Joukko-oppi

Lauri Hellan monisteesta
muokannut Kerkko Luosto

Luentomoniste, syksyn 2019 luennot

Sisältö

6

Luonnolliset luvut

Kuten aikaisemmin on selitetty, joukko-opin tavoitteena on, että *kaikki* matemaattiset oliot voidaan rakentaa joukkoina. Luonnolliset luvut ovat perustavanlaatuisimpia olioita, joiden kohdalla on epätriviaalia, miten rakentaminen pitäisi tehdä. Asettakaamme konstruktiolle seuraavat tavoitteet:

A) Koska luonnollisilla luvuilla lasketaan äärellisten joukkojen alkioiden lukumääriä, tulisi luonnollisen luvun edustaa kuvastamaansa mahtavuutta. Siis esimerkiksi luvun 7 tulisi olla seitsenalkioinen joukko.

B) Luonnolliset luvut pitäisi pystyä keräämään yhteen yhdeksi joukoksi ω. (Tässä siis merkintä eroaa totutusta, koska luonnollisten lukujen joukkoa useimmiten merkitään symbolilla $\mathbb{N}$.)

C) Luonnollisten lukujen käsitteen ympärille tulee muodostaa myös rakennetta. Järjestelmään liittyy siis luonnollisten lukujen lisäksi laskutoimitukset ja järjestys.

Nämä tavoitteet kytkeytyvät melko monimutkaisella tavalla toisiinsa. Tarkastellaan ensin tavoitteita B ja C. Jos tavoitteen A voisi unohtaa, niin olisi pitkälti samantekevää, miten luonnolliset luvut konstruoidaan. Oleelliseksi jää silloin, että luonnolliset luvut muodostavat äärettömän joukon, jossa alkiot seuraavat induktiivisesti toisiaan:

$$0 \mapsto 1 \mapsto 2 \mapsto 3 \cdots \mapsto n \mapsto \cdots$$

Jos tämä seuraajakuvaus tunnetaan, niin loput rakenteesta voidaan määritellä rekursiolla. Tämä oli Giuseppe Peanon lähtökohta, kun hän vuonna 1889 esitti luonnollisten lukujen aksioomansa [Pea89].

Peanon postulaatit

Määritelmä 6.1. *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:

P1) $e \notin \text{ran}(S)$.

P2) S on injektio.

P3) Jos $B \subseteq N \wedge e \in B \wedge \forall x(x \in B \rightarrow S(x) \in B)$, niin $B = N$.

Ennen Peanon systeemin käsitteen pureskelua todettakoon, mitä tämä merkitsee kiinnitettyjen tavoitteiden kannalta: Jos käytettävissä olisi yksikin Peanon systeemi, niin tavoitteet B ja C voitaisiin toteuttaa. Seuraajakuvauksen S avulla voitaisiin nimittäin rakentaa Peanon systeemiin laskutoimitukset ja järjestys rekursiivisesti; tähän palataan myöhemmin konkreettisen luonnollisten lukujen järjestelmän kohdalla. Tässä lähestymistavassa on vain joukko-opillisesti se ongelma, että jo käsiteltyjen aksioomien avulla ei voida osoittaa yhdenkään Peanon systeemin olemassaoloa, vaan tarvitaan äärettömyysaksiooma.

Äärettömyysaksiooma tullaan muotoilemaan huolellisesti niin, että tavoite A otetaan alusta alkaen huomioon. Ensin kiinnitetään itse asiassa seuraajamekanismi sopivasti niin, että tavoite saadaan triviaalisti toteutettua. Tämä kaikki toteutetaan seuraavassa alaluvussa.

Peanon postulaattien tarkoituksena on aksiomatisoida luonnollisten lukujen struktuuri, missä e vastaa lukua 0, ja S vastaa seuraajafunktiota $n \mapsto n + 1$. Myöhemmin osoitetaan, että aksiomatisointi on täydellinen: kaikki Peanon systeemit ovat isomorfisia sen systeemin kanssa, joka tullaan konstruoimaan ja joka kiinnitetään oikeaksi luonnollisten lukujen systeemiksi.

Kaikki kolme Peanon systeemien ehtoa ovat välttämättämiä. Jos ehto P1 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 P2 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 P3 jätettäisiin pois, sallittaisiin tulkintoja, joissa on luonnollisten lukujen struktuurin lisäksi erillisiä syklejä ja/tai erillisiä kokonaislukujen kopioita.

Induktiiviset joukot

Jotta luonnolliset luvut saadaan määriteltyä, pitäisi siis kiinnittää sopiva seuraajamekanismi, jonka avulla luonnollisia lukuja voidaan muodostaa. Zermelon [Zer08] ehdotus luonnollisiksi luvuiksi oli seuraava:

$$\begin{array}{cccccc} \emptyset, & \{\emptyset\}, & \{\{\emptyset\}\}, & \{\{\{\emptyset\}\}\}, & \ldots \\ 0_Z & 1_Z & 2_Z & 3_Z & \end{array}$$

Alaindeksi Z viittaa toisaalta Zermeloon, mutta myös korostaa sitä, että näitä *Zermelon luonnollisia lukuja* ei yleisesti (nollaa ja ykköstä lukuun ottamatta) hyväksytä oikeiksi luonnollisiksi luvuiksi. Zermelo käytti luonnollisten lukujen muodostamiseen alun perin siis seuraajamekanismia $a \mapsto \{a\}$. Tämän ajatuksen heikkoutena on, että tavoite A ei toteudu: 0_Z on tosin tyhjänä joukkona nollan alkion joukko ja 1_Z yksiö, mutta nollaa lukuun ottamatta kaikki muut Zermelon luonnolliset luvut olisivat yksiöitä. Luvusta 2 lähtien tavoite A ei siis toteudu.

Myöhemmin von Neumann [von23] lähestyi luonnollisten lukujen konstruoimisen ongelmaa eri tavalla:

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

Luonnolliset luvut saadaan siis rekursiivisesti määriteltyä edeltäjiensä avulla, ja tavoite A selvästi toteutuu. Von Neumannin määritelmästä onkin tullut joukko-opin standardimääritelmä. Huomataan (ja myöhemmin todistetaan), että sen mukaan pätee

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

Luonnollisten lukujen järjestys voidaan siis palauttaa alkiorelaatioon:

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

Toisaalta niiden järjestys voidaan myös ilmaista osajoukkorelaation avulla:

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

Edelleen havaitaan, että von Neumannin ideassa

$$n+1 = \{0,1,\ldots,n\} = \{0,1,\ldots,n-1\} \cup \{n\} = n \cup \{n\},$$

joten tähän ideaan liittyy seuraajamekanismi $a \mapsto a \cup \{a\}$.

Määritelmä 6.2. Kun a on joukko, sen *seuraaja* on

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

Huom. Myöhemmin pystytään tarkastamaan, että von Neumannin määritelmän perusteella luonnollisilla luvuilla pätee $n^+ = n + 1$.

