TAMPEREEN YLIOPISTO
Pro gradu -tutkielma

Anssi Koliini

SYT- ja PYM-matriisien unitaarisista vastineista

Matematiikan ja tilastotieteen laitos
Matematiikka
Maaliskuu 2009

Tampereen yliopisto

Matematiikan ja tilastotieteen laitos

KOLIINI, ANSSI: SYT- ja PYM-matriisien unitaarisista vastineista

Pro gradu -tutkielma, 64 s.

Matematiikka

Maaliskuu 2009

Tiivistelmä

Olkoon $A = \{x_1, x_2, \ldots, x_n\}$ pienimmästä suurimpaan alkioon järjestetty joukko positiivisia kokonaislukuja ja olkoon f aritmeettinen funktio. Joukon A ja aritmeettisen funktion f määräämällä SYT-matriisilla tarkoitetaan matriisia, jonka i. rivin j. alkio on funktion f arvo alkoiden x_i ja x_j suurimman yhteisen tekijän kohdalla. Vastaavasti määritellään joukon A ja funktion f määräämä PYM-matriisi pienimmän yhteisen monikerran avulla. Koska positiivisten kokonaislukujen joukko muodostaa hilan yhdessä jaollisuuden kanssa, niin esitetyt SYT- ja PYM-matriisien määritelmät ovat mielekkäitä, sillä suurin yhteinen tekijä ja pienin yhteinen monikerta ovat aina yksikäsitteisinä olemassa.

Positiivisen kokonaisluvun n unitaaritekijällä d tarkoitetaan luvun n sellaista tekijää, että $(d, n/d) = 1$. Kokonaislukujen joukko yhdessä unitaaritekijärelaation kanssa ei kuitenkaan muodosta hilaa, toisin kuin tavanomaisen jaollisuuden tapauksessa, sillä suurinta yhteistä unitaarimonikertaa ei välttämättä ole olemassa. Näin ollen yritys muodostaa PYM-matriisille unitaarinen vastine suoraan pienimmän yhteisen unitaarimonikerran avulla on tuomittu epäonnistumaan. SYT-matriisin unitaarinen vastine sen sijaan voidaan määritellä korvaamalla suurin yhteinen tekijä suurimmalla yhteisellä unitaaritekijällä.

Pentti Haukkanen, Pauliina Ilmonen, Ayse Nalli ja Juha Sillanpää esittelevät artikkelissa *On unitary analogs of GCD reciprocal LCM matrices* kolme erilaista menetelmää kokonaislukujen joukon sekä unitaaritekijärelaation laajentamiseen sellaiseksi, että laajennettu joukko yhdessä laajennetun unitaaritekijärelaation kanssa muodostaa hilan. Tällöin kutakin laajennusta hyödyntäen pystytään muodostamaan SYT- ja PYM-matriiseille tietynlaisia unitaarisia vastineita. Artikkelissa määritetään myös kaavat tiettyjen aritmeettisten funktioiden luokkien määräämien SYT- ja PYM-matriisien unitaaristen vastineiden Hadamardin osamäärän determinantille sekä osoitetaan, että konstruoidut laajennukset eroavat merkittävästi toisistaan tiettyjen ominaisuuksien suhteen. Tässä tutkielmassa perehdytään tämän artikkelin lauseiden todistuksiin, laajennusten konstruktioihin sekä tutustutaan suurimpaan osaan artikkelin ymmärtämiseen tarvittavista esitiedoista.

Sisältö

1 Johdanto

Olkoon $S = \{x_1, x_2, \ldots, x_n\}$ erisuurista positiivisista kokonaisluvuista koostuva joukko, joka on järjestetty siten, että $x_1 < x_2 < \cdots < x_n$. Tällöin sanotaan, että joukko S on *SYT-suljettu*, mikäli $(x_i, x_j) \in S$ jokaisella $i, j = 1, 2, \ldots, n$. Olkoon f aritmeettinen funktio. Määritellään matriisi $(\boldsymbol{S})_f$ asettamalla $[(\boldsymbol{S})_f]_{ij} = f(x_i, x_j)$. Tätä matriisia kutsutaan joukon S ja aritmeettisen funktion f määräämäksi SYT-matriisiksi. PYM-matriisi $[\boldsymbol{S}]_f$ määritellään korvaamalla edellisessä määritelmässä suurin yhteinen tekijä pienimmällä yhteisellä monikerralla.

H.J.S. Smith esitti 1800-luvulla monia merkittäviä lukuteoreettisia tuloksia liittyen muun muassa tiettyjen aritmeettisten funktioiden määräämien SYT- ja PYM-matriisien determinantteihin. Yhtenä Smithin tuloksista tunnetaan vuonna 1876 julkaistu *Smithin determinantiksi* kutsuttu kaava SYT-suljetun joukon $S = \{1, 2, \ldots, n\}$ ja identtisen funktion määräämän SYT-matriisin determinantille. Kyseisen kaavan mukaan

$$\det((\boldsymbol{S})_{Id}) = \varphi(1)\varphi(2)\cdots\varphi(n).$$

Erilaisia SYT- ja PYM-matriiseja koskevia tuloksia on Smithin esittämien tulosten innoittamana julkaistu runsaasti.

R. Vaidyanathaswamy tutki vuonna 1931 julkaisemassaan artikkelissa *The theory of multiplicative arithmetic functions* multiplikatiivisten aritmeettisten funktioiden ominaisuuksia. Tässä artikkelissa mainitaan tiettävästi ensimmäistä kertaa unitaaritekijän käsite. Unitaaritekijöiksi kutsutaan niitä luvun n tekijöitä d, joilla $(d, n/d) = 1$. Korvaamalla tavanomainen jaollisuus unitaarisella jaollisuudella voidaan määritellä suurimman yhteisen tekijän ja pienimmän yhteisen monikerran unitaariset vastineet, joita soveltamalla voidaan määritellä myös unitaariset vastineet SYT- ja PYM-matriiseille. Näitä matriiseja kutsutaan jatkossa lyhyesti SYUT- ja PYUM-matriiseiksi. Mainittuja määritelmiä ei kuitenkaan voida aina soveltaa täysin suoraviivaisesti johtuen pääosin siitä, että mielivaltaisilla positiivisilla kokonaisluvuilla n ja m ei välttämättä ole lainkaan pienintä yhteistä unitaarimonikertaa.

Pentti Haukkanen, Pauliina Ilmonen, Ayse Nalli ja Juha Sillanpää tarkastelevat artikkelissa *On unitary analogs of GCD reciprocal LCM matrices* tiettyjen aritmeettisten funktioiden määräämien SYUT- ja PYUM-matriisien Hadamardin osamäärän determinanttia, sekä esittävät erilaisia vaihtoehtoja tavanomaisesti määritellyn suurimman yhteisen unitaaritekijän puuttumisesta johtuvien ongelmien ratkaisemiseksi. Tässä tutkielmassa perehdytään tähän artikkeliin esittämällä muun muassa lauseiden todistusten yksityiskohdat sekä syventämällä artikkelissa esitettyjä pohjatietoja.

Lähteenä käytettävän artikkelin sisältö on tähän saakka hyvin vähän tutkittua. Aihealueista on kirjallisuudessa tutkittu laajalti ainoastaan luvussa 4.1 esiteltävää pienintä yhteistä pseudo-unitaarista monikertaa. Lu-

vussa 4.2 käsiteltävän hilateoreettisen tavan suurimman yhteisen unitaarimonikerran käsitteen laajentamiseksi esitteli Ismo Korkee artikkelissa *A note on meet and join matrices and special cases GCUD and LCUM matrices* vuonna 2005. Kyseinen artikkeli sisältyy Korkeen vuonna 2006 julkaistuun väitöskirjaan. Viimeisimpänä luvussa 4.3 käsiteltävä p^∞-unitaarinen PYUM esitellään tämän tutkielman lähdeartikkelissa [9] ensimmäistä kertaa kirjallisuudessa.

Artikkelin todistusten kannalta keskeisimmät asiat pyritään esittelemään tutkielman luvussa 3, mutta tietyt perusasiat oletetaan lukijan tuntemiksi. Tutkielman ymmärtämiseen vaaditaan ennen kaikkea hyvät lukuteorian tiedot, sillä suurin osa unitaaritekijöitä koskevista todistuksista edellyttää tavanomaisen jaollisuuden ominaisuuksien sujuvaa osaamista. Myös erilaisia todistustekniikoita, kuten induktio- ja vastaoletusperiaatetta, on kyettävä seuraamaan. Luvun 5 tarkasteluissa lukijalta edellytetään hyvää lineaarialgebran ja etenkin matriisilaskennan hallintaa. PYUM-laajennusten konstruoinnissa sovelletaan hilateoriaa sekä jokseenkin syvällistäkin topologiaa, joten tarvittaessa myös näiden alojen alkeet on kerrattava ennen tähän tutkielmaan perehtymistä. Mikäli lukija omaa vankat pohjatiedot mainituilta matematiikan aloilta, voi tutkielmasta sivuuttaa esitiedot unitaaritekijöiden ominaisuuksia sekä unitaarikonvoluutiota lukuun ottamatta ja siirtyä mainittujen lukujen jälkeen suoraan luvussa 4 konstruoitaviin laajennuksiin.

2 Merkinnöistä

Tutkielmassa pyritään käyttämään mahdollisimman paljon yleisessä käytössä olevia merkintöjä. Tässä luvussa esitellään lyhyesti suurin osa käytetyistä merkinnöistä. Tämä on tarpeen etenkin unitaaritekijöiden osalta, sillä monet unitaaritekijöitä koskevista merkinnöistä eivät ole vielä kovinkaan vakiintuneita. Aivan kaikkia käytettyjä merkintöjä ei ole mielekästä käydä läpi tässä luvussa, vaan harvemmin esiintyvät merkinnät esitellään määritelmien yhteydessä.

Unitaarisesta jaollisuusrelaatiosta käytetään tässä tutkielmassa merkintää $\|$. Mainittakoon, että esimerkiksi lähteessä [6] käytetään tästä poiketen merkintää $|^*$. Lukujen m ja n suurinta yhteistä unitaaritekijää merkitään symbolilla $(m, n)_{\oplus\oplus}$. Tavallisesta pienimmästä yhteisestä unitaarimonikerrasta käytetään merkintää $[m, n]^*$. Pienimmän yhteisen unitaarimonikerran laajennuksia koskevat merkinnät esitellään laajennuksia koskevissa luvuissa. Dirichlet'n konvoluutiota merkitään symbolilla $*$ ja unitaarikonvoluutiosta käytetään merkintää $\oplus$. Tavanomaista jaollisuutta merkitään symbolilla $|$, lukujen m ja n suurinta yhteistä tekijää symbolilla (m, n) ja pienintä yhteistä monikertaa symbolilla $[m, n]$.

Positiivisten kokonaislukujen joukkoa merkitään symbolilla $\mathbb{Z}_+$. Alkulukujen joukosta käytetään merkintää $\mathbb{P}$ ja kompleksilukujen joukosta mer-

kintää $\mathbb{C}$. Muita joukkoja merkitään isoilla kirjaimilla $A, B, C, \ldots$

Kokonaisluvuille käytetään pieniä kirjaimia $a, b, c, \ldots$ sekä tarvittaessa alaindekseja $a_i, b_i, c_i, \ldots$, missä i on positiivinen kokonaisluku. Alkulukuja merkitään yleensä kirjaimella p tai käyttämällä alaindeksejä $p_1, p_2, p_3, \ldots$ Luvun n kanonisesta alkutekijäesityksestä käytetään enimmäkseen merkintää $\prod_{p\in\mathbb{P}} p^{n(p)}$. Mikäli alkulukutekijöiden lukumäärä on asiayhteydessä keskeinen, niin käytetään kuitenkin merkintää $\prod_{p=1}^{r} = p_i^{n(p_i)}$, missä $n(p_i) > 0$ jokaisella $i = 1, 2, \ldots, r$.

Matriiseista käytetään pääsääntöisesti merkintöjä $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}, \ldots$ Tietyistä matriiseista käytetään tästä käytännöstä poikkeavia erikoismerkintöjä, jotka esitellään erikseen kunkin matriisin määrittelyn yhteydessä. Matriisin minoreita koskevat merkinnät esitellään luvussa 3.5. Matriisin $\boldsymbol{A}$ determinantista käytetään merkintää $\det(\boldsymbol{A})$ tai $|\boldsymbol{A}|$. Diagonaalimatriisia eli matriisia jonka kaikki nollasta eroavat alkiot sijaitsevat matriisin diagonaalilla merkitään $\operatorname{diag}(x_1, x_2, \ldots, x_n)$, missä alkiot $x_1, x_2, \ldots, x_n$ ovat mainitut diagonaalin alkiot.

Joukkojen topologioita ja joukkoperheitä merkitään yleensä kaunokirjaimin $\mathcal{S}, \mathcal{T}, \mathcal{U}, \ldots$ Joukon X potenssijoukkoa merkitään $\mathcal{P}(X)$. Topologisten avaruuksien pisteitä merkitään pienin kirjaimin $a, b, c \ldots$ Sekaannuksen vaaraa kokonaislukujen kanssa ei juurikaan tule, sillä tutkielmassa avaruuksien pisteet ovat yleensä juuri kokonaislukuja. Avaruuksien Y_i tulotopologiasta käytetään merkintää $\prod_{i\in I} Y_i$. Samaa merkintää käytetään myös hilatulosta. Se, kumpaa merkintää kulloinkin tarkoitetaan, käy tapauskohtaisesti ilmi asiayhteydestä.

3 Esitietoja

3.1 Hilateoriaa

Tutkielmassa tarkasteltavista pienimmän yhteisen unitaarimonikerran laajennuksista luvuissa 4.2 ja 4.3 esiteltävät määritelmät voidaan ymmärtää helposti hilateorian avulla. Tässä luvussa esitellään näiden lukujen hilateoreettisten tarkastelujen ymmärtämisen kannalta keskeisimmät käsitteet. Luvun asiasisältö seuraa pääosin Mika Erosen kirjoittamaa monistetta *Hilateoriaa*.

Määritelmä 3.1. (Ks. [3], s. 1) Olkoon P epätyhjä joukko ja $\leq$ joukossa P määritelty relaatio. Tällöin relaatio $\leq$ on *osittainen järjestys* ja struktuuri $\langle P, \leq \rangle$ on *osittain järjestetty joukko*, jos

(1) $x \leq x$,

(2) $x \leq y$ ja $y \leq x \Rightarrow x = y$,

(3) $x \leq y$ ja $y \leq z \Rightarrow x \leq z$

jokaisella $x, y, z \in P$.

Huomautus Osittaisen järjestyksen ehdoista (1),(2) ja (3) käytetään usein relaation ominaisuuksiin viittaavia nimiä refleksiivisyys, antisymmetrisyys ja transitiivisuus.

Määritelmä 3.2. (Ks. [3], s. 3) Olkoon $\langle P, \leq \rangle$ osittain järjestetty joukko ja olkoon $S \subseteq P$. Alkio $m \in S$ on joukon S

(1) *pienin alkio*, jos jokaisella $x \in S$ pätee, että $m \leq x$,

(2) *suurin alkio*, jos jokaisella $x \in S$ pätee, että $m \geq x$.

Määritelmä 3.3. (Ks. [3], s. 4) Olkoon $\langle P, \leq \rangle$ osittain järjestetty joukko ja olkoon $S \subseteq P$. Alkio $b \in P$ on joukon S

(1) *alaraja*, jos jokaisella $x \in S$ pätee, että $b \leq x$,

(2) *yläraja*, jos jokaisella $x \in S$ pätee, että $b \geq x$.

Määritelmä 3.4. (Ks. [3], s. 4) Olkoon $\langle P, \leq \rangle$ osittain järjestetty joukko ja olkoon $S \subseteq P$. Joukon S *pienin yläraja* eli *supremum* on joukon S ylärajojen joukon pienin alkio. Vastaavasti joukon S *suurin alaraja* eli *infimum* on joukon S alarajojen joukon suurin alkio. Joukon S pienimmästä ylärajasta käytetään merkintää $\sup S$ ja suurimmasta alarajasta vastaavasti merkintää $\inf S$.

Huomautus Alkiot $\inf S$ ja $\sup S$ eivät välttämättä aina ole olemassa mielivaltaisessa osittain järjestetyssä joukossa. Esimerkiksi supremumin tapauksessa ylärajojen joukko saattaa olla joko tyhjä tai se voi sisältää keskenään vertailuttomia alkioita, jolloin pienintä ylärajaa on mahdoton määrittää.

Määritelmä 3.5. (Ks. [3], s. 11) Olkoon $\langle L, \leq \rangle$ osittain järjestetty joukko. Tällöin struktuuri $\langle L, \leq \rangle$ on *hila*, jos $\sup\{x, y\}$ ja $\inf\{x, y\}$ ovat olemassa kaikilla $x, y \in L$.

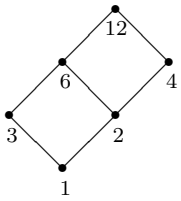
Määritelmä 3.6. (Ks. [3], s. 12) Olkoon $\langle L, \leq \rangle$ osittain järjestetty joukko. Tällöin $\langle L, \leq \rangle$ on *join-puolihila*, jos $\sup\{x, y\}$ on olemassa kaikilla $x, y \in L$.

Määritelmä 3.7. (Ks. [3], s. 12) Olkoon $\langle L, \leq \rangle$ osittain järjestetty joukko. Tällöin $\langle L, \leq \rangle$ on *meet-puolihila*, jos $\inf\{x, y\}$ on olemassa kaikilla $x, y \in L$.

Huomautus Struktuuri $\langle L, \leq \rangle$ on hila, jos ja vain jos se on sekä meet- että join-puolihila.

Esimerkki 3.1. Struktuuri $\langle T_{12}, | \rangle$ on hila, missä relaatiolla $|$ tarkoitetaan tavanomaista jaollisuutta ja joukolla T_{12} luvun 12 tekijöiden joukkoa. Tämän todistamiseksi riittää havaita, että relaatio $|$ on osittainen järjestys joukossa T_{12} ja että suurin yhteinen tekijä ja pienin yhteinen monikerta vastaavat kyseisen hilan alkioparien infimumia ja supremumia. Graafisesti tämä hila voidaan esittää Hasse-diagrammin (ks. [3] s. 2) avulla.

Kuva 1: Hila $\langle T_{12}, | \rangle$



Hilat voidaan määritellä yhtäpitävästi myös struktuureina $\langle P, \vee, \wedge \rangle$, missä binääriset laskutoimitukset $\vee$ ja $\wedge$ toteuttavat tietyt ehdot. Tämä algebrallinen määritelmä ei ole tämän tutkielman kannalta välttämätön ymmärtää täydellisesti, joten määritelmien yhtäpitävyyden todistava lause tyydytään esittämään ilman todistusta. Jatkossa supremumista käytetään selkeyden vuoksi merkintää $\vee$ ja infimumista merkintää $\wedge$, sillä hilaoperaatioiden $\vee$ ja $\wedge$ ominaisuuksista seuraa, että $x \vee y = \sup\{x, y\}$ ja vastaavasti $x \wedge y = \inf\{x, y\}$. Relaation $\leq$ ja laskutoimitusten $\wedge$ ja $\vee$ välinen yhteys selkenee seuraavan yksinkertaisen lauseen perusteella. Varsinainen struktuurien välinen ekvivalenssi esitetään lauseessa 3.2.

Lause 3.1. *(Ks. [3], s. 13) Olkoon $\langle P, \leq \rangle$ osittain järjestetty joukko ja olkoot $x, y \in P$. Tällöin seuraavat ehdot ovat yhtäpitäviä*

(1) $x \leq y$,

(2) $x \vee y = y$,

(3) $x \wedge y = x$.

Todistus. Todistetaan, että kohdat (1) ja (2) ovat ekvivalentit. Kohtien (1) ja (3) välinen yhtäpitävyys voidaan todistaa vastaavasti.

Jos $x \leq y$, niin y on joukon $\{x, y\}$ yläraja. Jos nyt z on myös joukon $\{x, y\}$ yläraja, niin on oltava $y \leq z$. Siis y on pienin joukon $\{x, y\}$ yläraja eli $x \vee y = y$. Jos $x \vee y = y$, niin y on pienin joukon $\{x, y\}$ yläraja. Tällöin siis $x \leq y$. □

Lause 3.2. *Rakenne $\langle L, \vee, \wedge \rangle$ on hila, jos joukko L on epätyhjä ja binääriset laskutoimitukset $\vee$ ja $\wedge$ toteuttavat seuraavat ehdot*

(1) $x \vee x = x$ *ja* $x \wedge x = x$,

(2) $x \vee y = y \vee x$ *ja* $x \wedge y = y \wedge x$,

(3) $x \vee (y \vee z) = (x \vee y) \vee z$ *ja* $x \wedge (y \wedge z) = (x \wedge y) \wedge z$,

(4) $x \vee (y \wedge z) = x$ *ja* $x \wedge (y \vee z) = x$

aina, kun $x, y, z \in L$.

Todistus. (Ks. [3], s. 13-15) □

Määritellään seuraavaksi hilojen suora tulo, jota hyödynnetään myöhemmin luvun 4.3 konstruktioissa. Määritelmä esitetään yleisemmässä muodossa kuin lähteessä. Joukkoperheen $\{L_i : i \in I\}$ karteesinen tulo $\prod_{i\in I} L_i$ oletetaan tunnetuksi. Mainittakoon kuitenkin, että kyseisen tulon alkiot voidaan mieltää äärellisinä tai äärettöminä lukujonoina riippuen joukon I mahtavuudesta. Yleisen karteesisen tulon määritelmän voi kerrata esimerkiksi lähteen [10] sivulta 25.

Määritelmä 3.8. (Vrt. [3], s. 20) Olkoon I indeksijoukko ja olkoot struktuurit $\langle L_i, \leq\rangle$ hiloja jokaisella $i \in I$. Määritellään relaatio $\leq$ joukossa $\prod_{i\in I} L_i$ siten, että

$$(a_i)_{i\in I} \leq (b_i)_{i\in I},$$

jos

$$a_i \leq b_i \text{ kaikilla } i \in I.$$

Tällöin struktuuria $\langle \prod_{i\in I} L_i, \leq\rangle$ sanotaan hilojen $\langle L_i, \leq\rangle, i \in I$, *suoraksi tuloksi*.

On helppo havaita, että hilojen suora tulo on hila. Lisäksi lauseen 3.1 perusteella havaitaan, että tällöin pätee $(a_i)_{i\in I} \vee (b_i)_{i\in I} = (a_i \vee b_i)_{i\in I}$ ja $(a_i)_{i\in I} \wedge (b_i)_{i\in I} = (a_i \wedge b_i)_{i\in I}$. (Ks. [3], s.13)

3.2 Unitaaritekijät

Tässä luvussa ryhdytään tarkastelemaan unitaaritekijöitä. Unitaaritekijöitä ei oleteta aiemmin tunnetuiksi vaan tarkastelut aloitetaan unitaaritekijöiden perusominaisuuksista. Luvussa esitetään myös muutamia yksinkertaisia esimerkkejä sekä todistetaan myöhemmissä luvuissa keskeisiä unitaaritekijöiden ominaisuuksia koskevia lauseita. Keskeisimpiä luvussa käytettyjä lähteitä ovat tutkielman päälähteenä käytetyn artikkelin lisäksi Rodney Hansenin ja Leonard Swansonin yhteistyössä kirjoittama *Unitary divisors* [6].

Määritelmä 3.9. (Ks. [6], s. 217) Luonnollisen luvun n tekijää d sanotaan luvun n *unitaaritekijäksi*, jos $(d, n/d) = 1$. Tällöin merkitään $d \parallel n$. Tällöin voidaan sanoa myös, että n on luvun d *unitaarimonikerta*.

Huomautus Jokaisella luvulla on olemassa triviaalit unitaaritekijät 1 ja luku itse. On helppo havaita myös, että luku on alkuluku tai alkuluvun potenssi, jos ja vain jos sen ainoat unitaaritekijät ovat triviaalit unitaaritekijät (ks. [6], s. 218).

Esimerkki 3.2. Luvun $36 = 2^2 3^2$ tekijät ovat $1, 2, 3, 4, 6, 9, 12, 18$ ja 36. Näistä unitaaritekijöitä ovat luvut $1, 4, 9$ ja 36. Esimerkiksi luku 6 ei ole unitaaritekijä, sillä $(6, 36/6) = (6, 6) = 6$. Huomaa, että unitaaritekijät nähdään helposti kanonisesta alkutekijäesityksestä.

Lause 3.3. *(Ks. [6], s. 218) Luonnollisen luvun* $n = \prod_{p\in\mathbb{P}} p^{n(p)}$ *unitaaritekijät ovat muotoa*

$$\prod_{p\in\mathbb{P}} p^{i_p},$$

missä $i_p = n(p)$ *tai* $i_p = 0$ *jokaisella* $p \in \mathbb{P}$.

Todistus. Olkoon $d = \prod_{p\in\mathbb{P}} p^{d(p)}$ luvun $n = \prod_{p\in\mathbb{P}} p^{n(p)}$ unitaaritekijä. Koska $d \mid n$, niin $d(p) \leq n(p)$ jokaisella $p \in \mathbb{P}$. Tehdään vastaoletus, että on olemassa sellainen $p' \in \mathbb{P}$, että $0 < d(p') < n(p')$. Nyt $p' \mid (n/d)$ ja $p' \mid d$, joten $1 < p' \mid (d, n/d)$. Seuraa ristiriita, sillä nyt luku d ei ole luvun n unitaaritekijä. Näin ollen vastaoletus on väärä, joten $d(p) = 0$ tai $d(p) = n(p)$ jokaisella alkuluvulla p.

Olkoon $d = \prod_{p\in\mathbb{P}} p^{i_p}$, missä $i_p = n(p)$ tai $i_p = 0$ kullakin p. Nyt $d \mid n$, sillä $i_p \leq n(p)$ jokaisella alkuluvulla p. Lisäksi tällöin $n/d = \prod_{p\in\mathbb{P}} p^{n(p)-i_p}$, joten jos $p \mid d$, niin $p \nmid n/d$. Näin ollen $(d, n/d) = 1$, joten d on luvun n unitaaritekijä. □

Huomautus (Ks. [6], s. 219) Edellisen lauseen perusteella voidaan nähdä, että luvun $n \in \mathbb{Z}_+$ unitaaritekijöiden lukumäärä on $2^{\omega(n)}$, missä $\omega(n)$ on luvun n alkulukutekijöiden lukumäärä. Havaitaan myös, että jos $d \parallel n$, niin myös $n/d \parallel n$.

Lause 3.4. *Relaatio* $\parallel$ *on osittainen järjestys joukossa* $\mathbb{Z}_+$.

Todistus. Refleksiivisyys ja antisymmetrisyys seuraavat suoraan jaollisuuden ominaisuuksista (ks. [7], s. 4). Transitiivisuuden todistamiseksi joudutaan tekemään hieman enemmän työtä (ks. [6], s. 218).

Valitaan mielivaltaiset luonnolliset luvut l,m ja n. Refleksiivisyys seuraa välittömästi, sillä nyt $l \mid l$ ja $(l, l/l) = (l/1) = 1$, joten $l \parallel l$.

Oletetaan sitten, että $l \parallel m$ ja $m \parallel l$. Nyt $l \mid m$ ja $m \mid l$, joten jaollisuuden antisymmetrian perusteella $l = m$. Siis relaatio $\parallel$ on antisymmetrinen.

Transitiivisuuden todistamisessa apuna käytetään lausetta 3.3. Olkoot $\prod_{p\in\mathbb{P}} p^{l(p)}$, $\prod_{p\in\mathbb{P}} p^{m(p)}$ ja $\prod_{p\in\mathbb{P}} p^{n(p)}$ lukujen l, m ja p kanoniset alkutekijäesitykset. Oletetaan, että $l \parallel m$ ja $m \parallel n$. Koska $l \parallel m$, niin lauseen 3.3 perusteella $l(p) = m(p)$ tai $l(p) = 0$ kullakin $p \in \mathbb{P}$. Samoin perustein joko $m(p) = n(p)$ tai $m(p) = 0$ kullakin $p \in \mathbb{P}$. Nyt siis joko $l(p) = n(p)$ tai $l(p) = 0$ kullakin $p \in \mathbb{P}$, joten lauseen 3.3 mukaan $l \parallel n$. Määritelmän 3.1 mukaan relaatio $\parallel$ on osittainen järjestys joukossa $\mathbb{Z}_+$. □

Määritelmä 3.10. (Ks. [6], s. 219) Olkoot m ja n luonnollisia lukuja. Luonnollinen luku d on lukujen m ja n *suurin yhteinen unitaaritekijä eli* SYUT *(engl.* greatest common unitary divisor, GCUD*)*, jos

(1) $d \parallel m$ ja $d \parallel n$,

(2) $e \parallel m$ ja $e \parallel n \Rightarrow e \parallel d$ kaikilla $e \in \mathbb{Z}_+$.

