III.0 Laskutoimitukset ja monoidit

Määr.: Joukon A (sisäinen) laskutoimitus on kuvaus $T : A \times A \to A$.

Yleensä merkitään $aTb = T(a,b) \in A$, kun $a, b \in A$.

Esim.: Hyödyllisiä laskutoimituksia ovat mm.:

a) yhteenlasku $(a,b) \mapsto a+b$ joukoissa $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Z}_n$ $(n \in \mathbb{N}_+)$, $\mathbb{Q}$ ja $\mathbb{R}$.

b) kertolasku $(a,b) \mapsto a \cdot b$ ao. kohdan joukoissa.

c) Operaatiot $(A,B) \mapsto A \cup B$ ja $(A,B) \mapsto A \cap B$ joukossa $\mathcal{P}(X)$, kun X on annettu joukko.

d) Kuvausten yhdistäminen $(f,g) \mapsto f \circ g$ joukossa $X^X = \{f \mid f : X \to X \text{ kuvaus}\}$, kun X ann. joukko.

e) Merk. $$\mathcal{M}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a,b,c,d \in \mathbb{R} \right\}$$
$\mathbb{R}$-kertoimisten (2×2)-matriisien joukko. $\mathcal{M}_2(\mathbb{R})$:ssä määr. yhteen- ja kertolasku kaavoilla
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix}$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}.$$

Määr.: Olkoon T joukon A laskutoimitus.

a) T on liitännäinen l. assosiatiivinen, jos kaikilla $a,b,c \in A$ on $aT(bTc) = (aTb)Tc$.

b) T on vaihdannainen l. kommutatiivinen, jos kaikilla $a,b \in A$ on $aTb = bTa$.

c) Alkio $e \in A$ on T:n neutraalialkio, jos kaikilla $a \in A$ on $eTa = a = aTe$.

Huom.: A:n laskutoimituksella T on korkeintaan yksi neutr. alkio.

Tod.: Ol. $e, e' \in A$ ja $eTa = aTe = a = e'Ta = aTe'$ $\forall a \in A$. Silloin
$$\begin{aligned} e &= eTe' && (aTe' = a,\ a = e) \\ &= e' && (eTa = a,\ a = e'). \quad \square \end{aligned}$$

Jos A:n laskutoim. T on liitännäinen ja $a_1, a_2, a_3 \in A$, void. merkitä

$$a_1 T a_2 T a_3 = (a_1 T a_2) T a_3 = a_1 T (a_2 T a_3).$$

Pitemmät "tulot" määr. rekursiivisesti:

$$a_1 T a_2 T \ldots T a_n = (a_1 T a_2 T \ldots T a_{n-1}) T a_n,$$

kun $a_1, \ldots, a_n \in A$, $n \geq 4$. Liitänn. $\Rightarrow$ saadaan sama tulos, vaikka tekijät ryhmiteltäisiin toisin kuin (kunhan järj. säilyy; induktiotod. siv.).

Esim.: $a_1 T (a_2 T (a_3 T a_4)) = (a_1 T a_2) T (a_3 T a_4)$
$= ((a_1 T a_2) T a_3) T a_4 \quad (= a_1 T a_2 T a_3 T a_4)$,
kun T liitännäinen.

Määr.: Joukko M varustettuna tietyllä laskutoimituksella T (l. pari (M, T)) on monoidi, jos T on liitännäinen ja sillä on neutr. alkio. Jos lisäksi T on vaihdannainen, (M, T) on kommutatiivinen monoidi.

Esim.: a) $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}_n, +)$ $(n \in \mathbb{N}_+)$, $(\mathbb{Q}, +)$ ja $(\mathbb{R}, +)$ ovat komm. monoideja (neutr. alkio $= 0$).

b) $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Z}_n, \cdot)$ $(n \in \mathbb{N}_+)$, $(\mathbb{Q}, \cdot)$ ja $(\mathbb{R}, \cdot)$ ovat myös komm. monoideja (neutr. alkio $= 1$).

c) X joukko $\Rightarrow$ $(\mathcal{P}(X), \cup)$ on komm. monoidi (neutr. alkio $= \emptyset$), samoin $(\mathcal{P}(X), \cap)$ (neutr. alkio $= X$).