Von Neumannin idean voi seuraajan käsitteen avulla nyt ilmaista niin, että kaikki luonnolliset luvut voidaan muodostaa tyhjästä joukosta seuraajaa käyttäen. Tätä intuitiivista ideaa ei kuitenkaan pysty suoraan pukemaan muodolliseksi määritelmäksi, joten teknisesti joudutaan etenemään kiertotietä: Joka tapauksessa pyritään tavoitteeseen B eli muodostamaan luonnollisten lukujen joukko ω. Tästä joukosta tiedetään, että sen pitäisi olla nollan ja seuraajan virittämä eli suppein joukko, joka sisältää tyhjän joukon ja on seuraajan suhteen suljettu.

Määritelmä 6.3. Joukko A on *induktiivinen*, jos se sisältää tyhjän joukon ja on suljettu seuraajien suhteen, ts.

a) $\emptyset \in A$ ja

b) $\forall a \in A\ (a^+ \in A)$.

Luonnollisten lukujen joukon tulisi olla siis suppein induktiivinen joukko, mutta kuten todettiin, aikaisemmista aksioomista ei seuraa tällaisen olemassaolo. Tarvitaan siis uusi joukko-opin aksiooma.

Äärettömyysaksiooma. On olemassa induktiivinen joukko:

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

Seuraavaksi määritellään luonnollisen luvun käsite.

Määritelmä 6.4. *Luonnollinen luku* on joukko, joka on alkiona jokaisessa induktiivisessa joukossa:

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

Lause 6.5. *On olemassa joukko, jonka alkioita ovat täsmälleen ne joukot, jotka ovat luonnollisia lukuja.*

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

$$\omega = \{x \in A \mid x \text{ kuuluu jokaiseen induktiiviseen joukkoon}\}.$$

Jos siis $x \in A$, niin x kuuluu jokaiseen induktiiviseen joukkoon, joten x on luonnollinen luku. Jos kääntäen x on luonnollinen luku eli kuuluu jokaiseen induktiiviseen joukkoon, niin erityisesti $x \in A$, sillä A on induktiivinen, ja koska x kuuluu muihinkin induktiivisiin joukkoihin, niin $x \in \omega$. Siis ω on kaikkien luonnollisten lukujen joukko. □

Ekstensionaalisuusaksiooman nojalla kaikkien luonnollisten lukujen joukko on yksikäsitteinen, joten voidaan kiinnittää todistuksessa käytetty merkintä: Luonnollisten lukujen joukkoa merkitään jatkossa symbolilla ω. Tärkeä huomio on myös, että ω on suppein induktiivinen joukko.

Lause 6.6. *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 $a^+ \in \omega$. □

Tässä vaiheessa on syytä myös todeta, että koska $\emptyset$ on luonnollinen luku, jolla ei ole alkioita, niin periaatteen A mukaisesti sen kuuluu olla luonnollinen luku nolla. Merkitään siis $0 = \emptyset$. Tyypillisesti merkintää 0 käytetään jatkossa, kun halutaan korostaa tyhjän joukon roolia luonnollisena lukuna. Koska ω on induktiivinen, myös 0^+, 0^{++}, 0^{+++} jne. ovat luonnollisia lukuja ja ω:n alkioita. Näille käytetään tuttuja merkintöjä

$$1 = 0^+, 2 = 1^+, 3 = 2^+ \text{ jne.}$$

Periaatteessa “ja niin edelleen” pystyttäisiin korvaamaan täsmällisellä esityksellä siitä, miten kymmenjärjestelmäesitys toimii, mutta käytännöllisistä syistä tällainen selitys ohitetaan.

Induktioperiaate ω:lle. Edellisen lauseen nojalla jokainen ω:n induktiivinen osajoukko on ω itse

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

Saman asian voi myös pyörittää seuraavaan muotoon:

Lause 6.7 (Induktiotodistus.)**.** *Olkoon $P(x)$ jokin luonnollisten lukujen x ominaisuus. Oletetaan, että*

1) *$P(0)$ pätee eli nollalla on ominaisuus P.*
2) *Jokaiselle luonnolliselle luvulle n pätee, että jos $P(n)$, niin $P(n^+)$.*

Tällöin $\forall x \in \omega\, P(x)$.

Todistus. Tarkastellaan joukkoa

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

Oletuksista seuraa, että B on induktiivinen:

1) $\emptyset \in B$.
2) Jos $n \in B$, niin $n^+ \in B$.

Siis induktioperiaatteen nojalla $B = \omega$ (koska $B \subseteq \omega$) eli $\forall x \in \omega\, P(x)$. □

Lause 6.8. *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:

1) $\emptyset = 0 \in B$.
2) 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. □

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

Luonnollisten lukujen joukko Peanon systeeminä

Määritelmä 6.9. *Luonnollisten lukujen seuraajafunktio* on joukko

$$\sigma = \{(n, n^+) \mid n \in \omega\}.$$

Apulause 6.10. *$(\omega, \sigma, 0)$ toteuttaa Peanon systeemin ehdot P1 ja P3.*

Todistus. Koska ω on induktiivinen, niin $0 \in \omega$ ja σ on funktio $\omega \to \omega$. Koska jokaisella $n \in \omega$ pätee $\sigma(n) = n^+ = n \cup \{n\} \neq \emptyset = 0$, niin $0 \notin \operatorname{ran}(\sigma)$. Siis P1 on voimassa.

Olkoon $B \subseteq \omega$ joukko, jolle pätee $0 \in B$ ja jokaisella $x \in B$ myös $\sigma(x) = x^+ \in B$. Tällöinhän B on induktiivinen ω:n osajoukko, joten ω:n induktioperiaatteen nojalla $B = \omega$. Siis myös P3 pätee. □

Jokseenkin yllättäen ehto P2 onkin vaikenkin asia tarkastettavaksi, kun todistetaan, että $(\omega, \sigma, 0)$ on Peanon systeemi. Tätä tarkastelua varten esitellään tärkeä tekninen joukko-opillinen käsite, joukon transitiivisuus.

Määritelmä 6.11. Joukko A on *transitiivinen*, jos jokainen A:n alkion alkio on A:n alkio:

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

Transitiivisuus voidaan määritellä usealla keskenään ekvivalentilla tavalla:

Apulause 6.12. *Kun A on joukko, seuraavat ovat yhtäpitäviä:*

a) A *on transitiivinen.*

b) $\bigcup A \subseteq A$.

c) Jokaisella $a \in A$ *pätee* $a \subseteq A$.

d) $A \subseteq \mathcal{P}(A)$.

Todistus. Todistetaan kohtien yhtäpitävyys syklin $a) \Rightarrow b) \Rightarrow c) \Rightarrow d) \Rightarrow a)$ kautta.

$a) \Rightarrow b)$: Oletetaan, että A on transitiivinen. Olkoon $x \in \bigcup A$, jolloin on olemassa $a \in A$, jolle $x \in a$. Koska $x \in a$, $a \in A$ ja A on transitiivinen, niin $x \in A$. Siis $\bigcup A \subseteq A$.