Tällöin merkitään $d = (m, n)_{\oplus\oplus}$.

Lause 3.5. *(Ks. [9], s. 4) Olkoot m ja n luonnollisia lukuja. Nyt*

$$(m, n)_{\oplus\oplus} = \prod_{p\in\mathbb{P}} p^{\rho(m(p),n(p))},$$

missä funktio ρ saa arvon $m(p)$, jos $m(p) = n(p)$ ja 0 muulloin.

Todistus. Olkoot m ja n mielivaltaisia luonnollisia lukuja. Lauseen 3.3 perusteella $\prod_{p\in\mathbb{P}} p^{\rho(m(p),n(p))} \parallel m$ ja $\prod_{p\in\mathbb{P}} p^{\rho(m(p),n(p))} \parallel n$, sillä $\rho(m(p), n(p))$ on joko 0 tai $m(p)$.

Olkoon $d \parallel m$ ja $d \parallel n$. Nyt oletuksen $d \parallel m$ ja lauseen 3.3 perusteella $d = \prod_{p\in\mathbb{P}} p^{i_p}$, missä $i_p = m(p)$ tai $i_p = 0$ kullakin $p \in \mathbb{P}$. Toisaalta oletuksen $d \parallel n$ ja edellä hyödynnetyn lauseen perusteella $d = \prod_{p\in\mathbb{P}} p^{i_p}$, missä kullakin $p \in \mathbb{P}$ pätee $i_p = n(p)$ tai $i_p = 0$. Nyt $i_p = m(p)$ vain, jos $m(p) = n(p)$. Muilla alkuluvuilla p pätee $i_p = 0$. Tällöin jälleen lauseen 3.3 perusteella $d \parallel \prod_{p\in\mathbb{P}} p^{\rho(m(p),n(p))}$, joten $(m, n)_{\oplus\oplus} = \prod_{p\in\mathbb{P}} p^{\rho(m(p),n(p))}$. □

Lause 3.6. *(Ks. [6], s. 219) Olkoot $m, n \in \mathbb{Z}_+$. Nyt*

$$(m, n) \leq (m, n)_{\oplus\oplus}.$$

Todistus. Olkoot $m, n \in \mathbb{Z}_+$. Merkitään $m = \prod_{p\in\mathbb{P}} p^{m(p)}$ ja $n = \prod_{p\in\mathbb{P}} p^{n(p)}$. Nyt

$$(m, n) = \prod_{p\in\mathbb{P}} p^{\min\{m(p),n(p)\}} \leq \prod_{p\in\mathbb{P}} p^{\rho(m(p),n(p))} = (m, n)_{\oplus\oplus}.$$

□

Lause 3.7. *Struktuuri $\langle \mathbb{Z}_+, \parallel \rangle$ on meet-puolihila.*

Todistus. Lauseen 3.4 mukaan $\parallel$ on osittainen järjestys joukossa $\mathbb{Z}_+$ ja lauseen 3.5 mukaan $(m, n)_{\oplus\oplus}$ on määritelty kaikilla $m, n \in \mathbb{Z}_+$. Määritelmän 3.7 mukaan struktuuri $\langle \mathbb{Z}_+, \parallel \rangle$ on siis meet-puolihila. □

Määritelmä 3.11. (Ks. [6], s. 220) Olkoot n ja m luonnollisia lukuja. Luonnollinen luku d on lukujen n ja m *pienin yhteinen unitaarimonikerta*, eli *PYUM* (engl. *least common unitary multiple, LCUM*), jos

(1) $n \parallel d$ ja $m \parallel d$,

(2) $n \parallel e$ ja $m \parallel e \Rightarrow d \parallel e$ kaikilla $e \in \mathbb{Z}_+$.

Tällöin merkitään $d = [n, m]_{\oplus\oplus}$.

Lause 3.8. *Olkoot $m, n \in \mathbb{Z}_+$. Jos $(m, n) = 1$, niin*

(1) $(m, n)_{\oplus\oplus} = 1$,

(2) $[m,n]_{\oplus\oplus} = mn$.

Todistus. Lauseen 3.6 mukaan $(m,n)_{\oplus\oplus} \leq (m,n)$, joten $(m,n)_{\oplus\oplus} = 1$.

Jos $(m,n) = 1$, niin luvuilla m ja n ei ole yhteisiä alkulukutekijöitä. Tällöin $mn = \prod_{p\in\mathbb{P}} p^{\max\{n(p),m(p)\}}$. Nyt lauseen 3.3 mukaan $m \parallel mn$ ja $n \parallel mn$. Oletetaan sitten, että $m \parallel d$ ja $n \parallel d$. Nyt lauseen 3.3 perusteella jokaisella alkuluvulla p pätee, että $d(p) = m(p)$, jos $m(p) > 0$ ja $d(p) = n(p)$, jos $n(p) > 0$. Näin ollen lauseen 3.3 mukaan saadaan, että $mn \parallel d$. On siis todistettu, että $[m,n]_{\oplus\oplus} = mn$. □

Huomautus Mielivaltaisten lukujen $m, n \in \mathbb{Z}_+$ pienintä yhteistä unitaarimonikertaa ei välttämättä ole olemassa. Esimerkiksi lukujen 3 ja 9 pienin yhteinen unitaarimonikerta $[3,9]_{\oplus\oplus}$ ei ole olemassa. Tämän havaitsemiseksi riittää huomata, että kaikki luvun 9 unitaarimonikerrat ovat jaollisia luvulla 9. Näin ollen myös lukujen 3 ja 9 pienin yhteinen unitaarimonikerta on jaollinen luvulla 9. Tällöin pienimmän yhteisen unitaarimonikerran ja luvun 3 suurin yhteinen tekijä on 3, mistä seuraa välittömästi ristiriita pienimmän yhteisen unitaarimonikerran määritelmän kanssa.

Seuraava pienimmän yhteisen unitaarimonikerran olemassaoloa koskeva lause todistetaan edellisen huomautuksen motivoimana. Lausetta hyödynnetään apulauseena luvussa 4.2.

Lause 3.9. *Olkoot $m, n \in \mathbb{Z}_+$. Seuraavat ehdot ovat yhtäpitäviä.*

(1) $[m,n]_{\oplus\oplus}$ *on olemassa,*

(2) kaikilla $p \in \mathbb{P}$ joko $m(p) = 0$, $n(p) = 0$ tai $m(p) = n(p)$,

missä $\prod_{p\in\mathbb{P}} p^{m(p)}$ ja $\prod_{p\in\mathbb{P}} p^{n(p)}$ ovat lukujen m ja n alkutekijäesitykset.

Todistus. Oletetaan, että $m, n \in \mathbb{Z}_+$. Oletetaan ensin, että $[m,n]_{\oplus\oplus}$ on olemassa. Tehdään seuraavaksi vastaoletus, että on olemassa sellainen $p' \in \mathbb{P}$, että $m(p'), n(p') > 0$ ja $m(p') \neq n(p')$. Yleisyyttä rajoittamatta voidaan lisäksi olettaa, että $m(p') > n(p')$. Valitaan mielivaltainen $d \in \mathbb{Z}_+$. Jos nyt $m \parallel d$ ja $n \parallel d$, niin on oltava $d(p) \geq m(p), n(p)$ jokaisella $p \in \mathbb{P}$. Tällöin $(d, d/n) \geq p'$, joten d ei ole luvun n unitaarimonikerta, eikä siis lukujen n ja m yhteinen unitaarimonikerta. Näin ollen luvuilla n ja m ei voi olla lainkaan yhteisiä unitaarimonikertoja, ei siis myöskään pienintä yhteistä unitaarimonikertaa. Tästä seuraa ristiriita, sillä oletuksen mukaan pienin yhteinen unitaarimonikerta on olemassa.

Oletetaan seuraavaksi, että kaikilla $p \in \mathbb{P}$ joko $m(p) = 0$, $n(p) = 0$ tai $m(p) = n(p)$. Todistetaan, että tällöin $[m,n]_{\oplus\oplus} = \prod_{p\in\mathbb{P}} p^{\max\{m(p),n(p)\}}$. Merkitään $d = \prod_{p\in\mathbb{P}} p^{\max\{m(p),n(p)\}}$. Lauseen 3.3 perusteella nähdään ensinnäkin, että tällöin $m \parallel d$ ja $n \parallel d$. Olkoon $e \in \mathbb{Z}_+$ sellainen luku, että $m \parallel e$ ja $n \parallel e$. Nyt lauseen 3.3 mukaan $e(p) = \max\{m(p), n(p)\}$ jokaisella $p \in \mathbb{P}$, jolla $m(p) > 0$ tai $n(p) > 0$. Sama lause kertoo myös, että tällöin $d \parallel e$. Siis $[m,n]_{\oplus\oplus} = d$. □

Huolimatta siitä, että struktuuri $\langle \mathbb{Z}_+, \| \rangle$ on meet-puolihila, se ei siis kuitenkaan ole hila. Tämä on juuri tarkastelun alla olevan ongelman "ydin". Koska mielivaltaisten lukujen pienimmän yhteisen unitaarimonikerran olemassaolosta ei ole varmuutta, emme voi korvata SYT-matriisin määritelmässä esiintyvää jaollisuusrelaatiota unitaaritekijärelaatiolla, sillä kaikki matriisin alkiot eivät välttämättä tulisi määritellyiksi. Jotta näin voitaisiin aina menetellä, on tätä struktuuria laajennettava sellaiseksi, että kaikille alkioille on olemassa pienin yhteinen unitaarimonikerta. Luvussa 4 tähän ongelmaan tarjotaan kolme lähestymistavaltaan erilaista ratkaisua.

3.3 Aritmeettiset funktiot

Tässä luvussa tutustutaan suppeasti aritmeettisiin funktioihin ja niihin liittyviin binäärioperaatioihin. Lähteenä käytetään pääosin Pentti Haukkasen kirjoittamaa luentomonistetta *Lukuteoriaa*. Tärkeinä erityistapauksina mainitaan Möbiuksen funktion sekä Möbiuksen käänteiskaavan unitaariset vastineet, joita hyödynnetään luvun 5 matriisien tarkasteluissa.

Lukuteoreettinen eli aritmeettinen funktio on kuvaus luonnollisten lukujen joukolta kompleksilukujen joukkoon. Kaikkien aritmeettisten funktioiden joukkoa merkitään yleensä symbolilla $\mathcal{A}$. Aritmeettisten funktioiden summa $f + g$ on sellainen aritmeettinen funktio, että $(f + g)(n) = f(n) + g(n)$, kun $n \in \mathbb{Z}_+$. Aritmeettisten funktioiden f ja g tulo fg on vastaavasti sellainen aritmeettinen funktio, että $(fg)(n) = f(n)g(n)$, kun $n \in \mathbb{Z}_+$. (Ks. [8], s. 27-28)

Määritelmä 3.12. (Ks. [8], s. 28) Olkoot f ja g aritmeettisia funktioita. Funktioiden f ja g *Dirichlet'n konvoluutio* $f * g$ on sellainen aritmeettinen funktio, että

$$(f * g)(n) = \sum_{d|n} f(d)g(n/d), n \in \mathbb{Z}_+.$$

Määritelmä 3.13. (Ks. [8], s. 28) Funktio δ on sellainen aritmeettinen funktio, että $\delta(1) = 1$ ja $\delta(n) = 0$ muulloin.

Huomautus Aritmeettinen funktio δ on neutraalialkio Dirichlet'n konvoluution suhteen.

Määritelmä 3.14. (Ks. [8], s. 27) Funktio ω on sellainen aritmeettinen funktio, että $\omega(1) = 0$ ja

$$\omega(n) = \sum_{\substack{p \in \mathbb{P} \\ p|n}} 1,$$

kun $n > 1$.

Huomautus Aritmeettinen funktio ω kertoo luvun erisuurten alkulukutekijöiden määrän.

Lause 3.10. *Struktuuri* $\langle \mathcal{A}, +, * \rangle$ *on kommutatiivinen ykkösrengas, missä ykkösfunktiona toimii* δ*.*

Todistus. (Ks. [8], s. 28-29) □

Lause 3.11. *Aritmeettisella funktiolla* f *on käänteisfunktio* f_*^{-1} *Dirichlet'n konvoluution suhteen, jos* $f(1) \neq 0$*. Käänteisfunktio* f_*^{-1} *saadaan tällöin rekursiivisesti kaavasta*

$$\begin{aligned} f_*^{-1}(1) &= 1 \\ f_*^{-1}(n) &= -\frac{1}{f(1)} \sum_{\substack{d \| n \\ d>1}} f(d) f_*^{-1}\left(\frac{n}{d}\right). \end{aligned}$$

Todistus. (Ks. [8], s. 29) □

Huomautus Aritmeettisen funktion f käänteiskuvauksesta käytetään monesti merkintää f^{-1} sekä Dirichlet'n konvoluution että luvussa 3.4 esiteltävän unitaarikonvoluution suhteen. Tässä tutkielmassa käytetään konvoluutioiden käänteiskuvauksista kuitenkin hieman tavanomaisesta poikkeavia merkintöjä, sillä saman merkinnän käyttäminen kummankin konvoluution yhteydessä heikentäisi selvästi tutkielman luettavuutta. Merkinnällä f_*^{-1} tarkoitetaan tässä tutkielmassa käänteisfunktiota Dirichlet'n konvoluution suhteen ja merkinnällä $f_\oplus^{-1}$ käänteisfunktiota unitaarikonvoluution suhteen. Merkintä f^{-1} varataan tutkielmassa yksinomaan funktion f alkukuvien esittämiseen.

Huomautus Kääntyvien aritmeettisten funktioiden joukosta käytetään tavallisesti merkintää $\mathcal{A}_0$.

Lause 3.12. *Struktuuri* $\langle \mathcal{A}_0, * \rangle$ *on Abelin ryhmä, jossa ykkösalkiona toimii funktio* δ*.*

Todistus. (Ks. [8], s. 29) □

Seuraavaksi määritellään muutamia aritmeettisten funktioiden ominaisuuksia. Näitä ominaisuuksia hyödynnetään useissa tutkielman loppuosan todistuksissa, joten näiden määritelmien omaksuminen on tärkeää todistusten seuraamiseksi.

Määritelmä 3.15. (Ks. [9], s. 11) Aritmeettista funktiota f sanotaan *semimultiplikatiiviseksi*, jos $f((m,n))f([m,n]) = f(m)f(n)$ aina, kun $m, n \in \mathbb{Z}_+$.

Määritelmä 3.16. (Ks. [9], s. 14) Aritmeettista funktiota f sanotaan *kvasimultiplikatiiviseksi*, jos $f(1) \neq 0$ ja $f(1)f(mn) = f(m)f(n)$ kaikilla sellaisilla $m, n \in \mathbb{Z}_+$, joilla $(m,n) = 1$.

Lause 3.13. *Olkoon f sellainen aritmeettinen funktio, että $f(1) \neq 0$. Nyt f on kvasimultiplikatiivinen, jos ja vain jos*

$$f(n) = f(1)^{-(r-1)} \prod_{i=1}^{r} f(p_i^{n(p_i)})$$

kaikilla positiivisilla kokonaisluvuilla $n = \prod_{i=1}^{r} p_i^{n(p_i)}$.

Todistus. Oletetaan ensin, että f on kvasimultiplikatiivinen aritmeettinen funktio. Todistetaan induktiolla luvun n alkulukutekijöiden lukumäärän suhteen, että tällöin $f(n) = f(1)^{-(r-1)} \prod_{i=1}^{r} f(p_i^{n(p_i)})$. Jos luvulla n ei ole lainkaan alkulukutekijöitä, niin $n = 1$. Nyt siis $f(n) = f(1) = f(1)^{-(0-1)}$. Tehdään induktio-oletus, että väite pätee kaikilla luvuilla, joilla on $k > 0$ alkulukutekijää. Olkoon $n = \prod_{i=1}^{k+1} p_i^{n(p_i)}$. Tällöin $(\prod_{i=1}^{k} p_i^{n(p_i)}, p_{k+1}^{n(p_{k+1})}) = 1$, joten kvasimultiplikatiivisuuden perusteella

$$f(n) = f(1)^{-1} f(\prod_{i=1}^{k} p_i^{n(p_i)}) f(p_{k+1}^{n(p_{k+1})}).$$

Nyt luvulla $\prod_{i=1}^{k} p_i^{n(p_i)}$ on k alkulukutekijää, joten soveltamalla induktio-oletusta saadaan edelleen, että

$$\begin{aligned} f(1)^{-1} f(\prod_{i=1}^{k} p_i^{n(p_i)}) f(p_{k+1}^{n(p_{k+1})}) &= f(1)^{-(k+1-1)} \prod_{i=1}^{k} f(p_i^{n(p_i)}) f(p_{k+1}^{n(p_{k+1})}) \\ &= f(1)^{-(k+1-1)} \prod_{i=1}^{k+1} f(p_i^{n(p_i)}). \end{aligned}$$

Induktioperiaatteen mukaan väite

$$f(n) = f(1)^{-(r-1)} \prod_{i=1}^{r} f(p_i^{n(p_i)})$$

pätee siis kaikilla kokonaisluvuilla $n = \prod_{i=1}^{r} p_i^{n(p_i)}$.

Oletetaan, että jokaisella positiivisella kokonaisluvulla $n = \prod_{i=1}^{r} p_i^{n(p_i)}$

$$f(n) = f(1)^{-(r-1)} \prod_{i=1}^{r} f(p_i^{n(p_i)}).$$

Valitaan sellaiset $m, n \in \mathbb{Z}_+$, että $(m, n) = 1$. Merkitään lukujen m ja n alkutekijäesityksiä merkinnöin $m = \prod_{i=1}^{r} p_i^{n(p_i)}$ ja $n = \prod_{i=r+1}^{r+s} p_i^{n(p_{r+i})}$, missä $n(p_i) > 0$ jokaisella $i = 1, 2, \ldots, r+s$. Huomaa, että oletuksen $(m, n) = 1$

perusteella $p_i \neq p_j$ kaikilla $i = 1, 2, \ldots, r$ ja $j = r+1, r+2, \ldots, r+s$. Nyt oletuksen perusteella

$$\begin{aligned} f(1)f(mn) =& f(1)f(\prod_{i=1}^{r+s} p_i^{n(p_i)}) \\ =& f(1)f(1)^{-(r+s-1)} \prod_{i=1}^{r+s} f(p_i^{n(p_i)}) \\ =& f(1)^{-(r+s-2)} \prod_{i=1}^{r+s} f(p_i^{n(p_i)}) \\ =& \left(f(1)^{-(r-1)} \prod_{i=1}^{r} f(p_i^{n(p_i)}) \right) \left(f(1)^{-(s-1)} \prod_{i=r+1}^{r+s} f(p_i^{n(p_i)}) \right) \\ =& f(m)f(n). \end{aligned}$$

Funktio f on siis kvasimultiplikatiivinen. □

Määritelmä 3.17. (Ks. [9], s. 14) Aritmeettista funktiota f sanotaan *multiplikatiiviseksi*, jos $f(1) = 1$ ja $f(mn) = f(m)f(n)$ aina, kun $m, n \in \mathbb{Z}_+$ ja $(m, n) = 1$.

Huomautus Kvasimultiplikatiivinen aritmeettinen funktio f on multiplikatiivinen, jos ja vain jos $f(1) = 1$. Toisaalta semimultiplikatiivinen aritmeettinen funktio g on kvasimultiplikatiivinen, jos ja vain jos $g(1) \neq 0$.

Lause 3.14. *(Ks. [8], s. 30) Olkoon f sellainen aritmeettinen funktio, että $f(1) = 1$. Nyt f on multiplikatiivinen, jos ja vain jos*

$$f(n) = \prod_{p \in \mathbb{P}} f(p^{n(p)})$$

kaikilla positiivisilla kokonaisluvuilla $n = \prod_{p \in \mathbb{P}} p^{n(p)}$.

Todistus. Oletetaan ensin, että f on multiplikatiivinen aritmeettinen funktio. Todistetaan väite induktiolla luvun n alkulukutekijöiden lukumäärän suhteen. Jos alkulukutekijöitä on 0, niin $n = 1$. Tällöin $f(n) = f(1) = \prod_{p \in \mathbb{P}} f(1)$. Tehdään induktio-oletus, että väite pätee luvulle n, jolla on $k > 0$ alkulukutekijää. Oletetaan, että luvulla $n = \prod_{p \in \mathbb{P}} p^{n(p)}$ on $k+1$ alkulukutekijää. Olkoon p' eräs luvun n alkulukutekijöistä. Tällöin luvulla $\prod_{p \in \mathbb{P} \setminus \{p'\}} p^{n(p)}$ on k alkulukutekijää ja lisäksi $(\prod_{p \in \mathbb{P} \setminus \{p'\}} p^{n(p)}, p'^{n(p')}) = 1$. Koska f on multipli-

katiivinen, niin saadaan että

$$\begin{aligned} f(n) =& f\left(\prod_{p\in\mathbb{P}} p^{n(p)}\right) \\ =& f(p'^{n(p')}) f\left(\prod_{p\in\mathbb{P}\setminus\{p'\}} p^{n(p)}\right) \\ =& f(p'^{n(p')}) \prod_{p\in\mathbb{P}\setminus\{p'\}} f(p^{n(p)}) \\ =& \prod_{p\in\mathbb{P}} f(p^{n(p)}). \end{aligned}$$

Oletetaan sitten, että $f(1) = 1$ ja $f(n) = \prod_{p\in\mathbb{P}} f(p^{n(p)})$ kaikilla positiivisilla kokonaisluvuilla $n = \prod_{p\in\mathbb{P}} f(p^{n(p)})$. Valitaan sellaiset $m, n \in \mathbb{Z}_+$, että $(m, n) = 1$. Olkoon $m = \prod_{p\in\mathbb{P}} p^{m(p)}$ ja $n = \prod_{p\in\mathbb{P}} p^{n(p)}$. Huomaa, että koska $(m, n) = 1$, niin $m(p) = 0$, jos $n(p) > 0$ ja vastaavasti $n(p) = 0$, jos $m(p) > 0$. Tällöin oletuksen mukaan

$$\begin{aligned} f(mn) =& \prod_{p\in\mathbb{P}} f(p^{m(p)+n(p)}) \\ =& \left(\prod_{p\in\mathbb{P}} f(p^{m(p)})\right)\left(\prod_{p\in\mathbb{P}} f(p^{n(p)})\right) \\ =& f(n)f(m). \end{aligned}$$

□

Määritelmä 3.18. (Ks. [9], s. 14) Aritmeettista funktiota f sanotaan *täydellisesti multiplikatiiviseksi*, jos $f(1) = 1$ ja $f(mn) = f(m)f(n)$ aina, kun $m, n \in \mathbb{Z}_+$.

Lause 3.15. *(Ks. [8], s. 35) Multiplikatiivinen aritmeettinen funktio f on täydellisesti multiplikatiivinen, jos ja vain jos*

$$f(p^a) = f(p)^a$$

jokaisella alkuluvulla p ja positiivisella kokonaisluvulla a.

Todistus. Todistetaan ensin induktiolla positiivisen kokonaislukupotenssin a suhteen, että jos f on täydellisesti multiplikatiivinen, niin

$$f(p^a) = f(p)^a$$

jokaisella alkuluvulla p ja positiivisella kokonaisluvulla a. Oletetaan, että aritmeettinen funktio f on täydellisesti multiplikatiivinen. Valitaan mielivaltainen alkuluku p. Väite pätee, kun $a = 1$, sillä tällöin $f(p^1) = f(p) = f(p)^1$. Oletetaan sitten, että $a > 1$. Tehdään induktio-oletus, että

$$f(p^{a-1}) = f(p)^{a-1}.$$

Täydellisen multiplikatiivisuuden määritelmän perusteella saadaan, että

$$f(p^a) = f(p^{a-1}p) = f(p^{a-1})f(p) = f(p)^{a-1}f(p) = f(p)^a.$$

Tällöin induktioperiaatteen nojalla

$$f(p^a) = f(p)^a$$

jokaisella alkuluvulla p ja positiivisella kokonaisluvulla a, jos f on täydellisesti multiplikatiivinen.

Oletetaan sitten, että aritmeettinen funktio f on multiplikatiivinen ja että

$$f(p^a) = f(p)^a$$

jokaisella alkuluvulla p ja positiivisella kokonaisluvulla a. Olkoot $m, n \in \mathbb{Z}_+$. Nyt lauseen 3.14 sekä oletuksen perusteella

$$\begin{aligned} f(mn) =& \prod_{p\in\mathbb{P}} f(p^{m(p)+n(p)}) \\ =& \prod_{p\in\mathbb{P}} \left(f(p)^{m(p)} f(p)^{n(p)}\right) \\ =& \prod_{p\in\mathbb{P}} f(p)^{m(p)} \prod_{p\in\mathbb{P}} f(p)^{n(p)} \\ =& \prod_{p\in\mathbb{P}} f(p^{m(p)}) \prod_{p\in\mathbb{P}} f(p^{n(p)}) \\ =& f(m)f(n). \end{aligned}$$

Koska multiplikatiivisuuden perusteella lisäksi $f(1) = 1$, niin määritelmän 3.18 mukaan aritmeettinen funktio f on täydellisesti multiplikatiivinen. □

Määritelmä 3.19. (Ks. [9], s. 14) Multiplikatiivista aritmeettista funktiota f sanotaan *vahvasti multiplikatiiviseksi*, jos $f(p^a) = f(p)$ aina, kun $p \in \mathbb{P}$ ja $a \in \mathbb{Z}_+$.

Määritelmä 3.20. (Ks. [8], s. 36) Lukujonon $(a_k)_{k=0}^{\infty}$ *muodollinen potenssisarja* on lauseke

$$a(x) = \sum_{k=0}^{\infty} a_k x^k.$$

Määritelmä 3.21. (Ks. [8], s. 36) *Muodollisten potenssisarjojen* $a(x)$ *ja* $b(x)$ *summa* $a(x) + b(x)$ on sellainen muodollinen potenssisarja, että

$$a(x) + b(x) = \sum_{k=0}^{\infty} (a_k + b_k)x^k.$$

Määritelmä 3.22. (Ks. [8], s. 36) *Muodollisten potenssisarjojen $a(x)$ ja $b(x)$ tulo $a(x)b(x)$* on sellainen muodollinen potenssisarja, että

$$a(x)b(x) = \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) x^k.$$

Toisinaan muodollisten potenssisarjojen tulosta käytetään myös nimitystä *Cauchyn tulo*.

Huomautus Symbolin x potenssi ilmaisee pelkästään kertoimensa paikan lukujonossa. Symbolille x ei anneta lukuarvoja, joten muodollinen potenssisarja on itse asiassa vaihtoehtoinen tapa lukujonojen esittämiseksi.

Määritelmä 3.23. (Ks. [8], s. 37) Olkoon p alkuluku ja f aritmeettinen funktio. Määritellään

$$f_p(x) = \sum_{k=0}^{\infty} f(p^k) x^k.$$

Tätä muodollista potenssisarjaa kutsutaan *aritmeettisen funktion f Bellin sarjaksi modulo p*.

Lause 3.16. *(Ks. [8], s. 37) Olkoot f ja g aritmeettisia funktioita. Nyt*

$$(f * g)_p(x) = f_p(x) g_p(x),$$

jokaisella alkuluvulla p.

