HELSINGIN YLIOPISTO — HELSINGFORS UNIVERSITET — UNIVERSITY OF HELSINKI

Tiedekunta/Osasto — Fakultet/Sektion — Faculty	Laitos — Institution — Department
Matemaattis-luonnontieteellinen	Matematiikan ja tilastotieteen laitos

Tekijä — Författare — Author

Matti Keskinen

Työn nimi — Arbetets titel — Title

Caleyn lause ja p-ryhmä

Oppiaine — Läroämne — Subject

Matematiikka

Työn laji — Arbetets art — Level	Aika — Datum — Month and year	Sivumäärä — Sidoantal — Number of pages
Pro gradu -tutkielma	Marraskuu 2012	29 s.

Tiivistelmä — Referat — Abstract

Tässä tutkelmassa esitellään algebrallisen ryhmän käsite sekä hieman tavallisesta poikkeava tapa ymmärtää permutaatioita. Työn tärkeimpinä kohtina voi pitää Caleyn lausetta, joka yhdistää permutaation ja ryhmän käsitteet, sekä p-ryhmän käsitettä. Työssä käsitellään myös pintapuolisesti suoraan tuloon liittyviä ryhmiä.

Varsinaisia esitietovaatimuksia työn ymmärtämiseksi ei ole, mutta tietynlainen matemaattinen yleissivisistys on toivottavaa. Kenen tahansa kandidaattitasoisen matematiikan opiskelijan kuitenkin pitäisi pystyä ymmärtämään tämän tutkielman oleellinen sisältö.

Esitelmäni perustuu Joseph J. Rotmanin kirjaan An Introduction to the Theory of Groups [2]. Tukena olen käyttänyt Tauno Metsänkylän ja Marjatta Näätäsen teosta Algebra I [1]. Permutaatioita käsittelevässä luvussa olen tukeutunut Pekka Tuomisen Todennäköisyyslaskenta I- kirjaan [3].

Permutaatioita oli tutkittu jo aikaisemminkin, mutta ryhmien teorian tutkimuksen aloitti varsinaisesti Galois (1811-1832). 1800-luvun lopussa ryhmäteoriaa tutkittiin lähinnä kahdessa päähaarassa. Nämä päähaarat olivat algebralliset ryhmät, erityisesti Lien ryhmät, sekä äärelliset ryhmät. 1900-luvulla ilmaantui kuitenkin kolmas päähaara, äärettömät ryhmät. Nykyään ryhmät esiintyvät monilla matematiikan aloilla, esimerkiksi geometriassa, topologiassa ja logiikassa.

Avainsanat — Nyckelord — Keywords

algebra, ryhmä, Caleyn lause, p-ryhmä, permutaatio

Säilytyspaikka — Förvaringsställe — Where deposited

Kumpulan tiedekirjasto

Muita tietoja — Övriga uppgifter — Additional information

Caleyn lause ja p-ryhmä

Matti Keskinen

Sisältö

Luku 1

Johdanto

Tässä tutkelmassa esitellään algebrallisen ryhmän käsite sekä hieman tavallisesta poikkeava tapa ymmärtää permutaatioita. Työn tärkeimpinä kohtina voi pitää Caleyn lausetta, joka yhdistää permutaation ja ryhmän käsitteet, sekä p-ryhmän käsitettä. Työssä käsitellään myös pintapuolisesti suoraan tuloon liittyviä ryhmiä.

Varsinaisia esitietovaatimuksia työn ymmärtämiseksi ei ole, mutta tietynlainen matemaattinen yleissivisistys on toivottavaa. Kenen tahansa kandidaattitasoisen matematiikan opiskelijan kuitenkin pitäisi pystyä ymmärtämään tämän tutkielman oleellinen sisältö.

Esitelmäni perustuu Joseph J. Rotmanin kirjaan An Introduction to the Theory of Groups [2]. Tukena olen käyttänyt Tauno Metsänkylän ja Marjatta Näätäsen teosta Algebra I [1]. Permutaatioita käsittelevässä luvussa olen tukeutunut Pekka Tuomisen Todennäköisyyslaskenta I- kirjaan [3].

Permutaatioita oli tutkittu jo aikaisemminkin, mutta ryhmien teorian tutkimuksen aloitti varsinaisesti Galois (1811-1832). 1800-luvun lopussa ryhmäteoriaa tutkittiin lähinnä kahdessa päähaarassa. Nämä päähaarat olivat algebralliset ryhmät, erityisesti Lien ryhmät, sekä äärelliset ryhmät. 1900-luvulla ilmaantui kuitenkin kolmas päähaara, äärettömät ryhmät. Nykyään ryhmät esiintyvät monilla matematiikan aloilla, esimerkiksi geometriassa, topologiassa ja logiikassa.

Luku 2

Esitiedot

Määritelmä 2.1. Joukon G *laskutoimitus* $*$ liittää jokaiseen järjestettyyn pariin (g_1, g_2) joukon G alkioita yksikäsitteisen joukon G alkion g_3. Joukon laskutoimitus on siis kuvaus $G \times G \to G$.

Määritelmä 2.2. Olkoon G epätyhjä joukko. Paria $(G, *)$ sanotaan *ryhmäksi*, jos se täyttää seuraavat ehdot:

G0 $*$ on joukossa G määritelty laskutoimitus.

G1 Jos a, b ja c ovat joukon G alkioita, niille pätee $a * (b * c) = (a * b) * c$. Kutsumme tätä ehtoa vastaisuudessa *liitäntälaiksi*.

G2 On olemassa sellainen *neutraalialkioksi* kutsuttu joukon G alkio e, että kaikille joukon G alkioille pätee

$$e * a = a = a * e. \tag{2.3}$$

G3 Jokaista joukon G alkiota a vastaa joukon G alkio a^{-1}. Tätä alkiota kutsutaan alkion a *käänteisalkioksi*. Käänteisalkiolla on seuraava ominaisuus:

$$a * a^{-1} = a^{-1} * a = e. \tag{2.4}$$

Määritelmä 2.5. Ryhmän G alkioiden lukumäärää merkitään $|G|$. Tätä lukumäärää kutsutaan ryhmän *kertaluvuksi*.

Määritelmä 2.6. Jos ryhmän G laskutoimitus on vaihdannainen, eli kaikille $a, b \in G$ pätee

$$a * b = b * a, \tag{2.7}$$

ryhmää kutsutaan *Abelin ryhmäksi*.

Vastaisuudessa ryhmän laskutoimituksesta käytetään niinsanottua multiplikatiivista merkintätapaa, eli kahden ryhmän G alkion a ja b välistä laskutoimitusta merkitään ab.

Lause 2.8. *Ryhmän G neutraalialkio e on yksikäsitteinen.*

Todistus. Jos myös e' on joukon G neutraalialkio, niin määritelmän mukaan $e' = ee' = e$. □

Lause 2.9. *Ryhmän G kunkin alkion a käänteisalkio a^{-1} on yksikäsitteinen.*

Todistus. Jos alkiolla a on myös käänteisalkio a', niin operoimalla yhtälöä $aa' = e$ vasemmalta alkiolla a^{-1} saadaan $(a^{-1}a)a' = a^{-1}e$. Ryhmän määritelmän kohtien G3 ja G2 tämä on ekvivalenttia sen kanssa, että $a' = a^{-1}$. □

Esimerkki 2.10. Mainio esimerkki Abelin ryhmästä ovat reaalilukujen joukko $\mathbb{R}$. Laskutoimituksena on normaali lukujen yhteenlasku. Yhteenlasku on joukon $\mathbb{R}$ suhteen suljettu, sillä laskemalla kaksi reaalilukua yhteen saadaan aina reaaliluku. Liitäntälaki on voimassa, sillä yhteenlaskussa pätee kaikille $a, b, c \in \mathbb{R}$:

$$a + (b + c) = (a + b) + c. \tag{2.11}$$

Neutraalialkio on luku 0 ja alkion $a \in \mathbb{R}$ vasta-alkio on sen vastaluku $-a$.

Esimerkki 2.12. Hieman monimutkaisempi esimerkki ryhmästä on sellaiset kompleksiluvut $\{x + yi \mid x, y \in \mathbb{R}\}$, joille pätee: $x^2 + y^2 = 1$. Laskutoimituksena ryhmässä on kompleksilukujen kertolasku. Kutsutaan tätä joukkoa S^1:ksi.

