Algebra II

Jokke Häsä

Matematiikan ja tilastotieteen laitos, kevät 2010

Korjattu keväällä 2016

Helsingin yliopisto

Sisältö

Peruskäsitteet

0. Kertausta

Tässä luvussa kerrataan lyhyesti sellaiset peruskäsitteet ja merkinnät, joiden oletetaan olevan tuttuja aiemmalta algebran kurssilta.

0.1. Laskutoimitukset. Olkoon X joukko. Joukon X *laskutoimitus* on kuvaus $*\colon X \times X \to X$, joka liittää jokaiseen pariin (x, y) yksikäsitteisen alkion joukosta X. Tätä alkiota kutsutaan laskutoimituksen *tulokseksi* ja sitä merkitään tavalliseen tapaan $x * y$. Laskutoimituksella varustettua joukkoa voidaan ajatella parina $(X, *)$.

Joukon X laskutoimitusta $*$ kutsutaan

1) *liitännäiseksi*, jos $(x * y) * z = x * (y * z)$ kaikilla $x, y, z \in X$
2) *vaihdannaiseksi*, jos $x * y = y * x$ kaikilla $x, y \in X$.

Jos laskutoimitus toteuttaa liitännäisyysehdon, sulkeiden sijainti on merkityksetön myös pidemmissä laskulausekkeissa. (Voidaan todistaa induktiolla.) Tällöin kaikki lausekkeet voidaan kirjoittaa ilman sulkeita, ja potenssimerkintä

$$\underbrace{x * x * \cdots * x}_{n \text{ kpl}} = x^n \qquad (n \geq 1)$$

on hyvin määritelty. Toisinaan käytetään myös tulomerkintää

$$x_1 * x_2 * \cdots * x_n = \prod_{i=1}^{n} x_i.$$

Jos laskutoimitus on vaihdannainen, tulomerkinnässä ei tarvitse pitää huolta alkioiden järjestyksestä. Tällaisessa tapauksessa voidaan käyttää mitä tahansa äärellistä indeksijoukkoa I ja kirjoittaa

$$\prod_{i \in I} x_i.$$

Laskutoimituksen *neutraalialkioksi* kutsutaan sellaista alkiota e, jolle pätee

$$x * e = x \quad \text{ja} \quad e * x = x \qquad \text{kaikilla } x \in X.$$

Laskutoimituksen neutraalialkio on aina yksikäsitteinen, sillä jos e ja e' toteuttavat neutraalisuusehdon, niin

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

Jos laskutoimituksella on neutraalialkio, voidaan puhua myös *käänteisalkioista*. Alkio y on alkion x käänteisalkio, jos

$$x * y = e \quad \text{ja} \quad y * x = e,$$

missä e on laskutoimituksen neutraalialkio. Alkion x käänteisalkiota merkitään yleensä x^{-1}. Jos tällainen alkio on olemassa, sanotaan että x on *kääntyvä*. Käänteisalkiot ovat yksikäsitteisiä, mikäli laskutoimitus on liitännäinen. Tällöin nimittäin, jos y ja y' ovat molemmat x:n käänteisalkioita, saadaan

$$y = y * e = y * (x * y') = (y * x) * y' = e * y' = y',$$

eli $y = y'$.

Toisinaan puhutaan erikseen myös vasemman- ja oikeanpuoleisista neutraali- ja käänteisalkioista. Esimerkiksi kuvaus $f\colon X \to X$ on injektiivinen, jos ja vain jos se on vasemmalta kääntyvä, kun laskutoimituksena on kuvausten yhdistäminen, eli jos ja vain jos on olemassa kuvaus $g\colon X \to X$, jolle pätee $g \circ f = \mathrm{id}$. Voidaan myös näyttää, että kuvaus on surjektiivinen, jos ja vain jos sillä on oikeanpuoleinen käänteisalkio.

Neutraalialkion olemassaolo mahdollistaa nollapotenssin ja tyhjän tulon määrittelyn. Määritellään

$$x^0 = e, \qquad \text{ja} \qquad \prod_{i=n}^{m} x_i = e \quad \text{jos} \quad m < n.$$

Negatiiviset potenssit voidaan puolesta määritellä käänteisalkion avulla, jos sellainen löytyy:

$$x^{-n} = (x^{-1})^n, \quad \text{missä } n > 0.$$

(Potenssi- ja tulomerkintöjen käyttäminen vaatii tietysti laskutoimituksen liitännäisyyttä.) Näitä määritelmiä käytettäessä voidaan kaikille kokonaislukupotensseille m ja n johtaa seuraavat tutut lait:

$$x^m * x^n = x^{m+n} \quad \text{ja} \quad (x^m)^n = x^{nm}.$$

Negatiivisten potenssien tapauksessa vaaditaan tietysti alkion x kääntyvyyttä.

Tavallisesti laskutoimituksia merkitään joko *multiplikatiivisesti* kertolaskun tapaan tai *additiivisesti* yhteenlaskun tapaan. (Jälkimmäisessä tapauksessa laskutoimitus on tyypillisesti vaihdannainen.) Merkintätapoihin liittyvät tulkinnat ja nimitykset selviävät oheisesta taulukosta.

	multiplikatiivinen	additiivinen
laskutoimitus	$x \cdot y$ tai xy (tulo)	$x + y$ (summa)
potenssimerkintä	x^n	nx (monikerta)
tulomerkintä	$\prod_{i=1}^{n} x_i$	$\sum_{i=1}^{n} x_i$ (summa)
neutraalialkio	1 (ykkösalkio)	0 (nolla-alkio)
käänteisalkio	x^{-1}	$-x$ (vasta-alkio)

Yhteenlaskun yhteydessä käytetään usein myös *erotusmerkintää*

$$x - y = x + (-y).$$

Joukko X saatetaan myös varustaa useammalla kuin yhdellä laskutoimituksella. Kun yhtä laskutoimitusta merkitään multiplikatiivisesti ja toista additiivisesti, kertolaskut ajatellaan laskettaviksi ennen yhteenlaskuja. Esimerkiksi $x+y\cdot z$ tarkoittaa lauseketta $x + (y \cdot z)$. Lisäksi sanotaan, että tällaiset laskutoimitukset toteuttavat *osittelulain*, mikäli ehdot

$$x \cdot (y + z) = x \cdot y + x \cdot z \quad \text{ja} \quad (x + y) \cdot z = x \cdot z + y \cdot z$$

pätevät kaikilla $x, y, z \in X$.

0.2. Perusrakenteet. Eräs tavallisimpia algebrallisia rakenteita on ryhmä. Ryhmät kuvaavat symmetrioita, ja lisäksi vaihdannaiset ryhmät toimivat pohjana monille monimutkaisemmille rakenteille.

MÄÄRITELMÄ 0.1. Paria $(G, *)$, missä $*$ on joukon G laskutoimitus, nimitetään *ryhmäksi*, mikäli se toteuttaa seuraavat ehdot:

(G1) Laskutoimitus $*$ on liitännäinen.
(G2) Laskutoimituksella $*$ on neutraalialkio joukossa G.
(G3) Jokaisella alkiolla $x \in G$ on käänteisalkio joukossa G.

Jotta laskutoimitus olisi ylipäätään määritelty joukossa G, sen tulosten on sisällyttävä joukkoon G. Tämä on tarkistettava ennen kuin ehtoja (G1)–(G3) ryhdytään tarkastelemaan.

Ryhmässä alkioiden käänteisalkiot ovat yksikäsitteisiä, koska laskutoimitus on liitännäinen. Mikäli laskutoimitus on lisäksi vaihdannainen, rakennetta nimitetään *vaihdannaiseksi* eli *Abelin*[1] *ryhmäksi*.

Eräitä esimerkkejä ryhmistä ovat

- $(\mathbb{Z}, +)$ (vaihdannainen ryhmä)
- $(\mathbb{Q}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$ (vaihdannainen ryhmiä)
- $(\mathbb{Z}_n, +)$, jäännösluokat varustettuna yhteenlaskulla modulo n (vaihdannainen ryhmä)
- jonkin joukon kaikki bijektiot varustettuna kuvausten yhdistämisellä
- kääntyvät $n \times n$ -reaalimatriisit varustettuna matriisien kertolaskulla.

Ryhmän G alkioiden lukumäärää nimitetään ryhmän *kertaluvuksi* ja merkitään $|G|$. Ryhmän G *alkion* x *kertaluku* puolestaan määritellään seuraavasti: jos e on ryhmän G neutraalialkio ja ehto $x^n = e$ pätee jollain positiivisella kokonaisluvulla n, alkion x kertaluku on tällaisista luvuista pienin. Mikäli ehto ei päde, sanotaan kertaluvun olevan ääretön. Neutraalialkio itse on ainoa alkio, jonka kertaluku on 1. Jos alkion kertaluku on 2, alkio on oma käänteisalkionsa. Alkion kertalukua merkitään $\mathrm{ord}(x)$.

Eräs ryhmälaskutoimituksen tärkeä perusominaisuus on *supistussääntö*. Jos x, y ja z ovat ryhmän alkioita ja e on ryhmän neutraalialkio, niin voidaan päätellä

$$x * y = x * z \quad \Rightarrow \quad \underbrace{(x^{-1} * x)}_{e} * y = \underbrace{(x^{-1} * x)}_{e} * z \quad \Rightarrow \quad y = z.$$

Supistussääntöä varten tarvitaan ryhmäaksioomia. Tämän säännön avulla voidaan myös todistaa seuraava aputulos.

LEMMA 0.2. *Olkoon $(G, *)$ ryhmä. Jos $x * y = y$ pätee joillain $x, y \in G$, niin x on G:n neutraalialkio.*

Lemman kontrapositio on "jos x ei ole neutraalialkio, niin kaikilla $x, y \in G$ pätee $x * y \neq y$". Toisin sanoen ryhmässä millä tahansa neutraalialkiosta poikkeavalla alkiolla kertominen muuttaa kaikkia muita alkioita.

Rakennetta, joka toteuttaa ryhmän määritelmästä ehdot (G1) ja (G2), nimitetään *monoidiksi*. Tyypillisiä esimerkkejä monoideista ovat luonnollisten lukujen

[1] Norjalainen Niels Henrik Abel, 1802–1829, todisti vähintään viidennen asteen yleisten polynomiyhtälöiden ratkeamattomuuden.

vaihdannainen monoidi $(\mathbb{N}, +)$ (neutraalialkiona 0) sekä kaikkien jostain joukosta X itseensä määriteltyjen kuvausten joukko kuvausten yhdistämisellä varustettuna (neutraalialkiona identtinen kuvaus). Jos rakenne toteuttaa vain ehdon (G1), sitä kutsutaan *puoliryhmäksi*. Muita ryhmien kaltaisia rakenteita ovat *luupit*, jotka eivät ole välttämättä liitännäisiä, mutta joissa on neutraalialkio ja jokaisella alkiolla vasen ja oikea käänteisalkio, sekä *grupoidit*, jotka ovat kuten ryhmiä, mutta laskutoimituksen tulos ei ole välttämättä määritelty kaikille alkiopareille.

Kahden laskutoimituksen rakenteista tavallisimpia ovat renkaat ja kunnat.

MÄÄRITELMÄ 0.3. Rakennetta $(R, +, \cdot)$ kutsutaan *renkaaksi*, jos se täyttää seuraavat ehdot:

(R1) Pari $(R, +)$ muodostaa vaihdannaisen ryhmän.
(R2) Pari $(R, \cdot)$ muodostaa monoidin.
(R3) Osittelulait pätevät.

Rengasta nimitetään *vaihdannaiseksi*, mikäli kertolasku on vaihdannainen.

Renkaan kertolaskulla on siis neutraalialkio, jota kutsutaan ykkösalkioksi, ja kertolasku on liitännäinen. Käänteisalkioita kertolaskun suhteen ei kuitenkaan välttämättä löydy. Seuraavassa esimerkkejä renkaista:

- $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$
- $(\mathbb{Z}_n, +, \cdot)$ (modulaariaritmetiikka)
- $n \times n$ -reaalimatriisit
- Minkä tahansa vaihdannaisen ryhmän G endomorfismien joukko $\mathrm{End}(G)$ (homomorfismit ryhmältä G itselleen) varustettuna pisteittäisellä yhteenlaskulla: $(f + g)(x) = f(x) + g(x)$, ja kuvausten yhdistämisellä.

Osittelulaeista seuraa, että renkaassa R pätee $0 \cdot x = x \cdot 0 = 0$ kaikilla $x \in R$, sillä

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

josta yhteenlaskuryhmän $(R, +)$ supistussääntöä käyttämällä saadaan $0 = 0 \cdot x$. Yhtälö $x \cdot 0 = 0$ todistetaan samalla tavalla. Säännöistä $1 \cdot x = x$ ja $0 \cdot x = 0$ seuraa nyt, että jos $0 = 1$, niin rengas koostuu pelkästään nolla-alkiosta (ns. *nollarengas*).

Renkaan R kääntyviä alkioita kutsutaan renkaan *yksiköiksi*. Niiden joukkoa merkitään R^*, ja ne muodostavat ryhmän renkaan kertolaskun suhteen.

Olkoon jatkossa R vaihdannainen rengas, jossa $0 \neq 1$. On mahdollista, että $x \cdot y = 0$, vaikka $x \neq 0$ ja $y \neq 0$. Tällaisessa tapauksessa alkioita x ja y kutsutaan *nollanjakajiksi* tai *nollantekijöiksi*. Mikäli kuitenkin kaikilla $x, y \in R$ pätee

$$x \cdot y = 0 \qquad \Longrightarrow \qquad x = 0 \quad \text{tai} \quad y = 0,$$

vaihdannaista rengasta R nimitetään *kokonaisalueeksi*. Kokonaisalueessa ei siis ole nollanjakajia. Esimerkiksi $(\mathbb{Z}, +, \cdot)$ on kokonaisalue.

Erikoistapaus kokonaisalueesta on kunta.

MÄÄRITELMÄ 0.4. Vaihdannaista rengasta $(K, +, \cdot)$ nimitetään *kunnaksi*, jos $0 \neq 1$ ja pari $(K \setminus \{0\}, \cdot)$ on vaihdannainen ryhmä.

Vaihdannainen epätriviaali rengas on siis kunta, jos ja vain jos se sisältää kaikkien nollasta poikkeavien alkioidensa käänteisalkiot eli $K^* = K \setminus \{0\}$. Jokainen

kunta on kokonaisalue, sillä jos $xy = 0$ joillain $x, y \in K$, ja $x \neq 0$, niin

$$y = x^{-1}xy = x^{-1} \cdot 0 = 0.$$

Lisäksi jokainen äärellinen kokonaisalue on kunta. Jos nimittäin K on äärellinen kokonaisalue ja $x \in K \setminus \{0\}$, niin jokainen x:n (positiivinen) potenssi on nollasta poikkeava. Koska K on äärellinen, niin joillain $n, m \in \mathbb{N}$, $n > m \geq 1$, pätee $x^n = x^m$. Tästä saadaan

$$0 = x^n - x^m = x^m(x^{n-m} - 1).$$

Edelleen, koska K on kokonaisalue ja $x^m \neq 0$, täytyy päteä $x^{n-m} - 1 = 0$. Tällöin $1 = x^{n-m} = x^{n-m-1} \cdot x$, eli x^{n-m-1} on alkion x käänteisalkio.

Tuttuja kuntia ovat lukualueet $\mathbb{Q}$, $\mathbb{R}$ ja $\mathbb{C}$ tavallisine laskutoimituksineen.

0.3. Alirakenteet ja virittäminen. Hyvin yleisesti muotoiltuna laskutoimitusrakenteen X alirakenteella tarkoitetaan osajoukkoa $Y \subset X$, jolle pätevät seuraavat ehdot:

- Joukko Y on suljettu kaikkien X:n laskutoimitusten suhteen.
- Joukko Y sisältää kaikkien X:n laskutoimitusten neutraalialkiot.
- Jos alkiolla $x \in Y$ on joukossa X käänteisalkio x^{-1} jonkin laskutoimituksen suhteen, niin $x^{-1} \in Y$.

Nämä ehdot toteutuvat hieman eri muodoissa eri rakenteiden yhteydessä. Ehdoista seuraa, että alirakenne on aina samaa tyyppiä kuin ympäröivä rakenne: aliryhmä on aina itsekin ryhmä, alirengas on rengas jne. Käänteinen väite ei kuitenkaan päde. Esimerkiksi joillakin renkailla on osajoukkoja, jotka ovat itse renkaita, mutta eivät ympäröivän renkaan alirenkaita, koska niiden ykkösalkio on eri kuin ympäröivässä renkaassa.

MÄÄRITELMÄ 0.5. Ryhmän $(G, \cdot)$ osajoukko H on G:n *aliryhmä*, jos

(H1) H on suljettu laskutoimituksen suhteen eli $gh \in H$ kaikilla $g, h \in H$.
(H2) H sisältää ryhmän G neutraalialkion.
(H3) H sisältää kaikkien alkioidensa käänteisalkiot, eli $g^{-1} \in H$ kaikilla $g \in H$.

Tällöin merkitään $H \leq G$.

Ehtoa (H2) ei tarvitse erikseen tarkistaa, jos muut ehdot ovat voimassa ja H on epätyhjä. Tällöin nimittäin löytyy jokin $g \in H$, ja ehdoista (H3) ja (H1) seuraa, että $g^{-1} \in H$ ja $e = g \cdot g^{-1} \in H$. Myös ensimmäinen ja viimeinen ehto voidaan yhdistää, jolloin saadaan seuraava toisinaan kätevä tulos.

LAUSE 0.6 (Aliryhmäkriteeri). *Ryhmän G osajoukko H on G:n aliryhmä, jos ja vain jos*

(1) $H \neq \emptyset$
(2) $gh^{-1} \in H$ kaikilla $g, h \in H$.

Myös seuraava tulos on kätevä monissa tilanteissa.

LAUSE 0.7. *Ryhmän G osajoukko H on G:n aliryhmä, jos ja vain jos se on ryhmä.*

Lause ei seuraa suoraan aliryhmän määritelmästä, sillä ryhmällä H voisi periaatteessa olla esimerkiksi eri neutraalialkio kuin ryhmällä G. Voisi siis päteä

$e'g = g$ kaikilla $g \in H$, vaikka e' ei olisikaan koko ryhmän G neutraalialkio. Lemman 0.2 nojalla tämä on kuitenkin mahdotonta. Tulos seuraa tästä sekä ryhmän G käänteisalkioiden yksikäsitteisyydestä.

Alkioon g liittyvät aliryhmän H vasen ja oikea *sivuluokka* määritellään joukkoina

$$gH = \{gh \mid h \in H\} \quad \text{ja} \quad Hg = \{hg \mid h \in H\}.$$

Voidaan osoittaa, että kaikki tietyn aliryhmän vasemmat (tai yhtä hyvin oikeat) sivuluokat muodostavat koko ryhmän osituksen. Lisäksi, jos aliryhmä on äärellinen, kaikki sivuluokat ovat samankokoisia.[1] Tästä seuraa ryhmäteorian kenties tärkein tulos.

LAUSE 0.8 (Lagrange[2]). *Olkoon G äärellinen ryhmä ja H sen aliryhmä. Tällöin G:n alkioiden lukumäärä on jaollinen aliryhmän H alkioiden lukumäärällä.*

Aliryhmän sivuluokkien lukumäärää nimitetään aliryhmän *indeksiksi* ja merkitään $[G : H]$. Indeksin avulla Lagrangen lause voidaan esittää myös hieman täsmällisemmässä muodossa: $[G : H] = |G|/|H|$.

Mikä tahansa rakenteen X osajoukko S ei ole välttämättä alirakenne, mutta se voidaan aina täydentää alirakenteeksi lisäämällä siihen sopivasti alkioita. Pienintä alirakennetta, joka sisältää joukon S, nimitetään *S:n virittämäksi* alirakenteeksi ja merkitään $\langle S \rangle$. Voidaan osoittaa, että $\langle S \rangle$ on kaikkien niiden alirakenteiden leikkaus, jotka sisältävät joukon S.

Esimerkiksi ryhmän G osajoukon S virittämä aliryhmä löydetään lisäämällä S:ään tarvittaessa G:n neutraalialkio, kaikki mahdolliset S:n alkioista muodostettavat tulot sekä kaikki S:n alkioiden käänteisalkiot. Tiivistäen tämä voidaan kirjoittaa muotoon

$$\langle S \rangle = \{x_1 x_2 \cdots x_k \mid k \in \mathbb{N},\ x_i \in S \text{ tai } x_i^{-1} \in S \text{ kaikilla } i \leq k\}.$$

Äärellisen joukon $S = \{x_1, \ldots, x_n\}$ virittämää aliryhmää voidaan merkitä yksinkertaisesti $\langle x_1, \ldots, x_n \rangle$.

Jos $G = \langle x \rangle$ jollain $x \in G$, eli koko ryhmä on yhden alkionsa virittämä, ryhmää kutsutaan *sykliseksi*. Sykliset ryhmät ovat vaihdannaisia ja niiden rakenne on muutenkin hyvin yksinkertainen. Äärellinen syklinen ryhmä voidaan kirjoittaa muodossa

$$\langle x \rangle = \{e, x, x^2, \ldots, x^{n-1}\},$$

missä e on neutraalialkio ja n alkion x kertaluku. Ääretön syklinen ryhmä on puolestaan muotoa

$$\langle x \rangle = \{\ldots, x^{-2}, x^{-1}, e, x, x^2, \ldots\}.$$

Ryhmän $\langle x \rangle$ kertaluku on siis molemmissa tapauksissa sama kuin alkion x kertaluku. Syklisen ryhmän kaikki aliryhmät ovat myös syklisiä.

Toisinaan käytetään hieman vapaamuotoista merkintää $G = C_n$, kun halutaan sanoa, että G on syklinen ryhmä, jonka kertaluku on n (voi olla myös ääretön). Esimerkiksi $\mathbb{Z}_3 = C_3$ ja $\mathbb{Z} = C_\infty$.

---

[1] Myös äärettömän aliryhmän sivuluokat ovat yhtä mahtavia.

[2] Joseph-Louis Lagrange (1736–1813) ei todistanut nimeään kantavaa lausetta, mutta käytti joitain sen erityistapauksia polynomiyhtälöitä koskevassa tutkimuksessaan.

0.4. Tulorakenteet. Useimmista algebrallisista rakenteista voidaan muodostaa tulorakenteita karteesisen tulon avulla. Esimerkiksi kahden ryhmän $(G, *)$ ja $(H, \circ)$ *tuloryhmä* on joukko

$$G \times H = \{(g, h) \mid g \in G, h \in H\},$$

jonka laskutoimitus määritellään pisteittäin:

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 * g_2, h_1 \circ h_2).$$

Samalla tavoin voidaan määritellä kahden renkaan R ja S *tulorengas* $R \times S$. Myös useamman, jopa äärettömän monen rakenteen tulo on mahdollinen.

Jos rakenteissa on neutraalialkioina e_1 ja e_2, tulorakenteen neutraalialkio on (e_1, e_2). Samaten käänteisalkioille, mikäli tällaisia on, pätee

$$(g, h)^{-1} = (g^{-1}, h^{-1}).$$

Edelleen, jos Y_1 ja Y_2 ovat rakenteiden X_1 ja X_2 alirakenteita, niin $Y_1 \times Y_2$ on tulorakenteen $X_1 \times X_2$ alirakenne. Tulorakenteella voi kuitenkin olla myös sellaisia alirakenteita, jotka eivät itse ole tulomuotoa; esimerkiksi joukko

$$\{(n, n) \mid n \in \mathbb{Z}\}$$

on tulorenkaan $\mathbb{Z} \times \mathbb{Z}$ alirengas, vaikka se ei ole muotoa $A \times B$ millään $\mathbb{Z}$:n alirenkailla A ja B.

Kahden kunnan karteesinen tulo ei kuitenkaan ole kunta pisteittäisten laskutoimitusten suhteen. Tämän näkee esimerkiksi siitä, että alkiolla $(1, 0)$ ei ole käänteisalkiota, vaikka kunnan määritelmän mukaan kaikilla nolla-alkiosta $(0, 0)$ poikkeavilla alkioilla pitäisi olla käänteisalkio.

0.5. Homomorfismit. Samantyyppisiä algebrallisia rakenteita voidaan verrata toisiinsa *homomorfismien* avulla. Kuvausta f struktuurista $(X, *)$ struktuuriin $(Y, \circ)$ kutsutaan homomorfismiksi, jos seuraavat ehdot pätevät:

(HM1) $f(x * y) = f(x) \circ f(y)$ kaikilla $x, y \in X$.

(HM2) Jos laskutoimituksella $*$ on neutraalialkio e_X, niin $f(e_X) = e_Y$, missä e_Y on laskutoimituksen $\circ$ neutraalialkio.

Ehdot siis takaavat, että kuvaus säilyttää laskutoimitusten tulokset sekä neutraalialkiot. Jos laskutoimituksia on kaksi tai useampia, ehtojen tulee päteä kunkin laskutoimituksen osalta.

Homomorfismi $f\colon (X, *) \to (Y, \circ)$ kuvaa mahdolliset käänteisalkiot käänteisalkioiksi. Tämä seuraa yhtälöketjuista

$$f(x) \circ f(x^{-1}) = f(x * x^{-1}) = f(e_X) = e_Y$$
$$\text{ja} \quad f(x^{-1}) \circ f(x) = f(x^{-1} * x) = f(e_X) = e_Y,$$

joiden perusteella $f(x)^{-1} = f(x^{-1})$. Induktiolla voidaan lisäksi todistaa, että

$$f(x^n) = f(x)^n$$

pätee kaikilla kokonaisluvuilla n.

Homomorfismien merkitys on siinä, että ne säilyttävät algebralliset ominaisuudet. Esimerkiksi alirakenteen kuva homomorfismissa on vastaavanlainen alirakenne maalirakenteessa. Myös liitännäisyys-, vaihdannaisuus- ja ositteluominaisuudet säilyvät. Erityisesimerkki homomorfismista on bijektiivinen eli kääntyvä homomorfismi, jota nimitetään *isomorfismiksi*. Se kuvaa rakenteet toisikseen säilyttäen

algebralliset ominaisuudet molempiin suuntiin, jolloin nämä ns. *isomorfiset rakenteet* ovat täysin samankaltaiset toistensa kanssa, alkioiden ja laskutoimitusten nimeämistä vaille identtiset.

Ryhmien tapauksessa myös homomorfismin kohdalla saadaan muutamia yksinkertaistuksia. Ensinnäkin ryhmien välisen kuvauksen $f\colon (G,*) \to (H,\circ)$ tapauksessa jälkimmäistä homomorfiaehtoa (HM2) ei tarvitse erikseen tarkastella, sillä ensimmäisestä ehdosta seuraa

$$f(e_G) = f(e_G * e_G) = f(e_G) \circ f(e_G),$$

josta ryhmän H supistussäännön avulla tulee $e_H = f(e_G)$.

Toinen seikka liittyy ryhmähomomorfismin *ytimeen*

$$\operatorname{Ker} f = \{x \in G \mid f(x) = e_H\}.$$

Ydin sisältää aina vähintään neutraalialkion e_G, mutta se voi sisältää muitakin alkioita. Itse asiassa voidaan osoittaa, että kuvaus f on injektiivinen, jos ja vain jos $\operatorname{Ker} f = \{e_G\}$. Kyseinen ehto seuraa injektiivisyydestä, koska $f(e_G) = e_H$. Toinen suunta nähdään seuraavasti. Oletetaan, että $f(x) = f(y)$ joillain $x, y \in G$. Tällöin

$$e_H = f(x) \circ f(y)^{-1} = f(x * y^{-1}),$$

joten $x * y^{-1}$ on ytimessä $\operatorname{Ker} f$. Jos ydin sisältää vain neutraalialkion e_G, niin $x * y^{-1} = e_G$, ja edelleen $x = y$. Tämä todistaa injektiivisyyden.

Ryhmähomomorfismia koskien voidaan tässä yhteydessä mainita seuraava helposti muistettava sääntö.

LAUSE 0.9. *Ryhmähomomorfismi $f\colon G \to H$ on*

- *injektiivinen, jos ja vain jos* $\operatorname{Ker} f = \{e_G\}$
- *surjektiivinen, jos ja vain jos* $\operatorname{Im} f = H$.

Rengashomomorfismin $f\colon R \to S$ ydin määritellään nolla-alkion alkukuvana:

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

Rengashomomorfismin ydin on siis sama kuin renkaan yhteenlaskuryhmään liittyvän vastaavan ryhmähomomorfismin ydin. Tästä seuraa, että myös rengashomomorfismi on injektiivinen, jos ja vain jos sen ydin on yksiö.

Kunnat koostuvat kahdesta vaihdannaisesta ryhmästä, ja tämä mahdollistaa vielä erään yksinkertaistuksen.

LAUSE 0.10. *Jokainen kuntahomomorfismi $f\colon K \to L$ on injektiivinen.*

Tulos seuraa siitä, että rengashomomorfismin ydin on aina *ideaali* (tähän palataan myöhemmin) ja millä tahansa kunnalla K on vain triviaalit ideaalit $\{0_K\}$ ja K. Vaihtoehto $\operatorname{Ker} f = K$ ei tule kysymykseen, koska $f(1_K) = 1_L \neq 0_L$. Siispä $\operatorname{Ker} f = \{0_K\}$, mistä seuraa, että f on injektiivinen.

0.6. Polynomit. Olkoon R rengas. Yhden tuntemattoman R-kertoimiseksi polynomiksi kutsutaan äärellistä muodollista summaa

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0,$$

missä alkiot $a_0, \ldots, a_n$ kuuluvat renkaaseen R ja X on pelkkä symboli. Näitä alkioita kutsutaan polynomin *kertoimiksi* ja symbolia X *tuntemattomaksi* tai *muuttujaksi*. Polynomin *aste* $\deg(f)$ on suurin sellainen n, jolla kerroin a_n on nollasta poikkeava. Nollapolynomin 0 astetta ei määritellä, tai sen voidaan ajatella

olevan $-\infty$. Kaikkien R-kertoimisten yhden tuntemattoman polynomien joukkoa merkitään $R[X]$. Tämä joukko on rengas polynomien tavallisen yhteen- ja kertolaskun suhteen. Astetta nolla olevat polynomit voidaan yhdessä nollapolynomin kanssa samastaa kerroinrenkaaseen R, ja näitä kutsutaan $R[X]$ *vakiopolynomeiksi*.

Jos kerroinjoukkona on kunta, polynomeille pätee erittäin käyttökelpoinen jakoyhtälö. (Todistetaan myöhemmin luvussa 6.4.)

LAUSE 0.11 (Polynomien jakoyhtälö). *Olkoon K kunta, ja olkoot f ja g kaksi K-kertoimista polynomia. Oletetaan, että $g \neq 0$. Tällöin löytyy yksikäsitteiset $q, r \in K[X]$, joille pätee $f = qg + r$ ja $\deg(r) < \deg(g)$.*

Voidaan myös määritellä useamman kuin yhden tuntemattoman polynomeja. Tuntemattomien $X_1, \ldots, X_k$ polynomi on muodollinen summa

$$f = \sum_{i=0}^{m} a_i \overline{X}_i,$$

missä kukin $\overline{X}_i$ on muotoa $X_1^{n_1} X_2^{n_2} \cdots X_k^{n_k}$ oleva *monomi*. Monomissa tuntemattomien X_i kirjoitusjärjestyksellä ei ole väliä: tuntemattomien ajatellaan olevan keskenään vaihdannaisia. Kaikkien R-kertoimisten k:n tuntemattoman polynomien joukkoa merkitään symbolilla $R[X_1, \ldots, X_k]$. Usein tuntemattomia merkitään myös muilla kirjaimilla, kuten Y ja Z.

Monomin $X_1^{n_1} X_2^{n_2} \cdots X_k^{n_k}$ *aste* on monomissa esiintyvien eksponenttien summa $n_1 + n_2 + \cdots + n_k$, ja polynomin aste on suurin siinä esiintyvän monomin aste. Esimerkiksi $XY + 3Z - 2XZ^2 + 10$ on joukon $\mathbb{Z}[X, Y, Z]$ polynomi, jonka aste on monomin XZ^2 aste eli kolme.

1. Tekijärakenteet

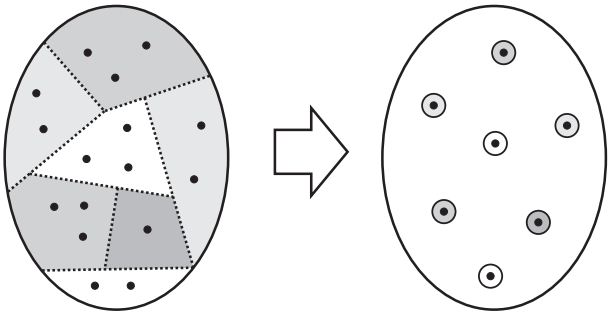
Tekijärakenteita esiintyy joka puolella algebraa, ja tekijäryhmät ja -renkaat ovatkin tuttuja aiemmilta algebran kursseilta. Tässä luvussa kerrataan niihin liittyvät perustulokset ja tarkastellaan samalla tekijärakenteita hieman yleisemmältä kannalta. Tekijärakenteen idean ymmärtäminen on avain monien algebrallisten konstruktioiden ja päättelyketjujen ymmärtämiseen.

Tekijärakenteita voidaan soveltaa eri tarkoituksiin ja niitä voidaan tarkastella erilaisista näkökulmista, vaikka kyseessä onkin aina täsmälleen sama konstruktio. Tekijärakenteiden avulla voidaan muun muassa yksinkertaistaa tilanteita jättämällä tarpeettomia yksityiskohtia huomiotta tai konstruoida uusia rakenteita, jotka toteuttavat jotkin halutut ehdot. Seuraavassa on esimerkkejä näistä käyttötavoista.

