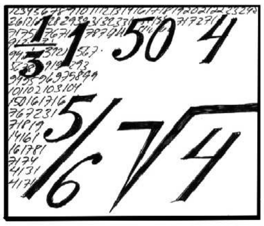


Onko $\sqrt{-1}$ olemassa? Keskipituinen kertomus lukujen olemuksesta, 2. osa

Antti Valmari
Ohjelmistotekniikan laitos
Tampereen teknillinen yliopisto

Tiivistelmä

Tämän kirjoituksen tavoitteena on kertoa lukujen olemuksesta ja matemaattisen määrittelemisen luonteesta tavallista helppotajuisemmin. Kirjoituksessa pohditaan muun muassa, miksi $\frac{1}{0}$ ei ole luku, mutta $\sqrt{-1}$ on. Myös selviää, miksi uusien lukujen keksiminen on loppunut kompleksilukuihin.

Nollan käänteisarvo

Nyt kun vähennyslasku on määritelty siten, että jokainen vähennyslasku on laskettavissa, on luonnollista yrittää tehdä sama jakolaskulle. Tunnetusti ykkönen on kertolaskun suhteen samankaltaisessa roolissa kuin nolla yhteenlaskun. Olemme jo muotoilleet tämän lakina (8): ”On olemassa luku 1 siten, että jokaisella luvulla a pätee $a \cdot 1 = a$”. Lakia täytyy kuitenkin täydentää ehkä yllättävällä vaatimuksella:

(11) $1 \neq 0$

Tämä on todellakin tarpeen vaatia! Nimittäin järjestelmä, jossa on vain yksi olento 0 toteuttaa kaikki lait (1), …, (10) ja jatkossa annettavat lait (12), …, (17). Siinä kaikki laskutoimitukset tuottavat saman tuloksen 0.

Seuraava yhteenlaskua matkiva askel olisi julistaa, että jokaista lukua a kohti on olemassa luku $\frac{1}{a}$ siten, että $a \cdot \frac{1}{a} = 1$. Kuten hyvin tiedetään, matemaatikot ovat kuitenkin rajanneet nollan pois tästä säännöstä:

(12) Jos $a \neq 0$, niin on olemassa luku $\frac{1}{a}$ siten, että $a \cdot \frac{1}{a} = 1$.

Miksi $\frac{1}{0}$ eli nollan käänteisarvo on jätetty pois? Olemme oppineet, että matemaatikko saa määritellä uusia olentoja ihan niinkuin haluaa, eikä ole tarpeen miettiä, ovatko ne ”oikeasti” olemassa. Eikö nollan käänteisarvo voitaisi ottaa mukaan ihan vain julistamalla, että sekin on olemassa? Päästäisiin eroon siitä riesasta, että nollalla ei saa jakaa!

Nollan käänteisarvo voidaan ottaa käyttöön, jos halutaan. Valitettavasti seuraukset ovat ikäviä. Nollan käänteisarvo on olento $\frac{1}{0}$ siten, että $0 \cdot \frac{1}{0} = 1$. Käyttämällä tätä lakia, kertolaskun liitännäisyyttä sekä kokonaislukujen ominaisuuksia $2 \cdot 0 = 0$ ja $2 \cdot 1 = 2$ saadaan $1 = 0 \cdot \frac{1}{0} = (2 \cdot 0) \cdot \frac{1}{0} = 2 \cdot (0 \cdot \frac{1}{0}) = 2 \cdot 1 = 2$. Tätä ei voida hyväksyä, koska se muuttaisi tavallisten lukujen ominaisuuksia. Kakkonen ei ole ykkönen! Koska tavallisten lukujen lakeja ei saa muuttaa, niin ei ole muuta keinoa saada $0 \cdot \frac{1}{0} = 1$ voimaan kuin luopua kertolaskun liitännäisyydestä silloin, kun laskussa on mukana $\frac{1}{0}$. Tässä tapauksessa siis $(2 \cdot 0) \cdot \frac{1}{0} \neq 2 \cdot (0 \cdot \frac{1}{0})$.

Tämä harmillinen tulos voidaan esittää myös jakolaskun lakien rikkoutumisena $\frac{2 \cdot 0}{0} \neq 2 \cdot \frac{0}{0}$. Säännöstä ”nollalla ei saa jakaa” päästiin eroon, mutta nollalla jakamiseen pitää soveltaa eri lakeja kuin muihin jakolaskuihin. Siis nollalla jako pitää silti käsitellä erikoistapauksena. Tavoiteltu hyöty jäi saamatta.

Eivätkä ongelmat lopu tähän. Olkoon x mikä tahansa luku. Lakien (9), (2) ja (7) nojalla saadaan $x \cdot 1 = x \cdot (1 + 0) = x \cdot (0 + 1) = x \cdot 0 + x \cdot 1$. Lisäämällä molemmille puolille $-(x \cdot 1)$ ja soveltamalla lakeja (10), (3), (10), (9) ja (5) saadaan $0 = x \cdot 1 + (-(x \cdot 1)) = (x \cdot 0 + x \cdot 1) + (-(x \cdot 1)) = x \cdot 0 + (x \cdot 1 + (-(x \cdot 1))) = x \cdot 0 + 0 = x \cdot 0 = 0 \cdot x$. Siis $0 \cdot x = 0$. Tämäkin on ristiriidassa tavoitteen $0 \cdot \frac{1}{0} = 1$ kanssa. Tässä laskussa ei käytetty kertolaskun liitännäisyyttä, joten jokin toinenkin laki on uhrattava, jotta $0 \cdot \frac{1}{0} = 1$ saadaan voimaan.

Nollan käänteisarvo $\frac{1}{0}$ ei siis ole samanlainen hyödyllinen kiltti apulainen kuin negatiiviset luvut, vaan pahantapainen olento, joka rikkoo ainakin kahta rationaalilukujen noudattamaa lakia eikä tuo sitä hyötyä, jota varten se kutsuttiin mukaan. On parempi potkaista se ulos. Niin matemaatikot ovat tehneet. Jos jossakin on sovelluksia, joissa nollan käänteisarvon ominaisuudet ovat enemmän hyödyksi kuin haitaksi, niin siellä sen voi ja kannattaa ottaa käyttöön. Se käyttäytyy kuitenkin niin eri tavalla kuin tavalliset luvut, että silloinkin on parempi olla kutsumatta sitä luvuksi.

Esimerkiksi raja-arvojen yhteydessä käytetään usein olentoja ∞ ja $-\infty$, jotka voitaisiin ajatella nollan käänteisarvoksi ja sen vastaluvuksi. Jos niille määritellään yhteenlasku, niin se tehdään yleensä niin, että jos a on reaaliluku, niin $a + \infty = \infty + a = \infty$ ja $a + (-\infty) = (-\infty) + a = -\infty$. Mutta tällöin $(1 + \infty) + (-\infty) = \infty + (-\infty) = 0$ ja $1 + (\infty + (-\infty)) = 1 + 0 = 1$, joten liitännäisyyslaki ei päde. Liitännäisyyslaki on niin tärkeä laki, että matemaatikot luopuvat mieluummin laista (1) kuin siitä. Ei siis yleensä määritellä, että $-\infty$ on ∞:n vastaluku, vaan että $\infty + (-\infty)$ ei ole määritelty.

