V.1 Renkaan määritelmä ja esimerkkejä

Määr.: Joukko R varustettuna kahdella laskutoimituksella $+$ ("yhteenlasku") ja $\cdot$ ("kertolasku") (eli kolmikko $(R,+,\cdot)$) on **rengas**, jos

i) $(R,+)$ on Abelin ryhmä,
ii) $(R,\cdot)$ on monoidi, ja
iii) $a(b+c) = ab+ac$, $(a+b)c = ac+bc$ $\forall a,b,c \in R$
(osittelulait l. distributiivisuus).

Jos lisäksi kertolasku on vaihdannainen, kyseessä on **kommutatiivinen rengas**.

Renkaan R laskutoimitusten on siis toteutettava seur. aksioomat:

- $a+(b+c) = (a+b)+c$, $a(bc) = (ab)c$ $\forall a,b,c \in R$
- $a+b = b+a$ $\forall a,b \in R$
- $\exists\, 0_R, 1_R \in R$ s.e. $a+0_R = a$ $(= 0_R+a)$ ja $1_R \cdot a = a = a \cdot 1_R$ $\forall a \in R$
- jokaisella $a \in R$ on vastaalkio $-a \in R$ s.e. $a+(-a) = 0_R$ $(= (-a)+a)$
- $a(b+c) = ab+ac$, $(a+b)c = ac+bc$ $\forall a,b,c \in R$.

Komm. renkaassa R lisäksi $ab = ba$ $\forall a,b \in R$.

Esim. 0: Yksiö $\{a\}$ on rengas, kun määr. $a+a=a$ ja $a \cdot a = a$.

Esim. 1: Seuraavat ovat komm. renkaita:
$(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$.
Rengas $(\mathbb{Q},+,\cdot)$ konstruoidaan $(\mathbb{Z},+,\cdot)$:stä käyttäen luv. VI.

Esim. 4: $(\mathbb{Z}_n,+,\cdot)$ on komm. rengas (jäännösluokkarengas).

Esim. 2: $(M_2(\mathbb{R}),+,\cdot)$ on (ei-komm.) rengas.

Esim. 5: Boolen renkaat. Ol. X joukko. Tällöin

$(\mathcal{P}(X), \Delta, \cap)$ on kommut. rengas, kun määr. $A \Delta B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$ ("symmetrinen erotus")
$\forall A, B \subset X$. Nolla-alkio $= \emptyset$, ykkösalkio $= X$.

Esim.: Tulorenkaat. Ol. R ja R' renkaita.
Kart. tulosta $R \times R'$ tulee rengas, kun määr.

$$(a,a') + (b,b') = (a+b, a'+b')$$
$$(a,a') \cdot (b,b') = (ab, a'b') \qquad (a,b \in R;\ a',b' \in R').$$

(Lause III 4 $\Rightarrow$ $(R \times R', +)$ on Ab. ryhmä; vastaavasti $(R \times R', \cdot)$ on monoidi. Osittelulait:
$(a,a') \cdot ((b,b') + (c,c')) = (a,a') \cdot (b+c, b'+c')$
$= (a(b+c), a'(b'+c')) = (ab+ac, a'b'+a'c')$
$= (ab, a'b') + (ac, a'c') = (a,a') \cdot (b,b') + (a,a') \cdot (c,c')$;
toinen vastaavasti.)
Tässä R:n ja R':n tulorenkaassa on erityisesti
$0_{R \times R'} = (0_R, 0_{R'})$, $-(a,a') = (-a,-a')$ ja $1_{R \times R'} = (1_R, 1_{R'})$.

Esim. 3: Funktiorenkaat. Ol. $X \neq \emptyset$ joukko ja R rengas. Joukosta

$$R^X = \{f \mid f \text{ on kuvaus } X \to R\}$$

tulee rengas, kun määr. alkioiden $f, g \in R^X$ summa $f+g$ ja tulo $f \cdot g$ "pisteittäin":

$$(f+g)(x) = f(x) + g(x) \quad \forall x \in X$$
$$(f \cdot g)(x) = f(x) \cdot g(x) \quad -\text{"}-$$

(harj.teht.). R^X:n nolla-alkio on vakiokuvaus $\bar{0} : x \mapsto 0_R$, ykkösalkio on vakiokuvaus $\bar{1} : x \mapsto 1_R$, ja $(-f)(x) = -f(x)$ $\forall x \in X$, kun $f \in R^X$.

