}^n$. Koska vapaan äärellisulotteisen Abelin ryhmän dimensio on yksikäsitteinen, tästä heti nähdään, että $n = \dim(A/\operatorname{Tor} A)$ on yksikäsitteisesti määrätty.
Koska

$$\operatorname{Tor} A = \mathbb{Z}_{m_1} \oplus \ldots \mathbb{Z}_{m_k}$$

myös riippuu vain $A$, riittää näyttää, että *äärellisen* Abelin ryhmän $A$ esitys muodossa

$$A = \mathbb{Z}_{m_1} \oplus \ldots \mathbb{Z}_{m_k},$$

missä $m_1 | m_2 | \ldots | m_{k-1} | m_k$, on yksikäsitteinen.
Ennen kuin jatketaan, pannan merkille eräs aputulos, jonka todistus jätämme lukijalle harjoitustehtäväksi.

**Lemma 5.7.** *Olkoot $n, m$ positiiviset kokonaisluvut. Tällöin seuraavat ehdot ovat yhtäitäviä.*
*1) $\mathbb{Z}_n \oplus \mathbb{Z}_m$ on syklinen,*
*2) $Z_n \oplus \mathbb{Z}_m \cong \mathbb{Z}_{nm}$,*
*3) $n$ ja $m$ ovat keskenään jaottomat, eli 1 on niiden ainoa yhteinen positiivinen tekijä $\mathbb{Z}$:ssä.*

Palataan hajotelmaan

$$A = \mathbb{Z}_{m_1} \oplus \dots \mathbb{Z}_{m_k},$$

jossa $m_1|m_2|\dots|m_{k-1}|m_k$. Kirjoitetaan suurin indeksi $m_k$ muodossa

$$m_k = p_1^{l_{1,k}} p_2^{l_{2,k}} \dots p_s^{l_{s,k}},$$

missä $p_1, \dots, p_s$ (erilaiset) alkuluvut ja $l_{i,k} > 0$, $i = 1, \dots, s$. Tämä on mahdollista, sillä jokainen luonnollinen voidaan tunnetusti kirjoittaa (yksikäsitteisellä tavalla) alkulukujen tulona.
Koska $m_i|m_{i+1}$, $i = 1, \dots, k-1$, jokaisen indeksin $m_i$ alkutekijät ovat myös $m_k$:n alkulukutekijät. Näin ollen voidaan kirjoittaa

$$m_i = p_1^{l_{1,i}} p_2^{l_{2,i}} \dots p_s^{l_{s,i}},$$

$i = 1, \dots, k$. Tässä kertoimet $l_{r,i}$ toteuttavat lisäksi epäyhtälöketjuja

$$0 \leq l_{r,1} \leq l_{r_2} \leq \dots \leq l_{r_k},$$

jokaisella $r = 1, \dots, s$. Huomaa, että eivät kaikki potenssit $l_{r,i}$ eivät enää vältämättä ole positiivisia, vaan jotkut niistä saattavat olla myös 0.

Koska erilaiset alkuluvut (ja yleisemmin niiden potenssit) ovat keskenään jaottomat, Lemman (5.7) nojalla voimme jokainen tekijä $\mathbb{Z}_{m_i}$ kirjoittaa suorana summana

$$\mathbb{Z}_{m_i} = \oplus_r \mathbb{Z}_{p_j}^{l_{i,r}}, \tag{5.8}$$

missä tietenkin riittää ottaa summa niistä termeistä joille $l_{i,r} > 0$. Jos oletamme, että näin on tehty, jokainen summassa oikealla puoleella esiintyvää syklinen ryhmä on epätriviaali.
Jokaisella $r = 1, \dots, s$ olkoon

$$A_r = \{a \in A \mid p_r^k a = 0 \text{ jollakin } k \in \mathbb{N}, e > 0\}.$$

Toisin sanoen $A_r$ koostuu alkosta, joiden kertaluku on alkuluvun $p_r$ potenssi. Määritelmänsä mukaan $A_r$ riippuu vain $A$:sta, ei hajotelmasta (5.4). Helposti nähdään, että $A_r$ on aliryhmä. Ryhmänä se on esimerkki niin sanotusta äärellistä $p_r$-ryhmästä.

