Tampereen yliopisto
Pro gradu -tutkielma

Logiikasta lukujoukkoihin

Heikki Rantalaiho

Matematiikan ja tilastotieteen laitos
Matematiikka
2010

Tiivistelmä:

Tässä tutkielmassa tarkastellaan kriittisesti kaiken muun matematiikan vaatimien peruskäsitteiden määrittelyä Zermelon-Fraenkelin aksiomatisointia noudattavan joukko-opin avulla. Havaitaan intuitionististinen lähestymistapa perustelluksi, etenkin ajatus lukumäärästä väistämättä ensisijaiseksi. Heti alussa kiinnitetään erityistä huomiota logiikan ja joukko-opin ongelmalliseen suhteeseen kvanttorien määrittelyssä. Kehäpäätelmät osoittautuvat mahdottomiksi täysin välttää. Annetaan joukon olemassaololle jo ennen aksiomatisointia alustava määritelmä kvanttorien käytön oikeutukseksi. Asetetaan tässä määriteltävyys perusvaatimukseksi ja tutustutaan sitä lähellä olevaan laskettavuuteen Turingin koneiden avulla.

Seuraavaksi aksioomat käydään yksi kerrallaan läpi, jolloin huomataan niistä monet saatavan teoreemoina kun käytössä on määriteltävyyteen perustuva joukon määritelmä. Johdetaan aksioomista tärkeimmät perustulokset pitäen tavoitteena saada työkaluja lukujen määrittelyyn. Korvausaksioomia todetaan käytetyllä kielellä olevan ääretön määrä ja äärettömyysaksiooman todetaan olevan rekursiivinen. Huomataan laskettavuuden johtavan valinta-aksioomaan. Esitetään relaatiot ja kuvaukset ja niiden perusominaisuudet sekä todistetaan tärkeimmät teoreemat. Määritellään mahtavuus ja todistetaan Schröderin-Bernsteinin teoreema.

Määritellään luonnollisten lukujen laskutoimitukset ja osoitetaan niiden noudattavan haluttuja laskusääntöjä. Muodostetaan luonnollisten lukujen järjestys joukko-oppia käyttäen mutta kyseenalaistetaan pitääkö koko luonnollisten lukujen kokoelman olla joukko. Osoitetaan Cantorin teoreema virheelliseksi kun pitäydytään määriteltävissä käsitteissä ja saadaan luonnolliset luvut yhtämahtaviksi potenssijoukkonsa kanssa. Esitetään kokonais- ja rationaaliluvut laskutoimituksineen ja järjestyksineen sekä osoitetaan ne yhtämahtaviksi kuin luonnolliset luvut. Tätä varten konstruoidaan bijektio rationaaliluvuilta luonnollisille luvuille.

Määritellään reaaliluvut Dedekindin leikkauksina ja esitetään niille järjestys. Todetaan Cantorin diagonaaliargumentti pätemättömäksi myös trikotomiaan vedoten. Kyseenalaistetaan lopuksi vahvasti koko tehdyn työn mielekkyys, perusteena etenkin loogisesti hataran äärettömyysaksiooman käyttö. Käsitellään lyhyesti äärettömän olemusta ja esitetään näkökanta, jonka mukaan kaikki äärettömät kokoelmat ovat aitoja luokkia.

Sisältö

1 Taustaa ja merkintöjä

1.1 Pyrkimys joukko-opin aksiomatisointiin

Matemaattisen käsitteistön aksiomatisointi otettiin päämääräksi 1800-luvun loppupuolella; ratkaiseva alkusysäys tälle oli aikansa johtavan matemaatikon **Richard Dedekind**in teos "Was sind und was sollen die Zahlen?", jossa ensimmäistä kertaa pyrittiin systemaattisesti formuloimaan ennen naiivin intuition varassa olleet aritmetiikan peruskäsitteet kuten luku. Matematiikan formalisointia jatkoivat ensin **Gottlob Frege** joukko-opissa ja **David Hilbert** geometriassa. Fregen paradoksillaan kriisiin ajanut **Bertrand Russel** ja **Alfred North Whitehead** pyrkivät koko matematiikan aksiomatisointiin teoksellaan "Principia Mathematica"; myöhemmin samaan pyrki nimeä **Nicolas Bourbaki** käyttänyt ranskalainen kollektiivi.

Näissä **Kurt Gödel**in ja **Alfred Tarski**n mahdottomiksi osoittamissa yrityksissä täydellisesti määritellä koko matematiikka lähdetään liikkelle *aksiomaattisesta joukko-opista*. Luvut ja muut käsitteet pyrittiin määrittelemään joukkoina.

Yleensä matematiikassa tullaan toimeen ns. *naiivilla joukko-opilla*, jossa joukko on alkioidensa määräämä kokonaisuus, käytössä ovat tavanomaiset joukkojen laskutoimitukset ja jokaista kaavaa vastaa jokin joukko. Tämä johtaa kuitenkin paradokseihin ja epätäsmällisiin käsitteisiin, tutuimpana kaikkien joukkojen muodostaman joukon muodostama joukko ja Russelin paradoksi eli kysymys: "Kylän parturi leikkaa täsmälleen niiden kyläläisten hiukset, jotka eivät leikkaa omia hiuksiaan. Leikkaako hän omat hiuksensa?".

Joukko-opin aksiomatisoinilla pyritään niin täsmällisesti kuin mahdollista määrittelemään *joukko* ja *joukkoon kuuluminen*. Esitetään tässä yleisimmin käytetty *Zermelon-Fraenkelin aksioomajärjestelmä*, merkitään **ZF**. Usein **ZF**:än lisätään vielä *valinta-aksiooma*, jolloin systeemistä käytetään lyhennettä **ZFC**.

Tässä aksiomatisoinnissa oletetaan taustalle vallalla oleva filosofia, jonka mukaan matematiikka on sitä tutkivasta subjektista riippumaton, yksikäsitteinen ja muuttumaton rakennelma. Tällainen matematiikkaa pelkästään jo valmiiksi olevaa

tutkivana eli *analyyttisenä* tieteenä pitävä filosofia tunnetaan nimellä *platonismi*. Jo tämän ajatuksen ilmaisu edellyttää kielen ja kieli sitä ymmärtävän subjektin. Jos rajoitetaan matematiikka olemaan subjektin tuntemien välttämättömien totuuksien kokonaisuus, niin se ei ole kiinteä rakennelma. Tämä filosofia on nimeltään *intuitionismi*. Intuinitionismissa matematiikkaa pidetään aidosti uutta luovana eli *synteettisenä* tieteenä. Tässä esityksessä käytetään tavanomaista logiikkaa. Käytetään logiikasta, jossa kaavalla on totuusarvo vain jos se voidaan määrittää, nimitystä *konstruktivismi*. Intuitionismille annetaan hyvin laaja merkitys eli se on käsitys, jonka mukaan kieli ja sitä käyttävä subjekti edeltävät matematiikkaa.

Aksiomatisoinnin tavoitteena on saada joukko-opista kieli, jonka avulla muu matematiikka määritellään. Joukko-opin aksiomatisointi on silti sekin puolestaan suoritettava jollakin riittävän ilmaisukykyisellä ja tarkalla kielellä, eli *aakkostolla* ja *kieliopilla*. Kieli on ennen muuta tapa varastoida, välittää ja muokata informaatiota.

Kaikista merkityksistään mahdollisimman täysin riisuttu formaali logiikka niin pitkälle kuin mahdollista abstrahoitunakin vaatii kieliopin, joka on sitä perustavampaa *metakieltä* ja joka taas vaatii metametakielisen kieliopin. Platonismin mukaan matematiikka itse on perustavin kieli, jota kaikkien kielten kieliopit noudattavat ja siis matematiikka sisältää oman kielioppinsa. Intuitionitisen käsityksen mukaan viime kädessä jokainen kieli aina perustuu metameta...metakielelle, *arkikielelle*, joka nojautuu aistikokemuksien välisille suhteille annetuille nimille ja siten fyysiseen universumiin. Tämä esityskin on kirjoitettu suomeksi kutsutulla arkikielellä, jonka sitä äidinkielenään puhuva lukija on lapsena oppinut juuri aistimaansa todellisuutta mallintamalla. Epätäsmällisiin muotoiluihin ajaudutaan väistämättä, kun todellisuutta yritetään kuvailla kielellä, joka on tuon todellisuuden osa.

Jo propositiologiikan operaattorien saaminen onnistuu vain lauseen ja siitä riippumattoman lauseen totuustaulukon käsitteen avulla. Erillisten lauseiden on siis saatava joko totuusarvo tosi tai siitä eroava epätosi ja on kyettävä erottamaan näiden yhdistelmät toisistaan. Propositiologiikan kielioppi vaatii täten ainakin käsitteet “ja”, “toisistaan riippumattomat”, “erilliset”, “tosi-epätosi”, “joko-tai” ja “yhdistelmä”. Jokainen näistä sisältää implisiittisesti käsitteen **kaksi**, joka taas edellyttää käsitettä **yksi**. Nämä ovat luonnollisia lukuja ja siis matematiikan perusteita joukko-opille rakennettaessa vasta pitkän matkan päässä. Ennen ensimmäistäkään joukko-opin aksioomaa siis havaitaan, että meillä on jo jonkinlainen käsitys lukumäärästä. Tämä ei ainakaan puolla joukko-opin käyttöä lukujen määrittelyssä.

Vaikka tässä esityksessä pyritään jos suinkin mahdollista käyttämään suomenkielisiä termejä, kuten kuvaus ja yhdiste eikä funktio ja unioni, niin loogisten symbolien suhteen näin ei tehdä objekti- ja metakielen sekoittamisen ehkäisemiseksi. Ongelma,

johon ei suomessa ole vakiintunutta ratkaisua, on mitä sanaa käyttää symbolista $=$. Yhtäsuuruus viittaa harhaanjohtavasti kokoon, joten yleensä käytetään termiä sama. Koska kyseessä on aivan objektikielen peruskäsite, niin sen käytöstä pitäisi metakielessä luopua, jolloin eri tasoilla esiintyisi helposti sekaannuksia aiheuttaen SAMA sana. Käytetään tässä esityksessä termiä *identtinen*. Samoin tässä sana *lause* varataan loogiselle kaavalle, jonka totuusarvo voidaan aina määrittää. Aksioomista loogisesti johdettu tulos on tässä *teoreema*. Vielä erotetaan pitkät nuolet *yhtäpitävyys* $\Longleftrightarrow$ ja *looginen seuraus* $\Longrightarrow$ tarkoittamaan metakielistä määrittelyä tai päättelyä. Nämä suoritetaan siis aina ennen mitään matemaattisia operaattoreita. Yhtäpitävyyden ja ekvivalenssin sekoittamisesta ei koidu suurta vahinkoa, mutta implikaatiota merkitsevä $\Rightarrow$ ja $\Longrightarrow$ on erotettava toisistaan; toisaalta induktiotodistuksissa nämäkin saatetaan käytännössä samaistaa.

1.2 Joukko-opin ja logiikan ongelmallinen suhde

Platonistisen kaanonin mukaan yksinkertaisin joukko-opin aksiomatisointiin riittävä kieli on ensimmäisen kertaluvun identtisyydellä varustettu predikaattilogiikka (esim.[Suppes, Hella, Levy]). Predikaattilogiikan määrittelyssä puolestaan aivan yhtä vakiintuneesti edellytetään joukko-oppia (esim. [Merikoski et al., Copi]). Kvanttorien tavanomainen käyttö edellyttää, että ennalta tiedetään *universumi*, johon niillä viitataan. Kaikissa löytämissäni logiikan alkeisteoksissa sen ilmoitetaan olevan epätyhjä muuttujiksi käyvistä alkioista koostuva joukko U. Joukon käsitettä vasta määriteltäessä tämä ei luonnollisesti käy.

Suomalaiset aakkoset tarkoittavat tässä aina joukkoja ja kreikkalaiset loogisia lauseita ellei muuta erikseen sovita. Merkitään joukkoon kuulumista symbolilla "$\in$"; lauseke $a \in b$ luetaan "a on joukon b *alkio*", "a kuuluu joukkoon b" tai "a kuuluu b:hen". *Identtisyys* "$=$" ja joukkoon kuuluminen ovat *predikaatteja*, joilla toisiinsa yhdistetyt *muuttujat* muodostavat aina *kaavan*. Jos siis a ja b ovat muuttujia, niin $a = b$ ja $a \in b$ ovat aina kaavoja. Jos αja β ovat kaavoja, niin myös *negaatio* $\neg\alpha$ ja *konnektiivilla* yhdistetyt kaavat *konjunktio* $\alpha \wedge \beta$, *disjunktio* $\alpha \vee \alpha$, *implikaatio* $\beta \Rightarrow \alpha$ja *ekvivalenssi* $\beta \Leftrightarrow \beta$ ovat kaavoja. Oletetaan tunnetuiksi sulkumerkinnät (ja) sekä sovitaan, että ilman sulkuja suoritetaan ensin $\neg$, sitten $\wedge$ sekä $\vee$, sitten $\Rightarrow$ja viimeiseksi $\Leftrightarrow$. [1]

[1] Tässä kirjoituksessa on siis lähteistä [Hella, Suppes, Merikoski et al.] poiketen voimassa sopimus, jonka mukaan implikaatio suoritetaan ennen ekvivalenssia. Perusteena tähän on ainoastaan kirjoittajan henkilökohtainen tottumus. Kansainvälisesti vähintään yhtä yleinen, etenkin tietojenkäsittelyssä tavallinen sopimus, jonka mukaan konjunktio suoritetaan ennen disjunktiota, taas ei tässä ole voimassa. Joissain vanhoissa teoksissa käytetty sääntö, jonka mukaan tasa-arvoiset operaattorit suoritettaisiin oikealta vasemmalle ei sekään päde. Siis $\alpha \vee \beta \wedge \gamma$ ja $\alpha \Rightarrow \beta \Rightarrow \gamma$ eivät ole hyvinmääriteltyjä logiikan kaavoja, sen sijaan tässä esityksessä $\alpha \Rightarrow \beta \Leftrightarrow \gamma$ on.

Oletetaan tunnetuiksi identtisyydellä varustetun propositiologiikan päättelysäännöt. Merkki, jossa operaattorin päälle on vedetty viiva yläoikealta alavasemmalle tarkoittaa sen negaatiota, esim. $a \notin b$ tarkoittaa samaa kuin $\neg a \in b$. Merkintä $\alpha \Leftarrow \beta$ tarkoittaa samaa kuin $\beta \Rightarrow \alpha$. Kaavan *totuusarvo*, joko *tosi* tai *epätosi*, riippuu enintään sen *vapaista muuttujista*. Jos kaava sisältää vapaan muuttujan, se on *avoin*, muutoin se on *suljettu*. Kaava, jonka totuusarvo on aina sama on *lause*, erityisesti suljettu kaava on lause. Lauseen kanssa on aina yhtäpitävä joko *tautologia* $\top$ tai *kontradiktio* $\bot$. Näistä voidaan muodostaa avoin kaava vapaalla muuttujalla x sijoittamalla $\top \Longleftrightarrow x = x$ ja $\bot \Longleftrightarrow x \neq x$.

Vielä vaaditaan käsitteet *universaalikvanttori* $\forall$ ja *eksistenssi-* eli *olemassaolokvanttori* $\exists$. Määritellään ensin merkityksestä piittaamatta että jos $\phi(x)$ on kaava, jossa x on vapaa muuttuja niin $\exists x\phi(x)$ ja $\forall x\phi(x)$ ovat kaavoja, joissa x ei enää ole vapaa muuttuja vaan *sidottu*. Määritellään myös olemaan voimassa tuttu yhteys

(UE): $\forall x\phi(x) \Leftrightarrow \neg\exists x\neg\phi(x)$.

Predikaatit suoritetaan aina ennen kvanttoreita, joten voidaan vailla sekaannuksen vaaraa käyttää lyhenteitä $\forall a \in b\alpha$ ja $\exists a \in b\alpha$; edellinen siis tarkoittaa $\forall a(a \in b \Rightarrow \alpha)$ eikä $\forall a(a \in b \wedge \alpha)$ ja jälkimmäinen $\exists a(a \in b \wedge \alpha)$ eikä $(\exists a(a \in b)) \Rightarrow \alpha$. Kvanttorin vaikutusalue päättyy vain jo sitä ennen olevan sulkumerkin "(" vastinpariin ")", joten mitään joskus käytettyjä sääntöjä kvanttorien ja konnektiiivien välisestä suoritusjärjestyksestä ei tarvita. Tuohon sulkumerkkiin se kuitenkin loppuu aina, joten esimerkiksi Suppesin jatkuvasti käyttämät tyylin $(\forall x)\alpha$ merkinnät eivät ole kieliopin mukaisia kaavoja.

Tässä haluttu kvanttorien universumi koostuu kaikista joukoista. Tämä universumi on ensin määriteltävä tai aksiomatisointi ei ole loogisesti kestävä, vaan siinä kehäpäätelmänä puhutaan sellaisesta oliosta, jota vasta määritellään. Kaavalle $\forall x\beta(x)$ pitää saada merkitys "jokaisella joukolla x pätee $\beta(x)$" ja kaavalle $\exists y\alpha(y)$ "on olemassa joukko y, jolla pätee $\alpha(y)$". Edellinen viittaa kokoelmaan ja jälkimmäinen sen yksittäiseen jäseneen, joten jälkimmäinen on perustavampi käsite jos kokoelma on epätyhjä. Sillä, että jokin ehto pätee jokaisella joukolla tarkoitetaan **UE**:n mukaan että ei ole olemassa joukkoa, jolla sen negaatio pätee. Riittää siis määritellä joukkoja koskeva ominaisuus "olla olemassa", jolla on yksikäsitteinen negaatio "ei ole olemassa".

1.3 Joukon olemassaolo

Tavallisesti joukon olemassaolon määritelmäksi otetaan vain sen kuuluminen kvanttorien universumiin, jonka saatetaan väittää tulevan määritellyksi aksiomatisoinnin edetessä. Se, että joukko on olemassa täsmälleen silloin kun se kuuluu kaikkien joukkojen kokoelmaan on kieltämättä selvää. Parempi yritys on asettaa joukolle olemassaolon ehdoksi aksioomien toteuttaminen. Minkään aksiooman kanssa ei ole ristiriidassa määritellä joukko b pelkästään niin, että $b \neq \emptyset$, jolloin kaavan $b = \{\emptyset\}$ totuusarvoa ei tiedetä. Tällaiset oliot eivät tuo joukko-oppiin mitään uutta eikä niitä *Occamin partaveitsen* mukaan tule hyväksyä.

Ei voida sallia mitään joukkoja, joihin kuuluminen ei ole yleisellä muuttujalla yksikäsitteinen kaava. Olemassaolon edellytyksenä on oltava joukon yksikäsitteisyys. Joukon yksikäsitteisyys vaatii, että voidaan muodostaa yhden vapaan muuttujan ehto, joka on tosi täsmälleen joukon alkioilla. Yleisesti olio on määriteltävissä jos se voidaan ristiriidattomasti ja yksikäsitteisesti kuvailla jollain kielellä. Jos kaavan toteuttavien muuttujien kokoelma ei toteuta aksioomia se on **ZF**:ssä ristiriitainen eikä ole joukko. Aksioomien kanssa ristiriidaton kaava määrittää joukon. Tässä riittää vaatia säännöllisyysaksiooman toteutuminen, mahdolliset ristiriidat syntyvät siitä.

Atomikaava on äärellisen pitkä. Äärellisen kaavan negaatio on äärellisen pitkä. Kvanttorilla äärellisestä kaavasta muodostettu kaava on äärellisen pitkä. Kaksi äärellistä kaavaa konnektiivilla yhdistämällä saatu kaava on äärellisen pitkä. Muutoin muodostettu lauseke ei ole kaava. Kaava on siis aina äärellisen pitkä, vaikka logiikan alkeiden yhteydessä usein korostetaan kaavan voivan olla myös ääretön. Äärellinen kaava, jonka toteuttaisi äärettömän monta muuttujaa olisi välttämättä muotoa, jossa vain kiellettäisiin ehdon toteutuminen äärellisellä määrällä muuttujia, ja johtaisi siten kaikkien joukkojen joukkoon eikä toteuttaisi aksioomia. Jos halutaan äärettömät joukot käyttöön täytyy ehdoksi hyväksyä muukin kuin tässä esitelty kaava.

