Äärettömyyksien vertailu joukko-opissa

Jorma Tammenmaa

Matematiikan LuK-aine

Jyväskylän yliopisto
Matematiikan ja tilastotieteen laitos
Kevät 2016

1 Johdanto

Tämän opinnäytetyön tarkoitus on esitellä kardinaalilukujen määritelmä, kardinaalilukujen peruslaskutoimitukset ja valikoima perustuloksia. Työssä käsitellään myös pintapuolisesti järjestyksien teoriaa ja ordinaaliluvun määritelmän –johon oleellisesti kuuluu käsite *hyvä-järjestys–* , jotta voimme antaa täsmällisen määritelmän myös äärettömien joukkojen kardinaaliluvuille. Aiheen laajuuden vuoksi joudumme kuitenkin sivuuttamaan jonkin verran aiheen täsmällisen käsittelyyn vaadittavaa tekniikkaa. Lisäksi tulemme opinnäytteen alkupuolella tarkastelemaan jonkin verran joukko-opin historiaa, joka toivottavasti yhdessä esitettävän teorian kanssa voi antaa motivaatiota joukko-opin syvempään opiskeluun, niin itselle kuin mahdolliselle lukijalle. Päätuloksia ei työssä varsinaisesti ole, mutta sitä lukiessa kannattaa pitää mielessään, että on olemassa monenlaisia äärettömyyksiä, ei vain yhtä sorttia, niin kuin voisi ensimmäisenä ehkä ajatella. Itseasiassa myöhemmin nähdään, että joukko-opillisia äärettömyyksiä on paljon, jopa äärettömästi. Tulemme myös huomaamaan, että käsite äärettömyys on yllättävän monimutkainen joukko-opista käsin tarkasteltuna. Esimerkkinä erilaisista äärettömyyksistä voidaan antaa numeroituvat ja ei-numeroituvat joukot. Edellistä vastaa esimerkiksi luonnollisten lukujen joukko $\mathbf{N}$ ja jälkimmäistä vastaa reaalilukujen joukko $\mathbf{R}$.

Tarkastelun tulen aloittamaan historialla, käsitteiden intuitiivisella tarkastelulla ja aiheeseen liittyvillä ongelmilla. Esityksen alkupuoli on pääasiassa lyhyt katsaus joukko-opin valtavirtaan. Jokaisella oppialalla on niihin kuuluvat suuret ongelmat ja ilmiöt ja jos sellaisia joukko-opissa voisi katsoa olevan, niin parhaiten sitä mielestäni ilmentävät kontinuumihypoteesi, äärettömyyksiin liittyvät havainnot, tavoite löytää suuret kardinaalit sisältävä ydinmalli, aksioomajärjestelmän ristiriidattomuus ja metajoukko-oppi, joista jälkimmäisimpään kuuluvat esimerkiksi *Kurt Gödelin* (1906–1978) ja *Paul Cohenin* (1934–2007) työt [1] (tarkempaa esitystä kannattaa hakea *Lassi Kuritun* vapaana jaetuista monisteista [2] ja lisää avoimia ongelmia tarjoaa ainakin [6]).

Esitys perustuu pääasiassa *Herbert B. Endertonin* kirjaan [1]. Historiallisen näkökulman olen sen sijaan hakenut Lassi Kuritun joukko-opin monisteesta [2] ja *John Stillwellin* kirjasta [3]. Tarkat viitteet löytyvät opinnäytteen lopusta.

2 Joukko-opin historiaa ja alustusta

Matematiikassa, kuten monessa muussakin oppiaineessa, historialla on ollut tärkeä merkitys käsitteiden ja ajatusten muotoutumiselle. Se, mikä nykyään on täsmällinen hiottu aksiomaattinen formaalisysteemi, on aikanaan ollut keskeneräinen, ei-formaali, kiistanalainen ja jatkuvien korjauksien alaisena[1]. Kyseinen piirre on esillä myös matematiikan nykytutkimuksessa. Esimerkiksi logiikan[2] filosofian ja tutkimuksen parissa keskustellaan [10] usein siitä, onko olemassa jokin *oikea* logiikka erotuksena *väärästä* logiikasta ja jos sellainen on, niin miten teemme tarvittavan demarkaation ei-logiikan ja logiikan välille. Esimerkiksi klassisen logiikan muodostavien 2-arvoisen lauselogiikan ja predikaattilogiikan konnektiivit ovat *totuusfunktionaalisia*[3], kun taas modaalilogiikan modaalioperaattorit (joita ovat esimerkiksi intuitiivisesti tutut *välttämätön* ja *mahdollinen*) eivät ole[4]. Esimerkiksi loogikko-filosofi Willard Van Orman Quine piti modaalilogiikan tulkintaa ongelmallisena, sillä se vaatii ensisijaisesti essentialismin[5] hyväksymistä. Tämän ja muiden seikkojen takia [10] ei pitänyt modaalilogiikkaa tarpeellisena laajennuksena klassiselle logiikalle. Quinen mielestä formalisoinnin tavoitteena on saada ”sopiva kieli tieteelle” eivätkä modaalioperaattorit hänen mielestään ole siihen tavoitteeseen tarpeellisia. Quinen mukaan modaalilogiikka ei siis vastaa luonnollista käsitystämme päättelystä, eikä teoria siten ole oikeaa logiikkaa [10]. Vastalauseena voimme todeta, että tieteessä käytetään usein *subjunktiivisia konditionaaleja*, eli lauseita muotoa ”Jos x:n pistää happoon, niin x liukenee ”. Joidenkin mielestä edellisiä lauseita ei voi kuvata klassisen logiikan avulla, vaan tarvitaan *mahdollisuuden* käsitettä [10]. Matematiikassa analoginen tilanne on, kun keskustellaan siitä, kuuluisiko matematiikan olla äärellistä vai ääretöntä. Tätä tutkimuksen ja erityisen matematiikan piirrettä voisi tavallaan pitää tieteen harjoittamisen poliittisena ulottuvuutena.

Tärkeänä esimerkkinä jo mainitusta matematiikan dialektisesta hengestä ja yleisesti tieteen vertailevasta arvioinnista, voidaan mainita matemaatikko-loogikko-filosofin Bernand Russelin (1872–1970) nimettyä Russelin paradoksia ja sen vaikutusta matematiikan perustan tutkimukseen [2, 8].

Kyseinen paradoksi johtuu liian epätäsmällisestä ja liberaalista joukkojen konstruoimisesta. Russell konstruoi paradoksinsa käyttäen eräitä Fregen hyväksymiä periaatteita, jotka liittyivät propositioiden samaistamiseen funktioiksi. Fregen teoriassa, propositioihin sijoitetaan subjektin paikalle argementeiksi erinäisiä olioita. Riippuen

[1] Hyvänä kirjana käsitteen muodostamisesta voisin ehdottaa Imre Lakatosin kirjaa [4].

[2] Logiikkaa voi hahmottaa esimerkiksi oppina pätevästä päättelystä.

[3] Konnektiivi on totuusfunktionaalinen, jos yhdistelmän, jonka pääkonnektiivina kyseinen konnektiivi toimii, totuusarvo riippuu täysin yhdistelmän osien totuusarvoista. Esimerkiksi klassisen logiikan implikaatio konnektiivin totuusarvo riippuu vain sen etu- ja takajäsenestä, joten se on totuusfunktionaalinen.

[4] Ei-formaalissa keskustelussa ja päättelyssä kyseiset termit ovat kuitenkin usein mukana, mistä esimerkkeinä tarjoan; ”On mahdollista, että alienit kruunaavat minut Antarktiksen kuninkaaksi” tai ”On mahdollista, että mahdollistan elämäni syömällä mäkäräisiä muiden laskuun. Siispä: On välttämättä mahdollista, että mahdollistan elämäni syömällä mäkäräisiä muiden laskuun.”.

[5] Essentialismi on ajatus, että olennoilla on joitakin ominaisuuksia välttämättömästi.

sitten annetusta argumentista, saamme propositiolla arvon tosi tai epätosi [6].

Oletetaan nyt että joukkoja voi konstruoida millä säännöllä tahansa. Tällöin erityisesti voimme konstruoida joukon $E = \{x|x \notin x\}$. Nyt kuitenkin kyseisen joukon olettamisesta olemassaolevaksi seuraa, että $E \in E \leftrightarrow E \notin E$, ja edelleen klassisen logiikan[7] ristiriidasta voimme muodollisesti johtaa mitä tahansa (klassisen logiikan sääntö Ex falso Quodlibet), mikä on selvästi kova vastaisku teorialle. Frege sai tiedon ristiriidasta, kun toista painosta hänen kirjasta Grundgesetze der Arithmetik (englanniksi "The basic laws of arithmetic", suomeksi "Aritmetiikan peruslait") oltiin julkaisemassa [8]. Hän yritti korjata ristiriidan rajoittamalla erästä kirjassa esiintynyttä lakia, sisällytti jopa yrityksen johdantoon, mutta ei onnistunut siltikään pelastamaan teoriaansa. Ongelma kuitenkin johti joukko-opin perusteiden etsimiseen ja aksiomatisointimallien muodostamiseen, minkä takia kyseinen paradoksikin saatiin torjuttua.

