MATEMATIIKAN JOUKKO-OPILLISIA PERUSTEITA

Simo Hämäläinen

Pro gradu -tutkielma
Helmikuu 2011

MATEMATIIKAN LAITOS
TURUN YLIOPISTO

TURUN YLIOPISTO
Matematiikan laitos

HÄMÄLÄINEN, SIMO: Matematiikan joukko-opillisia perusteita
Pro gradu -tutkielma, 78 s.
Matematiikka
Helmikuu 2011

Tutkielman aiheena on joidenkin matematiikan peruskäsitteiden esittäminen joukko-opin keinoin. Muun muassa järjestetyt parit eli kahden komponentin vektorit ja luonnolliset luvut voidaan kohtalaisen yksinkertaisesti esittää pelkistettyinä joukkoina. Pelkistetyt joukot ovat joukkoja, joiden kaikki jäsenet, jäsenten jäsenet ja niin edespäin ovat joukkoja.

Määritelmät ja todistukset esitetään formalismin hengessä matemaattisella symbolikielellä. Tarkoitus on varmistua, että perustelut todella noudattavat tutkielman alussa asetettuja sääntöjä ja sopimuksia ja perustuvat tutkielmassa esitettyihin aksioomiin. Aksiomaattisen joukko-opin suhdetta intuitioon perustuvaan naiiviin joukko-oppiin pyritään selvittämään perustelemalla syitä eri aksioomien asettamiselle.

Monen asetetun aksiooman tarkoitus on mahdollistaa uusien joukkojen muodostaminen tai toisin ilmaisten kertoa, minkälaisia joukkoja on olemassa. Tällaisia aksioomia asetettaessa on oltava varovainen, jottei teoria ajaudu ristiriitaan. Joukkoja on voitava määritellä esimerkiksi ominaisuuden perusteella, jonka täyttävät alkiot valitaan joukon jäseniksi. Siksi esitetään separaatioaksiooma, jonka muoto on niin kutsutun Russellin paradoksin vuoksi harkittava tarkoin.

Lopuksi tarkastellaan lyhyesti äärettömiä joukkoja ja joukkoina esitettyjen luonnollisten lukujen yhteenlaskua. Yksinkertaisuudestaan huolimatta äärettömyyden ja yhteenlaskun käsitteet osoittautuvat tämän tutkielman puitteissa liian hankaliksi, kun ne yritetään esittää täsmällisen formaalisesti.

Asiasanat: Aksioomat, formalismi, joukko-oppi, matematiikan perusteet, luonnolliset luvut.

1. $((\mathrm{A} \wedge \mathrm{B}) \Leftrightarrow \neg(\mathrm{A} \Rightarrow \neg\mathrm{B}))$
2. $((\mathrm{A} \vee \mathrm{B}) \Leftrightarrow (\neg\mathrm{A} \Rightarrow \mathrm{B}))$
3. $((\mathrm{A} \Leftrightarrow \mathrm{B}) \Leftrightarrow \neg((\mathrm{A} \Rightarrow \mathrm{B}) \Rightarrow \neg(\mathrm{B} \Rightarrow \mathrm{A})))$
4. $(\neg\neg\mathrm{A} \Leftrightarrow \mathrm{A})$
5. $((\mathrm{A} \vee \mathrm{B}) \Leftrightarrow (\mathrm{B} \vee \mathrm{A}))$
6. $(\neg(\mathrm{A} \vee \mathrm{B}) \Leftrightarrow (\neg\mathrm{A} \wedge \neg\mathrm{B}))$
7. $(\neg(\mathrm{A} \wedge \mathrm{B}) \Leftrightarrow (\neg\mathrm{A} \vee \neg\mathrm{B}))$
8. $((\mathrm{A} \Rightarrow \mathrm{B}) \Leftrightarrow (\neg\mathrm{B} \Rightarrow \neg\mathrm{A}))$
9. $((\mathrm{A} \vee \mathrm{A}) \Leftrightarrow \mathrm{A})$
10. $((\mathrm{A} \Rightarrow (\mathrm{B} \Rightarrow \mathrm{C})) \Leftrightarrow (\mathrm{B} \Rightarrow (\mathrm{A} \Rightarrow \mathrm{C})))$
11. $((\mathrm{A} \Rightarrow (\mathrm{B} \Rightarrow \mathrm{C})) \Leftrightarrow ((\mathrm{A} \wedge \mathrm{B}) \Rightarrow \mathrm{C}))$
12. $(((\mathrm{A} \wedge \mathrm{B}) \Rightarrow (\mathrm{B} \Rightarrow \mathrm{C})) \Leftrightarrow ((\mathrm{A} \wedge \mathrm{B}) \Rightarrow \mathrm{C}))$
13. $((\mathrm{A} \wedge (\mathrm{B} \wedge \mathrm{C})) \Leftrightarrow ((\mathrm{A} \wedge \mathrm{B}) \wedge \mathrm{C}))$
14. $((\mathrm{A} \vee (\mathrm{B} \vee \mathrm{C})) \Leftrightarrow ((\mathrm{A} \vee \mathrm{B}) \vee \mathrm{C}))$
15. $(((\mathrm{A} \Rightarrow \mathrm{B}) \wedge (\mathrm{A} \Rightarrow \mathrm{C})) \Leftrightarrow (\mathrm{A} \Rightarrow (\mathrm{B} \wedge \mathrm{C})))$
16. $(((\mathrm{A} \vee \mathrm{B}) \wedge (\mathrm{C} \vee \mathrm{B})) \Leftrightarrow ((\mathrm{A} \wedge \mathrm{C}) \vee \mathrm{B}))$
17. $((\mathrm{A} \Rightarrow \mathrm{B}) \Leftrightarrow ((\mathrm{B} \wedge \mathrm{A}) \Leftrightarrow \mathrm{A}))$
18. $(((\mathrm{A} \wedge \neg\mathrm{A}) \vee \mathrm{B}) \Leftrightarrow \mathrm{B})$
19. $(\mathrm{A} \Leftrightarrow \mathrm{A})$
20. $(\mathrm{A} \Rightarrow \mathrm{A})$
21. $((\mathrm{A} \Leftrightarrow \mathrm{B}) \Leftrightarrow (\neg\mathrm{A} \Leftrightarrow \neg\mathrm{B}))$
22. $(\mathrm{A} \Rightarrow (\mathrm{B} \Rightarrow \mathrm{A}))$
23. $(\mathrm{A} \Rightarrow (\mathrm{B} \Rightarrow (\mathrm{A} \wedge \mathrm{B})))$
24. $((\mathrm{A} \Rightarrow \mathrm{B}) \Rightarrow ((\mathrm{B} \Rightarrow \mathrm{C}) \Rightarrow (\mathrm{A} \Rightarrow \mathrm{C})))$
25. $((\mathrm{A} \Leftrightarrow \mathrm{B}) \Rightarrow (\mathrm{A} \Rightarrow \mathrm{B}))$
26. $(\mathrm{A} \Rightarrow (\mathrm{A} \vee \mathrm{B}))$
27. $(((\mathrm{A} \Rightarrow \mathrm{B}) \wedge (\mathrm{C} \Rightarrow \mathrm{B})) \Rightarrow ((\mathrm{A} \vee \mathrm{C}) \Rightarrow \mathrm{B}))$
28. $(((\mathrm{A} \Leftrightarrow \mathrm{B}) \wedge \mathrm{A}) \Rightarrow \mathrm{B})$
29. $(((\mathrm{A} \Rightarrow \mathrm{B}) \wedge (\mathrm{C} \Rightarrow \mathrm{D})) \Rightarrow ((\mathrm{A} \vee \mathrm{C}) \Rightarrow (\mathrm{B} \vee \mathrm{D})))$
30. $(((\mathrm{A} \vee \mathrm{B}) \wedge \mathrm{C}) \Rightarrow ((\mathrm{A} \wedge \mathrm{C}) \vee (\mathrm{B} \wedge \mathrm{C})))$
31. $(\mathrm{A} \Rightarrow (\neg\mathrm{A} \Rightarrow \mathrm{B}))$
32. $((\mathrm{A} \wedge \mathrm{B}) \Rightarrow \mathrm{A})$
33. $((\mathrm{A} \Leftrightarrow (\mathrm{B} \wedge \mathrm{C})) \Rightarrow (\mathrm{B} \Rightarrow (\mathrm{A} \Leftrightarrow \mathrm{C})))$
34. $((\mathrm{A} \Rightarrow \mathrm{B}) \Rightarrow ((\mathrm{C} \wedge \mathrm{A}) \Rightarrow \mathrm{B}))$
35. $(((\mathrm{A} \vee \mathrm{B}) \Rightarrow \mathrm{C}) \Rightarrow (\mathrm{A} \Rightarrow \mathrm{C}))$
36. $((((\mathrm{A} \wedge \mathrm{B}) \Rightarrow \mathrm{D}) \wedge ((\mathrm{A} \wedge \mathrm{C}) \Rightarrow \mathrm{D})) \Leftrightarrow ((\mathrm{A} \wedge (\mathrm{B} \vee \mathrm{C})) \Rightarrow \mathrm{D}))$
37. $((\mathrm{A} \Rightarrow (\mathrm{B} \wedge (\mathrm{B} \Rightarrow \mathrm{C}))) \Rightarrow (\mathrm{A} \Rightarrow \mathrm{C}))$
38. $(((\mathrm{A} \wedge \mathrm{B}) \vee \mathrm{C}) \Rightarrow (\mathrm{A} \vee \mathrm{C}))$
39. $((\mathrm{A} \wedge (\mathrm{B} \vee \mathrm{C})) \Rightarrow ((\mathrm{A} \wedge \mathrm{C}) \vee \mathrm{B}))$

kvs(n)
- Jos x ei esiinny A:ssa: $(\forall x\mathrm{A}x \Leftrightarrow \mathrm{A})$ ja $(\exists x\mathrm{A}x \Leftrightarrow \mathrm{A})$.
- Jos x ei esiinny A:ssa: $(\forall x(\mathrm{A} \Rightarrow \mathrm{B})x \Leftrightarrow (\mathrm{A} \Rightarrow \forall x\mathrm{B}x))$ ja $(\exists x(\mathrm{A} \Rightarrow \mathrm{B})x \Leftrightarrow (\mathrm{A} \Rightarrow \exists x\mathrm{B}x))$.
- $(\forall x(\mathrm{A} \wedge \mathrm{B})x \Leftrightarrow (\forall y\mathrm{A}(y/x)y \wedge \forall z\mathrm{B}(z/x)z))$
- $(\forall x\mathrm{A}x \Leftrightarrow \neg\exists y\neg\mathrm{A}(y/x)y)$

ekvmp $((\exists x\mathrm{A}x \wedge (\mathrm{A} \Rightarrow \mathrm{B})) \Rightarrow \exists y\mathrm{B}(y/x)y)$

$\exists\leftarrow$(n) Jos todistusrivi n on lause $\exists x\mathrm{A}x$ ja x esiintyy A:ssa, niin todistukseen saa kirjoittaa rivin $\mathrm{A}x \leftarrow a$, jossa a on todistukseen nähden uusi muuttuja.

sij(n) Jos rivi n on sijoitusmerkintä $\mathrm{A}x \leftarrow a$, niin todistukseen saa kirjoittaa rivin $\mathrm{A}(a/x)$.

$\exists$ Jos A on kaava ja a on vakio, joka esiintyy kaavassa A, ja jos x on muuttuja, joka ei esiinny kaavassa A, niin $(\mathrm{A} \Rightarrow \exists x\mathrm{B}x)$ on kaavamalli. B on kaava, joka on saatu vaihtamalla vähintään yksi vakion a esiintymistä kaavassa A muuttujalla x.

$\forall\leftarrow$ Jos A on kaava ja y on muuttuja tai vakio, $(\forall x\mathrm{A}x \Rightarrow \mathrm{A}(y/x))$ on kaavamalli. Jos y on vakio, sen pitää olla todistuksessa sijoitusmerkinnässä tai väitteen oletuksena esitelty vakio.

$\forall$(n) Jos todistusrivi n on kaava A ja x ei ole kaavassa A sidottu muuttuja, niin todistukseen saa kirjoittaa rivin $\forall x\mathrm{A}x$.

Sisältö

1 Johdanto **1**

2 Symbolit **7**

2.1 Kaavat ja symbolien käyttö 8

2.2 Kaavojen keskinäiset suhteet ja kaavamallit 13

2.3 Formaalinen määritelmä ja todistus 17

2.4 Kvanttoreita koskevat päättelysäännöt 20

3 Joukot **25**

3.1 Joukko-opin symbolit ja kuulumisrelaatio 26

3.2 Unioni, leikkaus, potenssijoukko ja kahden joukon yhdiste . . . 30

3.3 Tyhjästä on hyvä nyhjästä 35

3.4 Joukot, luokat ja separaatioaksiooma 39

3.5 Identtisyys 44

3.6 Relaatio, funktio ja mahtavuus 49

3.7 Joukkojen hierarkia 57

4 Luvut **61**

4.1 Luonnolliset luvut joukkoina 61

4.2 Luonnolliset luvut joukkona 64

4.3 Äärettömyys ja luonnollisten lukujen yhteenlasku 68

5 Lopuksi **73**

Kirjallisuutta **77**

1 Johdanto

Tämän pro gradu -tutkielman pääaihe on joukko-oppi matematiikan perusteiden näkökulmasta. Tarkemmin pyritään osoittamaan, miten tiettyjä matematiikan peruskäsitteitä, etenkin luonnolliset luvut, voidaan esittää joukko-opin keinoin. Tähän kaikkeen pyritään pragmaattisen formalistisella otteella, jotta todistukset eivät jäisi mielikuvituksen varaan vaan pääteltäisiin määrättyihin sääntöihin vedoten. Koska logiikka ei ole tutkielman pääaihe, matematiikan loogista päättelyä koskevat säännöt kuitenkin oletetaan ennalta tunnetuiksi, eikä niitä tässä tutkielmassa täsmällisesti perustella.

Tutkielman teema on matemaattisten tulosten luotettavuus. Tarkoitus on mahdollisimman pitkälle edetä niin pienin askelin, että lukijan on koko ajan mahdollista hyväksyä tuloksiin johtavat päättelyketjut. Tämä vaatii kuitenkin sitä, että lukija hyväksyy toisessa luvussa esitetyt päättelyä koskevat sopimukset ja sen jälkeen kulloinkin asetetut joukko-oppia koskevat aksioomat. Yrityksenä on myös auttaa tarkkailemaan, miten esitetyt aksioomat laillistavat tai eivät laillista joitakin intuitiivisia käsityksiä joukko-opista.

Matematiikan todistuksia on syytä tarkkailla kriittisesti. Otetaan esimerkki todistuksesta, joka vetoaa mielikuvitukseen sillä tavalla, että todistus tuntuu täysin pätevältä. Tunnettu todistus reaalilukujen ylinumeroituvuudesta etenee seuraavasti: Oletetaan, että reaalilukujen joukko välillä $(0, 1)$ on numeroituva. Koska se on numeroituva, voidaan olettaa annetuksi lista, jonka n:s rivi on n:s reaaliluku lukuvälillä $(0, 1)$. Muodostetaan uusi reaaliluku r seuraavasti: jos n:nnen luvun n:s desimaali on 5, luvun r n:s desimaali on 4, ja jos n:nnen luvun n:s desimaali on jotain muuta, niin luvun r n:s desimaali on 5. Luku r ei esiinny oletetulla listalla. Siispä tällaista listaa ei ole ja reaalilukujen joukko lukuvälillä $(0, 1)$ on ylinumeroituva.

Saman tapainen argumentti voidaan esittää sille, että rationaalilukujen joukko on ylinumeroituva. Oletetaan, että on annettu numeroituva lista, jossa on kaikki rationaaliluvut väliltä $(0, 1)$. Tehdään seuraava operaatio järjestyksessä rivi riviltä: Jos rivin n luvun n:s desimaali on yhtäsuuri kuin luvun n jakojäännös 10:llä jakaessa eli ensimmäisen rivin ensimmäinen desimaali on 1, 34. rivin 34. desimaali on 4, 867. rivin 867. desimaali on 7 ja niin poispäin, niin rivi jätetään paikoilleen. Jos taas näin ei ole, rivi vaihdetaan ensimmäiseen sellaiseen kyseisen rivin *jälkeiseen* riviin, että ehto toteutuu. Oletetaan, että supersuorituksella (engl. *supertask*, [13]: s. 37, 177) tällä tavalla voidaan

käydä läpi koko lista. Huomataan, että uuden listan diagonaaliluvuksi tulee 0,12345678901234567890... eli $0,\overline{1234567890}$. Siispä luku $0,\overline{0123456789}$ ei voi kuulua listaan, vaikka onkin rationaaliluku. Samaan tapaan kuin reaalilukujen tapauksessa päätellään, että rationaalilukujen joukko on ylinumeroituva. (Esimerkki on Antonio Leon Sanchezin artikkelista [9].)

Todistukset ovat aika lailla samanlaisia, mutta toisen perustelu on pätevä ja toisen väärä. Mitä sellaista toisessa todistuksessa on väärin, mikä ei ole väärin ensimmäisessäkin todistuksessa? Eikö listaa saisi järjestää uudestaan, vaikka tiedetään, että toisessa todistuksessa kuvailtu prosessi voidaan suorittaa mille tahansa listan luvulle? Miksi numeroituvasti ääretön lista voidaan ensinkään olettaa mahdolliseksi, jos sen uudestaan järjestämistä ei voi hyväksyä? Sanchez kiinnittää huomion tällaisen oletetun listan outoon epäsymmetrisyyteen: mitä tahansa listan lukua edeltää äärellinen määrä ja seuraa ääretön määrä lukuja ([9]: 11).

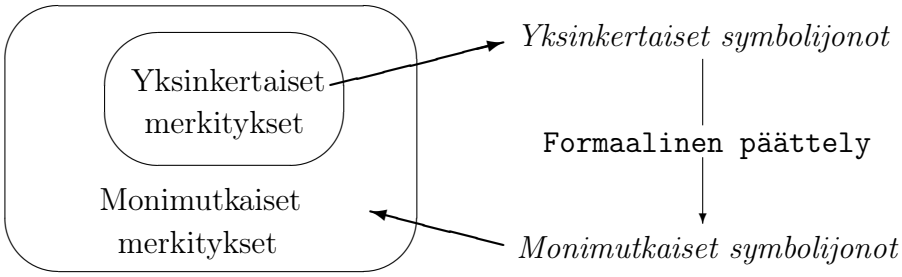
Todistus voi olla hämäävä myös siten, ettei lukija huomaa, mitä oletamuksia todistus vaatii. John Mayberry osoittaa lyhyellä perustelulla, että säännöllisyysperiaatetta noudattamattomalla joukolla x on jäsenet x_1, x_2, x_3, ..., jotka muodostavat loputtoman kuuluvuusrelaation suhteen laskevan jonon $\ldots \in x_3 \in x_2 \in x_1 \in x$ (tai äärellisen silmukan, jos joillakin eri indekseillä i ja j $x_i = x_j$). Säännöllisyysperiaatteen (engl. *principle of regularity*) mukaan nimittäin kaikista joukoista y löytyy sellainen jäsen z, että $(z \cap y) = \emptyset$. Jos siis x ei noudata tätä periaatetta, voidaan löytää sellaiset joukon x jäsenet $x_1, x_2, x_3, \ldots$, että $x_1 \in x$, $x_2 \in (x_1 \cap x)$, $x_3 \in (x_2 \cap x)$ ja niin edelleen. Mayberry huomauttaa, että tässä jotenkin niin jokapäiväisen matemaattisessa todistuksessa tarvitaan valinta-aksioomaa. ([12]: s. 148, 149.) Perustelu tuntuu helpolta, mutta mistä oikein voi huomata, mitä periaatteita tai aksioomia todistus tarvitsee?

Muun muassa tällaisten todistuksia koskevien kysymysten vuoksi päämääränä on matemaattisesti tarkka aksiomaattinen esitys. Pyrkimys yksinkertaisuuteen, yksiselitteisyyteen ja yhtenäisyyteen sekä muihin matematiikan hyveisiin ei tee työtä helpoksi. Päinvastoin, kun matematiikkaa koetetaan puhdistaa inhimillisen ajattelun heikkouksista, inhimillisen ajattelijan on yhä vain vaikeampi sitä käsittää. Aksiomaattisen esityksen tarkoitus on silti helposti ymmärrettävä. Idealistisesti matematiikan esittäminen aksiomaattisesti tarjoaa keinon tietää jotain varmasti: kunhan ensin hyväksyy muutaman välttämättä oletettavan itsestäänselvyyden, pettämättömät matemaattiset

todistukset tarjoavat loputtomasti hienoja ja hämmästyttäviä tuloksia.

Formalismi tarjoaa keinon pettämättömien matemaattisten todistusten esittämiseen. Tällä koneaivojen aikakaudella mikään ei ole vakuuttavampaa, kuin että väitteet ja päättelyketjut voidaan esittää muodossa, jonka tietokonekin voi ymmärtää. Formalismin ajatus – ainakin käytännönläheisen matemaatikon[1] mielestä – on formalisoida perustavaa laatua olevat ja kaikkien hyväksymät helpot merkitykset symbolijonoiksi, asettaa symboleja ja symbolijonoja koskevia kaikkien hyväksymiä sääntöjä ja sitten sopia, ettei symboleilla ja niitä koskevilla säännöillä ole minkäänlaista intuitiivista merkitystä. Sääntöjen ja valmiiksi hyväksyttyjen symbolijonojen avulla muodostetaan uusia ja taas uusia teorian osaksi hyväksyttäviä symbolijonoja, jotka sitten muutetaan ikään kuin takaisin informaalisiksi merkityksiksi.

Näin päättelyprosesseissa ja tuloksissa ei ole kiistanalaisuutta, kunhan vain ensin päästään yksimielisyyteen yksinkertaisten merkitysten formalisoinnista ja formaalista päättelyä koskevista säännöistä. Kun formaalisella päättelyllä on saavutettu kiistattomia ja monimutkaisia tuloksia, niiden "deformaalistetut" merkitykset ovat niin ikään kiistattomia, vaikkeivät ne intuitiivisesti silti tuntuisikaan. Ideaa voitaisiin havainnollistaa kuvalla.



Yksinkertaisten intuitiivisten ja matemaattisten totuuksien suhdetta hieman eri näkökulmasta kuvailevat Alfred Whitehead ja Bertrand Russell teoksensa *Principia mathematica* esipuheessa ([19]: sivu v):

> [T]he early deductions . . . give reasons rather for believing the premisses because true consequenses follow from them, than for believing the consequenses because they follow from the premisses.

Matematiikan formaalistavien aksioomien täytyy siis tuottaa yksinkertaiset

[1] Jos matematiikka ajatellaan filosofian osa-alueeksi, matematiikka edustaa käytännöllistä filosofiaa parhaimmillaan: matematiikassa on tarkoitus saavuttaa tuloksia, ei vain kyseenalaistaa niitä.

intuitiiviset tulokset luotettavasti, jotta niiden aiheuttamiin monimutkaisiin tuloksiin voidaan luottaa.

Formalismi ei kuitenkaan ole näin yksinkertainen oikotie onneen. Mahdollisimman varmoilla tuloksilla ja yksinkertaiseksi karsitulla symbolikielellä on hintansa. A. Mathias osoittaa artikkelissaan [10], että kun Nicolas Bourbaki kirjassaan [3] määrittelee merkin 1 tarkoittamaan joukon $\{\emptyset\}$ kardinaliteettia, määritelmä on lyhennysmerkintöjen purkamisen jälkeen Bourbakin esittelemän seitsemän symbolin avulla kirjoitettuna 4 523 659 424 929 symbolin pituinen. Tämän ongelman takia tuntuu helposti käyvän niin, että käsitteille annetaan perusteellinen määritelmä mutta käytännössä käsitteitä sovelletaan intuition eikä määritelmän ohjaamana. Tässä tutkielmassa tällaista käytäntöä vältetään mahdollisimman pitkälle, mutta mahtavuuden määritelmä 3.24 osoittautuu ylivoimaiseksi formaalisessa todistuksessa käytettäväksi.

Toinen ongelma liittyy formaalisten tulosten muuttamiseen merkityksiksi. Esimerkiksi joukko-opin avulla esitetään, että luonnollinen luku 0 on tyhjä joukko ja 1 on joukko, joka sisältää vain ja ainoastaan tyhjän joukon. Miten ihmeessä nämä muka ovat lukuja? Perusteluksi voidaan sanoa, että nämä ja muut joukkoina esitetyt luonnolliset luvut täyttävät luonnollisille luvuille esitetyt ehdot. Todellisuudessa kuitenkin – myönnettäköön – formaalisen esityksen erikoisuuksiin täytyy totuttautua altistumalla niille jatkuvasti, jotta hyväksyy ne intuitiivisen käsityksen vastineiksi. Siispä asiaan perehtyneiden mielestä formaaliset päätelmät antavat hyviä tuloksia intuition matemaattisille oliolle, kun taas formalismille altistumaton voi olla sitä mieltä, etteivät formaaliset päätelmät edes koske intuitiivista matematiikkaa.

Perinteisesti aksiomaattisen esityksen on täytettävä kolme vaatimusta: sen on oltava *riippumaton*, *täydellinen* ja *ristiriidaton*. Riippumattomuus tarkoittaa sitä, ettei mikään perusolettamuksista saa olla johdettavissa muista perusolettamuksista. Täydellisyys tarkoittaa sitä, että jokainen mahdollinen muodostettavissa oleva lause on todistettavissa todeksi tai epätodeksi. Ristiriidattomuus vaatii, etteivät kaikki lauseet ole tosia. Jos kaikki lauseet olisivat tosia, löytyisi keskenään ristiriitaisia tosia lauseita. Toisaalta päättelysääntöjen mukaan kaikki lauseet ovat tosia, jos löydetään kaksi keskenään ristiriitaista lausetta.

Pragmaattisuuden nimissä tämä tutkielma myöntää itselleen erivapauden hylätä riippumattomuuden ja täydellisyyden vaatimukset. Tarkoitus on saada tuloksia vaikka sitten olettamalla toisistaan riippuvia totuuksia. Toisaalta

tarkoitus on myös hyväksyä todistettujen tuloksien muodostama teoria, vaikka teoriaa olisi jopa mahdotonta osoittaa täydelliseksi. Ristiriidattomuuden vaatimusta ei voi kuitenkaan edes tulosten saavuttamisen nimissä hylätä; ristiriitainen teoria on arvoton. Ristiriidattomuuden osoittaminen ei kuitenkaan ole täysin yksinkertaista, mikä tulee ilmi esimerkiksi Nicolas Bourbakin teoksen *Théorie des ensembles* johdannossa ([2]: s. 9):

> Toutefois, depuis 40 ans qu'on a formulé avec assez de précision les axiomes de cette théorie et qu'on s'est appliqué à en tirer des conséquences dans les domaines les plus variés des mathématiques, on n'a jamais rencontré de contradiction, et on est fondé à espérer qu'il ne s'en produira jamais.

Ristiriidattomuuden osoittamisen työläyden vuoksi tässä tutkielmassa on tyytyminen siihen luottamukseen, että matematiikan perusteita vuosien ajan tutkineet matemaatikot ovat saaneet aikaan luotettavia tuloksia. Tutkielma ei kuitenkaan seuraa täsmällisesti mitään tiettyä matematiikan perusteista tehtyä edes jossain määrin vakiintunutta ja hyväksyttyä esitystä vaan pyrkii sulauttamaan monien kirjoittajien – onneksi maineikkaiden kirjoittajien – ajatuksia ja ideoita. Nämä ajatukset ja ideat ovat luonnollisestikin sulautuneet kirjoittajan matemaattisesti vielä harmittavan harjaantumattomissa ajatteluprosesseissa. Täten se, etteivät tutkielmassa esitetyt päättelysäännöt ja aksioomat johda ristiriitaan, jää uskon kysymykseksi.

Esityksessä pyritään täyttämään seuraavat kohdat, jotka John Mayberryn mukaan aksiomaattisen esityksen on toteuttava: teoriaan on sisällytettävä (1) ensikäsitteet, joilla kaikki muut käsitteet määritellään, (2) määrittelemistä koskevat säännöt, (3) perusolettamukset, joille kaikki todistukset perustuvat, sekä (4) todistamista koskevat säännöt ([11]: s. 18). Selvä jako tehdään määritelmien, todistusten ja lauseiden eli todistettujen tulosten sekä määrittelemistä ja todistamista koskevien sääntöjen välillä. Määritelmät, todistukset ja lauseet ovat teorian symbolijonoja, kun taas määrittelemistä ja todistamista koskevat säännöt esitetään yksiselitteisyyteen pyrkivällä luonnollisella kielellä.

On hyvä huomata, että luonnolliseen kieleen tukeutuminen on välttämätöntä. Matemaattiset määritelmät ja todistukset pyritään kyllä esittämään symboleilla, mutta määritelmiä ja todistuksia koskevat säännöt ovat ikään kuin eri tasolla. Nämä säännöt on esitettävä muutoin kuin matematiikan

symbolikielen keinoin, koska ennen tällaisten sääntöjen esittämistä ei ole olemassa matematiikan symbolikielen keinoja. Siitä syystä erehdyksille alttein osa tutkielmassa on ehkäpä toinen luku, joka esittelee käytettävien symbolien käyttösäännöt.

Tutkielma perustuu pääasiallisesti teoksiin *Théorie des ensembles* (Nicolas Bourbaki, [2]), *Einleitung in die Mengenlehre* (Abraham Fraenkel, [7]), *Foundations of set theory* (Abraham Fraenkel, Yehoshua Bar-Hillel ja Azriel Levy, [8]), *The foundations of mathematics in the theory of sets* (John Mayberry, [12]) ja *Set theory and its philosophy* (Michael Potter, [13]). Innoittajana on ollut myös Whiteheadin ja Russellin *Principia mathematica* [19]. Muita lähteitä on mainittu niissä yhteyksissä, joissa niitä on tarvittu. Tutkielman matematiikan perusteita esittelevän luonteen vuoksi tutkielman lukemiseen ei varsinaisesti tarvita esitietoja matematiikan alalta, mutta todellisuudessa ainakin niin sanotun naiivin joukko-opin tuntemus on huomattavaksi eduksi.

2 Symbolit

Symbolit ovat keino matematiikan esittämiseen formaalisesti. Matemaattisen symbolikielen tulisi erota luonnollisesta kielestä siinä, että säännönmukaisesti muodostetut symbolijonot voidaan tulkita vain yhdellä tavalla. Tätä tulkintaa eivät määrää monimerkityksiset ja -vivahteiset symbolien merkityksiä kuvailevat sanat – symboleille ei pitäisi formalismin hengessä antaa merkityksiä – vaan mahdollisimman selkeästi esitetyt päättelysäännöt. Toisin sanoen symbolijonon vaikutus määräytyy sen mukaan, miten sitä voidaan käyttää apuna matemaattisessa todistuksessa. Matemaattisen symbolikielen täsmällisyys riippuu täten päättelysääntöjen esittämisen täsmällisyydestä.

Tässä luvussa nuo päättelysäännöt pyritään esittämään yksitulkintaisesti valottaen tarpeen tullen myös sitä, miksi mitäkin sääntöä tai sopimusta tarvitaan. Symbolit ja niitä koskevat säännöt noudattavat suurimmaksi osaksi yleisiä matematiikan käytäntöjä, mutta osin ne on räätälöity tämän tutkielman tarpeisiin. Tutkielman kannalta tärkeitä oppaita symboleita koskeviin sääntöihin ovat Bourbakin *Théorie des ensembles* [2], Rosserin *Logic for mathematicians* [15] ja Whiteheadin ja Russellin *Principia mathematica* [19].