Lähteissä esitetty väite, että ensimmäisen kertaluvun predikaattilogiikka olisi riittävä kieli ei pidä paikkaansa. Äärettömyysaksiooma ei ole ensimmäisen kertaluvun logiikan kieltä, koska siinä eksitenssikvanttorilla sidotun muuttujan kaavassa muuttuja esiintyy myöhemmin vapaana. Edellytetään käytettäväksi vahvempaa kieltä. Kuten joukko-opissa yleensä tehdäänkin, niin hyväksytään myös määrittävät ehdot, jotka voidaan ilmaista äärellisellä *algoritmilla* eli kaikilla muuttujilla saman äärellisen ohjeen mukainen päättelyketju suorittamalla. Perinteinen nimitys näille on *määriteltävissä oleva* eli *määriteltävä* joukko. Tässä sen synonyymina voisi käyttää olemassaolevaa.

Määritelmä 1.3.1: Joukko on äärellisesti kaavana tai algoritmina esitettävissä olevan, enintään yhden vapaan muuttujan ehdon toteuttavien alkioiden kokoelma, joka on alkioton tai sisältää alkion, joka ei itse kuulu mihinkään kokoelman alkioon. Eksistenssikvanttori ilmaisee juuri tällaisen joukon olemassaolon ja universaalikvanttori kaikkia tällaisia joukkoja koskevan ominaisuuden.

Tästä seuraa suoraan tyhjän joukon olemassaolo, sillä ehtoa $x \neq x$ ei toteuta mikään joukko.

Teoreema 1.3.2: $\exists \emptyset \forall x (x \notin \emptyset)$ $\square$.

Joukkojen olemassaolon oletetaan Levyllä seuraavan siitä, että niistä ylipäänsä puhutaan, Suppesilla tätä ei varsinaisesti edes käsitellä ja luentomonisteessa esitetään erillinen tyhjän joukon aksiooma.

On helpompaa määritellä olioita kuin kuvailla niitä. Jos joukon määrittelevänä ehtona on vaikkapa algoritmi, jonka määrittely edellyttää meta-algoritmia niin joukko voi saada suhteessa määritelmäänsä hyvin nopeasti monimutkaistuvia ominaisuuksia, jolloin se tiedetään yksikäsitteiseksi mutta sen kaikkia ominaisuuksia ei voida täysin kuvailla. Jos joukko voidaan kuvailla algoritmilla, joka kaikilla muuttujilla äärellisen monen askeleen jälkeen saa totuusarvon, niin se on *laskettavissa oleva* eli *laskettava joukko*.

1.4 Laskettavuudesta

Katsotaan nyt hieman tarkemmin 1900-luvun puolessavälissä syntynyttä *laskettavuuden teoriaa*, jonka kehittämisestä pitää erikseen mainita epätäydellisyyslauseestaan tunnettu Kurt Gödel ja ennen muuta **Alan Turing**. Hän keksi erittäin tehokkaan tavan mallintaa algoritmista ajattelua, alunalkaen ajatuskokeena, mutta tietotekniikan kehittyessä yhä konkreettisempana. Tämä keksintö on *Turingin kone*; idealisoitu tietokone, jollaisen hän osoitti voitavan ohjelmoida suorittamaan mitä vain laskutoimitusta, johon voi vastata kyllä tai ei. Sellainen voidaan määritellä varmasti kolmellasadalla symbolilla.

Turingin kone lukee $a-1$ eri aakkosesta mudostetun n merkkiä pitkän syötteen i, joiden mukaan se aloittaa lukemaan nauhalta jonkin a eri symbolista, jonka korvaa toisella ennen kuin siirtyy nauhalla askeleen kerrallaan oikeaan tai vasempaan ja mahdollisesti vaihtaa tilaansa johonkin s erilaisesta tai pysähtyy. Koneen liikesuunta, tila, ja kirjoitettu symboli rippuvat *siirtymäfunktiosta* f joka sisältää $s \times a$ ohjetta toimia jollain $s \times a \times 2$ tavasta; tästä ks. [Aaronson]. Tässä luvut a, i ja s eivät ole kovinkaan suuria. On kuitenkin huomioitava, että nauhan pituus oletetaan äärettömäksi. Mitä tahansa Turingin konetta simuloiva *universaali Turingin kone* saadaan jo jos $< s, a > \in \{< 24, 2 >, < 7, 4 >, < 2, 5 >\}$, ja ilmeisesti tähän riittää pienin epätriviaali $< 2, 3 >$-kone. Mielivaltaisen suuren koneen simulointi vaatii mielivaltaisen pitkän syötteen.

Churchin-Turingin hypoteesin mukaan kaikki laskettavissa olevat ongelmat voidaan ratkaista Turingin koneella. Hypoteesia pidetään yleisesti pätevänä, vaikka sen todistaminen katsotaan mahdottomaksi. Jos määriteltävissä olioissa on hankaluutena vaikeus saada niistä kiinteää joukkoa, niin laskettavilla ongelmallista on niiden määrittely. Churchin-Turingin hypoteesi on vaikea todistaa, sitä kun ei oikein saa formaaliksi väittämäksi. Laskettavuudelle on muitakin määritelmiä, *lambda-analyysi* ja *rekursiiviset kuvaukset* sivuutetaan kuitenkin tässä, ne ovat oleellisesti yhtäpitäviä tapoja Turingin koneen kanssa. Turingin, Gödelin ja **Alonzo Churchin** työhön pohjautuminen on joka tapauksessa käytetyin tapa. Huomionarvoista näissä kaikissa on se, että ne olettavat lukumäärän tunnetuksi käsitteeksi, mikä edellyttää intuinitionismia.

Laskettavuudella pyritään huomioimaan fyysisen todellisuuden asettamia rajoja. Tunnetuin rajoitus on seuraava. Turingin kone voi aina joko pysähtyä tai olla pysähtymättä. Itse se ei osaa tätä *pysähtymisongelmaa* yleisesti ratkaista. Turingin todistus tälle on muotoa, johon joukko-opissa turvaudutaan usein; nimittäin kone, joka osaisi ratkaista yleisen pysähtymisongelmansa määrittäisi ehdon, joka olisi muotoa

$$\forall f \forall i \varphi(i,f) = \begin{cases} 1, & (i,f) pysähtyy \\ 0, & (i,f) ei\, pysähdy \end{cases}.$$

Seuraavaksi siihen voitaisiin sitten ohjelmoida diagonaaliargumentti

$$p = \begin{cases} pysähdy; & \varphi(p,p) = 0 \\ älä\, pysähdy; & \varphi(p,p) = 1 \end{cases}.$$

Tätä vastaa sellainen laskettavien joukkojen ominaisuus, että kaikkien laskettavien joukkojen kokoelma on joukko, jonka ylinumeroituvuuden hyväksyvä platonistikin tunnustaa numeroituvasti äärettömäksi. Se ei kuitenkaan ole laskettavasti numeroituva, ellei laskettavuuden määritelmää laajenneta.

Yleistetty pysähtymisongelma on ehkäpä kaikkein tunnetuin *ratkeamaton ongelma*. Ei siis ole olemassa yleistä algoritmia, jolla voisi määrittää pysähtyykö mielivaltainen siirtymäfunktio ja syöte. Voidaan silti millä tahansa k määrittää algoritmi, joka ratkaisee pysähtymisongelman kun $f + i = k$. Kun k saa yhä suurempia arvoja, algoritmi tosin monimutkaistuu aina enemmän suhteessa edelliseen. Osoittautuu, että monimutkaisin on tilanne, jossa $f = k$ eli syöte on tyhjä ja siirtymäfunktio mahdollisimman monimutkainen.

Muodostetaan nyt kaikki mahdolliset 2 symbolin ja n tilan Turingin koneet ja valitaan niistä se joka pysähtyy tyhjällä syötteellä viimeisenä. Merkitään sen ennen pysähtymistään ottamien askelten määrää $BB(n)$ (sanoista "busiest beaver"). Ei voida millään yleisellä algoritmilla määrittää lukua $BB(n)$; tästä kun saataisiin ratkaisu pysähtymisongelmaan, koska mikään yli $BB(n)$ askelta jatkuva ohjelma ei pysähtyisi. Ei ole mitään nopeampaa tapaa määrittää $BB(n)$ kuin todella muodostaa kaikki n eri tilalla saatavat koneet ja ajaa ne. Nämä vuonna 1962 keksinyt **Tilbor Rado** osoitti hieman myöhemmin, että $BB(n)$ on *epälaskettava kuvaus*, joka kasvaa n:n kasvaessa nopeammin kuin mikään laskettavissa oleva.

Tiedetään, että $BB(0) = 0, BB(1) = 1, BB(2) = 4, BB(3) = 21$ ja $BB(4) = 107$. Tämän jälkeen ei ole enää kuin alarajoja, $BB(5)$ tuskin on kuitenkaan enemmän kuin $47\,176\,870$, näin monen askeleen jälkeen on 5 symbolia pitkä ohjelma pysähtynyt vuonna 1989 ja $88\,000\,000$ epätriviaalista ohjelmasta enää $0,3\%$:n kohdalla on pysähtyminen mahdollista. Asiaa on siis tutkittu ja jatkuvasti simuloitu kohta 50 vuotta laskutehokkuden aina kasvaessa. $BB(6) \leq 2,5 \cdot 10^{2879}$, mikä on suurin toistaiseksi löydetty arvo, tämä taas vaikuttaisi olevan edelleen kasvussa.

Määriteltävissä olevien olioiden sijaan yleisempää on rajoittua laskettaviin. Lukujen kohdalla tämä onkin perusteltua, sillä kaikki väitetyt esimerkit määriteltävistä vaan ei laskettavista luvuista joko ovat laskettavia tai eivät ole lukuja.

Vaikka yleisen pysähtymisongelman ratkaisulle ei ole algoritmia, niin sen kaikille erityistapauksille on. Universaalille Turingin koneelle on aina kaikkien mielivaltaisen pitkien syötteiden pysähtymiselle vielä pidemmällä mutta edelleen äärellisellä syötteellä ilmaistavissa oleva algoritmi. Vaikka BB ei ole laskettava kuvaus, niin $BB(n)$ on laskettava luku kullakin äärellisellä n; algoritmi on siis se, että muodostetaan kaikki 2 symbolin ja n tilan koneet ja ajetaan ne tyhjällä syötteellä ja katsotaan suurin ennen pysähtymistä otettu askelmäärä. Sen osoittaminen, ettei mikään tätä pitempään jatkava pysähdy, onnistuu sekin jollakin äärellisellä Turingin koneella.

Mielivaltaisen Turingin koneen pysähtymisen todennäköisyyttä ilmaiseva *Chaitinin vakio* Ω on laskettava aivan samassa mielessä kuin π, e tai algebralliset luvut; näiden avulla äärellisesti muodostettujen epäyhtälöiden totuus saadaan aina äärellisellä algoritmilla määritettyä. Minkään irrationaaliluvun binääri- tai desimaalikehitelmiä ei voi määrittää äärellisellä algoritmilla. Tämä tarkoittaa vain sitä, että tuollainen päättymätön kehitelmä ei ole luku eli numerojonolla ei voi ilmaista irrationaalilukua, ainoastaan sen mielivaltaisen tarkat ala- ja ylärajat. Cantorin diagonaaliargumentissa reaalilukujen ylinumeroituvuudelle konstruoitu numerojono ei sekään ole luku.

Epälaskettavien joukkojen määritelmä sisältää aina algoritmin, joka ei pysähdy. Tällaisen joukon kaikkia ominaisuuksia ei tunneta, joten sen yksikäsitteisyys pitää erikseen olettaa. Tällainen oletus tehdään tässä vain kerran, sen jälkeen tuohon joukkoon kuuluminen on kaava. Tuo joukko, jota ei voi ilman kehäpäätelmää pysähtyvällä algoritmilla määrittää, on luonnollisten lukujen joukko $\mathbb{N}$. Toinen platonistisesti tuolla tavoin määritelty joukko on $\mathbb{R}$.

2 Zermelon-Fraenkelin aksioomat

Tutkitaan nyt aksioomia tarkemmin yksi kerrallaan. Nämä ovat siis kieliopin mukaisia kaavoja, jotka määritellään tosiksi.

2.1 Ekstensionaalisuus

Joukkojen identtisyys määritellään luonnollisella tavalla. Tämä saadaan teoreemana hyödyntämällä joukolle asetettua edellytystä määrittävän ehdon yksikäsitteisyydestä.

Teoreema 2.1.1 *Ekstensionaalisuusteoreema* **(ET)**:
$\forall A \forall B(\forall x(x \in A \Leftrightarrow x \in B)) \Rightarrow A = B$.

Todistus: Valitaan mielivaltaiset A ja B, joilla $\forall x(x \in A \Leftrightarrow x \in B)$. Koska A ja B ovat joukkoja, niitä vastaavat yhden vapaan muuttujan ehdot $x \in A \Longleftrightarrow \varphi_A(x)$ ja $x \in B \Longleftrightarrow \varphi_B(x)$. Siispä $\forall x(x \in A \Leftrightarrow x \in B) \Longleftrightarrow \forall x(\varphi_A(x) \Leftrightarrow \varphi_B(x)) \Longleftrightarrow A = B$ $\square$.

Sanallisesti esitettynä: Kaksi joukkoa ovat identtiset jos niillä on identtiset alkiot. Ekstensionaalisuusaksiooman mukaan joukko voidaan siis yksikäsitteisesti kuvailla luettelemalla sen alkiot. Jos siis

(1) $x \in A \Leftrightarrow (x = a \vee x = b \vee \ldots)$,

missä $\ldots$ tarkoittaa disjunktiolla toisiinsa liitettyjä muotoa $y = x$ olevia kaavoja, niin voidaan merkitä

(2) $A = \{a, b, \ldots\}$,

missä $\ldots$ tarkoittaa pilkuilla toisistaan erotettuina täsmälleen kaikkia niitä alkioita, jotka esiintyvät kaavassa **(1)**.

Tässä platonistit käyttävät poikkeuksetta alaindekseinä luonnollisia lukuja, mikä äkkiseltään vaikuttaa melko intuinitionistiselta.

Seuraava on olennaisesti muista aksioomista poikkeavaa muotoa. Siinä esiintyvä ψ on mielivaltainen ehto. Joukkojen suhteen kyseessä on siis oma aksioomansa jokaista tällaista ehtoa kohden ja näitä taas voidaan muiden aksioomien perusteella osoittaa olevan rajattoman suuri määrä. On mahdotonta esittää **ZF** äärellisellä määrällä ensimmäisen kertaluvun aksioomia.

Tällaisesta kokoelmasta aksioomia käytetään englanniksi nimitystä "axiom schema". Suomeksi sanotaan yleensä vain "aksioomat"; kuitenkin "axiom schema" on mielestäni eri asia kuin vain "axioms", siksi siitä käytetäänkin myös nimitystä "aksioomakaavio" tai "aksioomajärjestelmä". Aksioomasto on mielestäni hyvä käännös, joka sanatarkan vastineen puuttuessa käyttää suomelle ominaista päätettä merkityksen säilyttämiseen.

2.2 Korvausaksioomasto ja osajoukkoteoreemasto

Lähteissä tähän liitetyt vaatimukset vapaista muuttujista ovat hieman outoja, yleisimmin edellytetty "A ei ψ:n vapaa muuttuja" on mahdoton koska $\psi(y,x)$ on määritelty täsmälleen silloin kun x kuuluu joukkoon A. Sen sijaan pitää vaatia, että A ei ole y:n vapaa muuttuja. Jos jokin muu muuttuja vaikuttaa ehdon totuusarvoon, niin saadaan useita kahden muuttujan kaavoja. Kolmen vapaan muuttujan ehdosta $\phi(x,y,z)$ voidaan muodostaa ehto $\psi(x,\{y,z\})$ ja muiden kahden muuttujan pysyessä samana ehdon totuusarvoon vaikuttavien y:n tai z:n arvo antaa niin monta eri ehtoa kuin on eri tilanteita, jossa sitä muuttamalla muuttuu ehdon totuus, saadaan siis ehdot $\psi_{y1}(x,z), \psi_{y2}(x,z), ..., \psi_{yn}(x,z), \psi_{z1}(x,y), ..., \psi_{zm}(x,y)$.

Korvausaksioomasto **(KA)**: Kun ψ on kahden vapaan muuttujan ehto, niin
$\forall b(\forall w \in b \forall v \forall u(\psi(w,u) \wedge \psi(w,v) \Rightarrow u = v) \Rightarrow$
$\exists a \forall x(x \in a \Leftrightarrow \exists y \in b(\psi(y,x))))$ on aksiooma.

Siis ehdon, jonka ensimmäisen parametrin kuuluessa annettuun joukkoon jälkimmäisinä toteuttavat ja tällöin yksikäsitteiset parametrit muodostavat joukon.

Tässä on siis oma aksioomansa jokaista ehtoa ψ kohden. Tästä saadaan usein omana aksioomastonaan annettu seuraus, joka on muodostettu korvaamaan

Abstraktioaksiooma **(AA)**:$\forall \varphi \exists A \forall x(x \in A \Leftrightarrow \varphi(x))$ (Frege 1893),

missä ensimmäinen kvanttori koskee ehtojen kokoelmaa, eli **AA** on korkeamman kertaluvun logiikkaa.

Tästä seuraa mm. *Russelin paradoksi* (1901): ehdolla $\varphi(x) \Longleftrightarrow x \notin x$ saadaan

$\exists A \forall x(x \in A \Leftrightarrow x \notin x)$, jonka takaamaan joukkoon A sijoitus $x = A$ tuottaa kontradiktion $A \in A \Leftrightarrow A \notin A$.

Tämä saadaan estettyä vaatimalla valmis perusjoukko, jolloin saadaan

Teoreema 2.2.1: *Osajoukkoteoreemasto* **(OT)**: Jokaista yhden muuttujan ehtoa φ kohden $\forall B \exists A \forall x(x \in A \Leftrightarrow x \in B \wedge \varphi(x))$ on teoreema.

Todistus: Jokaisesta kaavasta $\varphi(x)$ voidaan muodostaa $\psi(w, u) = \varphi(w) \wedge w = u$, jota vastaava korvausaksiooma saadan muotoon $\forall B(\forall w \in b \forall u \forall v(\varphi(w) \wedge w = u \wedge \varphi(w) \wedge w = v \Rightarrow u = v) \Rightarrow \exists A \forall x(x \in A \Leftrightarrow \exists y \in B(\varphi(y) \wedge y = x))$, mikä on sama kuin ehtoa φ vastaava osajoukkoteoreema $\square$.

Tässä kaikki kvanttorit viittavat kyllä joukkoihin toisin kuin abstraktioaksioomassa, mutta tässä on vain tehty silmänkääntötemppu. "Jokaista ehtoa φ kohden" on vain sanallinen esitys merkinnälle $\forall \varphi$, sama temppu tehdään myös **KA**:ssa.

Siis jokaista ehtoa ja joukkoa kohden voidaan muodostaa uusi joukko, johon kuuluvat täsmälleen ne alkuperäisen joukon alkiot, jotka toteuttavat ehdon. Otetaan tälle merkintä

$A = \{x \in B \mid \varphi(x)\}$.

Nimensä mukaisesti tämän avulla voidaan tuottaa juuri osajoukkoja, joten osajoukkouden käsite on syytä määritellä.

Määritelmä 2.2.2: **(i)** $A \subseteq B \Longleftrightarrow \forall x(x \in A \Rightarrow x \in B)$, luetaan A on joukon B *osajoukko* eli A on B:n osajoukko.

(ii) Jos lisäksi $A \neq B$, niin A on B:n *aito osajoukko*, merk. $A \subset B$.

Voidaan myös merkitä $A \supseteq B$, jos B on A:n osajoukko; vastaavasti voidaan käyttää symbolia $\supset$. Joissain lähteissä merkitään osajoukkoutta $\subset$ ja aitoa osajoukkoutta $\subsetneq$, mutta tässä esityksessä notaatio on tämä.

Seuraavat kaksi lausetta pätevät myös aidolle osajoukkoudelle ja niiden todistukset seuraavat suoraan osajoukkouden määritelmässä käytetyn implikaation ominaisuuksista.

Teoreema 2.2.3: $\forall A(\emptyset \subseteq A \subseteq A)\,\square$.

Teoreema 2.2.4: $\forall A \forall B \forall C(A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C)\,\square$.

Voidaan siis merkitä $A \subseteq B \subseteq C$. Selvästi tällöin $A \subset B \vee B \subset C \Leftrightarrow A \subset C$.