Edellä on puhuttu nollan käänteisarvosta ikäänkuin se olisi yksikäsitteinen, ennalta määrätty olento. Sen tarkka luonne määräytyy kuitenkin vasta sitten, kun on annettu niin paljon sääntöjä, että sen käyttäytyminen kaikissa tilanteissa on määräytynyt. $f$skeisessä esimerkissä $\infty + 1 = \infty$, mutta jossain toisessa sovelluksessa voi olla parempi valita $\frac{1}{0} + 1 \neq \frac{1}{0}$. Nollalla voi siis olla erilaisia käänteisarvoja eri tarkoituksia varten. Niille kaikille on kuitenkin yhteistä, että ne rikkovat kertolaskun liitännäisyyttä ja ainakin yhtä muuta rationaalilukujen lakia. Tämä johtuu siitä, että ainoa edellä olevissa laskelmissa käytetty nollan käänteisarvon ominaisuus on, että $0 \cdot \frac{1}{0} = 1$.

Millä oikeudella sitten vaadittiin, että nollan käänteisarvon on noudatettava lakia $0 \cdot \frac{1}{0} = 1$? Eikö sen tilalle voi valita jonkin muun lain? Kyllä voi, mutta niin määriteltyä olentoa ei ole mitään järkeä kutsua ”nollan käänteisarvoksi”. Matematiikassa ”a:n käänteisarvolla” on johdonmukaisesti tarkoitettu sellaista olentoa $\frac{1}{a}$, että $a \cdot \frac{1}{a} = 1$. (Tapana on myös vaatia $\frac{1}{a} \cdot a = 1$, mutta sitä ei tarvitse sanoa erikseen silloin, kun kertolasku on vaihdannainen.) Määritellä saa mitä tahansa. Määritellyn olennon nimi pitää kuitenkin valita siten, että se ei ole ristiriidassa aikaisempien nimivalintojen kanssa.

Mitä luvut ovat?

Totesimme, että nollan käänteisarvon voi määritellä monellakin tavalla, mutta se käyttäytyy joka tapauksessa niin eri tavalla kuin oikeat luvut, että sitä ei pidä kutsua luvuksi. Mikä sitten kelpaa luvuksi?

Matematiikassa on tarkasti määritelty merkitys käsitteille ”luonnollinen luku”, ”kokonaisluku”, ”rationaaliluku”, ”reaaliluku” ja niin edelleen, mutta ei käsitteelle ”luku”. Tästä seuraa, että matemaatikko voi ottaa käyttöön uudenlaisia olentoja ja alkaa kutsua niitä luvuiksi. Tästä ei kuitenkaan seuraa, että mitä tahansa kutsutaan luvuiksi. Uusien olentojen pitää muistuttaa tuttuja lukuja tarpeeksi paljon ja olla niihin tarpeeksi läheisessä suhteessa, jotta matemaatikot kelpuuttavat ne luvuiksi. Vaikka ei ole määritelty, miten paljon on tarpeeksi paljon, matemaatikot ovat tähän asti aina päässeet asiasta yhteisymmärrykseen.

Lukua ei tee luvuksi sen ”omat” ominaisuudet, vaan jäsenyys järjestelmässä, jonka kaikki olennot yhdessä noudattavat jotakin kokoelmaa lakeja. Luvun -2 ominaisuus $2 + (-2) = 0$ puhuu paitsi -2:sta, myös luvuista 2 ja 0 sekä yhteenlaskusta. Laki ”on olemassa $-a$” tarkoittaa itse asiassa, että ”$-a$” on mukana puheena olevassa järjestelmässä. Peruskysymys ei siis ole, onko jokin olento luku, vaan onko jokin olentojen järjestelmä lukujoukko. (Tapana on sanoa ”lukujoukko”, vaikka ”lukujärjestelmä” olisi parempi sana, sillä mukaan kuuluvat lukujen lisäksi ainakin yhteenlasku ja kertolasku.) Esimerkiksi ilmauksilla ”luonnolliset luvut” ja ”rationaaliluvut” viitataan tällaisiin järjestelmiin. Luvuilla täytyy voida laskea, tai muuten niitä ei sanota luvuiksi!

Kaikki tutut lukujärjestelmät noudattavat ainakin lakeja (1), ..., (8). Näitä lakeja käytetään laskuissa niin rutiininomaisesti, että jos yksikin niistä menetettäisiin, laskemisen luonne muuttuisi ihan toisenlaiseksi. Esimerkiksi vektoreilla ja matriiseilla on osittain toiset lait. Välillä on hankala muistaa, miten niillä saa ja ei saa laskea. Mutta niitäpä ei kutsutakaan luvuiksi. Kuten edellä nähtiin, nollan käänteisarvoa ei voida ottaa käyttöön menettämättä ainakin kahta laeista (1), ..., (8).

Edellä totesimme, että lait (1), ..., (8) riittävät määräämään, että luvut 1, 2, 3, ... käyttäytyvät yhteen- ja kertolaskuissa kuten luonnolliset luvut, *jos kaikki nämä luvut ovat erisuuria*. Vaikka lakien (8) ja (1) ansiosta luvut 1, $1+1$, $(1+1)+1$, ... ovat kaikki varmasti olemassa, tähänastiset lait eivät riitä takaamaan, että ne ovat erisuuria. Laskemalla muuten normaalisti, mutta asettamalla $5 = 0$ (mistä seuraa $6 = 1$, $7 = 2$ ja niin edelleen) saadaan järjestelmä, jossa on viisi olentoa, joiden laskutoimitukset käyttäytyvät seuraavasti (olemme panneet olentojen päälle pienen viivan muistutukseksi, että ne eivät ole tuttuja lukuja):

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Tämä järjestelmä noudattaa kaikkia lakeja (1), ..., (12). Lakien (1), (2), (4), (5), (8), (9), (10) ja (12) voimassaolo on hyvin helppo tarkastaa näistä taulukoista. Koska järjestelmän olennot ovat erit, on laki (11) voimassa. Lakien (3), (6) ja (7) tarkastaminen vaatii enemmän työtä, mutta kyllä nekin pätevät.

Tämän viisialkioisen ja muiden samantapaisten järjestelmien alkioita ei ole tapana kutsua luvuiksi. Matemaatikon sana mille tahansa järjestelmälle, joka noudattaa lakeja (1), ..., (12) on *kunta*. Rationaalilukujen järjestelmä, reaalilukujen järjestelmä ja tämä viisialkioinen järjestelmä ovat kuntia. Kokonaislukujen järjestelmä ei ole kunta, koska laki (12) ei päde, eli kaikilla nollasta poikkeavilla alkioilla ei ole käänteisalkioita.

