Äärellisulotteinen lineaarialgebra, kevät 2015.
Harjoitus 2.
Ratkaisuehdotuksia.

1. Olkoot X ja Y joukkoja ja olkoon $f\colon X \to Y$ kuvaus.
   a) Oletetaan, että $X \neq \emptyset$. Osoita, että f on injektio jos ja vain jos on olemassa $g\colon Y \to X$ siten, että $g \circ f = \mathrm{id}_X$. Onko tällainen kuvaus g silloin yksikäsitteinen? Mitä tapahtuu kun $X = \emptyset$?
   b) Osoita, että f on surjektio jos ja vain jos on olemassa $g\colon Y \to X$ siten, että $f \circ g = \mathrm{id}_Y$. Onko tällainen kuvaus g silloin yksikäsitteinen?
   Tässä $\mathrm{id}_A\colon A \to A$ tarkoittaa joukon A identtistä kuvausta.

   Ratkaisu: a) Olkoot $f\colon X \to Y$ ja $g\colon Y \to X$ sellaisia, että $g \circ f = \mathrm{id}_X$. Olkoot $x, x' \in X$ siten, että $f(x) = f(x')$. Tällöin

   $$x = \mathrm{id}_X(x) = (g \circ f)(x) = g(f(x)) = g(f(x')) = (g \circ f)(x') = \mathrm{id}_X(x') = x'.$$

   Näin ollen f on injektio.

   Kääntäen olkoon $f\colon X \to Y$ injektio, missä $X \neq \emptyset$. Konstruoidaan $g\colon Y \to X$ siten, että $g \circ f = \mathrm{id}_X$.Tämä ehto siis tarkoittaa täsmälleen sitä, että kaikilla $x \in X$ pätee

   $$g(f(x)) = x \tag{1}$$

   eikä g:stä vaadita mitään muuta. Tästä nähdään, että jos $y \in Y$ on muotoa $y = f(x)$ jollakin $x \in X$, niin on pakko olla $g(y) = x$, erityisesti kuvauksen g arvo alkiossa y on yksikäsitteisesti määrätty. Jos taas $y \notin f(X)$ ei ole kuvajoukon $f(X)$ alkio, niin ehto 1 ei kerro arvosta $g(y)$ mitään, joten se voidaan valita vapaasti. Tällöin voidaan asettaa siis $g(y) = x_0$, missä x_0 on mielivaltainen X:n alkio. Sellainen on olemassa, koska oletamme, että X on epätyhjä (juuri tässä kohdassa tarvitaan oletusta "X on epätyhjä").

   Täsmällinen kuvauksen g määritelmä on siis seuraava. Valitaan $x_0 \in X$, tämä voidaan tehdä, koska X oletetaan olevan epätyhjä. Määritellään

   $$g(y) = \begin{cases} x, \text{ jos } f(x) = y, \\ x_0, \text{ jos } y \notin f(X). \end{cases}$$

   Osoitetaan, että tämä sääntö määrittelee kuvauksen. Nimittäin jos $y \in f(X)$, kuvauksen g määritelmä näyttyy riippuvan sellaisen $x \in X$ valinnasta, jolle pätee $f(x) = y$. Mutta oletamme f injektioksi, joten, jos on olemassa $x \in X$ jolle pätee $f(x) = y$, niin tällainen x on **yksikäsitteinen** (kaksi eri alkiota eivät voi kuvautua injektiossa samalle alkiolle y). Näin ollen g on hyvinmääritelty kuvaus. Kaikilla $x \in X$ pätee

   $$(g \circ f)(x) = g(f(x)) = x,$$

   sillä jos valitaan $y = f(x)$, niin $x \in X$ on sellainen, että $f(x) = y$. Olemme osoittaneet, että g on olemassa. Lisäksi edellä käydystä tarkastelusta seuraa, että

ehdon täyttävän g arvot joukossa $f(X)$ ovat yksikäsitteisesti määrättyjä. Joukossa $Y \setminus f(X)$ kuvauksen g arvot voidaan taas valita vapaasti. Tästä seuraa, että kuvaus g on yksikäsitteinen jos ja vain jos f on bijektio tai $X = \{x_0\}$ on yhden alkion joukko. Nimittäin, jos $f(X) = Y$ (eli f on surjektio), joukko $Y \setminus f(X)$ on tyhjä, eikä mitään vapaa valintaa päästä tekemään. Tällöin f on siis bijektio ja g on välttämättä sen **käänteiskuvaus** $f^{-1}\colon Y \to X$. Jos taas $X = \{x_0\}$ on yhden alkion joukko, niin g:n arvoja joukon $f(X)$ ulkopuolella voidaan valita vain yhdellä tavalla eli asettamalla $g(y) = x_0$ kaikilla $y \in Y \setminus f(X)$ (itse asiassa väistämättä myös kaikilla $y \in Y$). Silloinkin g on yksikäsitteinen.