$b) \Rightarrow c)$: Oletetaan, että $\bigcup A \subseteq A$. Kun $a \in A$, niin $a \subseteq \bigcup A \subseteq A$, mikä todistaa kohdan c.

$c) \Rightarrow d)$: Oletetaan, että $\forall a \in A \ (a \subseteq A)$. Siis jokaisella $a \in A$ pätee $a \in \mathcal{P}(A)$, joten $A \subseteq \mathcal{P}(A)$.

$d) \Rightarrow a)$: Oletetaan, että $A \subseteq \mathcal{P}(A)$. Testataan, onko A transitiivinen. Olkoot $a \in A$ ja $x \in a$. Koska $a \in A \subseteq \mathcal{P}(A)$, niin $a \in \mathcal{P}(A)$ eli $a \subseteq A$. Siis $x \in a \subseteq A$, mistä seuraa $x \in A$. Siis A on transitiivinen. □

Esimerkki 6.13. $A = \{\emptyset, \{\{\emptyset\}\}\}$ ei ole transitiivinen, koska $\{\emptyset\} \in \{\{\emptyset\}\} \in A$, mutta $\{\emptyset\} \notin A$. Sen sijaan $B = A \cup \{\{\emptyset\}\}$ on transitiivinen: Käytetään edellisen apulauseen kohtaa c. Joukon B alkiot ovat $\emptyset$, $\{\emptyset\}$ ja $\{\{\emptyset\}\}$. Triviaalisti $\emptyset \subseteq B$. Lisäksi $\{\emptyset\} \subseteq B$, sillä $\emptyset \in B$, ja $\{\{\emptyset\}\} \subseteq B$, sillä $\{\emptyset\} \in B$. Siis B on transitiivinen.

Lause 6.14. *Jos a on transitiivinen, niin $\bigcup a^+ = a$.*

Todistus. Koska a on transitiivinen, niin $\bigcup a \subseteq a$ ja

$$\bigcup a^+ = \bigcup (a \cup \{a\}) = \left(\bigcup a\right) \cup \left(\bigcup \{a\}\right) = \left(\bigcup a\right) \cup a = a.$$

□

Lause 6.15. *Jokainen luonnollinen luku on transitiivinen.*

Todistus. Todistetaan induktiolla luvun $n \in \omega$ suhteen, että n on transitiivinen.

1) 0 on transitiivinen, sillä $\bigcup 0 = \bigcup \emptyset = \emptyset = 0 \subseteq 0$.

2) Oletetaan, että n on transitiivinen. Tällöin edellisen lauseen mukaan

$$\bigcup n^+ = n \subseteq n \cup \{n\} = n^+,$$

joten apulauseen 6.12 nojalla n^+ on transitiivinen.

□

Lause 6.16. *ω on transitiivinen eli jokainen $n \in \omega$ on ω:n osajoukko.*

Todistus. Todistetaan induktiolla luvun $n \in \omega$ suhteen, että $n \subseteq \omega$.

1) Triviaalisti $0 = \emptyset \subseteq \omega$.

2) Oletetaan, että $n \subseteq \omega$. Tällöin $n \subseteq \omega$ ja $\{n\} \subseteq \omega$, joten $n^+ = n \cup \{n\} \subseteq \omega$. Siis myös $n^+ \subseteq \omega$.

□

Lause 6.17. *$(\omega, \sigma, 0)$ on Peanon systeemi.*

Todistus. Apulauseen 6.10 nojalla tiedetään jo, että Peanon systeemin ehdot P1 ja P3 ovat voimassa. Riittää siis tarkastaa, että myös ehto P2 täyttyy eli σ on injektio. Oletetaan, että $\sigma(m) = \sigma(n)$ eli $m^+ = n^+$, missä $m, n \in \omega$. Koska m ja n ovat transitiivisia (lause 6.15), niin lausetta 6.14 soveltamalla saadaan $m = \bigcup m^+ = \bigcup n^+ = n$. Siis σ on injektio. □

Tässä vaiheessa voidaan todeta, että luonnollisille luvuille asetetut tavoitteet B ja C saadaan toteutettua, kunhan osoitetaan, että systeemiin $(\omega, \sigma, 0)$ voidaan rakentaa aritmetiikka ja järjestys. Näitä konstruktioita varten tarvitaan rekursiota.

Rekursio

Olkoon A joukko, $f\colon A \to A$ funktio, ja $a \in A$. Intuitiivisesti on selvää, että funktion $h\colon \omega \to A$ voidaan määritellä 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.

Rekursiolause. *Olkoon A joukko, $a \in A$ ja $f\colon A \to A$. Tällöin on olemassa yksikäsitteinen sellainen kuvaus $h\colon \omega \to A$, että*

$$h(0) = a$$

ja jokaisella $n \in \omega$ pätee

$$h(n^+) = f(h(n)).$$

Todistus. Kuten todettiin, tulos on uskottava, mutta sen todistus vaatii huolellista tekniikkaa. Ideana on, että kuvaus h muodostetaan pienistä paloista. Sen perustelemiseksi, että $h(n) = m$, tarvitaan nimittäin kuvauksen h arvot kohdissa $0, 1, \ldots, n-1$, ts. kuvauksesta h pitää tuntea ainakin rajoittuma

$$h \restriction \{0, 1, \ldots, n\} = \{(0, h(0)), (1, h(1)), \ldots, (n, h(n))\}.$$

Tämä idea johtaa seuraavaan apukäsitteeseen: Sanotaan, että funktio η on *hyväksyttävä*, jos $\operatorname{dom}(\eta) \subseteq \omega$, $\operatorname{ran}(\eta) \subseteq A$ ja seuraavat ehdot ovat voimassa:

H1) Jos $0 \in \operatorname{dom}(\eta)$, niin $\eta(0) = a$.

H2) Jos $n^+ \in \operatorname{dom}(\eta)$, niin myös $n \in \operatorname{dom}(\eta)$ ja $\eta(n^+) = f(\eta(n))$.

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

$(*)$ $\quad (n, y) \in h \iff \eta(n) = y$ jollakin hyväksyttävällä funktiolla η.

Todistetaan seuraavat asiat:

a) $\operatorname{dom}(h) = \omega$,

b) h on funktio,

c) h on hyväksyttävä,

d) h on yksikäsitteinen kuvaus, joka toteuttaa lauseen ehdon.

a) Väitteen $\operatorname{dom}(h) = \omega$ todistamiseksi osoitetaan induktiolla luvun $n \in \omega$ suhteen, että $n \in \operatorname{dom}(h)$.

a1) Funktio $\{(0, a)\}$ on hyväksyttävä, joten $(0, a) \in h$ ja siis $0 \in \operatorname{dom}(h)$.

a2) Oletetaan, että $n \in \operatorname{dom}(h)$. On siis olemassa $\eta \in \mathcal{H}$, jolla $n \in \operatorname{dom}(\eta)$. Jos $n^+ \in \operatorname{dom}(\eta)$, on myös $n^+ \in \operatorname{dom}(h)$. Jos taas $n^+ \notin \operatorname{dom}(\eta)$, määritellään $\eta' = \eta \cup \{(n^+, f(\eta(n)))\}$. Selvästi η' on kuvaus, $\operatorname{dom}(\eta') \subseteq \omega$ ja $\operatorname{ran}(\eta') \subseteq A$. Kuvaus η' on myös hyväksyttävä:

1) Jos $0 \in \operatorname{dom}(\eta')$, niin $\eta'(0) = \eta(0) = a$, sillä $\eta \in \mathcal{H}$.

