Luku 1

Johdanto: Algebralliset Struktuurit

1.1 Algebralliset operaatiot

Nykypäivän terminologian mukaan algebra on matematiikan osa-alue, joka tutkii pääsääntöisesti erilaisilla algebrallisilla operaatioilla varustettuja joukkoja ja sellaisia niiden välisiä kuvauksia, jotka säilyttävät nämä operaatiot. Tällä kurssilla törmäämme jatkuvasti kahdentyyppiseen algebralliseen operaatioon - joukon "sisäisiin" algebrallisiin operaatioihin ja "ulkoisiin" toimintatyyppisiin operaatioihin. Tutustumme molempiin tarkemmin tässä ja seuraavassa luvussa.

Olkoon X joukko. *Algebrallinen operaatio* joukossa X on mikä tahansa kuvaus $f\colon X \times X \to X$. Toinen nimitys, jota käytetään algebrallisen operaation synonyyminä, on *laskutoimitus* joukossa X. Laskutoimitus siis liittää kahteen X:n alkioon a, b (tässä järjestyksessä) tämän laskutoimituksen *tuloksen* $f(a, b)$, joka on myös X:n alkio. Vaikka laskutoimitus onkin kuvaus, tällaista merkintää käytetään harvoin. Sen sijaan algebrassa on tapana käyttää laskutoimituksen symboleina (enemmän tai vähemmän) tuttuja merkkejä $+, \cdot, \times, \circ, \oplus, \otimes$. Tällöin laskutoimituksen tulosta **ei** merkitä $+(a, b)$, $\cdot(a, b)$ jne., vaan $a + b$, $a \cdot b$ ja niin poispäin. Kun laskutoimituksen symbolina on $+$ eli *plusmerkki*, puhutaan alkioiden a ja b *summasta* $a + b$, kun se on $\cdot$ - puhutaan alkioiden a ja b *tulosta* $a \cdot b$ jne. Jälkimäisessä tapauksessa on varsin tavallista, että jätetään laskutoimitus jopa kokonaan merkitsemättä, jolloin alkioiden a ja b tuloa merkitäänkin vain ab. Kutsumme tällaista merkintätapa *multiplikatiiviseksi*. Kun symbolina on plusmerkki $+$, puhutaan *additiivisesta* laskutoimituksen merkintätavasta.

Näiden symbolien ja merkintöjen käyttötavoista on olemassa kutakuinkin vakiintuneita käytäntöjä ja perinteitä, jotka selviävät kokemuksen ja kontekstin myötä. Näitä perinteitä on syytä noudattaa, mutta samalla on pidettävää mielessä, että kyse on vain merkintätavoista ja matemaattinen sisältö ei riipu siitä, mitä merkintöjä käytetään. Esimerkkinä tällaisesta traditiosta mainitaan tähän väliin, että additiivista merkintätapa $a + b$ käytetään lähes poikkeuksetta kun laskutoimitus on *vaihdannainen* eli $a + b = b + a$ kaikille lähtöjoukon alkioille a, b.

Esimerkki 1.1. *1. Vanhimpia ihmiselle tunnettuja laskutoimituksia on melko varmasti positiivisten kokonaislukujen yhteenlasku. Tämä on siis joukossa $\mathbb{N}_+ = \{1, 2, 3, \ldots\}$ määritelty laskutoimitus $+$. Ihmiset tiesivät että lukumääriä voi laskea yhteen ennen kirjallisuuden keksimistäkin. Itse asiassa nykytietojen mukaan monet eläimetkin pystyvät laskemaan pieniä lukumääriä. Sen sijaan nollan keksimiseen meni pitkään - sen käyttö vakiintui länsimaissa vasta noin 500 vuotta sitten.*

2. Vähennyslasku "$-$" on myös laskutoimitus kokonaislukujen joukossa $\mathbb{Z}$. Sen sijaan luonnollisten lukujen joukossa tätä laskutoimitusta ei voi määritellä, sillä on olemassa luonnollisten lukujen pareja (a, b), joille $a - b$ ei ole enää luonnollinen luku, esim. $1 - 2 = -1 \notin \mathbb{N}$. Jotta vähennyslasku olisi mahdollista määritellä yleisesti, tarvitaan myös negatiivisia lukuja. Nämä ovat suurinpiirtein yhtä vanha keksintö kuin nolla.

On selvää, että tällä tavalla määritelty algebrallisen operaation käsite on liian laaja ollakseen mielenkiintoinen - sellainen operaatio on määritelmän mukaan mikä tahansa kuvaus $X \times X \to X$ eikä tällaisesta yleisesti voi sanoa mitään sen enempää. Algebrassa rajoitutaankin tutkimaan lähinnä algebrallisia operaatioita, jotka toteuttavat tiettyjä lisäominaisuuksia, yleensä sellaisia, jotka voidaan muotoilla pelkästään operaation ja joukon alkioiden avulla. Tällaisia ominaisuuksia on luonnollista kutsua *algebrallisiksi* ominaisuuksiksi. Esimerkiksi ominaisuus "$a+b = b+a$ kaikilla a, b" on algebrallinen. Sen sijaan ominaisuus "$\mathbb{R}$:n yhteenlasku on jatkuva operaatio" ei ole algebrallinen, sillä sen muotoilussa esiintyy topologinen jatkuvuuden käsite.
Annetaan muutama esimerkki tärkeistä algebrallisista ominaisuuksista.
- **Assosiatiivisuus**. Olkoon $\cdot$ joukossa X määritelty laskutoimitus. Sitä sanotaan *assosiatiiviseksi* tai *liitännäiseksi* jos

$$(ab)c = a(bc) \text{ kaikilla } a, b, c \in X.$$

Huomaa, että käytämme tässä multiplikatiivista merkintätapaa, jossa emme käytä minkäänlaista erikoismerkkiä itse operaatiolle.
Liitännäisessä laskutoimituksessa mielivaltaisen pitkän tulon $a_1a_2 \dots a_n$ lopputulos ei riipu siitä, miten sulut laitetaan alkioiden ympärille. Ei-liitännäisessä laskutoimituksessa tämä ei pidä paikkansa ja kolmen tai useamman alkion tulo voi riippua välivaiheiden suoritusjärjestyksestä.

Esimerkkejä 1.2. *1. Kokonaislukujen vähennyslasku ei ole liitännäinen, sillä esimerkiksi*

$$7 - (5 - 2) = 4 \neq 0 = (7 - 5) - 2.$$

2. Tärkeimpiä esimerkkejä assosiatiivisista laskutoimituksista on kuvausten yhdistäminen. Olkoon X mielivaltainen joukko ja olkoon $Y = X^X$ kaikkien kuvausten $f\colon X \to X$ muodostama joukko. Kuvausten yhdistäminen $(f, g) \mapsto g \circ f$ on joukossa Y määritelty assosiatiivinen laskutoimitus, sillä

$$(f \circ g) \circ h = f \circ (g \circ h)$$

aina kun nämä yhdistetyt kuvaukset ovat määriteltyjä.

-**Kommutatiivisuus**. Joukon X laskutoimitus on *kommutatiivinen* tai *vaihdannainen* jos $ab = ba$ kaikilla $a, b \in X$. Koulusta tutut luvuille määritellyt laskutoimitukset eli esimerkiksi reaalilukujen yhteenlasku ja kertolasku ovat kommutatiivisia. Korkeassa matematiikassa sen sijaan vaihdannaiset operaatiot ovat paljon harvinaisempia kuin koulumatematiikassa.
Kuvausten yhdistäminen joukossa X^X ei ole vaihdannainen, jos X:ssä on vähintään kaksi alkiota. Esimerkiksi jos $X = \mathbb{R}$, $f(x) = x + 1$, $g(x) = x^2$, niin

$$f \circ g = (x + 1)^2 \neq x^2 + 1 = g \circ f.$$

Toinen kuuluisa esimerkki, joka havainnollista sen, miksi toimintojen peräkkäinen yhdistäminen ei yleensä ole vaihdannainen, on seuraava. Olkoot A operaatio ”laita alushousut jalkaan” ja B operaatio ”laita housut jalkaan”. Tällöin $B \circ A$ edustaa tapaa , jolla tavalliset ihmiset yleensä pukeutuvat ja $A \circ B$ on tapa, jolla Teräsmies pukeutuu.
Kuten yllä on jo mainittu, algebrassa on tapana käyttää symbolia + lähes poikkeuksetta ainoastaan vaihdannaisten laskutoimitusten tapauksessa. Tällöin vaihdannaisuusehto näyttää tietenkin seuraavanlaiselta,

$$a + b = b + a$$

-**Neutraalialkio**. Olkoon $\cdot$ joukon X laskutoimitus. Alkiota $e \in X$ sanotaan laskutoimituksen *neutraalialkioksi* jos

$$ex = x = xe$$

kaikilla $x \in X$. Esimerkiksi positiivisten kokonaislukujen yhteenlaskulla ei ole neutraalialkiota - sehän on nimenomaan nollan rooli. Kun joukkoon lisätään nolla, eli tarkastellaan yhteenlaskua luonnollisten lukujen $\mathbb{N} = \{0, 1, 2, \ldots\}$ joukossa, tällä laskutoimituksella on neutraalialkio.
Kuvausten $X \to X$ yhdistämisellä on neutraalialkio - se on *identtinen* kuvaus $\mathrm{id}\colon X \to X$, joka on määritelty kaavalla $\mathrm{id}(x) = x$ kaikilla $x \in X$.
Neutraalialkio on aina yksikäsitteinen, jos olemassa, eli laskutoimituksella voi olla korkeintaan yksi neutraalialkio. Tämä nähdään seuraavasti. Olkoot $e, e' \in X$ molemmat neutraalialkioita. Tällöin neutraalialkion määritelmästä seuraa suoraan, että

$$e = e'e = e'.$$

Neutraalialkiota merkitään usein symbolilla 1, kun laskutoimitusta merkitään *multiplikatiivisesti*, eli tulona $\cdot$. Sen sijaan, jos laskutoimituksen merkkinä käytetään plusmerkkiä $+$, neutraalialkiota merkitään tavallisesti symbolilla 0 (ja kutsutaan, yllätys, yllätys, *nollaksi* tai nolla-alkioksi).
-**Käänteisalkiot**. Olkoon $\cdot$ joukossa X määritelty laskutoimitus, jolla on neutraalialkio e, ja olkoon $x \in X$. Alkiota $y \in X$ sanotaan x:n *vasemmanpuoleiseksi käänteisalkioksi* jos $yx = e$. Vastaavasti jos $xy = e$, y on x:n *oikeanpuoleinen käänteisalkio*. Jos y on sekä vasemman- että oikeanpuoleinen x:n käänteisalkio, sitä sanotaan yksinkertaisesti x:n *käänteisalkioksi* ja merkitään symbolilla x^{-1}. Jos laskutoimituksen symbolina käytetään $+$-merkkiä, puhutaan x:n *vasta-alkiosta*, jota merkitään silloin symbolilla $-x$.

Esimerkkinä tarkastellaan taas luonnollisten lukujen yhteenlaskua. Tällä on neutraalialkio 0, mutta se onkin ainoa alkio, jolla on vasta-alkio - tässä tapauksessa nolla on itsensä vasta-alkio. Jos halutaan kaikille alkioille vasta-alkiot, joukkoon on lisättävää negatiiviset kokonaisluvut. $\mathbb{Z}$ onkin yhteenlaskun suhteen sellainen joukko, jolla on neutraalialkio ja jokaisella alkiolla on vasta-alkio.
Seuraavana esimerkkinä tarkastellaan taas kuvausten joukkoja X^X varustettuna kuvausten yhdistämisellä. Voidaan osoittaa (harjoitustehtävä), että kuvauksella $f\colon X \to Y$ on vasemmanpuoleinen käänteisalkio $g\colon X \to X$ jos ja vain jos f on injektio ja vastaavasti kuvauksella $f\colon X \to Y$ on olemassa oikeanpuoleinen käänteisalkio jos ja vain jos f on surjektio. Näin ollen f:llä on käänteisalkio jos ja vain jos f on bijektio.
Esimerkiksi olkoon $f\colon \mathbb{Z} \to \mathbb{Z}$ määritelty alkiolla $f(n) = 2n$. Tällöin f on injektio, joten sillä on vasemmanpuoleinen käänteisalkio. Ei ole vaikeata antaa esimerkkiä tällaisesta alkiosta. Olkoon esimerkiksi $g\colon \mathbb{Z} \to \mathbb{Z}$ määritelty kaavalla $g(n) = n/2$ jos n on parillinen ja $g(n) = 0$ muuten. Tällöin $g \circ f = \mathrm{id}$. Jos taas määritellään $g'\colon \mathbb{Z} \to \mathbb{Z}$ kaavalla $g'(n) = n/2$ kun n on parillinen

ja $g'(n) = 1$ muuten, myös g' on f:n vasemmanpuolinen käänteisalkio. Itse asiassa ei ole vaikeaa nähdä, että f:llä on jopa äärettömän monta erilaista vasemmanpuoleista käänteisalkiota. Näin ollen vasemmanpuoleinen käänteisalkio ei ole välttämättä yksikäsitteinen. Sama pätee oikeanpuoleiselle käänteisalkiolle. Sen sijaan käänteisalkio on yksikäsitteinen, kunhan laskutoimitus on liitännäinen. Pätee jopa yleisempi väite - olkoon y x:n vasemmanpuoleinen käänteisalkio ja z x:n oikeanpuoleinen käänteisalkio ja oletetaan, että laskutoimitus on liitännäinen. Tällöin

$$y = ye = y(xz) = (yx)z = ez = z.$$

-**Ryhmät**. Olkoon $\cdot$ joukossa G määritelty laskutoimitus. Paria $(G, \cdot)$ sanotaan *ryhmäksi* jos $\cdot$ on liitännäinen, sillä on neutraalialkio ja jokaisella $g \in G$ on käänteisalkio.
Vaihdannaista ryhmää sanotaan myös *Abelin ryhmäksi*.
Esimerkiksi kokonaislukujen joukko varustettuna yhteenlaskulla on Abelin ryhmä. Samoin rationaaliluvut tai reaaliluvut muodostavat vaihdannaisen ryhmän yhteenlaskun suhteen. Kertolasku reaalilukujen joukossa sen sijaan ei ole ryhmälaskutoimitus, sillä nollalla ei ole käänteisalkiota. Jos rajoitutaan nollasta eroaviin lukuihin saadaan ryhmä $(\mathbb{R} \setminus \{0\}, \cdot)$.

Esimerkki 1.3. *Olkoon X mielivaltainen joukko. Jos X:ssä on vähintään kaksi alkiota, on olemassa kuvauksia $X \to X$ jotka eivät ole bijektioita. Tällöin pari $(X^X, \circ)$ ei siis ole ryhmä. Saadaksemme ryhmän meidän on rajoitettavaa tarkastelu pelkästään bijektioihin (sillä vain bijektiolla voi olla käänteisalkio $\circ$:n suhteen). Määritellään siis*

$$\mathrm{Perm}(X) = \{f \colon X \to X \text{ on bijektio}\},$$

niin sanottu X:n permutaatiojoukko. *Jos $g, f \in \mathrm{Perm}(X)$, myös yhdistetty kuvaus $g \circ f \colon X \to X$ on bijektio, joten $\circ$ on hyvin määritelty laskutoimitus joukossa* $\mathrm{Perm}(X)$. *Se on liitännäinen, sillä kuvausten yhdistäminen on liitännäinen operaatio. Identtinen kuvaus* $\mathrm{id} \colon X \to X$ *on bijektio ja toimii laskutoimituksen neutraalialkiona. Viimeiseksi huomataan, että jokaisella bijektiolla $f \colon X \to X$ on käänteiskuvaus $f^{-1} \colon X \to X$, joka on myös bijektio. Näin ollen* $(\mathrm{Perm}(X), \circ)$ *on ryhmä. Helposti nähdään, että jos X:ssä on vähintään* 3 *alkiota, tämä ryhmä ei ole vaihdannainen.*

Usein törmätään tilanteeseen, jossa samassa joukossa on määritelty samanaikaisesti kaksi tai enemmänkin algebrallista operaatiota. Esimerkiksi reaalilukuja voidaan sekä laskea yhteen että kertoa keskenään. Tämä on esimerkki *renkaasta*.

- **Renkaat**. Olkoon R joukko, jossa on määritelty kaksi laskutoimitusta: $+$ ja $\cdot$. Kolmikkoa $(R, +, \cdot)$ sanotaan *renkaaksi*, jos
a) $(R, +)$ on vaihdannainen ryhmä,
b) $\cdot$ on liitännäinen, ja
c) seuraavat, niin sanotut *osittelulait*

$$(a + b)c = ac + bc,$$
$$a(b + c) = ab + ac,$$

pätevät kaikilla $a, b, c \in R$.
Operaatiota $+$ sanotaan renkaan *yhteenlaskuksi*, operaatiota $\cdot$ - renkaan *tuloksi* tai *kertolaskuksi*. Yhteenlaskun neutraalialkiota merkitään 0 ja sanotaan renkaan *nolla-alkioksi*. Jos renkaan tulolla on neutraalialkio, sitä merkitään symbolilla 1. Tässä tapauksessa rengasta sanotaan *ykköselliseksi* renkaaksi. Rengas on *vaihdannainen*, jos sen kertolasku on vaihdannainen operaatio. Vaihdannaisessa renkaassa riittää olettaa ,että pätee yksi osittelulaista, sillä toinen seuraa siitä silloin.