Oletetaan kääntäen, että $f(X) \neq Y$ ja X:ssä on vahintaan kaksi eri alkiota $x_0, x_1 \in X$. Tällöin kaavoilla

$$g_1(y) = \begin{cases} x, \text{ jos } f(x) = y, \\ x_0, \text{ jos } y \notin f(X), \end{cases}$$

$$g_2(y) = \begin{cases} x, \text{ jos } f(x) = y, \\ x_1, \text{ jos } y \notin f(X). \end{cases}$$

määritellyt kuvauksen $g_1, g_2\colon Y \to X$ ovat eri kuvauksia ja kummallekin pätee $g_1 \circ f = \mathrm{id}_X = g_2 \circ f$.

Huomautus: Itse asiassa g ei tarvitsee määritellä vakiona joukon $f(X)$ ulkopuolella. Yleinen ehdon $g \circ f = \mathrm{id}_X$ määrittelemä kuvaus on muotoa

$$g(y) = \begin{cases} x, \text{ jos } f(x) = y, \\ h(y), \text{ jos } y \notin f(X), \end{cases}$$

missä $h\colon Y \setminus f(X) \to X$ on mielivaltainen kuvaus (eli valitaan jokaisella $y \notin f(X)$ sen arvo $g(y) = h(y) \in X$ mielivaltaisesti muiden joukon $Y \setminus f(X)$ arvoista riippumatta).

Mietitään vielä mitä tapahtuu jos $X = \emptyset$. Ainoa kuvaus $f\colon \emptyset \to Y$ on niin sanottu *tyhjä kuvaus* $\emptyset\colon \emptyset \to Y$. Tämän ymmärtämiseksi palautetaan mieleen kuvauksen formaali määritelmä. Nimittäin formaalisti kuvaus $f\colon X \to Y$ on sama asia kuin sen *graafi*

$$\{(x, f(x)) \mid x \in X\}$$

eli sellainen *relaatio* $f \subset X \times Y$ joka toteuttaa seuraavaa kaksi ehtoa.

(1) Kaikilla $x \in X$ on olemassa $y \in Y$ jolle $(x, y) \in f$ (intuitiivisesti - "jokaisella lähtöjoukon alkiolla x on kuva $f(x)$").

(2) Kaikilla $x \in X$ ja $y, z \in Y$ ehdoista $(x, y), (x, z) \in f$ seuraa, että $y = z$ (intuitiivisesti - mikään x ei voi kuvautua kahdelle eri alkiolle, $y = f(x) = z$).

Olkoon X tyhjä. Tällöin joukko $X \times Y$ on myös tyhjä ja ainoa tyhjän joukon osajoukko on tyhjä joukko itse. Näin ollen ainoa mahdollinen relaatio $f\colon X \to Y$ on tällöin tyhjä joukko. "Tyhjän joukon logiikalla" nähdään, että tämä relaatio toteuttaa kuvauksen ehdot (1) ja (2) yllä. Esimerkiksi kaikilla $x \in X = \emptyset$ on olemassa

$y \in Y$ siten, että $(x, y) \in \emptyset$, sillä jos näin ei olisi, olisi olemassa $x \in X$ jolle tämä ei ole totta. Tämä erityisesti tarkoittaa sitä, että löytyisi jokin alkion $x \in X$, mikä on mahdotonta, sillä X on tyhjä[1]. Samalla tavalla nähdään, että jokaisen $x \in X$ kuva $f(x)$ on yksikäsitteinen.

Näin ollen, kiinteällä Y, on olemassa tasan yksi kuvaus $f\colon \emptyset \to Y$. Tyhjän joukon logiikalla helposti nähdään, että tämä kuvaus on injektio. Mietitään löytyykö kuitenkin kuvausta $g\colon Y \to X$, jolle pätee $g \circ f = \mathrm{id}_X$. Jos $Y \neq \emptyset$, niin ei ole olemassa kuvauksia $g\colon Y \to \emptyset$ (mihin kuvaat Y:n alkioita, jos maalipuoli on tyhjä?). Jos taas $Y = \emptyset$ etsitään kuvausta $g\colon \emptyset \to \emptyset$ ja yllä olevan nojalla on olemassa tasan yksi sellainen kuvaus - tyhjä kuvaus. Tällöin $g \circ f = \mathrm{id}_X$ pätee, sillä tämän yhtälön molemmat puolet on ainoa kuvaus $\emptyset \to \emptyset$.

Yhteenveto: g on yksikäsitteinen jos ja vain jos f in bijektio tai joukossa X on korkeintaan yksi alkio. Jos $X = \emptyset$ kuvaus g on olemassa jos ja vain jos $Y = \emptyset$.

b) Olkoot $f\colon X \to Y$ ja $g\colon Y \to X$ sellaisia, että $f \circ g = \mathrm{id}_Y$. Olkoon $y \in Y$. Tällöin alkiolle $x = g(y) \in X$ pätee

$$f(x) = f(g(y)) = (f \circ g)(y) = \mathrm{id}_Y(y) = y.$$

Tämä osoittaa sen, että f on surjektio.

Kääntäen olkoon $f\colon X \to Y$ surjektio. Konstruoidaan sellainen $g\colon Y \to X$ jolle pätee $f \circ g = \mathrm{id}_Y$. Olkoon $y \in Y$. Tällöin täytyy päteä $f(g(y)) = y$, joten $x = g(y)$ on sellainen alkio, jolle pätee $f(x) = y$. Tällainen taas löytyy mille tahansa y koska f on surjektio.

