Lukualueet

Juha Lehrbäck ja Jouni Parkkonen

Lukijalle

Tämä moniste perustuu Jouni Parkkosen vuosina 2006–2008 ja Juha Lehrbäckin vuonna 2009 pitämien Lukualueet-kurssien luentoihin. Monisteen keskeinen materiaali on tarkoitettu 7 viikon mittaiselle luentokurssille, lisäksi mukana on jonkin verran ylimääräistä ja syventävää materiaalia.

Kurssilla konstruoidaan lukualueet $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ja $\mathbb{C}$ lähtien luonnollisista luvuista $\mathbb{N}$. Samalla käydään läpi näiden lukualuiden laskutoimitusten ja järjestysten ominaisuuksia. Lukualuiden $\mathbb{Z}$ ja $\mathbb{Q}$ konstruktiot ja näihin liittyvät laskutoimitukset ovat melko suoraviivaisia, mutta ne tarjoavat hyvää harjoitusta ekvivalenssirelaatioiden käytöstä. Reaalilukujen joukon $\mathbb{R}$ konstruktio Cauchyn jonojen avulla on hieman työläämpi, samoin kuin analyysin kannalta erittäin keskeisen reaalilukujen joukon täydellisyyden osoittaminen. Kompeksilukujen joukon yhteydessä johdamme 3. asteen polynomiyhtälöiden yleisen ratkaisukaavan ja todistamme algebran peruslauseen.

Kurssin suorittaminen ei vaadi suurempia esitietoja, tosin matemaattinen peruspäättely, (naiivi) joukko-oppi ja funktioihin liityvät perusmääritelmät oletetaan tunnetuiksi. Kun viittaamme muihin laitoksemme kursseihin käytämme lyhenteitä

EA - Euklidiset avaruudet
LAG1 - Lineaarinen algebra ja geometria 1.

1. Johdanto

Die ganzen Zahlen hat der liebe Gott gemacht,
alles andere ist Menschenwerk.

— Leopold Kronecker —

Luonnollisilla luvuilla $1, 2, 3, 4, \ldots$ laskeminen on kehittynyt käytännön tarpeesta ilmaista lukumääriä ja havainnosta, että esimerkiksi kolmen omenan ja kolmen lehmän muodostamilla joukoilla on todella jokin yhteinen ominaisuus. Käytännön kautta ovat syntyneet myös luonnollisten lukujen laskutoimitukset, erityisesti yhteen- ja kertolaskut, joiden on huomattu noudattavan monia nykyisin itsestäänselviltä tuntuvia "laskusääntöjä". Mutta mitä ovat negatiiviset luvut, rationaaliluvut ja irrationaaliluvut (tai jopa kompleksiluvut) ja miksi näillä voidaan laskea siinä missä luonnollisilla luvuillakin?

Lähdemme hakemaan näihin kysymyksiin vastauksia ylla olevaa Leopold Kroneckerin kommenttia mukaillen: otamme lähtökohdaksi tutun luonnollisten lukujen joukon $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$, jota Kroneckerkin tarkoittaa puhuessaan kokonaisluvuista (*ganzen Zahlen*). Nolla on tässä otettu mukaan luonnollisten lukujen joukkoon lähinnä mukavuussyistä, vaikka se ei olekaan lukualuiden kehityksen kannalta yhtä "luonnollinen" kuin luvut $1, 2, 3, 4, \ldots$. Joukko $\mathbb{N}$ varustetaan kahdella laskutoimituksella (yhteen- ja kertolasku, '$+$' ja '$\cdot$') sekä järjestyksellä '$\leq$', joiden ominaisuudet oletetaan "intuitiivisesti tunnetuiksi". Jatkossa kertolasku merkitään usein ilman pistettä: $a \cdot b = ab$.

Luonnollisista lukuvuista lähtien konstruoimme asteittain "kaiken muun" (*alles andere*), eli lukualueet

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

sekä näiden laskutoimitukset ja järjestykset.

Aloitamme formaalilla laskutoimituksen määritelmällä:

Määritelmä 1.1. Epätyhjän joukon A *laskutoimitus* on kuvaus $* : A \times A \to A$. Laskutoimituksen tulosta merkitään yleensä $*(a, b) = a * b$.

Laskutoimitus on siis sääntö, joka liittää kahteen joukon A alkioon a, b joukon A alkion $a * b$.

Esimerkki 1.2. (a) Luonnollisten lukujen yhteen- ja kertolasku ovat laskutoimituksia: yhteenlasku on kuvaus

$$+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N},\ +(m, n) = m + n \qquad (\text{eli } (m, n) \mapsto m + n),$$

ja kertolasku on kuvaus

$$\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N},\ \cdot(m, n) = m \cdot n\ (= mn) \qquad (\text{eli } (m, n) \mapsto mn).$$

(b) Joukon X osajoukot muodostavat X:n *potenssijoukon* $\mathscr{P}(X) = \{A \subset X\}$. Joukkojen leikkaus ja yhdiste ovat potenssijoukon $\mathscr{P}(X)$ laskutoimituksia: $(A, B) \mapsto A \cap B$, $(A, B) \mapsto A \cup B$.

(c) Olkoon $X \neq \emptyset$ ja olkoon $\mathscr{F}(X) = \{f \colon X \to X\}$ kaikkien X:n funktioiden joukko. Kuvausten yhdistäminen on joukon $\mathscr{F}(X)$ laskutoimitus: $(f, g) \mapsto f \circ g$.

(d) Matriisien yhteen- ja kertolaskut kaikkien 2×2 -matriisien joukossa $\mathrm{M}_{2\times 2}$ ovat laskutoimituksia. Yhteenlasku on laskutoimitus myös 2×3 -matriisien joukossa, mutta kertolasku ei ole.

Luonnollisten lukujen laskutoimituksilla on seuraavat tärkeät ominaisuudet:

(a) *assosiatiivisuus* eli *liitännäisyys*:

$$a + (b + c) = (a + b) + c$$
$$a(bc) = (ab)c$$

kaikilla $a, b, c \in \mathbb{N}$;

(b) *kommutatiivisuus* eli *vaihdannaisuus*:

$$a + b = b + a$$
$$ab = ba$$

kaikilla $a, b \in \mathbb{N}$;

(c) *distributiivisuus* eli *osittelulaki*

$$(a + b)c = ac + bc$$

pätee kaikilla $a, b, c \in \mathbb{N}$.

(d) Lisäksi yhteenlaskulla on *neutraalialkio* $0 \in \mathbb{N}$:

$$a + 0 = 0 + a = a \qquad \text{kaikilla } a \in \mathbb{N};$$

ja kertolaskulla on neutraalialkio $1 \in \mathbb{N}$:

$$a \cdot 1 = 1 \cdot a = a \qquad \text{kaikilla } a \in \mathbb{N}.$$

On tärkeää huomata, että kaikki laskutoimitukset eivät toteuta näitä ominaisuuksia.

Esimerkki 1.3. (a) Joukon $\mathscr{P}(X)$ laskutoimitukset $\cap$ ja $\cup$ ovat kommutatiivisia: $A \cap B = B \cap A$ ja $A \cup B = B \cup A$ kaikilla $A, B \in \mathscr{P}(X)$. Ne ovat myös assosiatiivisia ja lisäksi distributiivisia toistensa suhteen.

(b) Joukon $\mathscr{F}(X)$ laskutoimitus $\circ$ on assosiatiivinen: $f \circ (g \circ h) = (f \circ g) \circ h$ kaikilla $f, g, h \in \mathscr{F}(X)$. Laskutoimitus $\circ$ ei ole kuitenkaan kommutatiivinen, sillä yleensä $f \circ g \neq g \circ f$.

Määritelmä 1.4. Olkoon $A \neq \emptyset$ ja olkoon $*$ joukon A laskutoimitus. Alkio $e \in A$ on laskutoimituksen $*$ *neutraalialkio*, jos $e * a = a = a * e$ kaikilla $a \in A$. Alkio $\bar{a} \in A$ on alkion $a \in A$ *käänteisalkio*, jos $\bar{a} * a = a * \bar{a} = e$.

Esimerkki 1.5. (a) Kuten jo totesimmekin, 0 on luonnollisten lukujen yhteenlaskun neutraalialkio ja 1 on luonnollisten lukujen kertolaskun neutraalialkio. Useimmilla luonnollisilla luvuilla ei ole käänteisalkiota kummankaan laskutoimituksen suhteen.

(b) Identtinen kuvaus $\mathrm{id}\colon X \to X$, $\mathrm{id}(x) = x$, on joukon $\mathscr{F}(X)$ laskutoimituksen $\circ$ neutraalialkio:

$$\mathrm{id} \circ f = f = f \circ \mathrm{id} \qquad \text{kaikilla } f \in \mathscr{F}(X).$$

Jos $f \in \mathscr{F}(X)$ on bijektio, sen käänteiskuvaus f^{-1} on kuvauksen f käänteisalkio laskutoimituksen $\circ$ suhteen: $f \circ f^{-1} = \mathrm{id} = f^{-1} \circ f$. Toisaalta, jos $f \in \mathscr{F}(X)$ ei ole bijektio, ei sillä ole myöskään käänteisalkiota.

(c) Martiisien kertolasku (vrt. LAG1) joukossa $\mathrm{M}_{2\times 2}$ ei ole kommutatiivinen, sillä yleensä $AB \neq BA$. Kertolasku on kuitenkin assosiatiivinen ja lisäksi distributiivinen yhteenlaskun suhteen. Matriisien kertolaskulla on joukossa $\mathrm{M}_{2\times 2}$ myös neutraalialkio

$$I_{2\times 2} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Laskutoimituksia voidaan määritellä useamman joukon karteesiseen tuloon:

Esimerkki 1.6. Luonnollisten lukujen yhteenlaskun avulla saadaan yhteenlasku joukkoon $\mathbb{N} \times \mathbb{N}$: $(m, n) + (p, q) = (m + p, n + q)$.

Luonnollisten lukujen järjestys ' $\leq$ ' on eräs esimerkki *relaatiosta*.

Määritelmä 1.7. *Relaatio* joukossa A on joukon $A \times A$ osajoukko. Jos $\mathrm{R} \subset A \times A$ on relaatio, niin usein merkitään $a \,\mathrm{R}\, b \iff (a, b) \in \mathrm{R}$.

Esimerkki 1.8. (a) Määritellään relaatio R joukossa $\mathbb{N}$ asettamalla

$$a \,\mathrm{R}\, b \Longleftrightarrow b = a + 3p \text{ jollakin } p \in \mathbb{N}.$$

Tämä relaatio liittyy niin sanottuihin *kongruensseihin*; katso myös Esimerkki 1.14.

(b) Määritellään joukossa $\mathscr{P}(X)$ relaatio R asettamalla

$$A \,\mathrm{R}\, B \iff A \cap B \neq \emptyset.$$

Määritelmä 1.9. Joukon A relaatio R on

- *refleksiivinen*, jos $a \,\mathrm{R}\, a$ kaikilla $a \in A$;
- *symmetrinen*, jos kaikilla $a, b \in A$ pätee: $a \,\mathrm{R}\, b \implies b \,\mathrm{R}\, a$,
- *transitiivinen*, jos kaikilla $a, b \in A$ pätee:

$$a \,\mathrm{R}\, b \text{ ja } b \,\mathrm{R}\, c \implies a \,\mathrm{R}\, c;$$

- *antisymmetrinen*, jos kaikilla $a, b \in A$ pätee: $a \,\mathrm{R}\, b$ ja $b \,\mathrm{R}\, a \implies a = b$.

Relaatio on

- *ekvivalenssirelaatio*, jos se on refleksiivinen, symmetrinen ja transitiivinen;
- *osittainen järjestys*, jos se on refleksiivinen, antisymmetrinen ja transitiivinen;
- *täydellinen järjestys*, jos se on osittainen järjestys ja lisäksi kaikille $a, b \in A$ pätee joko $a \,\mathrm{R}\, b$ tai $b \,\mathrm{R}\, a$.

Jos R on täydellinen järjestys joukossa A, niin paria (A, R) sanotaan *täysin järjestetetyksi* joukoksi.

Esimerkki 1.10. (a) Luonnollisten lukujen järjestykselle ' $\leq$ ' pätee

- $n \leq n$ (refleksiivisyys)
- $n \leq m,\ m \leq n \implies m = n$ (antisymmetrisyys)
- $n \leq m,\ m \leq p \implies n \leq p.$ (transitiivisuus)

Lisäksi aina joko $n \leq m$ tai $m \leq n$, joten ' $\leq$ ' on joukon $\mathbb{N}$ täydellinen järjestys.

(b) Joukon X potenssijoukon $\mathscr{P}(X)$ relaatio ' $\subset$ ' on osittainen, mutta ei täydellinen järjestys:

- $A \subset A$
- $A \subset B,\ B \subset A \implies A = B$
- $A \subset B,\ B \subset C \implies A \subset C,$

mutta joukoille $A, B \in \mathscr{P}(X)$ ei välttämättä päde $A \subset B$ tai $B \subset A$ (mieti esimerkki!).

Huomioita: (i) Jos $a \leq b$, voidaan käyttää myös merkintää $b \geq a$.

(ii) Jos ' $\leq$ ' on osittainen järjestys, niin usein käytetään myös relaatiota

$$a < b \iff a \leq b \text{ ja } a \neq b.$$

Huomaa, että ‘ $<$ ‘ ei ole Määritelmän 1.9 mielessä järjestysrelaatio, sillä se ei ole refleksiivinen.

Ekvivalenssirelaatiota merkitään usein symbolilla ‘ $\sim$ ‘ eli jos (a, b) on kyseisen relaation alkio, niin merkitään $a \sim b$. Jos $\sim$ on ekvivalenssirelaatio, niin jokainen joukon A alkio a määrää *ekvivalenssiluokan*

$$[a] = \{b \in A : a \sim b\}.$$

Joukon A alkioiden määräämät ekvivalenssiluokat muodostavat uuden joukon, jota kutsutaan ekvivalenssirelaatiota $\sim$ vastaavaksi A:n *tekijäjoukoksi* ja merkitään $A/\sim$.

Lemma 1.11. *Olkoon $\sim$ joukon A ekvivalenssirelaatio ja olkoot $a, b \in A$. Tällöin*

$$a \sim b \iff [a] = [b].$$

Todistus. Harjoitustehtävä. □

Esimerkki 1.12. (a) Helpoin esimerkki ekvivalenssirelaatiosta on luonnollisten lukuejen relaatio ‘ $=$ ‘. Tällöin $[n] = \{n\}$ kaikilla $n \in \mathbb{N}$.

(b) Joukon $\mathbb{N} \times \mathbb{N}$ relaatio

$$(m, n) \sim (p, q) \iff m = p$$

on ekvivalenssirelaatio. Tekijäjoukko $(\mathbb{N} \times \mathbb{N})/\sim$ voidaan samastaa (”luonnollisella tavalla”) joukon $\mathbb{N}$ kanssa: alkiota $n \in \mathbb{N}$ vastaa ekvivalenssiluokka $[(n, 0)] = \{(n, m) : m \in \mathbb{N}\}$.

(c) Myös joukon $\mathbb{N} \times \mathbb{N}$ relaatio

$$(m, n) \sim (p, q) \iff mq = np$$

on ekvivalenssirelaatio. Tällä lausekkeella määriteltyä ekvivalenssirelaatiota tullaan tarvitsemaan myöhemmin rationaalilukujen konstruktion yhteydessä.

(d) Esimerkin 1.8 (b)-kohdan relaatio ei ole ekvivalenssirelaatio. Se on kyllä refleksiivinen ja symmetrinen, mutta ei transitiivinen.

Määritelmä* ja Lause* 1.13. [1] Jos $*$ on laskutoimitus ja $\sim$ on ekvivalenssirelaatio joukossa A, ne ovat *yhteensopivat*, jos $a * b \sim a' * b'$ aina kun $a \sim a'$ ja $b \sim b'$. Tällöin laskutoimitus $*$ määrää *tekijälaskutoimituksen* $*$ joukossa $A/\sim$ säännöllä $[a] * [b] = [a * b]$.

Esimerkki* 1.14. Olkoon relaatio $\equiv$ kokonaislukujen joukossa $\mathbb{Z}$ määritelty säännöllä $a \equiv b$, jos on $k \in \mathbb{Z}$ siten, että $b = a + 3k$. Tällöin $\equiv$ on ekvivalenssirelaatio:

(1) $a = a + 3 \cdot 0$ kaikilla $a \in \mathbb{Z}$,
(2) jos $b = a + 3k$ jollain $k \in \mathbb{Z}$, niin $a = b + 3 \cdot (-k)$,
(3) jos $b = a + 3k$ ja $c = b + 3n$ joillain $k, n \in \mathbb{Z}$, niin $c = a + 3(k + n)$.

Ekvivalenssirelaatiota $\equiv$ kutsutaan *kongruenssiksi*. Yhteenlasku on yhteensopiva ekvivalenssirelaation $\equiv$ kanssa: Jos $a' = a + 3m$ ja $b' = b + 3n$, niin

$$a' + b' = a + b + 3(m + n).$$

Siis kokonaislukujen yhteenlasku määrää laskutoimituksen kolmen alkion joukolla

$$\mathbb{Z}/\equiv \; = \{[0], [1], [2]\}.$$

[1] Tällaiset *:llä merkityt kohdat ovat lisätietoa, joka ei varsinaisesti kuulu kurssin sisältöön ja/tai vaatimuksiin

2. Kokonaisluvut

Useimmilla luonnollisilla luvuilla ei siis ole käänteisalkiota yhteen- ja/tai kertolaskun suhteen. Tämä on läheisessä yhteydessä siihen, etteivät vähennys- ja jakolaskut ole Määritelmän 1.1 mukaisia luonnollisten lukujen laskutoimituksia (koska niiden tulokset eivät ole aina luonnollisia lukuja). Tässä mielessä luonnollisten lukujen joukko on "liian pieni" näiden laskutoimitusten suhteen.

Laajennamme aluksi lukualuetta $\mathbb{N}$ siten, että jokaisella alkiolla on tässä uudessa struktuurissa eli kokonaislukujen joukossa $\mathbb{Z}$ käänteisalkio yhteenlaskun suhteen. Tällöin myös vähennyslasku voidaan määritellä lukualueessa $\mathbb{Z}$.

Ideana on määritellä kokonaisluvut "luonnollisten lukujen muodollisina erotuksina". Jos m ja n ovat luonnollisia lukuja ja $m \geq n$, niin erotus $m-n$ on olemassa luonnollisena lukuna; se on yhtälön $n+x=m$ ratkaisu $x \in \mathbb{N}$. Toisaalta tämä sama luonnollinen luku x voidaan esittää erotuksena äärettömän monella eri tavalla. Erityisesti huomataan, että

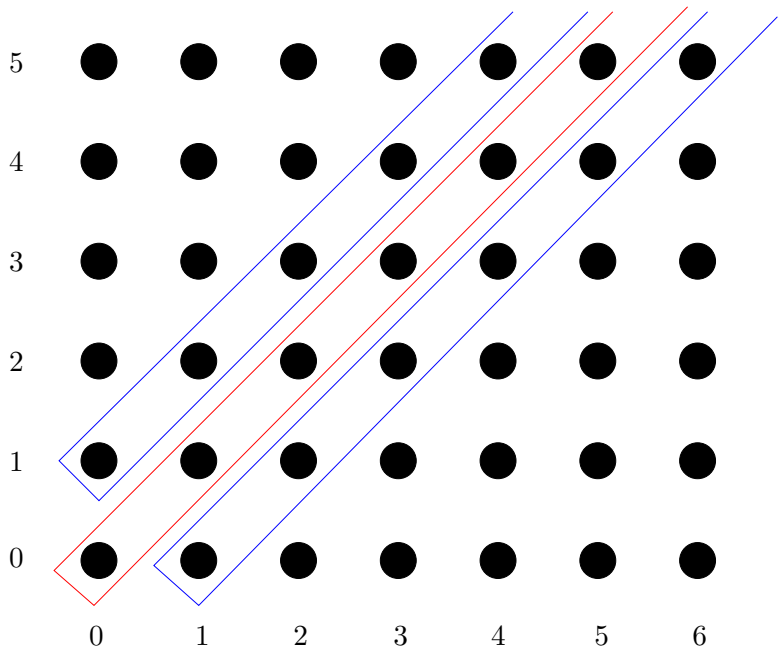
$$m-n=p-q \iff m+q=p+n.$$

Mutta tässä oikealla puolella esiintyy vain luonnollisten lukujen yhteenlasku, joten oikean puolen yhtälö on määritelty kaikille $m,n,p,q \in \mathbb{N}$, riippumatta siitä onko $m \geq n$ ja $p \geq q$.

Tämän havainnon opastamana määrittelemme joukkoon $\mathbb{N} \times \mathbb{N}$ relaation $\sim$ asettamalla

$$(m,n) \sim (p,q) \iff m+q=p+n. \tag{1}$$

Havainnollisesti tämä siis tarkoittaa juuri sitä, että luvuilla m ja n on sama "erotus" kuin luvuilla p ja q.



Kuva 1. Relaation $\sim$ luokat $[(0,1)]$, $[(0,0)]$ ja $[(1,0)]$.

Lemma 2.1. *Kaavalla* (1) *määritelty relaatio* $\sim$ *on joukon* $\mathbb{N}\times\mathbb{N}$ *ekvivalenssirelaatio.*

Todistus. Olkoot $m, n, p, q, r, s \in \mathbb{N}$. Tällöin:

(1) $(m, n) \sim (m, n)$, koska $m + n = m + n$.

(2) $(m, n) \sim (p, q) \iff m + q = p + n \iff p + n = m + q \iff (p, q) \sim (m, n)$.

(3) $(m, n) \sim (p, q) \implies m+q = p+n$ ja $(p, q) \sim (r, s) \implies p+s = r+q$. Laskemalla nämä yhtälöt yhteen saadaan

$$(m + q) + (p + s) = (p + n) + (r + q)$$

ja niinpä

$$(m + s) + (p + q) = (r + n) + (p + q).$$

Luonnollisten lukujen yhteenlaskun ominaisuuksien nojalla (huomaa, että tässä ei tarvita vähennyslaskua) tästä seuraa, että $m + s = r + n$, joten relaation $\sim$ määritelmän nojalla $(m, n) \sim (r, s)$.

Olemme osoittaneet, että $\sim$ on refleksiivinen, symmetrinen ja transitiivinen, joten se on ekvivalenssirelaatio. □

Nyt voimme määritellä kokonaislukujen joukon ekvivalenssirelaatiota $\sim$ vastaavana tekijäjoukkona:

Määritelmä 2.2. *Kokonaislukujen joukko* on

$$\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\sim,$$

missä siis $(m, n) \sim (p, q) \iff m + q = p + n$. Merkitsemme parin $(m, n) \in \mathbb{N} \times \mathbb{N}$ määräämää ekvivalenssiluokkaa jatkossa lyhyesti vain $[m, n] = [(m, n)] \in \mathbb{Z}$.

Kokonaislukujen *yhteenlasku* määritellään asettamalla

$$[m, n] + [p, q] = [m + p, n + q] \tag{2}$$

ja *kertolasku* asettamalla

$$[m, n] \cdot [p, q] = [mp + nq, mq + np]. \tag{3}$$

HUOMAUTUKSIA: (i) Laskutoimitusten määritelmät ovat "järkeviä": Kun $[m, n]$ ajatellaan erotuksena $m - n$, niin lausekkeet (2) ja (3) vastaavat lausekkeita

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

ja

$$(m - n)(p - q) = (mp + nq) - (mq + np).$$

(ii) Kokonaislukujen laskutoimitukset ovat *hyvin määriteltyjä*. Tämä tarkoittaa sitä, että laskutoimitusten tulokset eivät riipu ekvivalenssiluokasta valituista edustajista. Todistamme tämän yhteenlaskulle:

Oletetaan, että $(m', n') \in [m, n]$ ja $(p', q') \in [p, q]$, jolloin relaation $\sim$ määritelmän mukaan pätee

$$m + n' = m' + n \quad \text{ja} \quad p + q' = p' + q. \tag{4}$$

Koska yhteenlasku määriteltiin asettamalla $[m, n] + [p, q] = [m + p, n + q]$, niin nyt täytyy siis osoittaa, että

$$[m + p, n + q] = [m' + p', n' + q']. \tag{5}$$

Laskemalla kohdan (4) yhtälöt yhteen saadaan

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

eli

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

Mutta tällöinhän $(m+p,n+q)\sim(m'+p',n'+q')$, mistä (5) seuraa Lemman 1.11 nojalla.

Kertolasku käsitellään harjoitustehtävänä.

HUOMAUTUS*: Edellisen huomautuksen (ii)-kohdan tulos voidaan ilmaista myös seuraavasti: Kohdassa 1.6 määritelty joukon $\mathbb{N}\times\mathbb{N}$ laskutoimitus

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

on yhteensopiva kokonaisluvut määrittelevän ekvivalenssirelaation $\sim$ kanssa, jolloin kokonaislukujen yhteenlasku saadaan vastaavana tekijälaskutoimituksena (vertaa kohtaan 1.13).

Luonnollisten lukujen laskutoimitusten ominaisuudet yleistyvät myös kokonaisluvuille ja lisäksi kaikille kokonaisluvuille saadaan käänteisalkio yhteenlaskun suhteen:

Lause 2.3. (a) *Kokonaislukujen yhteenlasku ja kertolasku ovat assosiatiivisia eli*

$$a+(b+c)=(a+b)+c$$
$$a(bc)=(ab)c$$

kaikilla $a,b,c\in\mathbb{Z}$.

(b) *Kokonaislukujen yhteenlasku ja kertolasku ovat kommutatiivisia eli*

$$a+b=b+a$$
$$ab=ba$$

kaikilla $a,b\in\mathbb{Z}$.

(c) *Kokonaislukujen kertolasku on distributiivinen yhteenlaskun suhteen eli*

$$(a+b)c=ac+bc$$

kaikilla $a,b,c\in\mathbb{Z}$.

(d) *Kokonaislukujen yhteenlaskun neutraalialkio on* $[0,0]$ *ja kertolaskun neutraalialkio on* $[1,0]$.

(e) *Jokaisella alkiolla* $[m,n]\in\mathbb{Z}$ *on vastaluku* $[n,m]\in\mathbb{Z}$ *(eli käänteisalkio yhteenlaskun suhteen):*

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

Todistus. (a) Todistetaan yhteenlaskun assosiatiivisuus. Olkoot $a=[m,n]$, $b=[p,q]$ ja $c=[r,s]$ kokonaislukuja. Käyttäen hyväksi luonnollisten lukujen yhteenlaskun assosiatiivisuutta saamme

$$\begin{aligned}(a+b)+c&=[m+p,n+q]+[r,s]=[(m+p)+r,(n+q)+s]\\&=[m+(p+r),n+(q+s)]=[m,n]+[p+r,q+s]\\&=a+(b+c).\end{aligned}$$

Kertolaskun käsittely jätetään harjoitustehtäväksi.

