Renkaat ja Kunnat 19.1.2021

Laskutoimituksella varustettu joukko $(G, *)$ on *ryhmä*, jos

- laskutoimitus $*$ on assosiatiivinen,
- laskutoimituksella $*$ on neutraalialkio ja
- jokaisella $g \in (G, *)$ on käänteisalkio.

Kahdella laskutoimituksella varustettu joukko $(R, +, \cdot)$ on *(ykkösellinen) rengas*, jos $+$ ja $\cdot$ ovat assosiatiivisia ja

(1) $(R, +)$ on kommutatiivinen ryhmä,

(2) kertolasku on distributiivinen yhteenlaskun suhteen ja

(3) kertolaskulla on neutraalialkio $1 = 1_R \in R$.

Ryhmä $(R, +)$ on renkaan $(R, +, \cdot)$ *additiivinen ryhmä*.
Rengas on *kommutatiivinen rengas*, jos sen kertolasku on kommutatiivinen.

Huom. Joissakin kirjoissa ei vaadita neutr. alkiota kertolaskulle.

Jos $(S, *)$ on ryhmä ja $a, b, c \in S$ ja $a*b = a*c$, niin koska a:lla on käänteis-alkio $a^{-1} \in S$ ja $*$ on assos. saadaan

$$b = (a^{-1}*a)*b = a^{-1}*(a*b) = a^{-1}*(a*c) = (a^{-1}*a)*c = c.$$

Siis void. supistaa $a*b = a*c \Rightarrow b = c$

(1) Vastaavasti $b*a = c*a \Rightarrow b = c$.

Kysymys: Miksi normi $n: \mathbb{C} \to [0, \infty[$ on surj.:
Jos $x \geq 0$, niin sillä on $\sqrt{x} \in \mathbb{R} \subset \mathbb{C}$

$$n(\sqrt{x}) = \sqrt{x}\,\overline{\sqrt{x}} = \sqrt{x}^2 = x.$$

$$\overline{\sqrt{x}} = \sqrt{x}$$

$\Rightarrow x \in n(\mathbb{C})$.

Ryhmässä pätee supistussääntö.

Huom. Laskut. var. joukossa $(\mathbb{Z}, \cdot)$ ei päde supistussääntö:

$$0 \cdot 1 = 0 = 0 \cdot 2 \quad \text{mutta} \quad 1 \neq 2.$$

Prop. 3.5. Olk G, G' ryhmiä ja $\varphi : G \to G'$ homomorfismi.

1) φ kuvaa G:n n.a:n G':n n.a:ksi

2) $\varphi(g^{-1}) = \varphi(g)^{-1} \quad \forall g \in G.$

Tod. 1) olk. $e \in G$, $e' \in G'$ neutraalialkiot.

$$e' \underline{\underline{\varphi(e)}} = \varphi(e) = \varphi(ee) \underset{\substack{\uparrow \\ \varphi \text{ homom.}}}{=} \varphi(e)\underline{\underline{\varphi(e)}} \overset{\text{supista}}{\Longrightarrow} e' = \varphi(e). \quad \square$$

2) $$\varphi(g^{-1})\varphi(g) \underset{\substack{\uparrow \\ \varphi \text{ homom.}}}{=} \varphi(g^{-1}g) = \varphi(e) \underset{1)}{=} e'$$

$$\varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(e) = e'. \quad \square$$

Prop. 3.9. Olk. R rengas

1) $0_R x = 0_R = x 0_R \quad \forall x \in R$

2) $x(-y) = \boxed{(-x)y = -(xy)}$

$(-x)(-y) = xy$

3) $x(y-z) = xy - xz$

$(y-z)x = yx - zx$

$+$:n n.a on 0_R

$\cdot$:n n.a. on 1_R

$-(xy)$ on xy:n vasta-alkio: pätee

$\underbrace{xy + (-(xy))}_{xy - xy} = 0_R$

Tod. 1) $\underline{\underline{0_R x}} = x = 1_R x = (0_R + 1_R) x \overset{\text{distr.}}{=} 0_R x + 1_R x = \underline{\underline{0_R x + x}}$

supista

$\Rightarrow \quad \underline{\underline{0_R = 0_R x}}$. Toinen yhtälö tod. samoin.

<u>2) ja 3) Harj.</u>

<u>Esim.</u> $-x = (-1_R) x$.

$-x = (-1_R)x = -(1_R x)$

③

Prop. 3.11. Olk R rengas, $\# R \geq 2$. Tällöin

lukumäärä

1) $0_R \neq 1_R$

3) 0_R:llä ei ole käänteisalkiota.

Tod. 1) Jos $0_R = 1_R$, niin kaikille $x \in R$ pätee

$$x = 1_R x = 0_R x \underset{P.3.9(1)}{=} 0_R \implies \# R = 1.$$

2) Harj.

