Tero Harju (2008/2010)

Äärellisesti generoitujen Abelin ryhmien peruslause

Merkintä $|X|$ on joukon koko (eli $\#X$).

Vapaat Abelin ryhmät

Tässä kappaleessa käytetään Abelin ryhmille additiivista merkintää.

Abelin ryhmä G on joukon $B = \{a_1, a_2, \ldots, a_n\}$ generoima **vapaa Abelin ryhmä**, jos jokainen $g \in G$ voidaan esittää yksikäsitteisesti muodossa

$$g = m_1 a_1 + m_2 a_2 + \ldots + m_n a_n \quad (m_i \in \mathbb{Z}).$$

Tässä tapauksessa B on ryhmän G **kanta**.

<u>Esimerkki</u> 1.1. Ryhmä $\mathbb{Z}$ on vapaa: joukot $\{1\}$ ja $\{-1\}$ ovat sen kantoja. Yleisemmin $\mathbb{Z}^n = \mathbb{Z} \oplus \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}$ on vapaa kantana $\{e_1, e_2, \ldots, e_n\}$, missä $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$.

Todetaan, ettei vapaan Abelin ryhmän nolla-alkio 0 voi kuulua mihinkään kantaan, sillä $0 + 0 = 0$ antaa kaksi esitystä joukon $\{0, \ldots\}$ suhteen.

<u>Esimerkki</u> 1.2. Toisaalta $\mathbb{Z}_2$ ei ole vapaa, sillä muutoin sen kantana olisi välttämättä $\{1\}$, mutta esimerkiksi $2 \cdot 1 + 1 \equiv 1 \pmod 2$ eli alkiolla 1 on useita esityksiä.

<u>Lemma</u> 1.1. *Olkoon G äärellisesti generoitu Abelin ryhmä. Tällöin sen kaikki minimaaliset generoijajoukot ovat äärellisiä.*

Todistus. Harjoitustehtävä. □

<u>Lause</u> 1.1. *Olkoon G äärellisesti generoitu vapaa Abelin ryhmä. Tällöin ryhmän G jokaisessa kannassa on yhtä monta alkiota. Tätä lukua kutsutaan ryhmän G* ***asteeksi****.*

Todistus. Edeltävän mukaan ryhmällä G on (äärellinen) kanta $B = \{a_1, \ldots, a_n\}$. Tarkastellaan ryhmän G aliryhmää $2G = \{2g \mid g \in G\} \trianglelefteq G$, ja sen tekijäryhmää $G/2G = \{g + 2G \mid g \in G\}$. Kun $g \in G$, niin $g = \sum m_i a_i$ joillain $m_i \in \mathbb{Z}$, sanokaamme $m_i = 2k_i + r_i$, missä $0 \le r_i \le 1$. Siten

$$g + 2G = \sum_{i=1}^{n} (2k_i + r_i) a_i + 2G = \sum_{i=1}^{n} r_i a_i + 2 \sum_{i=1}^{n} k_i a_i + 2G = \sum_{i=1}^{n} r_i a_i + 2G\,.$$

Tässä $r_i \in \{0, 1\}$ ja siten $|G/2G| = 2^n$, missä $|G/2G|$ on riippumaton kannan B valinnasta. Näin ollen jokaisessa kannassa on tarkalleen n alkiota. □

Lause 1.2. *Olkoon G astetta n oleva vapaa Abelin ryhmä kantana $B = \{a_1, a_2, \ldots, a_n\}$ ja olkoon H Abelin ryhmä. Tällöin jokainen kuvaus $f' \colon B \to H$ laajenee yksikäsitteisesti homomorfismiksi $f \colon G \to H$, missä $f(a_n) = f'(a_n)$.*

Todistus. Määritellään

$$f(m_1 a_1 + \ldots + m_n a_n) = m_1 f'(a_1) + \ldots + m_n f'(a_n)\,,$$

jolloin väite todetaan helposti oikeaksi. □

Lause 1.3. *Samaa astetta olevat vapaat Abelin ryhmät G_1 ja G_2 ovat isomorfiset.*

