# 5 Rationaaliluvut

Edellisessä luvussa olemme konstruoineet luonnollisten lukujen joukko $\mathbb{N} = \{0, 1, \ldots\}$. Tässä luvussa laajennamme luonnollisten lukujen joukko ensin kokonaislukujen joukoksi ja sitten rationaalilukujen joukoksi. Molemmat laajennukset perustuvat *ekvivalenssirelaatioiden* käyttöön.

## 5.1 Ekvivalenssirelaatiot

Aloitetaan motivoimalla kokonaislukujen tarpeellisuutta. Motivaatio, johon päädytään, antaa samalla konkreettisen tavan konstruoida kokonaislukuja.
Algebran näkökulmasta negatiivisia kokonaislukuja tarvitaan, koska lineaarisella yhtälöllä $x + a = b$, missä $x$ on tuntematon, $a, b \in \mathbb{N}$ kiinteitä luonnollisia lukuja, ei aina ole ratkaisuja $\mathbb{N}$:ssä. Itse asiassa Proposition 74 mukaan tällaisella yhtälöllä on $\mathbb{N}$:ssä (yksikäsitteinen) ratkaisu jos ja vain jos $a \leq b$. Esimerkiksi yhtälöllä $x + 2 = 1$ ei ole ratkaisuja $\mathbb{N}$:ssä.
Näin ollen yritetään konstruoida kokonaislukuja lineaaristen yhtälöiden $x + a = b$, $a, b \in \mathbb{N}$ ratkaisuina. Voidaan ajatella, että mikä tahansa tällainen yhtälö "synnyttää" kokonaisluvun $x = b - a$, joka on tämän yhtälön ratkaisu. Koska yhtälö $x + a = b$ tunnetaan täydellisesti kun tunnetaan luonnollisia lukuja $a, b \in \mathbb{N}$ (annettuina tässä järjestyksessä), on luonnollista koodata vastaava kokonaisluku parilla $(a, b)$.
Tämä ei kuitenkaan vielä riittää - emme voi määritellä kokonaislukuja pareina $(a, b)$ eli joukkona $\mathbb{N} \times \mathbb{N}$. Syy tähän on se, että erilaiset yhtälöt saattavat vastata samoja kokonaislukuja. Esimerkiksi yhtälöillä $x + 2 = 1$ ja $x + 7 = 6$ pitäisi olla sama ratkaisu - kokonaisluku $-1$.
Näin ollen oikea tapa ei ole ajatella, että pari $(a, b)$ "on" kokonaisluku, vaan, että tämä pari *edustaa* erään kokonaisluvun. Eri parit saattavat edustaa samaa kokonaislukua. Esimerkiksi eri parit $(2, 1)$ ja $(7, 6)$ edustavat samaa kokonaislukua $-1$.
Tässä esimerkissä huijasimme hiukan, sillä käytimme ennestään tuttua tietoa kokonaisluvuista. Jos leikitään, että tunnetaan vain luonnollisia lukuja, mistä voimme tietää, että yhtälöillä $x + 2 = 1$ ja $x + 7 = 6$ "pitää" olla sama ratkaisu?

Vastataan tähän kysymykseen tutkimalla yleisesti milloin parit $(a, b)$ ja $(c, d)$ edustavat samaa kokonaislukua. Koska mitään kokonaislukuja ei vielä ole, ensin pitää tietysti määritellä tarkemmin mitä haemme.
Oletetaan, että $\mathbb{Z}$ on joku joukko, joka sisältää luonnollisten lukujen joukon $\mathbb{N}$, $\mathbb{N} \subset \mathbb{Z}$. Kuvitellaan myös, että $\mathbb{Z}$:ssä on määritelty yhteenlasku $+$, joka yhtyy osajoukossa $\mathbb{N}$ luonnollisten lukujen tavalliseen yhteenlaskuun. Lisäksi

oletetaan, että tämä yhteenlasku on liitännäinen operaatio.
Olkoot $a, b, c, d$ luonnollisia lukuja ja olkoon $x \in \mathbb{Z}$ sellainen alkio, joka on sekä yhtälön $x + a = b$, että yhtälön $x + c = d$ ratkaisu. Tutkitaan, onko tällöin mitään yhteyttä parien $(a, b)$ ja $(c, d)$ välillä, joka voidaan ilmastaa pelkästään joukon $\mathbb{N}$ struktuurin avulla.
Kahdesta luonnollisesta luvusta $a, c$ toinen on pienempi tai yhtä suuri kuin toinen, oletetaan esimerkiksi, että $a \leq c$. Tällöin Proposition 74 nojalla on olemassa sellainen $n \in \mathbb{N}$, jolle $a + n = c = n + a$ (luonnollisten lukujen yhteenlasku tiedetään olevan vaihdannainen). Tällöin

$$d = x + c = x + (a + n) = (x + a) + n = b + n.$$

Huomaa, että +:n oletettu liitännäisyys käytettiin laskun toisessa vaiheessa. Lisäämällä saatuun yhtälöön $b + n = d$ molemmille puolelle luku $a$, saadaan

$$b + c = b + (n + a) = (b + n) + a = d + a = a + d.$$

Saatiin ehto $a + d = b + c$, joka on ilmaistu kokonaan joukon $\mathbb{N}$ sisällä. Koska tilanne on täysin symmetrinen parien $(a, b)$ ja $(c, d)$ suhteen, sama ratkaisu saadaan jos $c \leq a$.

Ehto $a + d = b + c$ määrittelee joukossa $\mathbb{N} \times \mathbb{N}$ erään relaation $\sim$,

$$(a, b) \sim (c, d) \text{ jos } a + d = b + c.$$

Tämä relaatio on esimerkki *ekvivalenssirelaatiosta*.

**Määritelmä 77.** *Relaatio $\sim$ joukossa $X$ on ekvivalenssirelaatio, jos*

*(i)* $x \sim x$ *jokaisella* $x \in X$ *(refleksivisyys),*

*(ii) kaikilla* $x, y \in X$*, jos* $x \sim y$*, niin myös* $y \sim x$ *(symmetrisyys),*

*(iii) kaikilla* $x, y, z \in X$*, jos* $x \sim y$ *ja* $y \sim z$*, niin* $x \sim z$ *(transitiivisuus).*

**Esimerkkejä 78.** *1. Olkoon $\sim$ relaatio reaalilukujen joukossa $\mathbb{R}$,*

$$x \sim y \text{ jos } x^2 = y^2.$$

*Tällöin $\sim$ on ekvivalenssirelaatio. Nimittäin jokaisella $x \in \mathbb{R}$ pätee $x^2 = x^2$, joten relaatio on refleksiivinen. Jos $x \sim y$, niin $x^2 = y^2$, mistä seuraa, että $y^2 = x^2$, joten $y \sim x$. Lopuksi, jos $x^2 = y^2$ ja $y^2 = z^2$, joten $x^2 = z^2$, joten $\sim$ on myös transitiivinen.*
*Huomaa, että $x \sim y$ jos ja vain jos $x = y$ tai $x = -y$.*

2. *Olkoon $\sim$ relaatio EU-kansalaisten joukossa, $x \sim y$ jos $x$ ja $y$ ovat saman maan kansalaisia. Tällöin $\sim$ on refleksiivinen ja symmetrinen, mutta se ei ole transitiivinen, koska ihmisellä voi olla monen eri maan kansalaisuus. Esimerkiksi olkoon $x$ mikä tahansa Suomen kansalainen, $z$ mikä tahansa Saksan kansalainen ja $y$ Saksan ja Suomen kaksoiskansalainen. Tällöin $x \sim y$ ja $y \sim z$ , mutta ei välttämättä $x \sim z$.*
   *Näin ollen $\sim$ ei ole ekvivalenssirelaatio*

3. *Reaalilukujen järjestysrelaatio $\leq$ on refleksiivinen ja transitiivinen, niin kuin mikä tahansa osittaisjärjestys. Se ei kuitenkaan ole symmetrinen, esimerkiksi $0 \leq 1$, mutta ei $1 \leq 0$. Näin ollen $\leq$ ei ole ekvivalenssirelaatio.*

**Esimerkki 79.** *Osoitetaan, että yllä johdettu relaatio $\sim$,*

$$(a, b) \sim (c, d) \text{ jos } a + d = b + c$$

*joukossa $\mathbb{N} \times \mathbb{N}$ on ekvivalenssirelaatio.*
*Olkoot $(a, b), (c, d), (e, f) \in \mathbb{N} \times \mathbb{N}$ mielivaltaiset.*
*(1) $a + b = a + b$ kaikilla $a, b \in \mathbb{N}$, joten $(a, b) \sim (a, b)$ jokaisella parilla $(a, b) \in \mathbb{N} \times \mathbb{N}$.*
*(2) Oletetaan, että $(a, b) \sim (c, d)$. Tällöin $a + d = b + c$, joten, luonnollisten lukujen yhteenlaskun vaihdannaisuuden nojalla, pätee myös $c + b = d + a$. Relaation $\sim$ määritelmän nojalla tämä tarkoittaa, että $(c, d) \sim (a, b)$.*
*(3) Oletetaan, että $(a, b) \sim (c, d)$ ja $(c, d) \sim (e, f)$. Haluamme osoittaa, että $(a, b) \sim (e, f)$. Oletusten mukaan pätevät yhtälöt $a+d = b+c$ ja $c+f = d+e$. Näistä seuraa, että*

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

*missä käytimme hyväksi myös $\mathbb{N}$:n yhteenlaskun $+$ vaihdannaisuutta ja liitännäisyyttä hyväksi.*
*Propositiosta 74(iv) ("supistussääntö") seuraa, että $a + f = b + e$, eli $(a, b) \sim (e, f)$.*
*Näin ollen relaatio on ekvivalenssirelaatio.*

Hienoa, mutta mitäs sitten? Miten ekvivalenssirelaation käsite auttaa meitä konstruoimaan kokonaislukuja? Tämä tehdään ekvivalenssirelaatioon liittyvien ekvivalenssiluokkien kautta. Määrittelemme kokonaisluvun joukkona, jonka muodostavat kaikki parit $(a, b) \in \mathbb{N} \times \mathbb{N}$, jotka ovat keskenään relaatiossa $\sim$, eli kaikki parit jotka edustavat saman kokonaisluvun (eli ovat saman lineaarisen yhtälön "ratkaisuja").

**Määritelmä 80.** *Olkoon $\sim$ ekvivalenssirelaatio joukossa $X$ ja olkoon $x \in X$. Alkion $x$* ekvivalenssiluokka *on $X$:n osajoukko*

$$\bar{x} = \{y \in X \mid x \sim y\}.$$

*Alkion $x$ ekvivalenssiluokka koostuu siis tasan niistä $X$:n alkioista, jotka ovat relaatiossa $x$:n kanssa.*

**Lemma 81.** *Olkoon $\sim$ ekvivalenssirelaatio joukossa $X$. Tällöin $X$ on erillinen yhdiste relaation $\sim$ ekvivalenssiluokista, joista kaikki ovat epätyhjiä. Tarkemmin seuraavat ominaisuudet pätevät*
*(1) $\bar{x} \neq \emptyset$ kaikilla $x \in X$.*
*(2) Jos $x, y \in X$, niin joko $\bar{x} = \bar{y}$ tai*

$$\bar{x} \cap \bar{y} = \emptyset.$$

*(3) Olkoon $\mathcal{O}$ kaikkien ekvivalenssiluokkien muodostama joukko. Tällöin*

$$\bigcup \mathcal{O} = X.$$

*Todistus.* Koska $x \sim x$ relaation refleksiivisyyden nojalla, jokaisella $x \in X$ pätee $x \in \bar{x}$, joten erityisesti mikään ekvivalenssiluokka ei ole tyhjä. Lisäksi tästä automaattisesti seuraa myös, että $x \in \bigcup \mathcal{O}$, joten ekvivalenssiluokkien yhdiste on koko joukko $X$.
Olkoot $x, y \in X$. Osoitetaan, että jos $\bar{x} \cap \bar{y} \neq \emptyset$, niin itse asiassa $\bar{x} = \bar{y}$. Tästä ominaisuudesta erityisesti seuraa, että ekvivalenssiluokkien muodostama kokoelma $\mathcal{O}$ $X$:n osajoukkoja on erillinen.
Jos $\bar{x} \cap \bar{y} \neq \emptyset$, niin on olemassa $z \in X$ siten, että $z \in \bar{x}$ ja $z \in \bar{y}$. Ekvivalenssiluokkien määritelmän nojalla $x \sim z$ ja $y \sim z$. Koska $\sim$ on symmetrinen, jälkimmäisesti ehdosta seuraa, että $z \sim y$. Koska $x \sim z$ ja $z \sim y$, relaation transitiivisuuden nojalla $x \sim y$. Symmetrisyyden nojalla myös $y \sim x$.
Osoitetaan nyt, että $\bar{x} = \bar{y}$. Olkoon $u \in \bar{x}$. Tällöin $x \sim u$, joten, koska $y \sim x$, transitivisuuden nojalla $y \sim u$, eli $u \in \bar{y}$. Näin ollen $\bar{x} \subset \bar{y}$. Käänteinen sisältyvyys osoitetaan samalla tavalla. □

Edellinen tulos tarkoittaa sitä, että ekvivalenssirelaation määrittelemät ekvivalenssiluokat muodostavat joukon $X$ *osituksen.*
Potenssijoukon $\mathcal{P}(X)$ osajoukko $\mathcal{O}$ on joukon $X$ *ositus*, jos se toteuttaa seuraavia ehtoja.

(i) $\emptyset \notin \mathcal{O}$.

