Renkaat ja Kunnat 18.1.2021

$\{e, a, b\}$

$*$	e	a	b
e	e	a	b
a	a	e	e
b	b	e	b

1.7 2. laskut. var. joukot.

Määr. $A \neq \emptyset$, $*, \oplus$ laskutoimituksia A:ssa. Tällöin $(A, *, \oplus)$ on 2 laskut. var. joukko.

Määr. $(A, *, \oplus)$ on 2. laskut. var. joukko. $*$ on distributiivinen $\oplus$:n suhteen, jos

$$\boxed{\begin{aligned} a*(b\oplus c) &= (a*b)\oplus(a*c) \\ (b\oplus c)*a &= (b*a)\oplus(c*a) \end{aligned}}$$

osittelulait. $\forall a, b, c \in A$.

Esim 1) $\mathbb{Z}$:n, $\boxed{\mathbb{Q}\text{:n ja } \mathbb{R}\text{:n}}$ $\cdot$ on $+$:n suhteen distributiivinen.

$\mathbb{Z}$ yleistetään $\downarrow$ renkaat

$\mathbb{Q}, \mathbb{R}$ $\downarrow$ kunnat.

2) $M_n(\mathbb{R}) = (\{n\times n\text{-matriisit}\}, +, \cdot)$

matr. kertolasku on distr. yhteenlaskun suht. $\forall A, B, C \in M_n(\mathbb{R})$

LAG: $A(B+C) = AB + AC$ ja $(B+C)A = BA + CA$

Kompleksiluvut.

Määr. $\mathbb{C} = (\mathbb{R}^2, +, \cdot)$ $(a,b)\cdot(c,d) = (ac-bd,\ ad+bc)$

$\boxed{\mathbb{R}^2\text{:n } +}$

$i = (0,1)$ on imaginaariyksikkö.

Lemma 1.22 1) $+$ ja $\cdot$ ovat assosiatiivisia ja kommutatiivisia.
$\cdot$ on distr. $+$:n suhteen.

2) Olk. $z, w \in \mathbb{C}$ s.e. $zw = 0$. Tällöin $z=0$ tai $w=0$.

Tod. 1) Tylsä harj.   2) Harj. (LAG:sta voi olla iloa).

Lemma 1.23 Kuvaus $j: \mathbb{R} \to \mathbb{C}$, $j(x) = (x,0)$ on injektiivinen
kahdella laskut. varustettujen joukkojen homomorfismi.
(homomorfismi $+$:lle ja $\cdot$:lle)

Tod. Jos $j(x) = j(y)$, niin $(x,0) = (y,0)$. Siis $x=y$. $\Rightarrow j$ injektio.

Olk. $x, y \in \mathbb{R}$. $j(x+y) = (x+y,0) = (x,0)+(y,0) = j(x)+j(y)$

$j(xy) = (xy,0) \underset{\text{lasku}}{=} (x,0)(y,0) = j(x)\,j(y)$.

L. 1.23 $\rightsquigarrow$ void. ajatella vektoria $(a,0) \in \mathbb{C}$ reaalilukuna a.

$$(a,b) = (a,0) + (0,b) = a\underbrace{(1,0)}_{1} + b\underbrace{(0,1)}_{i} = a + bi$$

$(1,0)$ on kertolaskun neutr. alkio.

Huom. $(1,0)(c,d) = (c - 0d, d + 0c) = (c,d)$

$i^2 = (0,1)(0,1) = (-1,0) = -1$

$\mathbb{C}$:n kertolasku näillä merkinnöillä

$$(a+ib)(c+id) = ac + iad + ibc + \underbrace{i^2}_{=-1} bd = (ac-bd) + i(ad+bc)$$

L. 1.22 2) $\Rightarrow$ $\mathbb{C}-\{0\}$ on $(\mathbb{C},\cdot)$:n vakaa osajoukko.

$\rightsquigarrow$ $\cdot$ indusoi laskutoimituksen $\mathbb{C}-\{0\}$:ssa. $\rightsquigarrow$ $\mathbb{C}^\times = (\mathbb{C}-\{0\}, \cdot)$.

