TURUN YLIOPISTO

Valinta-aksiooma ja sen rooli matematiikassa

Leo Karppinen

Pro gradu -tutkielma
Joulukuu 2023

Tarkastajat:
Prof. Vesa Halava
Yliopistotutkija Ville Salo

MATEMATIIKAN JA TILASTOTIETEEN LAITOS

TURUN YLIOPISTO
Matematiikan ja tilastotieteen laitos

Leo Karppinen: Valinta-aksiooma ja sen rooli matematiikassa
Pro gradu -tutkielma, 29 s.
Matematiikka
Joulukuu 2023

Tässä tutkielmassa esitellään valinta-aksiooma ja käsitellään lauseita eri matematiikan aloilta, joiden todistukset edellyttävät valinta-aksioomaa. Lisäksi tutkitaan lyhyesti, mihin sitä ei tarvita. Tutkielmassa perehdytään myös Vitalin joukkoihin ja Banachin-Tarskin paradoksiin, joihin liittyvät lauseet todistetaan seikkaperäisesti. Lopuksi esitetään ratkaisuehdotus, jonka tavoitteena on välttää Banachin-Tarskin paradoksi.

Asiasanat: valinta-aksiooma, joukko-oppi, Banachin-Tarskin paradoksi.

Sisällys

1 Johdanto

1.1 Pohjatiedot

Lukemista helpottaa, jos seuraavat asiat ovat yleisellä tasolla tuttuja:

1. Joukko-opin perusteet
2. Ensimmäisen kertaluvun logiikan ja kaavojen perusteet
3. Ordinaali- ja kardinaalilukujen perustiedot
4. Kunnan käsite
5. Aksiomaattis-deduktiivisen teorian käsite
6. Mittateorian perusteet, erityisesti Lebesguen mitta
7. Ainakin lievästi filosofinen asenne ja avoin mieli

Lähtökohtaisesti väitteet todistetaan täsmällisesti ja ilman syvällisiä taustaoletuksia, mutta jotkin lauseet, jotka eivät ole varsinaista ydinasiaa, esitetään todistuksetta, ja todistuksiin vain viitataan.

1.2 Mikä on valinta-aksiooma?

Valinta-aksiooma on Zermelo-Fraenkel -joukko-opin (lyhennetään ZF) aksiooma, josta on kiistelty 1900-luvulla varsin paljon [2, 3]. Valinta-aksiooma voidaan muotoilla monilla eri tavoilla, jotka ovat keskenään yhtäpitäviä, mutta yleisimmin esitettävä ja helpoimmin ymmärrettävä muotoilu on seuraava:

Aksiooma 1. VALINTA-AKSIOOMA. Jokaiselle joukkokokoelmalle X, jonka joukot ovat epätyhjiä ja erillisiä, on olemassa joukko Y, joka sisältää tarkalleen yhden jäsenen jokaisesta joukosta $x \in X$. Toisin muotoiltuna $Y \cap x = \{z\}$ jollain $z \in x$, kaikilla $x \in X$.

Intuitiivisesti ajateltuna valinta-aksiooma vaikuttaa itsestäänselvältä, ja äärellisille joukoille se voidaankin johtaa muista ZF-aksioomista. Kuitenkin aksioomalla on joitain hätkähdyttäviä seurauksia, jotka tuntuvat joko järjenvastaisilta tai ovat vähintäänkin teoreettisesti hankalia. Tosin ilman valinta-aksioomaa monet hyödylliset tulokset eivät ole todistettavissa ja jotkin yhtälailla hankalat hirviöt syntyvät kuin valinta-aksioomaa käytettäessä. Niels Bohrilta peräisin oleva lainaus tiivistää asian osuvasti.

"There are two kinds of truth. To the one kind belong statements so simple and clear that the opposite assertions obviously could not be defended. The other kind, the so-called "deep truths", are statements in which the opposite also contains deep truth." -Niels Bohr [2]

1.3 Merkinnät ja niiden selitykset

Listataan seuraavaksi tässä tutkielmassa käytettyjä merkintöjä.

1. $dom(R)$ = relaation R *määrittelyjoukko*, eli pisteet, joissa se on määritelty. Sitä kutsutaan myös relaation *vasemmaksi projektioksi.* Relaatio on kahden joukon karteesisen tulon osajoukko.

2. $ran(R)$ = relaation R *arvojoukko* tai *maalijoukko* (engl. *range*), eli pisteet, jotka se voi saada arvoikseen. Sitä kutsutaan myös relaation *oikeaksi projektioksi.*

3. $F(A)$ = joukon A kuva funktiossa F, eli funktiolla kuvataan jokainen joukon A alkio.

4. $F|A$ = funktion F *rajoittuma* joukkoon A, eli sen määrittelyjoukoksi otetaan joukko $A \subseteq dom(F)$.

5. $P(X)$ = joukon X *potenssijoukko*, eli joukko, jonka alkioina ovat joukon X kaikki osajoukot.

6. $seq(t)$ = jos alkio t kuuluu johonkin (järjestettyyn) joukkoon A, niin $seq(t) = \{a \in A \mid a < t\}$.

7. $B \preccurlyeq A$ = joukko A *dominoi* joukkoa B. Ks. määritelmä 4. Banachin-Tarskin paradoksia käsittelevässä luvussa 5.3 merkintä tarkoittaa, että joukko B on *yhtähajotettava* jonkin joukon A osajoukon kanssa. Ks. määritelmä 32.

8. $A \sim B$ = joukko A on *yhtämahtava* joukon B kanssa. Ks. määritelmä 4. Luvussa 5.3 merkintä tarkoittaa, että A ja B ovat *yhtähajotettavia.* Ks. määritelmä 31.

9. $|X|$ = joukon X alkioiden lukumäärä eli *kardinaliteetti.*

10. $\aleph_0$ = luonnollisten lukujen joukon kardinaliteetti.

11. $\dot{\mathbb{R}} = \mathbb{R} \cup \{\infty\}$

12. SO_3 = yksikköpallopinnan kiertojen ryhmä.

13. G_3 = avaruuden $\mathbb{R}^3$ isometrioiden ryhmä.

2 Valinta-aksiooman eri muodot

Valinta-aksioomalla on monia keskenään yhtäpitäviä muotoja. Seuraavassa lauseessa esitellään niistä neljä, jotka sanovat käytännössä kaikki saman asia, eli että joukoista voidaan poimia yksi alkio. Lisäksi on olemassa lauseita, jotka ovat yhtäpitäviä valinta-aksiooman kanssa, mutta sanovat kuitenkin jotain muuta. Niitä käsitellään myöhemmissä luvuissa. Kappale perustuu kirjaan [1].

Lause 1. *Seuraavat väitteet ovat yhtäpitäviä.*

1. *Valinta-aksiooma I: Jokaiselle relaatiolle R on olemassa sellainen funktio F, että $F \subseteq R$ ja $dom(F) = dom(R)$.*

2. *Valinta-aksiooma II: Jos H on funktio, $dom(H) = I$ ja $H(i) \neq \emptyset$ kaikilla $i \in I$, niin on olemassa sellainen funktio f, että $dom(f) = I$ ja $f(i) \in H(i)$ kaikilla $i \in I$. Tämä muotoilu tarkoittaa siis sitä, että epätyhjien joukkojen karteesinen tulo on epätyhjä, ja sitä kutsutaan myös multiplikatiiviseksi aksioomaksi.*

3. *Valinta-aksiooma III: Jokaiselle joukolle A on olemassa sellainen funktio $F : P(A)\backslash\{\emptyset\} \to A$, että $F(B) \in B$ kaikilla $B \in P(A)$.*

4. *Valinta-aksiooma IV: Jokaiselle joukkokokoelmalle X, jonka joukot ovat epätyhjiä ja alkiovieraita, on olemassa joukko Y, joka sisältää tarkalleen yhden jäsenen jokaisesta joukosta $x \in X$. Toisin muotoiltuna $Y \cap x = \{z\}$ jollain $z \in x$ ja kaikilla $x \in X$.*

Todistus. $1 \Rightarrow 2$. Olkoon H funktio, $dom(H) = I$ ja $H(i) \neq \emptyset$ kaikilla $i \in I$. Määritellään relaatio

$$R = \{(i, x) \mid i \in I \text{ ja } x \in H(i)\}.$$

Tällöin kohdan 1 mukaan on olemassa sellainen funktio F, että $dom(F) = dom(R) = I$ ja $F \subseteq R$. Nyt $(i, F(i)) \in F$ kaikilla $i \in I$, eli $(i, F(i)) \in R$, joten $F(i) \in H(i)$.

$2 \Rightarrow 4$. Olkoon X joukko epätyhjiä ja alkiovieraita joukkoja. Olkoon H identiteettikuvaus joukossa X. Tällöin $H(A) \neq \emptyset$ kaikilla $A \in X$. Tällöin kohdan 2 mukaan on olemassa sellainen funktio f, että $dom(f) = dom(H) = X$ ja $f(A) \in A$ kaikilla $A \in X$. Olkoon $C = ran(f)$. Tällöin $B \cap C = \{f(B)\}$ kaikilla $B \in X$. Koska $f(B) \in B$, niin $\{f(B)\}$ on yhden alkion joukko ja koska kaikki B ovat alkiovieraita, niin kohdan 4 väite toteutuu.

$4 \Rightarrow 3$. Olkoon X jokin joukko. Määritellään joukko

$$A = \{\{B\} \times B \mid B \subseteq X \text{ ja } B \neq \emptyset\}.$$

Tällöin jokainen joukon A jäsen on epätyhjä. Jos $(x, y) \in (\{B\} \times B \cap \{C\} \times C)$, niin $x = B = C$, joten joukon A jäsenet ovat alkiovieraita. Olkoon D sellainen joukko, että kaikilla B

$$D \cap (\{B\} \times B) = \{(B, x)\}, \text{ missä } x \in B.$$

D on olemassa kohdan 4 nojalla. Muodostetaan uusi joukko $F = D \cap \bigcup A$. Tällä saadaan joukon A ulkopuoliset joukot ulos. Kaikki joukon F alkiot kuuluvat johonkin joukkoon $(\{B\} \times B)$, eli ne ovat muotoa (B, x). Koska

$$F \cap (\{B\} \times B) = \{(B, x)\},$$

niin jokaisella epätyhjällä $B \subseteq X$ on olemassa sellainen yksikäsitteinen $x \in B$, että $(B, x) \in F$. Tällöin F on funktio, ja $F(B) = x \in B$, eli F on joukon X valintafunktio.

$3 \Rightarrow 1$. Olkoon R mielivaltainen relaatio. Tällöin kohta 3 takaa valintafunktion V olemassaolon joukolle $ran(R)$, siis $V(B) \in B$ kaikilla $B \subseteq ranR$, $B \neq \emptyset$. Määritellään funktio F. Funktion määrittelyjoukko on $dom(F) = dom(R)$ ja

$$F(x) = V(\{y \mid xRy\}).$$

Nyt koska V on valintafunktio, niin $F(x) \in \{y \mid xRy\}$, eli $(x, F(x)) \in R$, joten $F \subseteq R$. $\square$

3 Mihin valinta-aksioomaa tarvitaan?

Valinta-aksioomaa tarvitaan monien eri matematiikan alojen lauseiden todistamiseen. Osa näistä tuloksista on hyödyllisiä, intuitiivisia ja jopa perustavanlaatuisia siinä määrin, että valinta-aksiooman hylkääminen johtaa joihinkin kummallisiin lopputuloksiin.

3.1 Hyvinjärjestyslause

Yksi keskeisimpiä lauseita, jonka todistus edellyttää valinta-aksioomaa tai jotain sen vastinetta, on hyvinjärjestyslause. Valinta-aksioomaa oli käytetty eri muodoissaan jo ennen 1900-lukua, mutta 1904 Zermelo käytti aksioomaa tietoisesti todistaakseen, että jokainen joukko voidaan hyvinjärjestää. Zermelo julkaisi päivitetyn version artikkelistaan vuonna 1908. [2] Vaikka tulos ei olekaan erityisen intuitiivinen, se on joissain tapauksissa varsin hyödyllinen. Tarvittavat apulauseet ja pohjatiedot jätetään tässä todistamatta, koska ne eivät tarkalleen ottaen kuulu itse aiheeseen, ja se johtaisi turhan pitkälle sivuraiteelle. Todistukset ja tarkemmat selitykset löytyvät lähteen [1] luvusta 7.