Renkaassa voidaan määritellä vähennyslasku $-$ kaavalla $a - b = a + (-b)$ (missä $-b$ on siis alkion b vasta-alkio Abelin ryhmässä $(R, +)$. Tälle pätevät seuraavat tutut säännöt, missä $a, b, c \in R$ mielivaltaiset.

$$a(b - c) = ab - ac,$$
$$(a - b)c = ac - bc,$$
$$(-a)b = -(ab) = a(-b).$$
$$(-a)(-b) = ab.$$

Lisäksi, jos rengas on ykkösellinen, $(-1)a = -a$ kaikilla $a \in R$. Todistukset jätetään harjoitustehtäväksi.

Esimerkkejä 1.4. *1. Kuten yllä on jo mainittu, kokonaisluvut, rationaaliluvut tai vastaavasti reaaliluvut, muodostavat renkaan tavallisen yhteenlaskun ja kertolaskun suhteen. Nämä renkaat ovat ykkösellisiä ja vaihdannaisia.*

2. Olkoon R parillisten kokonaislukujen joukko. Tämä joukko on suljettu tavallisen yhteen- ja kertolaskun suhteen, joten se on rengas. Tämä rengas on vaihdannainen mutta ei ykkösellinen.

3. *Olkoon $n \in \mathbb{N}$ ja olkoon R kaikkien $(n \times n)$-matriisien joukko. Koska samankokoiset neliömatriisit voidaan laskea yhteen ja kertoa keskenään, R:ssä on määritelty laskutoimitukset $+$ ja $\cdot$. Kolmikko $(R, +, \cdot)$ on ykkösellinen rengas. Tämä todistetaan kurssilla "Lineaarialgebra ja matriisilaskenta", ja kerrataan tällä kurssilla kohta uudestaan.*

Olkoon $(R, +, \cdot)$ ykkösellinen rengas. Määritelmämme mukaan tällöin $(R, +)$ on ryhmä, joten jokaisella $x \in R$ on olemassa vasta-alkio $-x$. Voiko sama pätеä kertolaskulle, eli voiko $(R, \cdot)$ myös olla ryhmä? Osoittautuu, että se on mahdollista vain yhdessä erikoistapauksessa. Nimittäin renkaassa R pätee $0 \cdot x = 0 = x \cdot 0$ kaikilla $x \in R$. Tämä seuraa osittelulaista:

$$0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x,$$

mistä lisäämällä $0 \cdot x$:n vasta-alkio saadaan $0 \cdot x = 0$. Toinen yhtälö todistetaan toisen osittelulain avulla samalla tavalla. Näin ollen, jos 0:llä olisi käänteisalkio $a \in R$, pätisi silloin

$$1 = 0 \cdot a = 0.$$

Tästä seuraa puolestaan, että kaikilla $x \in R$

$$x = 1 \cdot x = 0 \cdot x = 0,$$

eli renkaassa on tasan yksi alkio. Tällaista rengasta sanotaan *triviaaliksi* renkaaksi.
Samalla näemme, että jos ykkösellisessä renkaassa on vähintään kaksi alkiota, niin
1) $1 \neq 0$,
2) nollalla ei voi olla käänteisalkiota kertolaskun suhteen.
Näin ollen parasta mitä voi tapahtua on se, että kaikilla nollasta eroavilla alkioilla on käänteisalkio kertolaskun suhteen.

- **Kunnat**. Rengas on *kunta*, jos se on ykkösellinen, vaihdannainen, epätriviaali ja jokaisella nollasta eroavalla alkiolla on käänteisalkio kertolaskun suhteen.

Esimerkki 1.5. *Rationaalilukujen rengas ja reaalilukujen rengas ovat molemmat kuntia. Tämä on tunnettua analyysin peruskurssilta. Kokonaislukujen rengas ei ole kunta, itse asiassa ainoat $\mathbb{Z}$:ssä kääntyvät alkiot ovat* 1 *ja* -1.

Kunnassa voidaan määritellä "murtoluvut" eli kaikilla $a \in K, b \neq 0$ merkitään $\frac{a}{b} = ab^{-1} = b^{-1}a$. Näillä voidaan laskea samoilla säännöillä niin kuin murtoluvulle, kuten myös laaventaa ja supistaa yhteiset tekijät,

$$\frac{ad}{bd} = \frac{a}{b},$$

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd},$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Tässä $a, b, c, d \in K, b, d \neq 0$. Huomaa, että kunnassa kahden nollasta eroavan alkio a, b tulo ab on myös nollasta eroava (harjoitustehtävä).

Tärkeä esimerkki kunnasta on **kompleksilukujen kunta** $\mathbb{C}$. Palautetaan mieleen sen konstruktio. Joukkona $\mathbb{C}$ on reaalilukuparien $(x, y), x, y \in \mathbb{R}$, joukko eli $\mathbb{R}^2$. Yhteenlasku määritellään komponenteittain,

$$(x, y) + (x', y') = (x + x', y + y').$$

On melko selvää, että tällöin $(\mathbb{C}, +)$ on Abelin ryhmä. Nolla-alkio on $(0, 0)$ ja alkion (x, y) vasta-alkio on $(-x, -y)$. Kertolaskun määritelmä on hieman monimutkaisempi. Muodollisesti se määritellään seuraavalla kaavalla,

$$(x, y) \cdot (x', y') = (xx' - yy', xy' + x'y). \tag{1.6}$$

Liitäntä- ja osittelulakien osoittaminen jätetään lukijalle harjoitustehtäväksi. Myöhemmin, kun olemme kehittäneet lineaarialgebrallisia menetelmiä, esitämme tavan osoittaa, että $\mathbb{C}$ on kunta, soveltamalla lineaaristen kuvausten teoriaa. Tähän väliin mainitsemme vielä, että kertolaskun neutraalialkio on $(1, 0)$ ja alkion $(x, y) \neq (0, 0)$ käänteisalkio kertolaskun suhteen on

$$\left(\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2} \right).$$

Kompleksilukujen kertolaskun kaava saattaa näyttää oudolta ensinäkemältä, joten valaistaan vähän mistä siinä on kyse. Ensinnäkin, jos tarkastellaan vain muotoa $(x, 0)$ olevia lukuja, niin niiden kertolasku, ja itse asiassa myös yhteenlasku, näyttävät samalta kuin reaalilukujen kertolasku, sillä

$$(x, 0 + (y, 0) = (x + y, 0) \text{ ja}$$

$$(x, 0) \cdot (y, 0) = (xy, 0).$$

Tästä johtuen on luonnollista ”samaistaa” kompleksiluku $(x, 0)$ vastaavan reaaliluvun x kanssa ja merkitä sitä siis pelkästään x:llä.
Merkitään $i = (0, 1)$. Tällöin jokaisella $y \in \mathbb{R}$ pätee $iy = (0, 1) \cdot (y, 0) = (0, y)$ (tarkista!), joten jokainen kompleksiluku (x, y) voidaan kirjoittaa muotoon

$$(x, y) = (x, 0) + (0, y) = x + iy.$$

Tällainen esitys on yksikäsitteinen, sillä pari (x, y):hän määräytyy yksikäsitteisesti komponenteistaan x ja y.
Lisäksi helpolla laskulla voidaan todeta, että

$$i^2 = i \cdot i = (0, 1) \cdot (0, 1) = (-1, 0) = -1.$$

Näin ollen voidaan ajatella, että kompleksiluvut ovatkin muotoa $x+iy$ olevia lausekkeita, joissa x ja y ovat reaalilukuja ja i on niin sanottu *imaginääriyksikkö*, jolla on ominaisuus $i^2 = -1$. Tunnetusti millään reaaliluvulla ei tällaista ominaisuutta ole, sillä reaaliluvun neliö on aina ei-negatiivinen luku.
Tarkastellaan nyt asiaa käänteisesessä järjestyksessä. Kuvitellaan, että halutaan ”laajentaa” reaalilukujen systeemi $(\mathbb{R}, +, \cdot)$ sellaiseksi lukujärjestelmäksi, jossa luvut voidaan edelleenkin laskea yhteen ja kertoa keskenään, ja lisäksi yhtälöllä $z^2 = -1$ on ratkaisu.

Oletetaan, että meillä on sellainen systeemi ja olkoon i sellainen sen alkio, jolle $i^2 = -1$. Koska uudessakin järjestelmässä on yhteenlasku ja kertolasku, voimme kertoa luku i millä tahansa reaaliluvulla y, jolloin saadaan alkiot muotoa iy, ja voimme laskea yhteen mielivaltaisen $x \in \mathbb{R}$ ja juuri konstruoidun alkion yi. Nähdään siis, että uusi lukualue sisältää ainakin kaikki muotoa $x + iy$ olevat luvut.
Jos oletetaan lisäksi, että kertolasku on vaihdannainen ja osittelulait pätevät, nähdään, että silloin täytyy olla

$$(x + iy) \cdot (x' + iy') = xx' + i(x'y) + i(xy') + i^2yy' = (xx' - yy') + i(xy' + xy').$$

Jos nyt merkitään $x + iy = (x, y)$, nähdään, että tämähän on sama kuin kaava 1.6. Näin olleen kompleksilukuihin ja niiden kertolaskuun päädytään luonnollisella tavalla, jos halutaan laajentaa reaalilukujen systeemiä niin, että yhtälöllä

$$x^2 + 1 = 0$$

on ratkaisuja.
Yllä oleva yhtälö on esimerkki *polynomiyhtälöstä*, eli yhtälöstä, joka on muotoa

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0.$$

Kuntaa, jossa jokaisella polynomiyhtälöllä on ainakin yksi ratkaisu, sanotaan *algebrallisesti suljetuksi* kunnaksi. Reaalilukujen kunta $(\mathbb{R}, +, \cdot)$ ei tunnetusti ole algebrallisesti suljettu - onhan juuri yhtälö

$$x^2 + 1 = 0$$

sellainen polynomiyhtälö, jolla ei ole reaalilukuratkaisuja. Olemme nähneet, että kompleksilukujen kunnassa tällä yhtälöllä on ratkaisu $i = (0, 1)$. Osoittautuu, että kompleksilukujen kunta itse asiassa on algebrallisesti suljettu. Tämä tosiasia tunnetaan nimellä "Algebran peruslause". Palaamme algebran peruslauseeseen, algebrallisesti suljettuihin kuntiin ja polynomeihin myöhemmin, kun tutkimme äärellisulotteisten vektoriavaruuksien teoriaa.

- **Potenssit ja monikerrat.** Edellisessä kappaleessa käytimme polynomiyhtälön määritelmän yhteydessä alkion potensseja x^n, joten palautetaan mieleen miten ne määritellään. Olkoon X laskutoimituksella $\cdot$ varustettu joukko, $x \in X$ ja n positiivinen kokonaisluku. Määrittelemme x:nnen *n's potenssin* x^n rekursiivisesti induktiolla asettamalla

$$x^1 = x,$$

$$x^{n+1} = x^n \cdot x.$$

Kun laskutoimitus on liitännäinen, pätee siis

$$x^n = \underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ kertaa}}.$$

Jos laskutoimituksella on neutraalialkio e, voidaan määritellä myös nollas potenssi asettamalla $x^0 = e$. Jos x:llä on käänteisalkio x^{-1}, myös negatiivisten potenssien märitteleminen onnistuu - tällöin asetetaan (kun $n < 0$)

$$x^n = (x^{-1})^{-n}.$$

Jos laskutoimitusta merkitään additiivisesti, puhutaan potenssin sijaan x:n *monikerrasta*, jota merkitään nx:llä.
Voidaan osoittaa, että laskutoimituksen ollessa liitännäinen, pätevät tutut kaavat

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

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

Nämä ovat voimassa aina kun kaikki niissä esiintyvät potenssit ovat määriteltyjä. Erityisesti kaavat ovat aina tosia kun n ja m ovat positiivisia. Ryhmässä

potenssikaavat ovat aina määriteltyjä ja siis voimassa.

Jos laskutoimitus merkitään additiivisesti ja puhutaan monikerroista, niin yllä mainut kaavat näyttävät seuraavanlaisilta:

$$(n+m)x = nx + mx,$$
$$n(mx) = (nm)x.$$

Potenssikaavojen osoittaminen (esim. induktiolla) jätetään lukijalle harjoitustehtäväksi.

1.2 Modulit ja vektoriavaruudet

Ensimmäisessä luvussa olemme määritelleet joukon ”sisäisen” laskutoimituksen käsitteen ja käyneet läpi muutaman tärkeän esimerkin tällaisilla laskutoimituksilla varustetuista algebrallisista objekteista.
Usein törmätään myös hieman yleisempiin algebrallisiin operaatioihin, jotka ovat muotoa $f\colon Y \times X \to X$ olevia kuvauksia, missä Y ja X ovat joukkoja, mahdollisesti varustettuja muilla algebrallisilla struktuureilla. Tällaista kuvausta sanotaan joukon Y *(vasemmanpuoleiseksi) algebralliseksi operaatioksi joukossa* X. Jälleen kerran symbolin $f(y,x)$ sijasta yleensä käytetään ”multiplikatiivistaa” merkintää $y \cdot x$ tai yksinkertaisesti yx, eli ajatellaan, että X:n alkiot ikään kuin ”kerrotaan” vasemmalta Y:n alkioilla.
Joskus tarkastellaan *oikeapuolisia* Y:n algebrallisia operaatioita joukossa X eli kuvauksia $f\colon X \times Y \to X$. Tällöin luonnollinen merkintä on xy.
Tällä kurssilla lähes kaikki tämäntyyppiset operaatiot ovat vasemmanpuolisia.

Esimerkki 1.7. *Olkoon X joukko ja $X^X = Y$ joukko kuvauksia $f\colon X \to X$. Luonnollinen Y:n ”evaluointi”-operaatio joukossa X voidaan määritellä kaavalla $f \cdot x = f(x)$. Huomaa, että tässä joukolla Y on luonnollinen algebrallinen struktuuri - kuvausten yhdistämislaskutoimitus $\circ$. Seuraavat kaavat pätevät suoraan määritelmän nojalla:*

$$\mathrm{id} \cdot x = x \text{ kaikilla } x \in X,$$

$$(g \circ f)x = g \cdot (f \cdot x) \text{ kaikilla } g, f \in Y, x \in X.$$

Jos molemmat esiintyvät operaatiot kirjoitetaan multiplikatiivisesti ilman mitään erikoissymboleja, toinen yhtälö saa muodon

$$(gf)x = g(fx),$$

joka "näyttää assosiatiivisuudelta".
Jos rajoitetaan tarkastelu Y:n osajoukkoon $G = \mathrm{Perm}(X)$, saadaan esimerkki niin sanotusta ryhmän toiminnasta. *Ryhmän G toiminta joukossa X on kuvaus $G \times X \to X$, $(g, x) \mapsto gx$ jolle pätevät ehdot*

$$ex = x, x \in X,$$

$$g(g'x) = (gg')x, g, g \in G, x \in X.$$

Tässä siis e on G:n neutraalialkio.
Ryhmien toimintoja ovat erittäin tärkeitä matematiikassa. Niitä tutkitaan tarkemmin mm. kursseilla "Algebra II" ja "Transformaatioryhmät".

Nyt voimme vihdoinkin määritellä tämän kurssin keskeiset tutkimusobjektit - modulit ja vektoriavaruudet. Olkoon $(R, +, \cdot)$ (ykkösellinen) rengas. Olkoon M joukko ja oletetaan, että kuvaukset $+ \colon M \times M \to M$ ja $\cdot \colon R \times M \to M$ ovat annettuja. Kolmikko $(M, +, \cdot)$ on (vasemmanpuoleinen) *R-moduli*, jos seuraavat ehdot toteutuvat,

i) $(M, +)$ on Abelin ryhmä.

ii) $(r + r')m = rm + r'm$ kaikilla $r, r' \in R, m \in M$,

iii) $r(m + m') = rm + rm'$ kaikilla $r \in R, m, m' \in M$,

iv) $(rr')m = r(r'm)$ kaikilla $r, r' \in R, m \in M$,

v) jos R on ykkösellinen, oletamme lisäksi, että $1m = m$ kaikilla $m \in M$.

