

Johdatus yliopistomatematiikkaan

Lotta Oinonen, Johanna Rämö

Koonnut Johanna Rämö. Pohjana on käytetty Lotta Oinosen materiaalia Johdatus yliopistomatematiikkaan.

18. kesäkuuta 2025

Tämä moniste on lisensoitu Creative Commons BY-NC-SA-lisenssillä.

Itä-Suomen yliopisto
Fysiikan ja matematiikan laitos

Sisällys

I	Merkinnät ja työkalut	1
1	Perusasioita joukoista	1
1.1	Merkintöjä	1
1.2	Yhdiste, leikkaus ja erotus	2
1.3	Tyhjä joukko	3
1.4	Osajoukko	3
1.5	Joukkojen samuus	6
1.6	Perusjoukko ja komplementti	7
1.7	Potenssijoukko	8
1.8	Joukkojen karteeminen tulo eli tulojoukko	9
2	Lukujen käsittelyä	12
2.1	Jaollisuus, parillisuus ja parittomuus	12
2.2	Summamerkintä	13
3	Logiikkaa	16
3.1	Loogiset konnektiivit	16
3.2	Milloin propositiolauseet ilmaisevat saman asian? – Looginen ekvivalenssi	18
3.3	Kvanttorit	20
3.4	Kvanttorit ja negaatiot	22
3.5	Kvanttorien järjestys	23
II	Todistaminen	24
4	Väitteen kumoaminen vastaesimerkillä	24
5	Lausekkeisiin liittyviä todistuksia	26
5.1	Kuinka osoittaa kaksi lauseketta samoiksi?	26
5.2	Kuinka osoittaa, että lauseke on toista suurempi?	29
6	Implikaatio- ja ekvivalenssitodistukset	31
6.1	Implikaatiotodistus eli jos ... niin -väitteen todistaminen	31
6.2	Ekvivalenssitodistus eli jos ja vain jos -väitteen todistaminen	32
6.3	Ekvivalenssi ja yhtälönratkaisu	33
6.4	Osajoukoksi osoittaminen	36
6.5	Kahden joukon osoittaminen samoiksi	37
6.6	Erilaisten todistustyyppien yhdistelmät	39
7	Epäsuora todistaminen	40

7.1	Kontrapositiotodistus	40
7.2	Ristiriitatodistus	41
8	Matemaattinen induktio	44
III Kuvaukset ja relaatiot		56
9	Perusasioita kuvauksista	56
9.1	Kuvauksen määritelmä	56
9.2	Kuva	60
9.3	Alkukuva	63
9.4	Injektio	67
9.5	Surjektio	71
9.6	Yhdistetty kuvaus	77
9.7	Käänteiskuvaus ja bijektio	80
10	Työkaluja reaalifunktioiden rakentamisen	88
10.1	Potenssit ja juuret	88
10.2	Polynomit	90
10.3	Eksponentti- ja logaritmifunktiot	93
10.4	Trigonometriaa	99
11	Relaatiot	106
11.1	Mitä relaatiot ovat?	106
11.2	Relaation täsmällinen määritelmä	106
11.3	Ekvivalenssirelaatio	107
11.4	Ekvivalenssiluokat	109
11.5	Kuvaus relaationa	112
IV Kompleksiluvut		113
12	Kompleksiluvut	113
12.1	Kompleksilukujen esittely	113
12.2	Kompleksilukujen määritelmä	114
12.3	Mihin kompleksilukuja tarvitaan?	117
12.4	Kompleksiluvuilla laskeminen	118
12.5	Kompleksiluvun liittoluku ja itseisarvo	118
12.6	Kompleksiluvun käänteisluku ja kompleksilukujen osamäärä	121
12.7	Yhtälöiden ratkaisemisesta	124
12.8	Napaesitys	126
12.9	Eksponenttiesitys	135
12.10	Binomiyhtälö	139
12.11	Toisen asteen yhtälö	142

Luku I

Merkinnät ja työkalut

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

Taulukko 1.1: Lukujoukkoja.

Joukon kaikkien alkioiden luetteleminen ei ole aina mahdollista. Esimerkiksi merkinnästä $B = \{\dots, -6, -4, -2, 0, 2, 4, 6, \dots\}$ 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

$$B = \{m \in \mathbb{Z} \mid m = 2n \text{ missä } n \in \mathbb{Z}\} \quad \text{tai} \quad B = \{2n \mid n \in \mathbb{Z}\}.$$

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 $A = \{z \in \mathbb{Z} \mid |z| \leq 2\}$.

Kun joukko määritellään ehdon avulla, pystyviivan vasemmalla puolella kerrotaan, minkä tyyppisiä joukon alkioita ovat. Esimerkiksi merkinnästä $B = \{m \in \mathbb{Z} \mid m = 2n \text{ missä } n \in \mathbb{Z}\}$ nähdään, että joukon B alkioita ovat tyypiltään kokonaislukuja. Pystyviivan oikealle puolelle kirjoitetaan ehto, joka alkiolta 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

{alkioiden tyyppi | ehto, joka alkiolta 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

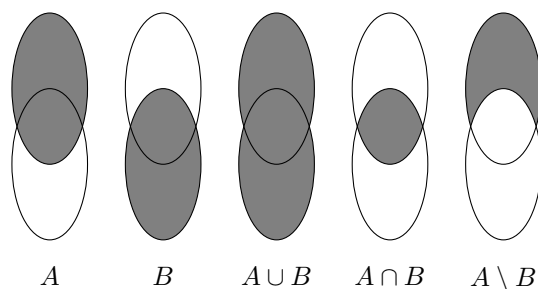
Joukoista voidaan muodostaa uusia joukkoja erilaisten joukko-operaatioiden avulla. Näistä yleisimmät on määritelty alla, ja niitä on havainnollistettu niin sanotuilla Vennin kaavioilla kuvassa 1.1.

Määritelmä 1.1. 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 $A \setminus B = \{x \mid x \in A \text{ ja } x \notin B\}$.

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

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

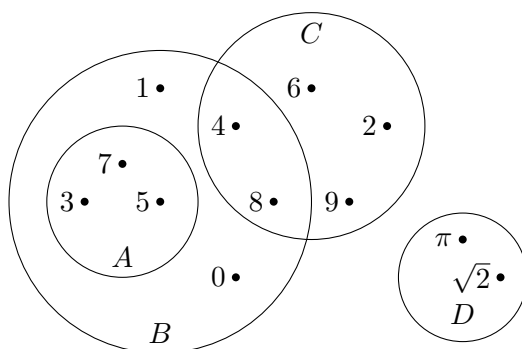


Kuva 1.1: Joukot A ja B sekä niiden yhdiste, leikkaus ja erotus tummennettuna.

Esimerkki 1.2. 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 $A \setminus B = \{0, 4\}$. Joukkojen B ja A erotus on $B \setminus A = \{1, 3\}$.

Jos kahdella joukolla ei ole yhteisiä alkioita, eli niiden leikkaus on tyhjä joukko, sanotaan, että kyseiset joukot ovat *erilliset*. Esimerkiksi kuvan 1.3 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 1.3 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.



Kuva 1.2: Joukot A ja C ovat erilliset. Joukot A ja C sekä joukot A ja B kohtaavat.

1.3 Tyhjä joukko

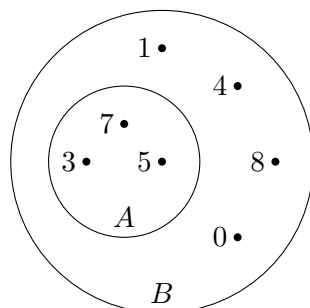
Joukko-operaatioiden tuloksena voi joskus olla joukko, johon ei kuulu yhtään alkioita. Esimerkiksi joukoilla $A = \{1, 2\}$ ja $B = \{3, 4\}$ ei ole yhteisiä alkioita, joten niiden leikkaus $A \cap B$ on joukko, jossa ei ole yhtään alkioita. Tällaista joukkoa sanotaan tyhjäksi joukoksi.

Määritelmä 1.3. *Tyhjä joukko* tarkoittaa joukkoa, jossa ei ole yhtään alkioita. 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

Kuvassa 1.3 on esitetty joukot $A = \{3, 5, 7\}$ ja $B = \{1, 3, 4, 5, 7, 8, 0\}$. Joukon A jokainen alkio kuuluu joukkoon B . Sanotaan, että A on joukon B *osajoukko*.



Kuva 1.3: Joukko A on joukon B osajoukko.

Määritelmä 1.4. 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 1.5. 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 1.6. 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 $\{5, -1\}$ alkioit yksitellen. Tämä ei kuitenkaan aina ole mahdollista, esimerkiksi jos tarkasteltavassa joukossa on loputtomasti alkioita. Myöhemmin luvussa 6.4 harjoitteleme yleisemmän tekniikan osajoukoksi osoittamiseen.

Esimerkki 1.7. Merkitään $B = \{x \in \mathbb{Z} \mid x^2 - x = 0\}$. Näytetään, että $\{1, 2\} \not\subset B$.

Tarkastellaan joukon $\{1, 2\}$ alkioita. 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 1.8. Oletetaan, että A on joukko. Päätellään, että $\emptyset \subset A$. 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. 1.7). Tyhjässä joukossa \emptyset ei kuitenkaan ole yhtään alkioita. Joukossa \emptyset ei siis ole sellaista alkioita, 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 1.7 esiteltävä potenssijoukon käsite on esimerkki tällaisesta tilanteesta. Seuraavassa esimerkissä havainnollistetaan osajoukon ja joukossa alkiona olevan joukon eroa.

Esimerkki 1.9. 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.

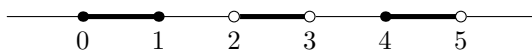
Havaitaan, että $A \subset X$, sillä $A = \{2, 3\}$, ja $2 \in X$ ja $3 \in X$ (jokainen joukon A alkio kuuluu joukkoon X). Toisaalta $B \not\subset X$, sillä $1 \in B$ mutta $1 \notin X$ (joukossa B on alkio 1, joka ei kuulu joukkoon X).

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 1.10. 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:

$$\begin{aligned}]a, b[&= \{x \in \mathbb{R} \mid a < x < b\} & [a, b] &= \{x \in \mathbb{R} \mid a \leq x \leq b\} \\ [a, b[&= \{x \in \mathbb{R} \mid a \leq x < b\} &]a, b] &= \{x \in \mathbb{R} \mid a < x \leq b\} \end{aligned}$$



Kuva 1.4: suljettu väli $[0, 1]$, avoin väli $]2, 3[$ ja puoliavoin väli $[4, 5[$

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

Määritelmä 1.11. Oletetaan, että c on reaaliluku. Tällöin

$$\begin{aligned}]-\infty, c[&= \{x \in \mathbb{R} \mid x < c\} &]c, \infty[&= \{x \in \mathbb{R} \mid x > c\} \\]-\infty, c] &= \{x \in \mathbb{R} \mid x \leq c\} & [c, \infty[&= \{x \in \mathbb{R} \mid x \geq c\} \end{aligned}$$

1.5 Joukkojen samuus

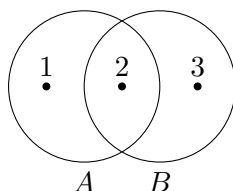
Edellisissä kappaleissa tutustuimme osajoukon määritelmään. Tässä kappaleessa tutkimme, milloin kaksi joukkoa ovat samat.

Määritelmä 1.12. Joukot A ja B ovat *samat*, jos niissä on täsmälleen samat alkiot eli kaikilla alkiolla x pätee seuraava: $x \in A$, jos ja vain jos $x \in B$. Tällöin merkitään $A = B$.

Esimerkki 1.13. Päteekö väite $(A \cup B) \setminus B = A$ kaikilla joukoilla A ja B ?

Oletetaan, että A ja B ovat joukkoja. 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 $A \cap B = \emptyset$. Jotta väite olisi totta, sen pitää kuitenkin päteä *kaikilla* joukoilla.



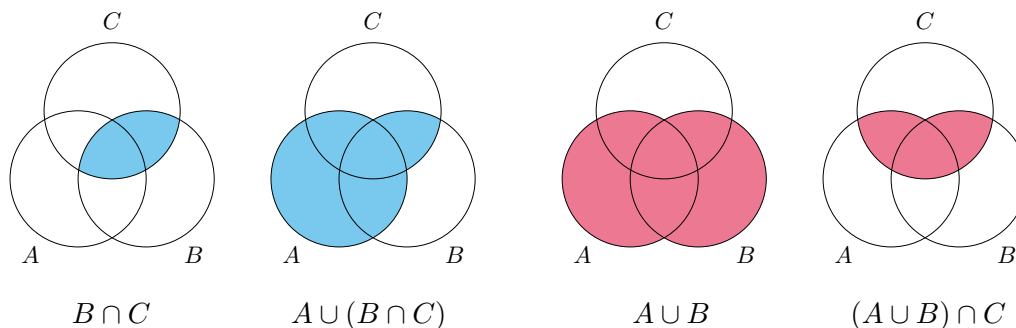
Kuva 1.5: On olemassa joukot A ja B , joilla väite $(A \cup B) \setminus B = A$ ei päde.

Joukkojen samuutta koskevia väitteitä on joskus hyödyllistä tutkia Vennin kaavioiden avulla.

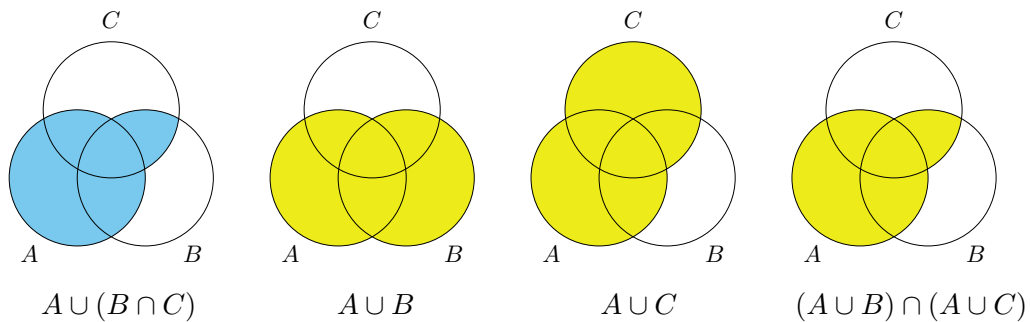
Esimerkki 1.14. Tutkitaan Vennin kaavioiden avulla, kumpi seuraavista yhtälöistä näyttäisi pätevän kaikilla joukoilla A , B ja C :

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

Vennin kaaviot kannattaa piirtää esimerkiksi vaiheittain kuten alla.



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



Kuva 1.7: 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 1.7 vasemmanpuolimmainen ja oikeanpuolimmainen Vennin kaavio ovat identtiset. Sen sijaan kuvassa 1.6 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. Myöhemmin luvussa 6.5 harjoittelemme todistustekniikan, jolla joukot voi osoittaa samoiksi ilman piirtämistä.

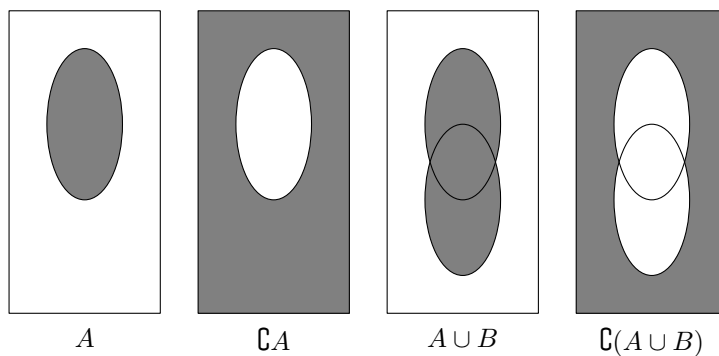
1.6 Perusjoukko ja komplementti

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

Määritelmä 1.15. 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 .



Kuva 1.8: 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 1.16. 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.

1.7 Potenssijoukko

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

Määritelmä 1.17. Oletetaan, että X on joukko. Joukon X *potenssijoukko* tarkoittaa sen kaikkien osajoukkojen muodostamaa joukkoa

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

Esimerkki 1.18. 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 1.19. 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. 1.8) eli erityisesti $\emptyset \subset Y$. Lisäksi joukko itse on itsensä osajoukko (esim. 1.9) 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 alkioita: \emptyset ja $\{3, 1, 4\}$. (Nämä alkioita ovat itsekin joukkoja, mutta siitä huolimatta ne ovat joukon Y alkioita). 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.

1.8 Joukkojen karteeminen 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) . Esimerkiksi $(-4, -5)$ on järjestetty pari samoin kuin $(\sqrt{17}, -101)$.

Järjestetyille pareille pätee

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

Siis esimerkiksi $(1 + 2, 2^3) = (3, 8)$ mutta $(3, 8) \neq (8, 3)$.

Järjestetyssä parissa (a, b) symbolit a ja b ovat niin kutsuttuja *komponentteja*. Jos komponentit ovat desimaalilukuja, on selkeintä käyttää komponenttien erottimena puolipistettä, jotta erilaiset pilkut eivät mene sekaisin. Voidaan siis esimerkiksi kirjoittaa $(-3,1; 2,54)$.

Järjestetyn parin käsitteen avulla voidaan määritellä joukkojen karteeminen tulo. Joukkojen A ja B karteesisessa tulossa $A \times B$ ovat alkioina kaikki mahdolliset järjestetyt parit, joissa ensimmäisenä komponenttina on joukon A alkio ja toisena komponenttina joukon B alkio.

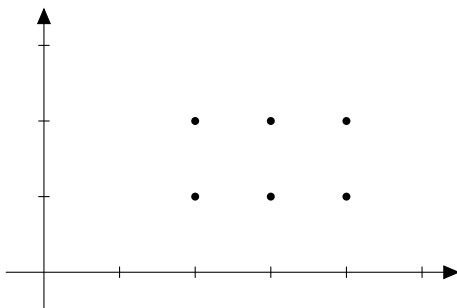
Määritelmä 1.20. Oletetaan, että A ja B ovat joukkoja. Joukkojen A ja B *karteeminen tulo* eli *tulojoukko* on joukko

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

Esimerkki 1.21. Määritetään joukkojen $C = \{2, 3, 4\}$ ja $D = \{1, 2\}$ karteeminen 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:

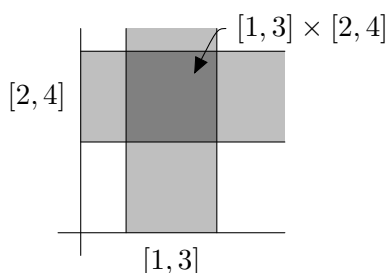


Kuva 1.9: Joukko $C \times D = \{(2, 1), (2, 2), (3, 1), (3, 2), (4, 1), (4, 2)\}$ koordinaatistossa.

Esimerkki 1.22. Hahmotellaan koordinaatiston avulla, miltä näyttää karteeminen tulo $[1, 3] \times [2, 4]$. Tässä $[1, 3]$ on suljettu väli, jota sisältää kaikki reaaliluvut lähtien luvusta 1 ja päättyen lukuun 3. Samoin $[2, 4]$ on suljettu väli.

Karteesisessa tulossa $[1, 3] \times [2, 4]$ on alkioina esimerkiksi $(1, 7/2)$, $(3/2, 10/3)$ ja $(1, 1; \pi)$. Koska suljetuilla väleillä on äärettömän monta reaalinlukua, tulee myös karteesiseen tuloon äärettömän monta alkioita.

Karteesisen tulon $[1, 3] \times [2, 4]$ alkioita ovat järjestettyjä pareja, joiden ensimmäinen komponentti on välillä $[1, 3]$. Kuvaan 1.10 hahmoteltu harmaa pystysuora kaistale kuvaa tällaisia järjestettyjä pareja. Toisen komponentin pitää puolestaan olla välillä $[2, 4]$. Tällaiset järjestetyt parit ovat vaakasuorassa harmaassa kaistaleessa. Karteesisessa tulossa ovat kaikki ne järjestetyt parit, jotka osuvat molempiin kaistaleisiin. Tämä alue on väritetty kuvassa tummanharmaalla.



Kuva 1.10: Joukko $[1, 3] \times [2, 4]$ koordinaatistossa havainnollistettuna.

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

Esimerkki 1.23. Merkitään $A = \{1, 2\}$. Joukon A potenssijoukko on sen kaikkien osajoukkojen muodostama joukko $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, A\}$. Määritellään joukko B asettamalla

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

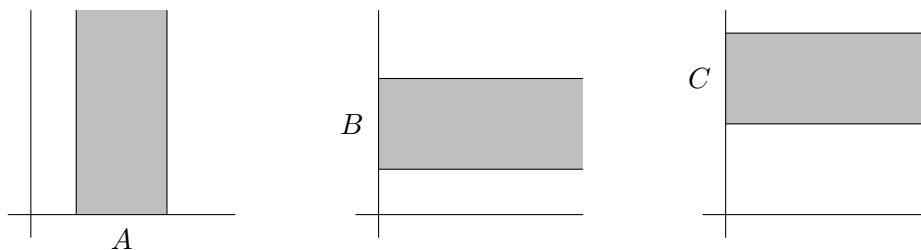
Havaitaan, että joukko B voidaan kirjoittaa myös luettelemalla siihen kuuluvat alkioita:

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

Vennin kaaviot eivät sovellu kovin hyvin tulojoukkoja koskevien yleisten väitteiden tutkimiseen. Tulojoukkoja voi kuitenkin havainnollistaa koordinaatiston avulla kuten jo aiemmin nähtiin. Seuraavassa esimerkissä tutkitaan kuvan avulla, miten karteesinen tulo suhtautuu muihin joukko-operaatioihin.

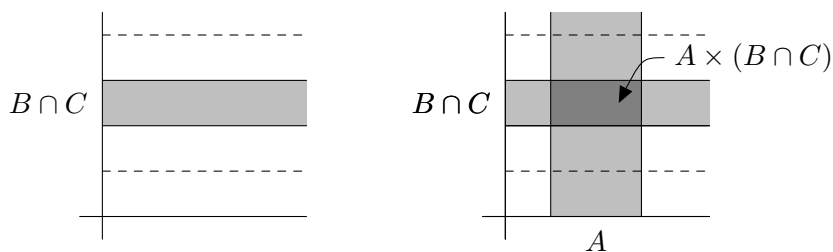
Esimerkki 1.24. Oletetaan, että A , B ja C ovat joukkoja. Havainnollistetaan piirroksella joukkoja $A \times (B \cap C)$ ja $(A \times B) \cap (A \times C)$.

Aloitetaan joukosta $A \times (B \cap C)$ ja toimitaan samalla tavalla kuin esimerkissä 1.22.



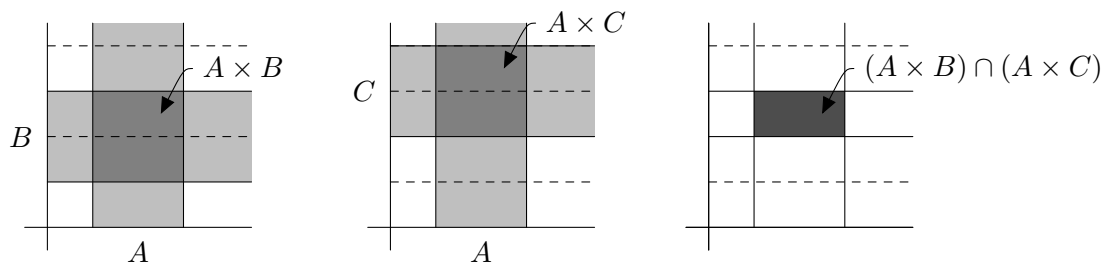
Kuva 1.11: Joukot A , B ja C .

Leikkausta $B \cap C$ vastaava vaakasuora kaistale on kuvassa 1.12. Tulojoukko $A \times (B \cap C)$ on joukkoa A vastaavan kaistaleen ja joukkoa $B \cap C$ vastaavan kaistaleen leikkaus, joka on merkitty kuvaan 1.12 tummanharmaalla.



Kuva 1.12: 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 1.13 tummanharmaalla. Kuvassa 1.13 näkyy havainnollistus myös tulojoukolle $A \times C$. Niiden leikkauksena saadaan joukko $(A \times B) \cap (A \times C)$.



Kuva 1.13: Joukot $A \times B$, $A \times C$ ja $(A \times B) \cap (A \times C)$.

Esimerkin 1.24 havainnollituksen perusteella joukot $A \times (B \cap C)$ ja $(A \times B) \cap (A \times C)$ näyttävät olevan samat. Tämä väite voidaan osoittaa täsmällisesti sitten, kun opitaan todistustekniikoita luvussa 6.

2 Lukujen käsittelyä

Tässä luvussa esitellään lukuja koskevia käsitteitä ja tekniikoita, joita tullaan tarvitsemaan todistusten rakentamisessa. Ensin tutustutaan jaollisuuteen ja sen jälkeen summamerkinnän käsittelyyn.

2.1 Jaollisuus, parillisuus ja parittomuus

Jotkin kurssilla käsiteltävistä väitteistä koskevat jaollisuutta sekä parillisia ja parittomia lukuja. Jotta voidaan laatia näitä koskevia täsmällisiä todistuksia, tarvitaan käsitteille määritelmät.

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 2.1. 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 $m \nmid z$.

Esimerkki 2.2. Oletetaan, että $k \in \mathbb{Z}$. Tällöin lauseke $6k^2 + 3(-4 + 2k)$ on jaollinen kolmella, sillä

$$6k^2 + 3(-4 + 2k) = 3(2k^2 - 4 + 2k)$$

ja $2k^2 - 4 + 2k \in \mathbb{Z}$. Toisin sanoen $3 \mid 6k^2 + 3(-4 + 2k)$.

Määritelmä 2.3. 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 $35 = 5 \cdot 7$.

Jos kokonaisluku on jaollinen kahdella, se on pariton. Muussa tapauksessa luku on pariton.

Määritelmä 2.4. 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 $6 \in \mathbb{Z}$.

Tarkastellaan sitten hiukan abstraktimpaa tapausta.

Esimerkki 2.5. Oletetaan, että $k \in \mathbb{Z}$. Osoitetaan parittomuuden määritelmän avulla, että lauseke $3(k + 1) + 5k$ on pariton. Tämä tehdään muuttamalla lauseke muotoon $2a + 1$, missä

a on jokin kokonaisluku. Etukäteen ei voi tietää, mikä tulee luvun a tilalle, vaan se selviää matkan varrella.

Aloitetaan sieventämällä lauseketta:

$$3(k+1) + 5k = 3k + 3 + 5k = 8k + 3.$$

Erotetaan lausekkeesta termi $+1$, jolloin saadaan

$$8k + 3 = 8k + 2 + 1.$$

Nyt voidaan vielä ottaa luku 2 yhteiseksi tekijäksi, jolloin lauseke saadaan haluttuun muotoon:

$$8k + 2 + 1 = 2(4k + 1) + 1.$$

On siis osoitettu, että

$$3(k+1) + 5k = 2(4k + 1) + 1,$$

$4k + 1 \in \mathbb{Z}$. Lauseke on siis pariton.

Edellisessä esimerkissä saattaa jo varhaisemmassa vaiheessa nähdä, että luku on pariton. Joku voisi päätellä, että koska $8k$ on parillinen ja 3 on pariton, niiden summa on pariton. Tämä päättely ei ole väärin. Tässä tehtävässä oli kuitenkin tavoitteena harjoitella juuri määritelmän käyttöä, minkä vuoksi lausekkeen muokkausta piti jatkaa pidemmälle. Lisäksi tällä kurssilla ei ole osoitettu, että parillisen ja parittoman luvun summa on pariton. Kyseinen päättelyaskel olisi ollut siis iso hyppy ilman kunnollisia perusteluita.

Edellisessä esimerkissä alusta asti tavoitteena oli osoittaa, että luku on pariton. Usein tehtävissä ei kuitenkaan tiedä, onko luku parillinen tai pariton. Tällöin täytyy ensin kokeilemalla tai arvaamalla selvittää, onko kyse parillisesta vai parittomasta luvusta, ja tämän jälkeen osoittaa väite täsmällisesti.

2.2 Summamerkintä

Matematiikassa saatetaan käsitellä pitkiä summia kuten vaikkapa summaa

$$2 + 4 + 6 + 8 + \dots + 24.$$

Tällaisten summien kirjoittaminen ja muokkaaminen on tehokkaampaa summamerkin avulla:

$$2 + 4 + 6 + 8 + \dots + 24 = \sum_{j=1}^{12} 2j.$$

Summamerkinnässä symbolin j paikalle sijoitetaan luvut $1, 2, \dots, 12$ ja saadut lausekkeet lasketaan yhteen: $2 \cdot 1 + 2 \cdot 2 + 2 \cdot 2 + \dots + 2 \cdot 12$.

Esimerkki 2.6. Lasketaan summan

$$\sum_{j=0}^5 j - 3$$

arvo. Sijoitetaan symbolin j tilalle kokonaisluvut lähtien luvusta 0 ja päättyen lukuun 5. Näin saadut luvut summataan yhteen:

$$\begin{aligned}\sum_{j=0}^5 j - 3 &= (0 - 3) + (1 - 3) + (2 - 3) + (3 - 3) + (4 - 3) + (5 - 3) \\ &= -2 - 1 + 0 + 1 + 2 = 0.\end{aligned}$$

Seuraavassa esimerkissä summaaminen ei pääty mihinkään tiettyyn lukuun, vaan yleiseen kokonaislukuun n .

Esimerkki 2.7. Kirjoitetaan auki summamerkintä

$$\sum_{j=3}^n 5j^2 + 1.$$

Sijoitetaan symbolin j tilalle kokonaisluvut lähtien luvusta 3 ja päättyen lukuun n . Saadaan

$$\sum_{j=3}^n 5j^2 + 1 = (5 \cdot 3^2 + 1) + (5 \cdot 4^2 + 1) + (5 \cdot 5^2 + 1) + \cdots + (5n^2 + 1).$$

Aiemmissa esimerkeissä niin kutsuttuna *summausindeksinä* käytettiin symbolia j . Mikä tahansa muukin symboli käy summausindeksiksi.

Esimerkki 2.8. Kirjoitetaan summamerkinnän avulla summa

$$5 + 8 + 11 + 14 + 17 + 20.$$

Summassa luvut esiintyvät kolmen välein, joten summattavaan kannattaa yrittää kirjoittaa kolmen monikerta. Lisäksi summaamisen pitää alkaa luvusta 5, jonka voi kirjoittaa muodossa $5 = 3 \cdot 1 + 2$. Siksi summausindeksi lähtee liikkeelle luvusta 1.

Testataan, tuottaako summa

$$\sum_{i=1}^6 3i + 2$$

halutun tuloksen. Nähdään, että

$$\begin{aligned}\sum_{i=1}^6 3i + 2 &= (3 \cdot 1 + 2) + (3 \cdot 2 + 2) + (3 \cdot 3 + 2) + (3 \cdot 4 + 2) + (3 \cdot 5 + 2) + (3 \cdot 6 + 2) \\ &= 5 + 8 + 11 + 14 + 17 + 20\end{aligned}$$

niin kuin pitääkin.

Summan voi kirjoittaa usealla eri tavalla summamerkinnän avulla. Myös esimerkiksi

$$\sum_{i=0}^5 3i + 5$$

tuottaa halutun tuloksen.

Usein on hyödyllistä muuntaa yksi summamerkintä toisenlaiseksi summamerkinnäksi. Tätä tarvitaan todistusten välivaiheena erityisesti niin kutsutuissa induktiotodistuksissa, joita käsitellään luvussa 8.

Esimerkki 2.9. Osoitetaan, että

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

Toisin sanoen summasta on mahdollista irrottaa viimeinen summattava erilleen.

Osoitetaan väite lähtemällä liikkeelle yhtälön vasemmasta puolesta ja päätymällä oikeaan. Kirjoitetaan ensin vasen puoli auki:

$$\sum_{i=0}^{k+1} 2i = 0 + 2 + 4 + \cdots + 2(k+1).$$

Tavoitteena on saada aikaan summa, jossa summataan vain symboliin k asti. Kirjoitetaan näkyviin toiseksi viimeinen summattava, jolloin haluttu summa tulee näkyviin:

$$\begin{aligned} 0 + 2 + 4 + \cdots + 2(k+1) &= 0 + 2 + 4 + \cdots + 2k + 2(k+1) \\ &= (0 + 2 + 4 + \cdots + 2k) + 2(k+1) \\ &= \sum_{i=0}^k +2i + 2(k+1). \end{aligned}$$

On siis osoitettu, että

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

3 Logiikkaa

Tässä luvussa tutustutaan joihinkin logiikan käsitteisiin ja merkintöihin.

3.1 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 3.2.

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

Taulukko 3.2: 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* $p_0, p_1, p_2 \dots$, 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 3.2 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 3.1. Negaatiolla \neg on seuraava totuustaulu:

A	$\neg A$
1	0
0	1

Määritelmän 3.1 totuustaulusta nähdään, että negaatio vaihtaa propositiolauseen totuusarvon: jos propositiolause on tosi, on sen negaatio epätosi, ja päinvastoin. Merkintä $\neg A$ luetaan ”ei A ”.

Määritelmä 3.2. Konjunktioilla \wedge ja disjunktioilla \vee on seuraavat totuustaulut:

A	B	$A \wedge B$	A	B	$A \vee B$
1	1	1	1	1	1
1	0	0	1	0	1
0	1	0	0	1	1
0	0	0	0	0	0

Määritelmän 3.2 totuustaulusta nähdään, että konjunktio $A \wedge B$ (luetaan ” A ja B ”) on tosi täsmälleen siinä tapauksessa, että propositiolauseet A ja B ovat molemmat tosia. Konjunktio 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 jälkiruokan, 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 3.2 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 3.3. Implikaatiolla \rightarrow ja ekvivalenssilla \leftrightarrow on seuraavat totuustaulut:

A	B	$A \rightarrow B$	A	B	$A \leftrightarrow B$
1	1	1	1	1	1
1	0	0	1	0	0
0	1	1	0	1	0
0	0	1	0	0	1

Määritelmän 3.3 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 3.3 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 3.4. Havainnollistetaan implikaation määritelmää tarkastelemalla lupausta ”jos saat kokeesta vähintään 40 pistettä, niin pääset kurssista läpi”. Se voidaan kirjoittaa propositiolauseena $p_0 \rightarrow p_1$, 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 3.3 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 3.3 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 3.3 implikaation totuustaulun alinta riviä. Tässäkään tapauksessa lupaus ei ole rikottu.

Tarkasteltava implikaatio on epätosi ainoastaan tilanteessa, jossa saat kokeesta vähintään 40 pistettä mutta et kuitenkaan pääse kurssia läpi. Tällöin lupaus ei ole pidetty. Tilanne vastaa määritelmän 3.3 implikaation totuustaulun toista riviä, jossa etujäsen on tosi ja takajäsen epätosi.

3.2 Milloin propositiolauseet ilmaisevat saman asian? – Looginen ekvivalenssi

Joskus kaksi propositiolauseetta voivat ilmaista saman asian mutta eri tavalla. Tällä kurssilla asiaa pitää miettiä erityisesti kahdessa tapauksessa: lauseiden negaatioiden sekä implikaatioiden kohdalla. Käsitellään asiaa ensin kautta ja sitten esitetään tarkemmat perustelut totuustaulujen avulla. Aloitetaan lauseiden negaatioista.

Tarkastellaan vaikkapa lausetta ”Tänään uin ja syön jäätelön.” Tällöin päivän ohjelma menee pieleen siinä tapauksessa, että en mene uimaan tai en syö jäätelöä. Kumman tahansa asian puuttuminen tekee lauseesta epätoden. Lauseen negaatio on ”Tänään ei ui tai en syö jäätelöä.” Negaatiota muodostettaessa ja-sana muuttuu siis tai-sanaksi. Ilmaistaan sama vielä loogisten konnektiivien avulla. Merkitään lausetta ”Tänään uin.” symbolilla A ja lausetta ”Tänään syön jäätelön.” symbolilla B . Nyt lauseella $\neg(A \wedge B)$ on sama merkitys kuin lauseella $\neg A \vee \neg B$.

Sama pätee myös toisin päin. Lauseen ”Haluan mehun tai teen.” negaatio on ”En halua mehua ja en halua teetä.” Tai-sana muuttuu siis ja-sanaksi, kun muodostetaan lauseen negaatio. Loogisten konnektiivien avulla ilmaistuna lauseella $\neg(A \vee B)$ on sama merkitys kuin lauseella $\neg A \wedge \neg B$.

Siirrytään sitten implikaatioon eli jos . . . niin -muotoisten väitteiden tarkasteluun. Lauseen ”Jos sataa, taivaalla on pilviä” kanssa saman asian ilmaisee lause ”Jos taivaalla ei ole pilviä, ei sada.” Lauseilla $A \rightarrow B$ sekä $\neg B \rightarrow \neg A$ on siis sama merkitys.

Alaluvun loppuosa käsittelee edellisten esimerkkien ilmiöitä täsmällisesti Propositiolauseita, jotka ilmaisevat saman asian kutsutaan *loogisesti ekvivalenteiksi*. Tämän käsitteen avulla voidaan osoittaa, että esimerkkilauseet tosiaan ilmaisevat saman asian.

Määritelmä 3.5. Propositiolauseet A ja B ovat loogisesti ekvivalentteja, jos ekvivalenssin $A \leftrightarrow B$ totuusarvo on aina 1.

Ekvivalenssin $A \leftrightarrow B$ totuusarvo on 1 täsmälleen silloin, kun propositionaalisilla A ja B on sama totuusarvo. Loogisesti ekvivalenttien propositionaalisien totuusarvot ovat siis aina samat.

Aloitetaan osoittamalla, että negaatio muuttaa ja-sanaksi kuten esimerkin kohdalla huomattiin.

Esimerkki 3.6. Merkitään lausetta ”Tänään uin.” symbolilla A ja lausetta ”Tänään syön jäätelön.” symbolilla B . Nyt tutkittavat propositionaaliset ovat $\neg(A \wedge B)$ ja $\neg A \vee \neg B$. Osoitetaan, että nämä ovat loogisesti ekvivalentteja. 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 propositionaalisilla $\neg(A \wedge B)$ ja $\neg A \vee \neg B$ on aina samat totuusarvot, joten niiden ekvivalenssin totuusarvo on aina 1. Propositionaaliset $\neg(A \wedge B)$ ja $\neg A \vee \neg B$ ovat siis loogisesti ekvivalentit. Voidaan ajatella, että ne ilmaisevat saman asian mutta eri tavoilla.

Käsitellään vielä toistakin esimerkkiä negaatiosta. Siinä nähdään, kuinka implikaation negaation voi ilmaista konjunktion avulla.