d) X joukko $\Rightarrow$ $(X^X, \circ)$ on monoidi, neutr. alkiona id_X. Tämä ei ole komm., jos $\# X \geq 2$:
Ol. $x_1, x_2 \in X$, $x_1 \neq x_2$. Määr. $f, g : X \to X$ s.e. $f(x) = g(x) = x \quad \forall x \in X \setminus \{x_1, x_2\}$ ja $f(x_1) = f(x_2) = x_1$, $g(x_1) = g(x_2) = x_2$. Silloin $(f \circ g)(x_1) = x_1$, $(g \circ f)(x_1) = x_2$, joten $f \circ g \neq g \circ f$.

e) $(\mathcal{M}_2(\mathbb{R}), +)$ on komm. monoidi, neutr. alkiona $O_2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$; $(\mathcal{M}_2(\mathbb{R}), \cdot)$ on monoidi, neutr. alkiona $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (ks. Lin. alg. I). $(\mathcal{M}_2(\mathbb{R}), \cdot)$ ei ole komm., sillä esim.

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

f) $(n\mathbb{Z}, +)$ on komm. monoidi ($n \in \mathbb{N}_+$). $(n\mathbb{Z}, \cdot)$ ei ole monoidi, kun $n \geq 2$ (ei neutr. alkiota).

Mieliv. monoidissakin laskutoimitusta merk. usein $(a, b) \mapsto a \cdot b$, jolloin puhutaan <u>multiplikatiivisesta</u> monoidista. Multipl. monoidin M neutr. alkiota merk. yleensä $1 = 1_M$.

Erit. komm. monoidin laskutoimitusta merk. usein $(a, b) \mapsto a + b$, jolloin puh. <u>additiivisesta</u> monoidista. Addit. monoidin M neutr. alkiota merk. yleensä $0 = 0_M$.

Olk. M multipl. monoidi. Alkioiden $a_1, \ldots, a_n \in M$ tuloa merk.:

$$a_1 a_2 \cdot \ldots \cdot a_n = \prod_{k=1}^{n} a_k .$$

Jos $a_1 = \ldots = a_n = a \in M$, kyseessä ovat a:n <u>potenssit</u> a^n; rekursiivinen määr.

$$a^0 = 1_M, \quad a^{n+1} = a^n \cdot a \quad \forall n \in \mathbb{N}.$$

<u>Lause</u>: $\quad a^{m+n} = a^m \cdot a^n, \quad a^{mn} = (a^m)^n \quad \forall m, n \in \mathbb{N}.$

Tod.: Induktio n:n suhteen ($m \in \mathbb{N}$ kiinteä).

a) $a^{m+0} = a^m = a^m \cdot 1_M = a^m \cdot a^0$;
$a^{m \cdot 0} = a^0 = 1_M = (a^m)^0$.

b) $a^{m+(n+1)} = a^{(m+n)+1} = a^{m+n} \cdot a \overset{\text{ind.ol.}}{=} (a^m \cdot a^n) \cdot a$
$= a^m \cdot (a^n \cdot a) = a^m \cdot a^{n+1}$;
$a^{m(n+1)} = a^{mn+m} = a^{mn} \cdot a^m \overset{\text{ind.ol.}}{=} (a^m)^n \cdot a^m$
$= (a^m)^{n+1}$. $\square$

Addit. monoidissa M merk. $a_1 + a_2 + \ldots + a_n = \sum_{k=1}^{n} a_k$. Potenssien sijasta puhutaan alkion $a \in M$ <u>monikerroista</u> na:

$$0 \cdot a = 0_M, \quad (n+1) \cdot a = na + a \quad \forall n \in \mathbb{N}.$$
($\uparrow$ $0 \in \mathbb{N}$)

Ed. lauseen kaavat saavat tässä muodon

$$(m+n)a = ma + na, \quad (mn)a = m(na) \quad \forall m, n \in \mathbb{N}.$$

Määr.: (Multipl.) monoidin M alkio $a \in M$ on kääntyvä, jos on olem. sellainen $b \in M$, että $ab = 1_M = ba$. Tällöin b:tä kutsutaan a:n käänteisalkioksi.

Huom.: Monoidin alkiolla on korkeintaan yksi käänteis-alkio.

