Äärellisulotteinen lineaarialgebra, kevät 2015.
Harjoitus 3.
Ratkaisuehdotuksia

1. Määritellään kaikilla $a, b \in \mathbb{R}$ funktio $f_{a,b}\colon \mathbb{R} \to \mathbb{R}$ kaavalla $f_{a,b}(x) = ax + b$, $x \in \mathbb{R}$. Olkoot

$$G = \{f_{a,b} \mid a, b \in \mathbb{R}, a \neq 0\},$$
$$H = \{f_{a,0} \mid a \in \mathbb{R}, a \neq 0\},$$
$$N = \{f_{1,b} \mid b \in \mathbb{R}\},$$
$$G' = \{\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \mid a, b \in \mathbb{R}, a \neq 0\}.$$

   a) Osoita, että G on ryhmä kuvausten yhdistämisen suhteen. Osoita myös, että G on ryhmänä isomorfinen ryhmän $(G', \cdot)$ kanssa. Tässä $\cdot$ on matriisien kertolasku.

   b) Olkoon $A\colon G \to H$, $A(f_{a,b}) = f_{a,0}$. Osoita, että A on surjektiivinen ryhmähomomorfismi, jonka ydin on N. Osoita tämän avulla, että N on ryhmän G normaali aliryhmä ja tekijäryhmä G/N on isomorfinen ryhmän H kanssa.

   c) Onko H ryhmän G normaali aliryhmä? Onko H isomorfinen jonkun toisen tutun ryhmän kanssa?

Ratkaisu: a) Osoitetaan ensin, että G on todellakin ryhmä kuvausten yhdistämisen suhteen. Aloitetaan tarkistamalla, että kuvausten yhdistämisenoperaatio $\circ$ on hyvinmääritelty laskutoimitus joukossa G, toisin sanoen $f \circ g \in G$ kaikilla $f, g \in G$. Olkoot $a, b, c, d \in \mathbb{R}$, $a, c \neq 0$ ja olkoon $x \in \mathbb{R}$. Tällöin

$$(f_{a,b} \circ f_{c,d})(x) = f_{a,b}(f_{c,d})(x) = f_{a,b}(cx+d) = a(cx+d)+b = (ac)x+(ad+b) = f_{ac,ad+b}(x).$$

Näin ollen

$$f_{a,b} \circ f_{c,d} = f_{ac,ad+b}. \tag{1}$$

Koska $ac \neq 0$ kun $a, c \neq 0$ (reaalilukujen renkaassa voimassa oleva "nollasääntö"), tästä nähdään erityisesti, että $f_{a,b} \circ f_{c,d} \in G$ kun $f_{a,b}, f_{c,d} \in G$.

Koska $\mathrm{id}_{\mathbb{R}} = f_{1,0} \in G$ ja koska identtinen kuvaus on neutraalialkio kuvausten yhdistämisen suhteen, joukon G laskutoimituksella $\cdot$ on olemassa neutraalialkio $f_{1,0}$. Osoitetaan seuraavaksi, että $f_{a,b}$ on bijektio kaikilla $a, b \in \mathbb{R}$, $b \neq 0$. Koska $ay+b = x$ jos ja vain jos $y = (x-b)/a$, kuvauksella $f_{a,b}$ on olemassa käänteiskuvaus

$$f_{a,b}^{-1} = f_{\frac{1}{a}, -\frac{b}{a}} \in G. \tag{2}$$

Tästä nähdään, että

- G on permutaatioryhmän $\mathrm{Perm}(X) = \{f\colon X \to X \mid f \text{ on bijektio}\}$ osajoukko.

– Itse asiassa G on jopa tämän ryhmän aliryhmä. Tässä $\mathrm{Perm}(X)$ on varustettu vanhalla kunnon kuvausten yhdistämisoperaatiolla.

Erityisesti siis $(G, \circ)$ on todellakin ryhmä.

Määritellään kuvaus $\alpha\colon G \to M(2 \times 2; \mathbb{R})$,

$$\alpha(f_{a,b}) = \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}.$$

Ensinnäkin, tämä kuvaus on hyvinmääritelty, koska kuvauksen $f_{a,b}$ esitys tässä muodossa on *yksikäsitteinen*, tarkoittaen, että jos $f_{a,b} = f_{c,d}$, niin $a = c$ ja $b = d$. Helpoiten tämän näkee siitä, että $f_{a,b}(0) = b$ ja $f_{a,b}(1) = a + b$. Tästä seuraa, että jos $f_{a,b} = f_{c,d}$, niin $b = d$ ja $a + b = c + d$. Näistä tietenkin saadaan heti $a = c$ ja $b = d$. Näin ollen α on hyvin määritelty. Osoitetaan, että se on yhteensopiva laskutoimitusten $\circ$ (kuvausten yhdistäminen) ja $\cdot$ (matriisienkertolasku) kanssa. Yhtälön (1) ja matriisin kertolaskun määritelmästä seuraa, että

$$\alpha(f_{a,b} \circ f_{c,d}) = \alpha(f_{ac,ad+b}) = \begin{bmatrix} ac & ad+b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} c & d \\ 0 & 1 \end{bmatrix} = \alpha(f_{a,b}) \cdot \alpha(f_{c,d}).$$