Todistus. Muodollisessa potenssisarjassa $(f*g)_p(x)$ kirjainosan x^k kerroin on $(f * g)(p^k) = \sum_{d|p^k} f(d)g(p^k/d)$. Tämä kerroin voidaan kirjoittaa muodossa $\sum_{i=0}^{k} f(p^i)g(p^{k-i})$, joka on muodollisten potenssisarjojen tulon määritelmän perusteella muodollisten potenssisarjojen $f_p(x)$ ja $g_p(x)$ tulon kirjainosan x^k kerroin. □

Lause 3.17. *(Ks. [8], s. 37) Olkoot f ja g multiplikatiivisia aritmeettisia funktioita. Nyt $f = g$, jos ja vain jos $f_p(x) = g_p(x)$ jokaisella alkuluvulla p.*

Todistus. Lauseen 3.14 perusteella funktion arvot alkulukujen potensseilla määräävät yksikäsitteisesti multiplikatiivisen funktion arvot muissa pisteissä. □

Lause 3.18. *Olkoon f sellainen aritmeettinen funktio, että $f(1) \neq 0$. Nyt $(f_*^{-1})_p(x) = \frac{1}{f_p(x)}$ jokaisella alkuluvulla p.*

Todistus. Olkoon p mielivaltainen alkuluku. Tällöin käänteisfunktion määritelmän perusteella $f * f_*^{-1} = \delta$, joten $(f * f_*^{-1})_p(x) = \delta_p(x)$. Lauseen 3.16 mukaan $(f * f_*^{-1})_p(x) = f_p(x)(f_*^{-1})_p(x)$, joten

$$(f_*^{-1})_p(x) = \frac{\delta_p(x)}{f_p(x)} = \frac{1}{f_p(x)}.$$

□

Lause 3.19. *(Ks. [8], s. 38) Olkoot f ja g sellaisia multiplikatiivisia aritmeettisia funktioita, että $f_p(x)g_p(x) = 1$ kaikilla $p \in \mathbb{P}$. Tällöin $f_*^{-1} = g$.*

Todistus. Lauseen 3.18 mukaan $(f_*^{-1})_p(x) = \frac{1}{f_p(x)} = g_p(x)$. Tästä seuraa suoraan lauseen 3.17 perusteella, että $f_*^{-1} = g$. □

Määritelmä 3.24. (Ks. [15], s. 611-612) Aritmeettinen funktio f on *astetta* (r, s) *oleva aritmeettinen rationaalifunktio*, jos on olemassa sellaiset täydellisesti multiplikatiiviset aritmeettiset funktiot $g_1, g_2, \ldots, g_r$ ja $h_1, h_2, \ldots, h_s$, että

$$f = g_1 * g_2 * \cdots * g_r * (h_1)_*^{-1} * (h_2)_*^{-1} * \cdots * (h_s)_*^{-1}.$$

Huomautus Englanninkielisissä lähteissä usein esiintyvällä sanalla *totient* tarkoitetaan astetta $(1, 1)$ olevia aritmeettisia rationaalifunktioita. Vastaavaa suomenkielistä termiä ei ole käytössä. Usein suomenkielisissä teksteissä kuitenkin lainataan suoraan englanninkielistä termiä.

Lause 3.20. *(Vrt. [15], s. 593, 611-612 ja 616) Olkoon f multiplikatiivinen aritmeettinen funktio. Funktio f on astetta (r, s) oleva aritmeettinen rationaalifunktio, jos ja vain jos jokaisella alkuluvulla p on olemassa sellaiset kompleksiluvut $a_1(p), a_2(p), \ldots, a_s(p)$ ja $b_1(p), b_2(p), \ldots, b_r(p)$, että*

$$f_p(x) = \frac{1 + a_1(p)x + a_2(p)x^2 + \cdots + a_s(p)x^s}{1 + b_1(p)x + b_2(p)x^2 + \cdots + b_r(p)x^r}.$$

Todistus. Oletetaan ensin, että f on astetta (r, s) oleva aritmeettinen rationaalifunktio. On siis olemassa sellaiset täydellisesti multiplikatiiviset aritmeettiset funktiot $g_1, g_2, \ldots, g_r$ ja $h_1, h_2, \ldots, h_s$, että

$$f = g_1 * g_2 * \cdots * g_r * (h_1)_*^{-1} * (h_2)_*^{-1} * \cdots * (h_s)_*^{-1}.$$

Olkoon p mielivaltainen alkuluku. Nyt täydellisen multiplikatiivisuuden perusteella saadaan

$$(g_i)_p(x) = \sum_{k=0}^{\infty} g_i(p^k)x^k = \sum_{k=0}^{\infty}(g_i(p)x)^k = (1 - g_i(p)x)^{-1}$$

kaikilla $i = 1, 2, \ldots, r$. Vastaavasti $(h_i)_p(x) = (1 - h_i(p)x)^{-1}$, joten lauseen 3.18 mukaan $((h_i)_*^{-1})_p(x) = (1 - h_i(p)x)$ jokaisella $i = 1, 2, \ldots, s$. Nyt saadaan funktion f Bellin sarjaksi

$$\begin{aligned} f_p(x) &= (g_1 * g_2 * \cdots * g_r * (h_1)_*^{-1} * (h_2)_*^{-1} * \cdots * (h_s)_*^{-1})_p(x) \\ &= (g_1)_p(x)(g_2)_p(x) \cdots (g_r)_p(x)((h_1)_*^{-1})_p(x)((h_2)_*^{-1})_p(x) \cdots ((h_s)_*^{-1})_p(x) \\ &= \frac{(1 - h_1(p)x)(1 - h_2(p)x) \cdots (1 - h_s(p)x)}{(1 - g_1(p)x)(1 - g_2(p)x) \cdots (1 - g_r(p)x)}. \end{aligned}$$

Bellin sarjan osoittaja koostuu s kompleksilukukertoimisen ensimmäisen asteen muodollisen potenssisarjan tulosta, joten potenssisarjojen tulon aste on korkeintaan s. Vastaava tarkastelu nimittäjälle osoittaa, että nimittäjän aste on korkeintaan r. Kertomalla tulot auki saadaan kertoimista sellaiset kompleksiluvut $a_1(p), a_2(p), \ldots, a_s(p)$ ja $b_1(p), b_2(p), \ldots, b_r(p)$, että

$$f_p(x) = \frac{1 + a_1(p)x + a_2(p)x^2 + \cdots + a_s(p)x^s}{1 + b_1(p)x + b_2(p)x^2 + \cdots + b_r(p)x^r}.$$

Oletetaan seuraavaksi, että jokaista alkulukua p kohti on olemassa sellaiset kompleksiluvut $a_1(p), a_2(p), \ldots, a_s(p)$ ja $b_1(p), b_2(p), \ldots, b_r(p)$, että

$$f_p(x) = \frac{1 + a_1(p)x + a_2(p)x^2 + \cdots + a_s(p)x^s}{1 + b_1(p)x + b_2(p)x^2 + \cdots + b_r(p)x^r}.$$

Koska kompleksilukujen kunta on algebrallisesti suljettu, niin on olemassa sellaiset luvut $a'_1(p), a'_2(p), \ldots, a'_s(p)$ ja $b'_1(p), b'_2(p), \ldots, b'_r(p)$, että

$$f_p(x) = \frac{(1 - a'_1(p)x)(1 - a'_2(p)x)\cdots(1 - a'_s(p)x)}{(1 - b'_1(p)x)(1 - b'_2(p)x)\cdots(1 - b'_r(p)x)}.$$

Määritellään seuraavaksi täydellisesti multiplikatiiviset funktiot asettamalla $g_i(p) = b'_i(p)$ jokaisella $i = 1, 2, \ldots, r$ ja $h_j(p) = a'_j$ jokaisella $j = 1, 2, \ldots, s$ aina, kun p on alkuluku.

Olkoon p mielivaltainen alkuluku. Täydellisen multiplikatiivisuuden perusteella aritmeettisten funktioiden g_i ja h_i Bellin sarjoiksi saadaan tällöin $(g_i)_p(x) = (1 - b'_i(p)x)^{-1}$ ja $(h_i)_p(x) = (1 - a'_i(p)x)^{-1}$. Edelleen lauseen 3.18 mukaan $((h_i)_*^{-1})_p(x) = (1 - a'_i(p)x)$. Nyt lauseen 3.16 mukaan

$$\begin{aligned}
&(g_1 * g_2 * \cdots * g_r * (h_1)_*^{-1} * (h_2)_*^{-1} * \cdots * (h_s)_*^{-1})_p(x) \\
&\quad = (g_1)_p(x)(g_2)_p(x)\cdots(g_r)_p(x)((h_1)_*^{-1})_p(x)((h_2)_*^{-1})_p(x)\cdots((h_s)_*^{-1})_p(x) \\
&\quad = \frac{(1 - a'_1(p)x)(1 - a'_2(p)x)\cdots(1 - a'_s(p)x)}{(1 - b'_1(p)x)(1 - b'_2(p)x)\cdots(1 - b'_r(p)x)}.
\end{aligned}$$

Koska f on multiplikatiivinen ja multiplikatiivisten funktioiden Dirichlet'n tulo $g_1 * g_2 * \cdots * g_r * (h_1)_*^{-1} * (h_2)_*^{-1} * \cdots * (h_s)_*^{-1}$ on multiplikatiivinen, niin lauseen 3.17 mukaan $f = g_1 * g_2 * \cdots * g_r * (h_1)_*^{-1} * (h_2)_*^{-1} * \cdots * (h_s)_*^{-1}$. □

3.4 Unitaarikonvoluutio

Seuraavaksi määritellään unitaarikonvoluutio sekä todistetaan tutkielman kannalta keskeisimmät unitaarikonvoluution ominaisuuksia koskevat lauseet. Luvun lähteinä on käytetty multiplikatiivisten funktioiden unitaarikonvoluutioiden osalta teosta *The theory of multiplicative arithmetic functions*, jonka kirjoitti jo 1930-luvun vaihteessa intialainen matemaatikko Ramaswamy Vaidyanathaswamy. Lähteenä on käytetty myös Rodney Hansenin ja Leonard

Swansonin kirjoittamaa artikkelia *Unitary divisors* sekä Pentti Haukkasen kirjoittamaa luentomonistetta *Lukuteoriaa*. Viimeisenä mainitussa luentomonisteessa todistetaan useita Dirichlet'n konvoluution perusominaisuuksia. Dirichlet'n konvoluutio ja unitaarikonvoluutio ovat ominaisuuksiltaan jokseenkin samankaltaisia, sillä ne molemmat kuuluvat K-konvoluutioiden luokkaan (ks. [8], s. 41). Tässä luvussa todistetaan vastaavat perusominaisuudet unitaarikonvoluutiolle luentomonisteessa esitettyjen Dirichlet'n konvoluutiota koskevien todistusten pohjalta.

Määritelmä 3.25. (Ks. [1], s. 66) Aritmeettisten funktioiden f ja g *unitaarikonvoluutio* $f \oplus g$ on sellainen aritmeettinen funktio, että

$$(f \oplus g)(n) = \sum_{d \| n} f(d)g(n/d), n \in \mathbb{Z}_+.$$

Lause 3.21. *Unitaarikonvoluutio on kommutatiivinen.*

Todistus. (Vrt. [8], s. 28) Jos $d \parallel n$, niin $d \mid n$ ja $(d, n/d) = 1$. Tällöin $(n/d) \mid n$ ja $(n/d, n/(n/d)) = (n/d, n) = (n, n/d) = 1$, joten $(n/d) \parallel n$. Luku n/d käy siis läpi kaikki luvun n unitaaritekijät, jos d käy läpi kaikki luvun n unitaaritekijät.

Olkoot sitten f ja g aritmeettisia funktioita ja olkoon $n \in \mathbb{Z}_+$. Nyt siis

$$\begin{aligned}(f \oplus g)(n) &= \sum_{d \| n} f(d)g(n/d) \\ &= \sum_{(n/d) \| n} g(n/d)f(d) \\ &= \sum_{d \| n} g(d)f(n/d) = (g \oplus f)(n).\end{aligned}$$

Näin ollen $f \oplus g = g \oplus f$. □

Lause 3.22. *Unitaarikonvoluutio on assosiatiivinen.*

Todistus. (Vrt. [8], s. 28) Olkoot f, g ja h aritmeettisia funktioita. Valitaan mielivaltainen positiivinen kokonaisluku n. Nyt

$$\begin{aligned}((f \oplus g) \oplus h)(n) &= \sum_{\substack{d \| n \\ dc = n}} (f \oplus g)(d)h(c) \\ &= \sum_{\substack{d \| n \\ dc = n}} \left(\sum_{\substack{a \| d \\ ab = d}} f(a)g(b) \right) h(c) \\ &= \sum_{\substack{d \| n \\ dc = n}} \sum_{\substack{a \| d \\ ab = d}} f(a)g(b)h(c)\end{aligned}$$

$$
\begin{aligned}
&= \sum_{\substack{a\|n,\ b\|n,\ c\|n \\ abc=n}} f(a)g(b)h(c) \\
&= \sum_{\substack{a\|n \\ aD=n}} \sum_{\substack{b\|D \\ bc=D}} f(a)g(b)h(c) \\
&= \sum_{\substack{a\|n \\ aD=n}} f(a) \left(\sum_{\substack{b\|D \\ bc=D}} g(b)h(c) \right) \\
&= \sum_{\substack{a\|n \\ aD=n}} f(a)(g \oplus h)(D) \\
&= (f \oplus (g \oplus h))(n).
\end{aligned}
$$

Siis $f \oplus (g \oplus h) = (f \oplus g) \oplus h$ kaikilla aritmeettisilla funktioilla f, g ja h. □

Lause 3.23. *Aritmeettinen funktio δ on ykkösfunktio unitaarikonvoluution suhteen.*

Todistus. (Vrt. [8], s. 28) Kommutatiivisuuden perusteella riittää todistaa, että $f \oplus \delta = f$. Olkoon f mielivaltainen aritmeettinen funktio ja olkoon n positiivinen kokonaisluku.

$$(f \oplus \delta)(n) = \sum_{d\|n} f(d)\delta(n/d) = f(n)\delta(1) = f(n).$$

□

Lause 3.24. *(Vrt. [8], s. 29) Aritmeettisella funktiolla f on käänteisfunktio $f_\oplus^{-1}$ unitaarikonvoluution suhteen, jos $f(1) \neq 0$. Tällöin $f_\oplus^{-1}$ saadaan rekursiivisesti kaavasta*

$$
\begin{aligned}
f_\oplus^{-1}(1) &= 1 \\
f_\oplus^{-1}(n) &= -\frac{1}{f(1)} \sum_{\substack{d\|n \\ d>1}} f(d) f_\oplus^{-1}\left(\frac{n}{d}\right).
\end{aligned}
$$

Todistus. Oletetaan, että $f(1) \neq 0$. Ja määritellään $f_\oplus^{-1}$ kuten edellä. Nyt

$(f \oplus f_{\oplus}^{-1})(1) = (f_{\oplus}^{-1} \oplus f)(1) = f(1)f_{\oplus}^{-1}(1) = f(1)\frac{1}{f(1)} = 1 = \delta(1)$. Lisäksi

$$\begin{aligned}(f_{\oplus}^{-1} \oplus f)(n) =& (f \oplus f_{\oplus}^{-1})(n) \\ =& \sum_{d\|n} f(d)f_{\oplus}^{-1}(\frac{n}{d}) \\ =& f(1)f_{\oplus}^{-1}(n) + \sum_{\substack{d\|n \\ d>1}} f(d)f_{\oplus}^{-1}(\frac{n}{d}) \\ =& f(1)f_{\oplus}^{-1}(n) - f(1)\frac{-1}{f(1)} \sum_{\substack{d\|n \\ d>1}} f(d)f_{\oplus}^{-1}(\frac{n}{d}) \\ =& f(1)f_{\oplus}^{-1}(n) - f(1)f_{\oplus}^{-1}(n) = 0 = \delta(n),\end{aligned}$$

kun $n > 1$.

Olkoon g mielivaltainen aritmeettinen funktio. Oletetaan lisäksi, että $f(1) = 0$. Nyt $(f \oplus g)(1) = f(1)g(1) = 0 \neq 1 = \delta(1)$, joten funktiolla f ei ole käänteisfunktiota unitaarikonvoluution suhteen. □

Huomautus Funktio f on kääntyvä sekä Dirichlet'n konvoluution että unitaarikonvoluution suhteen, jos $f(1) \neq 0$.

Lause 3.25. *Struktuuri $\langle \mathcal{A}_0, \oplus \rangle$ on Abelin ryhmä, jossa ykkösalkiona toimii funktio δ.*

Todistus. Väite seuraa suoraan lauseista 3.21,3.22,3.23 ja 3.24. □

Seuraavaksi ryhdytään todistamaan muutamia multiplikatiivisten aritmeettisten funktioiden unitaarikonvoluutioihin liittyviä tuloksia. Lisätietoa aiheesta löytyy esimerkiksi lähteen [15] sivuilta 606-611.

Lause 3.26. *Jos aritmeettiset funktiot f ja g ovat multiplikatiivisia, niin myös niiden unitaarikonvoluutio $f \oplus g$ on multiplikatiivinen.*

Todistus. (Vrt. [8], s. 30) Valitaan sellaiset $m, n \in \mathbb{Z}_+$, että $(m, n) = 1$. Jos nyt $d \parallel mn$, niin on olemassa sellaiset $a, b \in \mathbb{Z}_+$, että $a \parallel m$,$b \parallel n$ ja $d = ab$. Lisäksi tällöin $(a, b) = 1$ ja $(m/a, n/b) = 1$. Nyt unitaarikonvoluution

määritelmän perusteella saadaan, että

$$\begin{aligned}
(f \oplus g)(mn) &= \sum_{d \| mn} f(d) g((mn)/d) \\
&= \sum_{\substack{a \| m \\ b \| n}} f(ab) g((mn)/(ab)) \\
&= \sum_{\substack{a \| m \\ b \| n}} f(ab) g((m/a)(n/b)) \\
&= \sum_{\substack{a \| m \\ b \| n}} f(a) f(b) g(m/a) g(n/b) \\
&= \sum_{\substack{a \| m \\ b \| n}} f(a) g(m/a) f(b) g(n/b) \\
&= \left(\sum_{a \| m} f(a) g(m/a) \right) \left(\sum_{b \| n} f(b) g(n/b) \right) \\
&= (f \oplus g)(m)(f \oplus g)(n).
\end{aligned}$$

□

Lause 3.27. *Jos f on multiplikatiivinen, niin $f_{\oplus}^{-1}$ on multiplikatiivinen.*

Todistus. (Vrt. [8], s. 30) Todistetaan väite induktiolla lauseen 3.24 käänteisfunktion konstruktion suhteen. Jos f on multiplikatiivinen, niin $f(1) = 1$, joten $f_{\oplus}^{-1}$ on olemassa. Tällöin lauseen 3.24 mukaan $f_{\oplus}^{-1}(1) = 1/f(1) = 1$. Valitaan sitten sellaiset $m, n \in \mathbb{Z}_+$, että $(m, n) = 1$. Jos $m = 1$ tai $n = 1$, niin triviaalisti $f_{\oplus}^{-1}(mn) = f_{\oplus}^{-1}(m) f_{\oplus}^{-1}(n)$. Voidaan siis olettaa, että $m, n > 1$, jolloin myös $mn > 1$. Tehdään vielä induktio-oletus, että väite pätee kaikilla $m', n' \in \mathbb{Z}_+$, joilla $(m', n') = 1$ ja $m'n' < mn$. Nyt lauseen 3.24 perusteella saadaan, että

$$\begin{aligned}
f_{\oplus}^{-1}(mn) &= -\frac{1}{f(1)} \sum_{\substack{d \| mn \\ d > 1}} f(d) f_{\oplus}^{-1}((mn)/d) \\
&= -\frac{1}{1} \sum_{\substack{a \| m \\ b \| n \\ ab > 1}} f(ab) f_{\oplus}^{-1}((mn)/(ab)) \\
&= -\sum_{\substack{a \| m \\ b \| n \\ ab > 1}} f(ab) f_{\oplus}^{-1}((m/a)(n/b))
\end{aligned}$$

$$
\begin{aligned}
&= -\sum_{\substack{a\|m\\ b\|n\\ ab>1}} f(a)f(b)f_{\oplus}^{-1}(m/a)f_{\oplus}^{-1}(n/b)\\
&= f(1)f(1)f_{\oplus}^{-1}(m/1)f_{\oplus}^{-1}(n/1) - \sum_{\substack{a\|m\\ b\|n}} f(a)f_{\oplus}^{-1}(m/a)f(b)f_{\oplus}^{-1}(n/b)\\
&= f_{\oplus}^{-1}(m)f_{\oplus}^{-1}(n) - \left(\sum_{a\|m} f(a)f_{\oplus}^{-1}(m/a)\right)\left(\sum_{b\|n} f(b)f_{\oplus}^{-1}(n/b)\right)\\
&= f_{\oplus}^{-1}(m)f_{\oplus}^{-1}(n) - (f\oplus f_{\oplus}^{-1})(m)(f\oplus f_{\oplus}^{-1})(n)\\
&= f_{\oplus}^{-1}(m)f_{\oplus}^{-1}(n) - \delta(m)\delta(n)\\
&= f_{\oplus}^{-1}(m)f_{\oplus}^{-1}(n).
\end{aligned}
$$

□

Määritelmä 3.26. Funktio ζ on sellainen aritmeettinen funktio, että $\zeta(n) = 1$ kaikilla $n \in \mathbb{Z}_+$.

Tavanomainen *Möbiuksen funktio* määritellään funktion ζ käänteisfunktiona Dirichlet'n konvoluution suhteen. Tässä tutkielmassa tarvitaan kuitenkin *Möbiuksen funktion unitaarista vastinetta*, joka määritellään vastaavasti käyttämällä Dirichlet'n konvoluution käänteisfunktion sijaan unitaarikonvoluution käänteisfunktiota. Tämän luvun lopussa määritellään vielä *Möbiuksen käänteiskaavalle unitaarinen vastine* (lause 3.30) käyttäen tavanomaisessa *Möbiuksen käänteiskaavassa* (ks. [8], s. 32) Möbiuksen funktion sijaan tämän unitaarista vastinetta.

Määritelmä 3.27. (Ks. [8], s. 31) Funktio μ^* on sellainen aritmeettinen funktio, että $\mu^* = \zeta_{\oplus}^{-1}$. Funktiota μ^* kutsutaan *Möbiuksen funktion unitaariseksi vastineeksi.*

Huomautus Aritmeettinen funktio $\zeta_{\oplus}^{-1}$ on olemassa, sillä $\zeta(1) = 1 \neq 0$.

Lause 3.28. *Möbiuksen funktion unitaarinen vastine on multiplikatiivinen.*

Todistus. Väite seuraa suoraan lauseesta 3.24. □

Lause 3.29.

$$\mu^*(n) = (-1)^{\omega(n)}$$

kaikilla $n \in \mathbb{Z}_+$.

Todistus. Multiplikatiivisuuden perusteella $\mu^*(1) = 1$. Olkoon p mielivaltainen alkuluku ja olkoon a positiivinen kokonaisluku. Tällöin lauseen 3.24 perusteella saadaan

$$\mu^*(p^a) = -\frac{1}{\zeta(1)}\sum_{\substack{d\|p^a\\ d>1}} \zeta(d)\mu^*(\frac{p^a}{d}) = -\zeta(p^a)\mu^*(1) = -\mu^*(1) = -1.$$

Olkoon n mielivaltainen positiivinen kokonaisluku ja olkoon $\prod_{i=1}^{r} p_i^{a_i}$ luvun n kanoninen alkutekijäesitys. Nyt multiplikatiivisuuden perusteella

$$\begin{aligned}\mu^*(n) =& \mu^*(\prod_{i=1}^{r} p_i^{a_i}) \\ =& \prod_{i=1}^{r} \mu^*(p_i^{a_i}) \\ =& (-1)^r \\ =& (-1)^{\omega(n)}.\end{aligned}$$

□

Lause 3.30. *Olkoot f ja g aritmeettisia funktioita. Tällöin*

$$f(n) = \sum_{d\|n} g(d)$$

kaikilla $n \in \mathbb{Z}_+$, jos ja vain jos

$$g(n) = \sum_{d\|n} \mu^*(d) f(n/d)$$

kaikilla $n \in \mathbb{Z}_+$.

Todistus. Olkoot f ja g aritmeettisia funktioita. Oletetaan ensin, että

$$f(n) = \sum_{d\|n} g(d)$$

jokaisella $n \in \mathbb{Z}_+$. Tällöin unitaarikonvoluution määritelmän perusteella

$$\begin{aligned}f(n) =& \sum_{d\|n} g(d) \\ =& \sum_{d\|n} g(d)\zeta(n/d) \\ =& (g \oplus \zeta)(n)\end{aligned}$$

kaikilla $n \in \mathbb{Z}_+$ eli $f = g \oplus \zeta$. Edelleen unitaarikonvoluution assosiatiivisuuden perusteella

$$\begin{aligned}f \oplus \mu^* =& (g \oplus \zeta) \oplus \mu^* \\ =& g \oplus (\zeta \oplus \mu^*) \\ =& g \oplus \delta \\ =& g,\end{aligned}$$

joten unitaarikonvoluution määritelmän perusteella

$$g(n) = \sum_{d\|n} f(d)\mu^*(n/d)$$

jokaisella $n \in \mathbb{Z}_+$.

Oletetaan seuraavaksi, että

$$g(n) = \sum_{d\|n} f(d)\mu^*(n/d)$$

jokaisella $n \in \mathbb{Z}_+$. Nyt unitaarikonvoluution määritelmän mukaan $g = f \oplus \mu^*$. Assosiatiivisuuden perusteella saadaan

$$\begin{aligned} g \oplus \zeta =& (f \oplus \mu^*) \oplus \zeta \\ =& f \oplus (\mu^* \oplus \zeta) \\ =& f \oplus \delta \\ =& f, \end{aligned}$$

joten unitaarikonvoluution määritelmän mukaan

$$\begin{aligned} f(n) =& \sum_{d\|n} g(d)\zeta(n/d) \\ =& \sum_{d\|n} g(d). \end{aligned}$$

□

Huomautus Edellä todistettua lausetta kutsutaan *Möbiuksen käänteiskaavan unitaariseksi vastineeksi.*

3.5 Lineaarialgebraa

Määritelmä 3.28. (Ks. [5], s. 2) Olkoon $\boldsymbol{A} = [a_{ij}]$ $m \times n$-matriisi. Merkitään

$$\boldsymbol{A}\begin{pmatrix} l_1 & l_2 & \dots & l_p \\ k_1 & k_2 & \dots & k_p \end{pmatrix} = \begin{vmatrix} a_{l_1k_1} & a_{l_1k_2} & \cdots & a_{l_1k_p} \\ a_{l_2k_1} & a_{l_2k_2} & \cdots & a_{l_2k_p} \\ \vdots & \vdots & \ddots & \vdots \\ a_{l_pk_1} & a_{l_pk_2} & \cdots & a_{l_pk_p} \end{vmatrix}.$$

Mikäli $1 \leq l_1 < l_2 < \cdots < l_p \leq n$ ja $1 \leq k_1 < k_2 < \cdots < k_p \leq m$, niin tätä determinanttia kutsutaan matriisin $\boldsymbol{A}$ rivien $l_1, l_2, \cdots, l_p$ ja sarakkeiden $k_1, k_2, \cdots, k_p$ määräämääksi *minoriksi.*

Yleensä determinantti määritellään rekursion avulla. Yhtäpitävänä määritelmänä esitetään toisinaan Leibnizin kaava determinanteille, joka todistetaan seuraavaksi rekursiivisesta määritelmästä välittömästi seuraavien determinantin perusominaisuuksien avulla. Matriisin determinantti ominaisuuksineen oletetaan tunnetuksi. Aiheen hyvin kattavana lähteenä mainittakoon Stephen Friedbergin, Arnold Inselin ja Lawrence Spencen kirjoittama kirja *Linear algebra*, jonka sivuilla 199-236 esitetään tarvittavat determinantteja koskevat todistukset. Syvällisempää tietoa matriiseista löytyy esimerkiksi lähteestä [5]. Leibnizin kaavaa hyödynnetään tämän luvun lopussa esitettävän Cauchy-Binet -kaavan todistuksessa. Kyseistä kaavaa tarvitaan luvussa 5 esitettävien tutkielman loppuosassa tarvittavien lauseiden todistuksissa.

Lause 3.31. *(Ks. [5], s. 2)*
Olkoon $\boldsymbol{A}$ $n \times n$*-matriisi. Nyt*

$$\det(\boldsymbol{A}) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{\alpha=1}^{n} a_{\sigma(\alpha)\alpha},$$

missä S_n *on joukon* $\{1, 2, \ldots, n\}$ *permutaatioiden joukko ja* sgn *permutaation merkkifunktio.*

Todistus. Todistetaan väite induktiolla matriisin dimension suhteen.

Olkoon matriisi $\boldsymbol{A} = [a_{11}]$ mielivaltainen 1×1-matriisi. Nyt

$$\sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{\alpha=1}^{1} a_{\sigma(\alpha)\alpha} = a_{11} = \det(\boldsymbol{A}),$$

joten Leibnizin kaava pätee 1×1-matriiseille.

