Renkaat toisessa ulottuvuudessa

LuK-tutkielma
Niko Kulmala
2501248
Matematiikan tieteiden laitos
Oulun yliopisto
kevät 2021

Sisällys

1 Johdanto **2**

2 Ryhmä **3**

3 Rengas **7**
3.1 Renkaan perusteet 7
3.2 Renkaan ideaali 8
3.3 Tekijärengas 9
3.4 Rengashomomorfismi 12
3.5 Kunnan teoriaa 15

4 Toisenlaiset operaatiot **17**

1 Johdanto

Tämän tutkielman aiheena on algebrallisten renkaiden erilaiset ryhmät ja sekä niiden operaatiot. Tarkoituksena on tutkia joukkoja, joita ryhmä- ja rengasteorian opetuksissa ei ole niin paljoa käytetty ja tutkia niiden käyttäytymistä renkaassa ja sen osa-alueissa. Operaatiot itsessään omat samankaltaisia kuin ennenkin, mutta ryhmän alkioista johtuen ne soveltuvat niihin hieman eri tavalla.

Ryhmän käsite tuli epäsuorasti käyttöön Niels Henrik Abelin ja Évariste Galoisin kautta heidän työstään polynomiyhtälöistä, joiden rationaaliset kertoimet ovat astetta viisi tai sitä suurempia.
Vuonna 1857 Karl von Staudt julkaisi hänen teoriansa, joka pystyi tuottamaan geometrisen mallin, mikä täyttää ryhmän aksioomat. Teoria tunnetaan nimellä "*Algebra of Throws*". Tätä kehitettä on usein kutsuttu yhtenä tekijänä matematiikan perusteisiin.
Vuonna 1871, Richard Dedekind esitteli joukon reaali- tai kompleksinumeroita, jotka toimivat neljän eri aritmeettisen operaation alla. Tämä joukko sai kutsumanimekseen ryhmä (*körper*). Hän määritteli myös renkaat, mutta itse termin "rengas"(*zahlring*) keksi David Hilbert. Vuonna 1893 termin "ryhmä "englannin kieleen toi Eliakim Hastings Moore.
Motivoituneena invarianttiteorian tutkimiseen David Hilbert opiskeli ideaaleita polynomisissa renkaissa todistaen hänen kuuluisan teoriansa ("*Basis Theorem*") vuonna 1893.

Työn lukemiseen suositellaan algebran ryhmien ja renkaiden peruskäsitteiden tuntemista, mutta soveltuu myös uutta tietoa omaavalle. Aliryhmät, homomorfismit ja kunnan käsitteet on hyvä tuntea.

2 Ryhmä

Määritelmä 2.1. Olkoon $G \neq \emptyset$ ja $*$ joukon operaatio. Pari $(G,*)$ on *ryhmä*, mikäli seuraavat neljä ehtoa ovat voimassa:

1. Operaatio $(*)$ on binäärinen eli

   $$a * b \in G$$

   aina, kun a, $b \in G$.

2. Operaatio $(*)$ on assosiatiivinen eli

   $$(a * b) * c = a * (b * c)$$

   aina, kun a, b, $c \in G$.

3. Joukossa G on sellainen yksiselitteinen alkio e, että

   $$a * e = e * a = a$$

   aina, kun $a \in G$. Tätä alkiota kutsutaan *neutraalialkioksi*.

4. Aina, kun $a \in G$, on olemassa sellainen yksiselitteinen alkio $a^{-1} \in G$, että

   $$a * a^{-1} = a^{-1} * a = e$$

   Alkiota a^{-1} kutsutaan alkion a *käänteisalkioksi*.

Lisäksi jos $(G, *)$ toteuttaa ehdon

5. Operaatio $(*)$ on kommutatiivinen eli

   $$a * b = b * a$$

   aina, kun a, $b \in G$.

Näin kyseessä on *Abelin ryhmä* eli kommutatiivinen ryhmä.

Määritelmä 2.2. Olkoon $(G, *)$ ja $H \subseteq G$, $H \neq \emptyset$. Jos $(H, *)$ on ryhmä, sanotaan sitä *ryhmän* $(G, *)$ *aliryhmäksi*; merkitään $(H, *) \leq (G, *)$ tai lyhyemmin $H \leq G$.

Lause 2.3. (Aliryhmäkriteeri 1). Olkoot $G, *)$ ryhmä ja $H \subseteq G$, $H \neq \emptyset$. Tällöin $H \leq G$ jos ja vain jos seuraavat ehdot toteutuvat:

1. $a, b \in H \Rightarrow a * b \in H$;
2. $a \in H \Rightarrow a^{-1} \in H$.

Lause 2.4 (Aliryhmäkriteeri 2). Olkoon $(G, *)$ ryhmä ja $H \subseteq G, H \neq \emptyset$. Tällöin $H \leq G$ jos ja vain jos seuraava ehto toteutuu:

3. $a, b \in H \Rightarrow a * b^{-1} \in H$.

Todistus. $\Rightarrow$ Olkoon nyt $H \leq G$. Tällöin H on ryhmä ja sillä on siis neutraalialkio eli H on epätyhjä. Alkio $b \in H$, joten tällöin myös $b^{-1} \in H$. Alkio $a \in H$, joten $a * b^{-1} \in H$.

$\Leftarrow$ Olkoon nyt H epätyhjä ja $a * b^{-1} \in H$ kaikilla $a, b \in H$. Olkoon e ryhmän G neutraalialkio. Jos $a \in H$, niin tällöin $a * a^{-1} = e \in H$. Tällä perusteella joukossa H on neutraalialkio. Lisäksi $a^{-1} * e = a^{-1} \in H$, joten kaikilla H:n alkioilla on käänteisalkio joukossa H. Assosiatiivisuus voidaan todeta siten, että joukon H alkiot ovat joukon G alkioita ja ovat näin ollen assosiatiivisia ryhmän $(G, *)$ binäärioperaation suhteen. Binäärisyys osoittautuu aikaisemman esimerkin avulla. Kun $a, b \in H$, niin tällöin saadaan $a * b = a * (b^{-1})^{-1} \in H$.

Näin ollen $(H, *)$ on ryhmä ja siis $H \leq G$. □

Määritelmä 2.5. Olkoon G ryhmä ja $a \in G$. Tällöin joukko

$$H = \{a^k | k \in \mathbb{Z}\}$$

on *alkion a generoima syklinen ryhmä*; merkitään $H = \langle a \rangle$. Alkio a on *generoija*.

Määritelmä 2.6 Olkoon $N \leq G$ Aliryhmää N sanotaan *normaaliksi* mikäli $a * N = N * a$ aina, kun $a \in G$. Tällöin merkitään $N \trianglelefteq G$.
Jatkossa merkitään $a * N = aN$ selkeyden vuoksi.

Määritelmä 2.7 Olkoon nyt $(N, *) \trianglelefteq (G, *)$.
Sivuluokkien joukossa $\{aN | a \in G\}$ voidaan määritellä operaatio $(*)$ seuraavasti:

$$aN * bN = (a * b)N.$$

Näin saatu operaatio $(*)$ on hyvin määritelty eli se ei ole riippuvainen sivuluokkien aN ja bN edustajista. Lisäksi sivuluokkien joukko $\{aN | a \in G\}$ yhdessä kyseisen operaation kanssa on ryhmä.

