# Johdatus yliopistomatematiikkaan

Lotta Oinonen

1. maaliskuuta 2016

Helsingin yliopisto
Matematiikan ja tilastotieteen laitos

# Sisältö

# 1 Perusasioita joukoista

## 1.1 Merkintöjä

Joukko voidaan määritellä luettelemalla siihen kuuluvat alkiot. Esimerkiksi voidaan merkitä $A = \{-2, -1, 0, 1, 2\}$. Tästä merkinnästä nähdään, mitkä luvut ovat joukon $A$ alkioita. Esimerkiksi luku 1 on joukon $A$ alkio, mikä merkitään symbolikielellä $1 \in A$. Tämä merkintä luetaan ”yksi kuuluu joukkoon $A$”. Toisaalta esimerkiksi luku 4 ei ole joukon $A$ alkio, mikä merkitään symbolikielellä $4 \notin A$. Tämä luetaan ”neljä ei kuulu joukkoon $A$”.

Jos joukko määritellään luettelemalla siihen kuuluvat alkiot, ei järjestyksellä ole merkitystä. Siis esimerkiksi joukot $\{1, 2, 3\}$ ja $\{3, 1, 2\}$ ovat samat. Joukko ei myöskään muutu, vaikka sama alkio toistetaan useampaan kertaan: esimerkiksi joukot $\{1, 2, 3, 2, 1\}$ ja $\{3, 2, 1\}$ ovat samat.

Monille lukujoukoille on oma symbolinsa. Ne on lueteltu alla taulukossa 1.1. Jossain yhteyksissä luku nolla lasketaan kuuluvaksi luonnollisten lukujen joukkoon, toisinaan taas ei. Kysymyksessä on siis sopimusasia. Tällä kurssilla sovitaan, että nolla on luonnollinen luku.

| | |
|---|---|
| Luonnolliset luvut | $\mathbb{N} = \{0, 1, 2, \ldots\}$ |
| Kokonaisluvut | $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ |
| Rationaaliluvut | $\mathbb{Q} = \{\, m/n \mid m, n \in \mathbb{Z} \text{ ja } n \neq 0 \,\}$ |
| Reaaliluvut | $\mathbb{R}$ |
| Kompeksiluvut | $\mathbb{C} = \{(a, b) \mid a \in \mathbb{R} \text{ ja } b \in \mathbb{R}\}$ |

Taulukko 1.1: Lukujoukkoja.

Joukon kaikkien alkioiden luetteleminen ei ole aina mahdollista. Esimerkiksi merkinnästä $B = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$ voidaan päätellä, että joukko $B$ muodostuu parillisista kokonaisluvuista. Sama asia voidaan merkitä täsmällisemmin antamalla ehto, joka joukon alkioiden täytyy toteuttaa. Joukko $B$ voidaan ehdon avulla merkitä $B = \{\, m \in \mathbb{Z} \mid m = 2n \text{ missä } n \in \mathbb{Z} \,\}$ tai $B = \{2n \mid n \in \mathbb{Z}\}$.

Myös joukko $A = \{-2, -1, 0, 1, 2\}$ voidaan esittää ehdon avulla: $A = \{z \in \mathbb{Z} \mid -2 \leq z \leq 2\,\}$. Muitakin mahdollisuuksia on, esimerkiksi $A = \{z \in \mathbb{Z} : |z| \leq 2\,\}$.

Kun joukko määritellään ehdon avulla, pystyviivan vasemmalla puolella kerrotaan, minkä tyyppisiä joukon alkiot ovat. Esimerkiksi merkinnästä $B = \{\, m \in \mathbb{Z} \mid m = 2n \text{ missä } n \in \mathbb{Z} \,\}$ nähdään, että joukon $B$ alkiot ovat tyypiltään kokonaislukuja. Pystyviivan oikealle puolelle kirjoitetaan ehto, joka alkioilta vaaditaan. Joukon $B = \{\, m \in \mathbb{Z} \mid m = 2n \text{ missä } n \in \mathbb{Z} \,\}$ tapauksessa vaaditaan, että luvut ovat parillisia. Merkinnät ovat siis aina muotoa

$$\{\text{alkioiden tyyppi} \mid \text{ehto, joka alkioilta vaaditaan}\}.$$

Joskus pystyviivan tilalla saatetaan käyttää kaksoispistettä. Tätä merkintätapaa näkee vanhoissa kirjoissa sekä tilanteissa, joissa pystyviiva voisi sekoittua esimerkiksi itseisarvomerkkeihin.

## 1.2 Yhdiste, leikkaus ja erotus

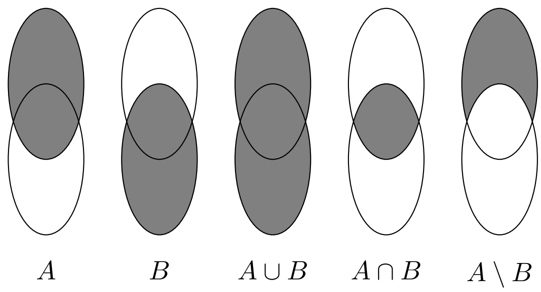
Joukoista voidaan muodostaa uusia joukkoja erilaisten joukko-operaatioiden avulla. Näistä yleisimmät on määritelty alla, ja niitä on havainnollistettu niin sanotuilla Vennin kaavioilla kuvassa 1.1.

**Määritelmä 1.2.1.** Oletetaan, että $A$ ja $B$ ovat joukkoja. Joukkojen $A$ ja $B$

- *yhdiste* on joukko $A \cup B = \{\, x \mid x \in A \text{ tai } x \in B \,\}$,
- *leikkaus* on joukko $A \cap B = \{\, x \mid x \in A \text{ ja } x \in B \,\}$,
- *erotus* on joukko $A \smallsetminus B = \{\, x \mid x \in A \text{ ja } x \notin B \,\}$.

Merkintä $A \smallsetminus B$ luetaan ”$A$ pois $B$”.

Huomaa, että matematiikan ”tai” ei ole poissulkeva: ehto $x \in A$ tai $x \in B$ sallii myös tapauksen, jossa alkio kuuuu sekä joukkoon $A$ että joukkoon $B$. Siten yhdisteen $A \cup B$ muodostavat kaikki alkiot, jotka kuuluvat ainakin toiseen joukoista $A$ ja $B$.




Kuva 1.1: Joukot $A$ ja $B$ sekä niiden yhdiste, leikkaus ja erotus tummennettuna.

**Esimerkki 1.2.2.** Merkitään $A = \{0, 2, 4\}$ ja $B = \{1, 2, 3\}$. Joukkojen $A$ ja $B$ yhdiste on $A \cup B = \{0, 1, 2, 3, 4\}$, leikkaus on $A \cap B = \{2\}$ ja erotus on $A \smallsetminus B = \{0, 4\}$. Joukkojen $B$ ja $A$ erotus on $B \smallsetminus A = \{1, 3\}$.

## 1.3 Tyhjä joukko

Joukko-operaatioiden tuloksena voi joskus olla joukko, johon ei kuulu yhtään alkiota. Esimerkiksi joukoilla $A = \{1, 2\}$ ja $B = \{3, 4\}$ ei ole yhteisiä alkiota, joten niiden leikkaus $A \cap B$ on joukko, jossa ei ole yhtään alkiota. Tällaista joukkoa sanotaan tyhjäksi joukoksi.

**Määritelmä 1.3.1.** *Tyhjä joukko* tarkoittaa joukkoa, jossa ei ole yhtään alkiota. Tyhjää joukkoa merkitään symbolilla $\emptyset$ ja joskus myös merkinnällä $\{\ \}$.

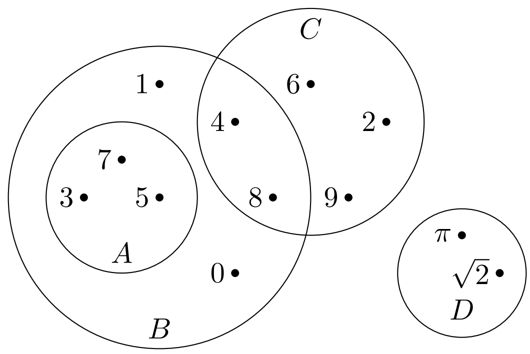
Edellä mainittujen joukkojen $A = \{1, 2\}$ ja $B = \{3, 4\}$ leikkaus on tyhjä joukko: $A \cap B = \emptyset$.

## 1.4 Osajoukko

Jos kahdella joukolla ei ole yhteisiä alkiota, eli niiden leikkaus on tyhjä joukko, sanotaan, että kyseiset joukot ovat *erilliset*. Esimerkiksi kuvan 1.2 joukot $A = \{3, 5, 7\}$ ja $C = \{2, 4, 6, 8, 9\}$ ovat erilliset, samoin joukot $B$ ja $D$.

Jos kahdella joukolla on ainakin yksi yhteinen alkio, eli niiden leikkaus ei ole tyhjä joukko, sanotaan, että joukot *kohtaavat* toisensa. Esimerkiksi kuvan 1.2 joukko $C = \{2, 4, 6, 8, 9\}$ kohtaa joukon $B = \{1, 3, 4, 5, 7, 8, 0\}$, sillä $C \cap B = \{4, 8\} \neq \emptyset$. Joukossa $C$ on kuitenkin myös sellaisia alkioita, jotka eivät kuulu joukkoon $B$, esimerkiksi alkio 2.

Myös joukko $A = \{3, 5, 7\}$ kohtaa joukon $B = \{1, 3, 4, 5, 7, 8, 0\}$, koska niiden leikkaus ei ole tyhjä. Huomataan lisäksi, että joukon $A$ jokainen alkio kuuluu joukkoon $B$. Tällöin sanotaan, että $A$ on joukon $B$ *osajoukko*.




Kuva 1.2: Joukko $A$ on joukon $B$ osajoukko.

**Määritelmä 1.4.1.** Joukko $A$ on joukon $B$ *osajoukko*, jos kaikilla $x \in A$ pätee myös $x \in B$. Tällöin sanotaan, että $A$ *sisältyy* joukkoon $B$, ja merkitään $A \subset B$. Merkintä $A \not\subset B$ tarkoittaa, että $A$ ei ole joukon $B$ osajoukko.

Kun osoitetaan joukkoa $A$ joukon $B$ osajoukoksi, pitää varmistua siitä, että *jokainen* joukon $A$ alkioista on myös joukon $B$ alkio. Toisaalta, jos osoitetaan, että joukko $A$ ei ole joukon $B$ osajoukko, riittää löytää joukosta $A$ *yksi* sellainen alkio, joka ei kuulu joukkoon $B$.

**Esimerkki 1.4.2.** Merkitään $A = \{-3, 0, 3\}$. Huomataan, että joukko $A$ on rationaalilukujen joukon osajoukko eli $A \subset \mathbb{Q}$, sillä jokainen joukon $A$ alkioista voidaan kirjoittaa murtolukumuodossa: $-3 = -3/1$, $0 = 0/1$ ja $3 = 3/1$. Siis $-3 \in \mathbb{Q}$, $0 \in \mathbb{Q}$ ja $3 \in \mathbb{Q}$.

Toisaalta joukko $A$ ei ole luonnollisten lukujen joukon osajoukko eli $A \not\subset \mathbb{N}$, sillä joukon $A$ alkio $-3$ ei ole luonnollinen luku: $-3 \in A$ mutta $-3 \notin \mathbb{N}$.

**Esimerkki 1.4.3.** Olkoon $A = \{\, x \in \mathbb{R} \mid x^4 - 5x^3 - x^2 + 5x = 0 \,\}$. Näytetään, että $\{5, -1\} \subset A$.

Joukon $A$ määritelmästä nähdään, että sen muodostavat tietynlaiset reaaliluvut. Luvut 5 ja $-1$ ovat kumpikin reaalilukuja. Lisäksi sijoittamalla havaitaan, että ne toteuttavat joukon $A$ ehdon: $5^4 - 5 \cdot 5^3 - 5^2 + 5 \cdot 5 = 5^4 - 5^4 - 5^2 + 5^2 = 0$ ja

$$(-1)^4 - 5 \cdot (-1)^3 - (-1)^2 + 5 \cdot (-1) = 1 + 5 - 1 - 5 = 0\,.$$

Siten $5 \in A$ ja $-1 \in A$. Näin ollen $\{5, -1\} \subset A$.

---

Edellisessä esimerkissä osoitettiin joukko $\{5, -1\}$ toisen joukon osajoukoksi tarkastelemalla joukon $\{5, -1\}$ alkiot yksitellen. Tämä ei kuitenkaan aina ole mahdollista, esimerkiksi jos tarkasteltavassa joukossa on loputtomasti alkioita. Seuraavassa esimerkissä tutustutaan päättelytekniikkaan, jossa tarkasteltavan joukon koolla ei ole merkitystä.

**Esimerkki 1.4.4.** Osoita, että $B \subset C$, missä

$$B = \{\, x \in \mathbb{R} \mid \sin 3x = \cos x \,\} \quad \text{ja} \quad C = \{\, x \in \mathbb{R} \mid (\sin 3x - \cos x)(x^2 - 5x) = 0 \,\}.$$

Oletetaan, että $b \in B$ (eli *kuvitellaan*, että $b$ on joukon $B$ alkio). Tällöin alkio $b$ toteuttaa joukon $B$ ehdot, joten sille pätee $b \in \mathbb{R}$ ja $\sin 3b = \cos b$.

Yhtälö $\sin 3b = \cos b$ saadaan muokattua muotoon $\sin 3b - \cos b = 0$. Siitä on etua, kun lähdetään tutkimaan, toteuttaako tarkasteltava alkio $b$ joukon $C$ ehdon. Nimittäin joukon $C$ ehdossa $(\sin 3x - \cos x)(x^2 - 5x) = 0$ esiintyy sopivasti tekijä $(\sin 3x - \cos x)$.

Lasketaan, mitä joukon $C$ ehdossa esiintyvästä lausekkeesta $(\sin 3x - \cos x)(x^2 - 5x)$ tulee, jos siihen sijoitetaan $b$:

$$(\sin 3b - \cos b)(b^2 - 5b) = 0 \cdot (b^2 - 5b) = 0\,.$$

Huomataan, että tulos on nolla, eli alkio $b$ toteuttaa joukon $C$ ehdon. Lisäksi jo aikaisemmin todettiin, että $b \in \mathbb{R}$. Siis $b \in C$.

Tämä päättely toimii *mille tahansa* joukon $B$ alkiolle. Siten voidaan päätellä, että jokainen joukon $B$ alkio kuuluu joukkoon $C$ eli $B \subset C$.

---

Tyhjä joukko $\emptyset$ voidaan osoittaa minkä tahansa joukon osajoukoksi. Ennen kuin teemme sen, palautetaan vielä mieleen, miten osoitetaan, ettei annettu joukko ole toisen joukon osajoukko.

**Esimerkki 1.4.5.** Merkitään $B = \{\, x \in \mathbb{Z} \mid x^2 - x = 0 \,\}$. Näytetään, että $\{1, 2\} \not\subset B$.

Tarkastellaan joukon $\{1, 2\}$ alkiota 2. Havaitaan, että $2^2 - 2 = 4 - 2 = 2 \neq 0$. Luku 2 ei siis toteuta joukon $B$ ehtoa. Tämän vuoksi $2 \notin B$. Siis $\{1, 2\} \not\subset B$.

**Esimerkki 1.4.6.** Oletetaan, että $A$ on joukko. Päätellään, että $\emptyset \subset A$.

Tavallisen logiikan mukaan on kaksi vaihtoehtoa: tyhjä joukko joko *on* joukon $A$ osajoukko tai *ei ole* joukon $A$ osajoukko. Mitään kolmatta vaihtoehtoa ei ole, eivätkä vaihtoehdot $\emptyset \subset A$ tai $\emptyset \not\subset A$ voi olla tosia yhtä aikaa, vaan toinen on tosi ja toinen epätosi.

Mietitään aluksi, voisiko sittenkin päteä, että $\emptyset \not\subset A$. Tällöin joukossa $\emptyset$ pitäisi olla alkio, joka ei kuulu joukkoon $A$ (vrt. esim. 1.4.5). Tyhjässä joukossa $\emptyset$ ei kuitenkaan ole yhtään alkiota. Joukossa $\emptyset$ ei siis ole sellaista alkiota, joka ei kuulu joukkoon $A$. Näin vaihtoehto $\emptyset \not\subset A$ on epätosi.

Koska vaihtoehto $\emptyset \not\subset A$ on epätosi, täytyy toisen vaihtoehdon olla tosi. Siis $\emptyset \subset A$.

---

Joissakin tilanteissa tavataan joukkoja, joiden alkiot ovat nekin joukkoja. Kappaleessa 1.8 esiteltävä potenssijoukon käsite on esimerkki tällaisesta tilanteesta. Seuraavassa esimerkissä havainnollistetaan osajoukon ja joukossa alkiona olevan joukon eroa.

**Esimerkki 1.4.7.** Merkitään $X = \{2, 3, \{1\}, \{4, 2\}\}$ ja $A = \{2, 3\}$, $B = \{1\}$ ja $C = \{\{1\}, 3\}$. Mitkä joukoista $A$, $B$, $C$ ja $X$ ovat joukon $X$ osajoukkoja?

Joukon $X$ merkinnästä nähdään, että sen alkiot ovat luku 2, luku 3, joukko $\{1\}$ eli ykkösen *yksiö* ja joukko $\{4, 2\}$ eli lukujen 4 ja 2 *kaksio*. Joukossa $X$ on siis alkioina kaksi lukua ja kaksi joukkoa.

Havaitaan, että $A \subset X$, sillä $A = \{2, 3\}$, ja $2 \in X$ ja $3 \in X$ (jokainen joukon $A$ alkio kuuluu joukkoon $X$). Toisaalta $B \not\subset X$, sillä $1 \in B$ mutta $1 \notin X$ (joukossa $B$ on alkio 1, joka ei kuulu joukkoon $X$).

Joukko $C$ on joukon $X$ osajoukko eli $C \subset X$, sillä $C = \{\{1\}, 3\}$, ja $\{1\} \in X$ ja $3 \in X$ (jokainen joukon $C$ alkio kuuluu joukkoon $X$). Lisäksi joukko $X$ on itsensä osajoukko eli $X \subset X$, sillä jokainen joukon $X$ alkio kuuluu joukkoon $X$.

---

Avoimet, suljetut ja puoliavoimet välit ovat reaalilukujen joukon osajoukkoja.

**Määritelmä 1.4.8.** Oletetaan, että $a$ ja $b$ ovat reaalilukuja ja $a < b$. Tällöin määritellään avoin väli $]a, b[$, suljettu väli $[a, b]$ sekä puoliavoimet välit $[a, b[$ ja $]a, b]$ seuraavasti:

$$]a, b[ = \{ x \in \mathbb{R} \mid a < x < b \} \qquad [a, b] = \{ x \in \mathbb{R} \mid a \leq x \leq b \}$$

$$[a, b[ = \{ x \in \mathbb{R} \mid a \leq x < b \} \qquad ]a, b] = \{ x \in \mathbb{R} \mid a < x \leq b \}$$


Kuva 1.3: suljettu väli $[0, 1]$, avoin väli $]2, 3[$ ja puoliavoin väli $[4, 5[$

Symbolien $\infty$ ja $-\infty$ avulla voidaan osoittaa, että väli on rajaton. Rajattomat välit määritellään seuraavasti:

**Määritelmä 1.4.9.** Oletetaan, että $c$ on reaaliluku. Tällöin

$$]-\infty, c[ = \{ x \in \mathbb{R} \mid x < c \} \qquad ]c, \infty[ = \{ x \in \mathbb{R} \mid x > c \}$$

$$]-\infty, c] = \{ x \in \mathbb{R} \mid x \leq c \} \qquad [c, \infty[ = \{ x \in \mathbb{R} \mid x \geq c \}$$

## 1.5 Osajoukoksi osoittaminen

Aikaisemmin olemme jo tutustuneet siihen, miten annettu joukko osoitetaan toisen joukon osajoukoksi (esim. 1.4.3–1.4.4). Abstraktissakin tilanteessa voidaan käyttää samaa ideaa kuin esimerkissä 1.4.4: otetaan tarkasteltavasta joukosta yksi alkio umpimähkään ja näytetään, että se kuuluu toiseen joukkoon. Näin tehdään myös seuraavassa esimerkissä.

**Esimerkki 1.5.1.** Oletetaan, että $A$ ja $B$ ovat joukkoja. Osoitetaan, että $(A \cup B) \smallsetminus B \subset A$.

Oletetaan, että $a \in (A \cup B) \smallsetminus B$. Tästä voidaan erotuksen määritelmän nojalla päätellä, että $a \in A \cup B$ ja $a \notin B$. Edelleen koska $a \in A \cup B$, voidaan yhdisteen määritelmän nojalla päätellä, että $a \in A$ tai $a \in B$. Näistä jälkimmäinen vaihtoehto ei voi toteutua, koska jo aikaisemmin päädyttiin siihen, että $a \notin B$. Voidaan siis olla varmoja, että ensimmäinen vaihtoehto on totta eli $a \in A$.

Yllä oleva päättely voidaan tehdä mille tahansa joukon $(A \cup B) \smallsetminus B$ alkiolle, joten jokainen joukon $(A \cup B) \smallsetminus B$ alkio kuuluu joukkoon $A$.

## 1.6 Joukkojen osoittaminen samaksi

Edellisissä kappaleissa tutustuimme osajoukon määritelmään ja siihen, miten sen avulla osoitetaan joukko toisen joukon osajoukoksi. Tässä kappaleessa sovellamme osajoukoksi osoittamista kahden joukon samaksi osoittamiseen. Aloitetaan määrittelemällä, mitä tarkoitetaan sillä, että kaksi joukkoa ovat samat.

**Määritelmä 1.6.1.** Joukot $A$ ja $B$ ovat *samat*, jos niissä on täsmälleen samat alkiot eli kaikilla alkioilla $x$ pätee seuraava: $x \in A$, jos ja vain jos $x \in B$. Tällöin merkitään $A = B$.

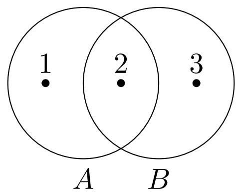
**Esimerkki 1.6.2.** Päteekö väite $(A \cup B) \smallsetminus B = A$ kaikilla joukoilla $A$ ja $B$?

Oletetaan, että $A$ ja $B$ ovat joukkoja. Esimerkissä 1.5.1 näytettiin, että tällöin

$$(A \cup B) \smallsetminus B \subset A.$$

Tämä tarkoittaa, että jokainen joukon $(A \cup B) \setminus B$ alkio kuuluu joukkoon $A$. Tästä ei kuitenkaan voida päätellä, että joukot $(A \cup B) \setminus B$ ja $A$ olisivat samat. Voi nimittäin olla, että joukossa $A$ on sellaisia alkioita, jotka eivät kuulu joukkoon $(A \cup B) \setminus B$.

Kumotaan väite "$(A \cup B) \setminus B = A$ kaikilla joukoilla $A$ ja $B$" antamalla *vastaesimerkki*. Valitaan vaikkapa $A = \{1, 2\}$ ja $B = \{2, 3\}$. Tällöin $(A \cup B) \setminus B = \{1, 2, 3\} \setminus \{2, 3\} = \{1\}$. Siten $(A \cup B) \setminus B \neq A$. Tästä nähdään, että väite ei pidä paikkaansa kaikilla joukoilla $A$ ja $B$. Huomaa, että väite saattaa kuitenkin päteä jossain erityistapauksessa, esimerkiksi jos $B = \emptyset$ tai jos $A \cap B = \emptyset$.




Kuva 1.4: On olemassa joukot $A$ ja $B$, joilla väite $(A \cup B) \setminus B = A$ ei päde.

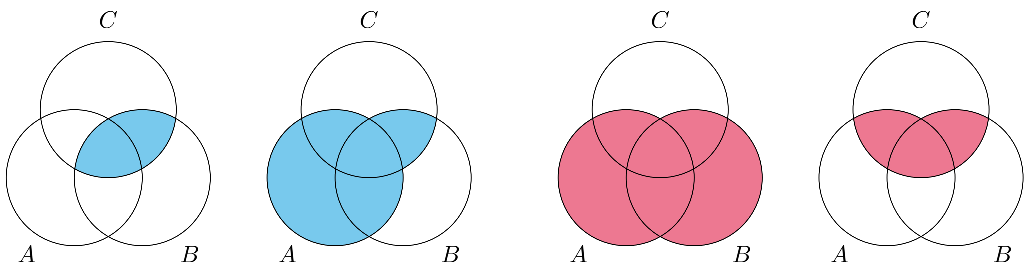
---

Joukkojen samuutta koskevia väitteitä on joskus hyödyllistä tutkia Vennin kaavioiden avulla ennen väitteiden täsmällistä todistamista.

**Esimerkki 1.6.3.** Tutkitaan Vennin kaavioiden avulla, kumpi seuraavista yhtälöistä näyttäisi pätevän kaikilla joukoilla $A$, $B$ ja $C$:

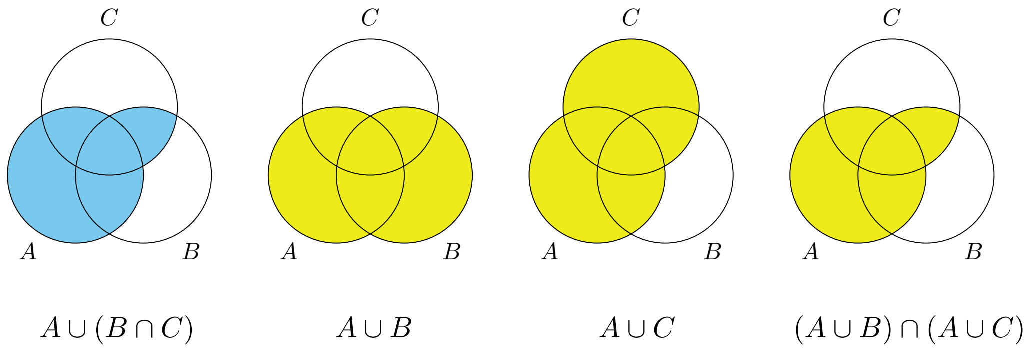
$$A \cup (B \cap C) = (A \cup B) \cap C \qquad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)\,.$$

Vennin kaaviot kannattaa piirtää esimerkiksi vaiheittain kuten alla.




$B \cap C$ $\qquad$ $A \cup (B \cap C)$ $\qquad$ $A \cup B$ $\qquad$ $(A \cup B) \cap C$

Kuva 1.5: Yhtälön $A \cup (B \cap C) = (A \cup B) \cap C$ tutkiminen Vennin kaavioiden avulla.




Kuva 1.6: Yhtälön $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ tutkiminen Vennin kaavioiden avulla.

Näyttäisi siltä, että yhtälö $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ pätee aina, sillä kuvassa 1.6 vasemmanpuolimmainen ja oikeanpuolimmainen Vennin kaavio ovat identtiset. Sen sijaan kuvassa 1.5 päädyttiin keskenään erilaisiin Vennin kaavioihin.

---

Monissa tilanteissa Vennin kaaviot eivät riitä perustelemaan joukkojen samuutta, vaan tarvitaan toisenlaista päättelyä. Esimerkiksi jos tarkasteltavia joukkoja on enemmän kuin kolme, käy oikeanlaisen Vennin kaavion piirtäminen hankalammaksi, ja äärettömän monen joukon tapauksessa se on mahdotonta. Lisäksi kaavioiden tulkinta vaatii huolellisuutta: joissain tilanteissa osa Vennin kaavion alueista voi vastata tyhjää joukkoa, mikä saattaa hankaloittaa oikeiden johtopäätösten tekemistä.

Seuraavaksi harjoittelemme osoittamaan kaksi joukkoa samaksi tekniikalla, joka perustuu joukkojen samuuden määritelmään 1.6.1. Määritelmän mukaan joukot $X$ ja $Y$ ovat samat, jos niissä on täsmälleen samat alkiot; ts. jos jokainen joukon $X$ alkio kuuluu joukkoon $Y$ ja jokainen joukon $Y$ alkio kuuluu joukkoon $X$. Joukkojen samuus voidaan siis todistaa osoittamalla kumpikin joukko toisen osajoukoksi.

Todistus, jossa kaksi joukkoa osoitetaan samaksi, muodostuu siis kahdesta osasta. Nämä osat saatetaan joskus erottaa toisistaan merkeillä "$\subset$" ja "$\supset$", jotka muistuttavat todistuksen kirjoittajaa ja myös lukijaa siitä, kumpaa joukkoa ollaan osoittamassa toisen joukon osajoukoksi. Näin on tehty myös seuraavassa esimerkissä.

**Esimerkki 1.6.4.** Oletetaan, että $A$, $B$ ja $C$ ovat joukkoja. Osoitetaan, että

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

"$\subset$": Oletetaan, että $x \in A \cup (B \cap C)$. Yhdisteen määritelmän nojalla voidaan päätellä, että $x \in A$ tai $x \in B \cap C$. Koska ei voida olla varmoja siitä, kumpi näistä vaihtoehdoista on voimassa, täytyy kumpikin niistä tarkastella erikseen. Näin voidaan varmistua siitä, että haluttuun johtopäätökseen päädytään kaikissa mahdollisissa tapauksissa.

Tapaustarkastelu:

- Oletetaan, että $x \in A$. Yhdisteen määritelmän nojalla voidaan tästä päätellä, että $x \in A \cup B$ ja $x \in A \cup C$. Koska $x$ on näiden molempien joukkojen alkio, voidaan leikkauksen määritelmän nojalla päätellä, että $x \in (A \cup B) \cap (A \cup C)$.
- Oletetaan, että $x \in B \cap C$. Leikkauksen määritelmän nojalla voidaan päätellä, että $x \in B$ ja $x \in C$. Koska $x \in B$, niin yhdisteen määritelmän nojalla $x \in A \cup B$. Toisaalta koska $x \in C$, niin yhdisteen määritelmän nojalla $x \in A \cup C$. Koska $x$ kuuluu sekä joukkoon $A \cup B$ että joukkoon $A \cup C$, niin $x \in (A \cup B) \cap (A \cup C)$.

Kaikissa mahdollisissa tapauksissa päädytään siis johtopäätökseen, että $x \in (A \cup B) \cap (A \cup C)$.

Edellä tehty päättely pätee mille tahansa joukon $A \cup (B \cap C)$ alkiolle, joten joukon $A \cup (B \cap C)$ jokainen alkio kuuluu joukkoon $(A \cup B) \cap (A \cup C)$. Siis

$$A \cup (B \cap C) \subset (A \cup B) \cap (A \cup C).$$

Huomaa, että matematiikan ”tai” ei ole poissulkeva, vaan edellä tapaustarkastelussa on mahdollista, että $x$ kuuluu kumpaankin joukoista $A$ ja $B$. Miksi sitten ei erikseen käsitelty vaihtoehtoa, jossa $x \in A$ ja $x \in B$? Itse asiassa tämä vaihtoehto sisältyy edellä käsiteltyihin tapauksiin. Nimittäin ensimmäisessä tapauksessa oletetaan, että $x \in A$ eikä oteta mitään kantaa siihen, kuuluuko $x$ joukkoon $B$ vai ei. Siten ensimmäinen tapaus sisältää sekä tapauksen, jossa $x \in B$, että tapauksen, jossa $x \notin B$. Vastaavasti jälkimmäisessä tapauksessa oletetaan vain, että $x \in B$ eikä oteta kantaa siihen, kuuluuko $x$ joukkoon $A$ vai ei.

”$\supset$”: Oletetaan, että $x \in (A \cup B) \cap (A \cup C)$. Leikkauksen määritelmän nojalla voidaan päätellä, että $x \in A \cup B$ ja $x \in A \cup C$.

Yhdisteen määritelmän soveltaminen sekä joukkoon $A \cup B$ että joukkoon $A \cup C$ johtaa helposti sekavaan tilanteeseen, jossa virhepäätelmien riski kasvaa. Turvaudutaan siis hiukan erilaiseen menettelytapaan. Voidaan olla varmoja, että joka tapauksessa pätee joko $x \in A$ tai $x \notin A$. Tutkitaan nämä vaihtoehdot erikseen:

- Oletetaan, että $x \in A$. Tällöin yhdisteen määritelmän mukaan $x \in A \cup (B \cap C)$.
- Oletetaan, että $x \notin A$. Koska kuitenkin tiedetään, että $x \in A \cup B$, voidaan päätellä, että $x \in B$. Vastaavasti koska $x \in A \cup C$ ja oletuksen mukaan $x \notin A$, niin $x \in C$. Siis $x \in B$ ja $x \in C$, joten leikkauksen määritelmän mukaan $x \in B \cap C$. Tästä seuraa yhdisteen määritelmän nojalla, että $x \in A \cup (B \cap C)$.

Kaikissa mahdollisissa tapauksissa päädytään johtopäätökseen, että $x \in A \cup (B \cap C)$.

Edellä tehty päättely pätee mille tahansa joukon $(A \cup B) \cap (A \cup C)$ alkiolle, joten joukon $(A \cup B) \cap (A \cup C)$ jokainen alkio kuuluu joukkoon $A \cup (B \cap C)$. Tämä tarkoittaa, että

$$(A \cup B) \cap (A \cup C) \subset A \cup (B \cap C).$$

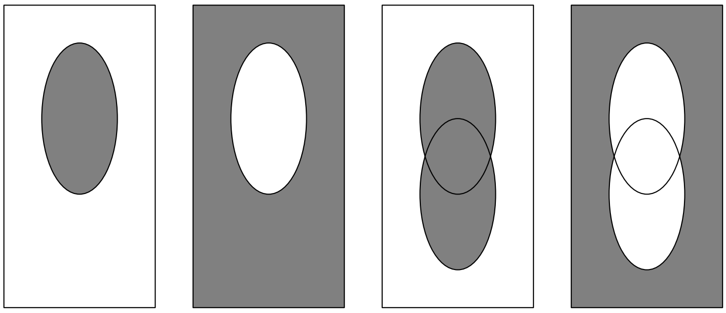
Päättelysuunnat ”$\subset$” ja ”$\supset$” yhdessä osoittavat, että $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. $\square$

## 1.7 Perusjoukko ja komplementti

Usein tarkastellaan jonkin tietyn joukon eri osajoukkoja ja alkioita. Tätä joukkoa, jonka osajoukkoja ja alkoita tutkitaan, sanotaan *perusjoukoksi.*

**Määritelmä 1.7.1.** Olkoon $X$ tarkasteltava perusjoukko. Joukon $A \subset X$ *komplementti* on joukko
$$\complement A = \{\, x \in X \mid x \notin A \,\}\,.$$

Joukon $A$ komplementti voidaan ilmaista joukkojen erotuksen avulla: $\complement A = X \setminus A$. Sille käytetään joskus myös merkintää $A^c$ tai $\bar{A}$. Esimerkiksi topologiassa merkintä $\bar{A}$ tarkoittaa niin sanottua suljettua joukkoa, minkä vuoksi emme käytä sitä komplementin merkintänä.



$A$ $\quad$ $\complement A$ $\quad$ $A \cup B$ $\quad$ $\complement(A \cup B)$

Kuva 1.7: Joukot $A$ ja $\complement A$ sekä $A \cup B$ ja $\complement(A \cup B)$.

Perusjoukkoa ei välttämättä aina erikseen ilmoiteta, vaan se pitää päätellä asiayhteydestä.

**Esimerkki 1.7.2.** Tarkastellaan luonnollisten lukujen joukon $\mathbb{N}$ osajoukkoja $A = \{0, 1, 2, 3\}$ ja $B = \{\, n \in \mathbb{N} \mid n = 2k \text{ missä } k \in \mathbb{N} \,\}$. Määritetään $\complement A$ ja $\complement B$.

Ensimmäisestä virkkeestä voidaan päätellä, että perusjoukkona on luonnollisten lukujen joukko. Komplementin määritelmän mukaan

$$\complement A = \{n \in \mathbb{N} \mid n \notin A\} = \{4, 5, 6, 7, \dots\} = \{\, n \in \mathbb{N} \mid n \geq 4 \,\}$$
$$\complement B = \{n \in \mathbb{N} \mid n \notin B\} = \{1, 3, 5, 7, \dots\} = \{\, m \in \mathbb{N} \mid m = 2k + 1 \text{ missä } k \in \mathbb{N} \,\}.$$

Huomataan, että joukko $B$ on parillisten luonnollisten lukujen joukko ja sen komplementti $\complement B$ on parittomien luonnollisten lukujen joukko.

**Lause 1.7.3** (**de Morganin lait**). *Oletetaan, että $A$ ja $B$ ovat joukon $X$ osajoukkoja. Tällöin*

$$\complement(A \cup B) = \complement A \cap \complement B \quad \text{ja} \quad \complement(A \cap B) = \complement A \cup \complement B.$$

*Todistus.* Todistetaan ensimmäinen väite ja jätetään toisen väitteen todistus harjoitustehtäväksi. Osoitetaan siis, että $\complement(A \cup B) = \complement A \cap \complement B$ näyttämällä kumpikin joukko toisen osajoukoksi samaan tapaan kuin esimerkissä 1.6.4.

”$\subset$”: Oletetaan, että $x \in \complement(A \cup B)$. Komplementin määritelmän nojalla tästä voidaan päätellä, että $x \in X$ ja $x \notin A \cup B$.

Voiko alkio $x$ tässä tilanteessa kuulua joukkoon $A$? Jos $x \in A$, niin silloin yhdisteen määritelmän mukaan $x \in A \cup B$. Koska kuitenkin edellä todettiin, että $x \notin A \cup B$, niin voidaan päätellä, että $x \notin A$. Vastaavasti koska $x \notin A \cup B$, niin $x \notin B$.

Koska $x \in X$ ja $x \notin A$, niin komplementin määritelmän mukaan $x \in \complement A$. Vastaavasti koska $x \in X$ ja $x \notin B$, niin $x \in \complement B$. Näin $x \in \complement A$ ja $x \in \complement B$, joten leikkauksen määritelmän mukaan $x \in \complement A \cap \complement B$.

”$\supset$”: Oletetaan, että $x \in \complement A \cap \complement B$. Leikkauksen määritelmän nojalla voidaan tästä päätellä, että $x \in \complement A$ ja $x \in \complement B$. Komplementin määritelmän mukaan tällöin $x \in X$ ja $x \notin A$ ja $x \notin B$. Koska $x \notin A$ ja $x \notin B$, niin $x \notin A \cup B$. Siis $x \in X$ ja $x \notin A \cup B$, mikä komplementin määritelmän mukaan tarkoittaa, että $x \in \complement(A \cup B)$. □

## 1.8 Potenssijoukko

Kappaleessa 1.4 tutustuttiin osajoukon käsitteeseen. Tässä kappaleessa siirrytään tarkastelemaan jonkin annetun joukon kaikkia osajoukkoja ja niiden muodostamaa joukkoa.

**Määritelmä 1.8.1.** Oletetaan, että $X$ on joukko. Joukon $X$ *potenssijoukko* tarkoittaa sen kaikkien osajoukkojen muodostamaa joukkoa

$$\mathcal{P}(X) = \{\, A \mid A \subset X \,\}.$$

**Esimerkki 1.8.2.** Joukolla $X = \{3, 1, 4\}$ on seuraavat osajoukot: tyhjä joukko $\emptyset$, yhden alkion osajoukot eli yksiöt $\{3\}$, $\{1\}$, $\{4\}$, kahden alkion osajoukot eli kaksiot $\{3, 1\}$, $\{3, 4\}$, $\{1, 4\}$ ja joukko itse $X$. Kun nämä kerätään yhdeksi joukoksi, saadaan joukon $X$ potenssijoukko:

$$\mathcal{P}(X) = \{\, \emptyset,\ \{3\},\ \{1\},\ \{4\},\ \{3, 1\},\ \{3, 4\},\ \{1, 4\},\ X \,\}.$$

**Esimerkki 1.8.3.** Olkoon $Y = \{\emptyset, \{3, 1, 4\}\}$. Määritä $\mathcal{P}(Y)$.

Potenssijoukon määrittämiseksi pitää tutkia, mitä osajoukkoja joukolla $Y$ on. Tiedetään, että tyhjä joukko $\emptyset$ on minkä tahansa joukon osajoukko (esim. 1.4.6) eli erityisesti $\emptyset \subset Y$. Lisäksi joukko itse on itsensä osajoukko (esim. 1.4.7) eli erityisesti $Y \subset Y$. Joukolla $Y$ on siis ainakin kaksi osajoukkoa: $\emptyset$ ja $Y$. Onko sillä muita osajoukkoja?

Huomataan, että joukossa $Y$ on kaksi alkiota: $\emptyset$ ja $\{3, 1, 4\}$. (Nämä alkiot ovat itsekin joukkoja, mutta siitä huolimatta ne ovat joukon $Y$ alkiota). Voidaan päätellä, että joukolla $Y$ on osajoukkoina myös kaksi yksiötä: alkion $\emptyset$ yksiö $\{\emptyset\}$ ja alkion $\{3, 1, 4\}$ yksiö $\{\{3, 1, 4\}\}$.

Kaksialkioisella joukolla $Y$ on siis yhteensä neljä osajoukkoa: tyhjä joukko $\emptyset$, yksiöt $\{\emptyset\}$ ja $\{\{3,1,4\}\}$ sekä joukko $Y$ itse. Joukon $Y$ potenssijoukko on siten

$$\mathcal{P}(Y) = \{\, \emptyset,\ \{\emptyset\},\ \{\{3,1,4\}\},\ Y\,\}.$$

---

Myös potenssijoukkojen tapauksessa kaksi joukkoa osoitetaan samaksi näyttämällä kumpikin toisen osajoukoksi. Tätä on havainnollistettu seuraavassa esimerkissä.

**Esimerkki 1.8.4.** Oletetaan, että $A$ ja $B$ ovat joukkoja. Osoita, että $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.

"$\subset$": Oletetaan, että $X \in \mathcal{P}(A \cap B)$. Tästä voidaan potenssijoukon määritelmän nojalla päätellä, että $X$ on joukon $A \cap B$ osajoukko eli $X \subset A \cap B$. Tästä puolestaan seuraa lemman 3.3.4 nojalla, että $X \subset A$ ja $X \subset B$. Potenssijoukon määritelmän mukaan tällöin $X \in \mathcal{P}(A)$ ja $X \in \mathcal{P}(B)$. Leikkauksen määritelmän mukaan tästä seuraa, että $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$.

"$\supset$": Oletetaan, että $Y \in \mathcal{P}(A) \cap \mathcal{P}(B)$. Tästä voidaan leikkauksen määritelmän nojalla päätellä, että $Y \in \mathcal{P}(A)$ ja $Y \in \mathcal{P}(B)$. Potenssijoukon määritelmän mukaan tällöin $Y \subset A$ ja $Y \subset B$. Tästä voidaan lemman 3.3.4 nojalla päätellä, että $Y \subset A \cap B$. Koska $Y$ on joukon $A \cap B$ osajoukko, niin $Y \in \mathcal{P}(A \cap B)$. $\square$

Huomaa, että esimerkissä nojauduttiin lemmaan 3.3.4, jonka mukaan $X \subset A \cap B$, jos ja vain jos $X \subset A$ ja $X \subset B$. Jos tätä tulosta ei olisi ollut käytettävissä, olisi sekin pitänyt todistaa.

## 1.9 Joukkojen karteesinen tulo eli tulojoukko

Tiedämme jo, että joukossa alkioiden järjestyksellä ei ole väliä: esimerkiksi $\{3,8\} = \{8,3\}$. Jos alkioiden järjestyksellä on väliä, päädytään kahden alkion tapauksessa niin sanotun järjestetyn parin käsitteeseen. *Järjestetty pari* on muotoa $(a,b)$ ja sille pätee

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

Siis esimerkiksi $(1+2, 2^3) = (3,8)$ mutta $(3,8) \neq (8,3)$. Järjestettyjen parien avulla voidaan esimerkiksi ilmaista tasokoordinaatiston pisteiden koordinaatteja.

Järjestetyn parin käsitteen avulla voidaan määritellä joukkojen karteesinen tulo:

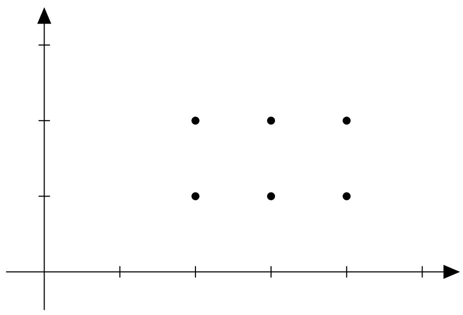
**Määritelmä 1.9.1.** Oletetaan, että $A$ ja $B$ ovat joukkoja. Joukkojen $A$ ja $B$ *karteesinen tulo* eli *tulojoukko* on joukko

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

**Esimerkki 1.9.2.** Määritetään joukkojen $C = \{2,3,4\}$ ja $D = \{1,2\}$ karteesinen tulo $C \times D$. Määritelmän mukaan se on

$$C \times D = \{\, (x,y) \mid x \in C \text{ ja } y \in D\,\} = \{(2,1),\ (2,2),\ (3,1),\ (3,2),\ (4,1),\ (4,2)\}.$$

Tulojoukkoa $C \times D$ voi havainnollistaa koordinaatistossa:



Kuva 1.8: Joukko $C \times D = \{(2,1),\ (2,2),\ (3,1),\ (3,2),\ (4,1),\ (4,2)\}$ koordinaatistossa.

---

Tulojoukon alkiot eivät välttämättä ole lukupareja, vaan ne voivat olla minkä tahansa olioiden muodostamia järjestettyjä pareja. Seuraavassa esimerkissä tarkastellaan joukkojen muodostamia järjestettyjä pareja.

**Esimerkki 1.9.3.** Merkitään $A = \{1, 2\}$. Joukon $A$ potenssijoukko on sen kaikkien osajoukkojen muodostama joukko $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, A\}$. Määritellään joukko $B$ asettamalla

$$B = \{(X, Y) \in \mathcal{P}(A) \times \mathcal{P}(A) \mid X \subset Y\}.$$

Havaitaan, että joukko $B$ voidaan kirjoittaa myös luettelemalla siihen kuuluvat alkiot:

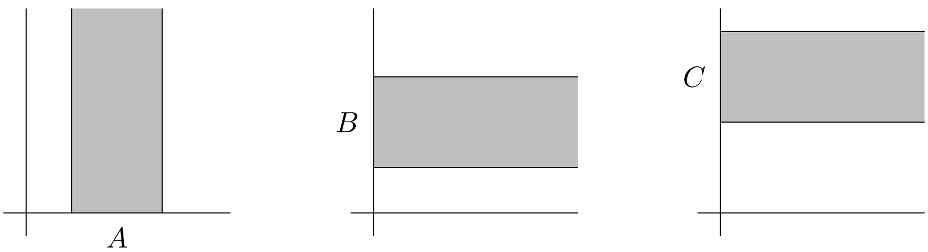
$$B = \{(\emptyset, \emptyset), (\emptyset, \{1\}), (\emptyset, \{2\}), (\emptyset, A), (\{1\}, \{1\}), (\{1\}, A), (\{2\}, \{2\}), (\{2\}, A), (A, A)\}.$$

---

Vennin kaaviot eivät sovellu kovin hyvin tulojoukkoja koskevien yleisten väitteiden tutkimiseen. Tulojoukkoja voidaan kuitenkin havainnollistaa piirroksilla kuten seuraavassa esimerkissä.

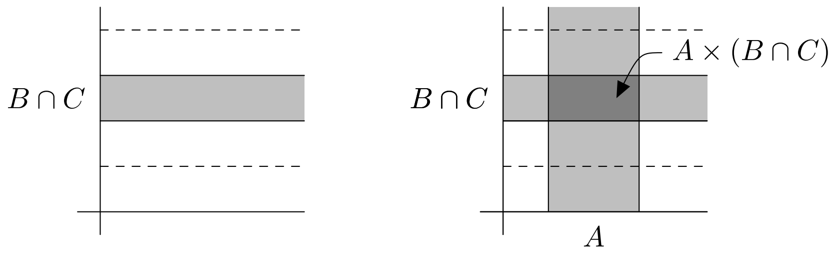
**Esimerkki 1.9.4.** Oletetaan, että $A$, $B$ ja $C$ ovat joukkoja. Havainnollistetaan piirroksella joukkoja $A \times (B \cap C)$ ja $(A \times B) \cap (A \times C)$.

Merkitään tulojoukossa vasemmalla esiintyvä joukko $A$ koordinaatiston vaaka-akselille ja piirretään sen levyinen pystysuora kaistale (kuva 1.9). Merkitään sitten oikealla esiintyvät joukot $B$ ja $C$ pystyakselille niin, että ne menevät osittain päällekkäin, ja piirretään niitä vastaavat vaakasuorat kaistaleet.



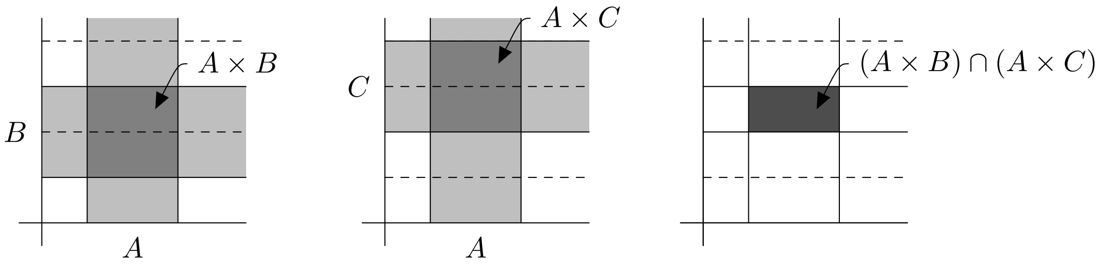

Kuva 1.9: Joukot $A$, $B$ ja $C$.

Leikkausta $B \cap C$ vastaava vaakasuora kaistale on kuvassa 1.10. Tulojoukko $A \times (B \cap C)$ on joukkoa $A$ vastaavan kaistaleen ja joukkoa $B \cap C$ vastaavan kaistaleen leikkaus, joka on merkitty kuvaan 1.10 tummanharmaalla.




Kuva 1.10: Joukot $B \cap C$ ja $A \times (B \cap C)$.

Vastaavasti tulojoukko $A \times B$ on joukkoa $A$ vastaavan kaistaleen ja joukkoa $B$ vastaavan kaistaleen leikkaus, joka on merkitty kuvaan 1.11 tummanharmaalla. Kuvassa 1.11 näkyy havainnollistus myös tulojoukolle $A \times C$. Niiden leikkauksena saadaan joukko $(A \times B) \cap (A \times C)$.




Kuva 1.11: Joukot $A \times B$, $A \times C$ ja $(A \times B) \cap (A \times C)$.

---

Esimerkin 1.9.4 havainnollistuksen perusteella joukot $A \times (B \cap C)$ ja $(A \times B) \cap (A \times C)$ näyttävät olevan samat. Todistetaan seuraavaksi, että tämä havainto pitää paikkansa, olivatpa joukot $A$, $B$ ja $C$ mitä tahansa joukkoja. Käytetään jälleen kappaleessa 1.6 esiteltyä tekniikkaa, jolla kaksi joukkoa osoitetaan samaksi näyttämällä, että kumpikin on toisen osajoukko.

**Esimerkki 1.9.5.** Osoitetaan, että $A \times (B \cap C) = (A \times B) \cap (A \times C)$ kaikilla joukoilla $A$, $B$ ja $C$.

Oletetaan, että $A$, $B$ ja $C$ ovat joukkoja. Näytetään, että tällöin $A \times (B \cap C) = (A \times B) \cap (A \times C)$. Tehdään tämä osoittamalla sisältyminen molempiin suuntiin.

"$\subset$": Oletetaan, että $x \in A \times (B \cap C)$. Tulojoukon määritelmän nojalla voidaan päätellä, että $x$ on tietynlainen järjestetty pari. Tarkemmin sanottuna $x = (s, t)$, missä $s \in A$ ja $t \in B \cap C$. Koska $t \in B \cap C$, voidaan leikkauksen määritelmän nojalla päätellä edelleen, että $t \in B$ ja $t \in C$.

Mitä nyt voidaan sanoa järjestetystä parista $(s,t)$? Koska $s \in A$ ja $t \in B$, niin tulojoukon määritelmän mukaan $(s,t) \in A \times B$. Lisäksi $x = (s,t)$, joten $x \in A \times B$. Vastaavasti koska $s \in A$ ja $t \in C$, niin $x = (s,t) \in A \times C$. Koska $x$ kuuluu sekä joukkoon $A \times B$ että joukkoon $A \times C$, voidaan leikkauksen määritelmän nojalla päätellä, että $x \in (A \times B) \cap (A \times C)$.

”$\supset$”: Oletetaan, että $y \in (A \times B) \cap (A \times C)$. Leikkauksen määritelmän nojalla $y \in A \times B$ ja $y \in A \times C$. Alkio $y$ on siis tietynlainen järjestetty pari. Tarkemmin sanottuna $y = (a,d)$, missä $a \in A$, $d \in B$ ja $d \in C$. Koska $d$ kuuluu sekä joukkoon $B$ että joukkoon $C$, voidaan päätellä, että $d \in B \cap C$. Koska $a \in A$ ja $d \in B \cap C$, niin tulojoukon määritelmän mukaan $y = (a,d) \in A \times (B \cap C)$.

Päättelyt ”$\subset$” ja ”$\supset$” yhdessä osoittavat, että $A \times (B \cap C) = (A \times B) \cap (A \times C)$. Koska todistuksen alussa oletettiin, että $A$, $B$ ja $C$ ovat joukkoja, eikä mitään muita niitä koskevia oletuksia tehty, pätee tämä päättely riippumatta siitä, mitä joukkoja $A$, $B$ ja $C$ ovat. Voidaan siis päätellä, että $A \times (B \cap C) = (A \times B) \cap (A \times C)$ kaikilla joukoilla $A$, $B$ ja $C$. $\square$

# 2 Logiikkaa

Tässä luvussa tutustutaan joihinkin logiikan käsitteisiin ja merkintöihin. Lisätietoja ja tarkennuksia löytyy esimerkiksi Jouko Väänäsen kirjasta Logiikka I

## 2.1 Loogiset konnektiivit

Väitelauseen tunnistaa siitä, että se voi olla tosi tai epätosi. Esimerkiksi $10 > 8$ on väitelause, samoin $\sqrt{2} \in \mathbb{Z}$. Näistä ensimmäinen eli $10 > 8$ on tosi, jälkimmäinen eli $\sqrt{2} \in \mathbb{Z}$ puolestaan epätosi. Väitelauseista voidaan rakentaa monimutkaisempia väitelauseita *loogisten konnektiivien* avulla. Niistä tavallisimmat on lueteltu alla taulukossa 2.1.

| Nimitys | Symboli | Merkitys |
|---|---|---|
| Negaatio | $\neg$ | ei |
| Konjuktio | $\wedge$ | ja |
| Disjunktio | $\vee$ | tai |
| Implikaatio | $\rightarrow$ | jos ..., niin ... |
| Ekvivalenssi | $\leftrightarrow$ | ...jos ja vain jos ... |

Taulukko 2.1: Loogisia konnektiiveja.

Konnektiivien lisäksi monimutkaisempien väitteiden muodostamiseen tarvitaan sulkeita osoittamaan konnektiivien soveltamisen järjestys. Esimerkiksi $A \wedge (B \vee C)$ tarkoittaa eri asiaa kuin $(A \wedge B) \vee C$. Tässä $A$, $B$ ja $C$ ovat *propositiolauseita*, jotka symboloivat väitelauseita. Ne muodostetaan *propositiosymboleista* $p_0$, $p_1$, $p_2$ ..., konnektiiveista ja sulkeista. Esimerkiksi väite ”jos sataa tai tuulee kovasti, niin en lähde merelle” voidaan kirjoittaa propositiolauseena $(p_0 \vee p_1) \rightarrow \neg p_2$, missä lause ”sataa” on korvattu propositiosymbolilla $p_0$, lause ”tulee kovasti” propositiosymbolilla $p_1$ ja lause ”lähden merelle” propositiosymbolilla $p_2$.

Taulukossa 2.1 mainittujen konnektiivien tarkka merkitys määritellään totuustaulujen avulla. Propositiolauseen *totuustaulu* on taulukko, jossa sen *totuusarvot* (tosi/epätosi) on listattu kaikissa tapauksissa. Jos propositiolause on tosi, merkitään totuustaulussa vastaavaan kohtaan totuusarvo 1. Jos propositiolause on epätosi, merkitään totuustaulussa vastaavaan kohtaan totuusarvo 0.

**Määritelmä 2.1.1.** Negaatiolla $\neg$ on seuraava totuustaulu:

| $A$ | $\neg A$ |
|---|---|
| 1 | 0 |
| 0 | 1 |

Määritelmän 2.1.1 totuustaulusta nähdään, että negaatio vaihtaa propositiolauseen totuusarvon: jos propositiolause on tosi, on sen negaatio epätosi, ja päinvastoin. Merkintä $\neg A$ luetaan "ei $A$".

**Määritelmä 2.1.2.** Konjunktiolla $\wedge$ ja disjunktiolla $\vee$ on seuraavat totuustaulut:

| $A$ | $B$ | $A \wedge B$ |
|---|---|---|
| 1 | 1 | 1 |
| 1 | 0 | 0 |
| 0 | 1 | 0 |
| 0 | 0 | 0 |

| $A$ | $B$ | $A \vee B$ |
|---|---|---|
| 1 | 1 | 1 |
| 1 | 0 | 1 |
| 0 | 1 | 1 |
| 0 | 0 | 0 |

Määritelmän 2.1.2 totuustaulusta nähdään, että konjuktio $A \wedge B$ (luetaan "$A$ ja $B$") on tosi täsmälleen siinä tapauksessa, että propositiolauseet $A$ ja $B$ ovat molemmat tosia. Konjuktion määritelmä vastaa siis ja-sanan arkikielestä tuttua merkitystä.

Arkikielessä tai-sanaa käytetään kahdella erilaisella tavalla. Esimerkiksi lauseessa "lounaaseen sisältyy kahvi tai jälkiruoka" kysymyksessä on niin sanottu poissulkeva tai, mikä tarkoittaa, että asiakas voi valita kahvin tai jälkiruoan, mutta ei molempia. Toisaalta esimerkiksi lauseesta "jos sataa tai tulee kovasti, niin en lähde merelle" voidaan päätellä, että merimatka jää väliin silloinkin, kun sekä sataa että tuulee kovasti.

Määritelmän 2.1.2 totuustaulusta nähdään, että disjunktio $A \vee B$ (luetaan "$A$ tai $B$") on epätosi täsmälleen siinä tapauksessa, että propositiolauseet $A$ ja $B$ ovat molemmat epätosia. Kaikissa muissa tapauksissa disjunktio on tosi. Vertaamalla tätä havaintoa edellisiin arkikielen esimerkkeihin huomataan, että disjunktio ei ole poissulkeva.

**Määritelmä 2.1.3.** Implikaatiolla $\rightarrow$ ja ekvivalenssilla $\leftrightarrow$ on seuraavat totuustaulut:

| $A$ | $B$ | $A \rightarrow B$ |
|---|---|---|
| 1 | 1 | 1 |
| 1 | 0 | 0 |
| 0 | 1 | 1 |
| 0 | 0 | 1 |

| $A$ | $B$ | $A \leftrightarrow B$ |
|---|---|---|
| 1 | 1 | 1 |
| 1 | 0 | 0 |
| 0 | 1 | 0 |
| 0 | 0 | 1 |

Määritelmän 2.1.3 totuustaulusta nähdään, että implikaatio $A \rightarrow B$ (luetaan "jos $A$, niin $B$") on epätosi vain yhdessä tapauksessa: *etujäsenen* $A$ ollessa tosi ja *takajäsenen* $B$ ollessa epätosi. Huomaa, että jos etujäsen $A$ on epätosi, on implikaatio $A \rightarrow B$ tosi riippumatta takajäsenen totuusarvosta.

Määritelmän 2.1.3 totuustaulusta nähdään, että ekvivalenssi $A \leftrightarrow B$ (luetaan "$A$ jos ja vain jos $B$") on tosi täsmälleen niissä tapauksissa, joissa propositiolauseilla $A$ ja $B$ on sama totuusarvo.

**Esimerkki 2.1.4.** Havainnollistetaan implikaation määritelmää tarkastelemalla lupausta ”jos saat kokeesta vähintään 40 pistettä, niin pääset kurssista läpi”. Se voidaan kirjoittaa propositiolauseena $p_0 \to p_1$, missä lause ”saat kokeesta vähintään 40 pistettä” on korvattu propositiosymbolilla $p_0$ ja lause ”pääset kurssista läpi” on korvattu propositiosymbolilla $p_1$. Tämä implikaatio on tosi seuraavissa tilanteissa:

– Saat kokeesta vähintään 40 pistettä ja pääset kurssista läpi. Implikaatio on tosi, sillä sekä sen etujäsen että takajäsen ovat tosia. Tämä tilanne vastaa määritelmässä 2.1.3 implikaation totuustaulun ylintä riviä. Tässä tapauksessa lupaus on pidetty.