- Olkoon n kokonaisluku. Jäännösluokkarengas $\mathbb{Z}_n$ on kokonaislukujen renkaan $\mathbb{Z}$ tekijärengas, jonka alkioita ovat jäännösluokat $[a] = a+n\mathbb{Z}$. Jäännösluokat yksinkertaistavat laskuja, jos ollaan kiinnostuttu vain lukujen jakojäännöksistä. Esimerkiksi jos $n = 3$, voidaan laskea
$$[8^{999}] = [-1]^{999} = [-1] = [2].$$
Luvulla 8^{999} on siis kolmella jaettaessa jakojäännöksenä 2.
- Neliön symmetriaryhmään D_4 kuuluu neljä kiertoa ja neljä peilausta. Kierrot muodostavat normaalin aliryhmän N. Jos σ on mikä tahansa peilaus, tekijäryhmä D_4/N sisältää kaksi alkiota: N ja σN. Kaikki peilaukset sisältyvät sivuluokkaan σN. Kahden alkion ryhmän laskutoimitus on aina samanlainen, joten tiedetään, että $(\sigma N)^2 = N$. Tämä voidaan tulkita siten, että kahden peilauksen tulo on aina kierto.
- Kuvitellaan, että halutaan rengas, joka sisältää neliöjuuren luvulle 2 (tulkittuna ykkösalkion monikertana), mutta jossa yhtälö $3\sqrt{2} = 1$ pätee. Lähdetään liikkeelle reaalilukujen alirenkaasta
$$R = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}.$$
Vaadittu yhtälö voidaan kirjoittaa muodossa $3\sqrt{2} - 1 = 0$. Renkaan ideaali vastaa tekijärenkaassa nolla-alkiota, joten pyritään saamaan aikaan ideaali, joka sisältäisi alkion $3\sqrt{2} - 1$. Yksinkertaisinta on käyttää kyseisen alkion virittämää ideaalia $I = \langle 3\sqrt{2} - 1\rangle$. Nyt tekijärenkaassa R/I pätee $(\sqrt{2}+I)^2 = ((\sqrt{2})^2)+I = 2+I$, joten sivuluokka $\sqrt{2}+I$ on alkion $2 + I$ neliöjuuri. Toisaalta
$$3(\sqrt{2} + I) = (3\sqrt{2} - 1) + I) + (1 + I) = I + (1 + I) = 1 + I,$$
joten vaadittu yhtälö pätee.

1.1. Ekvivalenssirelaatiot. Tekijärakenteen taustalla on aina *ositus*. Ositus jakaa rakenteen X erillisiin epätyhjiin osiin, jotka yhdessä sisältävät kaikki alkuperäisen rakenteen X alkiot. Tekijärakenteen alkioina toimivat sitten nämä osat, ja jokaisen yksittäisen osan sisältämä rakenne jätetään tekijärakenteessa huomiotta.

Toinen tapa ymmärtää tekijärakennetta on, että ajatellaan *samastettavaksi* samaan osaan sisältyvät alkiot. Tällöin niiden väliset erot ikään kuin tahallisesti unohdetaan. Tällä tavalla ajattelemalla päädytään ekvivalenssin käsitteeseen.



KUVA 1. Tekijärakenteessa samaan osaan kuuluvat alkiot samastetaan.

Jos R on jokin kaksipaikkainen relaatio, niin merkintä xRy tarkoittaa, että x on relaatiossa alkion y kanssa.[1]

MÄÄRITELMÄ 1.1. Kaksipaikkainen relaatio $\sim$ joukossa X on *ekvivalenssirelaatio*, jos se toteuttaa seuraavat ehdot kaikilla alkioilla $x, y, z \in X$:

(E1) Relaatio $\sim$ on *refleksiivinen*, eli $x \sim x$.
(E2) Relaatio R on *symmetrinen*, eli jos $x \sim y$, niin $y \sim x$.
(E3) Relaatio R on *transitiivinen*, eli jos $x \sim y$ ja $y \sim z$, niin $x \sim z$.

Olkoon $\sim$ jokin ekvivalenssirelaatio joukossa X. Alkion $x \in X$ sanotaan olevan *ekvivalentti* alkion $y \in X$ kanssa, jos $x \sim y$. Alkion x *ekvivalenssiluokaksi relaation* $\sim$ *suhteen* nimitetään joukkoa, joka sisältää kaikki x:n kanssa ekvivalentit alkiot:

$$[x]_\sim = \{y \in X \mid x \sim y\}.$$

Ekvivalenssiluokkaa voidaan merkitä myös $[x]$ tai $\overline{x}$, jos relaatio on asiayhteydestä selvä. Alkiota x nimitetään ekvivalenssiluokkansa *edustajaksi*. Kaksi ekvivalenssiluokkaa $[x]$ ja $[y]$ ovat samat, jos ja vain jos x on ekvivalentti y:n kanssa. Tällöin sekä x että y ovat saman ekvivalenssiluokan edustajia.

Relaation $\sim$ kaikkien ekvivalenssiluokkien joukkoa merkitään $X/\sim$. Ekvivalenssiluokat muodostavat joukon X osituksen. Kääntäen jokainen ositus määrittelee ekvivalenssirelaation, jossa samaan osaan kuuluvat alkiot ovat keskenään ekvivalentteja.

Olkoon nyt $(X, *)$ jokin algebrallinen rakenne, jonka tekijärakenne halutaan muodostaa. Ideana on valita sopiva ekvivalenssirelaatio $\sim$ samastamaan sellaiset alkiot, joiden eroja ei haluta huomioida. Näin saatavaan ositukseen $X/\sim$ määritellään sitten uusi laskutoimitus $\circledast$, joka vastaa luonnollisella tavalla alkuperäistä laskutoimitusta:

$$[x] \circledast [y] = [x * y] \quad \text{kaikilla } x, y \in X.$$

Tässä määritelmässä on eräs ongelma. Laskutoimituksen $\circledast$ täytyisi liittää jokaiseen pariin $([x], [y])$ yksikäsitteinen kolmas alkio $[x] \circledast [y]$. Kaavan antama tulos $[x * y]$ riippuu kuitenkin joukon X alkioista x ja y. Kukin ekvivalenssiluokka voi sisältää monia eri alkioita $x_1, x_2, x_3, \ldots$, ja tällöin $[x_1] = [x_2] = [x_3]$, jne. Jotta laskutoimituksen $[x] \circledast [y]$ tulos olisi yksikäsitteinen, on siis pidettävä huoli siitä, että

[1] Tarkasti määriteltynä kaksipaikkainen relaatio R tarkoittaa osajoukkoa järjestettyjen parien joukossa $X \times X$. Alkio x on relaatiossa alkion y kanssa, mikäli $(x, y) \in R$.

se ei riipu joukon X alkioista vaan ainoastaan niiden edustamista luokista. (Toisinaan sanotaan, että tällöin kaavan antama laskutoimitus on ”hyvin määritelty”.) Tämä on seuraavan määritelmän perusta.

MÄÄRITELMÄ 1.2. Olkoon X joukko, jossa on määritelty laskutoimitus $*$ sekä ekvivalenssirelaatio $\sim$. Jos kaikilla $x, x', y, y' \in X$ pätee

$$x \sim x' \quad \text{ja} \quad y \sim y' \qquad \Rightarrow \qquad x * y \sim x' * y',$$

sanotaan, että laskutoimitus $*$ on *yhteensopiva* relaation $\sim$ kanssa.

Yhteensopivuus takaa sen, että tekijärakenteessa voidaan määritellä alkuperäistä laskutoimitusta vastaava laskutoimitus.

LAUSE 1.3 (Tekijärakenteen määritelmä). *Olkoon $*$ laskutoimitus joukossa X, ja olkoon $\sim$ laskutoimituksen $*$ kanssa yhteensopiva ekvivalenssirelaatio. Tällöin on olemassa joukon $X/\!\sim$ laskutoimitus $\circledast$, jolle pätee*

$$[x] \circledast [y] = [x * y]$$

kaikilla $x, y \in X$.

TODISTUS. Jotta lauseessa annettu kaava määrittelisi laskutoimituksen $\circledast$ tuloksen yksikäsitteisesti, täytyy ekvivalenssiluokan $[x' * y']$ olla sama aina, kun $x' \in [x]$ ja $y' \in [y]$. Olkoot siis $x', y' \in X$ sellaisia, että $x' \sim x$ ja $y' \sim y$. Koska laskutoimitus $*$ on yhteensopiva ekvivalenssirelaation kanssa, pätee $x * y \sim x' * y'$. Tällöin

$$[x * y] = [x' * y'],$$

eli laskutoimituksen $\circledast$ tulos ei riipu luokkien $[x]$ ja $[y]$ edustajien valinnasta, vaan on aina sama luokka $[x * y]$. □

Yleensä tekijärakenteen laskutoimitusta merkitään samalla symbolilla kuin alkuperäisen rakenteen laskutoimitusta. Mikäli laskutoimituksella on rakenteessa X neutraalialkio e, sen ekvivalenssiluokka $[e]$ toimii neutraalialkiona tekijärakenteessa. Tämä nähdään siitä, että $[e] * [x] = [e * x] = [x]$ kaikilla $x \in X$. Samaten alkuperäisen rakenteen käänteisalkioiden luokista tulee käänteisalkioita tekijärakenteessa, eli $[x^{-1}] = [x]^{-1}$, jos $x \in X$ on kääntyvä.

ESIMERKKI 1.4. Tarkastellaan monoidin $(\mathbb{N}, +)$ ositusta parillisiin ja parittomiin lukuihin. Tätä ositusta vastaa ekvivalenssirelaatio

$$n \sim n' \iff n + n' = 2k \quad \text{jollain } k \in \mathbb{N}.$$

Relaatio $\sim$ on yhteensopiva yhteenlaskun kanssa, sillä jos pätee $m + m' = 2k$ ja $n + n' = 2l$, niin

$$(m + n) + (m' + n') = 2k + 2l = 2(k + l) \quad \text{ja} \quad k + l \in \mathbb{N}.$$

Nyt voidaan määritellä laskutoimitus $[m] + [n] = [m + n]$, missä tulos riippuu vain siitä, ovatko m ja n parillisia vai parittomia. Neutraalialkiona toimii $[0]$ eli parillisten lukujen luokka, minkä voi tulkita niin, että parillisen luvun lisääminen säilyttää parillisuuden ja parittomuuden. Saatu kaksialkioinen tekijämonoidi on itse asiassa ryhmä, sillä toinen ekvivalenssiluokka $[1]$ on oma vasta-alkionsa.

Voitaisiin myös tarkastella luonnollisten lukujen monoidin jakoa osiin $\{0, 1, 2\}$ (*pienet* luvut) ja $\{3, 4, 5, \dots\}$ (*suuret* luvut). Tätä ositusta kuvaavassa relaatiossa kaksi alkiota ovat ekvivalentteja, jos molemmat ovat pieniä tai molemmat suuria.

Ekvivalenssirelaatio ei kuitenkaan ole yhteensopiva laskutoimituksen kanssa, sillä kahden pienen luvun summa voi olla joko pieni (esim. $1+1=2$) tai suuri (esim. $2+2=3$). Näin ollen luokkien ”pienet” ja ”suuret” yhteenlaskua ei voida määritellä.

1.2. Tekijäryhmät ja tekijärenkaat. Olkoon G multiplikatiivinen ryhmä. Seuraavat määritelmät ja tulokset ovat tuttuja aiemmilta algebran kursseilta.

MÄÄRITELMÄ 1.5. Aliryhmää $H \leq G$ kutsutaan *normaaliksi*, jos sen vasemmat ja oikeat sivuluokat ovat samat, eli $gH = Hg$ kaikilla $g \in G$. Jos H on G:n normaali aliryhmä, merkitään $H \trianglelefteq G$.

LAUSE 1.6 (Normaalisuuskriteeri). *Aliryhmä H on normaali ryhmässä G, jos ja vain jos kaikilla $g \in G$ pätee $gHg^{-1} \subset H$ eli*

$$ghg^{-1} \in H \quad \textit{jokaisella } h \in H.$$

Minkä hyvänsä aliryhmän sivuluokat muodostavat aina koko ryhmän osituksen. Jokaista aliryhmää vastaa siis ekvivalenssirelaatio, jossa alkiot ovat ekvivalentteja täsmälleen silloin, kun ne kuuluvat samaan sivuluokkaan. Koska sivuluokat eivät leikkaa toisiaan ja $x \in xH$ pätee kaikilla x, nähdään, että $xH = x'H$ pätee, jos ja vain jos $x' \in xH$. Tämä puolestaan on yhtäpitävää sen kanssa, että $x^{-1}x' \in H$.

LAUSE 1.7. *Oletetaan, että $N \trianglelefteq G$. Tällöin ekvivalenssirelaatio*

$$x \sim x' \iff x^{-1}x' \in N$$

on yhteensopiva ryhmän G laskutoimituksen kanssa.

Normaalin aliryhmän N suhteen voidaan siis muodostaa tekijäryhmä, jossa samastetaan samaan sivuluokkaan kuuluvat alkiot. Tätä tekijäryhmää merkitään G/N.

Kun tekijäryhmät määritellään normaalin aliryhmän avulla, herää kysymys, voisiko ryhmälle muodostaa tekijärakenteen myös jollakin muulla tavalla. Vastaus on kielteinen, eli ryhmän kukin tekijärakenne saadaan aina jostakin normaalista aliryhmästä.

LAUSE 1.8. *Oletetaan, että $\sim$ on ryhmässä G määritelty, laskutoimituksen kanssa yhteensopiva ekvivalenssirelaatio. Tällöin neutraalialkion luokka $[e]$ on normaali aliryhmä G:ssä, ja kaikilla $g, g' \in G$ pätee $g \sim g'$, jos ja vain jos $g^{-1}g' \in [e]$.*

TODISTUS. Merkitään $N = [e]$ ja osoitetaan ensin, että N on aliryhmä. Ensinnäkin $e \in N$. Olkoot $g, h \in N$. Tällöin $g \sim e$ ja $h \sim e$, joten $gh \sim ee = e$, koska laskutoimitus on yhteensopiva relaation $\sim$ kanssa. Näin ollen $gh \in N$. Samasta syystä pätee

$$e = g^{-1}g \sim g^{-1}e = g^{-1}.$$

Täten $g^{-1} \in N$, ja N on G:n aliryhmä.

Osoitetaan sitten, että ekvivalenssirelaatio on vaadittua muotoa. Olkoot sitä varten $g, g' \in G$. Oletetaan ensin, että $g \sim g'$. Tällöin $g^{-1}g' \sim g^{-1}g = e$, joten $g^{-1}g' \in N$. Toisaalta, jos $g^{-1}g' \in N$, niin $g^{-1}g' \sim e$. Tällöin

$$g' = gg^{-1}g' \sim ge = g.$$

Voidaan siis todeta, että $g \sim g'$, jos ja vain jos $g^{-1}g' \in N$.

Yllä on osoitettu, että N on G:n aliryhmä ja kaikilla $g \in G$ pätee $gN = [g]$. Samalla tavoin voidaan osoittaa, että $Ng = [g]$ kaikilla $g \in G$, mistä seuraa, että N:n vasemmat ja oikeat sivuluokat ovat samat. Tämä tarkoittaa, että N on normaali. □

Renkaiden kohdalla on pidettävä huoli siitä, että tekijärakenteeseen liittyvä ekvivalenssirelaatio on yhteensopiva *molempien* laskutoimitusten suhteen. Koska renkaan yhteenlaskuryhmä on vaihdannainen, kaikki sen aliryhmät ovat automaattisesti normaaleja. Kertolaskun mukaan liittämistä varten aliryhmän on lisäksi toteutettava ns. *ideaalisuusehdot*.

MÄÄRITELMÄ 1.9. Renkaan $(R, +, \cdot)$ yhteenlaskuryhmän aliryhmää A kutsutaan *ideaaliksi*, jos kaikilla $r \in R$ ja $a \in A$ pätee

$$ra \in A \qquad \text{ja} \qquad ar \in A.$$

Pelkästään ensimmäisen ehdon toteuttavia aliryhmiä kutsutaan *vasemmanpuoleisiksi* ideaaleiksi ja pelkästään jälkimmäisen ehdon toteuttavia *oikeanpuoleisiksi*.

Huomautus. Ideaalin ehdot on helpompi mieltää, kun pohtii kysymystä ”minkälainen sivuluokka voidaan ottaa tekijärenkaan nolla-alkioksi?” Koska renkaassa pätee aina $r \cdot 0 = 0 \cdot r = 0$, täytyy tämän luokan myös toteuttaa $[r]A = A[r] = A$ kaikilla $r \in R$. Tämä johtaa ideaalin ehtoihin.

Renkaan yhteenlaskuryhmässä aliryhmän A sivuluokkaositusta vastaava ekvivalenssirelaatio tulee muotoon $r - r' \in A$. Jos A on ideaali, tämän relaation avulla voidaan muodostaa tekijärengas.

LAUSE 1.10. *Olkoon A ideaali renkaassa R. Tällöin ekvivalenssirelaatio*

$$r \sim r' \iff r - r' \in A$$

on yhteensopiva renkaan kertolaskun kanssa.

Renkaan R tekijärengasta ideaalin A suhteen merkitään R/A. Kuten ryhmien tapauksessa, myös nyt jokainen laskutoimitusten kanssa yhteensopiva ekvivalenssirelaatio on peräisin jostain ideaalista. Todistus sivuutetaan.

LAUSE 1.11. *Oletetaan, että $\sim$ on renkaassa R määritelty, molempien laskutoimitusten kanssa yhteensopiva ekvivalenssirelaatio. Tällöin nolla-alkion luokka $A = [0]$ on ideaali renkaassa R, ja kaikilla $r, r' \in R$ pätee $r \sim r'$ jos ja vain jos $r - r' \in A$.*

1.3. Esimerkki: käänteisalkioiden lisääminen. Vaikka useimmat jäljempänä käsiteltävät rakenteet pohjautuvatkin ryhmiin tai renkaisiin, käsitellään tässä esimerkin vuoksi tekijärakennetta, joka ei ole tekijäryhmä eikä -rengas. Samantapaisia konstruktioita tavataan myöhemminkin tässä materiaalissa.

Positiivisia kokonaislukuja voi laskea yhteen ilman rajoituksia, mutta vähennyslaskua varten on otettava käyttöön negatiiviset luvut. Koulussa opitaan, että jos m ja n ovat kokonaislukuja ja $m < n$, niin $m - n$ on negatiivinen luku, joka vastaa positiivista lukua $n - m$ (on sen vastaluku). Algebrassa negatiiviset luvut voidaan määritellä tekijärakenteen avulla.

Tarkastellaan saman tien yleisempää tilannetta, jossa $(M, +)$ on mikä tahansa vaihdannainen monoidi (esimerkiksi $M = \mathbb{N}$). Yritetään luoda rakenne, joka sisältäisi monoidin M mutta jossa kaikkien alkioiden erotukset olisi määritelty. Tätä

varten muodostetaan ensin joukko, joka sisältää muodollisesti kaikki mahdolliset erotukset, ja näistä samastetaan tekijärakenteen avulla ne, joiden tulisi vastata samaa alkiota.

Lähdetään liikkeelle tulomonoidista $(M \times M, +)$, jossa yhteenlasku määritellään pisteittäin: $(a,b)+(c,d) = (a+c, b+d)$. Neutraalialkiona toimii $(0,0)$, missä 0 on monoidin M neutraalialkio. Jokaista paria $(a,b) \in M \times M$ voidaan nyt pitää muodollisena erotuksena "$a-b$", ja kukin alkuperäisen monoidin alkio $a \in M$ voidaan ajatella parina $(a,0)$.

Tulomonoidi ei kuitenkaan riitä ratkaisuksi, sillä siinä kaikki parit (a,b) ja (a',b') ovat eri alkioita, kun taas erotusten $a-b$ ja $a'-b'$ tulisi olla samat, jos vain $a+b' = a'+b$. Tällaiset parit on siis samastettava. Teknisistä syistä samastamiseen käytettävä relaatio kirjoitetaan muodossa

$$(a,b) \sim (a',b'), \quad \text{jos} \quad a+b'+c = a'+b+c \quad \text{jollain } c \in M.$$

On suoraviivaista osoittaa, että relaatio $\sim$ on yhteenlaskun kanssa yhteensopiva ekvivalenssirelaatio, joten tekijärakenteessa $G = M \times M/\!\sim$ on lauseen 1.3 nojalla voimassa yhteenlasku

$$[(a,b)] + [(c,d)] = [(a+c, b+d)].$$

Lisäksi voidaan nähdä, että tekijärakenteessa G jokainen alkio on kääntyvä, sillä

$$[(a,b)] + [(b,a)] = [(a+b, b+a)] = [(0,0)] \quad \text{kaikilla } a,b \in M.$$

Tämä vastaa tarkalleen sitä koulusta tuttua ajatusta, että erotuksen $a-b$ vastaalkion olisi oltava $b-a$. Huomataan, että G on näin ollen vaihdannainen ryhmä.

Määritellään vielä kuvaus $\eta\colon M \to G$ kaavalla $\eta(a) = [(a,0)]$. Ei ole vaikea näyttää, että η on monoidihomomorfismi, joten sen avulla voidaan monoidin M alkiot tulkita ryhmän G alkioiksi, aivan kuten monoidin $\mathbb{N}$ alkiot tulkitaan ryhmän $\mathbb{Z}$ alkioiksi. Erona kokonaislukuihin on kuitenkin se, että η ei ole aina välttämättä injektiivinen kuvaus, joten monoidia M ei voi välttämättä ajatella ryhmän G alimonoidina.

1.4. Homomorfismit ja tekijärakenteet. Oletetaan, että on määritelty algebrallinen rakenne $(X, *)$ ja sen tekijärakenne $X/\!\sim$ ekvivalenssirelaation $\sim$ suhteen. Olkoon lisäksi $(Y, \dot{})$ jokin toinen samaa tyyppiä oleva rakenne. Tavallinen tilanne on, että halutaan määritellä kuvaus $\overline{f}\colon X/\!\sim \to Y$ kaavalla

$$\overline{f}([x]) = f(x). \qquad (*)$$

Voitaisiin esimerkiksi haluta määritellä jäännösluokkarenkaiden $\mathbb{Z}_m$ ja $\mathbb{Z}_n$ välille kuvaus kaavalla $\overline{f}([a]_m) = [2a]_n$. Mahdollinen ongelma tulee siitä, että kuva-alkio $f(x)$ voi riippua luokan $[x]$ edustajasta.

MÄÄRITELMÄ 1.12. Olkoon X joukko, jossa on määritelty ekvivalenssirelaatio $\sim$. Olkoon lisäksi f kuvaus X:ltä joukkoon Y. Jos kaikilla $x, x' \in X$ pätee

$$x \sim x' \qquad \Rightarrow \qquad f(x) = f(x'),$$

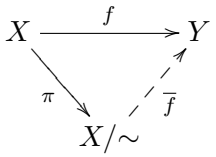
sanotaan, että kuvaus f on *yhteensopiva* ekvivalenssirelaation $\sim$ kanssa.

Huomautus. Kuvauksen ja laskutoimituksen yhteensopivuudessa annetun relaation kanssa on itse asiassa kyse samasta asiasta, sillä laskutoimituskin on kuvaus $*\colon (x,y) \mapsto x*y$. Tässä on kuitenkin annettu molemmat määritelmät erikseen selkeyden vuoksi.

Toisinaan on kätevää, jos kuvauksiin liittyvissä merkinnöissä ei tarvitse viitata rakenteiden alkioihin vaan ainoastaan itse kuvauksiin. Kuvausta $\pi\colon X \to X/{\sim}$, $\pi(x) = [x]$, joka liittää jokaiseen alkioon sen edustaman ekvivalenssiluokan, nimitetään *kanoniseksi surjektioksi*. Tekijärakenteen määritelmästä seuraa suoraan, että kanoninen surjektio on aina homomorfismi. Käyttämällä kanonista surjektiota ehto $(*)$ voidaan kirjoittaa muodossa

$$f = \overline{f} \circ \pi.$$

Kyseinen ehto voidaan myös ilmaista seuraavana kaaviona:



Mikäli ehto toteutuu, sanotaan että kaavio *kommutoi*. Sanotaan myös, että f on *hajotettu* kulkemaan tekijärakenteen $X/{\sim}$ kautta.

Lause 1.13 (Homomorfismin hajottaminen). *Olkoon f homomorfismi rakenteesta $(X, *)$ rakenteeseen $(Y, \cdot)$, ja olkoon $\sim$ joukossa X määritelty laskutoimituksen kanssa yhteensopiva ekvivalenssirelaatio. Jos f on yhteensopiva ekvivalenssirelaation $\sim$ kanssa, on olemassa yksikäsitteinen homomorfismi $\overline{f}\colon X/{\sim} \to Y$, jolle pätee*

$$f = \overline{f} \circ \pi,$$

missä π on kanoninen surjektio $X \to X/{\sim}$.

Todistus. Olkoot $x, x' \in X$ sellaisia, että $\pi(x) = \pi(x')$. Tällöin $x \sim x'$, ja koska f on yhteensopiva relaation $\sim$ kanssa, myös $f(x) = f(x')$. Koska $f(x')$ on siis sama alkio kaikilla $x' \in [x]$, voidaan kuvauksen $\overline{f}$ arvot määritellä yksikäsitteisesti valitsemalla $\overline{f}([x]) = f(x)$. Näin saatu $\overline{f}$ on homomorfismi, sillä

$$\overline{f}([x] * [y]) = \overline{f}([x * y]) = f(x * y) = f(x) \cdot f(y) = \overline{f}([x]) \cdot \overline{f}([y]),$$

ja mahdollinen neutraalialkion luokka $[e]$ kuvautuu alkiolle $f(e)$, joka puolestaan on struktuurin Y neutraalialkio. Kuvauksen $\overline{f}$ yksikäsitteisyys seuraa siitä, että jokainen tekijärakenteen alkio on muotoa $[x]$ jollain $x \in X$, ja kuvauksen $\overline{f}$ on toteutettava ehto $\overline{f}([x]) = f(x)$ kaikilla $x \in X$. □

Huomautus. Edellisessä lauseessa mainittu ehto on itse asiassa välttämätön, eli kaavan $f = \overline{f} \circ \pi$ määrittelemä kuvaus on olemassa, jos ja vain jos f on yhteensopiva ekvivalenssirelaation kanssa. Huomaa lisäksi, että $\operatorname{Im} \overline{f} = \operatorname{Im} f$.

Esimerkki 1.14. Jatketaan esimerkin 1.4 tarkastelua. Niin sanottu *inkluusiokuvaus* $\iota\colon (\mathbb{N}, +) \to (\mathbb{Z}, +)$, $\iota(n) = n$, on monoidihomomorfismi. Se ei kuitenkaan ole yhteensopiva ekvivalenssirelaation kanssa, sillä esim. $\iota(0) \neq \iota(2)$, vaikka $0 \sim 2$. Tekijämonoidista $\mathbb{N}/{\sim}$ ei siis saada kuvausta ι vastaavaa homomorfismia kokonaisluvuille. Tämä olisikin luonnotonta: kyseisen homomorfismin kuvassa voisi olla korkeintaan kaksi alkiota (koska tekijämonoidi on kaksialkioinen), mutta toisaalta sen pitäisi olla sama kuin $\operatorname{Im} \iota$, joka on ääretön.

Tarkastellaan sitten kuvausta $g\colon (\mathbb{N}, +) \to (\{1, -1\}, \cdot)$, $g(n) = (-1)^n$, joka on myös homomorfismi. Jos $n \sim n'$, joillain $n, n' \in \mathbb{N}$, niin jollain $k \in \mathbb{N}$ pätee

$$g(n) = (-1)^n = (-1)^{2k-n'} = \left((-1)^2\right)^k \cdot \left((-1)^{-1}\right)^{n'} = 1^k \cdot (-1)^{n'} = g(n').$$

Siispä g on yhteensopiva relaation $\sim$ kanssa. Näin ollen on olemassa homomorfismi $\overline{g}\colon \mathbb{N}/\!\sim \to \{1,-1\}$, jolle pätee $[0]\mapsto 1$ ja $[1]\mapsto -1$. Koska tämä homomorfismi on bijektiivinen, se on itse asiassa ryhmäisomorfismi.

1.5. Homomorfialauseet. Ryhmien ja renkaiden tapauksessa homomorfismien hajottaminen johtaa tuttuihin homomorfialauseisiin.

LAUSE 1.15. *Olkoon $f\colon G\to H$ ryhmähomomorfismi, ja olkoon $N\trianglelefteq G$. Jos $N\subset \operatorname{Ker} f$, niin on olemassa yksikäsitteinen homomorfismi $\overline{f}\colon G/N\to H$, jolle pätee $\overline{f}([g])=f(g)$ kaikilla $g\in G$. Toisaalta mikäli ehto $N\subset \operatorname{Ker} f$ ei päde, kyseistä homomorfismia ei ole olemassa.*

TODISTUS. Oletetaan ensin, että $N\subset \operatorname{Ker} f$. Olkoot $g,g'\in G$ sellaiset, että $g'\sim g$ eli $g^{-1}g'\in N$. Oletuksen perusteella

$$f(g)^{-1}f(g')=f(g^{-1}g')=e_H,$$

joten $f(g)=f(g')$. Kuvaus f on siis yhteensopiva relaation $\sim$ kanssa, joten kuvauksen $\overline{f}$ olemassaolo seuraa lauseesta 1.13.

Oletetaan sitten, että $N\not\subset \operatorname{Ker} f$. Tällöin löytyy jokin $h\in N$, jolle $f(h)\neq e_H$. Toisaalta $[h]=[e_G]$ ja $f(e_G)=e_H$, joten millekään kuvaukselle ei voi päteä $[g]\mapsto f(g)$ kaikilla $g\in G$. □

Tunnetusti ryhmähomomorfismin ydin on normaali aliryhmä. Yllä olevasta lauseesta saadaan siten erityistapauksessa $\operatorname{Ker} f=N$ tuttu homomorfialause.

KOROLLAARI 1.16 (Ryhmien homomorfialause). *Olkoon $f\colon G\to H$ ryhmähomomorfismi. Tällöin ryhmät $G/\operatorname{Ker} f$ ja $\operatorname{Im} f$ ovat isomorfiset.*

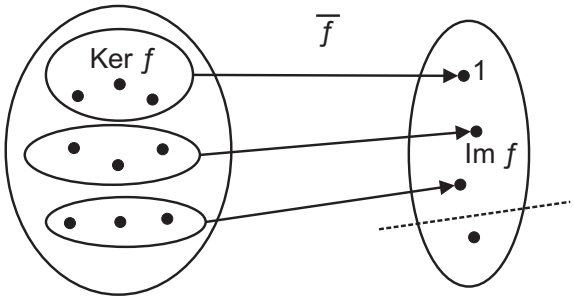
$$\begin{array}{ccc} G & \xrightarrow{\ f\ } & H \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle\iota} \\ G/\operatorname{Ker} f & \xrightarrow{\ \cong\ } & \operatorname{Im} f \end{array}$$

(Kaavioissa kaksoisnuoli viittaa yleensä surjektioon ja koukkunuoli injektioon; tässä ι on inkluusiokuvaus.)

TODISTUS. Edellisen lauseen nojalla löytyy homomorfismi $\overline{f}\colon G/\operatorname{Ker} f\to H$, jolle pätee $\overline{f}([g])=f(g)$ kaikilla $g\in G$. Tarkistetaan injektiivisyys. Olkoon $g\in G$ sellainen, että $[g]\in \operatorname{Ker}\overline{f}$. Tällöin $f(g)=\overline{f}([g])=e_H$, joten $g\in \operatorname{Ker} f=[e_G]$. Täten $[g]=[e_G]$, mistä seuraa, että $\operatorname{Ker}\overline{f}=\{[e_G]\}$. Täten $\overline{f}$ on injektiivinen. Rajoittamalla maalijoukko aliryhmään $\operatorname{Im} f$, saadaan kuvauksesta $\overline{f}$ edelleen bijektiivinen homomorfismi $\tilde{f}\colon G/\operatorname{Ker} f\to \operatorname{Im} f$. □

Renkaiden tapauksessa on tarkasteltava molempia laskutoimituksia. Tunnetusti rengashomomorfismin ydin on aina ideaali. Seuraavien rengashomomorfismien hajotukseen liittyvien lauseiden todistukset sivuutetaan, koska ne ovat aivan samanlaiset kuin ryhmien tapauksessa.

LAUSE 1.17. *Olkoon $f\colon R\to S$ rengashomomorfismi, ja olkoon A renkaan R ideaali. Jos $A\subset \operatorname{Ker} f$, niin on olemassa yksikäsitteinen rengashomomorfismi $\overline{f}\colon R/A\to S$, jolle pätee $\overline{f}([r])=f(r)$ kaikilla $r\in R$. Toisaalta mikäli ehto $A\subset \operatorname{Ker} f$ ei päde, kyseistä homomorfismia ei ole olemassa.*



KUVA 2. Homomorfismi $\overline{f}$ kuvaa ytimen sivuluokat yksi yhteen kuvajoukon alkioille

KOROLLAARI 1.18 (Renkaiden homomorfialause). *Olkoon* $f\colon R \to S$ *rengashomomorfismi. Tällöin renkaat* $R/\operatorname{Ker} f$ *ja* $\operatorname{Im} f$ *ovat isomorfiset.*

Lineaarialgebraa

Tässä osassa tutkitaan aluksi tutun lineaarialgebran yleistystä, jossa skalaarikertoimet eivät välttämättä muodosta kuntaa. Sen jälkeen tutustutaan joihinkin uusiin lineaarialgebrallisiin konstruktioihin, kuten tensorituloihin ja algebroihin.

