Matematiikka tutuksi -kurssi

Permutaatiot

Avoin yliopisto & Matematiikan ja tilastotieteen laitos
Helsingin yliopisto
Kesä 2015

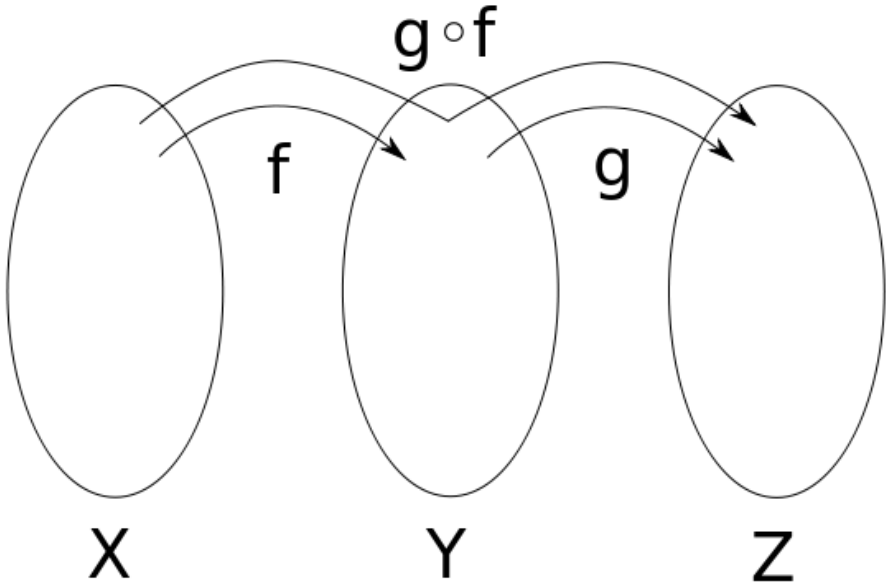
Juulia Lahdenperä

Yhdistetty kuvaus

Olkoot $f : X \to Y$ ja $g : Y \to Z$ kuvauksia. **Yhdistetty kuvaus** $g \circ f : X \to Z$ määritellään yhtälöllä

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

kaikilla $x \in X$.



Yhdistetty kuvaus

Esimerkki. Olkoot

$$f : \mathbb{R} \setminus \{0\} \to \mathbb{R}, \ f(x) = \frac{1}{x}$$

ja

$$g : \mathbb{R} \to \mathbb{R}, \ g(x) = x^2 + 1.$$

Nyt yhdistetty kuvaus $g \circ f : \mathbb{R} \setminus \{0\} \to \mathbb{R}$ on

$$(g \circ f)(x) = g(f(x)) = g\left(\frac{1}{x}\right) = \left(\frac{1}{x}\right)^2 + 1.$$

Huomaa, että yhdistettyä kuvausta $f \circ g$ ei voida määrittää, sillä funktio f ei liitä funktion g maalijoukon alkioon 0 mitään alkiota joukosta $\mathbb{R}$.

Yhdistetty kuvaus

Esimerkki. Määritellään

$$h : \mathbb{N} \to \mathbb{N},\ h(n) = n^2$$

ja

$$j : \mathbb{N} \to \mathbb{N},\ j(n) = 2n.$$

Nyt yhdistetty kuvaus $h \circ j(n) : \mathbb{N} \to \mathbb{N}$ on

$$(h \circ j)(n) = h(j(n)) = h(2n) = (2n)^2 = 4n^2.$$

Yhdistetty kuvaus $j \circ h : \mathbb{N} \to \mathbb{N}$ on

$$(j \circ h)(n) = j(h(n)) = j(n^2) = 2n^2.$$

Huomaa, että kuvausten yhdistäminen ei ole vaihdannainen operaatio (esimerkiksi tässä $h \circ j \neq j \circ h$).

Identtinen kuvaus

Joukon A **identtinen kuvaus** on kuvaus $id_A : A \to A$, jolle pätee $f(a) = a$ kaikilla $a \in A$. Toisin sanoen identtinen kuvaus pitää kaikki joukon A alkiot paikoillaan.