Tässä esityksessä käytetään seuraavia symboleja:

- Symbolit x, y, z, u, v ja w ovat muuttujia.
- Symboli $\square$ on sidotun muuttujan paikoitin.
- Symbolit a, b, c ja d ovat vakioita.
- Symbolit A, B, C, D ja E ovat lyhennysmerkintöjä kaavoille.
- Symbolit $\neg$, $\Rightarrow$, $\wedge$, $\vee$ ja $\Leftrightarrow$ ovat konnektiiveja.
- Symbolit $\exists$ ja $\forall$ ovat kvanttoreita.
- Symbolit (,), [,], $\leftarrow$, $'$, : ja / ovat apusymboleja.

Näiden lisäksi voidaan käyttää muitakin symboleita, kunhan vain ilmoitetaan, minkälaisesta symbolista on kysymys. Poikkeuksena tästä säännöstä voidaan ilman eri ilmoitusta muodostaa uusia symboleita yläpilkun $'$ avulla: yläpilkku liitetään muuttujaan, kaavalyhennysmerkintään tai vakioon, jolloin symboliyhdiste katsotaan vastaavanlaiseksi uudeksi symboliksi. Esimerkiksi x' on muuttujasymboli.

Konnektiivit ja apusymbolit ovat käyttötarkoitukseltaan yksinkertaisia symboleja. Konnektiiveja tarvitaan kaavojen muodostamiseen, ja apusymboleja tarvitaan monenlaisissa yhteyksissä. Näiden käyttötapa selviää kuitenkin kaavojen muodostamista ja muuta symbolien käyttöä käsiteltäessä. Muiden symbolien käyttöön on kuitenkin lähemmin perehdyttävä.

2.1 Kaavat ja symbolien käyttö

Mikä tahansa esitellyistä symboleista muodostettu jono, esimerkiksi jono $a\neg\wedge \leftarrow \mathrm{A}'\forall$, ei välttämättä ole teorian kannalta kiinnostava. Teorian kannalta kiinnostavia symbolijonoja ovat pääasiassa *kaavat*. Kaavat muodostetaan niitä koskevien sääntöjen mukaan. Lisäksi sovitaan, ettei mikään symbolijono, jota ei muodosteta sääntöjen mukaan, ole kaava. Seuraavassa listassa esitetään sääntöjä, joilla jo kaavoiksi todetuista symbolijonoista voidaan muodostaa uusia kaavoja. Lisäksi lista esittelee yhden uuden useasta symbolista koostuvan kaavalyhennysmerkinnän. Kaavaa voidaan symbolilistan mukaan merkitä yhdellä symbolilla. Esimerkiksi kaavalyhennysmerkintä A ei itsessään ole kaava, vaan se viittaa symbolijonoon, joka on kaava ja joka voidaan kokonaisuudessaan vaihtaa symbolin A tilalle, missä yhteydessä A esiintyneekin. A ja B ovat seuraavassa kaavalyhennysmerkintöjä ja x ja y ovat muuttujia.

- $(\mathrm{A} \wedge \mathrm{B})$ on kaava.[2]
- $(\mathrm{A} \vee \mathrm{B})$ on kaava.
- $\neg\mathrm{A}$ on kaava.
- $(\mathrm{A} \Rightarrow \mathrm{B})$ on kaava.
- $(\mathrm{A} \Leftrightarrow \mathrm{B})$ on kaava.
- $\mathrm{A}(y/x)$ on kaavalyhennysmerkintä, jossa x ja y ovat muuttujia tai vakioita ja joka viittaa kaavaan, joka saadaan korvaamalla lyhennysmer-

[2]Onko $(\mathrm{A} \wedge \mathrm{B})$ tosiaan kaava? $(\mathrm{A} \wedge \mathrm{B})$ on kaava täysin täsmällisesti vasta sitten, kun kaavalyhennysmerkinnät A ja B on korvattu niiden tarkoittamilla aidoilla kaavoilla. Symbolijono $(\mathrm{A} \wedge \mathrm{B})$ ei ole myöskään kaavalyhennysmerkintä. Ratkaistaan ongelma venyttämällä kaavan käsitettä kaavalyhennysmerkinnän käsitteen sijasta, eli symbolijonon $(\mathrm{A} \wedge \mathrm{B})$ kaltaiset väliinputoajat sovitaan kaavoiksi.

kin A tarkoittaman kaavan jokaisen muuttujan x esiintymä muuttujan y esiintymällä.

Kaavat muodostuvat *osakaavoista*. Kaavan A osakaavat ovat kaava A itse ja jokainen kaava, johon on kaavan A muodostamista varten sovellettu jotain edellisistä tai myöhemmin esitettävistä kvanttoreita koskevista kaavanmuodostussäännöistä. Siispä esimerkiksi kaavan $\forall x(\square_x \in a \vee a \in \square_x)x$ osakaavat ovat koko kaava itse ja $(x \in a \vee a \in x)$, $x \in a$ sekä $a \in x$.

Sekaannusta voi aiheuttaa se, että A ja muut kaavalyhennysmerkinnät voivat olla eri tilanteissa lyhennysmerkintöjä eri kaavoille. Tässä mielessä kaavalyhennysmerkinnät ovat erityislaatuisia: ne ovat ikään kuin paikanpitäjiä oikeille kaavoille tai jopa kaavalyhennysmerkinnöistä muodostetuilla kaavoille, ja sama symboli voi eri tilanteissa pitää paikkaa eri kaavoille, tai eri symbolit voivat pitää paikkaa samalle kaavalle. Esimerkiksi symboli A voi olla kaavassa (A $\wedge$ C) lyhennysmerkintä kaavalle (A $\vee$ B), missä jälkimmäisessä kaavassa A onkin lyhennysmerkintä jollekin muulle kaavalle. Tällainen merkintä vaikuttaa ristiriitaiselta, mutta todellisuudessa se ei sodi sitä sopimusta vastaan, että kaavalyhennysmerkintä on yhdessä kaavassa vain yhden kaavan lyhenne mutta eri kaavoissa se saa olla eri kaavojen lyhenne. Nimittäin jos A on kaavan (A $\vee$ B) lyhenne kaavassa (A $\wedge$ C), tämä jälkimmäinen on sama kuin ((A $\vee$ B) $\wedge$ C), jossa taas A on saman kaavan lyhenne kuin kaavassa (A $\vee$ B). Näin huomataan, että vaikka A toimii lyhenteenä eri kaavoille, se toimii lyhenteenä eri kaavoille eri kaavojen – ei yhden ja saman kaavan – yhteydessä. Toki hämmentävää kaavalyhennysmerkintöjen käyttöä pyritään välttämään.

Lyhennysmerkintä on välttämätön, sillä kaavojen muodostamista koskevat säännöt olisi mahdotonta esittää ilman niitä. Lisäksi tämän luvun esittämillä tiedoilla ei voida muodostaa vielä yhtään oikeaksi kaavaksi luokiteltavaa symbolijonoa, jossa ei esiinny kaavalyhennysmerkintöjä. Kaavalyhennysmerkinnät eivät kuitenkaan kuulu siinä mielessä formaalisten symbolien joukkoon, että niitä ei käytetä formaalisissa todistuksissa (vrt. [4]: s. 6). Vaikka kaavalyhennysmerkinnät tässä esitetäänkin muiden, formaalisten symbolien kanssa, nämä informaaliset symbolit rinnastuvat ennemminkin luonnolliseen kieleen, joka tietenkin on välttämätön väline matematiikan formaalisen kielen esittämisessä. Esimerkiksi ¬A lyhentää luonnollisen kielen lauseen *mielivaltaisen kaavan eteen on kirjoitettu ¬-konnektiivi*. Vaikka ¬A vaikuttaa täsmällisemmältä, se on itse asiassa yhtä epämääräinen kuin tuo luonnollisen

kielen lause.

On tärkeää huomata, että kaavalyhennysmerkintä viittaa symbolijonoon, josta voidaan tietää, mistä symboleista se koostuu ja missä järjestyksessä nämä ovat. Esimerkiksi voidaan tietää, mitä esiintymiä muuttujalla x on kaavassa A – tarkemmin "lyhennysmerkin A tarkoittamassa kaavassa" – eli montako kertaa ja missä kohdin x sijaitsee symbolijonossa, jota A merkitsee. Niinpä jatkossa on perusteltua puhua "kaavasta A", ja näin tehdäänkin, kun oikeasti tarkoitetaan kaavaksi kutsuttua säännönmukaista symbolijonoa, johon A viittaa.

Hieman kaavalyhennysmerkintöjen tapaan muuttujiakin voidaan ajatella paikanpitäjinä. Yksi niiden tehtävistä on osoittaa, mihin kohti voi sijoittaa toisen muuttujan tai vakion. Tämä pätee omalla säännönmukaisella tavallaan formaalisissa todistuksissa ja laajemmin ja epämääräisemmin muussa tekstissä, jossa käytetään muuttujia. Formaalisen todistuksen ulkopuolella muuttuja on siksi lähes yhtä epämääräinen symboli kuin kaavalyhennysmerkintä. Esimerkiksi kun myöhemmin esitetään symbolijono $x \in y$ kaavaksi (symboli $\in$ esitellään myöhemmin), muuttujien x ja y tilalle voidaan todellisuudessa ajatella mitkä tahansa muuttujat tai vakiot, ei pelkästään muuttujia x ja y. Samoin kaavalyhennysmerkinnässä $\mathrm{A}(y/x)$ muuttujien x ja y tilalla voi aivan hyvin olla mitä tahansa muita muuttujia tai vakioita. Tavallisesti kuitenkin muuttujan tilalle saa vapaasti vaihtaa toisen muuttujan, ellei selvästi osoiteta vakionkin kelpaavan.

Muuttujat ovat siis matematiikan formaalisessa symbolikielessä melko vapaasti keskenään vaihdettavissa. Tarkemmin sanottuna sovitaan, että kaavat A ja $\mathrm{A}(y/x)$ ovat samoja kaavoja, jos x ja y tosiaan ovat muuttujia ja muuttujalla y ei ole yhtään esiintymää kaavassa A. Toisaalta yhdessä ja samassa symbolijonossa (tavanomaisimmin kaavassa) yhden muuttujan kaikki esiintymät ovat niin sanotusti aina samassa roolissa, eli jos näistä esiintymistä yhden tilalle sijoitetaan muuttuja tai vakio, tämä sijoitetaan samalla kaikkien muuttujan esiintymien tilalle tuossa symbolijonossa. Siksi kaavat A ja $\mathrm{A}(y/x)$ eivät välttämättä ole samoja, jos muuttujalla y on esiintymiä kaavassa A.

Esimerkein valotettuna edellä esitetty tarkoittaa sitä, että kaavat $\neg x \in y$ ja $\neg z \in u$ ovat käytännössä sama kaava vain eri muuttujilla esitettynä. Kaavat $\neg x \in y$ ja $\neg y \in y$ ovat eri kaavoja, koska kaavassa $\neg x \in y$ muuttujat x ja y voivat pitää paikkaa eri muuttujille tai vakioille mutta kaavassa

$\neg y \in y$ muuttuja y pitää paikkaa vain yhdelle muuttujalle tai vakiolle. Samat huomiot pitävät paikkansa muillekin symbolijonoille kuin kaavoille, erikoistapauksena myös kaavalyhennysmerkinnälle $\mathrm{A}(y/x)$, jonka tilalla yleisenä kaavalyhennysmerkintänämallina voitaisiin käyttää merkintää $\mathrm{A}(u/z)$ mutta ei $\mathrm{A}(x/x)$.

Muuttujien ainutlaatuisena ominaispiirteenä on, että ne voivat olla vapaita tai sidottuja. Oikeastaan muuttujien mahdollisuus vapauteen on tekninen apukeino ja kaikki muuttujat voitaisiin ajatella sidotuiksi, mutta silti nimenomaan muuttujan sidosteisuuden osoittamiselle on määrätyt keinonsa. Silmiinpistävin näistä keinoista on sidotun muuttujan paikoitin $\square$, joka ei koskaan esiinny ilman alaindeksiä, johon on kirjoitettu sidottu muuttuja. Esimerkiksi $\square_x$ pitää sidotun muuttujan x paikkaa. Kaavassa sidotun muuttujan paikoitin $\square_x$ katsotaan muuttujan x esiintymäksi, minkä takia muun muassa kaavassa $\mathrm{A}(y/x)$ kaavan A symbolit $\square_x$ vaihdetaan symboleiksi $\square_y$. Sidotun muuttujan paikoitin $\square$ on jäljitelty Bourbakilta [2], joka tosin ei käyttänyt sitä aivan samalla tavoin, kuin tässä tutkielmassa käytetään. Yksi merkinnän eduista on, ettei muuttujan sidosteisuudesta ainakaan ole mitään epäselvyyttä.

Bourbaki esittelee $\square$-symbolin ilmeisesti siksi, että tietyn muuttujan sitovassa kaavassa ei Bourbakin esittelemässä syntaksissa esiinny yhtään tämän muuttujan esiintymää, koska kaikki esiintymät on korvattu symbolilla $\square$. Mielenkiintoinen yksityiskohta on, ettei Bourbaki merkitse muuttujaa alaindeksillä vaan symbolin $\square$ sidosteisuus osoitetaan symbolijonon alle piirretyllä ”liitoksella” (ransk. *liaison*, vrt. ransk. *lié* ’sidottu’). Täysin samanlaista vaikutusta sidotun muuttujan paikoittimella ei ole tässä tutkielmassa esitettävässä syntaksissa, mutta silti sidotun muuttujan paikoitin alleviivaa melko onnistuneesti sidotun ja vapaan muuttujan vaikutuspiirin eroa. Tällä tarkoitetaan epämääräisesti sitä, että sovitusti muuttujan vaikutuspiiri on symbolijono eli tavallisesti kaava, jossa se esiintyy. Tämä pitääkin täysin paikkansa vapaalle muuttujalle, mutta sidotun muuttujan vaikutuspiiri on itse asiassa vain se osakaava, jossa muuttuja on sidottu.

Esimerkiksi symbolijono $(\exists x \square_x \in yx \wedge \forall xz \in \square_x x)$ on sääntöjen mukaan muodostettu kaava. Tässä kaavassa muuttuja x esiintyy kahdessa sellaisessa osakaavassa, jossa se on sidottu. Ensimmäisessä sidos loppuu ennen $\wedge$-konnektiivia, ja jälkimmäinen sidos alkaa vasta tämän konnektiivin jälkeen. Niinpä sidotun muuttujan x eri sidosten vaikutuspiirit ovat erilliset,

minkä vuoksi ensimmäisen sidoksen muuttujalla x ja toisen sidoksen muuttujalla x ei ole mitään tekemistä keskenään. Tämä tulisi paljon selvemmin ilmi Bourbakin tavasta käyttää symbolia $\square$ ja tämän symbolin esiintymien ja muuttujan sitovan symbolin välisiä liitoksia. Tässä tutkielmassa ei käytetä liitoksia, joten sidotun muuttujan symbolilla (eli sillä, onko sidottu muuttuja x vai y) on merkitystä päättelysääntöjä sovellettaessa.

Seuraava lista esittelee symbolijonot, joissa muuttuja on sidottu, eli sijoitusmerkinnän ja kvanttoreilla muodostetut kaavat. Jos x on muuttuja ja A sekä $\exists x\mathrm{A}x$ ja $\forall x\mathrm{A}x$ ovat kaavoja, sanotaan, että x on sidottu noissa kaavoissa ja kaikissa kaavoissa, joiden osakaavoja ne ovat. Jos x esiintyy kaavassa, jonka mikään osakaava ei ole $\exists x\mathrm{A}x$ tai $\forall x\mathrm{A}x$ (missä A on kaava), muuttuja x on tuossa kaavassa vapaa.

- $\exists x\mathrm{A}x$ on kaava, jos x ei ole sidottu muuttuja kaavassa A eli jos x on vapaa tai ei esiinny kaavassa A. Kaavassa $\exists x\mathrm{A}x$ muuttuja x on sidottu muuttuja ja jokainen muuttujan x esiintymä kaavassa A korvataan muuttujalla indeksoidulla sidotun muuttujan paikoittimella $\square_x$.

- $\forall x\mathrm{A}x$ on kaava, jos x ei ole sidottu muuttuja kaavassa A. Kaavassa $\forall x\mathrm{A}x$ muuttuja x on sidottu muuttuja ja jokainen muuttujan x esiintymä kaavassa A korvataan muuttujalla indeksoidulla sidotun muuttujan paikoittimella $\square_x$.

- $\mathrm{A}x \leftarrow a$ on sijoitusmerkintä, jos x ei ole sidottu kaavassa A. Sijoitusmerkinnässä $\mathrm{A}x \leftarrow a$ muuttuja x on kuitenkin sidottu ja jokainen muuttujan x esiintymä kaavassa A korvataan muuttujalla indeksoidulla sidotun muuttujan paikoittimella $\square_x$. Symboli a pitää paikkaa vakiolle.

Tässä kohdin lienee perusteltua selventää sidotun muuttujan paikoittimen $\square$ käyttöä. Sen tarkoitus on siis osoittaa selvästi, missä kohdin on sidottu muuttuja. Se saattaa kuitenkin aluksi aiheuttaa sekaannusta, joten on syytä antaa esimerkkejä, milloin sidotun muuttujan paikoitinta käytetään. Kaavanmuodostusäännöistä käy ilmi, että muuttuja x voi olla sidottu sijoitusmerkinnässä $\mathrm{A}x \leftarrow a$ tai kvanttorin kanssa muodostetussa kaavassa. Esimerkiksi $\neg x \in \square_y y \leftarrow a$ on kaavanmuodostussääntöjen mukaisesti muodostettu, samoin kuin $\exists x\forall y(\square_y \in \square_x \Leftrightarrow \square_y \in z)yx$. Ensimmäisessä esimerkissä y on sidottu ja x vapaa muuttuja. Toisessa esimerkissä x ja y ovat sidottuja muuttujia ja z on vapaa muuttuja. Kuitenkin, jos sijoitukselle $\neg x \in \square_y y \leftarrow a$

käytetään lyhennysmerkintää A$x \leftarrow a$, kaavassa A eli kaavassa $\neg x \in y$ kummatkin muuttujat – myös y – ovat vapaita. Samoin toisen esimerkin kvanttorien avulla muodostetun kaavan osakaavassa $(y \in x \Leftrightarrow y \in z)$ kaikki muuttujat ovat vapaita.

Sijoitusmerkintään kuuluu vakio a. Vaikka symbolit a, b, c ja d esitellään vakioiksi, ne ovat pikemminkin parametreja tai *yleisiä vakioita*. Tämä tarkoittaa sitä, ettei esimerkiksi a tarkoita aina samaa vakioita eli että se ei ole vakio. Näitä yleisiä vakioita voidaan käyttää todistuksissa vakioina, mikä tarkoittaa, että ne ovat vakioita eli (tämän tutkielman tapauksessa) tiettyjä ja samoja joukkoja koko todistuksen ajan. Niitä voidaan muussa tekstissä käyttää vakioiden paikanpitäjinä eli osoittamaan, että siihen symbolijonon kohtaan, jossa yleinen vakio esiintyy, voidaan sijoittaa ainoastaan vakio. Näin on sijoitusmerkinnän laita. Merkintään A$x \leftarrow a$ voidaan symbolin a tilalle sijoittaa ainoastaan vakio. Todistuksessa sijoitusmerkinnän tarkoitus onkin vakion esitteleminen. *Aito vakio* sitä vastoin on vakio, jota käytetään läpi koko tutkielman tietyllä yleisistä muuttujista eli parametreistä riippumattomalla tavalla määriteltyyn muuttujaan viitatessa.

Kaavoista erityisasemassa ovat *lauseet*. Kaava on lause, jos siinä ei ole vapaita muuttujien esiintymiä. Lauseet ovat merkityksellisiä, koska matemaattinen teoria muodostuu lauseista.

2.2 Kaavojen keskinäiset suhteet ja kaavamallit

Kaavojen muodostamiseen ei tarvittaisi viittä konnektiivia. Tavallista onkin esitellä kaksi konnektiivia, esimerkiksi konnektiivit $\neg$ ja $\Rightarrow$, ja esittää muut konnektiivit näiden avulla. Tautologialistan kolme ensimmäistä tautologiaa esittävät, miten tämä onnistuu. Itse asiassa konnektiiveja ei tarvittaisi kuin yksi, Shefferin viiva | ([19]: s. `xvi`). Tämän konnektiivin avulla esitettynä $\neg$A on (A|A) ja (A $\Rightarrow$ B) on (((A|B)|B)|((A|B)|B)).

Viiden konnektiivin esitteleminen on kuitenkin paljon käytännöllisempää kuin vain yhden tai kahden, koska näin kaavoista saadaan lyhyempiä ja helpommin luettavia. Lisäksi viiden konnektiivin ansiosta kaavat on nopeasti tulkittavissa luonnollisella kielellä. Vaikka formaalisessa päättelyssä symboleille ei pidä antaa merkityksiä tai ainakaan näiden merkitysten ei saa antaa ohjata päättelyä, matemaattista symbolikieltä käyttääkseen on käytännössä vältämätöntä ajatella konnektiiveille jotkin merkitykset. Konnektiivin $\neg$

merkitys on 'ei' tai 'ei pidä paikkaansa, että', konnektiivin $\vee$ 'tai' ja konnektiivin $\wedge$ 'ja'. Kaava $(A \Rightarrow B)$ tarkoittaa luonnollisella kielellä 'jos A, niin B' tai 'A:sta seuraa B', ja $(A \Leftrightarrow B)$ tarkoittaa 'A, jos ja vain jos B' tai 'A on ekvivalentti kaavan B kanssa' tai 'A tarkoittaa samaa kuin B'. Täten kaava $((\neg A \vee B) \Leftrightarrow (A \Rightarrow B))$ tulkitaan luonnolliselle kielelle esimerkiksi 'se, että A ei pidä paikkaansa tai B pitää paikkansa, on ekvivalentti eli samaa tarkoittava sen kanssa, että A:sta seuraa B'.

Luonnolliselle kielelle kaavoja käännettäessä tulee vastaan sellaisia ilmauksia kuten *pitää paikkansa*, *on epätosi* tai *pätee, että*. Matemaattisilla lauseilla ja joillakin muilla kaavoilla on tosiaan totuusarvo: yleisesti ajatellaan, että kukin lause on tosi tai epätosi. Tässä tutkielmassa lause tai yleisemmin kaava on tosi, jos se esiintyy matemaattisessa todistuksessa. Epätodelle ei kuitenkaan ole tällaista näin helppoa määritelmää. (Pitäisi olla varmuus teorian ristiriidattomuudesta, jotta voitaisiin sanoa kaavaa A epätodeksi, kun $\neg A$ on tosi.) Muun muassa tästä syystä tässä tutkielmassa kartetaan totuusarvoista puhumista.

Miten voidaan sitten tietää, minkälaisia kaavoja todistuksissa voi esiintyä? Aksiomaattisen esityksen ideana on antaa valmiiksi muutama peruskaavamalli, joiden mukaisia kaavoja saa vapaasti todistukseen kirjoittaa, ja päättelysäännöt, joiden avulla jo kirjoitettujen kaavojen perusteella voidaan todistukseen kirjoittaa uusia kaavoja. J. Rosser esittää kirjassaan ([15]: s. 56) kolme peruskaavamallia, joiden perusteella voidaan päätellä *modus ponens* -päättelysäännöllä muut tarpeelliset kaavamallit:

(1) $(A \Rightarrow (A \wedge A))$,

(2) $((A \wedge B) \Rightarrow A)$ ja

(3) $((A \Rightarrow B) \Rightarrow (\neg(B \wedge C) \Rightarrow \neg(C \wedge A)))$.

Whitehead ja Russell esittelevät *Principia mathematicassa* ([19]: s. `xix`) Jean Nicodin löytämän yhden Shefferin viivaa hyödyntävän peruskaavamallin, jonka perusteella muut kaavamallit voidaan todistaa (kaavassa käytetään selvennyksen vuoksi samaan tarkoitukseen eri sulkeita (), $\big(\big)$, [] ja {}):

$$\big(\{A|(B|C)\} \mid [\{D|(D|D)\}|\{(E|B)|((A|E)|(A|E))\}]\big)$$

Ainoa päättelysääntö on: jos tiedetään A ja $(A|(B|C))$, voidaan päätellä C.

On huomattava, ettei esitettyjä kaavoja sellaisenaan saa kirjoittaa todistukseen, koska kaavalyhennysmerkinnät eivät ole formaalisessa todistuksessa käytettäviä symboleja. Ideana on, että kun näistä peruskaavamalleista saadaan johdettua uusi kaavamalli, esimerkiksi $(A \Rightarrow A)$, tämä johtaminen toimii mallina, miten formaalisessa todistuksessa oikeista kaavoista saataisiin johdettua oikea kaava, joka voidaan kaavalyhennysmerkinnöin kirjoittaa muodossa $(A \Rightarrow A)$. Oikeasti siis ei ole sovittu vain yhtä tai muutamaa kaavaa, jonka todistukseen saa vapaasti kirjoittaa, vaan niin monta kaavaa, kuin mielikuvitus antaa periksi sijoittaessaan kaavalyhennysmerkintöjen tilalle oikeita kaavoja.

Kaikkien tarpeellisten kaavamallien – ja tarpeellisia kaavamalleja on monia – johtaminen on pitkällistä ja huomattavan hankalaa puuhaa. Siksi tutkielmassa vain esitetään lista kaavamalleista, joiden pitäisi olla johdettavissa esimerkiksi kolmesta edellä esitetystä peruskaavamallista yhdessä listan kolmen ensimmäisen kaavamallin kanssa, jotka osoittavat konnektiivien $\wedge$, $\vee$ ja $\Leftrightarrow$ suhteen konnektiiveihin $\neg$ ja $\Rightarrow$.

Pitkän valmiiksi annetun listan esittäminen sotii sitä formalismin ajatusta vastaan, että vain mahdollisimman yksinkertaiset ajatukset formaalistetaan. Nämä kaavamallit esitetään lähes perusteetta, eikä niiden yhteyttä helppoihin merkityksiin osoita kuin lyhyesti esitetyt konnektiivien merkitykset. Toisaalta kuka tahansa matemaattiseen loogiseen päättelyyn tai konnektiivien totuustauluihin perehtynyt on yhtä mieltä listan kaavamallien yksinkertaisuudesta mutta tietenkin tietoinen myös loogisen päättelyn tai totuustaulujen piirteistä, jotka eivät tunnu yksinkertaisilta ja kiistattomilta, jollaista päättelyn tietenkin pitäisi olla.

Seuraavassa listassa esitetään *todistuksiin sovellettavat kaavamallit* eli lyhyesti kaavamallit. A, B, C ja D ovat kaavalyhennysmerkintöjä.

1. $((A \wedge B) \quad \Leftrightarrow \quad \neg(A \Rightarrow \neg B))$
2. $((A \vee B) \quad \Leftrightarrow \quad (\neg A \Rightarrow B))$
3. $((A \Leftrightarrow B) \quad \Leftrightarrow \quad \neg((A \Rightarrow B) \Rightarrow \neg(B \Rightarrow A)))$
4. $(\neg\neg A \quad \Leftrightarrow \quad A)$
5. $((A \vee B) \quad \Leftrightarrow \quad (B \vee A))$
6. $(\neg(A \vee B) \quad \Leftrightarrow \quad (\neg A \wedge \neg B))$

7. $(\neg(A \wedge B) \quad \Leftrightarrow \quad (\neg A \vee \neg B))$
8. $((A \Rightarrow B) \quad \Leftrightarrow \quad (\neg B \Rightarrow \neg A))$
9. $((A \vee A) \quad \Leftrightarrow \quad A)$
10. $((A \Rightarrow (B \Rightarrow C)) \quad \Leftrightarrow \quad (B \Rightarrow (A \Rightarrow C)))$
11. $((A \Rightarrow (B \Rightarrow C)) \quad \Leftrightarrow \quad ((A \wedge B) \Rightarrow C))$
12. $(((A \wedge B) \Rightarrow (B \Rightarrow C)) \quad \Leftrightarrow \quad ((A \wedge B) \Rightarrow C))$
13. $((A \wedge (B \wedge C)) \quad \Leftrightarrow \quad ((A \wedge B) \wedge C))$
14. $((A \vee (B \vee C)) \quad \Leftrightarrow \quad ((A \vee B) \vee C))$
15. $(((A \Rightarrow B) \wedge (A \Rightarrow C)) \quad \Leftrightarrow \quad (A \Rightarrow (B \wedge C)))$
16. $(((A \vee B) \wedge (C \vee B)) \quad \Leftrightarrow \quad ((A \wedge C) \vee B))$
17. $((A \Rightarrow B) \quad \Leftrightarrow \quad ((B \wedge A) \Leftrightarrow A))$
18. $(((A \wedge \neg A) \vee B) \quad \Leftrightarrow \quad B)$
19. $(A \quad \Leftrightarrow \quad A)$
20. $(A \quad \Rightarrow \quad A)$
21. $((A \Leftrightarrow B) \quad \Leftrightarrow \quad (\neg A \Leftrightarrow \neg B))$
22. $(A \quad \Rightarrow \quad (B \Rightarrow A))$
23. $(A \quad \Rightarrow \quad (B \Rightarrow (A \wedge B)))$
24. $((A \Rightarrow B) \quad \Rightarrow \quad ((B \Rightarrow C) \Rightarrow (A \Rightarrow C)))$
25. $((A \Leftrightarrow B) \quad \Rightarrow \quad (A \Rightarrow B))$
26. $(A \quad \Rightarrow \quad (A \vee B))$
27. $(((A \Rightarrow B) \wedge (C \Rightarrow B)) \quad \Rightarrow \quad ((A \vee C) \Rightarrow B))$
28. $(((A \Leftrightarrow B) \wedge A) \quad \Rightarrow \quad B)$
29. $(((A \Rightarrow B) \wedge (C \Rightarrow D)) \quad \Rightarrow \quad ((A \vee C) \Rightarrow (B \vee D)))$
30. $(((A \vee B) \wedge C) \quad \Rightarrow \quad ((A \wedge C) \vee (B \wedge C)))$

31. $(A \Rightarrow (\neg A \Rightarrow B))$

32. $((A \wedge B) \Rightarrow A)$

33. $((A \Leftrightarrow (B \wedge C)) \Rightarrow (B \Rightarrow (A \Leftrightarrow C)))$

34. $((A \Rightarrow B) \Rightarrow ((C \wedge A) \Rightarrow B))$

35. $(((A \vee B) \Rightarrow C) \Rightarrow (A \Rightarrow C))$

36. $((((A \wedge B) \Rightarrow D) \wedge ((A \wedge C) \Rightarrow D)) \Leftrightarrow ((A \wedge (B \vee C)) \Rightarrow D))$

37. $((A \Rightarrow (B \wedge (B \Rightarrow C))) \Rightarrow (A \Rightarrow C))$

38. $(((A \wedge B) \vee C) \Rightarrow (A \vee C))$

39. $((A \wedge (B \vee C)) \Rightarrow ((A \wedge C) \vee B))$

Kaavamallit eivät ole loogisesti riippumattomia. Seuraavassa alaluvussa esitettyjen päättelysääntöjen avulla moni kaavamalleista voitaisiin johtaa toisista kaavamalleista. Listan tarkoitus on kuitenkin esittää kaavoja, joita tutkielman todistuksissa tarvitaan.