2. Modulit

Vektoriavaruudet ovat vaihdannaisia ryhmiä, joissa jokin kunta toimii skalaarikertolaskun kautta. Tämä kunta on tyypillisesti joko reaali- tai kompleksilukujen kunta, mutta myös muut kunnat tuottavat samankaltaisen rakenteen. Hyväksymällä kerroinrakenteeksi kunnan sijaan rengas saadaan rakenne nimeltä *moduli*. Modulien teoria poikkeaa melko paljon vektoriavaruuksien teoriasta. Yleisellä modulilla ei esimerkiksi välttämättä ole kantaa, ja vaikka olisikin, kannan pituus ei ole välttämättä yksikäsitteinen, jolloin dimension käsitettä ei voida määritellä. Toisaalta moduleita esiintyy useammissa tilanteissa kuin vektoriavaruuksia. Esimerkiksi jokainen vaihdannainen ryhmä voidaan varustaa modulirakenteella, jossa skalaarikertoimina toimivat kokonaisluvut. Myös niin kutsutussa esitysteoriassa käytetään laajasti hyväksi moduleita.

2.1. Modulit ja lineaarikuvaukset. Rajoitutaan modulien yhteydessä yksinkertaisuuden vuoksi vaihdannaisiin kerroinrenkaisiin ellei toisin mainita.

MÄÄRITELMÄ 2.1. Olkoon R vaihdannainen rengas, ja olkoon $(M, +)$ vaihdannainen ryhmä, jossa on määritelty renkaan R *skalaarikertolasku* $(a, x) \mapsto a.x$ kaikilla $a \in R$ ja $x \in M$. Ryhmää M nimitetään *R-moduliksi*, mikäli seuraavat ehdot toteutuvat kaikilla $a, b \in R$ ja $x, y \in M$:

(M1) $1.x = x$
(M2) $(ab).x = a.(b.x)$
(M3) $(a + b).x = a.x + b.x$
(M4) $a.(x + y) = a.x + a.y$.

Rengasta R kutsutaan modulin M *kerroinrenkaaksi*.

Skalaarikertolaskua on tässä korostettu pisteellä, mutta piste jätetään yleensä käytännössä pois. Puhuttaessa R-modulista oletetaan jatkossa, että R on jokin vaihdannainen rengas. Jos kerroinrengas on asiayhteydestä selvä, voidaan R-modulia kutsua yksinkertaisesti moduliksi.

Huomaa, että jos R on kunta, modulin määritelmä on täsmälleen sama kuin vektoriavaruuden määritelmä. Moduli on siis vektoriavaruuden yleistys, jossa skalaarikerrointen ei tarvitse olla kääntyviä. Kuten vektoriavaruuksien tapauksessa, modulin aksioomista voidaan helposti johtaa tuttuja laskusääntöjä, kuten $0.x = 0$, $(-1).x = -x$ jne., kunhan ne eivät vaadi kerroinalkioiden kääntyvyyttä.

Esimerkki 2.2. Esimerkkejä moduleista:

- Jokainen K-vektoriavaruus on K-moduli.
- Jokainen vaihdannainen rengas R on itse R-moduli, kun skalaarikertolaskuksi otetaan renkaan oma kertolasku.
- Jokainen vaihdannainen ryhmä on $\mathbb{Z}$-moduli, kun skalaarikertolaskuksi määritellään monikerran ottaminen: $n.x = x + \cdots + x$ (n kertaa). Tämä on itse asiassa ainoa tapa, jolla renkaan $\mathbb{Z}$ skalaarikertolasku voidaan määritellä vaihdannaisessa ryhmässä.
- Jos M on vaihdannainen ryhmä, jonka jokaisen alkion kertaluku jakaa luvun n, voidaan ryhmässä M määritellä jäännösluokkarenkaan $\mathbb{Z}_n$ skalaarikertolasku kaavalla $[k]_n.x = kx$ (monikerta). Tämä toteutuu muun muassa silloin kun $|M| = n$. Toisaalta esimerkiksi Kleinin neliryhmä on $\mathbb{Z}_2$-moduli. Kun p on alkuluku, rengas $\mathbb{Z}_p$ on kunta, ja jokainen $\mathbb{Z}_p$-moduli on siis vektoriavaruus.
- Vaihdannaisen renkaan R ideaalit ovat R-moduleja, kun skalaarikertolaskuna on renkaan R kertolasku. Ideaalit ovat samalla rengasmodulin R alimoduleja (määritelmä seuraa jäljempänä). Alirenkaat eivät yleensä ole modulin R alimoduleja.

Olkoot M ja N joitain R-moduleja. Kuvausta $f\colon M \to N$ kutsutaan *R-modulihomomorfismiksi* tai *R-lineaarikuvaukseksi*, jos se on skalaarikertolaskun säilyttävä ryhmähomomorfismi, eli seuraavat ehdot pätevät kaikilla $x, y \in M$ ja $a \in R$:

(L1) $f(x + y) = f(x) + f(y)$
(L2) $f(a.x) = a.f(x)$.

Bijektiivistä lineaarikuvausta nimitetään *lineaariseksi isomorfismiksi*. Lineaarikuvauksen ydin on sama kuin vastaavan ryhmähomomorfismin ydin, eli nollan alkukuva.

Esimerkki 2.3. Tarkastellaan kaikkien R-modulihomomorfismien $M \to N$ joukkoa $\mathrm{Hom}_R(M, N)$. Määritellään tässä joukossa pisteittäiset laskutoimitukset

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

Voidaan osoittaa, että tällä tavoin määritellyt kuvaukset $f + g$ ja $a.f$ ovat itsekin modulihomomorfismeja kaikilla $f, g \in \mathrm{Hom}_R(M, N)$ ja $a \in R$, joten joukko $\mathrm{Hom}_R(M, N)$ on suljettu kyseisten laskutoimitusten suhteen. Lisäksi laskutoimitukset toteuttavat ehdot (M1)–(M4), joten $\mathrm{Hom}_R(M, N)$ on itse asiassa R-moduli.

Jos R on kunta, modulit M ja N ovat vektoriavaruuksia. Oletetaan, että nämä avaruudet ovat äärellisulotteisia, ja merkitään $\dim M = m$ ja $\dim N = n$. Tällöin jokainen lineaarikuvaus $M \to N$ vastaa tavalliseen tapaan jotakin $n \times m$ -matriisia, jonka alkiot ovat renkaassa R. Edelleen joukko $\mathrm{Hom}_R(M, N)$ voidaan ajatella matriisijoukkona $R^{n\times m}$. Yllä määritellyt laskutoimitukset vastaavat tällöin tuttuja matriisien yhteenlaskua ja skalaarikertolaskua.

2.2. Ali- ja tekijämodulit. Modulin M *alimoduli* N on ryhmän M aliryhmä, joka on vakaa skalaarikertolaskun suhteen. Kaikilla $x, y \in N$ ja $a \in R$ (kerroinrengas) täytyy siis päteä seuraavat ehdot:

(AM1) $x + y \in N$
(AM2) $a.x \in N$.

Lisäksi alimodulin on oltava epätyhjä. Tällöin aliryhmän ehdoista riittää tarkistaa vain vakaus yhteenlaskun suhteen (AM1), sillä muut ehdot seuraavat epätyhjyydestä, moduliaksioomista ja ehdosta (AM2). Mielivaltaisten alimodulien leikkaus on aina alimoduli. Lineaarikuvausten kuvat ja ytimet ovat myös alimoduleja.

Olkoot A ja B kaksi modulin M alimodulia. Niiden *summa* on

$$A + B = \{a + b \mid a \in A,\, b \in B\}.$$

Siitä, että modulit ovat vaihdannaisia ryhmiä, seuraa, että alimodulien summa on aina aliryhmä. Se on samalla pienin aliryhmä, joka sisältää summattavansa, mikä voidaan ilmaista kaavalla $A+B = \langle A \cup B \rangle$. Lisäksi alimodulien summa on suljettu skalaarikertolaskun suhteen, koska $r(a+b) = ra+rb \in A+B$ pätee kaikilla $a \in A$ ja $b \in B$. Täten alimodulien summa on itsekin alimoduli.

Summaa voidaan yleistää äärettömän monelle alimodulille yllä mainitun viritysominaisuuden avulla. Olkoon $(M_i)_{i\in I}$ perhe[1] modulin M alimoduleita. Määritellään näiden alimodulien summa seuraavasti:

$$\sum_{i\in I} M_i = \left\langle \bigcup_{i\in I} M_i \right\rangle.$$

Toisin sanoen summa on sellaisten alkioiden x virittämä aliryhmä, joista kukin sisältyy johonkin alimoduleista M_i. Summan alkiot ovat siis muotoa

$$x_{i_1} + x_{i_2} + \cdots + x_{i_n},$$

missä jokainen x_{i_k} sisältyy johonkin alimoduliin M_{i_k}. Tämä voidaan ilmaista myös sanomalla, että alkiot ovat summia $\sum_{i\in I} x_i$, missä $x_i \in M_i$ kaikilla i, ja $x_i = 0$ lukuunottamatta äärellistä määrää indeksejä i. Alimodulien yleinen summa on aina alimoduli.

Esimerkki 2.4. Tarkastellaan reaalilukujen yhteenlaskuryhmää $\mathbb{Z}$-modulina. Määritellään kullakin alkuluvulla p joukko

$$M_p = \{n/p^k \mid n \in \mathbb{Z}, k \in \mathbb{N}\}.$$

Joukot M_p ovat $\mathbb{Z}$-modulin $\mathbb{R}$ alimoduleja. Määritetään näiden alimodulien summa $S = \sum_p M_p$. Selvästikin jokaisella p pätee $M_p \subset \mathbb{Q}$, ja $\mathbb{Q}$ on modulin $\mathbb{R}$ alimoduli. Täten $S \subset \mathbb{Q}$, koska S on pienin alimoduli, joka sisältää kaikki modulit M_p. Toisaalta jokainen rationaaliluku voidaan ilmaista summana $\sum_{i=0}^{n} m_i/p_i^{k_i}$, missä osoittajat ovat kokonaislukuja ja nimittäjät alkulukujen potensseja. Siispä $S = \mathbb{Q}$.

Modulin M mikä tahansa alimoduli N on normaali aliryhmä, koska M on vaihdannainen ryhmä. Aliryhmän N suhteen voidaan siis muodostaa tekijäryhmä. Tästä tekijäryhmästä tulee *tekijämoduli*, kun sivuluokkien skalaarikertolasku määritellään kaavalla

$$a(x + N) = ax + N.$$

Sivuluokkien skalaarikertolasku on automaattisesti hyvin määritelty. Jos nimittäin $x - y = n$ jollain $n \in N$, niin $ax - ay = an \in N$. Tekijämodulia merkitään tavalliseen tapaan symbolilla M/N. Moduleille pätee samanlainen homomorfialause kuin ryhmille ja renkaille.

[1]Perheellä tarkoitetaan kuvausta $i \mapsto M_i$ indeksijoukolta I johonkin alimodulien joukkoon. Jos $I = \mathbb{N}$, tämä on sama kuin jono $(M_0, M_1, M_2, \dots)$.

2.3. Vapaat modulit. Vektoriavaruuksille on ominaista, että niiden vektorit voidaan ilmaista yksikäsitteisesti kantavektorien yhdistelminä. Tässä luvussa tarkastellaan moduleja, joilla on vastaava ominaisuus.

Olkoon X joukko R-modulin M alkioita. Kiinnitetään jokin joukon X indeksöinti $X = \{x_i\}_{i\in I}$. Äärellistä summaa $\sum_i r_i x_i$, missä $r_i \in R$ kaikilla i, kutsutaan joukon X *lineaarikombinaatioksi* eli *lineaariseksi yhdistelmäksi*. Jos jokainen modulin M alkio voidaan ilmaista joukon X lineaarikombinaationa, sanotaan, että X *virittää* modulin M. Edelleen jos kullakin lineaarikombinaatiolla pätee $\sum_i r_i x_i = 0$ vain siinä tapauksessa, että $r_i = 0$ kaikilla i, sanotaan, että osajoukko X on *vapaa* eli että sen alkiot ovat *lineaarisesti riippumattomia*. Jos osajoukko ei ole vapaa, se on *sidottu*.

MÄÄRITELMÄ 2.5. Olkoon M jokin R-moduli. Osajoukkoa $B \subset M$ kutsutaan modulin M *kannaksi*, jos B on vapaa joukko, joka virittää modulin M. Jos tällainen osajoukko löytyy, modulia M kutsutaan *vapaaksi*.

Vapaassa modulissa jokainen alkio voidaan esittää kanta-alkioiden lineaarikombinaationa. Tämä esitys on lisäksi yksikäsitteinen, sillä jos $\sum_i r_i b_i = \sum_i r'_i b_i$, niin $\sum_i (r_i - r'_i) b_i = 0$, ja koska B on vapaa, tästä seuraa, että $r_i = r'_i$ kaikilla i.

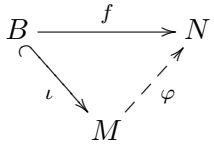
Huomautus. Vapautta tarkasteltaessa on tärkeää, että indeksijoukko on ennalta valittu ja että lineaarikombinaatiossa samat indeksit eivät toistu. Muuten voisi väittää, että yksiö $\{x_1\}$ ei olisi vapaa, koska lineaarikombinaatio $x_1 - x_1$ on nolla, vaikka kertoimet eivät ole nollia. Toisinaan käytetään joukon X sijasta indeksöityä jonoa tai perhettä $(x_i)_{i\in I}$. Ero tulee näkyviin tilanteissa, joissa sama alkio toistuu, sillä esimerkiksi jono (x, x) on sidottu, kun taas joukkona $\{x, x\} = \{x\}$ on vapaa.

ESIMERKKI 2.6. Esimerkkejä vapaista moduleista:

- Lineaarialgebran peruskurssilla on osoitettu, että jokaisella äärellisvirritteisellä $\mathbb{R}$-vektoriavaruudella on kanta, joten jokainen tällainen vektoriavaruus on vapaa $\mathbb{R}$-moduli. Sama todistus toimii millä tahansa kerroinkunnalla. Valinta-aksioomaa käyttämällä voidaan todistaa, että myös muilla kuin äärellisvirritteisillä vektoriavaruuksilla on kanta.
- Mikä tahansa vaihdannainen rengas R on itse vapaa R-moduli, kantana yksiö $\{1\}$. Yleisemmin karteesinen tulo R^n on vapaa moduli kaikilla $n \in \mathbb{N}$, kun laskutoimitukset määritellään pisteittäin. Tulomodulin R^n *luonnollinen kanta* koostuu alkioista $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, missä ykkösalkio on i:nnellä paikalla.
- Jos R on vaihdannainen rengas, R-alkioisten $n \times m$ -matriisien joukko $R^{n\times m}$ on R-moduli, laskutoimituksina matriisien yhteenlasku ja skalaarikertolasku. Matriisimoduli on vapaa moduli, jonka luonnollisen kannan muodostavat alkeismatriisit E_{ij}, joissa on rivillä i ja sarakkeessa j renkaan R ykkösalkio ja muut alkiot ovat nollia.
- Vaihdannaista ryhmää kutsutaan vapaaksi, jos se on vapaa $\mathbb{Z}$-modulina. Rationaalilukujen joukko $\mathbb{Q}$ ei ole vapaa ryhmä. Myöskään jäännösluokkaryhmä $\mathbb{Z}_n$ ei ole vapaa, mikä seuraa muun muassa jäljempänä todistettavasta lauseesta 3.5. Tuo lause osoittaa, että jokainen vapaa vaihdannainen ryhmä on isomorfinen ryhmistä $\mathbb{Z}$ koostuvan suoran summan kanssa. Erityisesti siis jokainen vapaa vaihdannainen ryhmä on ääretön.

Jokainen vapaassa modulissa määritelty lineaarikuvaus määräytyy täysin kannan alkioiden kuvien perusteella.

LAUSE 2.7. *Olkoon M vapaa R-moduli, jolla on kanta B, ja olkoon $\iota\colon B \to M$ inkluusiokuvaus. Oletetaan lisäksi, että N on jokin toinen R-moduli ja $f\colon B \to N$ on mikä tahansa kuvaus. Tällöin on olemassa yksikäsitteinen R-lineaarinen kuvaus $\varphi\colon M \to N$, jolle pätee $\varphi \circ \iota = f$ eli oheinen kaavio kommutoi.*



TODISTUS. Jokaisella vapaan modulin alkiolla $x \in M$ on yksikäsitteinen esitys $x = \sum_i r_i b_i$ kannan alkioiden lineaarikombinaationa. Jos $\varphi\colon M \to N$ on lineaarikuvaus, jolle pätee $\varphi(b) = f(b)$ kaikilla $b \in B$, niin

$$\varphi(x) = \varphi\left(\sum_i r_i b_i\right) = \sum_i r_i \varphi(b_i) = \sum_i r_i f(b_i). \qquad (*)$$

Jos haluttu lineaarikuvaus siis on olemassa, sen arvot määräytyvät yksikäsitteisesti ehdosta $\varphi(x) = \sum_i r_i f(b_i)$.

Toisaalta mikään ei estä määrittelemästä kuvausta $\varphi\colon M \to N$ juuri ehdon $(*)$ avulla. Tällaiselle kuvaukselle pätee selvästi $\varphi(b) = f(b)$. On lisäksi helppo tarkistaa, että φ on R-lineaarinen. □

Edellisen lauseen sovelluksena todistetaan seuraavaksi, että vapaat modulit, joilla on sama kanta, ovat isomorfisia. Tilanne on siis sama kuin vektoriavaruuksilla, ja tulos voitaisiin myös todistaa samalla tavalla. Laaditaan todistus nyt kuitenkin yleisemmässä muodossa käyttäen hyväksi ainoastaan edellistä lausetta. Todistuksesta tulee abstraktimpi ja sen ymmärtäminen vaatii hieman paneutumista, mutta hyötynä on, että samaa todistusrakennetta voidaan käyttää vastaavissa tilanteissa myös jatkossa.

LAUSE 2.8. *Olkoot M ja N vapaita moduleja, joilla on sama kanta. Tällöin M ja N ovat isomorfisia.*

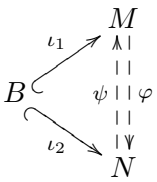
TODISTUS. Olkoon B modulien M ja N yhteinen kanta. Merkitään inkluusiokuvauksia $\iota_1\colon B \to M$ ja $\iota_2\colon B \to N$. Ideana on käyttää edellistä lausetta vuorotellen kumpaankin inkluusioon. Kuvauksesta ι_2 saadaan tuon lauseen nojalla lineaarikuvaus $\varphi\colon M \to N$, jolle pätee

$$\varphi \circ \iota_1 = \iota_2.$$

Kuvauksesta ι_1 puolestaan saadaan lineaarikuvaus $\psi\colon N \to M$, jolle pätee

$$\psi \circ \iota_2 = \iota_1.$$

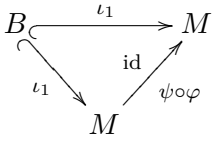
Nyt riittää osoittaa, että φ ja ψ ovat toistensa käänteiskuvauksia. Se tehdään vetoamalla edellisen lauseen yksikäsitteisyysosaan.



Tarkastellaan yhdistettyä kuvausta $\psi \circ \varphi$. Huomataan, että

$$(\psi \circ \varphi) \circ \iota_1 = \psi \circ (\varphi \circ \iota_1) = \psi \circ \iota_2 = \iota_1.$$

Kuvaus $\psi \circ \varphi$ on siis lineaarikuvaus $M \to M$, jolle pätee $(\psi \circ \varphi) \circ \iota_1 = \iota_1$. Selvästi myös identtinen kuvaus on lineaarikuvaus, jolle pätee $\mathrm{id}_M \circ \iota_1 = \iota_1$. Kuitenkin edellisen lauseen perusteella tämän ehdon toteuttava kuvaus on yksikäsitteinen, joten täytyy päteä $\psi \circ \varphi = \mathrm{id}_M$.



Samalla tavoin voidaan näyttää, että $\varphi \circ \psi = \mathrm{id}_N$. Täten lineaarikuvaukset φ ja ψ ovat toistensa käänteiskuvauksia, ja edelleen modulit M ja N ovat isomorfisia. □

3. Modulikonstruktioita

3.1. Modulien suorat summat ja tulot. Useimpien algebrallisten perusrakenteiden tapauksessa kahden rakenteen karteesinen tulo on myös samantyyppinen rakenne. (Tämä ei koske tiettyjä erityisrakenteita, kuten kokonaisalueita tai kuntia.) Kahden R-modulin karteesista tuloa nimitetään *suoraksi summaksi* ja merkitään $M \oplus N$. Se on R-moduli, joka koostuu pareista (m, n), missä $m \in M$ ja $n \in N$. Useamman modulin tapauksessa summaa voidaan merkitä

$$\bigoplus_{i=1}^{n} M_i,$$

ja sen alkioiksi tulevat n-jonot $(m_1, m_2, \ldots, m_n)$, missä $m_i \in M_i$ kaikilla i. Ääretömän indeksijoukon tapauksessa suoran summan määritelmä poikkeaa karteesisen tulon määritelmästä. Molemmat ovat kuitenkin R-moduleja, ja jälkimmäistä nimitetään *suoraksi tuloksi*.

MÄÄRITELMÄ 3.1. Olkoon $(M_i)_{i\in I}$ jokin perhe R-moduleita. Modulien M_i *suora tulo* koostuu alkioperheistä $x = (x_i)_{i\in I}$, missä $x_i \in M_i$ kaikilla i. Suora tulo on R-moduli, kun laskutoimitukset määritellään pisteittäin:

$$(x + y)_i = x_i + y_i \qquad \text{ja} \qquad (ax)_i = ax_i.$$

Suoraa tuloa merkitään $\prod_{i\in I} M_i$.

Suora summa määritellään suoran tulon osajoukkona. Oletetaan jälleen, että $(M_i)_{i\in I}$ on jokin perhe R-moduleita.

MÄÄRITELMÄ 3.2. Modulien M_i *suora summa* koostuu alkioperheistä $(x_i)_{i\in I}$, missä $x_i \in M_i$ kaikilla i ja lisäksi $x_i \neq 0$ vain äärellisellä määrällä indeksejä. Suora summa on R-moduli, kun laskutoimitukset määritellään pisteittäin kuten suorassa tulossa. Suoraa summaa merkitään $\bigoplus_{i\in I} M_i$.

Suoran summan alkiot ovat siis perheitä, joissa vain äärellisen moni jäsen on nollasta poikkeava. Tällaista perhettä sanotaan *äärelliskantajaiseksi*.

Tulo- ja summamoduleihin liittyen viitataan usein *kanonisiin projektioihin* $\pi_j \colon \prod_{i\in I} M_i \to M_j$, $\pi_j(x) = x_j$ sekä *kanonisiin injektioihin* $\iota_j \colon M_j \to \bigoplus_{i\in I} M_i$, $\iota_j(y) = (x_i)_{i\in I}$, missä

$$x_i = \begin{cases} y, & \text{kun } i = j \\ 0 & \text{muuten.} \end{cases}$$

Esimerkiksi jos indeksijoukko on $I = \{1, 2, 3, 4\}$ ja $a \in M_2$, voidaan kirjoittaa $\iota_2(a) = (0, a, 0, 0)$. Sekä kanoniset projektiot että kanoniset injektiot ovat modulihomomorfismeja. Jokainen suoran summan alkio (x_i) voidaan kirjoittaa äärellisenä summana $\sum_i \iota_i(x_i)$. Sama ei päde suoran tulon alkioille, mikäli indeksijoukko on ääretön.

Huom. Ryhmäteoriassa vaihdannaisten ryhmien $(G_i, +)$ suora summa konstruoidaan samalla tavoin kuin modulien suora summa. Suoraksi tuloksi nimitetään kuitenkin täsmälleen samaa konstruktiota siinä tapauksessa, että ryhmän laskutoimitusta merkitään kertolaskuna. Kummassakin rakenteessa siis alkioina ovat perheet (g_i), joissa g_i on 0 lukuunottamatta äärellistä määrää indeksejä. Jos tämä äärellisyysrajoitus jätetään pois, saadaan modulien suoraa tuloa vastaava

rakenne, jota ryhmien tapauksessa kutsutaan *rajoittamattomaksi* suoraksi tuloksi tai summaksi, laskutoimituksesta riippuen.

	modulit	ryhmät
suora summa	äärelliskantajainen tulo	äärelliskantajainen, laskutoimituksena yhteenlasku
suora tulo	karteesinen tulo	äärelliskantajainen, laskutoimituksena kertolasku
rajoittamaton tulo	—	karteesinen tulo

TAULUKKO 1. Erot modulien ja ryhmien suorien summien ja tulojen nimityksissä

Olkoon I mikä tahansa indeksijoukko. Kun rengasta R ajatellaan R-modulina, voidaan muodostaa suora summa $\bigoplus_{i\in I} R$, jota merkitään $R^{(I)}$. Tämä on vapaa moduli. Sen *luonnollinen kanta* koostuu alkioista $e_j = (\delta_{ij})_{i\in I}$, missä $j \in I$ ja

$$\delta_{ij} = \begin{cases} 1, & \text{jos } i = j \\ 0 & \text{muuten.} \end{cases}$$

Luonnollisen kannan alkiot ovat siis renkaan ykkösalkion kuvia kanonisissa injektioissa, eli $e_i = \iota_i(1)$. Indeksijoukon I ja modulin $R^{(I)}$ kannan välillä on luonnollinen bijektio $i \leftrightarrow e_i$. Tätä käytetään usein samastamaan kyseiset joukot, jolloin sanotaan, että $R^{(I)}$ on *joukon I virittämä vapaa moduli*.

ESIMERKKI 3.3. Olkoon R vaihdannainen rengas ja X jokin joukko. Vapaan modulin $R^{(X)}$ mikä tahansa alkio voidaan kirjoittaa luonnollisen kannan alkioiden (äärellisenä) summana. Kun samastetaan kanta-alkio ja sitä vastaava joukon X alkio, voidaan modulin $R^{(X)}$ jokainen alkio kirjoittaa muodollisena lineaarikombinaationa

$$\sum_{x\in X} r_x x = \sum_{x\in X} r_x e_x.$$

Tässä $r_x = 0$ lukuunottamatta äärellistä määrää indeksejä.

Esimerkiksi polynomit määritellään usein algebrassa tuntemattoman potenssien muodollisina lineaarikombinaatioina. Nyt tämä voidaan määritellä täsmällisesti. Jos R on mikä tahansa vaihdannainen rengas, vapaa moduli $R^{(\mathbb{N})}$ koostuu äärelliskantajaisista jonoista renkaan R alkioita, indeksöityinä luonnollisilla luvuilla. Jos kutakin kannan alkiota e_n merkitään tuntemattoman potenssina X^n, muodostavat vapaan modulin alkiot polynomeja, esimerkiksi

$$(1, -3, 0, 2, 0, \dots) = e_0 - 3e_1 + 2e_3 = 1 - 3X + 2X^3.$$

Nähdään siis, että $R[X] = R^{(\mathbb{N})}$.

ESIMERKKI 3.4. Kuten esimerkeissä 2.2 ja 2.6 todettiin, jokainen vaihdannainen ryhmä on $\mathbb{Z}$-moduli, ja jos tämä moduli on vapaa, ryhmää kutsutaan vapaaksi vaihdannaiseksi ryhmäksi. Nyt nähdään, että on mahdollista konstruoida

vapaa vaihdannainen ryhmä $\mathbb{Z}^{(X)}$ minkä tahansa virittäjäjoukon X suhteen. Tämä ryhmä koostuu joukon X alkioista sekä niiden (muodollisista) summista ja erotuksista.

Algebrallisessa topologiassa vapaita vaihdannaisia ryhmiä käytetään muun muassa homologiaryhmien yhteydessä. Joukko X koostuu tällöin jonkin topologisen avaruuden T yleistetyistä kolmioista eli *simplekseistä*. Nämä ovat euklidisten kolmioiden tai niiden n-ulotteisten vastineiden, kuten tetraedrien, kuvia jatkuvissa kuvauksissa. Vapaassa ryhmässä $\mathbb{Z}^{(X)}$ voidaan simplekseistä ottaa summia ja erotuksia, joita kutsutaan ketjuiksi. Tätä ryhmää tutkimalla saadaan tietoa avaruuden T rakenteesta.

Muotoa $R^{(X)}$ olevat modulit eivät itse asiassa ole millään tavoin vapaiden modulien erikoistapauksia, sillä lauseen 2.8 perusteella jokainen vapaa moduli, jolla on kantanaan X, on isomorfinen modulin $R^{(X)}$ kanssa. Tämä on seurausta vapaan modulin niin kutsutusta universaaliominaisuudesta, joka on ilmaistu lauseessa 2.7. Seuraavassa alaluvussa tarkastellaan universaaliominaisuuksia hieman tarkemmin. Kirjoitetaan kuitenkin ensin muistiin mainittu isomorfiatulos.

LAUSE 3.5. *Jos M on vapaa R-moduli kantanaan B, niin $M \cong R^{(B)}$.*

3.2. Universaaliominaisuudet. Lausetta 2.7 nimitetään vapaan modulin universaaliominaisuudeksi. Moniin rakenteisiin liittyy samantyyppinen ominaisuus. Universaaliominaisuus ilmaisee, että jonkin tyyppiset kuvaukset voidaan hajottaa kulkemaan universaalirakenteen kautta siten, että kuvauksen sisä- tai ulkofunktiona toimii universaalirakenteeseen liittyvä kanoninen kuvaus. Vapaiden modulien tapauksessa kanoninen kuvaus on kannan inkluusiokuvaus.

Universaaliominaisuudella on monia sovelluksia. Yksi liittyy kuvausten muodostamiseen. Esimerkiksi vapaan modulin tapauksessa universaaliominaisuudesta seuraa, että lineaarikuvauksen määrittelemiseksi riittää määritellä kannan alkioiden kuvat. Tuloksena on yksikäsitteinen lineaarikuvaus vapaalta modulilta, ja näin vältytään esimerkiksi kuvauksen olemassaolon sekä lineaarisuuden tarkistamiselta.

Toinen hyöty universaaliominaisuudesta on, että universaalirakenne on aina yksikäsitteinen. Todistus noudattaa samoja linjoja kuin lauseen 2.8 todistus. Esimerkiksi vapaista moduleista puhuttaessa voidaan aina viitata tyyppiä $R^{(B)}$ olevaan moduliin, koska kaikki vapaat modulit, joilla on sama kanta, ovat isomorfisia.

Kolmanneksi universaaliominaisuus karakterisoi sen toteuttavan rakenteen. Vapaiden modulien isomorfisuus eli lause 2.8 todistettiin viittaamatta kertaakaan itse modulien vapauteen. Tästä seuraa, että itse asiassa kaikki modulit, jotka toteuttavat kyseisen universaaliominaisuuden, ovat keskenään isomorfisia. Koska eräs näistä, vaikkapa $R^{(B)}$, on vapaa, kaikki universaaliominaisuuden toteuttavat modulit ovat vapaita.

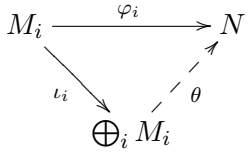
Edellä mainitut ominaisuudet voisi esittää täsmällisesti ja todistaa *kategoriateorian* avulla, mutta emme paneudu siihen tässä. Kategoriateoriassa universaaliobjektit jaetaan alku- ja päätösobjekteihin riippuen siitä, toimiiko niihin liittyvä kanoninen kuvaus sisä- vai ulkofunktiona. Esimerkiksi vapaa moduli on alkuobjekti.

Ainoa kysymys, johon kategoriateoria ei yleensä tuo vastausta, on universaalirakenteen olemassaolo. Tällainen rakenne täytyy yleensä konstruoida joka tilanteessa erikseen. Toisinaan kylläkin kategoriateoriaa voidaan käyttää johtamaan

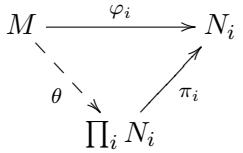
yhden universaalirakenteen olemassaolosta toisen vastaavantyyppisen olemassaolo. Vapaan modulin tapauksessa universaalirakenne $R^{(B)}$ konstruoitiin juuri ennen esimerkkiä 3.3.

Myös suorat summat ja tulot toteuttavat kumpikin erään universaaliominaisuuden. Suoriin summiin liittyvät kanoniset injektiot ι_i ja suoriin tuloihin kanoniset projektiot π_i. Todistukset sivuutetaan.

LAUSE 3.6 (Suoran summan universaaliominaisuus). *Olkoon (M_i) jokin perhe R-moduleja. Oletetaan lisäksi, että N on R-moduli ja φ_i on R-lineaarinen kuvaus $M_i \to N$ jokaisella i. Tällöin löytyy yksikäsitteinen R-lineaarinen kuvaus $\theta\colon \bigoplus_i M_i \to N$, jolle pätee $\varphi_i = \theta \circ \iota_i$ kaikilla i, eli oheinen kaavio kommutoi jokaisella i.*



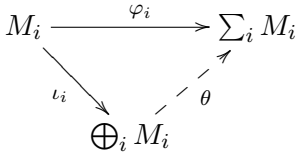
LAUSE 3.7 (Suoran tulon universaaliominaisuus). *Olkoon (N_i) jokin perhe R-moduleja. Oletetaan lisäksi, että M on R-moduli, ja φ_i on R-lineaarinen kuvaus $M \to N_i$ jokaisella i. Tällöin löytyy yksikäsitteinen R-lineaarinen kuvaus $\theta\colon M \to \prod_i N_i$, jolle pätee $\varphi_i = \pi_i \circ \theta$ kaikilla i, eli oheinen kaavio kommutoi jokaisella i.*



Seuraava lauseen todistus toimii esimerkkinä universaaliominaisuuden käytöstä kuvauksen määrittelemiseksi. Lauseessa selvitetään, milloin jokin moduli on isomorfinen suoran summan kanssa.