Täsmällisesti menetellään seuraavasti. Jokaisella $y \in Y$ *valitaan* yksi $x_y = x \in X$ jolle pätee $f(x_y) = y$. Tämä on mahdollista, koska f on surjektio[2]. Jokaisella $y \in Y$ asetetaan $g(y) = x_y$. Tällöin kaikilla $y \in Y$ pätee

$$(f \circ g)(y) = f(g(y)) = f(x_y) = y = \mathrm{id}_X(y).$$

Kuvaus g ei ole yksikäsitteinen jos ainakin yhdellä $y \in Y$ voidaan tehdä x_y:n valinta ainakin kahdella eri tavalla eli jos ja vain jos jollakin $y \in Y$ on olemassa $x, x' \in X$, $x \neq x'$ siten, että $f(x) = y = f(x')$. Selvästi tämä on yhtäpitävä sen kanssa, että f

[1]Tämä on esimerkki niin sanotusta ”tyhjän joukon loogikasta”. Tyhjälle joukolle X muotoa ”kaikilla $x \in X$...” olevat väitteet ovat aina tosia. Nimittäin jos jokin tällainen väite ei olisi totta, löytyisi *vastaesimerkki* eli sellainen $x \in X$ jolle väite ei päde, jolloin erityisesti tyhjästä joukosta löytyisi alkio.

[2]Jos ollaan ihan tarkoja, tässä kohdassa joudumme käyttämään kuuluisaa *valintaaksiomaa*. Asian ydin on seuraava. Koska f on surjektio, jokaiselle kiinteälle $y \in Y$ voidaan valita jokin $x \in X$ jolle pätee $f(x) = y$, mutta yleisesti ottaen tämä x ei ole yksikäsitteinen, joten joudutaan tekemään *valinta*. Todistuksessa teemme tällaisen valinnan jokaisella $y \in Y$ *samanaikaisesti*. Intuitiivisesti on selvää, että tämän pitäisi olla mahdollista, mutta, ehkä yllättäen, tätä ei voi johtaa muista joukko-opin periaatteista, joten pitää turvautua valintaaksiomaan, joka sanoo, että tämäntyyppinen samanaikainen valinta voidaan aina tehdä, olipa joukko Y kuinka tahansa iso.

ei ole injektio. Näin ollen g on yksikäsitteinen jos ja vain jos f on bijektio, jolloin välttämättä $g = f^{-1}$.

Algebrallinen tausta. Olkoon $\cdot$ liitännäinen laskutoimitus joukossa Y jolla on neutraalialkio e. Alkion $x \in Y$ *vasemmanpuoleinen käänteisalkio* on sellainen $y \in Y$, jolle pätee $yx = e$. Oikeanpuoleinen käänteisalkio on taas sellainen $z \in Y$ jolle pätee $xz = e$.

Olkoon X joukko ja tarkastellaan kaikkien kuvausten $f\colon X \to X$ muodostamaa joukkoa X^X. Tämä joukko voidaan varustaa liitännäisellä laskutoimituksella $\circ$ (kuvausten yhdistäminen, kts. Esim. 1.3.2). Tehtävän tuloksista seuraa, että tämän laskutoimituksen suhteen kuvauksella $f\colon X \to X$ on vasemmanpuoleinen käänteisalkio joukossa X^X jos ja vain jos f on injektio ja vastaavasti oikeanpuoleinen käänteisalkio jos ja vain jos f on surjektio. Lisäksi, jos f on injektio, joka ei ole surjektio, yleensä sen vasemmanpuoleinen käänteisalkio ei ole yksikäsitteinen, kuten olemme osoittaneet yllä. Vastaavasti b)-kohdan tuloksista seuraa, että oikeanpuoleisen käänteisalkion ei tarvitse olla yksikäsitteinen. Voidaan osoittaa, että jos alkiolla $x \in Y$ on olemassa sekä (ainakin yksi) vasemmanpuoleinen käänteisalkio y, että (ainakin yksi) oikeanpuoleinen käänteisalkio z, niin niiden täytyy olla samat, $y = z$, joten tällöin kaikki alkion vasemman- ja oikeanpuoleiset käänteisalkiot ovat samoja ja alkiolla on yksikäsitteinen käänteisalkio. Tämä osoitetaan oleellisesti samalla tavalla kuin käänteisalkion yksikäsitteisyys (huom. liitännäisyyttä tarvitaan edelleenkin).

Soveltamalla edellä mainittua tehtävän tuloksiin joukossa X^X, nähdään, että kuvauksella $f\colon X \to X$ on käänteisalkio jos ja vain jos f on bijektio, jolloin tämä käänteisalkio on f:n käänteiskuvaus. Tämä on sopusoinnissa joukko-opin perustietojen kanssa ja pätee tunnetusti myös yleisemmin bijektiolle $f\colon X \to Y$.

