Johdatus matematiikkaan

Luento 8

Mikko Salo
13.9.2017

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

Sisältö

1. Kertausta

Kurssin suorittaminen

Kurssi suoritetaan lopputentillä (20.9. tai 4.10.). Arvostelu hyväksytty/hylätty. Tentissä on aikaa 4 h, ja hyväksyttyyn suoritukseen tarvitaan 50 % tentin maksimipisteistä.

Tentin materiaali:

- luentokalvot (8 luentoa)
- laskuharjoitustehtävät (4 harjoitusta)

Muistakaa ilmoittautua tenttiin (ja kurssille), to 14.9. klo 16 mennessä!

Muistakaa myös tehdä kurssin palautekysely.

Kurssin rakenne

Kurssin laajuus 3 op ($\approx$ 79 h työskentelyä):

Luennot	18 h
Laskuharjoitukset	8 h
Itsenäinen opiskelu	40 h
Tenttiin valmistautuminen	9 h
Tentti	4 h
Yhteensä	79 h

Itsenäistä opiskelua $\approx$ 4 h / kontaktipäivä!

Matematiikkaa oppii vain laskemalla!

Esimerkki

Matemaattisen päättelyn tunnusmerkkejä ovat: *varmuus* ja *täsmällisyys*. Kuinka "todistat" väitteen:

$$\frac{1}{1\,000} - \frac{1}{1\,001} < \frac{1}{1\,000\,000}?$$

Todistus.

$$\begin{aligned}\frac{1}{1\,000} - \frac{1}{1\,001} &= \frac{1\,001}{1\,000 \cdot 1\,001} - \frac{1\,000}{1\,000 \cdot 1\,001} \\ &= \frac{1\,001 - 1\,000}{1\,001\,000} \\ &= \frac{1}{1\,001\,000} < \frac{1}{1\,000\,000}\end{aligned}$$

koska $1\,001\,000 > 1\,000\,000$. $\square$

Esimerkki

- Todistus on väitteen yksityiskohtainen perustelu. Jokainen askel on niin selvästi perusteltu, että lukija/kuulija voi vakuuttua väitteen paikkansapitävyydestä.

Yleinen väite: jos n on mikä hyvänsä positiivinen kokonaisluku, niin

$$\frac{1}{n} - \frac{1}{n+1} = \frac{n+1}{n(n+1)} - \frac{n}{n(n+1)} = \frac{1}{n(n+1)} < \frac{1}{n^2}$$

sillä $n(n+1) > n^2$.

- Samalle väitteelle voi olla useita erilaisia todistuksia.

Esimerkki

- Todistusta etsitään usein kokeilemalla erilaisia asioita suttupaperilla. Lopuksi varsinainen todistus kirjoitetaan siististi ylös, usein ”käänteisessä järjestyksessä”.

Väite. $\sqrt[8]{8!} < \sqrt[9]{9!}$

Todistus. Koska $1 \cdot 2 \cdot \ldots \cdot 8 < 9^8$, pätee

$$8! < 9^8$$

Kertomalla molemmat puolet luvulla $(8!)^8$ saadaan

$$(8!)^9 < ((8!) \cdot 9)^8 = (9!)^8.$$

Korottamalla molemmat puolet potenssiin $\frac{1}{72}$ saadaan väite

$$\sqrt[8]{8!} < \sqrt[9]{9!}. \qquad \square$$

Matemaattinen teksti

Matematiikka on luonnontieteiden kieli. Opintojen alussa menee yleensä aikaa, ennen kuin uuden kielen käyttö omaksutaan (vrt. kiinan kielen opettelu).

Matemaattisen tekstin osia ovat mm.

