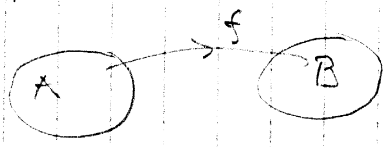
II. JOUKOT JA RELAATIOT

II.1 Kuvauksista (= funktio)



Määr.: Kuvaus f joukosta A joukkoon B liittää jokaiseen alkioon $x \in A$ 1-käs. määrätyn alkion $f(x) \in B$.

Tällöin merk. $f: A \to B$.

A: f:n lähtöjoukko l. määrittelyjoukko

B: f:n maalijoukko

Kun $x \in A$, merk. myös $f: x \mapsto f(x)$; $f(x)$ on x:n kuva (-alkio) f:nä eli f:n arvo x:llä.

Määr.: Jos $f: A \to B$ ja $g: C \to D$ ovat kuvauksia, niin

$$f = g \iff A = C,\ B = D \text{ ja } f(x) = g(x)\ \forall x \in A\ (= C).$$

Esim.: a) Kaava $f(x) = x^2$ $\forall x \in \mathbb{R}$ määrittelee kuvauksen $f: \mathbb{R} \to \mathbb{R}$. Kaava $g(x) = x^2$ $\forall x \in \mathbb{R}$ määr. kuvauksen $g: \mathbb{R} \to \mathbb{R}_+ = \{y \in \mathbb{R} \mid y \geq 0\}$ (sillä $x^2 \geq 0$ $\forall x \in \mathbb{R}$).
Määr. $\Rightarrow$ $f \neq g$ (eri maalijoukko), vaikka $f(x) = g(x)$ $\forall x \in \mathbb{R}$.

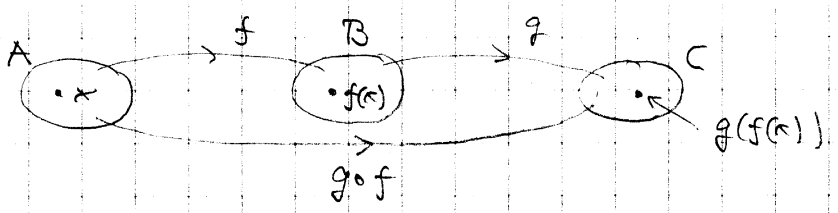
b) Kaava $f(x) = \frac{1}{x}$ ei määr. kuvausta $f: \mathbb{R} \to \mathbb{R}$ ($\frac{1}{x}$ ei ole määritelty, kun $x = 0$).

Huom.: Vain f (eikä $f(x)$) on ao. kuvauksen "nimi". Ei voi sanoa "kuvaus $x^2: \mathbb{R} \to \mathbb{R}$". Voi sanoa "kaavan $x \mapsto x^2$ määrittelemä kuvaus $\mathbb{R} \to \mathbb{R}$".

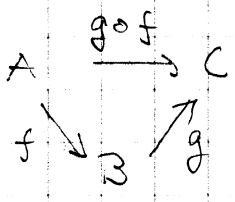
Esim.: Joukon A identtinen kuvaus $id_A: A \to A$ määr. kaavalla $id_A(x) = x$ $\forall x \in A$.
Jos $B \subset A$ on osajoukko, niin kanoninen injektio (l. inkluusio) $i = i_{B,A}: B \to A$ määr. kaavalla $i(x) = x$ $\forall x \in B$ (eri. $i_{A,A} = id_A$).
Myös merk. $i: B \hookrightarrow A$.

Määr.: Ol. $f: A \to B$ ja $g: B \to C$ kuvauksia. Yhdistetty kuvaus $g \circ f: A \to C$ määr. kaavalla

$(g \circ f)(x) = g(f(x)) \quad \forall x \in A$ (joskus merk. $gf = g \circ f$).



