Renkaat ja Kunnat 26.1.2021

Jos R, R' renkaita, kuvaus $\varphi : R \to R'$ on **rengashomomorfismi** jos

$$\varphi(a+b) = \varphi(a) + \varphi(b) \quad \forall a,b \in R$$
$$\varphi(ab) = \varphi(a)\varphi(b) \quad \forall a,b \in R$$
$$\varphi(1_R) = 1_{R'}$$

$$\ker \varphi = \varphi^{-1}(\{0\}) = \{r \in R : \varphi(r) = 0\}.$$ φ:n **ydin**.

Prop. 3.21. φ injektio $\Leftrightarrow \ker\varphi = \{0_R\}$

Tod. $\underline{\Rightarrow}$: ol. φ injektio. $\varphi(0_R) = 0_{R'}$

$\Downarrow$

jos $\varphi(x) = \varphi(0_R)$, niin $x = 0_R$ $\Big\} \Rightarrow \ker\varphi = \{0_R\}$.

$\underline{\Leftarrow}$: Jos φ ei ole injektio, niin on $x, y \in R$ s.e. $\varphi(x) = \varphi(y)$, $x \neq y$

$$\Rightarrow \varphi(\underbrace{x-y}_{\neq 0_R}) \overset{\varphi\text{ hom}}{=} \varphi(x) - \varphi(y) = 0_{R'} \Rightarrow x - y \in \ker\varphi \Rightarrow \ker\varphi \neq \{0_R\}.$$

$x - y \neq 0_R$

□

1

Esim. Olk. $q \in \mathbb{N} - \{0,1\}$ ja olk. $\pi : \mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$, $\pi(k) = k + q\mathbb{Z}$.

$$\ker \pi = \pi^{-1}(0 + q\mathbb{Z}) = q\mathbb{Z} = \{ lq : l \in \mathbb{Z} \}.$$

Prop. 3.23. Olk. $\varphi : R \to R'$ rengashomomorfismi.

1) Jos $S \subset R$ on alirengas, niin $\varphi(S) \subset R'$ on alirengas

2) Jos $S' \subset R'$ on alirengas, niin $\varphi^{-1}(S') \subset R$ on alirengas.

Tod 1) Olk. $S \subset R$ alirengas.

Olk. $x', y' \in \varphi(S)$. Tällöin on $x, y \in S$ s.e. $\varphi(x) = x'$, $\varphi(y) = y'$.

$$x' + y' = \varphi(x) + \varphi(y) \overset{\varphi \text{ homom:lle}}{=} \varphi(\underbrace{x+y}_{\in S}) \in \varphi(S)$$

$$x'y' = \varphi(x)\varphi(y) \underset{\varphi \text{ homom:lle}}{=} \varphi(\underbrace{xy}_{\in S}) \in \varphi(S)$$

$$-1_R \in S \Rightarrow -1_{R'} = -\varphi(1_R) \overset{\text{p.3.5(2)}}{=} \varphi(\underbrace{-1_R}_{\in S}) \in \varphi(S).$$

Alirengastesti $\Rightarrow \varphi(S)$ on alirengas.

2

2) Harj.

Seuraus. Jos $\varphi : R \to R'$ on rengashomomorfismi, niin

$\varphi(R)$ on R':n alirengas

$\varphi^{-1}(R')$ on R:n alirengas.

Prop. 3.25 Olk. R rengas. Tällöin on täsmälleen yksi homomorfismi

$\varphi : \mathbb{Z} \to R$.

(Huom. $id : \mathbb{Z} \to \mathbb{Z}$ on ainoa rengashomom $\mathbb{Z} \to \mathbb{Z}$
$id(k) = k \quad \forall k \in \mathbb{Z}$)

Tod. Olk. $\varphi : \mathbb{Z} \to R$, $\varphi(k) = \underbrace{1_R + 1_R + \dots + 1_R}_{k \text{ kpl.}} = \underbrace{\overset{\in \mathbb{Z}}{k}\, \overset{\in R}{1_R}}_{k\text{:s monikerta}}$.

merkintä! ks. luku 1.9.

φ on rengashomomorfismi:

$\varphi(1) = 1_R$. OK.

Olk. $m, n \in \mathbb{Z}$. $\varphi(m+n) = (m+n)1_R = \underbrace{(1_R + \dots + 1_R)}_{m} + \underbrace{(1_R + \dots + 1_R)}_{n} = m1_R + n1_R$

$= \varphi(m) + \varphi(n)$.

ol. $m, n \geq 1$. $\varphi(mn) = (mn)1_R = \underbrace{1_R + \dots + 1_R}_{mn} = \left.\begin{array}{l} (\underbrace{1_R + \dots + 1_R}_{n}) \\ + (\underbrace{1_R + \dots + 1_R}_{n}) \\ \vdots \\ + (\underbrace{1_R + \dots + 1_R}_{n}) \end{array}\right\} m \text{ kertaa}$

$$\overset{\text{distr.}}{=} (\underbrace{1_R + \cancel{1_R +} \dots + 1_R}_{m \text{ kpl}})(\underbrace{1_R + \dots + 1_R}_{n \text{ kpl.}}) = \varphi(m)\varphi(n).$$

Jos $m = 0^{\in \mathbb{Z}}$ määr.: $m 1_R = 0_R$.

