.

3 Lyhyt katsaus aksiomaattiseen joukko-oppiin[2]

Matematiikan historia, erittäin lyhyt oppimäärä.

Sinänsä matematiikka on yksi vanhimpia ihmisten harrastamia tieteitä. Matematiikkaa tutkittiin ja matemaattisia tuloksia sovellettiin jo ainakin Muinais-Egyptissä ja oletettavasti sitä ennenkin. Meni kuitenkin tuhansia vuosia, ennen kuin tajuttiin, että matematiikkaa kaipaa perusta ja formaalisointia. Osittain tämä johtui siitä, että pitkään ei ollut erityistä tarvetta formalismiin. Sellaisia matemaattisia objekteja kuten luvut, geometriset kuviot tai funktiot käsiteltiin "intuitioon" pohjalta ja se riitti. Muinais-Kreikassa kyllä tosin huomattiin, että geometrian tutkimus helpottuu ja täsmällistyy, jos se tehdään "aksiomaattisesti" eli johdetaan kaikki tulokset pienestä joukosta lähtöoletuksia ("aksioomista"), jotka tuntuivat "intuitiivisesti selviltä" eli oli helposti hyväksyttävissä sellaisinaan. Euklidisesta geometriasta tuli historian ensimmäinen esimerkki aksiomaattisesta teoriasta. Hyvin pitkään se oli myös ainoa aksiomaattinen teoria. Syystä tai toisesta tuhansien vuosien aikaan kukaan ei varsinaisesti yrittänyt aksiomatisoida muita matemaattisia aloja ja käsitteitä. Kuitenkin mitä enemmän matemaattista tietoa ihmiskunta on onnistunut löytämään[3], sitä enemmän vastaan alkoi tulla tilanteita, joissa intuitio ei enää riittänyt. Jossakin vaiheessa (suurin piirtein 1800-luvulla) alkoi tulla selväksi, että matematiikka kaipaa kunnon perustan.

Vuonna 1874 saksalainen matemaatikko Georg Cantor julkaisi tieteelliseen artikkelin " Ueber eine Eigenschaft des Inbegriffes aller reellen algebraischen Zahlen" ("Algebrallisten lukujen karakteristisesta ominaisuudesta"), jossa hän esitti keksimänsä joukko-opin alkeita. Cantor kehitti joukko-oppia "puolivahingossa", työkaluna omaan tutkimukseen, joka käsitteli muun muassa trigonometrisia polynomeja eli oli muuten aika kaukana puhtaasta joukko-opista. Pian kuitenkin selvisi, että tässä ja muissa Cantorin artikkelissa esitetyt joukko-opilliset ideat kelpaavat aivan mainiosti matematiikan

[2]Tämä kappale ei ole kurssin kannalta aivan välttämätön ja lisätty yleissivistyksen ja selkeyden vuoksi. Jatkossa tarvitsemme siitä vain tietoa valinta-aksioomasta ja äärettömyysaksioomasta. Kappaleen ymmärtäminen ei ole tärkeätä ja sen voi halutessaan jättää lukematta. Kappaleen sisällöstä ei tule pakollisia kotitehtäviä.

[3]tai keksimään. Kysymys siitä, onko matematiikka jotakin mitä "löydetään" eli objektiivisesti olemassa ihmisistä riippumatta, vai onko se vain ihmisten keksimä työkalu on mielenkiintoinen filosofinen ongelma.

perusteeksi. Osoittautui, että kaikki tähän menneessä keksityt matemaattiset käsitteet, kuten reaaliluvut, funktiot, geometriset ja algebralliset oliot, voidaan esittää joukko-opin puitteissa - kaikkia niitä voi tulkita erikoistapauksina ”joukoista”. Vaikka jotkut matemaatikot vastusti joukko-oppia ja erityisesti äärettömien joukkojen käsittelyä aitoina matemaattisina olioina[4], loppujen lopuksi joukko-oppi hyväksyttiin matematiikan lähtökohdaksi.
Tässä joukko-opissa oli kuitenkin vakavia puutteitakin. Uudella matematiikan perustalla ei itsellään ollut perusta. Cantorin kehittämä joukko-oppi oli ”naiivia” ja epäformaalia. Se onnistui ikään kuin korvamaan kaikki aikaisemmat erilliset intuitiiviset käsitykset sieltä ja täältä yhdellä ”joukon” intuitiivisena käsitteenä. Koska koko matematiikan perustan löytäminen liittyi vahvasti myös pyrkimykseen formalisoida matematiikkaa niin pitkälle kuin oli mahdollista, ei-formalisoitu ”naiivi” joukko-oppi tuntui tietenkään epätyydyttävältä ratkaisulta.
Formaalisuuden puute ei kuitenkaan ole naiviin joukko-opin suurin ongelma. Jos naiivi käsitys joukosta ”mielivaltaisesta ajateltavissa olevana kokoelmana” toimisi aina moitteettomasti, sen epäformaalin luonteen kanssa olisi voinut elää. Kuitenkin paljon vakavampi ongelma ilmeni, kun paljastui, että naiivi joukko-oppi *johtaa ristiriitoihin.*

Mikä on ristiriita ja miksi se on huono asia?
Nykymatematiikka on melko ”liberaali” tiede. Mitä vaan voidaan tutkia matemaattisesti, kunhan se on määritelty täsmällisesti, myös tilanteita jotka eivät ole sopusoinnissa muun matematiikan tai ”todellisuuden ” kanssa. Esimerkiksi voidaan tutkia matemaattisesti mitä tapahtuu jos $1+1=3$. Melkein kaikki on sallittua - paitsi ristiriidat.
Sanalla ”ristiriita” on matematiikassa tarkka merkitys. Ristiriidalla tarkoitetaan tilannetta, jossa onnistumme todistamaan jokin väite A sekä todeksi, että epätodeksi. Teorian kannalta se tarkoittaa sitä, että tilanne on ”mahdoton” - sillä ei voi olla niin sanottua *mallia.* Malli on matemaattinen olio, joka toteuttaa joitakin oletuksia (eli *aksioomia*). Esimerkiksi mikä tahansa joukko, joka toteuttaa reaalilukujen määritelmän on malli reaalilukujen aksioomille.
Jos oletukset johtavat ristiriitaan - se tarkoittaa sitä, että näillä oletuksella ei voi olla mallia, ne eivät voi päteä samanaikaisesti missään ”maailmassa”, jopa abstraktissa matemaattisessa maailmassa. Esimerkiksi, jos onnistumme todistamaan reaalilukujen aksioomista lähtien, että on olemassa reaaliluku, joka on samaan aikaan positiivinen ja negatiivinen, tämä tarkoittaa sitä, että

