Lauri Hella

Joukko-oppi

Luentomoniste, Syksy 2011

Tampereen yliopisto
Informaatiotieteiden yksikkö
Matematiikka

Luku 1

Naiivia joukko-oppia

Tällä kurssilla perehdytään *aksiomaattiseen joukko-oppiin*, jossa joukon käsitteeseen liittyvä intuitio pyritään kuvailemaan aksioomien avulla. Joukkoja koskevat väitteet todistetaan näistä aksioomeista samaan tapaan kuin muillakin matematiikan aloilla.

Toisaalta matematiikan joukko-opillisissa tarkasteluissa tullaan yleensä toimeen niin sanotulla *naiivilla joukko-opilla*, jossa lähtökohtana on joukko-opin varsinaisen aksioomajärjestelmän sijasta joukkojen perusominaisuus *ekstensionaalisuus*, joukkojen perusoperaatiot, sekä yleinen joukkojen muodostusperiaate *joukkoabstraktio*. Kertaamme aluksi näihin liittyvät merkintätavat, ja valaisemme kahdella esimerkillä joukkoabstraktioon liittyviä ongelmia.

Joukko on kokoelma olioita (alkiot), joka muodostaa kokonaisuuden. Jos t on joukon A alkio (eli t kuuluu joukkoon A), merkitsemme

$$t \in A.$$

Vastaavasti, jos t ei ole A:n alkio, merkitsemme $t \notin A$.

Esimerkki 1.1 Olkoon A niiden alkulukujen jouko, jotka ovat pienempiä kuin 10. Siis $A = \{2, 3, 5, 7\}$.

Olkoon B yhtälön $x^4 - 17x^3 + 101x^2 - 247x + 210 = 0$ ratkaisujen joukko. Voidaan todeta, että $B = \{2, 3, 5, 7\}$.

Siis joukoilla A ja B on samat alkiot, joten ne ovat sama joukko: $A = B$.

Ekstensionaalisuusperiaate (EP): Kaksi joukkoa ovat samat, jos niillä on samat alkiot. Toisaalta, jos A ja B ovat sama olio, niin logiikan periaatteiden mukaan niillä on on oltava samat ominaisuudet; erityisesti niillä on samat alkiot. Siis ekstensionaalisuusperiaate voidaan muotoilla seuraavasti

$$A = B \quad \text{joss} \quad (\text{kaikilla } x \text{ pätee: } x \in A \Leftrightarrow x \in B).$$

Tämä voidaan kirjoittaa myös predikaattilogiikan kaavana

$$A = B \ \leftrightarrow \ \forall x \, (x \in A \leftrightarrow x \in B).$$

Tyhjä joukko $\emptyset$:

$$A = \emptyset \quad \text{joss} \quad \forall x\,(x \notin A).$$

Ekstensionaalisuusperiaatteen nojalla $\emptyset$ on yksikäsitteinen.

Järjestämätön pari: Jos x ja y ovat alkioita, niin $\{x, y\}$ on joukko. Ekstensionaalisuusperiaatteesta seuraa, että $\{x, y\} = \{y, x\}$, ja $\{x, x\} = \{x\}$.

Edelleen, jos x, y ja z ovat alkioita, voidaan muodostaa joukko $\{x, y, z\}$, ja yleisemmin, alkioista $x_1, \ldots, x_n$ voidaan muodostaa joukko $\{x_1, \ldots, x_n\}$.

Esimerkki 1.2 $\{\emptyset\} \neq \emptyset$, sillä joukossa $\{\emptyset\}$ on yksi alkio, nimittäin $\emptyset$, mutta joukossa $\emptyset$ ei ole yhtään alkiota. Samoin $\{\{\emptyset\}\} \neq \{\emptyset\}$: molemmissa joukoissa on yksi alkio, mutta alkiot eivät ole samat.

Yhdiste ja leikkaus: Jos A ja B ovat joukkoja, niin

- $A \cup B$ on niiden alkioiden joukko, jotka kuuluvat A:han *tai* B:hen
- $A \cap B$ on niiden alkioiden joukko, jotka kuuluvat A:han *ja* B:hen.

Osajoukot: Joukko A on joukon B osajoukko, $A \subseteq B$, jos jokainen A:n alkio on myös B:n alkio. Siis

$$A \subseteq B \;\text{ joss }\; \forall x\,(x \in A \to x \in B).$$

Erityisesti $\emptyset \subseteq B$ jokaisella joukolla B.

Varoitus: Älkää sekoittako väitteitä $A \in B$ ja $A \subseteq B$ toisiinsa!

Esimerkki 1.3 $\emptyset \subseteq \emptyset$, mutta $\emptyset \notin \emptyset$. $\{\emptyset\} \in \{\{\emptyset\}\}$, mutta $\{\emptyset\} \not\subseteq \{\{\emptyset\}\}$.

Potenssijoukko: $\mathcal{P}(A)$ on joukon A osajoukkojen joukko:

$$\mathcal{P}(A) = \{\, x \mid x \subseteq A \,\}$$

Esimerkki 1.4 $\mathcal{P}(\emptyset) = \{\emptyset\},\ \mathcal{P}(\{\emptyset\}) = \big\{\emptyset, \{\emptyset\}\big\},\ \mathcal{P}(\{0,1\}) = \big\{\emptyset, \{0\}, \{1\}, \{0,1\}\big\}$.

Jos joukossa A on n alkiota, niin joukossa $\mathcal{P}(A)$ on 2^n alkiota.

Joukkoabstraktio: Jos $p(x)$ on predikaatti, niin voidaan muodostaa niiden alkioiden joukko, joilla $p(x)$ on tosi:

$$\{\, x \mid p(x) \,\}.$$

Tosin predikaatille $p(x)$ on asetettava tiettyjä rajoituksia, sillä muuten joukon $\{\, x \mid p(x) \,\}$ olemassaolo voi johtaa paradokseihin, kuten kohta nähdään.

Esimerkki 1.5

$$\begin{aligned}
&\mathcal{P}(A) = \{\, x \mid x \text{ on } A\text{:n osajoukko} \,\}, \\
&A \cap B = \{\, x \mid x \in A \text{ ja } x \in B \,\}, \\
&A \cup B = \{\, x \mid x \in A \text{ tai } x \in B \,\}, \\
&\{\, z \mid z \neq z \,\} = \emptyset, \\
&\{\, n \mid n \text{ on parillinen alkuluku} \,\} = \{2\}.
\end{aligned}$$

Berryn paradoksi: Olkoon $p(x)$ predikaatti

> "x on luonnollinen luku, joka voidaan määritellä lauseella, jossa on korkeintaan 1000 merkkiä."

Oletetaan, että predikaatti $p(x)$ määrittelee joukon: $A = \{\, x \mid p(x) \,\}$.

Selvästi joukko A on äärellinen, koska alle 1000:n merkin pituisia lauseita on vain äärellinen määrä. Siis on olemassa pienin sellainen luonnollinen luku y, joka ei kuulu joukkoon A. Nyt lause

> "y on pienin luonnollinen luku, jota ei voi määritellä lauseella, jossa on korkeintaan 1000 merkkiä."

määrittelee luvun y, ja selvästi tässä lauseessa on vähemmän kuin 1000 merkkiä. Siis A:n määritelmän perusteella $y \in A$, vaikka y valittiin joukon A ulkopuolelta!

Berryn paradoksiin johtaa se, että siinä oleva predikaatti $p(x)$ käyttää vapaasti käsitettä "olla määriteltävissä". Paradoksi voidaan välttää rajoittamalla kieltä, jossa predikaatin saa muotoilla. Matematiikassa luonteva rajoitus on, että $p(x)$ on predikaattilogiikan kaava.

Tämäkään rajoitus ei riitä paradoksien välttämiseen:

Russellin paradoksi: Olkoon $p(x)$ predikaattilogiikan kaava $x \notin x$ ja olkoon R sitä vastaava joukko: $R = \{\, x \mid p(x) \,\}$.

Tarkastellaan kysymystä, onko R itsensä alkio. Jos $R \in R$, niin $p(R)$ on tosi, eli $R \notin R$, mikä on mahdotonta. Siis on oltava $R \notin R$. Mutta tällöin $p(R)$ on tosi, joten $R \in R$!

Koska ei ole mahdollista ristiriidattomasti päättää, onko $R \in R$ vai $R \notin R$, koko joukkoa R ei voida hyväksyä.

Russelin (ja muista samantapaisista) paradoksista päästään eroon korvaamalla yleinen joukkoabstraktio erotteluperiaatteella, joka sallii vain osajoukkojen muodostamisen predikaattilogiikan kaavojen avulla:

Erotteluperiaate: Jos A on joukko ja $p(x)$ on kaava, niin $\{\, x \in A \mid p(x) \,\}$ on joukko.

Toisaalta kaikki muotoa $\{\, x \mid p(x) \,\}$ olevat joukkojen kokoelmat ovat sinänsä mielekkäitä (kun $p(x)$ on predikaattilogiikan kaava), ja niitä on tapana kutsua *luokiksi* (class). Jotkut niistä ovat vain "liian suuria" ollakseen joukkoja, eli ne eivät ole minkään joukon alkioita. Tällaisia luokkia sanotaan *aidoiksi luokiksi* (proper class).

Hahmottelemme seuraavaksi intuitiivisen kuvan kaikkien joukkojen muodostamasta (aidosta) luokasta $V = \{\, x \mid x = x \,\}$.

Kumulatiivinen hierarkia: Joukot "muodostetaan" käyttämällä potenssijoukko-operaatiota lähtemällä liikkeelle jostakin annetusta "atomien" joukosta A. Muodostetaan nouseva ketju

$$V_0 \subseteq V_1 \subseteq V_2 \subseteq V_3 \subseteq \cdots$$

joukkoja seuraavasti:

$$\begin{aligned}
V_0 &= A \\
V_1 &= V_0 \cup \mathcal{P}(V_0) = A \cup \mathcal{P}(A) \\
V_2 &= V_1 \cup \mathcal{P}(V_1) \\
&\vdots \\
V_{n+1} &= V_n \cup \mathcal{P}(V_n) \\
&\vdots
\end{aligned}$$

Ideana on, että tämä ketju ei "pääty koskaan": kun V_n on määritelty kaikilla luonnollisilla luvuilla n, asetetaan $V_\omega = \bigcup_{n\in\omega} V_n$, missä ω on luonnollisten lukujen joukko $\{0, 1, 2, \dots\}$. Tämän jälkeen asetetaan $V_{\omega+1} = V_\omega \cup \mathcal{P}(V_\omega)$, jne.

Yleisemmin: kun vaiheessa α on muodostettu joukko V_α, niin seuraavassa vaiheessa $\alpha + 1$ asetetaan $V_{\alpha+1} = V_\alpha \cup \mathcal{P}(V_\alpha)$. Ja aina kun γ on kokoelma vaiheita, jossa ei ole viimeistä vaihetta, ja jolla V_α on muodostettu kaikilla vaiheilla α, jotka kuuluvat vaiheeseen γ, määritellään $V_\gamma = \bigcup_{\alpha\in\gamma} V_\alpha$.

Tässä konstruktion vaiheet (α ja γ) ovat *ordinaaleja*, joihin tutustutaan myöhemmin kurssilla.

Kaikki joukot kuuluvat näin muodostettuun kumulatiiviseen hierarkiaan. Täsmällisemmin sanottuna: olio a on joukko jos ja vain jos on olemassa vaihe α, jolla $a \in V_\alpha$.

Esimerkki 1.6 Olkoot a ja b joukkoja. Siis $a \in V_\alpha$ jollain α ja $b \in V_\beta$ jollain β. Voidaan olettaa, että β on myöhempi vaihe kuin α. Tällöin $V_\alpha \subseteq V_\beta$, joten $a \in V_\beta$. Tällöin $\{a, b\} \in \mathcal{P}(V_\beta)$ ja siis $\{a, b\} \in V_{\beta+1}$.

Vastaavasti nähdään, että jos $a_1, \ldots, a_n$ ovat joukkoja, niin on olemassa vaihe α, jolla $a_1, \ldots, a_n \in V_\alpha$, jolloin $\{a_1, \ldots, a_n\} \in V_{\alpha+1}$.

Kuten aikaisemmin sanoimme jokainen kokoelma C joukkoja on luokka. Luokka C on aito, jos se on liian suuri joukoksi siinä mielessä, että se ulottuu läpi koko kumulatiivisen hierarkian: jokaisella vaiheella α on olemassa C:n alkio a, jolla $a \notin V_\alpha$ (eli a on muodostettu vasta jossakin α:aa myöhäisemmässä vaiheessa).

Atomien joukko A voidaan valita tilanteen mukaan. Esimerkiksi analyysin yhteydessä se voisi olla reaalilukujen tai kompleksilukujen joukko, muodollisten kielten tutkimuksessa aakkosto (perusmerkkien joukko), jne. Matematiikkaa tarkasteltaessa atomien joukkoa ei kuitenkaan tarvita, sillä reaaliluvut ja kaikki muutkin matematiikassa tutkittavat oliot voidaan määritellä puhtaina joukkoina. Siksi voimme lähteä oletuksesta $A = \emptyset$. Määrittelemme siis

$$\begin{aligned}
V_0 &= \emptyset, \\
V_1 &= V_0 \cup \mathcal{P}(V_0), \\
V_2 &= V_1 \cup \mathcal{P}(V_1), \\
V_{n+1} &= V_n \cup \mathcal{P}(V_n), \\
V_\omega &= \bigcup_{n \in \omega} V_n, \\
V_{\alpha+1} &= V_\alpha \cup \mathcal{P}(V_\alpha), \text{ ja} \\
V_\gamma &= \bigcup_{\alpha \in \gamma} V_\alpha,
\end{aligned}$$

kun γ on kokoelma vaiheita, jossa ei ole viimeistä vaihetta.

Myöhemmin toteamme, että joukot V_α ovat *transitiivisia*: jokainen V_α:n alkio on myös V_α:n osajoukko. Siis $V_\alpha \subseteq \mathcal{P}(V_\alpha)$, joten joukon $V_{\alpha+1}$ määritelmä voidaan yksinkertaistaa muotoon $V_{\alpha+1} = \mathcal{P}(V_\alpha)$.

Kaikkien joukkojen luokka V on luonnollisesti aito luokka: $V_{\alpha+1} \in V$, ja intuitiivisesti on selvää, että $V_{\alpha+1} \notin V_\alpha$, joten V ei sisälly mihinkään kumulatiivisen hierarkian tasoon V_α. Huomaa myös, että jos V olisi joukko, niin soveltamalla siihen erotteluperiaatetta kaavalla $x \notin x$ saataisiin muodostettua osajoukko $\{\, x \in V \mid x \notin x \,\}$, ja päädyttäisiin Russellin paradoksiin.

Aksiomaattinen menetelmä

Joukko-opin aksiomatisoinnissa lähdetään liikeelle kahdesta primitiivisestä käsiteestä, jotka ovat

joukko, ja

alkiorelaatio $\in$.

Näihin käsitteisiin liittyvä intuitio pyritään ilmaisemaan muotoilemalla sopivia aksioomeja. Aksioomat ovat predikaattilogiikan lauseita, ja niistä päätellään edelleen *loogisia seurauksia*: aksioomien looginen seuraus on predikaattilogiikan lause φ, joka on tosi kaikissa primitiivisten käsitteiden tulkinnoissa, joissa aksioomat ovat tosia.

Joukko-opissa predikaattilogiikan atomikaavoja ovat kaikki muotoa $x \in y$ ja $x = y$ olevat kaavat. Muut kaavat muodostetaan näistä tuttuun tapaan käyttämällä konnektiiveja

$\neg$	ei
$\wedge$	ja
$\vee$	tai
$\rightarrow$	jos ... niin
$\leftrightarrow$	jos ja vain jos (joss)

sekä kvanttoreita

$\forall x$	jokaisella x
$\exists x$	on olemassa x.

Muuttujina voidaan x:n ja y:n ohella vapaasti käyttää muitakin isoja ja pieniä kirjaimia (toisinaan myös alaindeksien kanssa).

Joukko-opin tulkinta, eli *malli*, muodostuu epätyhjästä kokoelmasta U olioita, sekä kokoelmasta E järjestettyjä pareja (u, v), joiden komponentit kuuluvat kokoelmaan U. Kokoelman U alkiot ovat mallin joukkoja, ja joukko u tulkitaan joukon v alkioksi, jos $(u, v) \in E$. Tässä U ja E voivat olla aitoja luokkia; esimerkiksi edelläkuvattu kumulatiivinen hierarkia määrää mallin, jossa $U = V$ ja $E = \{\, (a, b) \mid a \in b \,\}$.

Toisaalta U voi myös olla joukko, jolloin E on (kaksipaikkainen) relaatio joukossa U, eli $E \subseteq U^2$. Tällöin järjestetty pari (U, E) on *suunnattu graafi*. Kääntäen, mitä hyvänsä sunnattua graafia (U, E) voi käyttää joukko-opin tulkintana; tosin graafiteoriassa tutkimuskohteena olevat graafit eivät yleensä toteuta mitään joukko-opin aksioomeja.

Esimerkki 1.7 Otetaan aksioomaksi EP (ekstensionaalisuusperiaate): $\forall A \forall B \big(A = B \leftrightarrow \forall x(x \in A \leftrightarrow x \in B)\big)$.

(1) Olkoon φ lause "Ei ole olemassa kahta eri joukkoa, joilla ei ole yhtään alkiota".

$$\varphi := \neg \exists A \exists B \big(A \neq B \wedge \forall x(x \notin A) \wedge \forall x(x \notin B)\big).$$

Selvästi φ on EP:n looginen seuraus.

(2) Sen sijaan lause "On olemassa joukot a ja b s.e. $a \in b$"

$$\psi = \exists x \exists y (x \in y),$$

ei ole EP:n looginen seuraus. Nimittäin, jos tarkastellaan mallia (U, E), missä $U = \{a\}$ ja $E = \emptyset$, niin EP on tosi, mutta ψ ei ole tosi, sillä mallin ainoa joukko a ei ole minkään joukon alkio. (Mallin (U, E) mielessä $a = \emptyset$, ja muita joukkoja ei ole.)

(3) Olkoon θ "yksiöaksiooma": $\forall x \exists A \forall y (y \in A \leftrightarrow y = x)$. Nyt lause ψ on θ:n looginen seuraus, sillä jokaisessa mallissa (U, E) on ainakin yksi joukko $a \in U$, ja yksiöaksioomasta seuraa, että on myös olemassa joukko $b \in U$, jolla $(a, b) \in E$. (Lisäksi a on ainoa joukko, joka kuuluu joukkoon b, eli mallin (U, E) mielessä $b = \{a\}$).

Luku 2

Aksioomat ja joukkojen laskutoimitukset

Tässä luvussa esittelemme osan joukko-opin aksioomeista, sekä katsomme miten ne liittyvät tuttuihin joukko-opin laskutoimituksiin.

Muotoilemme ensimmäiseksi aksioomaksi ekstensionaalisuusperiaatteen:

Ekstensionaalisuusaksiooma

$$\forall A \forall B \big(\forall x (x \in A \leftrightarrow x \in B) \rightarrow A = B \big).$$

Huom. Ekstensionaalisuusaksiooma on muotoiltu hieman eri tavalla kuin ekstensionaalisuusperiaate Esimerkissä 1.7. Muotoilut ovat kuitenkin keskenään ekvivalentit, sillä käänteinen implikaatio $A = B \rightarrow \forall x((x \in A \leftrightarrow x \in B))$ on loogisesti pätevä.

Toiseksi tarvitsemme aksiooman, joka takaa että tyhjä joukko on olemassa:

Tyhjän joukon aksiooma

$$\exists B \forall x (x \notin B).$$

Kolmas aksiooma tekee mahdolliseksi muodostaa kahden joukon järjestämättömiä pareja:

Pariaksiooma

$$\forall u \forall v \exists B \forall x \big(x \in B \leftrightarrow (x = u \vee x = v) \big).$$

Muotoilemme seuraavaksi väliaikaisen aksiooman, jonka mukaan kaikilla joukoilla x ja y on olemassa yhdiste $x \cup y$. Korvaamme tämän myöhemmin vahvemmalla yhdisteaksioomalla.

Yhdisteaksiooma (heikko versio)

$$\forall a \forall b \exists B \forall x \big(x \in B \leftrightarrow (x \in a \vee x \in b)\big).$$

Tarvitsemme myös aksiooman, joka sanoo, että kaikilla joukoilla on potenssijoukko:

Potenssijoukkoaksiooma

$$\forall a \exists B \forall x (x \in B \leftrightarrow x \subseteq a).$$

Huom. Tässä $x \subseteq a$ on lyhennysmerkintä kaavalle $\forall y(y \in x \to y \in a)$.

Esittelemme myöhemmin vielä lisää aksioomeja (erotteluaksioomat, valinta-aksiooma, äärettömyysaksiooma, korvausaksioomat ja säännöllisyysaksiooma).

Käytämme tavalliseen tapaan seuraavia lyhennysmerkintöjä joukoille, joiden olemassaolo seuraa edelläolevista aksioomista:

- tyhjä joukko $\emptyset$ on se yksikäsitteinen joukko B, jolla pätee $\forall x(x \notin B)$
- joukon a potenssijoukko $\mathcal{P}(a)$ on se yksikäsitteinen joukko B jolla pätee $\forall x(x \in B \leftrightarrow x \subseteq a)$
- (järjestämätön) pari $\{u, v\}$ on se yksikäsitteinen joukko B, jolla pätee $\forall x\big(x \in B \leftrightarrow (x = u \vee x = v)\big)$
- (kahden joukon) yhdiste $x \cup y$ on se yksikäsitteinen joukko B, jolla pätee $\forall z\big(z \in B \leftrightarrow (z \in x \vee z \in y)\big)$
- yksiö $\{x\}$ on joukko $\{x, x\}$
- kun n:n alkion joukko $\{x_1, \dots, x_n\}$ on määritelty, niin $n+1$:n alkion joukko määritellään asettamalla $\{x_1, \dots, x_{n+1}\} = \{x_1, \dots, x_n\} \cup \{x_{n+1}\}$.

Nämä ovat lyhennysmerkintöjä, joita voi vapaasti käyttää joukko-opin kaavoissa.

Esimerkki 2.1 Tarkastellaan joukko-opin tulkintaa (U, E), missä $U = \omega$, ja E on ω:n tavallinen järjestys: $(n, m) \in E$ joss $n < m$. Toisin sanoen mallin (U, E) mukaan $n = \{0, \dots, n-1\}$ kullakin luonnollisella luvulla n; erityisesti $0 = \emptyset$.

On helppo nähdä, että ekstensionaalisuusaksiooma ja tyhjän joukon aksiooma ovat tosia mallissa (U, E). Samoin yhdisteaksiooman heikko versio on tosi: mallin (U, E) mielessä $m \cup n$ on pienempi luvuista m ja n.

Myös potenssijoukkoaksiooma on tosi: selvästi mallissa (U, E) pätee ekvivalenssi $k \subseteq n \iff k \leq n$, joten $n+1$ joukon n potenssijoukko mallin (U, E) mielessä.

Huomaa, että mallin (U, E) "ulkopuolelta katsottuna" $n+1$ ei tietenkään ole koko potenssijoukko $\mathcal{P}(n)$: siitä puuttuvat esimerkiksi joukon $n = \{0, \dots, n-1\}$ osajoukot $\{1\}, \dots, \{n-1\}$, kun $n \geq 2$.

Todetaan vielä lopuksi, että pariaksiooma ei ole tosi mallissa (U, V): koska 1 on mallin joukko, pariaksiooman perusteella mallissa pitäisi olla myös joukko $\{1, 1\} = \{1\}$, mutta kuten yllä todettiin, tämä joukko puuttuu. Olemme näin osoittaneet, että pariaksiooma ei ole muiden tässä esimerkissä mainittujen aksioomien looginen seuraus.

Yleiset yhdisteet ja leikkaukset

Diskreetin matematiikan kurssilla määritellään indeksöidyn joukkoperheen $\mathcal{B} = \{\, B_i \mid i \in I \,\}$ yhdiste kaavalla

$$\bigcup_{i \in I} B_i = \{\, x \mid \exists i(i \in I \wedge x \in B_i) \,\}.$$

Tällä kurssilla tätä joukkoa merkitään $\bigcup \mathcal{B}$, ja sitä sanotaan $\mathcal{B}$:n yhdisteeksi. Itse asiassa yhdiste määritellään mille hyvänsä joukolle A asettamalla:

$$\bigcup A = \{\, x \mid \exists y(y \in A \wedge x \in y) \,\}.$$

Samaan tapaan voimme määritellä, jokaiselle epätyhjälle joukolle A leikkauksen:

$$\bigcap A = \{\, x \mid \forall y(y \in A \rightarrow x \in y) \,\}.$$

Jos $A = \emptyset$, tämä määritelmä ei käy, sillä $\bigcap A$ olisi tällöin kaikkien joukkojen luokka. Jätämme siis tyhjän joukon leikkauksen $\bigcap \emptyset$ määrittelemättä. (Voisimme välttää ongelman myös sopimalla, että $\bigcap \emptyset = \emptyset$.)

Yleisen yhdisteen olemassaoloa ei voi todistaa aikaisemmista joukko-opin aksioomista. Siksi otamme käyttöön uuden aksiooman, joka samalla korvaa edelläesitetyn yhdisteaksiooman heikon version:

Yhdisteaksiooma

$$\forall A \exists B \forall x \big(x \in B \leftrightarrow \exists y \in A(x \in y)\big)$$

Tässä $\exists y \in A\, \varphi$ on logiikassa käytetty lyhennysmerkintä kaavalle $\exists y(y \in A \wedge \varphi)$. Vastaavasti $\forall y \in A\, \varphi$ tarkoittaa kaavaa $\forall y(y \in A \rightarrow \varphi)$.

Esimerkki 2.2

$$\bigcup\{\{2,4,6\},\{6,16,26\},\{0\}\} = \{2,4,6,6,16,26,0\} = \{0,2,4,6,16,26\},$$
$$\bigcup\Big\{\{\{\emptyset\},\{\emptyset,\{\emptyset\}\}\},\{\{\{\emptyset\},\emptyset\}\},\{\emptyset\}\Big\} = \Big\{\{\emptyset\},\{\emptyset,\{\emptyset\}\},\emptyset\Big\}.$$

Entä tarvitaanko (yleisten) leikkausten olemassaoloa varten oma aksioomansa? Vastaus on, että varsinaista leikkausaksioomaa ei tarvita, mutta sen sijaan tarvitsemme kyllä aksioomia, jotka takaavat tiettyjen osajoukkojen olemassaolon. Muotoilemme siis erotteluperiaatetta vastaavat aksioomat:

Erotteluaksioomat (osajoukkoaksioomat) Jos $\varphi(x,t_1,\dots,t_n)$ on joukko-opin kaava, niin siihen liittyy aksiooma

$$\forall t_1 \dots \forall t_n \forall c \exists B \forall x\big(x \in B \leftrightarrow x \in c \land \varphi(x,t_1,\dots,t_n)\big).$$

Joukkoa B merkitään $\{\, x \in c \mid \varphi(x,t_1,\dots,t_n) \,\}$. Joukot $t_1,\dots,t_n$ ovat tässä parametreja, joiden valinnasta joukko B riippuu; kaavassa φ ei välttämättä tarvitse olla yhtään parametria.

Esimerkki 2.3 Kahden joukon leikkaus $a \cap b = \{\, x \in b \mid x \in a \,\}$ on olemassa erotteluaksiooman

$$\forall a \forall b \exists B \forall x (x \in B \leftrightarrow x \in b \land x \in a)$$

perusteella. Tässä kaavaksi on otettu $\varphi(x,a) = x \in a$; a on siis parametri.

Kahden joukon erotus $a \setminus b = \{\, x \in a \mid x \notin b \,\}$ saadaan puolestaan erotteluaksioomalla

$$\forall b \forall a \exists B \forall x (x \in B \leftrightarrow x \in a \land x \notin b).$$

Todistamme kohta erotteluaksiooman avulla yleisten leikkausten olemassaolon. Sitä ennen annamme vielä muutamia esimerkkejä.

Esimerkki 2.4 Olkoon ω luonnollisten lukujen joukko $\{0,1,2,\dots\}$. Sopivilla erotteluaksioomilla saadaan mm. seuraavat ω:n osajoukot:

$$\{\, x \in \omega \mid \text{“}x \text{ on parillinen”} \,\}$$
$$\{\, x \in \omega \mid \text{“}x \text{ on alkuluku”} \,\}$$
$$\{\, x \in \omega \mid \text{“}x \text{ on 2:n potenssi”} \,\}$$

Luonnollisesti näiden joukkojen määritelmissä ehdot “x on...” pitää ilmaista joukko-opin kaavoilla. Tämä on mahdollista, kun ensin määritellään luonnollisten lukujen joukko, ja luonnollisten lukujen laskutoimitukset joukko-opissa (tämä tehdään Luvussa 4).

Esimerkki 2.5 Joukko $\{ x \in \mathcal{P}(a) \mid \text{“}x \text{ on } a\text{:n yhden alkion osajoukko”} \}$ saadaan erotteluaksioomalla joukosta $\mathcal{P}(a)$ käyttämällä kaavaa

$$\exists y \big(y \in x \wedge \forall z (z \in x \to z = y) \big).$$

Erotteluaksiooman avulla voidaan todistaa joukkojen olemassaolo, mutta siitä seuraa myös, että ei ole olemassa kaikkien joukkojen joukkoa:

Lause 2.1 *Ei ole olemassa joukkoa, jonka alkioita kaikki joukot ovat.*

Todistus. Olkoon A joukko. Osoitetaan, että kaikki joukot eivät ole A:n alkioita. Erotteluaksioomalla saadaan A:lle osajoukko $B = \{ x \in A \mid x \notin x \}$.

Väitämme, että $B \notin A$.

Tehdään vastaoletus: $B \in A$. Tällöin B:n määritelmän perusteella pätee $B \in B$ joss $(B \in A \wedge B \notin B)$. Koska vastaoletuksen perusteella $(B \in A \wedge B \notin B)$ joss $B \notin B$, päädymme ristiriitaan: $B \in B$ joss $B \notin B$.

Siis vastaoletus on väärä, eli $B \notin A$ □

Huom: Myöhemmin kurssilla otetaan käyttöön säännöllisyysaksiooma, josta seuraa, että mikään joukko ei ole itsensä alkio. Siis joukko-opin tavallisessa ZFC aksiomatisoinnissa $x \notin x$ pätee kaikilla joukoilla x, joten ylläolevassa todistuksessa $B = A$.

On myös olemassa säännöllisyysaksiooman kanssa vaihtoehtoinen aksiooma (AFA, *Anti Foundation Axiom*), josta seuraa, että on olemassa joukkoja, jotka ovat itsensä alkioita.

Lause 2.2 *Jokaisella epätyhjällä joukolla A on olemassa leikkaus $\bigcap A$.*

Todistus. Olkoon $A \neq \emptyset$. Voimme siis valita alkion $c \in A$. Erotteluaksiooman avulla voidaan muodostaa joukko B, jolla pätee

$$\forall x \big(x \in B \leftrightarrow x \in c \wedge \forall y \in A (x \in y) \big).$$

Koska $c \in A$, pätee $\forall y \in A(x \in y) \to x \in c$, ja siis

$$x \in c \wedge \forall y \in A(x \in y) \leftrightarrow \forall y \in A(x \in y).$$

Näin ollen $B = \{ x \mid \forall y \in A(x \in y) \} = \bigcap A$. □

Jos $b \in A$, niin selvästi $b \subseteq \bigcup A$ ja $\bigcap A \subseteq b$. Edelleen on helppo nähdä, että jos $A \subseteq B$, niin $\bigcup A \subseteq \bigcup B$. Toisaalta $\bigcap B \subseteq \bigcap A$ aina kun $A \subseteq B$ ja $A \neq \emptyset$.

Esimerkki 2.6

$$\bigcap\big\{\{1,2,8\},\{2,8\},\{4,8\}\big\} = \{8\},$$
$$\bigcup\big\{\{1,2,8\},\{2,8\},\{4,8\}\big\} = \{1,2,8,2,8,4,8\} = \{1,2,4,8\}.$$

Esimerkki 2.7

$$\begin{aligned}
&\bigcap\{a\} = a,\\
&\bigcap\{a,b\} = a \cap b,\\
&\bigcap\big\{\{a\},\{a,b\}\big\} = \{a\} \cap \{a,b\} = \{a\},\\
&\bigcup\bigcap\big\{\{a\},\{a,b\}\big\} = \bigcup\{a\} = a.
\end{aligned}$$

Toisaalta

$$\bigcap\bigcup\big\{\{a\},\{a,b\}\big\} = \bigcap\{a,b\} = a \cap b.$$

Esimerkki 2.8 Jos $\{\{x\},\{x,y\}\} \in A$, niin $\{x,y\} \in \bigcup A$, joten $x \in \bigcup\bigcup A$ ja $y \in \bigcup\bigcup A$.

Joukkojen algebra

Joukkojen perusoperaatiot eli -laskutoimitukset ovat yhdiste, leikkaus ja erotus:

$$\begin{aligned}
A \cup B &= \{\, x \mid x \in A \vee x \in B \,\}\\
A \cap B &= \{\, x \mid x \in A \wedge x \in B \,\}\\
A \setminus B &= \{\, x \mid x \in A \wedge x \notin B \,\} \quad (B\text{:n komplementti } A\text{:n suhteen})
\end{aligned}$$

Joukkojen algebraksi voidaan kutsua kokonaisuutta $\langle \emptyset, \cup, \cap, \setminus, \subseteq \rangle$, jossa on mukana laskutoimitusten lisäksi yhdisteen neutraalialkio $\emptyset$, sekä osajoukkorelaatio $\subseteq$. Joukkojen algebra on analoginen esimerkiksi reaalilukujen (tai kokonaislukujen) laskutoimitusten ja järjestyksen muodostaman kokonaisuuden $\langle 0, +, \cdot, -, \leq \rangle$ kanssa.

Siksi on luonnollista kysyä, minkälaisia laskulakeja $\emptyset$, $\cup$, $\cap$, $\setminus$ ja $\subseteq$ noudattavat.

Vaihdannaisuus:

$$\begin{aligned}
A \cup B &= B \cup A \qquad \text{ja}\\
A \cap B &= B \cap A
\end{aligned}$$

Liitännäisyys:

$$A \cup (B \cup C) = (A \cup B) \cup C \qquad \text{ja}$$
$$A \cap (B \cap C) = (A \cap B) \cap C$$

Osittelulait:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \qquad \text{ja}$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

De Morganin lait:

$$C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B) \qquad \text{ja} \tag{2.1}$$
$$C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B) \tag{2.2}$$

Tyhjään joukkoon liittyviä sääntöjä:

$$A \cup \emptyset = A,$$
$$A \cap \emptyset = \emptyset,$$
$$A \cap (C \setminus A) = \emptyset.$$

Kaikki nämä laskusäännöt voidaan todistaa yksinkertaisilla päättelyillä. Käymme tässä esimerkin vuoksi läpi kolme erilaista todistusta De Morganin laille (2.1):

Tapauksiin jakaminen. Kullakin x pätee yksi seuraavista kahdeksasta vaihtoehdosta:

(1) $x \in A$, $x \in B$, $x \in C$
(2) $x \in A$, $x \in B$, $x \notin C$
(3) $x \in A$, $x \notin B$, $x \in C$
(4) $x \in A$, $x \notin B$, $x \notin C$
(5) $x \notin A$, $x \in B$, $x \in C$
(6) $x \notin A$, $x \in B$, $x \notin C$
(7) $x \notin A$, $x \notin B$, $x \in C$
(8) $x \notin A$, $x \notin B$, $x \notin C$

Osoitetaan kussakin tapauksista (1)–(8) erikseen, että

$$(*) \qquad x \in C \setminus (A \cup B) \iff x \in (C \setminus A) \cap (C \setminus B):$$

(1) Oletetaan, että $x \in A \wedge x \in B \wedge x \in C$. Tällöin $x \in A \cup B$, joten $x \notin C \setminus (A \cup B)$. Toisaalta $x \notin C \setminus A$, joten $x \notin (C \setminus A) \cap (C \setminus B)$. Siis ekvivalenssi $(*)$ on voimassa.

$\vdots$

(8) Oletetaan, että $x \notin A \wedge x \notin B \wedge x \notin C$. Koska $x \notin C$, on $x \notin C \setminus (A \cup B)$. Samoin $x \notin C \setminus A$, joten $x \notin (C \setminus A) \cap (C \setminus B)$. Siis $(*)$ pätee.

$\square$

Suoraviivainen todistus (luonnollinen päättely). Oletetaan ensin, että $x \in C \setminus (A \cup B)$. Siis $x \in C$ ja $x \notin A \cup B$, joten $x \notin A$ ja $x \notin B$. Siis ($x \in C$ ja $x \notin A$) ja ($x \in C$ ja $x \notin B$), joten $x \in C \setminus A$ ja $x \in C \setminus B$. Niinpä $x \in (C \setminus A) \cap (C \setminus B)$.

Oletetaan sitten, että $x \in (C \setminus A) \cap (C \setminus B)$. Siis $x \in C \setminus A$ ja $x \in C \setminus B$ eli $x \in C$ ja $x \notin A$ ja $x \notin B$. Tällöin $x \in C$ ja $x \notin A \cup B$, joten $x \in C \setminus (A \cup B)$. $\square$

Ekvivalenssiketju (laskuharjoitustyyli). Jokaisella x pätee:

$$
\begin{aligned}
& x \in C \setminus (A \cup B) \\
\Leftrightarrow\ & x \in C \wedge x \notin A \cup B \\
\Leftrightarrow\ & x \in C \wedge x \notin A \wedge x \notin B \\
\Leftrightarrow\ & (x \in C \wedge x \notin A) \wedge (x \in C \wedge x \notin B) \\
\Leftrightarrow\ & x \in C \setminus A \wedge x \in C \setminus B \\
\Leftrightarrow\ & x \in (C \setminus A) \cap (C \setminus B).
\end{aligned}
$$

$\square$

Osajoukkorelaatiolle ja laskutoimituksille ovat voimassa seuraavat säännöt:

Monotonisuusominaisuudet:

$$
\begin{aligned}
A \subseteq B &\Rightarrow A \cup C \subseteq B \cup C \\
A \subseteq B &\Rightarrow A \cap C \subseteq B \cap C \\
A \subseteq B &\Rightarrow \bigcup A \subseteq \bigcup B
\end{aligned}
$$

Antimonotonisuusominaisuudet:

$$
\begin{aligned}
A \subseteq B &\Rightarrow C \setminus B \subseteq C \setminus A \\
\emptyset \neq A \subseteq B &\Rightarrow \bigcap B \subseteq \bigcap A
\end{aligned}
$$

Yleistämme vielä lopuksi osittelulait ja De Morganin lait yleisille yhdisteille ja leikkauksille.