Tehdään seuraavaksi induktio-oletus, että Leibnizin kaava pätee kaikille $n-1 \times n-1$-matriiseille. Olkoon matriisin A dimensio $n \times n$. Kehittämällä matriisin $\boldsymbol{A}$ determinantti alinta riviä pitkin saadaan

$$\det(\boldsymbol{A}) = \sum_{i=1}^{n} (-1)^{i+n} a_{in} \det(\widetilde{\boldsymbol{A}}_{in}),$$

missä matriisin $\boldsymbol{A}$ alimatriisi $\det(\widetilde{\boldsymbol{A}}_{in})$ on saatu matriisista $\boldsymbol{A}$ poistamalla siitä rivi n ja sarake i. Matriisin $\widetilde{\boldsymbol{A}}_{in}$ dimensio on siis $n-1 \times n-1$. Soveltamalla nyt induktio-oletusta saadaan edelleen, että

$$\det(\widetilde{\boldsymbol{A}}_{in}) = \sum_{\sigma \in S_{n-1}} \operatorname{sgn}(\sigma) \prod_{\alpha=1}^{n-1} a_{\sigma_i^*(\alpha)\alpha},$$

missä

$$\sigma_i^*(\alpha) = \begin{cases} \sigma(\alpha), & \text{kun } \sigma(\alpha) < i \\ \sigma(\alpha) + 1, & \text{kun } \sigma(\alpha) \geq i. \end{cases}$$

Apufunktio σ_i^* joudutaan määrittelemään siksi, että matriisin $\boldsymbol{A}$ saraketta i ei esiinny lainkaan alimatriisissa $\widetilde{\boldsymbol{A}}_{in}$. Määritellään edelleen joukon S_n permutaatio $\sigma_i = \sigma_i^* \cup \{(n, i)\}$.

Nyt siis

$$\begin{aligned}\det(\boldsymbol{A}) &= \sum_{i=1}^{n} a_{in}(-1)^{i+n} \sum_{\sigma \in S_{n-1}} \operatorname{sgn}(\sigma) \prod_{\alpha=1}^{n-1} a_{\sigma_i^*(\alpha)\alpha} \\ &= \sum_{i=1}^{n} \sum_{\sigma \in S_{n-1}} (-1)^{i+n} \operatorname{sgn}(\sigma) a_{in} \prod_{\alpha=1}^{n-1} a_{\sigma_i^*(\alpha)\alpha} \\ &= \sum_{i=1}^{n} \sum_{\sigma \in S_{n-1}} \operatorname{sgn}(\sigma_i) \prod_{\alpha=1}^{n} a_{\sigma_i(\alpha)\alpha}.\end{aligned}$$

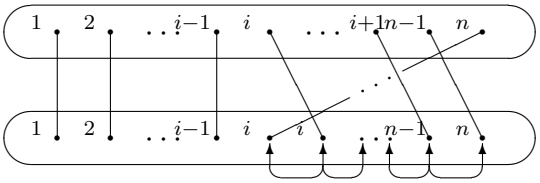
Huomaa, että $\operatorname{sgn}(\sigma_i) = \operatorname{sgn}(\sigma_i^*)(-1)^{n+i}$. Jos τ on peruspermutaatio, niin permutaatio τ_i voidaan saattaa peruspermutaatioksi $n - i$ kappaleella transpositioita (ks. kuva 2). Kuviossa nuolet kuvaavat transpositioita, jotka suoritetaan järjestyksessä vasemmalta oikealla.

Nyt $\operatorname{sgn}(\tau_i) = (-1)^{n-i} \operatorname{sgn}(\tau) = (-1)^{n+i}$. Jos siis permutaatio σ voidaan saattaa peruspermutaatioksi k transpositiolla, niin σ_i voidaan saattaa peruspermutaatioksi $k + n - i$ permutaatiolla. Tällöin

$$\operatorname{sgn}(\sigma_i) = (-1)^{k+n-1} = (-1)^k(-1)^{n-i} = \operatorname{sgn}(\sigma)(-1)^{n-i} = \operatorname{sgn}(\sigma)(-1)^{n+i}.$$

Kuva 2: Permutaation τ_i järjestäminen peruspermutaatioksi

Permutaatio τ_i:



Koska edelleen $\cup\{\sigma_i : \sigma \in S_{n-1}, i = 1, 2, \ldots, n-1\} = S_n$, niin nyt pätee

$$\det(\boldsymbol{A}) = \sum_{\sigma^* \in S_n} \operatorname{sgn}(\sigma^*) \prod_{\alpha=1}^{n} a_{\sigma(\alpha)\alpha}.$$

□

Lause 3.32. *Olkoon $\boldsymbol{C}$ $m \times m$-matriisi, joka voidaan esittää $m \times n$-matriisin $\boldsymbol{A}$ ja $n \times m$-matriisin $\boldsymbol{B}$ matriisitulona eli $\boldsymbol{C} = \boldsymbol{AB}$. Tällöin*

$$\det(\boldsymbol{C}) = \sum_{1 \le k_1 < \cdots < k_m \le n} \boldsymbol{A} \begin{pmatrix} 1 & 2 & \dots & m \\ k_1 & k_2 & \dots & k_m \end{pmatrix} \boldsymbol{B} \begin{pmatrix} k_1 & k_2 & \dots & k_m \\ 1 & 2 & \dots & m \end{pmatrix}.$$

Todistus. (Ks. [5], s. 8-10) Koska $\boldsymbol{C} = \boldsymbol{AB}$, niin $[\boldsymbol{C}]_{ij} = \sum_{\alpha=1}^{n} a_{i\alpha} b_{\alpha j}$, missä $[\boldsymbol{A}]_{ij} = a_{ij}$ ja $[\boldsymbol{B}]_{ij} = b_{ij}$. Näin ollen determinantin n-lineaarisuusominaisuuden (ks. [4], s. 212) perusteella

$$\boldsymbol{C} = \sum_{\alpha_1,\dots,\alpha_m=1}^{n} \begin{vmatrix} a_{1\alpha_1} b_{\alpha_1 1} & a_{1\alpha_2} b_{\alpha_2 2} & \cdots & a_{1\alpha_m} b_{\alpha_m m} \\ a_{2\alpha_1} b_{\alpha_1 1} & a_{2\alpha_2} b_{\alpha_2 2} & \cdots & a_{2\alpha_m} b_{\alpha_m m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m\alpha_1} b_{\alpha_1 1} & a_{m\alpha_2} b_{\alpha_2 2} & \cdots & a_{m\alpha_m} b_{\alpha_m m} \end{vmatrix} \tag{3.1}$$

$$= \sum_{\alpha_1,\dots,\alpha_m=1}^{n} \begin{vmatrix} a_{1\alpha_1} & a_{1\alpha_2} & \cdots & a_{1\alpha_m} \\ a_{2\alpha_1} & a_{2\alpha_2} & \cdots & a_{2\alpha_m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m\alpha_1} & a_{m\alpha_2} & \cdots & a_{m\alpha_m} \end{vmatrix} \begin{vmatrix} b_{\alpha_1 1} & 0 & \cdots & 0 \\ 0 & b_{\alpha_2 2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & b_{\alpha_m m} \end{vmatrix} \tag{3.2}$$

$$= \sum_{\alpha_1,\dots,\alpha_m=1}^{n} \boldsymbol{A} \begin{pmatrix} 1 & 2 & \dots & m \\ \alpha_1 & \alpha_2 & \dots & \alpha_m \end{pmatrix} \prod_{i=1}^{m} b_{\alpha_i i}. \tag{3.3}$$

Jos nyt $m > n$, niin lukujen $k_1, k_2, \dots, k_m$ joukossa on aina vähintään kaksi samaa lukua, sillä $1 \le k_i \le n$ jokaisella $i = 1, 2, \dots, m$. Tällöin kaavassa 3.3 esiintyvästä summasta saadaan 0, sillä kaikissa summan minoreissa esiintyvissä matriiseissa on kaksi identtistä riviä (ks. [4], s. 215). Näin ollen vasemman puolen summa on 0. Toisaalta tällöin kaavan 3.3 oikea puoli on itse asiassa tyhjä summa eli 0.

Jos taas $m \le n$, niin riittää tutkia summan ne termit, joissa luvut $\alpha_1, \alpha_2, \dots, \alpha_m$ ovat pareittain erilliset, sillä muuten valintaa vastaavat minorit ovat nollia. Jaetaan seuraavaksi summattavat ryhmiin sen mukaan miten luvut $\alpha_1, \alpha_2, \dots, \alpha_m$ on valittu huomioon ottamatta valintajärjestystä. Huomaa, että kussakin tällaisessa ryhmässä on $m!$ summattavaa, sillä alkiot voidaan järjestää $m!$ eri tavalla.

Olkoot $1 \le k_1 < k_2 < \ldots < k_m \le n$ tällainen lukujen valinta ja olkoon S_m joukon $\{1, 2, \dots, m\}$ permutaatioiden joukko. Nyt

$$\begin{aligned} &\sum_{\sigma \in S_m} \boldsymbol{A} \begin{pmatrix} 1 & 2 & \dots & m \\ k_{\sigma(1)} & k_{\sigma(2)} & \dots & k_{\sigma(m)} \end{pmatrix} \prod_{i=1}^{m} b_{\sigma(k_i) i} \\ &= \sum_{\sigma \in S_m} \operatorname{sgn}(\sigma) \boldsymbol{A} \begin{pmatrix} 1 & 2 & \dots & m \\ k_1 & k_2 & \dots & k_m \end{pmatrix} \prod_{i=1}^{m} b_{k_{\sigma(i)} i} \\ &= \boldsymbol{A} \begin{pmatrix} 1 & 2 & \dots & m \\ k_1 & k_2 & \dots & k_m \end{pmatrix} \sum_{\sigma \in S_m} \operatorname{sgn}(\sigma) \prod_{i=1}^{m} b_{k_{\sigma(i)} i}, \end{aligned}$$

on kaikkien tätä valintaa vastaavien termien summa. Soveltamalla Leibnizin lausetta saadaan edelleen, että

$$\begin{aligned}&\boldsymbol{A}\begin{pmatrix} 1 & 2 & \dots & m \\ k_1 & k_2 & \dots & k_m \end{pmatrix} \sum_{\sigma \in S_m} \operatorname{sgn}(\sigma) \prod_{i=1}^{m} b_{k_{\sigma(i)} i} \\ =&\boldsymbol{A}\begin{pmatrix} 1 & 2 & \dots & m \\ k_1 & k_2 & \dots & k_m \end{pmatrix} \boldsymbol{B}\begin{pmatrix} k_1 & k_2 & \dots & k_m \\ 1 & 2 & \dots & m \end{pmatrix}.\end{aligned}$$

□

3.6 Topologiaa

Luvuissa 4.2 ja 4.3 esitettävät laajennukset konstruoidaan lähtökohtaisesti topologiaa sekä hilateoriaa hyödyntäen. Tässä luvussa esitetään näiden laajennusten konstruointiin tarvittavat topologiset käsitteet. Tämän tutkielman kannalta luvun keskeisimmät käsitteet ovat yhden pisteen kompaktisointi sekä tulotopologia. Luvun tiedot ovat pääosin lähteistä [16], [2] ja [11].

Määritelmä 3.29. (Ks. [2], s. 62) Olkoon X joukko ja olkoon $\mathcal{T} \subseteq \mathcal{P}(X)$. Joukkoperhettä $\mathcal{T}$ sanotaan joukon X *topologiaksi, jos*

(1) $X \in \mathcal{T}$ *ja* $\emptyset \in \mathcal{T}$*,*

(2) $A_i \in \mathcal{T}$ *kaikilla* $i \in \mathbb{Z}_+ \Rightarrow \cup_{i=1}^{\infty} A_i \in \mathcal{T}$*,*

(3) $A_i \in \mathcal{T}$ *kaikilla* $i = 1, 2, 3, \dots, n \Rightarrow \cap_{i=1}^{n} A_i \in \mathcal{T}$*.*

Paria $\langle X, \mathcal{T} \rangle$, missä $\mathcal{T}$ on joukon X topologia, voidaan tällöin kutsua *topologiseksi avaruudeksi.* Mikäli joukon X topologia on asiayhteydestä selvä, voidaan myös puhua lyhyesti topologisesta avaruudesta X tai vain avaruudesta X, jos on selvä, että tarkoitetaan topologista avaruutta.

Määritelmän perusteella voidaan välittömästi nähdä, että joukko $\{\emptyset, X\}$ on aina joukon X topologia. Tätä topologiaa kutsutaan joukon X *indiskreetiksi topologiaksi.* Indiskreetti topologia on suppein mahdollinen joukon X topologia.Kohtuullisen helposti havaitaan myös, että joukko $\mathcal{P}(X)$ on joukon X topologia. Tätä topologiaa kutsutaan vastaavasti joukon X *diskreetiksi topologiaksi* ja tämä on luonnollisesti laajin mahdollinen joukon X topologia. Tässä tutkielmassa sovelletaan lähinnä diskreettejä topologioita. Lisää esimerkkejä erilaisista yksinkertaisista topologioista löytyy lähteestä [2] sivulta 63.

Seuraavaksi määritellään lyhyesti muutamia topologisia peruskäsitteitä, joita tarvitaan tämän luvun määritelmissä ja lauseissa. Topologisen avaruuden alkioita kutsutaan pisteiksi. Topologiaan kuuluvia joukkoja kutsutaan *avoimiksi joukoiksi.* Vastaavasti voidaan sanoa, että joukko on *suljettu*, jos sen komplementti on avoin. Huomaa, että topologiassa joukko voi olla yhtä

aikaa sekä avoin että suljettu. Niitä avoimia joukkoja, jotka sisältävät pisteen a kutsutaan pisteen a *ympäristöiksi*. Joukon A *kosketuspisteellä* tarkoitetaan pistettä, jonka jokainen ympäristö leikkaa joukkoa A. Joukon A kaikkien kosketuspisteiden joukosta käytetään merkintää $\mathrm{cl}(A)$. Tätä joukkoa kutsutaan joukon A *sulkeumaksi*. (Ks. [2], s. 12, 63 ja 68)

Huomautus Diskreetissä topologiassa kaikki joukot ovat sekä avoimia että suljettuja.

Määritelmä 3.30. (Ks. [2], s. 137) Olkoon $\mathcal{T}$ joukon X topologia. Jos jokaisella $a, b \in X$ on olemassa erilliset ympäristöt, niin sanotaan että $\mathcal{T}$ on *Hausdorffin topologia*.

Joukon X osajoukon A *peitteeksi* kutsutaan sellaista joukkoperhettä, jonka alkiot ovat avoimia joukkoja, joiden yhdisteeseen osajoukko A sisältyy. Vastaavasti jos $\mathcal{C}$ ja $\mathcal{G}$ ovat joukon A peitteitä ja $\mathcal{G} \subseteq \mathcal{C}$, niin sanotaan että peite $\mathcal{G}$ on joukon A peitteen $\mathcal{C}$ osapeite (ks. [11], s. 49). Peitteiden avulla voidaan määritellä seuraavana esiteltävä kompaktisuuden käsite.

Määritelmä 3.31. (Ks. [2], s. 137) Olkoon $\mathcal{T}$ joukon X topologia. Jos jokaisella joukon X avoimella peitteellä on olemassa äärellinen osapeite, niin $\mathcal{T}$ on *kompakti topologia*.

Huomautus Jos avaruuden X topologia $\mathcal{T}$ on kompakti tai Hausdorffin topologia, niin usein sanotaan lyhyesti, että avaruus X on kompakti tai että X on Hausdorffin avaruus.

Määritelmä 3.32. (Ks. [2], s. 77) Olkoon $\langle X, \mathcal{T} \rangle$ topologinen avaruus ja olkoon $Y \subset X$. Topologiaa $\mathcal{T}_Y = \{U \cap Y : U \in \mathcal{T}\}$ kutsutaan *topologian $\mathcal{T}$ joukkoon Y indusoimaksi topologiaksi*. Tällöin avaruus Y on avaruuden X *topologinen aliavaruus*.

Koska X on topologinen avaruus, niin topologian $\mathcal{T}$ indusoima topologia on todellakin topologia. Tämä voidaan todistaa suoraan topologian määritelmän avulla käyttäen apuna tietoa siitä, että X on topologinen avaruus. Lisäksi voidaan sanoa lyhyesti joukon Y olevan kompakti, jos tarkoitetaan, että aliavaruus Y on kompakti.

Lause 3.33. *Olkoon $\langle X, \mathcal{T} \rangle$ Hausdorffin avaruus ja olkoot $A, B \subseteq X$ kompakteja joukkoja. Jos $A \cap B = \emptyset$, niin joukoilla A ja B on olemassa erilliset ympäristöt.*

Todistus. Jos $A = \emptyset$ tai $B = \emptyset$, niin väite on triviaali. Voidaan siis olettaa, että $A, B \neq \emptyset$. Oletetaan ensin, että $B = b$. Koska $\mathcal{T}$ on Hausdorffin topologia, voidaan kullekin joukon A alkiolle a valita sellaiset ympäristöt U_a ja V_a, että $a \in U_a$, $b \in V_a$ ja $U_a \cap V_a = \{\infty\}$. Nyt $\cup_{a \in A} U_a$ on joukon A peite, jolla on kompaktisuuden perusteella äärellinen osapeite $\cup_{a \in A'} U_a$. Tällöin $\cup_{a \in A'} U_a$ ja

$\cap_{a\in A'} V_a$ ovat joukkojen A ja b erilliset ympäristöt. Huomaa, että topologian määritelmän 3.29 mukaan avointen joukkojen äärellinen leikkaus ja ääretön yhdiste ovat avoimia.

Olkoon B mielivaltainen kompakti joukko. Soveltamalla yksiön tapausta voidaan valita kullekin $b \in B$ sellaiset erilliset ympäristöt U_b ja V_b, että $A \subseteq U_b$ ja $b \in V_b$. Nyt siis $\cap_{b\in B} V_b$ on joukon B peite. Kompaktisuuden perusteella joukolle B saadaan äärellinen osapeite $\cup_{b\in B'} V_b$. Nyt joukot $\cap_{b\in B'} U_b$ ja $\cup_{b\in B'} V_b$ ovat joukkojen B ja A erilliset ympäristöt. □

Lause 3.34. *Olkoon $\langle X, \mathcal{T}\rangle$ kompakti Hausdorffin avaruus. Joukon $A \subseteq X$ indusoima aliavaruus on kompakti, jos ja vain jos A on suljettu.*

Todistus. Oletetaan ensin, että A on kompakti avaruus. Olkoon $x \in X \setminus A$. Koska yksiö $\{x\}$ on kompakti, niin lauseen 3.33 mukaan joukoilla $\{x\}$ ja A on erilliset ympäristöt U_x ja V_x. Nyt joukko $X \setminus A$ voidaan esittää muodossa $\cup_{x\in X} U_x$, joten $X \setminus A$ on avointen joukkojen yhdisteenä avoin. Siis A on suljettu.

Oletetaan sitten, että A on suljettu. Olkoon $\{U_i : i \in I\}$ mielivaltainen joukon A avoin peite määritelmän 3.32 mukaisessa topologiassa $\mathcal{T}_A$. Nyt topologian $\mathcal{T}_A$ määritelmän perusteella jokaista $i \in I$ kohti on olemassa sellaiset joukot $V_i \in \mathcal{T}$, että $V_i \cap A = U_i$. Nyt $\{V_i : i \in I\} \cup \{X \setminus A\}$ on joukon X avoin peite, jolla on kompaktisuuden perusteella äärellinen osapeite $\{V_i : i \in J\} \cup \{X \setminus A\}$. Nyt $\{U_i : i \in J\}$ on joukon A peitteen $\{U_i : i \in I\}$ äärellinen osapeite. Topologia $\mathcal{T}_A$ on siis kompakti. □

Lause 3.35. *(Ks. [2], s. 246) Olkoon $\langle X, \mathcal{T}\rangle$ Hausdorffin avaruus. Olkoon ∞ jokin alkio, joka ei kuulu joukkoon X. Määritellään seuraavaksi joukossa $X^* = X \cup \{\infty\}$ topologia $\mathcal{T}^* = \mathcal{T} \cup \mathcal{T}_\infty$, missä*

$$\mathcal{T}_\infty = \{U \subseteq X^* : \infty \in U \text{ ja } X \setminus U \text{ on kompakti}\}.$$

Nyt avaruus $\langle X^*, \mathcal{T}^*\rangle$ on kompakti avaruus, jota kutsutaan avaruuden $\langle X, \mathcal{T}\rangle$ yhden pisteen kompaktisoinniksi.

Todistus. Todistetaan ensin, että $\mathcal{T}^*$ on joukon X^* topologia. Nyt $\emptyset \in \mathcal{T}$. Toisaalta $X \setminus X^* = \emptyset$ on triviaalisti kompakti topologiassa $\mathcal{T}$, joten $X^* \in \mathcal{T}_\infty$. Siis $\emptyset, X^* \in \mathcal{T}^*$.

Oletetaan seuraavaksi, että $A_i \in \mathcal{T}^*$ jokaisella $i \in \mathbb{Z}_+$. Jos $\infty \notin \cup_{i\in I} A_i$, niin $A_i \in \mathcal{T}$ jokaisella $i \in \mathbb{Z}_+$. Koska $\mathcal{T}$ on topologia, niin tällöin $\cup_{i\in I} A_i \in \mathcal{T}$ ja edelleen $\cup_{i\in I} A_i \in \mathcal{T}^*$. Jos taas $\infty \in \cup_{i\in I} A_i$, niin $X \setminus A_i$ on suljettu topologiassa $\mathcal{T}$ jokaisella $i \in I$. Tämä johtuu siitä, että jos $\infty \in A_i$, niin $X \setminus A_i$ on kompakti, jolloin $X \setminus A_i$ on suljettu lauseen 3.34 perusteella. Jos $\infty \notin A_i$, niin joukko A_i on avoin topologiassa $\mathcal{T}$, jolloin $X \setminus A_i$ on suljettu. Nyt $X \setminus \cup_{i\in I} A_i = \cap_{i\in I}(X \setminus A_i)$ on suljettujen joukkojen leikkauksena suljettu topologiassa $\mathcal{T}$. Nyt lauseen 3.34 mukaan $X \setminus \cup_{i\in I} A_i$ on kompakti. Siis $\cup_{i\in I} A_i \in \mathcal{T}_\infty$, joten $\cup_{i\in I} A_i \in \mathcal{T}^*$.

Oletetaan, että $A_i \in \mathcal{T}^*$ jokaisella $i = 1, 2, \ldots, n$. Jos $\infty \in \cap_{i=1}^n A_i$, niin $\infty \in A_i$ jokaisella $i = 1, 2, \ldots, n$, jolloin $A_i \in \mathcal{T}_\infty$ jokaisella $i = 1, 2, \ldots, n$. Tällöin joukko $X \setminus A_i$ on kompakti jokaisella $i = 1, 2, \ldots, n$. Edelleen joukko $X \setminus \cap_{i=1}^n A_i = \cup_{i=1}^n (X \setminus A_i)$ on kompaktien joukkojen äärellisenä yhdisteenä kompakti, joten $\cap_{i=1}^n A_i \in \mathcal{T}_\infty$. Jos $\infty \notin \cap_{i=1}^n A_i$, niin on olemassa sellainen $k \in \{1, 2, \ldots, n\}$, että $A_k \in \mathcal{T}$. Topologian $\mathcal{T}^*$ määritelmän perusteella $A_i \cap X \in \mathcal{T}$ jokaisella $i = 1, 2, \ldots, n$, joten koska $\mathcal{T}$ on topologia, niin $\cap_{i=1}^n A_i \in \mathcal{T}$. Näin ollen $\cap_{i \in 1}^n A_i \in \mathcal{T}^*$. Kokoelma $\mathcal{T}^*$ on siis joukon X^* topologia.

Todistetaan vielä, että $\mathcal{T}^*$ on kompakti. Olkoon $\{A_i : i \in I\}$ mielivaltainen joukon X^* avoin peite. Koska $\infty \in \cup_{i \in I} A_i$, niin on olemassa sellainen $k \in I$, että $\infty \in A_k$, eli $A_k \in \mathcal{T}_\infty$. Nyt $X \setminus A_k$ on kompakti joukko, jonka avoimella peitteellä $\{A_i : i \in I, i \neq k\}$ on olemassa kompaktisuuden perusteella äärellinen osapeite $\{A_i : i \in J\}$. Tällöin $\{A_i : i \in J\} \cup \{A_k\}$ on joukon X^* peitteen $\{A_i : i \in I\}$ äärellinen osapeite. Siis topologia $\mathcal{T}^*$ on kompakti. □

Huomautus Mikäli noudatetaan tavanomaista joukko-opillista aksiomatisointia (ZFC aksiomatisointi) on aina olemassa jokin alkio, joka ei kuulu joukkoon X. Tämä johtuu siitä, että ”kaikkien joukkojen joukko” on itse asiassa aito luokka eikä joukko. ”Kaikkien joukkojen joukon” hyväksyminen joukoksi aiheuttaisi ristiriidan erotteluaksiooman kanssa (ks. [10], s. 10).

Määritelmä 3.33. (Ks. [16], s. 121) Olkoon $\mathcal{T}$ joukon X topologia. Jos jokaisella joukon X pisteellä a on olemassa jokin ympäristö U siten, että $\mathrm{cl}(U)$ on kompakti, niin $\langle X, \mathcal{T} \rangle$ on *lokaalisti kompakti topologinen avaruus.*

Lause 3.36. *(Ks. [16], s. 122-123) Olkoon $\langle X^*, \mathcal{T}^* \rangle$ Hausdorffin avaruuden $\langle X, \mathcal{T} \rangle$ yhden pisteen kompaktisointi. Jos $\langle X, \mathcal{T} \rangle$ on lokaalisti kompakti, niin $\langle X^*, \mathcal{T}^* \rangle$ on Hausdorffin avaruus.*

Todistus. Oletetaan, että $\langle X, \mathcal{T} \rangle$ on lokaalisti kompakti Hausdorffin avaruus. Valitaan mielivaltaisesti sellaiset joukon X^* pisteet a ja b, että $a \neq b$. Jos nyt $a, b \in X$, niin topologian $\mathcal{T}$ Hausdorffin ominaisuuden perusteella on olemassa sellaiset erilliset ympäristöt U ja V, että $a \in U$ ja $b \in V$. Oletetaan seuraavaksi, että $a = \infty$ tai $b = \infty$. Yleisyyttä rajoittamatta voidaan olettaa, että $b = \infty$. Nyt $a \in X$, joten topologian $\mathcal{T}$ lokaalin kompaktiuden perusteella on olemassa sellainen pisteen a ympäristö U, että $\mathrm{cl}(U)$ on kompakti joukon X osajoukko. Koska lisäksi $\infty \in X \setminus \mathrm{cl}(U)$, niin topologian $\mathcal{T}^*$ määritelmän perusteella $X \setminus \mathrm{cl}(U)$ on avoin joukko avaruudessa X^*. Nyt U ja $X \setminus \mathrm{cl}(U)$ ovat pisteiden a ja b erilliset ympäristöt. Siis määritelmän 3.30 mukaan X^* on Hausdorffin avaruus. □

Huomautus Voidaan lisäksi todistaa, että Hausdorffin avaruuden kompaktisointi on lokaalisti kompakti, jos ja vain jos kyseinen kompaktisointi on Hausdorffin avaruus (ks. [16], s. 122-123). Emme tutkielmassa kuitenkaan

ryhdy todistamaan tätä suuntaa, sillä lauseen edellä esitetty muotoilu riittää kattamaan tutkielman tarpeet.

Seuraavaksi ryhdytään määrittelemään topologisten avaruuksien karteesiselle tulolle mielekästä topologiaa. Ennen tähän tarkoitukseen soveltuvan *tulotopologian* määrittelemistä on kuitenkin tutustuttava topologian kannan ja esikannan käsitteisiin.

Määritelmä 3.34. (Ks. [16], s. 17) Olkoon $\mathcal{T}$ joukon X topologia. Olkoon $\mathcal{B} \subseteq \mathcal{T}$. Jos jokainen joukon $\mathcal{T}$ alkio voidaan esittää yhdisteenä joukon $\mathcal{B}$ alkioista, niin sanotaan että $\mathcal{B}$ on *topologian $\mathcal{T}$ kanta.*

Määritelmä 3.35. (Ks. [16], s. 21) Olkoon $\langle X, \mathcal{T} \rangle$ topologinen avaruus ja olkoon $\mathcal{A} \in \mathcal{P}(X)$. Jos joukon $\mathcal{A}$ jäsenten äärelliset leikkaukset muodostavat topologian $\mathcal{T}$ kannan, niin sanotaan että $\mathcal{A}$ on *topologian $\mathcal{T}$ esikanta.*

Jos jokin topologian $\mathcal{T}$ kanta $\mathcal{B}$ tunnetaan, niin voidaan sanoa, että $\mathcal{B}$ virittää topologian $\mathcal{T}$ tai topologisen avaruuden $\langle X, \mathcal{T} \rangle$. Vastaavaa terminologiaa voidaan käyttää myös esikantojen yhteydessä. Huomaa, että topologian kanta tai esikanta virittää aina yksikäsitteisen topologian, mutta yksittäisellä topologialla voi toki olla useita erilaisia virittäviä kantoja tai esikantoja.