Siispä $g \circ f$ on määr. $\Leftrightarrow$ f:n maalij. = g:n lähtöj.. $g \circ f$:n määrittelyä ilmaistaan myös sanomalla, että nuolikaavio



"kommutoi" (ts. alkiot kuvautuvat samoin kumpaakin reittiä myöten).

Esim.: $f, g : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$, $g(x) = x+1 \quad \forall x \in \mathbb{R}$

$\Rightarrow \quad (g \circ f)(x) = g(f(x)) = g(x^2) = x^2 + 1 \quad \forall x \in \mathbb{R}$

$(f \circ g)(x) = f(g(x)) = f(x+1) = (x+1)^2 = x^2 + 2x + 1 \quad \forall x \in \mathbb{R}.$

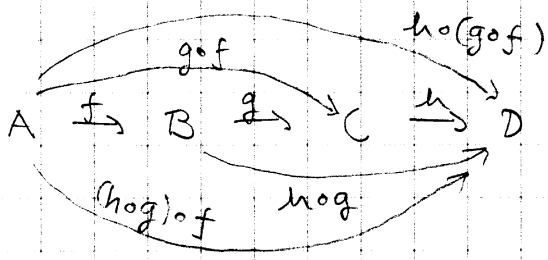
Ent. $(g \circ f)(1) = 2 \neq 4 = (f \circ g)(1)$, joten tässä $g \circ f \neq f \circ g$.

Lause: Ol. $f : A \to B$, $g : B \to C$, $h : C \to D$ kuvauksia. Silloin

a) $h \circ (g \circ f) = (h \circ g) \circ f$

b) $id_B \circ f = f \circ id_A$.

Tod.: a)



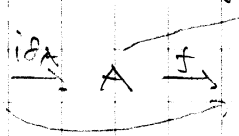
Molemmat kuvauksia $A \to D$.

Riittää siis os., että arvot ovat samat.

$x \in A \Rightarrow (h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x)))$

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

b)



$x \in A \Rightarrow (id_B \circ f)(x) = id_B(f(x)) = f(x)$

$= f(id_A(x)) = (f \circ id_A)(x)$. $\square$

Määr.: Ol. $f: A \to B$ kuvaus ja $A_0 \subset A$, $B_0 \subset B$.
A_0:n kuva (-joukko) kuvauksessa f on

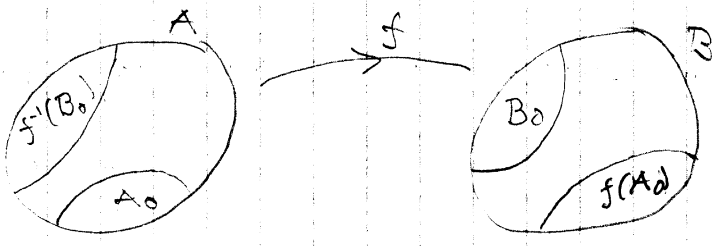
$$f(A_0) = \{ y \in B \mid \exists x \in A_0 \text{ s.e. } y = f(x) \}$$
$$= \{ f(x) \mid x \in A_0 \} \subset B ;$$

B_0:n alkukuva (-joukko) kuvauksessa f on

$$f^{-1}(B_0) = \{ x \in A \mid f(x) \in B_0 \} \subset A .$$

Ehk. $f(A) = \{ f(x) \mid x \in A \}$ on f:n kuva (-joukko) eli arvojoukko (joskus merk. $f(A) = \mathrm{Im}(f)$).

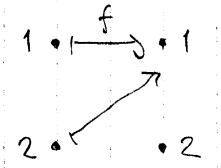
Varoitus: Merkinnässä $f^{-1}(B_0)$ ei ole kysymys "käänteiskuvauksesta".



Lemma: Yo. kiinteässä $A_0 \subset f^{-1}(f(A_0))$ ja $f(f^{-1}(B_0)) \subset B_0$.