Yleistetyt osittelulait:

$$
\begin{aligned}
A \cup \bigcap \mathcal{B} &= \bigcap \{\, A \cup X \mid X \in \mathcal{B} \,\}, \qquad \mathcal{B} \neq \emptyset, \\
A \cap \bigcup \mathcal{B} &= \bigcup \{\, A \cap X \mid X \in \mathcal{B} \,\}.
\end{aligned}
$$

Huom: Joukko $\mathcal{C} = \{\, A \cup X \mid X \in \mathcal{B} \,\}$ on olemassa, sillä

$$A \cup X \in \mathcal{P}\Big(A \cup \bigcup \mathcal{B}\Big) \quad \text{kullakin } X \in \mathcal{B},$$

joten $\mathcal{C} = \{\, Y \in \mathcal{P}(A \cup \bigcup \mathcal{B}) \mid \exists X(X \in \mathcal{B} \wedge Y = A \cup X) \,\}$ saadaan erotteluaksioomalla.

Yleistetyt De Morganin lait:

$$\begin{aligned} C \setminus \bigcup \mathcal{A} &= \bigcap \{\, C \setminus X \mid X \in \mathcal{A} \,\} \qquad \text{ja} \\ C \setminus \bigcap \mathcal{A} &= \bigcup \{\, C \setminus X \mid X \in \mathcal{A} \,\}, \end{aligned}$$

kun $\mathcal{A} \neq \emptyset$.

Huom: Voidaan käyttää myös merkintätapoja

$$\bigcap \mathcal{A} = \bigcap_{X \in \mathcal{A}} X \qquad \text{ja} \qquad \bigcup \mathcal{A} = \bigcup_{X \in \mathcal{A}} X.$$

Esimerkki 2.9

$$\bigcap \{\, C \setminus X \mid X \in \mathcal{A} \,\} = \bigcap_{X \in \mathcal{A}} (C \setminus X)$$

Luku 3

Relaatiot ja funktiot

Järjestetyt parit

Järjestettyä paria (x, y) pidetään matematiikassa usein primitiivisenä käsitteenä: sitä ei määritellä muiden käsitteiden avulla, mutta sille asetetaan aksioomaksi

$$(x, y) = (u, v) \text{ joss } x = u \wedge y = v.$$

Joukko-opissa järjestetty pari on kuitenkin tarkoituksenmukaista määritellä tiettynä joukkona. Heti alkuun on syytä huomata, että järjestämätön pari $\{x, y\}$ ei kelpaa määritelmäksi, sillä $\{x, y\} = \{y, x\}$, vaikka olisikin $x \neq y$. Sen sijaan käytämme järjestetylle parille seuraavaa määritelmää:

Määritelmä 3.1 $\langle x, y\rangle = \big\{\{x\}, \{x, y\}\big\}$.

Huom: Käytämme siis järjestetylle parille merkintää $\langle x, y\rangle$, joka poikkeaa matematiikassa yleisesti käytetystä merkinnästä (x, y). Syynä tähän on se, että määrittelemme myöhemmin järjestetyt n-jonot $(x_1, \ldots, x_n)$ funktion käsitteen avulla, ja järjestetty 2-jono (x_1, x_2) *ei ole* sama joukko, kuin järjestetty pari $\langle x_1, x_2\rangle$.

Osoitamme seuraavaksi, että yllämääritelty järjestetty pari toteuttaa vaaditun aksiooman:

Lause 3.1 $\langle u, v\rangle = \langle x, y\rangle \Leftrightarrow u = x \wedge v = y$.

Todistus. Jos $u = x$ ja $v = y$, on selvää, että $\langle u, v\rangle = \langle x, y\rangle$. Oletetaan sitten, että $\langle u, v\rangle = \langle x, y\rangle$ eli $\{\{u\}, \{u, v\}\} = \{\{x\}, \{x, y\}\}$. Tällöin $\{u\} \in \{\{x\}, \{x, y\}\}$ ja $\{u, v\} \in \{\{x\}, \{x, y\}\}$. Siis joko (a) $\{u\} = \{x\}$ tai (b) $\{u\} = \{x, y\}$. Samoin joko (c) $\{u, v\} = \{x\}$ tai (d) $\{u, v\} = \{x, y\}$.

Oletetaan ensin, että (b) pätee. Tällöin $u = x = y$ ja (c) $\Leftrightarrow$ (d) $\Leftrightarrow$ $u = v = x$. Siis $u = x$ ja $v = y$ $(= x = u)$.

Jos taas (a) pätee, on $u = x$, jolloin (d):stä seuraa, että $y = u$ tai $y = v$. Ensimmäisessä tapauksessa (b) on voimassa ja väite $x = u$ ja $y = v$ seuraa kuten edellä. Jälkimmäisessä tapauksessa $u = x$ ja $v = y$.

Jos taas (c) pätee, edetään samalla tavalla kuin tapauksessa (b). $\square$

Olkoot A ja B ovat joukkoja. Joukkojen A ja B *karteesinen tulo* on

$$A \times B = \{ \langle x, y \rangle \mid x \in A \wedge y \in B \}.$$

Meidän on vielä perusteltava karteesisen tulon $A \times B$ olemassaolo joukko-opin aksioomilla.

Apulause 3.2 *Jos $x \in C$ ja $y \in C$, niin $\langle x, y \rangle \in \mathcal{P}(\mathcal{P}(C))$*

Todistus.

$$\begin{aligned} & x \in C \wedge y \in C \\ \Rightarrow\ & \{x\} \in \mathcal{P}(C) \wedge \{x, y\} \in \mathcal{P}(C) \\ \Rightarrow\ & \langle x, y \rangle = \big\{\{x\}, \{x, y\}\big\} \in \mathcal{P}(\mathcal{P}(C)). \end{aligned}$$

$\square$

Seuraus 3.3 *Kaikilla joukoilla A ja B on olemassa karteesinen tulo $A \times B$, eli joukko, joka sisältää täsmälleen alkiot $\langle x, y \rangle$, missä $x \in A$ ja $y \in B$.*

Todistus. Apulauseen 3.2 perusteella on olemassa joukko D, joka sisältää kaikki parit $\langle x, y \rangle$, missä $x \in A$, $y \in B$, nimittäin $D = \mathcal{P}(\mathcal{P}(A \cup B))$.

Erotteluaksioomalla tästä saadaan joukko

$$E = \{ w \in D \mid \exists x \exists y (x \in A \wedge y \in B \wedge w = \langle x, y \rangle) \}.$$

Selvästi $E = A \times B$. $\square$

Relaatiot

Tarkastellaan joukon $\{0, 1, 2, 3, 4\}$ tavallista järjestysrelaatiota $<$. Kuten Diskreetin matematiikan kurssilla esitetään, relaatiot voidaan havainnollistaa nuolikuvioilla, polkukuviolla, matriiseilla tai esittämällä ne koordinaatistossa. Järjestysrelaatiota voidaan myös havainnollistaa Hasse-diagrammeilla.

Joukko-opissa järjestys $<$ tulkitaan joukoksi järjestettyjä pareja:

$$< \ = \ \{\langle 0,1 \rangle, \langle 0,2 \rangle, \langle 0,3 \rangle, \langle 0,4 \rangle, \langle 1,2 \rangle, \langle 1,3 \rangle, \langle 1,4 \rangle, \langle 2,3 \rangle, \langle 2,4 \rangle, \langle 3,4 \rangle\}.$$

Sama tulkinta voidaan tehdä muillekin relaatioille, ja otammekin tämän tulkinnan relaation käsitteen määritelmäksi:

Määritelmä 3.2 Relaatio on joukko, jonka kaikki alkiot ovat järjestettyjä pareja. Siis joukko A on relaatio joss sillä pätee

$$\forall u \in A \exists x \exists y (u = \langle x, y \rangle).$$

Esimerkki 3.1 Olkoon $\omega = \{0, 1, 2, \dots\}$ (luonnollisten lukujen joukko).

Luonnollisten lukujen jaollisuusrelaatio on joukko

$$R = \{\, \langle m, n \rangle \in \omega \times \omega \mid \exists p \in \omega \, (m \cdot p = n) \,\}.$$

Luonnollisten lukujen identiteettirelaatio on joukko

$$I_\omega = \{\, \langle n, n \rangle \in \omega \times \omega \mid n \in \omega \,\}.$$

Määritelmä 3.3 Olkoon A joukko. A:n *määrittelyjoukko* $\mathrm{dom}(A)$ määritellään ehdolla

$$x \in \mathrm{dom}(A) \;\Leftrightarrow\; \exists y \, (\langle x, y \rangle \in A).$$

A:n *arvojoukko* $\mathrm{ran}(A)$ määritellään ehdolla

$$x \in \mathrm{ran}(A) \;\Leftrightarrow\; \exists y \, (\langle y, x \rangle \in A).$$

A:n *kenttä* $\mathrm{fld}(A)$ määritellään asettamalla

$$\mathrm{fld}(A) = \mathrm{dom}(A) \cup \mathrm{ran}(A).$$

Huom: Yleensä matematiikassa käytetään näitä käsitteitä vain kun A on relaatio (tai funktio). Tämä rajoitus ei ole mitenkään välttämätön; jos joukossa A on alkioita, jotka eivät ole järjestettyjä pareja, ne voidaan yksinkertaisesti jättää pois, kun määritetään $\mathrm{dom}(A), \mathrm{ran}(A)$ ja $\mathrm{fld}(A)$.

Perustelemme seuraavaksi joukkojen $\mathrm{dom}(A)$, $\mathrm{ran}(A)$ ja $\mathrm{fld}(A)$ olemassaolon. Tähän tarvitaan seuraava aputulos.

Apulause 3.4 *Jos $\langle x, y \rangle \in A$, niin $x, y \in \bigcup\bigcup A$.*

Todistus. Oletetaan, että $\{\{x\}, \{x, y\}\} \in A$. Tällöin $\{x, y\} \in \bigcup A$, mistä edelleen seuraa, että $x, y \in \bigcup\bigcup A$. □

Nyt $\mathrm{dom}(A)$ ja $\mathrm{ran}(A)$ saadaan joukosta $\bigcup\bigcup A$ erotteluaksioomalla:

$$\mathrm{dom}(A) = \{x \in \bigcup\bigcup A \mid \exists y \, (\langle x, y \rangle \in A)\},$$
$$\mathrm{ran}(A) = \{x \in \bigcup\bigcup A \mid \exists y \, (\langle y, x \rangle \in A)\}.$$

Joukon $\mathrm{fld}(A) = \mathrm{dom}(A) \cup \mathrm{ran}(A)$ olemassaolo seuraa puolestaan yhdisteaksioomasta.

Käytämme tästä lähtien usein tavallista merkintätapaa xRy joukko-opillisen merkinnän $\langle x, y \rangle \in R$ sijasta. Joskus voidaan käyttää myös ketjumerkintää $xRyRz$ lyhennysmerkintänä kaavalle $xRy \wedge yRz$.

Järjestetyt kolmikot

Järjestetyn parin käsitteen avulla voidaan helposti määritellä järjestetyn kolmikon käsite asettamalla

$$\langle x, y, z \rangle = \langle \langle x, y \rangle, z \rangle$$

Selvästi tällöin pätee $\langle x, y, z \rangle = \langle u, v, w \rangle \Leftrightarrow x = u \wedge y = v \wedge z = w$. Edelleen voimme määritellä järjestetyt nelikot (viisikot, kuusikot jne.) samalla idealla:

$$\langle x, y, z, u \rangle = \langle \langle \langle x, y \rangle, z \rangle, u \rangle.$$

Tässä kolmikon määritelmässä on kuitenkin se harmillinen piirre, että se ei ole symmetrinen kolmikon komponenttien suhteen: $\langle \langle x, y \rangle, z \rangle$ ei yleensä ole sama joukko kuin $\langle x, \langle y, z \rangle \rangle$. Erityisesti $(A \times B) \times C = A \times (B \times C)$ pätee vain poikkeusapauksissa, sillä edellinen joukko on $\{ \langle \langle x, y \rangle, z \rangle \mid x \in A \wedge y \in B \wedge z \in C \}$, ja jälkimmäinen on $\{ \langle x, \langle y, z \rangle \rangle \mid x \in A \wedge y \in B \wedge z \in C \}$.

Tämä ongelma ratkaistaan esittelemällä kohta järjestetyn 3-jonon (x, y, z) käsite, ja yleisemmin järjestetyn n-jonon $(x_0, \ldots, x_{n-1})$ käsite. Järjestetyn n-jonon määritelmä perustuu funktion käsitteeseen, joka on seuraavan alaluvun aihe.

Funktiot

Perinteisesti matematiikassa funktiot ajatellaan sääntöinä, jotka liittävät tarkasteltavan joukon alkioihin toisia alkioita. Tyypillisiä esimerkkejä tällaisista säännöistä ovat erilaiset lausekkeet, jotka on muodostettu annetuista perusfunktioista, joiden avulla funktion arvo voidaan laskea, kun argumentin arvo on annettu.

Esimerkki 3.2 Lauseke $x^2 - x + 2$ määrää reaalilukujen (tai rationaalilukujen tai kokonaislukujen) funktion $x \mapsto x^2 - x + 2$. Erityisesti

$$3 \mapsto 8, \quad -2 \mapsto 8, \quad 1 \mapsto 2, \quad \tfrac{1}{2} \mapsto \tfrac{7}{4}, \quad \sqrt{2} \mapsto 4 - \sqrt{2}.$$

Vastaavasti järjestetyt parit $\langle 3, 8 \rangle$, $\langle -2, 8 \rangle$, $\langle 1, 2 \rangle$, $\langle \frac{1}{2}, \frac{7}{4} \rangle$, $\langle \sqrt{2}, 4 - \sqrt{2} \rangle$ kuuluvat tämän funktion kuvaajaan.

Joukko-opissa annetaan täsmällinen ja mahdollisimman yleinen määritelmä funktion käsitteelle:

Määritelmä 3.4 Funktio on relaatio F siten, että jokaisella $x \in \mathrm{dom}(F)$ on olemassa vain yksi $y \in \mathrm{ran}(F)$ siten, että $\langle x, y \rangle \in F$. Toisin sanoen joukko F on funktio, jos se on relaatio ja sillä pätee

$$\forall x \in \mathrm{dom}(F) \exists y \in \mathrm{ran}(F) \big(xFy \wedge \forall z \in \mathrm{ran}(F)(xFz \rightarrow z = y) \big).$$

Jos $\langle x, y \rangle \in F$, niin y on F:n arvo pisteessä x ja sitä merkitään $y = F(x)$.

Huom: Merkintä $F(x)$ voidaan yleistää mille hyvänsä joukoille F ja x asettamalla

$$F(x) = \bigcup\{\, y \mid \langle x, y\rangle \in F \,\}.$$

Tällöin $F(x) = \emptyset$ aina kun x ei ole F:n määrittelyjoukossa $\mathrm{dom}(F)$. Toisaalta, jos F on funktio ja $x \in \mathrm{dom}(F)$, niin näin määritelty $F(x)$ on se yksikäsitteinen $y \in \mathrm{ran}(F)$, jolla $\langle x, y\rangle \in F$, niin kuin pitääkin.

Esimerkki 3.3 Tyhjä joukko $\emptyset$ on relaatio, koska siinä ei ole yhtään alkiota, joka ei ole järjestetty pari. Selvästi $\mathrm{dom}(\emptyset) = \emptyset$ ja $\mathrm{ran}(\emptyset) = \emptyset$, ja $\emptyset$ on myös funktio.

Funktion käsite on siis määritelty kiinnittämättä lähtöjoukkoa ja maalijoukkoa samalla. Nämä ja niihin liittyvä tuttu merkintätapa voidaan määritellä erikseen seuraavasti: Funktio F on funktio joukolta A joukolle B, $F\colon A \to B$, jos $\mathrm{dom}(F) = A$ ja $\mathrm{ran}(F) \subseteq B$.

Määritelmä 3.5 Olkoon $F\colon A \to B$ funktio.

$F\colon A \to B$ on *surjektio*, jos $\mathrm{ran}(F) = B$.

$F\colon A \to B$ on *injektio*, jos

$$\forall x \in A \forall y \in A\big(F(x) = F(y) \to x = y\big).$$

$F\colon A \to B$ on *bijektio*, jos se on sekä surjektio että injektio.

Esimerkki 3.4 (1) Tyhjä joukko on funktio tyhjältä joukolta mille hyvänsä joukolle B, eli voimme merkitä $\emptyset\colon \emptyset \to B$. Tämä funktio on aina injektio, ja se on surjektio joss $B = \emptyset$.

(2) Jokaisella joukolla A määritellään A:n identtinen funktio asettamalla

$$I_A = \{\, \langle x, x\rangle \in A \times A \mid x \in A \,\}.$$

Siis $I_A(x) = x$ jokaisella $x \in A$. Funktio $I_A\colon A \to A$ on aina bijektio, ja $I_\emptyset = \emptyset$.

Yleistämme seuraavaksi Injektion käsitteen mielivaltaisille joukoille. Nimeämme tämän yleistyksen *yksijuurisuudeksi*:

Määritelmä 3.6 Olkoon A joukko. A on yksijuurinen, jos

$$\forall y \in \mathrm{ran}(A) \exists x \in \mathrm{dom}(A)\big(xAy \land \forall z \in \mathrm{dom}(A)(zAy \to z = x)\big)$$

Huom: Jos F on funktio, niin F on yksijuurinen jos ja vain jos F on injektio. Toisaalta jos F ei ole funktio, niin ehto

$$\forall x \in \mathrm{dom}(F) \forall y \in \mathrm{dom}(F) \big(F(x) = F(y) \rightarrow x = y \big)$$

ei ole välttämättä yhtäpitävä yksijuurisuuden kanssa.

Seuraavaksi määrittelemme lisää käsitteitä, jotka ovat tärkeitä funktioille, mutta voidaan yleistää mille hyvänsä joukoille.

Määritelmä 3.7 Olkoot A, F ja G joukkoja.

(a) F:n *käänteisjoukko* on

$$F^{-1} = \{ \langle u, v \rangle \mid vFu \}.$$

(b) F:n ja G:n *yhdistetty joukko* on

$$F \circ G = \{ \langle u, v \rangle \mid \exists t \colon (uGt \wedge tFv) \}.$$

(c) F:n *rajoittuma joukkoon* A on

$$F \restriction A = \{ \langle u, v \rangle \mid uFv \wedge u \in A \}.$$

(d) A:n *kuva* F*:n suhteen* on

$$F[\![A]\!] = \mathrm{ran}(F \restriction A) = \{ v \mid \exists u \in A(uFv) \}.$$

Huomaa, että jos F on funktio, niin $F[\![A]\!] = \{ F(u) \mid u \in A \}$.

Joukkojen F^{-1}, $F \circ G$, $F \restriction A$ ja $F[\![A]\!]$ olemassaolo voidaan todistaa sopivilla osajoukkoaksioomilla. Seuraavassa esimerkissä käsitellään käänteisjoukon olemassaolo.

Esimerkki 3.5 Joukkojen $\mathrm{dom}(F)$ ja $\mathrm{ran}(F)$ olemassaolo on perusteltu aikaisemmin. Näiden olemassolosta seuraa joukon $\mathrm{ran}(F) \times \mathrm{dom}(F)$ olemassaolo. Nyt F^{-1} saadaan karteesisen tulon $\mathrm{ran}(F) \times \mathrm{dom}(F)$ osajoukkona:

$$F^{-1} = \{ \langle u, v \rangle \in \mathrm{ran}(F) \times \mathrm{dom}(F) \mid \langle v, u \rangle \in F \}.$$

Seuraavaksi muutamia esimerkkejä käänteisjoukoista, kuvajoukoista, rajoittumista ja yhdistetyistä joukoista.

Esimerkki 3.6 Olkoon $F \colon \mathbb{R} \to \mathbb{R}$ funktio $F(x) = x^2$, ja olkoon $A = [-1, 2] = \{ x \in \mathbb{R} \mid -1 \leq x \leq 2 \}$.

Tällöin $F[\![A]\!] = [0, 4]$, $F^{-1}[\![A]\!] = [-\sqrt{2}, \sqrt{2}]$. Huomaa, että F^{-1} ei ole funktio!

Esimerkki 3.7 Olkoon $g\colon \mathbb{R} \to \mathbb{R}$ funktio $g(x) = \sin x$. Tällöin g^{-1} ei ole funktio. Sen sijaan, jos $f = g \restriction [-\pi/2, \pi/2]$, niin f on injektio, ja siten f^{-1} on funktio. ($f^{-1}(x) = \arcsin x$).

Esimerkki 3.8 Tarkastellaan ihmisten joukkoa. Olkoon P vanhemmuusrelaatio

$$P = \{\, \langle x, y\rangle \mid x \text{ on } y\text{:n vanhempi} \,\}.$$

Tällöin $P^{-1} = \{\, \langle x, y\rangle \mid x \text{ on } y\text{:n lapsi} \,\}$ ja

$$\begin{aligned} P \circ P &= \{\, \langle x, y\rangle \mid \text{on olemassa } z\colon xPz \text{ ja } zPy \,\} \\ &= \{\, \langle x, y\rangle \mid x \text{ on } y\text{:n isovanhempi} \,\}. \end{aligned}$$

Jos $A = \{\, x \mid x \text{ on syntynyt Puolassa} \,\}$, niin

$$P \circ P[\![A]\!] = \{\, y \mid \text{ainakin yksi } y\text{:n isovanhemmista on syntynyt Puolassa} \,\}.$$

Esimerkki 3.9 Olkoon $F = \{\langle \emptyset, a\rangle, \langle \{\emptyset\}, b\rangle\}$. Tällöin F on funktio; F on injektio joss $a \neq b$.

Huomataan, että $F^{-1} = \{\langle a, \emptyset\rangle, \langle b, \{\emptyset\}\rangle\}$. Selvästi F^{-1} on funktio joss $a \neq b$. $F \restriction \emptyset = \emptyset$, mutta $F \restriction \{\emptyset\} = \{\langle \emptyset, a\rangle\}$. Siis $F[\![\{\emptyset\}]\!] = \{a\}$, mutta $F(\{\emptyset\}) = b$.

Tarkastelemme seuraavaksi käänteisjoukkoihin liittyviä perustuloksia.

Lause 3.5 *Jokaisella joukolla F pätee:*

$$\mathrm{dom}(F^{-1}) = \mathrm{ran}(F), \qquad \mathrm{ran}(F^{-1}) = \mathrm{dom}(F).$$

Jos F on relaatio, niin lisäksi pätee $(F^{-1})^{-1} = F$.

Todistus. Väitteet seuraavat suoraan määritelmistä. □

Lause 3.6 *Jokaisella joukolla F pätee*

$$F^{-1} \textit{ on funktio joss } F \textit{ on yksijuurinen.}$$

Jos F on relaatio, niin pätee myös

$$F \textit{ on funktio joss } F^{-1} \textit{ on yksijuurinen.}$$

Todistus. Harjoitustehtävä. □

Lause 3.7 *Olkoon F injektio.*

(a) Jos $x \in \mathrm{dom}(F)$, niin $F^{-1}\big(F(x)\big) = x$.

(b) Jos $y \in \mathrm{ran}(F)$, niin $F\big(F^{-1}(y)\big) = y$.

Todistus. Koska F on injektio, on se yksijuurinen relaatio, joten lauseen 3.6 perusteella F^{-1} on funktio. Siis $F^{-1}(y)$ on määritelty jokaisella $y \in \mathrm{ran}(F)$.

(a) Oletetaan, että $x \in \mathrm{dom}(F)$. Tällöin $\langle x, F(x)\rangle \in F$, joten $\langle F(x), x\rangle \in F^{-1}$. Siis $F(x) \in \mathrm{dom}(F^{-1})$ ja

$$F^{-1}\big(F(x)\big) = x.$$

(b) Oletetaan sitten, että $y \in \mathrm{ran}(F)$. Lauseesta 3.5 seuraa, että $y \in \mathrm{dom}(F^{-1})$. Nyt $\langle y, F^{-1}(y)\rangle \in F^{-1}$, mistä seuraa, että $F^{-1}(y), y\rangle \in F$. Siis väite

$$F\big(F^{-1}(y)\big) = y$$

pätee. □

Seuraavaksi käsittelemme funktioiden yhdistämistä.

Lause 3.8 *Olkoot F ja G funktioita. Tällöin $F \circ G$ on funktio ja jokaisella $x \in \mathrm{dom}(F \circ G)$ pätee $(F \circ G)(x) = F(G(x))$.*

Todistus. Oletetaan, että $x(F \circ G)y$ ja $x(F \circ G)y'$. Tällöin on olemassa t s.e. xGt ja tFy ja on olemassa t' s.e. xGt' ja $t'Fy'$. Koska G on funktio, on oltava $t = t'$. Koska F on funktio ja tFy ja tFy', on $y = y'$. Siis $F \circ G$ on funktio.

Oletetaan, että $x \in \mathrm{dom}(G)$ ja $G(x) \in \mathrm{dom}(F)$. Pitää osoittaa, että $x \in \mathrm{dom}(F \circ G)$ ja $(F \circ G)(x) = F(G(x))$.

$\langle x, G(x)\rangle \in G$ ja $\langle G(x), F(G(x))\rangle \in F$, joten $\langle x, F(G(x))\rangle \in F \circ G$, ja koska $F \circ G$ on funktio, pätee $(F \circ G)(x) = F(G(x))$.

Kääntäen, jos $x \in \mathrm{dom}(F \circ G)$, niin on olemassa t s.e. $\langle x, t\rangle \in G$ ja $\langle t, (F \circ G)(x)\rangle \in F$. Tällöin $x \in \mathrm{dom}(G)$, $t = G(x)$ ja $G(x) \in \mathrm{dom}(F)$. □

Esimerkki 3.10 Oletetaan, että G on injektio. Lauseen 3.8 perusteella $G^{-1} \circ G$ on funktio ja

$$\mathrm{dom}(G^{-1} \circ G) = \{\, x \in \mathrm{dom}(G) \mid G(x) \in \mathrm{dom}(G^{-1}) \,\} = \mathrm{dom}(G).$$

Jos $x \in \mathrm{dom}(G)$, niin $(G^{-1} \circ G)(x) = G^{-1}(G(x)) = x$. Siis $G^{-1} \circ G = I_{\mathrm{dom}(G)}$. Samoin nähdään, että $G \circ G^{-1} = I_{\mathrm{dom}(G^{-1})} = I_{\mathrm{ran}(G)}$.

Lause 3.9 *Kaikilla joukoilla F ja G pätee:*

$$(F \circ G)^{-1} = G^{-1} \circ F^{-1}.$$

Todistus. $(F \circ G)^{-1}$ ja $G^{-1} \circ F^{-1}$ ovat molemmat relaatioita, joten riittää osoittaa, että ne sisältävät täsmälleen samat järjestetyt parit:

$$\begin{aligned} \langle x, y\rangle \in (F \circ G)^{-1} &\Leftrightarrow \langle y, x\rangle \in F \circ G \\ &\Leftrightarrow \exists t(yGt \wedge tFx) \\ &\Leftrightarrow \exists t(tG^{-1}y \wedge xF^{-1}t) \\ &\Leftrightarrow \exists t(xF^{-1}t \wedge tG^{-1}y) \\ &\Leftrightarrow \langle x, y\rangle \in G^{-1} \circ F^{-1}. \end{aligned}$$

$\square$

Lause 3.10 *Oletetaan, että $F\colon A \to B$ on funktio, ja $A \neq \emptyset$.*

(a) *On olemassa funktio $G\colon B \to A$ s.e. $G \circ F = I_A$ (vasemman puoleinen käänteisfunktio) joss F on injektio.*

(b) *On olemassa funktio $H\colon B \to A$ s.e. $F \circ H = I_B$ (oikean puoleinen käänteisfunktio) joss F on surjektio.*

Todistus. Todistamme tässä vain kohdan (a); kohdan (b) todistuksessa tarvitaan uusi joukko-opin aksiooma.

(a) Oletetaan ensin, että on olemassa $G\colon B \to A$ s.e. $G \circ F = I_A$. Jos $F(x) = F(y)$, niin $x = G(F(x)) = G(F(y)) = y$. Siis F on injektio.

Oletetaan sitten, että F on injektio. Valitaan $a_0 \in A$ ($\neq \emptyset$). Määritellään

$$G(y) = \begin{cases} F^{-1}(y), & \text{jos } y \in \operatorname{ran}(F) \\ a_0, & \text{jos } y \in B \setminus \operatorname{ran}(F) \end{cases}$$

eli $G = F^{-1} \cup (B \setminus \operatorname{ran}(F)) \times \{a_0\}$.

Tällöin G on funktio ja $G(F(x)) = F^{-1}(F(x)) = x$ jokaisella $x \in \operatorname{dom}(F) = A$. Siis $G \circ F = I_A$ $\square$

Lauseen 3.10 kohdan (b) implikaatiota oikealta vasemmalle ei voi todistaa ilman valinta-aksioomaa:

Valinta-aksiooma (1. muotoilu). *Jokaisella relaatiolla R on olemassa funktio $H \subseteq R$, jolla* $\operatorname{dom}(H) = \operatorname{dom}(R)$.

Lauseen 3.10 kohdan (b) *todistus.* Oletetaan, että on olemassa $H\colon B \to A$ s.e. $F \circ H = I_B$. Tällöin jokaisella $y \in B$ on $(F \circ H)(y) = y$ eli $y = F(H(y))$, joten $y \in \operatorname{ran}(F)$. Siis $\operatorname{ran}(F) = B$ eli F on surjektio.

Oletetaan sitten, että F on surjektio. Valinta-aksiooma antaa funktion $H \subseteq F^{-1}$ s.e. $\operatorname{dom}(H) = \operatorname{dom}(F^{-1}) = \operatorname{ran}(F) = B$. Nyt jokaisella $y \in B$ pätee $\langle y, H(y)\rangle \in F^{-1}$, siis $\langle H(y), y\rangle \in F$ ja $F(H(y)) = y$. $\square$

Lause 3.11 *Kaikilla joukoilla F pätee*

(a) $$F[\![A \cup B]\!] = F[\![A]\!] \cup F[\![B]\!]$$
$$F\left[\!\!\left[\bigcup \mathcal{A}\right]\!\!\right] = \bigcup\{\, F[\![A]\!] \mid A \in \mathcal{A} \,\}$$

(b) $$F[\![A \cap B]\!] \subseteq F[\![A]\!] \cap F[\![B]\!]$$
$$F\left[\!\!\left[\bigcap \mathcal{A}\right]\!\!\right] \subseteq \bigcap\{\, F[\![A]\!] \mid A \in \mathcal{A} \,\}, \quad \mathcal{A} \neq \emptyset$$

Yhtäsuuruus on voimassa, jos F on yksijuurinen.

(c) $F[\![A]\!] \setminus F[\![B]\!] \subseteq F[\![A \setminus B]\!]$.

Todistus. Harjoitustehtävä. □

Esimerkki 3.11

$$\begin{aligned}
&F\colon \mathbb{R} \to \mathbb{R}, \quad F(x) = x^2 \\
&A = [-2, 0], \quad B = [1, 2] \\
&A \cap B = \emptyset \Rightarrow F[\![A \cap B]\!] = \emptyset \\
&F[\![A]\!] = [0, 4], \quad F[\![B]\!] = [1, 4] \Rightarrow F[\![A]\!] \cap F[\![B]\!] = [1, 4].
\end{aligned}$$

Huom: Jos F on funktio, niin F^{-1} on aina yksijuurinen. Siis lauseen 3.11 perusteella pätee

$$\begin{aligned}
F^{-1}[\![A \cup B]\!] &= F^{-1}[\![A]\!] \cup F^{-1}[\![B]\!] \\
F^{-1}[\![A \cap B]\!] &= F^{-1}[\![A]\!] \cap F^{-1}[\![B]\!]\,.
\end{aligned}$$

Olkoot A ja B joukkoja. Kaikkien funktioiden joukkoa A:lta B:lle merkitään

$$\begin{aligned}
{}^{A}B &= \{\, F \mid F : A \to B \,\} \\
&= \{\, F \mid F \text{ on funktio, } \mathrm{dom}(F) = A,\ \mathrm{ran}(F) \subseteq B \,\}
\end{aligned}$$

Jos joukossa B on n alkiota ja joukossa A on m alkiota, niin funktiojoukossa ${}^{A}B$ on n^m alkiota.

Huom: Joukolle ${}^{A}B$ käytetään usein myös merkintää B^A. Jos A ja B ovat kardinaalilukuja, niin B^A tarkoittaa kardinaalilukua B potenssiin A, joka ei ole funktiojoukko ${}^{A}B$.

Miten joukon ${}^{A}B$ olemassaolo todistetaan? Kukin $F\colon A \to B$ on joukon $A \times B$ osajoukko ja siten $F \in \mathcal{P}(A \times B)$. Siispä ${}^{A}B \subseteq \mathcal{P}(A \times B)$ ja ${}^{A}B$ saadaan osajoukkoaksioomalla joukosta $\mathcal{P}(A \times B)$.

Esimerkki 3.12 Olkoon ω taas luonnollisten lukujen joukko. Tällöin ${}^{\omega}\{0,1\}$ on kaikkien funktioiden $f\colon \omega \to \{0,1\}$ joukko. Kukin tällainen f voidaan ajatella äärettömänä $0,1$-jonona: $(f(0), f(1), f(2), \dots)$.

Toisaalta jokainen ääretön $0,1$-jono $(a_0, a_1, a_2, \dots)$ on itse asiassa funktio $f : \omega \to \{0,1\}$, kun määritellään $f(n) = a_n$ jokaisella $n \in \omega$.

Esimerkki 3.13 Jos $A \neq \emptyset$, niin ${}^{A}\emptyset = \emptyset$. Toisaalta ${}^{\emptyset}\emptyset = \{\emptyset\}$ ja yleisemmin ${}^{\emptyset}A = \{\emptyset\}$ jokaisella A.

Huomaa, että vastaavat yhtälöt pätevät myös luonnollisten lukujen potenssilaskulle: $0^n = 0$, kun $n \neq 0$, $0^0 = 1$ ja $n^0 = 1$.

Indeksöidyt joukkoperheet

Voimme nyt määritellä indeksöidyn joukkoperheen käsitteen: Jos I on joukko, ja A_i on joukko jokaisella $i \in I$, niin vastaava indeksöity joukkoperhe on $\operatorname{ran}(F)$, missä F on se funktio, jolla $\operatorname{dom}(F) = I$ ja $F(i) = A_i$ jokaisella $i \in I$. Siis $\{\, A_i \mid i \in I \,\} = \operatorname{ran}(F) = \{\, F(i) \mid i \in I \,\}$.

Indeksöinti on siis vain toinen tapa puhua funktioista. Erityisesti

$$\bigcup_{i \in I} A_i = \bigcup \{\, A_i \mid i \in I \,\} = \bigcup \{\, F(i) \mid i \in I \,\} = \bigcup \operatorname{ran}(F).$$

Esimerkki 3.14 Olkoon $I = \{0,1,2,3\}$. Tällöin

$$\bigcup_{i \in I} F(i) = \bigcup \{F(0), F(1), F(2), F(3)\},$$
$$\bigcap_{i \in I} F(i) = \bigcap \{\, F(i) \mid i \in I \,\} = \bigcap \operatorname{ran}(F).$$

I-jonot ja yleiset karteesiset tulot

Jos I on joukko, ja f on funktio s.e. $\operatorname{dom}(f) = I$, niin funktio f voidaan ajatella I-jonona $(a_i)_{i \in I}$, missä $a_i = f(i)$ jokaisella $i \in I$. Alkiota $f(i)$ voidaan sanoa I-jonon f i:nneksi koordinaatiksi (tai komponentiksi).

Erikoistapauksena tästä määrittelemme järjestetyn n-jonon käsitteen seuraavasti: merkintä $(a_0, \dots, a_{n-1})$ tarkoittaa funktiota f, jolla $\operatorname{dom}(f) = \{0, \dots, n-1\}$ ja $f(i) = a_i$ kullakin $i < n$. Tätä merkintää voi käyttää myös ilman alaindeksejä; esimerkiksi (x, y, z) tarkoittaa funktiota g, jolla $g(0) = x$, $g(1) = y$ ja $g(2) = z$. Myös "väärä"indeksöinti $(b_1, \dots, b_n)$ tulkitaan samoin.

Huom: Yleisesti pätee $(a,b) \neq \langle a,b \rangle$, sillä $(a,b) = \{\langle 0,a \rangle, \langle 1,b \rangle\}$, kun taas $\langle a,b \rangle = \{\{a\},\{a,b\}\}$.

Olkoon H funktio, jolla $\mathrm{dom}(H) = I$. Joukkojen $H(i)$, $i \in I$, karteesinen tulo määritellään seuraavasti:

$$\prod_{i \in I} H(i) = \{\, f \mid f \text{ on funktio, } \mathrm{dom}(f) = I \text{ ja } \forall i \in I(f(i) \in H(i)) \,\}.$$

Siis joukon $\prod_{i \in I} H(i)$ alkiot ovat I-jonoja, joiden i:s koordinaatti on aina joukossa $H(i)$.