2. Olkoon H kokonaislukujen muodostaman ryhmän $(\mathbb{Z}, +)$ *aliryhmä*. Osoita, että on olemassa $n \in \mathbb{Z}$ siten, että

$$H = n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$$

Onko luku $n \in \mathbb{Z}$ tällöin yksikäsitteinen?

Ratkaisu: Jos $H = \{0\}$ on triviaali aliryhmä, asia on selvä, sillä $\{0\} = n\mathbb{Z}$ jos ja vain jos valitaan $n = 0$. Tällöin n on lisäksi yksikäsitteinen.

Oletetaan, että H on epätriviaali, tällöin on olemassa $k \in H$, $k \neq 0$. Koska H on aliryhmä, se on suljettu vasta-alkioiden suhteen, joten myös $(-k) \in H$. Koska kahdesta luvuista k ja $-k$ (täsmälleen) yksi on positiivinen, voidaan olettaa, että $k > 0$. H siis sisältää ainakin yhden positiivisen kokonaisluvun eli joukko $H' = H \cap \mathbb{N}_+$ on joukon $\mathbb{N}_+$ epätyhjä osajoukko. Positiivisten kokonaislukujen joukolla $\mathbb{N}_+$ on seuraava tärkeä ominaisuus: jokaisella sen epätyhjällä osajoukolla on *pienin* alkio. Voidaan siis valita joukon $H' = H \cap \mathbb{N}_+$ pienin alkio n. Osoitetaan, että

$H = n\mathbb{Z}$. Olkoon $k \in \mathbb{Z}$. Jos $k > 0$,

$$nk = \underbrace{n + \ldots + n}_{k \text{ kpl}} \in H,$$

sillä $n \in H$ ja H on suljettu yhteenlaskun suhteen. Koska H on suljettu vastaalkioiden, $-n \in H$. Näin ollen, jos $k < 0$ samalla tavalla kuin yllä nähdään, että

$$nk = (-n)(-k) = \underbrace{(-n) + \ldots + (-n)}_{(-k) \text{ kpl}} \in H.$$

Jos $k = 0$, $nk = 0 \in H$, sillä H sisältää aliryhmänä yhteenlaskun neutraalialkion 0.

Olemme osoittaneet, että

$$n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} \subset H.$$

Osoitetaan käänteinen inkluusio $H \subset n\mathbb{Z}$. Olkoon $m \in H$. Jakamalla luku m luvulla n saadaan *jakojäännös* $r \in \{0, 1, \ldots, n-1\}$, jolloin $m = nk + r$ jollakin $k \in \mathbb{Z}$. Koska $nk \in H$ ylläosoitetun nojalla ja koska H on suljettu vähennyslaskun suhteen, saadaan

$$r = n - mk \in H.$$

Jos $r \neq 0$, saadaan ristiriita luvun n valinnan kanssa, sillä tällöin $0 < r < n$ on positiivinen kokonaisluku, joka on joukossa H, mutta pienempi kuin n. Näin ollen täytyy olla $r = 0$, joten $m = nk \in n\mathbb{Z}$. Olemme osoittaneet, että $H \subset n\mathbb{Z}$.

Koska $n\mathbb{Z} = (-n)\mathbb{Z}$, luku n ei ole yksikäsitteinen, paitsi jos $n = 0$ (jolloin $H = \{0\}$ on triviaali aliryhmä).

3. Osoita, että joukko

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

on kunta, jos se varustetaan tavallisilla reaalilukujen yhteen- ja kertolaskulla. Osoita, että tässä kunnassa polynomiyhtälöllä $x^2 - 2 = 0$ on ratkaisuja, mutta polynomiyhtälöllä $x^2 - 3 = 0$ ei ole ratkaisuja. Onko kuvaus $f\colon \mathbb{Q}[\sqrt{2}] \to \mathbb{C}$, joka on määritelty kaavalla

$$f(a + b\sqrt{2}) = a + bi,\ a, b \in \mathbb{Q},$$

kuntien välinen homomorfismi? Tässä $\mathbb{C}$ on kompleksilukujen kunta. Entä kuvaus $f\colon \mathbb{Q}[\sqrt{2}] \to \mathbb{R}$, $f(a + b\sqrt{2}) = a + b\sqrt{5}$?

Ratkaisu: Koska $\mathbb{Q}[\sqrt{2}] \subset \mathbb{R}$ ja reaalilukujen kunta $(\mathbb{R}, +, \cdot)$ on tunnetusti kunta, riittää osoittaa, että $\mathbb{Q}[\sqrt{2}]$ on kunnan $(\mathbb{R}, +, \cdot)$ alikunta.

Aloitetaan osoittamalla, että $\mathbb{Q}[\sqrt{2}]$ on suljettu reaalilukujen yhteen- ja kertolaskun suhteen eli, että systeemi $(\mathbb{Q}[\sqrt{2}], +, \cdot)$ on ylipäätän hyvinmääritelty. Olkoot $a, b, c, d \in \mathbb{Q}$ rationaalilukuja. Tällöin

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in \mathbb{Q}[\sqrt{2}],$$

$$(a + b\sqrt{2})(c + d\sqrt{2}) = ac + ad\sqrt{2} + bc\sqrt{2} + 2bd$$
$$= (ac + 2bd) + (ad + bc)\sqrt{2} \in \mathbb{Q}[\sqrt{2}],$$

koska $a + c, b + d, ac + 2bd, ad + bc \in \mathbb{Q}$.