Tod.: 1) jos $x \in A_0$, niin kuvan määr. $\Rightarrow f(x) \in f(A_0)$; alkukuvan määr. $\Rightarrow$ tällöin $x \in f^{-1}(f(A_0))$.
2) jos $y \in f(f^{-1}(B_0))$, niin kuvan määr. $\Rightarrow$ $\exists x \in f^{-1}(B_0)$ s.e. $y = f(x)$; $x \in f^{-1}(B_0) \Rightarrow y = f(x) \in B_0$. □

Huom.: Yleensä $A_0 \neq f^{-1}(f(A_0))$, $f(f^{-1}(B_0)) \neq B_0$.
Esim. $f: \{1,2\} \to \{1,2\}$, $f(1) = f(2) = 1$



$$f^{-1}(f(\{1\})) = f^{-1}(\{1\}) = \{1,2\} \neq \{1\}$$
$$f(f^{-1}(\{2\})) = f(\phi) = \phi \neq \{2\} .$$

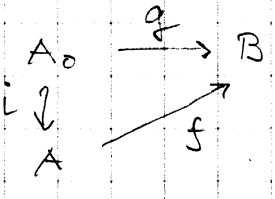
Ol. $f: A \to B$ kuvaus ja $A_0 \subset B$ osajoukko.
Kaava $g(x) = f(x)$ $\forall x \in A_0$ määrittelee kuvauksen

$$g = f \mid A_0 : A_0 \to B ,$$

jota kutsutaan f:n rajoittumaksi joukkoon A_0.

Tällöin f on g:n eräs *laajennus* (l. *jatke*) A:lle.

Olk. $i: A_0 \hookrightarrow A$ kan. injektio. Silloin g:n A:lle laajennus f tarkalleen silloin, kun seur. kaavio kommutoi:



Esim.: $\mathrm{id}_{\mathbb{R}}: \mathbb{R} \to \mathbb{R}$ on kan. injektion $i: \mathbb{R}_+ \hookrightarrow \mathbb{R}$ eräs laajennus. $f: \mathbb{R} \to \mathbb{R}$, $f(x) = |x|$, on i:n eräs toinen laajennus.

Injektiot, surjektiot ja bijektiot

Määr.: Olk. $f: A \to B$ kuvaus.

a) f on *injektio*, jos kaikilla $x_1, x_2 \in A$ pätee $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$ (eli $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$);

b) f on *surjektio*, jos $f(A) = B$;

c) f on *bijektio*, jos se on injektio ja surjektio.

Siispä $f: A \to B$ on

- injektio $\Leftrightarrow$ jokaista $y \in B$ kohti $\exists$ korkeintaan yksi $x \in A$ s.e. $y = f(x)$;
- surjektio $\Leftrightarrow$ jokaista $y \in B$ kohti $\exists$ ainakin yksi $x \in A$ s.e. $y = f(x)$;
- bijektio $\Leftrightarrow$ jokaista $y \in B$ kohti $\exists$ täsmälleen yksi $x \in A$ s.e. $y = f(x)$.

Esim.: $f: \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$ $\forall x \in \mathbb{R}$, ei ole injektio ($f(1) = f(-1)$, vaikka $1 \neq -1$) eikä surjektio ($-1 \notin f(\mathbb{R})$). Sen sijaan $g: \mathbb{R} \to \mathbb{R}_+$, $g(x) = x^2$ $\forall x \in \mathbb{R}$, on surjektio (kunhan $y \in \mathbb{R}_+$ on neliöjuuret $\in \mathbb{R}$). $g|\mathbb{R}_+: \mathbb{R}_+ \to \mathbb{R}_+$ on bijektio.

Esim.: a) $B \subset A \Rightarrow$ inkluusio $i: B \hookrightarrow A$ on injektio ("kanoninen" inj.).

b) $f: A \to B$ mielivaltainen kuvaus $\Rightarrow$ $g: A \to f(A)$, $g(x) = f(x)$ $\forall x \in A$, on surjektio.