Lause 2.8 Olkoon $(G, *)$ ryhmä ja $N \trianglelefteq G$. Tällöin

$$(\{aN | a \in G\}, *)$$

on ryhmä.

Todistus. Olkoon $bN, cN, dN \in \{aN|a \in G\}$. Tutkitaan toteutuvatko ryhmän ehdot.

1. Binäärisyys:
$$bN * cN = (b * c)N \in \{aN|a \in G\},$$
eli operaatio on binäärinen.

2. Assosiatiivisuus:
$$(bN * cN) * dN = (b * c)N * dN = ((b * c)d)N$$
$$= (b * (c * d))N = bN * (c * d)N = bN * (cN * dN),$$
eli operaatio on assosiatiivinen.

3. Neutraalialkio: Nyt $e \in G$, joten $eN \in \{aN|a \in G\}$. Tällöin
$$bN * eN = (b * e)N = bN$$
ja
$$eN * bN = (e * b)N = bN$$

4. Käänteisalkio: Olkoon $b \in G$, joten $b^{-1} \in G$ ja siten $b^{-1}N \in \{aN|a \in G\}$. Nyt
$$bN * b^{-1}N = (b * b^{-1})N = eN = N$$
ja
$$b^{-1}N * bN = (b^{-1} * b)N = eN = N$$
eli alkiolla bN on käänteisalkio eli ehto toteutuu.

Täten $(\{aN|a \in G\}, *)$ on ryhmä.

□

Määritelmä 2.9 Edellä esitettyä paria $(\{aN|a \in G\}, *)$ kutsutaan ryhmän *G tekijäryhmäksi normaalin aliryhmän N suhteen.* Kyseisestä ryhmästä käytetään merkintää G/N.

Määritelmä 2.10. Olkoot $(G, \cdot)$ ja $(H, *)$ ryhmiä. Kuvausta $f : G \to H$ sanotaan *ryhmähomomorfismiksi* ryhmältä G ryhmälle H, mikäli
$$f(a \cdot b) = f(a) * f(b)$$
aina kun $a, b \in G$.

Lause 2.11 Olkoon $f : G \to H$ ryhmähomomorfismi ja olkoot e_G ja e_H ryhmien G ja H neutraalialkiot. Tällöin
$$f(e_G) = e_H$$
ja
$$f(a^{-1}) = (f(a))^{-1}$$
aina, kun $a \in G$.

Todistus. Tutkitaan ensin ensimmäistä kohtaa:

$$f(e_G) * f(e_G) = f(e_G \cdot e_G)$$

Nyt operoidaan molemmat puolet käänteisalkiolla $f(e_G)^{-1}$ ja tällöin saadaan

$$f(e_G) = e_H.$$

Nyt toinen kohta:

$$f(a) * f(a^{-1}) = (f(a \cdot a^{-1}) = f(e_G) = e_H$$

ja

$$f(a^{-1}) * f(a) = e_H.$$

Näistä huomataan, että

$$f(a^{-1}) = (f(a))^{-1}.$$

□

Eli väite on tosi.

Määritelmä 2.12. Olkoon $f : G \to H$ ryhmähomomorfismi. Joukkoa

$$Im(f) = \{f(x) | x \in G\}$$

sanotaan homomorfismin f *kuvaksi* ja joukkoa

$$Ker(f) = \{x \in G | f(x) = e_H\}$$

sanotaan homomorfismin f *ytimeksi*.

Määritelmä 2.13. Ryhmähomomorfismia $f : G \to H$ sanotaan *ryhmäisomorfismiksi*, jos f on *bijektio*. Ryhmää G sanotaan isomorfiseksi ryhmän H kanssa, jos on olemassa jokin isomorfismi $f : G \to H$. Tällöin merkitään $G \cong H$ ja sanotaan myös, että ryhmät G ja H ovat rakenneyhtäläiset.

3 Rengas

3.1 Renkaan perusteet

Määritelmä 3.1.1. Kolmikko $(R, +, \cdot)$, missä R on reaalilukujen joukko, on *rengas*, kun

1. $(R, +)$ on Abelin ryhmä:
   - $(+)$ on binäärinen operaatio joukossa R eli $a+b \in R$ kaikilla $a, b \in R$.
   - $(+)$ on assosiatiivinen operaatio eli $a + (b + c) = (a + b) + c$ kaikilla $a, b, c \in R$.
   - Joukossa R on neutraalialkio operaation $(+)$ suhteen eli on olemassa sellainen alkio $\mathbf{0} \in R$, että $a+\mathbf{0} = \mathbf{0}+a = a$. Tätä alkiota nimitetään renkaan R *nolla-alkioksi*.
   - Jokaisella joukon R alkiolla on olemassa käänteisalkio joukossa R operaation $(+)$ suhteen eli jokaiselle $a \in R$ on olemassa sellainen alkio $-a \in R$, että $a + (-a) = -a + a = \mathbf{0}$. Tätä käänteisalkiota nimitetään alkion a vasta-alkioksi.
   - $(+)$ on kommutatiivinen operaatio eli $a + b = b + a$ kaikilla $a, b \in R$.
2. $(R, \cdot)$ on monoidi:
   - $(\cdot)$ on binäärinen operaatio joukossa R eli $a \cdot b \in R$ kaikilla $a, b \in R$.
   - $(\cdot)$ on assosiatiivinen operaatio eli $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ kaikilla $a, b, c \in R$.
   - Joukossa R on neutraalialkio operaation $(\cdot)$ suhteen eli on olemassa sellainen alkio $\mathbf{1} \in R$, että $a \cdot \mathbf{1} = \mathbf{1} \cdot a = a$ kaikilla $a \in R$. Tätä alkiota nimitetään renkaan R *ykkösalkioksi*.
3. Seuraavat distributiivisuus- eli osittelulait ovat voimassa:

   $$a \cdot (b + c) = a \cdot b + a \cdot c$$

   ja

   $$(a + b) \cdot c = a \cdot c + b \cdot c$$

   aina, kun $a, b, c \in \mathbb{R}$.

Lisäksi rengasta sanotaan kommutatiiviseksi, jos se on kommutatiivinen operaation $(\cdot)$ suhteen eli jos $a \cdot b = b \cdot a$ aina, kun $a, b \in R$.
Jatkossa merkinnällä R tarkoitetaan aina reaalilukujen joukkoa.

Määritelmä 3.1.2. Olkoot $(R, +)$ rengas ja $\emptyset \neq S \subseteq R$. Jos $(S, +, \cdot)$ on rengas, jolla on sama ykkösalkio kuin renkaalla R, niin sitä sanotaan renkaan R *alirenkaaksi*.

Lause 3.1.3 (Alirengaskriteeri) Renkaan $(R, +, \cdot)$ ei-tyhjä osajoukko S on renkaan R alirengas jos ja vain jos

1. $a, b \in S \Rightarrow a - b \in S$ eli $a + (-b) \in S$.
2. $a, b \in S \Rightarrow a \cdot b \in S$.
3. $\mathbf{1}_R \in S$.

