TAMPEREEN YLIOPISTO
Pro gradu -tutkielma

Timo Rahkonen

Ryhmälaajennukset ja ryhmäkohomologia

Matematiikan ja tilastotieteen laitos
Matematiikka
Marraskuu 2008

Tampereen yliopisto

Matematiikan ja tilastotieteen laitos

RAHKONEN, TIMO: Ryhmälaajennukset ja ryhmäkohomologia

Pro gradu -tutkielma, 39 s.

Matematiikka

Marraskuu 2008

Tiivistelmä

Tutkielman aiheena on ryhmälaajennusten ja ryhmäkohomologian esittely. Ryhmä G, jolla on normaali aliryhmä K voidaan jakaa ryhmiin K ja G/K. Ryhmälaajennusten tutkiminen asettaa päinvastaisen kysymyksen: millaisia ryhmiä G saadaan aliryhmästä K ja tekijäryhmästä $Q = G/K$?

Tutkielman toisessa luvussa esitellään lyhyesti esitietoina ryhmän toiminta ja G-modulit. Kolmannessa luvussa esitellään ryhmälaajennukset, ryhmien suorat tulot, nostot, lohkeavat laajennukset, ryhmien puolisuorat tulot, ryhmien komplementit ja ekvivalentit laajennukset sekä esitellään niiden ominaisuuksia. Neljännen luvun ensimmäisessä aliluvussa keskitytään ensimmäiseen kohomologiaryhmään. Ensin määritellään 1-kosyklit ja 1-koreunat ja lopulta ensimmäinen kohomologiaryhmä. Tämän jälkeen todistetaan joitakin ensimmäiseen kohomologiaryhmään liittyviä tuloksia. Toisessa aliluvussa keskitytään toiseen kohomologiaryhmään. Aluksi määritellään 2-kosyklit ja 2-koreunat ja näiden jälkeen toinen kohomologiaryhmä. Seuraavaksi todistetaan joitakin toiseen kohomologiaryhmään liittyviä tuloksia. Kolmannessa aliluvussa esitellään vielä lyhyesti n-kosyklit, n-koreunat ja yleisen kohomologiaryhmän määritelmä.

Sisältö

1 Johdanto

Tässä tutkielmassa tutustutaan ryhmälaajennuksiin ja ryhmäkohomologiaan. Tutkielman tarkoituksena on esitellä ryhmälaajennukset ja ryhmäkohomologia sekä niiden ominaisuuksia. Ryhmälaajennusten tutkiminen palautuu niin kutsuttuun laajennusongelmaan. Annetuille ryhmälle Q ja kommutatiiviselle ryhmälle K etsitään kaikki ryhmän K laajennukset G ryhmällä Q. Tässä tutkielmassa tarkastellaan Q-moduleja K ja etsitään operaattorit realisoivia laajennuksia. Tutkielman lukijan odotetaan tuntevan ryhmäteoriaa isomorfialauseisiin asti mukaanlukien kyseiset lauseet.

Luvussa 2 esitellään esitietoina ryhmän toiminta sekä G-modulit. Luvussa 3 määritellään ryhmän K laajennus G ryhmällä Q lyhyenä eksaktina jonona $1 \to K \to G \to Q \to 1$. Tämän jälkeen määritellään nostot $\ell\colon Q \to G$ ja esitellään joitakin nostoihin liittyviä tuloksia. Seuraavaksi määritellään lohkeavat laajennukset ja puolisuorat tulot näiden laajennusten keskimmäisinä ryhminä. Tämän jälkeen todistetaan, että kaikkien järjestettyjen parien joukko yhdessä laskutoimituksen $(a, x) + (b, y) = (a + xb, xy)$ kanssa on ryhmä ja puolisuora tulo. Seuraavaksi esitellään ekvivalentit laajennukset ja todistetaan, että laajennusten ekvivalenttius on ekvivalenssirelaatio.

Luku 4 on jaettu kolmeen alilukuun, joista ensimmäisessä, pykälässä 4.1 esitellään ensin 1-kosyklit ja 1-koreunat. Kosyklien ryhmän $Z^1(Q, K)$ ja koreunojen ryhmän $B^1(Q, K)$ avulla määritellään ensimmäinen kohomologiaryhmä tekijäryhmänä $H^1(Q, K) = Z^1(Q, K)/B^1(Q, K)$. Seuraavaksi todistetaan, että ensimmäisen kohomologiaryhmän ja ryhmän K kanssa komplementaaristen aliryhmien $H \leq K \rtimes Q$ konjugaattiluokkien joukon välillä on bijektio. Aliluvussa 4.2 esitellään 2-kosyklit ja todistetaan, että ryhmästä Q, Q-modulista K ja kosyklistä f saadaan aina rakennettua ryhmän K laajennus $G(K, Q, f)$ ryhmällä Q. Seuraavaksi todistetaan, että kun G on ryhmän K laajennus ryhmällä Q, niin on olemassa sellainen kosykli f, että laajennukset G ja $G(K, Q, f)$ ovat ekvivalentit. Seuraavaksi määritellään 2-koreunat sekä 2-kosyklien ja 2-koreunojen ryhmät $Z^2(Q, K)$ ja $B^2(Q, K)$. Näistä saadaan toinen kohomologiaryhmä $H^2(Q, K) = Z^2(Q, K)/B^2(Q, K)$. Tämän jälkeen luvun päätuloksena todistetaan Schreierin lause. Lopuksi todistetaan vielä Schur-Zassenhaussin lauseen kevyempi muoto. Aliluvussa 4.3 esitellään lyhyesti yleisen kohomologiaryhmän määritelmä ja sitä edeltävät tarvittavat tiedot.

Tutkielman päälähdeteoksena on käytetty Joseph J. Rotmanin kirjaa Advanced Modern Algebra (2002). Muista lähdeteoksista mainittakoon Dietrich Burden muistiinpanot Cohomology of groups with applications to number theory (2004) toisena paljon käytettynä lähteenä. Loput lähdeteokset ovat tarjonneet taustatukea edellä mainituille.

2 Ryhmän toiminta ja G-modulit

2.1 Ryhmän toiminta

Tässä luvussa esitellään ryhmän toiminta sekä joitakin sen seurauksia. Aloitetaan ryhmän toiminnan määritelmällä.

Määritelmä 2.1. Olkoot G ryhmä ja X joukko. Ryhmä G *toimii* joukossa X, jos on olemassa sellainen kuvaus $G \times X \to X$, $(g, x) \mapsto gx$, että

(i) $(g_1g_2)x = g_1(g_2x)$ aina, kun $g_1, g_2 \in G$ ja $x \in X$,

(ii) $1x = x$ aina, kun $x \in X$, missä 1 on ryhmän G neutraalialkio.

Jos ryhmä G toimii joukossa X, niin sanotaan että X on G-joukko.

Jos ryhmä G toimii joukossa X, niin kiinnittämällä alkio g saadaan kuvaus $\alpha_g \colon X \to X$, $x \mapsto gx$. Kiinnittämällä alkio g^{-1} saadaan kuvaukselle α_g käänteiskuvaus $\alpha_{g^{-1}}$, sillä $\alpha_g(\alpha_{g^{-1}}(x)) = \alpha_g(g^{-1}x) = g(g^{-1}x) = (gg^{-1})x = x$ ja täten α_g on bijektio. Siispä $\alpha_g \in S_X$, missä S_X on joukon X symmetrinen ryhmä. Määritellään nyt kuvaus

$$\alpha \colon G \to S_X, g \mapsto \alpha_g.$$

Osoitetaan, että kuvaus α on homomorfismi. Ensinnäkin $\alpha(gg') = \alpha_{gg'}$. Toisaalta, $\alpha(g)\alpha(g') = \alpha_g\alpha_{g'}$. Nyt ryhmän toiminnan määritelmän kohdan (i) perusteella

$$\alpha_g(\alpha_{g'}(x)) = \alpha_g(g'x) = g(g'x) = (gg')x = \alpha_{gg'}(x).$$

Täten $\alpha(gg') = \alpha(g)\alpha(g')$ ja kuvaus α on homomorfismi. Siis ryhmän G toiminnasta joukossa X saadaan homomorfismi $G \to S_X$. Kääntäen, jos $\varphi \colon G \to S_X$ on homomorfismi, niin määritellään $gx = \varphi(g)x$. Osoitetaan, että kuvaus φ määrittelee ryhmän G toiminnan joukossa X. Koska $(g_1g_2)x = \varphi(g_1g_2)x$ ja $g_1(g_2x) = \varphi(g_1)(g_2x) = \varphi(g_1)\varphi(g_2)x = \varphi(g_1g_2)x$, on $(g_1g_2)x = g_1(g_2x)$ ja täten ehto (i) on voimassa. Koska $1_Gx = \varphi(1)x = 1_{S_X}x = x$ niin myös ehto (ii) on voimassa.

Toiminnan sanotaan olevan *tehokas*, jos homomorfismi on injektio, siis jos $gx = x$ aina, kun $x \in X$ johtaa siihen, että $g = 1$. [4, s. 99] ja [3, s. 50].

Esimerkki 2.1. [4, s. 100] Osoitetaan, että ryhmä G toimii itsessään konjugaatiolla. Määritellään jokaisella $g \in G$ kuvaus $\alpha_g \colon G \to G$ konjugaatioksi $\alpha_g(x) = gxg^{-1}$.

Tällöin aina, kun $x \in G$,

$$\begin{aligned}(\alpha_g \circ \alpha_h)(x) &= \alpha_g(\alpha_h(x)) \\ &= \alpha_g(hxh^{-1}) \\ &= g(hxh^{-1})g^{-1} \\ &= (gh)x(gh)^{-1} \\ &= \alpha_{gh}(x).\end{aligned}$$

Siis $\alpha_g \circ \alpha_h = \alpha_{gh}$, ja täten aksiooma (i) on voimassa.

Aksiooman (ii) todistamiseksi huomataan, että aina, kun $x \in G$, niin $\alpha_1(x) = 1x1^{-1} = x$. Siispä $\alpha_1 = 1_G$ ja täten aksiooma (ii) on voimassa.

Määritelmä 2.2. Jos ryhmä G toimii joukossa X ja $x \in X$, niin alkion x *rata*, jolle käytetään merkintää $\mathcal{O}(x)$, on joukon X osajoukko

$$\mathcal{O}(x) = \{\, gx \mid g \in G \,\}.$$

Kaikkien ratojen joukolle käytetään merkintää $G\backslash X$. Alkion x *vakaaja*, jolle käytetään merkintää G_x, on ryhmän G aliryhmä

$$G_x = \{\, g \in G \mid gx = x \,\}.$$

Propositio 2.1. *Oletetaan, että ryhmä G toimii joukossa X. Määritellään joukossa X relaatio $x \equiv y$, jos on olemassa sellainen $g \in G$, että $y = gx$. Tällöin relaatio $\equiv$ on ekvivalenssirelaatio.* [4, s. 100]

Todistus. Ryhmän toiminnan ehdon (ii) mukaan $x = 1x$ kun $1 \in G$, joten $x \equiv x$ ja täten $\equiv$ on refleksiivinen. Oletetaan, että $x \equiv y$. Siis $y = gx$ jollakin $g \in G$. Tällöin $g^{-1}y = g^{-1}(gx) = (g^{-1}g)x = 1x = x$ ja koska $g^{-1} \in G$, niin $y \equiv x$ ja täten $\equiv$ on symmetrinen. Oletetaan sitten, että $x \equiv y$ ja $y \equiv z$. Siis $y = g_1x$ ja $z = g_2y$ joillakin $g_1, g_2 \in G$. Tällöin $z = g_2y = g_2(g_1x) = (g_2g_1)x$ ja koska $g_2g_1 \in G$, niin $x \equiv z$ ja täten $\equiv$ on transitiivinen. Täten $\equiv$ on ekvivalenssirelaatio. Alkion $x \in X$ ekvivalenssiluokka on rata $\mathcal{O}(x)$. □

Esimerkki 2.2. [4, s. 101] Edellisessä esimerkissä alkion $x \in G$ rata $\mathcal{O}(x)$ on

$$\{\, y \in G \mid y = axa^{-1} \quad \text{jollakin} \quad a \in G \,\}.$$

Tässä tapauksessa rataa $\mathcal{O}(x)$ kutsutaan alkion x *konjugaattiluokaksi* ja sille käytetään merkitää x^G. Alkion $x \in G$ vakaaja G_x puolestaan on

$$\{\, g \in G \mid gxg^{-1} = x \,\}.$$

Tätä ryhmän G aliryhmää, joka koostuu kaikista sellaisista $g \in G$, jotka kommutoivat alkion x kanssa, kutsutaan alkion x *keskukseksi* ryhmässä G ja sille käytetään merkintää $C_G(x)$.

Määritelmä 2.3. Mikäli joukossa $G\backslash X$ on vain yksi alkio niin sanotaan, että ryhmä G toimii *transitiivisesti* joukossa X.

Esimerkki 2.3. [5, s. 6] Olkoon X affiini suora yli kunnan K ja olkoon G yhdenmuotoisuuskuvausten ryhmä

$$G = \{\, x \mapsto ax + b \mid a \in K^* \quad \text{ja} \quad b \in K \,\}.$$

Kun $x_0, y_0 \in X$ ja määritellään kuvaus $g\colon X \to X$ säännöllä $g(x) = x+y_0-x_0$ (siis $a = 1$ ja $b = y_0-x_0$), niin $g(x_0) = y_0$. Täten aina, kun $x \in X$, on olemassa sellainen kuvaus $g \in G$, että $g(x) = y_0$. Tällöin alkion $x \in X$ rata on

$$\mathcal{O}(x) = \{\, g(x) \mid g \in G \,\} = X.$$

Täten joukossa $G\backslash X$ on vain yksi alkio, joten ryhmä G toimii transitiivisesti joukossa X. Jos $x \in X$, niin alkion x vakaaja on $G_x = \{\, g \in G \mid g(x) = x \,\}$. Siis jos $g \in G_x$, niin $g(x) = ax+b = x$. Tästä saadaan, että $b = x-ax$. Koska g on sellainen kuvaus, että $y \mapsto ay + b$, niin sijoittamalla $b = x - ax$ saadaan $ay+b = ay+x-ax = x+a(y-x)$. Täten $G_x = \{\, g \in G \mid g(y) = x+a(y-x) \,\}$.

2.2 G-modulit

Tässä luvussa esitellään lyhyesti G-modulit. Aloitetaan G-modulin määritelmällä.

Määritelmä 2.4. Olkoon G ryhmä. *Vasen G-moduli* on Abelin ryhmä M yhdessä sellaisen kuvauksen $G \times M \to M$, $(g, m) \mapsto gm$ kanssa, että aina, kun $g, h \in G$ ja $m, n \in M$,

(i) $g(m + n) = gm + gn$

(ii) $(gh)m = g(hm)$

(iii) $1m = m$.

Yhtäpitävästi vasen G-moduli on Abelin ryhmä M yhdessä ryhmähomomorfismin $T\colon G \to \mathrm{Aut}(M)$ kanssa, missä vastaavuus on $T(g)(m) = gm$ aina, kun $m \in M$. Tässä $\mathrm{Aut}(M)$ on ryhmän M kaikkien automorfismien, siis isomorfismien $M \to M$, ryhmä. Laskutoimituksena tässä ryhmässä on kuvausten yhdistäminen. [2, s. 21].

Esimerkki 2.4. [2, s. 22] Olkoon M Abelin ryhmä. Määritellään $gm = m$ aina, kun $g \in G$ ja $m \in M$. Tätä ryhmän G toimintaa kutsutaan triviaaliksi toiminnaksi ja ryhmää M kutsutaan triviaaliksi G-moduliksi.

Määritelmä 2.5. Olkoon M G-moduli. Määritellään

$$M^G = \{\, m \in M \mid gm = m \quad \text{aina, kun} \quad g \in G \,\}.$$

Tällöin M^G on modulin M alimoduli, jota kutsutaan *invarianttien moduliksi.*

Jos M on triviaali G-moduli, niin $M^G = M$ [2, s. 22].