Jos jokin lukujen järjestelmä halutaan määritellä yksikäsitteisesti, niin tarvitaan lisää lakeja, joilla suljetaan väärät kunnat pois. Reaalilukujen tapauksessa tämä tehdään kahdessa vaiheessa. Ensin vaaditaan, että reaaliluvut voidaan asettaa suuruusjärjestykseen, joka käyttäytyy laskutoimitusten suhteen tutulla tavalla. Jokaiselle reaaliluvulle a, b ja c pätee:

(13) Tasan yksi seuraavista pätee: $a < b$, $a = b$ tai $b < a$.

(14) Jos $a < b$ ja $b < c$, niin $a < c$.

(15) Jos $a < b$, niin $a + c < b + c$.

(16) Jos $0 < a$ ja $0 < b$, niin $0 < ab$.

Tällä vaatimuksella saadaan aikaan, että 1, $1+1$, $(1+1)+1$, ... todellakin ovat kaikki eri lukuja. Nimittäin, lakien (9) ja (8) ansiosta 0 ja 1 ovat olemassa, ja laki (11) sanoo, että $1 \neq 0$. Lain (13) nojalla joko $0 < 1$ tai $1 < 0$. Jos $0 < 1$, niin lakien (10), (2) ja (15) nojalla $1 = 1 + 0 = 0 + 1 < 1 + 1$ eli $1 < 1 + 1$. Lisäämällä ykkönen kummallekin puolelle ja soveltamalla lakia (15) uudelleen saadaan $1+1 < (1+1)+1$. Tätä toistamalla saadaan $1 < 1+1 < (1+1)+1 < ((1+1)+1)+1 < \ldots$. Jos olisikin $1 < 0$, niin samanlaisella päättelyllä saataisiin $\ldots < ((1 + 1) + 1) + 1 < (1 + 1) + 1 < 1 + 1 < 1$.

Nyt tarvitsee vielä osoittaa, että jos $a_1 < a_2 < a_3 < \ldots$ tai $\ldots < a_3 < a_2 < a_1$, niin luvut a_i ovat kaikki keskenään erisuuria. Ensimmäisessä tapauksessa soveltamalla lakia (14) toistuvasti saadaan $a_1 < a_3$, $a_1 < a_4$ ja niin edelleen. Vanhastaan tiedettiin, että $a_1 < a_2$. Lain (13) nojalla näistä seuraa, että $a_1 \neq a_2$, $a_1 \neq a_3$, $a_1 \neq a_4$ ja niin edelleen. Samalla tavalla voidaan osoittaa, että $a_2 \neq a_3$, $a_2 \neq a_4$, $a_2 \neq a_5$ ja niin edelleen, ja yleensä, että $a_i \neq a_j$ kun $i < j$. Samanlainen päättely toimii myös jälkimmäisessä tapauksessa.

Tämän tuloksen ansiosta lakeja (1), ..., (9), (11), (13), (14) ja (15) noudattava järjestelmä sisältää väojäämättä luonnollisten lukujen kanssa samalla tavalla käyttäytyvän osajärjestelmän. Jälleen kerran noudatamme sitä periaatetta, että koska kyseistä osajärjestelmää ei mitenkään voi erottaa luonnollisista luvuista, sanomme, että se *on* luonnolliset luvut. Lakien (10) ja (12) ansiosta mukana ovat muutkin rationaaliluvut, myös negatiiviset, ja niiden yhteen-, vähennys-, kerto- ja jakolaskuista tulevat ne tulokset, jotka koulussa opittiin. Toisaalta rationaaliluvut toteuttavat lait (1), ..., (16), joten rationaalilukujen järjestelmä on pienin nämä lait toteuttava järjestelmä.

Edellä otettiin huomioon mahdollisuus, että $1 < 0$. Ilman lakia (16) tämä olisi todellakin mahdollista! Sen huomaa siitä, että jos "$<$" käännetään toisinpäin muotoon "$>$", niin lait (13), ..., (15) ovat yhä voimassa, mutta (16) rikkoutuu. Siis vasta laki (16) on se, joka kertoo, kumminpäin luvut on asetettu suuruusjärjestykseen.

Mahdollisuus $1 < 0$ voidaan sulkea pois seuraavasti. Edellä osoitettiin, että $x \cdot 0 = 0$. Siitä seuraa, että $0 = x\cdot 0 = x\cdot(1+(-1)) = x\cdot 1+x\cdot(-1) = x+x\cdot(-1)$. Siis $x \cdot (-1)$ on x:n vastaluku eli $-x$. Niinpä $(-1) \cdot (-1) = -(-1) = 1$. Jos $1 < 0$, niin lisäämällä kummallekin puolelle -1 saadaan $0 < -1$. Niinpä laki (16) vaatii, että $0 < (-1) \cdot (-1) = 1$. Siis samanaikaisesti $1 < 0$ ja $0 < 1$. Se rikkoo lakia (13). Vaihtoehto $1 < 0$ on siis mahdoton, joten ainoa jäljelle jäävä vaihtoehto $0 < 1$ on oikea.

Reaalilukujen järjestelmä tulee täysin määritellyksi, kun lisätään vielä yksi laki, niin sanottu *täydellisyysaksiooma*. Se on nykyaikainen muotoilu asiasta, jonka nimi on *Dedekindin leikkaus*, ja jonka keksi Richard Dedekind 1800-luvun jälkipuoliskolla [1, s. 788–789]. Se on monimutkainen ilmaista täsmällisesti, mutta sen perusajatus on seuraava. Ajatellaan, että kaikki reaaliluvut jaetaan millä tahansa periaatteella kahteen epätyhjään osaan, ”pienet luvut” ja ”suuret luvut”, siten, että jokainen pieni luku on pienempi kuin jokainen suuri luku. Täydellisyysaksiooma sanoo, että joko pienten lukujen joukossa on suurin tai suurten lukujen joukossa on pienin.

Tämän ymmärtämiseksi tarkastelkaamme jakoa, jossa ”pienet luvut” sisältävät kaikki negatiiviset luvut, nollan, sekä ne positiiviset luvut, joiden neliö on enintään 2. ”Suuret luvut” ovat tietysti loput positiiviset luvut.

