4 Abelin ryhmät

Ensimmäisellä ryhmäteorian kurssilla käytiin läpi lähinnä syklisiä ryhmiä. Tällä kurssilla keskitymme epäkommutatiivisiin esimerkkeihin. On kuitenkin niin, että äärellisesti viritettyjen Abelin ryhmien teoria on syytä nähdä ainakin kerran elämässä ja se on suhteellisen helppo myös, joten käykäämme se tässä lyhyesti läpi. Tämän teorian perusteella saamme myös helposti luokiteltua loput ryhmät, joiden kertaluku on kahdeksan ja näemme, että nämä kolme ovat epäisomorfisia.

4.1 Suorat tulot ja summat

4.1.1 Ulkoinen suora tulo

Olkoot $G_1, \ldots, G_n$ ryhmiä. Muodostamme karteesisen tulon $G := G_1 \times G_2 \times \cdots \times G_n$ ja tälle joukolle määrittelemme kaksipaikkaisen operaation yksinkertaisesti $(g_1, \ldots, g_n)(h_1, \ldots, h_n) = (g_1h_1, \ldots, g_nh_n)$, eli jokaisessa komponentissa i tulo noudattaa ryhmän G_i tuloa.

Tehtävä 23. Todista, että tämä on ryhmä.

Kutsumme ryhmää $G = G_1 \times G_2 \times \cdots \times G_n$ ryhmien $G_1, \ldots, G_n$ (ulkoiseksi) suoraksi tuloksi. Huomaa, että komponenttien G_i järjestyksellä ei ole ryhmän määritelmässä mitään väliä.

Ryhmällä $G = G_1 \times G_2 \times \cdots \times G_n$ on seuraavat ominaisuudet

(i) Jokaista indeksiä i kohden, on olemassa $H_i \leq G$, ja $H_i \cong G_i$, eli

$$H_i = \{(1, \ldots, g_i, \ldots, 1) : g_i \in G_i\}.$$

Lisäksi huomaamme, että

$$G/H_i \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n.$$

(ii) Jokainen $g \in G$ voidaan kirjoittaa yksikäsitteisesti $g = h_1 \ldots h_n$, jossa jokainen $h_i \in H_i$. Eli jos $g = (g_1, \ldots, g_n)$, niin $h_i = (1, \ldots, g_i, \ldots, 1)$ jokaiselle i. Tästä seuraa, että jos jokainen G_i on äärellinen, niin $|G| = |G_1||G_2| \ldots |G_n|$.

Tämä konstruktio toimii mille tahansa ryhmille G_i.

4.1.2 Sisäinen suora tulo

Olettakaamme nyt vuorostamme, että G on ryhmä, ja sillä on aliryhmät $H_1, \ldots, H_n$ ja niillä ominaisuudet.

(i) $H_i \lhd G$, kaikille $i = 1, \ldots, n$.

(ii) Jokainen $g \in G$ voidaan yksikäsitteisesti kirjoittaa muodossa $g = h_1 \ldots h_n$, jossa jokainen $h_i \in H_i$

Huomaamme, että näistä kahdesta seuraa

(iii) $G = H_1 \ldots H_n$.

(iv) $H_i \bigcap H_1 \ldots H_{i-1} H_{i+1} \ldots H_n = 1$ jokaiselle indeksille i.

(v) Jos $i \neq j$, silloin H_i:n ja H_j:n alkiot kommutoivat keskenään.

(vi) Jos $g = h_1 \ldots h_n$ ja $g' = h'_1 \ldots h'_n$, jossa $h_i, h'_i \in H_i$ jokaiselle i:lle, silloin $gg' = (h_1 h'_1) \ldots (h_n h'_n)$.

Huomaamme, että voimme määritellä yksikäsitteisen isomorfismin $\tau : G \longrightarrow H_1 \times H_2 \times \cdots \times H_n$, jossa siis jokainen $H_i \mapsto 1 \times \cdots \times H_i \times \cdots \times 1$.

Kutsumme tällöin ryhmää G:tä aliryhmiensä $H_1, \ldots, H_n$ (sisäiseksi) suoraksi tuloksi. Toisinaan merkitsemme myös $G = H_1 \times H_2 \times \cdots \times H_n$, vaikka tämä onkin lievää merkintätavan väärinkäyttöä.