Äärettömyyden käsite on aiheuttanut päänvaivaa kautta matematiikan historian. Tähän on osaltaan varmasti vaikuttanut ihmisen oletettu rajallisuus, jonka mukaan emme ainakaan matematiikan ulkopuolella pysty tekemään äärettömiä prosesseja. Koska kuitenkin aksioomien tulisi olla matematiikassa intuitiivisia, niin äärettömyydet on koettu varsin ongelmallisiksi. Varsinkin äärettömyyksien eräs ilmentymä reaaliluvut ja niiden ominaisuudet ovat vaatineet ihmiskunnalta suuria ponnistuksia. Asia havainnollistuu esimerkiksi siinä, että ensimmäisiä määritelmiä saatiin vasta Richard Dedekindin (1831–1916) töistä 1800-luvun loppupuolella, vaikka varsinkin Zenonin (n. 490–420 eaa.) paradoksit – jotka tunnemme Aristoteleen (384–322 eaa) ja Platonin (427–347 eaa.) töiden kautta (tarkemmin [3] sivut 54, 182, 526) – ennakoivat jatkumon käsitettä, joka on reaalilukujen tarkastellessa yksi oleellinen omainaisuus. Kyseiset paradoksit aiheuttivat kummastusta ja vastustusta aikalaisissaan, mikä todennäköisesti johtuu juurikin äärettömyyksien ja reaalilukujen (katkeamaton viiva) vaikeasta käsitettävyydestä.[3] Kuitenkin esimerkiksi Bernand Russellin mukaan:

> *"In this capricious world nothing is more capricious than posthumous fame. One of the most notable victims of posterity's lack of judgement is the Eleatic Zeno. Having invented four arguments all immeasurably subtle and profound, the grossness of subsequent philosophers pronounced him to be a mere ingenious juggler, and his arguments to be one and all sophisms. After two thousand years of continual refutation, these sophisms were reinstated, and made the foundation of a mathematical renaissance ...."* [5]

Joukon käsitettä muotoiltiin 1800-luvun lopussa tavoitteena saada juurikin esimerkiksi vastauksia reaalilukuihin liittyviin kysymyksiin. Joukko-opin perustajana pidetään suhteellisen yleisesti Georg Cantoria (1845–1918), joka opiskeli Berliinissä Weierstrassin johdolla ja valmistui tohtoriksi vuonna 1869 lukuteoriaa käsittelevällä

[6]Ks. esim. [8] .

[7]On kuitenkin olemassa ei-klassisia logiikoita, kuten esimerkiksi parakonsistentti logiikka, jossa Ex Falso Quodlibet ei ole sääntö. Havainnollistavaa on, että arjessa ihmisten mielipiteet ja ajatukset voivat hyvinkin olla ristiriidassa tai jännitteessä keskenään, mutta kuitenkaan kovin moni tuskin ajattelee, että tästä seuraisi henkilön sitoutuminen kaikkiin mahdollisiin propositioihin.

väitöskirjalla. Kuitenkin Bolzano tutki ennen Cantoria jo esimerkiksi numeroituvuuden käsitettä [9]. Cantorin itse ajautui tarkastelemaan joukkoja tutkittuaan Fourier-sarjoja eli sarjoja muotoa $a_1 \sin(x) + a_2 \sin(2x) + a_3 \sin(3x) + \cdots$. Tutkiessaan kyseisiä sarjoja hän alkoi tarkastelemaan yhä yleisempiä reaalilukujoukkoja ja huomasi, että joitakin reaalilukuja koskeavia operaatioita voitiin toistaa enemmän kuin äärellisen verran. Cantor esimerkiksi todisti, että reaalilukujen ja kokonaislukujen välille ei voi konstruoida bijektiota, sekä esitti abstraktin joukon käsitteen ja transfiniittilukujen käsitteen. Cantor loi ajatuksiensa taustalle oman matematiikan filosofian, joka houkutteli esiin kannattajia[8] ja vastustajia, joista tunnetuimpana voisi mainita Leopold Kronecker (1823–1891), jonka matematiikan filosofinen kanta suosi finitismiä eli oppia jonka mukaan matematiikan tulisi olla ”äärellistä”. Merkillepantavaa on, että Kronecker ei uskonut edes irrationaalilukujen olemassaoloon, vaan katsoi vain luonnolliset luvut *olemassaoleviksi*, joiden äärellisiin ominaisuuksiin matematiikka tulisikin rajoittaa. Tässäkin tulee painottaa jo mainittua teorioiden ja näkökantojen keskustelevaa luonnetta. Knoneckerin filosofialla on kuitenkin ollut voimaa selittää suurta osaa matematiikasta, ja esimerkiksi Bouwer kehitti myöhemmin Kroneckerin filosofian pohjalta (1881–1966) intuitionisnin ja konstruktiivisen matematiikan [9].

Mutta miksi alan puhumaan joukko-opista kun juuri lupasin uppoutua äärettömyyksiin? Syy on se, että joukko-opilla on tärkeä rooli äärettömyyksien tarkastelemisessa; se tarjoaa ilmiöstä matemaattisen teorian. Formaali logiikka tarjoaa toisaalta käsityksen todistuksesta, juurikin ratkaisemaan paradokseja, jotka ovat syntyneet äärettömyyksien ajattelemisesta. Siispä matematiikassa on alueita, jotka ovat erillisestä nimityksestä huolimatta läheisissä tekemisissä toistensa kanssa. Esimerkiksi logiikan ja metamatematiikkan tulokset osoittavat sen, että joukko-oppi ei voi todistaa omaa ristiriidattomuuttaan, vaan tarvitaan edelleen jotain vahvempaa teoriaa tai kieltä. (Täsmällisestä esityksestä kiinnostuneen kannattaa tarkastella esimerkiksi Kuritun monisteita [2].)

3 Primitiiviset käsitteet

Kuten aiemmin mainittiin, joitakin käsitteitä ja ajatuksia olisi hyvä selventää ja aksiomatisoida, jotta vältämme monia ongelmia. Tehdään joitakin edelliseen huomioon liittyviä asioita tässä, mutta ei luovuta historiallisesti lähestymisestä. Luultavasti jokaisella meistä on jonkinlainen käsitys käsitteestä ”joukko”. Esimerkiksi laiskanläksyt voisivat olla eräs joukko ja erakkojen joukko voisi olla toinen joukko. Ajattelemme ehkä, että joukko koostuu alkioista, jotka voimme mielessämme ainakin yksilöidä erilliseksi kyseisestä joukosta. Joku voi kuitenkin nyt ajatella joukkoa, joka koostuu alkioista, jotka ovat itsekin joukkoja. Asian havainnollistamiseksi, jokainen joukko X kuuluu esimerkiksi joukkoon $\{X\}$. Tällöin voimme kysyä, onko olemassa joukkoa, johon kaikki joukot kuuluvat. Suhteellisen helposti voimme todistaa – käyttäen ak-

[8]Esimerkiksi Dedekind, jonka töiden ansiosta Cantor havaitsi, että reaalilukujen täydellisyydestä seuraa reaalilukujen ylinumeroituvuus, ja Mittag-Leffler (1846–1927), joka sovelsi joukko-opin menetelmiä funktioteoriaan

sioomia jolloin asiasta tulee teoreema – että vastaus on kieltävä[9]. Siispä ainakin jotain rajoituksia joukkoille löytyy, mutta olisi toivottavaa, jos voitaisiin joskus keskustella kaikkien joukkojen *kokoelmasta.*

Bernand Russell ja Alfred North Whitehead (1861–1947) ratkaisivat kyseisen ongelman, järjestämällä joukot hiearkisesti alkaen atomeista, jotka ovat alimmalla tasolla, minkä jälkeen ylemmällä tasolla on joukot, jonka alkioita alemman tason atomit ovat, ja sitä ylempi taso kooskuu joukoista, jonka alkioita ovat edellisen tason joukot. Kun jatkamme tätä prosessia äärettömästi, niin saamme äärettömästi jatkuvan hierarkian. Kun nyt etenemme hierarkiassa ylöspäin, niin päädymme yhä monimutkaisempiin joukkoihin.

On myös olemassa vaihtoehtoisia tapoja välttää kyseinen ongelma:

I Zermelo-Fraenkel:n vaihtoehto: Ei anneta kaikkien joukkojen kokoelmalle mitään ontologista asemaa. Tässä vaihtoehdossa on vain kaksi peruskäsitettä: *joukko* ja *joukon alkiona olo.*

II Von Neumann-Bernays:n vaihtoehto: Kutsutaan yleisesti jokaista joukkojen kokoelmaa luokaksi. Tällöin siis erityisesti kaikkien joukkojen kokoelma on luokka. Sovitaan lisäksi, että hierarkiamme alin taso koostuu vain tyhjästä joukosta (tässä siis hankkiudumme eroon joukko-opille ulkoisista atomeista), jolloin kaikki joukkomme ovat myös luokkia. Kuitenkin esimerkiksi kaikkien joukkojen luokka on liian iso joukoksi, joten voimme kutsua sitä aidoksi luokaksi erotuksena luokista, jotka ovat myös joukkoja. Luokka voi siis olla joukko, mutta ei välttämättömästi, kun taas joukko on esityksessämme aina myös luokka.

Tässä esityksessä käytämme suurelta osin vaihtoehtoa yksi. Toimimme jatkossa ZFC-teoriassa (Zermelo-Fraenkel:n joukko-oppi varustettuna valinta-aksioomalla).