Seuraavaksi osoitamme, että $(\mathbb{Q}[\sqrt{2}], +)$ on ryhmän $(\mathbb{R}, +)$ aliryhmä. Koska osoitimme jo, että $\mathbb{Q}[\sqrt{2}]$ on suljettu yhteenlaskun suhteen, riittää vielä näyttää, että $\mathbb{Q}[\sqrt{2}]$ sisältää yhteenlaskun neutraalialkion 0 ja on suljettu vasta-alkioiden suhteen. Edellinen väite seuraa siitä, että $0 = 0 + 0\sqrt{2}$, missä $0, 0 \in \mathbb{Q}$. Jälkimmäinen väite taas seuraa sitä, että

$$-(a + b\sqrt{2}) = (-a) + (-b)\sqrt{2}.$$

Joukko $\mathbb{Q}[\sqrt{2}]$ sisältää myös reaalilukujen kertolaskun neutraalialkion 1, sillä $1 = 1 + 0 \cdot \sqrt{2}$. Olemme osoittaneet, että $(\mathbb{Q}[\sqrt{2}], +, \cdot)$ on renkaan $(\mathbb{R}, +, \cdot)$ alirengas. Täytyy vielä tarkistaa, että $\mathbb{Q}[\sqrt{2}]$ on suljettu käänteialkioiden suhteen. Olkoon $a, b \in \mathbb{Q}$ siten, että $a + b\sqrt{2} \neq 0$. Tällöin laventamalla tekijällä $(a - b\sqrt{2})$ saadaan

$$(a+b\sqrt{2})^{-1} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}].$$

Huomaa, että oletuksesta $a + b\sqrt{2} \neq 0$ seuraa, että myös $a - b\sqrt{2} \neq 0$, joten sillä voi jakaa. Nimittäin, jos $a - b\sqrt{2} = 0$, niin $a = b\sqrt{2}$. Jos $b \neq 0$, tästä saadaan, että $\sqrt{2} = a/b \in \mathbb{Q}$, mikä ei tunnetusti pidä paikkaansa. Näin ollen $b = 0$, jolloin myös $a = b\sqrt{2} = 0$, mistä seuraa, että $a + b\sqrt{2} = 0$, vastoin oletusta.

Olemme osoittaneet, että $\mathbb{Q}[\sqrt{2}]$ on kunnan $(\mathbb{R}, +, \cdot)$ alikunta, erityisesti $(\mathbb{Q}[\sqrt{2}], +, \cdot)$ on kunta.

Koska $\pm\sqrt{2} = 0 + (\pm 1) \cdot \sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, polynomiyhtälön $x^2 - 2 = 0$ ainoat reaaliset ratkaisut $\pm\sqrt{2}$ ovat alikunnan $\mathbb{Q}[\sqrt{2}]$ alkioita, erityisesti tällä yhtälöllä on ratkaisuja kunnassa $\mathbb{Q}[\sqrt{2}]$.
Tarkistetaan, onko polynomiyhtälöllä $x^2 - 3 = 0$ ratkaisuja kunnassa $\mathbb{Q}[\sqrt{2}]$. Koska tämä on kunnan $\mathbb{R}$ alikunta ja kunnassa $\mathbb{R}$ tämän yhtälön ainoat ratkaisut ovat reaaliluvut $\pm\sqrt{3}$, riittää tutkia pätekö väite $\pm\sqrt{3} \in \mathbb{Q}[\sqrt{2}]$. Jos tämä on totta, on olemassa $a, b \in \mathbb{Q}$ siten, että

$$a + b\sqrt{2} = \pm\sqrt{3}.$$

Ottamalla tämän yhtälön kummastakin puolesta neliöjuuren, saadaan

$$(a^2 + 2b^2) + 2ab\sqrt{2} = 3.$$

Jos $ab \neq 0$, tästä seuraa, että

$$\sqrt{2} = \frac{3 - a^2 - 2b^2}{2ab} \in \mathbb{Q}.$$

Tämä on ristiriita, sillä kakkosen neliöjuuri ei tunnetusti ole rationaaliluku. Näin ollen täytyy olla $ab = 0$ eli $a = 0$ tai $b = 0$. Jos $a = 0$, saadaan $2b^2 = 3$, jolloin saadaan $b = \pm\sqrt{3/2} \in \mathbb{Q}$. Samalla tavalla kuin osoitetaan, että $\sqrt{2}$ ei ole rationaaliluku voidaan näyttää, että myöskin $\sqrt{3/2}$ ei ole rationaaliluku. Näin ollen tapaus $a = 0$ johtaa ristiriitaan. Tapauksessa $b = 0$ saadaan samanlainen ristiriita, sillä tällöin täytyy olla $a = \pm\sqrt{3} \in \mathbb{Q}$. Näin ollen polynomiyhtälöllä $x^2 - 3 = 0$ ei ole ratkaisuja kunnassa $\mathbb{Q}[\sqrt{2}]$.

