V. 3 (osa) Alirenkaat

Määr.: Renkaan R osajoukko S on R:n **alirengas**, jos

i) $1_R \in S$,
ii) $a - b \in S$ aina, kun $a, b \in S$, ja
iii) $ab \in S$ aina, kun $a, b \in S$.

Huom.: a) i) & ii) $\Leftrightarrow$ S on $(R,+)$:n aliryhmä (alir. krit.);
i) & iii) $\Leftrightarrow$ S on monoidin $(R,\cdot)$ "alimonoidi".
b) Alirengas on indus. laskutoim. suhteen itsekin rengas.

Esim. 1: Seuraavassa jok. rengas on (kaupien (ait.)) alirengas: $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. $\mathbb{Z}$:n ainoa alirengas on $\mathbb{Z}$ ($S \subset \mathbb{Z}$ alirengas $\Rightarrow 1 \in S \Rightarrow n = n \cdot 1 \in S$ $\forall n \in \mathbb{Z}$ (moniherta) $\Rightarrow S = \mathbb{Z}$).

Esim. 2: $M_2(R)$:n osajoukko $R = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in R \right\}$ on rengas matriisien yhteen- ja kertolaskun suhteen. R ei ole $M_2(R)$:n alirengas, sillä

$$1_{M_2(R)} = I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \notin R \qquad \left(1_R = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right).$$

Esim. 3: Kun $n \in \mathbb{N}_+$, on joukko

$$\mathbb{Z}[\sqrt{n}] = \{ a + b\sqrt{n} \mid a, b \in \mathbb{Z} \} \subset \mathbb{R}$$

renkaan $\mathbb{R}$ alirengas (tod. harj. teht.), jos $n \in \mathbb{Z}$, $n < 0$, ja merk. $\sqrt{n} = i\sqrt{-n} \in \mathbb{C}$, on vastaavasti $\mathbb{Z}[\sqrt{n}]$ renkaan $\mathbb{C}$ alirengas. Erikoistapaus $n = -1$: $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i] = \{ a + bi \mid a, b \in \mathbb{Z} \}$ Gaussin kokonaislukujen rengas.

Esim. 4: $\mathbb{R}^{\mathbb{R}} = \{ f \mid f : \mathbb{R} \to \mathbb{R}$ kuvaus$\}$ on tunnetusti rengas (erik.tapaus funktiorenkaasta R^X).

$$C^0(\mathbb{R}) = \{ f \in \mathbb{R}^{\mathbb{R}} \mid f \text{ on jatkuva} \}$$

on $\mathbb{R}^{\mathbb{R}}$:n alirengas (vakioluvun. $\overline{1}$ on jatkuva; f, g jatkuvia $\Rightarrow f - g$ ja $f \cdot g$ ovat jatkuvia), samoin

$$C^1(\mathbb{R}) = \{ f \in \mathbb{R}^{\mathbb{R}} \mid f \text{ on jatkuvasti derivoituva} \}.$$

Myös $P = \{f \in \mathbb{R}^{\mathbb{R}} \mid f$ on polynomikuvaus$\}$ on alirengas ($f: \mathbb{R} \to \mathbb{R}$ pol.kuv. $\Leftrightarrow \exists n \in \mathbb{N}$ ja valmiit $a_0, a_1, \ldots, a_n \in \mathbb{R}$ s.e. $f(x) = a_0 + a_1 x + \ldots + a_n x^n \quad \forall x \in \mathbb{R}$). Tässä

$$P \subsetneq C^1(\mathbb{R}) \subsetneq C^0(\mathbb{R}) \subsetneq \mathbb{R}^{\mathbb{R}}.$$

I.5 Rengashomomorfismit ja -isomorfismit

Määr.: Olk. R ja R' renkaita. Kuvaus $f: R \to R'$ on (rengas-) homomorfismi, jos

i) $f(a+b) = f(a) + f(b) \quad \forall a, b \in R$,
ii) $f(ab) = f(a) f(b)$ — " —, ja
iii) $f(1_R) = 1_{R'}$.

Bijektiivinen (rengas-) homom. on (rengas-) isomorfismi.

