8. Renkaat

Tarkastelemme seuraavaksi rakenteita, joissa on määritelty kaksi assosiatiivista laskutoimitusta, joista toinen on kommutatiivinen. Vaadimme näillä laskutoimituksilla varustetulta joukolta joitakin samoja ominaisuuksia joita kokonaisluvuilla on, mutta kertolasku ei välttämättä ole kommutatiivinen.

Määritelmä 8.1. Olkoon $R \neq \emptyset$ joukko, jolla on määritelty kaksi assosiatiivista laskutoimitusta, kommutatiivinen laskutoimitus yhteenlasku $+$ ja toinen laskutoimitus, jota merkitsemme kertolaskulla. Kolmikko $(R, +, \cdot)$ on *(ykkösellinen) rengas*, jos

(1) $(R, +)$ on kommutatiivinen ryhmä,
(2) kertolasku on distributiivinen yhteenlaskun suhteen ja
(3) kertolaskulla on neutraalialkio $1 = 1_R \in R$.

Laskutoimituksen $+$ neutraalialkiolle käytetään merkintää $0 = 0_R$. Ryhmä $(R, +)$ on renkaan R *additiivinen ryhmä*. Rengas on *kommutatiivinen*, jos kertolasku on kommutatiivinen.

Kertolaskun distributiivisuus yhteenlaskun suhteen renkaassa R tarkoittaa, että kaikille $a, b, c \in R$ pätee $a(b + c) = ab + ac$ ja $(b + c)a = ba + ca$.

Esimerkki 8.2. (a) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ ja $(\mathbb{C}, +, \cdot)$ ovat kommutatiivisia renkaita.

(b) Olkoon $q \in \mathbb{N}$. Kongruenssiluokkien muodostama joukko $\mathbb{Z}/q\mathbb{Z}$ varustettuna kokonaislukujen yhteen- ja kertolaskujen tekijälaskutoimituksilla on kommutatiivinen rengas. (Harjoitustehtävä 81)

(c) Olkoon $X \neq \emptyset$, ja olkoon R rengas. Olkoon $\mathscr{F}(X, R)$ joukko, joka koostuu kaikista kuvauksista joukolta X renkaaseen R. Määritellään tässä joukossa yhteen- ja kertolasku pisteittäin: Olkoot $f, g \in \mathscr{F}(X, R)$. Asetamme

$$(f + g)(x) = f(x) + g(x) \quad \text{ja} \quad (fg)(x) = f(x)g(x)$$

kaikilla $x \in X$. Joukko $\mathscr{F}(X, R)$ varustettuna näillä laskutoimituksilla on rengas, jota kutsutaan *funktiorenkaaksi*. Laskutoimitusten assosiatiivisuus, yhteenlaskun kommutatiivisuus ja kertolaskun distributiivisuus yhteenlaskun suhteen seuraa siitä, että funktioiden arvot ovat renkaassa R ja funktioiden laskutoimitukset on määritelty pisteittäin. Kertolaskun neutraalialkio on vakiofunktio $1\colon X \to R$, joka määritellään asettamalla $1(x) = 1 \in R$ kaikilla $x \in X$.

Tässä esimerkissä merkitsemme kuten on tapana renkaan $\mathscr{F}(X, R)$ yhteen- ja kertolaskuja samoilla merkinnöillä $+$ ja $\cdot$ kuin renkaan R laskutoimituksia. Samoin yhteen- ja kertolaskun neutraalialkioille on tapana käyttää merkintöjä 0 ja 1 useimmissa renkaissa.

Rengas $\mathscr{F}(X, R)$ on kommutatiivinen, jos R on kommutatiivinen. Esimerkiksi siis $\mathscr{F}(\mathbb{R}, \mathbb{R})$ on kommutatiivinen rengas.

Propositio 8.3. *Olkoon R rengas. Tällöin*

(1) $0_R \cdot x = 0_R$ *kaikilla* $x \in R$,
(2) $x(-y) = (-x)y = -(xy)$ *kaikilla* $x, y \in R$,
(3) $x(y - z) = xy - xz$ *ja* $(y - z)x = yx - zx$ *kaikilla* $x, y, z \in R$,

Todistus. (1) Distributiivisuuden nojalla

$$0_R x + x = (0_R + 1_R)x = 1_R x = x$$

kaikilla $x \in R$. Supistussäännöstä seuraa, että $0_R x = 0_R$.