– Saat kokeesta alle 40 pistettä ja pääset kurssista läpi. Implikaatio on tosi, sillä etujäsen on epätosi. Tämä tilanne vastaa määritelmässä 2.1.3 implikaation totuustaulun kolmatta riviä. Todellisessa elämässä tällainen tilanne saattaa syntyä, jos koe on esimerkiksi odotettua vaikeampi ja opettaja päättää laskea pisterajoja. Huomaa, että tarkasteltu lupaus ei sulje pois mahdollisuutta päästä kokeesta läpi alle 40 pisteellä.

– Saat kokeesta alle 40 pistettä etkä pääse kurssista läpi. Implikaatio on tosi, sillä etujäsen on epätosi. Tämä tilanne vastaa määritelmässä 2.1.3 implikaation totuustaulun alinta riviä. Tässäkään tapauksessa lupausta ei ole rikottu.

Tarkasteltava implikaatio on epätosi ainoastaan tilanteessa, jossa saat kokeesta vähintään 40 pistettä mutta et kuitenkaan pääse kurssia läpi. Tällöin lupausta ei ole pidetty. Tilanne vastaa määritelmän 2.1.3 implikaation totuustaulun toista riviä, jossa etujäsen on tosi ja takajäsen epätosi.

## 2.2 Looginen ekvivalenssi

Propositiolausetta, joka on aina tosi, sanotaan *tautologiaksi*. Tautologia tarkoittaa siis propositiolausetta, jonka totuusarvo on aina 1. Totuustaulun avulla voidaan tutkia, onko propositiolause tautologia. Esimerkiksi propositiolause $p_0 \vee \neg p_0$ on tautologia, mikä nähdään seuraavasta totuustaulusta:

| $p_0$ | $\neg p_0$ | $p_0 \vee \neg p_0$ |
|---|---|---|
| 1 | 0 | 1 |
| 0 | 1 | 1 |

Tautologian käsitteen avulla voidaan määritellä, mitä tarkoitetaan, kun sanotaan, että kaksi propositiolausetta ovat loogisesti ekvivalentit.

**Määritelmä 2.2.1.** Propositiolauseet $A$ ja $B$ ovat *loogisesti ekvivalentteja*, jos ekvivalenssi $A \leftrightarrow B$ on tautologia. Toisin sanottuna propositiolauseet $A$ ja $B$ ovat loogisesti ekvivalentteja, jos ekvivalenssin $A \leftrightarrow B$ totuusarvo on aina 1.

Huomaa, että määritelmästä 2.2.1 voidaan päätellä, että loogisesti ekvivalenttien propositiolauseiden totuusarvot ovat aina samat.

**Esimerkki 2.2.2.** Osoitetaan, että konjunktion negaatio $\neg(A \wedge B)$ on loogisesti ekvivalentti disjunktion $\neg A \vee \neg B$ kanssa. Laaditaan totuustaulu ekvivalenssille $(\neg(A \wedge B)) \leftrightarrow (\neg A \vee \neg B)$.

| $A$ | $B$ | $A \wedge B$ | $\neg(A \wedge B)$ | $\neg A$ | $\neg B$ | $\neg A \vee \neg B$ | $(\neg(A \wedge B)) \leftrightarrow (\neg A \vee \neg B)$ |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 |
| 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |
| 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |

Totuustaulusta nähdään, että propositiolauseilla $\neg(A \wedge B)$ ja $\neg A \vee \neg B$ on aina samat totuusarvot, joten niiden ekvivalenssin totuusarvo on aina 1. Propositiolauseet $\neg(A \wedge B)$ ja $\neg A \vee \neg B$ ovat siis loogisesti ekvivalentit. Voidaan ajatella, että ne ilmaisevat saman asian mutta eri tavoilla.

**Esimerkki 2.2.3.** Yritetään etsiä implikaation negaation $\neg(A \to B)$ kanssa loogisesti ekvivalentti propositiolause. Alla olevasta totuustaulusta nähdään, että implikaatio $A \to B$ on epätosi täsmälleen siinä tilanteessa, että propositiolause $A$ on tosi ja $B$ on epätosi:

| $A$ | $B$ | $A \to B$ |
|---|---|---|
| 1 | 1 | 1 |
| 1 | 0 | 0 |
| 0 | 1 | 1 |
| 0 | 0 | 1 |

Tämä vastaa tilannetta, jossa implikaation negaatio $\neg(A \to B)$ on tosi. Näin voidaan päätellä, että $\neg(A \to B)$ on loogisesti ekvivalentti konjuktion $A \wedge \neg B$ kanssa.

Tarkistetaan asia laatimalla totuustaulu ekvivalenssille $(\neg(A \to B)) \leftrightarrow (A \wedge \neg B)$:

| $A$ | $B$ | $A \to B$ | $\neg(A \to B)$ | $\neg B$ | $A \wedge \neg B$ | $(\neg(A \to B)) \leftrightarrow (A \wedge \neg B)$ |
|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 1 | 1 | 1 |
| 0 | 1 | 1 | 0 | 0 | 0 | 1 |
| 0 | 0 | 1 | 0 | 1 | 0 | 1 |

Totuustaulusta nähdään, että propositiolauseilla $\neg(A \to B)$ ja $A \wedge \neg B$ on aina samat totuusarvot, joten niiden ekvivalenssin totuusarvo on aina 1. Propositiolauseet $\neg(A \to B)$ ja $A \wedge \neg B$ ovat siis loogisesti ekvivalentit. Voidaan ajatella, että ne ilmaisevat saman asian mutta eri tavoilla.

Esimerkiksi implikaation ”jos aurinko paistaa, lähden Suomenlinnaan” negaatio on esimerkin 2.2.3 mukaan loogisesti ekvivalentti lauseen ”aurinko paistaa ja en lähde Suomenlinnaan” kanssa. Huomaa, että implikaation negaatio vastaa tilannetta, jossa alkuperäisen implikaation etujäsen on tosi mutta takajäsen ei.

**Esimerkki 2.2.4.** Implikaation $A \to B$ *kontrapositio* tarkoittaa implikaatiota $\neg B \to \neg A$. Osoitetaan totuustaulun avulla, että implikaatio ja sen kontrapositio ovat loogisesti ekvivalentit:

| $A$ | $B$ | $A \to B$ | $\neg B$ | $\neg A$ | $\neg B \to \neg A$ | $(A \to B) \leftrightarrow (\neg B \to \neg A)$ |
|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 0 | 0 | 1 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 1 |
| 0 | 1 | 1 | 0 | 1 | 1 | 1 |
| 0 | 0 | 1 | 1 | 1 | 1 | 1 |

Esimerkiksi implikaation ”jos aurinko paistaa, lähden Suomenlinnaan” kontrapositio on ”jos en lähde Suomenlinnaan, niin aurinko ei paista”. Se on esimerkin 2.2.4 nojalla loogisesti ekvivalentti alkuperäisen implikaation kanssa. Molemmat lauseet kertovat siis saman asian mutta eri sanoin.

## 2.3 Kvanttorit

Väite, jossa esiintyy niin sanottu *vapaa muuttuja*, voi olla jollakin muuttujan arvolla tosi ja jollakin muuttujan arvolla epätosi. Esimerkki tällaisesta väiteestä on $x^2 - 2x + 1 = 0$, jossa $x$ on vapaa muuttuja. Havaitaan, että jos esimerkiksi $x = 5$, tarkasteltava väite on epätosi, sillä $x^2 - 2x + 1 = 5^2 - 2 \cdot 5 + 1 = 16 \neq 0$. Toisaalta jos esimerkiksi $x = 1$, väite on tosi, sillä $x^2 - 2x + 1 = 1^2 - 2 \cdot 1 + 1 = 0$.

Vapaita muuttujia sisältävien väitteiden tapauksessa ollaan usein kiinnostuneita siitä, onko väite tosi kaikilla muuttujan arvoilla tai ainakin yhdellä muuttujan arvolla. Nämä asiat voidaan ilmaista niin sanottujen *kvanttoreiden* avulla. Ne on lueteltu alla taulukossa 2.2.

| Kaava | Merkitys |
|---|---|
| $\forall x A$ | $A$ pätee kaikilla muuttujan $x$ arvoilla |
| $\exists x A$ | $A$ pätee joillakin muuttujan $x$ arvoilla |

Taulukko 2.2: Kvanttorit

**Esimerkki 2.3.1.** Tulkitaan seuraavat kokonaislukuja koskevat väitteet suomen kielelle ja päätellään, ovatko ne tosia vai epätosia.

(a) Väite: $\exists x(3x - 12 = 3)$

Tulkinta: On olemassa kokonaisluku, joka toteuttaa yhtälön $3x - 12 = 3$.

Väite on tosi, sillä se toteutuu esimerkiksi, jos $x = 5$. Nimittäin $3 \cdot 5 - 12 = 15 - 12 = 3$.

(b) Väite: $\forall x(x < 2 \to x^2 < 4)$

Tulkinta: Kaikilla kokonaisluvuilla $x$ pätee, että jos $x < 2$, niin $x^2 < 4$.

Väite on epätosi, sillä jos esimerkiksi $x = -5$, niin implikaation etujäsen on tosi mutta takajäsen on epätosi: $-5 < 2$ mutta $(-5)^2 = 25 \geq 4$.

(c) Väite: $\exists x(x^2 = -1)$.

Tulkinta: On olemassa kokonaisluku, jonka toinen potenssi on $-1$.

Väite on epätosi, sillä kertolaskun laskusääntöjen nojalla kaikkien kokonaislukujen toinen potenssi on epänegatiivinen.

(d) Väite: $\forall x(x^2 + 3 > 1)$

Tulkinta: Kaikilla kokonaisluvuilla $x$ pätee, että $x^2 + 3 > 1$.

Väite on tosi. Perustelu: Oletetaan, että $x \in \mathbb{Z}$. Kaikkien kokonaislukujen toinen potenssi on aina epänegatiivinen, joten $x^2 \geq 0$. Tästä seuraa, että $x^2 + 3 \geq 3$. Voidaan päätellä, että tällöin $x^2 + 3 > 1$.

**Esimerkki 2.3.2.** Monet matematiikassa esiintyvät määritelmät voidaan muotoilla logiikan symbolikielellä. Tässä esimerkissä ilmaistaan joukkoja koskevia väitteitä kvanttoreiden ja muiden logiikan symboleiden avulla.

(a) Oletetaan, että $A$ ja $B$ ovat joukkoja. Tarkastellaan väitettä $A \subset B$.

Määritelmän 1.4.1 mukaan joukko $A$ on joukon $B$ osajoukko, jos joukon $A$ jokainen alkio on myös joukon $B$ alkio. Toisin sanottuna kaikkien alkioiden pitää täyttää ehto ”jos alkio kuuluu joukkoon $A$, niin se kuuluu joukkoon $B$”. Väite $A \subset B$ voidaan siis kirjoittaa muodossa $\forall x(x \in A \to x \in B)$.

(b) Oletetaan, että $B$ ja $C$ ovat joukkoja. Tarkastellaan väitettä $B \not\subset C$.

Osajoukon määritelmästä seuraa, että joukko $B$ ei ole joukon $C$ osajoukko, jos joukossa $B$ on yksikin alkio, joka ei kuulu joukkoon $C$. Väite $B \not\subset C$ voidaan siis kirjoittaa muodossa $\exists x(x \in B \land x \notin C)$.

(c) Oletetaan, että $A$, $B$ ja $C$ ovat joukkoja. Tarkastellaan väitettä $A \cap B \subset B \setminus C$.

Käytetään aluksi osajoukon määritelmää, jolloin väite voidaan kirjoittaa samaan tapaan kuin a-kohdassa: $\forall x(x \in A \cap B \to x \in B \setminus C)$. Yhdistämällä tähän leikkauksen ja joukkojen erotuksen määritelmät (ks. määritelmä 1.2.1) voidaan väite kirjoittaa muodossa $\forall x\big((x \in A \land x \in B) \to (x \in B \land x \notin C)\big)$ .

(d) Oletetaan, että $A$, $B$, $C$ ja $D$ ovat joukkoja. Tarkastellaan väitettä $A \setminus B = C \cup D$.

Määritelmän 1.6.1 mukaan kaksi joukkoa ovat samat, jos niissä on täsmälleen samat alkiot. Toisin sanottuna kaikkien alkioiden pitää täyttää ehto ”alkio kuuluu joukkoon

$A \setminus B$, jos ja vain jos alkio kuuluu joukkoon $C \cup D$". Tämän tiedon avulla alkuperäinen väite saadaan muotoon $\forall x(x \in A \setminus B \leftrightarrow x \in C \cup D)$. Soveltamalla vielä erotuksen ja yhdisteen määritelmiä päädytään muotoon $\forall x((x \in A \wedge x \notin B) \leftrightarrow (x \in C \vee x \in D))$.

## 2.4 Kvanttorit ja negaatiot

Väite "kaikki kissat ovat mustia" voidaan kumota vastaesimerkillä. Jos löydetään yksikin kissa, joka ei ole musta, osoittaa se edellä mainitun väitteen epätodeksi. Voidaan päätellä, että väitteen "kaikki kissat ovat mustia" negaatio on "on olemassa kissa, joka ei ole musta".

Toisaalta väitteen "on olemassa vihreä kissa" kumoaminen on työläämpää. Tämä väite saadaan näytettyä epätodeksi, jos osoittautuu, ettei yksikään kissa ole vihreä. Toisin sanottuna väitteen "on olemassa vihreä kissa" negaatio on "kaikilla kissoilla pätee, etteivät ne ole vihreitä".

Osoittautuu, että edelliset havainnot negaation vaikutuksesta kvanttoreihin pätevät yleisesti: kaavat $\neg\forall x A$ ja $\exists x \neg A$ ovat loogisesti ekvivalentteja, samoin kaavat $\neg\exists x A$ ja $\forall x \neg A$.

Kvanttoreita sisältävien väitteiden loogista ekvivalenssia ei voi tutkia totuustaulujen avulla. Lisätietoja predikaattilogiikan loogisen ekvivanlenssin käsitteestä löytyy esimerkiksi kirjasta Logiikka I

**Esimerkki 2.4.1.** Alla olevaan taulukkoon on koottu joitakin väitteitä ja niiden negaatioita sekä suomeksi että logiikan symbolikielellä.

| Väite | | Negaatio | |
|---|---|---|---|
| Joku on iloinen. | $\exists x I(x)$ | Kukaan ei ole iloinen. | $\forall x \neg I(x)$ |
| Kaikki ovat iloisia. | $\forall x I(x)$ | Joku ei ole iloinen. | $\exists x \neg I(x)$ |

**Esimerkki 2.4.2.** Monimutkaisempien väitteiden negaatioita voidaan muokata vaiheittain. Tarkastellaan esimerkiksi väitettä "kaikki iloiset ovat ahkeria". Logiikan symbolikielellä sama asia voidaan ilmaista kaavana $\forall x(I(x) \to A(x))$. Etsitään tämän kaavan negaation kanssa loogisesti ekvivanlentti kaava.

Negaatio $\neg\forall x(I(x) \to A(x))$ voidaan esimerkin 2.4.1 tapaan kirjoittaa loogisesti ekvivalentissa muodossa $\exists x \neg(I(x) \to A(x))$. Implikaation negaatio $\neg(I \to A)$ on puolestaan loogisesti ekvivalentti konjuktion $I \wedge \neg A$ kanssa (esim. 2.2.3). Soveltamalla tätä tietoa päädytään kaavaan $\exists x(I(x) \wedge \neg A(x))$. Suomeksi sama asia voidaan ilmaista väitteenä "joku on iloinen mutta ei ahkera".

| | Suomeksi | Logiikan symbolikielellä |
|---|---|---|
| Väite: | Kaikki iloiset ovat ahkeria. | $\forall x(I(x) \to A(x))$ |
| Negaatio: | Joku on iloinen mutta ei ole ahkera. | $\exists x(I(x) \wedge \neg A(x))$ |

**Esimerkki 2.4.3.** Tarkastellaan väitettä ”joku iloinen on ahkera”. Logiikan symbolikielellä sama asia voidaan ilmaista kaavana $\exists x(I(x) \wedge A(x))$. Etsitään tämän kaavan negaation kanssa loogisesti ekvivanlentti kaava.

Negaatio $\neg\exists x(I(x) \wedge A(x))$ voidaan esimerkin 2.4.1 tapaan kirjoittaa loogisesti ekvivalentissa muodossa $\forall x\neg(I(x) \wedge A(x))$. Konjuktion negaatio $\neg(I \wedge A)$ on puolestaan loogisesti ekvivalentti disjuktion $\neg I \vee \neg A$ kanssa (esim. 2.2.2). Näin päädytään kaavaan $\forall x(\neg I(x) \vee \neg A(x))$. Suomeksi tämän voidaan ajatella vastaavan väitettä ”jokainen on surullinen tai laiska”.

Totuustaulujen avulla voidaan osoittaa, että konjunktion negaatio $\neg(I \wedge A)$ on loogisesti ekvivalentti myös implikaation $I \rightarrow \neg A$ kanssa. Tämä voidaan päätellä myös esimerkistä 2.4.2 korvaamalla propositiolause $A$ propositiolauseella $\neg A$. Käyttämällä tätä tietoa saadaan kaava $\forall x\neg(I(x) \wedge A(x))$ loogisesti ekvivalenttiin muotoon $\forall x(I(x) \rightarrow \neg A(x))$. Suomeksi sama asia voidaan ilmaista väitteenä ”kukaan iloinen ei ole ahkera”.

| | Suomeksi | Logiikan symbolikielellä |
|---|---|---|
| Väite: | Joku iloinen on ahkera. | $\exists x(I(x) \wedge A(x))$ |
| Negaatioita: | Jokainen on surullinen tai laiska | $\forall x(\neg I(x) \vee \neg A(x))$ |
| | Kukaan iloinen ei ole ahkera. | $\forall x(I \rightarrow \neg A)$ |

## 2.5 Kvanttorien järjestys

Jos väitteessä on useampia muuttujia, saatetaan kvanttoreitakin tarvita enemmän kuin yksi. Kvanttoreiden järjestys vaikuttaa oleellisesti väitteen merkitykseen. Tätä havainnollistetaan seuraavissa esimerkeissä.

**Esimerkki 2.5.1.** Tulkitaan seuraavat kokonaislukuja koskevat väitteet suomen kielelle ja päätellään, ovatko ne tosia vai epätosia.

(a) Väite: $\forall x\exists y(x + y = 5)$.

Tulkinta: Jokaista kokonaislukua $x$ kohti on olemassa jokin sellainen kokonaisluku $y$, että lukujen $x$ ja $y$ summa on 5.

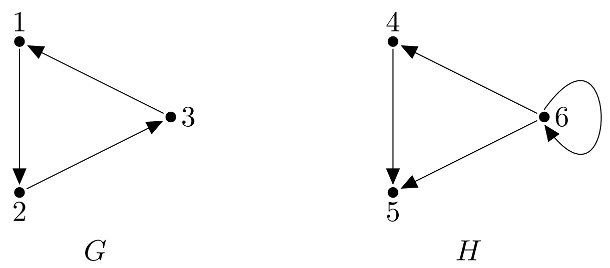
Väite on tosi, sillä olipa $x$ mikä tahansa kokonaisluku, voidaan aina valita $y = 5 - x$. Tällöin $y$ on kokonaisluku ja $x + y = x + (5 - x) = 5$.

(b) Väite: $\exists y\forall x(x + y = 5)$.

Tulkinta: On olemassa sellainen kokonaisluku $y$, että sen ja minkä tahansa kokonaisluvun $x$ summa on 5.

Väite on epätosi. Perustelu: Jos väitetty luku $y$ olisi olemassa, se tarkoittaisi, että esimerkiksi $y+0 = 5$ ja $y+1 = 5$. Ensimmäisestä yhtälöstä seuraa, että $y = 5$. Toisesta taas seuraa, että $y = 4$. Yhdistämällä nämä tiedot päädytään ristiriitaan $5 = 4$. Väitteessä mainittua lukua $y$ ei siis voi olla olemassa.

**Esimerkki 2.5.2.** Tarkastellaan alla olevia suunnattuja verkkoja $G$ ja $H$. Merkintä $R(x, y)$ tarkoittaa tässä esimerkissä, että solmusta $x$ on nuoli solmuun $y$. Esimerkiksi verkossa $G$ pätee $R(2, 3)$, sillä solmusta 2 on nuoli solmuun 3.




Tutkitaan, onko väite $\forall x \exists y R(x, y)$ tosi verkoissa $G$ ja $H$.

$G$: väite on tosi, sillä verkon $G$ jokaisesta solmusta on nuoli johonkin solmuun.

$H$: väite on epätosi, sillä solmusta 5 ei ole nuolta mihinkään solmuun.

Tutkitaan, onko väite $\exists x \forall y R(x, y)$ tosi verkoissa $G$ ja $H$.

$G$: väite on epätosi, sillä mistään verkon $G$ solmusta ei ole nuolta kaikkiin solmuihin.

$H$: väite on tosi, sillä solmusta 6 on nuoli kaikkiin solmuihin.

Huomaa, että voi olla $y = x$. Esimerkiksi väite $\exists x \forall y R(x, y)$ olisi epätosi myös verkossa $H$, jos solmusta 6 ei olisi nuolta siihen itseensä.

# 3 Todistustekniikkaa

## 3.1 Väitteen kumoaminen vastaesimerkillä

Monissa tilanteissa kohdataan väitteitä, jotka koskevat esimerkiksi kaikkia kokonaislukuja, kaikkia reaalilukuja tai kaikkia joukkoja. Esimerkkejä tällaisista väitteistä ovat vaikkapa seuraavat:

- Jokaisen parittoman kokonaisluvun toinen potenssi on pariton.
- Kaikilla $a, b \in \mathbb{R}$ pätee, että $(a+b)^2 = a^2 + 2ab + b^2$.
- Kaikilla joukoilla $A$ ja $B$ pätee, että $(A \cup B) \setminus B \subset A$.

Yllä mainitut väitteet ovat kaikki tosia, mutta toisinaan vastaan tulee myös samantyyppisiä epätosia väitteitä kuten

- Kaikilla $n \in \mathbb{Z}$ pätee, että luku $n^2 - n + 11$ on alkuluku.
- Kaikilla $a, b \in \mathbb{R}$ pätee, että $(a+b)^2 = a^2 + b^2$.
- Kaikilla joukoilla $A$ ja $B$ pätee, että $(A \cup B) \setminus B = A$.

Tällaisten väitteiden kumoaminen onnistuu vastaesimerkin avulla. Sitä havainnollistetaan seuraavissa esimerkessä. Määritellään kuitenkin ensin, mitä alkuluvun käsitteellä tarkoitetaan.

**Määritelmä 3.1.1.** Kokonaisluku $p > 1$ on *alkuluku*, jos sen ainoat positiiviset tekijät ovat 1 ja $p$.

Huomaa, että määritelmän mukaan luku 1 ei ole alkuluku. Pienimmät alkuluvut ovat 2 ja 3. Esimerkiksi luvut 4 ja 35 eivät ole alkulukuja, sillä $4 = 2 \cdot 2$ ja $35 = 5 \cdot 7$.

**Esimerkki 3.1.2.** Tarkastellaan väitettä, jonka mukaan luku $n^2 - n + 11$ on alkuluku kaikilla $n \in \mathbb{Z}$. Osoitetaan väite epätodeksi antamalla vastaesimerkki. Kokeilemalla tai muuten järkeilemällä huomataan, että jos $n = 11$, niin

$$n^2 - n + 11 = 11^2 - 11 + 11 = 11^2 = 11 \cdot 11,$$

joka ei ole alkuluku. Siis väite on epätosi.

Huomaa, että joidenkin kokonaislukujen tapauksessa $n^2 - n + 11$ on alkuluku. Esimerkiksi luvun $n = 2$ tapauksessa $n^2 - n + 11 = 13$, joka on alkuluku.

**Esimerkki 3.1.3.** Tarkastellaan väitettä, jonka mukaan $(a+b)^2 = a^2 + b^2$ kaikilla $a, b \in \mathbb{R}$. Osoitetaan väite epätodeksi antamalla vastaesimerkki. Valitaan esimerkiksi $a = 1$ ja $b = 2$. Tällöin yhtälön vasen puoli on $(a+b)^2 = 3^2 = 9$ ja oikea puoli on $a^2 + b^2 = 1^2 + 2^2 = 5$. Siis tässä tapauksessa $(a+b)^2 \neq a^2 + b^2$. Väite on siis epätosi.

Huomaa, että joillakin luvuilla väitetty yhtälö kuitenkin pätee. Esimerkiksi jos $a = 0$ ja $b = 1$, on yhtälön vasen puoli $(a+b)^2 = 1^2 = 1$ ja oikea puoli $a^2 + b^2 = 0^2 + 1^2 = 1$. Siis tässä tapauksessa yhtälö pätee.

**Esimerkki 3.1.4.** Tarkastellaan väitettä, jonka mukaan kaikilla joukoilla $A$, $B$ ja $C$ pätee yhtälö $A \cup (B \cap C) = (A \cup B) \cap C$.

Kumotaan väite vastaesimerkin avulla. Valitaan vaikkapa $A = \{1, 2\}$, $B = \{2, 3\}$ ja $C = \{1, 3\}$. Tällöin $A \cup (B \cap C) = \{1, 2\} \cup \{3\} = \{1, 2, 3\}$ ja $(A \cup B) \cap C = \{1, 2, 3\} \cap \{1, 3\} = \{1, 3\}$. Siis tässä tapauksessa $A \cup (B \cap C) \neq (A \cup B) \cap C$. Väite on siis epätosi.

Voidaanko siis päätellä, että $A \cup (B \cap C) \neq (A \cup B) \cap C$ kaikilla joukoilla $A$, $B$ ja $C$?

Näytetään vastaesimerkin avulla, että näinkään ei voida päätellä. Valitaan $A = \{1, 2\}$, $B = \{2\}$ ja $C = \{1, 2\}$. Tällöin $A \cup (B \cap C) = \{1, 2\} \cup \{2\} = \{1, 2\}$ ja $(A \cup B) \cap C = \{1, 2\} \cap \{1, 2\} = \{1, 2\}$. Siis tässä tapauksessa $A \cup (B \cap C) = (A \cup B) \cap C$.

## 3.2 ”Jos . . . , niin . . . ” -tyyppisen väitteen todistaminen

Tässä kappaleessa perehdytään siihen, miten ”jos $P$, niin $Q$” -tyyppisiä väitteitä todistetaan. Esimerkkejä tällaisista väitteistä ovat vaikkapa seuraavat:

- Jos $a, b \in \mathbb{R}$ ja $0 < a < b$, niin $a^2 < b^2$.
- Jos kokonaisluku $m$ on parillinen, niin $m^2$ on parillinen.
- Jos joukoilla $A$ ja $B$ pätee $A \subset B$, niin $A \cup B = B$.

Väite ”jos $P$, niin $Q$” vastaa implikaatiota $P \to Q$, jolla on määritelmän 2.1.3 mukaan seuraava totuustaulu:

| $P$ | $Q$ | $P \to Q$ |
|---|---|---|
| 1 | 1 | 1 |
| 1 | 0 | 0 |
| 0 | 1 | 1 |
| 0 | 0 | 1 |

Totuustaulusta nähdään, että implikaatio $P \to Q$ on epätosi täsmälleen yhdessä tilanteessa: silloin, kun sen etujäsen $P$ on tosi ja takajäsen $Q$ on epätosi (totuustaulun toisella rivillä). Implikaation $P \to Q$ todistamiseksi pitää siis osoittaa, että tämä tilanne ei koskaan toteudu.

Totuustaulusta nähdään myös, että implikaatio $P \to Q$ on tosi niissä tapauksissa, joissa sen etujäsen $P$ on epätosi (totuustaulun kolmannella ja neljännellä rivillä). Näistä tapauksista ei siis tarvitse huolehtia, vaan riittää keskittyä tarkastelemaan tilannetta, jossa etujäsen $P$ on tosi.

Väite ”jos $P$, niin $Q$” voidaan todistaa seuraavasti:
- Oletetaan, että etujäsen $P$ on tosi. Toisin sanottuna oletetaan, että $P$ pätee.
- Päätellään, että tällöin myös $Q$ pätee.

**Esimerkki 3.2.1.** Oletetaan, että $a$, $b \in \mathbb{R}$. Osoitetaan, että jos $0 < a < b$, niin $a^2 < b^2$.

Oletetaan, että tarkasteltavan implikaation etujäsen on tosi. Toisin sanottuna oletetaan, että $0 < a < b$. Tavoitteena on näyttää, että tällöin myös implikaation takajäsen on tosi. Toisin sanottuna tavoitteena on näyttää, että $a^2 < b^2$.

Oletuksen mukaan $a < b$. Tämän epäyhtälön molemmat puolet voidaan kertoa luvulla $a$. Koska oletuksen mukaan $a > 0$, epäyhtälön suunta säilyy. Saadaan siis uusi epäyhtälö

$$a^2 < ab.$$

Toisaalta epäyhtälön $a < b$ molemmat puolet voidaan kertoa luvulla $b$. Koska oletuksen mukaan myös $b > 0$, epäyhtälön suunta säilyy. Saadaan siis uusi epäyhtälö

$$ab < b^2.$$

Yhdistämällä näiden epäyhtälöiden tiedot voidaan päätellä, että $a^2 < ab < b^2$, joten $a^2 < b^2$.

Väite ”jos $0 < a < b$, niin $a^2 < b^2$” on nyt todistettu, sillä saatiin näytettyä, että oletuksesta $0 < a < b$ seuraa $a^2 < b^2$.

---

Ennen seuraavaa esimerkkiä määritellään, mitä tarkoitetaan parillisella ja parittomalla kokonaisluvulla.

**Määritelmä 3.2.2.** Kokonaisluku $m$ on *parillinen*, jos se voidaan kirjoittaa muodossa $m = 2k$, missä $k \in \mathbb{Z}$. Kokonaisluku $m$ on *pariton*, jos se voidaan kirjoittaa muodossa $m = 2k + 1$, missä $k \in \mathbb{Z}$.

Esimerkiksi luku 8 on parillinen, sillä $8 = 2 \cdot 4$, missä $4 \in \mathbb{Z}$. Luku 13 on puolestaan pariton, sillä $13 = 2 \cdot 6 + 1$, missä $6 \in \mathbb{Z}$.

**Esimerkki 3.2.3.** Osoitetaan, että jos kokonaisluku $m$ on parillinen, niin $m^2$ on parillinen.

Oletetaan, että tarkasteltavan implikaation etujäsen on tosi. Toisin sanottuna oletetaan, että kokonaisluku $m$ on parillinen. Tavoitteena on näyttää, että tällöin myös implikaation takajäsen on tosi. Toisin sanottuna tavoitteena on näyttää, että $m^2$ on parillinen.

Koska kokonaisluku $m$ on parillinen, se voidaan kirjoittaa muodossa $m = 2k$, missä $k \in \mathbb{Z}$. Tällöin

$$m^2 = (2k)^2 = 4k^2 = 2 \cdot 2k^2,$$

missä $2k^2 \in \mathbb{Z}$, sillä se on kokonaislukujen tulo. Luku $m^2$ on siis kaksi kertaa jokin kokonaisluku, joten se on parillinen.

Väite ”jos kokonaisluku $m$ on parillinen, niin $m^2$ on parillinen” on nyt todistettu, sillä saatiin näytettyä, että oletuksesta $m$ on parillinen seuraa, että $m^2$ on parillinen.

**Esimerkki 3.2.4.** Olkoot $A$ ja $B$ joukkoja. Osoitetaan, että jos $A \subset B$, niin $A \cup B = B$.

Oletetaan, että tarkasteltavan implikaation etujäsen on tosi. Toisin sanottuna oletetaan, että $A \subset B$. Tavoitteena on näyttää, että tällöin myös implikaation takajäsen on tosi. Toisin sanottuna tavoitteena on näyttää, että $A \cup B = B$. Koska kysymyksessä on joukkojen identtisyys, osoitetaan sisältyminen molempiin suuntiin. Käytetään kappaleessa 1.6 opiskeltua tekniikkaa.

”$\subset$”: Oletetaan, että $x \in A \cup B$. Tästä voidaan yhdisteen määritelmän nojalla päätellä, että $x \in A$ tai $x \in B$. Koska ei voida olla varmoja, kumpi näistä vaihtoehdoista pätee, täytyy tehdä tapaustarkastelu. Sen avulla varmistetaan, että jokaisessa mahdollisessa tapauksessa päädytään haluttuun johtopäätökseen.

- Oletetaan, että $x \in A$. Todistuksen alussa tehdyn oletuksen mukaan $A \subset B$. Siis jokainen joukon $A$ alkio kuuluu myös joukkoon $B$. Näin voidaan päätellä, että $x \in B$.
- Oletetaan, että $x \in B$. Tässäkin tapauksessa $x \in B$.

Siis molemmissa tapauksissa $x \in B$. Näin on osoitettu, että $A \cup B \subset B$.

Huomaa, että matematiikan ”tai” ei ole poissulkeva, vaan edellä on mahdollista, että tarkasteltava alkio kuuluu sekä joukkoon $A$ että joukkoon $B$. Tätä tapausta ei kuitenkaan tarvitse käsitellä erikseen, sillä käsitellyt tapaukset kattavat myös sen. Esimerkiksi ensimmäisessä tapauksessa oletetaan, että $x \in A$ eikä oteta mitään kantaa siihen, kuuluuko $x$ joukkoon $B$ vai ei.

”$\supset$”: Oletetaan, että $x \in B$. Tällöin yhdisteen määritelmän nojalla voidaan päätellä, että $x \in A \cup B$. Tämä osoittaa, että $B \subset A \cup B$.

Päättelyt ”$\subset$” ja ”$\supset$” yhdessä osoittavat, että $A \cup B = B$.

Väite ”jos $A \subset B$, niin $A \cup B = B$” on nyt todistettu, sillä saatiin näytettyä, että oletuksesta $A \subset B$ seuraa $A \cup B = B$.

**Esimerkki 3.2.5.** Oletetaan, että $A$, $B$ ja $C$ ovat joukkoja. Osoitetaan, että jos $A \subset B$ ja $A \not\subset C$, niin $B \not\subset C$.

Oletetaan, että tarkasteltavan implikaation etujäsen on tosi. Toisin sanottuna oletetaan, että $A \subset B$ ja $A \not\subset C$. Tavoitteena on näyttää, että tällöin myös implikaation takajäsen on tosi. Toisin sanottuna tavoitteena on näyttää, että $B \not\subset C$. Yritetään löytää alkio, joka kuuluu joukkoon $B$ mutta ei kuulu joukkoon $C$.

Oletuksen mukaan $A \not\subset C$, joten voidaan päätellä, että on olemassa $a \in A$, jolle pätee $a \notin C$. Toisaalta oletuksen mukaan $A \subset B$, joten jokainen joukon $A$ alkio kuuluu joukkoon $B$. Näin ollen erityisesti $a \in B$. Siis olemassa alkio $a \in B$, jolla pätee $a \notin C$. Tästä voidaan päätellä, että $B \not\subset C$. (Vrt. esim. 1.4.5 ja 1.4.7.)

Väite ”jos $A \subset B$ ja $A \not\subset C$, niin $B \not\subset C$” on nyt todistettu, sillä saatiin näytettyä, että oletuksesta $A \subset B$ ja $A \not\subset C$ seuraa $B \not\subset C$.

## 3.3 ”Jos ja vain jos” -tyyppisen väitteen todistaminen

Tässä kappaleessa perehdytään siihen, miten ”$P$ jos ja vain jos $Q$” -tyyppisiä väitteitä todistetaan. Esimerkkejä tällaisista väitteistä ovat vaikkapa seuraavat:

– Kokonaisluvulle $n$ pätee $6 \mid n$, jos ja vain jos $2 \mid n$ ja $3 \mid n$.

– Yhtälö $x^2 - 6x + 9 = 0$ toteutuu, jos ja vain jos $x = 3$.

– Joukoilla $A$, $B$ ja $X$ pätee $X \subset A \cap B$, jos ja vain jos $X \subset A$ ja $X \subset B$.

Väite ”$P$ jos ja vain jos $Q$” vastaa ekvivalenssia $P \leftrightarrow Q$, jolla on määritelmän 2.1.3 mukaan seuraava totuustaulu:

| $P$ | $Q$ | $P \leftrightarrow Q$ |
|---|---|---|
| 1 | 1 | 1 |
| 1 | 0 | 0 |
| 0 | 1 | 0 |
| 0 | 0 | 1 |

Totuustaulusta nähdään, että ekvivalenssi $P \leftrightarrow Q$ on epätosi tapauksissa, joissa $P$:llä ja $Q$:lla on eri totuusarvot (totuustaulun toisella ja kolmannella rivillä). Ekvivalenssin $P \leftrightarrow Q$ todistamiseksi pitää siis osoittaa, että tällaiset tapaukset eivät koskaan toteudu.

Totuustaulusta nähdään myös, että ekvivalenssi $P \leftrightarrow Q$ on tosi tapauksessa, jossa sekä $P$ että $Q$ ovat epätosia (totuustaulun neljännellä rivillä). Tästä tapauksesta ei siis tarvitse huolehtia.

Väite ”$P$ jos ja vain jos $Q$” todistetaan kahdessa osassa:

– Oletetaan, että $P$ pätee. Päätellään, että tällöin myös $Q$ pätee.

– Oletetaan, että $Q$ pätee. Päätellään, että tällöin myös $P$ pätee.

Huomaa, että väitteen ”$P$ jos ja vain jos $Q$” todistus muodostuu todistuksesta implikaatiolle ”jos $P$, niin $Q$” ja implikaatiolle ”jos $Q$, niin $P$’. Nämä todistuksen osat voidaan erottaa toisistaan merkeillä ”$\Rightarrow$” ja ”$\Leftarrow$”. Niiden avulla on helpompi muistaa, kumpaa suuntaa ollaan todistamassa. Näin on tehty myös seuraavissa esimerkeissä.

**Esimerkki 3.3.1.** Oletetaan, että $n \in \mathbb{Z}$. Osoitetaan, että luku 6 jakaa luvun $n$, jos ja vain jos sekä luku 2 että luku 3 jakavat luvun $n$.

”$\Rightarrow$”: Oletetaan, että $6 \mid n$. Jaollisuuden määritelmän 4.1.3 mukaan tällöin on olemassa sellainen $a \in \mathbb{Z}$, että $n = 6a$. Voidaan siis kirjoittaa $n = 2 \cdot 3a$, missä $3a \in \mathbb{Z}$ kahden kokonaisluvun tulona. Näin $2 \mid n$. Toisaalta voidaan kirjoittaa $n = 3 \cdot 2a$, missä $2a \in \mathbb{Z}$. Näin $3 \mid n$.

”$\Leftarrow$”: Oletetaan, että $2 \mid n$ ja $3 \mid n$. Jaollisuuden määritelmän 4.1.3 mukaan tällöin on olemassa sellainen $a \in \mathbb{Z}$, että $n = 2a$, ja sellainen $b \in \mathbb{Z}$, että $n = 3b$.

Kirjoittamalla $n$ erotuksena $3n - 2n$ saadaan pääteltyä seuraavasti:

$$n = 3n - 2n = 3 \cdot 2a - 2 \cdot 3b = 6a - 6b = 6(a - b),$$

missä $a - b \in \mathbb{Z}$ kahden kokonaisluvun erotuksena. Siis 6 jakaa luvun $n$.

**Esimerkki 3.3.2.** Osoitetaan, että yhtälö $x^2 - 6x + 9 = 0$ toteutuu, jos ja vain jos $x = 3$.

”$\Rightarrow$”: Oletetaan, että yhtälö $x^2 - 6x + 9 = 0$ toteutuu. Sen vasen puoli voidaan kirjoittaa muodossa $(x-3)^2$, sillä

$$(x-3)^2 = (x-3)(x-3) = x^2 - 3x - 3x + 9 = x^2 - 6x + 9.$$

Yhtälö saadaan siis muotoon $(x-3)^2 = 0$. Nolla on ainoa luku, jonka toinen potenssi on nolla, joten voidaan päätellä, että $x - 3 = 0$. Siten $x = 3$.

”$\Leftarrow$”: Oletetaan, että $x = 3$. Tällöin

$$x^2 - 6x + 9 = 3^2 - 6 \cdot 3 + 9 = 9 - 18 + 9 = 0.$$

Siis yhtälö $x^2 - 6x + 9 = 0$ toteutuu.

**Esimerkki 3.3.3.** Oletetaan, että $X$ on joukko ja $A$, $B \subset X$. Osoitetaan, että $A \subset B$, jos ja vain jos $\complement A \cup B = X$.

”$\Rightarrow$”: Oletetaan, että $A \subset B$. Pitää näyttää, että tällöin $\complement A \cup B = X$. Tehdään tämä osoittamalla sisältyminen molempiin suuntiin.

”$\subset$”: Oletetaan, että $s \in \complement A \cup B$. Tästä voidaan yhdisteen määritelmän nojalla päätellä, että $s \in \complement A$ tai $s \in B$. Koska täytyy varmistua siitä, että oikeaan lopputulokseen päästään kaikissa mahdollisissa tilanteissa, tehdään tapaustarkastelu:

- Oletetaan, että $s \in \complement A$. Tällöin komplementin määritelmän nojalla $s \in X$ ja $s \notin A$. Tässä tapauksessa siis $s \in X$.
- Oletetaan, että $s \in B$. Alun oletusten mukaan $B \subset X$, joten jokainen joukon $B$ alkio kuuluu joukkoon $X$. Siis erityisesti $s \in X$.

Siis kaikissa mahdollisissa tapauksissa $s \in X$.

”$\supset$”: Oletetaan, että $m \in X$. Tästä on vaikea edetä suoraan, joten lähdetään miettimään asiaa joukkoon $A$ kuulumisen kannalta. Voidaan olla varmoja, että joko $m \in A$ tai $m \notin A$. Muita vaihtoehtoja ei ole, eivätkä mainintut kaksi vaihtoehtoa voi olla voimassa yhtä aikaa. Tutkitaan ne erikseen:

- Oletetaan, että $m \in A$. Todistuksen alussa tehdyn oletuksen mukaan $A \subset B$, joten voidaan päätellä, että $m \in B$.
- Oletetaan, että $m \notin A$. Kuitenkin oletuksen mukaan $m \in X$. Tällöin komplementin määritelmän mukaan $m \in \complement A$.

Molemmissa tapauksissa voidaan yhdisteen määritelmän nojalla päätellä, että $m \in \complement A \cup B$.

"$\Leftarrow$": Oletetaan, että $\complement A \cup B = X$. Pitää osoittaa, että tällöin $A \subset B$. Pitää siis näyttää, että jokainen joukon $A$ alkio kuuluu myös joukkoon $B$.

Oletetaan, että $a \in A$. Oletuksen mukaan $A \subset X$, joten voidaan päätellä, että $a \in X$. Lisäksi oletuksen mukaan $X = \complement A \cup B$. Yhdistämällä nämä tiedot saadaan pääteltyä, että $a \in \complement A \cup B$. Tästä seuraa yhdisteen määritelmän nojalla, että $a \in \complement A$ tai $a \in B$. Oletuksen mukaan kuitenkin $a \in A$, joten ensimmäinen vaihtoehto $a \in \complement A$ ei voi olla totta. Siis $a \in B$.

---

Seuraavaa osajoukkoihin liittyvää lemmaa käytettiin esimerkissä 1.8.4. Lemma tarkoittaa apulausetta eli todistettua tulosta, jota käytetään jonkin toisen, yleensä merkittävämmän tuloksen todistamiseen.

**Lemma 3.3.4.** *Oletetaan, että $A$, $B$ ja $X$ ovat joukkoja. Tällöin $X \subset A \cap B$, jos ja vain jos $X \subset A$ ja $X \subset B$.*

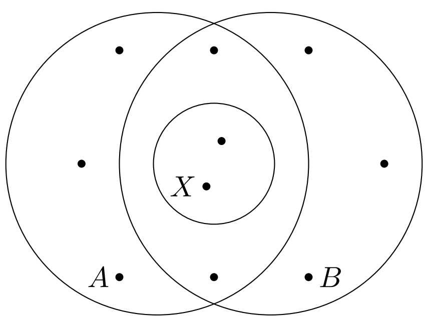
*Todistus.* "$\Rightarrow$": Oletetaan, että $X \subset A \cap B$. Pitää osoittaa, että $X \subset A$ ja $X \subset B$. Toisin sanottuna pitää näyttää kaksi asiaa: ensiksi, että jokainen joukon $X$ alkio kuuluu myös joukkoon $A$, ja toiseksi, että jokainen joukon $X$ alkio kuuluu myös joukkoon $B$.

Oletetaan, että $x \in X$. Oletuksen mukaan $X \subset A \cap B$, joten voidaan päätellä, että $x \in A \cap B$. Leikkauksen määritelmän nojalla tästä seuraa, että $x \in A$ ja $x \in B$.

Edellinen päättely osoittaa, että jokainen joukon $X$ alkio kuuluu joukkoon $A$. Siis $X \subset A$. Samoin se osoittaa, että jokainen joukon $X$ alkio kuuluu joukkoon $B$. Siis $X \subset B$.

"$\Leftarrow$": Oletetaan, että $X \subset A$ ja $X \subset B$. Pitää osoittaa, että $X \subset A \cap B$. Toisin sanottuna pitää näyttää, että jokainen joukon $X$ alkio kuuluu joukkoon $A \cap B$.

Oletetaan, että $x \in X$. Koska oletuksen mukaan $X \subset A$, niin $x \in A$. Vastaavasti koska oletuksen mukaan $X \subset B$, niin $x \in B$. Siis $x$ kuuluu sekä joukkoon $A$ että joukkoon $B$, joten leikkauksen määritelmän nojalla $x \in A \cap B$. $\square$




Kuva 3.1: $X \subset A \cap B$, jos ja vain jos $X \subset A$ ja $X \subset B$.

## 3.4 Kontrapositiotodistus

Kappaleessa 3.2 perehdyttiin ”jos $P$, niin $Q$” -tyyppisten väitteiden todistamiseen. Tässä kappaleessa tutustutaan tapaan todistaa tällaisia väitteitä epäsuorasti.

Esimerkissä 2.2.4 osoitettiin totuustaulujen avulla, että implikaatio $P \to Q$ ja sen kontrapositio $\neg Q \to \neg P$ ovat loogisesti ekvivalentit eli niillä on täsmälleen samat totuusarvot. Ne sanovat siis saman asian, mutta eri tavalla.

| $P$ | $Q$ | $P \to Q$ | $\neg Q$ | $\neg P$ | $\neg Q \to \neg P$ |
|---|---|---|---|---|---|
| 1 | 1 | 1 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 |
| 0 | 1 | 1 | 0 | 1 | 1 |
| 0 | 0 | 1 | 1 | 1 | 1 |

Taulukko 3.1: Implikaatio ja sen kontrapositio ovat loogisesti ekvivalentit.

Implikaatio $P \to Q$ voidaankin todistaa näyttämällä, että sen kontrapositio $\neg Q \to \neg P$ on tosi. Tämä tehdään kappaleessa 3.2 esitetyllä tavalla: olettamalla, että etujäsen $\neg Q$ on tosi, ja näyttämällä, että tällöin myös takajäsen $\neg P$ on tosi.

Kontrapositiotodistus väitteelle ”jos $P$, niin $Q$” rakentuu seuraavasti:

- Oletetaan, että $\neg Q$ on tosi.
- Päätellään, että tällöin myös $\neg P$ on tosi.

**Esimerkki 3.4.1.** Oletetaan, että $m \in \mathbb{Z}$. Osoitetaan, että jos $m^2$ on parillinen, niin $m$ on parillinen. Tehdään kontrapositiotodistus.

Oletetaan, että $m$ ei ole parillinen. Tällöin $m$ on pariton, joten $m = 2k + 1$ jollakin $k \in \mathbb{Z}$. Tästä seuraa, että

$$m^2 = (2k+1)^2 = (2k+1)(2k+1) = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1,$$

missä $2k^2 + 2k \in \mathbb{Z}$. Siis $m^2$ on pariton. Toisin sanottuna $m^2$ ei ole parillinen.

Näin on todistettu, että jos $m$ ei ole parillinen, niin $m^2$ ei ole parillinen. Tämä on alkuperäisen väitteen kontrapositio, joten myös alkuperäinen väite on todistettu.

**Esimerkki 3.4.2.** Oletetaan, että $A$ ja $B$ ovat joukkoja. Osoitetaan, että jos $A \cup B = B$, niin $A \subset B$. Tehdään kontrapositiotodistus.

Oletetaan, että $A \not\subset B$. Tällöin on olemassa $a \in A$, jolla pätee $a \notin B$. Koska $a \in A$, niin $a \in A \cup B$. Toisaalta $a \notin B$. Siis $A \cup B \neq B$.

Näin on todistettu, että jos $A \not\subset B$, niin $A \cup B \neq B$. Tämä on alkuperäisen väitteen kontrapositio, joten myös alkuperäinen väite on todistettu.

## 3.5 Ristiriitatodistus

Kappaleessa 3.4 tutustuttiin kontrapositiotodistukseen, joka on yksi epäsuoran päättelyn tyyppi. Tässä kappaleessa perehdytään toiseen epäsuoran päättelyn tyyppiin, ristiriitatodistukseen. Kontrapositiotodistuksella voitiin todistaa ”jos $P$, niin $Q$”-tyyppisiä väitteitä. Ristiriitatodistus puolestaan soveltuu kaikenlaisten väitteiden todistamiseen.

Ristiriitatodistus väitteelle $P$ rakentuu seuraavasti:

- Tehdään vastaoletus eli oletetaan, että $\neg P$ on tosi.
- Päätellään ristiriita $C \wedge \neg C$.

Ristiriitatodistuksessa siis todistetaan implikaatio $\neg P \to (C \wedge \neg C)$. Alla olevasta taulukosta 3.2 nähdään, että se on loogisesti ekvivalentti alkuperäisen väitteen $P$ kanssa.

| $P$ | $C$ | $\neg P$ | $C \wedge \neg C$ | $\neg P \to (C \wedge \neg C)$ |
|---|---|---|---|---|
| 1 | 1 | 0 | 0 | 1 |
| 1 | 0 | 0 | 0 | 1 |
| 0 | 1 | 1 | 0 | 0 |
| 0 | 0 | 1 | 0 | 0 |

Taulukko 3.2: Propositiolauseet $P$ ja $\neg P \to (C \wedge \neg C)$ ovat loogisesti ekvivalentit.

**Esimerkki 3.5.1.** Osoitetaan, että kaikilla kokonaisluvuilla $a$ ja $b$ pätee $a^2 - 4b \neq 2$.

Tehdään vastaoletus, että on olemassa kokonaisluvut $a$ ja $b$, joilla $a^2 - 4b = 2$. Tällöin

$$a^2 = 2 + 4b = 2(1 + 2b),$$

missä $1 + 2b \in \mathbb{Z}$. Siis $a^2$ on parillinen. Tästä seuraa esimerkin 3.4.1 nojalla, että myös luku $a$ on parillinen. Toisin sanottuna $a = 2k$, missä $k \in \mathbb{Z}$.

Alkuperäinen yhtälö $a^2 - 4b = 2$ voidaan nyt kirjoittaa muodossa $(2k)^2 - 4b = 2$ eli $4k^2 - 4b = 2$. Jakamalla yhtälön molemmat puolet luvulla 2 päästään yhtälöön $2k^2 - 2b = 1$. Siis

$$1 = 2(k^2 - b),$$

missä $k^2 - b \in \mathbb{Z}$. Tämä tarkoittaa, että luku 1 on parillinen. Toisaalta tiedetään, että luku 1 ei ole parillinen. Päädyttiin ristiriitaan.

Koska vastaoletus johti ristiriitaan, on alkuperäinen väite tosi. Siis kaikilla kokonaisluvuilla $a$ ja $b$ pätee $a^2 - 4b \neq 2$.

---

Seuraavassa esimerkissä todistetaan ”jos ja vain jos”-tyyppinen väite käyttäen kappaleessa 3.3 esiteltyä tekniikkaa. Todistuksessa käytetään myös epäsuoraa päättelyä.

**Esimerkki 3.5.2.** Oletetaan, että $A$ ja $B$ ovat joukkoja. Osoitetaan, että $A \cup B = B$, jos ja vain jos $A \setminus B = \emptyset$.

"$\Rightarrow$": Oletetaan, että $A \cup B = B$. Pitää näyttää, että tällöin $A \setminus B = \emptyset$. Käytetään epäsuoraa päättelyä.

Muodostetaan väitteelle $A \setminus B = \emptyset$ vastaoletus eli antiteesi: oletetaan, että $A \setminus B \neq \emptyset$. Vastaoletuksesta seuraa, että on olemassa $x \in A \setminus B$. Erotuksen määritelmän nojalla $x \in A$ ja $x \notin B$.

Koska $x \in A$, niin yhdisteen määritelmän mukaan $x \in A \cup B$. Oletuksen mukaan $A \cup B = B$. Yhdistämällä nämä tiedot saadaan pääteltyä, että $x \in B$.

Näin päädytään ristiriitaan: $x \notin B$ ja $x \in B$. Koska vastaoletus johti ristiriitaan, on alkuperäinen väite tosi. Siis $A \setminus B = \emptyset$.

"$\Leftarrow$": Oletetaan, että $A \setminus B = \emptyset$. Pitää näyttää, että tällöin $A \cup B = B$. Tehdään tämä osoittamalla kumpikin joukko toisen osajoukoksi.

"$\subset$": Oletetaan, että $x \in A \cup B$. Tästä voidaan yhdisteen määritelmän nojalla päätellä, että $x \in A$ tai $x \in B$. Jotta voidaan olla varmoja siitä, että oikeaan johtopäätökseen päädytään kaikissa mahdollisissa tapauksissa, tehdään tapaustarkastelu:

- Oletetaan, että $x \in A$. Tästä on vaikea edetä suoraan, joten mietitään asiaa joukon $B$ kannalta. Varmasti joko $x \in B$ tai $x \notin B$. Muita vaihtoehtoja ei ole.

  Jos $x \notin B$, niin oletuksen $x \in A$ nojalla voidaan päätellä, että $x \in A \setminus B$. Toisaalta oletuksen mukaan $A \setminus B = \emptyset$. Näin $x \in \emptyset$, mikä on mahdotonta. Vaihtoehto $x \notin B$ ei siis ole mahdollinen, joten $x \in B$.
- Oletetaan, että $x \in B$. Tällöinkin $x \in B$.

Kaikissa mahdollisissa tapauksissa $x \in B$.

"$\supset$": Oletetaan, että $x \in B$. Tällöin yhdisteen määritelmän nojalla $x \in A \cup B$.

---

Jos ristiriitatodistusta halutaan käyttää "jos $P$, niin $Q$"-tyyppisen väitteen todistamisessa, on vastaoletuksen muotoilussa oltava tarkkana. Implikaation negaatio $\neg(P \to Q)$ on esimerkin 2.2.3 mukaan loogisesti ekvivalentti konjuktion $P \land \neg Q$ kanssa. Vastaoletus väitteelle "jos $P$, niin $Q$" on siis muotoa "$P$ ja $\neg Q$". Tätä havainnollistetaan seuraavassa esimerkissä. Siinä esiintyvä väite todistettiin suoralla todistuksella jo esimerkissä 3.2.5.

**Esimerkki 3.5.3.** Oletetaan, että $A$, $B$ ja $C$ ovat joukkoja. Osoitetaan, että jos $A \subset B$ ja $A \not\subset C$, niin $B \not\subset C$.

Tehdään vastaoletus, että $A \subset B$ ja $A \not\subset C$ ja $B \subset C$. Koska $A \subset B$ ja $B \subset C$, voidaan näyttää, että $A \subset C$:

Oletetaan, että $a \in A$. Koska $A \subset B$, niin $a \in B$. Koska $B \subset C$, niin $a \in C$.

Siis $A \subset C$ ja $A \not\subset C$. Koska vastaoletus johti ristiriitaan, on alkuperäinen väite tosi. Siis väite "jos $A \subset B$ ja $A \not\subset C$, niin $B \not\subset C$" pätee.

Vastaoletuksen muotoilu voi olla helpompaa, jos alkuperäisen väitteen jakaa ensin osiin. Seuraavassa esimerkissä esitetään toinen tapa esimerkin 3.5.3 väitteen todistamiseen.

**Esimerkki 3.5.4.** Oletetaan, että $A$, $B$ ja $C$ ovat joukkoja. Osoitetaan, että jos $A \subset B$ ja $A \not\subset C$, niin $B \not\subset C$.

Koska kysymyksessä on ”jos $P$ niin $Q$”-tyyppinen väite, käytetään kappaleessa 3.2 esiteltyä tekniikkaa. Oletetaan, että tarkasteltavan implikaation etujäsen on tosi. Toisin sanottuna oletetaan, että $A \subset B$ ja $A \not\subset C$. Tavoitteena on näyttää, että tällöin myös implikaation takajäsen on tosi. Toisin sanottuna tavoitteena on näyttää, että $B \not\subset C$.

Muodostetaan tälle väitteelle vastaoletus: oletetaan, että $B \subset C$. Yhdistämällä alkuperäinen oletus $A \subset B$ ja vastaoletus $B \subset C$ voidaan näyttää, että $A \subset C$:

Oletetaan, että $a \in A$. Koska $A \subset B$, niin $a \in B$. Koska $B \subset C$, niin $a \in C$.

Siis $A \subset C$ ja $A \not\subset C$. Koska vastaoletus johti ristiriitaan, on alkuperäinen väite tosi. Siis $B \not\subset C$.

# 4 Matemaattinen induktio

Joidenkin väitteiden todistamiseksi pitää näyttää, että kaikilla luonnollisilla luvuilla on jokin ominaisuus $P$. Esimerkkejä tällaisista väitteistä ovat vaikkapa seuraavat:

- kaikilla $n \in \mathbb{N}$ pätee, että $0 + 1 + 2 + \cdots + n = n(n + 1)/2$.
- kaikilla $n \in \mathbb{N}$ pätee seuraava: jos $x \in \mathbb{R}$ ja $x > -1$, niin $(1 + x)^n \geq 1 + nx$.
- kaikilla $n \in \mathbb{N} \setminus \{0, 1, 2\}$ pätee, että $n$-kulmion kulmien summa on $(n - 2)\pi$.

Koska luonnollisia lukuja on äärettömän paljon, emme voi tarkistaa yksitellen, onko niillä kaikilla ominaisuus $P$. Tarvitaan jokin toinen keino tämäntyyppisten väitteiden todistamiseen.

Luonnollisten lukujen joukko $\mathbb{N}$ määritellään niin, että se toteuttaa niin sanotun *induktioaksiooman*, joka on olla olevan määritelmän kohta 5.

**Määritelmä 4.0.1.** *Luonnollisten lukujen joukolla* $\mathbb{N}$ on seuraavat ominaisuudet:

1. Nolla on luonnollinen luku; ts. $0 \in \mathbb{N}$.
2. Jokaista luonnollista lukua $n$ kohti on olemassa täsmälleen yksi luonnollinen luku $s(n)$, jota sanotaan luvun $n$ *seuraajaksi*.
3. Nolla ei ole minkään luonnollisen luvun seuraaja; ts. $0 \neq s(n)$ kaikilla $n \in \mathbb{N}$.
4. Eri luvuilla on eri seuraajat; ts. jos $m \neq n$, niin $s(m) \neq s(n)$.
5. Oletetaan, että $A \subset \mathbb{N}$. Oletetaan lisäksi, että $0 \in A$, ja että kaikilla $n \in \mathbb{N}$ pätee: jos $n \in A$, niin $s(n) \in A$. Tällöin $A = \mathbb{N}$.

Määritelmässä 4.0.1 mainittu luonnollisen luvun $n$ seuraaja $s(n)$ tarkoittaa lukua $n + 1$. Esimerkiksi luvun 3 seuraaja on $s(3) = 4$.

## 4.1 I induktioperiaate

Induktioaksioomasta saadaan johdettua I induktioperiaate, joiden avulla voidaan todistaa luonnollisia lukuja koskevia väitteitä.

**Lause 4.1.1 (I induktioperiaate).** *Oletetaan, että seuraavat ehdot ovat voimassa:*

1. *Luvulla* 0 *on ominaisuus* $P$.
2. *Kaikilla luonnollisilla luvuilla pätee:*
   *jos luvulla* $n$ *on ominaisuus* $P$*, niin sitä seuraavalla luvulla* $n + 1$ *on ominaisuus* $P$.

*Tällöin kaikilla luonnollisilla luvuilla on ominaisuus* $P$.

*Todistus.* Merkitään $A = \{n \in \mathbb{N} \mid \text{ luvulla } n \text{ on ominaisuus } P\}$. Havaitaan, että $A \subset \mathbb{N}$. Oletuksen ehdon 1 nojalla $0 \in A$ ja ehdon 2 nojalla kaikilla $n \in \mathbb{N}$ pätee, että jos $n \in A$, niin $n + 1 \in A$. Toisin sanottuna kaikilla $n \in \mathbb{N}$ pätee, että jos $n \in A$, niin $s(n) \in A$. Tällöin määritelmän 4.0.1 kohdan 5 eli induktioaksiooman nojalla $A = \mathbb{N}$. Siis kaikilla luonnollisilla luvuilla on ominaisuus $P$. $\square$

Logiikan symboleiden avulla lause 4.1.1 voidaan kirjoittaa seuraavaan muotoon:

**Lause 4.1.1** (**I induktioperiaate**). *Oletetaan, että seuraavat ehdot ovat voimassa:*

1. $P(0)$.
2. $\forall n \in \mathbb{N} \ \big(P(n) \to P(n+1)\big)$.

