Koulumatematiikan perusteet
800104P

Matemaattisten tieteiden laitos

Oulun yliopisto

2009

”Ihmisen henkistä toimintaa ei voi sanoa taiteeksi ellei se perustu matemaattiseen ajatteluun ja todistukseen”

- Leonardo da Vinci

Sisältö

1 Johdanto **5**

2 Luonnolliset luvut **7**

2.1 Lukukäsite ja luvun merkitseminen 7

2.2 Luonnollisten lukujen määrittely Peanon aksiomien avulla . . 8

2.3 Luonnollisten lukujen yhteen- ja kertolasku 10

2.4 Jaollisuus 12

2.5 Alkuluvut ja yhdistetyt luvut 13

3 Lukujärjestelmät **15**

3.1 Siirtyminen järjestelmästä toiseen 16

3.2 Laskutoimitukset 17

4 Kokonaisluvut **19**

4.1 Kokonaislukujen määrittely 20

4.2 Kokonaislukujen yhteen- ja kertolasku 21

4.3 Kokonaislukujen järjestys 23

4.4 Luonnollisten lukujen ja kokonaislukujen välinen yhteys 24

4.5 Kokonaislukujen jaollisuus 25

5 Rationaaliluvut **27**

5.1 Rationaalilukujen järjestys 28

5.2 Kokonaiset rationaaliluvut ja kokonaisluvut 29

5.3 Rationaalilukujen desimaaliesitys 31

6 Reaaliluvut **37**

6.1 Lukusuora 37

6.2 Desimaaliesitys 37

6.3 Rationaali- ja irrationaaliluvut 39

6.4 Desimaalilukujen aritmetiikasta 40

6.5 Reaalilukujen täydellisyys 41
6.6 Reaalilukujen aritmetiikan määrittely 44
6.7 Muita konstruktioita 45

7 Joukkojen mahtavuudet **47**

Viitteet **50**

Esipuhe

Tämä luentomoniste on syntynyt keväällä 2006 ja 2007 pitämieni luentojen pohjalta. Tekstin puhtaaksikirjoituksesta on vastannut Jonna Makkonen ja haluan esittää hänelle parhaat kiitokseni

Oulussa keväällä 2007
Jukka Kemppainen

1 Johdanto

Matematiikan alkuperä liittyy jokapäiväiseen elämään.

Suurin osa matematiikasta on kehittynyt alkujaan luvun, suuruuden ja muodon käsitteiden ajattelusta. Alkeellisten lukuun, suuruuteen ja muotoon liittyvien käsitteiden juuret voi jäljittää ihmiskunnan alkuun, ja ihmistä monia miljoonia vuosia vanhemmista elämänmuodoista on löydetty viitteitä matemaattisiin käsitteisiin.

Aluksi primitiiviset luvun, suuruuden ja muodon käsitteet liittyivät ehkä kontrastiin pikemmin kuin samankaltaisuuteen, yhden ja monen väliseen eroon, eri objektien kokojen väliseen eroon, pyöreyden ja suoruuden erilaisuuteen. Tiede ja matematiikka syntyivät kuitenkin lukujen ja muotojen samankaltaisuuden oivaltamisesta. Esimerkiksi yhdellä sudella, yhdellä lampaalla ja yhdellä puulla on yhteinen ominaisuus; se että niitä on yksi. Samaan tapaan havaittiin, että joidenkin toisenlaisten ryhmien, esimerkiksi parien, välille voidaan tehdä kääntäen yksikäsitteinen vastaavuus. Esimerkiksi kädet voidaan liittää pareittain jalkoihin, silmiin ja niin edelleen. Suuri askel modernin matematiikan suuntaan otettiin, kun havaittiin, että tietyillä ryhmillä on yhteinen abstrakti ominaisuus, jota kutsutaan luvuksi.

Aikoinaan ajateltiin, että matematiikka liittyy suoraan aistiemme havaintojen maailmaan, ja puhdas matematiikka vapautui luonnon havainnoinnin rajoituksista vasta 1800-luvulla. Moderni matematiikka koostuu peruskäsitteistä, niiden välisistä perussuhteista, perustotuuksista (aksiomeista) sekä edellisistä loogisesti johdetuista lauseista. Määrittelemällä uusia käsitteitä (joista osa voidaan määritellä peruskäsitteiden avulla) voidaan lauseiden joukkoa edelleen laajentaa.

Esimerkki. Euklidisessa geometriassa

1) piste ja suora ovat peruskäsitteitä joita ei määritellä;

2) piste ja suora asetetaan perussuhteeseen, esim. ”suora kulkee pisteen kautta” (Insidenssin suhde);

3) uusi käsite ympyrä voidaan määritellä pisteiden joukkona, joilla on sama etäisyys kiinteästä pisteestä O (etäisyys voidaan edelleen palauttaa pisteisiin);

4) ”Kahden eri pisteen kautta kulkee täsmälleen yksi suora” on aksiomi;

5) esimerkiksi Pythagoraan lause voidaan loogisesti johtaa aksiomeista.

Näin matematiikalle on luotu looginen rakenne. Matematiikka onkin ainutlaatuista, sillä vain siinä ei ole merkittäviä korjauksia, ainoastaan laajennuksia. Esimerkiksi Eukleideen jokainen lause on edelleen voimassa, niitä ei tarvitse korjata (vertaa esimerkiksi fysiikassa Einsteinin korjaukset Newtonin liikelakeihin ja painovoimateoriaan).

Tällä kurssilla perehdytään kouluissa tarvittavan aritmetiikan ja algebran matemaattisiin perusteisiin, erityisesti lukujoukkoihin ja lukujärjestelmiin.

2 Luonnolliset luvut

Joukko-opin kertausta ja merkintöjä

Käydään lyhyesti läpi tällä kurssilla tarvittavia joukko-opin alkeita.

Jos A on joukko, niin merkintä $x \in A$ (luetaan x kuuluu joukkoon A) tarkoittaa, että x on joukon A alkio. Vastaavasti merkinnällä $x \notin A$ tarkoitetaan, että x ei ole joukon A alkio. Edelleen joukot A ja B ovat samat ja merkitään $A = B$, jos niillä on samat alkiot. Jos joukot A ja B eivät ole samat, niin merkitään $A \neq B$.

Usein joukoille käytetty merkintätapa on $\{x \in E | P(x)\}$, missä E on perusjoukko ja P alkioita x koskeva ominaisuus, joka on joko tosi tai epätosi kaikilla $x \in E$. Jos perusjoukosta ei ole epäselvyyttä, jätetään se merkitsemättä näkyviin. Huomaa kuitenkin, että esimerkiksi $\{x | 1 \leq x \leq 5\}$ on suljettu väli $[1, 5]$, jos $E = \mathbb{R}$, ja joukko $\{1, 2, 3, 4, 5\}$, jos $E = \mathbb{Z}$.

Joukkoa A sanotaan joukon B osajoukoksi ja merkitään $A \subseteq B$, jos jokainen joukon A alkio kuuluu joukkoon B. Joukko A on joukon B aito osajoukko ja merkitään $A \subsetneq B$, jos $A \subseteq B$ ja $A \neq B$.

Joukkojen A ja B erotuksella $A \setminus B$ tarkoitetaan joukkoa $\{x \in A | x \notin B\}$.

2.1 Lukukäsite ja luvun merkitseminen

Luvun 1 käsite on ollut käytössä lähes kaikilla luonnonkansoilla. Lukukäsitteen kehitys on pitkä ja asteittainen. Viitteitä kehityksestä on joissakin kielissä, joiden kieliopissa on säilynyt yhden, kahden tai enemmän kuin kaksi toisistaan erottava kolmijako. Vielä tänäkin päivänä löytyy heimoja, jotka eivät osaa laskea kahta pidemmälle.

Matematiikan kehitys on saanut alkunsa luonnollisten lukujen tutkimuksesta. Jokaisella on intuitiivinen käsitys luonnollisista luvuista $1, 2, \ldots$, joiden muodostamalle joukolle käytetään merkintää $\mathbb{N}$. Intuitiivisen käsitteen pukeminen tarkaksi matemaattiseksi objektiksi ei ole kuitenkaan yksinkertaista (tämän osoittavat jo historialliset seikat). Tarkastellaan esimerkiksi luvun 2 määrittelyä. Mitä vikaa on seuraavassa määritelmässä: ”Se on kaikkien sellaisten joukkojen ominaisuus, joissa on 2 alkiota”? Kyseessä on ”kehämääritelmä”. Määritelmän itseensä viittaavuudesta voidaan päästä eroon viittaamalla tiettyyn joukkoon. Luku 2 on se, mikä on yhteistä kaikille joukoille, joissa on sama määrä alkioita kuin joukossa $\{\emptyset, \{\emptyset\}\}$ ($\emptyset$ on tyhjä joukko, jossa ei ole yhtään alkiota).

Huomautus. Joukko $\{\emptyset\}$ ei ole tyhjä. Siinä on yksi alkio, $\emptyset$.

Tämä uusi määritelmä nojautuu edelleen käsitteeseen ”luku” osassa ”sama määrä alkioita kuin”. Käsite ”joukoissa A ja B on sama määrä alkioita” voidaan määritellä ilman, että luvuista tiedetään mitään. Kuinka tämä tapahtuu, käy ilmi seuraavasta käytännön ongelmasta.

Esimerkki. Elokuvateatterin lipunmyyjällä on nippu lippuja illan näytäntöä varten. Hän ei ehdi itse tarkistamaan, onko lippuja täsmälleen yhtä monta kuin teatterissa on istumapaikkoja. Lipunmyyjän 5-vuotias tyttö on reipas ja lupaa auttaa, mutta hän ei osaa laskea lippujen lukumäärää. Miten tyttö ratkaisee ongelman?

Luonnollisten lukujen aksiomaattinen perusta voidaan edellä kuvatulla tavalla palauttaa joukko-oppiin (joka voidaan myös aksiomatisoida).

Eri kansoilla oli muinoin käytössä erilaisia merkitsemistapoja luonnollisille luvuille. Luvun merkitseminen on yhteydessä käytettyyn *kantalukujärjestelmään*. Me olemme tottuneet käyttämään kymmenjärjestelmää ja arabialaisia numeroita $0, 1, 2, 3, 4, 5, 6, 7, 8$ ja 9. Tarkastellaan joitakin muita tapoja seuraavassa esimerkissä.

Esimerkki.

2.2 Luonnollisten lukujen määrittely Peanon aksiomien avulla

Seuraavassa tarkoituksena on esittää luonnollisille luvuille eksakti määritelmä (siinä määrin kuin se tämän kurssin puitteissa on mahdollista).

Eräs tapa määritellä luonnoliset luvut on määrittelyn palauttaminen edellisen kappaleen tapaan joukko-oppiin. Vaikka edellä luonnollisilla luvuilla tarkoitettiin lukuja $1, 2, \ldots$, on aritmetiikan kannalta luontevampaa aloittaa luvusta 0 luvun 1 sijaan. Luku 0 on pienin luku ja sen määrittelee joukko $\emptyset$. Luvun 1 määrittelee joukko $\{\emptyset\}$, luvun 2 määrittelee joukko $\{\emptyset, \{\emptyset\}\}$ ja niin edelleen. Matemaatikko John von Neumann määritteli luonnolliset luvut edellä kuvatulla tavalla vuonna 1923. Menetellään tässä kuitenkin toisin.

Lukua 0 seuraa luku 1. Lukua 1 seuraa luku 2... Yleisesti jokaisella luvulla n on *seuraaja*, jota merkitään symbolilla $s(n)$. Vaaditaan, että kahdella eri luvulla ei voi olla samaa seuraajaa. Lisäksi luonnollisten lukujen joukolta vaaditaan, että se on suppein sellaisista joukoista S, joilla on ominaisuudet:

(i) $0 \in S$;

(ii) Jos $n \in S$, niin $s(n) \in S$ ($n \in S \Rightarrow s(n) \in S$).

Kirjoitetaan edellä mainittu aksiomien muotoon. Ensimmäisen luonnollisten lukujen aksiomaattisen määrittelyn esitti italialainen matemaatikko Giuseppe Peano vuonna 1889. Peruskäsitteitä ovat luku, nolla ja seuraaja, joita ei määritellä.

Luonnollisten lukujen joukko, merkitään $\mathbb{N}_0$ (0 on mukana), on joukko, jolla on ominaisuudet:

(A1) $0 \in \mathbb{N}_0$ (0 on luonnollinen luku);

(A2) Jos $n \in \mathbb{N}_0$, niin $s(n) \in \mathbb{N}_0$ (jokaisen luvun seuraaja on luonnollinen luku);

(A3) Jos $s(n) = s(m)$, niin $n = m$ (kahdella eri luvulla ei voi olla samaa seuraajaa);

(A4) $s(n) \neq 0$ kaikilla $n \in \mathbb{N}_0$ (0 ei ole minkään luvun seuraaja);

(A5) Jos joukolla $S \subseteq \mathbb{N}_0$ on ominaisuudet

(i) $0 \in S$,

(ii) $n \in S \Rightarrow s(n) \in S$,

niin $S = \mathbb{N}_0$ (Induktioaksiomi).

Aksiomit (A1) – (A5) ovat Peanon aksiomit.

Ei ole kuitenkaan mitään takeita siitä, että edellä mainittua joukkoa olisi olemassa, joten lisäksi joudutaan ottamaan aksiomi

(A6) On olemassa ehdot (A1) – (A5) täyttävä joukko $\mathbb{N}_0$.

Edellä on kaikki mitä tarvitaan aritmetiikan määrittelyyn. Erityisen tehokkaaksi osoittautuu induktioaksiomi (A5).

Lause 2.2.1. *Jos $n \in \mathbb{N}_0$, $n \neq 0$, niin on olemassa sellainen yksikäsitteinen $m \in \mathbb{N}_0$, että $n = s(m)$.*

Todistus. Luennoilla.

□

Lauseen 2.2.1 todistusperiaatetta nimitetään induktioperiaatteeksi. Jos taas joukko S on muotoa

$$S = \{n \in \mathbb{N}_0 \mid P(n)\},$$

saadaan

Lause 2.2.2. *(Induktioperiaate)*
Olkoon P luonnollisia lukuja koskeva ominaisuus. Oletetaan, että

(i) $P(0)$ *on tosi,*

(ii) jos $n \in \mathbb{N}_0$ *ja* $P(n)$ *on tosi, niin* $P(n+1)$ *on tosi.*

Tällöin $P(n)$ *on tosi kaikilla* $n \in \mathbb{N}_0$.