Määritelmä 2.6. Olkoot M ja N G-moduleja. Kuvaus $\varphi\colon M \to N$ on *G-modulien homomorfismi*, jos

(i) $\varphi(m + m') = \varphi(m) + \varphi(m')$

(ii) $\varphi(gm) = g\varphi(m)$

aina, kun $g \in G$ ja $m, m' \in M$. Merkitään kaikkien G-modulien homomorfismien $\varphi\colon M \to N$ joukkoa $\mathrm{Hom}_G(M, N)$.

3 Ryhmälaajennukset

Aloitetaan tutkimalla yhtä ryhmäteorian perusongelmista. Ryhmä G, jolla on normaali aliryhmä K, voidaan jakaa ryhmiin K ja G/K. Laajennusten tutkiminen sisältää päinvastaisen kysymyksen: millaisia ryhmiä G saadaan normaalista aliryhmästä K ja tekijäryhmästä $Q = G/K$? Esimerkiksi Lagrangen lauseen perusteella tiedetään, että $|G| = |Q||K|$ jos Q ja K ovat äärellisiä. [4, s. 784].

Määritelmä 3.1. Olkoon

$$\cdots \to G_{n+1} \xrightarrow{d_{n+1}} G_n \xrightarrow{d_n} G_{n-1} \to \cdots$$

jono ryhmiä ja ryhmähomomorfismeja. Jonon sanotaan olevan on *eksakti*, jos $\operatorname{im} d_{n+1} = \ker d_n$ kaikilla n.

Esimerkki 3.1. [2, s. 3] *Lyhyt eksakti jono* on muotoa

$$1 \to A' \xrightarrow{\alpha} A \xrightarrow{\beta} A'' \to 1.$$

Jonon eksaktiudesta voidaan päätellä, että α on injektio, β on surjektio ja

$$A' \cong \alpha(A') = \ker(\beta),$$

joten $\alpha(A')$ on ytimenä ryhmän A normaali aliryhmä. Joskus ryhmä A' samaistetaan kuvaansa $\alpha(A')$. Lisäksi saadaan

$$A/\ker\beta \cong \beta(A) = A'',$$

joten A'' on isomorfinen tekijäryhmän A/A' kanssa.

Määritelmä 3.2. Olkoot K ja Q ryhmiä. Ryhmän K *laajennus* ryhmällä Q on lyhyt eksakti jono

$$1 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1.$$

Vaihtoehtoisesti sanotaan, että ryhmä G on ryhmän K laajennus, jos sillä on sellainen normaali aliryhmä K_1, että $K_1 \cong K$ ja $G/K_1 \cong Q$. Termiä *laajennus* käytetään yleisesti molemmissa merkityksissä. [4, s. 785]

Määritelmä 3.3. Jos H ja K ovat ryhmiä, niin niiden *suora tulo*, merkitään $H \times K$, on kaikkien järjestettyjen parien (h, k) joukko, missä $h \in H$ ja $k \in K$.

Propositio 3.1. *Olkoot H ja K ryhmiä. Tällöin niiden suora tulo $H \times K$ yhdessä laskutoimituksen*

$$(h, k)(h', k') = (hh', kk')$$

kanssa on ryhmä. [4, s. 90]

Todistus. Osoitetaan ensin, että laskutoimitus on assosiatiivinen. Oletetaan, että $(h,k),(h',k'),(h'',k'') \in H \times K$. Tällöin

$$\begin{aligned}(h,k)[(h',k')(h'',k'')] &= (h,k)(h'h'',k'k'') \\ &= (h(h'h''),k(k'k'')) \\ &= ((hh')h'',(kk')k'') \\ &= (hh',kk')(h'',k'') \\ &= [(h,k)(h',k')](h'',k'').\end{aligned}$$

Siispä laskutoimitus on assosiatiivinen. Osoitetaan sitten, että neutraalialkio on $(1,1)$:

$$(h,k)(1,1) = (h1,k1) = (h,k)$$

ja

$$(1,1)(h,k) = (1h,1k) = (h,k).$$

Lopuksi osoitetaan, että alkion $(h,k) \in H \times K$ käänteisalkio on (h^{-1},k^{-1}):

$$(h,k)(h^{-1},k^{-1}) = (hh^{-1},kk^{-1}) = (1,1)$$

ja

$$(h^{-1},k^{-1})(h,k) = (h^{-1}h,k^{-1}k) = (1,1).$$

Täten $H \times K$ yhdessä laskutoimituksen $(h,k)(h',k') = (hh',kk')$ kanssa on ryhmä. □

Propositio 3.2. *Olkoot G ja G' ryhmiä ja olkoot $K \lhd G$ ja $K' \lhd G'$ normaaleja aliryhmiä. Tällöin $K \times K' \lhd G \times G'$ ja on olemassa isomorfismi*

$$(G \times G')/(K \times K') \cong (G/K) \times (G'/K').$$

Todistus. [4, s. 91] Osoitetaan ensin, että $K \times K' \lhd G \times G'$. Riittää osoittaa, että $(g,g')(k,k')(g,g')^{-1} \in K \times K'$ aina, kun $(g,g') \in G \times G'$ ja $(k,k') \in K \times K'$. Nyt

$$(g,g')(k,k')(g,g')^{-1} = (gkg^{-1},g'k'g'^{-1}),$$

ja koska $K \lhd G$ ja $K' \lhd G'$, niin $gkg^{-1} \in K$ ja $g'k'g'^{-1} \in K'$. Siispä $(g,g')(k,k')(g,g')^{-1} \in K \times K'$, joten $K \times K' \lhd G \times G'$.

Osoitetaan sitten, että lauseessa esitetty isomorfismi on olemassa. Olkoot $\pi\colon G \to G/K$ ja $\pi'\colon G' \to G'/K'$ luonnolliset kuvaukset, siis $\pi(g) = gK$ ja $\pi'(g') = g'K'$. Määritellään kuvaus $f\colon G \times G' \to (G/K) \times (G'/K')$ säännöllä

$$f\colon (g,g') \mapsto (\pi(g),\pi(g')) = (gK,g'K').$$

Osoitetaan, että kuvaus f on homomorfismi, $\operatorname{im} f = (G/K) \times (G'/K')$ ja että $\ker f = K \times K'$, sillä tällöin ensimmäinen isomorfialause antaa halutun isomorfismin.

Ensinnäkin, kuvaus f on homomorfismi, sillä

$$\begin{aligned} f(g,g')f(h,h') &= (gK, g'K')(hK, h'K') \\ &= ((gh)K, (g'h')K') \\ &= f(gh, g'h') \\ &= f((g,g')(h,h')). \end{aligned}$$

Osoitetaan sitten, että $\operatorname{im} f = (G/K) \times (G'/K')$. Koska kuvaukset π ja π' ovat luonnollisina kuvauksina surjektioita, niin myös kuvaus f on surjektio. Täten $\operatorname{im} f = (G/K) \times (G'/K')$.

Osoitetaan lopuksi, että $\ker f = K \times K'$.

$$\begin{aligned} \ker f &= \{\, (g,g') \mid (\pi(g), \pi'(g') = (K,K') \,\} \\ &= \{\, (g,g') \mid (gK, g'K') = (K,K') \,\} \\ &= \{\, (g,g') \mid g \in K, g' \in K' \,\} \\ &= K \times K' \end{aligned}$$

Nyt ensimmäisen isomorfialauseen perusteella $(G \times G')/(K \times K') \cong (G/K) \times (G'/K')$. □

Propositio 3.3. *Jos G on ryhmä, jolla on sellaiset normaalit aliryhmät H ja K, että $H \cap K = \{1\}$ ja $HK = G$, niin $G \cong H \times K$.*

Todistus. [4, s. 91] Osoitetaan ensin, että jos $g \in G$, niin muoto $g = hk$, missä $h \in H$ ja $k \in K$, on yksikäsitteinen. Oletetaan, että $hk = h'k'$. Tällöin $h'^{-1}h = k'k^{-1} \in H \cap K = \{1\}$. Täten $h' = h$ ja $k' = k$. Nyt voidaan määritellä kuvaus $\varphi\colon G \to H \times K$ säännöllä $\varphi(g) = (h,k)$, missä $g = hk$, $h \in H$ ja $k \in K$. Osoitetaan, että kuvaus φ on homomorfismi. Sitä ennen täytyy osoittaa, että jos $h \in H$ ja $k \in K$, niin $hk = kh$. Olkoot siis $h \in H$ ja $k \in K$. Koska K on normaali aliryhmä, niin $(hkh^{-1})k^{-1} \in K$. Toisaalta, koska H on normaali aliryhmä, niin $h(kh^{-1}k^{-1}) \in H$. Siis $hkh^{-1}k^{-1} \in H \cap K$. Mutta koska $H \cap K = \{1\}$, niin $hkh^{-1}k^{-1} = 1$ ja täten $hk = kh$. Olkoon sitten $g' = h'k'$. Siis $gg' = hkh'k'$. Nyt

$$\begin{aligned} \varphi(gg') &= \varphi(hkh'k') \\ &= \varphi(hh'kk') \\ &= (hh', kk') \\ &= (h,k)(h',k') \\ &= \varphi(h,k)\varphi(h',k'). \end{aligned}$$

Siispä φ on homomorfismi. Osoitetaan lopuksi, että φ on bijektio. Jos $(h,k) \in H \times K$, niin silloin alkiolla $g \in G$, joka määritellään $g = hk$, on $\varphi(g) = (h,k)$, siispä φ on surjektio. Jos $\varphi(g) = (1,1)$, niin silloin $g = 1$ ja täten $\ker \varphi = 1$ ja φ on injektio. Täten kuvaus φ on bijektio, ja koska se on myös homomorfismi, on kuvaus φ isomorfismi. □

Huomautus. [4, s. 91] Täytyy olettaa, että molemmat aliryhmät H ja K ovat normaaleja. Esimerkiksi, symmetrisellä ryhmällä S_3 on aliryhmät $H = \langle(123)\rangle$ ja $K = \langle(12)\rangle$. Nyt $H \lhd S_3$, $H \cap K = \{1\}$ ja $HK = S_3$, mutta $S_3 \ncong H \times K$ (sillä syklisinä ryhminä ryhmät H ja K ovat kommutatiivisia, ja täten suora tulo $H \times K$ on kommutatiivinen). Tämä johtuu siitä, että K ei ole ryhmän S_3 normaali aliryhmä.

Esimerkki 3.2. [4, s. 785] Suora tulo $K \times Q$ on ryhmän K laajennus ryhmällä Q, sillä kun määritellään kuvaukset $i\colon K \to K \times Q$ ja $p\colon K \times Q \to Q$ säännöillä $i(k) = (k, 1)$ ja $p(k, q) = q$, niin tällöin $\operatorname{im} i = \{\, (k, 1) \mid k \in K \,\} = \ker p$, joten

$$0 \to K \xrightarrow{i} K \times Q \xrightarrow{p} Q \to 1$$

on lyhyt eksakti jono. Vastaavasti $K \times Q$ on myös ryhmän Q laajennus ryhmällä K.

Esimerkki 3.3. [2, s. 4] Olkoot $C_3 = \langle a\rangle$, $C_6 = \langle b\rangle$ ja $C_2 = \langle c\rangle$. Kun määritellään kuvaus $i\colon C_3 \to C_6$ säännöillä $i(1) = 1$, $i(a) = b^2$ ja $i(a^2) = b^4$ ja kuvaus $p\colon C_6 \to C_2$ säännöillä $p(1) = p(b^2) = p(b^4) = 1$ ja $p(b) = p(b^3) = p(b^5) = c$, niin tällöin $\operatorname{im} i = \ker p$, ja täten

$$1 \to C_3 \xrightarrow{i} C_6 \xrightarrow{p} C_2 \to 1$$

on lyhyt eksakti jono. Siispä syklinen ryhmä C_6 on ryhmän C_3 laajennus ryhmällä C_2. Tässä C_3 on ryhmän C_6 normaali aliryhmä ja koska Lagrangen lauseen perusteella $|C_6/C_3| = 2$, niin $C_6/C_3 \cong C_2$. Toisaalta, kun $D_3 = \{1, s, s^2, t, st, s^2t\}$ ja kuvaukset $i\colon C_3 \to D_3$ ja $p\colon D_3 \to C_2$ määritellään säännöillä $i(1) = 1$, $i(a) = s$, $i(a^2) = s^2$ ja $p(1) = p(s) = p(s^2) = 1$, $p(t) = p(st) = p(s^2t) = c$, niin $\operatorname{im} i = \ker p$, joten myös

$$1 \to C_3 \xrightarrow{i} D_3 \xrightarrow{p} C_2 \to 1$$

on lyhyt eksakti jono. Täten myös diedriryhmä D_3 on ryhmän C_3 laajennus ryhmällä C_2. Ryhmä C_3 on ryhmän D_3 normaali aliryhmä, sillä sen indeksi on $[D_3 : C_3] = 2$. Tekijäryhmä D_3/C_3 on isomorfinen ryhmän C_2 kanssa, sillä Lagrangen lauseen perusteella $|D_3/C_3| = 2$. Huomaa, että ryhmä C_2 ei ole ryhmän D_3 normaali aliryhmä, joten D_3 ei ole ryhmän C_2 laajennus ryhmällä C_3.

Esimerkki 3.4. [2, s. 8] Koska alternoiva ryhmä A_n on symmetrisen ryhmän S_n normaali aliryhmä, niin identtisellä kuvauksella $\mathrm{id}_{S_n}\colon A_n \to S_n$ on $\operatorname{im} \mathrm{id}_{S_n} = A_n$. Kun $C_2 = \langle -1\rangle = \{-1, 1\}$, niin permutaation $\sigma \in S_n$ merkki on kuvaus $\varepsilon\colon S_n \to C_2$, joka määritellään säännöllä $\varepsilon(\sigma) = (-1)^r$, missä $\sigma = \tau_1 \circ \cdots \circ \tau_r$ ja $\tau_1, \ldots, \tau_r \in S_n$ ovat vaihtoja. Nyt $\ker \varepsilon = A_n$. Tällöin

$$1 \to A_n \xrightarrow{\mathrm{id}_{S_n}} S_n \xrightarrow{\varepsilon} C_2 \to 1$$

on lyhyt eksakti jono, joten symmetrinen ryhmä S_n on alternoivan ryhmän A_n laajennus ryhmällä C_2. Tässä $S_n/A_n \cong C_2$, sillä Lagrangen lauseen perusteella $|S_n/A_n| = 2$.

Määritelmä 3.4. Jos

$$1 \to K \to G \xrightarrow{p} Q \to 1$$

on laajennus, niin *nosto* on kuvaus $\ell\colon Q \to G$, jolla $p\ell = \mathrm{id}_Q$, missä $p\ell$ on kuvauksien p ja ℓ yhdistetty kuvaus. Kuvaus ℓ ei välttämättä ole homomorfismi.

Esimerkki 3.5. [2, s. 8] Määritellään esimerkissä 3.4 esiteltyyn laajennukseen

$$1 \to A_n \xrightarrow{\mathrm{id}_{S_n}} S_n \xrightarrow{\varepsilon} C_2 \to 1$$

kuvaus $\ell\colon C_2 \to S_n$ säännöillä $\ell(1) = \mathrm{id}$ ja $\ell(-1) = \tau$, missä $\tau \in S_n$ on vaihto. Tällöin $p(\ell(1)) = p(\mathrm{id}) = 1$ ja $p(\ell(-1)) = p(\tau) = -1$, joten $p\ell = \mathrm{id}_{C_2}$. Siispä kuvaus ℓ on nosto.