Loput todistetaan harjoitustehtävässä 83. □

Edellä osoitettujen laskusääntöjen avulla on helppo osoittaa seuraavat perusominaisuudet

Propositio 8.4. *Olkoon R rengas. Jos $\#R \geq 2$, niin*

(1) $0 \neq 1$ *ja*
(2) *yhteenlaskun neutraalialkiolla* 0 *ei ole käänteisalkiota kertolaskun suhteen.*

Todistus. (1) Jos $1 = 0$, niin kaikille $x \in R$ pätee Proposition 8.3 nojalla

$$x = 1\,x = 0\,x = 0.$$

Toinen väite todistetaan harjoitustehtävänä 85. □

Renkaan yhteen- ja kertolaskuiksi kutsuttujen laskutoimitusten ei tarvitse olla tavanomaisia lukujen yhteen- ja kertolaskuja tai näistä lukujen 1 ja 3 konstruktioilla muodostettuja laskutoimituksia vaan ne voivat olla mitä tahansa laskutoimituksia, joilla on vaaditut ominaisuudet.

Esimerkki 8.5. (a) Olkoon $(A, +)$ kommutatiivinen ryhmä. Olkoon

$$\mathrm{Hom}(A, A) = \{\phi\colon A \to A : \phi \text{ on homomorfismi}\}.$$

Varustamme joukkoon $\mathrm{Hom}(A, A)$ kahdella laskutoimituksella: Homomorfismien yhteenlasku määritellään asettamalla

$$(\phi + \phi')(a) = \phi(a) + \phi'(a),$$

ja kertolaskuna käytetään homomorfismien yhdistämistä. Yhteenlasku on laskutoimitus: Jos $\phi, \phi' \in \mathrm{Hom}(A, A)$, niin

$$\begin{aligned}(\phi + \phi')(a + b) &= \phi(a + b) + \phi'(a + b) = \phi(a) + \phi(b) + \phi'(a) + \phi'(b)\\ &= (\phi + \phi')(a) + (\phi + \phi')(b),\end{aligned}$$

joten $\phi + \phi' \in \mathrm{Hom}(A, A)$. Laskutoimituksella varustettu joukko $(\mathrm{Hom}(A, A), +)$ on kommutatiivinen ryhmä. Laskutoimituksen assosiatiivisuus ja kommutatiivisuus osoitetaan harjoitustehtävässä 84. Homomorfismien yhteenlaskun neutralialkio on nollahomomorfismi 0, $0(a) = 0$ kaikille $a \in A$, ja homomorfismin ϕ käänteisalkio yhteenlaskun suhteen on homomorfismi $-\phi$, joka määritellään asettamalla $(-\phi)(a) = -\phi(a)$ kaikilla $a \in A$

Identtinen homomorfismi on homomorfismien kertolaskun neutraalialkio, joten tarkastettavaksi jää kertolaskun distributiivisuus yhteenlaskun suhteen: Jos $\phi, \psi, \zeta \in \mathrm{Hom}(A, A)$,niin

$$(\psi + \zeta)\phi(a) = \psi\phi(a) + \zeta\phi(a) = (\psi\phi + \zeta\phi)(a),$$

ja

$$\phi(\psi + \zeta)(a) = \phi(\psi(a) + \zeta(a)) = \phi\psi(a) + \phi\zeta(a) = (\phi\psi + \phi\zeta)(a).$$

Koska homomorfismien yhdistäminen on renkaan $\mathrm{Hom}(A, A)$ kertolasku, homomorfismien yhdistetty kuvaus on yllä merkitty ilman yhdistetyn kuvauksen merkkiä $\circ$.

(b) Olkoon R rengas, $\#R \geq 2$. Kaikkien R-kertoimisten $n \times n$-matriisien joukko $\mathrm{M}_n(R)$ varustettuna matriisien yhteen- ja kertolaskulla on rengas. Kaikki muut ominaisuudet paitsi distributiivisuus osoitettiin tapauksessa $n = 2$ ja $R = \mathbb{R}$ Esimerkissä 1.13(b) ja harjoitustehtävässä 4. Kun $n \geq 2$, niin $\mathrm{M}_n(R)$ ei ole kommutatiivinen rengas, koska matriisien kertolasku ei ole kommutatiivinen.

