4 Luonnolliset luvut

4.1 Hyvinjärjestetyt joukot

Tässä luvussa tarvitsemme seuraavia joukko-opillisia periaatteita.
Valinta-aksiooma.
Tämä periaate sanoo seuraava. Olkoon $(A_i)_{i\in I}$ indeksoitu joukkoperhe. Oletetaan lisäksi, että A_i on epätyhjä joukko jokaisella $i \in I$. Tällöin on olemassa perhe $(x_i)_{i\in I}$ siten, että $x_i \in A_i$ jokaisella $i \in I$.
Voimme siis tehdä mielivaltainen määrä samanaikaisia valintoja tarvittaessa. Useimmiten käytännön sovelluksissa valinta-aksiooma tuntuu itsestään selvältä.
Äärettömyysaksiooma sanoo, että ainakin yksi ääretön joukko on olemassa. Tässä luvussa näytämme kuinka yhden äärettömän joukon avulla (josta ei siis tiedetä mitään muuta kuin vain se, että se on ääretön) voidaan konstruoida luonnollisten lukujen joukko.
Tapamme konstruoida luonnollisten lukujen joukko tulee nojautumaan hyvinjärjestettyjen joukkojen teoriaan, joten ensin joudumme tutustumaan siihen.

Määritelmä 47. *Olkoon $\leq$ relaatio joukossa X (toisin sanoen $\leq \subset X \times X$). Sanomme, että $\leq$ on* osittainen järjestys *jos seuraavat ehdot pätevät.*

(i) Kaikilla $x \in X$ pätee $x \leq x$ (relaation refleksivisyys*).*

(ii) Olkoot $x, y \in X$. Jos $x \leq y$ ja $y \leq x$, niin $x = y$ (relaation antisymmetrisyys*).*

(iii) Olkoot $x, y, z \in X$. Jos $x \leq y$ ja $y \leq z$, niin $x \leq z$ (relaation transitiivisuus*).*
Lisäksi, jos pätee ehto

(iv) Kaikilla $x, y \in X$ joko $x \leq y$ tai $y \leq x$,

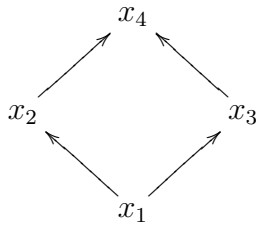
relaatio $\leq$ on (täysi) järjestys[9].
Osittaisjärjestetty joukko on pari $(X, \leq)$, jossa $\leq$ on osittainen järjestys joukossa X. Jos $\leq$ on järjestys, $(X, \leq)$ on (täysin) järjestetty joukko.

Reaalilukujen aksioomat D(i)-D(iv) ilmaisevat tasan sen, että $\leq$ on täysi järjestysrelaatio joukossa $\mathbb{R}$.
Osittaisjärjestetty joukko on määritelmän mukaan pari $(X, \leq)$, jossa X on

[9]Myös termi ”lineaarinen järjestys” on yleisesti käytössä.

joukko ja $\leq$ jokin järjestysrelaatio X:ssä. Usein kuitenkin merkitsemme osittaisjärjestetty joukko $(X, \leq)$ lyhyemmin pelkästään X:llä.
Jos osittaisjärjestetyssä joukossa $x \leq y$ sanotaan, että "x on pienempi tai yhtä suuri kuin y".

Esimerkki 48. *Tärkeä esimerkki osittaisesta järjestyksestä saadaan joukkojen välisestä sisältyvyysrelaatiosta $\subset$. Nimittäin olkoon A joukko. Tällöin sen potenssijoukossa $\mathcal{P}(A)$ on määritelty relaatio $\subset$. Tämä relaatio on osittainen järjestys. Tämä nähdään seuraavasti.*
1) Jokaiselle B:n osajoukolla pätee $B \subset B$,
2) Oletaan, että $B \subset C$ ja $C \subset B$. Tällöin $B = C$, kuten joukkojen yhtäsuuruusperiaatteista seuraa.
3) Jos $B \subset C$ ja $C \subset D$, niin jokainen B:n alkio on C:ssä ja jokainen C:n alkio on vastaavasti D:ssä. Erityisesti jokainen B:n alkio on D:ssä, joten $B \subset D$.
Jos joukossa A on ainakin kaksi alkiota, tämä relaatio ei ole järjestys. Esimerkiksi jos $a, b \in A$, $a \neq b$, niin joukoille $B = \{a\}$ ja $C = \{b\}$ ei päde $B \subset C$ tai $C \subset B$. Samassa joukossa voidaan määritellä osittaisjärjestys $\supset$, joka on määritelty "kääntämällä" järjestyksen $\subset$ määritelmää, eli $B \supset C$ tarkoittaa, että $C \subset B$. Helposti nähdään, että tämä relaatio toteuttaa osittaisen järjestyksen ehtoja.
Yleisemmin olkoon $(X, \leq)$ jokin osittaisjärjestetty joukko. Tällöin voimme määritellä relaatio $\geq$ asettamalla $x \geq y$ jos ja vain jos $y \leq x$. Tällöin $\geq$ on osittaisjärjestys. Se on järjestys jos ja vain jos alkuperäinen osittaisjärjestys $\leq$ on järjestys.
Tarkastellaan vielä vähän tarkemmin osittaisjärjestettyä joukkoa $X = \mathcal{P}(\{a, b\})$, jonka muodostavat kahden alkion joukon osajoukot sisältyvyysrelaationa $\subset$ varustettuna. Joukossa X on neljä alkiota, ne ovat $x_1 = \emptyset$, $x_2 = \{a\}$, $x_3 = \{b\}$, $x_4 = \{a, b\}$. Näiden välissä vallitsevia järjestetyssuhteita voidaan havainnollistaa diagrammilla



Tällaisessa diagrammissa alkio x on pienempi tai yhtä suuri kuin y jos x:stä pääsee y:hyn kulkemalla "polkua" yhdensuuntaisia nuolia pitkin.
Samassa joukossa voidaan määritellä täysi järjestys $\leq$ lisäämällä sisältyvyysrelaatioon mukaan ehto $x_2 \leq x_3$. Formaalisti $\leq = \subset \cup \{(x_2, x_3)\}$. Käytännös-

sä tämä on "luonnollinen järjestys", jossa $x_i \leq x_j$ jos ja vai jos indeksi i on luonnollisena lukuna joukosta $\{1, 2, 3, 4\}$ pienempi tai yhtä suuri kuin indeksi j. Tässä viitamme tavalliseen tuttuun pienten luonnollisten lukujen järjestykseen (joka määritellään tarkasti tässä luvussa myöhemmin). Järjestystä $\leq$ voi havainnollistaa diagrammilla

$$x_1 \longrightarrow x_2 \longrightarrow x_3 \longrightarrow x_4 \ .$$

Olkoon $(X, \leq)$ osittaisjärjestetty joukko ja $Y \subset X$ osajoukko. Tällöin Y:ssä voidaan määritellä luonnollinen järjestys $\leq'$ rajoittamalla X:n järjestystä Y:hyn. Formaalisti siis $\leq' = \leq \cap Y \times Y$. Käytännössä kyseessä on "sama relaatio", mutta pienemmässä joukossa. Yleensä merkitsemme tällä tavalla määriteltyä osajoukon osittaisjärjestystä samalla symbolilla kuin alkuperäinen X:n järjestys eli $(Y, \leq)$ on osittaisjärjestetyn joukon $(X, \leq)$ osittaisjärjestetty osajoukko. Jos $(Y, \leq)$ sattuu olemaan täysin järjestetty, se sanotaan *ketjuksi X:ssä.*
Aina kun puhumme osittaisjärjestetyn joukon $(X, \leq)$ osajoukosta Y tarkoitamme X:n osajoukkoa, joka varustetaan tällä X:n järjestyksen rajoittumalla.

Esimerkki 49. *Tarkastellaan edellisen esimerkin osittaisjärjestettyä joukkoa $X = \mathcal{P}(\{a, b\})$. Merkitään sen alkioita x_i:llä, $i = 1, \ldots 4$, kuten edellä. Osajoukko*

$$\{x_1, x_2, x_4\}$$

on ketju X:ssä, samoin osajoukko

$$\{x_1, x_3, x_4\}.$$

Osajoukko $\{x_1, x_2, x_3\}$ taas ei ole ketju - alkiot x_2 ja x_3 eivät ole verrattavissa keskenään.

Osittaisjärjestetyssä joukossa $(X, \leq)$ voidaan määritellä luonnollisella tavalla "johdonnaisia" relaatioita $\geq$, ("suurempi tai yhtä suuri") $<$("pienempi kuin"), $>$("suurempi kuin"). Näistä ensimmäinen on määritelty jo esimerkissä yllä - $x \geq y$ on sama asia kuin $y \leq x$. Relaatio $\geq$ itse toteuttaa osittaisjärjestyksen ehtoja.
Relaatio $x < y$ määritellään tarkoittamaan $x \leq y$ ja $x \neq y$ ja $x > y$ vastaavasti tarkoittaa, että $y \leq x$ ja $x \neq y$. Nämä toteuttavat seuraavia *aidon järjestysrelaation* ominaisuuksia.

Lemma 50. *Olkoon $(X, \leq)$ osittaisjärjestetty joukko. Tällöin relaatio $<$ toteuttaa seuraavia ehtoja.*

(i) Jokaisella $x \in X$ väite $x < x$ ei päde (relaation antirefleksivisyys*)*

(ii) Olkoot $x, y, z \in X$. Jos $x < y$ ja $y < z$, niin $x < z$. (relaation transitiivisuus*)*

Relaatio $>$ toteuttaa samantyyppisiä ehtoja.
Jos $(X, \leq)$ on täysin järjestetty, relaatio $<$ (ja $>$) toteuttaa lisäksi ehdon

(i)' Olkoot $x, y \in X$. Tällöin täsmälleen yksi seuraavista väitteistä pätee:

$$x < y \text{ tai } x = y \text{ tai } y < x.$$

Ehto (i) yllä tällöin seuraa tästä ehdosta.

Todistus. Harjoitustehtävä (vrt. Lemma 5). □

(Osittais)järjestettyjen joukkojen teoriaa voidaan kehittää myös ottamalla lähtökohdaksi relaatio $<$, joka toteuttaa edellisen Lemman ehtoja. Tällöin $\leq$ määritellään ehdolla $x \leq y$ jos ja vain jos $x < y$ tai $x = y$ ja se toteuttaa osittaisjärjestyksen ehtoja. Tämä tapa "koodata" järjestyksen käsitettä relaation $<$ avulla on täysin ekvivalentti meidän tavan kanssa.
Osittaisjärjestettyjä joukkoja voidaan "vertailla" keskenään järjestystä säilyttävien kuvausten avulla.

Määritelmä 51. *Olkoot $(X, \leq)$ ja $(Y, \leq')$ osittaisjärjestettyjä joukkoja ja $f \colon X \to Y$ kuvaus. Sanomme f* morfismiksi *jos se säilyttää järjesysrelaation eli jos kaikilla $a, b \in X$, $a \leq b$ pätee*

$$f(a) \leq f(b).$$

Injektiivinen morfismi on monomorfismi.
Jos f on bijektiivinen morfismi, jonka käänteiskuvaus f^{-1} on myös morfismi, f sanotaan isomorfismiksi.

Termi "isomorfismi " saattaa olla lukijalle tuttu algebran kursseilta, joilla tällä sanolla tarkoitetaan esimerkiksi ryhmien välistä kuvausta, joka säilyttää ryhmien laskutoimituksia. Yleisesti matematiikassa sanaa "isomorfismi" käytetään usein merkityksessä "struktuuria täydellisesti säilyttävä bijektiivinen kuvaus", joten termin sisältö riippuu siitä, minkälaisista struktuureista on kyse. Morfismi on yleisempi käsite - se on mikä tahansa kuvaus joka säilyttää kyseessä olevaa struktuuria, siirtää se maalijoukkoon. Isomorfismi on tällöin bijektivinen morfismi, jonka käänteiskuvaus (joka on olemassa, koska kuvaus oletetaan bijektiiviseksi, Lemma 31) on myös morfismi.

Algebrassa ehto "f^{-1} myös morfismi " voidaan poistaa isomorfismin määritelmästä, koska voidaan osoittaa, että jos bijektiivinen kuvaus säilyttää esimerkiksi kertolaskun, sen käänteiskuvaus automaattisesti säilyttää kertolaskun myös, joten määritelmässä ei tarvitse siitä erikseen mainita.
Osittaisjärjestettyjen joukkojen kohdalla asia ei ole niin yksinkertainen ja bijektiivinen morfismi ei vältämättä ole isomorfismi.