Tästä seuraa lause

Lause 4.1 (Kiinalainen jäännösluokkalause)**.** *Olkoon* $n = p_1^{k_1} \cdots p_m^{k_m}$. *Silloin*

$$C_n \cong C_{p_1^{k_1}} \times \cdots \times C_{p_m^{k_m}}.$$

Todistus. Määritellään kaikille $1 \leq i \leq m$ ryhmä $P_i = \langle x_i \rangle \cong C_{p_i^{m_i}}$. Nyt alkion $(x_1, \ldots, x_n) \in P_1 \times \cdots \times P_m$ kertaluku on $p_1^{k_1} \times \cdots \times p_m^{k_m} = n$, joten $P_1 \times \cdots \times P_m \cong C_n$, koska ryhmä on syklinen. □

Korollaari 4.2. *Jos* $m = pq$, *kahden erillisen alkuluvun tulo, on* $C_m \cong C_p \times C_q$.

Esimerkiksi totesimme kertalukua kuusi olevien ryhmien luokittelussa, että $C_6 \cong C_2 \times C_3$.

Huomaa, että tämä on sama kiinalainen jäännösluokkalause kuin alkeellisessa lukuteoriassa.

Olkoot $n_1, \ldots, n_k$ pareittain suhteellisia alkulukuja. Silloin mille tahansa kokonaisluvuille $a_1, \ldots, a_k$ on olemassa kokonaisluku x, joka toteuttaa kongruenssiyhtälöryhmän

$$\begin{aligned} x &\equiv a_1 \mod n_1 \\ x &\equiv a_2 \mod n_2 \\ &\vdots \\ x &\equiv a_k \mod n_k. \end{aligned}$$

Lisäksi kaikki ratkaisut x ovat kongruentteja modulo N, missä $N = n_1 n_2 \ldots n_k$.

Tämä siis syklisten ryhmien lauseessa todistaa, että kuvaus

$$C_n \longrightarrow C_{p_1^{k_1}} \times \cdots \times C_{p_m^{k_m}}$$

on surjektiivinen.

Teoreeman julkaisi ensimmäisen kerran kiinalainen matemaatikko Sun Tzu kolmannella vuosisadalla. Alkuperäinen Sun Tsun ongelma kuuluu seuraavasti. Kuinka monta sotilasta on Han Xingin armeijassa? Jos sotilaat marssivat kolmen riveissä, kaksi sotilasta jää yli. Jos he marssivat viiden riveissä, kolme jää yli, ja jos he marssivat seitsemän riveissä, kaksi jää yli?

Ongelma voidaan ilmaista kongruenssiyhtälöryhmänä:

$$\begin{aligned} x &\equiv 2 \mod 3 \\ x &\equiv 3 \mod 5 \\ x &\equiv 2 \mod 7 \end{aligned}$$

Luvut 3, 5 ja 7 ovat pareittain keskenään jaottomia, joten voimme soveltaa kiinalaista jäännöslausetta.

Ensimmäisestä yhtälöstä saamme, että $x = 3t+2$, jollekin kokonaisluvulle t. Sijoitamme tämän toiseen yhtälöön ja saamme, $3t + 2 \equiv 3 \mod 5$. Tästä seuraa, että $t \equiv 2 \mod 5$, joten $t = 5u+2$, ja siis $x = 3(5u+2)+2 = 15u+8$, jonka voimme sijoittaa viimeiseen yhtälöön $15u + 8 \equiv 2 \mod 7$. Tämän kongruenssin ratkaisu on $u \equiv 1 \mod 7$, joten $u = 7v + 1$, mikä lopulta tuottaa vastauksen $x = 15(7v + 1) + 8 = 105 + 23$. Joten $x \equiv 23 \mod 105$. Sotilaiden määrä voi siis olla 23, 128, 233, 338 jne.

Tehtävä 24. Ratkaise ryhmä

$$\begin{aligned} x &\equiv 1 \mod 5 \\ x &\equiv 2 \mod 6 \\ x &\equiv 3 \mod 7. \end{aligned}$$

Kiinalainen jäännösluokkalause ei kuitenkaan auta Abelin ryhmien luokittelussa kovinkaan pitkälle, sillä tiedämme esimerkiksi, että kaikki äärelliset Abelin ryhmät eivät ole muotoa C_{p^n}, esimerkiksi $C_4 \ncong C_2 \times C_2$. On siis kaksi äärellistä Abelin ryhmää, joiden kertaluku on neljä.

