Luonnollisten lukujen ja kokonaislukujen määritteleminen

LuK-tutkielma
Jussi Piippo
Matemaattisten tieteiden yksikkö
Oulun yliopisto
Kevät 2017

Sisältö

1 Johdanto

Työni käsittelee aihetta, joka otetaan itsestäänselvyytenä miltei jokaisella koulutusasteella, eli lukujoukkojen konstruoimista. Erityisesti huomioni kiinnittyi luonnollisiin lukuihin, kokonaislukuihin sekä rationaalilukuihin, sillä nämä kolme joukkoa kytkeytyvät hyvin toisiinsa algebrallisesti. Perusrakenteena selitän ensin joukko-opin perusaksioomat sekä tiedot, jota tekstini ymmärtäminen vaatii. Tämän jälkeen siirryn luonnollisten lukujen joukon rakentamiseen ja tästä kokonaislukuihin. Perustelen myös jokaisen lukujoukon kohdalla, mistä näiden joukkojen peruslaskutoimitukset, eli yhteenlasku, vähennyslasku ja kertolasku tulevat joukko-opin ja ryhmäteorian avulla.

Pyrin välttämään lähdeteokseni suoraa kääntämistä ja yritin tehdä työstä sellaisen, että siinä näkyy oma persoonani sekä innostukseni matematiikkaa kohtaan. Tästä huolimatta esimerkit ovat suoria lainauksia lähdeteoksesta, mutta näiden perustelut ja todistukset lukuunottamatta Lauseen 3.1 ja muutamaa Lauseen 3.4 todistusta ovat itse kehiteltyjä. Työni on siis tehty kokonaan teoksen [1] sekä sen avulla kehiteltyjen perusteluiden avulla.

Jotta lukija ymmärtää tekstin hyvin, vaatii tämä perusosaamisen joukko-opista, kuten vaikka sen, miten joukkojen väliset operaatiot toimivat tai miten joukot kytkeytyvät toisiinsa. Kaikki vaadittavat asiat kuitenkin löytyvät kappaleesta 2 eli 'Esitietoja' -kappaleesta.

2 Esitietoja

2.1 Joukko-opin perusaksioomat

Aksiooma 2.1. *On olemassa joukko X.*

Huomautus 2.1. Aksioomasta 2.1 seuraa, että on olemassa tyhjä joukko $\emptyset$, kun asetetaan $\emptyset = \{y \in X \mid y \neq y\}$.

Aksiooma 2.2. *On olemassa joukko $I = \{\emptyset \in I \ \&(x \in I \ \rightarrow (x \cup \{x\}) \in I)\}$.*

Aksiooma 2.3. *Jokaiselle alkiolle a ja b on olemassa joukko X siten, että $a \in X$ ja $b \in X$.*

Huomautus 2.2. Aksioomasta 2.3 saadaan joukko
$\{a, b\} := \{x \in X \mid x = a \vee x = b\}$

Aksiooma 2.4. *Jokaista kokoelmaa $\mathcal{F}$ kohden on olemassa joukko U siten, että $\bigcup \mathcal{F} \subset U$.*

Aksiooma 2.5. *Jokaisella joukolla X on olemassa joukko P siten, että se sisältää joukon $\mathcal{P}(X)$ eli X:n kaikkien osajoukkojen potenssijoukon.*

Näiden lisäksi joukoille X ja Y on voimassa ehto:

Aksiooma 2.6. *$X = Y$ jos ja vain jos ne sisältävät täsmälleen samat alkiot.*

2.2 Merkintöjä

Seuraavat käsitteet seuraavat joukko-opin perusaksioomista.

$X \cup Y = \bigcup\{X, Y\}$ on joukkojen X ja Y yhdiste.

$\bigcap \mathcal{F} = \{z \in \bigcup \mathcal{F} \mid \forall F \in \mathcal{F} \ (z \in F)\}$ on kokoelman $\mathcal{F}$ joukkojen leikkaus.

$X \cap Y = \bigcap\{X, Y\}$ on joukkojen X ja Y leikkaus.

$\mathcal{P}(X) = \{Z \mid Z \subset X\}$ on X:n kaikkien osajoukkojen joukko, potenssijoukko.