Esimerkki 3.7. Yritetään etsiä implikaation negaation $\neg(A \rightarrow B)$ kanssa loogisesti ekvivalentti propositionaalisuus. Alla olevasta totuustaulusta nähdään, että implikaatio $A \rightarrow B$ on epätosi täsmälleen siinä tilanteessa, että propositionaalisuus A on tosi ja B on epätosi:

A	B	$A \rightarrow B$
1	1	1
1	0	0
0	1	1
0	0	1

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

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

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

Esimerkiksi implikaation ”jos aurinko paistaa, lähdän kävelyllä” negaatio on esimerkin 3.7 mukaan loogisesti ekvivalentti lauseen ”aurinko paistaa ja en lähde kävelyllä” kanssa. Huomaa, että implikaation negaatio vastaa tilannetta, jossa alkuperäisen implikaation etujäsen on tosi mutta takajäsen ei.

Lopuksi näytetään, että implikaation voi kirjoittaa myös toisella tavalla, niin kutsutun *kontrapositio* avulla. Tässä esimerkissä ei siis muodosteta implikaation negaatiota, vaan ainoastaan kirjoitetaan implikaatio uudessa muodossa.

Esimerkki 3.8. Implikaation $A \rightarrow B$ *kontrapositio* tarkoittaa implikaatiota $\neg B \rightarrow \neg A$. Esimerkiksi implikaation ”Jos sataa, taivaalla on pilviä.” kontrapositio on ”Jos taivaalla ei ole pilviä, ei sada.”. Osoitetaan totuustaulun avulla, että implikaatio ja sen kontrapositio ovat loogisesti ekvivalentit. Molemmat lauseet kertovat siis saman asian mutta eri sanoin.

A	B	$A \rightarrow B$	$\neg B$	$\neg A$	$\neg B \rightarrow \neg A$	$(A \rightarrow B) \leftrightarrow (\neg B \rightarrow \neg A)$
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

Propositiolauseita, joka on aina tosi, sanotaan *tautologiaksi*. Tautologia tarkoittaa siis propositiolauseita, jonka totuusarvo on aina 1. Propositiolauseet A ja B ovat siis loogisesti ekvivalentteja, jos $A \leftrightarrow B$ on tautologia.

3.3 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 3.3.

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

Taulukko 3.3: Kvanttorit

Esimerkki 3.9. 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: $\forall x(x < 2 \rightarrow x^2 < 4)$

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 3.10. 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 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 $\forall x(x \in A \rightarrow x \in B)$.

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 $\exists x(x \in B \wedge x \notin C)$.

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: $\forall x(x \in A \cap B \rightarrow x \in B \setminus C)$. Yhdistämällä tähän leikkauksen ja joukkojen erotuksen määritelmät (ks. määritelmä 1.1) voidaan väite kirjoittaa muodossa $\forall x((x \in A \wedge x \in B) \rightarrow (x \in B \wedge x \notin C))$.

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

Määritelmän 1.12 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 $\forall x((x \in A \wedge x \notin B) \leftrightarrow (x \in C \vee x \in D))$.

3.4 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 $\neg\forall xA$ ja $\exists x\neg A$ ovat loogisesti ekvivalentteja, samoin kaavat $\neg\exists xA$ ja $\forall x\neg A$.

Kvanttoreita sisältävien väitteiden loogista ekvivalenssia ei voi tutkia totuustaulujen avulla. Lisätietoja predikaattilogiikan loogisen ekvivalenssin käsitteestä löytyy esimerkiksi kirjasta [Logiikka I](#)

Esimerkki 3.11. Alla olevaan taulukkoon on koottu joitakin väitteitä ja niiden negaatioita sekä suomeksi että logiikan symbolikielellä.

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

Esimerkki 3.12. Monimutkaisempien väitteiden negaatioita voidaan muokata vaiheittain. Tarkastellaan esimerkiksi väitettä ”kaikki iloiset ovat ahkeria”. Logiikan symbolikielellä sama asia voidaan ilmaista kaavana $\forall x(I(x) \rightarrow A(x))$. Etsitään tämän kaavan negaation kanssa loogisesti ekvivalentti kaava.

Negaatio $\neg\forall x(I(x) \rightarrow A(x))$ voidaan esimerkin 3.11 tapaan kirjoittaa loogisesti ekvivalenttissa muodossa $\exists x\neg(I(x) \rightarrow A(x))$. Implikaation negaatio $\neg(I \rightarrow A)$ on puolestaan loogisesti ekvivalentti konjunktin $I \wedge \neg A$ kanssa (esim. 3.7). 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.	$\forall x(I(x) \rightarrow A(x))$
Negaatio:	Joku on iloinen mutta ei ole ahkera.	$\exists x(I(x) \wedge \neg A(x))$

Esimerkki 3.13. 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 ekvivalentti kaava.

Negaatio $\neg \exists x(I(x) \wedge A(x))$ voidaan esimerkin 3.11 tapaan kirjoittaa loogisesti ekvivalentissa muodossa $\forall x \neg(I(x) \wedge A(x))$. Konjuktin negaatio $\neg(I \wedge A)$ on puolestaan loogisesti ekvivalentti disjuktin $\neg I \vee \neg A$ kanssa (esim. 3.6). 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 konjuktin negaatio $\neg(I \wedge A)$ on loogisesti ekvivalentti myös implikaation $I \rightarrow \neg A$ kanssa. Tämä voidaan päätellä myös esimerkistä 3.12 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.	$\forall x(I \rightarrow \neg A)$

3.5 Kvanttorien järjestys

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

Esimerkki 3.14. 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.

Luku II

Todistaminen

4 Väitteen kumoaminen vastaesimerkillä

Tässä luvussa tutustutaan todistustekniikkaan, jolla voi osoittaa väitteen vääräksi. 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 $a, b \in \mathbb{R}$ pätee, että $(a + b)^2 = a^2 + b^2$.
- Kaikilla joukoilla A ja B pätee, että $(A \cup B) \setminus B = A$.
- Kaikilla $n \in \mathbb{Z}$ pätee, että luku $n^2 - n + 11$ on alkuluku.

Tällaisten väitteiden kumoaminen onnistuu vastaesimerkin avulla. Sitä havainnollistetaan seuraavissa esimerkeissä.

Esimerkki 4.1. 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 4.2. 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 $A \cup (B \cap C) = (A \cup B) \cap C$.

Seuraavassa esimerkissä tarvitaan alkuluvun käsitettä, joka esiteltiin määritelmässä 2.3. Alkuluvun ainot positiiviset tekijät ovat 1 ja luku itse.

Esimerkki 4.3. Tarkastellaan väitettä, jonka mukaan luku $n^2 - n + 11$ on alkuluku kaikilla $n \in \mathbb{Z}$. Osoitetaan väite epätodeksi antamalla vastaesimerkki. Kokeilemalla tai muuten järjelemällä 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.

5 Lausekkeisiin liittyviä todistuksia

Tässä luvussa kerrotaan, kuinka kaksi lauseketta osoitetaan samoiksi ja kuinka osoitetaan, että lauseke on toista suurempi.

5.1 Kuinka osoittaa kaksi lauseketta samoiksi?

Tässä alaluvussa tutkitaan, kuinka osoittaa kaksi lauseketta samoiksi tai lauseke toista suuremmaksi. Tätä tarvitaan usein todistusten välivaiheissa. Asioita saatetaan käsitellä eri tavalla kuin mihin olet koulussa tai aiemmissa opinnoissasi tottunut. Tämä johtuu siitä, että nyt kiinnitetään erityistä huomiota siihen, päättelyiden loogiseen perustaan eli siihen *miksi* päättelyt toimivat. Tällöin päättelyt ovat yleistettävissä monenlaisiin ja monimutkaisiinkin tilanteisiin.

Oletetaan, että $a, b \in \mathbb{R}$. Osoitetaan, että $(a + b)^2 = a^2 + 2ab + b^2$:

$$\begin{aligned}(a + b)^2 &= a^2 + 2ab + b^2 \\(a + b)(a + b) &= a^2 + 2ab + b^2 \\aa + ab + ba + bb &= a^2 + 2ab + b^2 \\a^2 + ab + ab + b^2 &= a^2 + 2ab + b^2 \\a^2 + 2ab + b^2 &= a^2 + 2ab + b^2 \\a^2 + 2ab + b^2 - (a^2 + 2ab + b^2) &= 0 \\0 &= 0.\end{aligned}$$

Koska päädytään lopputulokseen, joka on aina tosi, väite pätee. Vai olemmeko itse asiassa todistaneet yhtään mitään?

Ennen kuin pureudutaan edellisen todistuksen ongelmiin, tutkitaan toista esimerkkiä. Osoitetaan, että $3 = 17$:

$$\begin{aligned}3 &= 17 && \parallel \cdot 0 \\0 \cdot 3 &= 0 \cdot 17 \\0 &= 0.\end{aligned}$$

Päädytään lopputulokseen $0 = 0$, joka on aina tosi. Siis $3 = 17$.

Edellinen todistus ei varmastikaan ole pätevä. Sen rakenne on aivan samanlainen kuin ensimmäisen todistuksen, joten ensimmäisessä todistuksessa on jotain pielessä.

Ensimmäinen ongelmana on, että kummassakaan todistuksessa ei ole kerrottu, miten allekain kirjoitetut yhtälöt riippuvat toisistaan. Kirjoitetaan jälkimmäisen todistuksen yhtälöketju uudelleen käyttäen implikaatio- ja ekvivalenssinuolia:

$$\begin{aligned}3 &= 17 \\ \Rightarrow \quad 0 \cdot 3 &= 0 \cdot 17 \\ \Leftrightarrow \quad 0 &= 0.\end{aligned}$$

Olemme siis itse asiassa osoittaneet, että *jos* $3 = 17$, *niin* $0 = 0$. Toisin sanoen lähdimme liikkeelle väitteestä ($3 = 17$) ja lopputuloksi tuli jotain, joka jo tiedettiin ($0 = 0$). Matemaattisen todistuksen pitäisi kulkea aivan toiseen suuntaan! Sen, mitä halutaan todistaa, on oltava lopputulos. Siksi todistus ei toimi.

Kirjoitetaan sitten uudelleen todistuksista ensimmäinen. Nyt jokaisen väliin sopiikin ekvivalenssinuoli:

$$\begin{aligned} & (a + b)^2 = a^2 + 2ab + b^2 \\ \Leftrightarrow & (a + b)(a + b) = a^2 + 2ab + b^2 \\ \Leftrightarrow & aa + ab + ba + bb = a^2 + 2ab + b^2 \\ \Leftrightarrow & a^2 + ab + ab + b^2 = a^2 + 2ab + b^2 \\ \Leftrightarrow & a^2 + 2ab + b^2 = a^2 + 2ab + b^2 \\ \Leftrightarrow & a^2 + 2ab + b^2 - (a^2 + 2ab + b^2) = 0 \\ \Leftrightarrow & 0 = 0. \end{aligned}$$

Nyt tiedetään, että väite $0 = 0$ on yhtäpitävä väitteen $(a + b)^2 = a^2 + 2ab + b^2$ kanssa. Koska $0 = 0$ pätee, myös $(a + b)^2 = a^2 + 2ab + b^2$ pätee.

Vaikka edellinen todistus on loogisesti pätevä, se on melko monimutkainen. Jokaisen ekvivalenssinuolen kohdalla on tarkistettava, että edellisestä väitteestä seuraa jälkimmäinen ja jälkimmäisestä edellinen. Tuntuu myös hieman kummalliselta, että yhtälön oikea puoli pysyy samanlaisena lähes todistuksen loppuun saakka.

Kirjoitetaan edellä esitetty todistus uudelleen järkevämmällä ja helpommalla tavalla

Esimerkki 5.1. Osoitetaan, että $(a + b)^2 = a^2 + 2ab + b^2$. Lähdetään liikkeelle yhtälön vasemmasta puolesta ja muokataan sitä:

$$\begin{aligned} (a + b)^2 &= (a + b)(a + b) \\ &= aa + ab + ba + bb \\ &= a^2 + ab + ab + b^2 \\ &= a^2 + 2ab + b^2. \end{aligned}$$

Näin olemme osoittaneet, että $(a + b)^2 = a^2 + 2ab + b^2$.

Huomaa, että ekvivalenssinuolia ei itse asiassa tarvittu lainkaan.

Jos lausekkeet ovat monimutkaisia, suoraviivaisin tapa niiden samaksi osoittamiseen on laskea erikseen auki vasen ja oikea puoli ja todeta, että tulos on sama. Tutkitaan, kuinka tämä tapahtuu käytännössä.

Esimerkki 5.2. Oletetaan, että $n \in \mathbb{N}$. Osoitetaan, että

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

Ryhdytään muokkaamaan yhtälön vasenta puolta:

$$\frac{n^2 + n}{2} + n + 1 = \frac{n^2 + n}{2} + \frac{2n + 2}{2} = \frac{n^2 + n + 2n + 2}{2} = \frac{n^2 + 3n + 2}{2}.$$

Tämän pidemmälle on vaikea edetä, joten siirrytään oikeaan puoleen.

Yhtälön oikeaa puolta muokkaamalla saadaan

$$\frac{(n + 1)^2 + (n + 1)}{2} = \frac{n^2 + 2n + 1 + n + 1}{2} = \frac{n^2 + 3n + 2}{2}.$$

Koska vasemmasta ja oikeasta puolesta saadaan sama tulos, pätee yhtälö. Tosin sanoen on osoitettu, että

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

Eräs tyypillinen tilanne, jossa täytyy osoittaa kaksi lauseketta samoiksi syntyy osoitettaessa, että jokin luku toteuttaa yhtälön. Tutkitaan tällaista esimerkkiä.

Esimerkki 5.3. Osoitetaan, että luku 1 toteuttaa yhtälön $\sqrt{x^2 - x + 4} = x^2 + 1$. On siis osoitettava, että $\sqrt{1^2 - 1 + 4} = 1^2 + 1$. Lasketaan ensin yhtälön vasen puoli:

$$\sqrt{1^2 - 1 + 4} = \sqrt{1 + 3} = \sqrt{4} = 2,$$

ja sitten oikea puoli:

$$1^2 + 1 = 1 + 1 = 2.$$

Koska molemmista laskuista tulee sama tulos, pätee yhtälö $\sqrt{x^2 - x + 4} = x^2 + 1$, kun $x = 1$. Siis luku 1 toteuttaa yhtälön $\sqrt{x^2 - x + 4} = x^2 + 1$.

Ohjeita lausekkeiden osoittamiseen samoiksi

- Vältä todistuksia, jotka lähtevät liikkeelle todistettavasta yhtäsuuruudesta ja päättyvät johtopäätökseen $0 = 0$.
- Todistettavan väitteen pitää olla lopputulos, ei lähtökohta.
- Jos sinun täytyy osoittaa jokin yhtäsuuruus todeksi, seuraavat menetelmät ovat toimivia:
 - Laske auki ensin vasen puoli ja sitten oikea puoli. Totea, että molemmissa tapauksissa tuli sama vastaus. Tämä toimii aina ja on hyvä menetelmä erityisesti monimutkaisten lausekkeiden kanssa.
 - Lähde liikkeelle yhtälö vasemmasta puolesta ja etene yhtäsuuruuksien avulla oikeaan puoleen.
 - Sama kuin edellä, mutta lähde liikkeelle oikeasta puolesta.

5.2 Kuinka osoittaa, että lauseke on toista suurempi?

Koulussa epäyhtälöitä yleensä ratkaistiin eli etsitiin kaikki luvut, joilla epäyhtälö pätee. Nyt tutustumme epäyhtälöiden erilaiseen käyttötarkoitukseen, joka tulee olemaan tarpeellinen tehtäessä päätelmiä ja todistettaessa yleisiä tuloksia. Matematiikassa epäyhtälöitä käytetään nimittäin siihen, että lausekkeelle etsitään jokin ylä- tai alaraja. Tätä kutsutaan ylöspäin tai alaspäin *arvioinniksi*. Ohessa on listattu muutamia esimerkkejä epäyhtälöihin liittyvistä väitteistä, joita opetellemme todistamaan:

- $3 + 10^{-100} < 9 + 10^{-99}$
- Oletetaan, että h on reaaliluku ja $0 \leq h \leq 1$. Tällöin $(3 + h)^2 \geq 9 + 7h$.
- Oletetaan, että reaaliluvulle k pätee $k \geq 4$. Tällöin $3^{k+1} > (k + 1)^3$.

Ryhdytään tutkimaan, kuinka nämä väitteet voisi todistaa.

Esimerkki 5.4. Osoitetaan, että $3 + 10^{-100} < 9 + 10^{-99}$. Lähdetään liikkeelle vasemmanpuoleisesta lausekkeesta ja keksitään lausekkeita, jotka ovat suurempia tai yhtä suuria. Tällä tavoin edetään pienin askelin kohti oikeanpuoleista lauseketta. Seuraavanlainen päättely osoittaa väitteen todeksi:

$$3 + 10^{-100} = 3 + 10^{-1} \cdot 10^{-99} = 3 + \frac{10^{-99}}{10} \stackrel{(1)}{<} 9 + \frac{10^{-99}}{10} \stackrel{(2)}{<} 9 + 10^{-99}.$$

Kohdassa (1) hyödynnettiin tietoa siitä, että $3 < 9$. Jos nimittäin lausekkeeseen lisää suuremman luvun, suurenee lauseke. Kohdassa (2) puolestaan jätettiin pois nimittäjä, jolloin lauseke suureni. Jos positiivisen luvun jakaa kymmenellä, on tulos pienempi kuin silloin, jos lukua ei jaa kymmenellä. Siksi lauseke suurenee, kun nimittäjä poistetaan. Näin on osoitettu, että $3 + 10^{-100} < 9 + 10^{-99}$.

Todistuksen idea on siis tehdä ketju yhtälöitä ja epäyhtälöitä niin, että jokaisessa vaiheessa siirrytään kohti suurempaa tai yhtä suurta lukua. Vähintäänkin yhdessä kohtaa täytyy olla aito epäyhtälö, jotta voidaan päätellä, että $3 + 10^{-100}$ on aidosti pienempi kuin $9 + 10^{-99}$.

Mistä sitten tiedetään, mitä välivaiheiksi tulee? Esimerkiksi kohdassa (2) voisi myös päätellä $3 + \frac{10^{-99}}{10} < 10 + \frac{10^{-99}}{10}$, sillä $3 < 10$. Näin ei kuitenkaan kannata tehdä, sillä lopputuloksessa on luku 9. Arviointi vaatiikin kokeilua ja pohtimista.

Vasemmanpuoleisesta lausekkeesta kannattaa kaivaa esiin elementtejä, jotka muistuttavat oikeanpuoleista lauseketta. Esimerkiksi edellä vasemmanpuoleinen lauseke muutettiin muotoon, jossa näkyy oikean puolen 10^{-99} . Lauseketta voi suurentaa muun muassa lisäämällä siihen positiivisen luvun, pienentämällä positiivisen luvun nimittäjää tai suurentamalla positiivisen luvun kerrointa.

Esimerkki 5.5. Oletetaan, että $h \in \mathbb{R}$ ja $0 \leq h \leq 1$. Osoitetaan, että $(3 + h)^2 \leq 9 + 7h$.

Lähdetään liikkeelle vasemmanpuoleisesta lausekkeesta $(3 + h)^2$ ja arvioidaan sitä ylöspäin yrittäen päästä kohti lauseketta $9 + 7h$:

$$(3 + h)^2 = 9 + 6h + h^2 = 9 + 6h + h \cdot h \stackrel{(1)}{\leq} 9 + 6h + 1 \cdot h = 9 + 6h + h = 9 + 7h.$$

Kohdassa (1) hyödynnettiin tietoa $0 \leq h \leq 1$. Jos nimittäin epänegatiivisen luvun kerrointa suurentaa, suurenee lauseke.

Esimerkki 5.6. Oletetaan, että reaaliluvulle k pätee $k \geq 4$. Osoitetaan, että $3^{k+1} > (k+1)^3$. Arvioidaan epäyhtälön oikeaa puolta alaspäin käyttäen toistuvasti oletusta $k \geq 4$:

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

Oletusta $k \geq 4$ käytettiin kohdissa (1) ja (2). Kohdassa (3) hyödynnettiin myös tietoa $4k^2 > 3k^2$. Kun positiivisen luvun kerrointa pienentää, pienenee luku.

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

Ohjeita ylöspäin ja alaspäin arviointiin

- Jos sinun pitää osoittaa, että jokin lauseke on pienempi tai suurempi kuin toinen, lähde liikkeelle vasemmanpuoleisesta lausekkeesta. Etene ylös tai alaspäin kohti oikeanpuoleista lauseketta sen mukaan, pitääkö vasemmanpuoleinen lauseke osoittaa pienemmäksi vai suuremmaksi kuin oikeanpuoleinen.
- Voit myös aloittaa oikeanpuoleisesta lausekkeesta ja edetä kohti vasemmanpuoleista.
- Lauseketta voi suurentaa muun muassa seuraavilla keinoilla
 - lisäämällä siihen positiivisen luvun
 - suurentamalla positiivisen luvun kerrointa
 - pienentämällä positiivisen luvun jakajaa.
- Vastaavasti lauseke pienenee päinvastaisilla toimilla.

6 Implikaatio- ja ekvivalenssitodistukset

6.1 Implikaatiotodistus eli jos ... niin -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.

Väite ”jos P , niin Q ” vastaa implikaatiota $P \rightarrow Q$.

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 6.1. 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 $a^2 < b^2$.

Edellisessä todistuksessa oli mukana selityksiä, jotka valottavat todistuksen eri osia. Niiden tarkoitus oli selventää todistuksen kulkua sellaiselle henkilölle, joka ei ole nähnyt implikaatiotodistusta aiemmin. Tällaisia selityksiä ei kuitenkaan tyypillisesti ole varsinaisissa todistuksissa. Seuraavassa esimerkissä näkyy pelkkä todistus ja selitykset on jätetty pois.

Esimerkki 6.2. Osoitetaan, että jos kokonaisluku m on parillinen, niin m^2 on parillinen.

Oletetaan, että kokonaisluku m on parillinen. Nyt on osoitettava, että m^2 on parillinen.

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

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

missä $2k^2 \in \mathbb{Z}$. Koska m^2 on kaksi kertaa jokin kokonaisluku, se on parillinen.

Väite ”jos kokonaisluku m on parillinen, niin m^2 on parillinen” on nyt todistettu.

6.2 Ekvivalenssitodistus eli jos ja vain jos -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 $P \leftrightarrow Q$. Se voidaan kirjoittaa kahden implikaation avulla muodossa $(P \rightarrow Q) \wedge (Q \leftarrow P)$. Väitteen ” P jos ja vain jos Q ” todistus muodostuukin todistuksesta implikaatiolle ”jos P , niin Q ” ja implikaatiolle ”jos Q , niin P ”.

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.

Aluksi kun ekvivalenssitodistuksen rakenne ei ole vielä tuttu, voit todistuksen hahmottamisessa auttaa eri osien erottaminen toisistaan merkeillä ” \Rightarrow ” ja ” \Leftarrow ”. Niiden avulla on helpompi muistaa, kumpaa suuntaa ollaan todistamassa. Näin on tehty seuraavissa esimerkeissä.

Esimerkki 6.3. 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 2.1 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 2.1 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 6.4. 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.

6.3 Ekvivalenssi ja yhtälöratkaisu

Yhtälöratkaisu on koulusta tuttua, mutta usein sitä tehdään mekaanisesti sen kummempia ajattelematta. Jotta pystytään ratkaisemaan monimutkaisempia yhtälöitä, on kuitenkin tärkeää ymmärtää, mitä yhtälöratkaisussa tapahtuu. Yhtälöratkaisu liittyy läheisesti ekvivalenssin käsitteeseen.

Ryhdytään ratkaisemaan yhtälöä $\sqrt{x+2} = -x$:

$$\begin{aligned}\sqrt{x+2} &= -x \\ (\sqrt{x+2})^2 &= (-x)^2 \\ x+2 &= x^2 \\ -x^2 + x + 2 &= 0 \\ x &= \frac{-1 \pm \sqrt{1 - 4(-1) \cdot 2}}{-2} \\ x &= \frac{-1 \pm 3}{-2} \\ x &= -1 \text{ tai } x = 2.\end{aligned}$$

Saadaan siis kaksi ratkaisua, $x = -1$ ja $x = 2$. Ensimmäinen luvuista todellakin on yhtälön ratkaisu, sillä $\sqrt{-1+2} = \sqrt{1} = 1$ ja $-(-1) = 1$. Toinen luvuista ei yllättäen toteutakaan yhtälöä, sillä $\sqrt{2+2} = \sqrt{4} = 2 \neq -2$. Siten $x = 2$ ei ole yhtälön ratkaisu! Mikä meni vikaan?

Ensimmäinen ongelma on, että yhtälöitä kirjoittaessa ei ole kerrottu, miten allekaiset yhtälöt liittyvät toisiinsa. Ovatko ne kenties yhtäpitäviä? Vai onko jälkimmäinen aina edellisen looginen seuraus? Näitä suhteita voidaan ilmaista ekvivalenssi- ja implikaationuolilla tai sanallisesti.

Tutkitaan vaikkapa esimerkin kolmatta ja neljättä yhtälöä. Kun yhtälön $x+2 = x^2$ molemmille puolille lisätään $-x^2$, saadaan $-x^2 + x + 2 = 0$. Jos siis yhtälö $x+2 = x^2$ pätee, myös yhtälö $-x^2 + x + 2 = 0$ pätee. Näin ollen yhtälö $-x^2 + x + 2 = 0$ on yhtälön $x+2 = x^2$ looginen seuraus, mikä voidaan kirjoittaa myös implikaationuolen avulla:

$$x+2 = x^2 \Rightarrow -x^2 + x + 2 = 0.$$

Toisaalta myös yhtälöstä $-x^2 + x + 2 = 0$ seuraa yhtälö $x+2 = x^2$. Tämän voi osoittaa lisäämällä yhtälön molemmille puolille x^2 . Toisin sanoen

$$-x^2 + x + 2 = 0 \Rightarrow x+2 = x^2.$$

Nyt tiedetään, että yhtälö $x+2 = x^2$ pätee, jos ja vain jos yhtälö $-x^2 + x + 2 = 0$ pätee. Tällöin sanotaan, että yhtälöt ovat *yhtäpitäviä*. Saman asian voi ilmaista ekvivalenssinuolella:

$$x+2 = x^2 \Leftrightarrow -x^2 + x + 2 = 0.$$

Koska yhtälö $x+2 = x^2$ on totta täsmälleen samoilla luvuilla kuin yhtälö $-x^2 + x + 2 = 0$, niiden ratkaisut ovat samat. Näin on aina: yhtäpitävillä yhtälöillä on samat ratkaisut.

Aiemman esimerkin yhtälönratkaisuyritys tuottaa ylimääräisiä ratkaisuja, sillä yhtälöketjun kaksi ensimmäistä yhtälöä eivät ole yhtäpitäviä. Tämä johtuu toiseen potenssiin korottamisesta. Tutkitaan hieman tarkemmin, mitä toiseen potenssiin korottaminen tekee yhtälölle.

Oletetaan, että $a, b \in \mathbb{R}$. Jos luvut a ja b ovat samoja, niiden neliöt ovat samoja, eli $a = b \Rightarrow a^2 = b^2$. Jos taas kahden luvun neliöt ovat samoja, luvut eivät välttämättä ole samoja. Esimerkiksi lukujen 2 ja -2 neliöt ovat samat. Ei siis voida kirjoittaa $a^2 = b^2 \Rightarrow a = b$. Näin ollen ei myöskään voida käyttää ekvivalenssinoiota: ei päde $a^2 = b^2 \Leftrightarrow a = b$.

Edellisen nojalla pätee $\sqrt{x+2} = -x \Rightarrow (\sqrt{x+2})^2 = (-x)^2$. Laitetaan vielä kaikki nuolet paikoilleen alussa esitettyyn yhtälöketjuun:

$$\begin{aligned} & \sqrt{x+2} = -x \\ \Rightarrow & (\sqrt{x+2})^2 = (-x)^2 \\ \Leftrightarrow & x+2 = x^2 \\ \Leftrightarrow & -x^2 + x + 2 = 0 \\ \Leftrightarrow & x = \frac{-1 \pm \sqrt{1 - 4(-1) \cdot 2}}{-2} \\ \Leftrightarrow & x = \frac{-1 \pm 3}{-2} \\ \Leftrightarrow & x = -1 \text{ tai } x = 2. \end{aligned}$$

Nyt nähdään, miksi yhtälönratkaisu meni pieleen. Jos $\sqrt{x+2} = -x$, niin joko $x = -1$ tai $x = 2$. Yhtälön mahdollisia ratkaisuja ovat siis -1 ja 2 . Toiseen suuntaan ei voida kuitenkaan päätellä mitään, eli ehdosta " $x = -1$ tai $x = 2$ " ei seuraa, että $\sqrt{x+2} = -x$. Siksi tulokseksi saatiin ylimääräisiä lukuja, jotka eivät ole yhtälön ratkaisuja.

Kirjoitetaan vielä lopuksi huolellisesti yhtälön ratkaisu. Se tehdään kahdessa osassa.

Ratkaisu: Ratkaistaan yhtälö $\sqrt{x+2} = -x$. Nähdään, että

$$\begin{aligned} & \sqrt{x+2} = -x \\ \Rightarrow & (\sqrt{x+2})^2 = (-x)^2 \\ \Rightarrow & x+2 = x^2 \\ \Rightarrow & -x^2 + x + 2 = 0 \\ \Rightarrow & x = \frac{-1 \pm \sqrt{1 - 4(-1) \cdot 2}}{-2} \\ \Rightarrow & x = \frac{-1 \pm 3}{-2} \\ \Rightarrow & x = -1 \text{ tai } x = 2. \end{aligned}$$

Nyt tiedetään, että jos yhtälö $\sqrt{x+2} = -x$ pätee, niin $x = -1$ tai $x = 2$. Yhtälön ratkaisuja ovat siis joko $x = -1$ tai $x = 2$ tai molemmat. Tarkistetaan sijoittamalla, mitkä kaikki ovat ratkaisuja:

Huomataan, että $\sqrt{-1+2} = \sqrt{1} = 1$ ja $-(-1) = 1$, joten luku -1 on toteuttava yhtälön $\sqrt{x+2} = -x$. Siten $x = -1$ on yhtälön ratkaisu. Toisaalta $\sqrt{2+2} = \sqrt{4} = 2 \neq -2$, joten luku 2 ei toteuta yhtälöä eikä siten ole ratkaisu.

Siten yhtälön ainoa ratkaisu on $x = -1$.

Huomaa, edellä yhtälönratkaisun välivaiheisiin kirjoitettiin implikaationuolet, vaikka ekvivalenssinuolikin olisi sopinut moneen paikkaan. Ekvivalenssinuoliten antamasta lisätiedosta ei tässä tapauksessa olisi kuitenkaan mitään hyötyä, sillä niitä ei kuitenkaan voi käyttää joka välivaiheessa.

Ylipäätään *ekvivalenssinuolia ei kannata käyttää, ellei niitä välttämättä tarvita*. Jos pärjät implikaationuolella, käytä sitä. Ekvivalenssinuolen tapauksessa pitää nimittäin aina tarkistaa että väitteet todella ovat yhtäpitäviä. Se jää helposti tekemättä tai ainakin aiheuttaa lisävaivaa niin kirjoittajalle kuin lukijallekin. Jos kirjoittaa $A \Leftrightarrow B$ täytyy nimittäin tarkistaa kaksi asiaa: väitteestä A täytyy seurata väite B ja väitteestä B täytyy seurata väite A .

Jopa seuraavanlainen merkintätapa on hämäävä:

$$\begin{aligned} x + 2 = x^2 & \qquad \qquad \qquad || - x^2 \\ \Leftrightarrow -x^2 + x + 2 = 0 \end{aligned}$$

Viivan oikealla puolella oleva kommentti perustelee, kuinka ratkaisu etenee ylhäältä alas. Ekvivalenssinuoli tarkoittaa sitä, että päättelyn pitää olla totta myös alhaalta ylös. Sitä ei kuitenkaan perustella millään tavalla.

Koulusta tuttuja 1. ja 2. asteen reaalityhtälöitä saa ratkaista ekvivalenssien avulla, sillä tiedämme, mitä operaatioita yhtälöille saa tehdä niin, että yhtäpitävyys säilyy. Voidaan esimerkiksi kirjoittaa

$$\begin{aligned} 2x + 3 &= 1 \\ \Leftrightarrow 2x &= -2 \\ \Leftrightarrow x &= -1. \end{aligned}$$

tai

Seuraavat yhtälöt ovat yhtäpitäviä:

$$\begin{aligned} 2x + 3 &= 1 \\ 2x &= -2 \\ x &= -1. \end{aligned}$$

Monimutkaisempia yhtälöitä pitää kuitenkin käsitellä suurella varovaisuudella, sillä ne eivät välttämättä ratkea ekvivalenssien avulla. Sama pätee hieman eksoottisempiin yhtälöihin, joiden muuttujat eivät ole lukuja (esim. matriiseja tai vaikkapa permutaatioita sisältävät yhtälöt). Niiden ratkaisussa implikaatioiden käyttäminen on yleensä järkevämpää ja turvallisempaa kuin ekvivalenssien.

Ohjeita yhtälöiden ratkaisemiseen

- Yhtälöitä ei voi vain kirjoittaa allekkain kertomatta, miten yhtälöt riippuvat toisistaan. Käytä nuolia tai sanoja.
- Kaikki yhtälöt eivät ratkea yhtäpitäviä yhtälöitä muodostamalla. Eräs tapa ratkaista yhtälö on johtaa siitä uusia yhtälöitä ja tarkistaa lopuksi, mitkä saaduista ratkaisuksista ovat alkuperäisen yhtälön ratkaisuja.
- Muista, että ekvivalenssinuolossa on kaksi suuntaa.
- Älä käytä ekvivalenssinuolia, jos implikaationuoli riittää.
- Älä käytä nuolia, jos pärjät suomen kielen sanoilla. Yhtälönratkaisussa nuolet ovat kuitenkin usein käytännöllisiä.
- Koulusta tutut 1. ja 2. asteen yhtälöt saa ratkaista samaan tapaan kuin ennenkin. Yhtälöiden keskinäinen riippuvuus on kuitenkin ilmaistava nuolin tai sanoin.

6.4 Osajoukoksi osoittaminen

Erikoistapaus implikaatiotodistuksesta on osajoukoksi osoittaminen. Aikaisemmin luvussa 1.4 olemme tutkineet konkreettisissa tapauksissa, milloin annettu joukko on toisen joukon osajoukko. Nyt lähdemme rakentamaan todistuksia, jotka toimivat abstrakteissa tilanteissa. Määritelmän 1.4 mukaan joukko A on joukon B *osajoukko*, jos kaikilla $x \in A$ pätee myös $x \in B$. Kyseessä on jos...niin -muotoisen väitteen todistus eli implikaatiotodistus.

Esimerkki 6.5. Oletetaan, että A ja B ovat joukkoja. Osoitetaan, että $(A \cup B) \setminus B \subset A$.

Oletetaan, että $a \in (A \cup B) \setminus B$. 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 $(A \cup B) \setminus B$ alkion, joten jokainen joukon $(A \cup B) \setminus B$ alkio kuuluu joukkoon A .

Esimerkki 6.6. Oletetaan, että A , B ja C ovat joukkoja. Osoitetaan, että

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

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 $x \in (A \cup B) \cap (A \cup C)$. Siten on osoitettu, että

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

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.

6.5 Kahden joukon osoittaminen samoiksi

Erikoistapaus ekvivalenssitodistuksesta on joukkojen osoittaminen samoiksi. Määritelmän 1.12 mukaan joukot A ja B ovat samat, jos niissä on täsmälleen samat alkiot eli kaikilla alkiolla x pätee seuraava: $x \in A$, jos ja vain jos $x \in B$.

Samalla tavalla kuin ekvivalenssitodistus koostuu kahdesta implikaatiotodistuksesta, joukot voi osoittaa samoiksi tekemällä kaksi osajoukkotodistusta: joukot osoitetaan samoiksi osoittamalla kumpikin joukko toisen osajoukoksi.

Todistus, jossa kaksi joukkoa osoitetaan samaksi, muodostuu siis kahdesta osasta. Nämä voi todistamista harjoitellessa 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 6.7. Oletetaan, että A , B ja C ovat joukkoja. Osoitetaan, että

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

” \subset ”: 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 $x \in A \cup (B \cap C)$. Tämä tarkoittaa, että

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

” \supset ”: Tämä on osoitettu esimerkissä 6.6.

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

Niin kutsutut de Morganin lait todistetaan osoittamalla joukot samoiksi.

Lause 6.8 (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 6.7.

” \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 $x \in \complement(A \cup B)$. \square

Seuraavassa esimerkissä osoitetaan potenssijoukot samoiksi. Esimerkissä ei enää käytetä apumerkintöjä ” \subset ” ja ” \supset ”, mutta todistuksen rakenne on sama kuin aiemmin. Ensin osoitetaan vasemmanpuoleinen joukko oikeanpuoleisen joukon osajoukoksi ja sitten oikeanpuoleinen vasemmanpuoleisen osajoukoksi.

Esimerkki 6.9. Oletetaan, että A , B ja C ovat joukkoja. Esimerkissä 1.24 huomattiin kuvan avulla, että $A \times (B \cap C) = (A \times B) \cap (A \times C)$. Todistetaan tämä hyödyntäen todistustekniikkaa kahden joukon osoittamiseksi samoiksi.

Oletetaan ensin, 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 $x \in (A \times B) \cap (A \times C)$.

Oletetaan sitten, 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 $y = (a, d) \in A \times (B \cap C)$.

Siten on osoitettu, että $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

6.6 Erilaisten todistustyyppien yhdistelmät

Seuraavissa esimerkeissä implikaatio- ja ekvivalenssitodistukset yhdistyvät osajoukkotodistuksiin ja joukkojen osoittamiseen samoiksi. Tämä tuo todistuksiin lisää kerroksia. Jotta todistusten rakennetta on helpompi seurata, käytetään esimerkeissä apumerkintöjä ” \subset ” ja ” \Rightarrow ”.

Esimerkki 6.10. 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 ?? 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 $B \subset A \cup B$.

Päätetyt ” \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 6.11. 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. 1.7 ja 1.9.)

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 $B \not\subset C$.

Esimerkki 6.12. 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 mainitut 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 $a \in B$.

7 Epäsuora todistaminen

7.1 Kontrapositiotodistus

Kappaleessa 6 perehdyttiin implikaatiotodistukseen eli ”jos P , niin Q ” -tyyppisten väitteen todistamiseen. Kyseessä oli niin kutsuttu suora todistus. Toisinaan tällaista suoraa todistusta

on vaikea rakentaa. Silloin on hyödyllistä muuttaa väite erilaiseen muotoon ja tehdä niin kutsuttu epäsuora todistus.