Jos $(x+yi)$ ja $(z+wi) \in S^1$, niin $(x+yi)(z+wi) \in S^1$. Kerrotaan kaksi joukon alkiota toisillaan:

$$(x + yi)(z + wi) = (xz - yw) + (zy + xw)i.$$

Nyt tulolle pätee

$$\begin{aligned}(xz - yw)^2 + (zy + xw)^2 &= x^2z^2 - 2xzyw + y^2w^2 + z^2y^2 + 2xzyw + x^2w^2 \\ &= x^2(z^2 + w^2) + y^2(w^2 + z^2) \\ &= x^2 + y^2 = 1\end{aligned}$$

Joukon S^1 neutraalialkio on selvästi reaaliluku 1, sillä jos $(x + yi) \in S^1$, niin $(x + yi)1 = 1(x + yi) = (x + yi)$ja $1 = 1 + 0i$, missä $1^2 + 0^2 = 1$

Koska jokaisen joukon S^1 alkion moduli on 1, ja koska jokainen kompleksiluku voidaan kirjoittaa muodossa $z = r(\cos(\varphi) + i\sin(\varphi))$, missä $\varphi \in [0, 2\pi[$, voimme kirjoittaa jokaisen

ryhmän S^1 alkion muodossa $(\cos(\varphi) + i\sin(\varphi))$. Tästä johtuen kiertokulma määrittelee ryhmän alkion yksikäsitteisesti. Oletetaan, että $a, b, c \in S^1$. Nyt

$$\begin{aligned}(ab)c &= ((\cos(\varphi) + i\sin(\varphi))((\cos(\varphi') + i\sin(\varphi')))((\cos(\varphi'') + i\sin(\varphi'')) \\ &= (\cos(\varphi)\cos(\varphi') + i\cos(\varphi)\sin(\varphi') \\ &\quad + i\sin(\varphi)\cos(\varphi') - \sin(\varphi)\sin(\varphi'))((\cos(\varphi'') + i\sin(\varphi'')) \\ &= (\cos(\varphi + \varphi') + i\sin(\varphi + \varphi')((\cos(\varphi'') + i\sin(\varphi'')) \\ &= \cos(\varphi + \varphi' + \varphi'') + i\sin(\varphi + \varphi' + \varphi'') \\ &= a(bc).\end{aligned}$$

Liitäntälaki on siis voimassa. Jokaiselle alkiolle löytyy käänteisalkio äskeisten laskujen perusteella. Alkion $z = \cos(\varphi) + i\sin(\varphi)$ käänteisalkio on $z^{-1} = \cos(-\varphi) + i\sin(-\varphi)$. Nyt $zz^{-1} = 1$.

Määritelmä 2.13. Olkoon G ryhmä. Jos $H \subset G$ ja H on ryhmä ryhmän G laskutoimituksen suhteen, H on ryhmän G *aliryhmä*. Aliryhmää merkitään seuraavasti:

$$H \leq G. \tag{2.14}$$

Jos H on ryhmän G aito osajoukko, aliryhmää H kutsutaan *aidoksi aliryhmäksi*. Sitä merkitään seuraavasti:

$$H < G. \tag{2.15}$$

Esimerkki 2.16. Edellämainitun ryhmän $\mathbb{R}$ eräs aliryhmä on kokonaislukujen joukko $\mathbb{Z}$. Selvästi pätee $\mathbb{R} \supset \mathbb{Z}$. Osoitetaan, että $\mathbb{Z}$ itse on ryhmä. Laskutoimitus on suljettu joukossa, sillä kokonaislukujen yhteenlaskun summa on aina kokonaisluku. Myös liitäntälaki on voimassa, sillä kokonaislukujen joukossa pätee kaikille $a, b, c \in \mathbb{Z}$

$$a + (b + c) = (a + b) + c. \tag{2.17}$$

Neutraalialkio on luku 0 ja alkion $a \in Z$ käänteisalkio on sen vastaluku $-a$. $\mathbb{Z}$ on myös Abelin ryhmä, sillä kaikille $a, b \in \mathbb{Z}$ pätee $a + b = b + a$.

Lause 2.18. *Aliryhmien leikkaus on aliryhmä.*

Todistus. Olkoon G ryhmä ja $S_1, S_2 ... S_n$ sen aliryhmiä. Nyt e_G on jokaisen aliryhmän $S_i, i \in \{1, 2, 3...n\}$ alkio. Jos $a, b \in \cap S_i$, niin $a, b \in S_i$ jokaisella i. Koska jokainen S_i on ryhmä, myös $ab \in S_i$ jokaisella $i \in \{1, 2, 3...n\}$. Nyt $ab \in \bigcap S_i$, joten laskutoimitus on suljettu joukon suhteen. Samalla ajatuksella jokaiselle alkiolle $a \in \cap S_i$ löytyy yksikäsitteinen käänteisalkio $a^{-1} \in \cap S_i$. Liitännäisyys on voimassa, koska kaikki alkiot ovat ryhmän G alkioita. □

Määritelmä 2.19. Jos G on ryhmä ja $a \in G$, alkion a kaikkien potenssien joukkoa kutsutaan *alkion a synnyttämäksi aliryhmäksi*. Tätä merkitään $\langle a \rangle$. Aliryhmän $\langle a \rangle$ alkioiden lukumäärää kutsutaan *alkion a kertaluvuksi*. Sitä merkitään $|\langle a \rangle|$.

Määritelmä 2.20. Ryhmää G sanotaan *sykliseksi ryhmäksi*, jos on olemassa $a \in G$ siten, että $G = \langle a \rangle$.

Lause 2.21. *Jos G on ryhmä ja alkiolla $a \in G$ on äärellinen kertaluku m, niin m on pienin mahdollinen positiivinen vakio, jolla $a^m = e_G$.*

Todistus. Jos $a = e_G$, niin $m = 1$. Jos $a \neq e_G$, on olemassa vakio $k > 1$ siten, että $e, a, a^2 ... a^{k-1}$ ovat ryhmän G eri alkioita ja $a^k = a^i$, kun $0 \leq i \leq k-1$. Väitetään, että $a^k = e_G = a^0$. Jos $a^k = a^i$ jollakin $i \geq 1$, silloin $k - i \leq k - 1$ ja $a^{k-i} = e_G$, mikä on ristiriita, sillä listassa $e, a, a^2 ... a^{k-1}$ ei ollut kahta samaa alkiota. Tästä seuraa, että k on pienin mahdollinen vakio, jolla $a^k = e_G$. Nyt pitää enää todistaa, että $k = m$, eli että $\langle a \rangle = e, a, a^2 ... a^{k-1}$. Syklisen ryhmän määritelmän perusteella $\langle a \rangle \supset \{e, a, a^2 ... a^{k-1}\}$. Todistaaksemme, että $\langle a \rangle \subset \{e, a, a^2 ... a^{k-1}\}$ oletetaan, että a^l on alkion a potenssi. Käyttämällä jakoyhtälöä [1, s.12] saadaan $l = qk + r$, missä $0 \leq r < k$. Nyt

$$a^l = a^{qk+r} = a^{qk} a^r = (a^k)^q a^r = a^r. \tag{2.22}$$

Koska $a^l = a^r \in \{e, a, a^2 ... a^{k-1}\}$, $\langle a \rangle \subset \{e, a, a^2 ... a^{k-1}\}$ ja lause on todistettu. □

Luku 3

Tekijäryhmä

Määritelmä 3.1. Olkoon $H \leq G$. Ryhmän G kuhunkin alkioon a liittyvää osajoukkoa

$$aH = \{ah \mid h \in H\} \tag{3.2}$$

sanotaan aliryhmän H *vasemmaksi sivuluokaksi* ryhmässä G. Vastaavasti määritellään oikeat sivuluokat Ha.