Miten tästä eteenpäin luokittelun kanssa?

4.2 Ryhmän virittäjät

Syklinen ryhmässä C_n on alkio g, jonka kertaluku on n ja $C_n = \langle g \rangle$. Kutsumme alkiota g ryhmän C_n virittäjiksi. Voimme yleistää virittäjän käsitettä useampiin virittäjiin.

Määritelmä 4.3. Olkoon S ryhmän G osajoukko. Joukon S virittämä aliryhmä on

$$\langle S \rangle := \bigcap_{S \subset H \leq G} H.$$

Jos $\langle S \rangle = G$, kutsumme joukon S alkioita ryhmän G virittäjiksi tai generaattoreiksi. Jos virittäjäjoukko on äärellinen, kutsutaan ryhmää G äärellisesti viritetyksi.

Propositio 4.4. *Ryhmän G osajoukon S virittämä aliryhmä koostuu kaikista tuloista*

$$\langle S \rangle = \{ s_1^{e_1} s_2^{e_2} \dots s_l^{e_l} : s_i \in S, e_i = \pm 1, l = 1, 2, \dots \},$$

jos $l = 0$, määrittelemme tyhjäksi tuloksi ykkösalkion.

Todistus. Merkitään yhtälön oikeanpuoleista joukkoa H:lla. $S \subseteq H$ ja koska $H \leq G$, saamme $\langle S \rangle \subseteq H$. Toisaalta, jos M on mikä tahansa aliryhmä, joka sisältää joukon S, niin sisältää aliryhmä M kaikki tulot, jotka saadaan muodostettua joukosta S, joten $H \leq M$, kaikille $S \subseteq M \leq G$. Niinpä

$$H \subseteq \bigcap_{S \subset M \leq G} H = \langle S \rangle.$$

□

Esimerkki 4.5. Alkiot r ja a virittivät edellisen luvun esimerkissä ryhmän D_8. Ryhmä D_8 on siis kahden alkion virittämä.

Huomaa, että ryhmällä voi olla monta virittäjäjoukkoa. Virittäjäjoukkoa kutsutaan minimaaliseksi, jos jonkun alkion poisto tarkoittaa sitä, että ryhmä ei enää virity. Myöskään minimaalinen virittäjäjoukko ei ole yksikäsitteinen. Minimaalinen ei tarkoita, että alkioitten määrä olisi minimaalinen.

Tehtävä 25. (i) Mitkä alkiot virittävät äärettömän syklisen ryhmän $\mathbb{Z}$?

(ii) Etsi ryhmän S_3 minimaaliset virittäjäjoukot.

(iii) Osoita, että kumpikin joukko $(12), (13), (14)$ ja $(12), (1234)$ ovat ryhmän S_4 minimaalinen virittäjäjoukko. Löydätkö vielä lisää minimaalisia virittäjäjoukkoja? Yleistä tulos koskemaan kaikkia ryhmiä S_n.

4.3 Vapaa Abelin ryhmä

Olkoon $\mathbb{G}$ ryhmäluokka (esimerkiksi kaikki ryhmät, Abelin ryhmät, ratkeavat ryhmät, äärelliset ryhmät). Olkoon G mikä tahansa ryhmä luokassa $\mathbb{G}$, joka on joukon $\{a_i : i \in I\}$ virittämä. Ryhmää $F := \langle x_i : i \in I\rangle$ kutsutaan vapaaksi luokassa $\mathbb{G}$ jos jokainen virittäjäkuvaus $x_i \mapsto a_i$ laajenee ryhmähomomorfismiksi $F \longrightarrow G$. Toisinaan ryhmää F kutsutaan myös joukon $\{x_i : i \in I\}$ vapaasti virittämäksi. Indeksijoukon I mahtavuutta kutsutaan vapaan ryhmän rankiksi. Rankki voi olla äärellinen tai ääretön.