Määritelmä 1. Relaatiota $<\subseteq A \times A$ sanotaan *hyvinjärjestykseksi joukossa* A, jos se toteuttaa seuraavat ehdot:

1. Relaatio $<$ on *transitiivinen*, eli jos $x < y$ ja $y < z$, niin $x < z$ kaikilla $x, y, z \in A$.
2. Kaikilla $x, y \in A$ joko $x < y,\ x = y,$ tai $x > y$.
3. Kaikilla epätyhjillä osajoukoilla $B \subseteq A$ on olemassa sellainen $x \in B$, että kaikilla $y \in B$ $x < y$ tai $x = y$ (merkitään $x \leq y$).

Lause 2. Transfiniittinen rekursio -skeema. *Olkoon $\gamma(x, y)$ ensimmäisen kertaluvun kaava ja $<$ hyvinjärjestys joukossa A. Jos mille tahansa funktiolle f on olemassa sellainen yksikäsitteinen y, että $\gamma(f, y)$ on tosi, niin silloin on olemassa sellainen yksikäsitteinen funktio, että*

1. *$dom(F) = A$ ja*
2. *$\gamma(F|seq(t), F(t))$ kaikilla $t \in A$.*

Todistus. [1], s.180. □

Määritelmä 2. Olkoon A joukko ja $<$ hyvinjärjestys. Paria $(A, <)$ sanotaan *hyvinjärjestetyksi struktuuriksi*. Kaavalla $y = ran(x)$ ja transfiniittisella rekursiolla voidaan määritellä sellainen funktio E, että

1. $dom(E) = A$ ja
2. $E(t) = ran(E|seq(t)) = \{E(x) \mid x < t\}$.

Joukko $a = ran(E)$ on struktuurin $(A, <)$ $\in$–kuva (sanotaan "epsilon-kuva").

Määritelmä 3. Olkoon $<$ hyvinjärjestys joukossa A. Joukon A *ordinaaliluku* on struktuurin $(A, <)$ $\in$–kuva. Ordinaaliluku a on joukko, joka on jonkin hyvinjärjestetyn struktuurin $\in$–kuva. Ordinaaliluvut ovat siis hyvinjärjestettyjä joukkoja. Jatkossa kaikkien ordinaalilukujen luokkaa merkitään *Ord*.

Lause 3. *Ordinaalilukujen luokka on hyvinjärjestetty relaation* $\epsilon_A = \{(x, y) \in A \times A \mid x \in y\}$ *suhteen, missä* $A = Ord$.

Todistus. [1] s. 192. □

Määritelmä 4. Sanotaan, että joukko A *dominoi* joukkoa B, jos on olemassa injektio $f : B \to A$. Merkitään $B \preccurlyeq A$. Jos joukkojen A ja B välillä on bijektio, niin sanotaan, että ne ovat *yhtämahtavia* ja merkitään $A \sim B$.

Lause 4. *Jokaiselle joukolle* X *on olemassa (pienin) ordinaaliluku, jota se ei dominoi. Tätä lukua kutsutaan joukon* X *Hartogin luvuksi.*

Todistus. [1] s.195. □

Lemma 1. *Jos* $<_A$ *on hyvinjärjestys joukossa* A*, ja* $f : B \to A$ *on bijektio, niin joukko* B *voidaan hyvinjärjestää.*

Todistus. Olkoon $b_1, b_2 \in B$. Määritellään järjestys $<_B$ seuraavasti:

$$b_1 <_B b_2, \text{ jos } f(b_1) <_A f(b_2).$$

Koska $<_A$ on hyvinjärjestys, niin $<_B$ on myös hyvinjärjestys. □

Seuraavan lauseen todistus on korjattu versio lähteestä [2].

Lause 5. *Seuraavat ovat yhtäpitäviä:*

1. *Valinta-aksiooma.*

2. *Jokaiselle joukolle* A *on olemassa hyvinjärjestysrelaatio.*

Todistus. $1 \Rightarrow 2$. Olkoon X joukko. Valinta-aksiooman III (3) mukaan on olemassa sellainen funktio $V : P(X) \setminus \{\emptyset\} \to X$, että $V(A) \in A$ kaikilla epätyhjillä $A \subseteq X$. Olkoon $\aleph = \{a \in Ord \mid a < \aleph\}$ joukon X Hartogin luku. Määritellään transfiniittisella rekursiolla funktio $g : \aleph \to X \cup \infty$,

$$g(a) = \begin{cases} V(X \setminus \{g(b) \mid b < a\}), \text{ jos } X \neq \{g(b) \mid b < a\} \\ \infty, \text{ muulloin} \end{cases}$$

Koska $\aleph > |X|$, niin on olemassa sellainen a, että $g(a) = \infty$. Olkoon $y = min\{a < \aleph \mid g(a) = \infty\}$. Tällöin funktion g rajoittuma joukosta $z = \{a \in Ord \mid a < y\}$ joukkoon X on bijektio. Koska joukko z koostuu ordinaaliluvuista, niin lauseen 3 mukaan se on hyvinjärjestetty. Nyt lemman 1 nojalla joukko X voidaan hyvinjärjestää.

$2 \Rightarrow 1$. Olkoon X jokin joukko. Oletuksen mukaan se voidaan hyvinjärjestää. Olkoon $A \subseteq X$ ja a_m sen pienin alkio. Nyt voidaan muodostaa valintafunktio $V(A) = a_m$. □

Huomautus 1. Hyvinjärjestetystä joukosta voidaan valita pienin alkio ilman valinta-aksiooman käyttöä. Samoin mielivaltaisesta kokoelmasta hyvinjärjestettyjä joukkoja voidaan valita pienimmät alkiot kustakin. Tämä onnistuu niin sanotun osajoukkoaksiooman avulla. Aihetta käsitellään tarkemmin luvussa 4.

3.2 Zornin lemma

Zornin lemma on valinta-aksiooman kanssa yhtäpitävä tulos, joka koskee maksimaalisten alkioiden olemassaoloa. Zornin lemmalla voidaan todistaa monia tärkeitä lauseita, kuten se, että jokaisella vektoriavaruudella on kanta. Kappale perustuu kirjoihin [1] ja [2].

Määritelmä 5. *Osittainen järjestys* joukossa A on relaatio $<$, joka toteuttaa ehdot:

1. $<$ on *transitiivinen*, eli jos kaikilla $x, y, z \in A$ $x < y$ ja $y < z$, niin $x < z$ ja
2. $<$ on *irrefleksiivinen*, eli kaikilla $x \in A$ $x \not< x$.

Huomautus 2. Merkintää $\leq$ käytetään jatkossa lyhennysmerkintänä ilmaukselle "$<$ tai $=$".

Määritelmä 6. *Ketju* on osittain järjestetyn joukon A osajoukko $K \subseteq A$, jossa kaikilla $x, y \in K$ joko $x \leq y$ tai $x \geq y$.

Määritelmä 7. Järjestetyn joukon A *yläraja* on sellainen alkio b, että $a \leq b$ kaikilla $a \in A$.

Huomautus 3. Joukon ylärajan ei tarvitse välttämättä kuulua itse joukkoon. Esimerkiksi välin $(0, 1)$ eräs yläraja tavanomaisen järjestysrelaation suhteen on 2.

Määritelmä 8. Osittain järjestetyn joukon A *maksimaalinen alkio* on sellainen $M \in A$, että $M \geq a$ kaikilla $a \in A$.

Pian esitellään *Zornin lemma* ja todistetaan sen olevan yhtäpitävä valinta-aksiooman kanssa. Sitä ennen todistetaan kuitenkin välitulos, johon tarvitaan kaksi lemmaa. Seuraavat lemmat ja niiden todistukset ovat kirjoittajan omia.

Lemma 2. *Aito osajoukkorelaatio $\subset$ on osittainen järjestys joukossa A.*

Todistus.

1. Transitiivisuus. Jos $X \subset Y$, niin $x \in Y$ kaikilla $x \in X$. Samoin jos $Y \subset Z$, niin $y \in Z$ kaikilla $y \in Y$. Tällöin $x \in Z$ kaikilla $x \in X$ eli $X \subset Z$.
2. Irrefleksiivisyys. Aito sisältyminen $\subset$ on irrefleksiivinen.

□

Lemma 3. *Olkoon $K \subseteq A$ ketju. Jos $\bigcup K \in A$, niin ketjulla K on yläraja joukossa A relaation $\subset$ suhteen.*

Todistus. Olkoon $K \subseteq A$ ketju relaation $\subset$ suhteen ja $\bigcup K \in A$. Unionin määritelmän nojalla jos $X \in K$, niin $X \subseteq \bigcup K$ kaikilla X. Koska $\bigcup K \in A$, niin se on ketjun K yläraja joukossa A. □

Seuraavan lauseen todistus on kirjoittajan oma.

Lause 6. *Seuraavat lauseet ovat yhtäpitäviä:*

1. Zornin lemma. *Jos osittain järjestetyn joukon A jokaisella epätyhjällä ketjulla on yläraja joukossa A, niin joukolla A on maksimaalinen alkio.*

2. *Jos joukon A jokaisella ketjulla $K \subseteq A$ pätee $\bigcup K \in A$, niin joukossa A on alkio, joka ei ole minkään muun alkion osajoukko.*

Todistus. $1 \Rightarrow 2$

Tämä seuraa lemmoista 2 ja 3.

$2 \Rightarrow 1$

Olkoon A osittain järjestetty joukko, jonka jokaisella epätyhjällä ketjulla on yläraja joukossa A. Muodostetaan jokaista alkiota $a \in A$ kohti joukko

$$x_a = \{x \in A \mid x < a\}.$$

Kootaan näin saadut joukot uudeksi joukoksi

$$X = \{x_a \mid a \in A\}.$$

Nyt $x_a \subset x_b$ jos ja vain jos $a < b$. Olkoon $K \subseteq A$ epätyhjä ketju ja $K_X \subseteq X$ sitä vastaava ketju joukossa X. Oletuksen mukaan ketjulla K on yläraja $Y \in A$ relaation $<$ suhteen, joten myös ketjulla K_X on yläraja $Y_X \in X$ relaation $\subset$ suhteen. Näin ollen $\bigcup K_X \subset Y_X$, joten $K_X \in X$. Nyt kohdan 2 nojalla joukossa X on olemassa sellainen joukko M_X, joka ei ole minkään muun joukon osajoukko. Sitä vastaa alkio $M \in A$, joka on maksimaalinen joukkojen A ja X järjestysrelaatioiden $<$ ja $\subset$ vastaavuuden perusteella. □

Lause 7. *Seuraavat ovat yhtäpitäviä:*

1. *Zornin lemma*

2. *Valinta-aksiooma*

Todistus. Todistus etenee siten, että ensin todistetaan lauseen 6 avulla, että Zornin lemmasta seuraa valinta-aksiooma, ja että hyvinjärjestyslauseesta seuraa Zornin lemma. Koska hyvinjärjestyslause on ekvivalentti valinta-aksiooman kanssa, niin tulos seuraa lauseesta 6.

1. Zornin lemma $\Rightarrow$ valinta-aksiooma.

   Olkoon R mielivaltainen relaatio. Määritellään joukko

   $$A = \{f \mid f \subseteq R,\ f \text{ on funktio}\}.$$

   Olkoon $K \subseteq A$ ketju. Jos $(x, y) \in \bigcup K$ ja $(x, z) \in \bigcup K$, niin $(x, y) \in g \in K$ ja $(x, z) \in h \in K$ joillain funktioilla g ja h. Koska K on ketju, niin joko $g \subseteq h$ tai $h \subseteq g$. Molemmissa tapauksissa (x, y) ja (x, z) kuuluvat yhteen funktioon eli $y = z$. Siis $\bigcup K \in A$. Lauseen 6 väitteen 2 mukaan joukossa A on olemassa maksimaalinen funktio F. Osoitetaan, että $dom(F) = dom(R)$. Jos näin ei ole, niin valitaan mielivaltainen $x \in dom(R) \backslash dom(F)$. Koska $x \in dom(R)$, niin on olemassa sellainen y, että xRy. Määritellään

   $$G = F \cup \{(x, y)\}.$$

   $G \in A$ ja $F \subset G$, mikä on ristiriidassa funktion F maksimaalisuuden kanssa. Siis $dom(F) = dom(R)$, ja valinta-aksiooma on todistettu.