LAUSE 3.8. *Oletetaan, että $(M_i)_{i\in I}$ on perhe R-modulin M alimoduleja, joille pätee $\sum_i M_i = M$ ja $M_i \cap \sum_{j\neq i} M_j = \{0\}$ kaikilla i. Tällöin M on isomorfinen suoran summan $\bigoplus_i M_i$ kanssa.*

TODISTUS. Jokaisella i voidaan määritellä inkluusiokuvaus $\varphi_i\colon M_i \to M$, missä $\varphi_i(x) = x$. Suoran summan universaaliominaisuuden perusteella on olemassa R-lineaarinen kuvaus $\theta\colon \bigoplus_i M_i \to M$, jolle pätee $\theta \circ \iota_i = \varphi_i$ kaikilla i. Osoitetaan, että θ on bijektio.



Todetaan ensin, että jos $x = (x_i) \in \bigoplus_i M_i$, niin

$$\theta(x) = \theta\left(\sum_i \iota_i(x_i)\right) = \sum_i \varphi_i(x_i) = \sum_i x_i.$$

Surjektiivisuuden osoittamiseksi oletetaan, että $y \in M$ on mielivaltainen. Koska $M = \sum_i M_i$, alkio y voidaan kirjoittaa äärellisenä summana $y = \sum_i x_i$, missä $x_i \in M_i$ kaikilla i. Nyt $x = \sum_i \iota_i(x_i)$ on suoran summan $\bigoplus_i M_i$ alkio, ja yllä todetun perusteella $\theta(x) = \sum_i x_i = y$.

Oletetaan sitten, että $\theta(x) = 0$ jollain $x \in \bigoplus_i M_i$. Tämä tarkoittaa sitä, että $\sum_i x_i = 0$. Edelleen jokaisella i pätee

$$x_i = -\sum_{i \neq j} x_j.$$

Yhtälön vasen puoli on alimodulin M_i alkio, ja oikea puoli taas kuuluu summamoduliin $\sum_{i \neq j} M_j$. Oletuksen mukaan näiden leikkaus on triviaali, joten $x_i = 0$. Koska tämä pätee kaikilla i, saadaan $x = 0$. Näin ollen $\operatorname{Ker} \theta$ on triviaali, joten θ on injektio. □

3.3. Tensoritulot. Monet tutuissa vektoriavaruuksissa määriteltävät tulot ovat *bilineaarisia* eli lineaarisia molempien tekijöiden suhteen. Jos vektorien tuloa merkitään $(x, y) \mapsto x \otimes y$, bilineaarisuus tarkoittaa siis sitä, että

$$\begin{aligned} &(x+y) \otimes z = x \otimes z + y \otimes z, \qquad (ax) \otimes y = a(x \otimes y) \\ \text{sekä} \quad &x \otimes (y+z) = x \otimes y + x \otimes z, \qquad x \otimes (ay) = a(x \otimes y). \end{aligned}$$

Esimerkiksi vektoriavaruuksien pistetulo $x \cdot y$ ja kolmiulotteisen reaaliavaruuden ristitulo $x \times y$ ovat bilineaarisia tuloja. Tässä alaluvussa tutustutaan modulien tensorituloon, joka on tietyssä mielessä universaali bilineaarinen tulo. Aloitetaan määrittelemällä bilineaariset kuvaukset.

MÄÄRITELMÄ 3.9. Olkoon R vaihdannainen rengas, ja olkoot M, N ja P kolme R-modulia. Kuvaus f tulojoukolta $M \times N$ moduliin P on *R-bilineaarinen*, jos se on lineaarinen molempien komponenttien suhteen, eli kaikilla $x, y \in M$, $z, w \in N$ sekä $a \in R$ pätee

(B1) $f(x+y, z) = f(x, z) + f(y, z)$
(B2) $f(x, z+w) = f(x, z) + f(x, w)$
(B3) $f(ax, z) = af(x, z)$
(B4) $f(x, az) = af(x, z)$.

Esimerkiksi reaaliavaruuden pistetulo on edellisen määritelmän merkinnöin kuvaus $f\colon \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$, $f(x, y) = x \cdot y$. Huomaa, että bilineaariselle kuvaukselle pätevät kaavat $f(x, 0) = 0$ ja $f(0, y) = 0$, sillä esimerkiksi $f(x, 0) = f(x, 0.0) = 0.f(x, 0) = 0$.

ESIMERKKI 3.10. Ennen yleisen tensoritulon konstruktiota tarkastellaan tilannetta äärellisviritteisissä vapaissa moduleissa. Koska kaikki vapaat modulit saman kannan suhteen ovat isomorfisia, eikä kannan alkioiden merkinnällä ole väliä, voidaan rajoittua tyyppiä R^m oleviin summamoduleihin.

Olkoot $x = (x_1, \ldots, x_m) \in R^m$ ja $y = (y_1, \ldots, y_n) \in R^n$. Näiden alkioiden tulolta $\eta\colon (x, y) \mapsto x \otimes y$ halutaan seuraavat ominaisuudet:

(1) tulokuvauksen η on oltava bilineaarinen
(2) mikä tahansa bilineaarinen kuvaus $(x, y) \mapsto f(x, y)$ on voitava muodostaa tulosta $x \otimes y$ jonkin lineaarikuvauksen avulla.

Oletetaan, että $f\colon R^m \times R^n \to P$ on jokin bilineaarinen kuvaus R-moduliin P. Koska f on lineaarinen molempien komponenttien suhteen, nähdään, että

$$f(x,y) = \sum_{i=1}^{m} x_i f(e_i, y) = \sum_{i=1}^{m} x_i \sum_{j=1}^{n} y_j f(e_i, e_j) = \sum_{i=1}^{m}\sum_{j=1}^{n} x_i y_j f(e_i, e_j).$$

Näin ollen kuvaus f määräytyy täysin arvoista $p_{ij} = f(e_i, e_j) \in M$.

Koska kertoimien tulot $x_i y_j$ esiintyvät näemmä minkä tahansa bilineaarisen kuvauksen yhteydessä, on mahdollisimman yleisessä tapauksessa pidettävä kaikki tällaiset tulot mukana. Toisaalta arvot p_{ij} vaihtelevat kuvauksesta toiseen. Tätä ideaa seuraten määritellään alkioiden x ja y tensoritulo matriisina

$$x \otimes y = \begin{bmatrix} x_1y_1 & x_1y_2 & \cdots & x_1y_n \\ x_2y_1 & x_2y_2 & \cdots & x_2y_n \\ \vdots & & & \vdots \\ x_my_1 & x_my_2 & \cdots & x_my_n \end{bmatrix} \in R^{m\times n}.$$

Tämä matriisi ei esitä mitään lineaarikuvausta, vaan on vain tapa luetella kaikki mahdolliset tulot $x_i y_j$. Kyseistä matriisia kutsutaan joskus alkioiden x ja y *ulkotuloksi* tai *dyadituloksi*. Nyt bilineaarinen kuvaus f voidaan kirjoittaa muodossa

$$f(x,y) = \sum_{i,j} x_i y_j p_{ij} = \sum_{i,j} (x \otimes y)_{ij} p_{ij}.$$

Kuvaus f on siis yhdistelmä kuvauksesta $(x,y) \mapsto x \otimes y$, joka on bilineaarinen, sekä kuvauksesta $L\colon R^{m\times n} \to M$, $L(A) = \sum_{i,j} A_{ij} p_{ij}$, joka puolestaan on lineaarinen. Toisin sanoen $f = L \circ \eta$.

Konkreettisena esimerkkinä katsotaan, miltä reaalitason pistetulo näyttää tensoritulon avulla kirjoitettuna. Tässä tapauksessa $R = \mathbb{R}$, $m = n = 2$ ja $P = \mathbb{R}$. Pistetuloa varten tarvitaan summa koordinaattien tuloista x_1y_1 ja x_2y_2, joten määritellään lineaarikuvaus L kaavalla $L(A) = A_{11} + A_{22}$. Nyt nähdään, että

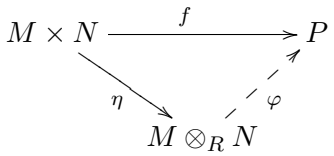
$$f(x,y) = (L \circ \eta)(x,y) = L(x \otimes y) = (x \otimes y)_{11} + (x \otimes y)_{22} = x_1y_1 + x_2y_2.$$

Tämä on tason pistetulon kaava.

Edellisessä esimerkissä tarkasteltiin vapaita moduleja, ja tensoritulo johdettiin ajatuksesta, että sen avulla voidaan määritellä mikä tahansa bilineaarinen kuvaus. Tämä on itse asiassa eräs universaaliominaisuus, joten luvun 3.2 pohdintojen nojalla sen toteuttava rakenne on yksikäsitteinen.

Vapaiden modulien tensoritulo on helppo määritellä kantojen avulla. Yleisessä tapauksessa tilanne on hankalampi. Siirretään hankaluuksia tuonnemmaksi käyttämällä konkreettisen määritelmän sijaan aluksi universaaliominaisuutta. Sanotaan siis, että R-modulien M ja N tensoritulo $M \otimes_R N$ on mikä tahansa R-moduli, jolle on määritelty R-bilineaarinen *kanoninen kuvaus* $\eta\colon M \times N \to M \otimes_R N$ ja joka toteuttaa seuraavassa esitettävän universaaliominaisuuden. Koska tällainen rakenne on isomorfiaa vaille yksikäsitteinen, voimme käyttää tätä ominaisuutta määritelmänä. Rakenteen olemassaolo todistetaan myöhemmin alaluvussa 3.4.

Ominaisuus 3.11 (Tensoritulon universaaliominaisuus). *Olkoot M, N ja P joitain R-moduleja, ja olkoon $f\colon M \times N \to P$ jokin R-bilineaarinen kuvaus. Tällöin on olemassa yksikäsitteinen R-lineaarinen kuvaus $\varphi\colon M \otimes_R N \to P$, jolle pätee $\varphi \circ \eta = f$ eli oheinen kaavio kommutoi.*



Jos kerroinrengas on selvä, voidaan modulien tensorituloa merkitä yksinkertaisesti $M \otimes N$. Kanonisen kuvauksen arvoja merkitään $\eta(x, y) = x \otimes y$. Tämä kuvaus on siis etsitty bilineaarinen tulo. Esimerkissä 3.10 määritelty vapaiden äärellisviritteisten modulien tensoritulo toteuttaa esimerkin tekstin perusteella yllä mainitun universaaliominaisuuden.

Huomaa, että kanoninen kuvaus ei välttämättä ole surjektio, joten moduli $M \otimes N$ voi sisältää alkioita, jotka eivät ole muotoa $x \otimes y$. Seuraava lemma kuitenkin osoittaa, että tätä muotoa olevat alkiot virittävät kyseisen modulin.

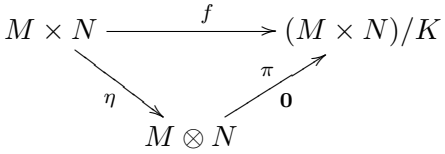
LEMMA 3.12. *Jokainen tensoritulon $M \otimes_R N$ alkio voidaan kirjoittaa äärellisenä summana $\sum_i x_i \otimes y_i$, missä $x_i \in M$ ja $y_i \in N$ kaikilla i.*

TODISTUS. Merkitään $K = \langle \operatorname{Im} \eta \rangle \subset M \otimes N$. Moduli K on siis kaikkien tuloalkioiden $x \otimes y$ virittämä alimoduli tensoritulomodulissa $M \otimes N$. Tarkoituksena on osoittaa, että $K = M \otimes N$, käyttämällä universaaliominaisuuden yksikäsitteisyysosaa.

Määritellään kuvaus $f \colon M \times N \to (M \otimes N)/K$ kaavalla

$$f(x, y) = [x \otimes y].$$

Jos kanonista surjektiota merkitään $\pi \colon M \otimes N \to (M \otimes N)/K$, huomataan, että $f = \pi \circ \eta$. Määritellään sitten nollakuvaus $\mathbf{0} \colon M \otimes N \to (M \otimes N)/K$ kaavalla $\mathbf{0}(v) = [0]$ kaikilla $v \in M \otimes N$. Koska $\operatorname{Im} \eta \subset K$, nähdään, että $f = \mathbf{0} \circ \eta$. Universaaliominaisuuden yksikäsitteisyysosasta seuraa tällöin, että $\pi = \mathbf{0}$. Tämä on mahdollista vain, jos $(M \otimes N)/K = \{[0]\}$ eli $M \otimes N = K$.



Nyt siis tiedetään, että alkioiden tensoritulot virittävät tensoritulomodulin, joten jokainen tensoritulon $M \otimes_R N$ voidaan kirjoittaa muodossa $\sum_i a_i(x_i \otimes y_i)$, missä $a_i \in R$, $x_i \in M$ ja $y_i \in N$ kaikilla i. Tensoritulon bilineaarisuutta käyttämällä saadaan

$$\sum_i a_i(x_i \otimes y_i) = \sum_i (a_i x_i) \otimes y_i.$$

Koska $a_i x_i \in M$, tämä todistaa väitteen. □

Jos modulit eivät ole vapaita, niiden tensoritulolla voi toisinaan olla odottamattomia ominaisuuksia.

ESIMERKKI 3.13. Oletetaan, että m ja n ovat keskenään jaottomia luonnollisia lukuja, ja tarkastellaan $\mathbb{Z}$-modulien $\mathbb{Z}_m$ ja $\mathbb{Z}_n$ tensorituloa. Koska m ja n ovat keskenään jaottomat, löytyy kokonaisluvut a ja b, joille pätee $am + bn = 1$. Olkoot

nyt $[x] \in \mathbb{Z}_m$ ja $[y] \in \mathbb{Z}_n$. Alkioiden tensoritulo on bilineaarinen, joten voidaan päätellä

$$\begin{aligned}[x] \otimes [y] &= (am + bn)([x] \otimes [y]) = am([x] \otimes [y]) + bn([x] \otimes [y]) \\ &= a((m[x]) \otimes [y]) + b([x] \otimes (n[y])) = a([0] \otimes [y]) + b([x] \otimes [0]) = 0.\end{aligned}$$

Kaikkien alkioiden tulot ovat siis nollia. Koska nämä tulot virittävät tensoritulon, nähdään, että $\mathbb{Z}_m \otimes \mathbb{Z}_n = \{0\}$.

Seuraavassa lauseessa luetellaan joitakin tensoritulon ominaisuuksia.

LAUSE 3.14. *Olkoot M, N ja P kolme R-modulia. Tällöin on olemassa seuraavat yksikäsitteiset R-modulien isomorfismit:*

i)	$M \otimes N \cong N \otimes M$,	*missä* $x \otimes y \mapsto y \otimes x$
ii)	$(M \otimes N) \otimes P \cong M \otimes (N \otimes P)$,	*missä* $(x \otimes y) \otimes z \mapsto x \otimes (y \otimes z)$
iii)	$(M \oplus N) \otimes P \cong (M \otimes P) \oplus (N \otimes P)$,	*missä* $(x, y) \otimes z \mapsto (x \otimes z, y \otimes z)$
iv)	$R \otimes M \cong M$,	*missä* $a \otimes x \mapsto ax$.

Viimeisessä kohdassa rengasta R ajatellaan R-modulina rengaskertolaskun suhteen.

TODISTUS. Todistetaan esimerkin vuoksi kohta i). Määritellään kuvaukset $f\colon M \times N \to N \otimes M$ ja $g\colon N \times M \to M \otimes N$ kaavoilla

$$f(x, y) = y \otimes x \quad \text{ja} \quad g(y, x) = x \otimes y \quad \text{kaikilla } x \in M \text{ ja } y \in N.$$

Nähdään helposti, että nämä kuvaukset ovat bilineaarisia, joten universaaliominaisuuden perusteella on olemassa yksikäsitteiset lineaarikuvaukset

$$\varphi\colon M \otimes N \to N \otimes M \quad \text{ja} \quad \psi\colon N \otimes M \to M \otimes N,$$

joille pätee $\varphi(x \otimes y) = f(x, y) = y \otimes x$ ja $\psi(y \otimes x) = g(y, x) = x \otimes y$ kaikilla $x \in M$ ja $y \in N$. Koska muotoa $x \otimes y$ olevat alkiot virittävät tensoritulon, on helppo päätellä, että φ ja ψ ovat toistensa käänteiskuvauksia ja siten isomorfismeja. □

Huomautus. Edellistä lausetta voi tulkita siten, että R-modulit muodostavat ikään kuin oman algebrallisen rakenteensa, joiden laskutoimitukset $\oplus$ ja $\otimes$ toteuttavat lauseen vaihdannaisuus-, liitännäisyys- ja osittelulait. Kertolaskun $\otimes$ ”neutraalialkio” on kerroinrengas R.

Seuraavassa esimerkissä tarkastellaan erästä tensoritulon sovellusta.

ESIMERKKI 3.15. *Skalaarien laajennus.* Toisinaan käytössä olevan modulin kerroinrengas ei sovellu haluttuun tarkoitukseen ja sitä täytyy muuttaa. Tyypillisesti kyse on esimerkiksi kokonaisalueen laajentamisesta kunnaksi tai vaikkapa reaalilukujen laajentamisesta kompleksiluvuiksi.

Olkoon R renkaan S alirengas. Renkaassa S voidaan määritellä renkaan R skalaarikertolasku kaavalla $a.b = ab$ kaikilla $a \in R$ ja $b \in S$, jolloin renkaasta S tulee R-moduli. Jos M on jokin toinen R-moduli, voidaan nyt muodostaa tensoritulo

$$M_S = S \otimes_R M.$$

Moduli M_S on lähtökohtaisesti R-moduli, mutta tensoritulon bilineaarisuus mahdollistaa myös renkaan S skalaarikertolaskun määrittelemisen. Tämä tehdään asettamalla kaikilla $a \in S$ ja kaikilla virittäjäalkioilla $s \otimes m \in S \otimes M$

$$a.(s \otimes m) = (as) \otimes m.$$

Sanotaan, että M_S on saatu modulista M *skalaareja laajentamalla.*

Skalaarien laajentamista voidaan käyttää esimerkiksi vapaan modulin dimension tutkimiseen. Lauseen 2.8 nojalla tiedetään, että mikäli $m = n$ joillain luonnollisilla luvuilla m ja n, vapaat modulit R^m ja R^n ovat isomorfisia. Käänteistä väitettä voidaan pitää dimension yksikäsitteisyystuloksena.

Tarkastellaan aluksi vapaita $\mathbb{Z}$-moduleja ja oletetaan, että $\mathbb{Z}^m \cong \mathbb{Z}^n$. Laajennetaan kummankin modulin kertoimet rationaaliluvuiksi muodostamalla tensoritulot $\mathbb{Z}^m_{\mathbb{Q}} = \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}^m$ ja $\mathbb{Z}^n_{\mathbb{Q}} = \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}^n$. Ei ole vaikea osoittaa, että $\mathbb{Q}$-moduli $\mathbb{Z}^m_{\mathbb{Q}}$ on isomorfinen modulin $\mathbb{Q}^m$ kanssa kaikilla m. Saadaan siis $\mathbb{Q}$-isomorfismien ketju

$$\mathbb{Q}^m \cong \mathbb{Z}^m_{\mathbb{Q}} \cong \mathbb{Z}^n_{\mathbb{Q}} \cong \mathbb{Q}^n.$$

Toisaalta, koska $\mathbb{Q}$ on kunta, modulit $\mathbb{Q}^m$ ja $\mathbb{Q}^n$ ovat vektoriavaruuksia, joiden dimensiot ovat m ja n. Vektoriavaruuden dimensio on yksikäsitteinen, mistä seuraa, että $m = n$. Siispä myös modulin $\mathbb{Z}^m$ dimensio (kannan pituus) on yksikäsitteinen.

Dimension yksikäsitteisyystulos pätee muillekin kerroinrenkaille kuin kokonaisluvuille. Yleisen kokonaisalueen tapauksessa voidaan skalaarit laajentaa vastaavaan *osamääräkuntaan*, joista kerrotaan enemmän luvussa 5.2. Mikäli kyseessä on vaihdannainen rengas R, joka ei välttämättä ole kokonaisalue, konstruktiota voidaan muuttaa seuraavasti. Valitaan renkaan R *maksimaalinen ideaali* M (olemassaolo todistetaan myöhemmin luvussa 5.3), ja käytetään kanonista surjektiota π kuntaan R/M. Tämän kuvauksen avulla voidaan määritellä renkaan R skalaarikertolasku kunnassa R/M kaavalla $r.x = \pi(r)x$. Tämän jälkeen muodostetaan tensoritulo $(R/M) \otimes_R R$ ja jatketaan kuten yllä.

Moduleita voi määritellä myös epävaihdannaisilla kerroinrenkailla. Tällöin niiden teoria kuitenkin muuttuu hieman, ja esimerkiksi skalaarien laajennus ei enää onnistu edellä esitetyllä tavalla. Epävaihdannaisen kerroinrenkaan tapauksessa onkin olemassa vapaita moduleita, jotka ovat isomorfisia, vaikka niiden kannat ovat eripituisia.

3.4. Tensoritulon olemassaolo. Osoitetaan vielä, että universaaliominaisuuden 3.11 toteuttava rakenne on aina olemassa, konstruoimalla se vapaiden modulien avulla.

Olkoot M ja N mielivaltaisia R-moduleja. Ryhdytään rakentamaan modulia, joka tulee sisältämään kaikki tulot $x \otimes y$, missä $(x, y) \mapsto x \otimes y$ on mahdollisimman yleinen bilineaarinen kuvaus. Konstruktio on analoginen luvun 1.3 esimerkin kanssa, jossa lisättiin käänteisalkioita monoidin alkioille. Ideana on lähteä liikkeelle modulista, jonka virittävät parit (x, y). Näitä pareja voidaan pitää muodollisina tuloina. Sen jälkeen samastetaan alkioita ekvivalenssirelaation avulla niin, että bilineaarisuusehdot täyttyvät: esimerkiksi jokainen pari $(x+y, z)$ samastetaan summan $(x, z) + (y, z)$ kanssa.

Tarkoitukseen soveltuu vapaa R-moduli $R^{(M\times N)}$, jota merkitään jatkossa kirjaimella C. Tämän modulin luonnollisen kannan muodostavat alkioperheet $e_{(x,y)}$, missä $(x, y) \in M \times N$. Kuten tapana on, samastetaan jokainen kanta-alkio vastaavan parin (x, y) kanssa. Tällöin C koostuu kyseisten parien lineaarikombinaatioista, joiden kertoimet ovat renkaassa R. Tarkastellaan seuraavia neljää muotoa olevia lineaarikombinaatioita, missä $x, y \in M$, $z, w \in N$ ja $a \in R$:

$$(x+y,z)-(x,z)-(y,z)$$
$$(x,z+w)-(x,z)-(x,w)$$
$$(ax,z)-a(x,z)$$
$$(x,az)-a(x,z).$$

Olkoon D se modulin C alimoduli, jonka virittävät yllä mainitut lineaarikombinaatiot. Konstruoidaan näillä merkinnöillä tekijämoduli C/D. Määritellään lisäksi kuvaus $\eta\colon M\times N\to C/D$ kaavalla $\eta(x,y)=[(x,y)]$, jolloin $\eta=\pi\circ\iota$, missä π on tekijärakenteen kanoninen surjektio ja ι vapaan modulin kanoninen injektio.

LAUSE 3.16. *Yllä määritellyt moduli C/D ja kuvaus η toteuttavat tensoritulon universaaliominaisuuden 3.11.*

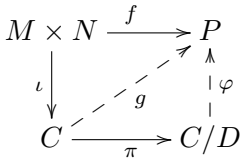
TODISTUS. Olkoon P jokin R-moduli ja $f\colon M\times N\to P$ bilineaarinen kuvaus. Koska parit $(x,y)\in M\times N$ muodostavat vapaan modulin C kannan, voidaan f laajentaa lineaarikuvaukseksi $g\colon C\to P$ yksikäsitteisesti vapaan modulin universaaliominaisuuden perusteella. Olkoon u jokin tensoritulon konstruktiossa määritellyn alimodulin D virittäjäalkio. Tällöin $g(u)=0$, koska f on bilineaarinen; esimerkiksi jos $u=(ax,y)-a(x,y)$, niin

$$g(u)=g\big((ax,y)-a(x,y)\big)=g(ax,y)-ag(x,y)=f(ax,y)-af(x,y)=0.$$

Koska $g(u)=0$ jokaisella modulin D virittäjällä u, nähdään, että $D\subset\operatorname{Ker} g$. Modulien homomorfialauseen nojalla on nyt olemassa yksikäsitteinen R-modulien homomorfismi $\varphi\colon C/D\to P$, jolle pätee $g=\varphi\circ\pi$, missä π on tekijärakenteen C/D kanoninen surjektio. Nyt voidaan päätellä

$$\varphi\circ\eta=\varphi\circ\pi\circ\iota=g\circ\iota=f.$$

Tämä todistaa universaaliominaisuuden. □



KUVA 3. Lauseen 3.16 todistukseen liittyvä kommutoiva kaavio. Yläkolmio saadaan vapaan modulin universaaliominaisuudesta ja alakolmio modulien homomorfialauseesta. Kuvaus ι on inkluusiokuvaus, π kanoninen surjektio ja $\eta=\pi\circ\iota$.

4. Algebrat

Usein modulissa halutaan määritellä modulirakenteen lisäksi sisäinen bilineaarinen kertolasku. Esimerkiksi matriiseja voidaan paitsi laskea yhteen ja kertoa luvuilla myös kertoa keskenään, ja matriisikertolasku on yhteensopiva sekä yhteenlaskun että skalaarikertolaskun kanssa. Tällaista rakennetta nimitetään algebraksi. Eri lähteissä algebran määritelmään saatetaan lisätä oletuksia kertolaskun ominaisuuksista: sen voidaan esimerkiksi vaatia olevan liitännäinen tai sillä voidaan olettaa olevan neutraalialkio. Toisinaan taas kerroinrenkaan vaaditaan olevan kunta. Tässä materiaalissa oletukset pidetään kuitenkin minimissään.

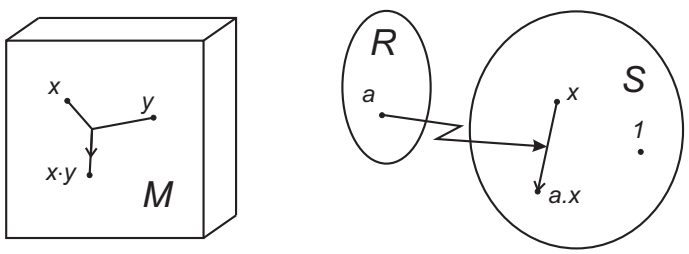
4.1. Perusominaisuudet. Aloitetaan algebran määritelmästä.

MÄÄRITELMÄ 4.1. Olkoon R vaihdannainen rengas ja olkoon A jokin R-moduli, jossa on määritelty R-bilineaarinen kertolasku $(x, y) \mapsto x \cdot y$ kaikilla $x, y \in A$. Tällaista modulia A nimitetään *R-algebraksi*. Jos kertolasku on liitännäinen tai vaihdannainen tai jos sillä on neutraalialkio, algebraa kutsutaan vastaavasti *liitännäiseksi*, *vaihdannaiseksi* tai *ykköselliseksi*.

Algebrassa on siis kolme laskutoimitusta: yhteenlasku, kertolasku ja skalaarikertolasku. Yhteenlasku on ryhmälaskutoimitus, osittelulait pätevät molemmille kertolaskuille, ja skalaarikertoimet menevät sisälle sekä summiin että tuloihin. Yleensä sekä skalaarikertolaskua että algebrakertolaskua merkitään yksinkertaisesti xy. Jos niiden sekoittuminen halutaan välttää, voidaan niille käyttää eri merkintöjä. Muun muassa seuraavat laskusäännöt pätevät missä tahansa algebrassa:

$$\begin{aligned} (a+b)x &= ax + bx & a(x \cdot y) &= (ax) \cdot y = x \cdot (ay) \\ (x+y) \cdot z &= x \cdot z + y \cdot z & -(x \cdot y) &= (-x) \cdot y = x \cdot (-y) \\ a(x+y) &= ax + ay & 0_R x &= 0_A \cdot x = x \cdot 0_A = 0_A. \\ (-1)x &= -x \end{aligned}$$

Liitännäisen ja ykkösellisen algebran kertolasku täyttää renkaan kertolaskun ehdot, joten tällaista algebraa voidaan pitää renkaana (ei välttämättä vaihdannaisena), jossa on lisäksi määritelty skalaarikertolasku. Toisaalta jokainen vaihdannainen rengas R on R-moduli oman sisäisen kertolaskunsa suhteen, ja vaihdannainen rengas R onkin liitännäinen, vaihdannainen ja ykkösellinen R-algebra.



KUVA 4. Algebra on moduli M, jossa on määritelty bilineaarinen kertolasku. Liitännäinen ja ykkösellinen algebra voidaan nähdä myös renkaana S, jossa on määritelty toisen renkaan skalaarikertolasku.

Esimerkki 4.2. Esimerkkejä algebroista:

- Olkoon R rengas. Neliömatriisien modulissa $R^{n\times n}$ voidaan määritellä tuttu matriisikertolasku, joka tekee kyseisestä modulista *matriisialgebran*.
- Polynomirenkaassa $R[X_1,\dots,X_n]$ kerroinrengas R voidaan samastaa vakiopolynomien kanssa. Tällöin skalaarikertolasku voidaan määritellä samalla säännöllä kuin polynomikertolasku, jolloin polynomirenkaasta tulee vaihdannainen *polynomialgebra*.
- Olkoon R mikä tahansa rengas, ei välttämättä vaihdannainen. Niin kuin ryhmien tapauksessa, R voidaan varustaa renkaan $\mathbb{Z}$ skalaarikertolaskulla $na = a+\cdots+a$ (n kertaa). Jokainen rengas on siis $\mathbb{Z}$-algebra. Kuten ryhmillä, tämä on ainoa tapa, jolla $\mathbb{Z}$ voi toimia renkaassa R, joten liitännäisten ja ykkösellisten $\mathbb{Z}$-algebrojen teoria vastaa renkaiden teoriaa.
- Kuten yllä todettiin, vaihdannainen rengas R on R-algebra. Yleisemmin, jos R ja S ovat vaihdannaisia renkaita ja $f\colon R\to S$ on rengashomomorfismi, voidaan S varustaa skalaarikertolaskulla $a.b = f(a)\cdot b$. Tällöin renkaasta S tulee R-algebra.
- Jos K on kunta, jokainen K-algebra on vektoriavaruus. Tällöin voidaan puhua muun muassa algebran *dimensiosta*. Jos vektoriavaruudessa on lisäksi määritelty jokin lisärakenne, kuten normi tai topologia, voidaan vastaavasti puhua normillisista tai topologisista algebroista.
- Kompleksilukujen kunta $\mathbb{C}$ on vektoriavaruutena samastettavissa tason $\mathbb{R}^2$ kanssa. Kompleksilukujen kertolasku on yhteensopiva avaruuden $\mathbb{R}^2$ vektorilaskutoimitusten kanssa, joten $\mathbb{C}$ on kaksiulotteinen $\mathbb{R}$-algebra.
- Olkoon M jokin R-moduli. Modulin M sisäisten lineaarikuvausten modulista $\mathrm{End}_R(M) = \mathrm{Hom}_R(M,M)$ tulee R-algebra, modulin M *endomorfismialgebra*, kun kertolaskuksi valitaan kuvausten yhdistäminen. Tämä yleistää ensimmäisessä kohdassa mainittua matriisialgebraa.

Algebrojen ali- ja tekijästruktuurit sekä algebrojen väliset homomorfismit määritellään niin, että ne säilyttävät sekä modulirakenteen että algebran kertolaskun.

Määritelmä 4.3. Annetun R-algebran A alimoduli B on *alialgebra*, jos se toteuttaa ehdon

$$xy\in B \qquad \text{kaikilla } x,y\in B.$$

Alimodulia I kutsutaan *ideaaliksi*, jos

$$ax\in I \quad\text{ja}\quad xa\in I \qquad \text{kaikilla } a\in A \text{ ja } x\in I.$$

Algebran A ideaalin I suhteen voidaan muodostaa *tekijäalgebra* A/I kuten minkä tahansa modulin yhteydessä. Tekijäalgebran kertolasku toteuttaa kaavan $(a+I)(b+I) = ab+I$. Se, että tekijärakenteen kertolasku on hyvin määritelty, voidaan todistaa aivan samoin kuin renkaiden yhteydessä, koska todistuksessa ei käytetä A:n kertolaskun liitännäisyyttä eikä ykkösalkiota.

Määritelmä 4.4. Olkoot A ja B jotkin kaksi R-algebraa. Lineaarikuvausta $\varphi\colon A\to B$ kutsutaan *algebrahomomorfismiksi*, jos

$$\varphi(xy) = \varphi(x)\varphi(y) \quad \text{kaikilla } x,y\in A.$$

Jos A ja B ovat ykkösellisiä, kuvaukselta φ vaaditaan lisäksi, että $\varphi(1_A) = 1_B$.

Algebrahomomorfismin ydin on ideaali, ja algebrahomomorfismeille pätee samanlainen homomorfialause kuin moduleille yleensä.

4.2. Algebrojen kannat. Jos jokin R-algebra on R-modulina vapaa, sitä kutsutaan *vapaaksi algebraksi*. Vapaalla algebralla on siis kanta. Osoittautuu, että kannan alkioiden kertotaulu määrittää täysin koko algebran kertolaskun.

LAUSE 4.5. *Olkoon A vapaa R-algebra, jolla on kanta B.*

i) Algebra A on liitännäinen, jos ja vain jos $(ab)c = a(bc)$ kaikilla kannan alkioilla $a, b, c \in B$.

ii) Alkio $e \in A$ on ykkösalkio, jos ja vain jos $ea = a$ ja $ae = a$ kaikilla $a \in B$.

iii) Algebra A on vaihdannainen, jos ja vain jos $ab = ba$ kaikilla $a, b \in B$.