Lause 3.3. *Olkoon $S \leq G$. Silloin $Sa = Sb$ jos ja vain jos $ab^{-1} \in S$ ja $aS = bS$ jos ja vain jos $b^{-1}a \in S$.*

Todistus. Jos $Sa = Sb$, silloin $a = ea \in Sa = Sb$ ja siksi on olemassa $s \in S$ siten että $a = sb$. Siispä $ab^{-1} = s \in S$. Oletetaan, että $ab^{-1} = c \in S$. Silloin $a = cb$. Nyt haluamme todistaa, että $Sa = Sb$. Tämä onnistuu siten, että näytämme, että jokainen $x \in Sa$ kuuluu joukkoon Sb ja toisinpäin. Jos $x \in Sa$, silloin $x = sa$ jollakin $s \in S$ ja äskeisen perusteella $x = sbc \in Sb$. Toisaalta, jos $y \in Sb$, $y = s'b$ jollakin $s' \in S$ ja $y = s'c^{-1}a \in Sa$. Siispä $Sa = Sb$. Todistus vasempien sivuluokkien tapauksessa on samanlainen. □

Lause 3.4. *Jos $S \leq G$, niin missä tahansa kahdessa vasemmassa tai oikeassa sivuluokassa on joko samat alkiot tai ei yhtään samaa alkiota.*

Todistus. Osoitetaan, että jos on olemassa alkio $x \in Sa \cap Sb$, niin $Sa = Sb$. Jos tällainen x on olemassa, sen täytyy olla muotoa $sb = x = ta$, missä $s, t \in S$. Siispä $ab^{-1} = t^{-1}s \in S$ ja lauseen 3.3 perusteella $Sa = Sb$. □

Lause 3.5. *Jos $S \leq G$, niin aliryhmän S vasempien sivuluokkien määrä ryhmässä G on sama, kuin sen oikeiden sivuluokkien määrä ryhmässä G.*

Todistus. Merkitään oikeiden sivuluokkien joukkoa R ja vasempien sivuluokkien joukkoa L. Nyt pitäisi osoittaa, että näiden kahden joukon välillä on bijektio.

Kuvaus $f : L \to R, f(aH) = Ha^{-1}$ toteuttaa tämän ehdon. Se on hyvin määritelty, sillä lauseen 3.3 mukaan jos $aH = bH$, niin $b^{-1}a \in H$. Kun $b^{-1}a \in H$, myöskin $ab^{-1} \in H$, sillä H on ryhmä. Koska näin on, lauseen 3.3 mukaan $Ha^{-1} = Hb^{-1}$. Kuvaus on bijektio, koska käänteisalkiot ovat yksikäsitteisiä. Kun a käy läpi ryhmän G, myös a^{-1} käy läpi ryhmän G. □

Määritelmä 3.6. Ryhmän G sivuluokkien määrää aliryhmän S suhteen merkitään $[G : S]$. Koska vasempia ja oikeita sivuluokkia on lauseen 3.5 mukaan yhtä monta, voidaan niiden määrää merkitä yhdellä merkintätavalla.

Lauseen 3.4 perusteella mikä tahansa ryhmä G voidaan jakaa erillisiin osiin sen aliryhmän S sivuluokkien avulla. Jos $[G : S] = n$, voidaan valita sellaiset $g_1, g_2, g_3...g_n \in G$, joille pätee:

$$G = Sg_1 \cup Sg_2 \cup g_3... \cup Sg_n. \tag{3.7}$$

Lause 3.8. *Jos G on äärellinen ryhmä ja $S \leq G$, niin luku $|S|$ jakaa luvun $|G|$ ja $[G : S]$=$|G|/|S|$.*

Todistus. Äskeisen perusteella ryhmä G voidaan jakaa seuraavasti osiin valitsemalla sopivat $g_1, g_2, g_3...g_n \in G$, joille pätee

$$G = Sg_1 \cup Sg_2 \cup g_3... \cup Sg_n. \tag{3.9}$$

Siispä $|G| = \sum |Sg_i|$. Koska $f_i : S \to Sg_i, f_i(s) = sg_i$ on bijektio, $|Sg_i| = |S|$ jokaisella i. Siispä $|G| = n|S|$, missä $n = [G : S]$. □

Lause 3.10. *Jos G on äärellinen ryhmä ja $a \in G$, niin alkion a kertaluku jakaa luvun $|G|$.*

Todistus. Alkion a kertaluku on määritelmän 2.19 perusteella $|\langle a \rangle|$ ja se jakaa luvun $|G|$ lauseen 3.8 perusteella. □

Lause 3.11. *Jos p on alkuluku, G ryhmä ja $|G| = p$, niin G on syklinen ryhmä.*

Todistus. Olkoon $a \in G$ ja $a \neq e$. Silloin syklisessä aliryhmässä $\langle a \rangle$ on enemmän kuin yksi alkio, sillä se sisältää ainakin alkiot e ja a. Nyt lauseen 3.10 mukaan alkion a kertaluku jakaa luvun p. Koska p on alkuluku, $|\langle a \rangle| = p = |G|$ ja $\langle a \rangle = G$. □

Määritelmä 3.12. Ryhmän G aliryhmää N sanotaan *normaaliksi*, jos sen vasemmat ja oikeat sivuluokat yhtyvät. Toisin sanoen jokaiselle $a \in G$ pätee

$$aN = Na. \tag{3.13}$$

Normaalia aliryhmää merkitään $N \trianglelefteq G$.

Lause 3.14. *Olkoon $G \geq N$. Silloin $N \trianglelefteq G$ jos ja vain jos*

$$ana^{-1} \in N \quad \forall a \in G, n \in N. \tag{3.15}$$

Todistus. Oletetaan, että $N \trianglelefteq G$. Koska $Na = aN$, kun $a \in G$, jokaiselle $n \in N$ löytyy $n_1 \in N$ siten että $an = n_1 a$. Tästä seuraa, että $ana^{-1} = n_1 \in N$. Sitten käsitellään toinen suunta. Olkoon $a \in G$. Nyt on osoitettava, että $aN = Na$. Olkoon $n \in N$. Merkitään $ana^{-1} = n_1$. Oletuksen mukaan $n_1 \in N$. Saadaan siis, että $an = n_1 a \in Na$. Täten $aN \subset Na$. Sovelletaan nyt oletusta alkioihin a^{-1} ja n. Silloin saadaan, että $a^{-1}na = n_2 \in N$, siis $na = an_2 \in aN$. Tämä osoittaa, että $Na \supset aN$. □

Määritelmä 3.16. Jos $N \trianglelefteq G$, niin aliryhmän N sivuluokkien joukkoa ryhmässä G merkitään G/N. Toisin sanoen

$$G/N = \{aN \mid a \in G\}. \tag{3.17}$$

Äskeisellä idealla voidaan toteuttaa myös monimutkaisempiakin joukkoja. Oletetaan, että G on joukko ja N ja H sen aliryhmiä. Joukkoa, joka sisältää aliryhmien N ja H alkioiden välisten laskutoimitusten tulot merkitään seuravasti:

$$NH. \tag{3.18}$$

Toisin sanoen

$$NH = \{nh \mid n \in N, h \in H\}. \tag{3.19}$$

Kyseisiä merkintöjä voi usein sieventää, sillä esimerkiksi joukko NN on tässä tapauksessa sama kuin joukko N, sillä N on ryhmä ja laskutoimitus ryhmän sisällä on suljettu.

Lause 3.20. *Oletetaan, että $N \trianglelefteq G$. Joukko G/N on ryhmä seuraavasti määritellyn laskutoimituksen suhteen:*

$$aN \cdot bN = abN. \tag{3.21}$$

Todistus. Todistetaan ensin, että laskutoimitus on hyvin määritelty. Oletetaan, että $aN = a'N$ ja $bN = b'N$. Silloin $a \in a'N$ ja $b \in b'N$, joten

$$a = a'n_1, b = b'n_2, (n_1, n_2 \in N). \tag{3.22}$$

Nyt $ab = a = a'n_1 b'n_2$. Koska aliryhmä N on normaali, niin $Nb' = b'N$ ja alkio $n_1 b'$ voidaan kirjoittaa muotoon $b'n_3$, missä $n_3 \in N$. Tuloksena on

$$ab = a'b'n_3 n_2 \in a'b'N. \tag{3.23}$$

Tämä osoittaa, että $abN = a'b'N$, toisin sanoen $aNbN = a'Nb'N$. Liitäntälain voimassaolo seuraa ryhmän G liitäntälaista. Neutraalialkiona on N ja alkion aN käänteisalkiona on $a^{-1}N$. □

Määritelmä 3.24. Ryhmää $(G/N, \cdot)$ sanotaan *tekijäryhmäksi* ryhmän N suhteen.

Määritelmä 3.25. Olkoon G ryhmä ja $G \geq N$. Kuvausta $f : G \to G/N, f(a) = Na$ kutsutaan *luonnolliseksi kuvaukseksi*.