OT välttää Russelin paradoksin; sijoitus $\varphi(x) \Longleftrightarrow x \notin x$ teoreemaan

$\forall b \exists a \forall x(x \in a \Leftrightarrow x \in b \wedge \varphi(x))$

johtaa lausekkeeseen $\forall b \exists a \forall x(x \in a \Leftrightarrow x \in b \wedge x \notin x)$, johon sijoitus $x = a$ antaa

$\forall b \exists a(a \in a \Leftrightarrow a \in b \wedge a \notin a) \Longleftrightarrow \forall b \exists a(\neg(a \in a) \wedge \neg(a \in b \wedge \neg(a \in a))) \Longleftrightarrow \forall b \exists a(a \notin a \wedge a \notin b)$,

joka ei ole kontradiktio.

Seuraava aksiooma on tässä sisällytetty jo joukon määritelmään. Se estää alkeellisimmat paradoksit.

2.3 Säännöllisyysaksiooma

Säännöllisyysaksiooma (**SA**): $\forall A \exists b \in A(\exists x \in A(\forall y \in x(y \notin A))))$.

Tämän mukaan jokaisella epätyhjällä joukolla on ainakin yksi alkio, jonka mikään alkio ei kuulu alkuperäiseen joukkoon, eli mikään epätyhjä joukko ei sisällä yhteistä alkiota kaikkien alkioidensa kanssa.

Saadaan tärkeä tulos, jonka mukaan mikään joukko ei ole itsensä alkio.

Teoreema 2.3.1: $\forall a(a \notin a)$.

Todistus: Selvästi $\emptyset \notin \emptyset$, joten valitaan mielivaltainen $a \neq \emptyset$, jolloin $\exists b \in a$ ja muodostetaan kaava $\psi(w,u) \Leftrightarrow w = b \wedge u = a$, jolloin **KA**:n avulla joukosta a saadaan $\{a\}$. Selvästi $\{a\} \neq \emptyset$, joten **SA** mukaan $\exists x \in \{a\} \wedge (\forall y(y \in x \Rightarrow y \notin \{a\}))$ eli $\forall y(y \in a \Rightarrow y \notin \{a\})$. Sijoittamalla $y = a$ pätee erityisesti
$(a \in a \Rightarrow a \notin \{a\}) \Longleftrightarrow (a \in a \Rightarrow \bot) \Longleftrightarrow a \notin a$ □.

Russelin paradoksin ehdon täyttää siis jokainen joukko. Nyt kaavaa $\varphi(x) \Longleftrightarrow x \notin x$ vastaava **OT** antaa $\forall b \exists a \forall x(x \in a \Leftrightarrow x \in b \wedge x \notin x)$, mikä on **2.3.1** mukaan $\forall b \exists a \forall x(x \in a \Leftrightarrow x \in b \wedge \top)$, eli $\forall b \exists a(a = b)$. Samoin jos sijoitetaan ennen teoreeman käyttöä $x = a$, niin saadaan $\forall b \exists a(a \notin a \wedge a \notin b)$, mikä on **2.3.1** nojalla yhtä kuin $\forall b \exists a(a \notin b)$, minkä toteuttaa ainakin $a = b$.

Rajoitttautuminen vain osajoukkojen muodostamiseen on välttämätöntä; abstraktioaksioomalla ja nyt varmasti sallitulla ehdolla $\varphi(x) \Longleftrightarrow x \notin x$ päätyisimme kyllä Russelin paradoksiin sijoittamalla $x = A$. Abstraktioaksioomaan sijoitettu ehto $\varphi(x) \Longleftrightarrow \top$ johtaisi kaikkien joukkojen joukkoon V, jolle pätisi $\forall x(x \in V)$, erityisesti siis $V \in V$ vastoin teoreemaa **2.3.1**. Kaikkien joukkojen kokoelma ei siis säännölisyysaksiooman voimassaollessa ole joukko, vaan *aito luokka*.

Emme vieläkään tiedä, onko epätyhjiä joukkoja edes olemassa. Osajoukkona oleminen on oleellinen käsite seuraavassa tämän takaavassa yleensä aksioomaksi laskettavassa, mutta joukon määritelmästä tässä teoreemana saatavassa tuloksessa.

2.4 Potenssijoukko

Teoreema 2.4.1: *Potenssijoukkoteoreema* **(PT)**: $\forall A \exists B = \{x \mid x \subseteq A\}$.

Todistus: Valitaan mielivaltainen A. Se koostuu ehdon $\varphi_A(x)$ toteuttavista joukoista. Muodostetaan ehto $\varphi_B(x) \Longleftrightarrow \forall y \in x(\varphi_A(y))$. Tässä y on sidottu ja x ainoa vapaa muuttuja, lisäksi $\varphi_B(\emptyset)$ on tosi, joten **SA** ei estä että B on joukko, sillä $\emptyset$ on vaadittava erillinen alkio □.

Tämä tarkoittaa, että jokaista joukkoa kohden on olemassa sen kaikista osajoukoista koostuva joukko.

Potenssijoukko on yksikäsitteinen, merkitään symbolilla $\mathcal{P}$.

Määritelmä 2.4.2: $\mathcal{P}(A) = \{x \mid x \subseteq A\}$.

Suoraan **PT**:n avulla joukon Ø ainoa osajoukko Ø muodostaa joukon$\{\emptyset\}$, joka synnyttää osajoukkojensa muodostaman joukon $\{\emptyset, \{\emptyset\}\}$, jonka potenssijoukko taas on $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\{\emptyset\}, \{\{\emptyset\}\}\}\}$, jonka osajoukoista saadaan jälleen uusi joukko, jne.

Tällaisessa joukossa, jonka olemassaolo on aksiooman takaama ja jonka voimme aina mekaanisesti konstruoida, on aina alkioina kaikki edellisen joukon alkioiden yksinään muodostamat joukot ja tyhjä joukko, siis enemmän alkioita kuin missään aiemmassa. Se on siis **ET**:n perusteella eri joukko kuin mikään aiempi. Tämäkin viittaisi siihen, että lukumäärä edeltää aksiomatisoinnissa joukkoa.

Tämä tarkoittaa, että voimme muodostaa rajatta lisää joukkoja tyhjästä joukosta **PT**:n avulla, joten joukkoja on potentiaalisesti ääretön määrä.

PT:n mukaan myös erityisesti $\{\emptyset, \{\emptyset\}\}$ on joukko, mikä mahdollistaa joskus aksioomanakin esitetyn parin muodostamisen.

Teoreema 2.4.3: $\forall a \forall b \exists c = \{a, b\}$.

Todistus: Valitaan mielivaltaiset a ja b ja muodostetaan kaava $\psi(w, x) \iff (w = \emptyset \wedge x = a) \vee (w = \{\emptyset\} \wedge x = b)$, jota vastaava **KA** muodostaa joukosta $\{\emptyset, \{\emptyset\}\}$ halutun parin $\{a, b\}$ $\square$.

Siis mitä vain kahta joukkoa kohden on joukko, jossa ne ovat ainoat alkiot.

Erityisesti jos sijoitetaan tähän $b = a$, saadaan

Teoreema 2.4.4: $\forall a \exists c = \{a\}$ $\square$.

Monen tärkeän joukon konstruoiminen vaatii alkioille järjestyksen. Sellainen saadaan pienellä tempulla.

Määritelmä 2.4.5: Joukko$\{\{x\}, \{x, y\}\}$ on joukkojen x ja y *järjestetty pari*, merkitään $< x, y >$.

Muodostetaan siis ensin kahdesta oliosta **2.4.3**:n nojalla pari ja sitten saadusta parista ja sen järjestykseen ensimmäiseksi halutun alkion muodostamasta joukosta uusi pari. Järjestetty pari on triviaalisti yksikäsitteinen.

Nyt saadaan tulos, jonka mukaan mitkään kaksi joukkoa eivät voi molemmat sisältää toisiaan.

Teoreema 2.4.5: $\forall A \forall B(A \notin B \vee B \notin A)$.

Todistus: Valitaan mielivaltaiset A ja B ja muodostetaan **2.4.3**:n mahdollistama joukko $\{A, B\}$ sekä huomataan että se selvästi on epätyhjä. Nyt **SA**:n mukaan $\exists x \in \{A, B\} \wedge \forall y(y \in x \Rightarrow y \notin \{A, B\})$. Valitaan tällainen x. Koska $x = A \vee x = B$, saadaan

$(\forall y(y \in A \Rightarrow y \notin \{A, B\})) \vee (\forall z(z \in B \Rightarrow z \notin \{A, B\}))$, mihin sijoittamalla $y = B$ ja $z = A$ saadaan

$(B \in A \Rightarrow B \notin \{A, B\}) \vee (A \in B \Rightarrow A \notin \{A, B\}) \Longleftrightarrow (B \in A \Rightarrow \bot) \vee (A \in B \Rightarrow \bot) \Longleftrightarrow B \notin A \vee A \notin B$ □.

Erityisesti saadaan sijoittamalla $B = \{A\}$ seuraus $\forall A(\{A\} \notin A)$.

Todistus oli vastaava kuin teoreeman **2.3.2** ja olisikin riittänyt todistaa **2.4.5**, jolloin **2.3.2** olisi seurannut siitä erikoistapauksena, jossa $A = B$. Tässä [Suppes] s. 53 toteaa, että vastaava päättely on voimassa kolmen tai useamman joukon sykleille joten teoreema voidaan yleistää näille. Tämä toteamus puhuu eksplisiittisesti lukumäärästä ja implisiittisesti induktion käsitteestä.

Koska **OT**:n mukaan $\forall B \forall C \exists A \forall x(x \in A \Leftrightarrow x \in B \wedge x \notin C)$ ja $\forall B \forall C \exists A \forall x(x \in A \Leftrightarrow x \in B \wedge x \in C)$, saadaan tutut määritelmänomaiset teoreemat.

Teoreema 2.4.6: $\forall B \forall C \exists A = \{x \in B \mid x \notin C\}$ □; joukkoa A kutsutaan joukkojen B ja C *erotukseksi* tai joukon C *komplementiksi* joukon B suhteen, merkitään $B \setminus C$

ja

Teoreema 2.4.7: Jos $\forall B \forall C \exists A = \{x \in B \mid x \in C)$ □; joukkoa A kutsutaan joukkojen B ja C *leikkaukseksi*, merkitään $B \cap C$.

Sen sijaan kahden joukon yhdiste ei ole osajoukko, joten sitä ei voi **OT**:lla muodostaa. Seuraava aksiooma mahdollistaa tämän ja sen yleistyksen.

2.5 Yhdisteaksiooma

Tätä ei ilman induktioperiaatetta saada teoreemana vaan tämä on ainakin toistaiseksi aito aksiooma.

Yhdisteaksiooma **(YA)**: $\forall A \exists C = \{x \mid \exists B(x \in B \wedge B \in A)\}$.

Sanoiksi puettuna jokaisella joukolla on olemassa täsmälleen sen kaikkien alkioiden kaikista alkioista koostuva joukko.

Seuraavaksi määriteltävän joukon olemassaolo seuraa triviaalisti yhdisteaksioomasta.

Määritelmä 2.5.1: $\bigcup A = \{x \mid \exists B(x \in B \wedge B \in A)\}$, joukkoa $\bigcup A$ kutsutaan joukon A *yhdisteeksi* tai lyhyesti A:n yhdisteeksi.

Vastaava yleinen leikkaus eli joukon kaikille alkioille yhteisten alkioiden joukko voidaan määritellä vain epätyhjille joukoille ellei erikseen sovita, että $\bigcap \emptyset = \emptyset$.

Teoreema 2.5.2: $\forall A \neq \emptyset \exists L = \{x \mid \forall Y(Y \in A \Rightarrow x \in Y\}$

Todistus: Valitaan mielivaltainen $A \neq \emptyset$, jolloin$\forall Y(Y \in A \Rightarrow x \in Y)\}$ on **OT**:n kelpaava $\varphi(x)$. Erityisesti joukolle $\bigcup A$ pätee $\exists L \forall x(x \in L \Leftrightarrow x \in \bigcup A \wedge \forall Y(Y \in A \Rightarrow x \in Y)\} \Longleftrightarrow \exists L = \{x \mid \exists B(B \in A \wedge x \in B)\} \wedge \forall Y(Y \in A \Rightarrow x \in Y)\}$. Koska jälkimmäisestä ehdosta aina, kun $Y \in A$ seuraa ensimmäinen sijoituksella $Y = B$, voidaan ensimmäinen ehto jättää huomiotta ja siis $\exists L = \{x \mid \forall Y(Y \in A \Rightarrow x \in Y)\}$ $\square$.

Nyt voidaan määritelmää **2.5.1** vastaavasti määritellä

Määritelmä 2.5.3: $\bigcap A = \{x \mid \forall B(B \in A \Rightarrow x \in B\}$, kun $A \neq \emptyset$, $\bigcap A$ on joukon A leikkaus eli A:n leikkaus.

Kahden joukon yhdisteen olemassaolo voidaan nyt myös todistaa.

Teoreema 2.5.4: $\forall B \forall C \exists A = \{x \mid x \in B \vee x \in C\}$; joukkoa A kutsutaan joukkojen B ja C *yhdisteeksi* eli *unioniksi*, merk. $B \cup C$.

Todistus: Valitaan mielivaltaiset B ja C, muodostetaan **2.4.3** takaama joukko $\{B, C\}$ ja sovelletaan tähän yhdisteaksioomaa, jonka mukaan $\exists A = \{x \mid \exists D(x \in D \wedge D \in \{B, C\})\} = \{x \mid \exists D(x \in D \wedge (D = B \vee D = C))\} = \{x \mid x \in B \vee x \in C\}$ □.

Kahden joukon leikkaus ja yhdiste muistuttavat loogisia konnektiiveja $\wedge$ ja $\vee$, joiden avulla ne muodostetaan. Ne ovat niiden tavoin vaihdannaisia ja liitännäisiä ja noudattavat osittelulakeja, todistukset seuraavat suoraan logiikan vastaavista tuloksista. Liitännäisyyden nojalla voidaan puhua useammankin joukon yhdisteistä ja leikkauksista. Yhdisteaksiooman nimi on mielekäs juuri tästä syystä. Tuttujen joukko-opillisten laskusääntöjen todistukset saadaan **ET**:n nojalla vastaavista logiikan säännöistä samaan tapaan kuin seuraavan, myöhemmin esitettävän Schröderin-Bernsteinin teoreeman todistuksessa olennaisen aputuloksen.

Teoreema 2.5.5: $\forall Z \forall X \subseteq Z \forall Y \subseteq Z(X \subseteq Z \setminus Y \Leftrightarrow Y \subseteq Z \setminus X)$,

Todistus: Valitaan mielivaltaiset X, Y ja Z siten, että $X \subseteq Z \wedge Y \subseteq Z$. Nyt

$X \subseteq Z \setminus Y \Longleftrightarrow (\forall a(a \in X \Rightarrow (a \in Z \wedge a \notin Y))) \Longleftrightarrow \forall a((a \notin Z \vee a \in Y) \Rightarrow a \notin X) \Longleftrightarrow \forall a((a \in Y \Rightarrow a \in Z) \wedge (a \in Y \Rightarrow a \notin X)) \Longleftrightarrow Y \subseteq Z \setminus X$ □.

Joukon yhdisteen ottaminen on potenssijoukon muodostamisen osittainen käänteisoperaatio. Seuraavat kaksi tulosta selventävät tätä:

Teoreema 2.5.4:$\bigcup \mathcal{P}(A) = A$.

Todistus:
$\bigcup \mathcal{P}(A) = \{x \mid \exists B(x \in B \wedge B \in \mathcal{P}(A))\} = \{x \mid \exists B(x \in B \wedge B \subseteq A\} = \{x \mid x \in A\} = A$□.

Joukon potenssijoukon yhdiste on siis joukko itse.

Teoreema 2.5.5:$A \subseteq \mathcal{P}(\bigcup A)$.

Todistus: Teoreema on selvästi tosi jos $A = \emptyset$. Valitaan mielivaltainen $x \in A$. Nyt on voimassa $(\forall z \in x)(\exists B = x)(z \in B \wedge B \in A) \Longleftrightarrow \forall z(z \in x \Rightarrow z \in (\bigcup A) \cap x) \Longleftrightarrow x \subseteq \bigcup A \cap x \Leftrightarrow x \in \mathcal{P}(\bigcup A) \cap \{x\} \Longrightarrow x \in \mathcal{P}(x)$ □.

Todistuksesta ilmenee lisäksi, että $A = \mathcal{P}(\bigcup A) \Leftrightarrow (\forall x \in A) \bigcup A = x \Leftrightarrow A = \{\{z\}\}$ eli A:ssa on täsmälleen yksi täsmälleen yhden alkion joukko. Yleensä joukko on yhdisteensä potenssijoukon osajoukko tämän ollessa sitä huomattavasti laajempi.

Nyt on vihdoin kasassa riittävästi tuloksia, että onnistuu kahden joukon karteesinen tulon osoittamisen joukoksi:

Teoreema 2.5.6: $\forall A \forall B \exists C \forall x (x \in C \Leftrightarrow \exists y \exists z (y \in A \wedge z \in B \wedge x =< y, z >)$.

Todistus: Valitaan mielivaltaiset A ja B. Jos jompikumpi joukoista on tyhjä, toteutuu teoreema triviaalisti kun asetetaan $C = \emptyset$. Oletetaan sitten, että $A \neq \emptyset \neq B$.

Nyt voidaan muodostaa **2.5.4** ja **PT** nojalla joukko $\mathcal{P}(\mathcal{P}(A \cup B))$. Tämä ja ehto $\varphi(x) \Leftrightarrow \exists y \exists z (y \in A \wedge z \in B \wedge x =< y, z >)$ voidaan sijoittaa **OT**:on tuloksena

$\exists D = \{x \in \mathcal{P}(\mathcal{P}(A \cup B)) |\ \exists y \exists z (y \in A \wedge z \in B \wedge x =< y, z >)\}$.

Oletetaan nyt $\varphi(x)$, jolloin $\exists y \in A \wedge \exists z \in B$ ja **PT**:n perusteella voidaan muodostaa joukot $\{y\}$, $\{y, z\}$ ja edelleen $\{\{y\}, \{y, z\}\}$. Kahden joukon yhdisteen, osajoukon ja potenssijoukon määritelmien perusteella $\varphi(x) \Longrightarrow (y \in A \cup B \wedge z \in A \cup B) \Longrightarrow (\{y\} \subseteq A \cup B \wedge \{y, z\} \subseteq A \cup B) \Longrightarrow (\{y\} \in \mathcal{P}(A \cup B) \wedge \{y, z\} \in \mathcal{P}(A \cup B)) \Longrightarrow (\{\{y\}, \{y, z\}\} \subseteq \mathcal{P}(A \cup B)) \Longrightarrow x \in \mathcal{P}(\mathcal{P}(A \cup B)) \wedge \varphi(x) \Longrightarrow x \in D$.

Selvästi myös $x \in D \Longrightarrow \varphi(x)$, joten joukko D kelpaa teoreeman edellyttämäksi joukoksi C $\square$.

Määritelmä 2.5.7: Joukkojen A ja B *karteesinen tulo*
$A \times B = \{< a, b > |\ a \in A \wedge b \in B\}$.

Olemme jo tähänkin päästäksemme välttämättä tarvinneet lukumäärää ilmaisevia käsitteitä "yksi" ja "kaksi". Oikeastaan olemme joutuneet käyttämään myös käsitettä "kolme", näin on tehty aina kun aksioomassa tai teoreemassa on esitetty eksistenssikvanttorilla uusi, kahdesta aiemmasta riippuva olio. Esimerkiksi kahdesta alkiosta muodostettu pari tai kahden joukon leikkaus on kolmas käsite. Toteamalla yhdiste ja leikkaus keskenään eri käsitteiksi olisi päädytty lukumäärään neljä.

Lukumäärät olisi siis syytä saada hyvinmääritellyiksi käsitteiksi. Lisäksi tarvittaisiin menetelmä, jolla lukumäärästä riippumaton tulos voitaisiin yleistää, kuten teoreema **2.4.2** Suppesin mukaan. Nämä vaatimukset toteutetaan yksinkertaisimmalla mahdollisella tavalla, kun määritellään *luonnolliset luvut* $\mathbb{N}$. Ne ovat olio, joka toteuttaa seuraavat, ensimmäisenä ne täsmällisesti muotoilleen **Giuseppe Peano**n mukaan nimetyt postulaatit:

(P1) $0 \in \mathbb{N}$

(P2) $n \in \mathbb{N} \Longrightarrow n+1 \in \mathbb{N}$

(P3) $\nexists n \in \mathbb{N}(n+1) = 0$

(P4) $\forall x \in \mathbb{N} \forall y \in \mathbb{N}(x+1 = y+1) \Longrightarrow x = y$

(P5') Jos $\varphi(x)$ on kaava, niin $\varphi(0) \wedge \forall x \in \mathbb{N}(\varphi(x) \Rightarrow \varphi(x+1)) \Longrightarrow \forall x \in \mathbb{N}(\varphi(x))$ on postulaatti.