Käytännössä usein käytetään merkintöjä

$$\prod_{i \in I} A_i \qquad \text{ja} \qquad (a_i)_{i \in I} \quad \text{tulon} \prod_{i \in I} A_i \text{ alkioille.}$$

Esimerkki 3.15 Jos $H(i) = A$ jokaisella $i \in I$, niin

$$\prod_{i \in I} H(i) = {}^{I}A.$$

Esimerkki 3.16 Olkoon $I = \omega$. Tällöin karteesisen tulon $\prod_{i \in \omega} H(i)$ alkiot ovat ω-jonoja $(f(0), f(1), f(2), \ldots)$.

On selvää, että jos $H(i) = \emptyset$ jollain $i \in I$, on $\prod_{i \in I} H(i) = \emptyset$.

Entä onko $\prod_{i \in I} H(i)$ epätyhjä, jos $H(i) \neq \emptyset$ jokaisella $i \in I$? Intuitiivisesti tämä tuntuu todelta, mutta sen todistamiseen tarvitaan valinta-aksioomaa! Itse asiassa, tämä väite on yksi valinta-aksiooman ekvivalenteista muotoiluista:

Valinta-aksiooma (2. muotoilu). *Jokaisella joukolla I ja jokaisella funktiolla H, jolla* $\mathrm{dom}(H) = I$ *pätee:*

$$\textit{jos } H(i) \neq \emptyset \textit{ jokaisella } i \in I, \textit{ niin} \prod_{i \in I} H(i) \neq \emptyset.$$

Ekvivalenssirelaatiot

Aloitetaan valmistelevalla esimerkillä.

Esimerkki 3.17 Jaetaan ω kolmeen osajoukkoon ("laatikkoon") seuraavasti

$$\begin{aligned} L_0 &= \{0, 3, 6, 9, 12, \ldots\} \\ L_1 &= \{1, 4, 7, 10, 13, \ldots\} \\ L_2 &= \{2, 5, 8, 11, 14, \ldots\} \end{aligned}$$

Määritellään A:ssa relaatio R:

$$xRy \Leftrightarrow x \text{ ja } y \text{ ovat samassa "laatikossa".}$$

Tällä relaatiolla R on seuraavat ominaisuudet

(a) R on *refleksiivinen* A:ssa: $\forall x \in A(xRx)$
(b) R on *symmetrinen*: $\forall x \forall y(xRy \rightarrow yRx)$
(c) R on *transitiivinen*: $\forall x \forall y \forall z(xRy \land yRz \rightarrow xRz)$

Määritelmä 3.8 R on ekvivalenssirelaatio joukossa A, jos R on relaatio, joka on refleksiivinen A:ssa, symmetrinen ja transitiivinen.

Seuraava lause osoittaa, että jokainen symmetrinen ja transitiivinen relaatio on ekvivalenssirelaatio. Refleksiivisyysoletus tarvitaan vain, jotta ekvivalenssirelaatio on määritelty koko joukossa A.

Lause 3.12 *Jos R on symmetrinen ja transitiivinen, niin se on ekvivalenssirelaatio joukossa* $\mathrm{fld}(R) = \mathrm{dom}(R) \cup \mathrm{ran}(R)$.

Todistus. Ensinnäkin R on relaatio joukossa $\mathrm{fld}(R)$. Pitää vielä osoittaa, että R on refleksiivinen joukossa $\mathrm{fld}(R)$.

Oletetaan siis, että $x \in \mathrm{fld}(R)$. Tällöin on olemassa $y \in \mathrm{fld}(R)$ s.e. xRy (tai yRx). Koska R on symmetrinen, pätee myös yRx (xRy), joten transitiivisuuden perusteella xRx. $\square$

Kuten Esimerkissä 3.17 näimme, joukon A jako erillisiin osajoukkoihin määrittelee A:n ekvivalenssirelaation. Kääntäen, jos R on ekvivalenssirelaatio joukossa A, niin sen avulla voidaan määritellä A:n jako erillisiin osajoukkoihin (eli ositus).

Määritelmä 3.9 Jos R on joukko,

$$[x]_R = \{\, t \mid xRt \,\}.$$

Jos R on ekvivalenssirelaatio ja $x \in \mathrm{fld}(R)$, niin $[x]_R$ on x:n ekvivalenssiluokka (modulo R). Jos R on yhteydestä selvä, voidaan käyttää lyhempää merkintää $[x]$.

Apulause 3.13 *Oletetaan, että R on ekvivalenssirelaatio A:ssa ja $x, y \in A$. Tällöin*

$$[x]_R = [y]_R \ \ \textit{joss} \ \ xRy.$$

Todistus. $\Rightarrow$: Oletetaan, että $[x]_R = [y]_R$. Koska yRy, niin $y \in [y]_R = [x]_R$, joten xRy.

$\Leftarrow$: Oletetaan, että xRy. Tällöin jokaisella $t \in A$:

$$t \in [y]_R \Rightarrow yRt \overset{R \text{ trans.}}{\Rightarrow} xRt \Rightarrow t \in [x]_R.$$

Siis $[y]_R \subseteq [x]_R$. Vaihtamalla x ja y keskenään ja R:n symmetrisyyttä käyttäen nähdään, että $[x]_R \subseteq [y]_R$. Siispä $[x]_R = [y]_R$. $\square$

Määritelmä 3.10 Joukon A ositus Π on joukko A:n epätyhjiä osajoukkoja, jolla pätee

(a) jos $B, C \in \Pi$, $B \neq C$, niin $B \cap C = \emptyset$;
(b) $\forall x \in A \exists B \in \Pi (x \in B)$ eli $A = \bigcup \Pi$.

Huom: Jos $A = \emptyset$, sen ainoa ekvivalenssirelaatio on $\emptyset$. Samoin $\emptyset$ on joukon A ainoa ositus.

Lause 3.14 *Jos R on ekvivalenssirelaatio A:ssa, niin $\{\, [x]_R \mid x \in A \,\}$ on A:n ositus.*

Todistus. Kukin $[x]_R \subseteq A$ ja $[x]_R \neq \emptyset$, koska $x \in [x]_R$.

(a) Jos $[x]_R \cap [y]_R \neq \emptyset$, on olemassa t s.e. $t \in [x]_R$ ja $t \in [y]_R$. Tällöin xRt ja yRt, joten symmetrisyyden perusteella tRy ja transitiivisuuden perusteella xRy. Apulauseen 3.13 perusteella $[x]_R = [y]_R$.
(b) $\forall x \in A \colon x \in [x]_R$, joten $A = \bigcup \{\, [x]_R \mid x \in A \,\}$.

$\square$

Ekvivalenssirelaatioon R liittyvää A:n ositusta on tapana merkitä "jakolaskumerkinnällä"

$$A/R = \{\, [x]_R \mid x \in A \,\}.$$

Esimerkki 3.18 (jatkoa Esimerkille 3.17) Määritellään relaatio $\sim$ ω:ssa seuraavasti:

$$m \sim n \iff m - n \text{ on jaollinen 3:lla.}$$

Tällöin

$$\begin{aligned}
[0]_\sim &= \{0, 3, 6, 9, \dots\} \\
[1]_\sim &= \{1, 4, 7, 10, \dots\} \\
[2]_\sim &= \{2, 5, 8, 11, \dots\}
\end{aligned}$$

Huomaa, että $[3]_\sim = [0]_\sim$, $[4]_\sim = [1]_\sim$, $[5]_\sim = [2]_\sim$, jne.

Kongruenssit

Jos R on joukon A ekvivalenssirelaatio, on olemassa ilmeinen tapa määritellä funktio $\varphi : A \to A/R$: asetetaan $\varphi(x) = [x]_R$ jokaisella $x \in A$. Selvästi φ on surjektio; sitä sanotaan *luonnolliseksi surjektioksi* (tai *kanoniseksi surjektioksi*). Huomaa, että $xRy \iff \varphi(x) = \varphi(y)$, kun $x, y \in A$.

Kääntäen, jokaiseen funktioon voidaan liittää luonnollisella tavalla ekvivalenssirelaatio:

Esimerkki 3.19 Olkoon $F\colon A \to B$ funktio. Määritellään relaatio $\sim$ asettamalla $x \sim y \iff F(x) = F(y)$. Tällöin on suoraviivaista todeta, että $\sim$ on A:n ekvivalenssirelaatio.

Relaation $\sim$ ekvivalenssiluokat saadaan alkukuvina joukon $\mathrm{ran}(F)$ alkioista: $[x]_\sim = F^{-1}[\![\{F(x)\}]\!]$, kun $x \in A$. Toisin sanoen, $A/{\sim} = \{\, F^{-1}[\![\{b\}]\!] \mid b \in \mathrm{ran}(F)\,\}$.

Olkoon $\varphi : A \to A/{\sim}$ luonnollinen surjektio. Tällöin on olemassa yksikäsitteinen funktio $\hat{F}\colon A/{\sim} \to B$, jolla pätee $F = \hat{F} \circ \varphi$. Nimittäin, jos $e \in A/{\sim}$, voimme määritellä $\hat{F}(e) = F(x)$ missä x on mikä hyvänsä ekvivalenssiluokan e alkio (jolloin $e = [x]_\sim$). Tämä on järkevä määritelmä ($\hat{F}$ on *hyvin määritelty*), sillä jos $x, y \in e$ ovat eri alkioita, pätee $F(x) = F(y)$ relaation $\sim$ määritelmän nojalla.

Oletetaan, että R on ekvivalenssirelaatio joukossa A ja $F\colon A \to A$ on funktio. Tarkastelemme yleisesti seuraavaa kysymystä: Onko mahdollista määritellä funktio

$$\hat{F}\colon A/R \to A/R \quad \text{siten että} \quad \hat{F}([x]_R) = [F(x)]_R?$$

Tutkimme ensin muutamaa esimerkkitapausta.

Esimerkki 3.20 Olkoon $\sim$ joukon ω ekvivalenssirelaatio, joka on määritelty ehdolla

$$m \sim n \;\Leftrightarrow\; m - n \text{ on jaollinen kuudella.}$$

Olkoot $F_i : \omega \to \omega$, $i < 3$, funktiot

$$\begin{aligned} F_0(n) &= 2n, \\ F_1(n) &= n^2, \\ F_2(n) &= 2^n. \end{aligned}$$

Tällöin $\hat{F}_0$ on olemassa: jos $n \sim m$, on $n - m$ jaollinen kuudella, jolloin $F_0(n) - F_0(m) = 2n - 2m = 2(n - m)$ on myös jaollinen kuudella.

$$\begin{aligned} \hat{F}_0([0]) &= [F_0(0)] = [0], \\ \hat{F}_0([1]) &= [F_0(1)] = [2], \\ &\vdots \\ \hat{F}_0([5]) &= [F_0(5)] = [10] = [4]. \end{aligned}$$

Myös $\hat{F}_1$ on olemassa: $F_1(n) - F_1(m) = n^2 - m^2 = (n + m)(n - m)$, joka on jaollinen kuudella, jos $n - m$ on. Esimerkiksi

$$\begin{aligned} \hat{F}_1([3]) &= [F_1(3)] = [9] = [3], \\ \hat{F}_1([4]) &= [F_1(4)] = [16] = [4], \\ \hat{F}_1([2]) &= [F_1(2)] = [4]. \end{aligned}$$

Sen sijaan $\hat{F}_2$ ei ole olemassa: $0 \sim 6$, mutta $F_2(0) = 2^0 = 1$, $F_2(6) = 2^6 = 64$ ja $[1] \neq [64] = [4]$, joten $F_2(0) \nsim F_2(6)$.

Yleisessä tapauksessa $\hat{F}$ on olemassa täsmälleen silloin, kun F ja R ovat keskenään yhteensopivat seuraavassa mielessä.

Määritelmä 3.11 Funktio $F : A \to A$ on yhteensopiva ekvivalenssirelaation R kanssa, jos

$$\forall x \in A \forall y \in A (xRy \to F(x)RF(y)).$$

Tällöin sanotaan myös, että R on *kongruenssi* F:n suhteen.

Lause 3.15 *Oletetaan, että R on ekvivalenssirelaatio A:ssa ja $F\colon A \to A$. Jos F on yhteensopiva R:n kanssa, niin on olemassa yksikäsitteinen funktio*

$$(*) \qquad \hat{F}\colon A/R \to A/R \quad s.e \quad \forall x \in A(\hat{F}([x]_R) = [F(x)]_R).$$

Jos F ei ole yhteensopiva R:n kanssa, niin tällaista $\hat{F}$ ei ole olemassa.

Todistus. Oletetaan ensin, että F ei ole yhteensopiva R:n kanssa. Tällöin on olemassa $x, y \in A$ s.e. xRy, mutta $F(x)RF(y)$ *ei* päde. Siis $[x]_R = [y]_R$, mutta $[F(x)]_R \neq [F(y)]_R$. Toisaalta vaatimus $(*)$ edellyttäisi, että

$$[F(x)]_R = \hat{F}([x]_R) = \hat{F}([y]_R) = [F(y)]_R,$$

mikä on mahdotonta.

Oletetaan, sitten, että F on yhteensopiva R:n kanssa. Ehtoa $(*)$ varten pitäisi olla $\langle [x], [F(x)] \rangle \in \hat{F}$ jokaisella $x \in A$. Pitää osoittaa, että tällä tavalla määritelty relaatio on itse asiassa funktio $A/R \to A/R$.

Ensinnäkin huomataan, että $\mathrm{dom}(\hat{F}) = A/R$, koska $\langle [x], [F(x)] \rangle \in \hat{F}$ jokaisella ekvivalenssiluokalla $[x]$. Selvästi myös $\mathrm{ran}(\hat{F}) \subseteq A/R$.

Tarkastellaan sitten pareja $\langle [x], [F(x)] \rangle, \langle [y], [F(y)] \rangle \in \hat{F}$. Jos $[x] = [y]$, on xRy, joten yhteensopivuuden määritelmän perusteella $F(x)RF(y)$ eli $[F(x)] = [F(y)]$.

Siis $\hat{F}$ on funktio $A/R \to A/R$, jolla ehto $(*)$ pätee. □

Yleistetään tarkastelu seuraavaksi kaksipaikkaisille funktioille. Oletetaan siis, että $F\colon A \times A \to A$ on funktio, ja R on joukon A ekvivalenssirelaatio. Tällöin sanotaan, että F yhteensopiva R:n kanssa, eli R on kongruenssi F:n suhteen, jos

$$\forall x \forall y \forall u \forall v \big(xRu \wedge yRv \to F(x,y)RF(u,v)\big).$$

Lauseesta 3.15 voidaan todistaa versio, joka pätee kaksipaikkaisille funktioille.

Huom: Käytämme tässä lyhennysmerkintää $F(x,y)$ oikean merkinnän $F(\langle x,y \rangle)$ sijaan. Jatkossa saa vapaasti käyttää myös lyhennysmerkintää $G(x_0, \ldots, x_{n-1}) := G((x_0, \ldots, x_{n-1}))$ n-jonojen funktioille, jne.

Esimerkki 3.21 Tarkastellaan kokonaislukujen $\mathbb{Z}$, yhteenlaskua $+\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}\colon \langle x, y \rangle \mapsto x + y$. Olkoon R joukon $\mathbb{Z}$ ekvivalenssirelaatio $xRy \;\Leftrightarrow\; x - y$ on jaollinen viidellä.

Jos xRu ja yRv pätevät, ovat $x - u$ ja $y - v$ viidellä jaollisia, jolloin myös $(x + y) - (u + v) = (x - u) + (y - v)$ on viidellä jaollinen, joten $(x + y)R(u + v)$. Siispä R on kongruenssi yhteenlaskun suhteen.

Järjestysrelaatiot

Määritelmä 3.12 Joukon A lineaarinen järjestys on relaatio $R \subseteq A \times A$, jolla pätee

(a) R on transitiivinen,

(b) R toteuttaa trikotomian A:ssa: kaikilla $x, y \in A$ pätee tasan yksi ehdoista

$$xRy, \qquad yRx, \qquad x = y.$$

Lause 3.16 *Olkoon R lineaarinen järjestys A:ssa. Tällöin*

(i) *R on irrefleksiivinen:* $\forall x \in A(\neg xRx)$,
(ii) *R on yhtenäinen:* $\forall x \in A \forall y \in A\big(x \neq y \to (xRy \vee yRx)\big)$,
(iii) *R ei sisällä syklejä: ei ole olemassa alkioita $x_1, \ldots, x_n \in A$ s.e.*

$$x_1 R x_2 \wedge x_2 R x_3 \wedge \cdots \wedge x_{n-1} R x_n \wedge x_n R x_1.$$

Todistus. Kohdat (i) ja (ii) jätetään harjoitustehtäväksi. Kohta (iii) todistetaan induktiolla n:n suhteen käyttäen transitiivisuutta ja lopuksi irrefleksiivisyyttä. □

Lineaarijärjestystä merkitään yleensä symbolilla $<$.

Luku 4

Luonnolliset luvut

Zermelo (1908) määritteli luonnolliset luvut seuraavasti:

$$\begin{array}{ccccc} \emptyset, & \{\emptyset\}, & \{\{\emptyset\}\}, & \{\{\{\emptyset\}\}\}, & \dots \\ 0 & 1 & 2 & 3 & \end{array}$$

Myöhemmin von Neumann otti käyttöön hieman erilaisen määritelmän:

$$\begin{aligned} 0 &= \emptyset, \\ 1 &= \{0\} = \{\emptyset\}, \\ 2 &= \{0,1\} = \{\emptyset, \{\emptyset\}\}, \\ 3 &= \{0,1,2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \\ &\vdots \\ n+1 &= \{0,1,\dots,n\} \end{aligned}$$

Von Neumannin määritelmästä on tullut joukko-opin standardimääritelmä. Huomaa, että sen mukaan pätee

$$\begin{aligned} &0 \in 1, 0 \in 2, 0 \in 3, \dots, 1 \in 2, 1 \in 3, \dots, 2 \in 3, \dots \\ &0 \subseteq 1 \subseteq 2 \subseteq 3 \subseteq \dots \end{aligned}$$

Luonnollisten lukujen järjestys voidaan siis palauttaa alkiorelaatioon:

$$n < m \iff n \in m.$$

Toisaalta niiden järjestys voidaan myös ilmaista osajoukkorelaation avulla:

$$n \leq m \iff n \subseteq m.$$

Induktiiviset joukot

Määritelmä 4.1 Jos a on joukko, sen seuraajajoukko on

$$a^+ = a \cup \{a\}.$$

Huom: Von Neumannin määritelmän perusteella luonnollisilla luvuilla pätee $n^+ = n + 1$.

Määritelmä 4.2 Joukko A on induktiivinen, jos

(1) $\emptyset \in A$ ja
(2) $\forall a \in A(a^+ \in A)$ ("A on suljettu seuraajan suhteen").

Luonnollisten lukujen joukko tullaan määrittelemään induktiivisen joukon käsitteen avulla. Tarvitsemme tätä varten vielä uuden joukko-opin aksiooman, joka takaa induktiivisten joukkojen olemassaolon.

Äärettömyysaksiooma. On olemassa induktiivinen joukko:

$$\exists A\big(\emptyset \in A \wedge \forall a \in A(a^+ \in A)\big).$$

Seuraavaksi määrittelemme luonnollisen luvun käsitteen.

Määritelmä 4.3 Luonnollinen luku on joukko, joka on alkiona jokaisessa induktiivisessa joukossa:

$$x \text{ on luonnollinen luku } \Leftrightarrow \forall A(\text{“}A \text{ induktiivinen”} \rightarrow x \in A).$$

Lause 4.1 *On olemassa joukko, jonka alkioita ovat täsmälleen ne joukot, jotka ovat luonnollisia lukuja.*

Todistus. Olkoon A induktiivinen joukko. Osajoukkoaksioomalla saadaan A:n osajoukko W, jossa ovat ne A:n alkiot, jotka kuuluvat kaikkiin induktiivisiin joukkoihin.

$$\begin{aligned} x \in W &\Leftrightarrow x \in A \wedge x \in B \text{ jokaisella induktiivisella joukolla } B \\ &\Leftrightarrow x \in B \text{ jokaisella induktiivisella joukolla } B. \end{aligned}$$

Siis W on etsitty luonnollisten lukujen joukko. $\square$

Luonnollisten lukujen joukkoa merkitään symbolilla ω.

$$\begin{aligned} x \in \omega &\Leftrightarrow x \text{ on luonnollinen luku} \\ &\Leftrightarrow x \in B \text{ jokaisella induktiivisella joukolla } B \\ &\Leftrightarrow x \in \bigcap \underbrace{\{\, B \mid B \text{ on induktiivinen} \,\}}_{\text{aito luokka}} \end{aligned}$$

Lause 4.2 *ω on induktiivinen ja ω on jokaisen induktiivisen joukon osajoukko.*

Todistus. $\emptyset \in \omega$, sillä $\emptyset$ on luonnollinen luku, koska $\emptyset \in B$ jokaisella induktiivisella joukolla B.

Jos $a \in \omega$, niin $a \in B$ jokaisella induktiivisella joukolla B. Tällöin $a^+ \in B$ jokaisella induktiivisella joukolla B, joten $a^+ \in \omega$. $\square$

Induktioperiaate ω:lle. Jokainen ω:n induktiivinen osajoukko on ω itse

$$\forall B(B \subseteq \omega \wedge \text{“}B \text{ induktiivinen”} \to B = \omega).$$

Induktiotodistukset. Halutaan todistaa, että ominaisuus $P(x)$ pätee jokaisella luonnollisella luvulla x.

Muodostetaan joukko

$$B = \{\, x \in \omega \mid P(x) \,\}.$$

Todistetaan, että B on induktiivinen:

(i) $\emptyset \in B$.
(ii) Jos $a \in B$, niin $a^+ \in B$.

Induktioperiaatteesta saadaan $B = \omega$ (koska $B \subseteq \omega$) eli $\forall x \in \omega\, P(x)$.

Lause 4.3 *Kaikki luonnolliset luvut paitsi* 0 *ovat toisen luonnollisen luvun seuraajia.*

Todistus. Olkoon $B = \{\, x \in \omega \mid x = 0 \vee \exists y \in \omega(x = y^+) \,\}$. Tällöin

(i) $\emptyset = 0 \in B$
(ii) Oletetaan, että $x \in B$. Tällöin myös $x^+ \in B$, sillä kaava $\exists y \in \omega(x^+ = y^+)$ on selvästi tosi.

Siis induktioperiaatteella saadaan, että $B = \omega$, joten kaikki luonnolliset luvut $x \neq 0$ ovat toisen luonnollisen luvun seuraajia. $\square$

Huom: 0 ei ole minkään luonnollisen luvun seuraaja: luvun a seuraaja on $a \cup \{a\}$, joka on aina epätyhjä joukko, kun taas $0 = \emptyset$.

Peanon postulaatit

Peanon systeemi on epätyhjästä joukosta N, funktiosta $S\colon N \to N$ ja alkiosta $e \in N$ muodostuva kolmikko:

$$(N, S, e)$$

joka toteuttaa seuraavat ehdot:

(i) $e \notin \mathrm{ran}(S)$
(ii) S on injektio
(iii) Jos $B \subseteq N \wedge e \in B \wedge \forall x(x \in B \rightarrow S(x) \in B)$, niin $B = N$.

Näiden Peanon postulaattien tarkoituksena on aksiomatisoida luonnollisten lukujen struktuuri, missä e vastaa lukua 0, ja S vastaa seuraajafunktiota $n \mapsto n + 1$. Osoitamme myöhemmin, että aksiomatisointi on täydellinen: kaikki Peanon systeemit ovat isomorfisia "oikean" luonnollisten lukujen struktuurin kanssa.

Kaikki kolme Peanon systeemien ehtoa ovat välttämättömiä. Jos ehto (i) jätettäisiin pois, sallittaisiin kolmikot, joissa N on äärellinen ja S muodostaa syklin: $N = \{a_0, \ldots, a_n\}$, $e = a_0$, $S(a_i) = a_{i+1}$, kun $i < n$ ja $S(a_n) = a_0$.

Jos puolestaan ehto (ii) jätettäisiin pois, sallittaisiin niin ikään äärellisiä tulkintoja, joissa S muodostuu syklistä sekä polusta joka yhdistää e:n tähän sykliin: $N = \{a_0, \ldots, a_n\}$, $e = a_0$, $S(a_i) = a_{i+1}$, kun $i < n$ ja $S(a_n) = a_i$ jollain $i > 0$.

Lopuksi, jos ehto (iii) jätettäisiin pois, sallittaisiin tulkintoja, joissa on luonnollisten lukujen struktuurin lisäksi erillisiä syklejä ja/tai erillisiä kokonaislukujen kopioita.

Määritelmä 4.4 Luonnollisten lukujen seuraajafunktio on joukko

$$\sigma = \{ \langle n, n^+ \rangle \mid n \in \omega \}.$$

Lause 4.4 $(\omega, \sigma, 0)$ *on Peanon systeemi.*

Todistus. Koska ω on induktiivinen, niin $0 \in \omega$ ja σ on funktio $\omega \rightarrow \omega$.

Peanon systeemien ehto (i) seuraa siitä, että $0 = \emptyset$ ei ole minkään luonnollisen luvun seuraaja, kuten huomautimme Lauseen 4.3 jälkeen. Ehto (iii) seuraa puolestaan suoraan ω:n induktioperiaatteesta.

ω:n induktioperiaate antaa suoraan ehdon (iii). Koska $0 = \emptyset$, mutta $n^+ = n \cup \{n\} \neq \emptyset$ jokaisella $n \in \omega$, on selvää, että $0 \neq \mathrm{ran}(\sigma)$.

Ehdon (ii) todistuksessa tarvitaan transitiivisen joukon käsite; täydennämme todistuksen myöhemmin. □

Määritelmä 4.5 Joukko A on *transitiivinen*, jos jokainen A:n alkion alkio on A:n alkio:

$$\forall x \forall a (x \in a \wedge a \in A \rightarrow x \in A)$$

Huom: Transitiivisuus voidaan määritellä usealla keskenään ekvivalentilla tavalla:

$$\begin{aligned}A \text{ on transitiivinen } &\Leftrightarrow \bigcup A \subseteq A \\ &\Leftrightarrow \forall a \in A(a \subseteq A) \\ &\Leftrightarrow A \subseteq \mathcal{P}A.\end{aligned}$$

Esimerkki 4.1 $A = \big\{\emptyset, \{\{\emptyset\}\}\big\}$ ei ole transitiivinen, koska $\{\emptyset\} \in \{\{\emptyset\}\} \in A$, mutta $\{\emptyset\} \notin A$. Sen sijaan $A \cup \{\{\emptyset\}\}$ on transitiivinen.

Lause 4.5 *Jos a on transitiivinen, niin $\bigcup a^+ = a$.*

Todistus. $\bigcup a^+ = \bigcup(a \cup \{a\}) = \bigcup a \cup \bigcup\{a\} = \underbrace{\bigcup A}_{\substack{\text{trans.}\\ \subseteq a}} \cup a = a.$ □

Lause 4.6 *Jokainen luonnollinen luku on transitiivinen.*

Todistus. Todistetaan väite induktiolla: olkoon $B = \{\, x \in \omega \mid x \text{ on transitiivinen} \,\}$.

(i) Selvästi $0 \in B$.

(ii) Oletetaan, että $x \in B$. Tällöin $\bigcup x^+ \overset{4.5}{=} x \subseteq x \cup \{x\} = x^+$, joten Määritelmän 4.5 perässä olevan huomautuksen nojalla $x^+ \in B$.

Siis B on induktiivinen, joten $B = \omega$. □

Lause 4.7 *ω on transitiivinen eli jokainen $x \in \omega$ on ω:n osajoukko.*

Todistus. Todistetaan induktiolla, että $\forall x \in \omega(x \subseteq \omega)$. Olkoon $B = \{\, x \in \omega \mid x \subseteq \omega \,\}$.

(i) $0 \in B$, sillä $0 = \emptyset \subseteq \omega$.

(ii) Oletetaan, että $x \in B$. Tällöin $x \subseteq \omega$ ja $\{x\} \subseteq \omega$, joten $x^+ = x \cup \{x\} \subseteq \omega$. Siis myös $x^+ \in B$.

□

Lauseen 4.4 todistus (σ on injektio). Oletetaan, että $m^+ = n^+$, $m, n \in \omega$. Tällöin $\bigcup m^+ = \bigcup n^+$, jolloin lauseiden 4.6 ja 4.5 perusteella $m = n$. □

Rekursio

Olkoon A joukko, $F\colon A \to A$ funktio, ja $a \in A$. Intuitiivisesti on selvää, että voimme määritellä funktion $h\colon \omega \to A$ rekursiolla seuraavasti:

$$\begin{aligned} h(0) &= a \\ h(1) &= F(h(0)) = F(a) \\ h(2) &= F(h(1)) = F(F(a)) \\ &\vdots \\ h(n^+) &= F(h(n)) = \underbrace{F(\dots F}_{n+1}(a)\dots) \end{aligned}$$

Funktion h olemassaolo ja yksikäsitteisyys pitää kuitenkin todistaa joukko-opin aksioomeista.

Rekursioteoreema. *Olkoon A joukko, $a \in A$ ja $F\colon A \to A$. Tällöin on olemassa yksikäsitteinen funktio $h\colon \omega \to A$, jolla pätee*

$$h(0) = a \quad \text{ja jokaisella } n \in \omega\text{:} \quad h(n^+) = F(h(n)).$$

Todistus. Sanotaan, että funktio v on hyväksyttävä, jos $\mathrm{dom}(v) \subseteq \omega$, $\mathrm{ran}(v) \subseteq A$ ja seuraavat ehdot ovat voimassa:

(i) Jos $0 \in \mathrm{dom}(v)$, niin $v(0) = a$.
(ii) Jos $n^+ \in \mathrm{dom}(v)$, niin myös $n \in \mathrm{dom}(v)$ ja $v(n^+) = F(v(n))$.

Olkoon $\mathcal{K}$ kaikkien hyväksyttävien funktioiden joukko ja olkoon $h = \bigcup \mathcal{K}$. Siis

(∗) $\qquad \langle n, y\rangle \in h \ \Leftrightarrow\ v(n) = y$ jollakin hyväksyttävällä funktiolla v.

Todistetaan seuraavat asiat:

(1) h on funktio,
(2) h on hyväksyttävä,
(3) $\mathrm{dom}(h) = \omega$,
(4) h on yksikäsitteinen.

(1) Olkoon $S = \{\, n \in \omega \mid$ on olemassa korkeintaan yksi y s.e. $\langle n, y\rangle \in h \,\}$. Osoitetaan, että S on induktiivinen.

Jos $\langle 0, y_1\rangle \in h$ ja $\langle 0, y_2\rangle \in h$, niin ehdon (∗) mukaan on olemassa hyväksyttävät funktiot v_1 ja v_2, joilla $v_1(0) = y_1$ ja $v_2(0) = y_2$. Tällöin kohdan (i) perusteella $v_1(0) = a = v_2(0)$, joten $y_1 = y_2 = a$. Siis $0 \in S$.

Oletetaan sitten, että $k \in S$. Jos $\langle k^+, y_1\rangle \in h$ ja $\langle k^+, y_2\rangle \in h$, niin ehdon (∗) perusteella on olemassa funktiot $v_1, v_2 \in \mathcal{K}$, joilla $v_1(k^+) = y_1$ ja $v_2(k^+) = y_2$. Tällöin kohdan (ii) perusteella $k \in \mathrm{dom}(v_1)$, $k \in \mathrm{dom}(v_2)$. Koska $k \in S$, on

$v_1(k) = v_2(k)$, joten $v_1(k^+) = F(v_1(k)) = F(v_2(k)) = v_2(k^+)$ eli $y_1 = y_2$. Siis myös $k^+ \in S$.

Induktioperiaatteesta seuraa, että $S = \omega$ eli h on funktio.

(2) $h = \bigcup \mathcal{K}$ on hyväksyttävä funktio: kohdan (1) perusteella h on funktio, ja selvästi $\mathrm{dom}(h) \subseteq \omega$ ja $\mathrm{ran}(h) \subseteq A$.

(i) Jos $0 \in \mathrm{dom}(h)$, niin on olemassa hyväksyttävä funktio v s.e. $v(0) = h(0)$. Koska $v \in \mathcal{K}$, on $v(0) = a$ ja siis $h(0) = a$.

(ii) Olkoon $n^+ \in \mathrm{dom}(h)$. Tällöin on olemassa $v \in \mathcal{K}$, jolla $h(n^+) = v(n^+)$ ja $n \in \mathrm{dom}(v)$. Siis $n \in \mathrm{dom}(h)$ ja $h(n) = v(n)$, sillä h on funktio. Siispä $h(n^+) = v(n^+) = F(v(n)) = F(h(n))$.

(3) $\mathrm{dom}(h) = \omega$: Osoitetaan, että $\mathrm{dom}(h)$ on induktiivinen. Funktio $\{\langle 0, a\rangle\}$ on hyväksyttävä, joten $\langle 0, a\rangle \in h$ ja siis $0 \in \mathrm{dom}(h)$.

Oletetaan, että $k \in \mathrm{dom}(h)$. On siis olemassa $v \in \mathcal{K}$, jolla $k \in \mathrm{dom}(v)$. Jos $k^+ \in \mathrm{dom}(v)$, on myös $k^+ \in \mathrm{dom}(h)$. Jos taas $k^+ \notin \mathrm{dom}(v)$, määritellään $v' = v \cup \{\langle k^+, F(v(k))\rangle\}$. Selvästi v' on funktio, $\mathrm{dom}(v') \subseteq \omega$, $\mathrm{ran}(v') \subseteq A$. Funktio v' on hyväksyttävä:

(i) Jos $0 \in \mathrm{dom}(v')$, niin $v'(0) = v(0) \overset{v \in \mathcal{K}}{=} a$.

(ii) Jos $n^+ \in \mathrm{dom}(v')$, niin joko $n^+ \in \mathrm{dom}(v)$ tai $n^+ = k^+$ eli $n = k$; molemmissa tapauksissa $n \in \mathrm{dom}(v) \subseteq \mathrm{dom}(v')$. Edellisessä tapauksessa pätee $v'(n^+) = v(n^+) \overset{v \in \mathcal{K}}{=} F(v(n)) = F(v'(n))$. Jälkimmäisessä tapauksessa puolestaan pätee $v'(n^+) = v'(k^+) = F(v(k)) = F(v'(k)) = F(v'(n))$.

Koska v' on hyväksyttävä funktio ja $k^+ \in \mathrm{dom}(v')$, pätee $k^+ \in \mathrm{dom}(h)$.

(4) h on yksikäsitteinen: Oletetaan, että h_1 ja h_2 toteuttavat lauseen ehdot. Osoitetaan, että joukko

$$S = \{\, n \in \omega \mid h_1(n) = h_2(n) \,\}$$

on induktiivinen. Tästä seuraa, että $h_1 = h_2$.

Koska h_1 ja h_2 ovat hyväksyttäviä funktioita, pätee $h_1(0) = a = h_2(0)$, joten $0 \in S$.

Oletetaan sitten, että $k \in S$. Nyt $h_1(k^+) = F(h_1(k)) \overset{k \in S}{=} F(h_2(k)) = h_2(k^+)$. Siis $k^+ \in S$. □

Esimerkki 4.2 Olkoon $\mathbb{Z} = \{\dots, -1, 0, 1, 2, \dots\}$ kokonaislukujen joukko. Ei ole olemassa funktiota $h\colon \mathbb{Z} \to \mathbb{Z}$ siten, että jokaisella $a \in \mathbb{Z}$ pätee

$$h(a+1) = h(a)^2 + 1.$$

Toisaalta, jos $F\colon \mathbb{Z} \to \mathbb{Z}$ on funktio

$$F(a) = \begin{cases} a+1, & \text{jos } a < 0; \\ a, & \text{jos } a \geq 0, \end{cases}$$

niin on olemassa äärettömän monta eri funktiota $h\colon \mathbb{Z} \to \mathbb{Z}$ s.e. $h(0) = 0$ ja $h(n+1) = F(h(a))$.

Siis rekursioteoreemaa ei voi yleistää kokonaislukujen joukkoon!

Lause 4.8 *Olkoon (N, S, e) Peanon systeemi. Tällöin (ω, σ, o) ja (N, S, e) ovat keskenään isomorfiset: on olemassa bijektio $h\colon \omega \to N$ siten, että $h(0) = e$ ja jokaisella $n \in \omega$ pätee $h(\sigma(n)) = S(h(n))$.*

Todistus. Rekursioteoreeman nojalla on olemassa yksikäsitteinen funktio $h\colon \omega \to N$, joka toteuttaa ehdot

$$\begin{aligned} h(0) &= e, \\ h(n^+) &= S(h(n)) \ \text{ kaikilla } \ n \in \omega. \end{aligned}$$

Koska $\sigma(n) = n^+$, funktio h toteuttaa vaatimuksen $h(\sigma(n)) = S(h(n))$ kaikilla $n \in \omega$.

Pitää vielä osoittaa, että h on bijektio.

Osoitetaan ensin, että h on surjektio käyttämällä Peanon induktiopostulaattia joukolle $\operatorname{ran}(h)$ systeemissä (N, S, e). Ensinnäkin $e \in \operatorname{ran}(h)$, koska $h(0) = e$. Toiseksi, jos $x \in \operatorname{ran}(h)$, niin on olemassa $n \in \omega$, jolla $h(n) = x$. Tällöin $h(n^+) = S(h(n)) = S(x)$, joten myös $S(x) \in \operatorname{ran}(h)$. Siis $\operatorname{ran}(h)$ on induktiivinen, joten $\operatorname{ran}(h) = N$.

Osoitetaan lopuksi, että h on injektio. Tällä kerralla käytämme luonnollisten lukujen induktioperiaatetta. Olkoon

$$T = \{\, n \in \omega \mid \forall m \in \omega (m \neq n \to h(m) \neq h(n)) \,\}.$$

Jos $m \neq 0$, niin $m = p^+$, jollain $p \in \omega$. Tällöin $h(m) = h(p^+) = S(h(p)) \neq e = h(0)$. Siis $0 \in T$.