*Tällöin* $\forall n \in \mathbb{N} \ P(n)$.

Induktiotodistus rakentuu kahdesta osasta, sillä pitää varmistaa, että molemmat induktioperiaatteessa mainitut ehdot toteutuvat. *Alkuaskeleessa* varmistetaan, että tutkittava väite pätee luvun nolla tapauksessa. *Induktioaskeleessa* osoitetaan, että implikaatio $P(n) \to P(n+1)$ on tosi kaikilla $n \in \mathbb{N}$. Se tapahtuu seuraavasti:

- Oletetaan, että $k \in \mathbb{N}$. Oletetaan lisäksi, että tarkasteltava väite pätee luvulla $k$.
- Näytetään, että tällöin väite pätee seuraavalla luvulla $k + 1$.

Alkuaskeleesta ja induktioaskeleesta voidaan induktioperiaatteen nojalla päätellä, että tutkittava väite pätee kaikilla luonnollisilla luvuilla.

**Esimerkki 4.1.2.** Osoitetaan induktiolla, että kaikilla $n \in \mathbb{N}$ pätee yhtälö

$$\sum_{j=0}^{n} 2j = n(n+1)\,.$$

Yhtälön vasemmalla puolella näkyvä summamerkintä tarkoittaa, että symbolin $j$ paikalle sijoitetaan luvut $0, 1, \ldots, n$ ja saadut lausekkeet lasketaan yhteen: $2 \cdot 0 + 2 \cdot 1 + 2 \cdot 2 + \cdots + 2 \cdot n$. Tarkasteltava yhtälö voidaan siten kirjoittaa myös muodossa

$$0 + 2 + 4 + \cdots + 2n = n(n+1).$$

<u>Alkuaskel</u>: Tutkitaan, päteekö yhtälö, jos $n = 0$.

Oletetaan, että $n = 0$. Yhtälön vasen puoli on tällöin

$$\sum_{j=0}^{n} 2j = \sum_{j=0}^{0} 2j = 2 \cdot 0 = 0$$

ja yhtälön oikea puoli on puolestaan $n(n+1) = 0 \cdot (0+1) = 0$. Yhtälön vasen ja oikea puoli ovat siis yhtä suuret, joten yhtälö pätee tässä tapauksessa.

Induktioaskel: Aloitetaan tekemällä induktio-oletus. Oletetaan, että $k \in \mathbb{N}$ ja

$$\sum_{j=0}^{k} 2j = k(k+1)\,. \tag{IO}$$

Tämä yhtälö voidaan kirjoittaa myös muodossa $0 + 2 + 4 + \cdots + 2k = k(k+1)$.

Seuraavaksi tavoitteena on näyttää induktio-oletuksen avulla, että vastaava yhtälö pätee myös seuraavalle luonnolliselle luvulle $k+1$. Pitää todistaa niin sanottu induktioväite:

$$\sum_{j=0}^{k+1} 2j = (k+1)(k+2)\,. \tag{IV}$$

Tämä yhtälö on muodostettu tutkittavasta yhtälöstä sijoittamalla kirjaimen $n$ paikalle $k+1$. Se voidaan kirjoittaa myös muodossa $0 + 2 + 4 + \cdots + 2k + 2(k+1) = (k+1)(k+2)$.

Tutkitaan yhtälön (IV) vasen ja oikea puoli erikseen samaan tapaan kuin alkuaskeleessa tehtiin. Vasemman puolen summa voidaan kirjoittaa ensin auki, jolloin huomataan, että summan termit viimeistä lukuunottamatta ovat samat kuin induktio-oletuksen yhtälössä (IO). Käytetään induktio-oletusta kohdassa (IO) ja sievennetään:

$$\begin{aligned}\sum_{j=0}^{k+1} 2j &= (0 + 2 + 4 + \cdots + 2k) + 2(k+1) \\ &= \sum_{j=0}^{k} 2j + 2(k+1) \overset{\text{(IO)}}{=} k(k+1) + 2(k+1) = k^2 + k + 2k + 2 = k^2 + 3k + 2.\end{aligned}$$

Yhtälön oikean puolen sulut voidaan kertoa auki, jolloin saadaan

$$(k+1)(k+2) = k^2 + 2k + k + 2 = k^2 + 3k + 2.$$

Vertaamalla vasenta ja oikeaa puolta havaitaan, että ne ovat samat. Siis yhtälö (IV) pätee.

Johtopäätös: Alkuaskeleesta ja induktioaskeleesta seuraa induktioperiaatteen nojalla, että kaikilla $n \in \mathbb{N}$ pätee yhtälö

$$\sum_{j=0}^{n} 2j = n(n+1)\,.$$

---

Seuraava esimerkki induktiotodistuksesta liittyy lukujen jaollisuuteen. Tiedämme, että esimerkiksi luku 22 on jaollinen luvulla 11, sillä jakolasku menee tasan: $22/11 = 2$. Toisella tavalla sama asia voidaan ilmaista sanomalla, että luku 22 voidaan kirjoittaa luvun 11 monikertana: $22 = 2 \cdot 11$. Tätä näkökulmaa käytetään, kun määritellään, mitä kokonaislukujen jaollisuudella tarkoitetaan.

**Määritelmä 4.1.3.** Kokonaisluku $z$ on *jaollinen kokonaisluvulla* $m$, jos jollakin kokonaisluvulla $a$ pätee $z = am$. Tällöin merkitään $m \mid z$ ja sanotaan, että luku $m$ *jakaa* luvun $z$. Jos luku $z$ ei ole jaollinen luvulla $m$, merkitään $m \nmid z$.

**Esimerkki 4.1.4.** Osoitetaan induktiolla, että luku 11 jakaa luvun $5^{2n} - 3^n$ kaikilla $n \in \mathbb{N}$.

Alkuaskel: Tutkitaan, jakaako luku 11 luvun $5^{2n} - 3^n$, jos $n = 0$.

Oletetaan, että $n = 0$. Tällöin

$$5^{2n} - 3^n = 5^{2\cdot 0} - 3^0 = 1 - 1 = 0 = 0 \cdot 11,$$

missä $0 \in \mathbb{Z}$. Siis jos $n = 0$, niin luku $5^{2n} - 3^n$ on jaollinen luvulla 11.

Induktioaskel: Aloitetaan tekemällä induktio-oletus. Oletetaan, että $k \in \mathbb{N}$, ja oletetaan, että luku 11 jakaa luvun $5^{2k} - 3^k$. Tästä seuraa määritelmän 4.1.3 nojalla, että on olemassa $a \in \mathbb{Z}$, jolla pätee

$$5^{2k} - 3^k = a \cdot 11. \tag{1}$$

Seuraavaksi tavoitteena on näyttää induktio-oletuksen avulla, että luku 11 jakaa myös luvun $5^{2(k+1)} - 3^{k+1}$. Muokataan tarkasteltavaa lukua potenssisääntöjen avulla:

$$5^{2(k+1)} - 3^{k+1} = 5^{2k+2} - 3^{k+1} = 5^{2k} \cdot 5^2 - 3^k \cdot 3 = 25 \cdot 5^{2k} - 3 \cdot 3^k. \tag{2}$$

Yhtälö (1) voidaan kirjoittaa muodossa $5^{2k} = a \cdot 11 + 3^k$. Käyttämällä tätä tietoa voidaan yhtälöketjua (2) jatkaa:

$$\begin{aligned}
5^{2(k+1)} - 3^{k+1} &= 25 \cdot (a \cdot 11 + 3^k) - 3 \cdot 3^k \\
&= 25 \cdot a \cdot 11 + 25 \cdot 3^k - 3 \cdot 3^k \\
&= 25a \cdot 11 + (25 - 3) \cdot 3^k \\
&= 25a \cdot 11 + 22 \cdot 3^k \\
&= 25a \cdot 11 + 2 \cdot 11 \cdot 3^k \\
&= (25a + 2 \cdot 3^k) \cdot 11\,.
\end{aligned}$$

Koska $a \in \mathbb{Z}$ ja $k \in \mathbb{N}$, voidaan päätellä, että $25a+2\cdot 3^k$ on kokonaisluku. Siis luku $5^{2(k+1)}-3^{k+1}$ on jaollinen luvulla 11.

Johtopäätös: Alkuaskeleesta ja induktioaskeleesta seuraa induktioperiaatteen nojalla, että luku 11 jakaa luvun $5^{2n} - 3^n$ kaikilla $n \in \mathbb{N}$.

---

Induktiolla voi todistaa myös sellaisia väitteitä, jotka pätevät kaikille luonnollisille luvuille jostain positiivisesta luonnollisesta luvusta lähtien. Esimerkiksi väite $3^n > n^3$ on epätosi, jos

$n = 3$, mutta pätee kaikilla luonnollisilla luvuilla $n \geq 4$, kuten seuraava esimerkki osoittaa. Tällaisissa tilanteissa täytyy alkuaskeleessa varmistaa, että väite pätee pienimmällä tarkastellulla luonnollisella luvulla.

**Esimerkki 4.1.5.** Osoitetaan induktiolla, että $3^n > n^3$ kaikilla luonnollisilla luvuilla $n \geq 4$.

Alkuaskel: Tutkitaan, päteekö epäyhtälö pienimmän tarkasteltavan luonnollisen luvun eli luvun 4 tapauksessa. Havaitaan, että $3^4 = 81$ ja $4^3 = 64$, joten $3^4 > 4^3$.

Induktioaskel: Aloitetaan tekemällä induktio-oletus. Oletetaan, että $k \in \mathbb{N}$ ja

$$3^k > k^3. \tag{IO}$$

Seuraavaksi tavoitteena on näyttää induktio-oletuksen avulla, että vastaava epäyhtälö pätee myös seuraavalle luonnolliselle luvulle $k + 1$. Kertomalla induktio-oletuksen epäyhtälön (IO) molemmat puolet positiivisella luvulla 3 saadaan uusi epäyhtälö $3 \cdot 3^k > 3k^3$, joka voidaan kirjoittaa myös muotoon

$$3^{k+1} > k^3 + k^3 + k^3. \tag{3}$$

Arvioidaan epäyhtälön (3) oikeaa puolta varovasti alaspäin käyttäen toistuvasti oletusta $k \geq 4$:

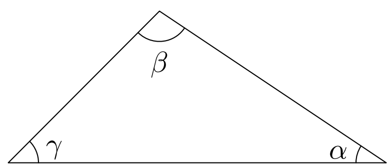
$$\begin{aligned}
3^{k+1} &> k^3 + k^3 + k^3 \\
&= k^3 + k \cdot k^2 + k^2 \cdot k \\
&\geq k^3 + 4k^2 + 16k \\
&= k^3 + 4k^2 + 15k + k \\
&\geq k^3 + 4k^2 + 15k + 4 \\
&> k^3 + 3k^2 + 3k + 1 = (k+1)^3.
\end{aligned}$$

Saadusta epäyhtälöketjusta voidaan päätellä, että $3^{k+1} > (k + 1)^3$.

Johtopäätös: Alkuaskeleesta ja induktioaskeleesta seuraa induktioperiaatteen nojalla, että kaikilla luonnollisilla luvuilla $n \geq 4$ pätee $3^n > n^3$.

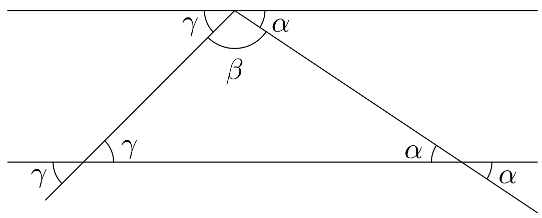
**Esimerkki 4.1.6.** Osoitetaan induktiolla, että $n$-kulmion kulmien summa on $(n-2)\pi$ kaikilla luonnollisilla luvuilla $n \geq 3$.

Alkuaskel: Tutkitaan, päteekö väite pienimmän tarkasteltavan luonnollisen luvun eli luvun 3 tapauksessa. Merkitään kolmikulmion eli kolmion kulmia $\alpha$, $\beta$ ja $\gamma$ kuten kuvassa 4.1.




Kuva 4.1: Kolmio, jonka kulmat ovat $\alpha$, $\beta$ ja $\gamma$

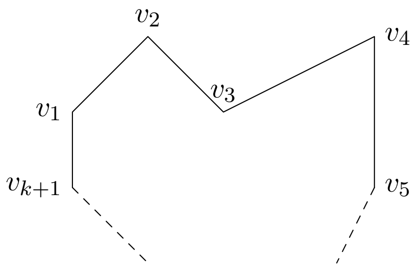
Piirtämällä kulmaa $\beta$ vastaavaan kolmion kärkeen kolmion kannan suutainen suora ja jatkamalla kolmion sivuja kuten kuvassa 4.2 voidaan päätellä, että kulmien summa $\alpha + \beta + \gamma$ on oikokulma eli 180 astetta eli $\pi$ radiaania. Siis kolmion kulmien summa on $(3 - 2)\pi$.




Kuva 4.2: Kolmion kulmien summa $\alpha + \beta + \gamma$ on 180 astetta eli $\pi$ radiaania.

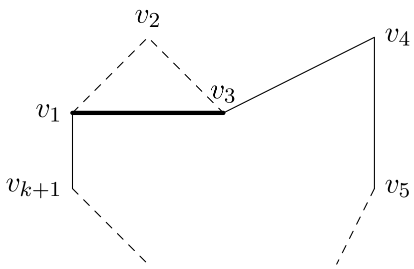
<u>Induktioaskel</u>: Aloitetaan tekemällä induktio-oletus. Oletetaan, että luonnollinen luku $k \geq 3$ ja $k$-kulmion kulmien summa on $(k - 2)\pi$.

Tarkastellaan $(k+1)$-kulmiota, jonka kärjet ovat $v_1$,$v_2$, $v_3$, $\ldots$, $v_{k+1}$. Sitä on havainnollistettu kuvassa 4.3:




Kuva 4.3: Osa $(k+1)$-kulmiosta, jonka kärjet ovat $v_1$, $v_2$, $v_3$,$\ldots$, $v_{k+1}$.

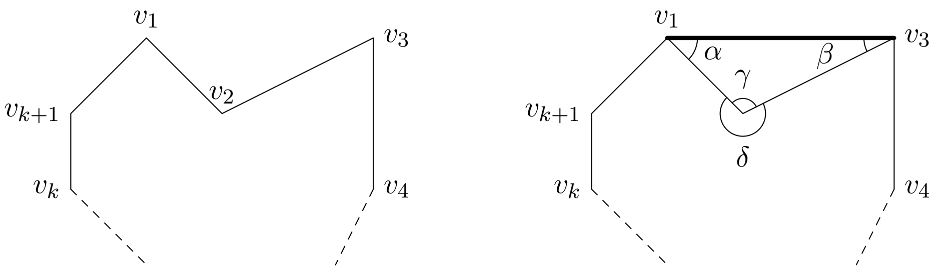
Piirtämällä jana kärjestä $v_1$ kärkeen $v_3$ saadaan muodostettua $k$-kulmio $v_1 v_3 \ldots v_{k+1}$, jonka kulmien summa on induktio-oletuksen mukaan $(k-2)\pi$. Sitä on havainnollistettu kuvassa 4.4:




Kuva 4.4: Induktio-oletuksen mukaan $k$-kulmion $v_1 v_3 \ldots v_{k+1}$ kulmien summa on $(k - 2)\pi$.

Koska alkuperäinen $(k + 1)$-kulmio saadaan yhdistämällä $k$-kulmio $v_1 v_3 \ldots v_{k+1}$ ja kolmio $v_1 v_2 v_3$, saadaan $(k+1)$-kulmion kulmien summaksi $(k-2)\pi + \pi = (k-1)\pi = ((k+1) - 2)\pi$.

Äskeisessä tilanteessa syntynyt $k$-kulmio sisältyi alkuperäiseen $(k+1)$-kulmioon. Joskus voi käydä myös toisin. Kuvassa 4.5 on havainnollistettu toista mahdollista tilannetta, jossa alkuperäinen $(k+1)$-kulmio sisältyy syntyvään $k$-kulmioon.




Kuva 4.5: Syntyvä $k$-kulmio sisältää alkuperäisen $(k+1)$-kulmion.

Koska kolmion $v_1v_2v_3$ kulmien summa on $\alpha+\beta+\gamma=\pi$ ja täyskulma on 360 astetta eli $2\pi$, saadaan pääteltyä kulman $\delta$ suuruus:

$$\delta = 2\pi - \gamma = 2\pi - (\pi - \alpha - \beta) = \pi + \alpha + \beta.$$

Induktio-oletuksen nojalla $k$-kulmion $v_1v_3\ldots v_{k+1}$ kulmien summa on $(k-2)\pi$. Alkuperäisen $(k+1)$-kulmion kulmien summa on siten

$$\begin{aligned}(k-2)\pi - \alpha - \beta + \delta &= (k-2)\pi - \alpha - \beta + (\pi + \alpha + \beta) = (k-2)\pi + \pi = (k-1)\pi \\ &= ((k+1)-2)\pi.\end{aligned}$$

<u>Johtopäätös</u>: Alkuaskeleesta ja induktioaskeleesta seuraa induktioperiaatteen nojalla, että $n$-kulmion kulmien summa on $(n-2)\pi$ kaikilla luonnollisilla luvuilla $n \geq 3$.

---

Seuraava esimerkki osoittaa, että induktioaskeleen todistaminen voi onnistua silloinkin, kun varsinainen väite ei päde. Induktiotodistus vaatii siis toimiakseen sekä alkuaskeleen että induktioaskeleen.

**Esimerkki 4.1.7.** Tarkastellaan väitettä "luku 9 jakaa luvun $10^n+1$ kaikilla $n \in \mathbb{N}$". Pyritään todistamaan tämä väite induktiolla.

Aloitetaan induktioaskeleesta ja osoitetaan, että kaikilla $n \in \mathbb{N}$ pätee, että jos luku 9 jakaa luvun $10^n+1$, niin luku 9 jakaa luvun $10^{n+1}+1$.

Oletetaan, että $k \in \mathbb{N}$. Oletetaan lisäksi, että luku 9 jakaa luvun $10^k+1$. Tästä seuraa määritelmän 4.1.3 nojalla, että on olemassa $a \in \mathbb{Z}$, jolla pätee

$$10^k + 1 = a \cdot 9. \tag{4}$$

Kertomalla yhtälön (4) molemmat puolet luvulla 10 saadaan yhtälö $10 \cdot (10^k+1) = 10 \cdot a \cdot 9$. Kertomalla sen vasemman puolen sulut auki saadaan $10^{k+1} + 10 = 10 \cdot a \cdot 9$. Tämän yhtälön avulla voidaan päätellä, että

$$10^{k+1} + 1 = 10^{k+1} + (10-9) = (10^{k+1}+10) - 9 = 10 \cdot a \cdot 9 - 9 = (10a-1) \cdot 9.$$

Tässä $10a - 1 \in \mathbb{Z}$, sillä $a \in \mathbb{Z}$. Siis luku $10^{k+1} + 1$ on jaollinen luvulla 9.

Induktioaskeleessa tehty päättely todistaa, että kaikilla $n \in \mathbb{N}$ pätee, että jos luku 9 jakaa luvun $10^n + 1$, niin luku 9 jakaa luvun $10^{n+1} + 1$. Logiikan symboleilla tämä voidaan kirjoittaa

$$\forall n \in \mathbb{N}\ (P(n) \to P(n+1)),$$

missä $P(n)$ tarkoittaa, että luku 9 jakaa luvun $10^n + 1$.

Pelkkä induktioaskel ei kuitenkaan riitä todistamaan väitettä ”luku 9 jakaa luvun $10^n + 1$ kaikilla $n \in \mathbb{N}$”. Alkuaskeleessa tulee ongelmia, sillä jos $n = 0$, niin

$$10^n + 1 = 10^0 + 1 = 1 + 1 = 2$$

ja $9 \nmid 2$. Koska $10^0 + 1$ ei ole jaollinen luvulla 9, väite ”luku 9 jakaa luvun $10^n + 1$ kaikilla $n \in \mathbb{N}$” on epätosi.

---

Pelkkä alkuaskel ei myöskään riitä todistamaan väitettä oikeaksi, kuten seuraava esimerkki osoittaa.

**Esimerkki 4.1.8.** Tarkastellaan väitettä ”epäyhtälö $n^2 \leq 2^{n-1}$ pätee kaikilla $n \in \mathbb{N}$”. Pyritään todistamaan tämä väite induktiolla.

Aloitetaan alkuaskeleesta. Havaitaan, että $0^2 = 0$ ja $2^{0-1} = 2^{-1} = 1/2$. Siis $0^2 \leq 2^{0-1}$.

Induktioaskeleessa voi yrittää käyttää samankaltaista päättelyä kuin esimerkissä 4.1.5. Kokeilemalla kuitenkin huomaa, että induktioaskeleen tekeminen ei tunnu millään onnistuvan. Itse asiassa väite ”epäyhtälö $n^2 \leq 2^{n-1}$ pätee kaikilla $n \in \mathbb{N}$” on epätosi, sillä esimerkiksi

$$5^2 = 25 \not\leq 16 = 2^4 = 2^{5-1}.$$

## 4.2 II induktioperiaate

Joidenkin luonnollisia lukuja koskevien väitteiden todistaminen käy helpommin niin sanotun II induktioperiaatteen avulla. Se poikkeaa I induktioperiaatteesta induktio-oletuksen osalta.

**Lause 4.2.1** (**II induktioperiaate**). *Oletetaan, että seuraavat ehdot ovat voimassa:*

1. *Luvulla* 0 *on ominaisuus* $P$.
2. *Kaikilla luonnollisilla luvuilla pätee:*

   *jos luvulla* $n$ *ja kaikilla sitä pienemmillä luonnollisilla luvuilla on ominaisuus* $P$*, niin luvulla* $n+1$ *on ominaisuus* $P$.

*Tällöin kaikilla luonnollisilla luvuilla on ominaisuus* $P$.

Ennen II induktioperiaatteen todistusta muotoillaan se logiikan symboleiden avulla. Merkintöjen yksinkertaistamiseksi lyhennetään merkintä $\forall j \in \mathbb{N}\ (j \leq n \to P(j))$ muotoon $\forall j \leq n\ P(j)$.

**Lause 4.2.1** (**II induktioperiaate**). *Oletetaan, että seuraavat ehdot ovat voimassa:*

1. $P(0)$.
2. $\forall n \in \mathbb{N}\ \big((\forall j \leq n\ P(j)) \to P(n+1)\big)$.

*Tällöin* $\forall n \in \mathbb{N}\ P(n)$.

*Todistus.* Oletetaan, että $n \in \mathbb{N}$. Sovitaan, että merkintä $Q(n)$ tarkoittaa, että $\forall j \leq n\ P(j)$.

Todistetaan aluksi I induktioperiaatteen avulla, että $Q(n)$ on tosi kaikilla $n \in \mathbb{N}$.

Alkuaskel: Merkintä $Q(0)$ tarkoittaa, että $\forall j \leq 0\ P(j)$. Lukua 0 pienempiä luonnollisia lukuja ei ole, ja $P(0)$ on tosi oletuksen nojalla. Näin voidaan päätellä, että $\forall j \leq 0\ P(j)$ on tosi. Siis $Q(0)$ on tosi.

Induktioaskel: Aloitetaan tekemällä induktio-oletus. Oletetaan, että $n \in \mathbb{N}$ ja $Q(n)$ on tosi. Tämä tarkoittaa, että $\forall j \leq n\ P(j)$ on tosi. Tällöin oletuksen nojalla $P(n+1)$ on tosi. Koska $\forall j \leq n\ P(j)$ on tosi ja lisäksi $P(n+1)$ on tosi, niin $\forall j \leq n+1\ P(j)$ on tosi. Siis $Q(n+1)$ on tosi.

Johtopäätös: Alkuaskeleesta ja induktioaskeleesta seuraa induktioperiaatteen nojalla, että $Q(n)$ on tosi kaikilla $n \in \mathbb{N}$.

Näin on todistettu, että kaikilla luonnollisilla luvuilla $n$ pätee $\forall j \leq n\ P(j)$. Tästä seuraa, että kaikilla luonnollisilla luvuilla $n$ pätee $P(n)$. ☐

**Esimerkki 4.2.2.** Määritellään lukujono $(z_n)$ rekursiivisesti asettamalla $z_0 = 2$, $z_1 = 1$ ja

$$z_n = z_{n-1} + 2z_{n-2}$$

kaikilla $n \geq 2$. Lukujono $(z_n)$ alkaa siis seuraavasti:

$$\begin{aligned}
z_0 &= 2 \\
z_1 &= 1 \\
z_2 &= z_1 + 2z_0 = 5 \\
z_3 &= z_2 + 2z_1 = 7 \\
z_4 &= z_3 + 2z_2 = 17 \\
z_5 &= z_4 + 2z_3 = 31
\end{aligned}$$

Osoitetaan II induktioperiaatteen avulla, että $z_n = 2^n + (-1)^n$ kaikilla $n \in \mathbb{N}$.

Alkuaskel: Tutkitaan, päteekö väitetty yhtälö, jos $n = 0$. Lukujonon $(z_n)$ määritelmän mukaan $z_0 = 2$. Huomataan, että myös $2^0 + (-1)^0 = 1 + 1 = 2$. Siis $z_0 = 2^0 + (-1)^0$.

Induktioaskel: Aloitetaan tekemällä induktio-oletus. Oletetaan, että $k \in \mathbb{N}$ ja $z_j = 2^j + (-1)^j$ kaikilla luonnollisilla luvuilla $j \leq k$.

Seuraavaksi tavoitteena on näyttää induktio-oletuksen avulla, että myös $z_{k+1} = 2^{k+1} + (-1)^{k+1}$. Koska lukujonon $(z_n)$ määritelmän rekursiokaavaa voi käyttää vasta jäsenestä $z_2$ alkaen, täytyy luku $z_1$ käsitellä erikseen:

- Jos $k = 0$, niin $z_{k+1} = z_1$. Lukujonon $(z_n)$ määritelmän mukaan $z_1 = 1$. Huomataan, että myös $2^1 + (-1)^1 = 2 - 1 = 1$. Siis tässä tapauksessa $z_{k+1} = 2^{k+1} + (-1)^{k+1}$.
- Jos $k \geq 1$, niin $k + 1 \geq 2$. Luvun $z_{k+1}$ laskemiseen voidaan siis tässä tapauksessa käyttää määritelmän rekursioyhtälöä. Sen ja induktio-oletuksen avulla saadaan

$$
\begin{aligned}
z_{k+1} = z_k + 2z_{k-1} &\overset{\text{(IO)}}{=} 2^k + (-1)^k + 2 \cdot (2^{k-1} + (-1)^{k-1}) \\
&= 2^k + (-1)^k + 2^k + 2 \cdot (-1)^{k-1} \\
&= 2 \cdot 2^k + (-1) \cdot (-1)^{k-1} + 2 \cdot (-1)^{k-1} \\
&= 2^{k+1} + (-1 + 2) \cdot (-1)^{k-1} \\
&= 2^{k+1} + 1 \cdot (-1)^{k-1} \\
&= 2^{k+1} + (-1)^2 \cdot (-1)^{k-1} \\
&= 2^{k+1} + (-1)^{k+1}.
\end{aligned}
$$

  Huomaa, että induktio-oletuksen mukaan $z_k = 2^k + (-1)^k$ ja $z_{k-1} = 2^{k-1} + (-1)^{k-1}$, sillä $k$ ja $k - 1$ ovat kumpikin luonnollisia lukuja ja pienempiä tai yhtä suuria kuin $k$.

Johtopäätös: Alkuaskeleesta ja induktioaskeleesta seuraa II induktioperiaatteen nojalla, että $z_n = 2^n + (-1)^n$ kaikilla $n \in \mathbb{N}$.

**Esimerkki 4.2.3.** Osoitetaan, että jokainen luonnollinen luku $n \geq 2$ on joko alkuluku tai alkulukujen tulo.

Alkuaskel: Määritelmän 3.1.1 mukaan ykköstä suurempi kokonaisluku on alkuluku, jos sen ainoat positiiviset tekijät ovat 1 ja kyseinen luku itse. Huomataan, että luku 2 on alkuluku, sillä sen ainoat positiiviset tekijät ovat 1 ja 2.

Induktioaskel: Aloitetaan tekemällä induktio-oletus. Oletetaan, että $k \geq 2$ on luonnollinen luku. Oletetaan lisäksi, että kaikilla luonnollisilla luvuilla $2 \leq j \leq k$ pätee, että $j$ on joko alkuluku tai alkulukujen tulo.

Seuraavaksi tavoitteena on näyttää induktio-oletuksen avulla, että myös luku $k + 1$ on joko alkuluku tai alkulukujen tulo. Tutkitaan lukua $k + 1$.

- Jos $k + 1$ on alkuluku, ei asiaa tarvitse tutkia sen enempää.
- Jos $k + 1$ ei ole alkuku, se voidaan kirjoittaa tulona $k + 1 = ab$, missä kokonaisluvuille $a$ ja $b$ pätee $1 < a < k + 1$ ja $1 < b < k + 1$. Lukuihin $a$ ja $b$ voidaan siis käyttää induktio-oletusta, jonka mukaan luvut $a$ ja $b$ ovat alkulukuja tai alkulukujen tuloja. Koska $k + 1 = ab$, seuraa tästä, että $k + 1$ on alkulukujen tulo.

Molemmissa tapauksissa $k + 1$ on joko alkuluku tai alkulukujen tulo.

Johtopäätös: Alkuaskeleesta ja induktioaskeleesta seuraa II induktioperiaatteen nojalla, että jokainen luonnollinen luku $n \geq 2$ on joko alkuluku tai alkulukujen tulo.

# 5 Perusasioita kuvauksista

## 5.1 Kuvauksen määritelmä

**Määritelmä 5.1.1.** Oletetaan, että $X$ ja $Y$ ovat joukkoja. *Kuvaus joukosta $X$ joukkoon $Y$* on sääntö, joka liittää joukon $X$ jokaiseen alkioon täsmälleen yhden alkion joukosta $Y$.

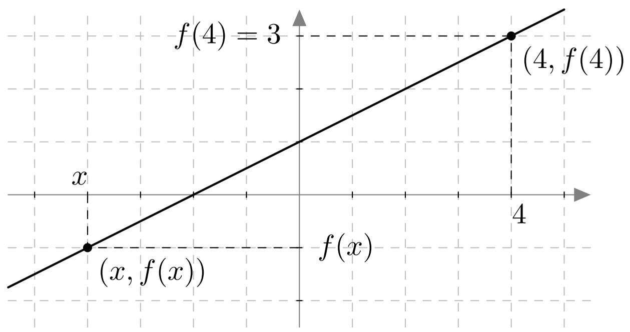
Merkintä $f\colon X \to Y$ tarkoittaa, että $f$ on kuvaus joukosta $X$ joukkoon $Y$. Joukko $X$ on kuvauksen $f$ *lähtö* ja joukko $Y$ on kuvauksen $f$ *maali*.

Merkintä $f(x)$ tarkoittaa sitä joukon $Y$ alkiota, jonka kuvaus $f\colon X \to Y$ liittää alkioon $x \in X$. Alkio $f(x)$ on nimeltään alkion $x$ *kuva-alkio*.

**Esimerkki 5.1.2.** Koulusta tutut funktiot ovat kuvauksia. Esimerkiksi yhtälö $f(x) = 0{,}5x+1$ määrittelee kuvauksen $f\colon \mathbb{R} \to \mathbb{R}$. Tässä kuvauksessa alkion $x$ kuva-alkio on $f(x) = 0{,}5x + 1$. Kuvaus $f$ liittää siis jokaiseen reaalilukuun toisen reaaliluvun, joka saadaan kertomalla alkuperäinen luku luvulla 0,5 ja lisäämällä tulokseen 1.

Laskemalla huomataan, että esimerkiksi $f(0) = 0{,}5 \cdot 0 + 1 = 1$ ja $f(2) = 0{,}5 \cdot 2 + 1 = 2$. Tällöin voidaan merkitä myös $0 \mapsto 1$ ja $2 \mapsto 2$.

Piirtämällä koordinaatistoon kaikki pisteet $(x, y)$, missä $x \in \mathbb{R}$ ja $y = f(x)$, saadaan piirrettyä funktion $f$ kuvaaja. Kuvaajan pisteen $y$-koordinaatti on siis $x$-koordinaattia vastaava kuva-alkio $f(x)$. Sanotaan myös, että $f(x)$ on funktion *arvo* kohdassa $x$.

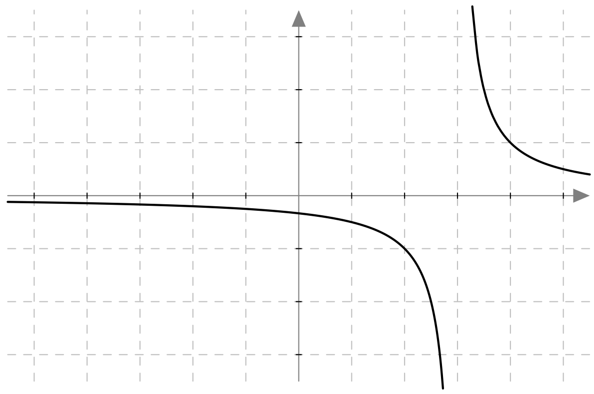



Kuva 5.1: Osa esimerkissä 5.1.2 tarkastellun funktion $f$ kuvaajasta.

**Esimerkki 5.1.3.** Yhtälö

$$g(x) = \frac{1}{x-3}$$

määrittelee kuvauksen $g\colon \mathbb{R} \setminus \{3\} \to \mathbb{R}$. Jos $x \neq 3$, on jakaja nollasta poikkeava ja osamäärä on määritelty. Lisäksi osamäärä on aina yksikäsitteinen reaaliluku (ei ole mahdollista saada monta erilaista tulosta samalla luvulla $x$). Kuvauksen määritelmä siis toteutuu: sääntö $g$ liittää joukon $\mathbb{R} \setminus \{3\}$ jokaiseen alkioon täsmälleen yhden alkion joukosta $\mathbb{R}$.



Kuva 5.2: Osa esimerkissä 5.1.3 tarkastellun funktion $g\colon \mathbb{R} \setminus \{3\} \to \mathbb{R}$ kuvaajasta.

---

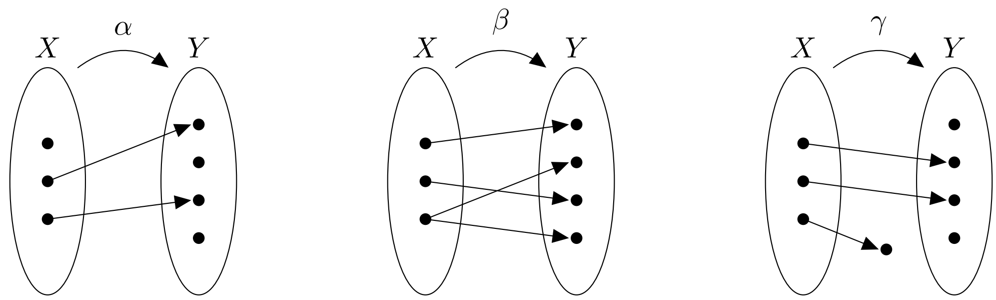
Edellisissä esimerkeissä esiintyneiden kuvausten lähtönä ja maalina oli reaalilukujen joukko tai jokin sen osajoukko. Kuvauksen määritelmän mukaan lähtö ja maali voivat kuitenkin olla mitä tahansa joukkoja.

**Esimerkki 5.1.4.** Olkoon $X$ kaikkien niiden opiskelijoiden joukko, jotka saivat opinto-oikeuden Helsingin yliopistoon 1.9.2014. Määritellään sääntö $f$ asettamalla

$$f(x) = \text{opiskelijan } x \text{ syksyn 2014 aikana suorittama opintopistemäärä.}$$

Havaitaan, että näin määritelty $f$ on kuvaus joukosta $X$ joukkoon $\mathbb{Q}$, sillä se liittää joukon $X$ jokaiseen alkioon täsmälleen yhden rationaaliluvun.

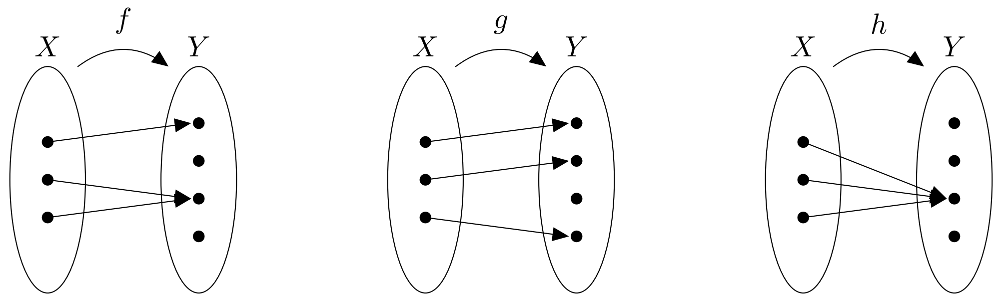
**Esimerkki 5.1.5.** Alla on havainnollistettu sääntöjä $\alpha$, $\beta$ ja $\gamma$ kuvassa 5.3. Osoittautuu, että mikään niistä ei ole kuvaus joukosta $X$ joukkoon $Y$.




Kuva 5.3: Säännöt $\alpha$, $\beta$ ja $\gamma$ eivät ole kuvauksia joukosta $X$ joukkoon $Y$.

Sääntö $\alpha$ ei ole kuvaus $X \to Y$, sillä joukossa $X$ on alkio, johon $\alpha$ ei liitä yhtään joukon $Y$ alkiota. Sääntö $\beta$ ei ole kuvaus $X \to Y$, sillä joukossa $X$ on alkio, johon $\beta$ liittää useamman kuin yhden joukon $Y$ alkion. Sääntö $\gamma$ ei ole kuvaus $X \to Y$, sillä joukossa $X$ on alkio, johon liitetty alkio ei kuulu joukkoon $Y$.

**Esimerkki 5.1.6.** Alla on havainnollistettu sääntöjä $f$, $g$ ja $h$ kuvassa 5.4. Ne kaikki ovat kuvauksia joukosta $X$ joukkoon $Y$, sillä ne liittävät joukon $X$ jokaiseen alkioon täsmälleen yhden alkion joukosta $Y$.




Kuva 5.4: Säännöt $f$, $g$ ja $h$ ovat kuvauksia joukosta $X$ joukkoon $Y$.

Huomaa, että maalissa $Y$ voi olla sellaisia alkioita, joihin ei kuvaudu yhtään alkiota. Toisaalta samalla maalin $Y$ alkiolle voi kuvautua useampi alkio.

**Esimerkki 5.1.7.** Oletetaan, että $a,\, b \in \mathbb{Z}$ ja $b \neq 0$. Määritellään sääntö $h$ asettamalla

$$h\left(\frac{a}{b}\right) = \frac{2a}{a^2 + b^2}\,.$$

Onko tällä tavalla määritelty $h$ kuvaus $\mathbb{Q} \to \mathbb{Q}$?

Tiedetään, että jokainen rationaaliluku voidaan kirjoittaa muodossa $a/b$, missä $a,\, b \in \mathbb{Z}$ ja $b \neq 0$. Lisäksi oletuksesta $b \neq 0$ seuraa, että $b^2 > 0$. Näin ollen nimittäjä $a^2 + b^2 \geq 0 + b^2 > 0$ ja siten osamäärä $2a/(a^2 + b^2)$ on aina määritelty.

Ongelma syntyy siitä, että jokainen rationaaliluku voidaan kirjoittaa usealla eri tavalla muodossa $a/b$, missä $a,\, b \in \mathbb{Z}$ ja $b \neq 0$. Esimerkiksi luku $1/2$ voidaan kirjoittaa myös muodossa $2/4$ tai $4/8$. Sen kuva-alkion pitäisi kuitenkin olla yksikäsitteinen. Toisin sanottuna tulos ei saisi riippua siitä, missä muodossa alkuperäinen luku on esitetty. Huomataan, että näin ei kuitenkaan ole:

$$h\left(\frac{1}{2}\right) = \frac{2 \cdot 1}{1^2 + 2^2} = \frac{2}{5}$$

$$h\left(\frac{2}{4}\right) = \frac{2 \cdot 2}{2^2 + 4^2} = \frac{4}{20} = \frac{1}{5}$$

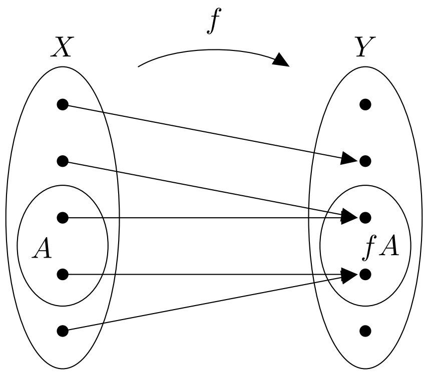
Näin $h(1/2) \neq h(2/4)$, vaikka $1/2 = 2/4$. Sääntö $h$ siis liittää alkioon $1/2$ ainakin kaksi eri alkiota joukosta $\mathbb{Q}$, joten $h$ ei ole kuvaus $\mathbb{Q} \to \mathbb{Q}$.

## 5.2 Kuva

**Määritelmä 5.2.1.** Oletetaan, että $f\colon X \to Y$ on kuvaus. Oletetaan lisäksi, että $A \subset X$. Joukon $A$ *kuva* kuvauksessa $f$ on joukko

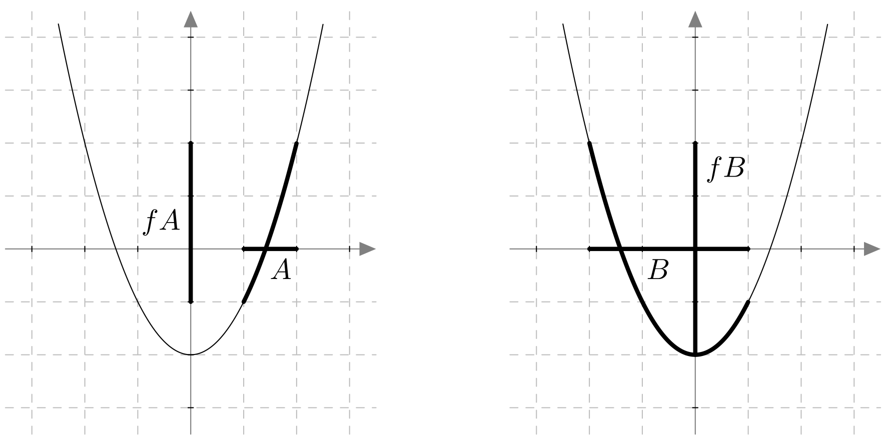
$$fA = \{\, y \in Y \mid y = f(a),\ \text{missä } a \in A \,\}.$$

Kuvan $fA$ muodostavat siis ne maalin alkiot, jotka ovat joukon $A$ alkioiden kuva-alkoita. Se voidaan joukkona merkitä myös lyhyesti $fA = \{\, f(a) \mid a \in A \,\}$.




Kuva 5.5: Kuvan $fA$ muodostavat joukon $A$ alkioiden kuva-alkiot.

**Esimerkki 5.2.2.** Tarkastellaan funktiota $f\colon \mathbb{R} \to \mathbb{R}$, jolla $f(x) = x^2 - 2$ kaikilla $x \in \mathbb{R}$. Funktion $f$ kuvaajan avulla voidaan päätellä, että esimerkiksi joukon $A = [1, 2]$ kuva on $fA = [-1, 2]$ ja joukon $B = [-2, 1]$ kuva on $fB = [-2, 2]$. Huomaa, että joukot $A$ ja $B$ merkitään vaaka-akselille, ja kuvat $fA$ ja $fB$ muodostuvat pystyakselille.

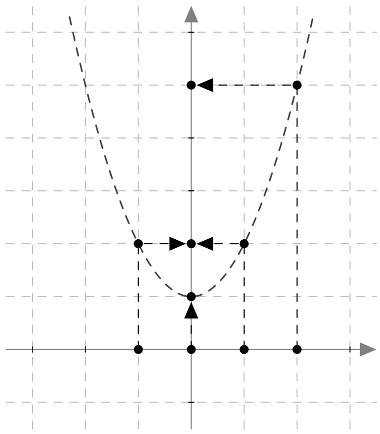



Kuva 5.6: Joukon $A = [1, 2]$ kuva $fA = [-1, 2]$ ja joukon $B = [-2, 1]$ kuva $fB = [-2, 2]$.

**Esimerkki 5.2.3.** Olkoon $f\colon \mathbb{Z} \to \mathbb{R}$ kuvaus, jolle $x \mapsto x^2 + 1$ kaikilla $x \in \mathbb{Z}$. Merkitään $A = \{-1, 0, 1, 2\}$. Määritetään $fA$.

Kuvan määritelmän mukaan

$$\begin{aligned} fA &= \{y \in \mathbb{R} \mid y = f(a), \text{ missä } a \in A\} = \{f(a) \mid a \in A\} = \{f(-1), f(0), f(1), f(2)\} \\ &= \{1, 2, 5\} \end{aligned}$$



Kuva 5.7: Joukon $A = \{-1, 0, 1, 2\}$ kuva on $fA = \{1, 2, 5\}$.

---

**Esimerkki 5.2.4.** Oletetaan, että $A = \{1, 2, 3\}$. Potenssijoukon $\mathcal{P}(A)$ muodostavat kaikki joukon $A$ osajoukot. Tässä tapauksessa

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, A\}.$$

Tarkastellaan kuvausta $f\colon \mathcal{P}(A) \to \mathcal{P}(A)$, jolla $f(X) = X \cup \{1\}$ kaikilla $X \in \mathcal{P}(A)$. Siis esimerkiksi $f(\emptyset) = \{1\}$, $f(\{2\}) = \{1, 2\}$, $f(\{3\}) = \{1, 3\}$ ja $f(A) = A$.

Joukko $B = \{\{2\}, \{2, 3\}\}$ on joukon $\mathcal{P}(A)$ osajoukko, sillä $\{2\} \in \mathcal{P}(A)$ ja $\{2, 3\} \in \mathcal{P}(A)$. Joukon $B$ kuva kuvauksessa $f$ on

$$\begin{aligned} fB &= \{Y \in \mathcal{P}(A) \mid Y = f(X), \text{ missä } X \in B\} = \{f(X) \mid X \in B\} = \{f(\{2\}), f(\{2, 3\})\} \\ &= \{\{1, 2\}, A\} \end{aligned}$$

Joskus on oltava erityisen tarkkana sen suhteen, tarkoitetaanko kuva-alkiota vai kuvaa. Esimerkiksi tyhjä joukko $\emptyset$ on yhtä aikaa joukon $\mathcal{P}(A)$ alkio ja osajoukko. Alkion $\emptyset \in \mathcal{P}(A)$ kuva-alkio on $f(\emptyset) = \{1\}$. Osajoukon $\emptyset \subset \mathcal{P}(A)$ kuva on

$$f\emptyset = \{Y \in \mathcal{P}(A) \mid Y = f(X), \text{ missä } X \in \emptyset\} = \emptyset.$$

Korostamme kuva-alkio ja kuvan eroa käyttämällä kuva-alkion tapauksessa aaltosulkuja ja jättämällä kuvan tapauksessa sulut pois. Merkintä $f(\emptyset)$ tarkoittaa siis alkion $\emptyset$ kuva-alkiota ja merkintä $f\emptyset$ osajoukon $\emptyset$ kuvaa. Kaikissa kirjoissa näin ei kuitenkaan tehdä. Silloin on asiayhteydestä pääteltävä, kumpi käsite on kysymyksessä.

Seuraavassa esimerkissä tarkastellaan joukkojen $A$ ja $B$ yhdisteen kuvaa $f[A \cup B]$. Tässä merkinnässä sulkuja ei voi jättää pois, joten käytämme hakasulkuja, jotta ero kuva-alkio ja kuvan välillä olisi mahdollisimman selkeä.

**Esimerkki 5.2.5.** Olkoon $f \colon X \to Y$ kuvaus. Osoitetaan, että $f[A \cup B] = fA \cup fB$ kaikilla joukoilla $A$, $B \subset X$.

Oletetaan, että $A$, $B \subset X$. Koska väitteenä on kahden joukon identtisyys, perustellaan sisältyminen molempiin suuntiin:

"$\subset$": Oletetaan, että $y \in f[A \cup B]$. Kuvan määritelmän mukaan tällöin $y \in Y$ ja $y = f(x)$ jollakin $x \in A \cup B$. Koska $x \in A \cup B$, niin $x \in A$ tai $x \in B$. Tapaustarkastelu:

- Jos $x \in A$, niin kuvan määritelmän mukaan $f(x) \in fA$. Koska $y = f(x)$, niin $y \in fA$.
- Jos $x \in B$, niin kuvan määritelmän mukaan $f(x) \in fB$. Koska $y = f(x)$, niin $y \in fB$.

Molemmissa tapauksissa voidaan päätellä, että $y \in fA \cup fB$.

"$\supset$": Oletetaan, että $y \in fA \cup fB$. Tällöin $y \in fA$ tai $y \in fB$. Tapaustarkastelu:

- Jos $y \in fA$, niin kuvan määritelmän mukaan $y = f(a)$ jollakin $a \in A$. Koska $a \in A$, niin $a \in A \cup B$. Tällöin kuvan määritelmän mukaan $f(a) \in f[A \cup B]$. Koska $y = f(a)$, niin $y \in f[A \cup B]$.
- Jos $y \in fB$, niin kuvan määritelmän mukaan $y = f(b)$ jollakin $b \in B$. Koska $b \in B$, niin $b \in A \cup B$. Tällöin kuvan määritelmän mukaan $f(b) \in f[A \cup B]$. Koska $y = f(b)$, niin $y \in f[A \cup B]$.

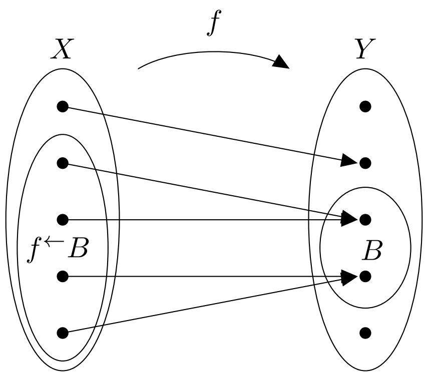
Päättelyt "$\subset$" ja "$\supset$" yhdessä osoittavat, että $f[A \cup B] = fA \cup fB$. Koska tarkastellut joukot $A$ ja $B$ saattoivat olla mitä tahansa joukon $X$ osajoukkoja, pätee tulos kaikilla joukon $X$ osajoukoilla $A$ ja $B$.

## 5.3 Alkukuva

**Määritelmä 5.3.1.** Oletetaan, että $f\colon X \to Y$ on kuvaus. Oletetaan lisäksi, että $B \subset Y$. Joukon $B$ *alkukuva* kuvauksessa $f$ on joukko

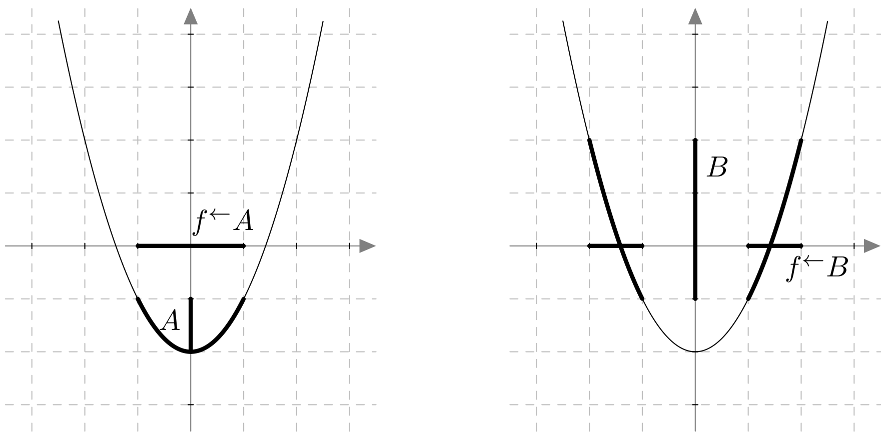
$$f^{\leftarrow}B = \{\, x \in X \mid f(x) \in B \,\}.$$

Alkukuvan $f^{\leftarrow}B$ muodostavat siis ne lähdön alkiot, joiden kuva-alkiot kuuluvat joukkoon $B$. Joissakin kirjoissa joukon $B$ alkukuvalle käytetään merkintää $f^{-1}B$ tai $f^{-1}(B)$.




Kuva 5.8: Alkukuvan $f^{\leftarrow}B$ muodostavat ne lähdön alkiot, jotka kuvautuvat joukkoon $B$.

**Esimerkki 5.3.2.** Tarkastellaan funktiota $f\colon \mathbb{R} \to \mathbb{R}$, jolla $f(x) = x^2 - 2$ kaikilla $x \in \mathbb{R}$. Funktion $f$ kuvaajan avulla voidaan päätellä, että esimerkiksi joukon $A = [-2,-1]$ alkukuva on $f^{\leftarrow}A = [-1,1]$ ja joukon $B = [-1,2]$ alkukuva on $f^{\leftarrow}B = [-2,-1] \cup [1,2]$. Huomaa, että joukot $A$ ja $B$ merkitään pystyakselille, ja alkukuvat $f^{\leftarrow}A$ ja $f^{\leftarrow}B$ muodostuvat vaaka-akselille.




Kuva 5.9: Joukon $A$ alkukuva $f^{\leftarrow}A$ ja joukon $B$ alkukuva $f^{\leftarrow}B$.

**Esimerkki 5.3.3.** Olkoon $f\colon \mathbb{Z} \to \mathbb{R}$ kuvaus, jolle $x \mapsto x^2 + 1$ kaikilla $x \in \mathbb{Z}$. Merkitään $B = \{-1, 1, 2, 3\}$. Määritetään $f^{\leftarrow}B$.

Alkukuvan määritelmän mukaan

$$f^{\leftarrow}B = \{x \in \mathbb{Z} \mid f(x) \in B\} = \{x \in \mathbb{Z} \mid x^2 + 1 \in B\} = \{x \in \mathbb{Z} \mid x^2 + 1 \in \{-1, 1, 2, 3\}\}.$$

Alkukuvan määrittämiseksi on siis ratkaistava kokonaislukujen joukossa yhtälöt $x^2 + 1 = -1$, $x^2 + 1 = 1$, $x^2 + 1 = 2$ ja $x^2 + 1 = 3$. Koska kaikilla $x \in \mathbb{Z}$ pätee $x^2 \geq 0$, ensimmäisellä yhtälöllä ei ole ratkaisuja. Toisella yhtälöllä on täsmälleen yksi ratkaisu:

$$x^2 + 1 = 1 \;\Leftrightarrow\; x^2 = 0 \;\Leftrightarrow\; x = 0.$$

Kolmannella yhtälöllä on kaksi ratkaisua:

$$x^2 + 1 = 2 \;\Leftrightarrow\; x^2 = 1 \;\Leftrightarrow\; x = -1 \;\vee\; x = 1.$$

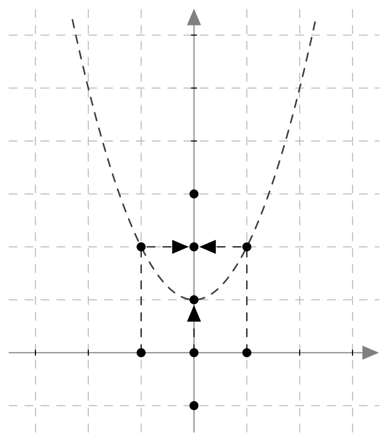
Viimeisellä yhtälöllä ei ole ratkaisua kokonaislukujen joukossa, sillä

$$x^2 + 1 = 3 \;\Leftrightarrow\; x^2 = 2 \;\Leftrightarrow\; x = -\sqrt{2} \;\vee\; x = \sqrt{2}.$$

Alkukuvaksi saadaan siis

$$f^{\leftarrow}B = \{x \in \mathbb{Z} \mid f(x) \in B\} = \{-1, 0, 1\}.$$

Sitä on havainnollistettu alla kuvassa 5.10.



Kuva 5.10: Joukon $B = \{-1, 1, 2, 3\}$ alkukuva on $f^{\leftarrow}B = \{-1, 0, 1\}$.

---

**Esimerkki 5.3.4.** Oletetaan, että $A = \{1, 2, 3\}$. Potenssijoukon $\mathcal{P}(A)$ muodostavat kaikki joukon $A$ osajoukot. Tässä tapauksessa

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, A\}.$$

Tarkastellaan esimerkistä 5.2.4 tuttua kuvausta $f\colon \mathcal{P}(A) \to \mathcal{P}(A)$, jolla $f(X) = X \cup \{1\}$ kaikilla $X \in \mathcal{P}(A)$. Siis esimerkiksi $f(\{2\}) = \{1,2\}$, $f(\{3\}) = \{1,3\}$ ja $f(A) = A$.

Joukko $B = \{\{2\},\{1,3\}\}$ on joukon $\mathcal{P}(A)$ osajoukko, sillä $\{2\} \in \mathcal{P}(A)$ ja $\{1,3\} \in \mathcal{P}(A)$. Joukon $B$ alkukuva kuvauksessa $f$ on

$$\begin{aligned} f^{\leftarrow}B &= \{X \in \mathcal{P}(A) \mid f(X) \in B\} = \{X \in \mathcal{P}(A) \mid f(X) = \{2\} \ \lor \ f(X) = \{1,3\}\} \\ &= \{\{3\},\{1,3\}\} \end{aligned}$$

Myös joukko $C = \{\{2,3\}\}$ on joukon $\mathcal{P}(A)$ osajoukko, sillä $\{2,3\} \in \mathcal{P}(A)$. Sen alkukuva kuvauksessa $f$ on

$$f^{\leftarrow}C = \{X \in \mathcal{P}(A) \mid f(X) \in C\} = \{X \in \mathcal{P}(A) \mid f(X) = \{2,3\}\} = \emptyset.$$

Huomaa, että alkukuva on aina olemassa, mutta joskus se saattaa olla tyhjä joukko kuten tässä esimerkissä $f^{\leftarrow}C = \emptyset$.

---

Seuraavassa esimerkissä tarkastellaan joukkojen $C$ ja $D$ leikkauksen alkukuvaa $f^{\leftarrow}[C \cap D]$. Jos alkukuvan yhteydessä tarvitaan sulkuja, käytämme hakasulkuja kuten kuvan tapauksessa.

**Esimerkki 5.3.5.** Olkoon $f\colon X \to Y$ kuvaus. Osoitetaan, että $f^{\leftarrow}[C \cap D] = f^{\leftarrow}C \cap f^{\leftarrow}D$ kaikilla joukoilla $C$, $D \subset Y$.

Oletetaan, että $C$, $D \subset Y$. Koska väitteenä on kahden joukon identtisyys, perustellaan sisältyminen molempiin suuntiin:

"$\subset$": Oletetaan, että $x \in f^{\leftarrow}[C \cap D]$. Tällöin alkukuvan määritelmän mukaan $x \in X$ ja $f(x) \in C \cap D$. Tästä voidaan päätellä, että $f(x) \in C$ ja $f(x) \in D$. Koska $x \in X$ ja $f(x) \in C$, niin alkukuvan määritelmän mukaan $x \in f^{\leftarrow}C$. Toisaalta $x \in X$ ja $f(x) \in D$, joten alkukuvan määritelmän mukaan $x \in f^{\leftarrow}D$. Näin ollen $x \in f^{\leftarrow}C \cap f^{\leftarrow}D$.

"$\supset$": Oletetaan, että $x \in f^{\leftarrow}C \cap f^{\leftarrow}D$. Tällöin $x \in f^{\leftarrow}C$ ja $x \in f^{\leftarrow}D$. Koska $x \in f^{\leftarrow}C$, niin alkukuvan määritelmän mukaan $x \in X$ ja $f(x) \in C$. Toisaalta $x \in f^{\leftarrow}D$, joten alkukuvan määritelmästä seuraa, että $f(x) \in D$. Näin ollen $f(x) \in C \cap D$. Koska $x \in X$ ja $f(x) \in C \cap D$, niin alkukuvan määritelmän mukaan $x \in f^{\leftarrow}[C \cap D]$.

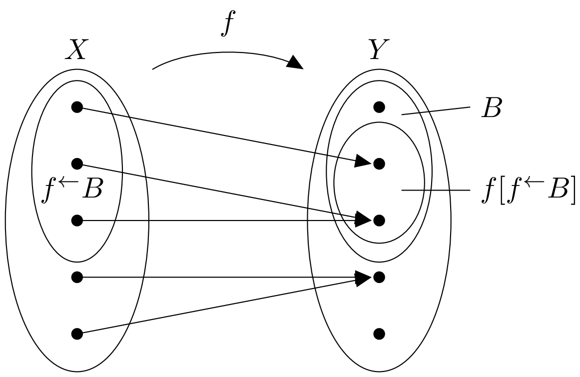
Päättelyt "$\subset$" ja "$\supset$" yhdessä osoittavat, että $f^{\leftarrow}[C \cap D] = f^{\leftarrow}C \cap f^{\leftarrow}D$. Koska tarkastellut joukot $C$ ja $D$ saattoivat olla mitä tahansa joukon $Y$ osajoukkoja, pätee tulos kaikilla joukon $Y$ osajoukoilla $C$ ja $D$.