2. Hyvinjärjestyslause $\Rightarrow$ Zornin lemma.

   Olkoon A joukko, joka on suljettu ketjujen unionien suhteen. Hyvinjärjestyslauseen mukaan joukossa A on olemassa hyvinjärjestys $<$. Transfiniittisella rekursiolla voidaan määritellä funktio $F : A \to \{0, 1\}$,

$$F(B) = \begin{cases} 1, & \text{jos B sisältää jokaisen joukon } C < B, \text{ jolle } F(C) = 1, \\ 0, & \text{muuten.} \end{cases}$$

   Olkoon $K = \{B \in A \mid F(B) = 1\}$. Joukko K on ketju relaation $\subset$ suhteen, sillä kaikilla $A, B \in K$ jos $A < B$, niin $A \subset B$ ja sama toisinpäin. Koska K on ketju, niin $\bigcup K \in A$. Väitetään, että $\bigcup K$ on joukon A maksimaalinen alkio. Tehdään vastaoletus, että on olemassa sellainen $D \in A$, että $\bigcup K \subseteq D$. Tällöin $D \in K$, koska se sisältää jokaisen jäsenen ketjusta K. Näin ollen $D \subseteq \bigcup K$, jolloin $D = \bigcup K$. Toisin sanoen $\bigcup K$ on maksimaalinen.

$\square$

3.3 Vektoriavaruuden kanta

Zornin lemmalla voidaan todistaa, että jokaisella vektoriavaruudella on kanta. Tämä on sikäli hyödyllistä, että kantavektoreiden avulla voidaan esittää vektoriavaruuden jokainen vektori. Seuraavat määritelmät ovat peräisin lähteistä [10, 11].

Määritelmä 9. *Kunta* on joukko K, jossa on määritelty binäärioperaatiot $\oplus$ ja $\odot$, jotka toteuttavat seuraavat aksioomat kaikilla $a, b, c \in K$:

1. $a \oplus (b \oplus c) = (a \oplus b) \oplus c$,
2. on olemassa sellainen alkio $0_K \in K$, että $a \oplus 0_K = 0_K \oplus a = a$,
3. jokaista alkiota $a \in K$ kohti on olemassa sellainen alkio $b \in K$, että $a \oplus b = b \oplus a = 0_K$,
4. $a \oplus b = b \oplus a$,
5. $a \odot (b \odot c) = (a \odot b) \odot c$,
6. on olemassa sellainen alkio $1_K \in K$, että $1_K \odot a = a \odot 1_K = a$,
7. $a \odot (b \oplus c) = a \odot b \oplus a \odot c$,
8. $a \odot b = b \odot a$ ja
9. jokaisella alkiolla $k \neq 0_K$ on olemassa sellainen alkio $l \in K$, että $k \odot l = 1_K$.

Määritelmä 10. *Vektoriavaruus* yli kunnan K on joukko V, jossa on määritelty operaatiot yhteenlasku $V \times V \to V$, merkitään $+$, ja skalaarilla kertominen $K \times V \to V$, merkitään $\cdot$, jotka toteuttavat seuraavat aksioomat kaikilla $x, y, z \in V$ ja $a, b \in K$:

1. $x + y = y + x$,

2. $(x + y) + z = x + (y + z)$,

3. on olemassa sellainen $\Theta \in V$, että $x + \Theta = x$,

4. jokaista alkiota $x \in V$ kohti on olemassa sellainen alkio $y \in V$, että $x + y = \Theta$,

5. $a \cdot (x + y) = a \cdot x + a \cdot y$,

6. $(a \oplus b) \cdot x = a \cdot x + b \cdot x$,

7. $(a \odot b) \cdot x = a \cdot (b \cdot x)$ ja

8. $1_K \cdot x = x$.

Määritelmä 11. *Vektoriavaruuden kanta.* Vektoriavaruuden kanta on joukko vektoreita, jotka ovat lineaarisesti riippumattomia ja joiden lineaarikombinaationa voidaan esittää mikä tahansa avaruuden vektori.

Seuraavan lauseen todistus perustuu kirjaan [1], ja käyttää Zornin lemmaa, joten sen todistus edellyttää valinta-aksioomaa.

Lause 8. *Jokaisella vektoriavaruudella on kanta.*

Todistus. Olkoon V vektoriavaruus ja L lineaarisesti riippumattomien vektorien joukkojen joukko. Olkoon $K \subseteq L$ ketju relaation $\subset$ suhteen. Koska kaikilla $x \in K$ joukon x vektorit ovat lineaarisesti riippumattomia ja joko $x \subseteq y$ tai $y \subseteq x$ kaikilla $y \in K$, niin myös $\bigcup K$ on joukko lineaarisesti riippumattomia vektoreita. Siis $\bigcup K \in L$. Lauseen 6 väitteen 2 mukaan on olemassa maksimaalinen lineaarisesti riippumattomien vektoreiden joukko M. Koska M on maksimaalinen, niin jokainen vektori $v \in V$ on lineaarisesti riippuvainen jostain osajoukosta $m \subseteq M$, eli se voidaan esittää vektoreiden $w \in m$ lineaarikombinaationa. Joukko M on siis vektoriavaruuden V kanta. $\square$

Huomautus 4. On osoitettu, että edellinen lause on itse asiassa ekvivalentti valinta-aksiooman kanssa. Tässä tutkielmassa jätetään kyseinen tulos todistamata. Asiasta kiinnostuneet voivat lukea lisää lähteestä [5].

3.4 Ultrafiltterit ja epästandardi analyysi

Seuraava osuus perustuu kirjaan [6]. Valinta-aksiooma mahdollistaa epästandardin analyysin. Epästandardi analyysi pohjautuu niin sanottujen epästandardien kuvausten käyttöön, joilla voidaan esimerkiksi kuvata reaaliluvut $\mathbb{R}$ hyperreaaliluvuiksi ${}^*\mathbb{R}$, joissa on infinitesimaalilukuja sekä äärettömiä lukuja. Epästandardin kuvausten olemassaolon osoittaminen edellyttää, että jokaisella äärettömällä joukolla on vapaa ultrafiltteri, johon tarvitaan valinta-aksioomaa. Epästandardi analyysi on standardimenetelmiä (eli ns. klassista analyysiä tai elementaarista analyysiä) tehokkaampi työkalu esimerkiksi ei-mitallisten funktioiden tutkimiseen.

Määritelmä 12. Olkoon J joukko. Joukko $F \subseteq P(J)$ on *filtteri*, jos

1. $(A \in F$ ja $A \subseteq B \subseteq J) \Rightarrow B \in F$,

2. $A, B \in F \Rightarrow A \cap B \in F$ ja

3. $\emptyset \notin F$.

Määritelmä 13. Filtteri F on *vapaa*, jos $\bigcap F = \emptyset$.

Määritelmä 14. Filtteri F on *ultrafiltteri*, jos se ei sisälly aidosti mihinkään muuhun filtteriin.

Seuraava lemma ja sen todistus ovat kirjoittajan käsialaa.

Lemma 4. *Filtterien ketju on suljettu unionien suhteen, toisin sanoen jos F_i ovat filttereitä ja $F_i \subseteq F_j$ tai $F_j \subseteq F_i$ kaikilla i, j, niin $\bigcup_i F_i$ on filtteri.*

Todistus.

1. Oletetaan, että jokin $A \in \bigcup_i F_i$ ja $A \subseteq B \subseteq J$ jollain B. Tällöin $A \in F_i$ jollain i, jolloin myös $B \in F_i$, joten $B \in \bigcup_i F_i$.

2. Oletetaan, että jotkin $A, B \in \bigcup_i F_i$. Tällöin $A \in F_i$ ja $B \in F_j$ joillain i, j. Koska $F_i \subseteq F_j$ tai $F_j \subseteq F_i$ kaikilla i, j, niin A ja B kuuluvat samaan filtteriin, jolloin myös niiden leikkaus $A \cap B$ kuuluu siihen. Tällöin $A \cap B \in \bigcup_i F_i$.

3. Koska $\emptyset \notin F_i$ kaikilla i, niin $\emptyset \notin \bigcup_i F_i$.

□

Seuraava tulos on tärkeä epästandardissa analyysissä, ja se käyttää Zornin lemmaa, joten se edellyttää valinta-aksioomaa.

Lause 9. *Jokaisella äärettömällä joukolla on vapaa ultrafiltteri.*

Todistus. Olkoon J ääretön joukko. Muodostetaan joukko $F = \{J \backslash J_0 \mid J_0 \subseteq J \text{ on äärellinen}\}$.

1. Osoitetaan, että F on filtteri joukossa J. Jos jokin $A = J \backslash J_A \in F$ ja $A \subseteq B \subseteq J$ jollain B, niin B voidaan esittää muodossa $J \backslash J_B$, missä J_B on äärellinen. Tämä seuraa siitä, että $B = J \backslash B^C$, ja koska $A \subseteq B$, niin $J \backslash J_A \subseteq J \backslash B^C$, joten $B^C \subseteq J_A$, joten B^C on äärellinen. Siis $B \in F$. Jos $A = J \backslash J_A \in F$ ja $B = J \backslash J_B \in F$, niin

$$\begin{aligned} A \cap B &= J \backslash J_A \cap J \backslash J_B = J \cap J_A^C \cap J \cap J_B^C \\ &= J \cap J \cap J_A^C \cap J_B^C = J \cap J_A^C \cap j_B^C = J \backslash (J_A^C \cap J_B^C)^C \\ &= J \backslash (J_A \cup J_B). \end{aligned}$$

Koska J_A ja J_B ovat äärellisiä, niin $A \cap B \in F$. Selvästi $\emptyset \notin F$, koska tyhjä joukko on äärellinen. Siis F on filtteri.

2. Osoitetaan, että F on vapaa. Jos $\bigcap F = \bigcap \{J \backslash J_0 \mid J_0 \subseteq J \text{ on äärellinen}\} \neq \emptyset$, niin on olemassa sellainen x, että $x \in J \backslash J_i$ kaikilla i. Kuitenkin $\{x\}$ on äärellinen, joten $J \backslash \{x\} \in F$, eli $x \notin \bigcap F$. Siis $\bigcap F = \emptyset$, joten määritelmällisesti F on vapaa.

3. Joukon J filtterit muodostavat ketjuja sisältymisrelaation $\subset$ suhteen. Tarkastellaan ketjua, johon F kuuluu. Koska lemman 4 filtterien ketju on suljettu unionien suhteen, niin Zornin lemmasta seuraa suoraan, että on olemassa maksimaalinen filtteri, joka on siis ultrafiltteri U. Koska F on vapaa, niin myös U on vapaa.

$\square$

3.5 Ongelmat äärettömyydessä

Tämä alaluku perustuu lähteeseen [2].

Historiallisesti äärettömän käsite aiheutti matemaatikoille harmaita hiuksia. Miten äärettömyys ja äärellisyys pitäisi määritellä? Vanhin määritelmä äärettömyydelle on Richard Dedekindin määritelmä.

Määritelmä 15. Joukkoa X sanotaan *Dedekind-äärettömäksi*, jos on olemassa sellainen $Y \subset X$, että $Y \sim X$. Muutoin joukko on *Dedekind-äärellinen.*

Toinen määritelmä on peräisin Alfred Tarskilta.

Määritelmä 16. Joukkoa X sanotaan *äärelliseksi*, jos jokaisella potenssijoukon $P(X)$ osajoukolla on minimaalinen alkio sisältymisrelaation $\subset$ suhteen. Joukko, joka ei ole äärellinen, on *ääretön.*

Huomautus 5. Jatkossa äärellistä ja ääretöntä käytetään Tarskin määritelmän mukaan.

Kun valinta-aksiooma hyväksytään, määritelmät ovat keskenään yhtäpitävät. Kuitenkin yhtäpitävyyden osoittamiseen tarvitaan valinta-aksioomaa. Vielä pahempaa on se, että ilman valinta-aksioomaa Dedekind-äärettömyyden käsite aiheuttaa hankalia seurauksia.

Määritelmä 17. Merkinnällä $\aleph_0$ (lausutaan "aalef") tarkoitetaan luonnollisten lukujen joukon $\mathbb{N}$ suuruutta eli *kardinaliteettia.*

Lemma 5. *Seuraavat ovat yhtäpitäviä:*

1. $\aleph_0 \leq |X|$
2. $|X| = |X| + 1$
3. *X on Dedekind-ääretön.*

Todistus. $(1 \Rightarrow 2)$

Olkoon $f : \mathbb{N} \to X$ injektio ja ∞ alkio, joka ei kuulu joukkoon X. Tällöin $g : X \to X \cup \{\infty\}$,

$$g(x) = \begin{cases} \infty, \text{ jos } x = f(0) \\ f(n), \text{ jos } x = f(n+1) \\ x, \text{ muutoin} \end{cases}$$

on bijektio, eli $|X| = |X| + 1$.