Eräs tärkeä seikka tulevassa käsittelyssämme on *valinta-aksiooman* hyväksyminen ja sen käyttö varsinkin esityksen loppupuolella. Jos emme nimittäin olettaisi valinta-aksioomaa, niin monet todistuksistamme kaatuisivat ja muutenkin asioiden käsittely olisi ongelmallista, minkä jatkossa tulemme huomaamaan. Mutta miksi tarvitsemme valinta-aksioomaa ja mikä aksiooman sisältö edes on? Vastaus siihen on, että valinta-aksiooman hyväksyttäessä oletamme voivamme tehdä äärettömiä valintaprosesseja, joissa valinta tehdään *yhtäaikaisesti.* Tällainen periaate osoittautuu erittäin käyttökelpoiseksi, kun haluamme muodostaa tai osoittaa jonkin joukon olevan olemassa. Esimerkiksi ZFC-teorian[10] teoreema, jonka mukaan jokaiselle joukolle voidaan muodostaa hyvä-järjestys, on yhtäpitävä valinta-aksiooman kanssa. Jos nyt emme olettaisi valinta-aksioomaa, niin emme toisaalta voisi osoittaa, että jokainen joukko on yhtä mahtava jonkin ordinaaliluvun kanssa, emmekä sitten voisi määritellä mielivaltaisen joukon A kardinaalilukua ”pienimmäksi ordinaaliluvuksi, joka on yhtämahtava A:n kanssa”, vaan joutuisimme tekemään määritelmän eri tavalla [7].

[9] Tee antiteesi ja konstruoi joukko $\{x \in A \mid x \notin x\}$ ja tarkastele kuuluuko kyseinen joukko A:han, kun A on antiteesin lupaama joukko.

[10] Zermelo–Fraenkel joukko-oppi, jossa oletetaan valinta-aksiooma.

Karkeasti valinta-aksiooman eräs muotoilu ilmaisee, että on olemassa joukko, joka koostuu äärettömästä määrästä yhtäaikaisesti valitsemiamme alkioita. Täsmällisemmin ilmaistuna eräs valinta-aksiooman muotoilu on:

Kaikille joukoille I pätee: Jos $H(i) \neq \varnothing$ kaikille $i \in I$, niin on olemassa funktio f lähtöjoukolla I varustettuna siten, että $f(i) \in H(i)$ kaikille $i \in I$ (valintafunktion olemassaolon olettaminen).

Valinta-aksioomalla on kuitenkin paljon erilaisia muotoiluja ja yhtäpitävyyksiä ([1] s. 151–158), joista osa saattaa aluksi vaikuttaa varsin yllättäviltä. Esimerkkinä voidaan mainita erityisesti tähän opinnäytteeseen kuuluva kardinaalien vertailu:

Jokaiselle joukolle A ja B pätee, että joko joukosta A on olemassa injektiivinen kuvaus joukkoon B tai joukosta B on injektiivinen kuvaus joukkoon A tai toisin sanottuna jokaiselle kardinaaliluvulle α ja β pätee $\alpha \leq \beta$ tai $\beta \leq \alpha$.

On tärkeää kuitenkin huomioida, että emme tarvitse valinta-aksioomaa, jos teemme vain äärellisen määrän valintoja tai voimme täsmällisesti sanoa, mitkä alkiot valitsemme epätyhjien joukkojen kokoelman joukoista. Historiallisesti valinta-aksioomalla on ollut erilainen status muihin joukko-opin aksioomiin nähden, mikä liittyy myös aiemmin mainittuun vaatimukseen matematiikan äärellisyydestä tai äärettömyydestä. Jos nimittäin otamme teorian intuitiiviseksi perustaksi matematiikan ulkopuolisen arkielämän, niin vahvasti ainakin vaikuttaa siltä, että ihmiset eivät voi tehdä ääretöntä määrää yhtäaikaisia valintoja, ja koska toisaalta aksioomilta yleensä vaaditaan "intuitiivisuutta", niin valinta-aksiooma ei arkielämän valossa sellainen joidenkuiden mielestä voi olla. Nykyään valinta-aksiooma on sen sijaan ainakin klassisen logiikan hyväksyneiden parissa otettu asialliseksi aksioomaksi.

Valinta-aksiooman tarpeellisuutta voi hahmottaa esimerkiksi Russelin antaman esimerkin mukaan: Jos meillä on $\aleph_0$:n (pienimmän äärettömän kardinaalin) verran kenkäpareja, niin voimme valita yhden kengän jokaisesta kenkäparista ilman valinta-aksioomaa. Valitsemme vain jokaisesta parista oikean kengän. Jos meillä sen sijaan on $\aleph_0$ paria sukkia, niin ilman valinta-aksioomaa emme voi tehdä vastaavaa valintaa.

Tarkastellaan sitten vielä *sisältyvyyssääntöjä*, joilla muodostamme usein joukkoja. Todetaan ensiksi, että, sisältyvyyssäännöt tulee ilmaista mahdollisimman yksiselitteisesti, jottei tule esimerkiksi seuraavanlaista ongelmaa: konstruoidaan joukko[11]

$$\{x | x \text{ on määriteltävissä yhdellä rivillä kirjoituskoneella}\}.$$

Nyt esimerkiksi luku 12 kuuluu joukkoon, sillä sen määritelmä mahtuu yhdelle riville. Toisaalta jos määritelmä ylittää yhden rivin kirjoituskoneella, niin kyseinen alkio ei kuulu joukkoon. Selvästi alkioita joukussa on vain äärellinen määrä[12], joten lukija voisi tässä välissä miettiä mitä tapahtuu kun valitaan pienin alkio, joka ei kuulu tarkasteltavana olevaan joukkoon, eli siis alkio

pienin positiivinen kokonaisluku, jota ei voida määritellä yhdellä rivillä.

[11] Tämä esimerkki on muotoiltu G.G. Berryn esimerkistä, jonka hän antoi vuonna 1906.

[12] On vain äärellinen määrä symboleita näppäimistössä ja käyttäen kiinnitettyä sivu kokoa ja kirjainten kokoa, on raja kuinka monta symbolia mahtuu yhdelle riville.

Tämä ongelma ratkeaa aksiomatisoinnin tuloksena, kun esitetään miten joukkoja konstruoidaan yksiselitteisesti, johon ei kuitenkaan tässä opinnäytteessä mennä (tarkemmin kirjassa [1] kappale 2 kokonaisuudessaan).

4 Kardinaaliluvut

Seuraavaksi mietimme miten voisimme vertailla äärettömien joukkojen kokoja. Todetaan ensin, että äärellisten joukkojen tapauksessa vertailussa ei pitäisi olla mitään erityisen hankalaa. Ensimmäisenä äärettömässä tapauksessa varmaan voisi tulla mieleen, että joukko A on suurempi kuin joukko B, jos B on A:n aito osajoukko. Näinhän se menee, jos $B \subset A$, mutta entä jos kumpikaan joukoista ei sisälly toiseensa tai jos joukot ovat jopa pistevieraita? Miten tällöin voisimme vertailla äärettömien joukkojen kokoja? Antakoon seuraava tapauskertomus ideaa mahdollisesta ajattelutavasta, jolla meidän tulisi lähestyä toimivaa määritelmää:

Oletetaan hetkeksi, että emme osaa laskea lukua 2 pidemmälle. Kuvitellaan sitten tilanne, jossa haluaisimme rajoitteistamme huolimatta osoittaa, että meillä yhtä monta varvasta ja sormea. Emme voi nyt kuitenkaan laskea varpaiden ja sormien lukumääriä, joita voisimme sitten vertailla, vaan meidän tulee keksiä tapa kiertää rajamme. Hetken aikaa pohdittuamme keksimme, että voimme asettaa sormet ja varpaat vastakkain. Saamme siis varpaiden ja sormien välille yksi-yhteen-vastaavuuden, jolloin voimme todeta, että niitä täytyy olla yhtä paljon. Löysimme siis tavan osoittaa, että varpaita ja sormia on yhtä paljon, ilman että meidän tarvitsee laskea varpaiden ja sormien lukumääriä.

Tämän esimerkin mukaisesti voimme määritellä apuvälineen äärettömien ja äärellisten joukkojen vertailuun:

Määritelmä 1. Joukko A on yhtämahtava joukon B kanssa, jos ja vain jos, on olemassa bijektiivinen funktio joukosta A joukkoon B. Tällaisessa tapauksessa merkitsemme $A \approx B$.

Esimerkki 2. Avoin väli $(0,1) = \{x \in \mathbf{R} | 0 < x < 1\}$ on yhtämahtava reaalilukujen joukon $\mathbf{R}$ kanssa.

Todistus. Valitaan halutuksi bijektioksi funktio $f : (0,1) \to \mathbf{R}$ siten, että $f(x) = \frac{1}{x} - \frac{1}{1-x}$.

Nyt f on bijektio ja jätämme tämän lukijan tarkastettavaksi. Siispä $(0,1) \approx \mathbf{R}$. $\square$

Esimerkki 3. Osoitetaan, että suljettu väli $[0,1] = \{x \in \mathbf{R} \mid 0 \leq x \leq 1\}$ on yhtämahtava avoimen välin $(0,1)$ kanssa.