($a, b \in S \implies a+b \in S$, $ab \in S$)

Määr. Olk. R rengas, $S \neq \emptyset$, $S \subset R$. Ol. että S on $(R,+)$:n ja $(R,\cdot)$:n vakaa osajoukko ja että S on rengas indusoiduilla laskutoimituksilla ja $1_S = 1_R$. Tällöin S on R:n alirengas.

Esim. 1) $\mathbb{Z} \subset \mathbb{Q}$ on alirengas.

2) $S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{R} \right\} \subset M_2 \mathbb{R}$ on rengas mutta ei $M_2(\mathbb{R})$:n alirengas.

$1_S = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1_R$

$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \quad \forall a \in \mathbb{R}$. $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} -a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a+b & 0 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix}$

$\implies S$ on vakaa $+$:lla ja $\cdot$:lla.

Miksi halutaan $1_S = 1_R$.

$\varphi(x+y) = \varphi(x)+\varphi(y)$ ja $\varphi(xy) = \varphi(x)\varphi(y)$ $\forall x,y \in R$.

Määr. Olk. R, R' renkaita. 2. laskut. varustettujen joukkojen homomorfismi $\varphi : R \to R'$ on rengashomomorfismi, jos $\varphi(1_R) = 1_{R'}$.

Alirenkaalle $S \subset R$ vaaditaan $1_S = 1_R$, että kuvaus $i : S \to R$, $i(x) = x$ on rengashomomorfismi. (Tämä on aina 2. laskut. var. joukkojen homom. jos S on vakaa $+$:lle ja $\cdot$:lle)

Lemma 3.14 Jos $S \subset R$ on R:n alirengas, niin $0_S = 0_R$.

Tod.

$$0_R + 0_S = 0_S = 0_S + 0_S \overset{\text{supista}}{\Longrightarrow} 0_R = 0_S. \quad \blacksquare$$

Prop. 3.15 (Alirengastesti) R rengas, $S \subset R$ on R:n alirengas, jos ja vain jos

1) $x, y \in S \Rightarrow x+y \in S$ ja $xy \in S$

2) $-1_R \in S$

Tod. Harj.

Esim. 3.16 $C = \left\{ \begin{pmatrix} x & y \\ -y & x \end{pmatrix} : x, y \in \mathbb{R} \right\} < M_2(\mathbb{R})$

Os. että C on alirengas. Käytetään alirengastestiä (Prop. 3.15.)

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix} + \begin{pmatrix} s & t \\ -t & s \end{pmatrix} = \begin{pmatrix} x+s & y+t \\ \underbrace{-y-t}_{=-(y+t)} & x+s \end{pmatrix} \in C$$

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix}\begin{pmatrix} s & t \\ -t & s \end{pmatrix} = \begin{pmatrix} xs-yt & xt+ys \\ -ys-xt & -yt+xs \end{pmatrix} \in C.$$

$$1_{M_2(\mathbb{R})} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \qquad -1_{M_2(\mathbb{R})} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in C.$$

$\Rightarrow$ C on $M_2(\mathbb{R})$:n alirengas.

Esim. (Funktiorengas) Olk. $X \neq \emptyset$, R rengas.

$$\mathcal{F}(X,R) = \{ f : X \to R \}$$

Määr. laskutoimitukset pisteittäin:

$(f+g)(x) = f(x) + g(x) \quad \forall x \in X$

$(fg)(x) = f(x)g(x) \quad$ — " — .

Laskutoimitukset assos. ja distr. koska $\mathbb{R}$:n + ja $\cdot$ ovat assos. ja distr. pätee $\mathbb{R}$:ssä.
ja + on komm. on komm.

$$(f+g)(x) = f(x)+g(x) \overset{\uparrow}{=} g(x)+f(x) = (g+f)(x) \quad \forall\, x \in X$$

$\mathbb{R}$:n +:in komm.

$\Rightarrow f+g = g+f.$ Siis $\mathcal{F}(X,\mathbb{R})$:n + on komm.

$(\mathcal{F}(X,\mathbb{R}),+)$ on komm. ryhmä: +:n n.a. on 0-funktio:

$0(x) = 0_{\mathbb{R}} \ \forall\, x \in X$ ja $(-f)(x) = -f(x) \ \forall x \in X$.

<u>JMA</u>: Jos $f, g : \mathbb{R} \to \mathbb{R}$ on jva, niin $f+g$ on jva, fg — " — } jvien funktioiden joukko on vakaa

Vakiofunktio $1 : \mathbb{R} \to \mathbb{R}$, $1(x) = 1 \ \forall\, x \in \mathbb{R}$

$-1 : \mathbb{R} \to \mathbb{R}$ on jva.

Huom. $1 \cdot f = f \ \forall\, f \in \mathcal{F}(\mathbb{R},\mathbb{R})$

Siis $C(\mathbb{R},\mathbb{R}) = \{ f : \mathbb{R} \to \mathbb{R} \text{ jva} \} \subset \mathcal{F}(\mathbb{R},\mathbb{R})$ on alirengas. $\square$