Oletetaan sitten, että $k \in T$. Jos $h(k^+) = h(m)$, niin äskeisen perusteella $m \neq 0$, joten $m = p^+$ jollakin $p \in \omega$. Siis $S(h(k)) = h(k^+) = h(p^+) = S(h(p))$. Koska S on injektio, on oltava $h(k) = h(p)$, joten $k = p$ (koska $k \in T$) ja siis $k^+ = p^+ = m$. Siis $k^+ \in T$. □

Aritmetiikka

Aloitetaan tarkastelemalla funktiota $\omega \to \omega$, joka liittää lukuun n luvun $5 + n$. Sille voidaan antaa seuraava rekursiivinen määritelmä:

$$\begin{aligned} 5 + 0 &= 5 \\ 5 + n^+ &= (5 + n)^+ \end{aligned}$$

Yleisemmin, voimme määritellä jokaisella luonnollisella luvulla m funktion $\omega \to \omega$, joka liittää lukuun n luvun $m+n$ seuraavasti:

$$\begin{cases} A_m(0) = m \\ A_m(n^+) = (A_m(n))^+ \end{cases}$$

Rekursioteoreeman perusteella on olemassa yksikäsitteinen $A_m \colon \omega \to \omega$, joka toteuttaa yllä olevat ehdot.

Mutta miten näiden funktioiden avulla saadaan määriteltyä luonnollisten lukujen yhteenlasku? Yhteenlasku on joukon ω *kaksipaikkainen laskutoimitus*, eli funktio

$$f \colon \omega^2 \to \omega.$$

Tässä $\omega^2 = \{\, (x,y) \mid x,y \in \omega \,\}$; vastaavasti merkintä ω^n tarkoittaa joukkoa $\{\, (x_0,\dots,x_{n-1}) \mid x_0,\dots,x_{n-1} \in \omega \,\}$, kun $n \in \omega$.

Määritelmä 4.6 Yhteenlasku $+$ on kaksipaikkainen laskutoimitus joukolla ω, joka on määritelty seuraavasti:

$$+(m,n) = A_m(n)$$

kaikilla $m,n \in \omega$. Toisin sanoen, yhteenlasku on relaatio

$$+ = \{\, \langle (m,n), p \rangle \in \omega^2 \times \omega \mid p = A_m(n) \,\}.$$

Funktiomerkinnän $+(m,n)$ sijasta summa voidaan kirjoittaa tavalliseen tapaan muodossa $m+n$.

Suoraan funktioiden A_m rekursiivisesta määritelmästä seuraa yhteenlaskun rekursiokaava:

Lause 4.9 *Kaikilla $m,n \in \omega$ pätee*

(A1) $$m + 0 = m,$$

(A2) $$m + n^+ = (m+n)^+.$$

Huom: Soveltamalla ehtoa (A2) tapauksessa $n = 0$ nähdään, että $m + 1 = m + 0^+ = (m+0)^+$. Koska ehdon (A1) perusteella $m + 0 = m$, saadaan edelleen $m^+ = m + 1$. Seuraajafunktio σ siis liittää jokaiseen lukuun m luvun $m+1$, niin kuin pitääkin.

Määritellään seuraavaksi luonnollisten lukujen kertolasku samalla idealla. Lähtökohtana on havainto, että osittelulain perusteella $m \cdot (n+1) = m \cdot n + m$.

Olkoon $m \in \omega$. Funktio $M_m \colon \omega \to \omega$ määritellään rekursiolla seuraavasti:

$$\begin{cases} M_m(0) = 0 \\ M_m(n^+) = M_m(n) + m. \end{cases}$$

Koska yhteenlasku on jo määritelty, rekursioteoreeman perusteella on olemassa yksikäsitteinen funktio $M_m \colon \omega \to \omega$, joka toteuttaa ylläolevat ehdot.

Määritelmä 4.7 Kertolasku $\cdot$ on kaksipaikkainen laskutoimitus joukolla ω siten, että kaikilla $m, n \in \omega$ pätee

$$\cdot(m, n) = M_m(n).$$

Siis kertolasku on relaatio

$$\cdot = \{ \langle (m, n), p \rangle \in \omega^2 \times \omega \mid p = M_m(n) \}.$$

Merkinnän $\cdot(m, n)$ sijasta käytetään yleensä merkintää $m \cdot n$.

Lause 4.10 *Kaikilla $m, n \in \omega$ pätee:*

(M1) $$m \cdot 0 = 0,$$

(M2) $$m \cdot n^+ = m \cdot n + m.$$

Huom: Merkinnässä $m \cdot n + m$ oletetaan tavalliseen tapaan, että kertolasku suoritetaan ennen yhteenlaskua. Käytämme tätä sopimusta myös jatkossa.

Samaan tapaan voidaan määritellä eksponenttifunktiot $(m, n) \mapsto m^n$. Määritellään ensin funktiot $E_m : \omega \to \omega$, $m \in \omega$, käyttämällä potenssien laskusääntöjä, ja sen jälkeen yhdistetään nämä yhdeksi funktioksi, joka toteuttaa ehdot:

(E1) $$m^0 = 1,$$

(E2) $$m^{n^+} = m^n \cdot m.$$

Esimerkki 4.3 Lasketaan $2 + 3$ käyttäen yhteenlaskun rekursiivista määritelmää.

$$\begin{aligned} 2 + 0 &= 2 \qquad \text{(A1)} \\ 2 + 1 &\overset{\text{(A2)}}{=} (2 + 0)^+ = 2^+ = 3 \\ 2 + 2 &\overset{\text{(A2)}}{=} (2 + 1)^+ = 3^+ = 4 \\ 2 + 3 &\overset{\text{(A2)}}{=} (2 + 2)^+ = 4^+ = 5 \end{aligned}$$

Todistamme seuraavaksi yhteenlaskun ja kertolaskun tutut perusominaisuudet.

Lause 4.11 *Seuraavat yhtälöt pätevät kaikilla $m, n, p \in \omega$:*

(1) *yhteenlaskun liitännäisyys*

$$m + (n + p) = (m + n) + p$$

(2) *yhteenlaskun vaihdannaisuus*

$$m + n = n + m$$

(3) *osittelulaki*

$$m \cdot (n + p) = m \cdot n + m \cdot p$$

(4) *kertolaskun liitännäisyys*

$$m \cdot (n \cdot p) = (m \cdot n) \cdot p$$

(5) *kertolaskun vaihdannaisuus*

$$m \cdot n = n \cdot m.$$

Todistus. Jokainen kohta todistetaan induktiolla! Kohdat (1), (4) ja (5) jätetään kuitenkin harjoitustehtäviksi.

(2) Todistamme ensin kaksi aputulosta:

(a) **Väite:** $0 + n = n$ jokaisella $n \in \omega$.
Todistus. Olkoon $A = \{ n \in \omega \mid 0 + n = n \}$. Riittää osoittaa, että joukko A on induktiivinen.
$0 \in A$ suoraan ehdon (A1) perusteella. Oletetaan sitten, että $k \in A$. Tällöin

$$0 + k^+ \overset{\text{(A2)}}{=} (0 + k)^+ \overset{k \in A}{=} k^+,$$

joten myös $k^+ \in A$. Siispä A on induktiivinen.

(b) **Väite:** $m^+ + n = (m + n)^+$ kaikilla $m, n \in \omega$.
Todistus. Olkoon $B = \{ n \in \omega \mid m^+ + n = (m + n)^+ \}$, missä $m \in \omega$ on kiinteä. Osoitetaan, että B on induktiivinen.
$0 \in B$, sillä $m^+ + 0 \overset{\text{(A1)}}{=} m^+ \overset{\text{(A1)}}{=} (m + 0)^+$. Edelleen, jos $k \in B$, niin

$$m^+ + k^+ \overset{\text{(A2)}}{=} (m^+ + k)^+ \overset{k \in B}{=} (m + k)^{++} \overset{\text{(A2)}}{=} (m + k^+)^+,$$

joten $k^+ \in B$. Siis B on induktiivinen.

Nyt voidaan todistaa lauseen kohta (2). Olkoon $n \in \omega$ kiinteä, ja olkoon

$$C = \{ m \in \omega \mid m + n = n + m \}.$$

Osoitetaan, että C on induktiivinen.

Aputuloksen (a) nojalla $0 + n = n$ ja ehdon (A1) nojalla $n = n + 0$, joten $0 \in C$.

Oletetaan sitten, että $k \in C$. Tällöin

$$k^+ + n \overset{\text{(b)}}{=} (k+n)^+ \overset{k \in C}{=} (n+k)^+ \overset{\text{(A2)}}{=} n + k^+,$$

joten $k^+ \in C$. Siis C on induktiivinen.

(3) Olkoon $A = \{\, p \in \omega \mid m \cdot (n+p) = m \cdot n + m \cdot p \,\}$, missä $m, n \in \omega$ ovat kiinteitä. Riittää osoittaa, että joukko A on induktiivinen.

Ensinnäkin $0 \in A$, sillä

$$m \cdot (n+0) \overset{\text{(A1)}}{=} m \cdot n \overset{\text{(A1)}}{=} m \cdot n + 0 \overset{\text{(M1)}}{=} m \cdot n + m \cdot 0$$

Oletetaan sitten, että $k \in A$. Tällöin

$$\begin{aligned} m \cdot (n + k^+) &\overset{\text{(A2)}}{=} m \cdot (n+k)^+ \\ &\overset{\text{(M2)}}{=} m \cdot (n+k) + m \\ &\overset{k \in A}{=} (m \cdot n + m \cdot k) + m \overset{(1)}{=} m \cdot n + (m \cdot k + m) \\ &\overset{\text{(M2)}}{=} m \cdot n + m \cdot k^+. \end{aligned}$$

Siis myös $k^+ \in A$. □

Luonnollisten lukujen järjestys

Kuten aikaisemmin todettiin, von Neumannin määritelmän perusteella luonnollisten lukujen tavallinen järjestys voidaan palauttaa alkiorelaatioon ja toisaalta myös osajoukkorelaatioon: $m < n \;\Leftrightarrow\; m \in n$ ja $m \leq n \;\Leftrightarrow\; m \subseteq n$.

Siksi on luonnollista ottaa alkiorelaatio joukon ω järjestyksen määritelmäksi. Mutta ensin alkiorelaatio pitää tulkita joukon ω kaksipaikkaisena relaationa (eli joukon $\omega \times \omega$ osajoukkona), ja sen jälkeen on todistettava, että tämä relaatio toteuttaa lineaarijärjestyksen aksioomat.

Määritellään siis kaksipaikkainen relaatio $\in_\omega$ joukossa ω asettamalla

$$\in_\omega = \{\, \langle m, n \rangle \in \omega \times \omega \mid m \in n \,\}.$$

Tavoitteena on siis todistaa, että $\in_\omega$ on lineaarijärjestys ω:lla.

Apulause 4.12 *Relaatio $\in_\omega$ on transitiivinen.*

Todistus. Oletetaan, että $\langle m, n \rangle \in \in_\omega$ ja $\langle n, p \rangle \in \in_\omega$. Siis $m \in n$ ja $n \in p$, ja koska p on transitiivinen joukko, pätee myös $m \in p$, eli $\langle m, p \rangle \in \in_\omega$. □

Pitää vielä todistaa, että relaatio $\in_\omega$ toteuttaa trikotomian:

kaikilla $m, n \in \omega$ pätee täsmälleen yksi ehdoista $m \in n$, $n \in m$, $m = n$.

Tätä varten tarvitaan seuraava apulause.

Apulause 4.13

(a) $\forall m, n \in \omega \colon m \in n \;\Leftrightarrow\; m^+ \in n^+$,

(b) $\forall m \in \omega \colon m \notin m$.

Todistus. (a) Oletetaan ensin, että $m^+ \in n^+$. Koska $n^+ = n \cup \{n\}$, tällöin $m^+ \in n$ tai $m^+ = n$. Koska $m \in m^+$, edellisessä tapauksessa väite $m \in n$ pätee joukon n transitiivisuuden perusteella, ja jälkimmäisessä tapauksessa suoraan oletuksen $m = n$ perusteella. Siis $m^+ \in n^+ \;\Rightarrow\; m \in n$.

Implikaatio toiseen suuntaan todistetaan induktiolla. Olkoon T joukko $\{\, n \in \omega \mid \forall m \in n \colon m^+ \in n^+ \,\}$. Tällöin $0 \in T$, koska $m \notin 0$ millään m. Oletetaan sitten, että $k \in T$. Pitää osoittaa, että $k^+ \in T$ eli $\forall m \in k^+ \colon m^+ \in k^{++}$. Oletetaan siis, että $m \in k^+$. Tällöin joko $m \in k$ tai $m = k$. Edellisessä tapauksessa $m^+ \in k^+ \subseteq k^{++}$, koska $k \in T$. Jos taas $m = k$, on $m^+ = k^+$ ja $k^+ \in k^{++}$, joten $m^+ \in k^{++}$. Siis $k^+ \in T$ eli T on induktiivinen.

(b) Väite todistetaan induktiolla. Olkoon $T = \{\, n \in \omega \mid n \notin n \,\}$. Tällöin $0 \in T$, koska $0 = \emptyset$. Oletetaan, että $k \in T$, ja tehdään vastaoletus: $k^+ \notin T$, eli $k^+ \in k^+$. Tällöin kohdan (a) perusteella $k \in k$, mikä on mahdotonta, koska $k \in T$. Siis $k^+ \in T$ ja T on induktiivinen. $\square$

Trikotomialaki relaatiolle $\in_\omega$. *Kaikilla $m, n \in \omega$ pätee tasan yksi ehdoista $m \in n$, $n \in m$, $m = n$.*

Todistus. Ensinnäkin korkeintaan yksi näistä ehdoista pätee:

> Jos olisi $m \in n \wedge n \in m$, saataisiin transitiivisuuden perusteella $m \in m$, mikä on mahdotonta apulauseen 4.13 nojalla.
>
> Jos taas pätisi $m \in n \wedge m = n$ (tai $n \in m \wedge m = n$), olisi myös $m \in m$, ja saataisiin sama ristiriita.

Vielä pitää osoittaa, että vähintään yksi ehdoista pätee. Tehdään tämä taas induktiolla.

Olkoon $T = \{\, n \in \omega \mid \forall m \in \omega (m \in n \vee n \in m \vee m = n) \,\}$. Pitää ensin osoittaa, että $0 \in T$, eli kaikilla $m \in \omega$ pätee jokin ehdoista $m \in 0$, $0 \in m$ tai $m = 0$. Jos m on 0, tämä selvästi pätee. Todistetaan induktiolla, että jos $m \neq 0$, niin $0 \in m$:

> Olkoon $B = \{\, m \in \omega \mid m \neq 0 \Rightarrow 0 \in m \,\}$. Selvästi $0 \in B$. Jos $k \in B$, niin $0 \in k \subseteq k^+$, joten $k^+ \in B$.

Oletetaan sitten, että $k \in T$. Siis jokaisella $m \in \omega$ pätee joko $m \in k$, $k \in m$ tai $m = k$. Ensimmäisessä tapauksessa pätee joukon k^+ transitiivisuuden perusteella $m \in k^+$. Keskimmäisessä tapauksessa pätee $k^+ \in m^+$ Apulauseen 4.13 nojalla. Viimeisessä tapauksessa taas $m^+ = k^+$. Siis joka tapauksessa yksi ehdoista $m \in k^+$, $k^+ \in m$, $m = k^+$ on voimassa, joten $k^+ \in T$. $\square$

Merkitsemme $A \subset B$, jos A on B:n aito osajoukko, eli

$$A \subset B \;\Leftrightarrow\; A \subseteq B \wedge A \notin B.$$

Seuraus 4.14 *Kaikilla $m, n \in \omega$ pätee*

$$m \in n \;\Leftrightarrow\; m \subset n.$$

Todistus. Oletetaan ensin, että $m \in n$. Tällöin $m \subseteq n$, koska n on transitiivinen joukko. Trikotomiaehdon perusteella $m \neq n$, joten osajoukkorelaatio on aito: $m \subset n$.

Oletetaan kääntäen, että $m \subset n$. Tällöin $m \neq n$ ja $n \notin m$, sillä muuten edellä olevan päättelyn mukaan olisi $n \subset m$. Nyt trikotomiaehdosta seuraa, että $m \in n$. $\square$

Lause 4.15 *Kaikilla $m, n, p \in \omega$ pätee:*

(1) $$m \in n \;\Leftrightarrow\; m + p \in n + p.$$

Jos lisäksi $p \neq 0$, pätee myös:

(2) $$m \in n \;\Leftrightarrow\; m \cdot p \in n \cdot p.$$

Todistus. (1) "$\Rightarrow$": Oletetaan, että $m, n \in \omega$ s.e. $m \in n$. Olkoon $A = \{ p \in \omega \mid m + p \in n + p \}$. Osoitetaan, että A on induktiivinen. Ensinnäkin $0 \in A$, sillä $m + 0 = m \;\in\; n = n + 0$. Oletetaan sitten, että $k \in A$. Siis $m + k \in n + k$, joten Lauseen 4.13(a) perusteella $(m + k)^+ \in (n + k)^+$. Koska $(m + k)^+ = m + k^+$ ja $(n + k)^+ = n + k^+$, tästä seuraa, että $k^+ \in A$.

"$\Leftarrow$": Oletetaan, että $m + p \in n + p$. Nyt trikotomian perusteella $m \in n$ tai $m = n$ tai $n \in m$. Jos olisi $m = n$, niin pätisi $n + p \in n + p$, mikä on Apulauseen 4.13(b) mukaan mahdotonta. Jos olisi $n \in m$, niin äskeisen perusteella pätisi $n + p \in m + p \in n + p$, jolloin transitiivisuuden perusteella $n + p \in n + p$, mikä on taas mahdotonta. Siis on oltava $m \in n$.

'(2) "$\Rightarrow$": Oletetaan, että $p \neq 0$ ja $m \in n$. Olkoon $B = \{ q \in \omega \mid m \cdot q^+ \in n \cdot q^+ \}$. Osoitetaan, että B on induktiivinen. Nyt $0 \in B$, sillä $m \cdot 0^+ = (m \cdot 0) + m = 0 + m = m$ ja samoin $n \cdot 0^+ = n$, joten $m \cdot 0^+ \in n \cdot 0^+$ oletuksen perusteella.

Oletetaan sitten, että $k \in B$. Tällöin $m \cdot k^{++} = m \cdot k^{+} + m$ ja $n \cdot k^{++} = n \cdot k^{+} + n$, joten riittää osoittaa, että $m \cdot k^{+} + m \in n \cdot k^{+} + n$. Tämä nähdään seuraavasti: Induktio-oletuksen ja kohdan (1) perusteella $m \cdot k^{+} + m \in n \cdot k^{+} + m$. Käyttämällä yhteenlaskun vaihdannaisuutta ja kohtaa (1) toistamiseen saadaan $n \cdot k^{+} + m = m + n \cdot k^{+} \in n + n \cdot k^{+} = n \cdot k^{+} + n$. Siis transitiivisuuden nojalla pätee $m \cdot k^{+} + m \in n \cdot k^{+} + n$. Tästä jo seuraakin, että $k^{+} \in B$.

"$\Leftarrow$": Tämä implikaatio todistetaan samalla tavalla kuin kohdassa (1). □

Seuraus 4.16 *Kaikilla $m, n, p \in \omega$ pätee:*

(1)
$$m + p = n + p \ \Rightarrow \ m = n.$$

Jos lisäksi $p \neq 0$, pätee myös:

(2)
$$m \cdot p = n \cdot p \ \Rightarrow \ m = n.$$

Todistus. (1) Jos $m + p = n + p$, niin ei ole mahdollista, että $m \in n$, koska tällöin olisi Lauseen 4.15 perusteella $m + p \in n + p$ ja siis $n + p \in n + p$. Samoin ei ole mahdollista, että $n \in m$. Siis trikotomian perusteella $m = n$.

Kohta (2) todistetaan samalla tavalla. □

Joukon A lineaarijärjestys $<$ on *hyvinjärjestys*, jos jokaisessa A:n epätyhjässä osajoukossa on pienin alkio:

$$\forall B \in \mathcal{P}(A)(B \neq \emptyset \rightarrow \exists m \in B \forall x \in B(m < x \vee m = x)).$$

Luonnollisten lukujen hyvinjärjestyslause. *Luonnollisten lukujen järjestys $\in_\omega$ on hyvinjärjestys.*

Todistus. Oletetaan, että $B \subseteq \omega$ on osajoukko, jossa ei ole pienintä alkiota. Osoitetaan, että tällöin $B = \emptyset$, eli $\omega \setminus B = \omega$.

On kuitenkin hankala todistaa suoraan, että $\omega \setminus B$ on induktiivinen. Sen sijaan määritellään $C = \{ m \in \omega \mid \neg \exists n \in m(n \in B) \}$, ja osoitetaan, että C on induktiivinen. Nyt $0 \in C$, koska ei ole olemassa $n \in 0$. Oletetaan sitten, että $k \in C$. Jos $n \in k^{+}$, niin $n \in k$ tai $n = k$. Edellisessä tapauksessa $n \notin B$, koska $k \in C$. Jälkimmäisessä tapauksessa $n \notin C$, sillä muuten $n = k$ olisi selvästi joukon B pienin alkio. Siispä $k^{+} \in C$.

Nyt voidaan päätellä, että $B = \emptyset$: jos olisi $n \in B$ jollain $n \in \omega$, niin olisi $n^{+} \notin C$, mikä on mahdotonta, koska $C = \omega$. □

Seuraus 4.17 *Ei ole olemassa funktiota $f \colon \omega \rightarrow \omega$ siten, että $f(n^{+}) \in f(n)$ kaikilla $n \in \omega$.*

Todistus. Jos tällainen funktio f olisi olemassa, niin joukolla $\{ f(n) \mid n \in \omega \} = \operatorname{ran}(f)$ ei olisi pienintä alkiota, vaikka $\operatorname{ran}(f) \neq \emptyset$. $\square$

Vahva induktioperiaate ω:lle. *Jos $A \subseteq \omega$ ja jokaiselle $n \in \omega$ pätee*

$$(\forall m \in n(m \in A)) \to n \in A, \tag{$*$}$$

niin $A = \omega$.

Todistus. Olkoon $A \subseteq \omega$ joukko, joka toteuttaa ehdon $(*)$. Tehdään vastaoletus: $A \neq \omega$. Tällöin $\omega \setminus A \neq \emptyset$. Olkoon m joukon $\omega \setminus A$ pienin alkio. Nyt $\forall p \in m(p \in A)$, joten ehdon$(*)$ perusteella $m \in A$, mikä on vastoin oletusta, että $m \in \omega \setminus A$. $\square$

Luku 5

Kardinaaliluvut

Yhtämahtavuus

Yhtämahtavuuden käsite määritellään tuttuun tapaan bijektioiden avulla.

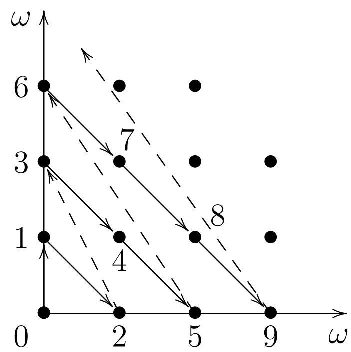
Määritelmä 5.1 Joukot A ja B ovat *yhtämahtavia*, $A \approx B$, jos on olemassa bijektio $f : A \to B$.

Esimerkki 5.1 $\omega \times \omega \approx \omega$

Eräs bijektio $J : \omega \times \omega \to \omega$ on

$$J(m, n) = \frac{1}{2}\big((m+n)^2 + 3m + n\big).$$

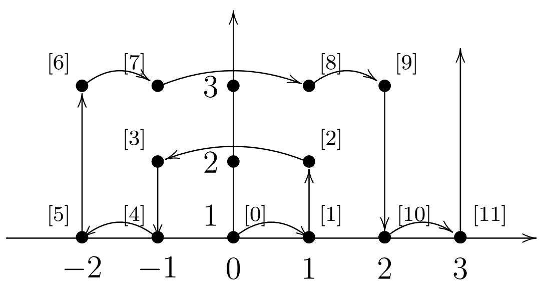
Se saadaan viereisestä kuviosta. (Huom: samalla tavalla nähdään, että $\omega^2 \approx \omega$.)



Esimerkki 5.2 $\omega \approx \mathbb{Q}$

Idea: Rationaalilukujen joukko $\mathbb{Q}$ voidaan määritellä kaikkien osamäärien r/s joukkona, missä $r \in \mathbb{Z}$ ja $s \in \mathbb{Z}$, $s > 0$. Nämä osamäärät r/s voidaan puolestaan esittää järjestettyinä pareina $\langle r, s\rangle$ tason $\mathbb{Z} \times \mathbb{Z}$ yläpuoliskossa; kukin rationaaliluku tosin esiintyy äärettömän monta kertaa, sillä $r/s = 2r/2s = 3r/3s = \cdots$. Käymällä läpi sopivassa järjestyksessä kaikki parit $\langle r, s\rangle$, ja jättämällä väliin saman rationaaliluvun toistot saadaan bijektio $\omega \to \mathbb{Q}$.

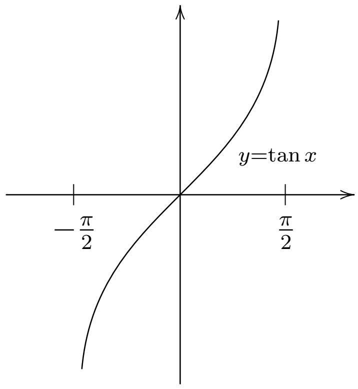
Sopiva bijektio saadaa esimerkiksi kuviosta:

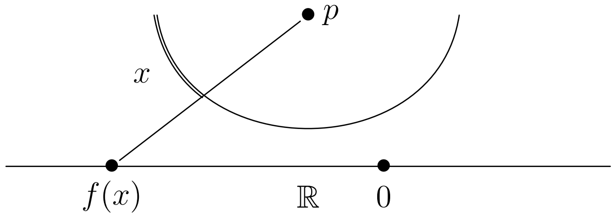


Esimerkki 5.3 $]0,1[= \{x \in \mathbb{R} \mid 0 < x < 1\} \approx \mathbb{R}$

Funktio $f :]0,1[\to \mathbb{R}$, $f(x) = tan\frac{\pi(2x-1)}{2}$ on bijektio.

Geometrinen konstruktio: puoliympyrän pituus on 1, säde on $r = \frac{1}{\pi}$.





Esimerkki 5.4 Jokaisella joukolla A pätee $\mathcal{P}(A) \approx {}^{A}2$. Tässä

$$ {}^{A}2 = \{f : A \to \{0,1\} \mid f \text{ on funktio}\}, $$

kuten Luvussa 3 määriteltiin.

Tämä nähdään seuraavasti. Olkoon $H : \mathcal{P}(A) \to {}^{A}2$ funktio, jolla $H(B) = \chi_B$, missä $\chi_B : A \to 2$ on B:n *karakteristinen* funktio eli

$$ \chi_B(x) = \begin{cases} 1, & \text{jos } x \in B \\ 0, & \text{jos } x \in A \setminus B. \end{cases} $$

Osoitetaan, että H on bijektio.

H on surjektio, koska jos $g \in {}^{A}2$, niin $g = H(\{x \in A \mid g(x) = 1\})$.

H on injektio, sillä jos $B,\ C \in \mathcal{P}(A)$ ja $B \neq C$, niin on olemassa $x \in (B \setminus C) \cup (C \setminus B)$. Tällöin $(H(B))(x) \neq (H(C))(x)$, joten $H(B) \neq H(C)$.

Lause 5.1 *Kaikilla joukoilla A, B ja C pätee:*

(a) $A \approx A$.
(b) *Jos* $A \approx B$, *niin* $B \approx A$.
(c) *Jos* $A \approx B$ *ja* $B \approx C$, *niin* $A \approx C$.

Todistus. Harjoitustehtävä. □

Huom: Relaatio $\approx$ ei kuitenkaan ole ekvivalenssirelaatio, sillä ei ole olemassa joukkoa

$$ \{\langle A, B\rangle \mid A \approx B\}. $$

Tämä on aito luokka. Samoin $\{B \mid A \approx B\}$ on aito luokka jokaisella joukolla $A \neq \emptyset$, joten relaation $\approx$ ekvivalenssiluokkia ei voi käyttää vapaasti joukkojen määritelmissä.

Seuraavaksi todistamme kaksi samankaltaista tulosta Cantorin kuuluisalla diagonaali-argumentilla.

Lause 5.2 (Cantor 1873)

(a) $\omega \not\approx \mathbb{R}$.
(b) *Jokaisella A pätee $A \not\approx \mathcal{P}(A)$.*

Todistus. (a) Olkoon $f : \omega \to \mathbb{R}$ funktio. Osoitetaan, että f ei ole surjektio.

Aloitetaan listaamalla reaalilukujen $f(0), f(1), f(2), \ldots$ desimaalikehitelmät:

$$
\begin{array}{rccccccc}
f(0) = & m_0, & \boxed{a_{0,0}} & a_{0,1} & a_{0,2} & a_{0,3} & \cdots \\
f(1) = & m_1, & a_{1,0} & \boxed{a_{1,1}} & a_{1,2} & a_{1,3} & \\
f(2) = & m_2, & a_{2,0} & a_{2,1} & \boxed{a_{2,2}} & a_{2,3} & \\
f(3) = & m_3, & a_{3,0} & a_{3,1} & a_{3,2} & \boxed{a_{3,3}} & \\
\vdots & & & & & & \ddots
\end{array}
$$

Listassa m_i on $f(i)$:n kokonaisosa ($m_i \in \mathbb{Z}$) ja $a_{i,j}$ on $f(i)$:n $j+1$:s desimaali ($a_{i,j} \in \{0, 1, 2, \ldots, 9\}$).

Muodostetaan taulukon diagonaalin avulla uusi reaaliluku z:

$$z = 0, b_0 b_1 b_2 \ldots, \quad \text{missä } b_i = \begin{cases} 7, & \text{jos } a_{i,i} \neq 7 \\ 6, & \text{jos } a_{i,i} = 7 \end{cases}$$

Nyt $z \neq f(i)$, koska z:n $(i+1)$:s desimaali on eri kuin $f(i)$:n $(i+1)$:s desimaali: $b_i \neq a_{i,i}$. Siis $z \notin \mathrm{ran}(f)$, joten f ei ole surjektio.

(b) Olkoon $g : A \to \mathcal{P}(A)$ funktio. Osoitetaan, että g ei ole surjektio.

Konstruoidaan osajoukko $B \subseteq A$, jolla $g(x) \neq B$ jokaisella $x \in A$:

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

Nyt jokaisella $x \in A$ pätee

$$x \in B \iff x \notin g(x),$$

joten ei ole olemassa $x \in A$, jolla $B = g(x)$. Koska kuitenkin $B \in \mathcal{P}(A)$, g ei ole surjektio. $\square$

Äärelliset joukot

Intuitiivisesti joukko on äärellinen, jos sen alkioiden lukumäärä on luonnollinen luku. Tehdään tästä täsmällinen määritelmä:

Määritelmä 5.2 Joukko A on *äärellinen*, jos $A \approx n$ jollain $n \in \omega$ Muutoin A on *ääretön.*

Lokeroperiaate. *Mikään $n \in \omega$ ei ole yhtämahtava aidon osajoukkonsa kanssa.*

Todistus. Olkoon funktio $f : n \to n$ injektio. Riittää osoittaa, että tällöin $\operatorname{ran}(f) = n$. Tehdään tämä induktiolla.

Olkoon

$$T = \{n \in \omega \mid \forall f : n \to n \ (f \text{ on injektio} \Rightarrow f \text{ on surjektio})\}$$

Tällöin $0 \in T$, sillä ainoa injektio $f : 0 \to 0$ on $f = \emptyset$ ja $\operatorname{ran}(\emptyset) = \emptyset = 0$.

Oletetaan sitten, että $k \in T$. Olkoon $f : k^+ \to k^+$ injektio. Nyt $f \restriction k$ on myös injektio. On kaksi mahdollisuutta:

(1) $f \restriction k$ on injektio $k \to k$. Koska $k \in T$, on $\operatorname{ran}(f \restriction k) = k$. Koska f on injektio, on tällöin oltava $f(k) = k$. Muttä tällöin myös $k \in \operatorname{ran}(f)$, joten f on surjektio.

(2) On olemassa $p \in k$ s.e. $f(p) = k$. Palautetaan tilanne tapaukseen (1) määrittelemällä funktio $\hat{f} : k^+ \to k^+$ asettamalla

$$\begin{aligned} \hat{f}(p) &= f(k) \\ \hat{f}(k) &= k \\ \hat{f}(x) &= f(x), \text{ kun } x \in k^+ \text{ ja } x \neq p, k. \end{aligned}$$

Selvästi $\hat{f}$ on injektio $k^+ \to k^+$ ja tapauksen (1) perusteella $\hat{f}$ on surjektio. Toisaalta $\operatorname{ran}(\hat{f}) = \operatorname{ran}(f)$, joten myös f on surjektio. Siis $k^+ \in T$.

Täten T on induktiivinen. $\square$

Seuraus 5.3 *Mikään äärellinen joukko ei ole yhtämahtava aidon osajoukkonsa kanssa.*

Todistus. Oletetaan, että joukko A on äärellinen, $B \subseteq A$ sekä $g : A \to B$ on bijektio. Osoitetaan, että $A = B$.

Koska A on äärellinen, jollain $n \in \omega$ on olemassa bijektio $f : A \to n$. Nyt koska f ja g ovat bijektioita, myös $f \circ g \circ f^{-1} : n \to f[\![B]\!]$ on bijektio. Täten lokeroperiaatteen nojalla $f[\![B]\!] = n$. Tästä seuraa edelleen, että $A = B$. $\square$

Seuraus 5.4

(a) *Jos A on yhtämahtava aidon osajoukkonsa kanssa, A on ääretön.*

(b) *ω on ääretön.*

Todistus. Kohta (a) seuraa suoraan seurauksesta 5.3. Kohta (b) voidaan todeta määrittelemällä funktio $f : \omega \to \omega \setminus \{0\}$ se. $f : n \mapsto n^+$. f on bijektio, joten $\omega \approx \omega \setminus \{0\}$. Nyt (a)-kohdan perusteella ω on ääretön. □

Seuraus 5.5 *Jokaisella äärellisellä joukolla A, on olemassa yksikäsitteinen $n \in \omega$, jolla $A \approx n$.*

Todistus. Olkoon $A \approx m$ ja $A \approx n$. Tällöin $m \approx n$. Trikotomian perusteella $m = n$, $m \subset n$ tai $n \subset m$. Lokeroperiaatteen nojalla kaksi viimeistä vaihtoehtoa ovat mahdottomia, joten $m = n$. □

Mahtavuus eli kardinaali(luku): Jos $A \approx n$, kun $n \in \omega$, merkitään

$$\operatorname{card}(A) = n \qquad \text{tai} \qquad |A| = n.$$

Tämä ei luonnollisestikaan sovellu äärettömille joukoille. Myöhemmin määritellläänkin jokaiselle äärettömälle joukolle A sen mahtavuus $\operatorname{card}(A)$, joka on sellainen joukko, jolla pätee ehdot

$$\begin{aligned} &\operatorname{card}(A) = \operatorname{card}(B) \;\Leftrightarrow\; A \approx B \;\text{ ja} \\ &\operatorname{card}(A) \approx A. \end{aligned}$$

Erityisesti luonnollisten lukujen joukon mahtavuudelle käytetään seuraavaa merkintää:

$$\operatorname{card}(\omega) = \aleph_0 \quad \text{(heprealaisen aakkoston alef)}$$

Kardinaalilukuja merkitään kirjaimilla κ, λ, μ, ν. Lisäksi merkitään

$$K_\kappa = \{X \mid \operatorname{card}(X) = \kappa\}.$$

K_κ on aito luokka, jos $\kappa \neq 0$. Kun $\kappa = 0$, $K_0 = \{\emptyset\}$.

Apulause 5.6 *Jos $C \subset n$, kun $n \in \omega$, niin on olemassa $m \in n$, jolla $C \approx m$.*

Todistus. Olkoon

$$T = \{n \in \omega \mid \text{jokaisella } C \subset n \text{ on olemassa } m \in n \text{ s.e. } C \approx m\}.$$

Osoitetaan, että T on induktiivinen: Ensinnäkin $0 \in T$, sillä 0:lla ei ole aitoja osajoukkoja. Oletetaan sitten, että $k \in T$. Olkoon $C \subset k^+$. Tällöin on kolme vaihtoehtoa:

(1) $C = k$. Tällöin $C \approx k \in k^+$.

(2) $C \subset k$. Koska $k \in T$, on olemassa $m \in k$ s.e. $C \approx m$. Nyt $m \in k \subseteq k^+$, joten $m \in k^+$.

(3) $k \in C$. Tällöin $C = (C \cap k) \cup \{k\}$ ja $C \cap k \subset k$. Koska $k \in T$, on olemassa $m \in k$ s.e. $C \cap k \approx m$. Siis on olemassa bijektio $f : C \cap k \to m$. Tällöin $f \cup \{\langle k, m\rangle\}$ on bijektio $C \to m^+$. Siis $C \approx m^+$. Koska $m \in k$, on $m^+ \in k^+$.

Kaikissa tapauksissa voidaan päätellä, että $k^+ \in T$. $\square$

Seuraus 5.7 *Jos A on äärellinen ja $B \subseteq A$, niin B on äärellinen.*

Todistus. Olkoot $B \subseteq A$ ja $f : A \to n$, $n \in \omega$ bijektio. Tällöin $B \approx f[\![B]\!] \subseteq n$, joten apulauseen 5.6 perusteella on olemasssa $m \in n$ s.e. $B \approx m$. $\square$

Kardinaalilukujen aritmetiikkaa

Yhteen- ja kertolaskun intuitio:

- Luvut ovat mahtavuuksia.
- Summa on erillisen yhdisteen mahtavuus.
- Tulo on karteesisen tulon mahtavuus.

Määritelmä 5.3 Olkoot κ ja λ kardinaalilukuja.

(a) $\kappa + \lambda = \mathrm{card}(K \cup L)$, missä $\mathrm{card}(K) = \kappa$, $\mathrm{card}(L) = \lambda$ ja $K \cap L = \emptyset$.
(b) $\kappa \cdot \lambda = \mathrm{card}(K \times L)$, missä $\mathrm{card}(K) = \kappa$ ja $\mathrm{card}(L) = \lambda$.
(c) $\kappa^\lambda = \mathrm{card}({}^L K)$, missä $\mathrm{card}(K) = \kappa$ ja $\mathrm{card}(L) = \lambda$.

