Renkaat ja Kunnat 1.2.2021

$$\boxed{\mathbb{Z} \xrightarrow{\varphi} R \quad \varphi(k) = k\,1_R}$$

1_R:in k:s monikerta.

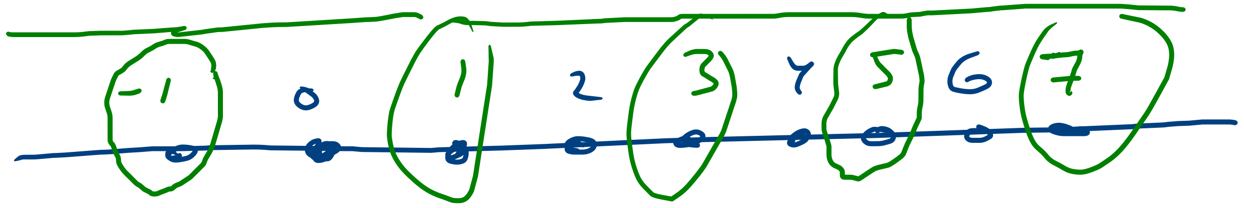
Karakteristika: $\exists_1$ rengashomom.

jos φ on injektio $\iff \ker\varphi = \{0\}$, sanotaan että R:n karakteristika on 0.

Muuten on pienin pos k s.e. $\varphi(k) = 0_R$. Tällöin R:n kar. on k $\chi(R)$

$$\underset{\in \mathbb{Z}}{k}\,\underset{\in R}{1_R} = \underbrace{1_R + 1_R + 1_R \cdots + 1_R}_{k \text{ kpl}} = 0_R \qquad \neq 0$$

$1 + 2\mathbb{Z} = -1 + 2\mathbb{Z} = 3 + 2\mathbb{Z}$



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

φ:n ydin on $\chi(R)\mathbb{Z} = \{ n\chi(R) : n \in \mathbb{Z}\}$.

4 Kunnat

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\mathbb{Z}/4\mathbb{Z}$

alkiolla $2+4\mathbb{Z}$ ei ole käänteisalkiota (kertolaskun suhteen)

$4 \equiv -1 \mod 5$

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\mathbb{Z}/5\mathbb{Z}$

Määr. Olk. R rengas, $u \in R$. Jos u:lla on käänteisalkio, niin u on yksikkö (unit)

- Kaikki $\mathbb{Z}/5\mathbb{Z}$:n alkiot paitsi 0 ovat yksiköitä.
- $\mathbb{Z}/4\mathbb{Z}$:n yksiköt ovat $1+4\mathbb{Z}$ ja $3+4\mathbb{Z}$.

Merkintä $(R\text{:n yksiköt}, \cdot) = R^\times$

R:n yksiköiden ryhmä = R:n multiplikatiivinen ryhmä

Esim. $\mathbb{R}^\times = (\mathbb{R} - \{0\}, \cdot)$

$\mathbb{C}^\times = (\mathbb{C} - \{0\}, \cdot)$

$\mathbb{Z}^\times = (\{-1, 1\}, \cdot)$ vakaa osajoukko $(\mathbb{Z}, \cdot)$:ssa.

$\mathbb{Q}^\times = (\mathbb{Q} - \{0\}, \cdot)$

Lemma. Olk. R rengas. R:n yksiköiden joukko on vakaa $(R,\cdot)$:ssa.

Tod. Olk. $u, v \in R$ yksiköitä. Täksin $\exists\, u^{-1}, v^{-1} \in R$ s.e. $\boxed{uu^{-1} = 1 = u^{-1}u, \quad vv^{-1} = 1 = v^{-1}v}$

$\boxed{\text{Siis } u^{-1}, v^{-1} \text{ ovat yksiköitä.}}$

Os. että uv on yksikkö: $(uv)(v^{-1}u^{-1}) \underset{\text{assos.}}{=} u\underbrace{(vv^{-1})}_{=1}u^{-1} = uu^{-1} = 1.$

$(v^{-1}u^{-1})(uv) = \cdots = 1.$

Siis yksiköiden joukko on vakaa. □

Prop. 4.1 $R^\times$ on ryhmä.