Laskutoimitusta $+$ sanotaan modulin M yhteenlaskuksi, laskutoimitusta $\cdot \colon R \times M \to M$ taas sanotaan M:n *skalaarituloksi*. Nimitys viittaa siihen, että R:n alkiot ajatellaan *skalaareina*, joilla sitten kerrotaan modulin alkioita vasemmalta.
Huomaa, että olemme tarkoituksella käyttäneet samoja symboleja merkitsemään eri laskutoimituksia - $+$ tarkoittaa yllä sekä R:n yhteenlaskua, että M:n yhteenlaskua. Yleensä matematiikassa tällaista symbolien "ylikuormittamista" ei katsota hyväksi, mutta joissakin tapauksissa se on sallittua ja on jopa vakiintunut tapa. Tämä on juuri sellainen tapaus. Asiayhteydestä pitäisi käydä selväksi mitä laskutoimitusta milloinkin tarkoitetaan. Esimerkiksi tarkastellaan yhtälöä, joka esiintyy yllä kohdassa ii) eli yhtälöä

$$(r + r')m = rm + r'm.$$

Tässä vasemmalla puolella $r+r'$ viittaa yhteenlaskuun renkaassa R, sen sijaan oikealla puolella rm ja rm' ovat jo M:n alkioita, joten lausekkeessa $rm+rm'$ plus-merkki viittaa jo modulin M yhteenlaskuun. Samoin yhtälössä

$$(rr')m = r(r'm)$$

vasemmalla puolella ensin kerrotaan alkiot r ja r' renkaassa R keskenään ja sitten lopputuloksella kerrotaan modulin alkiolla m. Oikealla puolella taas esiintyy vain M:ssä määritelty skalaarikertolasku.
Yhtälössä $r(m+m') = rm + rm'$ molemmilla puolilla esiintyvät M:n laskutoimitukset.

K-moduli V on *K-vektoriavaruus*, jos K on kunta.

Yllä määritelty modulin käsite tunnetaan kirjallisuudessa nimellä *vasemmanpuoleinen moduli*. Nimitys viittää siihen, että notaatiossa skalaarit kertovat modulin alkioita vasemmalta, jolloin modulin ehto iv) näyttää erityisen luonnolliselta.
On olemassa myös *oikeanpuoleisen R-modulin* käsite. Se määritellään muuten samalla tavalla kuin vasemmanpuoleinen moduli, mutta skalaarikertolasku on kuvaus $M \times R \to M$, jossa alkion $m \in M$ ja skalaarin $r \in R$ kertolasku kirjoitetaan mr. Modulin ehton näyttävät (notaatiota vaille) samoilta, paitsi että yhtälön iv) sijaasta oletetaan, että on voimassa ehto

iv)* $m(rr') = (mr)r'$ kaikilla $r, r' \in R, m \in M$.

Tällä kursilla tutkimme vain vasemmanpuoleisia moduleita, joista käytetään pelkästään nimitystä ”moduli”. Koska rajoitumme myöhemmin vain tapauksiin joissa R on kommutatiivinen rengas, tai jopa kunta, tämä ei ole itse asiassa mikään rajoitus, sillä mikä tahansa vasemmanpuoleinen moduli tällöin voidaan tulkita luonnollisella tavalla oikeanpuoleiseksi moduliksi yksinkertaisesti kirjoitamalla rm:n sijaasta mr, ja päinvastoin. Jätetään lukijan tehtäväksi miettiä, miksi tämä ei toimisi ei-vaihdannaisen renkaan tapauksessa.

Esimerkkejä 1.8. *1. Olkoon R rengas. Tällöin R on R-moduli, missä modulin yhteenlasku on sama kuin R:n yhteenlasku ja skalaarikertolasku $R \times R \to R$ on R:n rengas-kertolasku. Modulin ehdot toteutuvat, sillä kertolasku on liitännäinen ja osittelulait ovat voimassa.*

2. Yleisemmin olkoon $n \in \mathbb{N}$ mielivaltainen ja olkoon

$$M = R^n = \{(r_1, \ldots, r_n) \mid r_i \in R, i = 1, \ldots, n\}.$$

Määritellään yhteenlasku $M \times M \to M$ ja skalaarikertolasku $R \times M \to M$ koordinaateittain,

$$(r_1, \ldots, r_n) + (r_1, \ldots, r_n) = (r_1 + r_1', \ldots, r_n + r_n'),$$

$$r(r_1, \ldots, r_n) = (rr_1, \ldots, rr_n).$$

Helposti nähdään, että nämä toteuttavat modulin ehdot. Itse asiassa tämä seuraa myös seuraavasta esimerkistä, josta tämä esimerkki on erikoistapaus.

3. *Olkoon X mielivaltainen joukko ja R rengas. Kuvausten joukolla $R^X = \{f \colon X \to R\}$ on luonnollinen R-modulin struktuuri, joka määritellään "pisteittäin". Tarkemmin sanoen olkoot $f, g \in R^X, r \in R$. Määritellään $f + g, rf \in R^X$ kaavoilla*

$$(f + g)(x) = f(x) + g(x) \text{ (huom., yhteenlasku } R\text{:ssä)},$$

$$(rf)(x) = rf(x) \text{ (huom., kertolasku } R\text{:ssä)}.$$

Tarkistetaan, että tällöin M on R-moduli. Ensin käydään läpi $+$:n ominaisuudet. Olkoot $f, g, h \in R^X$ ja $r, r' \in R$. Tällöin

$$((f+g)+h)(x) = (f+g)(x)+h(x) = (f(x)+g(x))+h(x) = f(x)+(g(x)+h(x)) =$$

$$= f(x)+(g+h)(x) = (f+(g+h))(x), \text{ sillä yhteenlasku on liitännäinen } R\text{:ssä}.$$

Koska tämä pätee kaikilla $x \in X$, saadaan siis, että $(f + g) + h = f + (g + h)$ (kaksi kuvausta ovat samat täsmälleen kun niillä on samat arvot kaikissa määrittelyjoukon pisteissä).
Samalla tavalla tarkistetaan kaikki muut ominaisuudet. Määritellään nollakuvaus $0 \in R^X$ luonnollisesti asettamalla se pisteittäin nollaksi, $0(x) = 0$ kaikilla $x \in X$. Vastaalkio $-f$ määritellään ehdolla $(-f)(x) = -f(x)$. Saadaan

$$(f+g)(x) = f(x)+g(x) = g(x)+f(x) = (g+f)(x), \text{ joten } f+g = g+f.$$

$$(f + 0)(x) = f(x) + 0(x) = f(x) + 0 = f(x), \text{ joten } f + 0 = f,$$

$$(f+(-f))(x) = f(x)+(-f)(x) = f(x)+(-f(x)) = 0 = 0(x), \text{ joten } f+(-f) = 0.$$

Näin ollen $(R^X, +)$ on vaihdannainen ryhmä. Seuraavaksi tarkistetaan vielä skalaarikertolaskun ominaisuudet. Käyttämällä renkaan R ominaisuuksia nähdään

$$((r+r')f)(x) = (r+r')f(x) = rf(x)+r'f(x) = (rf)(x)+(rf')(x) = (rf+rf')(x),$$

$$\textit{joten } (r+r')f = rf + rf',$$

$$(r(r'f))(x) = r((r'f)(x)) = r(r'f(x)) = (rr')f(x) = ((rr')f)(x),$$

$$\textit{joten } r(r'f) = (rr')f,$$

$$(r(f+g))(x) = r(f+g)(x) = r(f(x)+g(x)) =$$

$$= rf(x) + rg(x) = (rf)(x) + (rg)(x) = (rf+rg)(x),$$

$$\textit{joten } r(f+g) = rf + rg.$$

Lopuksi, jos R on ykkösellinen

$$(1 \cdot f)(x) = 1 \cdot f(x) = f(x), \ \textit{joten } 1 \cdot f = f.$$

Olkoon $n \in \mathbb{N}$. Tällöin $(r_1, \ldots, r_n) \in R^n$ voidaan ajatella kuvauksena $\{1, \ldots, n\} \to R$. Näin ollen edellinen esimerkki 2) on erikoistapaus tästä esimerkistä, jossa $X = \{1, \ldots, n\}$ on äärellinen n:n alkion joukko. Tämän takia sivuutimme moduli-ominaisuuksien todistuksen esimerkeissä 1) ja 2).
Kun $n = 0$ saadaan niin sanottu triviaali R-moduli *jossa on vain nollaalkio, $R^{\{0\}} = \{0\}$.*

1.3 Homomorfismit

Kahdessa edeltävässä luvussa olemme nähneet paljon esimerkkejä erilaisilla laskutoimituksilla varustetuista joukoista. Samassa joukossa voidaan määritellä mielivaltainen määrä erityyppisiä laskutoimituksia, mukaan lukien "skalaarikertolaskuja", joiden määritelmässä esiintyvät siis toiset joukot. Tällaista "systeemiä", jonka muodostavat joukko ja joku kokoelma sen laskutoimituksia sanomme *algebralliseksi struktuuriksi*. Kaksi algebrallista struktuuria ovat *samaa tyyppiä*, jos niissä on sama määrä samantyyppisiä laskutoimituksia, jotka mahdollisesti toteuttavat joitakin lisäehtoja. Periaatteessa kaikki, mitä tähän asti olemme tehneet, oli erilaisten tällaisten tyyppien tarkastelu. Esimerkiksi, jos joukossa X on määritelty yksi laskutoimitus $\cdot$, joka on liitännäinen, jossa on neutraalialkio ja jossa jokaisella alkiolla on käänteisalkio, kyseessä on algebrallinen struktuuri *ryhmä*. Kaikki ryhmät siis kuuluvat samaan tyyppiin algebrallisesta struktuurista - *ryhmän tyyppiin*. Samoin rengas on sellainen algebrallinen struktuuri, jossa joukolla on kaksi laskutoimitusta $+$ ja $\cdot$, jotka toteuttavat lisäksi kaikki renkaan aksioomat. R-modulin tyypissä taas meillä on kaksi laskutoimitusta, joista toinen eli yhteenlasku $+$ on joukon sisäinen laskutoimitus ja toinen eli skalaarikertolasku $\cdot$ on kiinitetyn renkaan R operaatio modulissa. Lisäksi kaikki modulin aksioomat oletetaan

päteviksi.
Emme anna mitään sen täsmällisempää määritelmää algebralliselle struktuurille ja sen tyypille, esimerkeistä näiden merkityksen pitäisi tulla selväksi.

Huomattava osa nykymatematiikkaa on juuri erilaisilla struktuureilla varustettujen joukkojen tutkimista. Esimerkiksi topologiassa tutkitaan joukkoja, joissa on määritelty *topologia* eli eräs tapa ajatella tämä joukko geometriseksi olioksi. Algebrassa taas olemme kiinnostuneita algebrallisilla struktuureilla varustetuista joukoista.

Joukot ja niiden struktuurit eivät kuitenkaan riitä yksinään. Yhtä tärkeitä ovat niiden väliset *kuvaukset* ja muut relaatiot. Tietenkään, jos joukoilla oletetaan olevan lisästruktuuria, mitkä tahansa niiden väliset kuvaukset eivät ole kiinnostavia, vaan ainoastaan sellaiset, jotka ovat jossakin mielessä *yhteensopivia* näiden struktuurien kanssa. Tällaisia kuvauksia sanotaan yleisesti *morfismeiksi*. Esimerkiksi topologiassa luonnolliset morfismit ovat jatkuvat kuvaukset.

Mitä tämä ”yhteensopivuus” tarkoittaisi algebrassa? Olkoot X ja Y molemmat yhdellä laskutoimituksella varustettuja joukkoja. Merkitsemme molempia laskutoimituksia multiplikatiivisesti. Sanomme, että kuvaus $f\colon X \to Y$ on *yhteensopiva laskutoimitusten kanssa*, jos kaikilla $x, x' \in X$ pätee

$$f(xx') = f(x)f(x').$$

Tässä siis vasemmalla puolella esiintyy X:n laskutoimitus ja oikealla puolella Y:n laskutoimitus. Jos laskutoimitukset ajatellaan kuvauksina $X \times X \to X$, $Y \times Y \to Y$ (mitä ne määritelmän mukaan ovatkin) yhteensopivuusehto voidaan myös ilmaista kommutatiivisena diagrammina

$$\begin{array}{ccc} X \times X & \longrightarrow & X \\ \downarrow{\scriptstyle f\times f} & & \downarrow{\scriptstyle f} \\ Y \times Y & \longrightarrow & Y. \end{array}$$

Myös nimitystä ”*laskutoimitusta säilyttävä kuvaus*” käytetään.

Esimerkki 1.9. *Tarkastellaan laskutoimitukset* $+$ *:ssä (reaalilukujen tavallinen yhteenlasku) ja* $\cdot$ *:ssä (kompleksilukujen kertolasku). Määritellään kuvaus* $f\colon \mathbb{R} \to \mathbb{C}$ *kaavalla* $f(x) = (\cos x, \sin x)$*. Sinin ja kosinin yhteenlaskukaavat implikoivat silloin, että*

$$f(x+y) = (\cos(x+y), \sin(x+y)) = (\cos x \cos y - \sin x \sin y, \sin x \cos y + \cos x \sin y) =$$

$$= (\cos x, \sin x) \cdot (\cos y, \sin y).$$

Näin ollen f on yhteensopiva annettujen laskutoimitusten kanssa.

Olemme määritelleet myös toisentyyppisen laskutoimitus-käsitteen eli joukon Y laskutoimituksen joukossa X, $(y, x) \mapsto yx$. Jos oletetaan, että X ja X' ovat molemmat varustettuja tälläisellä Y:n laskutoimituksella (huom. joukko Y siis sama molemmilla struktuureilla), niin sanomme, että kuvaus $f\colon X \to Y$ *on yhteensopiva laskutoimitusten kanssa*, jos kaikilla $y \in Y$ ja $x \in X$ pätee

$$f(yx) = yf(x).$$

Nyt voimme palata kysymykseen, mitä sopivat "morfismit" algebrallisten struktuurien välillä ovat. Olkoot X ja Y joukkoja, joissa molemmissa on määritelty *samantyyppiset* algebralliset struktuurit. Tällöin niiden välinen *homomorfismi* on sellainen kuvaus $f\colon X \to Y$ joka on yhteensopiva vastaavien laskutoimitusten suhteen ja lisäksi säilyttää struktuuriin liittyvät ehdot. Taaskaan emme anna mitään täsmällistä formaalia määritelmää, vaan tyydymme sen sijaan konkreettisiin esimerkkeihin, jotka lienevät riittäviä selvittämään, mistä on kyse.

Esimerkiksi, olkoot $(G, \cdot)$ ja $(G', \cdot)$ molemmat ryhmiä. Käytämme tässä tarkoituksella samaa symbolia tarkoittamaan kahta erilaista laskutoimitusta, jotta lukija tottuisi tähän yleiseen käytäntöön.

Kuvaus $f\colon G \to G'$ on *ryhmien välinen homomorfismi*, jos se on yhteensopiva laskutoimitusten kanssa, eli jos ja vain jos kaikilla $g, h \in G$ pätee

$$f(gh) = f(g)f(h). \tag{1.10}$$

Periaatteessa yleisen käytännön mukaan meidän pitäisi vielä vaatia, että f säilyttää neutraalialkiot ja käänteisalkiot, eli

$$f(e_G) = e_H \text{ ja } f(g^{-1}) = (f(g))^{-1} \text{ kaikilla } g \in G. \tag{1.11}$$

Tämä ei kuitenkaan ole tarpeellista tässä yhteydessä, sillä voidaan todistaa, että mikä tahansa ryhmähomomorfismi, eli ryhmien välinen kuvaus, joka toteuttaa ehdon 1.10, toteuttaa automaattisesti myös ehdot 1.11. Todistetaan vaikka ensimmäinen ehto. Jos f on ryhmähomomorfismi, pätee

$$f(e_G) = f(e_G e_G) = f(e_G)f(e_G),$$

mistä kertomalla $f(e_G)$:n käänteisalkiolla G':ssä saadaan $f(e_G) = e_{G'}$. Ominaisuuden $f(g^{-1}) = (f(g))^{-1}$ todistaminen jätetään harjoitustehtäväksi.

Esimerkki 1.12. *Edellisen esimerkin kuvaus* $f\colon (\mathbb{R},+) \to (\mathbb{C},\cdot)$, $f(x) = (\cos x, \sin x)$ *ei ole ryhmähomomorfismi, sillä vaikka* $(\mathbb{R},+)$ *on ryhmä,* $(\mathbb{C},\cdot)$ *ei ole sellainen - nollalla ei ole käänteisalkiota kertolaskun suhteen.*
Kuitenkin joukossa $C^* = \mathbb{C}\setminus\{0\}$ *voidaan määritellä samanlainen kertolasku kuin* $\mathbb{C}$*:ssä ja tällä laskutoimituksella varustettuna* $(\mathbb{C}^*,\cdot)$ *on ryhmä. Kuvauksen* f *määritelmästä seuraa, että* $f(x) \neq 0$ *kaikilla* $x \in \mathbb{R}$*. Näin ollen* f *voidaan ajatella kuvauksena* $\mathbb{R} \to \mathbb{C}^*$*. Nyt sekä lähtö-, että maalijoukko ovat molemmat ryhmiä, ja* f *säilyttää laskutoimituksen, joten* f *on ryhmähomomorfismi.*

Seuraavaksi tarkastellaan kahden renkaan $(R,+,\cdot)$ ja $(R',+,\cdot)$ välisiä kuvauksia. Kuvausta $f\colon R \to R'$ sanotaan *rengashomomorfismiksi*, jos se on yhteensopiva sekä yhteenlaskun, että kertolaskun suhteen, eli jos kaikilla $x, y \in R$ pätee

$$f(x+y) = f(x) + f(y) \text{ ja } f(xy) = f(x)f(y). \tag{1.13}$$

Jos molemmat renkaat ovat ykkösellisiä, oletamme lisäksi, että $f(1_R) = 1_{R'}$. Tällä kertaa tämä on tarpeellinen lisäoletus, sillä se ei seuraa välttämättä ehdoista 1.13 - katso esimerkkejä alla.