Todistus. Olkoot $B_1 = \{a_1, a_2, \ldots, a_n\}$ ja $B_2 = \{b_1, b_2, \ldots, b_n\}$ vastaavasti näiden ryhmien kantoja. Tällöin kuvaus $f' \colon B_1 \to G_2$ ehdosta $f'(a_i) = b_i$ laajenee homomorfismiksi $f \colon G_1 \to G_2$. Kuvaus f on surjektiivinen, sillä B_2 generoi ryhmän G_2, ja se on injektiivinen, koska B_2 on kanta. Täten f on isomorfismi. □

Edeltävän nojalla saadaan:

Lause 1.4. *Jokainen astetta n oleva vapaa Abelin ryhmä on isomorfinen ryhmän $\mathbb{Z}^n = \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}$ kanssa.*

Lause 1.5. *Jokainen äärellisesti generoitu Abelin ryhmä on vapaan Abelin ryhmän homomorfinen kuva.*

Todistus. Olkoon $G = \langle g_1, \ldots, g_n \rangle$ ja olkoon $B = \{e_1, \ldots, e_n\}$ astetta n olevan vapaan Abelin ryhmän H kanta. Tällöin kuvaus $f' \colon B \to G$ ehdosta $f'(e_i) = g_i$ laajenee homomorfismiksi $f \colon H \to G$, joka on surjektiivinen. Täten $G = f(H)$. □

Tässä on erityisesti $G \cong H/\operatorname{Ker}(f)$.

Torsiovapaat ryhmät

Ryhmä G on **torsioryhmä**, jos sen jokaisen alkion g kertaluku $\operatorname{ord}(g)$ on äärellinen. Ryhmä G on **torsiovapaa**, jos jokaisen alkion $a \neq 1$ kertaluku on ääretön.

Esimerkki 1.3. Abelin ryhmät $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ja $\mathbb{C}$ ovat torsiovapaita yhteenlaskun suhteen. Tekijäryhmä $\mathbb{Q}/\mathbb{Z}$ on torsioryhmä, sillä $p \cdot (q/p) \in \mathbb{Z}$ kaikille $q/p \in \mathbb{Q}$. Kertolaskun suhteen $\mathbb{Q} \setminus \{0\}$ on torsiovapaa, mutta $\mathbb{C} \setminus \{0\}$ ei ole.

Vuonna 1902 Burnside esitti seuraavan ongelman: Ovatko äärellisesti generoidut torsioryhmät välttämättä äärellisiä? Kysymys sai negatiivisen vastauksen, kun Golod ja Shafarevich (1964) osoittivat, että on olemassa kolmen alkion generoima ääretön ryhmä, jonka alkioiden kertaluvut ovat alkuluvun p potensseja. Adjan ja Novikov (1968) todistivat, että kun $n \geq 4381$ on pariton luku, niin on olemassa kahden alkion generoima ääretön ryhmä, jossa $g^n = 1$ kaikille g.

Olkoon G Abelin ryhmä. Alkio $g \in G$ on **torsioalkio**, jos on $n \geq 1$, jolla $ng = 0$. Merkitään

$$T(G) = \{g \in G \mid g \text{ torsioalkio}\}.$$

Lause 1.6. *Olkoon G Abelin ryhmä. Tällöin $T(G) \trianglelefteq G$ on torsioryhmä ja $G/T(G)$ on torsiovapaa.*

Todistus. Selvästi $0 \in T(G)$. Jos $g_1, g_2 \in T(G)$, sanokaamme $ng_1 = 0$ ja $mg_2 = 0$, niin $nm(g_1 - g_2) = 0$ ja siten $g_1 - g_2 \in T(G)$. Siis $T(G) \leq G$. Myös $T(G) \trianglelefteq G$, koska G on Abelin ryhmä.