Lauseessa kohtaa (i) sanotaan perusaskeleeksi ja kohtaa (ii) induktioaskeleeksi. Käytännössä kohdassa (ii) tehdään ensin niin sanottu induktio-oletus "$P(n)$ on tosi" ja sitten induktioväite "$P(n+1)$ on tosi". Tämän jälkeen todistetaan väite "jos $P(n)$ on tosi, niin $P(n+1)$ on tosi" käyttämällä induktio-oletusta.

2.3 Luonnollisten lukujen yhteen- ja kertolasku

Määritellään aritmeettinen operaatio + (yhteenlasku) rekursiivisesti asettamalla

(Y1) $m + 0 = m$ kaikilla $m \in \mathbb{N}_0$,

(Y2) $m + s(n) = s(m + n)$ kaikilla $n, m \in \mathbb{N}_0$.

Vastaavasti operaatio $\cdot$ (kertolasku) määritellään asettamalla

(K1) $m \cdot 0 = 0$ kaikilla $m \in \mathbb{N}_0$,

(K2) $m \cdot s(n) = m \cdot n + m$ kaikilla $n, m \in \mathbb{N}_0$.

Yhteen- ja kertolasku toteuttavat seuraavat laskusäännöt.

Lause 2.3.1. *Kaikilla* $m, n, p \in \mathbb{N}_0$ *pätee*

(1) $(m + n) + p = m + (n + p)$ *(assosiatiivisuus),*

(2) $m + n = n + m$ *(kommutatiivisuus),*

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

(4) $m \cdot n = n \cdot m$,

(5) $m \cdot (n + p) = m \cdot n + m \cdot p$ *(distriputiivilaki).*

Todistus. Luennoilla. □

Koska $s(0) = 1$, niin yhteenlaskun määritelmän mukaan $s(n) = n+1$ (vertaa intuitiivista käsitystä seuraajasta).

Aksiomi (A3) voidaan kirjoittaa nyt muodossa "jos $m + 1 = n + 1$, niin $m = n$", josta induktiolla saadaan supistussäännöt.

Lause 2.3.2. *Jokaisella* $m, n, p \in \mathbb{N}_0$

(6) jos $m + p = n + p$, *niin* $m = n$,

(7) jos $q \neq 0$, $m \cdot q = n \cdot q$, *niin* $m = n$.

Tarkastellaan seuraavassa luonnollisten lukujen järjestystä.

Järjestys $\geq$ joukossa $\mathbb{N}_0$ määritellään seuraavasti:

(J1) $m \geq n$ jos ja vain jos on olemassa sellainen $p \in \mathbb{N}_0$, että $m = n + p$.

Vastaavasti järjestykset $\leq$, $>$ ja $<$ määritellään seuraavasti:

(J2) $m \leq n$ jos ja vain jos $n \geq m$.

(J3) $m > n$ jos ja vain jos $m \geq n$ ja $m \neq n$.

(J4) $m < n$ jos ja vain jos $n > m$.

Luonnollisten lukujen järjestykselle pätee:

Lause 2.3.3. *Jos* $m, n \in \mathbb{N}_0$, *niin tarkalleen yksi seuraavista ehdoista on voimassa:* $m < n$, $m = n$ *tai* $m > n$.

Tarkastellaan vielä lopuksi luonnollisten lukujen erotusta. Jos $m, n \in \mathbb{N}_0$ ja $m \geq n$, niin järjestyksen $\geq$ ja lauseen 2.3.2 mukaan on olemassa sellainen yksikäsitteinen $p \in \mathbb{N}_0$, että

$$m = n + p.$$

Käytetään luvulle p merkintää $p = m - n$.
Lukua p sanotaan lukujen m ja n *erotukseksi* ja laskutoimitusta, jolla luvuista m ja n saadaan p, sanotaan *vähennyslaskuksi.*
Palataan tähän kokonaislukujen yhteydessä.

Ennen kuin siirrytään tarkastelemaan luonnollisten lukujen jaollisuutta, palataan vielä hetkeksi induktioperiaatteeseen.

Induktioperiaatteen muita muotoja

Joskus induktiotodistuksessa aloitetaan jostain kiinteästä $k \in \mathbb{N}_0$ eli oletetaan, että $P(k)$ on tosi. Induktioaskeleessa todistetaan väite "jos $P(m)$ on tosi, niin $P(m+1)$ on tosi" jollakin $m \geq k$. Tällöin $P(n)$ on tosi kaikilla $n \geq k$. Tämä on yhtäpitävä induktioperiaatteen kanssa.

Joskus induktioperiaatetta käytetään muodossa:

(I1) $P(0)$ on tosi;

(I2) Jos $n \in \mathbb{N}_0$ ja $P(m)$ on tosi kaikilla $m \leq n$, niin $P(n+1)$ on tosi.

Tällöin $P(n)$ on tosi kaikilla $n \in \mathbb{N}_0$.

Yllä olevaa periaatetta sanotaan *täydellisen induktion periaatteeksi.* Tämäkin on yhtäpitävää induktioperiaatteen kanssa.

Täydellisen induktion periaatteen avulla voidaan osoittaa jatkossa tarvittava *hyvinjärjestysperiaate.*

Lause 2.3.4. *(Hyvinjärjestysperiaate)*
Jokaisessa joukon $\mathbb{N}_0$ epätyhjässä osajoukossa on pienin alkio.

Todistus. Luennoilla.

□

2.4 Jaollisuus

Kaikille on tuttua, että esimerkiksi luku 12 voidaan jakaa kolmeen osaan ($12 = 4 \cdot 3$), mutta esimerkiksi lukua 11 ei voi jakaa kolmeen osaan.

Yleisesti luonnollinen luku m on *jaollinen* luvulla $n \neq 0$, jos on olemassa sellainen $q \in \mathbb{N}_0$, että $m = qn$. Tällöin sanotaan, että n on luvun m tekijä tai, että n jakaa luvun m ja merkitään $n \mid m$. Muussa tapauksessa merkitään $n \nmid m$.

Esimerkki. $5 \mid 20$, sillä $20 = 4 \cdot 5$. Edelleen $2 \nmid 5$, sillä $2 \cdot 1 = 2 < 5$, $2 \cdot 2 = 4 < 5$ ja $2 \cdot k \geq 6$ aina, kun $k \geq 3$. Luvun 6 tekijät ovat $1, 2, 3$ ja 6.

Jos luvut m ja n eivät ole jaollisia, on jakolaskun tuloksena *jakojäännös*.

Esimerkki. $5 = 2 \cdot 2 + 1$

Lause 2.4.1. *(Jakoalgoritmi)*
Olkoot $m, n \in \mathbb{N}_0, n \neq 0$. *On olemassa sellaiset yksikäsitteiset luvut* $q, r \in \mathbb{N}_0$, *että*

$$m = qn + r, \text{ missä } 0 \leq r < n.$$

Todistus. Luennoilla.

□

2.5 Alkuluvut ja yhdistetyt luvut

Jokainen nollaa suurempi luonnollinen luku on jaollinen itsellään ja luvulla 1. Tekijöitä 1 ja m sanotaan luvun $m \in \mathbb{N}$ triviaaleiksi tekijöiksi.
Jos luvulla $m \in \mathbb{N}, m \geq 2$, ei ole muita kuin triviaalit tekijät, sanotaan lukua m *alkuluvuiksi*. Muussa tapauksessa lukua sanotaan *yhdistetyksi luvuksi*.

Esimerkki. $2, 3, 5, 7$ ja 11 ovat alkulukuja, mutta $4, 10$ ja 15 ovat yhdistettyjä lukuja ($4 = 2 \cdot 2, 10 = 2 \cdot 5$ ja $15 = 3 \cdot 5$).

Jos k on lukujen $m, n \in \mathbb{N}$ tekijä, sanotaan sitä lukujen m ja n *yhteiseksi tekijäksi*. Selvästikin 1 on aina minkä tahansa lukujen yhteinen tekijä. Jos 1 on lukujen $m, n \in \mathbb{N}$ ainoa yhteinen tekijä, sanotaan lukuja m ja n *suhteellisiksi alkuluvuiksi*.

Lukua $k \in \mathbb{N}$ sanotaan lukujen $m, n \in \mathbb{N}$ *suurimmaksi yhteiseksi tekijäksi*, merkitään $k = \text{syt}(m, n)$, jos

(i) $k \mid n$ ja $k \mid n$ (ts. k on lukujen m ja n tekijä),

(ii) $l \mid m$ ja $l \mid n \Rightarrow l \mid k$ (k on yhteisistä tekijöistä suurin).

Lukujen $m, n \in \mathbb{N}$ suurimman yhteisen tekijän etsimiseksi on olemassa menetelmä, joka perustuu seuraaviin tuloksiin:

(i) Jos $r_1 = q_1 r_2$, niin $r_2 = \text{syt}(r_1, r_2)$;

(ii) Jos $r_1 = q_1 r_2 + r_3$, missä $r_3 \neq 0$, niin $\text{syt}(r_1, r_2) = \text{syt}(r_2, r_3)$.

Molemmat seuraavat suoraan syt:n määritelmästä.

Eukleideen algoritmi

Lukujen r_1 ja r_2 suurin yhteinen tekijä löydetään soveltamalla toistuvasti jakoalgoritmia:

$$\begin{aligned} r_1 &= q_1 r_2 + r_3 && (r_3 < r_2), \\ r_2 &= q_2 r_3 + r_4 && (r_4 < r_3), \\ &\vdots \\ r_i &= q_i r_{i+1} + r_{i+2} && (r_{i+2} < r_{i+1}). \end{aligned}$$

Koska $r_2 > r_3 > \ldots$ päättyy prosessi äärellisen askelmäärän jälkeen hyvinjärjestysperiaatteen mukaan. Siis on olemassa sellainen i, että $r_{i+2} = 0$ ja $r_{i+1} \neq 0$. Tällöin $r_{i+1} = \text{syt}(r_1, r_2)$.

Esimerkki. Lasketaan $\text{syt}(612, 221)$.
Käytetään Eukleideen algoritmia:

$$\begin{aligned} 612 &= 2 \cdot 221 + 170, \\ 221 &= 1 \cdot 170 + 51, \\ 170 &= 3 \cdot 51 + 17, \\ 51 &= 3 \cdot 17. \end{aligned}$$

Siis $\text{syt}(612, 221) = 17$.

Usein kouluissa suurin yhteinen tekijä määrätään toisella tavalla. Keskeisessä asemassa ovat tällöin alkuluvut. Kaikki yhdistetyt luonnolliset luvut voidaan esittää niiden tulona. Esimerkiksi luonnollinen luku 105 on yhdistetty luku, sillä $105 = 3 \cdot 35 = 5 \cdot 21 = 7 \cdot 15$. Edelleen $35 = 5 \cdot 7$, $21 = 3 \cdot 7$ ja $15 = 3 \cdot 5$, joten luvulla 105 on esitykset $3 \cdot 5 \cdot 7$, $5 \cdot 3 \cdot 7$ ja $7 \cdot 3 \cdot 5$. Luvun 105 kaikki alkutekijät ovat jokaisessa esityksessä tarkalleen samat.
Yleisesti voidaan osoittaa:

Lause 2.5.1. *Aritmetiikan peruslause*
Jokainen luonnollinen luku $n \geq 2$ voidaan esittää täsmälleen yhdellä tavalla alkutekijöiden tulona kun tekijöiden järjestystä ei huomioida kyseessä olevassa tulossa.

Todistus. Todistus jätetään lukijalle harjoitustehtäväksi. □

3 Lukujärjestelmät

Sormilla laskeminen

Lukujärjestelmämme perustuu lukuun kymmenen mutta miksi juuri näin? Luultavasti syynä on se, että meillä on kymmenen sormea. Sormilla laskeminen on yleistä niin alkukantaisten kuin sivistyneiden kansojen keskuudessa.

Pulmatilanne syntyy kun ylitämme luvun kymmenen. Kehittyneissä yhteisöissä tämä ei tuota vaikeuksia, mutta toisin ovat asiat esimerkiksi paimentolaisilla ja alkukantaisilla kansoilla. Heiltä puuttuvat paitsi lukujen kirjalliset symbolit - numerot - myös vähänkin suurempien lukujen nimet.
Miten he pystyvät sitten selvittämään esimerkiksi karjansa pääluvun? Tämä ei ole ongelma. Se voi tapahtua esimerkiksi seuraavalla tavalla. Laskija koskettaa vuoron perään jokaista elikkoa sormellaan, jonka tämän jälkeen kou- kistaa. Kun kaikki sormet on koukistettu, hän ottaa apumiehen ja koukistaa tältä yhden sormen, avaa kätensä ja jatkaa toimitusta. Kun apumiehen sormet on koukistettu, otetaan toinen apumies jne. Jos laumassa on esimerkiksi 3783 elikkoa, on kolmannella apumiehellä koukussa kolme sormea, toisella seitsemän, ensimmäisellä kahdeksan ja laskijalla jälleen kolme. Numeroita ei tunneta, ei edes lukujen nimiä, mutta silti tulos on kaikille selvä.

Edellä esitetty ei ole pelkästään ajatusleikki. On melko varmaa, että jotkut paimentolaisheimot ovat menetelleet juuri edellä kuvatulla tavalla. Mahdollisesti vielä tänäkin päivänä toimitaan joissakin yhteisöissä samoin.

Kymmenjärjestelmä

Ajatellaan nyt tilannetta, että karjanlaskija haluaisi tallentaa jollakin tavalla tiedon karjan suuruudesta. Kuva käsistä koukistettuine sormineen kelpaisi tietysti sellaisenaan, ja niin lieneekin tehty aikojen alussa. Eräänä päivänä joku terävä ajattelija huomaa sitten oikotien: koukistettuje sormien lukumäärä ilmaistaan numeroin $1, 2, \ldots, 9$ (tai joillakin muilla symboleilla) ja kunkin apumiehen numeron jälkeen asetetaan ”ykkösmerkki” K (kymmenen), S (sata), T (tuhat) jne.
Karjaesimerkin luku voidaan siis lyhesti merkitä muodossa

$$3T7S8K3. \tag{1}$$

Luvussa (1) esiintyvät yksiköt ovat kantaluvun 10 potensseja:

$$K = 10 = 10^1, S = 10^2, T = 10^3 \ldots,$$

joten luku (1) voidaan esittää myös muodossa

$$3 \cdot 10^3 + 7 \cdot 10^2 + 8 \cdot 10 + 3$$

eli kantaluvun 10 *potenssisummana*.