(2 ⇒ 3)

Bijektion g käänteiskuvaus g^{-1} rajattuna joukkoon X on injektio joukolta X joukkoon $X \backslash \{g^{-1}(\infty)\} \subset X$. Siis X on yhtämahtava aidon osajoukkonsa kanssa eli Dedekind-ääretön.

(3 ⇒ 1)

Olkoon $f : X \to Y$ injektio ja $Y \subset X$. Olkoon $y \in X \backslash f[X]$. Määritellään rekursiivisesti funktio $g : \mathbb{N} \to X$,

$$g(0) = y, \text{ ja } g(n+1) = f(g(n)).$$

Tällöin g on injektio, joten $\aleph_0 \leq |X|$. □

Lause 10. *Zermelo-Fraenkel -joukko-opissa on mahdollista, että*

1. *Dedekind-äärelliset unionit Dedekind-äärellisistä joukoista voivat olla Dedekind-äärettömiä,*

2. *Dedekind-äärellisen joukon kuva (jollain kuvauksella) voi olla Dedekind-ääretön ja*

3. *Dedekind-äärellisen joukon potenssijoukko voi olla Dedekind-ääretön.*

Todistus. On olemassa Zermelo-Fraenkel -joukko-opin malli, jossa on olemassa sellainen jono (X_n), että $X_n = \{x_n, y_n\}$, joukot X_n ovat parittain erillisiä ja $X = \bigcup_n X_n$ on Dedekind-äärellinen. (Tämä on jo itsessään kummallista.) Mallin tarkempi, tosin silti varsin pintapuolinen tarkastelu lähteessä [2].

1. Muodostetaan jokaista $x \in X$ kohti joukko $Y_x = \{x, n\}$, missä n on se luku, jolla $x \in X_n$. Tällöin $Y = \bigcup_x Y_x$ on Dedekind-äärellinen unioni Dedekind-äärellisistä joukoista, mutta koska funktio $f : \mathbb{N} \to Y$, $f(n) = n$ on injektio, niin $Y = \mathbb{N} \cup \bigcup_n X_n$ on Dedekind-ääretön.

2. Potenssijoukko $P(X)$ on Dedekind-ääretön, koska $f : \mathbb{N} \to P(X)$, $f(n) = \bigcup_{n \leq m} X_m$ on injektio.

3. Funktio $f : X \to \mathbb{N}$, $f(x) = n$, $x \in X_n$ on surjektio, joten joukon X kuva $f(X) = \mathbb{N}$ on Dedekind-ääretön.

□

Edellisen lauseen tulokset ovat epäintuitiivisia. Tarskin määritelmä sen sijaan toimii paremmin.

Lemma 6. *Jos X ja Y ovat äärellisiä, niin myös $X \cup Y$ on äärellinen.*

Todistus. Olkoon $U \subseteq P(X \cup Y)$ ja $U \neq \emptyset$. Joukko $B = \{A \cap X \mid A \in U\}$ sisältää minimaalisen alkion b, koska X on äärellinen. Joukko $C = \{A \cap Y \mid A \in U \text{ ja } A \cap X = B\}$ sisältää myös minimaalisen alkion c, koska Y on äärellinen. Näin ollen $b \cup c$ on joukon U minimaalinen alkio. □

Lemma 7. *Seuraavat ovat yhtäpitävät:*

1. *X on äärellinen*

2. *Jos $U \subseteq P(X)$, $\emptyset \in U$ ja $(A \in U \ \& \ x \in X \Rightarrow A \cup \{x\} \in U)$, niin $X \in U$.*

Todistus. ($\Rightarrow$) Olkoon X äärellinen ja U joukko, joka toteuttaa lauseen ehdot. Äärellisyyden määritelmän nojalla kokoelmalla

$$B = \{X \backslash A \mid A \in U\} \subseteq P(X)$$

on minimaalinen alkio $b \subset X$ relaation $\subset$ suhteen. Tällöin joukolla U on maksimaalinen alkio $A = X \backslash b$. Osoitetaan, että $b = \emptyset$. Tehdään vastaoletus, että on olemassa $c \in b$. Tällöin $c \notin A$. Koska $b \subset X$, niin $c \in X$, jolloin joukon U oletusten nojalla $A \cup \{c\} \in U$, mikä on ristiriita joukon A maksimaalisuuden kanssa. Siis $b = \emptyset$, ja silloin $X = A \in U$.

($\Leftarrow$) Olkoon U kaikkien joukon X äärellisten osajoukkojen joukko. Koska U toteuttaa lauseen sille asettamat ehdot lemman 6 nojalla, niin $X \in U$, joten X on äärellinen. □

Lause 11. 1. *Äärellisten joukkojen äärelliset unionit ovat äärellisiä.*

2. *Äärellisen joukon potenssijoukko on äärellinen.*

3. *Äärellisen joukon kuva on äärellinen kaikilla kuvauksilla.*

Todistus.

1. Olkoon M äärellinen joukko äärellisiä joukkoja. Olkoon $U = \{B \subseteq M \mid \bigcup B$ on äärellinen$\}$. Joukko U toteuttaa lemman 7 joukon U oletukset lemman 6 nojalla, joten $M \in U$ eli $\bigcup M$ on äärellinen.

2. Olkoon X äärellinen joukko. Olkoon $U = \{A \subseteq X \mid P(A)$ on äärellinen$\}$. Tällöin U toteuttaa lemman 7 joukon U oletukset lemman 6 nojalla, joten $X \in U$ eli $P(X)$ on äärellinen.

3. Olkoon X äärellinen ja $f : X \to Y$ surjektio. Jos $U \subseteq P(Y)$ on epätyhjä, niin $B = \{f^{-1}[A] \mid A \in U\} \subseteq P(X)$ on epätyhjä, ja sisältää siten minimaalisen alkion m. Tällöin $f[m]$ on joukon U minimaalinen alkio, joten U on äärellinen. □

Lause 12. *Jos joukko X on äärellinen, niin X on Dedekind-äärellinen.*

Todistus. Tehdään vastaoletus, että X on Dedekind-ääretön. Tällöin lemman 5 nojalla on olemassa injektio $f : \mathbb{N} \to X$. Näin ollen kokoelma $U = \{\{f(m) \mid m \geq n \mid n \in \mathbb{N}\} \subseteq X$ on epätyhjä, mutta sillä ei ole minimaalista alkiota. Siis X on ääretön, mikä on ristiriita oletuksen kanssa, joten vastaoletus on väärä ja X on Dedekind-äärellinen. □

Seuraava lause käyttää valinta-aksioomaa.

Lause 13. *Joukko X on Dedekind-ääretön jos ja vain jos X on ääretön.*

Todistus. ($\Rightarrow$) Tämä seuraa lauseesta 12 kontrapositiolla.

($\Leftarrow$) Osoitetaan, että jokainen ääretön joukko on Dedekind-ääretön. Jos X on ääretön, niin jokaisella $n \in \mathbb{N}$ joukko X_n, joka koostuu injektiivisistä n-tuplista joukossa X on epätyhjä. Valinta-aksiooman nojalla on olemassa funktio $f_n \in \Pi_n X_n$. Funktioiden f_n ketjuttaminen muodostaa jonon (x_n) joukossa X, jolla on ääretön arvojoukko *(engl. range)*. Toistuvien termien kumoaminen muodostaa injektion $g : \mathbb{N} \to X$, joten lemman 5 nojalla X on Dedekind-ääretön. □

3.6 Kardinaliteettien vertailtavuus

On luonnollista ajatella, että kaikkien joukkojen koko olisi vertailtavissa. Tämän tuloksen todistamiseen tarvitaan kuitenkin valinta-aksioomaa.

Lause 14. *Seuraavat ovat yhtäpitäviä:*

1. *Kaikilla joukoilla a ja b joko $a \preccurlyeq b$ tai $a \succcurlyeq b$.*

2. *Valinta-aksiooma.*

Todistus. ($1 \Rightarrow 2$)

Tämä osuus on lähteestä [1]. Olkoon A jokin joukko, ja $\aleph$ sen Hartogin luku (ks. lause 4). Koska A ei dominoi joukkoa $\aleph$, niin oletuksen mukaan $A \prec \aleph$. Tällöin on olemassa injektio $f : A \to \aleph$, jonka avulla A voidaan hyvinjärjestää. Relaatio

$$x < y \Leftrightarrow f(x) \in f(y)$$

on hyvinjärjestys, koska f on injektio ja $\aleph$ on hyvinjärjestetty. Kardinaalien vertailukelpoisuudesta siis seuraa hyvinjärjestyslause, joka on yhtäpitävä valinta-aksiooman kanssa.

($2 \Rightarrow 1$)

Tämä osuus on lähteestä [2]. Olkoon A ja B mielivaltaisia joukkoja. Valinta-aksiooma takaa, että kaikki joukot voidaan hyvinjärjestää. Hyvinjärjestetyt joukot ovat joko isomorfisia tai toinen niistä on isomorfinen toisen alkuosan $seq(t)$ kanssa. Siis $A \preccurlyeq B$ tai $A \succcurlyeq B$. □

4 Mihin valinta-aksioomaa ei tarvita?

Yleisesti valinta-aksioomaa ei tarvita tilanteissa, joissa on mahdollista nimetä valittava alkio. Bertrand Russell havainnollistaa asiaa esimerkillä: Jos on olemassa ääretön joukko kenkäpareja, niin valinta-aksioomaa ei tarvita siihen, että valitsee joka parista toisen kengän, koska voi valita kaikista pareista vasemman (tai oikean) kengän. Sen sijaan sukkapareista ei pysty valitsemaan mielekkäästi toista sukkaa, joten äärettömän sukkaparijoukon tapauksessa valinta-aksioomaa tarvitaan valitsemaan yksi sukka joka parista [2]. Luku on pääosin kirjoittajan omaa käsialaa.

Joukko-opissa on aksiooma, jonka avulla voidaan valita alkio, jos sen nimeäminen on mahdollista.

Aksiooma 2. *Osajoukkoaksiooma* tai *Separaatioaksiooma.* Jokaisella kaavalla φ, joka ei sisällä kirjainta B, seuraava kaava on aksiooma:

$$\forall t_1 \forall t_2 \ldots \forall t_n \forall C \exists B (x \in B \leftrightarrow (x \in C \ \ \& \ \ \varphi(x))).$$

Aksiooma voidaan esittää myös toisessa muodossa: jos A on joukko ja φ kaava, joka ei sisällä kirjainta B, on olemassa joukko

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

Aksiooma siis sanoo, että jos jollain kaavalla φ voidaan määritellä joukko alkioita joukosta A, nämä alkiot voidaan erottaa omaksi joukokseen $X \subseteq A$. Esimerkiksi hyvinjärjestettyjen joukkojen kohdalla tämä on erityisen helppoa.

4.1 Hyvinjärjestetyt joukot

Lause 15. *Olkoon X kokoelma hyvinjärjestettyjä, erillisiä ja epätyhjiä joukkoja H_i. Tällöin on olemassa joukko V, joka sisältää tarkalleen yhden alkion jokaisesta H_i, toisin sanoen valinta-aksiooma pätee teoreemana.*

Todistus. Hyvinjärjestettyjen joukkojen tapauksessa valintajoukko voidaan muodostaa eksplisiittisesti osajoukkoaksioomalla. Jos X on kokoelma hyvinjärjestettyjä, erillisiä joukkoja H_i, niin silloin valintajoukko on

$$V = \{x \in \bigcup_i H_i \mid x \text{ on joukon } H_i \text{ pienin alkio jollain } i\}.$$

Koska pienin alkio on yksikäsitteinen, niin joukko sisältää vain yhden alkion kustakin joukosta H_i. □

Lemma 8. *Jokainen numeroituva joukko voidaan hyvinjärjestää.*

Todistus. Tunnetusti luonnollisten lukujen joukko $\mathbb{N}$ on hyvinjärjestetty tavanomaisen järjestysrelaation $<$ suhteen. Määritelmällisesti numeroituva joukko A on yhtämahtava joukon $\mathbb{N}$ kanssa, joten lemman 1 nojalla A voidaan hyvinjärjestää. □

Seuraus 1. *Jos X on kokoelma erillisiä ja epätyhjiä joukkoja X_i, joiden unioni $\bigcup X$ on numeroituva, niin valinta-aksiooma pätee teoreemana.*

4.2 Äärellinen valinta

Jos valintoja tehdään vain äärellinen määrä, niin valinta-aksioomaa ei tarvita. Erityisesti, jos joukko $X \neq \emptyset$, niin silloin on olemassa jokin $x \in X$, ja tätä alkiota voidaan käyttää myöhemmin, eikä tähän tarvita valinta-aksioomaa [1].