(b) Harjoitustehtävä.

(c) Harjoitustehtävä.

(d) $[m,n]+[0,0]=[m,n]$ ja $[m,n][1,0]=[m+0,0+n]=[m,n]$.

(e) Nyt $[m,n]+[n,m]=[m+n,n+m]$. Toisaalta kaikilla $k\in\mathbb{N}$ pätee $(k,k)\sim(0,0)$ (sillä $k+0=0+k$), joten $[k,k]=[0,0]$ ja erityisesti $[m+n,n+m]=[0,0]$. Siispä $[m,n]+[n,m]=[0,0]$. □

MERKINTÄ: Merkitsemme kokonaisluvun $a=[m,n]\in\mathbb{Z}$ vastalukua $-a$, jolloin lauseen 2.3 perusteella $-a=[n,m]$. Huomaa, että tällöin $-a=[0,1][m,n]$.

Määritelmä 2.4. Määrittelemme kokonaislukujen *vähennyslaskun* $-:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$ asettamalla $a-b=a+(-b)$.

Kokonaislukujen kertolaskun suhteen käänteisalkio on olemassa ainoastaan luvuilla $[1,0]$ ja $[0,1]$ (totea!), joten kerto- ja jakolaskujen suhteen $\mathbb{Z}$ on vielä liian pieni lukualue; tähän ongelmaan palaamme myöhemmin.

Haluamme, että kokonaislukujen joukko on luonnollisten lukujen joukon laajennus, joten joukon $\mathbb{N}$ tulisi olla joukon $\mathbb{Z}$ osajoukko. Kuitenkin $\mathbb{Z}$ on määritelty joukon $\mathbb{N}\times\mathbb{N}$ abstraktina tekijäjoukkona, eikä $\mathbb{N}$ ole tämän joukon osajoukko. Voimme kiertää tämän ongelman tekemällä matematiikassa hyvin usein käytetyn tempun: samastamme joukon $\mathbb{N}$ sopivan (joukon $\mathbb{N}$ kanssa bijektiivisen) kokonaislukujen osajoukon kanssa.

Lause 2.5. *Määritellään kuvaus* $i\colon\mathbb{N}\to\mathbb{Z}$ *asettamalla* $i(n)=[n,0]$. *Tällöin* i *on injektio, jolle pätee*

$$i(m+n)=i(m)+i(n)\quad \textit{ja}\quad i(mn)=i(m)i(n)$$

kaikilla $m,n\in\mathbb{N}$.

Todistus. Todistetaan aluksi injektiivisyys: Jos $i(n)=i(m)$, niin $[n,0]=[m,0]$. Mutta tällöin $n+0=m+0$, joten $n=m$. Siispä i on injektio.

Olkoot sitten $m,n\in\mathbb{N}$. Tällöin

$$i(m+n)=[m+n,0]=[m,0]+[n,0]=i(m)+i(n)$$

ja vastaavasti

$$i(mn)=[mn,0]=[m,0][n,0]=i(m)i(n).$$

□

Lauseen 2.5 mukaan kuvauksesta i saadaan bijektio $i\colon\mathbb{N}\to i(\mathbb{N})\subset\mathbb{Z}$, joka "säilyttää laskutoimitukset" eli ei ole merkitystä lasketaanko luvut m ja n yhteen tai kerrotaanko ne luonnollisina lukuina vai vastaavina kokonaislukuina $[m,0]$ ja $[n,0]$.

Luonnollisten lukujen järjestysrelaatio ' $\leq$ ' voidaan myös laajentaa kokonaislukujen joukkoon $\mathbb{Z}$. Muista, että joukon X relaatio R on osittainen järjestys, jos se on refleksiivinen, antisymmetrinen ja transitiivinen. Jos lisäksi kaikille $a,b\in X$ pätee $a\,\mathrm{R}\,b$ tai $b\,\mathrm{R}\,a$, niin R on täydellinen järjestys. Jos R on täydellinen järjestys joukossa X, niin (X,R) on täysin järjestetty.

Määritelmä 2.6. Määritellään joukon $\mathbb{Z}$ relaatio ' $\leq$ ' asettamalla

$$[m,n]\leq[p,q]\iff m+q\leq p+n.$$

HUOMIOITA: (i) Huomaa, että oikealla puolella esiintyy vain joukon $\mathbb{N}$ järjestys ' $\leq$ '.

(ii) Kun $[m,n]$ ajatellaan erotukseksi $m-n$, niin määritelmä sanoo:

$$m-n\leq p-q\iff m+q\leq p+n.$$

Lause 2.7. *Edellä määritelty relaatio ‘ $\leq$ ‘ on kokonaislukujen joukon $\mathbb{Z}$ täydellinen järjestys. Lisäksi kaikilla $m, n \in \mathbb{N}$ pätee*

$$i(m) \leq i(n) \iff m \leq n.$$

Todistus. (1) Osoitetaan aluksi, että relaatio ‘ $\leq$ ‘ on hyvin määritelty: Olkoon $[m, n] \leq [p, q]$ ja olkoot $(m', n') \in [m, n]$ ja $(p', q') \in [p, q]$. Tällöin siis $m+q \leq p+n$, ja toisaalta $m+n' = m'+n$, $p+q' = p'+q$, ja pitää osoittaa, että myös $m'+q' \leq p'+n'$. Mutta näin on, sillä

$$\begin{aligned}(m' + q') + (p + n) &= (m' + n) + (p + q') = (m + n') + (p' + q) \\ &= (m + q) + (p' + n') \leq (p + n) + (p' + n').\end{aligned}$$

(2) Tarkistetaan sitten, että osittaisen järjestyksen vaatimukset täyttyvät:

- $[m, n] \leq [m, n]$ on selvä;
- Jos $[m, n] \leq [p, q]$ ja $[p, q] \leq [m, n]$, niin $m + q \leq p + n$ ja $m + q \geq p + n$, joten luonnollisten lukujen järjestyksen ‘ $\leq$ ‘ antisymmetrisyyden perusteella $m + q = p + n$ eli $[m, n] = [p, q]$;
- Jos $[m, n] \leq [p, q]$ ja $[p, q] \leq [r, s]$, niin $m + q \leq p + n$ ja $p + s \leq r + q$, jolloin

  $$m + q + p + s \leq p + n + r + q,$$

  mistä seuraa $m + s \leq r + n$ eli $[m, n] \leq [r, s]$.

(3) Olkoot $[m, n], [p, q] \in \mathbb{Z}$. Koska ‘ $\leq$ ‘ on joukon $\mathbb{N}$ täydellinen järjestys, niin nyt joko $m + q \leq p + n$ tai $m + q \geq p + n$, joten $[m, n] \leq [p, q]$ tai $[m, n] \geq [p, q]$. Siten ‘ $\leq$ ‘ on joukon $\mathbb{Z}$ täydellinen järjestys.

(4) Olkoot $m, n \in \mathbb{N}$. Tällöin

$$i(m) \leq i(n) \iff [m, 0] \leq [n, 0] \iff m + 0 \leq n + 0 \iff m \leq n.$$

□

Määritellään nyt *positiivisten kokonaislukujen* joukko $\mathbb{Z}_+$ asettamalla

$$\mathbb{Z}_+ = \{[k, 0] \in \mathbb{Z} : k \in \mathbb{N},\ k \neq 0\}.$$

Joukkoa

$$-\mathbb{Z}_+ = \{[0, k] : k \in \mathbb{N},\ k \neq 0\}$$

sanotaan puolestaan *negatiivisten kokonaislukujen joukoksi.* Merkitään lisäksi $0 = [0, 0] \in \mathbb{Z}$. Tällöin seuraavat ominaisuudet pätevät:

Lemma 2.8. (a) *Kun $a, b \in \mathbb{Z}_+$, niin $a + b \in \mathbb{Z}_+$ ja $ab \in \mathbb{Z}_+$.*

(b) $\mathbb{Z} = -\mathbb{Z}_+ \cup \{0\} \cup \mathbb{Z}_+$.

(c) $\mathbb{Z}_+ \cap -\mathbb{Z}_+ = \emptyset$.

(d) *Kaikilla $a \in \mathbb{Z}$ pätee $a^2 \in \mathbb{Z}_+ \cup \{0\}$.*

Todistus. (a) Olkoot $a = [m, 0],\ b = [n, 0]$, $m, n \in \mathbb{N}$. Tällöin $a + b = [m + n, 0]$. Koska $m + n \in \mathbb{N}$ ja $m + n \neq 0$, niin $a + b \in \mathbb{Z}_+$. Samoin $ab = [mn, 0] \in \mathbb{Z}_+$.

(b) Olkoon $a = [m, n] \in \mathbb{Z}$. Jos $m = n$, niin $a = 0$ (vertaa Lauseen 2.3 kohdan (e) todistukseen). Jos taas $m > n$, niin on olemassa $k \in \mathbb{N}$, $k \geq 1$, siten, että $m = n + k$. Mutta tällöin $m + 0 = k + n$ eli $[m, n] = [k, 0]$, joten $a \in \mathbb{Z}_+$. Vastaavasti, jos $m < n$, niin löytyy $k \in \mathbb{N}$, $k \geq 1$, siten, että $m + k = 0 + n$. Tällöin $[m, n] = [0, k]$, joten

$a \in -\mathbb{Z}_+$. Koska joku edellä käsitellyistä vaihtoehdoista on aina voimassa, niin väite seuraa.

(c) Harjoitustehtävä.

(d) Harjoitustehtävä. □

SOPIMUS: Tästedes samastamme lukualueen $\mathbb{N}$ vastaavan kokonaislukujen osajoukon $i(\mathbb{N}) = \mathbb{Z}_+ \cup \{0\}$ kanssa ja merkitsemme kaikilla $n \in \mathbb{N}$

$$n = [n, 0] \in \mathbb{Z}.$$

Tällä tulkinnalla luonnollisten lukujen joukosta $\mathbb{N}$ tulee kokonaislukujen joukon $\mathbb{Z}$ osajoukko. Lauseen 2.8 perusteella jokainen nollasta poikkeava kokonaisluku on joko positiivinen kokonaisluku (ja siten luonnollinen luku) tai jonkun positiivisen kokonaisluvun vastaluku eli negatiivinen kokonaisluku. Merkitsemmekin jatkossa kaikilla $n \in \mathbb{N}$

$$-n = [0, n] \in \mathbb{Z}.$$

HUOMAUTUKSIA: (i) Kun $[m, n] \in \mathbb{Z}$, niin edellistä merkintää käyttäen voimme kirjoittaa, että

$$[m, n] = [m, 0] + [0, n] = m + (-n) = m - n$$

eli luku $[m, n]$ *on* todella erotus $m - n$.

(ii) Kokonaislukujen järjestys voitaisiin määritellä myös joukon $\mathbb{Z}_+$ avulla, sillä kaikilla $a, b \in \mathbb{Z}$ pätee

$$a \leq b \iff b - a \in \mathbb{Z}_+ \cup \{0\} \quad (= \mathbb{N})$$

tai yhtäpitävästi (ja tässä yhteydessä luonnollisemmin)

$$a < b \iff b - a \in \mathbb{Z}_+ ;$$

yksityiskohdat jätetään harjoitustehtäväksi.

Todistetaan vielä muutamia hyödyllisiä kokonaislukujen laskutoimitusten ominaisuuksia.

Lemma 2.9. (a) *Jos* $a, b, c \in \mathbb{Z}$ *ja* $a + c = b + c$, *niin* $a = b$.

(b) *Jos* $a, b \in \mathbb{Z}$ *ja* $ab = 0$, *niin* $a = 0$ *tai* $b = 0$.

(c) *Jos* $a, b \in \mathbb{Z}$, $c \in \mathbb{Z} \setminus \{0\}$ *ja* $ac = bc$, *niin* $a = b$.

Todistus. (a) Koska $c + (-c) = 0$, niin oletusta $a + c = b + c$ käyttäen saamme

$$\begin{aligned} a = a + 0 = a + (c + (-c)) = (a + c) + (-c) \\ = (b + c) + (-c) = b + (c + (-c)) = b. \end{aligned}$$

(b) Jos $a = 0$, niin väite seuraa, joten voimme olettaa, että $a \neq 0$. Lemman 2.8 perusteella nyt löytyy $k \in \mathbb{N}$, $k \geq 1$, siten, että $a = [k, 0]$ tai $a = [0, k]$. Olkoon nyt $b = [p, q] \in \mathbb{Z}$. Jos $a = [k, 0]$, niin

$$[0, 0] = ab = [k, 0][p, q] = [kp, kq],$$

joten $kp = kq$. Koska $k \geq 1$, niin tästä seuraa $\mathbb{N}$:n kertolaskun ominaisuuksien perusteella että $p = q$, jolloin $b = [p, p] = 0$. Tapaus $a = [0, k]$ käsitellään aivan vastaavasti.

(c) Seuraa (a)- ja (b)-kohdista; harjoitustehtävä. □

———————

HISTORIAA: Negatiivisia kokonaislukuja tavataan jo hyvin varhaisissa kiinalaisissa ja intialaisissa lähteissä, yleensä kuvaamaan velkaa. Ensimmäinen (tunnettu) järjestelmällinen negatiivisten lukujen (ja nollan!) aritmetiikan esitys löytyy intialaisen Brahmaguptan (598–670) töistä. Intiasta negatiiviset luvut levisivät hitaasti Arabiaan ja edelleen Eurooppaan, mutta niiden käyttö oli aluksi hyvin varautunutta. Esimerkiksi algebrallisten yhtälöiden negatiiviset juuret jätettiin systemaattisesti huomioimatta vielä 1500-luvulla. Ensimmäisiä uuden ajan matemaatikkoja, jotka käsittelivät negatiivia lukuja luonnollisena osana lukujärjestelmää, olivat Michael Stifel (1487–1567, Saksa) ja Rafael Bombelli (1526–1572, Italia). Yhtälöiden negatiiviset ratkaisut ovat lisäksi esillä ainakin Thomas Harriotin (1560–1621, Englanti) ja Albert Giraldin (1595–1632, Ranska/Hollanti) töissä, jotka eivät kuitenkaan tulleet omana aikanaan kovin tunnetuiksi. Girald oli ilmeisesti myös ensimmäisiä, joka esitti ajatuksen, että negatiiviset luvut asettuvat "vastakkaiseen suuntaan" positiivilukuihin nähden. Tämä käsitys yleistyi 1600- ja 1700-luvuilla, kun analyyttisessä geometriassa alettiin käyttää koordinaattiakseleita, joissa esiintyi myös negatiivisia lukuja. Epäluulo negatiivisia lukuja kohtaan oli kuitenkin hyvin yleistä vielä 1700- ja 1800-luvuillakin.

Idea negatiivisten kokonaislukujen määrittelemisestä luonnollisten lukujen parien ekvivalenssiluokkina on peräisin Leopold Kroneckerilta (1823–1891, Saksa) vuodelta 1887. Hänen esityksensä tosin poikkesi jonkin verran tällä kurssilla käyttämästämme, jota lähempänä on Rickhard Dedekindin (1831–1916, Saksa) määritelmä vuodelta 1913.

3. RATIONAALILUVUT

Ainoat kokonaisluvut, joilla on käänteisluku kertolaskun suhteen, ovat 1 ja -1. Toisaalta jakolasku onnistuu joillekin kokonaisluvuille, mutta ei kaikille. Jos kuitenkin $a, b, c, d \in \mathbb{Z}$ ja osamäärät $\frac{a}{b}$ ja $\frac{c}{d}$ ovat kokonaislukuja, niin

$$\frac{a}{b} = \frac{c}{d} \iff ad = bc;$$

esimerkiksi

$$\frac{12}{3} = \frac{8}{2} \iff 12 \cdot 2 = 3 \cdot 8.$$

Tämä havainto johtaa meidät määrittelemään rationaaliluvut kokonaislukujen "muodollisten osamäärien" avulla, samaan tapaan kuin kokonaisluvut määriteltiin luonnollisten lukujen "muodollisina erotuksina".

Merkitään $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ ja määritellään relaatio $\sim$ joukossa $\mathbb{Z} \times \mathbb{Z}^*$ asettamalla

$$(a, b) \sim (c, d) \iff ad = bc. \tag{6}$$

Lemma 3.1. *Kaavalla* (6) *määritelty relaatio* $\sim$ *on joukon* $\mathbb{Z} \times \mathbb{Z}^*$ *ekvivalenssirelaatio.*

Todistus. Olkoot $a, c, e \in \mathbb{Z}$ ja $b, d, f \in \mathbb{Z}^*$. Tällöin:

(1) $(a, b) \sim (a, b)$, koska $ab = ba$.

(2) $(a, b) \sim (c, d) \iff ad = bc \iff cb = da \iff (c, d) \sim (a, b)$.

(3) $(a, b) \sim (c, d) \implies ad = bc$ ja $(c, d) \sim (e, f) \implies cf = de$. Kertomalla nämä yhtälöt puolittain saadaan

$$(ad)(cf) = (bc)(de),$$

ja niinpä

$$(af)(cd) = (be)(cd).$$

Jos nyt $cd \neq 0$, niin Lemman 2.9 (c)-kohdan nojalla $af = be$, jolloin siis $(a,b) \sim (e,f)$. Jos taas $cd = 0$, niin Lemman 2.9 (b)-kohdan perusteella $c = 0$ (koska $d \in \mathbb{Z}^*$), joten myös

$$ad = bc = 0 \quad \text{ja} \quad de = cf = 0.$$

Koska edelleen $d \neq 0$, niin $a = 0$ ja $e = 0$. Niinpä $af = 0 = be$, joten tässäkin tapauksessa $(a,b) \sim (e,f)$.

Koska $\sim$ on refleksiivinen, symmetrinen ja transitiivinen, on se ekvivalenssirelaatio. □

Määritelmä 3.2. *Rationaalilukujen joukko* on

$$\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}^*)/\sim,$$

missä siis $(a,b) \sim (c,d) \iff ad = bc$. Alkion $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$ määräämää ekvivalenssiluokkaa merkitään jälleen lyhyesti $[a,b] = [(a,b)] \in \mathbb{Q}$.

Rationaalilukujen *yhteenlasku* määritellään asettamalla

$$[a,b] + [c,d] = [ad + bc, bd]$$

ja *kertolasku*

$$[a,b][c,d] = [ac, bd].$$

HUOMAUTUKSIA: (i) Koska rationaaliluvut määrittelevä ekvivalenssirelaatio pohjautuu kokonaislukujen kertolaskuun, tulee rationaalilukujen kertolaskusta "luonnollisemman näköinen" kuin yhteenlaskusta.

(ii) Laskutoimitukset on jälleen määritelty "järkevästi" : Kun rationaaliluku $[a,b]$ ajatellaan osamääränä $\frac{a}{b}$, niin yhteenlasku saa muodon

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

ja kertolasku muodon

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

(iii) Rationaalilukujen laskutoimitukset ovat hyvin määriteltyjä. Näytetään tämä yhteenlaskulle: Olkoot siis $(a',b') \in [a,b]$ ja $(c',d') \in [c,d]$. Pitää osoittaa, että

$$[a'd' + b'c', b'd'] = [ad + bc, bd]$$

eli että

$$(a'd' + b'c')(bd) = (b'd')(ad + bc)$$

eli yhtäpitävästi

$$a'd'bd + b'c'bd = b'd'ad + b'd'bc. \tag{7}$$

Mutta koska $a'b = b'a$ ja $c'd = d'c$, niin

$$a'd'bd = (a'b)(d'd) = (b'a)(d'd) = b'd'ad$$

ja

$$b'c'bd = (c'd)(b'b) = (d'c)(b'b) = b'd'bc,$$

joten yhtälö (7) pitää paikkansa, ja siten väite on todistettu.

Kertolasku jätetään harjoitustehtäväksi.

MERKINTÄ: Merkitsemme jatkossa usein $[p,q] = \frac{p}{q} = p/q$. Muista kuitenkin, että tarkoitamme tällä merkinnällä parin $(p,q) \in \mathbb{Z} \times \mathbb{Z}^*$ määräämää ekvivalenssiluokkaa.

Kaikki kokonaislukujen laskutoimitusten hyvät ominaisuudet pätevät myös rationaalilukujen laskutoimituksille, ja lisäksi jokaiselle nollasta poikkeavalle rationaaliluvulle saadaan käänteisalkio kertolaskun suhteen:

Lause 3.3. (a) *Rationaalilukujen yhteenlasku ja kertolasku ovat assosiatiivisia.*

(b) *Rationaalilukujen yhteenlasku ja kertolasku ovat kommutatiivisia.*

(c) *Rationaalilukujen kertolasku on distributiivinen yhteenlaskun suhteen.*

(d) *Rationaalilukujen yhteenlaskun neutraalialkio on* $0 = [0,1]$ *ja kertolaskun neutraalialkio on* $1 = [1,1]$.

(e) *Jokaisella* $[p,q] \in \mathbb{Q}$ *on vastaluku* $[-p,q] \in \mathbb{Q}$ *(eli käänteisalkio yhteenlaskun suhteen):*

$$[p,q] + [-p,q] = [0,1].$$

(f) *Jokaisella* $[p,q] \in \mathbb{Q} \setminus \{[0,1]\}$ *on käänteisluku* $[q,p] \in \mathbb{Q} \setminus \{[0,1]\}$ *(eli käänteisalkio kertolaskun suhteen):*

$$[p,q][q,p] = [1,1].$$

Todistus. (a) Seuraa melko suoraan kokonaislukujen laskutoimitusten assosiatiivisuudesta; esimerkiksi

$$[a,b]\big([c,d][e,f]\big) = [a,b][ce,df] = [a(ce),b(df)] = [(ac)e,(bd)f] = \dots$$

(b) Seuraa melko suoraan kokonaislukujen laskutoimitusten kommutatiivisuudesta; esimerkiksi

$$[a,b] + [c,d] = [ad+bc,bd] = [cb+da,db] = [c,d] + [a,b].$$

(c) Harjoitustehtävä.

(d) Helppo lasku.

(e) Tässä riittää huomata, että $[0,m] = [0,1]$ kaikille $m \in \mathbb{Z}^*$.

(f) Tässä riittää huomata, että $[m,m] = [1,1]$ kaikille $m \in \mathbb{Z}^*$. □

Huomautus: Nollalla $0 = [0,1]$ ei voi olla käänteislukua, koska kaikilla $[p,q] \in \mathbb{Q}$

$$[0,1][p,q] = [0 \cdot p, 1 \cdot q] = [0,q] \neq [1,1] = 1.$$

Merkintä: Merkitsemme luvun $a = [p,q] \in \mathbb{Q}$ vastalukua $-a = [-p,q]$ ja käänteisalkiota $\frac{1}{a} = a^{-1} = [q,p]$.

Määritelmä 3.4. (1) Määrittelemme uuden laskutoimituksen, *jakolaskun*, joukossa $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ asettamalla $a/b = a \cdot b^{-1}$ kaikille $a,b \in \mathbb{Q}^*$, missä b^{-1} on siis rationaaliluvun $b \neq 0$ käänteisluku. Käytämme myös merkintää $\frac{a}{b} = a/b$.

(2) Rationaalilukujen vähennyslasku määritellään asettamalla $a-b = a+(-b)$ kaikille $a,b \in \mathbb{Q}$.

Edellisessä luvussa samastimme luonnollisten lukujen joukon $\mathbb{N}$ lukualueen $\mathbb{Z}$ osajoukoksi. Nyt haluamme tehdä saman joukolle $\mathbb{Z}$ uuden lukualueen $\mathbb{Q}$ suhteen. Tätä varten määrittelemme kuvauksen $j\colon \mathbb{Z} \to \mathbb{Q}$ asettamalla $j(m) = [m,1]$.

Lemma 3.5. *Kuvaus* j *on injektio, jolle pätee*

$$j(m+n) = j(m) + j(n) \quad ja \quad j(mn) = j(m)j(n)$$

kaikilla $m,n \in \mathbb{Z}$.

Todistus. Samaan tapaan kuin Lause 2.5 (Harjoitustehtävä). □

Rationaalilukujen järjestyksen määrittelemistä varten otamme käyttöön *positiivisten rationaalilukujen joukon*

$$\mathbb{Q}_+ = \left\{ \frac{m}{n} \in \mathbb{Q} : m, n \in \mathbb{Z}_+ \right\}.$$

Vastaavasti *negatiivisten rationaalilukujen joukko* on

$$-\mathbb{Q}_+ = \left\{ \frac{-m}{n} \in \mathbb{Q} : m, n \in \mathbb{Z}_+ \right\}.$$

Muista, että $\frac{m}{n} = [m, n]$. Joukolla $\mathbb{Q}_+$ on samankaltaisia ominaisuuksia kuin positiivisten kokonaislukujen joukolla $\mathbb{Z}_+$:

Lemma 3.6. (a) *Jos* $a, b \in \mathbb{Q}_+$, *niin* $a + b \in \mathbb{Q}_+$ *ja* $ab \in \mathbb{Q}_+$.

(b) $\mathbb{Q} = -\mathbb{Q}_+ \cup \{0\} \cup \mathbb{Q}_+$.

(c) $\mathbb{Q}_+ \cap -\mathbb{Q}_+ = \emptyset$.

(d) *Kaikilla* $a \in \mathbb{Q}$ *pätee* $a^2 \in \mathbb{Q}_+ \cup \{0\}$.

(e) *Kaikilla* $a \in \mathbb{Q}_+$ *pätee* $a^{-1} \in \mathbb{Q}_+$.

Todistus. (a) Olkoot $a = m/n$ ja $b = p/q$, missä $m, n, p, q \in \mathbb{Z}_+$. Tällöin $a + b = (mq + np)/nq$. Lemman 2.8 perusteella $mq, np, mq + np, nq \in \mathbb{Z}_+$, joten $a + b \in \mathbb{Q}_+$. Vastaavasti nähdään, että $ab \in \mathbb{Q}_+$.

Loput kohdat harjoitustehtäviä. □

Myös Lemma 2.9 yleistyy rationaaliluvuille:

Lemma 3.7. (a) *Jos* $a, b, c \in \mathbb{Q}$ *ja* $a + c = b + c$, *niin* $a = b$.

(b) *Jos* $a, b \in \mathbb{Q}$ *ja* $ab = 0$, *niin* $a = 0$ *tai* $b = 0$.