---

Seuraavan esimerkin tulosta on havainnollistettu kuvassa 5.11.

**Esimerkki 5.3.6.** Olkoon $f\colon X \to Y$ kuvaus. Osoitetaan, että $f[f^{\leftarrow}B] \subset B$ kaikilla $B \subset Y$.

Oletetaan, että $B \subset Y$. Oletetaan, että $y \in f[f^{\leftarrow}B]$. Tällöin kuvan määritelmän mukaan $y \in Y$ ja $y = f(x)$ jollakin $x \in f^{\leftarrow}B$. Koska $x \in f^{\leftarrow}B$, niin alkukuvan määritelmän nojalla $f(x) \in B$. Koska $y = f(x)$, niin $y \in B$.




Kuva 5.11: Jos $B$ on maalin osajoukko, niin $f[f^{\leftarrow}B] \subset B$.

**Esimerkki 5.3.7.** Oletetaan, että $X$ ja $Y$ ovat joukkoja. Tutkitaan, päteekö yhtälö $f[f^{\leftarrow}B] = B$ kaikilla kuvauksilla $f\colon X \to Y$ ja osajoukoilla $B \subset Y$.

Kuvan 5.11 tilanteessa $f[f^{\leftarrow}B] \neq B$, joten vastaesimerkin keksiminen näyttäisi olevan mahdollista. Yritetään siis löytää sellainen kuvaus $f$ ja sellainen joukko $B$, että $f[f^{\leftarrow}B] \neq B$.

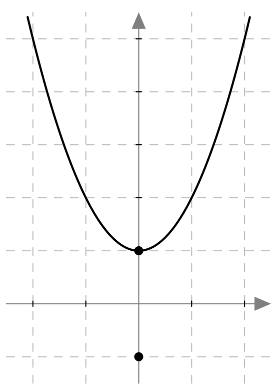
Olkoon $f\colon \mathbb{R} \to \mathbb{R}$ kuvaus, jolla $f(x) = x^2 + 1$ kaikilla $x \in \mathbb{R}$. Olkoon $B = \{-1, 1\}$. Tällöin

$$f^{\leftarrow}B = \{\, x \in \mathbb{R} \mid f(x) \in B \,\} = \{\, x \in \mathbb{R} \mid x^2 + 1 \in \{-1, 1\} \,\} = \{0\}.$$

Siten

$$f[f^{\leftarrow}B] = f\{0\} = \{\, f(x) \mid x \in \{0\} \,\} = \{f(0)\} = \{1\} \neq B.$$

Tilannetta on havainnollistettu alla kuvassa 5.12.



Kuva 5.12: Joukon $B = \{-1, 1\}$ alkukuvan kuva on $f[f^{\leftarrow}B] = \{1\}$.

## 5.4 Injektio

Injektion käsitteen avulla kuvauksia voidaan luokitella sen mukaan, kuvautuvatko jotkin alkiot samaksi alkioksi vai eivät.

**Määritelmä 5.4.1.** Kuvaus $f\colon X \to Y$ on *injektio*, jos kaikilla $x_1,\ x_2 \in X$ yhtälöstä $f(x_1) = f(x_2)$ seuraa, että $x_1 = x_2$.

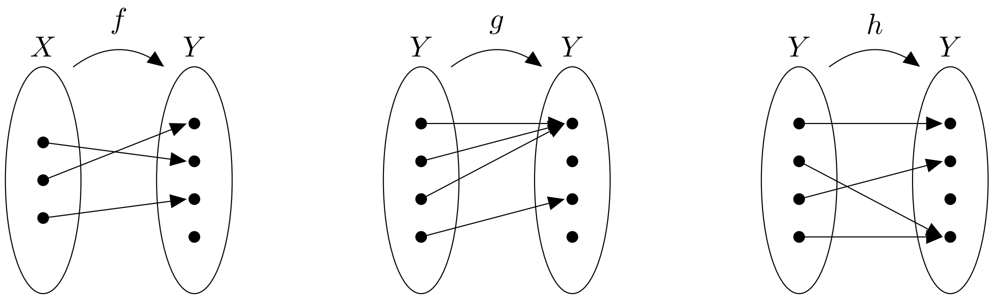
Logiikan symboleiden avulla injektion määritelmän ehto voidaan kirjoittaa seuraavasti:

$$\forall x_1 \forall x_2 (f(x_1) = f(x_2) \to x_1 = x_2).$$

Implikaation $P \to Q$ kontrapositio on $\neg Q \to \neg P$, joten määritelmän ehto voidaan kirjoittaa loogisesti ekvivalentissa muodossa

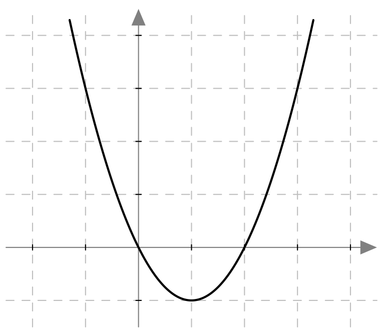
$$\forall x_1 \forall x_2 (x_1 \neq x_2 \to f(x_1) \neq f(x_2)).$$

Havaitaan, että injektio tarkoittaa kuvausta, jossa eri alkiot kuvautuvat aina eri alkioksi eivätkä koskaan samaksi. Injektion käsitettä on havainnollistettu alla kuvassa 5.13.




Kuva 5.13: Kuvaus $f$ on injektio, kuvaukset $g$ ja $h$ eivät ole injektiota.

**Esimerkki 5.4.2.** Tarkastellaan funktiota $f\colon \mathbb{R} \to \mathbb{R}$, jolla $f(x) = x^2 - 2x$ kaikilla $x \in \mathbb{R}$. Funktion $f$ kuvaajasta havaitaan, että $f$ ei ole injektio, sillä se saa saman arvon useassa eri kohdassa. Esimerkiksi $f(-1) = f(3)$, vaikka $-1 \neq 3$.



Kuva 5.14: Funktio $x \mapsto x^2 - 2x$ ei ole injektio.

**Esimerkki 5.4.3.** Olkoon $g\colon \mathbb{R} \to \mathbb{R}$ funktio, jolle $g(x) = 2 - 0{,}25x$ kaikilla $x \in \mathbb{R}$. Osa sen kuvaajasta on piirretty kuvaan 5.15. Kuvaajan perusteella funktio $g$ näyttäisi olevan injektio, sillä sen kuvaaja leikkaa minkä tahansa vaaka-akselin suuntaisen suoran enintään kerran. Siitä voidaan päätellä, että funktio $g$ ei saa mitään arvoa kahdessa eri kohdassa. Osoitetaan tämä vielä täsmällisesti.

Oletetaan, että $x_1,\, x_2 \in \mathbb{R}$. Oletetaan lisäksi, että $g(x_1) = g(x_2)$. Tällöin

$$2 - 0{,}25x_1 = 2 - 0{,}25x_2.$$

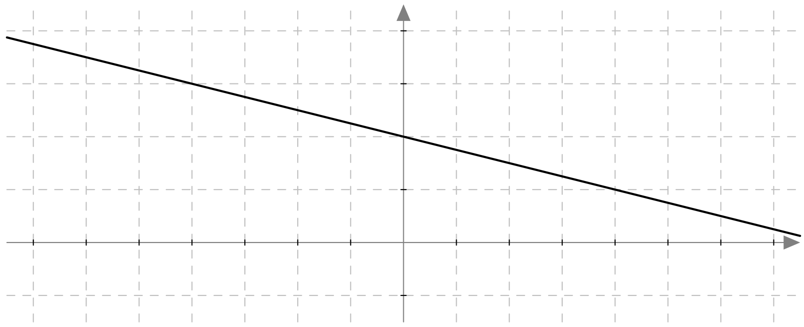
Vähentämällä tämän yhtälön molemmilta puolilta luku 2 päästään yhtälöön

$$-0{,}25x_1 = -0{,}25x_2.$$

Kertomalla yhtälön molemmat puolet luvulla $-4$ saadaan yhtälö

$$x_1 = x_2.$$

Näin on näytetty, että kaikilla $x_1,\, x_2 \in \mathbb{R}$ yhtälöstä $g(x_1) = g(x_2)$ seuraa, että $x_1 = x_2$. Siis kuvaus $g$ on injektio.

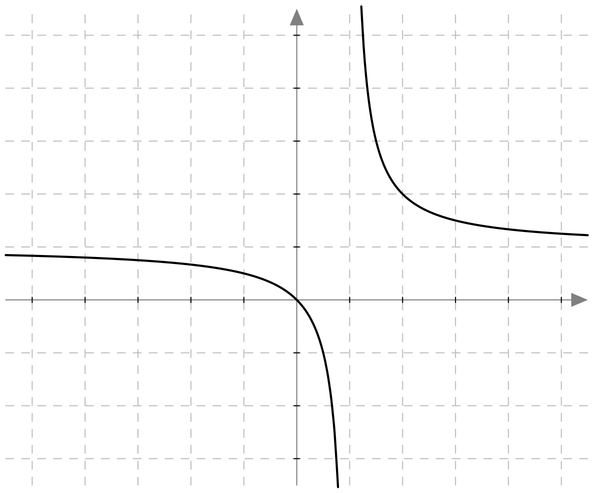


Kuva 5.15: Funktio $x \mapsto 2 - 0{,}25x$ on injektio.

**Esimerkki 5.4.4.** Tarkastellaan funktiota $h\colon \mathbb{R} \setminus \{1\} \to \mathbb{R}$, jolla

$$h(x) = \frac{x}{x-1}$$

kaikilla $x \in \mathbb{R} \setminus \{1\}$. Osa sen kuvaajasta on piirretty kuvaan 5.16. Kuvaajan perusteella funktio $h$ näyttäisi olevan injektio, sillä sen kuvaaja leikkaa minkä tahansa vaaka-akselin suuntaisen suoran enintään kerran. Siitä voidaan päätellä, että funktio $h$ ei saa mitään arvoa kahdessa eri kohdassa.



Kuva 5.16: Funktio $x \mapsto x/(x-1)$ on injektio.

Osoitetaan vielä täsmällisesti, että funktio $h$ on injektio. Oletetaan, että $x_1,\ x_2 \in \mathbb{R} \setminus \{1\}$. Oletetaan lisäksi, että $h(x_1) = h(x_2)$. Tällöin

$$\frac{x_1}{x_1 - 1} = \frac{x_2}{x_2 - 1}\,.$$

Kertomalla tämän yhtälön molemmat puolet nimittäjien tulolla $(x_1 - 1)(x_2 - 1)$ saadaan

$$x_1(x_2 - 1) = x_2(x_1 - 1).$$

Kertomalla sulut auki päästään yhtälöön

$$x_1x_2 - x_1 = x_1x_2 - x_2.$$

Vähentämällä tämän yhtälön molemmilta puolilta tulo $x_1x_2$ saadaan yhtälö

$$-x_1 = -x_2.$$

Kertomalla tämän yhtälön molemmat puolet luvulla $-1$ havaitaan, että

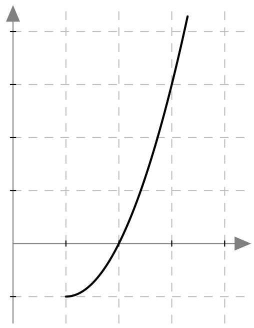
$$x_1 = x_2.$$

Näin on osoitettu, että kaikilla $x_1,\ x_2 \in \mathbb{R}$ yhtälöstä $h(x_1) = h(x_2)$ seuraa, että $x_1 = x_2$. Siis kuvaus $h$ on injektio.

---

Joissakin tapauksessa lähtöjoukko vaikuttaa siihen, onko kuvaus injektio vai ei. Esimerkissä 5.14 nähtiin, että kuvaus $x \mapsto x^2 - 2x$, jonka lähtö on $\mathbb{R}$, ei ole injektio. Seuraavassa esimerkissä osoitetaan, että kuvaus $x \mapsto x^2 - 2x$, jonka lähtö on $[1, \infty[$, on injektio.

**Esimerkki 5.4.5.** Tarkastellaan funktiota $\rho\colon [1, \infty[ \to \mathbb{R}$, jolle $\rho(x) = x^2 - 2x$ kaikilla $x \in \mathbb{R}$. Sen kuvaaja on piirretty kuvaan 5.17.



Kuva 5.17: Funktio $x \mapsto x^2 - 2x$, jonka lähtö on $[1, \infty[$, on injektio.

Osoitetaan, että $\rho$ on injektio. Oletetaan, että $a, b \in [1, \infty[$. Oletetaan lisäksi, että $\rho(a) = \rho(b)$. Tällöin $a^2 - 2a = b^2 - 2b$ eli

$$a^2 - b^2 - 2a + 2b = 0.$$

Tämä yhtälö voidaan kirjoittaa muodossa

$$(a + b)(a - b) - 2(a - b) = 0$$

ja edelleen muodossa

$$(a - b)(a + b - 2) = 0.$$

Tulon nollasäännön nojalla tämä yhtälö toteutuu, jos ja vain jos $a - b = 0$ tai $a + b - 2 = 0$. Nämä yhtälöt voidaan kirjoittaa myös muodossa $a = b$ ja $a = 2 - b$.

Tarkastellaan tarkemmin yhtälöä $a = 2 - b$. Oletuksen mukaan $b \in [1, \infty[$, joten $-b \leq -1$. Yhtälöstä $a = 2 - b$ saadaan näin arvio $a = 2 - b \leq 2 - 1 = 1$. Tästä voidaan päätellä, että yhtälö $a = 2 - b$ toteutuu välillä $[1, \infty[$, jos ja vain jos $a = 1 = b$.

Näin on osoitettu, että kaikilla $a, b \in [1, \infty[$ yhtälöstä $\rho(a) = \rho(b)$ seuraa, että $a = b$. Siis kuvaus $\rho$ on injektio.

## 5.5 Surjektio

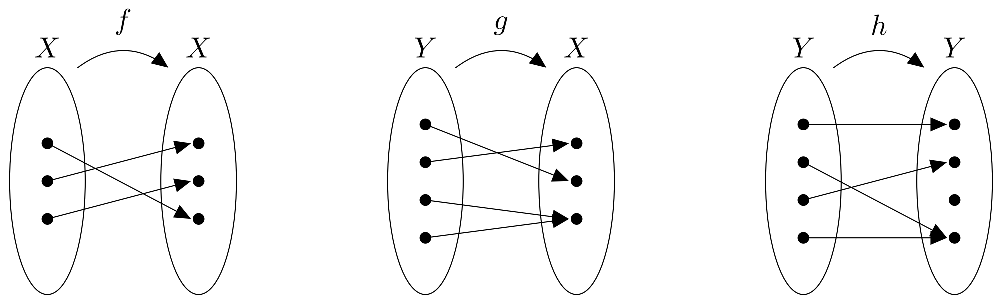
Surjektion käsitteen avulla kuvauksia voidaan luokitella sen mukaan, kuvautuuko kaikille maalin alkioille jokin alkio vai ei.

**Määritelmä 5.5.1.** Kuvaus $f\colon X \to Y$ on *surjektio*, jos jokaisella $y \in Y$ on olemassa ainakin yksi sellainen $x \in X$, että $f(x) = y$.

Logiikan symboleiden avulla surjektion määritelmän ehto voidaan kirjoittaa seuraavasti:

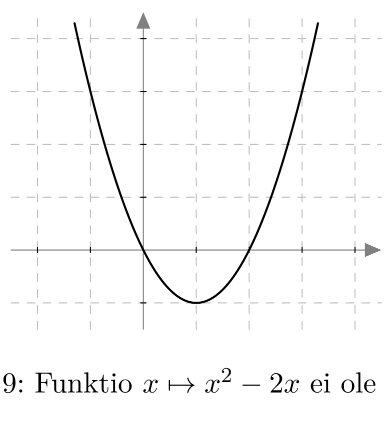
$$\forall y \exists x (f(x) = y).$$

Havaitaan, että surjektio tarkoittaa kuvausta, jossa kaikille maalin alkioille kuvautuu yksi tai useampi alkio. Surjektion käsitettä on havainnollistettu alla kuvassa 5.18.




Kuva 5.18: Kuvaukset $f$ ja $g$ ovat surjektioita, kuvaukset $h$ ei ole surjektio.

**Esimerkki 5.5.2.** Tarkastellaan funktiota $f\colon \mathbb{R} \to \mathbb{R}$, jolla $f(x) = x^2 - 2x$ kaikilla $x \in \mathbb{R}$. Funktion $f$ kuvaajasta havaitaan, että $f$ ei ole surjektio, sillä $f(x) \geq -1$ kaikilla $x \in \mathbb{R}$.



Kuva 5.19: Funktio $x \mapsto x^2 - 2x$ ei ole surjektio.

Perustellaan vielä täsmällisesti, että edellä tarkasteltu funktio $f\colon \mathbb{R} \to \mathbb{R}$, jolla $f(x) = x^2 - 2x$ kaikilla $x \in \mathbb{R}$, ei ole surjektio. Tehdään vastaoletus, että $f$ on surjektio. Silloin surjektion määritelmän mukaan jokaista $y \in \mathbb{R}$ kohti on olemassa sellainen $x \in \mathbb{R}$, että $f(x) = y$. Erityisesti esimerkiksi lukua $-2 \in \mathbb{R}$ kohti on olemassa sellainen $a \in \mathbb{R}$, että $f(a) = -2$. Tällöin $a^2 - 2a = -2$. Lisäämällä tämän yhtälön molemmille puolille luku 1 saadaan yhtälö

$$a^2 - 2a + 1 = -1.$$

Koska $(a-1)^2 = a^2 - 2a + 1$, voidaan saatu yhtälö kirjoittaa muodossa

$$(a-1)^2 = -1.$$

Näin on päädytty ristiriitaan, sillä minkään reaaliluvun toinen potenssi ei ole $-1$. Koska vastaoletus johti ristiriitaan, on alkuperäinen väite tosi. Siis $f$ ei ole surjektio.

Toinen tapa osoittaa, että funktio $f$ ei ole surjektio, on tarkastella yhtälöä $f(x) = -2$. Havaitaan, että

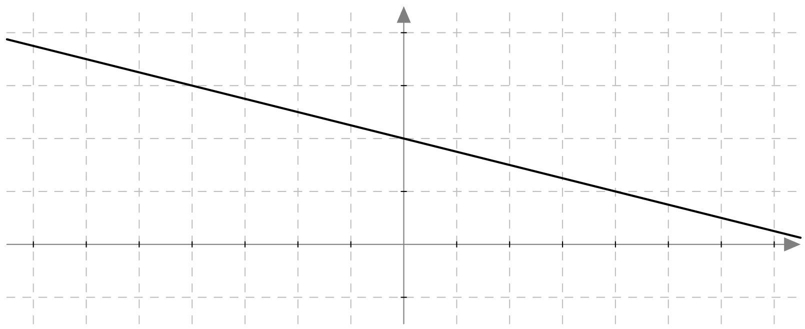
$$f(x) = -2 \;\Leftrightarrow\; x^2 - 2x = -2 \;\Leftrightarrow\; x^2 - 2x + 2 = 0.$$

Huomataan, että yhtälöllä $x^2 - 2x + 2 = 0$ ei ole ratkaisuja reaalilukujen joukossa, sillä sen diskriminantti on negatiivinen: Toisen asteen yhtälön ratkaisukaavalla saadaan

$$x = \frac{-(-2) \pm \sqrt{(-2)^2 - 4 \cdot 1 \cdot 2}}{2 \cdot 1} = \frac{2 \pm \sqrt{-4}}{2}.$$

Tästä nähdään, että yhtälön $x^2 - 2x + 2 = 0$ diskriminantti on $-4$. Tarkastellulla yhtälöllä ei ole ratkaisuja reaalilukujen joukossa, koska negatiivisen luvun neliöjuuri ei ole määritelty. Siis $f(x) \neq -2$ kaikilla $x \in \mathbb{R}$, joten $f\colon \mathbb{R} \to \mathbb{R}$ ei ole surjektio.

**Esimerkki 5.5.3.** Olkoon $g\colon \mathbb{R} \to \mathbb{R}$ funktio, jolle $g(x) = 2 - 0{,}25x$ kaikilla $x \in \mathbb{R}$. Osa sen kuvaajasta on piirretty kuvaan 5.20. Kuvaajan perusteella funktio $g$ näyttäisi olevan surjektio, sillä sen kuvaaja leikkaa minkä tahansa vaaka-akselin suuntaisen suoran ainakin kerran (jotkin niistä kuvan 5.20 ulkopuolella). Siitä voidaan päätellä, että funktio $g$ saa jokaisen arvon ainakin yhdessä kohdassa.

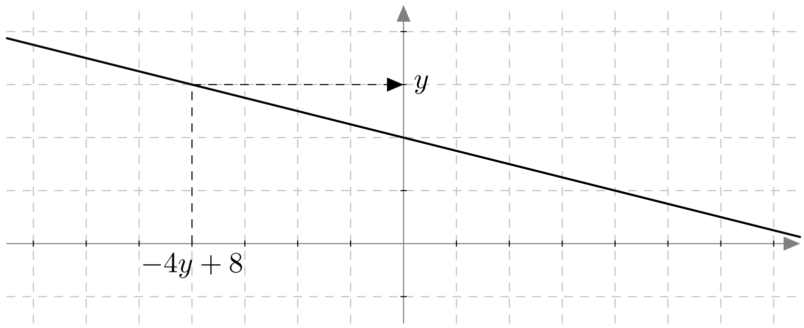


Kuva 5.20: Funktio $x \mapsto 2 - 0{,}25x$ on surjektio.

Osoitetaan vielä täsmällisesti, että edellä tarkasteltu funktio $g\colon \mathbb{R} \to \mathbb{R}$, jolle $g(x) = 2 - 0{,}25x$ kaikilla $x \in \mathbb{R}$, on surjektio. Oletetaan, että $y \in \mathbb{R}$. Tällöin myös $-4y + 8 \in \mathbb{R}$ ja lisäksi

$$g(-4y + 8) = 2 - 0{,}25 \cdot (-4y + 8) = 2 + y - 2 = y.$$

Näin on näytetty, että jokaista $y \in \mathbb{R}$ kohti on olemassa sellainen $x = -4y + 8 \in \mathbb{R}$, että $g(x) = y$. Siis $g$ on surjektio.



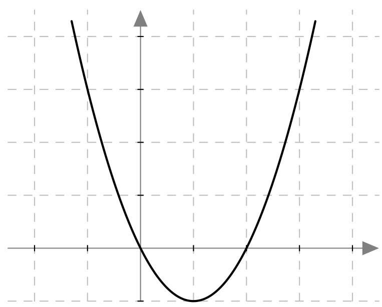

Kuva 5.21: Jokaista lukua $y \in \mathbb{R}$ kohti löytyy luku $x = -4y + 8 \in \mathbb{R}$, jolla $g(x) = y$.

Nyt herää kysymys, miten edellä osattiin ryhtyä tarkastelemaan juuri lukua $-4y + 8$. Se löydettiin ratkaisemalla $x$ yhtälöstä $g(x) = y$:

$$g(x) = y \;\Leftrightarrow\; 2 - 0{,}25x = y \;\Leftrightarrow\; -0{,}25x = y - 2 \;\Leftrightarrow\; x = -4(y - 2) = -4y + 8.$$

Tätä etsintävaihetta ei kuitenkaan tarvitse ottaa mukaan varsinaiseen perusteluun, vaan sen voi tehdä esimerkiksi suttupaperilla. Kun sopiva alkio on löytynyt, riittää perustella, että se kuuluu tarkastellun kuvauksen lähtöön ja että sen kuva-alkio on alkuperäinen $y$.

**Esimerkki 5.5.4.** Tarkastellaan kuvausta $\tau\colon \mathbb{R} \to [-1, \infty[$, jolle $\tau(x) = x^2 - 2x$ kaikilla $x \in \mathbb{R}$. Osa sen kuvaajasta on piirretty kuvaan 5.22. Kuvaajan perusteella funktio $\tau$ näyttäisi olevan surjektio, sillä sen maaliksi on valittu sopivasti $[-1, \infty[$.

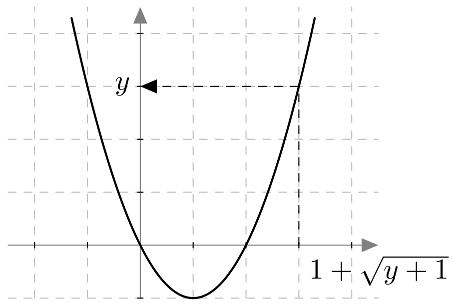


Kuva 5.22: Funktio $x \mapsto x^2 - 2x$, jonka maali on $[-1, \infty[$, on surjektio.

Osoitetaan, että kuvaus $\tau$ on surjektio. Oletetaan, että $y \in [-1, \infty[$. Tällöin $y \geq -1$, joten $y + 1 \geq 0$. Näin $1 + \sqrt{y+1}$ on määritelty ja lisäksi

$$\begin{aligned} \tau(1+\sqrt{y+1}) &= (1+\sqrt{y+1})^2 - 2(1+\sqrt{y+1}) \\ &= 1 + 2\sqrt{y+1} + (y+1) - 2 - 2\sqrt{y+1} \\ &= 1 + y + 1 - 2 \\ &= y. \end{aligned}$$

Näin on näytetty, että jokaista $y \in [-1, \infty[$ kohti on olemassa sellainen $x = 1 + \sqrt{y+1} \in \mathbb{R}$, että $\tau(x) = y$. Siis $\tau$ on surjektio.




Kuva 5.23: Jos $y \geq -1$, niin $\tau(1 + \sqrt{y+1}) = y$.

Jälleen herää kysymys, miten edellä osattiin ryhtyä tarkastelemaan juuri lukua $1 + \sqrt{y+1}$. Se löydettiin ratkaisemalla $x$ yhtälöstä $\tau(x) = y$:

$$\tau(x) = y \;\Leftrightarrow\; x^2 - 2x = y \;\Leftrightarrow\; x^2 - 2x - y = 0 \;\Leftrightarrow\; x = \frac{2 \pm \sqrt{4 - 4(-y)}}{2}$$

Ratkaisut voidaan sieventää:

$$x = \frac{2 \pm \sqrt{4 - 4(-y)}}{2} = \frac{2 \pm \sqrt{4(1+y)}}{2} = \frac{2 \pm 2\sqrt{1+y}}{2} = 1 \pm \sqrt{1+y} = 1 \pm \sqrt{y+1}$$

Huomataan, että todistuksessa olisi yhtä hyvin voinut käyttää lukua $1 - \sqrt{y+1}$.

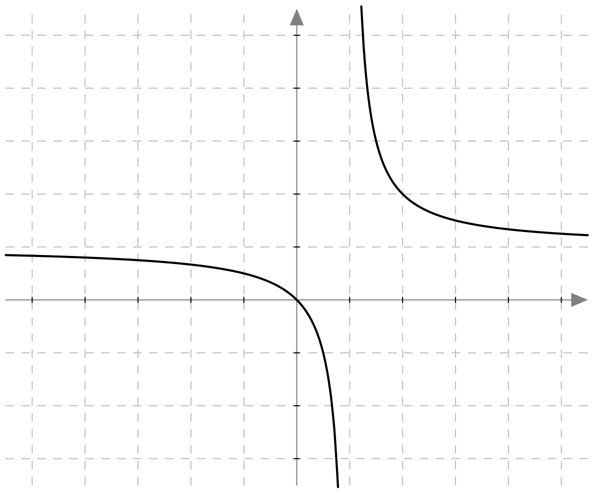
**Esimerkki 5.5.5.** Tarkastellaan funktiota $h\colon \mathbb{R} \setminus \{1\} \to \mathbb{R}$, jolla

$$h(x) = \frac{x}{x-1}$$

kaikilla $x \in \mathbb{R} \setminus \{1\}$. Osa sen kuvaajasta on piirretty kuvaan 5.24. Tutkitaan funktion $h$ surjektiivisuutta tutkimalla yhtälöä $h(x) = y$. Jos $x \in \mathbb{R} \setminus \{1\}$, voidaan päätellä seuraavasti:

$$\begin{aligned} h(x) = y \;&\Leftrightarrow\; \frac{x}{x-1} = y \;\Leftrightarrow\; x = y(x-1) \;\Leftrightarrow\; x = yx - y \;\Leftrightarrow\; x - yx = -y \\ &\Leftrightarrow\; (1-y)x = -y\,. \end{aligned}$$

Jos $y = 1$, alin yhtälö saa muodon $0x = -1$. Tämä yhtälö ei toteudu millään $x \in \mathbb{R} \setminus \{1\}$. Mikään joukon $\mathbb{R} \setminus \{1\}$ alkio ei siis kuvaudu luvuksi 1, joten kuvaus $h$ ei ole surjektio.



Kuva 5.24: Funktio $x \mapsto x/(x-1)$, jonka maali on $\mathbb{R}$, ei ole surjektio.

Perustellaan vielä toisella tavalla, että edellä tarkasteltu funktio $h$ ei ole surjektio. Tehdään vastaoletus, että $h$ on surjektio. Silloin surjektion määritelmän mukaan jokaista $y \in \mathbb{R}$ kohti on olemassa sellainen $x \in \mathbb{R} \setminus \{1\}$, että $h(x) = y$. Erityisesti esimerkiksi lukua $1 \in \mathbb{R}$ kohti on olemassa sellainen $a \in \mathbb{R} \setminus \{1\}$, että $h(a) = 1$ eli

$$\frac{a}{a-1} = 1.$$

Tästä seuraa, että $a = a - 1$ ja siten $0 = -1$. Tämä on ristiriita. Siis vastaoletus on epätosi ja alkuperäinen väite pätee. Näin ollen $h$ ei ole surjektio.

---

Kuvauksen surjektiivisuus tarkoittaa, että lähdön kuva on koko maali. Tämä osoitetaan seuraavassa lauseessa.

**Lause 5.5.6.** *Kuvaus $f\colon X \to Y$ on surjektio, jos ja vain jos $fX = Y$.*

*Todistus.* ”$\Rightarrow$”: Oletetaan, että $f\colon X \to Y$ on surjektio. Tavoitteena on näyttää, että $fX = Y$. Tehdään tämä osoittamalla sisältyminen molempiin suuntiin.

”$\subset$”: Oletetaan, että $b \in fX$. Tällöin kuvan määritelmän mukaan $b = f(x)$ jollakin $x \in X$. Koska kuvauksen $f$ maali on $Y$, niin $f(x) \in Y$. Koska $b = f(x)$, niin $b \in Y$.

”$\supset$”: Oletetaan, että $y \in Y$. Oletuksen mukaan $f\colon X \to Y$ on surjektio, joten on olemassa sellainen $x \in X$, jolla $f(x) = y$. Siis $y \in fX$ kuvan määritelmän nojalla.

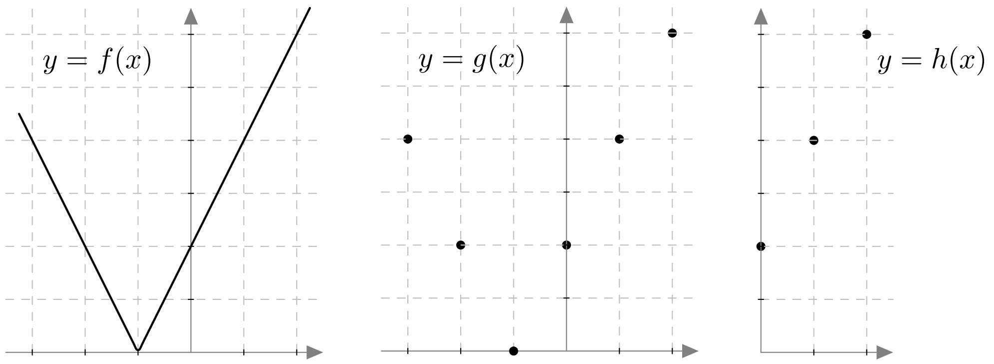
”$\Leftarrow$”: Oletetaan, että $fX = Y$. Tavoitteena on näyttää, että $f\colon X \to Y$ on surjektio.

Oletetaan, että $y \in Y$. Oletuksen mukaan $Y = fX$, joten $y \in fX$. Tällöin kuvan määritelmän mukaan on olemassa sellainen $x \in X$, että $f(x) = y$. $\square$

Esimerkeissä 5.4.2, 5.4.5, 5.5.2 ja 5.5.4 havaittiin, että kuvauksen $x \mapsto x^2 - 2x$ injektiivisyys ja surjektiivisuus riippuuvat siitä, mitä kuvauksen lähtö- ja maalijoukko ovat. Tämän vuoksi kuvausten sanotaan olevan samoja vain siinä tapauksessa, että niiden lähtö- ja maalijoukot ovat samat.

**Määritelmä 5.5.7.** Oletetaan, että $f$ ja $g$ ovat kuvauksia $X \to Y$. Kuvaukset $f$ ja $g$ ovat *samat* eli $f = g$, jos $f(x) = g(x)$ kaikilla $x \in X$.

**Esimerkki 5.5.8.** Tarkastellaan kuvauksia $f\colon \mathbb{R} \to [0, \infty[$, $g\colon \mathbb{Z} \to \mathbb{N}$ ja $h\colon \mathbb{N} \to \mathbb{N}$, joilla kaikilla $x \mapsto |2x + 2|$. Niiden kuvaajat on piirretty kuvaan 5.25. Kuvaukset $f$, $g$ ja $h$ ovat kaikki eri kuvauksia, sillä niiden lähtö- ja maalijoukot eivät ole samoja.




Kuva 5.25: Kuvaukset $f$, $g$ ja $h$ ovat eri kuvauksia.

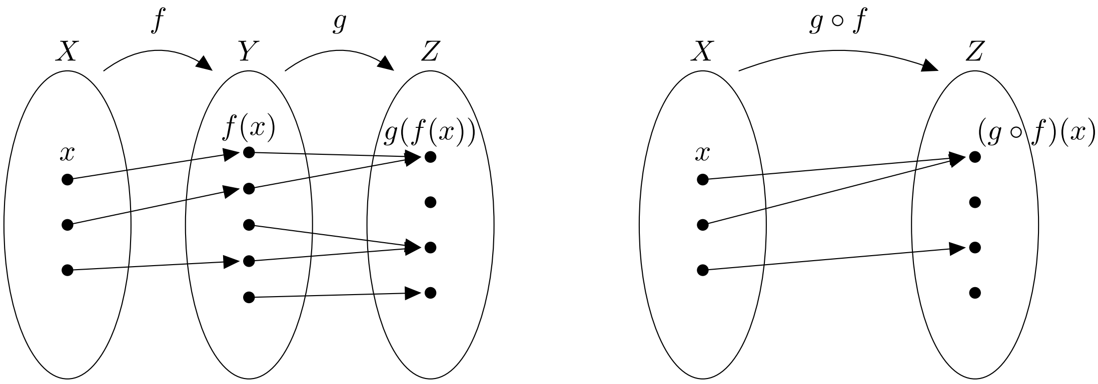
## 5.6 Yhdistetty kuvaus

**Määritelmä 5.6.1.** Oletetaan, että $f\colon X \to Y$ ja $g\colon Y \to Z$ ovat kuvauksia. *Yhdistetty kuvaus* $g \circ f\colon X \to Z$ määritellään asettamalla

$$(g \circ f)(x) = g(f(x))$$

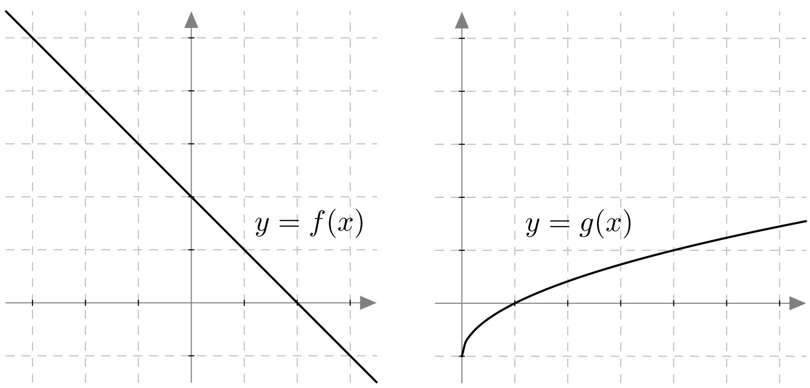
kaikilla $x \in X$.

Huomaa, että yhdistetty kuvaus määritellään vain siinä tapauksessa, että ensimmäisen kuvauksen maali on sama kuin jälkimmäisen kuvauksen lähtö. Huomaa myös kuvausten järjestys: ensimmäinen kuvaus kirjoitetaan yhdistetyssä kuvauksessa oikealle puolelle. Yhdistettyä kuvausta on havainnollistettu alla kuvassa 5.26.




Kuva 5.26: Yhdistetty kuvaus $g \circ f\colon X \to Z$ määritellään asettamalla $(g \circ f)(x) = g(f(x))$.

**Esimerkki 5.6.2.** Tarkastellaan funktiota $f\colon \mathbb{R} \to \mathbb{R}$, jolla $f(x) = 2 - x$ kaikilla $x \in \mathbb{R}$, ja funktiota $g\colon [0, \infty[ \to \mathbb{R}$, jolla $g(x) = \sqrt{x} - 1$ kaikilla $x \geq 0$. Niiden kuvaajat on piirretty kuvaan 5.27.



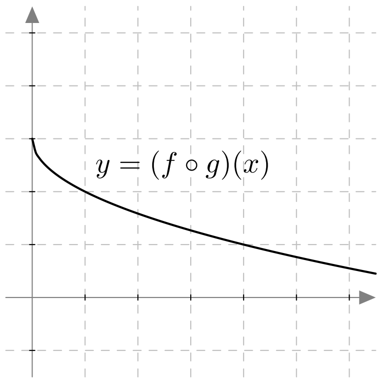

Kuva 5.27: Esimerkin 5.6.2 funktioiden $f$ ja $g$ kuvaajat.

Havaitaan, että yhdistetty kuvaus $g \circ f$ ei ole määritelty, koska kuvauksen $f\colon \mathbb{R} \to \mathbb{R}$ maali on eri kuin kuvauksen $g\colon [0, \infty[ \to \mathbb{R}$ lähtö.

Yhdistetty kuvaus $f \circ g$ puolestaan on määritelty, sillä kuvauksen $g\colon [0, \infty[ \to \mathbb{R}$ maali on sama kuin kuvauksen $f\colon \mathbb{R} \to \mathbb{R}$ lähtö. Yhdistetylle kuvaukselle $f \circ g\colon [0, \infty[ \to \mathbb{R}$ pätee

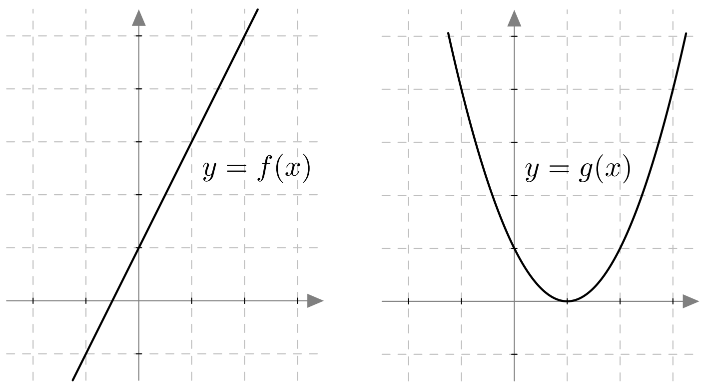
$$(f \circ g)(x) = f(g(x)) = f(\sqrt{x} - 1) = 2 - (\sqrt{x} - 1) = 2 - \sqrt{x} + 1 = 3 - \sqrt{x}.$$

Sen kuvaaja on piirretty kuvaan 5.28.




Kuva 5.28: Yhdistetyn funktion $f \circ g$ kuvaaja.

**Esimerkki 5.6.3.** Tarkastellaan funktioita $f\colon \mathbb{R} \to \mathbb{R}$ ja $g\colon \mathbb{R} \to \mathbb{R}$, joilla $f(x) = 1 + 2x$ ja $g(x) = (x - 1)^2$ kaikilla $x \in \mathbb{R}$. Niiden kuvaajat on piirretty kuvaan 5.29.




Kuva 5.29: Esimerkin 5.6.3 funktioiden $f$ ja $g$ kuvaajat.

Yhdistetty kuvaus $g \circ f\colon \mathbb{R} \to \mathbb{R}$ on määritelty. Sille pätee

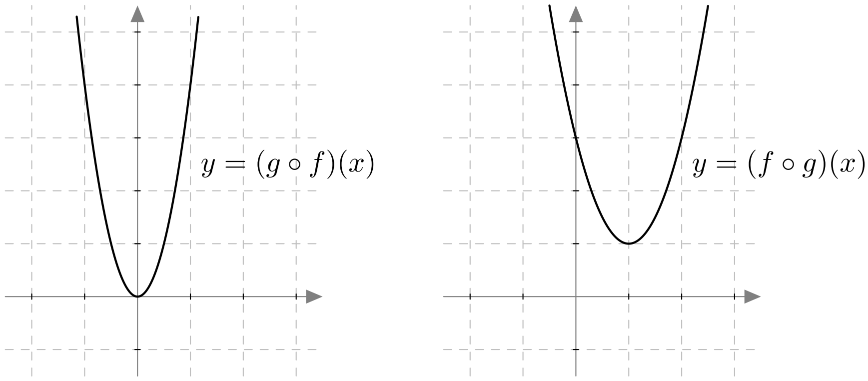
$$(g \circ f)(x) = g(f(x)) = g(1 + 2x) = (1 + 2x - 1)^2 = (2x)^2 = 4x^2$$

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

Myös yhdistetty kuvaus $f \circ g\colon \mathbb{R} \to \mathbb{R}$ on määritelty. Sille pätee

$$\begin{aligned}(f \circ g)(x) &= f(g(x)) = f((x-1)^2) = 1 + 2(x-1)^2 = 1 + 2(x^2 - 2x + 1) \\ &= 1 + 2x^2 - 4x + 2 = 2x^2 - 4x + 3\end{aligned}$$

Yhdistettyjen funktioiden $g \circ f$ ja $f \circ g$ kuvaajat on piirretty kuvaan 5.30. Havaitaan, että $g \circ f \neq f \circ g$, sillä esimerkiksi $(g \circ f)(0) = 0$ mutta $(f \circ g)(0) = 3$.




Kuva 5.30: Esimerkin 5.6.3 yhdistettyjen funktioiden $g \circ f$ ja $f \circ g$ kuvaajat.

---

Seuraavissa esimerkeissä osoitetaan, että injektiivisistä kuvauksista yhdistetty kuvaus on injektio ja surjektiivisista kuvauksista yhdistetty kuvaus on surjektio.

**Esimerkki 5.6.4.** Oletetaan, että $f\colon X \to Y$ ja $g\colon Y \to Z$ ovat injektioita. Osoitetaan, että yhdistetty kuvaus $g \circ f\colon X \to Z$ on injektio.

Oletetaan, että $a, b \in X$. Oletetaan lisäksi, että $(g \circ f)(a) = (g \circ f)(b)$. Tämä yhtälö voidaan yhdistetyn kuvauksen määritelmän nojalla kirjoittaa muodossa $g(f(a)) = g(f(b))$. Kuvauksen $g$ injektiivisyyden nojalla tästä yhtälöstä seuraa, että $f(a) = f(b)$. Myös kuvaus $f$ on injektio, joten yhtälöstä $f(a) = f(b)$ seuraa, että $a = b$.

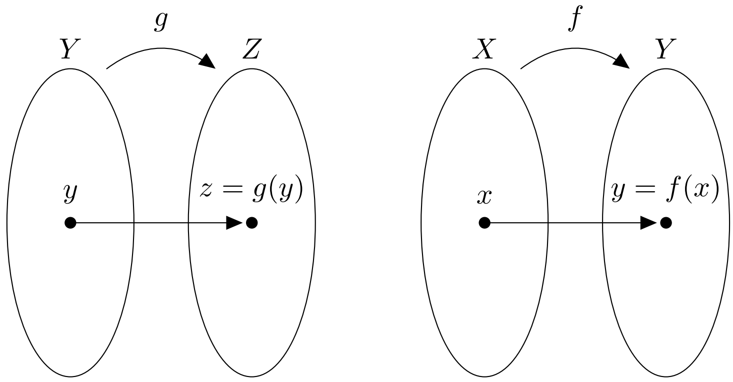
Näin on näytetty, että yhtälöstä $(g \circ f)(a) = (g \circ f)(b)$ seuraa, että $a = b$. Siis $g \circ f$ on injektio.

**Esimerkki 5.6.5.** Oletetaan, että $f\colon X \to Y$ ja $g\colon Y \to Z$ ovat surjektioita. Osoitetaan, että yhdistetty kuvaus $g \circ f\colon X \to Z$ on surjektio.

Oletetaan, että $z \in Z$. Koska $g$ on surjektio, on olemassa sellainen $y \in Y$, että $g(y) = z$. Koska myös $f$ on surjektio, on olemassa sellainen $x \in X$, että $f(x) = y$. On siis olemassa sellainen $x \in X$, että

$$(g \circ f)(x) = g(f(x)) = g(y) = z.$$

Tämä tarkoittaa, että $g \circ f$ on surjektio. Ratkaisun välivaiheita on havainnollistettu kuvassa 5.31.




Kuva 5.31: Kuvausten $g$ ja $f$ surjektiivisuuden avulla löydetään ensin $y$ ja sitten $x$.

**Esimerkki 5.6.6.** Oletetaan, että $f\colon X \to Y$, $g\colon Y \to Z$ ja $h\colon Z \to W$ ovat kuvauksia. Osoitetaan, että kuvausten yhdistäminen on liitännäinen operaatio eli että yhdistetyt kuvaukset $h \circ (g \circ f)\colon X \to W$ ja $(h \circ g) \circ f\colon X \to W$ ovat samat.

Oletetaan, että $x \in X$. Yhdistetyn kuvauksen määritelmän mukaan

$$(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))).$$

ja

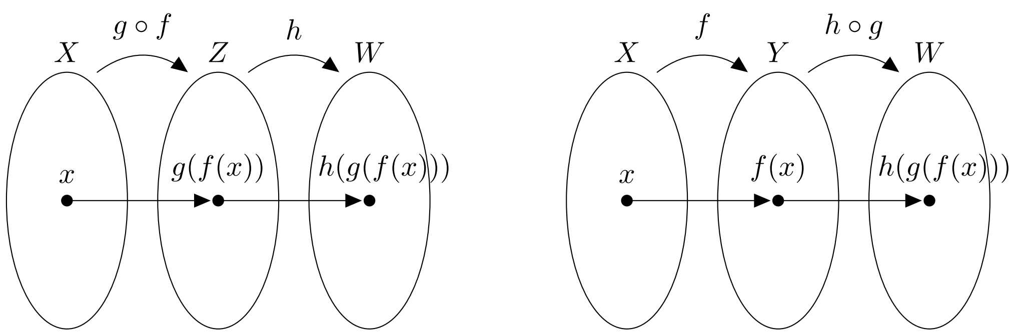
$$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x))).$$

Näiden kuvausten muodostumista on havainnollistettu alla kuvassa 5.32.

Havaitaan, että kaikilla $x \in X$ pätee

$$(h \circ (g \circ f))(x) = ((h \circ g) \circ f)(x).$$

Siis kuvaukset $h \circ (g \circ f)\colon X \to W$ ja $(h \circ g) \circ f\colon X \to W$ ovat samat eli $h \circ (g \circ f) = (h \circ g) \circ f$.




Kuva 5.32: Kuvausten yhdistäminen on liitännäinen operaatio eli $h \circ (g \circ f) = (h \circ g) \circ f$.

## 5.7 Käänteiskuvaus ja bijektio

Aloitetaan määrittelemällä identtisen kuvauksen käsite. Sitä tarvitaan myöhemmin käänteiskuvauksen määritelmässä.

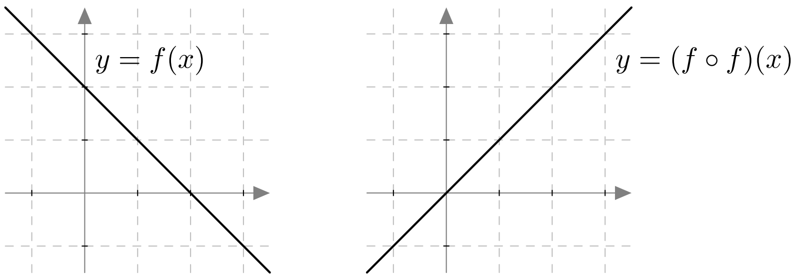
**Määritelmä 5.7.1.** Joukon $X$ *identtinen kuvaus* tarkoittaa kuvausta $\mathrm{id}_X \colon X \to X$, jolla $\mathrm{id}_X(x) = x$ kaikilla $x \in X$.

Identtinen kuvaus tarkoittaa siis kuvausta, joka ei muuta alkioita mitenkään. Joskus tällainen kuvaus syntyy kuvauksia yhdistämällä. Seuraavassa esimerkissä tarkastellaan kuvausta $f$, joka kaksi kertaa peräkkäin tehtynä ei muuta alkioita mitenkään.

**Esimerkki 5.7.2.** Tarkastellaan kuvausta $f\colon \mathbb{R} \to \mathbb{R}$, jolla $f(x) = 2 - x$ kaikilla $x \in \mathbb{R}$. Määritetään yhdistetty kuvaus $f \circ f \colon \mathbb{R} \to \mathbb{R}$. Oletetaan, että $x \in \mathbb{R}$. Tällöin

$$(f \circ f)(x) = f(f(x)) = f(2-x) = 2 - (2-x) = 2 - 2 + x = x.$$

Havaitaan, että $(f \circ f)(x) = x = \mathrm{id}_{\mathbb{R}}(x)$ kaikilla $x \in \mathbb{R}$. Yhdistetty kuvaus $f \circ f \colon \mathbb{R} \to \mathbb{R}$ on siis sama kuin joukon $\mathbb{R}$ identtinen kuvaus $\mathrm{id}_{\mathbb{R}}$ eli $f \circ f = \mathrm{id}_{\mathbb{R}}$.




Kuva 5.33: Esimerkin 5.7.2 kuvaukselle $f$ pätee $f \circ f = \mathrm{id}$.

**Määritelmä 5.7.3.** Oletetaan, että $f\colon X \to Y$ on kuvaus. Jos on olemassa sellainen kuvaus $g\colon Y \to X$, että

$$g \circ f = \mathrm{id}_X \quad \text{ja} \quad f \circ g = \mathrm{id}_Y\,,$$

niin sanotaan, että kuvaus $g$ on kuvauksen $f$ *käänteiskuvaus* ja merkitään $f^{-1} = g$.

Esimerkissä 5.7.2 näytettiin, että kuvaukselle $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = 2 - x$, pätee $f \circ f = \mathrm{id}$. Tämä tarkoittaa määritelmän 5.7.3 mukaan, että kuvaus $f$ on oma käänteiskuvauksensa eli $f^{-1} = f$.

**Esimerkki 5.7.4.** Tarkastellaan funktioita $f\colon \mathbb{R} \to \mathbb{R}$ ja $g\colon \mathbb{R} \to \mathbb{R}$, joilla $f(x) = 4 - 3x$ ja $g(x) = 4/3 - x/3$ kaikilla $x \in \mathbb{R}$. Määritetään yhdistetyt funktiot $g \circ f$ ja $f \circ g$.

Oletetaan, että $x \in \mathbb{R}$. Tällöin

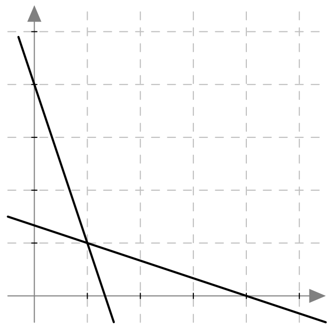
$$(g \circ f)(x) = g(f(x)) = g(4 - 3x) = \frac{4}{3} - \frac{4-3x}{3} = \frac{4}{3} - \frac{4}{3} + x = x = \mathrm{id}(x).$$

Tästä voidaan päätellä, että $g \circ f\colon \mathbb{R} \to \mathbb{R}$ ja $\mathrm{id}\colon \mathbb{R} \to \mathbb{R}$ ovat sama kuvaus eli $g \circ f = \mathrm{id}$. Lisäksi

$$(f \circ g)(x) = f(g(x)) = f\Big(\frac{4}{3} - \frac{x}{3}\Big) = 4 - 3\Big(\frac{4}{3} - \frac{x}{3}\Big) = 4 - 4 + x = x = \mathrm{id}(x).$$

Tästä voidaan päätellä, että $f \circ g\colon \mathbb{R} \to \mathbb{R}$ ja $\mathrm{id}\colon \mathbb{R} \to \mathbb{R}$ ovat sama kuvaus eli $f \circ g = \mathrm{id}$.

Havaitaan, että käänteiskuvauksen määritelmän ehdot täyttyvät: $g \circ f = \mathrm{id}$ ja $f \circ g = \mathrm{id}$ eli kumpikin yhdistetty kuvaus on identtinen kuvaus. Siis $g$ on kuvauksen $f$ käänteiskuvaus eli $g = f^{-1}$. Tilannetta on havainnollistettu kuvassa 5.34.




Kuva 5.34: Kuvaukset $f$ ja $g$ ovat toistensa käänteiskuvauksia.

---

Käänteiskuvauksen määritelmä 5.7.3 ei suoraan sulje pois mahdollisuutta, että kuvauksella olisi useampi kuin yksi käänteiskuvaus. Jos kuvauksella $f$ voisi olla useampia käänteiskuvauksia, ei merkintä $f^{-1}$ olisi mielekäs, koska ei voitaisi olla varmoja, mihin käänteiskuvaukseen se viittaa. Voidaankin osoittaa, että kuvauksella voi olla enintään yksi käänteiskuvaus. Tämä tehdään esimerkissä 5.7.6. Sitä ennen esimerkissä 5.7.5 havaitaan, että identtisen kuvauksen yhdistäminen toiseen kuvaukseen ei muuta tätä kuvausta.

**Esimerkki 5.7.5.** Olkoon $f\colon X \to Y$ kuvaus. Näytetään, että $f \circ \mathrm{id}_X = f$ ja $\mathrm{id}_Y \circ f = f$.

Oletetaan, että $x \in X$. Yhdistetyn kuvauksen määritelmän mukaan

$$(f \circ \mathrm{id}_X)(x) = f(\mathrm{id}_X(x)) = f(x).$$

Tästä nähdään, että kuvaukset $f \circ \mathrm{id}_X\colon X \to Y$ ja $f\colon X \to Y$ ovat samat eli $f \circ \mathrm{id}_X = f$. Toisaalta myös

$$(\mathrm{id}_Y \circ f)(x) = \mathrm{id}_Y(f(x)) = f(x).$$

Siis kuvaukset $\mathrm{id}_Y \circ f\colon X \to Y$ ja $f\colon X \to Y$ ovat samat eli $\mathrm{id}_Y \circ f = f$.

**Esimerkki 5.7.6.** Osoitetaan, että kuvauksella $f\colon X \to Y$ on enintään yksi käänteiskuvaus.

Tehdään vastaoletus, että kuvauksella $f$ on ainakin kaksi käänteiskuvausta. Vastaoletuksen nojalla on siis olemassa kuvaukset $g\colon Y \to X$ ja $h\colon Y \to X$, joille pätee $g \neq h$ sekä lisäksi käänteiskuvauksen määritelmän nojalla $g \circ f = \mathrm{id}_X$, $f \circ g = \mathrm{id}_Y$, $h \circ f = \mathrm{id}_X$ ja $f \circ h = \mathrm{id}_Y$. Käyttämällä näitä yhtälöitä sekä esimerkkien 5.7.5 ja 5.6.6 tuloksia saadaan

$$g = \mathrm{id}_X \circ g = (h \circ f) \circ g = h \circ (f \circ g) = h \circ \mathrm{id}_Y = h.$$

Vastaoletus johti ristiriitaan $g \neq h$ ja $g = h$. Siis alkuperäinen väite pätee eli kuvauksella $f\colon X \to Y$ on enintään yksi käänteiskuvaus.

---

Edellisen esimerkin mukaan kuvauksella on enintään yksi käänteiskuvaus. On siis mahdollista, että kuvauksella ei ole lainkaan käänteiskuvausta. Osoittautuu, että käänteiskuvaus on olemassa täsmälleen niillä kuvauksilla, jotka ovat sekä injektioita että surjektioita. Tällaisia kuvauksia sanotaan bijektioiksi, kuten alla olevasta määritelmästä käy ilmi.

**Määritelmä 5.7.7.** *Bijektio* tarkoittaa kuvausta, joka on sekä injektio että surjektio.

**Lause 5.7.8.** *Oletetaan, että $f\colon X \to Y$ on kuvaus. Kuvauksella $f$ on käänteiskuvaus, jos ja vain jos kuvaus $f$ on bijektio.*

*Todistus.* "$\Rightarrow$": Oletetaan, että on olemassa $f^{-1}\colon Y \to X$. Osoitetaan, että $f$ on bijektio.

- Osoitetaan, että $f$ on injektio. Oletetaan, että $x_1$, $x_2 \in X$. Oletetaan lisäksi, että $f(x_1) = f(x_2)$. Soveltamalla kuvausta $f^{-1}$ alkioon $f(x_1) = f(x_2) \in Y$ saadaan yhtälö

  $$f^{-1}(f(x_1)) = f^{-1}(f(x_2)).$$

  Yhdistetyn kuvauksen määritelmän mukaan tämä yhtälö voidaan kirjoittaa muodossa

  $$(f^{-1} \circ f)(x_1) = (f^{-1} \circ f)(x_2).$$

  Käänteiskuvauksen määritelmän mukaan $f^{-1} \circ f = \mathrm{id}_X$, joten saadaan yhtälö

  $$\mathrm{id}_X(x_1) = \mathrm{id}_X(x_2).$$

  Siis $x_1 = x_2$.

  Näin on osoitettu, että kaikilla $x_1$, $x_2 \in X$ oletuksesta $f(x_1) = f(x_2)$ päädytään johtopäätökseen $x_1 = x_2$. Siis $f$ on injektio.
- Osoitetaan, että $f\colon X \to Y$ on surjektio. Oletetaan, että $y \in Y$. Koska $f^{-1}$ on kuvaus $Y \to X$, niin on olemassa tasan yksi $f^{-1}(y) \in X$. Lisäksi

  $$f(f^{-1}(y)) = (f \circ f^{-1})(y) = \mathrm{id}(y) = y.$$

  Siis jokaista $y \in Y$ kohti on olemassa joukon $X$ alkio $f^{-1}(y)$, joka kuvautuu alkioksi $y$ kuvauksessa $f$. Näin $f$ on surjektio.

"$\Leftarrow$": Oletetaan, että $f\colon X \to Y$ on bijektio. Määritellään sääntö $g$ asettamalla $g(y) = x$, jos ja vain jos $y = f(x)$. Osoitetaan, että $g$ on kuvauksen $f$ käänteiskuvaus.

- Osoitetaan aluksi, että $g$ on kuvaus $Y \to X$. Oletetaan, että $y \in Y$.

  Koska $f$ on surjektio, on olemassa ainakin yksi sellainen $x \in X$, että $f(x) = y$ eli $g(y) = x$. Siis kuva-alkio $g(y)$ on olemassa ja kuuluu joukkoon $X$.

  Toisaalta koska $f$ on injektio, on olemassa vain yksi sellainen $x \in X$, että $f(x) = y$ eli $g(y) = x$. Siis kuva-alkio $g(y)$ on yksikäsitteinen.

- Osoitetaan, että kuvaus $g$ on kuvauksen $f$ käänteiskuvaus. Tarkastellaan aluksi yhdistettyä kuvausta $g \circ f\colon X \to X$. Oletetaan, että $x \in X$. Merkitään $y = f(x)$, jolloin kuvauksen $g$ määritelmän nojalla $g(y) = x$. Tämän tiedon ja yhdistetyn kuvauksen määritelmän avulla saadaan

  $$(g \circ f)(x) = g(f(x)) = g(y) = x = \mathrm{id}_X(x).$$

  Havaitaan, että kuvaukset $g \circ f\colon X \to X$ ja $\mathrm{id}_X\colon X \to X$ ovat samat eli $g \circ f = \mathrm{id}_X$.

  Tarkastellaan vielä yhdistettyä kuvausta $f \circ g\colon Y \to Y$. Oletetaan, että $y \in Y$. Merkitään $x = g(y)$, jolloin kuvauksen $g$ määritelmän nojalla $f(x) = y$. Tämän tiedon ja yhdistetyn kuvauksen määritelmän avulla saadaan

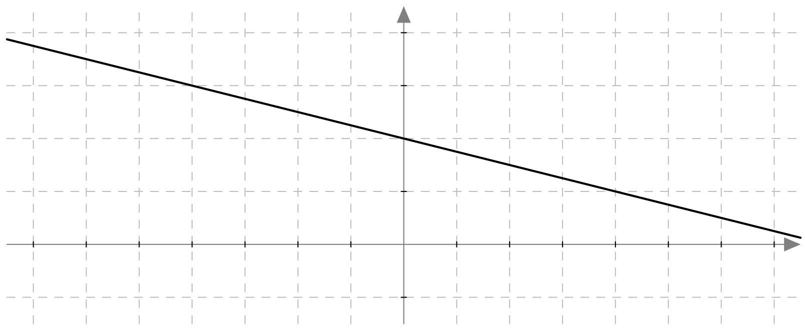
  $$(f \circ g)(y) = f(g(y)) = f(x) = y = \mathrm{id}_Y(y).$$

  Havaitaan, että kuvaukset $f \circ g\colon Y \to Y$ ja $\mathrm{id}_Y\colon Y \to Y$ ovat samat eli $f \circ g = \mathrm{id}_Y$.