Huom: (a)-kohdassa tarvittavat erilliset joukot K ja L voidaan aina löytää: Jos $K \cap L \neq \emptyset$, niin siirrytään tarkastelemaan joukkoja $K \times \{0\}$ ja $L \times \{1\}$. Selvästi $K \times \{0\} \cap L \times \{1\} = \emptyset$ ja $K \times \{0\} \approx K$ ja $L \times \{1\} \approx L$.

Ylläolevassa määritelmässä $\kappa + \lambda$, $\kappa \cdot \lambda$ ja κ^λ kiinnitetään valitsemalla jotkin joukot K ja L, joiden mahtavuudet ovat κ ja λ. Vielä pitää osoittaa, että tulokset eivät riipu joukkojen K ja L valinnasta:

Lause 5.8 *Oletetaan, että $K_1 \approx K_2$ ja $L_1 \approx L_2$. Tällöin*

(a) *jos $K_1 \cap L_1 = \emptyset$ ja $K_2 \cap L_2 = \emptyset$, niin $K_1 \cup L_1 \approx K_2 \cup L_2$*
(b) $K_1 \times L_1 \approx K_2 \times L_2$
(c) ${}^{L_1}K_1 \approx {}^{L_2}K_2$.

Todistus. Olkoot $f : K_1 \to K_2$ ja $g : L_1 \to L_2$ bijektioita.

Kohta (a) seuraa siitä, että $f \cup g : K_1 \cup L_1 \to K_2 \cup L_2$ on bijektio.

(b) Olkoon $h : K_1 \times L_1 \to K_2 \times L_2$ funktio, joka saadaan asettamalla $h(\langle x, y\rangle) = \langle f(x), g(x)\rangle$. On suoraviivaista osoittaa, että h on bijektio.

(c) Määritellään $H : {}^{L_1}K_1 \to {}^{L_2}K_2$ asettamalla

$$H(j) = f \circ j \circ g^{-1} \ \text{ kaikilla } j \in {}^{L_1}K_1.$$

Osoitetaan sitten, että H on bijektio.

H on injektio: Jos $j, j' \in {}^{L_1}K_1$ ja $j \neq j'$, niin on olemassa $t \in L_1$, jolla $j(t) \neq j'(t)$. Tällöin $f(j(t)) \neq f(j'(t))$ koska f on injektio. Siispä

$$H(j)(g(t)) = f(j(t)) \neq f(j'(t)) = H(j')(g(t)),$$

joten $H(j) \neq H(j')$.

H on surjektio: Jos $d \in {}^{L_2}K_2$, niin $d = H(j)$, missä $j = f^{-1} \circ d \circ g$, sillä $H(f^{-1} \circ d \circ g) = d$. □

Esimerkki 5.5

(1) $2 + 2 = 4$

(2) $m \cdot n = \operatorname{card}(m \times n)$ ja $m^n = \operatorname{card}({}^n m)$ kaikilla $m, n \in \omega$

(3) Kaikilla $n \in \omega$ pätee:

$$\begin{aligned} n + \aleph_0 &= \aleph_0, \\ n \cdot \aleph_0 &= \aleph_0, \qquad \text{kun } n \neq 0. \\ \big(0 \cdot \aleph_0 &= \operatorname{card}(\emptyset \times \omega) = 0\big) \end{aligned}$$

Edelleen

$$\begin{aligned} \aleph_0 + \aleph_0 &= \aleph_0 \qquad \big(\omega \times \{0\} \cup \omega \times \{1\} \approx \omega\big) \\ \aleph_0 \cdot \aleph_0 &= \aleph_0. \qquad \big(\omega \times \omega \approx \omega\big) \end{aligned}$$

(4) Kaikilla kardinaaliluvuilla κ pätee:

$$\kappa + 0 = \kappa, \qquad \kappa \cdot 0 = 0, \qquad \kappa \cdot 1 = \kappa.$$

(5) Jokaisella kardinaaliluvulla κ pätee myös

$$\begin{aligned} &\kappa^0 = 1 && && \big({}^{\emptyset}K = \{\emptyset\}\big). \\ &0^\kappa = 0, && \text{kun } \kappa \neq 0 && \big({}^{K}\emptyset = \emptyset, \text{ jos } K \neq \emptyset\big) \\ &0^0 = 1 \end{aligned}$$

(6) Koska $\mathcal{P}(A) \approx {}^A 2$, kaikilla joukoilla A pätee $\operatorname{card}(\mathcal{P}(A)) = 2^{\operatorname{card}(A)}$. Erityisesti $\operatorname{card}(\mathcal{P}(\omega)) = 2^{\aleph_0}$.

(7) Cantorin lauseen 5.2 perusteella kaikilla kardinaaliluvuilla κ,

$$\kappa \neq 2^\kappa \qquad \big(\text{erityisesti } \aleph_0 \neq 2^{\aleph_0}\big).$$

(8) Kaikilla kardinaaliluvuilla κ on voimassa

$$\kappa + \kappa = 2 \cdot \kappa \qquad \big(A \times \{0\} \cup A \times \{1\} = A \times 2 \approx 2 \times A\big).$$

Todistamme seuraavaksi, että kardinaalilukujen laskutoimitukset toteuttavat suuren osan tavallisista laskusäännöistä.

Lause 5.9 *Kaikilla kardinaaliluvuilla κ, λ ja μ on voimassa*

(1) $\kappa + \lambda = \lambda + \kappa$ *ja* $\kappa \cdot \lambda = \lambda \cdot \kappa$
(2) $\kappa + (\lambda + \mu) = (\kappa + \lambda) + \mu$ *ja* $\kappa \cdot (\lambda \cdot \mu) = (\kappa \cdot \lambda) \cdot \mu$
(3) $\kappa \cdot (\lambda + \mu) = \kappa \cdot \lambda + \kappa \cdot \mu$
(4) $\kappa^{\lambda+\mu} = \kappa^{\lambda} \cdot \kappa^{\mu}$
(5) $(\kappa \cdot \lambda)^{\mu} = \kappa^{\mu} \cdot \kappa^{\mu}$
(6) $(\kappa^{\lambda})^{\mu} = \kappa^{\lambda \cdot \mu}$

Todistus. Olkoot K, L ja M joukkoja, joilla $\mathrm{card}(K) = \kappa$, $\mathrm{card}(L) = \lambda$ ja $\mathrm{card}(M) = \mu$. Oletetaan lisäksi, että $K \cap L = K \cap M = L \cap M = \emptyset$.

Kohdat (1)–(6) palautuvat seuraaviin yhtämahtavuuksiin:

(1) $K \cup L \approx L \cup K$ ja $K \times L \approx L \times K$
(2) $K \cup (L \cup M) \approx (K \cup L) \cup M$ ja $K \times (L \times M) \approx (K \times L) \times M$
(3) $K \times (L \cup M) \approx K \times L \cup K \times M$
(4) ${}^{L \cup M}K \approx {}^{L}K \times {}^{M}K$
(5) ${}^{M}(K \times L) \approx {}^{M}K \times {}^{M}L$
(6) ${}^{M}({}^{L}K) \approx {}^{L \times M}K$

Kohtien (1)–(5) todistukset jätetään harjoitustehtäviksi.

Kohta (6): Joukon ${}^{M}({}^{L}K)$ alkiot ovat funktioita $f : M \to {}^{L}K$, joten

$$\begin{aligned} f(m) &\in {}^{L}K \quad \text{kullakin } m \in M \\ (f(m))(l) &\in K \quad \text{kullakin } l \in L. \end{aligned}$$

Joukon ${}^{L \times M}K$ alkiot ovat funktioita $g : L \times M \to K$

$$\underbrace{g(\langle l, m \rangle)}_{\text{merk. } g(l,m)} \in K.$$

Määritellään funktio $H : {}^{M}({}^{L}K) \to {}^{(L \times M)}K$ asettamalla

$$H(f) = g \quad \text{jokaisella } f \in {}^{M}({}^{L}K),$$

missä $g \in {}^{(L \times M)}K$ on se funktio, jolla jokaisella $m \in M$ ja $l \in L$ pätee

$$g(l, m) = (f(m))(l).$$

Osoitetaan sitten, että H on bijektio.

H on injektio: Jos $f, f' \in {}^M({}^L K)$ ja $f \neq f'$, niin on olemassa $m \in M$ s.e. $f(m) \neq f'(m)$. Tällöin on olemassa myös $l \in L$ s.e. $(f(m))(l) \neq (f'(m))(l)$. Siis $H(f)(l, m) \neq H(f')(l, m)$ eli $H(f) \neq H(f')$.

H on surjektio: Jos $g \in {}^{(L \times M)}K$, niin $g = H(f)$, missä $f \in {}^M({}^L K)$ on funktio, jolla $(f(m))(l) = g(l, m)$ kaikilla $l \in L$ ja $m \in M$. $\square$

Luvussa 4 määriteltiin luonnollisten lukujen yhteenlasku, kertolasku ja eksponenttifunktio rekursiolla. Toisaalta edellä määriteltiin kardinaaliluvuille samat laskutoimitukset, jotka siis erityisesti koskevat myös luonnollisia lukuja. Osoitetaan seuraavaksi, että tämä ei johda ongelmiin:

Lause 5.10 *Olkoot m ja n äärellisiä kardinaaleja (eli $m, n \in \omega$). Tällöin*

$$\begin{aligned} m + n &= m +_\omega n \\ m \cdot n &= m \cdot_\omega n \\ m^n &= m {\uparrow}_\omega n, \end{aligned}$$

missä vasemmat puolet viittaavat kardinaaliaritmetiikan operaatioihin ja oikeat puolet rekursiivisesti määriteltyihin luonnollisten lukujen operaatioihin.

Todistus. Todistetaan lause induktiolla. Todetaan ensin, että kaikilla kardinaaliluvuilla κ ja λ on voimassa seuraavat yhtälöt:

(a1) $\kappa + 0 = \kappa$

(a2) $\kappa + (\lambda + 1) = (\kappa + \lambda) + 1$

(m1) $\kappa \cdot 0 = 0$

(m2) $\kappa \cdot (\lambda + 1) = \kappa \cdot \lambda + \kappa$

(e1) $\kappa^0 = 1$

(e2) $\kappa^{\lambda+1} = \kappa^\lambda \cdot \kappa$

Näiden yhtälöiden todistukset ovat triviaaleja tai seuraavat suoraan lauseesta 5.9.

Lisäksi jokaisella $n \in \omega$ pätee $n + 1 = n^+ = \mathrm{card}(n^+) = \mathrm{card}(n \cup \{n\})$.

Olkoot $m \in \omega$ ja

$$T = \{n \in \omega \mid m + n = m +_\omega n\}.$$

Osoitetaan, että joukko T on induktiivinen: Ensinnäkin $0 \in T$, koska kohdan (a1) perusteella $m + 0 = m$ ja yhteenlaskun ehdon (A1) mukaan $m +_\omega 0 = m$.

Oletetaan sitten, että $k \in T$. Tällöin

$$\begin{aligned} m + k^+ &= m + (k + 1) \\ &\overset{a2}{=} (m + k) + 1 \\ &\overset{k \in T}{=} (m +_\omega k) + 1 \\ &= (m +_\omega k)^+ \\ &= m +_\omega k^+. \end{aligned}$$

Siis $k^+ \in T$. Täten T on induktiivinen.

Muut kohdat todistetaan samoin. $\square$

Seuraus 5.11 *Jos A ja B ovat äärellisiä, niin $A \cup B$, $A \times B$ ja ${}^BA$ ovat äärellisiä.*

Todistus. Olkoot $\operatorname{card}(A) = m$ ja $\operatorname{card}(B) = n$, missä $m, n \in \omega$. Tällöin $\operatorname{card}(A \times B) = m \cdot n = m \cdot_\omega n \in \omega$ ja $\operatorname{card}({}^BA) = m^n = m{\uparrow_\omega}n \in \omega$.

Yhdisteen tapaus todetaan seuraavasti: $A \cup B = A \cup (B \setminus A)$, joten

$$\operatorname{card}(A \cup B) = m + \operatorname{card}(B \setminus A) = m +_\omega p \in \omega,$$

missä $p = \operatorname{card}(B \setminus A) \leq n$. $\square$

Kardinaalilukujen järjestys

Määritelmä 5.4 A on *korkeintaan yhtämahtava* kuin B, $A \preccurlyeq B$, jos on olemassa injektio $f : A \to B$.

Huom: Jos $f : A \to B$ on injektio, niin $f : A \to \operatorname{ran}(f)$ on bijektio, joten $A \approx \operatorname{ran}(f) \subseteq B$. Siispä $A \preccurlyeq B$ jos ja vain jos on olemassa $C \subseteq B$, jolla $A \approx C$.

Määritelmä 5.5 Olkoot κ ja λ kardinaalilukuja. Tällöin $\kappa \leq \lambda$, jos on olemassa joukot K ja L, joilla $\operatorname{card}(K) = \kappa$, $\operatorname{card}(L) = \lambda$ ja $K \preccurlyeq L$.

Kardinaalilukujen κ ja λ järjestys on siis määritelty viittaamalla joukkoihin K ja L, joiden mahtavuuksia ne ovat. Taas on todistettava, että järjestys on hyvin määritelty, eli se ei riipu valituista joukoista.

Lause 5.12 *Olkoot K, K', L ja L' joukkoja, joilla $K \approx K'$ ja $L \approx L'$. Tällöin*

$$K \preccurlyeq L \iff K' \preccurlyeq L'.$$

Todistus. Olkoon $f : K \to K'$ ja $g : L \to L'$ bijektioita.

Jos $h : K \to L$ on injektio, niin myös $g \circ h \circ f^{-1} : K' \to L'$ on myös injektio. Siis $K \preccurlyeq L \Rightarrow K' \preccurlyeq L'$.

Implikaatio oikealta vasemmalle todistetaan vastaavasti. $\square$

Kardinaalilukujen tiukka järjestys määritellään tavalliseen tapaan: $\kappa < \lambda$, jos $\kappa \leq \lambda$ ja $\kappa \neq \lambda$. Toisin sanoen $\operatorname{card}(K) < \operatorname{card}(L)$ jos ja vain jos $K \preccurlyeq L$ ja $K \not\approx L$.

On helppo todeta, että $\kappa \leq \lambda$ jos ja vain jos $\kappa < \lambda$ tai $\kappa = \lambda$.

Esimerkki 5.6

(1) Jos $A \subseteq B$, niin $\mathrm{card}(A) \leq \mathrm{card}(B)$. Aina kun $\kappa \leq \lambda$, niin on olemassa joukot K ja L, joilla $\mathrm{card}(K) = \kappa$, $\mathrm{card}(L) = \lambda$ ja $K \subseteq L$.

(2) Kaikilla kardinaaleilla κ on voimassa $0 \leq \kappa$.

(3) Kaikilla äärellisillä kardinaaleilla n pätee $n < \aleph_0$. Edelleen äärellisten kardinaalilukujen järjestys on sama kuin luonnollisten lukujen järjestys $\leq_\omega$: kaikilla $m, n \in \omega$ pätee

$$m \leq_\omega n \;\Leftrightarrow\; m \leq n.$$

(4) Jokaisella kardinaaliluvulla κ on voimassa $\kappa < 2^\kappa$. Nimittäin Cantorin lauseen 5.2 nojalla $\kappa \neq 2^\kappa$. Toisaalta funktio $f : A \to \mathcal{P}(A)$, $f(x) = \{x\}$ on injektio, joten $A \preccurlyeq \mathcal{P}(A) \approx {}^{A}2$, eli $\kappa \leq 2^\kappa$, missä $\mathrm{card}(A) = \kappa$.

Seuraavaksi halutaan osoittaa, että $\leq$ on järjestysrelaatio kardinaalien luokassa. Tätä varten on todistettava seuraavat asiat:

Kaikilla kardinaaleilla κ, λ ja μ on voimassa

(1) $\kappa \leq \kappa$ (refleksiivisyys),
(2) $\kappa \leq \lambda \wedge \lambda \leq \mu \;\Rightarrow\; \kappa \leq \mu$ (transitiivisuus),
(3) $\kappa \leq \lambda \wedge \lambda \leq \kappa \;\Rightarrow\; \kappa = \lambda$ (antisymmetrisyys),
(4) joko $\kappa \leq \lambda$ tai $\lambda \leq \kappa$ (vertailullisuus).

Ehto (1) on triviaalisti voimassa, sillä määritelmän perusteella jokaisella A pätee $A \preccurlyeq A$.

Ehto (2) todistetaan seuraavasti: Jos $f : A \to B$ ja $g : B \to C$ ovat injektioita, niin myös $g \circ f : A \to C$ on injektio. Siis jos $A \preccurlyeq B$ ja $B \preccurlyeq C$, niin $A \preccurlyeq C$.

Ehto (4) vaatii oman aksioomansa (ks. valinta-aksiooman viides muotoilu Lauseessa 5.14).

Ehto (3) puolestaan tunnetaan nimellä *Schröderin ja Bernsteinin lause*:

Schröderin–Bernsteinin lause.

(a) *Jos $A \preccurlyeq B$ ja $B \preccurlyeq A$, niin $A \approx B$.*
(b) *Kaikilla kardinaaleilla κ ja λ, jos $\kappa \leq \lambda$ ja $\lambda \leq \kappa$, niin $\kappa = \lambda$.*

Todistus. Todistetaan kohta (a); lauseen kohta (b) on sen välitön seuraus.

Olkoot A ja B joukkoja ja $f : A \to B$ ja $g : B \to A$ injektioita. Tarkoitus on muodostaa näiden avulla bijektio $h : A \to B$.

Määritellään ensin rekursiolla joukot C_n, $n \in \omega$:

$$\begin{cases} C_0 = A \setminus \mathrm{ran}(g) \\ C_{n+} = g[\![f[\![C_n]\!]]\!] \end{cases}$$

Nyt voidaan määritellä funktio $h : A \to B$ asettamalla

$$h(x) = \begin{cases} f(x), & \text{jos } x \in \bigcup_{n\in\omega} C_n \\ g^{-1}(x), & \text{jos } x \notin \bigcup_{n\in\omega} C_n \end{cases}$$

Osoitetaan seuraavaksi, että h on injektio. Oletetaan, että $x, x' \in A$ ja $x \neq x'$. Tällöin on neljä tapausta sen mukaan ovatko x ja x' joukossa $\bigcup_{n\in\omega} C_n$ vai eivät:

- Jos $x, x' \in \bigcup_{n\in\omega} C_n$, niin $h(x) = f(x) \neq f(x') = h(x')$, sillä f on injektio.
- Jos $x, x' \notin \bigcup_{n\in\omega} C_n$, niin $h(x) = g^{-1}(x) \neq g^{-1}(x') = h(x')$, sillä g^{-1} on injektio.
- Jos $x \in \bigcup_{n\in\omega} C_n$ ja $x' \notin \bigcup_{n\in\omega} C_n$, niin $x \in C_m$, jollain $m \in \omega$, jolloin $h(x) = f(x) \in f[\![C_m]\!]$. Toisaalta $h(x') = g^{-1}(x') \notin f[\![C_m]\!]$, koska muuten olisi $x' \in g[\![f[\![C_m]\!]]\!] = C_{m+1}$.
- Tapaus $x \notin \bigcup_{n\in\omega} C_n$ ja $x' \in \bigcup_{n\in\omega} C_n$ menee samoin kuin edellinen.

Todistetaan lopuksi, että h on surjektio. Oletetaan, että $y \in B$. Jos $y = f(x)$ jollain $x \in \bigcup_{n\in\omega} C_n$, niin $y = h(x)$, joten $y \in \text{ran}(h)$. Oletetaan sitten, että tällaista x ei ole olemassa. Todistetaan induktiolla, että tällöin $g(y) \notin C_n$ kaikilla $n \in \omega$. Olkoon siis $T = \{n \in \omega \mid g(y) \notin C_n\}$.

- Ensinnäkin $g(y) \notin C_0 = A \setminus \text{ran}(g)$, joten $0 \in T$.
- Oletetaan sitten, että $n \in T$. Koska $y \notin f[\![C_n]\!]$, pätee myös $g(y) \notin C_{n^+} = g[\![f[\![C_n]\!]]\!]$.

Siis $g(y) \in A \setminus \bigcup_{n\in\omega} C_n$, joten $h(g(y)) = g^{-1}(g(y)) = y$, josta nähdään, että $y \in \text{ran}(h)$. $\square$

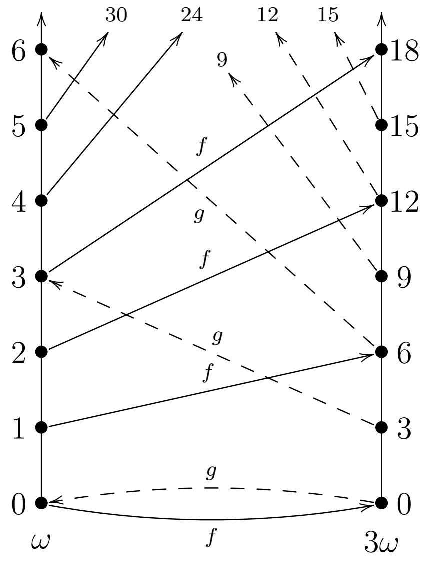
Esimerkki 5.7 Valaistaan Schröderin ja Bernsteinin lauseen todistusta konkreettisella esimerkillä. Olkoon 3ω kaikkien 3:lla jaolisten luonnollisten lukujen joukko: $3\omega = \{3 \cdot m \mid m \in \omega\}$. Selvästi 3ω ja ω ovat yhtämahtavia: funktio $l : \omega \to 3\omega$, $l(n) = 3 \cdot n$, on bijektio.

Toisaalta, jos annetaan mitkä hyvänsä injektiot $f : \omega \to 3\omega$ ja $g : 3\omega \to \omega$, niin edelläolevan todistuksen mukaisesti voidaan muodostaa bijektio $h : \omega \to 3\omega$, jolla pätee $h \subseteq f \cup g^{-1}$. Bijektio h määritellään niin, että $h(x) = g^{-1}(x)$ aina kun se on mahdollista; muussa tapauksessa asetetaan $h(x) = f(x)$.

Tarkastellaan tässä esimerkissä injektioita:

$$\begin{aligned} f &: \omega \to 3\omega, & f(n) &= 6n \\ g &: 3\omega \to \omega, & g(n) &= n \end{aligned}$$

Määritellään siis $h : \omega \to 3\omega$ niin, että $h(x) = g^{-1}(x)$ aina kun mahdollista. Heti aluksi voidaan asettaa $h(0) = g^{-1}(0) = 0$. Kun $x = 1$, tämä ei kuitenkaan ole mahdollista, sillä $1 \notin \operatorname{ran}(g)$. Siksi täytyy asettaa $h(1) = f(1) = 6$. Samoin on pakko asettaa $h(2) = f(2) = 12$. Sen sijaan $3 \in \operatorname{ran}(g)$ ja voidaan asettaa $h(3) = g^{-1}(3) = 3$. Seuraavaksi luvuilla 4 ja 5 pitää määritellä $h(4) = f(4) = 24$ ja $h(5) = f(5) = 30$, koska $4, 5 \notin \operatorname{ran}(g)$. Tämän jälkeen on pakko asettaa $h(6) = f(6) = 36$, sillä arvo $g^{-1}(6) = 6$ on jo varattu: $h(1) = 6$. Samoin $h(12) = f(12) = 72$, koska $h(2) = f(2) = 12$ on jo varattu.



Tämä johtaa äärettömään prosessiin. Joissakin vaiheissa on pakko asettaa $h(x) = f(x)$, koska $x \notin \operatorname{ran}(g)$ tai koska $g^{-1}(x)$ on jo annettu jonkin toisen luvun $y < x$ kuvaksi.

Seuraavassa esimerkissä on joitakin Schröderin ja Bernsteinin lauseen sovelluksia.

Esimerkki 5.8

(a) Jos $A \subseteq B \subseteq C$ ja $A \approx C$, niin $A \approx B \approx C$. Nimittäin jos $\kappa = \operatorname{card}(A) = \operatorname{card}(C)$ ja $\lambda = \operatorname{card}(B)$, niin tällöin $\kappa \le \lambda \wedge \lambda \le \kappa$, joten $\kappa = \lambda$

(b) Koska $]0,1[\subseteq [0,1] \subseteq \mathbb{R}$ ja tunnetusti $]0,1[\approx \mathbb{R}$ (ks. Esimerkki 5.3), pätee kohdan (a) perusteella $[0,1] \approx]0,1[$ ja $[0,1] \approx \mathbb{R}$.

(c) On suoraviivaista osoittaa, että transitiivisuudesta pätee myös seuraava vahvempi versio:

$$\kappa \le \lambda < \mu \ \Rightarrow \kappa < \mu$$
$$\kappa < \lambda \le \mu \ \Rightarrow \kappa < \mu$$

(d) Osoitetaan seuraavaksi, että $\mathbb{R} \approx {}^{\omega}2$, ja siten myös $\mathbb{R} \approx \mathcal{P}(\omega)$. Riittää osoittaa, että $\mathbb{R} \preccurlyeq {}^{\omega}2$ ja ${}^{\omega}2 \preccurlyeq \mathbb{R}$. Koska $]0,1[\approx \mathbb{R}$, voidaan ensimmäinen vertailu todistaa määrittelemällä injektio $H :]0,1[\to {}^{\omega}2$.
Esitetään tätä varten välin $]0,1[$ reaaliluvut binaarikehitelminä

$$x = 0, x_1x_2x_3x_4\ldots,$$

missä $x_j = 0$ tai $x_j = 1$. Asetetaan

$$(H(x))(n) = x_n.$$

Funktio H on injektio, sillä jos $H(x) = H(y)$, niin $x_n = y_n$ jokaisela $n \in \omega$, jolloin $x = y$.
Toisaalta funktio $F : {}^{\omega}2 \to \mathbb{R}$, jolla $F(g) = \underbrace{g(0), g(1)g(2)g(3)\ldots}_{\text{desimaaliluku}}$, on selvästi injektio.

(e) Edellisen kohdan perusteella $\text{card}(\mathbb{R}) = \text{card}({}^{\omega}2) = 2^{\aleph_0}$. Edelleen joukon $\mathbb{R} \times \mathbb{R}$ mahtavuus voidaan laskea seuraavasti:

$$\text{card}(\mathbb{R} \times \mathbb{R}) = 2^{\aleph_0} \cdot 2^{\aleph_0} = 2^{\aleph_0 + \aleph_0} = 2^{\aleph_0}.$$

Kardinaalilukjen järjestykselle ja laskutoimituksille on voimassa tutut yhteensopivuussäännöt:

Lause 5.13 *Olkoon κ, λ ja μ kardinaaleja.*

(a) $\kappa \leq \lambda \Rightarrow \kappa + \mu \leq \lambda + \mu$
(b) $\kappa \leq \lambda \Rightarrow \kappa \cdot \mu \leq \lambda \cdot \mu$
(c) $\kappa \leq \lambda \Rightarrow \kappa^{\mu} \leq \lambda^{\mu}$
(d) $\kappa \leq \lambda \Rightarrow \mu^{\kappa} \leq \mu^{\lambda}$, *paitsi jos* $\kappa = \mu = 0$ *ja* $\lambda \neq 0$

Todistus. Olkoot K, L ja M joukot, joilla $\text{card}(K) = \kappa$, $\text{card}(L) = \lambda$ ja $\text{card}(M) = \mu$. Oletetaan lisäksi, että $K \subseteq L$ ja että $L \cap M = \emptyset$. (Tällöin myös $K \cap M = \emptyset$.)

Kohdat (a), (b) ja (c) seuraavat välittömästi siitä, että

$$K \cup M \subseteq L \cup M, \quad K \times M \subseteq L \times M, \quad \text{ja} \quad {}^{M}K \subseteq {}^{M}L.$$

(d) Oletetaan ensin, että $\mu = 0$. Tällöin oletuksen mukaan $\kappa \neq 0$ tai $\lambda = 0$, joten $\mu^{\kappa} = 0 \leq \mu^{\lambda}$ tai $\mu^{\kappa} \leq 1 = \mu^{\lambda}$.

Oletetaan sitten, että $\mu \neq 0$ eli $M \neq \emptyset$. Olkoon $a \in M$. Määritellään kullakin $f : K \to M$ funktio $G(f) : L \to M$ asettamalla

$$(G(f))(x) = \begin{cases} f(x), & \text{jos } x \in K \\ a, & \text{jos } x \in L \setminus K \end{cases}$$

Tällöin on suoraviivaista todeta, että $G : {}^{K}M \to {}^{L}M$ on bijektio. □

Esimerkki 5.9 Mitä on $\aleph_0 \cdot 2^{\aleph_0}$? Käyttämällä edellisen lauseen kohtaa (b) kahteen kertaan saadaan seuraava epäyhtälöketju:

$$2^{\aleph_0} \leq \aleph_0 \cdot 2^{\aleph_0} \leq 2^{\aleph_0} \cdot 2^{\aleph_0} = 2^{\aleph_0}$$

Siis $\aleph_0 \cdot 2^{\aleph_0} = 2^{\aleph_0}$.

Valinta-aksiooma

Lause 5.14 *Seuraavat ehdot ovat yhtäpitäviä:*

(1) **Valinta-aksiooma I**
Jokaisella relaatiolla R on olemassa funktio $F \subseteq R$, jolla $\mathrm{dom}(F) = \mathrm{dom}(R)$.

(2) **Valinta-aksiooma II**
Epätyhjien joukkojen karteesinen tulo on epätyhjä eli

$$\prod_{i \in I} A_j \neq \emptyset, \quad \textit{jos} \quad A_j \neq \emptyset \quad \textit{kaikilla } i \in I.$$

(3) **Valinta-aksiooma III**
Jokaisella joukolla A on olemassa (valinta)funktio F, jolla $\mathrm{dom}(F) = \mathcal{P}(A) \setminus \{\emptyset\}$ *ja $F(X) \in X$ jokaisella epätyhjällä $X \in \mathcal{P}(A)$.*

(4) **Valinta-aksiooma IV**
Olkoon $\mathcal{A}$ joukko, jolla pätee
(a) $A \neq \emptyset$ jokaisella $A \in \mathcal{A}$, ja
(b) $A \cap B = \emptyset$ aina kun $A, B \in \mathcal{A}$ ja $A \neq B$.
Tällöin on olemassa joukko C, jolla $C \cap A$ sisältää täsmälleen yhden alkion jokaisesta $A \in \mathcal{A}$.

(5) **Kardinaalien vertailtavuus**
Kaikilla joukoilla C ja D, joko $C \preccurlyeq D$ tai $D \preccurlyeq C$. Siis kaikilla kardinaaleilla λ ja κ, joko $\lambda \leq \kappa$ tai $\kappa \leq \lambda$.

(6) **Zornin lemma**
Olkoon $\mathcal{A}$ joukko, jolla $\bigcup \mathcal{B} \in \mathcal{A}$ jokaisella ketjulla[1] *$\mathcal{B} \subseteq \mathcal{A}$. Tällöin $\mathcal{A}$ sisältää maksimaalisen alkion. Tässä alkio M on maksimaalinen, jos sillä pätee $A \in \mathcal{A} \wedge M \subseteq A \;\Rightarrow\; M = A$.*

Todistus. Todistetaan yhtäpitävyys vielä vain osittain seuraavan kaavion mukaisesti:

$$\begin{tikzcd}
(6) \arrow[r, Rightarrow] \arrow[d, Rightarrow] & (1) \arrow[r, Rightarrow] & (2) \arrow[d, Rightarrow] \\
(5) & (3) \arrow[u, Rightarrow] & (4) \arrow[l, Rightarrow]
\end{tikzcd}$$

Puuttuvat implikaatiot todistetaan luvussa 6.

(1) $\Rightarrow$ (2): Oletetaan, että $H(i) \neq \emptyset$ jokaisella $i \in I$. Määritellään relaatio R seuraavasti:

$$R = \{\langle i, x\rangle \mid i \in I \wedge x \in H(i)\}.$$

1. $\mathcal{B}$ on ketju, jos $C \subseteq D$ tai $D \subseteq C$ pätee kaikilla $C, D \in \mathcal{B}$.

Valinta-aksiooma I:n perusteella on olemassa funktio $F \subseteq R$, jolla $\mathrm{dom}(F) = \mathrm{dom}(R) = I$. Jokaisella $i \in I$, $\langle i, F(i)\rangle \in F \subseteq R$, joten $F(i) \in H(i)$. Siis (2) pätee.

(2) $\Rightarrow$ (4): Olkoon $\mathcal{A}$ joukko, joka toteuttaa ehdot

(a) $\forall B \in \mathcal{A} : B \neq \emptyset$
(b) $\forall B, C \in \mathcal{A} : B \neq C \Rightarrow B \cap C = \emptyset$.

Olkoon $H = \mathrm{id}_{\mathcal{A}}$, jolloin $\mathcal{A}$ on itse indeksijoukko I. Nyt $H(B) = B \neq \emptyset$ jokaisella $B \in \mathcal{A}$. (2):n perusteella on olemassa funktio F s.e. $\mathrm{dom}(F) = \mathcal{A}$ ja $F(B) \in H(B) = B$ jokaisella $B \in \mathcal{A}$.

Olkoon $C = \mathrm{ran}(F)$. Jos $B \in \mathcal{A}$, niin $B \cap C = \{F(B)\}$: selvästi $F(B) \in B \cap C$, ja jos $F(B') \in B \cap C$, niin $F(B') \in B \cap B'$, mikä ei ole mahdollista, jollei $B = B'$.

Siis (4) pätee.

(4) $\Rightarrow$ (3): Olkoon A joukko. Määritellään

$$\mathcal{A} = \big\{\{B\} \times B \mid B \in \mathcal{P}(A) \setminus \{\emptyset\}\big\}$$

Nyt (a) $\{B\} \times B = \emptyset$ jokaisella $\{B\} \times B \in \mathcal{A}$ ja (b) jos $\{B\} \times B \neq \{B'\} \times B'$, niin $(\{B\} \times B) \cap (\{B'\} \times B') = \emptyset$. (4):n perusteella on olemassa C s.e. $C \cap (\{B\} \times B) = \{\langle B, x\rangle\}$ jollain $x \in B$ (jokainen $\{B\} \times B \in \mathcal{A}$).

C voi sisältää näiden parien lisäksi muitakin alkioita, joten määritellään:

$$F = C \cap \left(\bigcup \mathcal{A}\right)$$

Nyt F on funktio s.e. $\mathrm{dom}(F) = \mathcal{P}(A) \setminus \{\emptyset\}$. Lisäksi $F(B) \in B$ jokaisella $B \in \mathcal{P}(A) \setminus \{\emptyset\}$.

Siis (3) pätee.

(3) $\Rightarrow$ (1): Olkoon R relaatio. Olkoon $A = \mathrm{ran}(R)$. (3):n perusteella on olemassa funktio G s.e. $G(B) \in B$ jokaisella $B \subseteq A$, $B \neq \emptyset$. Määritellään funktio F s.e. $\mathrm{dom}(F) = \mathrm{dom}(R)$ asettamalla

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

Selvästi $F \subseteq R$. Siis (1) pätee.

(6) $\Rightarrow$ (1): Määritellään

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

Jos $\mathcal{B} \subseteq \mathcal{A}$ on ketju, niin kaikilla $f, g \in \mathcal{B}$ pätee $f \subseteq g$ tai $g \subseteq f$. Tällöin $\bigcup \mathcal{B} \subseteq R$, koska jokaisella $f \in \mathcal{B} : f \subseteq R$. $\bigcup \mathcal{B}$ on myös funktio, sillä jos $\langle x, y\rangle \in \bigcup \mathcal{B}$ ja

$\langle x, y' \rangle \in \bigcup \mathcal{B}$, niin on olemassa $f \in \mathcal{B}$ s.e. $\langle x, y \rangle \in f$ ja $g \in \mathcal{B}$ s.e. $\langle x, y' \rangle \in g$. Koska $\mathcal{B}$ on ketju, on $f \subseteq g$ tai $g \subseteq f$. Siis $\langle x, y \rangle, \langle x, y' \rangle \in f$ tai $\langle x, y \rangle, \langle x, y' \rangle \in g$. Koska f ja g ovat funktioita, on oltava $y = y'$. Siis $\bigcup \mathcal{B} \in \mathcal{A}$.

Zornin lemman ehto on voimassa, joten (6):n perusteella on olemassa maksimaalinen $F \in \mathcal{A}$. Nyt $F \subseteq R$. Osoitetaan vielä, että $\mathrm{dom}(F) = \mathrm{dom}(R)$.

Tehdään vastaoletus: $\mathrm{dom}(F) \subset \mathrm{dom}(R)$ eli on olemassa $x \in \mathrm{dom}(R)$ s.e. $x \notin \mathrm{dom}(F)$.

Olkoon $y \in \mathrm{ran}(R)$ s.e. xRy. Määritellään funktio $F' = F \cup \{\langle x, y \rangle\}$. Selvästi $F' \subseteq R$, joten $F' \in \mathcal{A}$. Toisaalta $F \subset F'$. Tämä on ristiriita, koska F on $\mathcal{A}$:n maksimaalinen alkio. Siis $\mathrm{dom}(F) = \mathrm{dom}(R)$. Siispä (1) pätee.

(6) $\Rightarrow$ (5): Olkoon C ja D joukkoja. Määritellään

$$\mathcal{A} = \{f \mid f \text{ on injektio, } \mathrm{dom}(f) \subseteq C, \mathrm{ran}(f) \subseteq D\}$$

Olkoon $\mathcal{B} \subseteq \mathcal{A}$ ketju. Tällöin $\bigcup \mathcal{B}$ on funktio (kuten todistuksen edellisessä kohdassa), $\mathrm{dom}(\bigcup \mathcal{B}) \subseteq C$ ja $\mathrm{ran}(\bigcup \mathcal{B}) \subseteq D$. $\bigcup \mathcal{B}$ on injektio (todistetaan samalla tavalla). Siis $\bigcup \mathcal{B} \in \mathcal{A}$. Zornin lemma (6) antaa maksimaalisen funktion $F \in \mathcal{A}$.