Kymmenjärjestelmämme on kehittynyt suunnilleen edellä kuvatulla tavalla. Kyseessä ei kuitenkaan vielä ole nykyinen *kymmenkantainen* merkintätapa.

Paikkajärjestelmä

Arabialaisten matemaatikkojen ansiosta merkinnässä (1) yksiköt (kymmenen potenssit) on kirjoitettu valmiiksi vasemmalta oikealle. Jos yksikkömerkinnät jätetään pois, ilmoittaa jokaisen luvun numeron *sijainti luvussa*, mitä lukuyksiköä se esittää. Soveltamalla tätä merkintää *paikkajärjestelmään*, saadaan lukua (1) tuttuun muotoon 3783, missä numerot vasemmalta oikealle esittävät tuhansia, satoja, kymmeniä ja ykkösiä.

Eräs tärkeä seikka on kuitenkin huomioitava. Jos luvussa (1) ei olisi satoja lainkaan, ei lukua voitaisi merkitä 383, koska tällöin kolmonen ilmoittaisi satoja eikä tuhansia. Vasta luvun 0 käyttöönotto (alunperin intialaisten ja arabialaisten toimesta) tekee paikkajärjestelmän virheettömän käytön täysin mahdolliseksi.

3.1 Siirtyminen järjestelmästä toiseen

Luvun 10 sijasta kantaluvuksi voidaan valita mikä tahansa yhtä suurempi luonnollinen luku. Miksei luku 1 kelpaa?

Luonnollisen luvun n k-kantainen ($k \geq 2$) esitys saadaan jakoyhtälöä (lause 2.4.1) soveltamalla.

Jakoyhtälön mukaan

$$n = q_0 k + r_0, 0 \leq r_0 \leq k - 1$$

Jos $q_0 < k$, niin $n = q_0 k + r_0$,
muulloin

$$q_0 = q_1 k + r_1, 0 \leq r_1 \leq k - 1.$$

Jos $q_1 < k$, niin $n = q_1 k^2 + r_1 k + r_0$.

Jatkamalla kuten edellä saadaan äärellisen askelmäärän jälkeen luvulle n k-kantainen esitys:

$$n = r_t k^t + r_{t-1} k^{t-1} + \ldots + r_1 k + r_0,$$

missä $r_t \neq 0$, $0 \leq r_i \leq k-1$, $i = 0, 1, \ldots, t$
Sitä voidaan merkitä myös seuraavasti:

$$n = (r_t r_{t-1} \ldots r_0)_k.$$

Esimerkki. Esimerkkejä kantamuunnoksista.

3.2 Laskutoimitukset

Edellä tarkasteltujen lukumerkintöjen käyttöönotto on osaltaan helpottanut laskutoimituksia.
Tarkastellaan lukujen 238 ja 35 yhteenlaskua. Luvut voidaan esittää muodossa

$$238 = 2 \cdot 10^2 + 3 \cdot 10 + 8 \text{ ja } 35 = 3 \cdot 10 + 5$$

Lasketaan ensin yhteen ykköset $8+5 = 13 = 10+3$. Näin ollen kun kymmenet lasketaan yhteen, täytyy summaan lisätä vielä yksi: $3+3+1 = 7$. Vastaavasti kun lasketaan yhteen sadat, saadaan $2 + 0 = 2$.
Näin ollen summana on 273.
Lasku voidaan suorittaa myös allekkain seuraavasti:

$$\begin{array}{cccc} & & {\scriptstyle 1} & \\ & 2 & 3 & 8 \\ + & & 3 & 5 \\ \hline & 2 & 7 & 3 \end{array}$$

Vastaavasti voidaan laskea minkä tahansa kannan lukuja yhteen.
Esimerkiksi olkoot yhteenlaskettavat $1423_5 = 1 \cdot 5^3 + 4 \cdot 5^2 + 2 \cdot 5 + 3$ ja $120_5 = 1 \cdot 5^2 + 2 \cdot 5$. Nämä voidaan laskea allekkain kuten edellä:

$$\begin{array}{ccccc} & {\scriptstyle 1} & & & \\ & 1 & 4 & 2 & 3_5 \\ + & & 1 & 2 & 0_5 \\ \hline & 2 & 0 & 4 & 3_5 \end{array}$$

Vähennyslasku toimii vastaavasti. Tarkastellaan esimerkkinä 5-kantaisen luvun 335_5 vähentämistä luvusta 1020_5:

$$\begin{array}{ccccc} & & {\scriptstyle 4} & {\scriptstyle 11} & {\scriptstyle 10} \\ & 1 & 0 & 2 & 0_5 \\ - & & 3 & 3 & 3_5 \\ \hline & & 1 & 3 & 2_5 \end{array}$$

Tarkastellaan kertolaskua esimerkkien avulla.
Käytetään hyväksi luvun potenssisummaesitystä. Esimerkiksi tulo $126 \cdot 311$

voidaan esittää seuraavalla tavalla:

$$\begin{aligned}126 \cdot 311 &= (1 \cdot 10^2 + 2 \cdot 10 + 6) \cdot 311 = 1 \cdot 311 \cdot 10^2 + 2 \cdot 311 \cdot 10 + 6 \cdot 311 \\ &= 1 \cdot 311 \cdot 10^2 + 2 \cdot 311 \cdot 10 + 6 \cdot (3 \cdot 10^2 + 1 \cdot 10 + 1) \\ &= 31100 + 6220 + 18 \cdot 10^2 + 6 \cdot 10 + 6 = 31100 + 6220 + 1866 \\ &= 39186.\end{aligned}$$

Vastaava allekkainlasku on:

$$\begin{array}{cccccc} & & & 3 & 1 & 1 \\ & & \cdot & 1 & 2 & 6 \\ \hline & & 1 & 8 & 6 & 6 \\ & & 6 & 2 & 2 & \\ + & 3 & 1 & 1 & & \\ \hline & 3 & 9 & 1 & 8 & 6 \end{array}$$

Lasketaan toisena esimerkkinä kahden binääriluvun 1110_2 ja 1101_2 tulo. Tulo kymmenjärjestelmässä on seuraava:

$$1110_2 \cdot 1101_2 = (2^3 + 2^2 + 2)(2^3 + 2^2 + 1) = 14 \cdot 13 = 182.$$

Vastaavasti suoraan laskemalla allekkain saadaan

$$\begin{array}{cccccccc} & & & & 1 & 1 & 0 & 1 \\ & & & \cdot & 1 & 1 & 1 & 0 \\ \hline & & & 1 & 1 & 0 & 1 & 0 \\ & & 1 & 1 & 0 & 1 & & \\ + & 1 & 1 & 0 & 1 & & & \\ \hline 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0_2 \end{array}$$

4 Kokonaisluvut

Kappaleessa 2.3 määriteltiin luonnollisten lukujen m ja n erotus $m-n$, joka on määritelty ainoastaan, kun $m \geq n$. Esimerkiksi erotusta $2-7$ ei ole määritelty, joten täytyy ottaa käyttöön negatiiviset luvut.

Lapsille negatiiviset luvut esitetään usein lukusuoran avulla. Luku 0 sijoitetaan origoon, luku 1 mittayksikön päähän oikealle, luku 2 mittayksikön päähän oikealle luvusta 1 jne.
Negatiiviset luvut sijoitetaan vastaavalla tavalla origon vasemmalle puolelle.

Näin saatu lukujoukko, jota sanotaan kokonaislukujen joukoksi, on luonnollisten lukujen laajennus joka koostuu luonnollisista luvuista sekä luvuista muotoa $-n$, missä $n \in \mathbb{N}$.

Menetellään tässä kuitenkin toisin.
Liitetään joukkoon $\mathbb{N}_0$ negatiiviset luvut luonnollisten lukujen erotusten avulla. Huomattava on, että sama luku voidaan esittää eri tavoin tällaisena erotuksena. Esimerkiksi $-1 = 0-1 = 1-2 = 2-3 = \ldots$
Sijoitetaan näin kutakin lukua vastaavat lukuparit samaan "luokkaan", jolloin saadaan kokonaisluvuille täsmällisempi määritelmä.
Määritellään ensin kuitenkin tarvittavia käsitteitä.

Epätyhjien joukkojen A ja B *tulojoukko* eli karteesinen tulo on

$$A \times B = \{(a,b) \mid a \in A \text{ ja } b \in B\}.$$

Siis $A \times B$ koostuu kaikista niistä järjestetyistä pareista (a,b), missä $a \in A$ ja $b \in B$.

Olkoot A ja B epätyhjiä joukkoja. Joukon $A \times B$ osajoukko R sanotaan joukkojen A ja B *relaatioksi*.
Jos $A = B$, niin osajoukkoa $R \subseteq A \times B$ sanotaan relaatioksi joukossa A ja mikäli (x,y) kuuluu tähän osajoukkoon, niin merkitään xRy ja sanotaan, että x on relaatiossa y:n kanssa.

Esimerkki. Olkoot $X = \{1,2,3,4,5\}$, $Y = \{6,7,8,9,10\}$ ja

$$R = \{(1,6),(1,7),(1,8),(1,9),(1,10),(2,6),(2,8),\\ (2,10),(3,6),(3,9),(4,8),(5,10)\},$$

joten xRy jos ja vain jos x on y:n tekijä.

Erityisen tärkeä relaatio tässä yhteydessä on:

Määritelmä 4.0.1. *Relaatio R joukossa $A \neq \emptyset$ on* ekvivalenssirelaatio*, jos kaikilla $x, y, z \in A$*

(i) xRx *(refleksiivisyys),*

(ii) $xRy \Rightarrow yRx$ *(symmetrisyys),*

(iii) $xRy, yRz \Rightarrow xRz$ *(transitiivisuus).*

Esimerkki. 1) Olkoon A="Toppilan yläasteen oppilaat". Määritellään relaatio $\sim$ joukossa A asettamalla

$$x \sim y \Leftrightarrow x \text{ on samalla luokalla kuin } y.$$

2) Luonnollisten lukujen yhteydessä määritelty järjestys $\geq$ on relaatio joukossa $\mathbb{N}_0$, joka on refleksiivinen ja transitiivinen mutta ei symmetrinen.

Määritelmä 4.0.2. *Jos $a \in A$ ja R on ekvivalenssirelaatio joukossa A, niin joukkoa*

$$[a] = \{x \in A \mid xRa\}$$

sanotaan a:n määräämäksi ekvivalenssiluokaksi *ja a:ta kyseisen luokan edustajaksi.*

Esimerkki. Aiemmassa esimerkissä $[a] = 7B$, jos a on luokan $7B$ opppilas.

Voidaan osoittaa, että ekvivalenssirelaatio jakaa annetun joukon pareittain erillisiin ekvivalenssiluokkiin. Kukin alkio kuuluu täsmälleen yhteen luokkaan.
Käytetään tätä hyväksi seuraavassa.

4.1 Kokonaislukujen määrittely

Aiemmin kappaleessa 2.3 todettiin että erotus $m - n$, missä $m, n \in \mathbb{N}_0$ on määritelty, kun $m \geq n$. Edelleen, jos $m, n, r, s \in \mathbb{N}_0$ ja $m \geq n$, $r \geq s$, niin

$$m - n = r - s \Leftrightarrow m + s = r + n.$$

Huomaa, että oikea puoli on hyvin määritelty ilman rajoituksia lukuihin $m, n, r, s \in \mathbb{N}_0$. Tämä antaa aiheen määritellä erotus myös tapauksessa $m < n$.

Määritellään relaatio $\sim$ joukossa $\mathbb{N}_0$ asettamalla

$$(m, n) \sim (r, s) \Leftrightarrow m + s = n + r. \tag{2}$$

Kyseessä on itseasiassa ekvivalenssirelaatio. Kokonaisluvut voidaan määritellä ekvivalenssirelaatioina.

Määritelmä 4.1.1. *Olkoon $\sim$ kaavalla (2) määritelty ekvivalenssirelaatio joukossa $\mathbb{N}_0$. Ekvivalenssiluokkien $[(m, n)]$, missä $m, n \in \mathbb{N}_0$, muodostamaa joukkoa sanotaan kokonaislukujen joukoksi $\mathbb{Z}$. Ekvivalenssiluokkia sanotaan kokonaisluvuiksi.*

4.2 Kokonaislukujen yhteen- ja kertolasku

Kokonaislukujen yhteenlasku määritellään seuraavasti.

Määritelmä 4.2.1. *Olkoot $[(m, n)], [(r, s)] \in \mathbb{Z}$. Määritellään edellä mainittujen lukujen yhteenlasku asettamalla*

$$[(m, n)] + [(r, s)] = [(m + r, n + s)]$$

Intuitio: jos yllä olevassa määritelmässä ajattelee ekvivalenssiluokkia $[(m, n)]$ ja $[(r, s)]$ erotuksina $m - n$ ja $r - s$, niin yhteenlaskun määritelmä voidaan kirjoittaa muodossa $(m - n) + (r - s) = (m + r) - (n + s)$.

Ei ole itsestään selvää, että yhteenlasku on hyvin määritelty eli että se on riippumaton ekvivalenssiluokkien edustajien valinnasta.

Jos $(m, n) \sim (m', n')$ eli $m + n' = n + m'$ ja $(r, s) \sim (r', s')$ eli $r + s' = r' + s$,

niin $(m+r)+(n'+s') = (n+s)+(m'+r')$ eli $(m+r, n+s) \sim (m'+r', n'+s')$,

joten $[(m + r, n + s)] = [(m' + r', n' + s')]$.

Yhteenlasku on siis hyvin määritelty.

Yksinkertaistetaan merkintöjä ekvivalenssiluokille asettamalla
$[(m, n)] = [m, n]$.

Kokonaislukujen kertolasku määritellään seuraavasti:

Määritelmä 4.2.2. *Olkoot $[m, n], [r, s] \in \mathbb{Z}$. Edellä mainittujen lukujen kertolasku määritellään asettamalla*

$$[m, n] \cdot [r, s] = [mr + ns, ms + nr].$$

Intuitio: jos yllä olevia ekvivalenssiluokkia ajattelee erotuksina $m-n$ ja $r-s$, niin kertolaskun määritelmä voidaan kirjoittaa muodossa $(m-n)\cdot(r-s) = (mr+ns)-(ms+nr)$.

Kuten yhteenlaskun tapauksessa, voidaan osoittaa, että kertolasku on hyvin määritelty (HT).