(Huom.: i) $\Leftrightarrow$ f on ryhmähomom. $(R,+) \to (R',+)$;
ii) & iii) $\Leftrightarrow$ f on "monoidien homom." $(R,\cdot) \to (R',\cdot)$.)

Ol. $f: R \to R'$ rengashomom. Tällöin ent. $f(0_R) = 0_{R'}$ ja $f(-a) = -f(a) \quad \forall a \in R$; edelleen $f(na) = n \cdot f(a)$ $\forall a \in R$, $\forall n \in \mathbb{Z}$. Lisäksi $f(a^n) = f(a)^n \quad \forall a \in R$, $\forall n \in \mathbb{N}$. Viim. kaava pätee myös, kun $n < 0$, mikäli $a \in R^*$, ts. a on käänty vä R:ssä:

Lause: Jos $f: R \to R'$ on rengashomom., niin $f(R^*) \subset R'^*$; $f(a^{-1}) = f(a)^{-1} \quad \forall a \in R^*$.

Tod.: Kun $a \in R^*$, on $f(a) \cdot f(a^{-1}) = f(aa^{-1}) = f(1_R) = 1_{R'}$ ja samoin $f(a^{-1}) \cdot f(a) = 1_{R'}$; näin $f(a) \in R'^*$ ja $f(a)^{-1} = f(a^{-1})$. □

Esim.: a) Kan. surj. $p: \mathbb{Z} \to \mathbb{Z}_n$ $(n \in \mathbb{N}_+)$ on rengashomom.

b) R rengas $\Rightarrow$ $\mathrm{id}_R: R \to R$ on rengasisom.;
$f: R \to R'$, $g: R' \to R''$ rengashomom. (tai -isom.) $\Rightarrow$ $g \circ f: R \to R''$ rengashomom. (tai -isom.);
$f: R \to R'$ rengasisom. $\Rightarrow$ $f^{-1}: R' \to R$ rengasisom.;
$S \subset R$ alirengas $\Rightarrow$ kan. inj. $S \hookrightarrow R$ on rengashomom. (tod. lukuun ryhmille).

c) R' rengas $\Rightarrow$ $\exists$ täsm. yksi rengashomom. $\mu : \mathbb{Z} \to R'$, niin. $\mu(n) = n \cdot 1_{R'}$ $\forall n \in \mathbb{Z}$.

Tod.: $\mu : \mathbb{Z} \to R'$ rengashomom. $\Rightarrow$ $f(n) = f(n \cdot 1) = n \cdot f(1) = n \cdot 1_{R'}$ $\forall n \in \mathbb{Z}$;
(↖ monikerta kääntäen, Lause 3 $\Rightarrow$ kaava $\mu(n) = n \cdot 1_{R'}$ $\forall n \in \mathbb{Z}$ määr. rengashomom. $\mu : \mathbb{Z} \to R'$. □

d) Olk. Σ joukko. Kun $A \subset \Sigma$, olkoon $\chi_A : \Sigma \to \mathbb{Z}_2$ A:n karakteristinen funktio, ts. $\chi_A(x) = \bar{1}$, kun $x \in A$, ja $\chi_A(x) = \bar{0}$, kun $x \in \Sigma \setminus A$. Kuvaus

$$\chi : (\mathcal{P}(\Sigma), \Delta, \cap) \longrightarrow (\mathbb{Z}_2^{\Sigma}, +, \cdot)$$
$$A \longmapsto \chi_A$$

on rengasisomorfismi; χ:n kääntökuvaus on $\mathbb{Z}_2^{\Sigma} \ni f \mapsto f^{-1}(\{\bar{1}\}) \in \mathcal{P}(\Sigma)$ (kaav. tehtävä).

Seuraus: $f : R \xrightarrow{\sim} R'$ rengasisom. $\Rightarrow$ $f(R^*) = R'^*$, jolloin f:n rajoittuma on ryhmäisom. $R^* \xrightarrow{\sim} R'^*$.