2.3 Formaalinen määritelmä ja todistus

Formaalinen määritelmä esittelee lyhennysmerkinnän. Määritelmä on aina muodossa

$$A :: B,$$

missä A on lyhennysmerkintä symbolijonolle, jonka määritelmä määrittelee kaavaksi, ja B on kaavalyhennysmerkintä. Lisäksi jokaisen kaavassa A esiintyvän muuttujan ja vakion on esiinnyttävä kaavassa B, ja jokaisen kaavan B vapaan muuttujan on esiinnyttävä kaavassa A. A :: B voidaan lukea ”A on määritelty samaksi kuin B”. Symbolilla A lyhennetty kaava on määritelmän asettama lyhennysmerkintä symbolilla B lyhennetylle kaavalle. Määritelmä A :: B käsitetään muuttujien ja vakioiden kannalta yhdeksi symbolijonoksi, eli jos esimerkiksi x on kaavoille A ja B yhteinen muuttuja ja jos sen tilalle määritelmää käytettäessä sijoitetaan jokin muu muuttuja tai vakio, sijoitus täytyy tehdä kaikkiin muuttujan x esiintymiin kummassakin kaavassa A ja B. Käytännössä määritelmän tarkoitus on esitellä uuden symbolin käyttöä;

esimerkiksi määritelmä 3.3 esittelee relaatiosymbolin = käytön. Informaalisia määritelmiä ovat muun muassa uusien luonnollisella kielellä esitettyjen käsitteiden merkitykset.

Formaalinen todistus on ryhmä rivejä, joista jokainen on oikeutettu esiintymään todistuksessa. Viimeisen rivin on oltava lause. Jonkin formaalisen todistuksen viimeisellä rivillä esiintynyttä lausetta kutsutaan todistetuksi lauseeksi. Tähän lauseeseen päästään kaavamallien ja päättelysääntöjen avulla aksioomista, todistetuista lauseista ja mahdollisesta oletuksesta. Todistus siis käsitetään kirjoitetuksi rivi riviltä niin, että ylin rivi on kirjoitettu ennen muita rivejä ja muut rivit on kirjoitettu sen alle järjestyksessä.

Todistus todistaa aina jonkin väitteen. Väite esittää lauseen, joka on tarkoitus päätellä todistuksen viimeiseksi riviksi, jolloin siitä siis tulee todistettu lause. Väitteessä annetaan myös mahdollinen oletus ja mahdolliset todistuksessa esiintyväksi vaaditut rivit. Tässä tutkielmassa oletukseksi ei millekään lauseelle tarvita kuin valmiita vakioita. Jos lauseen B todistus tarvitsee oletukseksi vakion a, sanotaan, että lause B on todistettavissa, kun oletetaan a vakioksi, ja merkitään $a :\Rightarrow:$ B. Oletettu vakio on aina yleinen määrittelemätön vakio. Väitteessä saa olettaa myös useamman vakion valmiiksi, jolloin eri vakiot erotetaan toisistaan pilkulla.

Merkitään symboleilla X ja Y symbolijonoa, joka on kaava tai sijoitusmerkintä. Jos X on todistuksessa esiintyväksi vaadittu rivi ja B on todistettava lause, väite merkitään [X]B. Esiintyväksi vaadittuja rivejä voi olla useampiakin, jolloin ne erotetaan toisistaan hakasulkeiden sisällä pilkulla. Väitteessä voi olla oletettuja vakioita, esiintyväksi vaadittuja rivejä ja todistettava lause. Esimerkiksi jos oletetaan a ja b vakioiksi ja todistuksessa on vaadittu esiintyviksi kaavat tai sijoitusmerkinnät X ja Y ja todistettava lause on B, niin väite merkitään $a, b :\Rightarrow:$ [X, Y]B. Todistuksessa esiintyväksi vaadittuja rivejä tarvitaan, kun todistetaan vakion yksikäsitteisyyttä tai jos lauseessa esiintyy vakio, jota ei voi olettaa ja jonka olemassaolosta ei ole takeita (ks. lause 3.7).

Todistuksessa kukin rivi koostuu kolmesta osasta. Jokainen todistuksen rivi leimataan omalla (todistukseen nähden) ainutkertaisella merkillään, johon alla olevissa päättelysäännöissä viitataan symbolilla n tai symbolilla m. Tämä leima löytyy heti rivin alusta yläindeksiksi kirjoitettuna. Välittömästi leiman jälkeen seuraa lyhenne (esimerkiksi päättelysäännön tai aksiooman lyhenne), joka oikeuttaa varsinaisen todistusrivin kirjoittamisen. Jokaisen rivin toinen palsta koostuu tästä oikeutetusta todistusrivistä.

Kaavamalleihin ja todistusten riveihin viitattaessa tarvitaan arabialaisia numeroita. Huomattakoon, ettei oikeastaan luonnollisten lukujen merkitsemistä arabialaisin numeroin tarvitse tuntea. Vaikka todistusten rivit käytännön vuoksi kymmenpaikkajärjestelmää käyttäen onkin numeroitu järjestyksessä 1, 2, 3 ja niin poispäin, ei ole välttämätöntä ajatella näitä merkintöjä luonnollisina lukuina, jotka esiintyvät seuraaja-järjestyksessä luvusta yksi alkaen. Tämä on hyvä huomata, koska tässä vaiheessa tutkielmaa ei ole vielä esitetty, mitä luonnolliset luvut ovat.

MP(n,m) Tämä on päättelysääntö *modus ponens*: jos todistusrivi n on kaava A ja todistusrivi m on kaava (A $\Rightarrow$ B), niin todistukseen saa kirjoittaa todistusrivin B.

$\mathbf{k}^m$ Todistukseen saa kirjoittaa kaavamallin m mukaisen todistusrivin eli kaavan, jossa kaavamallin m kaikki kaavalyhennysmerkinnät on korvattu oikeilla kaavoilla.

$\mathbf{s}^m_m(n)$ Tämä sääntö on *sievennyssopimus*: Jos todistusrivin n kaava tai sijoitusmerkintä sisältää osakaavan A ja kaavamallilistan rivi m (käytetään yläindeksiä s^m) on kaava (A $\Leftrightarrow$ B), niin todistukseen saa kirjoittaa rivin n todistusrivin, jonka osakaava A on korvattu kaavalla B. Samaa sääntöä voi soveltaa todistusrivin m suhteen (käytetään alaindeksiä s_m), jos todistusrivi m on kaava (A $\Leftrightarrow$ B).

$\mathbf{m}m(n)$ Jos määritelmä m on A :: B ja todistusrivin n kaava tai sijoitusmerkintä sisältää osakaavan B (tai vastaavasti osakaavan A), niin todistukseen saa kirjoittaa rivin n todistusrivin, jonka osakaava B (tai osakaava A) on korvattu kaavalla A (tai kaavalla B).

Lisäksi todistukseen saa tietenkin kirjoittaa aksiooman tai jo aiemmin todistetun lauseen. Jos todistukseen kirjoitetaan aksiooma tai lause, rivin oikeutuksen lyhenteeksi tulee aksiooman yhteydessä esitetty lyhenne tai lyhenne Am, jossa m on aksiooman numero, tai Lm, jossa m on lauseen numero. Jos todistukseen kirjoitettavan lauseen väitteeseen kuuluu oletettu yleinen vakio, tämän vakion esiintymien tilalle lauseeseen on oltava sijoitettavissa todistuksessa oletuksessa tai sijoitusmerkinnässä esitelty vakio. Lisäksi jos lauseen väitteeseen kuuluu todistuksessa esiintyviksi vaadittuja rivejä, näiden rivien on esiinnyttävä myös siinä todistuksessa, jossa lausetta käytetään apuna.

Päättelysääntö modus ponens ei kaivanne selittelyjä. Luonnolliselle kielelle käännettynä se tarkoittaa vain, että jos tiedetään A ja tiedetään A:sta seuraavan B:n, niin tiedetään B. Toinen sääntö vain toistaa aiemmin mainitun sopimuksen, että minkä tahansa kaavamallilistan mukaisen kaavan saa kirjoittaa todistukseen. Neljäskään päättelysääntö ei ole lainkaan luonnoton. Määritelmän tarkoitus on nimenomaan määritellä vanhastaan tunnettu kaava uuden merkintätavan kanssa vaihtokelpoiseksi. Tämän olisi voinut ilmaista niinkin, että jos määritelmä m on A :: B, niin todistukseen saa kirjoittaa $(\mathrm{A} \Leftrightarrow \mathrm{B})$, ja lopusta olisi pitänyt huolen sievennyssopimus.

Sievennyssopimus vaatii hieman lähempää tarkastelua. Tosin sekin on luonnollinen sääntö, kun otetaan huomioon $\Leftrightarrow$-konnektiiville annettu merkitys. Toisaalta sievennyssopimus voisi olla pitkällisten perustelujen tulos (engl. *substitution theorem*, ks. [15]: luvut IV–VI), ei vain sovittu helpotus. Sievennyssopimuksen voi ajatella myös niin, että jos todistuksessa esiintyy kaava $(\mathrm{A} \Leftrightarrow \mathrm{B})$ ja esimerkiksi kaava $(\mathrm{C} \wedge \mathrm{A})$, niin kaava $(\mathrm{C} \wedge \mathrm{B})$ voidaan kirjoittaa todistukseen siksi, että kaavan $(((\mathrm{A} \Leftrightarrow \mathrm{B}) \wedge (\mathrm{C} \wedge \mathrm{A})) \Rightarrow (\mathrm{C} \wedge \mathrm{B}))$ pitäisi olla yksi todistuksiin sovellettavista kaavamalleista, jotka voidaan johtaa peruskaavamalleista. Niinpä sievennyssopimus on käytännöllinen vaikkeikaan välttämätön päättelysääntö.

2.4 Kvanttoreita koskevat päättelysäännöt

Koska matemaattinen teoria koostuu lauseista eli kaavoista, joissa ei ole vapaita muuttujia, ja koska kvanttorien avulla sidotaan muuttujia, kvanttoreita koskevilla päättelysäännöillä on erityinen asemansa todistuksissa. Seuraava lista esittää nämä säännöt.

kvs(n) Jos todistusrivi n on kaava, todistukseen saa kirjoittaa todistusrivin, joka on saatu rivin n kaavasta soveltamalla sievennyssopimusta ja jotakin seuraavista kvanttoreihin liittyvistä todistuksiin sovellettavista kaavamalleista:

- Jos kaavan $\forall x\mathrm{A}x$ osakaavassa A ei ole yhtään muuttujan x esiintymää, niin kaava $(\forall x\mathrm{A}x \Leftrightarrow \mathrm{A})$ on kaavamalli. Samoin ehdoin $(\exists x\mathrm{A}x \Leftrightarrow \mathrm{A})$ on kaavamalli.
- Jos kaavassa A ei ole yhtään muuttujan x esiintymää, niin kaava $(\forall x(\mathrm{A} \Rightarrow \mathrm{B})x \Leftrightarrow (\mathrm{A} \Rightarrow \forall x\mathrm{B}x))$ on kaavamalli. Samoin ehdoin

myös kaava $(\exists x(\mathrm{A} \Rightarrow \mathrm{B})x \;\Leftrightarrow\; (\mathrm{A} \Rightarrow \exists x\mathrm{B}x))$ on kaavamalli.

- Kaava $(\forall x(\mathrm{A} \wedge \mathrm{B})x \;\Leftrightarrow\; (\forall y\mathrm{A}(y/x)y \wedge \forall z\mathrm{B}(z/x)z))$ on kaavamalli.
- Kaava $(\forall x\mathrm{A}x \;\Leftrightarrow\; \neg\exists y\neg\mathrm{A}(y/x)y)$ on kaavamalli.

ekvmp Kaava $((\exists x\mathrm{A}x \wedge (\mathrm{A} \Rightarrow \mathrm{B})) \Rightarrow \exists y\mathrm{B}(y/x)y)$ on kaavamalli.

$\exists\leftarrow(n)$ Jos todistusrivi n on lause $\exists x\mathrm{A}x$ ja jos kaavassa A on muuttujan x esiintymiä, niin todistukseen saa kirjoittaa todistusrivin $\mathrm{A}x \leftarrow a$, jossa symboli a pitää paikkaa vakiolle, joka ei esiinny väitteen oletuksessa eikä todistuksen aiemmilla riveillä.

sij(n) Jos todistusrivi n on sijoitusmerkintä $\mathrm{A}x \leftarrow a$, niin todistukseen saa kirjoittaa rivin $\mathrm{A}(a/x)$.

$\exists$ Jos A on kaava ja a on vakio, joka esiintyy kaavassa A, ja jos x on muuttuja, joka ei esiinny kaavassa A, niin $(\mathrm{A} \Rightarrow \exists x\mathrm{B}x)$ on todistuksiin sovellettava kaavamalli. Tässä B on kaava, joka on saatu vaihtamalla vähintään yksi vakion a esiintymistä kaavassa A muuttujalla x.

$\forall\leftarrow$ Jos A on kaava ja y on muuttuja tai vakio, $(\forall x\mathrm{A}x \Rightarrow \mathrm{A}(y/x))$ on todistuksiin sovellettava kaavamalli. Jos y on vakio, sen pitää olla todistuksessa sijoitusmerkinnässä tai väitteen oletuksena esitelty vakio.

$\forall(n)$ Jos todistusrivi n on kaava A ja x ei ole kaavassa A sidottu muuttuja, niin todistukseen saa kirjoittaa rivin $\forall x\mathrm{A}x$.

Samalla tavoin kuin muutkin kaavamallit myös näiden sääntöjen, muun muassa sääntöjen kvs (”kvanttorinsiirto”) ja ekvmp (”eksistentiaalikvanttorin modus ponens”), esittämät kaavamallit ovat matemaattiseen logiikkaan perehtyneelle lähes itsestäänselviä. Toisaalta nekään eivät ole yksinkertaisia. Niin kvs kuin nämä muutkin säännöt voitaisiin johtaa pienemmästä määrästä yleisempiä ja käyttökelpoisempia sääntöjä (ks. esim. [2]: s.35–43). Näin tällaiset säännöt valmiiksi sopimalla kuitenkin päästään huomattavasti helpommalla.

Kvanttoreista kenties merkityksellisempi on eksistentiaalikvanttori $\exists$, koska se mahdollistaa uuden vakion esittelyn sijoitusmerkinnällä. Eksistentiaalikvanttorin merkitys informaalisesti on ’on olemassa’. Jos jotakin on olemassa,

tälle olemassaolevalla voidaan varata oma symbolinsa, vakio. Tämän alleviivaamiseksi tässä tutkielmassa käytetään periaatteessa ylimääräistä sijoitusmerkintää. Sijoitusmerkintä $\mathrm{A}x \leftarrow a$ siis kertoo, että a on vakio, jolla on tietty oma merkityksensä koko todistuksessa ellei peräti koko tutkielmassa.

Universaalikvanttori $\forall$ on tehtävältään hieman eksistentiaalikvanttoria teknisempi. Vaikka sen informaalinen merkitys on suureellinen 'kaikelle olevaiselle pätee, että ...', sitä koskevat päättelysäännöt ovat osittain teknisiä keinoja vapaiden muuttujien sitomiseksi ja sidottujen muuttujien vapauttamiseksi. Päättelysääntö $\forall{\leftarrow}(n)$ mahdollistaa sidotun muuttujan vapauttamisen, millä on merkitystä siinä, että yleensä todistuksissa on helpompi päätellä kaavoilla, joissa on mahdollisimman vähän kvanttoreita. Päättelysääntö $\forall(n)$ taas mahdollistaa vapaan muuttujan sitomisen. Tämän säännön ansiosta lähes jokainen kaava voidaan ajatella lauseena, koska jokaisen sellaisen kaavan, jossa sama muuttuja ei esiinny vapaana ja sidottuna, vapaat muuttujat voidaan muuttaa sidotuiksi. Nämä päättelysäännöt ikään kuin formaalistavat sen ajatuksen, että 'kaikille muuttujille x pätee, että ...' tarkoittaa samaa kuin 'mielivaltaiselle muuttujalle x pätee, että ...'. Esimerkiksi kaavasta $\neg x \in \emptyset$ voidaan päätellä $\forall x \neg \Box_x \in \emptyset x$ ja toisinpäin.

Toki $\forall$-kvanttorilla on tärkeä merkityksensä, niin kuin $\exists$-kvanttoria koskevilla säännöillä on tekniset piirteensä. $\forall{\leftarrow}(n)$-päättelysäännön merkitys tulee ilmi, kun sijoitettava symboli (säännössä symboli y) on vakio. Jos jokin kaava pätee kaikelle olevaiselle, se pätee mille tahansa jo esitellylle vakiolle. Lisäksi universaalikvanttori on kaikkea muuta kuin tekninen, kun se esiintyy kaavan "sisällä" siinä mielessä, että kaava ei ole muotoa $\forall x \mathrm{A}x$ vaan esimerkiksi muotoa $\exists y \forall x \mathrm{A}xy$.[3] Toisaalta päättelysääntö $\exists(n)$ helpottaa teknisesti formaalista päättelyä. Esimerkiksi lauseesta $a = a$ voidaan päätellä $\exists x \Box_x = ax$, ja niinpä vakion a nimi ikään kuin vaihtaa, kun sijoitetaan uusi vakio $b = a$.

Päättelysääntöjä käytetään todistuksissa esitettyä väljemmin tilan säästämiseksi. Esimerkiksi jos todistukseen kirjoitettu sekä rivi A että B, siihen voidaan kolmen päättelyn ketjulla kirjoittaa rivi $(\mathrm{A} \wedge \mathrm{B})$: ensin kirjoitetaan kaava 23 ja sitten sovelletaan kahdesti päättelysääntöä MP. Koska näin yk-

[3]Vertaa, miten Hao Wang esittää artikkelissaan formaalisia kaavoja niin, että toisinaan kaavan aloittavat universaalikvantifioinnit jätetään panematta ilmi, mikä sitä vastoin on mahdotonta eksistentiaalikvanttorin jälkeisten universaalikvantifiointien suhteen ([18]: 151).

sinkertaiseen päättelyyn tuntuu turhalta tuhlata kolmea riviä, todistuksissa päättelyketju lyhennetään säännöksi ”k^{23},MP,MP”. Haittapuolena tässä ja monessa muussa käyttöön otettavassa sääntöyhdistelmässä on, ettei sääntöön ole kirjattu rivejä, joiden avulla päättely suoritetaan. Tämä ei aiheuttane kuitenkaan suuria ongelmia todistuksiin perehtyvälle. Lisäksi kaavamalleja 4 ja 5 kohdellaan todistuksissa itsestäänselvyyksinä siinä mielessä, että niiden käyttöä ei aina panna ilmi. Kaavalla 5 perustellaan todistuksissa myös $\wedge$- ja $\Leftrightarrow$-konnektiivien kommutatiivisuutta, joka on helposti johdettavissa kaavamallien avulla.

Sääntölyhennelmän ”k^{23},MP,MP” tapaan muissakaan lyhennelmissä ei välttämättä viitata riveihin, vaikka säännön käyttö periaatteessa niin vaatisikin. Esimerkiksi sääntölyhennelmä ”A$\emptyset$,$\exists\leftarrow$” viittaa siihen, että ensin kirjoitetaan aksiooma A$\emptyset$ ja sitten sovelletaan siihen saman tien sääntöä $\exists\leftarrow(n)$, jossa (n) on pakko jättää pois, koska aksioomaa A$\emptyset$ ei kirjoitettukaan näkyviin. Toisaalta sääntöjä $\exists$ ja $\forall\leftarrow$ käytetään usein riviviitteen kanssa. Jos rivi n on kaava $\forall x\mathrm{A}x$, sääntö $\forall\leftarrow(n)$ tarkoittaa, että kaavaan A on sijoitettu muuttujan x tilalle jokin vakio tai muuttuja y. Näin ei tarvitse ensin kirjoittaa kaavaa $(\forall x\mathrm{A}x \Rightarrow \mathrm{A}(y/x))$ ja sitten käyttää modus ponens -sääntöä. Ensimmäisissä todistuksissa sääntölyhennelmiä pyritään käyttämään hillitysti, jotta todistusten päättelyketjuja olisi helpompi oppia seuraamaan.

3 Joukot

Nyt kun matemaattiset työkalut eli päättelysäännöt ovat käytettävissä, on aika käsitellä sitä, mitä työstetään, eli todellisuutta. Yksinkertaisuuden vuoksi tämän tutkielman käsittelemä todellisuus koostuu joukoista. Toisin sanoen mikä tahansa, mikä on, on joukko.[4] Vaihtoehtoisesti voitaisiin lähtötilanteeksi valita perusalkioita (engl. *individuals*, saks. *Urelemente*, [13]: s. 24), joista joukkoja kootaan.

Perusalkioiden olettaminen annetuiksi lienee tähän tutkielmaan valittua näkökulmaa perustellumpi intuitiiviselta kannalta, koska vaikka perusalkioiden olemusta ei mitenkään määriteltäisi, voisi perusalkiot kuvitella asioiksi, joita me havaitsemme kokemassamme maailmankaikkeudessa. On vaikea kuvitella, että matematiikka voisi mitenkään mallintaa maailmaa, jos se käsittelee pelkkiä joukkoja. Kaiken lisäksi, jos todellisuus on pelkkiä joukkoja, joukonkaan käsite ei ole täysin intuitiivinen. Tämä johtuu siitä, että jos perusalkioita ei hyväksytä, on pakko hyväksyä tyhjä joukko ja yhden alkion joukko, jotka eivät sanan arkimerkityksessä ole mitään joukkoja. (Ks. [12]: luku 3.3, jossa Mayberry esittää tyhjäksi joukoksi joukkoa $\emptyset = \{\bot, \top\}$, missä $\bot$ ja $\top$ ovat valittuja perusalkiovakioita. Niinpä $\{a\}$ olisi lyhennysmerkintä joukolle $\{a, \bot, \top\}$.)

Matemaattinen käsittely kuitenkin helpottuu, kun todellisuudeksi valitaan ne joukot, jotka ovat olemassa. Tällaista todellisuutta kutsutaan *pelkistettyjen joukkojen* muodostamaksi (engl. *pure sets*, ks. esim. [13]: s.50 tai [16]: s. 87). Tämän valinnan etu on muun muassa se, että näin muuttujat ja vakiot viittaavat vain yhdenlaisiin matemaattisiin olioihin, joukkoihin. Joukko-opissa $\exists$-kvanttorin merkitys on, että se nimenomaan varmistaa joukkoon viittaamisen (vrt. [7]: s. 271). Jos siis todistuksessa esiintyy sijoitusmerkintä, tiedetään, että sijoitettava vakio (eli a sijoitusmerkinnässä $\mathrm{A}x \leftarrow a$) viittaa joukkoon. Siksi vakiota voidaan kutsua myös joukoksi.

Tämän luvun esitys joukko-opista perustuu muun muassa Abraham Fraenkelin teokseen *Einleitung in die Mengenlehre* [7], John Mayberryn kirjaan *The foundations of mathematics in the theory of sets* [12], Bourbakin *Théorie des ensemblesiin* [2] ja Abraham Fraenkelin, Yehoshua Bar-Hillelin

[4] Tästähän seuraa, ettei todellisuutta ole olemassa, koska kaikkien joukkojen joukkoa ei ole olemassa, mikä myöhemmin todetaan. Tällaiset hyvin olennaisetkin filosofian alaan kuuluvat vaikeudet sivuutetaan tässä matematiikan tutkielmassa.

ja Azriel Levyn teokseen *Foundations of set theory* [8]. Esitetyt aksioomat ja määritelmät ovat tunnettuja ja esiintyvät idealtaan melko samanlaisina kaikissa joukko-opin aksiomaattisesti esittävissä teoksissa. Missä esitykset eroavat, on tutkielmaan pyritty valitsemaan mahdollisimman yksinkertaisen esityksen mahdollistavat määritelmät ja aksioomat. Esimerkiksi myöhemmin esitetään Fraenkelin *Axiom der Bestimmtheit* (Bourbakin ja monen muun *l'axiome d'extensionalitén* sijaan), minkä ansiosta ei tarvitse esittää yleistä identtisyysrelaatiota vaan voidaan tyytyä joukkojen väliseen identtisyyteen.

3.1 Joukko-opin symbolit ja kuulumisrelaatio

Joukko-oppi tarvitsee uusia symboleja. Seuraava lista esittelee näitä symboleja, mutta niiden käyttö selvenee tavallisesti uusien määritelmien myötä. Symbolien luokittelua ei ole tarkoitettu kuin suuntaa-antavaksi, joten esimerkiksi relaatio- ja funktiovakioita voi ajatella ihan vain yleisinä vakioina. Tässä ja aiemmin esitellyistä vakioista on huomattava, että ne viittaavat joukkoihin, ja siksi vakioita voi kutsua joukoiksi ja toisinpäin.

- Symbolit $\in$, $\subseteq$ ja $=$ ovat relaatiosymboleja.
- Symbolit $\bigcup$, $\bigcap$, $\mathscr{P}$ $\cup$, $\cap$, $\mathcal{P}$, $|$, $\{$, $\}$, $\left\{$, $\right\}$, $($, $)$, $\left($, $\right)$ ja pilkku(,) ovat operaatiosymboleja.
- Symboli r on relaatiomuuttuja. Symboli f on funktiomuuttuja.
- Symboli R on relaatiovakio. Symboli F on funktiovakio.
- Symboli $\emptyset$ on vakio, joka viittaa tyhjään joukkoon.

Relaatiosymboli $\in$ on joukko-opin perusrelaation kuulumisrelaation symboli. Tämän symbolin avulla määritellään, että kun x ja y ovat muuttujia tai vakioita, niin

$$x \in y \text{ on kaava.}$$

Kaava $x \in y$ voidaan lukea "x kuuluu joukkoon y" tai "x on joukon y jäsen", vaikkakin kuulumisrelaation merkitys formaalisessa mielessä tulee aksioomista.

Relaatiosymboli mahdollistaa vihdoinkin aitojen kaavojen muodostamisen, koska juuri esitetty sääntö on ensimmäinen kaavan muodostamiseen liittyvä sääntö, jossa ei esiinny kaavalyhennysmerkintää. Käytetään kuulumisrelaatiota heti hyödyksi ja määritellään sen avulla symbolin $\subseteq$ käyttö. Relaatiosymboli $\subseteq$ on sisältymisrelaation symboli. Määritelmä määrittelee käyttöön uuden kaavan: $x \subseteq y$.

Määritelmä 3.1. Jos jokainen joukon x jäsen on myös joukon y jäsen, sanotaan, että x sisältyy joukkoon y eli että x on joukon y osajoukko. Tämä merkitään $x \subseteq y$, jossa x ja y ovat muuttujia tai vakioita. Formaalisesti siis määritellään uusi kaava, joka on lyhennysmerkintä muodostettavissa olevalle kaavalle:

$$x \subseteq y :: \forall z(\square_z \in x \Rightarrow \square_z \in y)z$$

Esitetään ja todistetaan nyt tutkielman ensimmäinen lause. Oikeastaan kyseessä ei ole mikään joukko-opin lause (eihän siinä edes vedota joukko-opin aksioomiin) vaan edellisessä luvussa sovittujen päättelytekniikoiden soveltamista. Tuloskin on täysin triviaali, yksinkertaisempi ja helpommin suoralta kädeltä hyväksyttävä kuin jotkin kaavamallit tai päättelysäännöt. Silti formaalinen todistus kompuroi todistuksen läpi raskaan oloisesti. Jos tämä ei johdu todistuksen huonosta laadinnasta, se kertoo formaalisen symbolikielen epäkäytännöllisestä vaikeudesta.

Lause 3.2. *Sisältymisrelaatio on transitiivinen. Tämä tarkoittaa sitä, että jos $x \subseteq y$ ja $y \subseteq z$, niin $x \subseteq z$. Formaalisesti:*

$$\forall x \forall y \forall z((\square_x \subseteq \square_y \wedge \square_y \subseteq \square_z) \Rightarrow \square_x \subseteq \square_z)zyx$$

Todistus.

$^1\forall\leftarrow$	$(\forall w((\square_w \in x \Rightarrow \square_w \in y) \wedge (\square_w \in y \Rightarrow \square_w \in z))w$
	$\Rightarrow ((u' \in x \Rightarrow u' \in y) \wedge (u' \in y \Rightarrow u' \in z)))$
$^2\mathrm{k}^{24},\mathrm{s}^{11}$	$(((u' \in x \Rightarrow u' \in y) \wedge (u' \in y \Rightarrow u' \in z))$
	$\Rightarrow (u' \in x \Rightarrow u' \in z))$

$^{3}\mathrm{k}^{24}$	$(\ (\forall w((\Box_w \in x \Rightarrow \Box_w \in y) \wedge (\Box_w \in y \Rightarrow \Box_w \in z))w \Rightarrow$ $((u' \in x \Rightarrow u' \in y) \wedge (u' \in y \Rightarrow u' \in z)))$ $\Rightarrow \quad (\ (((u' \in x \Rightarrow u' \in y) \wedge (u' \in y \Rightarrow u' \in z)) \Rightarrow$ $(u' \in x \Rightarrow u' \in z)) \quad \Rightarrow$ $(\forall w((\Box_w \in x \Rightarrow \Box_w \in y) \wedge (\Box_w \in y \Rightarrow \Box_w \in z))w \Rightarrow$ $(u' \in x \Rightarrow u' \in z)) \ ) \ \ )$
$^{4}\mathrm{MP}(1,3)$	$(\ (((u' \in x \Rightarrow u' \in y) \wedge (u' \in y \Rightarrow u' \in z)) \Rightarrow$ $(u' \in x \Rightarrow u' \in z)) \quad \Rightarrow$ $(\forall w((\Box_w \in x \Rightarrow \Box_w \in y) \wedge (\Box_w \in y \Rightarrow \Box_w \in z))w \Rightarrow$ $(u' \in x \Rightarrow u' \in z)) \ )$
$^{5}\mathrm{MP}(2,4)$	$(\forall w((\Box_w \in x \Rightarrow \Box_w \in y) \wedge (\Box_w \in y \Rightarrow \Box_w \in z))w$ $\Rightarrow (u' \in x \Rightarrow u' \in z))$
$^{6}\mathrm{kvs}(5)$	$((\forall u(\Box_u \in x \Rightarrow \Box_u \in y)u \wedge \forall v(\Box_v \in y \Rightarrow \Box_v \in z)v)$ $\Rightarrow (u' \in x \Rightarrow u' \in z))$
$^{7}\forall(6)$	$\forall u'((\forall u(\Box_u \in x \Rightarrow \Box_u \in y)u \wedge \forall v(\Box_v \in y \Rightarrow \Box_v \in z)v)$ $\Rightarrow (\Box_{u'} \in x \Rightarrow \Box_{u'} \in z))u'$
$^{8}\mathrm{kvs}(7)$	$((\forall u(\Box_u \in x \Rightarrow \Box_u \in y)u \wedge \forall v(\Box_v \in y \Rightarrow \Box_v \in z)v)$ $\Rightarrow \forall u'(\Box_{u'} \in x \Rightarrow \Box_{u'} \in z)u')$
$^{9}\mathrm{m}3.1(8)$	$((x \subseteq y \wedge y \subseteq z) \Rightarrow x \subseteq z)$
$^{10}\forall(9)$	$\forall z((x \subseteq y \wedge y \subseteq \Box_z) \Rightarrow x \subseteq \Box_z)$
$^{11}\forall,\forall(10)$	$\forall x \forall y \forall z((\Box_x \subseteq \Box_y \wedge \Box_y \subseteq \Box_z) \Rightarrow \Box_x \subseteq \Box_z)zyx$

□

Tämä ensimmäinen todistus on pyritty esittämään esimerkin vuoksi mahdollisimman täydellisenä, vaikka siinäkin on kaksi pientä oikaisua: Rivillä 2 on kaavamallia 24 sievennetty kaavamallin 11 mukaisesti. Rivillä 9 on käytetty määritelmää 3.1 kolmeen kertaan. Samoin viimeisellä rivillä on rivin 10 mallin mukaisesti käytetty sääntöä $\forall(n)$ mutta kahdesti samalla kertaa. Sääntöjen yhdistelmiä käytetään jatkossa runsaammin todistusten lyhentämiseksi. Esimerkiksi rivien 3–5 tylsän tekniseen päättelyyn voitaisiin viitata lyhyesti sääntöyhdistelmällä "k^{24},MP,MP".