Kaikilla kuvauksilla $f : A \to B$ pätee

$$f \circ id_A = f \quad \text{ja} \quad id_B \circ f = f.$$

Käänteiskuvaus

Olkoon $f : A \to B$ kuvaus. Kuvaus $g : B \to A$ on kuvauksen f **käänteiskuvaus**, jos

$$g \circ f = id_A \quad \text{ja} \quad f \circ g = id_B.$$

Tällöin käänteiskuvausta g merkitään f^{-1}. Toisin sanoen

$$f^{-1}(f(a)) = a \quad \text{kaikilla} \quad a \in A$$

ja

$$f(f^{-1}(b)) = b \quad \text{kaikilla} \quad b \in B.$$

Kuvauksella on käänteiskuvaus jos ja vain jos se on bijektio.

Käänteiskuvaus

Esimerkki. Kuvauksen $f : \mathbb{R} \to \mathbb{R},\ f(x) = 2x + 1$ käänteiskuvaus on kuvaus $f^{-1} : \mathbb{R} \to \mathbb{R},\ f^{-1}(x) = \frac{1}{2}x - \frac{1}{2}$, sillä

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

ja

$$\begin{aligned}(f \circ f^{-1})(x) = f(f^{-1}(x)) &= \left(\frac{1}{2}x - \frac{1}{2}\right) = 2\left(\frac{1}{2}x - \frac{1}{2}\right) + 1 \\ &= x - 1 + 1 = x\end{aligned}$$

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

Käänteiskuvaus I

Joskus kuvauksen käänteiskuvauksen voi päätellä suoraan kuvauksen lausekkeesta. Se ei aina kuitenkaan ole yksinkertaista. **Miten käänteiskuvauksen sitten löytää?**

Esimerkki. Olkoon $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 5x + 6$. Huomataan, että kyseessä on bijektio. Tällöin käänteiskuvaus on olemassa. Käänteiskuvauksen löytää seuraavasti:
Tutkitaan kuvauksen f lauseketta. Huomataan, että

$$\begin{aligned} y &= 5x + 6 \\ \Rightarrow y - 6 &= 5x \\ \Rightarrow \frac{y-6}{5} &= x. \end{aligned}$$

Muodostetaan tämän avulla käänteiskuvausehdokas $g : \mathbb{R} \to \mathbb{R}$, $g(x) = \frac{x-6}{5}$. Tarkistetaan sitten, onko $f \circ g = g \circ f = id$:

Käänteiskuvaus II

$$(f \circ g)(x) = f(g(x)) = f(\frac{x-6}{5}) = 5(\frac{x-6}{5}) + 6$$
$$= x - 6 + 6 = x = id$$

ja

$$(g \circ f)(x) = g(f(x)) = g(5x+6) = \frac{(5x+6)-6}{5} = \frac{5x}{5}$$
$$= x = id.$$

Näin ollen kuvaus g on kuvauksen f käänteiskuvaus, ja voidaan merkitä $g = f^{-1}$.

Permutaatiot

Joukon **permutaatio** on bijektio joukolta itselleen. Se kuvaa joukon sisäistä muutosta, ja tietyssä mielessä permutaatio onkin joukon alkioiden uudelleenjärjestelyä. Permutaatioilla lasketaan kuten kuvauksilla – ensin oikeanpuoleinen ja sitten vasemmanpuoleinen permutaatio. Permutaatioiden σ ja τ tulo on siis $\sigma\tau = \sigma \circ \tau$.