Määritelmä 8.6. Jos R on rengas ja alkiolla $u \in R$ on käänteisalkio kertolaskun suhteen, niin u on renkaan R *yksikkö*. Renkaan R *yksiköiden ryhmä* (tai *multiplikatiivinen ryhmä*) on

$$R^\times = \{u \in R : u \text{ on yksikkö}\}$$

varustettuna renkaan R kertolaskun indusoimalla laskutoimituksella.

Propositio 8.7. *Renkaan yksiköiden joukko varustettuna kertolaskulla on ryhmä.*

Todistus. Renkaan R kertolasku on assosiatiivinen laskutoimitus, jonka neutraalialkio on 1. Yksiköiden joukko on vakaa kertolaskun suhteen: Jos u ja v ovat yksiköitä, niin uv on yksikkö koska

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

Kertolasku on siis assosiatiivinen laskutoimitus yksiköiden joukossa. Laskutoimituksella on neutraalialkio koska 1 on yksikkö. Määritelmän mukaan jokaisella yksiköllä u on käänteisalkio u^{-1} renkaassa R. Myös u^{-1} on yksikkö koska $(u^{-1})^{-1} = u$. □

Jos renkaassa on ainakin kaksi alkiota, niin $0 \neq 1$ ja 0 ei ole yksikkö.

Määritelmä 8.8. Olkoon R rengas, jossa on ainakin kaksi alkiota. Jos kaikki renkaan R nollasta poikkeavat alkiot ovat yksiköitä, niin R on *jakorengas*. Kommutatiivinen jakorengas on *kunta*. Jakorengas, joka ei ole kunta on *vino kunta*.

Määritelmä 8.9. Olkoon R rengas, $\#R \geq 2$.

(1) Jos $a, b, c \in R$ siten, että $ab = c$, niin a ja b ovat alkion c *tekijöitä*.
(2) Jos $a, b \in R$, $a, b \neq 0$, ja $ab = 0$, niin a ja b ovat *nollan jakajia*.
(3) Jos renkaassa R ei ole nollan jakajia, ja R on kommutatiivinen, niin R on *kokonaisalue*.

Jos $d, m \in R$ ja d on alkion m tekijä sanotaan joskus, että d jakaa alkion m ja merkitään $d \mid m$.

Esimerkki 8.10. (a) $\mathbb{Z}$ on kokonaisalue mutta se ei ole jakorengas eikä siis kunta. Renkaan $\mathbb{Z}$ ainoat yksiköt ovat ± 1.

(b) $\mathbb{Q}$, $\mathbb{R}$ ja $\mathbb{C}$ ovat kuntia.

(c) Matriisirengas $\mathrm{M}_n(R)$ ei ole kokonaisalue, kun $n \geq 2$, koska monella matriisilla ei ole käänteismatriisia. Esimerkiksi $\mathrm{M}_n(\mathbb{R})^\times = \mathrm{GL}_n(\mathbb{R})$.

(d) *Hamiltonin kvaterniot* on joukko

$$\mathbb{H} = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \in \mathrm{M}_2(\mathbb{C}) \right\}.$$

varustettuna matriisien yhteenlaskulla ja matriisien kertolaskulla. Suoraviivainen lasku osoittaa, että $\mathbb{H}$ vakaa yhteenlaskun ja kertolaskun suhteen ja että se on rengas renkaasta $\mathrm{M}_2(\mathbb{C})$ indusoiduilla laskutoimituksilla. Lisäksi

$$\det \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} = |a|^2 + |b|^2,$$

joten jokainen $A \in \mathbb{H} \setminus \{0\}$ on kääntyvä matriisi. Lisäksi

$$\frac{1}{|a|^2 + |b|^2} \begin{pmatrix} \bar{a} & -b \\ \bar{b} & a \end{pmatrix} \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} = I_2,$$

joten kaikki nollasta poikkeavat alkiot ovat yksiköitä. Jakorengas $\mathbb{H}$ ei ole kommutatiivinen sillä esimerkiksi

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = - \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}.$$

Siis Hamiltonin kvaterniot on vino kunta.