Määritelmä 3.3. Jos x ja y ovat joukkoja, niin sanotaan, että x on identti-

nen joukon y kanssa täsmälleen silloin, kun x sisältyy joukkoon y ja y sisältyy joukkoon x. Formaalisesti:

$$x = y :: (x \subseteq y \wedge y \subseteq x)$$

Määritelmän 3.3 esittelemä identiteettirelaatio on malliesimerkki ekvivalenssirelaatiosta. Tämä tarkoittaa sitä, että se on refleksiivinen, transitiivinen ja symmetrinen. Refleksiivisyys tarkoittaa, että kukin joukko on identtinen itsensä kanssa. Transitiivisuus tarkoittaa vastaavaa kuin sisältymisrelaation tapauksessa. Identiteettirelaatio on symmetrinen, koska jos joukko x on identtinen joukon y kanssa, myös päinvastainen pitää paikkansa eli y on identtinen joukon x kanssa.

Lause 3.4. *Identiteettirelaatio, jonka relaatiosymboli on $=$, on refleksiivinen, transitiivinen ja symmetrinen. Toisin sanoen se on ekvivalenssirelaatio. Formaalisesti:*

$$\text{a)}\quad \forall x \Box_x = \Box_x x$$

$$\text{b)}\quad \forall x \forall y \forall z((\Box_x = \Box_y \wedge \Box_y = \Box_z) \Rightarrow \Box_x = \Box_z) zyx$$

$$\text{c)}\quad \forall x \forall y (\Box_x = \Box_y \Leftrightarrow \Box_y = \Box_x) yx$$

Todistus. Todistetaan näistä helpoista tuloksista vain kohta b:

^{1}L3.2,$\forall\leftarrow$,$\forall\leftarrow$,$\forall\leftarrow$	$((x \subseteq y \wedge y \subseteq z) \Rightarrow x \subseteq z)$
^{2}k^{34}	$(((x \subseteq y \wedge y \subseteq z) \Rightarrow x \subseteq z)$ $\Rightarrow (((z \subseteq y \wedge y \subseteq z) \wedge (x \subseteq y \wedge y \subseteq z)) \Rightarrow x \subseteq z))$
^{3}MP(1,2)	$(((z \subseteq y \wedge y \subseteq x) \wedge (x \subseteq y \wedge y \subseteq z)) \Rightarrow x \subseteq z)$
^{4}L3.2,$\forall\leftarrow$,$\forall\leftarrow$,$\forall\leftarrow$	$((z \subseteq y \wedge y \subseteq x) \Rightarrow z \subseteq x)$
^{5}k^{34},s^{5},MP	$(((z \subseteq y \wedge y \subseteq x) \wedge (x \subseteq y \wedge y \subseteq z)) \Rightarrow z \subseteq x)$
^{6}k^{23},MP,MP	$((((z \subseteq y \wedge y \subseteq x) \wedge (x \subseteq y \wedge y \subseteq z)) \Rightarrow x \subseteq z)$ $\wedge(((z \subseteq y \wedge y \subseteq x) \wedge (x \subseteq y \wedge y \subseteq z)) \Rightarrow z \subseteq x))$
^{7}s^{15}(6)	$(((z \subseteq y \wedge y \subseteq x) \wedge (x \subseteq y \wedge y \subseteq z)) \Rightarrow (x \subseteq z \wedge z \subseteq x))$
^{8}s^{13,5}(7)	$(((x \subseteq y \wedge y \subseteq x) \wedge (y \subseteq z \wedge z \subseteq y)) \Rightarrow (x \subseteq z \wedge z \subseteq x))$
^{9}m3.3(8)	$((x = y \wedge y = z) \Rightarrow x = z)$
$^{10}\forall$,$\forall$,$\forall$(9)	$\forall x \forall y \forall z((\Box_x = \Box_y \wedge \Box_y = \Box_z) \Rightarrow \Box_x = \Box_z) zyx$

□

Selvästikin $(x = y \Leftrightarrow \forall z(\square_z \in x \Leftrightarrow \square_z \in y)z)$. Todistusten lyhentämiseksi tätä kaavaa käytetään ikään kuin identtisyyden määritelmänä, ja siihen viitataan lyhenteellä m3.1,3.3 tai m3.3,3.1.

3.2 Unioni, leikkaus, potenssijoukko ja kahden joukon yhdiste

Jos x on joukko eli vakio, voidaan joukon x avulla muodostaa (tai toiselta filosofiselta näkökannalta katsottuna tietää olemassa olevaksi) monenlaisia joukkoja: Unioni joukossa x eli joukon x jäsenten unioni on joukko, jonka jäseniä ovat kaikki joukon x jäsenten jäsenet mutteivät mitkään muut joukot. Leikkaus joukossa x eli joukon x jäsenten leikkaus on joukko, jonka jäsenet ovat joukon x jokaiselle jäsenelle yhteiset jäsenet. Joukon x potenssijoukko on joukko, jonka jäseninä ovat kaikki joukon x osajoukot. Unioniin, leikkaukseen ja potenssijoukkoihin viittaminen joukkoina mahdollistetaan formaalisti aksioomissa 1, 2 ja 3. Lisäksi tarvitaan yhdistämisaksiooma (saks. *Axiom der Paarung*), joka mahdollistaa kahden joukon yhdistämisen joukoksi, jonka jäseniä ovat ainoastaan nämä kaksi joukkoa.

Aksiooma 1 (A$\cup$)**.** Unioni joukossa x on joukko.

$$\forall x \exists y \forall z(\square_z \in \square_y \Leftrightarrow \exists u(\square_u \in \square_x \wedge \square_z \in \square_u)u)zyx$$

Aksiooma 2 (A$\cap$)**.** Leikkaus joukossa x on joukko.

$$\forall x \exists y \forall z(\square_z \in \square_y \Leftrightarrow \forall u(\square_u \in \square_x \Rightarrow \square_z \in \square_u)u)zyx$$

Aksiooma 3 (A$\mathcal{P}$)**.** Jos x on joukko, voidaan viitata joukon x potenssijoukkoon eli joukkoon, jonka jäsenet ovat joukon x osajoukot.

$$\forall x \exists y \forall z(\square_z \in \square_y \Leftrightarrow \square_z \subseteq \square_x)zyx$$

Aksiooma 4 (Ayhd)**.** Jos x ja y ovat joukkoja, on olemassa joukko, jonka jäsenet ovat täsmälleen nämä joukot.

$$\forall x \forall y \exists z \forall u(\square_u \in \square_z \Leftrightarrow (\square_u = \square_x \vee \square_u = \square_y))uzyx$$

Määritelmä 3.5. Määritellään unionin, leikkauksen, potenssijoukon ja yhdistetyn joukon kaavoille lyhennysmerkinnät.

- $(y) \bigcup u :: \forall x(\square_x \in y \Leftrightarrow \exists z(\square_z \in u \wedge \square_x \in \square_z)z)x$

- $(y)\bigcap u :: \forall x(\square_x \in y \Leftrightarrow \forall z(\square_z \in u \Rightarrow \square_x \in \square_z)z)x$
- $(y)\mathscr{P}u :: \forall x(\square_x \in y \Leftrightarrow \square_x \subseteq u)x$
- $(y)\Big\{u, v\Big\} :: \forall x(\square_x \in y \Leftrightarrow (\square_x = u \vee \square_x = v))x$

Määritellyt kaavat näyttävät hieman oudoilta, koska kaikkien oikean puolen kaavan vapaiden muuttujien täytyy esiintyä vasemmalla puolella. Merkinnän $(y)\bigcap u$ voi lukea vaikkapa "y on leikkaus joukossa u" ja muut merkinnät vastaavalla tavalla. Käytännössä tätä määritelmää käytetään esimerkiksi sijoituksessa $(\square_x)\bigcup yx \leftarrow c$. Määritelmän 3.5 mukaan aksiooma 1 voidaan kirjoittaa muodossa $\forall x\exists z(\square_z)\bigcup \square_x zx$, aksiooma 2 muodossa $\forall x\exists z(\square_z)\bigcap \square_x zx$, aksiooma 3 muodossa $\forall x\exists z(\square_z)\mathscr{P}\square_x zx$ ja aksiooma 4 muodossa $\forall x\forall y\exists z(\square_z)\Big\{\square_x, \square_y\Big\}zyx$.

Nämä neljä ensimmäistä joukko-opin aksioomaa ovat niin sanottuja ehdollisia olemassaoloaksioomia, joiden avulla voidaan määritellä uusia joukkoja jo olemassaolevista joukoista. Ne ovat ehdollisia siksi, ettei päättelysääntöä $\exists\leftarrow(n)$ voi käyttää näihin aksioomiin, mikäli uloimpien universaalikvanttoreiden sitomien muuttujien tilalle ei sijoiteta vakioita. Päättelysääntö nimittäin vaatii, että eksistentiaalikvanttorilla muodostettu kaava, johon sitä sovelletaan, on lause.

Määritelmän 3.5 esittelemien merkintöjen sijasta olisi mukavampi käyttää tuttuja merkintöjä $\cup a$, $\cap a$, $\mathcal{P}a$ ja $\{a, b\}$. Nämä tutut merkinnät eivät kuitenkaan ole kaavoja, jotka voitaisiin esitellä määritelmässä, vaan ne tarkoittavat joukkoja eli ne ovat yleisiä vakioita. Onkin järkevää sopia, ettei vakion tarvitse olla yksi ainoa symboli tai yhden symbolin ja muutaman yläpilkun $'$ muodostama yhdistelmä. Niinpä vakioksi sopii mikä tahansa vielä käyttöönottamaton symboli tai symboliyhdistelmä, joka ei johda epämääräisiin merkintöihin. Esimerkiksi kahden joukon unionia ei voi merkitä yhdistelmällä $a \cup b$, koska silloin ei tietäisi, tarkoittaako merkintä $a \cup b \cup c$ joukkojen $a \cup b$ ja c vai joukkojen a ja $b \cup c$ unionia. Tällaista uuden vakion käyttöönottamista kutsutaan vakion eli joukon *määrittelyksi* (ei siis *määritelmäksi*).

Joukon määrittely on muotoa $a : \mathrm{A}x \leftarrow a$, missä A on kaava, jonka ainoa vapaa muuttuja on x, ja a on yleinen vakio, jonka sijaan on määrittelyyn kirjoitettu uusi vakiota tarkoittava symboli tai symboliyhdistelmä. Jos määritelty uusi symboliyhdistelmä sisältää vakioita, näiden vakioiden on esiinnyttävä kaavassa A. Jos yleinen vakio esiintyy kaavassa A, sen täytyy olla osana määriteltävää symboliyhdistelmää. Yleisten vakioiden tilalle voidaan

määrittelyä käytettäessä sijoittaa mitä tahansa vakioita. Jos määrittelyssä esiintyy tälläisia yleisiä vakioita, se esittelee uuden yleisen vakiomerkinnän (esim. $(a \cup b)$ on yleinen vakiomerkintä). Jos määrittelyssä ei esiinny yleisiä vakioita, se määrittelee aidon vakion (esim. $\emptyset$ on aito vakio).

Määritellyn vakiomerkinnän ei pitäisi sisältää muuttujia. Poikkeuksena muuttujan sisällyttäminen hyväksytään määrittelylle 3.13, koska siinä muuttujan käyttäminen ei aiheuta sekaannusta. Informaalisen tekstin joukossa vakiomerkintöihin sijoitetaan muuttujia havainnollisuuden tähden. Niinpä formaalisen tekstin ulkopuolella esimerkiksi lauseessa 3.17 kirjoitetaan $\{u, v\} \in \mathcal{P}(a \cup b)$ eikä $((x)\left\{u, v\right\} \Rightarrow x \in \mathcal{P}(a \cup b))$, jota muotoa on itse todistuksessa käytettävä.

Kun jokin symboliyhdistelmä on määritelty vakioksi, samaa symboliyhdistelmää ei saa enää määritellä miksikään muuksi. Muodossa $a : \mathrm{A}x \leftarrow a$ määriteltyä vakiota a voidaan esimerkiksi käyttää lauseiden väitteissä, jolloin todistuksessa on vaadittava esiintyväksi rivi $\mathrm{A}x \leftarrow a$, ellei ole todistettu lausetta $\exists x \mathrm{A}x$ tai ellei muuten ole selvää, että vakioksi määritelty symboliryhmä viittaa olemassa olevaan joukkoon. Uusista vakiomerkinnöistä on vielä huomattava, ettei vakiomerkinnän sisäinen vakion esiintymä ole vakion esiintymä kaavassa. Esimerkiksi kaavassa $\emptyset \subseteq (a \cup b)$ ei ole yhtään vakion a esiintymää, koska vakiomerkintä $(a \cup b)$ on miellettävä kaavassa yhdeksi symboliksi. Tämän takia pelkät vakioiden kuten $\{a, b\}$ määrittelyt eivät riitä vaan tarvitaan kaavan $(z)\left\{x, y\right\}$ tapaisten oudon oloisten kaavojen määritelmiä.

Sanotaan, että määrittelyllä $a : \mathrm{A}x \leftarrow a$ määritelty joukko on *yksikäsitteinen*, mikäli on olemassa todistus, jossa on rivit $\mathrm{A}x \leftarrow b$, $\mathrm{A}x \leftarrow c$ ja $b = c$. Toisin sanoen on voitava todistaa väite $[\mathrm{A}x \leftarrow b, \mathrm{A}x \leftarrow c]b = c$. Esimerkiksi jos a ja b ovat joukkoja, niin joukot $\{a, b\}$, $(a \cup b)$, $(a \cap b)$ ja $\mathcal{P}a$ ovat yksikäsitteisiä.

Määrittely 3.6. Määritellään unionia, leikkausta, potenssijoukkoa, kahden joukon yhdistettä, kahden joukon unionia, kahden joukon leikkausta ja kolmen joukon yhdistettä tarkoittavat yleiset vakiot. Määrittelyt ovat määrittelevien kaavojen $\Leftrightarrow$-konnektiivin ansiosta yksikäsitteiset.

- $\cup a : (\square_x) \bigcup ax \leftarrow \cup a$
- $\cap a : (\square_x) \bigcap ax \leftarrow \cap a$

- $\mathcal{P}a : (\square_x)\mathscr{P}ax \leftarrow \mathcal{P}a$
- $\{a,b\} : (\square_x)\Big\{a,b\Big\}x \leftarrow \{a,b\}$
- $(a \cup b) : \forall x(\square_x \in \square_y \Leftrightarrow (\square_x \in a \vee \square_x \in b))xy \leftarrow (a \cup b)$
- $(a \cap b) : \forall x(\square_x \in \square_y \Leftrightarrow (\square_x \in a \wedge \square_x \in b))xy \leftarrow (a \cap b)$
- $\{a\} : (\square_x)\Big\{a,a\Big\}x \leftarrow \{a\}$
- $\{a,b,c\} : \forall x(\square_x \in \square_y \Leftrightarrow ((\square_x = a \vee \square_x = b) \vee \square_x = c))xy \leftarrow \{a,b,c\}$

Jos a ja b ovat joukkoja, myös $\cup a$, $\cap b$, $\mathcal{P}a$, $\{b\}$ ja $\{a,b\}$ ovat joukkoja. Esimerkiksi yhdistämisaksiooman nojalla todistukseen voidaan kirjoittaa sijoitusmerkintä $(\square_x)\Big\{a,b\Big\}x \leftarrow \{a,b\}$, koska vakiot a ja b voidaan sijoittaa aksiooman uloimpien universaalikvanttorien sitomien muuttujien tilalle. Toisaalta mikään aksiooma ei suoraan varmista joukkojen $(a \cup b)$, $(a \cap b)$ tai $\{a,b,c\}$ olemassaoloa. Todistetaan siksi seuraava lause. Tarkoitus on myös osoittaa, etteivät esitettyjen aksioomien, määritelmän ja määrittelyn lupaukset monenlaisten joukkojen muodostamisen mahdollisuudesta ja tuttujen joukko-opin operaatiosymboleiden käyttökelpoisuudesta jää aivan kokonaan sokean uskon asiaksi.

Lause 3.7. *Oikeastaan* $(a \cup b)$ *on vaihtoehtoinen merkintä joukolle* $\cup\{a,b\}$. *Kahden joukon unioni on siis olemassa.*

$$a,b :\Rightarrow: [\forall x(\square_x \in \square_y \Leftrightarrow (\square_x \in a \vee \square_x \in b))xy \leftarrow (a \cup b)](a \cup b) = \cup\{a,b\}$$

Todistus. Unioniaksiooma on sisemmän eksistentiaalikvanttorikaavansa vuoksi hieman hankala käytettäväksi. Joukolla $\{a,b\}$ on kuitenkin vain kaksi jäsentä, joten unionin muodostaminen siinä ei ole kohtuuttoman vaikeaa. On olemassa sellainen z, että $y \in z$ ja $z \in \{a,b\}$, jos ja vain jos z on identtinen joko joukon a tai joukon b kanssa. Niinpä $y \in \cup\{a,b\}$ täsmälleen silloin, kun y on joukon a tai joukon b jäsen, mikä tarkoittaa sitä, että $y \in (a \cup b)$.

[1]Ayhd	$\forall x\forall y\exists u\forall z(\square_z \in \square_u \Leftrightarrow (\square_z = \square_x \vee \square_z = \square_y))zuyx$
[2]$\forall\leftarrow$,$\forall\leftarrow$(1)	$\exists u\forall z(\square_z \in \square_u \Leftrightarrow (\square_z = a \vee \square_z = b))zu$
[3]$\exists\leftarrow$(2)	$\forall z(\square_z \in \square_u \Leftrightarrow (\square_z = a \vee \square_z = b))zu \leftarrow \{a,b\}$
[4]sij,$\forall\leftarrow$(3)	$(z \in \{a,b\} \Leftrightarrow (z = a \vee z = b))$

[5]$\forall,\forall\leftarrow$(4),k[25],MP $((a = a \vee a = b) \Rightarrow a \in \{a, b\})$

[6]L3.4 $a = a$

[7]k[26],MP $(a = a \vee a = b)$

[8]MP(7,5) $a \in \{a, b\}$

[9]k[23],MP $(x \in a \Rightarrow (a \in \{a, b\} \wedge x \in a))$

[10]kvs $((a \in \{a, b\} \wedge x \in a) \Rightarrow \exists z(\Box_z \in \{a, b\} \wedge x \in \Box_z)z)$

[11]k[24],MP,MP $(x \in a \Rightarrow \exists z(\Box_z \in \{a, b\} \wedge x \in \Box_z)z)$

[12]kuten(11) $(x \in b \Rightarrow \exists z(\Box_z \in \{a, b\} \wedge x \in \Box_z)z)$

[13]k[23],MP,MP $((x \in a \Rightarrow \exists z(\Box_z \in \{a, b\} \wedge x \in \Box_z)z)$
$\wedge(x \in b \Rightarrow \exists z(\Box_z \in \{a, b\} \wedge x \in \Box_z)z))$

[14]k[27],MP $((x \in a \vee x \in b) \Rightarrow \exists z(\Box_z \in \{a, b\} \wedge x \in \Box_z)z)$

[15]k[20],m3.3,3.1 $((z = a \wedge x \in z) \Rightarrow (\forall y(\Box_y \in z \Leftrightarrow \Box_y \in a)y \wedge x \in z))$

[16]s[1,8],kvs(15) $((z = a \wedge x \in z) \Rightarrow \neg(x \in z \Rightarrow \exists y\neg(\Box_y \in z \Leftrightarrow \Box_y \in a)y))$

[17]kvs,kvs(16) $((z = a \wedge x \in z) \Rightarrow \forall y\neg(x \in z \Rightarrow \neg(\Box_y \in z \Leftrightarrow \Box_y \in a))y)$

[18]s[8,1],kvs,$\forall\leftarrow$(17) $((z = a \wedge x \in z) \Rightarrow ((x \in z \Leftrightarrow x \in a) \wedge x \in z))$

[19]k[28] $(((x \in z \Leftrightarrow x \in a) \wedge x \in z) \Rightarrow x \in a)$

[20]k[24],MP,MP $((z = a \wedge x \in z) \Rightarrow x \in a)$

[21]kuten(20) $((z = b \wedge x \in z) \Rightarrow x \in b)$

[22]k[23],MP,MP $(((z = a \wedge x \in z) \Rightarrow x \in a) \wedge ((z = b \wedge x \in z) \Rightarrow x \in b))$

[23]k[29],MP $(((z = a \wedge x \in z) \vee (z = b \wedge x \in z)) \Rightarrow (x \in a \vee x \in b))$

[24]k[30,24],MP,MP,s_4 $((z \in \{a, b\} \wedge x \in z) \Rightarrow (x \in a \vee x \in b))$

[25]ekvmp $((\exists z(\Box_z \in \{a, b\} \wedge x \in \Box_z)z \wedge ((z \in \{a, b\} \wedge x \in z) \Rightarrow$
$(x \in a \vee x \in b))) \Rightarrow \exists y(x \in a \vee x \in b)y)$

[26]s[5,11](25) $(((z \in \{a, b\} \wedge x \in z) \Rightarrow (x \in a \vee x \in b))$
$\Rightarrow (\exists z(\Box_z \in \{a, b\} \wedge x \in \Box_z)z \Rightarrow \exists y(x \in a \vee x \in b)y))$

[27]MP(24,26)	$(\exists z(\square_z \in \{a,b\} \wedge x \in \square_z)z \Rightarrow \exists y(x \in a \vee x \in b)y)$
[28]kvs(27)	$(\exists z(\square_z \in \{a,b\} \wedge x \in \square_z)z \Rightarrow (x \in a \vee x \in b))$
[29]k[23],MP,MP,s[1,3]	$(\exists z(\square_z \in \{a,b\} \wedge x \in \square_z)z \Leftrightarrow (x \in a \vee x \in b))$
[30]A$\cup$,$\forall\leftarrow$	$\exists y \forall x(\square_x \in \square_y \Leftrightarrow \exists z(\square_z \in \{a,b\} \wedge \square_x \in \square_z)z)xy$
[31]$\exists\leftarrow$(30)	$\forall x(\square_x \in \square_y \Leftrightarrow \exists z(\square_z \in \{a,b\} \wedge \square_x \in \square_z)z)xy \leftarrow \cup\{a,b\}$
[32]s$_{29}$,$\exists\leftarrow$(30)	$\forall x(\square_x \in \square_y \Leftrightarrow (\square_x \in a \vee \square_x \in b))xy \leftarrow (a \cup b)$
[33]sij,s$_{29}$(32)	$\forall x(\square_x \in (a \cup b) \Leftrightarrow \exists z(\square_z \in \{a,b\} \wedge \square_x \in \square_z)z)x$
[34]sij,$\forall\leftarrow$(31)	$(x \in \cup\{a,b\} \Leftrightarrow \exists z(\square_z \in \{a,b\} \wedge x \in \square_z)z)$
[35]s$_{34}$(33)	$\forall x(\square_x \in (a \cup b) \Leftrightarrow \square_x \in \cup\{a,b\})x$
[36]m3.1,3.3(35)	$(a \cup b) = \cup\{a,b\}$

□

Todistus osoittaa (rivi 32), että joukko $(a \cup b)$ on todella olemassa, kun a ja b ovat joukkoja. Samoin joukko $(a \cap b)$ on olemassa ja se on identtinen joukon $\cap\{a,b\}$ kanssa. Joukko $\{a,b,c\}$ taas on sama kuin joukko $(\{a,b\} \cup \{c\})$. Voidaan määritellä myös joukko $\{a,b,c,d\}$, joka on identtinen joukon $(\{a,b,c\} \cup \{d\})$ kanssa, ja samalla tavoin mikä tahansa äärellisen monen joukon yhdiste.

3.3 Tyhjästä on hyvä nyhjästä

On aika asettaa ensimmäinen absoluuttinen eli ehdoton olemassaoloaksiooma. Ehdolliset olemassaoloaksioomat alkavat universaalikvanttorilla $\forall$, joten ne eivät kerro minkään selvästi määritellyn joukon olemassaolosta. Ehdoton olemassaoloaksiooma alkaa eksistentiaalikvanttorilla $\exists$, ja niinpä sellaisella on mahdollista varmistaa tietyn ominaisuuden täyttävän joukon olemassaolo. Aksiooman A$\emptyset$ tarkoitus on asettaa olemassaoloon yksikäsitteinen joukko, jonka pohjalta ehdollisten olemassaoloaksioomien avulla voidaan muodostaa todellisuuden eli kaikkien joukkojen luokan joukkoja.

Mikä olisi järkevä joukko lähteä liikkeelle todellisuuden muodostamisessa (jos nyt ajatellaan todellisuus konstruoitavaksi)? Koska tähän asti asetetuista aksioomista yksikään ei varmista minkään selvästi määritellyn joukon ole-

massaoloa, ensimmäinen olemassa olevaksi asetettava joukko ei voi sisältää yhtään olemassa olevaa joukkoa. Koska toisaalta käsiteltävässä todellisuudessa ei ole perusalkioita, tämä joukko ei voi sisältää niitäkään. Siispä olemassaolevaksi asetettava joukko ei sisällä mitään, ja täten se on tyhjä joukko. Tämä voi tuntua ensikädeltä hyvinkin oudolta, mutta toisaalta se ei ole sen oudompaa, ettei joukoista koostuvaa todellisuutta ole olemassa, jos kaikki olevainen on joukkoja.

Aksiooma 5 (A$\emptyset$)**.** On olemassa tyhjä joukko.

$$\exists x \forall y \ \neg \square_y \in \square_x \ yx$$

Määrittely 3.8. Tyhjää joukkoa tarkoittavana vakiona käytetään symbolia $\emptyset$.

$$\emptyset : \forall y \ \neg \square_y \in \square_x \ yx \leftarrow \emptyset$$

Vakio $\emptyset$ on aito vakio eikä pelkästään yleinen vakio. Niinpä symbolia $\emptyset$ käytetään tässä merkityksessä koko tutkielmassa senkin vuoksi, että tyhjä joukko on yksikäsitteinen, kuten lause 3.10 osoittaa. Sitä ennen todistetaan yksikäsitteisyyden todistamisen avuksi seuraava lause.

Lause 3.9. *Tyhjä joukko $\emptyset$ on minkä tahansa joukon osajoukko.*

$$\forall x \ \emptyset \subseteq \square_x x$$

Todistus. Yksikään joukko ei kuulu tyhjään joukkoon. Jos siis oletetaan jonkin joukon z kuuluvan tyhjään joukkoon, seuraa ristiriita, mistä seuraa mitä vain, esimerkiksi se, että joukko z kuuluu myös mihin tahansa joukkoon x. Tämä tarkoittaa, että tyhjä joukko sisältyy joukkoon x.

[1]A$\emptyset$	$\exists y \forall z \neg \square_z \in \square_y zy$
[2]$\exists\leftarrow$(1)	$\forall z \neg \square_z \in \square_y zy \leftarrow \emptyset$
[3]sij,$\forall\leftarrow$(2)	$\neg z \in \emptyset$
[4]k[31]	$(\neg z \in \emptyset \Rightarrow (\neg\neg z \in \emptyset \Rightarrow z \in x))$
[5]MP(3,4)	$(\neg\neg z \in \emptyset \Rightarrow z \in x)$
[6]s[4],$\forall$,$\forall$(5)	$\forall x \forall z (\square_z \in \emptyset \Rightarrow \square_z \in \square_x) zx$
[7]m3.1(6)	$\forall x \ \emptyset \subseteq \square_x x$

□

Yksikäsitteisyyden (informaalisen) määritelmän vuoksi lauseen 3.10 todistuksen väitteessä vaaditaan rivit $\forall z \neg \Box_z \in \Box_y zy \leftarrow \emptyset'$ ja $\forall z \neg \Box_z \in \Box_y zy \leftarrow \emptyset''$. Jos siis nämä esiintyvät todistuksessa ja todistetuksi lauseeksi saadaan $\emptyset' = \emptyset''$, niin voidaan sanoa, että joukko $\emptyset : \forall y \neg \Box_y \in \Box_x yx \leftarrow \emptyset$ on yksikäsitteinen. Todistuksessa käytetään lausetta 3.9 kaksi kertaa, niin että sekä $\emptyset'$ että $\emptyset''$ sijoitetaan lauseen 3.9 joukon $\emptyset$ tilalle. Tämä on täysin sallittua, koska lausetta 3.9 voi ajatella mallina, miten sen tulos voidaan todistaa mille tahansa joukolle, joka määritellään samalla tavalla kuin tyhjä joukko.

Lause 3.10. *Tyhjä joukko on yksikäsitteinen.*

$$[\forall z \neg \Box_z \in \Box_y zy \leftarrow \emptyset',$$

$$\forall z \neg \Box_z \in \Box_y zy \leftarrow \emptyset'']$$

$$\emptyset' = \emptyset''$$

Todistus. Jos sekä $\emptyset'$ että $\emptyset''$ ovat kummatkin tyhjiä joukkoja, lauseen 3.9 mukaan kumpikin sisältyy kumpaankin eli ne ovat samat joukot.

[1]A$\emptyset$	$\exists y \forall z \neg \Box_z \in \Box_y zy$
[2]$\exists$(1)	$\forall z \neg \Box_z \in \Box_y zy \leftarrow \emptyset'$
[3]$\exists$(1)	$\forall z \neg \Box_z \in \Box_y zy \leftarrow \emptyset''$
[4]L3.9	$\forall x\ \emptyset' \subseteq \Box_x x$
[5]L3.9	$\forall x\ \emptyset'' \subseteq \Box_x x$
[6]$\forall\leftarrow$(4)	$\emptyset' \subseteq \emptyset''$
[7]$\forall\leftarrow$(5)	$\emptyset'' \subseteq \emptyset'$
[8]k^{23}	$(\emptyset' \subseteq \emptyset'' \Rightarrow (\emptyset'' \subseteq \emptyset' \Rightarrow (\emptyset' \subseteq \emptyset'' \wedge \emptyset'' \subseteq \emptyset')))$
[9]MP(6,8),m3.3	$(\emptyset'' \subseteq \emptyset' \Rightarrow \emptyset' = \emptyset'')$
[10]MP(7,9)	$\emptyset' = \emptyset''$

□

Todistetaan vielä yksi tyhjää joukkoa koskeva lause. Mikään joukko ei ole tyhjän joukon jäsen, mutta silti tyhjälläkin joukolla on osajoukko, nimittäin tyhjä joukko itse. Muita osajoukkoja sillä ei luonnollisestikaan ole. Niinpä

joukolla $\mathcal{P}\emptyset$ on vain yksi jäsen, mistä syystä joukolla $\mathcal{P}\mathcal{P}\emptyset$ on kaksi jäsentä: $\emptyset$ (joka on minkä tahansa joukon osajoukko) ja $\mathcal{P}\emptyset$. Joukolla $\mathcal{P}\mathcal{P}\mathcal{P}\emptyset$ on neljä jäsentä, joukolla $\mathcal{P}\mathcal{P}\mathcal{P}\mathcal{P}\emptyset$ kuusitoista, joukolla $\mathcal{P}\mathcal{P}\mathcal{P}\mathcal{P}\mathcal{P}\emptyset$ niitä on 2^{16} ja niin edelleen.