Jos rationaaliluvuille tehdään tällainen jako, niin $\sqrt{2}$ ei ole kummassakaan osassa, koska se ei ole rationaaliluku. Pienten lukujen osa sisältää loputtomiin sen toinen toistaan tarkempia alalikiarvoja, kuten 1, 1,4, 1,41 ja 1,4142135. (Jokainen näistä on rationaaliluku. Esimerkiksi $1{,}4142 = \frac{14142}{10000}$.) Otetaan mikä tahansa pieni luku, niin sitä suurempi pieni luku löydetään valitsemalla $\sqrt{2}$:n alalikiarvo, jossa on tarpeeksi monta desimaalia. Mikään pienistä luvuista ei siis ole suurin pieni luku. Vastaavasti suurten lukujen osa sisältää loputtomiin tarkkenevia ylälikiarvoja, kuten 2, 1,5, 1,42 ja 1,4142136. Otetaan mikä tahansa suuri luku, niin tarpeeksi monidesimaalinen $\sqrt{2}$:n ylälikiarvo on sitä pienempi. Siis mikään suurista luvuista ei ole pienin suuri luku. Huomaamme, että rationaalilukujen joukko ei noudata täydellisyysaksioomaa.

Reaalilukujen tapauksessa täydellisyysaksiooma pakottaa ainakin yhden luvun olemassaolon, joka on joko suurin pienistä tai pienin suurista. Tämä luku ei ole mikään edellä luetelluista rationaalisista likiarvoista. Lakien (13), ..., (16) vuoksi tämän luvun neliön on pakko olla enintään yhtäsuuri kuin minkä tahansa suuren luvun neliön ja ainakin yhtäsuuri kuin minkä tahansa positiivisen pienen luvun neliön. Neliö ei siis voi olla muuta kuin 2, joten tämän luvun on oltava $\sqrt{2}$.

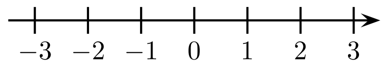
Samalla kun täydellisyysaksiooma pakottaa mukaan kaikki luvut, jotka sijaitsevat rationaalilukujen väleissä, se varmistaa, että mukaan ei tule olentoja, jotka olisivat suurempia kuin kaikki rationaaliluvut. Nimittäin, jos tällainen olento olisi mukana, reaaliluvut voitaisiin jakaa ”pieniin” ja ”suuriin” siten, että pieniä ovat kaikki rationaaliluvut ja niitä pienemmät luvut. Mikään rationaaliluku q ei ole pienistä luvuista suurin, koska myös $q + 1$ on rationaaliluku ja $q + 1 > q$. Mikään muu pieni luku ei voi olla suurin pieni luku, koska se on jotain rationaalilukua pienempi. Siis pienten lukujen joukossa ei ole suurinta. Niinpä täydellisyysaksiooman vuoksi suurten lukujen joukossa on oltava pienin luku. Olkoon sen nimi ω. Lain (15) nojalla $\omega - 1 < \omega$. Koska ω on pienin suuri luku, on $\omega - 1$ pieni luku, eli on olemassa rationaaliluku q siten, että $\omega - 1 \leq q$. Mutta silloinhan $\omega \leq q + 1$, mikä on ristiriidassa sen kanssa, että suurena lukuna ω ei ole rationaaliluku eikä mitään rationaalilukua pienempi. Siis suurten lukujen osan on pakko olla tyhjä, eli ei ole olemassa reaalilukua, joka on suurempi kuin kaikki rationaaliluvut.

Vastaavalla tavalla nähdään, että ei ole olemassa reaalilukua, joka on pienempi kuin kaikki rationaaliluvut.

Reaalilukujen joukko noudattaa täydellisyysaksioomaa siitä yksinkertaisesta syystä, että täydellisyysaksiooma on otettu mukaan reaalilukujen joukon määritelmään. Tätä ei voitu tehdä noin vain, vaan ensin piti varmistua, että se sopii yhteen reaalilukujen muiden lakien kanssa. Eihän nollan käänteisarvoakaan voitu ottaa mukaan, koska se ei sopinut yhteen tärkeiden lakien kanssa. Tämä tarkastus on valitettavasti liian monimutkainen asia tässä käsiteltäväksi.

(17) Täydellisyysaksiooma

Reaaliluvut voidaan asettaa molempiin suuntiin päättymättömälle suoralle. Se tunnetaan nimellä *lukusuora*.



Kompleksiluvut

Nyt voimme vihdoin ja viimein keskittyä olennon $\sqrt{-1}$ ongelmaan. Aluksi toteamme, että ainakaan reaaliluku se ei ole. Nimittäin, nolla se ei tietenkään ole, koska $0 \cdot 0 = 0 \neq -1$. Laki (16) takaa, että se ei ole mikään positiivinen reaaliluku. Negatiiviset vaihtoehdot saadaan suljettua pois osoittamalla, että kahden negatiivisen luvun tulo on positiivinen. Olkoot $a < 0$ ja $b < 0$. Lisäämällä molempiin vastaluvut molemmille puolille saadaan $0 < -a$ ja $0 < -b$. Lain (16) mukaan siis $0 < (-a)(-b)$. Toisaalta $(-a)(-b) = (a(-1))(b(-1)) = \ldots = (ab)((-1)(-1)) = (ab)1 = ab$. Siis $0 < ab$.

Kuitenkin yhtälöiden ratkaisemisesta saadut kokemukset houkuttelevat laskemaan olennolla $\sqrt{-1}$ ja muilla negatiivisten lukujen neliöjuurilla ikäänkuin ne olisivat lukuja. Esimerkiksi Geronimo Cardano ratkaisi vuoden 1545 kirjassaan kolmannen asteen yhtälöitä $x^3 = px + q$ tavalla, joka vastaa kaavaa $x = \sqrt[3]{A+B} + \sqrt[3]{A-B}$, missä $A = \frac{q}{2}$ ja $B = \sqrt{\frac{q^2}{4} - \frac{p^3}{27}}$ [1, s. 399–405]. (Cardano myönsi kirjassaan, että hän ei ollut tuloksen keksijä.) Yhtälön $x^3 = 3x + 2$ tapauksessa tämä johtaa nätisti välivaiheiden $A = 1$ ja $B = 0$ kautta oikeaan ratkaisuun $x = 2$. Mutta tapauksessa $x^3 = 15x + 4$ tämä tuottaa tulokseksi $x = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}$. Cardano ei tästä selvinnyt, vaikka hän tiesi, että $x = 4$ on yhtälön ratkaisu.

Rafael Bombelli hyväksyi tuloksen $\sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}} = 4$ päteväksi [1, s. 408]. Hän arvasi rohkeasti, että $\sqrt[3]{2 \pm \sqrt{-121}}$ ovat muotoa $a \pm b\sqrt{-1}$. Koska niiden summa on 4, on $a = 2$. Laskemalla $(2 \pm b\sqrt{-1})^3 = 8 \pm 12b\sqrt{-1} - 6b^2 \mp b^3\sqrt{-1} = (8 - 6b^2) \pm (12b - b^3)\sqrt{-1}$ havaitaan, että kaikki täsmää, jos $8 - 6b^2 = 2$ ja $(12b - b^3)\sqrt{-1} = 11\sqrt{-1} = \sqrt{-121}$. Tähän päästään sijoittamalla $b = 1$. Siis $\sqrt[3]{2 + \sqrt{-121}} = 2 + \sqrt{-1}$. Tämä ei auttanut yhtälön $x^3 = px + q$ ratkaisemisessa silloin, kun $\frac{q^2}{4} - \frac{p^3}{27} < 0$, mutta oli askel kompleksilukujen ominaisuuksien ymmärtämisen suuntaan.