Siis jälleen vaaditaan toisen kertaluvun logiikkaa, edellinen on sama kuin

(P5) $\forall \varphi(\varphi(0) \wedge \forall x \in \mathbb{N}(\varphi(x) \Rightarrow \varphi(x+1)) \Longrightarrow \forall x \in \mathbb{N}(\varphi(x)))$**.**

Tavanomaisena pyrkimyksenä on saada määriteltyä $\mathbb{N}$ niin, että se on joukko, jossa $0 = \emptyset$ ja $n+1 = n \cup \{n\}$. Pidetään nyt toistaiseksi tätä järjellisenä tavoitteena. Seuraavan aksiooman katsotaan yleisesti tähän riittävän. Aksiooma on rekursiivinen.

2.6 Äärettömyysaksiooma

Tässä aksiomatisoidaan olemassaolevaksi joukoksi kokoelma, johon lähes minkään joukon ei voi osoittaa olevan kuulumatta. Tässä vakiintunut symboli I ei tule sanasta "infinite" vaan sanasta "inductive".

Äärettömyysaksiooma **(ÄA')**: $\exists I(\emptyset \in I \wedge \forall x(x \in I \Rightarrow x \cup \{x\} \in I))$.

Tässä joukon I määrittävä ehto on $\varphi_I(x) \Longleftrightarrow \emptyset \in I \wedge x \cup \{x\} \in I$ ja aksiooma siis muotoa

(ÄA): $\exists I = \{x \mid \emptyset \in I \wedge x \cup \{x\} \in I\}$.

On siis olemassa ainakin yksi sellainen joukko, joka sisältää tyhjän joukon ja jokaisen alkionsa yhdisteen alkion muodostaman joukon kanssa. Kutsutaan tällaista joukkoa *induktionaaliseksi*. Tässä käytetään yleensä nimitystä induktiivinen; siitä saa kuitenkin helposti käsityksen että induktioperiaate olisi tällöin pätevä. Se on pätevä täsmälleen luonnollisilla luvuilla, joka on yksikäsitteinen olio ja näin ollen ainoastaan sitä kuvaava adjektiivi on turha.

Tämä rekursiivinen määritelmä ei suoraan määrittele yksikäsitteistä joukkoa.

Tyhjästä joukosta saadaan **PT**:n avulla muodostettua joukko $0' = \{\{\emptyset\}\}$. Olkoon I **ÄA**:n olemassaolevaksi takaama joukko. Hyvinmääritellyn kaavan $0' \in I$ totuusarvoa ei voida **ZF**:n aksioomista johtaa. Voidaan osoittaa, että vaikkapa $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \in I$, mutta $x \notin I$ voidaan osoittaa todeksi vain kun $x = I$ tai $x = \{I\}$, jos emme tiedä joukosta I muuta kuin että se on induktionaalinen.

Määritelmillä

(N0) $0 = \emptyset$

(NS) $n + 1 = n \cup \{n\}$ **P3** on selvästi tosi. Myös **P4** on tällöin tosi määritellään itse joukko $\mathbb{N}$ miten tahansa.

Teoreema 2.6.1: **P4**.

Todistus: Tehdään vastaoletus, jonka mukaan $\exists x, y$ siten, että $x \neq y$ mutta $x \cup \{x\} = y \cup \{y\}$. Symmetrian nojalla voidaan olettaa, että $\exists a(a \in x \wedge a \notin y)$. Nyt $a \in x \Longrightarrow a \in x \cup \{x\} \Longrightarrow a \in y \cup \{y\} \Longrightarrow a \in y \vee a = y \Longrightarrow a = y \Longrightarrow y \in x \Longrightarrow x \notin y \Longrightarrow x \neq y \wedge x \notin y \Longrightarrow x \notin y \cup \{y\} \Longrightarrow x \notin x \cup \{x\} \Longrightarrow x \neq x$, mikä on ristiriita. Siis vastaoletus on väärä ja teoreema pätee $\square$.

Suppes esittää luonnollisten lukujen määritelmänä

(N1) $\emptyset \in \mathbb{N}$; $0 = \emptyset$,

(N2) $n \in \mathbb{N} \Longrightarrow n \cup \{n\} \in \mathbb{N}$; $n + 1 = n \cup \{n\}$ ja

(N3) $(\emptyset \in A \subseteq \mathbb{N}) \wedge (\forall x(x \in A \Rightarrow x \cup \{x\} \in A)) \Longrightarrow A = \mathbb{N}$.

P1 ja **P2** toteutuvat nyt, ja **P5**:kin näyttäisi toteutuvan.

Luentomonisteessa [Hella]s.32 valitaan mielivaltainen **ÄA**:n takaama induktionaalinen joukko ja muodostetaan tästä **OT**:n avulla ω ehdolla "kuuluu jokaiseen induktionaaliseen joukkoon", joka ei tuossa muodossa ole predikaattilogiikan kaava. Jos kirjoitetaan tämä formaaliin muotoon, saadaan

$\forall x(x \in \omega \Leftrightarrow x \in I \wedge \forall A(\emptyset \in A \wedge \forall y(y \in A \Rightarrow y \cup \{y\} \in A) \Rightarrow x \in A))$, eli sama olio kuin Suppesin $\mathbb{N}$.

Kaikkien induktionaalisten joukkojen kokoelman leikkauksesta ei tiedetä kuin epätyhjyys. Äärettömyysaksiooman nojalla voidaan kuitenkin valita yksi sellainen, ja soveltaa siihen **OT**:a $\varphi(x) \Longleftrightarrow \forall y(\emptyset \in y \wedge (\forall z(z \in y \Longrightarrow z \cup \{z\} \in y)x \in y$. Tämän nojalla saadaan

Teoreema 2.6.2: $\exists \mathbb{N}(x \in I \mid \forall x(\forall I(\emptyset \in I \wedge \forall z(z \in I \Rightarrow z \cup \{z\} \in I)x \in I)\ \square$.

Siis on olemassa induktionaalinen joukko, joka on jokaisen induktionaalisen joukon osajoukko. Selvästi $\mathbb{N}$ toteuttaa postulaatit **P1** ja **P2**. Tälle ei ole mahdollista kirjoittaa määrittävää ehtona muutoin kuin rekursiivisena kaavana:

$\varphi_{\mathbb{N}}(x) \Longleftrightarrow 0 \in \mathbb{N} \wedge x + 1 \in \mathbb{N} \wedge \forall I(0 \in I \wedge \forall z \in I(z + 1 \in I))x \in I$.

Saadaan siis

Määritelmä 2.6.3 :
$\mathbb{N} = \{x \mid \emptyset \in \mathbb{N} \wedge x \cup \{x\} \in \mathbb{N} \wedge \forall I(\emptyset \in I \wedge \forall z \in I(z \cup \{z\} \in I))x \in I\}$; sanotaan $\mathbb{N}$ on *Luonnollisten lukujen joukko.*

Teoreema 2.6.4 : **P5**.

Todistus: Valitaan mielivaltainen ehto φ siten, että $\varphi(0) \wedge \forall x \in \mathbb{N}(\varphi(x) \Rightarrow \varphi(x + 1))$. Muodostetaan **OT**:n avulla joukko $A = \{y \in \mathbb{N} \mid \varphi(y)\} = \{y \mid (\emptyset \in \mathbb{N} \wedge y + 1 \in \mathbb{N} \wedge \forall I(\emptyset \in I \wedge \forall z \in I(z + 1 \in I))y \in I) \wedge \varphi(y) \wedge (\varphi(0) \wedge \forall x \in \mathbb{N}(\varphi(x) \Rightarrow \varphi(x + 1))\}$ Nyt $0 \in A \wedge \forall y \in A(y + 1) \in A$, joten $\forall x \in N(x \in A)$. Toisaalta myös $A \subseteq \mathbb{N}$, joten $A = \mathbb{N}$ ja siis $\forall x(x \in \mathbb{N} \Leftrightarrow x \in A)$ ja $x \in A \Longrightarrow \varphi(x)$, joista yhdessä saadaan $\forall x \in \mathbb{N}(\varphi(x))\ \square$.

Yksikäsitteiseen joukkoon $\mathbb{N}$ kuuluminen voidaan ilmaista vain päättymättömänä algoritmina. Vaikka algoritmi $x \in \mathbb{N} \Longleftrightarrow x + 1 \in \mathbb{N}$ on hyvinkin lyhyt niin se ei ilman lisäoletuksia pääty. Tämä tarkastelu joudutaan kuitenkin jokaisen muuttujan kohdalla ensin tekemään. Jos tämän jälkeen $\mathbb{N}$ hyväksytään joukoksi, niin muita päättymättömiä algoritmeja ei ainakaan ennen reaalilukujen muodostamista rationaaliluvuille suoritettavien laskutoimitusten raja-arvoina tarvita.

Luonnollisten lukujen joukko siis toteuttaa Peanon postulaatit. Laskutoimitukset voisimme $\mathbb{N}$:lle ottaa jo nyt; määritellään kuitenkin ensin relaation, kuvauksen ja yhtämahtavuuden käsitteet, jolloin saamme myös järjestyksen ja muut tavanomaiset lukujoukot.

Kirjoitetaan vielä kertaukseksi koko muunneltu **ZF**.

Ekstensionaalisuus **(ET)**: $\forall A \forall B(\forall x(x \in A \Leftrightarrow x \in B) \Rightarrow A = B)$.
Korvausaksiooma **(KA)**: $\forall_2 \psi \forall b(\forall w \in b \forall v \forall u(\psi(w,u) \wedge \psi(w,v) \Rightarrow u = v) \Rightarrow$
$\exists a = \{x | \ \exists y \in b(\psi(y,x))\}$, tässä kvanttorin $\forall_2$ universumina on loogisten lauseiden kokoelma.
Säännöllisyysaksiooma **(SA)**: $\forall A \neq \emptyset \exists x \in A(\forall y \in x(y \notin A))$.
Potenssijoukko **(PT)**: $\forall A \exists B = \{x \mid \forall y \in x(y \in A)\}$.
Yhdisteaksiooma **(YA)**: $\forall A \exists C = \{x \mid \exists B \in A(x \in B)\}$.
Äärettömyysaksiooma **(ÄA)**: $\exists I = \{x \mid \emptyset \in I \wedge x \cup \{x\} \in I\}$, tässä joukko määritellään rekursiivisesti päättymättömällä algoritmilla.

Jokaisesta joukosta saadaan potenssijoukko ja yhdiste ja näille määrittävä ehto. Alussa aivan samassa järjestyksessä kvanttorit ovat myös säännöllisyysaksioomassa. Sekin takaa epätyhjää joukkoa A kohden olemassaolevan joukon x. Määrittävää ehtoa aksiooma ei anna, $\varphi_x(y)$ ei ole $y \notin A$. Se kuitenkin sanoo, että jokaista epätyhjää joukkoa kohden on olemassa sen alkio.

Jokaisesta epätyhjästä joukosta siis voidaan ottaa tunnettu alkio. Jokaisen epätyhjistä joukoista koostuvan laskettavan joukon määrittävä ehto tunnetaan. Nämä yhdistämällä saadaan, että epätyhjien joukkojen muodostamasta joukosta voidaan valita yksi alkio kustakin. Tämä on merkillepantava tulos. Tässä nimittäin saatiin teoreemana laskettava *valinta-aksiooma*, jonka mukaan joukosta epätyhjiä joukkoja voidaan aina ottaa täsmälleen yksi kustakin erityisellä *valintakuvauksella*. Sille on useita ekvivalentteja muotoiluja, joista myöhemmin esitetään vähintään yhtämahtavuuden vertailullisuus. *Hyvinjärjestyvyyslauseen* mukaan taas jokainen joukko voidaan järjestää siten, että jokin alkio on pienin. Tämänkin säännöllisyysaksiooma ja laskettavuus vaikuttavat yhdessä takaavan. Valinta-aksioomaa vastustaneen **Alfred Tarskin** mukaan nimetty teoreema sanoo, että kaikilla äärettömillä joukoilla A on olemassa bijektio $A \to A \times A$. Vielä valinta-aksiooman kanssa yhtäpitävää on, että relaatiosta voidaan aina rajoittaa samalla määrittelyjoukolla varustettu kuvaus.

Nämä kaikki siis edellyttivät laskettavuutta, määriteltävyys ei riitä.

Otetaan seuraavaksi lisää joukko-opillisia perustyökaluja käyttöön. Pykälissä **3.1-3.4** esitetään melko nopeasti joltinenkin määrä peruskurssitason määritelmiä ja teoreemoja ilman suurempia pohdiskeluja triviaalit todistukset sivuuttaen.

3 Relaatiot ja kuvaukset

3.1 Relaatio

Relaation joukko-opillinen määritelmä ei ehkä aivan vastaa intuitiivista käsitystä. Se palautuu suoraan järjestettyyn pariin.

Määritelmä 3.1.1: Joukko R on *relaatio*, jos
$\forall x \in R(\exists A \wedge \exists B(x =< a, b > \wedge a \in A \wedge b \in B))$ eli jos sen kaikki alkiot ovat järjestettyjä pareja.

Tässä esityksessä iso kirjain R (ei pieni r saati reaalilukuja tarkoittava $\mathbb{R}$) mahdollisine indekseineen tarkoittaa aina relaatiota; esimerkiksi merkinnästä $x = R$ seuraa, että x on relaatio ja merkinnästä $\exists R_x \varphi$ seuraa, että on olemassa ehdon φ toteuttava relaatio. Muutkin oliot voivat toki olla relaatioita, mutteivät välttämättä.

Jos $< x, y > \in R$, merkitään xRy tai $R < x, y >$.

Määritelmä 3.1.2: Relaation R *määrittelyjoukko* $Dom(R) = \{x \mid (\exists y)xRy\}$.

Määritelmä 3.1.3: Relaation R *arvojoukko* $Rng(R) = \{y \mid (\exists x)xRy\}$.

Suoraan määritelmistä saadaan tyhjälle joukolle

Teoreema 3.1.4: **(i)** $\emptyset$ on relaatio ja $Dom(\emptyset) = Rng(\emptyset) = \emptyset$ mutta **(ii)**
$\nexists R \neq \emptyset(\emptyset = Dom(R) \vee \emptyset = Rng(R))$ $\square$.

Seuraavien nimitysten käyttöönotto veisi kohtuuttomasti tilaa jos kullakin olisi numeroitu määritelmänsä.

Jos $A = Dom(R)$ ja $B = Rng(R)$, niin sanotaan, että joukkojen A ja B *välillä* on relaatio R eli R on joukkojen A ja B *välinen*. Jos $A = Dom(R) = Rng(R)$, niin sanotaan, että *joukossa* A on relaatio R eli R on *joukon* A relaatio. Epätyhjien joukkojen A ja B välinen *täysi relaatio* on **2.7.5** nojalla aina muodostettavissa oleva joukko $A \times B = \{< x, y > |\ x \in A \wedge y \in B\}$. Sijoittamalla edelliseen $B = A$ saadaan epätyhjän joukon A täysi relaatio $\{< x, y > |\ x \in A \wedge y \in A\}$, josta **OA**:lla ehtona $\varphi(z) \Leftrightarrow (z =< u, v > \wedge u = v)$ saadaan tulos $\exists C = \{< x, x > |\ x \in A\}$. Tällainen C on joukon A *identtinen relaatio*, merkitään R^0_A. Määritellään vielä $\emptyset$ itsensä sekä täydeksi että identtiseksi relaatioksi.

Kahden epätyhjän joukon välisen täyden relaation olemassaolosta seuraa

Teoreema 3.1.5: $\forall A \forall B(A \neq \emptyset \neq B) \exists R(Dom(R) = A \wedge Rng(R) = B)$ □.

Joukkojen A ja B välillä on siis relaatio täsmälleen silloin kun $A = \emptyset \Leftrightarrow B = \emptyset$.

3.2 Relaation ominaisuuksia

Määritelmä 3.2.1: $R^{-1} = \{< y, x > |< x, y > \in R\}$. Tällöin sanotaan, että R^{-1} on R:n *käänteisrelaatio*.

Heti nähdään, että triviaalisti $\emptyset^{-1} = \emptyset$; samoin selvästi on voimassa

Teoreema 3.2.2: $(\forall R)(R^{-1})^{-1} = R$ □.

Lisäksi suoraan määritelmistä **3.1.2** ja **3.1.3** saadaan

Teoreema 3.2.3: $(\forall R) Dom(R^{-1}) = Rng(R)$ ja $Rng(R^{-1}) = Dom(R)$ □.

Määritelmä 3.2.4: $R_1 \circ R_2 = \{< x, y > |\ \exists z(< x, z > \in R_1 \wedge < z, y > \in R_2)\}$. Tällöin sanotaan, että $R_1 \circ R_2$ on R_1:n ja R_2:n *yhdistetty relaatio*.

Seuraavat lauseet ovat voimassa; niiden todistukset seuraavat suoraan määritelmistä ja sivuutetaan tässä:

Teoreema 3.2.5: $(\forall R_1 \forall R_2) R_1 \circ R_2 = \emptyset \Leftrightarrow Rng(R_1) \cap Dom(R_2) = \emptyset$ □,

Teoreema 3.2.6:
$(\forall R_1 \forall R_2)(Dom(R_1 \circ R_2) \subseteq Dom(R_1)) \wedge (Rng(R_1 \circ R_2) \subseteq Rng(R_2))\,\square$,

Teoreema 3.2.7: $(\forall R_1 \forall R_2 \forall R_3)(R_1 \circ R_2) \circ R_3 = R_1 \circ (R_2 \circ R_3)\,\square$; voidaan siis merkitä$R_1 \circ R_2 \circ R_3$.

Oletetaan seuraavissa määritelmissä, että R on joukossa A määritelty relaatio.

Määritelmä 3.2.8: R on *refleksiivinen* A:ssa jos $(\forall x \in A)xRx$.

Määritelmä 3.2.9: R on *irrefleksiivinen*A:ssa jos $(\forall x \in A)\neg xRx$.

Määritelmä 3.2.10: R on *symmetrinen* A:ssa jos $(\forall x \in A \forall y \in A)xRy \Leftrightarrow yRx$.

Määritelmä 3.2.11: R on *antisymmetrinen* A:ssa jos
$(\forall x \in A \forall y \in A)xRy \wedge yRx \Rightarrow x = y$.

Määritelmä 3.2.12: R on *transitiivinen* A:ssa jos
$(\forall x \in A \forall y \in A \forall z \in A)xRy \wedge yRz \Rightarrow xRz$.

Määritelmä 3.2.13: R on *vertailullinen* A:ssa jos $(\forall x \in A \forall y \in A)x \neq y \Rightarrow xRy \vee yRx$.

Näiden yleisesti tunnetut ominaisuudet ja seuraukset oletetaan tutuiksi, eikä niihin paneuduta tässä tarkemmin.

Määritelmä 3.2.14: R on *ekvivalenssirelaatio* joukossa A jos se on refleksiivinen, symmetrinen ja transitiivinen. Jos joukkojen A ja B välillä on ekvivalenssirelaatio, merkitään $A \sim B$. Sanotaan myös, että A ja B kuuluvat samaan *ekvivalenssiluokkaan.*

Määritelmä 3.2.15: R on A:n *osittainen järjestys* jos se on siinä refleksiivinen, antisymmetrinen ja transitiivinen.

Määritelmä 3.2.16: R on A:n *aito osittainen järjestys* jos se on siinä irrefleksiivinen, antisymmetrinen ja transitiivinen.

Määritelmä 3.2.17: R on A:n *järjestys* jos se on siinä refleksiivinen, antisymmetrinen, transitiivinen ja vertailullinen.

Määritelmä 3.2.18: R on A:n *aito järjestys* jos se on siinä irrefleksiivinen, antisymmetrinen, transitiivinen ja vertailullinen.

Käytetään myös sanontoja R järjestää A:n osittain, R järjestää A:n aidosti osittain, R järjestää A:n ja R järjestää A:n aidosti. Järjestyksien käsitteet ovat hyödyllisiä tuonnempana.

3.3 Kuvaus

Myös seuraava on relaation ominaisuus, mutta se on niin tärkeä, että sille on syytä omistaa oma lukunsa. Tätä on jopa käytetty joukon sijaan perusmuuttujana joukko-opin aksiomatisointia luotaessa. Tässä se kuitenkin on määritelty relaation ominaisuutena, minkä unohtaminen voi johtaa kehäpäätelmiin.