Lause: Ol. $f: A \to B$ kuvaus.

a) f on inj. $\iff A_0 = f^{-1}(f(A_0))$ $\forall A_0 \subset A$;

b) f on surj. $\iff f(f^{-1}(B_0)) = B_0$ $\forall B_0 \subset B$.

Tod.: a) $\Rightarrow$. Ol. f inj. ja $A_0 \subset A$. Joka tap: pätee $A_0 \subset f^{-1}(f(A_0))$ (tod. aik.), jäten jää todettavaksi, että $f^{-1}(f(A_0)) \subset A_0$.

$x \in f^{-1}(f(A_0)) \Rightarrow f(x) \in f(A_0) \Rightarrow \exists z \in A_0$ s.e. $f(z) = f(x)$; f inj. $\Rightarrow x = z \in A_0$.

$\Leftarrow$. Ol. $A_0 = f^{-1}(f(A_0))$ $\forall A_0 \subset A$.

V. f inj.

T. Olk. $x_1, x_2 \in A$, $f(x_1) = f(x_2)$.

Ol. $\Rightarrow \{x_1\} = f^{-1}(f(\{x_1\}))$

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

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

$\Rightarrow x_1 = x_2$. □

b) Harj. tehty. □

Olkoon $f: A \to B$ bijektio (usein merk. $f: A \xrightarrow{\sim} B$ tai $f: A \cong B$). Kullakin $y \in B$ on tällöin yhtälöllä $f(x) = y$ 1-kert. ratkaisu $x \in A$. Kun merk. tässä $x = g(y)$, saadaan kuvaus $g: B \to A$.

V. $g \circ f = id_A$, $f \circ g = id_B$.

T. 2) $y \in B \Rightarrow x = g(y) \in A$ on yhtälön $f(x) = y$ ratk.

$\Rightarrow (f \circ g)(y) = f(g(y)) = y$. $\therefore f \circ g = id_B$.

1) $x \in A \Rightarrow f((g \circ f)(x)) = (f \circ (g \circ f))(x) = ((f \circ g) \circ f)(x)$

$\overset{2)}{=} (id_B \circ f)(x) = f(x)$; f inj. $\Rightarrow (g \circ f)(x) = x$.

$\therefore g \circ f = id_A$. □

Yo. kuvaus g on bijektion f <u>käänteiskuvaus</u>, merk. $g = f^{-1}$.

Lemma: $f: A \to B$, $g: B \to A$ kuvauksia,

$g \circ f = id_A$

$\Rightarrow$ f on injektio ja g on surjektio.

Tod.: $x_1, x_2 \in A$, $f(x_1) = f(x_2) \Rightarrow x_1 = id_A(x_1) =$

$= (g \circ f)(x_1) = g(f(x_1)) = g(f(x_2)) = (g \circ f)(x_2) = id_A(x_2) = x_2$.

$\therefore$ f on injektio.

$x \in A \Rightarrow f(x) \in B$ ja $x = id_A(x) = (g \circ f)(x) = g(f(x)) \in g(B)$.

$\therefore$ $g(B) = A$, ts. g on surjektio. $\square$

(Kun $g \circ f = id_A$, sanotaan, että g on f:n (eräs) vasemmanpuoleinen käänt. kuvaus ja f g:n (eräs) oikeanpuoleinen käänt. kuvaus.)

Lause: Kuvaus $f: A \to B$ on bijektio
$\Leftrightarrow$ $\exists$ kuvaus $g: B \to A$ s.e. $g \circ f = id_A$, $f \circ g = id_B$.
Tällöin $g = f^{-1}$.

Tod.: $\Rightarrow$ todettiin jo yllä.