[4]Esimerkiksi siihen aikaan erittäin vaikutusvaltainen saksalainen matemaatikko Leopold Kronecker arvosteli Cantorin teoriaa ankkarasti.

mitään reaalilukuja ei voi olla olemassa.
Toinen seikka, joka tekee ristiriidasta "kelvottoman" matematiikan näkökulmasta, on se, että "ristiriidasta voidaan päätellä mitä vaan". Näin ollen, jos jokin teoria sisältää ristiriidan, niin tässä teoriassa **jokainen** väite on tosi - ja yhtä hyvin epätosi! Ristiriita siis tekee teoriasta täysin triviaalin ja tylsän - kun kaikki on totta, ei ole mitään tutkittavaa eikä saada mitään mielenkiintoisia tuloksia. Koska matematiikan päämääränä on erottaa tosia väitteittä epätosista, ristiriitaiset teoriat eivät ole kiinnostavia.

Mihin ristiriitoihin naiivi joukko-oppi johtaa? Kuuluisin ja historiallisesti myös ensimmäisiä tällaisia ristiriitoja on kuuluisa paradoksi, jonka keksi englantilainen matemaatikko ja filosofi Bernard Russell 1900-luvun alussa.

Russelin paradoksi on joukko-opillinen versio tunnetusta parturin paradoksista[5]. Kuvitellaan, että eräässä kylässä asuu tasan yksi miespuolinen parturi. Kylässä vallitsevan kulttuurin mukaan kaikilla miehillä pitää olla siististi ajellut kasvot, parrakkaita äijiä ei hyväksytä. Kuitenkin eivät aivan kaikki kylässä asuvat miehet osaa ajaa partaansa. Näin ollen parturimme **ajaa parran niiltä ja vain niiltä kylän miehiltä, jotka eivät aja partaansa itse**. Sääntö kuulostaa ensi näkemältä järkevältä, kunnes ruvetaan miettimään ajaako parturi oman parran itse. Jos hän ajaa partansa itse, niin hän on yksi niistä kylän miehistä, jotka ajavat partansa itse, eivätkä sitten tarvitse parturin palveluja. Sellaisten miesten partoja parturimmehan ei ajaa. Näin ollen, jos parturi ajaa partaansa, siitä seuraa, että hän ei ajaa partansa.
No, ehkä hän ei sitten ajakaan partaansa. Mutta tällöin hän on yksi niistä, jotka eivät ajaa partaansa itse, joten hänen on mentävä itseensä luo parranajolle! Päädytään taas hassuun ristiriitaan - jos hän ei ajaa partaansa, siitä seuraa, että hän ajaa partansa.

Varsinainen matemaattinen Russelin paradoksi määritellään seuraavasti. Joukkojen välillä joukko-opissa on määritelty kuuluvuussuhde - toiset joukot ovat toistensa alkioita. Esimerkiksi jokainen joukko on oman potenssijoukon alkio. Yleensä joukot eivät ole itseensä alkiota, esimerkiksi kaikkien kissojen muodostama joukko ei ole itse kissa. Periaatteessa voi olla myös joukkoja, jotka ovat itseensä alkioita. Esimerkiksi kaikkien joukkojen muodostama kokoelma eli kaikkien joukkojen joukko on itseensä alkio - onhan se itse joukko. Näin ollen voimme myös muodostaa joukon A, jonka alkiot ovat tasan ne

[5] Tai oikeastaan parturin paradoksi on "maallikon" versio Russelin paradoksista - se keksittiin Russelin paradoksin jälkeen nimenomaan havainnollistamaan Russelin paradoksia

joukot, jotka eivät ole itseensä alkioita. Toisin sanoen

$$A = \{X \text{ on joukko } \mid X \notin X\}.$$

Jokainen mielekäs väite on joko tosi tai ei. Näin ollen myös väitteen "$A \in A$" pitää olla joko totta tai epätotta. Molemmat vaihtoehdot kuitenkin johtavat ristiriitaan samalla tavalla kuin parturin paradoksissa. Jos A on A:n alkio, niin A on sellainen joukko joka ei ole itseensä alkio (A:n määritelmän mukaan) eli A ei ole A:n alkio. Oletus $A \in A$ siis johtaa itseensä vastakohtaan $A \notin A$. Koska mikään väite ei voi olla tosi ja epätosi samaan aikaan, tämä on mahdottomuus.
Jos taas $A \notin A$, se tarkoittaa sitä, että A on sellainen joukko, joka ei ole itseensä alkio, joten sen pitää kuulua joukkoon A (sen määritelmän nojalla) eli kuulua itseensä. Saatiin taas ristiriita - oletus $A \notin A$ johtaa itseensä vastakohtaan $A \in A$.
Molemmat vaihtoehdot johtavat ristiriitaan. Ainoa mahdollisuus selvittyä tästä on luopua joukon A olemassaolosta. Myös kaikkien joukkojen joukko ei voi olla olemassa, sillä jos se olisi olemassa, A olisi olemassa sen osajoukkona.