Lause 16. *Olkoon X äärellinen kokoelma epätyhjiä, erillisiä joukkoja X_i. Tällöin valinta-aksiooma pätee teoreemana.*

Todistus. Todistetaan väite induktiolla indeksin i suhteen.

1. ($i = 1$) Tällöin kokoelmassa X on vain yksi joukko X_1. Koska $X_1 \neq \emptyset$, on olemassa $x \in X_1$. Tällöin on olemassa joukko $\{x\}$.

2. Oletetaan, että väite pätee jollain $i = k$.

3. ($i = k+1$) Tällöin kokoelmassa X on $k+1$ joukkoa. Muodostetaan uusi kokoelma $Y = X \backslash X_n$, missä n on kokoelman jonkin joukon indeksi. Nyt kokoelmassa Y on k joukkoa, joten induktio-oletuksen nojalla on olemassa joukko V, jossa on tarkalleen yksi alkio kokoelman Y jokaisesta joukosta. Koska $X_n \neq \emptyset$, niin on olemassa $x \in X_n$. Muodostetaan uusi joukko $V_1 = V \cup \{x\}$, joka on haluttu valintajoukko.

Induktioperiaatteen nojalla väite pätee. □

5 Epäintuitiiviset seuraukset

Valinta-aksiooman avulla voidaan osoittaa joitakin todella epäintuitiivisia ja suorastaan järjenvastaisia tuloksia. Näistä kuuluisimmat ja eniten päätä vaivaavat lienevät Vitalin joukot ja Banachin-Tarskin paradoksi, joita tarkastellaan tässä luvussa. Vitalin joukot ovat joukkoja, jotka eivät ole Lebesgue-mitallisia, toisin sanoen on olemassa sellaisia joukkoja, jotka ovat erillisiä jostakin Vitalin joukosta, mutta niiden ja kyseisen Vitalin joukon unionin mitta on aidosti pienempi kuin niiden ja Vitalin joukon mittojen summa.

Banachin-Tarskin paradoksin mukaan kolmiulotteinen pallo voidaan leikata paloihin ja palat järjestellä uudelleen siten, että lopputuloksena on kaksi alkuperäisen pallon kanssa identtistä palloa. Tämä on intuitiivisesti jo niin järjetöntä, että helposti alkaa etsiä vikaa jostain. Usein syylliseksi on väitetty valinta-aksioomaa [2].

5.1 Lebesguen mitta lyhyesti

Tämä alaluku perustuu lähteeseen [7]. Ennen varsinaisten ydinasioiden läpikäymistä on hyvä kertoa lyhyesti, mikä on Lebesguen mitta.

Määritelmä 18. Joukkoa $I = (a_{11}, a_{12}) \times (a_{21}, a_{22}) \times \cdots \times (a_{n1}, a_{n2}) \subset \mathbb{R}^n$ sanotaan *avoimeksi n-väliksi.*

Määritelmä 19. N-välin $I = (a_{11}, a_{12}) \times (a_{21}, a_{22}) \times \cdots \times (a_{n1}, a_{n2})$ *geometrinen mitta* on $l(I) = (a_{12} - a_{11}) \cdot (a_{22} - a_{21}) \cdot \cdots \cdot (a_{n2} - a_{n1})$.

Määritelmä 20. Olkoon $A \subseteq \mathbb{R}^n$ ja $F = \{I_1, I_2, \dots\}$, missä kukin I_k on avoin n-väli tai tyhjä joukko ja $A \subset \bigcup_{k=1}^{\infty} I_k$. Joukkoa F kutsutaan joukon A *Lebesguen peitteeksi.* Sovitaan, että kukin peitteen joukko indeksoidaan vain kerran ja määritellään summa $S(F) = \sum_{k=1}^{\infty} l(I_k)$.

Määritelmä 21. Määritellään funktio $m^* : P(\mathbb{R}^n) \to \dot{\mathbb{R}}$,

$$m^*(A) = \inf\{S(F) \mid F \text{ on joukon } A \text{ Lebesguen peite.}\}$$

Funktiota m^* kutsutaan *Lebesguen ulkomitaksi.*

Määritellään seuraavaksi *Lebesgue-mitalliset* joukot niin sanotun *Carathéodoryn ehdon* avulla.

Määritelmä 22 (Carathéodoryn ehto)**.** Joukko $E \subset R^n$ on Lebesgue-mitallinen, jos

$$m^*(A) = m^*(A \cap E) + m^*(A \setminus E) \text{ kaikilla } A \subset \mathbb{R}^n.$$

Lebesgue-mitallisten joukkojen joukkoa merkitään Leb $\mathbb{R}^n$.

Määritelmä 23. Jos $E \subset \mathbb{R}^n$ on Lebesgue-mitallinen, niin merkitään

$$m^*(E) = m(E).$$

Funktio $m : \text{Leb } \mathbb{R}^n \to \dot{\mathbb{R}}$ on *Lebesguen mitta.*

Lause 17. *Lebesguen mitan ominaisuuksia:*

1. Monotonisuus. *Jos* $A \subseteq B$*, niin* $m(A) \leq m(B)$ *kaikilla* $A, B \in$ *Leb* $\mathbb{R}^n$.
2. *Jos joukot* $E_1, E_2, \ldots$ *ovat Lebesgue-mitallisia, niin* $\bigcup_{k=1}^{\infty} E_k$ *on mitallinen.*
3. Täysadditiivisuus. $\bigcup_{k=1}^{\infty} E_k = \sum_{k=1}^{\infty} E_k$ *kaikilla erillisillä* $E_k \in$ *Leb* $\mathbb{R}^n$.
4. Siirtoinvarianssi. *Jos* $E \in$ *Leb* $\mathbb{R}^n$*, niin* $E + r \in$ *Leb* $\mathbb{R}^n$ *ja* $m(E) = m(E + r)$ *kaikilla* $r \in \mathbb{R}^n$.

Todistus. Todistus sivuutetaan. Asiasta kiinnostuneet voivat lukea lisää lähteestä [7]. □

Lebesguen mitta antaa matemaattisen tulkinnan pituudelle, pinta-alalle, tilavuudelle ja niiden moniulotteisille vastineille. Lebesgue-mitalliset joukot ovat joukkoja, joiden kohdalla näistä ominaisuuksista voi järkevästi puhua. On kuitenkin olemassa reaalilukujen osajoukkoja, jotka eivät ole Lebesgue-mitallisia. Näillä joukoilla Carathéodoryn ehto ei toteudu, mikä siis tarkoittaa, että on olemassa sellainen joukko $A \in \mathbb{R}$, että $m^*(A) < m^*(A \cap E) + m^*(A \backslash E)$, missä E ei ole Lebesgue-mitallinen.

5.2 Vitalin joukot

Alaluku perustuu kirjaan [2].

Seuraavassa määritelmässä esiteltävän *Vitalin joukon* konstruktiossa käytetään valinta-aksioomaa.

Määritelmä 24. *Vitalin joukko.* Olkoon R sellainen relaatio joukossa $\mathbb{R}$, että

$$xRy \text{ jos ja vain jos } (x - y) \in \mathbb{Q}.$$

R on ekvivalenssirelaatio. Jokainen ekvivalenssiluokka leikkaa joukon $[0, 1]$. Valinta-aksioomaa käyttämällä valitaan jokaisesta ekvivalenssiluokasta tarkalleen yksi alkio kyseiseltä väliltä ja muodostetaan niistä joukko V, jota kutsutaan *Vitalin joukoksi.*

Lause 18. *Vitalin joukko* V *ei ole Lebesgue-mitallinen.*

Todistus. Joukko $I = \mathbb{Q} \cap [-1, 1]$ on numeroituva. Muodostetaan jokaista $r \in I$ kohti joukko $V_r = \{v + r \mid v \in V\}$. Joukot V_r ovat pareittain erillisiä, koska muutoin joukossa V olisi alkioita, jotka kuuluvat samaan ekvivalenssiluokkaan. Tällöin $A = \bigcup_{r \in I} V_r$ on numeroituva unioni pareittain erillisistä joukoista ja $[0, 1] \subseteq A \subseteq [-1, 2]$. Jos V on mitallinen, niin lauseen 17 nojalla jokainen V_r on mitallinen ja niiden mitta on sama kuin joukolla V. Näin ollen lauseen 17 nojalla joukko A on mitallinen, ja sen mitta on joko 0 tai ∞. Edellinen ei ole mahdollista, koska $[0, 1] \subseteq A$ implikoi $\mu(A) \geq 1$, ja jälkimmäinen ei ole mahdollista, koska $A \subseteq [-1, 2]$ implikoi $\mu(A) \leq 3$. Siis V ei ole mitallinen. □

Koska V ei ole Lebesgue-mitallinen, niin Carathéodoryn ehto ei päde jollekin joukolle $A \subset \mathbb{R}$. Toisin sanoen on olemassa sellaiset erilliset joukot, joiden unionin Lebesguen ulkomitta on aidosti pienempi kuin niiden ulkomittojen summa. Asian voi konkretioisda seuraavasti: kuvitellaan pöytä. Jos pöytä olisi ei-mitallinen, niin sen voisi sahata kahteen osaan niin, että osien pituuksien summa olisi suurempi kuin koko pöydän pituus.

5.3 Banachin-Tarskin paradoksi

Tämä alaluku perustuu kirjaan [8].

Määritelmä 25. Sanotaan, että ryhmä G *toimii* (engl. acts on) *joukossa* X, jos jokaista $g \in G$ kohti on olemassa sellainen funktio $g : X \to X$, että $g(h(x)) = (gh)(x)$ ja $1(x) = x$ kaikilla $g, h \in G$, $x \in X$ ja 1 on ryhmän G neutraalialkio.

Määritelmä 26. Olkoon G ryhmä, joka toimii joukossa X ja $E \subseteq X$. Joukko E on *G-paradoksaalinen* (engl. G-paradoxical), jos joillain $m, n \in \mathbb{N}$ on olemassa sellaiset erilliset joukon E osajoukot $A_1, \ldots, A_m, B_1 \ldots, B_n$ ja $g_1, \ldots, g_m, h_1, \ldots, h_n \in G$, että $E = \bigcup_{i=1}^m g_i(A_i)$ ja $E = \bigcup_{i=1}^n h_i(B_i)$.

Ryhmä G on *paradoksaalinen*, jos se on G-paradoksaalinen, kun G toimii itsessään vasemmalta operoituna.

Määritelmä 27. Joukon M generoima *vapaa ryhmä* F muodostuu kaikista äärellisistä sanoista, joiden kirjaimet kuuluvat joukkoon $\{\sigma, \sigma^{-1} \mid \sigma \in M\}$. Joukon M sanoja σ kutsutaan ryhmän *generaattoreiksi*. Ryhmäoperaationa on sanojen ketjutus ja neutraalialkiona tyhjä sana ϵ. Lisäksi kirjain ja sen vastakirjain kumoavat toisensa, siis $\sigma\sigma^{-1} = \epsilon$. Generoivan joukon kokoa sanotaan vapaan ryhmän *asteeksi.*

Ryhmää G sanotaan *vapaaksi*, jos se on isomorfinen jonkin vapaan ryhmän kanssa.

Huomautus 6. Vapaa ryhmä, jonka aste on vähintään 2, ei koskaan ole kommutatiivinen, sillä sanat katsotaan eri sanoiksi, jos kirjainten järjestystä vaihdetaan. Vain kirjain ja sen vastakirjain kommutoivat, siis esimerkiksi $\phi\phi^{-1} = \phi^{-1}\phi = 1$.

Seuraavan lauseen todistus on korjattu versio kirjan [8] todistuksesta.

Lause 19. *Vapaa ryhmä F, jonka aste on 2, on F-paradoksaalinen.*

Todistus. Olkoot σ ja τ ryhmän F generaattorit. Oletetaan, että ρ on jokin seuraavista ryhmän F alkioista: σ, σ^{-1}, τ tai τ^{-1}. Olkoon $W(\rho)$ niiden ryhmän F alkioiden joukko, jotka generaattoreiden avulla esitettynä alkavat vasemmalta kirjaimella ρ. Tällöin joukot $W(\sigma), W(\sigma^{-1}), W(\tau)$ ja $W(\tau^{-1})$ ovat parittain erillisiä.