Tod.: Ol. $b, b' \in M$, $ab = 1_M = ba$ ja $ab' = 1_M = b'a$
$\Rightarrow b = b \cdot 1_M = b \cdot (ab') = (ba) \cdot b' = 1_M \cdot b' = b'$. □

Kääntyvän alkion $a \in M$ käänt. alkio b on siis a:n 1-käs. määräämä; merk. $b = a^{-1}$ (multipl. monoidissa). Jos M on addit. monoidi, puhutaan mieluummin a:n vasta-alkiosta, merk. $-a$.

Kun M on (multipl.) monoidi, merk. $M^* = \{a \in M \mid a \text{ on kääntyvä}\}$.

Lemma: $a, b \in M^* \Rightarrow ab \in M^*$ ja $(ab)^{-1} = b^{-1}a^{-1}$.

Tod.: $(ab) \cdot (b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a \cdot 1_M \cdot a^{-1} = aa^{-1} = 1_M$,
$(b^{-1}a^{-1}) \cdot (ab) = b^{-1}(a^{-1}a)b = b^{-1} \cdot 1_M \cdot b = b^{-1}b = 1_M$. □

Määr.: Monoidi, jonka jokainen alkio on kääntyvä, on ryhmä. Ryhmä, jonka laskutoimitus on vaihdannainen, on kommutatiivinen l. Abelin ryhmä.

Joukko G varustettuna laskutoimituksellaan $(a, b) \mapsto ab$ on siis ryhmä $\Leftrightarrow$

i) $a(bc) = (ab)c \quad \forall a, b, c \in G$
ii) $\exists 1_G \in G$ s.e. $1_G \cdot a = a = a \cdot 1_G \quad \forall a \in G$
iii) $\forall a \in G \; \exists b \in G$ s.e. $ab = 1_G = ba$.

Lause: M (multipl.) monoidi $\Rightarrow$ M^* on ryhmä M:n laskutoimituksen suhteen.

Tod.: Le $\Rightarrow$ $ab \in M^*$, kun $a, b \in M^*$ $\Rightarrow$ kaava $(a, b) \mapsto ab$ määr. laskutoimituksen M^*:ssä.

$a(bc) = (ab)c \quad \forall a,b,c \in M \Rightarrow a(bc) = (ab)c \quad \forall a,b,c \in M^*$.

$1_M \in M^* \quad (1_M^{-1} = 1_M)$; $\quad 1_M \cdot a = a = a \cdot 1_M \quad \forall a \in M$

$\Rightarrow 1_M \cdot a = a = a \cdot 1_M \quad \forall a \in M^*$.

$a \in M^* \Rightarrow \exists a^{-1} \in M$, ja $a^{-1} \in M^* \quad ((a^{-1})^{-1} = a)$

$\Rightarrow a^{-1}$ kelpaa a:n käänt. alkioksi M^*:ssä. $\square$

Esim.: a) Seuraavat addit. komm. monoidit ovat Abelin ryhmiä (kaikilla alkioilla vasta-alkiot):
$(\mathbb{Z}, +)$, $(\mathbb{Z}_n, +)$ $(n \in \mathbb{N}_+)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$.
Monoidissa $(\mathbb{N}, +)$ vain 0:lla on vasta-alkio.

b) Multipl. komm. monoidien $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$ ja $(\mathbb{R}, \cdot)$ kääntyvät alkiot muod. Abelin ryhmät $(\{1\}, \cdot)$, $(\{1, -1\}, \cdot)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$ ja $(\mathbb{R} \setminus \{0\}, \cdot)$.

c) Merk. $\mathbb{Z}_n^* =$ monoidin $(\mathbb{Z}_n, \cdot)$ käänt. alkioiden joukko $(n \in \mathbb{N}_+)$, jolloin $[a]_n \in \mathbb{Z}_n^* \Leftrightarrow \mathrm{syt}(a, n) = 1$ (tod. aik.). Siis $(\mathbb{Z}_n^*, \cdot)$ on ryhmä.
$\mathbb{Z}_n^* \subset \mathbb{Z}_n$ (joukkona), $\#\mathbb{Z}_n = n < \infty \Rightarrow \mathbb{Z}_n^*$ on äärellinen. Merk.

$$\varphi(n) = \#\mathbb{Z}_n^* = \#\{a \in \mathbb{Z} \mid 0 \le a \le n-1,\ \mathrm{syt}(a,n) = 1\}.$$

$\varphi : \mathbb{N}_+ \to \mathbb{N}$ on ns. <u>Eulerin φ-funktio</u>. Jos p on alkuluku, niin $\mathbb{Z}_p^* = \{[1]_p, [2]_p, \ldots, [p-1]_p\}$
$\Rightarrow \varphi(p) = p - 1$.

d) Monoidissa $(\mathcal{P}(X), \cup)$ vain $\emptyset$ on kääntyvä;
" $(\mathcal{P}(X), \cap)$ " X — " —.