TODISTUS. Tarkastellaan esimerkiksi kohtaa (iii) ja oletetaan, että kannan alkiot ovat keskenään vaihdannaisia. Olkoot $x, y \in A$ mielivaltaisia alkioita. Ne voidaan kirjoittaa kanta-alkioiden lineaarikombinaatioina muodossa $x = \sum_i x_i b_i$ ja $y = \sum_j y_j b_j$. Algebrakertolaskun bilineaarisuuden avulla saadaan

$$\begin{aligned} x \cdot y &= \sum_i x_i b_i \cdot \sum_j y_j b_j = \sum_i x_i \left(\sum_j y_j (b_i \cdot b_j) \right) = \sum_{i,j} x_i y_j (b_i \cdot b_j) \\ &= \sum_{i,j} x_i y_j (b_j \cdot b_i) = \sum_j y_j \left(\sum_i x_i (b_j \cdot b_i) \right) = \sum_j y_j b_j \cdot \sum_i x_i b_i = y \cdot x. \end{aligned}$$

Algebra on siis vaihdannainen. Huomaa, että yllä käytettiin hyväksi kerroinrenkaan vaihdannaisuutta. Väitteen toinen suunta pätee selvästi, ja muut väitteet todistetaan samalla tavalla. □

LAUSE 4.6. *Olkoon A vapaa R-algebra, jolla on kanta B. Oletetaan lisäksi, että C on jokin toinen R-algebra, ja $\varphi\colon A \to C$ on R-lineaarinen kuvaus. Tällöin kuvaus φ on algebrahomomorfismi, jos ja vain jos kaikille kannan alkioille $a, b \in B$ pätee $\varphi(ab) = \varphi(a)\varphi(b)$.*

TODISTUS. Olkoot $x = \sum_i x_i b_i$ ja $y = \sum_j y_j b_j$ algebran A mielivaltaisia alkioita. Koska kuvaus φ on lineaarinen ja algebrakertolasku on bilineaarinen, saadaan

$$\begin{aligned} \varphi(x \cdot y) &= \varphi \left(\sum_{i,j} x_i y_j (b_i \cdot b_j) \right) = \sum_{i,j} x_i y_j \, \varphi(b_i \cdot b_j) = \sum_{i,j} x_i y_j \big(\varphi(b_i) \cdot \varphi(b_j)\big) \\ &= \sum_i x_i \varphi(b_i) \cdot \sum_j y_j \varphi(b_j) = \varphi(x) \cdot \varphi(y). \end{aligned}$$

Kuvaus φ on siis algebrahomomorfismi. Väitteen toinen suunta pätee selvästi. □

Olkoon A vapaa R-algebra, jolla on kanta B. Jokainen alkioiden $b_i, b_j \in B$ tulo voidaan kirjoittaa kanta-alkioiden lineaarikombinaationa muodossa

$$b_i \cdot b_j = \sum_k c_{ij}^k b_k \quad (k \text{ on yläindeksi, ei potenssi}).$$

Vakioita $c_{ij}^k \in R$ kutsutaan kyseisen algebran *rakennevakioiksi kannan B suhteen*. Kertolaskun bilineaarisuudesta seuraa, että rakennevakioiden tunteminen riittää algebran kertolaskun määrittämiseen, sillä

$$\sum_i x_i b_i \cdot \sum_j y_j b_j = \sum_{i,j} x_i y_j (b_i \cdot b_j) = \sum_{i,j,k} x_i y_j c_{ij}^k b_k. \qquad (*)$$

Yllä oleva kaava antaa kannan alkioista muodostettujen lineaarikombinaatioiden tulon yleisessä tapauksessa. Kääntäen, rakennevakioiden perhe (c_{ij}^k) voidaan valita kullakin i ja j täysin mielivaltaisesti, ja kaava $(*)$ määrittelee tällöin erään bilineaarisen kertolaskun. Kiteytetään nämä havainnot seuraavaan lauseeseen.

LAUSE 4.7. *Olkoon M vapaa R-moduli, jolla on kanta $B = \{b_i\}_{i\in I}$. Olkoon lisäksi $(c_{ij}^k)_{k\in I}$ jokin äärelliskantajainen perhe renkaan R alkioita kaikilla $i, j \in I$. Tällöin modulissa M voidaan määritellä sellainen yksikäsitteinen R-bilineaarinen kertolasku, jonka rakennevakioiksi kannan B suhteen tulevat vakiot c_{ij}^k.*

ESIMERKKI 4.8. Tarkastellaan kaksiulotteista reaaliavaruutta $\mathbb{R}^2$. Merkitään tämän avaruuden luonnollisen kannan vektoreita $1 = (1, 0)$ ja $i = (0, 1)$ ja määritellään kantavektorien kertotaulu seuraavasti:

$\cdot$	1	i
1	1	i
i	i	-1

Kertotaulun perusteella syntyvä $\mathbb{R}$-algebra on selvästi ykkösellinen, liitännäinen ja vaihdannainen. Tällä tavoin määritellään *kompleksilukualgebra*, joka on siis kaksiulotteinen reaalikertoiminen algebra. Kompleksialgebran rakennevakiot on lueteltu alla olevassa taulukossa.

(x, y)	$(1, 1)$	$(1, i)$	$(i, 1)$	(i, i)
c_{xy}^1	1	0	0	-1
c_{xy}^i	0	1	1	0

Koska kompleksialgebra on vaihdannainen ja jokaisella nollasta poikkeavalla alkiolla on käänteisalkio, kyseessä on kunta.

ESIMERKKI 4.9. *Kvaterniot.* William Hamilton[1] löysi vuonna 1843 kertotaulun neliulotteiselle reaalikertoimiselle algebralle $\mathbb{H}$, jonka hän risti kvaternioiksi[2]. Erityistä kvaternioalgebrassa on se, että kaikilla alkioilla on käänteisalkiot, joten jakolasku on mahdollista. Hamilton oli työskennellyt kauan löytääkseen kolmiulotteisen reaalialgebran, joka laajentaisi kompleksilukuja, kun hän ollessaan kävelyllä Dublinissa äkkiä tajusi saavansa ideansa toimimaan, jos lisäisi mukaan neljännen ulottuvuuden. Hän innostui keksinnöstään niin, että kaiversi siltä seisomalta kvaterniokannan kertolaskusäännöt Broughamin (nykyisin Broomin) sillan kiveykseen.

Jos kvaternioalgebran kantaa merkitään symboleilla 1, i, j ja k, kertotaulu näyttää tältä:

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Kertotaulusta nähdään, että kvaternioalgebra on liitännäinen ja ykkösellinen. Lisäksi jokaisella nollasta poikkeavalla alkiolla on käänteisalkio: esimerkiksi alkion

[1] William Rowan Hamilton, 1805–1865, irlantilainen fyysikko ja matemaatikko

[2] quaternio = nelikkö (lat.)

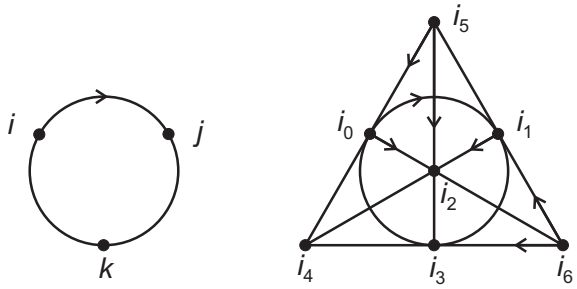
$1 + j$ käänteisalkio on $\frac{1}{2}(1 - j)$, sillä

$$(1 + j) \cdot \frac{1}{2}(1 - j) = \frac{1}{2}(1 - j + j - j^2) = 1.$$

Kvaternioalgebra ei kuitenkaan ole vaihdannainen, joten se ei ole kunta. Sen sijaan sitä nimitetään *jakoalgebraksi*. Kuten kompleksialgebrassa, jokainen ykkösalkiosta poikkeava kanta-alkio on luvun -1 neliöjuuri.

Kvaternioita käytettiin kolmiulotteisen reaaliavaruuden geometrian hahmottamiseen ennen vektoriavaruuden käsitteen syntyä; kvaternioiden avulla voidaan muun muassa muotoilla piste- ja ristitulo sekä kolmiulotteisen avaruuden kierrot. Hamiltonin alkuperäisenä tavoitteena olikin keksiä algebra, jossa kolmiulotteisia kiertoja voitaisiin kuvata kertolaskulla samaan tapaan kuin kompleksitasossa yksikköympyrän alkioilla kertominen kuvaa kaksiulotteisia kiertoja.

Normillinen algebra on sellainen, jonka taustalla olevassa vektoriavaruudessa voidaan määritellä kertolaskun kanssa yhteensopiva normi. (Esimerkiksi kompleksilukujen tavallinen normi on $|x + yi| = \sqrt{x^2 + y^2}$.) Voidaan osoittaa, että normillisia reaalisia jakoalgebroja on isomorfiaa vaille olemassa vain neljä: reaaliluvut $\mathbb{R}$, kompleksiluvut $\mathbb{C}$, kvaterniot $\mathbb{H}$ sekä *oktonioalgebra* $\mathbb{O}$, joka on kahdeksanulotteinen epäliitännäinen jakoalgebra. Jos oktonioalgebran kantaa merkitään $\{1, i_0, \ldots, i_6\}$, niin $\pm i_k$ on luvun -1 neliöjuuri jokaisella k.



KUVA 5. Kvaternioiden ja oktonioiden kertotaulut

Kvaternioiden ja oktonioiden kanta-alkioiden kertotaulut käyvät ilmi oheisesta kuvasta. Kahden kanta-alkion tulo on kolmas samalta viivalta löytyvä alkio. Nuolen suunta kertoo tulon etumerkin. Esimerkiksi kvaternioilla pätee $ji = -k$, ja oktonioilla on voimassa $i_0 i_1 = i_3$ ja $i_1 i_4 = -i_2$.

4.3. Ryhmä- ja monoidialgebrat. Olkoon $(G, *)$ jokin ryhmä ja olkoon R vaihdannainen rengas. Tarkastellaan vapaata R-modulia $R^{(G)}$. Tämän modulin luonnollisen kannan muodostavat alkiot e_g, missä $g \in G$, ja kukin näistä voidaan samastaa ryhmän alkion g kanssa. Koska kannan alkiot tällöin kuuluvat ryhmään G, niille voidaan määritellä luonnollinen kertolasku.

MÄÄRITELMÄ 4.10. *Ryhmäalgebra RG* on vapaa R-moduli $R^{(G)}$ varustettuna bilineaarisella kertolaskulla, joka toteuttaa ehdon $g \cdot h = g * h$ kaikilla kannan alkioilla $g, h \in G$.

Kahden ryhmäalgebran mielivaltaisen jäsenen tulo on

$$\sum_i a_i g_i \cdot \sum_j b_j h_j = \sum_{i,j} a_i b_j (g_i * h_j).$$

Ryhmäalgebrat ovat liitännäisiä ja ykkösellisiä, mikä seuraa ryhmäkertolaskun ominaisuuksista ja lauseesta 4.5. Samanlainen konstruktio voidaan tehdä lähtien liikkeelle ryhmän sijaan monoidista, jolloin tuloksena on monoidialgebra.

Esimerkki 4.11. Ryhmien esitysteoriassa tutkitaan homomorfismeja annetulta ryhmältä G jonkin vektoriavaruuden V kääntyvien lineaarikuvausten ryhmään $\mathrm{GL}(V)$. Tällaista homomorfismia kutsutaan ryhmän *esitykseksi* avaruudessa V. Jokainen ryhmän alkio siis esitetään matriisina, jolloin ryhmän tutkimiseksi päästään käyttämään lineaarialgebran käsitteitä, kuten ominaisarvoja, dimensiota jne. Esitysten avulla saadaan paljon tietoa ryhmän rakenteesta, ja esitysteoria on jatkuvasti tutkituimpia ryhmäteorian aloja.

Nykyisin on tapana sisällyttää esitysteoria modulien teoriaan käyttämällä hyväksi ryhmäalgebran käsitettä. Tarkastellaan jotakin ryhmää G ja sen esityksiä K-kertoimisissa vektoriavaruuksissa. Koska ryhmäalgebra KG on liitännäinen ja ykkösellinen, sitä voidaan pitää renkaana, ja jokaista ryhmän G esitystä vastaa eräs KG-moduli. On kuitenkin huomattava, että KG ei ole vaihdannainen rengas, ellei G ole vaihdannainen ryhmä, emmekä ole käsitelleet moduleja epävaihdannaisen kerroinrenkaan suhteen. Tällaisessa tapauksessa moduli voidaan kuitenkin määritellä tavalliseen tapaan, kunhan mainitaan erikseen, suoritetaanko skalaarikertolasku vasemmalta vai oikealta puolelta.

Olkoon V siis jokin K-kertoiminen vektoriavaruus, ja olkoon $\varphi\colon G \to \mathrm{GL}(V)$ ryhmähomomorfismi, jolloin $\varphi(g)$ on kääntyvä lineaarikuvaus jokaisella $g \in G$. Määritellään avaruuteen V renkaan KG kanta-alkioiden vasemmanpuoleinen skalaarikertolasku kaavalla

$$gx = \varphi(g)(x) \quad \text{kaikilla } g \in G \text{ ja } x \in V.$$

Kun tämä skalaarikertolasku laajennetaan lineaarisesti koko renkaan KG skalaarikertolaskuksi, avaruudesta V tulee vasen KG-moduli. Vastaavuus ryhmän G esitysten ja KG-modulien välillä on bijektiivinen.

4.4. Polynomialgebrat. Yhden muuttujan polynomit voidaan määritellä vapaina moduleina, kuten tehtiin esimerkissä 3.3. Polynomeja voidaan kuitenkin myös kertoa toisillaan, jolloin ne muodostavat algebran. Mikään ei myöskään pakota rajoittumaan konstruktiossa yhteen muuttujaan. Tässä alaluvussa konstruoidaan yleinen polynomialgebra ja todistetaan polynomeihin liittyvä universaaliominaisuus.

Olkoon R vaihdannainen rengas ja $I = \{1, 2, \ldots, n\}$ äärellinen indeksijoukko. Ruvetaan määrittelemään polynomialgebraa $R[X_1, \ldots, X_n]$, joka tulee koostumaan R-kertoimisista n:n tuntemattoman polynomeista. Tarkastellaan ensin tulomonoidia $M_n = \mathbb{N}^n$, joka koostuu jonoista $\nu = (\nu_1, \ldots, \nu_n)$, missä $\nu_i \in \mathbb{N}$ jokaisella i. Jonojen yhteenlasku määritellään pisteittäin.

Monoidi M_n sisältää konstruoitavan polynomialgebran monomit. Ryhdytään kirjoittamaan mielivaltainen alkio $\nu = (\nu_1, \ldots, \nu_n) \in M_n$ muodossa

$$X^\nu = X_1^{\nu_1} X_2^{\nu_2} \cdots X_n^{\nu_n}.$$

Jokaisesta jonon ν komponentista ν_i tulee siis tuntemattoman X_i eksponentti. Jos $\nu_i = 1$ jollain i, voidaan eksponentti jättää merkitsemättä, ja jos $\nu_i = 0$, voidaan koko tuntematon X_i^0 jättää pois. Tällöin $X^{e_i} = X_i$, missä $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ (ykkönen i:nnellä paikalla). Kahden jonon μ ja ν summa on tällä tavoin merkittynä

$$\mu + \nu = X^{\mu+\nu} = X_1^{\mu_1+\nu_1} X_2^{\mu_2+\nu_2} \cdots X_n^{\mu_n+\nu_n}.$$

Esimerkiksi $(2,1,0)+(0,1,1)=X_1^2X_2^2X_3$.

Tarkastellaan sitten vapaata modulia $R^{(M_n)}$, jonka alkioina ovat monoidin M_n alkioiden R-kertoimiset lineaarikombinaatiot

$$\sum_\nu a_\nu X^\nu, \quad \text{missä } a_\nu \in R \text{ ja } \nu \in M_n.$$

Algebrakertolaskun määrittelemiseksi riittää määritellä se kanta-alkioilla. Tämä puolestaan tehdään monoidin M_n laskutoimituksen avulla:

$$X^\mu \cdot X^\nu = X^{\mu+\nu} = X_1^{\nu_1+\mu_1}\cdots X_n^{\nu_n+\mu_n}.$$

Tällöin kahden yleisen alkion tulo on

$$\sum_\nu a_\nu X^\nu \cdot \sum_\mu b_\mu X^\mu = \sum_{\nu,\mu} a_\nu b_\mu X^{\nu+\mu}.$$

Konstruktio vastaa luvussa 4.3 esiteltyä monoidialgebran konstruktiota. Huomaa, että algebraan siirryttäessä monoidin yhteenlasku muuttui algebran kertolaskuksi ja samalla monoidin nolla-alkiosta $X^0=(0,\dots,0)$ tuli algebran ykkösalkio.

MÄÄRITELMÄ 4.12. Edellä konstruoitu monoidialgebra $R^{(M_n)}$ on R-kertoiminen n:n tuntemattoman *polynomialgebra*. Se on liitännäinen, vaihdannainen ja ykkösellinen R-algebra, ja sitä merkitään $R[X_1,\dots,X_n]$. Kanta-alkioita X^ν kutsutaan *monomeiksi*.

Polynomialgebra koostuu monomien lineaarikombinaatioista. Tyhjä lineaarikombinaatio on algebran nolla-alkio, ja sitä nimitetään *nollapolynomiksi*. Ykkösalkio on monoidin M_n nolla-alkio $X^0=(0,\dots,0)$. Monomin X^ν *aste* on eksponenttien summa $\sum_i \nu_i$, ja polynomin aste on suurin sen sisältämän monomin aste. Nollapolynomin asteeksi määritellään $-\infty$. Esimerkiksi monomin $X_2^5X_3$ aste on $5+1=6$. Polynomin f astetta merkitään $\deg(f)$.

Polynomia, jonka aste on 0 tai $-\infty$, nimitetään *vakiopolynomiksi* tai *vakioksi*. Kuvaus $\eta\colon a\mapsto aX^0$ on bijektio renkaan R ja vakiopolynomien välillä, ja sen avulla kerroinrengas voidaan samastaa vakioiden kanssa. Kuvaus η on myös rengashomomorfismi, mistä seuraa, että renkaan skalaarikertolasku yhtyy vakiopolynomeilla kertomiseen. Erityisesti η kuvaa renkaan ykkösalkion algebran ykkösalkioksi.

Polynomialgebralle pätee seuraava universaaliominaisuus.

LAUSE 4.13 (Polynomialgebran universaaliominaisuus.). *Olkoon R vaihdannainen rengas ja A jokin liitännäinen, vaihdannainen ja ykkösellinen R-algebra. Olkoon lisäksi $(x_1,\dots,x_n)$ jono A:n alkioita. Tällöin on olemassa yksikäsitteinen algebrahomomorfismi $\varphi\colon R[X_1,\dots,X_n]\to A$, jolle pätee $\varphi(X_i)=x_i$ jokaisella i.*

TODISTUS. Koska algebra A on liitännäinen ja ykkösellinen, se on kertolaskunsa suhteen monoidi. Määritellään kuvaus $g\colon M_n\to A$ kaavalla

$$g(X^\nu)=x_1^{\nu_1}\cdots x_n^{\nu_1}.$$

Kuvaus g on monoidihomomorfismi monoidilta M_n algebran A multiplikatiiviselle monoidille, sillä algebran A vaihdannaisuutta käyttäen saadaan

$$\begin{aligned} g(X^\mu\cdot X^\nu) &= g(X^{\mu+\nu}) = x_1^{\mu_1+\nu_1}\cdots x_n^{\mu_n+\nu_n} \\ &= (x_1^{\mu_1}\cdots x_n^{\mu_n})\cdot(x_1^{\nu_1}\cdots x_n^{\nu_n}) = g(X^\mu)\cdot g(X^\nu) \end{aligned}$$

ja $g(X^0)=x_1^0\cdots x_n^0=1_A$.

Koska $R[X_1, \ldots, X_n]$ on vapaa moduli, jonka kanta on M_n, vapaan modulin universaaliominaisuudesta seuraa, että on olemassa yksikäsitteinen R-lineaarinen kuvaus $\varphi\colon R[X_1, \ldots, X_n] \to A$, jolle pätee $\varphi(X^\nu) = g(X^\nu)$ kaikilla $X^\nu \in M_n$. Lauseen 4.6 nojalla lineaarikuvaus φ on lisäksi algebrahomomorfismi, sillä kannan alkioilla pätee

$$\varphi(X^\nu \cdot X^\mu) = g(X^\nu \cdot X^\mu) = g(X^\nu) \cdot g(X^\mu) = \varphi(X^\nu) \cdot \varphi(X^\mu).$$

Lisäksi jokaisella i pätee $\varphi(X_i) = g(X^{e_i}) = x_i$.

Olkoon sitten φ' toinen algebrahomomorfismi, joka toteuttaa lauseen oletukset. Koska φ' säilyttää kertolaskun, täytyy päteä

$$\varphi'(X^\nu) = \varphi'(X_1^{\nu_1} \cdots X_n^{\nu_n}) = \varphi'(X_1)^{\nu_1} \cdots \varphi'(X_n)^{\nu_n} = x_1^{\nu_1} \cdots x_n^{\nu_1}.$$

Näin ollen kuvaukset φ' ja φ yhtyvät monoidin M_n alkioilla, joten lineaarikuvauksen φ yksikäsitteisyydestä seuraa $\varphi' = \varphi$. □

MÄÄRITELMÄ 4.14. Edellisen lauseen kuvausta φ kutsutaan algebran A alkioihin $x_1, \ldots, x_n$ liittyväksi *sijoitushomomorfismiksi*. Polynomin $f = \sum_\nu a_\nu X^\nu$ arvo sijoitushomomorfismissa on

$$\varphi(f) = \sum_\nu a_\nu x_1^{\nu_1} \cdots x_n^{\nu_n}.$$

Tätä arvoa merkitään myös $f(x_1, \ldots, x_n)$.

Sijoitushomomorfismin avulla voidaan määritellä algebran A *polynomifunktio* $(x_1, \ldots, x_n) \mapsto f(x_1, \ldots, x_n)$. Tässä kohdassa on syytä huomata ero polynomin ja sen määräämän polynomifunktion välillä. Olkoon esimerkiksi $f = X^2 + X \in \mathbb{Z}_2[X]$. Nyt f ei ole nollapolynomi, mutta $f(x) = 0$ kaikilla $x \in \mathbb{Z}_2$, eli f:n määräämä funktio algebrassa $\mathbb{Z}_2$ on nollafunktio.

Jos $\varphi\colon R[X] \to A$ on alkioon $\alpha \in A$ liittyvä sijoitushomomorfismi ja $\varphi(f) = 0$, alkiota α nimitetään polynomin f *juureksi*. Polynomifunktion käsitteen avulla ilmaistuna α on polynomin f juuri, jos se on funktion $x \mapsto f(x)$ nollakohta eli $f(\alpha) = 0$.

Tässä luvussa määriteltiin polynomit äärellisen muuttujajoukon $\{X_1, \ldots, X_n\}$ suhteen. On myös mahdollista valita indeksijoukko I äärettömäksi. Tällöin monomimonoidi $M_I = \mathbb{N}^{(I)}$ koostuu alkioperheistä, joissa on vain äärellinen määrä nollasta poikkeavia alkioita. Muuten konstruktio etenee aivan samalla tavalla.

Renkaat

Tässä osassa tutustutaan joihinkin renkaiden ominaisuuksiin ja niiden sovelluksiin algebrassa. Ensimmäisessä luvussa kerrataan ja syvennetään kuntien ja kokonaisalueiden käsitteitä ja toisessa tarkastellaan jaollisuuden teoriaa kokonaisalueissa.

5. Kunnat ja kokonaisalueet

Kunnat ja kokonaisalueet ovat tuttuja rakenteita aiemmilta algebran kursseilta. Molemmat ovat vaihdannaisia ja epätriviaaleja renkaita. Kunnissa jokaisella nollasta poikkeavalla alkiolla on käänteisalkio, ja kokonaisaluetta puolestaan määrittelee nollanjakajien puuttuminen. Perusesimerkki kunnasta on rationaalilukujen joukko $\mathbb{Q}$ ja kokonaisalueesta kokonaislukujen joukko $\mathbb{Z}$, mistä kokonaisalueet ovat saaneet nimensäkin.

Tässä luvussa todetaan, että sekä kunnat että kokonaisalueet esiintyvät tekijärenkaina tietynlaisten ideaalien suhteen. Lisäksi esitellään, miten kokonaisalueeseen voidaan lisätä käänteisalkioita, minkä seurauksena kokonaisalueesta tulee aina jonkin kunnan alirengas.

5.1. Kunnat ja kokonaisalueet tekijärakenteina. Tekijärakenteita on lähestyttävä ideaalien kautta. Todetaan aluksi, että tekijärenkaan R/I ideaalit vastaavat yksi yhteen sellaisia renkaan R ideaaleja, jotka sisältävät ideaalin I. Suoraviivainen todistus jätetään lukijan harjoitustehtäväksi.

LEMMA 5.1. *Olkoon R rengas, jolla on ideaali I. Merkitään kanonista surjektiota $\pi\colon R \to R/I$, jolloin siis $\pi(x) = x + I$.*

(1) Jos J on renkaan R ideaali ja $I \subset J$, niin joukko $\pi J = \{x + I \mid x \in J\}$ on tekijärenkaan R/I ideaali.
(2) Jos $\mathcal{J}$ on tekijärenkaan R/I ideaali, niin joukko $\pi^{-1}\mathcal{J} = \{x \mid x + I \in \mathcal{J}\}$ on renkaan R ideaali, jolle pätee $I \subset \pi^{-1}\mathcal{J}$.

Edellistä lemmaa voi tarkastella sivuluokkien näkökulmasta seuraavasti. Tekijärenkaan ideaali $\mathcal{J}$ sisältää alkioinaan ideaalin I sivuluokkia. Alkukuvassa $\pi^{-1}\mathcal{J}$ nämä sivuluokat ”avataan”, ja niiden sisältämät alkiot kootaan uudeksi joukoksi. Joukko-opillisesti kyseessä on sivuluokkien yhdiste: $\pi^{-1}\mathcal{J} = \bigcup \mathcal{J}$. Toisaalta ideaalin $J \subset R$ kuvajoukossa πJ kaikki joukon J sisältämät sivuluokat yksinkertaisesti ”paketoidaan” tekijärenkaan alkioiksi.

Kunnat voidaan karakterisoida niiden sisältämien ideaalien avulla. Seuraava tulos on tuttu aiemmilta algebran kursseilta.

LAUSE 5.2. *Vaihdannainen rengas R on kunta, jos ja vain jos sillä on täsmälleen kaksi ideaalia: $\{0\}$ ja R.*

Tämän lauseen nojalla vaihdannaisen renkaan R tekijärengas R/I on kunta, mikäli sillä on täsmälleen kaksi ideaalia. Toisaalta jokainen tekijärenkaan ideaali vastaa lemman 5.1 nojalla sellaista renkaan R ideaalia, joka sisältää ideaalin I. Ideaalin I sisältäviä renkaan R ideaaleja saisi siis olla vain kaksi, jotta tekijärengas R/I olisi kunta. Näihin ideaaleihin on lisäksi luettava I ja R. Tämä on ideaalin I erityisominaisuus.

MÄÄRITELMÄ 5.3. Renkaan R ideaali I on *maksimaalinen*, jos $I \neq R$ ja millään ideaalilla J ei päde $I \subsetneq J \subsetneq R$.

Edellä olevan pohdiskelun seurauksena saadaan seuraava lause. Todistuksen yksityiskohdat jätetään lukijan harteille.

LAUSE 5.4. *Vaihdannaisen renkaan R tekijärengas R/I on kunta, jos ja vain jos I on renkaan R maksimaalinen ideaali.*

Tutkitaan sitten nollanjakajia. Tekijärenkaassa R/I nolla-alkiona toimii ideaali I. Sivuluokka $a + I$ on tekijärenkaassa R/I nollanjakaja, jos $a + I \neq I$ ja löytyy jokin $b + I \neq I$, jolle pätee $ab + I = I$. Kun sivuluokkien yhtäsuuruudet kirjoitetaan toisin, tämä tarkoittaa sitä, että $a \notin I$ ja $b \notin I$, mutta $ab \in I$. Tämän estämiseksi laaditaan seuraava määritelmä.

MÄÄRITELMÄ 5.5. Renkaan R ideaali I on *alkuideaali*, jos $I \neq R$ ja kaikilla $a, b \in R$ ehdosta $ab \in I$ seuraa $a \in I$ tai $b \in I$.

Jälleen kerran saadaan suoraan tekijärakenteita koskeva tulos.

LAUSE 5.6. *Vaihdannaisen renkaan R tekijärengas R/I on kokonaisalue, jos ja vain jos I on renkaan R alkuideaali.*

Siitä, että kunnat ovat kokonaisalueita, seuraa vastaava yhteys ideaalien välille.

LAUSE 5.7. *Jokainen maksimaalinen ideaali on alkuideaali.*

ESIMERKKI 5.8. Alkuideaalit liittyvät läheisesti alkulukuihin. Palautetaan mieleen, että kokonaislukujen renkaassa kaikki ideaalit ovat yhden alkion virittämiä. Ne ovat siis muotoa $\langle n \rangle$ jollain $n \in \mathbb{Z}$, ja koska $\mathbb{Z}$ on vaihdannainen, tällainen ideaali voidaan kirjoittaa muodossa $\langle n \rangle = \{kn \mid k \in \mathbb{Z}\}$. Nähdään, että $a \in \langle n \rangle$, jos ja vain jos a on jaollinen luvulla n. (Luku n voi olla myös nolla, mutta ainoa nollalla jaollinen luku on nolla itse.)

Oletetaan aluksi, että $n \neq 0$. Jos $ab \in \langle n \rangle$ joillain $a, b \in \mathbb{Z}$, niin n jakaa tulon ab. Jos n on alkuluku, sen täytyy Eukleideen lemman nojalla jakaa jompikumpi luvuista a ja b. Siispä jompikumpi luvuista a ja b on ideaalissa $\langle n \rangle$. Täten ideaali $\langle n \rangle$ on alkuideaali, jos n on alkuluku.

Alkulukujen virittämät ideaalit eivät kuitenkaan ole ainoita renkaan $\mathbb{Z}$ alkuideaaleja, sillä myös nollaideaali $\{0\} = \langle 0 \rangle$ on sellainen. Tämä nähdään helposti siitä, että $\mathbb{Z}$ on kokonaisalue. Kääntäen, jos luku n ei ole alkuluku eikä nolla, voidaan kirjoittaa $n = ab$, missä $a, b \in \mathbb{Z} \setminus \{1, -1, 0\}$. Tällöin $ab \in \langle n \rangle$, mutta toisaalta $a \notin \langle n \rangle$ ja $b \notin \langle n \rangle$. Siispä $\langle n \rangle$ on alkuideaali, jos ja vain jos n on alkuluku tai nolla.

Tarkastellaan vielä lähemmin renkaan $\mathbb{Z}$ alkuideaaleja. Jos p on alkuluku, tekijärengas $\mathbb{Z}/\langle p \rangle = \mathbb{Z}_p$ on äärellinen kunta. Ideaali $\langle p \rangle$ on siis lauseen 5.4 perusteella myös maksimaalinen. Toisaalta nollaideaali ei ole maksimaalinen, sillä se sisältyy

jokaiseen ideaaliin $\langle n \rangle$. Sama asia voitaisiin todeta myös huomaamalla, että tekijärengas $\mathbb{Z}/\langle 0 \rangle$ ei ole kunta, sillä se on isomorfinen renkaan $\mathbb{Z}$ kanssa. Voidaan siis päätellä, että nollaideaali on renkaan $\mathbb{Z}$ ainoa alkuideaali, joka ei ole maksimaalinen.

5.2. Kokonaisalueen osamääräkunta. Vaikka kokonaisalueissa kaikki alkiot eivät välttämättä ole kääntyviä, käänteisalkiot ovat kuitenkin olemassa jossain laajemmassa rakenteessa, ja toisinaan tarkastelu kannattaa siirtää tähän laajempaan rakenteeseen.

Esimerkki 5.9. Tutkitaan esimerkin vuoksi kokonaislukuyhtälöä $2x = 6$. Eräs ratkaisu on $x = 3$. Koska kyse on kokonaisalueesta, ratkaisun yksikäsitteisyys voidaan osoittaa kirjoittamalla $2x = 2 \cdot 3$ ja supistamalla kerroin 2 molemmilta puolilta päättelyllä

$$2x = 2 \cdot 3 \quad \Rightarrow \quad 2(x-3) = 0 \quad \Rightarrow \quad x - 3 = 0 \quad \Rightarrow \quad x = 3.$$

Tämä päättely voitiin kuitenkin suorittaa vasta, kun eräs ratkaisu yhtälölle oli löytynyt. Yhtälöä voidaan kuitenkin tarkastella myös kunnassa $\mathbb{Q}$, jonka alirengas $\mathbb{Z}$ on. Kunnassa kaikilla alkioilla on käänteisalkiot, joten voidaan päätellä

$$2x = 6 \quad \Rightarrow \quad \frac{1}{2} \cdot 2x = \frac{1}{2} \cdot 6 \quad \Rightarrow \quad x = 3.$$

Löytynyt ratkaisu on renkaassa $\mathbb{Z}$, ja se toteuttaa alkuperäisen yhtälön. Lisäksi ratkaisu on yksikäsitteinen kunnassa $\mathbb{Q}$, ja siksi sen on oltava yksikäsitteinen myös pienemmässä renkaassa $\mathbb{Z}$.