$\Leftarrow$ Ok. annetta $g: B \to A$ s.e. $g \circ f = id_A$, $f \circ g = id_B$.
Lemman nojalla $g \circ f = id_A \Rightarrow f$ inj. (ja g surj.)
$f \circ g = id_B \Rightarrow f$ surj. (ja g inj.).
Siten f on bijektio, ja $\exists$ käänt. kuv. $f^{-1}: B \to A$.
Lisäksi $g = id_A \circ g = (f^{-1} \circ f) \circ g = f^{-1} \circ (f \circ g) = f^{-1} \circ id_A = f^{-1}$. $\square$

Esim.: $\frac{3x-2}{x-2} = 3 + \frac{4}{x-2} \in \mathbb{R} \setminus \{3\}$ $\forall x \in \mathbb{R} \setminus \{2\}$

$\Rightarrow$ kaava $f(x) = \frac{3x-2}{x-2}$ määr. kuvauksen $f: \mathbb{R} \setminus \{2\} \to \mathbb{R} \setminus \{3\}$.

Vastaavasti kaava $g(y) = \frac{2y-2}{y-3} = 2 + \frac{4}{y-3}$

määr. kuvauksen $g: \mathbb{R} \setminus \{3\} \to \mathbb{R} \setminus \{2\}$.

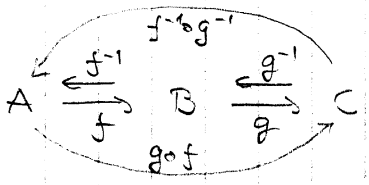
$$(g \circ f)(x) = \frac{2 \cdot \frac{3x-2}{x-2} - 2}{\frac{3x-2}{x-2} - 3} = \frac{6x - 4 - 2x + 4}{3x - 2 - 3 + 6} = x \quad \forall x \in \mathbb{R} \setminus \{2\}$$

$$(f \circ g)(y) = \frac{3 \cdot \frac{2y-2}{y-3} - 2}{\frac{2y-2}{y-3} - 2} = \frac{6y - 6 - 2y + 6}{2y - 2 - 2y + 6} = y \quad \forall y \in \mathbb{R} \setminus \{3\}$$

$\Rightarrow$ $g \circ f = id_{\mathbb{R} \setminus \{2\}}$, $f \circ g = id_{\mathbb{R} \setminus \{3\}}$
$\Rightarrow$ f on bijektio, ja $g = f^{-1}$. $\square$

Lause: $f: A \to B$, $g: B \to C$ bijektioita
$\Rightarrow$ $g \circ f: A \to C$ on bijektio ja

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$ (huomaa järjestys).



Tod.: $(f^{-1}\circ g^{-1})\circ(g\circ f) = f^{-1}\circ(g^{-1}\circ g)\circ f = f^{-1}\circ id_B \circ f$
$= f^{-1}\circ f = id_A$
ja vastaavasti $(g\circ f)\circ(f^{-1}\circ g^{-1}) = id_C$. □

II.2 Luonnolliset luvut; induktio

Määr.: "Luonnolliset luvut" on kolmikko $(\mathbb{N}, s, 0)$, missä $\mathbb{N}$ on joukko, $s: \mathbb{N}\to\mathbb{N}$ on kuvaus ja $0\in\mathbb{N}$ on alkio, kun seuraavat Peanon aksioomat ovat voimassa:

(P1) s on injektio;
(P2) $0 \notin s(\mathbb{N})$;
(P3) jos osajoukko $A\subset\mathbb{N}$ toteuttaa
a) $0\in A$, ja
b) kaikilla $n\in\mathbb{N}$, $n\in A \Rightarrow s(n)\in A$,
niin $A=\mathbb{N}$.

Tämän määr. avulla void. kehittää $\mathbb{N}$:n laskutoimitukset, järjestys jne., ja johtaa kaikki "tutut" ominaisuudet (kehittelemme kohta tätä).

(P3) on ns. induktioaksioomaa. Sen avulla voi os., että jokin $\mathbb{N}$:n osajoukko sisältää kaikki $\mathbb{N}$:n alkiot, tai että jokin ominaisuus on kaikilla $\mathbb{N}$:n alkioilla.