2) Jos $k^+ \in \operatorname{dom}(\eta')$, niin joko $k^+ \in \operatorname{dom}(\eta)$ tai $k^+ = n^+$ eli $k = n$; molemmissa tapauksissa $k \in \operatorname{dom}(\eta) \subseteq \operatorname{dom}(\eta')$. Edellisessä tapauksessa pätee $\eta'(k^+) = \eta(k^+) \overset{(\eta \in \mathcal{H})}{=} f(\eta(k)) = f(\eta'(k))$. Jälkimmäisessä tapauksessa puolestaan pätee $\eta'(k^+) = \eta'(n^+) = f(\eta(n)) = f(\eta'(n)) = f(\eta'(k))$.

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

b) Osoitetaan induktiolla luvun $n \in \omega$ suhteen, että jokaisella $n \in \omega$ on olemassa korkeintaan yksi y, jolle $(n, y) \in h$.

b1) Induktion aloitusaskel $n = 0$: Jos $(0, y_1) \in h$ ja $(0, y_2) \in h$, niin ehdon $(*)$ mukaan on olemassa hyväksyttävät funktiot η_0 ja η_1, joilla $\eta_0(0) = y_1$ ja $\eta_1(0) = y_2$. Tällöin kohdan H1 perusteella $\eta_0(0) = a = \eta_1(0)$, joten $y_1 = y_2 = a$.

b2) Oletetaan sitten, että induktioväite pätee arvolla n. Jos $(n^+, y_0) \in h$ ja $(n^+, y_1) \in h$, niin ehdon $(*)$ perusteella on olemassa kuvaukset $\eta_0, \eta_1 \in \mathcal{H}$, joille $\eta_0(n^+) = y_0$ ja $\eta_1(n^+) = y_1$. Tällöin kohdan H2 perusteella $n \in \mathrm{dom}(\eta_0)$, $n \in \mathrm{dom}(\eta_1)$. Induktio-oletuksen nojalla $\eta_0(n) = \eta_1(n)$, joten hyväksyttävyysehdosta H2 seuraa $y_0 = \eta_0(n^+) = f(\eta_0(n)) = f(\eta_1(n)) = \eta_1(n^+) = y_1$. Siis induktioväite pätee myös arvolla n^+.

Induktioväite, jonka todettiin siis olevan tosi kaikilla $n \in \omega$, on itse asiassa funktionaalisuusehto eli on näytetty, että h on kuvaus.

c) Osoitetaan, että $h = \bigcup \mathcal{H}$ on hyväksyttävä kuvaus: Kohtien a ja b nojalla tiedetään jo, että h on kuvaus $\omega \to A$.

H1) Koska $0 \in \mathrm{dom}(h)$, niin on olemassa hyväksyttävä funktio η, jolle $\eta(0) = h(0)$. Koska $\eta \in \mathcal{H}$, on $\eta(0) = a$ ja siis $h(0) = a$.

H2) Olkoon $n^+ \in \mathrm{dom}(h)$. Tällöin on olemassa $\eta \in \mathcal{H}$, jolla $h(n^+) = \eta(n^+)$ ja $n \in \mathrm{dom}(\eta)$. Siis $n \in \mathrm{dom}(h)$ ja $h(n) = \eta(n)$, sillä h on funktio. Siispä $h(n^+) = \eta(n^+) = f(\eta(n)) = f(h(n))$.

d) Oletetaan, että h_0 ja h_1 toteuttavat lauseen ehdot. Koska ne ovat siis hyväksyttäviä eli $h_0, h_1 \in \mathcal{H}$, niin $h_0 \cup h_1 \subseteq \bigcup \mathcal{H} = h$. Jos h_0 ja h_1 olisivat eri kuvauksia $\omega \to A$, niin $h_0 \cup h_1$ ei olisi kuvaus, mistä seuraisi, ettei myöskään h olisi kuvaus, mikä on vastoin kohtaa b. Siis $h_0 = h_1 (= h)$. □

Rekursiolause on luonnollisten lukujen rakenteessa pätevä tulos, joka ei yleisty luonnollisella tavalla kokonaislukujen rakenteeseen saatikka laajempiin tavanomaisiin lukualueisiin; tästä esitetään myöhemmin luonnollisten lukujen käsittelyn yhteydessä esimerkki. Sen sijaan ordinaalien yhteydessä huomataan, että induktiolle ja rekursiolle on olemassa hyvinjärjestetyissä joukoissa yleistykset, joita kutsutaan transfiniittiseksi induktioksi ja transfiniittiseksi rekursioksi.

Jatkossa rekursiolausetta sovelletaan toistuvasti luonnollisten lukujen aritmetiikkaa rakennettaessa. Ensimmäisenä rekursiolauseen sovelluksena kuitenkin todistetaan, että Peanon systeemit ovat keskenään isomorfisia.

Lause 6.18. *Olkoon (N, S, e) Peanon systeemi. Tällöin $(\omega, \sigma, 0)$ ja (N, S, e) ovat keskenään isomorfiset: on olemassa sellainen bijektio $h\colon \omega \to N$, 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 $\text{ran}(h)$ systeemissä (N, S, e). Ensinnäkin $e \in \text{ran}(h)$, koska $h(0) = e$. Toiseksi, jos $x \in \text{ran}(h)$, niin on olemassa $n \in \omega$, jolla $h(n) = x$. Tällöin $h(n^+) = S(h(n)) = S(x)$, joten myös $S(x) \in \text{ran}(h)$. Siis $\text{ran}(h)$ on induktiivinen, joten $\text{ran}(h) = N$.

Osoitetaan lopuksi, että h on injektio. Tällä kerralla käytetään 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 voidaan 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 kuvaus

$$f \colon \omega \times \omega \to \omega.$$

Määritelmä 6.19. *Luonnollisten lukujen yhteenlasku* $+$ on niiden kolmikoiden $(m, n, p) \in \omega \times \omega \times \omega$ joukko, jotka toteuttavat seuraavat ehdon: On olemassa kuvaus $f \colon \omega \to \omega$, jolle $f(n) = p$ ja joka toteuttaa rekursioehdot

$$\begin{cases} f(0) = m \\ f(k^+) = f(k)^+ \quad \text{kun } k \in \omega. \end{cases}$$

Määritelmä on hyvin tekninen, mutta pienen pureksinnan jälkeen on käsitettävissä, että se on itse asiassa täysin luonteva. Ensiksi huomataan, että yhteenlasku $+$ muodostetaan erottelulla joukosta $\omega \times \omega \times \omega = (\omega \times \omega) \times \omega$, joten $+$ on relaatio. Toinen havainto on, että kun $m, n \in \omega$ on annettu, niin rekursiolauseen nojalla on olemassa yksikäsitteinen $f\colon \omega \to \omega$, jolle rekursioehdot $f(0) = m$ ja $f(k^+) = f(k)^+$, kun $k \in \omega$, pätevät. Itse asiassa tämä f riippuu vain luvusta m ja on yllä esitelty kuvaus A_m. Siispä paria (m, n) vastaa vain yksi luku $p = f(n) = A_m(n)$, jolle $((m, n), p) = (m, n, p) \in +$. Tämä tarkoittaa, että $+$ on kuvaus $\omega \times \omega \to \omega$ eli joukon ω laskutoimitus, joten kun $(m, n, p) \in +$, voidaan merkitä $+(m, n) = n$ tai tutummalla tavalla $m + n = p$.