Määritelmä 3.3.1: Relaatio R on *kuvaus* eli *funktio*, jos $\forall x \forall y \forall z(< x, y > \in R \wedge < x, z > \in R) \Rightarrow y = z$.

Tässä esityksessä pienet kirjaimet f ja g mahdollisine indekseineen tarkoittavat aina kuvauksia. Jos $Dom(f) = A$ ja $Rng(f) \subseteq B$ ja
$\forall x \in A \forall y \in B \forall z \in B(xfy \wedge xfz \Rightarrow y = z)$, niin sanotaan että f on kuvaus jouko*lta* A jouko*lle* B, merkitään $f : A \to B$. Merkitään myös $y = f(x)$, jos $< x, y > \in f$. Kuvausta $f : A \to A$, $\forall x(f(x) = x)$ sanotaan *identtiseksi kuvaukseksi* jouko*lla* A, merkitään f_A^0. Myös $\emptyset$ on triviaalisti kuvaus. Jos $f : A \to B$, $C \subseteq A$ ja $D \subseteq B$, niin merkitään vielä $f[C] = \{f(x) \mid x \in C\}$, joukon C *kuva* kuvauksessa f ja $f^{(-1)}[D] = \{x \mid f(x) \in D\}$, joukon D *alkukuva* kuvauksessa f. Hakasulkuja on käytettävä, sillä on täysin mahdollista, että sekä $C \in A$ että $C \subseteq A$ ja $f(C) \neq f[C]$. Indeksin -1 ympärillä on sulut erottamassa sen pian määriteltävästä käänteiskuvauksesta; merkintä $f^{-1}[D]$ tarkoittaa joukon D kuvaa kuvauksessa f^{-1}, jota ei useinkaan ole edes määritelty, kun taas alkukuva aina on.

Määritelmä 3.3.2: Kuvaus f on *injektio* $A \to B$ jos $\forall x \in A \forall y \in A(f(x) = f(y) \Rightarrow x = y)$.

Määritelmä 3.3.3: Kuvaus f on *surjektio* $A \to B$ jos $\forall y \in B(\exists x \in A(y = f(x)))$ eli $Rng(f) = B$.

Määritelmä 3.3.4: Kuvaus f on *bijektio* $A \to B$ jos se on sekä injektio$A \to B$ että surjektio $A \to B$.

Relaatioita vastaavasti määritellään

Määritelmä 3.3.5: Kuvausten f ja g *yhdistetty kuvaus*
$f \circ g = \{< x, y > | \ \exists z(< x, z > \in f \wedge < z, y > \in g)\}$. Jos f on kuvaus $A \to B$ ja g kuvaus $C \to D$, niin $f \circ g$ on kuvaus $\{x \in A \mid f(x) \in C\} \to D$.

Teoreema 3.3.6: $\forall x \in Dom(f \circ g)(f \circ g(x) = g(f(x)))$.

Todistus: Valitaan mielivaltainen $x \in Dom(f \circ g)$, jolloin
$x \in Dom(f) \wedge f(x) \in Dom(g)$. Nyt $y = f \circ g(x) \Longleftrightarrow < x, y > \in f \circ g \Longleftrightarrow \exists z(< x, z > \in f \wedge < z, y > \in g) \Longleftrightarrow \exists z(z = f(x) \wedge y = g(z)) \Longleftrightarrow y = g(f(x))$ $\square$.

Yhdistetty kuvaus noudattaa liitäntälakia, tämän todistus on vastaava kuin relaatioilla.

Teoreema 3.3.7: Jos f ja g ovat injektioita, niin myös $f \circ g$ on injektio.

Todistus: Valitaan mielivaltaiset injektiot f ja g, muodostetaan niistä yhdistetty kuvaus $f \circ g$ ja valitaan joukosta $Dom(f \circ g)$ mielivaltaiset x ja y siten, että $f \circ g(x) = f \circ g(y)$. Siis **3.3.6** mukaan $g(f(x)) = g(f(y))$, joten **3.3.2** mukaan koska g on injektio, niin $f(x) = f(y)$ ja koska f on injektio, niin $x = y$. Siis $\forall x \forall y(f \circ g(x) = f \circ g(y)) \Rightarrow x = y$ □.

Käänteiskuvaus on määritelty täsmälleen injektioille:

Teoreema 3.3.8: Kuvauksen $f : A \to B$ käänteisrelaatio f^{-1} on kuvaus $Rng(f) \to A$ joss f on epätyhjä injektio $A \to B$.

Todistus: Valitaan mielivaltainen kuvaus $f : A \to B$, jonka käänteisrelaatio f^{-1} on kuvaus $Rng(f) \to A$. Selvästi $f \neq \emptyset$.

Valitaan nyt mielivaltaiset $x \in A$ ja $y \in A$, joilla $f(x) = f(y)$. Koska f^{-1} on kuvaus $Rng(f) \to A$, niin $Dom(f^{-1}) = Rng(f)$. Koska $f(x) = f(y) \in Rng(f) = Dom(f^{-1})$ niin $f^{-1}(f(x)) = f^{-1}(f(y))$, mistä **3.2.2** perusteella seuraa $x = y$. Siis f on injektio.

Oletetaan nyt, että f on epätyhjä injektio $A \to B$. Siis $Rng(f) \neq \emptyset$. Teoreeman **3.2.3** mukaan $Rng(f^{-1}) = Dom(f)$ ja $Dom(f^{-1}) = Rng(f)$. Koska f on kuvaus joukolta A, niin $Dom(f) = A$. Siis $Dom(f^{-1}) = Rng(f^{-1})$ ja $Rng(f^{-1}) = A$. Valitaan nyt mielivaltainen $x \in Rng(f)$ ja mielivaltaiset $y \in A$ ja $z \in A$, joilla pätee $xf^{-1}y$ ja $xf^{-1}z$ eli $yfx \wedge zfx \iff f(y) = x \wedge f(z) = x \iff f(y) = f(z)$. Koska f on injektio, niin tästä seuraa että $y = z$, joten $\forall x \in Rng(f) \forall y \in A \forall z \in A(xf^{-1}y \wedge xf^{-1}z \Rightarrow y = z)$, joten f^{-1} on kuvaus. Koska jo aiemmin todettiin, että $Dom(f^{-1}) = Rng(f)$ ja $Rng(f^{-1}) = A \subseteq A$, niin kyseessä on kuvaus $Rng(f) \to A$ □.

Määritelmä 3.3.9: Jos f on injektio $A \to B$, niin sen käänteisrelaatiota sanotaan f:n *käänteiskuvaukseksi* $f^{-1} : Rng(f) \to A$. Käänteiskuvaus on surjektio B:n osajoukolta $Rng(f) \to A$.

Teoreema 3.3.10: Kuvauksen $f : A \to B$ käänteiskuvaus on kuvaus $B \to A$ joss f on bijektio $A \to B$.

Todistus: Valitaan mielivaltainen kuvaus $f : A \to B$, jonka käänteiskuvaus on kuvaus $B \to A$. Siis $Dom(f^{-1}) = B$ ja teoreeman **3.2.3** mukaan $Dom(f^{-1}) = Rng(f)$, joten $Rng(f) = B$, joten f on surjektio $A \to B$. Tästä yhdessä edellisen teoreeman kanssa seuraa, että f on bijektio.

Oletetaan nyt, että f on bijektio $A \to B$. Teoreeman **3.2.3** mukaan $Rng(f^{-1}) = Dom(f)$ ja $Dom(f^{-1}) = Rng(f)$. Koska f on kuvaus joukolta A, niin $Dom(f) = A$ ja koska f on surjektio joukolle B, niin $Rng(f) = B$. Siis $Dom(f^{-1}) = B$ ja $Rng(f^{-1}) = A$. Tästä yhdessä edellisen teoreeman kanssa seuraa, että f^{-1} on kuvaus $B \to A$ □.

Teoreema 3.3.11: Jos f on epätyhjä injektio $A \to B$, niin $f \circ f^{-1} = f_A^0$.

Todistus: Koska f on kuvaus $A \to B$ ja f^{-1} määritelmän **3.3.8** perusteella kuvaus $Rng(f) \to A$, niin $f \circ f^{-1}$ on määritelmän **3.3.5** nojalla kuvaus $\{x \in A \mid f(x) \in Rng(f)\} \to A$ eli $A \to A$. Toisaalta **3.3.5** mukaan $f \circ f^{-1} = \{< x, y > | \exists z(< x, z > \in f \wedge < z, y > \in f^{-1})\} = \{< x, y > | \exists z(< x, z > \in f \wedge < y, z > \in f)\} = \{< x, y > | \exists z(z = f(x) \wedge z = f(y))\} = \{< x, y > | \exists z(f(x) = f(y))\}$. Koska f on injektio joukolta A, saadaan tästä $f \circ f^{-1} = \{< x, y > | x = y \wedge x \in A\} = f_A^0$ □.

Teoreema 3.3.12: Jos $A \subseteq B$, niin on olemassa injektio $A \to B$.

Todistus: Koska $\forall x \in A(x \in B)$, niin kuvaus $f : A \to B$, $f(x) = x$ on vaadittava injektio □.

Teoreema 3.3.13: Jos $\emptyset \neq A \subseteq B$, niin on olemassa surjektio $B \to A$.

Todistus: Koska $A \neq \emptyset$, voidaan valita $y \in A$. Valitaan tällainen y, minkä jälkeen kuvaus $g : B \to A$. $\begin{cases} g(x) = x, & x \in A \\ g(x) = y, & x \notin A \end{cases}$ on vaadittava surjektio □.

4 Joukkojen mahtavuus

4.1 Yhtämahtavuus ja enintään yhtämahtavuus

Joukkojen kokoja voidaan jossain erikoistapauksissa vertailla jollain niiden alkioiden ominaisuudella, mutta vakiintunut suuruusjärjestys on alkioiden määrä. Tämä mitataan tavalla, josta käytetään nimitystä *mahtavuus*. Joukkojen yhtämahtavuus ja enintään yhtämahtavuus määritellään kuvausten avulla.

Määritelmä 4.1.1: Joukot A ja B ovat *yhtämahtavat* jos on olemassa bijektio $A \to B$. Käytetään merkintää $A \cong B$.

Identtinen kuvaus on bijektio, joten yhtämahtavuus on refleksiivinen. Bijektion käänteiskuvaus on bijektio, joten yhtämahtavuus on symmetrinen. Kahdesta bijektiosta muodostettu yhdistetty kuvaus on bijektio, joten yhtämahtavuus on transitiivinen. Saadaan siis

Teoreema 4.1.2: $\forall A(A \cong A)\,\square$,

Teoreema 4.1.3 $\forall A \forall B(A \cong B \Leftrightarrow B \cong A)\,\square$ ja

Teoreema 4.1.4 $\forall A \forall B \forall C(A \cong B \wedge B \cong C) \Rightarrow A \cong C\,\square$.

Määritelmä 4.1.5: Joukko A on *äärellinen*, jos $\exists n \in \mathbb{N}(A \cong n)$. Jos joukko ei ole äärellinen niin se on *ääretön*.

Yhtämahtavuutta merkitäänkin usein samoin kuin ekvivalenssirelaatiota. Se ei kuitenkaan ole relaatio, koska $\{< A, B > | A \cong B\}$ ei ole joukko vaan aito luokka. Joka tapauksessa relaation käsitteen voi yleistää aidoille luokille aivan mielekkäästi ainakin tässä tapauksessa [Levy]s.33. Voidaan puhua *ekvivalenssiluokista* käytännössä samoin kuin relaation yhteydessä.

Yleensä joukkoihin liitetään *kardinaaliluku*, joka on yhtämahtavilla joukoilla sama. Äärellisillä joukoilla kardinaaliluku tarkoittaa triviaalisti joukon alkioiden lukumäärää. Vasta äärettömillä joukoilla kardinaaliluvun käsiteen määrittelystä tulee kunnollista tiedettä: äärettömät kardinaalit ovat aina *rajaordinaaleja*; etenkin Suppesin kirjassa oleelliset *ordinaalit* ovat äärellisillä joukoilla sama kuin kardinaali, äärettömillä ne ovat huomattavasti kardinaaleja tiheämmässä ja riippuvat miten monella eri tavalla joukko voidaan hyvinjärjestää.

Määritelmä 4.1.6: Joukko A on *enintään yhtämahtava* kuin joukko B jos on olemassa joukko C siten, että $A \cong C \subseteq B$. Tällöin merkitään $A \preceq B$. Käytetään myös luonnollista sanontaa B on *vähintään yhtämahtava* kuin A. Jos $A \preceq B \wedge A \ncong B$ niin sanotaan, että B on *mahtavampi kuin* A, sanaa aito ei tässä tarvita.

Teoreema 4.1.7: Kaikilla joukoilla A ja B pätee $A \preceq B$ jos ja vain jos on olemassa injektio $A \to B$.

Todistus: Jos $A \preceq B$, niin $(\exists C)A \cong C \subseteq B$. Siis joukolta A on määritelmän **4.1.1** mukaan bijektio, eli siis injektio, joukolle C, jolta on edelleen teoreeman **3.3.12** perusteella injektio joukolle B. Siis teoreeman **3.3.7** nojalla joukolta A on injektio joukolle B. Jos taas f on injektio $A \to B$, niin f on bijektio $A \to Rng(A) \subseteq B$, eli $A \cong Rng(A) \subseteq B$ $\square$.

Edellisestä ja teoreemasta **3.3.12** saadaan

Teoreema 4.1.8: $\forall A \forall B(A \subseteq B) \Rightarrow A \preceq B$ $\square$.

Relaatio$\preceq$ on refleksiivinen:

Teoreema 4.1.9: $\forall A(A \preceq A)$.

Todistus: $\forall A(A \cong A \subseteq A)$ $\square$.

Relaatio$\preceq$ on transitiivinen:

Teoreema 4.1.10 $\forall A \forall B \forall C(A \preceq B \wedge B \preceq C) \Rightarrow A \preceq C$.

Todistus: Valitaan mielivaltaiset joukot A, B ja C siten, että $A \preceq B \wedge B \preceq C$. Tällöin teoreeman **4.1.7** mukaan on olemassa injektiot $f : A \to B$ ja $g : B \to C$. Näiden yhdistetty kuvaus $f \circ g$ on määritelmän **3.3.5** ja teoreeman **3.3.7** mukaan injektio$\{x \in A \mid f(x) \in B\} \to C$. Koska $\forall x \in A(f(x) \in B)$, niin $f \circ g$ on siis injektio $A \to C$, joten **4.1.7** mukaan $A \preceq C$ □.

Helposti saadaan määritelmän **4.1.6** ja teoreeman **4.1.4** perusteella

Teoreema 4.1.11 $\forall A \forall B(A \cong B) \Rightarrow A \preceq B \wedge B \preceq A$.

Todistus: $\forall A \forall B(A \cong B) \Longrightarrow (A \cong B \subseteq B) \wedge (B \cong A \subseteq A)$ □.

Viimeinen teoreema toiseen suuntaan, eli antisymmetrisyyden takaava tulos $A \preceq B \wedge B \preceq A \Longrightarrow A \cong B$ tuntuu triviaalilta, mutta on yllättävän hankala todistaa. Todistetaan se seuraavaksi, mutta todetaan ensin että järjestyksen (jos siis yleistetään järjestys aidoille luokille) edellyttämä vertailullisuus eli $(\forall A \forall B) A \preceq B \vee B \preceq A$, mikä sekin vaikuttaa itsestäänselvältä, on mahdotonta todistaa äärettömille joukoille ilman valinta-aksioomaa; itse asiassa se on ekvivalentti valinta-aksiooman kanssa. Se onkin selvästi samankaltainen kuin hyvinjärjestyvyyslause.

4.2 Schröderin- Bernsteinin teoreema

Tästä teoreemasta käytetään myös nimeä Cantorin-Schröderin-Bernsteinin teoreema, sillä **Georg Cantor** todisti jo aiemmin, että teoreema pätee **ZFC**:ssä. Tässä esityksessä valinta-aksiooman käyttöön suhtaudutaan vähintäänkin kriittisesti ja joka tapauksessa on arvokas tulos, että teoreema ei sitä vaadi.

Teoreema 4.2.1: (*Schröderin-Bernsteinin teoreema*) Jos $A \preceq B \wedge B \preceq A$, niin $A \cong B$.

Todistus: Koska $A \preceq B$, niin voidaan **4.1.6** mukaan määritellä injektio $f : A \to B$ ja siis bijektio $f : A \to B_1$, $B_1 = Rng(f) \subseteq B$

ja koska $B \preceq A$, voidaan vastaavasti määritellä bijektio $g : B \to A_1 \subseteq A$.

Osoittaaksemme joukot A ja B yhtämahtaviksi riittää löytää joukko

$K \subseteq A \wedge g[B \setminus f[K]] = A \setminus K$,

jolloin kuvaus g^{-1}on siis määritelty joukossa $A \setminus K$ ja

(1) $g^{-1}[A \setminus K] = B \setminus f[K]$.

Silloin kuvaus $h(x) = \begin{cases} f(x); & x \in K \\ g^{-1}(x); & x \in A \setminus K \end{cases}$ on bijektio $A \to B$,

sillä kuvauksen h lähtöjoukko on $K \cup (A \setminus K) = A$ ja

maalijoukko on **(1)** perusteella $f[K] \cup (g^{-1}[A \setminus K]) = f[K] \cup B \setminus f[K] = B$.

Määritellään nyt joukko

$D = \{C \subseteq A \mid g[B \setminus f[C]] \subseteq A \setminus C\}$,

ja osoitetaan, että $\bigcup D$ on etsitty K.

Tässä todistuksessa olennainen on joukkojen laskusäännöistä teoreema

2.5.5: $(\forall Z \forall X \forall Y)(X \subseteq Z \wedge Y \subseteq Z) \Longrightarrow (X \subseteq Z \setminus Y \Leftrightarrow Y \subseteq Z \setminus X)$,

joka tuli jo esitettyä aiemmin mutta selkeyden vuoksi kirjoitetaan se nyt tähän uudelleen.

Joukon D määritelmästä seuraa **2.5.5** mukaan, että

(2) $C \in D \Leftrightarrow C \subseteq A \setminus g[B \setminus f[C]]$.

Nyt jos $C_1, C_2 \subseteq A \wedge C_1 \subseteq C_2$, niin $f([C_1] \subseteq f[C_2]$, ja siis **2.5.5** mukaan $B \setminus f[C_2] \subseteq B \setminus f[C_1]$, joten $g[B \setminus f[C_2]] \subseteq g[B \setminus f[C_1]]$ josta taas **2.5.5** mukaan saadaan $A \setminus g[B \setminus f[C_1]] \subseteq A \setminus g[B \setminus f[C_2]]$. On siis voimassa

(3) $(\forall C_1 \forall C_2)(C_1 \subseteq C_2 \subseteq A) \Rightarrow A \setminus g[B \setminus f[C_1]] \subseteq A \setminus g[B \setminus f[C_2]]$

Koska $(\forall C \in D)C \subseteq \bigcup D \subseteq A$, niin voidaan sijoittaa kaavaan **(3)** $C_1 = C$ ja $C_2 = \bigcup D$, jolloin saadaan $A \setminus g[B \setminus f[C]] \subseteq A \setminus g[B \setminus f[\bigcup D]]$, ja koska $C \in D$, niin tästä **(2)** mukaan seuraa

(4) $C \subseteq A \setminus g[B \setminus f[\bigcup D]]$.

Koska **(4)** pätee kaikilla joukon D alkioilla C, niin yleisen yhdisteen määritelmän mukaan on voimassa

(5) $\bigcup D \subseteq A \setminus g[B \setminus f[\bigcup D]]$.

Määritellään nyt joukko

$F = A \setminus g[B \setminus f[\bigcup D]]$.

Siis **(5)** mukaan $\bigcup D \subseteq F \subseteq A$, joten **(3)** mukaan

$A \setminus g[B \setminus f[\bigcup D]] \subseteq A \setminus g[B \setminus f[F]]$ eli $F \subseteq A \setminus g[B \setminus f[F]]$, siis **(2)** mukaan $F \in D$, joten $F \subseteq \bigcup D$, mikä siis on

(6) $A \setminus g[B \setminus f[\bigcup D]] \subseteq \bigcup D$.