- *määritelmät* (lyhyt nimi käsitteelle / symbolille)
- *esimerkit*
- *väitteet* (ilmaisevat yleisen tosiseikan, lause / teoreema / propositio / lemma)
- *todistukset*

Lauseet

Esimerkkilause (Kolmioepäyhtälö)

Kaikille reaaliluvuille a ja b pätee

$$|a+b| \leq |a| + |b|.$$

Esimerkkipropositio

Jos a ja b ovat reaalilukuja, niin pätee

$$2ab \leq a^2 + b^2.$$

Esimerkkilemma

Jokaiselle reaaliluvulle x pätee

$$x \leq |x|.$$

Todistukset

- Todistus on väitteen yksityiskohtainen perustelu. Jokainen askel on niin selvästi perusteltu, että lukija/kuulija voi vakuuttua väitteen paikkansapitävyydestä.

Lemma

Jokaiselle reaaliluvulle x pätee $x \leq |x|$.

Todistus.

Tapaus 1. $x \geq 0$. Tällöin $|x| = x$, ja selvästi

$$x = |x| \leq |x|.$$

Tapaus 2. $x < 0$. Tällöin $|x| = -x$, ja saadaan

$$x < 0 < -x = |x|.$$

Siis väite "$x \leq |x|$" on tosi kaikille reaaliluvuille x. $\square$

Vääräksi osoittaminen

Joskus voimme saada todistettavaksi lauseen, joka ei olekaan totta. Väitteen

Kaikille x pätee ominaisuus $P(x)$

vääräksi osoittamiseksi riittää löytää yksi x, jolle $P(x)$ ei päde. (Tätä kutsutaan vastaesimerkiksi.)

Väite. Kaikille reaaliluvuille x pätee $x^2 - 4x + 4 > 0$.

Yritykset osoittaa väite oikeaksi epäonnistuvat, joten yritetään löytää vastaesimerkki. Jos $x = 2$, niin väite saa muodon $2^2 - 4 \cdot 2 + 4 > 0$, eli $0 > 0$, mikä on epätosi. Vastaesimerkki $x = 2$ kumoaa väitteen.

Ongelmanratkaisua

G. Pólya esitteli kirjassaan "How to Solve It?" (1945) seuraavat askeleet matemaattisen ongelman ratkaisuun:

1. *Ymmärrä ongelma.*
2. *Tee suunnitelma.*
3. *Toteuta suunnitelma.*
4. *Arvioi ratkaisuasi.* Voisiko sitä parantaa?

Loogiset konnektiivit

Matemaattisessa todistamisessa voidaan käyttää logiikasta peräisin olevia symboleita (konnektiiveja):

$\Longrightarrow$	implikaationuoli, ”’seuraa”
$\Longleftrightarrow$	ekvivalenssinuoli, ”jos ja vain jos”
$\neg$	negaatio, ”ei”

Käytössä ovat myös universaalikvanttori $\forall$ (”kaikille”) ja eksistenssikvanttori $\exists$ (”on olemassa”).

Ylläolevat symbolit on hyvä tietää, kokeessa niitä ei vaadita.

Negaatio

Jokaisella väitelauseella A on vastakohta eli negaatio ($\neg A$). Esimerkiksi:

Väite	Negaatio
$\sqrt{2} \geq 3$	$\sqrt{2} < 3$
$2 \leq \pi \leq 3$	$\pi < 2$ tai $\pi > 3$
Kaikki tiet vievät Roomaan.	Jokin tie ei vie Roomaan.
Jos f on derivoituva, niin f on jatkuva.	On olemassa derivoituva f, joka ei ole jatkuva.

Negaation muodostamista tarvitaan epäsuorassa todistuksessa.

Jos ja vain jos –lauseet

Matematiikassa esiintyy usein ”jos ja vain jos”-lauseita:

Esimerkkilause

Kokonaisluku n on pariton jos ja vain jos n^2 on pariton.

Väite ”A jos ja vain jos B” (merkitään $A \Leftrightarrow B$) tarkoittaa samaa kuin väite ”A:sta seuraa B, ja B:stä seuraa A”.

Jos ja vain jos –väitteessä on kaksi suuntaa (”$A \Rightarrow B$” ja ”$A \Leftarrow B$”). Tällainen väite todistetaan yleensä kahdessa osassa (voidaan merkitä ”$\Rightarrow$” ja ”$\Leftarrow$”).