Lause 3.37. *(Ks. [16], s. 18) Olkoon X joukko, $\emptyset \neq A \subseteq X$ ja $\mathcal{B} \subseteq \mathcal{P}(X)$. Nyt A voidaan lausua yhdisteenä joukkoperheen $\mathcal{B}$ jäsenistä, jos ja vain jos jokaisella $x \in A$ on olemassa sellainen $B \in \mathcal{B}$, että $x \in B \subseteq A$.*

Todistus. Oletetaan ensin, että A voidaan lausua yhdisteenä joukkoperheen $\mathcal{B}$ jäsenistä. Jos nyt $x \in A$, niin yhdisteen määritelmän perusteella on olemassa sellainen $B \in \mathcal{B}$, että $x \in B$.

Oletetaan sitten, että jokaisella $x \in A$ on olemassa sellainen $B \in \mathcal{B}$, että $x \in B \subseteq A$. Nyt jokaista $x \in A$ kohti voidaan valita sellainen $B_x \in \mathcal{B}$, että $x \in B_x \subseteq A$. Nyt saadaan $\cup_{x \in A} B_x = A$, joten A voidaan lausua yhdisteenä joukkoperheen $\mathcal{B}$ jäsenistä. □

Lause 3.38. *(Vrt. [16], s. 19-20) Olkoon X joukko ja $\mathcal{B} \subseteq \mathcal{P}(X)$. Jos $\mathcal{B}$ on joukon X peite ja kaikilla $B_1, B_2, \ldots, B_n \in \mathcal{B}$ joko $\cap_{i=1}^n B_i = \emptyset$ tai $\cap_{i=1}^n B_i \in \mathcal{B}$, niin $\mathcal{B}$ on jonkin joukon X topologian kanta.*

Todistus. Oletetaan, että $\mathcal{B}$ on joukon X peite ja että jos $B_1, B_2, \ldots, B_n \in \mathcal{B}$, niin joko $\cap_{i=1}^n B_i = \emptyset$ tai $\cap_{i=1}^n B_i \in \mathcal{B}$.

Merkitään $\mathcal{B} = \{C_i : i \in I\}$, missä I on joukko indeksejä. Merkitään joukkoperheen $\mathcal{B}$ joukkojen yhdisteiden virittämää joukkoperhettä symbolilla $\mathcal{T}$. Siis $\mathcal{T} = \{\cup_{i \in J} C_i : J \subseteq I\}$. On siis todistettava, että $\mathcal{T}$ on joukon X topologia.

Jos $J = \emptyset$, niin $\cup_{i \in J} C_i = \emptyset$, joten $\emptyset \in \mathcal{T}$. Koska $\mathcal{B}$ on joukon X peite, niin $\cup_{i \in I} C_i = X$, joten myös $X \in \mathcal{T}$.

Olkoon $U_i \in \mathcal{T}$ jokaisella $i \in \mathbb{Z}_+$. Koska jokainen joukoista U_i on muotoa $\cup_{j \in J_i} C_j$, missä $J_i \subseteq I$, niin voidaan kirjoittaa $\cup_{i=1}^{\infty} U_i = \cup_{i=1}^{\infty} (\cup_{j \in J_i} C_j)$.

Merkitään $\cup_{i=1}^{\infty} J_i = J$. Koska nyt $J \subset I$, niin edelleen $\cup_{i=1}^{\infty} U_i = \cup_{j \in J} C_j$. Siis $\cup_{i=1}^{\infty} U_i \in \mathcal{T}$.

Olkoon seuraavaksi $U_i \in \mathcal{T}$ jokaisella $i = 1, 2, \ldots, n$. Oletetaan lisäksi, että $x \in \cap_{i=1}^{n} U_i$. Nyt lauseen 3.37 mukaan jokaisella $i = 1, 2, \ldots, n$ on olemassa sellainen C_{j_i}, että $x \in C_{j_i} \subseteq U_i$. Nyt oletuksen perusteella $\cap_{i=1}^{n} C_{j_i} \in \mathcal{B}$, sillä $\cap_{i=1}^{n} C_{j_i} \neq \emptyset$. Saadaan $x \in \cap_{i=1}^{n} C_{j_i} \subseteq \cap_{i=1}^{n} U_i$, joten lauseen 3.37 mukaan $\cap_{i=1}^{n} U_i$ voidaan esittää yhdisteenä joukon $\mathcal{B}$ alkioita. Näin ollen $\mathcal{B}$ on joukon X topologian $\mathcal{T}$ kanta. □

Lause 3.39. *(Ks. [16], s. 22) Olkoon X mielivaltainen joukko. Jos $\mathcal{A}$ on joukon X peite, niin $\mathcal{A}$ on jonkin joukon X topologian esikanta.*

Todistus. Olkoon $\mathcal{A}$ joukon X peite. Merkitään $\mathcal{A} = \{A_i : i \in I\}$. Olkoon joukkoperhe $\mathcal{B}$ joukon $\mathcal{A}$ äärellisten leikkausten kokoelma. Koska yhden alkion leikkaukset $\cap_{j \in \{i\}} A_j = A_i$ ovat äärellisiä, niin $A_i \in \mathcal{B}$ jokaisella $i \in I$. Koska $\mathcal{A}$ on joukon X peite, niin $X = \cup_{i \in I} A_i \subseteq \cup \mathcal{B}$. Joukkoperhe $\mathcal{B}$ on siis joukon X peite.

Olkoot $B_1, B_2, \ldots, B_n \in \mathcal{B}$. Nyt jokaisella $i = 1, 2, \ldots, n$ on olemassa sellainen äärellinen joukko $J_i \subseteq I$, että $B_i = \cap_{j \in J_i} A_j$ ja $A_j \in \mathcal{A}$. Nyt leikkaus $\cap_{i \in I}(\cap_{j \in J_i} B_j)$ voidaan kirjoittaa muodossa $\cap_{i \in J} B_i$, missä $J = \cup_{i=1}^{n} J_i$ on äärellisten joukkojen äärellisenä yhdisteenä äärellinen. On siis todistettu, että $\cap_{i=1}^{n} B_1 \in \mathcal{B}$. Lauseen 3.38 mukaan $\mathcal{B}$ on joukon X jonkin topologian kanta. □

Määritelmä 3.36. Olkoon $I \neq \emptyset$ joukko indeksejä ja olkoon $\mathcal{T}_i$ joukon Y_i topologia jokaisella $i \in I$. Oletetaan vielä, että $f_i : X \to Y_i$ on kuvaus jokaisella $i \in I$. Määritellään $\mathcal{A} = \{f_i^{-1} V : V \in \mathcal{T}_i, i \in I\}$. Nyt esikannan $\mathcal{A}$ virittämää joukon X topologiaa kutsutaan *kuvausperheen* $\{f_i : i \in I\}$ *indusoimaksi joukon X topologiaksi.*

On kohtuullisen helppo havaita, että koska edellisessä määritelmässä f_i on kuvaus jokaisella $i \in I$, niin jokaisella $x \in X$ on olemassa sellainen $y \in Y_i$, että $f_i(x) = y$. Näin ollen määritelmässä määritelty joukkoperhe $\mathcal{A}$ on todellakin joukon X peite ja täten lauseen 3.39 mukaan joukon X jonkin topologian esikanta.

Määritelmä 3.37. (Ks. [16], s. 45) Olkoon I epätyhjä joukko indeksejä ja olkoon $\mathcal{T}_i$ joukon Y_i topologia jokaisella $i \in I$. Määritellään seuraavaksi kuvaus $\mathrm{pr}_i : \prod_{i \in I} Y_i \to Y_i$ karteesisen tulon projektiona joukkoon Y_i. Kuvaus pr_i liittää kuhunkin karteesisen tulon alkioon kyseisen alkion i-koordinaatin, siis $\mathrm{pr}_i((y_j)_{j \in I}) = y_i$. Nyt kuvausperheen $\{\mathrm{pr}_i : i \in I\}$ indusoimaa karteesisen tulon $\prod_{i \in I} Y_i$ topologiaa kutsutaan topologioiden $\mathcal{T}_i$, $i \in I$, *tulotopologiaksi.*

Seuraavaksi määritellään topologisen kuvauksen jatkuvuuden käsite. Tämä olisi ollut kenties mielekästä jopa ennen tulotopologian määrittelemistä,

sillä eräs tulotopologian keskeinen ominaisuus on, että karteesisen tulon projektiot ovat jatkuvia tulotopologian suhteen (ks. [11], s. 90). Jatkuvuutta hyödynnetään myöhemmin topologisen puoliryhmän määritelmässä. Näitä tietoja tarvitaan tutkielman luvun 4.3 loppupuolella esitettävien lauseiden todistuksissa.

Määritelmä 3.38. (Ks. [2], s. 79) Olkoot X ja Y topologisia avaruuksia ja olkoon $f : X \to Y$ kuvaus. Jos avaruuden Y jokaisen avoimen joukon A alkukuva $f^{-1}(A)$ on avoin avaruudessa X, niin kuvaus f on *jatkuva*.

Lause 3.40. *(Ks. [2], s. 79) Olkoot X, Y ja Z topologisia avaruuksia ja olkoot $f : X \to Y$ ja $g : Y \to Z$ jatkuvia kuvauksia. Tällöin $g \circ f : X \to Z$ on jatkuva kuvaus.*

Todistus. Valitaan mielivaltainen avaruuden Z avoin joukko C. Koska g on jatkuva, niin $g^{-1}(C)$ on avoin avaruudessa Y. Edelleen kuvauksen f jatkuvuuden perusteella $f^{-1}(g^{-1}(C)) = (g \circ f)^{-1}(C)$ on avoin avaruudessa X. □

Lause 3.41. *(Ks. [2], s. 102) Olkoon I indeksijoukko ja olkoot X_i ja Y_i topologisia avaruuksia jokaisella $i \in I$. Olkoon $f_i : X_i \to Y_i$ kuvaus jokaisella $i \in I$. Määritellään kuvaus*

$$\prod_{i \in I} f_i : \prod_{i \in I} X_i \to \prod_{i \in I} Y_i$$

säännöllä $\prod_{i \in I} f_i((x_j)_{j \in I}) = (f_i(x_i))_{i \in I}$. Jos kuvaus f_i on jatkuva jokaisella $i \in I$, niin myös kuvaus $\prod_{i \in I} f_i$ on jatkuva.

Todistus. Valitaan mielivaltainen avaruuden $\prod_{i \in I} Y_i$ avoin joukko $(A_i)_{i \in I}$. Tulotopologian määritelmän perusteella joukko A_i on avoin avaruudessa Y_i jokaisella $i \in I$.

Joukon $(A_i)_{i \in I}$ alkukuvien joukko $(\prod_{i \in I} f_i)^{-1}(A_i)_{i \in I}$ voidaan funktion $\prod_{i \in I} f_i$ määritelmän perusteella esittää muodossa $(f_i^{-1}(A_i))_{i \in I}$. Koska kuvaukset f_i ovat oletuksen perusteella jatkuvia jokaisella $i \in I$, niin joukko $f_i^{-1}(A_i)$ on avoin avaruudessa X_i jokaisella $i \in I$. Tällöin tulotopologian määritelmän perusteella joukko $(f_i^{-1}(A_i))_{i \in I}$ on avoin avaruudessa $\prod_{i \in I} X_i$. □

Määritelmä 3.39. (Ks. [14]) Olkoon $A \neq \emptyset$ topologinen avaruus ja olkoon $\star$ kuvaus joukosta $A \times A$ joukkoon A. Struktuuria $\langle A, \star \rangle$ kutsutaan *topologiseksi puoliryhmäksi*, jos $\langle A, \star \rangle$ on puoliryhmä ja binäärinen laskutoimitus $\star$ on jatkuva.

Huomautus Topologisen puoliryhmän määritelmässä joukon $A \times A$ topologialla tarkoitetaan tulotopologiaa.

Seuraavaksi todistetaan yleisen topologian kuuluisimpiin lauseisiin kuuluva Tychonoffin lause. Tämän venäläismatemaatikko Andrey Tychonoffin

mukaan nimetyn lauseen on itse asiassa todettu olevan eräs valinta-aksiooman muotoilu. Ennen Tychonoffin lausetta esitetään vielä Alexanderin lauseena tunnettu lause, jota hyödyntäen Tychonoffin lause voidaan todistaa kohtuullisen helposti. Alexanderin lauseen todistuksessa tarvitaan valinta-aksioomaa, jota hyödynnetään todistuksessa Zornin lemman muodossa. Mikäli valinta-aksiooma, Zornin lemma sekä näiden yhtäpitävyys kuulostavat vierailta käsitteiltä, on suositeltavaa tutustua lähteen [10] sivuihin 64-65 ennen seuraavien lauseiden todistusten läpikäyntiä.

Lause 3.42. *(Ks. [11], s. 139) Olkoon $\langle X, \mathcal{T} \rangle$ esikannan $\mathcal{B}$ virittämä topologia. Jos jokaisella joukon X esikantapeitteellä $\mathcal{S} \subseteq \mathcal{B}$ on äärellinen osapeite, niin $\langle X, \mathcal{T} \rangle$ on kompakti topologia.*

Todistus. Olkoon $\mathcal{B}$ mielivaltainen topologian $\mathcal{T}$ esikanta. Oletetaan, että jokaisella esikannan $\mathcal{B}$ alkioista koostuvalla joukon X peitteellä on äärellinen osapeite. Tehdään seuraavaksi vastaoletus, että $\mathcal{T}$ ei ole kuitenkaan kompakti topologia. Joukolla X on siis olemassa peite, jolla ei ole olemassa äärellistä osapeitettä. Olkoon $\mathcal{M}$ kaikkien tällaisten peitteiden joukko. Olkoon $\mathcal{K}$ mielivaltainen joukon $\mathcal{M}$ alkioista koostuva ketju.

Jokaisella joukon X peitteellä $\mathcal{C} \in \mathcal{K}$ pätee $\mathcal{C} \subseteq \cup\mathcal{K}$. Näin ollen $\cup\mathcal{K}$ on ketjun $\mathcal{K}$ yläraja. Lisäksi nähdään, että tällöin $\cup\mathcal{K}$ on joukon X peite, sillä se sisältää ainakin yhden joukon X peitteen. Todistetaan vielä, että peitteellä $\cup\mathcal{K}$ ei ole olemassa äärellistä osapeitettä. Tehdään vastaoletus, että peitteellä $\cup\mathcal{K}$ on olemassa äärellinen osapeite $\mathcal{C}$. Koska $\mathcal{K}$ on ketju ja $\mathcal{C}$ äärellinen, niin on olemassa sellainen $\mathcal{C}' \in \mathcal{K}$, että $\mathcal{C} \subseteq \mathcal{C}'$. Tällöin peitteellä $\mathcal{C}'$ on olemassa äärellinen osapeite, mistä seuraa ristiriita. Näin ollen $\cup\mathcal{K} \in \mathcal{M}$.

Zornin lemman perusteella voidaan siis sanoa, että on olemassa maksimaalinen peite $\mathcal{C}_M \in \mathcal{M}$ jolla ei ole olemassa äärellistä osapeitettä. Jos siis $V \in \mathcal{T}$ ja $V \notin \mathcal{C}_M$, niin peitteellä $\mathcal{C}_M \cup \{V\}$ on olemassa äärellinen osapeite.

Nyt joukko $\mathcal{C}_M \cap \mathcal{B}$ ei voi olla joukon X esikantapeite, sillä tällöin esikantapeitteellä $\mathcal{C}_M \cap \mathcal{B}$ olisi äärellinen osapeite, joka olisi myös peitteen $\mathcal{C}_M$ äärellinen osapeite. On siis olemassa sellainen $x \in X$, että $x \notin \cup(\mathcal{B} \cap \mathcal{C}_M)$. Koska $\mathcal{C}_M$ on joukon X peite, niin on olemassa sellainen $C \in \mathcal{C}_M$, että $x \in C$. Koska $\mathcal{B}$ on esikanta, niin on olemassa sellaiset joukot $B_1, B_2, \ldots, B_n \in \mathcal{B}$, että $x \in \cap_{i=1}^{n} B_i \subseteq C$.

Koska alkio x valittiin joukon $\cup(\mathcal{B} \cap \mathcal{C}_M)$ ulkupuolelta, niin $B_i \notin \mathcal{C}_M$ jokaisella $i = 1, 2, \ldots, n$. Peitteen $\mathcal{C}_M$ maksimaalisuuden perusteella peitteellä $\mathcal{C}_M \cup \{B_i\}$ on tällöin olemassa äärellinen osapeite jokaisella $i = 1, 2, \ldots, n$. Kyseiset osapeitteet voidaan kirjoittaa muodossa $\mathcal{C}_i \cup \{B_i\}$. Nyt $\cup_{i=1}^{n} \mathcal{C}_i \cup \{C\}$ on joukon X peitteen $\mathcal{C}_M$ äärellinen osapeite, joten vastaoletus on väärä. Avaruus X on kompakti. □

Lause 3.43. *(Ks. [11], s. 143) Olkoon I indeksijoukko ja $\mathcal{T}_i$ joukon Y_i topologia jokaisella $i \in I$. Tällöin $X = \prod_{i \in I} Y_i$ on kompakti avaruus, jos ja vain jos Y_i on kompakti avaruus jokaisella $i \in I$.*

Todistus. Oletetaan ensin, että X on kompakti avaruus. Valitaan mielivaltainen $i \in I$. Olkoon $\mathcal{C}_i$ mielivaltainen joukon Y_i peite. Olkoon $\mathcal{C}_j = \{Y_j\}$, kun $j \neq i$. Nyt $\prod_{i\in I} \mathcal{C}_i$ on joukon $\prod_{i\in I} Y_i$ peite, joten sillä on olemassa äärellinen osapeite $\mathcal{C}' = \{U_1, U_2, \ldots, U_n\}$. Nyt $\{\mathrm{pr}_i(U_1), \mathrm{pr}_i(U_2), \ldots, \mathrm{pr}_i(U_n)\}$ on joukon Y_i peitteen $\mathcal{C}$ äärellinen osapeite. Avaruus Y_i on siis kompakti.

Oletetaan sitten, että Y_i on kompakti avaruus jokaisella $i \in I$. Todistetaan lauseen 3.42 avulla, että X on kompakti avaruus. Tulotopologian määritelmän mukaan kokoelma $\mathcal{S} = \{\mathrm{pr}_i^{-1}(U) : i \in I, U \in \mathcal{T}_i\}$ on avaruuden X esikanta. Olkoon $\mathcal{A}$ sellainen kokoelma esikannan $\mathcal{S}$ alkioita, että mikään joukon $\mathcal{A}$ äärellinen osajoukko ei peitä joukkoa X. Olkoon $\mathcal{A}$ joukon $\mathcal{S}$ äärellinen osajoukko. Määritellään jokaisella $i \in I$ joukko $\mathcal{B}_i = \{U \in \mathcal{T}_i : \mathrm{pr}_i^{-1}(U) \in \mathcal{A}\}$.

Koska mikään joukon $\mathcal{A}$ äärellinen osajoukko ei peitä joukkoa X, niin on olemassa sellainen $j \in I$, että mikään joukon $\mathcal{B}_j$ äärellinen osajoukko ei peitä joukkoa Y_j. Tällöin topologian $\mathcal{T}_j$ kompaktisuuden perusteella $\mathcal{B}_j$ ei ole joukon Y_j peite, joten on olemassa sellainen piste y_j, että $y_j \in X_j \setminus U$ jokaisella $U \in \mathcal{B}_j$. Nyt piste, jonka j-koordinaatti on y_j ei kuulu mihinkään joukon $\mathcal{A}$ alkioon, joten $\mathcal{A}$ ei ole joukon X peite.

Nyt on todistettu, että joukon X tulotopologian esikantapeitteellä ei ole äärellistä osapeitettä. Joukon X tulotopologia on siis lauseen 3.42 perusteella kompakti. □

Lause 3.44. *(Ks. [11], s. 92) Olkoon I indeksijoukko ja $\mathcal{T}_i$ joukon Y_i topologia jokaisella $i \in I$. Jos topologia $\mathcal{T}_i$ on Hausdorffin topologia jokaisella $i \in I$, niin tulotopologia $\prod_{i\in I} Y_i$ on Hausdorffin topologia.*

Todistus. Olkoot x ja y karteesisen tulon $\prod_{i\in I} Y_i$ pisteitä. Jos nyt $x \neq y$, niin on olemassa jokin $i \in I$ siten, että $x_i \neq y_i$, missä merkintä x_i tarkoittaa pisteen x i-koordinaattia. Koska avaruus Y_i on Hausdorffin avaruus, niin pisteillä x_i ja y_i on olemassa erilliset ympäristöt U ja V avaruudessa Y_i. Tulotopologiassa on siis olemassa joukot $\mathrm{pr}_i^{-1}(U)$ ja $\mathrm{pr}_i^{-1}(V)$, jotka ovat pisteiden x ja y erilliset ympäristöt. □

4 Laajennukset

4.1 Pseudo-PYUM

Määritelmä 4.1. Olkoot $m, n \in \mathbb{Z}_+$. Määritellään

$$[m, n]^* = \frac{mn}{(m, n)_{\oplus\oplus}}.$$

Lukua $[m, n]^*$ kutsutaan lukujen m ja n pseudo-PYUM:ksi.

Puheessa pseudo-PYUM:sta käytetään yleensä nimitystä *pienin yhteinen pseudo-unitaarinen monikerta*. Näin määriteltäessä luku $[m, n]^*$ on olemassa

kaikilla $m, n \in \mathbb{Z}_+$, joten pienimmän yhteisen unitaarimonikerran puuttumisesta aiheutuvat ongelmat voidaan ratkaista hyvin suoraviivaisesti käyttämällä pienintä yhteistä pseudo-unitaarista monikertaa tavanomaisen pienimmän yhteisen unitaarimonikerran sijaan.

Lause 4.1. *(Ks. [9], s. 4) Olkoot $m, n \in \mathbb{Z}_+$. Jos $[m, n]_{\oplus\oplus}$ on olemassa, niin $[m, n]^* = [m, n]_{\oplus\oplus}$.*

Todistus. Olkoot $m, n \in \mathbb{Z}_+$. Oletetaan, että $[m, n]_{\oplus\oplus}$ on olemassa. Olkoon $m = \prod_{p\in\mathbb{P}} p^{m(p)}$ ja $n = \prod_{p\in\mathbb{P}} p^{n(p)}$. Nähdään, että jokaisella alkuluvulla p on oltava $m(p) = 0$, $n(p) = 0$ tai $m(p) = n(p)$, sillä muuten pienintä yhteistä unitaarimonikertaa ei voi olla olemassa. Soveltamalla lausetta 3.5 saadaan $(m, n)_{\oplus\oplus} = \prod_{p\in\mathbb{P}} p^{\rho(m(p),n(p))}$, missä $\rho(m(p), n(p)) = m(p)$, jos $m(p) = n(p)$ ja $\rho(m(p), n(p)) = 0$ muulloin. Nyt

$$[m, n]^* = \frac{mn}{(m, n)_{\oplus\oplus}} = \prod_{p\in\mathbb{P}} p^{m(p)+n(p)-\rho(m(p),n(p))},$$

missä $m(p) + n(p) - \rho(m(p), n(p)) = m(p)$, jos $m(p) = n(p)$ tai $n(p) = 0$ ja $m(p) + n(p) - \rho(m(p), n(p)) = n(p)$, jos $m(p) = 0$. Nyt lauseen 3.3 mukaan $m \parallel [m, n]^*$ ja $n \parallel [m, n]^*$. Olkoon $d \in \mathbb{Z}_+$ sellainen, että $m \parallel d$ ja $n \parallel d$. Soveltamalla lausetta 3.3 saadaan

$$d = \prod_{p\in\mathbb{P}} p^{d(p)},$$

missä $d(p) = m(p)$, jos $m(p) \neq n(p) = 0$ tai $m(p) = n(p)$ ja $d(p) = n(p)$, jos $n(p) \neq m(p) = 0$. Muulloin $d(p) \in \mathbb{Z}_+$. Tällöin lauseen 3.3 mukaan $[m, n]^* \parallel d$. On siis todistettu, että $[m, n]^* = [m, n]_{\oplus\oplus}$. □

4.2 ∞-laajennettu PYUM

Olkoon $\mathcal{T}$ joukon $\mathbb{Z}_+$ diskreetti topologia. Määritellään joukon $\mathbb{Z}_+$ yksikköjen avulla joukon $\mathbb{Z}_+$ peite $\mathcal{C} = \{\{n\} | n \in \mathbb{Z}_+\}$. Koska peite $\mathcal{C}$ on ääretön, eikä sillä selvästikään ole äärellistä osapeitettä, niin topologia $\mathcal{T}$ ei ole kompakti. Toisaalta jokaisella $m, n \in \mathbb{Z}_+$ on olemassa topologiassa $\mathcal{T}$ erilliset ympäristöt, esimerkiksi $\{m\}$ ja $\{n\}$, joten $\mathcal{T}$ on Hausdorffin topologia. Lisäksi voidaan todeta, että koska jokaista pistettä a kohti on olemassa avoin joukko $A = \{a\}$, jonka sulkeuma $\mathrm{cl}(A) = \{a\}$ on kompakti, niin avaruus $\mathbb{Z}_+$ on lokaalisti kompakti.

Nyt joukolle $\mathbb{Z}_+^\infty = \mathbb{Z}_+ \cup \{\infty\}$ saadaan konstruoitua yhden pisteen kompaktisoinnin avulla mielekäs kompakti topologia, joka on lauseen 3.36 perusteella vieläpä Hausdorffin topologia. Mikäli topologian konstruoiminen joukolle $\mathbb{Z}_+^\infty$ ei olisi lainkaan mielekästä, voitaisiin yhtä hyvin tyytyä hieman yksinkertaistaen toteamaan, että jokaisella $x \in \mathbb{Z}_+^\infty$ pätee $x \parallel \infty$. Ismo Korkee soveltaa mainittua lähestymistapaa artikkelissa *A note on meet and*

join matrices and their special cases GCUD and LCUM matrices (ks. [12], s. 99-100). Tässä luvussa esitettävää topologista menetelmää hyödynnetään kuitenkin myös luvussa 4.3, joten on perusteltua esittää tarvittavat konstruktiot esimerkinomaisesti jo tässä yhteydessä. Esitettävät topologiset tarkastelut myös osoittavat, että muodostettu topologia $\langle \mathbb{Z}_+^\infty, \mathcal{T}^\infty \rangle$ on itse asiassa kompakti, mistä on merkittävää hyötyä tarkasteltaessa kyseistä struktuuria topologisesti.

Määritelmä 4.2. (Vrt. [12], s. 99) Määritellään kompakti topologinen avaruus $\langle \mathbb{Z}_+^\infty, \mathcal{T}^\infty \rangle$ Hausdorffin avaruuden $\langle \mathbb{Z}_+, \mathcal{T} \rangle$ yhden pisteen kompaktisointina.

Määritelmä 4.3. (Ks. [12], s. 99) Määritellään relaatio $\|^\infty$ joukossa $\mathbb{Z}_+^\infty$ siten, että $x \|^\infty y$ jos $x \| y$ tai $y = \infty$, kun $x, y \in \mathbb{Z}_+^\infty$.

Huomautus Relaation $\|$ ominaisuuksien tutkiminen joukossa $\mathbb{Z}_+^\infty$ ei ole kovinkaan mielekästä. Jatkossa relaatiosta $\|^\infty$ käytetäänkin joukossa $\mathbb{Z}_+^\infty$ yksinkertaisesti merkintää $\|$, kun sekaantumisen vaaraa ei ole.

Lause 4.2. *(Ks. [12], s. 99) Struktuuri $\langle \mathbb{Z}_+^\infty, \| \rangle$ on hila.*

Todistus. Todistetaan ensin, että relaatio $\|$ on osittainen järjestys joukossa $\mathbb{Z}_+^\infty$. Olkoot $x, y, z \in \mathbb{Z}_+^\infty$. Lauseessa 3.7 on todistettu refleksiivisyys, antisymmetrisyys ja transitiivisuus joukossa $\mathbb{Z}_+$, joten väitteen todistamiseksi joukossa $\mathbb{Z}_+^\infty$ riittää tutkia tapaukset $x = \infty, y = \infty$ tai $z = \infty$. Määritelmän perusteella nähdään suoraan, että refleksiivisyys pätee, sillä $x \| x$, jos $x = \infty$.

Oletetaan seuraavaksi, että $x \| y$ ja $y \| x$. Jos nyt $x = \infty$, niin $\infty \| y$. Tällöin on oltava $y = \infty$, joten $x = y$. Vastaavasti voidaan käsitellä tapaus $y = \infty$. Siis myös antisymmetrisyys on voimassa.