Tuloksista **(5)** ja **(6)** seuraa, että $A \setminus g[B \setminus f[\bigcup D]] = \bigcup D$ eli **2.5.5** mukaan $g[B \setminus f]\bigcup D]] = A \setminus \bigcup D$, ja koska joukon D määritelmästä seuraa, että $\bigcup D \subseteq A$, niin $\bigcup D$ todella täyttää joukolle K asetetut ehdot $\square$.

Yhdessä teoreeman **4.1.6** kanssa tästä seuraa suoraan

Teoreema 4.2.3: Jos on olemassa injektiot $A \to B$ ja $B \to A$, niin $A \cong B$ $\square$.

5 Äärettömät lukukokoelmat

Joukko-opin aksiomatisoinnin perusteluna pidetään yleensä eri lukujoukkojen konstruointia. Palataan nyt luvussa **2.7** määriteltyihin luonnollisiin lukuihin.

5.1 Luonnollisten lukujen laskutoimitukset

Tässä kappaleessa $x, y, z, k, n \in \mathbb{N}$. Postulaatin **P5** perusteella induktiotodistus on hyväksyttävä todistusmenetelmä. Mikään tämän kappaleen määritelmistä ja lauseista ei riipu siitä miten käsitteet 0 ja +1 on joukko-opillisesti määritelty, ainoastaan Peanon postulaateista.

Yhteenlasku määritellään rekursiivisesti; tämä ei johda pysähtymättömiin algoritmeihin koska induktioperiaate on nyt käytössä:

(N4) $x + 0 = x$.

(N5) $x + (y + 1) = (x + y) + 1$.

Teoreema 5.1.1 (yhteenlaskun liitännäisyys):$\forall x \forall y \forall z (x + y) + z = x + (y + z)$.

Todistus: Valitaan mielivaltaiset x ja y. Nyt **N4** perusteella

(a1) $(x + y) + 0 = x + y = x + (y + 0)$.

Oletetaan sitten, että pätee

(b1) $(x + y) + k = x + (y + k)$.

Nyt **N5** ja **b1** avulla saadaan

(c1)
$(x+y)+(k+1) = ((x+y)+k)+1 = (x+(y+k))+1 = x+((y+k)+1) = x+(y+(k+1))$.

Induktioperiaatteen nojalla tuloksista **a1** ja (**b1**⇒**c1**) seuraa teoreema □.

Teoreema 5.1.2 (yhteenlaskun vaihdannaisuus):$\forall x \forall y(x + y) = (y + x)$.

Todistus: Triviaalitapaukset täytyy käsitellä ensin erikseen.

Lemma 5.1.2.1: $\forall k(0 + k = k)$.

Todistus: Määritelmän **N4** mukaan

(a21) $0 + 0 = 0$.

Oletetaan nyt, että

(b21) $0 + k = k$.

Tällöin määritelmien **N5** ja **N4** sekä induktio-oletuksen **b21** mukaan myös

(c21) $0 + (k + 1) = (0 + k) + 1 = k + 1 = k + 1$.

Induktioperiaatteen nojalla lemma pätee.

Lemma 5.1.2.2: $\forall n(1 + n = n + 1)$.

Todistus: Määritelmän **N4** ja edellisen lemman perusteella

(a22) $1 + 0 = 1 = 0 + 1$.

Oletetaan sitten, että pätee

(b22) $1 + n = n + 1$,

jolloin määritelmän **N5** ja induktio-oletuksen **b22** johdosta pätee myös

(c22) $1 + (n + 1) = (1 + n) + 1 = (n + 1) + 1$.

Induktioperiaatteen nojalla lemma pätee □.

Valitaan nyt mielivaltainen x. Määritelmän **N4** ja lemman **5.1.2.1** mukaan

(a2) $x + 0 = x = 0 + x$.

Oletetaan nyt

(b2) $x + k = k + x$,

jolloin määritelmän **N5**, induktio-oletuksen **b3**, lemman **5.1.2.2** ja teoreeman **5.1.1** perusteella

(c2) $x + (k + 1) = (x + k) + 1 = (k + x) + 1 = k + (x + 1) = k + (1 + x) = (k + 1) + x$.

Induktioperiaatteen nojalla tuloksista **a2** ja (**b2**⇒**c2**) seuraa teoreema □.

Teoreema 5.1.3 (nollan yksikäsitteisyys): $\forall x(\forall y(x + y) = y \Rightarrow x = 0)$.

Todistus: Valitaan mielivaltainen x. Määritelmän **N4** perusteella

(a3) $x + 0 = 0 \Rightarrow x = 0$.

Oletetaan sitten, että

(b3) $x + k = k \Rightarrow x = 0$.

Nyt määritelmän **N5**, postulaatin **P4** ja induktio-oletuksen **b3** mukaan

(c3) $x + (k + 1) = k + 1 \Rightarrow (x + k) + 1 = k + 1 \Rightarrow x + k = k \Rightarrow x = 0$.

Induktioperiaatteen nojalla tuloksista **a3** ja (**b3**⇒**c3**) seuraa teoreema □.

Myös *kertolasku* määritellään rekursiivisesti:

(N6) $x \cdot 0 = 0$.

(N7) $x \cdot (y + 1) = (x \cdot y) + x$.

Teoreema 5.1.4 (osittelulaki): $\forall x \forall y \forall z (z \cdot (x + y)) = (z \cdot x) + (z \cdot y)$.

Todistus: Valitaan mielivaltaiset x ja z. Määritelmien **N4** ja **N6** nojalla

(a4) $z \cdot (x + 0) = z \cdot x = (z \cdot x) + 0 = (z \cdot x) + (z \cdot 0)$.

Tehdään induktio-oletus

(b4) $z \cdot (x + k) = (z \cdot x) + (z \cdot k)$.

Siitä seuraa yhdessä määritelmän **N7** ja teoreeman **5.1.1** kanssa

(c4)
$z \cdot ((x+(k+1)) = z \cdot ((x+k)+1) = (z \cdot (x+k)) + z = (z \cdot x) + (z \cdot k) + z = (z \cdot x) + z \cdot (k+1)$.

Induktioperiaatteen nojalla tuloksista **a4** ja (**b4**⇒**c4**) seuraa teoreema □.

Teoreema 5.1.5 (kertolaskun liitännäisyys):$\forall x \forall y \forall z (x \cdot y) \cdot z = x \cdot (y \cdot z)$.

Todistus: Valitaan mielivaltaiset x ja y. Nyt **N6** perusteella

(a5) $(x \cdot y) \cdot 0 = 0 = x \cdot 0 = x \cdot (y \cdot 0)$.

Oletetaan sitten, että pätee

(b5) $(x \cdot y) \cdot k = x \cdot (y \cdot k)$.

Nyt saadaan määritelmän **N7**, induktio-oletuksen **b4** ja osittelulain **5.1.4** avulla

(c5)
$(x\cdot y)\cdot(k+1) = ((x\cdot y)\cdot k)+(x\cdot y) = (x\cdot(y\cdot k))+(x\cdot y) = x\cdot((y\cdot k)+y) = x\cdot(y\cdot(k+1))$.

Induktioperiaatteen nojalla tuloksista **a5** ja (**b5**⇒**c5**) seuraa teoreema □.

Teoreema 5.1.6 (kertolaskun vaihdannaisuus): $\forall x\forall y((x\cdot y) = (y\cdot x))$.

Todistus: Valitaan mielivaltainen x. Tarvitaan ensin perusaskeleelle induktiolla saatava

Lemma 5.1.6.1: $\forall k(0\cdot k = 0)$.

Todistus: Määritelmän **N6** perusteella on voimassa

(a61) $0\cdot 0 = 0$.

Oletus

(b61) $0\cdot n = 0$

johtaa teoreeman **5.1.4**, lemman **5.1.2.1**, määritelmän **N7** ja tuloksen **a61** keralla seuraukseen

(c61) $0\cdot(n+1) = (0\cdot n)+(0\cdot 1) = 0+(0\cdot(0+1)) = 0+((0\cdot 0)+0) = 0+0+0 = 0$;

tämä on induktiotodistus lemmalle □.

Edellä johdetun tuloksen **5.1.6.2** ja määritelmän **N6** perusteella siis

(a6) $x\cdot 0 = 0 = 0\cdot x$.

Oletetaan nyt, että

(b6) $x \cdot k = k \cdot x$.

Induktioaskelta varten tarvitaan taas aputulos:

Lemma 5.1.6.2: $\forall k \forall n((k+1) \cdot n = (k \cdot n) + n)$.

Todistus: Valitaan mielivaltainen k, jolloin määritelmien **N6** ja **N4** nojalla

(a62) $(k+1) \cdot 0 = 0 = 0 + 0 = (k \cdot 0) + 0$.

Olkoon nyt voimassa

(b62) $(k+1) \cdot n = (k \cdot n) + n$.

Nyt määritelmää **N7**, induktio-oletusta **b62** sekä teoreemoja **5.1.2** ja **5.1.1** soveltaen saadaan

(c62)$(k+1) \cdot (n+1) = ((k+1) \cdot n) + (k+1) = ((k \cdot n) + n) + (k+1) =$
$((k \cdot n) + k) + (n+1) = (k \cdot (n+1)) + (n+1)$.

Siis induktioperiaatteen nojalla lemma pätee □.

Määritelmästä **N7**, induktio-oletuksesta **b6** ja lemmasta **5.1.6.2** saadaan näin ollen

(c6) $x \cdot (k+1) = (x \cdot k) + x = (k \cdot x) + x = (k+1) \cdot x$.

Induktioperiaatteen nojalla tuloksista **a6** ja (**b6**⇒**c6**) seuraa teoreema □.

Yhteen- ja kertolaskut ovat siis näin määriteltyinä luonnollisilla luvuilla sekä vaihdannaisia että liitännäisiä ja tavanomainen osittelulaki on myös voimassa. Tähän tietenkin käytetyillä rekursiivisilla määritelmillä pyrittiinkin. Minkäänlaista **ZF**- tai muutakaan joukko-oppia tässä osuudessa ei tarvittu mihinkään. Paras argumentti joukko-opin käytölle luonnollisten lukujen määrittelyssä on seuraava osuus.

5.2 Luonnollisten lukujen järjestys

Tässäkin käytetyn **John von Neumann**in käyttöönottaman +1:n määritelmän ansiosta luonnolliset luvut saadaan helposti järjestettyä joukkoon kuulumisen avulla.

Järjestysrelaation vertailullisuudelle tarvitaan triviaalin tuntuinen apulause, jota vastaava tulos kuitenkin täytyy jossain vaiheessa todistaa. Olemme tässä vasta osoittamassa järjestyksen olemassoloa, eli ei mitenkään voi olla selvää että saa ottaa seuraajarelaation molemmista puolista järjestyksen säilyttäen.

Teoreema 5.2.1: $\forall k, n \in \mathbb{N}(k \in n \Rightarrow k+1 \in n+1)$.

Todistus: Induktiolla n:n suhteen. Implikaatio on triviaalisti voimassa kun $n = \emptyset$. Oletetaan nyt, että

(1) $k \in n \Rightarrow k+1 \in n+1$

ja pyritään osoittamaan että

(2) $k \in n+1 \Rightarrow k+1 \in (n+1)+1$.

Saadaan $k \in n+1 \Leftrightarrow k \in n \cup \{n\} \Leftrightarrow k \in n \vee k = n$, mistä **(1)** mukaan

$(k+1 \in n+1 \vee k = n) \Rightarrow (k+1 \in n+1 \cup \{n+1\}) \vee (k = n \wedge n+1 \in \{n+1\})$

$\Rightarrow (k+1 \in (n+1)+1) \vee (k = n \wedge n+1 \in n+1 \cup \{n+1\}) \Rightarrow (k+1 \in (n+1)+1) \vee ((k = n) \wedge n+1 \in (n+1)+1) \Rightarrow$

$(k+1 \in (n+1)+1)$, joten **(2)** on voimassa ja siten myös teoreema $\square$.

Teoreema 5.2.2: Relaatio $\in$ järjestää kokoelman $\mathbb{N}$ aidosti.

Todistus: Selvästi **SA** mukaan $\in$ on irrefleksiivinen ja antisymmetrinen. Transitiivisuus (eli aiemmin luvattu lauseen **2.4.3** yleistys!) saadaan yksinkertaisella induktiolla:

Triviaalisti on voimassa vasemmalta puoleltaan epätosi implikaatio
$x \in y \wedge y \in \emptyset \Rightarrow x \in \emptyset$.

Oletetaan nyt, että $x \in y \wedge y \in k \Rightarrow x \in k$. Tällöin

$x \in y \wedge y \in (k+1) \Leftrightarrow x \in y \wedge y \in k \cup \{k\} \Leftrightarrow x \in y \wedge (y \in k \vee y \in \{k\}) \Leftrightarrow (x \in y \wedge y \in k) \vee (x \in y \wedge y = k) \Rightarrow x \in k \Rightarrow x \in k \cup \{k\} = k+1$; päättelyketju saattaa vaikuttaa kummalliselta, joten sitä on syytä havainnollistaa olettamalla aritmetiikka tunnetuksi: jos $x < y < k+1$, niin luonnollisesti $x < y \leq k$ eli $x < k$, josta seuraa $x < k+1$.

Vertailullisuus saadaan sekin induktiolla: Selvästi $\forall n \in \mathbb{N}(\emptyset \in n)$, induktiotodistus on aivan triviaali. Oletetaan nyt, että $(\forall k \in \mathbb{N})k = n \vee k \in n \vee n \in k$. Nyt jos $k = n \vee k \in n$, niin selvästi $k \in n \cup \{n\} = n + 1$. Jos taas $n \in k$, niin lauseen **5.3.1** mukaan $n + 1 \in k + 1 = k \cup \{k\} \Leftrightarrow n + 1 \in k \vee n + 1 = k$. Siis $(\forall k \in \mathbb{N})k = n + 1 \vee k \in n + 1 \vee n + 1 \in k$. Relaatio $\in$ on siis aito järjestysrelaatio kokoelmassa $\mathbb{N}$ □.

Jos $n \in \mathbb{N} \wedge m \in n$ merkitään $m < n$. Käytetään myös merkintää $n > m$. Jos $n < m \vee n = m$ merkitään $n \leq m$ ja $m \geq n$.

Teoreema 5.2.3: $(\forall m, n \in \mathbb{N})$ **(i)** $(m < n \Leftrightarrow m \subset n)$ ja **(ii)** $(m \leq n \Leftrightarrow m \subseteq n)$.

Todistus: **(i)** Oletetaan, että $m < n$ ja valitaan mielivaltainen $x \in m$, jolloin koska $m \in n$ niin transitiivisuuden nojalla $x \in n$ ja siis $m \subset n$. Oletetaan sitten, että $m \subset n$. Siis $m \neq n$ ja $\exists k \in \mathbb{N}(k \in n \wedge k \notin m)$. Tehdään vastaoletus, jonka mukaan $m > n$. Siis $n \in m$ ja $k \in n$, mistä transitiivisuuden nojalla $k \in m$, mikä on ristiriita. Siis koska $<$ on aito järjestysrelaatio, joka irrefleksiivisyyden, antisymmetrisyyden ja vertailullisuuden johdosta noudattaa *trikotomiaa*, eli täsmälleen yksi vaihtoehdoista $m < n$, $n < m$ ja $m = n$ on aina voimassa, seuraa vastaoletuksesta johdetusta ristiriidasta että $n < m$.

Kohta **(ii)** saadaan suoraan kohdasta **(i)** kun tarkastellaan erikseen tapaukset, joissa $m = n$ □.

Tästä seuraa, että relaatio $\subseteq$ on kokoelman $\mathbb{N}$ järjestys ja $\subset$ aito järjestys.

Luonnollisten lukujen kokoelmalle $\mathbb{N}$ saadaan teoreemana johdettua kaksikin eri aitoa järjestysrelaatiota **ZF**-aksioomista lähtien, mikä lukujen määrittelemistä joukkoina selvästi puoltaa.

Esitetään tässä vielä muutama muukin joukko-opin avulla määriteltyjen lukujen antama tulos.

Teoreema 5.2.4: $\forall k \forall n(k \in n \wedge n \in \mathbb{N} \Rightarrow k \in \mathbb{N})$

Todistus induktiolla: Kun $n = 0$, niin

(3) $k \in n \wedge n \in \mathbb{N} \Rightarrow k \in \mathbb{N}$

toteutuu triviaalisti. Oletetaan nyt, että **(3)** toteutuu, kun $n = m \in \mathbb{N}$. Jos $n = m + 1$, niin $k \in m + 1 \Rightarrow k \in m \cup \{m\} \Rightarrow k \in m \vee k = m$. Siis induktio-oletuksen ja oletuksen $m \in \mathbb{N}$ nojalla molemmissa tapauksissa $k \in \mathbb{N}$, joten **(3)** pätee kaikilla $n \in \mathbb{N}$ □.

Kahden luonnollisen luvun yhdiste on niistä suurempi ja leikkaus pienempi, todistukset seuraavat suoraan edellisestä lauseesta ja joukko-opin laskusäännöistä:

Teoreema 5.2.5: $\forall n \in \mathbb{N} \forall k \leq n (n \cup k = n \wedge n \cap k = k)$ □.

Kahden luonnollisen luvun joukko-opillinen erotus taas ei triviaalitapauksia lukuunottamatta ole luku, tosin saadun joukon kardinaali ilmaisisi erotuksen. Luonnollisen luvun yleinen leikkaus on triviaalisti Ø ja yleinen yhdiste intuitiivisen käsityksen mukainen:

Teoreema 5.2.6: $\forall n \in \mathbb{N} \bigcup (n + 1) = n$.

Todistus induktiolla: Kun $n = 0 = \emptyset$, niin $\bigcup (n + 1) = \bigcup \emptyset \cup \{\emptyset\} = \bigcup \{\emptyset\} = \emptyset$.

Oletetaan nyt, että $\bigcup (k + 1) = k$. Nyt

$\bigcup ((k + 1) + 1) = \bigcup ((k + 1) \cup \{k + 1\}) = \{x \mid \exists y \in (k + 1) \cup \{k + 1\} \wedge x \in y\} =$

$\{x \mid \exists y_1 (x \in y_1 \wedge y_1 \in (k + 1)) \vee \exists y_2 (x \in y_2 \wedge y_2 = (k + 1))\} =$

$\{x \mid \exists y_1 (x \in y_1 \wedge y_1 \in (k + 1))\} \cup \{x \mid \exists y_2 (x \in y_2 \wedge y_2 = (k + 1))\} =$

$\bigcup (k + 1) \cup \{x \mid x \in (k + 1)\} = k \cup \{x \mid x \in k \cup \{k\}\} = k \cup (k \cup \{k\}) = k \cup \{k\} = k + 1$ □.

5.3 Luonnollisten lukujen kokoelman olemus

Mikään tähän asti esitetty tulos ei riipu siitä onko $\mathbb{N}$ joukko. Taustalla ovat pelkästään määritelmät

N0 $0 = \emptyset$

NS $n + 1 = n \cup \{n\}$

ja oletus, jonka mukaan on olemassa kokoelma $\mathbb{N}$, jolla postulaatit **P1**, **P2** ja **P5** ovat voimassa. Jos halutaan, että $\mathbb{N}$ on joukko, niin vaaditaan **NA**.

Se, että $\mathbb{N}$ on joukko edellyttää siis että pätee

Äärettömyysaksiooma (**ÄA**): $\exists I = \{x \mid \emptyset \in I \wedge x \cup \{x\} \in I\}$.

Oletusta, jonka mukaan $\mathbb{N}$ on joukko tarvitaan lähinnä siksi, että saadaan vertailla äärettömyyksiä. Seuraavat kaksi tulosta siitä sentään saadaan.

Ensimmäinen tulos saadaan suoraan teoreemasta **2.5.4**.

Teoreema 5.3.2: $\bigcup \mathcal{P}(\mathbb{N}) = \mathbb{N}\square$.

Luonnollisten lukujen joukko on siis potenssijoukkonsa yhdiste. Seuraavaa ei intuitio aivan suoraan anna:

Teoreema 5.3.3: $\mathbb{N} = \bigcup \mathbb{N}$.

Todistus: $k \in \mathbb{N} \iff k \in \mathbb{N} \wedge k \cup \{k\} \in \mathbb{N}) \implies \exists n = k \cup \{k\}(n \in \mathbb{N} \wedge k \in n) \iff k \in \bigcup \mathbb{N} \iff \exists m \in \mathbb{N}(k \in m) \implies k \in \mathbb{N}$ $\square$.

Luonnollisten lukujen joukko on siis itsensä yhdiste. Sinänsä oikein kaunis tulos.