Selvästi $G' = \operatorname{Im} \alpha$. Rajoittamalla kuvaus α kuvaukseksi $\alpha\colon G \to G'$ (vaihdetaan maalijoukko), nähdään, että α on *surjektiivinen* kuvaus, joka on yhteensopiva laskutoimitusten kanssa. Seurauksen 1.40 nojalla myös G' on ryhmä (kääntyvien (2×2)-matriisien ryhmän $GL(2; \mathbb{R})$ aliryhmä, itse asiassa). Näin ollen $\alpha\colon G \to G'$ on bijektiivinenn ryhmien välinen homomorfismi, toisin sanoen ryhmien välinen isomorfismi.

b) Ajatellaan kuvausta $A\colon G \to H$, $A(f_{a,b}) = f_{a,0}$ ensin kuvauksena $A\colon G \to G$ (vaihdetaan maalijoukko G:ksi). Osoitetaan, että A on yhteensopiva G:n laskutoimituksen $\circ$ kanssa. Yhtälön (1) nojalla

$$A(f_{a,b} \circ f_{c,d}) = A(f_{ac,ad+b}) = f_{ac,0} = f_{ac,a0+0} = f_{a,0} \circ f_{c,0} = A(f_{a,b}) \circ A(f_{c,d}).$$

Näin ollen A on (kuvauksena $G \to G$) ryhmien välinen homomorfismi. Koska selvästi $H = \operatorname{Im} A$, Lemmasta 1.62 seuraa, että H on ryhmän G aliryhmä, erityisesti ryhmä. Kuvauksena $A\colon G \to H$ (maalijoukkona nyt H), kuvaus A on tällöin *surjektiivinen* ryhmien välinen homomorfismi. Soveltamalla ryhmien Isomorfialausetta 1.101 tähän kuvauksen, saadaan isomorfismi $\bar{A}\colon G/\operatorname{Ker} A \to H$. Koska ryhmän H neutraalialkio on $f_{1,0} = \mathrm{id}_{\mathbb{R}}$,

$$\operatorname{Ker} f = \{f_{1,b} \mid b \in \mathbb{R}\} = N.$$

Näin ollen N on homomorfismin ytimenä normaali aliryhmä. Lisäksi $\bar{A}$ on ryhmien G/N ja H välinen isomorfismi.

c) Koska ryhmän H alkioille pätee

$$f_{a,0} \circ f_{c,0} = f_{ac,0},$$

missä $a, c \in \mathbb{R}^*$ ovat yksikäsitteisiä, voidaan helposti päätellä, että $(H, \circ)$ on isomorfinen nollasta eroavien reaalilukujen ryhmän $(\mathbb{R}^*, \cdot)$ kanssa. Eksplisiittinen isomorfismi $H \to \mathbb{R}^*$ on esimerkiksi kuvaus $f_{a,0} \mapsto a$.

Tutkitaan vielä onko H normaali G:n aliryhmänä. Olkoot $g = f_{a,b} \in G$ ja $h = f_{c,0} \in H$, tutkitaan päätekö väite $ghg^{-1} \in H$. Tällöin (kts. 2 yllä)

$$g^{-1} = f_{\frac{1}{a},-\frac{b}{a}},$$

joten, yhtälön 1 nojalla

$$ghg^{-1} = f_{a,b} \circ f_{c,0} \circ f_{\frac{1}{a},-\frac{b}{a}} = f_{ac,b} \circ f_{\frac{1}{a},-\frac{b}{a}} =$$

$$f_{c,-bc+b}.$$

Nähdään, että $ghg^{-1} \neq H$ jos $b - bc = b(1 - c) \neq 0$. Näin käy esimerkiksi jos valitaan $b = c = 2$ (a:n arvolla ei ole merkitystä). Erityisesti on olemassa $g \in G$, $h \in H$, joille $ghg^{-1} \notin H$, joten H ei ole normaali G:ssä.

2. Olkoon R rengas ja olkoon $x \in R$. Olkoon

$$I_x = \{\sum_{i=1}^{n} a_i x b_i \mid a_i, b_i \in R, n \geq 1\}.$$

   a) Osoita, että I_x on renkaan R ideaali, itse asiassa (sisältyvyysrelaation suhteen) *pienin* renkaan R ideaali, joka sisältää alkion x.

   b) Olkoon R vaihdannainen. Totea, että tällöin $I_x = \{ax \mid a \in R\}$.