Määritelmän rekursioehdot voidaan siis purkaa – tavanomaisia merkintöjä käyttäen – yhteenlaskun rekursiokaavoiksi: Kaikilla $m, n \in \omega$ pätee

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

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

Huom. Soveltamalla ehtoja tapauksessa $n = 0$ nähdään, että

$$m + 1 = m + 0^+ \overset{(A2)}{=} (m + 0)^+ \overset{(A1)}{=} m^+.$$

Siis seuraajakuvaukselle σ pätee $\sigma(m) = m^+ = m + 1$, kun $m \in \omega$, eli σ liittää jokaiseen lukuun m luvun $m + 1$, niin kuin pitääkin.

Määritellään seuraavaksi luonnollisten lukujen kertolasku samalla idealla. Lähtökohtana on havainto, että jotta osittelulaki olisi voimassa, niin on pädettävä $m \cdot (n + 1) = m \cdot n + m$.

Olkoon $m \in \omega$. Määritellään funktio $M_m\colon \omega \to \omega$ rekursiolla seuraavasti:

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

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

Määritelmä 6.20. *Luonnollisten lukujen kertolasku* $\cdot$ on niiden kolmikoiden $(m, n, p) \in \omega \times \omega \times \omega$ joukko, jotka toteuttavat seuraavat ehdon: On olemassa kuvaus $g\colon \omega \to \omega$, jolle $g(n) = p$ ja joka toteuttaa rekursioehdot

$$\begin{cases} g(0) = 0 \\ g(k^+) = g(k) + m \quad \text{kun } k \in \omega. \end{cases}$$

Kertolaskusta voidaan tehdä vastaavat huomiot kuin yhteenlaskustakin: Ensinnäkin rekursiolauseen avulla saadaan perusteltua, että se on kuvaus $\cdot\colon \omega \times \omega \to \omega$ eli joukon ω laskutoimitus. Korvaamalla yleinen kuvausmerkintä laskutoimitusmerkinnällä, ts. merkitsemällä $m \cdot n = \cdot(m, n)$, kun $m, n \in \omega$, saadaan rekursioehdot kirjoitettua luonnollisemmin: 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. Käytetään tätä sopimusta myös jatkossa.

Saman mallin mukaisesti voidaan määritellä luonnollisten lukujen potenssiinkorotus eli kuvaus $(m, n) \mapsto m^n$, kun sovitaan erityisesti, että $0^0 = 0$. Samoin kuin kertolaskussa iteroitiin yhteenlaskua, niin potenssiinkorotuksessa iteroidaan kertolaskua. Kun tässä vaiheessa on jo selvää, miten aritmeettisten laskutoimitusten määrittelyssä käytetään rekursiolausetta ja merkintöjä, niin määritelmän voi esittää lyhyemmin:

Määritelmä 6.21. *Luonnollisten lukujen potenssiinkorotus* on se joukon ω laskutoimitus $(m, n) \mapsto m^n$, joka toteuttaa seuraavat rekursioehdot:

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

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

Esimerkki 6.22. Lasketaan $2 + 3$ käyttäen yhteenlaskun rekursiivista määritelmää.

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

Todistetaan seuraavaksi yhteenlaskun ja kertolaskun tutut perusominaisuudet.

Lause 6.23. *Seuraavat laskulait pätevät kaikilla $m, n, p \in \omega$:*

$$\begin{aligned} m + (n + p) &= (m + n) + p && \textit{(yhteenlasku on liitännäinen)} \\ m + n &= n + m && \textit{(yhteenlasku on vaihdannainen)} \\ m \cdot (n + p) &= m \cdot n + m \cdot p && \textit{(yhteen- ja kertolasku osittelevat)} \\ m \cdot (n \cdot p) &= (m \cdot n) \cdot p && \textit{(kertolasku on liitännäinen)} \\ m \cdot n &= n \cdot m. && \textit{(kertolasku on vaihdannainen)} \end{aligned}$$

Todistus. Jokainen laskulaki todistetaan induktiolla, mutta tässä tyydytään todistamaan yhteenlaskun vaihdantalaki ja osittelulaki. Liitäntälait ja kertolaskun vaihdantalaki jäävät harjoitustehtäviksi.

Yhteenlaskun vaihdannaisuuden todistus: Yhteenlaskuhan toteutti rekursioehdot

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

kun $m, n \in \omega$. Rekursio siis toteutettiin oikean muuttujan suhteen, ja on perusteltua kysyä, eikö vasemmanpuoleinen rekursio olisi ollut myöskin mahdollinen eli pätevätkö rekursioehdot

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

kaikilla $m, n \in \omega$. Vastaus on myönteinen, ja nämä ehdot voidaan todistaakin aputuloksina vaihdannaisuuden osoittamista varten.

a) **V**äite: $0 + n = n$ jokaisella $n \in \omega$.

Todistus. Osoitetaan väite induktiolla luvun $n \in \omega$ suhteen. $0 + 0 = 0$ pätee suoraan ehdon A1 perusteella. Oletetaan sitten, että $0 + n = n$. Tällöin

$$0 + n^+ \overset{(A2)}{=} (0 + n)^+ \overset{(\text{ind.ol.})}{=} n^+,$$

joten induktioväite pätee myös arvolla n^+.

b) **V**äite: $m^+ + n = (m + n)^+$ kaikilla $m, n \in \omega$.

Todistus. Kiinnitetään $m \in \omega$ ja todistetaan väite induktiolla luvun $n \in \omega$ suhteen. Väite pätee arvolla $n = 0$, sillä $m^+ + 0 \overset{(A1)}{=} m^+ \overset{(A1)}{=} (m + 0)^+$. Oletetaan, että väite pätee luvulle n. Tällöin

$$m^+ + n^+ \overset{(A2)}{=} (m^+ + n)^+ \overset{(\text{ind.ol.})}{=} (m + n)^{++} \overset{(A2)}{=} (m + n^+)^+,$$

joten väite pätee arvolla n^+.