Todistus. Muodostetaan funktio $f : [0,1] \to (0,1)$ seuraavalla tavalla:

Asetetaan ensin, että $1 := a_0$ ja $0 := b_0$. Määritellään sitten $f(a_0) = \frac{1}{2^{1+0}}$ ja $f(b_0) = \frac{1}{3^{1+0}}$. Merkitään sitten $\frac{1}{2} := a_1$ ja $\frac{1}{3} := b_1$, jolloin määritellään $f(a_1) = \frac{1}{2^{1+1}}$ ja $f(b_1) = \frac{1}{3^{1+1}}$. Jatketaan kuten aiemmin, kunnes saavumme vaiheeseen n. Nyt $f(a_{n-1}) = \frac{1}{2^{1+(n-1)}}$ ja $f(b_{n-1}) = \frac{1}{3^{1+(n-1)}}$. Merkitään sitten $\frac{1}{2^n} := a_n$ ja $\frac{1}{3^n} := b_n$.

Määritellään sitten $f(a_n) = \frac{1}{2^{1+n}}$ ja $f(b_n) = \frac{1}{3^{1+n}}$. Jatketaan vastaavasti prosessia kohti äärettömyyttä.

Saamme sitten lopulta joukot $\{a_i | i \in \omega\} := A$ ja $\{b_i | i \in \omega\} := B$, jolloin voimme kaikkiaan määritellä:

$$f(x) = \begin{cases} \frac{1}{2^{1+i}}, & \text{jos } x = a_i, \text{ jollakin } i \in \omega \\ \frac{1}{3^{1+j}}, & \text{jos } x = b_j, \text{ jollakin } j \in \omega \\ x, & \text{muuten.} \end{cases}$$

Ensinnäkin voidaan todeta, että f on hyvin määritelty, sillä $A \cap B = \varnothing$, mistä seuraa myös, että f on injektio. Lisäksi selvästi $0 < f(x) < 1$ ja f on selvästi surjektio. Kaikkiaan siis f on bijektio ja siten $[0, 1] \approx (0, 1)$. □

Näytämme seuraassa teoreemassa, että yhtämahtavuudella on kaikkien joukkojen luokassa ominaisuudet refleksiivisyys, symmetrisyys ja transitiivisuus, mutta nämä ominaisuudet eivät kuitenkaan muodosta ekvivalenssirelaatiota[13]. Tämä puute johtuu siitä, että yhtämahtavuus koskettaa kaikkia joukkoja. Jos kyseinen joukko olisi nimittäin olemassa, niin siitä seuraisi, että olisi joukko, johon kuuluu kaikki järjestetyt parit ja siitä taas seurausi, että on olemassa joukko johon kaikki joukot kuuluisivat, mikä on ristiriidassa aiemman kanssa (ks. kappale 3). Von Neumann-Bernays joukko-opissa voidaan kuitenkin muodostaa luokka $\{\langle A, B\rangle | A \approx B\}$, joka ei kuitenkaan ole joukko.

Lause 4. *Jokaiselle joukolle A,B ja C:*

1. *$A \approx A$ (refleksiivisyys),*

2. *Jos $A \approx B$, niin $B \approx A$,*

3. *Jos $A \approx B$ ja $B \approx C$, niin $A \approx C$.*

Todistus. Ensimmäisessä kohdassa määrittelemme funktion $f : A \to A$ siten, että $f(x) = x$. Selvästi f on bijektio, joten $A \approx A$.

Oletetaan sitten, että $A \approx B$, jolloin on olemassa bijektiivinen kuvaus $f : A \to B$. Tällöin f:llä on tunnetusti käänteisfunktio $f^{-1} : B \to A$, joka on triviaalisti bijektio. Siispä $B \approx A$.

Viimeisenä oletamme, että $A \approx B$ ja $B \approx C$. Nyt on olemassa bijektiot $f : A \to B$ ja $g : B \to C$, jolloin yhdistetty funktio $g \circ f : A \to C$ on haluamamme bijektio, sillä kahdesta bijektiosta yhdistetty funktio on bijektio. □

Seuraavassa teoreemassa tapaamme ensimmäisen kerran äärrettömyyksien keskinäisen eroavaisuuden.

Lause 5. *Luonnollisten lukujen joukko ω ei ole yhtämahtava reaalilukujen joukon* **R** *kanssa (Cantor 1873).*

[13] Ekvivalenssirelaatioista tarkemmin kirjan [1] sivuilla 54–63.

Todistus. Haluamme näyttää, että jokaiselle funktiolle $f : \omega \to \mathbf{R}$ löytyy reaaliluku z, joka ei kuulu f:n maalijoukkoon. Koska jokainen reaaliluku voidaan esittää desimaalikehitelmänä, niin voimme valita $z \in \mathbf{R}$ siten, että kokonaislukuosa on 0 ja $(n+1)$:n desimaalin paikalla on 7, paitsi jos $(n+1)$:n desimaalin paikalla $f(n)$:ssä on 7, jolloin $(n+1)$:n desimaalin paikalle luvussa z tulee 6.

Nyt z on reaaliluku, joka ei kuulu f:n maalijoukkoon, sillä se eroaa mielivaltaisen $n \in \omega$ kuvasta $(n+1)$:n desimaalin kohdalla. □

Lause 6. *Mikään joukko ei ole yhtämahtava potenssijoukkonsa kanssa.*

Todistus. Olkoon $g : A \to \mathcal{P}A$ funktio. Konstruoidaan nyt A:n osajoukko B, joka ei kuulu g:n maalijoukkoon. Eksplisiittisesti määritellään

$$B = \{x \in A | x \notin g(x)\}.$$

Nyt $B \subseteq A$, mutta jokaiselle $x \in A$ pätee: $x \in B \leftrightarrow x \notin g(x)$.
Siispä $B \neq g(x)$, joten B ei kuulu funktion g kuvaan. □

Vaikka puhetta on ollut otsikosta lähtien, että tarkastelemme äärettömyyksiä, niin tarkastellaan seuraavaksi hieman äärellisiä joukkoja. Seuraavaa määritelmää varten tulee tietää luonnollisten lukujen joukko-opillinen konstruktio, joten esittelemme sen lyhyesti tässä. Sivuutamme kuitenkin luonnollisten lukujen laskusäännöt ja muita asiaan kuuluvia tuloksia ja ilmiöitä[14].

Konstruoidaan tässä välissä luonnolliset luvut käyttäen joukkoja: Asetetaan $0 = \varnothing$, $1 = \{\varnothing\}$, $2 = \{\varnothing, \{\varnothing\}\}$, ja yleisesti jos n on luonnollinen luku, niin asetetaan sen seuraajalle $n + 1 := n^+$, että $n^+ = n \cup \{n\}$.

Voisimme nyt rekursioteoreemaa käyttäen määritellä luonnollisten lukujen laskutoimitukset, mutta sivuutamme tilan puutteen vuoksi ne tässä työssä.

Nyt konstruktiomme ominaisuuksiin kuuluu, että luonnollinen luku m on pienempi kuin luonnollinen luku n, jos $m \in n$, eli toisin sanoen merkitsemme $m < n$, jos $m \in n$. Vastaavasti merkitsemme $m \leq n$, jos $m \underline{\in} n$, eli toisin sanoen $m = n$ tai $m < n$.

Määritelmä 7. Joukko on äärellinen, jos ja vain jos, se on yhtämahtava jonkin luonnollisen luvun kanssa. Muussa tapauksessa joukko on ääretön.

Seuraavaksi haluamme näyttää, että äskeisessä määritelmässä esiintyvä luonnollinen luku on yksikäsitteinen. Jotta voimme todistaa väitteen tarvitsemme seuraavan periaatteen, joka on nimetty kyyhkyslakan mukaan.

Lause 8. *Mikään luonnollinen luku ei ole yhtämahtava sen aidon osajoukon kanssa (kyyhkyslakkaperiaate).*

Todistus. Oletetaan, että f on injektiivinen kuvaus joukosta n joukkoon n. Näytetään, että tällöin f:n maalijoukko on n kokonaisuudessaan, mikä todistaa halutun väitteen.

Todistetaan väite induktiolla n:nän suhteen. Määritellään tavoitettamme varten joukko

$$T = \{n \in \omega | f \text{ on injektio joukosta } n \text{ joukkoon } n \Rightarrow f \text{ n on surjektio}\}.$$

[14] Kiinnostuneen lukijan kannattaa lukea kirjan [1] kappale 4.

I $0 \in T$, sillä ainoa funktio joukosta $0 = \varnothing$ joukkoon 0 on $\varnothing$ ja selvästi kyseinen funktio on surjektio.

II Oletetaan sitten että $k \in T$ ja näytetään, että $k^+ = k \cup \{k\} \in T$. Olkoon nyt f injektiivinen kuvaus joukosta k^+ joukkoon k^+. Nyt tarkastelumme jakautuu alitapauksiin:

1. Oletetetaan ensin, että f kuvaa joukon k joukkoon k, eli tällöin myös f:n rajoittuma $f\lceil k$ kuvaa k:n joukkoon k. Nyt koska $k \in T$, niin $f\lceil k$ on surjektio, ja lisäksi koska f oli injektio niin ainoa mahdollisuus on, että $f(k) = k \notin k$.

   Siispä f on tässä tapauksessa surjektio.