Ratkaisu: a) Olkoon $I \subset R$ ideaali, jolle pätee $x \in I$. Tällöin ideaalin ehdoista seuraa, että $ax \in I$ kaikilla $a \in R$. Tästä puolestaan seuraa, että $axb = (ax)b \in I$ kaikilla $b \in R$. Näin ollen I sisältää ainakin kaikki tulot muotoa axb, missä $a, b \in R$ ovat mielivaltaisia. Koska $(I, +)$ on ideaalin määritelmän mukaan ryhmän $(R, +)$ aliryhmä, se on erityisesti suljettu myös yhteenlaskun suhteen, joten I sisältää myös kaikki mahdolliset summat muotoa axb olevista alkioista, eli kaikki alkiot muotoa

$$\sum_{i=1}^{n} a_i x b_i,$$

missä $a_i, b_i \in R, n \geq 1$. Olemme osoittaneet, että $I_x \subset I$. Osoitetaan vielä, että I_x on itse asiassa myös renkaan R ideaali, joka sisältää alkion x. Tällöin olemme näyttäneet, että I_x on R:n pienin (sisältyvyys relaation suhteen) ideaali, joka sisältää pisteen x.

Valitsemalla $n = 1, a_1 = b_1 = 0$, nähdään, että $0 = 0x0 \in I_x$. Jos $x = \sum_{i=1}^{n} a_i x b_i$ ja $y = \sum_{j=1}^{m} a'_j x b'_j$, niin $x + y$ voidaan selvästi esittää muodossa

$$x + y = \sum_{k=1}^{n+m} c_k x d_k,$$

missä $c_k = a_k$, $d_k = b_k$ kun $k = 1, \ldots, n$ ja $c_k = a_{n+j}$, $d_k = b_{n+j}$ kun$k = n + 1, \ldots, n + m$. Näin ollen $(I, +)$ on suljettu renkaan yhteenlaskun suhteen. Lisäksi (renkaan "merkkisäännöt")

$$-x = \sum_{i=1}^{n} -(a_i x b_i) = \sum_{i=1}^{n} (-a_i) x b_i \in I_x,$$

joten $(I, +)$ on suljettu myös vasta-alkion suhteen. Olemme näyttäneet, että $(I, +)$ on ryhmän $(R, +)$ aliryhmä.

Olkoon $r \in R$ mielivaltainen ja olkoon $x = \sum_{i=1}^{n} a_i x b_i \in I_x$. Tällöin (renkaan osittelulait)

$$rx = r(\sum_{i=1}^{n} a_i x b_i) = \sum_{i=1}^{n} (r a_i) x b_i \in I_x,$$

$$xr = (\sum_{i=1}^{n} a_i x b_i) r = \sum_{i=1}^{n} a_i x (b_i r) \in I_x,$$

joten myös toinen ideaalin ehto on voimassa. Olemme osoittaneet, että I_x on renkaan R ideaali. Valitsemalla $n = 1, a_1 = b_1 = 1_R$, nähdään myös, että $x = 1_R x 1_R \in I_x$.

b) Jos R on vaihdannainen $a_i x b_i = a_i b_i x = c_i x$ kaikilla $a_i, b_i \in R$, jolloin (osittelulaki)

$$\sum_{i=1}^{n} a_i x b_i = \sum_{i=1}^{n} c_i x = (\sum_{i=1}^{n} c_i) x = ax,$$

missä $a = \sum_{i=1}^{n} c_i$. Näin ollen

$$I_x \subset \{ax \mid a \in R\}.$$

Koska $x \in I_x$, toisaalta ideaalin ehdoista helposti saadaan

$$\{ax \mid a \in R\} \subset I_x.$$

Näin ollen $I_x = \{ax \mid a \in R\}$.

3. Kaikki polynomifunktiot $p\colon \mathbb{R} \to \mathbb{R}$ muodostavat renkaan $P(\mathbb{R})$ pisteittäisen yhteen- ja kertolaskun suhteen. Tämä pidetään tunnettuna. Olkoon $q\colon \mathbb{R} \to \mathbb{R}$, $q(x) = x^2 + 1$. Olkoon $I_q \subset P(\mathbb{R})$ kuten edellisessä tehtävässä. Osoita, että tekijärenkaassa $P(\mathbb{R})/I_q$ on olemassa sellainen alkio i, jolle pätee $i^2 = -1$.

Ratkaisu: Olkoon $p\colon \mathbb{R} \to \mathbb{R}$, $p(x) = x$ kaikilla $x \in \mathbb{R}$ (p on siis identtinen kuvaus). Tällöin $p^2 + 1 = q \in I_q$, joten tekijärenkaassa $P(\mathbb{R})/I_q$

$$\overline{p}^2 + 1 = \overline{p^2 + 1} = 0.$$

Näin ollen $i^2 = -1$ kun valitaan $i = \overline{p}$.