(ii) Perhe $\mathcal{O}$ on *erillinen* eli jos $A, B \in \mathcal{O}$, $A \neq B$, niin

$$A \cap B = \emptyset,$$

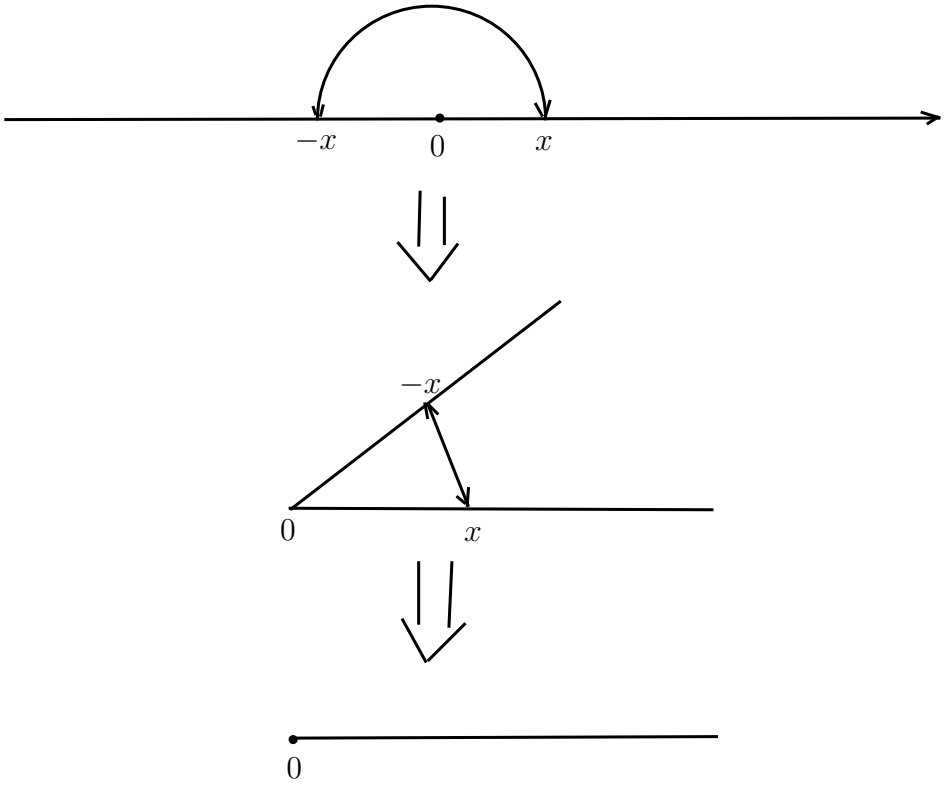
(iii) $\bigcup \mathcal{O} = X$.

Olkoon $\sim$ ekvivalenssirelaatio joukossa $X$. Tällöin sen ekvivalenssiluokat muodostavat $X$:n osituksen

$$X/\sim = \{\bar{x} \mid x \in X\}.$$

Tätä joukkoa sanotaan ekvivalenssirelaation $\sim$ määrittelemäksi $X$:n *tekijäjoukoksi*. Tekijäjoukossa ikään kuin "samastetaan" samoiksi alkioiksi joitakin joukon $X$ alkioita, jotka eivät ole $X$:ssä samoja alkioita. Tässä mielessä voidaan ajatella, että ekvivalenssirelaatio on "tapa määritellä yhtäsuuruus joukon $X$ alkioiden välillä uudestaan." Tästä syystä ekvivalenssirelaatioita sanotaan suomeksi usein myös "samastusrelaatioiksi".

**Esimerkki 82.** *Tarkastellaan joukossa $\mathbb{R}$ ekvivalenssirelaatiota $\sim$, $x \sim y$ jos $x^2 = y^2$. Tällöin jokaiselle $x \in \mathbb{R}$ ekvivalenssiluokka $\bar{x}$ on joukko $\{x, -x\}$. Tässä joukossa on 2 alkioita, paitsi kun $x = 0$, jolloin vastaava ekvivalenssiluokka on yksiö.*
*Geometrisesti tekijäjoukon $\mathbb{R}/\sim$ voi ajatella muodostuvan seuraavasti. Taivutetaan lukusuora nollan kohdalla ja "liimataan" yhteen jokainen luku vastalukunsa kanssa. Lopputuloksena on yksisuuntainen ääretön säie, joka alkaa pisteessä 0.*




Jokainen ekvivalenssirelaatio siis määrittelee kanonisella tavalla erään osituksen. Myös käänteinen pätee. Olkoon $\mathcal{O}$ joukon $X$ ositus. Tällöin relaatio $\sim$,

$$x \sim y \text{ jos on olemassa } O \in \mathcal{O} \text{ siten, että } x, y \in O$$

on ekvivalenssirelaatio $X$:ssä. Lisäksi tällöin relaation $\sim$ määräämä ositus $X/\sim$ on alkuperäinen ositus $\mathcal{O}$. Näiden väitteiden tarkka tarkastelu jätetään harjoitustehtäväksi.
Ekvivalenssirelaatiot ja ositukset ovat siis eri tapoja koodata joukko-opillisesti sama ilmiö (alkioiden samastus). Osituksia on helpompi ymmärtää intuitiivisesti, mutta ekvivalenssirelaatioita on helpompaa käyttää muodollisissa laskuissa.

## 5.2 Kokonaisluvut

Palataan nyt varsinaiseen kokonaislukujen konstruktioon. Määritellään joukossa $\mathbb{N} \times \mathbb{N}$ ekvivalenssirelaatio $\sim$

$$(a, b) \sim (c, d) \text{ jos } a + d = b + c.$$

Edellisessä luvussa olemme jo näyttäneet, että $\sim$ on todellakin ekvivalenssirelaatio. Sen määräämää tekijäjoukkoa $\mathbb{N} \times \mathbb{N}/\sim$ merkitään symbolilla $\mathbb{Z}$ ja sanotaan *kokonaislukujen joukoksi*. Joukon $\mathbb{Z}$ alkioita sanomme luonnollisesti *kokonaisluvuiksi*. Kokonaisluku on siis luokka $\overline{(a,b)}$, josta käytämme tässä yhteydessä myös merkintää $\langle a, b\rangle$.
Kokonaisluvuille on määriteltävää tuttuja laskuoperaatioita $+, \cdot$ sekä järjestysrelaatiota $<$. Ennen kuin mennään niihin, käsitellään vielä kysymys luonnollisten lukujen "upottamisesta" kokonaislukujen joukkoon. Nimittäin kokemuksemme mukaan jokainen luonnollinen luku on myös kokonaisluku, $\mathbb{N}$ on $\mathbb{Z}$:n osajoukko. Tässä vaiheessa formaalisti asia ei ole näin - jos lähdetään yhdestä kiinnitetystä luonnollisten lukujen mallista $\mathbb{N}$ ja konstruoidaan $\mathbb{Z}$ tekijäjoukkona $\mathbb{N} \times \mathbb{N}/\sim$, niin tällöin näille joukoille kirjaimellisesti ei päde $\mathbb{N} \subset \mathbb{Z}$. Täytyy kuitenkin muistaa, että matematiikassa käsitteille ei yleensä ole ainoata oikeata mallia, joukot kyseessä ovat vain eräitä tapoja konstruoida $\mathbb{N}$ ja $\mathbb{Z}$. Näin ollen vaatimus $\mathbb{N} \subset \mathbb{Z}$ on ymmärrettävää sillä tavalla, että konstruoidussamme joukossa $\mathbb{Z}$ on löydettävää osajoukko, joka olisi kopio $\mathbb{N}$:stä, joukon $\mathbb{Z}$ sisäinen "versio" luonnollisista luvuista.
Tämä osajoukko määritellään seuraavasti. Määritellään kuvaus $f\colon \mathbb{N} \to \mathbb{Z}$ kaavalla $f(n) = \langle n, 0\rangle$. Osoitetaan, että tämä kuvaus on injektio. Olkoot $n, m \in \mathbb{N}$ sellaiset, että $f(n) = f(m)$. Tällöin $(n, 0) \sim (m, 0)$, joten suoraan määritelmän $\sim$ nojalla pätee $n = n + 0 = 0 + m = m$. Kuvaus on siis injektio. Tästä seuraa, että kuvauksena $\mathbb{N} \to f(\mathbb{N})$ $f$ on bijektio, joten voimme "samastaa" $n \in \mathbb{N}$ ja $f(n) = \langle n, 0\rangle \in \mathbb{Z}$. Sitten, kun määritellään joukossa $\mathbb{Z}$ laskutoimituksia $+, \cdot$ ja järjestystä $\leq$, näytämme, että $f$ säilyttää niitä kaikkia. Samastamme siis $\mathbb{Z}$:n osajoukko $f(\mathbb{N})$ ja luonnollisten lukujen joukko $\mathbb{N}$ menettämättä mitään.

**Kokonaislukujen yhteenlasku.**
Olkoot $\langle a, b\rangle$, $\langle c, d\rangle$ kokonaislukuja. Määritellään niiden summaa kaavalla

$$\langle a, b\rangle + \langle c, d\rangle = \langle a + c, b + d\rangle. \tag{83}$$

Ennen kuin tällaista laskutoimitusta voi käyttää, on osoitettavaa, että se on **hyvin määritelty**. Miksi? Se johtuu siitä, että $+$ määriteltiin $\mathbb{Z}$:n alkioille käyttämällä jokaiselle alkiolle esitystä ekvivalenssiluokkana $\langle a, b\rangle$. Mitä oikeastaan on tapahtunut, on seuraava. Otamme kokonaislukuja $x, y \in \mathbb{Z}$. Joukon $\mathbb{Z}$ määritelmän nojalla $x$ ja $y$ ovat sivuluokkia, eli ne voidaan esittää muodossa $x = \langle a, b\rangle$, $y = \langle c, d\rangle$, joillakin $a, b \in \mathbb{N}, c, d \in \mathbb{N}$. Kuitenkin, tällainen esitys ei ole kuitenkaan yksikäsitteinen. Kysymys on siis siitä, että jos kaavassa 83 käytetään esityksen $x = \langle a, b\rangle$ sijaan esitystä $x = \langle a', b'\rangle$, jollakin $(a', b') \neq (a, b)$ ja samalla tavalla esityksen $y = \langle c, d\rangle$ sijaan esitystä

$y = \langle c', d' \rangle$, saadaanko näin sama tulos? Toisin sanoen, jos

$$(a, b) \sim (a', b') \text{ ja } (c, d) \sim (c', d'),$$

niin päätekö

$$\langle a + c, b + d \rangle = \langle a' + c', b' + d' \rangle?$$

Jos vastaus on kielteinen, ei laskutoimitusta voi määritellä näin. Tarkistetaan siis, että yhteenlaskun lopputulos ei riipu edustajien valinnasta.
Oletetaan, että $(a, b) \sim (a', b')$ ja $(c, d) \sim (c', d')$. Tällöin $a + b' = a' + b$ ja $c + d' = c' + d$, joten

$$(a+c)+(b'+d') = (a+b')+(c+d') = (a'+b)+(c'+d) = (a'+c')+(b+d).$$

Tästä puolestaan seuraa, että $(a + c, b + d) = (a' + c', b' + d')$. Kaavalla 83 määritelty laskutoimitus + on siis olemassa.

**Propositio 84.** *Yhteenlasku + joukossa $\mathbb{Z}$ toteuttaa seuraavia ominaisuuksia.*

*(i)* $x + y = y + x$ *kaikilla* $x, y \in \mathbb{Z}$.

*(ii)* $(x + y) + z = x + (y + z)$ *kaikilla* $x, y, z \in \mathbb{Z}$.

*(iii) Alkio* $\langle 0, 0 \rangle$ *on yhteenlaskun neutraalialkio, toisin sanoen kaikilla* $x \in \mathbb{Z}$ *pätee*

$$x + \langle 0, 0 \rangle = \langle 0, 0 \rangle + x = x.$$

*Lisäksi* $\langle 0, 0 \rangle$ *on ainoa alkio, jolla on tämä ominaisuus.*

*(iv) Jokaisella* $x \in \mathbb{Z}$ *on olemassa yksikäsitteinen vasta-alkio* $-x$ *eli sellainen kokonaisluku, jolle pätee*

$$x + (-x) = (-x) + x = \langle 0, 0 \rangle.$$

*Jos* $x = \langle a, b \rangle$, *niin* $-x = \langle b, a \rangle$.

*Todistus.* Valitaan kokonaisluvuille $x, y \in \mathbb{Z}$ edustajia eli merkitään $x = \langle a, b \rangle$, $y = \langle c, d \rangle$.
(i) Koska luonnollisten lukujen yhteenlasku on vaihdannainen (Lemma 74), saadaan

$$x+y = \langle a, b \rangle + \langle c, d \rangle = \langle a+c, b+d \rangle = \langle c+a, d+b \rangle = \langle c, d \rangle + \langle a, b \rangle = y+x.$$

(ii) Todistetaan samalla tavalla kuin (i) (HT).
(iii) Seuraa siitä, että 0 on neutraalialkio luonnollisten lukujen yhteenlaskun suhteen,

$$x + 0 = \langle a, b \rangle + \langle 0, 0 \rangle = \langle a + 0, b + 0 \rangle = x,$$

ja toinen yhtälö osoitetaan samalla tavalla tai vetoamalla vaihdannaisuuteen (ominaisuus (i)).
Neutraalialkion yksikäsitteisyys osoitetaan samalla tavalla kuin reaalilukujen alkion 0 yksikäsitteisyys (vrt. Lemma 2).
(iv) Vasta-alkion yksikäsitteisyys osoitetaan samalla tavalla kuin reaalilukujen vasta-alkion yksikäsitteisyys (vrt. Lemma 3). Olemassaolo nähdään seuraavasti. Olkoon $x = \langle a, b\rangle$ kuten yllä, ja olkoon $y = \langle b, a\rangle$. Osoitetaan, että $x + y = \langle 0, 0\rangle$.
Määritelmän mukaan

$$x + y = \langle a + b, b + a\rangle = \langle c, c\rangle,$$

missä $c = a + b = b + a$. Koska $c + 0 = 0 + c$, parit $(c, c)$ ja $(0, 0)$ ovat ekvivalentteja relaation $\sim$ suhteen, $(c, c) \sim (0, 0)$. Näin ollen $x + y = \langle 0, 0\rangle$ ja $y + x = x + y = \langle 0, 0\rangle$ vaihdannaisuuden nojalla (tai samantyyppisellä argumentilla). □

Vasta-alkion olemassaolo mahdollistaa vähennyslaskun käyttöönoton. Nimittäin määritellään kokonaisluvuille $x, y \in \mathbb{Z}$ erotuksen $x - y$ kaavalla

$$x - y = x + (-y).$$

Kokonaislukujen joukossa kaikilla lineaarisilla yhtälöillä $x + a = b$, $a, b \in \mathbb{Z}$, $x$ tuntematon, on yksikäsitteinen ratkaisu $x = b - a = b + (-a)$ (tarkista).
Palataan upotukseen $f\colon \mathbb{N} \to \mathbb{Z}$, $f(n) = \langle n, 0\rangle$. Jos haluamme samastaa kokonaisluku $f(n) = \langle n, 0\rangle$ luonnollisen luvun $n$ kanssa, olisi järkevä jos tämän samastuksen jälkeen algebrallinen operaatio yhteenlasku säilyisi samannäköisenä. Tämä on totta seuraavan tuloksen nojalla.

