5. Aliryhmät

Luvun 4 esimerkeissä esiintyy usein ryhmä $(G, *)$ ja jokin vakaa osajoukko $B \subset G$ siten, että $(B, *|_B)$ on ryhmä. Määrittelemme seuraavassa käsitteitä, jotka auttavat tällaisten tilanteiden käsittelyssä. Osajoukko $A \subset B$ on joukon B aito osajoukko, jos $A \neq B$.

Määritelmä 5.1. Olkoon G ryhmä. Olkoon $B \subset G$, $B \neq \emptyset$, vakaa osajoukko. Jos indusoidulla laskutoimituksella varustettu joukko B on ryhmä, niin se on ryhmän G *aliryhmä*. Jos $H \subset G$ on ryhmän G aliryhmä, käytämme merkintää $H \leq G$. Jos aliryhmä H on ryhmän G aito osajoukko, se on *aito aliryhmä* ja voimme käyttää merkintää $H < G$.

Merkinnät $H \leq G$ ja $H' < G$ sisältävät tietojen $H, H' \subset G$ ja $H' \neq G$ lisäksi siis sen, että H ja H' ovat ryhmiä, joiden laskutoimitus on ryhmän G laskutoimituksen indusoima. Seuraava tulos antaa keinon tarkastaa, onko jokin ryhmän osajoukko aliryhmä:

Propositio 5.2. *Ryhmän G osajoukko $H \neq \emptyset$ on aliryhmä, jos*

(1) *kaikilla $x, y \in H$ pätee $xy^{-1} \in H$, tai*
(2) *kaikilla $x, y \in H$ $xy \in H$ ja $y^{-1} \in H$.*

Todistus. Olkoon $e \in G$ neutraalialkio. Tarkastellaan ehtoa (1): Olkoon $h \in H$. Oletuksen mukaan $hh^{-1} \in H$, joten $e \in H$. Samoin $y^{-1} = ey^{-1} \in H$ kaikilla $y \in H$. Kaikki on siis kunnossa, jos H on vakaa osajoukko. Edellisen nojalla kaikille $x, y \in H$ pätee $xy = x(y^{-1})^{-1} \in H$.

Ehdosta (2) seuraa ehto (1), joten väite seuraa kohdasta (1). □

Esimerkki 5.3. (a) Jokaisella ryhmällä on aliryhmiä: ryhmä itse, ja neutraalialkion muodostama yhden alkion ryhmä.

(b) $(\{0\}, +) < (\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +) < (\mathbb{C}, +)$.

(c) $\{1\} < \{-1, 1\} < \mathbb{Q}^\times < \mathbb{R}^\times < \mathbb{C}^\times$.

(d) Neliömatriiseista koostuville ryhmille pätee muunmuassa

$$\{I_n\} < \{-I_n, I_n\} < \mathrm{GL}_n(\mathbb{Q}) < \mathrm{GL}_n(\mathbb{R}) < \mathrm{GL}_n(\mathbb{C})$$

kaikilla $n \geq 2$ ja

$$\{I_n\} < \{-I_n, I_n\} < \mathrm{SL}_n(\mathbb{Z}) < \mathrm{SL}_n(\mathbb{Q}) < \mathrm{SL}_n(\mathbb{R}) < \mathrm{GL}_n(\mathbb{R}) < \mathrm{GL}_n(\mathbb{C}),$$

kun n on parillinen.

Aliryhmillä on monia ominaisuuksia, jotka muistuttavat kursseilta Lineaarinen algebra 1 ja 2 tuttuja vektoriavaruuksien aliavaruuksien ominaisuuksia. Tämä ei ole yllättävää:

Esimerkki 5.4. Reaalinen vektoriavaruus (eli $\mathbb{R}$-vektoriavaruus) muodostuu laskutoimituksella varustetusta joukosta $(V, +)$, jossa on määritelty alkioiden kertominen reaaliluvulla. Reaaliluvulla kertominen tarkoittaa kuvausta $\mathbb{R} \times V \to V$, $(\lambda, v) \mapsto \lambda v$. Laskutoimitukselta ja reaaliluvulla kertomiselta oletetaan

(1) $(V, +)$ on kommutatiivinen ryhmä,
(2) $\lambda(v + w) = \lambda w + \lambda w$ kaikille $\lambda \in \mathbb{R}$ ja $v, w \in V$,
(3) $(\lambda + \mu)v = \lambda v + \mu v$ kaikille $\lambda, \mu \in \mathbb{R}$ ja $v \in V$,
(4) $\mu(\lambda v) = (\mu\lambda)v$ kaikille $\lambda, \mu \in \mathbb{R}$ ja $v \in V$ ja
(5) $1\, v = v$.