Erityisesti, jos K ja K' ovat molemmat kuntia, niiden välinen kuvaus $f\colon K \to K'$ on *kuntahomomorfismi*, jos se on rengashomomorfismi ja $f(1_K) = f(1_{K'})$. Tällöin kaikille $x \neq 0$ pätee $f(x^{-1}) = (f(x))^{-1}$ (harjoitustehtävä).

Esimerkkejä 1.14. *1. Olkoot* R *ja* R' *mielivaltaisia renkaita. Tällöin vakionollakuvaus* $f\colon R \to R'$, $f(x) = 0$ *kaikilla* $x \in R$*, on rengashomomorfismi, sillä*

$$f(x+y) = 0 = 0 + 0 = f(x) + f(y),$$

$$f(xy) = 0 = 0 \cdot 0 = f(x) \cdot f(y).$$

Jos molemmat renkaat ovat ykkösellisiä ja R' *on epätriviaali, nollakuvaus* **ei ole** *ykkösellisten renkaiden välinen homomorfismi. Erityisesti, jos kyse on kunnista, tällaista nollakuvausta ei koskaan hyväksytä kuntahomomorfismiksi.*

2. Olkoon R *kaikkien* 2×2*-matriisien muodostama rengas. Määritellään kuvaus* $f\colon \mathbb{Z} \to R$ *kaavalla*

$$f(n) = \begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix}.$$

Tällöin f *on rengashomomorfismi, mutta ei ole ykkösellisten renkaiden homomorfismi, sillä* $f(1)$ *ei ole* R*:n yksikköalkio.*

3. *Olkoon $R = \mathbb{R}^{\mathbb{R}}$ eli kaikkien kuvausten $\mathbb{R} \to \mathbb{R}$ rengas ja olkoon $a \in \mathbb{R}$. Määritellään kuvaus $A\colon R \to \mathbb{R}$ kaavalla $A(f) = f(a)$. Tällöin A on ykkösellisten renkaiden homomorfismi.*

Lopuksi tarkastellaan R-moduleja kiinteällä renkaalla R. Näiden välisiä morfismeja sanotaan *R-lineaarisiksi kuvauksiksi*. Täsmällisesti, olkoot M ja M' molemmat R-renkaita. Kuvausta $L\colon M \to M'$ sanotaan R-lineaariseksi, jos kaikilla $x, y \in M$ ja $r \in R$ pätee

$$L(x+y) = L(x) + L(y) \text{ ja } L(rx) = rL(x). \tag{1.15}$$

Esimerkkejä 1.16. *1) Olkoon V kaikkien (jokaisella pisteessä)* **derivoituvien** *kuvausten $f\colon \mathbb{R} \to \mathbb{R}$ muodostama $\mathbb{R}$-vektoriavaruus, tutuilla laskutoimituksilla*

$$(f+g)(x) = f(x) + g(x),$$
$$(rf)(x) = rf(x).$$

Koska derivoituvien kuvausten summa ja tulo ovat derivoituvia ja jokainen vakiokuvaus on derivoituva, nämä ovat hyvin määriteltyjä. Kuvaus $\frac{d}{dx}\colon V \to \mathbb{R}^{\mathbb{R}}$, $f \mapsto Df$ (funktio kuvataan sen derivaattafunktiolle) on vektoriavaruuksien V ja $\mathbb{R}^{\mathbb{R}}$ välinen $\mathbb{R}$-lineaarikuvaus. Huomaa, että tämä ei ole lineaarikuvaus $V \to V$, sillä derivoituvan funktion derivaatta ei välttämättä ole itse derivoituva funktio.

2) Olkoon V kaikkien jatkuvien funktioiden $f\colon [a,b] \to \mathbb{R}$ muodostama $\mathbb{R}$-vektoriavaruus. Tällöin kuvaus $L\colon V \to \mathbb{R}$,

$$L(f) = \int_a^b f(x)dx$$

on $\mathbb{R}$-lineaarinen.

Tämän kurssin keskeisiä aiheita on äärellisulotteisten vektoriavaruuksien välisten lineaarikuvausten tutkiminen.

-**Isomorismit.** Tärkeä erikoistapaus (homo)morfismista muodostavat *isomorfismi*. Kahden algebrallisen struktuurin välinen morfismi $f\colon X \to Y$ sanotaan *isomorfismiksi* jos se on bijektio. Morfismin määritelmästä yleensä seuraa, että bijektiivisen morfismin käänteiskuvaus $f^{-1}\colon Y \to X$ on myös morfismi. Esimerkiksi helposti tarkistetaan, että jos joukoissa X ja Y on laskutoimitukset $\cdot$ ja $f\colon X \to Y$ on kuvaus joka on yhteensopiva näiden laskutoimitusten suhteen, niin myös f^{-1} säilyttää nämä laskutoimitukset (tarkista!). Samoin, jos molemmissa on määritelty jonkun joukon Z laskutoimitus ja f

säilyttää sen, niin myös f^{-1} säilyttää sen (tarkista!). Jos molemmissa struktuureissa on esimerkiksi neutraalialkio jonkun laskutoimituksen suhteen ja f kuvaa toisen neutraalialkion toiselle, niin sama on totta käänteiskuvaukselle (käänteiskuvauksen määritelmän nojalla!). Näin ollen ainakin kaikissa meitä kiinnostavissa tapauksissa eli ryhmhomomorfismin/ryhmähomomorfismin ja lineaarisen kuvauksen kohdalla nähdään, että bijektiivisen morfismin käänteiskuvaus on myös ryhmä/rengas/modulien homomorfismi.

Jos kahden struktuurin X ja Y välillä on olemassa isomorfismi $f\colon X \to Y$, niin sanomme, että X ja Y ovat *isomorfiset* keskenään. Tällöin usein merkitään $X \cong Y$. Isomorfismia taas merkitään usein symbolisesti $f\colon X \xrightarrow{\cong} Y$. Isomorfiset struktuurit ovat "täysin samanlaiset" algebran näkökulmasta, eli ne eroavat vain alkioiden nimeämiseen suhteen. Algebra ei pysty näkemään niiden välillä mitään eroa. Olemme jo nähneet esimerkin tästä, kun puhuimme kompleksiluvuista. Nimittäin tarkastellaan muotoa $(x, 0)$ olevia kompleksilukuja. Näiden muodostama joukko Y on suljettu kompleksilukujen yhteen- ja kertolaskun suhteen, joten voimme määritellä Y:ssä yhteen-ja kertolasku luonnollisella tavalla. Kuten olemme aikaisemmin huomaneet, nämä "näyttävät" samoilta kuin vastaavat reaalilukujen operaatiot. Hienommin ilmaistuna tämä voidaan kiteyttää sanomalla, että kuvaus $i\colon \mathbb{R} \to Y$, $i(x) = (x, 0)$ on homomorfismi. Koska lisäksi se on bijektio, se on rengasisomorfismi. Alkiot $x \in \mathbb{R}$ ja $(x, 0) \in \mathbb{C}$ käyttäytyvät algebran näkökulmasta täysin samalla tavalla, sen takia ne "samastetaan" ja ajatellaan kompleksiluvun $(x, 0)$ olevan reaaliluku x.

1.4 Alistruktuurit

Olkoon X jollakin matemaattisella struktuurilla varustettu joukko ja olkoon $Y \subset X$ sen osajoukko. On hyvää tietää, milloin X:n struktuuri määrittelee samantyyppisen struktuurin osajoukkoon Y. Tällöin Y sanotaan X:n *alistruktuuriksi*.
Esimerkiksi tasossa $\mathbb{R}^2$ on määritelty luonnollinen geometrinen struktuuri - voimme laskea pisteiden etäisyyden, määritellä avoimet joukot, kulmat jne. Jos Y on tason osajoukko, esimerkiksi kolmio tai paraabeli, tämä tason geometrinen struktuuri määrittelee, ainakin osittain, samantyyppisen struktuurin Y:hun.
Meitä kiinnostaa luonnollisesti algebrallisen alistruktuurin käsite. Tarkastellaan ensin yksinkertaisin tilanne - olkoon X laskutoimituksella $\cdot$ varustettu joukko ja olkoon Y X:n osajoukko. Sanomme, että Y on *vakaa* laskutoimituksen $\cdot$ suhteen jos kaikilla $x, y \in Y$ pätee $xy \in Y$. On selvää, että jos

Y on vakaa, X:n laskutoimituksen rajoittuma määrittelee laskutoimituksen $\cdot\colon Y \times Y \to Y$. Voimme siis puhua algebrallisesta struktuurista $(Y, \cdot)$.
Samoin, jos X on varustettu joukon Z laskutoimituksella $Z \times X \to X, (z, x) \mapsto zx$, niin sen osajoukko $Y \subset X$ on *vakaa* tämän laskutoimituksen suhteen, jos kaikilla $z \in Z, y \in Y$ pätee $zy \in Y$. Taas on selvää, että tällöin voimme rajoittaa Z:n laskutoimitus X:ssä laskutoimitukseksi $Z \times Y \to Y$ osajoukossa Y.
Termin "vakaa laskutoimituksen suhteen" synonyymina käytetään myös termiä "suljettu" laskutoimituksen suhteen.

Esimerkki 1.17. *Tarkastellaan kokonaislukujen joukkoa $\mathbb{Z}$ varustettuna yhteenlaskulla. Tällöin positiivisten kokonaislukujen osajoukko $\mathbb{N}_+ = \{1, 2, 3, \dots, \}$ on vakaa $\mathbb{Z}$:ssä. Myös ei-negatiivisten kokonaislukujen osajoukko $\mathbb{N} = \{0, 1, \dots, \}$ on vakaa $\mathbb{Z}$:ssä. Parillisten kokonaislukujen joukko on vakaa, sillä kahden parillisen luvun summa on myös parillinen. Sen sijaan parittomien kokonaislukujen summa ei itse asiassa koskaan ole pariton. Esimerkiksi $1 + 3 = 4$. Näin ollen parittomien kokonaislukujen joukko ei ole suljettu yhteenlaskun suhteen.*
Tarkastellaan reaalilukujoukkoa $\mathbb{R}$ varustettuna $\mathbb{R}$-vektoriavaruuden struktuurilla eli varustettuna $\mathbb{R}$-skalaarikertolaskulla. Tällöin jos yritetään rajoittaa tämä laskutoimitus osajoukkoon $\mathbb{Q}$, niin se ei ole vakaa sen suhteen, sillä reaaliluvun ja rationaaliluvun tulo ei vältämättä ole rationaaliluku.

Tarkastella nyt yleistä tilannetta.
Olkoon X algebrallisella struktuurilla varustettu joukko ja olkoon $Y \subset X$. Tällöin Y on struktuurin X *alistruktuuri* jos se on vakaa jokaisen X:n laskutoimituksen suhteen ja lisäksi toteuttaa samat mahdolliset lisäehdot, jotka X toteuttaa. Tällöin myös merkitään usein $Y \leq X$.

Sellaiset ominaisuudet kuin laskutoimitusten liitännäisyys, vaihdannaisuus tai ositteleminen toistensa suhteen selvästi "periytyvät" automaattisesti X:n vakaisiin osajoukkoihin. Sen sijaan olemassaolo-ominaisuudet, kuten neutraalialkion tai käänteisalkioiden olemassaolo eivät välttämättä ole voimassa vakaassa osajoukossa, vaikka ne olisivat voimassa X:ssä, joten ne pitää vaatia alistruktuurilta erikseen. Teemme tähän liittyen heti seuraavan huomautuksen. Oletetaan, että algebrallisella oliolla X on neutraalialkio e. Tällöin **ei riittää**, jos oletamme, että sen alistruktuurilla samalla (indusoidulla) laskutoimituksella on neutraalialkio, vaan sen pitää olla sama neutraalialkio kuin koko X:ssä, eli sama alkio e. Nimittäin voi käydä myös niin, että vakaalla osajoukolla Y on neutraalialkio jonkun laskutoimituksen suhteen, joka ei ole neutraalialkio X:ssä. Vaikka tällainen osajoukko on sitten samaa tyyppiä

oleva algebrallinen struktuuri, sitä ei kuitenkaan lasketa X:n alistruktuuriksi.
Katsotaan nyt mitä alistruktuurin käsite tarkoittaa konkreettisesti minkäkin tutun struktuurin tapauksessa.
Olkoon $(G, \cdot)$ ryhmä ja $H \subset G$. Tällöin H on G:n *aliryhmä* jos

$$xy \in H \text{ for all } x, y \in H, \text{ eli } H \text{ on vakaa,} \tag{1.18}$$

$$e \in H, \text{ missä } e \text{ on } G\text{:n neutraalialkio ja,} \tag{1.19}$$

$$x^{-1} \in H \text{ kaikilla } x \in H. \tag{1.20}$$

Esimerkki 1.21. *Tarkastelemme ryhmän $(\mathbb{Z}, +)$ vakaita osajoukkoja edellisestä esimerkistä, eli osajoukot $\mathbb{N}_+$, $\mathbb{N}$ ja parillisten kokonaislukujen joukko. Positiivisten kokonaislukujen ryhmä ei ole aliryhmä, sillä se ei sisällä edes neutraalialkiota 0. Luonnollisten lukujen joukko $\mathbb{N}$ sisältää kyllä neutraalialkion, mutta ei ole suljettu vasta-alkioiden suhteen, sillä esimerkiksi $1 \in \mathbb{N}$, mutta $-1 \notin \mathbb{N}$. Näin ollen sekään ei ole aliryhmä.*

Parillisten kokonaislukujen osajoukko $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$ sen sijaan on aliryhmä - se on vakaa, se sisältää neutraalialkion 0 ja on suljettu vasta-alkioiden suhteen, sillä parillisen luvun vastaluku on parillinen.

Olkoon $(R, +, \cdot)$ rengas ja $R' \subset R$. Tällöin R' on R:n *alirengas* jos
1) $(R', +)$ on Abelin ryhmän $(R, +)$ aliryhmä,
2) R' on vakaa myös kertolaskun suhteen.
Jos lisäksi R on ykkösellinen ja 1 on sen neutraalialkio kertolaskun suhteen, R' on R:n *ykkösellinen alirengas* jos $1 \in R'$.
Jos K on kunta ja $K' \subset K$, sanomme, että K' on K:n *alikunta*, jos K' on K:n ykkösellinen alirengas, K' ei ole triviaali ja lisäksi K' on suljettu kertolaskun käänteisalkioiden suhteen eli kaikilla $k \in K', k \neq 0$ pätee $k^{-1} \in K'$.

Esimerkkejä 1.22.

1. *$(\mathbb{Z}, +, \cdot)$ on renkaan $(\mathbb{R}, +, \cdot)$ ykkösellinen alirengas. Jos $(\mathbb{R}, +, \cdot)$ ajatellaan kuntana, $(\mathbb{Z}, +, \cdot)$ ei kuitenkaan ole $(\mathbb{R}, +, \cdot)$:n alikunta, sillä $\mathbb{Z}$ ei ole suljettu käänteisalkioiden suhteen - esimerkiksi $2 \in \mathbb{Z}$, mutta $\frac{1}{2} \notin \mathbb{Z}$.*

2. *$(\mathbb{R}, +, \cdot)$ on kompleksilukukunnan $(\mathbb{C}, +, \cdot)$ alikunta, kunhan samaistetaan $x \in \mathbb{R}$ kompleksiluvun $(x, 0)$:n kanssa.*

3. *Parillisten lukujen joukko $2\mathbb{Z}$ on $\mathbb{Z}$:n aliryhmä yhteenlaskun suhteen. Se on myös vakaa kertolaskun suhteen. Näin ollen $(2\mathbb{Z}, +, \cdot)$ on $(\mathbb{Z}, +, \cdot)$:n*

alirengas. Jos kuitenkin ajatellaan $\mathbb{Z}$ **ykkösellisenä** *renkaana,* $2\mathbb{Z}$ *ei enää ole sen alirengas, sillä* $1 \notin 2\mathbb{Z}$.