Luku 4

Permutaatiot

Määritelmä 4.1. Kutsumme n-alkioisen joukon $E = \{a_1, a_2, a_3..., a_n\}$ eri alkioista muodostettua n-jonoa

$$(a_{i_1}, a_{i_2}, a_{i_3}...a_{i_n}) \tag{4.2}$$

joukon E *permutaatioksi.*

Lause 4.3. *n-alkioisella joukolla on $n!$ permutaatiota.*

Todistus. Merkitsemme n-permutaatioiden määrää p_n. Jakamalla $(n+1)$-permutaation muodostamisen 1. koordinaatin valintaan ja sen jälkeen n:n alkion järjestämiseen jonoon näemme, että

$$p_{n+1} = (n+1)p_n. \tag{4.4}$$

Koska $p_1 = 1$, päättelemme induktiivisesti, että $p_n = n!$ kaikilla $n \in \mathbb{N}$.[3, s.23] □

Edellä esitetty tapa käsitellä permutaatioita on perinteinen, mutta tässä työssä otamme käyttöön hieman toisenlaisen tavan ymmärtää permutaatio.

Määritelmä 4.5. Joukon $J_n = \{j_1, j_2, j_3...j_n\}$ permutaatioksi sanotaan bijektiivistä kuvausta $\alpha : J_n \to J_n$.

Esimerkki 4.6. Edellä mainitut kaksi eri määritelmää permutaatiolle saattavat vaikuttaa ensin kovin erilaisilta. Asian ymmärtämiseksi tarkastellaan joukkoa $A = \{a, b, c\}$. Joukossa on kolme alkiota, joten sillä on $3! = 6$ eri permutaatiota. Ne ovat $(a, b, c), (a, c, b)$, $(b, a, c), (b, c, a), (c, a, b)$ ja (c, b, a). Kun tarkastellaan toista määritelmää, huomataan, että bijektioita $A \to A$ on tasan yhtä monta kuin on järjestettyjä jonoja. Järjestettyjä jonoja

vastaavat bijektiot ovat $f_1 : a \mapsto a, b \mapsto b, c \mapsto c$, $f_2 : a \mapsto a, b \mapsto c, c \mapsto b$, $f_3 : a \mapsto b, b \mapsto a, c \mapsto c$, $f_4 : a \mapsto b, b \mapsto c, c \mapsto a$, $f_5 : a \mapsto c, b \mapsto a, c \mapsto b$, $f_6 : a \mapsto c, b \mapsto b, c \mapsto a$.

Ei ole sattumaa, että bijektioita ja järjestettyjä jonoja on yhtä monta. Jokainen järjestetty jono vastaa bijektiota, sillä jokaisella alkiolla on vastineensa alkuperäisessä joukossa, eikä järjestetyssä jonossa esiinny mitään alkiota kahta kertaa.

Määritelmä 4.7. Jokainen bijektio $\alpha : X \to X$ voidaan esittää kahden rivin avulla seuraavasti:

$$\alpha = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ \alpha x_1 & \alpha x_2 & \dots & \alpha x_n \end{pmatrix}$$

Ensimmäisellä rivillä ovat joukon X alkiot ja toisella rivillä on niiden kuvat, jotka ovat samat joukon X alkiot eri järjestyksessä.

Esimerkki 4.8. Kahden rivin representaation etuna on se, että nyt permutaatioita on helpompi yhdistää. Kahden permutaation yhdiste on permutaatio, sillä ne ovat molemmat bijektioita. Esimerkiksi jos

$$\alpha = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$$

ja

$$\beta = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix},$$

niin

$$\alpha\beta = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}.$$

Permutaatioiden yhdistäminen tapahtuu sillä tavalla, että ensin suoritetaan β ja sitten suoritetaan α. Alkiot a, b ja c kuvautuvat siis seuraavasti:

$$\alpha\beta(a) = \alpha(\beta(a)) = \alpha(a) = c, \tag{4.9}$$

$$\alpha\beta(b) = \alpha(\beta(b)) = \alpha(a) = a, \tag{4.10}$$

$$\alpha\beta(c) = \alpha(\beta(c)) = \alpha(a) = b. \tag{4.11}$$

Luku 5

r-sykli

Määritelmä 5.1. Jos $x \in X$ ja $\alpha \in S_X$, niin α *pitää paikallaan* alkion x, jos $\alpha(x) = x$ ja *siirtää* alkion x, jos $\alpha(x) \neq x$.

Määritelmä 5.2. Olkoon $i_1, i_2, i_3 ... i_r$ tiettyjä alkioita välillä $1-n$. Jos α pitää paikallaan loput vakiot $n-r$ ja jos

$$\alpha(i_1) = i_2, \alpha(i_2) = i_3, \cdots, \alpha(i_{r-1}) = i_r, \alpha(i_r) = i_1, \tag{5.3}$$

niin α on *r-sykli*. r-sykliä kutsutaan monesti myös r:n pituiseksi sykliksi. Yhden alkion pituinen sykli vastaa identiteettikuvausta.

Määritelmä 5.4. Kahden alkion pituista sykliä kutsutaan *transpositioksi*. Se siis vaihtaa kahden alkion paikkaa ja pitää paikallaan loput alkiot.

Esimerkki 5.5. r-syklejä voidaan kuvata merkintöjen selventämiseksi seuraavasti:

$$\alpha = \begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix} = (abcd)$$

$$\beta = \begin{pmatrix} a & b & c & d & e \\ b & c & d & e & a \end{pmatrix} = (abcde)$$

$$\delta = \begin{pmatrix} a & b & c & d & e \\ b & c & a & d & e \end{pmatrix} = (abc)(d)(e) = (abc).$$

Esimerkki 5.6. Äskeisen syklinotaation avulla voidaan käsitellä permutaatioiden yhdistämistä. Jos $\alpha = (ab)$ ja $\beta = (acdbe)$, niin $\alpha\beta(a) = \alpha \circ \beta(a) = \alpha(\beta(a)) = \alpha(c) = c$. Seuraavaksi $\alpha\beta(c) = \alpha \circ \beta(c) = \alpha(\beta(c)) = \alpha(d) = d$. Nyt $\alpha\beta(d) = \alpha(\beta(d)) = \alpha(b) = a$.

Nyt olemme palanneet alkioon a, joten testataan, mitä tapahtuu alkiolla b. Tällä alkiolla $\alpha\beta(b) = \alpha(\beta(b)) = \alpha(e) = e$. Jatketaan samaa rataa ja testataan alkio e. $\alpha\beta(e) = \alpha(\beta(e)) = \alpha(a) = b$. Olemme jälleen palanneet siihen alkioon, josta aloitettiin, joten sykli on valmis. Lopputulokseksi saatiin siis:

$$(ab)(acdbe) = (acd)(be). \tag{5.7}$$

Määritelmä 5.8. Kaksi permutaatiota $\alpha, \beta \in S_X$ ovat *erilliset*, jos toinen permutaatio siirtää jokaisen toisen permutaation paikallaan pitämän alkion. Toisin sanoen, jos $\alpha(x) \neq x$, niin $\beta(x) = x$. Toisaalta myös jos $\beta(x) \neq x$, niin $\alpha(x) = x$. Tietysti on mahdollista, että on olemassa $z \in X$ siten, että $\alpha(z) = z = \beta(z)$.