Esimerkki 52. *Olkoon $X = \mathcal{P}(\{a, b\})$. Esimerkissä 48 olemme määritelleet joukossa X kaksi erilaista järjestysrelaatiota - luonnollisen osajoukkojen sisältyvyys relaation $\subset$ ja relaation $\leq = \subset \cup \{(\{a\}, \{b\})\}$, jossa lisättiin sisältyvyysrelaation lisäksi vielä ehto $x_1 = \{a\} \leq \{b\} = x_2$. Identtinen kuvaus* $\mathrm{id}\colon X \to X$ *on morfismi osittaisjärjestetystä joukosta $(X, \subset)$ järjestetyyn joukkoon $(X, \leq)$. Lisäksi se on tietysti bijektio. Sen käänteiskuvaus* $\mathrm{id}\colon X \to X$ *ei ole kuitenkaan morfismi järjestetystä joukosta $(X, \leq)$ osittaisjärjestetyyn joukkoon $(X, \subset)$.*

Esimerkki 53. *Olkoon A joukko ja $X = \mathcal{A}$ joukon X potenssijoukko. Esimerkin 48 nojalla X:ssä voidaan määritellä osittaisjärjestyksiä $\subset$ ja $\supset$, jolloin voimme tarkastella osittaisjärjestettyjä joukkoja $(X, \subset)$ ja $(X, \supset)$.*
Osoitetaan, että kuvaus $f\colon (X, \subset) \to (X, \supset)$, $f(B) = A \setminus B$ on isomorfismi. Ensinnäkin $f \circ f = \mathrm{id}_X$, joten f on itseensä käänteiskuvaus, erityisesti f on bijektio. Olkoot $B, C \in X$, $B \subset C$. Tällöin $A \setminus C \subset A \setminus B$. Tämä nähdään seuraavasti. Jos $x \in A \setminus C$, niin $x \in A$ ja $x \notin C$. Jos olisi $x \in B$, niin sisältyvyyden $B \subset C$ nojalla pätisi myös $x \in C$, mikä on vastoin oletusta. Näin ollen $x \in A$ ja $x \notin B$ eli $x \in A \setminus B$. Näin ollen

$$f(B) = A \setminus B \supset A \setminus C,$$

joten $f\colon (X, \subset) \to (X, \supset)$ on morfismi.
Pitää vielä tarkistaa, että $f^{-1} = f\colon (X, \supset) \to (X, \subset)$ on morfismi. Tämä nähdään samalla tavalla kuin f:lle (käy läpi). Näin ollen f on isomorfismi.
Olkoon $B \subset A$ ja määritellään osittaisjärjestetty joukko $(Y, \supset)$, missä $Y = \mathcal{B}$. Määritellään kuvaus $f\colon X \to Y$ kaavalla $f(C) = C \cap B$. Helposti nähdään (HT) että f on surjektiivinen morfismi. Se ei kuitenkaan ole injektio, jos B on aito A:n osajoukko, sillä esimerkiksi $f(B) = f(A)$.

Täysin järjestettyjen joukkojen tapauksessa bijektiviinen morfismi on aina myös isomorfismi. Tämä on hyödyllistä tietää, koska tällä kurssilla olemme kiinnostuneita lähinnä vain täysin järjestetyistä joukoista.

Lemma 54. *Olkoon $(X, \leq)$* täysin *järjestetty joukko ja $(Y, \leq')$ osittaisjärjestetty joukko. Tällöin jokainen bijektiivinen morfismi $f\colon X \to Y$ on itse asiassa isomorfismi.*

Todistus. Olkoon $f\colon X \to Y$ bijektiivinen morfismi. Osoitetaan, että $g = f^{-1}\colon Y \to X$ on myös morfismi. Oletetaan, että $y, z \in Y$ ja $y \leq' z$. Merkitään $a = g(y)$ ja $b = g(z)$. Tällöin $f(a) = y$ ja $f(b) = z$. Meidän on osoitettavaa, että X:ssä pätee

$$g(y) = a \leq b = g(z).$$

Koska $(X, \leq)$ on täysin järjestetty, pätee joko $a \leq b$ tai $b < a$ (tämä on se todistuksen kohta, jossa tarvitaan "oletus X on täysin järjestetty"). Näin ollen riittää osoittaa, että oletus $b < a$ johtaa ristiriitaan.
Oletetaan, että $b < a$. Tällöin erityisesti $b \leq a$, joten, koska f on morfismi, pätee $z = f(b) \leq' f(a) = y$. Lisäksi, koska $a \neq b$ ja f on injektio, $y = f(a) \neq f(b) = z$, joten $z \leq' y$ ja $z \neq y$, toisin sanoen $z <' y$. Kuitenkin toisaalta $y \leq' z$ (oletus, josta lähdettiin). Lemman 50 mukaan ei voi olla samaan aikaan $z <' y$ ja $y \leq z'$, joten päädytiin ristiriitaan. Näin ollen oletus $b < a$ on mahdoton, joten on pakko olla $a \leq b$. Todistus on valmis. □

Seuraus 55. *Olkoon $(X, \leq)$ täysin järjestetty joukko ja $(Y, \leq')$ osittaisjärjestetty joukko. Olkoon $f\colon X \to Y$ monomorfismi ja merkitään $A = f(X)$. Tällöin rajoittuma $f\colon X \to A$ on järjestettyjen joukkojen välinen isomorfismi.*

Sanomme, että osittaisjärjestetyt joukot $(X, \leq)$ ja $(Y, \leq')$ ovat *isomorfisia*, jos on olemassa isomorfismi $f\colon X \to Y$. Tällöin merkitään $X \cong Y$. Huomaa, että jos $X \cong Y$, niin myös $Y \cong X$, sillä isomorfismin $f\colon X \to Y$ käänteiskuvaus on myös isomorfismi (miksi?). Lisäksi, jos $f\colon X \to Y$ ja $g\colon Y \to Z$ ovat osittaisjärjestettyjen joukkojen $(X, \leq)$, $(Y, \leq')$, $(Z, \leq'')$ välisiä isomorfismeja, yhdistetty kuvaus $g \circ f\colon X \to Z$ on myös isomorfismi (miksi?), joten pätee seuraava luonnollinen transitiivisuusominaisuus
jos $X \cong Y$ ja $Y \cong Z$, niin $X \cong Z$.
Isomorfiset järjestetyt joukot "näyttävät samalta" ja järjestettyjen joukkojen teoria ei pysty näkemään mitään eroa niiden välillä.
Yleisesti matematiikassa kaksi struktuuria ovat isomorfisia, jos niiden välissä on isomorfismi. Tällöin ne ovat "samanlaisia".

Olkoon $(X, \leq)$ osittaisjärjestetty joukko ja olkoot $x, y \in X$. Oletetaan, että $x < y$. Tällöin sanomme, että x on y:n *edeltäjä* ja y on x:n *seuraaja*. Jos lisäksi x:n ja y:n välillä ei ole muita alkioita, eli jos ei ole olemassa $z \in X$ jolle $x < z$ ja $z < y$, sanomme, että x on y:n *välitön edeltäjä* ja y on vastaavasti x:n *välitön seuraaja*.
Kaikki alkion edeltäjät muodostavat osajoukon $I(x)$, joka sanotaan (alkion x määrämäksi) *alkusegementiksi*. Toisin sanoen

$$I(x) = \{y \in X \mid y < x\}.$$

Erityisen tärkeitä alkusegmentit ovat hyvinjärjestettyjen joukkojen teoriassa, kuten jatkossa näemme.

Esimerkki 56. *Oletetaan reaalilukujen ominaisuuksia tunnettuina.*

(1) Reaalilukujen negatiivisten alkioiden joukko on 0*:n määrämä alkusegmenti* $I(0)$*. Ei-positiivisten lukujen joukko taas ei ole minkään alkion määrämä alkusegmentti.*

(2) Joukossa $\mathbb{R}$ *osajoukko*

$$\{x \in \mathbb{R} \mid x < 0 \text{ tai } x^2 < 2\}$$

on alkusegmentti, se on $I(\sqrt{2})$*. Rationaalilukujen joukossa* $\mathbb{Q}$ *joukko*

$$\{x \in \mathbb{Q} \mid x < 0 \text{ tai } x^2 < 2\}$$

ei ole alkusegmentti. Tämä johtuu juuri siitä, että $\mathbb{Q}$*:ssä ei ole alkiota jolle* $x^2 = 2$*.*

Osittaisjärjestetyssä joukossa voidaan määritellä tuttuja käsiteittä yläraja, alaraja, suurin alkio, pienin alkio jne.
Olkoon $(X, \leq)$ osittaisjärjestetty joukko ja $A \subset X$ sen osajoukko. Alkio $x \in X$ on A:n *yläraja* jos kaikilla $a \in A$ pätee $a \leq x$. Alkio x on osajoukon A *suurin alkio* jos se on A:n yläraja, joka itse on A:n alkio eli yläraja x jolle pätee myös $x \in A$.
Alaraja ja pienin alkio määritellään analogisesti. Alkio y on A:n alaraja jos kaikilla $a \in A$ pätee $y \leq a$. Jos lisäksi tässä $y \in A$, niin y sanotaan A:n pienemmäksi alkioksi.
Joukkoa, jolla on ainakin yksi yläraja, sanotaan *ylhäältä rajoitetuksi*. Vastaavasti joukkoa, jolla on ainakin yksi alaraja, sanotaan *alhaalta rajoitetuksi*. Joukko on *rajoitettu* jos se on sekä ylhäältä, että alhaalta rajoitettu.
Ylhäältä rajoitetulla joukolla voi olla monta erilaista ylärajaa, yläraja ei ole yleensä yksikäsitteinen. Jos x on A:n yläraja, niin mikä tahansa aidosti isompi alkio $y > x$ on myös yläraja (transitiivisuuden nojalla). Samoin alarajoja on yleensä paljon. Suurin ja pienin alkio taas ovat aina yksikäsitteisiä jos ne ovat olemassa. Osoitetaan tämä. Olkoon $A \subset X$ osajoukko ja olkoot $x, y \in A$ molemmat A:n suurin alkio. Koska y on A:n yläraja ja $x \in A$, niin erityisesti pätee $x \leq y$. Samalla perusteella nähdään, että $y \leq x$. Järjestysrelaation antisymmetrisyydestä (ominaisuus (ii) osittaisjärjestyksen määritelmässä) seuraa, että $x = y$.
Samalla tavalla nähdään, että pienin alkio on aina yksikäsitteinen, jos on olemassa.

Esimerkki 57. *Olkoon $X = \mathcal{P}(A)$ joukon A potenssijoukko osittaisjärjestyksellä varustettuna. Jokainen X:n alkio on rajoitettu sekä ylhäältä, että alhaalta X:ssä, sillä kaikilla $B \subset A$ pätee*

$$\emptyset \subset B \subset A,$$

joten $\emptyset$ kelpaa minkä tahansa osajoukon $Y \subset X$ alarajaksi ja koko joukko A kelpaa minkä tahansa osajoukon $Y \subset X$ ylärajaksi. Erityisesti $\emptyset$ on X:n pienin alkio ja A on X:n suurin alkio.
Olkoon edellä $A = \{a, b\}$ kahden alkion joukko ja merkitään $X = \mathcal{P}$:n alkioita $x_1, \ldots, x_4$, kuten esimerkissä 48. Osajoukko $Y = \{x_2, x_3\}$ on sekä alhaalta, että ylhäältä rajoitettu X:ssä, mutta sillä ei ole pienintä eikä suurinta alkiota. Huomaa, että x_2 esimerkiksi ei kelpaa pienimmäksi alkioksi, koska $x_2 \leq x_3$ ei päde. Se ei myöskään kelpaa suurimmaksi alkioksi, koska $x_3 \leq x_2$ ei päde. Samasta syystä x_3 ei ole pienin eikä suurin alkio.
Jos joukko Y tarkastellaan itsenäisenä osittaisjärjestettynä joukkona (ei X:n osajoukkona), se on esimerkki äärellisestä osittaisjärjestetystä joukosta, jolla ei ole pienintä eikä suurinta alkiota. Jos järjestys on täysi tämä ei ole mahdollista - jokaisessa täysin järjestetyssä äärellisessä joukossa on sekä pienin, että suurin alkio, mikä tuntuu intuitiivisesti aika selvältä. Emme osaa kuitenkin tätä vielä todista ihan täsmällisesti (tarvitaan induktiota).

Tärkeän luokan osittaisjärjestettyjä joukkoja muodostavat niin sanotut *hyvinjärjestetyt joukot*.