Tod.: f rengashomom. $\Rightarrow$ $f(R^*) \subset R'^*$; $\exists f^{-1}$, joka myös rengashomom. $\Rightarrow$ $f^{-1}(R'^*) \subset R^*$ $\Rightarrow$ $R'^* = f(f^{-1}(R'^*)) \subset f(R^*)$. □

Kuten Lause III.8, voidaan todistaa

Lause 9 (osa): Ol. $f : R \to R'$ rengashomom. Silloin
i) $S \subset R$ alirengas $\Rightarrow$ $f(S) \subset R'$ alirengas;
ii) $S' \subset R'$ –"– $\Rightarrow$ $f^{-1}(S') \subset R$ –"–. □

V.4 Ideaalit ja jäännösluokkarenkaat

Olkoon R rengas ja $H \subset R$ additiivinen alaryhmä (ks. $H \leq (R,+)$). $(R,+)$ Abelin ryhmä $\Rightarrow$ $H \trianglelefteq (R,+)$ $\Rightarrow$ void. muodostaa tekijäryhmä $(R/H, +)$, missä $R/H = \{x+H \mid x \in R\}$ ja

$$(x+H) + (y+H) = (x+y) + H \quad \forall x, y \in R.$$

Halutaisiinko määritellä R:n kertolaskun avulla R/H:lle kertolaskun.

Lemma: Kaava $(x+H)\cdot(y+H) = (xy)+H \quad \forall x,y \in R$ määrittelee R/H:ssa laskutoimituksen $\cdot$
$\Leftrightarrow$ H toteuttaa seur. lisäehdon:

$$xh \in H \text{ ja } hx \in H \text{ aina, kun } x \in R \text{ ja } h \in H.$$

Tod.: $\Leftarrow$. Ol. lisäehto voimassa. Silloin
$x+H = x'+H$, $y+H = y'+H \Rightarrow x-x' \in H$, $y-y' \in H$
$\Rightarrow xy - x'y' = xy - x'y + x'y - x'y'$
$= \underbrace{(x-x')}_{\in H}\cdot \underbrace{y}_{\in R} + \underbrace{x'}_{\in R}\cdot \underbrace{(y-y')}_{\in H} \in H$
$\in H$ $\in H$

$\Rightarrow (xy)+H = (x'y')+H$. $\therefore$ $\cdot$ hyvin määr. R/H:ssa.

$\Leftarrow$. Vastaol.: $\exists x_0 \in R$ ja $h_0 \in H$ s.e. $x_0h_0 \notin H$ (tai vastaavasti $h_0x_0 \notin H$). Tällöin $0_R + H = h_0 + H$, mutta $(x\cdot 0_R)+H = 0_R + H \neq (x_0h_0)+H$, joten yo. laskun ei määr. tuloa $(x+H)\cdot(0_R+H)$ 1-käsitteisesti. $\square$

Määr.: Renkaan R osjoukko I on R:n ideaali, jos

i) $I \neq \emptyset$,
ii) $a-b \in I$ aina, kun $a,b \in I$, ($\Leftrightarrow I \leq (R,+)$)
iii) $xa \in I$ ja $ax \in I$ aina, kun $x \in R$ ja $a \in I$.

Huom.: Jos $I \subset R$ on ideaali ja $1_R \in I$, niin $x = x\cdot 1_R \in I$ $\forall x \in R$, joten $I = R$. Erityisesti I on samoin R:n ideaali ja aitorengas vain, jos $I = R$.

Esim.: a) R:n triviaalit ideaalit $\{0_R\}$ ja R.
b) Renkaan $\mathbb{Z}$ ideaalit ovat $n\mathbb{Z}$, $n \in \mathbb{Z}$.
(Tod.: $n\mathbb{Z}$:t ovat $\mathbb{Z}$:n (kaikki) additiiv. aliryhmät. Lisäksi $n\mathbb{Z}$ tot. ehdan iii): $x \in \mathbb{Z}$, $np \in n\mathbb{Z} \Rightarrow$ $x\cdot np = np\cdot x = n\cdot(px) \in n\mathbb{Z}$. $\square$)

c) Ol. R kommut. rengas ja $a \in R$. Tällöin

$$\langle a \rangle = Ra = \{xa \mid x \in R\}$$

on R:n ideaali, alkion $a \in R$ virittämä **pääideaali** ($\langle a \rangle$ on (selvästi) pienin R:n ideaali, jolla a on).