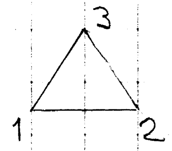
e) Ol. X joukko. Kuvaus $f : X \to X$ (eli $f \in X^X$) on kääntyvä monoidissa $(X^X, \circ)$ $\Leftrightarrow \exists\, g : X \to X$ s.e. $g \circ f = \mathrm{id}_X = f \circ g$ $\Leftrightarrow$ f on bijektio.
Merk. $S_X = \{f \mid f$ on bijektio $X \to X\}$
$\Rightarrow (S_X, \circ)$ on ryhmä, joukon X <u>permutaatioryhmä</u>.
Jos X on äärell., $\#X = n$, $X = \{x_1, x_2, \ldots, x_n\}$ (ts. on valittu jokin bij. $J_n \xrightarrow{\sim} X$), niin jokainen $f \in S_X$ voidaan esittää muodossa

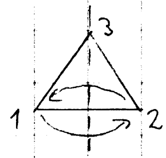
$$\begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ f(x_1) & f(x_2) & \cdots & f(x_n) \end{pmatrix};$$

tässä myös 2. rivillä esiintyy jok. X:n alkio täsm. yhden kerran.

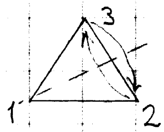
f) Erik. tap. edellisestä: jos $X = J_n = \{1,2,\dots,n\}$ ($n \in \mathbb{N}_+$), merk. $S_X = S_n$. Siis $(S_n, \circ)$ on ryhmä, ns. n:s <u>symmetrinen ryhmä</u>.

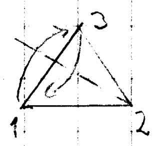
S_3:n alkiot geometrisine tulkintoineen (tasasiv. kolmion symmetriat):

$id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ 

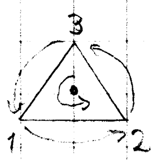
; $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ 

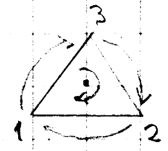
(peilaus) ;

$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ 

(peil.) ; $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ 

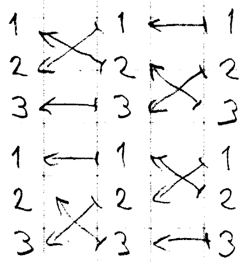
(peil.) ;

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ 

(kierto) ; $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ 

(kierto).

Tässä
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$
$$\neq$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$



Siten S_3 ei ole kommutatiivinen. Samoin S_X ei ole komm., kun $\# X \geq 3$.

g) Merk. $GL_2(\mathbb{R}) = \{ A \in M_2(\mathbb{R}) \mid A$ kääntyvä $(M_2(\mathbb{R}), \cdot)$:ssä $\}$
$\Rightarrow$ $(GL_2(\mathbb{R}), \cdot)$ on ryhmä (ei-komm.).

$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R}) \iff \exists$ käänt. matr. $A^{-1} \in M_2(\mathbb{R})$ s.e. $AA^{-1} = A^{-1}A = I_2$

$\iff \det(A) = ad - bc \neq 0$;

tällöin $$A^{-1} = \frac{1}{\det(A)} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Jos ryhmä G (t. ko. joukko) on äärellinen, san., että $\# G \in \mathbb{N}_+$ (huom.: ainakin $1_G \in G$!) on ryhmän G <u>kertaluku</u>. Myös merk. $\# G = |G|$.

<u>Esim.</u>: $|\mathbb{Z}_n| = n \in \mathbb{N}_+$ (addit. ryhmä) ;
$|\mathbb{Z}_n^*| = \varphi(n)$ (multipl. —"—).