Transitiivisuuden todistamiseksi oletetaan ensin, että $x \| y$ ja $y \| z$. Jos nyt $z = \infty$, niin nähdään suoraan, että $x \| z$. Jos taas $x = \infty$ tai $y = \infty$, niin on oltava $z = \infty$, jolloin $x \| z$. Näin ollen $\langle \mathbb{Z}_+^\infty, \| \rangle$ on osittain järjestetty joukko.

Todistetaan seuraavaksi, että infimum on aina olemassa. Oletetaan, että $x, y \in \mathbb{Z}_+$. Tällöin $(x, y)_{\oplus\oplus} \| x$ ja $(x, y)_{\oplus\oplus} \| y$. Koska nyt suurimman yhteisen unitaaritekijän määritelmän perusteella jokaisella $z \in \mathbb{Z}_+$, jolla $z \| x$ ja $z \| y$ pätee, että $z \| (x, y)_{\oplus\oplus}$ ja lisäksi $\infty \nparallel x$, niin $x \wedge y = (x, y)_{\oplus\oplus}$.

Oletetaan sitten, että $x = \infty$ tai $y = \infty$. Yleisyyttä rajoittamatta voimme olettaa, että $x = \infty$. Tällöin $y \| x$, joten lauseen 3.1 mukaan $x \wedge y = y$. Lukujen x ja y infimum on siis aina olemassa.

Oletetaan supremumin olemassaolon todistuksessa ensin, että $x, y \in \mathbb{Z}_+$ ja $[x, y]_{\oplus\oplus}$ on olemassa. Tällöin $x \| [x, y]_{\oplus\oplus}$ ja $y \| [x, y]_{\oplus\oplus}$. Koska pienimmän yhteisen unitaarimonikerran määritelmän mukaan jokaisella $z \in \mathbb{Z}$, jolla $x \| z$ ja $y \| z$ pätee $[x, y]_{\oplus\oplus} \| z$ ja lisäksi $[x, y]_{\oplus\oplus} \| \infty$, niin $x \vee y = [x, y]_{\oplus\oplus}$.

Jos taas $x, y \in \mathbb{Z}_+$, mutta $[x, y]_{\oplus\oplus}$ ei ole olemassa, niin luvuilla x ja y ei voi olla lainkaan yhteisiä unitaarimonikertoja positiivisten kokonaislukujen joukossa. Tämä havaittiin lauseen 3.9 todistuksessa. Näin ollen ∞ on ainoa alkio siten, että $x \parallel \infty$ ja $y \parallel \infty$, joten $x \vee y = \infty$.

Oletetaan lopuksi, että $x = \infty$ tai $y = \infty$. Voimme jälleen yleisyyttä rajoittamatta olettaa, että $x = \infty$. Nyt $y \parallel x$, joten lauseen 3.1 perusteella $x \vee y = x$. Lukujen x ja y supremum on siis aina olemassa. Struktuuri $\langle \mathbb{Z}_+^\infty, \| \rangle$ on siis hila.

□

Määritelmä 4.4. (Ks. [12], s. 99) Olkoot $m, n \in \mathbb{Z}_+^\infty$. Määritellään lukujen m ja n *∞-laajennettu PYUM* eli lyhyesti $[m, n]_\infty^*$ siten, että

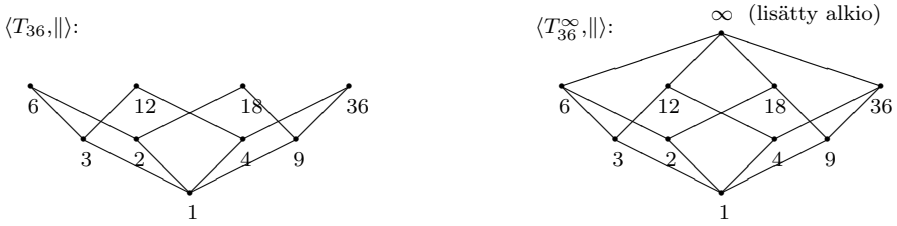
$$[m, n]_\infty^* = m \vee n,$$

missä $m \vee n$ on lukujen m ja n supremum hilassa $\langle \mathbb{Z}_+^\infty, \| \rangle$.

Huomautus Lauseen 4.2 todistuksessa havaittiin, että jos $[m, n]_{\oplus\oplus}$ on olemassa, niin $[m, n]_\infty^* = [m, n]_{\oplus\oplus}$. Samassa todistuksessa havaittiin myös, että mikäli $[m, n]_{\oplus\oplus}$ ei ole olemassa, niin $[m, n]_\infty^* = \infty$.

Seuraavassa kuviossa esitetään vastaava laajennus osittaiselle järjestykselle $\langle T_{36}, \| \rangle$. Huomaa, että meet-puolihilassa $\langle T_{36}, \| \rangle$ esimerkiksi luvuilla 2 ja 4 ei voi olla pienintä yhteistä unitaarimonikertaa, sillä näillä luvuilla ei ole yhteisiä unitaarimonikertoja. Laajennuksessa sen sijaan $[2, 4]_\infty^* = \infty$.

Kuva 3: Joukon T_{36} laajennus



4.3 p^∞-laajennettu PYUM

Tässä luvussa esiteltävä p^∞-laajennettu PYUM on aikaansaatu edellisen laajennuksen periaatetta hiomalla. Tarvittavissa konstruktioissa pyritään noudattamaan pääosin samoja askeleita kuin luvun 4.2 konstruktiossa. Käsite p^∞-laajennettu PYUM esitellään tämän tutkielman lähdeartikkelissa [9] ensimmäistä kertaa kirjallisuudessa.

Olkoon p alkuluku. Merkitään $U_p = \{p^0, p^1, p^2, ...\} = \{p^a : a = 0, 1, 2, ...\}$. Koska nyt $U_p \subseteq \mathbb{Z}_+$, niin lauseen 3.7 perusteella relaatio $\parallel$ on osittainjärjestys joukossa U_p. Lisäksi tällöin $(p^a, p^b)_{\oplus\oplus} \in U_p$ kaikilla luvuilla $a, b \in \{0, 1, 2, ...\}$,

sillä $(p^a, p^b)_{\oplus\oplus} = 1 = p^0$, jos $a \neq b$ ja p^a jos $a = b$. Pienin yhteinen unitaarimonikerta $[p^a, p^b]_{\oplus\oplus}$ ei kuitenkaan ole määritelty, kun $a \neq b$ ja $a, b > 0$. Tämä voidaan todeta esimerkiksi lauseen 3.9 avulla. Struktuuri $\langle U_p, \| \rangle$ on siis meet-semihila, mutta ei kuitenkaan hila. Huomaa myös, että esimerkiksi positiivisten kokonaislukujen ja tavallisen jaollisuusrelaation muodostama hila voidaan esittää joukkojen U_p ja jaollisuusrelaation muodostamien hilojen avulla käyttämällä hilatuloa. (Ks. [9], s. 5)

Olkoon $\mathcal{T}$ joukon U_p diskreetti topologia. Luvun 4.2 alussa havaittiin, että kokonaislukujen diskreetti topologia on lokaalisti kompakti Hausdorffin topologia, joka ei kuitenkaan ole kompakti. Joukon U_p diskreetille topologialle voidaan todistaa täsmälleen samat ominaisuudet. Nämä ominaisuudet voidaan lisäksi osoittaa täysin vastaavalla menettelyllä yksiköistä koostuvan peitteen avulla. Sovelletaan jälleen yhden pisteen kompaktisointia, jolloin avaruudelle U_p saadaan kompaktisointi U_p^*, joka on lauseen 3.36 perusteella kompakti Hausdorffin avaruus.

Määritelmä 4.5. (Ks. [9], s. 5) Olkoon $\langle U_p^*, \mathcal{T}^* \rangle$ Hausdorffin avaruuden $\langle U_p, \mathcal{T} \rangle$ yhden pisteen kompaktisointi. Merkitään lisättyä äärettömyyspistettä symbolilla p^∞.

Määritellään seuraavaksi relaation $\|$ laajennus $\|^*$ joukossa U_p^*. Koska $U_p^* \setminus U_p = \{p^\infty\}$, niin relaatiota $\|$ voidaan laajentaa yksinkertaisesti määrittelemällä alkion p^∞ p^∞-laajennetut unitaaritekijät ja unitaarimonikerrat.

Määritelmä 4.6. (Ks. [9], s. 5) Määritellään joukossa U_p^* relaatio $\|^*$ siten, että $p^a \|^* p^b$, jos $p^a \| p^b$ tai $p^b = p^\infty$, kun $p^a, p^b \in U_p^*$.

Huomautus Relaatiosta $\|^*$ käytetään jatkossa lyhyesti merkintää $\|$ käsiteltäessä joukkoa U_p^*, sillä ei ole kovinkaan mielekästä tarkastella relaation $\|$ ominaisuuksia joukossa U_p^*.

Lause 4.3. *(Ks. [9], s. 5) Struktuuri $\langle U_p^*, \| \rangle$ on hila.*

Todistus. Todistetaan ensin, että $\langle U_p^*, \| \rangle$ on osittain järjestetty. Valitaan mielivaltaiset $p^a, p^b, p^c \in U_p^*$. Lauseen 3.7 mukaan refleksiivisyys, antisymmetrisyys ja transitiivisuus pätevät joukossa $U_p \subset \mathbb{Z}_+$, joten riittää tutkia tapaukset $a = \infty, b = \infty$ tai $c = \infty$.

Määritelmän 4.6 mukaan $p^\infty \| p^\infty$, joten $p^a \| p^a$, kun $a = \infty$. Refleksiivisyys siis pätee.

Antisymmetrisyyden todistamiseksi oletetaan, että $p^a \| p^b$ ja $p^b \| p^b$. Jos nyt $a = \infty$, niin myös $b = \infty$, sillä määritelmän 4.6 perusteella p^∞ on ainoa sellainen alkio, että $p^a \| p^\infty$. Vastaavalla päättelyllä havaitaan myös, että jos $b = \infty$ niin myös $a = \infty$. Nyt $p^b = p^\infty = p^a$, joten relaatio $\|$ on antisymmetrinen joukossa U_p^*.

Todistetaan vielä transitiivisuus. Oletetaan, että $p^a \| p^b$ ja $p^b \| p^c$. Jos $c = \infty$, niin määritelmän 4.6 perusteella nähdään suoraan, että $p^a \| p^c$.

Mikäli $a = \infty$ tai $b = \infty$, niin on oltava myös $c = \infty$, sillä p^∞ on ainoa alkio, joka on alkion p^∞ unitaarimonikerta. Tällöin $p^a \parallel p^c$. Relaatio $\parallel$ on siis osittainen järjestys joukossa U_p^*.

Todistetaan seuraavaksi, että $p^a \wedge p^b$ ja $p^a \vee p^b$ ovat olemassa kaikilla $p^a, p^b \in U_p^*$. Todistetaan ensin, että $p^a \wedge p^b$ on olemassa. Mikäli $a, b \in \mathbb{Z}_+ \cup \{0\}$, niin lauseen 3.7 mukaan $p^a \wedge p^b = (p^a, p^b)_{\oplus\oplus}$. Tällöin $(p^a, p^b)_{\oplus\oplus} = p^0$, jos $a \neq b$ ja $(p^a, p^b)_{\oplus\oplus} = p^a$, jos $a = b$. Jos taas $a = \infty$, niin $p^b \parallel p^a$. Tällöin lauseen 3.1 mukaan $p^a \wedge p^b = p^b$. Vastaavasti voidaan todistaa tapaus $b = \infty$. Lukujen p^a ja p^b infimum on siis aina yksikäsitteisenä olemassa joukossa U_p^*.

Todistetaan sitten, että myös $p^a \vee p^b$ on olemassa kaikilla $p^a, p^b \in U_p^*$. Olkoot $a, b \in \mathbb{Z}_+ \cup \{0\}$. Jos nyt $[p^a, p^b]_{\oplus\oplus}$ on olemassa, niin on oltava $a = 0$, $b = 0$ tai $a = b$. Tällöin pätee, että $[p^a, p^b]_{\oplus\oplus} = p^a$, kun $b = 0$ tai $a = b$ ja $[p^a, p^b]_{\oplus\oplus} = p^b$, kun $a = 0$, joten $p^a \vee p^b = [p^a, p^b]_{\oplus\oplus}$. Mikäli $[p^a, p^b]_{\oplus\oplus}$ ei ole olemassa, niin $a, b > 0$ ja $a \neq b$. Tällöin määritelmän 4.6 perusteella $p^a \parallel p^\infty$ ja $p^b \parallel p^\infty$. Koska luvuilla p^a ja p^b ei ole muita yhteisiä unitaaritekijöitä kuin p^∞, niin on oltava $p^a \vee p^b = p^\infty$. Olkoon sitten $a = \infty$. Nyt määritelmän 4.6 perusteella $p^b \parallel p^a$, joten lauseen 3.1 mukaan $p^a \vee p^b = p^a$. Struktuuri $\langle U_p^*, \parallel \rangle$ on siis hila. □

Määritelmä 4.7. (Ks. [9], s. 6) Määritellään $\langle \mathbb{Z}_+^*, \parallel \rangle$ hilojen $\langle U_p^*, \parallel \rangle$ suorana tulona yli alkulukujen joukon.

Nyt siis $\mathbb{Z}_+^* = \prod_{p \in \mathbb{P}} U_p^*$. Hilojen suoran tulon määritelmän perusteella $(2^{a_2}, 3^{a_3}, 5^{a_5}, ...) \parallel (2^{b_2}, 3^{b_3}, 5^{b_5}, ...)$, jos ja vain jos $p^{a_p} \parallel p^{b_p}$ kaikilla $p \in \mathbb{P}$, missä $\parallel$ määritellään kullakin alkuluvulla p kuten hilassa $\langle U_p^*, \parallel \rangle$. Lisäksi hilojen suoran tulon määritelmän perusteella näin saatu struktuuri $\langle Z_+^*, \parallel \rangle$ on hila. (Ks. kuva 4)

Samaistamalla kokonaisluku n kanonista alkutekijäesitystään $\prod_{p \in \mathbb{P}} p^{n(p)}$ vastaavan lukujonon $(p^{n(p)})_{p \in \mathbb{P}}$ kanssa saadaan konstroitua yksinkertaisella tavalla injektio joukolta $\mathbb{Z}_+$ joukkoon $\mathbb{Z}_+^*$. Tämä menettely on mahdollinen aritmetiikan peruslauseen nojalla (ks. [7], s. 13-14). Lisätyt alkiot ovat siis muotoa $(p^{a_p})_{p \in \mathbb{P}}$, missä $a_p = \infty$ ainakin yhdellä alkuluvulla p.

Määritelmä 4.8. (Ks. [9], s. 7) Olkoot $m, n \in \mathbb{Z}_+^*$. Määritellään lukujen m ja n *p^∞-laajennettu PYUM* eli lyhyesti $[m, n]_{p^\infty}^*$ siten, että

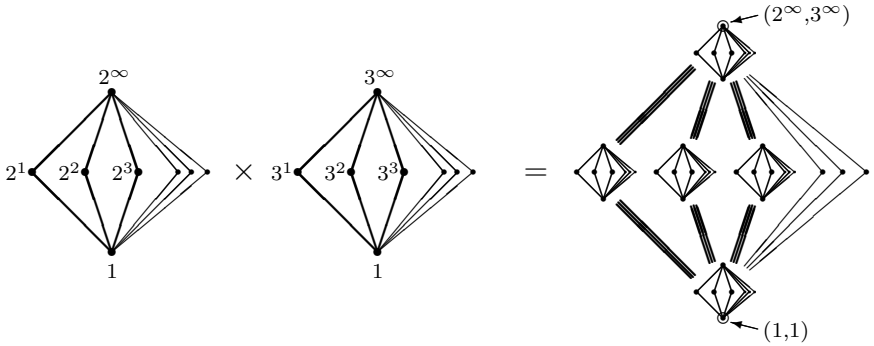
$$[m, n]_{p^\infty}^* = m \vee n,$$

missä $m \vee n$ on lukujen m ja n supremum hilassa $\langle \mathbb{Z}_+^*, \parallel \rangle$.

Esimerkki 4.1. Lukujen 6 ja 12 pienintä yhteistä unitaarimonikertaa ei ole määritelty, mutta

$$\begin{aligned}
[6, 12]_{p^\infty}^* &= (2^1, 3^1, 5^0, 7^0, ...) \vee (2^2, 3^1, 5^0, 7^0, ...) \\
&= (2^1 \vee 2^2, 3^1 \vee 3^1, 5^0 \vee 5^0, 7^0 \vee 7^0, ...) \\
&= (2^\infty, 3^1, 5^0, 7^0, ...).
\end{aligned}$$

Kuva 4: Hilojen U_2^* ja U_3^* tulohila (ks. [9], s. 6)



Luvun lopuksi todistetaan vielä yksi struktuurin $\langle \mathbb{Z}_+^*, \vee \rangle$ rakennetta kuvaava lause. Tässä lausessa hyödynnetään joukkoon $\mathbb{Z}_+^*$ konstruoitua topologiaa. Todistuksessa tarvitaan lisäksi jatkuvan kuvauksen ja topologisen puoliryhmän määritelmää.

Lause 4.4. *(Ks. [9], s. 5) Struktuuri $\langle \mathbb{Z}_+^*, \vee \rangle$ varustettuna tulotopologialla $\prod_{p\in\mathbb{P}} U_p^*$ on kommutatiivinen kompakti topologinen puoliryhmä, jossa laskutoimitus $\vee$ on idempotentti ja avaruus $\mathbb{Z}_+^*$ on Hausdorffin avaruus.*

Todistus. Koska struktuuri $\langle \mathbb{Z}_+^*, \vee \rangle$ on määritelmän 4.7 mukaan hila, voidaan lauseen 3.2 perusteella todeta, että $\langle \mathbb{Z}_+^*, \vee \rangle$ on kommutatiivinen puoliryhmä, jossa laskutoimitus $\vee$ on idempotentti. Kyseisen avaruuden kompaktius taas on välitön seuraus Tychonoffin lauseesta (lause 3.43), sillä avaruudet U_p^* ovat yhden pisteen kompaktisointeina kompakteja jokaisella $p \in \mathbb{P}$. Koska lisäksi avaruus U_p on Hausdorffin avaruus jokaisella alkuluvulla p, niin avaruus $\mathbb{Z}_+^*$ on lauseen 3.44 perusteella Hausdorffin avaruus.

Todistetaan vielä, että binäärinen laskutoimitus $\vee$ on jatkuva. Todistetaan ensin, että binäärinen laskutoimitus $\vee$ joukolta $U_p^* \times U_p^*$ joukkoon U_p^* on jatkuva jokaisella $p \in \mathbb{P}$. Valitaan mielivaltainen $p \in \mathbb{P}$. Olkoon X mielivaltainen avaruuden U_p^* avoin joukko. Oletetaan, että $p^\infty \notin X$. Koska nyt $p^\infty \vee p^a = p^a \vee p^\infty = p^\infty$ kaikilla $a \in \mathbb{Z}_+^\infty$, niin joukon X alkukuvat kuuluvat joukkoon $U_p \times U_p$. Alkukuvien joukko on tällöin avoin tulotopologiassa $U_p \times U_p$, sillä avaruuden U_p topologiana käytetään diskreettiä topologiaa. Alkukuvien joukko on siis avoin myös tulotopologiassa $U_p^* \times U_p^*$, sillä $U_p \subseteq U_p^*$.

Jos taas $p^\infty \in X$, niin voidaan kirjoittaa $X = Y \cup \{p^\infty\}$, missä $p^\infty \notin Y$. Tällöin joukon Y alkukuvien joukko kuuluu tapauksen $p^\infty \notin Y$ perusteella tulotopologiaan $U_p^* \times U_p^*$. Toisaalta joukon $\{p^\infty\}$ alkukuvien joukko on muotoa $\{(p^a, p^b) : a = \infty \text{ tai } b = \infty \text{ tai } a \neq b \text{ ja } a, b > 0\}$. Alkukuvien joukon projisointi kumman tahansa koordinaattiakselin suhteen antaa tällöin joukon $U_p \cup \{p^\infty\}$, joka kuuluu topologiaan U_p^*, sillä joukko U_p on triviaalisti kompakti avaruudessa U_p. Näin ollen joukon $\{p^\infty\}$ alkukuvien joukko on kompakti topologiassa $U_p^* \times U_p^*$. Koska alkuperäisen joukon X alkukuvien joukko

saadaan joukkojen Y ja $\{p^\infty\}$ alkukuvien yhdisteenä, niin myös joukon X alkukuvien joukko on avoin topologiassa $U_p^* \times U_p^*$. Laskutoimitus $\vee$ on siis jatkuva avaruudessa U_p jokaisella $p \in \mathbb{P}$. Edelleen lauseen 3.41 mukaan laskutoimitus $\vee$ on jatkuva avaruudessa $\mathbb{Z}_+^*$.

Struktuuri $\langle \mathbb{Z}_+^*, \vee \rangle$ varustettuna joukkojen U_p^* tulotopologialla on määritelmän 3.39 mukaisesti topologinen puoliryhmä. □

5 Tiettyjen matriisien determinanteista

Tässä luvussa esitetään lauseita ja määritelmiä, joita hyödynnetään jatkossa luvun 6.1 lauseiden todistuksissa. Luvussa keskitytään pääosin lähteen [9] sivuihin 7-11. Todistukset pyritään perustelemaan esitietoluvussa esiteltyjen lauseiden avulla hieman lähdeartikkelia yksityiskohtaisemmin.

Määritelmä 5.1. (Ks. [9], s. 7) Olkoon $S = \{x_1, x_2, ..., x_n\}$ järjestetty joukko erillisiä kokonaislukuja. Olkoon f aritmeettinen funktio, jolla $f(x) \neq 0$ kaikilla $x \in \mathbb{Z}_+$. Nyt $(\boldsymbol{S}^\times)_f$ on $n \times n$-matriisi, jolla

$$[(\boldsymbol{S}^\times)_f]_{ij} = \frac{f^2((x_i, x_j)_{\oplus\oplus})}{f(x_i)f(x_j)}.$$

Määritelmä 5.2. Olkoon μ^* Möbiuksen funktion unitaarinen vastine. Merkitään

$$B_f^*(x_i) = \sum_{\substack{d \| x_i \\ d \nmid x_t \\ t<i}} g_f(d),$$

missä

$$g_f(x) = \sum_{d \| x} f^2\left(\frac{x}{d}\right) \mu^*(d).$$

Lause 5.1. *Olkoon f aritmeettinen funktio ja g_f kuten määritelmässä. Nyt*

$$f^2(x) = \sum_{d \| x} g_f(d).$$

Todistus. Sovelletaan lausetta 3.30 eli Möbiuksen käänteiskaavan unitaarista vastinetta määritelmässä 5.2 esiintyvään funktion g_f määritelmään, jolloin saadaan

$$f^2(x) = \sum_{d \| x} g_f(d).$$

□

Lause 5.2. *(Ks. [9], s. 8) Olkoon $S = \{x_1, x_2, ..., x_n\}$ joukko erillisiä positiivisia kokonaislukuja ja olkoon $\bar{S} = \{d_1, d_2, ..., d_m\}$ minimaalinen SYUT-suljettu joukko, joka sisältää joukon S. Olkoon f sellainen aritmeettinen funktio, että $f(x) \neq 0$ kaikilla $x \in \mathbb{Z}_+$. Olkoon $\boldsymbol{C}$ sellainen $n \times m$-matriisi, että*

$$[\boldsymbol{C}]_{ij} = \begin{cases} \frac{\sqrt{B_f^*(d_j)}}{f(x_i)}, & \text{jos } d_j \parallel x_i \\ 0 & \text{muuten.} \end{cases}$$

Nyt $(\boldsymbol{S}^{\times})_f = \boldsymbol{C}\boldsymbol{C}^T$.

Todistus. Matriisitulon määritelmän perusteella

$$\begin{aligned}
[\boldsymbol{C}\boldsymbol{C}^T]_{ij} &= \sum_{k=1}^{m} [\boldsymbol{C}]_{ik}[\boldsymbol{C}^T]_{kj} \\
&= \sum_{k=1}^{m} [\boldsymbol{C}]_{ik}[\boldsymbol{C}]_{jk} \\
&= \sum_{\substack{d_k \parallel x_i \\ d_k \nparallel x_j}} \frac{\sqrt{B_f^*(d_k)}}{f(x_i)} \frac{\sqrt{B_f^*(d_k)}}{f(x_j)} \\
&= \frac{1}{f(x_i)f(x_j)} \sum_{d_k \parallel (x_i, x_j)_{\oplus\oplus}} B_f^*(d_k).
\end{aligned}$$

Edelleen funktion B_f^* määritelmän perusteella

$$\sum_{d_k \parallel (x_i, x_j)_{\oplus\oplus}} B_f^*(d_k) = \sum_{d_k \parallel (x_i, x_j)_{\oplus\oplus}} \sum_{\substack{d \parallel d_k \\ d \nparallel d_t \\ d_t < d_k}} g_f(d).$$

Tässä summassa kukin d tulee lasketuksi vain kerran, sillä jos jokin d' laskettaisiin kahdesti, niin olisi olemassa sellaiset luvut d_k ja d_l, että $d_k, d_l \parallel (x_i, x_j)_{\oplus\oplus}$ ja $d' \parallel d_k, d_l$. Lisäksi tulisi päteä, että jokaisella $d_t \parallel d_k$ pätee $d' \nparallel d_t$ ja jokaisella $d_s \parallel d_l$ pätee $d' \nparallel d_s$. Jos nyt $d_k = d_l$, niin selvästikään d' ei voi tulla lasketuksi kahdesti, sillä tällöin luku d' käy läpi luvun d_k tietyt unitaaritekijät. Jos taas $d_k \neq d_l$, niin joko $d_k < d_l$ tai $d_k > d_l$. Yleisyyttä rajoittamatta voidaan olettaa, että $d_k < d_l$. Jos nyt $d' \parallel d_l$, niin $d' \nparallel d_k$, sillä $d_k < d_l$. Siis luku d' tulee lasketuksi vain kerran. Määritelmän 5.1 perusteella

$$[(\boldsymbol{S}^{\times})_f]_{ij} = \frac{f^2((x_i, x_j)_{\oplus\oplus})}{f(x_i)f(x_j)},$$

joten on vielä osoitettava, että

$$f^2((x_i, x_j)_{\oplus\oplus}) = \sum_{d_k \parallel (x_i, x_j)_{\oplus\oplus}} \sum_{\substack{d \parallel d_k \\ d \nparallel d_t \\ d_t < d_k}} g_f(d).$$

Lauseen 5.1 perusteella

$$f^2((x_i, x_j)_{\oplus\oplus}) = \sum_{d \parallel (x_i, x_j)_{\oplus\oplus}} g_f(d).$$

Myös tässa summassa kukin d tulee lasketuksi vain kerran, sillä summaus käy läpi luvun $(x_i, x_j)_{\oplus\oplus}$ unitaaritekijät. Lisäksi jos jokin d' esiintyy ensimmäisessä summassa, niin tällöin on olemassa sellainen d_k, että $d_k \parallel (x_i, x_j)_{\oplus\oplus}$ ja $d' \parallel d_k$. Tällöin transitiivisuuden perusteella $d' \parallel (x_i, x_j)_{\oplus\oplus}$, joten kyseinen d' esiintyy myös jälkimmäisessä summassa.