Suora todistus

Suora todistus etenee vaiheittain suoraan oletuksista väitteeseen.

Väite. Jos luonnollinen luku n on pariton, niin n^2 on pariton.

Todistus.

$$\begin{aligned}
n \text{ pariton} &\implies n = 2k + 1 \text{ jollekin } k \\
&\implies n^2 = (2k+1)^2 \\
&\implies n^2 = (2k)^2 + 2 \cdot 2k \cdot 1 + 1^2 \\
&\implies n^2 = 4k^2 + 4k + 1 \\
&\implies n^2 = 2(2k^2 + 2k) + 1 \\
&\implies n^2 \text{ pariton.} \qquad \square
\end{aligned}$$

Epäsuora todistus

Epäsuora todistus: tehdään vastaväite ja johdetaan ristiriita.

Lause. Jos n on positiivinen kokonaisluku ja n^2 on pariton, niin n on pariton.

Todistus. Oletetaan, että n^2 on pariton. Tehdään *vastaväite* (vastaoletus, antiteesi): n on parillinen. Tällöin pätee

$$n = 2k$$

jollekin kokonaisluvulle k. Lasketaan

$$n^2 = (2k)^2 = 4k^2 = 2(2k^2).$$

Siis n^2 on parillinen. Tämä on *ristiriita* oletuksen, että n^2 on pariton, kanssa. Täten vastaväitteen on pakko olla epätosi. Tämä todistaa lauseen. □

Jaollisuus

Määritelmä

Kokonaisluku n on *jaollinen* positiivisella kokonaisluvulla m, jos

$$n = km$$

jollekin kokonaisluvulle k. Tällöin merkitään $m|n$, ja sanotaan, että luku m on luvun n *tekijä*. Luku $n \geq 2$ on *alkuluku*, jos se on jaollinen ainoastaan luvuilla 1 ja n.

Esimerkki

Luvun 12 tekijät ovat 1, 2, 3, 4, 6, ja 12. Ensimmäiset alkuluvut ovat 2, 3, 5, 7, 11, 13, 17, 19, $\ldots$.

Aritmetiikan peruslause

Jokainen kokonaisluku $n \geq 2$ voidaan kirjoittaa muodossa $n = p_1 p_2 \cdots p_k$, missä $p_1, \ldots, p_k$ ovat alkulukuja.

Rationaaliluvut

Määritelmä

Reaaliluku x on *rationaaliluku*, jos $x = \frac{m}{n}$ joillekin kokonaisluvuille m ja n, missä $n \geq 1$.

(Jos $x = \frac{m}{n}$ on rationaaliluku, aritmetiikan peruslauseen nojalla m (tai $-m$) ja n ovat alkulukujen tuloja. Supistamalla yhteiset tekijät lausekkeesta $\frac{m}{n}$ voidaan aina olettaa, että $x = \frac{k}{\ell}$ missä kokonaisluvuilla k ja ℓ ei ole yhteisiä tekijöitä.)

Määritelmä

Reaaliluku x on *irrationaaliluku*, jos se ei ole rationaaliluku.

Esimerkki

Luvut $\frac{7}{8}$, -2 ja $\frac{1}{100}$ ovat rationaalilukuja. Luvut $\sqrt{2}$ ja π ovat irrationaalilukuja.

$\sqrt{2}$ on irrationaalinen

Lause. $\sqrt{2}$ on irrationaalinen.