Jos $g + T(G) \in G/T(G)$ ja $n(g + T(G)) = ng + T(G) = T(G)$ (ryhmän $G/T(G)$ nolla-alkio), niin $m(ng) = 0$ jollain $m \geq 1$, eli $g \in T(G)$, ja siten $g + T(G) = T(G)$. □

Esimerkki 1.4. Todetaan, että $T(\mathbb{Z} \oplus \mathbb{Z}_2) = \{(0,0), (0,1)\}$ ja $\mathbb{Z} \oplus \mathbb{Z}_2/T(\mathbb{Z} \oplus \mathbb{Z}_2) \cong \mathbb{Z}$.

Lause 1.7. *Äärellisesti generoitu Abelin ryhmä G on vapaa jos ja vain jos se on torsiovapaa.*

Todistus. Ensinnä, jos G on vapaa, niin $G \cong \mathbb{Z}^n$ jollain n, ja näin ollen $T(G) = \{0\}$.

Toisaalta, oletetaan, että G on torsiovapaa, ja $G = \langle g_1, \ldots, g_n \rangle$, missä n on minimaalinen. Todistetaan väite induktiolla lukuun n.

Jos $n = 1$, niin $G = \langle g_1 \rangle \cong \mathbb{Z}$, joten väite on selvä. Olkoon sitten $n \geq 2$ ja että jollain $g \in G$ on kaksi esitystä generaattorien avulla:

$$g = m_1 g_1 + \ldots + m_n g_n = m_1' g_1 + \ldots + m_n' g_n \quad (m_i, m_i' \in \mathbb{Z}).$$

Vähentämällä toisistaan saadaan

$$k_1 g_1 + k_2 g_2 + \ldots + k_n g_n = 0 \quad (k_i \in \mathbb{Z}). \tag{1.1}$$

Oletetaan nyt, että (1.1) on valittu niin, että $\sum |k_i|$ on pienin mahdollinen. Tällöin varmastikin $\operatorname{syt}(k_1, \ldots, k_n) = 1$. (Muutoin jaetaan yhteinen tekijä pois vedoten ryhmän G torsiovapauteen.) Todetaan, että $|k_i| \neq 1$, sillä muutoin g_i voidaan lausua muiden generaattorien avulla vastoin luvun n minimaalisuutta. Voidaan olettaa myös, että $0 < |k_2| \leq |k_1|$, sanokaamme $k_1 = sk_2 + r$, missä $0 \leq r < |k_2|$. Merkitään $g_2' = g_2 + sg_1$. Nyt

$$rg_1 + k_2 g_2' + k_3 g_3 + \ldots + k_n g_n = 0\,.$$

Siis $G = \langle g_1, g_2', \ldots, g_n \rangle$, missä $0 \leq r < |k_1|$ vastoin summan $\sum |k_i|$ minimaalisuutta. Tämä on ristiriita todistaa väitteen. □

Äärellisesti generoidut Abelin ryhmät

Muistetaan, että Abelin ryhmä G on aliryhmiensä H ja N suora summa, eli $G = H \oplus N$, jos jokainen $g \in G$ voidaan esittää yksikäsitteisesti muodossa $g = a + b$, missä $a \in H$ ja $b \in N$. Vielä: $G = H \oplus N$ jos ja vain jos $H \cap N = \{0\}$ ja $G = H + N$.

Lause 1.8. *Olkoon G äärellisesti generoitu Abelin ryhmä. Tällöin*

$$G \cong T(G) \oplus G/T(G)\,,$$

missä $T(G)$ on äärellinen ja $G/T(G)$ on vapaa Abelin ryhmä, eli

$$G \cong T(G) \oplus \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}\,.$$

Todistus. Lauseen 1.6 mukaan $G/T(G)$ on torsiovapaa, ja lauseen 1.7 mukaan se on vapaa. Olkoon

$$\{e_1 + T(G), e_2 + T(G), \ldots, e_k + T(G)\} \quad (e_i \in G)$$

ryhmän $G/T(G)$ jokin kanta, ja merkitään $B = \{e_1, e_2, \ldots, e_k\}$. Merkitään $H = \langle B \rangle$. Jos nyt $\sum_{i=1}^{k} m_i e_i = 0$ joillain $m_i \in \mathbb{Z}$, niin myös $\sum_{i=1}^{k} m_i(e_i + T(G)) = T(G)$ $(= 0_{G/T(G)})$, ja siis vapauden perusteella $m_i = 0$ kaikilla i. Näin ollen H on vapaa, ja siten $H \cong G/T(G)$ lauseen 1.3 mukaan.