Jos taas jokin d' esiintyy jälkimmäisessä summassa, niin $d' \parallel (x_i, x_j)_{\oplus\oplus}$. Koska joukko $\bar{S}$ on SYUT-suljettu, niin on olemassa sellainen $l < m$, että $(x_i, x_j)_{\oplus\oplus} = d_l$. Olkoon sitten d_k pienin sellainen luku, että $d' \parallel d_k$. Nyt varmasti $d' \nparallel d_t$, jos $d_t < d_k$. Edelleen, koska $\bar{S}$ on SYUT-suljettu, niin on olemassa sellainen $d_r \leq d_k$, että $(x_i, d_k)_{\oplus\oplus} = d_r$. Nyt koska $d' \parallel x_i$ ja $d' \parallel d_k$, niin $d' \parallel d_r$. Nyt $d_r = d_k$, sillä minimaalisuuden perusteella $d_k \leq d_r$. Jos olisi $d_k < d_r$, niin ehdon $d' \nparallel d_t$, jos $d_t < d_k$ perusteella $d' \nparallel d_r$, mikä on ristiriita. Samalla tavoin voidaan todistaa, että $d_k \parallel x_j$, mistä seuraa, että $d_k \parallel (x_i, x_j)_{\oplus\oplus}$. Siis luku d' esiintyy myös ensimmäisessä summassa. Näin ollen

$$f^2((x_i, x_j)_{\oplus\oplus}) = \sum_{d_k \parallel (x_i, x_j)_{\oplus\oplus}} \sum_{\substack{d \parallel d_k \\ d \nparallel d_t \\ d_t < d_k}} g_f(d),$$

joten $(\boldsymbol{S}^{\times})_f = \boldsymbol{C}\boldsymbol{C}^T$. □

Lause 5.3. *(Ks. [9], s. 9) Olkoon $S = \{x_1, x_2, \ldots, x_n\}$ joukko erillisiä positiivisia kokonaislukuja. Olkoon $\boldsymbol{\Lambda}$ sellainen $m \times m$-diagonaalimatriisi, että*

$$\boldsymbol{\Lambda} = \operatorname{diag}(B_f^*(d_1), B_f^*(d_2), \ldots, B_f^*(d_m)),$$

missä $\{d_1, d_2, \ldots, d_m\} = \bar{S}$ on minimaalinen SYUT-suljettu joukko, joka sisältää joukon S. Olkoon $\boldsymbol{H}$ sellainen $n \times m$-matriisi, että

$$[\boldsymbol{H}]_{ij} = \begin{cases} \frac{1}{f(x_i)}, & \textit{jos } d_j \parallel x_i \\ 0 & \textit{muuten.} \end{cases}$$

Tällöin

$$(\boldsymbol{S}^{\times})_f = \boldsymbol{H}\boldsymbol{\Lambda}\boldsymbol{H}^T.$$

Todistus. Todistetaan väite edellä todistetun lauseen 5.2 avulla. Osoitetaan ensin, että $\boldsymbol{H}\boldsymbol{\Lambda}^{1/2} = \boldsymbol{C}$. Matriisitulon määritelmän perusteella

$$\begin{aligned} [\boldsymbol{H}\boldsymbol{\Lambda}^{1/2}]_{ij} &= \sum_{k=1}^{m} [\boldsymbol{H}]_{ik} [\boldsymbol{\Lambda}^{1/2}]_{kj} \\ &= \begin{cases} \frac{1}{f(x_i)} \sqrt{B_f^*(d_j)}, & \text{jos } d_j \parallel x_i \\ 0 & \text{muuten.} \end{cases} \end{aligned}$$

Siis $\boldsymbol{H}\boldsymbol{\Lambda}^{1/2} = \boldsymbol{C}$. Nyt lauseen 5.2 mukaan $(\boldsymbol{S}^{\times})_f = \boldsymbol{C}\boldsymbol{C}^T$, josta saadaan edelleen, että

$$\begin{aligned}\boldsymbol{C}\boldsymbol{C}^T =& (\boldsymbol{H}\boldsymbol{\Lambda}^{1/2})(\boldsymbol{H}\boldsymbol{\Lambda}^{1/2})^T = \boldsymbol{H}\boldsymbol{\Lambda}^{1/2}(\boldsymbol{\Lambda}^{1/2})^T\boldsymbol{H}^T \\ =& \boldsymbol{H}\boldsymbol{\Lambda}^{1/2}\boldsymbol{\Lambda}^{1/2}\boldsymbol{H}^T = \boldsymbol{H}\boldsymbol{\Lambda}\boldsymbol{H}^T.\end{aligned}$$

□

Lause 5.4. *(Ks. [9], s. 9) Olkoon $S = \{x_1, x_2, \ldots, x_n\}$ joukko erillisiä positiivisia kokonaislukuja. Olkoon f sellainen aritmeettinen funktio, että $f(x) \neq 0$ kaikilla $x \in \mathbb{Z}_+$. Jos S on SYUT-suljettu, niin*

$$\det((\boldsymbol{S}^{\times})_f) = \prod_{k=1}^{n} \frac{B_f^*(x_k)}{f^2(x_k)}.$$

Todistus. Nyt $S = \bar{S}$, sillä S on SYUT-suljettu, joten matriisin $\boldsymbol{C}$ dimensio on $n \times n$. Lisäksi tiedetään, että $\boldsymbol{C}$ on alakolmiomatriisi, sillä diagonaalin yläpuolisissa alkioissa ehto $x_j \parallel x_i$ ei voi olla voimassa, sillä näissä alkioissa $x_j > x_i$. Matriisin $\boldsymbol{C}$ determinantti voidaan siis laskea diagonaalialkioiden tulona (ks. [4], s. 218). Lauseessa 5.2 esitetyn matriisin $\boldsymbol{C}$ määritelmän perusteella matriisin $\boldsymbol{C}$ diagonaalialkiot ovat

$$[\boldsymbol{C}]_{kk} = \frac{\sqrt{B_f^*(x_k)}}{f(x_k)},$$

kun $k = 1, 2, \ldots, n$. Siis

$$\det(\boldsymbol{C}) = \prod_{k=1}^{n} \frac{\sqrt{B_f^*(x_k)}}{f(x_k)}.$$

Lauseen 5.2 perusteella $(\boldsymbol{S}^{\times})_f = \boldsymbol{C}\boldsymbol{C}^T$, joten

$$\begin{aligned}\det((\boldsymbol{S}^{\times})_f) =& \det(\boldsymbol{C}\boldsymbol{C}^T) = \det(\boldsymbol{C})\det(\boldsymbol{C}^T) = (\det(\boldsymbol{C}))^2 \\ =& \left(\prod_{k=1}^{n} \frac{\sqrt{B_f^*(x_k)}}{f(x_k)}\right)^2 \\ =& \prod_{k=1}^{n} \frac{B_f^*(x_k)}{f^2(x_k)}.\end{aligned}$$

□

Lause 5.5. *(Ks. [9], s. 10) Olkoon $\bar{S} = \{x_1, x_2, \ldots, x_n, \ldots, x_{n+s}\}$ minimaalinen SYUT-suljettu joukko, joka sisältää joukon $S = \{x_1, x_2, \ldots, x_n\}$ alkiot. Oletetaan lisäksi joukon $\bar{S}$ olevan järjestetty siten, että $x_1 < x_2 < \cdots < x_n$*

ja $x_{n+1} < x_{n+2} < \cdots < x_{n+s}$*. Olkoon* f *sellainen aritmeettinen funktio, että* $f(x) \neq 0$ *kaikilla* $x \in \mathbb{Z}_+$*. Nyt*

$$\det((\boldsymbol{S}^{\times})_f) = \sum_{1 \leq k_1 < k_2 < \cdots < k_n \leq n+s} \det(\boldsymbol{H}_{(k_1,k_1,\ldots,k_n)})^2 B_f^*(x_{k_1}) B_f^*(x_{k_2}) \cdots B_f^*(x_{k_n}),$$

missä merkintä $\boldsymbol{H}_{(k_1,k_2,\ldots,k_n)}$ *tarkoittaa sitä matriisin* $\boldsymbol{H}$ *alimatriisia, johon on otettu matriisin* $\boldsymbol{H}$ *sarakkeet* $k_1, k_2, \ldots, k_n$*. Matriisi* $\boldsymbol{H}$ *on määritelty kuten lauseessa 5.3.*

Todistus. Todistetaan ensin, että

$$\boldsymbol{C}_{(k_1,k_2,\ldots,k_n)} = \boldsymbol{H}_{(k_1,k_2,\ldots,k_n)} \operatorname{diag}\left(\sqrt{B_f^*(x_{k_1})}, \sqrt{B_f^*(x_{k_2})}, \ldots, \sqrt{B_f^*(x_{k_n})}\right).$$

Tehdään todistus laskemalla tulomatriisin alkio ij.

$$\begin{aligned}
&\left[\boldsymbol{H}_{(k_1,k_2,\ldots,k_n)} \operatorname{diag}\left(\sqrt{B_f^*(x_{k_1})}, \sqrt{B_f^*(x_{k_2})}, \ldots, \sqrt{B_f^*(x_{k_n})}\right)\right]_{ij} \\
=&\sum_{l=1}^{n} [\boldsymbol{H}_{(k_1,k_2,\ldots,k_n)}]_{il} \left[\operatorname{diag}\left(\sqrt{B_f^*(x_{k_1})}, \sqrt{B_f^*(x_{k_2})}, \ldots, \sqrt{B_f^*(x_{k_n})}\right)\right]_{lj} \\
=&[\boldsymbol{H}_{(k_1,k_2,\ldots,k_n)}]_{ij} \left[\operatorname{diag}\left(\sqrt{B_f^*(x_{k_1})}, \sqrt{B_f^*(x_{k_2})}, \ldots, \sqrt{B_f^*(x_{k_n})}\right)\right]_{jj} \\
=&[\boldsymbol{H}_{ik_j}] \left[\operatorname{diag}\left(\sqrt{B_f^*(x_{k_1})}, \sqrt{B_f^*(x_{k_2})}, \ldots, \sqrt{B_f^*(x_{k_n})}\right)\right]_{jj} \\
=&\begin{cases} \frac{1}{f(x_i)}\sqrt{B_f^*(x_{k_j})}, & \text{jos } x_{k_j} \parallel x_i \\ 0 & \text{muuten} \end{cases} \\
=&[\boldsymbol{C}]_{ik_j} = [\boldsymbol{C}_{(k_1,k_2,\ldots,k_n)}]_{ij}.
\end{aligned}$$

Lauseen 5.2 mukaan $(\boldsymbol{S}^{\times})_f = \boldsymbol{C}\boldsymbol{C}^T$, josta saadaan edelleen Cauchy-Binet kaavan avulla, että

$$\begin{aligned}
&\det((\boldsymbol{S}^{\times})_f) = \det(\boldsymbol{C}\boldsymbol{C}^T) \\
&= \sum_{1 \leq k_1 < k_2 < \cdots < k_n \leq n+s} \det(\boldsymbol{C}_{(k_1,k_1,\ldots,k_n)}) \det(\boldsymbol{C}^T_{(k_1,k_1,\ldots,k_n)}) \\
&= \sum_{1 \leq k_1 < k_2 < \cdots < k_n \leq n+s} \det(\boldsymbol{C}_{(k_1,k_1,\ldots,k_n)})^2 \\
&= \sum_{1 \leq k_1 < k_2 < \cdots < k_n \leq n+s} \det\Big(\boldsymbol{H}_{(k_1,k_1,\ldots,k_n)} \operatorname{diag}\Big(\sqrt{B_f^*(x_{k_1})}, \sqrt{B_f^*(x_{k_2})}, \ldots, \sqrt{B_f^*(x_{k_n})}\Big)\Big)^2 \\
&= \sum_{1 \leq k_1 < k_2 < \cdots < k_n \leq n+s} \det(\boldsymbol{H}_{(k_1,k_1,\ldots,k_n)})^2 \det\Big(\operatorname{diag}\Big(\sqrt{B_f^*(x_{k_1})}, \sqrt{B_f^*(x_{k_2})}, \ldots, \sqrt{B_f^*(x_{k_n})}\Big)\Big)^2 \\
&= \sum_{1 \leq k_1 < k_2 < \cdots < k_n \leq n+s} \det(\boldsymbol{H}_{(k_1,k_1,\ldots,k_n)})^2 \Big(\sqrt{B_f^*(x_{k_1})} \sqrt{B_f^*(x_{k_2})} \cdots \sqrt{B_f^*(x_{k_n})}\Big)^2 \\
&= \sum_{1 \leq k_1 < k_2 < \cdots < k_n \leq n+s} \det(\boldsymbol{H}_{(k_1,k_1,\ldots,k_n)})^2 B_f^*(x_{k_1}) B_f^*(x_{k_2}) \cdots B_f^*(x_{k_n}).
\end{aligned}$$

□

6 Laajennusten ominaisuuksista

Tutkielman lopuksi esitetään vielä luvussa 4 esitettyjen laajennusten avulla konstruoitujen SYUT- ja PYUM-matriisien tärkeimpiä ominaisuuksia lauseiden muodossa sekä esitetään jokseenkin yksinkertaisia esimerkkejä kutakin laajennustapaa vastaavista pseudo-, ∞- ja p^∞-unitaarisesti semimultiplikatiivisista funktioista. Luvun keskeisimpänä tarkoituksen on osoittaa määritelmässä 6.3 esiteltävien funktioluokkien jäsenten ominaisuuksien erot. Tähän pyritään osoittamalla esimerkkien ja lauseiden avulla, että tietyin menetelmin määritellyt funktiot, jotka kuuluvat johonkin näistä luokista, eivät välttämättä kuulu muihin luokkiin.

6.1 SYUT- ja PYUM-matriisien Hadamardin osamäärä

Määritelmä 6.1. (Ks. [9], s. 11) Olkoon $S = \{x_1, x_2, \ldots, x_n\}$ joukko erillisiä positiivisia kokonaislukuja ja olkoon f sellainen aritmeettinen funktio, että $f(x) \neq 0$ kaikilla $x \in \mathbb{Z}_+$. Määritellään $n \times n$-matriisit $(\boldsymbol{S}^{\oplus\oplus})_f$, $[\boldsymbol{S}^*]_f$, $[\boldsymbol{S}^*_\infty]_f$ ja $[\boldsymbol{S}^*_{p^\infty}]_f$ siten, että

$$\begin{aligned}
[(\boldsymbol{S}^{\oplus\oplus})_f]_{ij} &= f((x_i, x_j)_{\oplus\oplus}),\\
[[\boldsymbol{S}^*]_f]_{ij} &= f([x_i, x_j]^*),\\
[[\boldsymbol{S}^*_\infty]_f]_{ij} &= f([x_i, x_j]^*_\infty),\\
[[\boldsymbol{S}^*_{p^\infty}]_f]_{ij} &= f([x_i, x_j]^*_{p^\infty}).
\end{aligned}$$

Määritelmä 6.2. (Ks. [9], s. 11) Matriisit $(\boldsymbol{S}^{\oplus\oplus})_f/[\boldsymbol{S}^*]_f$, $(\boldsymbol{S}^{\oplus\oplus})_f/[\boldsymbol{S}^*_\infty]_f$ ja $(\boldsymbol{S}^{\oplus\oplus})_f/[\boldsymbol{S}^*_{p^\infty}]_f$ määritellään matriisin $(\boldsymbol{S}^{\oplus\oplus})_f$, sekä matriisien $[\boldsymbol{S}^*]_f$, $[\boldsymbol{S}^*_\infty]_f$ ja $[\boldsymbol{S}^*_{p^\infty}]_f$ Hadamardin osamäärän avulla, eli

$$\begin{aligned}
[(\boldsymbol{S}^{\oplus\oplus})_f/[\boldsymbol{S}^*]_f]_{ij} &= \frac{f((x_i, x_j)_{\oplus\oplus})}{f([x_i, x_j]^*)},\\
[(\boldsymbol{S}^{\oplus\oplus})_f/[\boldsymbol{S}^*_\infty]_f]_{ij} &= \frac{f((x_i, x_j)_{\oplus\oplus})}{f([x_i, x_j]^*_\infty)},\\
[(\boldsymbol{S}^{\oplus\oplus})_f/[\boldsymbol{S}^*_{p^\infty}]_f]_{ij} &= \frac{f((x_i, x_j)_{\oplus\oplus})}{f([x_i, x_j]^*_{p^\infty})}.
\end{aligned}$$

Seuraavaksi määritellään tavanomaista aritmeettisten funktioiden semimultiplikatiivisuutta muistuttava ominaisuus kullekin luvussa 4 konstruoiduista PYUM-laajennuksista. Näitä ominaisuuksia hyödynnetään luvussa 6.2 tehtävissä tarkasteluissa.

Määritelmä 6.3. (Ks. [9], s. 11) Olkoon $T \subseteq \mathbb{Z}_+$ ja olkoon f aritmeettinen funktio. Jos

$$f((m, n)_{\oplus\oplus}) f([m, n]^*) = f(m) f(n) \tag{1}$$

kaikilla $m, n \in T$, niin sanotaan, että f on *pseudo-unitaarisesti semimultiplikatiivinen joukossa T.*

Olkoon g joukossa $\mathbb{Z}_+^\infty$ määritelty kompleksilukuarvoinen funktio. Jos

$$g((m,n)_{\oplus\oplus})g([m,n]^*_\infty) = g(m)g(n) \tag{2}$$

kaikilla $m, n \in T$, niin sanotaan, että f on *∞-unitaarisesti semimultiplikatiivinen joukossa T.*

Olkoon h joukossa $\mathbb{Z}^*$ määritelty kompleksilukuarvoinen funktio. Jos

$$g((m,n)_{\oplus\oplus})g([m,n]^*_{p^\infty}) = g(m)g(n) \tag{3}$$

kaikilla $m, n \in T$, niin sanotaan, että f on *p^∞-unitaarisesti semimultiplikatiivinen joukossa T.*

Huomautus Esitetyt määritelmät voidaan ymmärtää tavanomaisen semimultiplikatiivisuuden laajennuksina (ks. 3.15). Luvussa 6.2 puhutaan yleisesti pseudo-, $\infty-$ tai p^∞-unitaarisesti semimultiplikatiivisista funktioista mainitsematta mitään erityistä joukkoa. Tällä ilmaisulla tarkoitetaan tässä yhteydessä joukossa $\mathbb{Z}_+$ pseudo-, $\infty-$ tai p^∞-unitaarisesti semimultiplikatiivisia funktioita. Huomaa, että tällaiset funktiot ovat pseudo-, ∞- tai p^∞-unitaarisesti semimultiplikatiivisia jokaisessa joukossa $T \subseteq \mathbb{Z}_+$.

Lause 6.1. *(Vrt. [9], s. 12) Olkoon $S = \{x_1, x_2, \ldots, x_n\}$ SYUT-suljettu joukko erillisiä positiivisia kokonaislukuja. Olkoon f sellainen aritmeettinen funktio, että $f(x) \neq 0$ kaikilla $x \in \mathbb{Z}_+$. Olkoon g sellainen joukossa $\mathbb{Z}_+^\infty$ määritelty kompleksilukuarvoinen funktio, että $g(x) \neq 0$ kaikilla $x \in \mathbb{Z}_+^\infty$. Olkoon h sellainen joukossa $\mathbb{Z}_+^*$ määritelty kompleksilukuarvoinen funktio, että $h(x) \neq 0$ kaikilla $x \in \mathbb{Z}_+^*$.*

Jos f on pseudo-unitaarisesti semimultiplikatiivinen joukossa S, niin

$$(\boldsymbol{S}^{\oplus\oplus})_f / [\boldsymbol{S}^*]_f = (\boldsymbol{S}^\times)_f.$$

Jos g on ∞-unitaarisesti semimultiplikatiivinen joukossa S, niin

$$(\boldsymbol{S}^{\oplus\oplus})_g / [\boldsymbol{S}^*_\infty]_g = (\boldsymbol{S}^\times)_g.$$

Jos h on p^∞-unitaarisesti semimultiplikatiivinen joukossa S, niin

$$(\boldsymbol{S}^{\oplus\oplus})_h / [\boldsymbol{S}^*_{p^\infty}]_h = (\boldsymbol{S}^\times)_h.$$

Todistus. Oletetaan, että funktio f on pseudo-unitaarisesti semimultiplikatiivinen joukossa S. Määritelmän 5.1 mukaan

$$\left[(\boldsymbol{S}^\times)_f\right] = \frac{f^2((x_i, x_j)_{\oplus\oplus})}{f(x_i)f(x_j)}.$$

Koska toisaalta funktio f on oletuksen mukaan pseudo-unitaarisesti semimultiplikatiivinen joukossa S, niin

$$\begin{aligned}\left[(S^{\oplus\oplus})_f/[S^*]_f\right]_{ij} =& \frac{f((x_i,x_j)_{\oplus\oplus})}{f([x_i,x_j]^*)}\\ =& \frac{f((x_i,x_j)_{\oplus\oplus})}{f(x_i)f(x_j)(f(x_i,x_j))^{-1}}\\ =& \frac{f^2((x_i,x_j)_{\oplus\oplus})}{f(x_i)f(x_j)}.\end{aligned}$$

Näin ollen

$$(\boldsymbol{S}^{\oplus\oplus})_f/[\boldsymbol{S}^*]_f = (\boldsymbol{S}^{\times})_f.$$

Lauseen muiden kohtien todistukset sivuutetaan, sillä ne voidaan todistaa ∞- tai p^∞ unitaariseen semimultiplikatiivisuuteen vedoten täysin vastaavalla päättelyllä. □

Lause 6.2. *(Vrt. [9], s. 12) Olkoon $S = \{x_1, x_2, \ldots, x_n\}$ SYUT-suljettu joukko erillisiä positiivisia kokonaislukuja. Olkoon f sellainen aritmeettinen funktio, että $f(x) \neq 0$ kaikilla $x \in \mathbb{Z}_+$. Olkoon g sellainen joukossa $\mathbb{Z}_+^\infty$ määritelty kompleksilukuarvoinen funktio, että $g(x) \neq 0$ kaikilla $x \in \mathbb{Z}_+^\infty$. Olkoon h sellainen joukossa $\mathbb{Z}^*$ määritelty kompleksilukuarvoinen funktio, että $h(x) \neq 0$ kaikilla $x \in \mathbb{Z}_+^*$.*

Jos f on pseudo-unitaarisesti semimultiplikatiivinen joukossa S, niin

$$\det((\boldsymbol{S}^{\oplus\oplus})_f/[\boldsymbol{S}^*]_f) = \prod_{k=1}^{n} \frac{B_f^*(x_k)}{f^2(x_k)}.$$

Jos g on ∞-unitaarisesti semimultiplikatiivinen joukossa S, niin

$$\det((\boldsymbol{S}^{\oplus\oplus})_g/[\boldsymbol{S}^*]_g) = \prod_{k=1}^{n} \frac{B_g^*(x_k)}{g^2(x_k)}.$$

Jos h on p^∞-unitaarisesti semimultiplikatiivinen joukossa S, niin

$$\det((\boldsymbol{S}^{\oplus\oplus})_h/[\boldsymbol{S}^*]_h) = \prod_{k=1}^{n} \frac{B_h^*(x_k)}{h^2(x_k)}.$$

Todistus. Koska $f(x) \neq 0$ kaikilla $x \in \mathbb{Z}_+$, niin jakamalla puolittain termillä $f((m,n)_{\oplus\oplus})$ semimultiplikatiivisuusehdosta saadaan, että

$$f([m,n]^*) = \frac{f(m)f(n)}{f((m,n)_{\oplus\oplus})}, \forall m,n \in \mathbb{Z}_+.$$

Edelleen pätee

$$\begin{aligned}[(\boldsymbol{S}^{\oplus\oplus})_f/[\boldsymbol{S}^*]_f]_{ij} =& \frac{f((x_i,x_j)_{\oplus\oplus})}{f([x_i,x_j]^*)}\\ =& \frac{f((x_i,x_j)_{\oplus\oplus})}{(f(x_i)f(x_j))/f((x_i,x_j)_{\oplus\oplus})}\\ =& \frac{f^2((x_i,x_j)_{\oplus\oplus})}{f(x_i)f(x_j)}.\end{aligned}$$

On siis todistettu, että tällöin

$$(\boldsymbol{S}^{\oplus\oplus})_f/[[\boldsymbol{S}^*]_f]_{ij} = (\boldsymbol{S}^{\times})_f.$$

Nyt lauseen 5.4 perusteella

$$\det((\boldsymbol{S}^{\oplus\oplus})_f/[[\boldsymbol{S}^*]_f]_{ij}) = \det((\boldsymbol{S}^{\times})_f) = \prod_{k=1}^{n}\frac{B_f^*(x_k)}{f^2(x_k)}.$$

Muut kohdat voidaan todistaa vastaavasti lauseeseen 5.4 vedoten. □

Lause 6.3. *(Ks. [9], s. 13) Olkoon f sellainen aritmeettinen funktio, että $f(x) \neq 0$ kaikilla $x \in \mathbb{Z}_+$. Olkoon g sellainen joukossa $\mathbb{Z}_+^\infty$ määritelty kompleksilukuarvoinen funktio, että $g(x) \neq 0$ kaikilla $x \in \mathbb{Z}_+^\infty$. Olkoon h sellainen joukossa $\mathbb{Z}_+^*$ määritelty kompleksilukuarvoinen funktio, että $h(x) \neq 0$ kaikilla $x \in \mathbb{Z}_+^*$.*

Oletetaan vielä, että $\boldsymbol{S} = \{x_1, x_2, \ldots, x_n\}$ on joukko erillisiä positiivisia kokonaislukuja. Olkoon $\bar{S} = \{x_1, x_2, \ldots, x_n, x_{n+1}, x_{n+2}, \ldots, x_{n+s}\}$ minimaalinen SYUT-suljettu joukko, joka sisältää joukon S. Oletetaan lisäksi joukon $\bar{S}$ olevan järjestetty siten, että $x_1 < x_2 < \cdots < x_n$ ja $x_{n+1} < x_{n+2} < \ldots < x_{n+s}$.

Jos f on pseudo-unitaarisesti semimultiplikatiivinen joukossa S, niin

$$\det((\boldsymbol{S}^{\oplus\oplus})_f/[\boldsymbol{S}^*]_f) = \sum_{1\leq k_1<k_2<\cdots<k_n\leq n+s} \det(\boldsymbol{H}_{(k_1,k_1,\ldots,k_n)})^2 B_f^*(x_{k_1})B_f^*(x_{k_2})\cdots B_f^*(x_{k_n}).$$

Jos g on ∞-unitaarisesti semimultiplikatiivinen joukossa S, niin

$$\det((\boldsymbol{S}^{\oplus\oplus})_g/[\boldsymbol{S}^*]_g) = \sum_{1\leq k_1<k_2<\cdots<k_n\leq n+s} \det(\boldsymbol{H}_{(k_1,k_1,\ldots,k_n)})^2 B_g^*(x_{k_1})B_g^*(x_{k_2})\cdots B_g^*(x_{k_n}).$$

Jos h on p^∞-unitaarisesti semimultiplikatiivinen joukossa S, niin

$$\det((\boldsymbol{S}^{\oplus\oplus})_h/[\boldsymbol{S}^*]_h) = \sum_{1\leq k_1<k_2<\cdots<k_n\leq n+s} \det(\boldsymbol{H}_{(k_1,k_1,\ldots,k_n)})^2 B_h^*(x_{k_1})B_h^*(x_{k_2})\cdots B_h^*(x_{k_n}).$$

Matriisi $\boldsymbol{H}_{(k_1,k_1,\ldots,k_n)}$ on määritelty kuten lauseessa 5.5.

Todistus. Kaikki kohdat seuraavat suoraan lauseista 5.5 ja 6.1. □

6.2 Pseudo-unitaarisesti semimultiplikatiiviset funktiot

Lause 6.4. *(Ks.[9], s. 15) Olkoon f aritmeettinen funktio. Jos f on pseudo-unitaarisesti semimultiplikatiivinen ja $f(1) = 1$, niin f on multiplikatiivinen ja*

$$f(p^a) = f(p)^{a-2} f(p^2)$$

jokaisella alkuluvulla p ja kokonaisluvulla $a \geq 2$.

Todistus. Todistetaan ensin multiplikatiivisuus. Valitaan sellaiset $m, n \in \mathbb{Z}_+$, että $(m, n) = 1$. Koska f on pseudo-unitaarisesti semimultiplikatiivinen, niin määritelmän 6.3 kohdan (1) mukaan

$$f(m)f(n) = f((m, n)_{\oplus\oplus}) f([m, n]^*).$$

Koska $(m, n) = 1$ ja lauseen 3.6 mukaan $(m, n)_{\oplus\oplus} \leq (m, n)$, niin myös $(m, n)_{\oplus\oplus} = 1$. Näin ollen pseudo-PYUM:n määritelmän mukaan

$$[m, n]^* = \frac{mn}{(m, n)_{\oplus\oplus}} = mn.$$

Siis

$$f(m)f(n) = f((m, n)_{\oplus\oplus}) f([m, n]^*) = f(1)f(mn) = f(mn),$$

joten f on multiplikatiivinen. On vielä todistettava, että

$$f(p^a) = f(p)^{a-2} f(p^2)$$

kaikilla alkuluvuilla p ja kokonaisluvuilla $a \geq 2$. Tämä todistetaan induktiolla. Valitaan mielivaltainen alkuluku p. Jos $a = 2$, niin

$$f(p^a) = f(p^2) = 1f(p^2) = f(p)^0 f(p^2) = f(p)^{2-2} f(p^2) = f(p)^{a-2} f(p^2).$$

Tehdään induktio-oletus, että väite

$$f(p^a) = f(p)^{a-2} f(p^2)$$

pätee, kun $a = k \geq 2$.