Russelin paradoksiin sisältyvä opetus on siinä, että joukko-opissa pitää luovuttaa intuitiivisesta näkökulmasta, jonka mukaan kaikki ajateltavissa olevat kokoelmat hyväksytään joukoksi matemaattisessa mielessä. Jos P on joku "ehto" tai "ominaisuus", emme aina voida määritellä joukon

$$\{x \mid x\text{:llä on } P\},$$

sillä sen olemassaolo voi tuottaa ristiriitoja. Russelin paradoksissa esimerkiksi päädytään ristiriitaan, kun yritetään määritellä tällä tavalla joukko ominaisuuden $P = (x \notin x)$ avulla.
'

Mutta jos emme saa enää "luoda" joukkoja mielivaltaisina kokoelmina aina omien tarpeiden mukaan, miten sitten muodostamme joukkoja? Miten teemme joukko-opillista matematiikkaa? Kokemus on osoittanut, että jos haluamme tehdä matematiikkaa ihan käytännönkin tasolla (esimerkiksi differentiaalilaskennan tasolla), nojaudumme jatkuvasti kaikenlaisiin joukko-opillisiin konstruktioihin kuten esimerkiksi yhdiste, leikkaus, potenssijoukko, osajoukon muodostaminen. Naiivissa joukko-opissa näiden operaatioiden mielekkyys on tavallaan itsestään selvää, sillä siinä joukko ajatellaan mielivaltaisena ajateltavissa olevana kokoelmana.
Ratkaisu on seuraava - kehitetään tarkkoja sääntöjä, jotka kertoisivat mitä joukkoja saamme muodostaa ja millä periaatteilla. Tällaisia sääntöjä sanotaan "joukko-opin aksioomiksi". Aksioomien pitäisi sallia yllämainittuja tärkeitä konstruktioita - yhdiste, leikkaus, potenssijoukko ja niin edelleen, niin

että pääsemme näiden aksioomien viitekehyksessä kehittämään kaikkea hyödylliseksi osoitettua matematiikkaa. Russelin paradoksin kaltaisia ristiriitaisia tilanteita pitää taas sulkea pois.

Aksiomaattinen joukko-oppi on joukko-opin tarkka formaalisointi tällaisten aksioomien avulla. On keksitty erilaisia tapoja aksiomatisoida joukko-oppia, seuraavassa tutustumme pintapuolisesti niistä kaikista ehkä tunnettuun eli **ZFC-teoriaan**. Nimitys ZFC on lyhenne teorian nimestä "**Z**ermelo-**F**raenkel set theory with the axiom of **c**hoice". Saksalainen matemaatikko Zermelo esitti ensimmäisen yrityksen aksiomatisoida joukko-oppia vuonna 1908. Myöhemmin hänen aksioomia täydennettiin ja tarkennettiin Abraham Fraenkelin työn seurauksena.
ZFC:ssä voi tehdä melkein kaiken, mitä naiivissa joukko-opissa voi tehdä. Joukoista voi muodostaa yhdisteitä, leikkauksia ja niin edelleen. Osajoukkoja voi konstruoida ehtojen avulla ja joukon potenssijoukko on aina olemassa. Käytännössä naiivilla joukko-opilla pärjää mainiosti, kunhan muistaa, että ei saa tarkastella mielivaltaisia kokoelmia (esimerkiksi "kaikki ryhmät" tai "kaikki joukot"), käyttää "epämatemaattisia" ehtoja (tässä tulee esimerkki kohta) tai määritellä objekteja, jotka viittaavat itseensä (tästäkin tulee valaiseva esimerkki).
Ennen kuin mennään varsinaisiin ZFC-aksioomiin, tarkastellaan hieman tarkemmin joukon muodostamista ehdon avulla, eli muodossa

$$\{x \mid x\text{:llä on ominaisuus } P\}.$$

Kuten Russelin paradoksi osoittaa, joukon muodostamista tällä periaatteella ei voi sallia ihan kaikilla mahdollisilla ominaisuuksilla P. Kuitenkin tämä on käytännössä tärkeä periaate, joten ei sitä voi ihan kokonaan kieltääkään. Esimerkiksi jos haluamme muodostaa positiivisten reaalilukujen joukon, se on konstruoituvaa muodossa

$$\{x \text{ on positiivinen reaaliluku}\}.$$

Olisi suorastaan mahdotonta tehdä matematiikkaa, jos kaikkea tällaista kieltää, joten pitää asettaa rajat sille minkälaisen ominaisuuden P on oltava, että kyseinen joukko olisi hyväksyttävissä joukoksi. ZFC:ssä tämä ratkaistaan seuraavalla kompromissilla - sallitaan ainoastaan **osajoukkojen** muodostamista tällä tavalla. Toisin sanoen jos A tunnetaan jo olevan joukko ja P on ominaisuus, hyväksytään myös osajoukon

$$B = \{x \in A \mid x\text{:llä on ominaisuus } P\}$$

olemassaoloa. Näin ollen, jos reaalilukujen joukko $\mathbb{R}$ oletetaan olevan olemassa, voimme käyttää tätä periaatetta muodostamaan positiivisten reaalilukujen joukko kaavalla

$$\{x \in \mathbb{R} \mid x > 0\}.$$

Tarkka lukija voisi tässä vaiheessa huomauttaa, että ”ominaisuus” on hieman epämääräinen käsite, ja jos kerran pyritään tehdä kaikki täsmällisesti ja formaalisti, eikös sekin pitää määritellä tarkasti? Vastaus on ”kyllä, olet oikeassa”. Sallituille ”ominaisuuksille” P annetaan täsmällinen määritelmä, jonka joukko-oppi itse asiassa lainaa matemaattiselta logiikalta. Meillä ei ole tällä kurssilla aikomusta mennä syvällisesti matemaattisen logiikan puolelle, mutta mainitaan kuitenkin lyhyesti miten ”ominaisuus” määritellään täsmällisesti. Ominaisuuden käsite korvataan ”loogisen kaavan” käsitteellä. Kaavoja rakennetaan niin sanotuista muuttujasymboleista $x, y, z, A, B, \ldots$, jotka voivat olla esimerkiksi kirjaimia, ja peruskaavoista, jotka ovat muotoa $x \in y$ ja $x = y$, yhdistämällä niitä tiettyjen sääntöjen mukaan. Nämä säännöt voidaan tiivistää seuraviin muotoihin - jos kaavat P ja Q ovat jo konstruoituja, voimme konstruoida kaavoja ’ei P’, ’P tai Q’, ’P ja Q’, ’P:stä seuraa Q’, P jos ja vain jos Q, ’kaikilla x pätee P’, ’on olemassa x niin, että P’. Luonnollisen kielen sanoille ’ei’, ’ja’, ’tai’ ja niin edelleen annetaan täsmällinen merkitys ja niitäkin ei kirjoiteta sanoin vain merkitään formaaleilla symboleilla $\neg$ (ei), $\vee$ (tai), $\wedge$ (ja), $\rightarrow$ (seuraa), $\Leftrightarrow$ (jos ja vain jos), $\forall$ (kaikilla), $\exists$ (on olemassa). Lisäksi käytetään sulkuja, jos lauseet ovat tarpeeksi monimutkaisia, osoittamaan missä järjestyksessä ne pitää lukea ja ymmärtää. Yhtäsuuruussymboli $=$ tulkitaan luonnollisella tavalla ja oletetaan, että se toteuttaa itsestään selviä yhtäsuuruuden ominaisuuksia, kuten $x = x$ on tosi jokaisella x ja niin edelleen.