**Lemma 85.** *Kuvaus $f\colon \mathbb{N} \to \mathbb{Z}$, $f(n) = \langle n, 0\rangle$ on injektio, joka säilyttää yhteenlaskun. Toisin sanoen jos $n, m \in \mathbb{N}$, niin*

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

*Todistus.* Injektiivisyys osoitettiin jo aikaisemmin. Kaikilla $n, m \in \mathbb{N}$ pätee

$$f(n) + f(m) = \langle n, 0\rangle + \langle m, 0\rangle = \langle n + m, 0 + 0\rangle = \langle n + m, 0\rangle.$$

□

Tämän tuloksen nojalla samastamme luonnollinen luku $n$ ja kokonaisluku $f(n)$, joten merkitään kokonaisluku $\langle n, 0\rangle$ symbolilla $n$. Huomaa, että näillä merkinnöillä yhteenlaskun neutraalialkio on kokonaisluku 0.

**Lemma 86.** *Jokainen kokonaisluku $x \in \mathbb{Z}$ voidaan esittää muodossa $x = n - m$, missä $n, m \in \mathbb{N}$*[13].
*Tässä siis käytämme eksplisiittisesti sopimusta $n = \langle n, 0\rangle$.*

*Todistus.* Olkoon $x \in \mathbb{Z}$. Tällöin on olemassa $n, m \in \mathbb{N}$ siten, että $x = \langle m, n\rangle$. Yhteenlaskun määritelmästä seuraa, että

$$x = \langle m, n\rangle = \langle n, 0\rangle + \langle 0, m\rangle.$$

Proposition 84 nojalla tiedämme, että $\langle 0, m\rangle = -\langle m, 0\rangle$. Kun sovelletaan tähän lisäksi sopimusta $n = \langle n, 0\rangle$, saadaan

$$x = \langle m, n\rangle = \langle n, 0\rangle - \langle m, 0\rangle = n - m.$$

□

**Kertolasku**.
Kokonaislukujen kertolaskun konstruktio ei ole niin suoraviivainen kuin yhteenlaskun kohdalla. Kahden kokonaisluvun $x = \langle a, b\rangle$ ja $y = \langle c, d\rangle$ tulo $xy$ EI OLE kokonaisluku $\langle ac, bd\rangle$.
Motivoituaksemme oikean määritelmän lähdetään siitä, että kahden luonnollisen luvun tulo kokonaislukuina on oltava tietysti sama kuin niiden tulo luonnollisina lukuina. Lisäksi vaaditaan, että osittelulait

$$(a + b)c = ab + ac, a(b + c) = ab + ac$$

ovat voimassa kaikilla $a, b, c, d \in \mathbb{Z}$. Kuten reaalilukujen tapauksessa (vrt. Luvun 1 tuloksia), helposti nähdään, että osittelulaista väistämättä seuraa, että $0 \cdot a = a \cdot 0 = 0$ kaikilla $a \in \mathbb{Z}$. Tästä puolestaan helposti johdetaan osittelulaki vähennyslaskulle,

$$(a - b)c = ab - ac, a(b - c) = ab - ac.$$

ja tutuu merkkisäännöt $a(-b) = -(ab) = (-a)b$.
Olkoot $a, b \in \mathbb{Z}$ kokonaislukuja. Lemman 86 nojalla on olemassa luonnolliset luvut $n, m, p, q$, siten, että $a = n - m, b = p - q$. Tästä osittelulakien ja merkkisääntöjen nojalla saadaan

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

Näin ollen $ab$ on määriteltävä ekvivalenssiluokkana $\langle np+mq, mp+nq\rangle$. Olemme epäformaalisti johtaneet kertolaskulle kaavan, jonka otamme nyt käyttöön

[13]tällainen esitys ei tietenkään ole yksikäsitteinen!

virallisesti.
Olkoot $a = \langle n, m\rangle, b = \langle p, q\rangle$ kokonaislukuja. Määritellään

$$ab = \langle np + mq, nq + mp\rangle. \tag{87}$$

Ensin pitää taas tarkistaa, että tämä määritelmä on järkevä, eli ei riipu edustajien valinnoista.
Olkoot $a = \langle n', m'\rangle, b = \langle p', q'\rangle$ toiset esitykset. Tällöin luonnollisten lukujen joukossa $\mathbb{N}$ pätee

$$n + m' = n' + m, p + q' = p' + q.$$

Meidän on todistettavaa, että $(np+mq, nq+mp) \sim (n'p'+m'q', n'q'+m'p')$, toisin sanoen pitää näyttää, että yhtälö

$$np + mq + n'q' + m'p' = nq + mp + n'p' + m'q'$$

pätee. Kerrotaan yhtälö $n + m' = n' + m$ ensin luvulla $p$ ja sitten luvulla $q$, jolloin saadaan

$$np + m'p = n'p + mp, nq + m'q = n'q + mq.$$

Näistä seuraa, että

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

Toisaalta

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

Laitamalla nämä yhteen, saadaan

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

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

Supistamalla yhteinen termi $(m'p + n'q)$ (mikä on mahdollista Lemman 74 nojalla), saadaan haluttu yhtälö

$$np + mq + n'q' + m'p' = nq + mp + n'p' + m'q'.$$

Olemme näin ollen näyttäneet, että kaavalla 87 määritelty kokonaislukujen kertolasku on hyvin määritelty.

**Propositio 88.** *Kertolasku joukossa $\mathbb{Z}$ toteuttaa seuraavia ominaisuuksia.*

*(i) $xy = yx$ kaikilla $x, y \in \mathbb{Z}$.*

*(ii)* $(xy)z = x(yz)$ *kaikilla* $x, y, z \in \mathbb{Z}$.

*(iii)* *Alkio* $1 = \langle 1, 0\rangle$ *on kertolaskun neutraalialkio, toisin sanoen kaikilla* $x \in \mathbb{Z}$ *pätee*

$$x \cdot 1 = 1 \cdot = x.$$

*Lisäksi* 1 *on ainoa alkio, jolla on tämä ominaisuus.*

*(iv)* *Osittelulait,kaikilla* $x, y, z \in \mathbb{Z}$ *pätee*

$$(x + y)z = xz + yz, x(y + z) = xy + xz.$$

*(v)* *Supistussääntö - jos* $ac = bc$ *ja* $c \neq 0$, *niin* $a = b$.

*Todistus.* HT (seuraa määritelmästä ja vastaavista luonnollisten lukujen ominaisuuksista). □

Edellisesta propositiosta voidaan johtaa muita tuttuja kertolaskun ominaisuuksia, kuten

$$-(-a) = a,$$

$$a(b - c) = ab - ac, (a - b)c = ab - ac$$

$$a(-b) = (-a)b = -(ab),$$

$$(-a)(-b) = ab,$$

$$(a \pm b)^2 = a^2 \pm 2ab + b^2,$$

$$a^2 - b^2 = (a - b)(a + b).$$

Tässä $2 = 1 + 1$ ja potenssi $a^2$ tarkoittaa luonnollisesti $a \cdot a$.
Yleisemmin kokonaislukujen joukossa voidaan määritellä positiivisia kokonaisia *potenssia*. Nimittäin olkoon $x \in \mathbb{Z}$, $n \in \mathbb{N}$. Potenssi $x^n$ määritellään induktiolla luonnollisen luvun $n$ suhteen seuraavasti,

$$x^0 = 1,$$

$$x^{n+1} = x^n \cdot x.$$

Voidaan helposti osoittaa, että tutut potenssisäännöt

$$x^{n+m} = x^n \cdot x^m,$$

$$(x^n)^m = x^{nm}$$

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

**Järjestys**.
Kokonaislukujen välillä voidaan määritellä järjestysrelaation $\leq$, joka on luonnollisten lukujen järjestysrelaation $\leq$ yleistys. Olkoot $x, y \in \mathbb{Z}$ ja esitetään kuten yleensä $x = n - m, y = p - q$, missä $m, n, p, q \in \mathbb{N}$. Jos haluamme, että kokonaislukujen järjestys toteuttaa tuttuja ominaisuuksia, $x \leq y$ eli

$$n - m \leq p - q$$

pitäisi olla yhtäpitävä ehdon $n + q \leq p + m$ kanssa. Koska luonnollisille luvuille $n + q$ ja $p + m$ järjestysrelaatio on määritelty, voidaan ottaa tämä ehto määritelmäksi.
Näin ollen olkoot $a = \langle n, m\rangle, b = \langle p, q\rangle$ kokonaislukuja. Sanotaan, että $a \leq b$, "$a$ on pienempi tai yhtä suuri kuin $b$" jos $n + q \leq p + m$ luonnollisten lukujen joukossa (missä $\leq$ tarkoittaa luonnollisten lukujen välistä järjestysrelaatiota).

**Propositio 89.** *Relaatio $\leq$ on hyvin määritelty ja on täysi järjestys joukossa $\mathbb{Z}$. Lisäksi kaikilla $a, b, c \in \mathbb{Z}$ pätee seuraavaa.*
*Jos $a \leq b$, niin $a + c \leq b + c$.*
*Jos $a \leq b$ ja $c \geq 0$, niin $ac \leq bc$.*
*Jokaiselle kokonaisluvulle $a \in \mathbb{Z}$ pätee tasan yksi seuraavista ehdoista.*
*$a > 0$ tai $-a > 0$ tai $a = 0$.*

*Todistus.* HT. □

Kokonaisluku $a$ on positiivinen jos ja vain jos $a > 0$. Se on negatiivinen jos $a < 0$. Edellisestä Propositiosta seuraa, että luku on negatiivinen tasan silloin kun se vasta-luku on positiivinen. Lisäksi kahden positiivisen luvun summa tai tulo ovat positiivisia.
Kokonaisluvun $a \in \mathbb{Z}$ *itseisarvo* $|a|$ määritellään

$$|a| = \begin{cases} a, \text{ jos } a \geq 0, \\ -a, \text{ jos } a < 0. \end{cases}$$

Määritelmästä seuraa, että itseisarvo on aina ei-negatiivinen.

Lemmassa 86 osoitimme, että kokonaisluku voidaan esittää (ei yksikäsitteisesti!) muodossa $n - m$, missä $n, m \in \mathbb{N}$. Kuitenkin epäformaalin koulumatematiikan perusteella tiedämme, että kokonaisluvuille on olemassa paljon yksinkertaisempi kuvaus - kokonaislukujen joukko $\mathbb{Z}$ koostuu tasan ei-negatiivisista kokonaisluvuista, eli luonnollisista luvuista ja negatiivisista, jotka ovat luonnollisten lukujen vasta-lukuja. Formuloidaan ja osoitetaan tämä karakterisaatio. Käytetään positiivisten luonnollisten lukujen muodostamalle joukolle merkintää

$$\mathbb{N}_+ = \{n \in \mathbb{N} \mid n > 0\} = \mathbb{N} \setminus \{0\}.$$

**Lemma 90.** *Olkoon $x \in \mathbb{Z}$ kokonaisluku. Tällöin $x \in \mathbb{N}$ jos ja vain jos $x \geq 0$. Lisäksi seuraavista kolmesta ehdosta pätee tasan yksi,*

$$x \in \mathbb{N}_+ \text{ tai } x = 0 \text{ tai } -x \in \mathbb{N}_+.$$

*Todistus.* Lemman 86 nojalla on olemassa esitys $x = n - m$, missä $n, m \in \mathbb{N}$. Joka tapauksessa joukossa $\mathbb{N}$ pätee $m \leq n$ tai $n \leq m$. Jos $m \leq n$, Lemman 76 nojalla on olemassa $k \in \mathbb{N}$ siten, että $n = m + k$. Tällöin $x = (m + k) - m = k \in \mathbb{N}$.
Jos taas $n \leq m$, niin $-x = m - n \in \mathbb{N}$ juuri todistetun nojalla, sillä $n \leq m$.

Olemme näyttäneet, että jokaiselle kokonaisluvulle $x$ pätee joko $x \in \mathbb{N}$ tai $-x \in \mathbb{N}$. Lisäksi jos $x \neq 0$, niin myös $-x \neq 0$, joten joko $x \in \mathbb{N}_+$ tai $-x \in \mathbb{N}_+$.
Osoitetaan, että kokonaisluku $x$ on luonnollinen luku, eli $x \in \mathbb{N}$ jos ja vain jos $x \geq 0$. Selvästi jokainen luonnollinen luku $n$ on kokonaislukuna muotoa $\langle n, 0\rangle$, $\in \mathbb{N}$, joten relaation $\leq$ määritelmän nojalla $n \geq 0$ myös $\mathbb{Z}$:n alkiona.
Kääntäen oletetaan, että $x = \langle n, m\rangle \geq 0 = \langle 0, 0\rangle$. Tällöin taas relaation $\leq$ määritelmän nojalla se on yhtäpitävä ehdon $m \leq n$. Kuten edellä nähtiin jo, tässä tapauksessa $x = n - m \in \mathbb{N}$.

Erityisesi ehdot $x \in \mathbb{N}_+$, $x = 0$, $-x \in \mathbb{N}_+$ ovat kokonaisluvulle $x$ yhtäpitäviä ehtojen $x > 0$, $x = 0$ tai $x < 0$. Edellisestä Propositiosta seuraa suoraan, että nämä ehdot ovat toistensa poissulkeavia. □

Pannaan erityisesti merkille, että täysin järjestetty joukko $(\mathbb{Z}, \leq)$ **ei** ole hyvinjärjestetty. Tämä seuraa helposti siitä, että siinä ei edes ole pienintä alkiota (jos $n \in \mathbb{Z}$, niin $n - 1 < n$).
Itse asiassa voidaan osoittaa (HT), että täysin järjestetty joukko $(X, \leq)$ ei ole hyvinjärjestetty jos ja vain jos se sisältää osajoukon $A \subset X$, joka on täysin järjestettynä joukkona isomorfinen joukon $(\mathbb{Z}, \leq)$ kanssa. Tässä mielessä $\mathbb{Z}$ on ikään kuin kanoninen minimaalinen mahdollinen ei-hyvinjärjestetty joukko.