Esimerkin kaltainen ”kunnan lainaaminen” onnistuu itse asiassa kaikilla kokonaisalueilla. Sitä käytettiin hyväksi myös skalaareja laajennettaessa esimerkissä 3.15. Tarvittava kunta saadaan yleisessä tapauksessa aikaan lisäämällä kokonaisalueeseen käänteisalkiota kaikille nollasta poikkeavilla alkioille. Menetelmä vastaa rationaalilukujen konstruointia kokonaislukujen renkaasta lähtien, ja samaa menetelmää käytettiin itse asiassa jo luvun 1.3 esimerkissä, jossa lisättiin käänteisalkioita monoidiin.

Olkoon R kokonaisalue. Merkitään $S = R \setminus \{0\}$. Karteesinen tulo $R \times S$ sisältää pareja (a, b), joita voidaan pitää muodollisina osamäärinä. Tietyt osamäärät halutaan samastaa, joten määritellään tulojoukkoon $R \times S$ relaatio ehdolla

$$(a_1, b_1) \sim (a_2, b_2), \quad \text{jos} \quad a_1 b_2 = a_2 b_1.$$

On suoraviivaista tarkistaa, että kyseinen relaatio on ekvivalenssirelaatio. Tekijärakenteen $(R \times S)/\!\sim$ alkioita nimitetään *osamääriksi* ja niitä merkitään murtolukumuodossa $[(a, b)]_\sim = a/b$. Seuraavan lauseen suoraviivainen todistus sivuutetaan.

Lause 5.10. *Seuraavat ehdot pätevät tekijärakenteelle $K = (R \times S)/\!\sim$:*

a) Kaavat $(a/b) + (c/d) = (ad + cb)/(bd)$ ja $(a/b)(c/d) = (ac)/(bd)$ määrittelevät yhteen- ja kertolaskun, jotka eivät riipu ekvivalenssiluokkien edustajien valinnasta.
b) Joukko K on vaihdannainen rengas a)-kohdan laskutoimitusten suhteen.
c) Kuvaus $\eta\colon R \to K$, $a \mapsto a/1$ on injektiivinen rengashomomorfismi.
d) Jos $a/b \in K$ ei ole nolla-alkio, sillä on käänteisalkio b/a.

Tekijärakennetta K nimitetään kokonaisalueen R *osamääräkunnaksi*. Tavallisesti rengas R samastetaan kunnan K alirenkaan kanssa kuvauksen η välityksellä. Esimerkiksi kokonaisalueen $\mathbb{Z}$ osamääräkunta on $\mathbb{Q}$, ja jokainen kokonaisluku n samastetaan osamäärän $n/1$ kanssa. Osamääräkunnan olemassaolo antaa uuden karakterisoinnin kokonaisalueelle: *rengas on kokonaisalue, jos ja vain jos se on jonkin kunnan alirengas.*

Mikäli vaihdannainen rengas ei ole kokonaisalue, osamääräkunnan konstruktio ei onnistu sellaisenaan eikä kaikille alkioille saada käänteisalkioita. Tämä näkyy välittömästi siitä, että yhteenlaskun ja kertolaskun määrittelevät kaavat eivät toimi oikein nollanjakajien läsnä ollessa. (Voidaan myös melko helposti todeta, että nämä ovat ainoat kaavat, joilla saadaan aikaan vaihdannainen rengas, jossa alkion a/b käänteisalkio on b/a.)

Hieman yleisempi konstruktio on kuitenkin mahdollinen. Siinä oletetaan, että joukko S on mikä tahansa kertolaskun suhteen suljettu joukko renkaan R alkioita. Ensinnäkin edellä määriteltyä relaatiota $\sim$ on muokattava, jotta se säilyisi transitiivisena:

$$(a_1, b_1) \sim (a_2, b_2), \quad \text{jos} \quad c(a_1 b_2 - a_2 b_1) = 0 \quad \text{jollain } c \in S.$$

Edellä mainitut kaavat määrittelevät nyt vaihdannaisen renkaan, jossa joukon S alkiot ovat kääntyviä. Kuvaus η ei välttämättä ole injektiivinen, joten alkuperäistä rengasta ei voida pitää syntyvän rakenteen alirenkaana. Itse asiassa syntyvä rengas voi olla jopa nollarengas. Injektiivisyys kuitenkin pelastuu, jos joukkoon S valitaan vain nollasta poikkeavia alkioita, jotka eivät ole nollanjakajia.

Tällaista yleisempää konstruktiota nimitetään renkaan *lokalisoinniksi* joukon S suhteen. Nimitys tulee algebrallisesta geometriasta, jossa lokalisointi mahdollistaa keskittymisen käyrien ja pintojen paikallisiin ominaisuuksiin.

5.3. Maksimaalisen ideaalin olemassaolo. Aiempana nähtiin, että vaihdannaisesta renkaasta saadaan kunta muodostamalla sen tekijärengas maksimaalisen ideaalin suhteen. Lisäksi mainittiin, että jokainen maksimaalinen ideaali on alkuideaali. Koska maksimaaliset ideaalit ovat tällä tavoin tärkeitä kuntien ja alkuideaalien lähteitä, on hyvä tietää, milloin sellaisia on olemassa.

Lause 5.11 (Krull). *Jokaisella renkaalla nollarengasta lukuun ottamatta on maksimaalinen ideaali.*

Krullin lauseen todistus on perusesimerkki *Zornin*[1] *lemman* käytöstä. Koska Zornin lemma on luonteeltaan joukko-opillinen, on tässä yhteydessä hyvä hieman perehtyä siihen liittyviin käsitteisiin.

Zornin lemma on niin sanotun *valinta-aksiooman* toinen muotoilu, joka sopii hyvin erilaisten maksimaalisten rakenteiden olemassaolotodistuksiin. Valinta-aksiooma puolestaan on joukko-opin aksiooma, jota tarvitaan esimerkiksi joukkojen välisten mahtavuuksien vertailuun, transfiniittisiin induktiotodistuksiin tai vaikkapa sellaisen joukon konstruktioon, joka ei ole Lebesgue-mitallinen. Aksiooman mukaan mille tahansa epätyhjien joukkojen kokoelmalle voidaan määritellä kuvaus, joka antaa joukon arvoksi aina jonkin sen sisältämän alkion. Tällaista kuvausta kutsutaan *valintafunktioksi*.

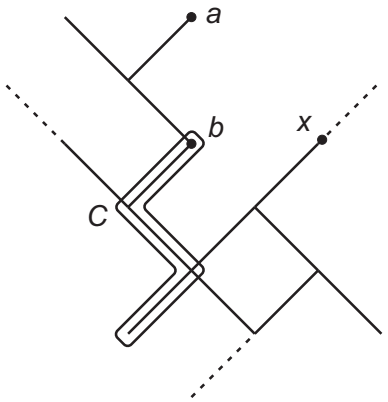
[1]Max August Zorn (1906–1993) oli saksalaissyntyinen amerikkalainen matemaatikko.

Ongelma valinta-aksioomasta – tai yhtä hyvin Zornin lemmasta – riippuvissa olemassaolotodistuksissa on se, että todistuksen tuottamasta joukosta tai rakenteesta ei yleensä voida sanoa mitään täsmällistä. Tässä mielessä valinta-aksiooma on sen naiivin joukko-opin perussäännön vastainen, että jokaisesta alkiosta pitäisi pystyä sanomaan, kuuluuko se annettuun joukkoon vai ei. Muun muassa tästä syystä on yleensä tapana mainita erikseen, jos todistuksessa nojaudutaan johonkin valinta-aksioomasta riippuvaan tulokseen.[1]

Olkoon $\mathcal{P}$ jokin joukko ja $\leq$ sen kaksipaikkainen relaatio. Tarkastellaan seuraavia ehtoja:

(J1) Kaikilla $a \in \mathcal{P}$ pätee $a \leq a$ (refleksiivisyys).
(J2) Jos $a \leq b$ ja $b \leq c$, niin $a \leq c$ (transitiivisuus).
(J3) Jos $a \leq b$ ja $b \leq a$, niin $a = b$ (antisymmetrisyys).
(J4) Kaikilla $a, b \in \mathcal{P}$ pätee $a \leq b$ tai $b \leq a$.

Jos relaatio $\leq$ on refleksiivinen, transitiivinen ja antisymmetrinen, paria $(\mathcal{P}, \leq)$ kutsutaan *osittaisjärjestykseksi*. Jos myös ehto (J4) toteutuu, pari on *täydellinen järjestys* eli *lineaarijärjestys*. Jos sekaannuksen vaaraa ei ole, osittaisjärjestykseksi tai lineaarijärjestykseksi voidaan nimittää myös joukkoa $\mathcal{P}$ tai relaatiota $\leq$. *Ketju* on osittaisjärjestyksen osajoukko, joka on relaation $\leq$ suhteen lineaarijärjestys. Alkio $m \in \mathcal{P}$ on osajoukon $A \subset \mathcal{P}$ *yläraja*, jos kaikilla $a \in A$ pätee $a \leq m$. Alkio m on *maksimaalinen*, jos ei ole olemassa alkiota $a \in \mathcal{P}$, jolle pätisi $m \leq a$ ja $a \neq m$.



KUVA 6. Osa erästä osittaisjärjestystä. Ylempänä olevat alkiot ovat alempana olevia ”suurempia”. Tässä järjestyksessä pätee siis $b \leq a$, mutta alkiota x ei voi vertailla alkion a tai b kanssa. Sekä a että b ovat molemmat ketjun C ylärajoja, ja a on maksimaalinen.

LEMMA 5.12 (Zornin lemma). *Oletetaan, että $\mathcal{P}$ on epätyhjä osittaisjärjestys, jossa jokaisella ketjulla on yläraja. Tällöin $\mathcal{P}$ sisältää maksimaalisen alkion.*

TODISTUS. Zornin lemma on yhtäpitävä joukko-opillisen valinta-aksiooman kanssa. Valinta-aksioomaa puolestaan ei voi todistaa muista joukko-opin aksioomista lähtien. Näiden väitteiden tarkistaminen sivuutetaan. (Zornin lemman ja

[1]Toinen syy on se, että valinta-aksiooman hyväksyminen todistuksen lähtökohdaksi voi johtaa paradoksaaliselta vaikuttaviin tuloksiin. Eräs tunnettu esimerkki on Banachin–Tarskin paradoksi, jossa valinta-aksiooman avulla konstruoidaan suljetun kuulan jako äärellisen moneen osaan, jotka uudelleenjärjestämällä saadaan kaksi alkuperäisen kokoista kuulaa.

valinta-aksiooman yhtäpitävyys löytyy muun muassa Herbert Endertonin teoksesta Elements of Set Theory. Valinta-aksiooman riippumattomuus on syvällisempi tulos. Se todistetaan yleensä pakotusmenetelmällä, mutta myös alkeellisempi todistus on mahdollinen. Lähteenä voi käyttää Thomas Jechin kirjaa The Axiom of Choice.) □

Osittaisjärjestykset ja Zornin lemma ovat näin muotoiltuina varsin abstrakteja, mutta niiden käyttö Krullin lauseen kaltaisten tulosten todistamiseksi muuttuu luontevaksi, kun siihen tottuu. Tyypillisesti osittaisjärjestyksenä toimii halutunlaisten osajoukkojen sisältyvyysjärjestys, jolloin maksimaalinen alkio on sellainen, joka ei sisälly mihinkään muuhun osittaisjärjestyksen alkioon.

KURLLIN LAUSEEN 5.11 TODISTUS. Olkoon R rengas, joka ei ole nollarengas. Tarkastellaan kaikkien renkaan R aitojen ideaalien muodostamaa kokoelmaa $\mathcal{P}$. Tämä on osittaisjärjestys sisältymisrelaation $\subset$ suhteen. Zornin lemman käyttö perustuu siihen havaintoon, että osittaisjärjestyksen $(\mathcal{P}, \subset)$ maksimaalinen alkio olisi määritelmän nojalla renkaan R maksimaalinen ideaali.

Ensinnäkin joukko $\mathcal{P}$ on epätyhjä, koska se sisältää vähintään nollaideaalin $\{0\}$. Osoitetaan, että jokaisella ketjulla on yläraja tässä osittaisjärjestyksessä. Olkoon sitä varten $\mathcal{A}$ jokin ketju. Selvästi jokainen $\mathcal{A}$:n alkio sisältyy yhdisteeseen $\bigcup \mathcal{A}$, joten riittää osoittaa, että $\bigcup \mathcal{A} \in \mathcal{P}$ eli että $\bigcup \mathcal{A}$ on aito ideaali.

Joukko $\bigcup \mathcal{A}$ on epätyhjä, koska $0 \in \{0\} \in \mathcal{A}$. Olkoot $r \in R$ ja $a, b \in \bigcup \mathcal{A}$. Nyt löytyy jotkin ideaalit A ja B, joille pätee $a \in A$ ja $b \in B$. Koska $\mathcal{A}$ on ketju, voidaan olettaa, että $A \subset B$. Tällöin $a, b \in B$, ja koska B on ideaali, myös alkiot $a - b$, ra ja ar kuuluvat joukkoon B. Näin ollen

$$a - b \in \bigcup \mathcal{A}, \quad ra \in \bigcup \mathcal{A} \quad \text{ja} \quad ar \in \bigcup \mathcal{A},$$

joten aliryhmäkriteerin ja ideaalin määritelmän perusteella $\bigcup \mathcal{A}$ on ideaali. Lisäksi $\bigcup \mathcal{A} \neq R$, koska kaikilla $A \in \mathcal{P}$ pätee $1 \notin A$. Yhdiste $\bigcup \mathcal{A}$ kuuluu siis osittaisjärjestykseen $\mathcal{P}$, jolloin se on eräs ketjun $\mathcal{A}$ yläraja.

Koska jokaisella ketjulla on yläraja osittaisjärjestyksessä $\mathcal{P}$, Zornin lemman perusteella joukossa $\mathcal{P}$ on maksimaalinen alkio. Tämä maksimaalinen alkio on haluttu maksimaalinen ideaali. □

Krullin lauseen todistusta hieman muuttamalla saadaan seuraava yleisempi tulos. Se voidaan myös johtaa seurauksena Krullin lauseesta.

KOROLLAARI 5.13. *Jos I on renkaan R aito ideaali, on olemassa renkaan R maksimaalinen ideaali, joka sisältää ideaalin I.*

TODISTUS. Krullin lauseen perusteella tekijärenkaalla R/I on maksimaalinen ideaali M. Lemman 5.1 nojalla tätä ideaalia vastaa renkaan R maksimaalinen ideaali, joka sisältää ideaalin I. □

6. Jaollisuus kokonaisalueissa

Eräs renkaiden teorian alkulähde oli lukuteoria. Monet lukuteoreettiset kysymykset vaativat ratketakseen kokonaislukujen ulkopuolelle siirtymisen. Ratkaisua kokonaislukuyhtälöön $x^2+y^2 = n$ saatetaan hakea esimerkiksi Gaussin kokonaislukujen renkaasta $\mathbb{Z}[i]$, jossa vasen puoli jakautuu tuloksi $(x+iy)(x-iy)$. Tällaisissa kokonaislukujen laajennoksissa on paljon tuttuja jaollisuusominaisuuksia, mutta myös joitakin vieraita ja kenties intuition vastaisia.

Toinen renkaiden teoriaan johtava polku lähti polynomirenkaiden tutkimuksesta. Polynomeja tarvitaan muun muassa kuntalaajennosten, ryhmäteorian invarianttien sekä algebrallisen geometrian tutkimiseen. Myös polynomien tutkimuksessa jaollisuusominaisuudet ovat keskeisiä.

Tässä luvussa tutustutaan erilaisiin jaollisuuteen liittyviin käsitteisiin, esitetään joitakin esimerkkejä lukuteoriasta, ja lopuksi keskitytään polynomien jaollisuuteen. Koska sekä kokonaislukujen laajennokset että kaikki käsiteltävät polynomirenkaat ovat kokonaisalueita, oletetaan koko luvussa, että R on kokonaisalue, vaikka jaollisuus voitaisiin sinänsä määritellä missä tahansa renkaassa.

MÄÄRITELMÄ 6.1. Alkio $a \in R$ *jakaa* alkion $b \in R$, jos $b = ac$ jollain $c \in R$. Tällöin merkitään $a \mid b$.

Jos alkio a jakaa alkion b, sanotaan myös, että b on *jaollinen* alkiolla a tai että a on b:n *tekijä*. Jokainen yksikkö, eli renkaan R kääntyvä alkio, on renkaan R kaikkien alkioiden tekijä. Nolla-alkio puolestaan on jaollinen kaikilla renkaan R alkioilla.

Alkioilla, jotka jakavat toisensa, on erityinen suhde.

MÄÄRITELMÄ 6.2. Olkoot $a, b \in R$. Jos $a \mid b$ ja $b \mid a$, sanotaan, että a ja b ovat toistensa *liittoalkioita*.

Liittoalkioilla on samat tekijät. Nolla-alkiolla ei ole muita liittoalkioita kuin nolla itse. Seuraavan lemman mukaan liittoalkiot eroavat toisistaan yksikön verran. Todistus on jaollisuuden määritelmään perustuva harjoitustehtävä.

LEMMA 6.3. *Oletetaan, että* $a, b \in R \setminus \{0\}$.

a) Jos $a = bc$ *pätee jollain yksiköllä* $c \in R$*, niin* a *ja* b *ovat liittoalkioita.*
b) Jos a *ja* b *ovat liittoalkioita, niin* $a = bc$ *jollain yksiköllä* $c \in R$*.*
c) Jos a *ja* b *ovat liittoalkioita ja* $a = bc$ *jollain* $c \in R$*, niin* c *on yksikkö.*
d) Kaikki yksiköt ovat toistensa liittoalkioita.

Esimerkiksi kokonaislukujen renkaassa on kaksi yksikköä: $\mathbb{Z}^* = \{1, -1\}$. Nollaa lukuun ottamatta jokaisen alkion liittoalkio saadaan kertomalla alkiota yksiköllä, joten nollasta poikkeavan kokonaisluvun ainoa liittoalkio on sen vastaluku.

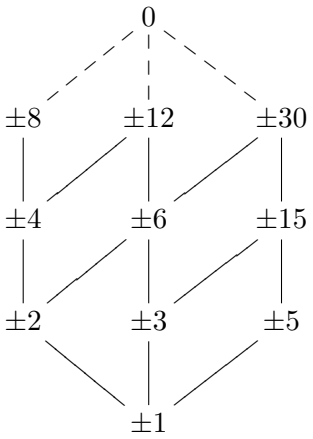
Lukujen suurin yhteinen tekijä määritellään tutulla tavalla.

MÄÄRITELMÄ 6.4. Olkoot $a, b \in R \setminus \{0\}$. Alkiota $d \in R$ nimitetään alkioiden a ja b *suurimmaksi yhteiseksi tekijäksi*, jos seuraavat ehdot pätevät:

i) Alkio d on alkioiden a ja b yhteinen tekijä eli $d \mid a$ ja $d \mid b$.
ii) Jos jollain $c \in R$ pätee $c \mid a$ ja $c \mid b$, niin $c \mid d$.

Jos 1 on alkioiden a ja b suurin yhteinen tekijä, sanotaan että a ja b ovat *jaottomia toistensa suhteen.*

Määritelmän sana *suurin* tarkoittaa jaollisuusrelaation mielessä suurinta. Jaollisuusrelaatio määrittelee osittaisjärjestyksen (ks. luku 5.3), jossa yksiköt ovat pienimpiä, sillä ne jakavat kaikki alkiot, ja nolla on suurin, sillä se on jaollinen kaikilla alkioilla. Oheisessa kuvassa on osa kokonaislukujen jaollisuusjärjestystä. Kuvaan on merkitty alkio ja sen liittoalkio samaan kohtaan, sillä niillä on täsmälleen samat ominaisuudet jaollisuusrelaation suhteen.



Huomaa, että jaollisuusjärjestys poikkeaa kokonaislukujen luontaisesta järjestyksestä negatiivisten lukujen kohdalla. Kuvasta nähdään esimerkiksi, että kokonaislukujen renkaassa lukujen 30 ja 12 suurimmat yhteiset tekijät ovat luvut 6 ja -6, sillä ne ovat molemmat lukujen 30 ja 12 alapuolella, mutta ylimpänä kaikista tällaisista luvuista. Vastaavasti lukujen -8 ja 30 suurimmat yhteiset tekijät ovat 2 ja -2. Pelkästään positiivisista kokonaisluvuista puhuttaessa suurin yhteinen tekijä voidaan määritellä kokonaislukujen luonnollisen järjestyksen suhteen, mutta yleisemmässä tilanteessa on käytettävä jaollisuusjärjestystä.

Kaikissa kokonaisalueissa kahdella alkiolla ei välttämättä ole suurinta yhteistä tekijää. Lisäksi alkioiden a ja b suurin yhteinen tekijä ei yleensä ole yksikäsitteinen, mistä syystä merkintä $d = \mathrm{syt}(a, b)$ ei periaatteessa ole käyttökelpoinen. Suurimman yhteisen tekijän määritelmästä kuitenkin seuraa, että kaikki kahden alkion suurimmat yhteiset tekijät ovat toistensa liittoalkioita. Merkinnän $d = \mathrm{syt}(a, b)$ voidaankin tulkita tarkoittavan, että d on *eräs* alkioiden a ja b suurin yhteinen tekijä, ja jokainen muu suurin yhteinen tekijä saadaan kertomalla alkiota d jollain yksiköllä. Erityisesti merkintä $\mathrm{syt}(a, b) = 1$ tarkoittaa tällöin, että jokainen suurin yhteinen tekijä on yksikkö.

6.1. Jaottomuus. Jokainen alkio on jaollinen kaikilla yksiköillä sekä omilla liittoalkioillaan. Näitä voidaan siksi pitää eräänlaisina triviaaleina tekijöinä. Jaottomasta alkioista puhutaan silloin, kun alkio ei ole jaollinen millään epätriviaalilla tekijällä. Koska nolla-alkio on joka tapauksessa jaollinen kaikilla alkioilla, se jätetään kokonaan tarkastelun ulkopuolelle.

MÄÄRITELMÄ 6.5. Oletetaan, että $a \in R$ ei ole nolla eikä yksikkö. Alkiota a sanotaan *jaottomaksi*, jos sen jokainen tekijä on joko yksikkö tai alkion a liittoalkio.

Jaollisuusjärjestyksessä jaottomat alkiot sijaitsevat välittömästi yksikköjen yläpuolella.

ESIMERKKI 6.6.

- Kokonaislukujen renkaassa jokainen alkuluku p on jaoton, sillä sen tekijöitä ovat vain luvut 1, -1, p ja $-p$, jotka ovat kaikki joko yksiköitä tai luvun p liittoalkioita. Alkuluvut ja niiden liittoalkiot ovat myös ainoat jaottomat kokonaisluvut.
- Jos K on kunta, polynomirenkaassa $K[x]$ jokainen nollasta poikkeava vakiopolynomi on kääntyvä alkio, siis yksikkö. Kääntäen ainoastaan vakiopolynomit ovat kääntyviä, mikä nähdään tarkastelemalla polynomien asteita. Tarkastellaan esimerkkinä jaottomasta alkiosta polynomirenkaan $\mathbb{R}[x]$ toisen asteen polynomia $f = x^2 + 1$. Voidaan helposti tarkistaa, että polynomilla f ei ole reaalijuuria. Tällöin sillä ei myöskään ole ensimmäisen asteen tekijöitä. Jos se siis kirjoitetaan muodossa $f = gh$, missä $g, h \in \mathbb{R}[x]$, toisella tekijöistä on oltava aste 0 ja toisella 2. Tällöin joko g tai h on vakiopolynomi, joten f on jaoton.

Kokonaisluvuilla jaottomista alkioista saadaan jokaiselle luvulle yksikäsitteinen alkutekijähajotelma. Yleisessä kokonaisalueessa tällaista hajotelmaa ei välttämättä ole, tai se ei ole yksikäsitteinen. Yksikäsitteisyyden vaatimus antaa aiheen määritellä niin kutsutut alkualkiot. Tämä yhteys nähdään myöhemmin luvussa 6.3 sekä lauseen 6.17 todistuksessa. Alkualkion määritelmä muistuttaa alkuideaalin määritelmää sekä Eukleideen lemmaa.

MÄÄRITELMÄ 6.7. Oletetaan, että $a \in R$ ei ole nolla eikä yksikkö. Alkiota a sanotaan *alkualkioksi*, jos kaikilla $b, c \in R$ ehdosta $a \mid bc$ seuraa $a \mid b$ tai $a \mid c$.

Alkualkioilla ja jaottomilla alkioilla on läheinen yhteys.

LAUSE 6.8. *Jokainen alkualkio on jaoton.*

TODISTUS. Oletetaan, että $a \in R$ on alkualkio ja $a = bc$ joillain $b, c \in R$. Tällöin sekä b että c jakavat alkion a. Toisaalta a jakaa triviaalisti tulon bc, joten koska a on alkualkio, a jakaa joko alkion b tai alkion c. Edellisessä tapauksessa a ja b ovat liittoalkioita, jolloin c on yksikkö. Jälkimmäisessä tapauksessa a ja c ovat liittoalkioita, ja b on yksikkö. Joka tapauksessa siis a on jaollinen vain yksiköillä ja omilla liittoalkioillaan. □

Kokonaislukujen renkaassa myös käänteinen väite pätee, mikä on Eukleideen lemman sisältö. Yleisessä tapauksessa kuitenkin alkualkiona oleminen on vahvempi ominaisuus kuin jaottomuus.

ESIMERKKI 6.9. Tarkastellaan rengasta $\mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\}$. Tässä renkaassa pätee

$$6 = (1 + i\sqrt{5})(1 - i\sqrt{5}).$$

Voidaan osoittaa, että luku 2 on jaoton renkaassa $\mathbb{Z}[i\sqrt{5}]$ mutta että 2 ei jaa kumpaakaan luvuista $1 + i\sqrt{5}$ ja $1 - i\sqrt{5}$ vaikka jakaakin näiden tulon. Täten 2 ei siis ole alkualkio.

Miten edellä olevat väitteet sitten osoitetaan? Lukurenkaiden jaollisuustutkimuksissa käytetään hyväksi *normikuvausta*, joka renkaan $\mathbb{Z}[i\sqrt{5}]$ tapauksessa on sama kuin kompleksiluvun normin neliö: $N(a+bi\sqrt{5}) = a^2+5b^2$. Normikuvaus on

multiplikatiivinen, eli $N(xy) = N(x)N(y)$, ja sen arvot ovat kokonaislukuja, joten jaollisuuskysymykset voidaan sen avulla siirtää kokonaislukujen renkaaseen.

Näytetään esimerkin vuoksi, että luku 2 on jaoton renkaassa $\mathbb{Z}[i\sqrt{5}]$. Oletetaan, että $2 = (a + bi\sqrt{5})(c + di\sqrt{5})$ joillain $a, b, c, d \in \mathbb{Z}$. Käyttämällä normikuvausta molemmille puolille saadaan kokonaislukuyhtälö

$$4 = (a^2 + 5b^2)(c^2 + 5d^2).$$

Koska yhtälön oikealla puolella molemmat tekijät ovat positiivisia kokonaislukuja, jotka yhtälön mukaan jakavat luvun 4, nähdään esimerkiksi, että a^2+5b^2 on joko 1, 2 tai 4. Tällöin on oltava $b = 0$, ja lopulta $a = \pm 1$ tai $a = \pm 2$. Kaikissa tapauksissa seurauksena on, että tekijä $a + bi\sqrt{5}$ on joko yksikkö tai luvun 2 liittoalkio, joten 2 on jaoton.

6.2. Pääideaalialueet. Ideaalia, joka on yhden alkion virittämä, kutsutaan *pääideaaliksi*. Vaihdannaisessa renkaassa R alkion a virittämä pääideaali $\langle a \rangle$ voidaan kirjoittaa muodossa $\{ra \mid r \in R\}$. Jos renkaan jokainen ideaali on pääideaali, rengasta kutsutaan *pääideaalirenkaaksi*, ja jos kyseessä on kokonaisalue, käytetään nimitystä *pääideaalialue* (engl. principal ideal domain).

Esimerkki 6.10. Pääideaalialueista tärkein esimerkki on kokonaislukujen rengas $\mathbb{Z}$. Toinen jatkon kannalta tärkeä esimerkki ovat yhden tuntemattoman polynomit, kun kerroinrenkaana on kunta. Molemmat rakenteet osoitetaan pääideaalirenkaiksi jakoyhtälöä hyödyntämällä. Polynomien jakoyhtälö todistetaan luvussa 6.4, ja samassa luvussa näytetään myös, että mainitunlainen polynomirengas on pääideaalirengas.

Pääideaalirenkaiden merkitys jaollisuuskysymyksissä liittyy siihen, että vaihdannaisessa renkaassa jaollisuus vastaa pääideaalien sisältymistä toisiinsa. Jos nimittäin $a \mid b$, niin $b \in \langle a \rangle$, ja edelleen $\langle b \rangle \subset \langle a \rangle$. Myös käänteinen väite pätee. Koska pääideaalirenkaassa jokainen ideaali on pääideaali, kaikki ideaalien sisältymiskysymykset voidaan muuttaa jaollisuuskysymyksiksi ja päinvastoin. Oletetaan seuraavissa tuloksissa, että R on jokin pääideaalialue.

Lause 6.11. *Jos $a, b \in R$, on olemassa* $\operatorname{syt}(a, b)$. *Lisäksi, jos $d = \operatorname{syt}(a, b)$, niin $d = xa + yb$ joillain $x, y \in R$.*

Todistus. Harjoitustehtävä. (Tutki ideaalia $\langle a, b \rangle$.) □

Lause 6.12. *Jos $p \in R$ on jaoton, ideaali $\langle p \rangle$ on maksimaalinen.*

Todistus. Olkoon $p \in R$ jaoton alkio. Tarkistetaan ensin, että $\langle p \rangle$ on aito ideaali. Jos $1 \in \langle p \rangle$, löytyy jokin $r \in R$, jolle pätee $1 = rp$. Tällöin p on yksikkö, eikä siis jaoton. Siispä $1 \notin \langle p \rangle$, joten $\langle p \rangle \neq R$.

Oletetaan sitten, että jollain ideaalilla I pätee $\langle p \rangle \subset I$. Koska R on pääideaalirengas, löytyy jokin $a \in R$, jolle pätee $\langle a \rangle = I$. Tällöin $p \in \langle a \rangle$, joten $a \mid p$. Koska p on jaoton, täytyy alkion a olla joko yksikkö tai alkion p liittoalkio.

Jos a on yksikkö, tiedetään, että $I = \langle a \rangle = R$. Jos taas a on alkion p liittoalkio, pätee $p \mid a$. Tästä puolestaan seuraa $\langle a \rangle \subset \langle p \rangle$, joten $I = \langle p \rangle$. Koska joka tapauksessa $I = R$ tai $I = \langle p \rangle$, nähdään, että ideaali $\langle p \rangle$ on maksimaalinen. □

Alkualkion määritelmästä nähdään helposti, että pääideaali on alkuideaali, jos ja vain jos sen virittäjä on alkualkio tai nolla. Koska jokainen alkualkio on jaoton, seuraa edellisestä lauseesta suoraan seuraava tulos (vrt. esimerkkiin 5.8).

KOROLLAARI 6.13. *Jokainen renkaan R nollaideaalista poikkeava alkuideaali on maksimaalinen.*

Koska maksimaaliset ideaalit ovat alkuideaaleja, saadaan vielä toinen seuraus.

KOROLLAARI 6.14. *Jokainen renkaan R jaoton alkio on alkualkio.*

6.3. Jaollisuusalueista. Kunnissa jaollisuusrelaatio ei ole mielenkiintoinen, koska kaikki nollasta poikkeavat alkiot ovat yksiköitä ja siis toistensa liittoalkioita. Toisaalta yleisessä kokonaisalueessa on käytännössä vaikea todistaa mitään jaollisuuteen liittyvää. Esitellään tässä alaluvussa yleisluontoisesti eräitä kokonaisalueiden tyyppejä, jotka sijoittuvat jaollisuusominaisuuksiltaan kuntien ja kokonaisalueiden väliin. Todistukset tyydytään luonnostelemaan, mutta niitä löytyy algebran perusoppikirjoista, esimerkkinä Nathan Jacobsonin *Lectures in Abstract Algebra I. Basic Concepts*.

Tekijöihinjakoalueet. Kokonaisalueessa, jossa jokainen nollasta ja yksiköstä poikkeava alkio voidaan esittää yksikäsitteisellä tavalla jaottomien alkioiden tulona, nimitetään tekijöihinjakoalueeksi (engl. unique factorisation domain). Jaon on oltava yksikäsitteinen sillä rajoituksella, että tekijöiden järjestyksellä ei ole väliä ja jokainen alkio voidaan korvata liittoalkiollaan. Kokonaislukujen rengas on tunnetusti tekijöihinjakoalue: esimerkiksi luvulla 60 on esitys $2 \cdot 2 \cdot 3 \cdot 5$, jota pidetään samana kuin esitystä $-5 \cdot 2 \cdot 3 \cdot (-2)$.

Tekijöihinjakoalueessa kahden alkion suurin yhteinen tekijä löytyy vertailemalla alkioiden tekijöihinjakoja. Lisäksi tekijöihinjakoalueessa jokainen jaoton alkio on alkualkio: jos p on jaoton ja $p \mid ab$, alkio p tai sen liittoalkio löytyy joko alkion a tai b tekijähajotelmasta. Hieman hankalampaa on osoittaa, että jos R on tekijöihinjakoalue, myös polynomirengas $R[X]$ on tekijöihinjakoalue. Tästä voidaan induktiolla päätellä edelleen, että rengas $R[X_1, \ldots, X_n]$ on tekijöihinjakoalue kaikilla n. Esimerkiksi $\mathbb{Z}[X, Y]$ on siis tekijöihinjakoalue.