Määritelmä 58. *Hyvinjärjestetty joukko on sellainen täysin järjestetty joukko $(X, \leq)$, jonka jokaisella epätyhjällä osajoukolla $A \subset X$ on X:ssä olemassa pienin alkio.*[10].
Jos $(X, \leq)$ on hyvinjärjestetty joukko, relaatiota $\leq$ sanotaan joukon X hyvinjärjestykseksi.

Hyvinjärjestetyn joukon määritelmästä seuraa helposti, että hyvinjärjestetyn joukon mielivaltainen osajoukko on myös hyvinjärjestetty joukko.

Reaalilukujen täysin järjestetty joukko $(\mathbb{R}, \leq)$ ei ole hyvinjärjestetty. Esimerkiksi positiivisten reaalilukujen joukko on epätyhjä, mutta siinä ei ole pienintä lukua (helppo seuraus Lemmasta 7).
Emme pysty tässä vaiheessa antamaan vielä täsmällisiä epätriviaaleja esimerkkejä hyvinjärjestetyjstä joukoista, mutta intuitiomme (sekä mahdollisesti aikaisempi matemaattinen koulutus) sanoo, että luonnollisten lukujen

[10]määritelmässä voidaan täysin järjestetty korvata osittaisjärjestetyllä, todistus harjoitustehtävänä.

joukon pitäisi olla hyvinjärjestetty sen tavallisen järjestyksen suhteen. Käytämme tätä intuitiivista mielikuvaa hyväksi määrittelemällä luonnollisten lukujen joukko eräänä hyvinjärjestettynä joukkona. Samalla tästä saadaan motivaatio hyvinjärjestettyjen joukkojen tutkimiseen.

Määritelmä 59. *Luonnollisten lukujen joukko on sellainen ääretön hyvinjärjestetty joukko* $(\mathbb{N}, \leq)$*, jonka jokainen alkusegmentti on äärellinen. Luonnollisten lukujen joukon alkioita kutsumme luonnollisesti luonnollisiksi luvuiksi.*

Tässä määritelmässä termejä "äärellinen" ja "ääretön" pitää tietenkin ymmärtää samalla tavalla kuin määrittelimme niitä edellisessä luvussa mahtavuusvertailujen kautta (Määritelmä 39).
Tämän aliluvun tavoitteena on osoittaa täsmällisesti, että yllämääritelty luonnollisten lukujen joukko on olemassa ja lisäksi yksikäsitteinen isomorfiaa vaille. Tietysti, jos $(\mathbb{N}, \leq)$ on hyvinjärjestetty joukko, joka toteuttaa määritelmän 59, niin mikä tahansa järjestetty joukko $(\mathbb{N}', \leq')$, joka on isomorfinen $(\mathbb{N}, \leq)$:n kanssa myös toteuttaa saman määritelmän, joten myös ON luonnollisten lukujen joukko. Se kuitenkin "näyttää" ihan samalta kuin $(\mathbb{N}, \leq)$ ja sillä on samoja ominaisuuksia, joten se kelpaa yhtä hyvin. Yksikäsitteisyys isomorfiaa vaille tarkoittaa, että tämä on pahinta mitä voi tapahtua - mitkä tahansa kaksi hyvinjärjestettyä joukkoa $(\mathbb{N}, \leq)$ ja $(\mathbb{N}', \leq')$, jotka toteuttavat määritelmän 59 ovat isomorfisia. Tässä mielessä luonnollisten lukujen joukko tulee siis olemaan "yksikäsitteinen".

Ennen kuin voidaan todistaa luonnollisten lukujen olemassaoloa ja yksikäsitteisyyttä, meidän on kehitettävää hyvinjärjestettyjen joukkojen teoriaa yleisesti.
Tyhjä joukko $\emptyset$ (varustettuna tyhjällä järjestysrelaatiolla) on triviaalisti hyvinjärjestetty (tyhjän joukon logiikka). Samoin yhden alkion järjestetty joukko $(\{x\}, \leq)$ varustettuna ainoana mahdollisena järjestysrelaatiollaan on hyvinjärjestetty. Kahden alkion joukon $\{x, y\}$ järjestysrelaatio on hyvinjärjestys jos ja vain jos se on täysijärjestys eli $x \leq y$ tai $y \leq x$.

Olkoon $(X, \leq)$ epätyhjä hyvinjärjestetty joukko. Tällöin X on itseensä epätyhjä osajoukko, joten X:llä on erityisesti pienin alkio. Tätä alkioita merkitsemme symbolilla 0 (*hyvinjärjestetyn joukon nolla-alkio*). Tyhjässä hyvinjärjestetystä joukossa pienintä alkioita ei tietenkään ole. Huomaa, että jos X on hyvinjärjestetty joukko, niin 0:n alkusegmentti $I(0)$ on tyhjä joukko. Suurinta alkiota hyvinjärjestyssä joukossa ei välttämättä ole. Esimerkiksi luonnollisten lukujen joukossa ei tunnetusti ole suurinta alkiota (tarkka todistus HT).

Olkoon $(X, \leq)$ hyvinjärjestetty jouko ja $x \in X$. Oletetaan lisäksi, että x *ei ole* X:n suurin alkio. Tästä seuraa, että joukko

$$S = \{y \in X \mid y > x\}$$

on epätyhjä. Nimittäin, koska x ei ole suurin alkio, ei ole totta, että kaikilla $y \in X$ pätee $y \leq x$, joten on olemassa ainakin yksi $y \in X$ jolle $y \leq x$ ei päde. Koska X on lisäksi täysin järjestetty, pitää olla $y > x$. Huomaa, että tämän tyyppinen argumentti EI menisi läpi osittaisjärjestetyssä joukossa, joka ei ole välttämättä täysin järjestetty.
Koska osajoukko S yllä ei ole tyhjä, hyvinjärjestetyn joukon määritelmästä seuraa, että S:ssä on olemassa pienin alkio y. Määritelmästä seuraa, että y on itse asiassa x:n välitön seuraaja X:ssä. Tätä alkiota merkitään x^+. Alkion x välitön seuraaja on siis pienin X:n alkio, joka on aidosti suurempi kuin x. Jos hyvinjärjestetyssä joukossa on suurin alkio, sillä ei tietenkään ole välitöntä seuraajaa.
Vaikka hyvinjärjestetyn joukon jokaisella alkiolla, joka ei ole suurin alkio, on olemassa välitön seuraaja, välitöntä edeltäjää sillä ei tarvitse olla, vaikka alkio ei ole pienin alkio 0 (jolla välitöntä edeltäjää ei tietysti ole). Tästä nähdään esimerkkejä myöhemmin.

Aloittamalla hyvinjärjestetyn joukon X pienemmästä alkiosta 0 voimme konstruoida alkioita

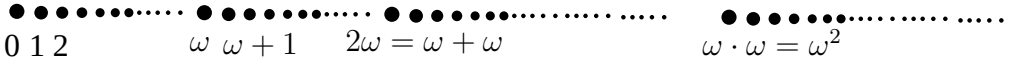
$$1 = 0^+, 2 = 1^+, 3 = 2^+ \text{ jne.}$$

edellyttäen tietysti, että alkio, josta otetaan välitön seuraaja ei ole suurin alkio. Intuitiivisesti on selvä, että tällä tavalla joko törmätään jossakin vaiheessa joukon suurempaan alkioon, jolloin X paljastuu olemaan äärellinen, tai sitten voidaan jatkaa tätä prosessia loputtomiin ja konstruoida alkioita $0, 1, 2, 3, 4, \ldots, 10, \ldots, 2765$ ja niin edelleen. Jälkimmäisessä tapauksessa näyttää siltä, että X ”alkaa” luonnollisten lukujen joukolla eli joukon alussa (järjestyksen suhteen) on ääretön pätkä, joka näyttää ihan luonnollisten lukujen joukolta. Tähän joukon X ei kuitenkaan tarvitse loppua! Jos näin löydetty ”luonnollisten lukujen” pätkä A on X:n aito osajoukko, epätyhjässä joukossa $X \setminus A$ on pienin alkio, merkitään sitä symbolilla ω. Nyt voidaan aloittaa ”alusta” ja muodostaa alkioita

$$\omega + 1 = \omega^+, \omega + 2, \ldots$$

ja niin edelleen. Saadaan ikään kuin uusi ”pätkä”, joka näyttää luonnollisilta luvuilta. Tämä prosessi voi taas loppua suurimpaan alkioon tai jatkua loputtomiin. Jälkimmäisessä tapauksessa jatketaan luvusta $\omega + \omega$ alkaen samalla

tavalla. Tällä tavalla joukko X ”tyhjennetään”. Todellisuudessa prosessi voi jatkua erittäin ”pitkään”. Joukolta $\mathbb{N}$ näyttäviä pätkiä voi tulla peräkkäin ääretön määrä. Alla annetussa kuvassa merkintä $\omega^2 = \omega \cdot \omega$ viittaa juuri tällaiseen mahdollisuuteen.



”To the infinity and beyond”

Palautetaan mieleen Luvussa 3 esille tullut esimerkki opiskelijoiden ja istumapaikkojen muodostamien joukkojen lukumäärien laskemista. Reaalielämästä tiedämme kaksi tapaa vertailla joukkojen kokoja. Ensimmäinen perustuu siihen, että oikeasti lasketaan kuinka monta alkiota joukossa on. Tämän tavan totesimme Luvussa 3 toistaiseksi kelvottamaksi, koska se perustui lukuihin, joita ei vielä ollut käytössä. Tämä johti siihen, että keksimme bijektioihin perustuvaa tapaa vertailla joukkoja, eli mahtavuuksia.
Nyt voimme palata ensimmäiseen tapaan vertailla joukkoja uudestaan eli ”laskemiseen”.
Luonnollisia lukuja keksittiin aikoinaan siihen, että äärellisen joukon alkioita voisi *laskea* käymällä niitä yksi kerrallaan kunnes kaikki saadaan laskettua. Oikeastaan siinä ei ole kyse ”laskemisesta” algebrallisessa mielessä vaan pikemminkin siitä, että käydään joukon alkioita läpi ja leimataan jokainen luonnollisella luvulla - alkio 1, alkio 2 ja niin edelleen. Tällaista leimaamista voi ajatella yrityksenä määritellä joukossa järjestystä alkioiden välillä - alkio 1 on pienin, seuraava on alkio 2 ja niin edelleen.

Hyvinjärjestys voi ymmärtää yleistyksenä tästä alkioiden laskemisen ”yksi kerrallaan” periaatteesta - sovellettuna mahdollisesti äärettömiin joukkoihin. Osoittautuu (emme mee tällä kurssilla tähän syvällisemmin), että äärellisen joukon kohdalla kaikki tavat laittaa äärellisen joukon alkioita hyvinjärjestykseen ovat oleellisesti samoja eli isomorfisia. Tietenkin konkrettisen äärellisen joukon alkioita voi laittaa eri tavalla järjestykseen, esimerkiksi voidaan aloittaa mistä tahansa alkiosta, mutta kuitenkin kaksi eri tapaa ovat isomorfisia keskenään. Sen sijaan jos joukko on ääretön, on olemassa hyvin paljon erilaisia tapoja käydä läpi sen alkioita. Esimerkiksi olkoon X joukko, joka on yhtämahtava luonnollisten lukujen joukon kanssa (tällaisia joukkoja sanotaan *numeroituviksi*). Tällöin yksi tapa määritellä siihen hyvinjärjestys olisi sama kuin luonnollisten lukujen hyvinjärjestys. Toinen tapa olisi jättää yksi alkio ω ”jälkiruoaksi” ja järjestää ensin kaikkia muita alkiota kuten luonnollisia lukuja ja lisätä ω vasta sen jälkeen joukon suurimmaksi alkioksi. Tämä

tapa ei ole isomorfinen edellisen kanssa. Tämä on helppo päätellä esimerkiksi siitä, että ensimmäisessä järjestyksessä ei ole suurinta alkiota, mutta toisessa on (isomorfisilla järjestyksillä on oltava samoja ominaisuuksia). Voidaan osoittaa, että oleellisesti erilasia (ei-isomorfisia) tapoja järjestää tällä tavalla äärettömän joukon alkioita "jonoon" (eli hyvinjärjestykseen) on jopa enemmän (mahtavuuden mielessä) kuin alkioita joukossa itse! Esimerkiksi ei-isomorfisia numeroituvia hyvinjärjestettyjä joukkoja on ylinumeroituva määrä.