**Luonnollisten lukujen joukko kokonaislukujen joukon osajoukkona**.
Olemme aikaisemmin määritelleet kanonisen upotuksen $f\colon \mathbb{N} \to \mathbb{Z}$, $f(n) = \langle n, 0\rangle$. Tämä upotus osoitettiin injektioksi, minkä seurauksena sovittiin samastaa luonnollinen luku $n \in \mathbb{N}$ ja kokonaisluku $\langle n, 0\rangle$. Huomaa, että injektivisyys tarvitaan varmistamaan, että näin kaksi erilaista luonnollista lukua eivät samastu samaksi kokonaisluvuksi.
Tämä samastuksen myötä voimme ajatella luonnollisten lukujen joukko $\mathbb{N}$

kokonaislukujen joukon $\mathbb{Z}$ osajoukkona, $\mathbb{N} \to \mathbb{Z}$. Lisäksi $N$:ssä ja $f(\mathbb{N})$ on aivan samanlainen algebrallinen ja järjestys-struktuuri. Aikaisemmin tämä osoitettiin vain yhteenlaskulle, joten käydään läpi yleinen tulos.

**Lemma 91.** *Kuvaus $f\colon \mathbb{N} \to \mathbb{Z}$, $f(n) = \langle n, 0\rangle$ on injektio, joka säilyttää yhteen-ja kertolaskun, sekä järjestyksen. Tarkemmin kaikilla $n, m \in \mathbb{N}$ pätee*

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

$$f(nm) = f(n)f(m).$$

*Lisäksi, jos $n \leq m$, niin $f(n) \leq f(m)$.*

*Todistus.* Injektivisisyystä ja kaavaa $f(n+m) = f(n) + f(m)$ osoitettiin jo aikaisemmin. Muut väitteet seuraavat samalla tavalla suoraan määritelmistä (tarkista!). □

**Jaollisuusteoria joukossa $\mathbb{Z}$.**
Olkoot $a, b \in \mathbb{Z}$ kokonaislukuja. Sanomme, että $a$ on $b$:n *tekijä*, jos on olemassa kokonaisluku $c$ jolle $b = ac$. Tällöin merkitään $a|b$ ja sanotaan myös, että $b$ on jaollinen $a$:llä.
Relaatio $|$ kokonaislukujen välillä on refleksiivinen ($a|a$ kaikilla $a \in \mathbb{Z}$) ja transitiivinen (jos $a$ on $b$:n tekijä ja $b$ on $c$:n tekijä, niin $a$ on $c$:n tekijä). Se ei kuitenkaan ole antisymmetrinen. Itse asiassa $a|b$ ja $b|a$ pätevät samaan aikaan jos ja vain jos $b = \pm a$ eli $a$ ja $b$ ovat toistensa vasta-lukuja (todistus HT).
Jokaisella kokonaisluvuilla $a$ on aina tekijöinä ainakin luvut $\pm a$ (eli $a$ ja sen vastaluku) sekä luvut $\pm 1$. Jos $a \neq \pm 1$ ja sillä ei ole muita tekijöitä kuin nämä, se sanotaan *alkuluvuksi*[14].
Luku on *parillinen*, jos se on jaollinen luvulla $2 = 1 + 1$. Muuten se on *pariton*.
Luku 2 on ainoa positiivinen parillinen alkuluku.

**Lemma 92. Jakoyhtälö**.
*Olkoot $a, b \in \mathbb{Z}$, $b \neq 0$. Tällöin on olemassa yksikäsitteiset luvut $q, r \in \mathbb{Z}$ siten, että*

$$a = qb + r$$

*ja $0 \leq r < |b|$.*
*Lukua $r$ sanotaan* jakojäännokseksi.

[14]Yksi syy siihen miksi 1 tai $-1$ ei lasketa alkuluvuiksi on siinä, että muuten aritmetiikan peruslauseen väite ei pätisi

*Todistus.* Tarkastellaan $\mathbb{N}$:n osajoukkoa

$$S = \{a - qb \mid q \in \mathbb{Z}, a - qb \geq 0\}.$$

Jos $a \geq 0$, niin $a \in S$ (valitaan $q = 0$). Jos $a < 0$ ja $b > 0$, niin valitaan $q = a$. Tällöin $a - qb = a(1 - b)$ on kahden ei-positiivisen luvun tulona ei-negatiivinen, joten $a - qb \in S$. Jos $a, b < 0$, niin valitaan $q = -a$.
Jokaisessa tapauksessa nähdään, että $S$ on epätyhjä. Koska $(\mathbb{N}, \leq)$ on hyvinjärjestetty, on olemassa

$$r = \min\{a - qb \mid q \in \mathbb{Z}, a - qb \geq 0\}$$

(huom. symbolilla "min" merkitään tästä lähtien joukon pienintä alkiota, jos se on olemassa). Nyt $a = qb + r$ ja $r \geq 0$, joten riittää osoittaa, että $r < |b|$. Tehdään vasta-oletus - $r \geq |b|$. Tällöin luku $r' = r - |b| = a - bq - |b| = a - (q \pm 1)b$ on ei-negatiivinen, joten kuuluu joukkoon $S$ ja $r' < r$. Tämä on kuitenkin ristiriidassa sen kanssa, että $r$ on pienin $S$:n alkio. Näin ollen $r < |b|$.
Lukujen $q$ ja $r$ yksikäsitteisyyden osoittaminen jätetään harjoitustehtäväksi. □

Olkoot $a, b \in \mathbb{Z} \setminus \{0\}$ nollasta eroavat kokonaisluvut. Kokonaisluku $c$ on lukujen $a$ ja $b$ *suurin yhteinen tekijä* jos

(i) $c|a$ ja $c|b$.

(ii) jos $d \in \mathbb{Z}$ on sellainen, että $d|a$ ja $d|b$, niin $d|c$.

Ehdosta (ii) helposti seuraa, että suurin yhteinen tekijä on merkkiä vaille yksikäsitteinen, eli jos $c$ ja $c'$ ovat molemmat lukujen $a$ ja $b$ suurimmat yhteiset tekijät niin $c' = \pm c$. Tämä nähdään seuraavasti. Oletetaan, että $c$ ja $c'$ molemmat toteuttavat ehtoja (i) ja (ii). Tällöin jos ehto (ii) sovelletaan lukuihin $d = c'$ ja $c$, saadaan $c'|c$. Symmetrian nojalla myös $c'|c$. Kuten yllä todettiin jo, $c|c'$ ja $c'|c$ ovat voimassa samaan aikaan jos ja vain jos $c' = \pm c$. Kääntäen helposti nähdään, että suurimman yhteisen tekijän vasta-luku on myös suurin yhteinen tekijä. Erityisesti, jos suurin yhteinen tekijä on ylipäätään olemassa, se voidaan valita positiivisena. Lukujen $a, b$ yksikäsitteinen positiivinen suurin yhteinen tekijä merkitään $\text{syt}(a, b)$.

**Lemma 93.** *Olkoot $a, b \in \mathbb{Z} \setminus \{0\}$ nollasta eroavat kokonaisluvut. Tällöin* $\text{syt}(a, b)$ *on olemassa. Lisäksi*

$$\text{syt}(a, b) = \min\{ax + by \mid x, y \in \mathbb{Z}, ax + by > 0\}.$$

*Erityisesti* $\text{syt}(a, b)$ *voidaan aina esittää muodossa $ax + by$ joillakin $x, y \in \mathbb{Z}$.*

*Todistus.* Valitsemalla esimerkiksi $x = \pm 1, y = 0$ (missä $x$:n merkki riippuu $a$:n merkistä), nähdään, että luonnollisten lukujen joukon $\mathbb{N}$ osajoukko

$$A = \{ax + by \mid x, y \in \mathbb{Z}, ax + by > 0\}$$

on epätyhjä. Koska $(\mathbb{N}, \leq)$ on hyvin järjestetty, $A$:ssä on olemassa pienin alkio

$$c = \min\{ax + by \mid x, y \in \mathbb{Z}, ax + by > 0\}.$$

Riittää osoittaa, että $c$ on lukujen $a$ ja $b$ suurin yhteinen tekijä.
Ensin osoitetaan, että $c$ on lukujen $a$ ja $b$ tekijä. Jakoyhtälön 92 nojalla on olemassa $q, r \in \mathbb{Z}$ siten, että $a = qc + r$, missä $0 \leq r < c$. Luvun $c$ määritelmän mukaan on olemassa $x, y \in \mathbb{Z}$ siten, että $c = ax + by$. Tällöin $r = a - qc = a - q(ax + bc) = (1 - qx)a + (-qb)c$. Jos $r > 0$, tästä seuraa, että $r \in A$. Mutta toisaalta $r < c$ ja $c$ on pienin $A$:n alkio. Saatu ristiriita osoittaa, että $r = 0$, joten $q = qc$. Tämä puolestaan tarkoittaa, että $c$ on $a$:n tekijä.
Samalla tavalla näytetään, että $c$ on $b$:n tekijä.
Olkoon $d$ yhteinen $a$:n ja $b$:n tekijä, $a = dp$, $b = dq$. Tällöin $c = ax + by = (px + qy)d$, mistä seuraa, että $d|c$. Näin ollen $c = \text{syt}(a, b)$. □

**Huomautus:** Jaollisuudesta olisimme voineet puhua jo luonnollisten lukujen kohdalla, niin kuin perinteisesti joskus tehdäänkin. Ovathan muinaiskreikkalaiset aikoinaan johtaneet samoja tuloksia, vaikka eivät negatiivisia kokonaislukuja käyttäneet. Kuitenkin jaollisuusteorian tuloksien todistaminen helpottuu huomattavasti, jos niitä tarkastelee kokonaislukujen kontekstissa. Nimittäin yllä olemme käyttäneet hyväksi vähennyslaskua. Edellisen lemman tulos ei päde, jos tarkastellaan vain positiivisia lukuja. Esimerkiksi lukujen 2 ja 3 suurin yhteinen tekijä on 1, mutta on selvä, että 1 ei voida esittää muodossa $2x + 3y$, jos vaaditaan $x, y \in \mathbb{N}$. Kokonaislukujen joukossa tämä on jo mahdollista,

$$1 = 2 \cdot (-1) + 3 \cdot 1.$$

Kokonaisluvut $a, b \in \mathbb{Z}$ ovat *keskenään jaottomat* jos $\text{syt}(a, b) = 1$. Edellisen Lemman nojalla $a$ ja $b$ ovat keskenään jaottomia jos ja vain jos $1 = ax + by$ joillakin $x, y \in \mathbb{Z}$.

**Lemma 94.** *Oletetaan, että $a, b, c \in \mathbb{Z}$, $a|bc$ ja $\text{syt}(a, b) = 1$. Tällöin $a|c$.*

*Todistus.* Koska $a$ ja $b$ ovat keskenään jaottomat, on olemassa $x, y \in \mathbb{Z}$ siten, että $1 = ax + by$. Tästä seuraa, että

$$c = c \cdot 1 = c(ax + by) = a(cx) + (bc)y.$$

Mutta oletuksen nojalla $bc = az$ jollakin $z \in \mathbb{Z}$. Näin ollen

$$c = a(cx) + a(zy) = a(cx + zy).$$

Näin ollen $a|c$. □

**Seuraus 95.** *Olkoon $p$ alkuluku ja oletetaan, että $p|a_1a_2 \dots a_k$, missä $a_1, \dots, a_k \in \mathbb{Z}$. Tällöin on olemassa $j = 1, \dots, k$ siten, että $p|a_j$.*

*Todistus.* Edellinen lemma ja induktio $k$:n suhteen. □

**Lause 96. Aritmetiikan peruslause**
*Jokainen nollasta eroava kokonaisluku $n \in \mathbb{Z} \setminus \{0\}$ voidaan esittää muodossa*

$$n = \varepsilon p_1^{k_1} p_2^{k_2} \dots p_r^{k_r},$$

*missä $\varepsilon \in \{1, -1\}$, $p_i$ ovat (erilaisia) positiivisia alkulukuja, $m \in \mathbb{N}$, $k_1, \dots, k_n$ positiivisia kokonaislukuja. Esitys on yksikäsitteinen lukujen $p_1, \dots, p_m$ järjestystä vaille. Toisin sanoen, jos myös*

$$n = \varepsilon' q_1^{l_1} q_2^{l_2} \dots q_r^{l_r},$$

*missä $\varepsilon' \in \{1, -1\}$, $q_i$ ovat (erilaisia) positiivisia alkulukuja, $r \in \mathbb{N}$, $l_1, \dots, k_r$ positiivisia kokonaislukuja, niin $\varepsilon = \varepsilon'$, $m = r$, joukot $\{p_1, \dots, p_m\}$ ja $\{q_1, \dots, q_m\}$ ovat samoja ja samoja alkulukuja vastaavat potenssit $k_i$ ja $l_j$ ovat samoja. (Huom. Tapaus $m = 0$ vastaa arvoa $n = \pm 1$, "tyhjä tulo" on määritelmän mukaan neutraalialkio 1).*

*Todistus.* Väite selvästi riittää osoittaa oletuksella $n > 0$.
Esityksen olemassaolo voidaan osoittaa induktiolla $n$:n suhteen. Riittää osoittaa, että kaikki luvut $n \in \mathbb{N}$, $n \geq 1$ voidaan esittää alkulukujen tulona. Koska $\mathbb{N}_+ = \mathbb{N} \setminus \{0\}$ on hyvinjärjestetty joukko, Lemman 60 nojalla riittää osoittaa, että osajoukko

$$S = \{n \in \mathbb{N} \mid |n \text{ voidaan kirjoittaa alkulukujen tulona } \}$$

on induktiivinen. Olkoon $n \in \mathbb{N}$ ja oletetaan, että kaikille $m < n$ pätee $m \in S$.
Jos $n$ on alkuluku, niin selvästi $n \in S$. Muuten $n$:llä on ainakin yksi aito tekijä $k > 0$, siten, että $k < n$ ja $k \neq 1$. Tällöin $n = kl$, missä $l \in \mathbb{N}$ ja pätee $l < n$. Luvut $k, l$ ovat siis molemmat aidosti pienempi kuin $n$, joten induktio-oletuksen nojalla $k, l \in S$ eli $k$ ja $l$ voidaan esittää alkulukujen tulona. Kertomalla näitä esityksiä keskenään, saadaan luvulle $n = kl$ esitys alkulukujen tulona. Näin ollen $n \in S$, mitä pitikin todistaa.