Esimerkki 5.9. Muunnetaan permutaatio

$$\alpha = \begin{pmatrix} a & b & c & d & e & f & g & h & i \\ f & d & a & b & e & c & h & i & g \end{pmatrix}$$

erillisten syklien yhdisteeksi. Aloitetaan taas alkiosta a. Nyt $\alpha(a) = f$ ja edelleen $\alpha(f) = c$. Koska $\alpha(c) = a$, olemme saaneet ensimmäisen syklin selville. Seuraava sykli aloitetaan alkiosta b. Lasketaan $\alpha(b) = d$ ja $\alpha(d) = b$. Toinen sykli on siis (bd). Alkio e kuvautuu itselleen, joten se muodostaa oman syklinsä (e). Sitten tarkastetaan mitä tapahtuu alkiolle g. Nyt $\alpha(g) = h$, $\alpha(h) = i$ ja $\alpha(i) = g$. Kokonaisuudeksi siis saadaan

$$\alpha = (afc)(bd)(e)(ghi) \tag{5.10}$$

Lause 5.11. *Kun $|X| = n$, niin jokainen permutaatio $\alpha \in S_X$ on joko sykli tai yhdistelmä erillisistä sykleistä.*

Todistus. Tehdään todistus induktiolla permutaation α siirtämien alkioiden määrän k suhteen. Lause on selvästi tosi, kun $k = 0$, sillä identiteettikuvaus on 1-sykli. Jos $k > 0$, niin olkoon i_1 alkio, jonka α siirtää. Määritellään $i_2 = \alpha(i_1), i_3 = \alpha(i_2) \cdots, i_{r+1} = \alpha(i_r)$. Vakio r on tässä pienin sellainen vakio, jolla $i_{r+1} \in \{i_1, i_2, i_3 \cdots, i_r\}$. Lista $\{i_1, i_2, i_3 \cdots, i_r\}$ ei voi jatkua loputtomiin, sillä on vain n kappaletta eri vaihtoehtoja. Väitämme, että $\alpha(i_r) = i_1$. Muulloin $\alpha(i_r) = i_j$ jollakin $j \geq 2$. Toisaalta $\alpha(i_{j-1}) = i_j$, mikä on ristiriita, sillä α on injektio. Olkoon β r-sykli $(i_1, i_2 \cdots, i_r)$. Jos $r = n$, niin sykli α on sama kuin sykli β. Jos $r < n$ ja Y koostuu lopuista $n - r$ kappaleesta alkioita, niin $\alpha(Y) = Y$ ja β pitää paikallaan joukon Y pisteet. Nyt

$$\beta(\{i_1, i_2, i_3 \cdots, i_r\}) = \alpha(\{i_1, i_2, i_3 \cdots, i_r\}). \tag{5.12}$$

Jos α' on permutaatio, jolla $\alpha'(Y) = \alpha(Y)$ ja joka pitää paikallaan alkiot $\{i_1, i_2, i_3 \cdots, i_r\}$, niin β ja α' ovat erilliset ja

$$\alpha = \beta\alpha'. \tag{5.13}$$

Koska α' siirtää vähemmän pisteitä kuin α, induktiohypoteesi osoittaa, että α' ja siksi myös α ovat erillisten syklien yhdisteitä.

□

Lause 5.14. *Kaksi erillistä sykliä permutoivat. Toisin sanoen, jos α ja β ovat erilliset, niin*

$$\alpha\beta = \beta\alpha. \tag{5.15}$$

Todistus. Olkoon a alkio, jonka α siirtää ja β pitää paikallaan. Nyt $\alpha(\beta(a)) = \alpha(a) = \beta(\alpha(a))$. Tämä siksi, että α on sykli ja a kuvautuu joksikin muuksi syklin jäseneksi. Kuvaus β ei siirrä näitä alkioita, joten yhtälö pätee. Päinvastainen tilanne, jossa α pitää paikallaan ja β siirtää alkion a todistetaan samalla tavalla. □

Määritelmä 5.16. Permutaation α *täydellinen jako* on permutaation α sellainen representaatio erillisten syklien avulla, joka sisältää yhden 1-syklin (i) jokaista permutaation α paikallaan pitämää alkiota i kohden.

Lause 5.17. *Jokainen permutaatio $\alpha \in S_X$ on yhdiste transpositioista.*

Todistus. Lauseen 5.11 mukaan jokainen permutaatio on joko sykli tai yhdiste erillisistä sykleistä. Siispä

$$(abc\cdots r) = (1r)(1r-1)\cdots(12). \tag{5.18}$$

□

Lause 5.19. *Kaikki joukon J_n permutaatiot muodostavat ryhmän kuvaustulon suhteen, jota kutsutaan n:n alkion symmetriseksi ryhmäksi.*

Todistus.

$$S_n = \{\alpha : J_n \to J_n \mid \alpha \quad on \quad bijektio.\} \tag{5.20}$$

Joukossa on voimassa laskutoimitus, sillä jokainen α on bijektio, siispä niiden yhdisteetkin ovat bijektioita. Liitäntälaki pätee, sillä ei ole merkitystä missä järjestyksessä permutaatioita suoritetaan, kunhan niiden paikkaa ei vaihdeta. Ykkösalkiona on joukon J_n identiteettikuvaus ja permutaation α käänteisalkiona käänteiskuvaus α^{-1}. □

Vastaisuudessa positiivisten kokonaislukujen muodostaman joukon $N_n = \{1, 2, 3...n\}$ permutaatioiden ryhmästä käytetään merkintää S_n, missä n kertoo kokonaislukujen joukon N_n alkioiden lukumäärän. Yleisen joukon G permutaatioiden ryhmästä käytetään merkintää S_G.

Lause 5.21. *Olkoon $\alpha \in S_X$ ja olkoon $\alpha = \beta_1\beta_2\cdots\beta_n$ kuvauksen α täydellinen jako erillisiin sykleihin. Tämä jako on yksikäsitteinen lukuunottamatta syklien järjestystä.*

Todistus. Todistus on pitkä ja se sivuutetaan. [2, s.7] □

Lause 5.22. *Olkoot $k, l > 0$. Silloin pätee*

$$(a \quad b)(a \quad c_1\cdots c_k \quad b \quad d_1\cdots d_k) = (a \quad c_1\cdots c_k)(b \quad d_1\cdots d_k) \tag{5.23}$$

ja

$$(a \quad b)(a \quad c_1\cdots c_k)(b \quad d_1\cdots d_k) = (a \quad c_1\cdots c_k \quad b \quad d_1\cdots d_k). \tag{5.24}$$

Todistus. Ensimmäisen yhtälön vasen puoli kuvaa alkioita seuraavasti: $a \mapsto c_1 \mapsto c_1; c_i \mapsto c_{i+1} \mapsto c_{i+1}$. Jos $i < k$, niin $c_k \mapsto b \mapsto a$. Edelleen $b \mapsto d_1 \mapsto d_1; d_j \mapsto d_{j+1} \mapsto d_{j+1}$. Kun $j < k$, kuvaus etenee näin: $d_l \mapsto a \mapsto b$. Samankaltainen tutkimus ensimmäisen yhtälön toiselle puolelle osoittaa yhtälön oikeaksi. Alempi yhtälö on vain ylempi yhtälö kerrottuna vasemmalta puolelta puolittain syklillä $(a \quad b)$. □

Määritelmä 5.25. Olkoon $\alpha \in S_n$ ja $\alpha = \beta_1\cdots\beta_t$ on täydellinen jako erillisiin sykleihin. Kuvauksen α *merkki* on tällöin

$$sgn(\alpha) = (-1)^{n-t}. \tag{5.26}$$

Lause 5.27. *Olkoon $\beta \in S_n$ ja τ transpositio. Silloin*

$$sgn(\tau\beta) = -sgn(\beta). \tag{5.28}$$

Todistus. Olkoon $\tau = (a \quad b)$ ja olkoon $\beta = \gamma_1\cdots\gamma_t$ kuvauksen β täydellinen jako erillisiin sykleihin. Jos a ja b esiintyvät samassa syklissä, vaikkapa syklissä γ_1, niin $\gamma_1 = (a \quad c_1\cdots c_k \quad b \quad d_1\cdots d_k)$. Syklin indeksillä ei ole väliä, koska erilliset syklit kommutoivat. Lauseen 5.22 mukaan

$$\tau\gamma_1 = (a \quad c_1\cdots c_k)(b \quad d_1\cdots d_k). \tag{5.29}$$

Tästä seuraa, että $\tau\beta = (\tau\gamma_1)\gamma_2\cdots\gamma_t$ on täydellinen jako, jossa on yksi sykli enemmän kuin täydellisessä jaossa $\beta = \gamma_1\cdots\gamma_t$. Siispä

$$sgn(\tau\beta) = (-1)^{n-(t+1)} = -sgn(\beta). \tag{5.30}$$

Toinen mahdollisuus on se, että a ja b ovat eri sykleissä. Merkitään näitä syklejä $\gamma_1 = (a \quad c_1\cdots c_k)$ ja $\gamma_2 = (b \quad d_1\cdots d_k)$. Oletuksena on, että $k, l \geq 0$. Nyt $\tau\beta = (\tau\gamma_1\gamma_2)\gamma_3\cdots\gamma_t$ ja lauseen 5.22 mukaan

$$\tau\gamma_1\gamma_2 = (a \quad c_1\cdots c_k \quad b \quad d_1\cdots d_k). \tag{5.31}$$

Siispä kuvauksen $\tau\beta$ täydellisessä jaossa on yksi sykli vähemmän, kuin kuvauksen β täydellisessä jaossa. Siksi

$$sgn(\tau\beta) = (-1)^{n-(t-1)} = -sgn(\beta). \tag{5.32}$$

□

Luku 6

Kuvauksista

Määritelmä 6.1. Olkoot $(G, *)$ ja $(H, \diamond)$ ryhmiä. Kuvausta $f : G \to H$ sanotaan *homomorfismiksi*, jos se toteuttaa homomorfiaehdon

$$f(a * b) = f(a) \diamond f(b) \tag{6.2}$$

kaikilla $a \in G$ ja $h \in H$.