Kokonaislukujen yhteen- ja kertolasku toteuttavat seuraavat laskusäännöt.

Lause 4.2.1. *Olkoot* $[m,n],[p,q],[r,s] \in \mathbb{Z}$. *Yhteen- ja kertolaskulle pätee:*

(1) $([m,n]+[p,q])+[r,s] = [m,n]+([p,q]+[r,s])$;

(2) $[m,n]+[p,q] = [p,q]+[m,n]$;

(3) $([m,n]\cdot[p,q])\cdot[r,s] = [m,n]\cdot([p,q]\cdot[r,s])$;

(4) $[m,n]\cdot[p,q] = [p,q]\cdot[m,n]$;

(5) $[m,n]\cdot([p,q]+[r,s]) = [m,n]\cdot[p,q]+[m,n]\cdot[r,s]$;

(6) On olemassa nolla-alkio $0 \in \mathbb{Z}$, *jolle* $a+0=a$ *kaikilla* $a \in \mathbb{Z}$;

(7) Jokaisella $a \in \mathbb{Z}$ *on vasta-alkio* $-a \in \mathbb{Z}$, *jolle* $a+(-a)=0$;

(8) On olemassa ykkösalkio $1 \in \mathbb{Z}$, *jolle* $1a = a$ *kaikilla* $a \in \mathbb{Z}$.

Todistus. Kohdat (1) - (5) seuraavat suoraan yhteen- ja kertolaskun määritelmästä ja luonnollisten lukujen vastaavien laskutoimitusten ominaisuuksista.

(6) Nolla-alkio on $[0,0]$, sillä $[m,n]+[0,0] = [m+0,+0] = [m,n]$.

(7) Luvun $[m,n]$ vastaluku on $[n,m]$, sillä

$$[m,n]+[n,m] = [m+n,n+m] = [m+n,m+n] = [0,0].$$

(8) Ykkösalkio on $[1,0]$, sillä

$$[1,0]\cdot[m,n] = [1m+0\cdot n, 1n+0\cdot m] = [m,n].$$

□

Milloin alkiot ovat sitten negatiivisia ja milloin positiivisia?

4.3 Kokonaislukujen järjestys

Kokonaisluku on joko positiivinen, negatiivinen tai nolla. Tämä määritellään seuraavasti:

1) $[m,n]$ on *positiivinen* ja merkitään $[m,n] \in \mathbb{Z}_+$, jos $m > n$ eli jos $m = n+p$ ja $0 \neq p \in \mathbb{N}_0$.
   Edellisestä seuraa, että positiivinen kokonaisluku $[m,n]$ on muotoa $[p,0]$, missä $0 \neq p \in \mathbb{N}_0$ määräytyy yksikäsitteisesti luvuista $m,n \in \mathbb{N}_0$.

2) $[m,n]$ on *negatiivinen* ja merkitään $[m,n] \in \mathbb{Z}_-$, jos $m < n$.
   Lauseen 4.2.1 kohdan (7) mukaan tämä voidaan ilmaista myös sanomalla, että $-[m,n] = [n,m]$ on positiivinen. Edelleen kohdan 1) mukaan negatiivinen kokonaisluku voidaan yhdellä tavalla lausua muodossa $[0,q]$, missä $0 \neq q \in \mathbb{N}_0$.

3) Kokonaisluku $[m,n]$ on nolla, jos $m = n$. Nolla voidaan yhdellä tavalla lausua muodossa $[0,0]$.

Nyt voidaan määritellä kokonaislukujen järjestys.

Määritelmä 4.3.1. *Olkoot $[m,n],[p,q] \in \mathbb{Z}$. Aito järjestys $<$ määritellään asettamalla*

(J1) $[m,n] < [p,q]$, *jos* $[p,q] - [m,n] \in \mathbb{Z}_+$ *ts.* $[p+n, q+m] \in \mathbb{Z}_+$.

Lisäksi asetetaan

(J2) $[m,n] \leq [p,q]$, *jos (J1) on voimassa tai* $[m,n] = [p,q]$,

(J3) $[m,n] > [p,q]$, *jos* $[p,q] < [m,n]$,

(J4) $[m,n] \geq [p,q]$, *jos* $[p,q] \leq [m,n]$.

Voidaan osoittaa, että kokonaislukujen järjestykselle pätee

Lause 4.3.1. *Olkoot $[m,n],[p,q] \in \mathbb{Z}$. Tällöin täsmälleen yksi seuraavista ehdoista on voimassa:*

$$[m,n] > [p,q], [m,n] = [p,q] \text{ tai } [m,n] < [p,q].$$

Todistus. Seuraa suoraan kokonaislukujen määritelmästä ja $\mathbb{N}_0$:n vastaavasta ominaisuudesta. □

4.4 Luonnollisten lukujen ja kokonaislukujen välinen yhteys

Edellä määritelty kokonaislukujen joukko ei ole luonnollisen lukujoukon $\mathbb{N}_0$ laajennus siinä mielessä kuin ehkä olisi toivottu, sillä $\mathbb{Z}$ koostuu järjestettyjen parien $(m, n) \in \mathbb{N}_0 \times \mathbb{N}_0$ määräämistä ekvivalenssiluokista. Osoittautuu, että luonnolliset luvut voidaan samaistaa ei-negatiivisten kokonaislukujen kanssa. Ei-negatiivisten kokonaislukujen joukolle käytetään merkintää $\mathbb{Z}_+^0 (= \mathbb{Z}_+ \cup [0, 0])$. Samaistaminen tarkoittaa sitä, että molemmat lukujoukot ovat suljettuja yhteen- ja kertolaskun suhteen ja että aritmetiikka ja järjestys säilyy samaistuksessa.

Tarkastellaan mitä samaistuksella tarkkaan ottaen tarkoitetaan. Palautetaan ensin mieleen *bijektion* käsite. Olkoot A ja B epätyhjiä joukkoja ja $f : A \to B$ funktio. Oletetaan, että funktion f määrittelyjoukko on A. Sanotaan, että f on bijektio, jos

(i) Jokaista $y \in B$ kohti on olemassa sellainen $x \in A$, että $f(x) = y$ (surjektio);

(ii) Kaikilla $x, y \in A$ ehdosta $f(x) = f(y)$ seuraa, että $x = y$ (injektio).

Edellisen kappaleen alussa todettiin, että jokainen $\mathbb{Z}_+^0$:n alkio voidaan täsmälleen yhdellä tavalla ilmaista muodossa $[n, 0], n \in \mathbb{N}_0$.

Tästä seuraa, että $\mathbb{Z}_+^0$ on *suljettu* yhteen- ja kertolaskun suhteen, sillä

1) $[m, 0] + [n, 0] = [m + n, 0] \in \mathbb{Z}_+^0$ kaikilla $m, n \in \mathbb{N}_0$,

2) $[m, 0] \cdot [n, 0] = [mn, 0] \in \mathbb{Z}_+^0$ kaikilla $m, n \in \mathbb{N}_0$.

Lisäksi $\mathbb{Z}_+^0$:n nolla-alkio on $[0, 0]$ ja ykkösalkio $[1, 0]$ (vertaa vastaavat $\mathbb{N}_0$:ssa).

Muodostetaan funktio $f : \mathbb{N}_0 \to \mathbb{Z}_+^0$ asettamalla $f(n) = [n, 0]$ kaikilla $n \in \mathbb{N}_0$. Funktiolla f on seuraavat ominaisuudet:

1) Funktio f on bijektio, sillä

   i) jokaista $[n, 0] \in \mathbb{Z}_+^0$ kohti on olemassa sellainen $x \in \mathbb{N}_0$, että $f(x) = [n, 0]$ (nimittäin $x = n$),

   ii) jos $f(m) = f(n)$, niin $m = n$
   (sillä $[m, 0] = [n, 0]$ eli $(m, 0) \sim (n, 0)$ eli $m + 0 = 0 + n$);

2) Funktio f säilyttää yhteen- ja kertolaskun seuraavassa mielessä:

$$f(m+n) = [m+n, 0] = [m, 0] + [n, 0] = f(m) + f(n),$$
$$f(mn) = [mn, 0] = [m, 0][n, 0] = f(m)f(n);$$

3) $\mathbb{N}_0$:n nolla-alkio ja ykkösalkio kuvautuvat $\mathbb{Z}_+^0$:n vastaaviksi:

$$f(0) = [0, 0] \text{ ja } f(1) = [1, 0];$$

4) Funktio f säilyttää järjestyksen $\leq$ määritelmän 4.3.1 mukaan:
jos $m \leq n$, niin $f(m) = [m, 0] \leq [n, 0] = f(n)$, sillä $[n, 0] - [m, 0] = [n + 0, 0 + m] = [n, m] \in \mathbb{Z}_+^0$.

Täten $\mathbb{N}_0$ ja $\mathbb{Z}_+^0$ ovat laskutoimitusten ja järjestyksen suhteen oleellisesti samat (isomorfiset), joten $\mathbb{N}_0$:n ja $\mathbb{Z}_+^0$:n alkiot voidaan samaistaa ja merkitä $n = [n, 0]$. Vastaavasti negatiiviselle alkioille $[0, n] \in \mathbb{Z}_-$ voidaan käyttää merkintää $-n$, missä $n \in \mathbb{N}$.

Samaistuksen jälkeen $\mathbb{Z}$ on $\mathbb{N}_0$:n laajennus.

4.5 Kokonaislukujen jaollisuus

Kokonaislukujen jaollisuus voidaan määritellä samalla tavalla kuin luonnollisille luvuille.

Määritelmä 4.5.1. *Jos $m, n \in \mathbb{Z}$ ja $n \neq 0$ ja jos on olemassa sellainen luku $k \in \mathbb{Z}$, että $m = kn$, niin sanotaan, että n on luvun m tekijä tai että n jakaa luvun m ja merkitään $n \mid m$.*

Jos $n \mid m$, eli on olemassa sellainen $k \in \mathbb{Z}$, että $m = kn$, niin $m = (-k)(-n)$, joten myös luvun n vastaluku on tekijä. Näin ollen jokaisella luvulla on aina myös positiivinen tekijä (ainakin luku 1).

Edellisen huomion mukaan syt voidaan määritellä seuraavasti:

Määritelmä 4.5.2. *Jos $m, n \in \mathbb{Z}$ ja ainakin toinen luvuista m ja n on erisuuri kuin 0, niin lukua $d > 0$ sanotaan lukujen m ja n suurimmaksi yhteiseksi tekijäksi ja merkitään $d = \text{syt}(m, n)$, jos seuraavat ehdot täyttyvät:*

(i) $d \mid m$ *ja* $d \mid n$*;*

(ii) Jos $k \mid m$ *ja* $k \mid n$*, niin* $k \mid d$*.*

Edelleen jakoalgoritmi voidaan todistaa myös kokonaisluvuille.

Lause 4.5.1 (Jakoalgoritmi)**.** *Jos $a, b \in \mathbb{Z}, b \neq 0$, niin on olemassa sellaiset yksikäsitteiset määrätyt $q, r \in \mathbb{Z}$, että*

$$a = qb + r, 0 \leq r < |b|, \tag{3}$$

missä

$$|b| = \begin{cases} b & , \textit{jos } b > 0; \\ -b & , \textit{jos } b < 0; \\ 0 & , \textit{jos } b = 0, \end{cases}$$

on luvun b itseisarvo.

Esimerkki. Tarkastellaan esimerkkinä lukujen -6 ja 9 syt:n määräämistä ja merkitään $d = \text{syt}(-6, 9)$. Koska $d \mid m$ jos ja vain jos $d \mid -m$, niin $d = \text{syt}(6, 9)$.
Määrätään d Eukleideen algoritmilla:

$$9 = 1 \cdot 6 + 3,$$
$$6 = 2 \cdot 3.$$

Siis $d = 3$.
Toisaalta ensimmäisen yhtälön mukaan $3 = 9 - 1 \cdot 6 = 1 \cdot 9 + 1 \cdot (-6)$, joten d voidaan ilmaista muodossa $d = x \cdot 9 + y \cdot (-6)$, missä $x, y \in \mathbb{Z}$. Tämä pätee myös yleisesti.

Lause 4.5.2. *Jos $a, b \in \mathbb{Z}$ ja ainakin toinen luvuista a ja b on nollasta eroava, niin $t = \text{syt}(a, b)$ voidaan esittää muodossa*

$$t = ax + by, \ \textit{missä } x, y \in \mathbb{Z}.$$

Todistus. Luennoilla. □

Esimerkki.

5 Rationaaliluvut

Määritellään rationaaliluvut samaan tapaan kuin kokonaisluvut.
Laajennetaan lukujoukkoa $\mathbb{Z}$ niin, että osamäärät $\frac{m}{n}$ tulevat määritellyiksi. Tätä varten olkoon S järjestettyjen parien (m, n), missä $m, n \in \mathbb{Z}$ ja $n \neq 0$, muodostama joukko. Määritellään joukossa S relaatio $\sim$ asettamalla

$$(m, n) \sim (p, q) \Leftrightarrow mq = np. \tag{4}$$

Intuitio: kaavaa (4) voi verrata rationaalilukujen ominaisuuteen $\frac{m}{n} = \frac{p}{q} \Leftrightarrow mq = np$.

Rationaalilukujen joukko $\mathbb{Q}$ määritellään relaation $\sim$ määräämien ekvivalenssiluokkien muodostamana joukkona ja ekvivalenssiluokkia $[m, n] \in \mathbb{Q}$ sanotaan *rationaaliluvuiksi*.

Rationaalilukujen joukossa määritellään yhteen- ja kertolasku seuraavasti:

Määritelmä 5.0.3. *Olkoot $[m, n], [p, q] \in \mathbb{Q}$. Yhteen- ja kertolasku määritellään asettamalla*

$$[m, n] + [p, q] = [mq + np, nq], \tag{5}$$

$$[m, n] \cdot [p, q] = [mp, nq]. \tag{6}$$

Jos ekvivalenssiluokkaa $[m, n]$ ajattelee osamääränä $\frac{m}{n}$, niin (5) on muotoa

$$\frac{m}{n} + \frac{p}{q} = \frac{mq + np}{nq}.$$

Vastaavasti (6) voidaan kirjoittaa muodossa

$$\frac{m}{n} \cdot \frac{p}{q} = \frac{mp}{nq}.$$

Huomautus. Kaavojen (5) ja (6) oikeat puolet ovat rationaalilukuja, sillä $n \neq 0$ ja $q \neq 0 \Rightarrow nq \neq 0$.