Todistus. $\Rightarrow Triviaali.$

$\Leftarrow$ Olkoon nyt S renkaan R osajoukko ja mainitut kohdat 1.-3. toteutuvat. Ehdosta 3. seuraa, että S on epätyhjä ja että sillä on ykkösalkio. Yhdessä ehdon 1. kanssa toteutuu aliryhmäkriteeri eli S on ryhmän R aliryhmä. Ehto 2. osoittaa binäärisyyden. Lisäksi koska alkiot ovat joukon R alkioita, ne toteuttavat assosiatiivisuuden ja osittelulait. □

Jatkossa käytetään operaatiosta $a \cdot b$ merkintää ab.

3.2 Renkaan ideaali

Määritelmä 3.2.1 Renkaan $(R, +, \cdot)$ ei-tyhjä osajoukko I on *ideaali*, jos

1. $(I, +) \leq (R, +)$.
2. $ra \in I$ ja $ar \in I$ aina, kun $a \in I$ ja $r \in R$.

Lause 3.2.2. Jos I on renkaan R ideaali ja $\mathbf{1}_R \in I$, niin $I = R$.

Todistus. Olkoon nyt I renkaan $(R, +\cdot)$ ideaali. Tällöin alirenkaan määritelmän kohdan 3 perusteella $1_R \in I$. Tästä seuraa ideaalin määritelmän 2 kohdan perusteella, että $r = r \cdot 1_R \in I$ kaikilla $r \in R$. Tällöin rengas itse on sen ainoa ideaali. □

Lause 3.2.3. Jos I ja J ovat renkaan R ideaaleja, niin tällöin myös niiden leikkaus

$$I \cap J = \{a | a \in I, a \in J\}$$

ja summa

$$I + J = \{a + b | a \in I, b \in J\}$$

ovat ideaaleja.

Todistus. Todistetaan leikkausta koskeva väite. Olkoon $a_1, a_2 \in I \cap J$, niin tällöin $a_1 + a_2 \in I$, koska $a_1, a_2 \in I$. Samoin myös $a_1 + a_2 \in J$ sillä $a_1, a_2 \in J$.

Todistetaan summaa koskeva väite. Joukot I ja J ovat ideaaleina epätyhjiä joukkoja, on niiden summakin epätyhjä.

Olkoon $a_1, a_2 \in I, b_1, b_2 \in J$ ja $c_i = a_i + b_i \in I + J$ kun $i = 1, 2$. Tällöin

$$c_1 - c_2 = a_1 + b_1 - (a_2 + b_2) = a_1 + b_1 - a_2 - b_2 = a_1 - a_2 + b_1 - b_2 \in I + J.$$

Nyt määritelmän 3.2.1 kohdan 2 perusteella $ra \in I$ ja $ar \in I$ sekä $rb \in J$ ja $br \in J$, kun $a \in I$, $b \in J$ ja $r \in R$. Tällöin

$$ra + rb = r(a + b) \in I + J$$

ja

$$ar + br = (a + b)r \in I + J$$

□

Määritelmä 3.2.4 Jos $(R, +, \cdot)$ on kommutatiivinen rengas ja $a \in R$, niin

$$< a > = Ra = \{ra | r \in R\}.$$

Määritelmä 3.2.5 Renkaan $(R, +, \cdot)$ ideaali on maksimaalinen, mikäli

1. $M \neq R$
2. jos I on renkaan R ideaali ja $M \subset I \subseteq R$, niin $I = R$.

Eli maksimaalinen ideaali M on laajin mahdollinen renkaan R aito ideaali.

3.3 Tekijärengas

Samalla tavoin kuin ryhmälle määritellään tekijäryhmä, voidaan renkaalle määritelä tekijärengas. Tekijäryhmät muodostetaan normaalien aliryhmien suhteen, jolloin sivuluokkien joukossa on mahdollista määritellä laskutoimitus. Tekijärenkaan tapauksessa on pystyttävä määrittelemään kaksi laskutoimitusta, yhteen- ja kertolasku.

Olkoon I renkaan $(R, +, \cdot)$ ideaali, jolloin $(I, +) \leq (R, +)$. Nyt $(R, +)$ on Abelin ryhmä, joten $(I, +) \trianglelefteq (R, +)$. Siten tekijärenkaan $(R/I, +)$ on olemassa. Tekijäryhmän $(R, +)$ alkioina ovat ideaalin I sivuluokat $r + I$, missä $r \in R$ ja sivuluokkien yhteenlasku $(+)$ toimii siten, että

$$(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$$

aina, kun $r_1, r_2 \in R$. Tällöin tekijäryhmän $(R/I, +)$ nolla-alkio on $\mathbf{0} + I = I$ ja alkion $a + I \in R/I$ vasta-alkio on alkio $(-a) + I$.

Määritellään sivuluokkien välinen kertolasku $(\cdot)$ siten, että

$$(r_1 + I) \cdot (r_2 + I) = (r_1 r_2) + I$$

Aina, kun $r_1, r_2 \in R$.

Osoitetaan, että näin määritelty kertolasku on hyvin määritelty eli tulo on riippumaton sivuluokkien edustajista:

Olkoon $a_1 + I = b_1 + I$ ja $a_2 + I = b_2 + I$. Tällöin $a_1 \in b_1 + I$ ja $a_2 = b_2 + I$, joten $a_1 = b_1 + i_1$ ja $a_2 = b_2 + i_2$ joillakin $i_1, i_2 \in I$. Näin ollen

$$\begin{aligned}(a_1 + I) \cdot (a_2 + I) = a_1 a_2 + I = (b_1 + i_1)(b_2 + i_2) + I \\ = (b_1 b_2 + b_1 i_2 + i_1 b_2 + i_1 i_2) + I \\ (b_1 b_2 + I) + (b_1 i_2 + I) + (i_1 b_2 + I) + (i_1 i_2 + I) \\ = (b_1 b_2 + I) + (\mathbf{0} + I) + (\mathbf{0} + I) + (\mathbf{0} + I) \\ b_1 b_2 + I = (b_1 + I) \cdot (b_2 + I),\end{aligned}$$

sillä $b_1 i_2, i_1 b_2, i_1 i_2 \in I$, koska I on ideaali. Tulo on siis riipumaton sivuluokkien edustajista ja on siten hyvin määritelty.

Määritelmä 3.3.1 Olkoon I renkaan $(R, +, \cdot)$ ideaali ja $R/I = \{r + I | r \in R\}$, missä $r + I = \{r + x | x \in I\}$. Tällöin $(R/I, +, \cdot)$ on rengas, missä $(+)$ ja $(\cdot)$ ovat edellä määrätyt sivuluokkien yhteen- ja kertolasku.

Todistus. Osoitetaan, että määritelmän 3.1.1 ehdot toteutuvat.