Lause: $\mathbb{N}\setminus s(\mathbb{N}) = \{0\}$ (s = "seuraajakuvaus").

Tod.: (P2) $\Rightarrow \{0\}\subset \mathbb{N}\setminus s(\mathbb{N})$.
Käänteen, merk. $A = \{0\}\cup s(\mathbb{N})$. Tällöin $A\subset\mathbb{N}$ ja
a) $0\in A$, ja b) $n\in A \Rightarrow s(n)\in s(\mathbb{N})\subset A$,
joten (P3) $\Rightarrow A=\mathbb{N}$. Näin ollen
$\mathbb{N}\setminus s(\mathbb{N}) = A\setminus s(\mathbb{N}) = (\{0\}\cup s(\mathbb{N}))\setminus s(\mathbb{N}) \subset \{0\}$. □

Huom.: Merk. $s(0)=1$, $s(1)=2$, ... kuten tav..

On mahdollista konstruoida kaikilla $m,n\in\mathbb{N}$ summa

$m+n \in \mathbb{N}$, jolla määräytyy 1-käsitteisesti kaavoista

$$m+0 = m \quad \forall m \in \mathbb{N}, \text{ ja}$$
$$m+s(n) = s(m+n) \quad \forall m \in \mathbb{N}, \forall n \in \mathbb{N}.$$

Erityisesti tällöin $m+1 = m+s(0) = s(m+0) = s(m) \quad \forall m \in \mathbb{N}$.

Summa toteuttaa seur. laskulait (todist. siv.):

i) $m+n = n+m \quad \forall m, n \in \mathbb{N}$ (vaihdannaisuus)
ii) $k+(m+n) = (k+m)+n \quad \forall k, m, n \in \mathbb{N}$ (liitännäisyys)
iii) $m+0 = m \quad \forall m \in \mathbb{N}$ (0 on neutraalialkio).

Todistamme vielä seur. 2 ominaisuutta: kaikilla $k, m, n \in \mathbb{N}$ pätee

iv) $k+n = m+n \Rightarrow k = m$ (supistussääntö)
v) $m+n = 0 \Rightarrow m = n = 0$.

Tod.: iv) Ol. $k, m \in \mathbb{N}$, $k \neq m$.
V. Kaikilla $n \in \mathbb{N}$ on $k+n \neq m+n$.
T. Merk. $A = \{n \in \mathbb{N} \mid k+n \neq m+n\}$.
a) $0 \in A$, sillä $k+0 = k \neq m = m+0$.
b) Ol. $n \in A$, ts. $k+n \neq m+n$. Silloin
$k+s(n) = s(k+n) \neq s(m+n)$ ($P1 \Rightarrow s$ inj.!)
$= m+s(n)$,
ts. $s(n) \in A$. ($P3$) $\Rightarrow A = \mathbb{N}$. □

v) Ol. $m, n \in \mathbb{N}$, $m+n = 0$. Vastaol.: $n \neq 0$.
$\mathbb{N} \setminus s(\mathbb{N}) = \{0\} \Rightarrow n \in s(\mathbb{N}) \Rightarrow n = s(k)$ eräällä $k \in \mathbb{N}$.
Tällöin $m+n = m+s(k) = s(m+k) \in s(\mathbb{N})$
$\Rightarrow m+n \neq 0$, RR. Siis täytyy olla $n = 0$,
ja edelleen $m = m+0 = m+n = 0$. □

Myös on mahd. konstruoida kaikilla $m, n \in \mathbb{N}$ tulo $m \cdot n \in \mathbb{N}$ s.e.

$$m \cdot 0 = 0 \quad \forall m \in \mathbb{N}, \text{ ja}$$
$$m \cdot s(n) = mn + m \quad \forall m \in \mathbb{N}, \forall n \in \mathbb{N}.$$

Seuraavat laskulait ovat voimassa:

i) $mn = nm$ $\forall m,n \in \mathbb{N}$ (vaihdann.)
ii) $k(mn) = (km)n$ $\forall k,m,n \in \mathbb{N}$ (liitänn.)
iii) $m \cdot 1 = m$ $\forall m \in \mathbb{N}$ (1 on neutr. alkio)
iv) $k(m+n) = km + kn$ $\forall k,m,n \in \mathbb{N}$ (osittelulaki).