2. Oletetaan sitten, että $f(p) = k$, jollakin $p < k$. Määritellään nyt g siten, että

$$g(p) = f(k), g(k) = f(p) = k \text{ ja } g(x) = f(x) \text{ muilla } x \in k^+.$$

   Tällöin g on injektio joukosta k^+ joukkoon k^+, ja lisäksi k on suljettu g:n alla. Siispä edellisen kohdan nojalla g on surjektio, joten myös mielivaltainen injektio f on surjektio.

Nyt kohtien (1) ja (2) nojalla f on kaikissa tapauksissa surjektio, ja siten T on induktiivinen, mistä taas saadaan että $T = \omega$. □

Seuraus 9. *Mikään äärellinen joukko ei ole yhtämahtava aidon osajoukkonsa kanssa.*

Todistus. Väite seuraa lauseesta 8, kun tarkastelu siirretään – asiaan kuuluvilla funktioilla – koskemaan luonnollisia lukuja. □

Seuraus 10. *Edellisestä seurauksesta seuraa edelleen, että*

1. *Jokainen joukko, joka on yhtämahtava aidon osajoukkonsa kanssa on ääretön*[15].

2. *Luonnollisten lukujen joukko ω on ääretön.*

Todistus. Ensimmäinen kohta seuraa suoraan edellisestä seurauksesta, ja jälkimmäinen kohta seuraa suoraa ensimmäisestä kohdasta, sillä funktio $f : \omega \to \omega \setminus \{0\}, f(n) = n^+$ on bijektio. □

Seuraus 11. *Jokainen äärellinen joukko on yhtämahtava yksikäsitteisen luonnollisen luvun kanssa.*

Todistus. Oletetaan, että $A \approx n$ ja $A \approx m$, joillekkin luonnollisille luvuille m ja n. Tällöin $m \approx n$. Trikotomian[16] nojalla $m \in n$, $n \in m$ tai $n = m$. Jos $m \in n$, on luonnollisten lukujen konstruktion vuoksi m joukon n aito osajoukko. Tämä on ristiriidassa lauseen 8. kanssa. Samoin myös $n \in m$ on mahdoton. Siispä $n = m$. □

[15]Itseasiassa Dedekindin vuonna 1888 antama määritelmä äärettömyydelle on seuraava: ”joukko on ääretön jos ja vain jos se on yhtämahtava jonkun osajoukkonsa kanssa.”

[16]Luonnollisten lukujen joukossa pätee täsmälleen yksi seuraavista: $m \in n$, $m = n$ tai $n \in m$. Katso tarkemmin kirjan [1] kappaaleesta 4.

Otetaan sitten käyttöön merkintä koskien äärellisiä joukkoa. Kun n on edellisen seurauksen lupaama yksikäsitteinen luonnolinen luku joukolle A, niin merkitsemme $\mathrm{kard}(A) = n$. Äärettömille joukoille B ja C merkitsemme $\mathrm{kard}(B) = \mathrm{kard}(C)$ jos ja vain jos $B \approx C$. Tarkempaa määritelmää ja merkintää äärettömille joukoille emme tässä tiivistelmässä käy läpi, sillä se vaatisi mittavaa teknistä käsittelyä[17]. Merkitään kuitenkin seuraavia tuloksia varten $\mathrm{kard}(\omega) = \aleph_0$; kyseinen merkintä periytyy meille Cantorilta.

Nyt jos haluaisimme määritellä täsmällisesti äärettömät kardinaaliluvut, niin meillä pitäisi olla tapa järjestää annettu struktuuri[18] siten, että jokaisella sen epätyhjällä osajoukolla on pienen alkio, eli toisin sanoen haluaisimme järjestää joukon siten, että sillä on ensimmäinen alkio, toinen alkio, kolmas alkio ja niin edelleen. Ordinaaliluvut ovat tavallaan lukuja, jotka mittaavat jokaisen hyvin-järjestetyn struktuurin *pituutta*, tai tietynlaisessa annetussa järjestyksessä tehtävä joukon alkioiden lukumäärän lasku. Tälläin tulisi tietenkin olla niin, että "kaukaa samannäköiset" struktuurit saisivat aina saman ordinaaliluvun. Lisäksi tarvitsemme teoreeman, jonka mukaan jokaisella joukolla on olemassa hyvä-järjestys[19] ja sen seurausta, jonka mukaan jokainen joukko on yhtämahtava jonkin ordinaaliluvun kanssa. Huomionarvoista on myös, että voisimme määritellä kardinaaliluvut myös ekvivalenssiluokkina ekvivalenssirelaation kaltaisen käsitteen $\approx$ suhteen. Tämä ei ole kuitenkaan tyydyttävää, sillä kuten aiemmin olemme todenneet: kaikkien joukkojen luokka ei ole joukko, joten $\approx$ ei ole varsinaisesti ekvivalenssirelaatio.

Voimme nyt asettaa seuraavan määritelmän (asiaan perehtymätön lukija voi hypätä suoraan seuraavaan määritelmän yli):

Määritelmä 12. Olkoon A mielivaltainen joukko. Joukon A *kardinaaliluku* on pienin A:n kanssa yhtämahtava ordinaaliluku.

Todistetaan seuravaksi, että äärellisen joukon osajoukko on äärellinen. Tarvitsemme todistukseen seuraavan lemman:

Lemma 13. *Jos C on luonnollisen luvun n aito osajoukko, niin $C \approx m$ jollekin $m < n$.*

Todistus. Todistetaan väite induktiolla. Muodostetaan sitä varten joukko

$$T = \{n \in \omega | \text{jokainen } n\text{:n aito osajoukko on yhtämahtava jonkin } n\text{:n alkion kanssa}\}.$$

I Triviaalisti $0 \in T$, sillä joukolla $0 = \varnothing$ ei ole aitoja osajoukkoja.

II Oletetaan sitten että $k \in T$ ja näytetään, että $k^+ \in T$. Oletetaan että $C \subset k^+$. Nyt tarkastelu jakautuu jälleen alatapauksiin:

(a) $C = k$. Tälläin $C \approx k \in k^+$.

[17] Tarvitaan mm. lineaarinen-järjestys, hyvä-järjestys, transfiniitti induktio, transfiniitti rekursio, valinta-aksiooma, korvaus-aksiooma, strutuurien isomorfisuus, ordinaaliluvut jne.

[18] Struktuuriksi kutsumme järjestettyä paria, johon kuuluu joukko ja sille annettu hyvä-järjestys.

[19] Tämän todistamiseen tarvitsemme valinta-aksioomaa.

(b) C on k:n aito osajoukko. Tällöin koska $k \in T$, niin oletuksen nojalla $C \approx m$, missä $m \in k \in k^+$.

(c) Muussa tapauksessa $k \in C$. Tällöin $C = (C \cap k) \cup \{k\}$ ja $C \cap k$ on k:n aito osajoukko. Nyt koska $k \in T$, niin löytyy $m \in k$, jolla $C \cap k \approx m$. Olkoon sitten f bijektio joukolta $C \cap k$ joukkoon m; tällöin $f \cup \{\langle k, m\rangle\}$ on bijektio joukosta C joukkoon m^+. Nyt koska $m \in k$, niin voidaan helposti osoittaa että $m^+ \in k^+$. Siten $C \approx m^+ \in k^+$, eli $k^+ \in T$.

Siispä $T = \omega$ ja aputulos on käytössämme. □

Palataan sitten varsinaisesti haluttuun tulokseen.

Seuraus 14. *Jokainen äärellisen joukon osajoukko on äärellinen.*

Todistus. Olkoon $A \subseteq B$. Olkoon lisäksi $f : B \to \text{kard}(B) = m$ bijektio. Tällöin $A \approx f[A] \subseteq n$ ja äskettäin todistetun aputuloksen nojalla $f[A] \approx m$, jollekin $m \underline{\in} n$. Siispä ω:n transitiivisuuden nojalla $m \in \omega$ ja mielivaitainen osajoukko A on täten äärellinen. □

Määritellään sitten kahden kardinaaliluvun (äärettömän tai äärellisen) summa, tulo ja potenssi.

Määritelmä 15. Olkoon ρ ja τ mielivaltaisia kardinaalilukuja.

I $\rho + \tau = \text{kard}(P \cup T)$, missä P ja T ovat mitkä tahansa pistevieraat joukot varustettuna kardaaliluvuilla ρ ja τ.

II $\rho \cdot \tau = \text{kard}(P \times T)$, missä P ja T ovat mitkä tahansa joukot varustettuna kardinaaliluvuilla ρ ja τ.

III $\rho^\tau = \text{kard}({}^T P)$, missä P ja T ovat mitkä tahansa joukot varustettuna kardinaaliluvuilla ρ ja τ. (Tässä joukko ${}^T P$ on kaikkien funktioiden joukko joukosta T joukkoon P.)

Nyt olisi toivottavaa ja jopa välttämätöntä, että annettu määritelmä olisi hyvin määritelty, eli että kardinaaleja edustamaan valitut joukot P ja T eivät vaikuta tulokseen. Olisi myöskin toivottavaa, että yllä mainittu määritelmä ei riitele aiemmin antamamme määritelmän kanssa, koskien vastaavia operaatioita luonnollisten lukujen joukossa. (Tarkemmin jälleen kerran kirjasta [1], kappale 4.)