Bombelli siis laski olennolla $\sqrt{-1}$ ikäänkuin se olisi luku, joka noudattaa samoja sääntöjä kuin muutkin luvut. Olennosta $\frac{1}{0}$ saamiemme kokemusten vuoksi tiedämme, että sellainen ei välttämättä ole turvallista. Meillä on kuitenkin yksi etu, jota Bombellilla ei ollut: tiedämme, että olennainen kysymys on, missä määrin lait (1), ..., (17) säilyvät.

Näimme, että jokaisen lakeja (13), ..., (16) noudattavan luvun neliö on 0 tai positiivinen. Nyt nimenomaan haluamme luvun, jonka neliö on negatiivinen. Näin ollen, vaikka kaikki tätä ennen käyttöönotetut luvut noudattavat lakeja (13), ..., (16), nyt niistä on pakko luopua ainakin osittain. Koska niiden tehtävä on asettaa luvut suuruusjärjestykseen, on yksinkertaisinta todeta, että $\sqrt{-1}$ on reaalilukujen suuruusjärjestyksen — siis lukusuoran — ulkopuolella, ja sitten unohtaa ne kaikki.

Lain (17) tehtävä on varmistaa, että kaikki reaaliluvut ovat mukana reaalilukujen järjestelmässä. Sitä ei voi sellaisenaan soveltaa uusille luvuille, koska se käyttää hyväkseen lukujen suuruusjärjestystä, jonka juuri menetimme. Toisaalta, jos vaadimme, että uusi järjestelmä on reaalilukujen laajennos, niin kaikki reaaliluvut ovat mukana ja lain (17) tehtävä on suoritettu.

Tutkikaamme siis, mitä seuraa, jos oletetaan reaalilukujen lisäksi sellaisen luvun i olemassaolo, että $i^2 = -1$, ja pidetään samanaikaisesti kiinni laeista (1), ..., (12). Syntyykö ristiriita, vai saadaanko aikaan toimiva lukujärjestelmä? Tai ehkä syntyy monta erilaista toimivaa lukujärjestelmää?

Lain (4) vuoksi uutta lukua i täytyy voida kertoa reaaliluvuilla. Siis bi on olemassa, kun b on reaaliluku. Uusia lukuja täytyy voida myös laskea yhteen reaalilukujen kanssa. Tällä tavalla saadaan lausekkeita muotoa $a + bi$. Voidaan osoittaa, että ne kaikki vastaavat eri lukuja. Nimittäin, jos $a_1 + b_1 i = a_2 + b_2 i$, niin $(b_1 - b_2)i = a_2 - a_1$. Jos $b_1 - b_2 \neq 0$, tästä saadaan edelleen $i = \frac{a_2 - a_1}{b_1 - b_2}$, joka on reaaliluku. Mutta i ei ole reaaliluku, joten $b_1 - b_2 = 0$ eli $b_1 = b_2$. Siitä seuraa $a_2 - a_1 = (b_1 - b_2)i = 0i = 0$. Niinpä $a_1 = a_2$.

Siis kun $b \neq 0$, niin jokainen olento muotoa $a + bi$ on uusi luku, joka pitää ottaa mukaan järjestelmään. ($a + 0i$ on tietenkin vanha tuttu reaaliluku a.) Niinpä niilläkin on voitava laskea yhteen- ja kertolaskuja. Tuleeko niistä tulokseksi lisää uusia lukuja, jotka on pakko ottaa mukaan, ja niin edelleen loputtomiin?

Yhteenlaskun vaihdannaisuus- ja liitännäisyyslain sekä osittelulain ansiosta kahden tällaisen olennon summa paljastuu samanlaiseksi olennoksi: $(a_1 + b_1 i) + (a_2 + b_2 i) = a_1 + b_1 i + a_2 + b_2 i = a_1 + a_2 + b_1 i + b_2 i = (a_1 + a_2) + (b_1 + b_2)i$. Yhteenlasku ei siis tuota enää lisää uusia olentoja. Myöskään kertolasku ei tuota lisää uusia olentoja, koska $(a_1 + b_1 i)(a_2 + b_2 i) = a_1 a_2 + a_1 b_2 i + b_1 a_2 i + b_1 b_2 i^2 = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2)i$.

Uusilla olennoilla pitää olla vasta- ja käänteisluvut. Onneksi on helppo huomata, että $-a - bi$ on olennon $a + bi$ vastaluku. Käänteisluvuksi kelpaa $\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$, mikä voidaan tarkastaa laskulla $(a + bi)(\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i) = (\frac{a^2}{a^2+b^2} + \frac{b^2}{a^2+b^2}) + (-\frac{ab}{a^2+b^2} + \frac{ba}{a^2+b^2})i = \frac{a^2+b^2}{a^2+b^2} = 1$. Se on olemassa, kun $a \neq 0$ tai $b \neq 0$, koska silloin $a^2 + b^2 > 0$.

Ei siis ole enää tarvetta ottaa mukaan lisää olentoja.

Olemme osoittaneet, että jos reaalilukujen joukko halutaan laajentaa kunnaksi, jossa on luku i siten, että $i^2 = -1$, niin on vain yksi tapa edetä. Mukana ovat kaikki parit muotoa $a + bi$, missä a ja b ovat reaalilukuja, ja yhteen- ja kertolaskut lasketaan näin:

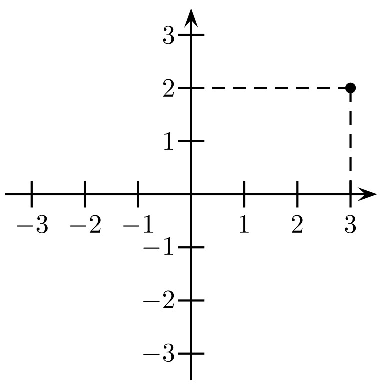
$$\begin{aligned} & (a_1 + b_1 i) + (a_2 + b_2 i) \\ = \;& (a_1 + a_2) + (b_1 + b_2)i \end{aligned}$$

$$\begin{aligned} & (a_1 + b_1 i)(a_2 + b_2 i) \\ = \;& (a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2)i \end{aligned}$$

Vielä on tarpeen tarkastaa, että näin syntyvä järjestelmä todella on kunta, ja että emme vahingossa muuttaneet reaalilukujen käyttäytymistä. Jos sijoitetaan vasta- ja käänteisluvun kaavoihin $b = 0$, saadaan $-a - 0i = -a$ ja $\frac{a}{a^2+0^2} - \frac{0}{a^2+0^2}i = \frac{1}{a}$, kuten pitääkin. Jos sijoitetaan summan ja tulon kaavoihin $b_1 = b_2 = 0$, huomataan, että tulokseksi saadaan tutut reaalilukujen summa ja tulo. Lait (1), (4), (10) ja (12) tuli jo tarkastettua, ja loppujen tarkastaminen on rutiinityötä.