Voidaan osoittaa, että kaavojen (5) ja (6) määrittelemät summa ja tulo ovat hyvin määriteltyjä.

Lause 5.0.3. *Olkoot $[m, n], [p, q], [r, s] \in \mathbb{Q}$. Yhteen- ja kertolaskulle pätee:*

(1) $([m, n] + [p, q]) + [r, s] = [m, n] + ([p, q] + [r, s])$;

(2) $[m,n]+[p,q]=[p,q]+[m,n]$*;*

(3) $([m,n]\cdot[p,q])\cdot[r,s]=[m,n]\cdot([p,q]\cdot[r,s])$*;*

(4) $[m,n]\cdot[p,q]=[p,q]\cdot[m,n]$*;*

(5) $[m,n]\cdot([p,q]+[r,s])=[m,n]\cdot[p,q]+[m,n]\cdot[r,s]$*;*

(6) On olemassa nolla-alkio $0\in\mathbb{Q}$*, jolle* $a+0=a$ *kaikilla* $a\in\mathbb{Q}$*;*

(7) Jokaisella $a\in\mathbb{Q}$ *on vasta-alkio* $-a\in\mathbb{Q}$*, jolle* $a+(-a)=0$*;*

(8) On olemassa ykkösalkio $1\in\mathbb{Q}$*, jolle* $1\cdot a=a$ *kaikilla* $a\in\mathbb{Q}$*;*

(9) Jokaisella $a\in\mathbb{Q}, a\neq 0$ *on olemassa* käänteisalkio*, merkitään* $a^{-1}\in\mathbb{Q}$*, jolle* $a\cdot a^{-1}=1$*.*

Todistus. Kohdat (1) - (5) seuraavat rationaalilukujen määritelmästä ja kokonaislukujen vastaavista ominaisuuksista.

Nolla-alkio on $[0,1]$ ja ykkösalkio $[1,1]$ (Totea laskemalla).

Yhtälöllä $[m,n]\cdot[x,y]=[1,1]$ on ratkaisu, kun $[m,n]\neq[0,1]$ eli kun $m\neq 0$. Ratkaisu on $[n,m]$. Tämä on rationaaliluku, sillä $m\neq 0$. Näin ollen luvun $[m,n]\neq[0,1]$ käänteisalkio on $[n,m]$. □

5.1 Rationaalilukujen järjestys

Määritellään järjestys rationaalilukujen joukossa. Rationaalilukua $[m,n]$ sanotaan *positiiviseksi* ja merkitään $[m,n]\in\mathbb{Q}_+$, jos $mn>0$. Voidaan todeta, että tämä määritelmä on ekvivalenssiluokan $[m,n]$ edustajan valinnasta riippumaton. Lisäksi edustaja (m,n) voidaan valita niin, että $m>0$ ja $n>0$. Vastaavasti rationaaliluku $[m,n]$ on *negatiivinen* ja merkitään $[m,n]\in\mathbb{Q}_-$, jos $mn<0$.

Merkitään $\mathbb{Q}_+^0=\mathbb{Q}_+\cup[0,1]$ ja $\mathbb{Q}_-^0=\mathbb{Q}_-\cup[0,1]$. Tällöin $\mathbb{Q}_+^0$ on *suljettu* yhteenlaskun suhteen, sillä jos $[m,n],[p,q]\in\mathbb{Q}_+^0$, niin $mn,pq\geq 0$. Voidaan olettaa, että $m,p\geq 0$ ja $n,q>0$, jolloin

$$[m,n]+[p,q]=[mq+np,nq]\in\mathbb{Q}_+^0.$$

Määritellään nyt rationaalilukujen järjestys seuraavasti:

Määritelmä 5.1.1. *(J1)* $[m,n]\leq[p,q]$*, jos* $[p,q]-[m,n]\in\mathbb{Q}_+^0$*.*

Vastaavasti määritellään järjestykset $\geq,<$ *ja* $>$ *asettamalla*

(J2) $[m,n] \geq [p,q] \Leftrightarrow [p,q] \leq [m,n]$,

(J3) $[m,n] < [p,q] \Leftrightarrow [p,q] - [m,n]$ *on positiivinen,*

(J4) $[m,n] > [p,q] \Leftrightarrow [p,q] < [m,n]$.

Voidaan osoittaa, että rationaalilukujen järjestykselle pätee:

Lause 5.1.1. *Olkoot* $[m,n], [p,q] \in \mathbb{Q}$. *Tällöin täsmälleen yksi seuraavista ehdoista on voimassa:*

$$[m,n] > [p,q], [m,n] = [p,q] \text{ tai } [m,n] < [p,q].$$

Tarkastellaan seuraavassa missä mielessä rationaalilukujen joukko voidaan tulkita joukon $\mathbb{Z}$ laajennukseksi.

5.2 Kokonaiset rationaaliluvut ja kokonaisluvut

Jos rationaaliluvussa $[m,n]$ luku m on jaollinen luvulla n, eli on olemassa sellainen $p \in \mathbb{Z}$, että $m = pn$, lukua $[m,n]$ sanotaan *kokonaiseksi* rationaaliluvuksi. Se voidaan tämälleen yhdellä tavalla esittää muodossa $[p,1]$.

Kokonaisten rationaalilukujen joukko (merkitään $\mathbb{Q}_1$) on *suljettu* yhteen- ja kertolaskun suhteen ja ne toteuttavat lauseen 5.0.3 ominaisuudet (1) - (8) (vertaa kokonaislukujen vastaavat ominaisuudet lauseessa 4.2.1).

Määritellään nyt kuvaus $f : \mathbb{Z} \to \mathbb{Q}$ asettamalla

$$f(n) = [n,1], n \in \mathbb{Z}. \tag{7}$$

Lause 5.2.1. *Kaavalla (7) määritellylle kuvaukselle* f *pätee:*

1) Funktio f *on bijektio joukolta* $\mathbb{Z}$ *joukolle* $\mathbb{Q}_1$*;*

2) Funktio f *säilyttää yhteen- ja kertolaskun seuraavassa mielessä:*

$$f(m+n) = f(m) + f(n),$$
$$f(m \cdot n) = f(m) \cdot f(n);$$

3) Joukon $\mathbb{Z}$ *nolla-alkio ja ykkösalkio kuvautuvat* $\mathbb{Q}_1$*:n vastaaviksi:*

$$f(0) = [0,1] \text{ ja } f(1) = [1,1];$$

4) Funktio f *säilyttää järjestyksen* $<$*, eli jos* $m < n$*, niin* $f(m) < f(n)$.

Todistus. Todistus jätetään lukijalle harjoitustehtäväksi. □

Täten $\mathbb{Z}$ ja $\mathbb{Q}_1$ ovat oleellisesti samat (isomorfiset) ja samaistamalla alkiot n ja $[n, 1]$ saadaan $\mathbb{Q}$ tulkituksi $\mathbb{Z}$:n laajennuksena.

Todistetaan vielä seuraava lause rationaalilukujen esittämisestä kokonaisten rationaalilukujen avulla.

Lause 5.2.2. *Jokainen rationaaliluku $[m, n]$ voidaan esittää muodossa*

$$[m, n] = [m, 1] \cdot [n, 1]^{-1}.$$

Todistus. Koska $[m, n] \in \mathbb{Q}$, on $n \neq 0$ ja siten $[n, 1]^{-1}$ on olemassa. Lisäksi

$$[m, n] \cdot [n, 1] = [mn, n] = [m, 1].$$

□

Koska yhtälön $[n, 1] \cdot [x, y] = [m, 1]$, missä $n \neq 0$, ratkaisu $[m, n]$ on yksikäsitteinen, voidaan jokainen rationaaliluku $[m, n]$ kirjoittaa muodossa

$$[m, n] = [m, 1] \cdot [n, 1]^{-1} =: \frac{[m, 1]}{[n, 1]}.$$

Edelleen $\mathbb{Q}_1$:n ja $\mathbb{Z}$:n samaistuksen jälkeen voidaan $[m, n] \in \mathbb{Q}$ kirjoittaa tutummassa muodossa $\frac{m}{n}$.

Nyt siis $\mathbb{Z}$:n ja $\mathbb{Q}_1$:n samaistuksen jälkeen on jokainen kokonaisluku muotoa $n = \frac{n}{1}$ oleva rationaaliluku. Edelleen jokaisen rationaaliluvun $\frac{m}{n} \neq 0$ käänteisluku on $\frac{n}{m}$.

Rationaalilukujen määrittelyn mukaan $\frac{m}{n}, \frac{k}{l} \in \mathbb{Q}$ ovat yhtäsuuret jos ja vain jos $ml = kn$. Yhdellä rationaaliluvulla on siis äärettömän monta eri esitysmuotoa. Eräs niistä on kuitenkin yksikäsitteinen, nimittäin *supistettu muoto* $\frac{m}{n}$, missä $syt(m, n) = 1$.

Rationaaliluvuille a ja $b \neq 0$, voidaan määritellä *osamäärä* (mikä ei kaikille kokonaisluvuille ole mahdollista) asettamalla

$$\frac{a}{b} = a \cdot b^{-1}.$$

Voidaan todeta, että yhteen-, vähennys-, kerto- ja jakolasku ovat rajoituksetta (lukuun ottamatta nollalla jakamista) tehtävissä rationaalilukujen joukossa.

Jos a ja b ovat rationaalilukuja ja $a \neq 0$, niin yhtälöllä $ax = b$ on yksikäsitteinen ratkaisu $x = \frac{b}{a}$. Tässä mielessä rationaalilukujen joukko korjaa kokonaislukujen puutteellisuuden.

5.3 Rationaalilukujen desimaaliesitys

Aiemmin todettiin, että jokainen positiivinen rationaaliluku voidaan kirjoittaa muodossa $\frac{m}{n}$, missä m ja n ovat positiivisia kokonaislukuja (katso rationaaliluvun positiivisuuden määritelmä). Edelleen jokainen negatiivinen rationaaliluku voidaan kirjoittaa muodossa $-\frac{m}{n}$, missä $m, n > 0$.

Tarkastellaan seuraavassa positiivisia kokonaislukuja $\frac{m}{n}$, missä $m, n > 0$. Aiemmin todettiin, että rationaaliluvulla on äärettömän monta esitysmuotoa. Käytännön laskuissa tärkeimpiä ovat ne esitykset, joissa *nimittäjä* on jokin kymmenen potenssi eli $10, 100, 1000$ ja niin edelleen. Tällaisilla rationaaliluvuilla on oma merkintätapa. Tarkastellaan seuraavaksi kuinka rationaaliluvuille saadaan *desimaaliesitys*.

Jakamalla *osoittaja* m nimittäjällä n saadaan jakoyhtälön

$$m = qn + r, 0 \leq r < n,$$

avulla esitys kokonaisosa+murto-osa:

$$\frac{m}{n} = q + \frac{r}{n} = q\frac{r}{n}.$$

Jos n on luvun 10 potenssi, niin erottamalla jakojäännös r kokonaisosasta pilkulla, saadaan luvulle $\frac{m}{n}$ desimaaliesitys.

Esimerkki. $73 = 0 \cdot 100 + 73$, joten $\frac{73}{100} = 0 + \frac{73}{100} = 0,73$.

Yleisemmin olkoon $a \in \mathbb{Q}, a \geq 0$. Otetaan nyt käyttöön merkintä

$$\lfloor a \rfloor = \text{ suurin kokonaisluku, joka on pienempi tai yhtäsuuri kuin } a.$$

Tämä on lattiafunktio ja tällöin siis $\lfloor a \rfloor \leq a < \lfloor a \rfloor + 1$. Luku a voidaan nyt esittää muodossa:

$$a = \lfloor a \rfloor + \alpha_0, \text{ missä } 0 \leq \alpha_0 < 1.$$

Jos luvulla a on esitys $a = q\frac{r}{n}$, niin $\lfloor a \rfloor = q$ (kokonaisosa) ja $\alpha_0 = \frac{r}{n}$ (murto-osa).

Oletetaan, että $\alpha_0 \neq 0$. Rationaaliluku $10\alpha_0$ voidaan esittää muodossa

$$10\alpha_0 = \lfloor 10\alpha_0 \rfloor + \alpha_1, \text{ missä } 0 \leq \alpha_1 < 1.$$

Merkitään $c_1 = \lfloor 10\alpha_0 \rfloor$. Koska $0 \leq \alpha_0 < 1$, niin $0 \leq c_1 \leq 9$. Luku a voidaan kirjoittaa nyt muotoon

$$\begin{aligned} a = \lfloor a \rfloor + \alpha_0 = \lfloor a \rfloor + \frac{10\alpha_0}{10} &= \lfloor a \rfloor + \frac{\lfloor 10\alpha_0 \rfloor + \alpha_1}{10} \\ &= \lfloor a \rfloor + \frac{c_1}{10} + \frac{\alpha_1}{10}. \end{aligned} \tag{8}$$

Jos $\alpha_1 \neq 0$, niin luvun a esitystä jatketaan seuraavalla tavalla. Olkoon

$$10\alpha_1 = c_2 + \alpha_2, \text{ missä } c_2 = \lfloor 10\alpha_1 \rfloor \text{ ja } 0 \leq \alpha_2 < 1. \tag{9}$$

Tällöin $0 \leq c_2 \leq 9$ ja laventamalla viimeinen termi esityksessä (8) kymmenellä ja sijoittamalla esitys (9) viimeisen termin paikalle saadaan

$$a = \lfloor a \rfloor + \frac{c_1}{10} + \frac{c_2}{10^2} + \frac{\alpha_2}{10^2}. \tag{10}$$

Jos $\alpha_2 \neq 0$, niin jatkamalla samalla tavalla saadaan luku a muotoon

$$a = \lfloor a \rfloor + \frac{c_1}{10} + \frac{c_2}{10^2} + \frac{c_3}{10^3} + \frac{\alpha_3}{10^3},$$

missä $0 \leq c_3 = \lfloor 10\alpha_2 \rfloor \leq 9$ ja $a_3 = 10\alpha_2 - \lfloor 10\alpha_2 \rfloor$. Toistamalla edellä esitettyä menettelyä saadaan rationaaliluvulle a desimaalikehitelmä

$$a = \lfloor a \rfloor, c_1 c_2 \ldots c_i \ldots,$$

missä $c_i = \lfloor 10\alpha_{i-1} \rfloor$ ja $\alpha_{i-1} = 10\alpha_{i-2} - \lfloor 10\alpha_2 \rfloor$.