Ensinnäkin on mahdollista valita kaksi pistevierasta joukkoa P ja T, joille pätee kard P$= \rho$ ja kard T$=\tau$, sillä jos ensimmäinen valinta ei onnistu halutusti, niin voimme siirtää tarkastelun koskemaan joukkoja $P \times \{0\}$ ja $T \times \{1\}$, jolloin viimeistään joukot ovat pistevieraat.

Seuraavan tuloksen avulla saamme osoitettua, että määritelmämme on hyvin määritelty, eikä aiheuta ongelmia.

Lause 16. *Oletetaan että $P_1 \approx P_2$ ja $T_1 \approx T_2$.*

I Jos $P_1 \cap T_1 = P_2 \cap T_2 = \varnothing$. niin $P_1 \cup T_1 \approx P_2 \cup T_2$.

II $P_1 \times T_1 \approx P_2 \times T_2$.

III ${}^{T_1}K_1 \approx {}^{T_2}K_2$.

Todistus. Todistetaan ensimmäinen kohta: Nyt oletuksien nojalla löytyy bijektiiviset funktiot $f : P_1 \to P_2$ ja $g : T_1 \to T_2$. Määritellään halutuksi funktioksi.

$$h(x) = \begin{cases} f(x) & \text{jos } x \in P_1 \\ g(x) & \text{jos } x \in T_1 \end{cases}.$$

Tämä funktio toimii, sillä oletuksen mukaan relevantit leikkaukset olivat pistevieraat.

Todistetaan sitten toinen kohta: Määritellään nyt halutuksi funktioksi $h(\langle x, y\rangle) = \langle f(x), g(y)\rangle$, jolloin selvästi h on bijektio tarkasteltujen joukkojen välillä.

Todistetaan sitten viimeinen kohta: Määritellän tarkastellujen joukkojen välille kuvaus $h(j) = f \circ j \circ g^{-1}$, jolloin funktio on seuraavien huomioiden nojalla bijektio. Ensinnäkin $H(j)$ on funktio joukosta T_2 joukkoon P_2. Nyt jos j ja i ovat toisistaan eroavat funktiot joukoista T_1 joukkoon P_1, niin $j(t) \neq i(t)$, jollakin $t \in T_1$. Siten:

$$H(j)(g(t)) = f(j(t)) \neq f(i(t)) = H(i)(g(t)),$$

sillä f on injektio, ja edelleen $H(j) \neq H(i)$, eli H on injektio.

Surjektiivisuuden näyttämiseksi olkoon $d : T_2 \to P_2$ mielivaltainen. Tällöin $H(f^{-1} \circ d \circ g) = d$, joten H on todellakin surjektio, ja siten kaikkiaan bijektio.

Asia on siis kaikkinaisuudessaan selvä ja määritelmämme on hyvin asetettu. □

Toteamme seuraavaksi muutaman tosiasian äsken määritellyistä laskutoimituksista.

Lause 17. *Kaikille kardinaaliluvuille a, b ja c.*

1. $a + b = b + a$ *ja* $a \cdot b = b \cdot a$ *("vaihdannaisuus").*
2. $a + (b + c) = (a + b) + c$ *ja* $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ *("assosiatiivisuus").*
3. $a \cdot (b + c) = a \cdot b + a \cdot c$ *("distributiivisuus").*
4. $a^{b+c} = a^b \cdot a^c$.
5. $(a \cdot b)^c = a^c \cdot b^c$.
6. $(a^b)^c = a^{b \cdot c}$.

Todistus. Todistetaan vain kohdat (4) ja (5). Muut ovat suoraviivaisia. Lukijan kannattaa kuitenkin käydä vähintään mielessään jokainen kohta. Olkoot A, B ja C pistevieraita joukkoja siten, että $\mathrm{kard}A = a$, $\mathrm{kard}B = b$ ja $\mathrm{kard}C = c$.

Todistetaan ensin kohta (4). Nyt riittää osoittaa, että ${}^{B \cup C}\mathrm{A} \approx {}^{B}\mathrm{A} \times {}^{C}\mathrm{A}$. Määritellään funktio $H : {}^{B \cup C}\mathrm{A} \to {}^{B}\mathrm{A} \times {}^{C}\mathrm{A}$ siten, että $H(f) = (f\lceil B, f\lceil C)$.

I Nyt jos $f \neq g$, niin $f(m) \neq g(m)$ jollakin $m \in C \cup B$. Lisäksi m kuuluu vain toiseen joukoista pistevierauden nojalla. Edellisestä saadaan, että joko $f\lceil B \neq g\lceil B$ tai $f\lceil C \neq g\lceil C$, ja siten $H(f) = (f\lceil B), f\lceil C) \neq (g\lceil B, g\lceil C) = H(g)$, eli H on injektio.

II Olkoon $(f, y) \in {}^B\mathrm{A} \times {}^C\mathrm{A}$ mielivaltainen. Koska A ja C ovat pistevieraita, niin voidaan valita funktioksi $(f \cup y) \in {}^{B \cup C}\mathrm{A}$, jolloin selvästi $H(f \cup y) = (f, y)$, eli H on surjektio.

Edellisten kohtien nojalla H on bijektio, joten kohta (4) on selvä.

Todistetaan sitten kohta (5). Nytkin väite palautuu siihen, että tulee osoittaa yhtämahtavuus ${}^C(\mathrm{A} \times \mathrm{B}) \approx {}^C\mathrm{A} \times {}^C\mathrm{B}$.

Määritellään $H : {}^C(\mathrm{A} \times \mathrm{B}) \to {}^C\mathrm{A} \times {}^C\mathrm{B}$ siten, että $H(f) = (f_1, f_2)$, missä $f_1 : C \to A$, $f_1(x) = a \in A$, kun $f(x) = (a, b)$, ja vastaavasti $f_2 : C \to B$, $f_2(x) = b \in B$.

I Olkoon $f \neq g$, kun $f, g \in {}^C(\mathrm{A} \times \mathrm{B})$.
Tällöin $f(x) \neq g(x)$, jollakin $x \in C$. Siten $a_1 \neq a_2$ tai $b_1 \neq b_2$, ja $H(f) = (f_1, f_2) \neq (f_3, f_4) = H(g)$, missä f_i:t saadaan määritellyistä funktioista.
Siispä H on injektio.

II Olkoon $(p, g) \in {}^C\mathrm{A} \times {}^C\mathrm{B}$ mielivaltainen. Valitaan $f : C \to A \times B$ siten, että $f(x) = (p(x), g(x)) \in A \times B$, jolloin $H(f) = (p, g)$, eli H on surjektio.

Edellisten kohtien nojalla H on bijektio, eli asian on taas selvä. □

Kun edellisessä lauseessa (17) palautetaan väitteet yhtämahtavuuksien osoittamiseen, niin itseasiassa kohdissa (1), (3) ja (5) pätee yhtämahtavien joukkojen välillä myös yhtäsuuruus, kun taas lopuissa kohdissa yhtäsuuruus ei päde, mikä voidaan helposti osoittaa. Kuitenkin joukkojen välille voidaan muodostaa niin sanottu luonnollinen bijektio.

Seuraava teoreema sanoo, että äsken määrittelemämme kardinaalilukujen laskutoimitukset, eivät riitele luonnollisten lukujen vastaavien toimitusten kanssa. Sivuutamme kuitenkin todistuksen, sillä se vaatisi esitystä luonnollisten lukujen joukko-opillisesta konstruktiosta (taas tuttu kirja [1], kappale 4.).

Lause 18. *Olkoon m ja n äärellisiä kardinaaleja. Tällöin $m + n = m +_\omega n$, $m \cdot n = m \cdot_\omega n$ ja $m^n = m^n$. Tässä $+_\omega$, $\cdot_\omega$ ja viimeisessä oikeanpuolimmainen m^n viittaavat luonnollisten lukujen vastaaviin laskutoimituksiin, niissä muodoissa, joissa ne tavanomaisesti tunnemme.*

Esimerkki 19. Määritellään joukon K permutaatio miksi tahansa bijektioksi joukolta K joukkoon K. Voimme nyt määritellä kertomaoperaation kardinaaliluvuille yhtälöllä

$$k! = \text{kard } \{f|\text{ f on permutaatio } K\text{:lla}\},$$

missä K on mikä tahansa joukko, jonka kardinaali on k. Näytetään että $k!$ on hyvin määritelty.

Todistus. Olkoot K ja R mielivaltaisia joukkoja, joilla on kard$K = a$ ja kard$R = a$. Tällöin $K \approx R$, eli on olemassa bijektio $f : K \to R$. Nyt tulee näyttää, että kard$\{j|j$ on permumaatio K:lla$\}$ = kard$\{g|$ g on permumaatio R:llä$\}$. Merkitään tarkasteltavia joukkoja järjestyksessä T_1 ja T_2. Haluamme nyt määritellä bijektion joukkojen välille.

Määritellään $H : T_1 \to T_2$ siten, että $H(j) = f \circ j \circ f^{-1}$. Tällöin H on selvästi funktio joukolta T_1 joukkoon T_2, ja $H(j)$ on funktio joukosta R joukkoon R. Tulee vielä osoittaa, että H on bijektio.