Näitä sääntöjä rekursiivisesti soveltamalla saadaan joukko-opillisia kaavoja. Tällaiset kaavat ovat oikeastaan *väitteitä*, jotka voivat olla tosia tai epätosia, rippuen tilanteesta. Esimerkiksi kaava ’on olemassa x siten, että kaikilla y pätee ($y \in x$ jos ja vain jos $y \notin y$)’ väittää, että on olemassa sellainen joukko x (teorian kaikki objektit, joihin muuttujasymbolit kaavassa viittaavat ovat joukkoja!), niin, että mikä tahansa muu joukko y on tämän x:n alkio jos ja vain jos y toteuttaa ehdon $y \notin y$. Toisin sanoen kaava asettaa Russelin paradoksissa esiintyvän joukon olemassaoloa. Kuten Russelin paradoksi osoittaa, tämä kaava ei voi olla tosi, jos ei haluta ajautua ristiriitoihin.

Kaava ’on olemassa x siten, että kaikille y ei päde $y \in x$’ puolestaan asettaa tyhjän joukon olemassaoloa. Tämä kaava on tosi tavanomaisessa joukko-opissa. Halutessaan kaikki joukko-opin aksioomat ja koko matematiikkaa voidaan kirjoittaa tällaisina loogisina kaavoina. Käytännössä tietenkin kaavoista tulee hyvin nopeasti liian pitkiä ja vaikeasti ymmärrettäviä, joten ne kirjoitetaan auki käyttämällä luonnollista kieltä ja lyhenteitä.

Palataksemme osajoukkojen muodostamiseen, voimme nyt muotoilla tällaista muodostamisperiaatetta täsmällisesti seuraavassa muodossa. Olkoon A joukko ja P kaava, jossa ei esiinny symboli B. Tällöin väite "on olemassa B siten että jokainen $x \in B$ kuuluu A:han ja toteuttaa ehdon P " on tosi. Tämä periaate on yksi ZFC-aksioomista, *osajoukko-aksiooma*.
Vaatimus "P:n täytyy olla laillinen formaaleilla säännöillä muodostettu kaava" on välttämätön myös siitä syystä, että ilman siitä voidaan ajautua taas ristiriitoihin.

Esimerkki 44. *Oletetaan luonnollisten lukujen* $\mathbb{N}$ *joukko tunnettuna ominaisuuksine. Yritetään muodostaa seuraava* $\mathbb{N}$*:n osajoukko*

$$A = \{n \in \mathbb{N} \mid n \textit{ ei voi karakterisoida yksikäsitteisesti}$$

$$\textit{järkevällä suomen kielen lauseella, jossa on kuusitoista sanaa}\}.$$

Suomen kieli on kaikessa rikkaudessaan kuitenkin äärellinen (sovitaan esimerkiksi, että saa käyttää vain sanoja, jotka esiintyvät jossakin tietyssä virallisessa sanakirjassa), joten on olemassa vain äärellinen määrä lauseita, jotka sisältävät 16 *sanaa. Koska* $\mathbb{N}$ *on ääretön, tästä seuraa, että pitää olla olemassa myös sellaisia luonnollisia lukuja, joita ei voi mitenkään karakterisoida* 16 *sanalla.* A *on siis epätyhjä. Jokaisessa* $\mathbb{N}$ *epätyhjässä osajoukossa on olemassa pienin alkio, näin ollen on olemassa pienin* $n \in A$*. Mutta tällöin* n *voidaan karakterisoida yksikäsitteisesti suomen kielen lauseella 'pienin luonnollinen luku, jota ei voi karakterisoida yksikäsitteisesti järkevällä suomen kielen lauseella, jossa on kuusitoista sanaa'. Tässä lauseessa on kuitenkin tasan* 16 *sanaa, joten* n *ei voi olla* A*:n alkio. Saadaan ristiriita.*
Ongelma on siinä, että ehto "n ei voi karakterisoida yksikäsitteisesti järkevällä suomen kielen lauseella, jossa on kuusitoista sanaa" ei ole muodostettu yllä annettujen sääntöjen mukaan. Se ei ole laillinen kaava. Se on ilmaistu luonnollisella kielellä ja luonnollinen ihmisten kieli ei ole formaali systeemi.

Käytännössä riittää muistaa, että osajoukkoja saa muodostaa käyttämällä ainoastaan täsmällisiä "matemaattisia" hyvinmääriteltyjä operaatioita ja käsitteitä. Niitä voi aina tarvittaessa palauttaa "lailliseen muotoon" (käytännössä harvoin kukaan jaksaa).

Esimerkki 45. *Yllä esitetyssä osajoukko-aksiooman muotoilussa mainitaan myös, että kaava* P *ei saa sisällä viittausta joukkoon* B*, joka yritetään määritellä ominaisuuden* P*. Seuraava esimerkki näyttää, miksi tämä rajoitus on*

välttämätön.
Yritetään määritellä $\mathbb{R}$:n osajoukko B kaavalla

$$B = \{x \in \mathbb{N} \mid x^2 \in B\}.$$

Tässä ominaisuus P on $(x^2 \in B)$ eli se sisältää viittaukseen joukkoon B itse. Kuitenkin tällaisessa osajoukon määritelmässä ei ole mitään järkeä. Jos esimerkiksi yritämme selvittää onko 2 B:n alkio, meidän pitää ensin selvittää kuuluko $4 = 2^2$ joukkoon B. Tämä puolestaan tarkoittaa, että pitää ensin selvittää onko $16 = 4^2 \in B$ totta ja niin edelleen. Emme koskaan pääse loppuun, joten emme pysty selvittää onko $2 \in B$ totta vai ei. Jos taas yritetään päätellä onko $1 \in B$, se palautuu kysymykseen onko $1^2 = 1 \in B$, eli samaan ongelmaan. Emme pääse pidemmälle kuin "$1 \in B$ jos ja vain jos $1 \in B$."