Esimerkki.

Päättymätön jaksollinen desimaaliesitys

Edellisen esimerkin rationaaliluvut olivat erityistä tyyppiä, koska niiden desimaaliesitykset olivat päättyviä. On myös sellaisia rationaalilukuja, joiden desimaaliesitykset jatkuvat loputtomiin. Esimerkiksi

$$\frac{1}{3} = 0,333\ldots \quad \text{ja} \quad \frac{5}{11} = 0,454545\ldots$$

Nämä saadaan jakokulmassa laskemalla:

$$
\begin{array}{r|llll}
 & 0, & 3 & 3 & \ldots \\
\hline
3 & 1, & 0 & 0 & \\
 & -\ & 9 & & \\
\cline{2-3}
 & & 1 & 0 & \\
 & & -\ & 9 & \\
\cline{3-4}
 & & & 1 & 0
\end{array}
$$

ja

$$
\begin{array}{r|llllll}
 & 0, & 4 & 5 & 4 & 5 & \ldots \\
\hline
11 & 5, & 0 & 0 & 0 & 0 & \\
 & -4 & 4 & & & & \\
\cline{2-3}
 & & 6 & 0 & & & \\
 & & -5 & 5 & & & \\
\cline{3-4}
 & & & 5 & 0 & & \\
 & & & -4 & 4 & & \\
\cline{4-5}
 & & & & 6 & 0 &
\end{array}
$$

Osoitetaan, että päättymätön desimaaliesitys on jaksollinen. Tarkastellaan tätä esimerkin avulla suorittamalla jakolasku $2/7$ jakokulmassa:

$$
\begin{array}{r|llllllll}
 & 0, & 2 & 8 & 5 & 7 & 1 & 4 & \\
\hline
7 & 2, & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 & -1 & 4 & & & & & & \\
\cline{2-3}
 & & 6 & 0 & & & & & \\
 & & -5 & 6 & & & & & \\
\cline{3-4}
 & & & 4 & 0 & & & & \\
 & & & -3 & 5 & & & & \\
\cline{4-5}
 & & & & 5 & 0 & & & \\
 & & & & -4 & 9 & & & \\
\cline{5-6}
 & & & & & 1 & 0 & & \\
 & & & & & -\ & 7 & & \\
\cline{6-7}
 & & & & & & 3 & 0 & \\
 & & & & & & -2 & 8 & \\
\cline{7-8}
 & & & & & & & 2 & 0
\end{array}
$$

Jakoprosessissa peräkkäiset jakojäännökset ovat $6, 4, 5, 1, 3$ ja 2. Kun jakojäännös 2 on tuloksena seuraavassa askeleessa, jaetaan 20 luvulla 7. Näin ollen jakoprosessi jatkuu samalla tavalla kuin alussa ja jakso on siis täyttynyt. Täten $\frac{2}{7}$ voidaan kirjoittaa muotoon

$$\frac{2}{7} = 0,\overline{285714}.$$

Koska jaettaessa luvulla 7 ovat kaikki jakojäännökset pienempiä kuin 7, niin

mahdollisia jakojäännöksiä on vain kuusi (luku 0 ei tule kysymykseen jakojäännöksenä koska tutkitaan päättymättömiä desimaaliesityksiä). Jatkettaessa jakolaskua jossain vaiheessa aina tulee jokin aikaisemmin esiintynyt jakojäännös.

Edellisessä jakolaskussa $2/7$ jakojäännös 2 tuli kuudennen askeleen jälkeen ja jakoprosessi palautui ensimmäiseen jakoon. Yleensä ei kuitenkaan tapahdu niin, että jakso alkaisi ensimmäisestä askeleesta. Esimerkiksi

$$\frac{211}{990} = 0,2\overline{13}.$$

Samalla tavalla yleisessä tapauksessa, suoritettaessa jakolasku $\frac{m}{n}$, mahdolliset jakojäännökset ovat $1, 2, \ldots, n-1$, joten jakolaskussa esiintyy jakso ennen n:ttä askelta. Näin saadaan jaksollinen desimaaliluku. Jos jossakin vaiheessa jakojäännös on nolla, on desimaaliesitys päättyvä. Näin ollen ollaan osoitettu toinen puoli seuraavasta lauseesta.

Lause 5.3.1. *Jokaisella rationaaliluvulla $\frac{m}{n}$ on päättyvä tai jaksollinen päättymätön desimaaliesitys. Kääntäen jokainen päättyvä tai päättymätön mutta jaksollinen desimaaliluku on rationaaliluku.*

Tarkastellaan aluksi esimerkin avulla päättymätöntä jaksollista desimaalilukua

$$x = 18,255\overline{123} \quad \text{tai} \quad x = 18,255123123\ldots$$

Kerrotaan tämä luku ensin sellaisella luvulla, että desimaalipilkku siirtyy ensimmäisen ja toisen jakson väliin eli luvulla 10^6:

$$10^6 x = 18255123,123\ldots$$

Tällöin $10^6 x - 10^3 x = 999000x = 18236868$, joten

$$x = \frac{18236868}{999000}$$

Näin ollen x on rationaaliluku. Tällä tavalla jaksollinen osa voidaan ”eliminoida” luvusta x.

Yleisessä tapauksessa menetellään samalla tavalla. Tarkastelun helpottamiseksi oletetaan, että tutkittavalla päättymättömällä jaksollisella desimaaliluvulla ei ole kokonaisosaa. Tämä rajoitus ei loukkaa tarkastelujen yleisyyttä. Olkoon

$$x = 0, a_1 a_2 \ldots a_s \overline{b_1 b_2 \ldots b_r},$$

missä $a_1, \ldots, a_s$ on jaksoton osa ja $b_1, \ldots, b_r$ toistuva jakso. Kerrotaan x ensin luvulla 10^{s+r} ja sitten luvulla 10^s, jolloin saadaan

$$10^{s+r}x = a_1 \ldots a_s b_1 \ldots b_r + 0, \overline{b_1 b_2 \ldots b_r},$$
$$10^s x = a_1 \ldots a_s + 0, \overline{b_1 \ldots b_r}.$$

Vähentämällä nämä luvut keskenään, saadaan

$$10^{s+r}x - 10^s x = a_1 \ldots a_s b_1 \ldots b_r - a_1 \ldots a_r,$$

joten,

$$x = \frac{a_1 \ldots a_s b_1 \ldots b_r - a_1 \ldots a_s}{10^{s+r} - 10^s}$$

ja on näin ollen rationaaliluku. Jos taas desimaaliluku on päättyvä eli

$$a_0, a_1 a_2 \ldots a_n,$$

on se muotoa

$$\frac{10^n a_0 + a_1 a_2 \ldots a_n}{10^n}$$

oleva rationaaliluku. Näin on todistettu lauseen toinenkin puoli.

Desimaaliesityksen yksikäsitteisyydestä

Jokaisella nollasta eroavalla päättyvällä desimaaliluvulla on päättymätön jaksollinen desimaaliesitys.
Tarkastellaan rationaaliluvun $\frac{1}{3}$ desimaaliesitystä

$$\frac{1}{3} = 0, 333 \ldots$$

Jos tämän yhtälön molemmat puolet kerrotaan luvulla 3, saadaan

$$1 = 0, 999 \ldots \tag{11}$$

Näin ollen päättyvät desimaaliluvut 1 ja 1,0 ja päättymätön jaksollinen desimaaliluku 0,999 ... ovat samat.

Tarkastellaan yhtälöä (11) toisella tavalla. Merkitään sen oikealla puolella olevaa desimaalilukua x:llä

$$x = 0, 999 \ldots \tag{12}$$

Kertomalla tämä yhtälö puolittain luvulla 10 saadaan

$$10x = 9, 999 \ldots = 9 + 0, 999 \ldots \tag{13}$$

Vähentämällä yhtälöt (12) ja (13) puolittain saadaan

$$9x = 9 \quad \text{eli} \quad x = 1.$$

Näin on toisella tavalla osoitettu, että yhtälö (11) pätee.

Jakamalla yhtälö (11) luvuilla $10, 100, 1000$ jne. saadaan

$$\begin{aligned} 0,1 &= 0,099\ldots, \\ 0,01 &= 0,0099\ldots, \\ 0,001 &= 0,00099\ldots \qquad \text{jne.} \end{aligned}$$

Käyttämällä hyväksi näitä esityksiä mikä tahansa päättyvä desimaaliluku voidaan kirjoittaa päättymättömäksi jaksolliseksi desimaaliluvuksi.

Esimerkki.

Se, kuinka monta desimaaliesitystä samalla rationaaliluvulla on, riippuu tulkinnasta. Esimerkiksi luku $0,42$ voidaan kirjoittaa muotoon $0,4199\ldots$ tai muotoihin

$$0,420; 0,4200; 0,42000; \ldots$$

Nämä jälkimmäiset ovat luvun $0,42$ *triviaaleja muotoja*, joten niitä ei lasketa mukaan. Kun puhutaan luvun $0,42$ päättymättömästä desimaaliesityksestä, tarkoitetaan esitystä $0,4199\ldots$ eikä esitystä $0,42000\ldots$.

6 Reaaliluvut

6.1 Lukusuora

Aiemmin kokonaislukujen yhteydessä oli maininta lukusuorasta. Lukusuora konstruoidaan siten, että valitaan annetulta vaakasuoralta kaksi erillistä pistettä, joita merkitään numeroilla 0 ja 1 vasemmalta oikealle. Näiden pisteiden välistä etäisyyttä sanotaan yksikköpituudeksi. Yksikköväliä käyttäen merkitään muut kokonaisluvut lukusuoralle niin, että $a < b$ jos ja vain jos kokonaislukua a esittävä piste on lukua b esittävän pisteen vasemmalla puolella.

Rationaaliluvun $\frac{a}{b}$ (oletetaan rajoituksetta, että $b > 0$) sijainti lukusuoralla määräytyy seuraavasti. Jaetaan yksikköväli b:hen yhtä pitkään osaan. Jos $a > 0$, mitataan a-kertainen edellä saadun osajanan pituinen matka oikealle ja asetetaan lukua $\frac{a}{b}$ vastaava piste lukusuoralle kyseiselle etäisyydelle origosta (joka on lukua 0 vastaava piste). Vastaavasti, jos $\frac{a}{b}$ on negatiivinen, mitataan sama etäisyys kuin edellä, mutta origosta vasemmalle, ja asetetaan lukua $\frac{a}{b}$ vastaava piste tälle etäisyydelle origosta.

Edellä mainitulla tavalla saatuja pisteitä sanotaan rationaalilukupisteiksi.

Rationaalilukujen tiheysominaisuudesta seuraa, että olivatpa rationaaliluvut x ja y kuinka lähellä toisiaan hyvänsä, niin silti niiden välistä löytyy äärettömän monta rationaalilukua. Näin ollen luulisi, että lukusuora täyttyy rationaaliluvuista.

Kuitenkin lukusuoralle jää reikiä (joita on itseasiassa "enemmän" kuin rationaalilukupisteitä). Esimerkiksi Pythagoraan lauseen mukaan yksikköneliön lävistäjän pituus, jota merkitään symbolilla $\sqrt{2}$, ei ole rationaaliluku. Näin ollen origosta $\sqrt{2}$ pituusyksikön päässä oleva piste ei ole rationaalilukupiste. Tällaisia pisteitä sanotaan irrationaalilukupisteiksi.

Reaaliluvuilla tarkoitetaan kaikkia niitä lukuja, jotka liittyvät lukusuoran pisteisiin. Jokainen reaaliluku on joko rationaaliluku tai irrationaaliluku, mutta ei molempia yhtä aikaa. Näin ollen jokainen reaaliluku, jota ei voi esittää muodossa $\frac{p}{q}$, missä $p, q \in \mathbb{Z}$ ja $q \neq 0$, on irrationaaliluku. Reaalilukujen joukolle käytetään merkintää $\mathbb{R}$.

6.2 Desimaaliesitys

Tarkastellaan reaaliluvun desimaaliesityksen määräämistä. Valitaan piste lukusuoralta. Vastatkoon se lukua $x > 0$. Desimaaliesitys saadaan seuraavasti:

(i) Valitaan sellainen kokonaisluku a_0, että $a_0 \leq x < a_0 + 1$;

(ii) Valitaan sellainen kokonaisluku a_1, että $0 \leq a_1 \leq 9$ ja

$$a_0 + \frac{a_1}{10} \leq x < a_0 + \frac{a_1 + 1}{10};$$

(iii) Kun on valittu $a_0, a_1, \ldots, a_{n-1}$, missä a_j:t ovat kokonaislukuja ja $0 \leq a_1, \ldots, a_{n-1} \leq 9$, niin valitaan sellainen $a_n \in \mathbb{Z}$, että $0 \leq a_n \leq 9$ ja

$$a_0 + \frac{a_1}{10} + \ldots + \frac{a_n}{10^n} \leq x < a_0 + \frac{a_1}{10} + \ldots + \frac{a_n + 1}{10^n}.$$

Yllä oleva prosessi on induktiivinen ja sen n:nnellä askeleella saadaan luvun x n:n desimaalin likiarvo.

Huomautus. Yllä olevalla prosessilla ei saada 9-jonoon päättyviä desimaaliesityksiä lainkaan.

Selvästi esimerkiksi luvun 0 desimaaliesitys on $0,000\ldots$.
Negatiivisille luvuille desimaaliesitys määritellään vastaluvun avulla. Jos $x < 0$ ja luvun $-x > 0$ desimaaliesitys on

$$a_0, a_1 a_2 a_3 \ldots,$$

niin määritellään, että luvun x desimaaliesitys on

$$-a_0, a_1 a_2 a_3 \ldots.$$

Reaalilukujen järjestys $<$ voidaan määritellä desimaaliesityksen avulla:

(i) Jos $x = a_0, a_1 a_2 \ldots$ ja $y = b_0, b_1 b_2 \ldots$ ovat positiivisia reaalilukuja, niin $x < y$ jos ja vain jos $a_0 < b_0$ tai $a_0 = b_0$ ja on olemassa sellainen $i_0 \in \mathbb{Z}_+$, että $a_j = b_j$ kun $j = 1, \ldots, i_0 - 1$ sekä $a_{i_0} < b_{i_0}$;

(ii) Jos x ja y ovat negatiivisia, niin $x < y$ jos ja vain jos $-y < -x$;

(iii) Jos x on negatiivinen ja y on ei-negatiivinen, niin $x < y$.