$m \leq -1$ määr. $m 1_R = \underbrace{(-m)}_{\geq 1}(-1_R) = \underbrace{(-1_R) + (-1_R) + \dots + (-1_R)}_{-m \text{ kertaa.}}$

homomorfisuus (mahd) negatiivisille m, n tark. kuten yllä.

4

Siis on ainakin 1 homomorfismi $\mathbb{Z} \to R$.

Olk $\psi : \mathbb{Z} \to R$ rengashomomorfismi. Tällöin $\psi(1) = 1_R$.

$$\psi(2) = \psi(1+1) = \psi(1) + \psi(1) = \underbrace{1_R + 1_R}_{2 \text{ kpl.}} = \varphi(2)$$

$$\Rightarrow \psi(k) = k\,\psi(1) = k\,1_R = \varphi(k)$$

$k \geq 1$

φ homom

Huomaa: $\psi(-k) \underset{\uparrow}{=} -\psi(k) = -\varphi(k) \overset{\downarrow}{=} \varphi(-k)$

ψ homom.

Lisäksi $\psi(0) = 0_R = \varphi(0)$ koska ψ ja φ ovat homomorfismeja.

$\Rightarrow \psi = \varphi$. $\square$

Määr. R rengas. Jos Prop. 3.25:in homomorfismi $k \mapsto k1_R$ on injektio, niin R:n karakteristika on $0 = \chi(R)$.

Muuten R:n karakteristika on

$$\chi(R) = \min\{k \in \mathbb{N}-\{0\} : k1_R = 0_R\}$$

$$\left(\begin{array}{l} k \in \operatorname{Ker} \varphi \\ \quad \varphi(k) = k1_R \end{array}\right)$$

Esim. 1) $\chi(\mathbb{Z}) = 0 = \chi(\mathbb{Q}) = \chi(\mathbb{R}) = \chi(\mathbb{C})$

2) $\chi(\mathbb{Z}/q\mathbb{Z}) = q$, $q \in \mathbb{N}-\{0,1\}$

$$k\underbrace{(1+q\mathbb{Z})}_{1_{\mathbb{Z}/q\mathbb{Z}}} = k+q\mathbb{Z} = \underbrace{0+q\mathbb{Z}}_{0_{\mathbb{Z}/q\mathbb{Z}}}, \quad k \geq 1$$

$$\iff k \equiv 0 \mod q.$$

$$\chi(\mathbb{Z}/q\mathbb{Z}) = \min\{k>0 : k(1+q\mathbb{Z}) = 0+q\mathbb{Z}\} = q.$$

Lemma 3.28 Jos $\chi(R) = q$, niin $qx = 0_R \ \forall x \in R$.

Huom: Tämä on epätriviaali väite, jos $q>0$. Tapaus $q=0$ tulee monik. määr.

Lemma 3.12. *Kommutatiivisessa renkaassa K pätee* binomikaava.[2]

$$(a+b)^n = \sum_{k=0}^{n} \underbrace{\binom{n}{k}}_{\in \mathbb{N}} \overset{\in K}{a}^{n-k} \overset{\in K}{b}^{k}$$

$$b^k = \underbrace{b \cdot b \cdot b \cdot \ldots \cdot b}_{k \text{ kpl.}}$$

alkion $a^{n-k} b^k$ $\binom{n}{k}$:s monikerta.

Tod. kuten (mahd.) aiemmilla kursseilla esim. reaalilukuille tehtiin. Tämän tuloksen voi ottaa tunnetuksi. (Tälle on käyttöä 3. harjoituksissa.)

Esim 1) $R = M_2(\mathbb{Z})$ $\quad 1_R = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $\quad k 1_R = \begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0_R$ $\quad \forall k \neq 0$.

$\Rightarrow \chi(M_2(\mathbb{Z})) = 0$.

2) $R = M_2(\mathbb{Z}/2\mathbb{Z})$ $\quad 1_R = \begin{pmatrix} 1+2\mathbb{Z} & 0+2\mathbb{Z} \\ 0+2\mathbb{Z} & 1+2\mathbb{Z} \end{pmatrix}$ $\quad 2\,1_R = \begin{pmatrix} 0+2\mathbb{Z} & 0+2\mathbb{Z} \\ 0+2\mathbb{Z} & 0+2\mathbb{Z} \end{pmatrix} = 0_R$

$\chi(R) = 2$.