4. 2×2*-matriisien joukko* $M(2 \times 2)$ *on tunnetusti ykkösellinen rengas matriisien yhteen- ja kertolaskun suhteen. Tarkastellaan sen osajoukkoa*

$$R = \{\begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix} \mid n \in \mathbb{Z}\}.$$

Tällöin R *on renkaan* $M(2 \times 2)$ *alirengas, jos viimeksi mainittua* **ei** *ajatella ykkösellisenä renkaana. Koska* $M(2 \times 2)$*:n yksikkö, eli matriisi* $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$*, ei ole* R*:ssä,* R *ei ole* $M(2 \times 2)$*:n ykkösellinen alirengas. Kuitenkin renkaana* R **on** *ykkösellinen, sillä matriisi* $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ *on* R*:ssä kertolaskun neutraalialkio.*

Esimerkki 1.23. *Kokonaislukujen joukko* $(\mathbb{Z}, +)$ *on Abelin ryhmä. Jokaisella* $m \in \mathbb{N}$ *määritellään osajoukko*

$$m\mathbb{Z} = \{mn \mid m \in \mathbb{Z}\}.$$

Tällöin $m\mathbb{Z}$ *on* $\mathbb{Z}$*:n aliryhmä (yhteenlaskun suhteen), sillä*

$$0 = m \cdot 0 \in m\mathbb{Z},$$

$$mn + mn' = m(n + n'), \text{ joten } m\mathbb{Z} \text{ on suljettu yhteenlaskun suhteen,}$$

$$-(mn) = \text{ joten } m\mathbb{Z} \text{ on suljettu vasta-alkioiden suhteen.}$$

Kääntäen voidaan osoittaa, että nämä ovat kaikki $\mathbb{Z}$*:n aliryhmät. Tämä jätetään harjoitustehtäväksi.*

Olkoon M R-moduli. Sen osajoukko M' on M:n *alimoduli*, jos

1) $(M', +)$ on $(M, +)$ aliryhmä ja

2) M' on suljettu skalaarikertolaskun suhteen, eli kaikilla $r \in R$ ja $m \in M'$, myös $rm' \in M'$.

Määritelmästä seuraa, että alimoduli on itse R-moduli.
K-vertoriavaruuden V alimodulia sanotaan *(vektori)aliavaruudeksi.*

Esimerkki 1.24. *Olkoon* V *kaikkien kuvausten* $f\colon \mathbb{R} \to \mathbb{R}$ $\mathbb{R}$*-vektoriavaruus (kts. esimerkki 1.8). Seuraavat ovat* V*:n aliavaruuksia -*

1. $V_0 = \{f \in V \mid f \text{ on jatkuva } 0\text{:ssä}\}$,

2. $C^0 = \{f \in V \mid f \text{ on jatkuva }\}$,

3. $C^1 = \{f \in V \mid f' \text{ on olemassa koko } \mathbb{R}\text{:ssä}\}$.

Esimerkki 1.25. *Kaikki polynomifunktiot $f\colon \mathbb{R} \to \mathbb{R}$ muodostavat vektoriavaruuden $\mathbb{R}^{\mathbb{R}}$ aliavaruuden P. Jokaisella $n \in \mathbb{N}$ kaikkien polynomit joiden aste on pienempi tai yhtäsuuri kuin n muodostavat P:n aliavaruuden P_n. Kun $m \leq n$ vektoriavaruus P_m on selvästi avaruuden P_n aliavaruus.*

Seuraavaksi tarkastellaan alistruktuurien ja homomorfismien yhteyksiä. Jos joukolla X on algebrallinen struktuuri ja $Y \subset X$ on sen alistruktuuri, niin inklusiokuvaus $i\colon Y \hookrightarrow X$ on vältämättä homomorfismi (tämän struktuurin tyypin suhteen).

Olkoot X ja Y laskutoimituksella varustettuja joukkoja ja $f\colon X \to Y$ niiden laskutoimitusten kanssa yhteensopiva kuvaus. Tällöin f:n *kuvajoukko*

$$\operatorname{Im} f = \{f(x) \mid x \in X\} \subset Y$$

on vakaa Y:n laskutoimituksen suhteen. Tämä nähdään seuraavasti - olkoot $x, y \in X$, tällöin

$$f(x) \cdot f(y) = f(xy) \in \operatorname{Im} f.$$

Jos joukossa X on neutraalialkio e, $f(e)$ on neutraalialkio $\operatorname{Im} f$:ssä, sillä

$$f(e) \cdot f(x) = f(ex) = f(x) = f(xe) = f(x) \cdot f(e).$$

Jos joukossa X alkiolla x on käänteisalkio x^{-1}, myös alkiolla $f(x) \in \operatorname{Im} f$ on käänteisalkio $f(x^{-1})$, sillä

$$f(x) \cdot f(x^{-1}) = f(xx^{-1}) = f(e) = f(x^{-1}x) = f(x^{-1}) \cdot f(x).$$

Näin ollen ainakin meitä kiinnostavien struktuurien tapauksessa $\operatorname{Im} f$ on jopa alistruktuuri. Tarkemmin pätee:

- Jos $f\colon G \to G'$ on ryhmien välinen homomorfismi, $\operatorname{Im} f$ on G':n aliryhmä.
- Jos $f\colon R \to R'$ on rengashomomorfismi, $\operatorname{Im} f$ on R':n alirengas. Jos R on ykkösellinen, $\operatorname{Im} f$ on ykkösellinen. Jos R on kunta ja $f(1) \neq 0$, niin $\operatorname{Im} f$ on kunta.

- Jos $L\colon M \to M'$ on lineaarinen kuvaus R-modulien välillä, $\operatorname{Im} f$ on R':n alimoduli.

Seuraavaksi tarkastellaan hieman erikoisempaa tilannetta , joka osoittautuu kuitenkin tärkeäksi meille. Olkoot G, G' **ryhmiä** ja olkoon $f\colon G \to G'$ ryhmähomomorfismi. Määritellään f:n *ydin* $\operatorname{Ker} f$ seuraavasti,

$$\operatorname{Ker} f = \{x \in G \mid f(x) = e'\},$$

missä e' on G':n neutraalialkio. Tällöin $\operatorname{Ker} f$ on aliryhmä G:ssä, sillä

- jos $x, y \in \operatorname{Ker} f$, niin $f(xy) = f(x)f(y) = e'e' = e'$,
- $e \in \operatorname{Ker} f$, sillä $f(e) = e'$,
- jos $x \in \operatorname{Ker} f$, niin $f(x^{-1}) = f(x)^{-1} = e'^{-1} = e'$.

Lisäksi $N = \operatorname{Ker} f$ ei ole mikä tahansa aliryhmä, vaan se toteuttaa seuraavan tärkeän lisäehdon:

- jos $x \in G$ on mielivaltainen ja $h \in N$, niin $xhx^{-1} \in N$.

Tällaisia aliryhmiä sanotaan *normaaleiksi*. Jos G on vaihdannainen ryhmä, mikä tahansa sen aliryhmä on automaattisesti normaali. Erityisesti näin on asian laita, kun tarkastellaan yhteenlaskuryhmiä $(R, +)$, $(M, +)$, missä $(R, +, \cdot)$ on rengas tai $(M, +, \cdot)$ on R-moduli.
Seuraavaksi tutkitaan rengas- ja modulihomoformismin ytimiä. Olkoot R, R' renkaita ja $f\colon R \to R'$ rengashomomorfismi. Tällöin se on erityisesti ryhmähomomorfismi yhteenlaskujen suhteen, joten voidaan edelleen määritellä sen ydin kuten edellä,

$$\operatorname{Ker} f = \{x \in R \mid f(x) = 0\}.$$

Yllätodistetun nojalla $I = \operatorname{Ker} f$ on $(R, +)$:n (normaali) aliryhmä. Se on myös suljettu kertolaskun suhteen, joten se on R:n alirengas. Itse asiassa I:llä on paljon vahvempi ominaisuus. Nimittäin, olkoon $x \in I$ ja olkoon $r \in R$ **mielivaltainen** alkio. Tällöin

$$f(rx) = f(r)f(x) = f(r) \cdot 0 = 0 \text{ ja}$$

$$f(xr) = f(x)f(r) = 0 \cdot f(r) = 0.$$

Toisin sanoen I:llä on seuraavat ominaisuudet,

- $(I, +)$ on $(R, +)$:n aliryhmä, ja

- kaikilla $x \in I, r \in R$ pätee $xr \in I$ ja $rx \in I$.

Tällaisia R:n alirenkaita sanotaan *ideaaleiksi*. Huomaa, että jos R sattuu olemaan ykkösellinen rengas, niin I silti hyvin harvoin on sen ykkösellinen alirengas. Nimittäin jos $1 \in I$ toinen ehto yllä implikoi, että kaikilla $r \in R$ pätee $r = r \cdot 1 \in I$, joten $I = R$.

Esimerkki 1.26. *Määritellään kaikki renkaat $(\mathbb{Z}, +, \cdot)$ ideaalit. Olkoon I $\mathbb{Z}$:n ideaali. Tällöin I on erityisesti aliryhmä yhteenlaskun suhteen, joten sen täytyy olla muotoa*

$$m\mathbb{Z} = \{mn \mid n \in \mathbb{Z}\}$$

jollakin $m \in \mathbb{N}$ (esimerkki 1.23). Osoitetaan, että kääntäen, jokainen tällainen osajoukko itse asiassa onkin ideaali. Olkoon $k \in \mathbb{Z}$ mielivaltainen, ja olkoon $x = mn \in m\mathbb{Z}$. Tällöin

$$kx = xk = k(mn) = m(kn) \in m\mathbb{Z},$$

sillä kokonaislukujen kertolasku on vaihdannainen.

Tarkastelemme normaaleja aliryhmiä ja ideaaleja vielä toisesta näkökulmasta seuraavassa luvussa. Tämän luvun päätämme tarkastelemalla vielä lineaarisen kuvauksen ydintä.

Olkoon $L\colon M \to M'$ R-modulien välinen lineaarinen kuvaus. Koska modulit ovat ryhmiä yhteenlaskun suhteen, on olemassa osajoukko

$$\operatorname{Ker} L = \{x \in M \mid L(x) = 0\}.$$

Lisäksi $\operatorname{Ker} L$ on aliryhmä $+$:n suhteen. Osoitetaan, että $\operatorname{Ker} L$ on itse asiassa jopa alimoduli. Olkoon $r \in R$ ja $x \in \operatorname{Ker} L$. Tällöin

$$L(rx) = rL(x) = r \cdot 0 = 0.$$

Näin ollen $\operatorname{Ker} L$ on M:n alimoduli.

Olemme osoittaneet, että ryhmä/rengas/moduli-homomorfismin ydin on aina normaali aliryhmä/ideaali/alimoduli. Seuraavassa luvussa todistamme käänteisen väitteen - mikä tahansa normaali aliryhmä/ideaali/alimoduli on jonkun ryhmä/rengas/moduli-homomorfismin ydin.

Ytimen ja kuvan avulla voidaan myös tutkia onko morfismi isomorfismi, kuten seuraava tulos osoittaa.

Lemma 1.27. *Olkoot X ja Y ryhmät/renkaat/modulit ja olkoon $f\colon X \to Y$ morfismi. Tällöin*
(i) f on injektio jos ja vain jos $\operatorname{Ker} f = \{e\}$ *on triviaali.*
(ii) f on surjektio jos ja vain jos $\operatorname{Im} f = Y$.

Todistus jätetään harjoitustehtäväksi.

1.5 Tekijästruktuurit

Tärkeä tapa muodostaa uusia struktuureja vanhoista on niin sanottu tekijästruktuurin käsite.
Palautetaan ensin mieleen sellaiset käsitteet kuin ekvivalenssirelaatiot ja alkioiden samaistaminen.
Olkoon X joukko. X:n *relaatio* E on mikä tahansa tulon $X \times X$ osajoukko E. Näin ollen relaatio on jokin kokoelma pareja (x, y), missä $x, y \in X$. Tällöin merkitään myös xEy ja sanotaan, että x on relaatiossa y:n kanssa. Relaatio siis ilmaisee jonkinlaisen *suhteen* X:n alkioiden välillä (mistä nimitys tuleekin).
Joukossa X määritelty relaatio $\sim$ on *ekvivalenssirelaatio*, jos

(i) $\sim$ on *refleksiivinen*, eli $x \sim x$ kaikilla $x \in X$,

(ii) $\sim$ on *symmetrinen*, eli jos $x \sim y$ joillakin $x, y \in X$, niin myös $y \sim x$,

(iii) $\sim$ on *transitiivinen*, eli jos $x \sim y$ ja $y \sim z$, niin tällöin aina $x \sim z$.

Ekvivalenssirelaatioilla on vahva yhteys joukon X *osituksiin*.
Joukon X ositus on kokoelma $\mathcal{O}$ X:n **epätyhjiä** osajoukkoja, joka toteuttaa seuraavat ehdot:

$$\bigcup \mathcal{O} = X, \text{ ja} \tag{1.28}$$

$$\text{jos } A, B \in \mathcal{O} \text{ niin } A \cap B = \emptyset \text{ tai } A = B. \tag{1.29}$$

Ensimmäinen ehto siis sanoo, että jokainen X:n piste kuuluu johonkinositukseen $\mathcal{O}$ kuuluvaan joukkoon. Toinen ehto puolestaan sanoo, että osituksen joukot ovat erillisiä. Näin ollen kokoelma X:n epätyhjiä osajoukkoja $\mathcal{O}$ on X:n ositus jos ja vain jos jokainen $x \in X$ kuuluu **tasan yhteen** kokoelman joukoista.
Kuten olemme jo mainineet, ekvivalenssirelaatioiden ja ositusten välillä on olemassa yhteys.

Lemma 1.30. *Olkoon $\sim$ joukossa X määritelty ekvivalenssirelaatio. Jokaisella $x \in X$ merkitään $\bar{x} = \{y \in X \mid x \sim y\}$. Tällöin*

$$\mathcal{O}_\sim = \{\bar{x} \mid x \in X\}$$

on X:n ositus.
Kääntäen, jos $\mathcal{O}$ on X:n ositus, relaatio $\sim_\mathcal{O}$, joka määritellään ehdolla

$$x \sim_\mathcal{O} y \text{ jos ja vain jos on olemassa } A \in \mathcal{O} \text{ siten että } x, y \in A$$

on ekvivalenssirelaatio.
Vastaavuudet $\sim \mapsto \mathcal{O}_\sim$ ja $\mathcal{O} \mapsto \sim_\mathcal{O}$ ovat toistensa käänteiskuvauksia, joten ne ovat myös bijektiota.

Todistus. Tunnettua matematiikan peruskursseilta, harjoitustehtävä. □

Jos $\sim$ on ekvivalenssirelaatio, edellä määriteltyä joukkoa

$$\bar{x} = \{y \in X \mid x \sim y\}$$

sanotaan x:n *ekvivalenssiluokaksi*. Alkio x on tällöin luokkansa *edustaja*. Jokainen ekvivalenssiluokan alkio voidaan valita tämän luokan edustajaksi.

Esimerkkejä 1.31. *1) Määritellään $\mathbb{R}$:ssä relaatio E ehdolla xEy jos $xy = 1$. Tällöin E ei ole refleksiivinen, joten se ei ole ekvivalenssirelaatio.*

2) Määritellään $\mathbb{R}$:ssä relaatio $\sim$ ehdolla $x \sim y$ jos $x^2 = y^2$. Tällöin $\sim$ on ekvivalenssirelaatio. Alkion x ekvivalenssiluokka $\bar{x}$ on joukko $\{x, -x\}$. Näin ollen 0:n luokka on yksiö ja muiden alkioiden luokat kaksioita.