Induktio.
Hyvinjärjestettyjen joukkojen tärkeys piilee muun muassa siinä, että ne ovat juuri sellaisia matemaattisia objekteja, joissa pätee *induktioperiaate*. Tuttu luonnollisten lukujen induktio on erikoistapaus tästä yleisestä ominaisuudesta, jota muotoillaan ja todistetaan täsmällisesti seuraavassa tuloksessa.

Olkoon $(X, \leq)$ järjestetty joukko ja $S \subset X$. Sanomme osajoukko S *induktiiviseksi*, jos se se toteuttaa jokaisella $x \in X$ seuraavan ehdon :
Jos jokaiselle $y \in X$, $y < x$ pätee $y \in S$, niin myös $x \in S$.
Huomaa, tämä ehto EI tarkoita sitä, että jokainen $x \in X$ olisi vältämättä joukossa S, vaan ainoastaan sitä, että X:n alkio x on S:n alkio JOS tiedämme jo, että kaikki sen edeltäjät ovat S:ssä.
Esimerkiksi $\mathbb{R}$:n osajoukko $S = \{x \in \mathbb{R} \mid x < 1\}$ ei ole induktiivinen. Se johtuu siitä, että alkiolle $1 \in \mathbb{R}$ pätee ehto "jokainen reaaliluku x joka on pienempi kuin 1 on S:n alkio", mutta $1 \notin S$.
Osajoukko $S = \{x \in \mathbb{R} \mid x \leq 1\}$ on taas induktiivinen $\mathbb{R}$:ssä. Osoitetaan tämä vasta-oletuksella. Olkoon $x \in \mathbb{R}$ sellainen, että jokainen $y < x$ on S:n alkio, mutta $x \notin S$, eli $x > 1$. Lemman 7 nojalla on olemassa $r \in \mathbb{R}$, $1 < r < x$. Tällöin $r < x$, mutta $r \notin S$. Tämä on vastoin oletusta "jokainen $y < x$ on S:n alkio". Näin ollen tapaus $x > 1$ on mahdoton ja täytyy olla $x \geq 1$, joten $x \in S$.
Yllä olemme näyttäneet esimerkin $\mathbb{R}$:n aidosta osajoukosta, joka on induktiivinen. Hyvinjärjestetyissä joukossa tällainen esimerkki on mahdoton.

Propositio 60. Induktio-periaate hyvinjärjestetyille joukoille.
Olkoon $(X, \leq)$ hyvinjärjestetty joukko. Olkoon $S \subset X$ induktiivinen osajoukko. Tällöin $S = X$.
Toisin sanoen X on ainoa itseensä osajoukko, joka sisältää alkion jos ja vain jos se sisältää kaikkia tämän alkion "edeltäjiä."

Todistus. Olkoon S joukko, joka toteuttaa Proposition ehdon. Väite $S = X$ on yhtäpitävä väitteen $X \setminus S = \emptyset$, joten todistetaan, että $A = X \setminus S$ on tyhjä joukko. Tehdään vasta-oletus - A on epätyhjä. Tällöin, koska X on

hyvinjärjestetty, A:llä on pienin alkio $x \in A$. Tästä seuraa, että jos y on x:n edeltäjä järjestysrelaatiossa, $y < x$, niin $y \notin A$ (muuten x ei olisi pienin A:n alkio). Mutta jos $y \notin A = X \setminus S$, se tarkoittaa sitä, että $y \in S$.
Toisin sanoen kaikilla $y < x$ pätee $y \in S$. Oletuksen nojalla tämä tarkoittaa sitä, että myös $x \in S$. Tämä on kuitenkin mahdotonta, sillä $x \in A = X \setminus S$. Näin ollen oletus $S \neq X$ johtaa ristiriitaan, joten täytyy olla $S = X$. □

Induktio-periaatetta käytetään, kun halutaan osoittaa joku väite kaikille hyvinjärjestetyn joukon alkioille. Olkoon $P(x)$ joku väite tai ominaisuus, joka riippuu X:n alkioista x. Haluamme osoittaa, että $P(x)$ on tosi kaikilla $x \in X$. Tällöin riittää osoittaa seuraava.
Oletetaan, että $x \in X$ on mielivaltainen ja oletetaan, että $P(y)$ on tosi kaikilla $y < x, y \in X$. Jos tämän jälkeen pystytään osoittamaan, että myös $P(x)$ on tosi, tästä induktio-periaatteella seuraa, että $P(x)$ on tosi kaikilla $x \in X$.
Tällainen väitteen todistaminen induktiolla perustuu edelliseen Propositioon seuraavalla tavalla. Muodostetaan X:n osajoukko

$$S = \{x \in X \mid P(x) \text{ on tosi}\}.$$

Tavoitteena on näyttää, että itse asiassa $S = X$. Mutta jos S:lle pätee aina, että oletuksesta kaikilla "$y < x$ on voimassa $y \in S$" seuraa $x \in S$, niin S toteuttaa edellisen proposition oletuksia, joten $S = X$, kuten pitikin todistaa.
Induktio-periaatteen käytöstä on vaikeata antaa konkreettisia esimerkkejä tässä vaiheessa, kun käytössämme ei ole vielä esimerkiksi luonnollisten lukujen joukkoa, mutta lukija on varmasti nähnyt aikaisemmin esimerkkejä induktion soveltamisesta luonnollisten lukujen joukossa.
Yleensä luonnollisia lukuja koskeva induktio-periaate muotoillaan hieman eri tavalla, esimerkiksi siihen sisältyy aina alkuaskel, jossa osoitetaan ensin, että väite pätee ensimmäiselle alkiolle 0. Proposition 60 muotoilussa versiossa induktiosta tämä "alkuaskel" sisältyy oletukseen jos valitaan x:ksi pienin X:n alkio 0. Nimittäin tällöin ei ole olemassa $y < x = 0$, joten väite $y \in S$ kaikilla $y < 0$ pätee triviaalisti (tyhjän joukon logiikka!). Näin ollen oletuksen mukaan pätee myös $0 \in S$. Alkuaskel on siis jo "koodattu" yllä muotoiluun induktio-periaatteeseen mukaan.
Lisäksi luonnollisten lukujen induktion kohdalla induktioaskel muotoillaan yleensä muodossa "jos $P(n)$ on totta, niin $P(n^+) = P(n+1)$ on myös totta". Palataan tähän tarkemmin myöhemmin luonnollisten lukujen kohdalla, jolloin näytetään, että ennestään tuttu induktio-periaate luonnollisille luvuille ja tämä uusi induktio-periaate ovat luonnollisten lukujen joukossa $\mathbb{N}$ yhtäpitäviä. Yleisissä hyvinjärjestetyissä joukoissa ne eivät ole (pidä tämä mielessä!).
Induktiolla voidaan myös konstruoida esimerkiksi kuvauksia. Oletetaan, että

$(X, \leq)$ on hyvinjärjestetty joukko ja Y mikä tahansa joukko, jossa siis emme oleta olevan mitään järjestystä tai muuta struktuuria. Tällöin voimme konstruoida haluttuja kuvauksia $f\colon X \to Y$ induktiolla. Tämä tarkoittaa sitä, että $f(x)$ konstruoidaan olettamalla, että $f(y)$ on jo konstruoitu kaikilla $y < x$ jolloin niitä voi käyttää kun määrää arvon $f(x)$. Tällaisen kuvauksen olemassaolo ja yksikäsitteisyys voidaan osoittaa vetoamalla (muun muassa) induktio-periaatteeseen. Tarkka perustelu sivutetaan.

Hyvinjärjestyslause.
Koska hyvinjärjestetyt joukot käyttäytyvät niin säännöllisesti ja niillä on niin paljon hyödyllisiä ominaisuuksia, herää kysymys siitä, mitä joukkoja voidaan *hyvinjärjestää* . Toisin sanoen jos X on mielivaltainen joukko, niin voidaanko X:ssä määritellä jokin hyvinjärjestys? Osoittautuu, että voidaan. Tätä tulosta sanotaan *hyvinjärjestyslauseeksi*. Emme todista tällä kurssilla tätä lausetta, sillä todistus on pitkä ja vaikea.

Lause 61. *Olkoon X joukko. Tällöin X:ssä on olemassa relaatio $\leq$ siten, että $(X, \leq)$ on hyvinjärjestetty joukko.*

Hyvinjärjestyslause on itse asiassa ekvivalentti valinta-aksiooman kanssa. Tämä tarkoittaa sitä, että hyvinjärjestyslauseen todistuksessa käytetään valinta-aksioomaa ja kääntäen, jos oletetaan todeksi kaikki muut joukko-opin aksioomat ja lisäksi oletetaan, että hyvinjärjestyslause pätee, niin valinta-aksiooma voidaan todistaa todeksi.
Hyvinjärjestyslause on erittäin tärkeä meidän kannalta, koska konstruoimme myöhemmin luonnollisia lukuja juuri tämän lauseen avulla. Seuraavaksi tutkitaan hyvinjärjestettyjen joukkojen välisiä monomorfismia. Osoittautuu, että niitä on olemassa ”juuri sopivasti”.

Lemma 62. *Olkoon $(X, \leq)$ hyvinjärjestetty joukko ja $f\colon X \to X$ monomorfismi X:stä itselleen. Tällöin $f(x) \geq x$ kaikilla $x \in X$.*

Todistus. Riittää todistaa, että vasta-oletus johtaa ristiriitaan. Vasta-oletus väittää, että on olemassa $x \in X$ jolle $f(x) < x$ (huom., tässä taas tarvitaan oletusta, että järjestys on täysi). Tämä on taas sama asia kuin osajoukon

$$S = \{x \in X \mid f(x) < x\}$$

epätyhjyys. Koska X on hyvinjärjestetty, epätyhjässä osajoukossa S on olemassa pienin alkio x. Sovelletaan yhtälöön

$$f(x) < x$$

kuvausta f. Koska f on injektiivinen morfismi, se säilyttää aitoja epäyhtälötitä eli ehdosta $a < b$ seuraa, että $f(a) < f(b)$. Nimittäin, f on morfismi, joten, koska erityisesti $a \leq b$, pätee $f(a) \leq f(b)$. Jos $f(a) = f(b)$, f:n injektiivisyyden nojalla pätee $a = b$, mikä on vastoin oletusta $a < b$. Näin ollen pätee jopa $f(a) < f(b)$. Kun tätä ominaisuutta sovelletaan epäyhtälöön $f(x) < x$, saadaan

$$f(f(x)) < f(x).$$

Jos merkitään $y = f(x)$, niin tälle alkiolle pätee
1) $y < x$ ja
2) $f(y) < y$ eli $y \in S$.
Kuitenkin x:n piti olla S:n pienin alkio ja nyt y on sitä pienempi S:n alkio. Saadaan ristiriita. Näin ollen S on tyhjä ja kaikilla $x \in X$ pätee $f(x) \geq x$. □

Olkoon $(X, \leq)$ osittaisjärjestetty joukko ja olkoon $S \subset X$ sellainen X:n osajoukko, joka on suljettu edeltäjien suhteen. Toisin sanoen jokaisella $x \in S$ ja $y < x$ pätee $y \in S$. Toinen tapa ilmaista tätä on sanoa, että jokaisella $x \in S$ alkusegmentti $I(x)$ on S:n osajoukko, $I(x) \subset S$. Tällöin sanomme S joukon X *ideaaliksi*.

Lemma 63. *Olkoon $(X, \leq)$ hyvinjärjestetty joukko ja olkoon S ideaali X:ssä. Tällöin joko $S = X$ tai on olemassa $z \in S$ siten, että $S = I(z)$ on alkusegmentti.*

Todistus. Oletetaan, että $S \neq X$. Tällöin epätyhjässä joukossa $X \setminus S$ on olemassa pienin alkio z. Osoitetaan, että $S = I(z)$.
Olkoon $x \in S$. Joka tapauksessa $x < z$, $x = z$ tai $z < x$. Tapaus $x = z$ on mahdoton, koska $x \in S$ ja $z \notin S$. Jos taas $z < x$, niin oletuksen nojalla $z \in S$ (se on x:n eräs edeltäjä), mikä taas johtaa ristiriitaan. Jäljellä on tapaus $x < z$ eli $x \in I(z)$. Olemme näyttäneet, että $S \subset I(z)$.
Kääntäen olkoon $x \in I(z)$. Tällöin $x \in S$, koska jos olisi $x \notin S$, joten $x \geq z$ (z oli $X \setminus S$:n pienin alkio). Tämä on mahdotonta, koska $x \in I(z)$ eli $x < z$. Näin ollen myös $I(z) \subset S$ pätee. Väite on todistettu. □

Seuraus 64. *Olkoon X hyvinjärjestetty joukko. Tällöin seuraavat ominaisuudet pätevät.*

(a) Olkoon $x \in X$ ja $A \subset I(x)$. Tällöin X ei ole hyvinjärjestettynä joukkona isomorfinen A:n kanssa.