(c) *Jos* $a, b \in \mathbb{Q}$, $c \in \mathbb{Q}^*$ *ja* $ac = bc$, *niin* $a = b$.

Todistus. (a) Todistetaan kuten kokonaisluvuille.

(b) Olkoot $a = m/n$ ja $b = p/q$, missä $m, p \in \mathbb{Z}$ ja $n, q \in \mathbb{Z}^*$. Jos $ab = 0$, niin

$$\frac{mp}{nq} = 0 = \frac{0}{1}.$$

Tällöin $mp = 0$, joten Lemman 2.9 nojalla $m = 0$ tai $p = 0$. Siispä $a = 0$ tai $b = 0$.

(c) Seuraa (a)- ja (b)-kohdista kuten kokonaisluvuille. Voidaan todistaa myös käyttäen luvun c käänteislukua samaan tapaan kuin (a)-kohdassa käytetään vastalukua. □

Nyt voimme määritellä järjestyksen rationaaliluvuille:

Määritelmä 3.8. Määritellään joukon $\mathbb{Q}$ relaatio ‘ $<$ ‘ asettamalla kaikille $a, b \in \mathbb{Q}$

$$a < b \iff b - a \in \mathbb{Q}_+ .$$

HUOMAUTUS: Rationaalilukujen summa (ja siten myös erotus) on hyvin määritelty, joten riittää huomata, että joukkoon $\mathbb{Q}_+$ kuuluminen ei riipu valitusta rationaaliluvun a edustajasta. Tällöin rationaalilukujen relaatio ‘ $<$ ‘ on hyvin määritelty.

Totuttuun tapaan asetamme vielä kaikille $a, b \in \mathbb{Q}$

$$a \leq b \iff a < b \text{ tai } a = b.$$

HUOMAUTUS: Kun $m, n, p, q \in \mathbb{Z}_+$, niin

$$\frac{m}{n} \leq \frac{p}{q} \iff mq \leq np. \tag{8}$$

Tämä ei kuitenkaan ole hyvä tapa määritellä rationaalilukujen järjestystä; pohdinta ja kaavan (8) perustelu jätetään harjoitustehtäväksi.

Lause 3.9. *Joukon $\mathbb{Q}$ relaatio ' $\leq$ ' täydellinen järjestys. Lisäksi kaikilla $m, n \in \mathbb{Z}$ pätee*

$$j(m) \leq j(n) \iff m \leq n.$$

Todistus. (1) Olkoot $a, b, c \in \mathbb{Q}$. Tällöin

- $a \leq a$
- Jos $a \leq b$ ja $b \leq a$, niin $b - a \in \mathbb{Q}_+ \cup \{0\}$ ja $b - a = -(a - b) \in -\mathbb{Q}_+ \cup \{0\}$. Koska Lemman 3.6 mukaan $\mathbb{Q}_+ \cap -\mathbb{Q}_+ = \emptyset$, niin välttämättä $b - a = 0$, jolloin $a = b$.
- Jos $a \leq b$ ja $b \leq c$, niin $b - a \in \mathbb{Q}_+ \cup \{0\}$ ja $c - b \in \mathbb{Q}_+ \cup \{0\}$, jolloin Lemman 3.6 (a)-kohdan avulla nähdään helposti, että

  $$c - a = (c - b) - (b - a) \in \mathbb{Q}_+ \cup \{0\}.$$

  Siispä $a \leq c$.

Näin ollen ' $\leq$ ' on joukon $\mathbb{Q}$ osittainen järjestys.

(2) Olkoot $a, b \in \mathbb{Q}$. Lemman 3.6 perusteella $b - a = 0$, $b - a \in \mathbb{Q}_+$ tai $a - b = -(b - a) \in \mathbb{Q}_+$. Niinpä $a \leq b$ tai $b \leq a$, joten järjestys ' $\leq$ ' on myös täydellinen.

(3) Olkoot $m, n \in \mathbb{Z}$. Tällöin

$$j(m) \leq j(n) \iff [m, 1] \leq [n, 1] \iff m \cdot 1 \leq 1 \cdot n \iff m \leq n,$$

missä keskimmäinen ekvivalenssi seuraa kaavasta (8). □

SOPIMUS: Tästedes samastamme kokonaisluvut vastaavan rationaalilukujen osajoukon $j(\mathbb{Z}) \subset \mathbb{Q}$ kanssa. Toisin sanoen, jos $m \in \mathbb{Z}$, niin $m = [m, 1] = m/1 \in \mathbb{Q}$.

HUOMAUTUS*: Olemme käyttäneet merkintää $a/b = \frac{a}{b}$ tähän asti kahdessa eri tarkoituksessa: jos $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$, niin $a/b = [a, b] \in \mathbb{Q}$, ja jos $(a, b) \in \mathbb{Q} \times \mathbb{Q}^*$, niin $a/b = a \cdot b^{-1} \in \mathbb{Q}$. Kun samastamme kokonaisluvut rationaalilukujen osajoukoksi, on syytä tarkistaa, että kokonaisluvuille molemmat merkinnät tarkoittavat samaa asiaa. Toki näin onkin, sillä jos $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$, niin samastuskuvausta j käyttäen saamme

$$a \cdot b^{-1} = [a, 1][b, 1]^{-1} = [a, 1][1, b] = [a, b].$$

HAVAINTOJA: Olemme siis saaneet laajennettua luonnollisten lukujen joukon $\mathbb{N}$ rationaalilukujen joukoksi $\mathbb{Q}$, joka sisältää joukon $\mathbb{N}$ osajoukkonaan luonnollisten samastusten kautta:

$$\mathbb{N} = i(\mathbb{N}) \subset \mathbb{Z} = j(\mathbb{Z}) \subset \mathbb{Q}.$$

Yhteen- ja kertolasku käyttäytyvät erittäin hyvin lukualueessa $\mathbb{Q}$: Kaikilla $a \in \mathbb{Q}$ on käänteisalkio yhteenlaskun suhteen (vastaluku $-a$) ja kaikilla $a \in \mathbb{Q} \setminus \{0\}$ käänteisalkio kertolaskun suhteen (käänteisluku $1/a$). Algebran ja analyysin kannalta rationaalilukujen joukko ei kuitenkaan ole vielä riittävän hyvä lukualue. Yksinkertainen aritmetiikkakin on vielä "vajaata", kuten seuraava esimerkki osoittaa:

Esimerkki 3.10. Yhtälöllä $x^2 = 2$ ei ole ratkaisua rationaalilukujen joukossa: Jos olisi $x = p/q \in \mathbb{Q}$ siten, että $x^2 = 2$, niin tällöin $p^2 = 2q^2$. Mutta nyt luku 2 esiintyy luvun p^2 alkutekijäesityksessä parillisen monta kertaa ja luvun $2q^2$ esityksessä parittoman monta kertaa, jolloin Aritmetiikan peruslauseen nojalla nämä luvut eivät voi olla yhtä suuria. Jos tälle yhtälölle halutaan ratkaisu, tarvitaan siis vielä laajempi lukualue.

Analyysin tarpeita varten esittelemme seuraavan määritelmän, joka toimii kaikissa muissakin (täysin) järjestetyissä lukualueissa.

Määritelmä 3.11. Luku $M \in \mathbb{Q}$ on joukon $A \subset \mathbb{Q}$ *yläraja*, jos $a \leq M$ kaikilla $a \in A$. Joukon A yläraja $M \in \mathbb{Q}$ on joukon A *pienin yläraja*, jos $M \leq M'$ kaikilla joukon A ylärajoilla M'. Vastaavasti luku $m \in \mathbb{Q}$ on joukon $A \subset \mathbb{Q}$ *alaraja*, jos $m \leq a$ kaikilla $a \in A$. Joukon A alaraja $m \in \mathbb{Q}$ on joukon A *suurin alaraja*, jos $m' \leq m$ kaikilla joukon A alarajoilla m'.

Joukko $A \subset \mathbb{Q}$ on *ylhäältä rajoitettu*, jos sillä on jokin yläraja $M \in \mathbb{Q}$, ja vastaavasti *alhaalta rajoitettu*, jos sillä on jokin alaraja $m \in \mathbb{Q}$. Jos joukolla on sekä ylä- että alaraja, se on *rajoitettu*.

HUOMAUTUS: Usein joukon A pienintä ylärajaa kutsutaan supremumiksi ja siitä käytetään merkintää $\sup A$. Suurinta alarajaa kutsutaan infimumiksi, merkitään $\inf A$.

Analyysin kannalta on äärimmäisen tärkeää, että jokaisella ylhäältä rajoitetulla joukolla on pienin yläraja. Joukossa $\mathbb{Q}$ näin ei kuitenkaan ole:

Esimerkki 3.12. Joukolla

$$A = \{x \in \mathbb{Q} : x^2 \leq 2\}$$

ei ole pienintä ylärajaa rationaalilukujen joukossa $\mathbb{Q}$: Oletetaan, että $a = p/q \in \mathbb{Q}$ onkin joukon A pienin yläraja. Esimerkin 3.10 perusteella $a^2 = p^2/q^2 \neq 2$, joten $a^2 < 2$ (eli $a \in A$) tai $a^2 > 2$. Jos $a^2 = p^2/q^2 < 2$, niin tarpeeksi suurilla $n \in \mathbb{N}$ pätee $(1 + 1/n)^2 < 2q^2/p^2$ (yksityiskohdat jätetään harjoitustehtäväksi). Tällöin $b = (1 + 1/n)p/q \in A$ ja $a < b$, joten a ei voikaan olla joukon A yläraja.

Vastaavaan tapaan osoitetaan, että mikään joukon

$$B = \{x \in \mathbb{Q} : x^2 > 2\}$$

alkio ei ole joukon A pienin yläraja. Kuitenkin $\mathbb{Q} = A \cup B$, joten joukolla A ei voi olla pienintä ylärajaa rationaalilukujen joukossa.

Kannattaa kiinnittää huomiota Esimerkkien 3.10 ja 3.12 samankaltaisuuteen, vaikka lähtökohta on näissä hyvin erilainen: ensimmäisessä yksinkertaisen yhtälön ratkaisun olemassaolo ja toisessa pienimmän ylärajan löytäminen.

Annetaan tässä vaiheessa vielä yksi tarpeellinen määritelmä:

Määritelmä 3.13. Luvun $a \in \mathbb{Q}$ *itseisarvo* on

$$|a| = \begin{cases} a, & \text{jos } a \in \mathbb{Q}_+, \\ -a, & \text{jos } a \in -\mathbb{Q}_+, \\ 0, & \text{jos } x = 0. \end{cases}$$

Lause 3.14. *Itseisarvolle pätee:*

(a) $|a| = 0 \iff a = 0$.

(b) $|a - b| \leq |a - c| + |c - b|$ *kaikilla* $a, b, c \in \mathbb{Q}$ *(kolmioepäyhtälö).*

(c) $|ab| = |a||b|$ *kaikilla* $a, b \in \mathbb{Q}$.

Todistus. Analyysi 1 / Harjoitustehtävä. □

HUOMAUTUS: Sama määritelmä toimii myös muissa täysin järjestetyissä lukualueissa ($\mathbb{Z}$ ja myöhemmin $\mathbb{R}$).

———————

HISTORIAA: Rationaali- tai murtolukuja on käsitelty jo varhaisissa sivilisaatioissa. Muinaisessa Egyptissä käytettiin ns. *yksikkömurtolukuja*, jotka olivat luonnollisten lukujen käänteislukuja. Kaikki muut murtoluvut esitettiin näiden summina; siis esimerkiksi luku 3/5 esitettiin muodossa "1/3 ja 1/5 ja 1/15". Tämä ei ollut laskujen kannalta kovin käytännöllistä, mutta egyptiläisillä oli mittavia taulukoita helpottamassa esimerkiksi yksikkömurtolukujen yhteenlaskua. Babylonialaisilla oli käytössä huomattavasti joustavampi systeemi, jossa murtoluvut ilmaistiin laskennallisesti kätevässä 60-kantaisessa järjestelmässä, siis nimittäjien $60, 60^2 = 3600, \ldots$ avulla. Siten esimerkiksi $1/5 = (0;12)_{60}$ (koska $1/5 = 12/60$) ja $1/50 = (0;1,12)_{60}$ (koska $1/50 = 1/60 + 12/3600$). Antiikin Kreikkalaiset esittivät murtoluvut (tai oikeastaan kokonaislukujen tai pituuksien *suhteet*) "osoittajan" ja "nimittäjän" avulla, mutta merkinnät poikkesivat nykyisistä.

Esimerkin 3.10 havainto $\sqrt{2} \notin \mathbb{Q}$ on oleellisesti peräisin Pythagoraan koulukunnasta noin 400-luvulta eKr. Tuolloin huomattiin, että neliön sivu ja lävistäjä ovat *yhteismitattomat* eli näiden suhdetta ei voi ilmaista kahden kokonaisluvun suhteena. Tarinan mukaan tämä järkytti suuresti Pythagoralaisten lukujen harmonialle perustunutta maailmankuvaa, ja yhteismitattomuuden keksijä päätettiinkin hukuttaa mereen, ettei vaarallinen tieto pääsisi leviämään.

Teoreettisemmin rationaalilukuja alettiin tarkastella kuitenkin vasta 1800-luvun alkupuolella. Rationaalilukujen joukon täsmällinen määritelmä kokonaislukuparien ekvivalenssiluokkina esiintyy ainakin Heinrich Weberin (1842–1913, Saksa) oppikirjassa *Lehrbuch der Algebra* vuodelta 1895; Kronecker tosin esitteli vastaavan (mutta monimutkaisemman) määritelmän jo vuonna 1887.

4. CAUCHYN JONOT

Edellisen luvun lopun esimerkit 3.10 ja 3.12 osoittavat, että rationaalilukujen joukossa on "reikiä". Seuraavana tavoitteenamme onkin "täyttää" nämä reiät sopivilla "irrationaaliluvuilla", toisin sanoen laajentaa rationaaliluvut edelleen suuremmaksi lukualueeksi $\mathbb{R}$, jossa näitä reikiä ei enää esiinny. Haluamme luonnollisesti, että $\mathbb{Q}$ voidaan jälleen tulkita tämän uuden lukualueen osaksi siten, että laskutoimitukset ja järjestys säilyvät.

Ideana on arvioida esimerkiksi lukua "$\sqrt{2}$"$\notin \mathbb{Q}$ rationaalilukujen jonolla, joka "suppenee" kohti lukua "$\sqrt{2}$". Ongelmana on kuitenkin se, ettei tällaista lukua "$\sqrt{2}$" ole (vielä) olemassa, joten ei voida myöskään määritellä, mitä tätä lukua kohti suppeneminen tarkoittaa. Tämä ongelma voidaan kiertää käyttämällä rationaalilukujen *Cauchyn jonoja*, joita käsittelemme tässä luvussa. Seuraavassa luvussa muodostamme näistä jonoista halutun lukualueen $\mathbb{R}$ sopivan ekvivalenssirelaation (taas!) avulla.

Aloitamme tarkastelemalla rationaalilukujen jonoja. Olkoon

$$\mathscr{J} = \mathscr{J}(\mathbb{Q}) = \{(a_n)_{n=1}^{\infty} : a_n \in \mathbb{Q}\}$$

kaikkien rationaalilukujonojen joukko. Määrittelemme yhteenlaskun ja kertolaskun joukossa $\mathscr{J}$ komponenteittain. Jos siis $\alpha = (a_n)_{n=1}^{\infty}$ ja $\beta = (b_n)_{n=1}^{\infty}$, niin

$$\alpha + \beta = (a_n + b_n)_{n=1}^{\infty} \quad \text{ja} \quad \alpha\beta = (a_n b_n)_{n=1}^{\infty}.$$

Näillä laskutoimituksilla on paljon tuttuja ominaisuuksia:

Lause 4.1. *Kaikilla $\alpha, \beta, \gamma \in \mathscr{J}$, $\alpha = (a_n)_{n=1}^{\infty}$, $\beta = (b_n)_{n=1}^{\infty}$ ja $\gamma = (c_n)_{n=1}^{\infty}$, jonojen laskutoimituksille ‘ + ‘ ja ‘ · ‘ pätee*

(a) *assosiatiivisuus*

$$\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$$
$$\alpha(\beta\gamma) = (\alpha\beta)\gamma$$

(b) *kommutatiivisuus*

$$\alpha + \beta = \beta + \alpha$$
$$\alpha\beta = \beta\alpha$$

(c) *ja distributiivisuus*

$$(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma.$$

Lisäksi

(d) *jono $0 = (0)_{n=1}^{\infty} = (0, 0, 0, \dots)$ on yhteenlaskun neutraalialkio ja jono $1 = (1)_{n=1}^{\infty} = (1, 1, 1, \dots)$ on kertolaskun neutraalialkio;*

(e) *jokaisella jonolla $\alpha = (a_n)_{n=1}^{\infty}$ on käänteisalkio $-\alpha = (-a_n)_{n=1}^{\infty}$ yhteenlaskun suhteen.*

Todistus. Kaikki ominaisuudet seuraavat suoraan jonojen laskutoimitusten määritelmästä ja rationaalilukujen laskutoimitusten vastaavista ominaisuuksista; yksityiskohtien tarkastaminen jätetään harjoitustehtäväksi. □

Huomautus: Monilla jonoilla ei ole käänteisalkiota kertolaskun suhteen: Olkoon esimerkiksi $\alpha = (0, a_2, a_3, \dots)$ ja $\beta = (b_1, b_2, b_3, \dots)$. Tällöin

$$\alpha\beta = (0, a_2 b_2, a_3 b_3, \dots) \neq (1, 1, 1, \dots) = 1,$$

joten jonolla α ei voi olla käänteisalkiota kertolaskun suhteen.

Huomautus*: Jono $\alpha = (a_n)_{n=1}^{\infty} \in \mathscr{J}$ voidaan tulkita kuvaukseksi

$$\alpha : \mathbb{Z}_+ \to \mathbb{Q},\ \alpha(n) = a_n.$$

Määritelmä 4.2. (1) Jono $(a_n)_{n=1}^{\infty} \in \mathscr{J}$ on *rajoitettu*, jos on $M \in \mathbb{Q}$ siten, että $|a_n| \leq M$ kaikilla $n \in \mathbb{Z}_+$.

(2) Jono $(a_n)_{n=1}^{\infty} \in \mathscr{J}$ *suppenee kohti lukua* $a \in \mathbb{Q}$, jos kaikilla $\varepsilon \in \mathbb{Q}_+$ on $N \in \mathbb{N}$ siten, että

$$|a_n - a| < \varepsilon, \quad \text{kun} \quad n \geq N.$$

(3) Jono $(a_n)_{n=1}^{\infty} \in \mathscr{J}$ on *Cauchyn jono*, jos kaikilla $\varepsilon \in \mathbb{Q}_+$ on $N \in \mathbb{N}$ siten, että

$$|a_n - a_m| < \varepsilon, \quad \text{kun} \quad n, m \geq N.$$

Jos jono $\alpha = (a_n)_{n=1}^{\infty} \in \mathscr{J}$ suppenee kohti lukua $a \in \mathbb{Q}$, on a jonon α *raja-arvo*. Tällöin käytetään merkintöjä:

$$a = \lim_{n\to\infty} a_n\,; \quad a_n \underset{n\to\infty}{\longrightarrow} a\,; \quad a_n \to a, \quad \text{kun} \quad n \to \infty.$$

Jos jono $\alpha \in \mathscr{J}$ suppenee kohti jotakin lukua $a \in \mathbb{Q}$, sanomme, että jono α *suppenee* (joukossa $\mathbb{Q}$). Jos jono ei suppene, se *hajaantuu*.

Esimerkki 4.3. (a) Jono $(a_n)_{n=1}^{\infty} \in \mathscr{J}$ on *vakiojono*, jos on olemassa $a \in \mathbb{Q}$ siten, että $a_n = a$ kaikilla $n \in \mathbb{Z}_+$. Tällöin myös $\lim_{n\to\infty} a_n = a$.

(b) Jono $(1/n)_{n=1}^{\infty} \in \mathscr{J}$ suppenee kohti lukua 0. Tämä nähdään seuraavasti: Olkoon $\varepsilon \in \mathbb{Q}_+$, jolloin $\varepsilon = p/q$ joillekin $p, q \in \mathbb{Z}_+$. Kun $n > q$, niin $np > qp \geq q \cdot 1$, jolloin $1/n < p/q = \varepsilon$. Näin ollen $|1/n - 0| = 1/n < \varepsilon$ kun $n > q$ eli kun $n \geq q + 1$, joten määritelmän 4.2(2) luvuksi N voidaan valita $q + 1$.

Määritelmän 4.2 käsitteet liittyvät läheisesti toisiinsa:

Lause 4.4. (a) *Jos jono $\alpha \in \mathscr{J}$ suppenee, niin α on Cauchyn jono.*

(b) *Jos jono $\alpha \in \mathscr{J}$ on Cauchyn jono, niin se on rajoitettu.*

Todistus. (a) Harjoitustehtävä; käytä kolmioepäyhtälöä.

(b) Jos $\alpha = (a_n)_{n=1}^{\infty} \in \mathscr{J}$ on Cauchyn jono, niin löytyy $N \in \mathbb{N}$ siten, että

$$|a_n - a_m| < 1 \in \mathbb{Q}_+, \quad \text{kun } n, m \geq N.$$

Olkoon nyt $M' = \max\{|a_n - a_N| : 1 \leq n \leq N\}$. Tällöin kaikilla $n \in \mathbb{Z}_+$

$$|a_n| \leq |a_n - a_N| + |a_N| \leq \max\{1, M'\} + |a_N|,$$

joten määritelmän 4.2(1) luvuksi M voidaan valita $M = \max\{1, M'\} + |a_N|$. □

HUOMAUTUS: Monet rationaalilukujen Cauchyn jonot eivät suppene joukossa $\mathbb{Q}$. Esimerkiksi jono

$$1 = \frac{1}{1},\ 2 = \frac{2}{1},\ \frac{3}{2},\ \frac{5}{3},\ \frac{8}{5},\ \frac{13}{8},\ \frac{21}{13}, \ldots,$$

joka jatkuu säännöllä

$$\frac{p_n}{q_n} = \frac{p_{n-1} + p_{n-2}}{q_{n-1} + q_{n-2}},$$

(Fibonaccin luvut!) on rationaalilukujen Cauchyn jono, joka ei suppene rationaalilukujen joukossa. Sivuutamme tämän seikan todistuksen. Mainittakoon, että kyseinen jono liittyy ketjumurtolukuihin ja kultaiseen leikkaukseen, sillä itse asiassa

$$\frac{p_n}{q_n} = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \cdots_1}}} \underset{n\to\infty}{\longrightarrow} \frac{1 + \sqrt{5}}{2} \notin \mathbb{Q}.$$

Merkitään tästä lähtien rationaalilukujen joukon $\mathbb{Q}$ Cauchyn jonojen joukkoa

$$\mathscr{C} = \mathscr{C}(\mathbb{Q}) = \{(a_n)_{n=1}^{\infty} \in \mathscr{J}(\mathbb{Q}) : (a_n)_{n=1}^{\infty} \text{ on Cauchyn jono}\}.$$

Lause 4.5. *Jonojen yhteen- ja kertolaskut määräävät laskutoimitukset myös Cauchyn jonojen joukossa, ts. jos $\alpha, \beta \in \mathscr{C}$, niin $\alpha + \beta \in \mathscr{C}$ ja $\alpha\beta \in \mathscr{C}$.*

Todistus. Olkoot siis $\alpha = (a_k)_{k=1}^{\infty} \in \mathscr{C}$ ja $\beta = (b_k)_{k=1}^{\infty} \in \mathscr{C}$. Osoitamme, että $\alpha\beta \in \mathscr{C}$. Koska Cauchyn jonot ovat rajoitettuja, niin löytyy $M_\alpha,\ M_\beta \in \mathbb{Q}_+$ siten, että $|a_k| \leq M_\alpha$ ja $|b_k| \leq M_\beta$ kaikilla $k \in \mathbb{Z}_+$. Olkoon sitten $\varepsilon \in \mathbb{Q}_+$. Koska α ja β ovat Cauchyn jonoja, niin löytyy $N_\alpha,\ N_\beta \in \mathbb{N}$ siten, että

$$|a_n - a_m| < \varepsilon/(2M_\beta) \quad \text{kun } n, m \geq N_\alpha \quad \text{ja}$$
$$|b_n - b_m| < \varepsilon/(2M_\alpha) \quad \text{kun } n, m \geq N_\beta.$$

Jos nyt valitaan $N = \max\{N_\alpha, N_\beta\}$ ja jos $n, m \geq N$, niin kolmioepäyhtälön nojalla

$$\begin{aligned} |a_n b_n - a_m b_m| &\leq |a_n b_n - a_n b_m| + |a_n b_m - a_m b_m| \\ &\leq |a_n||b_n - b_m| + |a_n - a_m||b_m| \\ &< M_\alpha \frac{\varepsilon}{2M_\alpha} + \frac{\varepsilon}{2M_\beta} M_\beta \leq \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon. \end{aligned}$$

Siispä myös tulojono $\alpha\beta$ on Cauchyn jono.

Yhteenlaskuun liittyvä vastaava tarkastelu jätetään harjoitustehtäväksi. □

Lause 4.6. *Joukon $\mathscr{C}$ laskutoimitukset ' + ' ja ' · ' toteuttavat Lauseen 4.1 ominaisuudet (a)–(e).*

Todistus. Ominaisuudet (a)–(d) seuraavat suoraan Lauseen 4.1 vastaavista kohdista.

Kohtaa (e) varten täytyy osoittaa, että Cauchyn jonon käänteisalkio yhteenlaskun suhteen on myös Cauchyn jono. Tämä seuraa Lauseesta 4.5, sillä nyt $-\alpha = (-1)_{n=1}^{\infty}\alpha$ ja $(-1)_{n=1}^{\infty}$ on vakiojonona Cauchyn jono. □

5. Reaaliluvut

Ideanamme oli määritellä reaaliluvut rationaalilukujen Cauchyn jonojen avulla. Siten esimerkiksi jonon $1\,; 1,4\,; 1,41\,; 1,414\,; 1,4142\,; \ldots$ pitäisi vastata reaalilukua $\sqrt{2}$. Monet rationaalilukujen Cauchyn jonot suppenevat kuitenkin kohti samaa lukua, esimerkiksi $1/n \to 0$, $\pm 1/2^n \to 0$ ja $(-1)^n/n \to 0$ kun $n \to \infty$. Samoin (liian) monilla Cauchyn jonoilla ei ole käänteisalkiota kertolaskun suhteen. Emme siis voi määritellä reaalilukuja suoraan rationaalilukujen Cauchyn jonojen joukoksi, mutta ongelmat saadaan korjattua määrittelemällä Cauchyn jonoille sopiva ekvivalenssirelaatio.