  Näin on osoitettu, että $g$ on kuvauksen $f$ käänteiskuvaus eli $g = f^{-1}$.

$\square$

**Esimerkki 5.7.9.** Esimerkeissä 5.4.3 ja 5.5.3 tarkasteltu kuvaus $g\colon \mathbb{R} \to \mathbb{R}$, $g(x) = 2 - 0{,}25x$, on sekä injektio että surjektio. Kuvaus $g$ on siis bijektio, joten sillä on lauseen 5.7.8 nojalla käänteiskuvaus $g^{-1}\colon \mathbb{R} \to \mathbb{R}$.



Kuva 5.35: Funktio $x \mapsto 2 - 0{,}25x$ on bijektio.

**Esimerkki 5.7.10.** Tarkastellaan funktiota $h\colon \mathbb{R} \to \mathbb{R}$, jolla $h(x) = x^4 - x^3 - 2x^2$ kaikilla $x \in \mathbb{R}$. Osa sen kuvaajasta on piirretty kuvaan 5.36.

Havaitaan, että funktio $h$ saa saman arvon kahdessa eri kohdassa, joten se ei ole injektio. Esimerkiksi $h(-1) = 0 = h(2)$, vaikka $-1 \neq 2$. Siten funktio $h$ ei ole bijektio, minkä vuoksi sillä ei ole käänteisfunktiota.

Kuva 5.36: Funktio $x \mapsto x^4 - x^3 - 2x^2$ ei ole bijektio, joten sillä ei ole käänteisfunktiota.

**Esimerkki 5.7.11.** Tarkastellaan kuvausta $g\colon \mathbb{Z} \to \mathbb{Z}$, jolla $f(n) = 3n + 2$ kaikilla $n \in \mathbb{Z}$. Esimerkiksi laskemalla muutamia kuvauksen $g$ arvoja huomataan, että kuvaus $g$ ei vaikuta olevan surjektio. Tarkempi tarkastelu osoittaa, että esimerkiksi $g(n) \neq 3$ kaikilla kokonaisluvuilla $n$:

$$g(n) = 3 \;\Leftrightarrow\; 3n + 2 = 3 \;\Leftrightarrow\; 3n = 1 \;\Leftrightarrow\; n = \frac{1}{3}.$$

Siis $g$ ei ole surjektio, joten se ei ole bijektio. Näin ollen kuvauksella $g$ ei ole käänteiskuvausta.

**Esimerkki 5.7.12.** Tarkastellaan funktiota $f\colon \mathbb{R} \setminus \{1\} \to \mathbb{R} \setminus \{2\}$, jolla

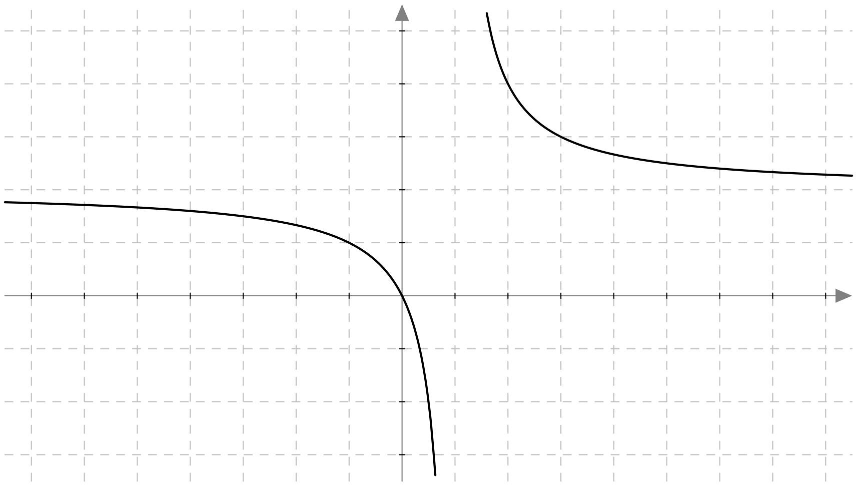
$$f(x) = \frac{2x}{x-1}$$

kaikilla $x \in \mathbb{R} \setminus \{1\}$. Osa sen kuvaajasta on piirretty kuvaan 5.37.

Tutkitaan, mikä voisi olla funktion $f$ käänteisfunktio. Oletetaan, että $y \in \mathbb{R} \setminus \{2\}$ ja tutkitaan yhtälöä $f(x) = y$:

$$\begin{aligned} f(x) = y \;\Leftrightarrow\; \frac{2x}{x-1} = y \;&\Leftrightarrow\; 2x = y(x-1) \;\wedge\; x \neq 1 \\ &\Leftrightarrow\; 2x = yx - y \;\wedge\; x \neq 1 \\ &\Leftrightarrow\; 2x - yx = -y \;\wedge\; x \neq 1 \\ &\Leftrightarrow\; (2-y)x = -y \;\wedge\; x \neq 1 \;\Leftrightarrow\; x = \frac{-y}{2-y} \;\wedge\; x \neq 1. \end{aligned}$$

Huomaa, että viimeisen ekvivalenssin kohdalla tarvitaan oletusta $y \in \mathbb{R} \setminus \{2\}$.



Kuva 5.37: Funktion $x \mapsto 2x/(x-1)$ kuvaaja.

Saadun ratkaisun perusteella funktion $f$ käänteisfunktio vaikuttaisi olevan

$$y \mapsto \frac{-y}{2-y}.$$

Näytetään vielä, että (1) tämä sääntö on todella kuvaus $\mathbb{R} \smallsetminus \{2\} \to \mathbb{R} \smallsetminus \{1\}$, ja että (2) käänteiskuvauksen määritelmän ehdot täyttyvät.

(1) Oletetaan, että $y \in \mathbb{R} \smallsetminus \{2\}$ . Tällöin osamäärä $-y/(2-y)$ on määritelty, sillä nimittäjä on nollasta poikkeva. Lisäksi osamäärä on yksikäsitteinen ja kuuluu joukkoon $\mathbb{R} \smallsetminus \{1\}$: yhtälöstä $-y/(2-y) = 1$ seuraisi $-y = 2 - y$ eli $0 = 2$, mikä on mahdotonta.

Siis voidaan määritellä kuvaus $g\colon \mathbb{R} \smallsetminus \{2\} \to \mathbb{R} \smallsetminus \{1\}$ asettamalla

$$g(x) = \frac{-x}{2-x}$$

kaikilla $x \in \mathbb{R} \smallsetminus \{2\}$.

(2) Osoitetaan, että $g$ on kuvauksen $f$ käänteiskuvaus. Oletetaan, että $x \in \mathbb{R} \smallsetminus \{2\}$. Tällöin

$$\begin{aligned}
(f \circ g)(x) &= f(g(x)) \\
&= f\left(\frac{-x}{2-x}\right) = \frac{2 \cdot \left(\frac{-x}{2-x}\right)}{\left(\frac{-x}{2-x}\right) - 1} = \frac{\frac{-2x}{2-x}}{\left(\frac{-x}{2-x}\right) - \left(\frac{2-x}{2-x}\right)} = \frac{\frac{-2x}{2-x}}{\frac{-x-(2-x)}{2-x}} \\
&= \frac{-2x}{(2-x)} \cdot \frac{(2-x)}{-x-2+x} = \frac{-2x}{-2} = x = \mathrm{id}(x).
\end{aligned}$$

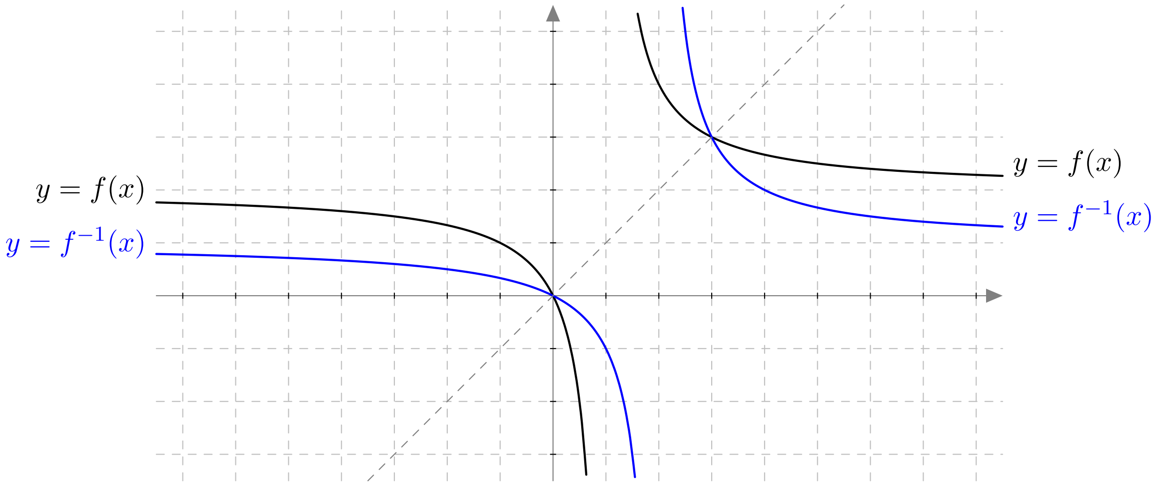
Siis kuvaukset $f \circ g$ ja $\mathrm{id}\colon \mathbb{R} \smallsetminus \{2\} \to \mathbb{R} \smallsetminus \{2\}$ ovat sama kuvaus eli $f \circ g = \mathrm{id}$.

Oletetaan vielä, että $x \in \mathbb{R} \setminus \{1\}$. Tällöin

$$
\begin{aligned}
(g \circ f)(x) &= g(f(x)) \\
&= g\left(\frac{2x}{x-1}\right) = \frac{-\left(\frac{2x}{x-1}\right)}{2-\left(\frac{2x}{x-1}\right)} = \frac{\frac{-2x}{x-1}}{\frac{2(x-1)}{(x-1)} - \left(\frac{2x}{x-1}\right)} = \frac{\frac{-2x}{x-1}}{\frac{2x-2-2x}{x-1}} \\
&= \frac{-2x}{(x-1)} \cdot \frac{(x-1)}{-2} = x = \mathrm{id}(x).
\end{aligned}
$$

Siis kuvaukset $g \circ f$ ja $\mathrm{id}\colon \mathbb{R} \setminus \{1\} \to \mathbb{R} \setminus \{1\}$ ovat sama kuvaus eli $g \circ f = \mathrm{id}$.

Näin on osoitettu, että $f \circ g = \mathrm{id}_{\mathbb{R} \setminus \{2\}}$ ja $g \circ f = \mathrm{id}_{\mathbb{R} \setminus \{1\}}$. Siis funktio $g$ on funktion $f$ käänteisfunktio eli $g = f^{-1}$. Tilannetta on havainnollistettu kuvassa 5.38.




Kuva 5.38: Funktion ja sen käänteisfunktion kuvaajat ovat symmetrisiä suoran $y = x$ suhteen.

# 6 Relaatiot

## 6.1 Relaation määritelmä

**Määritelmä 6.1.1.** Oletetaan, että $X$ ja $Y$ ovat joukkoja.

Jos $R \subset X \times Y$, sanotaan, että $R$ on *joukkojen $X$ ja $Y$ välinen relaatio.*

Jos $R \subset X \times X$, sanotaan, että $R$ on *joukon $X$ relaatio.*

Jos $(a, b) \in R$, sanotaan, että *alkio $a$ on relaatiossa $R$ alkion $b$ kanssa* ja merkitään $aRb$.

**Esimerkki 6.1.2.** Merkitään $X = \{1, 2, 3\}$ ja $Y = \{n \in \mathbb{N} \mid 1 \leq n \leq 9\}$. Tällöin esimerkiksi

$$R = \{(1, 1), (1, 2), (2, 4), (3, 6), (3, 9)\}$$

on joukkojen $X$ ja $Y$ välinen relaatio, sillä $R \subset X \times Y$. Lisäksi esimerkiksi

$$S = \{(1, 2), (2, 1), (3, 2)\}$$

on joukon $X$ relaatio, sillä $S \subset X \times X$.

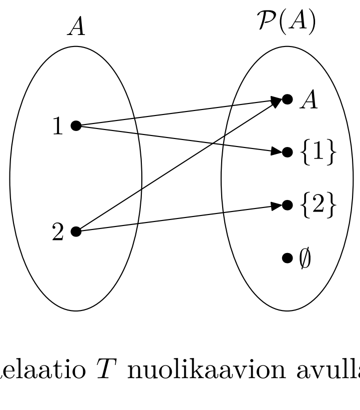
**Esimerkki 6.1.3.** Merkitään $X = \{1, 2\}$. Joukon $X$ potenssijoukko on sen kaikkien osajoukkojen muodostama joukko $\mathcal{P}(X) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$. Määritellään joukkojen $X$ ja $\mathcal{P}(X)$ välinen relaatio $T$ seuraavasti:

$$T = \{\, (a, A) \in X \times \mathcal{P}(X) \mid a \in A \,\}\,.$$

Havaitaan, että esimerkiksi $(1, \{1\}) \in T$, sillä $1 \in \{1\}$. Siis luku 1 on relaatiossa $T$ joukon $\{1\}$ kanssa. Toisaalta esimerkiksi $(2, \emptyset) \notin T$, sillä $2 \notin \emptyset$. Luku 2 ei siis ole relaatiossa joukon $\emptyset$ kanssa.

Relaatio $T$ voidaan esittää nuolikaavion avulla, kuten kuvassa 6.1, tai luettelemalla kaikki siihen kuuluvat järjestetyt parit:

$$T = \{(1, \{1\}), (1, \{1, 2\}), (2, \{2\}), (2, \{1, 2\})\}$$




Kuva 6.1: Relaatio $T$ nuolikaavion avulla esitettynä.

**Esimerkki 6.1.4.** Merkitään $X = \{1, 2, 3, 4, 5\}$. Määritellään joukon $X$ relaatio $R$ seuraavasti:

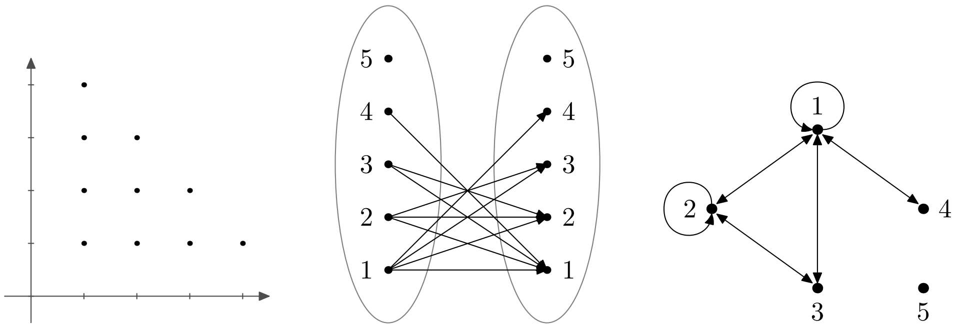
$$R = \{\, (a, b) \in X \times X \mid a + b < 6 \,\}.$$

Havaitaan, että esimerkiksi $(2, 3) \in R$, sillä $2 + 3 < 6$. Siis luku 2 on relaatiossa $R$ luvun 3 kanssa eli $2R3$. Toisaalta esimerkiksi $(5, 4) \notin R$, sillä $5 + 4 \not< 6$. Luku 5 ei siis ole relaatiossa luvun 4 kanssa.

Relaatio $R$ voidaan esittää luettelemalla kaikki siihen kuuluvat järjestetyt parit:

$$R = \{(1, 1), (1, 2), (2, 1), (1, 3), (3, 1), (1, 4), (4, 1), (2, 2), (2, 3), (3, 2)\}.$$

Sitä voidaan havainnollistaa koordinaatistossa sekä erilaisten nuolikaavioiden avulla:




Kuva 6.2: Relaatio $R$ havainnollistettuna eri tavoin.

## 6.2 Relaation refleksiivisyys, symmetrisyys ja transitiivisuus

**Määritelmä 6.2.1.** Oletetaan, että $R$ on joukon $X$ relaatio. Relaatio $R$ on

- *refleksiivinen*, jos kaikilla $x \in X$ pätee $xRx$ eli $(x, x) \in R$.
- *symmetrinen*, jos kaikilla $a$, $b \in X$ seuraava ehto toteutuu:

  jos $aRb$, niin $bRa$.
- *transitiivinen*, jos kaikilla $a$, $b$ $c \in X$ seuraava ehto toteutuu:

  jos $aRb$ ja $bRc$, niin $aRc$.

**Esimerkki 6.2.2.** Merkitään $X = \{1, 2, 3, 4, 5\}$. Tarkastellaan esimerkissä 6.1.4 määriteltyä joukon $X$ relaatiota $R$:

$$R = \{\, (a, b) \in X \times X \mid a + b < 6 \,\}.$$

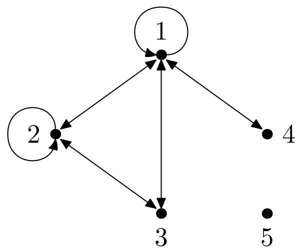
Relaation refleksiivisyyden, symmetrisyyden ja transitiivisuuden tutkimista voi helpottaa, jos relaatiota havainnollistaa nuolikaaviolla.

Kuvan 6.3 nuolikaaviosta nähdään, että esimerkiksi $(4,4) \notin R$. Relaatio $R$ ei siis ole refleksiivinen. Relaatio $R$ ei ole myöskään transitiivinen, sillä esimerkiksi $(3,1) \in R$ ja $(1,4) \in R$ mutta $(3,4) \notin R$.

Nuolikaaviossa kaikki nuolet eri pisteiden välillä kulkevat molempiin suuntiin, minkä vuoksi relaatio $R$ vaikuttaa olevan symmetrinen. Perustellaan tämä vielä tarkasti:

Oletetaan, että $a$, $b \in A$ ja $aRb$. Tällöin $a + b < 6$. Koska yhteenlaskettavien järjestyksellä ei ole väliä, myös $b + a < 6$. Tämä tarkoittaa, että $bRa$.

Siis relaatio $R$ on symmetrinen.




Kuva 6.3: Relaatio $R$ on symmetrinen, mutta ei refleksiivinen eikä transitiivinen.

**Esimerkki 6.2.3.** Merkitään $X = \{1, 2, 3\}$. Määritellään joukon $\mathcal{P}(X)$ relaatio $S$ seuraavasti:

$$S = \{(A, B) \in \mathcal{P}(X) \times \mathcal{P}(X) \mid A \subset B\}.$$

Huomataan, että relaatio $S$ on refleksiivinen, sillä kaikilla $A \in \mathcal{P}(X)$ pätee $A \subset A$.

Relaatio $S$ ei ole symmetrinen, sillä esimerkiksi $\{2\} \subset \{2, 3\}$ mutta $\{2, 3\} \not\subset \{2\}$. Tämä tarkoittaa, että $(\{2\}, \{2, 3\}) \in S$ mutta $(\{2, 3\}, \{2\}) \notin S$.

Näytetään, että relaatio $S$ on transitiivinen:

Oletetaan, että $A$, $B$, $C \in \mathcal{P}(X)$ ja $(A, B) \in S$ ja $(B, C) \in S$. Tämä tarkoittaa, että $A \subset B$ ja $B \subset C$. Voidaan päätellä, että $A \subset C$. Siis myös $(A, C) \in S$.

## 6.3 Ekvivalenssirelaatio ja ekvivalenssiluokat

**Määritelmä 6.3.1.** Oletetaan, että $R$ on joukon $X$ relaatio. Jos $R$ on refleksiivinen, symmetrinen ja transitiivinen, niin sanotaan, että $R$ on *ekvivalenssirelaatio*.

**Esimerkki 6.3.2.** Määritellään joukon $\mathbb{Z}$ relaatio $\sim$ ehdolla

$$a \sim b, \quad \text{jos erotus } \; a - b \; \text{ on jaollinen luvulla 5.}$$

Osoitetaan, että $\sim$ on ekvivalenssirelaatio.

– Osoitetaan, että relaatio $\sim$ on refleksiivinen.

  Oletetaan, että $a \in \mathbb{Z}$. Tällöin $a - a = 0 = 5 \cdot 0$, joten $5 \mid (a - a)$. Siis $a \sim a$. Tämä päättely pätee millä tahansa kokonaisluvulla, joten jokainen kokonaisluku on relaatiossa $\sim$ itsensä kanssa.

– Osoitetaan, että relaatio $\sim$ on symmetrinen.

  Oletetaan, että $a, b \in \mathbb{Z}$ ja $a \sim b$. Tällöin $a - b = 5k$ jollakin $k \in \mathbb{Z}$. Kertomalla tätä yhtälöä molemmin puolin luvulla $-1$ saadaan yhtälö $b - a = 5 \cdot (-k)$, missä $-k \in \mathbb{Z}$. Näin ollen $5 \mid (b - a)$. Siis $b \sim a$.

– Osoitetaan, että relaatio $\sim$ on transitiivinen.

  Oletetaan, että $a, b, c \in \mathbb{Z}$ ja lisäksi $a \sim b$ ja $b \sim c$. Tällöin $a - b = 5k$ jollakin $k \in \mathbb{Z}$ ja $b - c = 5m$ jollakin $m \in \mathbb{Z}$. Siten

  $$a - c = a - b + b - c = 5k + 5m = 5(k + m),$$

  missä $k + m \in \mathbb{Z}$. Näin $5 \mid (a - c)$. Siis $a \sim c$.

Relaatio $\sim$ on siis refleksiivinen, symmetrinen ja transitiivinen, joten se on ekvivalenssirelaatio.

**Määritelmä 6.3.3.** Oletetaan, että $R$ on joukon $X$ ekvivalenssirelaatio. Alkion $a \in X$ *ekvivalenssiluokka* on

$$[a]_R = \{\, x \in X \mid (x, a) \in R \,\} = \{\, x \in X \mid xRa \,\}.$$

Alkiota $a$ sanotaan ekvivalenssiluokan $[a]_R$ *edustajaksi.*

Kaikkien ekvivalenssiluokkien muodostamaa joukkoa merkitään $X/R$. Siis

$$X/R = \{\, [a]_R \mid a \in X \,\}.$$

Alkion $a \in X$ ekvivalenssiluokan muodostavat siis ne joukon $X$ alkiot, jotka ovat relaatiossa alkion $a$ kanssa. Ekvivalenssiluokan käsitettä havainnollistetaan seuraavassa esimerkissä.

**Esimerkki 6.3.4.** Olkoon $S$ kaikkien suomen kielen sanojen muodostama joukko. Määritellään joukon $S$ relaatio $\sim$ ehdolla

$$a \sim b, \quad \text{jos sana } a \text{ alkaa samalla kirjaimella kuin sana } b.$$

Varmistetaan aluksi, että $\sim$ on ekvivalenssirelaatio.

– Relaatio $\sim$ on refleksiivinen, sillä jokainen sana on itsensä kanssa relaatiossa $\sim$. Nimittäin jokaisella sanalla on sama alkukirjain kuin sillä itsellään.

– Relaatio $\sim$ on symmetrinen: jos sana $a$ alkaa samalla kirjaimella kuin sana $b$, niin sana $b$ alkaa samalla kirjaimella kuin sana $a$.

- Relaatio $\sim$ on transitiivinen: Jos sana $a$ alkaa samalla kirjaimella kuin sana $b$ ja sana $b$ alkaa samalla kirjaimella kuin sana $c$, niin kaikilla kolmella sanalla on sama alkukirjain. Erityisesti sana $a$ alkaa samalla kirjaimella kuin sana $c$.

Relaatio $\sim$ on siis refleksiivinen, symmetrinen ja transitiivinen, joten se on ekvivalenssirelaatio.

Määritetään seuraavaksi sanan AAMU ekvivalenssiluokka. Määritelmän mukaan

$$[\text{AAMU}]_\sim = \{\, s \in S \mid s \sim \text{AAMU} \,\} = \{\, s \in S \mid \text{ sana } s \text{ alkaa kirjaimella a} \,\}$$

Havaitaan, että sanan AAMU ekvivalenssiluokan muodostavat kaikki a-kirjaimella alkavat sanat. Vastaavalla tavalla päättelemällä huomataan, että relaation $\sim$ ekvivalenssiluokat ovat

$$[\text{AAMU}],\ [\text{BANAANI}],\ [\text{CELCIUS}],\ [\text{DEMOKRATIA}],\ \ldots,\ [\text{ÖLJY}].$$

Jokaisen ekvivalenssiluokan muodostavat siis kaikki tietyllä kirjaimella alkavat sanat. Tässä esimerkiksi sana DEMOKRATIA on valittu kaikkien d-kirjaimella alkavien sanojen edustajaksi.

Kaikkien ekvivalenssiluokkien joukko on

$$S/\sim\ = \big\{[\text{AAMU}],\ [\text{BANAANI}],\ [\text{CELCIUS}],\ [\text{DEMOKRATIA}],\ \ldots,\ [\text{ÖLJY}]\big\}$$

**Esimerkki 6.3.5.** Esimerkissä 6.3.2 määriteltiin joukon $\mathbb{Z}$ relaatio $\sim$ ehdolla

$$a \sim b, \quad \text{jos erotus} \quad a - b \quad \text{on jaollinen luvulla 5},$$

ja osoitettiin, että $\sim$ on ekvivalenssirelaatio. Määritetään sen ekvivalenssiluokat.

Tarkastellaan aluksi vaikkapa lukua 0. Ekvivalenssiluokan määritelmän mukaan

$$\begin{aligned}
[0]_\sim &= \{\, z \in \mathbb{Z} \mid z \sim 0 \,\} \\
&= \{\, z \in \mathbb{Z} \mid z - 0 = 5k \text{ jollakin } k \in \mathbb{Z} \,\} \\
&= \{\, z \in \mathbb{Z} \mid z = 5k \text{ jollakin } k \in \mathbb{Z} \,\} \\
&= \{\, 5k \mid k \in \mathbb{Z}\}.
\end{aligned}$$

Luvun 0 ekvivalenssiluokan muodostavat siis kaikki viidellä jaolliset luvut: $0$, $\pm 5$, $\pm 10$, $\pm 15$, $\pm 20$, $\pm 25$, $\pm 30, \ldots$

Luvun 1 ekvivalenssiluokaksi saadaan vastaavalla tavalla

$$\begin{aligned}
[1]_\sim &= \{\, z \in \mathbb{Z} \mid z \sim 1 \,\} \\
&= \{\, z \in \mathbb{Z} \mid z - 1 = 5k \text{ jollakin } k \in \mathbb{Z} \,\} \\
&= \{\, z \in \mathbb{Z} \mid z = 5k + 1 \text{ jollakin } k \in \mathbb{Z} \,\} \\
&= \{\, 5k + 1 \mid k \in \mathbb{Z}\}.
\end{aligned}$$

Havaitaan, että luvun 1 ekvivalenssiluokan muodostavat ne luvut, joiden jakojäännös viidellä jaettaessa on yksi. Siis luvut $1$, $6$, $11$, $16, \ldots$ ja luvut $-4$, $-9$, $-14$, $-19, \ldots$

Samaan tapaan havaitaan, että

$$\begin{aligned}[2]_\sim &= \{\, 5k+2 \mid k \in \mathbb{Z}\} \\ [3]_\sim &= \{\, 5k+3 \mid k \in \mathbb{Z}\} \\ [4]_\sim &= \{\, 5k+4 \mid k \in \mathbb{Z}\}.\end{aligned}$$

Voidaan osoittaa, että tässä ovat kaikki relaation $\sim$ ekvivalenssiluokat. Tämä liittyy siiden, että viidellä jaettaessa mahdolliset jakojäännökset ovat 0, 1, 2, 3 ja 4. Asiaa on havainnollistettu tarkemmin seuraavassa esimerkissä.

Kaikkien ekvivalenssiluokkien joukko on siis

$$\mathbb{Z}/\sim\, = \{[0]_\sim,\ [1]_\sim,\ [2]_\sim,\ [3]_\sim,\ [4]_\sim\}.$$

Jokaisen ekvivalenssiluokan muodostavat kaikki ne kokonaisluvut, joilla on sama jakojäännös luvulla 5 jaettaessa.

**Esimerkki 6.3.6.** Jatketaan esimerkin 6.3.5 ekvivalenssirelaation $\sim$ tarkastelua. Esimerkissä 6.3.5 nähtiin, että alkion 3 ekvivalenssiluokka on

$$[3]_\sim = \{\, 5k+3 \mid k \in \mathbb{Z}\} = \{\dots, -17, -12, -7, -2, 3, 8, 13, 18, 23, \dots\}.$$

Ekvivalenssiluokan $[3]_\sim$ muodostavat siis ne luvut, joiden jakojäännös viidellä jaettaessa on 3. Osoitetaan, että luvun 8 ekvivalenssiluokka on sama kuin luvun 3 ekvivalenssiluokka, eli että $[8]_\sim = [3]_\sim$. Koska ekvivalenssiluokat ovat joukkoja, näytetään sisältyminen molempiin suuntiin.

”$\subset$”: Oletetaan, että $x \in [8]_\sim$. Tällöin ekvivalenssiluokan määritelmän mukaan $x \sim 8$. Toisaalta $8 \sim 3$, sillä erotus $8 - 3 = 5$ on jaollinen luvulla 5. Koska $\sim$ on ekvivalenssirelaatio, se on transitiivinen. Transitiivisuuden nojalla voidaan päätellä, että myös $x \sim 3$. Tämä tarkoittaa, että $x \in [3]_\sim$.

”$\supset$”: Oletetaan, että $x \in [3]_\sim$. Tällöin $x \sim 3$. Lisäksi $3 \sim 8$, sillä erotus $3 - 8 = -5$ on jaollinen luvulla 5. Ekvivalenssirelaation $\sim$ transitiivisuuden nojalla tällöin myös $x \sim 8$. Siis $x \in [8]_\sim$.

# 7 Kompleksiluvut

Tämän luvun tarkoituksena on antaa perustaidot kompleksiluvuilla laskemiseen sekä niiden geometriseen tulkintaan.

## 7.1 Kompleksilukujen määritelmä

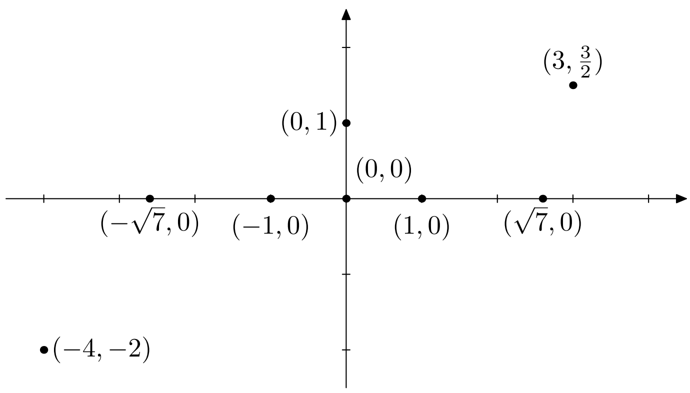
**Määritelmä 7.1.1.** *Kompleksilukujen joukko* $\mathbb{C}$ on joukko

$$\{\, (a,b) \mid a,b \in \mathbb{R} \,\}$$

varustettuna yhteenlaskulla ja kertolaskulla, jotka määritellään seuraavasti:

$$(a,b) + (c,d) = (a+c, b+d) \quad \text{ja} \quad (a,b) \cdot (c,d) = (ac - bd, ad + bc).$$

Kompleksiluvut ovat siis määritelmän mukaan reaalilukupareja. Ne vastaavat niin sanotun kompleksitason pisteitä, eli niitä voidaan havainnollistaa koordinaatistossa:




Kuva 7.1: Kompleksilukuja kompleksitasossa.

Kompleksilukujen yhteenlasku on määritelmän mukaan sama kuin lineaarialgebran kurssilla käsiteltävän avaruuden $\mathbb{R}^2$ vektoreiden yhteenlasku. Kompleksiluvut eroavat avaruuden $\mathbb{R}^2$ vektoreista siinä, että kompleksiluvuille on määritelty kertolasku: on mahdollista laskea kahden kompleksiluvun tulo, joka on edelleen kompleksiluku. Kompleksilukujen tulon laskeminen suoraan määritelmän mukaan on hiukan vaivalloista. Myöhemmin kappaleessa 7.2 esiteltävien merkintöjen avulla tulon laskeminen käy helpommin.

Reaaliluvut ajatellaan kompeksilukujen osajoukoksi samastamalla reaaliluku $a$ ja kompleksiluku $(a,0)$ eli tulkitsemalla kompleksitason vaaka-akseli lukusuorana. Voidaan osoittaa, että tällöin reaaliluvuilla saadaan samat tulokset riippumatta siitä, käytetäänkö niille kompleksilukujen yhteen- ja kertolaskua vai reaalilukujen yhteen- ja kertolaskua. Tätä havainnollistetaan seuraavassa esimerkissä.

**Esimerkki 7.1.2.** Oletetaan, että $a$, $b \in \mathbb{R}$. Tulkitaan reaaliluvut $a$ ja $b$ kompleksilukuina ja lasketaan niiden tulo:

$$(a, 0) \cdot (b, 0) = (ab - 0 \cdot 0, a \cdot 0 + 0 \cdot b) = (ab - 0, 0 + 0) = (ab, 0).$$

Huomataan, että tulos $(ab, 0)$ vastaa reaalilukua $ab$. Päädytään siis samaan tulokseen riippumatta siitä, käytetäänkö reaalilukujen vai kompleksilukujen kertolaskua.

---

Lisäksi voidaan osoittaa, että kompleksilukujen yhteen- ja kertolasku noudattavat samoja tuttuja laskusääntöjä kuin reaalilukujen yhteen- ja kertolasku. Tätä havainnollistetaan seuraavassa esimerkissä.

**Esimerkki 7.1.3.** Osoitetaan, että kompleksilukujen yhteenlasku on vaihdannainen eli yhteenlaskettavien järjestyksellä ei ole väliä.

Oletetaan, että $z$, $w \in \mathbb{C}$. Tällöin $z = (z_1, z_2)$ ja $w = (w_1, w_2)$, missä $z_1$, $z_2$, $w_1$, $w_2 \in \mathbb{R}$. Lähdetään muokkaamaan summaa $z + w$:

$$\begin{aligned} z + w = (z_1, z_2) + (w_1, w_2) &= (z_1 + w_1, z_2 + w_2) \\ &= (w_1 + z_1, w_2 + z_2) = (w_1, w_2) + (z_1, z_2) = w + z \end{aligned}$$

Saatiin yhtälöketju, jonka nojalla $z+w = w+z$. Perustelussa hyödynnettiin tietoa reaalilukujen yhteenlaskun vaihdannaisuudesta: koska $z_1$, $z_2$, $w_1$, $w_2 \in \mathbb{R}$, niin $z_1 + w_1 = w_1 + z_1$ ja $z_2 + w_2 = w_2 + z_2$.

---

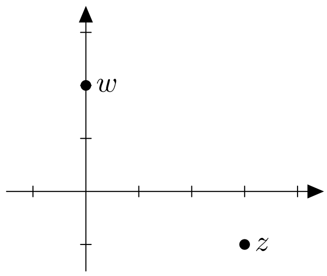
Kompleksiluvut ovat määritelmän mukaan reaalilukupareja. Niiden komponenteille käytetään nimityksiä reaaliosa ja imaginaariosa, jotka määritellään alla.

**Määritelmä 7.1.4.** Oletetaan, että $a$, $b \in \mathbb{R}$. Kompleksiluvun $z = (a, b)$ *reaaliosa* on $\operatorname{Re} z = a$ ja *imaginaariosa* on $\operatorname{Im} z = b$.

Kuten jo aiemmin todettiin, reaalilukujen joukko voidaan tulkita kompleksilukujen osajoukoksi ajattelemalla lukusuoraa kompleksitason vaaka-akselina. Kompleksitason pystyakselilla olevia lukuja (nollaa eli origoa lukuunottamatta) sanotaan puolestaan puhtaasti imaginaarisiksi luvuiksi:

**Määritelmä 7.1.5.** Oletetaan, että $z \in \mathbb{C}$ ja $z \neq 0$. Jos $\operatorname{Re} z = 0$, sanotaan kompleksiluvun $z$ olevan *puhtaasti imaginaarinen.*

**Esimerkki 7.1.6.** Kompleksiluvun $z = (3, -1)$ reaaliosa on $\operatorname{Re} z = 3$ ja imaginaariosa on $\operatorname{Im} z = -1$. Kompleksiluvun $w = (0, 2)$ reaaliosa on $\operatorname{Re} w = 0$ ja imaginaariosa on $\operatorname{Im} w = 2$. Se on puhtaasti imaginaarinen.




Kuva 7.2: Kompleksiluku $w$ on puhtaasti imaginaarinen, kompleksiluku $z$ puolestaan ei ole.

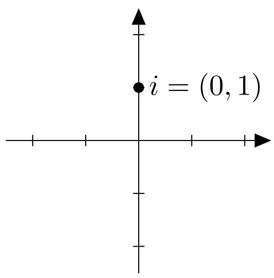
---

Kompleksilukujen avulla saadaan ratkaisuja sellaisillekin polynomiyhtälöille, joille ei reaalilukujen joukossa ole ratkaisua. Esimerkiksi yhtälöllä $x^2 = -1$ ei ole ratkaisua reaalilukujen joukossa, sillä reaalilukujen toiset potenssit ovat epänegatiivisia: $a^2 \geq 0$ kaikilla $a \in \mathbb{R}$. Osoittautuu kuitenkin, että tälle yhtälölle löytyy ratkaisu kompleksilukujen joukosta. Kertomalla lukua $(0, 1)$ itsellään saadaan

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

Saatu tulos vastaa reaalilukua $-1$, joten kysymyksessä on yhtälön $x^2 = -1$ yksi ratkaisu. Kompleksiluvulle $(0, 1)$ on annettu oma nimi, kuten seuraavasta määritelmästä käy ilmi.

**Määritelmä 7.1.7.** Kompleksilukua $(0, 1)$ kutsutaan *imaginaariyksiköksi* ja merkitään symbolilla $i$.




Kuva 7.3: Imaginaariyksikkö $i = (0, 1)$.

**Lause 7.1.8.** *Imaginaariyksikölle $i$ pätee $i^2 = -1$.*

*Todistus.* Imaginaariyksikön määritelmän mukaan $i = (0, 1)$. Soveltamalla kompleksilukujen kertolaskua saadaan

$$i^2 = (0, 1) \cdot (0, 1) = (0 - 1, 0 + 0) = (-1, 0) = -1. \qquad \square$$

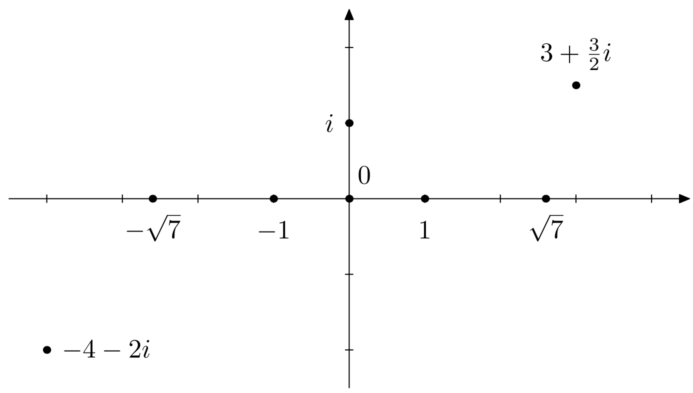
## 7.2 Kompleksilukujen esitys imaginaariyksikön avulla

Kompleksiluku $(a, b)$ voidaan imaginaariyksikön avulla kirjoittaa muodossa $a + bi$, mikä nähdään alla olevasta yhtälöketjusta:

$$(a, b) \overset{(1)}{=} (a, 0) + (0, b) \overset{(2)}{=} (a, 0) + (b, 0) \cdot (0, 1) \overset{(3)}{=} (a, 0) + (b, 0) \cdot i \overset{(4)}{=} a + bi\,.$$

Kohdassa (1) käytetään kompleksilukujen yhteenlaskun määritelmää. Kohdassa (2) käytetään kompleksilukujen kertolaskun määritelmää, jonka mukaan $(b, 0) \cdot (0, 1) = (0, b)$. Kohdassa (3) käytetään imaginaariyksikön määritelmää $i = (0, 1)$. Kohdassa (4) samastetaan kompleksiluvut $(a, 0)$ ja $(b, 0)$ reaalilukuihin $a$ ja $b$.

Kompleksilukujen joukko voidaan siis kirjoittaa muodossa $\mathbb{C} = \{\, a + bi \mid a, b \in \mathbb{R} \,\}$.




Kuva 7.4: Kompleksilukuja kompleksitasossa.

**Esimerkki 7.2.1.** Kompleksiluku $z = 6 - 9i$ voidaan kirjoittaa myös muodossa $z = (6, -9)$. Sen reaaliosa on $\operatorname{Re} z = 6$ ja imaginaariosa on $\operatorname{Im} z = -9$. Huomaa, että imaginaariyksikkö ei ole mukana imaginaariosassa.

## 7.3 Kompleksiluvuilla laskeminen

Jos kompleksiluvut kirjoitetaan imaginaariyksikön avulla summamuodossa, voidaan niiden summa ja tulo voidaan laskea kuten koulussa on opittu sieventämään reaalilukulausekkeita. Lisäksi pitää vain huomioida, että $i^2 = -1$ (lause 7.1.8).

**Esimerkki 7.3.1.** Merkitään $z = -4 - 2i$ ja $w = 3 + 5i$. Lasketaan lukujen $z$ ja $w$ summa yhdistämällä samanmuotoiset termit:

$$z + w = (-4 - 2i) + (3 + 5i) = -4 + 3 - 2i + 5i = -1 + 3i.$$

Lasketaan lukujen $z$ ja $w$ tulo kertomalla sulut auki:

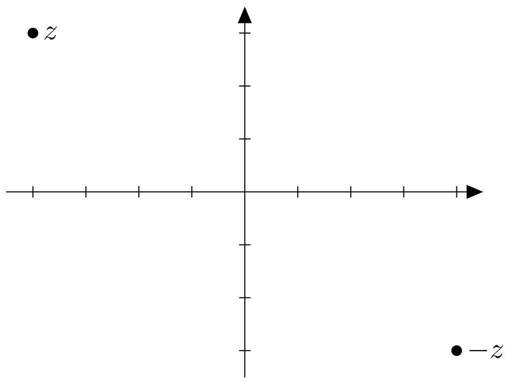
$$\begin{aligned} zw &= (-4 - 2i)(3 + 5i) = -4 \cdot 3 - 4 \cdot 5i - 2i \cdot 3 - 2i \cdot 5i = -12 - 20i - 6i - 10i^2 \\ &= -12 - 26i - 10 \cdot (-1) = -12 - 26i + 10 = -2 - 26i. \end{aligned}$$

Kuten reaaliluvuilla, myös jokaisella kompleksiluvulla on vastaluku. Kompleksilukujen erotus voidaan määritellä yhteenlaskun ja vastaluvun avulla:

**Määritelmä 7.3.2.** Oletetaan, että $a$, $b \in \mathbb{R}$. Kompleksiluvun $z = (a, b)$ *vastaluku* on $-z = (-a, -b)$. Kompleksilukujen $z$ ja $w$ *erotus* tarkoittaa summaa $z + (-w)$. Sitä merkitään $z - w$.

**Esimerkki 7.3.3.** Merkitään $z = -4 + 3i$ ja $w = -2 - i$. Määritetään luvun $z$ vastaluku vaihtamalla sekä reaaliosan että imaginaariosan merkki: $-z = -(-4 + 3i) = 4 - 3i$.

Lukujen $z$ ja $w$ erotusta laskiessa pitää huomata, että miinusmerkki vaikuttaa kaikkiin etumerkkeihin sulkujen sisällä: $z - w = (-4 + 3i) - (-2 - i) = -4 + 3i + 2 + i = -2 + 4i$.




Kuva 7.5: Kompleksiluku $z$ ja sen vastaluku $-z$.

## 7.4 Kompleksiluvun liittoluku ja itseisarvo

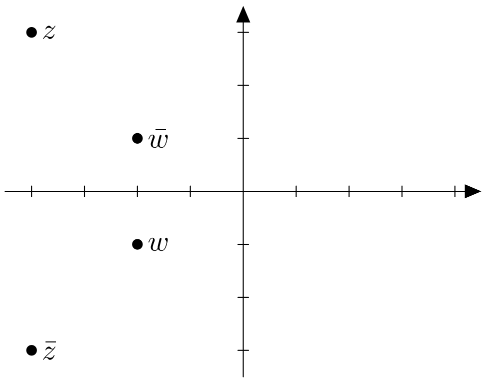
Jokaiselle kompleksiluvulle voidaan määritellä niin sanottu liittoluku, joka saadaan vaihtamalla alkuperäisen luvun imaginaariosan merkki:

**Määritelmä 7.4.1.** Oletetaan, että $a$, $b \in \mathbb{R}$. Kompleksiluvun $z = a + bi$ *liittoluku* eli *kompleksikonjugaatti* on

$$\bar{z} = a - bi.$$

Liittoluvun ottaminen vastaa siis kompleksitason pisteen peilaamista vaaka-akselin suhteen. Luvun $z$ liittoluvulle käytetään joissakin kirjoissa merkintää $z^*$.

**Esimerkki 7.4.2.** Kompleksilukujen $z = -4 + 3i$ liittoluku on $\bar{z} = -4 - 3i$. Kompleksiluvun $w = -2 - i$ liittoluku on $\bar{w} = -2 + i$. Näitä on havainnollistettu kuvassa 7.6.




Kuva 7.6: Kompleksiluvut $z$ ja $w$ sekä niiden liittoluvut $\bar{z}$ ja $\bar{w}$.

**Lause 7.4.3.** *Oletetaan, että* $z, w \in C$. *Tällöin*

(a) $\overline{z+w} = \bar{z} + \bar{w}$

(b) $\overline{zw} = \bar{z}\bar{w}$

(c) $\bar{\bar{z}} = z$

(d) *jos* $Im\, z = 0$, *niin* $\bar{z} = z$.

*Todistus.* Todistetaan malliksi a-kohta ja jätetään loput harjoitustehtäviksi.

Oletetaan, että $z, w \in C$. Tällöin $z = a + bi$ ja $w = c + di$, missä $a, b, c, d \in \mathbb{R}$. Summan $z + w$ liittoluvuksi saadaan

$$\overline{z+w} = \overline{(a+bi)+(c+di)} = \overline{a+c+(b+d)i} = a+c-(b+d)i.$$

Liittolukujen summaksi saadaan puolestaan

$$\bar{z} + \bar{w} = (a-bi)+(c-di) = a+c-bi-di = a+c-(b+d)i.$$

Tulokset ovat samat, joten $\overline{z+w} = \bar{z} + \bar{w}$. $\square$

---

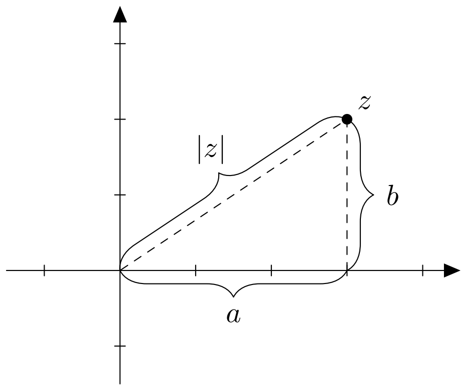
Reaaliluvun $a$ itseisarvo $|a|$ kertoo luvun $a$ etäisyyden nollasta. Esimerkiksi luvun $-4$ itseisarvo on $|-4| = 4$. Vastaava itseisarvon käsite voidaan määritellä myös kompleksiluvuille:

**Määritelmä 7.4.4.** Oletetaan, että $a, b \in \mathbb{R}$. Kompleksiluvun $z = a + bi$ *itseisarvo* on

$$|z| = \sqrt{a^2 + b^2}.$$

Itseisarvon toinen nimitys on *moduli*.

Huomaa, että määritelmässä neliöjuuren alla esiintyvä lauseke $a^2 + b^2$ on epänegatiivinen reaaliluku, minkä vuoksi siitä voidaan ottaa neliöjuuri.




Kuva 7.7: Kompleksiluvun itseisarvo kertoo luvun etäisyyden origosta.

Pythagoraan lauseen mukaan kuvassa 7.7 näkyvässä suorakulmaisessa kolmiossa kateettien neliöiden summa $a^2 + b^2$ on sama kuin hypotenuusan eli pisimmän sivun pituuden neliö. Hypotenuusan pituudeksi saadaan siten $\sqrt{a^2+b^2} = |z|$. Kompleksiluvun itseisarvo kertoo siis luvun etäisyyden kompleksitason origosta.

**Lause 7.4.5.** *Kompleksiluvun $z$ itseisarvolle pätee $|z| = \sqrt{z\bar{z}}$.*

*Todistus.* Oletetaan, että $z \in \mathbb{C}$. Tällöin $z = a + bi$ joillakin $a, b \in \mathbb{R}$. Lasketaan tulo $z\bar{z}$:

$$z\bar{z} = (a+bi)(a-bi) = a^2 - abi + abi - (bi)^2 = a^2 - b^2i^2 = a^2 - b^2 \cdot (-1) = a^2 + b^2.$$

Havaitaan, että $z\bar{z} = a^2 + b^2$, joten sen neliöjuuri on $\sqrt{z\bar{z}} = \sqrt{a^2+b^2} = |z|$. □

---

Voidaan osoittaa, että kompleksilukujen itseisarvolle pätevät reaalilukujen itseisarvon tutut ominaisuudet. Seuraavassa lauseessa todistetaan näistä ominaisuuksista yksi.

**Lause 7.4.6.** *Olkoot $z, w \in \mathbb{C}$. Tulon $zw$ itseisarvo on lukujen $z$ ja $w$ itseisarvojen tulo eli*

$$|zw| = |z| \cdot |w| .$$

*Todistus.* Todistus voidaan rakentaa yhtälöketjuna:

$$|zw| \overset{(1)}{=} \sqrt{(zw)(\overline{zw})} \overset{(2)}{=} \sqrt{(zw)(\bar{z}\bar{w})} \overset{(3)}{=} \sqrt{(z\bar{z})(w\bar{w})} \overset{(4)}{=} \sqrt{z\bar{z}}\sqrt{w\bar{w}} \overset{(5)}{=} |z| \cdot |w| .$$

Kohdassa (1) sovelletaan lausetta 7.4.5, jonka mukaan kompleksiluvun $zw$ itseisarvolle pätee

$$|zw| = \sqrt{(zw)(\overline{zw})}.$$

Kohdassa (2) käytetään lausetta 7.4.3, jonka mukaan $\overline{zw} = \bar{z}\bar{w}$.

Kohdassa (3) käytetään kompleksilukujen tulon liitännäisyyttä, jonka nojalla sulkujen paikkaa saa vaihtaa, ja kompleksilukujen tulon vaihdannaisuutta, jonka nojalla tulon tekijöiden järjestystä saa vaihtaa: $(zw)(\bar{z}\bar{w}) = z(w\bar{z})\bar{w} = z(\bar{z}w)\bar{w} = (z\bar{z})(w\bar{w})$.

Kohdassa (4) käytetään tietoa, että kompleksiluvun ja sen liittoluvun tulo on epänegatiivinen reaaliluku. Nimittäin lauseesta 7.4.5 seuraa, että $z\bar{z} = |z|^2 \geq 0$. Näin voidaan käyttää reaalilukujen neliöjuuren ominaisuutta $\sqrt{ac} = \sqrt{a}\sqrt{c}$ eli tulon neliöjuuri on sama kuin neliöjuurten tulo.

Kohdassa (5) sovelletaan uudelleen lausetta 7.4.5, jonka mukaan $\sqrt{z\bar{z}} = |z|$ ja $\sqrt{w\bar{w}} = |w|$. □

---

Reaaliluvuille pätee niin sanottu tulon nollasääntö: jos $a$, $b \in \mathbb{R}$ ja $ab = 0$, niin $a = 0$ tai $b = 0$. Itseisarvon ominaisuuksien avulla saadaan tulon nollasääntö todistettua myös kompleksiluvuille:

**Lause 7.4.7.** *Oletetaan, että $z$, $w \in \mathbb{C}$. Jos $zw = 0$, niin $z = 0$ tai $w = 0$.*

*Todistus.* Oletetaan, että $zw = 0$. Tällöin $|zw| = |0| = 0$. Toisaalta lauseen 7.4.5 nojalla $|zw| = |z||w|$. Yhdistämällä nämä tiedot voidaan päätellä, että $|z||w| = 0$. Reaalilukujen tulon nollasäännön mukaan tästä yhtälöstä seuraa, että $|z| = 0$ tai $|w| = 0$. Koska kompleksiluvun itseisarvo kertoo kyseisen luvun etäisyyden kompleksitason origosta, voidaan tästä päätellä, että $z = 0$ tai $w = 0$. □

## 7.5 Kompleksiluvun käänteisluku ja kompleksilukujen osamäärä

Kompleksiluvun itseisarvo kertoo kyseisen luvun etäisyyden kompleksitason origosta, joten voidaan päätellä, että kompleksiluvulle $z$ pätee $|z| = 0$, jos ja vain jos $z = 0$. Tästä seuraa, että osamäärä $1/|z|^2$ on määritelty kaikille nollasta poikkeaville kompleksiluvuille. Kyseisen osamäärän ja liittoluvun avulla saadaan määriteltyä kaikille nollasta poikkeaville kompleksiluvuille käänteisluku.

**Määritelmä 7.5.1.** Kompleksiluvun $z \neq 0$ *käänteisluku* on

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

Kompleksiluvun $z$ käänteislukua voidaan merkitä myös $1/z$ tai $\dfrac{1}{z}$.

Reaaliluvun ja sen käänteisluvun tulo on aina yksi. Esimerkiksi $3 \cdot (1/3) = 1$ ja $5 \cdot (1/5) = 1$. Sama pätee kompleksilukujen tapauksessa:

**Lause 7.5.2.** *Kompleksiluvun ja sen käänteisluvun tulo on yksi.*

*Todistus.* Käänteisluku on määritelty vain nollasta poikkeaville kompleksiluvuille, joten oletetaan, että $z \in \mathbb{C}$ ja $z \neq 0$. Kompleksiluvun $z$ ja sen käänteisluvun tulo on

$$z \cdot z^{-1} \overset{(1)}{=} z \cdot \Big(\frac{1}{|z|^2}\,\bar{z}\Big) = \frac{z\bar{z}}{|z|^2} \overset{(2)}{=} \frac{z\bar{z}}{z\bar{z}} = 1.$$

Kohdassa (1) käytetään käänteisluvun määritelmää. Kohdassa (2) sovelletaan lausetta 7.4.5, jonka mukaan $|z| = \sqrt{z\bar{z}}$. Siitä voidaan päätellä, että $|z|^2 = z\bar{z}$. □

---

Käänteisluvun ja kertolaskun avulla saadaan määriteltyä kompleksilukujen osamäärä:

**Määritelmä 7.5.3.** Oletetaan, että $z$, $w \in \mathbb{C}$ ja $w \neq 0$. Kompleksilukujen $z$ ja $w$ *osamäärä* on

$$\frac{z}{w} = z \cdot w^{-1}\,.$$

Käytännössä osamäärä on mukava sieventää laventamalla nimittäjän liittoluvulla. Laventaminen tarkoittaa, että sekä osoittaja että nimittäjä kerrotaan samalla luvulla (tässä tapauksessa nimittäjän liittoluvulla). Tätä havainnollistetaan seuraavissa esimerkeissä.

**Esimerkki 7.5.4.** Merkitään $z = -4 + 7i$ ja $w = -2 - i$. Määritetään luvun $z$ käänteisluku sekä lukujen $z$ ja $w$ osamäärä.

Luvun $z$ käänteisluku sievennetään laventamalla nimittäjän liittoluvulla kohdassa $(*)$:

$$\begin{aligned} z^{-1} &= \frac{1}{z} = \frac{1}{-4+7i} \overset{(*)}{=} \frac{-4-7i}{(-4-7i)(-4+7i)} = \frac{-4-7i}{(-4)^2-(7i)^2} = \frac{-4-7i}{16-49i^2} = \frac{-4-7i}{16+49} \\ &= \frac{-4-7i}{65} = -\frac{4}{65} - \frac{7}{65}\,i. \end{aligned}$$

Lukujen $z$ ja $w$ osamääräkin sievennetään laventamalla nimittäjän liittoluvulla kohdassa $(*)$:

$$\begin{aligned} \frac{z}{w} &= \frac{-4+7i}{-2-i} \overset{(*)}{=} \frac{(-2+i)(-4+7i)}{(-2+i)(-2-i)} = \frac{8-14i-4i+7i^2}{(-2)^2-i^2} = \frac{8-18i+7\cdot(-1)}{4-(-1)} \\ &= \frac{8-18i-7}{5} = \frac{1-18i}{5} = \frac{1}{5} - \frac{18}{5}\,i. \end{aligned}$$

**Esimerkki 7.5.5.** Määritetään kompeksiluvun $z = \dfrac{10}{-4+2i}$ reaaliosa ja imaginaariosa.

Lavennetaan nimittäjän liittoluvulla kohdassa $(*)$:

$$\begin{aligned} z &= \frac{10}{-4+2i} \overset{(*)}{=} \frac{10\cdot(-4-2i)}{(-4+2i)(-4-2i)} = \frac{-40-20i}{(-4)^2-(2i)^2} = \frac{-40-20i}{16-4i^2} \\ &= \frac{-40-20i}{16+4} = \frac{-40-20i}{20} = -2 - i. \end{aligned}$$

Siis $\operatorname{Re} z = -2$ ja $\operatorname{Im} z = -1$.

**Esimerkki 7.5.6.** Määritetään kompeksiluvun $z = \dfrac{2i}{1-3i} + \dfrac{1}{i}$ reaaliosa ja imaginaariosa.

Lavennetaan nimittäjien liittoluvuilla kohdassa $(*)$:

$$
\begin{aligned}
z = \frac{2i}{1-3i} + \frac{1}{i} &\overset{(*)}{=} \frac{2i(1+3i)}{(1-3i)(1+3i)} + \frac{1\cdot(-i)}{i(-i)} = \frac{2i+6i^2}{1^2-(3i)^2} + \frac{-i}{-i^2} = \frac{2i-6}{1-9i^2} + \frac{-i}{-(-1)} \\
&= \frac{2i-6}{1+9} + \frac{-i}{1} = \frac{2i-6}{10} + \frac{-10i}{10} = \frac{2i-6-10i}{10} = \frac{-6-8i}{10} = -\frac{3}{5} - \frac{4}{5}i.
\end{aligned}
$$

Siis $\operatorname{Re} z = -3/5$ ja $\operatorname{Im} z = -4/5$.

---

Itseisarvon tutut ominaisuudet pätevät myös kompleksilukujen käänteisluvuille kuten seuraava lause osoittaa.

**Lause 7.5.7.** *Oletetaan, että $z \in \mathbb{C}$ ja $z \neq 0$. Käänteisluvun $z^{-1}$ itseisarvo on itseisarvon käänteisluku $1/|z|$ eli*

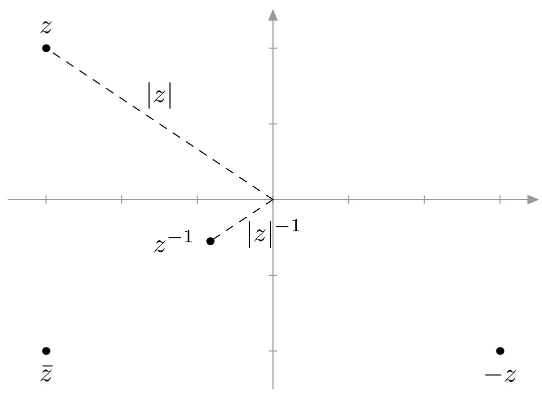
$$|z^{-1}| = \frac{1}{|z|}\,.$$

*Todistus.* Lauseen 7.4.6 mukaan itseisarvojen tulo on tulon itseisarvo, joten

$$|z^{-1}| \cdot |z| = |z^{-1}z| = |1| = 1.$$

Koska oletuksen mukaan $z \neq 0$, niin $|z| \neq 0$. Jakamalla luvulla $|z|$ saadaan

$$|z^{-1}| = \frac{1}{|z|}\,. \qquad \square$$




Kuva 7.8: Kompleksiluvun $z$ liittoluku, käänteisluku ja vastaluku.

## 7.6 Yhtälöiden ratkaisemisesta

Yhtälön ratkaisu voi joskus löytyä kokeilemalla tai arvaamalla kuten seuraavassa esimerkissä.

**Esimerkki 7.6.1.** Tutkitaan yhtälöä $\sqrt{2x-1} = x - 2$. Kokeilemalla huomataan, että luku 5 on kyseisen yhtälön ratkaisu. Nimittäin jos $x = 5$, niin

$$\sqrt{2x-1} = \sqrt{2 \cdot 5 - 1} = \sqrt{9} = 3 = 5 - 2 = x - 2.$$

Tämän perusteella ei kuitenkaan vielä tiedetä, onko tutkittavalla yhtälöllä muitakin ratkaisuja.