Kuvaus $f\colon \mathbb{Q}[\sqrt{2}] \to \mathbb{C},\ f(a + b\sqrt{2}) = a + bi,\ a, b \in \mathbb{Q}$, ei ole kuntien välinen homomorfismi, sillä se ei säilyttää kertolaskua. Esimerkiksi

$$f((\sqrt{2}^2) = f(2) = 2 \neq -1 = i^2 = f(\sqrt{2})^2.$$

Kuvaus $f\colon \mathbb{Q}[\sqrt{2}] \to \mathbb{R}$, $f(a+b\sqrt{2}) = a+b\sqrt{5}$ ei ole kuntien välinen homomorfismi samantapaisesta syistä,

$$f((\sqrt{2}^2) = f(2) = 2 \neq 5 = (\sqrt{5})^2 = f(\sqrt{2})^2.$$

4. Olkoon $\cdot$ liitännäinen laskutoimitus joukossa X. Olkoot $x, y \in X$ ja olkoot $n, m \in \mathbb{N}_+$ positiivisia kokonaislukuja. Osoita (esimerkiksi induktiolla), että

$$x^n x^m = x^{n+m},$$

$$x^{nm} = (x^n)^m.$$

Ratkaisu: Intuitiivisesti:

$$x^n x^m = \underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ kpl}} \underbrace{x \cdot x \cdot \ldots \cdot x}_{m \text{ kpl}} = x^{n+m},$$

$$(x^n)^m = \underbrace{\underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ kpl}} \underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ kpl}} \ldots \underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ kpl}}}_{m \text{ kpl}} = x^{nm}.$$

Osoitetaan vielä kumpikin väite formaalisti induktiolla luvun m suhteen. Aloitetaan ensimmäisestä väitteestä. Kun $m = 1$

$$x^n x^1 = x^n x = x^{n+1} = x^{n+m},$$

potenssin määritelmän mukaan. Oletetaan, että $x^n x^m = x^{n+m}$. Tällöin

$$x^n x^{m+1} \overset{(i)}{=} x^n (x^m x) \overset{(ii)}{=} (x^n x^m) x \overset{(iii)}{=} x^{n+m} x \overset{(iv)}{=} x^{(n+m)+1} \overset{(v)}{=} x^{n+(m+1)},$$

Välivaiheiden selitykset:
(i) Potenssin (induktiivinen) määritelmä: $x^{m+1} = x^m x$.
(ii) Laskutoimituksen liitännäisyys.
(iii) Induktio-oletus.
(iv) Potenssin määritelmä taas.

(v) Tavallinen kokonaislukujen yhteenlaskun liitännäisyys.

Seuraavaksi osoitetaan, että $x^{nm} = (x^n)^m$ induktiolla m:n suhteen. Kun $m = 1$ saadaan

$$x^{n1} = x^n = (x^n)^1$$

potenssin määritelmän mukaan. Oletetaan, että $x^{nm} = (x^n)^m$. Tällöin käyttämällä jo edellä osoitettua saadaan

$$x^{n(m+1)} = x^{nm+n} = x^{nm}x^n.$$

Induktio-oletuksen avulla tästä seuraa (potenssin rekursiivisen määritelmän nojalla)

$$x^{n(m+1)} = x^{nm}x^n = (x^n)^m x^n = (x^n)^{m+1}.$$

Väite on todistettu.

5. Kääntyvät (2×2)-kokoiset reaalikertoimiset matriisit muodostavat ryhmän $GL(2;\mathbb{R})$ matriisien kertolaskun suhteen (tämä oletetaan tunnetuksi). Määritellään kuvaus $f\colon \mathbb{R} \to GL(2;\mathbb{R})$ kaavalla

$$f(t) = \begin{bmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{bmatrix}.$$

Harj. 1.6 nojalla f on hyvin määritelty (eli $f(t)$ on todellakin kääntyvä matriisi kaikilla $t \in \mathbb{R}$). Osoita, että $f\colon (\mathbb{R},+) \to (GL(2;\mathbb{R}),\cdot)$ on ryhmien välinen homomorfismi. Mikä on tämän homomorfismin ydin? Onko f injektiivinen? Onko f surjektiivinen?

Ratkaisu: Olkoot $t, t' \in \mathbb{R}$. Tällöin käyttämällä sinin ja kosinin yhteenlaskukaavoja saadaan

$$f(t)f(t') = \begin{bmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{bmatrix} \cdot \begin{bmatrix} \cos t' & -\sin t' \\ \sin t' & \cos t' \end{bmatrix} = \begin{bmatrix} \cos t\cos t' - \sin t \sin t' & -\cos t \sin t' - \sin t \cos t' \\ \sin t \cos t' + \cos t \sin t' & -\sin t \sin t' + \cos t \cos t' \end{bmatrix}$$

$$= \begin{bmatrix} \cos(t+t') & -\sin(t+t') \\ \sin(t+t') & \cos(t+t') \end{bmatrix} = f(t+t').$$