Tutkitaan esimerkin avulla, kuinka implikaation voi muuttaa erilaiseen muotoon niin, että merkitys ei kuitenkaan muutu. Lauseen ”Jos sataa, taivaalla on pilviä” kanssa saman asian ilmaisee lause ”Jos taivaalla ei ole pilviä, ei sada.” Lauseilla $P \rightarrow Q$ sekä $\neg Q \rightarrow \neg P$ on siis sama merkitys. (Asia on osoitettu täsmällisesti esimerkissä 3.8.) Muotoa $\neg Q \rightarrow \neg P$ kutsutaan implikaation $P \rightarrow Q$ *kontrapositioksi*.

Implikaatio $P \rightarrow Q$ voidaan todistaa näyttämällä, että sen kontraposio $\neg Q \rightarrow \neg P$ on tosi. Tämä tehdään kappaleessa 6 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 7.1. 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 kontraposio, joten myös alkuperäinen väite on todistettu.

Esimerkki 7.2. 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 kontraposio, joten myös alkuperäinen väite on todistettu.

7.2 Ristiriitatodistus

Kappaleessa 7.1 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.
- Päädytään johonkin ristiriitaan.

Ris-

tiriita tarkoittaa, että todistuksessa on kaksi päinvastaista väitettä. Etukäteen ei välttämättä tiedä, millaiseen ristiriitaan todistuksessa päädytään. Seuraavat esimerkit havainnollistavat, millaisia ristiriidat voivat olla.

Esimerkki 7.3. 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 7.1 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 6.2 esiteltyä tekniikkaa. Todistuksessa käytetään myös epäsuoraa päättelyä.

Esimerkki 7.4. 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 $\neg(P \rightarrow Q)$ on esimerkin 3.7 mukaan loogisesti ekvivalentti konjunktion $P \wedge \neg Q$ 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 6.11.

Esimerkki 7.5. Oletetaan, että A , B ja C ovat joukkoja. Osoitetaan, että jos $A \subset B$ ja $A \not\subset C$, niin $B \not\subset C$.

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 7.5 väitteen todistamiseen.

Esimerkki 7.6. 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 6 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 $B \not\subset C$.

8 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 tämällyyppisten väitteiden todistamiseen.

I induktioperiaate

Edellä esitetyt väitteet voi todistaa hyödyntäen niin kutsuttua induktioperiaatetta.

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 .

Induktiodistustus rakentuu kahdesta osasta, sillä pitää varmistaa, että molemmat induktioperiaatteissa mainitut ehdot toteutuvat. *Alkuaskeleessa* varmistetaan, että tutkittava väite pätee luvun nolla tapauksessa. *Induktioaskeleessa* osoitetaan, että implikaatio $P(n) \rightarrow P(n+1)$ 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 8.1. Osoitetaan induktiolla, että n :n ensimmäisen parillisen luonnollisen luvun summa on $n(n + 1)$. Toisin sanoen osoitetaan kaikilla $n \in \mathbb{N}$ pätee yhtälö

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

Ennen varsinaista todistusta tutkitaan, mitä väite oikein tarkoittaa. Lähdetään laskemaan

vasemman puolen summia eri n :n arvoilla:

$$\begin{aligned}0 \\0 + 2 = 2 \\0 + 2 + 4 = 6 \\0 + 2 + 4 + 6 = 12\end{aligned}$$

Toisaalta oikean puolen lauseke $n(n + 1)$ saa seuraavanlaisia arvoja:

$$\begin{aligned}0 \cdot (0 + 1) = 0 \\1 \cdot (1 + 1) = 2 \\2 \cdot (2 + 1) = 6 \\3 \cdot (3 + 1) = 12\end{aligned}$$

Ainakin neljän ensimmäisen luonnollisen luvun perusteella väite vaikuttaa pätevän. On kuitenkin tärkeää huomata, että tämä ei vielä todista mitään sillä voi olla, että väite ei päde esimerkiksi luvulla $n = 100$. Nämä laskut eivät olekaan osa varsinaista todistusta. Nyt meillä on kuitenkin hiukan parempi kuva siitä, mitä väite sanoo. Kirjoitetaan seuraavaksi varsinainen todistus käyttämällä induktioperiaatetta.

Alkuaskel: Väitteen mukaan ensimmäinen luku, jolla väitteen pitää päteä on $n = 0$. Tutkitaan, päteekö yhtälö tässä tapauksessa. Oletetaan, että $n = 0$. Yhtälön vasen puoli on tällöin 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

$$0 + 2 + 4 + \dots + 2k = k(k + 1). \quad (\text{IO})$$

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

$$0 + 2 + 4 + \dots + 2(k + 1) = (k + 1)(k + 2). \quad (\text{IV})$$

Tämä yhtälö on muodostettu tutkittavasta yhtälöstä sijoittamalla symbolin n paikalle $k + 1$.

Tutkitaan yhtälön (IV) vasen ja oikea puoli erikseen ja osoitetaan, että ne ovat samat. Aloitetaan vasemmasta puolesta ja muokataan sitä niin, että saadaan näkyviin summa, joka on induktio-oletuksessa (IO):

$$0 + 2 + 4 + \dots + 2(k + 1) = 0 + 2 + 4 + \dots + 2k + 2(k + 1) = (0 + 2 + 4 + \dots + 2k) + 2(k + 1)$$

Sovelletaan sitten induktio-oletusta (IO) ensimmäiseen suluissa olevaan lausekkeeseen:

$$(0 + 2 + 4 + \dots + 2k) + 2(k + 1) = k(k + 1) + 2(k + 1).$$

Lopuksi kerrotaan sulut auki:

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

Muokataan sitten yhtälön (IV) oikeaa puolta. Kertomalla sulut auki 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.

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

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

Myös seuraava esimerkki koskee väitettä, jossa on summa ja joka todistetaan induktiolla. Tällä kertaa summa on kuitenkin kirjoitettu summamerkkiä käyttäen kuten luvussa 2.2. Tämä ei muuta todistuksen ideaa, ainoastaan merkintöjä.

Esimerkki 8.2. Osoitetaan induktiolla, että kaikilla $n \in \mathbb{N}$ pätee

$$\sum_{j=0}^n j^3 = \frac{n^2(n+1)^2}{4}.$$

Alkuaskel: Tutkitaan, päteekö yhtälö tapauksessa $n = 0$. Oletetaan, että $n = 0$. Yhtälön vasen puoli on tällöin

$$\sum_{j=0}^0 j^3 = 0^3 = 0.$$

Yhtälön oikea puoli on puolestaan

$$\frac{0^2(0+1)^2}{4} = \frac{0 \cdot 1}{4} = 0.$$

Yhtälö siis pätee, kun $n = 0$.

Induktioaskel: Aloitetaan tekemällä induktio-oletus. Oletetaan, että $k \in \mathbb{N}$ ja väite pätee tällä luvulla. Toisin sanoen

$$\sum_{j=0}^k j^3 = \frac{k^2(k+1)^2}{4}. \quad (\text{IO})$$

Seuraavaksi näytetään, että vastaava yhtälö pätee myös luvulle $k+1$. On siis todistettava induktioväite

$$\sum_{j=0}^{k+1} j^3 = \frac{(k+1)^2(k+2)^2}{4}. \quad (\text{IV})$$

Tämä yhtälö on muodostettu tutkittavasta yhtälöstä sijoittamalla symbolin n paikalle $k+1$. Osoitetaan, että yhtälön (IV) vasen ja oikea puoli ovat samat. Käytetään tässä induktio-oletusta (IO).

Lähdetään liikkeelle todistettavan yhtälön (IV) vasemmasta puolesta. Erotetaan siitä erillisen summan viimeinen termi. Näin saadaan näkyviin summa, joka on induktio-oletuksessa.

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

Edellä summamerkintä on kirjoitettu auki selvyuden vuoksi, mutta välivaiheita ei tarvitse kirjoittaa näkyviin, jos hahmottaa tilanteen suoraan.

Käytetään sitten induktio-oletusta (IO), jonka perusteella summalauseke voidaan kirjoittaa osamääränä:

$$\sum_{j=0}^k j^3 + ((k+1)^3) = \frac{k^2(k+1)^2}{4} + (k+1)^3.$$

Lasketaan seuraavaksi lausekkeet yhteen. Tätä varten jälkimmäinen lauseke täytyy muuttaa osamääräksi:

$$\begin{aligned}\frac{k^2(k+1)^2}{4} + (k+1)^3 &= \frac{k^2(k+1)^2}{4} + \frac{4(k+1)^3}{4} \\ &= \frac{k^2(k+1)^2 + 4(k+1)^3}{4}.\end{aligned}$$

Jatketaan lausekkeen muiokkaamista kertomalla auki potensseja ja yhdistelemällä summattavia:

$$\begin{aligned}\frac{k^2(k+1)^2 + 4(k+1)^3}{4} &= \frac{k^2(k+1)^2 + 4(k+1)^2(k+1)}{4} \\ &= \frac{k^2(k+1)^2 + 4(k^2 + 2k + 1)(k+1)}{4} \\ &= \frac{k^2(k+1)^2 + 4(k^3 + 2k^2 + k + k^2 + 2k + 1)}{4} \\ &= \frac{k^2(k+1)^2 + 4(k^3 + 3k^2 + 3k + 1)}{4} \\ &= \frac{k^2(k^2 + 2k + 1) + 4(k^3 + 3k^2 + 3k + 1)}{4} \\ &= \frac{k^4 + 2k^3 + k^2 + 4(k^3 + 3k^2 + 3k + 1)}{4} \\ &= \frac{k^4 + 2k^3 + k^2 + 4k^3 + 12k^2 + 12k + 4}{4} \\ &= \frac{k^4 + 6k^3 + 13k^2 + 12k + 4}{4}.\end{aligned}$$

Tämän pidemmälle lauseketta on vaikea sieventää. Siirrytään siis induktioväitteen (IV) vasempaan puoleen ja yritetään saada se samaan muotoon kuin mihin edellä päästiin:

$$\begin{aligned} \frac{(k+1)^2(k+2)^2}{4} &= \frac{(k^2+2k+1)(k^2+4k+4)}{4} \\ &= \frac{k^4+4k^3+4k^2+2k^3+8k^2+8k+k^2+4k+4}{4} \\ &= \frac{k^4+6k^3+13k^2+12k+4}{4}. \end{aligned}$$

Saatiin sama tulos kuin yhtälön (IV) oikeasta puolesta. Siten induktioväite (IV) pätee eli

$$\sum_{j=0}^{k+1} j^3 = \frac{(k+1)^2(k+2)^2}{4}. \quad (\text{IV})$$

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

$$\sum_{j=0}^n j^3 = \frac{n^2(n+1)^2}{4}.$$

Seuraava esimerkki induktiotodistuksesta liittyy lukujen jaollisuuteen.

Esimerkki 8.3. 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 2.1 nojalla, että on olemassa $a \in \mathbb{Z}$, jolla pätee

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

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:

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

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 8.4. 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 $k \geq 4$:

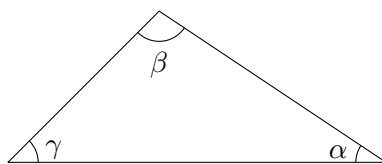
$$\begin{aligned}3^{k+1} &> k^3 + k^3 + k^3 \\&= k^3 + k \cdot k^2 + k^2 \cdot k \\&\geq k^3 + 4k^2 + 16k \\&= k^3 + 4k^2 + 15k + k \\&\geq k^3 + 4k^2 + 15k + 4 \\&> k^3 + 3k^2 + 3k + 1 = (k + 1)^3.\end{aligned}$$

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

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

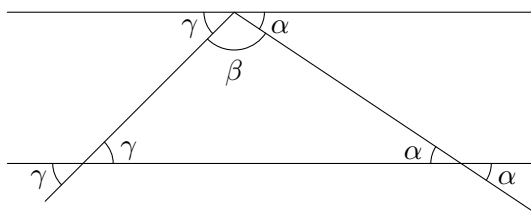
Esimerkki 8.5. Osoitetaan induktiolla, että n -kulmion kulmien summa on $(n-2)\pi$ kaikilla luonnollisilla luvuilla $n \geq 3$.

Alkuaskel: Tutkitaan, päteekö väite pienimmän tarkasteltavan luonnollisen luvun eli luvun 3 tapauksessa. Merkitään kolmikulmion eli kolmion kulmia α , β ja γ kuten kuvassa 8.1.



Kuva 8.1: Kolmio, jonka kulmat ovat α , β ja γ

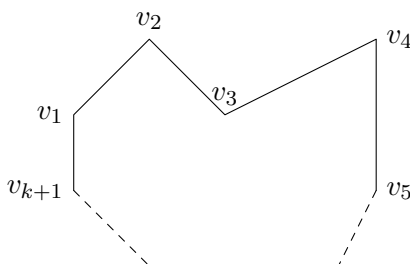
Piirtämällä kulmaa β vastaavaan kolmion kärkeen kolmion kannan suuntainen suora ja jatkamalla kolmion sivuja kuten kuvassa 8.2 voidaan päätellä, että kulmien summa $\alpha + \beta + \gamma$ on oikokulma eli 180 astetta eli π radiaania. Siis kolmion kulmien summa on $(3-2)\pi$.



Kuva 8.2: Kolmion kulmien summa $\alpha + \beta + \gamma$ on 180 astetta eli π radiaania.

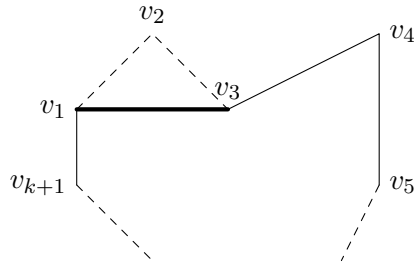
Induktioaskel: Aloitetaan tekemällä induktio-oletus. Oletetaan, että luonnollinen luku $k \geq 3$ ja k -kulmion kulmien summa on $(k-2)\pi$.

Tarkastellaan $(k+1)$ -kulmiota, jonka kärjet ovat $v_1, v_2, v_3, \dots, v_{k+1}$. Sitä on havainnollistettu kuvassa 8.3:



Kuva 8.3: Osa $(k+1)$ -kulmiosta, jonka kärjet ovat $v_1, v_2, v_3, \dots, v_{k+1}$.

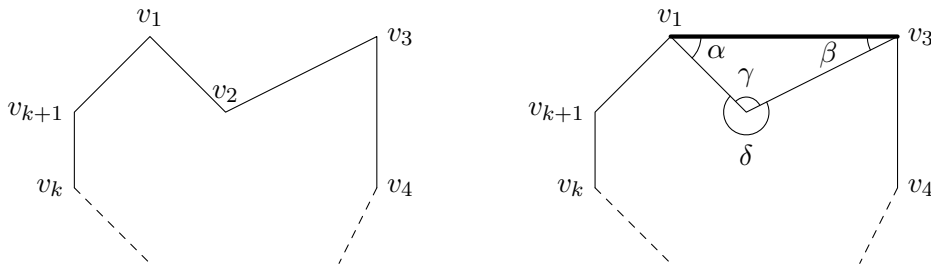
Piirtämällä jana kärjestä v_1 kärkeen v_3 saadaan muodostettua k -kulmio $v_1 v_3 \dots v_{k+1}$, jonka kulmien summa on induktio-oletuksen mukaan $(k-2)\pi$. Sitä on havainnollistettu kuvassa 8.4:



Kuva 8.4: Induktio-oletuksen mukaan k -kulmion $v_1v_3 \dots v_{k+1}$ kulmien summa on $(k-2)\pi$.

Koska alkuperäinen $(k+1)$ -kulmio saadaan yhdistämällä k -kulmio $v_1v_3 \dots v_{k+1}$ ja kolmio $v_1v_2v_3$, 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 8.5 on havainnollistettu toista mahdollista tilannetta, jossa alkuperäinen $(k+1)$ -kulmio sisältyy syntyvään k -kulmioon.



Kuva 8.5: 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 2π , saadaan pääteltyä kulman δ suuruus:

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

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

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

Johtobäätös: 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 8.6. 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 2.1 nojalla, että on olemassa $a \in \mathbb{Z}$, jolla pätee

$$10^k + 1 = a \cdot 9. \quad (4)$$

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

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

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 8.7. 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 8.4. Koikeilemalla 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

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

Nyt kun olemme esimerkkien kautta tutustuneet induktioperiaatteeseen, kirjoitetaan se vielä toisessa muodossa symboleiden avulla. Tämä saattaa auttaa hahmottamaan induktioperiaatetta.

I induktioperiaate. Oletetaan, että seuraavat ehdot ovat voimassa:

1) $P(0)$.

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

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

II induktioperiaate

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

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 $\forall j \in \mathbb{N} (j \leq n \rightarrow P(j))$ muotoon $\forall j \leq n P(j)$.

II induktioperiaate. *Oletetaan, että seuraavat ehdot ovat voimassa:*

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

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 $P(n)$. \square

Esimerkki 8.8. 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

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

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 .

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

Esimerkki 8.9. Osoitetaan, että jokainen luonnollinen luku $n \geq 2$ on joko alkuluku tai alkulukujen tulo.

Alkuaskel: Määritelmän 2.3 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.

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

Luku III

Kuvaukset ja relaatiot

9 Perusasioita kuvauksista

Tämä luku on Lotta Oinosen materiaalista ”Johdatus yliopistomatematiikkaan”.

9.1 Kuvauksen määritelmä

Määritelmä 9.1. 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 .

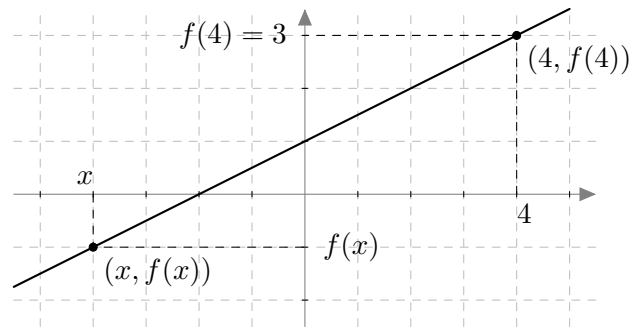
Merkintä $f: X \rightarrow Y$ tarkoittaa, että f on kuvaus joukosta X joukkoon Y . Joukko X on kuvauksen f *lähtö* ja joukko Y on kuvauksen f *maali*.

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

Esimerkki 9.2. Koulusta tutut funktiot ovat kuvauksia. Esimerkiksi yhtälö $f(x) = 0,5x + 1$ määrittelee kuvauksen $f: \mathbb{R} \rightarrow \mathbb{R}$. 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 .

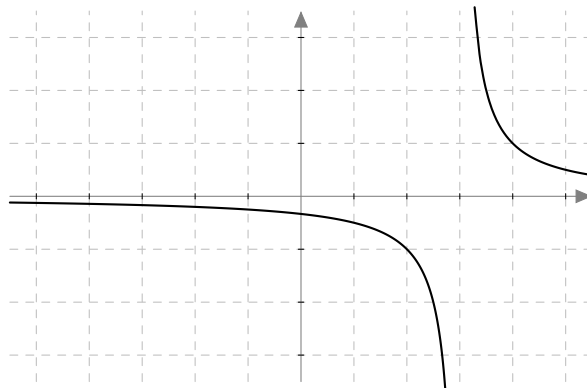


Kuva 9.1: Osa esimerkissä 9.2 tarkastellun funktion f kuvaajasta.

Esimerkki 9.3. Yhtälö

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

määrittelee kuvauksen $g: \mathbb{R} \setminus \{3\} \rightarrow \mathbb{R}$. Jos $x \neq 3$, on jakaja nolasta 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 9.2: Osa esimerkissä 9.3 tarkastellun funktion $g: \mathbb{R} \setminus \{3\} \rightarrow \mathbb{R}$ kuvaajasta.

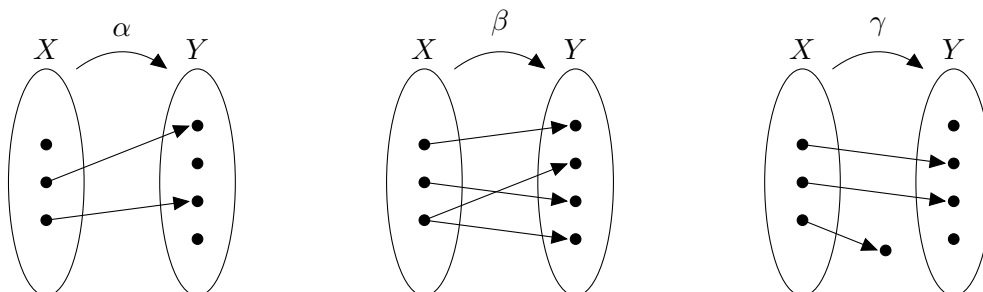
Edellisissä esimerkeissä esiintyneiden kuvausten lähtönä ja maalina oli reaalilukujen joukko tai jokin sen osajoukko. Kuvauksen määritelmän mukaan lähtö ja maali voivat kuitenkin olla mitä tahansa joukkoja.

Esimerkki 9.4. 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.

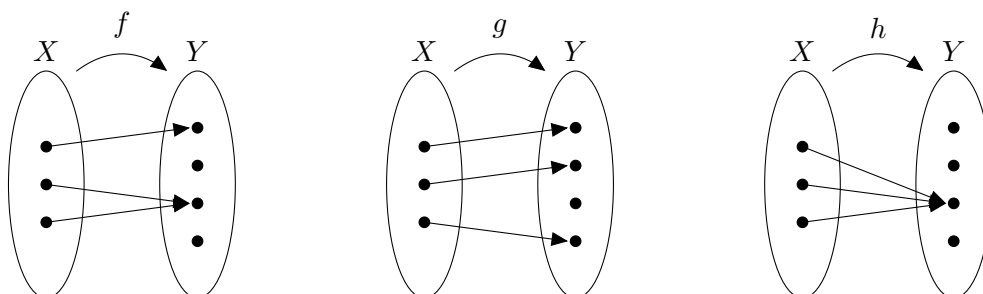
Esimerkki 9.5. Alla on havainnollistettu sääntöjä α , β ja γ kuvassa 9.3. Osoittautuu, että mikään niistä ei ole kuvaus joukosta X joukkoon Y .



Kuva 9.3: Säännöt α , β ja γ eivät ole kuvauksia joukosta X joukkoon Y .

Sääntö α ei ole kuvaus $X \rightarrow Y$, sillä joukossa X on alkio, johon α ei liitä yhtään joukon Y alkioita. Sääntö β ei ole kuvaus $X \rightarrow Y$, sillä joukossa X on alkio, johon β liittää useamman kuin yhden joukon Y alkion. Sääntö γ ei ole kuvaus $X \rightarrow Y$, sillä joukossa X on alkio, johon liitetty alkio ei kuulu joukkoon Y .

Esimerkki 9.6. Alla on havainnollistettu sääntöjä f , g ja h kuvassa 9.4. Ne kaikki ovat kuvauksia joukosta X joukkoon Y , sillä ne liittävät joukon X jokaiseen alkioon täsmälleen yhden alkion joukosta Y .



Kuva 9.4: Säännöt f , g ja h ovat kuvauksia joukosta X joukkoon Y .

Huomaa, että maalissa Y voi olla sellaisia alkioita, joihin ei kuvaudu yhtään alkioita. Toisaalta samalla maalilla Y alkioille voi kuvautua useampi alkio.

Esimerkki 9.7. 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 $\mathbb{Q} \rightarrow \mathbb{Q}$?

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:

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

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

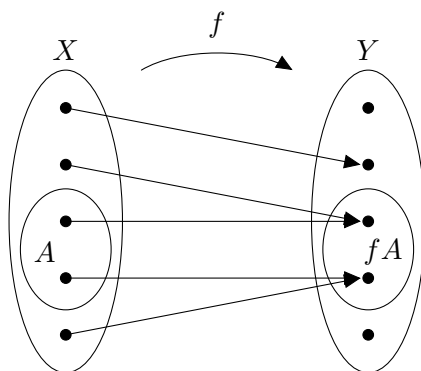
Näin $h(1/2) \neq h(2/4)$, vaikka $1/2 = 2/4$. Sääntö h siis liittää alkioon $1/2$ ainakin kaksi eri alkioita joukosta \mathbb{Q} , joten h ei ole kuvaus $\mathbb{Q} \rightarrow \mathbb{Q}$.

9.2 Kuva

Määritelmä 9.8. Oletetaan, että $f: X \rightarrow Y$ on kuvaus. Oletetaan lisäksi, että $A \subset X$. Joukon A kuva kuvauksessa f on joukko

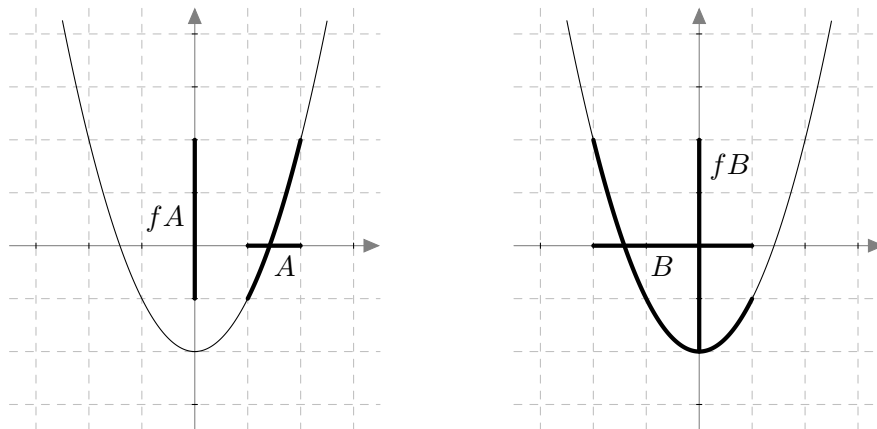
$$fA = \{y \in Y \mid y = f(a), \text{ missä } a \in A\}.$$

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



Kuva 9.5: Kuvan fA muodostavat joukon A alkioiden kuva-alkiot.

Esimerkki 9.9. Tarkastellaan funktiota $f: \mathbb{R} \rightarrow \mathbb{R}$, 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 vaak akselille, ja kuvat fA ja fB muodostuvat pysty akselille.

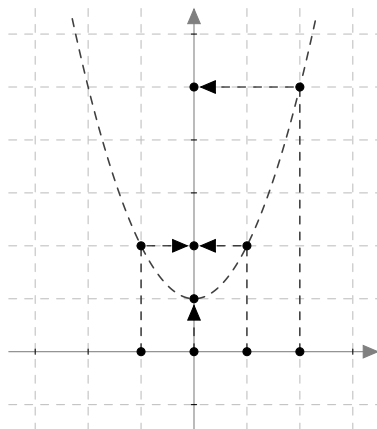


Kuva 9.6: Joukon $A = [1, 2]$ kuva $fA = [-1, 2]$ ja joukon $B = [-2, 1]$ kuva $fB = [-2, 2]$.

Esimerkki 9.10. Olkoon $f: \mathbb{Z} \rightarrow \mathbb{R}$ 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 9.7: Joukon $A = \{-1, 0, 1, 2\}$ kuva on $fA = \{1, 2, 5\}$.

Esimerkki 9.11. 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 $f: \mathcal{P}(A) \rightarrow \mathcal{P}(A)$, 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 9.12. Olkoon $f: X \rightarrow Y$ 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 $y \in f[A \cup B]$.

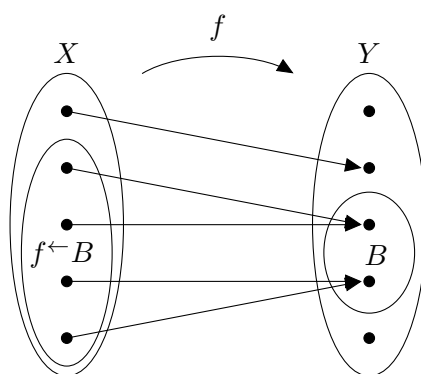
Päätelyt ” \subset ” ja ” \supset ” yhdessä osoittavat, että $f[A \cup B] = fA \cup fB$. Koska tarkastellut joukot A ja B saattoivat olla mitä tahansa joukon X osajoukkoja, pätee tulos kaikilla joukon X osajoukoilla A ja B .

9.3 Alkukuva

Määritelmä 9.13. Oletetaan, että $f: X \rightarrow Y$ on kuvaus. Oletetaan lisäksi, että $B \subset Y$. Joukon B alkukuva kuvauksessa f on joukko

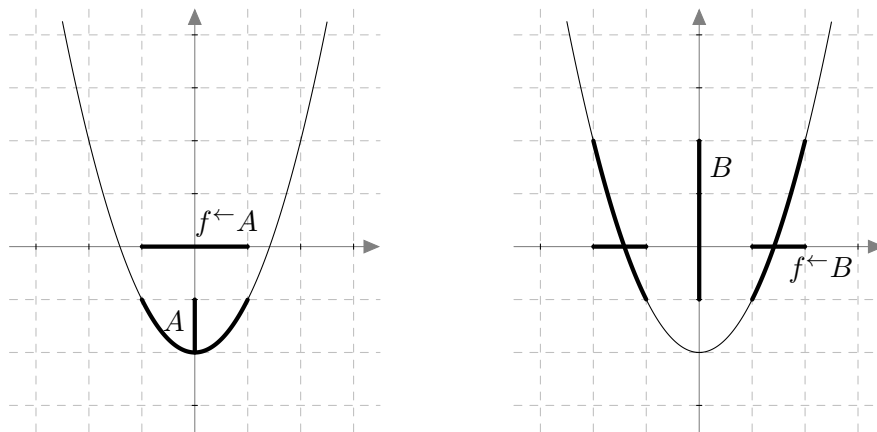
$$f^{-1}B = \{x \in X \mid f(x) \in B\}.$$

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



Kuva 9.8: Alkukuvan $f^{-1}B$ muodostavat ne lähdön alkiot, jotka kuvautuvat joukkoon B .

Esimerkki 9.14. Tarkastellaan funktiota $f: \mathbb{R} \rightarrow \mathbb{R}$, 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 $f^{-1}A = [-1, 1]$ ja joukon $B = [-1, 2]$ alkukuva on $f^{-1}B = [-2, -1] \cup [1, 2]$. Huomaa, että joukot A ja B merkitään pystyakselille, ja alkukuvat $f^{-1}A$ ja $f^{-1}B$ muodostuvat vaak akselille.



Kuva 9.9: Joukon A alkukuva $f^{-1}A$ ja joukon B alkukuva $f^{-1}B$.

Esimerkki 9.15. Olkoon $f: \mathbb{Z} \rightarrow \mathbb{R}$ kuvaus, jolle $x \mapsto x^2 + 1$ kaikilla $x \in \mathbb{Z}$. Merkitään $B = \{-1, 1, 2, 3\}$. Määritetään $f^{-1}B$.

Alkukuvan määritelmän mukaan

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

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:

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

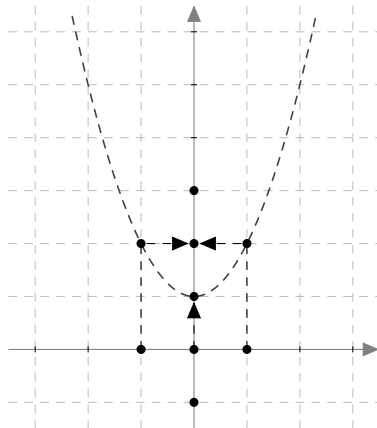
Viimeisellä yhtälöllä ei ole ratkaisua kokonaislukujen joukossa, sillä

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

Alkukuvaksi saadaan siis

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

Sitä on havainnollistettu alla kuvassa 9.10.



Kuva 9.10: Joukon $B = \{-1, 1, 2, 3\}$ alkukuva on $f^{-1}B = \{-1, 0, 1\}$.

Esimerkki 9.16. 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 9.11 tuttua kuvausta $f: \mathcal{P}(A) \rightarrow \mathcal{P}(A)$, 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

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

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

$$f^{-1}C = \{X \in \mathcal{P}(A) \mid f(X) \in C\} = \{X \in \mathcal{P}(A) \mid f(X) = \{2, 3\}\} = \emptyset.$$

Huomaa, että alkukuva on aina olemassa, mutta joskus se saattaa olla tyhjä joukko kuten tässä esimerkissä $f^{-1}C = \emptyset$.

Seuraavassa esimerkissä tarkastellaan joukkojen C ja D leikkauksen alkukuvaa $f^{-1}[C \cap D]$. Jos alkukuvan yhteydessä tarvitaan sulkuja, käytämme hakasulkuja kuten kuvan tapauksessa.

Esimerkki 9.17. Olkoon $f: X \rightarrow Y$ kuvaus. Osoitetaan, että $f^{-1}[C \cap D] = f^{-1}C \cap f^{-1}D$ 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 $x \in f^{-1}[C \cap D]$. 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 $x \in f^{-1}C$. Toisaalta $x \in X$ ja $f(x) \in D$, joten alkukuvan määritelmän mukaan $x \in f^{-1}D$. Näin ollen $x \in f^{-1}C \cap f^{-1}D$.

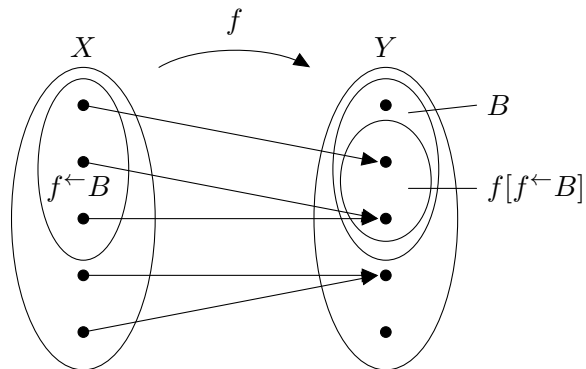
” \supset ”: Oletetaan, että $x \in f^{-1}C \cap f^{-1}D$. Tällöin $x \in f^{-1}C$ ja $x \in f^{-1}D$. Koska $x \in f^{-1}C$, niin alkukuvan määritelmän mukaan $x \in X$ ja $f(x) \in C$. Toisaalta $x \in f^{-1}D$, joten alkukuvan määritelmästä seuraa, että $f(x) \in D$. Näin ollen $f(x) \in C \cap D$. Koska $x \in X$ ja $f(x) \in C \cap D$, niin alkukuvan määritelmän mukaan $x \in f^{-1}[C \cap D]$.

Päättyvät ” \subset ” ja ” \supset ” yhdessä osoittavat, että $f^{-1}[C \cap D] = f^{-1}C \cap f^{-1}D$. 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 9.11.

Esimerkki 9.18. Olkoon $f: X \rightarrow Y$ kuvaus. Osoitetaan, että $f[f^{-1}B] \subset B$ kaikilla $B \subset Y$.

Oletetaan, että $B \subset Y$. Oletetaan, että $y \in f[f^{-1}B]$. Tällöin kuvan määritelmän mukaan $y \in Y$ ja $y = f(x)$ jollakin $x \in f^{-1}B$. Koska $x \in f^{-1}B$, niin alkukuvan määritelmän nojalla $f(x) \in B$. Koska $y = f(x)$, niin $y \in B$.



Kuva 9.11: Jos B on maalin osajoukko, niin $f[f^{-1}B] \subset B$.

Esimerkki 9.19. Oletetaan, että X ja Y ovat joukkoja. Tutkitaan, päteekö yhtälö $f[f^{-1}B] = B$ kaikilla kuvauksilla $f: X \rightarrow Y$ ja osajoukoilla $B \subset Y$.

Kuvan 9.11 tilanteessa $f[f^{-1}B] \neq B$, joten vastaesimerkin keksiminen näyttäisi olevan mahdollista. Yritetään siis löytää sellainen kuvaus f ja sellainen joukko B , että $f[f^{-1}B] \neq B$.

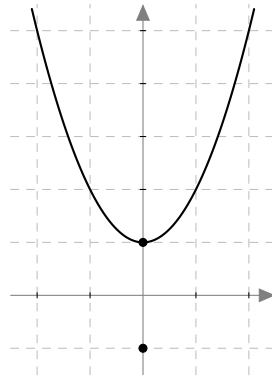
Olkoon $f: \mathbb{R} \rightarrow \mathbb{R}$ kuvaus, jolla $f(x) = x^2 + 1$ kaikilla $x \in \mathbb{R}$. Olkoon $B = \{-1, 1\}$. Tällöin

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

Siten

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

Tilannetta on havainnollistettu alla kuvassa 9.12.



Kuva 9.12: Joukon $B = \{-1, 1\}$ alkukuvan kuva on $f[f^{-1}B] = \{1\}$.

9.4 Injektio

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

Määritelmä 9.20. Kuvaus $f: X \rightarrow Y$ on *injektio*, jos kaikilla $x_1, x_2 \in X$ yhtälöstä $f(x_1) = f(x_2)$ seuraa, että $x_1 = x_2$.

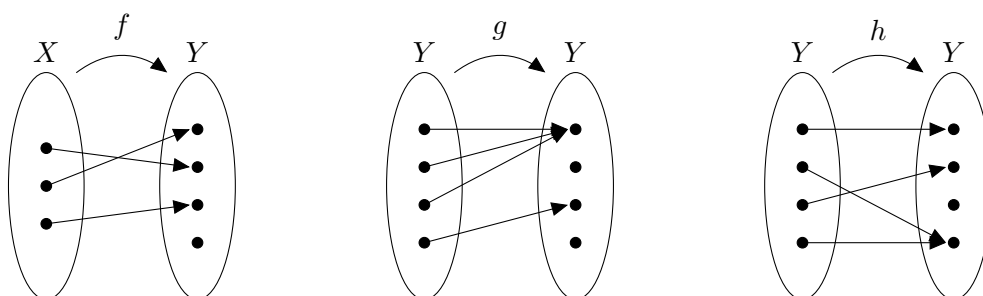
Logiikan symboleiden avulla injektio määritelmän ehto voidaan kirjoittaa seuraavasti:

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

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

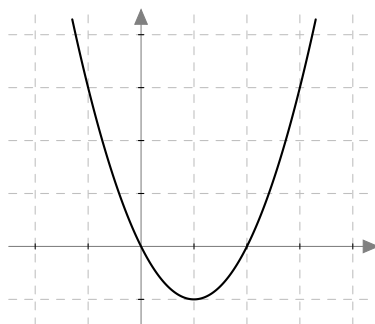
$$\forall x_1 \forall x_2 (x_1 \neq x_2 \rightarrow f(x_1) \neq f(x_2)).$$

Havaitaan, että injektio tarkoittaa kuvausta, jossa eri alkiot kuvautuvat aina eri alkioiksi eivätkä koskaan samaksi. Injektion käsitettä on havainnollistettu alla kuvassa 9.13.



Kuva 9.13: Kuvaus f on injektio, kuvaukset g ja h eivät ole injektioita.

Esimerkki 9.21. Tarkastellaan funktiota $f: \mathbb{R} \rightarrow \mathbb{R}$, 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 9.14: Funktio $x \mapsto x^2 - 2x$ ei ole injektio.