Intuitiivisesti ajatellen vapaa ryhmä on siis sellainen ryhmä, jossa ei ole yhtään relaatioita virittäjien välillä. Koska jos, sanokaamme $x_1x_2 = 1$ ryhmässä F, voi olla, että kuvaus $x_i \mapsto a_i$ ei ole homomorfismi, jos ryhmässä G $a_1a_2 \neq 1$.

Kaikki ryhmäluokat eivät sisällä vapaata ryhmää. Kaikkien ryhmien luokka sisältää vapaan ryhmän, jota käsittelemme myöhemmin tällä kurssilla. Myös Abelin ryhmät sisältävät vapaan ryhmän. Abelin ryhmissä yleensä käytetään additiivista merkintätapaa. Siksi yleensä merkitsemme ääretöntä syklistä ryhmää nimellä $\mathbb{Z}$, emmekä C_∞. Edellä käsitellyt suorat tulot ymmärretään tällä merkintätavalla suoriksi summiksi. Huomaa, että additiivisessa merkinnässä g^n on muodossa ng, ja jokaista suoran summan alkiot merkitään $a = \sum n_k a_k$, eikä $(a_1^{n_1}, \ldots, a_k^{n_k})$.

Lemma 4.6. *Olkoon G Abelin ryhmä. Oletamme, että tekijäryhmä G/N hajoaa äärettömien syklisten ryhmien suoraksi summaksi*

$$G/N = \bigoplus_{i\in I}(A_i/N),$$

$A_i = \langle a_i + N\rangle$. Silloin G on aliryhmiensä N ja $A = \langle a_i : i \in I\rangle$ suora summa.

Todistus. Ensiksikin huomaamme, että $G = N + A$. Oletetaan ristiriitaa varten, että $A \bigcap N$:ssa on epätriviaali alkio a. Tällöin $a = \sum n_k a_{i_k}$, koska tämä alkio kuuluu A:n. Kun siirrytään tekijäryhmään G/N saadaan

$$N = a + N = \sum(n_k a_{i_k} + N),$$

(koska $a \in N$) ja nyt seuraa suoran summan määritelmästä, että $n_k a_{i_k} + N = N$ kaikilla k. Koska A_{i_k}/N on ääretön syklinen ryhmä, tästä seuraa, että jokainen $n_k = 0$, mutta silloin $a = 0$, mikä on vaadittu ristiriita. □

Lause 4.7. *Abelin ryhmien luokassa vapaat ryhmät ovat täsmälleen äärettömien syklisten ryhmien suoria summia.*

Todistus. Olkoon $G = \bigoplus_{i \in I} \langle x_i \rangle$ äärettömien syklisten ryhmien $\langle x_i \rangle$ suora summa, ja olkoon A mikä tahansa ryhmä, jonka virittäjät ovat $a_i, i \in I$. Nyt voimme luonnollisella tavalla laajentaa virittäjäkuvauksen $x_i \mapsto a_i$ ryhmäepimorfismiksi $\sum n_k x_{i_k} \mapsto \sum n_k a_{i_k}$. Olemme siis todistaneet, että G on vapaa Abelin ryhmä, jonka rankki on äärettömien syklisten ryhmien määrä.

Olkoon G nyt vapaa Abelin ryhmä ja $\{x_i : i \in I\}$ vapaa virittäjäjoukko tälle ryhmälle. Vapaan ryhmän määritelmän mukaan, on olemassa epimorfismi τ ryhmästä F äärettömien syklisten ryhmien suoraan summaan $A = \bigoplus_{i \in I} \langle a_i \rangle$, joka laajentaa virittäjäkuvauksen $x_i \mapsto a_i$ ryhmäepimorfismiksi. Ensimmäisen isomorfialauseen perusteella $F/N \cong A$, jossa $N = Ker(\tau)$, joten tekijäryhmä F/N hajoaa (i.e. on sisäisesti isomorfinen) äärettömien syklisten ryhmien $\langle x_i + N \rangle, i \in I$ suoraksi summaksi. Edellisen lemman perusteella $F = N \bigoplus B$, jossa $B = \langle x_i : i \in I \rangle$. Kuitenkin aliryhmä B on saman joukon $\{x_i : i \in I\}$ virittämä kuin F, joten homomorfismin τ ytimen N pitää olla nolla, joten homomorfismi τ olikin isomorfismi. □

Tämä todistus myös osoittaa, että vapaan Abelin ryhmän rankki ei riipu ryhmän kannasta. Ryhmän rankki riippuu vain siitä, miten monen äärettömän syklisen ryhmän suora summa vapaa Abelin ryhmä on.