Näin ollen f on homomorfismi ryhmien $(\mathbb{R},+)$ ja $(Gl(2;\mathbb{R}),\cdot)$ välillä. Homomorfismin ydin koostuu niistä $t \in \mathbb{R}$ joille

$$\begin{bmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

eli niistä $t \in \mathbb{R}$ joille $\cos t = 1$ ja $\sin t = 1$. Toisin sanoen $\operatorname{Ker} f = 2\pi\mathbb{Z}$. Erityisesti homomorfismin ydin on epätriviaali, joten f ei ole injektio.

f ei myöskään ole surjektio, sillä kaikki (2×2)-kokoiset kääntyvät matriisit eivät ole välttämättä muotoa

$$\begin{bmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{bmatrix}$$

jollakin $t \in \mathbb{R}$. Esimerkiksi matriisi

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

ei ole sellainen. Tämä matriisi on kääntyvä esimerkiksi koska sen determinantti on $(-1) \neq 0$. Itse asiassa se on itseensä käänteismatriisi.

6. Olkoon

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

Osoita, että $H = \{I_2, -I_2, A, -A\}$ on matriisiryhmän $GL(2;\mathbb{R})$ aliryhmä (matriisien kertolaskun suhteen, kts. edellinen tehtävä). Tässä I_2 on (2×2)-kokoinen yksikkömatriisi. Onko ryhmä H isomorfinen ryhmän $(\mathbb{Z}_4, +)$ kanssa? Perustele.

Ratkaisu: Joukko H on suljettu matriisien kertolaskun suhteen. Nimittäin helposti nähdään, että $A^2 = I_2$, joten

$$(\pm I_2)(\pm I_2) = \pm I_2,$$
$$(\pm I_2)(\pm A) = \pm A = (\pm A)(\pm I_2),$$
$$(\pm A)(\pm A) = \pm I_2.$$

Lisäksi H sisältää kertolaskun neutraalialkion I_2. Lisäksi H on suljettu käänteisalkioiden suhteen, sillä edellisistä laskuista myös seuraa, että $(\pm A)^{-1} = \pm A$ ja tietysti $(\pm I_2)^{-1} = \pm I_2$. Näin ollen H on matriisiryhmän $GL(2;\mathbb{R})$ aliryhmä.

Ryhmät $(H, \cdot)$ ja $(\mathbb{Z}_4, +)$ *eivät* ole isomorfisia keskenään. Nimittäin edellisestä seuraa, että ryhmässä H jokaisen alkion x neliö on ryhmän neutraalialkio, $x^2 = e$. Ryhmässä $(\mathbb{Z}_4, +)$ taas on olemassa alkio, jolle tämä ei päde, esimerkiksi alkio 1_4, jolle $21_4 = 2_4 \neq 0_4$ (muista, että additiivisella merkinnällä potenssia x^2 vastaa monikerta $2x$). Toinen tällainen ryhmän $\mathbb{Z}_4$ alkio on 3_4. Näin ollen tarkasteltavien ryhmien alkioilla on "erilaset algebralliset ominaisuudet".

Osoitetaan, että ryhmät eivät ole isomorifisia formaalisti. Jos olisi olemassa isomorfismi $f\colon H \to \mathbb{Z}_4$, niin olisi olemassa (koska f surjektio) $x \in H$ jolle $f(h) = 1_4$. Tällöin olisi

$$2_4 = 1_4 + 1_4 = f(h) + f(h) = f(h \cdot h) = f(h^2) = f(I_2) = 0_4,$$

koska homomorfismi kuvaa neutraalialkio neutraalialkioksi. Koska $2_4 \neq 0_4$ saadaan ristiriita.

Ryhmän $(H, \cdot)$ *kertotaulu*:

$\cdot$	I_2	$-I_2$	A	$-A$
I_2	I_2	$-I_2$	A	$-A$
$-I_2$	$-I_2$	I_2	$-A$	A
A	A	$-A$	I_2	$-I_2$
$-A$	$-A$	A	$-I_2$	I_2

Ryhmän $(\mathbb{Z}_4, +)$ *kertotaulu*:

$+$	0_4	1_4	2_4	3_4
0_4	0_4	1_4	2_4	3_4
1_4	1_4	2_4	3_4	0_4
2_4	2_4	3_4	0_4	1_4
3_4	3_4	0_4	1_4	2_4

Huomautus: Voidaan osoittaa, että isomorfiaa vaille on olemassa vain kaksi erilaista neljän alkion ryhmää. Toinen on syklinen ryhmä $(\mathbb{Z}_4, +)$ ja toinen on niin sanottu *Kleinin neliryhmä* $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$, joka on isomorfinen tehtävän ryhmän H kanssa.

7. Esimerkissä 1.58 tarkasteltiin erästä neljän alkion ryhmää $H' = \{\pm 1, \pm i\}$ (varustettuna kompleksilukujen kertolaskuna). Onko ryhmä H' isomorfinen ryhmän $(\mathbb{Z}_4, +)$ kanssa? Perustele.