(b) Olkoot $x, y \in X$, $x \neq y$. Tällöin alkusegmentit $I(x)$ ja $I(y)$ eivät ole isomorfisia.

Todistus. (a) Tehdään vasta-oletus, olkoon $f\colon X \to A$ isomorfismi. Tällöin se voidaan tulkita injektiivisena morfismina $f\colon X \to X$ (vaihdetaan maalijoukko, saadaan eri kuvaus, mutta sillä on samat arvot alkuperäisen f:n kanssa, injektiivisyys säilyy, surjektiivisuus ei).
Edellisen lemman nojalla $f(y) \geq y$ kaikilla $y \in X$. Erityisesti $f(x) \geq x$. Toisaalta, koska $f(x) \in A \subset I(x)$ kaikilla $a \in A$, erityisesti pätee $f(x) \in I(x)$ eli $f(x) < x$. Saadaan ristiriita. Näin ollen kuvausta f ei voi olla olemassa.
(b) Jos $x \neq y$, niin $x < y$ tai $y < x$. Symmetrian vuoksi voimme esimerkiksi olettaa, että $x < y$. Tällöin $I(x)$ on hyvinjärjestetyn joukon $Y = I(y)$ alkusegmentti (jonka alkio $x \in Y$ määrää). (a) kohdan nojalla $I(x)$ ja $I(y)$ eivät voi olla isomorfisia. □

Seuraava lause on kenties hyvinjärjestettyjen joukkojen teorian tärkein tulos. Se sanoo muun muassa, että kaksi hyvinjärjestettyä joukkoa joko ovat isomorfisia tai toinen on isomorfinen toisen alkusegmentin kanssa. Erityisesti kahdesta hyvinjärjestetyistä joukoista toinen voidaan ”upottaa” toiseen osajoukkona.

Lause 65. *Olkoot X ja Y hyvinjärjestettyjä joukkoja. Tällöin täsmälleen yksi seuraavista mahdollisuuksista toteutuu.*

(i) On olemassa yksikäsitteinen isomorfismi $f\colon X \cong Y$.

(ii) On olemassa yksikäsitteinen $x \in X$ ja yksikäsitteinen isomorfismi $f\colon I(x) \to Y$,

(iii) On olemassa yksikäsitteinen $y \in Y$ ja yksikäsitteinen isomorfismi $f\colon X \to I(y)$.

Todistus. **Isomorfismin yksikäsitteisyys**.
Aloitetaan osoittamalla, että kahden hyvinjärjestetyn joukon välillä voi olla korkeintaan yksi isomorfismi $f\colon X \to Y$. Olkoot $f, g\colon X \to Y$ isomorfismeja. Tällöin $h = g^{-1}\colon Y \to X$ on isomorfismi, joten myös $j = h \circ f\colon X \to X$ on isomorfismi. Lemman 62 nojalla pätee $j(x) \geq x$ kaikilla $x \in X$. Tästä seuraa, koska g on morfismi, että

$$f(x) = g(j(x)) \geq g(x)$$

kaikilla $x \in X$. Tilanne on täysin symmetrinen f:n ja g:n näkökulmasta, joten samalla tavalla saadaan, että $g(x) \leq f(x)$ kaikilla $x \in X$. Koska $\leq$ on muun muassa antisymmetrinen, $f(x) = g(x)$ kaikilla $x \in X$. Toisin sanoen

$f = g$.
Osoitetusta seuraa, että jokaisessa kohdassa (i)-(iii) jos väitetty isomorfismi on olemassa, se on yksikäsitteinen. Lisäksi kohdissa (ii) ja (iii) x ja y ovat yksikäsitteisiä Korollaarin 64 nojalla. Nimittäin jos on olemassa kaksi erilaista $x, x' \in X, x \neq x'$ siten, että $I(x) \cong Y \cong I(x')$, niin alkusegmentit $I(x)$ ja $I(x')$ ovat myös keskenään isomorfisia, mutta tämä on vastoin Korollaarin 64 tulosta. Samalla tavalla nähdään, että kohdassa (iii) y:n on oltava yksikäsitteinen.
Näytetään vielä, että vaihtoehdot (i)-(iii) ovat toistensa poissulkevia. Tämäkin seuraa Korollaarista 64. Nimittäin jos olisi samaan aikaan $X \cong Y$ ja esimerkiksi $X \cong I(y)$, $y \in Y$, niin Y olisi isomorfinen segmenttinsa $I(y)$ kanssa, mikä on vastoin Korollaarin 64 tulosta. Samalla tavalla nähdään muidenkin tapausten keskinäinen ristiriitaisuus.

Isomorfismin olemassaolo.
Nyt kun kaikki yksikäsitteisyys- ja poissulkevuusväitteet osoitettiin todeksi, riittää näyttää, että X on isomorfinen Y:n tai sen alkusegmentin kanssa, tai Y on isomorfinen X:n alkusegmentin kanssa.
Ajatus on siinä, että induktiolla voisi konstruoida "yksi alkio kerrallaan" injektiivinen morfismi $f\colon X \to Y$, joka kuvaisi aina alkusegmentin alkusegmenteiksi. Nimittäin pienin X:n alkio 0 voidaan kuvata Y:n pienimmäksi alkioksi 0. Sen jälkeen seuraava alkio $1 = 0^+$ kuvataan vastaavaan Y:n alkioon ja näin jatketaan. Jos tämä prosessi jatkuu X:n loppuun asti , saadaan isomorfismi X:stä Y:lle tai sen alkusegmentille. Jos taas tämä prosessi "loppuu kesken" (Y:stä loppuu alkiot, joihin voi kuvata X:n alkiota), saadaan isomorfismi X:n alkusegmentistä koko Y:lle.
Tarkan todistuksen suoritamme kuitenkin vähän eritavalla, viittaamatta varsinaiseen induktio-periaatteeseen.

Määritellään X:n osajoukko S kaavalla

$$S = \{x \in X \mid \text{ on olemassa } y \in Y \text{ siten, että } I(x) \cong I(y)\}.$$

Toisin sanoen $x \in S$ jos ja vain jos x:n määrämä alkusegmentti $I(x)$ on isomorfinen jonkun Y:n alkusegmentin kanssa. Pannaan heti merkille seuraavaa havainto.
Jos $x \in X$ niin sellainen $y \in Y$, jonka määrämä alkusegmentti $I(y)$ on isomorfinen $I(x)$:n kanssa, on yksikäsitteinen. Tämä seuraa jälleen kerran Korollaarista 64.
Voimme siis asettaa kuvauksen $f\colon S \to Y$ kaavalla $f(x) = y$ on juuri se yksikäsitteinen $y \in Y$ jolle $I(x) \cong I(y)$.

Väite 1: f on injektiivinen morfismi.
Väitteen 1 todistus: Riittää osoittaa, että jos $a < b$, niin $f(a) < f(b)$. Huomaa, että tämä implikoi samalla sekä morfisuuden, että injektiivisuuden. Olkoot siis $a, b \in S$, $a < b$. Olkoot $y, z \in Y$ sellaisia, että $f(a) = y$, $f(b) = z$ eli on olemassa isomorfismit $\alpha\colon I(a) \to I(y)$ ja $\beta\colon I(b) \to I(z)$. Koska $a < b$, alkusegmentti $I(a)$ on alkusegmentin $I(b)$ alkusegmentti (missä $I(b)$ mielletään hyvinjärjestettynä joukkona). Osoitetaan, että $y < z$ vasta-oletuksella. Oletetaan, että $z \leq y$. Tällöin $I(z)$ on $I(y)$:n osajoukko, joten β voidaan ajatella kuvauksena $\beta\colon I(b) \to I(y)$. Yhdistetty kuvaus $\gamma = \alpha^{-1} \circ \beta\colon I(b) \to I(a)$ on olemassa ja injektio (injektiivisten kuvausten yhdistettynä kuvauksena). Tästä seuraa, että γ:n kuvajoukko $\gamma(I(b))$ on $I(a)$:n osajoukko, joka on isomorfinen $I(b)$:n kanssa. Näin ollen $I(b)$ on isomorfinen alkusegmentinsa $I(a)$ osajoukon kanssa. Tämä on osoitettu mahdottomaksi Lemmassa 62. Näin ollen $f(a) < f(b)$ ja olemme näyttäneet väitteen 1 todeksi.
Väitteestä 1 seuraa, että olemme konstruoineet isomorfismin $S \to f(S)$. Seuraavaksi osoitamme, että molemmat joukot S ja $f(S)$ ovat ideaaleja.

Väite 2: S on ideaali.
Väitteen 2 todistus:
Olkoon $x \in S$ ja $x' < x$. Tällöin on olemassa isomorfismi $\alpha\colon I(x) \to I(y)$, missä $y \in Y$. Isomorfismi kuvaa aina alkusegmentit alkusegmenteiksi (miksi?), joten α:n rajoittuma alkusegmentiin $I(x')$ on isomorfismi $I(x') \to I(y')$ jollakin $y' \in Y$. Tämä tarkoittaa sitä, että $x' \in S$.

Väite 3: $f(S)$ on ideaali.
Väitteen 3 todistus:
Tämä on samanlainen kuin edellisen väitteen todistus.
Olkoon $y \in S$ ja $y' < y$. Tällöin on olemassa isomorfismi $\alpha\colon I(x) \to I(y)$, missä $x \in X$ sellainen, että $f(x) = y$. Isomorfismi kuvaa aina alkusegmentit alkusegmenteiksi, joten α^{-1}:n rajoittuma alkusegmentiin $I(y')$ on isomorfismi $I(y') \to I(x')$ jollakin $x' \in Y$. Tämä tarkoittaa sitä, että α kuva $I(x')$ alkusegmentille $I(y')$, joten $x' \in S$.

Väitteistä 2 ja 3 sekä Lemmasta 63 nyt seuraa, että voimassa on yksi seuraavista neljästä vaihtoehdoista,

(i) $S = X$ ja $f(S) = Y$,

(ii) $S = I(x)$ on alkusegmentti ja $f(S) = Y$,

(iii) $S = X$ ja $f(S) = I(y)$ on alkusegmentti,

(iv) $S = I(x)$ ja $f(S) = I(y)$ ovat molemmat alkusegmentteja.

Jos voimassa on yksi vaihtoehdoista (i)-(iii), olemme valmiit.
Osoitetaan, että vaihtoehto (iv) on kuitenkin mahdoton. Nimittäin tällöin meillä on isomorfismi $f\colon I(x) \to I(y)$. Mutta tämähän tarkoittaa joukon S määritelmän nojalla, että $x \in S = I(x)$, mikä on mahdotonta, sillä se implikoisi, että $x < x$.

□

Edellinen tulos on tärkeä paitsi hyvinjärjestettyjen joukkojen teorian kannalta, myös siitä syystä, että Hyvinjärjestyslauseen (Lause 61) mukaan kaikki joukot voidaan hyvinjärjestää, jolloin tulosta voidaan tietyissä tapauksessa soveltaa mielivaltaisten joukkojen tutkimiseen.
Esimerkkinä tästä osoitetaan edellisessä luvussa todistamatta jääneitä mahtavuuden ominaisuuksia.

Propositio 66. *Olkoot X ja Y joukkoja. Tällöin joko $|X| \leq |Y|$ tai $|Y| \leq |X|$. Toisin sanoen kaikkien joukkojen mahtavuuksia voidaan vertailla keskenään. Lisäksi pätee*
Cantor–Bernstein–Schroederin Lause: *Jos $|X| \leq |Y|$ ja $|Y| \leq |X|$, niin $|X| = |Y|$.*

Todistus. Hyvinjärjestyslauseen 61 avulla [11] voidaan palauttaa ongelma tapaukseen, jossa X ja Y ovat hyvinjärjestettyjä joukkoja $(X, \leq)$ ja $(Y, \leq')$. Tällöin edellisestä Lauseesta seuraa suoraan, että on olemassa injektio $f\colon X \to Y$ tai injektio $Y \to X$. Ensimmäinen väite on todistettu.
Esitetään Cantor–Bernstein–Schroederin Lauseelle todistuksen luonnos.
Ensin osoitetaan (HT), että jokainen joukko X voidaan hyvinjärjestää niin, että se toteuttaa seuraavan ehdon - jokaisella $x \in X$ alkusegmentti $I(x)$ on mahtavuudeltaan aidosti pienempi kuin X, $|I(x)| < |X|$. Tällaisia hyvinjärjestettyjä joukkoja kutsutaan *ordinaaleiksi*. Riittää siis osoittaa väite ordinaaleille X ja Y. Lauseesta 65 seuraa tällöin, että $|X| = |Y|$, jolloin ollaan valmiit, tai X on isomorfinen Y:n alkusegmentin $I(y)$ kanssa tai toisinpäin Y on isomorfinen $I(x)$:n alkusegmentin kanssa. Symmetrian vuoksi voimme olettaa, että $X \cong I(y)$, $y \in Y$. Toisaalta, jos $|Y| \leq |X|$, niin on olemassa injektio $Y \to X$. Yhdistämällä tämä injektio isomorfismin $X \to I(y)$ kanssa, saadaan injektio $Y \to I(y)$, josta seuraa, että Y on samaa mahtavuutta jonkun osajoukkonsa A kanssa, joka sisältyy johonkin Y:n alkusegmentiin $I(y)$. Tämä voidaan osoittaa olevan mahdotonta (HT). □

[11] voidaan osoittaa, että ilman hyvinjärjestyslausetta proposition ensimmäistä väitettä ei voida osoittaa todeksi. Cantor–Bernstein–Schroederin Lause taas voidaan osoittaa todeksi myös ilman hyvinjärjestyslausetta.