Esimerkki 9.22. Olkoon $g: \mathbb{R} \rightarrow \mathbb{R}$ funktio, jolle $g(x) = 2 - 0,25x$ kaikilla $x \in \mathbb{R}$. Osa sen kuvaajasta on piirretty kuvaan 9.15. 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

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

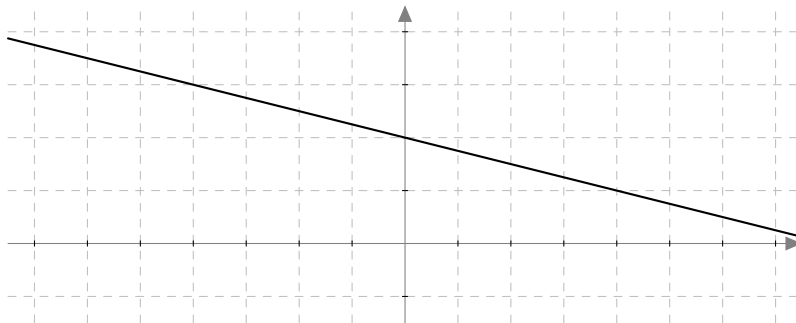
Vähentämällä tämän yhtälön molemmilta puolilta luku 2 päästään yhtälöön

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

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.

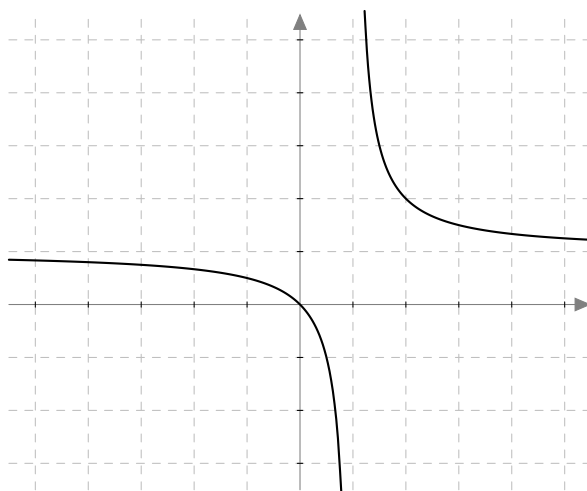


Kuva 9.15: Funktio $x \mapsto 2 - 0,25x$ on injektio.

Esimerkki 9.23. Tarkastellaan funktiota $h: \mathbb{R} \setminus \{1\} \rightarrow \mathbb{R}$, jolla

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

kaikilla $x \in \mathbb{R} \setminus \{1\}$. Osa sen kuvaajasta on piirretty kuvaan 9.16. 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 9.16: 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

$$-x_1 = -x_2.$$

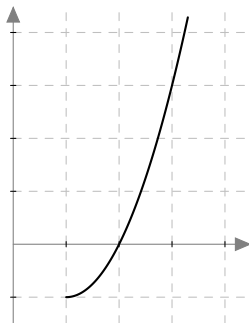
Kertomalla tämän yhtälön molemmat puolet luvulla -1 havaitaan, että

$$x_1 = x_2.$$

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 9.14 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 9.24. Tarkastellaan funktiota $\rho: [1, \infty[\rightarrow \mathbb{R}$, jolle $\rho(x) = x^2 - 2x$ kaikilla $x \in \mathbb{R}$. Sen kuvaaja on piirretty kuvaan 9.17.



Kuva 9.17: Funktio $x \mapsto x^2 - 2x$, jonka lähtö on $[1, \infty[$, on injektio.

Osoitetaan, että ρ 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 ρ on injektio.

9.5 Surjektio

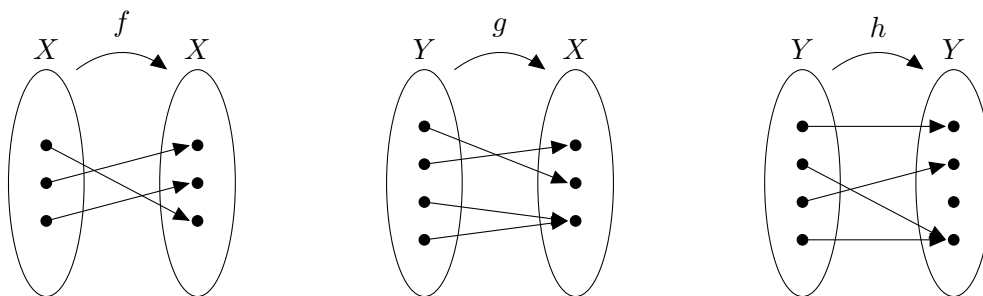
Surjektion käsitteen avulla kuvauksia voidaan luokitella sen mukaan, kuvautuuko kaikille maalin alkioille jokin alkio vai ei.

Määritelmä 9.25. Kuvaus $f: X \rightarrow Y$ 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:

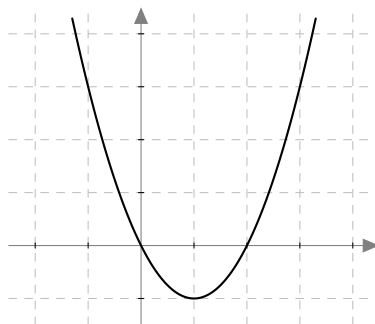
$$\forall y \exists x (f(x) = y).$$

Havaitaan, että surjektio tarkoittaa kuvausta, jossa kaikille maalin alkioille kuvautuu yksi tai useampi alkio. Surjektion käsitettä on havainnollistettu alla kuvassa 9.18.



Kuva 9.18: Kuvaukset f ja g ovat surjektioita, kuvaukset h ei ole surjektio.

Esimerkki 9.26. Tarkastellaan funktiota $f: \mathbb{R} \rightarrow \mathbb{R}$, 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 9.19: Funktio $x \mapsto x^2 - 2x$ ei ole surjektio.

Perustellaan vielä täsmällisesti, että edellä tarkasteltu funktio $f: \mathbb{R} \rightarrow \mathbb{R}$, jolla $f(x) = x^2 - 2x$ kaikilla $x \in \mathbb{R}$, ei ole surjektio. Tehdään vasta oletus, 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 vasta oletus 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

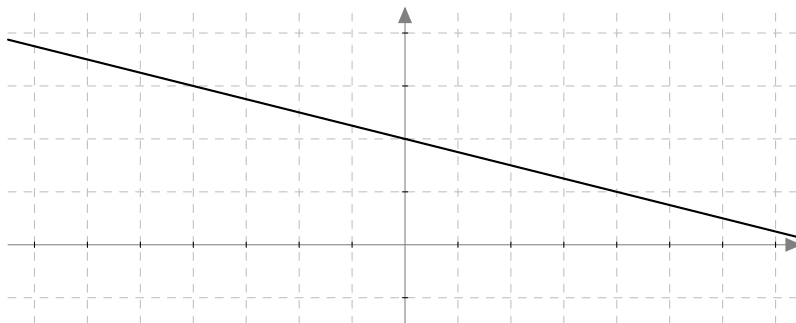
$$f(x) = -2 \Leftrightarrow x^2 - 2x = -2 \Leftrightarrow x^2 - 2x + 2 = 0.$$

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 $f: \mathbb{R} \rightarrow \mathbb{R}$ ei ole surjektio.

Esimerkki 9.27. Olkoon $g: \mathbb{R} \rightarrow \mathbb{R}$ funktio, jolle $g(x) = 2 - 0,25x$ kaikilla $x \in \mathbb{R}$. Osa sen kuvaajasta on piirretty kuvaan 9.20. Kuvaajan perusteella funktio g näyttäisi olevan surjektio, sillä sen kuvaaja leikkaa minkä tahansa vaaka-akselin suuntaisen suoran ainakin kerran (jotkin niistä kuvan 9.20 ulkopuolella). Siitä voidaan päätellä, että funktio g saa jokaisen arvon ainakin yhdessä kohdassa.

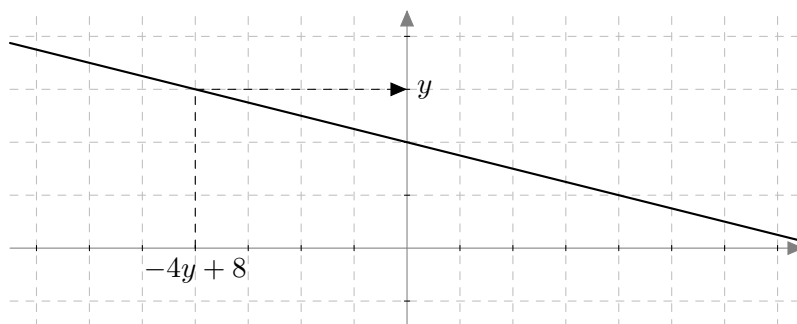


Kuva 9.20: Funktio $x \mapsto 2 - 0,25x$ on surjektio.

Osoitetaan vielä täsmällisesti, että edellä tarkasteltu funktio $g: \mathbb{R} \rightarrow \mathbb{R}$, 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.



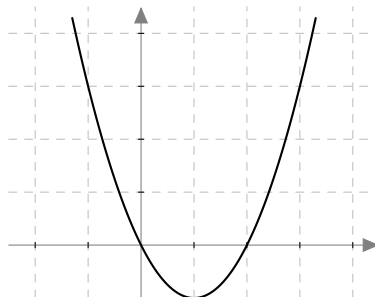
Kuva 9.21: Jokaista lukua $y \in \mathbb{R}$ kohti löytyy luku $x = -4y + 8 \in \mathbb{R}$, jolla $g(x) = y$.

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 9.28. Tarkastellaan kuvausta $\tau: \mathbb{R} \rightarrow [-1, \infty[$, jolle $\tau(x) = x^2 - 2x$ kaikilla $x \in \mathbb{R}$. Osa sen kuvaajasta on piirretty kuvaan 9.22. Kuvaajan perusteella funktio τ näyttäisi olevan surjektio, sillä sen maaliksi on valittu sopivasti $[-1, \infty[$.

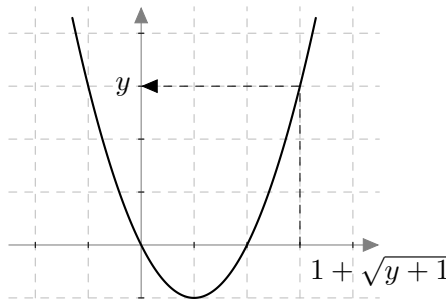


Kuva 9.22: Funktio $x \mapsto x^2 - 2x$, jonka maali on $[-1, \infty[$, on surjektio.

Osoitetaan, että kuvaus τ 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 τ on surjektio.



Kuva 9.23: 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 9.29. Tarkastellaan funktiota $h: \mathbb{R} \setminus \{1\} \rightarrow \mathbb{R}$, jolla

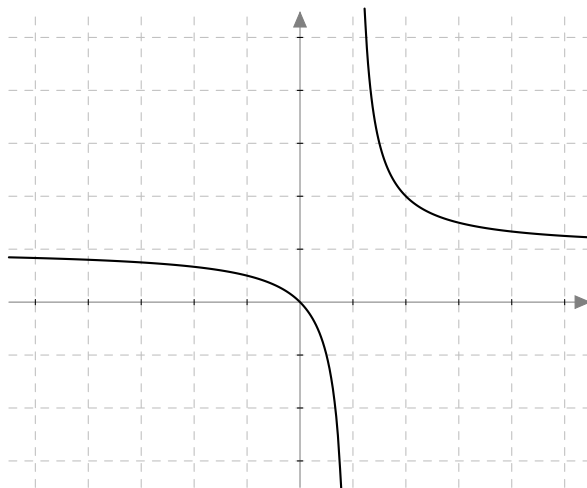
$$h(x) = \frac{x}{x - 1}$$

kaikilla $x \in \mathbb{R} \setminus \{1\}$. Osa sen kuvaajasta on piirretty kuvaan 9.24. Kuvaajan perusteella näyttää siltä, että mikään lähtöjoukon alkio ei kuvaudu luvulle 1. Kuvaus ei siis ole surjektio. Osoitetaan tämä ristiriitatodistuksella.

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 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 vasta oletus on epätosi ja alkuperäinen väite pätee. Näin ollen h ei ole surjektio.



Kuva 9.24: Funktio $x \mapsto x/(x-1)$, jonka maali on \mathbb{R} , ei ole surjektio.

Joskus kuvan perusteella voi olla vaikea löytää maalijoukon alkioita, jolle ei kuvaudu mitään. Toinen strategia tähän on yhtälön $h(x) = y$ tutkiminen. Jos $x \in \mathbb{R} \setminus \{1\}$, voidaan päätellä seuraavasti:

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

Nyt nähdään, että 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.

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

Lause 9.30. *Kuvaus $f: X \rightarrow Y$ on surjektio, jos ja vain jos $fX = Y$.*

Todistus. ” \Rightarrow ”: Oletetaan, että $f: X \rightarrow Y$ 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 $f: X \rightarrow Y$ on surjektio, joten on olemassa sellainen $x \in X$, jolla $f(x) = y$. Siis $y \in fX$ kuvan määritelmän nojalla.

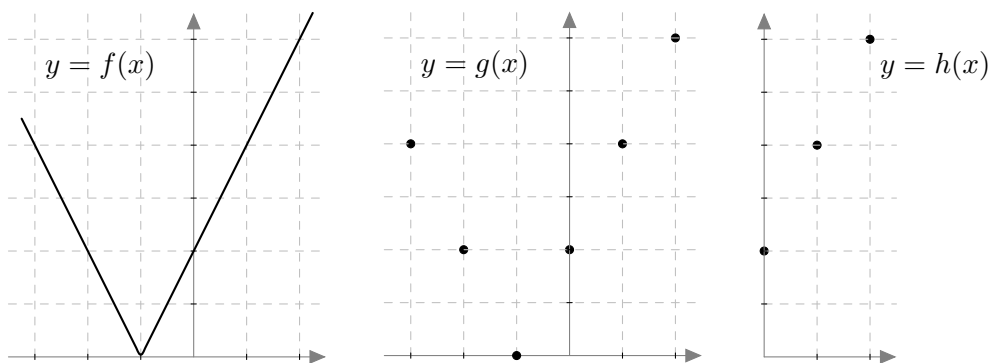
” \Leftarrow ”: Oletetaan, että $fX = Y$. Tavoitteena on näyttää, että $f: X \rightarrow Y$ on surjektio.

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 9.21, 9.24, 9.26 ja 9.28 havaittiin, että kuvauksen $x \mapsto x^2 - 2x$ injektiivisyys ja surjektiivisyys riippuvat siitä, mitä kuvauksen lähtö- ja maalijoukko ovat. Tämän vuoksi kuvausten sanotaan olevan samoja vain siinä tapauksessa, että niiden lähtö- ja maalijoukot ovat samat.

Määritelmä 9.31. Oletetaan, että f ja g ovat kuvauksia $X \rightarrow Y$. Kuvaukset f ja g ovat *samat* eli $f = g$, jos $f(x) = g(x)$ kaikilla $x \in X$.

Esimerkki 9.32. Tarkastellaan kuvauksia $f: \mathbb{R} \rightarrow [0, \infty[$, $g: \mathbb{Z} \rightarrow \mathbb{N}$ ja $h: \mathbb{N} \rightarrow \mathbb{N}$, joilla kaikilla $x \mapsto |2x + 2|$. Niiden kuvaajat on piirretty kuvaan 9.25. Kuvaukset f , g ja h ovat kaikki eri kuvauksia, sillä niiden lähtö- ja maalijoukot eivät ole samoja.



Kuva 9.25: Kuvaukset f , g ja h ovat eri kuvauksia.

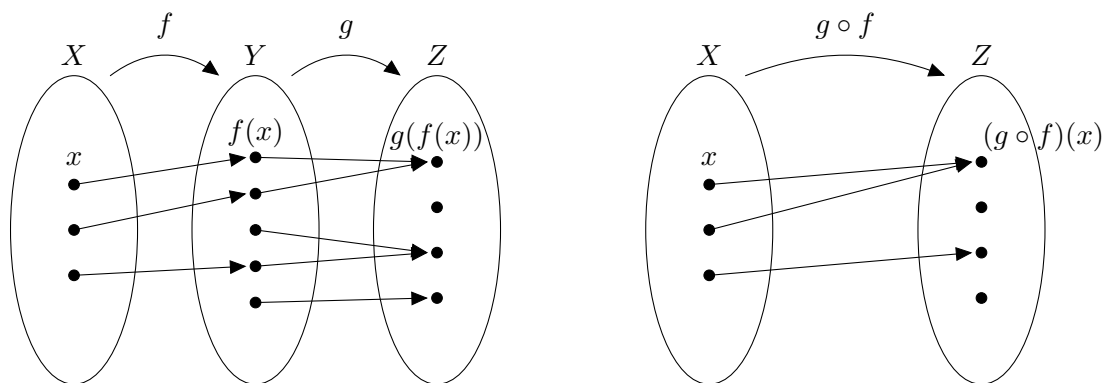
9.6 Yhdistetty kuvaus

Määritelmä 9.33. Oletetaan, että $f: X \rightarrow Y$ ja $g: Y \rightarrow Z$ ovat kuvauksia. *Yhdistetty kuvaus* $g \circ f: X \rightarrow Z$ määritellään asettamalla

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

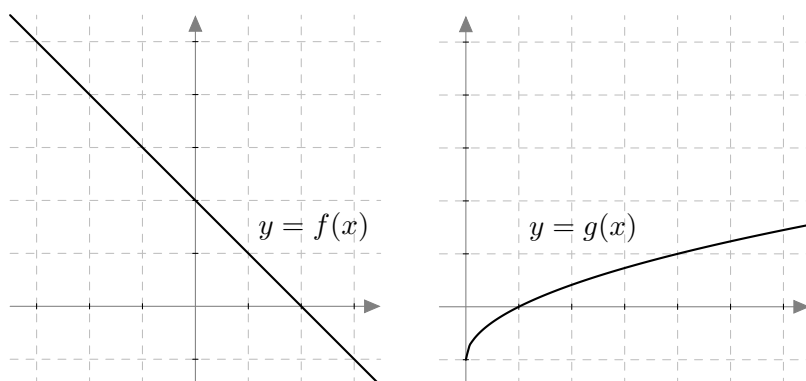
kaikilla $x \in X$.

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 9.26.



Kuva 9.26: Yhdistetty kuvaus $g \circ f: X \rightarrow Z$ määritellään asettamalla $(g \circ f)(x) = g(f(x))$.

Esimerkki 9.34. Tarkastellaan funktiota $f: \mathbb{R} \rightarrow \mathbb{R}$, jolla $f(x) = 2 - x$ kaikilla $x \in \mathbb{R}$, ja funktiota $g: [0, \infty[\rightarrow \mathbb{R}$, jolla $g(x) = \sqrt{x} - 1$ kaikilla $x \geq 0$. Niiden kuvaajat on piirretty kuvaan 9.27.



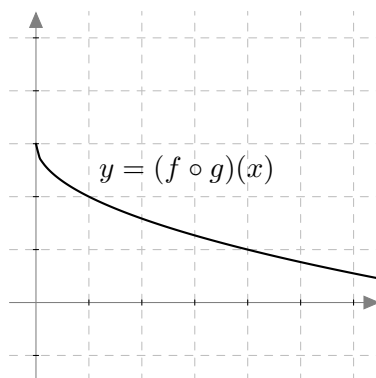
Kuva 9.27: Esimerkin 9.34 funktioiden f ja g kuvaajat.

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

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

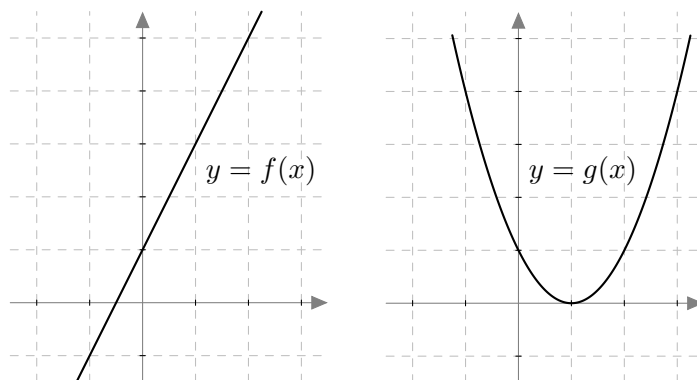
$$(f \circ g)(x) = f(g(x)) = f(\sqrt{x} - 1) = 2 - (\sqrt{x} - 1) = 2 - \sqrt{x} + 1 = 3 - \sqrt{x}.$$

Sen kuvaaja on piirretty kuvaan 9.28.



Kuva 9.28: Yhdistetyn funktion $f \circ g$ kuvaaja.

Esimerkki 9.35. Tarkastellaan funktioita $f: \mathbb{R} \rightarrow \mathbb{R}$ ja $g: \mathbb{R} \rightarrow \mathbb{R}$, joilla $f(x) = 1 + 2x$ ja $g(x) = (x - 1)^2$ kaikilla $x \in \mathbb{R}$. Niiden kuvaajat on piirretty kuvaan 9.29.



Kuva 9.29: Esimerkin 9.35 funktioiden f ja g kuvaajat.

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

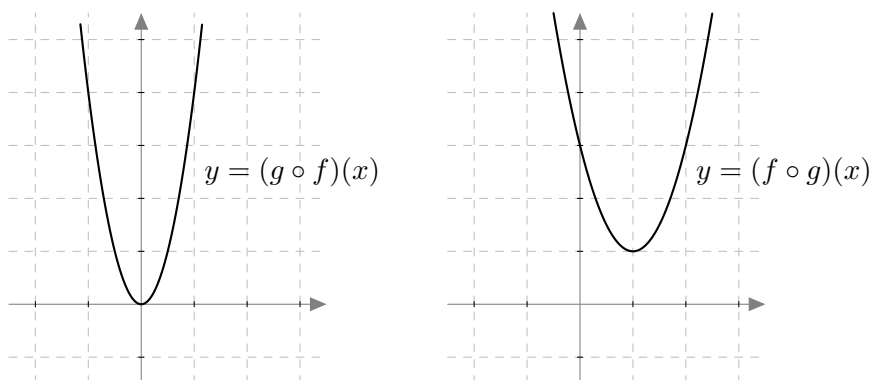
$$(g \circ f)(x) = g(f(x)) = g(1 + 2x) = (1 + 2x - 1)^2 = (2x)^2 = 4x^2$$

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

Myös yhdistetty kuvaus $f \circ g: \mathbb{R} \rightarrow \mathbb{R}$ 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 9.30. Havaitaan, että $g \circ f \neq f \circ g$, sillä esimerkiksi $(g \circ f)(0) = 0$ mutta $(f \circ g)(0) = 3$.



Kuva 9.30: Esimerkin 9.35 yhdistettyjen funktioiden $g \circ f$ ja $f \circ g$ kuvaajat.

Seuraavissa esimerkeissä osoitetaan, että injktiivisistä kuvauksista yhdistetty kuvaus on injktio ja surjektivisista kuvauksista yhdistetty kuvaus on surjektio.

Esimerkki 9.36. Oletetaan, että $f: X \rightarrow Y$ ja $g: Y \rightarrow Z$ ovat injktioita. Osoitetaan, että yhdistetty kuvaus $g \circ f: X \rightarrow Z$ on injktio.

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 injktiivisyyden nojalla tästä yhtälöstä seuraa, että $f(a) = f(b)$. Myös kuvaus f on injktio, joten yhtälöstä $f(a) = f(b)$ seuraa, että $a = b$.

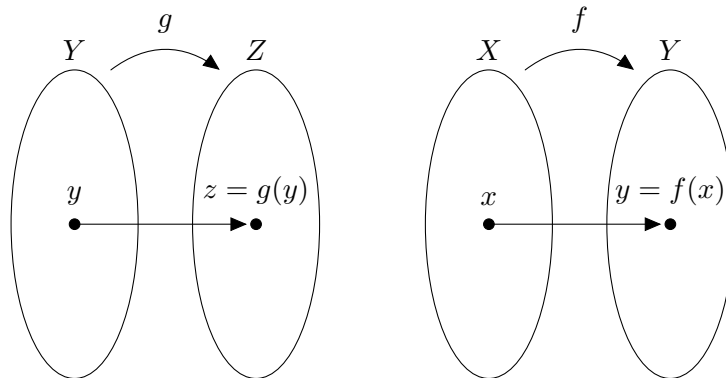
Näin on näytetty, että yhtälöstä $(g \circ f)(a) = (g \circ f)(b)$ seuraa, että $a = b$. Siis $g \circ f$ on injktio.

Esimerkki 9.37. Oletetaan, että $f: X \rightarrow Y$ ja $g: Y \rightarrow Z$ ovat surjektioita. Osoitetaan, että yhdistetty kuvaus $g \circ f: X \rightarrow Z$ 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 9.31.



Kuva 9.31: Kuvausten g ja f surjektiivisuuden avulla löydetään ensin y ja sitten x .

Esimerkki 9.38. Oletetaan, että $f: X \rightarrow Y$, $g: Y \rightarrow Z$ ja $h: Z \rightarrow W$ ovat kuvauksia. Osoitetaan, että kuvausten yhdistäminen on liitännäinen operaatio eli että yhdistetyt kuvaukset $h \circ (g \circ f): X \rightarrow W$ ja $(h \circ g) \circ f: X \rightarrow W$ 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

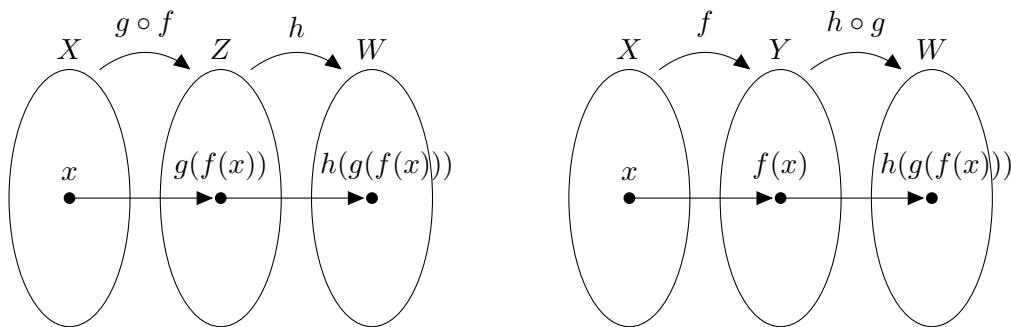
$$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x))).$$

Näiden kuvausten muodostumista on havainnollistettu alla kuvassa 9.32.

Havaitaan, että kaikilla $x \in X$ pätee

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

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



Kuva 9.32: Kuvausten yhdistäminen on liitännäinen operaatio eli $h \circ (g \circ f) = (h \circ g) \circ f$.

9.7 Käänteiskuvaus ja bijektio

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

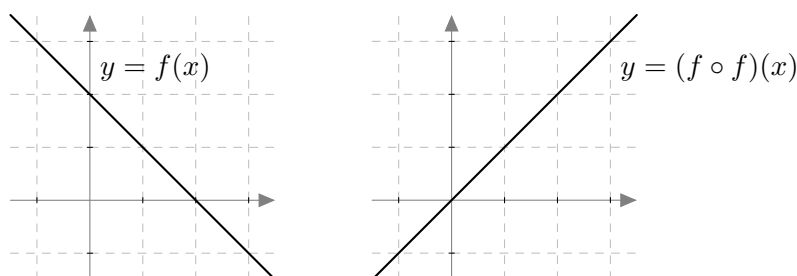
itelmä Joukon X *identtinen kuvaus* tarkoittaa kuvausta $\text{id}_X: X \rightarrow X$, jolla $\text{id}_X(x) = x$ kaikilla $x \in X$.

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 9.39. Tarkastellaan kuvausta $f: \mathbb{R} \rightarrow \mathbb{R}$, jolla $f(x) = 2 - x$ kaikilla $x \in \mathbb{R}$. Määritetään yhdistetty kuvaus $f \circ f: \mathbb{R} \rightarrow \mathbb{R}$. 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 $(f \circ f)(x) = x = \text{id}_{\mathbb{R}}(x)$ kaikilla $x \in \mathbb{R}$. Yhdistetty kuvaus $f \circ f: \mathbb{R} \rightarrow \mathbb{R}$ on siis sama kuin joukon \mathbb{R} identtinen kuvaus $\text{id}_{\mathbb{R}}$ eli $f \circ f = \text{id}_{\mathbb{R}}$.



Kuva 9.33: Esimerkin 9.39 kuvaukselle f pätee $f \circ f = \text{id}$.

Määritelmä 9.40. Oletetaan, että $f: X \rightarrow Y$ on kuvaus. Jos on olemassa sellainen kuvaus $g: Y \rightarrow X$, että

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

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

Esimerkissä 9.39 näytettiin, että kuvaukselle $f: \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = 2 - x$, pätee $f \circ f = \text{id}$. Tämä tarkoittaa määritelmän 9.40 mukaan, että kuvaus f on oma käänteiskuvausnsa eli $f^{-1} = f$.

Esimerkki 9.41. Tarkastellaan funktioita $f: \mathbb{R} \rightarrow \mathbb{R}$ ja $g: \mathbb{R} \rightarrow \mathbb{R}$, 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

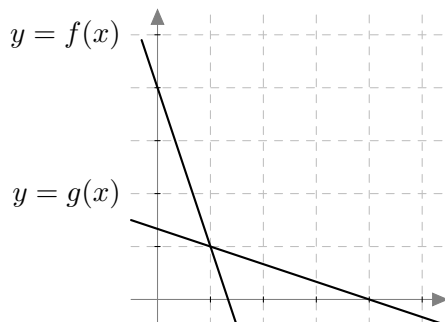
$$(g \circ f)(x) = g(f(x)) = g(4 - 3x) = \frac{4}{3} - \frac{4 - 3x}{3} = \frac{4}{3} - \frac{4}{3} + x = x = \text{id}(x).$$

Tästä voidaan päätellä, että $g \circ f: \mathbb{R} \rightarrow \mathbb{R}$ ja $\text{id}: \mathbb{R} \rightarrow \mathbb{R}$ ovat sama kuvaus eli $g \circ f = \text{id}$. Lisäksi

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

Tästä voidaan päätellä, että $f \circ g: \mathbb{R} \rightarrow \mathbb{R}$ ja $\text{id}: \mathbb{R} \rightarrow \mathbb{R}$ ovat sama kuvaus eli $f \circ g = \text{id}$.

Havaitaan, että käänteiskuvauksen määritelmän ehdot täyttyvät: $g \circ f = \text{id}$ ja $f \circ g = \text{id}$ eli kumpikin yhdistetty kuvaus on identtinen kuvaus. Siis g on kuvauksen f käänteiskuvaus eli $g = f^{-1}$. Tilannetta on havainnollistettu kuvassa 9.34.



Kuva 9.34: Kuvaukset f ja g ovat toistensa käänteiskuvauksia.

Käänteiskuvauksen määritelmä 9.40 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 9.43. Sitä ennen esimerkissä 9.42 havaitaan, että identtisen kuvauksen yhdistäminen toiseen kuvaukseen ei muuta tätä kuvausta.

Esimerkki 9.42. Olkoon $f: X \rightarrow Y$ kuvaus. Näytetään, että $f \circ \text{id}_X = f$ ja $\text{id}_Y \circ f = f$.

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

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

Tästä nähdään, että kuvaukset $f \circ \text{id}_X: X \rightarrow Y$ ja $f: X \rightarrow Y$ ovat samat eli $f \circ \text{id}_X = f$. Toisaalta myös

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

Siis kuvaukset $\text{id}_Y \circ f: X \rightarrow Y$ ja $f: X \rightarrow Y$ ovat samat eli $\text{id}_Y \circ f = f$.

Esimerkki 9.43. Osoitetaan, että kuvauksella $f: X \rightarrow Y$ on enintään yksi käänteiskuvaus.

Tehdään vasta oletus, että kuvauksella f on ainakin kaksi käänteiskuvausta. Vastaoletuksen nojalla on siis olemassa kuvaukset $g: Y \rightarrow X$ ja $h: Y \rightarrow X$, joille pätee $g \neq h$ sekä lisäksi käänteiskuvausten määritelmän nojalla $g \circ f = \text{id}_X$, $f \circ g = \text{id}_Y$, $h \circ f = \text{id}_X$ ja $f \circ h = \text{id}_Y$. Käyttämällä näitä yhtälöitä sekä esimerkkien 9.42 ja 9.38 tuloksia saadaan

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

Vastaoletus johti ristiriitaan $g \neq h$ ja $g = h$. Siis alkuperäinen väite pätee eli kuvauksella $f: X \rightarrow Y$ 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 9.44. *Bijektio* tarkoittaa kuvausta, joka on sekä injektio että surjektio.

Lause 9.45. *Oletetaan, että $f: X \rightarrow Y$ on kuvaus. Kuvauksella f on käänteiskuvaus, jos ja vain jos kuvaus f on bijektio.*

Todistus. ” \Rightarrow ”: Oletetaan, että on olemassa $f^{-1}: Y \rightarrow X$. 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

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

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

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

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 $f: X \rightarrow Y$ on surjektio. Oletetaan, että $y \in Y$. Koska f^{-1} on kuvaus $Y \rightarrow X$, niin on olemassa tasan yksi $f^{-1}(y) \in X$. Lisäksi

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

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 $f: X \rightarrow Y$ 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 $Y \rightarrow X$. 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 $g \circ f: X \rightarrow X$. 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

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

Havaitaan, että kuvaukset $g \circ f: X \rightarrow X$ ja $\text{id}_X: X \rightarrow X$ ovat samat eli $g \circ f = \text{id}_X$.

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

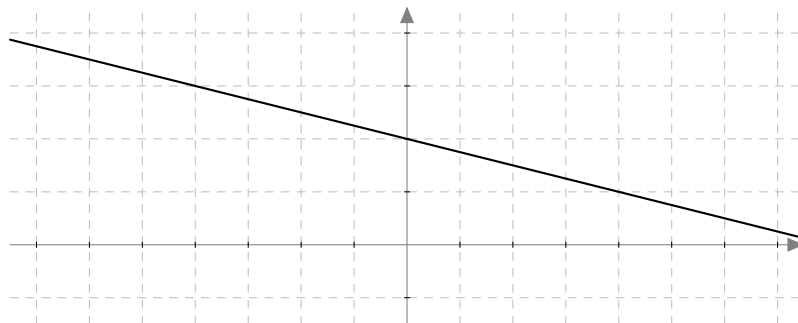
$$(f \circ g)(y) = f(g(y)) = f(x) = y = \text{id}_Y(y).$$

Havaitaan, että kuvaukset $f \circ g: Y \rightarrow Y$ ja $\text{id}_Y: Y \rightarrow Y$ ovat samat eli $f \circ g = \text{id}_Y$.

Näin on osoitettu, että g on kuvauksen f käänteiskuvaus eli $g = f^{-1}$.

□

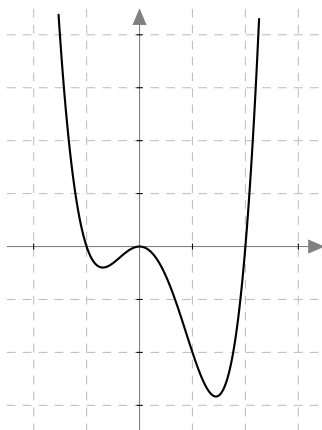
Esimerkki 9.46. Esimerkeissä 9.22 ja 9.27 tarkasteltu kuvaus $g: \mathbb{R} \rightarrow \mathbb{R}$, $g(x) = 2 - 0,25x$, on sekä injektio että surjektio. Kuvaus g on siis bijektio, joten sillä on lauseen 9.45 nojalla käänteiskuvaus $g^{-1}: \mathbb{R} \rightarrow \mathbb{R}$.



Kuva 9.35: Funktio $x \mapsto 2 - 0,25x$ on bijektio.

Esimerkki 9.47. Tarkastellaan funktiota $h: \mathbb{R} \rightarrow \mathbb{R}$, jolla $h(x) = x^4 - x^3 - 2x^2$ kaikilla $x \in \mathbb{R}$. Osa sen kuvaajasta on piirretty kuvaan 9.36.

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 käänteisfunktioita.



Kuva 9.36: Funktio $x \mapsto x^4 - x^3 - 2x^2$ ei ole bijektio, joten sillä ei ole käänteisfunktioita.

Esimerkki 9.48. Tarkastellaan kuvausta $g: \mathbb{Z} \rightarrow \mathbb{Z}$, 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 9.49. Tarkastellaan funktiota $f: \mathbb{R} \setminus \{1\} \rightarrow \mathbb{R} \setminus \{2\}$, jolla

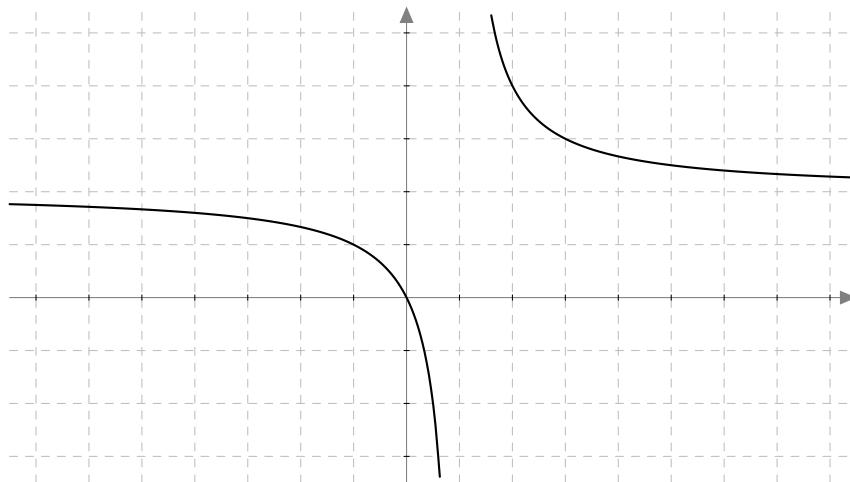
$$f(x) = \frac{2x}{x-1}$$

kaikilla $x \in \mathbb{R} \setminus \{1\}$. Osa sen kuvaajasta on piirretty kuvaan 9.37.

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 9.37: 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 $\mathbb{R} \setminus \{2\} \rightarrow \mathbb{R} \setminus \{1\}$, ja että (2) käänteiskuvauksen määritelmän ehdot täyttyvät.

- (1) Oletetaan, että $y \in \mathbb{R} \setminus \{2\}$. Tällöin osamäärä $-y/(2-y)$ on määritelty, sillä nimittäjä on nolasta poikkeava. Lisäksi osamäärä on yksikäsitteinen ja kuuluu joukkoon $\mathbb{R} \setminus \{1\}$: yhtälöstä $-y/(2-y) = 1$ seuraisi $-y = 2 - y$ eli $0 = 2$, mikä on mahdotonta.

Siis voidaan määritellä kuvaus $g: \mathbb{R} \setminus \{2\} \rightarrow \mathbb{R} \setminus \{1\}$ asettamalla

$$g(x) = \frac{-x}{2-x}$$

kaikilla $x \in \mathbb{R} \setminus \{2\}$.