Esimerkki 6.3. Esimerkiksi funktio $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$ on homomorfismi, sillä $\mathbb{R}$ on kertolaskun suhteen ryhmä ja

$$f(xy) = x^2y^2 = f(x)f(y). \tag{6.4}$$

Määritelmä 6.5. Olkoot G ja H ryhmiä ja f kuvaus $G \to H$. Kuvauksen f *kuvan* muodostavat ryhmän H alkiot b, joille pätee $f(a) = b | a \in G$. Toisin sanoen

$$Im(f) = \{f(a) \mid a \in G\}. \tag{6.6}$$

Esimerkki 6.7. Olkoon f kuvaus $\mathbb{R} \to \mathbb{R}$ siten, että $x \mapsto \frac{1}{x}$. Nyt kuvauksen f kuva on $\{\mathbb{R} \setminus 0\}$.

Määritelmä 6.8. Olkoot G ja H ryhmiä ja f kuvaus $G \to H$. Kuvauksen f *ytimen* muodostavat ryhmän G alkiot a, joille pätee $f(a) = e_H$. Homomorfismin ydintä merkitään $Ker(f)$.

Esimerkki 6.9. Olkoon f kuvaus $\mathbb{R} \to \mathbb{R}$ siten, että $x \mapsto x^2$. Laskutoimituksena on reaalilukujen kertolasku. Nyt kuvauksen f ytimen muodostavat alkiot -1 ja 1, sillä ne ovat ainoat alkiot, jotka kuvautuvat neutraalialkioksi 1.

Määritelmä 6.10. Homomorfismia $f : G \to H$ sanotaan *isomorfismiksi*, jos f on bijektiivinen. Ryhmää G sanotaan isomorfiseksi ryhmän H kanssa, jos on olemassa joku isomorfismi $f : G \to H$. Isomorfisia ryhmiä merkitään $G \simeq H$. Jos homomorfismi $f : G \to H$ on injektio, niin kuvaus $f : G \to Im(f)$ on bijektiivinen homomorfismi eli isomorfismi.

Lause 6.11. *Homomorfismi $f : G \to H$ säilyttää neutraalialkion ja käänteisalkiot.*

Todistus. Osoitetaan ensin neutraalialkion säilyvyys. Kerrotaan yhtälö $f(e_G)f(e_G) = f(e_G e_G)$ puolittain alkiolla $f(e_G)^{-1}$. Tästä saadaan $f(e_G) = e_H$. Käänteisalkioiden säilyvyys osoitetaan seuraavasti: $f(a)f(a^{-1}) = f(aa^{-1}) = f(e_G) = e_H = f(a)f(a)^{-1}$. □

Lause 6.12. *Homomorfismi $f : G \to H$ on injektio jos ja vain jos $Ker(f) = e_G$.*

Todistus. Olkoon f injektio. Koska $f(e_G) = e_H$, on tällöin $Ker(f) = e_G$. Nyt pitää todistaa vielä toinen suunta. Olkoot $x, y \in G$ ja $f(x) = f(y)$. Silloin

$$e_H = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy)^{-1}, \tag{6.13}$$

joten $xy^{-1} \in Ker(f)$. Oletuksesta $Ker(f) = e_G$ seuraa nyt $x = y$. Täten f on injektio. □

Lause 6.14. *Luonnollinen kuvaus $f : G \to G/N, f(a) = Na$ on homomorfismi.*

Todistus. Oletetaan, että $a, b \in G$. Nyt

$$f(a)f(b) = aNbN = abN = f(ab). \tag{6.15}$$

□

Lause 6.16. *Oletetaan, että G on ryhmä ja $G \trianglerighteq H$. Luonnollisen kuvauksen $f : G \to G/H, f(a) = aH$ ydin on H.*

Todistus. Neutraalialkio $e_{G/H}$ on H, kuten lauseen 3.20 todistuksessa todetaan. Nyt $aH = H$ ainoastaan silloin, kun $a \in H$ ryhmän laskutoimituksen määritelmän perusteella. Siispä ainoastaan joukkoon H kuuluvat alkiot kuvautuvat alkioksi $e_{G/H}$ ja muodostavat luonnollisen kuvauksen ytimen. □

Lause 6.17. *Jos $f : G \to H$ on homomorfismi, niin $Ker(f)$ on ryhmän G normaali aliryhmä.*

Todistus. Jos $a \in Ker(f)$, niin $f(a) = e_H$. Siispä kun $g \in G$, $f(gag^{-1}) = f(g)f(a)f(g)^{-1} = f(g)f(g)^{-1} = e_H$. Tämä osoittaa, että $Ker(f)$ on ryhmän G normaali aliryhmä.

□

Lause 6.18. *Olkoon $f : G \to H$ homomorfismi, jonka ydin on K. Silloin K on ryhmän G normaali aliryhmä ja $G/K \simeq Im(f)$.*

Todistus. K on lauseen 6.17 perusteella ryhmän G normaali aliryhmä. Määritellään

$$\phi : G/K \to H, \phi(Ka) = f(a). \tag{6.19}$$

Oletetaan, että $Ka = Kb$, toisin sanoen $Kab^{-1} = K$, eli $ab^{-1} \in K$. Tästä seuraa, että $e_H = f(ab^{-1}) = f(a)f(b^{-1})$, sillä f on homomorfismi. Siispä $f(b) = f(a)$. Nyt $\phi(Ka) = \phi(Kb)$, joten ϕ on hyvin määritelty. ϕ on homomorfismi, koska

$$\phi(KaKb) = \phi(Kab) = f(ab) = f(a)f(b) = \phi(Ka)\phi(Kb). \tag{6.20}$$

Kuvauksen ϕ määritelmän perusteella $Im\phi = Imf$. Lopuksi osoitetaan vielä, että ϕ on injektio. Jos $\phi(Ka) = \phi(Kb)$, niin $f(a) = f(b)$. Siispä $f(a)f(b)^{-1} = e_H$ ja $f(ab^{-1}) = e_H$. Nyt $ab^{-1} \in K$ ja $Ka = Kb$. Koska ϕ on homomorfismi ja injektio, se on isomorfismi. □

Lause 6.21. *Olkoot N ja T ryhmän G aliryhmiä, joista N on normaali. Silloin $N \cap T$ on normaali aliryhmä aliryhmän T suhteen ja $T/(N \cap T) \simeq NT/N$.*

Todistus. Olkoon $v : G \to G/N$ luonnollinen kuvaus ja olkoon $v' = v \mid T$ kuvauksen v rajoittuma joukossa T. Koska v' on homomorfismi, jonka ydin on $N \cap T$, lauseen 6.18 mukaan $(N \cap T) \lhd T$ ja $(T/N) \cap T \simeq Im(v')$. Joukko $Im(v')$ on niiden aliryhmän N sivuluokkien joukko, joissa on alkio, joka kuuluu aliryhmään T. Toisin sanoen puhutaan joukosta NT/N. Tämä osoittaa, että $T/N \cap T \simeq NT/N$. □

Lause 6.22. *Olkoon $K \leq H \leq G$, missä K ja H ovat normaaleja ryhmän G aliryhmiä. Silloin H/K on ryhmän G/K normaali aliryhmä ja*

$$(G/K)/(H/K) \simeq G/H. \tag{6.23}$$

Todistus. Olkoon $f : G/K \to G/H, f(Ka) = Ha$. f on hyvin määritelty, sillä $H \simeq K$. f on myös surjektio, sillä kun a käy läpi koko ryhmän G, käydään läpi myös jokainen sivuluokka, joka kuuluu joukkoon G/H. kuvauksen f ydin on H/K, sillä vain sellaiset sivuluokat aK kuvautuvat neutraalialkioksi H, joissa $a \in H$. Nyt lause tosi lauseen 6.18 mukaan. □