Lisäksi pätee nmm. tulon nollasääntö: jos $m,n \in \mathbb{N}$, niin

v) $mn = 0 \Rightarrow m = 0$ tai $n = 0$.

Tod.: v) Vastaol.: $m \neq 0$ ja $n \neq 0$. $\mathbb{N} \setminus \{0\} = s(\mathbb{N})$
$\Rightarrow \exists m', n' \in \mathbb{N}$ s.e. $m = s(m') = m'+1$, $n = s(n') =$
$= n'+1 \Rightarrow mn = (m'+1)\cdot(n'+1) =$
$= (m'+1)n' + (m'+1)\cdot 1 = m'n' + n' + m' + 1$ (i) – iv))
$= s(m'n' + n' + m') \in s(\mathbb{N}) = \mathbb{N} \setminus \{0\} \Rightarrow mn \neq 0$. □

$\mathbb{N}$:n järjestys (so. se, että $m \in \mathbb{N}$ on "korkeintaan yhtä suuri" kuin $n \in \mathbb{N}$) määr. yhtäpitävästi asettamalla:

$$m \leq n \iff \exists p \in \mathbb{N} \text{ s.e. } n = m + p.$$

Kaikilla $k,m,n \in \mathbb{N}$ pätee:

i) $n \leq n$ (refleksiivisyys)
ii) $m \leq n$ ja $n \leq m \Rightarrow m = n$ (antisymmetrisyys)
iii) $k \leq m$ ja $m \leq n \Rightarrow k \leq n$ (transitiivisuus).

Tod.: i) $n = n + 0$.
ii) $n = m + p$, $m = n + q$, $p,q \in \mathbb{N} \Rightarrow$
$n + 0 = n = m + p = (n+q) + p = n + (q+p)$
$\Rightarrow q + p = 0$ (supistussääntö) $\Rightarrow q = p = 0$
$\Rightarrow n = m + 0 = m$.
iii) $m = k + p$, $n = m + q \Rightarrow n = (k+p) + q = k + (p+q)$. □

Jos $m \leq n$ ja $m \neq n$, merk. $m < n$. Tällöin
$n = m + p$ jollakin $p \in \mathbb{N}$, ja $n = m + p \neq m$
$\Rightarrow p \neq 0$ (jos olisi $p = 0$, niin $n = m + 0 = m$, RR).
Käänteisesti, $p \neq 0 \Rightarrow m + p \neq m$ (sillä $m + p = m = m + 0$
$\Rightarrow p = 0$ (sup. sääntö)). Siispä

$$m < n \iff \exists p \in \mathbb{N}_+ \text{ s.e. } n = m + p,$$

missä $\mathbb{N}_+ = \mathbb{N} \setminus \{0\} = s(\mathbb{N}) = \{p \in \mathbb{N} \mid p > 0\}$.

Huom.: jos $m \leq n$, niin luku $p \in \mathbb{N}$ s.e. $n = m + p$ (n:n ja m:n "erotus") on 1-käs. määrätty (sillä $m + p = m + p' \Rightarrow p = p'$).

Lemma: $m < n \Rightarrow m + 1 \leq n$.

Tod.: $m < n \Rightarrow n = m + p$, $p \in \mathbb{N}_+ = s(\mathbb{N})$; $p = q + 1$ eräälle $q \in \mathbb{N} \Rightarrow n = m + p = m + (q + 1) = m + (1 + q) = (m + 1) + q \Rightarrow m + 1 \leq n$. □

Tästä seuraa, että m:n ja $(m+1)$:n välissä ei ole yhtään luonn. lukua.