Määritelmän mukaan reaalisen vektoriavaruuden V aliavaruus on osajoukko $H \subset V$, joka on vakaa vektoriavaruuden V yhteenlaskun ja reaaliluvulla kertomisen suhteen, ja on näillä operaatioilla varustettuna reaalinen vektoriavaruus. Erityisesti $(H, +)$ on additiivisen ryhmän $(V, +)$ aliryhmä.

Kaikki additiivisen ryhmän $(V, +)$ aliryhmät eivät ole $\mathbb{R}$-vektoriavaruuden V aliavaruuksia. Esimerkiksi $\mathbb{R}$-vektoriavaruudella $\mathbb{R}$ on vain kaksi aliavaruutta $\{0\}$ ja $\mathbb{R}$ mutta reaalilukujen additiivisella ryhmällä on paljon enemmän aliryhmiä: Esimerkiksi joukot

$$\alpha\mathbb{Z} = \{\alpha\, k : k \in \mathbb{Z}\}$$

ja

$$\alpha\mathbb{Q} = \{\alpha\, q : q \in \mathbb{Q}\}$$

ovat ryhmän $(\mathbb{R}, +)$ vakaita osajoukkoja kaikilla $\alpha \in \mathbb{R}$ ja on helppo tarkastaa, että

$$(\alpha\mathbb{Z}, +) < (\alpha\mathbb{Q}, +) < (\mathbb{R}, +)$$

kaikilla $\alpha \in \mathbb{R}$.

Jos W on toinen $\mathbb{R}$-vektoriavaruus, niin kuvaus $L\colon V \to W$ on ($\mathbb{R}$-)lineaarikuvaus, jos se on homomorfismi kommutatiivisesta ryhmästä $(V, +)$ kommutatiiviseen ryhmään $(W, +)$, joka on lisäksi yhteensopiva reaaliluvulla kertomisen kanssa: Kaikille $\lambda \in \mathbb{R}$ ja $v \in V$ pätee $L(\lambda v) = \lambda L(v)$.

Sen todistaminen, että kaikki homomorfismit reaalilukujen additiiviselta ryhmältä itselleen eivät ole lineaarikuvauksia on hieman monimutkaisempaa. G. Hamel todisti tämän tuloksen valinta-aksiooman avulla vuonna 1905.

Käyttämällä edellä olevassa määritelmässä reaalilukujen sijaan rationaalilukuja tai kompleksilukuja saadaan $\mathbb{Q}$-vektoriavaruuden ja $\mathbb{C}$-vektoriavaruuden ja vastaavien $\mathbb{Q}$- ja $\mathbb{R}$-lineaarikuvausten käsitteet.

Propositio 5.5. *Aliryhmien leikkaus on aliryhmä.*

Todistus. Harjoitustehtävä 43. □

Propositio 5.6. *Olkoon $\phi\colon G \to G'$ ryhmähomomorfismi. Olkoot $H \leq G$, $H' \leq G'$ aliryhmiä. Tällöin $\phi(H) \leq G'$ ja $\phi^{-1}(H') \leq G$ ovat aliryhmiä.*

Todistus. Olkoot $\phi(g), \phi(h) \in \phi(H)$. Tällöin

$$\phi(g)(\phi(h))^{-1} = \phi(g)\phi(h^{-1}) = \phi(gh^{-1}) \in \phi(H),$$

koska $gh^{-1} \in H$. Siis $\phi(H)$ on aliryhmä Proposition 5.2(1) nojalla.

Toinen väite todistetaan harjoitustehtävässä 44. □

Jokaiseen ryhmähomomorfismiin liittyy kaksi tärkeää aliavaruutta, yksi määrittelyjoukossa ja yksi maalijoukossa:

Määritelmä 5.7. Ryhmähomomorfismin $\phi\colon G \to G'$ *ydin* on $\ker\phi = \phi^{-1}(e')$ ja sen *kuva* on $\operatorname{Im}\phi = \phi(G)$.

Proposition 5.6 mukaan ryhmähomomorfismin ydin ja kuva ovat aliryhmiä.

Esimerkki 5.8. (a) Olkoon $\phi_q\colon \mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$ luonnollinen homomorfismi, $\phi_q(k) = [k] \in \mathbb{Z}/q\mathbb{Z}$. Homomorfismin ϕ_q ydin on $q\mathbb{Z}$.