Nyt voidaan vihdoinkin esittää aksiomaattinen ZFC-teoria pähkinäkuoressa.
Jokaisessa aksiomaattisessa teoriassa lähdetään joistakin *määrittelemättömistä käsitteistä*, joiden "todellisesta luonteesta" teoria ei siis tiedä mitään eikä välitä siitä. Esimerkiksi reaalilukujen aksiomaattisessa määritelmässä tällaisia perusobjekteja ovat reaalilukujen joukko $\mathbb{R}$ ja relaatiot $+, \cdot, \leq$. ZFC-teoriassa tällaisia peruskäsitteitä ovat "joukko" ja joukkojen välinen määritelty kuuluvuusrelaatio $\in$. Pannaan erityisesti merkille, että aksiomaattisessa joukko-opissa
(a) Ei ole olemassa mitään eroa joukkojen ja 'alkioiden' välille, itse asiassa kaikki objektit, mukaan lukien jokaisen joukon alkiot, ovat myös itse joukkoja.
(b) Kuuluvuusrelaatio $\in$ ei ymmärretä kirjanmielisesti, kuten joukko-opissa eikä joukkoa siis ajatella alkioidensa muodostavana kokoelmana, kuten naiivissa joukko-opissa. Oikeastaan ei oteta mitään kantaa siihen, mitä relaatio $\in$ "oikeasti " on ja minkälaisia objekteja joukot "oikeasti" ovat. Tärkeintä on se, että $\in$ on joku suhde teorian objektien välillä, joka toteuttaa ZFC:n aksioomia[6]. Tietysti konkreettinen naiivi tulkinta alkioiden muodostamasta joukosta on edelleenkin hyödyllinen mielikuva ja käytämme sitä jatkossakin.

Tässä sana "relaatio" täyttyy ymmärtää "alkeellisemmassa mielessä" - kyse ei ole joukko-opillisesta relaatiosta joukkojen alkioiden välillä (joka määriteltiin viime luvussa). Sehän voidaan määritellä vain joukko-opin sisällä, vas-

[6]Tietojenkäsittelyyn perehtyneelle tilanne on tuttu olioohjelmoinnista. Ei ole mitään merkitystä miten olio on toteutettu käytännössä, ainoastaan sen ominaisuudet näkyvät ulospäin ja ainoastaan niillä on merkitysä. Ei ole ainoata oikeata tapaa konstruoida olio, vaan mikä tahansa toimiva tapa on yhtähyvä kuin mikä tahansa muu

ta silloin kuin se on määritelty ja lisäksi vain joukkojen välillä. Asia käsitellään tarkemmin matemaattisessa logiikassa, tässä sivutamme tätä ongelmaa. Halutessaan asiaa voi ajatella näin - $\in$ on vain eräs symboli, jonka merkitystä emme määrittele. Aksioomat kertovat mitä ominaisuuksia tällä symbolilla on.

ZFC teorian aksioomat:

Ekstensionaalisuus-aksiooma - Kaksi joukkoa A ja B ovat sama joukko jos ja vain jos ne sisältävät samoja alkioita. Täsmällisesti - kaikilla A ja B väite $A = B$ pätee jos ja vain jos jokaisella joukolla x väite $x \in A$ pätee jos ja vain jos $x \in B$ pätee.

Tämä aksiooma saattaa tuntua itsestään selvältä ja turhalta, mutta se johtuu siitä, että joukkoja on tottunut ajattelemaan konkreettisesti alkioidensa muodostamana kokoelmana. Naiivissa joukko-opissa tämän aksiooman sisältämä väitehän seuraa joukkojen yhtäsuuruuden määritelmästä.
Aksiomaattisessa lähestymistavassa joudutaan lisäämään tämä periaate eksplisiittisesti aksioomana, koska se ei seuraa mistään muusta periaatteesta. Nythän $\in$ on vain joku suhde joidenkin objektien (joita me kutsumme "joukoiksi") välillä. Periaatteessa mikään ei estä sitä, että kahteen eri objektiin on liitetty samoja olioita. Esimerkiksi kuvitellaan "malli" joukko-opille, jossa on kolme objektia eli joukkoa, A, B, C. Relaatio $\in$ niiden välillä määritellään asettamalla, että $A \in B$ ja $A \in C$ (eikä mitään muita suhteita oleteta). Nyt B ja C "sisältävät" samoja alkioita, mutta ovat eri objektia.
Ekstensionaalisuus-aksiooma kannattaakin ymmärtää täsmällisenä formaalina tapana koodata naiivi ajatus "alkiot määritelevät muodostamansa joukon yksikäsitteisesti" tarkaksi matemaattiseksi väitteeksi. Juuri ekstensionaalisuus-aksiooman ansioista voimme käytännön laskuissa edelleenkin mieltää joukkoja alkioidensa muodostamin kokoelmina.

Osajoukkoaksiooma. Tästä puhuttiin jo edellä. Osajoukkoaksiooma sanoo, että jos A on joukko ja P on laillinen joukko-opillinen kaava eli "ominaisuus", joka ei sisällä viittausta symboliin B, niin on olemassa osajoukko

$$B = \{x \in A \mid P \text{ on tosi } x\text{:lle}\},$$

joka koostuu siis tasan niistä A:n alkioista, jotka toteuttavat ominaisuuden P.
Ekstensionaalisuus-aksioomasta seuraa, että tällainen osajoukko on myös yksikäsitteinen, koska kaksi joukkoa, jotka toteuttavat B:n määritelmän sisältävät täsmälleen samoja alkioita.