Tod.: i) $0_R = 0_R \cdot a \in \langle a \rangle \Rightarrow \langle a \rangle \neq \emptyset$.
ii) $xa, ya \in \langle a \rangle$ $(x, y \in R) \Rightarrow xa + ya = (x+y)a \in \langle a \rangle$.
iii) $x \in R$, $ya \in \langle a \rangle$ $(y \in R) \Rightarrow (ya) \cdot x = x \cdot (ya)$ (R kommut.!)
$= (xy)a \in \langle a \rangle$. □

d) jos R on kommut. ja $a_1, \ldots, a_k \in R$, niin vastaavasti

$$\langle a_1, \ldots, a_k \rangle = \{x_1 a_1 + \ldots + x_k a_k \mid x_1, \ldots, x_k \in R\}$$

on R:n pienin ideaali, jolla on alkiot $a_1, \ldots, a_k$.

Lause: $I, J \subset R$ R:n ideaaleja $\Rightarrow$ $I \cap J$ ja $I + J = \{a + b \mid a \in I, b \in J\}$ ovat R:n ideaaleja.
(Tod. helppo harj. tehtävä.) □

Erityisesti, jos R on kommut. ja $a_1, \ldots, a_k \in R$, niin $\langle a_1, \ldots, a_k \rangle = \langle a_1 \rangle + \ldots + \langle a_k \rangle = Ra_1 + \ldots + Ra_k$.

Esim.: Renkaan $\mathbb{Z}$ kaikki ideaalit $n\mathbb{Z} = \langle n \rangle$ $(n \in \mathbb{N})$ ovat pääideaaleja (siis $\mathbb{Z}$ on "pääideaalirengas", PIR = principal ideal ring). Erityisesti, jos $a_1, \ldots, a_k \in \mathbb{Z}$, niin $\exists d \in \mathbb{N}$ s.e.

$$\langle a_1, \ldots, a_k \rangle = \langle d \rangle.$$

V. $d = \mathrm{syt}(a_1, \ldots, a_k)$.
T. $a_i \in \langle a_1, \ldots, a_k \rangle = \langle d \rangle$ $\forall i \Rightarrow d \mid a_i$ $\forall i$.
Todistus $d \in \langle d \rangle = \langle a_1, \ldots, a_k \rangle \Rightarrow \exists x_1, \ldots, x_k \in \mathbb{Z}$ s.e. $d = x_1 a_1 + \ldots + x_k a_k$; jos siis $d' \mid a_i$ $\forall i$, niin $d' \mid d$. □

Esim.: Rengashomomorfismin $f: R \to R'$ ydin $\ker(f) = \{a \in R \mid f(a) = 0_{R'}\}$ on R:n ideaali.

Tod.: $f: (R, +) \to (R', +)$ ryhmähomom. $\Rightarrow \ker(f) \leq (R, +)$.
Lisäksi $x \in R$, $a \in \ker(f) \Rightarrow f(xa) = f(x) f(a) = f(x) \cdot 0_{R'} = 0_{R'}$
ja $f(ax) = f(a) f(x) = 0_{R'} \cdot f(x) = 0_{R'} \Rightarrow xa, ax \in \ker(f)$. □

yleisemmin pätee:

Lause 9 (loppu): Olk. $f: R \to R'$ rengashomom. Tällöin
iii) $I \subset R$ ideaali $\Rightarrow$ $f(I)$ on $\mathrm{Im}(f)$:n ideaali,
iv) $I' \subset R'$ -"- $\Rightarrow$ $f^{-1}(I')$ on R:n -"-. $\square$

(Huom.: Lause 9 i) $\Rightarrow$ $\mathrm{Im}(f) = f(R)$ on R':n alirengas.)

Lause 8: Olkoon R rengas ja $I \subset R$ ideaali. Tällöin $(R/I, +, \cdot)$ on rengas, R:n jäännösluokkarengas l. tekijärengas modulo I, missä $R/I = \{x+I \mid x \in R\}$ ja

$$(x+I)+(y+I) = (x+y)+I \qquad \forall x, y \in R$$
$$(x+I)\cdot(y+I) = (xy)+I \qquad \text{-"-}.$$

Kan. surjektio $p: R \to R/I$, $p(x) = x+I$ $\forall x \in R$, on rengashomom. ja $\ker(p) = I$.