Osoitetaan, että

$$(*) \qquad \mathrm{dom}(F) = C \text{ tai } \mathrm{ran}(F) = D.$$

Tehdään vastaoletus: $\mathrm{dom}(F) \neq C$ ja $\mathrm{ran}(F) \neq D$. Siis on olemssa $x \in C \setminus \mathrm{dom}(F)$ ja $y \in D \setminus \mathrm{ran}(F)$. Määritellään $F' = F \cup \{\langle x, y \rangle\}$. Nyt F' on injektio, $\mathrm{dom}(F') \subseteq C, \mathrm{ran}(F') \subseteq D$, joten $F' \in \mathcal{A}$. Tämä on ristiriita F:n maksimaalisuuden kanssa, sillä $F \subset F'$. Siis $(*)$ pätee.

Jos $\mathrm{dom}(F) = C$, niin F on injektio $C \to D$. Jos taas $\mathrm{ran}(F) = D$, on F^{-1} injektio $D \to C$. Siis joko $C \preccurlyeq D$ tai $D \preccurlyeq C$ □

Huomautus. Valinta-aksioomaa ei tarvita, kun tehdään valintafunktio ω:lle. Voidaan määritellä

$$F(A) = \text{"A:n pienin alkio", kun } A \subseteq \omega, A \neq \emptyset.$$

Valinta-aksioomaa ei myöskään tarvita, kun valitaan alkioita äärellisestä joukosta.

Esimerkki 5.10 Jos on olemassa surjektio $f : B \to A$, niin valinta-aksiooman perusteella on olemassa funktio $g \subseteq f^{-1}$ s.e. $\mathrm{dom}(g) = A$. Tällöin g on injektio $A \to B$ (ks. lause 3.10), joten $A \preccurlyeq B$. Toisaalta jos $A \preccurlyeq B$ ja $A \neq \emptyset$, niin on olemassa injektio $f : A \to B$. Tällöin $f^{-1} \cup (B \setminus \mathrm{ran}(f)) \times \{a\})$, missä $a \in \{A\}$, on surjektio $B \to A$. (Jos $A = \emptyset$ ja $B \neq \emptyset$, niin ei ole olemassa surjektiota $B \to A$.)

Siis

$$A \preccurlyeq B \Leftrightarrow \big(A = \emptyset \text{ tai on olemassa surjektio } f : B \to A\big).$$

Lause 5.15

(a) *Jos A on ääretön, niin $\omega \preccurlyeq A$.*
(b) *Jos κ on ääretön kardinaali, niin $\aleph_0 \leq \kappa$.*

Todistus. Määritellään rekursiolla funktio $h : \omega \to \mathcal{P}(A)$, missä $h(n) \subseteq A$ on äärellinen.

Olkoon F joukon A valintafunktio, eli jos $B \subseteq A$ ja $B \neq \emptyset$, niin $F(B) \in B$. Asetetaan sitten

$$\begin{aligned} &h(0) = \emptyset \\ &h(n^+) = h(n) \cup \{F(A \setminus h(n))\}. \end{aligned}$$

Rekursioteoreeman perusteella on olemassa yksikäsitteinen funktio $h : \omega \to \mathcal{P}(A)$, jolla nämä ehdot pätevät.

Määritellään funktio $g : \omega \to A$ asettamalla $g(n) = F(A \backslash h(n))$. Nyt g on injektio, sillä jos $n, m \in \omega$ ja $n \neq m$, niin joko $m \in n$ tai $n \in m$. Oletetaan, että $m \in n$. Tällöin $m \leq n$ ja siis

$$g(m) \in h(m^+) \subseteq h(n)$$

Mutta $g(n) \notin h(n)$, sillä $g(n) = F(A \setminus h(n)) \in A \setminus h(n)$.

Siis $g(m) \neq g(n)$, joten g on injektio. □

Havaintoja

(1) Jokainen ω:n ääretön osajoukko on yhtämahtava ω:n kanssa. (Huomaa, ettei ω:n tapauksessa tarvita valinta-aksioomaa.)
(2) Jos $\kappa < \aleph_0$, niin κ on äärellinen. Päinvastainen pätee myös, joten

$$\kappa < \aleph_0 \;\Leftrightarrow\; \kappa \text{ on äärellinen.}$$

(3) Äärellisten joukkojen osajoukot ovat äärellisiä: Jos $\mathrm{card}(A) \leq \mathrm{card}(B) < \aleph_0$, niin $\mathrm{card}(A) < \aleph_0$.

Seuraus 5.16 *Joukko A on ääretön jos ja vain jos A on yhtämahtava jonkin aidon osajoukkonsa kanssa.*

Todistus. Toinen suunta todistettiin jo aiemmin: seurauksen 5.4 mukaan, jos $A \approx B$ ja $B \subset A$, niin A on ääretön.

Olkoon A ääretön. Lauseen 5.15 perusteella on siis olemassa injektio $f : \omega \to A$.

Määritellään $g : A \to A$ asettamalla

$$\begin{aligned} g(f(n)) &= f(n^+), && \text{kun } n \in \omega \\ g(x) &= x, && \text{kun } x \notin \mathrm{ran}(f). \end{aligned}$$

Tällöin g on bijektio $A \to A \setminus \{f(0)\}$ □

Numeroituvat joukot

Määritelmä 5.6 Joukko A on *numeroituva*, jos $A \preccurlyeq \omega$ eli $\mathrm{card}(A) \leq \aleph_0$. Edelleen joukko A on *ylinumeroituva*, jos se ei ole numeroituva.

Siis A on numeroituva, jos A on äärellinen tai $\mathrm{card}(A) = \aleph_0$.

On suoraviivaista osoittaa, että jokainen numeroituvan joukon osajoukko on numeroituva. Edelleen kahden numeroituvan joukon A ja B yhdiste $A \cup B$ ja tulo $A \times B$ ovat numeroituvia.

Lause 5.17 *Numeroituvan monen numeroituvan joukon yhdiste on numeroituva.*

Toisin sanoen: jos $\mathcal{A}$ on numeroituva ja jokainen $A \in \mathcal{A}$ on numeroituva, niin $\bigcup \mathcal{A}$ on numeroituva.

Todistus. Voidaan olettaa, että $\mathcal{A} \neq \emptyset$, sillä $\bigcup \emptyset = \emptyset$ on numeroituva. Edelleen voidaan olettaa, että jokainen $A \in \mathcal{A}$ on epätyhjä, koska kaikilla joukoilla B pätee $\bigcup B = \bigcup \big(B \cup \{\emptyset\}\big)$.

Olkoon $\mathcal{A}$ siis numeroituva epätyhjä joukko numeroituvia epätyhjiä joukkoja. Konstruoidaan surjektio $f : \omega \times \omega \to \bigcup \mathcal{A}$. Tästä seuraa, että $\bigcup \mathcal{A} \preccurlyeq \omega \times \omega \preccurlyeq \omega$.

Koska $\mathcal{A}$ on numeroituva ja epätyhjä, on olemassa surjektio $G : \omega \to \mathcal{A}$. Siis $\mathcal{A} = \{G(m) \mid m \in \omega\}$. Edelleen koska $G(m)$ on numeroituva ja epätyhjä, on joukko

$$H(m) = \{g \mid g \text{ on surjektio } \omega \to G(m)\}$$

epätyhjä jokaisella $m \in \omega$. Siis valinta-aksiooman (muotoilu II) perusteella on olemassa funktio $F : \omega \to \bigcup_{m \in \omega} H(m)$, jolla $F(m) \in H(m)$ jokaisella $m \in \omega$.

Nyt $F(m)$ on surjektio $\omega \to G(m)$ jokaisella $m \in \omega$, ja voimme määritellä funktion $f : \omega \times \omega \to \bigcup \mathcal{A}$ asettamalla $f(m, n) = F(m)(n)$. On helppo todeta, että f on surjektio. $\square$

Esimerkki 5.11 Olkoon A joukko. *Jono* joukossa A on funktio $f : n \to A$, missä $n \in \omega$. (Jos $n = 0$, niin f on tyhjä jono, eli tyhjä funktio $\emptyset$.) Kaikkien joukon A jonojen joukkoa merkitään

$$\begin{aligned} \mathrm{Sq}(A) &= \{f \mid f \text{ on jono } A\text{:ssa}\} \\ &= {}^0A \cup {}^1A \cup {}^2A \cup \ldots \end{aligned}$$

(a) Osoitetaan ensin, että $\mathrm{Sq}(\omega) \approx \omega$.

Tämä voidaan todistaa Schröderin ja Bernsteinin lauseen avulla seuraavasti. Määritellään funktio $H : \mathrm{Sq}(\omega) \to \omega$ asettamalla

$$H(f) = 2^{f(0)+1} \cdot 3^{f(1)+1} \cdot \ldots \cdot p_{n-1}^{f(n-1)+1},$$

kun $f \in {}^n\omega$ ja p_i on i:s alkuluku. Koska jokaisella kokonaisluvulla on yksikäsitteinen esitys alkulukujen tulona, pätee

$$f \neq f' \;\Rightarrow\; H(f) \neq H(f').$$

Siis H on injektio. Toisaalta funktio $G : \omega \to \mathrm{Sq}(\omega)$, jolla $G(n) = f \in {}^1\omega$, missä $f(0) = n$, on selvästi injektio.

(b) Yleisemmin pätee, että jos joukko A on numeroituva, niin myös $\mathrm{Sq}(A)$ on numeroituva. Nimittäin jos $g : A \to \omega$ on injektio, ja $f : \mathrm{Sq}(\omega) \to \omega$ on bijektio, niin funktioiden g ja f avulla voidaan muodostaa injektio $\mathrm{Sq}(A) \to \omega$ (harjoitustehtävä.)

Äärettömien kardinaalilukujen aritmetiikkaa

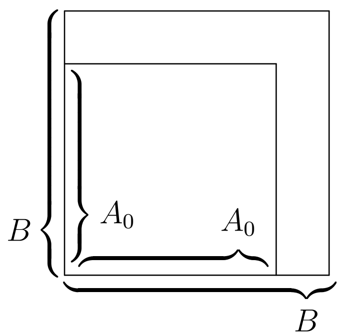
Apulause 5.18 *Jos κ on ääretön kardinaali, niin $\kappa \cdot \kappa = \kappa$.*

Todistus. Olkoon B joukko, jolla $\mathrm{card}(B) = \kappa$. Osoitetaan Zornin lemman avulla, että $B \times B \approx B$. Asetetaan

$$\mathcal{H} = \{\emptyset\} \cup \{f \mid f \text{ on bijektio } A \times A \to A \text{ jollain äärettömällä } A \subseteq B\}.$$

Osoitetaan aluksi, että $\mathcal{H}$ on suljettu ketjujen yhdisteiden suhteen. Olkoon siis $\mathcal{B} \subseteq \mathcal{H}$ ketju. Voidaan olettaa, että $\mathcal{B}$ sisältää jonkin epätyhjän funktion, sillä muuten olisi $\bigcup \mathcal{B} = \emptyset \in \mathcal{H}$. Kuten aikaisemmissa todistuksissa olemme nähneet, $\bigcup \mathcal{B}$ on joka tapauksessa injektiivinen funktio. Merkitään

$$A = \mathrm{ran}\big(\bigcup \mathcal{B}\big).$$



On helppo todeta, että $A = \bigcup\{\mathrm{ran}(f) \mid f \in \mathcal{B}\}$, ja että $A \subseteq B$ on ääretön joukko.

Osoitamme nyt, että $\mathrm{dom}(\bigcup \mathcal{B}) = A \times A$; tästä jo seuraakin, että $\bigcup \mathcal{B} \in \mathcal{H}$. Olkoon $\langle a, b\rangle \in A \times A$. Tällöin on olemassa funktiot $f, g \in \mathcal{B}$, joilla $a \in \mathrm{ran}(f)$ ja $b \in \mathrm{ran}(g)$. Koska $\mathcal{B}$ on ketju, on joko $f \subseteq g$ tai $g \subseteq f$; symmetrian perusteella voidaan olettaa, että näistä ensimmäinen ehto on voimassa. Nyt voidaan päätellä, että

$$\langle a, b\rangle \in \mathrm{ran}(g) \times \mathrm{ran}(g) = \mathrm{dom}(g) \subseteq \mathrm{dom}\big(\bigcup \mathcal{B}\big).$$

Siis $A \times A \subseteq \mathrm{dom}(\bigcup \mathcal{B})$. Kääntäen, jos $c \in \mathrm{dom}(\bigcup \mathcal{B})$, niin $c \in \mathrm{dom}(f)$ jollain $f \in \mathcal{B}$. Koska $\mathrm{dom}(f) = \mathrm{ran}(f) \times \mathrm{ran}(f)$ ja $\mathrm{ran}(f) \subseteq A$, nähdään, että $c \in A \times A$.

Nyt voidaan käyttää Zornin lemmaa: on olemassa maksimaalinen funktio $f_0 \in \mathcal{H}$. Olkoon $\mathrm{ran}(f_0) = A_0$, ja olkoon $\mathrm{card}(A_0) = \lambda$. Osoitetaan ensin, että $\lambda \geq \aleph_0$.

Koska B on ääretön joukko, sillä on osajoukko A, jolla $\mathrm{card}(A) = \aleph_0$. Tällöin on olemassa bijektio $f : A \times A \to A$, ja selvästi $f \in \mathcal{H}$. Nyt nähdään, että $f_0 \neq \emptyset$, sillä muuten olisi $f_0 \subset f$ vastoin oletusta, että f_0 on maksimaalinen. Joukon $\mathcal{H}$ määritelmästä seuraa, että A_0 on ääretön, eli $\lambda \geq \aleph_0$.

Koska $f_0 : A_0 \times A_0 \to A_0$ on bijektio, on $\lambda \cdot \lambda = \lambda$. Jos voitaisiin osoittaa, että $A_0 = B$, niin lauseen väite seuraisi välittömästi. Tämä ei kuitenkaan välttämättä pidä paikkaansa! Osoitetaan sen sijaan funktion f_0 maksimaalisuuden avulla, että $\lambda = \kappa$, joka toki riittää.

Osoitetaan tätä varten, että $\mathrm{card}(B \setminus A_0) < \lambda$. Tehdään vastaoletus: $\lambda \leq \mathrm{card}(B \setminus A_0)$. Tällöin joukolla $B \setminus A_0$ on osajoukko D, jolla $\mathrm{card}(D) = \lambda$. Tarkastellaan nyt joukkoa $(A_0 \cup D) \times (A_0 \cup D)$. Se voidaan jakaa erilliseksi yhdisteeksi neljästä osasta:

$$(A_0 \times A_0) \cup (A_0 \times D) \cup (D \times A_0) \cup (D \times D).$$

Kolmen viimeisen osan mahtavuudet ovat kaikki $\lambda \cdot \lambda = \lambda$, joten joukon $(A_0 \times D) \cup (D \times A_0) \cup (D \times D)$ mahtavuus on $\lambda + \lambda + \lambda \leq 3 \cdot \lambda \leq \lambda \cdot \lambda = \lambda$. Siispä on olemassa bijektio $g : (A_0 \times D) \cup (D \times A_0) \cup (D \times D) \to D$. Nyt $f_0 \cup g$ on bijektio $(A_0 \cup D) \times (A_0 \cup D) \to A_0 \cup D$, joten $f_0 \cup g \in \mathcal{H}$. Tämä on ristiriidassa sen kanssa, että f_0 on maksimaalinen. Vastaoletus on siis väärä, joten kardinaalilukujen vertailtavuuden perusteella $\mathrm{card}(B \setminus A_0) < \lambda$.

Nyt voimme saattaa todistuksen loppuun seuraavasti:

$$\kappa = \mathrm{card}(A_0) + \mathrm{card}(B \setminus A_0) \leq \lambda + \lambda = 2 \cdot \lambda \leq \lambda \cdot \lambda = \lambda \leq \kappa,$$

joten $\lambda = \kappa$ ja siis $\kappa \cdot \kappa = \kappa$. □

Absorptiolaki kardinaaliaritmetiikassa. *Jos κ ja λ ovat kardinaaleja, joilla $\max(\kappa, \lambda) \geq \omega$ ja $\min(\kappa, \lambda) > 0$, niin $\kappa + \lambda = \kappa \cdot \lambda = \max(\kappa, \lambda)$.*

Todistus. Oletetaan, että $\lambda \leq \kappa$. Tällöin

$$\kappa \leq \kappa + \lambda \leq \kappa + \kappa = \kappa \cdot 2 \leq \kappa \cdot \kappa \overset{5.18}{=} \kappa$$

Siis $\kappa + \lambda = \kappa = \max(\kappa, \lambda)$.

Toisaalta

$$\kappa \leq \kappa \cdot \lambda \leq \kappa \cdot \kappa = \kappa,$$

joten $\kappa \cdot \lambda = \kappa = \max(\kappa, \lambda)$. □

Huom: Äärettömille kardinaaleille ei voida määritellä vähennyslaskua:

$$0 + \kappa = \kappa + \kappa = \kappa$$

$$\kappa - \kappa = \begin{cases} \kappa \\ 0 \end{cases} \quad ?$$

Sama pätee jakolaskulle.

Esimerkki 5.12 $\kappa^\kappa = 2^\kappa$, kun $\kappa \geq \omega$:

$$\kappa^\kappa \leq (2^\kappa)^\kappa = 2^{\kappa \cdot \kappa} = 2^\kappa \leq \kappa^\kappa$$

Esimerkki 5.13 (a) Kuinka monta funktiota $\mathbb{R} \to \mathbb{R}$ on olemassa? Toisin sanoen, mitä on card$({}^{\mathbb{R}}\mathbb{R})$? Vastaus voidaan laskea seuraavasti:

$$\mathrm{card}({}^{\mathbb{R}}\mathbb{R}) = (2^{\aleph_0})^{2^{\aleph_0}} = 2^{\aleph_0 \cdot 2^{\aleph_0}} = \underset{\mathrm{card}(\mathcal{P}(\mathbb{R}))}{\underset{\shortparallel}{2^{2^{\aleph_0}}}} > 2^{\aleph_0}$$

(b) Kuinka monta jatkuvaa funtiota $\mathbb{R} \to \mathbb{R}$ on olemassa? Kysytään siis, mikä on card$(C(\mathbb{R}))$, kun

$$C(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ on jatkuva funktio}\}.$$

Tunnetusti jatkuvat funktiot määräytyvät yksikäsitteisesti rationaaliluvuilla saamiensa arvojen perusteella: jos $f, g, \in C(\mathbb{R})$ ja $f \restriction \mathbb{Q} = g \restriction \mathbb{Q}$, niin $f = g$. Tämä nähdään seuraavasti: jos $f \neq g$, niin

$$\exists x \in \mathbb{R}\big(f(x) \neq g(x) \text{ eli } f(x) - g(x) \neq 0\big)$$

Tällöin on olemassa avoin väli $\Delta =]x - \delta, x + \delta[$ s.e. $f(y) - g(y) \neq 0$ jokaisella $y \in \Delta$. Koska $\mathbb{Q}$ on $\mathbb{R}$:n tiheä osajoukko, on olemassa $q \in \mathbb{Q} \cap \Delta$. Nyt $f(q) \neq g(q)$, joten $f \restriction \mathbb{Q} \neq g \restriction \mathbb{Q}$.

Kuvaus $H : C(\mathbb{R}) \to {}^{\mathbb{Q}}\mathbb{R}$, missä $H(f) = f \restriction \mathbb{Q}$ on siis injektio. Siispä

$$\mathrm{card}(C(\mathbb{R})) \leq \mathrm{card}({}^{\mathbb{Q}}\mathbb{R}) = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0}$$

Toisaalta käyttämällä vakiofunktioita, voidaan muodostaa injektio $F : \mathbb{R} \to C(\mathbb{R})$, joten card$(C(\mathbb{R})) \geq$ card$(\mathbb{R}) = 2^{\aleph_0}$.

Kontinuumihypoteesi

Olemme osoittaneet, että $\aleph_0 < 2^{\aleph_0}$, mutta onko näiden kahden kardinaalin välissä muita kardinaalilukuja? Tämä on yhtä pitävä seuraavan kysymyksen kanssa:

Kysymys: Onko olemassa joukkoa A, jolla pätee $\omega \subset A \subset \mathbb{R}$ ja $\omega \not\approx A \not\approx \mathbb{R}$?

(Tässä ajattelemme, että luonnolliset luvut ovat reaalilukuja; tämä ei reaalilukujen joukko-opillisen määritelmän mukaan pidä paikkaansa, mutta toki $\mathbb{R}$ sisältää osajoukkonaan ω:n kanssa isomorfisen joukon.)

Kontinuumihypoteesi on oletus, että tällaista joukkoa ei ole olemassa, eli se on väite

Kontinuumihypoteesi (CH) Ei ole olemassa kardinaalilukua κ, jolla

$$\aleph_0 < \kappa < 2^{\aleph_0}.$$

Kurt Gödel osoitti vuonna 1940, että kontinuumihypoteesin negaatiota ($\neg$CH) ei voi todistaa edellä esitetyistä Zermelon–Fraenkelin aksioomeista edes valinta-aksiooman kanssa (ZFC aksioomat). Vuonna 1963 Paul Cohen osoitti pakottamismenetelmällä edelleen, ettei kontinuumihypoteesia itseäänkään voi todistaa ZFC-aksioomeista. Kontinuumihypoteesi on siis riippumaton joukko-opin ZFC aksioomista.

Kontinuumihypoteesi voidaan yleistää kardinaaleista $\aleph_0$ ja $2^{\aleph_0}$ muihin mahtavuuksiin. Millä hyvänsä äärettömällä kardinaalilla κ pätee $\kappa < 2^{\kappa}$, joten voidaan kysyä, onko niiden välissä muita kardinaalilukuja. Yleistetty kontinuumihypoteesi on olettamus, että vastaus on kielteinen kaikilla äärettömillä kardinaaleilla κ:

Yleistetty kontinuumihypoteesi (GCH) Jos κ on ääretön kardinaali, niin ei ole olemassa kardinaalia λ, jolla

$$\kappa < \lambda < 2^{\lambda}.$$

Myös yleistetty kontinuumihypoteesi on riippumaton joukko-opin aksioomista: sitä ei voi todistaa, eikä sen negaatiota voi todistaa ZFC:ssä.

Luku 6

Järjestykset ja ordinaalit

Osittaiset järjestykset

Määritelmä 6.1 Relaatio R on *osittainen järjestys*, jos

(1) R on transitiivinen, ja
(2) R on irrefleksiivinen, eli kaikilla x pätee $\langle x, x\rangle \notin R$.

Esimerkki 6.1
(a) Minkä hyvänsä joukon S osajoukkorelaatio

$$C_S = \{\langle A, B\rangle \mid A, B \subseteq S, A \subset B\}$$

on osittainen järjestys.

(b) Olkoon P positiivisten kokonaislukujen joukko: $P = \omega \setminus \{0\}$. "Tiukka" jaollisuusrelaatio

$$\{\langle a, b\rangle \in P \times P \mid q \cdot a = b \text{ jollain } q \neq 1\}$$

joukossa P on osittainen järjestys.

Osittaisille järjestyksille käytetään yleensä symbolia $<$. Tällöin voidaan normaaliin tapaan käyttää myös merkintää $x \leq y$, kun sallitaan alkioiden x ja y yhtäsuuruus. Siis

$$x \leq y \iff \bigl(x < y \text{ tai } x = y\bigr).$$

Lause 6.1 *Olkoon $<$ osittainen järjestys. Tällöin kaikilla x ja y:*

(a) *Korkeintaan yksi ehdoista*

$$x < y, \quad x = y, \quad y < x$$

on voimassa.

(b) $x \leq y \wedge y \leq x \Rightarrow x = y.$

Todistus. (a) Jos $x = y$, ei ole mahdollista, että $x < y$ tai $y < x$, koska molemmissa tapauksissa pätisi $x < x$ vastoin relaation $<$ irrefleksiivisyyttä. Edelleen, jos $x < y$, ei voi olla $y < x$, sillä muuten olisi transitiivisuuden perusteella $x < x$.

(b) Oletetaan, että $x \leq y$ ja $y \leq x$. Tällöin ($x < y$ tai $x = y$) tai ($y < x$ tai $y = x$). Koska kohdan (a) mukaan ei ole mahdollista, että $x < y$ ja $y < x$, on oltava $x = y$. □

Kuten Luvussa 3 määriteltiin, relaatio R on lineaarinen järjestys, jos R on transitiivinen ja toteuttaa trikotomian joukossa A: kaikilla $x, y \in A$ pätee täsmälleen yksi ehdoista

$$xRy, \quad x = y, \quad yRx.$$

Koska trikotomiasta seuraa irrefleksiivisyys, jokainen lineaarinen järjestys R on myös osittainen järjestys.

Olkoon R relaatio joukossa A (eli $R \subseteq A \times A$). Kutsumme jatkossa järjestettyä paria $\langle A, R \rangle$ *struktuuriksi*.

Jatkossa tarvitaan seuraavia järjestettyihin joukkoihin liittyviä käsitteitä.

Määritelmä 6.2 Olkoon $<$ (osittainen) järjestys joukossa A, $D \subseteq A$ ja $m \in A$.

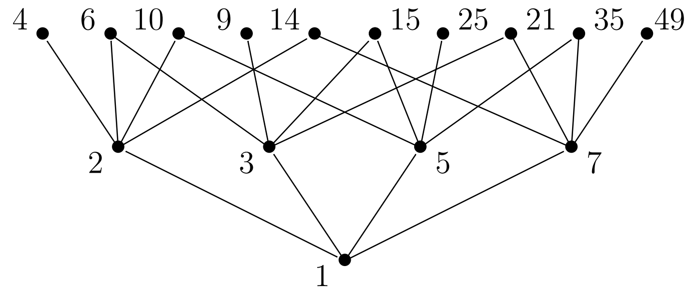
(a) m on joukon D *pienin alkio*, $x = \min D$, jos $m \in D$ ja kaikilla $a \in D$ pätee $m \leq a$.
(b) m on joukon D *suurin alkio*, $x = \max D$, jos $m \in D$ ja kaikilla $a \in D$ pätee $a \leq m$.
(c) m on joukon D *minimaalinen alkio*, jos $m \in D$ ja kaikilla $a \in D$ pätee $\neg\, a < m$.
(d) m on joukon D *maksimaalinen alkio*, jos $m \in D$ ja kaikilla $a \in D$ pätee $\neg\, m < a$.
(e) m on joukon D *alaraja*, jos jokaisella $a \in D$ pätee $m \leq a$.
(f) m on joukon D *yläraja*, jos jokaisella $a \in D$ pätee $a \leq m$.
(g) m on joukon D *suurin alaraja*, $x = \inf D$, jos jokaisella joukon D alarajalla a pätee $a \leq m$. Siis $\inf D = \max B$, missä B on joukon D alarajojen joukko.
(h) m on joukon D *pienin yläraja*, $x = \sup D$, jos jokaisella joukon D ylärajalla a pätee $m \leq a$. Siis $\sup D = \min C$, missä C on joukon D ylärajojen joukko.

Huomaa, että kaikilla osajoukoilla $D \subseteq A$ ei välttämättä ole suurinta eikä pienintä alkiota. Jos $\min D$ on olemassa, se on yksikäsitteinen; samoin $\max D$ on yksikäsitteinen. Toisaalta samalla joukolla voi olla useita minimaalisia (tai maksimaalisia) alkioita. Joukon D pienin alkio on aina myös minimaalinen alkio; päinvastainen pätee, jos $<$ on lineaarijärjestys, mutta ei yleisesti osittaisilla järjestyksillä.

Esimerkki 6.2 Tarkastellaan taas joukon $P = \omega \setminus \{0\}$ osittaista järjestystä, joka määritellään jaollisuuden avulla:

$$< = \{\langle x, y\rangle \in P \times P \mid \exists z(x = z \cdot y \land z \neq 1)\}.$$

Nyt 1 on joukon P pienin alkio. Olkoon $D = P \setminus \{1\}$. Tällöin joukolla D ei ole pienintä alkiota (eikä suurinta alkiota). Jokainen alkuluku on D:n minimaalinen alkio, ja 1 on D:n alaraja. Itse asiassa $1 = \inf D$, sillä 1 on joukon D ainoa alaraja.



Hyvinjärjestykset

Määritelmä 6.3 Lineaarijärjestys joukolla A on *hyvinjärjestys*, jos jokaisella A:n epätyhjällä osajoukolla on pienin alkio.

Luonnollisten lukujen joukon ω tavallinen järjestys on hyvinjärjestys. Sen sijaan kokonaislukujen tavallinen järjestys ei ole hyvinjärjestys: esimerkiksi joukossa $\{n \in \mathbb{Z} \mid n < 0\}$ ei ole pienintä alkiota.

Olkoon A epätyhjä joukko ja olkoon $<$ joukon A hyvinjärjestys. Tällöin joukossa A on pienin alkio t_0. Edelleen joukossa $A \setminus \{t_0\}$ on pienin alkio t_1, ja joukossa $A \setminus \{t_0, t_1\}$ on pienin alkio t_2; tätä alkioiden jonoa $t_0, t_1, t_2, \ldots$ voidaan jatkaa niin kauan, kun joukossa A riittää uusia alkioita. Näin saadaan jono

$$\begin{aligned} t_0 &= \min(A) \\ t_1 &= \min(A \setminus \{t_0\}) \\ &\vdots \\ t_n &= \min(A \setminus \{t_0, \ldots, t_{n-1}\}) \\ &\vdots \end{aligned}$$

Jos $A \setminus \{t_i \mid i \in \omega\} \neq \emptyset$, jonoa voidaan vieläkin jatkaa:

$$\begin{aligned} t_\omega &= \min(A \setminus \{t_i \mid i \in \omega\}) \\ t_{\omega+1} &= \min(A \setminus \{t_i \mid i \in \omega \cup \{\omega\}\}) \\ &\vdots \end{aligned}$$

Tämä jono voidaan esittää havainnollisesti suuruusjärjestyksen mukaisena nuolikuviona seuraavasti:

$$t_0 \bullet \longrightarrow t_1 \bullet \longrightarrow \cdots \longrightarrow t_n \bullet \longrightarrow \cdots \longrightarrow t_\omega \bullet \longrightarrow t_{\omega+1} \bullet \longrightarrow \cdots \longrightarrow t_{\omega\cdot 2} \bullet \longrightarrow \cdots$$

Intuitiivisesti hyvinjärjestykset ovat lineaarijärjestyksiä, joissa ei ole äärettömiä laskevia ketjuja $a_0 > a_1 > a_2 > \ldots$. Tämä intuitio voidaan muotoilla täsmälliseksi karakterisoinniksi seuraavasti:

Lause 6.2 *Olkoon $<$ joukon A lineaarijärjestys. Tällöin $<$ on hyvinjärjestys jos ja vain jos ei ole olemassa funktiota $f : \omega \to A$, jolla pätee*

$$\forall n \in \omega \big(f(n^+) < f(n) \big).$$

Todistus. Jos funktio $f : \omega \to A$ toteuttaa ehdon $f(n^+) < f(n)$ jokaisella $n \in \omega$, niin osajoukossa $\operatorname{ran}(f) \subseteq A$ ei ole pienintä alkiota. Tällöin $<$ ei ole hyvinjärjestys.

Oletetaan sitten, että $<$ ei ole hyvinjärjestys. On siis olemassa osajoukko $B \subseteq A$, jolla ei ole pienintä alkiota eli

$$\forall x \in B \exists y \in B \big(y < x \big).$$

Tällöin on olemassa funktio $f : \omega \to B$, jolla pätee

$$f(n^+) < f(n) \text{ jokaisella } n \in \omega.$$

Funktio f voidaan määritellä rekursiolla käyttäen hyväksi joukon B valintafunktiota; todistuksen yksityishdat jätetään harjoitustehtäväksi. $\square$

Määritelmä 6.4 Jos $<$ on osittainen järjestys joukossa A ja $t \in A$, niin joukko

$$\operatorname{seg} t = \{x \in A \mid x < t\}$$

on alkion t *määräämä alkusegmentti.*

Erityisesti jos $A = \omega$ ja $<$ on ω:n tavallinen järjestys, niin jokaisella $n \in \omega$ pätee

$$\operatorname{seg} n = \{m \in \omega \mid m < n\} = \{0, \ldots, n-1\} = n.$$

Transfiniittisen induktion periaate. *Olkoon $<$ hyvinjärjestys joukossa A. Olkoon B joukon A osajoukko, jolla pätee*

$$\forall t \in A \, (\operatorname{seg} t \subseteq B \to t \in B) \, .$$

Tällöin $B = A$.

Todistus. Jos $B \subset A$, niin $A \setminus B \neq \emptyset$, joten joukossa $A \setminus B$ on pienin alkio t. Nyt $t \notin B$, mutta $\operatorname{seg} t \subseteq B$. Siis B ei ole $<$-induktiivinen. $\square$

Todistusta voidaan havainnollistaa seuraavasti: Olkoon t_0 joukon A pienin alkio. Nyt $\operatorname{seg} t_0 = \emptyset$, joten $\operatorname{seg} t_0 \subseteq B$. Siis $t_0 \in B$. Olkoon sitten t_1 joukon $A \setminus \{t_0\}$ pienin alkio. Nyt $\operatorname{seg} t_1 = \{t_0\}$, joten $\operatorname{seg} t_1 \subseteq B$. Siis $t_1 \in B$. Ja niin edelleen aina alkioon t_ω saakka, jolla taas pätee $\operatorname{seg} t_\omega \subseteq B$, ja siten $t_\omega \in B$. Tätä voidaan edelleen jatkaa niin kauan, kuin joukossa A on alkioita. Kun alkiot loppuvat, voidaan todeta, että $B = A$.

Jos $B \subseteq A$ ja B toteuttaa kaavan $\forall t \in A\,(\operatorname{seg} t \subseteq B \to t \in B)$, niin sanotaan, että B on *$<$-induktiivinen*. Transfiniittisen induktion periaate voidaan siis muotoilla seuraavasti:

> Jos $<$ on hyvinjärjestys joukossa A, niin A:n ainoa $<$-induktiivinen osajoukko on A itse.

Lause 6.3 *Olkoon $<$ lineaarijärjestys joukossa A. Oletetaan, että A on ainoa $<$-induktiivinen A:n osajoukko. Tällöin $<$ on hyvinjärjestys.*

Todistus. Olkoon $C \subseteq A$. Osoitamme, että joko joukossa C on pienin alkio, tai $C = \emptyset$. Tarkastellaan tätä varten C:n "tiukkojen alarajojen joukkoa"

$$B = \{t \in A \mid \forall x \in C(t < x)\}.$$

Huomaa, että $B \cap C = \emptyset$. Jaetaan tarkastelu kahteen tapaukseen sen mukaan, onko B $<$-induktiivinen vai ei:

Tapaus 1: B ei ole $<$-induktiivinen. Siis on olemassa $t \in A$, jolla $\operatorname{seg} t \subseteq B$, mutta $t \notin B$. Osoitamme, että tällöin t on joukon C pienin alkio. Koska $t \notin B$, on olemassa $x \in C$, jolla $x \leq t$. Toisaalta ei voi olla $x < t$, koska $\operatorname{seg} t \subseteq B$ ja $B \cap C = \emptyset$. Siis on oltava $x = t$, joten $t \in C$. Lopuksi vielä todetaan, että koska $\operatorname{seg} t \cap C = \emptyset$, joukossa C ei ole yhtään pienempää alkiota kuin t.

Tapaus 2: B on $<$-induktiivinen. Lauseen oletuksen perusteella tällöin pätee $B = A$, ja koska $B \cap C = \emptyset$, tästä seuraa, että $C = \emptyset$. $\square$

Transfiniittinen rekursio

Määritelmä 6.5 Olkoon $<$ on hyvinjärjestys joukossa A ja B on joukko. Funktioiden joukko järjestyksen $<$ määräämiltä alkusegmenteiltä joukkoon B on

$$^{<A}B = \{f \mid f \text{ on funktio } \operatorname{seg} t \to B \text{ jollain } t \in A\}.$$

Transfiniittinen rekursiolause (heikko muotoilu). *Olkoon $<$ hyvinjärjestys joukossa A ja olkoon $G : {}^{<A}B \to B$ funktio.*

Tällöin on olemassa yksikäsitteinen funktio $F : A \to B$ siten, että kaikilla $t \in A$ pätee

$$F(t) = G(F \restriction \operatorname{seg} t).$$

Esimerkki 6.3 Joukon ω hyvinjärjestyksellä pätee $\operatorname{seg} n = \{x \in \omega \mid x \in n\} = n$. Siis ylläolevan lauseen perusteella on olemassa yksikäsitteinen funktio $F : \omega \to B$, jolla $F(n) = G(F \restriction n)$ kaikilla $n \in \omega$. Erityisesti siis

$$\begin{aligned}
F(0) &= G(F \restriction 0) = G(\emptyset) \\
F(1) &= G(F \restriction 1) = G(\{\langle 0, F(0)\rangle\}) \\
F(2) &= G(F \restriction 2) = G(\{\langle 0, F(0)\rangle, \langle 1, F(1)\rangle\}).
\end{aligned}$$

Erona Luvun 4 rekursiotoreemaan on siis se, että funktion F arvo luvulla n riippuu nyt eksplisiittisesti kaikista sen edellisistä arvoista $F(0), \ldots, F(n-1)$, kun Luvun 4 antama arvo viittaa vain funktion edelliseen arvoon $F(n-1)$.