Todistus. Tehdään *vastaväite*: $\sqrt{2}$ on rationaaliluku. Tällöin

$$\sqrt{2} = \frac{m}{n}$$

joillekin kokonaisluvuille m ja n, joilla ei ole yhteistä tekijää. Korotetaan toiseen potenssiin:

$$2 = \frac{m^2}{n^2}.$$

Siis $m^2 = 2n^2$. Tästä seuraa että m on parillinen[1], ts. $m = 2k$ jollekin k, ja $2n^2 = m^2 = (2k)^2 = 4k^2$. Tällöin $n^2 = 2k^2$ on parillinen, joten n on parillinen[1]. Siis m ja n ovat parillisia, mikä on *ristiriita*, sillä luvuilla m ja n ei ole yhteistä tekijää. □

[1] Perustele! (Epäsuora todistus tai aritmetiikan peruslause)

Induktiotodistus

Induktio on hyödyllinen periaate, jonka avulla voidaan todistaa väitteitä muotoa

$P(n)$ on tosi kaikille positiivisille kokonaisluvuille n.

Induktiotodistuksessa on kolme vaihetta:

1. **Perusaskel.** Todista väite kun $n = 1$ (ts. todista $P(1)$).
2. **Induktio-oletus.** Oleta väite todeksi tapauksessa $n = k$, missä $k \geq 1$ on mielivaltainen (ts. oleta $P(k)$).
3. **Induktioaskel.** Todista väite tapauksessa $n = k + 1$, kun oletetaan, että väite on tosi tapauksessa $n = k$ (ts. todista $P(k + 1)$).

Vahvassa induktiossa induktio-oletus olettaa väitteen todeksi kaikilla $n \leq k$.

Esimerkki

Väite. Kaikille $n = 1, 2, 3, \ldots$ pätee $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$.

Todistus. Todistetaan väite induktiolla.

1. Perusaskel. Väite pätee kun $n = 1$, sillä $1 = \frac{1(1+1)}{2}$.

2. Induktio-oletus. Oletetaan, että $1 + 2 + \ldots + k = \frac{k(k+1)}{2}$.

3. Induktioaskel. Todistetaan $1 + 2 + \ldots + (k+1) = \frac{(k+1)(k+2)}{2}$.
Induktio-oletuksen nojalla

$$
\begin{aligned}
1 + 2 + \ldots + k + (k+1) &= \frac{k(k+1)}{2} + (k+1) \\
&= \frac{k(k+1) + 2(k+1)}{2} = \frac{(k+1)(k+2)}{2}.
\end{aligned}
$$

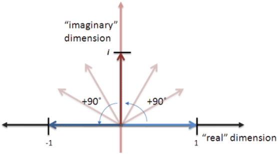
Induktioaskel on valmis. Väite seuraa induktioperiaatteen nojalla. $\square$

Kompleksiluvut

Tarkastellaan tason vektoreita (a, b), missä a ja b ovat reaalilukuja. Ajatellaan, että x-akseli koostuu reaaliluvuista, ja y-akseli koostuu "kuvitteellisista luvuista" (imaginääriluvuista).

Halutaan asettaa tason vektoreille uusi laskutoimitus, ns. kertolasku, jolle pätee

$$(0, 1) \cdot (0, 1) = (-1, 0).$$



Koska x-akseli koostuu reaaliluvuista, tämä tarkoittaisi sitä, että vektori $(0, 1)$ vastaa lukua $\sqrt{-1}$ (sen neliö on -1).

Tämän uuden laskutoimituksen ansiosta tason vektoreita voi ajatella kompleksilukuina.

Kompleksiluvut

Käytännössä kompleksilukuja ajatellaan olioina

$$z = a + ib, \qquad a,\ b \text{ reaalilukuja.}$$

Tässä i on ns. imaginääriyksikkö (vastaa vektoria $(0, 1)$). Yhteenlasku tapahtuu kuten tason vektoreilla:

$$(a + ib) + (c + id) = (a + c) + i(b + d).$$

Kertolaskua varten riittää tietää kaava $i^2 = -1$. Jos tämän muistaa, niin kompleksilukuja voi kertoa niin kuin reaalilukuja:

$$(a+ib)(c+id) = ac+a(id)+(ib)c+(ib)(id) = ac-bd+i(ad+bc)$$

Määritelmä takaa, että tämä on mahdollista (ja että yhteen- ja kertolaskussa termien järjestyksellä ei ole väliä tms).