4. a) Lemmassa 1.94 osoitetaan, että kokonaislukujen $m, n \in \mathbb{Z}$ suurin yhteinen tekijä $c = \text{syt}(m, n)$ voidaan esittää muodossa $c = mk + nl$, $k, l \in \mathbb{Z}$, mutta ei anneta mitään käytännön menetelmää, jonka avulla tällainen esitys voidaan löytää. Suosituin sellainen menetelmä on kuuluisa *Eukleideen algoritmi* (engl. Euclidean algorithm). Palauta mieleen tai selvitä (esim. internetin avulla) miten tämä algoritmi etenee. Esitä sen avulla $c = \text{syt}(126, 35)$ muodossa $c = 126k + 35l$.
b) Lauseen 1.95 todistuksessa näytetään, miten Lemman 1.94 tuloksen avulla voidaan laskea alkioiden käänteisalkioita renkaassa $\mathbb{Z}_m$ (jos olemassa). Laske tämän menetelmän ja Eukleideen algoritmin avulla 16_{21}^{-1}, 15_{21}^{-1}, 16_{23}^{-1}, jos ne ovat olemassa. Jos käänteisalkiota ei ole olemassa, selitä miksi.

Ratkaisu: a) Eukleideen algoritmi: Olkoot $m, n \in \mathbb{Z}$, $n \neq 0$. Oletetaan, että $m \geq n$. Kokonaislukujen *jakoyhtälön* nojalla on olemassa $0 \leq r_1 < |n|$ ja $k \in \mathbb{Z}$ siten, että

$$m = k_1 n + r_1.$$

Jos $r_1 \neq 0$ soveltamalla jakoyhtälö samalla tavalla pariin (n, r_1) (pariin (m, n) sijaan), nähdään, että

$$n = k_2 r_1 + r_2,$$

missä $0 \leq r_2 < r_1$. Jatkamalla samalla tavalla saadaan yhtälöitä

$$m = k_1 n + r_1,$$

$$n = k_2 r_1 + r_2,$$

$$r_1 = k_3 r_2 + r_3,$$

$$\dots$$

$$r_{i-2} = k_i r_{i-1} + r_i,$$

missä $r_1 > r_2 > \ldots > r_i \geq 0$. Koska ei-negatiiviset kokonaisluvut r_j pienenevät aidosti indeksin j mukaan, jossain vaiheessa päästään tilanteseen, jossa $r_{i+1} = 0$, jolloin siis

$$m = k_1 n + r_1,$$

$$n = k_2 r_1 + r_2,$$

$$r_1 = k_3 r_2 + r_3,$$

$$\dots$$

$$r_{i-2} = k_i r_{i-1} + r_i,$$

$$r_{i-1} = k_{i+1} r_i.$$

Tällöin $r_i = \text{syt}(m, n)$. Tämä nähdään seuraavasti. Viimeisestä yhtälöstä seuraa, että $r_i | r_{i-1}$. Tällöin toiseksi viimeisestä yhtälöstä seuraa, että $r_i | r_{i-2}$ jne. Nousemalla ylöspäin nähdään induktiolla, että $r_i | r_j$ kaikilla $j = 0, 1, \ldots, i$, missä $r_0 = n$. Viimeiksi ensimmäisestä yhtälöstä $m = k_1 r_0 + r_1$ nähdään, että $r_i | m$. Näin ollen r_i on ainakin lukujen m, n yhteinen tekijä. Näytetään seuraavaksi, että r_i voidaan esittää muodossa $r_i = mk + nl$, $k, l \in \mathbb{Z}$. Ensimmäisestä yhtälöstä seuraa, että

$r_1 = m + (-k_1)n$. Sijoittamalla tämä r_1:n esitys toiseen yhtälöön saadaan r_2 esitettyä muodossa $r_2 = tm + sn$ joillakin $t, s \in \mathbb{Z}$. Jatkamalla näin saadaan jokainen r_i esitettyä tällaisessa muodossa induktiivisesti. Lopuksi saadaan samanlainen esitys luvulle r_i. Olkoon nyt r jokin lukujen m, n yhteinen tekijä. Tällöin se jakaa myös jokaisen lineaarisen kombinaatioon muotoa $tm + sn$, $t, s \in \mathbb{Z}$, erityisesti on luvun r_i tekijä.

Olemme näyttäneet, että r_i on lukujen m ja n tekijä ja lisäksi jokainen näiden lukujen tekijä on myös luvun r_i tekijä. Toisin sanoen r_i on lukujen m ja n suurin yhteinen tekijä. Lisäksi algoritmin avulla saadaan muodostettua esitys $r_i = mk + nl$, $k, l \in \mathbb{Z}$.

Huomautus Eukleideen algoritmi antaa toisen tavan todistaa kahden kokonaisluvun suurimman yhteisen luvun sekä esityksen $\text{syt}(n, m) = kn + ml$ olemassaoloa (eli Lemman 1.94 tulosta).