Ratkaisu: Ryhmät $(H', \cdot)$ ja $(\mathbb{Z}_4, +)$ ovat isomorfisia. Sen huomaa parhaiten palauttamalla mieleen, että $(\mathbb{Z}_4, +)$ on niin sanottu *syklinen* ryhmä, eli yhden alkion virittämä ryhmä. Tällaiseksi alkioksi voidaan ottaa esimerkiksi alkio 1_4 (toinen valinta olisi $-1_4 = 3_4$). Jokainen ryhmän $(\mathbb{Z}_4, +)$ alkio voidaan esittää tämän virittäjän monikertana $n1_4$ jollakin $n \in \mathbb{Z}$, sitä väite "alkio 1_4 virittää ryhmän " tarkoittakin.

Kaikki **samankokoiset** sykliset ryhmät $(G, \cdot)$, $(G', \cdot)$ ovat isomorfisia keskenään, tämä osoitetaan kuvaamalla isomorfismissa f toisen ryhmän virittäjä x toisen ryhmän virittäjäksi y ja jatkamalla tämä valinta homomorfismiksi ainoalla mahdollisella tavalla, eli määrittelemällä $f(x^n) = y^n$ kaikilla $n \in \mathbb{N}$. Tämän jälkeen pitäisi tietysti vielä osoittaa, että tämä kuvaus on hyvinmääritelty ja todellakin antaa isomorfismin, yksityiskohtien pitäisi olla tuttuja algebran peruskurssilta.

Näin ollen $(H', \cdot)$ ja $(\mathbb{Z}_4, +)$ ovat isomorfisia jos ja vain jos H' on myös syklinen neljän alkion ryhmä. Tämä on taas totta jos ja vain jos siitä löytyy alkio, jonka *kertaluku* on tasan neljä. Ryhmän alkion $x \in G$ kertaluvuksi sanotaan pienentä positiivista kokonaislukua jolle pätee $x^n = e$, jos sellainen on olemassa. Huomataan, että $i \in H'$ on juuri sellainen alkio, sillä $i^2 = -1 \neq 1$, $i^3 = -i$, $i^4 = 1$. Samalla nähdään, että ryhmän H kaikki alkiot tosiaankin voidaan esittää alkion i potensseina, joten i todellakin on tämän ryhmän virittäjä.

Edellä on esitetty semi-heuristisia ajatuksia, jotka puhuttelevat sellaiselle lukijalle, jolle syklisen ryhmän ja kertaluvun käsitteet (sekä niiden yhteys) ovat tuttuja algebran peruskurssilta. Osoitetaan väite vielä täsmällisesti ja formaalisti. Määritellään kuvaus $f\colon (\mathbb{Z}_4, +) \to H'$ kaavalla

$$f(n_4) = i^n$$

kaikilla $n \in \mathbb{Z}$. Osoitetaan ensin, että tämä kuvaus on hyvinmääritelty. Olkoot $n, m \in \mathbb{Z}$ sellaisia, että $n_4 = m_4$. Tällöin $n - m = 4k$ jollakin $k \in \mathbb{Z}$ eli toisin sanoen

$n = m+4k$. Käyttämällä hyväksi potenssien laskusääntöjä (teht. 4), saadaan tällöin

$$f(n_4) = i^n = i^{m+4k} = i^m(i^4)^k = i^m 1^k = i^m = f(m_4).$$

Toisin sanoen kuvausken f määritelmä ei riipu edustajan valinnasta. Samojen sääntöjen avulla helposti nähdään, että f on homomorfismi:

$$f(n_4 + m_4) = f((n+m)_4) = i^{n+m} = i^n i^m = f(n_4)f(n_m).$$

Koska jokainen ryhmän H' alkio on imaginääriyksikön potenssi (kts. yllä), kuvaus f on surjektio. Koska kummatkin joukot $\mathbb{Z}_4$ ja H' ovat äärellisiä ja samankokoisia, mikä tahansa surjektio niiden välillä on myös injektio, joten f on myös bijektio. Injektivisyyttä voidaan tutkia myös suoraan - joukot ovat sen verran pieniä, että voidaan katsoa mitä tapahtuu alkioiden tasolla:

$$f(0_4) = 1, f(1_4) = i, f(2_4) = -1, f(3_4) = -i.$$

Tästä nähdään suoraan, että f on bijektio.
Olemme osoittaneet, että f on ryhmien välinen isomorfismi.

Teoreettisempi ja yleisempi tapa olisi käyttää ryhmien isomorfialausetta. Ensin määritellään kuvaus $g\colon \mathbb{Z} \to H'$ kaavalla $g(n) = i^n$. Sitten todetaan, että g on surjektio ja $\operatorname{Ker} g = 4\mathbb{Z}$ (tämä vaati tietysti vähän laskuja ja perusteluja). Isomorfialauseen 1.99 nojalla tällöin $Z_4 = \mathbb{Z}/4\mathbb{Z}$ ja H' ovat isomorfisia. Samalla tavalla voidaan yleisesti osoittaa, että mielivaltainen m:n alkion syklinen ryhmä G on isomorfinen ryhmän $(\mathbb{Z}_m, +)$ kanssa (mistä seuraa, että kaikki tällaiset ryhmät ovat isomorfisia keskenään).