Injektiivinen kuvaus $\phi\colon \mathbb{C} \to \mathbb{H}$, $\phi(z) = \operatorname{diag}(z, \bar{z})$ on homomorfismi yhteenlaskun ja kertolaskun suhteen, joten voimme samastaa sen kuvajoukon

$$\phi(\mathbb{C}) = \left\{ \begin{pmatrix} z & 0 \\ 0 & \bar{z} \end{pmatrix} \in \mathrm{M}_2(\mathbb{C}) \right\}.$$

kompleksilukujen kunnan kanssa. Kvaternioita käsitellessä onkin tapana käyttää esimerkiksi merkintöjä

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Tällöin

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1 \tag{7}$$

ja

$$\mathbf{ij} = \mathbf{k} = -\mathbf{ji}, \quad \mathbf{ki} = \mathbf{j} = -\mathbf{ik}, \quad \mathbf{jk} = \mathbf{i} = -\mathbf{kj}. \tag{8}$$

Matriisit 1, $\mathbf{i}$, $\mathbf{j}$ ja $\mathbf{k}$ virittävät avaruuden $\mathbb{H}$ neliulotteisena reaalisena vektoriavaruutena, joten Hamiltonin kvaterniot voidaan esittää reaalisina lineaarikombinaatioina

$$x = x_0 + x_1\mathbf{i} + x_2\mathbf{j} + x_3\mathbf{k},$$

$x_0, x_1, x_2, x_3 \in \mathbb{R}$, joilla voi laskea kuten kompleksiluvuilla huomioiden laskusäännöt (7) ja (8).

Esimerkki 8.11. Jos $A, B \in \mathrm{M}_n(R)$, ja niiden ainoat nollasta poikkeavat kertoimet ovat A_{11} ja B_{nn}, niin $AB = 0$. Siis matriisit A ja B ovat nollan jakajia.

Propositio 8.12. *Jakorenkaassa ei ole nollan jakajia. Erityisesti kunta on kokonaisalue.*

Todistus. Olkoon K jakorengas. Olkoot $a, b \in K$, $a, b \neq 0$. Tällöin a ja b ovat yksiköitä, joten niillä on käänteisalkiot kertolaskun suhteen. Oletetaan, että $ab = 0$. Silloin $b = a^{-1}0 = 0$, mikä on ristiriita. □

Lause 8.13. *Äärellinen kokonaisalue on kunta.*

Todistus. Olkoon E äärellinen kokonaisalue. Olkoon $a \in E$, $a \neq 0$. Kuvaus $\ell_a : E \to E$, $\ell_a(x) = ax$ on injektio: Jos $\ell_a(x) = \ell_a(y)$, niin $a(x - y) = 0$. Koska kokonaisalueessa E ei ole nollan jakajia, $x = y$. Kuvaus ℓ_a on surjektio, koska E on äärellinen. Siis on $\bar{a} \in E$, jolle $a\bar{a} = 1$. Koska E on kommutatiivinen, $\bar{a} = a^{-1}$. □

Määritelmä 8.14. Olkoot R ja R' renkaita. Kuvaus $\phi : R \to R'$ on rengashomomorfismi, jos

- ϕ on homomorfismi yhteenlaskulle ja kertolaskulle ja
- $\phi(1) = 1$.

Bijektiivinen rengashomomorfismi on *rengasisomorfismi*. Jos renkaat R ja R' ovat kuntia, sanotaan rengashomomorfismia $\phi\colon R \to R'$ *kuntahomomorfismiksi*.

Propositiossa 1.14 osoitettiin, että surjektiivinen homomorfismi kuvaa neutraalialkion neutraalialkioksi, mutta ilman surjektiivisuutta näin ei välttämättä ole. Ryhmähomomorfismille ei tarvita vastaavaa vaatimusta Proposition **??** nojalla. Erityisesti siis rengashomomorfismi kuvaa nollan nollaksi.

Esimerkki 8.15. (a) Luonnollinen kuvaus renkaasta $(\mathbb{Z}, +, \cdot)$ renkaaseen $(\mathbb{Z}/q\mathbb{Z}, +, \cdot)$ on surjektiivinen rengashomomorfismi.
(b)Kuvaus $h\colon \mathscr{F}(\mathbb{R}, \mathbb{R}) \to \mathbb{R}$, $h(f) = f(\frac{1}{2})$ on rengashomomorfismi:

$$h(f+g) = (f+g)(1/2) = f(1/2) + g(1/2) = h(f) + h(g),$$
$$h(fg) = (fg)(1/2) = f(1/2)g(1/2) = h(f)h(g)$$

ja

$$h(1) = 1(1/2) = 1.$$

Propositio 8.16. *(1) Jos $f\colon R \to S$ ja $g\colon S \to T$ ovat rengashomomorfismeja, niin $g \circ f$ on rengashomomorfismi.*
(2) Rengashomomorfismi $f\colon R \to S$ on rengasisomorfismi, jos ja vain jos on rengashomomorfismi $\bar{f}\colon S \to R$, jolle $\bar{f} \circ f = \mathrm{id}_R$ ja $f \circ \bar{f} = \mathrm{id}_S$.