Laajennukset on määritelty mielivaltaisille ryhmille K, mutta rajoitutaan tässä kommutatiivisiin ryhmiin K. Jos G on ryhmän K laajennus ryhmällä Q, niin olisi sekavaa kirjoittaa G multiplikatiivisena ja sen aliryhmä K additiivisena. Tästä syystä kirjoitetaan myös ryhmä G additiivisena, vaikkei se olisikaan kommutatiivinen. [4, s. 786]

Propositio 3.4. *Olkoon*

$$0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$$

kommutatiivisen ryhmän K laajennus ryhmällä Q ja olkoon $\ell\colon Q \to G$ nosto.

(i) *Määritellään konjugaatio $\theta_x\colon K \to K$ säännöllä*

$$\theta_x\colon a \mapsto \ell(x) + a - \ell(x)$$

aina, kun $x \in Q$. Tällöin θ_x on riippumaton alkion x noston $\ell(x)$ valinnasta.

(ii) *Kuvaus $\theta\colon Q \to \mathrm{Aut}(K)$, määritellään $x \mapsto \theta_x$, on homomorfismi.*

Todistus. [4, s. 786]

(i) Osoitetaan, että θ_x on riippumaton alkion x noston $\ell(x)$ valinnasta. Oletetaan, että $\ell'(x) \in G$ ja $p\ell'(x) = x$. Koska $p(-\ell(x) + \ell'(x)) = p(-\ell(x)) + p(\ell'(x)) = -x + x = 0$, niin $-\ell(x) + \ell'(x) \in \ker p = \mathrm{im}\, i = K$. Siis on olemassa sellainen $b \in K$, jolla $\ell'(x) = \ell(x) + b$. Täten

$$\begin{aligned} \ell'(x) + a - \ell'(x) &= \ell(x) + b + a - b - \ell(x) \\ &= \ell(x) + a - \ell(x), \end{aligned}$$

sillä K on kommutatiivinen.

(ii) Nyt $\theta_x(a) \in K$, sillä K on ryhmän G normaali aliryhmä. Osoitetaan sitten, että kuvaus θ_x on automorfismi. Kuvaus $\varphi_x \colon K \to K$, joka määritellään säännöllä $\varphi_x(a) = -\ell(x) + a + \ell(x)$, on kuvauksen θ_x käänteiskuvaus, sillä

$$\theta_x(\varphi_x(a)) = \ell(x) + (-\ell(x) + a + \ell(x)) - \ell(x) = a$$

ja

$$\varphi_x(\theta_x(a)) = -\ell(x) + (\ell(x) + a - \ell(x)) + \ell(x) = a.$$

Koska kuvauksella θ_x on käänteiskuvaus, niin θ_x on bijektio. Se on homomorfismi, sillä

$$\begin{aligned} \theta_x(a) + \theta_x(b) &= \ell(x) + a - \ell(x) + \ell(x) + b - \ell(x) \\ &= \ell(x) + a + b - \ell(x) \\ &= \theta_x(a + b). \end{aligned}$$

Osoitetaan lopuksi, että $\theta \colon Q \to \mathrm{Aut}(K)$ on homomorfismi. Jos $x, y \in Q$ ja $a \in K$, niin

$$\theta_x(\theta_y(a)) = \theta_x(\ell(y) + a - \ell(y)) = \ell(x) + \ell(y) + a - \ell(y) - \ell(x),$$

kun taas

$$\theta_{xy}(a) = \ell(xy) + a - \ell(xy).$$

Mutta koska $\ell(x) + \ell(y)$ ja $\ell(xy)$ ovat molemmat alkion xy nostoja, on kohdan (i) perusteella $\theta(x)\theta(y) = \theta_x\theta_y = \theta_{xy} = \theta(xy)$.

□

Kärjistetysti voidaan sanoa, että homomorfismi θ kertoo miten K on normaali ryhmässä G, sillä isomorfiset kopiot ryhmästä voivat olla ryhmän G normaaleja aliryhmiä eri tavoilla [4, s. 787]. Seuraava esimerkki havainnollistaa tällaista tilannetta.

Esimerkki 3.6. [4, s. 787] Olkoon K kertalukua 3 oleva syklinen ryhmä ja olkoon $Q = \langle x \rangle$ kertalukua 2 oleva syklinen ryhmä. Jos $G = K \times Q$, niin silloin G on kommutatiivinen ja K on ryhmän G keskuksessa $Z(G) = \{\, z \in G \mid zg = gz \quad \text{aina, kun} \quad g \in G \,\}$. Tällöin $\ell(x) + a - \ell(x) = a$ aina, kun $a \in K$ ja $\theta_x = \mathrm{id}_K$. Toisaalta, jos $G = S_3$, niin esimerkin 3.4 mukaan saadaan laajennus

$$1 \to A_3 \xrightarrow{\mathrm{id}_{S_3}} S_3 \xrightarrow{\varepsilon} C_2 \to 1.$$

Nyt $K = A_3$ ei ole ryhmän G keskuksessa. Jos esimerkissä 3.5 esitetyllä nostolla ℓ on $\ell(x) = (12)$, niin tällöin $(12)(123)(12) = (132)$ ja täten $\theta_x \neq \mathrm{id}_K$.

Mikäli homomorfismi θ on olemassa, saadaan ryhmään K skalaarilla kertominen. Tämä tekee ryhmästä K vasemman Q-modulin. [4, s. 787]

Propositio 3.5. *Olkoot K ja Q ryhmiä ja olkoon K kommutatiivinen. Tällöin homomorfismi $\theta\colon Q \to \mathrm{Aut}(K)$ tekee ryhmästä K vasemman Q-modulin, jos skalaarilla kertomiseksi määritellään*

$$xa = \theta_x(a)$$

aina, kun $a \in K$ ja $x \in Q$. Kääntäen, jos K on vasen Q-moduli, niin $x \mapsto \theta_x$ määrittelee homomorfismin $\theta\colon Q \to \mathrm{Aut}(K)$, missä $\theta_x\colon a \mapsto xa$.

Todistus (vrt. [4, s. 787]). Käydään läpi G-modulin määritelmän 2.4 kohdat (i)-(iii).

(i) Koska $\theta_x \in \mathrm{Aut}(K)$, niin $x(a+b) = xa+xb$ aina, kun $x \in Q$ ja $a, b \in K$.

(ii) $(xy)a = \theta_{xy}(a) = \theta_x(\theta_y(a)) = \theta_x(ya) = x(ya)$ aina, kun $x, y \in Q$ ja $a \in K$.

(iii) Koska θ on homomorfismi, niin $\theta(1) = \mathrm{id}_K$. Täten $1a = \theta_1(a) = a$ aina, kun $a \in K$.

Kohtien (i)-(iii) perusteella ryhmä K on Q-moduli.

Kääntäen oletetaan, että K on vasen Q-moduli ja osoitetaan, että kuvaus $\theta\colon Q \to \mathrm{Aut}(K), x \mapsto \theta_x$, missä $\theta_x\colon a \mapsto xa$, on homomorfismi. Osoitetaan ensin, että $\theta_x \in \mathrm{Aut}(K)$. Ensinnäkin $\theta_x(a) = xa \in K$, sillä $a \in K$, $x \in Q$ ja K on Q-moduli. Kuvaus θ_x on homomorfismi, sillä

$$\theta_x(a+b) = x(a+b) = xa + xb = \theta_x(a) + \theta_x(b),$$

koska K on Q-moduli. Kuvaus $\theta_{x^{-1}}$ on kuvauksen θ_x käänteiskuvaus, sillä

$$\theta_{x^{-1}}(\theta_x(a)) = \theta_{x^{-1}}(xa) = x^{-1}(xa) = (x^{-1}x)a = a$$

ja

$$\theta_x(\theta_{x^{-1}}(a)) = \theta_x(x^{-1}a) = x(x^{-1}a) = (xx^{-1})a = a.$$

Koska kuvauksella θ_x on käänteiskuvaus, on θ_x bijektio. Siispä kuvaus θ_x on isomorfismi. Täten $\theta_x \in \mathrm{Aut}(K)$. Nyt kuvaus θ on homomorfismi, sillä

$$\theta(xy) = \theta_{xy} = \theta_x\theta_y = \theta(x)\theta(y),$$

koska kuvaus θ_x on automorfismi. □

Seuraus 3.1. *Jos*

$$0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$$

on kommutatiivisen ryhmän K laajennus ryhmällä Q, niin K on vasen Q-moduli, jos määritellään

$$xa = \ell(x) + a - \ell(x),$$

missä $\ell\colon Q \to G$ on nosto, $x \in Q$ ja $a \in K$. Lisäksi skalaarilla kertominen on riippumaton noston ℓ valinnasta.

Todistus. Propositiot 3.4 ja 3.5. [4, s. 788] □

Määritelmä 3.5. Ryhmälaajennus

$$0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$$

on *lohkeava*, jos on olemassa homomorfismi $j\colon Q \to G$, jolla $pj = \mathrm{id}_Q$. Lohkeavan laajennuksen keskimmäistä ryhmää G kutsutaan ryhmän K *puolisuoraksi tuloksi* ryhmällä Q.

Siis laajennus on lohkeava, jos ja vain jos on olemassa nosto j, joka on myös homomorfismi.

Esimerkki 3.7. [2, s. 8] Seuraava laajennus on lohkeava:

$$1 \to SL_n(k) \xrightarrow{\iota} GL_n(k) \xrightarrow{\det} k^\times \to 1,$$

missä $SL_n(k)$ on kaikkien kääntyvien $n \times n$-matriisien joukko, joiden alkiot ovat kunnassa k; $GL_n(k)$ on kaikkien sellaisten $n \times n$-matriisien joukko, joiden determinantti on 1 ja alkiot ovat kunnassa k ja $k^\times$ on kunnan k multiplikatiivinen ryhmä.

Laajennus on lohkeava, sillä kun määritellään kuvaus $j\colon k^\times \to GL_n(k)$ säännöllä

$$a \mapsto \begin{pmatrix} 1 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 1 & 0 \\ 0 & \dots & 0 & a \end{pmatrix}$$

niin tällöin $j(ab) = j(a)j(b)$ ja $\det(j(a)) = a$, joten j on homomorfismi ja $\det \circ j = \mathrm{id}_{k^\times}$.

Esimerkissä 3.5 esitetty laajennuksen

$$1 \to A_n \xrightarrow{\mathrm{id}_{S_n}} S_n \xrightarrow{\varepsilon} C_2 \to 1$$

nosto ℓ on homomorfismi, sillä

$$\ell(-1 \cdot 1) = \ell(-1) = \tau = \tau \circ \mathrm{id} = \ell(-1)\ell(1),$$
$$\ell(1 \cdot 1) = \ell(1) = \mathrm{id} = \ell(1)\ell(1)$$

ja

$$\ell(-1 \cdot (-1)) = \ell(1) = \mathrm{id} = \tau \circ \tau = \ell(-1)\ell(-1).$$

Siispä laajennus on lohkeava.

Esimerkki 3.8. [2, s. 6] Esimerkin 3.3 perusteella $1 \to C_3 \to C_6 \xrightarrow{p} C_2 \to 1$ on laajennus, missä kuvaus p on määritelty säännöillä $p(1) = p(b^2) = p(b^4) = 1$ ja $p(b) = p(b^3) = p(b^5) = c$. Määritellään kuvaus $\ell\colon C_2 \to C_6$ säännöillä

$\ell(1) = 1$ ja $\ell(c) = b^3$. Tällöin kuvaus ℓ on nosto, sillä $p(\ell(1)) = p(1) = 1$ ja $p(\ell(c)) = p(b^3) = c$. Kuvaus on ℓ homomorfismi, sillä

$$\ell(1 \cdot 1) = \ell(1) = 1 = \ell(1)\ell(1),$$
$$\ell(cc) = \ell(c^2) = \ell(1) = 1 = b^6 = b^3b^3 = \ell(c)\ell(c)$$

ja

$$\ell(1c) = \ell(c) = b^3 = 1b^3 = \ell(1)\ell(c).$$

Koska ℓ on nosto ja homomorfismi, niin ryhmä C_6 on ryhmän C_3 puolisuora tulo ryhmällä C_2.

Propositio 3.6. *Olkoon G additiivinen ryhmä, jolla on normaali aliryhmä K.*

(i) *Jos $0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$ on lohkeava laajennus, missä $j\colon Q \to G$ toteuttaa ehdon $pj = \mathrm{id}_Q$, niin $i(K) \cap j(Q) = \{0\}$ ja $i(K) + j(Q) = G$.*

(ii) *Tässä tapauksessa jokainen $g \in G$ voidaan esittää yksikäsitteisesti muodossa $g = i(a) + j(x)$, missä $a \in K$ ja $x \in Q$.*

(iii) *Olkoon Q ryhmän G aliryhmä. Ryhmä G on ryhmän K puolisuora tulo ryhmällä Q, jos ja vain jos $K \cap Q = \{0\}$, $K + Q = G$ ja jokainen $g \in G$ voidaan esittää yksikäsitteisesti muodossa $g = a + x$, missä $a \in K$ ja $x \in Q$.*

Todistus. [4, s. 788]

(i) Jos $g \in i(K) \cap j(Q)$, niin $g = i(a) = j(x)$ joillakin $a \in K$ ja $x \in Q$. Nyt $p(g) = p(j(x)) = pj(x) = x$ ja $p(g) = p(i(a)) = pi(a) = 0$. Siis $x = 0$ ja edelleen $g = j(x) = 0$.

Jos $g \in G$, niin koska $pj = \mathrm{id}_Q$, on $p(g) = pjp(g)$ ja edelleen $p(g) - p(jp(g)) = p(g - jp(g)) = 0$ ja täten $g - (jp(g)) \in \ker p = \operatorname{im} i$. Siispä on olemassa sellainen $a \in K$, että $g - (jp(g)) = i(a)$ ja täten $g = i(a) + j(pg) \in i(K) + j(Q)$.

(ii) Koska $G = i(K) + j(Q)$, on jokaisella alkiolla $g \in G$ muoto $g = i(a) + j(pg)$. Todistaaksemme yksikäsitteisyyden, oletetaan, että $i(a) + j(x) = i(b) + j(y)$, missä $b \in K$ ja $y \in Q$. Tällöin $-i(b) + i(a) = j(y) - j(x) \in i(K) \cap j(Q) = \{0\}$, joten $i(a) = i(b)$ ja $j(x) = j(y)$.

(iii) Välttämättömyys on kohdan (ii) erikoistapaus kun molemmat i ja j ovat inkluusioita, siis $i(a) = a$ ja $j(x) = x$ aina, kun $a \in K$ ja $x \in Q$. Kääntäen oletetaan, että $K \cap Q = \{0\}$, $K + Q = G$ ja että jokaisella $g \in G$ on yksikäsitteinen muoto $g = a + x$ joillakin $a \in K$ ja $x \in Q$. Määritellään kuvaus $p\colon G \to Q$ säännöllä $p(a + x) = x$. Koska $K + Q = G$, niin jokaisella $x \in Q$ on olemassa sellainen $a \in K$, että $a + x = g$

jollakin $g \in G$ ja täten $p(a + x) = x$. Siispä p on surjektio. Kuvaus p on homomorfismi, sillä

$$p((a+x)+(b+y)) = p((a+b)+(x+y)) = x+y = p(a+x)+p(b+y).$$

Lopuksi, kuvauksen p ydin on K, sillä

$$\ker p = \{\, g \in G \mid g = a + 0, \quad a \in K \quad \text{ja} \quad 0 \in Q \,\}$$

ja koska $K \cap Q = \{0\}$, niin $a + 0 \in K$. Täten $\ker p = \{\, g \in G \mid g \in K \,\} = K$.

□

Nimitys puolisuora tulo tulee siitä, että ryhmien K ja Q suoran tulon G vaatimuksiin kuuluvat sekä $KQ = G$ ja $K \cap Q = \{1\}$, että molemmat aliryhmät K ja Q ovat normaaleja. Puolisuoran tulon tapauksessa vain toisen aliryhmän täytyy olla normaali. [4, s. 789]

Määritelmä 3.6. Jos ryhmän G aliryhmät K ja C täyttävät ehdot $C \cap K = \{1\}$ ja $KC = G$, niin ryhmää C kutsutaan ryhmän K *komplementiksi*.