Yhdisteaksiooma. Olkoon A joukko. Tällöin yhdiste A:n yli $\cup A$ on olemassa. Tässä A ajatellaan siis joukkoperheenä. Ovathan kaikki A:n alkiot itse joukkoja. Yhdisteeseen $\cup A$ kuuluvat määritelmän mukaan tasan ne joukot x, joille löytyy ainakin yksi $y \in A$, niin, että $x \in y$. Aksiooma asettaa, että on olemassa joukko, joka sisältää täsmälleen tällaisia joukkoja. Ekstensionaalisuus-aksioomasta jälleen seuraa, että $\cup A$ on myös yksikäsitteinen.
Aksioomasta erityisesti seuraa, että kahden joukon A, B yhdiste $A \cup B$ on olemassa, JOS on olemassa joukko $\{A, B\}$ (jonka yli ottamalla yhdisteen saa juuri joukon $A \cup B$) ja sitä itse asiassa emme voi vielä päätellä - tarvitaan muita aksioomia.
Leikkaukselle ja erotukselle sen sijaan erillisiä aksioomia ei tarvita, koska niiden olemassaolo voidaan johtaa osajoukkoaksioomasta. Esimerkiksi $A \cap B$ voidaan konstruoida sellaisena A:n osajoukkona, joka sisältää alkioita x, joille myös pätee $x \in B$ eli muodossa

$$A \cap B = \{x \in A \mid x \in B\}.$$

Samoin voidaan hoitaa mielivaltaisen leikkauksen $\cap A$ tapaus, **paitsi** jos $A = \emptyset$. Leikkaus tyhjän joukon yli $\cap\emptyset$ ei itse asiassa ole olemassa - määritelmän mukaan sen täytyy sisältää kaikkia joukkoja, mutta ei tällaista "kaikkien joukkojen joukkoa" ole ZFC:n teoriassa olemassa. Kuten Russelin paradoksin yhteydessä nähtiin, sen olemassaolo johtaisi ristiriitaan.

Potenssijoukkoaksiooma sanoo, että jokaisen joukon A potenssijoukko $\mathcal{P}(A)$ on olemassa. Potenssijoukko on siis joukko, johon kuuluvat alkioina tasan kaikki A:n osajoukot. Osajoukko määritellään samalla tavalla kuin naiivissa teoriassa - $B \subset A$ on lyhenne kaavalle 'jokaiselle $x \in B$ pätee $x \in A$'.

Korvausaksiooma. Epäformaalisti tämä aksiooma sanoo, että "kokoelma joka näyttää joukon kuvalta jossakin kuvauksessa on itse joukko ". Sen tarkka formulointi on aika monimutkainen, joten tyydytään vain epäformaalin käsittelyyn. Kyse on siis seuraavasta. Olkoon I jokin joukko ja kuvitellaan, että jokaisella $i \in I$ on annettu joukko A_i. Tämä melkein tarkoittaa sitä, että voimme muodostaa kuvauksen f, jonka määrittelyjoukko on I ja joka on määritelty kaavalla $f(i) = A_i$. Ongelma on kuitenkin siinä, että tältä kuvaukselta puuttuu "maalijoukko", eli emme tiedä a priori, että kaikki joukot A_i kuuluisivat johonkin joukkoon B. Korvausaksiooma sanoo juuri sen, että tällainen joukko löytyy, joten kuvauksen sekä kuvajoukon muodostaminen onnistuu. Täsmällistä määritelmää varten pitää tietenkin formalisoida miten tällainen "funktio", jolta puuttuu maalijoukko, tarkoittaa.

Esimerkkinä korvausaksiooman käytöstä näytetään, miten voidaan konstruoida kahden alkion joukko $\{A, B\}$ mielivaltaisille joukoille A ja B. Riittää konstruoida jokin yksi joukko $\{x, y\}$, jolla on tasan kaksi alkiota. Sen jälkeen voimme muodostaa 'kuvauksen' $f(x) = A, f(y) = B$, jolloin korvausaksioomasta seuraa, että kuvajoukko $\{A, B\}$ on olemassa. Tämän jälkeen voidaan vedota yhdisteaksiooman ja muodostaa yhdiste tämän joukon yli eli yhdisteen $A \cup B$.
Jäljellä on jonkun kahden alkion joukon konstruktio. Tämä ei itse asiassa onnistu vielä tässä vaiheessa, sillä miellä ei ole vielä yhtäkään aksioomaa, joka takaisi jonkun joukon olemassaoloa, ilman että pitää olettaa ensin jonkun toisen joukon olemassaoloa. Kaikki aksioomat tähän menneessä olivat "relatiivisia" - ne sanovat, että joitakin ominaisuuksia omaava joukko on olemassa, SILLÄ OLETUKSELLA, että joku toinen joukko on jo olemassa[7].
Alla esitetään äärettömyysaksioomaa, josta muun muassa seuraa ainakin yhden joukon X olemassaolo. Sen jälkeen voidaan esimerkiksi konstruoida (osajoukkoaksiooman avulla) tyhjä joukko X:n osajoukkona

$$\{x \in X \mid x \notin X\}.$$

Tämän jälkeen potenssiaksiooman avulla voidaan konstruoida potenssijoukko $\mathcal{P}(\emptyset)$, joka on tunnetusti yhden alkion joukko $\{\emptyset\}$. Tämän joukon potenssijoukko

$$\mathcal{P}(\mathcal{P}(\emptyset)) = \{\emptyset, \{\emptyset\}\}$$

sisältää puolestaan tasan kaksi alkiota. Olemme siis konstruoineet kahden alkion joukko, kuten pitikin.