**Määritelmä 5.9.** *Olkoon $A$ Abelin ryhmä ja $p \in \mathbb{N}$ alkuluku. Sanomme että $A$ on Abelin ryhmä, jos jokaisen sen alkion kertaluku on $p$:n jokin potenssi, eli jos kaikilla $x \in A$ on olemassa $k \in \mathbb{N}$ siten, että $p^k x = 0$.*

Aliryhmän $\mathbb{Z}_{m_i}$ hajotelmasta (5.8) nähdään, että (samoilla merkinnöillä kuin yllä) pätee $A_r \cap \mathbb{Z}_{m_i} = \mathbb{Z}_{p_r}^{l_{i,r}}$. Nimittäin, unohdetaan turhista indekseista hetkeksi ja tarkastellaan syklisen äärellisen ryhmän esitystä muodossa

$$\mathbb{Z}_m = \mathbb{Z}_{p_1^{k_1}} \oplus \mathbb{Z}_{p_2^{k_2}} \oplus \ldots \oplus \mathbb{Z}_{p_l^{k_l}},$$

missä $p_1, \ldots, p_l$ ovat alkuluvut ja siis oikealla esiintyvät ryhmät kaikki sykliset $p_i$-ryhmät. Tällöin jokainen $\mathbb{Z}_m$:n alkio $x$ voidaan tässä tulkinassa ajatella alkiona $x_1 + \ldots + x_l$, missä $x_i \in \mathbb{Z}_{p_i^{k_i}}$. Oletetaan, että lisäksi $x \in A_r$. Olkoon $k \in \mathbb{N}, k > 0$. Tällöin

$$p_r^k x = p_r^k x_1 + \ldots + p_j r^k x_l = 0,$$

missä jokainen $p_r^k x_i \in \mathbb{Z}_{p_i^{k_i}}$. Koska summa on suora, myös $p_j rk x_i = 0 \in \mathbb{Z}_{p_i^{k_i}}$. Olkoon $r \neq i$. Jos $x_i \neq 0$, niin edellisestä ja Lemmasta 5.1 seuraa, että sen kertaluku on $p_r$:n potenssi. Toisaalta saman Lemman mukaan $x_i$ kertaluvun täytyy olla $p_i^{k_i}$:n tekijä. Koska $p_i$ ja $p_r$ ovat eri alkuluvut, saadaan ristiriitä. Näin ollen $x_i = 0$ kaikilla $i \neq r$. Olemme näyttäneet, että $A_r \cap \mathbb{Z}_{m_i} \subset \mathbb{Z}_{p_r}^{k_r}$. Toinen suunta seuraa helposti $A_r$:n määritelmästä.
Näin ollen, kun palataan alkuperäisin merkintöihin, saadaan $A_r \cap \mathbb{Z}_{m_i} = \mathbb{Z}_{p_r}^{l_{i,r}}$ jokaisella $r, i$. Koska aliryhmien $\mathbb{Z}_{m_i}$ summa on suora, nähdään siis, että $A_r$ on suora summa $p_r$-ryhmistä $\mathbb{Z}_{p_r}^{l_{i,r}}$, missä $i$ käy läpi kaikki sellaiset indeksit $1, \ldots, k$, joilla vastaava potenssi $l_{i,r} > 0$. Aliryhmät $A_r$ riippuvat vain $A$:stä, ei hajotelmasta (5.4). Lisäksi indeksit $m_i$ saadaan takaisin tuloina

$$m_i = p_1^{l_{1,i}} p_2^{l_{2,i}} \ldots p_s^{l_{s,i}},$$

SS $i = 1, \ldots, k$, missä ne termit, joilla vastaava potenssi $l_{i,r} = 0$ ovat ykkösiä, joten eivät vaikuta. Jos pystymme siis osoittamaan, että $p_r$-ryhmän $A_r$ esitys

$$A_r = \oplus \mathbb{Z}_{p_r}^{l^{i,r}}$$

syklisten $p$-ryhmien suorana summana on yksikäsitteinen, samalla tulee todistettua mös, että kertoimet $m_1, \ldots, m_k$ ovat yksikäsitteisiä. Tämä on seuraavan Lemman sisältö.

**Lemma 5.10.** *Oletetaan, että $A_i, B_j$ ovat äärellisiä epätriviaaleja syklisiä $p$-ryhmiä ($p$ alkuluku), $i = 1, \ldots, r$, $j = 1, \ldots, s$ ja oletetaan, että*

$$A_1 \oplus A_2 \oplus \ldots \oplus A_r \cong B_1 \oplus B_2 \oplus \ldots \oplus B_s.$$

*Tällöin $r = s$ ja järjestystä vailla $A_i \cong B_i$ kaikilla $i = 1, \ldots, r$.*