Sovelletaan Eukleideen algoritmia pariin $(126, 35)$.

$$126 = 3 \cdot 35 + 21,$$

$$35 = 21 + 14,$$

$$21 = 14 + 7,$$

$$14 = 2 \cdot 7.$$

Näin ollen $\text{syt}(126, 35) = 7$ ja

$$7 = 21 - 14 = 21 - (35 - 21) = -35 + 2 \cdot 21 = -35 + 2(126 - 3 \cdot 35) = 2 \cdot 26 - 7 \cdot 35.$$

Huomaa, että käytännössä esitys $7 = k126 + l35$ kannattaa muodostaa ”alhaalta ylöspäin”.

b) Lausen 1.95 nojalla alkiolla m_n on renkaassa $\mathbb{Z}_n$ käänteisalkio kertolaskun suhteen jos ja vain jos m ja n ovat suhteellisia alkulukuja. Lisäksi Lauseen todistuksesta seuraa, että tämä käänteisluku löydetään käytännössä esityksen $1 = km + ln$ avulla, missä $1 = \text{syt}(n, m)$ tällöin.

Koska $\text{syt}(15, 21) = 3$, käänteisluku 15_{21}^{-1} ei ole olemassa. Toisaalta $\text{syt}(16, 21) = 1$ ja $\text{syt}(16, 23) = 1$, joten kumpikin käänteisalkio 16_{21}^{-1}, , 16_{23}^{-1} on olemassa. Löydetään ensin Eukleideen algoritmin avulla kokonaislukuja $k, l \in \mathbb{Z}$, joille $16k + 21l = 1$.

$$21 = 16 + 5,$$

$$16 = 3 \cdot 5 + 1,$$

joten $1 = 16 - 3 \cdot 5 = 16 - 3(21 - 16) = (-3) \cdot 21 + 4 \cdot 16$. Siirtymällä tästä kokonaislukuihin modulo 21, nähdään, että

$$1_{21} = (-3)_{21} \cdot 21_{21} + 4_{21} \cdot 16_{21} = 4_{21} \cdot 16_{21}.$$

Näin ollen $16_{21}^{-1} = 4_{21}$.

Samalla tavalla lasketaan 16_{23}^{-1}.

$$23 = 16 + 7,$$

$$16 = 2 \cdot 7 + 2,$$

$$7 = 3 \cdot 2 + 1,$$

joten $1 = 7 - 3 \cdot 2 = 7 - 3(16 - 2 \cdot 7) = (-3) \cdot 16 + 7 \cdot 7 = (-3) \cdot 16 + 7(23 - 16) = 7 \cdot 23 - 10 \cdot 16$. Siirtymällä tästä kokonaislukuihin modulo 23, nähdään, että

$$1_{23} = (-10)_{23} \cdot 16_{23} = 13_{23} \cdot 16_{23}.$$

Näin ollen $16_{23}^{-1} = 13_{23}$.

5. Olkoot $(R, +, \cdot)$ ja $(R', +, \cdot)$ renkaita. Määritellään karteesisessa tulossa $R \times R'$ laskutoimituksia $+, \cdot$ "koordinaateittain" eli kaavoilla

$$(r_1, r_1') + (r_2, r_2') = (r_1 + r_2, r_1' + r_2'),$$

$$(r_1, r_1') \cdot (r_2, r_2') = (r_1 r_2, r_1' r_2')$$

Tällöin (tämä voidaan pitää tunnettuna) $(R \times R', +, \cdot)$ on rengas, jota sanotaan renkaiden $(R, +, \cdot)$ ja $(R', +, \cdot)$ *tulorenkaaksi*.

a) Osoita, että kuvaus $f\colon \mathbb{Z} \to \mathbb{Z}_2 \times \mathbb{Z}_3$, $f(n) = (n_2, n_3)$ on surjektiivinen rengashomomorfismi.

b) Osoita a)-kohdan ja renkaiden isomorfialauseen avulla, että rengas $\mathbb{Z}_6$ on isomorfinen tulorenkaan $\mathbb{Z}_2 \times \mathbb{Z}_3$ kanssa.

c) Onko rengas $\mathbb{Z}_4$ isomorfinen tulorenkaan $\mathbb{Z}_2 \times \mathbb{Z}_2$ kanssa? Onko Abelin ryhmä $(\mathbb{Z}_4, +)$ isomorfinen Abelin ryhmän $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ kanssa?

Ratkaisu: Olkoot $m, n \in \mathbb{Z}$. Tällöin

$$f(nm) = ((n+m)_2, (n+m)_3) = (n_2+m_2, n_3+m_3) = (n_2, n_3)+(m_2, m_3) = f(n)+f(m),$$

$$f(nm) = ((nm)_2, (nm)_3) = (n_2 m_2, n_3 m_3) = (n_2, n_3)(m_2, m_3) = f(n)f(m).$$

Lisäksi $f(1) = (1_2, 1_3)$ on tulorenkaan $R \times R'$ ykkösalkio, sillä kaikilla $n, m \in \mathbb{Z}$ pätee $(n_2, m_3)(1_2, 1_3) = (n_2 1_2, m_3, 1_3) = (n_2, m_2)$. Näin ollen f on rengashomomorfismi.