Jos x ja y ovat reaalilukuja, joiden n desimaalin esitykset ovat samat, niin

$$a_0, a_1 \dots a_n \leq x < a_0, a_1 \dots a_n + \frac{1}{10^n},$$
$$a_0, a_1 \dots a_n \leq y < a_0, a_1 \dots a_n + \frac{1}{10^n}.$$

Vähentämällä toinen epäyhtälö ensimmäisestä saadaan

$$-\frac{1}{10^n} < x - y < \frac{1}{10^n}.$$

Jos x ja y ovat eri lukuja, niin riittää löytää sellainen luvun $n \in \mathbb{N}_0$ arvo, että lukujen x ja y erotuksen itseisarvo $|x - y|$ on suurempi kuin $\frac{1}{10^n}$.

Luvun $n \in \mathbb{N}_0$ olemassaolon takaa *Arkhimedeen ehto:* Jos ϵ on annettu positiivinen reaaliluku, niin on olemassa sellainen $n \in \mathbb{N}_0$, että $\frac{1}{10^n} < \epsilon$.

6.3 Rationaali- ja irrationaaliluvut

Yleensä ei ole helppoa osoittaa, että annettu luku on rationaalinen (esim. π on irrationaalinen, mutta sen todistaminen ei ole yksinkertaista). Kuitenkin siitä, että $\sqrt{2}$ on irrationaaliluku, seuraa, että minkä tahansa rationaalilukujen välistä löytyy irrationaalilukuja. Todistetaan ensin tarvittava lemma.

Lemma 6.3.1. *Jos $\frac{m}{n}$ ja $\frac{r}{s}$ ovat rationaalilukuja ja $\frac{r}{s} \neq 0$, niin $\frac{m}{n} + \frac{r}{s}\sqrt{2}$ on irrationaaliluku.*

Todistus. Luennoilla. □

Lause 6.3.1. *Kahden toisistaan eroavan rationaaliluvun välistä löytyy irrationaaliluku.*

Todistus. Luennoilla. □

Lause 6.3.2. *Kahden toisistaan eroavan irrationaaliluvun välistä löytyy rationaaliluku.*

Todistus. Luennoilla. □

Huomautus. Lauseiden 6.3.1 ja 6.3.2 perusteella ei pidä kuitenkaan luulla, että rationaali- ja irrationaalilukupisteet vuorottelisivat lukusuoralla.
Niiden keskinäinen sijainti lukusuoralla on itseasiassa hyvin monimutkaista. Reaalilukupisteet muodostavat lukusuoralla jatkumon eikä ole järkeä puhua siitä, mikä luku tulee annetun luvun jälkeen (vrt. kokonaisluvut, jolloin esim. 2 on luvun 1 seuraaja).

6.4 Desimaalilukujen aritmetiikasta

Vaikka päättymätön desimaaliesitys onkin kätevä tapa reaalilukujen esittämiseen, on se numeriikan kannalta kömpelö esitys. Esimerkiksi päättyvien desimaalilukujen summa on helpompi muodostaa aloittamalla yhteenlasku viimeisestä desimaalista. Päättymättömillä desimaaliluvuilla ei ole viimeistä desimaalia, josta aloittaa. Tämän vuoksi yhteenlasku on aloitettava kokonaisosasta ja sen jälkeen edettävä desimaali desimaalilta vasemmalta oikealle.

Esimerkki. Tarkastellaan esimerkkinä lukujen $\frac{2}{3} = 0,\overline{6}$ ja $\frac{2}{7} = 0,\overline{285714}$ yhteenlaskua

$$\begin{aligned}
0,6+0,2 &= 0,8\\
0,66+0,28 &= 0,94\\
0,666+0,285 &= 0,951\\
0,6666+0,2857 &= 0,9523\\
0,66666+0,28571 &= 0,95237\\
0,666666+0,285714 &= 0,952380
\end{aligned}$$

Tarkka summa on $\frac{20}{21} = 0,\overline{952380}$.

Esimerkiksi 1-desimaalisten esitysten summa ei anna tarkkaa vastausta yhden desimaalin tarkkuudella. Kuitenkin saadaan kasvava jono rationaalilukuja, jotka suppenevat kohti tarkkaa arvoa.

Teoreettisissa tarkasteluissa on hyödyllisempää käyttää reallilukujen approksimoinnissa kasvavia jonoja desimaaliesitysten sijaan.

Jonoista

Reaalilukujonolla tarkoitetaan päättymätöntä luetteloa

$$a_1, a_2, a_3, \ldots, a_n, \ldots,$$

missä $a_n \in \mathbb{R}$ jokaisella $n \in \mathbb{Z}_+$. Jonolle käytetään myös merkintää $(a_n)_{n=1}^{\infty}$.

Esimerkki.

Jonoille voidaan määritellä yhteen-, vähennys- ja kertolasku asettamalla

$$\begin{aligned}
(a_n) + (b_n) &= (a_n + b_n),\\
(a_n) - (b_n) &= (a_n - b_n),\\
(a_n) \cdot (b_n) &= (a_n b_n),
\end{aligned}$$

Jakolasku voidaan määritellä asettamalla

$$\frac{(a_n)}{(b_n)} = \left(\frac{a_n}{b_n}\right),$$

joka on määritelty ainoastaan, kun $b_n \neq 0$ kaikilla $n \in \mathbb{Z}_+$.

Suppeneminen

Reaaliluvun $x > 0$ desimaaliesitys saatiin rationaalilukujonon (a_n), missä a_n on luvun x n:s desimaali, "raja-arvona". Määritellään, mitä "raja-arvolla" tarkoitetaan.

Määritelmä 6.4.1. *Reaalilukujonon $(a_n)_{n=1}^{\infty}$ sanotaan suppenevan kohti raja-arvoa a, jos jokaista lukua $\epsilon > 0$ kohti on olemassa sellainen $N \in \mathbb{Z}_+$, että*

$$|a_n - a| < \epsilon \quad \textit{aina, kun} \quad n > N.$$

Jos raja-arvoa a ei ole olemassa, niin sanotaan, että jono $(a_n)_{n=1}^{\infty}$ hajaantuu.

Huomautus. Jos raja-arvo on olemassa, se on yksikäsitteinen.

Esimerkki.

Jos jono $(a_n)_{n=1}^{\infty}$ suppenee kohti lukua a, tulevat jonon termit a_n mielivaltaisen lähelle lukua a, kun n on "riittävän suuri".

6.5 Reaalilukujen täydellisyys

Tärkeitä erikoistapauksia jonoista $(a_n)_{n=1}^{\infty}$ ovat:

(i) Kasvava jono eli $a_{n+1} \geq a_n$ kaikilla $n \in \mathbb{Z}_+$;

(ii) Vähenevä jono eli $a_{n+1} \leq a_n$ kaikilla $n \in \mathbb{Z}_+$;

(iii) Ylhäältä rajoitettu jono eli on olemassa sellainen $M \in \mathbb{R}$, että $a_n \leq M$ kaikilla $n \in \mathbb{Z}_+$ (lukua M sanotaan ylärajaksi);

(iv) Alhaalta rajoitettu jono eli on olemassa sellainen $m \in \mathbb{R}$, että $a_n \geq m$ kaikilla $n \in \mathbb{Z}_+$ (lukua m sanotaan alarajaksi).

Jos kasvavaa ja ylhäältä rajoitettua jonoa havainnollistetaan lukusuoran avulla, niin riittää tarkastella ainoastaan väliä $[a_1, M]$, sillä kaikki muut jonon termit ovat tällä välillä.

Intuitiivisesti tuntuisi selvältä, että tällainen lukujono suppenee kohti jotain raja-arvoa a. Näin osoittautuukin reaalilukujen tapauksessa, mutta rationaaliluvuilla ei ole tällaista ominaisuutta. Esimerkiksi, jos $(a_n)_{n=1}^{\infty}$ on lukujono, missä a_n on luvun $\sqrt{2}$ n *desimaalin* esitys, se on kasvava ja ylhäältä rajoitettu mutta se ei kuitenkaan suppene kohti mitään rationaalilukua vaan kohti lukua $\sqrt{2}$, joka on irrationaaliluku. Reaaliluvut korjaavat tässä mielessä rationaalilukujen puutteellisuuden.

Osoitetaan seuraavaksi, että jokainen ylhäältä rajoitettu kasvava reaalilukujono suppenee. Sitä varten annetulle reaaliluvulle kannattaa johtaa esitys samaan tapaan kuin johdettiin desimaaliesitys. Valitaan lukusuoralta lukua $x \in \mathbb{R}$ vastaava piste. Tämän jälkeen:

1. Valitaan sellainen kokonaisluku a_0, että $a_0 \leq x < a_0 + 1$;

2. Valitaan sellainen kokonaisluku a_1, että $0 \leq a_1 \leq 9$ ja
$$a_0 + \frac{a_1}{10} \leq x < a_0 + \frac{a_1 + 1}{10};$$

3. Jos $a_0, a_1, \ldots, a_{n-1}$ on valittu, niin valitaan sellainen $a_n \in \mathbb{Z}$, että $0 \leq a_n \leq 9$ ja
$$a_0 + \frac{a_1}{10} + \ldots + \frac{a_n}{10^n} \leq x < a_0 + \frac{a_1}{10} + \ldots + \frac{a_n + 1}{10^n}.$$

Tällä tavalla saadaan luvulle x yksikäsittäinen esitys

$$a_0 \odot a_1 a_2 \ldots a_n \ldots,$$

joka yhtyy desimaaliesitykseen positiivisilla x, mutta negatiivisilla x eroaa desimaaliesityksestä. Esimerkiksi luvulle $x = -1,399\ldots$ saadaan yllä olevalla prosessista $a_0 = -2, a_1 = 6$ ja $a_j = 0$ kaikilla $j \geq 2$. Siis luvulle x saadaan esitys
$$-2 \odot 600\ldots$$

Tämän esitystavan etu desimaaliesitykseen verrattuna on, että jokaista $x \in \mathbb{R}$ kohti (riippumatta siitä onko x positiivinen vai ei) on kasvava jono rationaalilukuja, joka suppenee kohti lukua x. Nimittäin jos $x_n = a_0 \odot a_1 \ldots a_n$, niin selvästikin (x_n) on kasvava ja

$$|x - x_n| < \frac{1}{10^n}.$$

Joskus reaalilukujen desimaaliesitys määritellään yllä olevalla tavalla. Toinen etu on se, että järjestys voidaan määritellä kaikille x kuten desimaaliesityksen yhteydessä tehtiin positiivisille reaaliluvuille.

Nyt voidaan todistaa:

Lause 6.5.1. *Jos $(a_n)_{n=1}^{\infty}$ on ylhäältä rajoitettu kasvava reaalilukujono, niin $(a_n)_{n=1}^{\infty}$ suppenee.*

Todistus. Luennoilla. □

Tarkastellaan seuraavaksi jonojen sijaan ylhäältä rajoitettua epätyhjää joukkoa $S \subseteq \mathbb{R}$. Tällöin on olemassa sellainen $M \in \mathbb{R}$, että $x \leq M$ kaikilla $x \in S$. Voidaankin kysyä, että onko joukossa S olemassa suurinta alkiota. Valitettavasti näin ei aina ole, mutta pyritään valitsemaan ylärajoista paras mahdollinen edustaja eli niin sanottu pienin yläraja. Osoittautuu, että jokaisella epätyhjällä ylhäältä rajoitetulla joukolla on olemassa pienin yläraja.

Määritelmä 6.5.1. *Olkoon $S \subseteq \mathbb{R}$ epätyhjä ylhäältä rajoitettu joukko. Lukua M sanotaan joukon S pienimmäksi ylärajaksi, merkitään $M = \sup S$ (luetaan supremum), jos*

(i) $x \leq M$ kaikilla $x \in S$ (M on yläraja),

(ii) ehdosta $M' < M$ seuraa, että M' ei ole yläraja (M on ylärajoista pienin).

Vastaavasti voidaan määritellä suurin alaraja.

Määritelmä 6.5.2. *Olkoon $S \subseteq \mathbb{R}$ epätyhjä alhaalta rajoitettu joukko. Lukua m sanotaan joukon S suurimmaksi alarajaksi, merkitään $m = \inf S$ (luetaan infimum), jos*

(i) $x \geq m$ kaikilla $x \in S$ (m on alaraja),

(ii) ehdosta $m' > m$ seuraa, että m' ei ole alaraja (m on alarajoista suurin).

Esimerkki.

Nyt voidaan todistaa reaalilukujen täydellisyysominaisuus. Osoitetaan ensin kuitenkin sen duaalitulos.

Lause 6.5.2. *Jokaisella epätyhjällä alhaalta rajoitetulla joukolla $S \subseteq \mathbb{R}$ on suurin alaraja.*

Todistus. Luennoilla. □

Lause 6.5.3. *(Täydellisyysaksiomi)*
Jokaisella epätyhjällä rajoitetulla joukolla $S \subseteq \mathbb{R}$ on pienin yläraja.

Todistus. Todistus jätetään harjoitustehtäväksi. □

Huomautus. Oletus "S on epätyhjä" on välttämätön, sillä mikä tahansa luku on tyhjän joukon yläraja.

Aiemman esimerkin (b)-kohdan mukaan epätyhjällä ylhäältä rajoitetulla rationaalilukujoukolla ei välttämättä ole ylärajaa joukossa $\mathbb{Q}$. Lauseen 6.5.3 mukaan reaaliluvut korjaavat rationaalilukujen edellä mainitun puutteellisuuden. Toisin sanoen $\mathbb{R}$ on täydellinen mutta $\mathbb{Q}$ ei ole. Täydellisyysominaisuus on välttämätön esimerkiksi matemaattisen analyysin teoriassa.

6.6 Reaalilukujen aritmetiikan määrittely

Reaalilukujen aritmetiikka voitaisiin määritellä desimaalilukujen avulla. Käytetään tässä yhteydessä kuitenkin edellisen kappaleen esitystapaa.
Oletetaan, että kaikille on koulusta tuttua päättyvien desimaalilukujen aritmetiikka. Olkoot r_1 ja r_2 reaalilukuja ja olkoot niiden esitykset $a_0 \odot a_1 a_2 \ldots$ ja $b_0 \odot b_1 b_2 \ldots$. Merkitään $r_1^0 = a_0$ ja jokaisella $n \in \mathbb{Z}_+$ $r_1^n = a_0 \odot a_1 \ldots a_n$. Vastaavasti merkitään $r_2^0 = b_0$ ja $r_2^n = b_0 \odot b_1 \ldots b_n, n \in \mathbb{Z}_+$.
Olkoon $s_n = r_1^n + r_2^n$. Lukujen r_1 ja r_2 summa määritellään asettamalla

$$r_1 + r_2 = \sup\{s_n \mid n \in \mathbb{N}_0\}.$$

Yhteenlasku on hyvin määritelty.