Olkoon nyt sitten perinteiseen tapaan voimassa, että Peanon postulaatit toteuttava äärellisten luonnollisten lukujen ääretön kokoelma $\mathbb{N}$ on **ZF**-aksioomat toteuttava joukko, jollaisia ovat siis nyt äärellisen kaavan tai rekursiivisen ehdon määrittämät. Se noudattaa säännöllisyysaksioomaa ja vieläpä tiedetään että juuri $\emptyset$ on **SA**:n edellyttämä alkio. Jos johonkin joukkoon havaitaan kuuluvan täsmälleen kaikki luonnolliset luvut, niin **ET** nojalla se on juuri $\mathbb{N}$. Yhdiste havaittiin edellisessä teoreemassa erittäin elegantiksi.

Joukko $\mathcal{P}(\mathbb{N})$ on tärkein peruste sille, että $\mathbb{N}$ on joukko. Platonismin pyhimpiä opinkappaleita on, että äärettömien binäärijonojen ominaisuudettomasta eikä ainakaan joukkoa muodostavasta kokoelmasta kunkin jäsenen eteen 0. merkitsemällä oitis syntyvän joukon tavoin myös $\mathcal{P}(\mathbb{N})$ on *ylinumeroituva* ja siten mahdoton listata, kuten seuraavaksi koitetaan osoittaa.

Väittämä 5.3.4: *Cantorin teoreema*:$(\forall A) A \ncong \mathcal{P}(A)$.

Todistus: Selvästi teoreema pitää paikkansa, kun $A = \emptyset$. Oletetaan siis että $A \neq \emptyset$, jolloin on olemassa kuvaus $f : A \to \mathcal{P}(A)$; ainakin $f(x) = \{x\}$. Valitaan mielivaltainen sellainen ja osoitetaan, ettei se ole surjektio. Yritetään muodostaa A:lle **OT**:n avulla osajoukko seuraavalla tavalla, joka ei äärettömällä joukolla aina onnistu:

$B = \{x \in A \mid x \notin f(x)\}$

Jos B on A:n osajoukko niin se on $\mathcal{P}(A)$:n alkio eli jos f on surjektio, saataisiin $\exists c \in A(B = f(c))$. Nyt $(c \in B \Leftrightarrow c \in A \wedge c \notin f(c)) \Longleftrightarrow (c \in B \Leftrightarrow \top \wedge c \notin B)$, mikä on kontradiktio, joten teoreema pätisi jos B olisi joukko. Kuitenkin B on joukko vain, kun $x \notin f(x)$ on hyvinmääritelty kaava. Todistus ei siis mene läpi. Sen sijaan vastaesimerkki saadaan luotua

Teoreema 5.3.5: $\mathbb{N} \cong \mathcal{P}(\mathbb{N})$.

Todistus: Kirjoittamalla $\mathcal{P}(\mathbb{N}) = \{A \mid \forall x \in A(x \in \mathbb{N})\} = \{B \mid B = \{n \in \mathbb{N} \mid \varphi(n)\}\}$ saatava muoto ilmaisee, mistä potenssijoukossa on kyse. Se koostuu joukoista, joita siis pitää vastata äärellinen määrittävä kaava tai rekursiivinen ehto. Joukko $\mathcal{P}(\mathbb{N})$ koostuu siis yhtä monesta alkiosta, kuin on ehtoja $\phi(n) \Longleftrightarrow n \in \mathbb{N} \wedge \varphi(n)$. Muodostetaan ehtoja vastaamaan *Gödel-numerointi*, jolloin saadaan surjektio luonnollisilta luvuilta niiden määrämien joukkojen joukolle. Kuvaus $f(n) = \{n\}$ on puolestaan injektio, joten joukot ovat yhtämahtavat $\square$.

Siis Cantorin teoreema ei pidä yleisesti paikkaansa jos pitäydytään kaksiarvoisessa logiikassa, jolloin ei voida hyväksyä määrittelemättömiä olioita. Tässä käytetty kuvaus on teoriassa jopa laskettava, mutta ehto $x \notin f(x)$ ei ole äärellisesti määritelty, sillä mielivaltaisen moni ehdoista $\varphi(n)$ määrittelee äärettömän joukon.

Jos Cantorin teoreema pätisi, siitä seuraisi että ääretön joukko $\mathbb{N}$ on aidosti pienempi kuin sitä mahtavampi $\mathcal{P}(\mathbb{N})$. Muotoa "ääretön on aidosti pienempi kuin"- oleva väittämä olisi siis matemaattisesti todistettu apriorinen absoluuttinen totuus. Tässä tapauksessa pitäisi ilman muuta siirtyä periytyvästi äärellisiin joukkoihin ja korvata lukujoukot aidoilla luokilla.

Aidosta luokasta ei voi muodostaa potenssiluokkaa. Aito luokka ei ole kunnollinen käsite **ZF**:ssä. Sitä laajemmissa *von **N**eumannin-**B**ernaysin-**G**ödelin* ja ***M**orsen-**K**elleyn* aksiomatisoinneissa perustavin aitoja luokkia koskeva tulos on, että ne ovat kaikki yhtä mahtavia eikä mahtavampaa oliota ole. Tämä vastaa maallikon äärettömyyskäsitystä paljon paremmin kuin **ZF**:ssä käytetyt äärettömän ja *Dedekind-äärettömän* määritelmät; jälkimmäisessä edellytetään että joukko on yhtämahtava aidon osajoukkonsa kanssa. Mainittakoon vielä, että abstraktioaksioomaa ei tarvitse rajata osajoukkoihin jos sallitaan aidot luokat.

5.4 Periytyvästi äärelliset joukot

Jos rekursiiviset ehdot kielletään joukkojen määrittelevinä ehtoina, niin **ÄA** johtaa ristiriitaan ja silloin periytyvästi äärelliset joukot ovat ainoa mielekäs teoria. Silloin pitää huolehtia, että Peanon aksioomat toteuttava joukkojen kokoelma N on aito luokka. Selvästi jos yleistetään järjestysrelaatio aidolle luokalle niin $\in$ järjestää näin määritellyt *periytyvästi äärelliset joukot*; vastaavasti $\subset$ järjestää ne aidosti.

Tässä sanotaan usein virheellisesti, että otetaan aksioomaksi **ÄA**:n negaatio.

$\neg(\exists A(\emptyset \in A \wedge \forall B(B \in A \Rightarrow B \cup \{B\} \in A)) \Leftrightarrow \forall A(\emptyset \notin A \vee \exists B(B \in A \wedge B \cup \{B\} \notin A) \Leftrightarrow \forall A(\emptyset \in A \Rightarrow \exists B(B \in A \wedge B \cup \{B\} \notin A)$.

Tässä siis sanotaan, että kaikki tyhjän joukon sisältävät joukot sisältävät joukon, jonka yhdiste itsensä muodostaman joukon kanssa ei kuulu siihen. Tämän ehdon toteuttaisi mikä tahansa tyhjää joukkoa sisältämätön joukko, esimerkiksi **ÄA**:n joukosta muodostettu joukko $I \setminus \{\emptyset\}$, eli aktuaalisesti äärettömän joukon olemassaoloa tämä ei kiellä.

Toinen virheellinen menettelytapa on määritellä rekursiivisesti, että $\emptyset$ on periytyvästi äärellinen samoin kuin siitä ensin potenssijoukkoaksioomalla ja sitten muilla määritellyt joukot. Tämä on aivan turhaa, kyseiset joukot ovat äärellisiä muutenkin. Seuraava askel on sitten aksiomatisoida kaikkien periytyvästi äärellisten joukkojen kokoelma joukoksi. Tämä ei ole äärettömyysaksooman vastainen oletus, vaan äärettömyysaksiooma, jossa vain nimiä on vaihdettu.

Asetetaan aksioomaksi, että luonnolliset luvut muodostavat aidon luokan N, jolloin saadaan **NBG**:n notaatiota mukaillen

Rajallisuusaksiooma **(RA)**: $N \cong \mathcal{V} \wedge (\forall x \in N(x \cup \{x\} \in N \wedge (x = \emptyset \vee \exists y \in N(x = y \cup \{y\}))) \wedge (\emptyset \in I \wedge \forall z \in I(z \cup \{z\} \in I)) \Rightarrow x \in I))$,

missä isot kirjaimet viittaavat luokkiin, jotka siis eivät kuulu kvanttorien universumiin. Alussa esiintyvä $\mathcal{V}$ merkitsee kaikkien joukkojen kokoelmaa, joka tunnetaan aidoksi luokaksi, ja luonnolliset luvut asetetaan sen kanssa yhtämahtaviksi, jolloin nekin ovat aito luokka. Selvästi myös I on aito luokka, koska N on sen osaluokka. Koska joukot eivät saa olla aitoja luokkia ja äärettömältä joukolta on aina injektio luonnollisille luvuille niin kaikki joukot toteuttavat äärellisyyden määritelmän **4.1.5**.

6 Laajemmat lukujoukot

6.1 Kokonaisluvut

Muodostetaan nyt joukot $\mathbb{Z}$, $\mathbb{Q}$ ja $\mathbb{R}$. Näistä kaksi ensimmäistä saataisiin aivan vastaavasti aidoille luokille, tällöin ei tarvitsi erikseen osoittaa niitä yhtämahtaviksi.

Negatiiviset luvut voidaan määritellä järjestetyn parin avulla kun merkitään myös positiiviset kokonaisluvut järjestettyinä pareina. Tässä esitetyssä määritelmässä 0 on positiivinen kokonaisluku; muuten se täytyisi aina tarkastella erikseen. Tässä ei tarvitse ottaa koko ekvivalenssiluokkaa; tämän määritelmän mukaan esimerkiksi $< 7, 4 >$ ei ole kokonaisluku.

Määritelmä 6.1.1: *Negatiiviset kokonaisluvut* $\mathbb{Z}_- = \{< 0, n > | \ n \in \mathbb{N} \setminus 0\}$, *positiiviset kokonaisluvut* $\mathbb{Z}_+ = \{< n, 0 > | \ n \in \mathbb{N}\}$ ja *kokonaisluvut* $\mathbb{Z} = \mathbb{Z}_+ \cup \mathbb{Z}_-$.

Määritelmä 6.1.2 *Itseisarvo*: $\forall z \in \mathbb{Z} \mid z \mid = \begin{cases} x; & z =< x, 0 > \in \mathbb{Z}_+ \\ y; & z =< 0, y > \in \mathbb{Z}_- \end{cases}$.

Määritellään kokonaislukujen järjestys:

Määritelmä 6.1.3:$n \in \mathbb{Z}_+, k \in \mathbb{Z}_- k <_{\mathbb{Z}} n; n, k \in \mathbb{Z}_+ n <_z k \iff \mid n \mid < \mid k \mid; n, k \in \mathbb{Z}_- n <_{\mathbb{Z}} k \iff \mid n \mid > \mid k \mid$.

Todistetaan kokonaislukujen yhteenlaskua varten erotuksen eli luonnollisten lukujen ensimmäisen asteen yhtälön ratkaisun yksikäsitteisyys.

Teoreema 6.1.4: $\forall k, n \in \mathbb{N}(k < n) \Rightarrow \exists! m \in \mathbb{N}(k + m = n)$.

Todistus induktiolla: Osoitetaan ensin olemassaolo: Kun $n = 0$, on implikaatio triviaalisti tosi. Oletetaan nyt, että lause pitää paikkansa kun $n = n_0$ ja valitaan mielivaltainen $k < n_0 + 1$. Jos $k = n_0$, niin $m = 1$, jos $k < n_0$ niin induktio-oletuksen mukaan $\exists m_0 \in \mathbb{N}(n_0 + 1 = (k + m_0) + 1 = k + (m_0 + 1), (m_0 + 1) \in \mathbb{N})$.

Vielä pitää osoittaa yksikäsitteisyys, sekin todistetaan induktiolla: Yksinkertaistetaan väitettä ensin hieman: $\forall k \in \mathbb{N}(k+m=n \wedge k+x=n \Rightarrow k+m=k+x)$. Jos $m=0$, niin $\forall k \in \mathbb{N}$ jos $k+m=k+0=k=k+x$, niin teoreeman **5.1.3** nojalla $x=0$. Oletetaan nyt, että $\forall k \in \mathbb{N}(k+m=k+x \Rightarrow m=x)$.

Nyt $k+(m+1)=k+y \Rightarrow m+1=y$ pätee, jos $y=0$. Olkoon $y=z+1$, josta saadaan $k+(m+1)=k+(z+1) \Leftrightarrow (k+1)+m=(k+1)+z$, mistä seuraa, että $m=z$, sillä $k+1 \in \mathbb{N}$. Siis $m+1=z+1=y$ $\square$.

Määritelmä 6.1.5:
$(n \in \mathbb{Z}_+, k \in \mathbb{Z}_-)n +_{\mathbb{Z}} k = k +_{\mathbb{Z}} n \begin{cases} < m, 0 >, \mid k \mid + m = \mid n \mid; & \mid k \mid \leq \mid n \mid \\ < 0, m >, \mid n \mid + m = \mid k \mid; & \mid k \mid > \mid n \mid \end{cases}; (n, k \in \mathbb{Z}_+)n +_{\mathbb{Z}} k = < \mid n \mid + \mid k \mid, 0 >; (n, k \in \mathbb{Z}_-)(n +_{\mathbb{Z}} k \Leftrightarrow -(\mid n \mid + \mid k \mid)$.

Yhteenlasku on liitännäinen ja vaihdannainen; todistukset ovat triviaaleja kuten myös vaihdannaisuuden todistus vaikka määritelmästä tehtäisiin pitempi ottamalla erikseen $n \in \mathbb{Z}_-, k \in \mathbb{Z}_+$. Suoraan määritelmästä saadaan 0 yhteenlaskun neutraalialkioksi. Jokaisella kokonaisluvulla on myös yksikäsitteinen vastaluku:

Teoreema 6.1.6: $\forall n \in \mathbb{Z}(\exists!(-n)n + (-n) = 0)$.

Todistus: Valitaan mielivaltainen $n \in \mathbb{Z}$. Jos $n = < a, 0 > \in \mathbb{Z}_+$, niin $n + < 0, a > = < m, 0 >, \mid a \mid + m = \mid a \mid = < 0, 0 > = 0$. Jos $n = < 0, a > \in \mathbb{Z}_-$, niin $n + < a, 0 > = < 0, m >, \mid a \mid + m = \mid a \mid = < 0, 0 > = 0$. Yksikäsitteisyys seuraa teoreemasta **6.1.4** $\square$.

Vähennyslasku määritellään yhteenlaskuksi vastaluvun kanssa.

Määritelmä 6.1.7: $\forall x, y \in \mathbb{Z}(x - y) = x +_{\mathbb{Z}} (-y)$.

Määritellään kokonaislukujen kertolasku:

Määritelmä 6.1.8:
$\forall x, y \in \mathbb{Z}(x \cdot_{\mathbb{Z}} y = \begin{cases} < \mid x \mid \cdot \mid y \mid, 0 >; & x, y \in \mathbb{Z}_+ \vee x, y \in \mathbb{Z}_- \\ < 0, \mid x \mid \cdot \mid y \mid >; & x \in \mathbb{Z}_+, y \in \mathbb{Z}_- \vee x \in \mathbb{Z}_-, y \in \mathbb{Z}_+ \end{cases})$.

Luovutaan nyt alaindekseistä $+_{\mathbb{Z}}$ ja $\cdot_{\mathbb{Z}}$ sekä koko symbolista $\cdot$ jos sekaannuksen vaaraa ei ole. Määritellään seuraavaksi

Määritelmä 6.1.9 *Murtoluvut*: $\mathbb{F} = \{< p, q > | \ p \in \mathbb{Z}, q \in \mathbb{Z} \setminus 0\}$; kun $< p, q > \in \mathbb{F}$ merkitään $< p, q >= \frac{p}{q}$.

Määritelmä 6.1.10: $\frac{p}{q} + \frac{r}{s} = \frac{ps+qr}{qs}$

Määritelmä 6.1.11: $\frac{p}{q} \cdot \frac{r}{s} = \frac{pr}{qs}$.

Määritelmä 6.1.12: $\frac{p}{q} = 0 \iff p = 0; \frac{p}{q} > 0 \iff pq > 0; \frac{p}{q} < 0 \iff pq < 0; \frac{p}{q} < \frac{r}{s} \iff \begin{cases} ps < qr; & qs > 0 \\ ps > qr; & qs < 0 \end{cases}; \frac{p}{q} = \frac{r}{s} \iff ps = qr.$

6.2 Rationaaliluvut

Rationaaliluvut tavataan määritellä murtolukujen ekvivalenssirelaation $\frac{p}{q} \sim \frac{m}{n} \iff pn = qm$ määräämien osituksien joukkona. Kuitenkin määritelmässä $\mathbb{Q} = \mathbb{F}/\sim$ pitää pystyä esittämään kukin ekvivalenssijoukko yksikäsitteisesti, eikä tähän ole muuta keinoa kuin samaistaa kaikki joukon jäsenet yhteen sen edustajaan säännöllä $syt(p, q) = n \in \mathbb{N}_+$, ja valinta $n \neq 1$ johtaa vain vielä monimutkaisempaan määritelmään.

Ehdon $\varphi(< p, q >) \iff syt(p, q) = 1$ toteutumisen tarkistus ei onnistu äärellisellä kaavalla. Se onnistuu kuitenkin äärellisellä *Euklideen algoritmilla*. Algoritmi ehdoksi asetettaessa pitää ensin aina osoittaa, että se aina päättyy. Koska asetettaessa $f : \mathbb{F}_+ \to \mathbb{F}_+, f < a, b >=< b + a - max\{x \in \mathbb{N} \mid x \cdot b \leq a\} \cdot b, a >$ ja $f_0 = f < p, q >, f_{n+1} = \begin{cases} f(f_n), & f_n \neq < y, 0 > | \ y \in \mathbb{N} \\ f_n, & f_n =< y, 0 > | \ y \in \mathbb{N} \end{cases}$, pätee $\forall n > p + q(f_n =< y, 0 >)$, niin saadaan päättyvä algoritmi:

Määritelmä 6.2.1 *Suurin yhteinen tekijä* (*syt*): $\forall p, q \in \mathbb{N}_+ syt < p, q >= y(\exists k \in \mathbb{N}(f_k =< y, 0 >)) f : \mathbb{F}_+ \to \mathbb{F}_+, f < a, b >=< b + a - max\{x \in \mathbb{N} \mid x \cdot b \leq a\} \cdot b, b >.$

Tästä saadaan edelleen

Määritelmä 6.2.2 *Rationaaliluvut*:
$\mathbb{Q} =< 0_{\mathbb{Z}}, 1_{\mathbb{Z}} > \cup \{< p, q > \in \mathbb{F} \mid q >_{\mathbb{Z}} 0 \wedge syt <\mid p \mid, q >= 1\}$.

Tässä ei ole tarpeen osoittaa, että $\mathbb{Q} \cong \mathbb{F}$ ja $\mathbb{F} \cong \mathbb{N}$, vaan osoitetaan suoraan

Teoreema 6.2.3: $\mathbb{Q} \cong \mathbb{N}$

Todistus: Määritellään tässä positiiviset rationaaliluvut niin, että $0_{\emptyset} \notin \mathbb{Q}_+$. Selvästi väittämän $\mathbb{Q} \cong \mathbb{Q}_+$ totuus ei riipu nollan "positiivisuudesta". Tutkitaan kuviota, jossa osoittaja kasvaa vasemmalta oikealle ja nimittäjä ylhäältä alas ja ehdon $syt = 1$ toteutuminen huomioidaan:

♠	♣	q	↙	↙	↙	↙	↙	↙	↙	↙	↙	↙	↙	↙	↙	↙	↙	↙	↙	↙	↙
−1		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	p
0	1	2	x	o	x	o	x	o	x	o	x	o	x	o	x	o	x	o	x	o	−	
2	2	3	o	x	o	o	x	o	o	x	o	o	x	o	o	x	o	o	x	−		
4	2	4	x	o	x	o	x	o	x	o	x	o	x	o	x	o	x	o	−			
8	4	5	o	o	o	x	o	o	o	o	x	o	o	o	o	x	o	−				
10	2	6	x	x	x	o	x	o	x	x	x	o	x	o	x	x	−		−	−	−	−
16	6	7	o	o	o	o	o	x	o	o	o	o	o	o	x	−			−	”	o	”
20	4	8	x	o	x	o	x	o	x	o	x	o	x	o	−		−	−	−	j	o	s
26	6	9	o	x	o	o	x	o	o	x	o	o	x	−		−	−	s	y	t	=	1
32	4	10	x	o	x	x	x	o	x	o	x	o	−			−	m	u	u	t	e	n
42	10	11	o	o	o	o	o	o	o	o	o	−				−	−	−	−	”	x	”
46	4	12	x	x	x	o	x	o	x	x	−								−	−	−	−
56	12	13	o	o	o	o	o	o	o	−												
62	6	14	x	o	x	o	x	x	−													
70	8	15	o	x	o	x	x	−				v	i	i	m	e	i	n	e	n		
78	8	16	x	o	x	o	−					s	u	m	m	a		o	n			
94	16	17	o	o	o	−					p	i	s	t	e	e	s	e	e	n		
100	6	18	x	x	−						p	,	q		k	e	s	k	e	n		
118	18	19	o	−									j	ä	ä	v	ä	n				
126	8	20	−					d	i	a	g	o	n	a	a	l	i	n				
138	12	q	−		r	a	t	i	o	n	a	a	l	i	e	n		m	ä	ä	r	ä

$\spadesuit = -1 + \sum_{k=1}^{p+q-2}$; $\clubsuit = \sum_{n=1}^{k}$

Sitä käyttäen saadaan seuraava kuvaus:

$f : \mathbb{Q}_+ \to \mathbb{N}, f(\frac{p}{q}) =$

$$-1 + \left(\sum_{k=1}^{p+q-2} \sum_{n=1}^{k} \begin{cases} 1, & syt < k+1-n, n >= 1 \\ 0, & syt < k+1-n, n >\neq 1 \end{cases} \right) + \sum_{i=1}^{q} \begin{cases} 1, & syt < q+p-i, i >= 1 \\ 0, & syt < q+p-i, i >\neq 1 \end{cases}.$$

Se on määritelty kaikilla positiivisilla rationaaliluvuilla ja sen arvot kasvavat 1 kerrallaan alkaen 0:sta, joten se on bijektio $\mathbb{Q}_+ \to \mathbb{N}$.