Tod.: Lause IV.2 $\Rightarrow$ $(R/I, +)$ on Ab. ryhmä. Luvun alku $\Rightarrow$ kertolaskun lyhyin määr. R/I:ssä. Muut R/I:n rengasomin. seuraavat heti R:n vast. ominaisuuksista. $\square$

Huom.: Jäännösluokkarenkaassa R/I on nis:
$x+I = y+I \iff x-y \in I$; erit. $x+I = I\ (= 0_R+I)$
$\iff x \in I$.
$0_{R/I} = 0_R + I$; $1_{R/I} = 1_R + I$; $-(x+I) = (-x)+I$;
jos $x \in R^*$, niin $x+I \in (R/I)^*$ ja $(x+I)^{-1} = x^{-1}+I$
(vai olla $x+I \in (R/I)^*$, vaikka $x \notin R^*$).

Esim. 1: $(\mathbb{Z}/n\mathbb{Z}, +, \cdot) = (\mathbb{Z}_n, +, \cdot)$ (ks. luku I.2).

Lause 10 (Renkaiden homomorfialause): Rengashomomorfismi $f: R \to R'$ indusoi rengasisomorfismin

$$F: R/\ker(f) \xrightarrow{\sim} \mathrm{Im}(f), \quad x+\ker(f) \longmapsto f(x),$$

s.e. seur. kaavio kommutoi:

$$\begin{array}{ccc} R & \xrightarrow{f} & R' \\ {\scriptstyle p}\downarrow & & \uparrow{\scriptstyle i} \\ R/\ker(f) & \xrightarrow[\sim]{F} & \mathrm{Im}(f) \end{array}$$

(p kan. surj., i kan. inj.).

Tod.: Lause IV.4 $\Rightarrow$ F on (oddil.) ryhmähomom. Kun merk. $I = \ker(f)$, on lisäksi

$$F((x+I)\cdot(y+I)) = F((xy)+I) = f(xy)$$
$$= f(x)\cdot f(y) = F(x+I)\cdot F(y+I) \quad \forall x,y \in R, \text{ ja}$$
$$F(1_{R/I}) = F(1_R+I) = f(1_R) = 1_R. \quad \square$$

Esim.: a) Ol. R rengas, X joukko ja $x_0 \in X$. Funktiorenkaan R^X laskutoim. nojaav. $\Rightarrow$ kuvaus $\varphi: R^X \to R$, $\varphi(f) = f(x_0)$ $\forall f \in R^X$, on rengashomom. Lisäksi φ on surjektio ($a \in R \Rightarrow$ vakiokuv. $[\overline{a}: x \mapsto a] \in R^X$ ja $\varphi(\overline{a}) = a$) ja $\ker(\varphi) = \{f \in R^X \mid f(x_0) = 0_R\}$. Lause 10 $\Rightarrow$ φ indusoi rengasisomorfismin

$$R^X / \{f \in R^X \mid f(x_0) = 0\} \xrightarrow{\sim} R.$$

b) Ol. $n, k, l \in \mathbb{N}_+$, $n = k\cdot l$, $\text{syt}(k,l) = 1$. Kuvaus $f: \mathbb{Z} \to \mathbb{Z}_k \times \mathbb{Z}_l$, $f(x) = ([x]_k, [x]_l)$ $\forall x \in \mathbb{Z}$, on rengashomom., ja $x \in \ker(f) \Leftrightarrow [x]_k = [0]_k$ ja $[x]_l = [0]_l \Leftrightarrow k \mid x$ ja $l \mid x \Leftrightarrow n \mid x$ (koska $\text{syt}(k,l) = 1$); siten $\ker(f) = n\mathbb{Z}$.