Nyt voidaan vihdoinkin konstruoida luonnollisia lukuja. Ensin pitää tietysti määritellä, mitä tarkoitamme luonnollisilla luvuilla.

Propositio 67. *Luonnollisten lukujen joukko on olemassa ja yksikäsitteinen isomorfiaa vaille. Täsmällisemmin sanottuna, jos hyvinjärjestetyt joukot* $(\mathbb{N}, \leq)$ *ja* $(\mathbb{N}', \leq')$ *toteuttavat molemmat luonnollisten lukujen joukon määritelmän, on olemassa yksikäsitteinen hyvinjärjestettyjen joukkojen välinen isomorfismi*

$$f\colon (\mathbb{N}, \leq) \to (\mathbb{N}', \leq').$$

Todistus. **Olemassaolo.**
Äärettömyysaksiooman mukaan on olemassa ääretön joukko X. Hyvinjärjestyslauseen mukaan se voidaan hyvinjärjestää, eli on olemassa ääretön hyvinjärjestetty joukko $(X, \leq)$. Jos jokainen sen alkusegmentti on äärellinen, se toteuttaa luonnollisten lukujen joukon määritelmän ja olemme valmiit.
Muuten osajoukko

$$S = \{x \in X \mid I(x) \text{ on ääretön}\}$$

on epätyhjä. Olkoon x sen pienin alkio. Tällöin $\mathbb{N} = I(x)$ on ääretön hyvinjärjestetty joukko, jonka jokainen alkusegmentti on äärellinen eli sellainen joukko joka toteuttaa luonnollisten lukujen määritelmän.
Yksikäsitteisyys.
Olkoot $(\mathbb{N}, \leq)$ ja $(\mathbb{N}', \leq')$ molemmat äärettömiä hyvinjärjestettyjä joukkoja, joiden jokainen alkusegmentti on äärellinen. Tällöin $\mathbb{N}$ ei voi olla isomorfinen $\mathbb{N}'$:n alkusegmentin kanssa, sillä äärettömällä ja äärellisellä joukoilla ei voi olla sama mahtavuus. Samasta syystä $\mathbb{N}'$ ei voi olla isomorfinen $\mathbb{N}$:n alkusegmentin kanssa. Lauseen 65 nojalla jäljellä on vain yksi mahdollisuus - hyvinjärjestettyjen joukkojen $\mathbb{N}$ ja $\mathbb{N}'$ välillä on isomorfismi, jopa yksikäsitteinen. □

Seuraavassa aliluvussa tutkimme luonnollisten lukujen ominaisuuksia tarkemmin, muun muassa konstruoimme yhteen-ja kertolasku joukossa $\mathbb{N}$. Tässä luvussa käydään vielä läpi tuloksia, jotka liittävät luonnollisten lukujen mahtavuuden muiden joukkojen mahtavuuksiin.
Joukkoa, joka on yhtämahtava kuin luonnollisten lukujen joukko sanotaan *numeroituvaksi*. Kuten kohta näytämme, numeroituvuus on "pienin" ääretön mahtavuus - jokainen ääretön joukko joka ei ole numeroituva on mahtavuudelta aidosti isompi kuin $\mathbb{N}$. Tästä syystä sanomme äärettömiä joukkoja, jotka eivät ole numeroituvia, *ylinumeroituviksi*. Esimerkiksi Propositiosta 43 seuraa, että luonnollisten lukujen joukon potenssijoukko $\mathcal{P}(\mathbb{N})$ on ylinumeroituva. Voidaan osoittaa, että se on itse asiassa yhtämahtava kuin reaalilukujen joukko $\mathbb{R}$. Erityisesti $\mathbb{R}$ on ylinumeroituva.

Lemma 68. *Olkoon $(X, \leq)$ äärellinen epätyhjä hyvinjärjestetty joukko. Tällöin X:ssä on olemassa suurin alkio.*

Todistus. Harjoitustehtävä. □

Palautetaan mieleen, että epätyhjän hyvinjärjestetyn joukon pienintä alkiota (joka on aina olemassa) merkitään 0. Erityisesti luonnollisten lukujen joukossa on olemassa luku 0, pienin luonnollinen luku.
Palautetaan myös mieleen, että hyvinjärjestetyn joukon $(X, \leq)$ jokaisella alkiolla x, joka ei ole suurin alkio, on olemassa niin sanottu välitön seuraaja x^+. Määritelmän mukaan se on pienin alkio osajoukossa $\{y \in X \mid x < y\}$.
Luonnollisten lukujen joukossa määrittelemme $1 = 0^+$, $2 = 1^+$ jne.
Luonnollisten lukujen joukossa $\mathbb{N}$ **ei ole** suurinta alkiota. Tämän väitteen tarkka todistus jätetään harjoitustehtäväksi. Erityisesti jokaisella $n \in \mathbb{N}$ välitön seuraaja n^+ on olemassa.

Seuraus 69. *Jokainen nollasta eroava luonnollinen luku on yksikäsitteisen luonnollisen luvun välitön seuraaja.*
Tarkemmin olkoon $\mathbb{N}$ luonnollisten lukujen joukko ja olkoon $n \in \mathbb{N}$. Tällöin joko $n = 0$ tai on olemassa yksikäsitteinen $m \in \mathbb{N}$ siten, että $m^+ = n$.

Todistus. Tarkastellaan alkusegmenttiä $I(n)$. Jos $n \neq 0$, $I(n)$ sisältää nollan, joten erityisesti on epätyhjä. Lisäksi $\mathbb{N}$:n määritelmän mukaan $I(n)$ on äärellinen. Se on siis äärellinen hyvinjärjestetty joukko. Edellisen lemman nojalla $I(n)$:ssä on suurin alkio m. Tällöin $m^+ = n$ (tarkka perustelu harjoitustehtävänä). □

Edellisen lemman avulla voimme määritellä välittömän edeltäjän käsitettä. Olkoon $n \in \mathbb{N}$, $n \neq 0$. Tällöin yksikäsitteistä luonnollista lukua m jolle $m^+ = n$ sanotaan n:n *välittömäksi edeltäjäksi* ja merkitään n^-. Samalla tavalla voimme määritellä välittömän edeltäjän käsitteen missä tahansa hyvinjärjestetyssä joukossa, mutta tällöin välitön edeltäjä ei välttämättä ole olemassa jopa nollasta eroavalla alkiolla.

Esimerkki 70. *Olkoon $\mathbb{N}$ luonnollisten lukujen joukko ja $\infty \notin \mathbb{N}$ jokin alkio. Määritellään joukossa $\mathbb{N}^* = \mathbb{N} \cup \{\infty\}$ järjestys $\leq$ asettamalla, että $x \leq y$ jos ja vain jos $x, y \in \mathbb{N}$ ja $x \leq y$ luonnollisten lukujen joukossa tai jos $y = \infty$. Voidaan osoittaa (harjoitustehtävä), että $(\mathbb{N}^*, \leq)$ on tällöin hyvinjärjestetty joukko. Alkio ∞ on tällöin $\mathbb{N}^*$:n suurin alkio, joten sillä ei luonnollisestikaan ole välitöntä seuraajaa. Sillä ei myöskään ole välitöntä edeltäjää, sillä $\mathbb{N}$:ssä ei ole suurinta alkiota.*

Luonnollisten lukujen tapauksessa alkion $n \in \mathbb{N}$ välitöntä seuraajaa n^+ merkitään symbolilla $n+1$ ja välitöntä edeltäjää (jos $n \neq 0$) n^- merkitään symbolilla $n-1$. Tässä vaiheessa nämä ovat vain sovittuja merkintöjä. Tietysti kun myöhemmin määrittelemme luonnollisille luvuille tuttuja laskutoimituksia yhteen- ja vähennyslasku, nähdään, että nämä ovat sopusoinnissa niiden kanssa.

Propositio 71. *Olkoon X mielivaltainen joukko. Tällöin seuraavat ominaisuudet pätevät.*

(i) X on äärellinen jos ja vain jos on olemassa luonnollinen luku $n \in \mathbb{N}$ siten, että X on yhtämahtava luonnollisten lukujen joukon osajoukon

$$\{m \in \mathbb{N} \mid m < n\} = \{0, 1, \ldots, n-1\}$$

kanssa. Lisäksi tällainen n on tällöin yksikäsitteinen.

(ii) X on ääretön jos ja vain jos se sisältää numeroituvan osajoukon.

(iii) Jos X on ääretön ja ei ole numeroituva, niin $|\mathbb{N}| < |X|$. Luonnollisten lukujen mahtavuus on siis pienin mahdollinen äärettömän joukon mahtavuus.

Todistus. Harjoitustehtävä. □

Olkoon X äärellinen joukko ja olkoon n yksikäsitteinen luonnollinen luku, joka toteuttaa edellisen Proposition kohdan (i). Tällöin sanomme, että X:n *koko* on n ja merkitään sitä $|X| = n$. Kaksi äärellistä joukkoa ovat yhtämahtavat jos ja vain jos ne ovat *samankokoisia*, eli niillä on sama koko. Koon käsite mahdollista väitteiden todistamista todeksi äärellisessä joukossa induktiolla sen *koon* mukaan. Lisää matemaattisesta induktiosta luonnollisten lukujen joukossa seuraavassa aliluvussa.

4.2 Luonnollisten lukujen ominaisuuksia

Edellisessä aliluvussa olemme määrittäneet luonnollisten lukujen joukko parina $(\mathbb{N}, +)$, missä $\mathbb{N}$ on ääretön joukko ja $\leq$ on hyvinjärjestysrelaatio joukossa $\mathbb{N}$, jonka kaikki alkusegmentit ovat äärellisiä. Todistamme, että tällöin pari voidaan joukko-opissa konstruoida ja lisäksi kaikki tällaiset parit ovat isomorfisia, joten $\mathbb{N}$ on olennaisesti yksikäsitteinen.
Tiedämme, että luonnollisten lukujen joukossa on oltava muutakin struktuuria kuin järjestysrelaatio. Luonnollisia lukuja pitäisi myös pystyä laskemaan yhteen ja kertoa keskenään. Tässä aliluvussa määrittelemme $\mathbb{N}$:ssä molempia

laskutoimituksia $+, \cdot$ ja käymme läpi niiden ominaisuuksia.

Induktioperiaate luonnollisille luvuille.
Yleinen induktioperiaate hyvinjärjestetyille joukoille (Propositio 60) voidaan luonnollisten lukujen joukossa muotoilla myös erilaisella tavalla (joka ei muissa hyvinjärjestetyissä joukoissa toimi).
Olkoon $P(n)$ luonnollista lukua n koskeva väite ja oletetaan, että $P(n)$ on määritelty jokaisella $n \in \mathbb{N}$. Haluamme osoittaa, että $P(n)$ on tosi jokaisella $n \in \mathbb{N}$. Tällöin riittää osoittaa, että
1) väite $P(0)$ on tosi,
2) jokaisella luonnollisella luvulla $n \in \mathbb{N}$ jos $P(n)$ on tosi, niin myös $P(n+1)$ on tosi.
Tässä $n + 1 = n^+$ on luonnollisen luvun n välitön seuraaja.
Induktioperiaate seuraa seuraavasta propositiosta samalla tavalla kuin yleinen induktioperiaate hyvinjärjestetyille joukoille seuraa Propositiosta 60.