Väite 1. $G \cong T(G) \oplus H$.

Tod. Kun $g \in G$, niin on luvut $m_i \in \mathbb{Z}$, joilla

$$g + T(G) = \sum_{i=1}^{k} m_i\,(e_i + T(G)) = \left(\sum_{i=1}^{k} m_i e_i\right) + T(G)\,,$$

toisin sanoen $g - \sum m_i e_i \in T(G)$, ja siten on alkio $a \in T(G)$, jolla $g = a + \sum m_i e_i \in T(G) + H$. Siis $G = T(G) + H$.

Toisaalta jos $a_1 + \sum m_i e_i = a_2 + \sum n_i e_i$ joukossa $T(G) + H$, niin $\sum (m_i - n_i) e_i = a_2 - a_1 \in T(G)$, ja siten on luku $n \in \mathbb{Z}$, $n \neq 0$, niin, että $0 = n \cdot \sum (m_i - n_i) e_i = \sum n(m_i - n_i) e_i$. Mutta B on ryhmän H kanta, joten $n(m_i - n_i) = 0$ kaikilla i, eli $m_i = n_i$ kaikilla i. Lopulta myös $a_2 = a_1$, ja väite 1 on todistettu.

On osoitettu, että $G \cong T(G) \oplus G/T(G)$, missä $G/T(G)$ on vapaa.

Väite 2. $T(G)$ on äärellinen.

Olkoon $G = \langle g_1, g_2, \ldots, g_n \rangle$, missä edeltävän nojalla $g_i = a_i + h_i$ joillain $a_i \in T(G)$ ja $h_i \in H$. Kun $a \in T(G)$, on se muotoa $a = \sum m_i g_i = \sum m_i a_i + \sum m_i h_i$, missä $\sum m_i h_i \in T(G) \cap H = \{0\}$ suoran summan ominaisuuden perusteella. Siis $a = \sum m_i a_i$. Olkoot $r_i a_i = 0$ eli $\operatorname{ord}(a_i) = r_i$, kun $i = 1, 2, \ldots, n$. Tällöin jokainen $g \in T(G)$ on edeltävän mukaisesti muotoa $a = \sum m_i a_i$, missä $m_i < r_i$. Näin ollen $|T(G)| \leq r_1 r_2 \cdots r_n$, mikä todistaa väitteen. $\square$

Äärelliset Abelin ryhmät

Seuraava tulos liittyy jo Sylowin lauseisiin. Sitä varten, olkoon p alkuluku. Joukko

$$G_p = \{g \mid p^k \cdot g = 0 \text{ jollain } k \geq 0\}$$

on ryhmän G (p-)**primäärinen komponentti**.

Lemma 1.2. *Olkoon G kertalukua $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ oleva Abelin ryhmä, missä $p_1, \ldots, p_k$ ovat luvun n eri alkulukutekijät. Tällöin*

$$G \cong G_{p_1} \oplus G_{p_2} \oplus \ldots \oplus G_{p_k}.$$

Todistus. Abelin ryhmälle $G_p \leq G$ kuten helposti todetaan.