Lause: Osajoukossa $\emptyset \neq A \subset \mathbb{N}$ on pienin alkio, ts. sellainen $a_0 \in A$, että $x \geq a_0 \ \forall x \in A$.

Tod.: Merk. $B = \{b \in \mathbb{N} \mid b \leq x \ \forall x \in A\} \subset \mathbb{N}$. $0 \in B$, mutta $B \neq \mathbb{N}$ ($A \neq \emptyset \Rightarrow$ väl. val. $a \in A$; tällöin ei ole $a + 1 \leq a$, joten $a + 1 \notin B$). Siten implikaatio $b \in B \Rightarrow b + 1 \in B$ ei päde jokaisella $b \in B$ (muuten (P3) $\Rightarrow B = \mathbb{N}$), vaan $\exists a_0 \in B$ s.e. $a_0 + 1 \notin B$. $a_0 \in B \Rightarrow a_0 \leq x \ \forall x \in A$. Riittää siis tod.

V. $a_0 \in A$.

T. Vastaol.: $a_0 \notin A$. Tällöin $a_0 < x \ \forall x \in A$. Lemma $\Rightarrow a_0 + 1 \leq x \ \forall x \in A \Rightarrow a_0 + 1 \in B$, RR. □

Seuraus: $m, n \in \mathbb{N} \Rightarrow m \leq n$ tai $n \leq m$.

Tod.: joukossa $\{m, n\}$ on pienin alkio. □

Järjestys ja laskutoimitukset ovat yhteensopivat:

$$m < n, \ k \in \mathbb{N} \Rightarrow m + k < n + k;$$
$$m < n, \ k \in \mathbb{N}_+ \Rightarrow km < kn.$$

(Tod.: $m < n \Rightarrow n = m + p$, $p \in \mathbb{N}_+$. Kun $k \in \mathbb{N}$, on silloin $n + k = (m + p) + k = (m + k) + p$,

jolloin $m+k < n+p$. Jos $k \in \mathbb{N}_+$, on
$kn = k(m+p) = km + kp$, missä $kp \in \mathbb{N}_+$, joten
$km < kn$. □)

Induktiotodistukset: Halutaan osoittaa, että tietty n:stä riippuva väite $P(n)$ on tosi kaikilla $n \in \mathbb{N}$, ts. $\{n \in \mathbb{N} \mid P(n) \text{ on tosi}\} = \mathbb{N}$. (P3) $\Rightarrow$ riittää osoittaa, että

a) $P(0)$ on tosi, ja
b) jos $P(n)$ on tosi jollakin $n \in \mathbb{N}$, niin myös $P(n+1)$ on tosi.

Olk. $n_0 \in \mathbb{N}$. Jos hal. tod., että väite $P(n)$ on tosi kaikilla $n \in \mathbb{N}$, $n \geq n_0$, riittää tod., että

a) $P(n_0)$ on tosi, ja
b) jos $P(n)$ on tosi jollakin $n \geq n_0$, niin myös $P(n+1)$ on tosi.

(Tällöin nim. (P3) $\Rightarrow$
$\{n \in \mathbb{N} \mid n < n_0 \text{ tai } P(n) \text{ on tosi}\} = \mathbb{N}$.)

Esim.: Olk. $p \in \mathbb{N}$, $p \geq 2$
V. $p^n > n \quad \forall n \in \mathbb{N}_+$
T. Kun $n \in \mathbb{N}_+$, olk. $P(n)$ väite "$p^n > n$".
a) $P(1)$ on tosi, sillä $p^1 = p \geq 2 > 1$.
b) Ind.oletus: $n \in \mathbb{N}_+$ ja $P(n)$ on tosi, ts. $p^n > n$.
Silloin $p^{n+1} = p^n \cdot p > n \cdot p \geq n \cdot 2 = n + n$
$\geq n + 1$, joten $P(n+1)$ on tosi. □