Renkaat ja kunnat 8.2.2021

K on kommut. rengas. Jos $a, b, c \in K$ ja $ab = c$, niin a ja b } jakavat c:n
ovat c:n
teki jäitä. Merkintä $a \mid c$ ja $b \mid c$.

K on kokonaisalue, jos ($ab = 0 \Rightarrow a = 0$ tai $b = 0$)
Jos $a, b \in K - \{0\}$ ja $ab = 0$, niin a ja b ovat nollan jakajia.

Prop. 5.6. K kommut. rengas. K kokonaisalue $\Leftrightarrow$ K:ssa pätee kertolaskun supistussääntö.

→ jos $a \neq 0$ ja $ab = ac$, niin $b = c$.

Prop. 5.7. Kokonaisalueen karakteristika on 0 tai alkuluku.

① (K:n karakteristika on 0, jos rengashomomorfismi $\varphi : \mathbb{Z} \to K$, $\varphi(j) = j 1_K$, on injektio. Muuten kar. on $\min\{q \in \mathbb{N} - \{0,1\} : q 1_K = 0\}$)

Prop. 5.7. Kokonaisalueen karakteristika on 0 tai alkuluku.

Tod. Olk. K kommut. rengas. Ol. että $\chi(K) = q = ab$, missä $a, b \in \mathbb{N} - \{0, 1\}$. Olk. $\varphi : \mathbb{Z} \to K$, $\varphi(j) = j\,1_K$.

Koska $1 < a, b < \chi(K)$, pätee $\varphi(a) \neq 0_K \neq \varphi(b)$.

Kar. määritelmä $0_K = \varphi(q) = \varphi(ab) = \varphi(a)\varphi(b)$ (φ homom.) $\Rightarrow$ $\varphi(a)$ ja $\varphi(b)$ ovat nollan jakajia.

Siis K ei ole kokonaisalue. □

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

Lause 5.8. Äärellinen kokonaisalue on kunta.

Tod. Olk. E äärellinen kokonaisalue, $a \in E - \{0\}$. Oo. että a:lla on käänteisalkio.

Määr. $l_a : E \to E$, $l_a(x) = ax$ $\forall\, x \in E$. Os. että l_a on injektio:

Jos $l_a(x) = l_a(y)$, niin $ax = ay \overset{\text{kertolaskun sup. säänt.}}{\Longrightarrow} x = y$. $\Rightarrow$ l_a on inj.

Koska E on äärellinen, l_a on myös surjektio. Siis $1_E \in l_a(E)$, ② joten on $b \in E$ s.e. $1_E = l_a(b) = ab \overset{E \text{ kommut.}}{=} ba$. Siis $b = a^{-1}$. □

Lause (Wedderburn) Äärellinen jakorengas on kunta.

Olk. E kokonaisalue. Olk. $p \in E - (E^\times \cup \{0\})$. p on jaoton, jos
$(ab = p$ joillain $a, b \in E) \Rightarrow a \in E^\times$ tai $b = E^\times$.

Lukuteoriassa $\mathbb{Z}$:n positiivisia jauttomia alkioita sanotaan alkuluvuiksi.

[Luku $p \in \mathbb{N} - \{0,1\}$ on alkuluku, jos $(ab = p$ joillain $a, b \in \mathbb{N}) \Rightarrow (a = 1$ tai $b = 1)$]

Esim. Os. että $2 \in \mathbb{Z}[\sqrt{-3}]$ on jaoton. (kokonaisalue, koska $\mathbb{C}$:n alirengas)

$\mathbb{Z}[\sqrt{-3}] = \{a + bi\sqrt{3} : a, b \in \mathbb{Z}\}$.

Olk. $a \in \mathbb{Z}[\sqrt{-3}]$ s.e. $a \mid 2$. Tällöin $n(a) \mid (4 = n(2))$ reuleassa $\mathbb{Z}$.