Esim. 6: Endomorfismirenkaat. Olkoon A additiivinen Abelin ryhmä. Tark. joukkoa

$$\mathrm{End}(A) = \{f \mid f : A \to A \text{ on ryhmähomom.}\}$$

(homom. $A \to A$ = A:n endomorfismi). Kun $f, g \in \mathrm{End}(A)$, määr. $f+g : A \to A$ s.e. $(f+g)(a) = f(a) + g(a)$ $\forall a \in A$.
Tällöin $f+g \in \mathrm{End}(A)$, sillä

$$(f+g)(a+b) = f(a+b)+g(a+b) = f(a)+f(b)+g(a)+g(b)$$
$$= f(a)+g(a)+f(b)+g(b) \quad (+ \text{ kommut.!})$$
$$= (f+g)(a)+(f+g)(b) \quad \forall a,b \in A.$$

Siis laskutoim. $+ : \mathrm{End}(A) : ssa$. Lisäksi Lause III.10(i) $\Rightarrow f \circ g \in \mathrm{End}(A)$, kun $f, g \in \mathrm{End}(A)$, joten myös $\circ$ on laskutoim. $\mathrm{End}(A) : ssa$.

V. $(\mathrm{End}(A), +, \circ)$ on rengas.

T. Kuten Esim. 6 : ssa, $(\mathrm{End}(A), +)$ on Abelin ryhmä. Edelleen selvästi $\circ$ on liitännäinen ja id_A on yksikköalkio. Osittelulait: Kun $f, g, h \in \mathrm{End}(A)$, niin kaikilla $a \in A$ on

$$[(f+g)\circ h](a) = (f+g)(h(a)) = f(h(a))+g(h(a)) = [f\circ h + g\circ h](a),$$
$$[f\circ(g+h)](a) = f((g+h)(a)) = f(g(a)+h(a))$$
$$= f(g(a))+f(h(a)) \quad (f \text{ homom.!})$$
$$= [f\circ g + f\circ h](a),$$

joten $(f+g)\circ h = f\circ h + g\circ h$ ja $f\circ(g+h) = f\circ g + f\circ h$. □

Määr.: Renkaan R alkio u on *käänteyvä* l. *yksikkö*, jos u on käänteyvä monoidissa $(R, \cdot)$, ts. $\exists u^{-1} \in R$ s.e. $uu^{-1} = 1_R = u^{-1}u$. Lisäksi merk. $R^* = \{u \in R \mid u \text{ on käänteyvä}\}$.

Lause 1: $(R^*, \cdot)$ on ryhmä, renkaan R *yksikköryhmä* (tod. ait.). □

Esim. 7: Aiemmin on tutkittu yksikköryhmiä $\mathbb{Z}^* = \{1, -1\}$, $\mathbb{Z}_n^*$ $(n \in \mathbb{N}_+)$, $\mathbb{Q}^* = \mathbb{Q}\setminus\{0\}$, $\mathbb{R}^* = \mathbb{R}\setminus\{0\}$, $\mathbb{C}^* = \mathbb{C}\setminus\{0\}$ ja $M_2(\mathbb{R})^* = GL_2(\mathbb{R})$.

Esim.: R, R' renkaita $\Rightarrow (R\times R')^* = R^* \times R'^*$. (Olk. $(a,a') \in R\times R'$. Silloin $\exists (b,b') \in R\times R'$ s.e. $(a,a')\cdot(b,b') = (1_R, 1_{R'}) = (b,b')\cdot(a,a') \Leftrightarrow \exists b \in R, b' \in R'$ s.e. $ab = 1_R = ba$ ja $a'b' = 1_{R'} = b'a'$.)

Esim.: $\Sigma \neq \emptyset$ joukko, R rengas $\Rightarrow$
$$(R^\Sigma)^* = (R^*)^\Sigma = \{f \mid f : \Sigma \to R^* \text{ kuvaus}\}.$$

II. 2 Renkaan aritmetiikkaa

Olkoon $(R,+,\cdot)$ rengas. Abelin ryhmässä $(R,+)$ ja monoidissa $(R,\cdot)$ pätevät mm. seur. laskusäännöt:

- $-(-a) = a$, $-(a+b) = (-a)+(-b)$, $-0_R = 0_R$ $(a,b \in R)$
- R:n alkioiden monikerroille ryhmässä $(R,+)$ pätee
  $(m+n)a = ma+na$, $(mn)a = m(na)$,
  $m(a+b) = ma+mb$ $\forall a,b \in R$, $\forall m,n \in \mathbb{Z}$
- alkion $a \in R$ potensseille monoidissa $(R,\cdot)$ pätee
  $a^{m+n} = a^m \cdot a^n$, $a^{mn} = (a^m)^n$ $\forall m,n \in \mathbb{N}$.

Kun $a,b \in R$, merk. $a-b = a+(-b)$; $a-b$ on se 1-käs. alkio $x \in R$, jolla $x+b = a$.

Osittelulakien avulla saadaan muita laskusääntöjä. Esim. osittelulait + induktio $\Rightarrow$

$$a(b_1+\ldots+b_n) = ab_1+\ldots+ab_n,$$
$$(a_1+\ldots+a_m)b = a_1b+\ldots+a_mb,$$
$$(a_1+\ldots+a_m)(b_1+\ldots+b_n) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_ib_j = a_1b_1+a_1b_2+\ldots+a_mb_n,$$

kun $a, a_1, \ldots, a_m, b, b_1, \ldots, b_n \in R$.