Lukujen $a + bi$ järjestelmä on siis reaaliluvut sisältävä kunta. Se tunnetaan nimellä *kompleksiluvut*. Luvut muotoa bi, missä $b \neq 0$, ovat *imaginaariluvut*. Päättelystämme seuraa, että kompleksiluvuille ei ole vaihtoehtoa. Jos reaaliluvut laajennetaan kunnaksi, jossa on alkio, jonka neliö on -1, niin silloin kaikki kompleksiluvut tulevat vääjäämättä mukaan.

Sveitsiläinen Leonhard Euler (1707–1783) ymmärsi kompleksiluvut hyvin. Häneltä on peräisin luvun $\sqrt{-1}$ merkki i sekä hämmästyttävä tulos $e^{\pi i} = -1$, joka liittää toisiinsa luonnollisen logaritmijärjestelmän kantaluvun e, ympyrän kehän ja halkaisijan suhteen π ja imaginaariyksikön i [1, s. 622]. Mutta kompleksiluvut hyväksyttiin yleisesti vasta kun Carl Friedrich Gauss, joka on eräs historian suurimmista matematiikoista, näytti vuonna 1832, että ne vastaavat tason pisteitä [1, s. 710]. Caspar Wessel oli tosin keksinyt saman jo vuonna 1797, mutta hänen tuloksensa ei saanut ansaitsemaansa huomiota, kenties siksi, että hän ei julkaissut sitä kansainvälisessä tiedelehdessä vaan Tanskan akatemian sarjassa. Lukua $a + bi$ vastaa x-y-koordinaatiston piste (a, b). Esimerkiksi kuvan piste vastaa lukua $3 + 2i$.



3-ulotteisia lukuja?

Näimme, että reaaliluvut vastaavat (luku)suoran pisteitä ja kompleksiluvut vastaavat tason pisteitä. Suora on yksi- ja taso on kaksiulotteinen olento, joten reaaliluvut ovat yksi- ja kompleksiluvut ovat kaksiulotteisia lukuja. Maailma, jossa elämme, on kolmiulotteinen. Niinpä seuraava luonnollinen askel olisi kehittää kolmiulotteisia lukuja. Tässä luvussa huomaamme kuitenkin, että sellaisia ei voi olla olemassa. Siihen päästäksemme meidän on ensin tutkittava hieman polynomeja ja niiden nollakohtia.

Lauseketta $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, missä a_i:t ovat lukuja, kutsutaan *polynomiksi*. Jos $a_n \neq 0$, se on *n:nnen asteen* polynomi. Esimerkiksi $x^3 - 2x^2 + 16$ on kolmannen asteen polynomi. Polynomin *nollakohta* on sellainen luku x, että $a_nx^n + \cdots + a_0 = 0$. Luvut a_i ovat polynomin *kertoimet*. Polynomin $x^3 - 2x^2 + 16$ kertoimet ovat 1, -2, 0 ja 16. Sillä on kolme nollakohtaa: -2, $2 + 2i$ ja $2 - 2i$.

Edellä mainittu Gauss todisti vuonna 1799 julkaistussa väitöskirjassaan hienon tuloksen: jokaisella polynomilla, jonka kertoimet ovat kompleksilukuja ja jonka aste on ainakin yksi, on ainakin yksi nollakohta, joka on kompleksiluku [1, s. 698–699]. Tämä tulos on niin tärkeä, että sitä kutsutaan algebran peruslauseeksi. Valitettavasti todistus on liian monimutkainen tässä esitettäväksi.

Olkoon x_1 polynomin $a_nx^n + \cdots + a_0$ nollakohta. Jos luvut $b_{n-1}, \ldots, b_0$ on valittu siten, että $b_{n-1} = a_n$ ja muutoin $b_{j-1} = x_1b_j + a_j$, niin pienellä kertolaskulla voidaan tarkastaa, että $a_nx^n + \cdots + a_0 = (x - x_1)(b_{n-1}x^{n-1} + \cdots + b_0)$. Myös $b_{n-1}x^{n-1} + \cdots + b_0$ on polynomi. Jos sen aste on vähintään yksi, niin silläkin on nollakohta x_2 ja se voidaan jakaa muotoon $(x - x_2)(c_{n-2}x^{n-2} + \cdots + c_0)$. Tällä tavalla jatkamalla nähdään, että jokainen polynomi voidaan kirjoittaa muodossa $a_nx^n + \cdots + a_0 = (x - x_1)(x - x_2) \cdots (x - x_n)a_n$, missä $x_1, x_2, \ldots, x_n$ ovat polynomin nollakohtia. Polynomilla ei voi olla näiden lisäksi muita nollakohtia, koska muilla x:n arvoilla oikea puoli on nollasta poikkeavien lukujen $x - x_1$, $x - x_2$ ja niin edelleen sekä a_n tulo, ja siksi nollasta poikkeava.

Kompleksilukujen laskusäännöistä on helppo tarkastaa, että jos kompleksilukujen yhteen- tai kertolaskussa vaihdetaan kaikkien imaginaariosien etumerkit, niin tulos säilyy muuten ennallaan, paitsi että tuloksenkin imaginaariosan etumerkki vaihtuu. Toisin sanoen, jos $(a_1+b_1i)+(a_2+b_2i) = a+bi$, niin $(a_1-b_1i)+(a_2-b_2i) = a - bi$, ja jos $(a_1 + b_1i)(a_2 + b_2i) = a + bi$, niin $(a_1 - b_1i)(a_2 - b_2i) = a - bi$. Tästä seuraa, että jos polynomin kertoimet $a_0, \ldots, a_n$ ovat reaalilukuja ja polynomin arvo x:n arvolla $a + bi$ on $c + di$, niin polynomin arvo x:n arvolla $a - bi$ on $c - di$.

Erityisesti, jos $a + bi$ on reaalikertoimisen polynomin nollakohta, niin $c + di = 0$, joten $c = d = 0$ ja $c - di = 0$, joten myös $a - bi$ on kyseessä olevan polynomin nollakohta. Nollakohtia $a + bi$ ja $a - bi$ vastaavien tekijöiden $x - (a + bi)$ ja $x - (a - bi)$ tulo on $x^2 - 2ax + a^2 + b^2$. Se on toisen asteen polynomi, jonka kertoimet ovat reaalilukuja. Tästä seuraa, että jokainen reaalikertoiminen vähintään astetta yksi oleva polynomi voidaan esittää ensimmäistä ja toista astetta olevien reaalikertoimisten polynomien tulona. Esimerkkipolynomillemme $x^3 - 2x^2 + 16$ tämä tulo on $(x + 2)(x^2 - 4x + 8)$.