3) Koulumatematiikassa vektori *määritellään "suunnattuna janana" tasossa tai avaruudessa. Vektorilla on suunta ja pituus, mutta ei fiksattua alkupistettä, eli kaksi tällaista janaa pidetään "samana vektorina", jos niillä on sama pituus ja sama suunta, vaikka ne ovat janoina eri objektit. Tämä on itse asiassa oiva esimerkki ekvivalenssirelaatioiden käytöstä. Voimme siis formalisoida tällaista geometrista vektoria* ekvivalenssiluokkana*, johon kuuluvat kaikki tason tai avaruuden janat, joilla on sama suunta ja pituus.*

4) Seuraava esimerkki on erittäin tärkeä algebrassa. Olkoon $n \in \mathbb{N}$. Määritellään kokonaislukujen joukossa $\mathbb{Z}$ relaatio $\sim$ ehdolla $x \sim y$ jos ja vain jos $x - y$ on jaollinen n:llä, eli on olemassa $k \in \mathbb{N}$ siten, että

$x - y = nk$. Osoitetaan, että tämä on ekvivalenssirelaatio. Jokainen $x \in \mathbb{Z}$ on relaatiossa itsensä kanssa, sillä $x - x = 0 = n \cdot 0$ on jaollinen n:llä. Näin ollen $\sim$ on refleksiivinen.
Jos $x - y = nk$, niin $y - x = -nk = n \cdot (-k)$, joten $x \sim y$ implikoi $y \sim x$. Toisin sanoen $\sim$ on symmetrinen.
Lopuksi jos $x - y = nk$ ja $y - z = nl$, niin

$$x - z = (x - y) + (y - z) = nk + nl = n(k + l).$$

Näin ollen $\sim$ on transitiivinen. Relaatio $\sim$ on siis ekvivalenssirelaatio. Kun $n = 0$ jokaisen $x \in \mathbb{Z}$ ekvivalenssiluokka on yksiö $\{x\}$, tämä on esimerkki identtisestä *relaatiosta (alkio on relaatiossa vain itsensä kanssa). Olkoon sitten $n \geq 1$. Olkoon $x \in \mathbb{Z}$ mielivaltainen ja olkoon $l \in \{0, 1, \ldots, n - 1\}$ jakojäännös kun x jaetaan n:llä. Toisin sanoen voidaan kirjoittaa $x = nk + l$ jollakin $k \in \mathbb{Z}$. Helposti nähdään, että ekvivalenssiluokka $\bar{x}$ koostuu tasan niistä kokonaisluvuista jotka antavat n:llä jakaessaan jakojäännökseksi saman luvun l. Toisin sanoen x ja y ovat samassa ekvivalenssiluokassa jos ja vain jos niillä on sama jakojäännös n:llä jakaessaan. Tästä nähdään, että ekvivalenssiluokkia on tasan n kappaletta.*

Olkoon $\sim$ ekvivalenssirelaatio joukossa X. Määritellään *tekijäjoukko*

$$X/\sim = \{\bar{x} \mid x \in X\}.$$

Tekijäjoukon alkiot ovat siis ekvivalenssirelaatiota vastaavan osituksen alkiot. Määritellään myös kuvaus $p\colon X \to X/\sim$ kaavalla $p(x) = \bar{x}$. Tätä kuvausta sanotaan relaatioon $\sim$ liittyväksi *luonnolliseksi* tai *kanoniseksi projektioksi*. Luonnollinen projektio on aina surjektio.
Hyödyllinen tapa käsitellä ekvivalenssirelaatiota on ajatella, että relaatiossa olevat alkiot, $x \sim y$ *" samastetaan samaksi alkioksi"* eli vaikka X:ssä x ja y saattavat eri alkiot, tekijäjoukossa ne ajatellaankin samaksi alkioksi. Tämä mielikuva voidaan havainnollista erityisen helposti, kun joukko X on jokin "geometrinen" otus. Esimerkiksi olkoon X tason neliö ja ekvivalenssirelaatio X:ssä sellainen, joka samastaa pystyreunajanojen vastaavat pisteet keskenään. Voidaan ajatella että X:ssä *"liimataan"* nämä reunajanat yhteen, jolloin tekijäjoukoksi $X/\sim$ saadaan ontto putki.

Palataan nyt algebran pariin ja tutkitaan ensin yksinkertaisinta tapausta jossa joukossa X on määritelty joku laskutoimitus $\cdot$. Olkoon $\sim$ jokin joukon X ekvivalenssirelaatio. Haluamme määritellä tekijäjoukkoon $X/\sim$ kuvauksen p *indusoiman* laskutoimituksen, eli sellaisen laskutoimituksen, jonka

suhteen projektio $p\colon X \to X/\sim$ olisi yhteensopiva. Määritelmän mukaan se tarkoittaa, että pitäisi olla

$$p(xy) = p(x)p(y) \text{ eli}$$

$$\bar{x}\bar{y} = \overline{xy}. \tag{1.32}$$

Tästä nähdään, että jos vaadittu laskutoimitus on olemassa, se on yksikäsitteinen ja annettu kaavalla 1.32. Näin ollen ongelmalla on yksikäsitteinen ja myönteinen vastaus jos ja vain jos kaava 1.32 on hyvin määritelty.
Jotta kaava 1.32 olisi hyvin määritelty, oikean puolen $\overline{xy}$ täytyy olla sama riippumatta siitä mitä edustajia valitaan vasemmalla puollella. Toisin sanoen jos $\bar{x} = \bar{x'}$ ja $\bar{y} = \bar{y'}$, niin pitäisi myös olla $\overline{xy} = \overline{x'y'}$, muuten kaavassa 1.32 ei ole mitään järkeä.
Sanomme, että ekvivalenssirelaatio $\sim$ on *yhteensopiva* laskutoimituksen $\cdot$ kanssa, jos ehdoista $x \sim x', y \sim y'$ seuraa, että $xy \sim x'y'$. Yllä käydystä tarkastelusta seuraa siis, että tekijäjoukossa $X/\sim$ voidaan määritellä laskutoimitus siten, että $p\colon X \to X/\sim$ on homomorfismi jos ja vain jos $\sim$ on yhteensopiva X:n laskutoimituksen kanssa. Sanomme tällöin, että X $\sim$:n näin määritelty laskutoimitus on relaation $\sim$ *indusoima* laskutoimitus.
Tällä tavalla saatu algebrallinen struktuuri tekijäjoukossa sanotaan alkuperäisen struktuurin *tekijästruktuuriksi*.

Olkoon $\cdot$ X:n laskutoimitus ja $\sim$ X:n relaatio, joka on yhteensopiva $\sim$:n kanssa. Monet $\cdot$:n mielenkiintoiset ominaisuudet periytyvät $X/\sim$:n indusoituun laskutoimitukseen. Esimerkiksi oletetaan, että $\sim$ on liitännäinen. Tällöin kaikilla $x, y, z \in X$

$$(\bar{x}\bar{y})\bar{z} = \overline{xy}\bar{z} = \overline{(xy)z} = \overline{x(yz)} = \bar{x}\overline{yz} = \bar{x}(\bar{y}\bar{z}),$$

joten myös indusoitu laskutoimitus on liitännäinen. Samoin samastumisessa säilyvät sellaiset ominaisuudet kuin vaihdannaisuus tai osittelulaki (jos X:ssä on kaksi laskutoimitusta ja $\sim$ on yhteensopiva molempien kanssa). Samoin, jos e on neutraalialkio $\cdot$:n suhteen, sen luokka $\bar{e}$ on neutraalialkio indusoidussa laskutoimituksessa, sillä

$$\bar{e}\bar{x} = \overline{ex} = \bar{x} = \bar{x}\bar{e}.$$

Samoin nähdään, että jos x:llä on käänteisalkio, myös $\bar{x}$:llä on käänteisalkio ja

$$(\bar{x})^{-1} = \overline{x^{-1}}.$$

Näin ollen

- Jos X on (Abelin) ryhmä, $X/\sim$ on (abelin) ryhmä ja $p\colon X \to X/\sim$ on ryhmähomomorfismi. Ryhmä $X/\sim$ on X:n *tekijäryhmä*.
- Jos X on (vaihdannainen) (ykkösellinen) rengas, myös $X/\sim$ on (vaihdannainen) (ykkösellinen) rengas ja $p\colon X \to X/\sim$ on (ykkösellinen) rengashomomorfismi. Rengas $X/\sim$ on X:n *tekijärengas*.

Kaikki tämä on totta tietenkin sillä oletuksella, että $\sim$ on ekvivalenssirelaatio, joka on yhteensopiva kaikkien X:n laskutoimitusten kanssa.

Esimerkkejä 1.33. *1) Joukossa $\mathbb{Z}$ määritelty ekvivalenssirelaatio $x \sim y$ jos ja vain jos $x = \pm y$, ei ole yhteensopiva yhteenlaskun kanssa. Esimerkiksi $1 \sim -1$, $1 \sim 1$ mutta $1 + 1 = 2 \nsim 0 = 1 + (-1)$.*

2) Olkoon $n \in \mathbb{N}$ ja tarkastellaan $\mathbb{Z}$:n ekvivalenssirelaatiota $\sim_n$, jossa $x \sim_n y$ tarkoittaa, että $x - y$ on jaollinen n:llä, $x - y = nk$ jollakin $k \in \mathbb{Z}$. Tämä relaatio on yhteensopiva kokonaislukujen yhteenlaskun kanssa, sillä jos $x - x' = nk$ ja $y - y' = nl$, niin

$$(x + y) - (x' + y') = (x - x') + (y - y') = nk + nl = n(k + l).$$

Näin ollen tekijäjoukossa $\mathbb{Z}/\sim_n$, jota merkitään yleensä symbolilla $\mathbb{Z}_n$, on määritelty luonnollinen yhteenlasku, jolle pätee

$$\bar{x} + \bar{y} = \overline{x + y}.$$

Saadaan siis vaihdannainen ryhmä $(\mathbb{Z}_n, +)$, **kokonaisluvut modulo** *n. Kun $n \neq 0$, tässä ryhmässä on tasan n alkiota.*
Ekvivalenssirelaatio $\sim_n$ on yhteensopiva myös kononaislukujen kertolaskun kanssa. Todistetaan tämä. Oletetaan, että $x - x' = nk, y - y' = nl$. Tällöin

$$xy - x'y' = xy - xy' + xy' - x'y' = x(y - y') + (x - x')y' = n(lx + ky').$$

Näin ollen $\mathbb{Z}$:n kertolasku indusoi kertolaskun tekijästruktuuriin $\mathbb{Z}_n$. Koska $(\mathbb{Z}, +, \cdot)$ on vaihdannainen ykkösellinen rengas, myös $(\mathbb{Z}_n, +, \cdot)$ on vaihdannainen ykkösellinen rengas. Voidaan osoittaa, että rengas $\mathbb{Z}_n$ on kunta täsmälleen silloin, kun n on alkuluku (harjoitustehtävä).

Kuten olemme osoittaneet esimerkissä 1.31, 3) yllä, joukona $\mathbb{Z}_n$ on äärellinen joukko, jossa on tasan n alkiota, ja pätee $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

Kun olemme tekemisessä joukon $\mathbb{Z}_n$ alkioiden kanssa usein käytännössä poistamme yläviivan ja merkitään alkio $\overline{m} \in \mathbb{Z}_n$ yksinkertaisesti m:llä. Esimerkiksi kunnassa $\mathbb{Z}_2$ näillä merkinnöillä pätee

$$1 + 1 = 0.$$

Tarkastellaan seuraavaksi ulkopuolisen joukon Y laskutoimitusta joukossa X. Oletetaan siis, että X:ssä on määritelty (vasemmanpuoleinen) Y:n laskutoimitus $\cdot\colon Y \times X \to X$. Olkoon $\sim$ ekvivalenssirelaatio joukossa X. Haluamme määritellä Y laskutoimituksen tekijäjoukossa $X/\sim$ niin, että projektio $p\colon X \to X/\sim$ on yhteensopiva Y:n laskutoimitusten suhteen. Määritelmän mukaan se tarkoittaa sitä, että kaikilla $y \in Y$ ja kaikilla $x \in X$ pätee

$$p(yx) = yp(x), \text{ eli}$$

$$y\bar{x} = \bar{yx}. \tag{1.34}$$

Nähdään taas, että jos tällainen laskutoimitus joukossa $X/\sim$ on olemassa, niin se on yksikäsitteinen, ja annettu kaavalla 1.34. Lisäksi laskutoimitus voidaan määritellä sillä kaavalla, jos ja vain jos se on hyvinmääritelty, eli antaa saman lopputuloksen edustajan valinnasta riippumatta.
Päädymme siis seuraavanlaisen määritelmään - ekvivalenssirelaatio $\sim$ on *yhteensopiva* laskutoimituksen $\cdot\colon Y \times X \to X$ kanssa, jos ehdosta $x \sim x'$ seuraa, että $yx \sim yx'$ jokaisella $y \in Y$. Tällöin (ja vain tällöin) tekijäjoukossa $X/\sim$ voidaan määritellä Y:n laskutoimitus siten, että $p\colon X \to X/\sim$ on homomorfismi. Siinä tapauksessa sanomme, että joukossa $X \sim$ tällä tavalla määritelty Y:n laskutoimitus on relaation $\sim$ *indusoima* laskutoimitus.

Oletetaan, että M on R-moduli, R rengas ja oletetaan, että $\sim$ on M:n ekvivalenssirelaatio, joka on yhteensopiva sekä yhteenlaskun $+$, että skalaarikertolaskun $\cdot$ kanssa. Tällöin tekijäjoukossa $M/\sim$ voidaan määritellä sekä indusoitu yhteenlasku $+\colon M/\sim \times M/\sim \to M/\sim$, että indusoitu skalaarikertolasku $\cdot\colon R \times (M/\sim) \to M/\sim$. Helposti nähdään, että nämä laskutoimitukset määrittelevät joukossa $M/\sim$ R-modulin struktuurin (tarkista!). Kanoninen projektio $p\colon M \to M/\sim$ on tällöin R-lineaarinen kuvaus.

Algebrallisen struktuurin kanssa yhteensopivien ekvivalenssirelaatioiden ja sen alistruktuurien välillä vallitsee tärkeä yhteys, ainakin kaikissa meitä kiinnostavissa tapauksissa.

Nimittäin olkoon G *ryhmä* ja olkoon $\sim$ joukon G:n ekvivalenssirelaatio, joka on yhteensopiva G:n laskutoimituksen kanssa. Tällöin $p\colon G \to G/\sim$ on ryhmähomomorfismi, joten sillä on ydin

$$N = \operatorname{Ker} p = \{x \in G \mid p(x) = \bar{e} = p(e)\} = \{x \in G \mid x \sim e\}.$$

Näin ollen p:n ydin on yksinkertaisesti G: neutraalialkion ekvivalenssiluokka $\bar{e}$. Tästä myös nähdään, että kyseinen luokka on G:n *normaali aliryhmä* (koska homomorfismin ydin aina on). Palautetaan mieleen, että aliryhmä N on normaali, jos kaikilla $x \in G$ ja $n \in N$ pätee $xnx^{-1} \in N$. Koska $\sim$ on yhteensopiva laskutoimituksen kanssa, nähdään lisäksi, että $x \sim y$, jos ja vain jos $xy^{-1} \sim e$, eli jos ja vain jos $xy^{-1} \in N$.
Kääntäen, olkoon N jokin G:n *normaali* aliryhmä. Määritellään G:ssä relaatio $\sim$ ehdolla $x \sim y$, jos ja vain jos $xy^{-1} \in N$. Tällöin $\sim$ on ekvivalenssirelaatio (harj. tehtävä). Osoitetaan, että se on yhteensopiva laskutoimituksen kanssa. Oletetaan, että $x \sim y$, $x' \sim y'$ eli $xy^{-1} = n \in N$ ja $x'y'^{-1} = n' \in N$. Nyt

$$(xx')(yy')^{-1}) = xx'y'^{-1}y^{-1} = (xn'x^{-1})(xy^{-1}) \in N,$$

sillä N on aliryhmä, $xn'x^{-1} \in N$ normaalisuuden takia ja $xy^{-1} \in N$ oletuksen nojalla. Näin ollen $\sim$ on yhteensopiva laskutoimituksen kanssa.
Näemme siis, että ryhmän tapauksessa on olemassa yksinkertainen (bijektiivinen) vastaavuus laskutoimituksen kanssa yhteensopivien ekvivivalenssirelaatioiden ja normaalien aliryhmien välillä. Jos N on normaali aliryhmä, vastaava ekvivalenssirelaatio on määritelty ehdolla $xy^{-1} \in N$. Tällöin N on neutraalialkion ekvivalenssiluokka. Alkion $x \in G$ ekvivalenssiluokka on puolestaan xN. Tätä tekijäryhmää $G/\sim$ on tapana merkitä G/N. Normaali aliryhmä N on homomorismin $p\colon G \to G/N$ ydin. Olemme siis samalla osoittaneet viime sektiossa luvattua tulosta - jokainen normaali aliryhmä on jonkun ryhmähomomorismin ydin. Koska kääntäen väite osoitettiin viime luvussa, olemme todistaneet seuraava väite - ryhmän aliryhmä on normaali jos ja vain jos se on jonkun ryhmähomomorfismin ydin.

Jos G on *vaihdannainen* ryhmä, mikä tahansa sen aliryhmä H on normaali. Vastaava ekvivalenssirelaatio on määritelty ehdolla $x - y \in H$. Alkion $x \in G$ ekvivalenssiluokka on tällöin $x + H$. G:n jokainen aliryhmä on jonkun ryhmähomomorfismin ydin.

Olkoon R rengas ja $\sim$ R:n ekvivalenssirelaatio, joka on yhteensopiva sekä yhteen että kertolaskun suhteen. Tällöin 0:n ekvivalenssiluokka

$$I = \operatorname{Ker} p = \{x \in R \mid x \sim 0\}$$

on yllä olevan mukaan aliryhmä $+$:n suhteen (normaalisuudesta ei tarvitse olla huolissa, sillä $(R,+)$ on vaihdannainen) ja ekvivalenssirelaatio on määritelty ehdolla $x-y \in I$. Viime luvun tulosten nojalla I on itse asiassa R:n *ideaali* (sillä se on rengashomomorfismin $p\colon R \to R/\sim$ ydin). Palautetaan mieleen, että ideaali on sellainen R:n (ei välttämättä ykkösellinen) alirengas, joka toteuttaa lisäehdon

$$r \in R, x \in I \Rightarrow rx \in I \text{ ja } xr \in I.$$

Kääntäen, olkoon I renkaan R ideaali. Määritellään ekvivalenssirelaatio $x \sim y$ ehdolla $x-y \in I$. Koska I on erityisesti yhteenlaskun suhteen normaali aliryhmä, nähdään heti (edellisen kappaleen erikoistaupauksena), että $\sim$ on yhteensopiva yhteenlaskun kanssa. Osoitetaan, että se on myös yhteensopiva kertolaskun kanssa. Oletetaan, että $x \sim y, x' \sim y'$ eli $y-x = r, y'-x' = r' \in I$. Tällöin

$$yy' - xx' = yy' - yx' + yx' - xx' = y(y'-x') + (y-x)x' = yr + r'x \in I,$$

sillä I on ideaali.
Saamme siis seuraavan tuloksen - renkaan R molempien laskutoimitusten kanssa yhteensopivat ekvivalenssirelaatiot vastaavat R:n ideaaleja. Jos I on ideaali, vastaava relaatio on määritelty ehdolla $y-x \in I$. Tekijärengasta $R/\sim$ merkitään yleensä R/I.
Jokainen ideaali on jonkun rengashomomorfismin (nimittäin ainakin rengashomomorfismin $p\colon R \to R/I$) ydin.