---

Jos halutaan määrittää yhtälön kaikki ratkaisut, voidaan aluksi rajata mahdollisten ratkaisujen joukkoa. Tämä tehdään lähtemällä liikkeelle tutkittavasta yhtälöstä ja katsomalla, mitä siitä voidaan päätellä. Tätä on havainnollistettu seuraavassa esimerkissä.

**Esimerkki 7.6.2.** Tutkitaan yhtälöä $\sqrt{2x-1} = x - 2$. Voidaan päätellä seuraavasti:

$$\begin{aligned}\sqrt{2x-1} = x - 2 \;\Rightarrow\; (\sqrt{2x-1})^2 = (x-2)^2 \;\Rightarrow\; 2x - 1 = x^2 - 4x + 4 \\ \Rightarrow\; 0 = x^2 - 6x + 5 \;\Rightarrow\; x = \frac{6 \pm \sqrt{(-6)^2 - 4 \cdot 1 \cdot 5}}{2 \cdot 1} \\ \Rightarrow\; x = \frac{6 \pm 4}{2} \;\Rightarrow\; x = 5 \;\vee\; x = 1\end{aligned}$$

Tämä päättely osoittaa, että tarkasteltava yhtälön ratkaisut löytyvät joukosta $\{1, 5\}$. Millään muulla luvulla yhtälö ei voi toteutua.

Tehty päättely ei kuitenkaan takaa, että löydetyt luvut todella olisivat ratkaisuja. Esimerkiksi jos $x = 1$, niin $\sqrt{2x-1} = \sqrt{2 \cdot 1 - 1} = \sqrt{1} = 1$ mutta $x - 2 = 1 - 2 = -1$. Havaitaan, että luku 1 ei ole tutkittavan yhtälön ratkaisu.

---

Yhdistämällä esimerkkien 7.6.1 ja 7.6.2 tiedot voidaan päätellä, että yhtälöllä $\sqrt{2x-1} = x-2$ on tasan yksi ratkaisu, joka on $x = 5$. Yhtälön kaikkien ratkaisujen etsiminen vaatii siis kaksi vaihetta: mahdollisten ratkaisujen joukon rajaamisen sekä mahdollisten ratkaisujen tarkistamisen. Seuraava esimerkki havainnollistaa yhtälön ratkaisemista kompleksilukujen joukossa.

**Esimerkki 7.6.3.** Ratkaistaan kompleksilukujen joukossa yhtälö $iz + 3 = 5z - \dfrac{z}{i} + 2i$.

Rajataan aluksi mahdollisten ratkaisujen joukkoa tutkimalla, mitä voidaan päätellä lähtemällä oletuksesta, että yhtälö toteutuu.

$$\begin{aligned}iz + 3 = 5z - \frac{z}{i} + 2i \overset{(1)}{\Rightarrow} i^2 z + 3i = 5iz - z + 2i^2 \overset{(2)}{\Rightarrow} -z + 3i = 5iz - z - 2 \\ \overset{(3)}{\Rightarrow} 3i + 2 = 5iz \overset{(4)}{\Rightarrow} \frac{3i+2}{5i} = z\end{aligned}$$

Kohdassa (1) kerrotaan yhtälön molemmat puolet imaginaariyksiköllä $i$, jotta nimittäjä supistuu pois. Kohdassa (2) käytetään tietoa $i^2 = -1$. Kohdassa (3) yhtälön molemmille puolille lisätään $z + 2$, jotta päästään yhtälöön, jossa tuntematon $z$ esiintyy vain yhtälön toisella puolella. Kohdassa (4) jaetaan yhtälön molemmat puolet tuntemattoman kertoimella $5i$.

Laventamalla nimittäjän liittoluvulla saadaan tulos sievennettyä:

$$z = \frac{2+3i}{5i} = \frac{-5i(2+3i)}{-(5i)^2} = \frac{-10i - 15i^2}{-25i^2} = \frac{-10i + 15}{25} = \frac{3}{5} - \frac{2}{5}\,i = 0{,}6 - 0{,}4i.$$

Tämä päättely osoittaa, että tarkastellun yhtälön ratkaisut löytyvät joukosta $\{0{,}6 - 0{,}4i\}$. Mikään muu luku ei voi olla tarkastellun yhtälön ratkaisu. Kyseisellä yhtälöllä on siis enintään yksi ratkaisu. Periaatteessa on mahdollista, että yhtälöllä ei ole yhtään ratkaisua!

Tarkistetaan löydetty mahdollinen ratkaisu. Sijoitetaan $z = 0{,}6 - 0{,}4i$ yhtälön vasemmalle puolelle:

$$iz + 3 = i(0{,}6 - 0{,}4i) + 3 = 0{,}6i - 0{,}4i^2 + 3 = 0{,}6i + 0{,}4 + 3 = 3{,}4 + 0{,}6i.$$

Sijoitetaan $z = 0{,}6 - 0{,}4i$ yhtälön oikealle puolelle:

$$\begin{aligned} 5z - \frac{z}{i} + 2i &= 5(0{,}6 - 0{,}4i) - \frac{1}{i}(0{,}6 - 0{,}4i) + 2i = 3 - 2i - \frac{0{,}6}{i} + 0{,}4 + 2i \\ &= 3{,}4 - \frac{0{,}6}{i} = 3{,}4 - \frac{0{,}6i}{i^2} = 3{,}4 + 0{,}6i \end{aligned}$$

Yhtälön vasen ja oikea puoli ovat yhtä suuret, joten yhtälö toteutuu ja luku $0{,}6 - 0{,}4i$ on sen ratkaisu. Mahdollisten ratkaisujen joukon rajaaminen ja sijoittamalla tehty tarkistus yhdessä osoittavat, että yhtälöllä

$$iz + 3 = 5z - \frac{z}{i} + 2i$$

on tasan yksi ratkaisu, joka on $z = 0{,}6 - 0{,}4i$.

**Esimerkki 7.6.4.** Ratkaistaan kompleksilukujen joukossa yhtälö $3z - 4i = 1 + 2iz$.

Rajataan ensin mahdollisten ratkaisujen joukkoa:

$$\begin{aligned} 3z - 4i = 1 + 2iz \;\Rightarrow\; 3z = 1 + 2iz + 4i \;\Rightarrow\; 3z - 2iz = 1 + 4i \;\Rightarrow\; (3-2i)z = 1 + 4i \\ \Rightarrow\; z = \frac{1+4i}{3-2i} \end{aligned}$$

Tämä päättely osoittaa, että yhtälöllä on enintään yksi ratkaisu. Periaatteessa on mahdollista, että yhtälöllä ei ole yhtään ratkaisua!

Huomataan kuitenkin, että kaikkien implikaatioiden suunta voidaan kääntää:

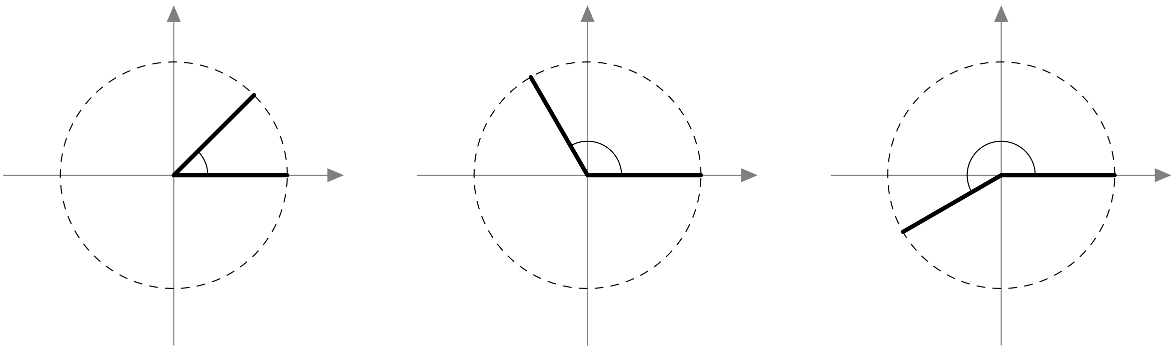
$$\begin{aligned} z = \frac{1+4i}{3-2i} \;\Rightarrow\; (3-2i)z = 1 + 4i \;\Rightarrow\; 3z - 2iz = 1 + 4i \;\Rightarrow\; 3z = 1 + 2iz + 4i \\ \Rightarrow\; 3z - 4i = 1 + 2iz. \end{aligned}$$

Nämä kaksi erisuuntaista päättelyä yhdessä osoittavat, että tarkastellulla yhtälöllä on tasan yksi ratkaisu, joka on

$$z = \frac{1+4i}{3-2i} = \frac{(3+2i)(1+4i)}{(3+2i)(3-2i)} = \frac{3+12i+2i+8i^2}{9-4i^2} = \frac{-5+14i}{13} = -\frac{5}{13} + \frac{14}{13}\,i\,.$$

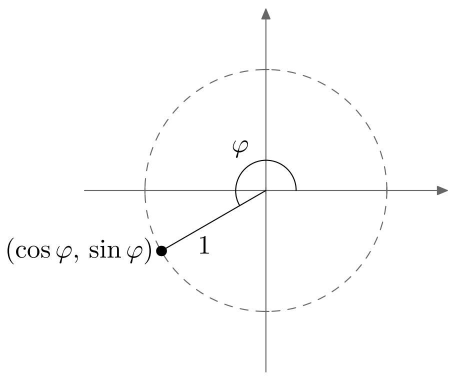
## 7.7 Napaesitys

Yksikköympyrä tarkoittaa ympyrää, jonka keskipiste on origossa ja jonka säde on yksi. Mikä tahansa kulma voidaan piirtää yksikköympyrään asettamalla kulman kärki origoon ja toinen kylki positiiviselle vaaka-akselille. Kulman suuruus määrää sen, mihin suuntaan kulman toinen kylki piirretään. Tätä on havainnollistettu kuvassa 7.9.



Kuva 7.9: Yksikköympyrään piirretyt 45 asteen, 120 asteen ja 210 asteen kulmat.

Trigonometriset funktiot sini ja kosini voidaan määritellä yksikköympyrän avulla. Kulman $\varphi$ kosini on kulmaa $\varphi$ vastaavan yksikköympyrän kehäpisteen vaakakoordinaatti. Vastaavasti kulman $\varphi$ sini on tämän kehäpisteen pystykoordinaatti. Tätä havainnollistetaan kuvassa 7.10.

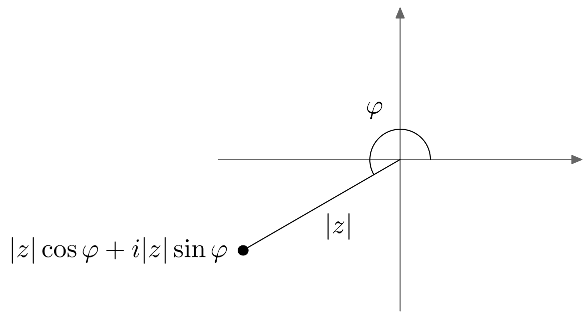



Kuva 7.10: Sini ja kosini yksikköympyrän avulla määriteltynä.

**Määritelmä 7.7.1.** Kompleksiluvun $z$ *napaesitys* tarkoittaa sen esittämistä muodossa

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

missä $|z|$ on luvun $z$ itseisarvo eli moduli ja $\varphi$ on luvun $z$ *vaihekulma* eli *argumentti.*

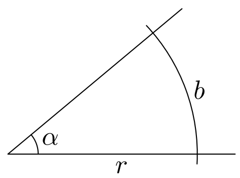



Kuva 7.11: Kompleksiluvun napaesitys.

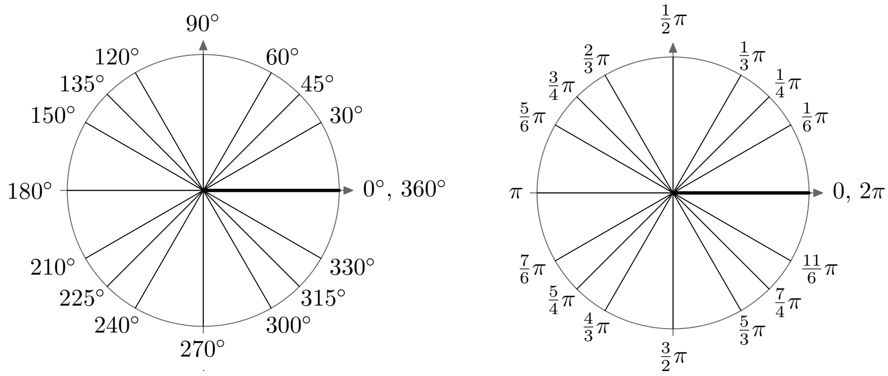
Kompleksiluvun vaihekulman yksikkönä on usein absoluuttinen kulmayksikkö eli radiaani.

**Määritelmä 7.7.2.** Kulman suuruus $\alpha$ *radiaaneina* on kulman rajoittaman ympyrän kaaren $b$ suhde ympyrän säteeseen $r$:

$$\alpha = \frac{b}{r}$$

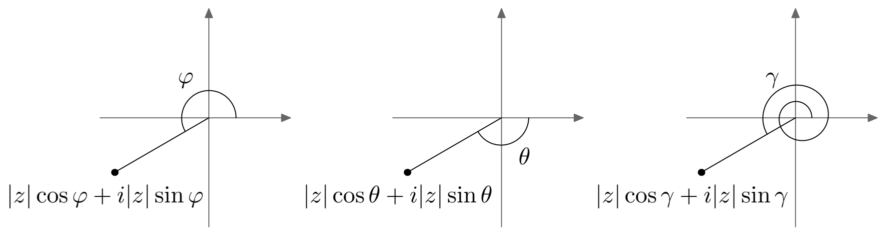



Täyskulma 360° vastaa $2\pi$ radiaania ja oikokulma 180° vastaa $\pi$ radiaania. Näistä voidaan johtaa muiden kulmien tarkkoja arvoja radiaaneissa. Joitakin niistä on merkitty kuvaan 7.12.




Kuva 7.12: Joitakin kulmia ilmaistuna asteissa ja radiaaneissa.

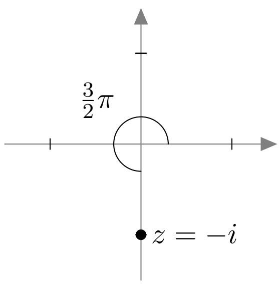
Kompleksiluvun vaihekulma ei ole yksikäsitteinen. Luvun 0 vaihekulmaksi voidaan valita mikä luku tahansa, sillä $0 = 0(\cos\varphi + i\sin\varphi)$ kaikilla $\varphi \in \mathbb{R}$. Nollasta poikkeavan kompleksiluvun vaihekulmat eroavat toisistaan jollain määrällä täysiä kierroksia. Toisin sanottuna nollasta poikkeavan kompleksiluvun tapauksessa kahden vaihekulman erotus on aina $n \cdot 2\pi$, missä $n \in \mathbb{Z}$. Tätä on havainnollistettu kuvassa 7.13.




Kuva 7.13: Kompleksiluvun $z$ eri vaihekulmia: $\theta = \varphi - 2\pi$ ja $\gamma = \varphi + 2\pi$.

**Esimerkki 7.7.3.** Määritetään kompleksiluvun $z = -i$ napaesitys.

Itseisarvon määritelmän mukaan $|z| = \sqrt{0^2 + (-1)^2} = \sqrt{1} = 1$. Merkitään luku $z = -i$ kompleksitasoon:



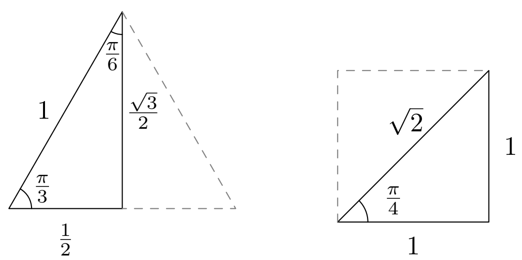

Kuva 7.14: Luku $z = -i$ kompleksitasossa.

Kuvan avulla voidaan päätellä, että luvun $z$ yksi vaihekulma on 270 astetta eli $3\pi/2$ radiaania. Näin luvun $z$ napaesitykseksi saadaan $z = \cos(3\pi/2) + i\sin(3\pi/2)$.

Vaihekulmaksi voidaan valita myös $-90$ astetta eli $-\pi/2$ radiaania. Tällöin päädytään vaihtoehtoiseen napaesitykseen $z = \cos(-\pi/2) + i\sin(-\pi/2)$.

---

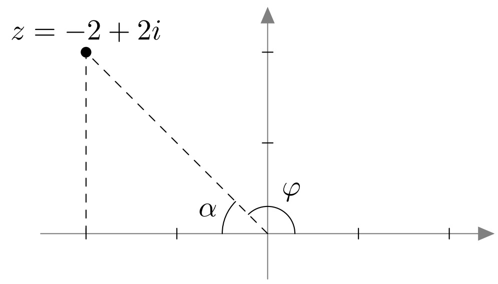
Joidenkin kompleksilukujen vaihekulman päätteleminen onnistuu niin sanottujen muistikolmioiden avulla. Ne voidaan johtaa tasasivuisesta kolmiosta ja neliöstä (kuva 7.15).




Kuva 7.15: Muistikolmiot.

**Esimerkki 7.7.4.** Määritetään kompleksiluvun $z = -2 + 2i$ napaesitys.

Itseisarvon määritelmän mukaan $|z| = \sqrt{(-2)^2 + 2^2} = \sqrt{8} = \sqrt{4 \cdot 2} = \sqrt{4} \cdot \sqrt{2} = 2\sqrt{2}$. Merkitään luku $z = -2 + 2i$ kompleksitasoon:

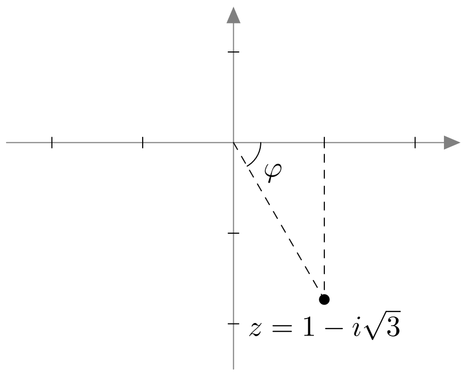



Kuva 7.16: Luku $z = -2 + 2i$ kompleksitasossa.

Kuvaan piirretyn suorakulmaisen kolmion molempien kateettien pituus on 2, joten $\alpha = 45°$. Luvun $z$ yksi vaihekulma on siten $\varphi = 180° - 45° = 135°$ eli $\varphi = 3\pi/4$. Näin luvun $z$ napaesitykseksi saadaan $z = 2\sqrt{2}\big(\cos(3\pi/4) + i\sin(3\pi/4)\big)$.

**Esimerkki 7.7.5.** Määritetään kompleksiluvun $z = 1 - i\sqrt{3}$ napaesitys.

Itseisarvon määritelmän mukaan $|z| = \sqrt{1^2 + \sqrt{3}^2} = \sqrt{4} = 2$. Merkitään luku $z = 1 - i\sqrt{3}$ kompleksitasoon:




Kuva 7.17: Luku $z = 1 - i\sqrt{3}$ kompleksitasossa.

Kuvaan piirretyn suorakulmaisen kolmion kateetit ovat 1 ja $\sqrt{3}$ ja hypotenuusa on 2. Havaitaan, että se on yhdenmuotoinen muistikolmion kanssa. Tästä voidaan päätellä, että $\varphi = -60°$ eli $\varphi = -\pi/3$. Näin luvun $z$ napaesitykseksi saadaan $z = 2\big(\cos(-\pi/3) + i\sin(-\pi/3)\big)$.

Vaihekulmaksi voidaan valita myös $360 - 60 = 300$ astetta eli $5\pi/3$ radiaania. Tällöin päädytään vaihtoehtoiseen napaesitykseen $z = 2\big(\cos(5\pi/3) + i\sin(5\pi/3)\big)$.

Liittoluvun ja käänteisluvun määrittäminen onnistuu hyvin myös napaesityksessä, kuten seuraava lause osoittaa.

**Lause 7.7.6.** *Oletetaan, että kompleksiluvulla $z$ on napaesitys $z = |z|(\cos\varphi + i\sin\varphi)$. Tällöin luvun $z$ liittoluku on*

$$\bar{z} = |z|(\cos(-\varphi) + i\sin(-\varphi))$$

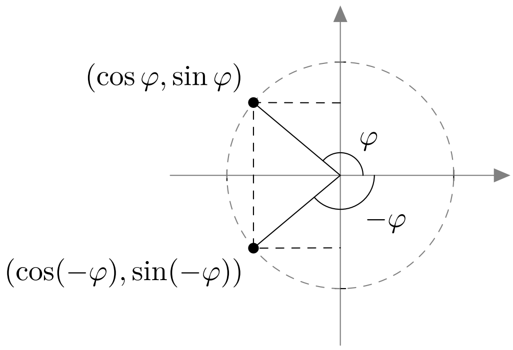
*ja käänteisluku on*

$$z^{-1} = |z|^{-1}(\cos(-\varphi) + i\sin(-\varphi)).$$

*Todistus.* Määritelmän 7.4.1 mukaan luvun $z = |z|\cos\varphi + i|z|\sin\varphi$ liittoluku on

$$\bar{z} = |z|\cos\varphi - i|z|\sin\varphi.$$

Yksikköympyrän avulla voidaan päätellä, että $\cos(-\varphi) = \cos\varphi$ ja $\sin(-\varphi) = -\sin\varphi$:




Kuva 7.18: Havaitaan, että $\cos(-\varphi) = \cos\varphi$ ja $\sin(-\varphi) = -\sin\varphi$.

Luvun $z$ liittoluku voidaan siis kirjoittaa muodossa

$$\bar{z} = |z|\cos(-\varphi) + i|z|\sin(-\varphi).$$

Käyttämällä määritelmää 7.5.1 ja liittoluvun $\bar{z}$ napaesitystä luvun $z$ käänteisluvuksi saadaan

$$z^{-1} = \frac{1}{|z|^2}\bar{z} = \frac{1}{|z|^2} \cdot |z|(\cos(-\varphi) + i\sin(-\varphi)) = \frac{1}{|z|}(\cos(-\varphi) + i\sin(-\varphi)).$$

$\square$

**Esimerkki 7.7.7.** Esimerkissä 7.7.5 etsittiin luvulle $z = 1 - i\sqrt{3}$ napaesitys

$$z = 2\big(\cos(-\pi/3) + i\sin(-\pi/3)\big).$$

Lauseen 7.7.6 mukaan luvun $z$ liittoluku on

$$\bar{z} = 2\big(\cos(\pi/3) + i\sin(\pi/3)\big)$$

ja käänteisluku on

$$z^{-1} = \frac{1}{2}\big(\cos(\pi/3) + i\sin(\pi/3)\big).$$

Napaesityksen avulla saadaan toinen tapa kompleksilukujen tulon ja osamäärän laskemiseen:

**Lause 7.7.8.** *Oletetaan, että luvuilla $z$, $w \in \mathbb{C}$ on napaesitykset $z = |z|(\cos\varphi + i\sin\varphi)$ ja $w = |w|(\cos\theta + i\sin\theta)$. Tällöin lukujen $z$ ja $w$ tulo on*

$$zw = |z||w|(\cos(\varphi+\theta) + i\sin(\varphi+\theta))$$

*ja osamäärä on*

$$\frac{z}{w} = \frac{|z|}{|w|}(\cos(\varphi-\theta) + i\sin(\varphi-\theta))$$

*Todistus.* Lasketaan napaesitysten tulo:

$$\begin{aligned}
zw &= |z|(\cos\varphi + i\sin\varphi)\cdot|w|(\cos\theta + i\sin\theta)\\
&= |z||w|(\cos\varphi + i\sin\varphi)(\cos\theta + i\sin\theta)\\
&= |z||w|(\cos\varphi\cos\theta + i\cos\varphi\sin\theta + i\sin\varphi\cos\theta + i^2\sin\varphi\sin\theta)\\
&= |z||w|(\cos\varphi\cos\theta + i(\cos\varphi\sin\theta + \sin\varphi\cos\theta) - \sin\varphi\sin\theta)\\
&= |z||w|(\cos\varphi\cos\theta - \sin\varphi\sin\theta + i(\cos\varphi\sin\theta + \sin\varphi\cos\theta))
\end{aligned}$$

Käyttämällä kosinin ja sinin summakaavoja

$$\begin{aligned}
\cos(\varphi+\theta) &= \cos\varphi\cos\theta - \sin\varphi\sin\theta\\
\sin(\varphi+\theta) &= \cos\varphi\sin\theta + \sin\varphi\cos\theta
\end{aligned}$$

saatu tulos voidaan kirjoittaa muodossa

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

Todistus perustui siis kosinin ja sinin summakaavoihin, jotka puolestaan voidaan perustella eri tavoin. Osoitteesta math.uaa.alaska.edu/∼smiley/trigproofs.html löytyy geometrinen todistus alle 90° kulmille. Osoitteesta www.intmath.com/analytic-trigonometry/2-sum-difference-angles löytyy kaksi erilaista yksikköympyrää hyödyntävää todistusta.

Osamäärää $z/w = zw^{-1}$ koskeva väite voidaan todistaa käyttämällä lausetta 7.7.6 ja äsken todistettua tulosta. Se jätetään harjoitustehtäväksi. □

**Esimerkki 7.7.9.** Lukujen $z = 1 - i\sqrt{3}$ ja $w = -2 + 2i$ napaesitykset ovat esimerkkien 7.7.5 ja 7.7.4 mukaan $z = 2(\cos(-\pi/3) + i\sin(-\pi/3))$ ja $w = 2\sqrt{2}(\cos(3\pi/4) + i\sin(3\pi/4))$. Lauseen 7.7.8 mukaan niiden tulo on

$$\begin{aligned}
zw &= 2\cdot 2\sqrt{2}\left(\cos\left(-\frac{1}{3}\pi + \frac{3}{4}\pi\right) + i\sin\left(-\frac{1}{3}\pi + \frac{3}{4}\pi\right)\right)\\
&= 4\sqrt{2}\left(\cos\left(\frac{5}{12}\pi\right) + i\sin\left(\frac{5}{12}\pi\right)\right).
\end{aligned}$$

Lukujen $z$ ja $w$ osamäärä on lauseen 7.7.8 mukaan

$$\begin{aligned}
\frac{z}{w} &= \frac{2}{2\sqrt{2}}\left(\cos\left(-\frac{1}{3}\pi - \frac{3}{4}\pi\right) + i\sin\left(-\frac{1}{3}\pi - \frac{3}{4}\pi\right)\right)\\
&= \frac{1}{\sqrt{2}}\left(\cos\left(-\frac{13}{12}\pi\right) + i\sin\left(-\frac{13}{12}\pi\right)\right).
\end{aligned}$$

Nollasta poikkeaville kompleksiluvuille voidaan määritellä negatiiviset potenssit:

**Määritelmä 7.7.10.** Oletetaan, että $z \in \mathbb{C}$ ja $n \in \mathbb{N}$. Oletetaan lisäksi, että $z \neq 0$. Merkintä $z^{-n}$ tarkoittaa luvun $z^n$ käänteislukua:

$$z^{-n} = (z^n)^{-1}.$$

Lisäksi määritellään, että $z^0 = 1$.

Kompleksilukujen potenssien laskemisessa auttaa niin sanottu de Moivren kaava, joka on saanut nimensä ranskalaisen matemaatikon Abraham de Moivren mukaan:

**Lause 7.7.11 (de Moivren kaava).** *Oletetaan, että kompleksiluvulla $z \neq 0$ on napaesitys $z = |z|(\cos\varphi + i\sin\varphi)$. Tällöin kaikilla $n \in \mathbb{Z}$ pätee*

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

*Todistus.* Todistetaan aluksi induktiolla, että kaikilla $n \in \mathbb{N}$ pätee $z^n = |z|^n(\cos n\varphi + i\sin n\varphi)$.

Alkuaskel: Jos $n = 0$, niin

$$|z|^n(\cos n\varphi + i\sin n\varphi) = |z|^0(\cos 0 + i\sin 0) = 1\cdot(1+0i) = 1 = z^0 = z^n.$$

Induktioaskel: Aloitetaan tekemällä induktio-oletus. Oletetaan, että $k \in \mathbb{N}$ ja

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

Käyttämällä induktio-oletusta ja lausetta 7.7.8 saadaan

$$\begin{aligned} z^{k+1} = z\cdot z^k &= |z|(\cos\varphi + i\sin\varphi)\cdot|z|^k(\cos k\varphi + i\sin k\varphi)\\ &= |z|^{k+1}(\cos(\varphi + k\varphi) + i\sin(\varphi + k\varphi))\\ &= |z|^{k+1}(\cos(k+1)\varphi + i\sin(k+1)\varphi). \end{aligned}$$

Johtopäätös: Alkuaskeleesta ja induktioaskeleesta seuraa induktioperiaatteen nojalla, että kaikilla $n \in \mathbb{N}$ pätee $z^n = |z|^n(\cos n\varphi + i\sin n\varphi)$.

Todistetaan väite vielä negatiivisille kokonaisluvuille. Oletetaan, että $m \in \mathbb{Z}$ ja $m < 0$. Tällöin $-m > 0$ ja määritelmän 7.7.10 nojalla $z^m = (z^{-m})^{-1}$. Käytämällä äsken todistettua tulosta ja lausetta 7.7.6 saadaan

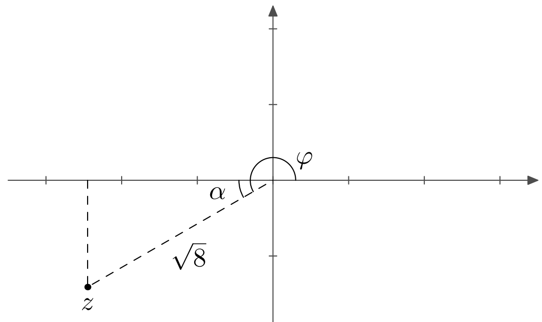
$$\begin{aligned} z^m = (z^{-m})^{-1} &= \Big(|z|^{-m}(\cos(-m\varphi) + i\sin(-m\varphi))\Big)^{-1}\\ &= (|z|^{-m})^{-1}(\cos m\varphi + i\sin m\varphi)\\ &= |z|^m(\cos m\varphi + i\sin m\varphi) \end{aligned}$$

Näin on osoitettu, että kaikilla $n \in \mathbb{Z}$ pätee $z^n = |z|^n(\cos n\varphi + i\sin n\varphi)$. □

**Esimerkki 7.7.12.** Olkoon $z = -\sqrt{6} - i\sqrt{2}$. Lasketaan de Moivren kaavan avulla $z^{10}$. Aloitetaan määrittämällä luvun $z$ napaesitys. Itseisarvon määritelmän mukaan

$$|z| = \sqrt{(-\sqrt{6})^2 + (-\sqrt{2})^2} = \sqrt{8} = \sqrt{4 \cdot 2} = \sqrt{4}\sqrt{2} = 2\sqrt{2}.$$

Vaihekulman selvittämistä varten merkitään luku $z$ kompleksitasoon:




Kuva 7.19: Luku $z = -\sqrt{6} - i\sqrt{2}$ kompleksitasossa.

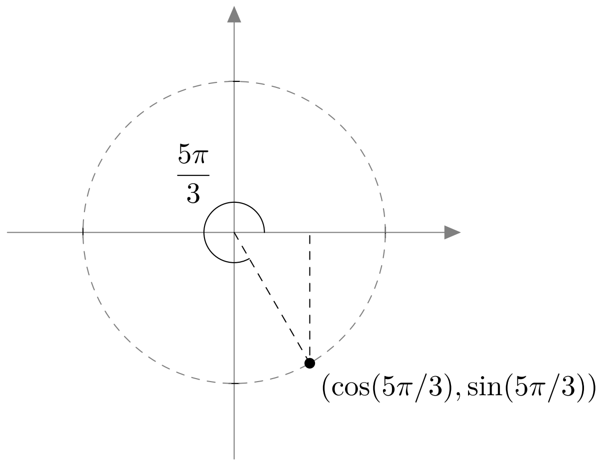
Kuvaan piirretyn suorakulmaisen kolmion kateettien pituudet ovat $\sqrt{6} = \sqrt{3}\sqrt{2}$ ja $\sqrt{2}$. Hypotenuusan pituus on $\sqrt{8} = 2\sqrt{2}$. Havaitaan, että kuvan 7.19 kolmio saadaan, kun kuvan 7.15 muistikolmion kaikki sivut kerrotaan luvulla $\sqrt{2}$. Kyseiset kolmiot ovat siis yhdenmuotoiset. Tästä voidaan päätellä, että $\alpha = \pi/6$. Luvun $z$ yksi vaihekulma on siten $\varphi = \pi + \alpha = 7\pi/6$. Luvun $z$ napaesitykseksi saadaan $z = 2\sqrt{2}\big((\cos(7\pi/6) + i\sin(7\pi/6)\big)$.

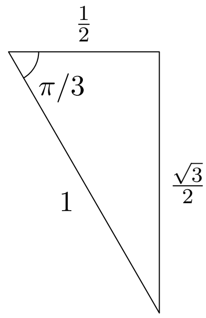
Luvun $z$ kymmenes potenssi voidaan nyt laskea de Moivren kaavalla (lause 7.7.11):

$$\begin{aligned}
z^{10} &= (2\sqrt{2})^{10}\big(\cos(10 \cdot 7\pi/6) + i\sin(10 \cdot 7\pi/6)\big) \\
&= 2^{10}\sqrt{2}^{10}\big(\cos(70\pi/6) + i\sin(70\pi/6)\big) \\
&= 2^{10}2^{5}\big(\cos(11\pi + 4\pi/6) + i\sin(11\pi + 4\pi/6)\big) \\
&= 2^{15}\big(\cos(5 \cdot 2\pi + \pi + 2\pi/3) + i\sin(5 \cdot 2\pi + \pi + 2\pi/3)\big) \\
&= 2^{15}\big(\cos(\pi + 2\pi/3) + i\sin(\pi + 2\pi/3)\big) \\
&= 2^{15}\big(\cos(5\pi/3) + i\sin(5\pi/3)\big)
\end{aligned}$$

Napaesityksestä voidaan siirtyä takaisin tavalliseen summamuotoiseen esitykseen. Yksikköympyrän ja muistikolmion avulla voidaan päätellä, että $\cos(5\pi/3) = 1/2$ ja $\sin(5\pi/3) = -\sqrt{3}/2$. Tätä on havainnollistettu kuvassa 7.20. Näin saadaan

$$z = 2^{15}\left(\frac{1}{2} - \frac{\sqrt{3}}{2}i\right) = 2^{14}(1 - i\sqrt{3}).$$




Kuva 7.20: Kosinin ja sinin arvojen päätteleminen yksikköympyrän ja muistikolmion avulla.

## 7.8 Eksponenttiesitys

Otetaan yksinkertaisuuden vuoksi käyttöön seuraava määritelmä:

**Määritelmä 7.8.1.** Oletetaan, että $\varphi \in \mathbb{R}$. Tällöin

$$e^{i\varphi} = \cos\varphi + i\sin\varphi\,.$$

Potenssisarjojen avulla voidaan eksponenttifunktio $x \mapsto e^x$ sekä trigonometriset funktiot sini ja kosini määritellä koko kompleksitasossa. Tällöin yllä olevassa määritelmässä 7.8.1 esiintyvä yhtälö eli niin sanottu Eulerin kaava saadaan todistettuna tuloksena. Lisätietoja tästä löytyy esimerkiksi Petri Olan kirjoittamasta Lukualueet-kurssin materiaalista. Koska potenssisarjojen teoria ei kuulu tämän kurssin esitietoihin, käytämme määritelmää 7.8.1.

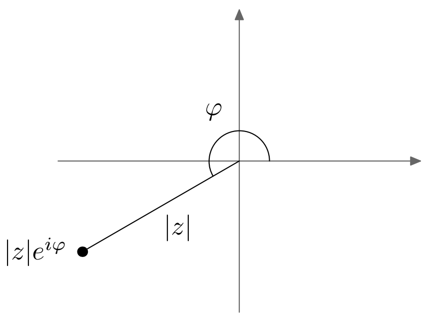
Määritelmän 7.8.1 avulla kompleksiluvun $z$ napaesitys $|z|(\cos\varphi + i\sin\varphi)$ voidaan kirjoittaa muodossa $|z|e^{i\varphi}$. Tätä esitysmuotoa kutsutaan luvun $z$ eksponenttiesitykseksi, kuten alla olevasta määritelmästä käy ilmi.

**Määritelmä 7.8.2.** Kompleksiluvun $z$ *eksponenttiesitys* tarkoittaa luvun $z$ esittämistä muodossa

$$z = |z|e^{i\varphi}\,,$$

missä $|z|$ on luvun $z$ itseisarvo ja $\varphi$ on luvun $z$ vaihekulma.

Kompleksiluvun $z$ eksponenttiesitystä on havainnollistettu kuvassa 7.21.

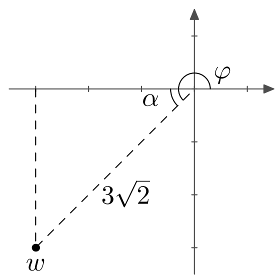



Kuva 7.21: Kompleksiluvun $z$ eksponenttiesitys.

**Esimerkki 7.8.3.** Määritetään kompleksiluvun $w = -3 - 3i$ eksponenttiesitys.

Itseisarvon määritelmän mukaan $|w| = \sqrt{(-3)^2 + (-3)^2} = \sqrt{18} = \sqrt{9 \cdot 2} = \sqrt{9}\sqrt{2} = 3\sqrt{2}$.

Merkitään luku $w = -3 - 3i$ kompleksitasoon:



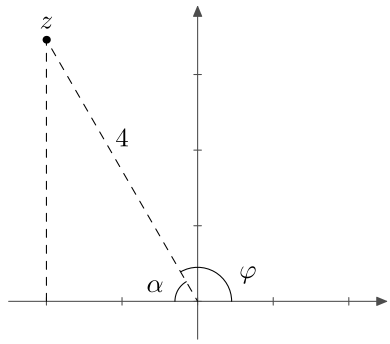

Kuva 7.22: Luku $w = -3 - 3i$ kompleksitasossa.

Kuvan 7.22 suorakulmaisesta kolmiosta saadaan pääteltyä, että $\alpha = \pi/4$. Luvun $w$ vaihekulmaksi voidaan siten valita $\varphi = \pi + \alpha = 5\pi/4$. Näin luvun $w$ eksponenttiesitykseksi saadaan

$$w = 3\sqrt{2}e^{\frac{5\pi}{4}i}.$$

**Esimerkki 7.8.4.** Määritetään kompleksiluvun $z = -2 + 2\sqrt{3}i$ eksponenttiesitys.

Itseisarvon määritelmän mukaan $|z| = \sqrt{(-2)^2 + (2\sqrt{3})^2} = \sqrt{16} = 4$. Merkitään luku $z = -2 + 2\sqrt{3}i$ kompleksitasoon:




Kuva 7.23: Luku $z = -2 + 2\sqrt{3}i$ kompleksitasossa.

Kuvan 7.23 suorakulmaisesta kolmiosta saadaan pääteltyä esimerkiksi muistikolmion avulla, että $\alpha = \pi/3$. Luvun $z$ vaihekulmaksi kelpaa siten $\varphi = \pi - \alpha = 2\pi/3$. Näin luvun $z$ eksponenttiesitykseksi saadaan

$$z = 4e^{\frac{2\pi}{3}i}.$$

---

Napaesityksen laskusääntöjä koskevista lauseista 7.7.6 ja 7.7.8 sekä de Moivren kaavasta 7.7.11 seuraa, että eksponenttiesitystä käytettäessä voidaan soveltaa tuttuja potenssien laskusääntöjä. Tätä havainnollistetaan seuraavissa esimerkeissä.

**Esimerkki 7.8.5.** Määritetään luvun $z = 3e^{-\frac{\pi}{2}i} \cdot 7e^{\frac{\pi}{4}i}$ itseisarvo, vaihekulma, reaaliosa ja imaginaariosa.

Itseisarvo ja vaihekulma saadaan sieventämällä lukua $z$ tuttujen laskusääntöjen avulla:

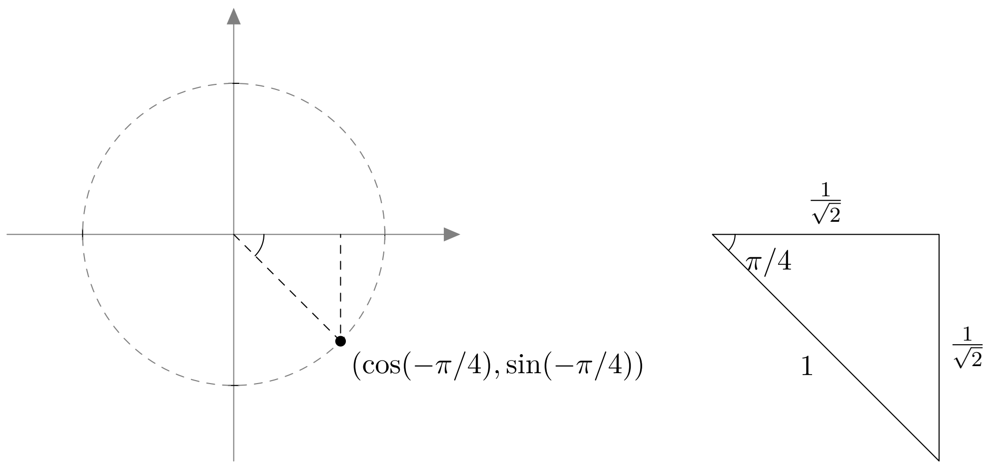
$$z = 3e^{-\frac{\pi}{2}i} \cdot 7e^{\frac{\pi}{4}i} = 3 \cdot 7e^{\left(-\frac{\pi}{2}+\frac{\pi}{4}\right)i} = 21e^{-\frac{\pi}{4}i}.$$

Havaitaan, että luvun $z$ itseisarvo on $|z| = 21$ ja luvun $z$ vaihekulmaksi kelpaa $-\pi/4$.

Reaaliosan ja imaginaariosan selvittämiseksi siirrytään napaesitykseen:

$$z = 21e^{-\frac{\pi}{4}i} = 21\left(\cos\left(-\frac{\pi}{4}\right) + i\sin\left(-\frac{\pi}{4}\right)\right) = 21\left(\frac{1}{\sqrt{2}} - i\frac{1}{\sqrt{2}}\right) = \frac{21\sqrt{2}}{2} - \frac{21\sqrt{2}}{2}i.$$

Kosinin ja sinin tarkat arvot voidaan tässä tapauksessa päätellä muistikolmion ja yksikköympyrän avulla. Muistikolmiosta saadaan itseisarvot, etumerkit päätellään kulman sijainnista yksikköympyrässä (kuva 7.24).




Kuva 7.24: Kosinin ja sinin arvojen päätteleminen yksikköympyrän ja muistikolmion avulla.

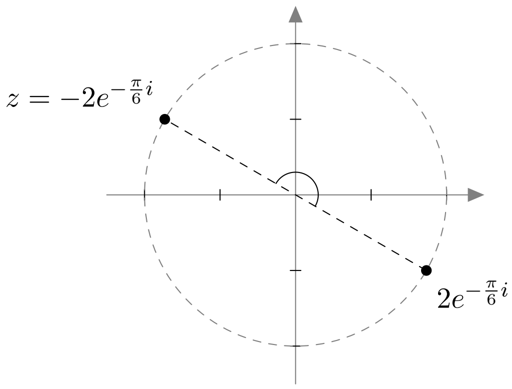
**Esimerkki 7.8.6.** Määritetään luvun $z = -2e^{-\frac{\pi}{6}i}$ itseisarvo ja vaihekulma sekä reaali- ja imaginaariosa.

Huomataan, että $z$ ei ole eksponenttiesityksessä, sillä kerroin $-2$ on negatiivinen. Käyttämällä luvun $-2$ eksponenttiesitystä $-2 = 2e^{\pi i}$ saadaan

$$z_2 = -2e^{-\frac{\pi}{6}i} = 2e^{\pi i} \cdot e^{-\frac{\pi}{6}i} = 2e^{(\pi-\frac{\pi}{6})i} = 2e^{\frac{5\pi}{6}i}.$$

Huomataan, että luvun $z$ itseisarvo on $|z| = 2$ ja luvun $z$ vaihekulmaksi kelpaa $5\pi/6$.

Toinen tapa itseisarvon ja vaihekulman selvittämiseksi on huomata, että luku $z = -2e^{-\frac{\pi}{6}i}$ on luvun $2e^{-\frac{\pi}{6}i}$ vastaluku. Tästä voidaan päätellä, että niiden itseisarvot ovat samat ja vaihekulmien erotus on $\pi$. Luvun $z$ itseisarvo on siten $|z| = 2$ ja luvun $z$ vaihekulmaksi kelpaa $-\pi/6 + \pi = 5\pi/6$. Tätä on havainnollistettu kuvassa 7.25.

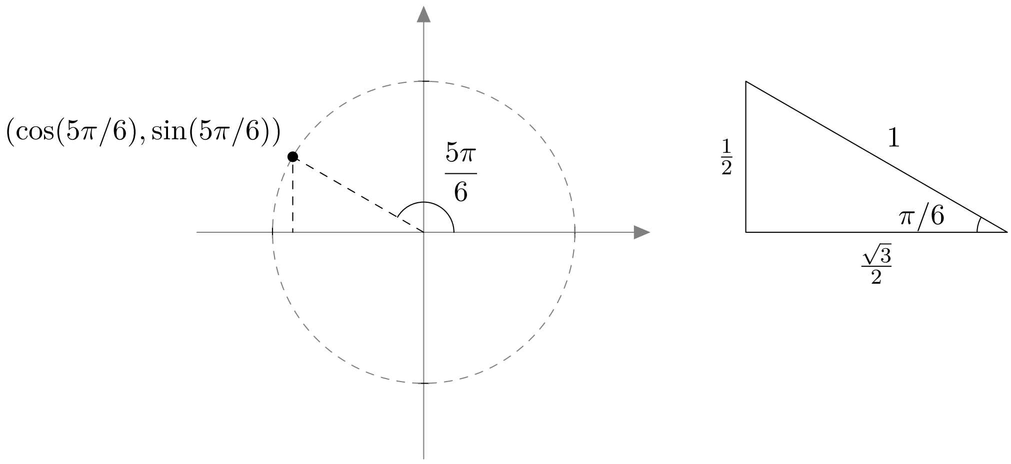



Kuva 7.25: Luku $z = -2e^{-\frac{\pi}{6}i}$ on luvun $2e^{-\frac{\pi}{6}i}$ vastaluku.

Reaali- ja imaginaariosan selvittämiseksi siirrytään napaesitykseen:

$$z = 2e^{\frac{5\pi}{6}i} = 2\left(\cos\left(\frac{5\pi}{6}\right) + i\sin\left(\frac{5\pi}{6}\right)\right) = 2\left(-\frac{\sqrt{3}}{2} + i\frac{1}{2}\right) = -\sqrt{3} + i.$$

Kosinin ja sinin tarkat arvot voidaan tässäkin tapauksessa päätellä muistikolmion ja yksikköympyrän avulla. Muistikolmiosta saadaan itseisarvot, etumerkit päätellään kulman sijainnista yksikköympyrässä (kuva 7.26).




Kuva 7.26: Kosinin ja sinin arvojen päätteleminen yksikköympyrän ja muistikolmion avulla.

## 7.9 Binomiyhtälö

Tässä kappaleessa sovelletaan kompleksilukujen eksponenttiesitystä niin sanottujen binomiyhtälöiden ratkaisemiseen.

**Määritelmä 7.9.1.** Oletetaan, että $w \in \mathbb{C}$ ja $n \in \mathbb{N}$, $n \geq 1$. Muotoa

$$x^n = w$$

olevaa yhtälöä kutsutaan *binomiyhtälöksi.*

Esimerkiksi yhtälöt $x^5 = 1$ ja $z^4 = 2\sqrt{3} - 2i$ ovat binomiyhtälöitä. Huomaa, että binomiyhtälössä tuntematonta voidaan merkitä muullakin kirjaimella kuin kirjaimella $x$.

**Esimerkki 7.9.2.** Ratkaistaan kompleksilukujen joukossa yhtälö $x^5 = 1$.

Aloitetaan muodostamalla ekponenttiesitys vakiolle 1. Koska luvun 1 itseisarvo on 1 ja sen vaihekulmaksi voidaan valita 0, saadaan eksponenttiesitykseksi $1 = e^{0i}$. Muodostetaan eksponenttiesitys myös tuntemattomalle $x$ merkitsemällä $x = re^{i\varphi}$, missä $\varphi, r \in \mathbb{R}$ ja $r \geq 0$.

Tarkasteltava yhtälö voidaan eksponenttiesitysten avulla kirjoittaa muodossa

$$(re^{i\varphi})^5 = e^{0i}.$$

Kompleksilukujen laskusääntöjen avulla yhtälön vasenta puolta voidaan sieventää, jolloin yhtälö saadaan muotoon

$$r^5 e^{5i\varphi} = e^{0i}. \tag{5}$$

Tämä yhtälö toteutuu, jos ja vain jos siinä esiintyvillä kompleksiluvuilla $r^5 e^{5i\varphi}$ ja $e^{0i}$ on sama itseisarvo ja niiden vaihekulmien erotus on $k \cdot 2\pi$ jollakin $k \in \mathbb{Z}$. Vaihekulmien ei siis tarvitse olla samoja, vaan ne voivat erota toisistaan yhden tai useamman täyden kierroksen verran. Yhtälön (5) kanssa yhtäpitävä yhtälöpari on siten

$$\begin{cases} r^5 = 1 \\ 5\varphi - 0 = k \cdot 2\pi, \end{cases}$$

missä $k \in \mathbb{Z}$. Tässä yhtälöparissa tuntemattomat $r$ ja $\varphi$ ovat reaalilukuja ja lisäksi $r \geq 0$, joten yhtälöpari voidaan ratkaista tavallisia reaalilukujen laskusääntöjä käyttäen:

$$\begin{cases} r^5 = 1 \\ 5\varphi - 0 = k \cdot 2\pi \end{cases} \Leftrightarrow \begin{cases} r = \sqrt[5]{1} \\ 5\varphi = k \cdot 2\pi \end{cases} \Leftrightarrow \begin{cases} r = 1 \\ \varphi = k \cdot \frac{2}{5}\pi. \end{cases}$$

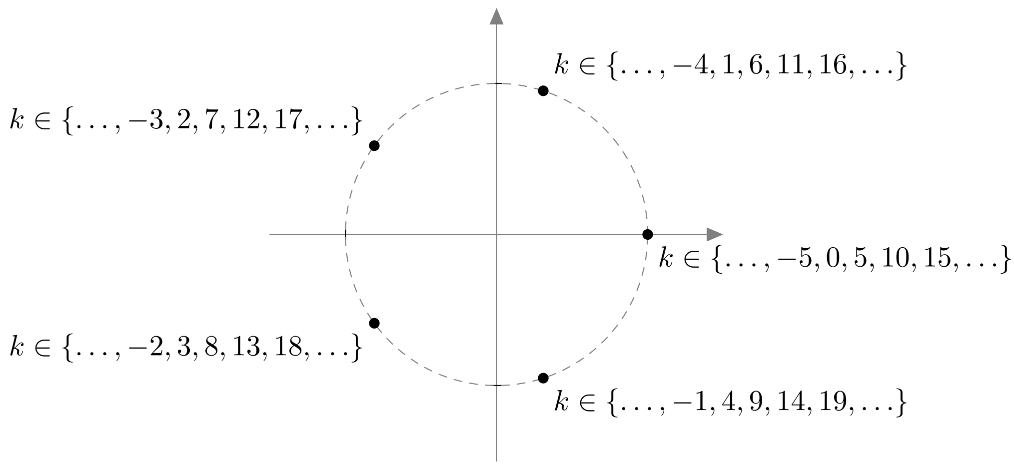
Yhtälöparin ratkaisut ovat siis

$$\begin{cases} r = 1 \\ \varphi = k \cdot \frac{2}{5}\pi, \end{cases}$$

missä $k \in \mathbb{Z}$. Havaitaan, että kaikkien ratkaisujen itseisarvo on 1, joten ne sijaitsevat kompleksitasossa yksikköympyrän kehällä. Eri ratkaisuja saadaan kaikkiaan viisi kappaletta:

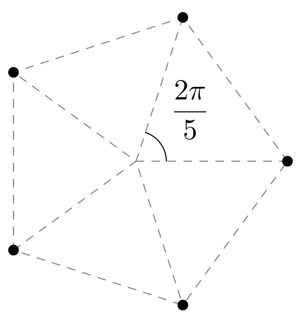
$$1, \quad e^{\frac{2}{5}\pi i}, \quad e^{\frac{4}{5}\pi i}, \quad e^{\frac{6}{5}\pi i}, \quad e^{\frac{8}{5}\pi i}.$$

Ne saadaan esimerkiksi tapauksissa, joissa $k \in \{0, 1, 2, 3, 4\}$. Muilla parametrin $k$ arvoilla saadut vaihekulmat tuottavat lopputulokseksi jonkin näistä samoista kompleksiluvuista. Tätä on havainnollistettu alla kuvassa 7.27.




Kuva 7.27: Yhtälön $x^5 = 1$ ratkaisut sijaitsevat kompleksitason yksikköympyrällä.

Yhtälön $x^5 = 1$ ratkaisut ovat nimeltään *viidennet ykkösen juuret*. Parametrin $k$ peräkkäisillä arvoilla saatujen ratkaisujen vaihekulmien ero on aina $2\pi/5$, joten viidennet ykkösen juuret ovat säännöllisen viisikulmion kärkipisteet. Tätä on havainnollistettu kuvassa 7.28.



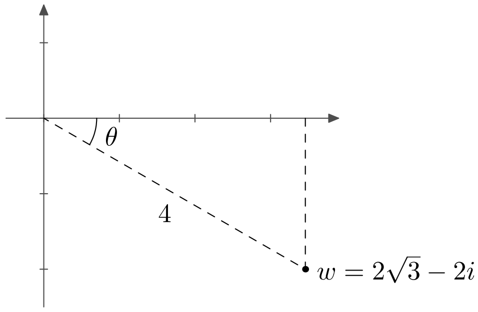

Kuva 7.28: Yhtälön $x^5 = 1$ ratkaisut muodostavat kompleksitasoon säännöllisen viisikulmion.

**Esimerkki 7.9.3.** Ratkaistaan kompleksilukujen joukossa yhtälö $z^4 = 2\sqrt{3} - 2i$.

Aloitetaan muodostamalla eksponenttiesitys vakiolle $2\sqrt{3} - 2i$. Sen itseisarvo on määritelmän mukaan

$$|2\sqrt{3} - 2i| = \sqrt{(2\sqrt{3})^2 + (-2)^2} = \sqrt{16} = 4.$$

Vaihekulma $\theta$ saadaan ratkaistua kuvan 7.29 suorakulmaisesta kolmiosta:




Kuva 7.29: Luku $w = 2\sqrt{3} - 2i$ kompleksitasossa.

Vakion $2\sqrt{3} - 2i$ eksponenttiesitykseksi saadaan näin $2\sqrt{3} - 2i = 4e^{-\frac{\pi}{6}i}$. Muodostetaan eksponenttiesitys myös tuntemattomalle $z$ merkitsemällä $z = re^{i\varphi}$, missä $\varphi$, $r \in \mathbb{R}$ ja $r \geq 0$.

Tarkasteltava yhtälö voidaan eksponenttiesitysten avulla kirjoittaa muodossa

$$(re^{i\varphi})^4 = 4e^{-\frac{\pi}{6}i}.$$

Kompleksilukujen laskusääntöjen avulla yhtälön vasenta puolta voidaan sieventää, jolloin yhtälö saadaan muotoon

$$r^4 e^{4i\varphi} = 4e^{-\frac{\pi}{6}i}. \tag{6}$$

Tämä yhtälö toteutuu, jos ja vain jos siinä esiintyvillä kompleksiluvuilla $r^4e^{4i\varphi}$ ja $4e^{-\frac{\pi}{6}i}$ on sama itseisarvo ja niiden vaihekulmien erotus on $k \cdot 2\pi$ jollakin $k \in \mathbb{Z}$. Vaihekulmien ei siis tarvitse olla samoja, vaan ne voivat erota toisistaan yhden tai useamman täyden kierroksen verran. Yhtälön (6) kanssa yhtäpitävä yhtälöpari on siten

$$\begin{cases} r^4 = 4 \\ 4\varphi - \left(-\dfrac{\pi}{6}\right) = k \cdot 2\pi, \end{cases}$$

missä $k \in \mathbb{Z}$. Ratkaistaan tästä yhtälöparista $r$ ja $\varphi$:

$$\begin{cases} r^4 = 4 \\ 4\varphi - \left(-\dfrac{\pi}{6}\right) = k \cdot 2\pi, \end{cases} \Leftrightarrow \begin{cases} r^2 = 2 \ \vee \ r^2 = -2 \\ 4\varphi = -\dfrac{\pi}{6} + k \cdot 2\pi \end{cases} \Leftrightarrow \begin{cases} r = \sqrt{2} \ \vee \ r = -\sqrt{2} \\ \varphi = -\dfrac{\pi}{24} + k \cdot \dfrac{\pi}{2}, \end{cases}$$

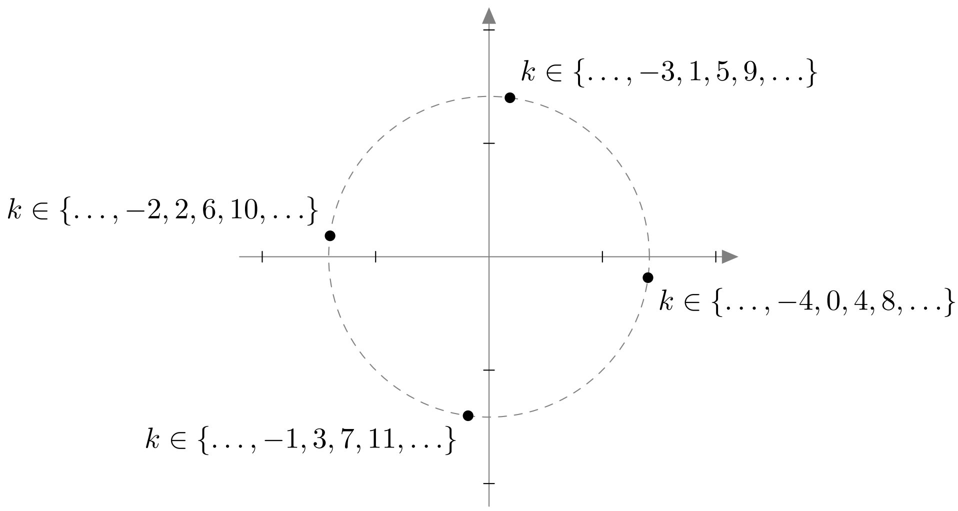
Huomaa, että vaihtoehto $r^2 = -2$ on aina epätosi eikä tuota ollenkaan ratkaisuja. Lisäksi oletuksen mukaan $r \geq 0$, joten ainoa mahdollinen vaihtoehto on $r = \sqrt{2}$. Ratkaisuiksi saadaan siis

$$\begin{cases} r = \sqrt{2} \\ \varphi = -\dfrac{\pi}{24} + k \cdot \dfrac{\pi}{2}, \end{cases}$$

missä $k \in \mathbb{Z}$. Havaitaan, että kaikkien ratkaisujen itseisarvo on $\sqrt{2}$, joten ne sijaitsevat kompleksitasossa origokeskisen $\sqrt{2}$-säteisen ympyrän kehällä. Eri ratkaisuja saadaan kaikkiaan neljä kappaletta:

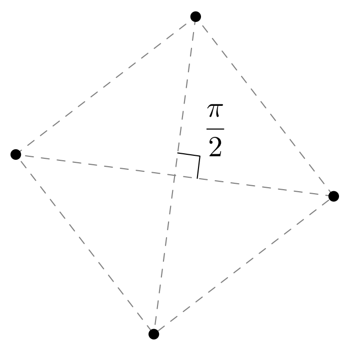
$$\sqrt{2}e^{-\frac{1}{24}\pi i}, \quad \sqrt{2}e^{\frac{11}{24}\pi i}, \quad \sqrt{2}e^{\frac{23}{24}\pi i}, \quad \sqrt{2}e^{\frac{35}{24}\pi i}.$$

Ne saadaan esimerkiksi tapauksissa, joissa $k \in \{0, 1, 2, 3\}$. Muilla parametrin $k$ arvoilla saadut vaihekulmat eroavat näistä jollain määrällä täysiä kierroksia ja tuottavat siis lopputulokseksi samat kompleksiluvut. Tätä on havainnollistettu alla kuvassa 7.30.




Kuva 7.30: Yhtälön $z^4 = 2\sqrt{3} - 2i$ ratkaisut sijaitsevat $\sqrt{2}$-säteisellä origokeskisellä ympyrällä.

Parametrin $k$ peräkkäisillä arvoilla saatujen ratkaisujen vaihekulmien ero on aina $\pi/2$, joten yhtälön $z^4 = 2\sqrt{3} - 2i$ ratkaisut ovat säännöllisen nelikulmion kärkipisteet. Tätä on havainnollistettu kuvassa 7.31.