Koska tekijöihinjakoalueessa jokainen jaoton alkio on alkualkio, nähdään esimerkin 6.9 perusteella, että rengas $\mathbb{Z}[i\sqrt{5}]$ ei ole tekijöihinjakoalue. Tämä voidaan nähdä myös suoraan. Esimerkiksi luvulla 6 on kaksi esitystä jaottomien alkioiden tulona:

$$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5}).$$

Esityksiä ei saa toisistaan vaihtamalla alkioita liittoalkioikseen, mikä voidaan osoittaa helposti normikuvausta käyttämällä.

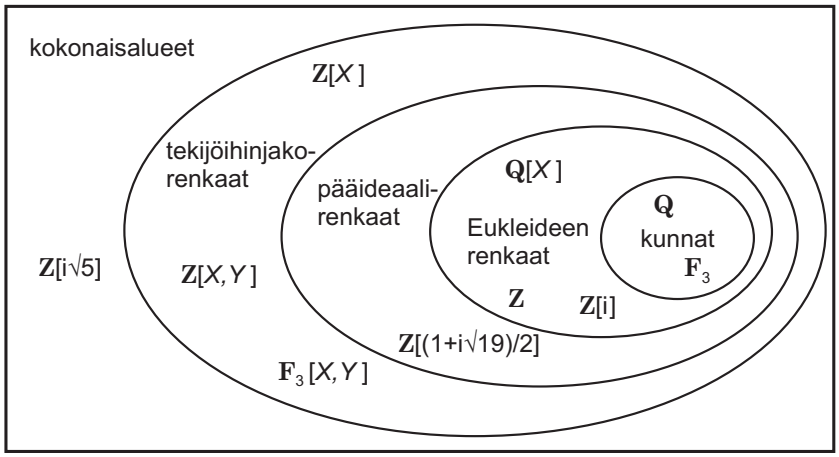
Matemaatikoille oli taannoin yllätys, että kaikissa lukurenkaissa ei esiinny yksikäsitteistä alkutekijöihinjakoa. Eräät ensimmäisistä Fermat'n suuren lauseen todistusyrityksistä käyttivät nerokkaalla tavalla kokonaislukujen laajennoksia, mutta ne kilpistyivät yksikäsitteisen alkutekijähajotelman puuttumiseen. Saksalainen matemaatikko Ernst Kummer (1810–1893) huomasi 1840-luvulla, että vaihtamalla alkualkiot alkuideaaleihin tekijöihinjako saadaan pelastettua. (Kummer käytti nykyaikaisten ideaalien sijaan kehittämiään "ideaalisia lukuja", ja Richard Dedekind määritteli nykyisen kaltaiset ideaalit vuonna 1876.) Esimerkiksi renkaassa $\mathbb{Z}[i\sqrt{5}]$ pääideaali $\langle 6 \rangle$ voidaan esittää yksikäsitteinä tulona alkuideaaleista:

$$\langle 6 \rangle = \langle 2, 1 + i\sqrt{5} \rangle^2 \langle 3, 1 + i\sqrt{5} \rangle \langle 3, 1 - i\sqrt{5} \rangle.$$

Pääideaalialueet. Pääideaalialueista oli puhetta jo edellä. Lisätään tässä se huomio, että pääideaalialueet ovat tekijöihinjakoalueita. Tekijähajotelman yksikäsitteisyys seuraa siitä, että pääideaalialueessa jokainen jaoton alkio on alkualkio (korollaari 6.14). Olkoot $p_1p_2\cdots p_m = q_1q_2\cdots q_n$ kaksi jonkin alkion esitystä jaottomien alkioiden tulona. Koska jaottomat alkiot ovat alkualkioita, nähdään, että p_1 jakaa jonkin alkioista q_i. Järjestystä vaihtamalla voidaan olettaa, että $p_1 \mid q_1$. Tällöin p_1 on alkion q_1 liittoalkio, koska q_1 on jaoton. Kokonaisalueen supistussäännön nojalla saadaan $p_2\cdots p_m = u_1q_2\cdots q_n$ jollain yksiköllä u_1. Induktion avulla nähdään lopulta, että kaikki tekijät p_i ja q_i vastaavat yksi yhteen toisiaan järjestyksen vaihtamista ja yksiköllä kertomista vaille.

Tekijähajotelman olemassaolo sen sijaan on hieman hankalampi nähdä. Sitä varten voitaisiin näyttää ensin, että pääideaalialueessa jokainen nouseva ideaalien ketju $I_1 \subsetneq I_2 \subsetneq \cdots$ on äärellisen pituinen. Tällaista rengasta kutsutaan yleisemmin *Noetherin renkaaksi*. Alkion a_1 alkutekijä löydetään nyt muodostamalla jono $a_1, a_2, a_3, \ldots$, missä $a_{i+1} \mid a_i$ jokaisella i. Tällöin vastaavat ideaalit muodostavat ketjun $\langle a_1\rangle \subset \langle a_2\rangle \subset \cdots$, jonka viimeinen alkio on jaottoman alkion virittämä. Näin jatkamalla saadaan lopulta etsitty tekijähajotelma.

Kaikki tekijöihinjakoalueet eivät ole pääideaalialueita: esimerkiksi useamman tuntemattoman polynomirengas $K[X_1, \ldots, X_n]$ ei ole pääideaalialue, vaikka K olisikin kunta. Samaten esimerkiksi polynomirengas $\mathbb{Z}[X]$ ei ole pääideaalialue vaikka onkin tekijöihinjakoalue.



KUVA 7. Erilaisia jaollisuusalueita.

Eukleideen alueet. Käytännössä monet pääideaalialueet osoitetaan sellaisiksi käyttämällä hyväksi jakoyhtälöä. Jakoyhtälön avulla voidaan lisäksi muotoilla Eukleideen algoritmi, joka takaa suurimman yhteisen tekijän olemassaolon ja Bézout'n lemman voimassaolon. Lisäksi jakoyhtälön avulla alkion jako jaottomien alkioiden tuloksi käy kätevämmin kuin yleisessä pääideaalialueessa.

Eukleideen alueeksi kutsutaan kokonaisaluetta R, jossa voidaan määritellä seuraavan ehdon toteuttava funktio $\varepsilon\colon R \to \mathbb{N}$:

> Jos $a, b \in R$ ja $b \neq 0$, niin löytyy sellaiset $q, r \in R$, että $a = bq + r$ ja joko $r = 0$ tai $\varepsilon(r) < \varepsilon(b)$.

Tällaista funktiota kutsutaan *Eukleideen funktioksi*. Eukleideen funktion merkitys on siinä, että sen avulla voidaan muotoilla jakoyhtälö, jossa jakojäännöksen

arvo Eukleideen funktiossa on pienempi kuin jakajan. Kokonaislukujen renkaassa Eukleideen funktiona toimii itseisarvofunktio, ja jos K on kunta, yhden tuntemattoman polynomirenkaassa $K[X]$ Eukleideen funktio saadaan polynomin asteesta.

Eukleideen alueet ovat pääideaalialueita. Jos nimittäin I on mikä tahansa Eukleideen alueen ideaali, voidaan valita alkio $a \in I$, jolla Eukleideen funktio saa minimiarvon. Tällainen aina löytyy, koska Eukleideen funktion maalijoukko on luonnollisten lukujen joukko. Tämän jälkeen voidaan käyttää jakoyhtälöä tavalliseen tapaan osoittamaan, että $I = \langle a \rangle$. Kaikki pääideaalialueet eivät kuitenkaan ole Eukleideen alueita, mistä esimerkkinä voidaan mainita rengas $\mathbb{Z}[(1+i\sqrt{19})/2]$. Todistus kuitenkin sivuutetaan.

6.4. Jaollisuus polynomirenkaissa. Polynomirengas, jonka kerroinrengas on kokonaisalue, on itsekin kokonaisalue. Tämä johtuu siitä, että polynomeja kerrottaessa tulopolynomin korkeimman asteen termin kerroin on yksinkertaisesti tekijäpolynomien korkeimman asteen kertoimien tulo, eikä se siis häviä.

Tässä alaluvussa todistetaan yhden muuttujan polynomien jakoyhtälö, kun kerroinrenkaana on kunta. Tämä tekee yhden tuntemattoman polynomirenkaasta Eukleideen alueen, jossa Eukleideen funktiona toimii polynomin aste (ks. edellinen alaluku). Eukleideen alueet ovat pääideaalialueita ja sen vuoksi niiden alkioilla on myös yksikäsitteinen alkutekijähajotelma. Tässä luvussa nämä seikat kuitenkin osoitetaan suoraan polynomien jakoyhtälöä käyttäen, koska se on yksinkertaisinta. Todistukset toimivat samalla esimerkkeinä Eukleideen alueessa toimimisesta. Koska myös kokonaislukujen rengas on Eukleideen alue, todistukset ovat hyvin samanlaisia kuin vastaavien tulosten todistukset kokonaisluvuilla.

LAUSE 6.15 (Polynomien jakoyhtälö). *Olkoon K kunta, ja olkoot $f, g \in K[X]$. Oletetaan, että $g \neq 0$. Tällöin löytyy yksikäsitteiset polynomit $q, r \in K[X]$, joille pätee $f = qg + r$ ja* $\deg(r) < \deg(g)$.

TODISTUS. Tarkastellaan joukkoa

$$\mathcal{R} = \{f - qg \mid q \in K[X]\}.$$

Tämä joukko on selvästi epätyhjä. Olkoon $r \in \mathcal{R}$ sellainen polynomi, jonka aste on pienin joukossa $\mathcal{R}$. Tällöin $f - qg = r$ jollain $q \in K[X]$. Jos $r = 0$, lauseessa etsityiksi polynomeiksi käyvät q ja r, sillä $\deg(r) = -\infty < \deg(g)$. Muussa tapauksessa merkitään $r = \sum_{i=0}^{n} a_i X^i$ ja $g = \sum_{i=0}^{m} b_i X^i$, missä $a_n \neq 0$ ja $b_m \neq 0$. Jos nyt pätee $\deg(r) \geq \deg(g)$, määritellään $q_1 = q + a_n b_m^{-1} X^{n-m}$. Tällöin

$$f - q_1 g = r - a_n b_m^{-1} X^{n-m} g,$$

ja tämän polynomin aste on pienempi kuin $n = \deg(r)$, koska monomin X^n kerroin on 0. Toisaalta $f - q_1 g$ on joukossa $\mathcal{R}$, mikä on ristiriita. Täten $\deg(r) < \deg(g)$, jolloin q ja r käyvät lauseessa etsityiksi polynomeiksi.

Yksikäsitteisyyden osoittamiseksi oletetaan, että polynomit q_1, q_2, r_1 ja r_2 toteuttavat muut lauseen ehdot. Tällöin $q_1 g + r_1 = q_2 g + r_2$, josta edelleen saadaan $(q_1 - q_2)g = r_1 - r_2$. Jos $q_1 \neq q_2$, niin polynomin $(q_1 - q_2)g$ aste on vähintään $\deg(g)$, joka on suurempi kuin $\deg(r_1 - r_2)$. Tämä on mahdotonta, joten $q_1 = q_2$, mistä seuraa, että $r_1 = r_2$. □

Huomautus. Todistuksessa tarvittiin vain kertoimen b_m kääntyvyyttä. Tulos pätee siksi missä tahansa kokonaisalueessa K, kunhan polynomin g korkeimman asteen kerroin on yksikkö.

LAUSE 6.16. *Jos K on kunta, polynomirengas $K[X]$ on pääideaalirengas.*

TODISTUS. Oletetaan, että K kunta ja I jokin renkaan $K[X]$ ideaali. Nolla-ideaali on nollapolynomin virittämä, joten voidaan olettaa, että I ei ole nollaideaali. Olkoon $p \in I$ jokin nollasta poikkeava polynomi, jonka aste on minimaalinen joukossa $I \setminus \{0\}$. Osoitetaan, että $I = \langle p \rangle$.

Olkoon $f \in I$. Jakoyhtälön nojalla löytyy jotkin $q, r \in K[X]$, joille pätee $f = qp + r$ ja $\deg(r) < \deg(p)$. Nyt $r = f - qp$ on ideaalin I alkio, mutta $\deg(p)$ on minimaalinen joukossa $I \setminus \{0\}$. Tästä seuraa, että $r = 0$, joten $f = qp \in \langle p \rangle$. Siten I on polynomin p virittämä. □

LAUSE 6.17. *Jos K on kunta, polynomirengas $K[X]$ on tekijöihinjakorengas.*

TODISTUS. Osoitetaan aluksi tekijähajotelman olemassaolo. Oletetaan, että $f \in K[X]$ ei ole nollapolynomi eikä yksikkö. Jos f on jaoton, hajotelma on valmis, joten oletetaan, että f ei ole jaoton. Tällöin $f = f_1 f_2$ joillain $f_1, f_2 \in K[X]$, joista kumpikaan ei ole yksikkö. Koska K on kunta, tästä seuraa, että f_1 ja f_2 eivät ole vakiopolynomeja, ja edelleen, että kummankin aste on aidosti pienempi kuin $\deg(f)$. Jos f_1 tai f_2 ei ole jaoton, jatketaan etsimällä jälleen epätriviaalit tekijät. Prosessi päättyy joskus, koska polynomin aste ei voi pienetä rajatta. Lopulta saadaan esitys $f = p_1 p_2 \cdots p_r$, missä jokainen p_i on jaoton.

Osoitetaan sitten yksikäsitteisyys. Oletetaan sitä varten, että

$$f = p_1 \cdots p_r = q_1 \cdots q_s,$$

missä jokainen p_i ja q_i on jaoton. Nyt p_1 jakaa tulon $q_1 \cdots q_s$. Korollaarin 6.14 nojalla p_1 on alkualkio, joten se jakaa jonkin polynomeista q_i. Järjestystä vaihtamalla voidaan olettaa, että $p_1 \mid q_1$. Toisaalta q_1 on jaoton, joten p_1 ja q_1 ovat liittoalkioita. Käyttämällä kokonaisalueen supistusääntöä voidaan päätellä, että $p_2 \cdots p_r = u_1 q_2 \cdots q_s$, missä u_1 on yksikkö. Induktion avulla nähdään lopulta, että $r = s$ ja että p_i ja q_i ovat liittoalkioita kaikilla i. □

Kuntalaajennokset

Kuntalaajennokset ovat tärkeä työkalu muun muassa lukuteoriassa ja algebrallisessa geometriassa. Niillä on myös historiallinen merkitys, sillä modernin algebran voidaan katsoa syntyneen pyrkimyksestä ratkaista polynomiyhtälöitä. Tämä pyrkimys johtaa luonnollisella tavalla rationaali- ja reaalilukujen kunnan laajentamiseen irrationaali- ja kompleksijuurilla. Abelin vuonna 1824 ja Ruffinin vuonna 1799 laatimat todistukset viidennen asteen polynomiyhtälöiden ratkeamattomuudelle sekä Galois'n vuonna 1830 muotoilema täsmällinen kriteeri yleisen polynomiyhtälön ratkeavuudelle kehittivät kuntalaajennosten teoriaa mutta loivat samalla pohjan ryhmäteorian synnylle. Tätä polynomiyhtälöiden abstraktia käsittelyä permutaatioiden avulla pidetään yleensä modernin algebrallisen ajattelun alkuna.

Kuntalaajennokset voidaan jakaa algebrallisiin ja transkendenttisiin sen mukaan, ovatko laajennoksen alkiot joidenkin alkuperäisen kunnan polynomien juuria vai eivät. Algebralliset keinot toimivat lähinnä algebrallisten laajennosten yhteydessä, joten keskitymme tulevissa luvuissa niihin. Algebrallisten laajennosten tutkimuksessa niin kutsutuilla minimipolynomeilla on keskeinen merkitys.

Kuntalaajennosten teorian kehittyminen 1800-luvulla mahdollisti myös eräiden ikivanhojen, antiikista peräisin olevien geometristen ongelmien ratkaisemisen. Tällaisiin kuuluu muun muassa kulman kolmiajaon ongelma, jonka ratkaisu esitetään teorian sovelluksena luvussa 8.2

7. Kunnan laajentaminen

Aloitetaan kuntalaajennoksiin tutustuminen esimerkillä.

Esimerkki 7.1. Tarkastellaan kolmen alkion kuntaa $\mathbb{Z}_3 = \{0, 1, -1\}$. Kunnista puhuttaessa tätä merkitään yleensä $\mathbb{F}_3$. Mikään kunnan alkioista ei ole polynomin $p = X^2 + 1$ juuri. Yritetään laajentaa kuntaa niin, että juuri saataisiin mukaan, mutta rakenne säilyisi edelleen kuntana. Reaalilukujen tapauksessa voitaisiin juuri löytää siirtymällä kompleksilukuihin, mutta $\mathbb{F}_3$ ei ole reaalilukujen kunnan osajoukko, joten emme voi noin vain lisätä imaginaariyksikköä mukaan.

Voimme kuitenkin edetä seuraavasti. Koska f on toisen asteen juureton polynomi, se on jaoton, sillä epätriviaalit tekijät olisivat ensimmäisen asteen polynomeja, joiden juuret olisivat myös polynomin f juuria. Lauseen 6.12 nojalla renkaan $\mathbb{F}_3[X]$ ideaali $\langle p \rangle$ on maksimaalinen, joten tekijärengas $L = \mathbb{F}_3[X]/\langle p \rangle$ on kunta. Tutkitaan kunnan L ominaisuuksia.

Ensinnäkin ideaali $\langle p \rangle$ sisältää nollapolynomin lisäksi ainoastaan polynomeja, joiden aste on vähintään kaksi. Täten tekijärenkaassa L kaikki korkeintaan ensimmäisen asteen polynomit kuuluvat eri sivuluokkiin. Toisaalta jakoyhtälöä soveltamalla nähdään, että jos $\deg(f) \geq 2$ jollain $f \in \mathbb{F}_3[X]$, niin $[f] = [g]$ jollain korkeintaan ensimmäisen asteen polynomilla $g \in \mathbb{F}_3[X]$. Esimerkiksi $[X^3] = [-X]$, sillä $X^3 = X \cdot p - X$. Näin päättelemällä voidaan todeta, että kunta L koostuu

seuraavista alkioista:

$$L = \{[0], [1], [-1], [X], [X+1], [X-1], [-X], [-X+1], [-X-1]\}.$$

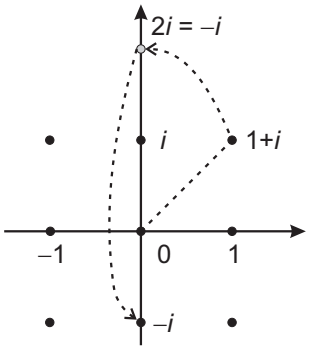
Samastetaan nyt korkeintaan ensimmäisen asteen polynomit sivuluokkiensa kanssa, ja jätetään hakasulut kirjoittamatta. Erityisesti vakiopolynomit voidaan ajatella kuntalaajennoksen L alkioina. Voidaan siis sanoa, että $\mathbb{F}_3$ on kunnan L alikunta. Laajennoksella L on väistämättä sama karakteristika kuin lähtökunnalla $\mathbb{F}_3$, sillä ykkösen monikerrat sisältyvät kaikki alikuntaan $\mathbb{F}_3$.

Laajennoksessa L voidaan määritellä lähtökunnan $\mathbb{F}_3$ skalaarikertolasku käyttämällä kunnan L sisäistä kertolaskua. Täten laajennoksesta tulee $\mathbb{F}_3$-vektoriavaruus. Sen virittävät alkiot 1 ja X, sillä kaikki kunnan L alkiot voidaan esittää näiden alkioiden lineaarikombinaationa, kuten yllä tehtiin. Laajennoksen L dimensio lähtökunnan $\mathbb{F}_3$ suhteen on siis 2.

Kunnassa L yhteenlasku toimii kuten vektorien yhteenlasku. Entä kertolasku? Sitä varten todetaan, että alkuperäisellä polynomilla p on juuri kunnassa L, sillä

$$p([X]) = [X]^2 + 1 = [X^2 + 1] = [p] = 0_L.$$

Kun hakasulut jätetään jälleen pois, voidaan siis sanoa, että kunnassa L pätee $X^2 = -1$. Tämä yhtälö riittää määrittelemään $\mathbb{F}_3$-algebran kertolaskun. Kyseisen yhtälön innoittamana voisimme lisäksi halutessamme merkitä $[X] = i$ ja suorittaa kertolaskut kuten kompleksiluvuilla, kuitenkin muistaen, että $3 = 0$ pätee kunnassa L. Näin onkin tehty kuvassa 8, jossa laajennos on esitetty kaksiulotteisena F_3-vektoriavaruutena.



KUVA 8. Kunnan $\mathbb{F}_3$ kaksiulotteinen laajennos. Kertolasku toimii samaan tapaan kuin kompleksiluvuilla. Esimerkiksi voidaan laskea $(1+i)^2 = 1 + 2i - 1 = 2i = -i$.

7.1. Kuntalaajennos ja sen aste. Määritellään nyt kuntalaajennokset yleisemmin ja tarkastellaan samalla niiden ominaisuuksia vektoriavaruuksina. Tässä alaluvussa esitettyjä tuloksia kannattaa verrata edelliseen esimerkkiin 7.1.

MÄÄRITELMÄ 7.2. Kunnan K *laajennos* L on mikä tahansa kunnan K ylikunta eli kunta, joka sisältää alikuntanaan kunnan K. Laajennosta merkitään L/K (lausutaan "L yli K:n"), ja kuntaa K kutsutaan laajennoksen *lähtökunnaksi*.

Kunnan K ylikunta L on K-algebra, kun skalaarikertolaskuksi valitaan kunnan L kertolasku. Laajennos L on siis erityisesti K-vektoriavaruus, joten sillä on dimensio.

Huomautus. Kuntalaajennosten yhteydessä käytettävä kauttaviiva (/) ei tarkoita tekijärakennetta. Sen jälkeinen kunta on yksinkertaisesti laajennoksen lähtökunta. Kun laajennosta ajatellaan vektoriavaruutena, kauttaviivan jälkeinen kunta toimii skalaarikuntana.

MÄÄRITELMÄ 7.3. Kuntalaajennoksen L/K *aste* on kunnan L dimensio K-vektoriavaruutena. Astetta merkitään $[L : K]$, ja se voi olla joko positiivinen kokonaisluku tai ääretön. Jos aste on äärellinen, laajennosta nimitetään *äärelliseksi laajennokseksi*, muuten kyseessä on *ääretön laajennos*.

ESIMERKKI 7.4. Seuraavat ovat esimerkkejä kuntalaajennoksista.

- Kompleksilukujen kunta $\mathbb{C}$ on reaalilukujen äärellinen laajennos. Pari $\{1, i\}$ muodostaa $\mathbb{C}$:n kannan $\mathbb{R}$-vektoriavaruutena, joten $[\mathbb{C} : \mathbb{R}] = 2$.
- Reaalilukujen kunta $\mathbb{R}$ on rationaalilukujen kunnan $\mathbb{Q}$ ääretön laajennos: esimerkiksi joukko $\{2^{1/n} \mid n \in \mathbb{N}, n \geq 1\}$ on vapaa kerroinkunnan $\mathbb{Q}$ suhteen (todistus jätetään harjoitustehtäväksi), joten laajennoksella $\mathbb{R}/\mathbb{Q}$ ei voi olla äärellistä kantaa.
- Esimerkissä 7.1 konstruoitiin alkukunnan $\mathbb{F}_3$ laajennos $\mathbb{F}_3[X]/\langle X^2 + 1\rangle$. Sama voidaan tehdä lähtien mistä tahansa kunnasta K kunnan $\mathbb{F}_3$ sijaan, kun käytetään jaotonta polynomia $p \in K[X]$. Tuloksena saadaan kunta $L = K[X]/\langle p\rangle$, jossa polynomilla p on juuri.
- Jos K on kunta, polynomirengas $K[X]$ on vapaa K-algebra, joka sisältää kunnan K (samastettuna vakiopolynomien kanssa). Rengas $K[X]$ ei ole kunta, joten se ei myöskään ole kunnan K laajennos. Se on kuitenkin kokonaisalue, jonka osamääräkunta on niin sanottu K-kertoimisten *rationaalilausekkeiden* joukko $K(X)$. Tämä joukko koostuu osamääristä f/g, missä $f, g \in K[X]$ ja $g \neq 0$. Kunta $K(X)$ on kunnan K laajennos. Lisäksi se sisältää vapaan joukon $\{1, X, X^2, \dots\}$, joten se on ääretön laajennos.

Peräkkäisten laajennosten asteille pätee seuraava transitiivisuustulos.

LAUSE 7.5. *Olkoon $K \subset L \subset M$ jono kuntia. Tällöin*

$$[M : K] = [M : L] \cdot [L : K].$$

Jos jompikumpi asteista $[M : L]$ ja $[L : K]$ on ääretön, niin $[M : K]$ on ääretön.

TODISTUS. Olkoot $\{a_i\}_{i\in I}$ ja $\{b_j\}_{j\in J}$ jotkin laajennosten L/K ja M/L kannat. Osoitetaan, että joukko $B = \{a_i b_j \mid i \in I, j \in J\}$ on laajennoksen M/K kanta. (Joukon B indeksöinnissä sallitaan $a_i b_j = a_k b_l$ eri indeksipareilla $(i, j) \neq (k, l)$. Todistuksesta kuitenkin seuraa, että tällaista tilannetta ei esiinny.)

Olkoon ensinnäkin $x \in M$. Tällöin voidaan kirjoittaa $x = \sum_j y_j b_j$, missä $y_j \in L$ kaikilla $j \in J$. Toisaalta jokaisella j pätee $y_j = \sum_i x_{ij} a_i$, missä $x_{ij} \in K$ kaikilla $i \in I$. Näin ollen $x = \sum_{i,j} x_{ij} a_i b_j$, mistä seuraa, että joukko B virittää K-vektoriavaruuden M.

Osoitetaan sitten, että B on vapaa. Oletetaan, että $\sum_{i,j} x_{ij} a_i b_j = 0$, missä $x_{ij} \in K$ kaikilla $i \in I$ ja $j \in J$. Joukko $\{b_j\}$ on vapaa L-avaruudessa M, ja $\sum_i x_{ij} a_i \in L$ kaikilla j, joten $\sum_i x_{ij} a_i = 0$ kaikilla j. Edelleen joukko $\{a_i\}$ on vapaa

K-avaruudessa L, joten $x_{ij} = 0$ kaikilla i ja j. Täten joukko B on laajennoksen M/K kanta. Siitä, että B on vapaa, seuraa erityisesti, että $a_i b_j \neq a_k b_l$, kun $i \neq k$ tai $j \neq l$. Näin saadaan lopulta $[M : K] = |B| = |I| \cdot |J| = [L : K] \cdot [M : L]$. Tämä sisältää myös sen tapauksen, että $[L : K]$ tai $[M : L]$ on ääretön. □

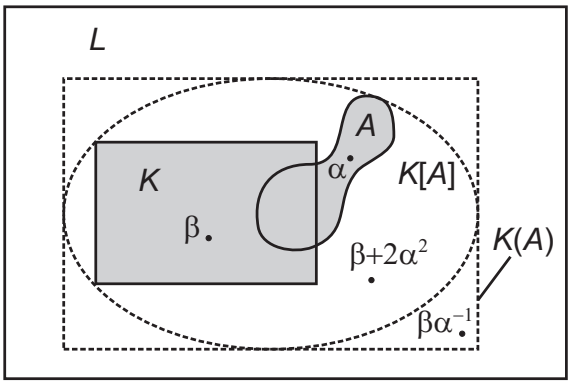
Jos $K \subset L \subset M$ on jono kuntia, laajennosta L/K kutsutaan laajennoksen M/K *alilaajennokseksi*. Edellisestä lauseesta seuraa, että jos aste $[M : K]$ on jokin positiivinen kokonaisluku n, asteet $[M : L]$ ja $[L : K]$ ovat luvun n tekijöitä. Erityisesti jos n on alkuluku, laajennoksella M/K ei ole epätriviaaleja alilaajennoksia L/K.

7.2. Laajennosten virittäminen. Kuntalaajennoksen käsittely algebrana helpottuu, jos sen kanta tunnetaan. Esimerkiksi kompleksilukujen kanta $\mathbb{R}$-algebrana on $\{1, i\}$, mikä tarkoittaa, että jokainen kompleksiluku voidaan kirjoittaa lineaarikombinaationa $a + bi$. Koska a ja b ovat jo läsnä reaalilukujen kunnassa, voidaan ajatella, että laajennos $\mathbb{C}$ on saatu lähtökunnasta $\mathbb{R}$ lisäämällä imaginaariyksikkö i. Tällöin sanotaan, että i virittää laajennoksen $\mathbb{C}/\mathbb{R}$. Huomaa, että kuntalaajennoksen virittäminen on eri asia kuin saman vektoriavaruuden virittäminen. Vektoriavaruuden $\mathbb{C}$ virittämiseen tarvitaan molemmat alkiot 1 ja i, laajennoksen virittämiseen riittää alkio i.

MÄÄRITELMÄ 7.6. Olkoon L kunnan K laajennos, ja olkoon $A \subset L$.

a) *Joukon A virittämä laajennoksen L/K alirengas* $K[A]$ on pienin kunnan L alirengas, joka sisältää sekä kunnan K että osajoukon A.
b) *Joukon A virittämä laajennoksen L/K alilaajennos* $K(A)$ on pienin kunnan L alikunta, joka sisältää sekä kunnan K että osajoukon A.

Tapauksessa, jossa joukko $A = \{a_1, \ldots, a_n\}$ on äärellinen, merkitään yksinkertaisesti $K[A] = K[a_1, \ldots, a_n]$ ja $K(A) = K(a_1, \ldots, a_n)$. Tällöin kuntaa $K(a_1, \ldots, a_n)$ nimitetään K:n *äärellisvirittеiseksi* laajennokseksi.



KUVA 9. Joukon A virittämät laajennoksen L/K alirengas $K[A]$ ja alilaajennos $K(A)$.

Koska alirenkaiden mielivaltainen leikkaus on alirengas ja sama pätee kunnille, joukot $K[A]$ ja $K(A)$ voidaan määritellä niiden alirenkaiden tai -kuntien leikkauksena, jotka sisältävät kunnan K sekä joukon A. Näin voidaan perustella joukkojen $K[A]$ ja $K(A)$ olemassaolo, joka ei määritelmän perusteella ole itsestään selvää.

Polynomialgebrat ovat vapaita äärellisviritteisiä algebroja. Sijoitushomomorfismista saadaan merkittävä yhteys K-kertoimisten polynomialgebrojen ja kunnan K äärellisviritteisten kuntalaajennosten välille.

LAUSE 7.7. *Olkoon L kunnan K laajennos, ja olkoot $a_1, \ldots, a_n \in L$. Tällöin*

$$K[a_1, \ldots, a_n] = \{f(a_1, \ldots, a_n) \mid f \in K[X_1, \ldots, X_n]\}$$

ja

$$K(a_1, \ldots, a_n) = \left\{ \frac{f(a_1, \ldots, a_n)}{g(a_1, \ldots, a_n)} \mid f, g \in K[X_1, \ldots, X_n],\ g(a_1, \ldots, a_n) \neq 0 \right\}.$$

Lisäksi $K(a_1, \ldots, a_n)$ on renkaan $K[a_1, \ldots, a_n]$ osamääräkunta.

TODISTUS. Olkoon $\varphi\colon K[X_1, \ldots, X_n] \to L$ alkioihin $a_1, \ldots, a_n$ liittyvä sijoitushomomorfismi. Tälle kuvaukselle pätee

$$\operatorname{Im}\varphi = \{f(a_1, \ldots, a_n) \mid f \in K[X_1, \ldots, X_n]\}.$$

Algebrahomomorfismin kuva on aina maalialgebran alialgebra, siis alirengas, joten $\operatorname{Im}\varphi$ on renkaan L alirengas.

Olkoon M nyt jokin toinen renkaan L alirengas, joka sisältää kunnan K lisäksi alkiot $a_1, \ldots, a_n$. Tällöin M sisältää myös kaikki kunnan K alkioista ja alkioista $a_1, \ldots, a_n$ muodostetut tulot sekä näiden summat. Siten $f(a_1, \ldots, a_n) \in M$ kaikilla $f \in K[X_1, \ldots, X_n]$. Näin ollen $\operatorname{Im}\varphi \subset M$, mistä määritelmän nojalla seuraa $K[a_1, \ldots, a_n] = \operatorname{Im}\varphi$.

Renkaan $K[a_1, \ldots, a_n]$ osamääräkunta Q puolestaan koostuu alkioista α/β, missä $\alpha, \beta \in K[a_1, \ldots, a_n]$ ja $\beta \neq 0$. Jokainen kunnan L alikunta, joka sisältää alkiot a_i, sisältää todistuksen alkuosan perusteella myös renkaan $K[a_1, \ldots, a_n]$. Tällöin se sisältää myös edellä mainitut osamäärät α/β, kunhan $\beta \neq 0$. Täten $K(a_1, \ldots, a_n) = Q$. □

ESIMERKKI 7.8. Laajennoksen $\mathbb{C}/\mathbb{Q}$ alilaajennos $\mathbb{Q}(i)$ koostuu edellisen lauseen nojalla osamääristä $f(i)/g(i)$, missä $f, g \in \mathbb{Q}[X]$ ja $g(i) \neq 0$. Koska $i^2 = -1$, voidaan olettaa, että f ja g ovat korkeintaan ensimmäisen asteen polynomeja. Tällöin

$$\mathbb{Q}(i) = \left\{ \frac{a + bi}{c + di} \mid a, b, c, d \in \mathbb{Q}, \text{ ja } c \neq 0 \text{ tai } d \neq 0 \right\}.$$

Edelleen $(c + di)^{-1} = q(c - di)$, missä $q = (c^2 + d^2)^{-1} \in \mathbb{Q}$, joten voidaan päätellä

$$\mathbb{Q}(i) = \{x + yi \mid x, y \in \mathbb{Q}\} = \mathbb{Q}[i].$$

Joukko $\{1, i\}$ virittää $\mathbb{Q}$-vektoriavaruuden $\mathbb{Q}[i]$. Lisäksi 1 ja i ovat lineaarisesti riippumattomia kerroinkunnan $\mathbb{Q}$ suhteen, joten $\{1, i\}$ on avaruuden $\mathbb{Q}[i]$ kanta. Laajennoksen $\mathbb{Q}(i)/\mathbb{Q}$ asteeksi saadaan näin ollen $[\mathbb{Q}(i) : \mathbb{Q}] = 2$.