Todistus. Harjoitustehtävät 86 ja 87. □

Kokonaislukujen renkaan $\mathbb{Z}$ kaikki alkiot ovat alkion 1 monikertoja. Tästä seuraa erityisominaisuus renkaassa $\mathbb{Z}$ määritellyille rengashomomorfismeille:

Propositio 8.17. *Olkoon R rengas. On täsmälleen yksi rengashomomorfismi $\phi\colon \mathbb{Z} \to R$.*

Todistus. Koska 1 virittää additiivisen ryhmän $(\mathbb{Z}, +)$, Proposition 5.13 nojalla halutunlaisia homomorfismeja on korkeintaan yksi. Väite seuraa havainnosta, että kuvaus $\phi\colon \mathbb{Z} \to R$, $\phi(n) = n1_R = 1_R + 1_R + \cdots + 1_R$, on rengashomomorfismi:

$$\phi(m+n) = (m+n)1_R = m1_R + n1_R = \phi(m) + \phi(n)$$

ja

$$\phi(mn) = mn1_R = m1_R n1_R = \phi(m)\phi(n).$$ □

Monilla renkailla on yhteen- ja kertolaskun suhteen vakaita osajoukkoja, jotka ovat renkaita.

Määritelmä 8.18. Olkoon R rengas ja olkoon $S \subset R$ vakaa yhteenlaskun ja kertolaskun suhteen. Jos S varustettuna indusoiduilla laskutoimituksilla on rengas ja jos $1_S = 1_R$, niin S on renkaan R *alirengas*. Jos R ja S ovat kuntia, niin S on kunnan R *alikunta*.

Määritelmän mukaan alirenkaan inkluusiokuvaus $i : S \to R$, $i(s) = s$ on rengashomomorfismi.

Esimerkki 8.19. (a) $\mathbb{Z}$ on renkaan $\mathbb{Q}$ alirengas.
(b) Joukko

$$S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{R} \right\} \subset \mathrm{M}_2(\mathbb{R})$$

on rengas renkaasta $\mathrm{M}_2(\mathbb{R})$ indusoiduilla laskutoimituksilla. Sen kertolaskun neutraalialkio on $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, joten S ei ole renkaan $\mathrm{M}_2(\mathbb{R})$ alirengas. Rengas S on rengasisomorfinen renkaan $\mathbb{R}$ kanssa: Kuvaus $a \mapsto \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ on rengasisomorfismi.

Alirenkaalle on samanlainen testi kuin aliryhmälle (Propositio 5.11).

Propositio 8.20. *Olkoon R rengas, ja olkoon $S \subset R$, $S \neq \emptyset$. Tällöin S on renkaan R alirengas, jos ja vain jos*

(1) *Kaikille $x, y \in S$ $x + y \in S$ ja $xy \in S$, ja*

(2) $-1 \in S$.

Todistus. Harjoitustehtävä 90. □

Esimerkki 8.21. (a) Samaan tapaan kuin permutaatioryhmille määriteltiin aliryhmiä rajoittumalla kuvauksiin, joilla on tiettyjä ominaisuuksia, voimme määritellä funktiorenkaiden $\mathscr{F}(X, R)$ alirenkaita. Kurssilla Analyysi 2 osoitetaan, että indusoiduilla laskutoimituksilla varustetut joukot

$$C(\mathbb{R}) = \{f\colon \mathbb{R} \to \mathbb{R} : f \text{ on jatkuva}\}, \text{ ja}$$
$$C^k(\mathbb{R}) = \{f\colon \mathbb{R} \to \mathbb{R} : f \text{ on } k \text{ kertaa jatkuvasti derivoituva}\},\ k \in \mathbb{N}.$$

ovat funktiorenkaan $\mathscr{F}(\mathbb{R}, \mathbb{R})$ alirenkaita

(b) Vektoriavaruuden $\mathbb{R}^n$ lineaarikuvaukset muodostavat renkaan $\mathrm{Hom}(\mathbb{R}^n, \mathbb{R}^n)$ alirenkaan

$$\mathrm{End}(\mathbb{R}^n) = \{L : \mathbb{R}^n \to \mathbb{R}^n : L \text{ on lineaarikuvaus}\}.$$