Määritelmä 5.1. Rationaalilukujen (Cauchyn) jono $\alpha = (a_k)_{k=1}^{\infty}$ on *nollajono*, jos se suppenee kohti lukua $0 \in \mathbb{Q}$. Merkitsemme rationaalilukujen nollajonojen joukkoa $\mathscr{N}(\mathbb{Q})$.

Lemma 5.2. *Olkoot $\alpha \in \mathscr{N}(\mathbb{Q})$ ja $\beta \in \mathscr{C}(\mathbb{Q})$. Tällöin $\alpha\beta \in \mathscr{N}(\mathbb{Q})$.*

Todistus. Harjoitustehtävä; vertaa Lauseen 4.5 todistukseen. □

Huomautus: Lemman 5.2 tulos ei päde, jos oletamme vain, että $\beta \in \mathscr{J}(\mathbb{Q})$. Esimerkiksi $(1/n)_{n=1}^{\infty} \in \mathscr{N}(\mathbb{Q})$ ja $(n)_{n=1}^{\infty} \in \mathscr{J}(\mathbb{Q})$, mutta näiden tulojono $(1)_{n=1}^{\infty}$ ei ole nollajono.

Määritellään joukossa $\mathscr{C}(\mathbb{Q})$ relaatio $\sim$ asettamalla

$$\alpha \sim \beta \iff \alpha - \beta \in \mathscr{N}(\mathbb{Q}). \tag{9}$$

Lemma 5.3. *Kaavalla (9) määritelty relaatio $\sim$ on joukon $\mathscr{C}(\mathbb{Q})$ ekvivalenssirelaatio.*

Todistus. Olkoot $\alpha, \beta, \gamma \in \mathscr{C}(\mathbb{Q})$. Tällöin:

(1) $\alpha \sim \alpha$, koska $\alpha - \alpha = (0)_{k=1}^{\infty} \in \mathscr{N}(\mathbb{Q})$.
(2) Jos $\alpha \sim \beta$, niin $\alpha - \beta \in \mathscr{N}(\mathbb{Q})$, jolloin Lemman 5.2 perusteella myös

$$\beta - \alpha = (-1)_{k=1}^{\infty}(\alpha - \beta) \in \mathscr{N}(\mathbb{Q}),$$

ja niinpä $\beta \sim \alpha$.

(3) Jos $\alpha \sim \beta$ ja $\beta \sim \gamma$, niin $\alpha - \beta \in \mathscr{N}(\mathbb{Q})$ ja $\beta - \gamma \in \mathscr{N}(\mathbb{Q})$, jolloin kolmioepäyhtälön avulla nähdään, että myös $\alpha - \gamma \in \mathscr{N}(\mathbb{Q})$.

Siispä $\sim$ on ekvivalenssirelaatio. □

HUOMAUTUS: Relaation $\sim$ transitiivisuus voidaan todistaa myös seurauksena yleisemmästä tuloksesta: Jos $\alpha, \beta \in \mathscr{N}(\mathbb{Q})$ ja $a, b \in \mathbb{Q}$, niin myös $a\alpha + b\beta \in \mathscr{N}(\mathbb{Q})$ (harjoitustehtävä).

Nyt voimme (lopultakin) määritellä reaalilukujen joukon rationaalilukujen Cauchyn jonojen ekvivalenssiluokkien avulla:

Määritelmä 5.4. *Reaalilukujen* joukko on tekijäjoukko

$$\mathbb{R} = \mathscr{C}(\mathbb{Q})/\sim \quad \Big(= \mathscr{C}(\mathbb{Q})/\mathscr{N}(\mathbb{Q}) \Big).$$

Reaalilukujen yhteen- ja kertolasku määritellään tuttuun tapaan ekvivalenssiluokkien avulla: Kun $\alpha = (a_n)_{n=1}^{\infty}$, $\beta = (b_n)_{n=1}^{\infty} \in \mathscr{C}$ ja $x = [\alpha]$, $y = [\beta] \in \mathbb{R}$, niin

$$x + y = [\alpha] + [\beta] = [(a_n + b_n)_{n=1}^{\infty}] \quad \text{ja} \quad xy = [\alpha][\beta] = [(a_n b_n)_{n=1}^{\infty}].$$

HUOMAUTUS: (i) Lauseen 4.5 perusteella $(a_n + b_n)_{n=1}^{\infty} \in \mathscr{C}$ ja $(a_n b_n)_{n=1}^{\infty} \in \mathscr{C}$, joten näitä jonoja vastaavat ekvivalenssiluokat ovat todella reaalilukuja.

(ii) Reaalilukujen laskutoimitukset ovat hyvin määriteltyjä. Todetaan tämä jälleen yhteenlaskulle (kertolasku jätetään harjoitustehtäväksi): Oletetaan siis, että $\alpha' \in [\alpha]$ ja $\beta' \in [\beta]$, jolloin $\alpha - \alpha'$ ja $\beta - \beta'$ ovat nollajonoja. Tällöin Lemman 5.2 jälkeisen huomautuksen nojalla

$$(\alpha + \beta) - (\alpha' + \beta') = (\alpha - \alpha') + (\beta - \beta') \in \mathscr{N}(\mathbb{Q}),$$

joten $[\alpha + \beta] = [\alpha' + \beta']$. Siispä reaalilukujen yhteenlasku on hyvin määritelty.

Seuraavassa lemmassa esitettävä tekninen havainto on hyvin keskeisessä osassa reaalilukujen ominaisuuksia todistettaessa.

Lemma 5.5. *Olkoon $\alpha \in \mathscr{C}(\mathbb{Q})$. Tällöin täsmälleen yksi seuraavista vaihtoehdoista on voimassa:*

(i) $\alpha \in \mathscr{N}(\mathbb{Q})$ *;*
(ii) *on $c \in \mathbb{Q}_+$ ja $N \in \mathbb{N}$ siten, että $a_n \geq c$ kaikilla $n \geq N$;*
(iii) *on $c \in -\mathbb{Q}_+$ ja $N \in \mathbb{N}$ siten, että $a_n \leq c$ kaikilla $n \geq N$.*

Todistus. Koska vaihtoehto (i) on yhtäpitävää sen kanssa, että on $c \in \mathbb{Q}_+$ ja $N \in \mathbb{N}$ siten, että $-c \leq a_n \leq c$ kaikilla $n \geq N$, ja koska ' $\geq$ ' on $\mathbb{Q}$:n täydellinen järjestys, niin on selvää, että korkeintaan yksi vaihtoehdoista (i)–(iii) voi olla voimassa jonolle $\alpha = (a_n)_{n=1}^{\infty} \in \mathscr{C}(\mathbb{Q})$. On siis vielä osoitettava, että joku vaihtoehdoista on aina voimassa.

Jos nyt $\alpha \in \mathscr{N}(Q)$, niin väite pätee. Siispä voimme olettaa, että $\alpha \notin \mathscr{N}(Q)$ eli että kaikille $\varepsilon \in \mathbb{Q}_+$ *ei ole olemassa* lukua $N \in \mathbb{N}$ siten, että pätisi $|a_n| \leq \varepsilon$ kun $n \geq N$. Tästä seuraa, että on olemassa *jokin* $\varepsilon \in \mathbb{Q}_+$ siten, että $|a_n| \geq \varepsilon$ äärettömän monelle $n \in \mathbb{Z}_+$. Toisaalta, koska α on Cauchyn jono, niin löytyy $N \in \mathbb{N}$ siten, että

$$|a_n - a_m| < \varepsilon/2 \quad \text{kun } n, m \geq N.$$

Nyt voidaan valita $N' \geq N$ siten, että $|a_{N'}| \geq \varepsilon$, jolloin joko $a_{N'} \geq \varepsilon$ tai $a_{N'} \leq -\varepsilon$. Jos $a_{N'} \geq \varepsilon$, niin kaikille $n \geq N$ saadaan

$$\varepsilon < a_{N'} = a_n + (a_{N'} - a_n) \leq a_n + |a_n - a_{N'}| < a_n + \varepsilon/2,$$

joten $a_n \geq \varepsilon/2 = c$ kaikilla $n \geq N$, eli (ii) on voimassa.

Vastaavasti osoitetaan, että tapauksessa $a_{N'} \leq -\varepsilon$ on voimassa vaihtoehto (iii). □

Lemma 5.5 osoittaa, että Cauchyn jonojen ekvivalenssiluokkiin siirtymällä olemme päässeet eroon kertolaskun käänteisalkioihin liittyvistä ongelmista (vrt. Lauseen 4.1 jälkeiseen huomautukseen). Erityisesti voimme nyt osoittaa, että kaikki rationaalilukujen laskutoimitusten hyvät ominaisuudet pätevät myös reaaliluvuille.

Lause 5.6. (a) *Reaalilukujen yhteenlasku ja kertolasku ovat assosiatiivisia.*

(b) *Reaalilukujen yhteenlasku ja kertolasku ovat kommutatiivisia.*

(c) *Reaalilukujen kertolasku on distributiivinen yhteenlaskun suhteen.*

(d) *Luku* $0 = [(0)_{n=1}^{\infty}] \in \mathbb{R}$ *on reaalilukujen yhteenlaskun neutraalialkio ja luku* $1 = [(1)_{n=1}^{\infty}] \in \mathbb{R}$ *on kertolaskun neutraalialkio.*

(e) *Jokaisella reaaliluvulla* x *on vastaluku* $-x$ *eli käänteisalkio yhteenlaskun suhteen.*

(f) *Jokaisella nollasta poikkeavalla reaaliluvulla* x *on käänteisluku* x^{-1} *eli käänteisalkio kertolaskun suhteen.*

Todistus. Ominaisuudet (a)–(d) seuraavat suoraviivaisesti Lauseen 4.1 vastaavista kohdista ja kohdassa (e) on helppo todeta, että jos $x = [(a_n)_{n=1}^{\infty}] \in \mathbb{R}$, niin $-x = [(-a_n)_{n=1}^{\infty}]$ on x:n vastaluku.

Siten riittää osoittaa, että kohta (f) pätee eli jokaisella $x \in \mathbb{R} \setminus \{0\}$ on käänteisalkio kertolaskun suhteen:

Kun $x \in \mathbb{R}$, voimme aina valita luvut $a_k \in \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ siten, että $x = [(a_k)_{k=1}^{\infty}]$ (harjoitustehtävä). Tällöin jonolle $(1/a_k)_{k=1}^{\infty}$ pätee

$$(a_k)_{k=1}^{\infty} \cdot (1/a_k)_{k=1}^{\infty} = (1)_{k=1}^{\infty}.$$

Jos siis valitsemme $x^{-1} = [(1/a_n)_{n=1}^{\infty}]$, niin $x \cdot x^{-1} = 1$. Huomaa kuitenkin, että näin voidaan valita vain jos myös jono $(1/a_k)_{k=1}^{\infty}$ on Cauchyn jono! Näin ollen on vielä osoitettava, että todella $(1/a_k)_{k=1}^{\infty} \in \mathscr{C}(\mathbb{Q})$. Tässä tarvitsemme oletusta $x = [(a_k)_{k=1}^{\infty}] \in \mathbb{R} \setminus \{0\}$.

Olkoon siis $\varepsilon \in \mathbb{Q}_+$. Koska $(a_k)_{k=1}^{\infty} \notin \mathscr{N}(\mathbb{Q})$, niin Lemman 5.5 avulla löytyy $N_1 \in \mathbb{N}$ ja $q \in \mathbb{Q}_+$ siten, että $|a_n| \geq q$ aina kun $n \geq N_1$. Toisaalta, koska $(a_k)_{k=1}^{\infty} \in \mathscr{C}(\mathbb{Q})$, voimme valita luvun $N_2 \in \mathbb{N}$ siten, että

$$|a_n - a_m| < q^2\varepsilon \quad \text{kun } n, m \geq N_2.$$

Jos nyt asetamme $N = \max\{N_1, N_2\}$, niin kaikille $n, m \geq N$ pätee

$$\left|\frac{1}{a_n} - \frac{1}{a_m}\right| = \left|\frac{a_m - a_n}{a_m a_n}\right| = \frac{|a_m - a_n|}{|a_m||a_n|} \leq \frac{|a_m - a_n|}{q^2} < q^2\varepsilon/q^2 = \varepsilon.$$

Siispä $(1/a_k)_{k=1}^{\infty}$ on Cauchyn jono, ja väite on todistettu. □

Määritelmä 5.7. Määrittelemme reaaliluvuille vähennys- ja jakolaskut aivan kuten rationaaliluvuille: Kun $x, y \in \mathbb{R}$, niin $x - y = x + (-y)$, ja jos lisäksi $y \neq 0$, niin asetamme $x/y = x \cdot y^{-1}$.

Seuraavana tavoitteenamme on määritellä reaaliluvuille järjestys. Tässä tarvitaan apuna *positiivisten reaalilukujen joukkoa*

$$\mathbb{R}_+ = \big\{[(a_k)_{k=1}^{\infty}] : \text{on } N \in \mathbb{N} \text{ ja } q \in \mathbb{Q}_+ \text{ siten, että } a_n \geq q \text{ kaikilla } n \geq N\big\};$$

vastaavasti $-\mathbb{R}_+$ on *negatiivisten reaalilukujen joukko.*

HUOMAUTUS: Joukko $\mathbb{R}_+$ on hyvin määritelty, sillä jos $a_k \geq q$ aina kun $k \geq N$ ja $(a_k)_{k=1}^{\infty} \sim (b_k)_{k=1}^{\infty}$, niin löytyy $N' \in \mathbb{N}$ siten, että $|b_k - a_k| < \frac{q}{2}$ kun $k \geq N'$. Kolmioepäyhtälön avulla nähdään, että nyt $b_k > q/2$ kun $k \geq \max\{N', N\} \in \mathbb{N}$.

Lemmassa 3.6 joukolle $\mathbb{Q}_+$ todistetut ominaisuudet pätevät myös joukolle $\mathbb{R}_+$:

Lemma 5.8. (a) *Jos $x, y \in \mathbb{R}_+$, niin $x + y \in \mathbb{R}_+$ ja $xy \in \mathbb{R}_+$.*

(b) $\mathbb{R} = -\mathbb{R}_+ \cup \{0\} \cup \mathbb{R}_+$.

(c) $\mathbb{R}_+ \cap -\mathbb{R}_+ = \emptyset$.

(d) *Kaikilla $x \in \mathbb{R}$ pätee $x^2 \in \mathbb{R}_+ \cup \{0\}$.*

(e) *Kaikilla $x \in \mathbb{R}_+$ pätee $x^{-1} \in \mathbb{R}_+$.*

Todistus. (a) Tarkastellaan tuloa: Olkoot $x = [(a_k)_{k=1}^{\infty}]$ ja $y = [(b_k)_{k=1}^{\infty}] \in \mathbb{R}_+$. Tällöin on $N_1 \in \mathbb{N}$ ja $q_1 \in \mathbb{Q}_+$ siten, että $a_k \geq q_1$ kun $k \geq N_1$, ja vastaavasti löytyy $N_2 \in \mathbb{N}$ ja $q_2 \in \mathbb{Q}_+$ siten, että $b_k \geq q_2$ kun $k \geq N_2$. Nyt $q_1 q_2 \in \mathbb{Q}_+$ ja $a_k b_k \geq q_1 q_2$ aina kun $k \geq \max\{N_1, N_2\}$, joten $xy \in \mathbb{R}_+$. Yhteenlasku käsitellään samaan tapaan.

(b) Olkoon $x = [(a_k)_{k=1}^{\infty}] \in \mathbb{R}$. Voimme olettaa, että $x \neq 0$. Tällöin Lemman 5.5 nojalla löytyy $q \in \mathbb{Q}_+$ ja $N \in \mathbb{N}$ siten, että joko

(i) $a_n \geq q$ kaikilla $n \geq N$, jolloin $x \in \mathbb{R}_+$, tai
(ii) $a_n \leq -q$ kaikilla $n \geq N$, jolloin $-a_n \geq q$ kaikilla $n \geq N$. Mutta nyt $-x = [(-a_k)_{k=1}^{\infty}] \in \mathbb{R}_+$, joten $x = -(-x) \in -\mathbb{R}_+$.

(c) Jos $[(a_k)_{k=1}^{\infty}] \in \mathbb{R}_+ \cap -\mathbb{R}_+$, niin on olemassa $q \in \mathbb{Q}_+$ siten, että $a_k \geq q$ ja $-a_k \geq q$ kun k on tarpeeksi suuri. Tällöin $a_k \in \mathbb{Q}_+ \cap -\mathbb{Q}_+ = \emptyset$, mikä on mahdotonta. Siispä $\mathbb{R}_+ \cap -\mathbb{R}_+ = \emptyset$.

(d) ja (e)-kohdat jätetään harjoitustehtäviksi. □

MERKINTÄ: Käytämme jatkossa myös merkintää $\mathbb{R}^* = \mathbb{R} \setminus \{0\} = \mathbb{R}_+ \cup -\mathbb{R}_+$.

Määritelmä 5.9. Määritellään joukon $\mathbb{R}$ relaatiot ' $<$ ' ja ' $\leq$ ' asettamalla kaikille $x, y \in \mathbb{R}$

$$x < y \iff y - x \in \mathbb{R}_+$$

ja

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

HUOMAUTUS: Relaatiot ' $<$ ' ja ' $\leq$ ' ovat hyvin määriteltyjä, sillä vähennyslasku ja joukkoon $\mathbb{R}_+$ kuuluminen ovat hyvin määriteltyjä.

Lause 5.10. *Relaatio ' $\leq$ ' on joukon $\mathbb{R}$ täydellinen järjestys.*

Todistus. Tarvittavat ominaisuudet todistetaan Lemman 5.8 avulla aivan kuten rationaalilukujen järjestystä koskevassa Lauseessa 3.9, joka todistettiin vastaavan Lemman 3.6 avulla. □

Haluamme samastaa rationaaliluvut sopivan reaalilukujen osajoukon kanssa. Tätä varten määrittelemme kuvauksen $i\colon \mathbb{Q} \to \mathbb{R}$, $i(q) = [(q)_{k=1}^{\infty}]$. Tällöin pätee:

Lause 5.11. *Kuvaus i on injektio. Lisäksi kaikilla $q, q' \in \mathbb{Q}$*

$$i(q + q') = i(q) + i(q') \quad \textit{ja} \quad i(qq') = i(q)i(q'),$$

sekä

$$i(q) \leq i(q') \iff q \leq q'.$$

Todistus. (1) Kuvauksen i injektiivisyyden tarkistus jätetään harjoitustehtäväksi.

(2) Olkoot $q, q' \in \mathbb{Q}$. Tällöin

$$i(q+q') = [(q+q')_{k=1}^{\infty}] = [(q)_{k=1}^{\infty}] + [(q')_{k=1}^{\infty}] = i(q) + i(q');$$

kertolasku käsitellään vastaavasti.

(3) Osoitetaan vielä, että kuvaus i säilyttää järjestyksen. Koska $q = q' \iff i(q) = i(q')$, niin riittää osoittaa, että $q < q' \iff i(q) < i(q')$. Nyt

$$q < q' \iff q' - q \in \mathbb{Q}_+$$

ja toisaalta

$$i(q) < i(q') \iff i(q') - i(q) = \left[(q')_{k=1}^{\infty}\right] - [(q)_{k=1}^{\infty}] = \left[(q'-q)_{k=1}^{\infty}\right] \in \mathbb{R}_+.$$

Joukon $\mathbb{R}_+$ määritelmän perusteella ehdosta $q' - q \in \mathbb{Q}_+$ seuraa, että $[(q'-q)_{k=1}^{\infty}] \in \mathbb{R}_+$, ja kääntäen, jos $[(q'-q)_{k=1}^{\infty}] \in \mathbb{R}_+$, niin $q' - q \geq p$ jollekin $p \in \mathbb{Q}_+$, jolloin myös $q' - q \in \mathbb{Q}_+$. Siispä $q < q' \iff i(q) < i(q')$. □

Sopimus: Tästedes samastamme rationaaliluvut vastaavan reaalilukujen osajoukon $i(\mathbb{Q}) \subset \mathbb{R}$ kanssa, ts. jos $q \in \mathbb{Q}$, niin $q = [(q)_{k=1}^{\infty}] \in \mathbb{R}$.

Huomautus: (i) Jatkossa merkinnällä $a > 0$ tarkoitetaan aina, että $a \in \mathbb{R}_+$.

(ii) Itseisarvo määritellään reaaliluvuille aivan samoin kuin rationaaliluvuille; määritelmässä joukko $\mathbb{Q}$ korvataan joukolla $\mathbb{R}$ ja joukko $\mathbb{Q}_+$ joukolla $\mathbb{R}_+$. Kolmioepäyhtälö todistetaan kuten rationaaliluvuille:

Lemma 5.12. *Kaikilla $x, y \in \mathbb{R}$ pätee*

$$|x+y| \leq |x| + |y|.$$

Kaikkien reaalilukujonojen joukkoa merkitään $\mathscr{J}(\mathbb{R})$. Lukujonoihin liittyvät määritelmät ovat joukossa $\mathbb{R}$ täysin samanlaiset kuin joukossa $\mathbb{Q}$:

Määritelmä 5.13. (1) Jono $(x_n)_{n=1}^{\infty} \in \mathscr{J}(\mathbb{R})$ on *rajoitettu*, jos on $M \in \mathbb{R}$ siten, että $|x_n| \leq M$ kaikilla $n \in \mathbb{Z}_+$.

(2) Jono $(x_n)_{n=1}^{\infty} \in \mathscr{J}(\mathbb{R})$ *suppenee kohti lukua* $x \in \mathbb{R}$, jos kaikilla $\varepsilon > 0$ on $N \in \mathbb{N}$ siten, että

$$|x_n - x| < \varepsilon \quad \text{kun} \quad n \geq N.$$

(3) Jono $(x_n)_{n=1}^{\infty} \in \mathscr{J}(\mathbb{R})$ on *Cauchyn jono*, merkitään $(x_n)_{n=1}^{\infty} \in \mathscr{C}(\mathbb{R})$, jos kaikilla $\varepsilon > 0$ on $N \in \mathbb{N}$ siten, että

$$|x_n - x_m| < \varepsilon \quad \text{kun} \quad n, m \geq N.$$

Huomautus: Lause 4.4 pätee myös, kun $\mathscr{J} = \mathscr{J}(\mathbb{R})$, eli suppenevat reaalilukujonot ovat Cauchyn jonoja ja Cauchyn jonot ovat rajoitettuja. Todistus on suora kopio rationaalilukujonojen tapauksesta.

Myös rationaalilukujen ”supistussäännöt” yleistyvät reaaliluvuille:

Lemma 5.14. (a) *Jos $x, y, z \in \mathbb{R}$ ja $x + z = y + z$, niin $x = y$.*

(b) *Jos $x, y \in \mathbb{R}$ ja $xy = 0$, niin $x = 0$ tai $y = 0$.*

(c) *Jos $x, y \in \mathbb{R}$, $z \in \mathbb{R}^*$ ja $xz = yz$, niin $x = y$.*

Todistus. Kohdat (a) ja (c) todistetaan kuten rationaaliluvuille, (b)-kohta vaatii pienen tarkastelun, joka jätetään harjoitustehtäväksi. □

Osoitamme seuraavaksi, että Luvun 3 lopussa havaitut rationaalilukujen joukkoon $\mathbb{Q}$ liittyvät analyysin ongelmat korjaantuvat reaalilukujen joukossa. Kirjaamme aluksi kaksi pientä aputulosta:

Lemma 5.15. *Olkoon $\gamma = (c_k)_{k=1}^{\infty}$ rationaalilukujen Cauchyn jono ja olkoon $c \in \mathbb{Q}_+$. Jos on olemassa $N \in \mathbb{N}$ siten, että $|c_k| < c$ aina kun $k \geq N$, niin $\big|[\gamma]\big| \leq c$.*

Todistus. Jos $\big|[\gamma]\big| = 0$, niin väite pätee.

Jos $[\gamma] \in \mathbb{R}_+$, niin $\big|[\gamma]\big| = [\gamma]$. Jos nyt olisikin $[\gamma] > c$, niin

$$[(c_k - c)_{k=1}^{\infty}] = [(c_k)_{k=1}^{\infty}] - [(c)_{k=1}^{\infty}] = [\gamma] - i(c) = [\gamma] - c \in \mathbb{R}_+.$$

Tällöin löytyy $q \in \mathbb{Q}_+$ ja $N' \in \mathbb{N}$ siten, että $c_k - c \geq q$ kaikilla $k \geq N'$, joten erityisesti $c_k \geq c + q > c$ kaikilla $k \geq N'$. Tämä johtaa ristiriitaan, sillä oletusta käyttäen saamme kaikille $k \geq \max\{N, N'\}$, että $c < c_k \leq |c_k| < c$.

Tapaus $[\gamma] \in -\mathbb{R}_+$ käsitellään samaan tapaan. □

Lemma 5.16. *Olkoon $\varepsilon \in \mathbb{R}_+$. Tällöin löytyy $\varepsilon' \in \mathbb{Q}_+$ siten, että $0 < \varepsilon' < \varepsilon$. Erityisesti jokaisella $M \in \mathbb{N}$ on $n \in \mathbb{N}$, jolle $M/n < \varepsilon$.*

Todistus. Harjoitustehtävä. □

HUOMAUTUS: Muista, että tässä vaiheessa samastamme rationaaliluvun $q \in \mathbb{Q}$ aina vakiojonoa $(q)_{n=1}^{\infty}$ vastaavan reaaliluvun kanssa, joten reaaliluvun ja rationaaliluvun vertaaminen on sallittua Lemmassa 5.16.

Totesimme edellisessä luvussa, että *rationaalilukujen* Cauchyn jonolla $\alpha \in \mathscr{C}(\mathbb{Q})$ ei välttämättä ole raja-arvoa *rationaalilukujen* joukossa. Seuraava lause osoittaa, että tämä ongelma poistuu, kun jonon $\alpha \in \mathscr{C}(\mathbb{Q})$ suppenemista tarkastellaan *reaalilukujen* joukossa (luonnollisen samastuksen kautta).