Lisäksi $F = W(\sigma) \cup \sigma W(\sigma^{-1})$, koska jos $h \in F \backslash W(\sigma)$, niin $\sigma^{-1}h \in W(\sigma^{-1})$ ja $h = \sigma\sigma^{-1}h \in \sigma W(\sigma^{-1})$. Vastaavasti $F = W(\tau) \cup \tau W(\tau^{-1})$.

Siis F on paradoksaalinen. □

Määritelmä 28. Jos ryhmä G toimii joukossa X, ja $g(x) = x$ joillain $g \in G \backslash 1_G$ ja $x \in X$, niin pistettä x sanotaan *epätriviaaliksi kiintopisteeksi.*

Lause 20. *Jos G on paradoksaalinen ja toimii joukossa X ilman epätriviaaleja kiintopisteitä, niin X on paradoksaalinen.*

Todistus. Oletetaan, että $A_i, B_j \subseteq G$, $g_i, h_j \in G$, missä $i, j = 1 \ldots n$ todistavat ryhmän G paradoksaalisuuden. Valinta-aksiooman nojalla on olemassa joukko M, joka sisältää tarkalleen yhden alkion jokaisesta joukosta $\{g(x) \mid g \in G\}$, missä $x \in X$ on kiinnitetty. Joukko $\{g(M) \mid g \in G\}$ on joukon X partitio. Koska ryhmä G toimii joukossa X ilman epätriviaaleja kiintopisteitä, niin joukot $g(M)$ ovat erillisiä. Olkoon $A_i^* = \bigcup\{g(M) \mid g \in A_i\}$ ja $B_j^* = \bigcup\{g(M) \mid g \in B_j\}$. Koska joukot

$A_1, \dots, A_m, B_1, \dots, B_n$ ovat parittain erillisiä, niin joukot A_i^* ja B_j^* muodostavat parittain erillisten joukon X osajoukkojen kokoelman. Nyt $X = \bigcup g_i(A_i^*) = \bigcup g_j(B_j^*)$, koska $G = \bigcup g_i(A_i) = \bigcup g_j(B_j)$. Siis X on G-paradoksaalinen. □

Kuten huomattiin, edellinen lause edellyttää valinta-aksiooman käyttöä. Näin ollen kaikki lauseet, jotka suoraan tai välillisesti käyttävät edellistä lausetta, tarvitsevat myös valinta-aksiooman toimiakseen.

Seuraus 2. *Joukko X on F-paradoksaalinen, jos astetta 2 oleva vapaa ryhmä F toimii siinä ilman epätriviaaleja kiintopisteitä.*

Määritelmä 29. *Yksikköpallopinnaksi* joukossa $\mathbb{R}^3$ sanotaan joukkoa

$$S^2 = \{(x, y, z) \in \mathbb{R}^3 \mid x^2 + y^2 + z^2 = 1\}.$$

Kierto ρ yksikköpallopinnalla on origokeskinen kierto, eli kierto yksikköpallopinnan keskipisteen ympäri.

Määritelmä 30. Ryhmä SO_3 on yksikköpallopinnan kiertojen ryhmä.

Lause 21. *Olkoon ϕ kierto z-akselin ympäri kulman $arccos(1/3)$ verran ja ρ kierto x-akselin ympäri saman kulman verran. Kierrot ϕ ja ρ generoivat 2. asteen vapaan ryhmän.*

Todistus. Kierrot ϕ ja ρ voidaan esittää matriiseina

$$\phi^{\pm 1} = \begin{pmatrix} 1/3 & \mp\frac{2\sqrt{2}}{3} & 0 \\ \pm\frac{2\sqrt{2}}{3} & 1/3 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \rho^{\pm 1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1/3 & \mp\frac{2\sqrt{2}}{3} \\ 0 & \pm\frac{2\sqrt{2}}{3} & 1/3 \end{pmatrix}.$$

Kiertojen epäkommutatiivisuus on helppo todeta jo ihan ajatuskokeella. Jäljelle jää osoittaa, ettei mikään sana, joka on eri kuin tyhjä sana, vastaa identiteettikiertoa. Koska $\phi \cdot 1 \cdot \phi^{-1} = \phi^{-1} \cdot 1 \cdot \phi = 1$, niin voidaan rajoittua sanoihin, jotka päättyvät kirjaimeen $\phi^{\pm 1}$.

Tehdään vastaoletus: on olemassa sellainen sana w, että se on identiteettikierto. Osoitetaan, että $w(1,0,0)^T = (a, b\sqrt{2}, c)^T/3^k$, missä $a, b, c \in \mathbb{Z}$ ja b ei ole jaollinen luvulla 3. Tästä seuraa, että $w(1,0,0)^T \neq (1,0,0)^T$, mikä on ristiriita.

Osoitetaan väite induktiolla sanan w pituuden suhteen. Jos sanan w pituus on 1, niin $w = \phi^{\pm 1} = (1, \pm 2\sqrt{2}, 0)^T/3$. Oletetaan sitten, että $w = \phi^{\pm 1}w'$ tai $w = \rho^{\pm 1}w'$, missä $w'(1,0,0)^T = (a', b'\sqrt{2}, c')^T/3^{k-1}$. Kertomalla w' yllä olevilla matriiseilla huomataan, että $w(1,0,0)^T = (a' \mp 4b', (b' \pm 2a')\sqrt{2}, 3c')^T/3^k$ tai $w(1,0,0)^T = (3a', (b' \mp 2c')\sqrt{2}, c' \pm 4b')^T/3^k$ riippuen siitä, alkaako w kirjaimella $\phi^{\pm 1}$ vai $\rho^{\pm 1}$. Joka tapauksessa $a, b, c \in \mathbb{Z}$.

Osoitetaan vielä, ettei b ole ikinä jaollinen luvulla 3. Käsiteltävänä on neljä tapausta:

1. $w = \phi^{\pm 1}\rho^{\pm 1}v$, missä v on jokin sana (voi olla tyhjä sana),
2. $w = \rho^{\pm 1}\phi^{\pm 1}v$,
3. $w = \phi^{\pm 1}\phi^{\pm 1}v$ ja

4. $w = \rho^{\pm 1}\rho^{\pm 1}v$.

Tapauksissa 1 ja 2 $b = b' \pm 2a'$ tai $b = b' \mp 2c'$, missä $3|a'$ tai $3|c'$. Koska induktio-oletuksen mukaan 3 ei jaa lukua b', niin se ei jaa lukua b.

Olkoon a'', b'', c'' ne kokonaisluvut, jotka ovat kierron $v(1,0,0)$ esityksessä. Tällöin tapauksessa 3

$$b = b' \pm 2a' = b' \pm 2(a'' \mp 4b'') = b' + b'' \pm 2a'' - 9b'' = 2b' - 9b''.$$

Koska 3 ei jaa lukua b', niin se ei jaa lukua b. Tapauksessa 4 saadaan vastaavalla tavalla $b = 2b' - 9b''$. Väite on todistettu. □

Seuraavaa tulosta kutsutaan Hausdorffin paradoksiksi, joka on väliaskel kohti Banachin-Tarskin paradoksia. Sen todistuksessa käytetään seurausta 2, joten se edellyttää valinta-aksioomaa.

Lause 22 (Hausdorffin paradoksi)**.** *On olemassa sellainen numeroituva joukko $D \subset S^2$, että $S^2 \backslash D$ on SO_3-paradoksaalinen.*

Todistus. Lauseen 21 kiertojen generoiman ryhmän (merkitään F) jokainen alkio, joka ei ole identiteettikierto, kiinnittää jonkin suoran. Olkoon D näiden suorien ja yksikköpallopinnan S^2 leikkauspisteiden joukko. Yhdellä suoralla on korkeintaan kaksi leikkauspistettä pallopinnan kanssa, ja koska ryhmä F on numeroituva, niin D on numeroituva. Jos $P \in S^2 \backslash D$ ja $g \in F$, niin $g(P) \in S^2 \backslash D$. Tämä siksi, että jos $g(P) \in D$, niin silloin jollain $h \in F$ $h(g(P)) = g(P)$. Tällöin $g^{-1}(h(g(P))) = g^{-1}(g(P)) = P$ eli $P \in D$, mikä on ristiriita.

Nyt ryhmä F, joka on toisen asteen vapaa ryhmä, toimii joukossa $S^2 \backslash D$ ilman epätriviaaleja kiintopisteitä, joten seurauksen 2 nojalla $S^2 \backslash D$ on SO_3-paradoksaalinen. □

Määritelmä 31. Olkoon G ryhmä, joka toimii joukossa X ja $A, B \subseteq X$. Joukot A ja B ovat *G-yhtähajotettavia* (engl. G-equidecomposable), jos on olemassa sellaiset A_i ja B_i, että

1. $A = \bigcup_{i=1}^{n} A_i$ ja $B = \bigcup_{i=1}^{n} B_i$,

2. $A_i \cap A_j = \emptyset$ ja $B_i \cap B_j = \emptyset$ kaikilla $i < j \leq n$ ja

3. on olemassa sellaiset $g_1, \ldots g_n \in G$, että $g_i(A_i) = B_i$ kaikilla $i \leq n$.

Jos A ja B ovat G-yhtähajotettavia, niin merkitään $A \sim_G B$. Tapauksissa, joissa ryhmä on selvä tai mielivaltainen, voidaan käyttää merkintää $A \sim B$. Tässä luvussa merkintää käytetään vain ja ainoastaan tässä merkityksessä, eikä kuvaamaan joukkojen yhtämahtavuutta.

Seuraavien kahden lauseen todistukset ovat kirjoittajan omia.

Lause 23. *Joukko $E \subseteq X$ on G-paradoksaalinen jos ja vain jos on olemassa sellaiset erilliset joukon E osajoukot A ja B, että $A \sim_G E$ ja $B \sim_G E$.*

Todistus. ($\Rightarrow$) Oletetaan, että $E \subseteq X$ on G-paradoksaalinen jollain ryhmällä G. Tällöin on olemassa sellaiset erilliset joukon E osajoukot $A_1, \dots, A_m, B_1 \dots, B_n$ ja $g_1, \dots, g_m, h_1, \dots, h_n \in G$, että $E = \bigcup_{i=1}^m g_i(A_i)$ ja $E = \bigcup_{i=1}^n h_i(B_i)$. Olkoon $A = \bigcup_{i=1}^m A_i$ ja $B = \bigcup_{i=1}^n B_i$. Tällöin $A \sim_G E$ ja $B \sim_G E$.

($\Leftarrow$) Oletetaan, että $A, B \subseteq E$, $A \cap B = \emptyset$ ja $A \sim_G E$ ja $B \sim_G E$. Tällöin on olemassa sellaiset erilliset joukot A_i sekä $g_i \in G$, että $A = \bigcup_{i=1}^n A_i$ ja $E = \bigcup_{i=1}^m g_i(A_i)$. Vastaava päättely joukolle B todistaa, että E on G-paradoksaalinen. □

Lause 24. *Olkoon G ryhmä, joka toimii joukossa X ja $E, E' \subseteq X$ ja $E \sim_G E'$. Jos E on G-paradoksaalinen, niin E' on myös.*

Todistus. Oletetaan, että E on G-paradoksaalinen. Tällöin lauseen 23 nojalla E sisältää sellaiset erilliset joukot A ja B, että $A \sim_G E$ ja $B \sim_G E$, joten $E = \bigcup_{i=1}^m g_i(A_i)$ joillain erillisillä $A_i \subseteq A$ ja $g_i \in G$. Koska $E \sim_G E'$, niin $E' = \bigcup_{j=1}^n g_j(E_j)$ joillain erillisillä $E_j \subseteq E$ ja $g_j \in G$. Olkoon $C_{ij} = g_i(A_i) \cap E_j$ ja $A_{ij} = g_i^{-1}(C_{ij})$. Nyt $E' = \bigcup_{i,j} g_j(g_i(A_{ij}))$, joten $A \sim_G E'$. Sama päättely voidaan toistaa joukolle B, joten $B \sim_G E'$. Koska $A, B \subseteq E$ ja $E \sim_G E'$, niin E' sisältää niiden "kopiot"A', B', ja $A' \sim_G E'$ ja $B' \sim_G E'$. Lauseen 23 nojalla E' on G-paradoksaalinen. □

Huomautus 7. Relaatio $\sim_G$ on ekvivalenssirelaatio. Selvästi $A \sim_G A$ ja $A \sim_G B$ jos ja vain jos $B \sim_G A$. Lauseen 24 todistus osoittaa transitiivisuuden.