2.3 Relaatiot

Määritelmä 2.3. Olkoot X ja Y epätyhjiä joukkoja. *Karteesinen tulo* $X \times Y$ voidaan määritellä joukkojen X ja Y alkioiden x ja y muodostamien parien joukkona eli

$$X \times Y = \{\langle x, y \rangle \mid x \in X, y \in Y\}.$$

Karteesisen tulon avulla saadaan määriteltyä binäärirelaatio.

Määritelmä 2.4. *Binäärirelaatio* joukossa X on $R \subset (X \times X)$. Alkio $x \in X$ on relaatiossa alkion $y \in X$ kanssa, jos $\langle x, y \rangle \in R$. Tällöin merkitään xRy.

Binäärirelaation yhteydessä puhutaan usein kolmesta ominaisuudesta: refleksiivisyydestä, symmetrisyydestä ja transitiivisuudesta.

Määritelmä 2.5. Relaatio R on *refleksiivinen*, jos xRx kaikille joukon X alkioille x.

Määritelmä 2.6. Relaatio R on *symmetrinen*, jos relaatiosta xRy seuraa, että yRx kaikilla joukon X alkioilla x ja y.

Määritelmä 2.7. Relaatio R on *transitiivinen*, jos ehdoista xRy ja yRz seuraa, että xRz kaikilla joukon X alkioilla x, y ja z.

Esimerkki 2.1. *Määritellään relaatio R joukossa $\mathbb{N}$ siten, että xRy jos ja vain jos $y = x^2$. Tällöin relaatiolla R ei ole mitään ylläolevista ominaisuuksista.*

Todistus. Refleksiivisyys: Vastaesimerkkinä valitaan $x = 2$, jolloin relaatio $x = x^2$ eli $2 = 2^2 = 4$ ei ole voimassa. Täten relaatio R ei ole refleksiivinen.

Symmetrisyys: Valitaan vastaesimerkiksi $x = 4$ ja $y = 2$, jolloin $x = y^2$ eli $4 = 2^2 = 4$ on voimassa, mutta tästä ei seuraa, että $y = x^2$ eli $2 = 4^2 = 16$ olisi voimassa. Täten relaatio R ei ole symmetrinen.

Transitiivisuus: Valitaan $x = 16$, $y = 4$ ja $z = 2$, jolloin relaatiot $x = y^2$ ja $y = z^2$ eli $16 = 4^2$ ja $4 = 2^2$ ovat voimassa. Tästä ei kuitenkaan seuraa, että relaatio $x = z^2$ eli $16 = 2^2$ olisi voimassa. Täten relaatio R ei ole transitiivinen. □

Erityishuomiona edelliseen esimerkkiin: Jos joukkomme olisi pelkästään luvun 1 tai luvun 0 muodostama joukko, relaatiolla xRy jos ja vain jos $x = y^2$ olisi kaikki kolme ominaisuutta.

Esimerkki 2.2. *Relaatio $=$ on refleksiivinen, symmetrinen ja transitiivinen joukossa $\mathbb{N}$.*

Esimerkistä 2.2 pääsemme varsinaisen aiheen kannalta tärkeimpään relaatioon, ekvivalenssirelaatioon.

Määritelmä 2.8. Kutsumme joukossa $X \times X$ määriteltyä binäärirelaatiota R *ekvivalenssirelaatioksi*, jos se on refleksiivinen, symmetrinen ja transitiivinen.

3 Luonnolliset luvut

3.1 Lukujoukon rakentaminen

Aksioomien 2.1 ja 2.3 perusteella on ymmärrettävää, että on olemassa joukot, kuten $\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\{\emptyset\}\}$ ja niin edelleen. Vielä ei ole kuitenkaan selvää, että on olemassa monimutkaisempia joukkoja, kuten $\mathbb{N}$ tai $\mathbb{Z}$.