1. Abelin ryhmä:

   - Binäärisyys: Olkoon $a + I, b + I \in R/I$. Tällöin

     $$(a + I) + (b + I) = (a + b) + I \in R/I.$$

   - Assosiatiivisuus: Olkoon $a + I, b + I, c + I \in R/I$. Tällöin

     $$\begin{aligned}(a + I) + ((b + I) + (c + I)) = (a + I) + ((b + c) + I) \\ = (a + (b + c)) + I \\ = ((a + b) + c) + I \\ = ((a + b) + I) + (c + I) \\ = ((a + I) + (b + I)) + (c + I).\end{aligned}$$

   - Neutraalioalkio: Olkoon $\mathbf{0} + I = I \in R/I$ ja

     $$(\mathbf{0} + I) + (a + I) = (a + I) = (a + I) + (\mathbf{0} + I)$$

     kaikilla $a + I \in R/I$, joten $\mathbf{0} + I = I$ on nolla-alkio joukossa R/I.

- Vasta-alkio: Olkoon $a + I \in R/I$. Tällöin $(-a) + I = -a + I \in R/I$ ja

$$(a + I) + (-a + I) = (a - a) + I = \mathbf{0} + I = (-a + I) + (a + I),$$

joten $-a + I$ on alkion $a + I$ vasta-alkio joukossa R/I.

- Kommutatiivisuus: Olkoon $a + I, b + I \in R/I$. Tällöin

$$(a + I) + (b + I) = (a + b) + I = (b + a) + I = (b + I) + (a + I).$$

Yllä olevien kohtien nojalla $(R/I, +)$ on Abelin ryhmä.

2. Monoidi:

- Binäärisyys: Olkoon $a + I, b + I \in R/I$. Tällöin

$$(a + I) \cdot (b + I) = ab + I \in R/I.$$

- Assosiatiivisuus: Olkoon $a + I, b + I, c + I \in R/I$. Tällöin

$$\begin{aligned}(a + I) \cdot ((b + I) \cdot (c + I)) &= (a + I) \cdot (bc + I) \\ &= a(bc) + I = (ab)c + I \\ &= (ab + I) \cdot (c + I) \\ &= ((a + I) \cdot (b + I) \cdot (c + I).\end{aligned}$$

- Ykkösalkio: Nyt $\mathbf{1} + I \in R/I$ ja

$$(\mathbf{1} + I) \cdot (a + I) = (a + I) = (a + I) = \cdot(\mathbf{1} + I)$$

kaikilla $a + I \in R/I$, joten $\mathbf{1} + I$ on ykkösalkio joukokssa R/I.

Yllä olevien kohtien nojalla $(R/I, \cdot)$ on monoidi.

3. Osittelulait: Olkoon $a + I, b + I, c + I \in R/I$. Tällöin

$$\begin{aligned}(a + I) \cdot ((b + I) + (c + I) &= (a + I) \cdot ((b + c) + I) \\ &= a(b + c) + I = (ab + ac) + I \\ &= (ab + I) + (ac + I) = (a + I) \cdot (b + I) + (a + I) \cdot (c + I)\end{aligned}$$

$$\begin{aligned}((a + I) + (b + I)) \cdot (c + I) &= ((a + b) + I) \cdot (c + I) \\ (a + b)c + I &= (ac + bc) + I \\ (ac + I) + (bc + I) &= (a + I) \cdot (c + I) + (b + I) \cdot (c + I).\end{aligned}$$

Näin osittelulait ovat voimassa joukossa R/I.

Kohtien 1-3 nojalla $(R/I, +, \cdot)$ on rengas. □

Määritelmä 3.3.2 Olkoon I renkaan $(R, +, \cdot)$ ideaali ja ideaalin I sivuluokkien joukko $R/I = \{r + I | r \in R\}$. Tällöin rengasta $(R/I, +, \cdot)$, missä $(+)$ ja $(\cdot)$ ovat edellä määritellyt sivuluokkien yhteen- ja kertolasku, sanotaan renkaan R *tekijärenkaaksi* ideaalin I suhteen.

3.4 Rengashomomorfismi

Määritelmä 3.4.1. Olkoon $(R, +, \cdot)$ ja $(R', \oplus, \otimes)$ renkaita. Tällöin kuvausta $f : R \to R'$ sanotaan *rengashomomorfismiksi*, jos se täyttää seuraavat ehdot:

1. $f(a + b) = f(a) \oplus f(b)$ kaikilla $a, b \in R$.
2. $f(a \cdot b) = f(a) \otimes f(b)$ kaikilla $a, b \in R$.
3. $f(\mathbf{1}_R) = \mathbf{1}_{R'}$.

Koska f on rengashomomofismi, on f myös ryhmähomomorfismi. Tällöin lauseen 1.7 nojalla pätee myös

$$f(\mathbf{0}_R) = \mathbf{0}_{R'}$$

ja

$$f(-a) = -f(a)$$

kaikilla $a \in R$.

Lause 3.4.2. Olkoon $f : (R, +, \cdot) \to (R', \oplus, \otimes)$ rengashomomorfismi. Tällöin seuraavat väitteet pätevät:

1. Jos S on renkaan R alirengas, niin $f(S)$ on renkaan R' alirengas.
2. Jos S' on renkaan R' alirengas, niin $f^{-1}(S')$ on renkaan R alirengas.
3. Jos I on renkaan R ideaali, niin $f(I)$ on renkaan $f(R)$ ideaali.
4. Jos I' on renkaan R' ideaali, niin $f^{-1}(I')$ on renkaan R ideaali.

Todistus. 1. Olkoon S renkaan $(R, +, \cdot)$ alirengas. Selvästi $f(S) \subseteq R'$ ja $f(S) \neq \emptyset$, sillä $\mathbf{0}_R \in S$, joten $f(\mathbf{0}_R) \in f(S)$. Olkoon $c, d \in f(S)$. Tällöin on olemassa sellaiset $a, b \in S$, että $c = f(a)$ ja $d = f(b)$.

(a) Koska S on renkaan R alirengas, niin $a - b \in S$. Tällöin

$$f(a - b) = f(a + (-b)) \in f(S).$$

Kuvaus f on rengashomomorfismi, joten

$$c \oplus (-d) = f(a) \oplus (-f(b)) = f(a) \oplus f(-b) = f(a + (-b)) \in f(S).$$

(b) Koska S on renkaan R alirengas, niin $a \cdot b \in S$. Näin ollen $f(a \cdot b) \in f(S)$. Koska f on rengashomomorfismi, niin

$$c \otimes (-d) = f(a) \otimes f(b) = f(a \cdot b) \in f(S).$$

(c) Koska S on renkaan R alirengas, niin $\mathbf{1}_R \in S$. Koska f on rengashomomorfismi, niin

$$\mathbf{1}_{R'} = f(\mathbf{1}_R) \in f(S).$$

Näiden kohtien ja alirengaskriteerin perusteella $f(S)$ on renkaan $R^{'}$ alirengas.

2. Olkoon $S^{'}$ renkaan $R^{'}$ alirengas. Selvästi $f^{-1}(S^{'}) \subseteq R$. Nyt f on rengashomomorfismi ja $S^{'}$ on renkaan $R^{'}$ alirengas, joten $f(\mathbf{0}_R) = \mathbf{0}_{R'} \in S^{'}$. Näin ollen $\mathbf{0}_{R'} \in f^{-1}(S^{'})$, joten $f^{-1}(S^{'}) \neq \emptyset$. Olkoon $a, b \in f^{-1}(S^{'})$. jolloin $f(a), f(b) \in S^{'}$.