Lause 3.11. *Tyhjän joukon ainoa osajoukko on tyhjä joukko.*

$$\forall x(\square_x \subseteq \emptyset \Rightarrow \square_x = \emptyset)x$$

Todistus.

[1]L3.9,$\forall\leftarrow$	$\emptyset \subseteq x$
[2]k^{23}	$(\emptyset \subseteq x \Rightarrow (x \subseteq \emptyset \Rightarrow (\emptyset \subseteq x \wedge x \subseteq \emptyset)))$
[3]MP(1,2)	$(x \subseteq \emptyset \Rightarrow (\emptyset \subseteq x \wedge x \subseteq \emptyset))$
[4]m3.3(3)	$(x \subseteq \emptyset \Rightarrow \emptyset = x)$
[5]L3.4,$\forall\leftarrow$,$\forall\leftarrow$	$(\emptyset = x \Leftrightarrow x = \emptyset)$
[6]s$_5$,$\forall$(4)	$\forall x(\square_x \subseteq \emptyset \Rightarrow \square_x = \emptyset)x$

□

Esimerkki 3.12. *Osoitetaan esimerkin vuoksi, mitä tyhjästä voi nyhjästä. Tyhjän joukon olemassaolo mahdollistaa muun muassa vakioiden $\mathcal{P}\emptyset$ ja $\{\emptyset\}$ muodostamisen. Mielenkiintoista kyllä nämä ovat kuitenkin identtiset joukot, mikä tässä esimerkissä on tarkoitus todistaa.*

$$\mathcal{P}\emptyset = \{\emptyset\}$$

Todistus. Joukon $\mathcal{P}\emptyset$ jäsenet ovat tyhjän joukon osajoukot, joita on vain yksi: $\emptyset$. Joukko $\{\emptyset\}$ on sama kuin joukko $\{\emptyset, \emptyset\}$, eli kunkin sen jäsenistä täytyy olla $\emptyset$ tai $\emptyset$. Täten $\emptyset$ on myös joukon $\{\emptyset\}$ ainoa jäsen, joten se ja $\mathcal{P}\emptyset$ ovat samat joukot.

[1]A$\mathcal{P}$	$\forall x \exists y(\square_y)\mathscr{P}\square_x\ yx$
[2]$\forall\leftarrow$,$\exists\leftarrow$(1)	$(\square_y)\mathscr{P}\emptyset\ y \leftarrow \mathcal{P}\emptyset$
[3]sij,m3.5,$\forall\leftarrow$(2)	$(z \in \mathcal{P}\emptyset \Leftrightarrow z \subseteq \emptyset)$
[4]L3.11,$\forall\leftarrow$,m3.3	$(x \subseteq \emptyset \Rightarrow (x \subseteq \emptyset \wedge \emptyset \subseteq x))$
[5]k^{32}	$((x \subseteq \emptyset \wedge \emptyset \subseteq x) \Rightarrow x \subseteq \emptyset)$
[6]k^{23},MP,MP	$((x \subseteq \emptyset \Rightarrow (x \subseteq \emptyset \wedge \emptyset \subseteq x)) \wedge ((x \subseteq \emptyset \wedge \emptyset \subseteq x) \Rightarrow x \subseteq \emptyset))$

^{7}m3.3,s^{1,3}	$(x \subseteq \emptyset \Leftrightarrow x = \emptyset)$
^{8}s$_{7}$(3)	$(x \in \mathcal{P}\emptyset \Leftrightarrow x = \emptyset)$
^{9}Ayhd	$\forall x \forall y \exists z (\square_z) \Big\{ \square_x, \square_y \Big\} zyx$
$^{10}\forall\leftarrow$,$\forall\leftarrow$(9)	$\exists z (\square_z) \Big\{ \emptyset, \emptyset \Big\} z$
$^{11}\exists\leftarrow$,m3.5(10)	$\forall x (\square_x \in \square_z \Leftrightarrow (\square_x = \emptyset \vee \square_x = \emptyset)) xz \leftarrow \{\emptyset\}$
^{12}sij,s^{9},$\forall\leftarrow$(11)	$(x \in \{\emptyset\} \Leftrightarrow x = \emptyset)$
^{13}s$_{12}$,$\forall$(8)	$\forall x (\square_x \in \mathcal{P}\emptyset \Leftrightarrow \square_x \in \{\emptyset\}) x$
^{14}s^{3,1},kvs(13)	$(\forall y (\square_y \in \mathcal{P}\emptyset \Rightarrow \square_y \in \{\emptyset\}) y \wedge \forall z (\square_z \in \{\emptyset\} \Rightarrow \square_z \in \mathcal{P}\emptyset) z)$
^{15}m3.1,3.3(14)	$\mathcal{P}\emptyset = \{\emptyset\}$

□

3.4 Joukot, luokat ja separaatioaksiooma

Nyt kun ensimmäinen ehdoton olemassaoloaksiooma on asetettu, voidaan muodostaa jos monenmoisia joukkoja. Joukosta $\emptyset$ voidaan muodostaa joukko $\mathcal{P}\emptyset$, ja näistä kahdesta joukosta voidaan muodostaa joukko $\{\emptyset, \mathcal{P}\emptyset\}$, josta saadaan joukko $\mathcal{P}\{\emptyset, \mathcal{P}\emptyset\}$ ja niin poispäin. Tähän mennessä asetettujen aksioomien nojalla on itse asiassa olemassa tai on muodostettavissa lukematon määrä joukkoja ja joukkoja, joilla on lukematon määrä jäseniä. Lukematon ei tässä tarkoita loputonta tai ääretöntä siinä merkityksessä, joka äärettömälle matematiikassa tavallisesti annetaan. Esimerkiksi yhdestä joukosta voidaan potenssiaksiooman nojalla muodostaa joukkoja, joissa on yli miljoona tai yli triljoona jäsentä, tai vieläkin valtavampia joukkoja, mutta kussakin tällaisessa joukossa on aina tietty äärellinen määrä jäseniä, koska kukaan ei pysty loputtomiin toistamaan potenssijoukon muodostusoperaatiota.

Tämä äärellinen lukemattomuus – omalla tavallaan siis oikeastaan ääretömyys – ei kuitenkaan riitä, sillä matematiikka tarvitsee ääretöntään sen sille antamassa merkityksessä. On voitava puhua luonnollisten lukujen tai reaalilukujen äärettömistä joukoista. Vieläpä joskus viitataan kaikkien ordinaalien kokonaisuuteen (ks. esim. [16]: 74–79, jonka sivulla 79 ordinaalien luokkaa käytetään ikään kuin funktion määrittelyjoukkona). Näissä äärettömissä joukoissa tai kokonaisuuksissa on eroja. Luonnollisten lukujen joukko

on niin sanotusti numeroituvasti ääretön, kun taas reaalilukujen joukko on ylinumeroituvasti ääretön (näihin äärettömyyksiin palataan myöhemmin). Kaikkien ordinaalien kokonaisuus on jo niin hankala käsite, että kaikkien ordinaalien joukon olemassaolon olettaminen johtaa ristiriitaan (niin sanottu Burali-Fortin paradoksi, ks. paradokseista esim [1]: s. 481–492). Muun muassa tämä paradoksi pakottaa jollakin tavalla rajoittamaan sitä, minkälainen kuviteltavissa oleva kokonaisuus on joukko.

Tässä tutkielmassa sovitaan, että kaikkia kuviteltavissa olevia kokonaisuuksia kutsutaan luokiksi. Tämä ei tietenkään ole millään tavalla täsmällinen tai formaalinen määritelmä. Näin sopimalla voidaan puhua kaikkien joukkojen tai kaikkien ordinaalien luokista, vaikka vastaavia joukkoja ei ole olemassa. Toisaalta koska kaikki olevainen tämän tutkielman mukaan koostuu joukoista, näitä luokkiakaan ei ole olemassa. Silti esimerkiksi kaikkien joukkojen luokka on käyttökelpoinen käsite, ja oikeastaan $\forall$-kvanttori viittaa kaikkien joukkojen luokan joukkoihin. Luokan käsite on tässä esitetty väljästi, koska tutkielma hylkää luokat olemassaolevina tarkastelun kohteina. Luokkiakin on mahdollista käyttää matemaattisessa tarkastelussa, mutta silloin paradoksien välttämiseksi on esiteltävä esimerkiksi niin kutsuttu tyyppien teoria (ks. luokista [14]: s. 260–300).

Eräs tapa päästä äärettömyyksiin on määritellä joukkoja (tai luokkia) niiden jäsenten ominaisuuksien mukaan. Määritellään esimerkiksi joukko T, jonka jäseniä ovat kaikki joukot, joilla on jäsenenään tyhjä joukko. On helppo kuvitella esimerkkejä tällaisista joukoista. On myös helppo kuvitella, ettei kaikkia joukon T jäseniä millään pysty luettelemaan; niitä täytyy siis olla ääretön määrä. Tavanomaisesti esitettynä joukolle T voidaan kaiken lisäksi antaa hieno ulkomuoto: $T = \{x \text{ on joukko} \mid \emptyset \in x\}$. Tämän tutkielman merkinnöin esitellään joukon määrittely $T : \forall x(\square_x \in \square_y \Leftrightarrow \emptyset \in \square_x)xy \leftarrow T$.

Onneksi tämä T ei (luultavasti) kuitenkaan ole asetettujen eikä myöhemmin asetettavien aksioomien avulla todistettavissa olemassa olevaksi. Toisin sanoen ei voida todistaa lausetta $\exists y \forall x(\square_x \in \square_y \Leftrightarrow \emptyset \in \square_x)xy$. Tällainen tapa äärettömien joukkojen muodostamiseen ei olisi kovin sovelias. Jos ennen tuntemattomien ja rajoittamattoman suuruisten joukkojen olemassaolo voitaisiin todistaa, kun vain annettaisiin hyvin määritelty joukon jäsenten täyttämä ominaisuus, jouduttaisiin vaikeuksiin.

Näihin vaikeuksiin johtaa niin sanottu Russellin paradoksi. Russellin paradoksi syntyy, kun tarkastellaan joukon määrittelyä $a : \forall x(\square_x \in \square_y \Leftrightarrow$

$\neg\Box_x \in \Box_x)xy \leftarrow a$. Tavanomaisemmin merkinnöin tarkastellaan siis määrittelyä $a = \{x \text{ on joukko} \mid x \notin x\}$. Itsensä sisältämättömyyden ominaisuus on kaavalla $x \notin x$ eli $\neg x \in x$ hyvin muodostettu ominaisuus, ja heti löytyy esimerkkejä joukoista, jotka kuuluvat luokkaan a. Yksi tällainen joukko on tyhjä joukko, joka määrittelynsä perusteella kuuluu siihen selvästi. Luokka a itse ei voi kuitenkaan olla joukko. Jos a olisi joukko, pitäisi olla mahdollista kysyä, onko a itse joukon a jäsen, onko $a \in a$. Huomataan, että $(a \in a \Leftrightarrow \neg\, a \in a)$, mistä seuraa $(a \in a \wedge \neg\, a \in a)$ eli ristiriita.

Vaikka siis matemaattiseen äärettömyyteen pääseminen vaatiikin joukkoopissa eri keinot, ajatus joukon määrittelemisestä jonkin sen alkioita yhdistävän ominaisuuden avulla on hedelmällinen. Ennen tällaisen määrittelemisen mahdollistavaa aksioomaa on ratkaistava kaksi ongelmaa: mikä on hyvin muodostettu ominaisuus, ja miten voidaan välttää Russellin paradoksi?

Jälkimmäinen ongelma ratkeaa siten, ettei asetetakaan uutta joukkotodellisuutta avartavaa olemassaoloaksioomaa (esimerkiksi potenssiaksioома ja yhdistämisaksioома ovat Fraenkelin mukaan "'erweiternden' bedingten Existenzaxiome", [7]) vaan asetetaan joukkoa kaventava tai rajoittava ehdollinen olemassaoloaksioома (Fraenkelin mukaan valinta-aksioома ja pian esitettävä separaatioaksioома ovat "'einschränkenden' bedingten Existenzaxiome"). Tämä rajoitus toteutetaan niin, että joukko muodostetaan jäsentensä yhteisen ominaisuuden perusteella aina jonkin jo olemassaolevan joukon sisällä. Toisin sanoen aksioома 6 (saks. *Axiom der Aussonderung*, engl. *axiom of comprehension*) mahdollistaa viittamisen erilaisiin jo tunnettujen joukkojen osajoukkoihin.

Hyvin muodostettuja ominaisuuksia tuntuu luonnolliselta lähestyä kaavojen kautta. Kun siis halutaan tietää, onko olemassa joukkoa, jonka jäsenet täyttävät tietyn ehdon, kysytään itse asiassa, millä ehdoin voidaan tehdä sijoitus $\forall y(\Box_y \in \Box_x \Leftrightarrow \mathrm{A})yx \leftarrow a$, jossa A on kaavalyhennysmerkintä ja a on niiden jäsenten joukko, joille kaava A on tosi. Kuten tuli jo ilmi, yhden ehdoista täytyy olla se, että sijoituksen vakion a täytyy kuulua johonkin ennalta tunnettuun joukkoon. Toinen ehto, joka vaikuttaisi varmistavan ehkäpä liioitellunkin hyvin kaavalla ilmaistun ominaisuuden hyvän muodon, on, että kaavassa A ei saa olla muita vapaita muuttujia kuin mahdollisesti x (vrt. [8]: *axiom of comprehension* s. 31, joka ei kiellä vapaita muuttujia mutta jonka aksioома on sen vuoksi monimutkaisempi ja epämääräisempi).

On hyvä huomata, että kaavalyhennysmerkinnän harmittava välttämät-

tömyys separaatioaksiooman esittämisessä tekee siitä oleellisesti erilaisen aksiooman jo esitettyihin aksioomiin verrattuna. Kaavalyhennysmerkinnät ovat siinä mielessä informaalisia symboleja, ettei niitä voi formaalisessa todistuksessa käyttää. Niinpä separaatioaksiooma, jossa esiintyy kaavalyhennysmerkintä A, on oikeastaan aksioomarypäs tai aksioomamalli (engl. *axiom schema*), jota voi käyttää, kun kaavalyhennysmerkinnän tilalle kirjoitetaan mikä tahansa kaava, jossa ei ole muita vapaita muuttujia kuin mahdollisesti yksi (aksiooman z), joka sidotaan aksiooman kolmannella kvanttorilla.

Aksioома 6 (Separaatioaksiooma)**.** Kun kaavalyhennysmerkinnän A tilalle kirjoitetaan kaava, jossa z on ainoa mahdollinen vapaa muuttuja, seuraava on aksiooma:

$$\forall x \exists y \forall z (\square_z \in \square_y \Leftrightarrow (\square_z \in \square_x \wedge \mathrm{A}))zyx$$

Separaatioaksiooma tekee mahdolliseksi merkinnän $\{x \in a \mid \mathrm{A}\}$ käyttämisen. Määrittelyssä on outoa se, että määritelty vakiomerkintä sisältää vapaan muuttujan x, joka määrittelyn oikealla puolella on sidottu muuttuja. Tällainen pieni mukavuussyistä johtuva epäjohdonmukaisuus ei aiheuta hankaluuksia uuden yleisen vakion käytössä.

Määrittely 3.13. Kun a on vakio ja A on kaava, jossa x on ainoa mahdollinen vapaa muuttuja, määritellään (määrittely on yksikäsitteinen):

$$\{x \in a \mid \mathrm{A}\} : \forall x (\square_x \in \square_y \Leftrightarrow (\square_x \in a \wedge \mathrm{A}))xy \leftarrow \{x \in a \mid \mathrm{A}\}$$

Osoitetaan nyt, että *Axiom der Aussonderungin* esittäminen rajoittavana ehdollisena olemassaoloaksioomana ei tuota Russellin paradoksia. Oleellisesti tämä johtuu siitä, ettei joukko $b : \{x \in a \mid \neg x \in x\}$ ole joukon a jäsen, mikä suoraan kertoo, että $\neg b \in b$ pitää paikkansa eikä suinkaan $(b \in b \Leftrightarrow \neg b \in b)$.

Lause 3.14. *Jos a on joukko, joukko $\{z \in a \mid \neg z \in z\}$ ei ole sen jäsen.*

$$a :\Rightarrow: \neg\{z \in a \mid \neg z \in z\} \in a$$

Todistus. Oletetaan, että joukko b eli $\{x \in a \mid \neg\ x \in x\}$ kuuluu joukkoon a. Silloin jos $b \in b$, niin $\neg b \in b$, ja toisinpäin eli $(b \in b \Leftrightarrow \neg\ b \in b)$, mikä on ristiriita. Siksi b ei kuulu joukkoon a.

[1]A6	$\forall x \exists y \forall z (\square_z \in \square_y \Leftrightarrow (\square_z \in \square_x \wedge \neg\square_z \in \square_z))zyx$
[2]$\forall\leftarrow$(1)	$\exists y \forall z (\square_z \in \square_y \Leftrightarrow (\square_z \in a \wedge \neg\square_z \in \square_z))zy$

$^{3}\exists\leftarrow(2)$	$\forall z(\square_z \in \square_y \Leftrightarrow (\square_z \in a \wedge \neg\square_z \in \square_z))zy \leftarrow b$
^{4}sij(3)	$\forall z(\square_z \in b \Leftrightarrow (\square_z \in a \wedge \neg\square_z \in \square_z))z$
$^{5}\forall\leftarrow(4)$	$(b \in b \Leftrightarrow (b \in a \wedge \neg b \in b))$
^{6}k^{33},MP	$(b \in a \Rightarrow (b \in b \Leftrightarrow \neg b \in b))$
^{7}s$^{3,1}(6)$	$(b \in a \Rightarrow ((b \in b \Rightarrow \neg b \in b) \wedge (\neg b \in b \Rightarrow b \in b)))$
^{8}s$^{2}(7)$	$(b \in a \Rightarrow ((\neg b \in b \vee \neg b \in b) \wedge (b \in b \vee b \in b)))$
^{9}s$^{9}(8)$	$(b \in a \Rightarrow (\neg b \in b \wedge b \in b))$
^{10}s$^{8,7}(9)$	$((b \in b \vee \neg b \in b) \Rightarrow \neg b \in a)$
^{12}k^{20},s^{2}	$(b \in b \vee \neg b \in b)$
^{13}MP(12,11)	$\neg b \in a$
^{14}m3.13(13)	$\neg\{z \in a \mid \neg z \in z\} \in a$

□

Lausetta ei voi todistaa muodossa $\forall x \neg b \in \square_x x$, koska joukon b määrittely riippuisi muuttujasta x, mikä ei ole mahdollista. Tästä vajavaisuudestaan huolimatta lause 3.14 on tärkeä, koska sen merkityksen voidaan ajatella olevan $\forall x \exists y \neg\square_y \in \square_x yx$, joka taas kvs-säännön perusteella tarkoittaa samaa kuin $\neg\exists x \forall y \square_y \in \square_x yx$, eli ei ole olemassa kaikkien joukkojen joukkoa. Intuitiivisesti lähes samaa tarkoittaa lause 3.15, jonka mukaan millään joukolla ei voi olla jäseninään kaikkia joukkoja.

Lause 3.15 (Kaikkien joukkojen luokka ei saa olla joukko)**.** *Jos kaikkien joukkojen joukko on olemassa, teoria ajautuu ristiriitaan, koska millään joukolla ei ole jäseninään kaikkia joukkoja.*

$$a :\Rightarrow: \neg\forall x \square_x \in ax$$

Todistus. Jos kaikki joukot kuuluvat joukkoon a, niin silloin myös $\{z \in a \mid \neg z \in z\}$ kuuluu siihen. Toisaalta tämä ei lauseen 3.14 mukaan pidä paikkaansa, mistä seuraa ristiriita.

^{1}A6	$\forall x \exists y \forall z(\square_z \in \square_y \Leftrightarrow (\square_z \in \square_x \wedge \neg\square_z \in \square_z))zyx$
$^{2}\forall\leftarrow,\exists\leftarrow(1)$	$\forall z(\square_z \in \square_y \Leftrightarrow (\square_z \in a \wedge \neg\square_z \in \square_z))zy$ $\leftarrow \{z \in a \mid \neg z \in z\}$

^{3}L3.14	$\neg\{z \in a \mid \neg z \in z\} \in a$
^{4}k^{22},MP	$(\forall x \Box_x \in ax \Rightarrow \neg\{z \in a \mid \neg z \in z\} \in a)$
$^{5}\forall\leftarrow$	$(\forall x \Box_x \in ax \Rightarrow \{z \in a \mid \neg z \in z\} \in a)$
^{6}k^{23},MP,MP	$((\forall x \Box_x \in ax \Rightarrow \{z \in a \mid \neg z \in z\} \in a)$ $\wedge(\forall x \Box_x \in ax \Rightarrow \neg\{z \in a \mid \neg z \in z\} \in a))$
^{7}s^{15,2,18}(6)	$\neg\forall x \Box_x \in ax$

□

Jos siis kaikkien joukkojen joukko on olemassa, päädytään ristiriitaan, ja ristiriidasta voidaan johtaa mitä tahansa. Tällöinhän voidaan siis myös todistaa, ettei kaikkien joukkojen joukkoa ole olemassa. Siispä ainakin informaalisesti on pääteltävä, ettei tämän tutkielman tarkoittamaa todellisuutta eli kaikkien joukkojen luokkaa ole olemassa, ja formaalisesti todistettavien lauseiden suhteen toivottava, ettei kaikkien joukkojen luokkaa voida osoittaa joukoksi.

Mielenkiintoisena sivuseikkana kerrottakoon, että valehtelijan parodoksiksi kutsutaan paradoksia, joka saa alkunsa luonnollisen kielen lauseesta *tämä on valhe*. Jos lause on tosi, se on valhe eli epätosi. Jos lause on epätosi, se ei ole valhe eli se on tosi. Tämä paradoksi voidaan ratkaista, kun oletetaan, että jokainen lause sisältää väitteen, että lause on tosi. Tämä oletus ei aiheuta muutoksia niiden lauseiden totuusarvoon, jotka tavalliseen tapaan sanovat jotain jostain muusta kuin itsestään. Esimerkiksi lause *tämä on omena* saa saman totuusarvon kuin lause (*tämä on omena* $\wedge$ *tämä on totta*), olipa "tämä" sitten oikeasti omena tai vaikkapa päärynä. Kuitenkin hieman samaan tapaan kuin lauseesta $(b \in b \Leftrightarrow (b \in a \wedge \neg b \in b))$ (a ja b ovat kuin lauseessa 3.14) seuraa, että $\neg b \in b$, lauseesta *tämä on valhe* eli toisin sanoen lauseesta (*tämä on valhe* $\wedge$ *tämä on totta*) seuraa, että lause *tämä on valhe* on yksinkertaisesti epätosi. Luonnollisilla ja melko viattomilla rajoituksilla valehtelijan paradoksi ja Russellin paradoksi eivät olekaan mitään paradokseja. ([14]: s. 297, 298.)

3.5 Identtisyys

Intuitiivisesti ajateltuna identiteettirelaatio on vahvin (Bourbaki kutsuu sitä hienoimmaksi, *la plus fine*, ekvivalenssirelaatioksi, [2]: s. 121) kuviteltavissa

oleva relaatio – vahva siinä mielessä, että jos $a = b$, niin alkioiden a ja b välillä on niin vahva sidos, että missä tahansa esiintyy a voidaan kuvitella myös b esiintyväksi. Tietyssä mielessä siis merkin a voidaan katsoa olevan viittaus täsmälleen samaan alkioon, johon merkki b viittaa. Tämän ominaisuutensa ansiosta identiteettirelaatio on matemaattisesti tuottoisa, sillä yksinkertaisuudestaan huolimatta mahdollisuus vaihtaa a ja b päittäin on tehokas matemaattisissa todistuksissa.

Tämän mainitun tehokkuuden vuoksi esimerkin 3.12 kaltaiset tulokset ovat tärkeitä: esimerkin ansiosta tiedetään, että missä tahansa $\mathcal{P}\emptyset$ esiintyykin, tilalle voidaan vaihtaa $\{\emptyset\}$. Tämä ei kuitenkaan vielä tutkielman esittämien tietojen valossa pidä täysin paikkaansa. Tähän mennessä muodostettu teoria ei ole *une théorie égalitaire* (ks. [2]: s. 44–49) eli teoria, jossa on täysin esitetty identiteettirelaation universaali luonne, vaan identiteettirelaatio on määritelty sisältyvyysrelaation kautta kuulumisrelaatiolla. Vaihtoehtoisesti olisi voitu esittää esimerkiksi Bourbakin esittämien kaltaisia identiteettirelaatiota koskevia aksioomia kuten aksiooma, jonka mukaan alkiota a koskevat ominaisuudet ovat täsmälleen samat kuin alkiota b koskevat ominaisuudet, jos $a = b$. Ongelmana olisi kuitenkin ”ominaisuuksien” määritteleminen ja kaikkiin ominaisuuksiin viittaaminen. Helpompaa on esitellä yksi primitiivirelaatio, joka voidaan ajatella ainoaksi ominaisuudeksi, ja tämän avulla määritellä kaikki muut relaatiot, myös identiteettirelaatio.

Tämän valinnan seurauksena tutkielman aksioomien on erottava yleisesti esitetyistä, joihin kuuluu *ojentuvuusaksiooma* eli *l'axiome d'extensionalité* ([2]: s. 62, engl. *axiom of extensionality*): $\forall x \forall y((\square_x \subseteq \square_y \wedge \square_y \subseteq \square_x) \Rightarrow \square_x = \square_y)yx$. Tämä aksioomahan on sisällöltään lähes sama kuin määritelmä 3.3, mutta ajatus on olennaisesti erilainen. *L'axiome d'extensionalité* kertoo identiteettirelaation avulla sisältyvyysrelaation kautta kuulumisrelaation luonteesta: jos kahdella joukolla on täsmälleen samat jäsenet, joukot ovat identtisiä. Identtisyyden olemus siis jo tunnetaan. Määritelmä 3.3 taas kertoo identiteettirelaatiosta kuulumisrelaation avulla: jos kahdella joukolla on täsmälleen samat jäsenet, niitä kutsutaan identtisiksi. Identtisyyden olemusta siis vasta esitellään.

Vaikka tutkielman käsittelemä todellisuus koostuukin vain joukoista, määritelmän 3.3 suoma tieto ei otaksuttavasti kuitenkaan varusta identiteettirelaatiota sillä ominaisuudella, joka sille toivotaan: jos $a = b$, joukon a tilalle saadaan vaihtaa joukko b ja päinvastoin. Mitä puuttuu? Nimittäin jos

kuulumis- eli $\in$-relaatio on ainoa primitiivirelaatio tai ”primitiiviominaisuus”, eikö se yksin määritä joukkojen samuuden? Kyllä näin on, mutta määritelmä 3.3 yhdessä sievennyssopimuksen kanssa kertoo vasta sen, että jos $a = b$, joukon a saa vaihtaa joukkoon b, kun a esiintyy kaavassa $x \in a$. Miten voidaan olla varmoja, että vaihtaminen käy päinsä, kun $a \in x$?

Apuun tulee Abraham Fraenkel, joka esittää joukko-opin hieman eri tavalla. Hän esittää aksiooman *Axiom der Bestimmtheit* ([7]: s. 274), jota tässä tutkielmassa nimitetään *identtisyysaksioomaksi*. Sen sisältö on juuri se, mitä kaivataan: identtisillä joukoilla ei ole ainoastaan täsmälleen samat jäsenet, vaan ne ovat jäseniä täsmälleen samoille joukoille[5].

Aksiooma 7 (Identtisyysaksiooma)**.**

$$\forall x \forall y(\square_x = \square_y \Rightarrow \forall z(\square_x \in \square_z \Leftrightarrow \square_y \in \square_z)z)yx$$

Seuraava lause esittää formaalisesti edellä esitetyn ajatuksen siitä että, kaavat $x \in a$ ja $x \in b$ sekä $a \in y$ ja $b \in y$ ovat samoja kaavoja, kun $a = b$. Koska todistus on täysin tekninen ja lause suoralta kädeltä hyväksyttävä määritelmien 3.1 ja 3.3 sekä aksiooman 7 perusteella, todistus sivuutetaan.

Lause 3.16. *Jos joukot a ja b ovat identtisiä, kaava $x \in a$ on ekvivalentti kaavan $x \in b$ kanssa. Samoin ekvivalentteja ovat kaavat $a \in y$ ja $b \in y$.*

$$\forall u \forall v(\square_u = \square_v \Rightarrow (\forall x(\square_x \in \square_u \Leftrightarrow \square_x \in \square_v)x$$

$$\wedge \forall y(\square_u \in \square_y \Leftrightarrow \square_v \in \square_y)y))vu$$

Oletetaan, että a ja b ovat joukkoja ja että todistuksessa esiintyy rivi $a = b$. Lisäksi huomataan, että on mahdollista purkaa määritelmien perusteella lyhennetyt kaavat lyhentämättömiksi. Esimerkiksi kaava $a = x$ voidaan purkaa ja muokata muotoon $\forall y(\square_y \in a \Leftrightarrow \square_y \in x)y$. Koska $\in$-relaatio on ainoa primitiivirelaatio, muuttujia tai vakioita esiintyy puretussa kaavassa ainoastaan osakaavoissa, jotka ovat muotoa $x \in y$. Jos siis joukko a esiintyy jollakin kuvaillulla tavalla puretulla todistuksen rivillä, se esiintyy aina joko osakaavassa $a \in x$ tai $x \in a$, missä x on muuttuja tai vakio. Todistukseen voidaan lisätä lause 3.16 ja sijoittaa siihen a ja b:

[5]Tämä ei ole täysin täsmällisesti esitetty ajatus, koska joukon kaikki jäsenet muodostavat joukon, mutta kaikki joukot, joiden jäsen jokin tietty joukko on, eivät muodosta joukkoa.

$(\forall x(\square_x \in a \Leftrightarrow \square_x \in b)x \wedge \forall y(a \in \square_y \Leftrightarrow b \in \square_y)y)$, jonka nojalla todistukseen voi kirjoittaa lauseet $(x \in a \Leftrightarrow x \in b)$ ja $(a \in y \Leftrightarrow b \in y)$, missä muuttujien x ja y tilalle on voinut sijoittaa mitkä tahansa muuttujat tai esitellyt vakiot. Niinpä sievennyssopimuksen nojalla kaava $(a \in y)$ voidaan vaihtaa kaavaksi $(b \in y)$ ja kaava $(x \in a)$ voidaan vaihtaa kaavaksi $(x \in b)$.