4.4 Äärellisesti viritetyt Abelin ryhmät

Lause 4.8 (Abelin ryhmien peruslause)**.** *Olkoon F_n vapaa Abelin ryhmä, jonka rankki n on äärellinen, ja olkoon $0 \neq A \leq F_n$. Silloin A on vapaa, ja ryhmillä A ja F_n on kannat $\{a_1, \ldots, a_k\}$ ja $\{f_1, \ldots, f_n\}$, joilla on seuraavat ominaisuudet: $k \leq n$, $a_i = m_i f_i$ kaikille $1 \leq i \leq k$ ja m_i jakaa m_{i+1}:n, kun $1 \leq i \leq k-1$.*

Todistus. Todistus on induktio ryhmän F_n rankin suhteen. Jos $n = 1$, on ryhmä syklinen ja isomorfinen $\mathbb{Z}$:n kanssa, joten väite on tosi. Olkoon $n > 1$. Oletetaan nyt, että väite on totta vapaille Abelin ryhmille, joiden rankki on $n - 1$.

Huomaamme ensin, että jos $\{x_1, \ldots, x_n\}$ on mikä tahansa ryhmän F_n (järjestetty) kanta, ja a mikä tahansa F_n:n alkio, silloin on olemassa yksikäsitteinen kokonaislukujen ännäkkö $(t_1, \ldots, t_n)$, joka määrittää

$$a = t_1 x_1 + \cdots + t_n x_n,$$

tämän kannan suhteen.

Valitaan nyt joku kanta ja $a_1 \in A$, siten että, tämän kannan ännäkön ensimmäinen kerroin on positiivinen ja pienin mahdollinen, kutsutaan tätä nimellä m_1. Merkitään tätä uutta kantaa $\{b_1, \ldots, b_n\}$, joten

$$a_1 = m_1 b_1 + t_2 b_2 + \cdots + t_n b_n.$$

Haluamme todistaa, että m_1 jakaa kaikki kertoimet t_i. Jakoyhtälön perusteella, voimme kirjoittaa $t_i = q_i m_1 + r_i, (0 \leq r_i < m_1)$. Määritellään uusi kanta

$$\{f_1 = b_1 + q_2 b_2 + \cdots + q_n b_n, b_2, \ldots, b_n\}. \tag{1}$$

Tämän kannan suhteen $a_1 = m_1 f_1 + r_2 b_2 + \cdots + r_n b_n$. Koska olimme valinneet m_1:n minimaaliseksi, jokainen $r_i = 0$. Niinpä $a_1 = m_1 f_1$.

Kirjoitetaan $B = A \bigcap F_{n-1}$, jossa $F_{n-1} = \langle b_2, \ldots, b_n \rangle$. Aiomme todistaa, että A on aliryhmiensä $\langle a_1 \rangle$ ja B:n suora summa. Koska $\langle a_1 \rangle \bigcap B = 0$, riittää todistaa, että $A = a_i + B$. Jos $a = mf_1 + b \in A$ missä $b \in F_{n-1}$ ja taas jakoyhtäkön perusteella $m = qm_1 + r, (0 \leq r < m_1)$. Tarkastelemme alkiota $a - qa_1 = mf_1 + b - qa_1 = (qm_1 + r)f_1 + b - q(m_1 f_1) = rf_1 + b \in A$, joten sillä on esitys kannassa (1). Jakoyhtäkön perusteella kanta-alkion f_1 kerroin on $r < m_1$, joten $r = 0$. Tästä seuraa, että $b = a - qa_1 \in A$ ja $b \in B$. Koska a oli mielivaltainen A:n alkio, saamme

$$A = \langle a_1 \rangle \oplus B.$$

Induktiivisen hypoteesin perusteella aliryhmällä B ja ryhmällä F_{n-1} on kannat $\{a_2, \ldots a_k\}$ ja $\{f_2, \ldots, f_n\}$, missä $k \leq n$, $a_i = m_i f_i, (2 \leq i \leq k)$ ja $m_i \mid m_{i+1}$ kaikille $2 \leq i < k$. Luonnollisesti joukot $\{a_1, \ldots, a_n\}$ ja $\{f_1, \ldots, f_n\}$ ovat kannat ryhmille A ja F_n. Jotta nämä kannat toteuttavat halutut ominaisuudet, riittää todistaa, että $m_1 \mid m_2$.