- (2) Osoitetaan, että g on kuvauksen f käänteiskuvaus. Oletetaan, että $x \in \mathbb{R} \setminus \{2\}$. Tällöin

$$\begin{aligned} (f \circ g)(x) &= f(g(x)) \\ &= f\left(\frac{-x}{2-x}\right) = \frac{2 \cdot \left(\frac{-x}{2-x}\right)}{\left(\frac{-x}{2-x}\right) - 1} = \frac{\frac{-2x}{2-x}}{\left(\frac{-x}{2-x}\right) - \left(\frac{2-x}{2-x}\right)} = \frac{\frac{-2x}{2-x}}{\frac{-x - (2-x)}{2-x}} \\ &= \frac{-2x}{(2-x)} \cdot \frac{(2-x)}{-x - 2 + x} = \frac{-2x}{-2} = x = \text{id}(x). \end{aligned}$$

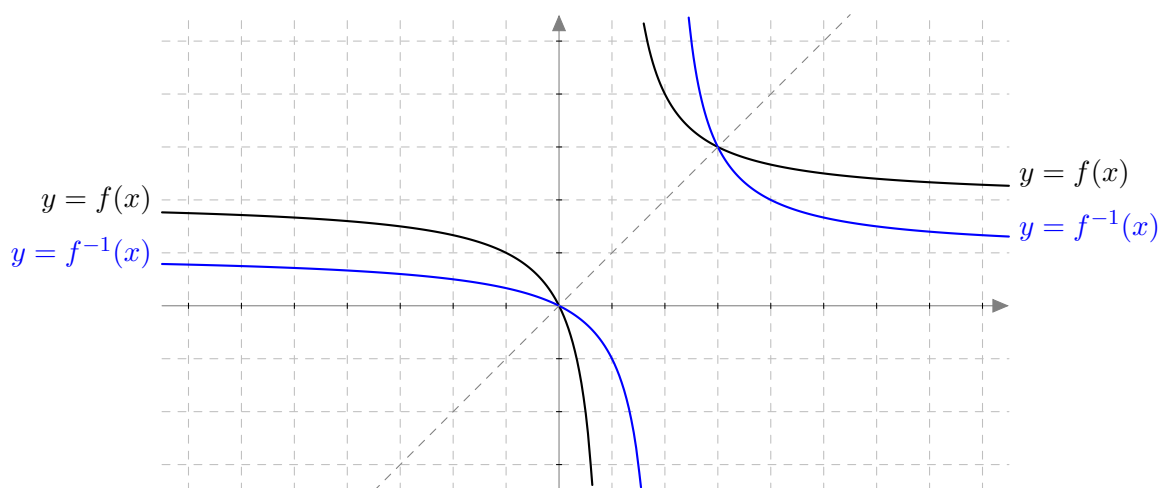
Siis kuvaukset $f \circ g$ ja $\text{id}: \mathbb{R} \setminus \{2\} \rightarrow \mathbb{R} \setminus \{2\}$ ovat sama kuvaus eli $f \circ g = \text{id}$.

Oletetaan vielä, että $x \in \mathbb{R} \setminus \{1\}$. Tällöin

$$\begin{aligned}
 (g \circ f)(x) &= g(f(x)) \\
 &= g\left(\frac{2x}{x-1}\right) = \frac{-\left(\frac{2x}{x-1}\right)}{2 - \left(\frac{2x}{x-1}\right)} = \frac{\frac{-2x}{x-1}}{\frac{2(x-1)}{(x-1)} - \left(\frac{2x}{x-1}\right)} = \frac{\frac{-2x}{x-1}}{\frac{2x-2-2x}{x-1}} \\
 &= \frac{-2x}{(x-1)} \cdot \frac{(x-1)}{-2} = x = \text{id}(x).
 \end{aligned}$$

Siis kuvaukset $g \circ f$ ja $\text{id}: \mathbb{R} \setminus \{1\} \rightarrow \mathbb{R} \setminus \{1\}$ ovat sama kuvaus eli $g \circ f = \text{id}$.

Näin on osoitettu, että $f \circ g = \text{id}_{\mathbb{R} \setminus \{2\}}$ ja $g \circ f = \text{id}_{\mathbb{R} \setminus \{1\}}$. Siis funktio g on funktion f käänteisfunktio eli $g = f^{-1}$. Tilannetta on havainnollistettu kuvassa 9.38.



Kuva 9.38: Funktion ja sen käänteisfunktion kuvaajat ovat symmetrisiä suoran $y = x$ suhteen.

10 Työkaluja reaalifunktioiden rakentamisen

10.1 Potenssit ja juuret

Tässä luvussa käsitellään koulusta potensseja ja juuria. Jos haluat kerrata nämä käsitteet vielä tarkemmin, löydät aiheeseen liittyvää lukiomatematiikan materiaalia osoitteesta <https://kisallioppiminen.fi/kurssit/maa2/luku4>.

Reaaliluvuille voidaan määritellä kokonaislukupotenssit. Negatiiviset potenssit määritellään käänteislukujen avulla.

Määritelmä 10.1. Olkoon n positiivinen kokonaisluku. Tällöin

1. $x^n = \underbrace{x \cdot x \cdots x}_{n \text{ kpl}}$
2. $x^0 = 1$
3. $x^{-n} = \frac{1}{x^n}$.

Edellisessä määritelmässä lukua x kutsutaan *kantaluvuksi* ja lukua n *eksponentiksi*. Seuraavaan lauseeseen on kerätty potenssien laskusääntöjä:

Lause 10.2. Olkoot $x, y \in \mathbb{R}$. Seuraavat kaavat pätevät kaikilla kokonaisluvuilla m ja n :

- a) $(x^n)^{-1} = (x^{-1})^n$
- b) $x^m \cdot x^n = x^{m+n}$
- c) $\frac{x^m}{x^n} = x^{m-n}$, jos $x \neq 0$.
- d) $(x^n)^m = x^{mn}$
- e) $(xy)^m = x^m y^m$
- f) $\left(\frac{x}{y}\right)^m = \frac{x^m}{y^m}$, jos $y \neq 0$.

Ennen lauseen todistusta havainnollistetaan sen joitakin tapauksia positiivisten kokonaislukujen ja kantaluvun 2 tapauksessa. Oletetaan, että $m, n \in \mathbb{N} \setminus \{0\}$. Tällöin

$$2^m \cdot 2^n = \underbrace{(2 \cdots 2)}_{m \text{ kpl}} \cdot \underbrace{(2 \cdot 2 \cdots 2)}_{n \text{ kpl}} = \underbrace{2 \cdot 2 \cdot 2 \cdots 2}_{m+n \text{ kpl}} = 2^{m+n}$$

ja

$$(2^m)^n = \underbrace{(2^m) \cdot (2^m) \cdots (2^m)}_{n \text{ kpl}} = \underbrace{(2 \cdots 2)}_{m \text{ kpl}} \cdot \underbrace{(2 \cdots 2)}_{m \text{ kpl}} \cdots \underbrace{(2 \cdots 2)}_{m \text{ kpl}} = \underbrace{2 \cdot 2 \cdot 2 \cdots 2}_{nm \text{ kpl}} = 2^{nm}.$$

Todistus. Todistetaan osa väitteistä. a) Väitteen osoittamiseksi on tarkasteltava eri tapauksia sen mukaan, onko n positiivinen, negatiivinen vai nolla. Tapaukset ovat hyvin samankaltaisia, joten todistamme niistä esimerkin vuoksi vain yhden.

Oletetaan, että $n > 0$. Tällöin

$$\begin{aligned} x^n \cdot (x^{-1})^n &= \underbrace{x \cdot x \cdots x}_{n \text{ kpl}} \cdot \underbrace{x^{-1} \cdot x^{-1} \cdots x^{-1}}_{n \text{ kpl}} \\ &= \underbrace{x \cdot x \cdots x}_{n-1 \text{ kpl}} \cdot 1 \cdot \underbrace{x^{-1} \cdot x^{-1} \cdots x^{-1}}_{n-1 \text{ kpl}} \\ &= \cdots = 1. \end{aligned}$$

Siten $x^n \cdot (x^{-1})^n = 1$, mistä seuraa, että $(x^n)^{-1} = (x^{-1})^n$. Samalla tavoin nähdään, että $(x^{-1})^n \cdot x^n = e$. Käänteisalkion määritelmän perusteella $(x^{-1})^n$ on alkion x^n käänteisalkio, eli $(x^n)^{-1} = (x^{-1})^n$.

b) Nyt on tarkasteltava eri tapauksia sen mukaan, ovatko m , n ja $m + n$ positiivisia, negatiivisia vai nollia. Todistetaan tapaus, jossa $m > 0$, $n < 0$ ja $m + n < 0$. Merkitään $n' = -n$. Nyt $n' > 0$ ja $m < n'$. Kohdan a) nojalla pätee $x^n = x^{-n'} = (x^{n'})^{-1} = (x^{-1})^{n'}$, joten voidaan päätellä seuraavasti:

$$\begin{aligned} x^m \cdot x^n &= \underbrace{x \cdot x \cdots x}_{m \text{ kpl}} \cdot \underbrace{x^{-1} \cdot x^{-1} \cdots x^{-1}}_{n' \text{ kpl}} \\ &= \underbrace{x^{-1} \cdot x^{-1} \cdots x^{-1}}_{n'-m \text{ kpl}} \\ &= (x^{-1})^{n'-m} = (x^{n'-m})^{-1} \\ &= x^{-(n'-m)} = x^{m+n}. \end{aligned}$$

d) Myös tällä kertaa on tarkasteltava useita tapauksia. Todistamme väitteen siinä tapauksessa, että $m < 0$ ja $n > 0$. Merkitään $m' = -m$, jolloin m' on positiivinen. Käyttämällä jälleen a)-kohdassa osoitettua tulosta saadaan

$$\begin{aligned} (x^n)^m &= (x^n)^{-m'} = ((x^n)^{-1})^{m'} = ((x^{-1})^n)^{m'} \\ &= \underbrace{x^{-1} \cdot x^{-1} \cdots x^{-1}}_{n \text{ kpl}} \cdots \underbrace{x^{-1} \cdot x^{-1} \cdots x^{-1}}_{n \text{ kpl}} \\ &\quad \underbrace{\hspace{10em}}_{m' \text{ kpl}} \\ &= \underbrace{x^{-1} \cdot x^{-1} \cdots x^{-1}}_{m'n \text{ kpl}} = (x^{-1})^{m'n} = x^{-m'n} = x^{mn}. \end{aligned}$$

Muiden tapauksien läpikäyminen jätetään harjoitustehtäväksi. □

Reaaliluvun eksponentti voi olla myös murtoluku. Oletetaan, että $n \in \mathbb{Z}$ ja x on positiivinen reaaliluku. Tällöin

$$x^{\frac{1}{n}} = \sqrt[n]{x}.$$

Jos lisäksi $m \in \mathbb{Z} \setminus \{0\}$, määritellään

$$x^{\frac{m}{n}} = \left(x^{\frac{1}{n}}\right)^m.$$

Esimerkiksi $x^3 = \sqrt[3]{x}$ ja $x^{\frac{2}{3}} = (\sqrt[3]{x})^2$.

Edelleen potenssin määritelmää voidaan laajentaa niin, että eksponentiksi voi laittaa minkä tahansa reaaliluvun. Tällöin lauseessa 10.2 esitellyt laskusäännöt pätevät myös reaalilukueksponenteille. Tämän lauseen todistus sivuutetaan.

Lause 10.3. *Olkoot $x, y \in \mathbb{R}$. Seuraavat kaavat pätevät kaikilla reaaliluvuilla m ja n , kun kantaluku on positiivinen:*

a) $(x^n)^{-1} = (x^{-1})^n$

b) $x^m \cdot x^n = x^{m+n}$

c) $\frac{x^m}{x^n} = x^{m-n}$ jos $x \neq 0$.

d) $(x^n)^m = x^{mn}$

e) $(xy)^m = x^m y^m$

f) $\left(\frac{x}{y}\right)^m = \frac{x^m}{y^m}$, jos $y \neq 0$.

10.2 Polynomit

Tässä luvussa käsitellään polynomeja. Jos haluat kerrata polynomifunktion käsitteen lukiomatematiikan näkökulmasta, löydät lisämateriaalia osoitteesta <https://kisallioppiminen.fi/kurssit/maa2/>.

Yhden tuntemattoman polynomi on äärellinen summa

$$p(x) = \sum_{k=0}^n a_k x^k = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$

missä $n \in \mathbb{N}$ ja $a_k \in \mathbb{R}$ kaikilla k . Lukuja a_n, \dots, a_0 kutsutaan polynomin $p(x)$ *kertoimiksi* ja symbolia x polynomin $p(x)$ *tuntemattomaksi* tai *muuttujaksi*. Summattavat $a_i x^i$ ovat polynomin *termejä*. Esimerkiksi

$$p(x) = 2x^3 - x^2 + 3x + 5$$

on polynomi

Kaksi polynomia ovat samat, jos ja vain jos niiden toisiaan vastaavissa termeissä on samat kertoimet. Jos jonkin termin kerroin on nolla, termi voidaan jättää kirjoittamatta. Lisäksi termien järjestystä polynomilausekkeessa saa muuttaa. Näin ollen esimerkiksi polynomit $3x^3 - 2x^2 + 0x + 2$ ja $2 - 2x^2 + 3x^3$ ovat samoja. Polynomit $-2x^4 - x + 5$ ja $-2x^4 - x - 5$ puolestaan eivät ole samoja.

Polynomeille voidaan määritellä yhteenlasku, jossa toisiaan vastaavien termien kertoimet lasketaan yhteen. Esimerkiksi polynomien $3x^2 - 4x + 10$ ja $-2x^5 - x^3 + 5x^2 + 4x$ summa on polynomi

$$-2x^5 - x^3 + 8x^2 + 10.$$

Polynomien tulo voidaan laskea kohtelemalla polynomeja laskulausekkeina ja käyttämällä osittelulakia sulkujen avaamiseksi. Esimerkiksi

$$\begin{aligned} (-4x^4 + 2x^2)(x^3 + 3x^2 + 2) &= -4x^7 - 12x^6 - 8x^4 + 2x^5 + 6x^4 + 4x^2 \\ &= -4x^7 - 12x^6 + 2x^5 - 2x^4 + 4x^2. \end{aligned}$$

Tutkitaan seuraavaksi, kuinka polynomeista voi muodostaa polynomifunktioita. Jos c on reaaliluku ja $p(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ on polynomi, merkitään

$$p(c) = a_0 + a_1c + a_2c^2 + \dots + a_nc^n.$$

Sanotaan, että alkio c on *sijoitettu* polynomiin $p(x)$. Esimerkiksi polynomiin $p(x) = -x^3 + 3x + 2$ voidaan sijoittaa luku 3, jolloin saadaan tulokseksi

$$p(3) = -3^3 + 3 \cdot 3 + 2 = -27 + 9 + 2 = -16.$$

Sijoituksen avulla voidaan määritellä polynomia $p(x)$ vastaava *polynomifunktio*

$$p: \mathbb{R} \rightarrow \mathbb{R}, \quad c \mapsto p(c).$$

Esimerkiksi polynomista $p(x) = -x^3 + 3x + 2 \in \mathbb{R}[x]$ saadaan polynomifunktio $p: \mathbb{R} \rightarrow \mathbb{R}$, $p(x) = -x^3 + 3x + 2$.

Usein polynomien ja polynomifunktioiden välille ei tehdä eroa. Tarkalleen ottaen polynomi on kuitenkin summalauseke ja polynomifunktio on kuvaus. Reaalilukukertoimisten polynomien tapauksessa polynomit ja niistä saadut polynomifunktiot voidaankin samastaa keskenään. Kun polynomit määritellään yleisemmin niin, etteivät kertoimet välttämättä ole reaalilukuja, eivät polynomit ja polynomifunktiot enää olekaan sama asia.

Määritelmä 10.4. Olkoon $p(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ polynomi. Oletetaan lisäksi, että $a_n \neq 0$. Lukua n kutsutaan polynomien *asteeksi* ja merkitään $\deg(p(x))$.

Polynomia, jonka aste on nolla, kutsutaan *vakiopolynomiksi*. Myös nollopolynomi 0 laskeaan vakiopolynomiksi, mutta sen astetta ei määritellä.

Esimerkiksi polynomien $-2x^5 - x^3 + 8x^2 + 10$ aste on 5.

Polynomien tulon asteen voi selvittää tekijöiden asteiden perusteella.

Lause 10.5. Oletetaan, että $p(x)$ ja $q(x)$ ovat nollostapoikkeavia polynomeja. Tällöin

$$\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x)).$$

Todistus. Oletetaan, että

$$p(x) = a_0 + a_1x + \cdots + a_mx^m \quad \text{ja} \quad q(x) = b_0 + b_1x + \cdots + b_nx^n,$$

missä $a_m \neq 0$ ja $b_n \neq 0$. Tällöin $\deg(p(x)) = m$ ja $\deg(q(x)) = n$. Polynomien tulo on

$$p(x)q(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + a_mb_nx^{m+n}.$$

Koska $a_m \neq 0$ ja $b_n \neq 0$, täytyy päteä $a_mb_n \neq 0$. Tästä seuraa, että $\deg(p(x)q(x)) = m+n$. \square

Määritelmä 10.6. Reaaliluku c on polynomien $p(x)$ *juuri*, jos $p(c) = 0$.

Vakiopolynomilla ei voi olla juuria, ellei se ole nollapolynomi. Toisaalta jos polynomi $p(x)$ ei sisällä lainkaan vakiotermiä (potenssia 0 vastaava kerroin on nolla), sille pätee $p(0) = 0$ eli nolla-alkio on sen juuri.

Polynomeille määritellään jaollisuus samalla tavalla kuin kokonaisluvuille.

Määritelmä 10.7. Polynomi $p(x)$ on *jaollinen polynomilla* $q(x)$, jos on olemassa sellainen polynomi $r(x)$, että $p(x) = r(x)q(x)$. Tällöin merkitään $q(x) \mid p(x)$.

Jos $p(x)$ on jaollinen polynomilla $q(x)$, sanotaan myös, että $q(x)$ *jakaa* $p(x)$:n tai $q(x)$ on $p(x)$:n *tekijä*. Esimerkiksi polynomi $x^2 - 1$ on jaollinen polynomilla $x + 1$, sillä $x^2 - 1 = (x - 1)(x + 1)$. Se on jaollinen myös vakiopolynomilla 3, sillä $x^2 - 1 = \frac{1}{3}(x^2 - 1) \cdot 3$.

Jos kokonaisluvun yrittää jakaa toisella kokonaisluvulla eikä jako mene tasan, jää jäljelle jakojäännös. Esimerkiksi $19 = 3 \cdot 5 + 4$, missä jakojäännös on 4. Tätä kutsutaan jakoyhtälöksi. Sama ilmiö esiintyy polynomeilla.

Lause 10.8. (Polynomien jakoyhtälö.) *Oletetaan, että $p(x)$ on polynomi ja $s(x)$ on nollasta poikkeava polynomi. Tällöin on olemassa yksikäsitteiset polynomit $q(x)$ ja $r(x)$, joille pätee*

$$p(x) = q(x)s(x) + r(x)$$

ja joko $r(x) = 0$ tai $\deg(r(x)) < \deg(s(x))$.

Todistus. Todistusta ei esitetä tässä, sillä se on melko pitkä. Lauseen todistusta käsitellään algebran kurssilla. \square

Polynomeille voi löytää tekijöitä juurten avulla.

Lause 10.9. *Oletetaan, että reaaliluku c on polynomien $p(x)$ juuri. Tällöin $x - c$ on polynomien $p(x)$ tekijä.*

Todistus. Oletetaan, että reaaliluku c on polynomien $p(x)$ juuri. Jakoyhtälön perusteella on olemassa polynomit $q(x)$ ja $r(x)$, joille pätee $p(x) = q(x) \cdot (x - c) + r(x)$. Lisäksi täytyy olla joko $r(x) = 0$ tai

$$\deg(r(x)) < \deg(x - c) = 1,$$

ja kummassakin tapauksessa $r(x)$ on vakiopolynomi. Nyt $r(x) = p(x) - q(x) \cdot (x - c)$, joten edellisen lemmän perusteella

$$r(c) = p(c) - q(c - c) = 0 - 0 = 0.$$

Koska $r(x)$ on vakiopolynomi, täytyy päteä $r(x) = 0$. Täten $p(x) = q(x) \cdot (x - c)$ eli $p(x)$ on jaollinen polynomilla $x - c$. \square

Esimerkiksi polynomilla $p(x) = 3x^3 + x^2 - 8x + 4$ on juuri -2 , sillä $p(-2) = 0$. Nyt edellisen lauseen mukaan $x + 2$ on polynomi $p(x)$ tekijä. Tämä tosiaankin pitää paikkansa, sillä

$$p(x) = (x - 2) \left(x^2 - \frac{5}{3}x + \frac{2}{3} \right).$$

Koska jokaisesta juuresta saadaan polynomille uusi tekijä, polynomien aste rajoittaa juurten määrää.

Lause 10.10 (Algebran peruslause). *Olkoon $p(x)$ nollasta poikkeava polynomi. Polynomien $p(x)$ juurten lukumäärä on korkeintaan $\deg(p(x))$.*

Todistus. Todistetaan väite induktiolla polynomien asteen suhteen.

1) *Alkuaskel.* Jos $\deg(p(x)) = 0$, polynomi P on nollasta poikkeava vakiopolynomi. Sillä ei ole juuria, joten väite pätee.

2) *Induktioaskel.* Oletetaan, että väite pätee luvulla n , ja osoitetaan, että se pätee myös luvulla $n + 1$. Olkoon $\deg(p(x)) = n + 1$. Jos polynomilla P ei ole juuria, väite on todistettu. Oletetaan siis, että $p(x)$:llä on juuri $a \in K$. Tällöin lauseen 10.9 perusteella on olemassa polynomi $q(x)$, jolle pätee $p(x) = (x - a)q(x)$. Olkoon nyt $b \in K$ polynomien $pq(x)$ juuri. Tällöin

$$0 = p(b) = (b - a)q(b).$$

Tulon nollasäännön perusteella täytyy päteä joko $b - a = 0$ tai $q(b) = 0$. Tästä seuraa, että $b = a$ tai b on polynomien $qq(x)$ juuri. Polynomilla $qq(x)$ on siis korkeintaan yksi juuri enemmän kuin polynomilla $q(x)$.

Koska $pq(x) = (x - a)q(x)$, lauseesta 10.5 seuraa, että

$$\deg(q(x)) = \deg(pq(x)) - \deg(x - a) = n + 1 - 1 = n.$$

Induktio-oletuksen nojalla polynomilla $qq(x)$ on korkeintaan n juurta. Edellä nähtiin, että polynomien P juuria on korkeintaan yksi enemmän eli yhteensä enintään $n + 1$. Väite pätee siis luvulla $n + 1$.

Induktioperiaatteen nojalla lause on todistettu. \square

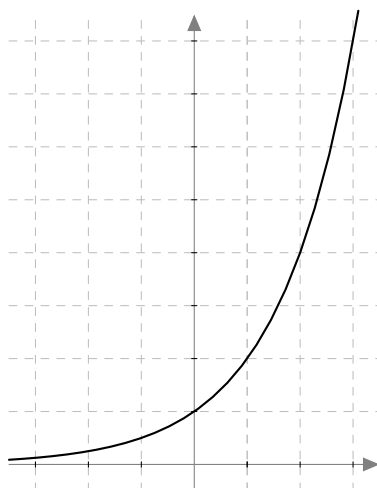
10.3 Eksponentti- ja logaritmfunktiot

Tämä luku on muokattu Lotta Oinosen materiaalista ”Johdatus yliopistomatematiikkaan”.

Tässä kappaleessa käsitellään eksponentti- ja logaritmfunktioita. Jos haluat kerrata näitä aiheita perusteellisemmin, löydät lukiomatematiikan lisämateriaalia osoitteesta <https://kisallioppiminen.fi/kurssit/maa8>.

Eksponttifunktio

Aloitetaan tarkastelemalla kaksikantaista eksponenttifunktiota $f: \mathbb{R} \rightarrow \mathbb{R}_+$, jolla $f(x) = 2^x$ kaikilla $x \in \mathbb{R}$. Alla kuvassa 10.39 on näkyvä osa sen kuvaajasta. Huomaa, että funktion f maaliksi voidaan valita positiivisten reaalilukujen joukko $\mathbb{R}_+ = \{x \in \mathbb{R} \mid x > 0\}$.



Kuva 10.39: 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

$$\begin{aligned} f(1/2) &= 2^{1/2} = \sqrt{2} \\ f(1/3) &= 2^{1/3} = \sqrt[3]{2} \\ f(-5/2) &= 2^{(-5/2)} = \frac{1}{2^{5/2}} = \frac{1}{\sqrt{2} \cdot \sqrt{2} \cdot \sqrt{2} \cdot \sqrt{2} \cdot \sqrt{2}} = \frac{1}{4\sqrt{2}} \end{aligned}$$

Jotta eksponenttifunktio saadaan määriteltyä koko reaalilukujen joukossa (siis erityisesti irrationaalilukujen $\mathbb{R} \setminus \mathbb{Q}$ joukossa), täytyy potenssi pystyä määrittelemään myös silloin, kun eksponentti on irrationaaliluku. Tähän tarvitaan enemmän matemaatiikan teoriaa. Emme syvenny siihen tässä sen tarkemmin.

Eksponttifunktiossa voi olla kantalukuna mikä tahansa positiivinen reaaliluku. Jos siis $k \in \mathbb{R}_+$, saadaan kuvaus

$$f: \mathbb{R} \mapsto \mathbb{R}, f(x) = k^x.$$

Eräs paljon käytetty ja sovelluksissa hyödyllinen kantaluku on Neperin luku $e \approx 2,718$, josta saadaan funktio

$$f : \mathbb{R} \mapsto \mathbb{R}, f(x) = e^x.$$

Logaritmifunktio

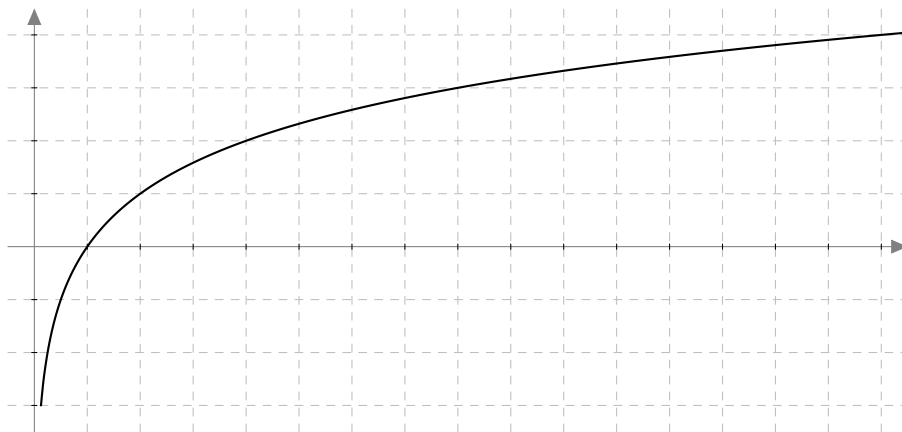
On mahdollista osoittaa, että eksponenttifunktiolla on käänteisfunktio. Tätä käänteisfunktiota kutsutaan logaritmiksi.

Määritelmä 10.11. Oletetaan, että $k \in \mathbb{R}_+$ ja $k \neq 1$. Logaritmifunktio $x \mapsto \log_k(x)$ on eksponenttifunktion $x \mapsto k^x$ käänteisfunktio. Toisin sanottuna

$$\log_k(x) = a \Leftrightarrow k^a = x.$$

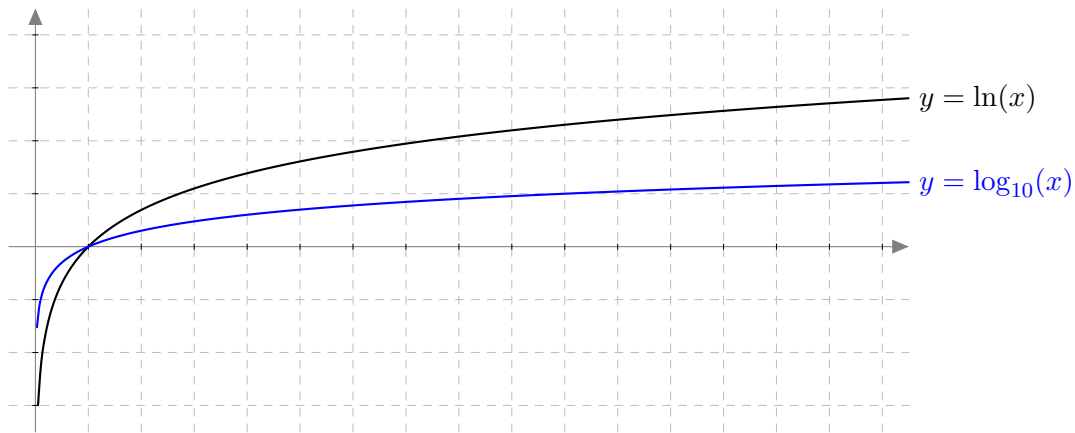
Edellä määriteltyä funktiota kutsutaan k -kantaiseksi logaritmifunktioksi.

Koska eksponenttifunktion kantalukuna voi olla vain positiivisia reaalilukuja, eksponenttifunktion arvot ovat aina positiivisia. Logaritmi on siis määritelty vain positiivisille reaaliluvuille. Määritelmän 10.11 mukaan logaritmi $\log_k(x)$ kertoo, mihin potenssiin luku k pitää korottaa, jolla tuloksena on x . Siis esimerkiksi $\log_2(8) = 3$ ja $\log_2(1) = 0$, sillä $2^3 = 8$ ja $2^0 = 1$. Osa kaksikantaisen logaritmifunktion kuvaajasta näkyy alla kuvassa 10.40.



Kuva 10.40: Osa kaksikantaisen logaritmifunktion $x \mapsto \log_2(x)$ kuvaajasta.

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 10.41.



Kuva 10.41: Logaritmifunktioiden $x \mapsto \log_{10}(x)$ ja $x \mapsto \ln(x)$ kuvaajat.

Kuvista näkyy, että logaritmifunktion arvot kasvavat melko hitaasti. Sama asia nähdään seuraavasta lauseesta.

Lause 10.12. *Oletetaan, että $k \in \mathbb{R}_+ \setminus \{1\}$, $x \in \mathbb{R}_+$ ja $c \in \mathbb{R}$. Tällöin $\log_k(x^c) = c \log_k(x)$.*

Todistus. Merkitään $a = \log_k(x)$. Tämä tarkoittaa logaritmin määritelmän 10.11 mukaan, että $k^a = x$. Soveltamalla lausetta 10.3 saadaan

$$x^c = (k^a)^c = k^{ca}.$$

Logaritmin määritelmän nojalla tällöin $\log_k(x^c) = ca$. Ottamalla huomioon, että $a = \log_k(x)$, päästään johtopäätökseen

$$\log_k(x^c) = c \log_k(x). \quad \square$$

Esimerkiksi luvun $1000 = 10^3$ 2-kantainen logaritmi on lauseen 10.12 nojalla vain kolminkertainen luvun 10 logaritmiin verrattuna: $\log_2(1000) = 3 \log_2(10)$.

Myös seuraava tulon logaritmia koskeva tulos perustuu lauseessa 10.3 mainittuihin eksponenttifunktion ominaisuuksiin.

Lause 10.13. *Oletetaan, että $k \in \mathbb{R}_+ \setminus \{1\}$ ja $x, y \in \mathbb{R}_+$. Tällöin $\log_k(xy) = \log_k(x) + \log_k(y)$.*

Todistus. Merkitään $a = \log_k(x)$ ja $b = \log_k(y)$. Logaritmin määritelmän 10.11 mukaan tällöin $x = k^a$ ja $y = k^b$. Soveltamalla lausetta 10.3 saadaan

$$xy = k^a \cdot k^b = k^{a+b}.$$

Tämä puolestaan tarkoittaa logaritmin määritelmän nojalla, että $\log_k(xy) = a + b$. Ottamalla huomioon, että $a = \log_k(x)$ ja $b = \log_k(y)$, päästään johtopäätökseen

$$\log_k(xy) = \log_k(x) + \log_k(y). \quad \square$$

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 10.12 ja 10.13 avulla saadaan vastaava tulos myös osamäärän logaritmile:

Lause 10.14. Oletetaan, että $k \in \mathbb{R}_+ \setminus \{1\}$ ja $x, y \in \mathbb{R}_+$. Tällöin $\log_k(x/y) = \log_k(x) - \log_k(y)$.

Todistus. Osamäärä x/y voidaan kirjoittaa tulona muodossa $x/y = x \cdot y^{-1}$. Soveltamalla lauseita 10.12–10.13 saadaan

$$\begin{aligned} \log_k\left(\frac{x}{y}\right) &= \log_k(x \cdot y^{-1}) = \log_k(x) + \log_k(y^{-1}) = \log_k(x) + (-1) \cdot \log_k(y) \\ &= \log_k(x) - \log_k(y). \end{aligned} \quad \square$$

Logaritmifunktion määritelmän mukaan $\log_k(x) = n$, jos ja vain jos $x = k^n$. Jälkimmäinen yhtälö voidaan kirjoittaa myös muodossa

$$\frac{x}{k^n} = 1.$$

Tämä tarkoittaa, että logaritmifunktion arvoja voidaan määrittää jakolaskun avulla. Asiaa on havainnollistettu seuraavissa esimerkeissä.

Esimerkki 10.15. 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 10.16. 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 $\log_2(24) \approx 5$.

EkspONENTTI- ja LOGARITMIYHTÄLÖIDEN RATKAISEMINEN

Esimerkki 10.17. Ratkaistaan yhtälö $2^x = 50$.

Tapa I: Käytetään 2-kantaisen logaritmin määritelmää, jonka mukaan

$$2^x = 50 \Leftrightarrow x = \log_2(50).$$

Siis yhtälöllä on tasan yksi ratkaisu, joka on $\log_2(50)$.

Ratkaisun likiarvo saadaan jakolaskun avulla:

Jaetaan lukua 50 kantaluvulla 2 kunnes tulos on mahdollisimman lähellä lukua 1:

$$\frac{50}{2} = 25, \quad \frac{25}{2} = 12,5, \quad \frac{12,5}{2} = 6,25, \quad \frac{6,25}{2} = 3,125, \\ \frac{3,125}{2} = 1,5625 \quad \frac{1,5625}{2} = 0,78125.$$

Päätellään, että $\log_2(50) \approx 6$, sillä kuudennen jakolaskun tulos on lähimpänä lukua 1.

Tapa II: Otetaan yhtälön molemmilta puolilta vaikkapa 10-kantainen logaritmi, jolloin saadaan uusi yhtälö

$$\log_{10}(2^x) = \log_{10}(50).$$

Muokataan yhtälön vasenta puolta logaritmien laskusäännöillä (potenssin logaritmi), jolloin saadaan yhtälö

$$x \log_{10}(2) = \log_{10}(50).$$

Jaetaan tuntemattoman kertoimella:

$$x = \frac{\log_{10}(50)}{\log_{10}(2)}.$$

Lopuksi tarkistetaan, että löydetty luku on todella alkuperäisen yhtälön ratkaisu. Tämä voidaan tehdä esimerkiksi sijoittamalla saatu tulos alkuperäiseen yhtälöön, jolloin laskimella tms. saadaan

$$2^{\frac{\log_{10}(50)}{\log_{10}(2)}} = 50.$$

Siis yhtälöllä on tasan yksi ratkaisu, joka on

$$\frac{\log_{10}(50)}{\log_{10}(2)}.$$

Ratkaisun likiarvo saadaan tavallisella laskimella: $\frac{\log_{10}(50)}{\log_{10}(2)} \approx 5,6$.

Edellisestä esimerkistä 10.17 voi päätellä, että

$$\log_2(50) = \frac{\log_{10}(50)}{\log_{10}(2)}.$$

Yleisesti voidaan osoittaa, että jos $a, b \in \mathbb{R}_+ \setminus \{1\}$ ja $x \in \mathbb{R}_+$, niin

$$\log_a(x) = \frac{\log_b(x)}{\log_b(a)}.$$

Yksinkertaisia logaritmiyhtälöitä voi ratkaista käyttämällä logaritmin määritelmää.

Esimerkki 10.18. Päätellään mikä luku x on, jos tiedetään, että

$$(a) \log_2(x) = 1 \quad (b) \log_2(x) = 4 \quad (c) \log_2(x) = 6,5 \quad (d) \log_2(x) = -3.$$

Käytetään logaritmin määritelmää:

- a) Jos $\log_2(x) = 1$, niin $x = 2^1 = 2$.
 b) Jos $\log_2(x) = 4$, niin $x = 2^4 = 16$.
 c) Jos $\log_2(x) = 6,5$, niin

$$x = 2^{6,5} = 2^{6+0,5} = 2^6 \cdot 2^{0,5} = 2^6 \cdot \sqrt{2} = 64\sqrt{2}.$$

- d) Jos $\log_2(x) = -3$, niin

$$x = 2^{-3} = \frac{1}{2^3} = \frac{1}{8}.$$

Esimerkki 10.19. Ratkaistaan yhtälö $\log_2(x) + \log_2(x + 6) = \log_2(16)$.

Muokataan yhtälön vasenta puolta logaritmien laskusäännöillä (tulon logaritmi), jolloin saadaan uusi yhtälö

$$\log_2(x(x + 6)) = \log_2(16).$$

Logaritmifunktio on aidosti kasvava ja sen vuoksi saa jokaisen arvonsa vain kerran. Näin ollen edellisestä yhtälöstä seuraa, että $x(x + 6) = 16$ eli $x^2 + 6x = 16$ eli

$$x^2 + 6x - 16 = 0.$$

Toisen asteen yhtälön ratkaisukaavalla saadaan

$$x = \frac{-6 \pm \sqrt{6^2 - 4 \cdot 1 \cdot (-16)}}{2 \cdot 1} = \frac{-6 \pm 10}{2}$$

eli

$$x = 2 \vee x = -8.$$

Lopuksi tarkistetaan, että löydetty luvut todella ovat alkuperäisen yhtälön ratkaisuja:

Huomataan, että $\log_2(2) + \log_2(8) = 1 + 3 = 4 = \log_2(16)$, joten luku 2 on alkuperäisen yhtälön ratkaisu.

Havaitaan, että $\log_2(-8) + \log_2(-2)$ ei ole määritelty, sillä logaritmi on määritelty vain positiivisille luvuille. Siis luku -8 ei ole alkuperäisen yhtälön ratkaisu.

Aiempi päättely osoittaa, että mitään muita ratkaisuja ei ole olemassa. Yhtälöllä on siis tasan yksi ratkaisu: $x = 2$.