Äärettömyysaksiooma. Tämä on listassamme ensimmäinen ja ainoa aksiooma, joka asettaa jonkun joukon olemassaoloa ilman mitään ennakko-oletuksia. Äärettömyysaksiooma sanoo, että on olemassa ainakin yksi ääretön joukko. Tässä "ääretön" määritellään edellisen luvun määritelmien mukaan eli mahtavuuksia kautta. Mahtavuudet taas vertaillaan käyttämällä kuvauksia, joten pitää ensin konstruoida relaation ja siis karteesisen tulon käsitteen ja osoittaa, että esimerkiksi kahden joukon karteesinen tulo on olemassa. Onneksi tämä seuraa aikaisemmista aksioomista. Tarkka perustelu sivutetaan. Erityisesti on olemassa ainakin yksi joukko eli teoriamme on epätyhjä. Nyt käyttämällä ainoata ääretöntä joukkoa, voidaan konstruoida paljon äärellisiä

[7] Matemaattinen loogikko olisi tästä eri mieltä, koska matemaattisessa logiikassa yleensä oletetaan, että kaikki mallit ovat epätyhjiä, joten jokaisen teoriaan, mukaan lukien ZFC:hen, sisältyy ikään kuin oletus siitä, että ainakin yksi objekti on olemassa. Me ei tästä loogikon saivartelusta välitetä.

joukkoja (sen osajoukkona), sen potenssijoukko, sen potenssijoukon potenssijoukko ja niin edelleen. Näin ollen yhdenkin äärettömän joukon olemassaolo implikoi muiden aksioomien avulla, että joukko-opista tulee tarpeeksi rikas. ”Oikeassa” aksiomaattisessa joukko-opissa äärettömyysaksiooma muotoillaan paljon teknisimmin - siinä vaaditaan käytännössä luonnollisten lukujen joukon olemassaoloa muodossa tai toisessa. Sellaiseen muotoillun on logiikoilla omia syitänsä, joihin emme tässä mene sen tarkemmin. Hieman ”naiivi” muotoilumme äärettömyysaksioomasta riittää mainiosti meidän tarkoituksiin tällä kurssilla.

Valintaaksiooma. Tämä on kaikista aksiomeista ”kiistanalaisin”. Se on ainoa joka mainitaan eksplisiittisesti teorian nimessä, siitä kirjain C lyhennessä ZFC tuleekin. Aksiooman maine johtuu siitä, että sitä pidetään vähemmän intuitiivisena ja itsestään selvältä kuin muita aksioomia. Joukko-opin tutkijat ovat erityisen kiinnostuneita esimerkiksi tutkia kuinka välttämätön se on, eli mitä voidaan todistaa olettamatta valinta-askioomaa. Aivan kaikkea ei kuitenkaan voi - kokemus on osoittanut, että valinta-aksiooma on erittäin hyödyllinen, ja ilman sitä ”ei pärjää” kovin hyvin. Monet tärkeät tulokset eivät päde ilman valinta-aksioomaa. Toisaalta sillä on paljon omituisia seurauksia, joita pidetään selvästi ”epäintuitiivisena”. Esimerkiksi valinta-aksioomasta seuraa kuuluisa ”Banach-Tarskin paradoksi”. Sen mukaan kolmeulotteisen avaruuden yksikköpallo voi jakaa paloihin, joista, kiertämällä ja järjestämällä niitä uudelleen, saadaan konstruoitua kaksi yksikköpalloa. Toisaalta, ilman valinta-aksioomaa ei voida esimeriksi osoittaa, että jatkuvuuden $\varepsilon - \delta$ määritelmä on yhtäpitävä jatkuvuuden määritelmän jonojen kautta kanssa. Ilman valinta-aksioomaa teoria on ikään kuin liian heikko, mutta sen kanssa - liian vahva.

Valinta-aksiooma sanoo seuraavaa. Oletetaan, että meillä on jokin indeksoitu joukkoperhe $(A_i)_{i \in I}$, missä siis I ja kaikki A_i ovat joukkoja. Oletetaan, että jokainen A_i on epätyhjä. Tällöin, valinta-aksiooman mukaan voimme ”valita” jokaisesta A_i:stä yhden alkion ja muodostaa niistä joukon. Toisin sanoen on olemassa joukko B siten, että $B \cap A_i$ on yksiö jokaisella $i \in I$.
On olemassa monta yhtäpitävää tapaa formuloida valinta-aksioomaa. Esimerkiksi yllä mainittu joukko B voidaan tulkita perheenä $(x_i)_{i \in I}$, missä $x_i \in A_i$ jokaisella $i \in I$. Tällainen alkio on määritelmän mukaan yleisen karteesisen tulon $\prod_{i \in I} A_i$ alkio. Näin ollen yksi tapa formuloida valintaa-aksioomaa on sanoa, että mielivaltainen karteesinen tulo epätyhjistä joukoista on epätyhjä.
Valinta-aksioomaa tarvitaan aina kun joudutaan tekemään samanaikaisia valintoja, joita ei voida suorittaa eksplisiittisesti. Sitä ei tarvitse sekoittaa pe-

riaatteeseen, jonka mukaan epätyhjästä joukosta voidaan valita yksi alkio. Siihen ei tarvita valinta-aksioomaa, kyse on vain epätyhjän joukon määritelmästä. Samalla tavalla äärellinen määrä valintoja voidaan tehdä ilman valinta-aksioomaa, eli jos indeksijoukko I on äärellinen, valinta-aksiooman väite voidaan todistaa (induktiolla I:n koon suhteen). Jos kuitenkin I on ääretön, tarvitaan valinta-aksioomaa.
Tunnettu tapa havainnollistaa valinta-aksiooman tarvetta on kuvitella, että äärettömän isossa kaapissa on äärettömän monta kenkäparia ja äärettömän monta sukkaparia. Haluamme varustaa sukilla ja kengillä äärettömän ison armeijan, joka koostuu yksijalkaisista piraateista. Oletetaan vielä yksinkertaisuuden vuoksi, että jokaisella piraatilla puuttuu juuri oikea jalka. Meidän pitää valita jokaisesta kenkäparista yhden kenkään ja jokaisesta sukkaparista yhden sukan. Ensimmäinen valinta voidaan suorittaa ilman valinta-aksioomaa, poimitaan vain jokaisesta parista vasen kenkä. Valinta-aksioomaa emme tarvitse sillä pystymme eksplisiittisesti muodostamaan valintafunktion - se on annettu kaavalla

$$f(\text{pari } x) = \text{parin } x \text{ vasen kenkä.}$$

Sukkien kohdalla kuitenkin joudumme turvautumaan valinta-aksioomaan, sillä parin kaksi sukkaa ovat täysin samanlaisia, niitä ei voi toisistaan erottaa, joten meillä ei ole mitään keinoa muodostaa valintafunktio ”käsin”.