Kun nyt tiedetään, että rekursioehdot pätevät myös vasemman muuttujan suhteen, niin yhteenlaskun vaihdannaisuus on mahdollista todistaa. Kiinnitetään $n \in \omega$ ja todistetaan induktiolla luvun $m \in \omega$ suhteen, että $m + n = n + m$.

Aputuloksesta a ja rekursioehdosta A1 seuraa $0 + n = n = n + 0$, joten induktioväite pätee arvolla $m = 0$.

Oletetaan sitten, että $m + n = n + m$. Tällöin

$$m^+ + n \overset{(b)}{=} (m + n)^+ \overset{(\text{ind.ol.})}{=} (n + m)^+ \overset{(A2)}{=} n + m^+,$$

joten väite pätee arvolla m^+.

Osittelulain todistus: Kiinnitetään $m, n \in \omega$ ja todistetaan osittelulaki $m \cdot (n + p) = m \cdot n + m \cdot p$ induktiolla luvun p suhteen.

Ensinnäkin induktioväite pätee arvolla $p = 0$, sillä

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

Oletetaan sitten, että induktioväite pätee arvolla p. Tällöin

$$\begin{aligned} m \cdot (n + p^+) &\overset{(A2)}{=} m \cdot (n + p)^+ \\ &\overset{(M2)}{=} m \cdot (n + p) + m \\ &\overset{(\text{ind.ol.})}{=} (m \cdot n + m \cdot p) + m \overset{(\cdot \text{ liitännäinen})}{=} m \cdot n + (m \cdot p + m) \\ &\overset{(M2)}{=} m \cdot n + m \cdot p^+. \end{aligned}$$

Siis väite pätee myös arvolla p^+. □

Luonnollisten lukujen järjestys

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

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.

Määritelmä 6.24. *Luonnollisten lukujen järjestys* $<$ on relaatio

$$< = \{ (m, n) \in \omega \times \omega \mid m \in n \}.$$

Tavoitteena on siis todistaa, että $<$ on joukon ω tiukka lineaarijärjestys.

Apulause 6.25. *Relaatio $<$ on transitiivinen.*

Todistus. Oletetaan, että $m < n$ ja $n < p$ eli $m, n, p \in \omega$, $m \in n$ ja $n \in p$. Koska p on transitiivinen joukko, pätee nyt $m \in p$ eli $m < p$. □

Pitää vielä todistaa, että relaatio $<$ toteuttaa trikotomian:

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

Tätä varten tarvitaan seuraava apulause.

Apulause 6.26.

a) Kaikilla $m, n \in \omega$ pätee $m < n$, jos ja vain jos $m^+ < n^+$.

b) Kaikilla $m \in \omega$ pätee $m \not< m$.

Todistus. a) Oletetaan ensin, että $m^+ < n^+$ eli $m^+ \in n^+$. 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 $m < n$.

Implikaatio toiseen suuntaan todistetaan induktiolla. Todistetaan nimittäin induktiolla luvun $n \in \omega$ suhteen, että jos $m \in n$, niin $m^+ \in n^+$. Aloitusaskeleessa ei ole mitään todistamista, sillä $0 = \emptyset$. Oletetaan sitten, että väite pätee luvulle n. Olkoon $m \in n^+$ eli joko $m \in n$ tai $m = n$. Edellisessä tapauksessa induktio-oletuksesta seuraa $m^+ \in n^+ \subseteq n^{++}$. Jos taas $m = n$, pätee $m^+ = n^+ \in n^{++}$. Siis molemmissa tapauksissa $m^+ \in n^{++} = (n^+)^+$.

b) Todistetaan induktiolla luvun $m \in \omega$ suhteen, että $m \not< m$ eli $m \notin m$.

Väite pätee triviaalista arvolla $m = 0$, koska 0 on tyhjä joukko. Oletetaan, että induktioväite on voimassa luvulle $m \in \omega$ eli $m \notin m$. Soveltamalla kohtaa a arvolla $m = n$ saadaan $m \notin m \iff m^+ \notin m^+$. Siis induktioväite pätee myös arvolla m^+. □

Lause 6.27 (Trikotomialaki relaatiolle $<$)**.** *Kaikilla $m, n \in \omega$ pätee tasan yksi ehdoista $m < n$, $m = n$ tai $n < m$.*

Todistus. Todistetaan siis, että kaikilla $m, n \in \omega$ pätee tasan yksi ehdoista $m \in n$, $m = n$ tai $n \in m$. Ensinnäkin korkeintaan yksi näistä ehdoista pätee:

> Jos olisi $m \in n \wedge n \in m$, saataisiin luvun m transitiivisuuden perusteella $m \in m$, mikä on mahdotonta apulauseen 6.26 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. Osoitetaan siis induktiolla luvun $n \in \omega$, että jokaisella $m \in \omega$ pätee $m \in n$, $m = n$ tai $n \in m$.

1) Todistetaan induktiolla (induktiotodistuksen sisässä) luvun $m \in \omega$ suhteen, että $m = 0$ tai $0 \in m$. Jos $m = 0$, niin tämä on triviaalia. Oletetaan, että $m = 0$ tai $0 \in m$. Tällöin joko $0 \in \{0\} = 0^+ = m^+$ tai $0 \in m \subseteq m^+$. Molemmissa tapauksissa siis $0 \in m^+$.

2) Oletetaan, että induktioväite pätee luvulle n. Olkoon $m \in \omega$, jolloin induktioväitteen nojalla $m \in n$, $m = n$ tai $n \in m$. Ensimmäisessä tapauksessa $m \in n \in n^+$ ja koska n^+ on transitiivinen, pätee $m \in n^+$. Toisessa tapauksessa saadaan samoin $m = n \in n^+$. Oletetaan sitten, että $n \in m$, jolloin apulauseen 6.26 nojalla $n^+ \in m^+$. Siis $n^+ \in m$ tai $n^+ = m$, joten induktioväite on todistettu.

□

Lause 6.28. *$(\omega, <)$ on tiukasti lineaarijärjestetty joukko.*

Todistus. Väitteen kanssa yhtäpitävää on, että relaatio $<$ on transitivinen ja toteuttaa trikotomiaehdon. Edellinen ehto on todistettu lemmassa 6.25 ja jälkimmäinen edellisessä lauseessa. □

Merkitään $A \subsetneq B$, jos A on B:n aito osajoukko, eli

$$A \subsetneq B \iff A \subseteq B \wedge A \neq B.$$

Seuraus 6.29. *Kaikilla $m, n \in \omega$ pätee*

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

ja

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

Todistus. Ensimmäinen ekvivalenssi seuraa tietenkin suoraan relaation $<$ määritelmästä. Oletetaan sitten, että $m \in n$. Tällöin $m \subseteq n$, koska n on transitiivinen joukko. Trikotomiaehdon perusteella $m \neq n$, joten osajoukkorelaatio on aito: $m \subsetneq n$.

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

Viimeinen väite seuraa suoraan jo todistetusta. □

Tässä vaiheessa on jo selvää, että luonnollisten lukujen järjestyksen yhteydessä voidaan yleensä käyttää tavanomaisia merkintöjä eli symboleita $<$ ja $\leq$, mutta joukko-opillisiin merkintöihin voidaan turvautua aina, kun se on todistuksissa tarpeellista.