Osoitetaan, että f on surjektio. Yksi tapa on käydä läpi maalijoukon $\mathbb{Z}_2 \times Z_3$ alkioita ja löytää jokaiselle ainakin yksi lähtöjoukon alkio, joka kuvautuu sille. Tämä on periaatteessa mahdollista, sillä maalijoukko $\mathbb{Z}_2 \times Z_3$ on suhteellisen pieni äärellinen joukko, sillä on vain 6 alkiota. Koska

$$f(0) = (0_2, 0_3),$$

$$f(1) = (1_2, 1_3),$$

$$f(2) = (2_2, 2_3) = (0_2, 2_3),$$

$$f(3) = (3_2, 3_3) = (1_2, 0_3),$$
$$f(4) = (4_2, 4_3) = (0_2, 1_3),$$
$$f(5) = (5_2, 5_3) = (1_2, 2_3),$$

nähdään suoraan, että f on surjektio.

Abstraktimpi tapaa lähestyä surjektiivisyyttä perustuu Lemman 1.94 käyttöön. Nimittäin 2 ja 3 ovat suhteellisia alkulukuja, joten Lemman 1.94 nojalla on olemassa $k, l \in \mathbb{Z}$ siten, että $1 = 2k + 3l$ (tässä tapauksessa voidaan selvästi valita $k = -1$, $l = 1$). Olkoot $s = 2k$, $t = 3l$, tällöin $s \in 2\mathbb{Z}$, $t \in 3\mathbb{Z}$ ja $s + t = 1$. Tästä seuraa, että

$$s_2 = 0_2, s_3 = s_3 + t_3 = 1_3,$$

$$t_2 = s_2 + t_2 = 1_2, t_3 = 0.$$

Näin ollen $f(t) = (1_2, 0_3)$, $f(s) = (0_2, 1_3)$. Tästä seuraa, että kaikilla $a, b \in \mathbb{Z}$

$$f(at + bs) = a(1_2, 0_3) + b(0_2, 1_3) = (a_2, b_3),$$

joten f on surjektio.

Huomautus: Samalla tavalla voidaan osoittaa yleisesti, että tulorengas $\mathbb{Z}_m \times Z_n$ on isomorfinen renkaan $\mathbb{Z}_{nm}$ kanssa kun n ja m ovat suhteellisia alkulukuja. Vielä yleisemmin vastaava tulos renkaiden teoriassa tunnetaan nimellä "Kiinalainen jäännöslause" (Chinese Reminder Theorem), googlaa, jos kiinnostaa.

c) Rengas $(\mathbb{Z}_4, +, \cdot)$ ei ole isomorfinen tulorenkaan $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, \cdot)$ kanssa. Itse asiassa jo Abelin ryhmät $(\mathbb{Z}_4, +)$ ja $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ eivät ole isomorfisia (jolloin selvästi myös renkaat eivät ole). Tämä johtuu siitä, että ryhmässä $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ jokaiselle alkiolle x pätee $2x = 0$. Ryhmässä $\mathbb{Z}_4$ on taas olemassa alkio $x = 1_4$, jolle tämä ei päde, $2 \cdot 1_4 = 2_4 \neq 0_4$.

Yleisemmin voidaan osoittaa, että ryhmät $(\mathbb{Z}_{nm}, +)$ ja $(\mathbb{Z}_n, +) \times (Z_m, +)$ ovat isomorfisia jos ja vain jos $\text{syt}(n, m) = 1$. Vastaaville renkaille pätee sama tulos.

6. Olkoon $V = \{x \in \mathbb{R} \mid x > 0\}$ positiivisten reaalilukujen joukko.
Määritellään laskutoimitukset $\oplus\colon V \times V \to V$, $\odot\colon \mathbb{R} \times V \to V$ kaavoilla

$$\oplus(x, y) = xy \text{ (tavallinen reaalilukujen kertolasku)},$$

$$\odot(r, x) = x^r \text{ (tavallinen reaalilukujen eskponentti)}.$$

Osoita, että $(V, \oplus, \odot)$ on $\mathbb{R}$-vektoriavaruus. Mikä on tämän vektoriavaruuden nollavektori? Mikä on vektorin $x \in V$ vasta-vektori?

Ratkaisu: Laskutoimitukset ovat hyvinmääriteltyjä, sillä kahden positiivisen reaaliluvun tulo on aina positiivinen reaaliluku, lisäksi positiivisen reaaliluvun x potenssi x^r on positiivinen reaaliluku kaikilla $r \in \mathbb{R}$.