Olkoon $g \in G$, $g \neq 0$, ja $\operatorname{ord}(g) = n = p_1^{c_1} \cdots p_k^{c_k}$, missä kukin $c_i \in \mathbb{Z}$ (mahdollisesti 0). Merkitään $n_i = n/p_i^{c_i}$, jolloin $\operatorname{syt}(n_1, n_2, \ldots, n_k) = 1$, ja näin ollen on olemassa luvut $m_1, \ldots, m_k$ niin, että $\sum_{i=1}^{k} m_i n_i = 1$. Nyt

$$g = \left(\sum_{i=1}^{k} m_i n_i \right) g = (m_1 n_1) g + \ldots + (m_k n_k) g\,.$$

Tässä $p_i^{c_i}(m_i n_i) g = (m_i n) g = 0$, sillä $\operatorname{ord}(g) = n$. Siis $(m_i n_i) g \in G_{p_i}$ kaikilla i, ja näin ollen $g \in G_{p_1} + G_{p_2} + \ldots + G_{p_k}$. Täten

$$G = G_{p_1} + G_{p_2} + \ldots + G_{p_k}.$$

Toisaalta, jos $g \in G_{p_i} \cap \big(G_{p_1} + \ldots + G_{p_{i-1}} + G_{p_{i+1}} + \ldots + G_{p_k}\big)$, niin $p_i^e g = 0$ jollain e, ja siten $\operatorname{ord}(g) = p_i^t$ jollain $t \leq e$. Myös $g = \sum_{j \neq i} g_j$, missä $g_j \in G_{p_j}$, sanokaamme $p_j^{d_j} g_j = 0$. Kun $m = p_1^{d_1} \cdots p_{i-1}^{d_{i-1}} \cdot p_{i+1}^{d_{i+1}} \ldots p_k^{d_k}$, niin $mg = 0$, ja siten $\operatorname{ord}(g) | m$. Mutta $p_i \nmid m$; ristiriita. Näin ollen jokaisella alkiolla g on yksikäsitteinen esitys summassa $G_{p_1} + G_{p_2} + \ldots + G_{p_k}$, ja väite seuraa. $\square$

Ryhmä G on p-**ryhmä**, jos sen kertaluku on alkuluvun potenssi. Lagrangen lauseen nojalla p-ryhmän jokaisen alkion kertaluku on saman alkuluvun p potenssi. Jokainen Abelin ryhmän primäärinen komponentti on siis p-ryhmä.

Lause 1.9. *Jokainen Abelin p-ryhmä G on syklisten ryhmien suora summa.*

Todistus. Olkoon $g \in G$ alkio jonka kertaluku on mahdollisimman suuri, ja merkitään $H = \langle g \rangle$, jolloin $|H| = p^n$ jollain $n \geq 1$. Voidaan olettaa, että $H \neq G$. (Muutoin G on syklinen.)

Väitetään, että $G = H \oplus F$ jollekin aliryhmälle $F \leq G$. Koska tässä F on myös p-ryhmä, lopullinen väite seuraa induktiivisesti.

Väite ($*$). On olemassa $C \leq G$, jolle $H \cap C = \{0\}$ ja $C \cong \mathbb{Z}_p$.

Tod. Olkoon $a \in G \setminus H$ ja olkoon alkion $a + H \in G/H$ kertaluku p^r, missä $r \geq 1$. Tällöin $p^r a \in H = \langle g \rangle$, joten $p^r a = sg$ jollekin $s \in \mathbb{Z}$. Koska $\operatorname{ord}(g) = p^n$ on

mahdollisimman suuri, niin $p^n a = 0$, ja siten $p^n a = (sp^{n-r})g = 0$. Siis p^n jakaa luvun sp^{n-r}, jolloin $p|s$, koska $r \neq 0$. Olkoon $s = ps'$. Valitaan

$$a_1 = p^{r-1}a - s'g \quad \text{ja} \quad C = \langle a_1 \rangle,$$

jolloin $pa_1 = p^r a - ps'g = sg - sg = 0$. Siis $\mathrm{ord}(a_1) = p$ ja näin ollen $|C| = p$. Siten $C \cong \mathbb{Z}_p$. Lisäksi $C \cap H = \{0\}$, sillä $a_1 \notin H$ (koska $p^{r-1}a \notin H$). Tämä todistaa väitteen $(*)$.