Lause 5.17. *Olkoon $\alpha = (a_n)_{n=1}^{\infty}$ rationaalilukujen Cauchyn jono. Tällöin jono α suppenee reaalilukujen joukossa, ja sen raja-arvo on jonoa α vastaava ekvivalenssiluokka $x = [\alpha] \in \mathbb{R}$.*

Todistus. Olkoon $\varepsilon > 0$. Täytyy siis osoittaa, että löytyy $N \in \mathbb{N}$ siten, että

$$|a_n - x| < \varepsilon \qquad \text{aina kun } n \geq N. \tag{10}$$

Lemman 5.16 perusteella on olemassa $\varepsilon' \in \mathbb{Q}_+$ siten, että $0 < \varepsilon' < \varepsilon$. Koska $(a_n)_{n=1}^{\infty}$ on $\mathbb{Q}$:n Cauchyn jono, on olemassa $N \in \mathbb{N}$ siten, että

$$|a_n - a_m| < \varepsilon' \quad \text{aina kun } n, m \geq N. \tag{11}$$

Koska voimme kirjoittaa $a_n = [(a_n)_{k=1}^{\infty}] \in \mathbb{R}$ (huom: vakiojono!) ja toisaalta $x = [(a_k)_{k=1}^{\infty}]$, niin

$$|a_n - x| = \big|[(a_n)_{k=1}^{\infty}] - [(a_k)_{k=1}^{\infty}]\big| = \big|[(a_n - a_k)_{k=1}^{\infty}]\big|.$$

Kiinnitetään nyt $n \geq N$ ja merkitään $c_k = a_n - a_k$. Tällöin kohdan (11) mukaan $|c_k| = |a_n - a_k| < \varepsilon'$ aina, kun $k \geq N$, jolloin Lemman 5.15 nojalla $\big|[(c_k)_{k=1}^{\infty}]\big| \leq \varepsilon'$. Mutta nythän

$$|a_n - x| = \big|[(c_k)_{k=1}^{\infty}]\big| \leq \varepsilon' < \varepsilon$$

aina, kun $n \geq N$, joten väite (10) pätee. Siispä $x = \lim_{n\to\infty} a_n$. □

Lauseen 5.17 avulla voimme nyt todistaa, että itse asiassa *kaikki muutkin* reaalilukujen Cauchyn jonot suppenevat joukossa $\mathbb{R}$.

Lause 5.18. *Jokainen reaalilukujen Cauchyn jono suppenee.*

Todistus. Ideana on arvioida reaalilukujen Cauchyn jonoa sopivalla rationaalilukujen Cauchyn jonolla, jolla on edellisen lauseen nojalla raja-arvo joukossa $\mathbb{R}$. Osoitamme, että tämän raja-arvon täytyy olla myös alkuperäisen jonon raja-arvo.

Olkoon $(x_n)_{n=1}^{\infty} \in \mathscr{C}(\mathbb{R})$. Jokainen $x_n \in \mathbb{R}$ on siis jonkun rationaalilukujen Cauchyn jonon määräämä ekvivalenssiluokka. Olkoon jono $(a_{n,k})_{k=1}^{\infty}$ lukua x_n vastaavan luokan edustaja, toisin sanoen $x_n = [(a_{n,k})_{k=1}^{\infty}]$. Lauseen 5.17 nojalla $x_n = \lim_{k\to\infty} a_{n,k}$, joten kaikille $n \in \mathbb{Z}_+$ löytyy indeksi $K_n \in \mathbb{N}$ siten, että

$$|x_n - a_{n,k}| < \frac{1}{n} \qquad \text{aina kun } k \geq K_n.$$

Siten erityisesti

$$|x_n - a_{n,K_n}| < \frac{1}{n} \qquad \text{kaikilla } n \in \mathbb{N}.$$

Merkitään $q_n = a_{n,K_n}$.

Olkoon nyt $\varepsilon > 0$. Koska $(x_n)_{n=1}^{\infty} \in \mathscr{C}(\mathbb{R})$, niin on olemassa $N \in \mathbb{N}$ siten, että $|x_n - x_m| < \varepsilon/3$, kun $n, m \geq N$. Lemman 5.16 avulla voidaan lisäksi valita $N_1 \geq N$ siten, että $1/N_1 < \varepsilon/3$. Tällöin kaikille $n \geq N_1$ pätee

$$|x_n - q_n| < \frac{1}{n} \leq \frac{1}{N_1} < \varepsilon/3. \tag{12}$$

Jos nyt $n, m \geq N_1$, niin

$$\begin{aligned} |q_n - q_m| &= |q_n - x_n + x_n - x_m + x_m - q_m| \\ &\leq |q_n - x_n| + |x_n - x_m| + |x_m - q_m| < \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon. \end{aligned}$$

Näin ollen $(q_n)_{n=1}^{\infty}$ on rationaalilukujen Cauchyn jono. Jos $x = [(q_n)_{n=1}^{\infty}] \in \mathbb{R}$ on tätä jonoa vastaava reaaliluku, niin Lauseen 5.17 perusteella $x = \lim_{n\to\infty} q_n$.

On siis vielä osoitettava, että $x = \lim_{n\to\infty} x_n$. Koska $x = \lim_{n\to\infty} q_n$, niin löytyy $N_2 \in \mathbb{N}$ siten, että $|x - q_n| < \varepsilon/2$, aina kun $n \geq N_2$. Tällöin kaikille $n \geq \max\{N_1, N_2\}$ saadaan arvion (12) avulla

$$|x_n - x| \leq |x_n - q_n| + |q_n - x| < \varepsilon/3 + \varepsilon/2 < \varepsilon,$$

joten todellakin $x_n \to x$, kun $n \to \infty$. □

HUOMAUTUS: Koska kaikki joukon $\mathbb{R}$ Cauchyn jonot suppenevat, sanotaan, että $\mathbb{R}$ on *täydellinen*.

Cauchyn jonojen suppenemisen avulla voimme nyt todistaa seuraavat analyysin kannalta erittäin tärkeät periaatteet; muista, että pienin yläraja ja suurin alaraja määritellään reaalilukujen osajoukoille aivan samoin kuin rationaalilukujen osajoukoille määritelmässä 3.11.

Lause 5.19. (a) *Olkoon $A \subset \mathbb{R}$ epätyhjä ja ylhäältä rajoitettu joukko. Tällöin joukolla A on pienin yläraja joukossa $\mathbb{R}$.*

(b) *Olkoon $B \subset \mathbb{R}$ epätyhjä ja alhaalta rajoitettu joukko. Tällöin joukolla B on suurin alaraja joukossa $\mathbb{R}$.*

Todistus. Todistamme (a)-kohdan, (b)-kohta voidaan joko todistaa samaan tapaan tai palauttaa (a)-kohtaan tarkastelemalla joukkoa $-B$.

(A) Valitaan kaikille $n \in \mathbb{N}$ pienin *kokonaisluku* y_n jolle y_n/n on joukon A yläraja, toisin sanoen,

$$y_n = \min\{y \in \mathbb{Z} : y/n \text{ on joukon } A \text{ yläraja}\}.$$

Tällainen luku y_n löytyy, sillä A on ylhäältä rajoitettu, joten y/n on varmasti joukon A yläraja tarpeeksi suurilla $y \in \mathbb{Z}$, ja toisaalta joku näistä ylärajoista y/n on pienin, sillä jokaisella alhaalta rajoitetulla kokonaislukujen epätyhjällä osajoukolla on minimi (tämä voidaan todistaa induktiolla).

Luvun y_n määritelmän nojalla löytyy $x_n \in A$, jolle

$$\frac{y_n - 1}{n} < x_n \leq \frac{y_n}{n}. \tag{13}$$

Olkoot nyt $m, n \in \mathbb{N}$ siten, että $\frac{y_n}{n} \leq \frac{y_m}{m}$. Tällöin

$$\frac{y_m}{m} - \frac{1}{m} = \frac{y_m - 1}{m} < \frac{y_n}{n} \leq \frac{y_m}{m},$$

sillä muuten y_m ei olisi minimaalinen (mieti!). Siispä

$$0 \leq \frac{y_m}{m} - \frac{y_n}{n} < \frac{1}{m},$$

joten erityisesti

$$\left|\frac{y_m}{m} - \frac{y_n}{n}\right| < \frac{1}{m}\,.$$

Olkoon nyt $\varepsilon > 0$. Kun $m, n > 1/\varepsilon$, niin edellisen arvion nojalla

$$\left|\frac{y_m}{m} - \frac{y_n}{n}\right| < \varepsilon\,,$$

joten jono $(y_n/n)_{n=1}^{\infty}$ on (rationaalilukujen) Cauchyn jono. Lauseen 5.17 mukaan se suppenee kohti raja-arvoa $w \in \mathbb{R}$.

(B) Osoitamme, että luku $w \in \mathbb{R}$ on joukon A pienin yläraja. Näytetään aluksi, että w on joukon A yläraja: Jos olisikin $x \in A$, jolle $w < x$, niin $x - w \in \mathbb{R}_+$. Tällöin raja-arvon määritelmän nojalla löytyy $n \in \mathbb{N}$, jolle

$$\left|w - \frac{y_n}{n}\right| < \frac{x - w}{2}.$$

Tästä seuraa pienellä laskulla (vertaa kohtaan (14) alla), että

$$x - \frac{y_n}{n} \geq \frac{x - w}{2} > 0.$$

Siispä $x > y_n/n$, mikä on ristiriidassa sen kanssa, että y_n/n on joukon A yläraja. Näin ollen luvun w täytyy olla joukon A yläraja.

Täytyy vielä osoittaa, että w on todella pienin joukon A ylärajoista: Olkoon $u < w$. Tällöin voidaan valita niin suuri $n \in \mathbb{N}$, että

$$\left|\frac{y_n}{n} - w\right| \leq \frac{w - u}{4} \in \mathbb{R}_+$$

ja lisäksi $1/n \leq (w - u)/4$, jolloin kohdan (13) perusteella on olemassa $x_n \in A$ siten, että

$$\frac{y_n}{n} - x_n \leq \frac{1}{n} \leq \frac{w - u}{4}.$$

Nyt

$$
\begin{aligned}
x_n - u &= x_n - \frac{y_n}{n} + \frac{y_n}{n} - w + w - u \\
&\geq -\frac{w-u}{4} \underbrace{- \left| \frac{y_n}{n} - w \right|}_{\geq -\frac{w-u}{4}} + w - u \geq \frac{w-u}{2} > 0,
\end{aligned} \tag{14}
$$

joten $A \ni x_n > u$, ja niinpä u ei voi olla joukon A yläraja. Siispä w on välttämättä pienin joukon A ylärajoista. □

HUOMAUTUS: Analyysin kursseilla on tapana ottaa (todistamattomaksi) perusoletukseksi (eli *aksioomaksi*) joko

(i) *(suljettujen) sisäkkäisten välien periaate*: Jos $I_1 \supset I_2 \supset \ldots$ ovat epätyhjiä sisäkkäisiä suljettuja ja rajoitettuja reaalilukuvälejä, niin niiden leikkaus $\bigcap_{i=1}^{\infty} I_i$ on epätyhjä;

tai

(ii) *täydellisyysaksiooma*: Jokaisella ylhäältä rajoitetulla epätyhjällä joukolla $A \subset \mathbb{R}$ on pienin yläraja.

Nämä periaatteet ovat nyt lauseita(!); (ii) on Lause 5.19, (i):n perustelu jätetään harjoitustehtäväksi.

HUOMAUTUS: Sisäkkäisten välien periaatteen avulla voidaan jokaiselle reaaliluvulle määrätä desimaalikehitelmä (katso esimerkiksi *Kilpeläinen: Analyysi I*). Näin Cauchyn jonojen ekvivalenssiluokkien avulla abstraktisti määritellyille reaaliluvuillemme saadaan tuttu "konkreettinen" esitys.

Käsitellään vielä rationaalilukujen ongelmia havainnollistaneet Esimerkit 3.10 ja 3.12 loppuun reaalilukujen joukossa:

Esimerkki 5.20. Yhtälöllä $x^2 = 2$ on ratkaisu reaalilukujen joukossa. Tämä nähdään seuraavasti: Olkoon

$$A = \{x \in \mathbb{R} : x^2 < 2\}.$$

Toistamalla Esimerkin 3.12 päättelyn joukossa $\mathbb{R}$ huomaamme, että mikään joukon A luvuista ei voi olla joukon A yläraja. Vastaavasti nähdään, ettei mikään joukon

$$B = \{x \in \mathbb{R} : x^2 > 2\}$$

luvuista voi olla joukon A pienin yläraja. Toisaalta A on epätyhjä (esim. $1 \in A$) ja ylhäältä rajoitettu (esim. 2 on yläraja), joten Lauseen 5.19 mukaan joukolla A on pienin yläraja $a \in \mathbb{R}$. Edellä todetun perusteella ei voi olla $a^2 < 2$ eikä $a^2 > 2$, joten välttämättä $a^2 = 2$.

Samalla päättelyllä saadaan, että myös joukon A suurin alaraja on yhtälön $x^2 = 2$ ratkaisu.

Itse asiassa kaikilla positiivisilla reaaliluvuilla on olemassa "kaikki" juuret:

Lause 5.21. *Olkoon $x \in \mathbb{R}_+$, ja olkoon $n \in \mathbb{N}$. Tällöin on $\sqrt[n]{x} \in \mathbb{R}_+$, jolle pätee $(\sqrt[n]{x})^n = x$. Lisäksi, jos $x, y \in \mathbb{R}_+$ ja $x < y$, niin $\sqrt[n]{x} < \sqrt[n]{y}$.*

Todistus. Luvun $\sqrt[n]{x}$ olemassaolo todistetaan samaan tapaan kuin esimerkissä 5.20 todistetaan luvun $\sqrt{2}$ olemassaolo. Järjestyksen säilyminen jätetään harjoitustehtäväksi. □

HUOMIOITA: (i) Lukua $\sqrt[n]{x}$ sanotaan luvun $x \in \mathbb{R}_+$ n:nneksi juureksi

(ii) Jos $x \in -\mathbb{R}_+$, niin yhtälöllä $r^n = x$ on ratkaisu $r \in -\mathbb{R}_+$ täsmälleen silloin, kun n on pariton.

(iii) Jos $x \in \mathbb{R}_+$ ja n on parillinen, niin yhtälöllä $r^n = x$ on ratkaisut $\pm\sqrt[n]{x}$.

———————

HUOMAUTUS* : Reaaliluvut on mahdollista määritellä myös rationaalilukujen *Dedekindin leikkausten* avulla: Sanomme, että joukko $A \subset \mathbb{Q}$ on Dedekindin leikkaus (DL), jos seuraavat ehdot ovat voimassa:

- $A \neq \emptyset$, $A \neq \mathbb{Q}$;
- Jos luvulle $x \in \mathbb{Q}$ löytyy $a \in A$ siten, että $x \leq a$, niin $x \in A$;
- Kaikille $a \in A$ löytyy $b \in A$ siten, että $a < b$.

Esimerkiksi joukko

$$A = \{a \in \mathbb{Q} : a < 0 \text{ tai } a^2 \leq 2\}$$

on Dedekindin leikkaus.

Reaalilukujen joukko voidaan nyt määritellä kaikkien rationaalilukujen Dedekindin leikkausten joukkona:

$$\mathbb{R} = \{A \subset \mathbb{Q} : A \text{ on DL}\},$$

jolloin rationaaliluku $q \in \mathbb{Q}$ voidaan samastaa joukon

$$Q = \{a \in \mathbb{Q} : a < q\}$$

kanssa.

Reaalilukujen yhteenlaskun määritelmä on suoraviivainen,

$$A + B = \{a + b : a \in A,\ b \in B\}.$$

Vähennyslasku määritellään asettamalla

$$A - B = \{a - b : a \in A,\ b \in \mathbb{Q} \setminus B\},$$

jolloin erityisesti

$$-B = 0 - B = \{a - b : a < 0,\ b \in \mathbb{Q} \setminus B\}.$$

Kertolaskun määritelmä on hieman mutkikkaampi. Määritellään tätä varten ensin järjestys joukkoon $\mathbb{R}$ asettamalla

$$A \leq B \iff A \subset B.$$

Jos nyt $A, B \in \mathbb{R}$ ja $A, B \geq 0$, niin

$$A \cdot B = \{ab : a \in A,\ a \geq 0 \text{ ja } b \in B,\ b \geq 0\} \cup \{q \in \mathbb{Q} : q < 0\}.$$

Jos $A < 0$ tai $B < 0$, niin kertolaskun määritelmä palautetaan positiivisten lukujen kertolaskuksi asettamalla (muodollisesti)

$$A \cdot B = -\big(A \cdot (-B)\big) = -\big(-A \cdot B)\big) = \big(-A \cdot (-B)\big);$$

jossakin näistä kohdista molemmat kerrottavat ovat ei-negatiivisia, tämä kohta määrittää muut tulot.

Määritelmien perusteella on melko selvää, että laskutoimitusten ominaisuuksien todistaminen on jonkin verran työläämpää kuin Cauchyn jonoihin perustuvassa määritelmässä (vrt. Lause 5.6). Toisaalta Dedekindin leikkausten avulla joukon $\mathbb{R}$ täydellisyyden osoittaminen on helppoa: Jos $\emptyset \neq \mathscr{A} \subset \mathbb{R}$ on ylhäältä rajoitettu, niin luku

$$M = \{q \in \mathbb{Q} : q \in A \text{ jollekin } A \in \mathscr{A}\} = \bigcup_{A \in \mathscr{A}} A$$

on joukon $\mathscr{A}$ pienin yläraja. Jos nimittäin $A \in \mathscr{A}$ ja $a \in A$, niin joukon M määritelmän nojalla $a \in M$. Siispä $A \subset M$ eli $A \leq M$, mistä näemme, että M on $\mathscr{A}$:n yläraja. Jos toisaalta M' on jokin $\mathscr{A}$:n yläraja ja $q \in M$, niin $q \in A$ jollekin $A \in \mathscr{A}$, jolloin $A \leq M'$ eli $A \subset M'$. Näin ollen myös $q \in M'$, joten $M \subset M'$ eli $M \leq M'$. Siispä M on $\mathscr{A}$:n ylärajoista pienin.

Vertaa tätä Lauseiden 5.17–5.19 todistuksiin, joissa sama asia perusteltiin Cauchyn jonojen avulla!

———————

Historiaa: Idea reaalilukujen määrittelemisestä rationaalilukujen avulla on vanha, se esiintyy tavallaan jo antiikin Kreikassa Eudoksoksen (408–355 eKr.) kehittämässä suhteiden teoriassa. Uuden ajan ensimmäinen tärkeä lukukäsitteen kehittäjä oli Simon Stevin (1548–1620, Hollanti), joka esitti ajatuksen, että kaikkia lukuja voidaan approksimoida mielivaltaisella tarkkuudella (päättyvien) desimaalilukujen avulla. Kesti kuitenkin pitkään ennen kuin reaaliluvuille saatiin täsmällinen ja käyttökelpoinen määritelmä. Esimerkiksi Augustin-Louis Cauchy (1789–1857, Ranska) ei kiinnittänyt oppikirjassaan *Cours d'analyse* (1821) suurempaa huomiota reaalilukujen määritelmään, totesi vain, että reaaliluvut saadaan rationaalilukujen jonojen raja-arvoina (hän ei siis varsinaisesti käyttänyt Cauchyn jonoja(!)).

Matemaattisen analyysin täsmällistyminen 1800-luvun kuluessa loi kuitenkin tarpeen myös reaalilukujen tarkalle määritelmälle, ja kävikin niin, että useat matemaatikot julkaisivat hyvin lyhyen ajan sisällä erilaisia konstruktioita reaaliluvuille: Richard Dedekind (1831–1916, Saksa) kehitteli Dedekindin leikkauksiin perustuvan reaalilukujen määritelmän vuonna 1858, mutta se julkaistiin vasta 1872. Georg Cantor (1845–1918, Venäjä/Saksa) esitteli samana vuonna 1872 oman reaalilukujen määritelmänsä rationaalilukujen Cauchyn jonojen avulla. Tätä lähestymistapaa (jota siis mekin tällä kurssilla noudatamme) olivat käyttäneet hieman aikaisemmin toisistaan riippumatta myös Charles Méray (1835–1911, Ranska) vuonna 1869 ja Eduard Heine (1821–1881, Saksa), myöskin vuonna 1872. Mainitaan tässä yhteydessä vielä Karl Weierstrass (1815–1897, Saksa), joka käytti luennoillaan täsmällistä desimaalikehitelmiin perustuvaa reaalilukujen määritelmää vuodesta 1865 alkaen (julkaistiin vuonna 1867).

Kaikki nämä erilaiset "mallit" reaaliluvuille johtavat kuitenkin oleellisesti samaan lopputulokseen, sillä ne ovat keskenään *isomorfisia*. Toisin sanoen, eri mallien välillä on olemassa bijektio, joka säilyttää joukon $\mathbb{R}$ rakenteen, eli laskutoimitukset ja järjestyksen.

6. Kompleksiluvut

Lauseen 5.21 mukaan jokaisella positiivisella reaaliluvulla on positiivinen n:s juuri kaikilla $n \in \mathbb{N}$. Sen sijaan esimerkiksi yhtälöllä $x^2 = -1$ ei ole ratkaisua reaalilukujen joukossa: $-1 \notin \mathbb{R}_+$ ja toisaalta kaikkien reaalilukujen neliöt ovat ei-negatiivisia.

Jotta tällekin yhtälölle saataisiin ratkaisu, täytyy lukualuetta laajentaa jälleen. Aikaisemmissa laajennuksissa kokonaislukujen välit "täytettiin" ensin rationaaliluvuilla ja sitten jäljelle jääneet reiät "tilkittiin" irrationaaliluvuilla. Näiden toimenpiteiden jälkeen ei joukossa $\mathbb{R}$ ole enää reikiä joihin lukualuetta voisi edelleen laajentaa. Miten uusi laajennus tulisi siis tehdä?

Idea: $\mathbb{R}$ on jo "täynnä", joten laajennetaan "sivulle".

Haluaisimme siis lisätä lukujärjestelmäämme mukaan alkion $\sqrt{-1}$ siten, että reaalilukujen laskutoimitukset voidaan suorittaa myös tässä uudessa joukossa ja toivon mukaan myös laskutoimitusten hyvät ominaisuudet säilyvät. Erityisesti lukuun $\sqrt{-1}$ täytyy voida lisätä reaaliluku ja sitä täytyy voida kertoa reaaliluvuilla, jolloin uuden lukualueemme tulee sisältää ainakin kaikki muotoa $a + b\sqrt{-1}$ olevat alkiot, missä $a, b \in \mathbb{R}$. Jos reaalilukujen laskusäännöt ovat edelleen voimassa, niin tätä muotoa olevien "lukujen" summaksi saadaan

$$(a + b\sqrt{-1}) + (c + d\sqrt{-1}) = (a + c) + (b + d)\sqrt{-1}$$

ja tuloksi

$$\begin{aligned}(a + b\sqrt{-1})(c + d\sqrt{-1}) &= ac + ad\sqrt{-1} + bc\sqrt{-1} + bd\sqrt{-1}\sqrt{-1} \\ &= (ac - bd) + (ad + bc)\sqrt{-1},\end{aligned}$$

missä käytimme hyväksi tietoa $\sqrt{-1}\sqrt{-1} = -1$. Siispä näiden laskutoimitusten tulokset ovat myös samaa muotoa olevia "lukuja".

Kun ajatelemme "lukua" $a + b\sqrt{-1}$ reaalilukuparina $(a, b) \in \mathbb{R}^2$, voimme asettaa edellisten havaintojen jälkeen täsmällisen määritelmän tälle uudelle lukualueelle:

Määritelmä 6.1. *Kompleksilukujen joukko* $\mathbb{C}$ on

$$\mathbb{C} = \mathbb{R}^2 = \{(a, b) : a, b \in \mathbb{R}\}$$

varustettuna komponenteittaisella yhteenlaskulla

$$(a, b) + (c, d) = (a + c, b + d)$$

ja kertolaskulla, joka määritellään asettamalla

$$(a, b)(c, d) = (ac - bd, ad + bc).$$

Kaikki reaalilukujen laskutoimitusten hyvät ominaisuudet yleistyvät todella myös kompleksiluvuille:

Lause 6.2. (a) *Kompleksilukujen yhteenlasku ja kertolasku ovat assosiatiivisia.*

(b) *Kompleksilukujen yhteenlasku ja kertolasku ovat kommutatiivisia.*

(c) *Kompleksilukujen kertolasku on distributiivinen yhteenlaskun suhteen.*

(d) *Alkio* $0 = (0, 0)$ *on kompleksilukujen yhteenlaskun neutraalialkio ja alkio* $1 = (1, 0)$ *on kertolaskun neutraalialkio.*

(e) *Jokaisella kompleksiluvulla* z *on vastaluku* $-z = (-1, 0)z$ *(käänteisalkio yhteenlaskun suhteen).*

(f) *Jokaisella nollasta poikkeavalla kompleksiluvulla* $z = (x, y)$ *on käänteisluku*

$$z^{-1} = \left(\frac{x}{x^2 + y^2}\,,\ \frac{-y}{x^2 + y^2}\right)$$

(käänteisalkio kertolaskun suhteen).

Todistus. (a) Yhteenlasku seuraa suoraan reaalilukujen yhteenlaskun assosiatiivisuudesta, kertolasku jätetään harjoitustehtäväksi.

(b) Seuraavat suoraan reaalilukujen laskutoimitusten kommutatiivisuudesta.

(c) Harjoitustehtävä.

(d) Helppo lasku.

(e) Käyttämällä hyväksi distributiivisuutta ja (d)-kohtaa saadaan

$$z + (-z) = (1,0)z + (-1,0)z = \big((1,0) + (-1,0)\big)z = (0,0)z = 0z = 0.$$

(f) Kun $z = (x,y) \neq (0,0)$, niin

$$(x,y)\left(\frac{x}{x^2+y^2}\,,\,\frac{-y}{x^2+y^2}\right) = \left(\frac{x^2}{x^2+y^2} + \frac{y^2}{x^2+y^2}\,,\,\frac{-xy}{x^2+y^2} + \frac{xy}{x^2+y^2}\right) = (1,0).$$

□

Määrittelemme kompleksilukujen vähennys- ja jakolaskut aivan kuten reaaliluvuille: Kun $z, w \in \mathbb{C}$, niin $z - w = z + (-w)$, ja jos lisäksi $w \neq 0$, niin $z/w = z \cdot w^{-1}$.

Myös reaalilukujen supistussäännöt yleistyvät kompleksiluvuille:

Lemma 6.3. (a) *Jos $z_1, z_2, w \in \mathbb{C}$ ja $z_1 + w = z_2 + w$, niin $z_1 = z_2$.*

(b) *Jos $z, w \in \mathbb{C}$ ja $zw = 0$, niin $z = 0$ tai $w = 0$.*

(c) *Jos $z_1, z_2, w \in \mathbb{C}$, $w \neq 0$ ja $z_1 w = z_2 w$, niin $z_1 = z_2$.*

Todistus. (a) Todistetaan kuten aiemmin muissa lukualueissa.