Lopuksi tarkastellaan vielä meidän kannaltamme erittäin tärkeää modulin tapausta. Olkoon M R-moduli ja $\sim$ yhteenlaskun ja skalaarikertolaskun kanssa yhteensopiva M:n ekvivalenssirelaatio. Olkoon $p\colon M \to M/\sim$ kanoninen projektio. Tällöin 0:n ekvivalenssiluokka

$$N = \operatorname{Ker} p = \{x \in M \mid x \sim 0\}$$

on lineaarisen kuvauksen ytimenä alimoduli ja ekvivalenssirelaation voidaan yhtäpitävästi lausua ehdolla $x-y \in N$.
Kääntäen olkoon N alimoduli ja määritellään ekvivalenssirelaatio ehdolla $x-y \in N$. Tällöin relaatio on ainakin yhteenlaskun kanssa yhteensopiva. Olkoon $r \in R$ ja oletetaan, että $x-y \in N$. Koska N on alimoduli

$$rx - ry = r(x-y) \in N.$$

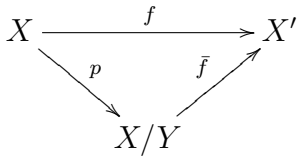
Toisin sanoen relaatio on yhteensopiva skalaarikertolaskun kanssa.
Nähdään siis, että modulien tapauksessa laskutoimitusten kanssa yhteensopivat ekvivalenssirelaatiot vastaavat alimoduleita. Jos N on M:n alimoduli,

vastaava relaatioehto on $x - y \in N$. Tekijämodulia on tapana merkitä symbolilla M/N.
Kanonisen projektion $p\colon M \to M/N$ ydin on alimoduli N. Näin ollen jokainen alimoduli on jonkun lineaarisen kuvauksen ydin.

Tekijästruktuurien tärkeimpiä sovelluksia ovat niin sanotut *isomorfialauseet* ja, yleisemmin, *hajoitelmalauseet*. Isomorfialause sanoo, että jokainen homomorfismi $f\colon X \to X'$ indusoi *isomorfismin* struktuurien $X/\operatorname{Ker} f$ ja $\operatorname{Im} f \subset X'$ välillä - kunhan X ja X' ovat tarpeeksi "säännöllisiä" algebrallisia struktuureja. Erityisesti nämä lauseet ovat voimassa kaikissa meitä kiinnostavissa tapauksissa.

Todistetaan ensin yleisempi hajotelmalause, joka on myös erittäin hyödyllinen.

Lause 1.35. *Olkoot X ja X' molemmat ryhmiä/(ykkösellisiä) renkaita/moduleja. Olkoon $f\colon X \to X'$ ryhmien/(ykkösellisten) renkaiden/modulien välinen homomorfismi.*
Olkoon $Y \subset X$ normaali aliryhmä/ideaali/alimoduli ja olkoon $p\colon X \to X/Y$ luonnollinen projektio. Tällöin on olemassa ryhmien/(ykkösellisten) renkaiden/modulien välinen homomorfismi $\bar{f}\colon X/Y \to X'$ siten, että $f = \bar{f} \circ p$,



jos ja vain jos $Y \subset \operatorname{Ker} f$. Jos $\bar{f}$ on olemassa, niin se on yksikäsitteinen ja $\operatorname{Im} \bar{f} = \operatorname{Im} f$. Erityisesti $\bar{f}$ on surjektio jos ja vain jos f on surjektio.
Lisäksi $\bar{f}$ on injektio jos ja vain jos $Y = \operatorname{Ker} f$.

Todistus. Oletetaan, että $\bar{f}$ on olemassa ja olkoon $y \in Y$. Tällöin

$$f(y) = \bar{f} \circ p(y) = \bar{f}(\bar{e}) = e',$$

missä e ja e' ovat vastaavasti X:n ja X' neutraalialkiot (nolla-alkiot rengas- ja modulitapauksessa). Näin ollen $Y \subset \operatorname{Ker} f$. Lisäksi jokaisella $x \in X$ pätee

$$\bar{f}(\bar{x}) = f(x),$$

joten $\bar{f}$ on yksikäsitteinen (jos olemassa).
Oletamme kääntäen, että $Y \subset \operatorname{Ker} f$. Määritellään $\bar{f}\colon X/Y \to X'$ kaavalla

$\bar{f}(\bar{x}) = f(x)$. Osoitetaan ensin, että $\bar{f}$ on hyvin määritelty. Olkoot $x, y \in X$ siten että $\bar{x} = \bar{y}$ eli $x^{-1}y \in Y$ ($y - x \in Y$ jos kyse on renkaasta tai modulista). Tällöin

$$f(x)^{-1}f(y) = f(x^{-1}y) = e,$$

sillä $x^{-1}y \in Y \subset \operatorname{Ker} f$. Tästä seuraa, että $f(x) = f(y)$. Olemme näyttäneet, että $\bar{f}$ on hyvin määritelty. Yhtälö $f = \bar{f} \circ p$ on selvästi voimassa. Jos $\cdot$ on jokin laskutoimitus X:ssä ja samalla symbolilla merkitsemme indusoitua laskutoimitusta X/Y:ssä, niin

$$\bar{f}(\bar{x} \cdot \bar{y}) = \bar{f}(\bar{x}\bar{y}) = \bar{f}(\bar{p}(xy)) = f(xy) = f(x)f(y) = \bar{f}(\bar{x}) \cdot \bar{f}(\bar{y}).$$

Näin ollen $\bar{f}$ on yhteensopiva jokaisen laskutomituksen kanssa. Jos kyse on moduleista, helposti nähdään samalla tavalla, että $\bar{f}$ on myös yhteensopiva skalaarikertolaskun kanssa. Jos kyse on ykkösellisistä renkaista, $\bar{f}(\bar{1}) = f(1) = 1'$, joten $\bar{f}$ on tällöin ykkösellisten renkaiden homomorfismi.
Koska p on surjektio,

$$\operatorname{Im} \bar{f} = \bar{f}(X/\operatorname{Ker} p) = \bar{f}(p(X)) = f(X) = \operatorname{Im} f.$$

Erityisesti $\bar{f}$ on surjektio tasan kun f on surjektio.
Oletetaan, että $Y \subsetneq \operatorname{Ker} f$ ja olkoon $x \in \operatorname{Ker} f$ sellainen, että $x \notin Y$. Tällöin $\bar{f}(\bar{x}) = f(x) = 0 = \bar{f}(\bar{e}) = \bar{f}(Y)$, vaikka $\bar{x} \neq Y$. Näin ollen $\bar{f}$ ei ole injektio.
Oletetaan, että $Y = \operatorname{Ker} f$. Oletetaan, että $x, y \in X$ ovat sellaiset, että

$$\bar{f}(\bar{x}) = f(x) = f(y) = \bar{f}(\bar{y}).$$

Tällöin $f(x^{-1}y) = f(x)^{-1}f(y) = e'$, joten $x^{-1}y \in \operatorname{Ker} f = Y$. Näin ollen $\bar{x} = \bar{y}$ tekijästruktuurissa X/Y. Näin ollen $\bar{f}$ on injektio. □

Isomorfialause on nyt helppo seuraus edellisestä hajotelmalauseesta.

Lause 1.36. *Olkoot X, X' kuten yllä ja $f\colon X \to Y$ vastaavien struktuurien homomorfismi. Tällöin indusoitu kuvaus $\bar{f}\colon X/\operatorname{Ker} f \to \operatorname{Im} f$, joka on määritelty ehdolla $\bar{f}(\bar{x}) = f(x)$, on vastaavien struktuurien* **isomorfismi**.

Isomorfialauseen nojalla jokainen homomorfismi siis määrittelee isomorfismin.

Esimerkki 1.37. *Olkoon C^0 kaikkien jatkuvien kuvausten $f\colon \mathbb{R} \to \mathbb{R}$ $\mathbb{R}$-vektoriavaruus ja olkoon C_1 sen aliavaruus, jonka muodostavat kaikki derivoituvat funktiot, joiden derivaatta f' on itse jatkuva kuvaus.*
Kuvaus $L\colon C^1 \to C^0$, $L(f) = f'$ on $\mathbb{R}$-lineaarinen. Tutkitaan minkä tuloksen saamme, kun sovelletaan siihen isomorfialauseetta. Ensin pitää selvittää kuvauksen ydin. Integraalilaskennan peruslauseen nojalla derivoituvan funktio

derivaatta on identtisesti nollakuvaus jos ja vain jos funktio on vakiofunktio. Merkitään W:llä kaikkien vakiokuvausten muodostamaa vektoriavaruutta, tällöin W on siis L:n ydin ja vektoriavaruutena isomorfinen $\mathbb{R}$:n kanssa. Määritelmän mukaan $f \in C^0$ kuuluu L:n kuvajoukkoon, jos on olemassa derivoituva g jolle $g' = f$. Mutta sellainenhan on olemassa jokaiselle jatkuvalle funktiolle - riittää ottaa g:ksi joku f:n integraalifunktio F (olemassa analyysin perustulosten nojalla). Näin ollen L on surjektio.
Isomorfialause nyt kertoo meille, että vektoriavaruudet C^1/W ja C^0 ovat isomorfiset.

Esimerkki 1.38. *Olkoon R ykkösellinen rengas. Tällöin erityisesti $(R, +)$ on Abelin ryhmä, joten voimme muodostaa ykkösalkion $1 \in R$ monikerrat $n \cdot 1$ jokaisella $n \in \mathbb{Z}$. Määritellään kuvaus $\phi\colon \mathbb{Z} \to R$ kaavalla $\phi(n) = n \cdot 1$. Tällöin ϕ on ykkösellisten renkkaiden homomorfismi. Tämän tarkka todistus jätetään harjoitustehtäväksi.*
Yleensä renkaan alkio $n \cdot 1$ merkitään yksinkertaisesti symbolilla n eli ikään kuin "samastetaan" kokonaisluku $n \in \mathbb{Z}$ ja vastaava "kokonaisluku" $n \in R$. Nämä renkaan kokonaisluvut käyttäytävät siis algebrallisesti samalla tavalla kuin tavalliset kokonaisluvut (koska ϕ on renkkaiden homomorfismi eli säilyttää yhteen-ja kertolaskun). Kuitenkin on tärkeätä muistaa, että kuvauksen ϕ ei tarvitse olla injektio, joten renkaassa voi käydä niin, että $n = m$ vaikka vastaavat kokonaisluvut n ja m ovatkin eri luvut. Esimerkiksi renkaassa $\mathbb{Z}_3$ pätee näillä merkinnöillä $1 = 4$.
Koska ϕ on rengashomomorfismi sen ydin $\operatorname{Ker}\phi$ *on renkaan $\mathbb{Z}$ ideaali. Näin olleen se on muotoa*

$$m\mathbb{Z} = \{n \mid n \in \mathbb{Z}\}$$

jollakin $m \in \mathbb{N}$ (esimerkki 1.26). Toisin sanoen renkaassa R tällöin $n = n'$ jos ja vain jos $n - n' \in m\mathbb{Z}$ eli $[n] = [n'] \in Z_m$!
Isomorfialauseesta seuraa, että $\operatorname{Im}\phi$ *on renkaana isomorfinen renkaan $\mathbb{Z}_m$ kanssa. Selvästi tällainen $m \in \mathbb{N}$ on tällöin yksikäsitteinen. Se sanotaan renkaan* karakteristikaksi
Jos $m = 0$, eli R:n karakteristika on 0, ϕ on injektio ja R sisältää alirenkaan, joka on isomorfinen $\mathbb{Z}$:n kanssa. Jos $m > 0$, renkaassa R pätee

$$m = \underbrace{1 + 1 + \ldots + 1}_{m \text{ kertaa}} = 0.$$

Tällöin R sisältää alirenkaan, joka on isomorfinen $\mathbb{Z}_m$:n kanssa.
Voidaan osoittaa, että kunnan (tai yleisemmin niin sanotun kokonaisalueen) karakteristika on aina joko nolla tai alkuluku.

Lukija saattaa ihmetellä, miksi emme puhuneet tekijästruktuurien/ ideaali/ hajotelma/ isomorfialauseen kohdalla ollenkaan kunnista ja niiden välisistä homomorfismeista. Syy tähän on se, että kuntahomomorfismi $f\colon K \to K'$ on **aina injektio** ja jokaisella kunnalla K on vain triviaaleja ideaaleja $\{0\}$ ja K. Tämä nähdään seuraavasti - olkoon $I \subset K$ ideaali, $I \neq \{0\}$. Tällöin on olemassa $x \in I, x \neq 0$. Koska x^{-1} on olemassa ja I on ideaali, tästä seuraa, että $1 = xx^{-1} \in I$. Mutta ideaali joka sisältää 1:n, on tunnetusti koko rengas. Näin ollen $\{0\}$ ja K ovat ainoat K:n ideaalit. Olkoon $f\colon K \to K'$ kuntahomomorfismi. Tällöin $\operatorname{Ker} f$ on ideaali, ja ei voi olla $K = \operatorname{Ker} f$ (sillä $f(1) = 1' \neq 0$), joten $\operatorname{Ker} f = \{0\}$ ja hajotelmalauseesta 1.35 seuraa tällöin, että f on injektio (valitaan $Y = \{0\}$, jolloin X/Y on olennaisesti X).
Isomorfialause 1.36 erityisesti implikoi tällöin, että jos $f\colon K \to K'$ on kuntahomomoformismi, se määrittelee isomoformismin $K \cong \operatorname{Im} f$.

Koska renkaan tekijärenkaat ovat muotoa R/I, missä I on jokin ideaali, kunnan ainoat tekijärenkaat ovat kunta K itse ja triviaalirengas $\{0\}$, joka ei edes lasketa kunnaksi. Näin ollen "tekijäkunnan " käsite on turha.

-Harjoitustehtävät:

1. Ovatko seuraavat hyvinmääriteltyjä laskutoimituksia joukossa X?
   Jos ovat, onko laskutoimitus liitännäinen? Vaihdannainen? Onko sillä neutraalialkio?
   Jos eivät ole, niin mistä se johtuu? Voidaanko tässä tapauksessa täsmentää/tiukentaa joukon X/laskutoimituksen määritelmää, niin, että siitä tulee hyvinmääritely? Onko se silloin liitännäinen, vaihdannainen, onko sillä neutraalialkio?

   a) X on kaikkien suomen kielen sanojen muodostama joukko. Laskutoimitus $\cdot\colon X \times X \to X$ määritelty seuraavasti - jos a ja b ovat sanat, tulo $a \cdot b$ on yhdyssana, joka saadaan yhdistämällä a ja b (tässä järjestyksessä). Esimerkiksi yhdys $\cdot$ sana=yhdyssana, lasku$\cdot$toimitus=laskutoimitus.

   b) Olkoon $A = \{x, y\}$. Äärellinen lauseke, joka on muodostettu kirjaimista x ja y, sanomme **aakoston A sanaksi**. Esimerkiksi x, xy, $yyxyx$ ovat kaikki aakoston A sanat. Hyväksymme sanaksi myös ns. " tyhjä sana", eli lauseke, jossa ei ole kirjamia. Olkoon X kaikkien aakoston A sanojen muodostama joukko. Määritelemme laskutoimitus $\cdot$ joukossa X sanojen katenoinnilla, eli $a \cdot b$ on sana, joka saadaan kirjoitamalla

sanan a perään sana b. Esimerkiksi $xx \cdot yx = xxyx$.

c)Olkoon X kaikkien koskaan eläneiden naispuoleisten ihmisten muodostama joukko. Määritellään laskutoimitus $\cdot$ seuraavasti. Jos X ja Y ovat naisia, niin $X \cdot Y$ on heidän viimeinen elossa ollut naispuoleinen esi-äiti (eli sellainen, että molemmat X ja Y ovat sen jälkeläisiä ja kaikista esi-äidistä kuollut viimeisenä).

d) X kaikkien kemiaalisten yhdisteiden joukko ja $x \cdot y$ - kemiaalinen yhdiste joka saadaan kun x ja y sekoitetaan ja annetaan reagoida keskenään.