Kuva 7.31: Yhtälön $z^4 = 2\sqrt{3} - 2i$ ratkaisut muodostavat kompleksitasoon neliön.

## 7.10 Toisen asteen yhtälö

**Esimerkki 7.10.1.** Tarkastellaan toisen asteen yhtälöä $x^2 = 25$. Yhtälöä muokkaamalla huomataan, että sillä on reaalilukujen joukossa kaksi ratkaisua:

$$x^2 = 25 \;\Leftrightarrow\; x^2 - 25 = 0 \;\Leftrightarrow\; x^2 - 5^2 = 0 \;\Leftrightarrow\; (x-5)(x+5) = 0$$

Tulon nollasäännön 7.4.7 mukaan viimeinen yhtälö toteutuu, jos ja vain jos $x - 5 = 0$ tai $x + 5 = 0$. Toisin sanottuna, jos ja vain jos $x = 5$ tai $x = -5$.

**Esimerkki 7.10.2.** Tarkastellaan toisen asteen yhtälöä $x^2 = -9$. Sillä ei ole ratkaisuja reaalilukujen joukossa, koska $x^2 \geq 0$ kaikilla $x \in \mathbb{R}$. Yhtälö $x^2 = -9$ voidaan kuitenkin kompleksilukujen joukossa ratkaista samaan tapaan kuin mikä tahansa binomiyhtälö:

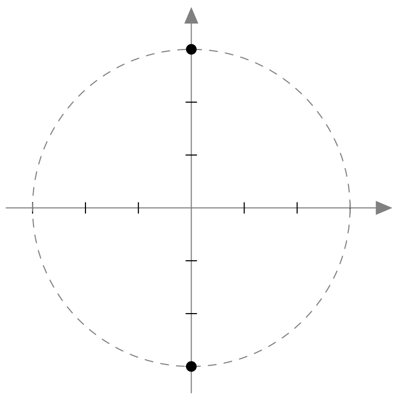
Eksponenttiesitysten avulla yhtälö $x^2 = -9$ voidaan kirjoittaa muodossa $(re^{i\varphi})^2 = 9e^{\pi i}$ eli muodossa $r^2e^{2i\varphi} = 9e^{\pi i}$. Tämä yhtälö toteutuu, jos ja vain jos siinä esiintyvillä kompleksiluvuilla $r^2e^{2i\varphi}$ ja $9e^{\pi i}$ on sama itseisarvo ja niiden vaihekulmien erotus on $k \cdot 2\pi$ jollakin $k \in \mathbb{Z}$. Tarkasteltavan yhtälön kanssa yhtäpitävä yhtälöpari on siten

$$\begin{cases} r^2 = 9 \\ 2\varphi - \pi = k \cdot 2\pi, \end{cases}$$

missä $k \in \mathbb{Z}$. Eksponenttiesityksessä itseisarvo $r \geq 0$, joten ratkaisuiksi saadaan

$$\begin{cases} r = 3 \\ \varphi = \dfrac{\pi}{2} + k \cdot \pi, \end{cases}$$

missä $k \in \mathbb{Z}$. Havaitaan, että yhtälöllä $x^2 = -9$ on kaksi eri ratkaisua: $3e^{\frac{\pi}{2}i} = 3i$ ja $3e^{\frac{3\pi}{2}i} = -3i$.



Kuva 7.32: Yhtälön $x^2 = -9$ ratkaisut $3i$ ja $-3i$ kompleksitasossa.

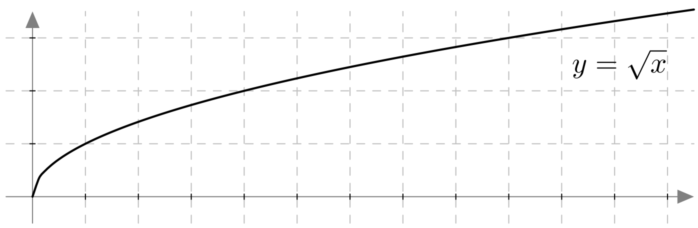
Toisen asteen yhtälöiden ratkaisemiseen liittyy myös neliöjuuren käsite, joka on määritelty epänegatiivisille reaaliluvuille:

**Määritelmä 7.10.3.** Oletetaan, että $a \in \mathbb{R}$ ja $a \geq 0$. Luvun $a$ *neliöjuuri* tarkoittaa reaalilukua $b$, jolla pätee:

$$b^2 = a \quad \text{ja} \quad b \geq 0.$$

Luvun $a$ neliöjuurta merkitään $\sqrt{a}$.

Määritelmän 7.10.3 mukaan luvun $a \geq 0$ neliöjuuri $\sqrt{a}$ on siis yhtälön $x^2 = a$ epänegatiivinen ratkaisu. Näin jokaiseen reaalilukuun $a \geq 0$ liitetään tasan yksi epänegatiivinen reaaliluku $\sqrt{a}$. Sääntö $x \mapsto \sqrt{x}$ on siis kuvaus $[0, \infty[ \to [0, \infty[$. Huomaa, että negatiivisen reaaliluvun neliöjuuri ei ole määritelty.




Kuva 7.33: Osa neliöjuurifunktion $x \mapsto \sqrt{x}$ kuvaajasta.

**Esimerkki 7.10.4.** Esimerkissä 7.10.1 saatiin yhtälön $x^2 = 25$ ratkaisuiksi 5 ja $-5$. Luvun 25 neliöjuuri on $\sqrt{25} = 5$, sillä $5^2 = 25$ ja $5 \geq 0$.

**Esimerkki 7.10.5.** Esimerkin 7.10.2 mukaan myös yhtälöllä $x^2 = -9$ on kaksi ratkaisua: $-3i$ ja $3i$. Negatiivisen luvun neliöjuuri ei kuitenkaan ole määritelty. Tutkitaan, mitä tapahtuisi, jos yritettäisiin määritellä $\sqrt{-9} = 3i$. Käyttämällä tavallisia laskusääntöjä saataisiin seuraava yhtälöketju:

$$9 = \sqrt{81} = \sqrt{(-9)(-9)} = \sqrt{-9}\sqrt{-9} = 3i \cdot 3i = 9i^2 = -9.$$

Vaihtoehtoinen määrittely $\sqrt{-9} = -3i$ johtaisi samanlaisiin ongelmiin:

$$9 = \sqrt{81} = \sqrt{(-9)(-9)} = \sqrt{-9}\sqrt{-9} = -3i \cdot (-3i) = 9i^2 = -9.$$

Havaitaan, että neliöjuuren laskusääntöä $\sqrt{ab} = \sqrt{a}\sqrt{b}$ ei voi käyttää, jos neliöjuuri yritetään määritellä negatiivisille reaaliluvuille.

Neliöjuuri voidaan määritellä negatiivisille reaaliluvuille ja yleisemmin kompleksiluvuille eksponenttiesityksen avulla asettamalla luvun $z = re^{i\varphi}$ neliöjuureksi $\sqrt{z} = \sqrt{r}e^{i\frac{\varphi}{2}}$. Tällöin joudutaan monikäsitteisyyden välttämiseksi rajoittamaan vaihekulma $\varphi$ esimerkiksi välille $[0, 2\pi[$ tai $]-\pi, \pi]$. Tuttuihin neliöjuuren laskusääntöihin ei kuitenkaan voi tällöin enää luottaa, kuten edellisistä yhtälöketjuista nähtiin.

Jatketaan toisen asteen yhtälöiden tutkimista.

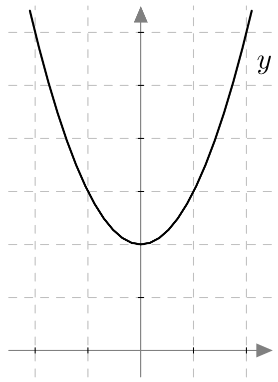
**Esimerkki 7.10.6.** Tarkastellaan yhtälöä $x^2 = -2$. Se voidaan ratkaista binomiyhtälönä samaan tapaan kuin esimerkissä 7.10.2. Käytetään nyt kuitenkin toista ratkaisutapaa, joka perustuu tulon nollasääntöön ja muistuttaa esimerkin 7.10.1 ratkaisua.

Muokataan yhtälö toiseen muotoon:

$$\begin{aligned} x^2 = -2 \;\Leftrightarrow\; x^2 = 2i^2 \;\Leftrightarrow\; x^2 - 2i^2 = 0 \;\Leftrightarrow\; x^2 - (i\sqrt{2})^2 = 0 \\ \Leftrightarrow\; (x - i\sqrt{2})(x + i\sqrt{2}) = 0 \end{aligned}$$

Kompleksilukujen tulon nollasäännön 7.4.7 mukaan viimeinen yhtälö toteutuu, jos ja vain jos $x - i\sqrt{2} = 0$ tai $x + i\sqrt{2} = 0$. Toisin sanottuna, jos ja vain jos $x = i\sqrt{2}$ tai $x = -i\sqrt{2}$.

Yhtälöllä $x^2 = -2$ eli yhtälöllä $x^2 + 2 = 0$ ei siis ole ratkaisuja reaalilukujen joukossa. Tämä merkitsee sitä, ettei yhtälön $y = x^2 + 2$ määrittelemä paraabeli kohtaa $x$-akselia. Tilannetta on havainnollistettu kuvassa 7.34.




Kuva 7.34: Yhtälöllä $x^2 + 2 = 0$ ei ole ratkaisuja reaalilukujen joukossa.

---

Esimerkin 7.10.6 tulos voidaan yleistää seuraavaksi lauseeksi:

**Lause 7.10.7.** *Oletetaan, että $r \in \mathbb{R}$ ja $r < 0$. Yhtälöllä $x^2 = r$ on kompeksilukujen joukossa tasan kaksi ratkaisua, jotka ovat $i\sqrt{|r|}$ ja $-i\sqrt{|r|}$.*

*Todistus.* Muokataan yhtälö $x^2 = r$ toiseen muotoon samaan tapaan kuin esimerkissä 7.10.6. Koska $r < 0$, pätee $r = -|r| = |r|\, i^2$.

$$\begin{aligned} x^2 = r \;\Leftrightarrow\; x^2 = |r|\, i^2 \;\Leftrightarrow\; x^2 - |r|\, i^2 = 0 \;\Leftrightarrow\; x^2 - \left(i\sqrt{|r|}\right)^2 = 0 \\ \Leftrightarrow\; \left(x - i\sqrt{|r|}\right)\left(x + i\sqrt{|r|}\right) = 0 \end{aligned}$$

Tulon nollasäännön 7.4.7 mukaan viimeinen yhtälö toteutuu, jos ja vain jos $x - i\sqrt{|r|} = 0$ tai $x + i\sqrt{|r|} = 0$. Toisin sanottuna, jos ja vain jos $x = i\sqrt{|r|}$ tai $x = -i\sqrt{|r|}$. $\square$

Yleisen toisen asteen yhtälön ratkaisemisessa tarvitaan niin sanottua neliöksi täydentämisen tekniikkaa, joka perustuu kaikilla reaali- ja kompleksiluvuilla pätevään yhtälöön

$$(a+b)^2 = a^2 + 2ab + b^2. \tag{7}$$

Neliöksi täydentämistä havainnollistetaan seuraavassa esimerkissä.

**Esimerkki 7.10.8.** Täydennetään neliöksi lauseke $x^2+x-6$. Muokataan lauseketta vaiheittain niin, että se muistuttaisi enemmän yhtälön (7) oikeaa puolta. Pidetään joka vaiheessa huolta, että yhtäsuuruus säilyy koko ajan:

$$x^2+x-6 = x^2 + 2\cdot\frac{1}{2}\cdot x - 6 = \underbrace{x^2 + 2\cdot\frac{1}{2}\cdot x + \left(\frac{1}{2}\right)^2}_{a=x \text{ ja } b=1/2} - \left(\frac{1}{2}\right)^2 - 6$$

Lausekkeeseen saatiin näkyviin yhtälön (7) oikeaa puolta muistuttava osa, joka voidaan kirjoittaa toiseen muotoon:

$$\underbrace{x^2 + 2\cdot\frac{1}{2}\cdot x + \left(\frac{1}{2}\right)^2}_{a=x \text{ ja } b=1/2} - \left(\frac{1}{2}\right)^2 - 6 = \underbrace{\left(x+\frac{1}{2}\right)^2}_{a=x \text{ ja } b=1/2} - \left(\frac{1}{2}\right)^2 - 6$$

Näin alkuperäinen lauseke saadaan muotoon

$$x^2+x-6 = \left(x+\frac{1}{2}\right)^2 - \frac{1}{4} - 6 = \left(x+\frac{1}{2}\right)^2 - \frac{25}{4}.$$

---

Tarkastellaan seuraavaksi yhtälöä $ax^2+bx+c=0$, jossa $a$, $b$, $c \in \mathbb{R}$ ja $a \neq 0$. Muokataan yhtälöä niin, että sen vasen puoli saadaan täydennettyä neliöksi:

$$\begin{aligned}
ax^2+bx+c=0 \;&\Leftrightarrow\; a^2x^2+abx+ac=0 \\
&\Leftrightarrow\; (ax)^2 + 2\cdot ax\cdot\frac{b}{2} = -ac \\
&\Leftrightarrow\; (ax)^2 + 2\cdot ax\cdot\frac{b}{2} + \left(\frac{b}{2}\right)^2 = -ac + \left(\frac{b}{2}\right)^2 \\
&\Leftrightarrow\; \left(ax+\frac{b}{2}\right)^2 = -\frac{4ac}{4} + \frac{b^2}{4} \\
&\Leftrightarrow\; \left(ax+\frac{b}{2}\right)^2 = \frac{b^2-4ac}{4} \qquad (*)
\end{aligned}$$

Havaitaan, että saadun yhtälön $(*)$ oikea puoli on epänegatiivinen, jos ja vain jos diskriminantti $b^2-4ac \geq 0$. Tässä tapauksessa ratkaisuiksi saadaan

$$ax+\frac{b}{2} = \pm\sqrt{\frac{b^2-4ac}{4}} = \pm\frac{\sqrt{b^2-4ac}}{2}$$

eli

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Jos yhtälön $(*)$ oikea puoli on negatiivinen eli diskriminantti $b^2 - 4ac < 0$, saadaan ratkaisuiksi lauseen 7.10.7 nojalla

$$ax + \frac{b}{2} = \pm i \sqrt{\left| \frac{b^2 - 4ac}{4} \right|} = \pm i \sqrt{\frac{|b^2 - 4ac|}{4}} = \pm i \frac{\sqrt{|b^2 - 4ac|}}{2}$$

eli

$$x = \frac{-b \pm i\sqrt{|b^2 - 4ac|}}{2a}.$$

---

Kootaan saadut tulokset seuraavaksi lauseeksi:

**Lause 7.10.9.** *Oletetaan, että $a$, $b$, $c \in \mathbb{R}$ ja $a \neq 0$. Yhtälön $ax^2 + bx + c = 0$ ratkaisut saadaan seuraavasti: Jos diskriminantti $b^2 - 4ac \geq 0$, yhtälön ratkaisut ovat*

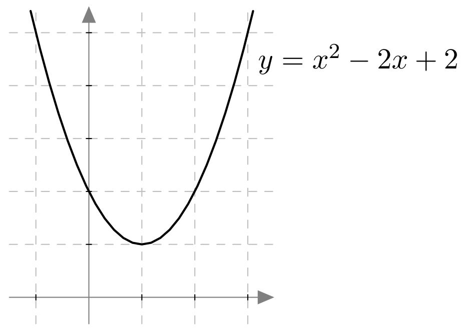
$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

*Jos diskriminantti $b^2 - 4ac < 0$, yhtälön ratkaisut ovat*

$$x = \frac{-b \pm i\sqrt{|b^2 - 4ac|}}{2a}.$$

**Esimerkki 7.10.10.** Ratkaistaan kompleksilukujen joukossa yhtälö $x^2 - 2x + 2 = 0$. Sen diskriminantti on negatiivinen: $b^2 - 4ac = (-2)^2 - 4 \cdot 1 \cdot 2 = 4 - 8 = -4$. Yhtälön ratkaisut ovat siten

$$x = \frac{-(-2) \pm i\sqrt{|(-2)^2 - 4 \cdot 1 \cdot 2|}}{2 \cdot 1} = \frac{2 \pm i\sqrt{|-4|}}{2} = \frac{2 \pm i\sqrt{4}}{2} = \frac{2 \pm 2i}{2} = 1 \pm i.$$

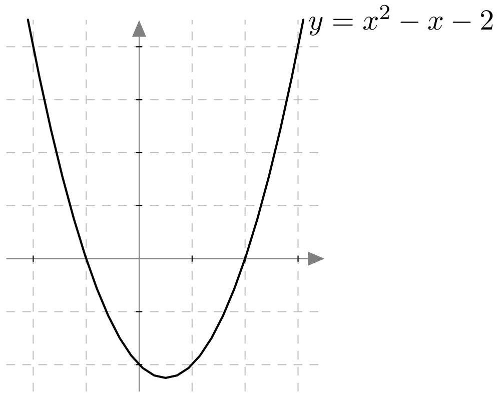



Kuva 7.35: Yhtälöllä $x^2 - 2x + 2 = 0$ ei ole ratkaisuja reaalilukujen joukossa.

**Esimerkki 7.10.11.** Ratkaistaan kompleksilukujen joukossa yhtälö $x^2 - x - 2 = 0$. Sen diskriminantti on positiivinen: $b^2 - 4ac = (-1)^2 - 4 \cdot 1 \cdot (-2) = 1 + 8 = 9$. Yhtälön ratkaisut ovat siten

$$x = \frac{-(-1) \pm \sqrt{(-1)^2 - 4 \cdot 1 \cdot (-2)}}{2 \cdot 1} = \frac{1 \pm \sqrt{9}}{2} = \frac{1 \pm 3}{2}.$$

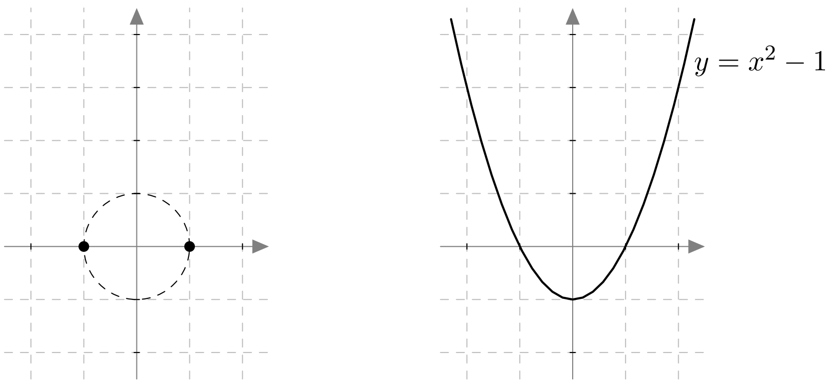
Ratkaisut ovat siis $x_1 = -1$ ja $x_2 = 2$. Tilannetta on havainnollistettu kuvassa 7.36.




Kuva 7.36: Yhtälön $x^2 - x - 2 = 0$ ratkaisut ovat $x_1 = -1$ ja $x_2 = 2$.

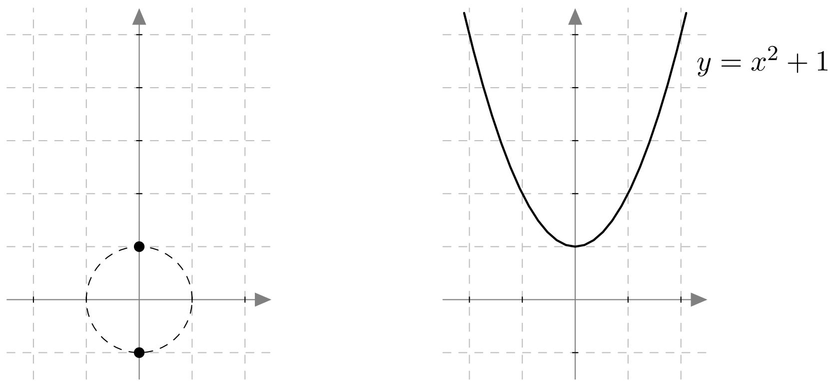
Seuraavissa esimerkeissä havainnollistetaan erityyppisiä toisen asteen yhtälöitä ja niiden ratkaisuja.

**Esimerkki 7.10.12.** Yhtälö $x^2 = 1$ toteutuu, jos ja vain jos $x = 1$ tai $x = -1$. Kyseinen yhtälö voidaan kirjoittaa myös muodossa $x^2 - 1 = 0$, joten sen ratkaisut ovat polynomifunktion $x \mapsto x^2 - 1$ nollakohdat. Alla olevassa kuvassa 7.37 on havainnollistettu yhtälön ratkaisuja kompleksitasossa.




Kuva 7.37: Yhtälön $x^2 = 1$ ratkaisut ovat funktion $x \mapsto x^2 - 1$ nollakohdat.

**Esimerkki 7.10.13.** Yhtälö $x^2 = -1$ toteutuu, jos ja vain jos $x = i$ tai $x = -i$. Alla olevassa kuvassa 7.38 on havainnollistettu yhtälön ratkaisuja kompleksitasossa. Ratkaisut eivät ole reaalisia, mikä nähdään myös siitä, ettei vastaavalla polynomifunktiolla $x \mapsto x^2 + 1$ ole nollakohtia.

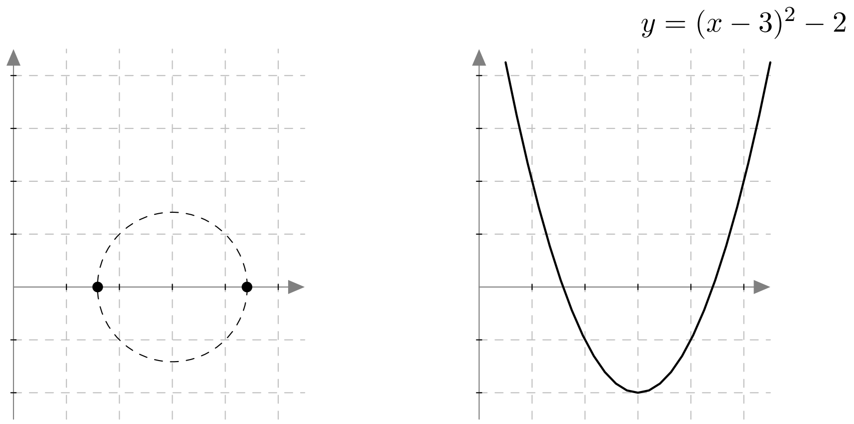



Kuva 7.38: Yhtälöllä $x^2 = -1$ ei ole ratkaisuja reaalilukujen joukossa.

**Esimerkki 7.10.14.** Ratkaistaan yhtälö $(x-3)^2 = 2$:

$$(x-3)^2 = 2 \;\Leftrightarrow\; x - 3 = \pm\sqrt{2} \;\Leftrightarrow\; x = 3 \pm \sqrt{2}.$$

Kuvassa 7.40 on havainnollistettu yhtälön ratkaisuja kompleksitasossa. Havaitaan, että ratkaisut sijaitsevat kompleksitasossa ympyrällä, jonka keskipiste on $(3, 0)$ ja säde on $\sqrt{2}$.

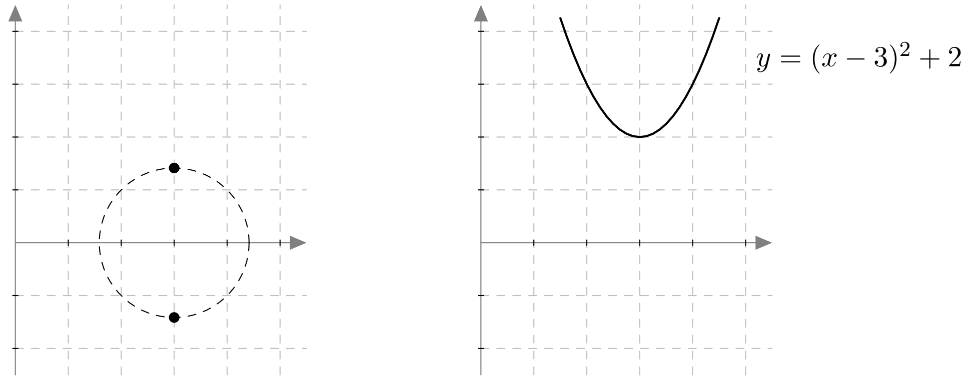



Kuva 7.39: Yhtälön $(x-3)^2 = 2$ ratkaisut ovat funktion $x \mapsto (x-3)^2 - 2$ nollakohdat.

**Esimerkki 7.10.15.** Ratkaistaan yhtälö $(x-3)^2 = -2$:

$$(x-3)^2 = -2 \;\Leftrightarrow\; x-3 = \pm i\sqrt{2} \;\Leftrightarrow\; x = 3 \pm i\sqrt{2}.$$

Kuvassa 7.39 on havainnollistettu yhtälön ratkaisuja kompleksitasossa. Havaitaan, että ratkaisut sijaitsevat kompleksitasossa ympyrällä, jonka keskipiste on $(3,0)$ ja säde on $\sqrt{2} = \sqrt{|-2|}$.




Kuva 7.40: Yhtälöllä $(x-3)^2 = -2$ ei ole ratkaisuja reaalilukujen joukossa.

**Esimerkki 7.10.16.** Tarkastellaan yhtälöä $(x-(3+4i))^2 = 2i$. Se voidaan kirjoittaa myös muodossa $x^2 - (6+8i)x + 22i - 7 = 0$. Kysymyksessä on siis kompleksikertoiminen toisen asteen yhtälö. Sen ratkaisemiseksi etsitään aluksi ne kompleksiluvut $z$, joilla $z^2 = 2i$.

Binomiyhtälö $z^2 = 2i$ voidaan ratkaista merkitsemällä $z = re^{i\varphi}$, missä $r$, $\varphi \in \mathbb{R}$ ja $r \geq 0$, ja käyttämällä myös vakiolle eksponenttiesitystä $2i = 2e^{i\cdot\pi/2}$. Tällöin

$$\begin{aligned} z^2 = 2i \;\Leftrightarrow\; r^2 e^{i\cdot 2\varphi} = 2e^{i\cdot\pi/2} &\;\Leftrightarrow\; r = \pm\sqrt{2} \;\wedge\; 2\varphi = \pi/2 + n\cdot 2\pi \\ &\;\Leftrightarrow\; r = \pm\sqrt{2} \;\wedge\; \varphi = \pi/4 + n\cdot\pi, \end{aligned}$$

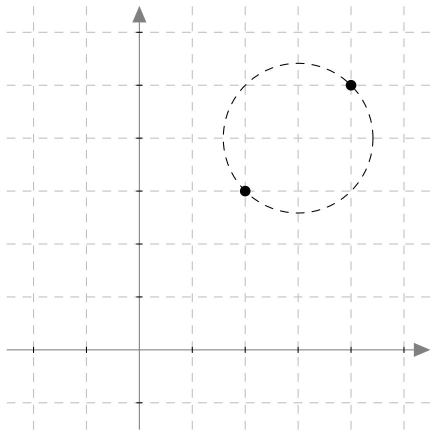
missä $n \in \mathbb{Z}$. Erilaisia ratkaisuja saadaan kaksi:

$$\begin{aligned} z_1 &= \sqrt{2}e^{i\cdot\pi/4} = 1 + i \\ z_2 &= \sqrt{2}e^{i\cdot 5\pi/4} = -1 - i. \end{aligned}$$

Alkuperäinen yhtälö $(x-(3+4i))^2 = 2i$ saadaan nyt ratkaistua:

$$(x-(3+4i))^2 = 2i \;\Leftrightarrow\; x-(3+4i) = \pm(1+i) \;\Leftrightarrow\; x = 4+5i \;\vee\; x = 2+3i.$$

Kuvasta 7.41 havaitaan, että ratkaisut sijaitsevat kompleksitasossa ympyrällä, jonka keskipiste on $3+4i$ ja säde on $\sqrt{2} = \sqrt{|2i|}$.



Kuva 7.41: Yhtälön $(x-(3+4i))^2 = 2i$ ratkaisut kompleksitasossa.

**Esimerkki 7.10.17.** Tarkastellaan kompleksikertoimista toisen asteen yhtälöä

$$x^2 - (2+4i)x + 8i - 6 = 0.$$

Muokataan yhtälöä niin, että sen vasen puoli saadaan täydennettyä neliöksi:

$$\begin{aligned}
x^2 - (2+4i)x + 8i - 6 = 0 \;&\Leftrightarrow\; x^2 - 2(1+2i)x + (1+2i)^2 - (1+2i)^2 + 8i - 6 = 0 \\
&\Leftrightarrow\; x^2 - 2(1+2i)x + (1+2i)^2 = (1+2i)^2 - 8i + 6 \\
&\Leftrightarrow\; (x-(1+2i))^2 = (1+2i)^2 - 8i + 6 \\
&\Leftrightarrow\; (x-(1+2i))^2 = 1 + 4i - 4 - 8i + 6 \\
&\Leftrightarrow\; (x-(1+2i))^2 = 3 - 4i.
\end{aligned}$$

Ratkaistaan seuraavaksi yhtälö $z^2 = 3-4i$. Merkitään $z = a+bi$, missä $a$, $b \in \mathbb{R}$. Tällöin

$$z^2 = 3-4i \;\Leftrightarrow\; (a+bi)^2 = 3-4i \;\Leftrightarrow\; a^2 + 2abi - b^2 = 3-4i.$$

Vertaamalla reaaliosia keskenään ja imaginaariosia keskenään saadaan tämän yhtälön kanssa yhtäpitävä yhtälöpari, josta voidaan ratkaista $a$ ja $b$:

$$\begin{cases} a^2 - b^2 = 3 \\ \quad 2ab = -4 \end{cases} \Leftrightarrow \begin{cases} a^2 - b^2 = 3 \\ \quad b = -\dfrac{2}{a} \end{cases} \Leftrightarrow \begin{cases} a^2 - \dfrac{4}{a^2} = 3 \\ \quad b = -\dfrac{2}{a} \end{cases} \Leftrightarrow \begin{cases} a^4 - 3a^2 - 4 = 0 \\ \quad b = -\dfrac{2}{a} \end{cases}$$

Yhtälöä $a^4 - 3a^2 - 4 = 0$ voidaan ajatella toisen asteen yhtälönä, jossa tuntematon on $a^2$. Näin saadaan

$$a^2 = \frac{-(-3) \pm \sqrt{(-3)^2 - 4\cdot 1 \cdot (-4)}}{2\cdot 1} = \frac{3 \pm \sqrt{25}}{2} = \frac{3 \pm 5}{2}.$$

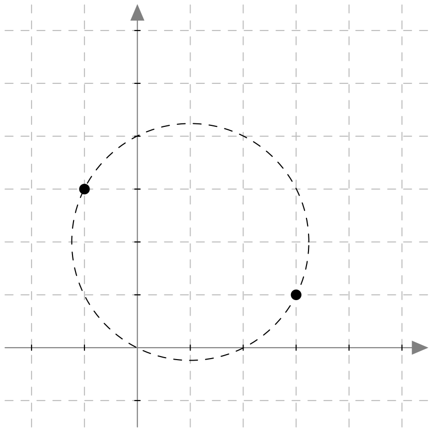
Koska $a \in \mathbb{R}$, sen toinen potenssi ei voi olla negatiivinen, ja siten ainoaksi ratkaisuksi saadaan $a^2 = 4$. Näin $a = \pm 2$ ja siten $b = -2/a = \mp 1$. Siis

$$z^2 = 3-4i \;\Leftrightarrow\; z = \pm(2-i).$$

Alkuperäinen yhtälö $(x - (1 + 2i))^2 = 3 - 4i$ saadaan nyt ratkaistua:

$$(x - (1 + 2i))^2 = 3 - 4i \iff x - (1 + 2i) = \pm(2 - i) \iff x = 3 + i \lor x = -1 + 3i.$$

Kuvasta 7.42 havaitaan, että ratkaisut sijaitsevat kompleksitasossa ympyrällä, jonka keskipiste on $1 + 2i$ ja säde on $\sqrt{5} = \sqrt{|3 - 4i|}$.



Kuva 7.42: Yhtälön $(x - (1 + 2i))^2 = 3 - 4i$ ratkaisut kompleksitasossa.

# 8 Tietojenkäsittelytieteen ja tilastotieteen työkaluja

## 8.1 Binomikertoimet ja kertoma

**Määritelmä 8.1.1.** Oletetaan, että $n$, $k \in \mathbb{N}$. *Binomikerroin*

$$\binom{n}{k}$$

ilmaisee, kuinka monta $k$-alkioista osajoukkoa on sellaisella joukolla, jossa on $n$ alkiota.

Merkintä $\binom{n}{k}$ luetaan ”$n$ yli $k$”. Laskimesta sen saa nappulasta `nCr`.

**Esimerkki 8.1.2.** Tarkastellaan joukkoa $\{1, 2, 3\}$, jossa on kolme alkiota. Sillä on seuraavat osajoukot: tyhjä joukko $\emptyset$, yksiöt $\{1\}$, $\{2\}$, $\{3\}$, kaksiot $\{2, 3\}$, $\{1, 3\}$, $\{1, 2\}$ ja joukko itse $\{1, 2, 3\}$. Laskemalla erikokoisten osajoukkojen lukumäärät saadaan selville seuraavat binomikertoimet:

$$\binom{3}{0} = 1, \quad \binom{3}{1} = 3, \quad \binom{3}{2} = 3, \quad \binom{3}{3} = 1.$$

Joukolla $\{1, 2, 3\}$ ei ole yhtään sellaista osajoukkoa, jonka alkioiden määrä on suurempi kuin kolme. Siten

$$\binom{3}{k} = 0$$

kaikilla luonnollisilla luvuilla $k \geq 4$.

**Esimerkki 8.1.3.** Oletetaan, että $n \in \mathbb{N} \setminus \{0\}$ ja merkitään $X = \{k \in \mathbb{N} \mid 1 \leq k \leq n\}$. Havaitaan, että joukon $X$ muodostavat luonnolliset luvut $1, \ldots, n$, joten joukon $X$ alkioiden lukumäärä on $n$.

Joukon $X$ ainoa nolla-alkioinen osajoukko on $\emptyset$. Yksialkioisia osajoukkoja joukolla $X$ on $n$ kappaletta, nimittäin yksiöt $\{1\}, \ldots, \{n\}$. Niiden komplementit $X \setminus \{1\}, \ldots, X \setminus \{n\}$ ovat puolestaan joukon $X$ $(n-1)$-alkioiset osajoukot. Niitä on siis yhtä paljon kuin yksialkioisia osajoukkoja, eli $n$ kappaletta. Sellaisia osajoukkoja, joissa on $n$ alkiota, joukolla $X$ on vain yksi, nimittäin joukko $X$ itse.

Näin saadaan pääteltyä seuraavat binomikertoimet:

$$\binom{n}{0} = 1, \quad \binom{n}{1} = n, \quad \binom{n}{n-1} = n, \quad \binom{n}{n} = 1.$$

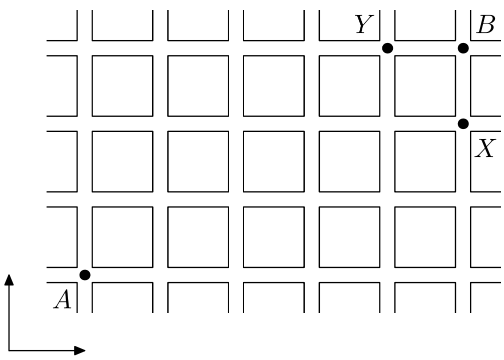
---

Pieniä binomikertoimia voi laskea niin sanotun *Pascalin kolmion* avulla (kuva 8.1). Se perustuu myöhemmin todistettavaan Pascalin identiteettiin (lause 8.1.5).

$$
\begin{array}{ccccccccc}
 & & & & \binom{0}{0} & & & & \\
 & & & \binom{1}{0} & & \binom{1}{1} & & & \\
 & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & \\
 & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & \\
\binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} \\
 & & & & \vdots & & & &
\end{array}
\qquad
\begin{array}{ccccccccc}
 & & & & 1 & & & & \\
 & & & 1 & & 1 & & & \\
 & & & & \searrow\ \swarrow & & & & \\
 & & 1 & & 2 & & 1 & & \\
 & & & \searrow\ \swarrow & & \searrow\ \swarrow & & & \\
 & 1 & & 3 & & 3 & & 1 & \\
 & & \searrow\ \swarrow & & \searrow\ \swarrow & & \searrow\ \swarrow & & \\
1 & & 4 & & 6 & & 4 & & 1 \\
 & & & & \vdots & & & &
\end{array}
$$

Kuva 8.1: Pascalin kolmiosta voidaan lukea binomikertoimien arvoja.

**Esimerkki 8.1.4.** Tarkastellaan erilaisia reittejä pisteestä $A$ pisteeseen $B$ kuvassa 8.2. Sallitaan vain sellaiset reitit, joissa jokaisella askeleella liikutaan joko yksi askel oikealle tai yksi askel ylöspäin, siis nuolten osoittamiin suuntiin. Jokainen tällainen reitti voidaan kuvata bittijonona, jossa 0 tarkoittaa askelta oikealle ja 1 tarkoittaa askelta ylös. Esimerkiksi reittiä, jossa liikutaan ensin pisteestä $A$ viisi askelta oikealle ja sen jälkeen kolme askelta ylös pisteeseen $B$, vastaa jono 0000 0111. Yksi askel tarkoittaa yhden ruudun sivun mittaista siirtymistä.




Kuva 8.2: Sallitut reitit pisteestä $A$ pisteeseen $B$ voidaan kuvata kahdeksan bitin jonoina.

Huomataan, että jokainen sallittu reitti muodostuu kahdeksasta askeleesta, joista kolmen askeleen pitää suuntautua ylöspäin. Jokaista sallittua reittiä vastaa siis täsmälleen yksi kahdeksan bitin jono, jossa on kolme ykköstä.

Kolme ykköstä sisältävä kahdeksan bitin jono voidaan muodostaa valitsemalla kahdeksan mahdollisen paikan joukosta ne paikat, joihin ykköset tulevat. Valitsemalla ykkösten paikoiksi esimerkiksi 3, 5 ja 6 saadaan jono 0010 1100. Kaikkien mahdollisten paikkojen joukosta $\{1, 2, 3, 4, 5, 6, 7, 8\}$ valittiin siis ykkösten paikoiksi osajoukko $\{3, 5, 6\}$.

Havaitaan, että kolme ykköstä sisältäviä kahdeksan bitin jonoja on yhtä monta kuin kahdeksan alkion joukolla on 3-alkioisia osajoukkoja, siis

$$\binom{8}{3}.$$

Tämä on siis myös erilaisten sallittujen reittien lukumäärä pisteestä $A$ pisteeseen $B$.

---

Edellisen esimerkin päättelyä soveltamalla voidaan todistaa niin sanottu Pascalin identiteetti, johon kuvassa 8.1 havainnollistettu Pascalin kolmio perustuu.

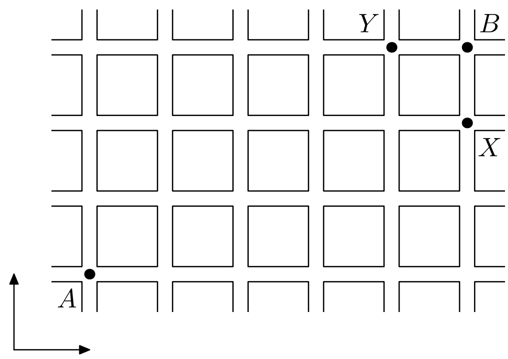
**Lause 8.1.5** (Pascalin identiteetti)**.** *Oletetaan, että* $n$, $k \in \mathbb{N}$ *ja* $0 < k < n$. *Tällöin*

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

*Todistus.* Tarkastellaan erilaisia reittejä pisteestä $A$ pisteeseen $B$. Sallitaan vain sellaiset reitit, joissa jokaisella askeleella liikutaan joko yksi askel oikealle tai yksi askel ylöspäin, siis nuolten osoittamiin suuntiin kuvassa 8.3. Oletetaan, että reitti pisteestä $A$ pisteeseen $B$ muodostuu yhteensä $n$ askeleesta, joista $n - k$ suuntautuu oikealle ja $k$ ylöspäin. Samaan tapaan kuin esimerkissä 8.1.4 voidaan päätellä, että tällaisten reittien lukumäärä on

$$\binom{n}{k}.$$

Huomataan, että jokainen näistä reiteistä kulkee joko pisteen $X$ tai pisteen $Y$ kautta, sillä reitin viimeisenkin askeleen pitää suuntautua ylöspäin tai oikealle.




Kuva 8.3: Jokainen sallittu reitti pisteestä $A$ pisteeseen $B$ kulkee joko pisteen $X$ tai $Y$ kautta.

Reitit pisteestä $A$ pisteeseen $X$ muodostuvat $n-1$ askeleesta, joista $k-1$ kappaletta suuntautuu ylöspäin. Niiden lukumäärä on

$$\binom{n-1}{k-1}.$$

Reitit pisteestä $A$ pisteeseen $Y$ muodotuvat $n-1$ askeleesta, joista $k$ kappaletta suuntautuu ylöspäin. Niiden lukumäärä on

$$\binom{n-1}{k}.$$

Kutakin reittiä voidaan jatkaa vain yhdessä tavalla pisteestä $X$ pisteeseen $B$. Tämä pätee myös pisteen $Y$ tapauksessa. Pisteestä $A$ pisteeseen $B$ kulkevien sallittujen reittien kokonaismääräksi saadaan siten pisteen $X$ kautta kulkevien ja pisteen $Y$ kautta kulkevien reittien lukumäärien summa

$$\binom{n-1}{k-1} + \binom{n-1}{k}.$$

Pisteestä $A$ pisteeseen $B$ kulkevien sallittujen reittien lukumäärä on nyt laskettu kahdella eri tavalla, ja yhdistämällä saadut tulokset voidaan päätellä, että

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}. \qquad \square$$

---

Seuraavaksi tavoitteena on johtaa kaava binomikertoimien laskemiseksi ilman Pascalin kolmiota. Siihen tarvitaan alla määriteltävää kertoman käsitettä.

**Määritelmä 8.1.6.** Määritellään luonnollisen luvun $n$ *kertoma* $n!$ asettamalla $0! = 1$ ja

$$(n+1)! = (n+1)n!$$

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

**Esimerkki 8.1.7.** Kertoman määritelmän mukaan $0! = 1$ ja

$$1! = 1 \cdot 0! = 1 \cdot 1 = 1$$

$$2! = 2 \cdot 1! = 2 \cdot 1 = 2$$

$$3! = 3 \cdot 2! = 3 \cdot 2 = 6$$

$$4! = 4 \cdot 3! = 4 \cdot 6 = 24$$

**Lause 8.1.8.** *Oletetaan, että $n \in \mathbb{N}$ ja $n \geq 1$. Luvun $n$ kertoma on luonnollisten lukujen $1, \ldots, n$ tulo; toisin sanottuna*

$$n! = 1 \cdots n.$$

*Todistus.* Induktiolla; jätetään harjoitustehtäväksi. □

**Lause 8.1.9.** *Oletetaan, että $n$, $k \in \mathbb{N}$ ja $k \leq n$. Tällöin*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

*Todistus.* Todistetaan väite induktiolla luvun $n$ suhteen.

Alkuaskel: Oletetaan, että $n = 0$. Koska $k \in \mathbb{N}$ ja $k \leq n$, niin $k = 0$. Yhtälön vasemmaksi puoleksi saadaan siis

$$\binom{n}{k} = \binom{0}{0} = 1.$$

Tässä käytettiin tietoa, että tyhjällä joukolla on vain yksi nolla-alkioinen osajoukko, nimittäin tyhjä joukko itse. Yhtälön oikeaksi puoleksi saadaan määritelmää 8.1.6 käyttäen

$$\frac{n!}{k!(n-k)!} = \frac{0!}{0!0!} = \frac{1}{1 \cdot 1} = 1.$$

Yhtälön vasen ja oikea puoli ovat yhtä suuret, joten yhtälö pätee.

Induktioaskel: Aloitetaan tekemällä induktio-oletus. Oletetaan, että $n \in \mathbb{N}$ ja että kaikilla luonnollisilla luvuilla $k \leq n$ pätee

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Seuraavaksi tavoitteena on näyttää induktio-oletuksen avulla, että kaikilla luonnollisilla luvuilla $\ell \leq n+1$ pätee vastaavasti

$$\binom{n+1}{\ell} = \frac{(n+1)!}{\ell!(n+1-\ell)!}. \tag{IV}$$

Oletetaan, että $\ell \in \mathbb{N}$ ja $\ell \leq n+1$. Jos $\ell = 0$, niin yhtälö (IV) on voimassa, sillä

$$\binom{n+1}{0} = 1 = \frac{(n+1)!}{(n+1)!} = \frac{(n+1)!}{0!(n+1-0)!}.$$

Tässä käytettiin tietoa, että $(n+1)$-alkioisella joukolla on vain yksi nolla-alkioinen osajoukko, nimittäin tyhjä joukko $\emptyset$.

Jos $\ell = n+1$, niin yhtälö (IV) on voimassa, sillä

$$\binom{n+1}{n+1} = 1 = \frac{(n+1)!}{(n+1)!} = \frac{(n+1)!}{(n+1)!0!}.$$

Tässä käytettiin tietoa, että $(n+1)$-alkioisella joukolla on vain yksi $(n+1)$-alkioinen osajoukko, nimittäin joukko itse.

Tarkastellaan lopuksi tapausta, jossa luvulle $\ell \in \mathbb{N}$ pätee $0 < \ell < n+1$ eli $1 \leq \ell \leq n$. Tällöin voidaan käyttää Pascalin identiteettiä (lause 8.1.5), jonka mukaan

$$\binom{n+1}{\ell} = \binom{n}{\ell-1} + \binom{n}{\ell} \tag{8}$$

Epäyhtälöistä $1 \leq \ell \leq n$ seuraa, että $0 \leq \ell - 1 \leq n-1$. Kumpaankin yhteenlaskettavaan voidaan siten käyttää induktio-oletusta, jolloin saadaan

$$\begin{aligned}\binom{n}{\ell-1} + \binom{n}{\ell} &= \frac{n!}{(\ell-1)!(n-(\ell-1))!} + \frac{n!}{\ell!(n-\ell)!} \\ &= \frac{n!}{(\ell-1)!(n-\ell+1)!} + \frac{n!}{\ell!(n-\ell)!}\end{aligned} \tag{9}$$

Laventamalla ensimmäistä murtolauseketta luvulla $\ell$ ja toista luvulla $n - \ell + 1$ saadaan yhteenlaskettavat samannimisiksi ja summa voidaan sieventää ottamalla yhteinen tekijä:

$$\begin{aligned}\frac{\ell \cdot n!}{\ell!(n-\ell+1)!} + \frac{(n-\ell+1)\cdot n!}{\ell!(n-\ell+1)!} &= \frac{n!}{\ell!(n+1-\ell)!}(\ell + n - \ell + 1) \\ &= \frac{n!}{\ell!(n+1-\ell)!}(n+1) \\ &= \frac{(n+1)!}{\ell!(n+1-\ell)!}\end{aligned} \tag{10}$$

Yhdistämällä yhtälöt (8), (9) ja (10) saadaan haluttu yhtälö (IV):

$$\binom{n+1}{\ell} = \frac{(n+1)!}{\ell!(n+1-\ell)!}$$

Johtopäätös: Alkuaskeleesta ja induktioaskeleesta seuraa induktioperiaatteen nojalla, että kaikilla $n \in \mathbb{N}$ pätee: jos $k \in \mathbb{N}$ ja $k \leq n$, niin

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

□

**Esimerkki 8.1.10.** Esimerkissä 8.1.4 pisteestä $A$ pisteeseen $B$ johtavien sallittujen reittien lukumääräksi saatiin

$$\binom{8}{3}.$$

Lauseen 8.1.9 avulla voidaan nyt laskea, että

$$\binom{8}{3} = \frac{8!}{3!(8-3)!} = \frac{8!}{3!5!} = \frac{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8}{1 \cdot 2 \cdot 3 \cdot 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5} = \frac{6 \cdot 7 \cdot 8}{2 \cdot 3} = 7 \cdot 8 = 56.$$

**Esimerkki 8.1.11.** Matemaattis-luonnontieteellisen tiedekunnan tiedekuntaneuvostossa on 19 jäsentä. Kuinka monella tavalla tiedekuntaneuvoston jäsenistä voidaan muodostaa kuusihenkinen toimikunta?

Kuusihenkinen toimikunta muodostetaan valitsemalla 19 jäsenen joukosta kuusi jäsentä, joten erilaisten vaihtoehtojen määrä on

$$\binom{19}{6} = \frac{19!}{6!(19-6)!} = \frac{19!}{6!13!} = \frac{14 \cdot 15 \cdot 16 \cdot 17 \cdot 18 \cdot 19}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6} = 7 \cdot 4 \cdot 17 \cdot 3 \cdot 19 = 27\,132.$$

**Esimerkki 8.1.12.** Tiedekuntaneuvoston 19 jäsenestä viisi on opiskelijoita. Kuinka monella tavalla tiedekuntaneuvoston jäsenistä voidaan muodostaa kuusihenkinen toimikunta, jos siinä saa olla enintään kaksi opiskelijaa?

Kysymyksen tilanteessa mahdollisia ovat toimikunnat, joissa ei ole yhtään opiskelijaa, sekä toimikunnat, joissa on yksi tai kaksi opiskelijaa. Tarkastellaan nämä eri vaihtoehdot erikseen.

Toimikunta, jossa ei ole yhtään opiskelijaa, voidaan muodostaa valitsemalla kaikki kuusi jäsentä 13 henkilökunnan edustajan joukosta. Erilaisia vaihtoehtoja on siten

$$\binom{13}{6} = \frac{13!}{6!7!} = \frac{8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6} = 3 \cdot 2 \cdot 11 \cdot 2 \cdot 13 = 1\,716.$$

Toimikunta, jossa on tasan yksi opiskelija, voidaan muodostaa valitsemalla ensin yksi jäsen viiden opiskelijan joukosta ja valitsemalla sen jälkeen loput viisi toimikunnan jäsentä 13 henkilökunnan edustajan joukosta. Erilaisia vaihtoehtoja on

$$\binom{5}{1} \cdot \binom{13}{5} = 5 \cdot \frac{13!}{5!8!} = 5 \cdot 1\,287 = 6\,435.$$

Toimikunta, jossa on tasan kaksi opiskelijaa, voidaan muodostaa valitsemalla ensin kaksi jäsentä viiden opiskelijan joukosta ja sen jälkeen loput neljä toimikunnan jäsentä 13 henkilökunnan edustajan joukosta. Erilaisia vaihtoehtoja on siten

$$\binom{5}{2} \cdot \binom{13}{4} = \frac{5!}{2!3!} \cdot \frac{13!}{4!9!} = 10 \cdot 715 = 7\,150.$$

Sellaisten toimikuntien lukumäärä, joissa on enintään kaksi opiskelijajäsentä, saadaan nyt laskemalla yhteen niiden toimikuntien määrät, joissa on 0, 1 tai 2 opiskelijajäsentä. Erilaisia vaihtoehtoja on yhteensä

$$\binom{13}{6} + \binom{5}{1} \cdot \binom{13}{5} + \binom{5}{2} \cdot \binom{13}{4} = 1\,716 + 6\,435 + 7\,150 = 15\,301.$$

**Lause 8.1.13.** *Oletetaan, että $a$, $b \in \mathbb{R}$. Tällöin kaikilla $n \in \mathbb{N}$, $n \geq 1$ pätee*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

Lause 8.1.13 on mahdollista todistaa induktiolla käyttäen apuna Pascalin identiteettiä (lause 8.1.5), mutta tällä kertaa todistus sivuutetaan.

**Esimerkki 8.1.14.** Poistetaan sulut polynomista $(x-2)^4$. Lauseen 8.1.13 mukaan

$$\begin{aligned}
(x-2)^4 &= \sum_{k=0}^{4} \binom{4}{k} x^{4-k} \cdot (-2)^k \\
&= \binom{4}{0} x^4 \cdot (-2)^0 + \binom{4}{1} x^3 \cdot (-2)^1 + \binom{4}{2} x^2 \cdot (-2)^2 + \binom{4}{3} x^1 \cdot (-2)^3 + \binom{4}{4} x^0 \cdot (-2)^4 \\
&= x^4 - 8x^3 + 24x^2 - 32x + 16
\end{aligned}$$

**Esimerkki 8.1.15.** Määritetään termin $x^{15}$ kerroin polynomissa $(4+2x)^{18}$.

Lauseen 8.1.13 mukaan kyseinen termi on

$$\begin{aligned}
\binom{18}{15} 4^{18-15} (2x)^{15} &= \frac{18!}{15!3!} \cdot 4^3 \cdot 2^{15} \cdot x^{15} = \frac{18 \cdot 17 \cdot 16}{3 \cdot 2 \cdot 1} \cdot 64 \cdot 32\,768 \cdot x^{15} \\
&= 3 \cdot 17 \cdot 16 \cdot 2\,097\,152 \cdot x^{15} = 1\,711\,276\,032\, x^{15},
\end{aligned}$$

joten kysytty kerroin on 1 711 276 032.

**Esimerkki 8.1.16.** Havaitaan, että esimerkiksi

$$\begin{aligned}
\binom{6}{0} - \binom{6}{1} + \binom{6}{2} - \binom{6}{3} + \binom{6}{4} - \binom{6}{5} + \binom{6}{6} &= 1 - 6 + 15 - 20 + 15 - 6 + 1 \\
&= 32 - 32 = 0.
\end{aligned}$$

Osoitetaan, että kysymys ei ole sattumasta. Näytetään, että kaikilla $n \in \mathbb{N}$, $n \geq 1$ pätee

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0.$$

Oletetaan, että $n \in \mathbb{N}$ ja $n \geq 1$. Lauseen 8.1.13 mukaan

$$(x-1)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} \cdot (-1)^k.$$

Sijoittamalla tähän $x = 1$ saadaan

$$0^n = \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} \cdot (-1)^k$$

eli

$$0 = \sum_{k=0}^{n} (-1)^k \binom{n}{k}.$$

## 8.2 Geometrinen lukujono ja geometrinen sarja

**Määritelmä 8.2.1.** Lukujono $(a_n)_{n\in\mathbb{N}}$ on *geometrinen*, jos on olemassa sellainen reaaliluku $q$, että kaikilla $n \in \mathbb{N}$ pätee

$$a_{n+1} = qa_n.$$

Lukua $q$ nimitetään geometrisen sarjan *suhdeluvuksi.*

**Esimerkki 8.2.2.** Määritellään lukujono $(a_n)_{n\in\mathbb{N}}$ asettamalla $a_n = 2 \cdot 3^n$ kaikilla $n \in \mathbb{N}$. Näin määritelty lukujono on geometrinen ja sen suhdeluku on 3, sillä kaikilla $n \in \mathbb{N}$ pätee

$$a_{n+1} = 2 \cdot 3^{n+1} = 2 \cdot 3 \cdot 3^n = 3 \cdot 2 \cdot 3^n = 3 \cdot a_n.$$

Lukujonon ensimmäinen jäsen on $a_0 = 2 \cdot 3^0 = 2 \cdot 1 = 2$. Seuraavat jäsenet saadaan kertomalla suhdeluvulla 3, joten jonoksi saadaan $(2, 6, 18, 54, 162, 486, 1458, \ldots)$.

**Esimerkki 8.2.3.** Lukujono $(1, 0, 1, 0, 1, 0, \ldots)$ ei ole geometrinen, sillä esimerkiksi sen kolmannelle jäsenelle $a_2$ pätee $a_2 \neq qa_1$ kaikilla $q \in \mathbb{R}$. Nimittäin $a_2 = 1$ mutta $a_1 = 0$, minkä vuoksi $qa_1 = 0 \neq a_2$ kaikilla $q \in \mathbb{R}$.

---

Jos lukujonon $(a_n)_{n\in\mathbb{N}}$ jäsenet ovat nollasta poikkeavia eli $a_n \neq 0$ kaikilla $n \in \mathbb{N}$, määritelmän yhtälö voidaan muuttaa muotoon

$$\frac{a_{n+1}}{a_n} = q.$$

Peräkkäisten jäsenten suhdetta tutkimalla voidaan siis monissa tilanteissa selvittää, onko lukujono geometrinen.

**Esimerkki 8.2.4.** Tutkitaan lukujonoa $(a_n)$, jolla $a_n = 6 + 12n$ kaikilla $n \in \mathbb{N}$. Tämä lukujono ei ole geometrinen, sillä peräkkäisten jäsenten suhde ei ole vakio. Esimerkiksi $a_1/a_0 = 18/6 = 3$ mutta $a_2/a_1 = 30/18 \approx 1{,}67$.

**Esimerkki 8.2.5.** Tarkastellaan lukujonoa $(b_n)$, jolla $b_n = 18 \cdot (1/3)^n$ kaikilla $n \in \mathbb{N}$. Sen peräkkäisten jäsenten suhde on vakio:

$$\frac{b_{n+1}}{b_n} = \frac{18 \cdot (1/3)^{n+1}}{18 \cdot (1/3)^n} = \frac{(1/3)}{1} = \frac{1}{3}.$$

Tämä tarkoittaa, että lukujono $(b_n)$ on geometrinen ja sen suhdeluku on $q = 1/3$.

---

Seuraavassa lauseessa osoitetaan, että geometrisen lukujonon jäsenet saadaan laskettua jono ensimmäisen jäsenen ja suhdeluvun avulla.

**Lause 8.2.6.** *Oletetaan, että $(a_n)_{n\in\mathbb{N}}$ on geometrinen lukujono, jonka suhdeluku on $q$. Tällöin*

$$a_n = a_0 q^n$$

*kaikilla luonnollisilla luvuilla $n \geq 1$.*

*Todistus.* Alkuaskel: Tutkitaan, päteekö yhtälö pienimmän tarkasteltavan luonnollisen luvun eli luvun 1 tapauksessa. Geometrisen lukujonon määritelmän 8.2.1 mukaan $a_1 = qa_0$. Tämä yhtälö voidaan kirjoittaa myös muodossa $a_1 = a_0q^1$. Väite siis pätee, jos $n = 1$.

Induktioaskel: Aloitetaan tekemällä induktio-oletus. Oletetaan, että $k \in \mathbb{N} \setminus \{0\}$ ja

$$a_k = a_0q^k. \tag{IO}$$

Seuraavaksi tavoitteena on näyttää induktio-oletuksen avulla, että vastaava yhtälö pätee myös seuraavan luonnollisen luvun $k+1$ tapauksessa. Käytetään geometrisen lukujonon määritelmää ja induktio-oletusta:

$$a_{k+1} = qa_k \overset{\text{(IO)}}{=} q(a_0q^k) = a_0q^{k+1}.$$

Johtopäätös: Alkuaskeleesta ja induktioaskeleesta seuraa induktioperiaatteen nojalla, että väite pätee kaikilla luonnollisilla luvuilla $n \geq 1$. □

---

Lauseen 8.2.6 mukaan geometrinen lukujono on muotoa

$$(a, aq, aq^2, aq^3, aq^4, aq^5, \ldots),$$

missä $a$ on jonon ensimmäinen jäsen ja $q$ on jonon suhdeluku. Jos yritetään laskea yhteen geometrisen lukujonon kaikki jäsenet, päädytään geometrisen sarjan käsitteeseen:

**Määritelmä 8.2.7.** Oletetaan, että $a, q \in \mathbb{R}$. *Geometrinen sarja* on päättymätön summa

$$\sum_{k=0}^{\infty} aq^k = a + aq + aq^2 + aq^3 + aq^4 + aq^5 + \ldots.$$

Yllä olevassa määritelmässä suhdeluku $q$ voi olla nolla. Yksinkertaisuuden vuoksi sovitaan, että $q^0 = 1$ myös siinä tapauksessa, että $q = 0$.

Äärettömän monen termin laskeminen yhteen tavalliseen tapaan on mahdotonta. Siirrytään sen vuoksi tarkastelemaan geometrisen sarjan osasummia, jotka muodostetaan laskemalla yhteen äärellisen monta geometrisen lukujonon jäsentä jonon alusta lukien. Muutamia osasummia on taulukossa 8.1.

| $n$ | Geometrisen sarjan $n$:s osasumma $S_n$ |
|---|---|
| 1 | $S_1 = \sum_{k=0}^{0} aq^k = a$ |
| 2 | $S_2 = \sum_{k=0}^{1} aq^k = a + aq$ |
| 3 | $S_3 = \sum_{k=0}^{2} aq^k = a + aq + aq^2$ |
| 4 | $S_4 = \sum_{k=0}^{3} aq^k = a + aq + aq^2 + aq^3$ |
| 5 | $S_5 = \sum_{k=0}^{4} aq^k = a + aq + aq^2 + aq^3 + aq^4$ |

Taulukko 8.1: Geometrisen sarjan osasummia.

**Määritelmä 8.2.8.** Oletetaan, että $a$, $q \in \mathbb{R}$ ja $n \in \mathbb{N} \setminus \{0\}$. Geometrisen sarjan

$$\sum_{k=0}^{\infty} aq^k = a + aq + aq^2 + aq^3 + aq^4 + aq^5 + \dots$$

$n$:s *osasumma* $S_n$ tarkoittaa sarjan $n$ ensimmäisen termin summaa

$$S_n = \sum_{k=0}^{n-1} aq^k = a + aq + aq^2 + \dots + aq^{n-1}.$$

Geometrisen sarjan käyttäytymistä voidaan tutkia osasummien avulla. Koska osasummat ovat tavallisia äärellisiä summia, voidaan niihin soveltaa tavallisia laskusääntöjä. Seuraava lause antaa yhden tavan geometrisen sarjan osasummien laskemiseen.