Esimerkkejä

Pätee $i^2 = -1$, $i^3 = i^2 \cdot i = -i$, $i^4 = i^2 \cdot i^2 = 1$. Lisäksi

$$(3+2i)+(4-3i) = (3+4)+(2-3)i = 7-i$$

ja

$$(3+2i)(4-3i) = 3 \cdot 4 - (2 \cdot (-3)) + i(2 \cdot 4 - 3 \cdot 3) = 18 - i.$$

Toisen asteen yhtälö

Lause

Olkoot a, b, c reaalilukuja ja $a \neq 0$. Yhtälön $az^2 + bz + c = 0$ (kompleksiluku)ratkaisut ovat

$$z = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \qquad \text{jos } b^2 - 4ac \geq 0,$$

$$z = \frac{-b \pm i\sqrt{4ac - b^2}}{2a} \qquad \text{jos } b^2 - 4ac < 0.$$

Esimerkki

Yhtälön $z^2 + 9 = 0$ ratkaisut ovat $z = \pm 3i$.

Jakolasku

Kompleksiluvuille voidaan määritellä yhteen- ja kertolaskun lisäksi jakolasku. Jos $z = a + ib$, käänteisluku $\frac{1}{z}$ on

$$\frac{1}{z} = \frac{1}{a+ib} = \frac{a-ib}{(a+ib)(a-ib)} = \frac{a-ib}{a^2+b^2}.$$

Jos z, w ovat kompleksilukuja ja $w \neq 0$, niin $\frac{z}{w} = z \cdot \frac{1}{w}$.

Esimerkkejä.

(a) $\frac{1}{3+4i} = \frac{3-4i}{(3+4i)(3-4i)} = \frac{3-4i}{3^2+4^2} = \frac{3}{25} - \frac{4}{25}i.$

(b) $\frac{2-5i}{3+4i} = (2-5i)\frac{1}{3+4i} = (2-5i)(\frac{3}{25} - \frac{4}{25}i) = -\frac{14}{25} - \frac{23}{25}i.$

Kertolasku

Jokainen kompleksiluku z on muotoa $z = r(\cos\alpha + i\sin\alpha)$ missä $r = |z|$ ja α on ns. suuntakulma (argumentti). Saadaan:

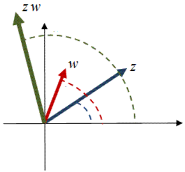
Lause. Kompleksilukujen z ja w tulo on

$$zw = rs(\cos(\alpha+\beta) + i\sin(\alpha+\beta))$$

kun $z = r(\cos\alpha + i\sin\alpha)$ ja $w = s(\cos\beta + i\sin\beta)$.

Siis kompleksilukujen z ja w kertolaskussa

- pituudet r ja s kerrotaan keskenään
- suuntakulmat α ja β lasketaan yhteen



Erityisesti i vastaa suuntakulmaa 90°, joten

i:llä kertominen $= 90^\circ$ kierto vastapäivään.

Joukko-oppia

Joukko on kokoelma objekteja (alkioita, jäseniä). Merkintöjä:

$x \in A$	(x kuuluu joukkoon A)
$x \notin A$	(x ei kuulu joukkoon A)
$A \subset B$	(joukko A on joukon B osajoukko, myös $A \subseteq B$)
$A \not\subset B$	(joukko A ei ole joukon B osajoukko)
$A = B$	(A ja B ovat samat joukot)
$\emptyset$	(tyhjä joukko)

A on B:n osajoukko jos jokainen A:n alkio on myös B:n alkio. Tyhjässä joukossa ei ole yhtään alkiota. Jos A koostuu alkioista x, jotka toteuttavat ehdon $P(x)$, merkitään

$$\begin{aligned} A &= \{x : x \text{ toteuttaa ehdon } P(x)\} \\ &= \{x \mid x \text{ toteuttaa ehdon } P(x)\}. \end{aligned}$$