(b) Vaatii pienen tarkastelun, joka jätetään harjoitustehtäväksi.

(c) Todistetaan kuten aiemmin muissa lukualueissa. □

Reaalilukujen joukko on luontevaa samastaa kompleksilukujen "x-akselin" kanssa. Määritellään siis kuvaus $j\colon \mathbb{R} \to \mathbb{C}$ asettamalla $j(x) = (x,0)$.

Lemma 6.4. *Kuvaus j on injektio, jolle pätee*

$$j(x+y) = j(x) + j(y) \quad \textit{ja} \quad j(xy) = j(x)j(y)$$

kaikilla $x, y \in \mathbb{R}$.

Todistus. Helppo harjoitustehtävä. □

Sopimus: Tästedes samastamme reaaliluvut vastaavan kompleksilukujen osajoukon $j(\mathbb{R}) \subset \mathbb{C}$ kanssa, ts. jos $x \in \mathbb{R}$, niin $x = (x,0) \in \mathbb{C}$.

Kompleksilukua $i = (0,1)$ kutsutaan *imaginaariyksiköksi*. Jokainen kompleksiluku $z = (a,b)$ voidaan nyt esittää summana

$$(a,b) = (a,0) + (0,b) = (a,0) + (0,1)(b,0) = a + ib,$$

missä viimeisessä vaiheessa käytetään edellä tehtyä sopimusta, jonka mukaan kompleksiluku $(a,0)$ samastetaan reaaliluvun a kanssa (vastaavasti luvulle b).

Näillä merkinnöillä kompleksilukujen laskutoimitukset saavat muodot

$$(a+ib) + (c+id) = (a+c) + i(b+d),$$
$$(a+ib)(c+id) = (ac-bd) + i(ad+bc).$$

HUOMAA: $i^2 = (0,1)(0,1) = (-1,0) = -1$, joten yhtälöllä $x^2 = -1$ on todella ratkaisu kompleksilukujen joukossa.

Määritelmä 6.5. (1) Kompleksiluvun $z = a + ib$ *reaaliosa* on $\mathrm{Re}(z) = a$ ja *imaginaariosa* on $\mathrm{Im}(z) = b$. Siispä $z = \mathrm{Re}(z) + i\,\mathrm{Im}(z)$.

(2) Luku $\overline{z} = a - ib$ on kompleksiluvun $z = a + ib$ *(kompleksi)konjugaatti* eli *liittoluku*.

Kompleksikonjugaatilla on seuraavat laskennalliset ominaisuudet:

Lemma 6.6. (a) *Jos* $z = x + iy \in \mathbb{C}$, *niin* $z\overline{z} = x^2 + y^2$ $\big(\in \mathbb{R}\big)$.

(b) $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$ *kaikilla* $z, w \in \mathbb{C}$.

(c) $\overline{z + w} = \overline{z} + \overline{w}$ *kaikilla* $z, w \in \mathbb{C}$.

(d) *Kaikilla* $z \in \mathbb{C}$ *pätee:* $z = \overline{z} \iff z \in \mathbb{R}$.

Todistus. (a) $z\overline{z} = (x + iy)(x - iy) = x^2 + y^2 + ixy - ixy = x^2 + y^2$.

(b) Harjoitustehtävä.

(c) Olkoon $z = a + ib$ ja $w = c + id$. Koska $z + w = a + c + i(b + c)$, niin

$$\overline{z + w} = a + c - i(b + c) = a - ib + c - id = \overline{z} + \overline{w}.$$

(d) Olkoon $z = x + iy$. Tällöin Lemmaa 6.3 käyttäen saamme

$$\begin{aligned} z = \overline{z} &\iff x + iy = x - iy \iff iy = -iy \\ &\iff y = -y \iff y = 0 \iff z \in \mathbb{R}. \end{aligned}$$

□

HUOMIO*: Kompleksiluvuille ei voi määritellä laskutoimitusten kanssa yhteensopivaa järjestystä, joka laajentaisi reaalilukujen järjestyksen. Jos tällainen järjestys ‘ $>$ ‘ nimittäin olisi olemassa, niin kaikille $z \in \mathbb{C} \setminus \{0\}$ olisi $z^2 > 0$: jos $z > 0$, niin pitäisi olla $z^2 = z \cdot z > 0$, ja jos $z < 0$, niin $-z > 0$, jolloin $z^2 = (-1)^2 z^2 = (-z)^2 > 0$. Kuitenkin $i \neq 0$ ja $i^2 = -1 < 0$, joten tällaista järjestystä ei voi olla olemassa.

Reaaliluvun itseisarvoa vastaava käsite voidaan kuitenkin määritellä myös kompleksiluvuille:

Määritelmä 6.7. Kompleksiluvun $z = x + iy$ *moduli* (eli itseisarvo) on

$$|z| = \sqrt{z\overline{z}} = \sqrt{x^2 + y^2} = \|(x, y)\|,$$

missä $\|\cdot\|$ on tason $\mathbb{R}^2$ *euklidinen normi* (vrt. LAG1 ja EA).

HUOMIOITA: (i) Jos $z \in \mathbb{R}$ (ts. $z = x + i \cdot 0$), niin

$$|z| = \sqrt{x^2} = \begin{cases} x, & \text{jos } x \geq 0, \\ -x, & \text{jos } x < 0. \end{cases}$$

(ii) $|z| = |\overline{z}|$ kaikilla $z \in \mathbb{C}$.

(iii) $\mathrm{Re}(z) \leq |z|$ ja $\mathrm{Im}(z) \leq |z|$ kaikilla $z \in \mathbb{C}$.

(iv) $|zw| = |z||w|$ kaikilla $z, w \in \mathbb{C}$ (harjoitustehtävä).

Lemma 6.8. *Kompleksilukujen moduli toteuttaa kolmioepäyhtälön:*

$$|z + w| \leq |z| + |w|$$

kaikilla $z, w \in \mathbb{C}$.

Todistus. Olkoot $z, w \in \mathbb{C}$. Laskemalla on helppo todeta, että

$$z\overline{w} + \overline{z}w = 2\,\mathrm{Re}(z\overline{w}) \leq 2|z\overline{w}| = 2|z||w|,$$

missä käytimme hyväksi lemmaa edeltäviä huomioita (ii)–(iv). Siten

$$\begin{aligned} |z+x|^2 &= (z+w)(\overline{z}+\overline{w}) = |z|^2 + z\overline{w} + \overline{z}w + |w|^2 \\ &\leq |z|^2 + 2|z||w| + |w|^2 = (|z| + |w|)^2, \end{aligned}$$

ja väite seuraa Lauseesta 5.21. □

Modulin avulla kompleksiluvun $z \neq 0$ käänteisluvulle saadaan helppo esitys:

$$z^{-1} = \frac{\overline{z}}{|z|^2}.$$

Esimerkki 6.9. Lasketaan mitä on kahden kompleksiluvun osamäärä z/w. Olkoon siis $z = a + ib$ ja $w = c + id \neq 0$. Tällöin

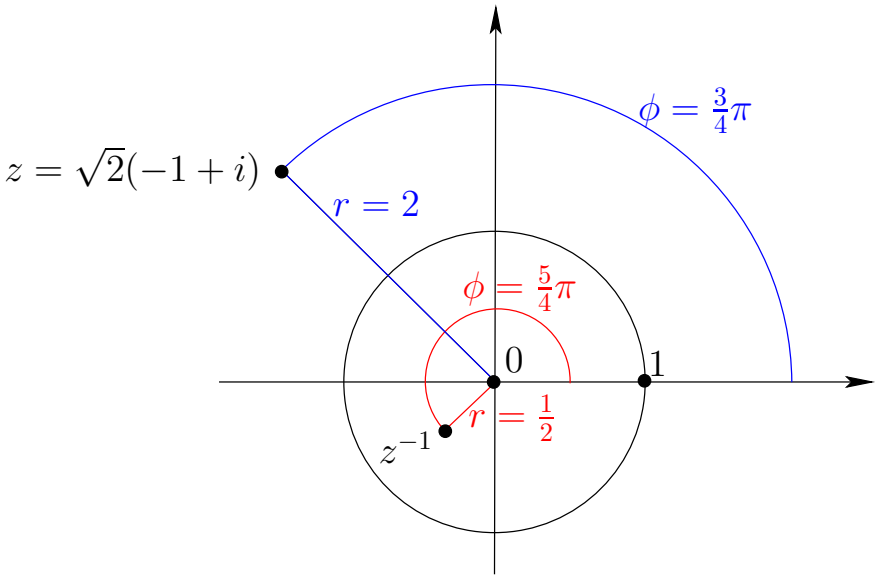
$$\frac{z}{w} = zw^{-1} = \frac{z\overline{w}}{|w|^2} = \frac{(a+ib)(c-id)}{c^2+d^2} = \frac{ac+bd}{c^2+d^2} + i\frac{bc-ad}{c^2+d^2}\,.$$

Napakoordinaatit:
Olkoon $z = x + iy \in \mathbb{C} \setminus \{0\}$, ja olkoon φ tason $\mathbb{R}^2$ vektorien $(1,0)$ ja (x,y) välinen kulma vastapäivään (eli "positiiviseen kiertosuuntaan"). Tällöin

$$x = \|(x,y)\| \cos\varphi = |z| \cos\varphi \quad \text{ja} \quad y = \|(x,y)\| \sin\varphi = |z| \sin\varphi,$$

joten voimme kirjoittaa

$$z = |z|(\cos\varphi + i \sin\varphi).$$



Kuva 2. Kompleksilukujen $z = \sqrt{2}(i-1)$ ja $z^{-1} = -\frac{1+i}{2\sqrt{2}}$ napakoordinaatit ovat $(2, \frac{3}{4}\pi)$ ja $(\frac{1}{2}, \frac{5}{4}\pi)$.

Tämän *napakoordinaattiesityksen* ja trigonometristen funktioiden yhteenlaskukaavojen avulla saamme havainnollisen esityksen kompleksilukujen kertolaskulle:

Lemma 6.10. (a) *Olkoot* $z = r(\cos\varphi + i\sin\varphi)$ *ja* $w = s(\cos\theta + i\sin\theta)$. *Tällöin*

$$zw = rs\big(\cos(\varphi+\theta) + i\sin(\varphi+\theta)\big).$$

(b) *Olkoot* $z_k = r_k(\cos\varphi_k + i\sin\varphi_k)$, $k = 1, 2, \ldots, n$. *Tällöin*

$$\prod_{k=1}^{n} z_k = \Big(\prod_{k=1}^{n} r_k\Big)\Big(\cos\Big(\sum_{k=1}^{n}\varphi_k\Big) + i\sin\Big(\sum_{k=1}^{n}\varphi_k\Big)\Big).$$

Todistus. (a) Sinin ja kosinin yhteenlaskukaavojen avulla saamme

$$\begin{aligned} &rs\big(\cos(\varphi+\theta) + i\sin(\varphi+\theta)\big) \\ &\qquad = rs\big(\cos\varphi\cos\theta - \sin\varphi\sin\theta + i(\sin\varphi\cos\theta + \cos\varphi\sin\theta)\big) \\ &\qquad = rs\big((\cos\varphi + i\sin\varphi)(\cos\theta + i\sin\theta)\big) \\ &\qquad = r(\cos\varphi + i\sin\varphi)\cdot s(\cos\theta + i\sin\theta) = zw. \end{aligned}$$

(b) Seuraa (a)-kohdasta induktiolla. □

Esimerkki 6.11. (a) Olkoon $z = r(\cos\varphi + i\sin\varphi) \in \mathbb{C}$. Koska $i = \cos(\pi/2) + i\sin(\pi/2)$, saadaan Lauseesta 6.10

$$iz = r\big(\cos(\varphi+\pi/2) + i\sin(\varphi+\pi/2)\big).$$

Siten luvulla i kertominen vastaa tasossa kiertoa kulman $\pi/2$ verran positiiviseen suuntaan.

(b) Erikoistapauksena Lauseen 6.10 (b)-kohdasta saadaan kuuluisa *de Moivren* kaava:

$$(\cos\varphi + i\sin\varphi)^k = \cos(k\varphi) + i\sin(k\varphi). \tag{15}$$

Napakoordinaattiesitystä ja kertolaskusääntöä käyttäen on helppo tutkia kompleksilukujen *juuria*:

Määritelmä 6.12. Jos $z, w \in \mathbb{C}$, $m \in \mathbb{Z}_+$ ja $z^m = w$, niin z on luvun w *m:s juuri.*

Lemma 6.13. *Luvulla* $1 \in \mathbb{C}$ *on* m *kappaletta* m*:nsiä juuria, toisin sanoen, yhtälöllä* $z^m = 1$ *on* m *(kompleksista) ratkaisua.*

Todistus. Olkoon

$$\zeta_m = \cos\frac{2\pi}{m} + i\sin\frac{2\pi}{m}.$$

Tällöin de Moivren kaavan (15) nojalla

$$\zeta_m^m = \cos 2\pi + i\sin 2\pi = 1,$$

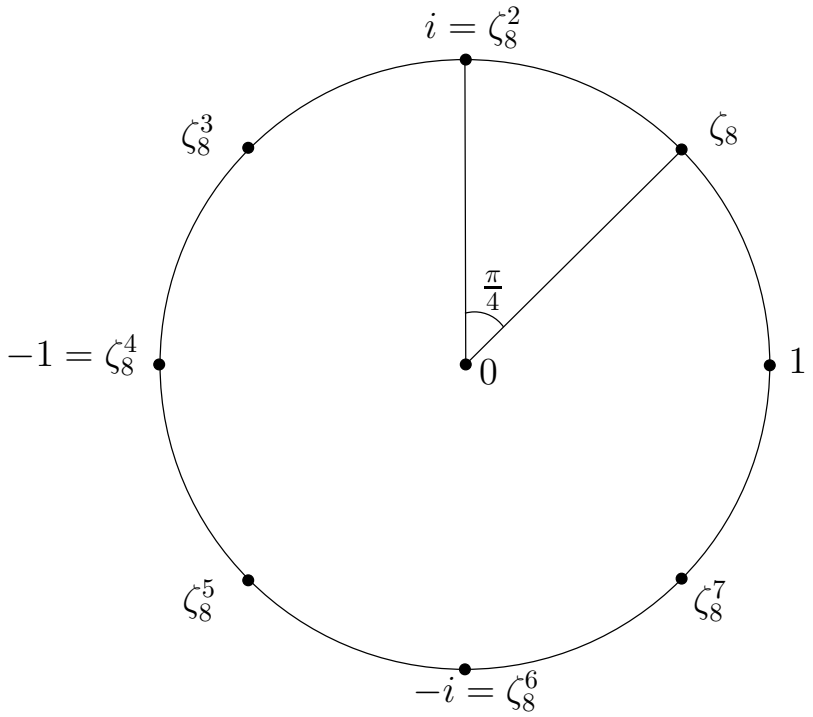
joten ζ_m on luvun 1 eräs m:s juuri. Jos nyt $n \in \{1, 2\ldots, m\}$, niin jälleen kaavaa (15) käyttäen saadaan

$$\zeta_m^n = \cos\frac{2\pi n}{m} + i\sin\frac{2\pi n}{m},$$

joten

$$(\zeta_m^n)^m = \cos\frac{2\pi nm}{m} + i\sin\frac{2\pi nm}{m} = 1.$$

Siispä kaikki luvut ζ_m^n (jotka ovat todella eri lukuja, kun $n \in \{1, 2\ldots, m\}$) ovat luvun 1 m:nsiä juuria. □



KUVA 3. Ykkösen kahdeksannet juuret.

HUOMAUTUS: $\zeta_m^m = 1 \in \mathbb{R}$ ja jos m on parillinen, niin

$$\zeta_m^{m/2} = \cos\tfrac{2\pi m/2}{m} + i\sin\tfrac{2\pi m/2}{m} = \cos\pi + i\sin\pi = -1 \in \mathbb{R}.$$

Nämä ovat ainoat reaaliset ratkaisut yhtälölle $z^m = 1$.

Lemman 6.13 ja napakoordinaattiesityksen avulla löydetään jokaisen nollasta poikkeavan kompleksiluvun juuret:

Lause 6.14. *Jokaisella kompleksiluvulla $w \in \mathbb{C}\setminus\{0\}$ on m kappaletta m:nsiä juuria.*

Todistus. Kun $w = r(\cos\varphi + i\sin\varphi)$, niin luku

$$z = \sqrt[m]{r}\Big(\cos\frac{\varphi}{m} + i\sin\frac{\varphi}{m}\Big)$$

on luvun w yksi m:s juuri. Kaikki muut ovat muotoa $z\zeta_m^n$, $n \in \{1,\dots,m\}$, missä ζ_m on ykkösen m:s juuri. Yksityiskohdat jätetään harjoitustehtäväksi. □

Esimerkki 6.15. Luvun $2 \in \mathbb{C}$ kolmannet juuret ovat $\sqrt[3]{2}$,

$$\sqrt[3]{2}\Big(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}\Big) = \sqrt[3]{2}\Big(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\Big)$$

ja

$$\sqrt[3]{2}\Big(\cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3}\Big) = -\sqrt[3]{2}\Big(\frac{1}{2} + i\frac{\sqrt{3}}{2}\Big).$$

HUOMAUTUS: Koska jokaisella kompleksiluvulla on useita juuria, täytyy positiivisille reaaliluvuille tunnettujen juurien laskusääntöjen kanssa olla varovainen kompleksilukujen joukossa. Esimerkiksi $\sqrt{a}\sqrt{b} = \sqrt{ab}$, kun $a, b \in \mathbb{R}_+$, mutta toisaalta

$$\sqrt{-1}\sqrt{-1} = i^2 = -1 \neq 1 = \sqrt{1} = \sqrt{(-1)(-1)}\,. \qquad \text{Missä vika?}$$

Tällaisia ongelmia käsitellään tarkemmin kompleksianalyysin kurssilla.

Edellä on siis saatu ratkaistua muotoa $z^m + a_0 = 0$, $m \in \mathbb{Z}_+$, $a_0 \in \mathbb{C}$, olevat yhtälöt. Tarkastellaan seuraavaksi muiden kompleksilukukertoimisten polynomiyhtälöiden ratkaisemista.

Aloitamme toisen asteen yhtälöistä. Jos $a_0, a_1, a_2 \in \mathbb{R}$, niin tunnetusti luvut

$$x_1 = \frac{-a_1 + \sqrt{a_1^2 - 4a_2a_0}}{2a_2} \quad \text{ja} \quad x_2 = \frac{-a_1 - \sqrt{a_1^2 - 4a_2a_0}}{2a_2}$$

ovat toisen asteen polynomiyhtälön

$$a_2x^2 + a_1x + a_0 = 0$$

ratkaisut, kunhan $a_1^2 - 4a_2a_0 \geq 0$, eli kun luvulla $a_1^2 - 4a_2a_0 \in \mathbb{R}$ on reaalinen neliöjuuri.

Toisaalta Lauseen 6.14 nojalla jokaisella kompleksiluvulla on neliöjuuri, ja suoraan laskemalla voimmekin todeta, että jokaisella toisen asteen *kompleksilukukertoimisella* yhtälöllä on kaksi ratkaisua *kompleksilukujen* joukossa. Kirjataan tämä tulos seuraavassa muodossa:

Lause 6.16. *Yhtälön*

$$z^2 + a_1z + a_0 = 0, \qquad a_0, a_1 \in \mathbb{C},$$

ratkaisuja ovat luvut

$$z_1 = -\frac{a_1}{2} + \sqrt{\left(\frac{a_1}{2}\right)^2 - a_0} \qquad \textit{ja} \qquad z_2 = -\frac{a_1}{2} - \sqrt{\left(\frac{a_1}{2}\right)^2 - a_0}\,.$$

Todistus. Havaitsemme, että

$$(z - z_1)(z - z_2) = z^2 + a_1z + a_0,$$

mistä väite seuraa. □

Myös kolmannen ja neljännen asteen (kompleksikertoimisille) polynomiyhtälöille on olemassa "ratkaisukaavat". Kolmannen asteen yhtälön ratkaisua varten tarvitsemme seuraavan toisen asteen yhtälöitä koskevan aputuloksen:

Lemma 6.17. *Olkoot $z_1, z_2 \in \mathbb{C}$. Jos $z_1 + z_2 = -a_1$ ja $z_1z_2 = a_0$, niin z_1 ja z_2 ovat polynomin $P(z) = z^2 + a_1z + a_0$ nollakohdat.*

Todistus. $(z - z_1)(z - z_1) = z^2 - (z_1 + z_2)z + z_1z_2$. □

Merkitään vielä

$$\zeta = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} = \frac{-1 + i\sqrt{3}}{2}\,,$$

jolloin $\zeta \in \mathbb{C}$ on (eräs) ykkösen kolmas juuri. Nyt voimme esittää kolmannen asteen yhtälön yleisen ratkaisun.

Lause 6.18 ("Cardanon kaavat")**.** *Yhtälön*

$$z^3 + pz + q = 0, \qquad p, q \in \mathbb{C}, \tag{16}$$

ratkaisuja ovat kompleksiluvut

$$z_1 = u_0 + v_0, \quad z_2 = \zeta u_0 + \zeta^2 v_0 \quad \textit{ja} \quad z_3 = \zeta^2 u_0 + \zeta v_0,$$

missä

$$u_0 = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} \qquad (17)$$
$$v_0 = \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

ja kuutiojuurten arvot on valittu siten, että

$$u_0 v_0 = -\frac{p}{3}.$$

HUOMAUTUS. Kaikki kolmannen asteen kompleksikertoimiset yhtälöt saadaan muuttujanvaihdolla muotoon (16): Jos yhtälöön

$$w^3 + a_1 w^2 + a_2 w + a_3 = 0$$

sijoitetaan $w = z - a_1/3$, saadaan muotoa (16) oleva yhtälö, joka voidaan ratkaista Lauseen 6.18 avulla. Alkuperäisen yhtälön ratkaisut saadaan nyt lisäämällä näihin ratkaisuihin $-a_1/3$. Näin ollen kaikki kolmannen asteen yhtälöt voidaan ratkaista Lauseen 6.18 avulla.

Lauseen 6.18 todistus. Sijoitetaan aluksi yhtälöön (16) $z = u + v$. Suoraviivaisen laskun jälkeen yhtälö saadaan muotoon

$$(u^3 + v^3 + q) + (3uv + p)(u + v) = 0. \qquad (18)$$

Tämä yhtälö toteutuu (ainakin) jos

$$u^3 + v^3 = -q \quad \text{ja} \quad uv = -p/3 \ \ (\text{jolloin } u^3 v^3 = -(p/3)^3\,).$$

Lemman 6.17 nojalla tällaiset u^3 ja v^3 ovat toisen asteen yhtälön

$$w^2 + qw - (p/3)^3 = 0$$

ratkaisuja. Mutta tämä yhtälö osataan aina ratkaista (Lause 6.16), ja ratkaisut ovat

$$-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3} \quad \text{ja} \quad -\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}.$$

Jos siis valitsemme

$$\begin{cases} u = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} \\ v = \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}, \end{cases} \qquad (19)$$

niin $u^3 + v^3 = -q$ ja $u^3 v^3 = -(p/3)^3$. Toisaalta, koska jokaisella kompleksiluvulla on kolme kappaletta kolmansia juuria, löytyy yhteensä yhdeksän eri kompleksilukuparia (u, v), jotka toteuttavat yhtälöparin (19). Nämä saadaan ottamalla ensin eräät ratkaisut u ja v ja muodostamalla sitten kaikki lukujen u, ζu, $\zeta^2 u$ ja v, ζv, $\zeta^2 v$ parit (vertaa Lauseeseen 6.14).

Kaikki nämä parit eivät kuitenkaan ole yhtälön (18) ratkaisuja, sillä tätä varten lukujen tulon täytyy olla $-p/3$. Toisaalta, jos (u_0, v) on jokin (19):n ratkaisu, on $(u_0 v)^3 = (-p/3)^3$, mistä näemme, että jokin tuloista $u_0 v$, $u_0(\zeta v)$, $u_0(\zeta^2 v)$ on $-p/3$; olkoon siis v_0 se luvuista v, ζv, $\zeta^2 v$, jolle $u_0 v_0 = -p/3$. Tällöin $z_1 = u_0 + v_0$ on todella yhtälön (16) ratkaisu.

Lisäksi nähdään, että yhtälöparin (19) muut ratkaisut, joiden tulo on $-p/3$, ovat $(\zeta u_0, \zeta^2 v_0)$ ja $(\zeta^2 u_0, \zeta v_0)$, joista saadaan yhtälön (16) ratkaisut z_2 ja z_3. Osa näistä

ratkaisuista voi tosin olla samojakin, jolloin yhtälölle saadaan kaksin- tai kolminkertainen juuri. □

Esimerkki 6.19. Ratkaistaan yhtälö

$$z^3 + 3z + 4 = 0 \tag{20}$$

ratkaisukaavan avulla. Nyt yhtälö on muotoa (16), missä $p = 3$ ja $q = 4$. Sijoittamalla nämä kaavaan (19) saadaan

$$u = \sqrt[3]{-\frac{4}{2} + \sqrt{\left(\frac{4}{2}\right)^2 + \left(\frac{3}{3}\right)^3}} = \sqrt[3]{-2 + \sqrt{5}} \in \mathbb{R}$$

ja

$$v = \sqrt[3]{-\frac{4}{2} - \sqrt{\left(\frac{4}{2}\right)^2 + \left(\frac{3}{3}\right)^3}} = \sqrt[3]{-2 - \sqrt{5}} = -\sqrt[3]{2 + \sqrt{5}} \in \mathbb{R}.$$

Koska lisäksi $uv = -\sqrt[3]{-2 + \sqrt{5}}\,\sqrt[3]{2 + \sqrt{5}} = -1 = -p/3$, on

$$z_1 = u + v = \sqrt[3]{-2 + \sqrt{5}} - \sqrt[3]{2 + \sqrt{5}}$$

yhtälön (20) eräs ratkaisu. Muita ratkaisuja ovat

$$z_2 = \zeta u + \zeta^2 v \quad \text{ja} \quad z_3 = \zeta^2 u + \zeta v.$$

Huom: Laskemalla voidaan todeta, että $z^3 + 3z + 4 = (z+1)(z^2 - z + 4)$, ja toisaalta $z^2 - z + 4 > 0$ kaikilla $z \in \mathbb{R}$, joten $z = -1$ on yhtälön (20) ainoa *reaalinen* ratkaisu. Koska myös $z_1 = u + v \in \mathbb{R}$, niin täytyy olla

$$\sqrt[3]{-2 + \sqrt{5}} - \sqrt[3]{2 + \sqrt{5}} = -1 \qquad (!)\,.$$

———————

Huomautus* (Reaalijuuret). Kun yhtälön

$$x^3 + px + q = 0 \tag{21}$$

kertoimet p ja q ovat reaalilukuja, olisi tietysti mielenkiintoista tietää, milloin myös ratkaisut ovat reaalisia. Osoittautuu, että reaalijuurten määrä riippuu ratkaisukaavassa neliöjuuren alla olevan luvun

$$D = \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3$$

merkistä.