Transfiniittisen reksursion heikko muotoilu lähtee oletuksesta, että (sopiva) maalijoukko B on etukäteen tiedossa. Tämä ei suinkaan ole aina mahdollista. Tarkastellaan esimerkiksi seuraavaa luonnollista rekursiivista määritelmää:

$$F(t) = \{F(x) \mid x < t\} = \operatorname{ran}(F \restriction \operatorname{seg} t).$$

Ei ole olemassa funktiota G, jolla $G(a) = \operatorname{ran}(a)$ kaikilla joukoilla a. (Tällainen G on aito luokka.) Toisaalta jokaisella joukolla B on toki olemassa funktio G, jolla $\operatorname{dom}(G) = B$ ja $G(a) = \operatorname{ran}(a)$ kaikilla $a \in B$. Mutta ei ole selvää, miten löydetän sopiva joukko B, jossa on varmasti kaikki tarvittavat alkiot ylläolevaa rekursiota varten. Siksi tarvitaan vahvempi muotoilu transfiniiitisesta rekursiosta, jossa funktio G korvataan kaavalla γ, joka toteuttaa funktioehdon:

Transfiniittinen rekursiolause (varsinainen muotoilu). *Jokaisella kaavalla $\gamma(x, y)$ seuraava on joukko-opin teoreema:*

Olkoon $<$ hyvinjärjestys joukossa A. Oletetaan, että jokaisella funktiolla f on olemassa yksikäsitteinen y, jolla kaava $\gamma(f, y)$ on tosi. Tällöin on olemassa yksikäsitteinen funktio F siten, että $\operatorname{dom}(F) = A$ ja jokaisella $t \in A$ pätee

$$\gamma\big(F \restriction \operatorname{seg} t, F(t)\big).$$

Esimerkki 6.4 Transfiniiittisen rekursiolauseen heikko muotoilu seuraa vahvasta muotoilusta valitsemalla kaavaksi $\gamma(x, y)$:

$$\gamma(x, y) := \big(x \in {}^{<A}B \wedge y = G(x)\big) \vee \big(x \notin {}^{<A}B \wedge y = \emptyset\big)$$

Korvausaksioomat

Jos H on luokka järjestettyjä pareja ja toteuttaa funktioehdon (eli jokaisella x on olemassa yksikäsitteinen y, jolla $\langle x, y\rangle \in H$) ja A on joukko, niin aiemmin esitetyistä aksioomeista ei seuraa, että on olemassa joukko

$$H[\![A]\!] = \{y \mid \exists x \in A(\langle x, y\rangle \in H)\}.$$

Tämän puutteen korvaamiseksi tarvitaan korvausaksioomat.

Korvausaksioomat. Jokaisella kaavalla $\varphi(x, y)$, joka ei sisällä symbolia B, seuraava lause on aksiooma:

$$\begin{aligned}&\forall A\big(\forall x \in A \forall y \forall z\big(\varphi(x,y) \wedge \varphi(x,z) \to y = z\big)\\ &\quad \to \exists B \forall y\big(y \in B \leftrightarrow \exists x \in A\, \varphi(x,y)\big)\big)\end{aligned}$$

Huom: Kaavassa $\varphi(x, y)$ voi olla muitakin vapaita muuttujia kuin x ja y. Tätä voitaisiin korostaa kirjoittamalla kaava muotoon $\varphi(x, y, t_1, \dots, t_n)$ ja lisäämällä muuttujia vastaavat universaalikvanttorit aksioomaan:

$$\forall t_1 \dots \forall t_n \forall A\big(\dots\big).$$

Tämä ei ole kuitenkaan tarpeen, sillä aksiooman ylläesitetty muoto on riittävän vahva.

Transfiniittisen rekursiolauseen todistus. Todistus on samankaltainen kuin rekursioteoreeman todistus Luvussa 4. Määrittelemme aluksi hyväksyttävän funktion käsitteelle sopivan vastineen: jos $t \in A$, niin funktio υ on *γ-konstruoitu alkioon t asti*, jos

(a) $\mathrm{dom}(\upsilon) = \{x \mid x \le t\} = \mathrm{seg}\, t \cup \{t\}$, ja

(b) $\gamma(\upsilon \restriction \mathrm{seg}\, x, \upsilon(x))$ pätee jokaisella $x \in \mathrm{dom}(\upsilon)$.

Osoitamme tämän jälkeen, että kaikki johonkin asti γ-konstruoidut funktiot ovat keskenään yhteensopivia, jolloin voidaan muodostaa kaikkien niiden yhdiste F. Lopuksi osoitamme, että F toteuttaa kaikki vaadittavat ehdot.

(1) Jos $t_1 \le t_2$, υ_1 on γ-konstruoitu alkioon t_1 saakka ja υ_2 on γ-konstruoitu alkioon t_2 saakka, niin $\upsilon_1(x) = \upsilon_2(x)$ jokaisella $x \le t_1$.

Tehdään vastaoletus: joukko $C = \{x \le t_1 \mid \upsilon_1(x) \ne \upsilon_2(x)\}$ on epätyhjä. Olkoon s joukon C pienin alkio. Tällöin $\upsilon_1 \restriction \mathrm{seg}\, s = \upsilon_2 \restriction \mathrm{seg}\, s$, ja siten $\gamma(\upsilon_1 \restriction \mathrm{seg}\, s, \upsilon_1(s))$ ja $\gamma(\upsilon_1 \restriction \mathrm{seg}\, s, \upsilon_2(s))$. Koska γ määrittää funktion, tästä seuraa, että $\upsilon_1(s) = \upsilon_2(s)$. Tämä on ristiriidassa sen kanssa, että $s \in C$.

Määritellään nyt luokka $\mathcal{K}$ asettamalla

$$\mathcal{K} = \{\upsilon \mid \exists t \in A\big(\upsilon \text{ on } \gamma\text{-konstruoitu alkioon } t \text{ asti}\big)\}.$$

Valitsemalla kohdassa (1) $t_1 = t_2 = t$ nähdään, että jokaisella $t \in A$ on olemassa korkeintaan yksi funktio υ, joka on γ-konstruoitu alkioon t asti. Siksi soveltamalla sopivaa korvausaksioomaa voidaan todeta, että $\mathcal{K}$ on joukko.

Olkoon $F = \bigcup \mathcal{K}$. Siis $\langle x, y\rangle \in F \Leftrightarrow \upsilon(x) = y$, jollain $\upsilon \in \mathcal{K}$. Todetaan heti aluksi, että F on funktio: jos $\upsilon_1, \upsilon_2 \in \mathcal{K}$, niin ne ovat yhteensopivat, kuten edellä on todettu.

(2) Kaikilla $x \in \operatorname{dom}(F)$ pätee $\gamma(F \restriction \operatorname{seg} x, F(x))$:

Jos $x \in \operatorname{dom}(F)$, niin $x \in \operatorname{dom}(\upsilon)$, jollain $\upsilon \in \mathcal{K}$. Tällöin $\gamma(\upsilon \restriction \operatorname{seg} x, \upsilon(x))$. Koska υ ja F ovat funktioita, ja $\upsilon \subseteq F$, on

$$\upsilon \restriction \operatorname{seg} x = F \restriction \operatorname{seg} x \quad \text{ja} \quad \upsilon(x) = F(x)$$

Siis $\gamma(F \restriction \operatorname{seg} x, F(x))$.

(3) $\operatorname{dom}(F) = A$:

Tehdään vastaoletus: $\operatorname{dom}(F) \neq A$. Olkoon t joukon $A \setminus \operatorname{dom}(F)$ on pienin alkio. Tällöin $\operatorname{seg} t \subseteq \operatorname{dom}(F)$. (Itse asiassa $\operatorname{seg} t = \operatorname{dom}(F)$.) Olkoon y se yksikäsitteinen joukko, jolla pätee $\gamma(F, y)$ ja olkoon $\upsilon = F \cup \{\langle t, y\rangle\}$. Tällöin υ on γ-konstruoitu alkioon t asti. Mutta tällöin $\upsilon \in \mathcal{K}$ ja siis $t \in \operatorname{dom}(F)$, mikä on ristiriita.

(4) F on yksikäsitteinen:

Olkoot F_1 ja F_2 funktioita, jotka toteuttavat vaaditut ehdot. Olkoon $B \subseteq A$ se joukko, jossa F_1 ja F_2 yhtyvät eli

$$B = \{t \in A \mid F_1(t) = F_2(t)\}.$$

Osoitetaan, että B on $<$-induktiivinen.

Olkoon $\operatorname{seg} t \subseteq B$. Siis $F_1 \restriction \operatorname{seg} t = F_2 \restriction \operatorname{seg} t$. Edelleen

$$\gamma(F_1 \restriction \operatorname{seg} t, F_1(t)) \quad \text{ja} \quad \gamma(F_2 \restriction \operatorname{seg} t, F_2(t)),$$

joten $F_1(t) = F_2(t)$ eli $t \in B$.

Siis $B = A$ eli $F_1 = F_2$. $\square$

Epsilon-kuvat

Olkoon $<$ hyvinjärjestys joukossa A. Olkoon $\gamma(x,y)$ kaava $y = \mathrm{ran}(x)$. Transfiniittinen rekursio antaa yksikäsitteisen funktion E, jolla pätee:

$$E(t) = \mathrm{ran}(E \restriction \mathrm{seg}\, t) \quad \text{jokaisella } t \in A.$$

Funktion E arvo joukon A alkiolla t voidaan sieventää seuraavaan muotoon:

$$E(t) = \mathrm{ran}(E \restriction \mathrm{seg}\, t) = E[\![\mathrm{seg}\, t]\!] = \{E(x) \mid x < t\}.$$

Jatkossa käytetään merkintää $\alpha = \mathrm{ran}(E)$. Joukkoa α sanotaan struktuurin $\langle A, <\rangle$ *epsilon-kuvaksi* (tai *$\in$-kuvaksi*).

Esimerkki 6.5 Olkoon $A = \{a, b, c, \ldots, ö\}$, kun $a < b < c < \ldots < ö$. Nyt

$$\begin{aligned}
E(a) &= \{E(x) \mid x < a\} = \emptyset = 0 \\
E(b) &= \{E(x) \mid x < b\} = \{E(a)\} = \{0\} = 1 \\
E(c) &= \{E(x) \mid x < c\} = \{E(a), E(b)\} = \{0, 1\} = 2 \\
&\vdots \\
E(ö) &= \{E(a), \ldots, E(ä)\} = \{0, \ldots, 27\} = 28
\end{aligned}$$

Merkitään $\in_\alpha = \{\langle x, y\rangle \in \alpha \times \alpha \mid x \in y\}$.

$\in_\alpha$ on relaatio α:ssa.

Lause 6.4 *Oletetaan, että $<$ on hyvinjärjestys joukossa A ja että E ja α on määritelty kuten edellä. Tällöin pätee:*

(a) *$E(t) \notin E(t)$ jokaisella $t \in A$.*
(b) *E on bijektio $A \to \alpha$.*
(c) *$\forall t \in A \forall s \in A\big(s < t \leftrightarrow E(s) \in E(t)\big)$.*
(d) *α on transitiivinen joukko.*

Todistus.

(a) Tehdään vastaoletus: joukko $B = \{t \in a \mid E(t) \in E(t)\}$ on epätyhjä. Olkoon t^* joukon B pienin alkio. Funktion E määritelmän perusteella on olemassa $s < t^*$, jolla $E(t^*) = E(s)$. Mutta tällöin $E(s) \in E(s)$, joten $s \in B$, mikä on mahdotonta, koska oletuksen mukaan $t^* = \min B$.

(b) Koska $\alpha = \mathrm{ran}(E)$, on E surjektio. Osoitetaan sitten, että E on injektio. Olkoot $s, t \in A$ s.e. $s \neq t$. Tällöin $s < t$ tai $t < s$. Oletetaan, että $s < t$. Funktion E määritelmän mukaan $E(s) \in E(t)$. Nyt (a)-kohdan perusteella $E(t) \notin E(t)$, joten $E(s) \neq E(t)$.

(c) Implikaatio $s < t \Rightarrow E(s) \in E(t)$ pätee suoraan funktion E määritelmän perusteella.
Oletetaan sitten, että $E(s) \in E(t)$ Tällöin on olemassa $x < t$, jolla $E(s) = E(x)$. Koska E on injektio, on oltava $s = x$. Siis $s < t$.

(d) Olkoon $v \in \alpha$ ja $u \in v$. Tällöin $v = E(t)$, jollain $t \in A$ ja $u = E(s)$, missä $s \in A$ ja $s < t$, joten $u \in \alpha$.

$\square$

Isomorfismit

Määritelmä 6.6 Struktuurit $\langle A, R\rangle$ ja $\langle B, S\rangle$ ovat *isomorfisia*, jos on olemassa bijektio $f : A \to B$, jolla on voimassa

$$\forall x \in A \forall y \in A\big(xRy \leftrightarrow f(x)Sf(y)\big)$$

Tällöin merkitään $\langle A, R\rangle \cong \langle\ B, S\rangle$. Funktiota f sanotaan *isomorfismiksi.*

Esimerkki 6.6 Lauseen 6.4 perusteella funktio E on isomorfismi struktuurien $\langle A, <\rangle$ ja $\langle \alpha, \in_\alpha\rangle$ välillä.

Lause 6.5 *Olkoon $\langle A, R\rangle$, $\langle B, S\rangle$ ja $\langle C, T\rangle$ struktuureja. Tällöin*

$$\begin{aligned}
&\langle A, R\rangle \cong \langle A, R\rangle \\
&\langle A, R\rangle \cong \langle B, S\rangle \;\Rightarrow\; \langle B, S\rangle \cong \langle A, R\rangle \\
&\langle A, R\rangle \cong \langle B, S\rangle \wedge \langle B, S\rangle \cong \langle C, T\rangle \;\Rightarrow\; \langle A, R\rangle \cong \langle C, T\rangle
\end{aligned}$$

Todistus. Jätetään Harjoitustehtäväksi. $\square$

Apulause 6.6 *Oletetaan, että $f : A \to B$ on injektio ja $<_B$ on osittainen järjestys. Määritellään joukossa A relaatio $<_A$ asettamalla*

$$<_A = \{\langle a, b\rangle \mid f(a) <_B f(b)\}.$$

Tällöin

(a) *$<_A$ on osittainen järjestys joukossa A;*
(b) *jos $<_B$ on lineaarinen järjestys, niin $<_A$ on myös lineaarinen järjestys;*
(c) *jos $<_B$ on hyvinjärjestys, niin $<_A$ on myös hyvinjärjestys.*

Todistus. (a) Irrefleksiivisyys: Oletetaan, että $a <_A b$. Tällöin $f(a) <_B f(b)$, ja koska $<_B$ on irrefleksiivinen, on $f(a) \neq f(b)$. Koska f on injektio, tästä seuraa, että $a \neq b$.

Transitiivisuus: Oletetaan, että $a <_A b$ ja $b <_A c$. Tällöin $f(a) <_B f(b)$ ja $f(b) <_B f(c)$, ja koska $<_B$ on transitiivinen, pätee edelleen $f(a) <_B f(c)$. Relaation $<_A$ määritelmän perusteella tästä seuraa, että $a <_A c$.

(b) Jätetään harjoitustehtäväksi.

(c) Oletetaan, että $\emptyset \neq C \subseteq A$. Tällöin joukko $D = f[\![C]\!] \subseteq B$ on epätyhjä, joten siinä on pienin alkio d järjestyksen $<_B$ suhteen. Olkoon c se yksikäsitteinen joukon C alkio, jolla $f(c) = d$. On suoraviivaista osoittaa, että c on joukon C pienin alkio järjestyksen $<_A$ suhteen. □

Lause 6.7 *Oletetaan, että $\langle A, <_A\rangle \cong \langle B, <_B\rangle$. Jos toinen struktuureista $\langle A, <_A\rangle$ ja $\langle B, <_B\rangle$ on osittainen järjestys, niin toinenkin on. Sama väite pätee myös lineaariselle järjestykselle ja hyvinjärjestykselle.*

Todistus. Jos esimerkiksi $\langle B, <_B\rangle$ on osittainen järjestys ja $f : A \to B$ on isomorfismi, niin f on injektio ja isomorfismin määritelmän mukaan

$$\forall x \in A \forall y \in A\big(x <_A y \iff f(x) <_B f(y)\big).$$

Tulos seuraa nyt Apulauseen 6.6 kohdasta (a).

Lineaarijärjestystä ja hyvinjärjestystä koskevat väitteet todistetaan samaan tapaan. □

Seuraus 6.8 *Oletetaan, että $<$ on hyvinjärjestys joukossa A ja olkoon α struktuurin $\langle A, <\rangle$ $\in$-kuva. Tällöin $\in_\alpha$ on joukon α hyvinjärjestys.*

Ordinaaliluvut

Lause 6.9 *Jos $\langle A, <_A\rangle$ ja $\langle B, <_B\rangle$ ovat hyvinjärjestettyjä struktuureja, niin $\langle A, <_A\rangle \cong \langle B, <_B\rangle$ jos ja vain jos niillä on sama $\in$-kuva.*

Todistus. Oletetaan ensin, että struktuureilla $\langle A, <_A\rangle$ ja $\langle B, <_B\rangle$ on sama $\in$-kuva α. Tällöin $\langle A, <_A\rangle \cong \langle \alpha, \in_\alpha\rangle \cong \langle B, <_B\rangle$, joten $\langle A, <_A\rangle \cong \langle B, <_B\rangle$.

Oletetaan sitten, että $f : A \to B$ on isomorfismi. Olkoon $E_1 : A \to \alpha_1$ ja $E_2 : B \to \alpha_2$, missä α_1 on struktuurin $\langle A, <_A\rangle$ $\in$-kuva ja α_2 on struktuurin $\langle B, <_B\rangle$ $\in$-kuva, ja funktiot E_1 ja E_2 ovat aikaisemman määritelmän mukaisia isomorfismeja. Siis kaikilla $s \in A$ ja kaikilla $t \in B$ pätee

$$E_1(s) = \{E_1(x) \mid x <_A s\}$$
$$E_2(t) = \{E_2(y) \mid y <_B t\}.$$

Osoitetaan transfiniittisella induktiolla, että jokaisella $s \in A$ pätee

$$E_1(s) = E_2(f(s)).$$

Olkoon $C = \{s \in A \mid E_1(s) = E_2(f(s))\}$. Oletetaan, että $\operatorname{seg} s \subseteq C$. Tällöin

$$\begin{aligned}
E_1(s) &= \{E_1(x) \mid x <_A s\} \\
&\overset{\text{IO}}{=} \{E_2(f(x)) \mid x <_A s\} && (\operatorname{seg} s \subseteq C) \\
&= \{E_2(f(x)) \mid f(x) <_B f(s)\} && (f \text{ on isomorfismi}) \\
&= \{E_2(y) \mid y <_B f(s)\} && (f[\![\operatorname{seg} s]\!] = \operatorname{seg} f(s)) \\
&= E_2(f(s)).
\end{aligned}$$

Siis $s \in C$, joten C on $<_A$-induktiivinen.

Nyt voimme päätellä seuraavasti:

$$\begin{aligned}
\alpha_1 &= \{E_1(s) \mid s \in A\} \\
&= \{E_2(f(s)) \mid s \in A\} \\
&= \{E_2(t) \mid t \in B\} && (f \text{ on bijektio } A \to B) \\
&= \alpha_2
\end{aligned}$$

$\square$

Määritelmä 6.7 Olkoon $<$ hyvinjärjestys joukossa A. Struktuurin $\langle A, < \rangle$ *ordinaaliluku* on sen $\in$-kuva α.

Ordinaali (eli ordinaaliluku) on joukko, joka on jonkin hyvinjärjestetyn struktuurin ordinaaliluku.

Olkoon $<$ joukon A osittainen järjestys ja $C \subseteq A$. Järjestyksen $<$ rajoittuma joukkoon C määritellään seuraavasti

$$<^\circ \; = \; < \cap \, (C \times C).$$

Tällöin saadaan uusi struktuuri $\langle C, <^\circ \rangle$. Erityisesti jos $C = \operatorname{seg} t$ jollain $t \in A$, niin saadaan struktuurin rajoittuma $\langle \operatorname{seg} t, <^\circ \rangle$ alkusegmenttiin $\operatorname{seg} t$.

Lause 6.10 *Oletetaan, että $<$ on osittainen järjestys joukossa A ja $C \subseteq A$. Tällöin $<^\circ$ on joukon C osittainen järjestys. Edelleen jos $<$ on lineaarinen järjestys/hyvinjärjestys, niin $<^\circ$ on lineaarinen järjestys/hyvinjärjestys.*

Todistus. Joukon C identtinen funktio $\mathrm{id}_C : C \to A$ on injektio, joten väite seuraa apulauseesta 6.6. $\square$

Lause 6.11 *Jos* $\langle A, <_A \rangle$ *ja* $\langle B, <_B \rangle$ *ovat hyvinjärjestettyjä struktuureja, niin joko* $\langle A, <_A \rangle \cong \langle B, <_B \rangle$*, tai on olemassa* $t \in A$ *s.e.* $\langle \operatorname{seg} t, <_A \rangle \cong \langle B, <_B \rangle$*, tai on olemassa* $s \in B$ *s.e.* $\langle A, <_A \rangle \cong \langle \operatorname{seg} s, <_B \rangle$*.*

Todistus. Olkoon e alkio, joka ei kuulu joukkoon B. Määritellään transfiniitisella rekursiolla funktio $F : A \to B \cup \{e\}$:

$$F(t) = \begin{cases} \min(B \setminus F[\![\operatorname{seg} t]\!]), & \text{jos } B \setminus F[\![\operatorname{seg} t]\!] \neq \emptyset \\ e, & \text{jos } B \setminus F[\![\operatorname{seg} t]\!] = \emptyset \end{cases}$$

Nyt on kolme eri tapausta:

Tapaus 1. $e \in \operatorname{ran}(F)$.

Olkoon $a \in A$ pienin alkio, jolla $F(a) = e$.
Väite: tällöin $F^\circ = F \restriction \operatorname{seg} a$ on isomorfismi $\langle \operatorname{seg} a, <_A^\circ \rangle \to \langle B, <_B \rangle$.

Selvästi $F^\circ : \operatorname{seg} a \to B$ on funktio ja F° on surjektio, sillä muuten olisi $B \setminus F^\circ[\![\operatorname{seg} a]\!] \neq \emptyset$, jolloin $F(a) \in B$.

Edelleen

$$\begin{aligned} x \leq_A y <_A a &\Rightarrow F[\![\operatorname{seg} x]\!] \subseteq F[\![\operatorname{seg} y]\!] \\ &\Rightarrow B \setminus F[\![\operatorname{seg} y]\!] \subseteq B \setminus F[\![\operatorname{seg} x]\!] \\ &\Rightarrow F(x) \leq_B F(y). \end{aligned}$$

Jos $x <_A y <_A a$, niin $F(x) \neq F(y)$, koska $F(x) \in F[\![\operatorname{seg} y]\!]$, mutta $F(y) \neq F[\![\operatorname{seg} y]\!]$. Siis $F(x) <_B F(y)$.

Kääntäen, jos $x, y <_A a$ ja $F(x) < F(y)$, niin $F(y) \not\leq_B F(x)$, joten $y \not\leq_A x$ eli $x <_A y$.

Todetaan vielä, että F° on injektio: jos $x, y <_A a$ ja $x \neq y$, on joko $x <_A y$ tai $y <_A x$. Edellisessä tapauksessa $F(x) <_B F(y)$ ja jälkimmäisessä tapauksessa $F(y) <_B F(x)$; joka tapauksessa $F(x) \neq F(y)$.

Siispä F° on isomorfismi $\langle \operatorname{seg} a, <_A^\circ \rangle \cong \langle B, <_B \rangle$.

Tapaus 2. $\operatorname{ran}(F) = B$.

Tällöin samaan tapaan kuin edellä nähdään, että F on isomorfismi $\langle A, <_A \rangle \cong \langle B, <_B \rangle$.

Tapaus 3. $\operatorname{ran}(F) \subset B$.

Tällöin on olemassa $b \in B$ s.e. $\operatorname{ran}(F) = \operatorname{seg} b$ ja F on isomorfismi $\langle A, <_A \rangle \cong \langle \operatorname{seg} b, <_B^\circ \rangle$.

□

Määritelmä 6.8 Alkiorelaatio eli $\in$-relaatio *hyvinjärjestää* joukon A, jos $\in_A = \{\langle x, y \rangle \in A \times A \mid x \in y\}$ on joukon A hyvinjärjestys.

Lause 6.12 *Olkoon α transitiivinen joukko, jonka $\in$-relaatio hyvinjärjestää. Tällöin α on ordinaali. Itse asiassa α on oma $\in$-kuvansa.*

Todistus. Riittää osoittaa, että $E(x) = x$ jokaisella $x \in \alpha$, missä E on $\in$-kuvan määräävä funktio. Tällöin nimittäin pätee

$$ran(E) = \{E(x) \mid x \in \alpha\} = \{x \mid x \in \alpha\} = \alpha.$$

Todetaan aluksi, että $\operatorname{seg} t = t$: Jos $x \in_\alpha t$, niin $x \in t$, joten $\operatorname{seg} t \subseteq t$. Toisaalta, jos $x \in t$, niin joukon α transitiivisuuden perusteella $x \in \alpha$, jolloin pätee $x \in_\alpha t$. Siis myös $t \subseteq \operatorname{seg} t$.

Oletetaan sitten, että $E(x) = x$ pätee jokaisella $x \in \operatorname{seg} t$. Tällöin

$$\begin{aligned} E(t) &= \{E(x) \mid x \in_\alpha t\} \\ &= \{x \mid x \in_\alpha t\} \\ &= \operatorname{seg} t \\ &= t. \end{aligned}$$

Siis transfiniittisen induktion perusteella saadaan, että $E(x) = x$ pätee jokaisella $x \in \alpha$. □

Lause 6.13 *Olkoot α, β ja γ ordinaaleja. Tällöin pätee:*

(a) *Ordinaalien luokan transitiivisuus: jokainen α:n alkio on ordinaali.*
(b) *Ordinaalien transitiivisuus: $\alpha \in \beta \wedge \beta \in \gamma \Rightarrow \alpha \in \gamma$.*
(c) *Ordinaalien irrefleksiivisyys: $\alpha \notin \alpha$.*
(d) *Trikotomia: täsmälleen yksi vaihtoehdoista $\alpha \in \beta$, $\alpha = \beta$ ja $\beta \in \alpha$ on voimassa.*
(e) *Hyvinjärjestys: Jokaisessa joukossa $S \neq \emptyset$ ordinaaleja on pienin alkio μ: $\mu \in \alpha$ tai $\mu = \alpha$ jokaisella $\alpha \in S$.*

Todistus. (a) Oletetaan, että $x \in \alpha$. Koska α on jonkin hyvinjärjestetyn struktuurin $\langle A, < \rangle$ $\in$-kuva, on olemassa $t \in A$, jolla $x = E(t)$. Osoitetaan, että x on tällöin struktuurin $\langle segt, <^\circ \rangle$ $\in$-kuva.

Ensinnäkin $\langle segt, <^\circ \rangle$ on Lauseen 6.10 perusteella hyvinjärjestetty struktuuri. Edelleen on helppo todeta, että struktuurin $\langle segt, <^\circ \rangle$ $\in$-kuva on $E[\![\operatorname{seg} t]\!] = E(t) = x$. Siis x on ordinaali.

(b) Tämä väite seuraa suoraan siitä, että kaikki $\in$-kuvat ovat transitiivisia joukkoja (Lause 6.4 (c)).

(c) Vastaoletus: $\alpha \in \alpha$. Olkoon $\langle A, < \rangle$ hyvinjärjestetty struktuuri, jonka $\in$-kuva α on, ja olkoon E vastaava funktio $A \to \alpha$. Vastaoletuksen perusteella on olemassa $t \in A$, jolla $\alpha = E(t)$. Mutta tällöin pätee $E(t) \in E(t)$, mikä on ristiriidassa Lauseen 6.4 (a) kanssa.

(d) Trikotomian “korkeintaan yksi” -ehto seuraa helposti transitiivisuudesta ja irrefleksiivisyydestä. Osoitetaan sitten, että ainakin yksi ehdoista $\alpha \in \beta$, $\alpha = \beta$ ja $\beta \in \alpha$ pätee.

Tarkastellaan tätä varten hyvinjärjestettyjä struktuureja $\langle \alpha, \in_\alpha \rangle$ ja $\langle \beta, \in_\beta \rangle$. Lauseen 6.11 mukaan joko $\langle \alpha, \in_\alpha \rangle \cong \langle \beta, \in_\beta \rangle$, tai on olemassa $\delta \in \beta$, jolla $\langle \alpha, \in_\alpha \rangle \cong \langle \operatorname{seg} \delta, \in_\beta^\circ \rangle$, tai on olemassa $\delta \in \alpha$, jolla $\langle \operatorname{seg} \delta, \in_\alpha^\circ \rangle \cong \langle \beta, \in_\beta \rangle$. Ensimmäisessä tapauksessa $\alpha = \beta$, toisessa tapauksessa $\alpha \in \beta$ ja kolmannessa tapauksessa $\beta \in \alpha$. Jätämme yksityiskohdat harjoitustehtäväksi.

(e) Olkoon S epätyhjä joukko ordinaaleja. Valitaan jokin alkio $\beta \in S$. Jos $\beta \cap S = \emptyset$, niin $\beta = \min S$. Tällöin nimittäin jokaisella $\alpha \in S$ pätee $\alpha \notin \beta$, ja siis trikotomian perusteella $\beta \in \alpha$ tai $\beta = \alpha$.

Oletetaan sitten, että $\beta \cap S \neq \emptyset$. Koska $\in_\beta$ on joukon β hyvinjärjestys, tällöin joukossa $\beta \cap S$ on pienin alkio μ. Osoitetaan nyt, että $\mu = \min S$. Oletataan tätä varten, että $\alpha \in S$. Jos $\alpha \notin \beta$, pätee trikotomian perusteella $\beta \in \alpha$ tai $\beta = \alpha$, joten $\mu \in \alpha$. Jos taas $\alpha \in \beta$, niin $\alpha \in \beta \cap S$, joten $\mu \in \alpha$ tai $\mu = \alpha$ alkion μ minimaalisuuden perusteella. □

Huom. Lauseiden 6.12 ja 6.13 perusteella ordinaalin käsite voitaisiin määritellä yhtäpitävästi seuraavasti: joukko α on ordinaali, jos se on transitiivinen ja $\in$-relaatio hyvinjärjestää sen.

Käytämme jatkossa usein $\in$-symbolin sijasta tavallista järjestyksen symbolia $<$ puhuttaessa ordinaalien järjestyksestä.

Seuraus 6.14

(a) *Jokainen transitiivinen joukko ordinaaleja on ordinaali.*
(b) 0 *on ordinaali.*
(c) *Jos* α *on ordinaali, niin* $\alpha^+ = \alpha \cup \{\alpha\}$ *on oridinaali.*
(d) *Jos* A *on joukko ordinaaleja, niin* $\bigcup A$ *on ordinaali.*

Todistus.

(a) Lauseen 6.13 perusteella jokainen joukko A ordinaaleja on $\in$-relaatiolla hyvinjärjestetty. Jos A on lisäksi transitiivinen, se on ordinaali lauseen 6.12 perusteella.

(b) $0 = \emptyset$ on transitiivinen joukko ordinaaleja, joten 0 on ordinaali (a)-kohdan perusteella.

(c) Lauseen 4.5 mukaan, jos x on transitiivinen, niin myös x^+ on transitiivinen, joten α^+ on transitiivinen. Koska siis α^+:n alkiot ovat ordinaaleja, α^+ on ordinaali.

(d) Jos $x \in \bigcup A$, niin $x \in \alpha$, jollain $\alpha \in A$, joten lauseen 6.13 (a)-kohdan perusteella x on ordinaali. Siis $\bigcup A$ on joukko ordinaaleja.
$\bigcup A$ on transitiivinen:

$$\begin{aligned}
\delta \in A &\Rightarrow \delta \in \alpha \in A && \text{jollain } \alpha \in A \\
&\Rightarrow \delta \subseteq \alpha \in A && \text{koska } \alpha \text{ on transitiivinen} \\
&\Rightarrow \delta \subseteq \bigcup A
\end{aligned}$$

$\bigcup A$ on siis transitiivinen, joten edelleen (a)-kohdan perusteella se on ordinaali.

□

Edellisen lauseen (d)-kohdan voi vahvistaa muotoon: Jos A on joukko ordinaaleja, niin $\bigcup A = \sup A$: nimittäin $\alpha \leq \bigcup A$ jokaisella $\alpha \in A$, ja jos $\alpha \leq \beta$ jokaisella $\alpha \in A$, niin $\bigcup A \leq \beta$.

Huom. Kaikilla ordinaaleilla α ja β on voimassa

$$\begin{aligned}
\alpha < \beta &\Rightarrow \alpha \subset \beta && \text{koska } \beta \text{ on transitiivinen} \\
&\Rightarrow \beta \not\leq \alpha && \text{muuten olisi } \beta < \beta \\
&\Rightarrow \alpha < \beta && \text{trikotomian perusteella}
\end{aligned}$$

Siispä saamme ekvivalenssin $\alpha \in \beta \Leftrightarrow \alpha \subset \beta$.

Koska $\bigcup A$ on $\sup A$ osajoukkorelaation $\subset$ suhteen, ja $\subset$ on sama kuin järjestys $<$ ordinaalien luokassa, on $\bigcup A = \sup A$ edellä sanotulla tavalla.

Burali-Fortin lause. *Ei ole olemassa joukkoa, johon kaikki ordinaalit kuuluvat.*

Todistus. Jos tällainen joukko olisi olemassa, niin olisi olemassa myös joukko $\mathrm{Ord} = \{\alpha \mid \alpha \text{ on ordinaali}\}$.

Tällöin koska Ord on transitiivinen joukko ordinaaleja, lauseen 6.13 perusteella Ord olisi itsekin ordinaali. Siis $\mathrm{Ord} \in \mathrm{Ord}$. Tämä on ristiriidassa lauseen 6.13 (c)-kohdan kanssa. □

“Velkojen maksu”

Hartogsin lause. *Jokaisella joukolla A on olemassa ordinaali α, jolla $\alpha \not\preceq A$.*

Todistus. Olkoon A joukko. Asetetaan

$$W = \{\langle B, < \rangle \mid B \subseteq A \text{ ja } < \text{ on hyvinjärjestys joukossa } B\}.$$

W on joukko, sillä jos $\langle B, < \rangle \in W$, niin $\langle B, < \rangle \in \mathcal{P}(A) \times \mathcal{P}(A \times A)$. Siis $W \in \mathcal{P}(\mathcal{P}(A) \times \mathcal{P}(A \times A))$ ja W saadaan erotteluaksiooman avulla.

Olkoon

$$D = \{\beta \mid \beta \text{ on jonkin } \langle B, < \rangle \in W \in\text{-kuva}\}.$$

Korvausaksiooman perusteella D on joukko. Buralin–Fortin lauseen perusteella on olemassa ordinaali $\alpha \notin D$.

Osoitetaan nyt, että $\alpha \not\preccurlyeq A$.

Tehdään vastaoletus: $\alpha \preccurlyeq A$. Siis on olemassa injektio $f : \alpha \to A$. Olkoon $B = \operatorname{ran}(f)$. Määritellään relaatio $<$ joukossa B:

$$x < y \;\Leftrightarrow\; f^{-1}(x) \in f^{-1}(y) \;\text{ kun } x, y \in B.$$

Nyt f on isomorfismi $\langle \alpha, \in_\alpha \rangle \cong \langle B, < \rangle$. Siis $\langle B, < \rangle \in W$ ja hyvinjärjestyksen $\langle B, < \rangle$ $\in$-kuva on α. Siispä $\alpha \in D$, mikä on ristiriita. $\square$

Hyvinjärjestysperiaate (HP). *Jokaisella joukolla A on olemassa hyvinjärjestys.*

Todistus. Olkoon G joukon A valintafunktio (valinta-aksiooman kolmas muotoilu). Olkoon α ordinaali, jolla $\alpha \not\preccurlyeq A$.

Määritellään transfiniittisella rekursiolla funktio $F : \alpha \to A \cup \{e\}$, missä $e \notin A$:

$$F(\gamma) = \begin{cases} G(A \setminus F[\![\gamma]\!]), & \text{jos } A \setminus F[\![\gamma]\!] \neq \emptyset \\ e, & \text{jos } A \setminus F[\![\gamma]\!] = \emptyset, \end{cases}$$

kun $\gamma \in \alpha$.

Tällöin on olemassa $\delta \in \alpha$, jolla $F(\delta) = e$, koska muuten $F : \alpha \to A$ olisi injektio vastoin oletusta $\alpha \not\preccurlyeq A$.

Jos nimittäin $\gamma < \beta < \alpha$ ja $F(\gamma), F(\beta) \neq e$, niin $F(\beta) \in A \setminus F[\![\beta]\!]$, mutta $F(\gamma) \in F(\beta)$, joten $F(\gamma) \neq F(\beta)$.

Olkoon $\mu = \min\{\delta \in \alpha \mid F(\delta) = e\}$, ja olkoon $F^\circ = F \restriction \mu$. Korvaamalla edelisessä päättelyssä α ordinaalilla μ nähdään, että $F^\circ : \mu \to A$ on injektio. Selvästi F° on myös surjektio.

Funktion F° avulla voidaan nyt määritellä hyvinjärjestys joukkoon A asettamalla:

$$<_A = \{\langle F^\circ(\gamma), F^\circ(\beta) \rangle \mid \gamma < \beta < \mu\}.$$

Tällöin nimittäin F° on isomorfismi $\langle \mu, \in_\mu \rangle \to \langle A, <_A \rangle$. $\square$

Esimerkki 6.7 Reaalilukujen joukko $\mathbb{R}$ voidaan hyvinjärjestää.

“Numeraatio”lause. *Mikä hyvänsä joukko on yhtämahtava jonkin ordinaalin kanssa.*

Todistus. Olkoon A joukko. Hyvinjärjestysperiaatteesta seuraa, että on olemassa A:n hyvinjärjestys $<$. Olkoon α $\langle A, < \rangle$:n $\in$-kuva. Nyt selvästi $A \approx \alpha$. $\square$

Voimme nyt määritellä kardinaaliluvut:

Määritelmä 6.9 Olkoon A joukko. Tällöin

$$\mathrm{card}(A) = \text{ pienin ordinaali } \alpha \text{, jolla } A \approx \alpha$$

Apulause 6.15

(a) *Kaikilla joukoilla A ja B pätee ekvivalenssi:* $\mathrm{card}(A) = \mathrm{card}(B) \;\Leftrightarrow\; A \approx B$.