*Todistus.* Esitetään kaikki esiintyvät sykliset ryhmät muodossa $A_i = \mathbb{Z}_{p^{k_i}}, B_j = \mathbb{Z}_{p^{l_j}}$. Järjestämällä suoran summat jäsenet uudelleen tarvittaessa, voimme olettaa, että

$$k_1 \geq k_2 \geq \ldots > k_n = k_{n+1} = \ldots = k_r = 1,$$

$$l_1 \geq l_2 \geq \ldots > l_n = k_{m+1} = \ldots = l_s = 1.$$

Identifioimalla isomorfiset ryhmät voidaan lisäksi olettaa, että

$$A_1 \oplus A_2 \oplus \ldots \oplus A_r = A = B_1 \oplus B_2 \oplus \ldots \oplus B_s. \tag{5.11}$$

Pitää osoittaa, että $r = s$ ja $k_i = l_i$ kaikilla $i = 1, \ldots, r$.
Tehdään tämä induktiolla ryhmän $A$ koon $|A|$ koon suhteen. Jos $|A| = 1$, asia on triviaalisti selvä.
Tarkastellaan osajoukkoa $pA = \{pa \mid a \in A\} \subset A$. Helposti nähdään, että tämä on $A$:n aliryhmä. Itse asiassa kuvaus $f\colon A \to A$, $f(a) = pa$ on ryhmähomorfismi (tarkista!), joten $pA = \operatorname{Im} f$ ja isomorfialauseen nojalla $pA \cong A/\operatorname{Ker} f$. Itse asiassa jokainen aliryhmä $A_i$ ja $B_j$ ovat $f$-invariantteja eli $f(A_i) = pA_i \subset A_i$ (samoin $B_j$:lle). Tästä seuraa, että $pA$ on $p$-ryhmä, joka voidaan kirjoittaa muodossa

$$pA_1 \oplus pA_2 \oplus \ldots \oplus pA_r = pA = pB_1 \oplus pB_2 \oplus \ldots \oplus pB_s. \tag{5.12}$$

Tarkastellaan erikseen miltä $pA$ näyttää sykliselle $p$-ryhmälle $A = \mathbb{Z}_{p^k}$ (jokainen $A_i$ ja $B_j$ on tätä muotoa). Kuvaus $f\colon A \to pA$ on surjektiivinen homomorfismi. Lasketaan mikä on sen ydin. $A$:n alkiot ovat muotoa $0, 1, \ldots, p, \ldots, p^{k-1}, \ldots, p^k - 1$, missä merkinnöissä "samastamme" kokonaisluvun $r$ ja sen luokan $\overline{r} \in \mathbb{Z}_n$. Luokka $r \in \operatorname{Ker} f$ jos kokonaislukujen tasolla luku $pr$ on jaollinen $p^k$:llä, mikä on mahdollista jos ja vain jos $r$ on jaollinen $p^{k_1}$. Näin ollen $\operatorname{Ker} f$ on syklinen aliryhmä, jonka virittää alkio $p^{k-1}$. Tarkastelemalla tämän alkion virittämän ryhmän alkiot nähdään, että niitä on tasan $p$ - ne ovat $0, p^{k-1}, 2p_{k-1}, \ldots, (p-1)p^{k-1}$, sillä seuraava potenssi $pp^{k-1} = p^k$ on jo nolla $A$:ssä. Erityisesi, koska isomorfialauseen nojalla $pA \cong A/\operatorname{Ker} f$, saadaan näiden koolle

$$|pA| = |A/\operatorname{Ker} f| = |A|/|\operatorname{Ker} f| = p^k/p = p^{k-1}.$$

Tämä on erikoistapaus äärellisten ryhmien teoriaan kuuluvasta Langrange'n Lauseesta, joka sanoo, että jos $H$ on äärellisen ryhmän $G$ aliryhmä, niin $|G/H| = |G|/|H|$.
Soveltamalla saatu tulos hajotelmaan (5.13) vasempaan puoleen, nähdään, että

$$p^{k_1-1}p^{k_2-1}\ldots p^{k_{n-1}-1} = |pA| < |A|.$$

Näin ollen $pA$ on $p$-ryhmä, jonka koko on pienempi kuin $A$:n koko, joten induktio-oletuksen mukaan väite pätee $pA$:lle. Koska saman hajotelmaan mukaan

$$pA_1 \oplus pA_2 \oplus \ldots \oplus pA_{k_{n-1}} = pA = pB_1 \oplus pB_2 \oplus \ldots \oplus pB_{m-1}, \tag{5.13}$$