Esimerkki 46. *Esimerkkinä tyypillisestä valinta-aksiooman suorasta sovelluksesta tarkastellaan Lemman 36 kohdan (v) väitettä, joka sanoo, että joukoille X ja Y pätee $|X| \leq |Y|$ jos ja vain jos $X = \emptyset$ tai on olemassa surjektio $f\colon Y \to X$. Se jäi edellisessä luvussa todistamatta, joten todistetaan se nyt.*
Oletetaan, että $X = \emptyset$ tai on olemassa surjektio $f\colon Y \to X$ ja osoitetaan, että $|X| \leq |Y|$. Jos $X = \emptyset$ asia on selvä (kts. esimerkki 34). Muuten oletetaan, että on olemassa surjektio $f\colon Y \to X$ ja osoitetaan, että on olemassa injektio $g\colon X \to Y$.
Koska f on surjektio, määritelmän mukaan jokaisella $x \in X$ on olemassa ainakin yksi $y_x \in Y$ jolle $f(y_x) = x$. Kuitenkin tällainen y_x ei ole välttämättä yksikäsitteinen, joten me joudumme **valitsemaan** *jokaisella $x \in X$ tasan yhden y_x jolle $f(y_x) = x$. Tähän tarvitaan valinta-aksiooma. Täsmällisesti siis kyse on siitä, että jokaisella $x \in X$ joukon Y osajoukko*

$$A_x = \{y \in Y \mid f(y) = x\}$$

(niin sanottu x:n alkukuva*) on epätyhjä. Valinta-aksiooman mukaan karteesinen tulo $\prod_{x \in X} A_x$ on epätyhjä, joten on olemassa perhe $(y_x)_{x \in X}$, missä $f(y_x) = x$ jokaisella $x \in X$. Tämä perhe määrittelee funktion $g\colon X \to Y$,*

kaavalla $g(x) = y_x$. *Osoitetaan, että tämä funktio on injektio. Olkoot* $x, x' \in X$ *sellaiset, että* $g(x) = g(x')$. *Tällöin siis* $y_x = y = y_{x'}$. *Soveltamalla tähän kuvausta* f *saadaan*

$$x = f(y_x) = f(y_{x'}) = x'.$$

Näin ollen g *on injektio. Koska on olemassa injektio* $X \to Y$, *pätee* $|X| \leq |Y|$.
Toisen suunnan todistamisessa ei tarvita valinta-aksioomaa, joten se jätetään harjoitustehtäväksi.

Nyt kun joukko-opin aksioomat on esitetty, seuraava luonnollinen kysymys on onko tällaista joukkojen maailmaa, joka toteuttaisi niitä ZFC-aksioomia olemassa ja onko se yksikäsitteinen. Yllättävä, ja ehkä hieman masentava, tosiasia on siinä, että sitä ei tiedetä. Ei tiedetä onko ZFC ristiriidaton, vai onko olemassa joku väite, jonka pystyy osoittamaan sekä todeksi että epätodeksi ZFC:n aksioomista (vähän niin kuin Russelin paradoksissa käy, jos oletamme kaikkien joukkojen joukkoa olemassa). Toistaiseksi ei pystytty löytämään sellaista ristiriita eikä mikään viittaa siihen, että sellainen löytyisi. Vielä yksi huono uutinen on siinä, että vaikka ZFC olisikin ristiriidaton, emme voi sitä koskaan tiedä. Tämä seuraa kuuluisasta *Gödelin epätäydellisyyslauseesta*, joka sanoo, että ristiriidattoman teorian ristiriidattomuutta ei pysty osoittamaan pysymällä teorian sisällä [8]. Ristiriidattomuus voi siis periaatteessa osoittaa todeksi jossakin ”isommassa teoriassa”, joka sisältäisi joukko-opin, mutta tällöin tätä ulkopuolista teoriaa koskisi sama ongelma. Seurauksena tästä on se, että emme pysty kehittämään konkreettista mallia joukko-opille emmekä tiedä onko sellainen ”olemassa”. Tästä seuraa, ett nykymatematiikkaa ikään kuin perustetaan myös oletukselle, että joukko-opille on olemassa malli.

Myös yksikäsitteisyys ei päde. Voidaan näyttää, että jos joukko-opin teorialla on ainakin yksi malli, niin niitä on paljon erilaisia. Suurin osa tutusta matematiikasta näyttää kaikissa malleissa samanlaisella, mutta on myös asioita jotka pätevät toisissa mutta ei toisissa. Kanoninen esimerkki tästä on *Kontinuumihypoteesi*, joka sanoo, että luonnollisten lukujen ja reaalilukujen mahtavuuksien välillä ei ole muita mahtavuuksia. Osoittautuu, että jos joukko-opin universumeja ylipäätän on, niin niiden joukossa on sekä sellaisia joissa Kontinuumihypoteesi pätee, että myös sellaisia, joissa se ei päde.

Tämän kurssin tavoite voidaan täsmällisesti muotoilla seuraavasti. Olkoon M jokin ”joukko-opillinen universumi”, jossa kaikki ZFC:n aksioomat

[8] Tarkemmin sanottuna tämä pätee tietyillä oletuksilla, jotka ZFC toteuttaa.

ovat voimassa. Tällöin tämä universumi sisältää reaalilukujen systeemin, eli sellaisen systeemin $(\mathbb{R}, +, \cdot, \leq)$, joka toteuttaa määritelmän 1. Lisäksi, kaikki tämän universumin reaalilukusysteemit ovat isomorfisia keskenään. Saman universumin sisällä reaalilukujen muodostama järjestelmä on isomorfinen. Erilaisten universumien reaaliluvut voivat kuitenkin toteuttaa erilaisia ominaisuuksia (esimerkiksi toisessa kontinuumihypoteesi voimassa ja toisessa ei).

Jatkossa emme joukko-opin aksioomista välitä sen erityisemmin ja käytännön tasolla esityksemme ja todistukset pysyvät ”naiivina”. Ainoat aksioomat joita varsinaisesti tulemme käyttämään eksplisiittisesti on valinta-aksiooma ja äärettömyysaksiooma. Toki aksioomien käytöstä on myös kyse aina kun esimerkiksi muodostetaan osajoukko ja funktio.