Lineaarikuvaukset ovat ryhmän $(\mathbb{R}^n, +)$ homomorfismeja itselleen, joten niiden summa on myös homomorfismi. Lisäksi aina, kun $L, L' \in \mathrm{End}(\mathbb{R}^n)$, $x \in \mathbb{R}^n$ ja $a \in \mathbb{R}$, myös

$$\begin{aligned}(L + L')(ax) &= L(ax) + L'(ax) = aL(x) + aL'(x) = a(L(x) + L'(x)) \\ &= a(L + L')(x),\end{aligned}$$

joten lineaarikuvauksen toinenkin ehto toteutuu. Lineaarialgebran kurssilla on osoitettu, että lineaarikuvausten yhdistetty kuvaus on lineaarikuvaus. Siis molemmat laskutoimitukset toteuttavat Proposition 8.20 ehdon (1). Lisäksi identtinen kuvaus $\mathrm{id}\colon \mathbb{R}^n \to \mathbb{R}^n$ on lineaarikuvaus, kuten myös $-\mathrm{id}$, joten Proposition 8.20 mukaan $\mathrm{End}(\mathbb{R}^n)$ on renkaan $\mathrm{Hom}(\mathbb{R}^n, \mathbb{R}^n)$ alirengas.

(c) Esimerkissä 4.13 käsitelty kuvaus $\mathrm{Mat}\colon \mathrm{End}(\mathbb{R}^n) \to \mathrm{M}_n(\mathbb{R})$, joka liittää lineaarikuvaukseen L sen matriisin kiinnitetyssä kannassa, on rengasisomorfismi. Jos $L, L' \in \mathrm{End}(\mathbb{R}^n)$, niin $(L + L')(v) = Lv + L'v$, joten

$$\mathrm{Mat}(L + L') = \mathrm{Mat}(L) + \mathrm{Mat}(L'),$$

eli Mat on ryhmähomomorfismi additiivisten ryhmien välillä. Lisäksi kaikille lineaarikuvauksille $L, L' \in \mathrm{End}(\mathbb{R}^n)$ pätee

$$\mathrm{Mat}(L'L) = \mathrm{Mat}(L')\,\mathrm{Mat}(L)$$

ja identtisen kuvauksen matriisi on I_n.

Alirenkaat ja rengashomomorfismit ovat yhteensopivia samaan tapaan kuin aliryhmät ja ryhmähomomorfismit:

Propositio 8.22. *Olkoon $\phi\colon R \to R'$ rengashomomorfismi.*
(1) Jos S on renkaan R alirengas, niin $\phi(S)$ on renkaan R' alirengas.
(2) Jos S' on renkaan R' alirengas, niin $\phi^{-1}(S')$ on renkaan R alirengas.

Todistus. (1) Proposition 5.6 mukaan $(\phi(S), +)$ on ryhmä, joten Propositiota 8.20 sovellettaessa riittää tarkastella kertolaskua ja kertolaskun neutraalialkion kuvautumista. Olkoot $\phi(a), \phi(b) \in \phi(S)$. Tällöin

$$\phi(a)\phi(b) = \phi(ab) \in \phi(S).$$

Koska $-1_R \in S$, pätee

$$\phi(-1_R) = -\phi(1_R) = -1_{R'} \in \phi(S).$$

Siis Proposition 8.20 oletukset ovat voimassa.
(2) Harjoitustehtävä 91. □

Harjoitustehtäviä.

Tehtävä 81. Osoita, että $\mathbb{Z}/q\mathbb{Z}$ varustettuna kokonaislukujen yhteen- ja kertolaskujen tekijälaskutoimituksilla on kommutatiivinen rengas.

Tehtävä 82. Olkoon X joukko. Määritellään joukkojen $A, B \in \mathscr{P}(X)$ *symmetrinen erotus* asettamalla

$$A \triangle B = (A \setminus B) \cup (B \setminus A).$$

Osoita, että $\big(\mathscr{P}(X), \triangle, \cap\big)$ on rengas. Onko se kommutatiivinen?