   (a) Koska $S^{'}$ on renkaan $R^{'}$ alirengas, niin $f(a) \oplus (-f(b)) \in S^{'}$. Koska f on rengashomomorfismi, niin

$$f(a-b) = f(a+(-b)) = f(a) \oplus f(-b) = f(a) \oplus (-f(b)) \in S^{'}.$$

   Näin ollen $a + (-b) = a - b \in f^{-1}(S^{'})$

   (b) Koska $S^{'}$ on renkaan $R^{'}$ alirengas, niin $f(a) \otimes f(b) \in S^{'}$. Koska f on rengashomomorfismi, niin

$$f(a \cdot b) = f(a) \otimes f(b) \in S^{'}$$

   Näin ollen $a \cdot b \in f^{-1}(S^{'})$.

   (c) Koska $S^{'}$ on renkaan $R^{'}$ alirengas, niin $\mathbf{1}_{R'} \in S^{'}$. Koska f on rengashomomorfismi, niin

$$f(\mathbf{1}_R) = \mathbf{1}_{R'} \in S^{'}.$$

   Näin ollen $\mathbf{1}_R \in f^{-1}(S^{'})$.

   Näiden kohtien ja alirengaskriteerin nojalla $f^{-1}(S^{'})$ on renkaan R alirengas.

3. Olkoon I renkaan R ideaali. Tällöin $\mathbf{0}_R \in I$, joten $\emptyset \neq I \subseteq R$. Näin ollen $\emptyset \neq f(I) \subseteq f(R)$. Koska R on renkaan R alirengas, niin edellä todistetun kohdan 1. nojalla $f(R)$ on renkaan $R^{'}$ alirengas. Siispä $f(R)$ on rengas.

   (a) Olkoon $c, d \in f(I)$. Tällöin on olemassa sellaiset $a, b \in I$, että $c = f(a)$ ja $d = f(b)$. Koska I on renkaan R ideaali, niin $(I, +) \leq (R, +)$ ja siten $a - b \in I$ ja edelleen $f(a-b) \in f(I)$. Koska f on rengashomomorfismi, niin

$$c \oplus (d) = f(a) \oplus (-f(b)) = f(a) \oplus f(-b) = f(a-b) \in f(I).$$

   Siispä $(f(I), \oplus) \leq (f(R), \oplus)$.

   (b) Olkoon $x \in f(I)$ ja $s \in f(R)$. Tällöin on olemassa sellaiset $a \in I$ ja $r \in R$, että $x = f(a)$ ja $s = f(r)$. Koska I renkaan R ideaali, niin

$a \cdot r, r \cdot a \in I$, jolloin $f(a \cdot r), f(r \cdot a) \in f(I)$. Koska f on rengashomomorfismi, niin

$$x \otimes s = f(a) \otimes f(r) = f(a \cdot r) \in f(I)$$

ja

$$s \otimes x = f(r) \otimes f(a) = f(r \cdot a) \in f(I).$$

Näiden kohtien perusteella $f(I)$ on renkaan $f(R)$ ideaali.

4. Olkoon $I^{'}$ renkaan $\mathbf{0}_{R'} \in I^{'}$, joten koska $f(\mathbf{0}_R) = \mathbf{0}_R$, niin $\mathbf{0}_R \in f^{-1}(I^{'})$. Siispä $\emptyset \neq f^{-1}(I^{'}) \subseteq R$.

   (a) Olkoon $a, b \in f^{-1}(I^{'})$. Tällöin $f(a).f(b) \in I^{'}$. Koska $I^{'}$ on renkaan $R^{'}$ ideaali, niin $(I^{'}, \oplus) \leq (R^{'}, \oplus)$ ja sitten $f(a) \oplus (-f(b)) \in I^{'}$. Koska f on rengashomomorfismi, niin

   $$f(a + (-b)) = f(a) \oplus f(-b) = f(a) \oplus (-f(b)) \in I^{'}$$

   Näin ollen $a + (-b) \in f^{-1}(I^{'})$ ja siten $(f^{-1}(I^{'}), +) \leq (R, +)$.

   (b) Olkoon $a \in f^{-1}(I^{'})$ ja $r \in R$. Tällöin $f(a) \in I^{'}$ ja $f(r) \in R^{'}$. Koska $I^{'}$ on renkaan $R^{'}$ ideaali, niin $f(a) \otimes f(r) \in I^{'}$ ja $f(r) \otimes f(a) \in I^{'}$. Koska f on rengashomomorfismi, niin

   $$f(a \cdot r) = f(a) \otimes f(r) \in I^{'}$$

   ja

   $$f(r \cdot a) = f(r) \otimes f(a) \in I^{'}.$$

   Siispä $a \cdot r, r \cdot a \in f^{-1}(I^{'})$.

   Näiden kohtien perusteella $f^{-1}(I^{'})$ on renkaan R ideaali.

□

Lause 3.4.3. Jos $f : R \to R^{'}$ on renkaan rengashomomorfismi, niin

1. $Ker(f)$ on renkaan ideaali.
2. $Im(f)$ on renkaan $R^{'}$ alirengas.

Todistus. Todistetaan kohdat 1. ja 2.

1. Koska $Ker(f) = f^{-1}(\{0_R\})$ ja $\{0_R\}$ on renkaan $R^{'}$ ideaali, niin lauseen 3.4.2. kohdan 4. nojalla $Ker(f)$ on renkaan R ideaali.
2. Koska $Im(f) = f(R)$ ja R on renkaan R alirengas, niin lauseen 3.4.2. kohdan 1. nojalla $Im(f)$ on renkaan $R^{'}$ alirengas.

□

3.5 Kunnan teoriaa

Määritelmä 3.5.1. Rengasta $(K, +, \cdot)$ sanotaan *kunnaksi*, jos seuraavat ehdot pätevät:

1. $(K, +)$ on Abelin ryhmä:
   - $(+)$ on binäärinen operaatio joukossa K eli $a+b \in K$ kaikilla $a, b \in K$.
   - $(+)$ on assosiatiivinen operaatio eli $a + (b + c) = (a + b) + c$ kaikilla $a, b, c \in K$.
   - On olemassa nolla-alkio $\mathbf{0} \in K$, jolle $a+\mathbf{0} = \mathbf{0}+a = a$ kaikilla $a \in K$.
   - Jokaiselle $a \in K$ on olemassa vasta-alkio $-a \in K$ jolle pätee $a + (-a) = -a + a = \mathbf{0}$.
   - $(+)$ on kommutatiivinen operaatio eli $a + b = b + a$ kaikilla $a, b \in K$.
2. Operaatiolle $(\cdot)$ pätevät seuraavat ehdot:
   - $(\cdot)$ on binäärinen operaatio joukossa $K \setminus \mathbf{\{0\}}$ eli $a \cdot b \in K \setminus \mathbf{\{0\}}$ kaikilla $a, b \in K \setminus \mathbf{\{0\}}$.
   - $(\cdot)$ on assosiatiivinen operaatio eli $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ kaikilla $a, b, c \in K \setminus \mathbf{\{0\}}$.
   - On olemassa ykkösalkio $\mathbf{1} \in K \setminus \mathbf{\{0\}}$, jolle $a \cdot \mathbf{1} = \mathbf{1} \cdot a = a$ kaikilla $a \in K \setminus \mathbf{\{0\}}$.
   - Jokaiselle $a \in K \setminus \mathbf{\{0\}}$ on olemassa käänteisalkio $a^{-1} \in K \setminus \mathbf{\{0\}}$, jolle pätee $a \cdot a^{-1} = a^{-1} \cdot a = \mathbf{1}$.
   - $(\cdot)$ on kommutatiivinen operaatio eli $a \cdot b = b \cdot a$ kaikilla $a, b \in K \setminus \mathbf{\{0\}}$.
3. Osittelulait pätevät:
   - $a \cdot (b + c) = a \cdot b + a \cdot c$ kaikilla $a, b, c \in K$.
   - $a + b) \cdot c = a \cdot c + b \cdot c$ kaikilla $a, b, c \in K$.