Siispä lauseen 3.16 ja sievennyssopimuksen nojalla voidaan sopia voimaan asetettavaksi seuraava päättelysääntö:

id$^m(n)$ Jos a ja b ovat joukkoja ja jos todistuksen rivi m on lause $a = b$, niin mitkä tahansa rivin n kaavan tai sijoitusmerkinnän joukon a esiintymistä voidaan vaihtaa joukon b esiintymiksi ja päinvastoin.

Identtisyysaksiooman avulla todistetaan seuraava lause.

Lause 3.17. *Jos a ja b ovat joukkoja ja $u \in a$ ja $v \in b$, niin silloin $\{u, v\} \in \mathcal{P}(a \cup b)$.*

$$a, b :\Rightarrow: \forall u \forall v((\square_u \in a \wedge \square_v \in b)$$
$$\Rightarrow \forall x((\square_x)\left\{\square_u, \square_v\right\} \Rightarrow \square_x \in \mathcal{P}(a \cup b))x)vu$$

Todistus. Jos $u \in a$ ja $v \in b$, niin sekä $u \in (a \cup b)$ että $v \in (a \cup b)$. Jos $x \in \{u, v\}$, niin $x = u$ tai $x = v$, mistä identtisyysaksiooman nojalla seuraa, että $x \in (a \cup b)$. Siksi $\{u, v\} \subseteq (a \cup b)$ eli $\{u, v\} \in \mathcal{P}(a \cup b)$.

$^1\forall\leftarrow$,m3.5	$((x)\left\{u, v\right\} \Rightarrow (y \in x \Leftrightarrow (y = u \vee y = v)))$
^{2}k^{25}	$((y \in x \Leftrightarrow (y = u \vee y = v)) \Rightarrow (y \in x \Rightarrow (y = u \vee y = v)))$
^{3}k^{24},MP,MP	$((x)\left\{u, v\right\} \Rightarrow (y \in x \Rightarrow (y = u \vee y = v)))$
^{4}s^{11}(3),k^{34},MP	$(((u \in a \wedge v \in b) \wedge ((x)\left\{u, v\right\} \wedge y \in x)) \Rightarrow (y = u \vee y = v))$
^{5}A7	$\forall y \forall x(\square_y = \square_x \Rightarrow \forall z(\square_y \in \square_z \Leftrightarrow \square_x \in \square_z)z)xy$
$^6\forall\leftarrow,\forall\leftarrow$(5)	$(y = u \Rightarrow \forall z(y \in \square_z \Leftrightarrow u \in \square_z)z)$
^{7}kvs(6)	$\forall z(y = u \Rightarrow (y \in \square_z \Leftrightarrow y \in \square_z))z$
$^8\forall\leftarrow$(7)	$(y = u \Rightarrow (y \in a \Leftrightarrow y \in a))$
^{9}k^{25,24},MP,MP	$(y = u \Rightarrow (u \in a \Rightarrow y \in a))$
^{10}s^{11}(9)	$((u \in a \wedge y = u) \Rightarrow y \in a)$
^{11}k^{34},MP,s^{13}	$(((u \in a \wedge v \in b) \wedge y = u) \Rightarrow y \in a)$

[12]L3.7,∃← $\forall y(\Box_y \in \Box_x \Leftrightarrow (\Box_y \in a \vee \Box_y \in b))yx \leftarrow (a \cup b)$

[13]sij,∀←(12) $(y \in (a \cup b) \Leftrightarrow (y \in a \vee y \in b))$

[14]k[25],MP,k[35],MP $(y \in a \Rightarrow y \in (a \cup b))$

[15]k[24],MP,MP $(((u \in a \wedge v \in b) \wedge y = u) \Rightarrow y \in (a \cup b))$

[16]kuten(15) $(((u \in a \wedge v \in b) \wedge y = v) \Rightarrow y \in (a \cup b))$

[17]k[23],MP,MP $((((u \in a \wedge v \in b) \wedge y = u) \Rightarrow y \in (a \cup b))$
$\wedge(((u \in a \wedge v \in b) \wedge y = v) \Rightarrow y \in (a \cup b)))$

[18]s[36](17) $(((u \in a \wedge v \in b) \wedge (y = u \vee y = v)) \Rightarrow y \in (a \cup b))$

[19]s[11](18) $((u \in a \wedge v \in b) \Rightarrow ((y = u \vee y = v) \Rightarrow y \in (a \cup b)))$

[20]k[34],MP $(((u \in a \wedge v \in b) \wedge ((x)\Big\{u, v\Big\} \wedge y \in x))$
$\Rightarrow ((y = u \vee y = v) \Rightarrow y \in (a \cup b)))$

[21]k[23],MP,MP,s[15] $(((u \in a \wedge v \in b) \wedge ((x)\Big\{u, v\Big\} \wedge y \in x))$
$\Rightarrow ((y = u \vee y = v) \wedge ((y = u \vee y = v) \Rightarrow y \in (a \cup b))))$

[22]k[37],MP $(((u \in a \wedge v \in b) \wedge ((x)\Big\{u, v\Big\} \wedge y \in x)) \Rightarrow y \in (a \cup b))$

[23]s[13,11](22) $(((u \in a \wedge v \in b) \wedge (x)\Big\{u, v\Big\}) \Rightarrow (y \in x \Rightarrow y \in (a \cup b)))$

[24]∀,kvs(23) $(((u \in a \wedge v \in b) \wedge (x)\Big\{u, v\Big\})$
$\Rightarrow \forall y(\Box_y \in x \Rightarrow \Box_y \in (a \cup b))y)$

[25]m3.1(24) $(((u \in a \wedge v \in b) \wedge (x)\Big\{u, v\Big\}) \Rightarrow x \subseteq (a \cup b))$

[26]A$\mathcal{P}$,∀←,∃← $\forall z(\Box_z \in \Box_y \Leftrightarrow \Box_z \subseteq (a \cup b))zy \leftarrow \mathcal{P}(a \cup b)$

[27]sij,∀←(26) $(x \subseteq (a \cup b) \Leftrightarrow x \in \mathcal{P}(a \cup b))$

[28]s$_{27}$(25) $(((u \in a \wedge v \in b) \wedge (x)\Big\{u, v\Big\}) \Rightarrow x \in \mathcal{P}(a \cup b))$

[29]s[11],∀(28) $\forall x((u \in a \wedge v \in b) \Rightarrow ((\Box_x)\Big\{u, v\Big\} \Rightarrow \Box_x \in \mathcal{P}(a \cup b)))x$

[30]kvs,∀,∀(29) $\forall u \forall v((\Box_u \in a \wedge \Box_v \in b)$
$\Rightarrow \forall x((\Box_x)\Big\{\Box_u, \Box_v\Big\} \Rightarrow \Box_x \in \mathcal{P}(a \cup b))x)vu$

□

Rivi 16 päätellään kuten rivi 15 sillä poikkeuksella, että on käytettävä hyväksi konnektiivien kommutatiivisuutta ja todistettavissa olevaa kaavaa $(x \in (a \cup b) \Leftrightarrow x \in (b \cup a))$. Rivillä 21 on huomattava, että toinen $\wedge$-konnektiivilla yhdistetyistä kaavoista tulee riviltä 4 ja toinen riviltä 20. Rivin 12 viittaus lauseeseen 3.7 ei sääntöjen vastaisesti viittaa todistettuun lauseeseen vaan siihen sivutulokseen, että kahden joukon unioni on olemassa. Huomattakoon vielä, että todistuksen mallin mukaan voidaan todistaa sama lause, jossa osakaava $(x)\Big\{u, v\Big\}$ on korvattu kaavalla $(x)\Big\{u, u\Big\}$. Näin muutettua lausetta tarvitaan lauseen 3.21 todistuksessa.

3.6 Relaatio, funktio ja mahtavuus

Funktio on yksi keskeisimmistä joukko-opin ja koko matematiikan käsitteitä. Ennen funktion määrittelemistä on määriteltävä relaatio. Tässä ei täsmällisesti ottaen tarkoiteta samanlaista relaatiota kuin $\in$-primitiivirelaatio tai sen avulla määritellyt $\subseteq$- ja $=$-relaatiot vaan tietynlaisia joukkoja, joita kutsutaan relaatioksi. Relaation määrittelemistä varten täytyy määritellä ensin järjestetty pari (a, b) ja sitten kahden joukon karteesinen tulo $(a \times b)$.

Määritelmä 3.18. *Järjestetty pari* on kahden yhdistetyn joukon yhdistetty joukko.

$$(y)\Big(u, v\Big) :: \forall x(\square_x \in y \Leftrightarrow ((\square_x)\Big\{u, u\Big\} \vee (\square_x)\Big\{u, v\Big\}))x$$

Määritellään samalla yleinen vakiomerkintä järjestetylle parille.

$$(a, b) : (\square_y)\Big(a, b\Big)y \leftarrow (a, b)$$

Lause 3.19. *Järjestetty pari* (a, b) *on sama joukko kuin* $\{\{a\}, \{a, b\}\}$.

$$a, b :\Rightarrow: [(\square_y)\Big(a, b\Big)y \leftarrow (a, b)](a, b) = \{\{a\}, \{a, b\}\}$$

Todistus.

[1]Ayhd,$\forall\leftarrow$,$\forall\leftarrow$ $\quad \exists z(\square_z)\Big\{a, a\Big\}z$

[2]$\exists\leftarrow$(1) $\quad (\square_z)\Big\{a, a\Big\}z \leftarrow \{a\}$

[3]sij,m3.5,$\forall\leftarrow$(2) $\quad (y \in \{a\} \Leftrightarrow (y = a \vee y = a))$

[4]Ayhd,$\forall\leftarrow$,$\forall\leftarrow$	$\exists z(\square_z)\Big\{a,b\Big\}z$
[5]$\exists\leftarrow$(4)	$(\square_z)\Big\{a,b\Big\}z \leftarrow \{a,b\}$
[6]sij,m3.5,$\forall\leftarrow$(5)	$(z \in \{a,b\} \Leftrightarrow (z = a \vee z = b))$
[7]Ayhd,$\forall\leftarrow$,$\forall\leftarrow$	$\exists z(\square_z)\Big\{\{a\},\{a,b\}\Big\}z$
[8]$\exists\leftarrow$(7)	$(\square_z)\Big\{\{a\},\{a,b\}\Big\}z \leftarrow \{\{a\},\{a,b\}\}$
[9]sij,m3.5(8)	$\forall x(\square_x \in \{\{a\},\{a,b\}\} \Leftrightarrow (\square_x = \{a\} \vee \square_x = \{a,b\}))x$
[10]m3.1,3.3(9)	$\forall x(\square_x \in \{\{a\},\{a,b\}\} \Leftrightarrow (\forall y(\square_y \in \square_x \Leftrightarrow \square_y \in \{a\})y \vee$ $\forall z(\square_z \in \square_x \Leftrightarrow \square_z \in \{a,b\})z))x$
[11]$s_{3,6}$(10)	$\forall x(\square_x \in \{\{a\},\{a,b\}\} \Leftrightarrow (\forall y(\square_y \in \square_x \Leftrightarrow (\square_y = a \vee$ $\square_y = a))y \vee \forall z(\square_z \in \square_x \Leftrightarrow (\square_z = a \vee \square_z = b))z))x$
[12]m3.5(11)	$\forall x(\square_x \in \{\{a\},\{a,b\}\} \Leftrightarrow ((\square_x)\Big\{a,a\Big\} \vee (\square_x)\Big\{a,b\Big\}))x$
[13]$\forall\leftarrow$(12)	$(x \in \{\{a\},\{a,b\}\} \Leftrightarrow ((x)\Big\{a,a\Big\} \vee (x)\Big\{a,b\Big\}))$
[14]$\exists$,m3.18(12)	$\exists y(\square_y)\Big(a,b\Big)y$
[15]$\exists\leftarrow$(14)	$(\square_y)\Big(a,b\Big)y \leftarrow (a,b)$
[16]sij,$\forall\leftarrow$(15)	$(x \in (a,b) \Leftrightarrow ((x)\Big\{a,a\Big\} \vee (x)\Big\{a,b\Big\}))$
[17]s_{13},$\forall$(16)	$\forall x(\square_x \in (a,b) \Leftrightarrow \square_x \in \{\{a\},\{a,b\}\})x$
[18]m3.1,3.3(17)	$(a,b) = \{\{a\},\{a,b\}\}$

□

Todistetun lauseen lisäksi edellinen todistus osoitti, että jos a ja b ovat joukkoja, myös (a,b) on joukko. Riville 14 saatiin nimittäin pääteltyä lause $\exists y(\square_y)\Big(a,b\Big)y$, joka voidaan päätellä mille tahansa vakioille a ja b. Nimitys järjestetty pari johtuu siitä, että joukkojen järjestyksellä on väliä eli (a,b) ei välttämättä ole sama kuin (b,a). Tämä käy selväksi seuraavasta lauseesta.

Lause 3.20. *Jos a, b, a' ja b' ovat joukkoja, niin $(a,b) = (a',b')$ täsmälleen silloin, kun $a = a'$ ja $b = b'$.*

$$a,b,a',b' :\Rightarrow: ((a,b) = (a',b') \Leftrightarrow (a = a' \wedge b = b'))$$

Todistus. Jos $a = a'$ ja $b = b'$, on selvää, että näistä muodostetut järjestetyt parit (a, b) ja (a', b') ovat samat. Jos $a = b$, tulos on melko selvä toisinkinpäin. Jos a ja b ovat erisuuria ja $(a, b) = (a', b')$, niin joukko $\{a\}$ on yhden jäsenen joukko ja joukko $\{a, b\}$ kahden jäsenen joukko. Siksi toisen joukoista $\{a'\}$ ja $\{a', b'\}$ täytyy olla yhden jäsenen joukko ja toisen kahden jäsenen joukko. Siksi $\{a\} = \{a'\}$ ja $\{a, b\} = \{a', b'\}$. Koska $\{a\} = \{a'\}$, $a = a'$. Sitten voidaan päätellä yhtälöstä $\{a, b\} = \{a', b'\}$, että $b = b'$.

[1] ...	$a \in \{a, b\}$
[2] ...	$(a \in \{a', b'\} \Leftrightarrow (a = a' \vee a = b'))$
[3] k^{20},m3.3,3.1	$(\{a, b\} = \{a', b'\} \Rightarrow \forall x(\Box_x \in \{a, b\} \Leftrightarrow \Box_x \in \{a', b'\})x)$
[4] kvs,$\forall\leftarrow$(3)	$(\{a, b\} = \{a', b'\} \Rightarrow (a \in \{a, b\} \Leftrightarrow a \in \{a', b'\}))$
[5] $\mathrm{k}^{25,24}$,MP,MP	$(\{a, b\} = \{a', b'\} \Rightarrow (a \in \{a, b\} \Rightarrow a \in \{a', b'\}))$
[6] s^{10}(5)	$(a \in \{a, b\} \Rightarrow (\{a, b\} = \{a', b'\} \Rightarrow a \in \{a', b'\}))$
[7] MP(1,6)	$(\{a, b\} = \{a', b'\} \Rightarrow a \in \{a', b'\})$
[8] s_2(7)	$(\{a, b\} = \{a', b'\} \Rightarrow (a = a' \vee a = b'))$
[9] kuten(8)	$(\{a, b\} = \{a', b'\} \Rightarrow (b = a' \vee b = b'))$
[10] kuten(8)	$((a, b) = (a', b') \Rightarrow (\{a\} = \{a'\} \vee \{a\} = \{a', b'\}))$
[11] kuten(8)	$(\{a\} = \{a'\} \Rightarrow a = a')$
[12] kuten(6)	$(a' \in \{a', b'\} \Rightarrow (\{a\} = \{a', b'\} \Rightarrow a' \in \{a\}))$
[13] kuten(7)	$(\{a\} = \{a', b'\} \Rightarrow a' \in \{a\})$
[14] ...	$(a' \in \{a\} \Leftrightarrow a = a')$
[15] s_{14}(13)	$(\{a\} = \{a', b'\} \Rightarrow a = a')$
[16] k^{23},MP,MP	$((\{a\} = \{a'\} \Rightarrow a = a') \wedge (\{a\} = \{a', b'\} \Rightarrow a = a'))$
[17] k^{29},MP	$((\{a\} = \{a'\} \vee \{a\} = \{a', b'\}) \Rightarrow (a = a' \vee a = a'))$
[18] k^{24},MP,MP	$((a, b) = (a', b') \Rightarrow (a = a' \vee a = a'))$
[19] s^{9}(18)	$((a, b) = (a', b') \Rightarrow a = a')$

^{20}kuten(9) $((a,b)=(a',b')\Rightarrow(\{a,b\}=\{a'\}\vee\{a,b\}=\{a',b'\}))$

^{21}kuten(15) $(\{a,b\}=\{a'\}\Rightarrow b=a')$

^{22}k^{23},MP,MP $((\{a,b\}=\{a'\}\Rightarrow b=a')$
$\wedge(\{a,b\}=\{a',b'\}\Rightarrow(b=a'\vee b=b')))$

^{23}k^{29},MP $((\{a,b\}=\{a'\}\vee\{a,b\}=\{a',b'\})$
$\Rightarrow(b=a'\vee(b=a'\vee b=b')))$

^{24}s^{14,9}(23) $((\{a,b\}=\{a'\}\vee\{a,b\}=\{a',b'\})\Rightarrow(b=a'\vee b=b'))$

^{25}k^{24},MP,MP $((a,b)=(a',b')\Rightarrow(b=a'\vee b=b'))$

^{26}kuten(25) $((a,b)=(a',b')\Rightarrow(b'=a\vee b=b'))$

^{27}k^{23},MP,MP $(((a,b)=(a',b')\Rightarrow(b=a'\vee b=b'))$
$\wedge((a,b)=(a',b')\Rightarrow(b'=a\vee b=b')))$

^{28}s^{15,16}(27) $((a,b)=(a',b')\Rightarrow((b=a'\wedge b'=a)\vee b=b'))$

^{29}k^{38,24},MP,MP $((a,b)=(a',b')\Rightarrow(a=a'\vee b=b'))$

^{30}k^{23},MP,MP $(((a,b)=(a',b')\Rightarrow((b=a'\wedge b'=a)\vee b=b'))$
$\wedge((a,b)=(a',b')\Rightarrow(a=a'\vee b=b')))$

^{31}s^{15,16,13}(30) $((a,b)=(a',b')\Rightarrow(((a=a'\wedge b=a')\wedge b'=a)\vee b=b'))$

^{32}L3.4 $((a=a'\wedge b=a')\Rightarrow a=b)$

^{33}k^{34},MP $(((a=a'\wedge b=a')\wedge b'=a)\Rightarrow a=b)$

^{34}k^{32} $(((a=a'\wedge b=a')\wedge b'=a)\Rightarrow b'=a)$

^{35}k^{23},MP,MP,s^{15} $(((a=a'\wedge b=a')\wedge b'=a)\Rightarrow(a=b\wedge b'=a))$

^{36}L3.4 $((a=b\wedge b'=a)\Rightarrow b=b')$

^{37}k^{24},MP,MP,s^{2} $(\neg((a=a'\wedge b=a')\wedge b'=a)\vee b=b')$

^{38}k^{22},MP,k^{23},MP,MP $(((a,b)=(a',b')\Rightarrow(((a=a'\wedge b=a')\wedge b'=a)\vee b=b'))$
$\wedge((a,b)=(a',b')\Rightarrow(\neg((a=a'\wedge b=a')\wedge b'=a)\vee b=b')))$

^{39}s^{15,16,18}(38) $((a,b)=(a',b')\Rightarrow b=b')$

^{40}k^{23},MP,MP,s^{15} $((a,b)=(a',b')\Rightarrow(a=a'\wedge b=b'))$

^{41} ... $((a = a' \wedge b = b') \Rightarrow (a, b) = (a', b'))$

^{42}k^{23},MP,MP,s^{1,3} $((a, b) = (a', b') \Leftrightarrow (a = a' \wedge b = b'))$

□

Perustelulla ”kuten” on lyhennetty moni päättelyketju, koska yleistä vakiota koskeva päättely on helppo soveltaa muihinkin vakioihin (esim. vakion a tilalle sijoitetaan $\{a\}$), kunhan muistetaan tiettyjen konnektiivien kommutatiivisuus ja identiteettirelaation symmetrisyys. Rivit 1, 2 ja 14 ovat luonnollisia seurauksia yhdistämisaksioomasta, joten todistuksen tiivistämiseksi niiden perustelut sivuutetaan. Rivi 41 ei seuraa yhtä helposti, mutta sitä edeltävät rivit sivuutetaan, koska tulos on niin ilmeinen. Jos nimittäin todistukseen saataisiin kirjoittaa rivi $(a = a' \wedge b = b')$, id-päättelysäännön avulla voitaisiin helposti päätellä rivi $(a, b) = (a', b')$ (vaikkeikaan suoraan, koska lauseessa $(a, b) = (a', b')$ ei formaalisesti ole yhtään joukkojen a, b, a' tai b' esiintymää). Niin sanottu *deduktiolause* (ks. esim. [15]: s. 75–76 tai [1]: s. 219, 227–228) sanookin, että jos kaava B voidaan päätellä, kun sovitaan todistukseen kirjoitettavaksi kaava A, voidaan päätellä kaava (A ⇒ B). Tätä tulosta ei osoiteta tässä tutkielmassa, ja toki rivi 36 on todistettavissa tutkielman esittämin keinoin.

Lause 3.21. *Jos a ja b ovat joukkoja, $u \in a$ ja $v \in b$, niin silloin järjestetty pari (u, v) on joukon $\mathcal{PP}(a \cup b)$ jäsen.*

$$a, b :\Rightarrow:$$

$$\forall u \forall v((\square_u \in a \wedge \square_v \in b) \Rightarrow \forall y((\square_y)\Big(\square_u, \square_v\Big) \Rightarrow \square_y \in \mathcal{PP}(a \cup b))y)vu$$

Todistus. Lauseen 3.17 perusteella $\{u\} \in \mathcal{P}(a \cup b)$ ja $\{u, v\} \in \mathcal{P}(a \cup b)$. Vielä saman lauseen nojalla $\{\{u\}, \{u, v\}\} \in \mathcal{P}(\mathcal{P}(a \cup b) \cup \mathcal{P}(a \cup b))$, jossa $\{\{u\}, \{u, v\}\} = (u, v)$ ja $(\mathcal{P}(a \cup b) \cup \mathcal{P}(a \cup b)) = \mathcal{P}(a \cup b)$.

$^{1}\forall\leftarrow$,m3.18 $((y)\Big(u, v\Big) \Rightarrow (x \in y \Leftrightarrow ((x)\Big\{u, u\Big\} \vee (x)\Big\{u, v\Big\})))$

^{2}k^{25,24},MP,MP $((y)\Big(u, v\Big) \Rightarrow (x \in y \Rightarrow ((x)\Big\{u, u\Big\} \vee (x)\Big\{u, v\Big\})))$

^{3}k^{24},s^{8,1},MP $(((u \in a \wedge v \in b) \wedge (y)\Big(u, v\Big))$
$\Rightarrow ((x \in y \Rightarrow ((x)\Big\{u, u\Big\} \vee (x)\Big\{u, v\Big\})) \wedge (u \in a \wedge v \in b)))$

$^{4}\mathrm{k}^{32,22,24}$,MP,MP $(((x \in y \Rightarrow ((x)\Big\{u,u\Big\} \vee (x)\Big\{u,v\Big\})) \wedge (u \in a \wedge v \in b))$
$\Rightarrow (x \in y \Rightarrow (u \in a \wedge v \in b)))$

$^{5}\mathrm{k}^{32,23}$,MP,MP,s^{15} $(((x \in y \Rightarrow ((x)\Big\{u,u\Big\} \vee (x)\Big\{u,v\Big\})) \wedge (u \in a \wedge v \in b))$
$\Rightarrow (x \in y \Rightarrow (((x)\Big\{u,u\Big\} \vee (x)\Big\{u,v\Big\}) \wedge (u \in a \wedge v \in b))))$

$^{6}\mathrm{k}^{24}$,MP,MP,$\mathrm{s}^{7,6,16}$ $(((u \in a \wedge v \in b) \wedge (y)\Big(u,v\Big)) \Rightarrow (x \in y \Rightarrow (((x)\Big\{u,u\Big\} \wedge$
$(u \in a \wedge v \in b)) \vee ((x)\Big\{u,v\Big\} \wedge (u \in a \wedge v \in b)))))$

^{7}L3.17,$\forall\leftarrow$,$\forall\leftarrow$,s^{11} $(((x)\Big\{u,u\Big\} \wedge (u \in a \wedge v \in b)) \Rightarrow x \in \mathcal{P}(a \cup b))$

$^{8}\ldots$,k^{23},MP,MP $((((x)\Big\{u,u\Big\} \wedge (u \in a \wedge v \in b)) \Rightarrow x \in \mathcal{P}(a \cup b))$
$\wedge(((x)\Big\{u,v\Big\} \wedge (u \in a \wedge v \in b)) \Rightarrow x \in \mathcal{P}(a \cup b)))$

$^{9}\mathrm{k}^{27}$,MP $((((x)\Big\{u,u\Big\} \wedge (u \in a \wedge v \in b)) \vee ((x)\Big\{u,v\Big\} \wedge (u \in a \wedge v \in b)))$
$\Rightarrow x \in \mathcal{P}(a \cup b))$

$^{10}\mathrm{k}^{24}$,s^{10},MP $((x \in y \Rightarrow$
$(((x)\Big\{u,u\Big\} \wedge (u \in a \wedge v \in b)) \vee ((x)\Big\{u,v\Big\} \wedge (u \in a \wedge v \in b))))$
$\Rightarrow (x \in y \Rightarrow x \in \mathcal{P}(a \cup b)))$

$^{11}\mathrm{k}^{24}$,MP,MP $(((u \in a \wedge v \in b) \wedge (y)\Big(u,v\Big)) \Rightarrow (x \in y \Rightarrow x \in \mathcal{P}(a \cup b)))$

$^{12}\forall$,kvs,m3.1(11) $(((u \in a \wedge v \in b) \wedge (y)\Big(u,v\Big)) \Rightarrow y \subseteq \mathcal{P}(a \cup b))$

^{13} $\ldots$ $(y \in \mathcal{PP}(a \cup b) \Leftrightarrow y \subseteq \mathcal{P}(a \cup b))$

$^{14}\mathrm{s}^{11}_{13}$,$\forall$,kvs,$\forall$,$\forall$(12) $\forall u \forall v((\Box_u \in a \wedge \Box_v \in b)$
$\Rightarrow \forall y((\Box_y)\Big(\Box_u,\Box_v\Big) \Rightarrow \Box_y \in \mathcal{PP}(a \cup b))y)vu$

□

Määritelmä 3.22. Kahden joukon a ja b *karteesinen tulo* on joukko, johon kuuluu kaikki järjestetyt parit (u, v), missä $u \in a$ ja $v \in b$.

$$(y)\Big(u \times v\Big) :: \forall x(\Box_x \in y \Leftrightarrow \exists u' \exists v'((\Box_{u'} \in u \wedge \Box_{v'} \in v) \wedge (\Box_x)\Big(\Box_{u'},\Box_{v'}\Big))v'u')x$$

Määritellään samalla yleinen merkintä joukolle, joka on joukkojen a ja b karteesinen tulo:

$$(a \times b) : (\Box_x)\Big(a \times b\Big)x \leftarrow (a \times b)$$

Lause 3.23. *Jos a ja b ovat joukkoja, joukko $(a \times b)$ on olemassa.*

$$a, b :\Rightarrow: \exists y(\Box_y)\Big(a \times b\Big)y$$

Todistus. Separaatioaksiooma takaa karteesisen tulon olemassaolon, jos vain on olemassa joukko, jonka osajoukoksi karteesinen tulo voidaan osoittaa. Lause 3.21 osoittaa, että kaikki järjestetyt parit, joiden ensimmäinen jäsen kuuluu joukkoon a ja toinen jäsen joukkoon b, kuuluvat joukkoon $\mathcal{PP}(a \cup b)$, jonka osajoukko $(a \times b)$ siis on.

[1]L3.21,$\forall\leftarrow$,$\forall\leftarrow$	$((u \in a \wedge v \in b) \Rightarrow \forall x((\Box_x)\Big(u, v\Big) \Rightarrow \Box_x \in \mathcal{PP}(a \cup b))x)$
[2]kvs,$\forall\leftarrow$(1)	$((u \in a \wedge v \in b) \Rightarrow ((x)\Big(u, v\Big) \Rightarrow x \in \mathcal{PP}(a \cup b)))$
[3]s[11](2)	$(((u \in a \wedge v \in b) \wedge (x)\Big(u, v\Big)) \Rightarrow x \in \mathcal{PP}(a \cup b))$
[4]ekvmp	$((\exists v((u \in a \wedge \Box_v \in b) \wedge (x)\Big(u, \Box_v\Big))v \wedge$ $(((u \in a \wedge v \in b) \wedge (x)\Big(u, v\Big)) \Rightarrow x \in \mathcal{PP}(a \cup b)))$ $\Rightarrow \exists v'\ x \in \mathcal{PP}(a \cup b)\ v')$
[5]s[5,11](4),MP	$(\exists v((u \in a \wedge \Box_v \in b) \wedge (x)\Big(u, \Box_v\Big))v \Rightarrow \exists v'\ x \in \mathcal{PP}(a \cup b)\ v')$
[6]kvs	$(\exists v((u \in a \wedge \Box_v \in b) \wedge (x)\Big(u, \Box_v\Big))v \Rightarrow x \in \mathcal{PP}(a \cup b))$
[7]kuten(6)	$(\exists u \exists v((\Box_u \in a \wedge \Box_v \in b) \wedge (x)\Big(\Box_u, \Box_v\Big))vu$ $\Rightarrow x \in \mathcal{PP}(a \cup b))$
[8]s[17](7)	$((x \in \mathcal{PP}(a \cup b) \wedge \exists u \exists v((\Box_u \in a \wedge \Box_v \in b) \wedge (x)\Big(\Box_u, \Box_v\Big))vu)$ $\Leftrightarrow \exists u \exists v((\Box_u \in a \wedge \Box_v \in b) \wedge (x)\Big(\Box_u, \Box_v\Big))vu)$
[9]A6,$\forall\leftarrow$	$\exists y \forall x(\Box_x \in \Box_y \Leftrightarrow (\Box_x \in \mathcal{PP}(a \cup b) \wedge$ $\exists u \exists v((\Box_u \in a \wedge \Box_v \in b) \wedge (\Box_x)\Big(\Box_u, \Box_v\Big))vu))xy$
[10]s$_8$(9)	$\exists y \forall x(\Box_x \in \Box_y \Leftrightarrow$ $\exists u \exists v((\Box_u \in a \wedge \Box_v \in b) \wedge (\Box_x)\Big(\Box_u, \Box_v\Big))vu)xy$
[11]m3.22(10)	$\exists y(\Box_y)\Big(a \times b\Big)y$

□

Karteesisen tulon osajoukkoja kutsutaan *relaatioiksi*. Relaatio R on siis joukko, joka on jonkin karteesisen tulon osajoukko. Tyhjä joukko on tietenkin

relaatio kaikkien karteesisten tulojen osajoukkona. Esimerkiksi jos a ja b ovat joukkoja, separaatioaksiooman nojalla on olemassa joukko

$$R : \forall x(\square_x \in \square_r \Leftrightarrow (\square_x \in (a \times b) \wedge$$

$$\exists u \exists v((\square_x)\Big(\square_u, \square_v\Big) \wedge \square_u \in \square_v)vu))xr \leftarrow R.$$

Karteesisen tulon $(a \times b)$ osajoukkona R on relaatio. Tämä joukko on hyvä esimerkki siitä, miksi karteesisen tulon osajoukkoja kutsutaan relaatioksi. Merkitään $x\ R\ y$, jos joukkojen x ja y järjestetty pari on relaation R jäsen. Silloin

$$(x\ R\ y \Leftrightarrow (x \in y \wedge (x \in a \wedge y \in b))),$$

eli oikeastaan relaatio R on $\in$-relaation rajoittuma: jotta kahta joukkoa x ja y voitaisiin verrata R-relaatiolla, täytyy olla $x \in a$ ja $x \in b$, kun taas $\in$-relaatiolla voidaan verrata mitä tahansa kahta kaikkien joukkojen luokan jäsentä.