Luonnollisten lukujen joukon $\mathbb{N}$ määräävät seuraava aksiooma sekä lause:

Määritelmä 3.1. Määritellään joukon x *seuraaja* $S(x)$ seuraavasti:

$$S(x) = x \cup \{x\}.$$

Lause 3.1. *On olemassa täsmälleen yksi joukko* $\mathbb{N}$*, jolle pätee seuraavat kolme ominaisuutta:*

1. $\emptyset \in \mathbb{N}$.
2. *Jokaiselle alkiolla* n, $n \in \mathbb{N} \rightarrow S(n) \in \mathbb{N}$.
3. *Olkoon* K *sellainen joukko, jolle ominaisuudet 1 ja 2 ovat voimassa. Tällöin* $\mathbb{N} \subset K$

Todistus. Aksiooman 2.2 nojalla on olemassa ainakin yksi joukko X, jolle ominaisuudet 1 ja 2 ovat voimassa. Olkoon nyt

$$F = \{Y \in \mathcal{P}(X) \mid \emptyset \in Y \ \& \ \forall x \in Y \ (S(x) \in Y)\}$$

eli F koostuu kaikista niistä X:n osajoukoista, jotka toteuttavat ehdot 1 ja 2. Siispä $X \in F$. Asetetaan $\mathbb{N} = \bigcap F$. On selvää, että minkä tahansa joukkojen, jotka toteuttavat ehdot 1 ja 2, leikkaus toteuttaa myös kyseiset ehdot. Osoittaaksemme, että myös ehto 3 toteutuu, olkoon K mikä tahansa joukko, joka toteuttaa ehdot 1 ja 2. Tällöin

$$(K \cap X) \in F \text{ joten } \mathbb{N} = \bigcap F \subset (K \cap X) \subset K.$$

□

Määritelmä 3.2. Lauseen 3.1 määräämää joukkoa $\mathbb{N}$ kutsutaan luonnollisten lukujen joukoksi ja sen alkioita luonnollisiksi luvuiksi. Luonnollisen luvun $n \in \mathbb{N}$ seuraajaa $S(n)$ merkitään $n + 1$. Lisäksi merkitään $0 = \emptyset$.

Erityishuomiona Lauseen 3.1 kohta 3 voidaan kirjoittaa seuraavalla tavalla:

Lause 3.2. $[0 \in K \ \& \ \forall x \ (x \in K \to S(x) \in K]$ *implikoi, että* $\mathbb{N} \subset K$

Lause 3.3. *Jos lisäksi tiedetään, että* $K \subset \mathbb{N}$,
niin $[0 \in K \ \& \ \forall x \ (n \in K \to n + 1 \in K)]$, *implikoi, että* $\mathbb{N} = K$

Joukolla $\mathbb{N}$ on tiettyjä ominaisuuksia, joita tarkastellaan seuraavassa kappaleessa.

3.2 Luonnollisten lukujen ominaisuuksia

Lause 3.4. *Luonnollisten lukujen joukon alkioilla* m, n *ja* p *on seuraavat ominaisuudet:*

1. $m \subset m + 1$ *ja* $m \in m + 1$.
2. *Jos* $x \in m$, *niin* $x \in \mathbb{N}$.
3. *Jos* $m \in n$, *niin* $m + 1 \subset n$.
4. *Jos* $m \in n$ *ja* $n \in p$, *niin* $m \in p$.
5. $n \notin n$
6. *Jos* $m + 1 = n + 1$, *niin* $m = n$.
7. $m \subset n$ *jos ja vain jos* $m \in n$ *tai* $m = n$.
8. $m \subset n$ *tai* $n \subset m$.

Todistus.

1. Määritelmän 3.1 nojalla $m + 1 = m \cup \{m\}$, josta nähdään suoraan, että $m \in m + 1$ sekä $m \subset m + 1$.

2. Olkoon $K = \{n \in \mathbb{N} \mid \forall n \ (x \in n \to x \in \mathbb{N})\}$ sekä $n \in K$ ja $x \in n + 1$. Koska $n+1 = n \cup \{n\}$, saamme kaksi tilannetta: joko $x \in n$ tai $x \in \{n\}$. Jos $x \in n$, niin $x \in \mathbb{N}$, sillä $n \in K$. Jos $x \in \{n\}$, niin $x = n$ jolloin $x \in \mathbb{N}$. Siispä $n \in K$ implikoi, että $n + 1 \in K$ eli Lauseen 3.3 nojalla kohta 2 on osoitettu.