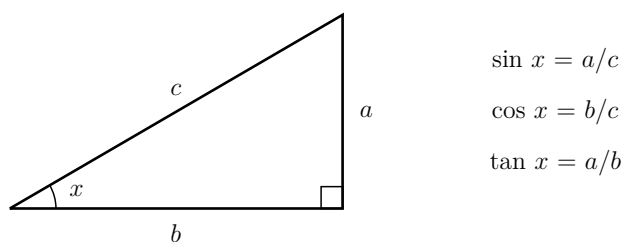
10.4 Trigonometriaa

Tämä luku on muokattu Jokke Häsän ja Jaakko Kortesharjun monisteesta ”Y100 kurssimateriaali”.

Tässä luvussa käsitellään koulusta tuttuja trigonometrisia funktioita. Jos haluat kerrata nämä käsitteet vielä tarkemmin, löydät aiheeseen liittyvää lukiomatematiikan materiaalia osoitteesta <https://kisallioppiminen.fi/kurssit/maa7/>.

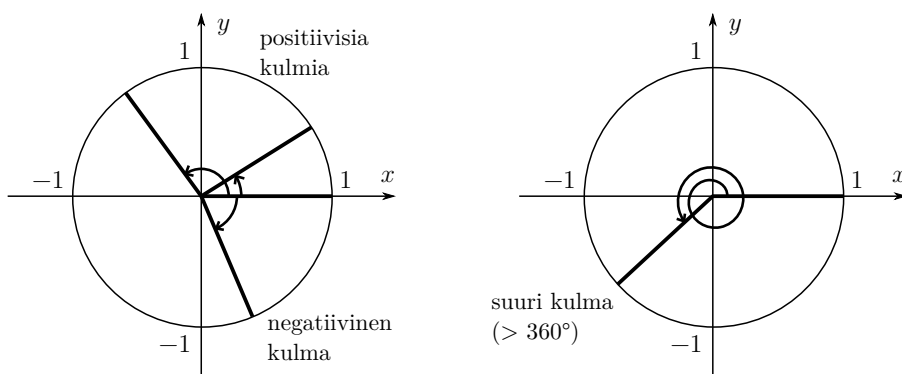
Trigonometrisia funktioita ovat koulusta tutut sini-, kosini- ja tangenttifunktiot. Sana ”trigonometria” tulee kreikan kielestä ja tarkoittaa kolmion mittaamista (’trigōnon’ = kolmio,

'metrein' = mitata). Trigonometriset funktiot ilmaisevat suorakulmaisen kolmion sivujen pituuksien suhteiden riippuvuutta annetusta kulmasta. Jos lähtöarvona on jokin kulman suuruus, esimerkiksi sinifunktion arvo tuolla lähtöarvolla saadaan seuraavasti: asetetaan kyseinen kulma toiseksi kulmaksi mihin tahansa suorakulmaiseen kolmioon ja luetaan tuon kulman vastaisen kateetin ja hypotenuusan pituuksien suhde. Tuo suhde on sinifunktion arvo eli annetun kulman sini. Trigonometrinen funktioiden perinteiset määritelmät näkyvät oheisesta kuvasta.

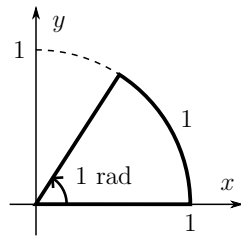


Suorakulmaisen kolmion avulla voidaan kuitenkin määrittää trigonometrinen funktioiden arvoja vain tietyillä kulman arvoilla, koska suorakulmaisessa kolmiossa kaikki muut kuin suora kulma ovat pienempiä kuin 90 astetta. Jos siis haluttaisiin määrittää sinin arvo vaikkapa lähtöarvolla 130, törmättäisiin vaikeuksiin. Asia korjaantuu määrittelemällä trigonometriset funktiot uudelleen ns. *yksikköympyrän* avulla.

Yksikköympyrä on koordinaatistoon piirretty ympyrä, jonka keskipiste on origossa ja säde on 1. Tähän ympyrään sijoitetaan kulmia siten, että niiden kärki on origossa ja toinen kylki x-akselin positiivisella osalla. Kulman suuruus tulkitaan positiiviseksi, jos se aukeaa x-akselilla olevasta kyljestä vastapäivään, ja negatiivinen, jos se aukeaa myötäpäivään. Yksikköympyrään voidaan piirtää myös täyskulmaa (360°) suurempi kulma kiertämällä ympyrä ympäri mahdollisesti useampaankin kertaan.



Matematiikassa kulman suuruus ilmoitetaan tavallisesti *radiaaneina*. Radiaani on sen kokoinen kulma, että yksikköympyrässä sitä vastaavan kaaren pituus on sama kuin kulma itse. Kulman koko on siis yksi radiaani, jos sitä vastaavan yksikköympyrän kaaren pituus on 1.

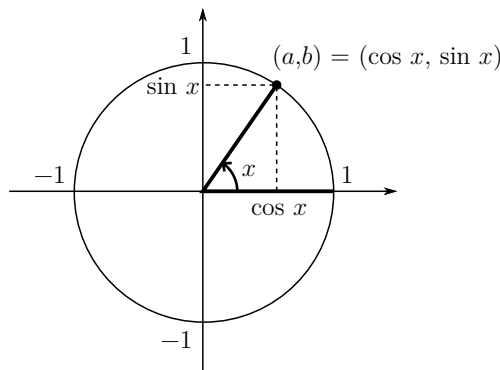


Radiaaneja käytettäessä yksikköä ei yleensä merkitä lainkaan näkyviin. Joskus saatetaan selvyuden vuoksi käyttää lyhennettä ”rad”. Koska yksikköympyrän kaaren puolikkaan pituus on π , puoliympyrää vastaavan kulman eli oikokulman suuruus on π radiaania. Toisaalta oikokulma on 180 astetta. Tästä saadaan radiaanien ja asteiden välille seuraava muunnoskaava:

$$\text{kulma radiaaneina} = \text{kulma asteina} \cdot \frac{\pi}{180}.$$

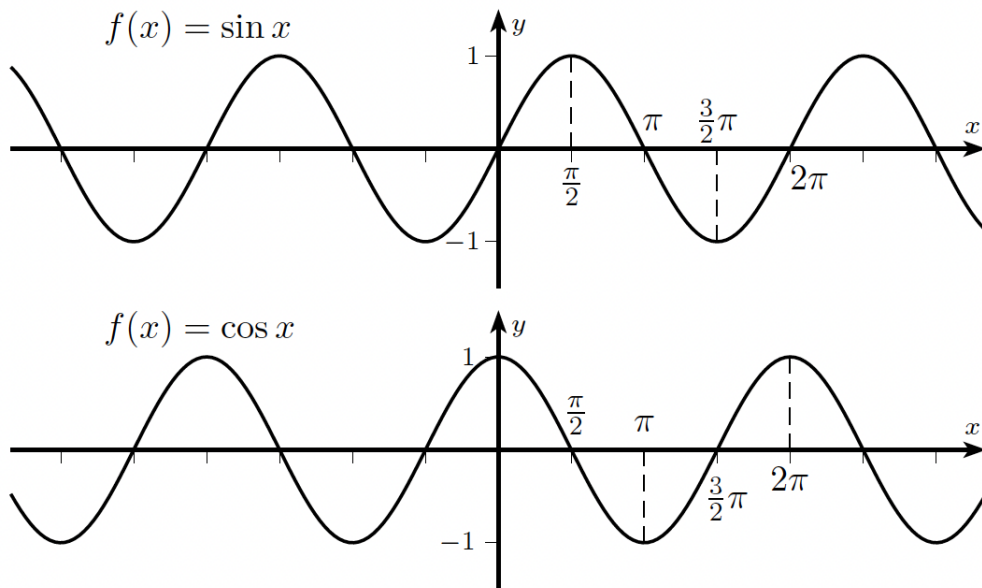
Sinifunktio ja kosinifunktio

Sini- ja kosinifunktiot voidaan määritellä yksikköympyrän avulla seuraavasti (ks. oheinen kuva). Olkoon x lähtöarvo. Piirretään yksikköympyrään kulma, jonka suuruus on x siten, että sen alkukylki tulee x-akselin positiiviselle osalle. Oletetaan, että loppukylki leikkaa yksikköympyrän pisteessä (a, b) . Tällöin sinifunktion arvo $\sin x$ on tuon leikkauspisteen y-koordinaatti eli a , ja kosinifunktion arvo $\cos x$ on saman leikkauspisteen x-koordinaatin arvo eli b .



Määritelmästä nähdään, että sini- ja kosinifunktion arvot sijoittuvat välille $[-1, 1]$, sillä yksikköympyrällä olevan pisteen x- ja y-koordinaatit eivät voi olla suurempia kuin 1 tai pienempiä kuin -1 . Kun negatiiviset kulmat ja yli täysympyrän menevät kulmat tulkitaan aiemmin selitetyllä tavalla, sini- ja kosinifunktiot voidaan määritellä kaikilla reaaliluvuilla. Niiden arvot tosin toistuvat aina täyskulman välein, kun yksikköympyrään piirretyn kulman loppukylki palaa taas x-akselille.

Sini- ja kosinifunktion arvoja laskettaessa käytetään yleensä kulmanyksikkönä radiaania. Funktioiden kuvaajat on piirretty seuraaviin kuviin. Kuvista huomataan, että sekä sini- että kosinifunktion kuvaajat toistavat itseään aina täyskulman eli 2π radiaanin välein. Tällaisia funktioita, joiden arvot toistuvat itseään, sanotaan *jaksollisiksi*. Sini- ja kosinifunktio ovat siis jaksollisia funktioita, joiden jakson pituus on 2π .



Sini- ja kosinifunktion kuvaajia vertailemalla huomataan, että niiden kuvaajat vastaavat toisiaan, kun toista siirretään hieman vaakasuunnassa. Tarkka määrä on itse asiassa $\pi/2$ (eli 90°). Kaavana voitaisiin ilmaista, että $\cos x = \sin(x + \pi/2)$.

Koska sini- ja kosinifunktio ovat jaksollisia, myös niiden nollakohdat toistuvat itseään säännöllisesti. Sinifunktio saa arvon nolla, kun kulman suuruus on nolla, ja nollakohdat toistuvat aina π radiaanin (eli 180°) välein. Nollakohdat voidaan siis ilmaista lyhyesti muodossa

$$x = n\pi, \quad \text{missä } n \text{ on kokonaisluku.}$$

Kosinin ensimmäinen nollakohta puolestaan on kohdassa $x = \pi/2$ (eli 90°), ja nollakohdat toistuvat π radiaanin välein. Täten nollakohdat voidaan ilmaista muodossa

$$x = \frac{\pi}{2} + n\pi, \quad \text{missä } n \text{ on kokonaisluku.}$$

Esimerkki 10.20. Etsitään väliltä $[0, 4]$ ne luvut x , jotka toteuttavat yhtälön

$$\sin\left(2x + \frac{\pi}{2}\right) = 0.$$

Tämä yhtälö toteutuu täsmälleen silloin, kun lauseke $2x + \pi/2$ on sinifunktion nollakohta. Eräs tällainen nollakohta on 0, ja muut saadaan tästä π :n välein. Voidaan siis päätellä, että yhtälö pätee, kun

$$2x + \frac{\pi}{2} = n\pi,$$

missä n voi olla mikä tahansa kokonaisluku. Tästä uudesta yhtälöstä voidaan helposti ratkaista

x :

$$\begin{aligned}2x + \frac{\pi}{2} &= n\pi \\ \Leftrightarrow 2x &= -\frac{\pi}{2} + n\pi \\ \Leftrightarrow x &= -\frac{\pi}{4} + \frac{n\pi}{2}.\end{aligned}$$

Saatu x on yhtälön ratkaisu aina, kun n on kokonaisluku. Sijoittamalla n :n paikalle eri kokonaislukuja saadaan muun muassa ratkaisut

$$\begin{aligned}-\frac{\pi}{4} + \frac{0}{2} &\approx -0,79, & -\frac{\pi}{4} + \frac{\pi}{2} &\approx 0,79, & -\frac{\pi}{4} + \frac{2\pi}{2} &\approx 2,36, \\ -\frac{\pi}{4} + \frac{3\pi}{2} &\approx 3,93 & \text{ja} & & -\frac{\pi}{4} + \frac{4\pi}{2} &\approx 5,50.\end{aligned}$$

Vain osa ratkaisuista osuu tutkittavalle välille $[0, 4]$. Nämä ratkaisut ovat (likiarvoina) 0,79, 2,36 ja 3,93.

Peruskaavoja

Sini- ja kosinifunktioiden jaksollisuudesta johtuen samat funktioiden arvot toistuvat tasavälein (2π :n välein) lukusuoraa pitkin liikuttaessa. Tämä voidaan ilmaista seuraavilla kaavoilla:

$$\begin{aligned}\sin x &= \sin(x + n \cdot 2\pi), \\ \cos x &= \cos(x + n \cdot 2\pi),\end{aligned}$$

kaikilla $x \in \mathbb{R}$ ja $n \in \mathbb{N}$. Yksikköympyrää tutkimalla voidaan lisäksi johtaa seuraavat säännöt sini- ja kosinifunktioiden arvoille:

$$\begin{aligned}\sin(-x) &= -\sin x, \\ \cos(-x) &= \cos x, \\ \sin x &= -\sin(x + \pi) = -\sin(x - \pi), \\ \cos x &= -\cos(x + \pi) = -\cos(x - \pi)\end{aligned}$$

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

Aiemmin mainittiin jo, että kosinifunktio saa samat arvot kuin sinifunktio sai aiemmissa (tai myöhemmissä) pisteissä):

$$\begin{aligned}\sin x &= \cos\left(x - \frac{\pi}{2}\right) = \cos\left(x + \frac{3\pi}{2}\right), \\ \cos x &= \sin\left(x + \frac{\pi}{2}\right) = \sin\left(x - \frac{3\pi}{2}\right).\end{aligned}$$

Lisäksi suorakulmaista kolmiota koskeva, geometriasta tuttu Pythagoraan lause on yhtäpitävä seuraavan ns. *trigonometrian peruskaavan* kanssa:

$$\sin^2 x + \cos^2 x = 1, \tag{1}$$

missä merkinnät $\sin^2 x$ ja $\cos^2 x$ tarkoittavat samaa kuin $(\sin x)^2$ ja $(\cos x)^2$. Ratkaisemalla tästä kaavasta $\sin x$ ja $\cos x$ saadaan sinin ja kosinin välille vielä seuraavat yhteydet:

$$\begin{aligned}\sin x &= \pm\sqrt{1 - \cos^2 x}, \\ \cos x &= \pm\sqrt{1 - \sin^2 x}.\end{aligned}$$

Näissä kaavoissa etumerkki täytyy valita sen mukaan, kumman etumerkin sini tai kosini saa annetulla kulman arvolla. Neliöjuurihan tuottaa kuitenkin aina positiivinen luvun.

Eriolaisten trigonometriaan liittyvien kaavojen johtamisessa ovat hyödyllisiä niin kutsutut summakaavat:

$$\begin{aligned}\sin(x + y) &= \sin x \cos y + \cos x \sin y \quad \text{ja} \\ \cos(x + y) &= \cos x \cos y - \sin x \sin y \quad \text{kaikilla } x, y \in \mathbb{R}.\end{aligned}$$

Summakaavojen todistusta ei esitetä tässä. Niiden perustelu löytyy esimerkiksi lisämateriaalina olevasta Antti Käenmäen monisteesta.

Tangenttifunktio

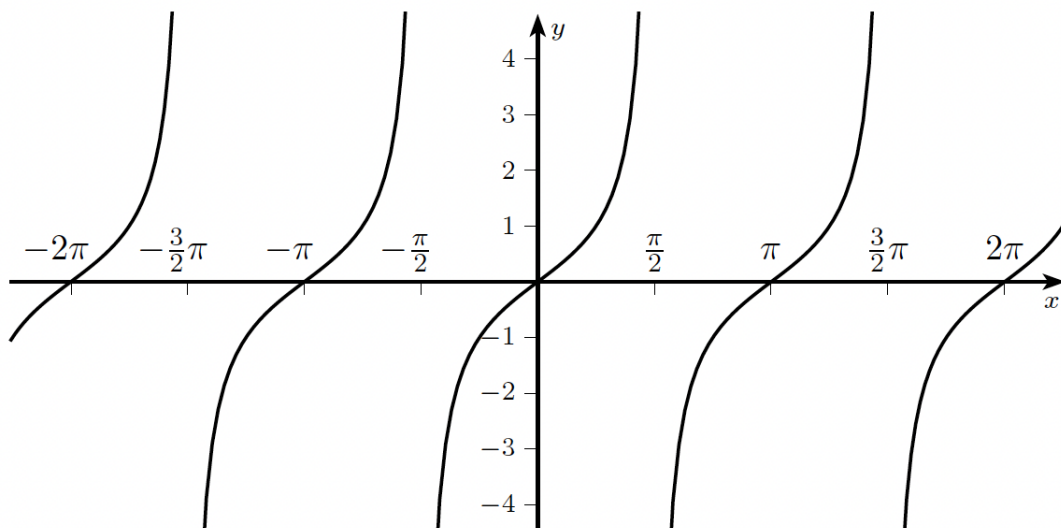
Tangenttifunktio on trigonometrinen funktio, jonka ominaisuudet poikkeavat melkoisesti sini- ja kosinifunktioiden ominaisuuksista. Tangenttifunktio määritellään sinin ja kosinin osamääränä:

$$\tan x = \frac{\sin x}{\cos x}.$$

Koska nolllalla ei voi jakaa, tangenttifunktio ei ole määritelty siellä, missä kosinifunktio saa arvon nolla. Toisin sanoen tangenttifunktion arvo $\tan x$ ei ole määritelty, kun

$$x = \frac{\pi}{2} + n\pi, \quad \text{missä } n \text{ on kokonaisluku.}$$

Tangenttifunktion kuvaaja on piirretty seuraavaan kuvaan.



Myös tangenttifunktio on jaksollinen, mutta tällä kertaa jaksona on π . Tangenttifunktion arvot toistuvat siis π :n välein. Tangenttifunktio saa arvon nolla silloin, kun osoittaja on nolla. Nollakohdat ovat siis samat kuin sinifunktiolla, eli ne ovat muotoa $n\pi$, missä n on mikä tahansa kokonaisluku.

11 Relaatiot

11.1 Mitä relaatiot ovat?

Matematiikassa olioiden välisiä suhteita kuvataan relaatioilla. Olio on relaatiossa toisen kanssa, jos ne toteuttavat tietyn suhdetta kuvaavan ehdon. Tuttu esimerkki relaatiosta on reaalilukujen järjestysrelaatio $<$. Esimerkiksi luku 1 on relaatiossa luvun $\sqrt{2}$ kanssa, sillä $1 < \sqrt{2}$. Luku 2 puolestaan ei ole kyseisessä relaatiossa luvun $\sqrt{2}$ kanssa.

Sanotaan, että R on joukon A relaatio, jos jokaiselle joukon A alkioparille (a, b) on määritetty, onko alkio a relaatiossa R alkion b kanssa vai ei. Jos a on relaatiossa R alkion b kanssa, merkitään aRb .

Esimerkki 11.1. Tarkastellaan joukon $A = \{1, 2, 3, 4, 5\}$ relaatiota R , joka määritellään ehdolla

$$aRb, \quad \text{jos } a + b < 6.$$

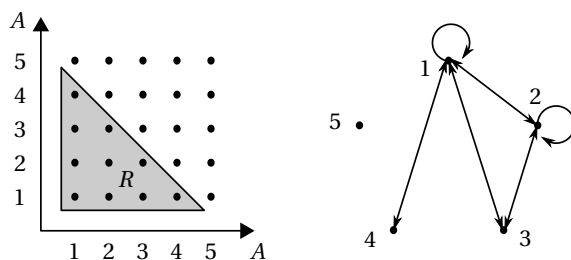
Esimerkiksi luku 2 on relaatiossa luvun 3 kanssa, koska $2 + 3 < 6$. Voidaan siis merkitä $2R3$. Toisaalta 2 ei ole relaatiossa luvun 4 kanssa.

Koska joukko A on kohtalaisen pieni, voidaan luetella kaikki parit, joiden jäsenet ovat relaatiossa toistensa kanssa. Relaation selvä symmetria helpottaa tätä tehtävää entisestään. Relaatiossa olevat parit ovat

$$(1, 1), (1, 2), (2, 1), (1, 3), (3, 1), (1, 4), (4, 1), (2, 2), (2, 3), (3, 2).$$

Nämä parit muodostavat karteesisen tulon $A \times A$ osajoukon.

Kuvassa 11.42 relaatiota vastaava osajoukko on merkitty koordinaatistoon. Samassa kuvassa on relaatiosta piirretty myös nuolidiagrammi. Nuoli kulkee luvusta a lukuun b täsmälleen silloin, kun a on relaatiossa b :n kanssa.



Kuva 11.42: Kaksi graafista esitystä relaatiosta R .

11.2 Relaation täsmällinen määritelmä

Tässä luvussa annetaan täsmällinen määritelmä relaatiolle. Tarkalleen ottaen joukon A relaatio on karteesisen tulon $A \times A$ osajoukko. Jos R on relaatio, ehto aRb merkitsee sitä, että $(a, b) \in R$. Relaatio voidaan määritellä myös kahden eri joukon alkioiden välille.

Määritelmä 11.2. 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 .

Usein relaatiota merkitään kirjaimen R sijasta jollakin symbolilla, esimerkiksi $<$, \subset tai \sim .

Esimerkki 11.3. 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 $S \subset X \times X$.

11.3 Ekvivalenssirelaatio

Relaatioiden erikoistapaus on ekvivalenssirelaatio, jota voidaan käyttää olioiden luokitteluun.

Tarkastellaan esimerkkinä luokittelusta Suomen asukkaiden muodostamaa joukkoa. Suomessa on noin 5 miljoonaa asukasta, mutta heidät voidaan jakaa karkeasti ryhmiin maakuntien mukaan. Jokainen ihminen on erilainen yksilö, mutta esimerkiksi hänen puhetavastaan, luonteenpiirteistään ja ruokatottumuksistaan voidaan sanoa paljon asuinmaakunnan perusteella. (Tässä oletetaan, että maakuntien rajat ovat selvät.) Matemaattisesti voidaan sanoa, että samassa maakunnassa asuvat ihmiset ovat keskenään ekvivalentteja.

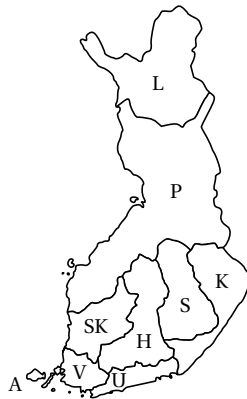
Ekvivalenssin käsitteellä on muutamia sitä luonnehtivia ominaisuuksia. Maakuntaesimerkin tapauksessa ne voidaan ilmaista seuraavasti.

- 1) Jokainen ihminen asuu samassa maakunnassa itsensä kanssa. Jokainen on siis itsensä kanssa ekvivalentti.
- 2) Jos Niina asuu Pekan kanssa samassa maakunnassa, niin Pekka asuu Niinan kanssa samassa maakunnassa. Ekvivalenttius on siis symmetristä.
- 3) Jos Niina asuu Pekan kanssa samassa maakunnassa ja Pekka asuu Tainan kanssa samassa maakunnassa, myös Niina asuu Tainan kanssa samassa maakunnassa.

Osoittautuu, että edellä mainitut ominaisuudet riittävät määrittelemään ekvivalenssin käsitteen.

Määritelmä 11.4. Olkoon R joukon A relaatio. Kyseessä on *ekvivalenssirelaatio*, jos R toteuttaa seuraavat ehdot kaikilla $a, b, c \in A$:

- 1) aRa (refleksiivisyys).
- 2) Jos aRb , niin bRa (symmetrisyys).
- 3) Jos aRb ja bRc , niin aRc (transitiivisyys).



Kuva 11.43: Maakuntien muodostama ositus Suomen asukkaiden joukossa.

Esimerkki 11.5. Tutkitaan reaalilukujen joukon järjestysrelaatiota $<$. Relaatio ei ole refleksiivinen, sillä luku ei voi olla itseään suurempi. Relaatio ei myöskään ole symmetrinen, sillä esimerkiksi $2 < 3$, mutta $3 < 2$ ei päde. Relaatio on transitiiivinen: jos $a < b$ ja $b < c$, niin $a < c$.

Esimerkki 11.6. Suomen asukkaiden joukossa voidaan määritellä ekvivalenssirelaatio M seuraavan ehdon avulla:

$$aMb, \quad \text{jos } a \text{ asuu samassa maakunnassa kuin } b.$$

Esimerkki 11.7. Olkoon L kaikkien tason suorien joukko. Määritellään relaatio \parallel seuraavasti:

$$l_1 \parallel l_2, \quad \text{jos suorat } l_1 \text{ ja } l_2 \text{ ovat yhdensuuntaisia.}$$

Jokainen suora on yhdensuuntainen itsensä kanssa, joten relaatio on refleksiivinen. Relaatio on myös symmetrinen: jos suora l_1 on yhdensuuntainen suoran l_2 kanssa, myös suora l_2 on yhdensuuntainen suoran l_1 kanssa. Lisäksi relaatio on transitiiivinen: jos suorat l_1 ja l_2 ovat yhdensuuntaiset ja suorat l_2 ja l_3 ovat yhdensuuntaiset, myös l_1 ja l_3 ovat yhdensuuntaiset. Siten relaatio on myös transitiiivinen. Kyseessä on siis ekvivalenssirelaatio.

Esimerkki 11.8. Tarkastellaan jälleen joukon $A = \{1, 2, 3, 4, 5\}$ relaatiota R , joka määritellään ehdolla

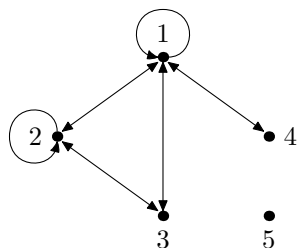
$$aRb, \quad \text{jos } a + b < 6.$$

Tutkitaan, kuinka relaation refleksiivisyys, symmetrisyys ja transitiiivisuus näkyvät nuolikaaviossa.

Kuvan 11.44 nuolikaaviosta nähdään, että esimerkiksi alkioon 4 ei mene nuolta alkioista itsestään. Siten 4 ei ole relaatiossa itsensä kanssa. Näin ollen relaatio R ei ole refleksiivinen.

Nuolikaaviossa kaikki nuolet eri pisteiden välillä menevät molempiin suuntiin. Tämä tarkoittaa sitä, että relaatio on symmetrinen.

Relaatio R ei ole transitiiivinen. Kaaviosta nähdään, että alkioista 3 menee nuoli alkioon 1 ja alkioista 1 nuoli edelleen alkioon 4. Siis $3R1$ ja $1R4$. Alkioista 3 ei kuitenkaan mene nuolta alkioon 4. Siten ei päde $3R4$.



Kuva 11.44: Relaatio R on symmetrinen, mutta ei refleksiivinen eikä transitiivinen.

Esimerkki 11.9. Määritellään kokonaisluvuille relaatio \sim seuraavasti:

$$a \sim b, \quad \text{jos } a - b \text{ on jaollinen luvulla } 5.$$

Osoitetaan, että kyseessä on ekvivalenssirelaatio. Olkoot $a, b, c \in \mathbb{Z}$.

- 1) Luku 5 jakaa erotuksen $a - a$, sillä $a - a = 5 \cdot 0$. Siten $a \sim a$, ja relaatio on refleksiivinen.
- 2) Oletetaan, että $a \sim b$. Nyt $5|(a - b)$, joten $a - b = 5k$ jollakin $k \in \mathbb{Z}$. Tästä seuraa, että $b - a = 5(-k)$. Siten $5|(b - a)$, mikä tarkoittaa sitä, että $b \sim a$. Relaatio on siis symmetrinen.
- 3) Oletetaan, että $a \sim b$ ja $b \sim c$. Nyt $5|(a - b)$ ja $5|(b - c)$. Tästä seuraa, että $a - b = 5k$ ja $b - c = 5l$ joillakin $k, l \in \mathbb{Z}$. Nähdään, että

$$a - c = (a - b) + (b - c) = 5k + 5l = 5(k + l),$$

joten $5|(a - c)$. Siten $a \sim c$, ja relaatio on transitiivinen.

Kyseistä relaatiota kutsutaan kongruenssiksi modulo 5. Jos alkiot a ja b ovat relaatiossa keskenään, merkitään $a \equiv b \pmod{5}$.

11.4 Ekvivalenssiluokat

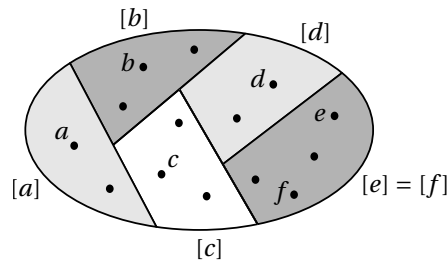
Niiden alkioiden joukkoa, jotka ovat ekvivalenssirelaatiossa jonkin alkion kanssa, kutsutaan tämän alkion ekvivalenssiluokaksi. Maakuntaesimerkissä samassa maakunnassa asuvat ihmiset muodostavat yhden ekvivalenssiluokan. Kuka tahansa asukas voidaan valita maakuntansa edustajaksi.

Määritelmä 11.10. Oletetaan, että \sim on joukon A ekvivalenssirelaatio. Alkion $a \in A$ ekvivalenssiluokka on

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

Jos asiayhteydestä on selvää, mikä ekvivalenssirelaatio on kyseessä, voidaan alaindeksi jättää merkitsemättä ja kirjoittaa $[a]_{\sim} = [a]$.

Koska jokainen alkio on itsensä kanssa ekvivalentti, kaikilla $a \in A$ pätee $a \in [a]_{\sim}$. Alkiota a kutsutaan ekvivalenssiluokansa $[a]_{\sim}$ edustajaksi. Kuvassa 11.45 on hahmoteltu ekvivalenssiluokkien ja niiden edustajien suhdetta. Relaation A kaikkien ekvivalenssiluokkien joukkoa merkitään A/\sim .



Kuva 11.45: Ekvivalenssiluokkia ja niiden edustajia.

Esimerkki 11.11. Esimerkin 11.7 suorien ekvivalenssirelaatiossa suoran l ekvivalenssiluokassa ovat kaikki suorat, jotka ovat yhdensuuntaisia suoran l kanssa. Kussakin ekvivalenssiluokassa ovat siis kaikki keskenään yhdensuuntaiset suorat. Jokaisen ekvivalenssiluokan edustajaksi voidaan valita sen sisältämistä suorista vaikkapa se, joka kulkee origon kautta.

Esimerkki 11.12. Olkoon S kaikkien suomen kielen sanojen muodostama joukko. Määritellään joukon S relaatio \sim ehdolla

$$a \sim b, \text{ jos sana } a \text{ alkaa samalla kirjaimella kuin sana } b.$$

Voidaan osoittaa, että kyseessä on ekvivalenssirelaatio. Tutkitaan, millaisia ovat tämän ekvivalenssirelaation ekvivalenssiluokat.

Määritelmän mukaan

$$[AAMU]_{\sim} = \{s \in S \mid s \sim AAMU\} = \{s \in S \mid \text{sana } s \text{ alkaa kirjaimella } a\}$$

Havaitaan, että sanan AAMU ekvivalenssiluokan muodostavat kaikki a-kirjaimella alkavat sanat. Vastaavalla tavalla päättelämällä huomataan, että relaation \sim ekvivalenssiluokat ovat

$$[AAMU], [BANAANI], [CELCIUS], [DEMOKRATIA], \dots, [\text{ÖLJY}].$$

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

$$S/\sim = \{[AAMU], [BANAANI], [CELCIUS], [DEMOKRATIA], \dots, [\text{ÖLJY}]\}$$

Esimerkki 11.13. Esimerkissä 11.9 määriteltiin joukon \mathbb{Z} relaatio \sim ehdolla

$$a \sim b, \text{ jos erotus } a - b \text{ on jaollinen luvulla } 5,$$

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: $0, \pm 5, \pm 10, \pm 15, \pm 20, \pm 25, \pm 30, \dots$

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 $1, 6, 11, 16, \dots$ ja luvut $-4, -9, -14, -19, \dots$

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 siihen, 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 11.14. Jatketaan esimerkin 11.13 ekvivalenssirelaation \sim tarkastelua. Esimerkissä 11.13 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 transitiiivinen. Transitiiivisuuden 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 transitiiivisuuden nojalla tällöin myös $x \sim 8$. Siis $x \in [8]_{\sim}$.

11.5 Kuvaus relaationa

Kuvaukset voidaan määritellä tietyntyyppisiksi relaatioiksi. Oletetaan, että tarkoituksena on määritellä kuvaus $F: A \rightarrow B$. Ideana on asettaa alkio a relaatioon alkion b kanssa silloin, kun b on a :n kuva eli $F(a) = b$. Koska a on lähtöjoukon A alkio ja b puolestaan kuuluu maalijoukkoon B , täytyy relaatio määritellä joukossa, joka sisältää sekä lähtö- että maalijoukon. Tähän voidaan soveltaa joukkojen yhdistettä.

Sanotaan, että joukon $A \cup B$ relaatio F on kuvaus $A \rightarrow B$, jos seuraavat ehdot pätevät:

- 1) Jokaisella parilla $(a, b) \in F$ pätee $a \in A$ ja $b \in B$.
- 2) Jokaista $a \in A$ kohti on olemassa täsmälleen yksi $(a, b) \in F$.

Tällaista määritelmää käytettäessä lause ” b on a :n kuva kuvauksessa F ” voidaan merkitä ainakin seuraavilla tavoilla: $F(a) = b$, $a \xrightarrow{F} b$, $(a, b) \in F$ ja aFb .

Luku IV

Kompleksiluvut

12 Kompleksiluvut

Tämä luku on muokattu Lotta Oinosen materiaalista ”Johdatus yliopistomatematiikkaan”.

Luvun tarkoituksena on antaa perustaidot kompleksiluvuilla laskemiseen sekä niiden geometriseen tulkintaan.

12.1 Kompleksilukujen esittely

Koko opintiesi ajan käsityksesi luvuista on muuttunut ja olet tutustunut aina vain laajempiin lukujoukkoihin. Kun alakoulussa harjoiteltiin vähennyslaskua, opittiin aluksi, että pienemmästä luvusta ei voi vähentää isompaa. Hiukan myöhemmin käyttöön otettiin negatiiviset luvut. Nyt vähentäminen onnistui! Sitten harjoiteltiin jakolaskua. Jos jako ei mennyt tasan, ei sitä voinut tehdä. Esimerkiksi luku 3 ei voinut jakaa viidellä. Kun käyttöön saatiin murtoluvut, ei jaon enää tarvinnutkaan mennä tasan. Reaaliluvut laajensivat lukujoukkoa entisestään ja esimerkiksi kaikista positiivisista luvuista oli mahdollista ottaa neliöjuuri.

Nyt astumme seuraavan askeleen lukujoukkojen laajentamisessa. Reaaliluvun toinen potenssi ei koskaan voi olla negatiivinen. Ei esimerkiksi ole olemassa sellaista reaalilukua x , jolla $x^2 = -1$. Lähdemme tutustumaan niin kutsuttuihin *kompleksiluvuihin*, jolla tämä on mahdollista.

Kompleksiluvut ovat muotoa $a + bi$, missä a ja b ovat reaalilukuja. Symbolia i kutsutaan *imaginääriyksiköksi*. Kompleksilukujen joukko voidaan siis kirjoittaa muodossa

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}.$$

Kompleksilukujen summa ja tulo lasketaan kuten koulussa on opittu sieventämään reaalilukulausekkeitä. Lisäksi imaginääriyksikölle pätee $i^2 = -1$, ja tämä on huomioitava laskuissa.

Esimerkki 12.1. 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:

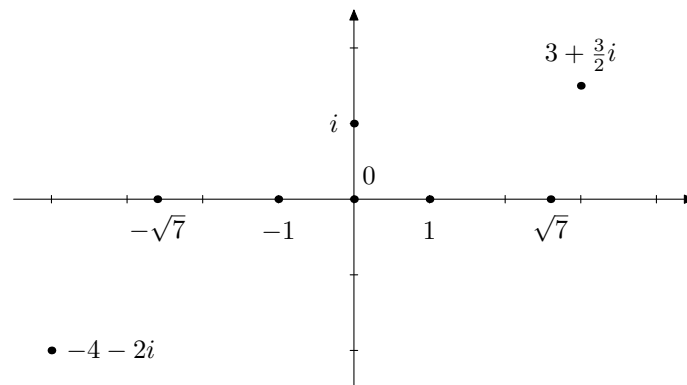
$$\begin{aligned} zw &= (-4 - 2i)(3 + 5i) = -4 \cdot 3 - 4 \cdot 5i - 2i \cdot 3 - 2i \cdot 5i = -12 - 20i - 6i - 10i^2 \\ &= -12 - 26i - 10 \cdot (-1) = -12 - 26i + 10 = -2 - 26i. \end{aligned}$$

Kuten alussa todettiin kompleksiluvun toinen potenssi voi olla negatiivinen reaaliluku. Esimerkiksi $i^2 = -1$ ja $(3i)^2 = 3i \cdot 3i = 9i^2 = 9(-1) = -9$.

Kompleksiluvussa $a + bi$ lukua a kutsutaan *reaaliosaksi* ja lukua b *imaginääriosaksi*. Esimerkiksi kompleksiluvun $\sqrt{5} - 4i$ reaaliosa on $\sqrt{5}$ ja imaginääriosa -4 .

Reaaliluku on *puhtaasti imaginäärinen*, jos sen imaginääriosa on 0. Esimerkiksi $17i$ on puhtaasti imaginäärinen. Toisaalta jos kompleksiluvun imaginääriosa on 0, kyseessä on reaaliluku. Myös reaaliluvut ovat siis kompleksilukuja.

Kompleksilukuja voi havainnollistaa pisteinä koordinaatistossa eli niin kutsutussa *kompleksitasossa*. Kompleksiluvussa $a + bi$ reaaliosa a vastaa vaaka-akselin koordinaattia ja imaginääriosa b pystyakselin koordinaattia. Kuvassa 12.1 on esitetty joitakin kompleksilukuja kompleksitasossa. Reaaliluvut sijaitsevat kompleksitason vaaka-akselilla, sillä niiden imaginääriosa on 0.



Kuva 12.1: Kompleksilukuja kompleksitasossa.

12.2 Kompleksilukujen määritelmä

Edellä kuvattiin, millaisia kompleksiluvut ovat ja miten niillä lasketaan. Jos ollaan tarkkoja, kompleksilukuja tai niiden laskutoimituksia ei ole vielä määriteltä täsmällisesti, vaan ainoastaan kuvailtu, millaisia ne ovat. Erityisesti tässä vaiheessa on epäselvää mikä symboli i oikein on.

Seuraavaksi annetaan kompleksilukujen muodollinen määritelmä. Määritelmän avulla voidaan käsitellä kompleksilukuja täsmällisesti ja vakuuttua siitä, että ne ovat olemassa. Käytännön laskuissa määritelmää ei kuitenkaan tällä kurssilla käytetä.