Jos $m, n \in \mathbb{Z}$, niin $n(m + ni\sqrt{3}) = m^2 + 3n^2$

$\Rightarrow n(a) \in \{1, 2, 4\}$ (ei ole minkään alkion normi)

$= 1 \Leftrightarrow m = \pm 1, n = 0$

$= 4 \Leftrightarrow [m, n = \pm 1$ (huom. $m^2 + 3n^2 \in \{0, 3, 12, \ldots\}$, $m = \pm 2, n = 0]$

$m^2 \in \{0, 1, 4, 9, \ldots\}$

$\Rightarrow n(a) = 1$ tai $n(a) = 4$.

Huom. • $n(a) = 1 \Rightarrow a \in \mathbb{Z}[\sqrt{-3}]^\times$

$a \bar{a}$ $\quad n(b) = n(ab) = n(2) = 4$

jos $n(a) = 4$ ja $ab = 2$, niin $n(b) = 1 \Rightarrow b \in \mathbb{Z}[\sqrt{-3}]^\times$.

siis $2 \in \mathbb{Z}[\sqrt{-3}]$ on jaoton.

Huom. $(i\sqrt{3})(-i\sqrt{3}) = 3$ siis $3 \in \mathbb{Z}[\sqrt{-3}]$ ei ole jaoton.

$\in \mathbb{Z}[\sqrt{-3}]$

Olk. E kokonaisalue. $p \in E - (E^\times \cup \{0\})$ on alkualkio (tai alkuluku),

jos $\forall a, b \in K$ pätee $\boxed{(p \mid ab) \Rightarrow (p \mid a \text{ tai } p \mid b)}$

Euklideen lemma. $\mathbb{Z}$:n jaottomat alkiot ovat alkualkioita. Ks. Lukut. 1.

Prop. 5.12. Kokonaisalueen alkualkiot ovat jaottomia.

Tod. Olk. K kokonaisalue ja olk. $p \in K$ alkualkio.

Siis: jos $a,b \in K$ s.e. $p \mid ab$, niin $p \mid a$ tai $p \mid b$.

K komm!

Os. että p on jaoton: Jos $ab = p$, niin $a \in K^\times$ tai $b \in K^\times$.

Ol. että $ab = p$. Siis erityisesti $p \mid ab$. p alkualkio

$\Rightarrow$ Väe: $p \mid a$ Siis on $c \in K$ s.e. $a = pc$.

Siis $pcb = p \overset{p \neq 0}{\Rightarrow} cb = 1 \Leftrightarrow b \in K^\times$. Siis p on jaoton. $\square$

sup.

Esim. Renkaassa $\mathbb{Z}[\sqrt{-3}]$ pätee $4 = 2 \cdot 2 = (1+i\sqrt{3})(1-i\sqrt{3})$

Siis $2 \mid (1+i\sqrt{3})(1-i\sqrt{3})$. Mutta $2 \nmid 1+i\sqrt{3}$ ja $2 \nmid 1-i\sqrt{3}$,

koska $n(2) = n(1 \pm i\sqrt{3})$. Jos nyt $2a = 1+i\sqrt{3}$, niin $n(a) = 1$

$\Rightarrow a \in \mathbb{Z}[\sqrt{-3}]^\times$.

Siis 2 on jaoton mutta ei alkualkio.

Lause 5.14 Olk. $q \in \mathbb{N} - \{0,1\}$. Tällöin seuraavat ovat yhtäpitäviä:

- q on alkuluku
- $\mathbb{Z}/q\mathbb{Z}$ on kokonaisalue $\Rightarrow$ $\mathbb{Z}/q\mathbb{Z}$ on äärellinen (L. 5.8)
- $\mathbb{Z}/q\mathbb{Z}$ on kunta.

Prop. 5.15 $q \geq 2$. $a + q\mathbb{Z} \in (\mathbb{Z}/q\mathbb{Z})^\times \Leftrightarrow \underline{\mathrm{syt}(a,q) = 1}$.

Tod. $(a+q\mathbb{Z})(b+q\mathbb{Z}) = ab + q\mathbb{Z}$

$= 1 + q\mathbb{Z}$

$\Leftrightarrow \exists\, k \in \mathbb{Z}$:

$\circledast$ $\boxed{ab + kq = 1}$ Bézout'n yhtälö

Lukut. 1: $\circledast$:llä on ratkaisu $\Leftrightarrow \mathrm{syt}(a,q) = 1$

Bézout