Yleensä $KC = \{\, kc \mid k \in K, c \in C \,\}$ ei ole ryhmän G aliryhmä. On mahdollista todistaa, että KC on ryhmän G aliryhmä, jos ja vain jos $KC = CK$. Tästä johtuen se onkin aliryhmä, jos K tai C on ryhmän G normaali aliryhmä. [2, s. 6]

Esimerkki 3.9. [2, s. 6] Ryhmän $G = S_3 = \{\mathrm{id}, (12), (13), (23), (132), (123)\}$ aliryhmät $K = \langle (123) \rangle = \{\mathrm{id}, (123), (312)\}$ ja $C = \langle (12) \rangle = \{\mathrm{id}, (12)\}$ ovat komplementaarisia, sillä

$$\begin{aligned} \mathrm{id} \circ \mathrm{id} &= \mathrm{id}, & (12) \circ \mathrm{id} &= (12), \\ \mathrm{id} \circ (123) &= (123), & (12) \circ (123) &= (23), \\ \mathrm{id} \circ (312) &= (312), & (12) \circ (312) &= (13), \end{aligned}$$

joten $CK = S_3$, ja koska $K = \{\mathrm{id}, (123), (312)\}$ ja $C = \{\mathrm{id}, (12)\}$, niin $C \cap K = \{\mathrm{id}\}$.

Ryhmän $G = S_4$ aliryhmät $K = \langle (12) \rangle = \{\mathrm{id}, (12)\}$ ja $C = \langle (234) \rangle = \{\mathrm{id}, (234), (243)\}$ eivät puolestaan ole komplementaarisia, sillä

$$\begin{aligned} \mathrm{id} \circ \mathrm{id} &= \mathrm{id}, & (12) \circ \mathrm{id} &= (12), \\ \mathrm{id} \circ (234) &= (234), & (12) \circ (234) &= (1234), \\ \mathrm{id} \circ (243) &= (423), & (12) \circ (243) &= (1243), \end{aligned}$$

joten $|KC| = 6$, ja täten $KC \neq S_4$.

Apulause 3.1. *Olkoot K ja C ryhmän G aliryhmiä. Tällöin K ja C ovat komplementaarisia, jos ja vain jos jokainen $g \in G$ voidaan esittää yksikäsitteisesti muodossa $g = kc$, missä $k \in K$ ja $c \in C$.*

Todistus. [2, s. 6] Oletetaan ensin, että K ja C ovat komplementaarisia. Tällöin $G = KC$, joten jokainen $g \in G$ voidaan esittää muodossa $g = kc$. Yksikäsitteisyyden osoittamiseksi oletetaan, että $g = kc = k'c'$, missä $k, k' \in K$ ja $c, c' \in C$. Nyt $k^{-1}gc'^{-1} = cc'^{-1} = k^{-1}k' \in K \cap C = \{1\}$, joten $k = k'$ ja $c = c'$.

Kääntäen, yksikäsitteisyydestä seuraa, että $G = KC$ ja $K \cap C = \{1\}$. □

Puolisuorassa tulossa G aliryhmä K on normaali. Toisaalta kuva $j(Q)$, jonka propositio 3.6 osoittaa ryhmän K komplementiksi, ei välttämättä ole normaali. Jos esimerkiksi $G = S_3$ ja $K = A_3 = \langle(123)\rangle$, niin voidaan valita $C = \langle\tau\rangle$, missä τ on mikä tahansa vaihto joukossa S_3. Tämä esimerkki osoittaa myös, etteivät komplementit ole yksikäsitteisiä. Kuitenkin ryhmän K mitkä tahansa kaksi komplementtia ovat keskenään isomorfisia, sillä kuten seuraava tulos osoittaa, on mikä tahansa ryhmän K komplementti isomorfinen tekijäryhmän G/K kanssa. [4, s. 789]

Propositio 3.7. *Olkoon G ryhmä ja olkoot K ja C sen aliryhmiä. Jos C on ryhmän K komplementti ryhmässä G, niin tällöin $C \cong G/K$.* [4, s. 789]

Todistus. Koska $G = KC$, niin jokainen $g \in G$ voidaan esittää yksikäsitteisesti muodossa $g = kc$. Täten jokainen $gK \in G/K$ voidaan esittää yksikäsitteisesti muodossa $gK = kcK$. Koska $kcc^{-1} = k$ ja $k \in K$, niin $kcc^{-1} \in K$ ja täten $kcK = cK$. Määritellään nyt kuvaus $f\colon C \to G/K$ säännöllä $f(c) = cK$. Osoitetaan, että kuvaus f on isomorfismi. Jos $f(c) = cK = K$, niin $c \in K$, ja täten $c \in C \cap K$. Koska $C \cap K = \{1\}$, niin $c = 1$, joten $\ker f = \{1\}$ ja täten f on injektio. Olkoon $gK \in G/K$. Koska $gK = cK$ jollain $c \in C$, niin on olemassa sellainen $c \in C$, että $f(c) = cK$. Täten kuvaus f on surjektio. Lopuksi, koska

$$f(cd) = cdK = cKdK = f(c)f(d),$$

niin kuvaus f on homomorfismi. Siispä kuvaus f on isomorfismi. □

Esimerkki 3.10. [2, s. 6] Ryhmät $C_2 = \langle\tau\rangle$, missä $\tau \in S_n$ on vaihto, ja A_n ovat komplementaarisia ryhmässä S_n, sillä kun $\sigma \in S_n$, niin σ voidaan esittää muodossa $\sigma = \tau_1 \circ \cdots \circ \tau_r$ ja koska $\tau^2 = 1$, niin $\sigma = \tau_1 \circ \cdots \circ \tau_r \circ \tau^2$. Täten $\sigma \in A_nC_2$. Koska vaihdon τ merkki on -1, niin $\tau \notin A_n$, joten $A_n \cap C_2 = \{1\}$.

Esimerkki 3.11. [2, s. 6] Sykliset ryhmät $C_n = \langle s\rangle$ ja $C_2 = \langle t\rangle$ ovat komplementaarisia ryhmässä $D_n = \{1, s, s^2, \ldots, s^{n-1}, t, st, s^2t, \ldots, s^{n-1}t\}$, sillä C_n on ryhmän D_n normaali aliryhmä, $C_n \cap C_2 = \{1\}$ ja

$$C_nC_2 = \{1, s, s^2, \ldots, s^{n-1}, t, st, s^2t, \ldots, s^{n-1}t\} = D_n.$$

Täten proposition 3.6 kohdan (iii) mukaan diedriryhmä D_n on ryhmän C_n puolisuora tulo ryhmällä C_2.

Puolisuoran tulon määritelmässä ytimen K ei tarvitse olla kommutatiivinen, ja tällaisia ryhmiä syntyykin itsestään. Esimerkiksi symmetrinen ryhmä S_n on alternoivan ryhmän A_n puolisuora tulo ryhmällä C_2, kuten esimerkissä 3.7 nähtiin.

Pitääksemme oletukset yhdenmukaisina, oletetaan jatkossa, että K on kommutatiivinen, vaikkei tätä oletusta aina tarvittaisikaan. [4, s. 789]

Esimerkki 3.12. [4, s. 789] Kuten esimerkissä 3.2 nähtiin,

$$0 \to K \xrightarrow{i} K \times Q \xrightarrow{p} Q \to 1$$

on laajennus. Määritellään nyt kuvaus $\ell\colon Q \to K \times Q$ säännöllä $\ell(q) = (0, q)$. Tällöin kuvaus ℓ on nosto, sillä $p(\ell(q)) = p(0, q) = q$. Kuvaus ℓ on myös homomorfismi, sillä

$$\ell(q) + \ell(q') = (0, q) + (0, q') = (0 + 0, qq') = (0, qq') = \ell(qq').$$

Täten suora tulo $K \times Q$ on ryhmän K puolisuora tulo ryhmällä Q. Vastaavasti $K \times Q$ on myös ryhmän Q puolisuora tulo ryhmällä K.

Määritelmä 3.7. Olkoon K Q-moduli. Ryhmän K laajennus G ryhmällä Q *realisoi operaattorit*, jos

$$xa = \ell(x) + a - \ell(x)$$

aina, kun $x \in Q$ ja $a \in K$.

Propositio 3.8. *Olkoon Q ryhmä ja olkoon K Q-moduli. Määritellään joukossa $K \times Q$ laskutoimitus*

$$(a, x) + (b, y) = (a + xb, xy).$$

Tällöin joukko $K \times Q$ yhdessä määritellyn laskutoimituksen kanssa on ryhmä, jolle käytetään merkintää $K \rtimes Q$.

Todistus. [4, s. 790] Tutkitaan ensin laskutoimituksen assosiatiivisuutta:

$$[(a, x) + (b, y)] + (c, z) = (a + xb, xy) + (c, z) = (a + xb + (xy)c, (xy)z).$$

Toisaalta,

$$(a, x) + [(b, y) + (c, z)] = (a, x) + (b + yc, yz) = (a + x(b + yc), x(yz)).$$

Ryhmän Q assosiatiivisuudesta seuraa, että $(xy)z = x(yz)$. Ensimmäiset koordinaatit ovat myös samat, sillä koska K on Q-moduli, niin

$$x(b + yc) = xb + x(yc) = xb + (xy)c.$$

Siispä laskutoimitus on assosiatiivinen. Joukon G neutraalialkio on $(0,1)$, sillä

$$(0,1)+(a,x)=(0+1a,1x)=(a,x)$$

ja

$$(a,x)+(0,1)=(a+x0,x1)=(a,x).$$

Alkion (a,x) käänteisalkio on $(-x^{-1}a,x^{-1})$, sillä

$$(-x^{-1}a,x^{-1})+(a,x)=(-x^{-1}a+x^{-1}a,x^{-1}x)=(0,1)$$

ja

$$(a,x)+(-x^{-1}a,x^{-1})=(a+x(-x^{-1}a),xx^{-1})=(0,1).$$

Täten $K\rtimes Q$ on ryhmä. □

Huomataan, että $(a,1)+(0,x)=(a,x)$ ryhmässä $K\rtimes Q$. [4, s. 790]

Propositio 3.9. *Olkoot Q ryhmä ja K Q-moduli. Tällöin $G=K\rtimes Q$ on ryhmän K operaattorit realisoiva puolisuora tulo ryhmällä Q.*

Todistus. [4, s. 790] Osoitetaan ensin, että G on puolisuora tulo. Määritellään kuvaus $p\colon G\to Q$ säännöllä $p\colon (a,x)\mapsto x$. Nyt määritelmänsä perusteella kuvaus p on surjektio ja sen ydin on $\ker p=\{\,(a,1)\mid a\in K\,\}$. Jos määritellään kuvaus $i\colon K\to G$ säännöllä $i\colon a\mapsto(a,1)$, niin

$$0\to K\xrightarrow{i}G\xrightarrow{p}Q\to 1$$

on lyhyt eksakti jono, sillä $\operatorname{im} i=\ker p$. Täten se on ryhmän K laajennus ryhmällä Q. Määritellään kuvaus $j\colon Q\to G$ säännöllä $j\colon x\mapsto(0,x)$. Tällöin j on homomorfismi, sillä $j(x)+j(y)=(0,x)+(0,y)=(0,xy)=j(xy)$. Nyt $pj(x)=p(j(x))=p(0,x)=x$, joten $pj=\mathrm{id}_Q$, ja täten laajennus on lohkeava. Siis G on ryhmän K puolisuora tulo ryhmällä Q.

Osoitetaan sitten, että G realisoi operaattorit. Jos $x\in Q$, niin jokaisella alkion x nostolla on muoto $\ell(x)=(b,x)$ jollain $b\in K$, ja

$$\begin{aligned}(b,x)+(a,1)-(b,x)&=(b+xa,x)+(-x^{-1}b,x^{-1})\\&=(b+xa+x(-x^{-1}b),xx^{-1})\\&=(b+xa-b,1)\\&=(xa,1).\end{aligned}$$

□

Palataan hetkeksi multiplikatiiviseen merkintään. Seuraavassa todistuksessa huomataan, että ryhmän $K\rtimes Q$ laskutoimitus seuraa yhtälöstä

$$(ax)(by)=a(xbx^{-1})xy.$$

[4, s. 791]

Lause 3.1. *Olkoon K Abelin ryhmä. Jos ryhmä G on ryhmän K puolisuora tulo ryhmällä Q, niin silloin ryhmällä K on Q-modulirakenne siten, että $G \cong K \rtimes Q$.*

Todistus. [4, s. 791] Oletetaan, että ryhmä K on ryhmän G normaali aliryhmä ja että ryhmä Q on ryhmän K komplementti. Kirjoitetaan ryhmät G ja Q additiivisina. Jos $a \in K$ ja $x \in Q$, niin määritellään

$$xa = x + a - x,$$

siis xa on alkion a konjugaatti alkiolla x. Proposition 3.6 mukaan jokainen $g \in G$ voidaan esittää yksikäsitteisesti muodossa $g = a + x$, missä $a \in K$ ja $x \in Q$. Yksikäsitteisyydestä seuraa, että kuvaus $\varphi\colon G \to K \rtimes Q$, joka määritellään säännöllä $\varphi\colon a + x \mapsto (a, x)$, on bijektio. Osoitetaan, että φ on isomorfismi.

$$\begin{aligned}\varphi((a+x)+(b+y)) &= \varphi(a+x+b+(-x+x)+y)\\ &= \varphi(a+(x+b-x)+x+y)\\ &= \varphi(a+xb+x+y)\\ &= (a+xb, x+y)\end{aligned}$$

Summan määritelmästä ryhmässä $K \rtimes Q$ saadaan

$$\begin{aligned}(a+xb, x+y) &= (a,x)+(b,y)\\ &= \varphi(a+x)+\varphi(b+y).\end{aligned}$$

□

Esimerkki 3.13. [4, s. 789]

(i) Osoitetaan, että Abelin ryhmä G on puolisuora tulo, jos ja vain jos se on suora tulo (jota yleensä kutsutaan suoraksi summaksi). Esimerkin 3.12 perusteella suora tulo on puolisuora tulo. Riittää siis osoittaa, että puolisuora tulo on suora tulo. Olkoon siis G Abelin ryhmä ja olkoon G ryhmän K puolisuora tulo ryhmällä Q. Tällöin edellisen lauseen perusteella $G \cong K \rtimes Q$. Koska G on kommutatiivinen, niin $xa = x+a-x = a$. Tällöin ryhmän $K \rtimes Q$ laskutoimitus $(a,x)+(b,y) = (a+xb, xy)$ saadaan muotoon $(a,x)+(b,y) = (a+xb, xy) = (a+b, xy)$, joka on suoran tulon laskutoimitus (kun ryhmä Q on multiplikatiivinen). Siispä $G \cong K \times Q$.

(ii) Olkoon G syklinen ryhmä kertalukua p^n. Osoitetaan, että G ei ole puolisuora tulo. Koska sykliset ryhmät ovat Abelin ryhmiä, riittää edellisen kohdan perusteella osoittaa, että G ei ole suora tulo. Olkoot K ja Q ryhmän G aitoja aliryhmiä. Tehdään vastaoletus, että $G = K \times Q$. Koska syklisen ryhmän aliryhmät ovat syklisiä, ja koska $|G| = |K||Q|$ ja $|G| = p^n$, niin $|K| = p^i$ ja $|Q| = p^j$, missä $i, j < p$.

Oletetaan, että $j \geq i$. Valitaan mielivaltainen $g = (k, q) \in G$. Nyt $p^j(k, q) = (p^j k, p^j q) = (0, 0)$, joten $p^j g = 0$ aina, kun $g \in G$. Tämä on ristiriita, sillä ryhmän G kertaluku on p^n ja $p^j < p^n$. Siispä vastaoletus on väärin, ja täten G ei ole suora tulo.