Määritelmä 12.2. Kompleksilukujen joukko \mathbb{C} on joukko

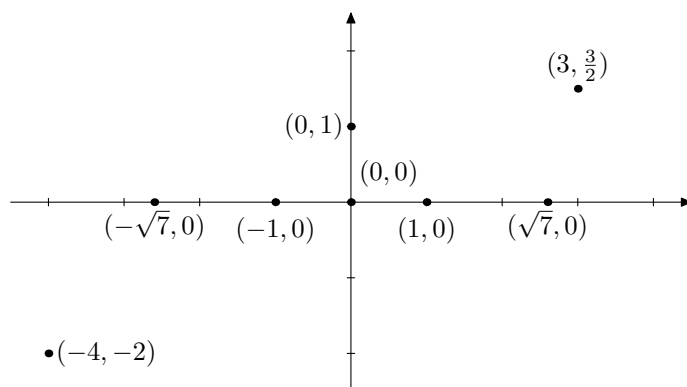
$$\{(a, b) \mid a, b \in \mathbb{R}\}$$

varustettuna yhteenlaskulla ja kertolaskulla, jotka määritellään seuraavasti:

$$(a, b) + (c, d) = (a + c, b + d) \quad \text{ja} \quad (a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

Määritelmän mukainen merkintä (a, b) vastaa aiemmin esiteltyä ilmaisua $a + bi$. Määritelmän hyvä puoli on se, että ei ole epäselvyyttä kompleksilukujen olemassaolosta tai siitä, mitä symboli i tarkoittaa. Määritelmän huono puoli on kuitenkin se, että kompleksilukujen tulon laskeminen on melko vaivalloista. Siksi tällä kurssilla käytetäänkin kompleksiluvuista käytännön laskuissa muotoa $a + bi$.

Kompleksiluvut ovat määritelmän mukaan reaalilukupareja. Nyt on luonnollista esittää kompleksiluvut kompleksitasossa kuten aiemminkin tehtiin. Kuvassa 12.2 on esitetty samat kompleksiluvut kuin aiemmin kuvassa 12.1.



Kuva 12.2: Kompleksilukuja kompleksitasossa.

Reaaliluvut ajatellaan kompleksilukujen osajoukoksi samastamalla reaaliluku a ja kompleksiluku $(a, 0)$ eli tulkitsemalla kompleksitason vaaka-akseli reaalilukusuorana. 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 12.3. 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 12.4. 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 $z_2 + w_2 = w_2 + z_2$.

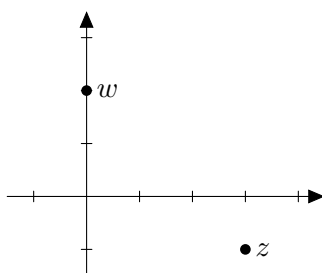
Aiemmin esiteltiin reaali-osa, imaginääriosa sekä puhtaasti imaginääriset luvut. Annetaan näille käsitteille täsmälliset määritelmät reaalilukuparimerkinnän avulla.

Määritelmä 12.5. Oletetaan, että $a, b \in \mathbb{R}$. Kompleksiluvun $z = (a, b)$ *reaali-osa* on $\operatorname{Re} z = a$ ja *imaginääriosa* on $\operatorname{Im} z = b$.

Määritelmä 12.6. Oletetaan, että $z \in \mathbb{C}$ ja $z \neq 0$. Jos $\operatorname{Re} z = 0$, sanotaan kompleksiluvun z olevan *puhtaasti imaginäärinen*.

Puhtaasti imaginääriset kompleksiluvut sijaitsevat kompleksitason pystyakselilla.

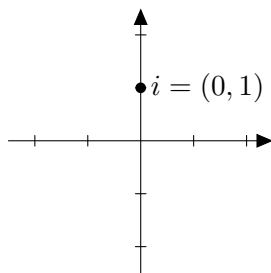
Esimerkki 12.7. Kompleksiluvun $z = (3, -1)$ reaali-osa on $\operatorname{Re} z = 3$ ja imaginääriosa on $\operatorname{Im} z = -1$. Kompleksiluvun $w = (0, 2)$ reaali-osa on $\operatorname{Re} w = 0$ ja imaginääriosa on $\operatorname{Im} w = 2$. Se on puhtaasti imaginäärinen.



Kuva 12.3: Kompleksiluku w on puhtaasti imaginäärinen, kompleksiluku z puolestaan ei ole.

Nyt voidaan määritellä täsmällisesti myös imaginääriyksikkö i ja osoittaa, että $i^2 = -1$.

Määritelmä 12.8. Kompleksilukua $(0, 1)$ kutsutaan *imaginääriyksiköksi* ja merkitään symbolilla i .



Kuva 12.4: Imaginaariyksikkö $i = (0, 1)$.

Lause 12.9. *Imaginaariyksikölle i pätee $i^2 = -1$.*

Todistus. Imaginaariyksikön määritelmän mukaan $i = (0, 1)$. Soveltamalla kompleksilukujen kertolaskua saadaan

$$i^2 = (0, 1) \cdot (0, 1) = (0 - 1, 0 + 0) = (-1, 0) = -1. \quad \square$$

Osoitetaan lopuksi, että määrittelemällä $i = (0, 1)$, voidaan kompleksiluku (a, b) kirjoittaa muodossa $a + bi$:

$$(a, b) \stackrel{(1)}{=} (a, 0) + (0, b) \stackrel{(2)}{=} (a, 0) + (b, 0) \cdot (0, 1) \stackrel{(3)}{=} (a, 0) + (b, 0) \cdot i \stackrel{(4)}{=} a + bi.$$

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 $(b, 0)$ reaalityyppisiin a ja b .

Huomaa, että 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.

12.3 Mihin kompleksilukuja tarvitaan?

Kompleksiluvut voivat tuntua kummallisilta ja tarpeettomiltakin. Mihin niitä oikein tarvitaan? Matematiikassa asiat voivat kuitenkin olla mielenkiintoisia jo ihan vain sen vuoksi, että ne ovat olemassa. On jännittävää, että on olemassa reaalityyppisten laajennos jossa neliö voi olla negatiivinen. Itse asiassa voidaan osoittaa, että kompleksilukujen joukossa mille tahansa polynomiyhtälölle löytyy ratkaisuja.

Kompleksiluvut vakiintuivat itse asiassa käyttöön jo ennen kuin negatiiviset luvut. Aikoinaan yhtälöissä ei niissä esiintynyt lainkaan negatiivisia lukuja. Mitä mika tarkoittaisi vaikkapa miinus kolme tomaattia? Samaan aikaan yhtälönratkaisussa kuitenkin hyödynnettiin kompleksilukuja. 1500-luvun Italiassa matemaatikot nimittäin huomasivat, että jos kolmannen asteen yhtälön ratkaisun välivaiheessa sallii negatiivisen luvun neliöjuuren, yhtälölle voi löytää ratkaisun. Tuon ajan matemaatikoiden mielestä negatiiviset luvut olivat siis luonnottomampia kuin kompleksiluvut!

Nykyään kompleksiluvuilla on useita sovelluskohteita. Niitä hyödynnetään esimerkiksi vaihtosähköpiirien yhteydessä ja signaalinkäsittelyssä.

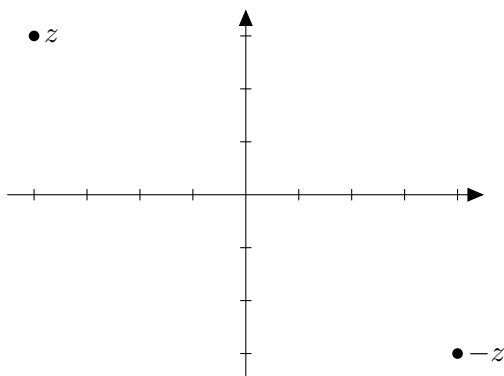
12.4 Kompleksiluvuilla laskeminen

Kuten reaalityyppisillä, myös jokaisella kompleksiluvulla on vastaluku. Kompleksilukujen erotus voidaan määrittellä yhteenlaskun ja vastaluvun avulla:

Määritelmä 12.10. 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 12.11. Merkitään $z = -4 + 3i$ ja $w = -2 - i$. Määritetään luvun z vastaluku vaihtamalla sekä reaali- 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 12.5: Kompleksiluku z ja sen vastaluku $-z$.

12.5 Kompleksiluvun liittoluku ja itseisarvo

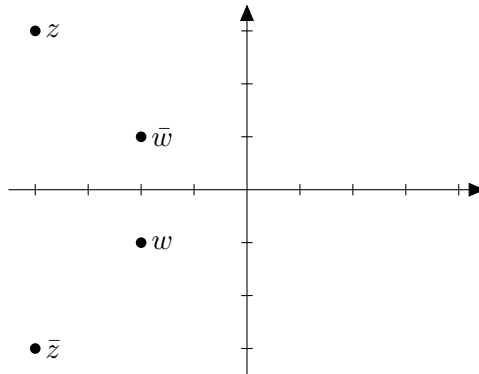
Jokaiselle kompleksiluvulle voidaan määrittellä niin sanottu liittoluku, joka saadaan vaihtamalla alkuperäisen luvun imaginaariosan merkki:

Määritelmä 12.12. 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 vaak-akselin suhteen. Luvun z liittoluvulle käytetään joissakin kirjoissa merkintää z^* .

Esimerkki 12.13. Kompleksilukujen $z = -4 + 3i$ liittoluku on $\bar{z} = -4 - 3i$. Kompleksiluvun $w = -2 - i$ liittoluku on $\bar{w} = -2 + i$. Näitä on havainnollistettu kuvassa 12.6.



Kuva 12.6: Kompleksiluvut z ja w sekä niiden liittoluvut \bar{z} ja \bar{w} .

Lause 12.14. Oletetaan, että $z, w \in \mathbb{C}$. Tällöin

- a) $\overline{z + w} = \bar{z} + \bar{w}$
- b) $\overline{z\bar{w}} = \bar{z}w$
- c) $\overline{\bar{z}} = z$
- d) jos $\text{Im}z = 0$, niin $\bar{z} = z$.

Todistus. Todistetaan malliksi a-kohta ja jätetään loput harjoitustehtäviksi.

Oletetaan, että $z, w \in \mathbb{C}$. 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 $\overline{z + w} = \bar{z} + \bar{w}$. □

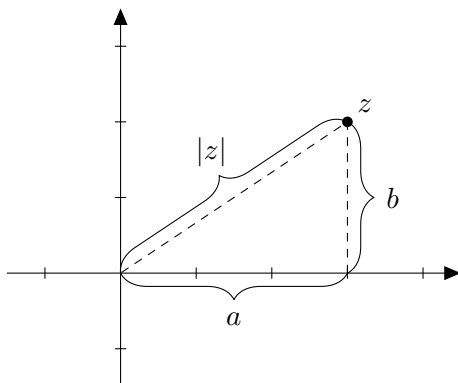
Reaaliluvun a itseisarvo $|a|$ kertoo luvun a etäisyyden nolasta. Esimerkiksi luvun -4 itseisarvo on $|-4| = 4$. Vastaava itseisarvon käsite voidaan määritellä myös kompleksiluvuille:

Määritelmä 12.15. 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 12.7: Kompleksiluvun itseisarvo kertoo luvun etäisyyden origosta.

Pythagoraan lauseen mukaan kuvassa 12.7 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 12.16. 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 reaalitylukujen itseisarvon tutut ominaisuudet. Seuraavassa lauseessa todistetaan näistä ominaisuuksista yksi.

Lause 12.17. 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 yhtälökettuna:

$$|zw| \stackrel{(1)}{=} \sqrt{(zw)(\overline{zw})} \stackrel{(2)}{=} \sqrt{(zw)(\bar{z}\bar{w})} \stackrel{(3)}{=} \sqrt{(z\bar{z})(w\bar{w})} \stackrel{(4)}{=} \sqrt{z\bar{z}}\sqrt{w\bar{w}} \stackrel{(5)}{=} |z| \cdot |w|.$$

Kohdassa (1) sovelletaan lausetta 12.16, jonka mukaan kompleksiluvun zw itseisarvolle pätee

$$|zw| = \sqrt{(zw)(\overline{zw})}.$$

Kohdassa (2) käytetään lausetta 12.14, 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 12.16 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 12.16, jonka mukaan $\sqrt{z\bar{z}} = |z|$ ja $\sqrt{w\bar{w}} = |w|$. \square

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 12.18. *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 12.16 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 $w = 0$. \square

12.6 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 12.19. Kompleksiluvun $z \neq 0$ käänteisluku on

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

Kompleksiluvun z käänteislukua voidaan merkitä myös $1/z$ tai $\frac{1}{z}$.

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 12.20. *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

$$z \cdot z^{-1} \stackrel{(1)}{=} z \cdot \left(\frac{1}{|z|^2} \bar{z} \right) = \frac{z\bar{z}}{|z|^2} \stackrel{(2)}{=} \frac{z\bar{z}}{z\bar{z}} = 1.$$

Kohdassa (1) käytetään käänteisluvun määritelmää. Kohdassa (2) sovelletaan lausetta 12.16, jonka mukaan $|z| = \sqrt{z\bar{z}}$. Siitä voidaan päätellä, että $|z|^2 = z\bar{z}$. \square

Käänteisluvun ja kertolaskun avulla saadaan määriteltyä kompleksilukujen osamäärä:

Määritelmä 12.21. 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 laentamalla nimittäjän liittoluvulla. Laventaminen tarkoittaa, että sekä osoittaja että nimittäjä kerrotaan samalla luvulla (tässä tapauksessa nimittäjän liittoluvulla). Tätä havainnollistetaan seuraavissa esimerkeissä.

Esimerkki 12.22. Merkitään $z = -4 + 7i$ ja $w = -2 - i$. Määritetään luvun z käänteisluku sekä lukujen z ja w osamäärä.

Luvun z käänteisluku sievennetään laentamalla nimittäjän liittoluvulla kohdassa (*):

$$\begin{aligned} z^{-1} &= \frac{1}{z} = \frac{1}{-4 + 7i} \stackrel{(*)}{=} \frac{-4 - 7i}{(-4 - 7i)(-4 + 7i)} = \frac{-4 - 7i}{(-4)^2 - (7i)^2} = \frac{-4 - 7i}{16 - 49i^2} = \frac{-4 - 7i}{16 + 49} \\ &= \frac{-4 - 7i}{65} = -\frac{4}{65} - \frac{7}{65}i. \end{aligned}$$

Lukujen z ja w osamääräkin sievennetään laentamalla nimittäjän liittoluvulla kohdassa (*):

$$\begin{aligned} \frac{z}{w} &= \frac{-4 + 7i}{-2 - i} \stackrel{(*)}{=} \frac{(-2 + i)(-4 + 7i)}{(-2 + i)(-2 - i)} = \frac{8 - 14i - 4i + 7i^2}{(-2)^2 - i^2} = \frac{8 - 18i + 7 \cdot (-1)}{4 - (-1)} \\ &= \frac{8 - 18i - 7}{5} = \frac{1 - 18i}{5} = \frac{1}{5} - \frac{18}{5}i. \end{aligned}$$

Esimerkki 12.23. Määritetään kompleksiluvun $z = \frac{10}{-4 + 2i}$ reaaliosa ja imaginaariosa.

Lavennetaan nimittäjän liittoluvulla kohdassa (*):

$$\begin{aligned} z &= \frac{10}{-4 + 2i} \stackrel{(*)}{=} \frac{10 \cdot (-4 - 2i)}{(-4 + 2i)(-4 - 2i)} = \frac{-40 - 20i}{(-4)^2 - (2i)^2} = \frac{-40 - 20i}{16 - 4i^2} \\ &= \frac{-40 - 20i}{16 + 4} = \frac{-40 - 20i}{20} = -2 - i. \end{aligned}$$

Siis $\operatorname{Re} z = -2$ ja $\operatorname{Im} z = -1$.

Esimerkki 12.24. Määritetään kompleksiluvun $z = \frac{2i}{1 - 3i} + \frac{1}{i}$ reaaliosa ja imaginaariosa.

Lavennetaan nimittäjien liittoluvuilla kohdassa (*):

$$\begin{aligned} z &= \frac{2i}{1 - 3i} + \frac{1}{i} \stackrel{(*)}{=} \frac{2i(1 + 3i)}{(1 - 3i)(1 + 3i)} + \frac{1 \cdot (-i)}{i(-i)} = \frac{2i + 6i^2}{1^2 - (3i)^2} + \frac{-i}{-i^2} = \frac{2i - 6}{1 - 9i^2} + \frac{-i}{-(-1)} \\ &= \frac{2i - 6}{1 + 9} + \frac{-i}{1} = \frac{2i - 6}{10} + \frac{-10i}{10} = \frac{2i - 6 - 10i}{10} = \frac{-6 - 8i}{10} = -\frac{3}{5} - \frac{4}{5}i. \end{aligned}$$

Siis $\operatorname{Re} z = -3/5$ ja $\operatorname{Im} z = -4/5$.

Itseisarvon tutut ominaisuudet pätevät myös kompleksilukujen käänteisluvuille kuten seuraava lause osoittaa.

Lause 12.25. *Oletetaan, että $z \in \mathbb{C}$ ja $z \neq 0$. Käänteisluvun z^{-1} itseisarvo on itseisarvon käänteisluku $1/|z|$ eli*

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

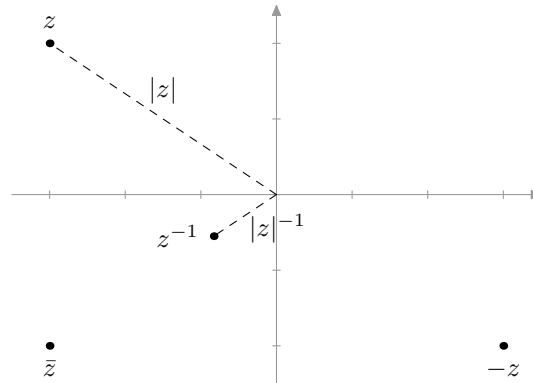
Todistus. Lauseen 12.17 mukaan itseisarvojen tulo on tulon itseisarvo, joten

$$|z^{-1}| \cdot |z| = |z^{-1}z| = |1| = 1.$$

Koska oletuksen mukaan $z \neq 0$, niin $|z| \neq 0$. Jakamalla luvulla $|z|$ saadaan

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

□



Kuva 12.8: Kompleksiluvun z liittoluku, käänteisluku ja vastaluku.

12.7 Yhtälöiden ratkaisemisesta

Yhtälön ratkaisu voi joskus löytyä kokeilemalla tai arvaamalla kuten seuraavassa esimerkissä.

Esimerkki 12.26. 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 12.27. 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 12.26 ja 12.27 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 12.28. Ratkaistaan kompleksilukujen joukossa yhtälö $iz + 3 = 5z - \frac{z}{i} + 2i$.

Rajataan aluksi mahdollisten ratkaisujen joukkoa tutkimalla, mitä voidaan päätellä lähtemällä oletuksesta, että yhtälö toteutuu.

$$\begin{aligned}iz + 3 = 5z - \frac{z}{i} + 2i &\stackrel{(1)}{\Rightarrow} i^2z + 3i = 5iz - z + 2i^2 \stackrel{(2)}{\Rightarrow} -z + 3i = 5iz - z - 2 \\ &\stackrel{(3)}{\Rightarrow} 3i + 2 = 5iz \stackrel{(4)}{\Rightarrow} \frac{3i + 2}{5i} = z\end{aligned}$$

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 12.29. 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:

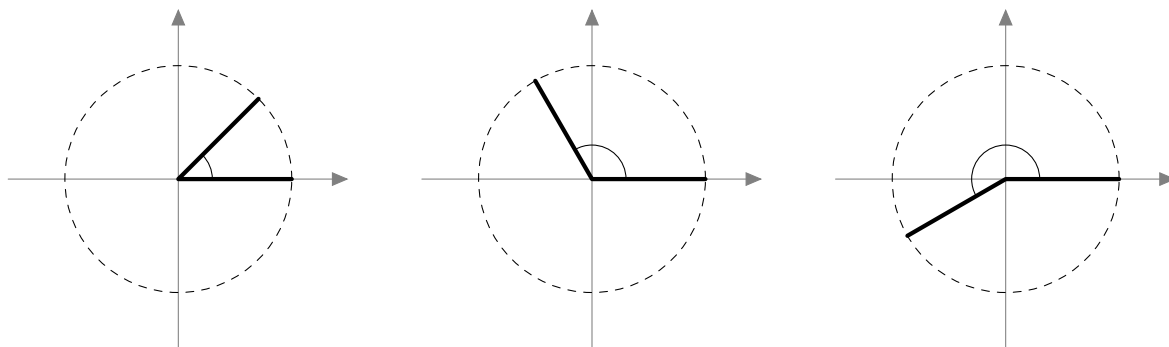
$$\begin{aligned} z = \frac{1 + 4i}{3 - 2i} &\Rightarrow (3 - 2i)z = 1 + 4i \Rightarrow 3z - 2iz = 1 + 4i \Rightarrow 3z = 1 + 2iz + 4i \\ &\Rightarrow 3z - 4i = 1 + 2iz. \end{aligned}$$

Nämä kaksi erisuuntaista päättelyä yhdessä osoittavat, että tarkastellulla yhtälöllä on tasan yksi ratkaisu, joka on

$$z = \frac{1 + 4i}{3 - 2i} = \frac{(3 + 2i)(1 + 4i)}{(3 + 2i)(3 - 2i)} = \frac{3 + 12i + 2i + 8i^2}{9 - 4i^2} = \frac{-5 + 14i}{13} = -\frac{5}{13} + \frac{14}{13}i.$$

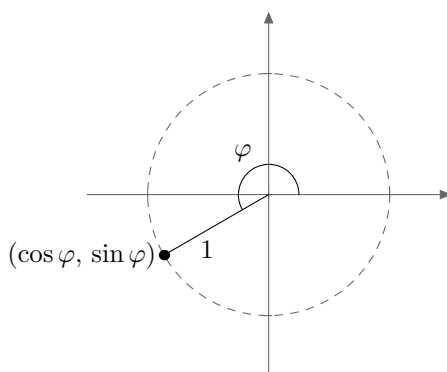
12.8 Napaesitys

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 vaakakselille. Kulman suuruus määrää sen, mihin suuntaan kulman toinen kylki piirretään. Tätä on havainnollistettu kuvassa 12.9.



Kuva 12.9: Yksikköympyrään piirretyt 45 asteen, 120 asteen ja 210 asteen kulmat.

Trigonometriset funktiot sini ja kosini voidaan määritellä yksikköympyrän avulla. Kulman φ kosini on kulmaa φ vastaavan yksikköympyrän kehäpisteen vaakakoordinaatti. Vastavasti kulman φ sini on tämän kehäpisteen pystykoordinaatti. Tätä havainnollistetaan kuvassa 12.10.

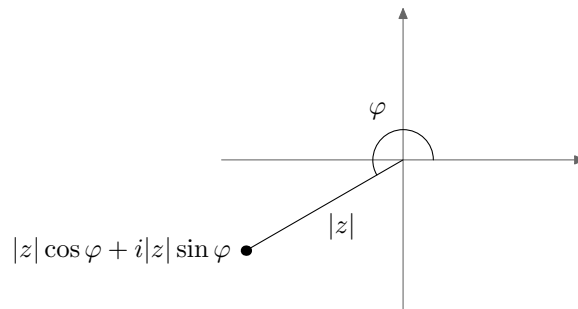


Kuva 12.10: Sini ja kosini yksikköympyrän avulla määriteltynä.

Määritelmä 12.30. Kompleksiluvun z *napaesitys* tarkoittaa sen esittämistä muodossa

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

missä $|z|$ on luvun z itseisarvo eli moduli ja φ on luvun z *vaihekulma* eli *argumentti*.

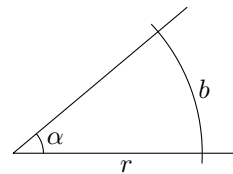


Kuva 12.11: Kompleksiluvun napaesitys.

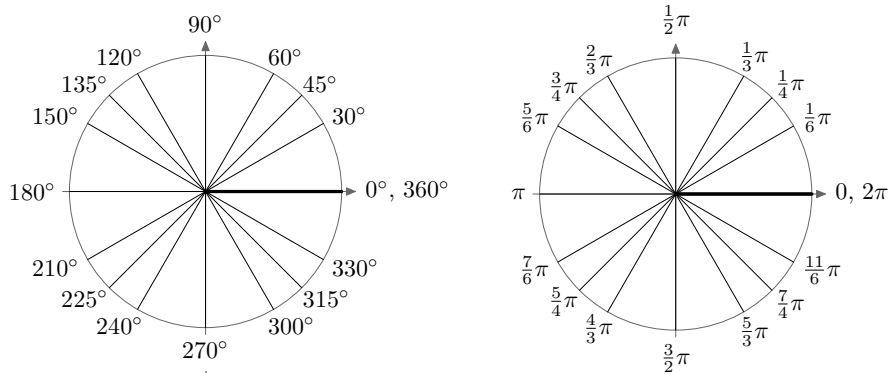
Kompleksiluvun vaihekulman yksikkönä on usein absoluuttinen kulmayksikkö eli radiaani.

Määritelmä 12.31. Kulman suuruus α radiaaneina on kulman rajoittaman ympyrän kaaren b suhde ympyrän säteeseen r :

$$\alpha = \frac{b}{r}$$

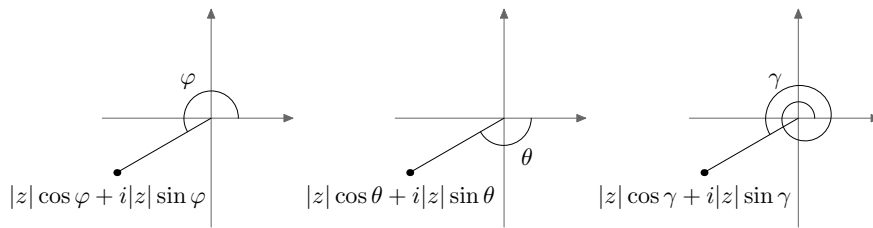


Täyskulma 360° vastaa 2π radiaania ja oikokulma 180° vastaa π radiaania. Näistä voidaan johtaa muiden kulmien tarkkoja arvoja radiaaneissa. Joitakin niistä on merkitty kuvaan 12.12.



Kuva 12.12: Joitakin kulmia ilmaistuna asteissa ja radiaaneissa.

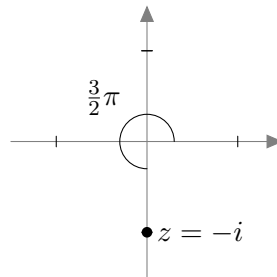
Kompleksiluvun vaihekulma ei ole yksikäsitteinen. Luvun 0 vaihekulmaksi voidaan valita mikä luku tahansa, sillä $0 = 0(\cos \varphi + i \sin \varphi)$ kaikilla $\varphi \in \mathbb{R}$. Nollasta poikkeavan kompleksiluvun vaihekulmat eroavat toisistaan jollain määrällä täysiä kierroksia. Toisin sanottuna nollasta poikkeavan kompleksiluvun tapauksessa kahden vaihekulman erotus on aina $n \cdot 2\pi$, missä $n \in \mathbb{Z}$. Tätä on havainnollistettu kuvassa 12.13.



Kuva 12.13: Kompleksiluvun z eri vaihekulmia: $\theta = \varphi - 2\pi$ ja $\gamma = \varphi + 2\pi$.

Esimerkki 12.32. Määritetään kompleksiluvun $z = -i$ napaesitys.

Itseisarvon määritelmän mukaan $|z| = \sqrt{0^2 + (-1)^2} = \sqrt{1} = 1$. Merkitään luku $z = -i$ kompleksitasoon:

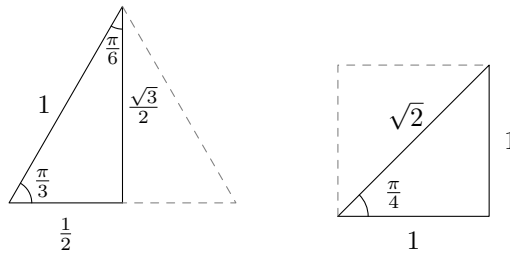


Kuva 12.14: Luku $z = -i$ kompleksitasossa.

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 $z = \cos(-\pi/2) + i \sin(-\pi/2)$.

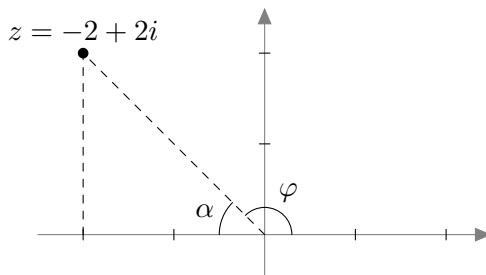
Joidenkin kompleksilukujen vaihekulman päätteleminen onnistuu niin sanottujen muistikolmioiden avulla. Ne voidaan johtaa tasasivuisesta kolmiosta ja neliöstä (kuva 12.15).



Kuva 12.15: Muistikolmiot.

Esimerkki 12.33. 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:

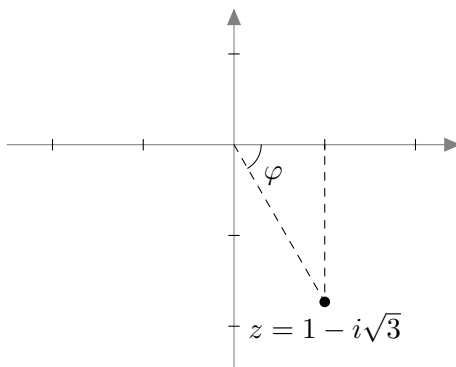


Kuva 12.16: Luku $z = -2 + 2i$ kompleksitasossa.

Kuvaan piirretyn suorakulmaisen kolmion molempien kateettien pituus on 2, joten $\alpha = 45^\circ$. Luvun z yksi vaihekulma on siten $\varphi = 180^\circ - 45^\circ = 135^\circ$ eli $\varphi = 3\pi/4$. Näin luvun z napaesitykseksi saadaan $z = 2\sqrt{2}(\cos(3\pi/4) + i \sin(3\pi/4))$.

Esimerkki 12.34. 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 12.17: 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 $\varphi = -60^\circ$ eli $\varphi = -\pi/3$. Näin luvun z napaesitykseksi saadaan $z = 2(\cos(-\pi/3) + i \sin(-\pi/3))$.

Vaihekulmaksi voidaan valita myös $360 - 60 = 300$ astetta eli $5\pi/3$ radiaania. Tällöin päädytään vaihtoehtoiseen napaesitykseen $z = 2(\cos(5\pi/3) + i \sin(5\pi/3))$.

Liittoluvun ja käänteisluvun määrittäminen onnistuu hyvin myös napaesityksessä, kuten seuraava lause osoittaa.

Lause 12.35. Oletetaan, että kompleksiluvulla z on napaesitys $z = |z|(\cos \varphi + i \sin \varphi)$. Tällöin luvun z liittoluku on

$$\bar{z} = |z|(\cos(-\varphi) + i \sin(-\varphi))$$

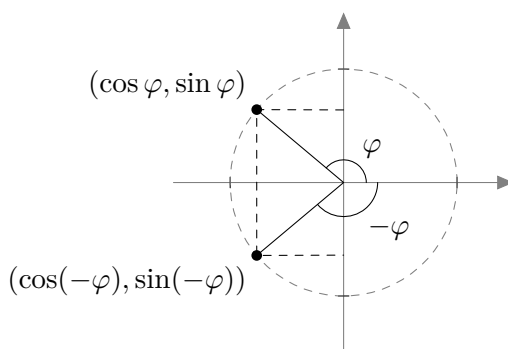
ja käänteisluku on

$$z^{-1} = |z|^{-1}(\cos(-\varphi) + i \sin(-\varphi)).$$

Todistus. Määritelmän 12.12 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 12.18: 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 12.19 ja liittoluvun \bar{z} napaesitystä luvun z käänteisluvuksi saadaan

$$z^{-1} = \frac{1}{|z|^2} \bar{z} = \frac{1}{|z|^2} \cdot |z|(\cos(-\varphi) + i \sin(-\varphi)) = \frac{1}{|z|}(\cos(-\varphi) + i \sin(-\varphi)).$$

□

Esimerkki 12.36. Esimerkissä 12.34 etsittiin luvulle $z = 1 - i\sqrt{3}$ napaesitys

$$z = 2(\cos(-\pi/3) + i \sin(-\pi/3)).$$

Lauseen 12.35 mukaan luvun z liittoluku on

$$\bar{z} = 2(\cos(\pi/3) + i \sin(\pi/3))$$

ja käänteisluku on

$$z^{-1} = \frac{1}{2}(\cos(\pi/3) + i \sin(\pi/3)).$$

Napaesityksen avulla saadaan toinen tapa kompleksilukujen tulon ja osamäärän laskemiseen:

Lause 12.37. 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 12.35 ja äsken todistettua tulosta. Se jätetään harjoitustehtäväksi. \square

Esimerkki 12.38. Lukujen $z = 1 - i\sqrt{3}$ ja $w = -2 + 2i$ napaesitykset ovat esimerkkien 12.34 ja 12.33 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 12.37 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 12.37 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 12.39. 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 12.40 (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

$$z^k = |z|^k(\cos k\varphi + i \sin k\varphi). \quad (\text{IO})$$

Käyttämällä induktio-oletusta ja lausetta 12.37 saadaan

$$\begin{aligned} z^{k+1} &= z \cdot z^k = |z|(\cos \varphi + i \sin \varphi) \cdot |z|^k(\cos k\varphi + i \sin k\varphi) \\ &= |z|^{k+1}(\cos(\varphi + k\varphi) + i \sin(\varphi + k\varphi)) \\ &= |z|^{k+1}(\cos(k+1)\varphi + i \sin(k+1)\varphi). \end{aligned}$$

Johtobäätös: 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 12.39 nojalla $z^m = (z^{-m})^{-1}$. Käytämällä äsken todistettua tulosta ja lausetta 12.35 saadaan

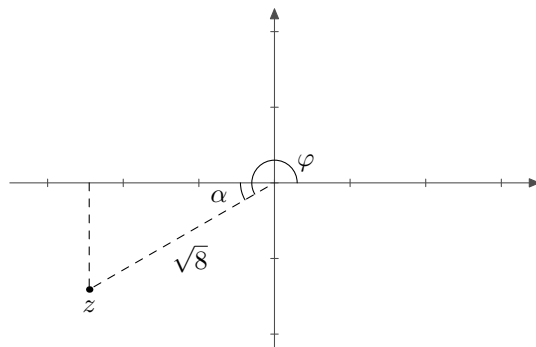
$$\begin{aligned} z^m &= (z^{-m})^{-1} = \left(|z|^{-m}(\cos(-m\varphi) + i \sin(-m\varphi)) \right)^{-1} \\ &= (|z|^{-m})^{-1}(\cos m\varphi + i \sin m\varphi) \\ &= |z|^m(\cos m\varphi + i \sin m\varphi) \end{aligned}$$

Näin on osoitettu, että kaikilla $n \in \mathbb{Z}$ pätee $z^n = |z|^n(\cos n\varphi + i \sin n\varphi)$. □

Esimerkki 12.41. Olkoon $z = -\sqrt{6} - i\sqrt{2}$. Lasketaan de Moivre'n 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 12.19: Luku $z = -\sqrt{6} - i\sqrt{2}$ kompleksitasossa.

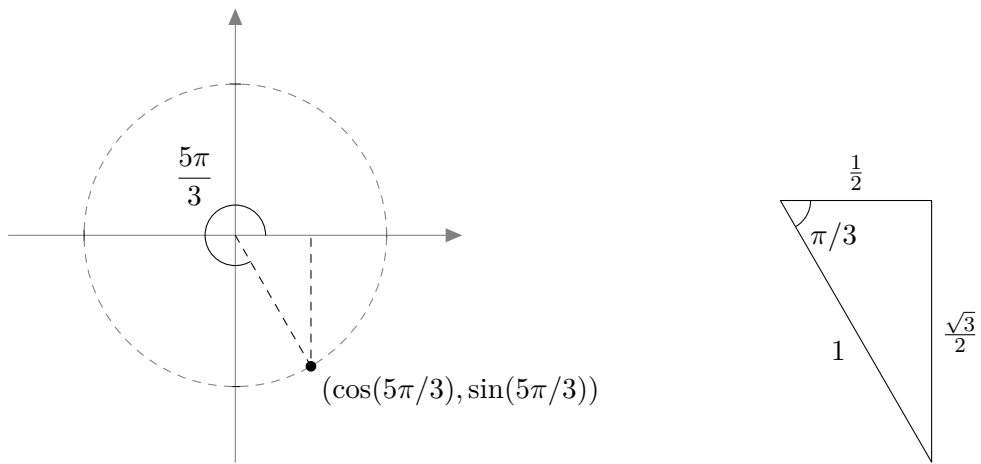
Kuvaan piirretyn suorakulmaisen kolmion kateettien pituudet ovat $\sqrt{6} = \sqrt{3}\sqrt{2}$ ja $\sqrt{2}$. Hypotenuusan pituus on $\sqrt{8} = 2\sqrt{2}$. Havaitaan, että kuvan 12.19 kolmio saadaan, kun kuvan 12.15 muistikolmion kaikki sivut kerrotaan luvulla $\sqrt{2}$. Kyseiset kolmiot ovat siis yhdenmuotoiset. Tästä voidaan päätellä, että $\alpha = \pi/6$. Luvun z yksi vaihekulma on siten $\varphi = \pi + \alpha = 7\pi/6$. Luvun z napaesitykseksi saadaan $z = 2\sqrt{2}(\cos(7\pi/6) + i\sin(7\pi/6))$.

Luvun z kymmenes potenssi voidaan nyt laskea de Moivre'n kaavalla (lause 12.40):

$$\begin{aligned} z^{10} &= (2\sqrt{2})^{10}(\cos(10 \cdot 7\pi/6) + i\sin(10 \cdot 7\pi/6)) \\ &= 2^{10}\sqrt{2}^{10}(\cos(70\pi/6) + i\sin(70\pi/6)) \\ &= 2^{10}2^5(\cos(11\pi + 4\pi/6) + i\sin(11\pi + 4\pi/6)) \\ &= 2^{15}(\cos(5 \cdot 2\pi + \pi + 2\pi/3) + i\sin(5 \cdot 2\pi + \pi + 2\pi/3)) \\ &= 2^{15}(\cos(\pi + 2\pi/3) + i\sin(\pi + 2\pi/3)) \\ &= 2^{15}(\cos(5\pi/3) + i\sin(5\pi/3)) \end{aligned}$$

Napaesityksestä voidaan siirtyä takaisin tavalliseen summuunmuotoiseen 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 12.20. Näin saadaan

$$z = 2^{15} \left(\frac{1}{2} - \frac{\sqrt{3}}{2}i \right) = 2^{14}(1 - i\sqrt{3}).$$



Kuva 12.20: Kosinin ja sinin arvojen päätteleminen yksikköympyrän ja muistikolmion avulla.