Käsitellään vielä luonnollisten lukujen järjestyksen ja aritmetiikan välistä suhdetta. Tähän liittyvät aidosti kasvavat ja kasvavat kuvaukset.

Määritelmä 6.30. Olkoot $(A, \leq)$ ja $(B, \leq')$ osittaisesti järjestettyjä joukkoja. Niiden välinen kuvaus $f\colon A \to B$ on *kasvava*, jos kaikilla $x, y \in A$ ehdosta $x \leq y$ seuraa $f(x) \leq' f(y)$. Kuvaus f on *aidosti kasvava*, jos vastaavasti kaikilla $x, y \in A$ ehdosta $x < y$ seuraa $f(x) <' f(y)$.

Kasvavia ja aidosti kasvavia kuvauksia voidaan käsitellä myös tiukasti järjestettyjen joukkojen yhteydessä, koska tiukkaa järjestystä aina vastaa osittainen järjestys.

Apulause 6.31. *Olkoot $(A, \leq)$ ja $(B, \leq')$ lineaarijärjestettyjä joukkoja ja $f\colon A \to B$ aidosti kasvava kuvaus. Tällöin:*

a) Kaikilla $x, y \in A$ pätee $x < y$, jos ja vain jos $f(x) < f(y)$.

b) f on injektio.

Todistus. a) Implikaatio vasemmalta oikealle seuraa suoraan määritelmästä. Oletetaan sitten, että alkioille $x, y \in A$ pätee $f(x) < f(y)$. Koska $\leq$ on lineaarijärjestys, se on vertailullinen, joten $x \leq y$ tai $y \leq x$. Ensiksi havaitaan, että jos olisi $x = y$, pätisi $f(x) = f(y)$, mikä on vastoin oletusta $f(x) < f(y)$. Siis $x \neq y$, joten on oltava $x < y$ tai $y < x$. Jälkimmäisestä vaihtoehdosta seuraisi kuvauksen f aidon kasvavuuden vuoksi $f(y) < f(x)$, mikä on myös vastoin oletusta $f(x) < f(y)$. Siis $x < y$.

b) Olkoot $x, y \in A$ eri alkioita. Tällöin lineaarijärjestyksen $\leq$ vertailullisuudesta seuraa $x \leq y$ tai $y \leq x$, mutta koska $x \neq y$, niin $x < y$ tai $y < x$. Koska f on aidosti kasvava, niin $f(x) < f(y)$ tai $f(y) < f(x)$. Siis joka tapauksessa $f(x) \neq f(y)$. □

Lause 6.32. *Kaikilla $m, n, p \in \omega$ pätee:*

$$m < n \iff m + p < n + p. \tag{1}$$

Jos lisäksi $p \neq 0$, pätee myös:

$$m < n \iff m \cdot p < n \cdot p. \tag{2}$$

Todistus. (1) Oletetaan, että luvuille $m, n \in \omega$ pätee $m < n$, ja osoitetaan ensin induktiolla luvun $p \in \omega$ suhteen, että $m + p < n + p$. Väite pätee arvolla $p = 0$, sillä suoraan oletuksesta saadaan $m + 0 = m < n = n + 0$. Oletetaan sitten, että $m + p = n + p$. Apulauseen 6.26 kohdasta a seuraa, että seuraajakuvaus σ on aidosti kasvava. Siis $m + p^+ = (m + p)^+ = \sigma(m + p) < \sigma(n + p) = (n + p)^+ = n + p^+$, ts. induktioväite pätee myös arvolla p^+.

Jokaisella $p \in \omega$ siis kuvaus $f\colon \omega \to \omega$, $f(x) = x + p$, on aidosti kasvava. Kohdan 1 väite seuraa siis edellisestä lemmasta.

'(2) Oletetaan, että luvuille $m, n \in \omega$ pätee $m < n$, ja osoitetaan induktiolla luvun $p \in \omega$ suhteen, että jos $p \neq 0$, niin $m \cdot p < n \cdot p$. Kun $p = 0$, induktioväite on triviaalisti tosi. Oletetaan sitten, että induktioväite pätee arvolla p. Jos $p = 0$, niin saadaan $m \cdot 0^+ = (m \cdot 0) + m = 0 + m = m < n = n \cdot 0^+$, ts. induktioväite pätee arvolla $p^+ = 0^+ =$

1. Oletaan sitten, että $p \neq 0$. Tällöin induktio-oletuksen mukaan $m \cdot p < n \cdot p$, mistä yhteenlaskun vaihdannaisuutta ja edellistä kohtaa toistuvasti soveltamalla seuraa

$$m \cdot p^+ = m \cdot p + m = m + m \cdot p = m + n \cdot p = n \cdot p + m < n \cdot p + n = n \cdot p^+.$$

Siis (järjestyksen $<$ transitiivisuuden vuoksi) $m \cdot p^+ < n \cdot p^+$ eli induktioväite toteutuu arvolla p^+.

On siis todistettu, että jokaisella $p \in \omega \setminus \{0\}$ kuvaus $f\colon \omega \to \omega$, $f(x) = x \cdot p$ on aidosti kasvava. Edellisen lemman nojalla tästä seuraa kohdan 2 ekvivalenssi. □

Seuraus 6.33. *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. Olkoon $p \in \omega$. Tarkastellaan kuvauksia $f\colon \omega \to \omega$, $f(x) = x + p$, ja $g\colon \omega \to \omega$, $g(x) = x \cdot p$. Edellisen lauseen mukaan f on joka tapauksessa aidosti kasvava ja g on myös, jos $p \neq 0$. Siis apulauseen 6.31 nojalla f on injektio ja g on myös, jos $p \neq 0$, mistä seuraa väite. □

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

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

Luonnollisten lukujen hyvinjärjestyslause. *Luonnollisten lukujen järjestys $<$ on hyvä.*

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

Sopivan induktioväitteen muotoileminen vaatii hiukan oveluutta. Osoitetaan siis induktiolla luvun $n \in \omega$ suhteen, että $n \cap B = \emptyset$. Kun $n = 0$, niin induktioväite pätee, sillä $0 \cap B = \emptyset \cap B = \emptyset$. Oletetaan sitten, että $n \cap B = \emptyset$. Tällöin

$$n^+ \cap B = (n \cup \{n\}) \cap B = (n \cap B) \cup (\{n\} \cap B) = \emptyset \cup (\{n\} \cap B) = \{n\} \cap B.$$

Induktio-oletuksen mukaan pätee $m \notin B$, kun $m \in n$ eli $m \in \omega$ ja $m < n$. Siis jos $n \in B$, niin n olisi joukon B pienin alkio. Tämä ei oletuksen mukaan ole mahdollista, joten $n^+ \cap B = \{n\} \cap B = \emptyset$.