Propositio 72. *Olkoon $S \subset \mathbb{N}$ osajoukko, joka toteuttaa seuraavia ehtoja.*
1) $0 \in S$.
2) Olkoon $n \in \mathbb{N}$. Tällöin jos $n \in S$, niin myös $n + 1 \in S$.
Tällöin $S = \mathbb{N}$.

Todistus. Riittää osoittaa, että S toteuttaa Proposition 60 oletuksia.
Olkoon $n \in \mathbb{N}$ mielivaltainen ja oletetaan tunnetuksi, että kaikilla $m < n$ pätee $m \in S$. Meidän pitää osoittaa, että $n \in S$.
Jos $n = 0$, tämä seuraa suoraan tämän proposition oletuksesta 1). Muuten Korollaarin 69 mukaan $n = m^+ = m + 1$ jollakin $m \in \mathbb{N}$. Koska $n = m + 1$, erityisesti pätee $m < n$. Oletuksestamme seuraa, että $m \in S$. Proposition oletuksesta taas seuraa tällöin, että $m + 1 = n \in S$. Todistus on valmis. □

Induktiolla voidaan myös määritellä esimerkiksi funktioita (ja tehdä muita konstruktioita) *rekursiivisesti*. Jos halutaan konstruoida kuvaus $f\colon \mathbb{N} \to X$, missä X on mielivaltainen joukko, riittää kertoa mikä on $f(0)$ ja miten $f(n + 1)$ määritellään, jos $f(n)$ tunnetaan jo. Voidaan osoittaa, että tällä periaatteella aina saadaan yksikäsitteinen kuvaus $f\colon \mathbb{N} \to X$ konstruoitua.

Esimerkki 73. *Olkoon $\mathbb{R}$ reaalilukujen joukko (eli mikä tahansa joukko, joka toteuttaa määritelmän 1).*

Määritellään induktiolla kuvaus $f\colon \mathbb{N} \to \mathbb{R}$ seuraavasti. Asetetaan
1) $f(0) = 0_R$, missä 0 vasemmalla puolella on luonnollinen luku $\mathbb{N}$ (pienin luonnollinen luku) ja $0_{\mathbb{R}} = 0$ oikealla puolella on reaaliluku 0 (reaalilukujen

aksioomasta A(iii)). 2) Oletetaan, että $f(n) \in \mathbb{R}$ on määritelty. Asetetaan $f(n^+) = f(n+1) = f(n) + 1$, missä 1 on reaaliluku 1 (aksioomasta B(iii)).
Osoitetaan, että $f\colon \mathbb{N} \to \mathbb{R}$ on injektiivinen järjestettyjen joukkojen morfismi. Tässä $\mathbb{R}$ varustetaan sen luonnollisella järjestyksellä $\leq$ (jonka olemassaolo asetetaan määritelmässä).
Riittää osoittaa, että jos $n < m$, niin $f(n) < f(m)$.
Osoitetaan tämä väite induktiolla m:n suhteen.
1) Jos $m = 0$ ei ole olemassa lukuja $n \in \mathbb{N}$ joille $n < m$, joten ei ole mitään todistettavaa.
2) Oletetaan, että väite pätee jollakin $m \in \mathbb{N}$. Kiinnitetään tämä m ja osoitetaan väite $m+1$:lle.
Olkoon siis $n \in \mathbb{N}$, $n < m + 1 = m^+$. Tällöin joko $n < m$ tai $n = m$ (koska kolmas vaihtoehto $n > m$ johtaa siihen, että $n \geq m^+ = m + 1$, välittömän seuraajan määritelmän nojalla). Jos $n < m$, induktio-oletuksen nojalla saadaan $f(n) < f(m) < f(m) + 1 = f(m+1)$.
Jos taas $n = m$, saadaan taas $f(n) = f(m) < f(m) + 1 = f(m+1)$. Väite on todistettu induktiolla.
Näin ollen $f\colon \mathbb{N} \to \mathbb{R}$ määrittelee isomorfismin $\mathbb{N} \cong f(\mathbb{N})$. Reaalilukujen joukon $\mathbb{R}$ osajoukkoa $f(\mathbb{N})$ sanomme joukon $\mathbb{R}$ luonnollisten lukujen osajoukoksi.
Jokainen reaalilukujen joukko siis sisältää "oman versionsa" luonnollisten lukujen joukosta.

Yhteenlasku $\mathbb{N}$:ssä.
Ennen kuin mennään varsinaiseen määritelmään, kielletään hetkellisesti mahdollisten sekaannusten vuoksi välittömän seuraajan n^+ merkitsemistä symbolilla $n+1$. Tämä johtuu siitä, että kun yhteenlasku määritellään, tällainen merkintä voi mennä sekaisin lukujen n ja 1 summan kanssa, sehän merkitään samalla tavalla symbolilla $n + 1$. Myöhemmin paljastuu että molemmat tulkinnat antavat saman luvun, mutta pidetään merkintöjä toistaiseksi erillään.

Yhteenlasku-operaatio luonnollisten lukujen joukossa määritellään induktiolla. Tarkemmin jokaisella $k \in \mathbb{N}$ määritellään (induktiolla luvun k suhteen) kuvauksen $f_k\colon \mathbb{N} \to \mathbb{N}$. Sen jälkeen asetetaan

$$k + n = f_k(n)$$

kaikilla $k, n \in \mathbb{N}$ ja näin saadaan yhteenlasku määriteltyä.
Kuvaukset f_k määritellään induktiolla seuraavasti. Olkoon $k \in \mathbb{N}$. Asetetaan $f_k(0) = k$. Jos oletetaan, että $f_k(n)$ on määritelty jollakin $n \in \mathbb{N}$, määritellään

$$f_k(n^+) = f_k(n)^+.$$

Induktio-periaatteen nojalla tämä määrittelee jokaisella $k \in \mathbb{N}$ yksikäsitteisen kuvauksen $f_k \colon \mathbb{N} \to \mathbb{N}$. Laskutoimitus $+ \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ määritellään sen jälkeen kaavalla

$$k + n = f_k(n)$$

kaikilla $k, n \in \mathbb{N}$.
Symbolilla $n + 1$ on nyt kaksi merkitystä, joten sekaannuksen välttämiseksi verifioidaan heti, että ne antavat saman lopputuloksen.
Toisaalta määrittelimme aikaisemmin, että $n + 1 = n^+$ tarkoittaa luvun n välitöntä seuraajaa järjestyksen mielessä. Toisaalta $n+1$ on nyt myös lukujen n ja 1 summa. Osoitetaan siis, että jos $n + 1$ tulkitaan summana, pätee $n + 1 = n^+$. Määritelmän mukaan $1 = 0^+$, joten

$$n + 1 = f_n(1) = f_n(0^+) = f_n(0)^+ = n^+.$$

Väite on todistettu. Nyt voimme myös kirjoittaa kuvauksen f_k rekursiivinen määritelmä muodossa

$$f_k(0) = k,$$
$$f_k(n + 1) = f_k(n) + 1.$$

Propositio 74. *Luonnollisten lukujen yhteenlasku on liitännäinen ja vaihdannainen ja* 0 *on sen neutraalialkio. Tarkemmin jokaisella $k, m, n \in \mathbb{N}$ pätevät seuraavat ominaisuudet.*

(i) $(k + m) + n = k + (m + n)$ *eli yhteenlasku on liitännäinen*

(ii) $m + n = n + m$ *eli yhteenlasku on vaihdannainen*

(iii) $n + 0 = 0 + n = n$ *kaikilla* $n \in \mathbb{N}$.

(iv) Pätee seuraava supistussääntö*:*
jos $m + k = n + k$, niin $m = n$.

Todistus. Liitännäisyyden

$$(k + m) + n = k + (m + n)$$

osoitamme induktiolla n:n suhteen.
Jos $n = 0$ saadaan

$$(k+m)+n = (k+m)+0 = f_{k+m}(0) = k+m = k+(f_m(0)) = k+(m+0) = k+(m+n).$$

Osoitetaan liitännäisyys vielä erikseen arvolla $n = 1$ (sillä tarvitsemme sen myöhemmin induktiovaiheessa). Pitää siis osoittaa, että kaikilla $k, m \in \mathbb{N}$ pätee

$$(k + m) + 1 = k + (m + 1).$$

Määritelmän mukaan $k + (m + 1) = f_k(m + 1) = f_k(m) + 1 = (k + m) + 1$. Väite on todistettu.
Oletetaan, että kaava $(k+m)+n = k+(m+n)$ pätee jollakin n ja osoitetaan se $(n + 1)$:lle. Määritelmän ja induktio-oletuksen nojalla

$$(k+m)+(n+1) = f_{k+m}(n+1) = f_{k+m}(n)+1 = ((k+m)+n)+1 = (k+(m+n))+1.$$

Juuri edellä osoitetun liitännäisyyden erikoistapauksen (jossa $n = 1$) nojalla voimme kirjoittaa

$$(k + (m + n)) + 1 = k + ((m + n) + 1)) = k + (m + (n + 1)).$$

Olemme osoittaneet, että

$$(k + m) + (n + 1) = k + (m + (n + 1)),$$

eli väite pätee myös $n + 1$:lle.
Vaihdannaisuuden todistus (induktiolla) jätetään harjoitustehtäväksi.
Jokaisella $n \in \mathbb{N}$ yhtälö

$$n + 0 = f_n(0) = n$$

pätee funktion f_n määritelmän nojalla. Yhtälö $0 + n = n$ seuraa puolestaan tästä ja vaihdannaisuudesta.
Supistussääntö, joka sanoo, että $n + k = m + k$ implikoi $n = m$, osoitetaan induktiolla k:n suhteen. Kun $k = 0$ saadaan suoraan

$$n = n + 0 = m + 0 = m.$$

Osoitetaan vielä tapaus $k = 1$ ennen kuin mennään yleiseen induktio-vaiheeseen. $n + 1 = m + 1$ tarkoittaa, että $n^+ = m^+$ eli n:llä ja m:llä on sama välitön seuraaja. Tästä helposti seuraa, että $n = m$ (tarkka perustelu harjoitustehtävänä).
Tehdään induktio-oletus - supistussääntö on tosi jollakin $k \in \mathbb{N}$. Oletetaan, että $n + (k + 1) = m + (k + 1)$. Liitännäisyyden nojalla tämä on sama asia kuin $(n + k) + 1 = (m + k) + 1$. Koska supistussääntö osoitettiin jo arvolla $k = 1$, tästä seuraa, että $n+k = m+k$. Induktio-oletuksen nojalla tästä taas seuraa, että $n = m$.

□

Luonnollisten lukujen kertolasku.
Kertolasku $n \cdot m$ määrittelemme induktiolla m:n suhteen. Asetetaan
1) $n \cdot 0 = 0$ ja
2) $n \cdot (m+1) = n \cdot m + n$, missä induktio-oletuksena oletamme, että $n \cdot m$ on jo määritelty. Huomaa, että käytämme tässä edellä määriteltyä yhteenlaskua

myös. Määritelmän motivaationa on tietysti osittelulaki $a(b+c) = ab+ac$ ja ajatus siitä $n \cdot 1 = n$ pitäisi olla voimassa kaikilla $n \in \mathbb{N}$.
Piste $\cdot$ yleensä jätetään merkitsemättä ja asetetaan yksinkertaisesti $nm = n \cdot m$.

Propositio 75. *Luonnollisten lukujen kertolasku toteuttaa seuraavia ominaisuuksia.*

(i) $(km)n = k(mn)$ *eli kertolaskulasku on liitännäinen*

(ii) $mn = nm$ *eli kertolasku on vaihdannainen*

(iii) $n \cdot 1 = 1 \cdot n = n$ *kaikilla* $n \in \mathbb{N}$.

(iv) Pätee seuraava supistussääntö*:*
jos $mk = nk$ *ja* $k \neq 0$*, niin* $m = n$.

(v) $k(m+n) = km+kn$ *eli osittelulaki on voimassa yhteen-ja kertolaskulle.*

Todistus. Harjoitustehtävä (suuri määrä induktiotodistuksia). □

Luonnollisten lukujen laskutoimitukset $+$, $\cdot$ ”sopivat hyvin” järjestysrelaation kanssa seuraavassa mielessä.

Propositio 76. *Olkoot* $n, m, k \in \mathbb{N}$ *ja oletetaan, että* $n \leq m$.
Tällöin

$$n + k \leq m + k,$$

$$nk \leq mk.$$

Lisäksi yhtälöllä $x + m = n$ *(jossa* x *on tuntematon) on olemassa ratkaisu jos ja vain jos* $m \leq n$*. Tällöin ratkaisu on myös yksikäsitteinen ja se voidaan merkitä* $x = n - m$.