**Lause 8.2.9.** *Oletetaan, että $a$, $q \in \mathbb{R}$ ja $n \in \mathbb{N} \setminus \{0\}$. Jos suhdeluku $q \neq 1$, geometrisen sarjan $n$:s osasumma on*

$$S_n = \sum_{k=0}^{n-1} aq^k = a \cdot \frac{1 - q^n}{1 - q}.$$

*Jos suhdeluku $q = 1$, geometrisen sarjan $n$:s osasumma on*

$$S_n = \sum_{k=0}^{n-1} aq^k = na.$$

*Todistus.* Induktiolla luvun $n$ suhteen; jätetään harjoitustehtäväksi. $\square$

**Esimerkki 8.2.10.** Lasketaan geometrisen sarjan $5 + 15 + 45 + \dots$ kuudes osasumma $S_6$.

Koska sarja on geometrinen, saadaan suhdeluku laskemalla peräkkäisten termien suhde: $q = a_1/a_0 = 15/5 = 3$. Lauseen 8.2.9 mukaan kysytty osasumma on siis

$$S_6 = \sum_{k=0}^{5} aq^k = \sum_{k=0}^{5} 5 \cdot 3^k = 5 \cdot \frac{1-3^6}{1-3} = 5 \cdot \frac{1-729}{-2} = 5 \cdot \frac{-728}{-2} = \frac{3640}{2} = 1820.$$

**Esimerkki 8.2.11.** Tarkastellaan geometrista sarjaa

$$\sum_{k=0}^{\infty} \left(-\frac{1}{2}\right)^k = 1 - \frac{1}{2} + \frac{1}{4} - \frac{1}{8} + \dots$$

Lasketaan sen osasummat $S_{10}$ ja $S_{20}$. Tarkasteltavan sarjan suhdeluku $q = -1/2$, joten lauseen 8.2.9 mukaan

$$S_{10} = \sum_{k=0}^{9} \left(-\frac{1}{2}\right)^k = 1 \cdot \frac{1-(-1/2)^{10}}{1-(-1/2)} = \frac{1-(-0{,}5)^{10}}{1{,}5} \approx 0{,}6660$$

$$S_{20} = \sum_{k=0}^{19} \left(-\frac{1}{2}\right)^k = 1 \cdot \frac{1-(-1/2)^{20}}{1-(-1/2)} = \frac{1-(-0{,}5)^{20}}{1{,}5} \approx 0{,}6667$$

---

Voidaan osoittaa, että jos geometrisen sarjan suhdeluvulle pätee $-1 < q < 1$, niin geometrisen sarjan osasummat lähestyvät lukua

$$\frac{a}{1-q},$$

missä $a$ on sarjan ensimmäinen termi. Tällöin sanotaan, että geometrinen sarja *suppenee* ja sen *summa* on $a/(1-q)$. Jos geometrinen sarja ei suppene, sanotaan, että se *hajaantuu.*

**Lause 8.2.12.** *Geometrinen sarja suppenee, jos ja vain jos sen suhdeluvulle pätee* $-1 < q < 1$. *Tällöin sen summa on*

$$\sum_{k=0}^{\infty} aq^k = \frac{a}{1-q}.$$

*Todistus.* Sivuutetaan. □

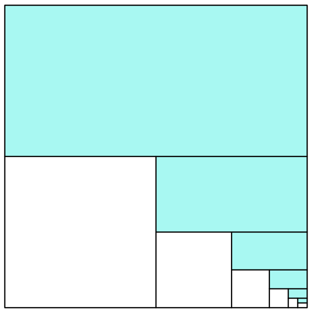
**Esimerkki 8.2.13.** Tarkastellaan esimerkin 8.2.11 geometrista sarjaa

$$\sum_{k=0}^{\infty} \left(-\frac{1}{2}\right)^k = 1 - \frac{1}{2} + \frac{1}{4} - \frac{1}{8} + \dots$$

Sen suhdeluvulle $q = -1/2$ pätee $-1 < q < 1$, joten lauseen 8.2.12 mukaan sarja suppenee ja sen summa on

$$\sum_{k=0}^{\infty} \left(-\frac{1}{2}\right)^k = \frac{1}{1-(-1/2)} = \frac{1}{3/2} = \frac{2}{3}$$

**Esimerkki 8.2.14.** Oletetaan, että alla olevan neliön sivun pituus on $s$. Mikä on väritetyn osan pinta-ala, jos väritystä jatketaan loputtomiin alla olevan kuvan mukaisesti?



Suurimman väritetyn suorakulmion pinta-ala on puolet alkuperäisen neliön pinta-alasta eli

$$A_0 = \frac{1}{2} \cdot s \cdot s = \frac{s^2}{2}.$$

Seuraavan väritetyn suorakulmion kumpikin sivu on puolet edellisen väritetyn suorakulmion vastaavasta sivusta, joten kaikilla $k \in \mathbb{N}$ pinta-alaksi $A_{k+1}$ saadaan

$$A_{k+1} = \frac{1}{4} A_k.$$

Väritettyjen suorakulmioiden pinta-alat muodostavat siis geometrisen lukujonon $(A_k)_{k\in\mathbb{N}}$, jonka suhdeluku $q = 1/4$. Koska $-1 < q < 1$, vastaava geometrinen sarja suppenee ja sen summa on

$$\sum_{k=0}^{\infty} A_k = \frac{A_0}{1-q} = \frac{s^2/2}{1-(1/4)} = \frac{s^2/2}{3/4} = \frac{s^2}{2} \cdot \frac{4}{3} = \frac{2}{3}s^2$$

eli 2/3 alkuperäisen neliön pinta-alasta.

**Esimerkki 8.2.15.** Erään vieraslajin populaation kooksi laskettiin syksyn alussa 1000 yksilöä. Populaatio pienenee joka talvi kylmyyden ja epäsuotuisten olojen vuoksi 30 % mutta keväisin alueelle muuttaa keskimäärin 100 uutta yksilöä. Mikä on populaation koko 10 vuoden kuluttua?

Muodostetaan lukujono $(a_n)_{n\in\mathbb{N}}$, jossa $a_n$ kertoo populaation koon syksyllä $n$ vuoden kuluttua alkuhetkestä. Jonon ensimmäinen jäsen on $a_0 = 1000$ eli populaation koko alkutilanteessa. Talven yli selviää 70 % edellisen syksyn populaatiosta ja lisäksi populaatio kasvaa keväällä sadalla yksilöllä, joten populaation koko seuraavana syksynä saadaan aina edellisestä kertomalla luvulla 0,7 ja lisäämällä 100. Toisin sanottuna kaikilla $n \in \mathbb{N}$ pätee

$$a_{n+1} = 0{,}7a_n + 100.$$

Esimerkiksi yhden vuoden kuluttua syksyllä populaation koko on

$$a_1 = 0{,}7a_0 + 100.$$

Kahden vuoden kuluttua syksyllä populaation koko on

$$a_2 = 0{,}7a_1 + 100 = 0{,}7(0{,}7a_0 + 100) + 100 = 0{,}7^2 a_0 + 0{,}7 \cdot 100 + 100.$$

Kolmen vuoden kuluttua syksyllä populaation koko on

$$\begin{aligned} a_3 &= 0{,}7a_2 + 100 \\ &= 0{,}7(0{,}7^2 a_0 + 0{,}7 \cdot 100 + 100) + 100 \\ &= 0{,}7^3 a_0 + 0{,}7^2 \cdot 100 + 0{,}7 \cdot 100 + 100. \end{aligned}$$

Vaikuttaa siltä, että populaation koko syksyllä $n$ vuoden kuluttua alkuhetkestä saadaan yhtälöstä

$$\begin{aligned} a_n &= 0{,}7^n a_0 + 0{,}7^{n-1} \cdot 100 + \cdots + 0{,}7^2 \cdot 100 + 0{,}7 \cdot 100 + 100 \\ &= 0{,}7^n a_0 + \sum_{j=0}^{n-1} 0{,}7^j \cdot 100, \end{aligned}$$

missä $n \geq 1$. Tämä voidaan todistaa induktiolla.

Kymmenen vuoden kuluttua syksyllä populaation koko on siis

$$a_{10} = 0{,}7^{10} a_0 + \sum_{j=0}^{9} 0{,}7^j \cdot 100 = 0{,}7^{10} \cdot 1000 + 100 \cdot \frac{1 - 0{,}7^{10}}{1 - 0{,}7} \approx 28{,}2 + 323{,}9 = 352{,}1$$

eli noin 350 yksilöä. Tässä käytettiin geometrisen sarjan osasumman laskemiseen lausetta 8.2.9.

**Esimerkki 8.2.16.** Jatkoa esimerkkiin 8.2.15. Tiedetään, että tarkasteltavan populaation koko syksyllä $n$ vuoden kuluttua alkuhetkestä saadaan yhtälöstä

$$a_n = 0{,}7^n a_0 + \sum_{j=0}^{n-1} 0{,}7^j \cdot 100,$$

missä $n \geq 1$. Kun $n$ kasvaa, ensimmäinen yhteenlaskettava $0{,}7^n a_0$ pienenee pienenemistään kohti nollaa ja toinen yhteenlaskettava

$$\sum_{j=0}^{n-1} 0{,}7^j \cdot 100$$

lähestyy vastaavaa geometrista sarjaa. Koska sen suhdeluvulle $q = 0{,}7$ pätee $-1 < q < 1$, kyseinen geometrinen sarja suppenee, ja voidaan päätellä, että populaation koko lähestyy vähitellen lukua

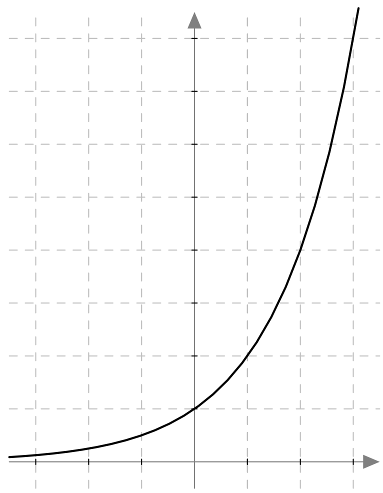
$$0 + \sum_{j=0}^{\infty} 0{,}7^j \cdot 100 = \frac{100}{1 - 0{,}7} = \frac{100}{0{,}3} = 333$$

eli noin 330 yksilöä.

## 8.3 Eksponentti- ja logaritmifunktiot

Tässä kappaleessa keskitytään kaksikantaisiin eksponentti- ja logaritmifunktioihin. Erityisesti kaksikantainen logaritmifunktio on tietojenkäsittelytieteen puolella tarpeellinen työkalu. Muut eksponentti- ja logaritmifunktiot käyttäytyvät samaan tapaan.

Tarkastellaan kaksikantaista eksponenttifunktiota $f\colon \mathbb{R} \to \mathbb{R}_+$, jolla $f(x) = 2^x$ kaikilla $x \in \mathbb{R}$. Alla kuvassa 8.4 on näkyvissä osa sen kuvaajasta. Huomaa, että funktion $f$ maaliksi voidaan valita positiivisten reaalilukujen joukko $\mathbb{R}_+ = \{x \in \mathbb{R} \mid x > 0\}$.



Kuva 8.4: Osa kaksikantaisen eksponenttifunktion $x \mapsto 2^x$ kuvaajasta.

Kokonaislukujen joukossa tämän eksponenttifunktion arvojen laskeminen onnistuu tavalliseen tapaan. Esimerkiksi

$$\begin{aligned} f(5) &= 2^5 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 32 \\ f(0) &= 2^0 = 1 \\ f(-3) &= 2^{-3} = \frac{1}{2^3} = \frac{1}{2 \cdot 2 \cdot 2} = \frac{1}{8} \end{aligned}$$

Rationaalilukujen joukossa funktion $f$ arvot saadaan laskettua ottamalla tarvittaessa käyttöön juurifunktiot. Esimerkiksi

$$\begin{aligned} f(1/2) &= 2^{\frac{1}{2}} = \sqrt{2} \\ f(1/3) &= 2^{\frac{1}{3}} = \sqrt[3]{2} \\ f(-5/2) &= 2^{\left(-\frac{5}{2}\right)} = \frac{1}{2^{\frac{5}{2}}} = \frac{1}{\sqrt{2} \cdot \sqrt{2} \cdot \sqrt{2} \cdot \sqrt{2} \cdot \sqrt{2}} = \frac{1}{4\sqrt{2}} \end{aligned}$$

Jotta kaksikantainen eksponenttifunktio saadaan määriteltyä koko reaalilukujen joukossa (siis erityisesti irrationaalilukujen $\mathbb{R} \setminus \mathbb{Q}$ joukossa), tarvitaan enemmän matemaatiikan teoriaa. Emme syvenny siihen tässä sen tarkemmin vaan sivuutamme myös seuraavan lauseen todistuksen.

**Lause 8.3.1.** *Oletetaan, että $a, b \in \mathbb{R}$. Tällöin $2^a \cdot 2^b = 2^{a+b}$ ja $(2^a)^b = 2^{ab}$.*

Positiivisten kokonaislukujen tapauksessa lauseen 8.3.1 tulosta voi havainnollistaa kertolaskun avulla. Oletetaan, että $m, n \in \mathbb{N} \setminus \{0\}$. Tällöin

$$2^m \cdot 2^n = \underbrace{(2 \cdots 2)}_{m \text{ kpl}} \cdot \underbrace{(2 \cdot 2 \cdots 2)}_{n \text{ kpl}} = \underbrace{2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdots 2}_{m+n \text{ kpl}} = 2^{m+n}$$

ja

$$(2^m)^n = \underbrace{(2^m) \cdot (2^m) \cdots (2^m)}_{n \text{ kpl}} = \underbrace{(2 \cdots 2)}_{m \text{ kpl}} \cdot \underbrace{(2 \cdots 2)}_{m \text{ kpl}} \cdots \underbrace{(2 \cdots 2)}_{m \text{ kpl}} = \underbrace{2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdots 2}_{nm \text{ kpl}} = 2^{nm}\,.$$

---

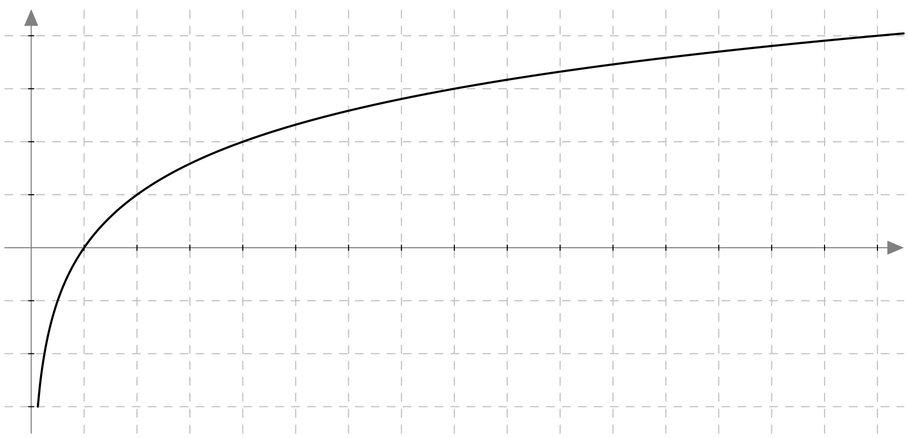
On mahdollista osoittaa, että eksponenttifunktiolla $x \mapsto 2^x$ on olemassa käänteisfunktio. Tätä käänteisfunktiota kutsutaan kaksikantaiseksi logaritmiksi.

**Määritelmä 8.3.2.** *Kaksikantainen logaritmifunktio* $x \mapsto \log_2(x)$ on eksponenttifunktion $x \mapsto 2^x$ käänteisfunktio. Toisin sanottuna

$$\log_2(x) = a \quad \Leftrightarrow \quad 2^a = x\,.$$

Koska eksponenttifunktio on kuvaus $\mathbb{R} \to \mathbb{R}_+$, on sen käänteisfunktion määrittelyjoukko $\mathbb{R}_+$. Logaritmi on siis määritelty vain positiivisille reaaliluvuille. Määritelmän 8.3.2 mukaan logaritmi $\log_2(x)$ kertoo, mihin potenssiin luku 2 pitää korottaa, jolla tuloksena on $x$. Siis esimerkiksi $\log_2(8) = 3$ ja $\log_2(1) = 0$, sillä $2^3 = 8$ ja $2^0 = 1$.

Kaksikantaista logaritmia voidaan merkitä myös $\mathrm{lb} = \log_2$. Osa kaksikantaisen logaritmifunktion kuvaajasta näkyy alla kuvassa 8.5.



Kuva 8.5: Osa kaksikantaisen logaritmifunktion $x \mapsto \log_2(x)$ kuvaajasta.

Kuvasta 8.5 näkyy, että logaritmifunktion arvot kasvavat melko hitaasti. Sama asia nähdään seuraavasta lauseesta.

**Lause 8.3.3.** *Oletetaan, että* $x \in \mathbb{R}_+$ *ja* $c \in \mathbb{R}$. *Tällöin* $\log_2(x^c) = c \log_2(x)$.

*Todistus.* Merkitään $a = \log_2(x)$. Tämä tarkoittaa logartimin määritelmän 8.3.2 mukaan, että $2^a = x$. Soveltamalla lausetta 8.3.1 saadaan

$$x^c = (2^a)^c = 2^{ca}.$$

Logaritmin määritelmän nojalla tällöin $\log_2(x^c) = ca$. Ottamalla huomioon, että $a = \log_2(x)$, päästään johtopäätökseen

$$\log_2(x^c) = c \log_2(x). \qquad \square$$

Esimerkiksi luvun $1000 = 10^3$ logaritmi on lauseen 8.3.3 nojalla vain kolminkertainen luvun 10 logaritmiin verrattuna: $\log_2(1000) = 3 \log_2(10)$.

---

Myös seuraava tulon logaritmia koskeva tulos perustuu lauseessa 8.3.1 mainittuihin eksponenttifunktion ominaisuuksiin.

**Lause 8.3.4.** *Oletetaan, että* $x, y \in \mathbb{R}_+$. *Tällöin* $\log_2(xy) = \log_2(x) + \log_2(y)$.

*Todistus.* Merkitään $a = \log_2(x)$ ja $b = \log_2(y)$. Logaritmin määritelmän 8.3.2 mukaan tällöin $x = 2^a$ ja $y = 2^b$. Soveltamalla lausetta 8.3.1 saadaan

$$xy = 2^a \cdot 2^b = 2^{a+b}.$$

Tämä puolestaan tarkoittaa logaritmin määritelmän nojalla, että $\log_2(xy) = a + b$. Ottamalla huomioon, että $a = \log_2(x)$ ja $b = \log_2(y)$, päästään johtopäätökseen

$$\log_2(xy) = \log_2(x) + \log_2(y). \qquad \square$$

Esimerkiksi jos luku 10 kerrotaan luvulla 8, kasvaa logaritmin arvo vain kolmella:

$$\log_2(80) = \log_2(8 \cdot 10) = \log_2(8) + \log_2(10) = 3 + \log_2(10).$$

---

Lauseiden 8.3.3 ja 8.3.4 avulla saadaan vastaava tulos myös osamäärän logaritmille:

**Lause 8.3.5.** *Oletetaan, että* $x, y \in \mathbb{R}_+$. *Tällöin* $\log_2(x/y) = \log_2(x) - \log_2(y)$.

*Todistus.* Osamäärä $x/y$ voidaan kirjoittaa tulona muodossa $x/y = x \cdot y^{-1}$. Soveltamalla lauseita 8.3.3–8.3.4 saadaan

$$\begin{aligned} \log_2\left(\frac{x}{y}\right) &= \log_2(x \cdot y^{-1}) = \log_2(x) + \log_2(y^{-1}) = \log_2(x) + (-1) \cdot \log_2(y) \\ &= \log_2(x) - \log_2(y). \end{aligned} \qquad \square$$

Kaksikantaisen logaritmifunktion määritelmän mukaan $\log_2(x) = n$, jos ja vain jos $x = 2^n$. Jälkimmäinen yhtälö voidaan kirjoittaa myös muodossa

$$\frac{x}{2^n} = 1.$$

Tämä tarkoittaa, että logaritmifunktion arvoja voidaan määrittää jakolaskun avulla. Asiaa on havainnollistettu seuraavissa esimerkeissä.

**Esimerkki 8.3.6.** Määritetään $\log_2(32)$ jakolaskun avulla. Katsotaan, kuinka monta kertaa luku 32 pitää jakaa luvulla 2, jotta tulokseksi saadaan 1:

$$\frac{32}{2} = 16, \quad \frac{16}{2} = 8, \quad \frac{8}{2} = 4, \quad \frac{4}{2} = 2, \quad \frac{2}{2} = 1.$$

Jakolaskuja tarvittiin viisi, joten $32/2^5 = 1$. Tästä voidaan päätellä, että $\log_2(32) = 5$.

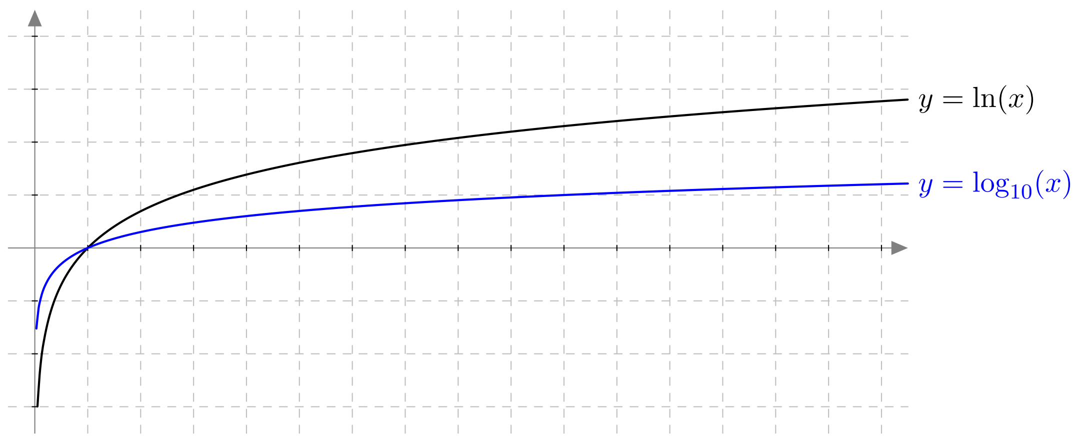
**Esimerkki 8.3.7.** Määritetään luvun $\log_2(24)$ likiarvo jakolaskun avulla. Katsotaan, kuinka monta kertaa luku 24 pitää jakaa luvulla 2, jotta tulos on mahdollisimman lähellä lukua 1:

$$\frac{24}{2} = 12, \quad \frac{12}{2} = 6, \quad \frac{6}{2} = 3, \quad \frac{3}{2} = 1{,}5, \quad \frac{1{,}5}{2} = 0{,}75\,.$$

Havaitaan, että viidennen jakolaskun jälkeen tulos on lähimpänä lukua 1. Siis $\log_2(24) \approx 5$.

---

Muita yleisesti käytettyjä logaritmifunktioita ovat eksponenttifunktion $x \mapsto 10^x$ käänteisfunktio *kymmenkantainen logaritmi* $x \mapsto \log_{10}(x)$ sekä eksponenttifunktion $x \mapsto e^x$ käänteisfunktio *luonnollinen logaritmi* $x \mapsto \ln(x)$, jonka kantaluku on Neperin luku $e \approx 2{,}718$. Niiden kuvaajat on piirretty kuvaan 8.6.




Kuva 8.6: Logaritmifunktioiden $x \mapsto \log_{10}(x)$ ja $x \mapsto \ln(x)$ kuvaajat.

## 8.4 Jaollisuus ja kongruenssi

Palautetaan mieleen luvussa 4 esiintynyt jaollisuuden määritelmä:

**Määritelmä 8.4.1.** Kokonaisluku $z$ on *jaollinen kokonaisluvulla* $m$, jos jollakin kokonaisluvulla $a$ pätee $z = am$. Tällöin merkitään $m \mid z$ ja sanotaan, että luku $m$ *jakaa* luvun $z$. Jos luku $z$ ei ole jaollinen luvulla $m$, merkitään $m \nmid z$.

Esimerkiksi luku 42 on jaollinen luvulla 6 eli $6 \mid 42$, sillä $42 = 7 \cdot 6$. Toisaalta luku 25 ei ole jaollinen luvulla 6, mikä havaitaan esimerkiksi tarkastelemalla yhtälöä $6x = 25$:

- Jos $x \leq 4$, niin $6x \leq 6 \cdot 4 = 24$.
- Jos $x \geq 5$, niin $6x \geq 6 \cdot 5 = 30$.

Mikään kokonaisluku ei siis toteuta yhtälöä $6x = 25$. Jos luku 25 kuitenkin jaetaan kuudella, osamäärän kokonaisosaksi saadaan 4:

$$\frac{25}{6} \approx 4{,}167.$$

Luku 25 voidaankin kirjoittaa muodossa $25 = 4 \cdot 6 + 1$. Vastaava yhtälö voidaan muodostaa muillekin kokonaisluvuille, kuten seuraava lause osoittaa. Sen todistus löytyy esimerkiksi kirjasta J. Häsä & J. Rämö: Johdatus abstraktiin algebraan.

**Lause 8.4.2** (**Jakoyhtälö**)**.** *Oletetaan, että $a, b \in \mathbb{Z}$ ja $b \neq 0$. Tällöin on olemassa tasan yksi sellainen $q \in \mathbb{Z}$ ja tasan yksi sellainen $r \in \mathbb{Z}$, että*

$$a = qb + r \quad ja \quad 0 \leq r < |b| \ .$$

**Määritelmä 8.4.3.** Oletetaan, että $a$, $b \in \mathbb{Z}$ ja $b \neq 0$. Luvun $a$ *jakojäännös* luvulla $b$ jaettaessa tarkoittaa jakoyhtälössä mainittua lukua $r$.
Merkintä $a \bmod b$ tarkoittaa luvun $a$ jakojäännöstä luvulla $b$ jaettaessa.

Esimerkiksi edellä huomattiin, että luku 25 voidaan kirjoittaa muodossa $25 = 4 \cdot 6 + 1$. Tästä voidaan päätellä, että $25 \bmod 6 = 1$. Toisin sanottuna luvun 25 jakojäännös kuudella jaettaessa on 1.

**Esimerkki 8.4.4.** Tarkastellaan neljällä jakamista sekä lukuja 11, 59 ja $-9$.

- Huomataan, että $11 \bmod 4 = 3$, sillä vastaava jakoyhtälö on $11 = 2 \cdot 4 + 3$.
- Huomataan, että $59 \bmod 4 = 3$, sillä vastaava jakoyhtälö on $59 = 14 \cdot 4 + 3$.
- Huomataan, että $-9 \bmod 4 = 3$, sillä vastaava jakoyhtälö on $-9 = -3 \cdot 4 + 3$.

**Määritelmä 8.4.5.** Oletetaan, että $a$, $b \in \mathbb{Z}$ ja $n \in \mathbb{N} \setminus \{0\}$. Jos luvuilla $a$ ja $b$ on sama jakojäännös luvulla $n$ jaettaessa, sanotaan, että luvut $a$ ja $b$ ovat *kongruentit modulo n* ja merkitään $a \equiv b \pmod{n}$.

Esimerkin 8.4.4 perusteella luvut 11 ja 59 ovat kongruentit modulo 4, sillä molempien jakojäännös neljällä jaettaessa on 3. Samassa esimerkissä nähtiin, että myös $-9 \equiv 11 \pmod{4}$.

Seuraava lause yhdistää kongruenssin ja jaollisuuden:

**Lause 8.4.6.** *Olkoot* $a$, $b \in \mathbb{Z}$ *ja* $n \in \mathbb{N} \setminus \{0\}$*. Tällöin* $a \equiv b \pmod{n}$*, jos ja vain jos* $n \mid (a-b)$*.*

*Todistus.* "$\Rightarrow$": Harjoitustehtävä.

"$\Leftarrow$": Oletetaan, että $n \mid (a-b)$. Tällöin on olemassa sellainen $k \in \mathbb{Z}$, että $a - b = kn$. Tästä seuraa, että $a = b + kn$.

Oletetaan, että luvun $b$ jakojäännös luvulla $n$ jaettaessa on $r$. Tällöin $b = qn + r$, missä $q$, $r \in \mathbb{Z}$ ja $0 \leq r < n$. Näin ollen

$$a = b + kn = qn + r + kn = (q + k)n + r,$$

missä $q + k \in \mathbb{Z}$ kahden kokonaisluvun summana ja lisäksi $r \in \mathbb{Z}$ ja $0 \leq r < n$. Siis luvun $a$ jakojäännös luvulla $n$ jaettaessa on $r$.

Luvuilla $a$ ja $b$ on siis sama jakojäännös luvulla $n$ jaettaessa, joten $a \equiv b \pmod{n}$. $\square$

**Esimerkki 8.4.7.** Esimerkiksi lukujen 257 ja 173 erotus on $257 - 173 = 84 = 21 \cdot 4$, joten $257 \equiv 173 \pmod{4}$.

**Lause 8.4.8.** *Olkoot* $a$, $b$, $c$, $d \in \mathbb{Z}$ *ja* $k$, $n \in \mathbb{N} \setminus \{0\}$*. Oletetaan, että* $a \equiv b \pmod{n}$ *ja* $c \equiv d \pmod{n}$*. Tällöin*

(a) $a + c \equiv b + d \pmod{n}$

(b) $ac \equiv bd \pmod{n}$

(c) $a^k \equiv b^k \pmod{n}$.

*Todistus.* Jätetään kohtien (a) ja (c) todistukset harjoitustehtäviksi. Kohdan (c) voi todistaa induktiolla käyttämällä apuna kohdan (b) tulosta.

(b) Oletuksen mukaan luvuilla $a$ ja $b$ on sama jakojäännös luvulla $n$ jaettaessa eli ne voidaan kirjoittaa muodossa $a = q_1 n + r$ ja $b = q_2 n + r$, missä $q_1$, $q_2$, $r \in \mathbb{Z}$ ja $0 \leq r < n$.

Oletuksen mukaan myös luvuilla $c$ ja $d$ on sama jakojäännös luvulla $n$ jaettaessa eli ne voidaan kirjoittaa muodossa $c = p_1 n + s$ ja $d = p_2 n + s$, missä $p_1$, $p_2$, $s \in \mathbb{Z}$ ja $0 \leq s < n$.

Lasketaan tulot:

$$ac = (q_1 n + r)(p_1 n + s) = q_1 p_1 n^2 + q_1 ns + p_1 nr + rs$$
$$bd = (q_2 n + r)(p_2 n + s) = q_2 p_2 n^2 + q_2 ns + p_2 nr + rs$$

Näiden erotukseksi saadaan

$$\begin{aligned} ac - bd &= q_1p_1n^2 - q_2p_2n^2 + q_1ns - q_2ns + p_1nr - p_2nr \\ &= n(q_1p_1n - q_2p_2n + q_1s - q_2s + p_1r - p_2r), \end{aligned}$$

missä $q_1p_1n - q_2p_2n + q_1s - q_2s + p_1r - p_2r \in \mathbb{Z}$, sillä kokonaislukujen summat, erotukset ja tulot ovat edelleen kokonaislukuja.

Siis luku $n$ jakaa erotuksen $ac - bd$, joten lauseen 8.4.6 mukaan $ac \equiv bd \pmod{n}$. □

**Esimerkki 8.4.9.** Lasketaan lauseen 8.4.8 kongruenssien laskusääntöjen avulla

$$(6^{2015} \cdot 500^{50} + 314^{99} \cdot 8^{2016}) \bmod 7.$$

Tarkastellaan yhteenlaskettavissa esiintyviä tulon tekijöitä erikseen:

- Ensinnäkin $6 - (-1) = 1 \cdot 7$, joten $6 \equiv -1 \pmod{7}$. Siis $6^{2015} \equiv (-1)^{2015} \pmod{7}$.
- Huomataan, että $500 - 3 = 71 \cdot 7$, joten $500 \equiv 3 \pmod{7}$. Tällöin $500^3 \equiv 3^3 \pmod{7}$. Koska $3^3 = 27$ ja $27 - (-1) = 4 \cdot 7$, niin $3^3 \equiv -1 \pmod{7}$. Siis $500^3 \equiv -1 \pmod{7}$. Nyt $500^{50} = (500^3)^{16} \cdot 500^2 \equiv (-1)^{16} \cdot 3^2 = 9 \pmod{7}$.
- Koska $314 - (-1) = 45 \cdot 7$, niin $314 \equiv -1 \pmod{7}$. Siten $314^{99} \equiv (-1)^{99} \pmod{7}$.
- Koska $8 - 1 = 1 \cdot 7$, niin $8 \equiv 1 \pmod{7}$. Siis $8^{2016} \equiv 1^{2016} \pmod{7}$.

Yhdistämällä nämä tiedot saadaan

$$6^{2015} \cdot 500^{50} + 314^{99} \cdot 8^{2016} \equiv (-1)^{2015} \cdot 9 + (-1)^{99} \cdot 1^{2016} \pmod{7}$$

eli

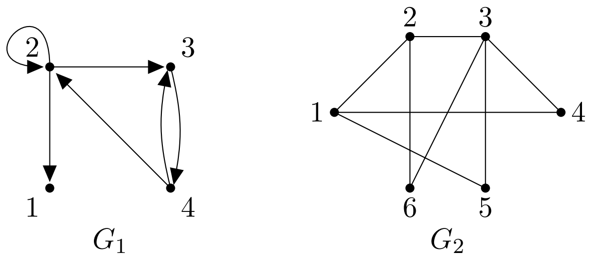
$$6^{2015} \cdot 500^{50} + 314^{99} \cdot 8^{2016} \equiv -10 \pmod{7}.$$

Luvun $-10$ jakojäännös seitsemällä jaettaessa on 4, sillä vastaava jakoyhtälö on $-10 = -2 \cdot 7 + 4$. Siis myös

$$(6^{2015} \cdot 500^{50} + 314^{99} \cdot 8^{2016}) \bmod 7 = 4.$$

## 8.5 Verkot

Verkot muodostuvat *solmuista* eli pisteistä ja *kaarista* eli nuolista tai viivoista pisteiden välillä. Kaksi erilaista verkkoa on kuvattu alla kuvassa 8.7.




Kuva 8.7: Suunnattu verkko $G_1$ ja suuntaamaton verkko $G_2$.

**Määritelmä 8.5.1.** *Suunnattu verkko* $G$ on pari $(V, E)$, missä $V \neq \emptyset$ on *solmujen* joukko ja

$$E = \{(a, b) \in V \times V \mid \text{solmusta } a \text{ on nuoli solmuun } b\}$$

on *kaarien* joukko.

Esimerkiksi kuvan 8.7 suunnatun verkon $G_1$ solmujen joukko on $V_1 = \{1, 2, 3, 4\}$ ja kaarien joukko on $E_1 = \{(2, 1), (2, 2), (2, 3), (3, 4), (4, 2), (4, 3)\}$.

Huomaa, että määritelmän 8.5.1 mukaan kaarien joukko $E$ on joukon $V \times V$ osajoukko eli solmujen joukon $V$ relaatio. Suomenkielisessä kirjallisuudessa suunnattuja verkkoja kutsutaan usein *suhteikoiksi*.

**Määritelmä 8.5.2.** Oletetaan, että $G = (V, E)$ on suunnattu verkko ja $a, b \in V$.

Merkintä $a \to b$ tarkoittaa, että $(a, b) \in E$. Tällöin sanotaan, että $a$ on kaaren $(a, b)$ *lähtösolmu* ja $b$ on kaaren $(a, b)$ *maalisolmu*. Sanotaan myös, että solmu $b$ on solmun $a$ *vierussolmu*.

Jos $(a, a) \in E$, sanotaan, että suunnatussa verkossa $G$ on *silmukka* solmussa $a$.

Solmun $a$ *lähtöaste* $\deg^+(a)$ on solmusta $a$ lähtevien nuolten lukumäärä.

Solmun $a$ *tuloaste* $\deg^-(a)$ on solmuun $a$ päättyvien nuolten lukumäärä.

Esimerkiksi kuvan 8.7 suunnatussa verkossa $G_1$ solmu 3 on solmun 2 vierussolmu, sillä $2 \to 3$. Toisaalta solmu 2 on solmun 4 vierussolmu, sillä $4 \to 2$. Kaaren $(4, 2)$ lähtösolmu on siis 4 ja maalisolmu on 2. Havaitaan, että suunnatussa verkossa $G_1$ on silmukka solmussa 2, sillä $(2, 2) \in E_1$. Solmun 2 lähtöaste $\deg^+(2) = 3$ ja tuloaste on $\deg^-(2) = 2$.

**Määritelmä 8.5.3.** *Suuntaamaton verkko* tai lyhyesti *verkko* $G$ on pari $(V, E)$, missä $V \neq \emptyset$ on *solmujen* joukko ja

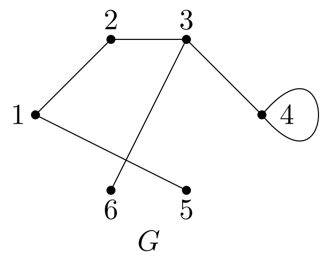
$$E = \{(a, b) \in V \times V \mid \text{solmusta } a \text{ on viiva solmuun } b\}$$

on *kaarien* joukko.

Määritelmän 8.5.3 mukaan myös suuntaamattoman verkon kaarien joukko $E$ on solmujen joukon $V$ relaatio. Koska viivoilla ei ole suuntaa, tämä relaatio on aina symmetrinen: jos $a$, $b \in V$ ja $(a, b) \in E$, niin myös $(b, a) \in E$.

Esimerkiksi kuvan 8.8 verkon $G$ solmujen joukko on $V = \{1, 2, 3, 4, 5, 6\}$ ja kaarien joukko on

$$E = \{(1, 2), (2, 1), (1, 5), (5, 1)(2, 3), (3, 2), (3, 4), (4, 3), (4, 4), (3, 6), (6, 3)\}.$$




Kuva 8.8: Suuntaamaton verkko $G$.

**Määritelmä 8.5.4.** Oletetaan, että $G = (V, E)$ on suuntaamaton verkko ja $a$, $b \in V$.

Jos solmujen $a$ ja $b$ välillä on viiva, niin sanotaan, että solmut $a$ ja $b$ ovat *vierekkäisiä.*

Jos $(a, a) \in E$, sanotaan, että verkossa $G$ on *silmukka* solmussa $a$.

Solmun $a$ *aste* $\deg(a)$ tarkoittaa niiden viivojen lukumäärää, joiden toisena päätepisteenä kyseinen solmu on.

Esimerkiksi kuvan 8.8 verkossa $G$ solmut 3 ja 6 ovat vierekkäisiä. Solmun 3 aste on $\deg(3) = 3$ ja solmun 6 aste on $\deg(6) = 1$. Solmun 4 aste on $\deg(4) = 3$. Solmussa 4 oleva silmukka kasvattaa siis solmun 4 astetta kahdella.

**Esimerkki 8.5.5.** Tarkastellaan suuntaamatonta verkkoa $G$, jonka viivojen lukumäärä on $m$. Jokainen viiva kasvattaa solmujen asteiden summaa kahdella: joko kasvattamalla kahden solmun astetta yhdellä tai silmukan tapauksessa kasvattamalla yhden solmun astetta kahdella. Näin voidaan päätellä, että solmujen asteiden summa on $2m$. Esimerkiksi kuvan 8.8 verkossa $G$ on kuusi viivaa ja sen solmujen asteiden summaksi saadaan

$$\sum_{k=1}^{6} \deg(k) = 2 + 2 + 3 + 3 + 1 + 1 = 12.$$

**Esimerkki 8.5.6.** Oletetaan, että $G = (V, E)$ on suuntaamaton verkko. Osoitetaan, että siinä on parillinen määrä sellaisia solmuja, joiden aste on pariton.

Olkoon $m$ verkon $G$ viivojen lukumäärä. Jokainen viiva kasvattaa solmujen asteiden summaa kahdella, joten solmujen asteiden summa on $2m$. Siis

$$\sum_{v \in V} \deg(v) = 2m.$$

Olkoon $V_1$ niiden verkon $G$ solmujen joukko, joiden aste on pariton. Olkoon vastaavasti $V_2$ niiden verkon $G$ solmujen joukko, joiden aste on parillinen. Ryhmitellään edellä esiintyneessä summassa yhteenlaskettavat uudelleen niin, että ensin lasketaan yhteen paritonasteisten solmujen asteet. Näin päädytään yhtälöön

$$\sum_{v \in V_1} \deg(v) + \sum_{v \in V_2} \deg(v) = 2m.$$

Tästä saadaan ratkaistua

$$\sum_{v \in V_1} \deg(v) = 2m - \sum_{v \in V_2} \deg(v).$$

Yhtälön oikealla puolella on nyt kahden parillisen luvun erotus, joka on parillinen. Tämä tarkoittaa, että myös paritonasteisten solmujen asteiden summa on parillinen. Tästä seuraa, että paritonasteisia solmuja on oltava parillinen määrä.

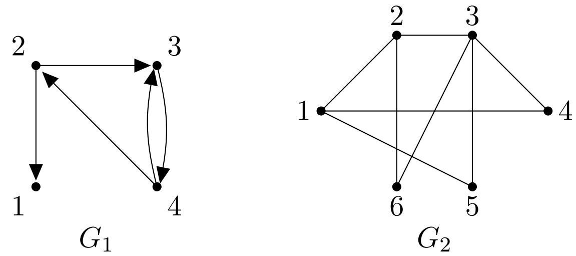
---

Sekä suunnattuja että suuntaamattomia verkkoja voidaan esittää matriisien avulla. Matriisi on suorakulmion muotoinen lukutaulukko. Esimerkiksi

$$A = \begin{bmatrix} 0 & 2 & 4 & 6 \\ 3 & 5 & 7 & 9 \end{bmatrix}$$

on $2 \times 4$-matriisi, jossa on kaksi riviä ja neljä saraketta. Matriisin alkioihin viitataan rivin ja sarakkeen numeroiden avulla. Esimerkiksi yllä olevassa matriisissa $A(1, 3) = 4$ ja $A(2, 4) = 9$. Merkintä $A(i, j)$ tarkoittaa siis alkoita, joka on matriisin $A$ rivillä $i$ sarakkeessa $j$.

**Määritelmä 8.5.7.** Oletetaan, että $G = (V, E)$ on suunnattu tai suuntaamaton verkko ja $i$, $j \in V$. Verkon $G$ *vierusmatriisi* tarkoittaa neliömatriisia $A$, jossa $A(i, j) = 1$, jos solmusta $i$ on kaari solmuun $j$, ja muuten $A(i, j) = 0$.




Kuva 8.9: Suunnattu verkko $G_1$ ja suuntaamaton verkko $G_2$.

Esimerkiksi kuvan 8.9 verkkojen $G_1$ ja $G_2$ vierusmatriisit ovat

$$A_{G_1} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \qquad A_{G_2} = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

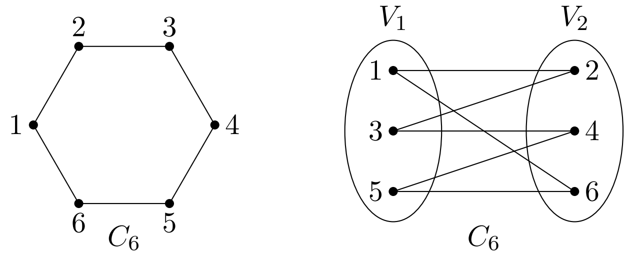
**Määritelmä 8.5.8.** Oletetaan, että $G = (V, E)$ on suunnattu tai suuntaamaton verkko, jossa ei ole yhtään silmukkaa eli $(v, v) \notin E$ kaikilla $v \in V$.

Jos $G$ on suunnattu verkko, sanotaan, että $G$ on *yksinkertainen suunnattu verkko.*

Jos $G$ on suuntaamaton verkko, sanotaan, että $G$ on *yksinkertainen verkko.*

Esimerkiksi kuvan 8.9 verkko $G_1$ on yksinkertainen suunnattu verkko ja verkko $G_2$ on yksinkertainen verkko. Seuraavaksi tarkastellaan vain yksinkertaisia verkkoja eli suuntaamattomia verkkoja, joissa ei ole silmukoita.

**Määritelmä 8.5.9.** Yksinkertainen verkko $G = (V, E)$ on *kaksijakoinen*, jos solmujen joukko $V$ voidaan jakaa kahdeksi erilliseksi ja epätyhjäksi joukoksi $V_1$ ja $V_2$ niin, että $V_1 \cup V_2 = V$ ja jokainen verkon $G$ viiva yhdistää solmut joukoista $V_1$ ja $V_2$.




Kuva 8.10: Yksinkertainen verkko $C_6$ on kaksijakoinen.

**Esimerkki 8.5.10.** Kuvasta 8.10 havaitaan, että verkko $C_6$ on kaksijakoinen, sillä sen solmujen joukko voidaan jakaa joukoiksi $V_1 = \{1, 3, 5\}$ ja $V_2 = \{2, 4, 6\}$, ja jokainen verkon $C_6$ viiva yhdistää solmut joukoista $V_1$ ja $V_2$.

**Lause 8.5.11.** *Yksinkertainen verkko on kaksijakoinen, jos ja vain jos sen solmut voidaan värittää kahdella värillä niin, etteivät mitkään kaksi vierekkäistä solmua ole samanvärisiä.*

*Todistus.* Oletetaan, että $G = (V, E)$ on yksinkertainen verkko.

"$\Rightarrow$": Oletetaan, että verkko $G$ on kaksijakoinen. Tällöin $V = V_1 \cup V_2$, missä joukot $V_1$ ja $V_2$ ovat erillisiä ja epätyhjiä ja lisäksi jokainen verkon $G$ viiva yhdistää solmun joukosta $V_1$ ja solmun joukosta $V_2$. Väritetään kaikki joukon $V_1$ solmut esimerkiksi punaiseksi ja kaikki joukon $V_2$ solmut mustiksi. Tällöin mitkään vierekkäiset solmut eivät ole samanvärisiä, sillä yksikään verkon $G$ viiva ei yhdistä kahta solmua joukosta $V_1$ tai kahta solmua joukosta $V_2$.

"$\Leftarrow$": Oletetaan, että verkon $G$ solmut voidaan värittää kahdella värillä (esimerkiksi vihreällä ja keltaisella) niin, etteivät mitkään kaksi vierekkäistä solmua ole samanvärisiä. Olkoon $V_1$ vihreällä väritettyjen solmujen joukko ja $V_2$ keltaisella väritettyjen solmujen joukko. Tällöin joukot $V_1$ ja $V_2$ ovat erillisiä ja epätyhjiä. Koska oletuksen mukaan mitkään vierekkäiset solmut eivät ole samanvärisiä, jokainen verkon $G$ viiva yhdistää solmut joukoista $V_1$ ja $V_2$. Siis $G$ on kaksijakoinen. □

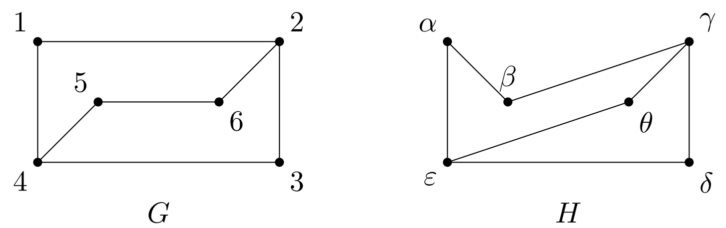
**Määritelmä 8.5.12.** Oletetaan, että $G_1 = (V_1, E_1)$ ja $G_2 = (V_2, E_2)$ ovat yksinkertaisia verkkoja. Verkot $G_1$ ja $G_2$ ovat *isomorfiset*, jos seuraavat ehdot toteutuvat:

(1) on olemassa bijektio $f : V_1 \to V_2$

(2) kaikilla $a, b \in V_1$ pätee, että solmut $a$ ja $b$ ovat vierekkäisiä verkossa $G_1$, jos ja vain jos solmut $f(a)$ ja $f(b)$ ovat vierekkäisiä verkossa $G_2$.

Kuvausta $f$ sanotaan tällöin *isomorfismiksi*.

**Esimerkki 8.5.13.** Kuvan 8.11 verkot $G$ ja $H$ ovat isomorfiset. Tutkimalla kuvaa 8.11 nimittäin huomataan, että verkon $H$ solmu $\theta$ voidaan kiepsauttaa solmujen $\alpha$ ja $\beta$ yläpuolelle, jolloin verkko $H$ näyttää samalta kuin verkko $G$.




Kuva 8.11: Verkot $G$ ja $H$ ovat isomorfiset.

Osoitetaan verkkojen $G$ ja $H$ isomorfisuus vielä täsmällisesti. Määritellään $F : \{1, 2, 3, 4, 5, 6\} \to \{\alpha, \beta, \gamma, \delta, \varepsilon, \theta\}$ seuraavasti:

$$F(1) = \theta \qquad F(2) = \gamma \qquad F(3) = \delta$$
$$F(4) = \varepsilon \qquad F(5) = \alpha \qquad F(6) = \beta.$$

Kuvaus $F$ on injektio, sillä mitään kaksi eri alkiota eivät kuvaudu samaksi. Kuvaus $F$ on myös surjektio, sillä jokaiselle maalin $\{\alpha, \beta, \gamma, \delta, \varepsilon, \theta\}$ alkiolle kuvautuu jokin alkio. Siis $F$ on bijektio.

Solmujen vierekkäisyyttä koskevan ehdon tutkimiseksi muodostetaan kummankin verkon vierusmatriisi. Verkon $G$ vierusmatriisi $A_G$ voidaan muodostaa tavalliseen tapaan. Verkon $H$ vierusmatriisissa $A_H$ järjestetään rivit ja sarakkeet kuvauksen $F$ mukaisesti järjestykseen $F(1)$, $F(2)$, $F(3)$, $F(4)$, $F(5)$, $F(6)$:

$$A_G: \quad \begin{array}{c|cccccc} & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 2 & 1 & 0 & 1 & 0 & 0 & 1 \\ 3 & 0 & 1 & 0 & 1 & 0 & 0 \\ 4 & 1 & 0 & 1 & 0 & 1 & 0 \\ 5 & 0 & 0 & 0 & 1 & 0 & 1 \\ 6 & 0 & 1 & 0 & 0 & 1 & 0 \end{array} \qquad A_H: \quad \begin{array}{c|cccccc} & \theta & \gamma & \delta & \varepsilon & \alpha & \beta \\ \hline \theta & 0 & 1 & 0 & 1 & 0 & 0 \\ \gamma & 1 & 0 & 1 & 0 & 0 & 1 \\ \delta & 0 & 1 & 0 & 1 & 0 & 0 \\ \varepsilon & 1 & 0 & 1 & 0 & 1 & 0 \\ \alpha & 0 & 0 & 0 & 1 & 0 & 1 \\ \beta & 0 & 1 & 0 & 0 & 1 & 0 \end{array}$$

Havaitaan, että näin muodostetut vierusmatriisit ovat samat. Tämä tarkoittaa, että kaikilla $a$, $b \in \{1, 2, 3, 4, 5, 6\}$ pätee, että solmut $a$ ja $b$ ovat vierekkäisiä verkossa $G$, jos ja vain jos solmut $F(a)$ ja $F(b)$ ovat vierekkäisiä verkossa $H$.

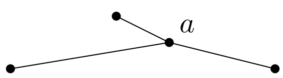
Näin on osoitettu, että isomorfisuuden määritelmän 8.5.12 molemmat ehdot täyttyvät. Siis edellä tarkasteltu kuvaus $F$ on isomorfismi ja verkot $G$ ja $H$ ovat isomorfiset.

**Lause 8.5.14.** *Oletetaan, että $G_1 = (V_1, E_1)$ ja $G_2 = (V_2, E_2)$ ovat yksinkertaisia verkkoja ja $f \colon V_1 \to V_2$ on isomorfismi. Tällöin*

- *verkoissa $G_1$ ja $G_2$ on yhtä monta solmua*
- *verkoissa $G_1$ ja $G_2$ on yhtä monta viivaa*
- *kaikilla $a \in V_1$ pätee, että $\deg(a) = \deg(f(a))$.*

*Todistus.* Oletuksen nojalla kuvaus $f \colon V_1 \to V_2$ on bijektio, joten joukossa $V_1$ ja $V_2$ on yhtä monta alkiota. Siis verkoissa $G_1$ ja $G_2$ on yhtä monta solmua.

Oletetaan, että $a \in V_1$. Solmun $a$ aste $\deg(a)$ on solmusta $a$ lähtevien viivojen lukumäärä. Se on siis sama kuin solmun $a$ vierekkäisten solmujen lukumäärä verkossa $G_1$.



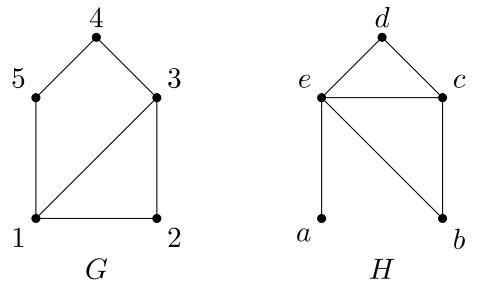

Kuva 8.12: Solmun $a$ aste on sama kuin solmun $a$ vierekkäisten solmujen lukumäärä.

Oletuksen nojalla kaikilla $a$, $b \in V_1$ pätee, että solmut $a$ ja $b$ ovat vierekkäisiä verkossa $G_1$, jos ja vain jos solmut $f(a)$ ja $f(b)$ ovat vierekkäisiä verkossa $G_2$. Tämä tarkoittaa, että solmulla $f(a)$ on verkossa $G_2$ yhtä monta vierekkäistä solmua kuin solmulla $a$ verkossa $G_1$. Solmusta $f(a)$ lähtee siis yhtä monta viivaa kuin solmusta $a$. Siis $\deg(f(a)) = \deg(a)$.

Koska $f\colon V_1 \to V_2$ on bijektio ja kaikilla $a \in V_1$ pätee, että $\deg(a) = \deg(f(a))$, on solmujen asteiden summa sama molemmissa verkoissa. Esimerkin 8.5.5 mukaan verkon viivojen määrä saadaan jakamalla solmujen asteiden summa kahdella. Tästä seuraa, että verkoissa $G_1$ ja $G_2$ on sama määrä viivoja. $\square$

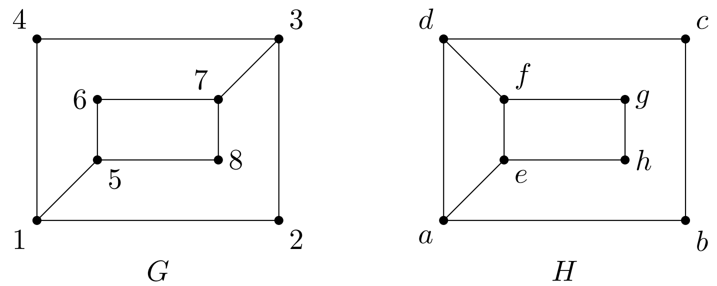
Lauseen 8.5.14 avulla voidaan joissakin tapauksissa osoittaa, että tarkasteltavat verkot eivät ole isomorfiset. Tätä havainnollistetaan seuraavassa esimerkissä.

**Esimerkki 8.5.15.** Tarkastellaan kuvan 8.13 verkkoja $G$ ja $H$. Niissä molemmissa on viisi solmua ja kuusi viivaa, mutta verkossa $G$ jokaisen solmun aste on vähintään kaksi, kun taas verkossa $H$ solmun $a$ aste on yksi eli $\deg(a) = 1$. Siis verkot $G$ ja $H$ eivät ole isomorfiset lauseen 8.5.14 nojalla.




Kuva 8.13: Verkot $G$ ja $H$ eivät ole isomorfiset.

**Esimerkki 8.5.16.** Tarkastellaan kuvan 8.14 verkkoja $G$ ja $H$. Niissä molemmissa on kahdeksan solmua ja kymmenen viivaa. Lisäksi kummassakin verkossa on neljä solmua, joiden aste on kaksi, ja neljä solmua, joiden aste on kolme.




Kuva 8.14: Verkot $G$ ja $H$ eivät ole isomorfiset.

Näytetään, etteivät verkot $G$ ja $H$ kuitenkaan ole isomorfiset. Tehdään vastaoletus, että ne ovat isomorfiset. Tällöin on olemassa isomorfismi $F\colon V_G \to V_H$ verkon $G$ solmujen joukosta verkon $H$ solmujen joukkoon.

Tarkastellaan verkon $G$ solmua 1, jonka aste on kolme. Lauseen 8.5.14 mukaan solmu 1 kuvautuu isomorfismissa $F$ joksikin verkon $H$ kolmiasteiseksi solmuksi eli solmuksi $a$, $d$, $e$ tai $f$. Havaitaan, että näistä jokaisella on kaksi vierekkäistä kolmiasteista solmua ja yksi vierekkäinen kaksiasteinen solmu. Esimerkiksi solmun $a$ vierussolmujen asteet ovat $\deg(d) = \deg(e) = 3$ ja $\deg(b) = 2$. Vastaava tilanne on solmuilla $d$, $e$ ja $f$.

Solmulla 1 puolestaan on kaksi vierekkäistä solmua, joiden aste on kaksi: solmut 2 ja 4. Lauseen 8.5.14 mukaan tällöin myös $\deg(F(2)) = \deg(F(4)) = 2$. Toisaalta isomorfisuuden määritelmän mukaan solmut $F(2)$ ja $F(4)$ ovat solmun $F(1)$ vierussolmuja verkossa $H$. Tämä on ristiriidassa sen kanssa, että verkon $H$ jokaisella kolmiasteisella solmulla on tasan yksi kaksiasteinen vierussolmu.

Vastaoletus johti ristiriitaan, joten alkuperäinen väite on tosi. Siis verkot $G$ ja $H$ eivät ole isomorfiset.

**Määritelmä 8.5.17.** Oletetaan, että $G$ on yksinkertainen verkko ja $n \in \mathbb{N}$, $n \geq 1$.

Verkon $G$ solmujen jono $v_1, \ldots, v_n$ on *polku* solmusta $v_1$ solmuun $v_n$, jos jonon jokaisesta solmusta on kaari jonon seuraavaan solmuun.

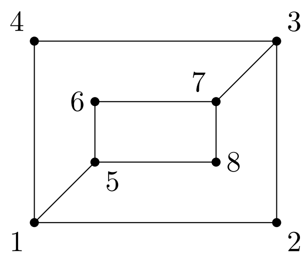
Polun $v_1, \ldots, v_n$ *pituus* on polkuun liittyvien kaarien lukumäärä eli $n - 1$.

Polku $v_1, \ldots, v_n$ on *sykli*, jos seuraavat ehdot toteutuvat:

(1) polun pituus on vähintään kaksi
(2) polun ensimmäinen ja viimeinen solmu ovat samat eli $v_1 = v_n$
(3) mikään muista solmuista $v_2, \ldots, v_{n-1}$ ei esiinny polussa useammin kuin kerran.

Polku on *yksinkertainen*, jos se on sykli tai jos mikään sen solmuista ei esiinny polussa useammin kuin kerran.

**Esimerkki 8.5.18.** Tarkastellaan kuvan 8.15 verkkoa $G$.




Kuva 8.15: Verkko $G$.

Polun $1, 4, 3, 7, 6, 5, 8, 7, 3, 2$ pituus on yhdeksän. Tämä polku ei ole sykli, koska sen ensimmäinen ja viimeinen solmu ovat eri solmut. Lisäksi esimerkiksi solmu 3 esiintyy polussa kaksi kertaa, joten polku ei ole yksinkertainen.

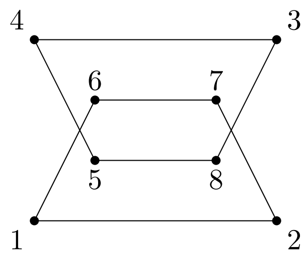
Polku $2, 3, 7, 6, 5, 1, 4$ on yksinkertainen, sillä mikään solmu ei esiinny siinä useammin kuin kerran. Sen pituus on kuusi. Tämäkään polku ei ole sykli, koska sen ensimmäinen ja viimeinen solmu ovat eri solmut.

Polun $8, 5, 1, 4, 3, 7, 8$ pituus on kuusi. Se on sykli, koska sen ensimmäinen ja viimeinen solmu ovat samat eikä mikään muista solmuista esiinny polussa useammin kuin kerran. Koska tämä polku on sykli, se on yksinkertainen.

Jono $1, 5, 7, 3$ ei ole verkon $G$ polku, koska verkossa $G$ ei ole kaarta solmusta 5 solmuun 7.

**Määritelmä 8.5.19.** Yksinkertainen verkko on *yhtenäinen*, jos sen minkä tahansa kahden eri solmun välillä on polku.

**Esimerkki 8.5.20.** Kuvan 8.15 verkko $G$ on yhtenäinen, mutta kuvan 8.16 verkko $H$ ei ole. Verkossa $H$ ei esimerkiksi ole polkua solmusta 4 solmuun 6.




Kuva 8.16: Verkko $H$.