Lukujoukkoja

$$
\begin{aligned}
\mathbb{N} &= \{1, 2, 3, 4, 5, \ldots\} && \text{(luonnolliset luvut)} \\
\mathbb{Z} &= \{\ldots, -2, -1, 0, 1, 2, \ldots\} && \text{(kokonaisluvut)} \\
\mathbb{Q} &= \{\frac{m}{n} \ : \ m \in \mathbb{Z}, n \in \mathbb{N}\} && \text{(rationaaliluvut)} \\
\mathbb{R} &= \{x \ : \ x \text{ reaaliluku}\} && \text{(reaaliluvut)} \\
\mathbb{C} &= \{a + bi \ : \ a, b \in \mathbb{R}\} && \text{(kompleksiluvut).}
\end{aligned}
$$

Pätee

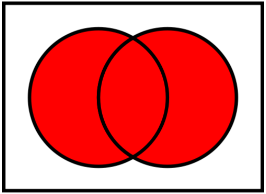
$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Joukko-operaatioita

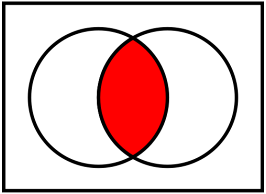
Olkoot A ja B joukkoja. Määritellään

$$
\begin{aligned}
A \cup B &= \{x : x \in A \text{ tai } x \in B\} && \text{(yhdiste)} \\
A \cap B &= \{x : x \in A \text{ ja } x \in B\} && \text{(leikkaus)} \\
B \setminus A &= \{x : x \in B \text{ ja } x \notin A\} && \text{(erotus)}
\end{aligned}
$$

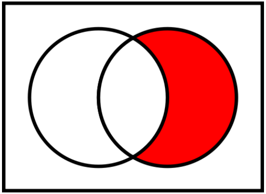
Joukko-operaatioita voi havainnollistaa Venn-diagrammeilla:



$A \cup B$



$A \cap B$



$B \setminus A$

Funktioista

Funktiot ovat kuvauksia yleisten joukkojen välillä.

Määritelmä

Olkoot A ja B epätyhjiä joukkoja. Funktio eli kuvaus $f : A \to B$ on sääntö, joka liittää jokaiseen joukon A alkioon a täsmälleen yhden joukon B alkion $f(a)$. Sanotaan, että

$$f(a) \text{ on funktion } f \text{ arvo pisteessä/alkiossa } a,$$

ja $f(a)$ on alkion a kuva kuvauksessa f (merkitään $a \mapsto f(a)$).

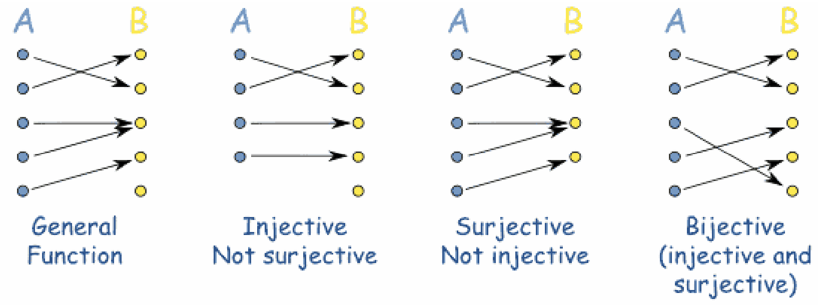
Jos $f : A \to B$ on funktio, joukkoa A sanotaan funktion f määrittelyjoukoksi ja joukkoa B sanotaan maalijoukoksi.