Induktiolla todistetusta väitteestä seuraa nyt jokaiselle $n \in \omega$, että $n \in n^+$, mutta $n^+ \cap B = \emptyset$, joten $n \notin B$. Siis $B = \emptyset$. □

Seuraus 6.34. *Ei ole olemassa kuvausta $f\colon \omega \to \omega$, jolle $f(n^+) < f(n)$ kaikilla $n \in \omega$.*

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

Esimerkki 6.35. Tarkastellaan rekursiivisen määrittelyn mahdollisuuksia kokonaislukujen rakenteessa. Ei ole olemassa sellaista kuvausta $h\colon \mathbb{Z} \to \mathbb{Z}$, että jokaisella $n \in \mathbb{Z}$ pätee

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

Jos nimittäin h olisi tällainen kuvaus, niin kaikilla $n \in \mathbb{Z}$ pätisi ensinnäkin $h(n) = h(n-1)^2 + 1 \geq 0 + 1 = 1 > 0$, joten h olisi kuvaus $\mathbb{Z} \to \omega$. Asetetaan $f\colon \omega \to \omega$, $f(n) = h(-n)$. Tällöin kaikilla $n \in \omega$ pätisi

$$\begin{aligned} f(n) &= h(-n) = h(-(n+1)+1) = h(-(n+1))^2 + 1 = f(n+1)^2 + 1 \\ &\geq f(n+1) + 1 > f(n+1), \end{aligned}$$

mikä on vastoin edellistä seurausta. Siis kaikkia rekursioehtoja ei voida toteuttaa kokonaislukujen rakenteessa.

Toisaalta rekursioehdot eivät määritä kuvauksia yksikäsitteisestikään. 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 kuvausta $h\colon \mathbb{Z} \to \mathbb{Z}$, joille $h(0) = 0$ ja $h(n+1) = F(h(a))$, nimittäin jokaisella $k \in \mathbb{N}$ kuvaus $h\colon \mathbb{Z} \to \mathbb{Z}$, $h(n) = \min\{k+n, 0\}$, toteuttaa rekursioehdon.

Siis rekursiolausetta ei voi yleistää kokonaislukujen joukkoon!

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

$$(*) \qquad (\forall m \in n(m \in A)) \to n \in A,$$

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 $m \in \omega \setminus A$. □

Äärelliset joukot

Intuitiivisesti joukko on äärellinen, jos on mahdollista konkreettisella tavalla laskea, kuinka monta alkiota joukossa on. Tällöin sen alkioiden lukumäärä on luonnollinen luku. Tehdään tästä täsmällinen määritelmä:

Määritelmä 6.36. Joukko A on *äärellinen*, jos $A \approx n$ jollain $n \in \omega$, muutoin A on *ääretön*.

Lokeroperiaate. *Jokainen luonnollinen luku on Dedekind-äärellinen eli mikään $n \in \omega$ ei ole yhtämahtava aidon osajoukkonsa kanssa.*

Todistus. Olkoon funktio $f\colon n \to n$ injektio. Riittää osoittaa, että tällöin $\operatorname{ran}(f) = n$. Osoitetaan siis induktiolla luvun $n \in \omega$ suhteen, että jokainen injektio $f\colon n \to n$ on myös injektio.

1) Ainoa injektio $f\colon 0 \to 0$ on $f = \emptyset$, jolle pätee ja $\operatorname{ran}(\emptyset) = \emptyset = 0$, joten f on tällöin surjektio. Siis induktioväite pätee arvolla $n = 0$.

2) Oletetaan sitten, että induktioväite pätee arvolla n. Olkoon $f\colon n^+ \to n^+$ injektio, jolloin $f \restriction n$ on myös injektio. On kaksi mahdollisuutta:

   a) $f \restriction n$ on injektio $n \to n$. Induktio-oletuksen nojalla $\operatorname{ran}(f \restriction n) = n$. Koska f on injektio, on tällöin oltava $f(n) = n$. Mutta tällöin myös $n \in \operatorname{ran}(f)$, joten f on surjektio.

   b) On olemassa $p \in n$, jolle $f(p) = n$. Palautetaan tilanne tapaukseen (1) määrittelemällä funktio $\hat{f} : n^+ \to n^+$ asettamalla

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

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

□

Seuraus 6.37. *Äärelliset joukot ovat Dedekind-äärellisiä.*

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 $A = B$. □

Seuraus 6.38.

a) Dedekind-äärettömät joukot ovat äärettömiä.

b) ω on ääretön.

Todistus. Kohta a seuraa suoraan seurauksesta 6.37. Kohta b voidaan todeta tarkastelemalla seuraajafunktiota σ. Kuvaus σ on bijektio kuvauksena $\omega \to \omega \setminus \{0\}$, joten $\omega \approx \omega \setminus \{0\}$. Siis ω on Dedekind-ääretön, joten a-kohdan perusteella se on ääretön. □

Seuraus 6.39. *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 $m = n$, $m \subsetneq n$ tai $n \subsetneq m$. Lokeroperiaatteen nojalla kaksi viimeistä vaihtoehtoa ovat mahdottomia, joten $m = n$. □

Apulause 6.40. *Kun $C \subsetneq n$ ja $n \in \omega$, niin on olemassa $m \in n$, jolla $C \approx m$.*

Todistus. Osoitetaan induktiolla luvun $n \in \omega$ suhteen, että jokaisella $C \subsetneq n$ on olemassa $m \in n$, jolle $C \approx m$. Väite pätee tietenkin arvolla $n = 0$, sillä 0:lla ei ole aitoja osajoukkoja. Oletetaan sitten, että väite pätee arvolla n. Olkoon $C \subsetneq n^+$. Tällöin on kolme vaihtoehtoa:

a) $C = n$. Tällöin $C \approx n \in n^+$.

b) $C \subsetneq n$. Induktio-oletuksen nojalla tällöin on olemassa $m \in n$, jolle $C \approx m$. Koska $m \in n \subseteq n^+$, niin $m \in n^+$.

c) $n \in C$. Tällöin $C = (C \cap n) \cup \{n\}$ ja $C \cap n \subsetneq n$. Induktio-oletuksen mukaan on olemassa $m \in n$, jolle $C \cap n \approx m$. Siis on olemassa bijektio $f : C \cap n \to m$. Tällöin $f \cup \{(n, m)\}$ on bijektio $C \to m^+$. Siis $C \approx m^+$. Koska $m \in n$, pätee $m^+ \in n^+$.

□

Seuraus 6.41. *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 6.40 perusteella on olemasssa $m \in n$, jolle $B \approx m$. □

Kirjallisuutta

[End77] Herbert B. Enderton. *Elements of set theory*. Academic Press, 1977.

[Pea89] Giuseppe Peano. *Arithmetices Principia. Nova methodo exposita.* Libreria Bocca, 1889.

[von23] J. von Neumann. Zur Einführung der transfiniten Zahlen. *Acta Litt. Sci. Szeged*, 1:199–208, 1923.

[Zer08] Ernst Zermelo. Untersuchungen über die Grundlagen der Mengenlehre. I. *Mathematische Annalen*, 65(2):261–281, 1908.