3. Todistus tapahtuu induktiolla. Logiikan nojalla väärästä väitteestä voi seurata mitä vain, joten väite

$$m \in 0 \to m + 1 \subset 0$$

on tosi. Oletetaan, että ehdosta $m \in n$ seuraa, että $m + 1 \subset n$. Olkoon nyt $m \in n + 1$. Tällöin Määritelmän 3.1 nojalla $m \in n \cup \{n\}$, eli $m \in n$ tai $m \in \{n\}$. Jos $m \in n$, todistus seuraa välittömästi induktio-oletuksesta. Jos $m \in \{n\}$, niin $m = n$. Tällöin myös $m + 1 = n + 1$ joten $m + 1 \subset n + 1$.

4. Olkoot $m \in n$ ja $n \in p$. Nyt kohdan 1 nojalla $n \subset n+1$ joten $m \in n+1$. Koska $n \in p$, niin kohdan 3 nojalla $n+1 \subset p$ joten $m \in n+1 \subset p$ jolloin $m \in p$.

5. Osoitus tapahtuu induktiolla. Selvästi $\emptyset \notin \emptyset$ eli $0 \notin 0$. Oletetaan, että $n \notin n$. On osoitettava, että $S(n) \notin S(n)$.

   Tehdä vastaoletus ja oletetaan, että $S(n) \in S(n)$. Tällöin Määritelmän 3.1 nojalla $n \cup \{n\} \in n \cup \{n\}$. Tästä saadaan kaksi tapausta: joko $n \cup \{n\} \in n$ tai $n \cup \{n\} \in \{n\}$.

   Koska $n \in n \cup \{n\}$, ensimmäisestä tapauksesta saadaan $n \in n \cup \{n\} \in n$, jolloin $n \in n$, mikä on ristiriita induktio-oletuksen kanssa.

   Koska $n \cup \{n\} \in \{n\}$, pätee $n \cup \{n\} = n$. Tällöin toisesta tapauksesta saadaan $n \in n \cup \{n\} = n$ jolloin $n \in n$ mikä on ristiriidassa induktio-oletuksen kanssa.

   Täten vastaoletus kumoutuu ja alkuperäinen väite on tosi. Siis $S(n) \notin S(n)$.

6. Olkoon $m+1 = n+1$. Määritelmän 3.1 nojalla $m+1 = m \cup \{m\}$ ja $n+1 = n \cup \{n\}$. Nyt Aksiooman 2.6 nojalla, koska $m+1 = n+1$, on näiden alkioiden oltava samat. Tällöin pätevät sekä $m \in n \cup \{n\}$ että $n \in m \cup \{m\}$. Ensimmäisestä seuraa, että $m \in n$ tai $m = n$ ja jälkimmäisestä, että $n \in m$ tai $n = m$. Näistä ainoa mahdollinen tapaus on, että $m = n$ ja $n = m$, sillä muut tapaukset johtavat ristiriitaan kohdan 5 nojalla.

7. "$\Leftarrow$" Jos $m = n$, niin $m \subset n$. Jos $m \in n$, niin kohdan 3 nojalla $m+1 \subset n$ ja kohdan 1 nojalla $m \subset m+1$ eli $m \subset n$.

   "$\Rightarrow$" Olkoon $K = \{n \in \mathbb{N} \mid m \subset n \rightarrow [m \in n \vee m = n]\}$. Riittää osoittaa, että $K = \mathbb{N}$. Nyt $0 \in K$, sillä $m \subset 0 = \emptyset$ implikoi, että $m = \emptyset = 0$. Oletetaan, että $n \in K$ ja että $m \subset n+1 = n \cup \{n\}$. Jos $m \not\subset n$, niin $n \in m$ ja kohdan 3 nojalla $n+1 \subset m$ sekä oletuksen mukaan $m \subset n+1$ eli $m = n+1$. Jos $m \subset n$, niin $m \in n$ tai $m = n$ koska $n \in K$. Molemmissa tapauksissa $m \in n \cup \{n\} = n+1$ joten $n+1 \in K$. Siis $0 \in K$ ja oletuksesta $n \in K$ seuraa, että $n+1 \in K$, joten induktion nojalla $K = \mathbb{N}$ mikä osoittaa väitteen.