Esimerkki 3.14. [4, s. 793] Olkoon k kunta ja olkoon $k^\times$ sen multiplikatiivinen ryhmä. Nyt $k^\times$ toimii kunnassa k kertolaskulla (jos $a \in k$ ja $a \neq 0$, niin additiivinen homomorfismi $x \mapsto ax$ on automorfismi jonka käänteiskuvaus on $x \mapsto a^{-1}x$). Täten ryhmä $k \rtimes k^\times$, joka proposition 3.9 mukaan on puolisuora tulo, on määritelty. Erityisesti, jos $(b, a), (d, c) \in k \rtimes k^\times$, niin

$$(b, a) + (d, c) = (ad + b, ac).$$

Affiini kuvaus on sellainen funktio $f\colon k \to k$, että $f\colon x \mapsto ax + b$, missä $a, b \in k$ ja $a \neq 0$. Kaikkien affiinien kuvausten joukko yhdessä kuvausten yhdistämisen kanssa on ryhmä $\mathrm{Aff}(1, k)$. Huomataan, että jos $g(x) = cx + d$, niin

$$\begin{aligned}(f \circ g)(x) &= f(cx + d) \\ &= a(cx + d) + b \\ &= (ac)x + (ad + b).\end{aligned}$$

Nyt kuvaus $\varphi\colon (b, a) \mapsto f$, missä $f(x) = ax + b$, on isomorfismi $k \rtimes k^\times \to \mathrm{Aff}(1, k)$. Kuvaus $\gamma\colon \mathrm{Aff}(1, k) \to k \rtimes k^\times$, joka määritellään säännöllä $\gamma(f) = (b, a)$, missä $f(x) = ax + b$, on kuvauksen φ käänteiskuvaus, sillä

$$\varphi(\gamma(f)) = \varphi(b, a) = f, \quad \text{missä} \quad f(x) = ax + b$$

ja

$$\gamma(\varphi(b, a)) = \gamma(f) = (b, a), \quad \text{missä} \quad f(x) = ax + b.$$

Täten kuvaus φ on bijektio. Osoitetaan sitten, että φ on homomorfismi. Ensinnäkin,

$$\varphi((b, a) + (d, c)) = \varphi(ad + b, ac) \quad \text{joten} \quad f(x) = (ac)x + (ad + b).$$

Toisaalta

$$\varphi(b, a)\varphi(d, c) = f \circ g \quad \text{ja} \quad (f \circ g)(x) = (ac)x + (ad + b).$$

Siispä $\varphi((b, a) + (d, c)) = \varphi(b, a)\varphi(d, c)$ ja täten φ on homomorfismi.

Kuinka voidaan kuvailla kaikki ryhmän K laajennukset G ryhmällä Q? Kaikkien laajennusten joukkoon saadaan luonnollinen ekvivalenssirelaatio. [2, s. 11]

Määritelmä 3.8. Olkoot Q ryhmä ja K Q-moduli. Ryhmän K kahden operaattorit realisoivan laajennuksen G ja G' ryhmällä Q sanotaan olevan *ekvivalentit*, jos on olemassa sellainen isomorfismi $\gamma\colon G \to G'$, että seuraavasta kaaviosta tulee kommutatiivinen.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K & \xrightarrow{i} & G & \xrightarrow{p} & Q & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}_K} & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \mathrm{id}_Q} & & \\ 1 & \longrightarrow & K & \xrightarrow{i'} & G' & \xrightarrow{p'} & Q & \longrightarrow & 1 \end{array}$$

Ekvivalenteille laajennuksille käytetään merkintää $(G, i, p) \simeq (G', i', p')$.

Oletetaan, että laajennukset G ja G' ovat ekvivalentit. Tällöin on olemassa sellainen isomorfismi $\gamma\colon G \to G'$, että $i' = \gamma i$ ja $p = p'\gamma$. Tämä määrittelee ekvivalenssirelaation. Relaatio on refleksiivinen, sillä $(G, i, p) \simeq (G, i, p)$, kun $\gamma = \mathrm{id}_G$. Se on symmetrinen, sillä $(G, i, p) \simeq (G', i', p')$ johtaa siihen, että $(G', i', p') \simeq (G, i, p)$ kuvauksella $\gamma^{-1}\colon G' \to G$. Transitiivisuuden osoittamiseksi tarkastellaan seuraavaa kaaviota.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K & \xrightarrow{i} & G & \xrightarrow{p} & Q & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}_K} & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \mathrm{id}_Q} & & \\ 1 & \longrightarrow & K & \xrightarrow{i'} & G' & \xrightarrow{p'} & Q & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}_K} & & \downarrow{\scriptstyle \gamma'} & & \downarrow{\scriptstyle \mathrm{id}_Q} & & \\ 1 & \longrightarrow & K & \xrightarrow{i''} & G'' & \xrightarrow{p''} & Q & \longrightarrow & 1 \end{array}$$

Oletetaan, että $(G, i, p) \simeq (G', i', p')$ ja $(G', i', p') \simeq (G'', i'', p'')$. Siis on olemassa sellaiset homomorfismit $\gamma\colon G \to G'$ ja $\gamma'\colon G' \to G''$, että

$$i' = \gamma i, \quad p = p'\gamma, \quad i'' = \gamma' i' \quad \text{ja} \quad p' = p''\gamma'.$$

Kun määritellään kuvaus $\gamma''\colon G \to G''$ säännöllä $\gamma'' = \gamma'\gamma$, niin saadaan

$$i'' = \gamma' i' = \gamma'\gamma i = \gamma'' i$$

ja

$$p = p'\gamma = p''\gamma'\gamma = p''\gamma''.$$

Täten $(G, i, p) \simeq (G'', i'', p'')$. [2, s. 12]

Koska ekvivalenttien laajennusten määritelmässä kuvaus $\gamma\colon G \to G'$ on isomorfismi, seuraa laajennusten ekvivalenttiudesta aina ryhmien G ja G' isomorfisuus. Käänteinen suunta ei sen sijaan päde, sillä kaksi laajennusta voivat olla epäekvivalentit, vaikka niiden keskimmäiset ryhmät G ja G' olisivatkin isomorfiset [4, s. 801]. Seuraavat kaksi esimerkkiä havainnollistavat tällaisia tapauksia.

Esimerkki 3.15. [4, s. 801] Oletetaan, että p on pariton alkuluku, ja tarkastellaan seuraavaa kaaviota.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \xrightarrow{i} & G & \xrightarrow{\pi} & Q & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}_K} & & \downarrow & & \downarrow{\scriptstyle \mathrm{id}_Q} & & \\ 0 & \longrightarrow & K & \xrightarrow{i'} & G' & \xrightarrow{\pi'} & Q & \longrightarrow & 1 \end{array}$$

Määritellään $K = \langle a \rangle$, syklinen ryhmä kertalukua p, $G = \langle g \rangle = G'$, syklinen ryhmä kertalukua p^2 ja $Q = \langle x \rangle$, missä $x = g + K$. Määritellään kuvaukset i ja i' säännöillä $i(a) = g^p$ ja $i'(a) = g^{2p}$ ja olkoot kuvaukset π ja π' luonnollisia kuvauksia. Osoitetaan, että kuvaus i' on injektio. Koska $K = \{a^n \mid 0 \leq n < p\}$, niin $i'(a^n) = g^{2np}$. Jos $g^{2np} = 1$, niin tällöin $p^2 | 2np$, josta edelleen saadaan $p|2n$. Koska $p \nmid 2$, niin $p|n$. Koska $n < p$, niin tästä seuraa, että $n = 0$. Täten $a^n = 1$. Siispä $\ker i' = \{1\}$, joten i' on injektio. Kuvauksen i osoittaminen injektioksi menee vastaavasti.

Oletetaan, että on olemassa sellainen isomorfismi $\gamma \colon G \to G'$, että kaaviosta tulee kommutatiivinen. Ensimmäisen neliön kommutatiivisuus johtaa siihen, että $\gamma(g^p) = g^{2p}$, siis $\gamma(g)^p = g^{2p}$. Koska γ on isomorfismi, niin $\gamma(g) = g^i$ jollain sellaisella i, että $p \nmid i$. Tässä $p \nmid i$ seuraa siitä, että $\mathrm{ord}(g^i) = \mathrm{ord}(g)/\operatorname{syt}(i, \mathrm{ord}(g))$ ja koska γ on isomorfismi, niin $\mathrm{ord}(g^i) = \mathrm{ord}(g)$ ja edelleen $\operatorname{syt}(i, \mathrm{ord}(g)) = 1$. Koska $\mathrm{ord}(g) = p^2$, niin $\operatorname{syt}(i, p^2) = 1$ ja täten myös $\operatorname{syt}(i, p) = 1$, joten $p \nmid i$. Nyt $g^{pi} = g^{2p}$, josta saadaan $g^{pi-2p} = 1$. Koska $\mathrm{ord}(g) = p^2$, niin $p^2 | (pi - 2p)$ ja edelleen $p | i - 2$. Siis $i - 2 = mp$, joten $i = 2 + mp$. Täten $\gamma(g) = g^{2+mp}$. Nyt toisen neliön kommutatiivisuudesta saadaan $g + K = g^{2+mp} + K$, joten $g^{1+mp} \in K$. Tällöin $g^{p(1+mp)} = 1$, ja täten $g^p (g^{p^2})^m = 1$. Mutta koska $g^{p^2} = 1$, niin tästä seuraa, että $g^p = 1$. Koska ryhmän G kertaluku on p^2, on tämä ristiriita. Siispä päättelemme, että laajennukset eivät ole ekvivalentit.

Esimerkki 3.16. [2, s. 13] Olkoon p alkuluku. Tällöin ryhmällä C_p on p epäekvivalenttia laajennusta G ryhmällä C_p.

Tarkastellaan seuraavia lyhyitä eksakteja jonoja

$$1 \to C_p \xrightarrow{\alpha} C_{p^2} \xrightarrow{\beta_i} C_p \to 1, \quad i = 1, \ldots, p-1.$$

Tässä $C_p = \langle a \rangle = \{1, a, a^2, \ldots, a^{p-1}\}$, $C_{p^2} = \langle g \rangle = \{1, g, g^2, \ldots, g^{p^2-1}\}$ ja homomorfismit α ja β ovat

$$\begin{aligned} &\alpha \colon C_p \to C_{p^2}, \quad a \mapsto g^p \\ &\beta_i \colon C_{p^2} \to C_p, \quad g \mapsto a^i, \quad i = 1, 2, \ldots, p-1. \end{aligned}$$

Nyt $\beta_i(\alpha(a)) = \beta_i(g^p) = a^{pi} = 1$ ryhmässä C_p, joten $\operatorname{im}\alpha \subset \ker\beta_i$. Toisaalta, kun $g^n \in \ker\beta_i$, niin $1 = \beta_i(g^n) = (a^i)^n = a^{in}$. Siis $p | in$, ja koska $p > i$, niin $p|n$, eli $n = mp$. Nyt $g^n = (g^p)^m = \alpha(a)^m = \alpha(a^m)$, joten $g^n \in \operatorname{im}\alpha$. Siispä

$\ker \beta_i \subset \operatorname{im} \alpha$. Täten $\operatorname{im} \alpha = \ker \beta_i$, joten jonot ovat eksakteja. Väitämme, että mitkä tahansa kaksi laajennusta β_i ja β_j, $i \neq j$, ovat epäekvivalentteja. Oletetaan, että $(C_p, \alpha, \beta_i) \simeq (C_p, \alpha, \beta_j)$, eli kaaviossa

$$\begin{array}{ccccccccc} 1 & \longrightarrow & C_p & \xrightarrow{\alpha} & C_{p^2} & \xrightarrow{\beta_i} & C_p & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & C_p & \xrightarrow{\alpha} & C_{p^2} & \xrightarrow{\beta_j} & C_p & \longrightarrow & 1 \end{array}$$

on $\alpha = \gamma\alpha$ ja $\beta_i = \beta_j\gamma$. Tästä seuraa, että

$$g^p = \alpha(a) = \gamma(\alpha(a)) = \gamma(g^p) = \gamma(g)^p.$$

Nyt $\gamma(g) = g^r$ virittää ryhmän C_{p^2}, sillä γ on isomorfismi. Siispä $\operatorname{ord}(g^r) = \operatorname{ord}(g)$, sillä $C_{p^2} = \langle g \rangle$. Koska $\operatorname{ord}(g^r) = \operatorname{ord}(g)/\operatorname{syt}(r, \operatorname{ord}(g))$ ja $\operatorname{ord}(g^r) = \operatorname{ord}(g)$, niin $\operatorname{syt}(r, \operatorname{ord}(g)) = 1$. Koska $\operatorname{ord}(g) = p^2$, niin $\operatorname{syt}(r, p^2) = 1$. Täten myös $\operatorname{syt}(r, p) = 1$, joten $p \nmid r$ ja $g^p = \gamma(g^p) = g^{pr}$ ryhmässä C_{p^2}. Tällöin $r \equiv 1 \pmod{p}$. Toisaalta

$$a^i = \beta_i(g) = \beta_j(\gamma(g)) = \beta_j(g^r) = a^{jr}$$

ryhmässä C_p. Tästä seuraa, että $i \equiv jr \pmod{p}$. Koska $r \equiv 1 \pmod{p}$, niin saadaan $i \equiv j \pmod{p}$. Mutta koska $i, j < p$, niin täytyy olla $i = j$, ja täten $\beta_i = \beta_j$. Näin olemme todistaneet väitteen.

4 Ryhmäkohomologia

4.1 Ensimmäinen kohomologiaryhmä

Aloitetaan 1-kosyklin määritelmällä.

Määritelmä 4.1. Olkoot Q ryhmä ja K Q-moduli. Kuvausta $f\colon Q \to K$, joka toteuttaa ehdon

$$f(xy) = xf(y) + f(x)$$

aina, kun $x, y \in Q$, kutsutaan *1-kosykliksi*.

Tästä eteenpäin tässä aliluvussa puhutaan 1-kosykleistä lyhyemmin kosykleinä. Määritellään sitten 1-koreunat, joista tässä aliluvussa käytetään määritelmän jälkeen nimitystä koreuna.

Määritelmä 4.2. Olkoot Q ryhmä ja K Q-moduli. Kuvausta $g\colon Q \to K$, joka toteuttaa ehdon

$$g(x) = xa - a$$

jollain $a \in K$, kutsutaan *1-koreunaksi*.

Määritelmä 4.3. Olkoot Q ryhmä ja K Q-moduli. Määritellään

$$Z^1(Q,K) = \{\text{ kaikki kosyklit} \quad f\colon Q \to K\,\}$$

ja

$$B^1(Q,K) = \{\text{ kaikki koreunat} \quad g\colon Q \to K\,\}.$$

Edellä määritellyistä joukoista $Z^1(Q,K)$ on Abelin ryhmä, jossa laskutoimituksena on pisteittäinen yhteenlasku $f + f'\colon x \mapsto f(x) + f'(x)$. Joukko $B^1(Q,K)$ on ryhmän $Z^1(Q,K)$ aliryhmä. Täten näistä kahdesta ryhmästä saadaan seuraava tekijäryhmä. [1, s. 3, 4]

Määritelmä 4.4. Tekijäryhmää $H^1(Q,K) = Z^1(Q,K)/B^1(Q,K)$ kutsutaan *ensimmäiseksi kohomologiaryhmäksi.*

Olkoon K triviaali Q-moduli, siis $qk = k$ aina, kun $q \in Q$ ja $k \in K$. Tällöin, jos $f \in Z^1(Q,K)$, niin $f(xy) = xf(y) + f(x)$. Koska $x \in Q$ ja $f(y) \in K$, niin $xf(y) = f(y)$. Nyt $f(xy) = f(y) + f(x)$ aina, kun $f \in Z^1(Q,K)$, joten $Z^1(Q,K) = \mathrm{Hom}(Q,K)$. Toisaalta, jos $g \in B^1(Q,K)$, niin $g(x) = xa - a$ ja koska $x \in Q$ ja $a \in K$, niin $xa = a$. Tällöin $g(x) = a - a = 0$ aina, kun $g \in B^1(Q,K)$, joten $B^1(Q,K) = 0$. Täten $H^1(Q,K) = \mathrm{Hom}(Q,K)$. [2, s. 25]

Apulause 4.1. *Olkoot Q ryhmä, K Q-moduli ja G ryhmän K laajennus ryhmällä Q. Jos C on ryhmän K komplementti ryhmässä G, niin $C = \ell(Q)$ jollain sellaisella nostolla $\ell\colon Q \to G$, että ℓ on homomorfismi.* [2, s. 26]

Todistus. Oletetaan, että C on ryhmän K komplementti ryhmässä G. Tällöin jokainen $g \in G$ voidaan esittää yksikäsitteisesti muodossa $g = kc$, missä $k \in K$ ja $c \in C$. Määritellään nyt kuvaus $\ell\colon Q \to G$ säännöllä $\ell(q) = c$, missä $g = kc$ ja $p(g) = q$. Jos $p(g') = q$ jollain $g' \in G$, niin tällöin $p(g) = q = p(g')$, joten $p(g')p(g)^{-1} = p(g')p(g^{-1}) = p(g'g^{-1}) = 1$, ja täten $g'g^{-1} \in K$. Nyt $g' = g'g^{-1}g = g'g^{-1}kc$, missä $g'g^{-1}k \in K$. Siis $p(g') = q$ ja $g' = (g'g^{-1}k)c$, joten $\ell(q) = c$.