Osoitetaan esityksen yksikäsitteisyys. Riittää osoittaa, että se on yksikäsitteinen positiivisille kokonaisluvuille, eli että jos

$$p_1^{k_1} p_2^{k_2} \dots p_m^{k_m} = q_1^{l_1} q_2^{l_2} \dots q_r^{l_r},$$

missä $p_1, \dots, p_m, q_1, \dots, q_r$ ovat alkulukuja, niin vasemmalla ja oikealla puolella esiintyvät samat alkuluvut samoilla potensseilla varustettuina.
Yhtälöstä seuraa, että $p_m$ on tulon $q_1^{l_1} q_2^{l_2} \dots q_r^{l_r}$ tekijä. Koska $p_m$ on alkuluku, edellisen seurauksen nojalla on olemassa $q_j$ siten, että $p_m | q_j$. Koska molemmat ovat positiivisia alkulukuja, tästä seuraa, että $p_m = q_j$ (huom., juuri tässä näin ei olisi voitu päätellä, jos 1 laskettaisi alkuluvuksi). Vaihtamalla tarvittaessa indekseja, voidaan olettaa, että $j = r$. Saadaan siis yhtälö

$$(p_1^{k_1} p_2^{k_2} \dots) p_m^{k_m} = (q_1^{l_1} q_2^{l_2} \dots) q_r^{l_r},$$

jossa $p_m = q_r$ esiintyy molemmilla puolella. Koska $p_m$ ei ole nolla, supistussäännön (Lemma 88) nojalla voidaan supistaa se yhtälön molemmilta puolelta , lisäksi niin monta kertaa kuin se esiintyy molemmilla puolella, eli ainakin $\min\{k_m, l_r\}$ kertaa. Jos $k_m \neq l_r$, niin jommallekummalle puolelle jää ainakin yksi tekijä $p_m$, joka ei esiinny toisella puolella. Tämä kuitenkin helposti nähdään mahdottomaksi samalla tavalla kuin edellä edellisen seurauksen avulla. Näin ollen $k_m = l_r$ ja supistuksen jälkeen saadaan yhtälö

$$p_1^{k_1} p_2^{k_2} \dots p_{m-1}^{k_{m-1}} = q_1^{l_1} q_2^{l_2} \dots q_{r-1}^{l_{r-1}},$$

jossa on molemmalla puolella aidosti vähemmän termejä kuin alkuperäisessä tilanteessa. Jatkamalla (induktiolla) saadaan väite. □

**Seuraus 97.** *Karteesinen tulo* $\mathbb{N} \times \mathbb{N}$ *on numeroituva,* $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$.

*Todistus.* Olkoon $N = \mathbb{N} \setminus \{0\}$ positiivisten luonnollisten lukujen joukko. Helposti nähdään, että seuraaja-kuvaus $f \colon \mathbb{N} \to N$, $x \to x^+$ on hyvin määritelty bijektio, joten $N$ on numeroituva.
Koska 2 on ainoa parillinen alkuluku, edellisen Proposition nojalla jokainen $n \in N$ voidaan kirjoittaa muodossa

$$n = 2^k p_1^{k_1} p_2^{k_2} \dots p_m^{k_m},$$

missä $k \in \mathbb{N}$ voi olla nolla (jos 2 ei ole luvun $n$ tekijä) ja $p_1, \dots, p_m$ ovat parittomia alkulukuja. Helposti nähdään, että parittomien lukujen tulo on pariton (miksi? mieti!), joten $n = 2^k l$, missä $k \in \mathbb{N}$ ja $l \in S$, missä $S \subset \mathbb{N}$ on parittomien positiivisten kokonaislukujen joukko. Lisäksi Aritmetiikan Peruslauseesta seuraa, että esitys muodossa $n = 2^k l$, missä $k \in \mathbb{N}$, $l \in S$, on

yksikäsitteinen.
Jakoyhtälöstä ja kokonaislukujen laskutoimitusten ominaisuuksista seuraa, että jokainen $l \in S$ voidaan esittää yksikäsitteisellä tavalla muodossa $l = 2m + 1$, missä $m \in \mathbb{N}$.
Näin ollen kuvaus $f\colon \mathbb{N}\times\mathbb{N} \to N$, $f(k, m) = 2^k(2m+1)$ on bijektio, joten $|\mathbb{N}\times\mathbb{N}| = |N|$. Koska aikaisemmin todettiin jo, että $|N| = |\mathbb{N}|$, väite seuraa. □

Voidaan osoittaa yleisesti, että $|X \times X| = |X|$ kun $X$ on ääretön joukko, mutta tämän yleisemmän väitteen todistus on paljon vaikeampi kuin erikoistapaus $X = \mathbb{N}$.

**Seuraus 98.** *Numeroituva tai äärellinen epätyhjä yhdiste numeroituvista joukoista on numeroituva.*

*Todistus.* Olkoon $A_i$ numeroituva joukko, $i \in I$, missä $I$ on epätyhjä äärellinen tai numeroituva indeksijoukko ja olkoon

$$B = \bigcup_{i\in\mathbb{N}} A_i$$

yhdiste. Koska $A_1 \subset B$, niin $|\mathbb{N}| = |A_1| \leq |B|$.
Valitaan jokaiselle joukolle $A_i$ jokin bijektio $f_i\colon \mathbb{N} \to A_i$. Pannaan erityisesti merkille, että tällaisen valinnan suorittamiseksi tarvitsemme valintaaksioomaa.
Kuvaus $f\colon \mathbb{N} \times I \to B$, $f(i, n) = f_i(n)$ on surjektio (huom, se ei välttämättä ole injektio, sillä erilaiset joukot $A_i$, $A_j$ saattavat leikata). Näin ollen Lemman 36(v) nojalla

$$|\mathbb{N} \times I| \geq |B|.$$

Koska $I$ on äärellinen tai numeroituva, on olemassa injektio $g\colon I \to \mathbb{N}$, mistä seuraa, että on olemassa injektio $h\colon \mathbb{N} \times I \to \mathbb{N} \times \mathbb{N}$, $h(n, i) = (n, g(i))$. Toisaalta, koska $I$ on epätyhjä, on olemassa injektio $\mathbb{N} \times \mathbb{N} \times I$, $n \mapsto (n, i_0)$, missä $i_0 \in I$. Näin ollen tästä ja edellisestä Lemmasta seuraa, että

$$|\mathbb{N}| \leq |\mathbb{N} \times I| \leq |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|.$$

Cantor–Bernstein–Schroederin Lauseen nojalla $|\mathbb{N} \times I| = |\mathbb{N}| = |B|$.

□

Erityisesti kokonaislukujen joukko on numeroituva, sillä se on yhdiste kahdesta numeroituvasta joukosta $\mathbb{N}$ ja $\{-x \mid x \in \mathbb{N}\}$.

**Kokonaisluvut reaalilukujen osajoukkona**.
Olkoon $\mathbb{R}$ (jokin) reaalilukujen joukko. Aikaisemmin näytimme (Esimerkki

73) miten määritellään joukon $\mathbb{R}$ "sisäinen" luonnollisten lukujen joukko $\mathbb{N} \subset \mathbb{R}$.
Palautetaan mieleen miten tämä konstruktio meni. Induktiolla määriteltiin kuvaus $f\colon \mathbb{N} \to \mathbb{R}$, $f(0_{\mathbb{N}}) = f(0_{\mathbb{R}})$, $f(n+1) = f(n) + 1_{\mathbb{R}}$. Sitten osoitettiin, että $f$ on järjestettyjen joukkojen isomorfismi, joten kuvajoukko $f(\mathbb{N}) = \mathbb{R}$ toteuttaa luonnollisten lukujen määritelmän. Tästä syystä voidaan samastaa $n \in \mathbb{N}$ ja $f(n) \in \mathbb{R}$ ja ajatella $\mathbb{N}$ joukon $\mathbb{R}$ osajoukkona.

**Lemma 99.** *Kuvaus $f\colon \mathbb{N} \to \mathbb{R}$ on myös algebrallinen isomorfismi. Toisin sanoen kaikilla $m, n \in \mathbb{N}$ pätee*

$$f(n+m) = f(n) + f(m),$$
$$f(nm) = f(n)f(m).$$

*Lisäksi $f(0) = 0$ ja $f(1) = 1$.*

*Todistus.* Harjoitustehtävä (induktio). □

Seuraavaksi näytetään miten kuvaus $f\colon \mathbb{N} \to \mathbb{R}$ voidaan laajentaa luonnollisella tavalla kokonaislukujen joukkoon. Seurauksena "löydetään" reaalilukujen joukon sisältä myös kokonaislukuja.

Aloitetaan määritelemalla kuvauksen $g\colon \mathbb{N} \times \mathbb{N} \to \mathbb{R}$ kaavalla

$$g(n, m) = f(n) - f(m).$$

Huomaa, että kuvaus on hyvin määritelty, sillä joukossa $\mathbb{R}$ vähennyslasku on määritelty.
Oletetaan, että parit $(n, m), (n', m')$ edustavat tekijäjoukossa $\mathbb{Z}$ saman kokonaisluvun. Tällöin $n + m' = m + n'$. Edellisen lemman avulla saadaan

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

Koska $\mathbb{R}$:ssä päätevät tutut algebralliset säännöt, tästä seuraa, että

$$g(n, m) = f(n) - f(m) = f(n') - f(m') = g(n', m').$$

Kuvaus $g$ siis saa saman arvon jokaisessa ekvivalenssiluokassa. Tästä seuraa, että jos määritelemme kuvauksen $\tilde{g}\colon \mathbb{Z} \to \mathbb{R}$ kaavalla $\tilde{g}(\langle n, m\rangle) = f(n) - f(m)$, tämä kuvaus tulee olemaan hyvin määritelty.

**Lemma 100.** *Kuvaus $\tilde{g}\colon \mathbb{Z} \to \mathbb{R}$ on hyvin määritelty injektio. Lisäksi se säilyttää kaikki struktuurit. Tarkemmin sanottuna olkoot $x, y \in \mathbb{Z}$. Tällöin*
*(i) $\tilde{g}(x + y) = \tilde{g}(x) + \tilde{g}(y)$,*
*(ii) $\tilde{g}(xy) = \tilde{g}(x)\tilde{g}(y)$,*
*(iii) $\tilde{g}(0) = 0$, $\tilde{g}(1) = 1$,*
*(iv) jos $x \leq y$, niin $\tilde{g}(x) \leq \tilde{g}(y)$.*

*Todistus.* Aloitetaan osoittamalla, että $\tilde{g}$ on injektio. Oletetaan, että $\tilde{g}(\langle n, m\rangle) = \tilde{g}(\langle n, m\rangle)$, eli

$$f(n) - f(m) = f(n') - f(m').$$

Tällöin joukossa $\mathbb{R}$ pätee

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

Koska $f$ on injektio, tästä saadaan, että $n + m' = n + m'$. Joukon $\mathbb{Z}$ määritelmän nojalla $\langle n, m\rangle = \langle n', m'\rangle$. Näin ollen $\tilde{g}$ on injektio.

Olkoot $a = \langle n, m\rangle, b = \langle n', m'\rangle \in \mathbb{Z}$. Tällöin $a + b = \langle n + n', m + m'\rangle$ ja $ab = \langle nn' + mm', nm' + n'm\rangle$, joten

$$\tilde{g}(a+b) = f(n+n') - f(m+m') = (f(n)-f(m)) + (f(n')-f(m')) = \tilde{g}(a)+\tilde{g}(b),$$

$$\tilde{g}(ab) = f(nn'+mm') - f(nm'+n'm) = f(n)f(n') + f(m)f(m') - f(n)f(m') - f(n')f(m) =$$

$$= f(n)(f(n')-f(m')) - f(m)(f(n')-f(m')) = (f(n)-f(m))(f(n')-f(m')) = \tilde{g}(a)\tilde{g}(b).$$

Lisäksi, jos $a \leq b$, niin $n + m' \leq n' + m$, joten

$$f(n) + f(m') \leq f(n') + f(m),$$

mistä seuraa, että $\tilde{g}(a) = f(n) - f(m) \leq f(n') - f(m') = \tilde{g}(b)$.

□

Tämä tuloksen nojalla samastamme kokonaisluvun $m \in \mathbb{Z}$ ja vastaavan reaaliluvun $\tilde{g}(m)$. Jokainen reaalilukujoukko sisältää siis oman "kopionsa" kokonaislukujen joukosta $\mathbb{Z}$.

**Kokonaislukujen aksiomaattinen kuvaus.**
Tapaamme määritellä kokonaislukuja poikkeaa tämän kurssin yleisestä filosofiasta siinä mielessä, että konstruoimme suoraan konkreettisen mallin kokonaisluvuille sen sijaan, että antaisimme aksiomaattisen määritelmän joukolle $\mathbb{Z}$ - samalla tavalla kuin olemme tehneet reaalilukujen ja luonnollisten lukujen kohdalla. Tämä johtuu käytännön syistä, tarvitsemme joukkoa $\mathbb{Z}$ (samoin kuin seuraavaksi tarkasteltavaa rationaalilukujen joukkoa $\mathbb{Q}$) vain "välivaiheena" reaalilukujen konstruktioon.
On kuitenkin täysin mahdollisesta kuvata $\mathbb{Z}$ aksiomaattisesti. Tätä varten tarvitsemme *järjestetyn renkaan* käsitettä.

**Rengas** on kolmikko $(R, +, \cdot)$, jossa $R$ on joukko, $+$ ja $\cdot$ ovat laskutoimituksia joukossa $R$ siten, että seuraavat ominaisuudet pätevät

(i) Kaikilla $x, y \in R$ pätee $x + y = y + x$.

(ii) Kaikilla $x, y, z \in R$ pätee $(x + y) + z = x + (y + z)$.

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

(iv) Jokaisella $x \in R$ on olemassa alkio $-x$ siten, että $x + (-x) = 0$.

(v) Kaikilla $x, y, z \in R$ pätee $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

(vi) On olemassa alkio $1 \in R$, siten, että $x \cdot 1 = x = 1 \cdot x$ kaikilla $x \in R$.

(vii) Kaikilla $x, y, z \in \mathbb{R}$ pätevät osittelulait

$$(x + y) \cdot z = x \cdot z + y \cdot z,$$

$$x \cdot (y + z) = xy + xz.$$

Renkaassa siis pätevät samat aksioomat kuin kunnassa (kts. Luku 1), eli reaalilukujen aksioomat A-C seuraavia poikkeuksia lukuun ottamatta.