Määritelmä 3.5.2. (Alikuntakriteeri). Kunnan $(K, +, \cdot)$ osajoukko $H, H \neq \emptyset$, on kunnan K alikunta jos ja vain jos seuraavat ehdot pätevät:

1. Osajoukossa H on vähintään kaksi alkiota.
2. $a - b = a + (-b) \in H$ kaikilla $a, b \in H$.
3. $\frac{a}{b} = a \cdot b^{-1} \in H$ kaikilla $a, b \in H, b \neq \emptyset$.

Määritelmä 3.5.3 Jos $(K, +, \cdot)$ ja $(K', \oplus, \otimes)$ ovat kuntia, niin rengashomomorfismia $f : K \to K'$ sanotaan *kuntahomomorfismiksi*. Vastaavasti rengasisomorfismia $f : K \to K'$ sanotaan *kuntaisomorfismiksi*.

Lause 3.5.3. Olkoon f kuntahomomorfismi $K \to K'$. Tällöin

$$f(a^{-1}) = f(a)^{-1}$$

kaikilla $a \in K \setminus \mathbf{\{0\}}$.

Lause 3.5.4.(Kuntalaajennuslause). Olkoon $(R, +,)$ kommutatiivinen rengas ja M renkaan R maksimaalinen ideaali. Tällöin tekijärengas R/M on kunta.

Todistus. Koska R on kommutatiivinen rengas, niin tekijärengas R/M on myös kommutatiivinen rengas.

Osoitetaan, että $(R/M \backslash \{\mathbf{0} + M\}, \cdot)$ on Abelin ryhmä. Koska R/M on kommutatiivinen rengas, riittää osoittaa, että jokaiselle tekijärenkaan nolla-alkiosta eroavalle alkiolle on olemassa käänteisalkio joukossa $R/M \backslash \{\mathbf{0} + M\}$.

Olkoon $a + M \in R/M$ ja $a + M \neq \mathbf{0} + M$. Tällöin $a \notin \mathbf{0} + M = M$, joten $(a) \neq M$. Lauseen 3.2.3 nojalla ideaalien summa $M + (a)$ on renkaan R ideaali ja selvästi $M \subset M + (a)$. Koska M on renkaan R maksimaalinen ideaali, niin $M + (a) = R$, ja edelleen lauseen 3.2.4 nojalla $R = M + Ra$.

Nyt $\mathbf{1} \in R$ eli $\mathbf{1} \in M + Ra$, joten $\mathbf{1} = m + ra$ joillakin $m \in M$ ja $r \in R$. Tällöin tekijärenkaan R/M ykkösalkio

$$\mathbf{1} + M = (m + ra) + M = (m + M) + (ra + M) = (\mathbf{0} + M) + (ra + M)$$

$$= ra + M = (r + M) \cdot (a + M).$$

Koska tekijärengas R/M on kommutatiivinen, niin myös

$$(a + M) \cdot (mr + M) = \mathbf{1} + M$$

Näin ollen $r + M$ on alkion $a + M$ käänteisalkio ja luonnollisesti $r + M \neq \mathbf{0} + M$.

Siispä tekijärengas $(R/M, +, \cdot)$ on kunta. □

4 Toisenlaiset operaatiot

Nyt aletaan tutkia renkaita aikaisemmista poikkeavilla operaattoreilla. Tarkoitus on selvittää, minkälaisia operaatioita voidaan käyttää ja että onko joillakin operaatioilla mahdollista ratkaista haastavampiakin ryhmiä.

Olkoon

$$\mathbb{R} \times \mathbb{R} = \{(x, y) | x, y \in \mathbb{R}\},$$

missä $\mathbb{R}$ on reaalilukujen joukko. Joukossa $\mathbb{R} \times \mathbb{R}$ yhteenlasku ja kertolasku määritellään

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2, y_1 y_2)$$

Osoitetaan, että tämä on rengas.

Oletus 4.1. Kolmikko $(\mathbb{R} \times \mathbb{R}, +, \cdot)$ on rengas.

1. $(\mathbb{R} \times \mathbb{R}, +)$ on Abelin ryhmä:
   - Binäärisyys: $(x_1, y_1) + (x_2, y_2) \in R \Rightarrow (x_1 + x_2, y_1 + y_2) \in \mathbb{R}$.
   - Assosiatiivisuus:
     $(x_1, y_1) + \big((x_2, y_2) + (x_3, y_3)\big) = \big((x_1, y_1) + (x_2, y_2)\big) + (x_3, y_3)$.
   - Neutraalialkio:
     $0_{\mathbb{R}\times\mathbb{R}}$ on sellainen alkio, että $(x_1, y_1) + 0_{\mathbb{R}\times\mathbb{R}} = 0_{\mathbb{R}\times\mathbb{R}} + (x_1, y_1) = (x_1, y_1)$.
   - Vasta-alkio:
     $(-x, -y) \in \mathbb{R}$ eli $(x_1, y_1)+(-x_1, -y_1) = (-x_1, -y_1)+(x_1, y_1) = 0_{\mathbb{R}\times\mathbb{R}}$.
   - Kommutatiivisuus: $(x_1, y_1) + (x_2, y_2) = (x_2, y_2) + (x_1, y_1)$.

   kaikilla $x, y \in \mathbb{R}$.

   Todistus. Käydään läpi kaikki Abelin ryhmän ehdot.