Tehtävä 83. Olkoon R rengas. Osoita, että

(1) $x(-y) = (-x)y = -(xy)$ kaikilla $x, y \in R$,
(2) $x(y-z) = xy - xz$ ja $(y-z)x = yx - zx$ kaikilla $x, y, z \in R$,

Tehtävä 84. Olkoon $(A, +)$ kommutatiivinen ryhmä. Osoita, että joukon $\mathrm{Hom}(A, A)$ laskutoimitus $+$, joka määritellään asettamalla

$$(\phi + \phi')(a) = \phi(a) + \phi'(a),$$

on assosiatiivinen ja kommutatiivinen.

Tehtävä 85. Olkoon $R \neq \{0\}$ rengas. Osoita, että yhteenlaskun neutraalialkiolla 0 ei ole käänteisalkiota kertolaskun suhteen.

Tehtävä 86. Olkoot $f\colon R \to S$ ja $g\colon S \to T$ rengashomomorfismeja. Osoita, että $g \circ f$ on rengashomomorfismi.

Tehtävä 87. Osoita, että rengashomomorfismi $f\colon R \to S$ on rengasisomorfismi, jos ja vain jos on rengashomomorfismi $\bar{f}\colon S \to R$, jolle $\bar{f} \circ f = \mathrm{id}_R$ ja $f \circ \bar{f} = \mathrm{id}_S$.

Tehtävä 88. Määritellään joukossa $\mathbb{Z}^3$ yhteenlasku komponenteittain ja kertolasku asettamalla

$$(a, b, c)(x, y, z) = (ax, bx + cy, cz)$$

kaikilla $(a, b, c), (x, y, z) \in \mathbb{Z}^3$. Onko $\mathbb{Z}^3$ varustettuna näillä laskutoimituksilla rengas? Onko se kommutatiivinen?

Tehtävä 89. Ovatko funktiorenkaat $\mathscr{F}\big([0,1], \mathbb{R}\big)$ ja $\mathscr{F}\big([0,2], \mathbb{R}\big)$ isomorfisia?

Tehtävä 90. Olkoon R rengas, ja olkoon $S \subset R$, $S \neq \emptyset$. Osoita, että S on renkaan R alirengas, jos ja vain jos

- $x + y \in S$ ja $xy \in S$ kaikilla $x, y \in S$, ja
- $-1 \in S$.

Tehtävä 91. Olkoon $\phi\colon R \to R'$ rengashomomorfismi. Olkoon S' renkaan R' alirengas. Osoita, että $\phi^{-1}(S')$ on renkaan R alirengas.

Tehtävä 92. Olkoon K kunta, ja olkoon $K' \subset K$ vakaa osajoukko, joka on kunta indusoiduilla laskutoimituksilla. Osoita, että kunnan K' yhteenlaskun ja kertolaskun neutraalialkiot ovat samat kuin kunnan K.

Tehtävä 93. Osoita, että kunnan K osajoukko K' on alikunta, jos ja vain jos

- $\#K' \geq 2$,
- $a - b \in K'$ kaikilla $a, b \in K'$, ja
- $ab^{-1} \in K'$ kaikilla $a, b \in K'$, $b \neq 0$.

[82] Vihje: Harjoitustehtävä 27.
[88] Vihje: $(1, 0, 1)$

Tehtävä 94. Olkoon

$$K = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathrm{M}_2(\mathbb{R}) \right\}$$

Osoita, että K varustettuna matriisien yhteen- ja kertolaskulla on kunta. Osoita, että kunta K on isomorfinen kompleksilukujen kunnan kanssa.

Tehtävä 95. Olkoot *Gaussin kokonaisluvut*

$$\mathbb{Z}[i] = \{a + ib \in \mathbb{C} : a, b \in \mathbb{Z}\},$$

ja *Gaussin rationaaliluvut*

$$\mathbb{Q}(i) = \{a + ib \in \mathbb{C} : a, b \in \mathbb{Q}\}.$$

Osoita, että $\mathbb{Z}[i]$ on rengas ja että $\mathbb{Q}(i)$ on kunta.

Tehtävä 96. Määritä Gaussin kokonaislukujen yksiköiden ryhmä.

Tehtävä 97. Osoita, että

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \in \mathbb{R} : a, b \in \mathbb{Z}\},$$

on reaalilukujen renkaan alirengas.

Tehtävä 98. Osoita, että $\mathbb{Z}[\sqrt{2}]^\times$ on ääretön.

[96]Vihje: Käytä kompleksilukujen normin ominaisuuksia.

[98]Vihje: Etsi sopiva yksikkö ja käytä Propositiota 8.7