- Kertolasku ei oleteta vaihdannaiseksi. Jos se kuitenkin on vaihdannainen, rengas sanotaan *vaihdannaiseksi*. Huomaa, että yhteenlasku kuitenkin aina ON vaihdannainen renkaassa. Tyypillinen esimerkki ei-vaihdannaisesta renkaasta on $(n \times n)$-neliömatriisien muodostama joukko.

- Ei vaadita $1 \neq 0$. Tosin *triviaali* rengas jossa $1 = 0$ on varsin tylsä - siinä on tasan yksi alkio. Joskus ominaisuus (vi) jätetään kokonaan väliin. Tällöin yllämääriteltyjä rengasta sanotaan *ykköselliseksi*.

- Käänteisalkion $x^{-1}, x \neq 0$ olemassaoloa ei myöskään vaadita. Huomaa, että vasta-alkioiden olemassaolo edelleenkin oletetaan olevan voimassa.

Rengas on siis yleisempi käsite kuin kunta. Jokainen kunta on (vaihdannainen) rengas, mutta käänteinen väite ei päde. Esimerkiksi kokonaislukujen systeemi $(\mathbb{Z}, +, \cdot)$ on vaihdannainen rengas, joka ei ole kunta.
Kertolaskun supistussääntö, jonka mukaan yhtälö $xy = zy$ implikoi, että $x = z$ tai $y = 0$ ei yleensä ole voimassa renkaissa. Jos vaihdannaisessa renkaassa tämä sääntö on kuitenkin voimassa, rengas sanotaan *kokonaisalueeksi*. Kokonaislukujen joukko $\mathbb{Z}$ on kokonaisalue. Itse asiassa koko termi "kokonaisalue" otettiin aikoinaan käyttöön juuri siitä syystä, että kokonaislukujen joukko toteuttaa kokonaisalueen määritelmän.

Rengas $R$ on *järjestetty* jos siinä on annettu myös täysi järjestysrelaatio $\leq$, joka on yhteensopiva laskutoimitusten suhteen, eli toteuttaa seuraavia ominaisuuksia.

(vii) Olkoot $x, y, z \in \mathbb{R}$ ja $x \leq y$. Tällöin $x + z \leq y + z$.

(viii) Olkoot $x, y, z \in \mathbb{R}$. Tällöin jos $x \leq y$ ja $0 \leq z$, niin $x \cdot z \leq y \cdot z$.

Tämän luvun tulokset osoittavat, että kokonaislukujen joukko $\mathbb{Z}$ on järjestetty rengas.
Voidaan osoittaa (todistus sivutetaan), että järjestetty rengas $R$ on isomorfinen järjestetyn renkaan $\mathbb{Z}$ kanssa jos ja vain jos $R$:n positiivisten alkioiden joukko $R_+$ on hyvinjärjestetty. Tässä "isomorfinen" tarkoittaa, että on olemassa bijektio $f\colon R \to \mathbb{Z}$, joka säilyttää kaikki algebralliset operaatiot sekä järjestyksen,

$$f(x + y) = f(x) + f(y),$$
$$f(xy) = f(x)f(y),$$
$$f(1_R) = 1_{\mathbb{Z}},$$

kaikilla $x, y \in R$ ja lisäksi jos $x \leq y$, niin $f(x) \leq f(y)$. Tämä tulos mahdollista seuraavan aksiomaattisen tavan määritellä kokonaislukuja (isomorfiaa vaille).

Määritellään kokonaislukujen joukko $\mathbb{Z}$ sellaisena järjestettynä renkaana, jonka positiivisten alkioiden joukko on hyvinjärjestetty.

**Tiivistelmä**.

Kokonaislukujen joukko $\mathbb{Z}$ määritellään tekijäjoukkona $(\mathbb{N}\times\mathbb{N})/\sim$, missä ekvivalenssirelaatio $\sim$ on määritelty ehdolla

$$(a, b) \sim (c, d) \text{ jos ja vain jos } a + d = c + b.$$

Alkion $(a, b)$ ekvivalenssiluokkaa merkitään $\langle a, b\rangle$. Yhteenlasku ja kertolasku määritellään formaalisti kaavoilla

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

$$\langle n, m\rangle \cdot \langle p, q\rangle = \langle np + mq, nq + mp\rangle,$$

missä oikealla puolella esiintyvät vastaavasti luonnollisten lukujen yhteen-ja kertolasku.
Järjestysrelaatio $\leq$ määritellään ehdolla

$$\langle n, m\rangle \leq \langle p, q\rangle \text{ jos ja vain jos } n + q \leq p + m,$$

missä oikealla puolella esiintyy luonnollisten lukujen välinen järjestysrelaatio.
Joukko $\mathbb{N}$ upotetaan joukon $\mathbb{Z}$ osajoukoksi kuvauksen $f\colon \mathbb{N} \to \mathbb{Z}$, $f(n) = \langle n, 0\rangle$ välityksellä. Tämä kuvaus on injektio, joka säilyttää yhteen-ja kertolaskutoimituksia sekä järjestyksen. Samastuksen $n = \langle n, 0\rangle$ avulla voimme kirjoittaa jokainen kokonaisluku $z$ kahden luonnollisen luvun erotuksena, $z = n - m, n, m \in \mathbb{N}$.

Systeemi $(\mathbb{Z}, +, \cdot, \leq)$ on järjestetty rengas, eli se toteuttaa seuraavia ominaisuuksia.

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

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

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

A(iv) Jokaisella $x \in \mathbb{Z}$ on olemassa yksikäsitteinen alkio $-x$ siten, että $x + (-x) = 0$.

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

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

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

B(iv) Olkoot $x, y, z \in \mathbb{Z}$, $z \neq 0$. Tällöin jos $xz = yz$, niin $x = z$.

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

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

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

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

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

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

E(ii) Olkoot $x, y, z \in \mathbb{Z}$. Tällöin jos $x \leq y$ ja $0 \leq z$, niin $x \cdot z \leq y \cdot z$.

Jos näitä verrataan reaalilukujen aksioomiin (Määritelmä 1), huomataan, että $\mathbb{Z}$ toteuttaa niistä kaikki, paitsi B(iv), joka asettaa käänteisalkioiden olemassaoloa kaikilla nollasta eroavilla luvuilla. Sen tilalla $\mathbb{Z}$:ssä on voimassa kertolaskun supistussääntö. Tämän säännön avulla seuraavassa luvussa onnistumme konstruoimaan $\mathbb{Z}$:lle laajennuksen $\mathbb{Q}$, jossa aksiooma B(iv) pätee.

Täydellisyysaksiooma F pätee $\mathbb{Z}$:ssä, mutta siitä ei ole meille mitään iloa ja menetämme sen joka tapauksessa konstruktion seuraavassa vaiheessa.

## 5.3 Rationaaliluvut

Luonnollisten lukujen joukon laajennus kokonaislukujen joukoksi liittyy yhteenlaskun "puutteellisiin" ominaisuuksiin joukossa $\mathbb{N}$. Kun näitä puutteita korjataan, saadaan kokonaislukujen joukko $\mathbb{Z}$, jossa kaikki lineaariset yhtälöt $x + a = b$ ratkeavat (jopa yksikäsitteisesti).
Samanlaista yhtälöiden ratkaisemisen ongelmaa on luonnollista tarkastella toisen laskutoimituksen, eli kertolaskun, suhteen. Yhtälöllä $ax = b$, missä $a, b \in \mathbb{Z}$ ei tunnetusti aina ole ratkaisua $\mathbb{Z}$:ssä. Esimerkiksi tällaista ratkaisua ei ole yhtälöllä $2x = 1$.
Pyritään seuraavasti löytämään joukolle $\mathbb{Z}$ laajennuksen, jossa tällaisilla yhtälöillä on olemassa (yksikäsitteinen) ratkaisu. Jos haluamme, että tässä laajennuksessa pätevät tavalliset algebralliset säännöt, aivan kirjaimellisesti tällainen laajennus ei ole mahdollinen. Nimittäin osittelulain olleessa voimassa, pätee aina $0 \cdot x = 0$, joten jos $a = 0$ ja $b \neq 0$, joten yhtälöllä $ax = b$ ei voi olla ratkaisuja. Näin ollen vaaditaan vain, että kyseisessä laajennuksessa kaikilla yhtälöillä $ax = b$, $a \neq 0$ on oltava ratkaisu. Lisäksi sovitaan, että laskutoimitusten vaihdannaisuus, liitännäisyys ja osittelulait pätevät.
Jos jokaisella yhtälöllä $ax = b$, $a \neq 0$ on ratkaisu ($a, b \in \mathbb{Z}$), niin erityisesti jokaisella yhtälöllä $nx = 1$, $n \in \mathbb{Z}, n \neq 0$ on oltava ratkaisu. Tällainen ratkaisu on määritelmän mukaan luvun $n$ käänteisalkio $n^{-1}$. Näin ollen halutun laajennuksen on oltava kunta.
Kääntäen jos laajennus on kunta, niin se riittää, sillä kunnassa yhtälöllä $ax = b, a \neq 0$ on aina yksikäsitteinen ratkaisu $x = a^{-1}b = b/a$.
Koska laajennuksemme sisältää kokonaislukuja ja on kunta, sen pitää sisältää myös kaikki "murtolausekkeet" $m/n = mn^{-1}$, $m, n \in \mathbb{Z}, n \neq 0$. Merkitään myös $m/n = \frac{m}{n}$. Kunnan aksiomeista seuraa (kts. Luku 1), että murtolausekkeille laskutoimitukset toteuttavat "koulusta tuttuja sääntöjä"

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

Lisäksi helposti nähdään, että $m/n = p/q$ jos ja vain jos $mq = np$ joukossa $\mathbb{Z}$.

Nämä tarkastelut kertovat meille miten laajennus $\mathbb{Q}$ pitää konstruoida. Määritellään joukossa $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ relaatio $\sim$ ehdolla

$$(m, n) \sim (p, q) \text{ jos ja vain jos } mq = pn.$$

Osoitetaan, että $\sim$ on ekvivalenssirelaatio.
(1) $mn = mn$, joten $(m, n) \sim (m, n)$ jokaisella alkiolla $(m, n) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$.
(2) Oletetaan, että $(m, n) \sim (p, q)$, eli $mq = pn$. Tällöin $pn = mq$, joten $(p, q) \sim (m, n)$.
(3) Oletetaan, että $(m, n) \sim (p, q)$ ja $(p, q) \sim (r, s)$. Tällöin $mq = pn$ ja $ps = rq$. Tästä seuraa, että

$$(ms)(qs) = (mq)(ss) = (pn)(ss) = (ps)(ns) = (rq)(ns) = (nr)(qs).$$

Koska $q, s \neq 0$, supistussäännön (Propositio 88) nojalla $ms = nr$. Tämä puolestaan tarkoittaa, että $(m, n) \sim (r, s)$.
Koska relaatio $\sim$ on ekvivalenssirelaatio, voidaan muodostaa tekijäjoukko

$$\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z} \setminus \{0\})/\sim .$$

Tämä joukko sanotaan *rationaalilukujen joukoksi*. Sen alkiot ovat ekvivalenssiluokkia $\overline{(m, n)}$ joille käytämme (toistaiseksi) merkintää $[m, n]$. Joukon $\mathbb{Q}$ alkioita sanotaan luonnollisesti *rationaaliluvuiksi*.
Joukossa $\mathbb{Q}$ määritellään laskutoimituksia $+$, $\cdot$ kaavoilla

$$[m, n] + [p, q] = [mq + np][nq],$$

$$[m, n] \cdot [p, q] = [mp, nq].$$

Tässä laskutoimitukset oikealla puolella ovat kokonaislukujen yhteen-ja kertolasku.

**Propositio 101.** *Laskutoimitukset $+$ ja $\cdot$ ovat hyvin määriteltyjä.*
*Kokonaisuus $(\mathbb{Q}, +, \cdot)$ on kunta.*
*Nolla-alkio on $[0, 1]$. Alkion $[m, n]$ vasta-alkio on $[-m, n]$.*
*Kertolaskun neutraalialkio on $[1, 1]$.*
*Alkion $[m, n] \neq [0, 0]$ käänteisalkio on $[n, m]$.*

*Todistus.* Osoitetaan ensin, että laskutoimitukset ovat hyvin määriteltyjä. Ensin pitää huomata, että kokonaislukujen kertolaskun supistussäännön (Lemma 88) nojalla $nq \neq 0$ kun $n \neq 0 \neq q$. Nimittäin oletetaan, että $nq = 0$. Tällöin $nq = n0$, joten supistussäännön nojalla joko $n = 0$ tai $q = 0$. Koska

oletuksemme mukaan kumpikin ehto ei päde, ei myöskään voi päteä $nq = 0$. Erityisesti yhteen-ja kertolaskun määritelmissä oikealla puolella esiintyvä alkio ainakin on todellakin joukon $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ alkion ekvivalenssiluokka.
Seuraavaksi näytetään, että määritelmä ei riipu edustajien valinnoista. Oletetaan, että $[m, n] = [m', n']$, $[p, q] = [p', q']$. Tällöin relaation $\sim$ määritelmän mukaan $mn' = m'n$ ja $pq' = p'q$. Meidän on osoitettavaa, että

$$(mq + np)(n'q') = (m'q' + n'p')(nq)$$

(yhteenlaskun määritelmä) ja

$$(mp)(n'q') = (m'p')(nq).$$

Toinen yhtälö seuraa suoraan laskulla

$$(mp)(n'q') = (mn')(pq') = (m'n)(p'q) = (m'p')(nq),$$

jossa sovelletaan kokonaislukujen kertolaskun vaihdannaisuutta ja liitännäisyyttä.
Ensimmäinen yhtälö onnistuu samantyyppisellä laskulla, jossa lisäksi käytetään hyväksi osittelulakia. Nimittäin kun $mn' = m'n$ ja $pq' = p'q$, pätee

$$(mq + np)(n'q') = (mn')(qq') + (pq')(nn') =$$

$$= (m'n)(qq') + (p'q)(nn') = (m'q' + n'p')(nq).$$

Operaatiot ovat siis hyvinmääriteltyjä.
Yhteenlaskun vaihdannaisuus ja liitännäisyys jätetään harjoitustehtäväksi. Alkio $[0, 1]$ on yhteenlaskun neutraalialkio, koska

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

kaikilla $m, n \in \mathbb{Z}, n \neq 0$. Alkion $[m, n]$ vasta-alkio on $[-m, n]$, koska

$$[m, n] + [-m, n] = [mn + (-m)n, n \cdot n] = [0, k],$$

missä $k = n^2$. Osoitetaan, että jokainen muotoa $[0, k]$ oleva rationaaliluku on nolla-alkio $[0, 1]$. Tämä seuraa suoraan relaation $\sim$ määritelmästä, sillä $0 \cdot k = 0 = 0 \cdot 1$.