(a) Jos $D > 0$, voidaan Cardanon kaavoissa (17) valita luvut u_0 ja v_0 kuutiojuurten reaalisiksi arvoiksi; tämä onnistuu, koska nyt kuutiojuurten alla on reaaliluvut, jolloin on myös selvää, että todella $u_0 v_0 = -p/3$. Tällöin $x_1 = u_0 + v_0$ on yhtälön (21) reaalinen ratkaisu.

Koska $\zeta = \frac{-1+i\sqrt{3}}{2}$ ja $\zeta^2 = \frac{-1-i\sqrt{3}}{2}$ (mieti!), ja lisäksi $u_0 \neq v_0$, niin yhtälön kaksi muuta ratkaisua ovat

$$\left.\begin{matrix} x_2 \\ x_3 \end{matrix}\right\} = -\tfrac{1}{2}(u_0 + v_0) \pm i\tfrac{\sqrt{3}}{2}(u_0 - v_0),$$

jotka eivät ole reaalilukuja. Tässä tapauksessa yhtälöllä (21) on siis täsmälleen yksi reaalinen ratkaisu, joka saadaan ”suoraviivaisesti” Cardanon kaavojen avulla (vertaa Esimerkkiin 6.19).

(B) Jos $D = 0$, niin voidaan valita $u_0 = v_0 = \sqrt[3]{-q/2} \in \mathbb{R}$, jolloin yhtälön (21) eräs ratkaisu on $x_1 = -2\sqrt[3]{q/2} \in \mathbb{R}$. Toisaalta $\zeta + \zeta^2 = -1$, mistä nähdään, että yhtälön kaksi muuta ratkaisua yhtyvät kaksinkertaiseksi juureksi $x_2 = x_3 = \sqrt[3]{q/2} \in \mathbb{R}$. Huomaa myös, että tapauksessa $q = 0$ (jolloin ehdon $D = 0$ perusteella myös $p = 0$), on yhtälöllä vain kolminkertainen juuri $x = 0$.

(C) Tapaus $D < 0$ on hieman mutkikkaampi. Huomaa, että nyt täytyy olla $p < 0$. Kirjoittamalla yhtälöt (19) napakoordinaattiesityksen avulla muotoon

$$\begin{aligned} u^3 &= -\tfrac{q}{2} + i\sqrt{-D} = r(\cos\varphi + i\sin\varphi) \\ v^3 &= -\tfrac{q}{2} - i\sqrt{-D} = r(\cos\varphi - i\sin\varphi)\,, \end{aligned} \tag{22}$$

saadaan ehdon $u^3v^3 = (-p/3)^3$ ja Lemman 6.10 nojalla $r = \big(\sqrt{-p/3}\big)^3$ (huom: $r > 0$), ja ehdon $u^3 + v^3 = -q$ avulla edelleen $\cos\varphi = -q/(2r)$; huomaa, että tässä φ täytyy valita siten, että $\sin\varphi > 0$ ja että luvuilla $\cos\varphi$ ja q on eri etumerkkit. Tällöin yhtälöiden (22) ratkaisuiksi saadaan

$$\begin{aligned} u_k &= \sqrt{-p/3}\big(\cos(\varphi/3 + k2\pi/3) + i\sin(\varphi/3 + k2\pi/3)\big) \\ v_l &= \sqrt{-p/3}\big(\cos(\varphi/3 + l2\pi/3) - i\sin(\varphi/3 + l2\pi/3)\big)\,, \end{aligned}$$

missä $k, l \in \{0, 1, 2\}$. Laskemalla voidaan todeta, että näille ratkaisuille pätee $u_kv_l = -p/3$ täsmälleen silloin, kun $k = l$. Näin ollen yhtälölle (21) saadaan ratkaisut

$$\begin{aligned} x_1 &= 2\sqrt{-p/3}\big(\cos(\varphi/3)\big) \\ x_2 &= 2\sqrt{-p/3}\big(\cos(\varphi/3 + 2\pi/3)\big) \\ x_3 &= 2\sqrt{-p/3}\big(\cos(\varphi/3 + 4\pi/3)\big), \end{aligned}$$

jotka ovat erisuuria reaalilukuja. Siispä yhtälöllä (21) on tässä tapauksessa kolme reaalista ratkaisua, vaikka Cardanon kaavoissa (17) esiintyy aidosti kompleksisia lukuja. Itse asiassa voidaan osoittaa, ettei reaalisia ratkaisuja x_1, x_2 ja x_3 voida esittää *algebrallisesti* (eli peruslaskutoimitusten '+', '−', '·' ja '/' sekä juurtenottojen avulla) ilman kompleksilukuja, vaan ratkaisujen reaalisessa esityksessä tarvitaan todella apuna myös trigonometrisia funktioita.

Esimerkki* 6.20. Ratkaistaan yhtälö $x^3 - 6x + 4 = 0$. Nyt

$$D = \left(\frac{4}{2}\right)^2 + \left(\frac{-6}{3}\right)^3 = 4 - 8 < 0,$$

joten olemme tapauksessa (C). Saamme $r = \big(\sqrt{-(-6)/3}\,\big)^3 = 2\sqrt{2}$ ja $\cos\varphi = -q/(2r) = -4/(4\sqrt{2}) = -1/\sqrt{2}$, jolloin voimme valita $\varphi = 3\pi/4$ $(= 135°)$, ja siten $\varphi/3 = \pi/4$ $(= 45°)$. Koska $\sqrt{-p/3} = \sqrt{2}$,

$$\cos(\pi/4 + 2\pi/3) = \cos(11\pi/12) = -(\sqrt{6} + \sqrt{2})/4$$

ja

$$\cos(\pi/4 + 4\pi/3) = \cos(19\pi/12) = (\sqrt{6} - \sqrt{2})/4,$$

niin saamme yhtälölle kolme ratkaisua

$$\begin{aligned} x_1 &= 2\sqrt{2}\big(\cos(\pi/4)\big) = 2\sqrt{2}/\sqrt{2} = 2 \\ x_2 &= 2\sqrt{2}\big(\cos(11\pi/12)\big) = -2\sqrt{2}(\sqrt{6} + \sqrt{2})/4 = -\sqrt{3} - 1 \\ x_3 &= 2\sqrt{2}\big(\cos(19\pi/12)\big) = 2\sqrt{2}(\sqrt{6} - \sqrt{2})/4 = \sqrt{3} - 1. \end{aligned}$$

HUOMAUTUS* (NELJÄNNEN ASTEEN YHTÄLÖ). Kaikki neljännen asteen kompleksikertoimiset yhtälöt voidaan muuttaa yksinkertaisella muuttujanvaihdolla muotoon

$$z^4 + pz^2 + qz + r = 0, \qquad p, q, r \in \mathbb{C}. \tag{23}$$

Tämä yhtälö voidaan ratkaista hyvin samaan tapaan kuin vastaava kolmannen asteen yhtälö (16): Sijoittamalla yhtälöön (23) $z = u + v + w$ nähdään pienten laskujen jälkeen, että yhtälö toteutuu, jos

$$u^2 + v^2 + w^2 = -p/2\ , \qquad uvw = -q/8$$

ja

$$u^2v^2 + u^2w^2 + v^2w^2 = (p^2 - 4r)/16.$$

Mutta tällöin luvut u^2, v^2 ja w^2 ovat kolmannen asteen yhtälön

$$z^3 + \tfrac{p}{2}z^2 + \tfrac{p^2-4r}{16} - \tfrac{q^2}{64} = 0$$

ratkaisut (mieti miksi; voit verrata tätä Lemmaan 6.17), jolloin u^2, v^2 ja w^2 voidaan ratkaista Cardanon kaavojen avulla. Koska lukujen u^2, v^2 ja w^2 neliöjuurten merkit tulee valita siten, että $uvw = -q/8$, nähdään pienen tarkastelun jälkeen, että yhtälölle (23) saadaan neljä mahdollista ratkaisua näiden neliöjuurien summina.

———————

HUOMAUTUS. Kolmannen (ja myös neljännen) asteen yhtälöiden ratkaisukaavalla ei ole mutkikkuutensa vuoksi nykyisin juurikaan käytännöllistä merkitystä, sillä kaikkien polynomiyhtälöiden likimääräiset ratkaisut löytyvät tehokkaamin erilaisten numeeristen algoritmien avulla. Sitä vastoin ratkaisukaavojen löytymisen teoreettiset seuraukset ovat olleet valtaisat.

HUOMAUTUS/HISTORIAA. Nuori norjalaismatemaatikko Niels Henrik Abel (1802–1829) osoitti vuonna 1824, että viidennen ja korkeamman asteen polynomeja *ei ole mahdollista ratkaista* tällaista yleistä ratkaisualgoritmia käyttäen. Italialainen Paolo Ruffini (1765–1822) oli tosin esittänyt saman tuloksen jo 1799, mutta hänen todistuksensa ei ollut täysin aukoton eikä myöskään kovin helposti luettava, joten Ruffini ei saanut ansaitsemaansa huomiota ja tunnustusta ennen Abelin työtä.

Korkeamman asteen yhtälöiden ratkeamattomuus todistetaan nykyisin yleensä käyttämällä ryhmäteoriaa, erityisesti niin sanottua *Galois'n teoriaa*, joka perustuu ranskalaisen Evariste Galois'n (1811–1832) töihin. Näihin asioihin tutustutaan lähemmin Algebran (jatko)kursseilla.

Vaikka korkeamman asteen yhtälöille ei olekaan olemassa yleistä "ratkaisukaavaa", voidaan silti osoittaa, että *jokaisella* kompleksikertoimisella polynomiyhtälöllä on ratkaisu, toisin sanoen, jokaisella joukon $\mathbb{C}$ (ja siten myös joukon $\mathbb{R}$) polynomilla on *kompleksinen* nollakohta. Tämän tuloksen – *Algebran peruslauseen* – todistuksessa on tärkeä tietää, että kaikki polynomit ovat *jatkuvia*:

Määritelmä 6.21. Funktio $f\colon \mathbb{C} \to \mathbb{C}$ (tai $f\colon \mathbb{C} \to \mathbb{R}$) on jatkuva pisteessä $z \in \mathbb{C}$, jos kaikille $\varepsilon > 0$ löytyy $\delta > 0$ siten, että

$$|f(z) - f(w)| < \varepsilon \quad \text{aina kun } |z - w| < \delta.$$

Sanomme, että funktio f on *jatkuva*, jos se on jatkuva jokaisessa pisteessä $z \in \mathbb{C}$.

HUOMAUTUS: Funktio $z \mapsto z$ on selvästi jatkuva. Lisäksi jatkuvien funktioiden summat ja tulot ovat jatkuvia (todistetaan aivan kuten Analyysin kursseilla reaalifunktioille), joten voimme todeta, että kaikki joukon $\mathbb{C}$ polynomifunktiot ovat todella jatkuvia.

Jatkossa tarvitsemme myös tietoa, että funktio $z \mapsto |z|$ on jatkuva (harjoitustehtävä) ja että jatkuvien funktioiden yhdistetyt funktiot ovat jatkuvia, jolloin erityisesti funktio $z \mapsto |P(z)|$ on jatkuva aina, kun P on kompleksikertoiminen polynomi.

Algebran peruslauseen todistuksessa käytetään myös seuraavaa tunnettua tulosta:

Lemma 6.22. *Jos $f\colon \mathbb{C} \to \mathbb{R}$ on jatkuva ja $A \subset \mathbb{C}$ on* kompakti*, eli suljettu ja rajoitettu, niin f saavuttaa joukossa A pienimmän ja suurimman arvonsa: löytyy pisteet $a_m, a_M \in A$ siten, että $f(a_m) \le f(a) \le f(a_M)$ kaikille $a \in A$.*

Lemma 6.22 todistetaan Euklidisten avaruuksien kurssilla; huomaa, että jatkuvuus joukossa $\mathbb{C}$ on sama asia kuin jatkuvuus tasossa $\mathbb{R}^2$, sillä $|x+iy| = \|(x,y)\|$. Vertaa tätä lemmaa myös joukon $\mathbb{R}$ vastaavaan suljettuja ja rajoitettuja välejä koskevaan tulokseen.

Lause 6.23 (ALGEBRAN PERUSLAUSE)**.** *Olkoon P kompleksikertoiminen polynomi (joka ei ole vakio). Tällöin on olemassa $z_0 \in \mathbb{C}$ siten, että $P(z_0) = 0$ eli z_0 on polynomin P nollakohta.*

Todistus. Olkoon siis

$$P(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0,$$

missä $a_0, a_1, \ldots, a_n \in \mathbb{C}$ ja $a_n \neq 0$ ($n \ge 1$). Merkitään $g(z) = |P(z)|$. Kun $z \neq 0$, voimme kirjoittaa

$$g(z) = \big|P(z)\big| = \big|a_n z^n\big|\Big|1 + \frac{a_{n-1}}{a_n z} + \cdots + \frac{a_0}{a_n z^n}\Big|. \tag{24}$$

(A) Osoitamme aluksi, että löytyy $R_0 > 0$ siten, että

$$\Big|1 + \frac{a_{n-1}}{a_n z} + \cdots + \frac{a_0}{a_n z^n}\Big| > \frac{1}{2} \quad \text{kun } |z| > R_0. \tag{25}$$

Huomaamme, että

$$\Big|\frac{a_{n-1}}{a_n z}\Big| = \Big|\frac{a_{n-1}}{a_n}\Big|\frac{1}{|z|} < \frac{1}{2n}, \quad \text{kun } |z| > 2n\Big|\frac{a_{n-1}}{a_n}\Big|;$$

aivan vastaavasti

$$\Big|\frac{a_{n-2}}{a_n z^2}\Big| = \Big|\frac{a_{n-2}}{a_n}\Big|\frac{1}{|z|^2} < \frac{1}{2n}, \quad \text{kun } |z|^2 > 2n\Big|\frac{a_{n-1}}{a_n}\Big|,$$

ja niin edelleen. Lisäksi $|z|^n \ge \cdots \ge |z|^2 \ge |z|$ kunhan $|z| \ge 1$. Niinpä saamme käänteisen kolmioepäyhtälön avulla kaikille $z \in \mathbb{C}$, joille

$$|z| > 2n \cdot \max\Big\{\Big|\frac{a_k}{a_n}\Big| : k \in \{0,1,\ldots,n-1\}\Big\} + 1,$$

että

$$\begin{aligned}\Big|1 + \frac{a_{n-1}}{a_n z} + \cdots + \frac{a_0}{a_n z^n}\Big| &\ge 1 - \Big|\frac{a_{n-1}}{a_n z}\Big| - \Big|\frac{a_{n-2}}{a_n z^2}\Big| - \ldots - \Big|\frac{a_0}{a_n z^n}\Big| \\ &> 1 - \underbrace{\frac{1}{2n} - \frac{1}{2n} - \ldots - \frac{1}{2n}}_{n \text{ kpl}} = \frac{1}{2}.\end{aligned}$$

Siten valitsemalla

$$R_0 = 2n \cdot \max\left\{\left|\frac{a_k}{a_n}\right| : k \in \{0,1,\ldots,n-1\}\right\} + 1$$

on arvio (25) voimassa.

(B) Merkitään nyt $g(0) = |P(0)| = K$. Yhtälön (24) ja vaiheen (A) avulla näemme, että

$$g(z) > |a_n z^n| \cdot \tfrac{1}{2} = |a_n||z|^n \cdot \tfrac{1}{2} > K,$$

kunhan

$$|z| > \max\left\{\sqrt[n]{2K/|a_n|}, R_0\right\};$$

merkitään $R = \max\{\sqrt[n]{2K/|a_n|}, R_0\}$. Koska funktio $g = |P|$ on jatkuva, saavuttaa se pienimmän arvonsa suljetussa pallossa

$$\overline{B}(0,R) = \{z \in \mathbb{C} : |z| \le R\}$$

(Lemma 6.22), joten löytyy $z_0 \in \overline{B}(0,R)$ siten, että

$$g(z) = |P(z)| \ge |P(z_0)| = g(z_0) \quad \text{kaikille } z \in \overline{B}(0,R).$$

Tällöin $g(z_0)$ on itse asiassa funktion g pienin arvo joukossa $\mathbb{C}$, sillä $g(z) > K = g(0) \ge g(z_0)$ jos $z \notin \overline{B}(0,R)$.

(C) Nyt riittää osoittaa, että $g(z_0) = 0$, jolloin myös $P(z_0) = 0$, eli z_0 on haluttu nollakohta.

Tehdään vastaoletus $P(z_0) = c_0 \neq 0$. Laskujen yksinkertaistamiseksi teemme muuttujanvaihdon sijoittamalla $z = w + z_0$ (eli $w = z - z_0$). Tällöin saamme uuden kompleksilukujen polynomin P_1, jolle pätee $P(z) = P(w + z_0) = P_1(w)$, erityisesti siis $P_1(0) = P(z_0) = c_0$. Tällöin voimme kirjoittaa

$$P_1(w) = c_0 + c_1 w + \cdots + c_n w^n = c_0 + c_m w^m + w^{m+1} Q(w), \tag{26}$$

missä m on pienin potenssi, jolle $c_m \neq 0$, ja $Q(w)$ on astetta $n-m-1$ oleva polynomi.

Käsittelemme ensin tapauksen $n = 2$, jolloin siis $P_1(z) = c_0 + c_1 z + c_2 z^2$ (Huomaa, että Lauseen 6.16 perusteella tiedämme, että ratkaisu on todella olemassa, mutta tapaus $n = 2$ käsitelläänkin tässä vain malliksi yleistä tapausta varten.) Jos $c_1 = 0$, niin suoralla sijoituksella nähdään, että $\sqrt{-(c_0/c_2)}$ on polynomin P_1 nollakohta, jolloin $\sqrt{-(c_0/c_2)} + z_0$ on alkuperäisen polynomin P on nollakohta eli väite pätee. Voimme siis olettaa, että $c_1 \neq 0$. Tällöin on mahdollista tutkia polynomin P_1 arvoja pisteissä $-\lambda(c_0/c_1)$, missä $0 < \lambda < 1$; nyt

$$P_1\Big(-\frac{\lambda c_0}{c_1}\Big) = c_0 - c_1\frac{\lambda c_0}{c_1} + c_2\frac{\lambda^2 c_0^2}{c_1^2} = c_0\Big(1 - \lambda + \lambda^2\frac{c_2 c_0}{c_1^2}\Big).$$

Koska $1 - \lambda > 0$ ja toisaalta $\left|\frac{c_2 c_0}{c_1^2}\right|\lambda < 1$ aina, kun $\lambda > 0$ on tarpeeksi pieni (eli kun $0 < \lambda < |c_1^2|/|c_2 c_0|$), niin saamme

$$\Big|P_1\Big(-\frac{\lambda c_0}{c_1}\Big)\Big| \le |c_0|\Big(1 - \lambda + \lambda^2\Big|\frac{c_2 c_0}{c_1^2}\Big|\Big) = |c_0|\Big(1 - \underbrace{\lambda\Big(1 - \lambda\Big|\frac{c_2 c_0}{c_1^2}\Big|\Big)}_{0< \ <1}\Big) < |c_0|$$

kunhan $0 < \lambda < |c_1^2|/|c_2 c_0|$. Tämä johtaa ristiriitaan, sillä $g(z_0) = |c_0|$ oli funktion g pienin arvo joukossa $\mathbb{C}$, ja nyt olisi kuitenkin

$$g(z_0 - \lambda c_0/c_1) = \big|P_1(-\lambda c_0/c_1)\big| < |c_0|,$$

kunhan $\lambda > 0$ on tarpeeksi pieni. Siispä täytyy olla $g(z_0) = |P_1(0)| = 0$, jolloin myös $P(z_0) = 0$.

(D) Yleistämme lopuksi edellisen tarkastelun kaikille $n \geq 3$. Valitaan $z_1 \in \mathbb{C}$ siten, että $z_1^m = -c_0/c_m$ (tällainen löytyy Lauseen 6.14 perusteella), ja olkoon taas $\lambda \in [0,1]$. Nyt lausekkeessa (26) esiintyvä funktio Q on polynomina jatkuva, $c_0 \neq 0$ ja lisäksi joukko $\{\lambda z_1 : \lambda \in [0,1]\}$ on kompakti, joten Lemman 6.22 perusteella löytyy $C > 0$, jolle

$$\left| z_1^{m+1} \frac{Q(\lambda z_1)}{c_0} \right| < C \quad \text{kaikille } \lambda \in [0,1].$$

Siten lauseketta (26), luvun z_1 valintaa ja kolmioepäyhtälöä käyttäen saamme

$$\begin{aligned} \big|P_1(\lambda z_1)\big| &= \big|c_0 + c_m(\lambda z_1)^m + (\lambda z_1)^{m+1} Q(\lambda z_1)\big| \\ &= \big|c_0 - c_m \lambda^m c_0/c_m + c_0 \lambda^{m+1} z_1^{m+1} Q(\lambda z_1)/c_0\big| \\ &\leq |c_0|\big(1 - \lambda^m + \lambda^{m+1}|z_1^{m+1} Q(\lambda z_1)/c_0|\big) < |c_0|\big(1 - \lambda^m(1 - C\lambda)\big)\,; \end{aligned}$$

(huomaa, että $1 - \lambda^m \geq 0$). Mutta tässä $1 - C\lambda > 0$ aina, kun $0 < \lambda < 1/C$. Tällöin $1 - \lambda^m(1 - C\lambda) < 1$, joten saadaan $|P_1(\lambda z_1)| < |c_0|$ aivan kuten kohdan (C) tapauksessa $n = 2$. Tämä johtaa ristiriitaan. Siispä täytyy olla $g(z_0) = 0$, jolloin myös $P(z_0) = 0$ eli haluttu nollakohta on todella olemassa. □

Olkoon nyt P_n jokin n:nnen asteen polynomi. Algebran peruslauseen nojalla polynomilla P_n on nollakohta z_n. Mutta tällöin P_n voidaan tunnetusti jakaa termillä $(z - z_n)$, ja tuloksena on $(n-1)$-asteinen polynomi P_{n-1}, ts. $P_n(z) = (z - z_n)P_{n-1}$ kaikilla $z \in \mathbb{C}$. Mutta nyt myös polynomilla P_{n-1} on kompleksinen nollakohta z_{n-1} (mikäli $n \geq 2$), ja löytyy $(n-2)$-asteinen polynomi P_{n-2} siten, että $P_n(z) = (z - z_n)(z - z_{n-1})P_{n-2}$ kaikilla $z \in \mathbb{C}$. Näin jatkamalla saadaan Algebran peruslauseen vahvennus:

Lause 6.24. *Jokaisella n:nnen asteen kompleksikertoimisella polynomilla on (kertaluvut huomioiden) täsmälleen n kompleksista nollakohtaa.*

HUOMAUTUS: Tässä vaiheessa kannattaa palata tämän luvun alkuun. Lähtökohtanamme oli, että halusimme ratkaista ehkäpä yksinkertaisimman polynomiyhtälön, jolla ei ole ratkaisua reaalilukujen joukossa: $x^2 + 1 = 0$. Laajensimme joukon $\mathbb{R}$ *pienimmäksi mahdolliseksi* lukualueeksi $\mathbb{C}$, jossa on määritelty yhteen- ja kertolasku yhteensopivasti reaalilukujen vastaavien laskutoimitusten kanssa ja joka sisältää alkion $i = \sqrt{-1}$, joka on siis yhtälön $x^2 + 1 = 0$ ratkaisu. Näin saimme aikaan lukualueen, jossa ei ole ainoastaan mahdollista ratkaista yhtälöä $x^2 + 1 = 0$, vaan *kaikki(!)* polynomiyhtälöt, olivatpa niiden kertoimet reaali- tai kompleksilukuja. Tämä on ehkä hieman yllättävää.

———————

HISTORIAA: Kaikki toisen asteen ("reaalikertoimiset") yhtälöt osattiin (periaatteessa) ratkaista jo muinaisessa Babyloniassa ja antiikin Kreikassa, tosin yhtälöt tulkittiin (yleensä) geometrisina ongelmina, jolloin negatiivisia kertoimia tai ratkaisuja ei hyväksytty.

Kolmannen ja neljännen asteen yhtälöiden ratkaisut julkaistiin ensimmäistä kertaa Geronimo Cardanon (1501–1576, Italia) kirjassa *Ars Magna* vuonna 1545, ja vaikka Cardano ei ollutkaan näiden alkuperäinen keksijä, kantavat kolmannen asteen yhtälön ratkaisukaavat edelleen hänen nimeään. Muotoa $x^3 + px = q$ $(p, q \geq 0)$ olevan

kolmannen asteen yhtälön ratkaisi ensimmäisenä ilmeisesti Scipione del Ferro (1465–1526, Italia) 1500-luvun alussa ja myöhemmin Niccolo 'Tartaglia' Fontana (1500–1557, Italia), joka oppi luultavasti ratkaisemaan muitakin (positiivikertoimisia) kolmannen asteen yhtälöitä. Tartaglia kertoi keksinnöstään Cardanolle, joka lupasi pitää ratkaisut salaisuutena, mutta julkaisi ne myöhemmin kirjassaan, mainiten kuitenkin ratkaisujen keksijöiksi del Ferron ja Tartaglian. Neljännen asteen yhtälön ratkaisu, joka siis julkaistiin samassa yhteydessä, on peräisin Cardanon oppilaalta Lodovico Ferrarilta (1522–1565, Italia). Monet pitävät kolmannen ja neljännen asteen yhtälöiden ratkaisemista ensimmäisenä suurena matemaattisena edistysaskeleena antiikin Kreikan matematiikan kukoistuskauden (noin 400 eKr. – 200 jKr.) jälkeen.

Kompleksilukujen "löytyminen" on läheisessä yhteydessä kolmannen asteen yhtälön yleiseen ratkaisuun, sillä ennen Cardanon kaavoja ei ollut mitään pakottavaa tarvetta käsitellä negatiivisten lukujen neliöjuuria; eihän esimerkiksi yhtälön $x^2 + 1 = 0$ ratkeamattomuus ole käytännön tai geometrisen tulkinnan kannalta mikään (suuri) ongelma. Lisäksi vielä 1700-luvullakin monet matemaatikot suhtautuivat epäröiden jopa negatiivisiin lukuihin.