Relaatiota F, $F \subseteq (a \times b)$, kutsutaan *funktioksi*, jos jokaista joukon a jäsentä x kohti on olemassa sellainen yksikäsitteinen joukon b jäsen y, että joukkojen x ja y järjestetty pari kuuluu relaatioon F. Toisin ilmaisten relaatio F on funktio, jos aina kun $x \in a$, on olemassa yksi ja vain yksi sellainen $y \in b$, että $(x, y) \in F$. Koska funktio liittää jokaiseen joukon a jäseneen x täsmälleen yhden joukon b jäsenen y, on luontevaa ja perusteltua merkitä $F(x)$, joka viittaa joukkoon, jos x on joukko. Tätä merkintää käyttäen $y = F(x)$ täsmälleen silloin, kun $(x, y) \in F$.

Tärkeitä funktioon liittyviä käsitteitä ovat *injektio* ja *surjektio*. Funktio F, $F \subseteq (a \times b)$ (merkitään myös $F : a \to b$), on injektiivinen, jos $F(x) = F(x')$ vain silloin, kun $x = x'$. Se on surjektiivinen, jos $\{x \in \cup\cup F \mid x \in b\} = b$ eli jos funktion maalijoukko b on sama kuin arvojoukko eli niiden joukkojen $y \in b$ joukko, jotka jonkin joukon $x \in a$ kanssa muodostavat funktioon kuuluvan järjestetyn parin $(x, y) \in F$. Jos funktio on sekä injektio että surjektio, sitä kutsutaan *bijektioksi*.

Funktion ja bijektion käsitteille ei ole tässä tutkielmassa tarpeen esittää tarkkoja formaalisia määritelmiä, koska niitä tarvitaan vain joukkojen keskinäisen suhteellisen mahtavuuden määrittelyyn. Funktion ja bijektiivisen funktion täyttämät formaaliset ehdot voitaisiin muodostaa määritelmän 3.24 mallin mukaisesti.

Määritelmä 3.24. Jos x ja y ovat joukkoja ja on osoitettavissa olemassa olevaksi funktio f, $f \subseteq (x \times y)$, joka on bijektio, joukkoja x ja y sanotaan *mahtavuudeltaan* yhtäsuuriksi. Tällöin merkitään $x \sim y$.

$$x \sim y ::$$

$$\exists f(\forall x'(\square_{x'} \in x \Rightarrow \exists u((\square_u \in y \wedge \forall z((\square_z)\Big(\square_{x'}, \square_u\Big) \Rightarrow \square_z \in \square_f)z) \wedge$$

$$\forall u'((\square_{u'} \in y \wedge \forall z'((\square_{z'})\Big(\square_{x'}, \square_{u'}\Big) \Rightarrow \square_{z'} \in \square_f)z') \Rightarrow \square_u = \square_{u'})u')u)x'$$

$$\wedge \forall y'(\square_{y'} \in y \Rightarrow \exists v((\square_v \in x \wedge \forall w((\square_w)\Big(\square_v, \square_{y'}\Big) \Rightarrow \square_w \in \square_f)w) \wedge$$

$$\forall v'((\square_{v'} \in x \wedge \forall w'((\square_{w'})\Big(\square_{v'}, \square_{y'}\Big) \Rightarrow \square_{w'} \in \square_f)w') \Rightarrow \square_v = \square_{v'})v')v)y')f$$

Määritelmä on hankalan monimutkainen, ja silti siitä puuttuu kokonaan se ehto, että löydetyn joukon f täytyy olla joukkojen x ja y karteesisen tulon osajoukko. Tämän ehdon lisääminen määritelmään ei kuitenkaan separaatioaksiooman ansiosta muuta joukkojen mahtavuuden käsitettä millään lailla, sillä jos on olemassa määritelmän joukko f, joksi sijoitetaan vakio F', kun a ja b ovat määritelmän muuttujien x ja y tilalle sijoitettuja joukkoja, joukko $F = \{x \in (a \times b) \mid x \in F'\}$ on bijektiivinen funktio, $F \subseteq (a \times b)$. Toisaalta jos on olemassa bijektiivinen funktio $F \subseteq (a \times b)$, tämä funktio kelpaa määritelmän joukoksi f.

Kaksi äärellistä joukkoa on intuitiivisesti ajateltuna mahtavuudeltaan yhtäsuurta, jos niillä on sama määrä alkioita. Siispä esimerkiksi joukot $\{\emptyset, \{\emptyset\}\}$ ja $\{\emptyset, \{\{\emptyset\}\}\}$ ovat mahtavuudeltaan yhtäsuuria, koska kummallakin on kaksi jäsentä. Lukumäärän käsitettä ei kuitenkaan ole vielä tässä tutkielmassa määritelty, joten sitä ei voi hyödyntää mahtavuutta määriteltäessä. Funktion käsitteeseen nojautuva määritelmä toimii äärellisten joukkojen lisäksi myös äärettömille joukoille. Itse asiassa äärellisyys ja äärettömyys määritellään mahtavuuden avulla.

3.7 Joukkojen hierarkia

Millainen on joukoista muodostettu todellisuus? Ainoa primitiivisominaisuus, jolla kahta eri joukkoa voidaan verrata, on kuulumisrelaatio. Tiedetään, että kaksi identtistä joukkoa ovat tämän ominaisuuden ja siksi myös kaikkien sen avulla määriteltyjen ominaisuuksien suhteen täysin samat. Täten ne ovat

joukkojen kaikkeudessa täsmälleen samassa kohtaa. Voidaanko joukkojen keskinäisestä suhteesta kuitenkin tietää enemmän?

Ainakin luonnossa joukoilla on selvä hierarkia. Jos joukko x kuuluu joukkoon y, joukko y ei kuulu joukkoon x. Esimerkiksi omalaatuinen molekyylien joukko solu kuuluu soluista muodostuvaan elimeen mutta elin ei kuulu soluun. Jos sitten y kuuluu joukkoon z, on vieläkin selvempää, että z ei kuulu joukkoon x. Elin kuuluu eliöön, mutta eliö ei millään voi kuulua soluun. Vastaava pitää tietenkin paikkansa kuinka pitkälle hierarkiaketjulle tahansa.

Samoin on luonnotonta, että olisi $x \in x$. Siksi luvussa 3.4 lyhyesti esitelty Russellin paradoksi on hieman vaikeasti ymmärrettävä. Miten voidaan kysyä, onko joukko $a = \{x \mid \neg x \in x\}$ itsensä jäsen, kun $a \in a$ on täyttä hölynpölyä? Kuitenkin $x \in y$ on kaava, olivatpa x ja y mitä muuttujia tai vakioita tahansa. Siksi $a \in a$ on lause, kun a on vakio. Lisäksi se voisi matemaattisessa joukko-opissa hyvinkin olla jollekin vakiolle tosi.

Pyrkimyksenä on, että matemaattinen joukko-oppi vastaisi ainakin perustuloksiltaan luonnollista joukko-oppia, ja siksi luonnollisen joukkojen hierarkian takaamiseksi esitetään uusi aksiooma, englanniksi niin kutsuttu *axiom of foundation* (ks. esim. [8]: s. 89). Tässä tutkielmassa sitä kutsutaan hierarkia-aksioomaksi, koska sen avulla voidaan todistaa muun muassa lause 3.25 (todistuksen idea löytyy muun muassa Mayberryltä, [12]: s. 148), joka osoittautuu käyttökelpoiseksi myöhemmin.

Aksiooma 8 (Hierarkia-aksiooma)**.** Jokaisella epätyhjällä joukolla x on jäsen y, jolla ei ole yhtään yhteistä jäsentä joukon x kanssa.

$$\forall x(\neg\Box_x = \emptyset \Rightarrow \exists y(\Box_y \in \Box_x \wedge \forall z\neg(\Box_z \in \Box_x \wedge \Box_z \in \Box_y)z)y)x$$

Lause 3.25. *Kun a ja b ovat joukkoja, ei voi olla yhtä aikaa voimassa $a \in b$ ja $b \in a$.*

$$a, b :\Rightarrow: \neg(a \in b \wedge b \in a)$$

Todistus.
Selvästikin joukko $\{a, b\}$ on epätyhjä, joten hierarkia-aksiooman mukaan sillä on jäsen, jolla ei ole yhteistä jäsentä joukon $\{a, b\}$ kanssa. Jos $a \in b$, tämä jäsen ei ole b, joten sen täytyy olla a, mikä tarkoittaa sitä, että $\neg b \in a$. Siispä $\neg(a \in b \wedge b \in a)$.

[1] ... $a \in \{a, b\}$

[2] ... $\neg a \in \emptyset$

[3]k[23],MP,MP,∃ $\exists x(\Box_x \in \{a,b\} \wedge \neg\Box_x \in \emptyset)x$

[4]s[1],kvs,m3.1(3) $\neg\{a,b\} \subseteq \emptyset$

[5]k[26],MP,s[7],m3.3 $\neg\{a,b\} = \emptyset$

[6]A8,∀← $(\neg\{a,b\} = \emptyset \Rightarrow$
$\exists y(\Box_y \in \{a,b\} \wedge \forall z\neg(\Box_z \in \{a,b\} \wedge \Box_z \in \Box_y)z)y)$

[7]MP(5,6),∃← $(\Box_y \in \{a,b\} \wedge \forall z\neg(\Box_z \in \{a,b\} \wedge \Box_z \in \Box_y)z)y \leftarrow c$

[8]k[22],MP,k[22],MP $((c = b \Rightarrow a \in c) \Rightarrow (c = b \Rightarrow a \in \{a,b\}))$

[9]k[20,23],MP,MP $(((c = b \Rightarrow a \in c) \Rightarrow (c = b \Rightarrow a \in c))$
$\wedge((c = b \Rightarrow a \in c) \Rightarrow (c = b \Rightarrow a \in \{a,b\})))$

[10]s[15](9) $((c = b \Rightarrow a \in c) \Rightarrow (c = b \Rightarrow (a \in c \wedge a \in \{a,b\})))$

[11]k[20],m3.3,3.1 $(c = b \Rightarrow \forall x(\Box_x \in b \Rightarrow \Box_x \in c)x)$

[12]kvs,∀←,s[10](11) $(a \in b \Rightarrow (c = b \Rightarrow a \in c))$

[13]k[24],MP,MP $(a \in b \Rightarrow (c = b \Rightarrow (a \in c \wedge a \in \{a,b\})))$

[14]s[11,5],∃,kvs(13) $((a \in b \wedge c = b) \Rightarrow \exists z(\Box_z \in \{a,b\} \wedge \Box_z \in c)z)$

[15]sij(7),k[32],MP $\forall z\neg(\Box_z \in \{a,b\} \wedge \Box_z \in c)z$

[16]k[22],MP,k[23],MP,MP $(((a \in b \wedge c = b) \Rightarrow \exists z(\Box_z \in \{a,b\} \wedge \Box_z \in c)z)$
$\wedge((a \in b \wedge c = b) \Rightarrow \forall z\neg(\Box_z \in \{a,b\} \wedge \Box_z \in c)z))$

[17]s[15,8,7],kvs(16) $((\forall z\neg(\Box_z \in \{a,b\} \wedge \Box_z \in c)z \vee$
$\neg\forall z\neg(\Box_z \in \{a,b\} \wedge \Box_z \in c)z) \Rightarrow \neg(a \in b \wedge c = b))$

[18]k[20],s[2,1],MP $(a \in b \Rightarrow \neg c = b)$

[19]sij(7),k[32],MP $c \in \{a,b\}$

[20] ... $(c = a \vee c = b)$

[21]k[22],MP,k[23],MP,MP $((a \in b \Rightarrow \neg c = b) \wedge (a \in b \Rightarrow (c = a \vee c = b)))$

[22]s[15],k[39,24],MP,MP $(a \in b \Rightarrow ((\neg c = b \wedge c = b) \vee c = a))$

$^{23}\mathrm{s}^{18}(22)$	$(a \in b \Rightarrow c = a)$
$^{24}\forall\leftarrow,\mathrm{s}^{1}(15)$	$(b \in \{a, b\} \Rightarrow \neg b \in c)$
$^{25}\ldots$	$b \in \{a, b\}$
$^{26}\mathrm{MP}(23,22)$	$\neg b \in c$
$^{27}\mathrm{k}^{22},\mathrm{MP}$	$(a \in b \Rightarrow \neg b \in c)$
$^{28}\mathrm{k}^{23},\mathrm{MP},\mathrm{MP},\mathrm{s}^{15}$	$(a \in b \Rightarrow (c = a \wedge \neg b \in c))$
$^{29}\mathrm{k}^{20},\mathrm{m3.3},3.1$	$(c = a \Rightarrow \forall x(\Box_x \in c \Leftrightarrow \Box_x \in a)x)$
$^{30}\mathrm{s}^{21},\mathrm{kvs},\forall\leftarrow(29)$	$(c = a \Rightarrow (\neg b \in c \Leftrightarrow \neg b \in a))$
$^{31}\mathrm{k}^{24},\mathrm{s}^{8,1},\mathrm{MP}$	$((c = a \wedge \neg b \in c) \Rightarrow ((\neg b \in c \Leftrightarrow \neg b \in a) \wedge \neg b \in c))$
$^{32}\mathrm{k}^{28,24},\mathrm{MP},\mathrm{MP}$	$((c = a \wedge \neg b \in c) \Rightarrow \neg b \in a)$
$^{33}\mathrm{k}^{24},\mathrm{MP},\mathrm{MP},\mathrm{s}^{1}$	$\neg(a \in b \wedge b \in a)$

□

Jos kuuluvuusrelaation suhteen loputtoman laskevan joukkojen jonon $\ldots \in u \in z \in y \in x$ formaalisesti täsmälliseksi vastineeksi ajatellaan joukkoa $a : (\neg\Box_y = \emptyset \wedge \forall x(\Box_x \in \Box_y \Rightarrow \exists z(\Box_z \in \Box_y \wedge \Box_z \in \Box_x)z)x)y \leftarrow a$, niin hierarkia-aksiooman ansiosta sellaista jonoa ei ole olemassa. Tämä on mielenkiintoista, sillä seuraavassa luvussa asetettava äärettömyysaksiooma varmistaa loputtoman nousevan jonon $x \in y \in z \in u \in \ldots$ olemassaolon.

Lause 3.26.

$$\neg\exists y(\neg\Box_y = \emptyset \wedge \forall x(\Box_x \in \Box_y \Rightarrow \exists z(\Box_z \in \Box_y \wedge \Box_z \in \Box_x)z)x)y$$

Todistus.

$^{1}\mathrm{A8}$	$\forall y(\neg\Box_y = \emptyset \Rightarrow$ $\exists x(\Box_x \in \Box_y \wedge \forall z\neg(\Box_z \in \Box_y \wedge \Box_z \in \Box_x)z)x)y$
$^{2}\mathrm{kvs},\mathrm{s}^{1,4}(1)$	$\neg\exists y(\neg\Box_y = \emptyset\wedge$ $\forall x(\Box_x \in \Box_y \Rightarrow \exists z(\Box_z \in \Box_y \wedge \Box_z \in \Box_x)z)x)y$

□

4 Luvut

Mihin joukkoja voidaan käyttää? Ehkäpä luonnollisin joukko-opin sovelluksista on luonnollisten lukujen aritmetiikka. *Jos Kallella on viisi omenaa ja Ullalla on kolme omenaa, montako omenaa Kallella ja Ullalla on yhteensä* on aritmeettinen tehtävä, jossa laskento on havainnollisesti upotettu joukko-oppiin.

Tässä luvussa luonnolliset luvut esitetään joukkoina. Luonnollisten lukujen voidaan ajatella olevan kiinteästi äärellisiin joukkoihin liittyvä käsite: jokaiseen äärelliseen joukkoon liittyy täsmälleen yksi luonnollinen luku ja vieläpä sellaisella lisäehdolla, että jos a ja b ovat joukkoja ja jos $a \sim b$, kumpaankin joukkoon a ja b liittyy sama luonnollinen luku. Miksei siis luonnollisia lukuja voisi niitäkin ajatella joukkoina?

Otetaan käyttöön muutama uusi symboli:

- Symboli + on operaatiosymboli.
- Symbolit **L**, **N**, 0, 1, 2 ja A ovat vakioita.

4.1 Luonnolliset luvut joukkoina

Koska tämä tutkielma käsittelee joukkoja, on luvutkin funktioiden ja relaatioiden lailla esitettävä joukkoina. Ensi alkuun tällainen ratkaisu kuulostaa oudolta. Omalla tavallaan se kuitenkin helpottaa teorian käsittelyä, koska edelleenkään ei tarvitse turvautua perusalkioihin vaan kaikki joukot ovat pelkistettyjä joukkoja. Yksinkertaisuuden periaate ei kuitenkaan ole ainoa syy lukujen ajattelemiseen joukkoina. Toinen syy on, ettei luonnollisia lukuja käytetä ainoastaan aritmeettisten laskutoimitusten laskemiseen vaan myös lukumäärän laskemiseen.

Luonnollisilla luvuilla voidaan laskea äärellisen joukon kardinaliteetti eli joukon jäsenien lukumäärä, jos jokaista luonnollista lukua n kohden on olemassa sellainen joukko, joka sisältää kaikki lukua n pienemmät luonnolliset luvut (tämä kardinaliteetin laskemisen ehto löytyy Eric Steinhartin artikkelista [17]; sovitaan tässä, että luonnollisista luvuista voidaan muodostaa joukkoja, vaikkeivät ne itse olisikaan joukkoja vaan perusalkioita). Vaikka kardinaliteetin laskemiseen voisi varmasti olla monia muitakin tapoja, tämä on pienellä muutoksella sopusoinnussa arkikokemuksen kanssa. Jos nimittäin

tehtävänä on laskea pöydällä olevien kuppien lukumäärä, yksinkertaisimmalta tuntuu osoittaa jokaista kuppia peräjälkeen ja leimata mielessään kukin kuppi jollakin luonnollisella luvulla järjestyksessä 1, 2, 3 ja niin edelleen. Niinpä jos pöydällä on kahdeksan kuppia, niiden lukumäärän laskija on mielessään käynyt läpi luvun kahdeksan lisäksi kaikki kahdeksaa pienemmät ja nollaa suuremmat luonnolliset luvut.

Pienin luonnollinen luku on kuitenkin 0 eikä 1, joten sovitaan, että kardinaliteetin laskemisessa lähdetäänkin liikkeelle luvusta 0. Toisin sanoen kahdeksan kupin laskemisessa käytäisiin läpi kaikki kahdeksaa pienemmät luonnolliset luvut. Tällä tavalla kardinaliteetin laskeminen tapahtuisi niin, että ensimmäinen leimaksi käyttämätön luku sovitaan kardinaliteetiksi. Kahdeksan kupin esimerkissä siis leimoiksi käytetään luvut 0–7, joten ensimmäinen leimaksi käyttämätön luku eli kuppien joukon kardinaliteetti on 8.

Tällä tavalla kuppien kardinaliteetiksi osoittautunut luonnollinen luku 8 täyttää omalta osaltaan edellä esitetyn kardinaliteetin laskemisen ehdon: on olemassa kaikkien lukua 8 pienempien luonnollisten lukujen joukko (merkitään tätä joukkoa joukoksi $8^<$), koska sen jäseniä tarvitaan leimoiksi laskettaville kupeille. Toisaalta joukkoa $8^<$ voidaan ajatella tyyppiesimerkkinä joukosta, jonka kardinaliteetti on kahdeksan. Määritelmän 3.24 mukaan kuppien joukon kardinaliteetti eli mahtavuus on 8, koska on olemassa bijektiivinen funktio, joka on kuppien joukon ja joukon $8^<$ karteesisen tulon osajoukko, ja koska joukon $8^<$ mahtavuus on 8.

Koska joukon mahtavuuden määritelmä ei millään tavalla viittaa luonnollisiin lukuihin, kuppien joukon kardinaliteettia määritelmän 3.24 mielessä pohtiessa herää kysymys, mikä tämä 8 on. Luonnollisiin lukuihin tutustumaton mutta joukkojen suhteellisen mahtavuuden käsitteen tunteva sanoisi, että se on ilmeisesti sovittu joukon $8^<$ kardinaliteetin symboliksi. Toisaalta joukon $8^<$ jäsenet ovat luonnollisia lukuja; mitä ne siis ovat? Jos nämä luonnolliset luvut olisivat joukon $8^<$ kardinaliteetin tapaan miellettävä pelkiksi eri kardinaliteettien symboleiksi, eivätkö luonnolliset luvut olisi silloin hieman liian epämääräisiä?

Tosin hieman tähän tapaan luonnolliset luvut voidaan mieltää luokiksi: kukin luonnollinen luku on kaikkien niiden äärellisten luokkien luokka, joilla on sama tietty kardinaliteetti. Esimerkiksi luku 1 olisi kaikkien niiden luokkien luokka, joilla on vain ainutkertainen jäsen. ([14]: s. 272, 279.) Toisin

sanoen jos a on joukko,

$$(a \in 1 \Leftrightarrow \exists x(\square_x \in a \wedge \forall y(\square_y \in a \Rightarrow \square_y = \square_x)y)x).$$

Tällainen lukujen määritteleminen ei tietenkään sovi tähän tutkielmaan muun muassa siksi, etteivät tällaiset luokat ole joukkoja ja siispä $a \in 1$ ei tarkoita mitään, koska jotta se olisi kaava, täytyisi sekä a:n että 1:n olla muuttujia tai joukkoja.

Helpompi ja käsitteellisesti yksinkertaisempi ratkaisu siihen, mitä luonnolliset luvut ovat, tuntuisi olevan itse joukon $8^<$ valitseminen luonnolliseksi luvuksi 8. Jos joukkoa $8^<$ voidaan ajatella tyyppiesimerkkinä joukosta, jonka kardinaliteetti on 8, miksei sitä voisi saman tien ajatella kardinaliteettina 8? Jos näin sovitaan, samaan tapaan luonnollinen luku 7 on sama kuin kardinaliteetti 7 eli joukko $7^<$ eli kaikkien lukua 7 pienempien luonnollisten lukujen joukko ja luku 6 on kaikkien sitä pienempien lukujen joukko ja niin edelleen. Pohjimmiltaan on siis ratkaistava, mikä on luku 0.

Koska 0 on pienin luonnollinen luku, sitä pienempiä luonnollisia lukuja ei ole olemassa, joten lukua 0 pienempien luonnollisten lukujen joukko eli joukko $0^<$ on tyhjä joukko. Siispä jos luonnollinen luku 0 sovitaan joukoksi $0^<$, kuten luku 8 sovittiin joukoksi $8^<$, symboli 0 on toinen merkintä joukolle $\emptyset$. Symboli 1 tarkoittaa joukkoa $\{0\}$ eli $\{\emptyset\}$, symboli 2 joukkoa $\{0, 1\}$ eli $\{\emptyset, \{\emptyset\}\}$, symboli 3 joukkoa $\{0, 1, 2\}$ eli $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$ ja symboli 8 joukkoa $\{0, 1, 2, 3, 4, 5, 6, 7\}$.

Edellä esitetty perustelu sille, miksi luonnolliset luvut sovitaan tietynlaisiksi joukoiksi, on epätäsmällinen. Pohdittaessa, miten luonnolliset luvut kannattaa esittää, perustelujen taustalla oli jonkinlainen valmis käsitys luonnollisista luvuista. Miten voidaan puhua lukua kahdeksan pienempien lukujen joukosta, jos ei vielä tiedetä, mitä luvut ja niiden järjestys ovat? Tarkoitus ei siis ollut osoittaa, minkälaisia joukkoja luonnolliset luvut välttämättä ovat vaan miksei intuitiivinen valmis käsitys luonnollisista luvuista ole täysin ristiriidassa sopimuksen kanssa, joka tässä tutkielmassa tehdään siitä, mitä luonnolliset luvut joukkoina ovat. Luonnollisten lukujen esittäminen muodossa $\emptyset$, $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$, ... ei siis ole pelkkää symboleilla hienostelua.

Määritelmä 4.1. Joukon seuraaja on sen ja siitä muodostetun yhden joukon yhdisteen unioni.

$$(x)y+ :: \forall z(\square_z \in x \Leftrightarrow (\square_z \in y \vee \square_z = y))z$$

Määritellään joukon seuraajan yleinen vakiomerkintä.

$$a^+ : (\square_x)a+\, x \leftarrow a^+$$

Kunkin joukon seuraaja on olemassa, koska selvästikin joukko a^+ on identtinen joukon $(a \cup \{a\})$ kanssa, mikä seuraa määrittelystä 3.6 ja siitä, että $(x \in \{a\} \Leftrightarrow x = a)$. Määritellään nyt edellisen määritelmän avulla luvut 0, 1 ja 2.

Määrittely 4.2. Luku 0 on tyhjä joukko. Luku 1 on luvun 0 ja luku 2 luvun 1 seuraaja. Nämä ovat aitoja vakioita.

$$0 : \square_x = \emptyset x \leftarrow 0$$

$$1 : (\square_x)0+\, x \leftarrow 1$$

$$2 : (\square_x)1+\, x \leftarrow 2$$

Koska tyhjä joukko on olemassa, luku 0 on olemassa. Sen seuraajana luku 1 ja tämän seuraajana luku 2 ovat olemassa. Onko kuitenkaan kaikkien kuvatulla tavalla muodostettujen luonnollisten lukujen muodostamaa joukkoa olemassa? On mahdollista todistaa minkä tahansa äärellisen joukon $\{0, 1, 2, \ldots, n\}$ olemassaolo, mutta kaikkien luonnollisten lukujen joukon olemassaolo varmistetaan aksioomalla. Sama aksiooma avaa, kuten tullaan huomaamaan, oven uusiin matemaattisiin seikkailuihin: äärettömiin joukkoihin.

4.2 Luonnolliset luvut joukkona

Aksiooma 9 (A∞, Äärettömyysaksiooma)**.** On olemassa joukko, jonka jäseniä ovat ainakin kaikki luonnolliset luvut.

$$\exists x(\emptyset \in \square_x \wedge \forall y(\square_y \in \square_x \Rightarrow \forall z((\square_z)\square_y+ \Rightarrow \square_z \in \square_x)z)y)x$$

Määrittely 4.3. Määritellään symboli **L** viittaamaan aksiooman A∞ tarkoittamaan joukkoon.

$$\mathbf{L} : (\emptyset \in \square_x \wedge \forall y(\square_y \in \square_x \Rightarrow \forall z((\square_z)\square_y+ \Rightarrow \square_z \in \square_x)z)y)x \leftarrow \mathbf{L}$$

Kun valitaan joukosta **L** jäsen a, voidaan kirjoittaa aksiooman mukaan

$$(a \in \mathbf{L} \Rightarrow \forall z((\square_z)a+ \Rightarrow \square_z \in \mathbf{L})z).$$

Koska a^+ on olemassa ja koska siitä syystä lause $(a^+)a+$ pitää paikkansa, voidaan kirjoittaa

$$(a \in \mathbf{L} \Rightarrow a^+ \in \mathbf{L}).$$

Toisin sanoen jos a kuuluu joukkoon $\mathbf{L}$ ja a on luonnollinen luku (esimerkiksi $\{\emptyset, \{\emptyset\}\}$ eli 2), niin sen seuraaja (esimerkiksi 2^+ eli $(2 \cup \{2\})$ eli $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$ eli 3) kuuluu myös joukkoon $\mathbf{L}$. Koska 0 eli $\emptyset$ kuuluu joukkoon $\mathbf{L}$, sen seuraaja, tämän seuraaja, tämän seuraaja ja niin edelleen kaikki seuraajat kuuluvat myös joukkoon $\mathbf{L}$, ja niinpä tämä tosiaan sisältää kaikki luonnolliset luvut.

Joukon $\mathbf{L}$ yksikäsitteisyydestä ei kuitenkaan ole takeita. Aksiooman A∞ olemassa olevaksi määräämä joukko ei ole välttämättä luonnollisten lukujen joukko: aksiooma ei kiellä siltä jäseniä, jotka eivät ole luonnollisia lukuja. Koska kaikki luonnolliset luvut ovat joukon $\mathbf{L}$ jäseniä, luonnollisten lukujen joukko on sen osajoukko. Luonnollisten lukujen joukko on itse asiassa jokaisen aksiooman 9 asettamat ehdot – ensinnäkin tyhjän joukon täytyy kuulua joukkoon ja toiseksi jokaisen jäsenen seuraajan on kuuluttava joukkoon – täyttävän joukon osajoukko. Siispä voidaan ajatella, että luonnollisten lukujen joukko $\mathbf{N}$ on kaikkien tällaisten joukkojen "$\mathbf{L}$" leikkaus. Kaikkien joukon $\mathbf{N}$ osajoukkonaan sisältävien joukkojen joukkoa ei ole olemassa, joten $\mathbf{N}$ ei voi olla varsinainen aksiooman 2 tarkoittama leikkaus vaan se täytyy määritellä toisella tavalla. ([8]: s. 46, 47.)

Määrittely 4.4. Määritellään vakio $\mathbf{N}$ joukoksi, jossa on jäseninä täsmälleen ne joukot, jotka ovat kaikkien aksiooman A∞ ehdot toteuttavien joukkojen jäseniä. Koska joukko $\mathbf{N}$ voidaan määritellä joukon $\mathbf{L}$ osajoukkona, aksiooma 6 takaa sen olemassaolon.

$$\mathbf{N} : \forall x(\square_x \in \square_y \Leftrightarrow (\square_x \in \mathbf{L} \wedge \forall z((\emptyset \in \square_z \wedge \forall u(\square_u \in \square_z \Rightarrow$$

$$\forall v((\square_v)\square_u+ \Rightarrow \square_v \in \square_z)v)u) \Rightarrow \square_x \in \square_z)z))xy \leftarrow \mathbf{N}$$

Onko $\mathbf{N}$ todellakin luonnollisten lukujen joukko? Jos hyväksytään niin sanotut luonnollisten lukujen Peano-aksioomat, $\mathbf{N}$ on luonnollisten lukujen joukko, jos se toteuttaa nämä aksioomat. Peanon aksioomat voidaan esittää viitenä kohtana ([6][6]: s.3, 4):

[6]A. Doneddun kirjassa *Géométrie euclidienne plane* on myös melko helposti ymmärrettävä selostus siitä, miten luonnollisten lukujen avulla voidaan muodostaa kokonais-, rationaali- ja reaaliluvut.