Määritelmä 32. Jos A on G-yhtähajotettava jonkin joukon B osajoukon kanssa, niin merkitään $A \preccurlyeq_G B$. Tapauksissa, joissa ryhmä G on selvä tai mielivaltainen, voidaan merkitä $A \preccurlyeq B$. Tässä luvussa merkintää käytetään vain ja ainoastaan tässä merkityksessä, eikä kuvaamaan joukkojen dominointia.

Lause 25 (Banachin-Schröderin-Bernsteinin lause)**.** *Olkoon G ryhmä, joka toimii joukossa X, ja $A, B \subseteq X$. Jos $A \preccurlyeq_G B$ ja $B \preccurlyeq_G A$, niin $A \sim_G B$. Relaatio $\preccurlyeq_G$ on siis ekvivalenssiluokkien $\sim_G$ osittainen järjestys joukossa $P(X)$.*

Todistus. Relaatio $\sim_G$ toteuttaa selvästi seuraavat ominaisuudet:

1. Jos $A \sim_G B$, niin on olemassa sellainen bijektio $g : A \to B$, että $C \sim_G g(C)$ aina, kun $C \subseteq A$.

2. Jos $A_1 \cap A_2 = \emptyset = B_1 \cap B_2$, $A_1 \sim_G B_1$ ja $A_2 \sim_G B_2$, niin $A_1 \cup A_2 \sim_G B_1 \cup B_2$.

Oletetaan, että $A_1 \subseteq A$ ja $B_1 \subseteq B$. Olkoon $f : A \to B_1$ ja $g : A_1 \to B$ bijektioita, jotka ovat olemassa kohdan 1 nojalla. Määritellään $C_0 = A \backslash A_1$, rekursiivisesti $C_{n+1} = g^{-1}(f(C_n))$ ja $C = \bigcup_{n=0}^\infty C_n$. Tällöin $g(A \backslash C) = B \backslash f(C)$, joten kohdan 1 nojalla $A \backslash C \sim_G B \backslash f(C)$. Samoin $C \sim_G f(C)$ ja kohdan 2 nojalla $A \backslash C \cup C \sim_G B \backslash f(C) \cup f(C)$, joten $A \sim_G B$. □

Lause 26. *Jos $D \subset S^2$ on numeroituva, niin $S^2 \sim_{SO_3} S^2 \backslash D$.*

Todistus. Olkoon l origon kautta kulkeva suora, joka ei leikkaa joukkoa D. Olkoon A sellaisten kulmien θ joukko, että $\rho(P) \in D$ joillain $n > 0$ ja $P \in D$, missä ρ on kierto suoran l ympäri $n\theta$ radiaanin verran. Tällöin A on numeroituva, joten voidaan valita sellainen θ, joka ei kuulu joukkoon A ja sitä vastaava kierto ρ_θ suoran l ympäri. Tällöin $\rho_\theta^n(D) \cap D = \emptyset$ kaikilla $n > 0$, joten $\rho_\theta^m(D) \cap \rho_\theta^n(D) = \emptyset$. Tällöin $S^2 = \bar{D} \cup (S^2 \backslash \bar{D}) \sim_{SO_3} \rho_\theta(\bar{D}) \cup (S^2 \backslash \bar{D}) = S^2 \backslash D$, missä $\bar{D} = \bigcup_{n=1}^\infty \rho_\theta^n(D)$. □

Määritelmä 33. Ryhmä G_3 on avaruuden $\mathbb{R}^3$ isometrioiden ryhmä.

Seuraavaksi esitellään Banachin-Tarskin paradoksi, jonka todistamiseen tarvitaan valinta-aksioomaa.

Lause 27 (Banachin-Tarskin paradoksi)**.** *S^2 on SO_3-paradoksaalinen, kuten mikä tahansa muukin origokeskinen pallopinta. Lisäksi mikä tahansa kiinteä pallo avaruudessa $\mathbb{R}^3$ on G_3-paradoksaalinen ja $\mathbb{R}^3$ on paradoksaalinen.*

Todistus. Hausdorffin paradoksista (lause 22) ja lauseista 24 ja 26 yhdessä seuraa, että S^2 on SO_3-paradoksaalinen. Koska yksikään tuloksista ei riipu pallopinnan koosta, niin tämä pätee mille tahansa origokeskiselle pallopinnalle.

Riittää tarkastella origokeskistä palloa, koska G_3 sisältää kaikki siirrot. Todistuksessa käsitellään yksikköpalloa B, mutta sama todistus käy mille tahansa pallolle. Pallopinnan S^2 hajottaminen antaa vastaavanlaisen hajotuksen myös pallolle kuvauksella $P \mapsto \{\alpha P \mid \alpha \in (0,1]\}$. Riittää siis osoittaa, että $B \sim_{G_3} B \setminus \{(0,0,0)\}$. Olkoon $P = (0,0,1/2)$ ja ρ äärettömän kertaluvun kierto pisteen P kautta kulkevan akselin ympäri, joka ei kulje origon kautta. Tällöin joukkoa $D = \{\rho^n((0,0,0)) \mid n \geq 0\}$ voidaan käyttää imaisemaan origo: $\rho(D) = D \setminus \{(0,0,0)\}$, joten $B \sim_{G_3} B \setminus \{(0,0,0)\}$.

Jos sen sijaan käytetään kuvausta $P \mapsto \{\alpha P \mid \alpha > 0\}$, niin voidaan vastaavalla tavalla osoittaa, että $\mathbb{R}^3 \sim_{G_3} \mathbb{R}^3 \setminus \{(0,0,0)\}$. $\square$

Banachin-Tarskin paradoksin mukaan siis mikä tahansa pallo avaruudessa $\mathbb{R}^3$ voidaan hajottaa erillisiin osiin ja kuvata siten, että saadaan kaksi palloa. Esimerkiksi Hausdorffin paradoksin 22 yhteydessä käytetyt kuvaukset toimivat. Tarvittaessa palasia voidaan siirtää siirtokuvauksella. Paradoksia voidaan myös vahventaa. Sitä ennen tarvitaan kuitenkin kolme määritelmää.

Määritelmä 34. *Metriikka* joukossa X on kuvaus $d : X^2 \to \mathbb{R}$, joka toteuttaa ehdot

1. $d(x,z) \leq d(x,y) + d(y,z)$ kaikilla $x,y,z \in X$,
2. $d(x,y) = d(y,x)$ kaikilla $x,y \in X$ ja
3. $d(x,y) = 0$ jos ja vain jos $x = y$. [12]

Määritelmä 35. Joukon X *sisäpiste* on sellainen piste $x \in X$, että on olemassa sellainen $\varepsilon > 0$, että $B(x,\varepsilon) = \{y \in X \mid m(x,y) < \varepsilon\} \subset X$, missä m on joukossa X määritelty metriikka. [12]

Määritelmä 36. Joukon X *sisus* (engl. *interior*) on sen sisäpisteiden muodostama joukko. [13]

Lause 28 (Banachin-Tarskin paradoksin vahva muoto)**.** *Jos A ja B ovat mitä tahansa rajoitettuja avaruuden $\mathbb{R}^3$ osajoukkoja, joilla on epätyhjä sisus, niin A ja B ovat yhtähajotettavia.*

Todistus. Riittää osoittaa, että $A \preccurlyeq B$, koska samalla tavalla saadaan $B \preccurlyeq A$ ja Banachin-Schröderin-Bernsteinin lauseesta 25 seuraa $A \sim B$. Olkoon K ja L sellaisia palloja, että $A \subseteq K$ ja $L \subseteq B$, ja olkoon $n \in \mathbb{N}$ niin suuri, että K voidaan peittää n kappaleella pallon L kopioita. Jos S on joukko erillisiä pallon L kopioita, niin Banachin-Tarskin paradoksia käyttämällä voidaan monistaa pallo L ja liikuttaa saadut kopiot siten, että $L \succcurlyeq S$. Siis $A \subseteq K \preccurlyeq S \preccurlyeq L \subseteq B$, joten $A \preccurlyeq B$. $\square$

Banachin-Tarskin paradoksin vahvasta muodosta seuraa se kuuluisa esimerkki, että herne voidaan hajottaa osiin ja kasata osat Auringon kokoiseksi.

6 Suhtautuminen valinta-aksioomaan historiassa ja lisää paradokseista

6.1 Yleinen suhtautuminen

Kun Zermelo muotoili valinta-aksiooman ensi kertaa vuonna 1904 hyvinjärjestyslauseen todistamiseksi, myrsky nousi. Tämä uusi aksiooma jakoi matemaatikkojen mielipiteitä. Konstruktivistit, kuten ranskalaiset Baire, Borel ja Lebesgue kritisoivat aksiooman epäkonstruktiivisuutta. Valinta-aksiooma takaa vain valintajoukon olemassaolon, muttei kerro mitään siitä, miten se määritellään. Lisää vettä arvostelijoiden myllyyn heittivät epäintuitiiviset tulokset, kuten Vitalin joukko ja erityisesti Banachin-Tarskin paradoksi. [2, 3]

Osa matemaatikoista hyväksyi valinta-aksiooman. Esimerkiksi David Hilbert totesi sen olevan olennainen osa matematiikkaa ja käytti sitä puolustuksena intuitionisteja vastaan [3]. Ironista kyllä, moni valinta-aksiooman kriitikoista käytti sitä huomaamattaan. Hardy huomautti, että Borel käytti valinta-aksioomaa indeksoimaan ylinumeroituvan joukon töissään. Sierpinski osoitti, että Lebesgue käytti valinta-aksioomaa todistaessaan mitallisten joukkojen numeroituvan unionin olevan mitallinen. Moore esitti monia esimerkkejä, joissa oli käytetty valinta-aksioomaa ennen kuin Zermelo julkaisi artikkelinsa, ja osa näiden esimerkkien tekijöistä kritisoivat uutta aksioomaa. [2]

1930-luvulla Kurt Gödel osoitti valinta-aksiooman olevan ristiriidaton Zermelon ja Fraenkelin ZF-aksioomien kanssa [3]. 1960-luvulla Paul Cohen osoitti, että valinta-aksiooma on riippumaton ZF-aksioomista [4]. Nämä tulokset antoivat hiukan lisää uskottavuutta valinta-aksiooman puolustajille, jotka niin sanotusti purivat luotia ja totesivat sen tuottavan epäintuitiivisia tuloksia, mutta hyväksyivät sen niistä huolimatta.

6.2 Kritiikkiä vain valinta-aksiooman syyttämisestä

Horst Herrlich kirjoittaa kirjassaan [2], että Banachin-Tarskin paradoksi ja Vitalin joukko ovat mahdollisia vain ZFC-joukko-opissa, eli kun joukko-opin Zermelo-Fraenkel -aksioomien lisäksi valinta-aksiooma on voimassa. Toisin sanoen pelkät ZF-aksioomat eivät riitä. On nimittäin olemassa sellaisia ZF-malleja, joissa kaikki reaalilukujen rajoitetut osajoukot ovat Lebesgue-mitallisia. Vitalin joukko ja Banachin-Tarskin paradoksi osoittavat ei-mitallisten joukkojen olemassaolon. Herrlich toteaa tämän osoittavan, että "here again AC (Axiom of Choice) is the villain".

On tietysti totta, että tässäkin tutkielmassa esitetyt täysin järjenvastaiset tulokset edellyttävät valinta-aksiooman käyttöä. On kuitenkin kapeakatseista syyttää yksinomaan valinta-aksioomaa tai ylipäätään keskittyä pelkästään siihen. Se on sama asia kuin syyttäisi autonrenkaita kolareista sillä perusteella, että jos autoissa ei olisi renkaita, ei tulisi kolareitakaan. Tässä vertauksessa on vielä se lisäarvo, että samaan tapaan kuin renkaiden poistaminen aiheuttaa merkittäviä ongelmia autoilulle, valinta-aksiooman hylkääminen johtaa myös inhottaviin tuloksiin, kuten Dedekind-äärettömyyden ongelmat lauseessa 10 tai kardinaalien vertailukelvottomuus lauseessa 14. Lisäksi myös muita vähintäänkin outoja asioita tapahtuu, joista voi lukea enemmän kirjasta [2].

Tutkitaan esimerkiksi Vitalin joukkoa. Käydään seuraavaksi läpi niin tarkasti kuin on mahdollista ja järkevää, mitä kaikkea sen konstruoimisessa oikein käytetään.