Olkoon $m_2 = \hat{q} m_1 + \hat{r}$, $0 \leq r < m_1$. Jos kirjoitamme alkion $a_2 - a_1 \in A$ uuden kannan $\{\hat{q} f_2 - f_1, f_2, \ldots, f_n\}$ mukaisesti, saamme

$$a_2 - a_1 = m_1(\hat{q} f_2 - f_1) + \hat{r} f_2.$$

Koska f_2:n kerroin on $\hat{r} < m_1$, voimme päätellä, kuten aina ennenkin, että $\hat{r} = 0$, joten $m_1 \mid m_2$, kuten vaadittua. □

Lause 4.9. *Jokainen äärellisesti viritetty Abelin ryhmä on syklisten aliryhmien suora summa. Eli se voidaan kirjoittaa muotoon*

$$A = C_{m_1} \bigoplus C_{m_2} \bigoplus \cdots \bigoplus C_{m_k} \bigoplus \mathbb{Z} \bigoplus \mathbb{Z} \bigoplus \cdots \bigoplus \mathbb{Z},$$

jossa $1 < m_1 \mid m_2 \mid m_3 \mid \cdots \mid m_k \neq 0$. Hajotelmassa m_i:t on määritelty yksikäsitteisesti, kuten myös äärettömien syklisten ryhmien $\mathbb{Z}$ määrä, jota kutsutaan äärettömän Abelin ryhmän torsio-vapaaksi rankiksi..

Todistus. Olkoon G äärellisesti viritetty Abelin ryhmä, jonka virittää n alkiota. Silloin G on isomorfinen jonkun vapaan ryhmän F_n tekijäryhmän F_n/A kanssa. Edellisen lauseen perusteella, ryhmät F_n ja A sisältävät kannat $f_1, \ldots, f_n$ ja $a_1, \ldots, a_k$, jolle pätee $a_i = m_i f_i$ kaikille $1 \leq i \leq k$. Koska $G \cong F_n/A$, lauseen todistukseen riittää osoittaa, että F_n/A on syklisten aliryhmiensä $< f_i + A >$ suora summa.

Ensiksikin, on selvää, että F_n/A on aliryhmien $< f_i + A >$ virittämä. Seuraavaksi oletamme, että nolla-alkio tekijäryhmässä F_n/A voidaan kirjoittaa muotoon $A = l_1 f_1 + \cdots + l_n f_n + A$. Tästä seuraa, että $l_1 f_1 + \cdots + l_n f_n = a \in A$. Kun kirjoitamme alkion a ylläolevan A:n kannan mukaan ja käytämme yhtälöä $a_i = m_i f_i$, voimme kirjoittaa seuraavat yhtälöt

$$l_1 f_1 + \cdots + l_n f_n = s_1 a_1 + \cdots + s_k a_k = s_1 m_1 f_1 + \cdots + s_k m_k f_k.$$

Koska jokainen alkio voidaan esittää yksikäsitteisesti vapaitten generaattorien f_i avulla, saamme, että $l_i = s_i m_i$ $(1 \leq i \leq k), l_j = 0, k < j \leq n$.

Tämä kuitenkin tarkoittaa, että kaikki alkiot $l_i f_i$ kuuluvat A:n, eli $l_i f_i + A = A$. Tämä antaa vaaditun yksikäsitteisyyden nolla-alkion esitykselle aliryhmän $< f_i + A >$ alkioitten summana. □

Esimerkki 4.10. Kuinka monta Abelin ryhmää on, joiden kertaluku on $243 = 3^5$? Abelin ryhmien peruslauseen nojalla, kukin tällainen ryhmä $A = C_{d_1} \bigoplus \cdots \bigoplus C_{d_k}$, missä $d_1 \mid d_2 \mid \cdots \mid d_k$ ja $d_1 d_2 \ldots d_k = 3^5$. Vaihtoehdot ovat

$$\begin{aligned}
C_3 \bigoplus C_3 \bigoplus C_3 \bigoplus C_3 \bigoplus C_3 \\
C_3 \bigoplus C_3 \bigoplus C_3 \bigoplus C_9 \\
C_3 \bigoplus C_9 \bigoplus C_9 \\
C_3 \bigoplus C_3 \bigoplus C_{27} \\
C_9 \bigoplus C_{27} \\
C_3 \bigoplus C_{81} \\
C_{243}
\end{aligned}$$

Ryhmiä on siis täsmälleen yhtä paljon kuin luvun 5 osituksia.