1. Luonnollisten lukujen joukolla $\mathbb{N}$ on jäsen 0.

2. Jokaisella joukon $\mathbb{N}$ jäsenellä on niin sanottu seuraaja, joka on yksikäsitteinen ja kuuluu luonnollisiin lukuihin.

3. Luku 0 ei ole minkään luonnollisen luvun seuraaja.

4. Jos luonnolliset luvut a ja b ovat erisuuret, niiden seuraajat ovat erisuuret.

5. Jos joukolla $\mathbb{N}$ on osajoukko A, jolla on jäseninään ainakin 0 ja jokaisen jäsenensä seuraaja, joukko A on identtinen joukon $\mathbb{N}$ kanssa.

Ensimmäinen ehto täyttyy: joukolla **N** on ainakin yksi jäsen, nimittäin luvuksi 0 sovittu tyhjä joukko. Koska jokaisella tämän joukon jäsenellä a on samaan joukkoon kuuluva määrittelynsä ansiosta yksikäsitteinen seuraaja a^+, toinen ehto täyttyy. Jos a on joukon **N** jäsen, niin a itse kuuluu joukkoon a^+, joten minkään luonnollisen luvun seuraaja ei ole 0 eli tyhjä joukko. Lauseet 4.5 ja 4.6 osoittavat, että joukko **N** täyttää loputkin luonnollisten lukujen joukolle esitetyt ehdot. Täten joukko **N** on yksi esimerkki mahdollisesta luonnollisten lukujen joukon mallista.

Lause 4.5. *Kahden eri joukon a ja b seuraajat ovat erisuuret. Koska tämä pätee kaikille joukoille, se pätee tietenkin erityisesti luonnollisille luvuille.*

$$a, b :\Rightarrow: (\neg\ a = b \Rightarrow \neg\ a^+ = b^+)$$

Todistus. Täytyy osoittaa, että joukot $(a \cup \{a\})$ ja $(b \cup \{b\})$ ovat erisuuret, kun a ja b eivät ole keskenään identtisiä. Tämä nähdään helposti epäsuoralla argumentilla. Koska $a \in a^+$ mutta $\neg\ \{a\} = \{b\}$, täytyisi olla $a \in b$, jos joukot a^+ ja b^+ olisivat identtiset. Samoin pitäisi olla $b \in a$, mikä on mahdotonta.

[1] k^{20},m3.3,3.1	$(a^+ = b^+ \Rightarrow \forall x(\square_x \in a^+ \Leftrightarrow \square_x \in b^+)x)$
[2] kvs,$\forall\leftarrow$(1)	$(a^+ = b^+ \Rightarrow (a \in a^+ \Leftrightarrow a \in b^+))$
[3] ...	$((a \in a^+ \Leftrightarrow (a \in a \vee a = a)) \wedge (a \in b^+ \Leftrightarrow (a \in b \vee a = b)))$
[4] s_3(2)	$(a^+ = b^+ \Rightarrow ((a \in a \vee a = a) \Leftrightarrow (a \in b \vee a = b)))$
[5] $\mathrm{k}^{25,24}$,MP,MP,s^{10}	$((a \in a \vee a = a) \Rightarrow (a^+ = b^+ \Rightarrow (a \in b \vee a = b)))$
[6] L3.4,k^{22},MP	$(a \in a \vee a = a)$

^{7}MP(6,5)	$(a^+ = b^+ \Rightarrow (a \in b \vee a = b))$
^{8}kuten(7)	$(a^+ = b^+ \Rightarrow (b \in a \vee a = b))$
^{9}k^{23},MP,MP,s^{15}	$(a^+ = b^+ \Rightarrow ((a \in b \vee a = b) \wedge (b \in a \vee a = b)))$
^{10}s^{16}(9)	$(a^+ = b^+ \Rightarrow ((a \in b \wedge b \in a) \vee a = b))$
^{11}L3.25,k^{22},MP	$(a^+ = b^+ \Rightarrow \neg(a \in b \wedge b \in a))$
^{12}k^{23},MP,MP,s^{15}	$(a^+ = b^+ \Rightarrow (((a \in b \wedge b \in a) \vee a = b) \wedge \neg(a \in b \wedge b \in a)))$
^{13}k^{39},s^{5}	$((((a \in b \wedge b \in a) \vee a = b) \wedge \neg(a \in b \wedge b \in a))$ $\Rightarrow (((a \in b \wedge b \in a) \wedge \neg(a \in b \wedge b \in a)) \vee a = b))$
^{14}k^{24},MP,MP	$(a^+ = b^+ \Rightarrow (((a \in b \wedge b \in a) \wedge \neg(a \in b \wedge b \in a)) \vee a = b))$
^{15}s^{18}(14)	$(a^+ = b^+ \Rightarrow a = b)$
^{16}s^{8}(15)	$(\neg\ a = b \Rightarrow \neg\ a^+ = b^+)$

□

Lause 4.6. *Jos joukolla* $\mathbf{N}$ *on osajoukko* A*, jolla on jäseninään tyhjä joukko* $\emptyset$ *ja kaikki jäseniensä seuraajat, niin* A *on identtinen joukon* $\mathbf{N}$ *kanssa.*

$$A :\Rightarrow:$$

$$((A \subseteq \mathbf{N} \wedge (\emptyset \in A \wedge \forall u(\Box_u \in A \Rightarrow \forall v((\Box_v)\Box_u + \Rightarrow \Box_v \in A)v)u)) \Rightarrow A = \mathbf{N})$$

Todistus. Tulos seuraa helposti joukon $\mathbf{N}$ määrittelystä. Luonnollisten lukujen joukon sisään ei aitona osajoukkona mahdu joukkoa, joka toteuttaa aksiooman A∞ ehdot, koska kaikkien tällaisten joukkojen kaikki jäsenet kuuluvat määrittelyn mukaan joukkoon $\mathbf{N}$.

^{1}A6,$\forall\leftarrow$,$\exists\leftarrow$	$\forall x(\Box_x \in \Box_y \Leftrightarrow (\Box_x \in \mathbf{L} \wedge \forall z((\emptyset \in \Box_z \wedge \forall u(\Box_u \in \Box_z \Rightarrow$ $\forall v((\Box_v)\Box_u + \Rightarrow \Box_v \in \Box_z)v)u) \Rightarrow \Box_x \in \Box_z)z))x \leftarrow \mathbf{N}$
^{2}sij,$\forall\leftarrow$(1)	$(x \in \mathbf{N} \Leftrightarrow (x \in \mathbf{L} \wedge \forall z((\emptyset \in \Box_z \wedge \forall u(\Box_u \in \Box_z \Rightarrow$ $\forall v((\Box_v)\Box_u + \Rightarrow \Box_v \in \Box_z)v)u) \Rightarrow x \in \Box_z)z))$
^{3}k^{32}	$((x \in \mathbf{L} \wedge \forall z((\emptyset \in \Box_z \wedge \forall u(\Box_u \in \Box_z \Rightarrow \forall v((\Box_v)\Box_u + \Rightarrow$ $\Box_v \in \Box_z)v)u) \Rightarrow x \in \Box_z)z)$ $\Rightarrow \forall z((\emptyset \in \Box_z \wedge \forall u(\Box_u \in \Box_z \Rightarrow \forall v((\Box_v)\Box_u + \Rightarrow$ $\Box_v \in \Box_z)v)u) \Rightarrow x \in \Box_z)z)$

$^4\forall\leftarrow$	$(\forall z((\emptyset \in \square_z \wedge \forall u(\square_u \in \square_z \Rightarrow \forall v((\square_v)\square_u+ \Rightarrow$ $\square_v \in \square_z)v)u) \Rightarrow x \in \square_z)z$ $\Rightarrow ((\emptyset \in A \wedge$ $\forall u(\square_u \in A \Rightarrow \forall v((\square_v)\square_u+ \Rightarrow \square_v \in A)v)u) \Rightarrow x \in A))$
^{5}k^{24},MP,MP,s$_2$	$(x \in \mathbf{N} \Rightarrow ((\emptyset \in A \wedge$ $\forall u(\square_u \in A \Rightarrow \forall v((\square_v)\square_u+ \Rightarrow \square_v \in A)v)u) \Rightarrow x \in A))$
^{6}s^{10}(5)	$((\emptyset \in A \wedge \forall u(\square_u \in A \Rightarrow \forall v((\square_v)\square_u+ \Rightarrow \square_v \in A)v)u)$ $\Rightarrow (x \in \mathbf{N} \Rightarrow x \in A))$
$^7\forall$,kvs,m3.1(6)	$((\emptyset \in A \wedge \forall u(\square_u \in A \Rightarrow \forall v((\square_v)\square_u+ \Rightarrow \square_v \in A)v)u)$ $\Rightarrow \mathbf{N} \subseteq A)$
^{8}k^{24},s^{8,1},MP,m3.3	$((A \subseteq \mathbf{N} \wedge (\emptyset \in A \wedge \forall u(\square_u \in A \Rightarrow \forall v((\square_v)\square_u+ \Rightarrow$ $\square_v \in A)v)u)) \Rightarrow A = \mathbf{N})$

□

4.3 Äärettömyys ja luonnollisten lukujen yhteenlasku

Lukujen ja joukko-opin tarkastelun lopuksi tarkastellaan vielä mielenkiintoisia käsitteitä, jotka osoittautuvat formaalisessa esityksessä harmillisen monimutkaisiksi. Ensin kerrotaan, mitä tarkoitetaan äärettömällä joukolla ja osoitetaan, että luonnolliset luvut ovat ääretön joukko. Ikävä kyllä tämä tieto on jätettävä informaalisen todistuksen varaan määritelmän 3.24 hankaluuden takia. Toinen esiteltävä käsite on yhteenlasku, johon liittyvien formaalisten kaavojen määritteleminen ei onnistu tutkielmassa esitettyjen sääntöjen puitteissa.

Olkoot a ja b erisuuria joukkoja, eli $\neg a = b$. Oletetaan vielä, että a on joukon b osajoukko, $a \subseteq b$. Toisin sanoen kaikki joukon a jäsenet ovat joukon b jäseniä mutta kaikki joukon b jäsenet eivät ole joukon a jäseniä. Tuntuu luonnolliselta, että tässä tapauksessa b on suurempi joukko kuin a. Niinpä antiikin Kreikan geometrian aksiomaattisesta esityksestään kuuluisa Eukleides asettikin: kokonaisuus on osaa suurempi ([12]: s. 47).

Toisaalta kaikkien luonnollisten lukujen joukko tuntuu aivan tavalliselta joukolta. Niinpä myös $\mathbf{N}_+ = \{x \in \mathbf{N} \mid \neg\, x = \emptyset\}$ on joukko. Selvästikin $\mathbf{N}_+ \subseteq \mathbf{N}$ ja $\neg\, \mathbf{N}_+ = \mathbf{N}$. Onko siis $\mathbf{N}$ suurempi joukko kuin $\mathbf{N}_+$? Tehdään ajatusleikki. Luettele niin monta luonnollista lukua eli joukon $\mathbf{N}$ jäsentä, kuin

jaksat. Oletko varma, ettei kukaan pysty luettelemaan sitä enempää aidosti positiivisia luonnollisia lukuja eli joukon $\mathbf{N}_+$ jäseniä? Jos joku pystyy luettelemaan enemmän jäseniä joukosta $\mathbf{N}_+$, kuin kukaan on koskaan aiemmin luetellut joukosta $\mathbf{N}$, onko sittenkin joukko $\mathbf{N}_+$ joukkoa $\mathbf{N}$ isompi? Jos hyväksytään joukkojen keskinäinen mahtavuus niiden keskinäisen ”yhtäsuuren isouden” mittariksi, joukot $\mathbf{N}$ ja $\mathbf{N}_+$ ovat itse asiassa yhtä isot.

Lause 4.7.

$$\mathbf{N} \sim \mathbf{N}_+$$

Todistus. Koska sekä $\mathbf{N}$ että $\mathbf{N}_+$ ovat joukkoja, myös $(\mathbf{N} \times \mathbf{N}_+)$ on joukko. Valitaan tästä karteesisesta tulosta osajoukkoon F kaikki sellaiset ja vain sellaiset jäsenet (n, n^*) (n ja n^* ovat luonnollisia lukuja esittäviä vakioita), että $n^* = n^+$. Jos $n \in \mathbf{N}$, niin $n^+ \in \mathbf{N}$. Koska $\neg n^+ = \emptyset$, niin n^+ on myös joukon $\mathbf{N}_+$ jäsen, $n^+ \in \mathbf{N}_+$. Toisaalta joukon $\mathbf{N}$ määrittelyn ansiosta kaikki luonnolliset luvut n^*, jotka ovat erisuuria kuin $\emptyset$, voidaan esittää muodossa n^+, jossa $n \in \mathbf{N}$. Täten (n, n^*), jossa $n^* = n^+$, kuuluu joukkoon F, olipa n mikä tahansa joukon $\mathbf{N}$ jäsen tai n^* mikä tahansa joukon $\mathbf{N}_+$ jäsen.

Kaikilla nollasta eroavilla luonnollisilla luvuilla on yksikäsitteinen edeltäjä, mikä on lauseen 4.5 tulos toisin ilmaistuna. Siispä jos (n, n^*) ja (n', n^*) ovat relaation F jäseniä, niin $n = n'$. Koska lisäksi jokaisen joukon seuraaja on yksikäsitteinen, (n, n^*) ja (n, n^*_*) ovat kummatkin relaation F jäseniä vain, jos $n^* = n^*_*$. Täten relaatio F on bijektiivinen funktio, $F \subseteq (\mathbf{N} \times \mathbf{N}_+)$, eli $\mathbf{N} \sim \mathbf{N}_+$. □

Toisaalta on siis luonnollista, että kokonaisuus on osaansa suurempi, mutta toisaalta taas luonnollisten lukujen joukko ei ole tällainen kokonaisuus. Tämä johtuu siitä, että Eukleideen asettama sopimus pätee joukoille, joiden kaikki jäsenet voidaan ainakin periaatteessa luetella, eli äärellisille joukoille. Intuition mukaan $\mathbf{N}$ on kuitenkin ääretön joukko, ja tällaisen äärettömyyden hyväksyntä vaatii Eukleideen sopimuksen hylkäämistä ([12]: s. 47). 1800-luvun lopun ja 1900-luvun alun matemaatikko Richard Dedekind määrittelikin äärettömän joukon sellaiseksi, joka on yhtä mahtava jonkin aidon eli erisuuren osajoukkonsa kanssa ([5]: s. 356).

Kaikki äärettömät joukot eivät kuitenkaan ole yhtä mahtavia. Voidaan osoittaa, että olipa a mikä tahansa joukko, on voimassa $\neg a \sim \mathcal{P}a$. Lisäksi $a \subseteq \mathcal{P}a$, mistä syystä voidaan sanoa, että $\mathcal{P}a$ on joukkoa a mahtavampi.

Siispä $\neg\mathbf{N} \sim \mathcal{P}\mathbf{N}$, vaikka molemmat joukot ovat äärettömiä. Ääretöntä joukkoa, joka on yhtä mahtava kuin $\mathbf{N}$, kutsutaan numeroituvasti äärettömäksi joukoksi, ja joukkoa, joka on ääretön muttei yhtä mahtava kuin $\mathbf{N}$ (vaan välttämättä siis mahtavampi kuin $\mathbf{N}$), kutsutaan ylinumeroituvasti äärettömäksi joukoksi. Voidaan esimerkiksi osoittaa, että reaalilukujen joukko $\mathbf{R}$ on yhtä mahtava kuin joukko $\mathcal{P}\mathbf{N}$, joten reaaliluvut ovat ylinumeroituvasti ääretön joukko. (Reaalilukujen ylinumeroituvuudesta esim. [13]: s. 173.)

Koetetaan määritellä luonnollisten lukujen yhteenlasku. Käytännön laskuissa määritelmä 4.8 toimii ainakin jotenkuten, mutta tosi asiassa määritelmä on laskettava informaaliseksi ideaksi, miten formaalinen yhteenlaskun määritelmä voisi toimia. Määritelmä nimittäin rikkoo määritelmille asetettuja sääntöjä.

Määritelmä 4.8. Määritellään joukon ja tyhjän joukon summa ja kahden joukon summa.

$$(z)\Big(x + 0\Big) :: z = x$$

$$(z)\Big(x + y\Big) :: \forall u((y)\Box_u + \Rightarrow \forall v((\Box_v)\Big(x + \Box_u\Big) \Rightarrow (z)\Box_v +)v)u$$

Esitellään vakiomerkintä kahden joukon summalle.

$$(a + b) : (\Box_x)\Big(a + b\Big)x \leftarrow (a + b)$$

Kuten mainittiin, määritelmä 4.8 on laiton. Ensiksikin määritellyssä kaavassa $(z)\Big(x+0\Big)$ esiintyy vakio, joka ei esiinny määritelmän oikealla puolella. Tämän seurauksena ei voida osoittaa esimerkiksi, että $(y = 0 \Rightarrow (x)\Big(x+y\Big))$. Toiseksi määritelmän seurauksena kaavalla $(z)\Big(x + 0\Big)$ on kaksi merkitystä. Kolmanneksi kaavan $(z)\Big(x + y\Big)$ määritelmässä ei saisi olla osakaavaa $(v)\Big(x + u\Big)$, koska sen merkitys ei ole ennalta tiedetty. Sovitaan siksi, ettei määritelmän toista riviä saa käyttää, jos muuttujan y tilalle sijoitetaan tyhjä joukko eli 0. Sovitaan lisäksi aksioomiksi seuraavat lauseet, joihin todistuksessa viitataan kirjainyhdistelmällä ns, ”nollasumma”:

$$\forall x\forall y\forall z((\Box_x = \Box_z \wedge \Box_y = 0) \Rightarrow (\Box_z)\Big(\Box_x + \Box_y\Big))zyx$$

$$\forall x\forall y\forall z(((\Box_z)\Big(\Box_x + \Box_y\Big) \wedge \Box_y = 0) \Rightarrow \Box_x = \Box_z)zyx$$

Tällaista määritelmää kutsutaan rekursiiviseksi. Määritelmä määrittelee kaavan $(z)\Big(x+0\Big)$, jonka avulla voidaan määritellä kaikki määriteltävissä olevat summakaavat kuten $(z)\Big(x+1\Big)$, $(z)\Big(x+2\Big)$ ja niin edelleen aina loputtomiin asti. Rekursiivinen määritelmä on matematiikassa erittäin tärkeässä osassa. Esimerkiksi juuri luonnollisten lukujen yhteenlaskun määritteli hieman tässäkin esitetyn kaltaisesti rekursiivisesti jo Dedekind 1800-luvulla ([5]: s. 379). Rekursiivisen määritelmän käyttäminen voidaan perustella täsmällisesti (ks. esim. [13]: s. 92–95), mutta tämän tutkielman osalta sovitaan, että yhteenlaskutoimituksen määritelmä on säännönvastainen poikkeus.

Koska formaaliselle määritelmälle asetetut säännöt eivät mahdollista sen ehdon asettamista, että kaavassa $(x)\Big(a+b\Big)$ sekä joukon a että joukon b täytyy olla luonnollisia lukuja, joukko $(a+b)$ ei välttämättä ole luonnollisten lukujen yhteenlasku. Joukon $(a+b)$ ensimmäinen yhteenlaskettava a voi nimittäin olla mikä tahansa joukko. Toisaalta $(a+b)$ ei ole olemassa, mikäli b ei ole 0 tai jokin sen seuraajista eli jos se ei ole luonnollinen luku. Esimerkiksi joukkoa $\mathcal{P}2$ eli $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$ ei voida esittää minkään joukon seuraajana, ja siksi ei voida kirjoittaa $\exists x(\Box_x)\Big(a+\mathcal{P}2\Big)x$.

5 Lopuksi

Onnistuuko tutkielma luotettavien matemaattisten tulosten esittämisessä? Mikäli todistukset noudattavat täsmällisesti toisessa luvussa esitettyjä päättelysääntöjä, luotettavuus palautuu noiden päättelysääntöjen luotettavuuteen. Niiden luotettavuus ei kuitenkaan ole triviaalia, sillä monet kaavamallit ja päättelysäännöt ovat melko mutkikkaita. Lisäksi jotkin niistä voivat johtaa ei-toivottuihin tuloksiin. Esimerkiksi tarpeelliseksi osoittautunut sääntö ekvmp, jonka mukaan $((\exists x \mathrm{A}x \wedge (\mathrm{A} \Rightarrow \mathrm{B})) \Rightarrow \exists y \mathrm{B}(y/x)y)$ on kaavamalli, johtaa ei-toivottuun seuraukseen: voidaan todistaa joukon olemassaolo ennen ensimmäistä absoluuttista olemassaoloaksiooma esimerkiksi seuraavalla tavalla:

[1]L3.4,$\forall\leftarrow$	$y = y$
[2]k[22],MP	$(\forall z(\square_z \in y \Leftrightarrow \square_z \subseteq x)z \Rightarrow y = y)$
[3]A$\mathcal{P}$,$\forall\leftarrow$	$\exists y \forall z(\square_z \in \square_y \Leftrightarrow \square_z \subseteq x)zy$
[4]k[23],MP,MP	$(\exists y \forall z(\square_z \in \square_y \Leftrightarrow \square_z \subseteq x)zy$ $\wedge(\forall z(\square_z \in y \Leftrightarrow \square_z \subseteq x)z \Rightarrow y = y))$
[5]ekvmp	$((\exists y \forall z(\square_z \in \square_y \Leftrightarrow \square_z \subseteq x)zy \wedge$ $(\forall z(\square_z \in y \Leftrightarrow \square_z \subseteq x)z \Rightarrow y = y))$ $\Rightarrow \exists u(\square_u = \square_u)u$
[6]MP(4,5)	$\exists u(\square_u = \square_u)u$

Samaan tapaan voidaan todistaa mistä tahansa lauseesta $\forall x \mathrm{A}x$ lause $\exists x \mathrm{A}x$. Niinpä on hyväksyttävä se, mitä Whitehead ja Russell kirjoittavat teoksessaan *Principia mathematica* ([19]: s. 20): se mikä pätee kaikille, pätee mille tahansa, ja jos jokin väite pätee mille tahansa, on olemassa olio, jolle se pätee. Aksiooman A$\emptyset$ asettama tyhjä joukko ei siis ole ensimmäinen olemassa olevaksi osoitettava joukko vaan ensimmäinen joukko, jolla on ominaisuus, joka ei päde kaikille mahdollisille joukoille.

Myös tutkielman esittämä jako vakioihin ja muuttujiin voidaan kyseenalaistaa. Tarkoitus on pitää joukkoon viittaaminen (vakio) ja joukkoon viittaamisen mahdollisuus (muuttuja) johdonmukaisesti erillään, mutta tämä johdonmukaisuus ei välttämättä heijastu todistetuista lauseista. $\forall$-päättelysääntöhän sisältää ajatuksen, että mille tahansa todistettavissa oleva

on kaikille joukoille todistettavissa. Kuitenkin useiden lauseiden väitteissä – muun muassa todistettaessa, että **N** täyttää Peanon aksioomat – oletettiin todistuksen helpottamiseksi ellei peräti *mahdollistamiseksi* yleisiä vakioita, joille tuloksia todistettiin, kun tarkoitus oli osoittaa, että lause pätee mille tahansa joukolle. Toisin sanoen ∀-päättelysäännön ajatusta sovellettiin ainakin implisiittisesti noin vain perustelematta vakioillekin.

Muun muassa näistä puutteistaan huolimatta tutkielma onnistuu melko rajallisesta sovittujen totuuksien joukosta johtamaan joukko-opin perustuloksia. Kenties tutkielman esittämiä matemaattisen määrittelemisen ja todistamisen keinoja hieman korjaamalla voitaisiin päästä pitkällekin kuten reaalilukujen esittämiseen joukkoina. Esimerkiksi voidaan todistaa seuraava perustavanlaatuinen lause. Tosin jotta se olisi täysin formaalinen tulos, määritelmiä koskevat lauseet tarvitsisivat työstämistä.

Lause 5.1.

$$(1 + 1) = 2$$

Todistus.

[1] ...,$\exists\leftarrow$	$\square_x = \emptyset x \leftarrow 0$
[2] ...,$\exists\leftarrow$	$(\square_x)0+\ x \leftarrow 1$
[3]sij,m4.1,$\forall\leftarrow$(2)	$(x \in 1 \Leftrightarrow (x \in 0 \vee x = 0))$
[4] ...	$((x \in 0 \vee x = 0) \Leftrightarrow x = 0)$
[5]k^{20},m4.1	$((1)u+ \Rightarrow \forall x(\square_x \in 1 \Leftrightarrow (\square_x \in u \vee \square_x = u))x)$
[6]kvs,$\forall\leftarrow$,s$_{3,4}$(5)	$((1)u+ \Rightarrow ((x \in u \vee x = u) \Leftrightarrow x = 0))$
[7]k^{25,35,24},MP,MP	$(((x \in u \vee x = u) \Leftrightarrow x = 0) \Rightarrow (x = u \Rightarrow x = 0))$
[8]k^{24},MP,MP	$((1)u+ \Rightarrow (x = u \Rightarrow x = 0))$
[9]$\forall$,$\forall\leftarrow$,s^{10}(8)	$(u = u \Rightarrow ((1)u+ \Rightarrow u = 0))$
[10]L3.4,MP	$((1)u+ \Rightarrow u = 0)$
[11] ...,$\exists\leftarrow$	$(\square_x)1+\ x \leftarrow 2$
[12] ...	$(v = 1 \Rightarrow (2)v+)$

[13]L3.4,m4.8 $(1)\Big(1+0\Big)$

[14]ns,$\forall\leftarrow$,$\forall\leftarrow$,$\forall\leftarrow$ $((u=0\wedge(v)\Big(1+u\Big))\Rightarrow v=1)$

[15]k[24],MP,MP,s[11] $(u=0\Rightarrow((v)\Big(1+u\Big)\Rightarrow(2)v+))$

[16]k[24],s[10],MP,MP $((1)u+\Rightarrow((v)\Big(1+u\Big)\Rightarrow(2)v+))$

[17]$\forall$,kvs,$\forall$(16) $\forall u((1)\Box_u+\Rightarrow\forall v((\Box_v)\Big(1+\Box_u\Big)\Rightarrow(2)\Box_v+)v)u$

[18]m4.8,$\exists$,$\exists\leftarrow$(17) $(\Box_x)\Big(1+1\Big)\leftarrow(1+1)$

[19]sij,m4.8(18) $\forall u((1)\Box_u+\Rightarrow\forall v((\Box_v)\Big(1+\Box_u\Big)\Rightarrow((1+1))\Box_v+)v)u$

[20]$\forall\leftarrow$,MP,$\forall\leftarrow$ $((1)\Big(1+0\Big)\Rightarrow((1+1))1+)$

[21]MP(13,20),m4.1 $\forall x(\Box_x\in(1+1)\Leftrightarrow(\Box_x\in 1\vee\Box_x=1))x$

[22]sij(11),m4.1,$\forall\leftarrow$ $(x\in 2\Leftrightarrow(x\in 1\vee x=1))$

[23]s$_{22}$(21) $\forall x(\Box_x\in(1+1)\Leftrightarrow\Box_x\in 2)x$

[24]m3.1,3.3(23) $(1+1)=2$

□

Lauseen todistuksessa on muutama oikaisu, joista rivien 1, 2, 4 ja 11 oikaisut eivät kaivanne liiemmälti selittelyjä. Rivin 12 kaava on melko yksinkertainen mutta melko monta riviä tuhlaava tulos, joka seuraa välituloksista $(v=1\Rightarrow((x\in 1\vee x=1)\Rightarrow(x\in v\vee x=v)))$ ja $(v=1\Rightarrow((x\in v\vee x=v)\Rightarrow(x\in 1\vee x=1)))$.

Tämä ja muut tutkielman lauseet antavat oman tukensa sille, että joukko-opin aksioomat ja tulokset voivat olla säännönmukaisesti esitettävissä ja todistettavissa. Matematiikan perustaminen joukko-oppiin, kuten lukujen tai funktioiden esittäminen joukkoina, – tai yleensä matematiikan perusteiden esittäminen – ei selvästikään ole yksinkertainen tehtävä, mutta se syventää käsitystä matematiikan luonteen formaalisesta ja eksakstista puolesta. Tähän puoleen tutustuminen on kiehtova kamppailu oman intuition ennakkoluuloja vastaan.

Kirjallisuutta

[1] E. W. Beth: *Foundations of mathematics*, North-Holland, Amsterdam, 1959.

[2] N. Bourbaki: *Eléments de mathématique. XVII. Première partie: Les structures fondamentales de l'analyse. Livre I: Théorie des ensembles. Chapitre I: Description de la mathématique formelle. Chapitre II: Théorie des ensembles*, Hermann & C^{ie}, Pariisi, 1954.

[3] N. Bourbaki: *Eléments de mathématique. XX. Première partie: Les structures fondamentales de l'analyse. Livre I: Théorie des ensembles. Chapitre III: Ensembles ordonnés. Cardinaux. Nombres entiers*, Hermann & C^{ie}, Pariisi, 1956.

[4] C. C. Chang – H. J. Keisler: *Model theory*, North-Holland, Amsterdam, 1977.

[5] R. Dedekind: Was sind und was sollen die Zahlen?, ensimmäinen painos 1888, kuudes painos 1930, teoksessa R. Fricke – E. Noether – Ö. Ore (toim.): *Richard Dedekind – Gesammelte mathematische Werke*, osa 3, Fried. Viemeg & Sohn, Braunschweig, 1932.

[6] A. Doneddu: *Géométrie euclidienne plane*, Dunod, Pariisi, 1965.

[7] A. Fraenkel: *Einleitung in die Mengenlehre*, 3. uudistettu ja laajennettu painos, Springer, Berliini, 1928.

[8] A. Fraenkel – Y. Bar-Hillel – A. Levy: *Foundations of set theory*, toinen uudistettu painos, North-Holland, Amsterdam, 1973.

[9] A. Leon Sanchez: *Cantor versus Cantor*, verkkoartikkeli 2010, saatavilla osoitteesta http://arxiv.org/abs/1001.2874, luettu 28.1.2011.

[10] A. R. D. Mathias: A term of length 4 523 659 424 929, *Synthese* 133: 75–86, Kluwer, Alankomaat, 2002.

[11] J. P. Mayberry: What is required of a foundation for mathematics?, *Philosophia Mathematica* (3), Vol. 2, s. 16–35, 1994.

[12] J. P. Mayberry: *The foundations of mathematics in the theory of sets*. Encyclopedia of mathematics and its applications 82, Cambridge University Press, Cambridge, 2000.

[13] M. Potter: *Set theory and its philosophy*, Oxford University Press, Oxford, 2004.

[14] A. N. Prior: *Formal logic*, Clarendon, Oxford, 1955.

[15] J. B. Rosser: *Logic for mathematicians*, McGraw-Hill, New York, 1953.

[16] S. G. Simpson: *Foundations of mathematics*, Pennsylvania State University, Department of Mathematics, 2009. Luentomoniste, saatavilla osoitteesta http://www.math.psu.edu/simpson/courses/math558/, luettu 28.10.2010.

[17] E. Steinhart: Why numbers are sets, *Synthese* 133: 343–361, Kluwer, Alankomaat, 2002.

[18] H. Wang: On Zermelo's and von Neumann's axioms for set theory, *P. N. A. S.*, vol. 35, 1949.

[19] A. N. Whitehead – B. Russell: *Principia mathematica*, osa 1, Cambridge University Press, Cambridge, 1960. Ensimmäinen painos: 1913.