Funktioista

Injektio: kahdella eri alkiolla ei voi olla samaa kuvaa

Surjektio: jokainen maalijoukon alkio on jonkin pisteen kuva

Bijektio: injektio ja surjektio, 1-1 vastaavuus A:n ja B:n välillä

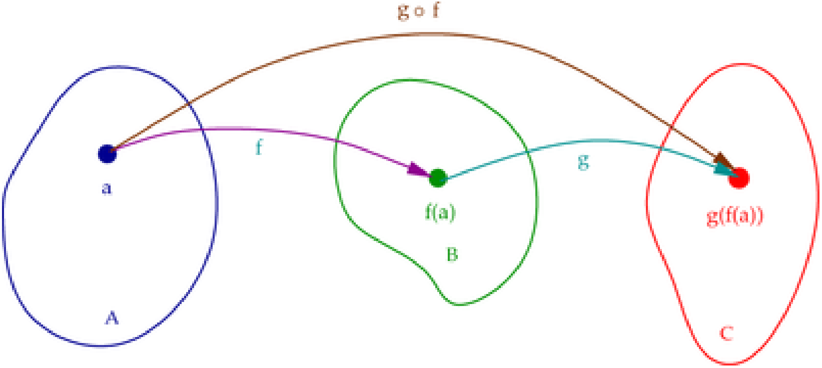


Yhdistetty funktio

Määritelmä

Olkoot $f : A \to B$ ja $g : B \to C$ funktioita. Funktioiden f ja g yhdistetty funktio $g \circ f$ on funktio

$$g \circ f : A \to C, \quad (g \circ f)(a) = g(f(a)).$$



Käänteisfunktio

Jos $f : A \to B$ on bijektio, niin jokaiselle $b \in B$ löytyy täsmälleen yksi $a \in A$, jolle $f(a) = b$. Tämä sääntö määrittelee funktion f käänteisfunktion

$$f^{-1} : B \to A.$$

Siis bijektiolle f voidaan määritellä käänteisfunktio $g = f^{-1}$, ja tämä toteuttaa ehdot

$$g(f(a)) = a \text{ kaikille } a \in A, \quad f(g(b)) = b \text{ kaikille } b \in B.$$

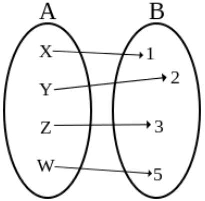
Toisaalta ylläolevat ehdot täyttävä kuvaus g on olemassa jos ja vain jos f on bijektio (miksi?), ja tällöin välttämättä $g = f^{-1}$.

Joukkojen mahtavuus

Määritelmä

Joukot A ja B ovat yhtä mahtavia, merkitään $|A| = |B|$, jos on olemassa jokin bijektio $f : A \to B$.

Muistetaan, että $f : A \to B$ on bijektio jos se on injektio (eri alkioilla on eri kuvat) ja surjektio (jokainen B:n alkio on jonkin A:n alkion kuva). Bijektio antaa siis 1-1 vastaavuuden A:n ja B:n alkioiden välillä.



On tietyssä mielessä luonnollista, että jos A:n ja B:n välillä on bijektio, niin A:ssa ja B:ssa on yhtä monta alkiota.

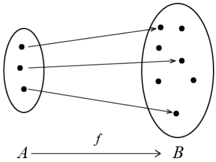
Äärettömät joukot

Yksinkertaisin ääretön joukko on $\mathbb{N} = \{1, 2, 3, \ldots\}$. Nähtiin

$$|\{n \in \mathbb{N} \,:\, n \text{ on parillinen}\}| = |\mathbb{N}|.$$

Määritelmä

- Joukko A on aidosti vähemmän mahtava kuin joukko B, merkitään $|A| < |B|$, jos on olemassa injektio $f : A \to B$ mutta ei ole olemassa bijektiota $A \to B$.
- Joukko A on numeroituvasti ääretön, jos $|A| = |\mathbb{N}|$.
- Joukko A on ylinumeroituva, jos $|\mathbb{N}| < |A|$.



Mahtavuuksien vertailua

Lause

Joukot $\mathbb{N}$, $\mathbb{Z}$ ja $\mathbb{Q}$ ovat numeroituvasti äärettömiä
(ts. $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}|$).

Toiset äärettömyydet ovat suurempia kuin toiset:

Lause (Cantor 1874)

Reaalilukujen joukko on ylinumeroituva (ts. $|\mathbb{N}| < |\mathbb{R}|$).

Todistus.

Epäsuora todistus ja Cantorin diagonaaliargumentti. $\square$