Luku 7

p-ryhmä

Määritelmä 7.1. Jos X on joukko, kutsumme *ekvivalenssirelaatioksi* sellaista $X \times X$:n osajoukkoa R, jolle pätee kaikilla $x, y, z \in X$:
(1) $(x, x) \in R$
(2) $(x, y) \in R \Rightarrow (y, x) \in R$
(3) $(x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R$

Esimerkki 7.2. Tarkastellaan kaikkien tason suorien joukkoa ja relaatiota "suora l_1 on yhdensuuntainen suoran l_2 kanssa". Tämä relaatio on ekvivalenssirelaatio, sillä selvästi jokainen suora on yhdensuuntainen itsensä kanssa. Samanlaiselta itsestäänselvyydeltä tuntuu kohta (2). Kohta kolme on myös tosi, sillä jos l_1 on yhdensuuntainen suoran l_2 kanssa, joka on yhdensuuntainen suoran l_3 kanssa, ovat myös l_1 ja l_3 yhdensuuntaiset.

Määritelmä 7.3. Jos G on ryhmä ja $x \in G$, niin alkiota axa^{-1}, missä $a \in G$, kutsutaan alkion x *konjugaatiksi*. Toisin sanoen y on alkion x konjugaatti, jos on olemassa $a \in G$ siten että $y = axa^{-1}$.

Lause 7.4. *Jos G on ryhmä, relaatio "y on alkion x konjugaatti" muodostaa ekvivalenssirelaation ryhmässä G.*

Todistus. Käydään kohta kohdalta läpi ekvivalenssirelaation määritelmä.
(1) Jokainen $x \in G$ on itsensä konjugaatti, sillä $e_G x e_G = x$.
(2) Jos y on alkion x konjugaatti, niin $y = axa^{-1}$ jollain $a \in G$. Nyt $ya = ax$, mistä seuraa $a^{-1}ya = x$, joten x on alkion y konjugaatti.
(3) Jos y on alkion x konjugaatti ja x on alkion z konjugaatti, niin y on alkion z konjugaatti. Tämä siksi, että $y = axa^{-1} = abzb^{-1}a^{-1} = (ab)z(ab)^{-1} = czc^{-1}$, joillakin $a, b, c \in G$. □

Määritelmä 7.5. Jos G on ryhmä ja $a \in G$, niin alkion a ekvivalenssiluokkaa, jonka relaatio "y on alkion x konjugaatti" muodostaa, kutsutaan alkion a *konjugaattiluokaksi*. Sitä merkitään a^G.

Määritelmä 7.6. Ryhmän G *keskukseksi* kutsutaan niiden alkioiden $a \in G$ joukkoa, joille kaikilla $g \in G$ pätee

$$ag = ga. \tag{7.7}$$

Ryhmän G keskusta merkitään $Z(G)$.

Lause 7.8. *Jos G on ryhmä, niin $Z(G)$ on ryhmän G normaali Abelin aliryhmä.*

Todistus. Käydään ensin läpi, miksi $Z(G)$ on ryhmä. Laskutoimitus on suljettu joukossa, sillä jos $a, b \in Z(G)$ ja $g \in G$, niin $abg = agb = gab$. Liitännäisyys seuraa ryhmän G ominaisuuksista. Alkion $a \in Z(G)$ käänteisalkio on a^{-1}. Tämä alkio kuuluu joukkoon $Z(G)$, sillä jos $g \in G$ ja $ag = ga$, niin $aga^{-1} = g$ ja $ga^{-1} = a^{-1}g$. Neutraalialkio on e_G. Ryhmä on Abelin ryhmä, sillä keskuksen määritelmän mukaan kaikille alkioille $a, b \in Z(G)$ pätee $ab = ba$. Ryhmä $Z(G)$ on normaali, sillä jos $a \in Z(G)$ ja $g \in G$, niin $gag^{-1} = gg^{-1}a = a$. □

Määritelmä 7.9. Jos G on ryhmä ja $a \in G$, alkion a *keskittäjäksi* kutsutaan niiden alkioiden $x \in G$ joukkoa, joille pätee

$$ax = xa. \tag{7.10}$$

Keskittäjää merkitään $C_G(a)$.

Lause 7.11. *Jos G on ryhmä ja $a \in G$, niin $C_G(a)$ on ryhmän G aliryhmä.*

Todistus. Laskutoimitus on suljettu joukossa $C_G(a)$, sillä jos $x, y \in C_G(a)$, niin $xya = xay = axy$. Liitännäisyys periytyy ryhmän G ominaisuuksista. Alkion x käänteisalkio on x^{-1}, sillä jos $ax = xa$, niin $x^{-1}ax = a$ ja $x^{-1}a = ax^{-1}$. Neutraalialkio periytyy ryhmästä G. □

Lause 7.12. *Jos $a \in G$, niin alkion a konjugaattien määrä on sama kuin sen keskittäjän sivuluokkien määrä ryhmässä G. Toisin sanoen*

$$|a^G| = [G : C_G(a)]. \tag{7.13}$$

Tämä saatu luku on luvun $|G|$ tekijä, kun G on äärellinen.

Todistus. Merkitään ryhmän $C = C_G(a)$ kaikkien vasempien sivuluokkien joukkoa ryhmässä G symbolilla G/C. Määritellään funktio $f : a^G \to G/C, f(gag^{-1}) = gC$. Tarkoituksena olisi nyt osoittaa, että f on bijektio. Kuvaus f on hyvin määritelty, sillä jos $gag^{-1} = hah^{-1}$ jollakin $h \in G$, niin $h^{-1}gag^{-1}h = a$ ja h^{-1} on vaihdannainen alkion a kanssa. Näin ollen $h^{-1}g \in C$ ja $hC = gC$. Funktio f on injektio, sillä jos $gC = f(gag^{-1}) = f(kak^{-1}) = kC$ jollakin $k \in G$, niin $k^{-1}g \in C$. Nyt $k^{-1}g$ on vaihdannainen alkion a kanssa ja $k^{-1}gag^{-1}k$. Tästä seuraa, että $gag^{-1} = kak^{-1}$. Funktio f on surjektio, koska jos $g \in G$, niin $gC = f(gag^{-1})$. Näin ollen funktio f on bijektio ja $|a^G| = |G/C| = [G : C_G(a)]$. Kun G on äärellinen, voidaan käyttää lausetta 3.8. □

Määritelmä 7.14. Jos p on alkuluku, *p-ryhmä* on ryhmä, jonka jokaisen alkion kertaluku on luvun p jokin potenssi.

Esimerkki 7.15. Tarkastellaan viiden alkion syklistä ryhmää $G5 = \{e_{G5}, g_1, g_1^2, g_1^3, g_1^4\}$. Nyt ryhmän jokainen sen neutraalialkiosta poikkeava alkio virittää saman aliryhmän $G5$. Näin ollen jokaisen alkion kertaluku on 5 poislukien alkio e_{G5}, jonka kertaluku on 1. Nämä ovat molemmat luvun 5 potensseja, joten $G5$ on p-ryhmä.