Kertolaskun vaihdannaisuus ja liitännäisyys seuraavat helpolla laskulla vastaavista kokonaislukujen ominaisuuksista. Nimittäin kun $n, m, p, q, r, s \in \mathbb{Z}, m, q, s \neq 0$, niin

$$[m, n][p, q] = [mp, nq] = [pm, qn] = [p, q][m, n],$$

$$([m,n][p,q])[r,s] = [mp,nq][r,s] = [(mp)r,(nq)s] =$$
$$= [m(pr),n(qs)] = [m,n][pr,qs] = [m,n]([p,q][r,s]).$$

Alkio $[1,1]$ on kertolaskun neutraali-alkio, sillä

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

Oletetaan, että $[m,n] \neq 0 = [0,1]$. Osoitetaan, että alkio $[n,m]$ on $[m,n]$:n käänteisalkio. Ensin huomataan, että $[n,m]$ on olemassa $\mathbb{Q}$:n alkiona eli $m \neq 0$. Nimittäin, jos olisi $m = 0$, niin olisi myös voimassa $m \cdot 1 = 0 = 0 \cdot n$, mistä seuraisi, että $[m,n] = [0,1]$, vastoin oletusta.
Seuraavaksi lasketaan

$$[m,n][n,m] = [mn,mn].$$

Huomataan, että $mn \cdot 1 = 1 \cdot mn = mn$, joten $[mn,mn] = [1,1]$, joka on kertolaskunneutraalialkio. Näin ollen $[n,m]$ todellakin on alkion $[m,n]$ käänteisalkio.

Jäljellä on osittelulaki. Sen osoittaminen todeksi jätetään harjoitustehtäväksi. □

Samalla tavalla kuin $\mathbb{N}$ aikoinaan upotettiin $\mathbb{Z}$:n osajoukoksi, upotamme kokonaislukujen joukko rationaalilukujen joukkoon. Se tehdään seuraavasti.

**Lemma 102.** *Määritellään kuvaus $g\colon \mathbb{Z} \to \mathbb{Q}$ kaavalla $g(m) = [m,1]$. Tällöin $g$ on injektio. Kaikilla $m,n \in \mathbb{Z}$ pätee*

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

$$g(mn) = g(m)g(n).$$

*Lisäksi $g(0) = 0$ ja $g(1) = 1$.*

*Todistus.* Oletetaan, että $[m,1] = g(m) = g(n) = [n,1]$, $m,n \in \mathbb{Z}$. Tällöin relaation $\sim$ määritelmän mukaan $m = m \cdot 1 = 1 \cdot n$. Näin ollen $g$ on injektio. Olkoot $m,n \in \mathbb{Z}$. Tällöin

$$g(m) + g(n) = [m,1] + [n,1] = [m \cdot 1 + n \cdot 1, 1 \cdot 1] = [m+n,1] = g(m+n),$$

$$g(m)g(n) = [m,1][n,1] = [mn,1] = [mn,1] = g(mn).$$

Lisäksi $g(0) = [0,1]$ on kunnan $\mathbb{Q}$ nolla-alkio (yhteenlaskun neutraalialkio) ja $g(1) = [1,1]$ on vastaavasti kertolaskun neutraalialkio. Tämä osoitettiin edellisessä Propositiossa. □

Edellisen tuloksen nojalla voidaan huoletta samastaa kokonaisluvun $m$ ja rationaaliluvun $[m, 1]$, jolloin $\mathbb{Z}$ voidaan ajatella $\mathbb{Q}$:n osajoukkona. Tämä myös mahdollistaa siirtymistä tutumpaan tapaan esittää rationaalilukuja. Nimittäin palautetaan mieleen, että kunnassa merkinnät $\frac{x}{y}$ ja $x/y$ ovat määriteltyjä kun $y \neq 0$ ja tarkoittavat $xy^{-1}$.

**Lemma 103.** *Jokainen rationaaliluku $q$ voidaan esittää muodossa*

$$q = \frac{m}{n},$$

*$m, n \in \mathbb{Z}, n \neq 0$. Esitys ei ole yksikäsitteinen, vaan*

$$\frac{m}{n} = q = \frac{m'}{n'}$$

*jos ja vain jos $mn' = m'n$.*

*Jokainen rationaaliluku $q$ voidaan esittää yksikäsitteisellä tavalla muodossa*

$$q = \frac{p}{q},$$

*missä* $\text{syt}(p, q) = 1$ *ja* $q > 0$.

*Todistus.* Jokainen rationaaliluku $q$ voidaan esittää ekvivalenssiluokkana $[m, n]$, missä $m, n \in \mathbb{Z}, n \neq 0$. Propositiosta 101 seuraa, että

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

Koska samastamme $[m, 1] = m \in \mathbb{Z}$, $[n, 1] = n \in \mathbb{Z}$, tämä voidaan kirjoittaa muodossa

$$q = mn^{-1} = \frac{m}{n}.$$

Kunnan aksioomeista seuraa, että murtolausekkeille pätee

$$\frac{m}{n} = q = \frac{m'}{n'}$$

jos ja vain jos $mn' = m'n$.

Osoitetaan, että jokainen rationaaliluku $q$ voidaan esittää yksikäsitteisellä tavalla muodossa

$$q = \frac{p}{q},$$

missä $\text{syt}(p, q) = 1$ ja $q > 0$. Otetaan mielivaltainen esitys $q = \frac{m}{n}$. Koska joukossa $\mathbb{Z}$ pätee $m(-n) = (-m)n$, yhtähyvin pätee $q = \frac{-m}{-n}$. Erityisesti

voidaan aina valita $q$:lle esitys $\frac{m}{n}$, jossa $n > 0$.
Olkoon $\text{syt}(m, n) = c > 0$. Lemmasta 93 seuraa, että $c$ on olemassa ja $c = xm + ny$ joillakin $x, y \in \mathbb{Z}$. Lisäksi $c$ on yhteinen tekijä sekä $m$:lle, että $n$:lle, joten $m = cp, n = cq$ joillakin $p, q \in \mathbb{Z}$. Supistamalla $c$ yhtälöstä $c = xm + ny = c(xp + yq)$, saadaan yhtälö $xp + yq = 1$. Koska $p$:n ja $q$:n jokainen tekijä jakaa myös lineaarisen kombinaation $xp + yq$, tästä seuraa, että $\text{syt}(p, q) = 1$. Lisäksi $mq = c(pq) = p(cq) = pn$, joten

$$q = [m, n] = [p, q] = \frac{p}{q}.$$

Esityksen olemassaolo on osoitettu. Se yksikäsitteisyys jaetaan harjoitustehtäväksi. □

Järjestysrelaatio $\leq$ joukossa $\mathbb{Q}$ määritellään seuraavasti. Olkoot $a, b \in \mathbb{Q}$. Edellisen lemman nojalla alkioita $a, b$ voidaan esittää muodoissa

$$a = \frac{m}{n}, b = \frac{p}{q},$$

missä $n, q > 0$. Asetetaan $a \leq b$ jos ja vain jos $mq \leq np$ (joukossa $\mathbb{Z}$).
Järjestysrelaation on hyvinmääritelty. Nimittäin oletetaan, että $a = \frac{m'}{n'}, b = \frac{p'}{q'}$, missä $n', q' > 0$. Tällöin $mn' = m'n$ ja $pq' = p'q$. Oletetaan, että $mq \leq np$. Tällöin, koska $n'$ ja $q'$ ovat molemmat positiivisia, pätee

$$(mq)n'q' \leq (np)n'q'.$$

Yhtälöiden $mn' = m'n$ ja $pq' = p'q$ nojalla tämä on sama asia kuin $m'q'nq \leq n'p'nq$. Tämä epäyhtälö voidaan kirjoittaa muodossa $(n'p' - m'q')nq \geq 0$. Koska $n, q > 0$, tulo $nq$ on myös positiivinen. Koska positiivisen ja negatiivisen kokonaisluvun tulo on aina negatiivinen, $n'p' - m'q'$ ei voi olla negatiivinen. Näin ollen $n'p' - m'q' \geq 0$, eli $m'q' \leq n'p'$. Näin ollen ehto $mq \leq np$ ei riipu edustajien valinnoista.

**Propositio 104.** *Relaatio $\leq$ on täysijärjestys joukossa $\mathbb{Q}$. Lisäksi seuraavat ominaisuudet pätevät.*

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

*(ii) Olkoot $x, y, z \in \mathbb{Q}$. Tällöin jos $x \leq y$ ja $0 \leq z$, niin $x \cdot z \leq y \cdot z$.*

*(iii) Upotus $\mathbb{Z} \to \mathbb{Q}$, $m \mapsto [m, 1]$ säilyttää järjestyksen. Toisin sanoen jos $m \leq n$ joukossa $\mathbb{Z}$, niin sama pätee joukossa $\mathbb{Q}$.*

*Todistus.* HT. □

Rationaalilukujen muodostama systeemi $(\mathbb{Q}, +, \cdot, \leq)$ on siis **järjestetty kunta**, eli sellainen kokonaisuus joka toteuttaa kaikkia reaalilukujen aksioomia, paitsi ehkä täydellisyysaksiooman. Näytetään vielä, että emme todellakaan ole vielä valmiit reaalilukujen joukon etsinnässä näyttämällä että täydellisyysaksiooma ei päde $\mathbb{Q}$:ssä. Lemman 9 nojalla riittää näyttää, että ei ole olemassa $q \in \mathbb{Q}$ jolle $q^2 = 2 = 1 + 1$. Tehdään vasta-oletus, olkoon $q \in \mathbb{Q}$ sellainen, että $q^2 = 2$. Voidaan olettaa, että $q > 0$. Proposition 101 nojalla on olemassa esitys

$$q = \frac{m}{n},$$

jossa $m, n > 0$ ja $\text{syt}(m, n) = 1$. Koska $q^2 = 2$, pätee $m^2 = 2n^2$. Erityisesti joukossa $\mathbb{Z}$ $2|m^2 = m \cdot m$, joten Seurauksen 95 nojalla $2|m$ (koska 2 on alkuluku). Tästä seuraa, että $4|m^2$, joten $m^2 = 4k$ jollakin $k \in \mathbb{Z}, k \neq 0$. Tästä seuraa, että $4k = 2n^2$ $2k = n^2$, mistä Seurauksen 95 nojalla taas $2|n$. Olemme siis päättyneet siihen, että $2|m$ ja $2|n$. Tämä on kuitenkin ristiriidassa ehdon $\text{syt}(m, n) = 1$ kanssa. Näin ollen $q$ ei ole olemassa.

**Lemma 105.** *Rationaalilukujen joukko $\mathbb{Q}$ on numeroituva.*

*Todistus.* Tulos seuraa Seurauksesta 98, sillä $\mathbb{Q}$ on numeroituva yhdiste joukoista $\mathbb{Q}_n$, $n \in \mathbb{N} \setminus \{0\}$,

$$\mathbb{Q}_n = \{\frac{m}{n} \mid m \in \mathbb{Z}\}.$$

Huomaa, että jokainen $\mathbb{Q}_n$ on numeroituva sillä kuvaus $m \to \frac{m}{n}$, $\mathbb{Z} \to \mathbb{Q}_n$ on bijektio ja $\mathbb{Z}$ tiedetään jo oleva numeroituva. □

**Arkhimedeen ehto**.
Rationaalilukujen järjestetty kunta on esimerkiksi niin sanotusta *Arkhimedeen kunnasta*. Havainnollisesti järjestetty kunta $K$ on Arkhimedeen, jos luonnollisten lukujen joukko ei ole ylhäältä rajoitettu $K$:ssä. Jotta tässä määritelmässä olisi järkeä, meidän pitäisi ensin määritellä mikä on "kunnan luonnollisten lukujen joukko". Se tehdään samalla tavalla kuin reaalilukujen tapauksessa. Ensin induktiolla konstruoidaan kuvaus $f\colon \mathbb{N} \to K$ asettamalla

$$f(0) = 0,$$

$$f(n + 1) = f(n) + 1.$$

Tällöin voidaan osoittaa (induktio, samalla tavalla kuin tapauksessa $K = \mathbb{R}$, vrt. Lemmaan 99), että $f$ on injektio joka säilyttää kaikki struktuurin osat, eli kaikilla $n, m \in \mathbb{N}$ pätee

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

$$f(nm) = f(n)f(m).$$

Lisäksi $f(0) = 0$ ja $f(1) = 1$.
Tämän tuloksen nojalla voimme samastaa $\mathbb{N}$ ja $f(\mathbb{N}) \subset K$, jolloin luonnollisten lukujen joukko tulkitaan kunnan $K$ osajoukkona.
Koska tällainen samastuksen jälkeen jokainen $n \in \mathbb{N}$ on kunnan $K$ alkio, jokaisella $a \in K$ on määritelty tulo $na \in K$. Voidaan osoittaa (induktiolla, miten muutenkin), että tällä alkiolla on luonnollinen tulkinta "alkion $a$ monikertana",

$$na = \underbrace{a + a + \ldots + a}_{n \text{ kertaa}}.$$

Koska järjestetty kunta $K$ on erityisesti järjestetty joukko, siinä voidaan puhua osajoukkojen ylärajoista, alarajoista jne. Erityisesti voidaan kysyä onko luonnollisten lukujen joukko $\mathbb{N} \subset K$ rajoitettu ylhäältä joukossa $K$. Jos vastaus tähän kysymykseen on kielteinen, järjestetty kunta $K$ sanotaan *Arkhimedeen kunnaksi*. Nimitys tulee muinaiskreikkalaisten geometrisista pohdinnoista. Nimittäin Arhimedineen-ehto kunnalle voidaan muotoilla myös seuraavasti - olkoot $a, b \in K, a, b > 0$ mitä tahansa positiivisia kunnan lukuja, on olemassa luonnollinen luku $n > 0$ jolle

$$na = \underbrace{a + a + \ldots + a}_{n \text{ kertaa}} > b.$$

Ylimääräiseksi harjoitustehtäväksi jätetään selvittää, miksi tämä muotoilu on ekvivalentti alkuperäisen kanssa. Geometrisesti tämä ehto voidaan tulkita tarkoittavan että olivatpa äärelliset janat $a$ ja $b$ mitkä tahansa, yhdistämällä $a$ itseensä kanssa tarpeeksi monta kertaa saadaan jana joka on pituudeltaan suurempi kuin $b$.
Kunta on siis Arkhimedeen, jos siinä ei ole olemassa alkioita $k$, jolle pätee $n < k$ kaikilla $n \in \mathbb{N}$.