Kuvaus poimii osoittajan ja nimittäjän summan määrittämän yläoikealta alavasemmalle vedetyn diagonaalin rationaaliluvut: vaikkapa
$f(\frac{11}{7}) = f(\frac{1}{16}) + \sum_{i=1}^{7} \begin{cases} 1, & syt < 18-i, i >= 1 \\ 0 & syt < 18-i, i >= 0 \end{cases} = 78+1+0+0+0+1+0+1 = 81.$

Toisin päin kuviosta nähdään että kun $n = 0,1,2,3,4,5,6,7,8$ niin
$f^{-1}(n) = \frac{1}{1}, \frac{2}{1}, \frac{1}{2}, \frac{3}{1}, \frac{1}{3}, \frac{4}{1}, \frac{3}{2}, \frac{2}{3}$.

Nyt kuvaus $g : \mathbb{N} \to \mathbb{Q}, g(n) = \begin{cases} f^{-1}(k), & n = 2k \\ -(f^{-1}(k)), & n = 2k+1 \end{cases}$ on myös bijektio, joten $\mathbb{N} \cong \mathbb{Q}$ □.

Näin suuri joukko, jota on siis mahdotonta ilmaista muutoin kuin algoritmin määrittämällä ehdolla algoritmin määräämästä joukosta, ei kuitenkaan platonistisen katsannon mukaan ole vielä suurin mahdollinen. Perinteisesti reaalilukuja on käytetty esimerkkinä tällaisesta ylinumeroituvasta joukosta. Se ei sellainen ole sen enempää kuin $\mathcal{P}(\mathbb{N})$.

6.3 Reaaliluvut

Määritellään tässä reaaliluvut siten, että ne saadaan **rationaaliluvuille suoritettavien operaatioiden raja-arvoina**: Dedekindin leikkauksina, Cauchyn jonoina tai näiden kanssa yhtäpitävällä täydellisyyslauseella. Myös siis esimerkiksi reaaliluku 2 saadaan raja-arvona. Luvut $2_{\mathbb{N}}, 2_{\mathbb{Z}}, 2_{\mathbb{Q}}$ ja $2_{\mathbb{R}}$ ovat kaikki eri joukkoja. Reaaliluvut saadaan järjestettyä osajoukkouden perusteella, reaaliluku on kaikkien itseään pienempien reaalilukujen yhdiste.

Määritelmä 6.3.1: Joukko D on *Dedekindin leikkaus* jos
$\emptyset \neq D = \{q \in \mathbb{Q} \mid \forall r <_{\mathbb{Q}} q(r \in D) \wedge \exists p \in D(q <_{\mathbb{Q}} p))\} \neq \mathbb{Q}$.

Dedekindin leikkaus D on siis rationaalilukujen epätyhjä aito osajoukko, joka on alhaalta rajoittamaton ja joka ei sisällä suurinta alkiota. Se on siis aina ensiksikin $\mathbb{Q}$:n osajoukko, ei rationaalilukujen muodostama satunnainen kokoelma vaan joukko, jonka alkiot ovat rationaalilukuja. Tämä tarkoittaa myös, että joukkoa D vastaa rationaaliluvuilla määritelty yhden vapaan muuttujan ehto.

Määritelmä 6.3.2: *Reaalilukujen* joukko
$\mathbb{R} = \{D \in \mathcal{P}(\mathbb{Q}) \mid \emptyset \neq D = \{q \in \mathbb{Q} \mid \forall r <_{\mathbb{Q}} q(r \in D) \wedge \exists p \in D(q <_{\mathbb{Q}} p))\} \neq \mathbb{Q}\}$.

Vaikka ehto $\varphi_{\mathbb{R}}$ on tässä melko pitkä, se on aivan sallittu ehto muodostaa $\mathcal{P}(\mathbb{Q})$:sta **OT**:lla joukko; tässä on vain olennaista se, että kyseessä on nimenomaan **PT**:n takaama osa**joukoista** koostuva $\mathcal{P}(\mathbb{Q})$. Osajoukon muodostaville ehdoille voidaan taas asettaa Gödel-numerointi kuten myös reaaliluvut synnyttäville ehdoille. Esimerkiksi $0_{\mathbb{R}} = \{q \in \mathbb{Q} \mid q < 0\}$ ja $\pi = \{q \in \mathbb{Q} \mid \forall n \in \mathbb{N}(q < 2 \cdot \prod_{k=1}^{n} \frac{(2k)^2}{(2k)^2-1})\}$. Kaikki reaaliluvut ovat siis äärettömiä joukkoja.

Reaalilukujen laskutoimitukset sivuutetaan tässä, joka tapauksessa ne kaikki voidaan esittää rationaalilukujen avulla Dedekindin leikkauksia käyttäen. Järjestys on syytä esittää erikseen, reaalilukujen järjestys määritellään osajoukkouden avulla.

Määritelmä 6.3.3: $\forall x, y \in \mathbb{R}(x <_{\mathbb{R}} y \iff x \subset y)$.

Joukko ei voi olla itsensä tai aidon osajoukkonsa aito osajoukko, joten $<_{\mathbb{R}}$ on irrefleksiivinen ja antisymmetrinen.

Teoreema 6.3.4: $<_{\mathbb{R}}$ on vertailullinen.

Todistus: Valitaan mielivaltaiset $x, y \in \mathbb{R}(x \not\subseteq y)$. Siis $\exists p \in x \setminus y$. Valitaan mielivaltainen $q \in y$. Jos nyt $p \leq q$, niin koska Dedekindin leikkaus y on alhaalta suljettu saataisiin $p \in y$, mikä olisi ristiriita, joten rationaalilukujen trikotomian nojalla on oltava $p > q$ ja koska myös Dedekindin leikkaus x on alhaalta suljettu niin $q \in x$ □.

Reaalilukuja pidetään siis yleisesti ylinumeroituvana joukkona, ja sellaisen ne muodostavatkin jos sallitaan määrittelemättömät joukot. Tämän todistuksessa tutkitaan kokoelmaa $B = \{0, b_1 b_2 b_3 ... \mid \forall i \in \mathbb{N} b_i \in \{0, 1\}\}$, mistä nähdään heti, että kyseessä ovat kaikki välin $[0, 1]$ päättymättömät binäärikehitelmät, jotka platonistismissa samaistetaan tuon välin reaalilukuihin. Äärellisen pituiset sisältyvät tähän kyllä, ne vain loppuvat äärettömään määrään nollia. Nollilla ja ykkösillä saadaan suoraan binäärilukuja, joten käytetään niitä, vaikka käsitelläänkin reaalilukuja eli raja-arvoja, siis esim. $1,000... = 0,111...$, kuvaus f kun ei tässä voi surjektiivisemmaksi muuttua saamalla saman arvon useampaan kertaan. Cantor käytti niitä myös ja näin saatavia binäärikehitelmiä kutsutaankin *Cantorin reaaliluvuiksi*, vaikkeivät ne ole reaalilukuja lainkaan. Ilman nollaa ja pilkkua kyseessä olisivat kaikki äärettömät binäärijonot, ja näitä ei ole mitenkään joukoiksi määritelty. Ei mielivaltainen päättymätön binäärijono pilkulla varustettuna ilmaise reaalilukua väliltä $[0, 1]$, vaan mielivaltainen reaaliluku väliltä $[0, 1]$ ilmaisee päättymättömän binäärijonon.

Nyt jos voitaisiin osoittaa, että B on joukko $[0,1]_{\mathbb{R}}$ ja surjektiota $\mathbb{N} \to B$ ei ole, niin olisi myönnettävä että reaaliväli $[0,1]$ on luonnollisia lukuja mahtavampi. Määriteltävyyttä joukon olemassaolon ehtona pidettäessä B ei ole joukko. Pelkistä **ZFC**-aksioomistakaan ei seuraisi, että se olisi joukko vaikka luovuttaisiin laskettavuusvaatimuksesta. Oletetaan silti, että se olisi joukko ja valitaan mielivaltainen kuvaus $f : \mathbb{N} \to [0,1]$, ja osoitetaan, ettei se ole surjektio. Listataan kuvauksen f antamat äärettömän monta binäärikehitelmää, jotka ovat määriteltävissä olemattoman pitkiä ja monimutkaisia.

$$
\begin{array}{lcccccccccccc}
f(0) & = & a_{0,0} & , & a_{0,1} & a_{0,2} & a_{0,3} & a_{0,4} & a_{0,5} & a_{0,6} & \cdots & a_{0,n} & \cdots \\
f(1) & = & a_{1,0} & , & a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} & a_{1,5} & a_{1,6} & \cdots & a_{1,n} & \cdots \\
f(2) & = & a_{2,0} & , & a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} & a_{2,5} & a_{2,6} & \cdots & a_{2,n} & \cdots \\
f(3) & = & a_{3,0} & , & a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} & a_{3,5} & a_{3,6} & \cdots & a_{3,n} & \cdots \\
f(4) & = & a_{4,0} & , & a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} & a_{4,5} & a_{4,6} & \cdots & a_{4,n} & \cdots \\
f(5) & = & a_{5,0} & , & a_{5,1} & a_{5,2} & a_{5,3} & a_{5,4} & a_{5,5} & a_{5,6} & \cdots & a_{5,n} & \cdots \\
f(6) & = & a_{6,0} & , & a_{6,1} & a_{6,2} & a_{6,3} & a_{6,4} & a_{6,5} & a_{6,6} & \cdots & a_{6,n} & \cdots \\
\vdots & & \vdots & & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \\
f(n) & = & a_{n,0} & , & a_{n,1} & a_{n,2} & a_{n,3} & a_{n,4} & a_{n,5} & a_{n,6} & \cdots & a_{n,n} & \cdots \\
\vdots & & & & & & & & & & & &
\end{array}
$$

ja nyt aktuaalisesti äärettömään listaan ei kuulu binäärikehitelmä
$b = b_0, b_1 b_2 b_3 b_4 b_5 b_6 \ldots b_n \ldots, \begin{cases} b_i = 0, & a_{i,i} = 1 \\ b_i = 1, & a_{i,i} = 0 \end{cases}$; vastaoletuksella saadaan
$(b = f(k)) \Longrightarrow (b_k = a_{k,k}) \Longrightarrow \bot$, joten $\nexists k \in \mathbb{N}(b = f(k)) \wedge b \notin Rng(f)$. Mutta tämän b:n määrittely vaatii, että$\forall i \in \mathbb{N}$ tiedetään $a_{i,i}$ vaikka yleisesti $a_{j,k}$ ei ole määriteltävissä. Toisaalta kokoelma B on myös niin epämääräinen, että b kyllä kuuluu siihen. Sen sijaan emme voi sanoa edes, onko $b > 0,5$ vaikka reaaliluvut noudattavat trikotomiaa. Reaalilukua Cantorin periaate siis ei vastaesimerkiksi tuota, eli niiden ylinumeroituvuutta se ei todista. Kokoelma B ei ole joukko eikä se edes koostu pelkistä reaaliluvuista. Jos ylläoleva olio b kuuluisi reaalilukuihin, eli Dedekindin leikkauksiin, ei valittu kuvaus f olisi täysin mielivaltainen, vaan kuuluisi numeroituvaan joukkoon määriteltävissä olevia kuvauksia, joille voimme määrittää kaikki arvot $f(n)$ numeroituvalla määrällä laskutoimituksia.

Kaikkien binäärikehitelmien joukko on siis mahtavampi kuin $\mathbb{N}$ jos se on joukko. **ZF**-aksioomista tai niiden seurauksista ei suoraan näe, onko se. Yksikäsitteisesti määriteltyjä trikotomiaa noudattavia Dedekindin leikkauksia tai Cauchyn jonoja, jollaisina reaalilukuja yleensä pidetään, kaikki binäärikehitelmät eivät ole. Suoritettavissa olevalla algoritmilla Dedekindin leikkauksina määriteltävissä olevia reaalilukuja on vain numeroituva määrä [Anand]. Niille saadaan kyllä Gödel-numeroinnilla surjektio luonnollisilta luvuilta aikaan.

Yleinen platonistinen käsitys olettaa ilmeisesti reaaliluvuiksi myös kaikki sellaiset rationaalilukujen osajoukot, joiden ilmaisemisessa vaaditaan päättymätöntä algoritmia.

Tästä olisi paljonkin lisää sanottavaa, mutta tässä **ZF-**joukko-oppia käsittelevässä tutkielmassa, jonka alkuperäinen tehtävänanto oli todistaa Schröderin-Bernsteinin teoreema, tämä kuitataan lyhyellä loppuluvulla.

7 Lopuksi

Tässä tutkielmassa on käsitelty **ZF**-aksiomatisoinnin asettamista matematiikan taustalle. Tutkielmaa tehdessäni olen kallistunut sille kannalle, että tämä ei ole paras tapa toimia, vaan joukon sijaan lukumäärä pitäisi asettaa jopa logiikkaa edeltäväksi peruskäsitteeksi. Joukko-opin aksiomatisoinnille taas **NBG** vaikuttaa paremmalta tavalta, ja vielä mieluummin kieltäisin äärettömien joukkojen olemassaolon kokonaan. Periytyvästi äärellisten joukkojen teoriassa oletetaan aidon luokan koko ainoaksi äärettömyydeksi, ja se ei ole joukko.

Aina, kun puhutaan mielivaltaisen suuresta tai rajattomasta määrästä tai käytetään merkintää ... tai jne. niin viitataan äärettömään. Tämä käsite on lukumäärän vertailun väistämätön seuraus. [Rotman] Tämä itsestään syntyvä *potentiaalinen ääretön* merkitsee "suurempi kuin mikään lukumäärä" tai "niin monimutkainen rakenne, ettei mikään subjekti voi sitä täysin kuvailla". Potentiaalista ääretöntä ei voi yksikäsitteisesti määritellä.

Potentiaalisesti ääretön merkitsee, että jotain on enemmän kuin mikään määriteltävissä oleva määrä. Jokaisen joukon alkioiden lukumäärä taas on yksikäsitteinen. Toisin sanoen ääretöntä lukumäärää ei ole olemassa. Ääretön ei siis ilmaise lukumäärää. Se ei siis ole joukolle sallittu ominaisuus.

Aidon luokan alkioiden lukumäärää ei ole olemassa. Aito luokka sisältää rajattoman monta jäsentä, eli aito luokka on potentiaalisesti ääretön.

Vallitsevan platonistisen käsityksen mukaan äärettömiä joukkoja on olemassa rajattoman monta erilaista, näitä kutsutaan *aktuaalisiksi äärettömyyksiksi*. Aktuaalisella äärettömyydellä ilmaistaan kiinteää määrää. Potentiaalinen ääretön on suurempi kuin mikään määrä, joten se on suurempi kuin mikään aktuaalinen ääretön.

Joukon määritelmän on oltava yksikäsitteinen ja yksikäsitteiset määritelmät eivät yleisesti saa sisältää päättymätöntä algoritmia. Ainoastaan päättymätön algoritmi mahdollistaa äärettömän olion kuvailemisen äärellisellä säännöllä. Äärettömyysaksioomakin sisältää tällaisen. Sen ilmaiseman olion alkioiden lukumäärä on suurempi kuin mikään raja, joka sille ennalta asetetaan. Ei ole lukumäärää x, jolla pätisi $x = x + 1$. Edellinen pätee suurilla kardinaaliluvuilla. Niiden kutsuminen luvuiksi on harhaanjohtavaa, sillä ne eivät ilmaise lukumäärää. Lukumäärän määritelmä on perustavampi kuin joukon, ja lukumäärillä pätee $x + 1 > x$.

Luonnollisten lukujen määrä on siis potentiaalisesti ääretön. Se on siten aito luokka.

Koska tutkielman aiheen kuitenkin oli **ZF**-aksiomatisointi, niin siinä on rakennettu teoriaa tälle sittemmin kestämättömäksi toteamalleni pohjalle. Matemaattista arvoa sillä ei siis äärettömyysaksioomaa hyödyntävien tulosten osalta ole, vaan tämä kaikki pitäisi heittää roskakoriin. Kyseessä on kuitenkin lähes vuoden työ, joka täyttänee yleisesti vaaditut edellytykset tulla hyväksytyksi pro gradu-tutkielmaksi. Esitän siis matemaattisena totuutena asiaa, joka ei päde. Tämä ei ole kunniallista ja olen tästä pahoillani.

Toinen asia, josta olen pahoillani on onnettoman termin "platonismi" käyttö. Se on kuitenkin niin vakiintunut, että käytin sitä tässäkin; parempi termi olisi bourbakismi tai vaikka kantilaisuus. Ideaopissaan **Platon** keksi koko abstraktin ajattelun voiman, jolle kaikki tiede ja sivistys perustuvat. Ideaopissaan hän nimenomaisesti teki kategorisen eron havaintojen ja ideoiden muodostamien todellisuuksien välille.

Matematiikkaa hän arvosti suuresti ja sen verran sitä osasikin, ettei hyväksynyt mitään totena vain sillä perusteella, että se oli nykyisen "platonismin" tavoin tuolloin auktoriteettina vallinnut pythagoralainen käsitys. Tässä kun nyt käsitellään mahdollisuutta yksikäsitteisesti kuvailla matemaattisia olioita on vaikkapa seuraava lainaus dialogista "Parmenides" perusteltu:

Parmenides: But the knowledge which we have, will answer to the truth which we have; and again, each kind of knowledge which we have, will be a knowledge of each kind of being which we have?

Sokrates: Certainly.

Parmenides: But the ideas themselves, as you admit, we have not, and cannot have?

Sokrates: No, we cannot.

[Platon]

Kirjallisuutta

[Aaronson] Scott Aaronson: Who Can Name the Bigger Number? Online: http://www.scottaaronson.com/writings/bignumbers.html

[Anand] Bhupinder Singh Anand: Three beliefs that lend illusory legitimacy to Cantor's diagonal argument. Verkkoessee 17.5. 2003. Online: arXiv:math/0304310v2 [math.GM]

[Copi] Irwing M. Copi: Introduction to logic. N.Y., Macmillan 1986

[Hella] Lauri Hella: Joukko-oppi, luentomoniste. Tampereen yliopisto, Matematiikan, tilastotieteen ja filosofian laitos, tammikuu 2005

[Levy] Azriel Levy: Basic Set Theory. Dover Publications 1979

[Merikoski et al.] Jorma Merikoski - Ari Virtanen - Pertti Koivisto: Diskreetti matematiikka I, opetusmoniste. Tampereen yliopisto, Matematiikan laitos 1996

[Platon] Platon: Parmenides. Akatemia, Ateena 370 eKr.

[Rotman] Brian Rotman: Ad Infinitum, The Ghost in Turing's Machine. Stanford University Press, Stanford, California 1993

[Suppes] Patrick Suppes: Axiomatic Set Theory. Dover Publications, N.Y 1960