Tarkistetaan vektoriavaruuden ehtoja (i)-(viii) määritelmästä 2.1. Olkoot $x, y, z \in V$, $r, s \in \mathbb{R}$.
(i) $(x \oplus y) \oplus z = (xy)z = x(yz) = x \oplus (y \oplus z)$, sillä reaalilukujen kertolasku on tunnetusti liitännäinen operaatio.
(ii) $x \oplus y = xy = yx = y \oplus x$, sillä reaalilukujen kertolasku on tunnetusti vaihdannainen operaatio.
(iii) Nolla-vektoriksi kelpaa reaaliluku 1, sillä $x \oplus 1 = x1 = x$ kaikilla $x \in V$.
(iv) Alkion $x \in V$ vasta-vektori on $y = x^{-1}$, sillä $x \oplus (1/x) = xx^{-1} = 1$, missä 1 on edellisen kohdan nojalla nolla-vektori. Huomaa, että $1/x$ on hyvinmääritelty kaikilla $x \in V$, sillä $0 \notin V$.
(v)

$$r \odot (s \odot x) = r \odot x^s = (x^s)^r = x^{sr} = (sr) \odot x.$$

potenssisäntöjen nojalla.
(vi)

$$(r + s) \odot x = x^{r+s} = x^r x^s = (r \odot x)(s \odot x) = (r \odot x) \oplus (s \odot x).$$

(vii)

$$r \odot (x \oplus y) = r \odot (xy) = (xy)^r = x^r y^r = (r \odot x)(s \odot y) = (r \odot x) \oplus (s \odot y).$$

Huomaa, että kohdissa (vi) ja (vii) käytettiin potenssisääntöjä $x^{r+s} = x^r x^s$, $(xy)^r = x^r y^r$.
(viii) $1 \odot x = x^1 = x$.

Kohdasta (iii) yllä seuraa, että vektoriavaruusden V nolla-vektori on $1 \in V$. Vektorin $v \in V$ vasta-vektori on v:n käänteisluku v^{-1}.

7.* Olkoon $(G, +)$ ryhmä. Sanomme, että G on *jakoryhmä*, jos kaikilla $x \in G$ ja $n \in \mathbb{N}, n \geq 1$ on olemassa $y \in G$ jolle $y^n = x$. Toisin sanoen jakoryhmä on ryhmä, jossa jokaisella alkiolla on olemassa jokaisen kertaluvun *juuri*.
Jos $(G, +)$ on additiivisesti merkitty Abelin ryhmä, se on jakoryhmä mikäli kaikilla $x \in G, n \in \mathbb{N}, n \geq 1$ on olemassa y jolle pätee $ny = x$.

a) Anna esimerkkejä Abelin ryhmistä, jotka ovat jakoryhmiä ja Abelin ryhmistä, jotka eivät ole jakoryhmiä. Onko jakoryhmän alkion n:s juuri välttämättä yksikäsitteinen? (Vihje: mieti esim. kompleksilukujen kertolaskua).

b) Olkoon $(V, +, \cdot)$ $\mathbb{Q}$-vektoriavaruus. Osoita, että $(V, +)$ on jakoryhmä.

c) Olkoon $(G, +)$ jakoryhmä. Voidaanko joukossa G määritellä $\mathbb{Q}$-skalaarikertolasku $\cdot : \mathbb{Q} \times G \to G$, siten, että $(G, +, \cdot)$ on $\mathbb{Q}$-vektoriavaruus? Jos voidaan, niin millä lisäehdoilla? Onko tällainen skalaarikertolasku tällöin yksikäsitteinen?

Ratkaisu: a) Nollasta eroavien reaalilukujen muodostama ryhmä $(\mathbb{R}^*, \cdot)$ ei ole jakoryhmä, sillä negatiivisilla luvuilla ei ole neliöjuurta. Sen aliryhmä $(\mathbb{R}_+, \cdot)$, missä $\mathbb{R}_+$ on positiivisten reaalilukujen joukko $\{x \in \mathbb{R} \mid x > 0\}$ taas on jakoryhmä kertolaskun suhteen, sillä jokaisella positiivisella reaaliluvulla $x > 0$ on tunnetusti

(jopa yksikäsitteinen) n:nnen kertaluvun juuri $\sqrt[n]{x}$. Nollasta eroavien kompleksilukujen ryhmä $\mathbb{C}^*$ kertolaskun suhteen on jakoryhmä, sillä jokaisella kompleksiluvulla $(x, y) = (r\cos\alpha, r\sin\alpha)$ on tunnetusti jokaisella $n \in \mathbb{N}$, $n \geq 1$ jopa n erilaista n:nnen kertaluvun juurta, sellaisiksi kelpaavat kompleksiluvut

$$(\sqrt[n]{r}\cos(\frac{\alpha + 2k\pi}{n}), \sqrt[n]{r}\sin(\frac{\alpha + 2k\pi}{n}), k = 0, \ldots, n-1.$$

Tästä esimerkistä myös nähdään, että jakoryhmässä alkion n:s juuri ei välttämättä ole yksikäsitteinen.

b) Olkoon $(V, +, \cdot)$ $\mathbb{Q}$-vektoriavaruus, olkoon $v \in V$ ja $n \in \mathbb{N}, n \geq 1$. Tällöin on olemassa $w = \frac{1}{n} \cdot v \in V$. Vektoriavaruuden ehdoista tällöin seuraa, että

$$n \cdot w = n \cdot (\frac{1}{n} \cdot v) = (n\frac{1}{n}) \cdot v = 1 \cdot v = v.$$