Tämän päättelyn lopputulos koskee pelkästään reaalilukuja eikä lainkaan imaginaarilukuja, joten se olisi ollut kiinnostava niidenkin menneen ajan matematiikoiden mielestä, jotka eivät hyväksyneet imaginaarilukuja. He eivät olisi kuitenkaan uskaltaneet ottaa tulosta käyttöön ilman todistusta, jossa ei käytetä imaginaarilukuja. Sellaista ei ole helppo löytää. Tässä on jälleen esimerkki siitä, että imaginaarilukuja tarvitaan välivaiheena matkalla tulokseen, joka ei käsittele imaginaarilukuja.

Nyt voidaan tutkia, mitä tapahtuu, jos reaalilukujen laajentamisen lähtökohtana ei olisikaan i, joka on polynomin $x^2 + 1$ nollakohta, vaan jonkin muun reaalikertoimisen polynomin nollakohta. Polynomina voi olla $x^4 + 1$ tai mikä tahansa muu reaalikertoiminen polynomi, jolla ei ole nollakohtaa reaalilukujen joukossa. Merkitsemme sen hypoteettista nollakohtaa symbolilla $\ddot{\imath}$.

Kuten edellä nähtiin, kyseessä oleva polynomi voidaan jakaa reaalikertoimisiin ensimmäisen ja toisen asteen tekijöihin. Luku $\ddot{\imath}$ on jonkin niistä nollakohta. Se ei voi olla ensimmäisen asteen tekijän $x - x_j$ nollakohta, koska silloin se olisi reaaliluku x_j. Se on siis jonkin toisen asteen tekijän $x^2 + px + q$ nollakohta, eli $\ddot{\imath}^2 + p\ddot{\imath} + q = 0$. Toisen asteen yhtälön ratkaisukaavasta tiedämme, että $p^2 - 4q < 0$ eli $4q - p^2 > 0$, koska muutoin polynomin $x^2 + px + q$ nollakohdat olisivat reaalilukuja, eikä uudelle luvulle $\ddot{\imath}$ olisi tilaa. Nyt voimme laskea $(p + 2\ddot{\imath})^2 = p^2 + 4p\ddot{\imath} + 4\ddot{\imath}^2 = 4(\ddot{\imath}^2 + p\ddot{\imath} + q) - 4q + p^2 = 4 \cdot 0 - 4q + p^2 = -(4q - p^2)$. Niinpä $\left(\frac{p+2\ddot{\imath}}{\sqrt{4q-p^2}}\right)^2 = \frac{-(4q-p^2)}{4q-p^2} = -1$.

Siis mukaan tunkeutui väkisin luku, jonka neliö on -1! Edellä näimme, että tällaisen luvun olemassaolo määrää kompleksiluvut yksikäsitteisesti. Huomaamme, että nollakohdan olettaminen *mille tahansa* reaalikertoimiselle polynomille, jolla ei sellaista ole reaalilukujen joukossa, johtaa aina samaan kompleksilukujen järjestelmään.

Nyt on helppo osoittaa, että kolmiulotteisia lukuja ei ole olemassa — eikä neli-, viisi-, kuusi- tai muitakaan, missä ulottuvuuksien määrä on äärellinen ja vähintään kolme. Päästäksemme reaaliluvuista eteenpäin tarvitsemme ainakin yhden uuden luvun $\ddot{\imath}$. Se ei saa olla minkään reaalikertoimisen polynomin nollakohta, koska muuten tulokseksi tulee kompleksiluvut, kuten äsken näimme. Näinollen esimerkiksi $\ddot{\imath}^4$ ei ole mikään niistä luvuista, jotka voidaan esittää muodossa $a + b\ddot{\imath} + c\ddot{\imath}^2 + d\ddot{\imath}^3$, koska muutoin se olisi polynomin $x^4 - dx^3 - cx^2 - bx - a$ nollakohta. Samasta syystä $a_1 + b_1\ddot{\imath} + c_1\ddot{\imath}^2 + d_1\ddot{\imath}^3 \neq a_2 + b_2\ddot{\imath} + c_2\ddot{\imath}^2 + d_2\ddot{\imath}^3$ paitsi kun $a_1 = a_2$, $b_1 = b_2$, $c_1 = c_2$ ja $d_1 = d_2$. Jokainen luvuista $\ddot{\imath}$, $\ddot{\imath}^2$, $\ddot{\imath}^3$, ... tarvitsee siis käyttöönsä oman uuden ulottuvuuden, eikä mikään äärellinen ulottuvuuksien määrä riitä.

Jos laajentaminen aloitetaan kompleksiluvuista, niin silloinkaan $\ddot{\imath}$ ei voi olla minkään kompleksikertoimisen polynomin nollakohta, koska sen kaikki nollakohdat löytyvät kompleksilukujen joukosta, kuten Gauss todisti. Samalla lailla kuin äsken nytkin saadaan tulokseksi, että jokainen luvuista $\ddot{\imath}$, $\ddot{\imath}^2$, $\ddot{\imath}^3$, ... luo oman ulottuvuuden.

Jos ulottuvuuksia sallitaan rajaton määrä, niin kompleksiluvuille löytyy laajennos, joka on kunta. Nimittäin lausekkeet muotoa polynomi jaettuna polynomilla, jossa kertoimet ovat kompleksilukuja ja jakaja on jokin muu polynomi kuin 0, ovat nekin olentoja, joita voi laskea yhteen ja kertoa keskenään. Kuinka ollakaan, niidenkin muodostama järjestelmä on kunta. Polynomien osamäärät ovat käsitteenä kuitenkin niin kaukana tutuista luvuista, että niitä ei kutsuta luvuiksi. (Jos tämä temppu tehdään rationaalikertoimisille polynomeille, saadaan rationaalilukujen laajennos, jossa on alkio, joka on suurempi kuin kaikki kokonaisluvut. Tämä osoittaa, että täydellisyysaksiooma on todellakin tarpeen todistettaessa, että mikään reaaliluku ei ole kaikkia rationaalilukuja suurempi.)

Kompleksiluvuille ei siis ole vaihtoehtoja. Ne on otettava joko sellaisenaan, tai on tyydyttävä reaalilukuihin tai johonkin reaalilukujen osajoukkoon, tai sitten on pakko siirtyä samantien rajatonulotteisiin olentoihin. Ei ole olemassa hieman kompleksilukujen kaltaista mutta kuitenkin erilaista järjestelmää. Ei ole olemassa kolmiulotteisia kompleksilukuja. Kompleksi- ja imaginaariluvut ovat omituisen joustamattomia ollakseen vain imaginaarisia — eli kuvitteellisia.