8. Olkoon $K = \{m \in \mathbb{N} \mid \forall n \in \mathbb{N}\,(n \notin m \rightarrow m \subset n)\}$. Aluksi osoitetaan, että $K = \mathbb{N}$. Nyt $0 \in K$ sillä $0 = \emptyset \subset n$ kaikilla luonnollisilla luvuilla n. Oletetaan, että $m \in K$ ja osoitetaan, että $m+1 \in K$. Olkoon $n \in \mathbb{N}$ sellainen, että $n \notin m+1 = m \cup \{m\}$. Tällöin $n \neq m$ ja $n \notin m$.

Kuitenkin, koska $m \in K$ ja $n \notin m$, niin $m \subset n$. Koska $m \subset n$ ja $m \neq n$, kohdan 7 nojalla $m \in n$, josta kohdan 3 nojalla $m + 1 \subset n$. Siispä ehdosta $m \in K$ seuraa, että $m + 1 \in K$, joten induktion nojalla $K = \mathbb{N}$. Seuraavaksi oletetaan, että $n,\ m \in \mathbb{N}$. Jos $n \subset m$, todistus on selvä. Jos $n \not\subset m$, kohdan 7 nojalla voidaan todeta, että $n \notin m$. Koska $m \in \mathbb{N} = K$, saamme $m \subset n$.

□

Lauseesta (3.4) seuraa lisäksi välittömästi, että jokainen luonnollinen luku $n = \{0, 1, 2, \ldots, n-1\}$. Erityisesti luku 0 kuuluu sen nojalla luonnollisiin lukuihin, sillä $0 = \emptyset$. Kuitenkaan merkintä $\{0, 1, 2, \ldots, n-1\}$ ei kuulu joukko-opin formaaliin merkintätapaan, sillä saman ilmaiseminen vaatisi äärettömän monta lausetta, yhden jokaista luonnollista lukua kohti. Näin ollen on järkevämpi käyttää intuitiivista merkintätapaa eli kirjoittaa vain n. Esimerkiksi on paljon helpompaa kirjoittaa 3 kuin $\{0, 1, 2\}$. Lauseen (3.4) avulla voimme myös määrittää luonnollisten lukujen m ja n suuruusjärjestyksen seuraavasti:

Määritelmä 3.3.

$$m < n \text{ jos ja vain jos } m \in n$$

ja

$$m \leq n \text{ jos ja vain jos } m \subset n.$$

Määritellään induktion avulla luonnollisten lukujen laskutoimitukset, eli summa ja tulo:

Määritelmä 3.4. Luonnollisten lukujen *summa* määritellään

$$m + 0 = m;\ m + S(n) = S(m + n).$$

Luonnollisten lukujen *tulo* määritellään

$$m0 = 0;\ mS(n) = (mn) + m.$$

Summa määrittelee, mitä on $m+S(n)$, mutta se ei kerro, mitä on $S(m)+n$.

Lause 3.5. *Luonnollisille luvuille m ja n pätee: $S(m) + n = m + S(n)$.*

Todistus. Tapahtuu induktiolla. Nyt $S(m)+0 = S(m) = S(m+0) = m+S(0)$ Määritelmän 3.4 nojalla. Oletetaan, että $S(m) + n = m + S(n)$. Osoitetaan, että $S(m) + S(n) = m + S\big(S(n)\big)$. Määritelmän 3.4 nojalla

$$S(m) + S(n) = S\big(S(m) + n\big)$$

josta induktio-oletuksen nojalla saadaan

$$S\big(S(m)+n\big) = S\big(m+S(n)\big).$$

Tästä edelleen Määritelmän 3.4 nojalla

$$S\big(m+S(n)\big) = m+S\big(S(n)\big).$$

Siis väite on osoitettu. □

Kokonaislukuja varten osoitetaan vielä luonnollisten lukujen summan kommutatiivisuus ja assosiatiivisuus:

Lause 3.6. *Luonnollisille luvuille n, m ja p pätee:*

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

Todistus. Tapahtuu induktiolla. Olkoot m, n ja p luonnollisia lukuja. Nyt

$$(m+n)+0 = m+n = m+(n+0)$$

on totta. Oletetaan, että

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

on voimassa. Todistetaan, että $(m+n)+S(p) = m+(n+S(p))$. Tällöin Määritelmän 3.4 nojalla

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

Induktio-oletuksen nojalla taas saadaan

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

josta edelleen Määritelmän 3.4 nojalla

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

Siis luonnollisten lukujen summa on assosiatiivinen.