Tehtävä 26.

1. Luokittele Abelin ryhmät, joiden koko on 60.
2. Kuinka monta Abelin ryhmää on, joiden koko on 17^7?
3. Kuinka monta Abelin ryhmää on, joiden koko on 2^{10}?

4.5 Vapaitten Abelin ryhmien aliryhmät

Äärettömällä syklisellä ryhmällä $\mathbb{Z}$ on vain yksi aliryhmä kutakin äärellistä indeksiä n, eli tietysti $n\mathbb{Z}$. Kuinka monta aliryhmää on $\mathbb{Z}^2$:ssa? Luokittelu ei äärettömien ryhmien tapauksessa ole järkevää, tai mahdollista. Äärellisesti viritetyissä ryhmissä voimme kuitenkin laskea aliryhmien määrän indeksin mukaan.

Määritelmä 4.11. Määritellään funktio $a_n(G)$ kirjoittamaan muistiin niiden aliryhmien määrä, joiden indeksi on täsmälleen n.

Esimerkki 4.12. Ylläolevan nojalla $a_n(\mathbb{Z}) = 1$ kaikille $n \geq 1$, koska jokaista indeksiä kohden on täsmälleen yksi aliryhmä.

Tarkastelemme $\mathbb{Z} \bigoplus \mathbb{Z}$:n aliryhmiä. Kuinka monta niitä on kutakin indeksiä n? Ensimmäinen epätriviaalitapaus on indeksi 2. Ainakin $2\mathbb{Z} \bigoplus \mathbb{Z}$ ja $\mathbb{Z} \bigoplus 2\mathbb{Z}$ ovat kumpainenkin indeksiltään kaksi. Onko muita? Itseasiassa on vielä kolmas aliryhmä, jonka indeksi on kaksi. Huomaa nimittäin, että suoran summan (tai tulon) kaikki aliryhmät eivät ole yksinkertaisesti pelkästään jommankumman komponentin aliryhmiä. Muistamme, että esimerkissä $C_2 \times C_2$ löysimme yhteensä kolme aliryhmää, jotka olivat indeksiltään kaksi ja isomorfisia C_2:n kanssa, eli $(1,0), (0,1), (1,1)$ generoimat aliryhmät. Vain kaksi ensimmäistä saadan suoraan komponenttien aliryhmänä. Tarvitsemme järeämpiä työkaluja.

Ensiksikin olemme todistaneet Lauseessa 4.8, että jos A on vapaan Abelin ryhmän F_k aliryhmä, on A:n kanta on rankiltaan pienempi tai yhtäsuuri kuin k. Eli tässä tapauksessa $\mathbb{Z} \bigoplus \mathbb{Z}$:n aliryhmän virittää korkeintaan kaksi alkiota. Koska tarkastelemme aliryhmiä, joiden indeksi on äärellinen luku n, huomaamme, että yhden alkion virittämä aliryhmä ei kelpaa, sillä sen tekijäryhmä on ääretön, $\mathbb{Z} \bigoplus \mathbb{Z}/m\mathbb{Z}$ ja näin ollen myös indeksi on ääretön. Äärellistä indeksiä olevan aliryhmän tulee siis kahden alkion virittämä.