V. f on surjektio.

T. $\text{syt}(k,l) = 1 \Rightarrow \exists a, b \in \mathbb{Z}$ s.e. $ak + bl = 1$. Tällöin $[ak]_l = [1-bl]_l = [1]_l$ ja $[bl]_k = [1-ak]_k = [1]_k$. Olk. $x, y \in \mathbb{Z}$. Silloin

$$f(yak + xbl) = ([yak+xbl]_k, [yak+xbl]_l)$$
$$= ([x]_k\cdot[bl]_k, [y]_l\cdot[ak]_l) = ([x]_k, [y]_l),$$

joten $([x]_k, [y]_l) \in \text{Im}(f)$. $\square$

$\therefore$ f indusoi rengasisom. $\mathbb{Z}_n \xrightarrow{\sim} \mathbb{Z}_k \times \mathbb{Z}_l$.

vrt. Esim. d) s. 72

b)-kohdan avulla void. laskea Eulerin φ-funktion arvot. Olk. $n \in \mathbb{N}$, $n \geq 2$; $n = p_1^{h_1}\cdot p_2^{h_2}\cdot\ldots\cdot p_r^{h_r}$, p_i:t eri alkulukuja, $h_i \in \mathbb{N}_+$ $\forall i \in \{1,\ldots,r\}$. b) + induktio $\Rightarrow$

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{h_1}} \times \mathbb{Z}_{p_2^{h_2}} \times \ldots \times \mathbb{Z}_{p_r^{h_r}} \quad \text{rengasisom.}$$

$$\Rightarrow \quad \mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{h_1}}^* \times \mathbb{Z}_{p_2^{h_2}}^* \times \ldots \times \mathbb{Z}_{p_r^{h_r}}^* \quad \text{ryhmäisom.}$$

$$\Rightarrow \quad \varphi(n) = |\mathbb{Z}_n^*| = |\mathbb{Z}_{p_1^{h_1}}^*| \times |\mathbb{Z}_{p_2^{h_2}}^*| \times \ldots \times |\mathbb{Z}_{p_r^{h_r}}^*| =$$

$$= \varphi(p_1^{h_1}) \cdot \varphi(p_2^{h_2}) \cdot \ldots \cdot \varphi(p_r^{h_r}).$$

Kun p on alkuluku (ts. $p \in \mathbb{P}$) ja $h \in \mathbb{N}_+$, on

$$\begin{aligned}\varphi(p^h) &= \#\{a \in \mathbb{Z} \mid 0 \le a \le p^h - 1,\ \mathrm{syt}(a, p^h) = 1\} \\ &= \#\{a \in \mathbb{Z} \mid 0 \le a \le p^h - 1,\ p \nmid a\} \\ &= \#(\{0, 1, \ldots, p^h - 1\} \setminus \{0 \cdot p, 1 \cdot p, \ldots, (p^{h-1} - 1) \cdot p\}) \\ &= p^h - p^{h-1} = p^h \cdot \left(1 - \frac{1}{p}\right).\end{aligned}$$

$$\therefore \quad \varphi(n) = \prod_{i=1}^{r} \varphi(p_i^{h_i}) = \prod_{i=1}^{r} p_i^{h_i} \left(1 - \frac{1}{p_i}\right)$$

$$= (p_1^{h_1} \cdot \ldots \cdot p_r^{h_r}) \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) =$$

$$= n \cdot \prod_{\substack{p \in \mathbb{P} \\ p \mid n}} \left(1 - \frac{1}{p}\right).$$

V.6 Kokonaisalueet, karakteristika

Määr.: Renkaan R alkio $a \in R$ on **nollanjakaja**, jos $a \neq 0_R$ ja $\exists b \in R$, $b \neq 0_R$, s.e. $ab = 0_R$ tai $ba = 0_R$.

Esim.: a) $\mathbb{Z}$:ssä ei ole nollanjakajia (tulon nollasääntö $\Rightarrow$ $k \cdot l = 0$ vain, kun $k = 0$ tai $l = 0$).

b) $[3]_{12} \in \mathbb{Z}_{12}$ on nollanjakaja, sillä $[3]_{12} \cdot [4]_{12} = [0]_{12}$.

c) $R \neq \{0\}$ rengas $\Rightarrow$ $(1,0)$ ja $(0,1)$ ovat nollanjakajia tulorenkaassa $R \times R$ $((1,0) \cdot (0,1) = (1 \cdot 0, 0 \cdot 1) = (0,0)$.

d) $\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \cdot \begin{pmatrix} 6 & 2 \\ -3 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$ on nollanjakaja $M_2(R)$:ssä.