   - Binäärisyys: $\Rightarrow$ Selvä.
   - Assosiatiivisuus:

$$\begin{aligned}
&(x_1, y_1) + \big((x_2, y_2) + (x_3, y_3)\big) \\
&= (x_1, y_1) + (x_2 + x_3, y_2 + y_3) \\
&= (x_1 + x_2 + x_3, y_1 + y_2 + y_3) \\
&= (x_1 + x_2, y_1 + y_2) + (x_3 + y_3) \\
&= \big((x_1, y_1) + (x_2, y_2)\big) + (x_3, y_3)
\end{aligned}$$

- Neutraalialkio: Oletetaan, että $0_{\mathbb{R}\times\mathbb{R}} = (0,0) \in \mathbb{R}$ Nyt

$$(x_1, y_1) + (0,0) = (0,0) + (x_1, y_1) = (x_1, y_1)$$

- Vasta-alkio: $\Rightarrow$ Selvä.
- Kommutatiivisuus:

$$\begin{aligned} &(x_1, y_1) + (x_2, y_2) \\ &= (x_1 + x_2, y_1 + y_2) \\ &= (x_2 + x_1, y_2 + y_1) \\ &(x_2, y_2) + (x_1, y_1) \end{aligned}$$

Eli $(\mathbb{R} \times \mathbb{R}, +)$ on Abelin ryhmä. □

2. $(\mathbb{R} \times \mathbb{R}, \cdot)$ on monoidi:

- Binäärisyys: $(x_1, y_1) \cdot (x_2, y_2) \in \mathbb{R} \Rightarrow (x_1x_2, y_1y_2) \in \mathbb{R}$.
- Assosiatiivisuus: $(x_1, y_1) \cdot \big((x_2, y_2) \cdot (x_3, y_3)\big) = \big((x_1, y_1) \cdot (x_2, y_2)\big) \cdot (x_3, y_3)$.
- Neutraalialkio:
  $1_{\mathbb{R}\times\mathbb{R}}$ on sellainen alkio, että $(x_1, y_1) \cdot 1_{\mathbb{R}\times\mathbb{R}} = 1_{\mathbb{R}\times\mathbb{R}} \cdot (x_1, y_1) = (x_1, y_1)$.

kaikilla $x, y \in \mathbb{R}$.

Todistus. Käydään läpi kaikki monoidin ehdot:

- Binäärisyys $\Rightarrow$ Selvä.
- Assosiatiivisuus:

$$\begin{aligned} &(x_1, y_1) \cdot \big((x_2, y_2) \cdot (x_3, y_3)\big) \\ &(x_1, y_1) \cdot (x_2x_3, y_2y_3) \\ &(x_1x_2x_3, y_1y_2y_3) \\ &(x_1x_2, y_1y_2) \cdot (x_3, y_3) \\ &\big((x_1, y_1) \cdot (x_2, y_2)\big) \cdot (x_3, y_3) \end{aligned}$$

- Neutraalialkio: Oletetaan, että $1_{\mathbb{R}\times\mathbb{R}} = (1,1) \in \mathbb{R}$. Nyt

$$(x_1, y_1) \cdot (1,1) = (1,1) \cdot (x_1, y_1) = (x_1, y_1)$$

Eli $(\mathbb{R} \times \mathbb{R}, \cdot)$ on monoidi.

□

3. Distribiivisuus- eli osittelulait ovat voimassa:

- $(x_1, y_1) \cdot \big((x_2, y_2) + (x_3, y_3)\big) = (x_1, y_1) \cdot (x_2, y_2) + (x_1, y_1) \cdot (x_3, y_3)$

- $\big((x_1, y_1) + (x_2, y_2)\big) \cdot (x_3, y_3) = (x_1, y_1) \cdot (x_3, y_3) + (x_2, y_2) \cdot (x_3, y_3)$

kaikilla $x, y \in \mathbb{R}$.

Todistus. Käydään molemmat kohdat läpi

- $(x_1, y_1) \cdot \big((x_2, y_2) + (x_3, y_3)\big) = (x_1, y_1) \cdot (x_2 + x_3, y_2 + y_3)$

  $= (x_1x_2 + x_1x_3, y_1y_2 + y_1y_3) = (x_1, y_1) \cdot (x_2, y_2) + (x_1, y_1) \cdot (x_3, y_3)$

- $\big((x_1, y_1) + (x_2, y_2)\big) \cdot (x_3, y_3) = (x_1 + x_2, y_1 + y_2) \cdot (x_3, y_3)$

  $(x_1x_3 + x_2x_3, y_1y_3 + y_2y_3) = (x_1, y_1) \cdot (x_3, y_3) + (x_2, y_2) \cdot (x_3, y_3)$

Osittelulait ovat siis voimassa. □

Kaikki ehdot täyttyvät, joten kolmikko $(\mathbb{R} \times \mathbb{R}, +, \cdot)$ on rengas.

Oletus 4.2 Kolmikko $(\mathbb{M}_{2\times2}(\mathbb{R}), +, \cdot)$ on rengas.

$\mathbb{M}_{2\times2}(\mathbb{R})$ on 2×2 matriisijoukko, missä a,b,c,d $\in \mathbb{R}$.

Todistus. 1. $(\mathbb{M}_{2\times2}, +)$ on Abelin ryhmä:

- Binäärisyys: Tiedetään, että $a + b \in \mathbb{R}$, kun a ja $b \in \mathbb{R}$, joten ehto täyttyy. Samoin tiedetään myös kommutatiivisuus.
- Assosiatiivisuus:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \left(\begin{bmatrix} e & f \\ g & h \end{bmatrix} + \begin{bmatrix} i & j \\ k & l \end{bmatrix} \right)$$

$$= \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e+i & f+j \\ g+k & h+l \end{bmatrix}$$

$$= \begin{bmatrix} a+e+i & b+f+j \\ c+g+k & d+h+l \end{bmatrix}$$

$$= \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix} + \begin{bmatrix} i & j \\ k & l \end{bmatrix}$$

$$= \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} \right) + \begin{bmatrix} i & j \\ k & l \end{bmatrix}$$

kaikilla $a, b, c, d, e, f, g, h, i, j, k \in \mathbb{R}$.

- Nolla-alkio $\mathbf{0}_{\mathbb{M}}$: $\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

- Vasta-alkio:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$= \begin{bmatrix} a-a & b-b \\ c-c & d-d \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Eli on Abelin ryhmä.

2. $(\mathbb{M}_{2\times 2}, \cdot)$ on monoidi:

   - Binäärisyys: Tiedetään, että $a \cdot b \in \mathbb{R}$, kun a ja $b \in \mathbb{R}$, joten ehto täyttyy.
   - Assosiatiivisuus: Tutkitaan ensin vasen puoli

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \left(\begin{bmatrix} e & f \\ g & h \end{bmatrix} \cdot \begin{bmatrix} i & j \\ k & l \end{bmatrix} \right)$$

$$= \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} ei+fk & ej+fl \\ gi+hk & gj+hl \end{bmatrix}$$

$$= \begin{bmatrix} aei+afk+bgi+bhk & aej+afl+bgj+bhl \\ cei+cfk+dgi+dhk & cej+cfl+dgj+dhl \end{bmatrix}.$$

   Sitten oikea puoli:

$$= \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} e & f \\ g & h \end{bmatrix} \right) \cdot \begin{bmatrix} i & j \\ k & l \end{bmatrix}$$

$$= \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix} \cdot \begin{bmatrix} i & j \\ k & l \end{bmatrix}$$

$$= \begin{bmatrix} aei+bgi+afk+bhk & aej+bgj+afl+bhl \\ cei+dgi+cfk+dhk & cej+dgj+cfl+dhl \end{bmatrix}.$$

   Koska $\mathbb{R}$:n alkiot ovat kommutatiiviset $(+)$ suhteen, ovat molemmat puolet yhtä suuret kaikilla $a, b, c, d, e, f, g, h, i, j, k \in \mathbb{R}$.