Rationaalilukujen kunnassa $K$ ylimääritelty yleinen upotus $f\colon \mathbb{N} \to \mathbb{Q}$ on määritelty ehdolla $f(n) = [n, 1] = \frac{n}{1}$ eli tämä tapa upottaa luonnollisia lukuja rationaalilukuihin vastaa aikaisempaa ketjua kanonisia upotuksia $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$.
Helposti nähdään, että järjestetty kunta $\mathbb{Q}$ on Arkhimedeen. Nimittäin olkoon $q = \frac{m}{n} \in \mathbb{Q}, n > 0$. Jos $m \leq 0$, niin $q \leq 0$. Muuten $q \leq m < m + 1 \in \mathbb{N}$. Näin ollen $\mathbb{N}$ ei ole ylhäältä rajoitettu $\mathbb{Q}$:ssä.

**Rationaaliluvut reaalilukujen osajoukkona**.
Olkoon $\mathbb{R}$ (jokin) reaalilukujen joukko. Edellisessä luvussa olemme konstruoineet kanonisen upotuksen $\mathbb{Z} \to \mathbb{R}$. Nyt voidaan jatkaa ja laajentaa tätä upo-

tusta rationaalilukujen joukkoon.

Olkoon $\tilde{g}\colon \mathbb{Z} \to \mathbb{R}$ aikaisemmin konstruoitu kanoninen upotus. Olemme näyttäneet, että $\tilde{g}$ on injektio ja säilyttää kaikki laskutoimitukset, sekä järjestyksen. Tarkemmin sanottuna kaikilla $n, m \in \mathbb{Z}$ pätee

$$\tilde{g}(n+m) = \tilde{g}(n) + \tilde{g}(m),$$

$$\tilde{g}(nm) = \tilde{g}(n)\tilde{g}(m).$$

Lisäksi $\tilde{g}(0) = 0$ ja $\tilde{g}(1) = 1$. Voidaan osoittaa (HT), että lueteltut ominaisuudet määrävät kuvauksen $\tilde{g}$ yksikäsitteisesti.

Määritellään kuvaus $h\colon \mathbb{Z} \times \mathbb{Z} \setminus \{0\} \to \mathbb{R}$,

$$h(p,q) = \frac{\tilde{g}(p)}{\tilde{g}(q)}.$$

Koska $q \neq 0$ ja $\tilde{g}$ on injektio, $\tilde{g}(q) \neq \tilde{g}(0) = 0$. Tästä seuraa, että $\mathbb{R}$:ssä luvulla $\tilde{g}(q)$ voidaan jakaa ja $h$ yllä on hyvin määritelty.
Seuraavaksi määritellään $\tilde{h}\colon \mathbb{Q} \to \mathbb{R}$ asettamalla

$$\tilde{h}([p,q]) = \frac{\tilde{g}(p)}{\tilde{g}(q)}, n, q \in \mathbb{Z}, q \neq 0.$$

**Lemma 106.** *Kuvaus $\tilde{h}\colon \mathbb{Q} \to \mathbb{R}$ on hyvin määritelty injektio. Lisäksi se säilyttää kaikki struktuurit. Tarkemmin sanottuna olkoot $x, y \in \mathbb{Q}$. Tällöin*
*(i) $\tilde{h}(x+y) = \tilde{h}(x) + \tilde{h}(y)$,*
*(ii) $\tilde{h}(xy) = \tilde{h}(x)\tilde{h}(y)$,*
*(iii) jos $x \leq y$, niin $\tilde{h}(x) \leq \tilde{h}(y)$.*
*Lisäksi*
*(iv) $\tilde{h}(0) = 0$, $\tilde{h}(1) = 1$,*

*Itse asiassa $\tilde{h}$ on ainoa kuvaus $\mathbb{Q} \to \mathbb{R}$, joka toteuttaa yllä luetteltuja ominaisuuksia (i)-(iv).*

*Todistus.* Olkoon $x = [m,n] = [m,n']$, missä $m, n, m', n' \in \mathbb{Z}, n, n' > 0$. Tällöin $mn' = m'n$, joten

$$\tilde{g}(m)\tilde{g}(n') = \tilde{g}(m')\tilde{g}(n).$$

Tämä yhtälö pätee $\mathbb{R}$:ssä, joka on kunta, joten tästä voidaan päätellä, että

$$h(m,n) = \frac{\tilde{g}(m)}{\tilde{g}(n)} = \frac{\tilde{g}(m')}{\tilde{g}(n')} = h(m',n').$$

Näin ollen $\tilde{h}$ on hyvin määritelty.

Väitteiden (i)-(iv) todistus jätetään harjoitustehtäväksi.

Olkoon $f\colon \mathbb{Q} \to \mathbb{R}$ mikä tahansa kuvaus, joka toteuttaa ominaisuuksia (i)-(iv) eli sellainen jolle kaikilla $x, y \in \mathbb{Q}$ pätee

$$f(x+y) = f(x) + f(y),$$

$$f(xy) = f(x)f(y),$$

, jos $x \leq y$, niin $f(x) \leq f(y)$, ja lisäksi $f(0) = 0$, $\tilde{h}(1) = 1$. Näytetään, että tällöin $f = \tilde{h}$.

Väite osoitetaan vaiheittain. Ensin osoitetaan, että $f(n) = \tilde{h}(n)$ kaikilla $n \in \mathbb{N} \subset \mathbb{Q}$. Tämä voidaan osoittaa induktiolla luvun $n$ suhteen. Alkuaskeleen tapaukset $n = 0$ ja $n = 1$ tulevat suoraan ehdosta (iii). Jos taas oletetaan, että $f(n) = \tilde{h}(n)$, niin

$$f(n+1) = f(n) + f(1) = f(n) + 1 = \tilde{h}(n) + 1 = \tilde{h}(n) + \tilde{h}(1) = \tilde{h}(n+1).$$

Näin ollen $f = \tilde{h}$ ainakin joukossa $\mathbb{N}$.
Seuraavaksi osoitetaan, että $f(x) = \tilde{h}(x)$ kun $x \in \mathbb{Z}$. Lemman 86 nojalla $x = n - m$ joillakin luonnollisilla luvuilla $n, m \in \mathbb{N}$. Laskemalla saadaan

$$f(x) + \tilde{h}(m) = f(x) + f(m) = f(x-m) = f(n) = \tilde{n},$$

mistä seuraa, että $f(x) = \tilde{h}(n) - \tilde{h}(m) = \tilde{h}(x)$, kuvauksen $\tilde{h}$ konstruktion perusteella. Näin ollen $f(x) = \tilde{h}(x)$ kaikilla $x \in \mathbb{Z}$.
Olkoon $q = \frac{n}{m} \in \mathbb{Q}$. Tällöin

$$f(q)\tilde{h}(m) = f(q)f(m) = f(qm) = f(n) = \tilde{h}(n),$$

mistä seuraa

$$f(q) = \frac{\tilde{h}(n)}{\tilde{h}(m)} = \tilde{h}(q),$$

taas kuvauksen $\tilde{h}$ konstruktion perustella. Näin ollen $f = \tilde{h}$, joten kuvauksen $\tilde{h}$ yksikäsitteisyys on osoitettu. □

Edellisen tuloksen nojalla voidaan samastaa joukko $\mathbb{Q}$ ja reaalilukujen osajoukko $\tilde{h}(\mathbb{Q})$ ja ajatella $\mathbb{Q}$ joukon $\mathbb{R}$ osajoukkona, $\mathbb{Q} \subset \mathbb{R}$.
Osoitetaan, että kahden reaaliluvun väliltä aina löytyy rationaaliluku. Sitä varten tarvitsemme ensin tietoa siitä, että $\mathbb{R}$ on itse asiassa Arkhimedeen kunta.

**Lemma 107.** *Luonnollisten lukujen joukko* $\mathbb{N}$ *ei ole rajoitettu ylhäältä* $\mathbb{R}$*:n osajoukkona.*

*Todistus.* Tehdään vasta-oletus - $\mathbb{N}$ on rajoitettu ylhäältä $\mathbb{R}$:n osajoukkona. Tällöin täydellisyysaksiooman nojalla on olemassa $x = \sup \mathbb{N} \in \mathbb{R}$. Koska $y = x - \frac{1}{2} < x$, reaaliluku $y$ ei ole $\mathbb{N}$:n yläraja. Näin ollen löytyy $n \in \mathbb{N}$ siten, että $n > y = x - \frac{1}{2}$. Mutta tällöin $m = n + 1 \in \mathbb{N}$ ja

$$m = n + 1 > y + 1 = x - \frac{1}{2} + 1 = x + \frac{1}{2} > x.$$

Tämä on ristiriita, koska $x$ oli $\mathbb{N}$:n yläraja. Näin ollen $\mathbb{N}$ ei ole ylhäältä rajoitettu $\mathbb{R}$:ssä. □

**Lemma 108.** $\mathbb{Q}$ *on tiheässä* $\mathbb{R}$*:ssä. Tarkemmin sanottuna olkoot* $x, y \in \mathbb{R}$*,* $x < y$*. Tällöin on olemassa* $r \in \mathbb{Q}$ *siten, että* $x < r < y$*.*

*Todistus.* Olkoot $x, y$ reaalilukuja, $x < y$. Haluamme löytää kokonaislukuja $m, n \in \mathbb{Z}$ siten, että

$$x < \frac{m}{n} < y.$$

Voidaan olettaa, että $n > 0$, jolloin epäyhtälö on ekvivalentti epäyhtälön $nx < m < ny$. Tämä taas voidaan ajatella tarkoittavan, että avoin väli $]nx, ny[ \subset \mathbb{R}$ sisältää jonkun kokonaisluvun.
Koska peräkkäisten kokonaislukujen välinen etäisyys on aina 1, intuitiivisesti on selvä, että jokainen $\mathbb{R}$:n avoin väli $]a, b[$ jonka pituus on $> 1$ (eli $b - a > 1$) sisältää ainakin yhden kokonaisluvun. Tämän väitteen tarkka todistus jätetään harjoitustehtäväksi.

Näin ollen riittää vain löytää $n \in \mathbb{N}$ jolle $n(y - x) = ny - nx > 1$ eli $n > 1/(y - x)$. Tällainen löytyy edellisen Lemman nojalla (jos ei löytyisi, luku $1/(y - x)$ olisi $\mathbb{N}$:n yläraja $\mathbb{R}$:ssä). □

Seuraavasta tuloksesta on hyötyä seuraavassa tuloksessa, sillä sen avulla sekä motivoidaan reaalilukujen konstruktiota, että osoitetaan reaalilukujen yksikäsitteisyyttä.

**Lemma 109.** *Olkoon* $\mathbb{R}$ *reaalilukujen joukko ja olkoon* $x \in \mathbb{R}$*. Tällöin*

$$x = \sup\{q \in \mathbb{Q} \mid q < x\} = \{\tilde{h}(q) \mid \tilde{h}(q) < x, q \in \mathbb{Q}\}.$$

*Todistus.* Olkoon $A = \{q \in \mathbb{Q} \mid q < x\}$. Tällöin erityisesti $q \leq x$ kaikilla $q \in A$, joten $A$ on ylhäältä rajoitettu ja $x$ on sen eräs yläraja. Edellisen lemman nojalla on olemassa $q \in \mathbb{Q}$ siten, että $x - 1 < q < x$, jolloin $q \in A$,

joten $A$ on epätyhjä. Erityisesti $\sup A$ on olemassa ja $\sup A \leq x$. Toinen suunta $x \leq \sup A$ osoitetaan vasta-oletuksella. Oletetaan, että $y = \sup A < x$. Edellisen lemman nojalla on olemassa $q \in \mathbb{Q}$ siten, että $y < q < x$. Tällöin $q \in A$, sillä se on rationaaliluku, joka on pienempi kuin $x$, mutta $q > \sup A$, mikä on mahdotonta. Näin ollen ei voi olla $\sup A < x$ ja ollaan valmiit. □

**Rationaalilukujen aksiomatisointi**.
Myös rationaalilukujen muodostama järjestetty kunta voidaan määritellä aksiomaattisesti. Yksi tapa olisi sanoa, että $\mathbb{Q}$ on "pienin" järjestetty kunta siinä mielessä, että se voidaan upottaa mihin tahansa järjestetyn kuntaan. Toinen tapa olisi määritellä sen niin sanottuna kokonaislukujen muodostaman kokonaisalueen *jakokuntana*. Emme me tässä yksityiskohtiin. Täsmällisesti jakokuntia tarkastellaan esimerkiksi Algebran kursseilla.

**Tiivistelmä.**
Rationaalilukujen joukko on numeroituva Arkhimedeen järjestetty kunta. Kaikki sen alkiot voidaan esittää kokonaislukujen osamäärinä muodossa

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

Laskutoimitukset ovat määritelty tutuilla murtolausekkeiden sieventämissäännöillä

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

Rationaalilukujen systeemi toteuttaa seuraavia väiteittä.

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

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

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

A(iv) Jokaisella $x \in \mathbb{Q}$ on olemassa alkio $-x$ siten, että $x + (-x) = 0$.

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

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

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

B(iv) Jokaisella $x \in \mathbb{Q}$, $x \neq 0$ on olemassa alkio $x^{-1}$ siten, että $xx^{-1} = 1$.

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

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

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

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

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

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

E(ii) Olkoot $x, y, z \in \mathbb{Q}$. Tällöin jos $x \leq y$ ja $0 \leq z$, niin $x \cdot z \leq y \cdot z$.

F Jokaisella $q \in \mathbb{Q}$ on olemassa $n \in \mathbb{N}$ siten, että $q < n$.

Huomaa erityisesti, että $\mathbb{Q}$ toteuttaa kaikkia reaalilukujen aksioomia, paitsi täydellisyysaksioomaan. Se korvataan heikomalla Arkhimedeen ehdolla.

Jokainen reaalilukujen joukko $\mathbb{R}$ sisältää ”kopion” rationaalukujen kunnasta $\mathbb{Q}$. Tarkemmin on olemassa yksikäsitteinen upotus $\mathbb{Q} \to \mathbb{R}$ joka säilyttää kaikki laskutoimitukset ja järjestysrelaation.