Voimme esittää tämän kannan 2×2-matriisin lineaarisesti riippumattomina riveinä (ajattele taas vektoriavaruuksia ja aliavaruuksia), joten ongelma kutistuu matriisien laskemiseen joukossa $\mathbb{M}_2(\mathbb{Z})$. On toisaalta mahdollista, että kaksi matriisia M ja N virittävät saman aliryhmän, mutta eri kannassa. Tämä tapahtuu täsmälleen silloin kun voimme riviredusoita (vastaa kannan vaihtoa) kummankin matriisin samaksi yläkolmiomatriisiksi. Huomaa, että riviredusoinnissa $\mathbb{Z}$:n yli saa kertoa matriisin rivin vain ± 1:llä (tämä on edelleen kanta), vaihtaa rivien järjestystä (uudelleenjärjestää kannan) ja lisätä kokonaisluku-kertaa rivin toiseen riviin (osoita, että tämäkin on kanta). Kaikki nämä operaatiot pitävät matriisin determinantin vakiona, ja matriisin determinantti määrää täsmälleen aliryhmän indeksin. Näillä operaatioilla

(erityisesti jakoyhtälöä käyttämällä), kukin matriisi saadaan yläkolmiomuotoon

$$\begin{pmatrix} m_{11} & m_{12} \\ 0 & m_{22} \end{pmatrix},$$

missä $0 \leq m_{12} < m_{22}$. Joten tällaiset yläkolmiomatriisit siis esittävät kunkin aliryhmän yksikäsitteisesti. Tällaisen matriisin determinantti on tietysti $m_{11}m_{22}$, joten indeksiä kaksi olevat aliryhmät ovat sellaisia, joissa $m_{11}m_{22} = 2$. Jos valitsemme $m_1 1 = 1$, niin $m_{22} = 2$, mikä jättää alkiolle m_{12} kaksi vaihtoehtoa. Jos $m_{11} = 2$ ja $m_{22} = 1$, on $m_{12} = 0$, joten on vain yksi vaihtoehto. Yhteensä on kolme vaihtoehtoa.

Yleisemmin saamme kertoimeksi $a_n(n) = \sigma(n)$.

Määritelmä 4.13. Olkoon n luonnollinen luku. Määrittelemme funktion $\sigma(n)$ laskemaan niiden luonnollisten lukujen summan, jotka jakavat luvun n. Esimerkiksi $\sigma(p) = p + 1$ kaikille alkuluvuille p ja $\sigma(p^n) = 1 + p + \cdots + p^n$. Toisaalta $\sigma(6) = 1 + 2 + 3 + 6 = 10$.

Tehtävä 27. Osoita, että σ on multiplikatiivinen, eli jos $(n, m) = 1$, silloin $\sigma(nm) = \sigma(n)\sigma(m)$.

Tehtävä 28. Numeroimalla sopivat kaksi kertaa kaksi yläkolmiomatriisit, todista, että ryhmälle $\mathbb{Z} \bigoplus \mathbb{Z}$, funktio $a_n(n) = \sigma(n)$. Helpointa on varmastikin lähteä pienistä erikoistapauksista liikkeelle.

4.5.1 Esseen aihe

Jos haluamme laskea aliryhmiä yleisemmin $\mathbb{Z}^d$:ssä, on hyödyllistä määritellä generoiva funktio

$$\zeta_{\mathbb{Z}^d}(s) = \sum_{n=1}^{\infty} a_n n^{-s},$$

missä kertoimet a_n ovat kuten määritelmässä 4.11, ja $s \in \mathbb{C}$. Tämä voidaan aluksi mieltää formaalina summana, mutta itseasiassa Abelin ryhmille tämä funktio suppenee aina kun $\Re(s) > d$.

Esimerkki 4.14. Laskujemme nojalla

$$\zeta_{\mathbb{Z}}(s) = \sum_{n=1}^{\infty} n^{-s} = \zeta(s),$$

joka on siis Riemannin zeeta-funktio. Toisaalta

$$\zeta_{\mathbb{Z}^2}(s) = \sum_{n=1}^{\infty} \sigma(n) n^{-s} = \zeta(s)\zeta(s-1).$$

Todista, että

$$\zeta_{\mathbb{Z}^d}(s) = \zeta(s)\zeta(s-1)\dots\zeta(s-(d-1)).$$

Tälle tulokselle on ainakin viisi todistusta. Osoita myös, että tällä funktiolla on Eulerin tulo, sekä ryhmäteoreettisesti, että lukuteoreettisesti. Määrittele aliryhmäin kasvu ja sen indeksi. Lähteeksi sopii esim. du Sautoy, The quest for order vs flight from ennui. Artikkelin löytää verkosta sivulta www.maths.ox.ac.uk/ dusautoy/newright.htm valikosta Preprints.