Lause 7.16. *Jos alkiolla $a \in G$ on äärellinen kertaluku ja $f : G \to H$ on homomorfismi, niin alkion a kertaluku on alkion $f(a)$ monikerta.*

Todistus. Olkoon alkion a kertaluku k. Nyt $f(e_G) = f(a^k) = f(a)^k = e_H$. Tämä siksi, että homomorfismi säilyttää lauseen 6.11 mukaan neutraalialkiot. Nyt luvun k täytyy olla alkion $f(a)$ kertaluvun monikerta. □

Lause 7.17. *Jos G on äärellinen Abelin ryhmä, jonka kertaluku on jaollinen alkuluvulla p, ryhmä G sisältää alkion, jonka kertaluku on p.*

Todistus. Merkitään $|G| = pm$, missä $m \geq 1$. Käytetään induktiota lauseen todistamiseksi. Kun $m = 1$, lause pätee lauseen 3.8 perusteella. Otetaan induktioaskel, ja oletetaan, että lause on tosi arvolla $m - 1$. Olkoon $x \in G$ alkio, jonka kertaluku on $t > 1$. Jos $p|t$, niin $e_G = x^t = x^{ps} = (x^p)^s$, missä $s \in \mathbb{R}$. Tämä tarkoittaa sitä, että alkion x kertaluku on p. Voimme siis olettaa, että p ei jaa lukua t. Koska G on Abelin ryhmä, $\langle x \rangle$ on sen normaali aliryhmä. Kaikilla $g \in G$ näet pätee

$$gxg^{-1} = gg^{-1}x = x. \tag{7.18}$$

Samasta syystä $G/\langle x \rangle$ on Abelin ryhmä. Sen alkioiden lukumäärä on lauseen 3.8 mukaan $|G|/t = pm/t$. Koska t ei jaa lukua p, täytyy olla vakio $m/t < m$. Induktio-oletuksen mukaan tässä ryhmässä on alkio y^*, jonka kertaluku on p. Luonnollinen kuvaus $v : G \to G/\langle x \rangle$ on surjektio, joten on olemassa $y \in G$, jolla $v(y) = y^*$. Lauseen 7.16 mukaan alkion y kertaluku on luvun p monikerta, joten lause on todistettu. □

Lause 7.19. *Äärellinen Abelin ryhmä G on p-ryhmä jos ja vain jos $|G|$ on alkuluvun p potenssi.*

Todistus. Jos $|G| = p^m$, niin lauseen 3.10 mukaan G on p-ryhmä. Toisen suunnan implikaation todistamiseksi oletetaan, että on olemassa alkuluku $q \neq p$, joka jakaa luvun $|G|$. Äskeisen lauseen perusteella G sisältää nyt alkion, jonka kertaluku on q, mikä on ristiriidassa sen kanssa, että G on p-ryhmä. □

Luku 8

Suora tulo

Määritelmä 8.1. Olkoot H ja K ovat ryhmiä. Näiden ryhmien *suora tulo* on ryhmä, jonka alkiot ovat järjestettyjä pareja (h, k), missä $h \in H$ ja $k \in K$. Suoraa tuloa merkitään $H \times K$. Laskutoimituksena ryhmässä on

$$(h, k)(h', k') = (hh', kk'). \tag{8.2}$$

Ryhmän neutraalialkio on (e_H, e_K) ja alkion (h, k) käänteisalkio on (h^{-1}, k^{-1}). Liitäntälaki on voimassa, sillä H ja K ovat ryhmiä.

Esimerkki 8.3. Tarkastellaan ryhmien $(\mathbb{R}, +)$ ja p-ryhmän $G5$ suoraa tuloa. Suoran tulon alkioita ovat järjestetyt parit (a, g), missä $a \in \mathbb{R}$ ja $g \in G5$. Ryhmän neutraalialkio on alkio $(0, e_{G5})$. Alkion (a, g) käänteisalkio on alkio $(-a, g^{-1})$.

Lause 8.4. *Olkoon G ryhmä ja H ja K sen normaaleja aliryhmiä. Jos $HK = G$ ja $H \cap K = e_G$, niin $G \simeq H \times K$.*

Todistus. Jos $a \in G$, niin $a = hk$ jollain $h \in H$ ja $k \in K$. Tämä siksi, että $G = HK$. Väitämme, että a määrittää alkiot h ja k yksikäsitteisesti. Jos $a = h_1k_1$, missä $h_1 \in H$ ja $k_1 \in K$, niin $hk = h_1k_1$. Tästä seuraa, että $h^{-1}h_1 = kk_1^{-1} \in H \cap K = e_G$. Siispä $h = h_1$ ja $k = k_1$. Olkoon $f : G \to H \times K, f(a) = (h, k)$, missä $a = hk$. Osoitetaan, että f on homomorfismi. Kun $a = hk \in G$ ja $a' = h'k' \in G$, niin $aa' = hkh'k'$. Tämä ei kuitenkaan ole homomorfismitarkastelun kanntalta sopiva muoto. Olisi mukavaa, jos pätisi $kh' = h'k$. Silloin voisimme helposti huomata kuvauksen f olevan homomorfismi. Tarkastellaan siis alkiota $h'kh'^{-1}k^{-1}$. Nyt $(h'kh'^{-1})k^{-1} \in K$, sillä $h'kh'^{-1} \in K$, koska K on normaali aliryhmä. Samoin $h'(kh'^{-1}k^{-1}) \in H$, koska H on normaali. Siispä $h'kh'^{-1}k^{-1} \in K \cap H = e_G$. Tästä seuraa, että $h'k = kh'$.

Nyt voidaan osoittaa, että f on homomorfismi. Kun a ja a' ovat kuten edellä,

$$f(aa') = f(khk'h') = f(kk'hh') = (kk', hh') = f(a)f(a'). \tag{8.5}$$

f on lauseen 6.12 mukaan injektio, koska $ker(f) = e_G$. Nyt on todistettu että f on homomorfismi sekä injektio, eli määritelmän 6.10 mukaan isomorfismi.

□

Lause 8.6. *Jos $A \lhd H$ ja $B \lhd K$, niin $A \times B \lhd H \times K$ ja*

$$(H \times K)/(A \times B) \simeq (H/A) \times (K/B). \tag{8.7}$$

Todistus. Homomorfismi $\phi : H \times K \to (H/A) \times (K/B), \phi(h,k) = (Ah, Bk)$, on surjektio ja $ker(\phi) = A \times B$. Lauseen 6.18 perusteella ϕ on isomorfismi. □

Luku 9

Caleyn lause

Määritelmä 9.1. Olkoon G ryhmä. Jokaiselle $g \in G$ voidaan määritellä *vasen translaatiokuvaus*:

$$L_g : G \to G, L_g(x) = gx. \tag{9.2}$$

Vasen translaatiokuvaus on bijektio ryhmän laskutoimituksen määritelmän perusteella.

Caleyn lause 9.3. Jokainen ryhmä G voidaan upottaa ryhmän S_G aliryhmäksi. Erityisesti, jos $|G| = n$, ryhmä G voidaan upottaa ryhmän S_n aliryhmäksi.

Todistus. Jokainen vasen translaatiokuvaus $L_g : G \to G, L_g(x) = gx$, on bijektio, joten $L_g \in S_G$. Pyrimme todistamaan, että funktio $L : G \to S_G, g \mapsto L_g$, on injektio sekä homomorfismi, sillä silloin $G \cong im(L)$. Jos $a \neq b$, niin $L_a(e) = a \neq b = L_b(e)$. Siispä $L_a \neq L_b$. Lopuksi todistetaan vielä, että $L_{ab} = L_a \circ L_b$. Jos $x \in G$, niin $L_{ab}(x) = (ab)x$. Toisaalta $(L_a \circ L_b)(x) = L_a(L_b(x)) = L_a(bx) = a(bx)$. Nämä ovat liitäntälain mukaan samat alkiot. □

Lause 9.4. *Jos $G \geq H$ ja $[G : H] = n$, niin on olemassa homomorfismi $p : G \to S_n$, jonka ytimelle pätee*

$$Ker(p) \leq H. \tag{9.5}$$

Todistus. Olkoon $a \in G$ ja X on aliryhmän H vasempien sivuluokkien joukko ryhmässä G. Määritellään funktio $p_a : X \to X, gH \mapsto agH$ jokaisella $g \in G$. Jokainen kuvaus p_a on bijektio, sillä X on ryhmä. Siispä jokainen p_a on joukon X permutaatio. Kuvaus $p : G \to S_X \simeq S_n, a \mapsto p_a$ on homomorfismi, sillä jos $a, b \in G$, niin

$$p(ab) = p_{ab} : X \to X, gH \mapsto abgH = p_a \circ p_b. \tag{9.6}$$

Jos $a \in Ker(p)$, niin $agH = gH$ kaikilla $g \in G$. Erityisesti $aH = H$, joten $a \in H$. Siispä $Ker(p) \leq H$. $\square$

Kirjallisuutta

[1] Tauno Metsänkylä ja Marjatta Näätänen: Algebra, 2. painos, Yliopistopaino, 2009.

[2] Joseph J. Rotman: An Introduction to the Theory of Groups, 4.painos, 1999.

[3] Pekka Tuominen: Todennäköisyyslaskenta I, 5. painos, Limes ry, 2000.