Lemma: Ol. R rengas ja $a \in R$, $a \neq 0$.

a) a ei nollanjakaja $\Leftrightarrow$ kuvaukset $x \mapsto ax$ ja $y \mapsto ya$ ovat injektioita $R \to R$.

b) $a \in R^*$ (ts. a käänteyvä) $\Rightarrow$ a ei nollanjakaja.

Tod.: a) $\Rightarrow$: Ol. a ei nollanjak. $ax = ax' \Rightarrow a(x - x') = 0 \Rightarrow x - x' = 0 \Rightarrow x = x'$. Siis $x \mapsto ax$ on injektio, ja samoin $y \mapsto ya$.

$\Leftarrow$: Ol. a on nollanjak. jos $ab = 0 = a \cdot 0$ jollakin $b \neq 0$, niin $x \mapsto ax$ ei ole inj.; samoin $ba = 0$, $b \neq 0 \Rightarrow y \mapsto ya$ ei inj.

b) $a \in R^* \Rightarrow x \mapsto ax$ ja $y \mapsto ya$ ovat jopa bijektioita $R \to R$ (käänt. kuv. $x \mapsto a^{-1}x$ ja $y \mapsto ya^{-1}$). □

Määr.: Komm. rengas $R \neq \{0_R\}$ (siis $1_R \neq 0_R$), jossa ei ole nollanjakajia, on kokonaisalue.

Kok.alueessa R pätee siis tulon nollasääntö: $a, b \in R$, $ab = 0 \Rightarrow a = 0$ tai $b = 0$ (ts. $a \neq 0 \neq b \Rightarrow ab \neq 0$). Samoin pätee supistussääntö (ks. Lemma, a): $a, b, c \in R$, $a \neq 0$, $ab = ac \Rightarrow b = c$.

Esim.: a) $\mathbb{Z}$ on kokonaisalue (siellä voimassa tulon nollasääntö). Jokainen renkaista $R = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ on myös kok.alue; näissä nim. $R^* = R \setminus \{0\}$, joten Lemma, b) $\Rightarrow$ ei nollantekijöitä.

b) Kok.alueen jokainen alirengas on kok.alue (tod. triv.). Siten mm. jokainen $\mathbb{R}$:n alirengas on kok.alue.

Lause: Olk. $n \in \mathbb{N}_+$. Silloin $\mathbb{Z}_n$ on kok.alue $\Leftrightarrow$ n on alkuluku.

Tod.: $\Rightarrow$: Or. n ei alkuluku $\Rightarrow n = k \cdot l$, missä $1 < k < n$ ja $1 < l < n$. Tällöin $[k]_n \neq [0]_n \neq [l]_n$, mutta $[k]_n \cdot [l]_n = [kl]_n = [n]_n = [0]_n$. $\therefore \mathbb{Z}_n$ ei kok.alue.

$\Leftarrow$: Or. $n = p$ alkuluku. Tällöin $\mathbb{Z}_p^* = \{[a]_p \mid \mathrm{syt}(a,p) = 1\} = \{[1]_p, [2]_p, \ldots, [p-1]_p\} = \mathbb{Z}_p \setminus \{[0]_p\}$ $\Rightarrow$ mikään $[a]_p$ ei nollanjak. $\Rightarrow \mathbb{Z}_p$ kok.alue. □

Esim. 6: Tark. yhtälöä $x^3 + 10x = 0$ $\mathbb{Z}_5$:ssä ja $\mathbb{Z}_7$:ssä (jolloin 10 tarkoittaa jäännösluokkaa $\overline{10}$). 5 ja 7 alkulukuja $\Rightarrow \mathbb{Z}_5$ ja $\mathbb{Z}_7$ molemmat kok.alueita.

a) $\mathbb{Z}_5$: ssä. $x^3 + 10x = x^3 = 0 \Leftrightarrow x = 0$ $(= [0]_5)$.

b) $\mathbb{Z}_7$: ssä. $x^3 + 10x = x(x^2+10) = x(x^2+3)$ $= x(x^2-4) = x(x-2)(x+2) = 0 \Leftrightarrow x = 0$ tai $x - 2 = 0$ tai $x + 2 = 0 \Leftrightarrow x = 0, 2$ tai 5 $(\in \mathbb{Z}_7!)$.