Osoitetaan, että ℓ on nosto. Koska $c = 1c \in G$, missä $1 \in K$, niin $p(\ell(q)) = p(c) = q$, missä $\ell(q) = c$, $g = 1c$ ja $p(g) = q$. Täten $p\ell = \mathrm{id}_Q$, joten kuvaus ℓ on nosto. Osoitetaan sitten, että ℓ on homomorfismi. Ensinnäkin, $\ell(q)\ell(q') = cc'$, missä $g = kc$, $g' = k'c'$, $p(g) = q$ ja $p(g') = q'$. Toisaalta, $p(gg') = qq'$ ja $gg' = kck'c' = kck'c^{-1}cc'$, ja koska $ck'c^{-1} \in K$, niin $kck'c^{-1} \in K$, joten $\ell(qq') = cc'$. Täten $\ell(q)\ell(q') = \ell(qq')$, joten kuvaus ℓ on homomorfismi.

Osoitetaan lopuksi, että $C = \ell(Q)$. Kuvauksen ℓ määritelmän perusteella $\ell(Q) \subset C$. Osoitetaan, että myös $C \subset \ell(Q)$. Valitaan mielivaltainen $c \in C$. Valitaan $g = 1c = c$, ja olkoon $p(g) = q$. Koska $g = 1c$ ja $p(g) = q$, niin tällöin $\ell(q) = c$. Täten $c \in \ell(Q)$, ja edelleen $C \subset \ell(Q)$. Siispä $C = \ell(Q)$. $\square$

Palautetaan lukijalle mieleen, että ryhmän G aliryhmä X on aliryhmän H konjugaatti, jos $X = aHa^{-1} = \{\, aha^{-1} \mid h \in H \,\}$ jollain $a \in G$. Täten ryhmän H konjugaattiluokka on joukko $\{\, X \leq G \mid X = aHa^{-1} \,\}$, missä $a \in G$. [4, s. 101]

Propositio 4.1. *Olkoon K Q-moduli. Tällöin on olemassa bijektio joukon $H^1(Q, K)$ ja ryhmän K kanssa komplementaaristen aliryhmien $H \leq K \rtimes Q$ konjugaattiluokkien joukon välillä, joka kuvaa ryhmän Q konjugaattiluokan nollaksi.*

Todistus (vrt. [2, s. 26]). On olemassa bijektio ryhmän K kanssa komplementaaristen aliryhmien $H \leq K \rtimes Q$ ja kosyklien $f \in Z^1(Q, K)$ välillä. Jos H on ryhmän K komplementti, niin edellisen apulauseen perusteella $H = \ell(Q)$ jollain sellaisella nostolla $\ell\colon Q \to K \rtimes Q$, joka on homomorfismi. Koska ℓ on nosto, niin $\ell(x) = (f(x), x)$ jollain $f\colon Q \to K$. Tällöin $H = \{\, (f(x), x) \mid x \in Q \,\}$. Osoitetaan, että $f \in Z^1(Q, K)$. Koska ℓ on homomorfismi, niin $\ell(x)\ell(x') = \ell(xx')$. Mutta koska

$$\ell(x)\ell(x') = (f(x), x)(f(x'), x') = (f(x) + xf(x'), xx')$$

ja

$$\ell(xx') = (f(xx'), xx'),$$

niin on oltava $f(xx') = f(x) + xf(x')$. Nyt kosyklin määritelmän mukaan $f \in Z^1(Q, K)$. Lisäksi kaksi komplementtia ovat konjugaatteja täsmälleen silloin, kun koreunat erottavat niiden kosyklit toisistaan, sillä jos H ja H' ovat konjugaatteja, niin $H' = aHa^{-1} = a\ell(Q)a^{-1}$ jollain $a \in K$. Siis $\ell'(x) = a\ell(x)a^{-1}$ aina, kun $x \in Q$. Mutta

$$(f'(x), x) = \ell'(x) = a\ell(x)a^{-1} = (a, 1)(f(x), x)(-a, 1) = (a + f(x) - xa, x),$$

joten $f'(x) = a + f(x) - xa$ ja edelleen $f(x) - f'(x) = xa - a$. Nyt koreunan määritelmän mukaan $f - f' \in B^1(Q, K)$. Täten ryhmän $B^1(Q, K)$ sivuluokat ryhmässä $Z^1(Q, K)$ vastaavat komplementtien H K-konjugaattiluokkia joukossa K, tai joukossa $K \rtimes Q$, sillä $K \rtimes Q = HK$. □

Seuraus 4.1. *Kaikki ryhmän K komplementit ryhmässä $K \rtimes Q$ ovat konjugaatteja, jos ja vain jos $H^1(Q, K) = 0$.* [2, s. 26]

Äärellisten ryhmien kohomologiaryhmille on voimassa seuraava tulos.

Propositio 4.2. *Oletetaan, että Q on äärellinen ryhmä ja että K on Q-moduli. Tällöin jokaisella ryhmän $H^1(Q, K)$ alkiolla on äärellinen kertaluku, joka jakaa luvun $|Q|$.*

Todistus. [2, s. 26] Olkoot $f \in Z^1(Q,K)$ ja $a = \sum_{y\in Q} f(y)$. Kosyklin määritelmän mukaan $xf(y) - f(xy) + f(x) = 0$. Kun summataan tämän kaavan mukaan, niin saadaan

$$\begin{aligned} 0 &= x\sum_{y\in Q} f(y) - \sum_{y\in Q} f(xy) + f(x)\sum_{y\in Q} 1 \\ &= xa - a + |Q|f(x). \end{aligned}$$

Tästä seuraa, että $|Q|f \in B^1(Q,K)$, tai että $|Q|Z^1(Q,K) \subseteq B^1(Q,K)$. Täten $|Q|H^1(Q,K) = 0$. □

Seuraus 4.2. *Oletetaan, että Q on äärellinen ryhmä ja että K on sellainen äärellinen Q-moduli, että* $\operatorname{syt}(|Q|,|K|) = 1$. *Tällöin $H^1(Q,K) = 0$.*

Todistus. [2, s. 26] Olkoon $f \in Z^1(Q,K)$. Koska $f(x) \in K$, niin $|K|f(x) = 0$ ryhmässä K. Tällöin, kun $f + B^1 \in H^1(Q,K)$, niin $|K|(f+B^1) = 0$ ryhmässä H^1, joten $\operatorname{ord}(f+B^1) \mid |K|$. Edellisen proposition mukaan $\operatorname{ord}(f+B^1) \mid |Q|$. Täten $\operatorname{ord}(f+B^1) \mid \operatorname{syt}(|K|,|Q|)$. Koska $\operatorname{syt}(|Q|,|K|) = 1$, niin $\operatorname{ord}(f+B^1) = 1$. Siispä $1(f+B^1) = f + B^1 = 0$. □

4.2 Toinen kohomologiaryhmä

Määritelmä 4.5. Olkoon G ryhmän K laajennus ryhmällä Q ja olkoon $\ell\colon Q \to G$ sellainen nosto, että $\ell(1) = 0$. Tällöin *2-kosykli* on sellainen kuvaus $f\colon Q \times Q \to K$, että

$$\ell(x) + \ell(y) = f(x,y) + \ell(xy)$$

aina, kun $x, y \in Q$.

Tästä eteenpäin 2-kosykleistä puhutaan lyhyemmin kosykleinä. On luonnollista valita sellaisia nostoja, joilla $\ell(1) = 0$. Tästä syystä kyseinen ehto on tässä tutkielmassa liitetty kosyklin määritelmään. Yleensä tällaisia kosyklejä kutsutaan normalisoiduiksi kosykleiksi.

Kosykli on riippuvainen noston ℓ valinnasta. Kun G on lohkeava laajennus, niin silloin on olemassa nosto joka on homomorfismi; vastaava kosykli on identtisesti 0. Tästä syystä kosykliä voidaankin pitää esteenä noston homomorfismina olemiselle. Kosyklit siis kuvaavat kuinka laajennus eroaa lohkeavasta laajennuksesta. [4, s. 795]

Esimerkki 4.1. [2, s. 17] Tarkastellaan laajennusta $1 \to C_2 \xrightarrow{\alpha} C_4 \xrightarrow{\beta} C_2 \to 1$, missä $K = C_2 = \langle a \rangle$, $C_4 = \langle g \rangle$, $Q = C_2 = \langle x \rangle$ ja $\alpha(a) = g^2$, $\beta(g) = x$. Osoitetaan, että nostoa $\ell\colon C_2 \to C_4$, $\ell(1) = 1$ ja $\ell(x) = g$, vastaava kosykli on $f\colon C_2 \times C_2 \to C_2$, $f(1,1) = f(1,x) = f(x,1) = 1$ ja $f(x,x) = a$. Tutkitaan asiaa kosyklin määritelmän $\ell(z)\ell(y) = f(z,y)\ell(zy)$ avulla. Kun $z = y = 1$, niin

$$\ell(z)\ell(y) = \ell(1)\ell(1) = 1 = f(1,1)\ell(1\cdot 1) = f(z,y)\ell(zy).$$

Kun $z = 1$ ja $y = x$, niin

$$\ell(z)\ell(y) = \ell(1)\ell(x) = 1g = f(1, x)\ell(1x) = f(z, y)\ell(zy).$$

Kun $z = x$ ja $y = 1$, niin

$$\ell(z)\ell(y) = \ell(x)\ell(1) = g1 = g = 1g = f(x, 1)\ell(x1) = f(z, y)\ell(zy).$$

Lopuksi, kun $z = y = x$, niin

$$\begin{aligned}\ell(z)\ell(y) &= \ell(x)\ell(x) = g^2 = a = f(x, x) = f(x, x)1 \\ &= f(x, x)\ell(1) = f(x, x)\ell(x^2) = f(x, x)\ell(xx) = f(z, y)\ell(zy).\end{aligned}$$

Edellisessä yhtälöketjussa kohta $g^2 = a$ tulee siitä, että ryhmä C_2 samaistetaan ryhmän C_4 aliryhmäksi injektiivisen homomorfismin α avulla, siis $C_2 = \alpha(C_2)$, ja täten myös ryhmän C_2 alkiot samaistetaan kuviensa kanssa. Koska $\alpha(a) = g^2$, niin $a = g^2$.

Koska kaikilla $z, y \in Q = C_2$ on voimassa yhtälö $\ell(z)\ell(y) = f(z, y)\ell(zy)$, niin kuvaus f nostoa ℓ vastaava kosykli.

Esimerkki 4.2. [2, s. 18] Määrätään laajennuksen $1 \to C_2 \xrightarrow{\alpha} G \xrightarrow{\beta} C_2 \to 1$ keskimmäinen ryhmä, kun kuvaukset α ja β sekä nosto ℓ ja kosykli f ovat samat kuin edellisessä esimerkissä.

Ryhmässä $G = C_2 \times C_2 = \{(1, 1), (1, a), (x, 1), (x, a)\}$ on seuraava kertolasku

$$(x, a)(y, b) = (xy, f(x, y)ab).$$

Koska $x^2 = a^2 = 1$, niin saadaan

$$\begin{aligned}(x, a)^4 &= ((x, a)(x, a))^2 = (x^2, f(x, x)a^2)^2 = ((1, a))^2 \\ &= (1, a)(1, a) = (1, f(1, 1)a^2) = (1, 1).\end{aligned}$$

Koska $(x, a)^2 = (1, a) \neq (1, 1)$, niin ryhmä G on isomorfinen ryhmän C_4 kanssa.

Propositio 4.3. *Olkoot Q ryhmä, K Q-moduli ja $0 \to K \to G \to Q \to 1$ operaattorit realisoiva laajennus. Jos $\ell\colon Q \to G$ on nosto, jolla $\ell(1) = 0$, ja $f\colon Q \times Q \to K$ on vastaava kosykli, niin*

(i) $f(1, y) = 0 = f(x, 1)$ *aina, kun $x, y \in Q$,*

(ii) kosykli-identiteetti *pätee: aina, kun $x, y, z \in Q$, niin*

$$f(x, y) + f(xy, z) = xf(y, z) + f(x, yz).$$

Todistus. [4, s. 796]

(i) Asetetaan $x = 1$ yhtälöön $\ell(x)+\ell(y) = f(x, y)+\ell(xy)$. Yhtälö saadaan muotoon $\ell(y) = f(1, y) + \ell(y)$, josta edelleen saadaan $f(1, y) = 0$. Asettamalla $y = 1$ yhtälö saadaan muotoon $\ell(x) = f(x, 1)+\ell(x)$, josta saadaan $f(x, 1) = 0$.

(ii) Kosykli-identiteetti seuraa ryhmän G assosiatiivisuudesta. Aina, kun $x, y, z \in Q$, niin

$$\begin{aligned}[\ell(x) + \ell(y)] + \ell(z) &= f(x, y) + \ell(xy) + \ell(z) \\ &= f(x, y) + f(xy, z) + \ell(xyz).\end{aligned}$$

Toisaalta,

$$\begin{aligned}\ell(x) + [\ell(y) + \ell(z)] &= \ell(x) + f(y, z) + \ell(yz) \\ &= \ell(x) + f(y, z) - \ell(x) + \ell(x) + \ell(yz) \\ &= xf(y, z) + \ell(x) + \ell(yz) \\ &= xf(y, z) + f(x, yz) + \ell(xyz).\end{aligned}$$

Nyt ryhmän G assosiatiivisuuden mukaan

$$f(x, y) + f(xy, z) + \ell(xyz) = xf(y, z) + f(x, yz) + \ell(xyz),$$

joten

$$f(x, y) + f(xy, z) = xf(y, z) + f(x, yz).$$

□

Kuten seuraavaksi osoitetaan, myös käänteinen suunta pätee. Seuraava tulos yleistää ryhmän $K \rtimes Q$ muodostamisen propositiossa 3.8. [4, s. 796]

Lause 4.1. *Olkoot Q ryhmä ja K Q-moduli. Kuvaus $f\colon Q \times Q \to K$ on kosykli, jos ja vain jos se toteuttaa kosykli-identiteetin*

$$xf(y, z) - f(xy, z) + f(x, yz) - f(x, y) = 0$$

ja $f(1, y) = 0 = f(x, 1)$ aina, kun $x, y, z \in Q$.

Tarkemmin sanottuna, ryhmällä K on olemassa operaattorit realisoiva laajennus G ryhmällä Q ja on olemassa nosto $\ell\colon Q \to G$, jota vastaava kosykli on f.