Todistus. Induktiolla luvun k suhteen. Kun $k = 0$ $n + k = n \leq m \leq m + k$ oletuksen nojalla ja $n \cdot 0 = 0 = m \cdot 0$, joten erityisesti $n \cdot 0 \leq m \cdot 0$.
Oletetaan, että väite on tosi luvulla k. Tällöin $n+k \leq m+k$, joten $n+(k+1) = (n + k)^+ \leq (m + k)^+ = m + (k + 1)$. Ensimmäinen väite on todistettu induktiolla.
Oletetaan taas, että $nk \leq mk$. Tällöin transitiivisuuden ja edellä todistetun nojalla

$$n(k + 1) = nk + n \leq nk + m \leq mk + m = m(k + 1).$$

Väite todistettu induktiolla.

Olkoot $n, m \in \mathbb{N}$. Osoitetaan, että on olemassa $k \in \mathbb{N}$ siten, että $m+k = n$ jos ja vain jos $m \leq n$. Oletetaan, että $m + k = n$ jollakin $k \in \mathbb{N}$. Tällöin $0 \leq k$, joten edellä todistetun nojalla

$$m = m + 0 \leq m + k = n.$$

Näin ollen oletus $m \leq n$ on välttämätön. Osoitetaan, että se on myös riittävä. Osoitetaan induktiolla luvun n suhteen, että kaikilla $m \leq n$ on olemassa yksikäsitteinen $k \in \mathbb{N}$ siten, että $n + k = m$. Yksikäsitteisyys seuraa suoraan supistussäännöstä (Lemma 74), sillä jos $n + k = m = n + k'$, niin $k = k'$. Riittää siis osoittaa olemassaolo.
Olkoon $n = 0$. Tällöin ainoa $m \in \mathbb{N}$ jolle pätee $m \leq n$ on $m = 0$. Selvästi on olemassa $k = 0$ jolle $0 + k = 0$. Alkuaskel on osoitettu todeksi.
Oletetaan, että $n \in \mathbb{N}$ on sellainen, että kaikilla luonnollisilla luvuilla $m \leq n$ on olemassa $k \in \mathbb{N}$ jolle $m + k = n$. Osoitetaan, että sama pätee luvulle $n + 1$. Olkoon $m \in \mathbb{N}$ sellainen, että $m \leq n + 1 = n^+$. Koska n^+ on luvun n välitön seuraaja, tästä seuraa, että joko $m \leq n$ tai $m = n+1$. Jälkimmäisessä tapauksessa nähdään heti, että $m + k = n + 1$ arvolla $k = 0$.
Jos taas $m \leq n$ induktio-oletuksen nojalla on olemassa $k \in \mathbb{N}$ jolle $m+k = n$. Yhteenlaskun ominaisuuksista seuraa, että

$$m + (k + 1) = (m + k) + 1 = n + 1.$$

Näin ollen $k + 1$ toteuttaa vaaditun omainaisuuden.
Väite on osoitettu induktiolla. □

Erityisesti edellisestä Propositiosta seuraa, että luonnollisten lukujen joukossa ei kaikilla lineaarisilla yhtälöillä $x + m = n$ on ratkaisuja. Esimerkiksi niitä ei löydy yhtälölle $x + 3 = 2$. Seuraavassa luvussa käytämme tätä tosiasiaa kokonaislukujen konstruktion motivaationa.

Tästä lähtien ajattelemme, että luonnollisten lukujen joukko on systeemi $(\mathbb{N}, +, \cdot, \leq)$, missä + ja $\cdot$ ovat edellä määriteltyjä operaatioita.

Kombinatoriikka[12]
Palautetaan mieleen, että jokaiseen äärelliseen joukkoon liitetään yksikäsitteinen luonnollinen luku $n = |A|$, joka karakterisoitu yksikäsitteisesti ehdolla $|A| = |I(n)|$ mahtavuus-mielessä. Tämä luku on A:n **koko**.
Nyt kun käytössämme ovat myös luonnollisten lukujen algebralliset operaatiot, voidaan johtaa tunnettuja kombinatorisia tuloksia. Esimerkiksi induk-

[12]Tätä osuutta ei käsitellä luennoilla

tiolla B:n koon $|B|$ suhteen voidaan osoittaa, että jos A, B ovat erillisiä äärellisiä joukkoja ($A \cap B = \emptyset$), myös yhdiste $A \cup B$ on äärellinen ja

$$|A \cup B| = |A| + |B|.$$

Tästä puolestaan voidaan johtaa yleisempi kaava

$$|A \cup B| = |A| + |B| - |A \cap B|,$$

joka on tosi kaikille äärellisille joukoille A, B (ei välttämättä erilliselle).
Myös kertolaskulle on olemassa luonnollinen tulkinta äärellisten joukkojen koko-käsitteen termeissä. Nimittäin jos A ja B ovat mielivaltaisia äärellisiä joukkoja, niin myös karteesinen tulo $A \times B$ on äärellinen ja

$$|A \times B| = |A| \cdot |B|.$$

Näistä tuloksista seuraa, että voimme ottaa niitä laskutoimitusten konstruktion lähtökohdaksi. Sen sijaan, että lukujen $n, m \in \mathbb{N}$ summan $n+m$ ja tulon nm määriteltäisi formaalisti induktiolla (kuten me tehtiin aikaisemmin) voi valita ensin erillisiä äärellisiä joukkoja A, B, joille $|A| = n, |B| = m$ ja asettaa

$$n + m = |A \cup B|,$$

$$nm = |A \times B|.$$

Voidaan näyttää, että tämä määritelmä on mielekäs ja antaa samoja laskutoimituksia kuten edellä. Monet laskutoimitusten algebralliset ominaisuudet tällöin voidaan helposti johtaa suoraan vastaavien joukkojen ominaisuuksien avulla. Esimerkiksi yhteenlaskun liitännäisyys seuraa tällöin yhdiste operaation $\cup$ liitännäisyydestä,

$$(n + m) + k = |(A \cup B) \cup C| = |A \cup (B \cup C)| = n + (m + k).$$

Tiivistelmä.
Luonnollisten lukujen joukko $(\mathbb{N}, \leq)$ määritellään äärettömänä hyvinjärjestettynä joukkona, jonka jokainen alkusegmentti on äärellinen. Joukko-opin aksioomista ja tuloksista seuraa, että tällainen joukko on olemassa ja on yksikäsitteinen isomorfiaa vaille.
Joukossa $\mathbb{N}$ määritellään myös yhteenlasku $+$ ja kertolasku $\cdot$. Ne määräytyvät yksikäsitteisesti ehdoilla

$$n + 0 = n \text{ kaikilla } n \in \mathbb{N}$$

$$n + m^+ = (n + m)^+ \text{ kaikilla } n, m \in \mathbb{N},$$

$$n \cdot 0 = 0 \text{ kaikilla } n \in \mathbb{N},$$

$$n \cdot m^+ = (n \cdot m) + n \text{ kaikilla } n, m \in \mathbb{N},$$

missä m^+ on luvun m välitön seuraaja järjestysrelaation $\leq$ suhteen. Struktuurissa $(\mathbb{N}, +, \cdot \leq)$ pätevät seuraavat ominaisuudet.

A(i) Kaikilla $x, y \in \mathbb{N}$ pätee $x + y = y + x$.

A(ii) Kaikilla $x, y, z \in \mathbb{N}$ pätee $(x + y) + z = x + (y + z)$.

A(iii) On olemassa yksikäsitteinen alkio $0 \in \mathbb{N}$ siten, että $x + 0 = x$ kaikilla $x \in \mathbb{N}$.

A(iv) Yhtälöstä $x + y = z + y$ seuraa $x = z$ kaikilla $x, y, z \in \mathbb{N}$

B(i) Kaikilla $x, y \in \mathbb{N}$ pätee $x \cdot y = y \cdot x$.

B(ii) Kaikilla $x, y, z \in \mathbb{N}$ pätee $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

B(iii) On olemassa yksikäsitteinen alkio $1 \in \mathbb{N}$, $1 \neq 0$ siten, että $x \cdot 1 = x$ kaikilla $x \in \mathbb{N}$.

B(iv) Yhtälöstä $xy = zy$ seuraa $x = z$ tai $y = 0$ kaikilla $x, y, z \in \mathbb{N}$

C Kaikilla $x, y, z \in \mathbb{N}$ pätee $(x + y) \cdot z = x \cdot z + y \cdot z$.

D(i) Kaikilla $x \in \mathbb{N}$ pätee $x \leq x$.

D(ii) Jos alkioille $x, y \in \mathbb{N}$ pätee $x \leq y$ ja $y \leq x$, niin $x = y$.

D(iii) Olkoot $x, y, z \in \mathbb{N}$. Tällöin jos $x \leq y$ ja $y \leq z$, niin myös $x \leq z$.

D(iv) Kaikilla $x, y \in \mathbb{N}$ joko $x \leq y$ tai $y \leq x$.

E(i) Olkoot $x, y, z \in \mathbb{N}$. Tällöin jos $x \leq y$, niin $x + z \leq y + z$.

E(ii) Olkoot $x, y, z \in \mathbb{N}$. Tällöin jos $x \leq y$, niin $x \cdot z \leq y \cdot z$.

F Relaatio $\leq$ on hyvinjärjestys.

Vertaa näitä ominaisuuksia reaalilukujen aksiomeihin (Määritelmä 1). Huomaa erityisesti, että reaalilukujen aksioomat A(iv) ja B(iv) (vasta-alkioiden ja käänteisalkioiden olemassaolo) eivät ole voimassa $\mathbb{N}$:ssä. Niiden tilalla joukosta $\mathbb{N}$ löytyvät ”supistussäännöt”, joita voidaan ajatella olevan yllämainittujen reaalilukujen aksioomien alkeellisiksi versioksi. Juuri ne mahdollistavat

sen, että voimme ”laajentaa” joukko $\mathbb{N}$ joukoiksi $\mathbb{Z}$ (kokonaisluvut), jossa pätee aksiooma reaalilukujen aksiooma A(iv) ja sitten rationaalilukujen joukoksi $\mathbb{Q}$, jossa pätee aksiooma B(iv). Näitä laajennuksia suoritetaan seuraavassa luvussa.
Reaalilukujen täydellisyysaksiooma sellaisenaan formaalisti pätee $\mathbb{N}$:ssä - jokaisessa $\mathbb{N}$:n epätyhjässä ylhäältä rajoitetulla osajoukolla on N:ssä pienin yläraja. Tämä seuraa siitä, että $\mathbb{N}$ on hyvinjärjestetty (mieti miten). Sama aksiooma on voimassa myös laajennuksessa $\mathbb{Z}$, mutta seuraavassa vaiheessa, eli laajennuksessa $\mathbb{Q}$ se menetetään. Tästä syystä $\mathbb{Q}$ ei vielä kelpaa reaalilukujen malliksi, vaan se pitää ”täydentää”.

Huomautus Peanon aksioomista.
Tämän kurssin tapa tarkastella luonnollisten lukujen joukkoa hyvinjärjestettyjen joukkojen teorian kautta on hieman ”epäortodoksinen”. Kirjallisuudessa useimmiten törmää toiseen tapaan määritellä luonnollisia lukuja, joka perustuu niin sanottuihin **Peanon aksiomeihin**.
Tämän lähestymistavan mukaan luonnollisten lukujen joukko määritellään systeeminä $(\mathbb{N}, S)$, missä $\mathbb{N}$ on joukko ja $S\colon \mathbb{N} \to \mathbb{N}$ on kuvaus. Lisäksi oletetaan, että seuraavat *Peanon aksioomat* ovat voimassa:

(i) On olemassa luku $0 \in \mathbb{N}$ siten, että $0 \notin S(\mathbb{N})$.

(ii) S on injektio.

(iii) Induktio-periaate: Olkoon $K \subset \mathbb{N}$ sellainen osajoukko, joka toteuttaa seuraavia ominaisuuksia.
- $0 \in K$,
- jos $n \in K$, niin myös $S(n) \in K$.
Tällöin $K = \mathbb{N}$.

Meidän konstruoima hyvinjärjestetty joukko $(\mathbb{N}, \leq)$ toteuttaa Peanon aksioomia seuraajakuvauksella $S(n) = n^+$. Kääntäen voidaan osoittaa, että joukossa, joka toteuttaa Peanon aksioomia voidaan määritellä hyvinjärjestys $\leq$, joka toteuttaa luonnollisten lukujen joukon määritelmää. Näin ollen tämä lähestymistapa on täysin ekvivalentti tällä kurssilla käytetyn lähestymistavan kanssa.