Cardanon kaavojen löytyminen johti kuitenkin merkillisiin ongelmiin. Huomattiin, että vaikka kaavoissa (19) esiintyisi neliöjuuren alla negatiivisia lukuja, saattavat kaavat esittää (oikein tulkittuina) yhtälön reaalisia juuria; vertaa Lauseen 6.18 jälkeisen huomautuksen 'Reaalijuuret' tapaukseen (c). Cardano mainitsee *Ars Magnassa* negatiivisten lukujen neliöjuuret, mutta pitää niitä käyttökelvottomina. Ensimmäinen systemaattinen kompleksilukujen käsittelijä oli Rafael Bombelli joka huomasi negatiivisten lukujen ja niiden neliöjuurten tarpeellisuuden kolmannen asteen yhtälöiden ratkaisuissa. Bombellin teos *L'Algebre* vuodelta 1572 johtikin siihen, että imaginaariluvuille täytyi antaa varovainen hyväksyntä ainakin laskennallisina apuvälineinä.

Kompleksilukujen ja -funktioiden tutkimus kehittyi varsinaiseksi matematiikan osa-alueeksi 1700-luvulla, alkaen Johann Bernoullin (1667–1748, Sveitsi), Roger Cotes'n (1682–1716, Englanti) ja Leonhard Eulerin (1707–1783, Sveitsi) kompleksista logaritmifunktiota koskevista tuloksista. Cotes ja Euler myös käyttivät merkintää $a + b\sqrt{-1}$ kuvaamaan tason pistettä (a, b), mutta he eivät huomanneet, että itse asiassa kompleksiluvut voidaan *määritellä* tason pisteiden avulla. Tämä geometrinen tulkinta, joka teki kompleksilukujen teoriasta huomattavasti helpommin lähestyttävän, on peräisin Jean-Robert Argandilta (1768–1822, Ranska) vuodelta 1806 – tosin norjalais-tanskalainen Caspar Wessel (1745–1818) oli keksinyt saman idean jo 1787 ja julkaisi tätä käsittelevän työn 1799, mutta yleiseen tietoon hänen tuloksensa tulivat vasta 1800-luvun lopulla. Ilmeisesti myös Carl Friedrich Gauss (1777–1855, Saksa) löysi geometrisen tulkinnan jo varhaisessa vaiheessa, mutta se esiintyy hänen julkaisuissaan ensimmäistä kertaa vasta 1832.

Euler uskoi jo 1700-luvun alkupuoliskolla, että jokainen reaalilukukertoiminen polynomi voidaan esittää ensimmäisen ja toisen asteen polynomien tulona, mutta Gaussia pidetään Algebran peruslauseen ensimmäisenä todistajana (reaalikertoimisille polynomeille), vaikka hänen todistuksensa vuodelta 1799 sisältää perustelemattomia geometrisia olettamuksia. Myöhemmin Gauss julkaisikin kolme vaihtoehtoista todistusta tälle lauseelle. Jean Le Rond d'Alembert (1717–1783, Ranska) oli esittänyt Algebran peruslauseelle todistuksen jo 1746, mutta hänen todistuksensa sisälsi useita kohtia, jotka vaativat tarkempaa perustelua. Argand täydensi d'Alembertin todistusta vuonna 1806, kun käytössä oli kompleksilukujen geometrinen tulkinta. Tämä todistus oli myös ensimmäinen, joka oli muotoiltu kompleksikertoimisille polynomeille. Itse asiassa meidän Lauseen 6.23 todistuksemme on hyvin lähellä d'Alembertin ja Argandin

alkuperäisiä ideoita; tärkeänä osana todistusta on tosin Lemman 6.22 ääriarvotulos, jolle Karl Weierstarss antoi tarkan perustelun vasta vuonna 1874, kun reaaliluvut ja jatkuvuus ymmärrettiin nykyisellä täsmällisyydellä.

Puhtaasti algebrallinen määritelmä kompleksiluvuille reaalilukujen pareina, varustettuna Määritelmän 6.1 laskutoimituksilla, on peräisin Sir William Rowan Hamiltonilta (1805–1865, Irlanti) vuodelta 1833. Löydettyään näin tavan kertoa reaalilukulukupareja (a, b) (eli kompleksilukuja $a+ib$) Hamilton halusi yleistää ajatuksen myös lukukolmikoille. Tätä yritystä kesti useiden tuskaisten vuosien ajan. Kerrotaan, että myös hänen lapsensa alkoivat tuntea isänsä turhautumisen ja tiedustelivat häneltä aamuisin: *Well, Papa, can you multiply triplets?* Kaikkien pettymykseksi Hamilton joutui päivästä toiseen vastaamaan, että vain yhteenlasku onnistui. Viimein, vuonna 1843 Hamilton tajusi, että kolmikoiden sijasta kompleksilukujen kertolasku piti yleistää *lukunelikoille* ja että tällöin täytyi lisäksi luopua kertolaskun kommutatiivisuudesta. Näin syntyivät *kvaterniot*.

7. Yleistyksiä ja perusteita*

7.1. **Kvaterniot*.** Merkitään avaruudessa $\mathbb{R}^4$

$$1 = (1,0,0,0)\,, \qquad j = (0,0,1,0)\,,$$
$$i = (0,1,0,0)\,, \qquad k = (0,0,0,1)\,,$$

jolloin voimme kirjoittaa kaikille $x \in \mathbb{R}^4$

$$x = (x_1, x_2, x_3, x_4) = x_1 + ix_2 + jx_3 + kx_4.$$

Sovitaan nyt, että alkioiden $x, y \in \mathbb{R}^4$ summa saadaan laskemalla komponenteittain yhteen, mutta muodostetaan tulo $x \cdot y$ peruskaavojen

$$i^2 = j^2 = k^2 = ijk = -1$$

avulla käyttäen assosiatiivisuutta ja distributiivisuutta. Tällöin saamme uuden lukualueen, *kvaternioiden* joukon $\mathbb{H} = \mathbb{R}^4$, joka on varustettu laskutoimituksilla

$$(x_1, x_2, x_3, x_4) + (y_1, y_2, y_3, y_4) = (x_1 + y_1\,,\ x_2 + y_2\,,\ x_3 + y_3\,,\ x_4 + y_4)$$

ja

$$\begin{aligned}(x_1, x_2, x_3, x_4) \cdot (y_1, y_2, y_3, y_4) = \big(\, & x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4\ , \\ & x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3\ , \\ & x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2\ , \\ & x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1\,\big)\,.\end{aligned}$$

Erityisesti

$$ij = k,\ jk = i \ \text{ ja } \ ki = j\,,$$

mutta

$$ji = -k,\ kj = -i \ \text{ ja } \ ik = -j\,.$$

Tästä näemme, ettei kvaternioiden kertolasku ole kommutatiivinen. Laskutoimituksilla ‘ + ‘ ja ‘ · ‘ on kuitenkin kaikki muut kompleksilukujen laskutoimitusten hyvät ominaisuudet. Jos lisäksi määritellään kvaternion $x = (x_1, x_2, x_3, x_4)$ *moduli* asettamalla

$$|x| = \sqrt{x_1^2 + x_2^2 + x_3^2 + x_4^2}\,,$$

niin kaikille $x, y \in \mathbb{H}$ pätee

$$|x \cdot y| = |x||y|. \tag{27}$$

Nykyisin tiedetään, että avaruuteen $\mathbb{R}^n$ voidaan määritellä kertolasku ‘ $\cdot$ ‘ siten, että yhtälö (27) on voimassa täsmälleen silloin kun $n \in \{1, 2, 4, 8\}$; nämä luvun n arvot vastaavat luonnollisesti reaalilukuja, kompleksilukuja ja kvaternioita sekä *oktonioita*, jotka keksittiin pian kvaternioiden löytymisen jälkeen. Siten Hamiltonin yritys löytää lukukolmikoille luonnollinen kertolasku oli tuomittu epäonnistumaan. Lisäksi Karl Weierstarss osoitti 1863, että $\mathbb{C}$ on joukon $\mathbb{R}$ ainoa *algebrallinen laajennus*, jonka laskutoimitukset ovat kommutatiivisia. Jos kompleksiluvut siis halutaan laajentaa isommaksi lukualueeksi (kuten kvaternioiksi tai oktonioksi), täytyy joistakin laskutoimitusten ominaisuuksista tinkiä: kvaternioiden kertolasku ei ole kommutatiivinen ja oktonioiden kertolasku ei ole kommutatiivinen eikä assosiatiivinen.

Kvaterniot saivat pian keksimisensä jälkeen tärkeitä sovelluksia fysiikasta, mutta 1800-luvun lopulla syntynyt helpommin omaksuttava vektorianalyysi – jonka kehittymiseen kvaternioillakin oli suuri vaikutus – korvasi kvaterniot monilla aloilla. Toisaalta kvaterniot ovat edelleen käyttökelpoisia työkaluja esimerkiksi 3- ja 4-ulotteisen euklidisen geometrian sekä 4- ja 5-ulotteisen hyperbolisen geometrian tutkimuksessa.

7.2. **Algebraa*.** Modernin algebran peruskäsite on abstrakti joukko G, jossa on määritelty laskutoimitus $*\colon G \times G \to G$. Perusesimerkkeinä toimivat usein lukualueet $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ja $\mathbb{C}$, sekä esimerkiksi kaikkien reaali- tai kompleksikertoimisten polynomien joukot, varustettuna laskutoimituksella ‘ $+$ ‘ tai ‘ $\cdot$ ‘.

Määritelmä 7.1. Laskutoimituksella ‘ $*$ ‘ varustettu joukko G, merkitään $(G, *)$, on *ryhmä*, jos

(i) $(a * b) * c = a * (b * c)$ kaikilla $a, b, c \in G$;
(ii) on $e \in G$ siten, että $a * e = e * a = a$ kaikilla $a \in G$;
(iii) kaikille $a \in G$ löytyy $a' \in G$ siten, että $a * a' = a' * a = e$.

Toisin sanoen, $(G, *)$ on ryhmä, jos ‘ $*$ ‘ on joukon G assosiatiivinen laskutoimitus, jolla on neutraalialkio $e \in G$ ja lisäksi kaikille $a \in G$ löytyy käänteisalkio.

Jos ‘ $*$ ‘ on lisäksi kommutatiivinen eli $a * b = b * a$ kaikilla $a, b \in G$, niin sanotaan, että $(G, *)$ on *Abelin ryhmä*.

Esimerkki 7.2. (a) Lukualueemme $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ja $\mathbb{C}$ ovat (Abelin) ryhmiä, kun laskutoimituksena on ‘ $+$ ‘.

(b) Joukot $\mathbb{Q}^*$, $\mathbb{R}^*$ ja $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ ovat (Abelin) ryhmiä, kun laskutoimituksena on ‘ $\cdot$ ‘.

Lukualueissamme on itse asiassa määritelty kaksi (yhteensopivaa) laskutoimitusta. Kokonaislukujen ja rationaalilukujen ominaisuuksia matkien saamme seuraavat määritelmät:

Määritelmä 7.3. (1) Laskutoimituksilla ‘ $+$ ‘ ja ‘ $\cdot$ ‘ varustettu joukko R, merkitään $(R, +, \cdot)$, on *(ykkösellinen) rengas*, jos

(i) $(R, +)$ on Abelin ryhmä;
(ii) $(ab)c = a(bc)$ kaikilla $a, b, c \in R$;
(iii) on $1 \in R$ siten, että $a \cdot 1 = 1 \cdot a = a$ kaikilla $a \in R$;
(iv) $(a + b)c = ac + bc$ ja $c(a + b) = ca + cb$ kaikilla $a, b, c \in R$.

Toisin sanoen, $(R, +, \cdot)$ on rengas, jos ‘ $\cdot$ ‘ on Abelin ryhmän $(R, +)$ assosiatiivinen laskutoimitus, jolla on neutraalialkio $1 \in R$ ja lisäksi ‘ $\cdot$ ‘ on distributiivinen laskutoimituksen ‘ $+$ ‘ suhteen. Laskutoimituksen ‘ $+$ ‘ neutraalialkiota on tapana merkitä symbolilla 0.

(2) Joukko $(K, +, \cdot)$ on *kunta*, jos

(i) $(K, +, \cdot)$ on (ykkösellinen) rengas;
(ii) ‘$\cdot$‘ on kommutatiivinen;
(iii) kaikille $a \in K \setminus \{0\}$ löytyy $a' \in K$ siten, että $aa' = a'a = 1$.

Esimerkki 7.4. (a) Lukualueet $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ja $\mathbb{C}$ ovat renkaita, kun laskutoimituksina ovat ‘$+$‘ ja ‘$\cdot$‘.

(b) Lukualueet $\mathbb{Q}$, $\mathbb{R}$ ja $\mathbb{C}$ ovat kuntia, kun laskutoimituksina ovat ‘$+$‘ ja ‘$\cdot$‘.

Ryhmien, renkaiden ja kuntien käyttökelpoisuus on siinä, että lukualueidemme lisäksi on olemassa valtava määrä joukkoja, joissa kyseiset ominaisuudet toteutuvat. Koska esimerkiksi ryhmän ominaisuuksista (i)–(iii) lähtien on mahdollista todistaa paljon muita hyödyllisiä asioita, ei näitä tarvitse tehdä kaikille mahdollisille joukoille erikseen, vaan riittää todeta, että (i)–(iii) ovat voimassa kyseisessä tapauksessa, jolloin koko ryhmiin liittyvä algebrallinen koneisto saadaan käyttöön. Näihin asioihin tutustutaan lähemmin algebran kursseilla, mutta todistetaan tässä esimerkin vuoksi yksi ryhmiin liittyvä tulos, joka on ollut esillä lukualueissammekin:

Lemma 7.5. *Olkoon $(G, *)$ ryhmä ja olkoot $a, b, c \in G$. Jos $a * c = b * c$, niin $a = b$.*

Todistus. Koska G on ryhmä, niin laskutoimitukselle ‘$*$‘ löytyy neutraalialkio $e \in G$ ja lisäksi alkiolla c on käänteisalkio $c' \in G$. Tällöin assosiatiivisuutta ja oletusta $a * c = b * c$ käyttäen saadaan

$$a = a * e = a * (c * c') = (a * c) * c' = (b * c) * c' = b * (c * c') = b * e = b.$$

Siispä $a = b$. □

Annetaan vielä lopuksi esimerkki ryhmästä, joka ei ole mikään lukualueistamme:

Esimerkki 7.6. Olkoon

$$S^1 = \{z \in \mathbb{C} : |z| = 1\}.$$

Tällöin S^1 varustettuna kompleksilukujen kertolaskulla on ryhmä:

Aluksi pitää siis todeta, että ‘$\cdot$‘ on todella joukon S^1 laskutoimitus. Tämä seuraa nyt siitä, että ‘$\cdot$‘ on joukon $\mathbb{C}$ laskutoimitus ja lisäksi kaikille $z, w \in S^1$ pätee $|zw| = |z||w| = 1$ eli myös $zw \in S^1$. Lisäksi

(i) ‘$\cdot$‘ on assosiatiivinen joukossa S^1 (koska on sitä myös joukossa $\mathbb{C}$);
(ii) $1 \in S^1$ ja $z \cdot 1 = 1 \cdot z = z$ kaikilla $z \in S^1$;
(iii) kaikille $z \in S^1$ pätee $z^{-1} \in S^1$, sillä

$$|z^{-1}| = \Big|\frac{\overline{z}}{|z|^2}\Big| = \frac{|\overline{z}|}{|z|^2} = \frac{|z|}{|z|^2} = \frac{1}{|z|} = 1.$$

Historiaa: Abstrakti ryhmäkäsite kehittyi 1800-luvun kuluessa, alkaen *permutaatioryhmien* tutkimuksesta, joka liittyi läheisesti Ruffinin ja Galois'n polynomiyhtälöiden ratkeavuutta koskeviin tutkimuksiin. Määritelmän 7.1 kaltainen abstrakti ryhmä esiintyy ensimmäistä kertaa Walter van Dyckin (1856–1934, Saksa) ja Heinrich Weberin vuonna 1882 (toisistaan riippumatta) julkaistuissa töissä.

7.3. **Reaalilukujen aksioomat*.** Analyysin kursseilla yleinen lähestymistapa on olettaa koko $\mathbb{R}$ ”intuitiivisesti tunnetuksi”. Tarkemmin sanottuna tällöin oletetaan, että on olemassa joukko $\mathbb{R}$ siten, että sen alkiot toteuttavat tietyt *perusaksioomat*, esimerkiksi:

On olemassa laskutoimitukset

$$+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R},\ (x, y) \mapsto x + y$$

ja

$$\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R},\ (x, y) \mapsto xy$$

siten, että

(R1) ‘ $+$ ‘ on kommutatiivinen
(R2) ‘ $+$ ‘ on assosiatiivinen
(R3) laskutoimituksella ‘ $+$ ‘ on neutraalialkio $0 \in \mathbb{R}$
(R4) jokaisella $x \in \mathbb{R}$ on vastaluku $-x \in \mathbb{R}$: $x + (-x) = 0$
(R5) ‘ $\cdot$ ‘ on kommutatiivinen
(R6) ‘ $\cdot$ ‘ on assosiatiivinen
(R7) laskutoimituksella ‘ $\cdot$ ‘ on neutraalialkio $1 \in \mathbb{R}$ ja lisäksi $1 \neq 0$
(R8) jokaisella $x \in \mathbb{R} \setminus \{0\}$ on käänteisluku $x^{-1} \in \mathbb{R}$: $x \cdot x^{-1} = 1$
(R9) ‘ $\cdot$ ‘ on distributiivinen laskutoimituksen ‘ $+$ ‘ suhteen.

Joukossa $\mathbb{R}$ on olemassa myös relaatio ‘ $<$ ‘, jolle pätee:

(R10) Kun $x, y \in \mathbb{R}$ niin täsmälleen yksi ehdoista $x = y$, $x < y$ ja $y < x$ on voimassa
(R11) ‘ $<$ ‘ on transitiivinen
(R12) jos $x < y$ ja $z \in \mathbb{R}$, niin $x + z < y + z$
(R13) jos $0 < x$ ja $0 < y$, niin $0 < xy$.

Lisäksi joukko $\mathbb{R}$ oletetaan täydelliseksi eli

(R14) jokaisella ylhäältä rajoitetulla epätyhjällä joukolla $S \subset \mathbb{R}$ on pienin yläraja.

Näiden ominaisuuksien varaan voidaan rakentaa koko (reaali)analyysin tarvitsema koneisto. Olemme kuitenkin tällä kurssilla oppineet, miten aksioomat (R1)–(R14) toteuttava joukko $\mathbb{R}$ voidaan *konstruoida*, jos oletetaan tunnetuksi ainoastaan luonnollisten lukujen joukon $\mathbb{N}$ ominaisuudet. Nämä on (ehkä/toivottavasti) helpompi hyväksyä, kuin vain olettaa (R1)–(R14) ilman perusteluja.

Historiaa: On ehkä hieman yllättävää, että ensimmäinen reaalilukujen aksioomajärjestelmä esiintyi itse asiassa David Hilbertin (1862–1943, Saksa) kirjassa *Grundlagen der Geometrie*(!) vuonna 1899.

7.4. **Luonnolliset luvut*.** Mitä sitten ovat ne luonnolliset luvut, joiden varaan kaikki muut lukualueet on rakennettu? Intuitiivinen käsityksemme luonnollisista luvuista on toki riittävä pohja kaikkiin ”käytännön” tarpeisiin, mutta matemaattisen täsmällisyyden vaatimuksiin se ei riitä. Siksi määrittelemmekin seuraavassa joukon $\mathbb{N}$ aksiomaattisesti joukko-oppiin nojaten.

Oletamme, että on olemassa joukko $\mathbb{N}$ ja funktio s: $\mathbb{N} \to \mathbb{N}$, niin sanottu *seuraajafunktio*, siten, että seuraavat aksioomat ovat voimassa:

(N1) s ei ole surjektio: löytyy alkio $0 \in \mathbb{N}$, jolle $0 \neq s(n)$ kaikilla $n \in \mathbb{N}$
(N2) s on injektio: jos $s(n) = s(m)$, niin $n = m$.

(N3) $\mathbb{N}$ on *induktiivinen joukko*: Jos $S \subset \mathbb{N}$ on sellainen, että $0 \in S$ ja lisäksi ehdosta $n \in S$ seuraa, että myös $s(n) \in S$, niin tällöin $S = \mathbb{N}$.

Osoittautuu, että tässä on kaikki, mitä tarvitaan luonnollisten lukujen tunnettujen ominaisuuksien (ja siten kaikkien kurssimme tulosten) todistamiseksi.

Aksiooma (N1) antaa meille yhden erityisasemassa olevan luonnollisen luvun 0. Tämän jälkeen voimme nimetä muita luonnollisia lukuja, esimerkiksi $s(0) = 1$, $s(1) = 2$, $s(2) = 3$ ja niin edelleen.

Luonnollisten lukujen laskutoimitukset voidaan määritellä aksioomaan (N3) perustuen "induktiivisesti" (tai oikeammin *rekursiivisesti*):

Yhteenlasku: Kaikille $m \in \mathbb{N}$ asetetaan

(i) $m + 0 = m$
(ii) $m + s(n) = s(m + n)$.

Tällöin erityisesti $m + 1 = m + (s(0)) = s(m + 0) = s(m)$, joten luvun 1 lisääminen johtaa samaan lopputulokseen kuin seuraajafunktio. Näin ollen, jos lukuun m lisätään n, tämä tarkoittaa "siirtymistä seuraajafunktion avulla n askelta eteenpäin luvusta m alkaen".

Kertolasku: Kaikille $m \in \mathbb{N}$ asetetaan

(i) $m \cdot 0 = 0$
(ii) $m \cdot s(n) = m \cdot n + m$.

Näiden määrittelyjen jälkeen voimmekin palata takaisin aivan kurssin alkuun ja *todistaa* seuraavat luonnollisten lukujen laskutoimitusten perusominaisuudet yllä olevia määritelmiä ja aksioomia (N1)–(N3) käyttäen:

Lause 7.7. (a) *Luonnollisten lukujen yhteen- ja kertolaskut ovat assosiatiivisia:*

$$a + (b + c) = (a + b) + c$$
$$a(bc) = (ab)c$$

kaikilla $a, b, c \in \mathbb{N}$*;*

(b) *Luonnollisten lukujen yhteen- ja kertolaskut ovat kommutatiivisia:*

$$a + b = b + a$$
$$ab = ba$$

kaikilla $a, b \in \mathbb{N}$*;*

(c) *Luonnollisten lukujen kertolasku on distributiivinen yhteenlaskun suhteen:*

$$(a + b)c = ac + bc$$

kaikilla $a, b, c \in \mathbb{N}$

(d) *Luku* $0 \in \mathbb{N}$ *on luonnollisten lukujen yhteenlaskun neutraalialkio:*

$$n + 0 = 0 + n = n \qquad \textit{kaikilla } n \in \mathbb{N}.$$

ja luku $1 = s(0) \in \mathbb{N}$ *on kertolaskun neutraalialkio:*

$$n \cdot 1 = 1 \cdot n = n \qquad \textit{kaikilla } n \in \mathbb{N}.$$

Todistus. Todistukset ovat lyhyitä ja suoraviivaisia induktiotodistuksia, mutta melko oleellista on se, missä järjestyksessä ne tehdään. Yhteenlaskun assosiatiivisuus ei

vaadi muita kohtia. Seuraavaksi kannattaa varmaan todistaa neutraalialkioihin liittyvä kohta (d), jota voi sitten hyödyntää muissa kohdissa, erityisesti yhteenlaskun kommutatiivisuudessa. Samoin distributiivisuus kannattaa todistaa ennen kertolaskun assosiatiivisuutta ja kommutatiivisuutta. Yksityiskohdat jätetään lukijalle (apua löytyy esimerkiksi kirjasta Stewart ja Tall) ja/tai lukuteorian kursseille. □

Mainitaan vielä seuraava lemma, jonka avulla todistettiin kokonaislukujen perusominaisuuksia:

Lemma 7.8. *Olkoot* $n, m, k \in \mathbb{N}$.
(a) *Jos* $n + k = m + k$, *niin* $n = m$.
(b) *Jos* $nk = mk$ *ja* $k \neq 0$, *niin* $n = m$

Todistus. Induktio. □

Nyt voimme määritellä joukkoon $\mathbb{N}$ järjestyksen ' $\leq$ ' asettamalla

$$m \leq n \iff m + k = n \text{ jollekin } k \in \mathbb{N}.$$

Lause 7.9. *Luonnollisten lukujen järjestys* ' $\leq$ ' *on*

- *refleksiivinen:* $n \leq n$ *kaikille* $n \in \mathbb{N}$;
- *antisymmetrinen: Jos* $n \leq m$ *ja* $m \leq n$, *niin* $m = n$;
- *transitiivinen: Jos* $n \leq m$ *ja* $m \leq p$, *niin* $n \leq p$.

Lisäksi kaikille $n, m \in \mathbb{N}$ *joko* $n \leq m$ *tai* $m \leq n$. *Toisin sanoen,* ' $\leq$ ' *on täydellinen järjestys.*

Todistus. Refleksiivisyys on selvä, antisymmetrisyys ja transitiivisuus saadaan pienten laskujen avulla ja viimeinen ehto seuraa suoraviivaisella induktiolla. □

Historiaa: Luonnollisten lukujen aksioomat (N1)–(N3) esiintyivät ensimmäisen kerran Giuseppe Peanon (1858–1932, Italia) vuonna 1889 julkaistussa teoksessa *Arithmetices principia, nova methodo exposita.*

Kirjallisuutta

Lukualueita ja algebraa:

H.-D. Ebbinghaus *et al.*: *Numbers*, Springer-Verlag, 1990.

S. Lang: *Undergraduate algebra*, Springer-Verlag, 1987.

T. Metsänkylä ja M. Näätänen: *Algebra*, Jyväskylän yliopistopaino, 1999.

I. Stewart ja D. Tall: *The foundations of mathematics*, Oxford University Press, 1977.

K. Väisälä: *Lukuteorian ja korkeamman algebran alkeet*, Otava, 1961.

Historiaa:

C. Boyer: *Tieteiden kuningatar I ja II*, Art House, 2000.

J. Stillwell: *Mathematics and its history*, Springer-Verlag, 1989.

B. L. van der Waerden: *A history of algebra*, Springer-Verlag, 1985.

The MacTutor History of Mathematics archive:
http://www-history.mcs.st-and.ac.uk/∼history/index.html