Todistus. [4, s. 796] Propositio 4.3 antaa välttämättömyyden. Riittää siis osoittaa käänteinen suunta. Määritellään joukon G olevan kaikkien järjestettyjen parien $(a, x) \in K \times Q$ joukko, ja määritellään tähän joukkoon laskutoimitus säännöllä

$$(a, x) + (b, y) = (a + xb + f(x, y), xy).$$

Täten, jos f on identtisesti 0, niin $G = K \rtimes Q$. Joukon G ryhmäksi osoittaminen on samankaltainen kuin propositiossa 3.8. Aloitetaan assosiatiivisuuden todistamisella:

$$\begin{aligned}[(a,x)+(b,y)]+(c,z) &= (a+xb+f(x,y),xy)+(c,z)\\ &= (a+xb+f(x,y)+xyc+f(xy,z),xyz)\end{aligned}$$

ja

$$\begin{aligned}(a,x)+[(b,y)+(c,z)] &= (a,x)+(b+yc+f(y,z),yz)\\ &= (a+xb+xyc+xf(y,z)+f(x,yz),xyz).\end{aligned}$$

Nyt kosykli-identiteetin mukaan

$$f(x,y)+f(xy,z) = xf(y,z)+f(x,yz),$$

joten

$$(a+xb+f(x,y)+xyc+f(xy,z),xyz) = (a+xb+xyc+xf(y,z)+f(x,yz),xyz)$$

ja täten assosiatiivisuus on voimassa.

Neutraalialkio on $(0,1)$, sillä

$$(a,x)+(0,1) = (a+x0+f(x,1),x1) = (a+0+0,x) = (a,x)$$

ja

$$(0,1)+(a,x) = (0+1a+f(1,x),1x) = (0+a+0,x) = (a,x).$$

Alkion (a,x) käänteisalkio on $(-x^{-1}a-x^{-1}f(x,x^{-1}),x^{-1})$, sillä

$$\begin{aligned}&(a,x)+(-x^{-1}a-x^{-1}f(x,x^{-1}),x^{-1})\\ &\quad= (a-xx^{-1}a-xx^{-1}f(x,x^{-1})+f(x,x^{-1}),xx^{-1})\\ &\quad= (a-a-f(x,x^{-1})+f(x,x^{-1}),1)\\ &\quad= (0,1)\end{aligned}$$

ja kosykli-identiteetin avulla saadaan

$$\begin{aligned}&(-x^{-1}a-x^{-1}f(x,x^{-1}),x^{-1})+(a,x)\\ &\quad= (-x^{-1}a-x^{-1}f(x,x^{-1})+x^{-1}a+f(x^{-1},x),x^{-1}x)\\ &\quad= (-x^{-1}f(x,x^{-1})+f(x^{-1},x),1)\\ &\quad= (f(x^{-1},xx^{-1})-f(x^{-1}x,x^{-1}),1)\\ &\quad= (f(x^{-1},1)-f(1,x^{-1}),1)\\ &\quad= (0-0,1)\\ &\quad= (0,1).\end{aligned}$$

Täten G on ryhmä.

Määritellään kuvaus $p\colon G \to Q$ säännöllä $p\colon (a,x) \mapsto x$. Nyt määritelmänsä mukaan kuvaus p on surjektio ja sen ydin on $\ker p = \{\,(a,1) \mid a \in K\,\}$. Kuvaus p on homomorfismi, sillä

$$p((a,x)+(b,y)) = p(a+xb+f(xy),xy) = xy = p(a,x)p(b,y).$$

Jos määritellään kuvaus $i\colon K \to G$ säännöllä $i\colon a \mapsto (a,1)$, niin tällöin $\operatorname{im} i = \ker p$ ja täten saadaan laajennus $0 \to K \xrightarrow{i} G \xrightarrow{p} Q \to 1$.

Osoitetaan sitten, että tämä laajennus realisoi operaattorit. Täytyy siis osoittaa, että jokaisella nostolla ℓ pätee $xa = \ell(x)+a-\ell(x)$ aina, kun $a \in K$ ja $x \in Q$. Nyt $\ell(x) = (b,x)$ jollakin $b \in K$ ja

$$\begin{aligned}\ell(x)+(a,1)-\ell(x) &= (b,x)+(a,1)-(b,x)\\ &= (b+xa,x)+(-x^{-1}b-x^{-1}f(x,x^{-1}),x^{-1})\\ &= (b+xa+x[-x^{-1}b-x^{-1}f(x,x^{-1})]+f(x,x^{-1}),1)\\ &= (xa,1).\end{aligned}$$

Lopuksi täytyy vielä osoittaa, että f on noston ℓ määräämä kosykli. Valitaan nosto $\ell(x) = (0,x)$ aina, kun $x \in Q$. Noston ℓ määräämä kosykli F on

$$\begin{aligned}F(x,y) &= \ell(x)+\ell(y)-\ell(xy)\\ &= (0,x)+(0,y)-(0,xy)\\ &= (f(x,y),xy)+(-(xy)^{-1}f(xy,(xy)^{-1}),(xy)^{-1})\\ &= (f(x,y)+xy[-(xy)^{-1}f(xy,(xy)^{-1})]+f(xy,(xy)^{-1}),xy(xy)^{-1})\\ &= (f(x,y),1).\end{aligned}$$

□

Määritelmä 4.6. Jos Q on ryhmä, K on Q-moduli ja f on kosykli, niin käytetään lauseessa 4.1 muodostetulle ryhmän K laajennuksen ryhmällä Q keskimmäiselle ryhmälle merkintää $G(K,Q,f)$.

Seuraava tulos osoittaa, että olemme löytäneet kaikki Q-modulin K laajennukset ryhmällä Q. [4, s. 797]

Lause 4.2. *Oletetaan, että Q on ryhmä, K on Q-moduli ja G on ryhmän K operaattorit realisoiva laajennus ryhmällä Q. Tällöin on olemassa sellainen kosykli $f\colon Q \times Q \to K$, että*

$$G \cong G(K,Q,f).$$

Todistus. [4, s. 798] Olkoot $\ell\colon Q \to G$ nosto ja $f\colon Q \times Q \to K$ sitä vastaava kosykli. Siis aina, kun $x,y \in K$, yhtälö

$$\ell(x)+\ell(y) = f(x,y)+\ell(xy)$$

pätee. Koska G on sivuluokkien erillinen yhdiste, $G = \bigcup_{x \in Q} K + \ell(x)$, niin jokainen $g \in G$ voidaan esittää yksikäsitteisesti muodossa $g = a + \ell(x)$ joillain $a \in K$ ja $x \in Q$. Yksikäsitteisyydestä seuraa, että kuvaus $\varphi\colon G \to G(K, Q, f)$, joka määritellään säännöllä

$$\varphi\colon g = a + \ell(x) \mapsto (a, x),$$

on hyvin määritelty bijektio. Osoitetaan, että φ on isomorfismi.

$$\begin{aligned}
\varphi(a + \ell(x) + b + \ell(y)) &= \varphi(a + \ell(x) + b - \ell(x) + \ell(x) + \ell(y)) \\
&= \varphi(a + xb + \ell(x) + \ell(y)) \\
&= \varphi(a + xb + f(x, y) + \ell(xy)) \\
&= (a + xb + f(x, y), xy) \\
&= (a, x) + (b, y) \\
&= \varphi(a + \ell(x)) + \varphi(b + \ell(y)).
\end{aligned}$$

□

Huomautus. Jos $a \in K$, niin $\varphi(a) = \varphi(a + \ell(1)) = (a, 1)$ ja jos $x \in Q$, niin $\varphi(\ell(x)) = (0, x)$. Tämä ei olisi tilanne, jos olisimme valinneet sellaisen noston ℓ, jolla $\ell(1) \neq 0$. [4, s. 798]

Huomautus. Laajennukset G ja $G(K, Q, f)$ eivät ole pelkästään isomorfiset, vaan ne ovat myös ekvivalentit. Tarkastellaan seuraavaa kaaviota

$$\begin{array}{ccccccccc}
0 & \longrightarrow & K & \xrightarrow{\ i\ } & G & \xrightarrow{\ p\ } & Q & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \mathrm{id}_K} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \mathrm{id}_Q} & & \\
0 & \longrightarrow & K & \xrightarrow{\ i'\ } & G(K, Q, f) & \xrightarrow{\ p'\ } & Q & \longrightarrow & 1
\end{array}$$

missä

$$\begin{aligned}
i&\colon K \to G, \quad a \mapsto a + \ell(1) \\
p&\colon G \to Q, \quad a + \ell(x) \mapsto x \\
i'&\colon K \to G(K, Q, f), \quad a \mapsto (a, 1) \\
p'&\colon G(K, Q, f) \to Q, \quad (a, x) \mapsto x \\
\varphi&\colon G \to G(K, Q, f), \quad a + \ell(x) \mapsto (a, x).
\end{aligned}$$

Nyt $i'(a) = (a, 1)$ ja $\varphi i(a) = \varphi(a + \ell(1)) = (a, 1)$, joten $i' = \varphi i$. Samoin $p(a + \ell(x)) = x$ ja $p'\varphi(a + \ell(x)) = p'(a, x) = x$, joten $p = p'\varphi$. Täten $(G, i, p) \simeq (G(K, Q, f), i', p')$. [4, s. 801]

Olemme nyt kuvailleet kaikki laajennukset kosyklien suhteen, mutta kosyklit määrittyvät nostoista. Millä tahansa laajennuksella on monia eri nostoja, joten kuvauksessamme, joka riippuu noston valinnasta, täytyy olla toistoa. [4, s. 798]

Apulause 4.2. *Olkoot Q ryhmä, K Q-moduli ja G ryhmän K operaattorit realisoiva laajennus ryhmällä Q. Olkoot ℓ ja ℓ' nostoja ja f ja f' niitä vastaavat kosyklit. Tällöin on olemassa sellainen kuvaus $h\colon Q \to K$, että $h(1) = 0$ ja aina, kun $x, y \in Q$,*

$$f'(x,y) - f(x,y) = xh(y) - h(xy) + h(x).$$

Todistus. [4, s. 798] Jokaisella $x \in Q$ molemmat $\ell(x)$ ja $\ell'(x)$ kuuluvat ryhmän K samaan sivuluokkaan ryhmässä G, ja täten on olemassa alkio $h(x) \in K$, jolla

$$\ell'(x) = h(x) + \ell(x).$$

Koska $\ell(1) = 0 = \ell'(1)$, niin $h(1) = 0$. Osoitetaan sitten, että apulauseessa esitetty yhtälö on voimassa:

$$\begin{aligned}
\ell'(x) + \ell'(y) &= [h(x) + \ell(x)] + [h(y) + \ell(y)] \\
&= h(x) + \ell(x) + h(y) - \ell(x) + \ell(x) + \ell(y) \\
&= h(x) + xh(y) + \ell(x) + \ell(y) \\
&= h(x) + xh(y) + f(x,y) + \ell(xy) \\
&= h(x) + xh(y) + f(x,y) - h(xy) + \ell'(xy).
\end{aligned}$$

Kosyklin määritelmän mukaan f' toteuttaa yhtälön $\ell'(x) + \ell'(y) = f'(x,y) + \ell'(xy)$. Täten

$$f'(x,y) = h(x) + xh(y) + f(x,y) - h(xy),$$

joka saadaan haluttuun muotoon

$$f'(x,y) - f(x,y) = xh(y) - h(xy) + h(x).$$

□

Määritelmä 4.7. Olkoot Q ryhmä ja K Q-moduli. Tällöin kuvausta $g\colon Q \times Q \to K$ kutsutaan *2-koreunaksi*, jos on olemassa sellainen kuvaus $h\colon Q \to K$, että $h(1) = 0$ ja aina, kun $x, y \in Q$,

$$g(x,y) = xh(y) - h(xy) + h(x).$$

Osoitimme apulauseessa 4.2, että jos f ja f' ovat laajennuksen G eri nostoista saatavia kosyklejä, niin silloin $f' - f$ on koreuna [4, s. 799]. Käytetään tästä eteenpäin 2-koreunoista nimitystä koreuna.

Määritelmä 4.8. Olkoot Q ryhmä ja K Q-moduli. Määritellään

$$Z^2(Q,K) = \{\, \text{kaikki kosyklit} \quad f\colon Q \times Q \to K \,\}$$

ja

$$B^2(Q,K) = \{\, \text{kaikki koreunat} \quad g\colon Q \times Q \to K \,\}.$$

Propositio 4.4. *Olkoot Q ryhmä ja K Q-moduli. Tällöin $Z^2(Q,K)$ on Abelin ryhmä, jossa laskutoimituksena on pisteittäinen yhteenlasku*

$$f + f' \colon (x,y) \mapsto f(x,y) + f'(x,y),$$

ja $B^2(Q,K)$ on ryhmän $Z^2(Q,K)$ aliryhmä.

Todistus. [4, s. 799] Joukon Z^2 ryhmäksi todistamiseksi riittää osoittaa, että $f - f'$ toteuttaa propositiossa 4.3 esiintyvät yhtälöt. Koska

$$(f - f')(1,y) = f(1,y) - f'(1,y) = 0 - 0 = 0$$

ja

$$(f - f')(x,1) = f(x,1) - f'(x,1) = 0 - 0 = 0,$$

on ensimmäinen yhtälö voimassa. Osoitetaan sitten, että myös toinen yhtälö on voimassa.

$$\begin{aligned}
&(f-f')(x,y) + (f - f')(xy,z) \\
&\quad = f(x,y) - f'(x,y) + f(xy,z) - f'(xy,z) \\
&\quad = f(x,y) + f(xy,z) - (f'(x,y) + f'(xy,z)) \\
&\quad = xf(y,z) + f(x,yz) - (xf'(y,z) + f'(x,yz)) \\
&\quad = x(f(y,z) - f'(y,z)) + f(x,yz) - f'(x,yz) \\
&\quad = x(f - f')(y,z) + (f - f')(x,yz).
\end{aligned}$$

Siis myös toinen yhtälö on voimassa. Täten $f - f' \in Z^2$ aina, kun $f, f' \in Z^2$, joten Z^2 on ryhmä.