Kuitenkin

$$n \cdot w = (\underbrace{1 + \ldots + 1}_{n \text{ kpl}})w = \underbrace{1w + \ldots + 1w}_{n \text{ kpl}} = \underbrace{w + \ldots + w}_{n \text{ kpl}} = nw.$$

Tässä $n \cdot w$ on skalaarikertolasku ja nw on alkion w monikerta Abelin ryhmässä $(V, +)$ (kts. myös huomautuksia asiasta Luvun 2 sivuilla 5-6). Näin ollen $nw = v$. Ollaan osoitettu, että $(V, +)$ on jakoryhmä.

c) Olkoon $(G, +)$ jakoryhmä. Oletetaan, että on olemassa skalaarikertolasku $\cdot : \mathbb{Q} \times G \to G$, siten, että $(G, +, \cdot)$ on $\mathbb{Q}$-vektoriavaruus. Tällöin $(G, +)$ on erityisesti Abelin ryhmä. Olkoon $v \in G$. Olkoon $n \in \mathbb{N}$ ja $n \geq 1$ ja olkoon $w \in G$ sellainen, että $nw = v$ ryhmässä $(G, +)$. Kuten b)-kohdan todistuksen kohdalla nähdään, että $v = nw = n \cdot w$. Vektoriavaruuden ehdoista seuraa tällöin, että

$$w = 1 \cdot w = (\frac{1}{n}n) \cdot w = \frac{1}{n} \cdot (n \cdot w) = \frac{1}{n} \cdot v.$$

Näin ollen alkio w, jolle pätee $nw = v$ on tällöin välttämättä *yksikäsitteinen*, sen täytyy olla alkio $\frac{1}{n} \cdot v$. Erityisesti sellaisessa jakoryhmässä, jossa n:s juuri ei ole yksikäsitteinen, ei voida määritellä $\mathbb{Q}$-skalaarikertolasku joka tekisi siitä $\mathbb{Q}$-vektoriavaruuden. Esimerkiksi a)-kohdassa mainittu nollasta eroavien kompleksilukujen ryhmä (kertolaskun suhteen) on Abelin jakoryhmä, josta ei saa $\mathbb{Q}$-vektoriavaruutta.

Osoitetaan kääntäen, että jokaisessa vaihdannaisessa jakoryhmässä $(G, +)$, jossa jokaisen alkion n:s juuri on yksikäsitteinen, voidaan määritellä $\mathbb{Q}$-skalaarikertolasku $\cdot : \mathbb{Q} \times G \to G$ siten, että $(G, +, \cdot)$. Väitämme lisäksi, että tällainen skalaarikertolasku on tällöin yksikäsitteinen. Olkoon $v \in G$ ja olkoon $q = m/n \in \mathbb{Q}$. Jos skalaarikertolasku $\cdot : \mathbb{Q} \times G \to G$ on olemassa, kuten yllä nähdään, että $w = \frac{1}{n} \cdot v$ on sellainen alkio, jolle $nw = v$. Oletuksen mukaan sellainen alkio on yksikäsitteinen. Lisäksi

$$q \cdot v = \frac{m}{n} \cdot v = m \cdot (\frac{1}{n}v) = m \cdot w = mw,$$

missä mw on alkion w monikerta Abelin ryhmässä $(G, +)$. Näin ollen jakoryhmän $(G, +)$ ryhmästruktuuri määrittelee tällöin skaalarikertolaskun yksikäsitteisesti. Kääntäen määritellään skalaarikertolasku $\cdot\colon \mathbb{Q} \times G \to G$ kaavalla

$$q \cdot v = mw, \tag{3}$$

missä $q = m/n$ ja $w \in G$ on sellainen, että pätee $nw = v$. Osoitetaan, että tämä on hyvinmääritelty kuvaus. Nimittäin jokainen rationaaliluku q voidaan esittää muodossa m/n monella tavalla. Olkoot $m, m', n, n' \in \mathbb{Z}, n, n \neq 0$ sellaisia, että $m/n = m'/n'$. Tällöin $mn' = m'n$ kokonaislukujen joukossa $\mathbb{Z}$. Olkoot $w, w' \in G$ sellaisia, että $nw = v = n'w'$. Nyt

$$n(mw) = m(nw) = m(n'w') = (mn')w' = (m'n)w' = n(m'w').$$

Koska oletamme, että jokaisen alkion n:s juuri ryhmässä G on yksikäsitteinen, tästä seuraa, että $mw = m'w'$. Näin ollen kaavalla 3 määritelmä laskutoimitus on hyvinmääritelty, toisin sanoen ei riipu luvun q esityksestä muodossa m/n.

Helposti nähdään, että tällä skalaarikertolaskulla varustettuna ryhmästä $(G, +)$ tulee $\mathbb{Q}$-vektoriavaruus $(G, +, \cdot)$. Vektoriavaruuden ehtojen tarkistus sivutetaan tässä.