□

Lause 3.7. *Luonnollisille luvuille n ja m pätee: $m + n = n + m$.*

Todistus. Tapahtuu induktiolla n:n suhteen. Induktioaskeleessa on osoitettava, että $m + 0 = 0 + m$. Tämä tapahtuu induktiolla m:n suhteen.

Selvästi $0 + 0 = 0 + 0$. Oletetaan, että $m + 0 = 0 + m$. Osoitetaan, että $S(m) + 0 = 0 + S(m)$. Nyt Lauseen 3.5 nojalla

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

jolloin Määritelmän 3.4 nojalla

$$m + S(0) = S(m + 0).$$

Tästä saadaan induktio-oletuksen nojalla

$$S(m + 0) = S(0 + m)$$

ja edelleen Määritelmän 3.4 nojalla

$$S(0 + m) = 0 + S(m).$$

Siispä induktioaskel on osoitettu todeksi.

Oletetaan nyt, että $m+n = n+m$ ja osoitetaan, että $m+S(n) = S(n)+m$. Nyt Määritelmän 3.4 nojalla

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

josta induktio-oletuksen nojalla

$$S(m + n) = S(n + m)$$

ja lopuksi Määritelmän 3.4 ja Lauseen 3.5 nojalla

$$S(n + m) = S(n) + m.$$

Siis luonnollisten lukujen yhteenlasku on kommutatiivinen. □

Osoitetaan kappaleen lopuksi vielä luonnollisten lukujen supistuslaki, jota tarvitaan seuraavassa kappaleessa.

Lause 3.8. *Luonnollisille luvuille n, m ja p pätee:*

$$m + p = n + p \rightarrow m = n$$

Todistus. Tapahtuu induktiolla. Nyt $m+0 = n+0 \to m = n$ on yhteenlaskun määritelmän nojalla voimassa. Oletetaan, että $m+p = n+p \to m = n$. Väite: $m + S(p) = n + S(p) \to m = n$.

Oletetaan, että $m + S(p) = n + S(p)$. Tällöin Määritelmän 3.4 saadaan

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

jolloin Lauseen 3.4 kohdan 6 nojalla

$$m + p = n + p.$$

Tästä saadaan induktio-oletuksen nojalla

$$m = n.$$

□

4 Kokonaisluvut

4.1 Lukujoukon rakentaminen

Kokonaislukuja voidaan esittää ekvivalenssiluokkina muodossa $[\langle m, n\rangle]$, missä n ja m ovat luonnollisia lukuja. Intuitiivisesti tämä lukupari voidaan ajatella lukujen erotuksena $m - n$, mutta erotusoperaatiota ei ole vielä määritelty, joten se täytyy ensin määritellä.

Määritelmä 4.1. Määritellään ekvivalenssirelaatio E joukossa $\mathbb{N} \times \mathbb{N}$ seuraavasti:

$$\langle m, n\rangle E\langle m', n'\rangle \text{ jos ja vain jos } m + n' = m' + n.$$

Esimerkiksi lukuparit $\langle 2, 3\rangle$ ja $\langle 4, 5\rangle$ ovat relaatiossa, koska $2 + 5 = 7 = 3 + 4$.

Lause 4.1. *Relaatio E on ekvivalenssirelaatio.*

Todistus.

1. Refleksiivisyys. $\langle m, n\rangle E\langle m, n\rangle$ selvästi, sillä $m + n = m + n$ on tosi.

2. Symmetrisyys. Oletetaan, että $\langle m, n\rangle E\langle m', n'\rangle$. Tällöin pätee $m+n' = m'+n$. Tällöin myös pätee $m'+n = m+n'$, jolloin myös $\langle m', n'\rangle E\langle m, n\rangle$.