1. Ekvivalenssirelaatio R

2. Valinta-aksiooma

3. Mitan ominaisuudet: siirtäminen ei vaikuta mittaan (siirtoinvarianssi), erillisten joukkojen unionin mitta on joukkojen mittojen summa (additiivisuus), joukon mitta on vähintään sen osajoukon mitta (monotonisuus)

4. Joukko-opin operaatiot unioni ja leikkaus

5. Reaaliluvut eivät ole diskreetti joukko

Näitä asioita tarvitaan Vitalin joukon tekemiseen, ja jos yksikin niistä ei ole voimassa, Vitalin joukkoa ei voi sellaisenaan konstruoida. Mikäli tällaisten ihmeellisten joukkojen olemassaoloa ei halua myöntää, niin on kyseenalaistettava yksi tai useampi yllä mainituista taustaoletuksista.

Tarkastellaan ensin Vitalin joukon konstruktiossa määriteltyä ekvivalenssirelaatiota. Ekvivalenssirelaation käsitettä on hankala lähteä kaatamaan, koska se on kuitenkin varsin luonnollisella tavalla määritelty. Vaikka sen väkisin tekisikin, niin relaatio xRy jos ja vain jos $(x - y) \in \mathbb{Q}$ toteuttaa silti ekvivalenssirelaation ehdot ja siten sillä on kaikki sen ominaisuudet, kutsuttiin sitä sitten millä nimellä hyvänsä. Ekvivalenssiluokkien osalta ongelma on pitkälti sama. Periaatteessa voitaisiin yrittää sanoa, etteivät ne ole joukkoja, mutta se herättää vain kysymyksen, miksi eivät. Lisäksi se ei välttämättä edes estäisi itse konstruktiota. Jos mennään niin pitkälle, että härkäpäisesti vain kielletään kaikki ekvivalenssirelaatioon liittyvät käsitteet, aiheutetaan vain uusia ongelmia. Vika ei siis näytä olevan määritellyssä relaatiossa.

Valinta-aksioomaa on kyseenalaistettu eri lähteissä ihan tarpeeksi, joten sitä ei tässä tutkielmassa lähdetä nyt tekemään. Todettakoon vain, että ilman valinta-aksioomaa saadaan aikaiseksi vain joukko ekvivalenssiluokkia, joilla ei varsinaisesti pysty tekemään yhtään mitään mitallisuuden suhteen. Valinta-aksiooma on olennainen muodostettaessa joukkoa, jolla voidaan osoittaa jotain.

Olisiko mitan käsitteessä jotain vikaa? Riippuu vähän siitä, miltä kantilta asiaa katsoo. Kaikkia haluttuja ominaisuuksia ei voida toteuttaa, joten jostain on tingittävä. Tämä taas saattaa aiheuttaa uusia epäintuitiivisia hirviöitä, kuten esimerkiksi siirtoinvarianssista luopuminen tuottaa joukkoja, joiden mittaa muuttuu, kun niitä siirretään. Jollain lailla järkevä vaihtoehto on luopua numeroituvasta additiivisuudesta (eli $\mu\big(\bigcup_{i=1}^{\infty} E_i\big) = \sum_{i=1}^{\infty} \mu(E_i)$), ja itse asiassa Stefan Banach osoitti, että on olemassa äärellisesti additiivisia mittoja joukossa $\mathbb{R}^2$ [2, 9]. Osa niistä tuottavat Lebesgue-mitallisilla joukoilla saman mitan kuin Lebesguen mitta. Niillä on kuitenkin joitakin kummallisia ominaisuuksia, kuten von Neumann osoitti [2]. Lisäksi Banachin-Tarskin paradoksi on yhä ongelma, eikä siis joukossa $\mathbb{R}^3$ ole kaikilla osajoukoilla määriteltyä mittaa. Joka tapauksessa mitan käsitteen pyörittely ei lopulta paljoa auta.

Unionin ja leikkauksen kieltäminen voisi kenties ratkaista ongelman, mutta seuraukset olisivat rumaa katsottavaa, vähän niin kuin sen jälkeen, kun kärpänen on tapettu atomipommilla. Mikäli joukkojen unioneita tai leikkauksia ei olisi, niin mitä ihmettä voitaisiin enää muutenkaan tehdä? Jotain kenties, mutta ainakin mittateorian ja sen osa-alueen todennäköisyyslaskennan kannalta tilanne menisi aika hankalaksi.

Jäljelle jää reaalilukujen joukko. Tämä onkin mielenkiintoinen tapaus, sillä reaaliluvuilla on joitakin kummallisia ominaisuuksia. Haluan erityisesti nostaa esille sen tosiasian, että lukuvälillä $[0,1]$ on ääretön määrä reaalilukuja, itse asiassa yhtä paljon kuin koko lukusuoralla. Tämä ominaisuus on avainasemassa Vitalin joukon konstruktiossa. Kuvitellaan hetken aikaa, että välillä $[0,1]$ olisikin n kappaletta lukuja. Ensinnäkin Lebesguen mitan mukaan sen mitta olisi 0. Ennen kaikkea on helppo määritellä välin mitaksi 1, ja joukon $A \subseteq [0,1]$, jossa on m lukua mitta olisi m/n. Yleisestikin numeroituvalle joukolle, kuten $\mathbb{N}$ on olemassa yksinkertainen mitta, joka laskee, montako alkiota annetussa osajoukossa on. Tätä kutsutaan laskentamitaksi (engl. counting measure). Jos joukko on vielä diskreetti, niin voidaan lukuväleille antaa luontevasti mitta, ja kaikki osajoukot ovat mitallisia. Mikäli nyt yritetään relaatiota R käyttämällä luoda Vitalin joukko, törmätään ongelmiin sen ei-mitaalisuuden osoittamisen kanssa: V on nimittäin tässä tapauksessa äärellinen, joten se on mitallinen.

Tehdään toinen koe: hylätään irrationaaliluvut, ja käytetään vain rationaalilukuja. Onko olemassa mittaa, joka on määritelty koko joukossa $P(\mathbb{Q})$ ja joka antaa lukuvälin $[a,b]_{\mathbb{Q}}$ mitaksi $b-a$? Vastaus on ei:

$$[0,1]_{\mathbb{Q}} = \bigcup_{x \in [0,1]_{\mathbb{Q}}} \{x\},$$

eli väli $[0,1]_{\mathbb{Q}}$ voidaan esittää erillisten, samankokoisten joukkojen numeroituvana unionina, jolloin sen mitta on joko 0 tai ∞. Tämä on ristiriidassa sen kanssa, että sen mitan pitäisi kaiken järjen mukaan olla 1. Se, että rajoitetulla välillä on äärettömän monta lukua, aiheuttaa jälleen ongelmia.

Mielestäni kaikkein järkevintä on hylätä premissi 5 eli luopua reaalilukujen joukosta ja korvata se paremmmin käyttäytyvällä lukujoukolla. Tämä voi kuulostaa radikaalilta, mutta todisteiden valossa alkaa näyttää vahvasti siltä siltä, että tarvitaan diskreetti ja numeroituva lukujoukko, jotta ei-mitallisia joukkoja ei ole. Tämä ratkaisu estää myös Banachin-Tarskin paradoksin, koska kyseinen tulos edellyttää ei-mitallisten joukkojen olemassaoloa. Mikäli myös lukuavaruus on diskreetti ja numeroituva, niin kaikki osajoukot ovat siinäkin mitallisia, eikä paradoksaalisia hajotelmia voida tehdä. Mikäli valinta-aksiooma hylätään, jolloin kaikki joukot saadaan myös mitallisiksi, joudutaan painimaan uusien ongelmien kanssa.

Huomautus 8. On huomattava, ettei ole vielä tiedossa, johtaako kuvattu lukusysteemin uudistaminen uusiin paradokseihin ja ongelmiin, koska asiaa ei vielä ole tutkittu.

Vastaavanlainen tarkastelu voitaisiin tehdä myös Banachin-Tarskin paradoksille, mutta tässä tutkielmassa se jätetään nyt tekemättä sekä aiheen monimutkaisuuden takia että siksi, koska ei-mitallisten joukkojen poistaminen ratkaisee myös tämän ongelman, kuten jo todettiin.

6.3 Loppuajatukset

Esitän, että nykyistä matematiikan teoriaa voisi uudistaa. Banachin-Tarskin paradoksia ei mielestäni voi sivuuttaa sanomalla, että matematiikka tuottaa epäintuitiivisia tuloksia. Ei ole mitään fyysistä perustetta uskoa, että sellainen olisi mahdollista. Mikäli joku toteaa, ettei sellaisia "palasia" ole oikeasti olemassa, niin samalla hän myöntää, että teoriamme käsittelee todellisuudesta irrallaan olevia olioita ja tuottaa ennusteita, jotka eivät pidä paikkaansa. Empiirisissä tieteissä sellainen teoria hylättäisiin tai vähintäänkin myönnettäisiin, että teoria on puutteellinen. Joku voisi sanoa, että matematiikka on jotain abstraktia ja maailmasta erillistä, eikä sen tarkoituskaan ole vastata todellista maailmaa. Mitä sellaisella teorialla oikein tekee?

Voidaan tietysti sanoa, että matematiikka ja sen aksiomatiosointi ovat eräänlaista mallintamista. Voi käydä niin, että haluttujen ominaisuuksien mukana tulee myös ei-toivottuja ominaisuuksia eli ns. paradokseja. Tämä on totta, ja paremman puutteessa tämä on hyvä argumentti. Kuitenkin olisi hyvä myös kyseenalaistaa olemassa olevaa teoriaa, ja jos näyttää siltä, että on olemassa malli, jonka selitysvoima on sama tai vahvempi kuin standarditeorian ja tämä uusi malli ei tuota paradokseja, niin on syytä hylätä vanha teoria ja käyttää uutta. Tietysti esittämäni uudistus vaatii erittäin tarkkaa tutkimusta, ennen kuin se voidaan hyväksyä.

Nähdäkseni valinta-aksiooma ei ole se, joka tuottaa ongelmia, vaan mielestäni se on nykyinen lukusysteemi. Filosofisesti voidaan argumentoida, että Banachin-Tarskin paradoksi antaa viitteitä siitä, että avaruus on diskreetti. Mikäli näin todellakin on, niin matematiikan teorian tulisi vastata sitä.

Viitteet

[1] Herbert B. Enderton, *Elements of Set Theory*, Academic Press, Elsevier, 1977

[2] Horst Herrlich, *Axiom of Choice*, Springer, Alankomaat, 2006

[3] Bell, John L., "The Axiom of Choice", The Stanford Encyclopedia of Philosophy (Winter 2021 Edition), Edward N. Zalta (ed.), URL = <https://plato.stanford.edu/archives/win2021/entries/axiom-choice/>, luettu 06.07.2023

[4] Paul J. Cohen, *The Independence of the Axiom of Choice*, 1963, https://stacks.stanford.edu/file/druid:pd104gy5838/SCM0405.pdf, luettu 06.07.2023

[5] Andreas Blass, *Existence of Bases Implies the Axiom of Choice*, Contemporary Mathematics Volume 31, 1984 https://dept.math.lsa.umich.edu/∼ablass/bases-AC.pdf, luettu 1.6.2023

Linkki ei toimi. Korvaa "∼"näppäimistöstä löytyvällä variantilla, koska LaTeX ei sitä jostain syystä tunnista, ja LaTeX:in versio ei kelpaa nettiosoitteessa.

[6] Martin Väth, *Nonstandard Analysis*, Birkhauser Verlag, 2007

[7] Ilkka Holopainen, *Mitta ja Integraali*, 2004, https://www.mv.helsinki.fi/home/iholopai/MitInt02.pdf, luettu 06.07.2023

[8] Stan Wagon, *The Banach-Tarski Paradox*, Cambridge University Press, New York, 1985

[9] Stefan Banach, *Sur le problème de la mesure*, Fundamenta Mathematicae, Volume 4, Issue 1, s.7-33 1923

[10] Markku Koppinen, *Algebran peruskurssi I*, Turun Yliopisto, 2005

[11] Markku Koppinen, *Algebran peruskurssi II*, Turun Yliopisto, 2008

[12] Jussi Väisälä, *Topologia I*, Limes ry, 2012

[13] Interior of a set. Encyclopedia of Mathematics. URL: http://encyclopediaofmath.org/index.php?title=Interior of a set"et"oldid=54692

(lisää alaviivat välien paikalle osoitteessa ja korvaa "et" asiaan kuuluvalla merkillä), luettu 29.11.2023