Etsitään sitten F induktiivisesti. Tätä varten olkoon $f\colon G \to G/C$ luonnollinen homomorfismi, eli $f(a) = a + C$. Nyt $f(H) = \langle g + C \rangle$ on tekijäryhmän G/C syklinen aliryhmä, jonka kertaluku on mahdollisimman suuri p^n. Koska $|G/C| < |G|$ ja G/C on p-ryhmä, induktio osoittaa, että

$$G/C \cong f(H) \oplus \bar{F} \tag{1.2}$$

jollain $\bar{F} \leq G/C$. Merkitään $F = f^{-1}(\bar{F})$. Nyt $F \leq G$ ja $C \subseteq F$ (sillä $C = 0_{G/C}$). Edelleen

$$\begin{aligned} h \in G &\implies h + C = m(g + C) + (d + C) \qquad (\text{sillä } (1.2) : d + C \in \bar{F}) \\ &\implies h - mg - d \in C \\ &\implies h = mg + (d + c) \in H + F \qquad (c \in C,\ d + c \in F)\,. \end{aligned}$$

Siis $G = H + F$. Toisaalta

$$\begin{aligned} h \in H \cap F &\implies f(h) \in f(H) \cap f(F) = f(H) \cap \bar{F} = \{0\} \qquad (\text{sillä } 1.2) \\ &\implies h \in \mathrm{Ker}(f) = C \\ &\implies h \in H \cap C \\ &\implies h = 0\,. \end{aligned}$$

Näin ollen $G = H \oplus F$. □

Seuraava tulos on Abelin ryhmien peruslause.

<u>Lause</u> 1.10. *Olkoon G äärellisesti generoitu Abelin ryhmä. Tällöin*

$$G \cong \mathbb{Z} \oplus \ldots \oplus \mathbb{Z} \oplus H,$$

missä H on äärellinen Abelin ryhmä, joka voidaan kirjoittaa muotoon

$$H \cong \mathbb{Z}_{p_1^{r_1}} \oplus \mathbb{Z}_{p_2^{r_2}} \oplus \ldots \oplus \mathbb{Z}_{p_n^{r_n}}\ ,$$

missä jokainen p_i on alkuluku (jotka eivät välttämättä ole erisuuria). Tämä esitys on yksikäsitteinen komponenttien järjestystä lukuunottamatta.

Todistus. Väitteen alkuosa on osoitettu lauseessa 1.8. Äärellisiä Abelin ryhmiä koskeva väite seuraa lauseesta 1.9, sillä jokainen syklinen ryhmä on isomorfinen jonkun ryhmän $\mathbb{Z}_m$ kanssa. □

<u>Lause</u> 1.11. *Olkoon G äärellinen Abelin ryhmä. Tällöin se on muotoa*

$$G \cong \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \ldots \oplus \mathbb{Z}_{d_t},$$

missä $d_i | d_{i+1}$ jokaisella i.

Todistus. Tiedetään, että $G \cong G_{p_1} \oplus \ldots \oplus G_{p_m}$ (luvut p_i ovat erisuuria alkulukuja), missä jokainen primäärinen komponentti

$$G_{p_i} = C_{i1} \oplus C_{i2} \oplus \ldots \oplus C_{ik} \quad \text{niin, että } |C_{ij}| \leq |C_{i(j+1)}| \tag{1.3}$$

on syklisten ryhmien C_{ij} suora summa. Tässä siis $|C_{ij}|$ jakaa kertaluvun $|C_{i(j+1)}|$, koska molemmat ovat alkuluvun p_i potensseja. Liittämällä tarvittaessa loppuun triviaaleja aliryhmiä $\{0\}$ voidaan olettaa, että esityksen (1.3) pituus k on sama kaikille p_i. Nyt

$$H_j = C_{1j} \oplus \ldots \oplus C_{kj}$$

on syklinen ryhmä, koska alkuluvut p_i ovat erisuuria (harjoitustehtävä). Selvästi $|H_j|$ jakaa kertaluvun $|H_{j+1}|$, ja lisäksi $G \cong H_1 \oplus H_2 \oplus \ldots \oplus H_k$ kuten vaadittua. $\square$