3. Transitiivisuus. Oletetaan, että $\langle m, n\rangle E\langle m', n'\rangle$ sekä $\langle m', n'\rangle E\langle m'', n''\rangle$. Tällöin pätee, että $m + n' = m' + n$ sekä $m' + n'' = m'' + n'$. Yhtäsuuruuksien nojalla

$$(m + n') + (m' + n'') = (m' + n) + (m'' + n')$$

josta assosiatiivisuuden ja kommutatiivisuuden nojalla saadaan

$$(m + n'') + (n' + m') = (m'' + n) + (n' + m').$$

Tästä saadaan Lauseen 3.8 nojalla

$$m + n'' = m'' + n$$

josta seuraa, että $\langle m, n\rangle E\langle m'', n''\rangle$.

Täten E on ekvivalenssirelaatio □

Relaation E avulla saadaan määriteltyä kokonaislukujen joukko.

Määritelmä 4.2. Kokonaislukujen joukko $\mathbb{Z}$ on relaation E ekvivalenssiluokkien joukko, eli $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/E$. Kokonaislukuja merkitään ekvivalenssiluokkina $[\langle m, n\rangle]$, missä m ja n ovat luonnollisia lukuja.

Kuten aiemmin todettu, tällä hetkellä luonnollisten lukujen erotus, jolla saadaan määrätyksi negatiiviset kokonaisluvut, on vain intuitiivinen merkitsemistapa. Määritelläksemme erotuksen, määritetään ensin kokonaislukujen summa.

Määritelmä 4.3. Kokonaislukujen $[\langle m, n\rangle]$ ja $[\langle m', n'\rangle]$ summa määritellään:

$$[\langle m, n\rangle] + [\langle m', n'\rangle] = [\langle m + m', n + n'\rangle]$$

Käyttäen tätä määritelmää määritellään ryhmäteorian avulla kokonaislukujen erotus.

Lause 4.2. *Joukko $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/E$ varustettuna operaatiolla $+$ on ryhmä.*

Todistus. Aluksi on osoitettava, että summa on hyvin määritelty, eli ekvivalenssiluokille määritelty summa ei muutu, jos luokista otetaan eri edustajat ja summa suoritetaan niillä. On siis osoitettava, että jos $\langle m', n'\rangle \in [\langle m, n\rangle]$ ja $\langle p', q'\rangle \in [\langle p, q\rangle]$, niin tällöin $[\langle m', n'\rangle + \langle p', q'\rangle] = [\langle m, n\rangle + \langle p, q\rangle]$.

Jos $\langle m', n'\rangle \in [\langle m, n\rangle]$ ja $\langle p', q'\rangle \in [\langle p, q\rangle]$, tällöin pätee $\langle m', n'\rangle E\langle m, n\rangle$ sekä $\langle p', q'\rangle E\langle p, q\rangle$, josta ekvivalenssirelaation E määritelmän nojalla saadaan

$$m + n' = m' + n \tag{1}$$
$$p + q' = p' + q. \tag{2}$$

Nyt

$$\langle m', n' \rangle + \langle p', q' \rangle = \langle m' + p', n' + q' \rangle,$$

jolloin lisäämällä pistepari $\langle m, m \rangle$, käyttämällä Lausetta 3.6 sekä kaavaa 1 saadaan

$$\langle (m + p') + m', (m + n') + q' \rangle = \langle (m + p') + m', (m' + n) + q' \rangle.$$

Käyttämällä Lauseita 3.6 ja 3.8 saadaan

$$\begin{aligned} \big[\langle (m + p') + m', m' + (n + q') \rangle\big] &= \big[\langle (m + p') + m', (n + q') + m' \rangle\big] \\ &= \big[\langle m + p', n + q' \rangle\big]. \end{aligned}$$

Lisäämällä pistepari $\langle q, q \rangle$ päästään muotoon

$$\langle m + p', n + q' \rangle + \langle q, q \rangle = \langle (m + p') + q, (n + q') + q \rangle.$$

Käyttämällä kaavaa 2 sekä Lauseita 3.6 ja 3.7 saadaan tästä

$$\begin{aligned} \big[\langle (m + p') + q, (n + q') + q \rangle\big] &= \big[\langle m + (p + q'), (n + q) + q' \rangle\big] \\ &= \big[\langle (m + p) + q', (n + q) + q' \rangle\big] \end{aligned}$$

josta Lauseen 3.8 ja Määritelmän 3.4 päästään muotoon

$$\begin{aligned} \big[\langle (m + p) + q', (n + q) + q' \rangle\big] &= \big[\langle m + p, n + q \rangle\big] \\ &= \big[\langle m, n \rangle\big] + \big[\langle p, q \rangle\big] \end{aligned}$$

.