I Olkoon $j_1, j_2 \in T_1$, mielivaltaisista toisistaan eroavia bijektioita. Tällöin niiden arvo jossain pisteessä $i \in K$ eroaa toisistaan, ja edelleen koska $f : K \to R$ on bijektio, niin $f(j_1(i)) \neq f(j_2(i))$. Nyt koska $f(i) \in R$ ja $H(j_1)(f(i)) = f(j_1(i)) \neq f(j_2(i)) = H(j_2)(f(i))$, niin $H(j_1) \neq H(j_2)$, eli H on injektio.

II Olkoon $g \in T_2$ mielivaltainen. Valitaan nyt $f^{-1} \circ g \circ f \in T_1$, mikä bijektioiden yhdistelmänä todellakin on bijektio. Nyt $H(f^{-1} \circ g \circ f \in T_1) = g$, eli H on täten surjektio.

Edellisten kohtien nojalla H on bijektio, ja siten aiemman tarkastelun nojalla $a!$ on hyvin määritelty. $\square$

Olemme tähän mennessä osoittaneet joukkoja yhtämahtaviksi, mutta milloin voisimme sano että joukko B on suurempi kuin joukko A? Vastauksesta riippumatta ainakin se onnistuu seuraavaa määritelmää käyttäen.

Määritelmä 20. Joukko B dominoi joukkoa A jos ja vain jos on olemassa injektiivinen kuvaus joukosta A joukkoon B. Tällöin merkitsemme $A \preceq B$.

Määritellään sitten kardinaaliluvuille, että kard $A \leq$ kard $B \leftrightarrow A \preceq B$. Taas pitäisi osoittaa, että äskeinen määritelmä on hyvin määritelty. Sivuutamme sen tässä kuitenkin tilanpuutteen vuoksi (ks. [1] sivut 145–146).

Nyt olisi asianmukaista, jos äskeinen määritelmämme toimisi kuten *järjestykseltä* voisi olettaa. Täsmällisemmin haluamme, että seuraavat pätevät kaikille kardinaaliluvuille a, b ja c:

1. $a \leq a$ (”refleksiivisyys”),
2. $a \leq b \leq c \to a \leq c$ (”transitiivisuus”),
3. $a \leq b$ ja $b \leq a \to a = b$ (”antisymmetrisyys”),
4. $a \leq b$ tai $b \leq a$ (”täydellisyys”).

Osoittautuu, että tämä järjestys on jopa hyvä. Nyt kohdat (1) ja (2) ovat varsin triviaaleja, mutta (3) kohta on kiinnostava, joten todistamme sen seuraavana teoreemana.

Tarvitsemme valinta-aksioomaa, jotta voimme määritellä ja todistaa tarvittavat aputulokset äärettömiä kardinaalien laskutoimituksia varten.

Lause 21. *Jos $A \preceq B$ ja $B \preceq A$, niin $A \approx B$ (Schröder-Bernsteinin teoreema).*

Todistus. Oletuksen nojalla löytyy injektiiviset funktiot $f : A \to B$ ja $g : B \to A$. Määritellään sitten rekursiivisesti C_n siten, että

$$C_0 = A \setminus \operatorname{ran} g \text{ ja } C_{n^+} = g[f[C_n]].$$

Määritellään sitten funktio $h : A \to B$ siten, että

$$h(x) = \begin{cases} f(x) & \text{jos } x \in C_n \text{ jollekin } n \\ g^{-1}(x) & \text{muuten} \end{cases}$$

Edellisessä täytyy huomata , että valinta toimii, sillä g on injektio ja $x \in \operatorname{ran} g$. Osoitetaan, että h on bijektio, jolloin asia on selvä:

Olkoon sitten $x_1, x_2 \in A$ siten, että $x_1 \neq x_2$. Koska f ja g^{-1} ovat molemmat injektiivisiä, niin riittää tarkastella tapausta, jossa $x_1 \in C_m$ ja $x_2 \notin \bigcup_{n\in\omega} C_n$. Tässä tapauksessa

$$h(x_1) = f(x_1) \in f[C_m],$$

kun taas

$$h(x_2) = g^{-1}(x_2) \notin f[C_m],$$

sillä, muuten $x_2 \in C_{m^+}$. Siispä $h(x_1) \neq h(x_2)$ ja h on injektio.

Osoitetaan vielä, että h on surjektio. Selvästi ainakin $f[C_n] \subseteq \operatorname{ran} h$, sillä $f[C_n] = h[C_n]$. Oletetaan sitten, että $y \in B \setminus \bigcup_{n\in\omega} f[C_n]$. Selvästi $g(y) \neq C_0$ ja $g(y) \notin C_{n^+}$, koska $C_{n^+} = g[f[C_n]], y \notin f[C_n]$ ja g on injektio. Siispä $h(g(y)) = g^{-1}(g(y)) = y$, eli $y \in \operatorname{ran} h$. Siispä h on bijektio ja täten $A \approx B$. □

Lause 22. *$\mathbf{R} \approx {}^{\omega}2$, ja siten $\mathbf{R} \approx \mathcal{P}\omega$.*

Todistus. Todistetaan väite käyttämällä Schröder-Bernsteinin teoreemaa.

Näytetään ensin, että $\mathbf{R} \preceq {}^{\omega}2$. Tämän osoittamiseksi konstruoimme injektiivisen funktion avoimelta väliltä (0,1) joukkoon ${}^{\omega}2$. Tämähän riittää sillä tiedetään, että $\mathbf{R} \approx (0,1)$. Funktio määritellään käyttämällä binääriesityksiä reaaliluvuille: kuvataan esimerkiksi reaaliluku, jonka binääriesitys on $0,1100010\ldots$ funktioksi joukossa ${}^{\omega}2$, jonka arvot ovat järjestyksessä 1, 1, 0, 0, 0, 1, 0,. . .,. Yleisesti reaaliluvulle $x \in (0,1)$, olkoon $H(z) : \omega \to 2$, jonka arvo n:ssä on yhtäkuin $(n+1)$:des bitti z:n binääriesityksessä. Selvästi H on ainakin injektio, ja lisäksi, jotta H olisi hyvin määritelty, niin valitaan aina päättymätön binääriesitys. Kun taas näytetään, että ${}^{\omega}2 \preceq \mathbf{R}$, niin käytetään desimaaliesityksiä: funktio joukossa ${}^{\omega}2$, jonka arvot ovat järjestyksessä 1, 1, 0, 0, 0, 1, 0, . . . kuvataan reaaliluvuksi, jonka desimaaliesitys on 0.1100010,. . ..
Kuvaus on selvästi injektio. □

Esimerkki 23. Näytetään suoralla todistuksella, että jokaiselle joukolle S pätee $S \preceq {}^{S}2$, mutta S ei ole yhtämahtava joukon ${}^{S}2$ kanssa.

Todistus. Olkoon siis S mielivaltainen joukko.

Määritellään kuvaus $f_0 : S \to {}^{S}2$ siten, että $f_0(x) = P : S \to 2$, missä

$$P(a) = \begin{cases} 1 & \text{jos } a = x \\ 0 & \text{muuten.} \end{cases}$$

Selvästi f_0 on injektio, joten $S \preceq {}^S 2$.

Olkoon sitten $f : S \to {}^S 2$ mielivaltainen.

Näytetään, että F ei voi olla surjektio, jolloin ei siis ole olemassa bijektiota $G : S \to {}^S 2$.

Määritellään nyt $g(x) = 1 - f(x)(x)$, $g : S \to 2$. Nyt

$$g(x) = \begin{cases} 0 & \text{kun } f(x)(x) = 1 \\ 1 & \text{kun } f(x)(x) = 0, \end{cases}$$

eli erityisesti $g \neq f(x)$ kaikilla $x \in S$, ja siten f ei ole surjektio.

Siispä asia on selvä. □

Lause 24. *Olkoon α ja β kardinaalilukuja, joista suurempi on ääretön ja pienempi on nollasta eroava. Tällöin pätee, että* $\alpha + \beta = \alpha \cdot \beta = \max(\alpha, \beta)$.

Todistus. Todistuksessa tarvitaan valinta-aksioomaan erästä muotoilua (Zornin lemma) ja aputulosta, jonka mukaan jokaiselle kardinaalille $\alpha \cdot \alpha = \alpha$. Todistus löytyy kirjan [1] sivuilta 164 ja tarvittavan lemman todistus saman kirjan sivuilta 162–163. □

Lause 25. *Olkoon α ja β kardinaalilukuja, joista suurempi on ääretön ja pienempi on suurempi tai yhtäsuuri kuin 2. Tällöin* $\max(\alpha, 2^\beta) \leq \alpha^\beta \leq \max(2^\alpha, 2^\beta)$.

Todistus.

1. Oletetaan ensin, että $2 \leq \alpha \leq \beta$. Tällöin ainakin $\alpha \leq \beta \leq 2^\beta \leq \alpha^\beta$. Lisäksi
$$\alpha^\beta \leq (2^\alpha)^\beta = 2^{\alpha \cdot \beta} = 2^\beta \leq \alpha^\beta,$$
joten yhtäsuuruus pätee. Siispä ainakin tässä tapauksessa väitteen epäyhtälöt pätee.