(b) Lineaarialgebrassa osoitettiin, että kaikille neliömatriiseille $A, B \in \mathrm{M}_n(\mathbb{R})$ pätee

$$\det(AB) = \det A \det B.$$

Kun rajoitetaan determinantti nollajoukkonsa komplementtiin saadaan siis ryhmähomomorfismi $\det\colon \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$. Determinantin ydin on $\mathrm{SL}_n(\mathbb{R})$. Determinantti voidaan määritellä samalla lausekkeella myös kompleksikertoimisille neliömatriiseille, jolloin saadaan ryhmähomomorfismi $\det\colon \mathrm{GL}_n(\mathbb{C}) \to \mathbb{C}^\times$, jonka ydin on $\mathrm{SL}_n(\mathbb{C})$.

Tarkastelemme ydintä ja kuvaa lähemmin luvussa 7. Seuraava ytimen ominaisuus on hyvä todeta jo tässä vaiheessa:

Propositio 5.9. *Ryhmähomomorfismi on injektio, jos ja vain jos sen ydin on neutraalialkion muodostama ryhmä.*

Todistus. Olkoon $\phi\colon G \to G'$ ryhmähomomorfismi. Aiemmin osoitettiin (harjoitustehtävä 29), että ryhmän G neutraalialkio e kuvautuu ryhmän G' neutraalialkioksi e', joten jos ϕ on injektio, sen ydin on $\{e\}$.

Oletetaan, että $\ker\phi = \{e\}$. Olkoot $x, y \in G$ siten, että $\phi(x) = \phi(y)$. Tällöin

$$\phi(xy^{-1}) = \phi(x)(\phi(y))^{-1} = e',$$

joten $xy^{-1} = e$ eli $x = y$. □

Proposition 5.9 mukaan ryhmähomomorfismin injektiivisyyden toteamiseksi riittää tarkastella neutraalialkion alkukuvaa.

Määritelmä 5.10. Olkoon G ryhmä, ja olkoon $B \subset G$, $B \neq \emptyset$. Joukon B *virittämä aliryhmä* $\langle B\rangle$ on pienin aliryhmä, joka sisältää joukon B. Joukon B alkiot ovat ryhmän $\langle B\rangle$ *virittäjiä*.

Joukon B virittämä aliryhmän aliryhmän määritelmässä voi todellakin puhua pienimmästä joukon B sisältävästä aliryhmästä sillä Proposition 5.5 nojalla

$$\langle B\rangle = \bigcap\{H \leq G : B \subset H\} \leq G\,.$$

Ryhmä $\langle B\rangle$ voidaan esittää konkreettisesti virittäjiensä avulla:

Propositio 5.11. *Olkoon G ryhmä, ja olkoon $B \subset G$, $B \neq \emptyset$. Joukon B virittämä aliryhmä on*

$$\left\{b_1^{\pm 1}b_2^{\pm 1}\cdot\cdots\cdot b_k^{\pm 1} : b_1, b_2, \ldots, b_k \in B, k \in \mathbb{N}\setminus\{0\}\right\}. \tag{6}$$

Todistus. Lausekkeen (6) antama osajoukko $\widetilde{B}$ on ryhmän G aliryhmä Propositioiden 4.3(5) ja 5.2 nojalla. Erityisesti se on ryhmä, joka sisältää joukon B, joten $\langle B\rangle \leq \widetilde{B}$.

Toisaalta $\langle B\rangle$ on ryhmän G aliryhmä, joten erityisesti se on vakaa osajoukko. Koska $B \subset \langle B\rangle$, niin induktiolla on helppo nähdä, että vakaudesta seuraa, että $\langle B\rangle$ sisältää kaikki muotoa $b_1^{\pm 1}b_2^{\pm 1}\cdot\cdots\cdot b_k^{\pm 1}$ olevat alkiot. Siis $\widetilde{B} \leq \langle B\rangle$. □

Esimerkki 5.12. (a) $(\mathbb{Z},+) = \langle 1\rangle = \langle -1\rangle$ ja kaikilla $q \in \mathbb{Z}\setminus\{-1,1\}$ pätee $\langle q\rangle < \mathbb{Z}$. Toisaalta $\mathbb{Z} = \langle 2,3\rangle = \langle 6,10,15\rangle$ koska $1 = 3-2 = 6+10-15$, mutta aliryhmät $\langle 2\rangle, \langle 3\rangle, \langle 6,10\rangle = \langle 2\rangle$, $\langle 6,15\rangle = \langle 3\rangle$ ja $\langle 10,15\rangle = \langle 5\rangle$ ovat ryhmän $(\mathbb{Z},+)$ aitoja aliryhmiä.