Tod.
- R:n $\circ$ on assos $\Rightarrow$ indus. laskutoimitus yks. joukossa on assos.
- 1_R on yksikkö: $1_R 1_R = 1_R \Rightarrow R^\times$:in laskut. on n.a.
- jokaisella $R^\times$:n alkiolla u on käänteisalkio u^{-1}. □

Huom: Jos $\#R \geq 2$, niin 0_R ei ole yksikkö.

Määr. Jos K on komm. rengas, jossa on väh. 2 alkiota ja jonka kaikki alkiot paitsi 0_K ovat yksiköitä, niin K on Kunta.

Jos R ei ole komm. ja $\#R \geq 2$ kaikki paitsi 0_R ovat yksiköitä, niin R on vino kunta.

R on jakorengas, jos se on kunta tai vino kunta.

Esim. • $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/5\mathbb{Z}$ ovat kuntia.

• $\mathbb{Z}$ ja $\mathbb{Z}/4\mathbb{Z}$ eivät ole kuntia

•

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

ja

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

.

$F = \{0, 1, \alpha, \beta\}$ laskutaulujen antamilla laskutoimituksilla on kunta, jossa on 4 alkiota.

Prop. 4.7 Olk. K kunta, R rengas, $\#R \geq 2$, $\varphi : K \to R$ rengashomomorfismi.

Tällöin φ on injektio ja $\varphi(K)$ on kunta.

Tod. $\varphi(1_K) = 1_R$ määr. nojalla

$\varphi(0_K) = 0_R$.

koska $0_R \neq 1_R$ Prop. 3.11 nojalla.

φ kuvaa K:n yksiköt yksiköiksi:

Olk. $u \in K$ yksikkö: Tällöin $\varphi(u)\varphi(u^{-1}) = \varphi(\underbrace{uu^{-1}}_{1_K}) = \varphi(1_K) = 1_R$

$\Leftrightarrow u \in K - \{0\}$.

$\varphi(u^{-1})\varphi(u) = \dots = 1_R$.

$\Rightarrow \varphi(u) \neq 0_R$

Siis $\varphi(u)$ on yksikkö kaikilla $u \in K - \{0\}$.

$\Rightarrow \varphi(K)$:n kaikki alkiot paitsi $0_R \in \varphi(K)$ ovat yksiköitä.

Prop. 1.10: $\varphi(K)$:n kertolasku on komm. koska $\varphi : K \to \varphi(K)$ on surjektio

Siis $\varphi(K)$ on kunta.

Muista Prop. 3.21: φ on injektio $\Leftrightarrow \ker\varphi = \{0_K\}$.

$\ker\varphi = \varphi^{-1}(\{0_R\})$

Edellä os. että $u \in K - \{0_K\} \Rightarrow \varphi(u) \neq 0_R$. $\square$

Huom. $\varphi : K \to \varphi(K)$ on rengasisomorfismi: Prop. 4.7:n mukaan φ on inj.

val maalijoukoksi kuvajoukko $\Rightarrow$ φ on surjektio.

Määr. Jos $k \in K$ alirengas s.e. k on kunta, niin k on K:n alikunta.

K ↑ kunta

Tällöin K on kunnan k laajennus tai kuntalaajennus.

Esim. $\mathbb{Q}$ on $\left\{ \begin{matrix} \mathbb{C}\text{:n} \\ \mathbb{R}\text{:n} \end{matrix} \right\}$ alikunta

$\mathbb{R}$ on $\mathbb{C}$:n alikunta

$\mathbb{R}$ on $\mathbb{Q}$:n kuntalaajennus

$\mathbb{C}$ — " —

$\mathbb{C}$ on $\mathbb{R}$:n kuntalaajennus.

Teht. 3.14 Vihje: Käytä L. 3.12 (Binomikaava)

$$(a+b)^{p} = \sum_{k=0}^{p} \underbrace{\binom{p}{k}}_{=0\ \forall k} a^{p-k} b^{k} = a^{p} + \underbrace{0+0+\cdots 0+}_{=0} b^{p}$$