Esimerkki.

Yhteenlasku on

(i) kommutatiivinen eli $x + y = y + x$ kaikilla $x, y \in \mathbb{R}$

(ii) assosiatiivinen eli $x + (y + z) = (x + y) + z$ kaikilla $x, y, z \in \mathbb{R}$.

Nyt voidaan merkitä, että $x = a_0 \odot a_1 a_2 \ldots$ on sama kuin $x = a_0 + 0, a_1 a_2 \ldots$.
Nolla-alkio on luonnollisesti luku 0. Alkion $x \in \mathbb{R}$ vasta-alkio on

$$-x = \sup\{y \in \mathbb{R} \mid x + y \leq 0\}.$$

Määritellään kertolasku aluksi ei-negatiivisille luvuille. Olkoot $x, y \in \mathbb{R}$, $x, y \geq 0$ ja olkoot niiden esitykset $x = a_0 + 0, a_1 a_2 \ldots$ ja $y = b_0 + 0, b_1 b_2 \ldots$ Merkitään $x^0 = a_0, y^0 = b_0$ ja $x^n = a_0 + 0, a_1 \ldots a_n, y^n = b_0 + 0, b_1 \ldots b_n$ kaikilla $n \geq 1$. Lukujen x ja y tulo määritellään asettamalla

$$x \cdot y = \sup\{x^n \cdot y^n \mid n \in \mathbb{N}_0\}.$$

Muussa tapauksessa määritellään:

1) Jos $x < 0$ ja $y \geq 0$, niin $x \cdot y = -((-x) \cdot y)$;

2) Jos $x \geq 0$ ja $y < 0$, niin $x \cdot y = -(x \cdot (-y))$;

3) Jos $x < 0$ ja $y < 0$, niin $x \cdot y = (-x) \cdot (-y)$.

Kertolasku on hyvin määritelty ja se on

(iii) kommutatiivinen eli $x \cdot y = y \cdot x$ kaikilla $x, y \in \mathbb{R}$,

(iv) assosiatiivinen eli $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ kaikilla $x, y, z \in \mathbb{R}$.

Ykkösalkio on luonnollisesti luku 1. Jos $x > 0$, niin alkion x käänteisalkio on

$$x^{-1} = \sup\{y > 0 \mid x \cdot y \leq 1\}.$$

Jos taas $x < 0$, niin $x^{-1} = -(-x)^{-1}$.

Yhteen- ja kertolaskulle pätee

(v) distributiivilaki eli $x \cdot (y + z) = x \cdot y + x \cdot z$ kaikilla $x, y, z \in \mathbb{R}$.

Yhteenlasku säilyttää järjestyksen eli jos $x < y$, niin $x + z < y + z$ kaikilla $z \in \mathbb{R}$.

Ei-negatiivisuus säilyy kertolaskussa, eli jos $x, y \geq 0$, niin $x \cdot y \geq 0$.

6.7 Muita konstruktioita

Desimaaliesityksen lisäksi on kaksi tapaa toteuttaa reaalilukujen konstruktio täsmällisesti. Käsitellään niitä lyhyesti tässä kappaleessa.

Ensimmäinen perustuu reaalilukujen approksimointiin rationaalilukujen avulla. Rationaaliluvuista muodostetaan *Cauchyn jonoja* $(a_n)_{n=1}^{\infty}$, missä $a_n \in \mathbb{Q}$ kaikilla $n \in \mathbb{Z}_+$.

Jono on Cauchyn jono, jos jokaista $0 < \epsilon \in \mathbb{Q}$ kohti on olemassa sellainen $N \in \mathbb{Z}_+$, että

$$|a_n - a_m| < \epsilon \text{ aina, kun } n, m > N.$$

Olkoon $\mathcal{C}$ tällaisten jonojen muodostama joukko. Koska löytyy useita jonoja, jotka suppenevat kohti tiettyä "reaalilukua" (vielä ei ole määritelty reaalilukua), niin sijoitetaan jonot (a_n) ja (b_n) samaan luokkaan, jos $(a_n - b_n)$ suppenee kohti nollaa. Huomaa, että jälkimmäisessä ehdossa ei itse asiassa vaadita jonojen suppenemista eikä tietoa reaaliluvuista, vaan ainoastaan rationaalilukujonon $(a_n - b_n)$ suppeneminen kohti nollaa, joka on rationaaliluku.

Määritellään joukossa $\mathcal{C}$ ekvivalenssirelaatio $\sim$ asettamalla

$$(a_n) \sim (b_n) \Leftrightarrow (a_n - b_n) \text{ suppenee kohti nollaa.}$$

Ekvivalenssiluokkien $[a_n]$ muodostamalle joukolle käytetään merkintää $\mathbb{R}$ ja ekvivalenssiluokkia sanotaan reaaliluvuiksi.

Rationaalilukuja edustavat luokat $[q]$, missä $(q)_{n=1}^{\infty}$ $(q \in \mathbb{Q})$ on vakiojono. Yhteen- ja kertolasku määritellään seuraavasti:

$$[a_n] + [b_n] = [a_n + b_n],$$
$$[a_n][b_n] = [a_n b_n].$$

Tämän konstruktion esitti Georg Cantor vuonna 1872. Voidaan osoittaa, että tämän konstruktion reaaliluvut muodostavat täydellisen järjestetyn kunnan.

Toinen konstruktio on samantapainen kuin lukusuoran aukkojen täyttäminen. Konstruktion esitti Richard Dedekind vuonna 1872.

Konstruktiossa lukusuoralla olevat rationaaliluvut jaetaan kahteen erilliseen osaan leikkaamalla lukusuora kahtia. Jos leikkauspiste on rationaalilukupiste, lisätään piste oikeanpuoleiseen osaan B, jolloin $\mathbb{Q} = A \cup B$. Jos taas leikkauspiste on irrationaalilukupiste, saadaan myös jako $\mathbb{Q} = A \cup B$. Riittää tarkastella vasemmanpuoleista osaa A. Näitä sanotaan Dedekindin leikkauksiksi.

Esimerkki.

Voidaan osoittaa, että Dedekindin leikkausten joukko muodostaa täydellisen järjestetyn kunnan.

7 Joukkojen mahtavuudet

Mikä on äärettömyys? Ehkäpä ensimmäinen luonnehdinta voisi olla ”jotain suurempaa kuin mikä tahansa luonnollinen luku”. Tietyssä mielessä tämä luonnehdinta onkin oikea. Kuitenkin osoittautuu, ettei löydy pelkästään yhtä äärettömyyttä vaan kokonainen äärettömyyksien hierarkia. Voi tuntua hieman yllättävältä, että rationaalilukuja on yhtä monta kuin luonnollisia lukuja. Tämä ominaisuus erottaa äärettömät joukot äärellisistä.

Sen sijaan, että kysyisimme ”kuinka monta alkiota”, on järkevämpää *vertailla* alkioiden lukumäärää kuin laskea alkioiden lukumäärä. Lukumäärien vertailu on alkeellisempi operaatio kuin lukumäärän laskeminen. Käsite ”joukoissa A ja B on sama määrä alkoita” tarkoittaa, että on olemassa bijektio $f : A \to B$.

Ennen kuin siirrytään tarkastelemaan äärettömyyksien hierarkiaa, tutkitaan mikä niistä on pienin. Vertailujoukoksi kannattaa valita $\mathbb{N}$ joukon $\mathbb{N}_0$ sijaan, sillä bijektio $f : \mathbb{N} \to B$ järjestää joukon B alkiot jonoon. Alkiota $f(1)$ voidaan sanoa ensimmäiseksi alkioksi, $f(2)$ toiseksi ja niin edelleen.

Määritellään joukot $\mathbb{N}(n)$, missä $n \in \mathbb{N}_0$, asettamalla $\mathbb{N}(0) = \emptyset$ ja

$$\mathbb{N}(n) = \{m \in \mathbb{N} \mid 1 \leq m \leq n\}, \text{ missä } n \in \mathbb{N}.$$

Sanotaan, että joukko X on

(i) äärellinen, jos on olemassa bijektio $f : \mathbb{N}(n) \to X$ jollekin $n \in \mathbb{N}_0$;

(ii) numeroituvasti ääretön, jos on olemassa bijektio $f : \mathbb{N} \to X$;

(iii) numeroituva, jos X on äärellinen tai numeroituvasti ääretön.

Jos X on äärellinen, niin voidaan sanoa, että joukossa X on n alkiota. Jos X on numeroituvasti ääretön, sanotaan, että joukossa X on $\aleph_0$ (lue: aalef nolla) alkiota.

Esimerkki.

Joukko-opissa äärettömyydelle voidaan antaa täsmällinen tulkinta. Joukko-opin isänä voidaan pitää Georg Cantoria. Hänen ratkaisunsa äärettömyyttä koskevaan ongelmaan oli *kardinaaliluvun* käsite. Sanotaan, että joukot A ja B ovat yhtämahtavat tai että joukoilla A ja B on sama kardinaaliluku ja merkitään $|A| = |B|$, jos on olemassa bijektio $f : A \to B$. Lisäksi sovitaan, että $\emptyset$ on yhtä mahtava itsensä kanssa.

Jos on olemassa bijektio

1) $f : \mathbb{N}(n) \to X$, niin sanotaan, että joukon X kardinaaliluku on n;

2) $f : \mathbb{N} \to X$, niin sanotaan, että joukon X kardinaaliluku on $\aleph_0$.

Jos on olemassa injektio $f : X \to Y$, niin X on korkeintaan yhtä mahtava kuin Y ja merkitään $|X| \leq |Y|$. Merkinnällä $|X| < |Y|$ tarkoitetaan, että $|X| \leq |Y|$ ja $|X| \neq |Y|$.

Yleisesti, jos $X \subseteq Y$, niin upotus (inkluusio) $i : X \to Y$, missä $i(x) = x$, on injektio, joten

$$X \subseteq Y \Rightarrow |X| \leq |Y|.$$

Kuitenkin jokainen ääretön joukko on yhtä mahtava sen aidon osajoukon kanssa.

Lause 7.0.1. *(Cantor)*
Jos joukko B on ääretön, niin on olemassa sellainen aito osajoukko $A \subsetneq B$, että $|A| = |B|$.

Todistus. Luennoilla. □

Lauseen 7.0.1 mukaan jokaisesta äärettömästä joukosta B voidaan valita numeroituvasti ääretön osajoukko X, joten $\aleph_0 = |X| \leq |B|$. Näin ollen $\aleph_0$ on pienin ääretön kardinaaliluku. Yllättävän monen joukon, joka intuitiivisesti tuntuu suuremmalta kuin $\mathbb{N}$, kardinaaliluku on $\aleph_0$ (esim. $|\mathbb{Q}| = |\mathbb{N}_0 \times \mathbb{N}_0| = |\mathbb{Z}| = \aleph_0$).

Esimerkki.

Syy, miksi numeroituva joukko voi olla äärellinen tai numeroituvasti ääretön, käy ilmi seuraavasta tuloksesta.

Lause 7.0.2. *Numeroituvan joukon osajoukko on numeroituva.*

Todistus. Luennoilla. □

Numeroituvia joukkoja yhdistelemällä saadaan edelleen numeroituvia joukkoja.

Lause 7.0.3. *Numeroituvien joukkojen numeroituva yhdiste on numeroituva.*

Todistus. Luennoilla.

□

Ei pidä kuitenkaan luulla, että jokainen joukko olisi numeroituva, vaan on olemassa ylinumeroituvia joukkoja joiden mahtavuus on suurempi kuin $\mathbb{N}$:n mahtavuus.

Lause 7.0.4. *Reaalilukujen joukko on ylinumeroituva.*

Todistus. Luennoilla. □

Olkoon $\aleph$ reaalilukujen kardinaaliluku. Koska $\mathbb{N} \subset \mathbb{R}$, on $\aleph_0 \leq \aleph$ ja lauseen 7.0.4 mukaan $\aleph_0 < \aleph$. On siis löydetty kardinaalilukua $\aleph_0$ suurempi kardinaaliluku. Osoitetaan, että löytyy itseasiassa kokonainen hierarkia äärettömiä joukkoja, joilla on eri kardinaaliluku. sitä varten olkoon A joukko ja

$$\mathcal{P}(A) = \{B \mid B \subset A\}$$

A:n osajoukkojen muodostama joukko. Joukkoa $\mathcal{P}(A)$ sanotaan A:n potenssijoukoksi.

Lause 7.0.5. *Jos A on joukko, niin $|A| < |\mathcal{P}(A)|$.*

Todistus. Luennoilla. □

Lauseen 7.0.5 mukaan saadaan kokonainen hierarkia erisuuruisia äärettömyyksiä:

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < \dots$$

Miten $\mathbb{R}$:n mahtavuus sijoittuu tähän? Voidaan osoittaa, että $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$, mutta jätetään se hautumaan...

TÄMÄ KURSSI PÄÄTTYY TÄHÄN!

Viitteet

[1] C. F. Blumfield & Z. E. Eicholz & M. E. Shanks, *Algebra II*, Addison Wesley Publishing, Inc., 1962.

[2] C. Boyer, *Tieteiden kuningatar, Matematiikan historia, osa I*, John Wiley & Sons, 1991.

[3] C. Boyer, *Tieteiden kuningatar, Matematiikan historia, osa II*, John Wiley & Sons, 1991.

[4] G. Flegg, *Lukujen historia – Sormilla laskemisesta tietokoneisiin –*, Art House Oy, 2002.

[5] J. Merikoski & M. Halmetoja & T. Tossavainen, *Johdatus matemaattisen analyysin teoriaan*, WSOY, 2004.

[6] L. Myrberg, *Algebra*, Vaasa Oy, 1978.

[7] I. Niven, *Numbers: Rational and Irrational*, The Mathematical Association of America, 1961.

[8] I. Stewart & D. Tall, *The Foundation of Mathematics*, Oxford University Press, 1977.

[9] L. M. Weiner, *Introduction to Modern Algebra*, Hartcourt, Brace & World, Inc., 1970.

[10] R. L. Wilder, *Introduction to the Foudation of Mathematics*, John Wiley & Sons, Inc., 1952.