(b) Kokeilemalla kaikki tapaukset on helppo nähdä, että jokainen nollasta poikkeava alkio virittää ryhmän $\mathbb{Z}/5\mathbb{Z}$:

$$\mathbb{Z}/5\mathbb{Z} = \langle [1]\rangle = \langle [2]\rangle = \langle [3]\rangle = \langle [4]\rangle\,.$$

Toisaalta $\mathbb{Z}/4\mathbb{Z} = \langle [1]\rangle = [3]\rangle$ mutta $\langle [2]\rangle < \mathbb{Z}/4\mathbb{Z}$.

Seuraava tulos osoittaa, että ryhmässä G määritelty ryhmähomomorfismi määräytyy yksikäsitteisesti, jos sen arvot tunnetaan virittäjäjoukossa.

Propositio 5.13. *Olkoon $G = \langle S\rangle$ ryhmä. Olkoot $\phi, \psi\colon G \to H$ ryhmähomomorfismeja, joille pätee $\phi|_S = \psi|_S$. Tällöin $\phi = \psi$.*

Todistus. Harjoitustehtävä 51. □

Kun ryhmän alkiot kirjoitetaan virittäjien avulla on kätevä käyttää monikertojen ja potenssien yleistyksiä ryhmille. Itse asiassa nämä käsitteet voidaan määritellä hieman yleisemmässä tapauksessa: Olkoon $(A, \cdot)$ assosiatiivisella laskutoimituksella varustettu joukko. Jokaiselle $a \in A$ määritellään positiiviset *potenssit*: Asetamme $a^1 = a$, ja kaikille $n \in \mathbb{N}$, $n \geq 1$ asetamme $a^{n+1} = aa^n$. Jos laskutoimituksella varustetussa joukossa $(A, \cdot)$ on neutraalialkio e, asetamme $a^0 = e$, ja jos alkiolla $a \in A$ on käänteisalkio, määrittelemme sen -1. potenssiksi käänteisalkion a^{-1}, ja kaikille $n \in \mathbb{Z}$, $n \leq -2$ asetamme $a^n = (a^{-1})^{-n}$.

Assosiatiivisella laskutoimituksella varustettu joukossa $(A, +)$ määrittelemme vastaavasti alkion a positiiviset *monikerrat* asettamalla $1\, a = a$, ja $(n+1)a = na + a$ kaikille $n \in \mathbb{Z}$, $n \geq 1$. Jos laskutoimituksella varustetussa joukossa $(A, +)$ on neutraalialkio, niin asetetaan $0\, a = 0 \in A$, ja jos alkiolla $a \in A$ on käänteisalkio laskutoimituksen $+$ suhteen, asetetaan $(-1)\, a = -a$, ja negatiivisille $n \in \mathbb{Z}$ asetamme $na = (-n)(-a)$.

Tavanomaiset laskulait pätevät potensseille ja monikerroille:

Lemma 5.14. *Olkoon $(G, \cdot)$ ryhmä. Tällöin*

(1) $(a^n)^m = a^{nm}$ *kaikilla* $a \in G$, $n, m \in \mathbb{Z}$.
(2) $a^n a^m = a^{n+m}$ *kaikilla* $a \in G$, $n, m \in \mathbb{Z}$.

Olkoon $(H, +)$ ryhmä. Tällöin

(3) $na + ma = (n+m)a$ *kaikilla* $a \in H$, $n, m \in \mathbb{Z}$.
(4) $n(ma) = (nm)a$ *kaikilla* $a \in H$, $n, m \in \mathbb{Z}$.

Todistus. Harjoitustehtävä 45. □

Määritelmä 5.15. Olkoon G multiplikatiivinen ryhmä ja olkoon H additiivinen ryhmä. Aliryhmät

$$\langle a \rangle = \{a^n : n \in \mathbb{Z}\} \leq G$$

ja

$$\langle b \rangle = \{n\, b : n \in \mathbb{Z}\} \leq H$$

ovat alkioiden $a \in G$ ja $b \in H$ *virittämät sykliset aliryhmät.*

Kokonaislukujen additiivisella ryhmällä on sykliset aliryhmät

$$n\mathbb{Z} = \langle n \rangle = \{kn : k \in \mathbb{Z}\},$$

$n \in \mathbb{N}$. Itse asiassa ryhmällä $(\mathbb{Z}, +)$ ei ole mitään muita aliryhmiä:

Propositio 5.16. *Kokonaislukujen additiivisen ryhmän $(\mathbb{Z}, +)$ kaikki aliryhmät ovat syklisiä.*

Todistus. Huomataan ensin, että $\{0\} = 0\,\mathbb{Z}$ ja $\mathbb{Z} = 1\,\mathbb{Z}$. Olkoon $H < \mathbb{Z}$, $H \neq \{0\}$ jokin aliryhmä. Olkoon q pienin positiivinen kokonaisluku aliryhmässä H. Tällöin siis $q\mathbb{Z} < H$.

Osoitamme, että $H = q\mathbb{Z}$. Jos on $m \in H \setminus q\mathbb{Z}$, niin $m = aq + b$ joillakin $a, b \in \mathbb{Z}$ siten, että $1 \leq b < q$. Nyt $b \in H$, joten q ei olekaan pienin positiivinen kokonaisluku ryhmässä H, mikä on ristiriita. Siis $H = q\mathbb{Z}$. □

Määritelmä 5.17. Ryhmä G on *syklinen ryhmä*, jos on $a \in G$ siten, että $G = \langle a \rangle$.

Edellä käsitellyistä esimerkeistä muunmuassa ryhmät $\mathbb{Z} = \langle 1 \rangle$ ja $\mathbb{Z}/q\mathbb{Z} = \langle [1] \rangle$, $q \geq 2$, ovat syklisiä. Sen sijaan esimerkiksi $\mathbb{Q}$ ja $\mathbb{R}$ eivät ole syklisiä. Reaaliluvuille tämä on selvää koska syklinen ryhmä on aina numeroituva, rationaalilukujen tapaus käsitellään harjoitustehtävässä 49.

Lause 5.18. *(1) Syklinen ryhmä, jossa on vähintään kaksi alkiota, on isomorfinen joko ryhmän $\mathbb{Z}$ tai jonkin ryhmän $\mathbb{Z}/q\mathbb{Z}$, $q \geq 2$ kanssa.*

(2) Syklisen ryhmän kuva ryhmähomomorfismissa on syklinen.

(3) Jokainen syklisen ryhmän aliryhmä on syklinen.

Todistus. (1) Olkoon $C = \langle g \rangle$ syklinen ryhmä ja olkoon $\phi\colon \mathbb{Z} \to C$, $\phi(n) = g^n$. Lemman 5.14 nojalla ϕ on homomorfismi ja ryhmän C määritelmän nojalla se on surjektio. Jos ϕ on injektio, se on isomorfismi.

Jos ϕ ei ole injektio, niin $\ker\phi = q\mathbb{Z}$ jollain $q \geq 2$. Olkoon $\psi\colon \mathbb{Z}/q\mathbb{Z} \to C$, $\psi([k]) = \phi(k) = g^k$. Kuvaus ψ on hyvin määritelty: jos $k \equiv k' \mod q$, niin $k - k' \in q\mathbb{Z} = \ker\phi$, joten $g^k = g^{k'}$. Kuvaus ψ on homomorfismi:

$$\psi([n])\psi([m]) = g^n g^m = g^{n+m} = \psi([n+m]) = \psi([n] + [m]).$$

Homomorfismi ψ on surjektio koska ϕ on surjektio. Huomataan vielä, että $\ker\psi = [0]$: Jos $\psi([k]) = e \in G$, niin $\phi(k) = e$, joten $k \in q\mathbb{Z}$ ja $[k] = [q]$.

(2) Harjoitustehtävä 50.

(3) Väite todistettiin sykliselle ryhmälle $(\mathbb{Z}, +)$ Propositiossa 5.16. Olkoon $C = \langle g \rangle$ syklinen ryhmä, ja olkoon $H < C$. Olkoon $\phi\colon \mathbb{Z} \to C$ homomorfismi $\phi(n) = g^n$. Tällöin $\phi^{-1}(H) \leq \mathbb{Z}$, joten $\phi^{-1}(H) = N\mathbb{Z}$ jollain $N \in \mathbb{Z}$, erityisesti ϕ^{-1} on syklinen ryhmä. Koska $H = \phi(\phi^{-1}(H))$, väite seuraa kohdasta (2). □

Koska Lauseen 5.18 mukaan kaikki keskenään yhtä mahtavat sykliset ryhmät ovat isomorfisia keskenään, voimme puhua abstraktista *n alkion syklisestä ryhmästä* C_n ja *äärettömästä syklisestä ryhmästä* C_∞. Toisinaan syklisille ryhmille käytetään merkintöjä Z_n ja Z_∞.