   - Ykkösalkio: Matriiseissa yleisenä ykkösalkiona toimii ykkösmatriisi

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a \cdot 1 + b \cdot 0 & a \cdot 0 + b \cdot 1 \\ c \cdot 1 + d \cdot 0 & c \cdot 0 + d \cdot 1 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

     Eli on monoidi.

3. Osittelulait: Ensin vasen puoli

- $$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \left(\begin{bmatrix} e & f \\ g & h \end{bmatrix} + \begin{bmatrix} i & j \\ k & l \end{bmatrix} \right) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} e+i & f+j \\ g+k & h+l \end{bmatrix}$$
$$= \begin{bmatrix} ae+ai+bg+bk & af+aj+bh+bl \\ ce+ci+dg+dk & cf+cj+dh+dl \end{bmatrix}$$
$$= \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix} + \begin{bmatrix} ai+bk & aj+bl \\ ci+dk & cj+dl \end{bmatrix}$$
$$= \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} e & f \\ g & h \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} i & j \\ k & l \end{bmatrix}$$
aina, kun $a, b, c, d, e, f, g, h, i, j, k \in \mathbb{R}$.

- $$\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} \right) \cdot \begin{bmatrix} i & j \\ k & l \end{bmatrix} = \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix} \cdot \begin{bmatrix} i & j \\ k & l \end{bmatrix}$$
$$= \begin{bmatrix} ai+ei+bk+fk & aj+ej+bl+fl \\ ci+gi+dk+hk & dj+dj+hl+hl \end{bmatrix}$$
$$= \begin{bmatrix} ai+bk & aj+bl \\ ci+dk & cj+dl \end{bmatrix} + \begin{bmatrix} ei+fk & ej+fl \\ gi+hk & dj+hl \end{bmatrix}$$
$$= \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} i & j \\ k & l \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} \cdot \begin{bmatrix} i & j \\ k & l \end{bmatrix}$$
aina, kun $a, b, c, d, e, f, g, h, i, j, k \in \mathbb{R}$.

Osittelulait pätevät.

Näillä perusteilla kolmikko $(\mathbb{M}_{2\times 2}(\mathbb{R}), +, \cdot)$ on rengas.

□

Kolmikko $(\mathbb{M}_{2\times 2}(\mathbb{R}), +, \cdot)$ ei kuitenkaan ole kommutatiivinen rengas, sillä

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}$$

ja

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}.$$

Oletus 4.3. Renkaan $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$ ei-tyhjä osajoukko $2\mathbb{Z} \times 2\mathbb{Z}$ on ideaali.

Olkoon

$$\mathbb{Z} \times \mathbb{Z} = \{(a, b) | a, b \in \mathbb{Z}\},$$

missä $\mathbb{Z}$ on kokonaislukujen joukko. Joukossa $\mathbb{Z} \times \mathbb{Z}$ yhteenlasku ja kertolasku määritellään samoin kuin joukossa $\mathbb{R} \times \mathbb{R}$.

Seurataan määritelmän 3.2.1. ehtoja ja tutkitaaan onko osajoukko $2\mathbb{Z} \times 2\mathbb{Z}$ renkaan $\mathbb{Z} \times \mathbb{Z}$ ideaali.

1. $(2\mathbb{Z} \times 2\mathbb{Z}, +) \leq (\mathbb{Z} \times \mathbb{Z}, +)$.
2. $(2a, 2b) \cdot (a, b) \in \mathbb{Z} \times \mathbb{Z}$ ja $(a, b) \cdot (2a, 2b) \in \mathbb{Z} \times \mathbb{Z}$ aina, kun $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ ja $(2a, 2b) \in 2\mathbb{Z} \times 2\mathbb{Z}$.

Todistus. 1. Lauseen 1.4. mukaan $(2\mathbb{Z} \times 2\mathbb{Z}, +) \leq (\mathbb{Z} \times \mathbb{Z}, +)$, jos ja vain jos

$$(a_1, b_1), (a_2, b_2) \in \mathbb{Z} \Rightarrow (a_1, b_1) + (a_2, b_2)^{-1} \in \mathbb{Z}.$$

Olkoon nyt $a = 2h$ ja $b = 2k$ kun $h, k \in \mathbb{Z}$.

$$(a_1, b_1) + (a_2, b_2)^{-1} = (a_1, b_1) - (a_2, b_2)$$

$$(2h_1, 2k_1) - (2h_2, 2k_2) = (2h_1 - 2h_2, 2k_1 - 2k_2) \in 2\mathbb{Z}$$

Koska $h, k \in \mathbb{Z}$, niin $h_1 - h_2$ ja $k_1 - k_2 \in \mathbb{Z}$.

Täten $(2\mathbb{Z} \times 2\mathbb{Z}, +) \leq (\mathbb{Z} \times \mathbb{Z}, +)$.

2. Olkoon nyt $m, n \in \mathbb{Z}$. Nyt

$$(a, b) \cdot (m, n) = (2h, 2k) \cdot (m, n) = 2((h \cdot m), 2(k \cdot n))$$

ja

$$(m, n) \cdot (a, b) = (m, n) \cdot (2h, 2k) = 2((m \cdot h), 2(n \cdot k))$$

missä $h \cdot m, m \cdot h, k \cdot n$ ja $n \cdot k \in \mathbb{Z}$.

Näiden tulosten perusteella $(2\mathbb{Z} \times 2\mathbb{Z})$ on renkaan $(\mathbb{Z} \times \mathbb{Z})$ ideaali. □

Oletus 4.4. Rengas $(\mathbb{R} \times \mathbb{R}, +, \cdot)$ ei ole kunta.

Todistus. Osoitetaan, että tässä kappaleessa tutkittu rengas ei ole kunta. Kun katsotaan määritelmää 3.4.1., huomataan, että riittää tutkia vain kohtaa 2:

- Binäärisyys: Olkoon nyt $(x_1, y_1) = (0, y)$ ja $(x_2, y_2) = (x, 0)$.

  $$(0, y) \cdot (x, 0) = (0 \cdot x, y \cdot 0) = (0, 0) = \{\mathbf{0}\}$$

  Saatiin nolla-alkio joukkoon kuuluvilla luvuilla. Nolla-alkiota ei tule löytyä joukosta kyseisellä operaatiolla.

Kyseessä on ristiriita.

Tällä perusteella rengas $(\mathbb{R} \times \mathbb{R}, +, \cdot)$ ei ole kunta. □

Viitteet

[1] Bhattacharya, P., Nagpaul, S. and Jain, S., 2015. Basic Abstract Algebra. 2nd ed. Cambridge: University of Cambridge.

[2] Niemenmaa, Markku - Myllylä, Kari - Törmä, Topi - Leinonen, Marko: *802355A Algebralliset rakenteet Luentorunko*, Oulun yliopisto 2016

[3] *J.J.O'Connor and E.F.Robertson, The development of Ring Theory* (`http://www-history.mcs.st-andrews.ac.uk/HistTopics/Ring_theory.html`), September 2004.