Tämä osoittaa, että yhteenlasku on hyvin määritelty.

1. Olkoot m, m', n ja n' luonnollisia lukuja. Tällöin $[\langle m, n \rangle]$ ja $[\langle m', n' \rangle]$ ovat kokonaislukuja. Nyt $[\langle m, n \rangle] + [\langle m', n' \rangle] = [\langle m + m', n + n' \rangle]$ ja koska m, m', n ja n' ovat luonnollisia lukuja, myös $m + m'$ ja $n + n'$ ovat luonnollisia lukuja, jolloin $[\langle m + m', n + n' \rangle]$ on kokonaisluku. Täten kokonaislukujen yhteenlasku on binäärinen operaatio.

2. Olkoot m, m', m'', n, n' ja n'' luonnollisia lukuja. Tällöin $\langle m, n\rangle, \langle m', n'\rangle$ ja $\langle m'', n''\rangle$ ovat kokonaislukuja. Nyt

$$\begin{aligned}\Big([\langle m, n\rangle] + [\langle m', n'\rangle]\Big) + [\langle m'', n''\rangle] &= [\langle m + m', n + n'\rangle] + [\langle m'', n''\rangle] \\ &= [\langle (m + m') + m'', (n + n') + n''\rangle] \\ &= [\langle m + (m' + m''), n + (n' + n'')\rangle] \\ &= [\langle m, n\rangle] + [\langle m' + m'', n' + n''\rangle] \\ &= [\langle m, n\rangle] + \Big([\langle m', n'\rangle] + [\langle m'', n''\rangle]\Big).\end{aligned}$$

   Täten kokonaislukujen yhteenlasku on assosiatiivinen operaatio.

3. Olkoot m ja n luonnollisia lukuja. Tällöin $[\langle m, n\rangle]$ on kokonaisluku. Nyt
$$[\langle m, n\rangle] + [\langle 0, 0\rangle] = [\langle m + 0, n + 0\rangle] = [\langle m, n\rangle]$$
   ja
$$[\langle 0, 0\rangle] + [\langle m, n\rangle] = [\langle 0 + m, 0 + n\rangle] = [\langle m, n\rangle]$$
   eli alkio $[\langle 0, 0\rangle]$ on kokonaislukujen neutraalialkio.

4. On osoitettava, että $\langle m, n\rangle + \langle n, m\rangle E\langle 0, 0\rangle$ joka osoittaa, että $\langle m, n\rangle$ sekä $\langle n, m\rangle$ ovat toistensa käänteisalkiot. Nyt Lauseen 3.7 nojalla pätee $(m + n) + 0 = (n + m) + 0$, joka tarkoittaa, että $\langle m + n, n + m\rangle E\langle 0, 0\rangle$, josta seuraa, että $\langle m, n\rangle + \langle n, m\rangle E\langle 0, 0\rangle$. Tämä osoittaa, että jokaisella kokonaisluvulla $[\langle m, n\rangle]$ on käänteisalkio, ja se on $[\langle n, m\rangle]$.

□

Edellisellä todistuksella oli tarkoitus helpottaa vähennyslaskun määrittelemistä. Koska osoitimme, että kokonaislukujen käänteisalkio $-[\langle m, n\rangle] = [\langle n, m\rangle]$, voidaan erotus määritellä seuraavasti:

Määritelmä 4.4.

$$[\langle m, n\rangle] - [\langle m', n'\rangle] = [\langle m, n\rangle + \langle n', m'\rangle]$$

Lopuksi vielä määritellään kokonaislukujen tulo seuraavasti:

Määritelmä 4.5.

$$[\langle m, n\rangle][\langle m', n'\rangle] = [\langle mm' + nn', mn' + nm'\rangle].$$

Kokonaislukujen tulon ominaisuuksia ei tarkastella tässä työssä.

Lähdeluettelo

[1] Krzysztof Ciesielski: *Set Theory for the Working Mathematician*. Cambridge University Press, Cambridge 1997.