12.9 Eksponenttitesitys

Otetaan yksinkertaisuuden vuoksi käyttöön seuraava määritelmä:

Määritelmä 12.42. 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 12.42 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 12.42.

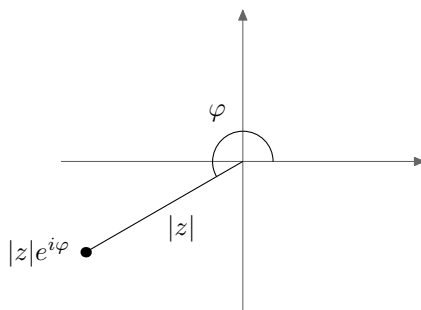
Määritelmän 12.42 avulla kompleksiluvun z napaesitys $|z|(\cos \varphi + i \sin \varphi)$ voidaan kirjoittaa muodossa $|z|e^{i\varphi}$. Tätä esitysmuotoa kutsutaan luvun z eksponenttitesitykseksi, kuten alla olevasta määritelmästä käy ilmi.

Määritelmä 12.43. Kompleksiluvun z eksponenttitesitys tarkoittaa luvun z esittämistä muodossa

$$z = |z|e^{i\varphi},$$

missä $|z|$ on luvun z itseisarvo ja φ on luvun z vaihekulma.

Kompleksiluvun z eksponenttitesitystä on havainnollistettu kuvassa 12.21.

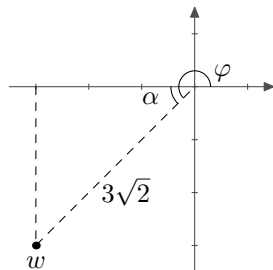


Kuva 12.21: Kompleksiluvun z eksponenttitesitys.

Esimerkki 12.44. Määritetään kompleksiluvun $w = -3 - 3i$ eksponenttitesitys.

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:



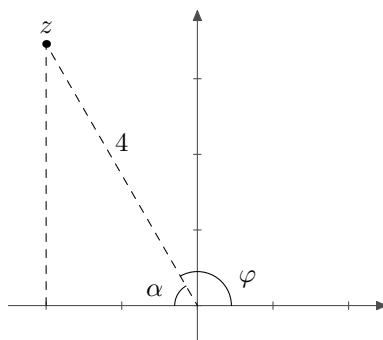
Kuva 12.22: Luku $w = -3 - 3i$ kompleksitasossa.

Kuvan 12.22 suorakulmaisesta kolmiosta saadaan pääteltyä, että $\alpha = \pi/4$. Luvun w vaihekulmaksi voidaan siten valita $\varphi = \pi + \alpha = 5\pi/4$. Näin luvun w eksponenttietesitykseksi saadaan

$$w = 3\sqrt{2}e^{\frac{5\pi}{4}i}.$$

Esimerkki 12.45. Määritetään kompleksiluvun $z = -2 + 2\sqrt{3}i$ eksponenttietisyys.

Itseisarvon määritelmän mukaan $|z| = \sqrt{(-2)^2 + (2\sqrt{3})^2} = \sqrt{16} = 4$. Merkitään luku $z = -2 + 2\sqrt{3}i$ kompleksitasoon:



Kuva 12.23: Luku $z = -2 + 2\sqrt{3}i$ kompleksitasossa.

Kuvan 12.23 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 eksponenttietesitykseksi saadaan

$$z = 4e^{\frac{2\pi}{3}i}.$$

Napaesityksen laskusääntöjä koskevista lauseista 12.35 ja 12.37 sekä de Moivre'n kaavasta 12.40 seuraa, että eksponenttietesitystä käytettäessä voidaan soveltaa tuttuja potenssien laskusääntöjä. Tätä havainnollistetaan seuraavissa esimerkeissä.

Esimerkki 12.46. Määritetään luvun $z = 3e^{-\frac{\pi}{2}i} \cdot 7e^{\frac{\pi}{4}i}$ itseisarvo, vaihekulma, reaali- ja imaginaariosa.

Itseisarvo ja vaihekulma saadaan sieventämällä lukua z tuttujen laskusääntöjen avulla:

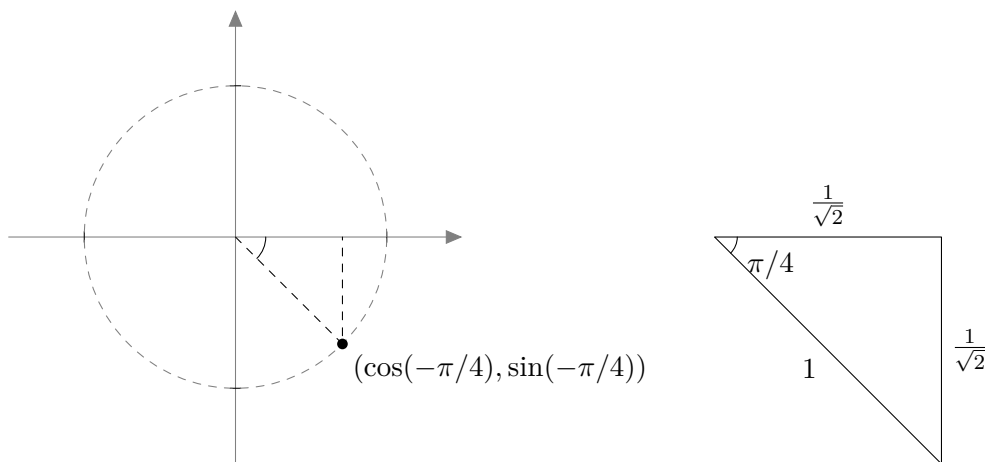
$$z = 3e^{-\frac{\pi}{2}i} \cdot 7e^{\frac{\pi}{4}i} = 3 \cdot 7e^{(-\frac{\pi}{2} + \frac{\pi}{4})i} = 21e^{-\frac{\pi}{4}i}.$$

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 12.24).



Kuva 12.24: Kosinin ja sinin arvojen päätteleminen yksikköympyrän ja muistikolmion avulla.

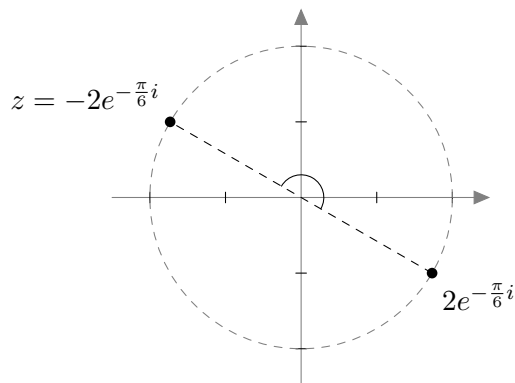
Esimerkki 12.47. Määritetään luvun $z = -2e^{-\frac{\pi}{6}i}$ itseisarvo ja vaihekulma sekä reaali- ja imaginaariosa.

Huomataan, että z ei ole eksponenttesityksessä, sillä kerroin -2 on negatiivinen. Käyttämällä luvun -2 eksponenttesitystä $-2 = 2e^{\pi i}$ 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 π . Luvun z itseisarvo on siten $|z| = 2$ ja luvun z vaihekulmaksi kelpaa $-\pi/6 + \pi = 5\pi/6$. Tätä on havainnollistettu kuvassa 12.25.

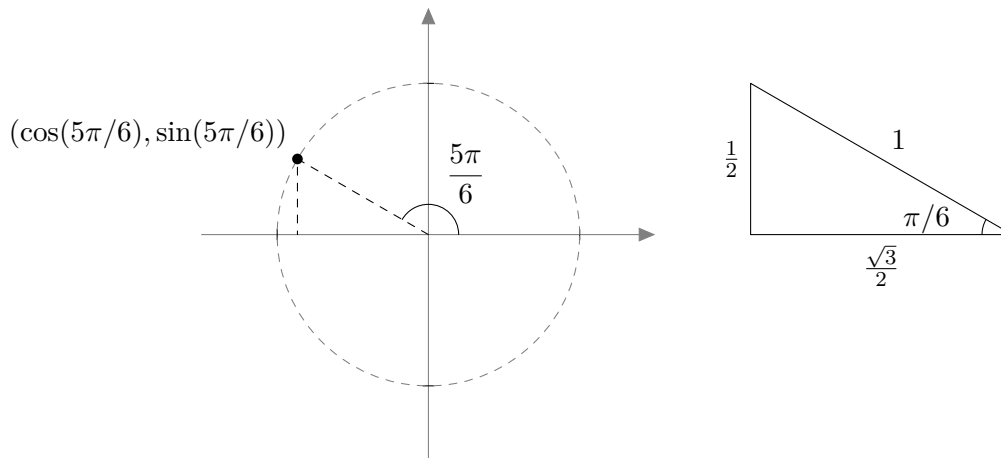


Kuva 12.25: Luku $z = -2e^{-\frac{\pi}{6}i}$ on luvun $2e^{-\frac{\pi}{6}i}$ vastaluku.

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 12.26).



Kuva 12.26: Kosinin ja sinin arvojen päättelemineen yksikköympyrän ja muistikolmion avulla.

12.10 Binomiyhtälö

Tässä kappaleessa sovelletaan kompleksilukujen eksponenttitesitystä niin sanottujen binomiyhtälöiden ratkaisemiseen.

Määritelmä 12.48. 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 12.49. Ratkaistaan kompleksilukujen joukossa yhtälö $x^5 = 1$.

Aloitetaan muodostamalla eksponenttitesitys vakiolle 1. Koska luvun 1 itseisarvo on 1 ja sen vaihekulmaksi voidaan valita 0, saadaan eksponenttitesitykseksi $1 = e^{0i}$. Muodostetaan eksponenttitesitys myös tuntemattomalle x merkitsemällä $x = re^{i\varphi}$, missä $\varphi, r \in \mathbb{R}$ ja $r \geq 0$.

Tarkasteltava yhtälö voidaan eksponenttitesitysten avulla kirjoittaa muodossa

$$(re^{i\varphi})^5 = e^{0i}.$$

Kompleksilukujen laskusääntöjen avulla yhtälön vasenta puolta voidaan sieventää, jolloin yhtälö saadaan muotoon

$$r^5 e^{5i\varphi} = e^{0i}. \quad (1)$$

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 (1) 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 φ ovat reaalilukuja ja lisäksi $r \geq 0$, joten yhtälöpari voidaan ratkaista tavallisia reaalilukujen laskusääntöjä käyttäen:

$$\begin{cases} r^5 = 1 \\ 5\varphi - 0 = k \cdot 2\pi \end{cases} \Leftrightarrow \begin{cases} r = \sqrt[5]{1} \\ 5\varphi = k \cdot 2\pi \end{cases} \Leftrightarrow \begin{cases} r = 1 \\ \varphi = k \cdot \frac{2}{5}\pi. \end{cases}$$

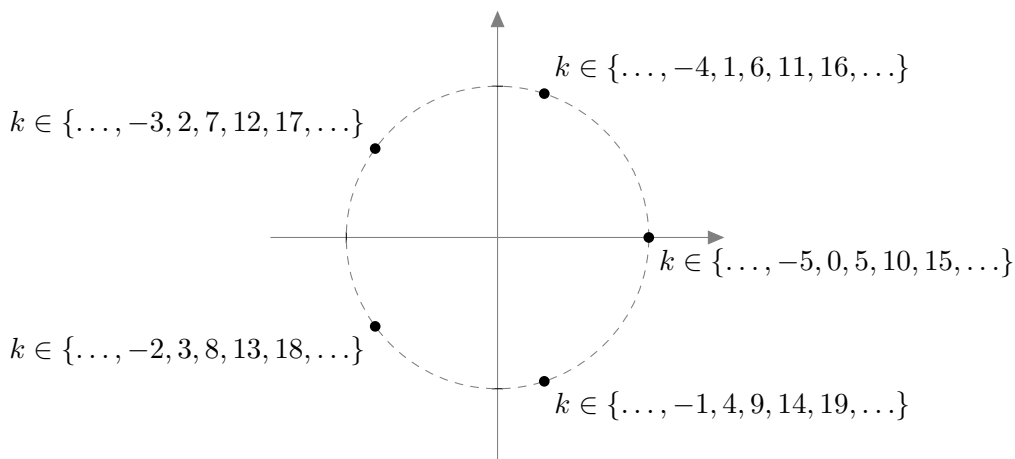
Yhtälöparin ratkaisut ovat siis

$$\begin{cases} r = 1 \\ \varphi = k \cdot \frac{2}{5}\pi, \end{cases}$$

missä $k \in \mathbb{Z}$. Havaitaan, että kaikkien ratkaisujen itseisarvo on 1, joten ne sijaitsevat kompleksitasossa yksikköympyrän kehällä. Eri ratkaisuja saadaan kaikkiaan viisi kappaletta:

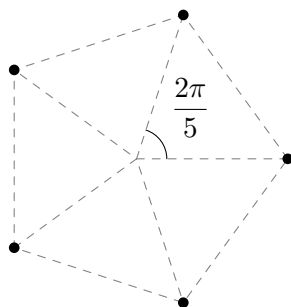
$$1, \quad e^{\frac{2}{5}\pi i}, \quad e^{\frac{4}{5}\pi i}, \quad e^{\frac{6}{5}\pi i}, \quad e^{\frac{8}{5}\pi i}.$$

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 12.27.



Kuva 12.27: 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 12.28.



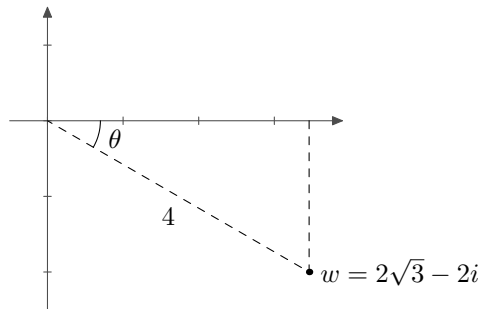
Kuva 12.28: Yhtälön $x^5 = 1$ ratkaisut muodostavat kompleksitasoon säännöllisen viisikulmion.

Esimerkki 12.50. Ratkaistaan kompleksilukujen joukossa yhtälö $z^4 = 2\sqrt{3} - 2i$.

Aloitetaan muodostamalla eksponenttesitys 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 θ saadaan ratkaistua kuvan 12.29 suorakulmaisesta kolmiosta:



Kuva 12.29: Luku $w = 2\sqrt{3} - 2i$ kompleksitasossa.

Vakion $2\sqrt{3} - 2i$ eksponenttesitykseksi saadaan näin $2\sqrt{3} - 2i = 4e^{-\frac{\pi}{6}i}$. Muodostetaan eksponenttesitys myös tuntemattomalle z merkitsemällä $z = re^{i\varphi}$, missä $\varphi, r \in \mathbb{R}$ ja $r \geq 0$.

Tarkasteltava yhtälö voidaan eksponenttesitysten avulla kirjoittaa muodossa

$$(re^{i\varphi})^4 = 4e^{-\frac{\pi}{6}i}.$$

Kompleksilukujen laskusääntöjen avulla yhtälön vasenta puolta voidaan sieventää, jolloin yhtälö saadaan muotoon

$$r^4 e^{4i\varphi} = 4e^{-\frac{\pi}{6}i}. \quad (2)$$

Tämä yhtälö toteutuu, jos ja vain jos siinä esiintyvillä kompleksiluvuilla $r^4 e^{4i\varphi}$ 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 (2) kanssa yhtäpitävä yhtälöpari on siten

$$\begin{cases} r^4 = 4 \\ 4\varphi - \left(-\frac{\pi}{6}\right) = k \cdot 2\pi, \end{cases}$$

missä $k \in \mathbb{Z}$. Ratkaistaan tästä yhtälöparista r ja φ :

$$\begin{cases} r^4 = 4 \\ 4\varphi - \left(-\frac{\pi}{6}\right) = k \cdot 2\pi, \end{cases} \Leftrightarrow \begin{cases} r^2 = 2 \vee r^2 = -2 \\ 4\varphi = -\frac{\pi}{6} + k \cdot 2\pi \end{cases} \Leftrightarrow \begin{cases} r = \sqrt{2} \vee r = -\sqrt{2} \\ \varphi = -\frac{\pi}{24} + k \cdot \frac{\pi}{2}, \end{cases}$$

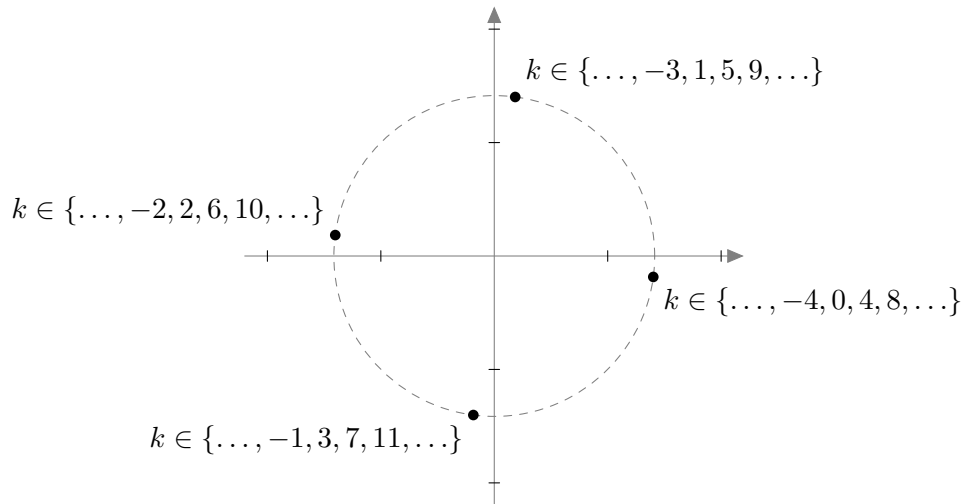
Huomaa, että vaihtoehto $r^2 = -2$ on aina epätosi eikä tuota ollenkaan ratkaisuja. Lisäksi oletuksen mukaan $r \geq 0$, joten ainoa mahdollinen vaihtoehto on $r = \sqrt{2}$. Ratkaisuiksi saadaan siis

$$\begin{cases} r = \sqrt{2} \\ \varphi = -\frac{\pi}{24} + k \cdot \frac{\pi}{2}, \end{cases}$$

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:

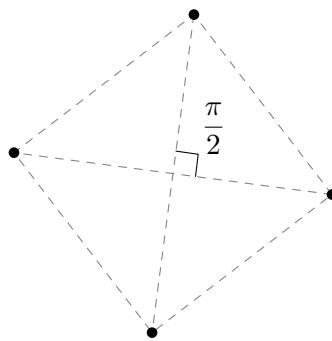
$$\sqrt{2}e^{-\frac{1}{24}\pi i}, \quad \sqrt{2}e^{\frac{11}{24}\pi i}, \quad \sqrt{2}e^{\frac{23}{24}\pi i}, \quad \sqrt{2}e^{\frac{35}{24}\pi i}.$$

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 12.30.



Kuva 12.30: 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 12.31.



Kuva 12.31: Yhtälön $z^4 = 2\sqrt{3} - 2i$ ratkaisut muodostavat kompleksitasoon neliön.

12.11 Toisen asteen yhtälö

Esimerkki 12.51. 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 12.18 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 12.52. Tarkastellaan toisen asteen yhtälöä $x^2 = -9$. Sillä ei ole ratkaisuja reaali-
lukujen joukossa, koska $x^2 \geq 0$ kaikilla $x \in \mathbb{R}$. Yhtälö $x^2 = -9$ voidaan kuitenkin kompleksi-
lukujen joukossa ratkaista samaan tapaan kuin mikä tahansa binomiyhtälö:

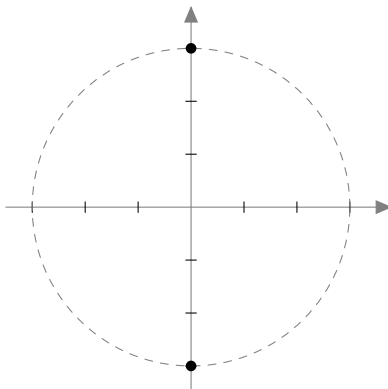
Eksponttitesitysten avulla yhtälö $x^2 = -9$ voidaan kirjoittaa muodossa $(re^{i\varphi})^2 = 9e^{\pi i}$
eli muodossa $r^2 e^{2i\varphi} = 9e^{\pi i}$. Tämä yhtälö toteutuu, jos ja vain jos siinä esiintyvillä kompleksi-
lukuilla $r^2 e^{2i\varphi}$ ja $9e^{\pi i}$ on sama itseisarvo ja niiden vaihekulmien 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 $k \in \mathbb{Z}$. Eksponttitesityksessä itseisarvo $r \geq 0$, joten ratkaisuiksi saadaan

$$\begin{cases} r = 3 \\ \varphi = \frac{\pi}{2} + k \cdot \pi, \end{cases}$$

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 12.32: Yhtälön $x^2 = -9$ ratkaisut $3i$ ja $-3i$ kompleksitasossa.

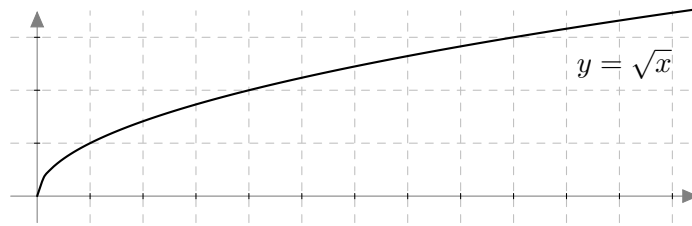
Toisen asteen yhtälöiden ratkaisemiseen liittyy myös neliöjuuren käsite, joka on määritelty epänegatiivisille reaaliluvuille:

Määritelmä 12.53. 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 12.53 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 $[0, \infty[\rightarrow [0, \infty[$. Huomaa, että negatiivisen reaaliluvun neliöjuuri ei ole määritelty.



Kuva 12.33: Osa neliöjuurifunktion $x \mapsto \sqrt{x}$ kuvaajasta.

Esimerkki 12.54. Esimerkissä 12.51 saatiin yhtälön $x^2 = 25$ ratkaisuksi 5 ja -5 . Luvun 25 neliöjuuri on $\sqrt{25} = 5$, sillä $5^2 = 25$ ja $5 \geq 0$.

Esimerkki 12.55. Esimerkin 12.52 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 φ 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.

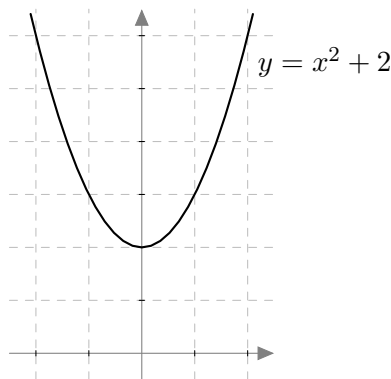
Esimerkki 12.56. Tarkastellaan yhtälöä $x^2 = -2$. Se voidaan ratkaista binomiyhtälönä samaan tapaan kuin esimerkissä 12.52. Käytetään nyt kuitenkin toista ratkaisutapaa, joka perustuu tulon nollasääntöön ja muistuttaa esimerkin 12.51 ratkaisua.

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 12.18 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 12.34.



Kuva 12.34: Yhtälöllä $x^2 + 2 = 0$ ei ole ratkaisuja reaalilukujen joukossa.

Esimerkin 12.56 tulos voidaan yleistää seuraavaksi lauseeksi:

Lause 12.57. Oletetaan, että $r \in \mathbb{R}$ ja $r < 0$. Yhtälöllä $x^2 = r$ on kompleksilukujen 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 12.56. Koska $r < 0$, pätee $r = -|r| = |r|i^2$.

$$\begin{aligned} x^2 = r &\Leftrightarrow x^2 = |r|i^2 \Leftrightarrow x^2 - |r|i^2 = 0 \Leftrightarrow x^2 - (i\sqrt{|r|})^2 = 0 \\ &\Leftrightarrow (x - i\sqrt{|r|})(x + i\sqrt{|r|}) = 0 \end{aligned}$$

Tulon nollasäännön 12.18 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

$$(a + b)^2 = a^2 + 2ab + b^2. \quad (3)$$

Neliöksi täydentämistä havainnollistetaan seuraavassa esimerkissä.

Esimerkki 12.58. Täydennetään neliöksi lauseke $x^2 + x - 6$. Muokataan lauseketta vaiheittain niin, että se muistuttaisi enemmän yhtälön (3) oikeaa puolta. Pidetään joka vaiheessa huolta, että yhtäsuuruus säilyy koko ajan:

$$x^2 + x - 6 = x^2 + 2 \cdot \frac{1}{2} \cdot x - 6 = x^2 + 2 \cdot \frac{1}{2} \cdot x + \underbrace{\left(\frac{1}{2}\right)^2}_{a=x \text{ ja } b=1/2} - \left(\frac{1}{2}\right)^2 - 6$$

Lausekkeeseen saatiin näkyviin yhtälön (3) 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:

$$\begin{aligned} ax^2 + bx + c = 0 &\Leftrightarrow a^2x^2 + abx + ac = 0 \\ &\Leftrightarrow (ax)^2 + 2 \cdot ax \cdot \frac{b}{2} = -ac \\ &\Leftrightarrow (ax)^2 + 2 \cdot ax \cdot \frac{b}{2} + \left(\frac{b}{2}\right)^2 = -ac + \left(\frac{b}{2}\right)^2 \\ &\Leftrightarrow \left(ax + \frac{b}{2}\right)^2 = -\frac{4ac}{4} + \frac{b^2}{4} \\ &\Leftrightarrow \left(ax + \frac{b}{2}\right)^2 = \frac{b^2 - 4ac}{4} \end{aligned} \quad (*)$$

Havaitaan, että saadun yhtälön (*) oikea puoli on epänegatiivinen, jos ja vain jos diskriminantti $b^2 - 4ac \geq 0$. Tässä tapauksessa ratkaisuksi 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 12.57 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 12.59. 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

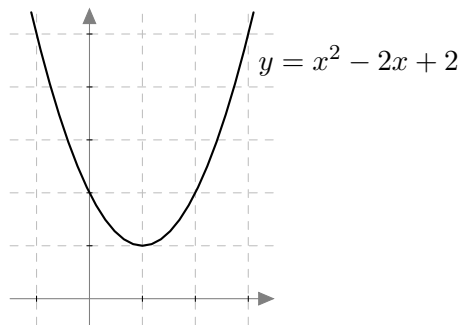
$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Jos diskriminantti $b^2 - 4ac < 0$, yhtälön ratkaisut ovat

$$x = \frac{-b \pm i \sqrt{|b^2 - 4ac|}}{2a}.$$

Esimerkki 12.60. 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

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

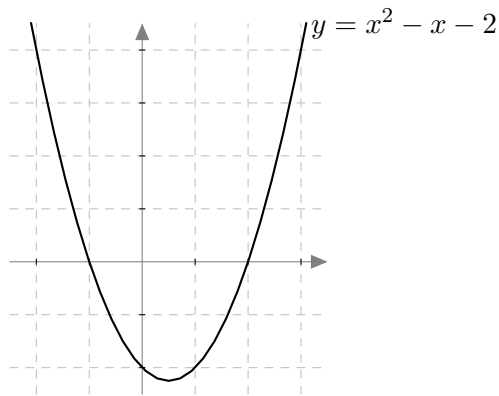


Kuva 12.35: Yhtälöllä $x^2 - 2x + 2 = 0$ ei ole ratkaisuja reaalilukujen joukossa.

Esimerkki 12.61. 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

$$x = \frac{-(-1) \pm \sqrt{(-1)^2 - 4 \cdot 1 \cdot (-2)}}{2 \cdot 1} = \frac{1 \pm \sqrt{9}}{2} = \frac{1 \pm 3}{2}.$$

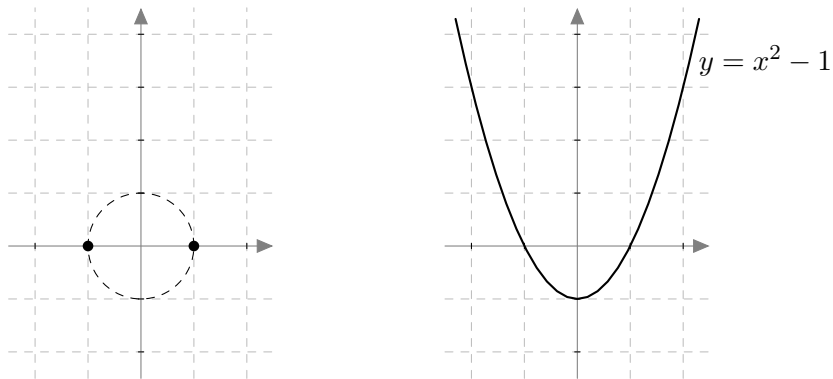
Ratkaisut ovat siis $x_1 = -1$ ja $x_2 = 2$. Tilannetta on havainnollistettu kuvassa 12.36.



Kuva 12.36: Yhtälön $x^2 - x - 2 = 0$ ratkaisut ovat $x_1 = -1$ ja $x_2 = 2$.

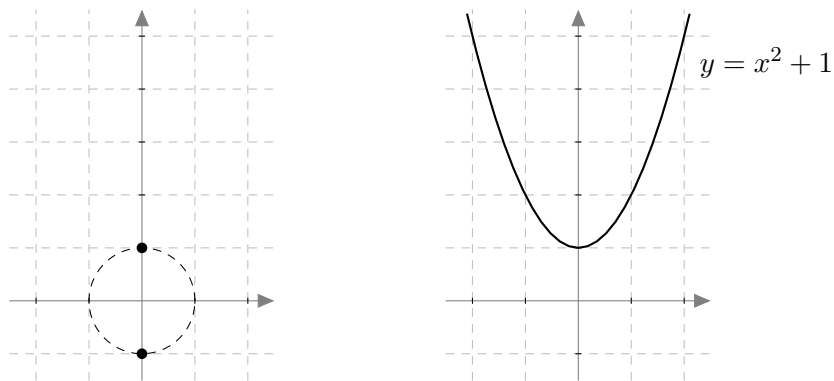
Seuraavissa esimerkeissä havainnollistetaan erityyppisiä toisen asteen yhtälöitä ja niiden ratkaisuja.

Esimerkki 12.62. 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 12.37 on havainnollistettu yhtälön ratkaisuja kompleksitasossa.



Kuva 12.37: Yhtälön $x^2 = 1$ ratkaisut ovat funktion $x \mapsto x^2 - 1$ nollakohdat.

Esimerkki 12.63. Yhtälö $x^2 = -1$ toteutuu, jos ja vain jos $x = i$ tai $x = -i$. Alla olevassa kuvassa 12.38 on havainnollistettu yhtälön ratkaisuja kompleksitasossa. Ratkaisut eivät ole reaalisia, mikä nähdään myös siitä, ettei vastaavalla polynomifunktiolla $x \mapsto x^2 + 1$ ole nollakohtia.

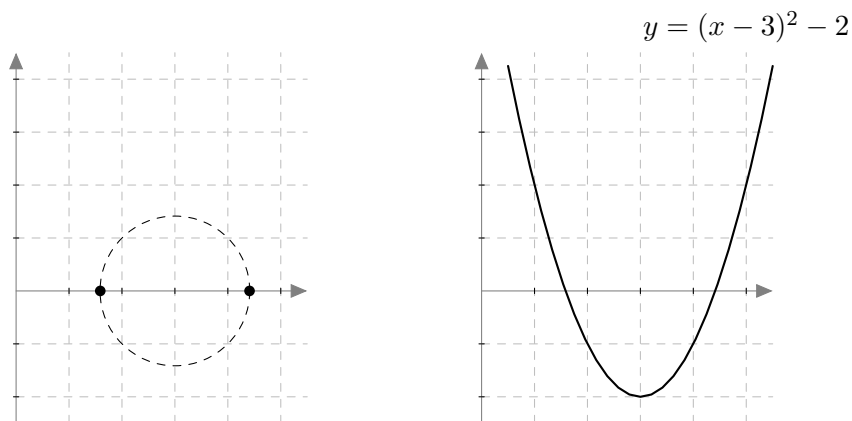


Kuva 12.38: Yhtälöllä $x^2 = -1$ ei ole ratkaisuja reaalilukujen joukossa.

Esimerkki 12.64. Ratkaistaan yhtälö $(x - 3)^2 = 2$:

$$(x - 3)^2 = 2 \Leftrightarrow x - 3 = \pm\sqrt{2} \Leftrightarrow x = 3 \pm \sqrt{2}.$$

Kuvassa 12.40 on havainnollistettu yhtälön ratkaisuja kompleksitasossa. Havaitaan, että ratkaisut sijaitsevat kompleksitasossa ympyrällä, jonka keskipiste on $(3, 0)$ ja säde on $\sqrt{2}$.

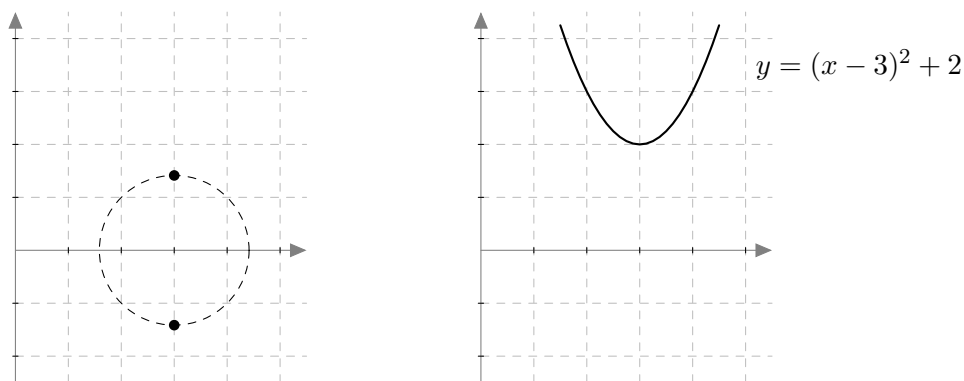


Kuva 12.39: Yhtälön $(x - 3)^2 = 2$ ratkaisut ovat funktion $x \mapsto (x - 3)^2 - 2$ nollakohdat.

Esimerkki 12.65. 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 12.39 on havainnollistettu yhtälön ratkaisuja kompleksitasossa. Havaitaan, että ratkaisut sijaitsevat kompleksitasossa ympyrällä, jonka keskipiste on $(3, 0)$ ja säde on $\sqrt{2} = \sqrt{|-2|}$.



Kuva 12.40: Yhtälöllä $(x - 3)^2 = -2$ ei ole ratkaisuja reaalilukujen joukossa.

Esimerkki 12.66. 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 eksponenttitesitystä $2i = 2e^{i\pi/2}$. Tällöin

$$\begin{aligned} z^2 = 2i &\Leftrightarrow r^2 e^{i \cdot 2\varphi} = 2e^{i\pi/2} \Leftrightarrow r = \pm\sqrt{2} \wedge 2\varphi = \pi/2 + n \cdot 2\pi \\ &\Leftrightarrow r = \pm\sqrt{2} \wedge \varphi = \pi/4 + n \cdot \pi, \end{aligned}$$

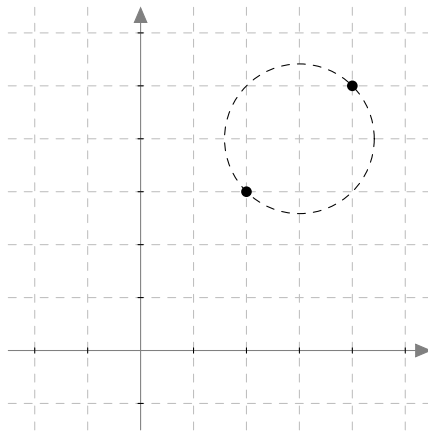
missä $n \in \mathbb{Z}$. Erilaisia ratkaisuja saadaan kaksi:

$$\begin{aligned} z_1 &= \sqrt{2}e^{i\pi/4} = 1 + i \\ z_2 &= \sqrt{2}e^{i\cdot 5\pi/4} = -1 - i. \end{aligned}$$

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 12.41 havaitaan, että ratkaisut sijaitsevat kompleksitasossa ympyrällä, jonka keskipiste on $3 + 4i$ ja säde on $\sqrt{2} = \sqrt{|2i|}$.



Kuva 12.41: Yhtälön $(x - (3 + 4i))^2 = 2i$ ratkaisut kompleksitasossa.

Esimerkki 12.67. 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 :

$$\begin{cases} a^2 - b^2 = 3 \\ 2ab = -4 \end{cases} \Leftrightarrow \begin{cases} a^2 - b^2 = 3 \\ b = -\frac{2}{a} \end{cases} \Leftrightarrow \begin{cases} a^2 - \frac{4}{a^2} = 3 \\ b = -\frac{2}{a} \end{cases} \Leftrightarrow \begin{cases} a^4 - 3a^2 - 4 = 0 \\ b = -\frac{2}{a} \end{cases}$$

Yhtälöä $a^4 - 3a^2 - 4 = 0$ voidaan ajatella toisen asteen yhtälönä, jossa tuntematon on a^2 . Näin saadaan

$$a^2 = \frac{-(-3) \pm \sqrt{(-3)^2 - 4 \cdot 1 \cdot (-4)}}{2 \cdot 1} = \frac{3 \pm \sqrt{25}}{2} = \frac{3 \pm 5}{2}.$$

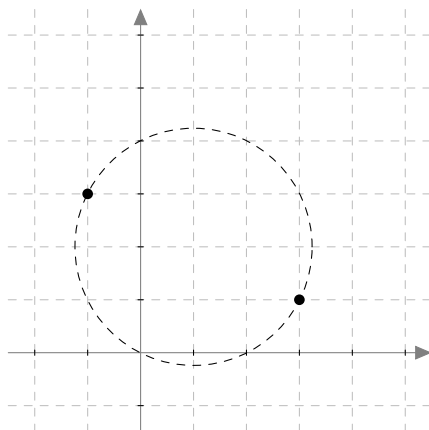
Koska $a \in \mathbb{R}$, sen toinen potenssi ei voi olla negatiivinen, ja siten ainoaksi ratkaisuksi saadaan $a^2 = 4$. Näin $a = \pm 2$ ja siten $b = -2/a = \mp 1$. Siis

$$z^2 = 3 - 4i \Leftrightarrow z = \pm(2 - i).$$

Alkuperäinen yhtälö $(x - (1 + 2i))^2 = 3 - 4i$ saadaan nyt ratkaistua:

$$(x - (1 + 2i))^2 = 3 - 4i \Leftrightarrow x - (1 + 2i) = \pm(2 - i) \Leftrightarrow x = 3 + i \vee x = -1 + 3i.$$

Kuvasta 12.42 havaitaan, että ratkaisut sijaitsevat kompleksitasossa ympyrällä, jonka keskipiste on $1 + 2i$ ja säde on $\sqrt{5} = \sqrt{|3 - 4i|}$.



Kuva 12.42: Yhtälön $(x - (1 + 2i))^2 = 3 - 4i$ ratkaisut kompleksitasossa.