2. Olkoot X ja Y joukkoja ja $f\colon X \to Y$ kuvaus.
   a) Osoita, että on olemassa $g\colon Y \to X$ siten, että $g \circ f = \mathrm{id}_X$, jos ja vain jos f on injektio.
   b) Osoita, että on olemassa $g\colon Y \to X$ siten, että $f \circ g = \mathrm{id}_Y$, jos ja vain jos f on surjektio.
   Tässä $\mathrm{id}_A\colon A \to A$ on joukon A identtinen kuvaus.

3. Olkoon $\cdot$ joukossa X määritelty liitännäinen laskutoimitus ja $x, y \in X$. Oletetaan, että laskutoimituksella on neutraalialkio ja alkiolla x ja y on olemassa käänteisalkiot. Osoita, että myös alkiolla xy on tällöin käänteisalkio ja
$$(xy)^{-1} = y^{-1}x^{-1}.$$

4. Olkoon $(X, \cdot)$ ryhmä, jossa $x^2 = x \cdot x = e$ jokaisella $x \in X$. Tässä e on X:n neutraalialkio. Osoita, että X on Abelin ryhmä. (Vihje: edellisestä tehtävästä saattaa olla hyötyä).

5. Olkoon $\cdot$ liitännäinen laskutoimitus joukossa X. Oletetaan, että
   i) X:ssä on olemassa *vasemmanpuoleinen* neutraalialkio e eli sellainen $e \in X$ jolle $ex = x$ kaikilla $x \in X$ ja
   ii) jokaisella $x \in X$ on olemassa $y \in X$ jolle $yx = e$. Osoita, että $(X, \cdot)$ on ryhmä.

6. Olkoon X joukko, jossa on laskutoimitus $\cdot$. Muotoa $ax = b$ tai $xa = b$ oleva yhtälö (missä $a, b \in X$ ja x tuntematon sanotaan *lineaariseksi*.

a) Olkoon X ryhmä. Osoita, että jokaisella lineaarisella yhtälöä on yksikäsitteinen ratkaisu.
b) Kääntäen olkoon X epätyhjä joukko, jossa on määritelty liitännäinen laskutoimitus $\cdot$. Oletetaan, että jokaisella X:n lineaarisella yhtälöllä on ainakin yksi ratkaisu joukossa X. Osoita, että $(X, \cdot)$ on itse asiassa ryhmä.

7. Olkoon $\cdot$ laskutoimitus joukossa X. Olkoon $x_1, \ldots, x_n$ mikä tahansa äärellinen *jono* X:n alkioita. Sanalla "jono" korostamme, että alkiot on varustettu indekseillä $1, \ldots, n$ eli laitettu järjestykseen. Määritelemme jonon tulon $x_1 x_2 \ldots x_n$ induktiolla siten, että kun $n = 2$ $x_1 x_2$ on sama kuin laskutoimituksen määritelemä alkioiden $x_1 x_2$ tulo ja $x_1 \ldots x_n x_{n+1}$ määritellään olevan $(x_1 \ldots x_n) \cdot x_{n+1}$. Toisin sanoen lasketaan kolmen ja enemmän alkion tulo vasemmalta oikealle yksi kerrallaan.
Olkoon $\cdot$ liitännäinen $n \geq 3$ ja $1 \leq s \leq n$. Osoita, että

$$(x_1 \ldots x_s) \cdot (x_{s+1} \ldots x_n) = x_1 \ldots x_n$$

kaikilla jonoilla $x_1, \ldots, x_n$.
Iteroimalla tämä tulos nähdään, että liitännäisen laskutoimituksen tapauksessa pitkissä tuloissa sulut voi asettaa "mihin vaan" ja lopputulos on aina sama.

8. Olkoon $\cdot$ vaihdannainen *ja liitännäinen* laskutoimitus. Olkoon $x_1, \ldots, x_n$ mielivaltainen äärellinen jono X:ssä ja olkoon $\sigma\colon \{1, \ldots, n\} \to \{1, \ldots, n\}$ **bijektio**. Osoita, että

$$x_{\sigma(1)} x_{\sigma(2)} \ldots x_{\sigma(n)} = x_1 \ldots x_n.$$

Toisin sanoen tuloa laskittaessa alkioiden järjestyksellä ei ole merkitystä.
b) Yllättäen, tämä tulos vaatii liitännäisyyden, vaihdannaisuus yksin ei riitä. Osoita tämä antamalla esimerkki vaihdannaisesta laskutoimituksessa, jossa a)-kohdan tulos ei päde jo arvolla $n = 3$.

9. Olkoon $(R, +, \cdot)$ rengas.
a) Osoita, että $(-a) \cdot b = -(ab) = a \cdot (-b)$ kaikilla $a, b \in R$.
b) Osoita, että tutut "muistikaavat"

$$a^2 - b^2 = (a - b)(a + b), \ (a + b)^2 = a^2 + 2ab + b^2$$

sen sijaan ovat voimassa kaikilla $a, b \in R$ jos ja vain jos R on kommutatiivinen rengas.

10. Olkoon K kunta. Kun $a, b \in K, b \neq 0$ määritellään "murtolauseke" $\frac{a}{b}$ kaavalla
$$\frac{a}{b} = ab^{-1} = b^{-1}a.$$
Osoita, että "koulusta tutut" kaavat
$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd},$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$
ovat voimassa.

11. Täydennän kompleksilukujen konstruuktio sektiossa 1.1. osoitamalla tarkasti määritelmistä lähtien, että se on kunta.

12. Osoita (induktiolla) potenssikaavat
$$x^n \cdot x^m = x^{n+m},$$
$$(x^n)^m = x^{nm},$$
missä $x \in X$, X:n laskutoimitus liitännäinen ja n, m sellaiset, että kaavoissa esiintyvät symbolit kaikki hyvinmääriteltyjä.

13. Olkoon $(A, +)$ Abelin ryhmä. Määritellään joukossa $P = A^A = \{f \colon A \to A\}$ laskutoimitukset $+$ ja $\cdot$ seuraavasti,
$$(f + g)(a) = f(a) + g(a),$$
$$(g \cdot f)(a) = g(f(a)).$$
Osoittaa, että $(P, +, \cdot)$ toteuttaa kaikki ykkösellisen renkaan ehdot, paitsi, että toinen osittelulaki ei päde. (jos A:ssä on vähintään kaksi alkioita).

14. Olkoon $(A, +)$ Abelin ryhmä ja $P = A^A$ kuten edellisessä tehtävässä. Tarkastellaan P:n osajoukkoa
$$Q = \mathrm{Hom}(A) = \{f \colon A \to A \mid f \text{ on ryhmähomomorfismi } \}.$$

Osoita, että Q on vakaa P:n molempien laskutoimitusten suhteen, joten algebrallinen struktuuri $(Q, +, \cdot)$ on hyvinmääritelty.
Osoita, että $(Q, +, \cdot)$ on itse asiassa ykkösellinen rengas.

15. Olkoon $(R, +, \cdot)$ rengas. Tällöin $A = (R, +)$ on Abelin ryhmä ja voimme muodostaa sen ryhmähomomorfismien renkaan $(Q, +, \cdot)$ kuten edellisessä tehtävässä.
Määritellään jokaisella $r \in R$ kuvauksen $f_r \colon R \to R$ kaavalla $f_r(a) = ra$ kaikilla $a \in R$. Osoittaa, että $f_r \in Q$ jokaisella $r \in R$ ja kuvaus $R \to Q$, $r \mapsto f_r$ on rengashomomorfismi.

16. Käännetään edellisen tehtävän asetelma. Olkoon A Abelin ryhmä ja olkoon Q sen homomorfismien muodostama rengas. Oletetaan, että $\alpha \colon (A, +) \to (Q, +)$ on jokin ryhmähomomorfismi. Määritellään A:ssä kertolasku $\cdot$ kaavalla
$$a \cdot b = \alpha(a)(b).$$
Osoita, että $(A, +, \cdot)$ toteuttaa kaikki renkaan ehdot, paitsi, että kertolasku ei vältämättä ole liitännäinen.

17. Olkoon $(R, +, \cdot)$ rengas ja olkoon $(M, +, \cdot)$ jokin R-moduli. Tällöin $A = (M, +)$ on Abelin ryhmä ja voimme muodostaa sen ryhmähomomorfismien renkaan $(Q, +, \cdot)$ kuten tehtävässä 2.
Määritellään jokaisella $r \in R$ kuvauksen $f_r \colon M \to M$ kaavalla $f_r(a) = ra$ kaikilla $a \in M$. Osoittaa, että $f_r \in Q$ jokaisella $r \in R$ ja kuvaus $R \to Q$, $r \mapsto f_r$ on rengashomomorfismi.
Onko tehtävä 15 tämän tehtävän erikoistapaus? Miksi/miksi ei?

18. Käännetään edellisen tehtävän asetelma. Olkoon $(M, +)$ Abelin ryhmä ja Q sen ryhmähomomorfismien rengas. Oletetaan, että R on rengas ja olkoon $\alpha \colon R \to Q$ jokin kuvaus. Määritellään M:ssä R-skalaarikertolasku kaavalla
$$r \cdot m = \alpha(r)(m).$$
Osoita, että $(M, +, \cdot)$ on R-moduli jos ja vain jos α on rengashomomorfismi.

19. Olkoon X joukko. Sen potenssijoukossa
$$\mathcal{P}(X) = \{A \subset X\}$$

on määritelty kaksi laskutoimitusta - kahden joukon unioni $\cup$ ja kahden joukon leikkaus $\cap$. Tutki mitä (ykkösillisen) renkaan aksioomeista toteuttaa kolmikko a) $(\mathcal{P}(X), \cup, \cap)$,
b) $(\mathcal{P}(X), \cap, \cup)$ (yhteenlasku ja kertolasku toisinpäin a)-kohdan verrattuna).

20. Jatkoa edelliseen tehtävään. Määritellään kuvaus $\mathcal{P}(X) \to \mathcal{P}(X)$ kaavalla $A \mapsto X/A$. Osoita, että tämä kuvaus on isomorfismi $(\mathcal{P}(X), \cup, \cap) \to (\mathcal{P}(X), \cap, \cup)$, eli on bijektio ja yhteensopiva vastaavien laskutoimitusten kanssa. Miten tämä kuvaus auttaisi edellisen tehtävän ratkaisussa?

21. Olkoon X joukko ja $\mathcal{P}(X)$ kuten edellisissä tehtävissä. Olkoon $x \in X$. Määritellän kuvaus $f\colon \mathcal{P}(X) \to \{0,1\}$, $f(A) = 1$ jos ja vain jos $x \in A$. Joukossa Y määritellään yhteenlasku ja kertolasku kuten reaaliluvuille, paitsi $1 + 1 = 0$. Tutki onko f laskutoimituksia säilyttävä kuvaus kun
a) $\mathcal{P}(X)$:ssä on $\bigcup$-laskutoimitus ja Y:ssä yhteenlasku,
b)$\mathcal{P}(X)$:ssä on $\bigcup$-laskutoimitus ja Y:ssä kertolasku,
c) $\mathcal{P}(X)$:ssä on $\bigcap$-laskutoimitus ja Y:ssä yhteenlasku,
d) $\mathcal{P}(X)$:ssä on $\bigcap$-laskutoimitus ja Y:ssä kertolasku.

22. 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

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

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

Osoita määritelmästä lähtien, että $(V, \oplus, \odot)$ on $\mathbb{R}$-vektoriavaruus. Mikä on nolla-vektori?

23. Osoita, että vasemmanpuoleisen ja oikeanpuoleisen M-modulin käsitteet ovat ekvivalentteja, kun R on vaihdannainen rengas. Miksi tämä ei toimi ei-vaihdannaiselle renkaalle?

24. Olkoon $(V, +, \cdot)$ $\mathbb{C}$-vektoriavaruus. Määritellään V:ssä erilainen $\mathbb{C}$-skalaarikertolasku $\odot$ kaavalla

$$(x + iy) \odot v = (x - iy) \cdot v.$$

Osoita, että $(V, +, \odot)$ on $\mathbb{C}$-vektoriavaruus.

25. Olkoon $\cdot$ liitännäinen laskutoimitus joukossa X ja oletetaan, että X:llä on neutraalialkio e tämän laskutoimituksen suhteen.
Määritellään

$$X^* = \{x \in X \mid x^{-1} \text{ on olemassa } \}.$$

Osoita, että osajoukko X^* on suljettu laskutoimituksen $\cdot$ suhteen.
Todista, että $(X^*, \cdot)$ on itse asiassa ryhmä.
Mikä on X^* kun
a) $X = \mathbb{R}$, laskutoimituksena tavallinen kertolasku.
b) $X = K$ jokin kunta, laskutoimituksena kunnan kertolasku.
c) $X = \mathbb{Z}$, laskutoimituksena tavallinen kertolasku.
d) $X = Y^Y$ jollakin joukolla Y, laskutoimituksena kuvausten yhdistäminen.

26. Olkoon R vaihdannainen rengas. Nollasta eroavaa alkiota $a \in R$ sanotaan *nollan jakajaksi* jos on olemassa $b \neq 0, b \in R$ jolla $ab = 0$. Rengas sanotaan *kokonaisalueeksi* jos mikään sen nolla-alkiosta eroava alkio ei ole nollan jakaja.
a) Osoita, että seuraavat ehdot ovat yhtäpitäviä vaihdannaiselle renkaalle R.

(i) R on kokonaisalue.

(ii) R:ssä on voimassa seuraava supistussääntö.
Olkoot $a, b, c \in R$. Tällöin jos

$$ab = ac,$$

niin joko $a = 0$ tai $b = c$.

(iii) Jokaisella $a \in R, a \neq 0$ kuvaus $f\colon R \to R$, $f(x) = ax$ on injektio.

Osoita, että jokainen kunta on kokonaisalue. Anna esimerkkejä vaihdannaisista renkaista, jotka ovat kokonaisalueita, mutta eivät ole kuntia ja vaihdannaisista renkaista jotka eivät ole kokonaisalueita.

b) Osoita, että jokainen *äärellinen* kokonaisalue on kunta, jos se on ykkösellinen renkaana (vihje: a)-kohdan ehto (iii)).

27. Olkoon $n \geq 1$ luonnollinen luku. Osoita, että seuraavat ehdot ovat yhtäpitäviä.

(i) $\mathbb{Z}_n$ on kunta.

(ii) $\mathbb{Z}_n$ on kokonaisalue.

(iii) n on alkuluku.

28. a) Edellisen tehtävän nojalla $\mathbb{Z}_7$ on kunta. Laske sen jokaisen nollasta eroavan alkion käänteisalkio (kertolaskun suhteen).
b) $\mathbb{Z}_9$ ei taas ole kunta. Laske millä sen alkioilla on käänteisalkio kertolaskun suhteen ja millä alkioilla taas ei ole.

29. Olkoon R vaihdannainen ykkösellinen rengas ja $x \in X$. Määritellään

$$I_x = \{rx \mid r \in R\}.$$

Osoita, että I_x on ideaali, $x \in I_x$ ja jos $J \subset R$ on ideaali, jolle $x \in J$, niin $I_x \subset J$. Toisin sanoen osoittaa, että I_x on sisältyvyysrelaation suhteen pienien R:n ideaali, joka sisältää x:n.
Miten I_x:n määritelmä pitää muuttaa jos tarkasteltava rengas ei ole ykkösellinen? ei ole vaihdannainen? ei ole kumpaakaan?

30. Olkoon R vaihdannainen ja ykkösellinen rengas. Osoita, että se on kunta jos ja vain jos sillä on vain triviaalit ideaalit $\{0\}$ ja R.

31. Määritellään ryhmähomomorfismi $f\colon (\mathbb{R}, +) \to (\mathbb{C}^*, \cdot)$ kaavalla

$$f(x) = (\cos x, \sin x).$$

(kts. esim. 1.9 ja 1.12). Mikä on sen kuvajoukko $\operatorname{Im} f$? Mikä on sen ydin $\operatorname{Ker} f$?
Minkälaisen tuloksen isomorfialause antaa, kun se sovelletaan tähän kuvaukseen?

32. Osoita tarkasti, että Abelin ryhmän $(\mathbb{Z}, +)$ jokainen aliryhmä on muotoa $n\mathbb{Z}$ jollakin $n \geq 0$.

33. Olkoon I renkaan R-ideaali ja olkoon M jokin R-moduli. Määritellään

$$N = \{xm \mid x \in I, m \in M\}.$$

Osoita, että N on M:n alimoduli, joten tekijämoduli M/N on olemassa ja on R-moduli.
Osoita, että M/N:ssä voidaan määritellä R/I skalaarikertolaskun kaavalla

$$(r + I)(m + N) = rm + N$$

ja M/N on R/I-moduli tällä varustettuna (ja yhteenlasku sama kuin ennen).

34. Olkoot

$$V = \{p\colon \mathbb{R} \to \mathbb{R} \text{ on polynomi } \},$$

$$W = \{p \in V \mid p(0) = 0\}.$$

Nämä ovat selvästi $\mathbb{R}$-vektoriavaruuksia. Osoita (isomorfialauseen avulla), että V/W on isomorfinen $\mathbb{R}$:n kanssa.