Osoitetaan sitten, että B^2 on ryhmän Z^2 aliryhmä. Aloitetaan osoittamalla, että jokainen koreuna g on kosykli. Täytyy siis osoittaa, että g toteuttaa proposition 4.3 molemmat yhtälöt. Koska

$$g(1,y) = 1h(y) - h(1y) + h(1) = h(y) - h(y) + 0 = 0$$

ja

$$g(x,1) = xh(1) - h(x1) + h(x) = 0 - h(x) + h(x) = 0,$$

on ensimmäinen yhtälö on voimassa. Myös toinen yhtälö on voimassa, sillä

$$\begin{aligned}
g(x,y) + g(xy,z) &= xh(y) - h(xy) + h(x) + xyh(z) - h(xyz) + h(xy) \\
&= xh(y) + h(x) + xyh(z) - h(xyz) + xh(yz) - xh(yz) \\
&= xyh(z) - xh(yz) + xh(y) + xh(yz) - h(xyz) + h(x) \\
&= x(yh(z) - h(yz) + h(y)) + xh(yz) - h(xyz) + h(x) \\
&= xg(y,z) + g(x,yz).
\end{aligned}$$

Seuraavaksi täytyy osoittaa, että B^2 on epätyhjä osajoukko. Olkoon $h\colon Q \to K$ kuvaus $h(x) = 0$ aina, kun $x \in Q$. Tällöin kuvaus $g\colon Q \times Q \to K$, $g(x, y) = 0$ aina, kun $x, y \in Q$, on koreuna, sillä

$$g(x, y) = 0 = xh(y) - h(xy) + h(x).$$

Siispä B^2 on epätyhjä. Osoitetaan lopuksi, että B^2 on suljettu vähennyslaskun suhteen. Jos $h, h'\colon Q \to K$ osoittavat kuvauksien g ja g' olevan koreunoja, siis $g(x, y) = xh(y) - h(xy) + h(x)$ ja $g'(x, y) = xh'(y) - h'(xy) + h'(x)$, niin tällöin

$$\begin{aligned}(g - g')(x, y) &= g(x, y) - g'(x, y) \\ &= xh(y) - h(xy) + h(x) - xh'(y) + h'(xy) - h'(x) \\ &= x(h - h')(y) - (h - h')(xy) + (h - h')(x).\end{aligned}$$

□

Laajennuksella on aina monia nostoja, ja täten myös monia kosyklejä. Koreuna kuitenkin erottaa kosyklit toisistaan. Tästä syystä seuraava tekijäryhmä syntyy kuin itsestään. [4, s. 800]

Määritelmä 4.9. *Toinen kohomologiaryhmä* määritellään tekijäryhmänä

$$H^2(Q, K) = Z^2(Q, K)/B^2(Q, K).$$

Propositio 4.5. *Olkoot Q ryhmä ja K Q-moduli. Ryhmän K kaksi operaattorit realisoivaa laajennusta G ja G' ryhmällä Q ovat ekvivalentit, jos ja vain jos laajennuksilla G ja G' on olemassa sellaiset kosyklit f ja f', että $f - f'$ on koreuna.*

Todistus. [4, s. 800] Oletetaan ensin, että laajennuksilla G ja G' on olemassa sellaiset kosyklit f ja f', että $f - f'$ on koreuna. Olkoot $\ell\colon Q \to G$ ja $\ell'\colon Q \to G'$ nostoja ja olkoot f ja f' niitä vastaavat kosyklit, siis

$$\ell(x) + \ell(y) = f(x, y) + \ell(xy)$$

ja

$$\ell'(x) + \ell'(y) = f'(x, y) + \ell'(xy)$$

aina, kun $x, y \in Q$. Koreunan määritelmän mukaan on olemassa sellainen kuvaus $h\colon Q \to K$, että $h(1) = 0$ ja

$$f(x, y) - f'(x, y) = xh(y) - h(xy) + h(x)$$

aina, kun $x, y \in Q$. Koska $G = \bigcup_{x \in Q} K + \ell(x)$ on erillinen yhdiste, niin jokainen $g \in G$ voidaan esittää yksikäsitteisesti muodossa $g = a + \ell(x)$ joillakin $a \in K$ ja $x \in Q$. Vastaavasti jokainen $g' \in G'$ voidaan esittää yksikäsitteisesti muodossa $g' = a + \ell'(x)$.

Määritellään kuvaus $\gamma\colon G \to G'$ säännöllä

$$\gamma(a + \ell(x)) = a + h(x) + \ell'(x).$$

Tämä kuvaus tekee kaaviosta

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \xrightarrow{i} & G & \xrightarrow{p} & Q & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}_K} & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \mathrm{id}_Q} & & \\ 0 & \longrightarrow & K & \xrightarrow{i'} & G' & \xrightarrow{p'} & Q & \longrightarrow & 1 \end{array}$$

kommutatiivisen, sillä jos $a \in K$, niin

$$\gamma(a) = \gamma(a + \ell(1)) = a + h(1) + \ell'(1) = a$$

ja toisaalta

$$p'\gamma(a + \ell(x)) = p'(a + h(x) + \ell'(x)) = x = p(a + \ell(x)).$$

Kuvaus γ on myös homomorfismi, sillä

$$\begin{aligned} \gamma([a + \ell(x)] + [b + \ell(y)]) &= \gamma(a + \ell(x) + b - \ell(x) + \ell(x) + \ell(y)) \\ &= \gamma(a + xb + \ell(x) + \ell(y)) \\ &= \gamma(a + xb + f(x, y) + \ell(xy)) \\ &= a + xb + f(x, y) + h(xy) + \ell'(xy) \end{aligned}$$

ja

$$\begin{aligned} &\gamma(a + \ell(x)) + \gamma(b + \ell(y)) \\ &\quad = (a + h(x) + \ell'(x)) + (b + h(y) + \ell'(y)) \\ &\quad = a + h(x) + \ell'(x) + b - \ell'(x) + \ell'(x) + h(y) + \ell'(y) \\ &\quad = a + h(x) + xb + \ell'(x) + h(y) - \ell'(x) + \ell'(x) + \ell'(y) \\ &\quad = a + h(x) + xb + xh(y) + \ell'(x) + \ell'(y) \\ &\quad = a + h(x) + xb + xh(y) + f'(x, y) + \ell'(xy) \\ &\quad = a + xb + (h(x) + xh(y) + f'(x, y)) + \ell'(xy) \\ &\quad = a + xb + f(x, y) + h(xy) + \ell'(xy). \end{aligned}$$

Oletetaan sitten, että laajennukset G ja G' ovat ekvivalentit. Siis on olemassa sellainen isomorfismi γ, että kaaviosta tulee kommutatiivinen, eli $\gamma(a) = a$ aina, kun $a \in K$ ja $x = p(\ell(x)) = p'\gamma(\ell(x))$ aina, kun $x \in Q$. Tästä seuraa, että $\gamma\ell\colon Q \to G'$ on nosto. Kun käytetään kuvausta γ kosyklin f määrittelevään yhtälöön $\ell(x) + \ell(y) = f(x, y) + \ell(xy)$ niin saadaan

$$\gamma\ell(x) + \gamma\ell(y) = \gamma f(x, y) + \gamma\ell(xy),$$

joten γf on noston $\gamma\ell$ määrittämä kosykli. Mutta $\gamma f(x, y) = \gamma(f(x, y)) = f(x, y)$ aina, kun $x, y \in Q$, sillä $f(x, y) \in K$. Täten f on myös toisen laajennuksen kosykli. Toisaalta, jos f' on mikä tahansa muu toisen laajennuksen kosykli, niin apulauseen 4.2 mukaan $f - f' \in B^2$. □

Lause 4.3 (**Schreier**). *Olkoot Q ryhmä, K Q-moduli ja olkoon $e(Q,K)$ kaikkien ryhmän K operaattorit realisoivien laajennusten ryhmällä Q ekvivalenssiluokkien joukko. Tällöin on olemassa bijektio*

$$\varphi\colon H^2(Q,K) \to e(Q,K)$$

joka kuvaa alkion 0 lohkeavan laajennuksen luokkaan.

Todistus. [4, s. 802] Käytetään laajennuksen $0 \to K \to G \to Q \to 1$ ekvivalenssiluokalle merkintää $[G]$. Määritellään kuvaus $\varphi\colon H^2(Q,K) \to e(Q,K)$ säännöllä

$$\varphi\colon f + B^2 \mapsto [G(K,Q,f)],$$

missä f on jokin laajennuksen kosykli ja kohdelaajennus on lauseessa 4.1 muodostettu laajennus.

Ensinnäkin, φ on hyvin määritelty injektio, sillä proposition 4.5 mukaan kosykleillä f ja g pätee $f + B^2 = g + B^2$, jos ja vain jos $[G(Q,K,f)] = [G(Q,K,g)]$. Kuvaus φ on myös surjektio, sillä jos $[G] \in e(Q,K)$, niin lauseen 4.2 ja sitä seuraavan huomautuksen perusteella $[G] = [G(Q,K,f)]$ jollain kosyklillä f, ja täten $[G] = \varphi(f + B^2)$. Lopuksi, nollakosykli vastaa puolisuoraa tuloa, ja koska puolisuora tulo on lohkeavan laajennuksen keskimmäinen ryhmä, niin täten kuvaus φ kuvaa alkion 0 lohkeavan laajennuksen luokkaan. □

Seuraus 4.3. *Olkoot Q ryhmä, K Q-moduli ja $H^2(Q,K) = \{0\}$. Tällöin jokainen ryhmän K operaattorit realisoiva laajennus ryhmällä Q on puolisuora tulo.*

Todistus. [4, s. 802] Edellisen lauseen mukaan joukossa $e(Q,K)$ on vain yksi alkio. Koska lohkeava laajennus on aina olemassa, täytyy tämän alkion olla lohkeavan laajennuksen ekvivalenssiluokka. Täten jokainen ryhmän K operaattorit realisoiva laajennus ryhmällä Q on lohkeava, ja niinpä näiden laajennusten keskimmäinen ryhmä on puolisuora tulo. □

Lause 4.4. *Olkoon G äärellinen ryhmä kertalukua mn, missä* $\operatorname{syt}(m,n) = 1$. *Jos K on kommutatiivinen normaali kertalukua m oleva aliryhmä, niin silloin ryhmällä K on komplementti ja G on puolisuora tulo.*

Todistus. [4, s. 803] Määritellään $Q = G/K$. Seurauksen 4.3 mukaan riittää osoittaa, että jokainen kosykli $f\colon Q \times Q \to K$ on koreuna. Määritellään kuvaus $\sigma\colon Q \to K$ säännöllä

$$\sigma(x) = \sum_{y \in Q} f(x,y).$$

Nyt σ on hyvinmääritelty, sillä Q on äärellinen ja K on kommutatiivinen. Summataan kosykli-identiteetti

$$xf(y,z) - f(xy,z) + f(x,yz) - f(x,y) = 0$$

kaikkien $z \in Q$ yli, jotta saadaan

$$x\sigma(y) - \sigma(xy) + \sigma(x) = nf(x, y)$$

(kun z vaihtelee yli kaikkien ryhmän Q alkioiden, niin tekee myös yz). Koska $\text{syt}(m, n) = 1$, niin on olemassa sellaiset kokonaisluvut s ja t, että $sm+tn = 1$. Määritellään kuvaus $h\colon Q \to K$ säännöllä

$$h(x) = t\sigma(x).$$

Huomataan, että $h(1) = 0$ ja

$$xh(y) - h(xy) + h(x) = f(x, y) - msf(x, y).$$

Mutta $sf(x, y) \in K$ ja siten $msf(x, y) = 0$. Täten f on koreuna. □

Huomautus. Edellistä lausetta kutsutaan Schur-Zassenhausin lauseeksi, mikäli sen oletuksista jätetään pois kohta K on kommutatiivinen. Sen todistaminen vaatisi kuitenkin korkeampaa ryhmäteorian tuntemusta kuin mitä tämän tutkielman lukijalta odotetaan, joten emme sitä todista.

4.3 Yleinen kohomologiaryhmä

Olemme edellä tarkastelleet ensimmäistä ja toista kohomologiaryhmää. Esitellään lopuksi vielä lyhyesti yleisen kohomologiaryhmän määritelmä. Sitä ennen täytyy kuitenkin määritellä n-kosyklit ja n-koreunat. Käytetään tulolle $Q \times Q \times \cdots \times Q$, jossa on n kappaletta ryhmiä Q, merkintää Q^n.

Määritelmä 4.10. Olkoot Q ryhmä ja K Q-moduli ja olkoon $C^n(Q, K)$ kaikkien kuvausten $f\colon Q^n \to K$ joukko. Jos $n = 0$, niin olkoon $C^0(Q, K) = \text{Hom}(1, K) \cong K$. Joukon $C^n(Q, K)$ alkioita kutsutaan *n-koketjuiksi.*

Propositio 4.6. *Joukko $C^n(Q, K)$ yhdessä laskutoimituksen*

$$(f + g)(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) + g(x_1, \ldots, x_n)$$

kanssa on kommutatiivinen ryhmä. [2, s. 22]

Todistus. Aloitetaan osoittamalla, että laskutoimitus + on assosiatiivinen:

$$\begin{aligned}(f + (g + f))(x_1, \ldots, x_n) &= f(x_1, \ldots, x_n) + (g + h)(x_1, \ldots, x_n) \\ &= f(x_1, \ldots, x_n) + g(x_1, \ldots, x_n) + h(x_1, \ldots, x_n) \\ &= (f + g)(x_1, \ldots, x_n) + h(x_1, \ldots, x_n) \\ &= ((f + g) + h)(x_1, \ldots, x_n).\end{aligned}$$

Osoitetaan seuraavaksi, että laskutoimitus + on kommutatiivinen. Koska K on Q-moduli ja $f(x_1, \ldots, x_n) \in K$ ja $g(x_1, \ldots, x_n) \in K$, niin

$$\begin{aligned}(f+g)(x_1, \ldots, x_n) &= f(x_1, \ldots, x_n) + g(x_1, \ldots, x_n) \\ &= g(x_1, \ldots, x_n) + f(x_1, \ldots, x_n) \\ &= (g+f)(x_1, \ldots, x_n).\end{aligned}$$

Neutraalialkio on nollakuvaus $0(x_1, \ldots, x_n) = 0$, sillä

$$(f+0)(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) + 0(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$$

ja

$$(0+f)(x_1, \ldots, x_n) = 0(x_1, \ldots, x_n) + f(x_1, \ldots, x_n) = f(x_1, \ldots, x_n).$$

Alkion f käänteisalkio on $-f$, sillä

$$(f + (-f))(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) - f(x_1, \ldots, x_n) = 0$$

ja

$$(-f + f)(x_1, \ldots, x_n) = -f(x_1, \ldots, x_n) + f(x_1, \ldots, x_n) = 0.$$

Täten joukko $C^n(Q, K)$ yhdessä laskutoimituksen + kanssa on kommutatiivinen ryhmä. □

Määritelmä 4.11. Määritellään kuvaus $\delta_n(f)\colon C^n(Q, K) \to C^{n+1}(Q, K)$, missä $f \in C^n(Q, K)$, säännöllä

$$\begin{aligned}\delta_n(f)(x_1, \ldots, x_{n+1}) = {} & x_1 f(x_2, \ldots, x_{n+1}) \\ & + \sum_{i=1}^{n} (-1)^i f(x_1, \ldots, x_{i-1}, x_i x_{i+1}, \ldots, x_{n+1}) \\ & + (-1)^{n+1} f(x_1, \ldots, x_n).\end{aligned}$$

Kuvaus $\delta_n(f)\colon C^n(Q, K) \to C^{n+1}(Q, K)$ on homomorfismi. Kun $n = 0$, niin kuvausta f pidetään joukon K alkiona, jotta tulossa $x_1 f$ olisi järkeä. [2, s. 22-23]

Määritelmä 4.12. Jos n-koketjulla f on $\delta_n(f) = 0$, niin tällöin n-koketjua f kutsutaan *n-kosykliksi*. Jos taas on olemassa sellainen $n-1$-koketju g, että $f = \delta_{n-1}(g)$, niin silloin n-koketjua f kutsutaan *n-koreunaksi*.

Määritelmä 4.13. Olkoot Q ryhmä ja K Q-moduli. Määritellään

$$Z^n(Q, K) = \{\, \text{kaikki } n\text{-kosyklit} \quad f\colon Q^n \to K \,\}$$

ja

$$B^n(Q, K) = \{\, \text{kaikki } n\text{-koreunat} \quad g\colon Q^n \to K \,\}.$$

Aivan kuten tapauksissa $n = 1$ ja $n = 2$, niin myös yleisesti $Z^n(Q, K)$ on ryhmä ja $B^n(Q, K)$ on sen aliryhmä [5, s. 29]. Näistä saadaan seuraava tekijäryhmä.

Määritelmä 4.14. Tekijäryhmää

$$H^n(Q, K) = Z^n(Q, K)/B^n(Q, K)$$

kutsutaan *yleiseksi kohomologiaryhmäksi*.

Viitteet

[1] Adam, Michael. Einführung in die Gruppenkohomologie. 2001. http://www.uni-math.gwdg.de/mad/seminar-algebra/index.html.

[2] Burde, Dietrich. Cohomology of groups with applications to number theory. Lecture Notes 2004. http://homepage.univie.ac.at/Dietrich.Burde/.

[3] Milne, James. Group Theory. Course Notes 2008. http://www.jmilne.org/math/.

[4] Rotman, Joseph J. Advanced Modern Algebra. Pearson Education, Inc. New Jersey 2002.

[5] Serre, Jean-Pierre. Groupes finis. 2005. http://arxiv.org/PS_cache/math/pdf/0503/0503154v5.pdf.