2. Oletetaan sitten, että $2 \leq \beta \leq \alpha$. Nyt jos $\alpha \leq 2^\beta$, niin $2^\beta \leq \alpha^\beta \leq (2^\beta)^\beta = 2^{\beta \cdot \beta} = 2^\beta$, joten yhtäsuuruus $\alpha^\beta = 2^\beta$ pätee. Jos taas $2^\beta \leq \alpha$, niin $\alpha^\beta \leq \alpha^\alpha = 2^\alpha$, eli taas epäyhtälöt pätee.

□

Lause 26. *Olkoon a, b ja c kardinaalilukuja. Tällöin:*

1. $a \leq b \to a + c \leq b + c$,
2. $a \leq b \to a \cdot c \leq b \cdot c$,
3. $a \leq b \to a^c \leq b^c$,
4. $a \leq b \to c^a \leq c^b$, *jos ei ole niin, että molemmat kardinaaliluvuista a ja c ovat yhtäsuuria kuin nolla.*

Todistus. Olkoon A, B ja C joukkoja, joiden kardinaalit ovat a, b ja c. Tällöin joukon ${}^C A$ kardinaali on a^c ja niin edelleen. Oletetaan sitten, että $a \leq b$, jolloin voimme valita joukot A, B ja C siten, että $A \subseteq B$ ja $B \cap C = \varnothing$.

Nyt ensimmäiset kolme kohtaa ovat selviä, sillä esimerkiksi $A \cup C \subseteq B \cup C$ ja muut voidaan todeta analogisesti. Viimeisessä kohdassa jaamme tarkastelun kahteen alatapaukseen:

I Oletetetaan ensin, että $c = 0$, jolloin $a \neq 0$. Tällöin $c^a = 0 \leq c^b$, joten tämä tapaus on selvä.

II Oletetaan sitten, että $c \neq 0$. Tällöin löytyy jokin $\kappa \in C$. Määritellään jokaiselle $f \in {}^A C$ funktio $G(f) : B \to C$, jolle

$$G(f)(x) = \begin{cases} f(x) & \text{jos } x \in A \\ \kappa & \text{muuten.} \end{cases}$$

Tällöin $G : {}^A C \to {}^B C$ ja G on selvästi injektio. □

Teoreema ei pidä kuitenkaan paikkaansa, jos järjestys $\leq$ korvataan järjestyksellä $<$. Tämä voidaan helposti nähdä, kun käytetään vastaesimerkeissä äärettömiä kardinaalilukuja. Annetaan vastaesimerkit:

Olkoot ensin $a = 1$, $b = 2$ ja $c = \aleph_0$.

I Nyt $1 < 2$, mutta $1 + \aleph_0 = \aleph_0 = 2 + \aleph_0$.

II Edelleen $1 < 2$, mutta $1 \cdot \aleph_0 = \aleph_0 = 2 \cdot \aleph_0$

III Myöskään kohta (3) ei toimi uudistettuna. Olkoot nyt $a = 1$, $b = 2$ ja $c = 0$. Nyt $A \subset B$, mutta ${}^{\varnothing}\mathrm{A} = \{\varnothing\} = {}^{\varnothing}\mathrm{B}$, eli yhtäsuuruus on kardinaalien potenssien välillä voimassa.

IV Järjestys ei myöskään säily kohdassa (4). Taaskin $1 < 2$, mutta $\aleph_0^1 = \aleph_0 = \aleph_0 \cdot \aleph_0 = \aleph_0^2$.

Lemma 27. *Jos $B \neq \varnothing$, niin $B \preceq A$ jos ja vain jos on olemassa surjektio joukosta A joukkoon B.*

Todistus. Tähän lemmaan tarvittavan lemman todistus löytyy kirjan [1] sivuilta 48–49 ja itse lemman todistus löytyy sivuilta 155–156. Todistuksessa tarvitaan erityisesti valinta-aksioomaa. □

Lemma 28. *Jokaiselle joukolle A pätee kard$\mathcal{P}A = 2^{kardA}$.*

Todistus. Todistuksessa käytetään tietoa ${}^A 2 \approx \mathcal{P}A$. Tarkka todistus löytyy kirjan [1] sivulta 141. □

Lemma 29. *Jokaiselle kardinaaliluvulle α pätee $\alpha < 2^\alpha$.*

Todistus. Seuraa tiedosta $A \preceq \mathcal{P}A$ kaikilla joukoilla A, edellisestä lemmasta ja Cantorin teoreemasta (lause 6). □

Edellisen aputuloksen seuraksena saamme, että ei ole olemassa suurinta kardinaalilukua.

Esimerkki 30. Näytetään viimeisenä, että äärettömälle kardinaalille α pätee $\alpha! = 2^\alpha$, missä $\alpha! = \text{kard } \{f \mid \text{f on permutaatio } A\text{:lla}\}$, jossa A on mikä tahansa joukko, jonka kardinaali on α.

Todistus. Merkitään ensin

$$E_A := \{f|f \text{ on } A\text{:n permutaatio}\}$$

ja

$$E_{A\times 2} := \{f|f \text{ on } A \times 2\text{:n permutaatio}\},$$

ja osoitetaan, että $E_A \approx E_{A\times 2}$. Muodostetaan tätä varten funktio $K : E_A \to E_{A\times 2}$ siten, että $K(f) = g^{-1} \circ f \circ g$, missä $g : E_{A\times 2} \to A$ on bijektio (tällainen g löytyy, sillä A on ääretön ja siten $A \times 2 \approx A$). K voidaan osoitaa helposti bijektioksi, joten $E_A \approx E_{A\times 2}$.

1. Osoitetaan ensin, että äärettömälle kaardinaalille α pätee $\alpha^\alpha = 2^\alpha$. Nyt

   $$\alpha^\alpha \leq (2^\alpha)^\alpha = 2^{\alpha\cdot\alpha} = 2^\alpha \leq \alpha^\alpha,$$

   joten yhtäsuuruus pätee. Siispä aputuloksen nojalla $\alpha! \leq \alpha^\alpha = 2^\alpha$, sillä $E \subseteq {}^A A$.

2. Osoitetaan sitten, että $2^\alpha \leq \alpha!$. Koska nyt $E_A \approx E_{A\times 2}$, niin riittää osoittaa, että $\mathcal{P}(A) \preceq E_{A\times 2}$. Muodostetaan tavoitetta varten funktio $H : \mathcal{P}(A) \to E_{A\times 2}$ siten, että $H(B) = f$, missä

   $$f(a, b) = \begin{cases} (a, b) & \text{kun } a \in B \\ (a, 1-b) & \text{kun } a \notin B, \end{cases}$$

   Nähdään, että f on selvästi joukon $A \times 2$ permutaatio. Lisäksi jos $H(B_1) = H(B_2)$, niin kuvapisteenä saadun f:n määritelmästä saadaan, että $a \in B_1$ jos ja vain jos $a \in B_2$, eli $B_1 = B_2$. Täten H on todellakin halutun kaltainen injektio, ja siten $2^\alpha = \text{kard}(\mathcal{P}(A)) \leq \text{kard}(E_{A\times 2}) = \alpha!$.

Siispä edellisten kohtien nojalla sekä $\alpha! \leq 2^\alpha$ että $2^\alpha \leq \alpha!$, joten Schröder-Bernsteinin teoreeman nojalla $\alpha! = 2^\alpha$, ja asia on täten selvä. □

5 Lopetus

Olemme tässä esityksessä esitelleet tavan vertailla joukkojen kokona, niin äärellisessä kuin äärettömässä tapauksessa. Tämän asian johdannaisena saimme myös kardinaalilukujen määritelmän ja niiden peruslaskutoimituksia. Olemme lisäksi näyttäneet, että on monenlaisia joukko-opillisia äärettömyyksiä. Seuraavaksi luontevaa olisi määritellä esimerkiksi *seuraajakardinaalit* ja käsitellä perusteellisemmin ordinaalilukuja, mutta vaihtoehtoja on varmasti lukuisia. Yleisesti voidaankin todeta, että joukko-opilla on alku, muttei loppua.[1]

Lähdeluettelo

[1] Herbert B. Enderton: *Elements of set theory.* Academic Press, An Imprint of Elsevier, 1977, Elsevier.

[2] Lassi Kurittu: aksiomaattinen joukko-oppi, luentomoniste http://users.jyu.fi/~lkurittu/joukko-oppia.pdf. (luettu 27.4.2016)

[3] John Stillwell *Mathematics and its history* Springer science + Business media, 2010.

[4] Imre Lakatos *Proofs and refutations* Cambridge University Press, 1976.

[5] J J O'Connor, E F Robertson: Zenon Elealaisen elämänkerta http://www-groups.dcs.st-and.ac.uk/~history/Biographies/Zeno_of_Elea.html (luettu 27.4.2016)

[6] Ralf Schindler, John Steel; joukko-opin avoimia ongelmia http://wwwmath.uni-muenster.de/logik/Personen/rds/list.html (luettu 27.4.2016)

[7] Math-stackexchange http://math.stackexchange.com/questions/53770/defining-cardinality-in-the-absence-of-choice (luettu 27.4.2016)

[8] Alexander George ja Daniel J. Velleman *Philosophies of mathematics*

[9] Juha Oikkonen, Jouko Väänänen: *Katsauksia matematiikan historiaan.* 1982 oy Gaudeamus ab

[10] Susan Haack *Philosophies of logic* Cambridge University Press, 1978, 15:sta printti 2006.