Lopuksi

Matemaatikot määrittelevät käsitteitä rakentamalla niitä aikaisemmista käsitteistä. Tässä kertomuksessa rakensimme negatiiviset rationaaliluvut positiivisista. Matemaatikko voi määritellä käsitteen myös luettelemalla siltä vaadittavat ominaisuudet. Reaalilukujen määrittelemiseksi riittää luetella tässä tekstissä esitetyt 17 lakia.

Kun käsite määritellään luettelemalla lakeja, on vaarana, että lait ovat keskenään ristiriidassa. Näin käy esimerkiksi, jos asetetaan laeiksi (1), ..., (11) sekä (12) siten muutettuna, että myös $\frac{1}{0}$ on olemassa. Jos lait ovat ristiriidassa, käsitteelle voidaan todistaa kaksi ominaisuutta, jotka eivät mitenkään voi olla yhtäaikaa voimassa — esimerkiksi $1 = 0$ ja $1 \neq 0$. Käsite on silloin mahdoton. Sitä ei ole olemassa.

Tämä periaate toimii myös toisinpäin. Lakikokoelma on varmasti ristiriidaton, jos voidaan antaa esimerkki käsitteestä, joka toteuttaa sen. Lait (1), ..., (12) ovat varmasti ristiriidattomat, koska kohdassa ”Mitä luvut ovat?” esitettiin viisialkioinen järjestelmä, joka toteuttaa ne. Toinen, tutumpi esimerkki ne toteuttavasta käsitteestä on rationaaliluvut. Viisialkioisessa järjestelmässä on se etu, että koska alkioita on vain viisi, jokainen laki voidaan tarkastaa erikseen jokaisella alkiolla, alkioiden parilla tai alkioiden kolmikolla. (Liitännäisyyslait ja osittelulaki puhuvat kolmesta alkiosta yhtäaikaa.) Lukija voi halutessaan tehdä tarkastuksen viimeistä yksityiskohtaa myöten. Rationaalilukuja on äärettömästi, joten tarkastusta ei voi tehdä jokaiselle rationaalilukukolmikolle erikseen, vaan on käytettävä epäsuoria keinoja.

Esimerkin antaminen on siis hyvä keino osoittaa, että lakikokoelma ei ole ristiriitainen.

Lakikokoelmilla määritteleminen on usein käsitteen käytön kannalta kätevämpi lähtökohta kuin rakentamalla määritteleminen. Lisäksi usein on olemassa monta käsitettä, jotka toteuttavat saman lakikokoelman — näimme, että on olemassa paljon erilaisia kuntia. Jos tällaisten käsitteiden ominaisuuksia tutkitaan lakikokoelmasta aloittaen, selville saadut asiat koskevat *kaikkia* lakikokoelman mukaisia käsitteitä — siis esimerkiksi kaikkia kuntia. Saadaan enemmän tuloksia samalla vaivalla. Lakikokoelmista aloittaminen auttaa yleensä myös paremmin ymmärtämään asioiden välisiä yhteyksiä.

Sitäpaitsi käsitteiden rakentamiseen aikaisemmista käsitteistä liittyy se ongelma, että niin ei voi tehdä, ennen kuin on määritelty ensimmäinen käsite, jolla päästään alkuun. Tämä ensimmäinen käsite voi olla esimerkiksi joukot tai luonnolliset luvut. Se täytyy määritellä lakikokoelman avulla.

Joukkoja ja luonnollisia lukuja on rajattomasti, joten niiden lakeja ei voi tarkastaa jokainen tapaus erikseen, niinkuin teimme viisialkioiselle esimerkkikunnalle. Usko joukkojen tai luonnollisten lukujen lakien ristiriidattomuuteen perustuu toisaalta siihen, että ne ovat hyvin yksinkertaisia ja uskottavan tuntuisia (ainakin matemaatikoiden mielestä!), ja toisaalta siihen, että niiden varaan on voitu rakentaa valtava määrä matematiikkaa ilman, että tuhoisia ristiriitoja on pulpahtanut esiin. Ristiriitaisuuksia on välillä ilmennyt, mutta aina ne on kyetty ratkaisemaan. Matematiikan ristiriidattomuuden puolesta puhuu myös se, että kännykät, avaruusraketit ja ydinvoimalaitokset toimivat (ainakin suurimman osan aikaa), vaikka ne on suunniteltu matematiikan avulla.

Molemmat tavat määritellä käsitteitä ovat siis tarpeen, ja ne ovat matematiikan tutkimuksessa vuorovaikutuksessa keskenään.

Matemaatikko saa siis määritellä käsitteitä aivan kuten haluaa, kunhan varoo ristiriitoja. Eikö tästä seuraa, että matematiikka on yhtä mielivaltaista kuin šhakkipelin säännöt?

Tämä kirjoitus on toivottavasti vakuuttanut lukijan siitä, että ei seuraa. Vaikka määritelmiä voi yrittää asettaa mielivaltaisesti, syntyvien käsitteiden ominaisuuksia ei voi säädellä mielivaltaisesti. Kuntaan ei pysty lisäämään nollan käänteisarvoa, vaikka kuinka maanittelisi. Kolmiulotteisia lukuja ei saa aikaan, vaikka kuinka yrittäisi. Jos niitä yrittää väkisin, saa aikaan ristiriitoja. Jos tekee määritelmään pienen muutoksen huolellisesti ristiriitoja välttäen, niin helposti käy niin, että saakin tulokseksi alkuperäisen käsitteen vain hieman naamioituna, kuten kävi yrityksessämme määritellä toisenlaisia kompleksilukuja olettamalla nollakohta polynomille x^4+1. Jos tekee määritelmään niin suuren ristiriidattoman muutoksen, että määritelty käsite muuttuu, niin muutosta ei pysty hienosäätämään halutuksi, vaan käsite loksahtaa johonkin toiseen niistä käsitteistä, jotka ovat mahdollisia.

Matemaattiset käsitteet ovat siis huomattavasti vähemmän vapaasti valittavissa kuin määritelmät. Ne ikäänkuin elävät omaa elämäänsä määritelmistä piittaamatta.

Kiitokset

Kiitän Tuomas T. Korppia aloitteen tekemisestä tämän kirjoituksen kirjoittamiseksi sekä osallistumisesta ideointiin.

Viitteet

[1] Boyer, Carl: *Tieteiden kuningatar, matematiikan historia.* Osa I sivut 1–469. Osa 2 sivut 471–982. Suomentanut Kimmo Pietiläinen. Art House, 1994.

[2] Cormen, Thomas H. & Leiserson, Charles E. & Rivest, Ronald L.: *Introduction to Algorithms.* The MIT Press, 1990.

[3] Nurmi, Timo & Rekiaro, Ilkka & Rekiaro, Päivi: *Suomalaisen sivistyssanakirja.* Gummerus Kirjapaino Oy, Jyväskylä 1995.

[4] Stroustrup, Bjarne: *The C++ Programming Language, Third Edition.* Addison-Wesley, 1997.