$a+bi = a + ib \in \mathbb{C}$

a = $\mathrm{Re}(a+ib)$ reaaliosa

b: $\mathrm{Im}(a+ib)$ imaginaariosa.

Jos $z = a+ib$, niin $\bar{z} = a - ib \in \mathbb{C}$ on z:n (kompleksi)konjugaatti ja

$n(z) = z\bar{z} = \underbrace{a^2+b^2}_{\in \mathbb{R} \subset \mathbb{C}}$ on z:n (algebrallinen) normi.

Huom. $z = 0 \iff n(z) = 0.$

Ol. $z \neq 0$. $z \dfrac{\bar{z}}{n(z)} = \dfrac{z\bar{z}}{n(z)} = \dfrac{n(z)}{n(z)} = 1.$ **Havainto:** Jokaisella $z \in \mathbb{C} - \{0\}$ on **Käänteisluku** (käänteisalkio :n suht.)

Prop. 1.26.

1) Konjugointi $\bar{\cdot} : \mathbb{C} \to \mathbb{C}$ on homomorfismi.

2) $\bar{\cdot} : \mathbb{C}^\times \to \mathbb{C}^\times$ —"— —

3) $n : (\mathbb{C}, \cdot) \to ([0,\infty[, \cdot)$ on homomorfismi. $n : \mathbb{C}^\times \to (]0,\infty[, \cdot)$ on homomorfismi } ja surjektio.

Tod. 3) Olk. $z, w \in \mathbb{C}$. Tällöin

$$n(zw) = (zw)\overline{(zw)} \overset{1)}{=} (zw)(\bar{z}\bar{w}) \underset{\substack{\text{assos} \\ \text{\& komm.}}}{=} (z\bar{z})(w\bar{w}) = n(z)\,n(w).$$

homom. OK.

Jos $x \in [0,\infty[$, niin $n(x) = n(x + 0i) = x\bar{x} = x^2$

Siis $\forall\, y \in [0,\infty[$ $y = n(\sqrt{y})$. Siis n on surjektio.

④

3 Renkaat

2 laskut var. joukoilla $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, M_n(\mathbb{R})$ on yhteisiä ominaisuuksia:
Kaikissa näissä Kaikilla alkioilla on käänteisalkio +:n suhteen
(vastaluku $\mathbb{Z}$:ssa, $\mathbb{Q}$:ssa, $\mathbb{R}$:ssä, $\mathbb{C}$:ssä), + on assos ja komm.
$\cdot$ on assosiatiivinen (Muista: $M_n(\mathbb{R})$:n $\cdot$ ei ole komm.) ja
$\cdot$:lle on neutraalialkio ($1 \in \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, $I_n = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \in M_n(\mathbb{R})$)

Esim 1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ komm. renkaita.
2) $M_n(\mathbb{R})$ on rengas. (ei komm, kun $n \geq 2$).

Määr. Olk. $(R, +, \cdot)$ 2 laskut var. joukko s.e.

1) + ja $\cdot$ ovat assosiatiivisia
2) + on kommutatiivinen
3) $\forall r \in (R,+)$ on käänteisalkio
4) $\cdot$ on distributiivinen +:n suhteen
5) $\cdot$:lla on neutraalialkio $1 = 1_R$.

Tällöin $(R, +, \cdot)$ on **rengas**. Jos $\cdot$ on komm. niin $(R,+,\cdot)$ on **komm. rengas**

Määr. Laskut. var. joukko $(G, *)$ on ryhmä, jos

$*$ on assos

$\forall g \in G$ on käänteisalkio (tästä ehdosta seuraa, että $*$:llä on neutraalialkio)

Jos $*$ on komm. niin $(G, *)$ on komm. ryhmä.

→ Renkaan määr on siis:

2 laskut var. joukko $(R, +, \cdot)$ on rengas, jos

1) $(R, +)$ on komm. ryhmä

2) $\cdot$ on assos ja se on distr. $+$:n suhteen

3) $\cdot$:lla on n. a. 1_R -

6