Esimerkki 5.19. (a) Ryhmän $(\mathbb{R}^2, +)$ alkiot $(0,1)$ ja $(1,0)$ virittävät aliryhmän

$$\langle (0,1), (1,0) \rangle = (\mathbb{Z}^2, +) < (\mathbb{R}^2, +).$$

$(\mathbb{Z}^2, +)$ ei ole syklinen ryhmä: Jos $a, b \neq 0$, niin $(-a, b)$ ei ole alkion $(a, b) \in \mathbb{Z}^2$ virittämässä aliryhmässä. Lisäksi alkioiden $(a, 0)$ ja $(0, a)$ virittämät sykliset ryhmät sisältyvät ryhmän $(\mathbb{Z}^2, +)$ aitoihin aliryhmiin $\mathbb{Z} \times \{0\}$ ja $\{0\} \times \mathbb{Z}$, joten myöskään tätä muotoa olevat alkiot eivät voi yksinään virittää ryhmää $(\mathbb{Z}^2, +)$.

(b) Esimerkissä 4.10 käsitelty *Kleinin neliryhmä* $K = \langle f, g \rangle$ ja sen kanssa isometrinen ryhmä

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \langle ([0],[1]), ([1],[0]) \rangle$$

eivät ole syklisiä, koska jokaisen neutraalialkiosta poikkeavan alkion virittämä syklinen ryhmä on isomorfinen ryhmän $\mathbb{Z}/2\mathbb{Z}$ kanssa. Erityisesti siis neljän alkion kommutativiset ryhmät $\mathbb{Z}/4\mathbb{Z}$ ja $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ eivät ole isomorfisia. Edellä käyttöönotetun syklisten ryhmien merkinnän avulla edellinen on hieman lyhyempi ilmaista: ryhmät C_4 ja $C_2 \times C_2$ eivät ole isomorfisia.

Harjoitustehtäviä.

Tehtävä 41. Osoita, että

$$\mathbb{S}^1 = \{z \in \mathbb{C} : |z| = 1\}$$

on ryhmän $\mathbb{C}^\times$ aliryhmä.

Tehtävä 42. Anna esimerkki surjektiivisesta homomorfismista $f\colon (\mathbb{R}, +) \to (\mathbb{S}^1, \cdot)$.

Tehtävä 43. Olkoon G ryhmä, olkoon $I \neq \emptyset$ jokin indeksijoukko ja olkoot $H_i \leq G$, $i \in I$. Osoita, että

$$\bigcap_{i \in I} H_i \leq G.$$

Tehtävä 44. Olkoon $\phi\colon G \to G'$ ryhmähomomorfismi. Olkoon $H' \leq G'$. Osoita: $\phi^{-1}(H') \leq G$.

Tehtävä 45. Todista Lemman 5.14 kohtien (1) ja (2) potenssien laskusäännöt.

Tehtävä 46. Määritä kaikki ryhmien $\mathbb{Z}/6\mathbb{Z}$ ja $\mathbb{Z}/7\mathbb{Z}$ aliryhmät.

Tehtävä 47. Osoita, että ryhmät $\mathbb{Z}/6\mathbb{Z}$ ja $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ ovat isomorfisia.

Tehtävä 48. Olkoon $q \in \mathbb{N} \setminus \{0\}$. Osoita, että joukko

$$G_q = \{w \in \mathbb{C} : w^q = 1\}$$

varustettuna kompleksilukujen kertolaskulla on ryhmän $\mathbb{C}^\times$ aliryhmä. Osoita, että ryhmä G_q on isomorfinen ryhmän $\mathbb{Z}/q\mathbb{Z}$ kanssa.

Tehtävä 49. Osoita, että rationaalilukujen additiivinen ryhmä ei ole syklinen.

Tehtävä 50. Olkoon C syklinen ryhmä ja olkoon $\phi\colon C \to G$ ryhmähomomorfismi. Osoita, että $\phi(C) \leq G$ on syklinen aliryhmä.

Tehtävä 51. Olkoon $G = \langle S \rangle$ ryhmä. Olkoot $\phi, \psi\colon G \to H$ ryhmähomomorfismeja, joille pätee $\phi|_S = \psi|_S$. Osoita, että $\phi = \psi$.

[47] Vihje: Osoita, että $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ on syklinen ryhmä.