Or. R kokonaisalue. Aiemmin on määritelty renkaanhomom. $\mu: \mathbb{Z} \to R$, $\mu(m) = m \cdot 1_R$ $\forall m \in \mathbb{Z}$. Ydin $\ker(\mu)$ on $\mathbb{Z}$:n ideaali $\Rightarrow \exists n \in \mathbb{N}$ s.e. $\ker(\mu) = n\mathbb{Z}$. Jos $n = 0$, μ on injektio, ts. $m \cdot 1_R \neq 0_R$ $\forall m \in \mathbb{Z} \setminus \{0\}$, ja $\mathbb{Z} \cong \mathrm{Im}(\mu) \subset R$ (alirengas). Jos taas $n > 0$,

$\min n = \min\{m \in \mathbb{N}_+ \mid m \cdot 1_R = 0_R\}$ ja μ indusoi renkaisomorfismin $\mathbb{Z}_n \xrightarrow{\sim} \mathrm{Im}(\mu)$. $\mathrm{Im}(\mu)$ R:n alirengas $\Rightarrow$ $\mathrm{Im}(\mu)$ kok. alue $\Rightarrow$ $\mathbb{Z}_n$ kok. alue $\Rightarrow$ n alkuluku.

Määr.: Kok. alueen R karakteristika on

$$\mathrm{char}(R) = \begin{cases} 0, & \text{jos } m \cdot 1_R \neq 0_R \ \forall m \in \mathbb{N}_+ \\ \min\{m \in \mathbb{N}_+ \mid m \cdot 1_R = 0_R\}, & \text{muulloin.} \end{cases}$$

Lause 11: Jos yllä $\mathrm{char}(R) \neq 0$, niin $\mathrm{char}(R)$ on alkuluku. Tod. yllä. □

Esim. 7: $\mathrm{char}(\mathbb{Z}) = \mathrm{char}(\mathbb{Q}) = \mathrm{char}(\mathbb{R}) = \mathrm{char}(\mathbb{C}) = 0$;
$\mathrm{char}(\mathbb{Z}_p) = p$, kun p on alkuluku.

Huom.: Ol. R kok. alue. Tark. alkioiden kertalukuja ryhmässä $(R, +)$. Määr. mukaan $\mathrm{char}(R) = 0$, jos $\mathrm{ord}(1_R) = \infty$, ja $\mathrm{char}(R) = \mathrm{ord}(1_R)$, jos $\mathrm{ord}(1_R) < \infty$. Itse asiassa $\mathrm{ord}(1_R) = \mathrm{ord}(a)$ $\forall a \in R \setminus \{0_R\}$, sillä

$$m \cdot a = 0_R \Leftrightarrow (m \cdot 1_R) \cdot a = 0_R \quad \text{(Lause 3)}$$
$$\Leftrightarrow m \cdot 1_R = 0_R \quad (R \text{ kok. alue}, a \neq 0_R).$$

Esim. 8: Ol. p alkuluku ja $1 \leq k \leq p-1$.
V. $p \mid \binom{p}{k}$.

T. $\binom{p}{k} = \dfrac{p(p-1)\cdot\ldots\cdot(p-k+1)}{1 \cdot 2 \cdot 3 \cdot \ldots \cdot k}$, tunnetusti tämä $\in \mathbb{N}_+$.

p on osittajan alkutekijä, ei nimittäjän alkutekijä $\Rightarrow$ p on osamäärän tekijä. □

Ol. R kok. alue, $\mathrm{char}(R) = p > 0$, $a, b \in R$. Silloin

$$(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \ldots + \binom{p}{p-1}ab^{p-1} + b^p$$
$$= a^p + b^p \quad (px = 0_R \ \forall x \in R).$$

Jos erit. $\mathrm{char}(R) = 3$ ja $x, y \in R$, niin

$$x^3 + y^3 = 0_R \Leftrightarrow (x+y)^3 = 0_R \Leftrightarrow x + y = 0_R$$
$$\Leftrightarrow x = -y.$$