saadaan tästä, että $n = m$ ja $k_i - 1 = l_i - 1$ kaikilla $i = 1, \ldots, k_{n-1}$. Huomaa, että ryhmät $A_{k_n}, A_{k_{n+1}}, \ldots$ ja samalaiset $B$-puoleella häviää näkyvistä sillä $pA$ versiot niistä ovat triviaaleja, yhden alkion ryhmiä.Olemme näyttäneet, että $k_i = l_i$ kun $i < n$.
Mutta koska $n = m$ ja $k_i = 1 = l_i$ kaikilla $i \geq n$, nekin indeksit ovat samat, kunhan näytetään vielä, että $r = s$ Väite todistettu. Mutta kaikkien aliryhmien $A_i, B_j$, $i, j \geq n$ koot ovat tasan $p$, joten vertamalla taas $A$:n erilaisten esitysten koot hajotelmassa (5.11) saadaan (ottamalla huomioon jo todistetut väitteet)

$$p^{k_1+\ldots+k_{n-1}} p^{r-n} = p^{k_1+\ldots+k_{n-1}} p^{s-n},$$

mistä seuraa, että $r = s$. Todistus on valmis. □

Samalla siis Abelin ryhmien struktuurilause 5.2 tuli todistetuksi.
Jokaisen äärellisviritteiseen Abelin ryhmään $A$ voidaan siis liittää jono $(n; m_1, \ldots, m_k)$ sen invariantteja, jotka määräytyvät esityksestä

$$A \cong \mathbb{Z}^n \oplus \mathbb{Z}_{m_1} \oplus \ldots \mathbb{Z}_{m_k}.$$

Luku $n$ on $A$:n *aste* (engl. rank). Jos $A$ on äärellinen, sen aste on 0. Jos taas $A$ on *torsiovapaa* eli $\operatorname{Tor} A = \{0\}$, niin $k = 0$ ja $A \cong \mathbb{Z}_n$ on jopa vapaa. Olemme todistaneet, että jokainen äärellisviritteinen torsiovapaa ryhmä on vapaa.
Ei-äärellisviritteisille ryhmille tämä ei päde - esim. $\mathbb{Q}$ on torsiovapaa, mutta ei ole vapaa (harjoitustehtävä).

**Abelin ryhmän eksponentti**.
Olkoon $A$ äärellinen Abelin ryhmä. Tällöin jokaisen $a \in A$ kertaluku on varmasti äärellinen, joten on olemassa $n_a \in \mathbb{N}, n_a > 0$ jolle $n_a a = 0$. Luvulla

$$n = \prod_{a \in A} n_a$$

on selvästi sellainen ominaisuus, että $na = 0$ kaikilla $a \in A$. Kun kerran tällaiset positiiviset kokonaisluvut ovat olemassa, on olemassa myös pienin. Sitä kutsutaan $A$:n *eksponentiksi*. Eksponentti on siis pienin positiivinen kokonaisluku $m$ siten, että $ma = 0$ kaikilla $a \in A$.
Eksponentin avulla voidaan karakterisoida Abelin ryhmät.

**Lemma 5.14.** *Olkoon $A$ äärellinen Abelin ryhmä ja $m$ sen eksponentti. Tällöin $A$ on syklinen jos ja vain jos $m = |A|$. Muuten $m < |A|$.*

*Todistus.* Struktuurilauseen 5.2 nojalla on olemassa esitys

$$A \cong \oplus \mathbb{Z}_{m_1} \oplus \dots \mathbb{Z}_{m_k},$$

missä $1 < m_1 | m_2 | \dots | m_k$. Koska tällainen esitys on lisäksi yksikäsitteinen, $A$ on syklinen jos ja vain jos $k = 1$, mikä puolestaan toteutuu jos ja vain jos $m_k = |A| = m_1 \dots m_k$. Toisaalta helposti nähdään, että $m_k a = 0$ kaikilla $a \in A$ ja $m_{k-1} \neq 0 \in \mathbb{Z}_{m_k} \subset A$, joten $m_k$ on $A$:n eksponentti. Väite seuraa. □

**Seuraus 5.15.** *Olkoon $K$ äärellinen kunta. Tällöin sen kääntyvien alkioiden multiplikaativinen ryhmä $K^* = K \setminus \{0\}$ on syklinen.*

*Todistus.* Olkoon $m$ ryhmän $A = K^*$ eksponentti. Edellisen lemman nojalla riittää osoittaa, että $m = |A|$. Tehdään vasta-oletus - $m < |A|$. Esponentin määritelmän mukaan jokaisella $x \in A$ pätee $x^m = 1$. Tämä on $m$-asteinen polynomiyhtälö, jolla on $|A| > m$ ratkaisuja. Tämä on kuitenkin mahdotonta Proposition 3.25 nojalla. □