(b) *Jokaisella äärellisellä joukolla A* $\mathrm{card}(A)$ *on se yksikäsitteinen luonnollinen luku n, jolla $n \approx A$.*

Todistus. (a) Suoraan määritelmän perusteella $\mathrm{card}(A) \approx A$ jokaisella joukolla A. Jos siis $\mathrm{card}(A) = \mathrm{card}(B)$, niin $A \approx \mathrm{card}(A) = \mathrm{card}(B) \approx B$, joten $A \approx B$.

Kääntäen, jos $A \approx B$, niin A ja B ovat yhtämahtavia täsmälleen samojen ordinaalien kanssa. Siis myös pienin ordinaali, joka on yhtämahtava joukon A kanssa, on samalla pienin ordinaali, joka on yhtämahtava joukon B kanssa.

(b) Harjoitustehtävä. $\square$

Hyvinjärjestysperiaatteen avulla voimme nyt todistaa valinta-aksioomien eri muotoilujen yhtäpitävyyden loppuun.

Lauseen 5.14 todistuksen loppu. Koska todistettiin jo, että $(3) \Rightarrow (HP)$, riittää toditaa, että $(5) \Rightarrow (HP)$ ja $(HP) \Rightarrow (6)$:

$$\begin{tikzcd}
(5) \arrow[dr, Rightarrow, dashed] & (6) \arrow[l, Rightarrow] \arrow[r, Rightarrow] & (1) \arrow[r, Rightarrow] & (2) \arrow[d, Rightarrow] \\
 & (HP) \arrow[u, Rightarrow, dashed] & (3) \arrow[l, Rightarrow] \arrow[u, Rightarrow] & (4) \arrow[l, Rightarrow]
\end{tikzcd}$$

$(5) \Rightarrow$ (HP): Olkoon A joukko ja α ordinaali, jolla $\alpha \not\preccurlyeq A$. Oletuksen (5) perusteella pätee, että $A \preccurlyeq \alpha$. Olkoon $f : A \to \alpha$ injektio. Määritellään joukon A relaatio $<_A$ asettamalla

$$<_A = \{\langle x, y \rangle \in A \times A \mid f(x) < f(y)\}$$

Nyt apulauseen 6.6 perusteella $<_A$ on joukon A hyvinjärjestys.

(HP) $\Rightarrow$ (6): Olkoon $\mathcal{A}$ joukko, joka on suljettu ketjujen yhdisteiden suhteen. Olkoon $<_{\mathcal{A}}$ hyvinjärjestys joukossa $\mathcal{A}$.

Määritellään transfiniittisella rekursiolla funktio $F : \mathcal{A} \to 2 = \{0, 1\}$ seuraavasti:

$$F(A) = \begin{cases} 1, & \text{jos } \forall B \in \mathcal{A}\big((B <_{\mathcal{A}} A \wedge F(B) = 1) \to B \subset A\big) \\ 0, & \text{muuten} \end{cases}$$

Olkoon $\mathcal{C} = \{A \in \mathcal{A} \mid F(A) = 1\}$.

Nyt $\mathcal{C}$ on ketju: jos $A, B \in \mathcal{C}$, niin $A <_{\mathcal{A}} B$ (tai $B <_{\mathcal{A}} A$) ja siis funktion F määritelmän mukaisesti $A \subset B$ (tai $B \subset A$).

Olkoon $C = \bigcup \mathcal{C} \in \mathcal{A}$. Jos $C \subseteq D \in \mathcal{A}$, niin $B \subset D$ jokaisella $B <_{\mathcal{A}} D$, jolla $F(B) = 1$, joten määritelmän mukaan $F(D) = 1$, eli $D \in \mathcal{C}$. Siis $D \subseteq \bigcup \mathcal{C} = C$. Siispä C on joukon $\mathcal{A}$ maksimaalinen alkio. $\square$

Määritelmä 6.10 Ordinaali α on *alkuordinaali*, jos $\alpha \not\approx \beta$ kaikilla $\beta \in \alpha$.

Jokainen kardinaali on alkuordinaali. Samoin jokainen alkuordinaali α on kardinaali, nimittäin $\mathrm{card}(\alpha) = \alpha$.

Myös kardinaalit on hyvinjärjestetty $\in$-relaatiolla: jos κ ja λ ovat kardinaaleja, niin voidaan päätellä seuraavasti:

$$\begin{aligned} \kappa \in \lambda &\Rightarrow \kappa \subset \lambda \\ &\Rightarrow \kappa \preccurlyeq \lambda \wedge \kappa \neq \lambda \\ &\Rightarrow \kappa \leq \lambda \wedge \kappa \neq \lambda \\ &\Rightarrow \kappa < \lambda. \end{aligned}$$

Toisaalta voidaan myös päätellä:

$$\begin{aligned} \kappa \notin \lambda &\Rightarrow \lambda \in \kappa \vee \lambda = \kappa \\ &\Rightarrow \lambda \leq \kappa \\ &\Rightarrow \kappa \not< \lambda. \end{aligned}$$

Siis on voimassa ekvivalenssi $\kappa < \lambda \Leftrightarrow \kappa \in \lambda$.

Edelleen kardinaalien järjestys on hyvinjärjestys: jokaisessa epätyhjässä joukossa kardinaaleja on pienin kardinaali.

Kardinaalien jono:

$$0 < 1 < 2 < \ldots < \underset{\omega}{\overset{\shortparallel}{\aleph_0}} < \ldots$$

$$0 < 1 < 2 < \ldots < \overset{\substack{\omega \\ \shortparallel}}{\aleph_0} < \overset{\substack{2^{\aleph_0} \\ \shortparallel\,(CH)}}{\aleph_1} < \aleph_2 < \ldots < \aleph_\omega < \ldots < \aleph_\alpha < \ldots$$

Kumulatiivisen hierarkian tasot

Kumulatiivisen hierarkian idea: $V_0 = \emptyset$, ja yleisemmin V_α sisältää ne joukot, joiden alkiot ovat joukossa V_β jollain $\beta \in \alpha$.

Muotoillaan tämä idea vielä uudelleen seuraavasti:

$$\begin{aligned} a \in V_\alpha &\Leftrightarrow a \subseteq V_\beta \text{ jollain } \beta \in \alpha \\ &\Leftrightarrow a \in \mathcal{P}(V_\beta) \text{ jollain } \beta \in \alpha \\ &\Leftrightarrow a \in \bigcup_{\beta \in \alpha} \mathcal{P}(V_\beta). \end{aligned}$$

Siis intuitiivisesti kumulatiivisen hierarkian taso V_α on joukko

$$V_\alpha = \bigcup \{\mathcal{P}(V_\beta) \mid \beta \in \alpha\}.$$

Tämä määritelmä voidaan tehdä täsmälliseksi transfiniittisella rekursiolla. On kuitenkin huomattava, että transifiniittinen rekursio pitää aina tehdä jonkin joukon hyvinjärjestyksen suhteen; sitä ei voi tehdä ordinaalien luokan suhteen. Siksi tasot V_α määritellään ensin johonkin ylärajaan δ asti.

Apulause 6.16 *Jokaisella ordinaalilla δ on olemassa yksikäsitteinen funktio F_δ s.e.* $\mathrm{dom}(F_\delta) = \delta$ *ja jokaisella $\alpha \in \delta$ pätee:*

$$F_\delta(\alpha) = \bigcup \{\mathcal{P}(F_\delta(\beta)) \mid \beta \in \alpha\}$$

Todistus. Käytetään transfiniittista rekursiota. Olkoon $\gamma(x, y)$ kaava

$$y = \bigcup \{\mathcal{P}(z) \mid z \in \mathrm{ran}(x)\}.$$

Selvästi jokaisella f on olemassa yksikäsitteinen joukko y, jolla $\gamma(f, y)$ on tosi. Transfiniittinen rekursio antaa yksikäsitteisen funktion F_δ, jolla pätee

$$F_\delta(\alpha) = \bigcup \{\mathcal{P}(z) \mid z \in \mathrm{ran}(F_\delta \restriction \mathrm{seg}\, \alpha)\}$$

jokaisella $\alpha \in \delta$. Koska $\mathrm{seg}\, \alpha = \alpha$ jokaisella ordinaalilla α, nähdään, että

$$z \in \mathrm{ran}(F_\delta \restriction \mathrm{seg}\, \alpha) \;\Leftrightarrow\; z = F_\delta(\beta) \text{ jollain } \beta \in \alpha.$$

Siispä $F_\delta(\alpha) = \bigcup \{\mathcal{P}(F_\delta(\beta)) \mid \beta \in \alpha\}$, niin kuin pitääkin. □

Apulause 6.17 *Olkoot δ ja ε ordinaaleja ja olkoot F_δ ja F_ε funktioita kuten apulauseessa 6.16. Tällöin $F_\delta(\alpha) = F_\varepsilon(\alpha)$, jokaisella $\alpha \in \delta \cap \varepsilon$.*

Todistus. Oletetaan, että $\delta < \varepsilon$; tapaus $\varepsilon < \delta$ menee samoin, ja tapaus $\delta = \varepsilon$ on triviaali. Osoitetaan transfiniittisella induktiolla, että $F_\delta(\alpha) = F_\varepsilon(\alpha)$ jokaisella $\alpha \in \delta$.

Olkoon $B = \{\alpha \in \delta \mid F_\delta(\alpha) = F_\varepsilon(\alpha)\}$. Oletetaan, että $\operatorname{seg}\alpha \subseteq B$. Pitää osoittaa, että tällöin $\alpha \in B$. Oletuksesta seuraa, että $F_\delta(\beta) = F_\varepsilon(\beta)$ jokaisella $\beta < \alpha$. Siispä

$$F_\delta(\alpha) = \bigcup\{\mathcal{P}(F_\delta(\beta)) \mid \beta < \alpha\} = \bigcup\{\mathcal{P}(F_\varepsilon(\beta)) \mid \beta < \alpha\} = F_\varepsilon(\alpha),$$

joten $\alpha \in B$. □

Määritelmä 6.11 Olkoon α ordinaali. Tällöin kumulatiivisen hierarkian vastaava taso on joukko

$$V_\alpha = F_\delta(\alpha),$$

missä δ on mikä hyvänsä ordinaali, jolla $\alpha \in \delta$ (esimerkiksi $\delta = \alpha^+$ kelpaa).

Lause 6.18 *Jokaisella ordinaalilla α*

$$V_\alpha = \bigcup\{\mathcal{P}(V_\beta) \mid \beta \in \alpha\}.$$

Todistus. Olkoon $\delta = \alpha^+$. Tällöin määritelmän mukaan $V_\alpha = F_\delta(\alpha)$, ja myös $V_\beta = F_\delta(\beta)$ jokaisella $\beta < \alpha$. Siispä

$$V_\alpha = \bigcup\{\mathcal{P}(F_\delta(\beta)) \mid \beta < \alpha\} = \bigcup\{\mathcal{P}(V_\beta) \mid \beta < \alpha\}.$$

□

Apulause 6.19 *V_α on transitiivinen joukko jokaisella ordinaalilla α.*

Todistus. Todistetaan jokaisella ordinaalilla δ, että jos $\alpha < \delta$, niin $V_\alpha = F_\delta(\alpha)$ on transitiivinen. Tämä tehdään transfiniittisella induktiolla hyvinjärjestyksen $\langle \delta, \in_\delta \rangle$ suhteen.

Olkoon

$$B = \{\alpha < \delta \mid V_\alpha \text{ on transitiivinen}\}.$$

Osoitetaan, että B on $\in_\delta$-induktiivinen, jolloin transfiniittisen induktioperiaatteen nojalla $B = \delta$.

Oletetaan siis, että $\operatorname{seg}\alpha \subseteq B$. (Huomaa, että $\operatorname{seg}\alpha = \alpha$.) Tällöin jokaisella $\beta < \alpha$ V_β on transitiivinen. Samoin jokainen $\mathcal{P}(V_\beta)$ on transitiivinen, sillä jokaisen transitiivisen joukon potenssijoukko on transitiivinen (harjoitustehtävä).

Nyt voimme päätellä seuraavasti:

$$\begin{aligned} x \in V_\alpha &\Rightarrow x \in \mathcal{P}(V_\beta) \text{ jollain } \beta < \alpha \\ &\Rightarrow x \subseteq \mathcal{P}(V_\beta) \text{ jollain } \beta < \alpha \\ &\Rightarrow x \subseteq \bigcup \{\mathcal{P}(V_\beta) \mid \beta < \alpha\} = V_\alpha. \end{aligned}$$

Siis V_α on transitiivinen, joten $\alpha \in B$. □

Ordinaali δ on *rajaordinaali*, jos se ei ole 0 eikä minkään muun ordinaalin α seuraaja α^+. Ordinaaleja on siis kolmea tyyppiä:

- 0,
- *seuraajaordinaalit* α^+,
- *rajaordinaalit*, esimerkiksi ω.

Huomaa, että jos δ on *rajaordinaali* ja $\beta < \delta$, niin $\beta^+ < \delta$.

Lause 6.20

(a) *Kaikilla ordinaaleilla β ja α pätee: $\beta < \alpha \Rightarrow V_\beta \subseteq V_\alpha$.*
(b) $V_0 = \emptyset$
(c) $V_{\alpha^+} = \mathcal{P}(V_\alpha)$
(d) $V_\delta = \bigcup_{\beta<\delta} V_\beta$, *kun δ on rajaordinaali.*

Todistus.

(a) Oletetaan, että $\beta < \alpha$. Tällöin $V_\beta \in \mathcal{P}(V_\beta) \subseteq V_\alpha$ $(= \bigcup_{\gamma\in\alpha} \mathcal{P}(V_\gamma))$. Siis $V_\beta \in V_\alpha$, joten $V_\beta \subseteq V_\alpha$, koska V_α on transitiivinen.

(b) Seuraa suoraan määritelmästä.

(c) (a)-kohdan perusteella:

$$\beta < \alpha \Rightarrow V_\beta \subseteq V_\alpha \Rightarrow \mathcal{P}(V_\beta) \subseteq \mathcal{P}(V_\alpha).$$

Täten

$$V_{\alpha^+} = \bigcup \{\mathcal{P}(V_\beta) \mid \beta \leq \alpha\} = \mathcal{P}(V_\alpha).$$

(d) Osoitetaan ensin, että $V_\delta \subseteq \bigcup_{\beta<\delta} V_\beta$:

$$\begin{aligned} x \in V_\delta &\Rightarrow x \in \mathcal{P}(V_\beta) && \text{jollain } \beta < \delta \\ &\overset{(c)}{\Rightarrow} x \in V_{\beta^+} && \text{jollain } \beta < \delta \\ &\Rightarrow x \in \bigcup_{\beta<\delta} V_\beta && \text{koska } \beta^+ < \delta. \end{aligned}$$

Osoitetaan sitten, että $\bigcup_{\beta<\delta} V_\beta \subseteq V_\delta$:

$$\begin{aligned} x \in \bigcup_{\beta<\delta} V_\beta &\Rightarrow x \in V_\beta \subseteq V_{\beta^+} = \mathcal{P}(V_\beta) && \text{jollain } \beta < \delta \\ &\Rightarrow x \in V_\delta. \end{aligned}$$

□

Määritelmä 6.12 Joukko A on *hyvinperustettu*, jos $A \subseteq V_\alpha$ jollain ordinaalilla α. Tällöin joukon A *aste*, $\text{rank}(A)$, on pienin ordinaali α, jolla tämä pätee.

Jokaisella hyvinperustetulla joukolla A pätee siis $A \subseteq V_{\text{rank}(A)}$, ja edelleen $A \in V_{\text{rank}(A)^+}$. Ordinaali $\text{rank}(A)$ kertoo, kuinka monta kertaa potenssijoukko-operaatiota pitää soveltaa lähtien tyhjästä joukosta, jotta kaikki joukon A alkiot saadaan muodostetuksi.

Jokainen ordinaali α on hyvinperustettu, ja $\text{rank}(\alpha) = \alpha$ (harjoitustehtävä).

Lause 6.21 *(a) Jos joukko A on hyvinperustettu, ja $a \in A$, niin myös a on hyvinperustettu ja* $\text{rank}(a) < \text{rank}(A)$.

(b) Jos jokainen joukon A alkio on hyvinperustettu, niin myös A on hyvinperustettu, ja $\text{rank}(A) = \bigcup\{(\text{rank}(a))^+ \mid a \in A\}$.

Todistus. (a) Oletetaan, että joukko A on hyvinperustettu, ja $a \in A$. Olkoon $\alpha = \text{rank}(A)$. Tällöin $A \subseteq V_\alpha$, joten $a \in V_\alpha$. Siis on olemassa $\beta < \alpha$, jolla $a \in \mathcal{P}(V_\beta)$, eli $a \subseteq V_\beta$. Tästä jo seuraakin, että a on hyvinperustettu, ja $\text{rank}(a) \leq \beta < \alpha = \text{rank}(A)$.

(b) Oletetaan, että kaikki joukon A alkiot ovat hyvinperustettuja. Määritellään ordinaali α asettamalla

$$\alpha = \bigcup\{(\text{rank}(a))^+ \mid a \in A\}.$$

Osoitetaan ensin, että $A \subseteq V_\alpha$; tästä seuraa, että A on hyvinperustettu, ja $\text{rank}(A) \leq \alpha$. Oletetaan siis, että $a \in A$; pitää osoittaa, että tällöin $a \in V_\alpha$. Tämä nähdään seuraavasti:

$$a \subseteq V_{\text{rank}(a)} \;\Rightarrow\; a \in V_{(\text{rank}(A))^+} \;\Rightarrow\; a \in V_\alpha.$$

Vielä pitää osoittaa, että $\alpha \leq \text{rank}(A)$. Kohdan (a) perusteella kaikilla $a \in A$ pätee $\text{rank}(a) < \text{rank}(A)$, ja näin ollen $(\text{rank}(a))^+ \leq \text{rank}(A)$. Siispä

$$\text{rank}(A) \geq \sup\{(\text{rank}(a))^+ \mid a \in A\} = \alpha.$$

□

Lause 6.22 *Seuraavat ehdot ovat yhtäpitävät:*

(a) *Jokainen joukko on hyvinperustettu.*
(b) *Jokaisella epätyhjällä joukolla A on alkio m, jolla $m \cap A = \emptyset$.*

Todistus. Täydennetään myöhemmin. □

Koska joukko-opin tavallisena lähtökohtana on ajatus, että kaikki joukot ovat kumulatiivisessa hierarkiassa, ja siten hyvinperustettuja, otetaan edellisen lauseen jälkimmäinen ehto yhdeksi joukko-opin aksioomaksi:

Säännöllisyysaksiooma

$$\forall A(A \neq \emptyset \rightarrow \exists m \in A(m \cap A = \emptyset))$$

Säännöllisyysaksioomasta seuraa, että mikään joukko ei ole itsensä alkio, eikä ole olemassa ääretöntä jonoa joukkoja, jotka muodostavat laskevan $\in$-ketjun:

Lause 6.23 *(a) Ei ole olemassa joukkoa a, jolla $a \in a$.*

(b) Ei ole olemassa joukkoja a ja b, joilla $a \in b$ ja $b \in a$.

(c) Ei ole olemassa funktiota f, jolla $\mathrm{dom}(f) = \omega$ *ja $f(n^+) \in f(n)$ jokaisella $n \in \omega$.*

Todistus. Todistus jätetään harjoitustehtäväksi. □

Luku 7

Ordinaalit ja järjestystyypit

Transfiniittisen rekursio ordinaalien suhteen

Olkoon G *luokkafunktio*, jonka määrittelyluokka on kaikkien joukkojen luokka V: siis G on luokka järjestettyjä pareja, ja jokaisella joukolla x on olemassa täsmälleen yksi joukko y, jolla $\langle x, y\rangle \in G$. Tarkoituksena on osoittaa, että tällöin on olemassa yksikäsitteinen luokkafunktio F, jonka määrittelyluokka on Ord, ja jolla on voimassa rekursioehto

$$F(\alpha) = G(F \restriction \alpha)$$

jokaisella $\alpha \in \mathrm{Ord}$. Huomaa, että tämä ei seuraa edellisen luvun transfiniittsestä rekursiolauseesta. Tämä lause koskee vain rekursiota jossakin joukossa määritellyn hyvinjärjestyksen suhteen, mutta Ord on aito luokka.

Koska aitoja luokkia ei esiinny joukko-opin kaavoissa, muotoillaan tämä transfiniittinen rekursio luokan Ord suhteen uudelleen niin, että luokkafunktiot G ja F korvataan vastaavilla kaavoilla $\gamma(x, y)$ ja $\varphi(x, y)$. Siis pari $\langle x, y\rangle$ on luokassa G jos ja vain jos kaava $\gamma(x, y)$ on tosi (ja vastaavasti luokalle F ja kaavalle φ). Yhtälö

$$F(\alpha) = G(F \restriction \alpha)$$

korvataan tällöin seuraavalla ilmauksella: jos f on funktio, jonka määrittelyjoukko on $\alpha \in \mathrm{Ord}$, ja jolla kaava $\varphi(\beta, f(\beta))$ pätee kaikilla $\beta \in \alpha$, niin tällöin se yksikäsitteinen y, jolla $\varphi(\alpha, y)$ pätee, on sama kuin se yksikäsitteinen z, jolla $\gamma(f, z)$ pätee.

Transfiniittinen rekursioskeema. *Olkoon $\gamma(x, y)$ joukko-opin kaava, jolla pätee ehto: kaikilla joukoilla f on olemassa yksikäsitteinen joukko y, jolla $\gamma(f, y)$ on tosi. Tällöin voidaan muodostaa joukko-opin kaava $\varphi(u, v)$ siten, että seuraava väite on tosi.*

Jokaisella ordinaalilla α on olemassa yksikäsitteinen y, jolla $\varphi(\alpha, y)$ on tosi. Lisäksi jos f on funktio, jolla $\mathrm{dom}(f) = \alpha \in \mathrm{Ord}$, ja jolla $\varphi(\beta, f(\beta))$ pätee kaikilla $\beta \in \alpha$, niin jokaisella joukolla y on voimassa

$$\varphi(\alpha, y) \quad \textit{jos ja vain jos} \quad \gamma(f, y).$$

Ennen kuin todistamme Transfiniittisen rekursioskeeman, valaisemme sitä esimerkin avulla. Otetaan ensin käyttöön apumerkintä:

$$t_\alpha \text{ on se yksikäsitteinen } y \text{, jolla } \varphi(\alpha, y).$$

Tällöin operaatio, jolla α kuvataan joukoksi t_α, on γ-konstruoitu seuraavassa mielessä: Aina kun f on tämän operaation rajoittuma johonkin ordinaaliin α (eli $\mathrm{dom}(f) = \alpha$ ja $f(\beta) = t_\beta$ jokaisella $\beta \in \alpha$), niin rekursioskeeman perusteella pätee $\gamma(f, t_\alpha)$. Tämä voidaan myös ilmaista lyhyesti kaavana $\gamma(t \restriction \alpha, t_\alpha)$.

Esimerkki 7.1 Kumulatiivinen hierarkia saadaan operaatiolla $\alpha \mapsto V_\alpha$. Tässä kaava $\gamma(f, y)$ on

$$y = \bigcup\{\mathcal{P}(z) \mid z \in \mathrm{ran}(f)\}.$$

Jos f on tämän operaation rajoittuma johonkin ordinaaliin α, niin $f(\beta) = V_\beta$ jokaisella $\beta \in \alpha$. Rekursioyhtälö voidaan siis kirjoittaa muotoon

$$V_\alpha = \bigcup\{\mathcal{P}(z) \mid z \in \mathrm{ran}(f)\} = \bigcup\{\mathcal{P}(V_\beta) \mid \beta \in \alpha\},$$

joten tuoksena on sama määritelmä joukoille V_α, kuin edellisessäkin luvussa.

Aalefit

Ordinaalioperaatiot

Ordinaalioperaatio on luokkafunktio, joka liittää jokaiseen ordinaaliin α ordinaalin t_α.

Ordinaalioperaatioiden ominaisuuksia:

- Operaatio $\alpha \mapsto t_\alpha$ on *monotoninen*, jos

$$\alpha \in \beta \;\Rightarrow\; t_\alpha \in t_\beta.$$

- Operaatio on *jatkuva*, jos

$$t_\delta = \bigcup_{\beta \in \delta} t_\beta, \text{ jokaisella rajaordinaalilla } \delta.$$

- Operaatio $\alpha \mapsto t_\alpha$ on *normaali operaatio*, jos se on sekä monotoninen että jatkuva.

Esimerkki 7.2 Operaatio $\alpha \mapsto \alpha^+$

(a) on monotoninen: jos $\alpha \in \beta$, niin $\alpha^+ \in \beta^+$ (harjoitustehtävä)
(b) ei ole jatkuva: $\bigcup_{n \in \omega} n^+ = \omega \neq \omega^+$

Esimerkki 7.3 $\alpha \mapsto \aleph_\alpha$ on normaali operaatio.

Huomautus.

$$\bigcup_{\alpha\in\lambda} t_\alpha = \sup\{t_\alpha \mid \alpha \in \lambda\}$$

Täten yhtäpitävä ehto jatkuvuudelle on $t_\lambda = \sup\{t_\beta \mid \beta \in \lambda\}$.

Lause 7.1 *Oletetaan, että $\alpha \mapsto t_\alpha$ on jatkuva operaatio. Jos jokaisella γ pätee, että $t_\gamma \in t_{\gamma^+}$, niin operaatio on monotoninen.*

Todistus. Todistetaan lause transfiniittisella induktiolla β:n suhteen:

$$\alpha \in \beta \Rightarrow t_\alpha \in t_\beta.$$

(1) $\beta = 0$: ei ole mitään todistettavaa.

(2) $\beta = \gamma^+$: Tällöin

$$\begin{aligned} \alpha \in \beta \quad &\Rightarrow \quad \alpha \Subset \gamma \\ &\overset{\text{ind. ol.}}{\Rightarrow} \quad t_\alpha \Subset t_\gamma \\ &\Rightarrow \quad t_\alpha \in t_{\gamma^+} = t_\beta \end{aligned}$$

(3) β on rajaordinaali: Tällöin

$$\begin{aligned} \alpha \in \beta &\Rightarrow \alpha \in \alpha^+ \in \beta \\ &\Rightarrow t_\alpha \in t_{\alpha^+} \Subset t_\beta \quad (t_\beta \text{ on supremum}) \end{aligned}$$

$\square$

Lause 7.2 *Olkoon $\alpha \mapsto t_\alpha$ normaali operaatio. Silloin jokaisella β, jos $t_0 \Subset \beta$, niin on olemassa suurin γ s.e. $t_\gamma \Subset \beta$.*

Toisin sanoen joukossa $\{\gamma \mid t_\gamma \Subset \beta\}$ on olemassa suurin alkio.

Todistus. Monotonisuuden perusteella $\{\alpha \mid t_\alpha \Subset \beta\}$ on transitiivinen joukko, joten se on ordinaali. Olkoon $\lambda = \{\alpha \mid t_\alpha \Subset \beta\}$. Jos $\lambda = \gamma^+$, niin t_γ on joukon $\{t_\alpha \mid t_\alpha \Subset \alpha\}$ suurin alkio.

λ ei voi olla rajaordinaali, sillä muuten olisi

$$t_\lambda = \sup\{t_\lambda \mid \alpha \in \lambda\} \Subset \beta,$$

joten $t_\lambda \in \{t_\alpha \mid \alpha \Subset \beta\}$ eli $\lambda \in \lambda$, mikä on ristiriita. $\square$

Lause 7.3 *Olkoon $\alpha \mapsto t_\alpha$ normaali operaatio ja $S \neq \emptyset$. Tällöin*

$$t_{\sup S} = \sup\{t_\alpha \mid \alpha \in S\}.$$

Todistus. Jos $\alpha \in S$, niin $\alpha \leq \sup S$, joten monotonisuuden perusteella pätee $t_\alpha \leq t_{\sup S}$. Koska tämä pätee jokaisella joukon S alkiolla α, nähdään, että

$$\sup\{t_\alpha \mid \alpha \in S\} \leq t_{\sup S}.$$

Osoitetaan sitten käänteinen epäyhtälö. Jos joukossa S on suurin ordinaali γ, on

$$t_{\sup S} = t_\gamma \leq \sup\{t_\alpha \mid \alpha \in S\}.$$

Oletetaan sitten, että joukossa S ei ole suurinta ordinaalia. Tällöin $\sup S$ on rajaordinaali, joten jatkuvuuden perusteella pätee $t_{\sup S} = \sup\{t_\beta \mid \beta \in \sup S\}$. Jos $\beta \in \sup S$, niin on olemassa $\gamma \in S$, jolla $\beta \in \gamma$. Monotonisuudesta seuraa, että $t_\beta \in t_\gamma$, joten $t_\beta \in \sup\{t_\alpha \mid \alpha \in S\}$. Koska tämä pätee kaikilla $\beta \in \sup S$, saadaan lopulta

$$t_{\sup S} = \sup\{t_\beta \mid \beta \in \sup S\} \leq \sup\{t_\alpha \mid \alpha \in S\}.$$

$\square$

Onko mahdollista, että jollain β, $t_\beta = \beta$?

Tällöin β on operaation $\alpha \mapsto t_\alpha$ *kiintopiste*.

Veblenin kiintopistelause. *Oletetaan, että $\alpha \mapsto t_\alpha$ on normaali operaatio. Tällöin operaatiolla on mielivaltaisen suuria kiintopisteitä: jokaisella β on olemassa γ s.e. $\beta \subseteq \gamma$ ja $t_\gamma = \gamma$.*

Todistus. Idea:

$$\overset{t^0_\beta}{\beta} \mapsto \overset{t^1_\beta}{t_\beta} \mapsto \overset{t^2_\beta}{t_{t_\beta}} \mapsto \cdots$$

Huomautus. $\delta \subseteq t_\delta$ jokaisella δ.

Jos $\beta = t_\beta$, niin $\gamma = \beta$ kelpaa.

Oletetaan sitten $\beta \in t_\beta$. Monotonisuuden perusteella $t_\beta \in t_{t_\beta}$ jne.

Merkitään $t^\circ_\beta = \beta$, $t^{n^+}_\beta = t_{t^n_\beta}$.

Olkoon $\lambda = \sup\{t^n_\beta \mid n \in \omega\}$

Osoitetaan, että $t_\lambda = \lambda$.

Selvästi λ on rajaordinaali: λ ei voi olla suraajaodinaali, sillä $t^n_\beta \in t^{n^+}_\beta$ jokaisella $n \in \omega$. Lauseesta 7.1 seuraa, että $t_\lambda = \sup\{t_\alpha \mid \alpha \in s\}$, missä $s = \{t^n_\beta \mid n \in \omega\}$.

Siis

$$t_\lambda = \sup\{t^{n^+}_\beta \mid n \in \omega\} = \sup\{t^n_\beta \mid n \in \omega\} = \lambda.$$

$\square$

Esimerkki 7.4 $\aleph$-jonon kiintopiste:

$$0 \in \aleph_0 \in \aleph_{\aleph_0} \in \cdots$$

Isomorfismityypit ja järjestysaritmetiikka

Isomorfismityypit:

$$\mathrm{it}\langle A, R\rangle = \mathrm{it}\langle B, S\rangle \Leftrightarrow \langle B, S\rangle \cong \langle A, R\rangle$$

Tässä oletetaan, että jokaiseen struktuuriin $\langle A, R\rangle$ voidaan liittää sen isomorfiatyypit siten että funktio it voidaan määritellä täsmällisesti.

Määritelmä 7.1 *Järjestystyyppi* on lineaarijärjestyksen isomorfiatyyppi.

Järjestystyyppejä merkitään kirjaimilla ρ, σ, τ ja η.

Järjestysten yhteenlasku
$\rho+\tau$ määritellään valitsemalla ensin $\langle A,\ R\rangle$ ja $\langle B, S\rangle$ s.e. $\mathrm{it}\langle A, R\rangle = \rho$, $\mathrm{it}\langle B, S\rangle = \tau$ ja $A \cap B = \emptyset$.

Määritellään, että

$$R \oplus S = R \cup S \cup (A \times B).$$

Nyt $\rho + \tau = \mathrm{it}\langle A \cup B, R \oplus S\rangle$.

Selvästi $R \oplus S$ on $A \cup B$:n lineaarinen järjestys.

Jos $\langle A, R\rangle \cong \langle A', R'\rangle$ ja $\langle B, S\rangle \cong \langle B', S'\rangle$, niin

$$\langle A \cup B, R \oplus S\rangle \cong \langle A' \cup B', R' \oplus S'\rangle,$$

joten yhteenlasku on hyvinmääritelty.

Ordinaalilla α merkitään $\mathrm{it}\langle \alpha, \in_\alpha\rangle = \overline{\alpha}$.

Esimerkki 7.5

- $\overline{1} + \overline{\omega} = \overline{\omega}$
- $\overline{\omega} + \overline{1} = \overline{\omega}^+ = \overline{\omega + 1}$
- Merkitään $\eta = \mathrm{it}\langle \mathbb{Q}, <\rangle$:

$$\overline{1} + \eta = \mathrm{it}\langle \mathbb{Q} \cup \{0\}, <\rangle.$$

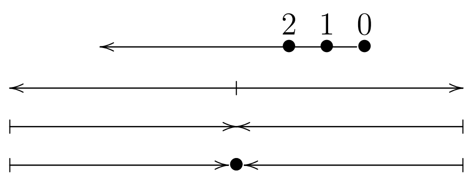
- $\eta + \overline{1} + \eta = \eta$
- $\eta + \eta = \eta$

Jos $\langle A, R\rangle$ on lineaarijärjestys, niin myös $\langle A, R^{-1}\rangle$ on lineaarijärjestys.

Merkitään: Jos $\mathrm{it}\langle A, R\rangle = \delta$, niin $\delta^* = \mathrm{it}\langle A, R^{-1}\rangle$.

Esimerkki 7.6

- $\overline{\omega}^*$:
- $\overline{\omega}^* + \overline{\omega} = \mathrm{it}\langle \mathbb{Z}, <\rangle$:
- $\overline{\omega} + \overline{\omega}^*$?:
- $\overline{\omega} + 1 + \overline{\omega}^*$:

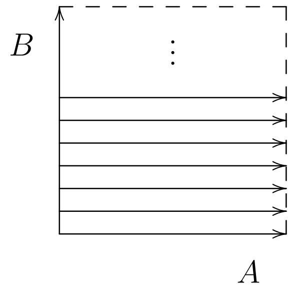


Järjestysten kertolasku
$\rho \cdot \tau$ määritellään seuraavasti: Valitaan $\langle A, R\rangle$ ja $\langle B, S\rangle$ s.e. it$\langle A, R\rangle = \rho$ ja it$\langle B, S\rangle = \tau$

Määritellään sitten

$$R * S = \{\big\langle\langle a_1, b_1\rangle, \langle a_2, b_2\rangle\big\rangle \in (A \times B) \times (A \times B) \mid b_1 S b_2 \text{ tai } (b_1 = b_2 \text{ ja } a_1 R a_2)\}$$

Heprealainen sanakirjajärjestys:



Nyt $\rho \cdot \tau = \text{it}\langle A \times B, R * S\rangle$.

Kertolasku on hyvinmääritelty: Jos $\langle A, R\rangle \cong \langle A', R'\rangle$ ja $\langle B, S\rangle \cong \langle B', S'\rangle$, niin

$$\langle A \times B, R * S\rangle \cong \langle A' \times B', R' * S'\rangle,$$

Esimerkki 7.7 $\overline{\omega} \cdot \overline{2}$: kaksi ω:aa peräkkäin $\overline{\omega} \cdot \overline{2} \neq \omega$.

$\overline{2} \cdot \overline{\omega} = \overline{\omega}$

$(\overline{\omega} + \overline{1}) \cdot \overline{2} = \overline{\omega} \cdot \overline{2} + \overline{1} \neq \overline{\omega} \cdot \overline{2} + \overline{2}$

Lause 7.4 *Seuraavat pätevät kaikkilla järjestystyypeillä* σ, τ, ρ

(a) $(\rho + \sigma) + \tau = \rho + (\sigma + \tau)$
$(\rho \cdot \sigma) \cdot \tau = \rho \cdot (\sigma \cdot \tau)$

(b) *Vasemman puoleinen osittelulaki*
$\rho \cdot (\sigma + \tau) = (\rho \cdot \sigma) + (\rho \cdot \tau)$

(c) *Neutraalialkio*
$\rho + \overline{0} = \overline{0} + \rho = \rho$
$\rho \cdot \overline{0} = \overline{0} \cdot \rho = \overline{0}$
$\rho \cdot \overline{1} = \overline{1} \cdot \rho = \rho$

7.1 Ordinaaliaritmetiikkaa

Korvataan $\overline{\alpha}$ α:lla itsellään. Siis

$$\alpha + \beta = \gamma \overset{\text{def}}{\Leftrightarrow} \overline{\alpha} + \overline{\beta} = \overline{\gamma}$$
$$\alpha \cdot \beta = \gamma \overset{\text{def}}{\Leftrightarrow} \overline{\alpha} \cdot \overline{\beta} = \overline{\gamma}$$

Lause 7.5 *Kaikilla ordinaaleilla α, β, γ*
$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$
$(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$
$\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma)$
$\alpha + 0 = 0 + \alpha = \alpha$
$\alpha \cdot 1 = 1 \cdot \alpha = \alpha$
$\alpha \cdot 0 = 0 \cdot \alpha = 0$

Todistus. Todistetaan määritelmien ja lauseen 7.4 avulla. □

Ordinaalien yhteen- ja kertolasku voidaan määritellä myös transfiniittisella rekursiolla:

Lause 7.6 *Kaikilla ordinaaleilla α ja β ja jokaisella rajaordinaalilla λ pätee*

(A1) $\alpha + 0 = \alpha$
(A2) $\alpha + \beta^+ = (\alpha + \beta)^+$
(A3) $\alpha + \lambda = \sup\{\alpha + \beta \mid \beta \in \lambda\}$

(M1) $\alpha \cdot 0 = 0$
(M2) $\alpha \cdot \beta^+ = \alpha \cdot \beta + \alpha$
(M3) $\alpha \cdot \lambda = \sup\{\alpha \cdot \beta \mid \beta \in \lambda\}$