Permutaatiot

Esimerkki

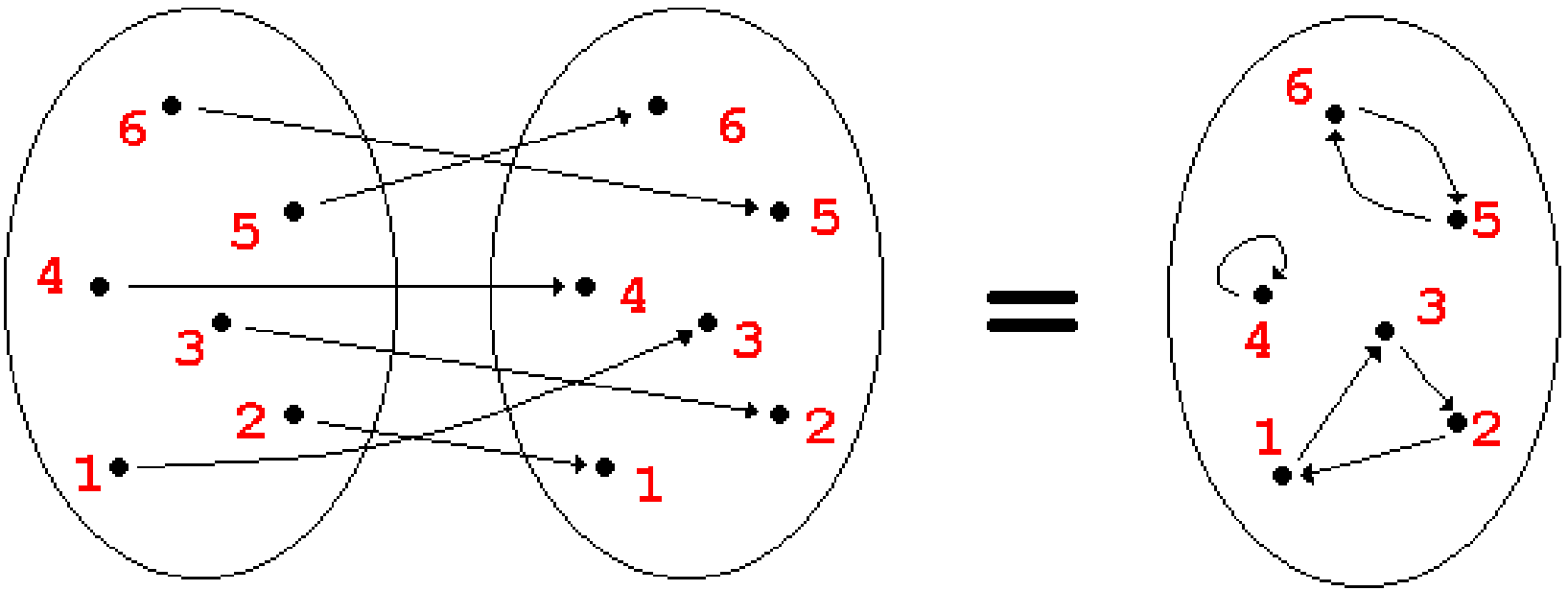
Olkoon permutaatio $\sigma \in S_6$ sellainen, että $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 2$, $\sigma(4) = 4$, $\sigma(5) = 6$ ja $\sigma(6) = 5$. Tätä permutaatiota voidaan nyt merkitä seuraavasti:

$$\begin{aligned}\sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) & \sigma(5) & \sigma(6) \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 6 & 5 \end{pmatrix} \\ &= \big(132\big)\big(4\big)\big(56\big) = \big(132\big)\big(56\big)\,.\end{aligned}$$

(Huomio. Joukko S_6 on kuuden alkion symmetrinen ryhmä. Siihen kuuluu lukujoukon $N = \{1, 2, 3, 4, 5, 6\}$ kaikki mahdolliset permutaatiot, joita on $6!$ kappaletta.)

Permutaatiot

Edellisen kalvon permutaation σ kuva. Huomaa, että jotkin alkiot kuvautuvat kehässä toisilleen, eivätkä vaikuta muihin alkioihin. Näitä sanotaan **sykleiksi**. Permutaatio σ muodostuu siis kolmesta syklistä.



Salakirjoituksista

Salakirjoituksen idea on piilottaa viesti sellaiseen muotoon, ettei sitä voi lukea muut kuin ne, jotka tietävät viestin salaamisessa käytetyn käytetyn. Salausta voidaan ajatella permutaationa ja salauksen purkamista salauspermutaation käänteispermutaationa.

Caesar- salakirjoitus on menetelmä, jossa jokainen kirjain siirtyy kolme pykälää eteenpäin. Näin ollen kirjain A kuvautuu kirjaimelle D, kirjain B kirjaimelle E jne. Toinen vastaava salausmenetelmä on **ROT13**, jossa jokainen kirjain siirtyy 13 pykälää eteenpäin. Tämän menetelmä on käytännöllinen, sillä viesti salataan ja puretaan samalla avaimella. (Englanninkielisissä aakkosissa on 26 kirjainta.)

Kaikki salaukset, joissa yksi kirjain koodataan tietyksi merkiksi, on helppo purkaa frekvenssianalyysimenetelmillä. Tämä perustuu viestin vertaamista käytetyn kielen yleisimpiin kirjaimiin ja kirjainyhdistelmiin, sekä niiden esiintyvyyteen sanan alussa, keskellä ja lopussa.