Lause 2: $a,b,c \in R \Rightarrow$

i) $0_R \cdot a = 0_R = a \cdot 0_R$;

ii) $a(-b) = (-a)b = -(ab)$, $(-a)(-b) = ab$;

iii) $a(b-c) = ab-ac$, $(a-b)c = ac-bc$.

o) jos $R \neq \{0_R\}$, niin $1_R \neq 0_R$.

Tod.: i) $0_R \cdot a = (0_R+0_R)\cdot a \overset{\text{osit.}}{=} 0_R a + 0_R \cdot a$
$\Rightarrow 0_R = 0_R \cdot a$ (sup. sääntö ryhmässä $(R,+)$).
Vastaavasti $a \cdot 0_R = 0_R$.

o) jos $1_R = 0_R$, niin $a = 1_R \cdot a = 0_R \cdot a = 0_R$ $\forall a \in R$.

ii) $ab + a(-b) = a(b+(-b)) = a \cdot 0_R = 0_R$
$\Rightarrow a(-b) = -(ab)$ (ab:n vasta-alkio).
Vastaavasti $(-a)b = -(ab)$. Lopuksi $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$.

iii) $a(b-c) = a(b+(-c)) = ab+a(-c) = ab+(-(ac)) = ab-ac$. Toinen vastaavasti. $\square$

Huom.: a) Monisteessa oletetaan aina, että $R \neq \{0_R\}$, ts. $1_R \neq 0_R$.

b) ii) $\Rightarrow$ merkintä $-ab$ ei aiheuta sekaannusta.

Monikertojen ja kertolaskun yhteys:

Lause 3: Jos $a, b \in R$ ja $m, n \in \mathbb{Z}$, niin

iv) $na = (n \cdot 1_R)a = a \cdot (n \cdot 1_R)$;

v) $n(ab) = (na)b = a(nb)$;

vi) $(ma)(nb) = (mn)(ab)$.

Tod.: v) Kun $n = 0$, on $n(ab) = 0_R$, $(na)b = 0_R \cdot b = 0_R$ ja $a(nb) = a \cdot 0_R = 0_R$.

Kun $n > 0$, on $(na)b = (a + \dots + a)b = ab + \dots + ab = n(ab)$, ja samoin $a(nb) = n(ab)$.

Kun $n > 0$, on viela $((-n)a)b = (-(na))b \overset{ii)}{=} -((na)b) = -(n(ab)) = (-n)(ab)$, ja samoin $a((-n)b) = (-n)(ab)$.

iv) seuraa v):stä ($na = n(1_R \cdot a) = (n \cdot 1_R)a$ jne.)

vi) $(ma)(nb) \overset{v)}{=} m(a(nb)) \overset{v)}{=} m(n(ab)) = (mn)(ab)$. □

Esim. 1: Renkaassa R on $(a+b)^2 = (a+b) \cdot (a+b) = (a+b) \cdot a + (a+b) \cdot b = a \cdot a + b \cdot a + a \cdot b + b \cdot b = a^2 + ab + ba + b^2$. Jos $ab = ba$, on siis $(a+b)^2 = a^2 + 2ab + b^2$. Yleisemmin, jos $ab = ba$ (esim. R kommut.) ja $n \in \mathbb{N}_+$, on

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

$$\left((a+b)^{n+1} = \left(\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \right) \cdot (a+b) \right.$$

$$= \sum_{k=0}^{n} \binom{n}{k} a^{n+1-k} b^k + \underbrace{\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^{k+1}}_{l = k+1 \;=\; \sum_{l=1}^{n+1} \binom{n}{l-1} a^{n+1-l} b^l}$$

$$= a^{n+1} + b^{n+1} + \sum_{k=1}^{n} \underbrace{\left[\binom{n}{k} + \binom{n}{k-1} \right]}_{= \binom{n+1}{k}} a^{n+1-k} b^k \qquad = \sum_{k=1}^{n+1} \binom{n}{k-1} a^{n+1-k} b^k$$

$$\left. \right)$$

Esim. 2: iv) $\Rightarrow$ $\mathbb{Z}_n$:ssä on $k\bar{a} = (k \cdot \bar{1})\bar{a} = \bar{k}\bar{a}$ $\forall k, a \in \mathbb{Z}$.

$\mathbb{Z}_2$:ssa $(\bar{a} + \bar{b})^2 = \bar{a}^2 + 2\bar{a}\bar{b} + \bar{b}^2 = \bar{a}^2 + \bar{0}\bar{a}\bar{b} + \bar{b}^2 = \bar{a}^2 + \bar{b}^2$ $\forall a, b \in \mathbb{Z}$.