Todistetaan, että väite pätee myös arvolla $a = k + 1$. Koska $(p, p^k)_{\oplus\oplus} = 1$ ja

$$[p, p^k]^* = \frac{pp^k}{(p, p^k)_{\oplus\oplus}} = \frac{p^{k+1}}{1} = p^{k+1},$$

niin

$$f(p^{k+1}) = f(1)f(p^{k+1}) = f((p, p^k)_{\oplus\oplus}) f([p, p^k]^*).$$

Koska f on on pseudo-unitaarisesti semimultiplikatiivinen, tästä saadaan edelleen, että

$$f((p, p^k)_{\oplus\oplus}) f([p, p^k]^*) = f(p)f(p^k).$$

Soveltamalla induktio-oletusta saadaan, että

$$f(p^{k+1}) = f(p)f(p^k) = f(p)(f(p)^{k-2}f(p^2)) = f(p)^{(k+1)-2}f(p^2).$$

Induktioperiaatteen mukaan väite pätee kaikilla kokonaisluvuilla $a \geq 2$. Koska alkuluku p valittiin mielivaltaisesti, väite pätee kaikilla alkuluvuilla p. □

Huomautus Edellisen väitteen implikaatio ei päde toiseen suuntaan. Vastaesimerkiksi voidaan ottaa sellainen multiplikatiivinen aritmeettinen funktio g, että $g(p) = 1$ ja $g(p^a) = 2$, kun $a > 1$ ja p on alkuluku. Tällöin $g(4)g(8) = 4 \neq 2 = g(1)g(32) = g((4,8)_{\oplus\oplus})g([4,8]^*)$, joten g ei ole pseudounitaarisesti semimultiplikatiivinen, mutta lauseen 6.4 ehto on voimassa.

Lause 6.5. *(Ks.[9], s. 16) Olkoon f aritmeettinen funktio. Jos f on multiplikatiivinen ja*

$$f(p^a) = f(p)^{a-2}f(p^2) \tag{1}$$

jokaisella alkuluvulla p ja kokonaisluvulla $a \geq 2$, niin f on astetta $(1,2)$ oleva aritmeettinen rationaalifunktio.

Todistus. Valitaan mielivaltainen alkuluku p. Nyt oletuksen (1) mukaan

$$f(p^k) = f(p)^{k-2}f(p^2)$$

kaikilla kokonaisluvuilla $k \geq 2$. Aritmeettisen funktion f Bellin sarja modulo p on siis

$$\begin{aligned} f_p(x) =& 1 + f(p)x + \sum_{n=2}^{\infty} f(p)^{n-2}f(p^2)x^n \\ =& 1 + f(p)x + f(p^2)x^2 \sum_{n=0}^{\infty} f(p)^n x^n. \end{aligned}$$

Lasketaan summa geometrisen sarjan summana, jolloin saadaan

$$\begin{aligned} f_p(x) =& 1 + f(p)x + f(p^2)x^2 \frac{1}{1 - f(p)x} \\ =& \frac{1 - (f(p)^2 - f(p^2))x^2}{1 - f(p)x}. \end{aligned}$$

Lauseen 3.20 mukaan f on siis astetta $(1,2)$ oleva aritmeettinen rationaalifunktio. □

Esimerkki 6.1. Olkoon f sellainen multiplikatiivinen aritmeettinen funktio, että

$$f(p^a) = \begin{cases} 1, & \text{jos } a = 1 \\ 0, & \text{jos } a > 1. \end{cases}$$

Tällöin f on pseudo-unitaarisesti semimultiplikatiivinen. Tämä on helppo havaita suoraan määritelmän avulla. Havaitaan ensin, että multiplikatiivisuuden perusteella $f(n) = 0$ tai $f(n) = 1$ jokaisella positiivisella kokonaisluvulla n.

Nyt $f(m)f(n) = 1$, jos ja vain jos luvuilla m ja n on pelkästään ensimmäistä astetta olevia alkulukutekijöitä. Tällöin myöskään lukujen n ja m suurimmalla yhteisellä unitaaritekijällä tai pienimmällä yhteisellä pseudounitaarimonikerralla ei voi olla muita kuin ensimmäistä astetta olevia alkulukutekijöitä. Näin ollen $f((m,n)_{\oplus\oplus})f([m,n]^*) = 1$.

Jos taas $f(m)f(n) = 0$, niin joko $f(m) = 0$ tai $f(n) = 0$. Tällöin joko luvulla m tai n on ainakin yksi vähintään astetta 2 oleva alkulukutekijä. Lukujen m ja n pienimmän yhteisen unitaarimonikerran vastaavan alkulukutekijän aste on tällöin myös vähintään 2, joten $f([m,n]^*) = 0$. Näin ollen $f((m,n)_{\oplus\oplus})f([m,n]^*) = 0$.

6.3 ∞-unitaarisesti semimultiplikatiiviset funktiot

Lause 6.6. *(Ks.[9], s. 17) Olkoon f joukossa $\mathbb{Z}_+^\infty$ määritelty kompleksilukuarvoinen funktio. Jos f on ∞-unitaarisesti semimultiplikatiivinen ja $f(p^a) \neq 0$ kaikilla alkuluvuilla p ja positiivisilla kokonaisluvuilla a, niin f on vakiofunktio.*

Todistus. Todistetaan ensin, että funktion f rajoittuma joukkoon $\mathbb{Z}_+$ on kvasimultiplikatiivinen. Valitaan sellaiset $m, n \in \mathbb{Z}_+$, että $(m,n) = 1$. Koska $(m,n) = 1$, niin lauseen 3.8 perusteella $(m,n)_{\oplus\oplus} = 1$ ja $[m,n]_\infty^* = mn$. Koska f on ∞-unitaarisesti semimultiplikatiivinen, niin määritelmän 6.3 kohdan (2) mukaan

$$f(m)f(n) = f((m,n)_{\oplus\oplus})f([m,n]_\infty^*) = f(1)f(mn) \tag{1}$$

kaikilla $m, n \in \mathbb{Z}_+$, joilla $(m,n) = 1$. Aritmeettinen funktio f on siis kvasimultiplikatiivinen. Valitaan seuraavaksi mielivaltainen alkuluku p ja sellaiset positiiviset kokonaisluvut a ja b, että $a \neq b$. Tiedetään, että $(p^a, p^b)_{\oplus\oplus} = 1$ ja $[p^a, p^b] = \infty$. Nyt määritelmän 6.3 kohdan (2) perusteella

$$f(p^a)f(p^b) = f((p^a,p^b)_{\oplus\oplus})f([p^a,p^b]_\infty^*) = f(1)f(\infty) = c, \tag{2}$$

missä kompleksiluku c on vakio. Valitsemalla tähän yhtälöön ensin $a = 1$ ja $b = 2$, ja sitten $a = 1$ ja $b = u \geq 2$ saadaan

$$f(p)f(p^2) = c = f(p)f(p^u).$$

Koska $f(p) \neq 0$, niin tästä seuraa, että $f(p^2) = f(p^u)$ kaikilla kokonaisluvuilla $u \geq 2$. Jos yhtälössä (2) valitaan ensin $a = 1$ ja $b = 3$ ja sitten $a = 2$ ja $b = 3$, saadaan

$$f(p)f(p^3) = c = f(p^2)f(p^3),$$

minkä perusteella saadaan $f(p) = f(p^2)$, sillä $f(p^3) \neq 0$. On siis todistettu, että

$$f(p) = f(p^u) \tag{3}$$

kaikilla kokonaisluvuilla $u \geq 1$. Edelleen kohtien (2) ja (3) perusteella

$$f(p)^2 = f(1)f(\infty) \tag{4}$$

kaikilla alkuluvuilla p. Valitaan sitten sellaiset alkuluvut p_1 ja p_2, että $p_1 \neq p_2$. Valitaan $m = p_1p_2$ ja $n = p_1p_2^2$. Nyt $(m,n)_{\oplus\oplus} = p_1$ ja $[m,n]^*_\infty = \infty$, joten määritelmän 6.3 kohdan (2) mukaan

$$f(m)f(n) = f((m,n)_{\oplus\oplus})f([m,n]^*_\infty) = f(p_1)f(\infty).$$

Toisaalta funktion f kvasimultiplikatiivisuuden perusteella saadaan, että

$$\begin{aligned} f(m)f(n) =& f(p_1p_2)f(p_1p_2^2) \\ =& f(1)f(p_1p_2)f(1)f(p_1p_2^2)f(1)^{-2} \\ =& f(p_1)f(p_2)f(p_1)f(p_2^2)f(1)^{-2} \\ =& f(p_1)^2f(p_2)f(p_2^2)f(1)^{-2}, \end{aligned}$$

joten

$$f(p_1)f(\infty) = f(p_1)^2f(p_2)f(p_2^2)f(1)^{-2}.$$

Edelleen kohdan (3) perusteella $f(p_2) = f(p_2^2)$, joten

$$f(p_1)f(\infty) = f(p_1)^2f(p_2)^2f(1)^{-2}.$$

Nyt kohdan (4) perusteella

$$\begin{aligned} f(p_1)f(\infty) =& (f(1)f(\infty))(f(1)f(\infty))f(1)^{-2} \\ =& f(\infty)^2. \end{aligned}$$

Koska $f(\infty) \neq 0$, niin $f(p_1) = f(\infty)$. Koska alkuluku p_1 valittiin mielivaltaisesti, niin $f(p) = f(\infty)$ kaikilla alkuluvuilla p. Edelleen kohtien (2) ja (4) mukaan

$$\begin{aligned} f(1)f(\infty) =& f(p)f(p^2) \\ =& f(p)^2 \\ =& f(\infty)f(p), \end{aligned}$$

joten koska $f(\infty) \neq 0$, niin

$$f(p) = f(1) \tag{5}$$

kaikilla alkuluvuilla p. Kohtien (2),(4) ja (5) perusteella on siis siis todistettu, että

$$f(p^u) = f(1) = f(\infty),$$

jokaisella alkuluvulla p ja kokonaisluvulla $u \geq 1$. Olkoon N mielivaltainen positiivinen kokonaisluku ja $p_1^{N_1} p_2^{N_2} \cdots p_r^{N_r}$ luvun N kanoninen alkutekijäesitys, missä $N_1, N_2, \ldots, N_r \geq 1$. Lauseen 3.13 perusteella

$$\begin{aligned} f(N) =& f(\prod_{i=1}^{r} p^{N(p)}) \\ =& f(1)^{-(r-1)} \prod_{i=1}^{r} f(p^{N(p)}) \\ =& f(1)^{-r+1} \prod_{i=1}^{r} f(1) \\ =& f(1)^{-r+1} f(1)^r \\ =& f(1), \end{aligned}$$

joten f on vakiofunktio. □

Esimerkki 6.2. Valitaan mielivaltainen $c \in \mathbb{C}$. Määritellään joukossa $\mathbb{Z}_+^\infty$ sellainen funktio f, että $f(n) = c$ kaikilla $n \in \mathbb{Z}_+^\infty$. Nyt f on ∞-unitaarisesti semimultiplikatiivinen. Tämä nähdään suoraan ∞-unitaarisen semimultiplikatiivisuuden määritelmästä, sillä $f(n)f(m) = c^2 = f((n,m)_{\oplus\oplus})f([n,m]_\infty^*)$ kaikilla $n, m \in \mathbb{Z}_+^\infty$. Esimerkin perusteella nähdään, että jokainen joukossa $\mathbb{Z}_\infty^*$ määritelty kompleksilukuarvoinen vakiofunktio on siis ∞-unitaarisesti semimultiplikatiivinen. Itse asiassa vakiofunktiot ovat aina myös pseudo-unitaarisesti semimultiplikatiivisia. (Ks. [9], s. 18)

Huomautus Yleisesti ottaen kaikki ∞-unitaarisesti semimultiplikatiiviset funktiot eivät kuitenkaan ole vakiofunktioita, sillä oletimme lauseessa 6.6, että funktio toteuttaa ∞-unitaarisen semimultiplikatiivisuuden lisäksi ehdon $f(p^a) \neq 0$ jokaisella $p \in \mathbb{P}$ ja $a \in \mathbb{Z}_+$.

6.4 p^∞-unitaarisesti semimultiplikatiiviset funktiot

Lause 6.7. *(Ks.[9], s. 18) Olkoon $f : \mathbb{Z}_+^* \to \mathbb{C}$ sellainen p^∞-unitaarisesti semimultiplikatiivinen funktio, että $f(1) = 1$ ja $f(p^2) \neq 0$ kaikilla alkuluvuilla p ja positiivisilla kokonaisluvuilla a. Tällöin*

(1) funktion f rajoittuma joukkoon $\mathbb{Z}_+$ on vahvasti multiplikatiivinen funktio ja

(2) $f(p^\infty) = f(p)^2$ kaikilla alkuluvuilla p.

Todistus. Valitaan sellaiset positiiviset kokonaisluvut m ja n, että $(m,n) = 1$. Määritelmän 6.3 kohdan (3) perusteella

$$f(m)f(n) = f((m,n)_{\oplus\oplus})f([m,n]_{p^\infty}^*).$$

Lauseen 3.8 perusteella nyt $(m,n)_{\oplus\oplus} = 1$ ja $[m,n]^*_{p^\infty} = mn$, joten

$$f(m)f(n) = f(1)f(mn) = f(mn).$$

Siis f on multiplikatiivinen. Valitaan mielivaltainen alkuluku p ja erisuuret positiiviset kokonaisluvut a ja b. Nyt $(p^a,p^b)_{\oplus\oplus} = 1$ ja $[p^a,p^b]^*_{p^\infty} = p^\infty$. Nyt

$$f(p^a)f(p^b) = f((p^a,p^b)_{\oplus\oplus}f([p^a,p^b]^*_{p^\infty}) = f(1)f(p^\infty) = f(p^\infty),$$

joten

$$f(p^a)f(p^b) = f(p^\infty)$$

kaikilla alkuluvuilla p ja positiivisilla kokonaisluvuilla a ja b, joilla $a \neq b$. Valitaan seuraavaksi $a = 1$ ja $b = u \geq 2$. Nyt siis

$$f(p)f(p^u) = f(p^\infty),$$

joten

$$f(p^u) = f(p^\infty)f(p)^{-1},$$

kun $u \geq 2$. Samoin saadaan, että

$$f(p)f(p^2) = f(p^\infty)$$

eli

$$f(p^2) = f(p^u) = f(p^\infty)f(p)^{-1},$$

kun $u \geq 2$. Toisaalta valinnoilla $a = 1$ ja $b = 3$, sekä $a = 2$ ja $b = 3$ saadaan

$$f(p)f(p^3) = f(p^2)f(p^3) = f(p^\infty),$$

siis

$$f(p) = f(p^2) = f(p^\infty)f(p^3)^{-1}.$$

On siis todistettu, että

$$f(p) = f(p^a),$$

kun $a \geq 1$. Näin ollen pätee myös, että

$$f(p)^2 = f(p)f(p) = f(p)f(p^2) = f(p^\infty).$$

□

Huomautus Käänteinen väite ei kuitenkaan päde. Yksinkertainen vastaesimerkki on sellainen funktio f, että $f(1) = 1$ ja $f(n) = 0$, kun $n \neq 1$.

Määritelmä 6.4. Olkoot $a,b \in \mathbb{Z}^\infty_+$. Määritellään joukossa $\mathbb{Z}^\infty_+$ alkioiden a ja b *minimi* $\min\{a,b\}$ siten, että

$$\min\{a,b\} = \begin{cases} a, & \text{jos } a,b \in \mathbb{Z}_+ \text{ ja } a \leq b \text{ tai } b = \infty \\ b, & \text{muuten.} \end{cases}$$

Määritelmä 6.5. Olkoot $m, n \in \mathbb{Z}_+^*$. Määritellään joukossa $\mathbb{Z}_+^*$ alkioiden $a = \prod_{p\in\mathbb{P}} p^{a_p}$ ja $b = \prod_{p\in\mathbb{P}} p^{b_p}$ *suurin yhteinen tekijä* (a, b) siten, että

$$(a, b) = \prod_{p\in\mathbb{P}} p^{\min\{a_p, b_p\}}.$$

Lause 6.8. *(Ks.[9], s. 18) Olkoon f joukossa $\mathbb{Z}_+^*$ määritelty kompleksilukuarvoinen funktio. Olkoon lisäksi $f(1) = 1$ ja $f(p^a) \neq 0$ jokaisella alkuluvulla p ja kokonaisluvulla a. Nyt*

$$f((m, n)_{\oplus\oplus})f([m, n]^*_{p^\infty}) = f(m)f(n) \text{ jokaisella } m, n \in \mathbb{Z}_+^*,$$

jos ja vain jos

(1) $f(mn) = f(m)f(n)$ jokaisella $m, n \in \mathbb{Z}_+^*$, joilla $(m, n) = 1$,

(2) $f(p^a) = f(p)$ jokaisella alkuluvulla p ja kokonaisluvulla a,

(3) $f(p^\infty) = f(p)^2$ jokaisella alkuluvulla p.

Todistus. Olkoon f joukossa $\mathbb{Z}_+^*$ määritelty sellainen kompleksilukuarvoinen funktio, että $f(1) = 1$ ja $f(p^a) \neq 0$ jokaisella alkuluvulla p ja kokonaisluvulla a. Oletetaan, että f on p^∞-unitaarisesti semimultiplikatiivinen. Nyt lauseen 6.7 mukaan funktion f rajoittuma joukkoon $\mathbb{Z}_+$ on vahvasti multiplikatiivinen, joten

$$f(p^a) = f(p)$$

ja lisäksi saman lauseen mukaan

$$f(p^\infty) = f(p)^2$$

jokaisella alkuluvulla p ja kokonaisluvulla a. On vielä todistettava, että

$$f(mn) = f(m)f(n)$$

kaikilla $m, n \in \mathbb{Z}_+^*$, joilla $(m, n) = 1$. Valitaan seuraavaksi sellaiset $m, n \in \mathbb{Z}_+^*$, että $(m, n) = 1$. Nyt jokaisella alkuluvulla p pätee, että $\min\{a_p, b_p\} = 0$. Siis joko $a_p = 0$ tai $b_p = 0$, joten

$$\begin{aligned}(m, n)_{\oplus\oplus} =& (2^{a_2}, 3^{a_3}, 5^{a_5}, \cdots) \wedge (2^{b_2}, 3^{b_3}, 5^{b_5}, \ldots)\\ =& (2^{a_2} \wedge 2^{b_2}, 3^{a_3} \wedge 3^{b_3}, 5^{a_5} \wedge 5^{b_5}, \ldots)\\ =& (1, 1, 1, \ldots) = 1.\end{aligned}$$

Toisaalta tällöin $p^{a_p} \vee p^{b_p} = p^{a_p+b_p}$, joten

$$\begin{aligned}[m, n]^*_{p^\infty} =& (2^{a_2}, 3^{a_3}, 5^{a_5}, \cdots) \vee (2^{b_2}, 3^{b_3}, 5^{b_5}, \ldots)\\ =& (2^{a_2} \vee 2^{b_2}, 3^{a_3} \vee 3^{b_3}, 5^{a_5} \vee 5^{b_5}, \ldots)\\ =& (2^{a_2+b_2}, 3^{a_3+b_3}, 5^{a_5+b_5}, \ldots) = mn.\end{aligned}$$

Koska f on p^∞-unitaarisesti semimultiplikatiivinen, niin

$$f(m,n)_{\oplus\oplus} f([m,n]^*_{p^\infty}) = f(1)f(mn) = f(mn).$$

Oletetaan seuraavaksi, että ehdot (1),(2) ja (3) pätevät. Todistetaan väite ensin kaikille alkuluvun potensseille. Olkoon p mielivaltainen alkuluku ja olkoot $a, b \in \mathbb{Z}_+^\infty$. Oletetaan ensin, että $p^a \parallel p^b$ (tai vastaavasti $p^b \parallel p^a$). Tällöin lauseen 3.1 mukaan $(p^a, p^b)_{\oplus\oplus} = p^a$ ja $[p^a, p^b]^*_{p^\infty} = p^b$, joten

$$f((p^a, p^b)_{\oplus\oplus}) f([p^a, p^b]^*_{p^\infty}) = f(p^a)f(p^b).$$

Jos $p^a \nparallel p^b$ ja $p^b \nparallel p^a$, niin $a, b \in \mathbb{Z}_+$ ja $a \neq b$. Tällöin

$$f((p^a, p^b)_{\oplus\oplus}) f([p^a, p^b]^*_{p^\infty}) = f(1)f(p^\infty) = 1f(p)^2 = f(p)^2.$$

Toisaalta

$$f(p^a)f(p^b) = f(p)f(p) = f(p)^2,$$

joten

$$f((p^a, p^b)_{\oplus\oplus}) f([p^a, p^b]^*_{p^\infty}) = f(p^a)f(p^b).$$

Väite pätee siis kaikille alkuluvun potensseille. Olkoon $n \in \mathbb{Z}_+^*$ sellainen alkio, että $n = \prod_{p\in\mathbb{P}} p^{a_p}$. Todistetaan seuraavaksi induktiolla alkulukutekijöiden lukumäärän suhteen, että

$$f(\prod_{p\in\mathbb{P}} p^{a_p}) = \prod_{p\in\mathbb{P}} f(p^{a_p}).$$

Jos luvulla n ei ole lainkaan alkulukutekijöitä, niin väite pätee, sillä tällöin

$$f(\prod_{p\in\mathbb{P}} p^{a_p}) = f(\prod_{p\in\mathbb{P}} 1) = f(1) = 1 = \prod_{p\in\mathbb{P}} 1 = \prod_{p\in\mathbb{P}} f(1) = \prod_{p\in\mathbb{P}} f(p^{a_p}).$$

Tehdään induktio-oletus, että väite pätee jokaisella luvulla jolla on k alkulukutekijää. Olkoon luvun n alkulukutekijöiden lukumäärä $k+1$. Olkoon p' jokin luvun n alkulukutekijöistä. Nyt luvulla $n/p'^{a_{p'}} = \prod_{p\in\mathbb{P}\setminus\{p'\}} p^{a_p}$ on k alkulukutekijää, joten induktio-oletuksen perusteella

$$f(\prod_{p\in\mathbb{P}\setminus\{p'\}} p^{a_p}) = \prod_{p\in\mathbb{P}\setminus\{p'\}} f(p^{a_p}).$$

Nyt $p'^{a_{p'}} \prod_{p\in\mathbb{P}\setminus\{p'\}} p^{a_p} = n$ ja $(p'^{a_{p'}}, \prod_{p\in\mathbb{P}\setminus\{p'\}} p^{a_p}) = 1$, joten ehdon (1) perusteella

$$\begin{aligned} f(p'^{a_{p'}} \prod_{p\in\mathbb{P}\setminus\{p'\}} p^{a_p}) &= f(p'^{a_{p'}}) \prod_{p\in\mathbb{P}\setminus\{p'\}} f(p^{a_p}) \\ &= \prod_{p\in\mathbb{P}} f(p^{a_p}). \end{aligned}$$

Olkoot $m, n \in \mathbb{Z}_+^*$. Merkitään $m = \prod_{p\in\mathbb{P}} f(p^{a_p})$ ja $n = \prod_{p\in\mathbb{P}} f(p^{b_p})$. Nyt

$$\begin{aligned}
f((m,n)_{\oplus\oplus})f([m,n]^*_{p^\infty}) =& f(\prod_{p\in\mathbb{P}}(p^{a_p},p^{b_p})_{\oplus\oplus})f(\prod_{p\in\mathbb{P}}[p^{a_p},p^{b_p}]^*_{p^\infty}) \\
=& \prod_{p\in\mathbb{P}} f((p^{a_p},p^{b_p})_{\oplus\oplus}) \prod_{p\in\mathbb{P}} f([p^{a_p},p^{b_p}]^*_{p^\infty}) \\
=& \prod_{p\in\mathbb{P}} f((p^{a_p},p^{b_p})_{\oplus\oplus})f([p^{a_p},p^{b_p}]^*_{p^\infty}) \\
=& \prod_{p\in\mathbb{P}} f(p^{a_p})f(p^{b_p}) \\
=& \prod_{p\in\mathbb{P}} f(p^{a_p}) \prod_{p\in\mathbb{P}} f(p^{b_p}) \\
=& f(\prod_{p\in\mathbb{P}} p^{a_p})f(\prod_{p\in\mathbb{P}} p^{b_p}) \\
=& f(m)f(n).
\end{aligned}$$

□

Lause 6.9. *(Ks.[9], s. 19) Olkoon f aritmeettinen funktio. Jos f on vahvasti multiplikatiivinen, niin f on astetta $(1,1)$ oleva aritmeettinen rationaalifunktio.*

Todistus. Olkoon p mielivaltainen alkuluku. Koska f on vahvasti multiplikatiivinen, niin funktion f Bellin sarjaksi saadaan

$$\begin{aligned}
f_p(x) =& \sum_{n=0}^{\infty} f(p^n)x^n \\
=& f(1) + \sum_{n=1}^{\infty} f(p^n)x^n \\
=& f(1) + \sum_{n=1}^{\infty} f(p)x^n \\
=& 1 + f(p)\sum_{n=1}^{\infty} x^n \\
=& 1 + \frac{f(p)x}{1-x} \\
=& \frac{1-(1-f(p))x}{1-x}.
\end{aligned}$$

Nyt lauseen 3.20 mukaan f on astetta $(1,1)$ oleva aritmeettinen rationaalifunktio. □

Esimerkki 6.3. (Ks. [9], s. 19) Määritellään joukossa $\mathbb{Z}^*_{p^\infty}$ sellainen kompleksilukuarvoinen funktio f, että

$$
\begin{aligned}
&f(1) = 1,\\
&f(p^a) = p \text{ kaikilla } p \in \mathbb{P} \text{ ja } a \in \mathbb{Z}_+,\\
&f(p^\infty) = p^2,\\
&f(mn) = f(m)f(n) \text{ kaikilla } m, n \in \mathbb{Z}^*_+, \text{ joilla } (m, n) = 1.
\end{aligned}
$$

Lauseen 6.8 mukaan f on p^∞-unitaarisesti semimultiplikatiivinen. Funktio f ei kuitenkaan ole ∞-unitaarisesti semimultiplikatiivinen. Tämä nähdään lauseen 6.6 perusteella, sillä tällöin funktion f rajoittuman joukkoon $\mathbb{Z}_+$ tulisi olla vakiofunktio, sillä $f(1) = 1$ ja $f(p^a) \neq 0$ kaikilla alkuluvuilla p ja positiivisilla kokonaisluvuilla a. Selvästikään funktion f rajoittuma joukkoon $\mathbb{Z}_+$ ei kuitenkaan ole vakiofunktio, sillä esimerkiksi $f(2) = 2 \neq 1 = f(1)$.

Viitteet

[1] Cohen, Eckford: *Arithmetical functions associated with the unitary divisor of an integer*, Mathematische Zeitschrift, Vol. 74, No. 1, 1960, s. 66-80.

[2] Dugundji, James: *Topology*, Allyn and Bacon Inc., Boston, 1967.

[3] Eronen, Mika: *Hilateoriaa*, Matematiikan, tilastotieteen ja filosofian laitos, moniste B50, 1999.

[4] Friedberg, Stephen H.; Insel, Arnold J. & Spence, Lawrence E.: *Linear algebra*, Pearson Education Inc., New Jersey, 2003.

[5] Gantmacher, F.R.: *The theory of matrices*, Chelsea Publishing Company, New York, 1977.

[6] Hansen, Rodney T. & Swanson, Leonard G.: *Unitary divisors*, Mathematics Magazine, Vol. 52, 1979, s. 217-222.

[7] Haukkanen, Pentti: *Algebra I*, luentomoniste. `http://mtl.uta.fi/Opetus/Algebra/algI04.pdf`, (27.8.2008).

[8] Haukkanen, Pentti: *Lukuteoriaa*, luentomoniste. `http://mtl.uta.fi/Opetus/Algebra/Lukuteoria/lukuteoria.pdf`, (2.7.2008).

[9] Haukkanen, Pentti; Ilmonen, Pauliina; Nalli, Ayse & Sillanpää, Juha: *On unitary analogs of GCD reciprocal LCM matrices*, käsikirjoitus, 2007, hyväksytty julkaistavaksi lehdessä Linear and Multilinear Algebra.

[10] Hella, Lauri: *Joukko-oppi*, luentomoniste. `http://mtl.uta.fi/Opetus/Joukko-oppi/JOuusi.pdf`, (26.8.2008).

[11] Kelley, John L.: *General topology*, American Book Company, New York, 1969.

[12] Korkee, Ismo: *On meet and join matrices associated with incidence functions*, Tampere University Press, Tampere, 2006.

[13] Sivaramakrishnan, R.: *Classical theory of arithmetic functions*, Marcel Dekker Inc., New York, 1989.

[14] Tanana, B.P. & Shevrin, L.N.: *Springer online reference works: Topological semi-group*, verkkolähde. `http://eom.springer.de/T/t093120.htm`, (20.10.2008).

[15] Vaidyanathaswamy, R.: *The theory of multiplicative arithmetic functions*, Transactions of American Mathematical Society, Vol. 33, No. 2, 1931, 579-662.

[16] Väisälä, Jussi: *Topologia II*, Limes Ry, Helsinki, 1999.