Edellisessä esimerkissä havaittiin, että toisinaan $K[a_1, \ldots, a_n] = K(a_1, \ldots, a_n)$. Tämä tapahtuu täsmälleen silloin, kun alkiot a_i ovat *algebrallisia*. Algebrallisiin laajennoksiin palataan myöhemmin.

Esimerkissä nähtiin myös, että laajennos $\mathbb{Q}(i)/\mathbb{Q}$ oli äärellinen. Kaikki äärellisviritteiset laajennokset eivät kuitenkaan ole äärellisiä. Tämä liittyy jälleen virittäjäalkioiden algebrallisuuteen. Esimerkiksi kunnan $\mathbb{Q}$ laajennoksella $\mathbb{Q}(\pi) \subset \mathbb{R}$ ei ole äärellistä kantaa.

Ääretönviritteisten laajennosten tutkiminen palautetaan äärellisviritteiseen tapaukseen seuraavan lauseen avulla.

LAUSE 7.9. *Olkoon L kunnan K laajennos, ja olkoon $A \subset L$. Jos $\alpha \in K(A)$, niin $\alpha \in K(a_1, \ldots, a_n)$ joillain $a_1, \ldots, a_n \in A$. Täten*

$$K(A) = \bigcup \{K(a_1, \ldots, a_n) \mid a_i \in A \text{ kaikilla } i\}.$$

TODISTUS. Merkitään $F = \bigcup \{K(a_1, \ldots, a_n) \mid a_i \in A\}$. Jokainen äärellisviritteinen kunta $K(a_1, \ldots, a_n)$, missä $a_i \in A$ kaikilla i, sisältyy kuntaan $K(A)$. Täten $F \subset K(A)$. Toisaalta F sisältää kunnan K sekä joukon A, joten jos se on kunta, sen täytyy sisältää myös $K(A)$. Osoitetaan siis, että F on kunta. Olkoot $\alpha, \beta \in F$. Tällöin $\alpha \in K(a_1, \ldots, a_n)$ ja $\beta \in K(b_1, \ldots, b_m)$ joillain $a_i, b_i \in A$. Nyt alkiot $\alpha \pm \beta$, $\alpha\beta$ ja α/β (jos olemassa) ovat kunnassa $K(a_1, \ldots, a_n, b_1, \ldots, b_m)$, ja tämä kunta puolestaan sisältyy yhdisteeseen F. Siispä F on kunta, ja näin ollen $K(A) = F$. □

8. Algebralliset laajennokset

Kuntia tutkittaessa voidaan kysyä, onko tietyllä polynomilla juuria kyseisessä kunnassa. Jollei ole, voidaan konstruoida kuntalaajennos, jossa juuri löytyy (vrt. esimerkkiin 7.1). Toisaalta mistä tahansa annetusta laajennoksesta voidaan kysyä, mitkä alkioista ovat jotkin lähtökunnan polynomin juuria. Tällä tavalla laajennoksen alkiot jaetaan algebrallisiin ja transkendenttisiin. Algebrallisia alkioita voidaan käsitellä tehokkaasti niin sanottujen minimipolynomien avulla. Lopulta voidaan kysyä, onko olemassa laajennosta, joka sisältäisi kaikkien lähtökunnan polynomien kaikki juuret. Esimerkiksi kompleksilukujen kunta sisältää kaikki reaalikertoimisten polynomien juuret.

8.1. Algebrallisuus ja minimipolynomit.

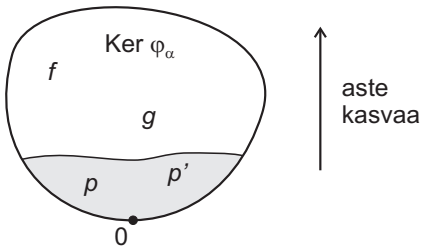
MÄÄRITELMÄ 8.1. Olkoon L kunnan K laajennos. Alkiota $\alpha \in L$ kutsutaan *algebralliseksi* kunnan K suhteen, jos on olemassa nollasta poikkeava polynomi $f \in K[X]$, jolle pätee $f(\alpha) = 0$. Jos tällaista polynomia ei ole, sanotaan, että α on *transkendenttinen* kunnan K suhteen. Jos kaikki kunnan L alkiot ovat algebrallisia kunnan K suhteen, sanotaan, että L on kunnan K *algebrallinen laajennos*.

Oletetaan, että L on kunnan K laajennos ja että $\alpha \in L$. Tarkastellaan sitä, miten algebrallisuus ja transkendenttisuus vaikuttavat alkioon α liittyvään sijoitushomomorfismiin $\varphi_\alpha \colon K[X] \to L$, $\varphi_\alpha(f) = f(\alpha)$. Ensinnäkin, mikäli α on transkendenttinen kunnan K suhteen, kaikilla nollasta poikkeavilla polynomeilla $f \in K[X]$ pätee $f(\alpha) \neq 0$. Tämä tarkoittaa, että sijoitushomomorfismin ydin

$$\operatorname{Ker} \varphi_\alpha = \{f \in K[X] \mid f(\alpha) = 0\}$$

on nollaideaali.

Vastaavasti α on algebrallinen, jos ja vain jos sijoitushomomorfismin ydin on epätriviaali. Koska $K[X]$ on pääideaalirengas (lause 6.16), ideaali $\operatorname{Ker} \varphi_\alpha$ on jonkin yhden polynomin p virittämä, eli $\operatorname{Ker} \varphi_\alpha = \langle p \rangle$. Tutkitaan tätä polynomia tarkemmin.



KUVA 10. Sijoitushomomorfismin ytimen virittää mikä tahansa minimaalisen asteen omaava nollasta poikkeava polynomi.

Koska jokainen ideaalin $\langle p \rangle$ polynomi on jaollinen polynomilla p, nähdään, että polynomin p aste on minimaalinen joukon $\operatorname{Ker} \varphi_\alpha$ nollasta poikkeavien polynomien keskuudessa (ks. kuva 10). Joukossa $\operatorname{Ker} \varphi_\alpha$ voi toki olla monia polynomin p kanssa samanasteisia polynomeja, mutta koska ne ovat kaikki jaollisia polynomilla p, ne eroavat tästä jollain vakiopolynomilla. Ne ovat siis polynomin p

liittoalkioita, ja ne kaikki virittävät saman ideaalin $\operatorname{Ker}\varphi_\alpha$. Polynomin p määräämiseksi yksikäsitteisesti riittää siis viritysominaisuuden lisäksi vaatia esimerkiksi, että korkeimman asteen kerroin on 1 eli että p on niin sanottu *pääpolynomi*. Tälle virittäjäpolynomille on varattu erityisnimi.

MÄÄRITELMÄ 8.2. Oletetaan, että $\alpha \in L$ on algebrallinen kunnan K suhteen. Alkion α *minimipolynomi* kunnan K suhteen on sellainen nollasta poikkeava pääpolynomi $p \in K[X]$, jolle pätee $p(\alpha) = 0$ ja jonka aste on pienin tällaisten polynomien joukossa. Alkion α minimipolynomia kunnan K suhteen merkitään $p = \min(K, \alpha)$.

Määritelmän mukaan minimipolynomille p pätee $p(\alpha) = 0$, joten $p \in \operatorname{Ker}\varphi_\alpha$. Edelleen minimipolynomin p aste on minimaalinen, joten määritelmää edeltävän pohdinnan nojalla p virittää ytimen $\operatorname{Ker}\varphi_\alpha$. Alkion α minimipolynomi voidaankin karakterisoida niin, että se on *se pääpolynomi, joka virittää alkioon α liittyvän sijoitushomomorfismin ytimen.*

ESIMERKKI 8.3. Luku $\sqrt{2}$ on algebrallinen kunnan $\mathbb{Q}$ suhteen, sillä se on polynomin $X^2 - 2$ juuri. Koska $\sqrt{2}$ ei ole rationaaliluku, se ei ole minkään ensimmäisen asteen rationaalikertoimisen polynomin juuri. Näin ollen $\min(\mathbb{Q}, \sqrt{2}) = X^2 - 2$. Sen sijaan $\min(\mathbb{R}, \sqrt{2}) = X - \sqrt{2}$.

Alkion α minimipolynomista on muun muassa se hyöty, että sen aste kertoo laajennoksen $K(\alpha)$ asteen. Seuraavassa lauseessa tämä seikka on koottu yhteen muiden ominaisuuksien kanssa.

LAUSE 8.4. *Olkoon L kunnan K laajennos, ja olkoon $\alpha \in L$ algebrallinen kunnan K suhteen. Merkitään $\min(K, \alpha) = p$.*

i) Olkoon $f \in K[X]$. Tällöin $f(\alpha) = 0$, jos ja vain jos $p \mid f$.
ii) Minimipolynomi p on jaoton renkaassa $K[X]$.
iii) Rengas $K[\alpha]$ on kunta, ja $K[\alpha] = K(\alpha)$.
iv) Jos n on polynomin p aste, niin alkiot $1, \alpha, \ldots, \alpha^{n-1}$ muodostavat laajennoksen $K(\alpha)/K$ kannan. Erityisesti laajennoksen $K(\alpha)$ aste on n, ja laajennos on äärellinen.

TODISTUS. i) Harjoitustehtävä.

ii) Oletetaan, että $p = fg$ joillain $f, g \in K[X]$, jolloin

$$f(\alpha)g(\alpha) = p(\alpha) = 0.$$

Alkiot $f(\alpha)$ ja $g(\alpha)$ ovat kunnassa L. Koska L on kokonaisalue, pätee $f(\alpha) = 0$ tai $g(\alpha) = 0$. Edellisestä kohdasta seuraa, että p jakaa jommankumman polynomeista f ja g. Toisaalta f ja g jakavat molemmat oletuksen nojalla polynomin p, joten jompikumpi niistä on polynomin p liittoalkio ja toinen siis yksikkö. Täten p on jaoton.

iii) Lauseen 7.7 mukaan $K[\alpha] = \operatorname{Im}\varphi_\alpha$, ja toisaalta $\langle p \rangle = \operatorname{Ker}\varphi_\alpha$. Algebrojen homomorfialauseesta seuraa nyt, että $K[X]/\langle p \rangle \cong K[\alpha]$. Kunnan L alirenkaana $K[\alpha]$ on kokonaisalue, joten $\langle p \rangle$ on alkuideaali. Toisaalta $K[X]$ on pääideaalirengas, joten korollaarin 6.13 nojalla ideaali $\langle p \rangle$ on maksimaalinen. Täten $K[\alpha]$ on itse asiassa kunta. Lisäksi $K[\alpha] = K(\alpha)$, koska $K[\alpha] \subset K(\alpha)$ ja $K(\alpha)$ on pienin kunta, joka sisältää sekä kunnan K että alkion α.

iv) Olkoon $n = \deg(p)$. Viritysominaisuuden tarkistamista varten oletetaan, että $x \in K(\alpha)$. Edellisen kohdan nojalla $x = f(\alpha)$ jollain $f \in K[X]$. Jakoyhtälöstä nähdään, että $f = qp + r$ joillain $q, r \in K[X]$, joille pätee $\deg(r) < n$. Nyt $f(\alpha) = r(\alpha)$, koska $p(\alpha) = 0$. Alkio $x = r(\alpha)$ on siis lineaarikombinaatio alkioista $1, \alpha, \ldots, \alpha^{n-1}$.

Vapauden osoittamiseksi oletetaan, että $\sum_{i=0}^{n-1} c_i \alpha^i = 0$ joillain $c_i \in K$. Tällöin polynomille $g = \sum_{i=0}^{n-1} c_i X^i$ pätee $g(\alpha) = 0$, joten kohdan i) perusteella p jakaa polynomin g. Kuitenkin polynomin g aste on pienempi kuin n, joten polynomin g on oltava nollapolynomi. Toisin sanoen $c_i = 0$ kaikilla i, joten joukko $\{1, \alpha, \ldots, \alpha^{n-1}\}$ on vapaa. Kyseinen joukko muodostaa siis laajennoksen $K(\alpha)$ kannan kerroinkunnan K suhteen. Loput väitteet seuraavat tästä suoraan. □

Esimerkki 8.5. Esimerkissä 7.8 selvitettiin laajennoksen $\mathbb{Q}(i)/\mathbb{Q}$ alkiot, minkä jälkeen todettiin, että kyseisen laajennoksen aste on kaksi. Lausetta 8.4 käyttämällä alkioita ei tarvitse selvittää asteen löytämiseksi, vaan voidaan edetä seuraavasti. Luku i on polynomin $f = X^2 + 1$ juuri. Lauseen kohdan i) perusteella luvun i minimipolynomi jakaa polynomin f renkaassa $\mathbb{Q}[X]$. Koska f on toisen asteen polynomi, jolla ei ole juuria kunnassa $\mathbb{Q}$, se on jaoton, ja siksi minimipolynomin liittoalkio. Toisaalta f on pääpolynomi, joten f on itse kyseinen minimipolynomi. Lauseen kohdasta iv) selviää lopulta, että $[\mathbb{Q}(i) : \mathbb{Q}] = 2$.

Esimerkki 8.6. Tarkastellaan laajennosta $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Polynomille $f = X^3 - 2$ pätee $f(\sqrt[3]{2}) = 0$, ja toisaalta f on jaoton renkaassa $\mathbb{Q}[X]$. Nyt voidaan edellisen esimerkin tapaan päätellä, että f on luvun $\sqrt[3]{2}$ minimipolynomi, jolloin laajennoksen $\mathbb{Q}(\sqrt[3]{2})$ aste on 3. Lauseen 8.4 kohdasta iii) seuraa, että $\mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q}(\sqrt[3]{2})$, joten jokainen laajennoksen alkio on muotoa $a + b\sqrt[3]{2} + c\sqrt[3]{4}$. Tämä koskee myös käänteislukuja x^{-1}, kun $x \in \mathbb{Q}[\sqrt[3]{2}]$.

Esimerkki 8.7. Kompleksiluku $\omega = e^{2\pi i/3} = -1/2 + i\sqrt{3}/2$ on polynomin $f = X^3 - 1$ juuri. Tämä polynomi jakautuu tekijöihin renkaassa $\mathbb{Q}[X]$ seuraavasti: $f = (X - 1)(X^2 + X + 1)$. Lauseen 8.4 kohdan ii) nojalla f ei siis voi olla luvun ω minimipolynomi kunnan $\mathbb{Q}$ suhteen. Voidaan kuitenkin helposti tarkistaa, että jälkimmäinen tekijä $X^2 + X + 1$ on jaoton renkaassa $\mathbb{Q}[X]$ ja että sillä on juurenaan ω. Siispä alkion ω minimipolynomi on $X^2 + X + 1$, ja $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$.

Ei ole vaikea nähdä, että äärellinen laajennos on aina äärellisviritteinen, sillä alkiot, jotka virittävät laajennoksen vektoriavaruutena, virittävät sen myös algebrana. Lisäksi äärellinen laajennos on aina algebrallinen, sillä transkendenttisen alkion potensseista saadaan mielivaltaisen suuria vapaita joukkoja. Näistä havainnoista saadaan seuraava lause.

Lause 8.8. *Olkoon L kunnan K äärellinen laajennos. Tällöin L on äärellisviritteinen ja algebrallinen kunnan K suhteen.*

Äärellisviritteinen laajennos ei ole aina äärellinen, sillä esimerkiksi $\mathbb{Q}(\pi)$ on kunnan $\mathbb{Q}$ ääretön laajennos. Jos virittäjät ovat algebrallisia, tilanne on toinen.

Lause 8.9. *Olkoon L kunnan K laajennos, ja olkoon n positiivinen kokonaisluku. Oletetaan, että $\alpha_i \in L$ on kunnan K suhteen algebrallinen alkio kaikilla $i \in \{1, \ldots, n\}$. Tällöin $K[\alpha_1, \ldots, \alpha_n]$ on kunnan K äärellinen laajennos, jonka asteelle pätee*

$$[K[\alpha_1, \ldots, \alpha_n] : K] \leq \prod_{i=1}^{n} [K(\alpha_i) : K].$$

TODISTUS. Käytetään induktiota virittäjien lukumäärän n suhteen. Tapaus $n = 1$ seuraa suoraan lauseesta 8.4. Oletetaan induktioaskelta varten, että $n \geq 1$ ja että väite pätee mille tahansa renkaalle $K[\beta_1, \ldots, \beta_n]$, missä jokainen β_i on algebrallinen.

Tarkastellaan rengasta $K[\alpha_1, \ldots, \alpha_{n+1}]$, missä jokainen α_i on algebrallinen. Merkitään $K' = K[\alpha_1, \ldots, \alpha_n]$, jolloin $K[\alpha_1, \ldots, \alpha_{n+1}] = K'[\alpha_{n+1}]$. Induktio-oletuksen nojalla K' on kunnan K algebrallinen laajennos, erityisesti kunta. Koska α_{n+1} on algebrallinen kunnan K ja siten myös kunnan K' suhteen, lauseesta 8.4 seuraa, että $K'[\alpha_{n+1}]$ on kunta ja $K'[\alpha_{n+1}] = K'(\alpha_{n+1})$.

Merkitään $f = \min(K, \alpha_{n+1})$, jolloin $f(\alpha_{n+1}) = 0$. Koska $f \in K[X] \subset K'[X]$, lauseen 8.4 mukaan minimipolynomi $\min(K', \alpha_{n+1})$ jakaa polynomin f. Täten

$$[K'(\alpha_{n+1}) : K'] \leq [K(\alpha_{n+1}) : K] < \infty.$$

Induktio-oletuksen ja lauseen 7.5 perusteella saadaan

$$[K'[\alpha_{n+1}] : K] = [K'[\alpha_{n+1}] : K'] \cdot [K' : K] \leq \prod_{i=1}^{n+1} [K(\alpha_i) : K].$$

Induktioperiaatteen nojalla lauseen väitteet pätevät. □

Edellisestä lauseesta nähdään, että lauseen 8.8 implikaatio voidaan kääntää. Toisin sanoen äärellisviritteinen ja algebrallinen laajennos on aina äärellinen. Tulosta ei voida laajentaa äärettömälle virittäjäjoukolle, sillä esimerkiksi joukko $\{2^{1/n} \mid n \in \mathbb{N}, n \geq 1\}$ virittää kunnan $\mathbb{Q}$ algebrallisen laajennoksen, jonka aste on ääretön.

Lauseista 8.8 ja 8.9 saadaan suoraan seuraava ehto alkion algebrallisuudelle.

KOROLLAARI 8.10. *Olkoon L kunnan K laajennos. Tällöin $\alpha \in L$ on algebrallinen kunnan K suhteen, jos ja vain jos $[K(\alpha) : K]$ on äärellinen.*

Lauseesta 7.5 seuraa, että laajennoksen äärellisyys on transitiivinen ominaisuus. Tätä tulosta käyttämällä voidaan lopuksi todistaa, että myös laajennoksen algebrallisuus on transitiivista.

LAUSE 8.11. *Olkoon $K \subset L \subset M$ jono kuntia. Jos L/K ja M/L ovat algebrallisia laajennoksia, niin M/K on algebrallinen.*

TODISTUS. Oletetaan, että $x \in M$. Olkoon $p = a_0 + a_1 X + \cdots + a_n X^n$ alkion x minimipolynomi kunnan L suhteen. Merkitään $K' = K(a_0, \ldots, a_n)$. Koska L on algebrallinen kunnan K suhteen ja $a_i \in L$ jokaisella i, laajennos K'/K on äärellinen lauseen 8.9 perusteella. Nyt $p \in K'[X]$, joten x on algebrallinen kunnan K' suhteen. Täten $[K'(x) : K']$ on äärellinen, ja

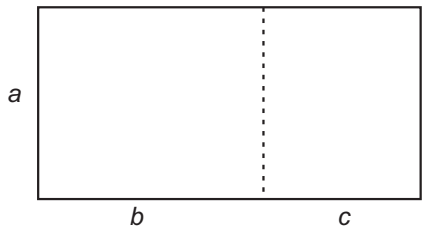
$$[K'(x) : K] = [K'(x) : K'] \cdot [K' : K] < \infty.$$

Edelleen $K(x) \subset K'(x)$, joten $[K(x) : K] < \infty$. Lauseesta 8.8 seuraa, että laajennos $K(x)/K$ on algebrallinen. Erityisesti siis alkio x on algebrallinen kunnan K suhteen, ja koska x oli mielivaltainen, koko laajennos M/K on algebrallinen. □

8.2. Sovellus: harppi–viivainkonstruktiot. Edellä käsiteltyä algebrallisten laajennosten teoriaa voidaan käyttää tiettyjen klassisten geometristen konstruktio-ongelmien tutkimiseen. Nämä konstruktiot, joista ehkä tunnetuin kulkee nimellä ympyrän neliöinti, ovat askarruttaneet matemaatikkojen mieliä antiikista

1800-luvulle saakka, jolloin niiden toteuttaminen viimein osoitettiin mahdottomaksi algebrallisten menetelmien avulla.

Antiikin Kreikassa geometrialla oli erityisen tärkeä sija matemaattisessa kirjallisuudessa. Algebrallisten merkintöjen puuttuessa geometriaa käytettiin laajasti matemaattisten (eli lähinnä geometristen ja lukuteoreettisten) tulosten esittämiseen. Lukuja edustivat eripituiset janat: yhteenlasku tulkittiin kahden janan liittämiseksi peräkkäin, ja kahden luvun tulo tarkoitti sellaisen suorakulmion muodostamista, jonka sivut vastasivat kerrottavia lukuja. Näin voitiin esittää esimerkiksi osittelulaki $a(b+c) = ab+ac$ jakamalla suorakulmio, jonka sivujen pituudet ovat a ja $b+c$, kahdeksi suorakulmioksi, jotka vastasivat tuloja ab ja ac.



KUVA 11. Osittelulakia esittävä geometrinen konstruktio.

Perinteisen tarinan mukaan filosofi Platon[1] vaati, että geometriset konstruktiot olisi toteutettava vain harppia ja viivainta hyväksi käyttäen. Viivaimella sai piirtää rajattoman pitkän suoran kahden tunnetun pisteen kautta, ja harpilla oli sallittua piirtää ympyrä, jonka keskipiste ja säde tunnettiin. (Alun perin säännöt annettiin vielä tiukemmassa muodossa, mutta ne olivat yhtäpitävät tässä esitettyjen kanssa.) Pian nousi esiin kolme ongelmaa, joita kreikkalaiset eivät pystyneet ratkaisemaan edes lukemattomien yritysten jälkeen:

1. *Ympyrän neliöinti.* On tuotettava sellaisen neliön sivu, jonka pinta-ala on sama kuin annetulla ympyrällä.
2. *Kuution kahdentaminen.* On tuotettava sellaisen kuution sivu, jonka tilavuus on kaksi kertaa annetun kuution tilavuus.
3. *Kulman kolmiajako.* On tuotettava kulma, jonka suuruus on kolmasosa annetun kulman suuruudesta.

Kreikkalaisten epäonnistuminen yllä mainittujen tehtävien ratkaisemisessa ei ollut osoitus heidän kyvyttömyydestään. Vuonna 1837 Pierre Wantzel nimittäin osoitti, että 2. ja 3. konstruktio eivät olisi mahdollisia suorittaa pelkästään harpilla ja viivaimella. Myös 1. konstruktio on mahdoton, mutta tämän todistaminen onnistui vasta, kun Ferdinand von Lindemann osoitti vuonna 1882 luvun π transkendenttisuuden.

Selvitetään nyt, miten geometriset konstruktio-ongelmat voidaan formuloida algebran kielellä. Tarkasteltavina ovat tason pistejoukot $G \subset \mathbb{R}^2$, joita nimitetään *kuvioiksi*. *Kuvion G suora* on suora, joka kulkee joukon G kahden pisteen kautta. *Kuvion G ympyrä* taas on ympyrä, jonka keskipiste on joukossa G ja säde kahden joukon G pisteen välinen etäisyys.

[1]Platon (428/427–348/347 eKr.), ateenalainen filosofi, Ateenan Akatemian perustaja. Platon oli aikanaan huomattava vaikuttaja myös matematiikan alalla, vaikka hänen ei tiedetä itse tuottaneen omaperäisiä matemaattisia tuloksia.

Olkoon annettu kuvio $G_0 \subset \mathbb{R}^2$. *Geometrinen konstruktio joukosta* G_0 on äärellinen jono kuvioita

$$G_0 \subset G_1 \subset \cdots \subset G_n,$$

missä $G_{i+1} = G_i \cup \{P_{i+1}\}$ kaikilla $i < n$ ja P_{i+1} on jokin kuvion G_i suorien tai ympyröiden leikkauspiste. Sanotaan, että kuvio G *voidaan konstruoida kuviosta* G_0, jos on olemassa geometrinen konstruktio $G_0 \subset \cdots \subset G_n$, missä $G_n = G$.

Edellä on ainoastaan käännetty antiikin konstruktiometodi nykymatematiikan kielelle. Algebra tulee mukaan, kun pohditaan kuvion pisteiden koordinaatteja ja erityisesti sitä, miten nuo koordinaatit saadaan rationaalikoordinaatteja laajentamalla. Määritellään siis *kuvion* G *kunta* K_G laajennoksena $\mathbb{Q}(A)$, missä A sisältää kaikkien kuvion G pisteiden x- ja y-koordinaatit.

Seuraava lause antaa algebrallisen ehdon kuvion konstruoitavuudelle.

LAUSE 8.12. *Jos kuvio* G *voidaan konstruoida kuviosta* G_0*, kuvion kunnan asteelle pätee*

$$[K_G : K_{G_0}] = 2^n$$

jollain $n \in \mathbb{N}$.

TODISTUS. Olkoon $G_0 \subset \cdots \subset G_n = G$ geometrinen konstruktio. Analyyttisen geometrian perusteista tiedetään, että jokaista kuvion G_i suoraa ja ympyrää kuvaa polynomiyhtälö, jonka kertoimet ovat kunnassa K_{G_i} ja joka on korkeintaan toista astetta. Edelleen tiedetään, että näiden suorien ja ympyröiden leikkauspisteiden löytämiseksi on ratkaistava korkeintaan toisen asteen yhtälöpari, jonka ratkaisut ovat muotoa $x = a_1 + b_1\sqrt{c}$ ja $y = a_2 + b_2\sqrt{c}$, missä $a_1, a_2, b_1, b_2, c \in K_{G_i}$. Täten $K_{G_{i+1}} \subset K_{G_i}(\sqrt{c})$. Koska luvun $\sqrt{c}$ minimipolynomi kunnan K_{G_i} suhteen on korkeintaan toista astetta, saadaan lopulta $[K_{G_{i+1}} : K_{G_i}] \leq 2$. Väite seuraa tästä induktiolla, kun käytetään lausetta 7.5. □

Yllä oleva lause pätee myös käänteisessä muodossa: jos aste $[K_G : K_{G_0}]$ on luvun kaksi potenssi, kuvio G voidaan konstruoida kuviosta G_0. Tätä ei kuitenkaan tarvita silloin, kun konstruktioita osoitetaan mahdottomiksi, kuten seuraavassa esimerkissä tehdään.

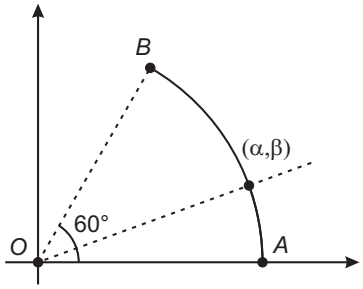
ESIMERKKI 8.13. *Kulman kolmiajako.* Osoitetaan, että esimerkiksi 60° kulmaa ei voi jakaa kolmeen osaan harpilla ja viivaimella. Valitaan koordinaatisto niin, että annettu 60 asteen kulma tulee suorien OA ja OB väliin, missä $O = (0, 0)$, $A = (1, 0)$ ja $B = (1/2, \sqrt{3}/2)$ (ks. kuva 12). Olkoon $G_0 = \{O, A, B\}$, jolloin $K_{G_0} = \mathbb{Q}(\sqrt{3})$ ja $[K_{G_0} : \mathbb{Q}] = 2$.

Oletetaan, että kulma AOB voidaan jakaa kolmeen osaan. Tällöin syntyvän kulman kyljen ja origokeskisen yksikköympyrän leikkauspiste (joka siis myös voidaan konstruoida) on (α, β), missä $\alpha = \cos 20°$ ja $\beta = \sin 20°$. Oletuksen mukaan voidaan konstruoida kuvio G, joka sisältää pisteen (α, β).

Tutkitaan tarkemmin koordinaattia α. Kolminkertaisen kulman kosinin kaavasta nähdään, että

$$\cos(3 \cdot 20°) = 4\cos^3 20° - 3\cos 20° = 4\alpha^3 - 3\alpha.$$

Koska $\cos 60° = 1/2$, tästä seuraa, että α on polynomin $8X^3 - 6X - 1$ juuri. Voidaan helposti tarkistaa, että tämä polynomi on jaoton kunnan $\mathbb{Q}$ suhteen, joten se



KUVA 12. Kulman kolmiajako.

on minimipolynomin $\min(\mathbb{Q}, \alpha)$ liittoalkio. Siispä kyseisen minimipolynomin aste on 3, ja edelleen $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Lauseiden 8.12 ja 7.5 perusteella

$$[K_G : \mathbb{Q}] = [K_G : K_{G_0}] \cdot [K_{G_0} : \mathbb{Q}] = 2^n \cdot 2 = 2^{n+1}$$

jollain $n \in \mathbb{N}$, mutta toisaalta

$$[K_G : \mathbb{Q}] = [K_G : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] = [K_G : \mathbb{Q}(\alpha)] \cdot 3.$$

Tämä on selvästi mahdotonta, joten kuviota G ei voida konstruoida.

Edellinen esimerkki osoittaa, että mielivaltaisen kulman jakamiseksi kolmeen osaan harpilla ja viivaimella ei voi olla olemassa yleistä menetelmää. Joitakin kulmia silti voidaan jakaa kolmeen osaan: esimerkiksi 30 asteen kulma voidaan konstruoida, mikä tarkoittaa sitä, että suoran kulman kolmiajako onnistuu.

8.3. Transkendenttiluvut. Alkion todistamiseksi algebralliseksi riittää löytää polynomi, jonka juuri kyseinen alkio on. Transkendenttisuuden todistaminen voi sen sijaan olla hankalampaa. Jotkin tapaukset ovat kuitenkin selkeitä. Oletetaan esimerkiksi, että K on kunta, ja tarkastellaan polynomialgebran $K[X]$ jakokuntaa $K(X)$. Tämä kunta on kunnan K laajennos. Lisäksi kaikkien K-kertoimisten polynomien joukko $K[X]$ sisältyy kuntaan $K(X)$, ja alkioon X liittyvä sijoitushomomorfismi $K[X] \to K(X)$ on inkluusiokuvaus. Toisin sanoen sijoitettaessa alkio X polynomiin f tuloksena on f. Siispä $f(X) = 0$, jos ja vain jos $f = 0$, joten $X \in K(X)$ on transkendenttinen.

Useimmiten transkendenttisista luvuista puhuttaessa tarkoitetaan reaali- tai kompleksilukuja, jotka ovat transkendenttisia rationaalilukujen kunnan suhteen. Nykyään on tunnettua, että transkendenttisia lukuja on olemassa, vieläpä runsain mitoin. On nimittäin varsin helppo osoittaa, että $\mathbb{Q}$-kertoimisia polynomeja on vain numeroituva määrä, jolloin myös niiden juuria on numeroituvan monta (ks. lemma 8.18). Siispä niin kutsuttujen *algebrallisten lukujen* joukko

$$\mathbb{A} = \{\alpha \in \mathbb{C} \mid \alpha \text{ on algebrallinen kunnan } \mathbb{Q} \text{ suhteen}\}$$

on numeroituva. Toisaalta kompleksilukujen joukko on ylinumeroituva, joten valtaosa kompleksiluvuista (tai yhtä hyvin reaaliluvuista) on transkendenttisia.

Yllä esitetty päättely on mahdollista tehdä vain, jos kompleksilukujen joukon ylinumeroituvuus tunnetaan. Viimeksi mainitun seikan todisti Georg Cantor vuonna 1878. Kuitenkin jo aiemmin – tarkemmin sanottuna vuonna 1844 – Joseph Liouville oli osoittanut, että eräät hänen löytämänsä luvut ovat transkendenttisia reaalilukuja. Näitä lukuja kutsutaan nykyään Liouvillen luvuiksi. Liouvillen

löytö oli ensimmäinen osoitus transkendenttisten lukujen olemassaolosta. Tunnetumpi esimerkki transkendenttisesta luvusta saatiin vuonna 1873, kun Charles Hermite osoitti Neperin luvun e transkendenttisuuden. Hieman myöhemmin, eli vuonna 1882, Ferdinand von Lindemann onnistui Hermiten menetelmää mukaillen osoittamaan, että myös luku π on transkendenttinen rationaalilukujen suhteen. Lindemannin ja Hermiten todistukset käyttävät analyyttisiä menetelmiä.

Avoimeksi ongelmaksi sen sijaan on jäänyt muun muassa se, onko e algebrallinen vai transkendenttinen laajennoksen $\mathbb{Q}(\pi)$ suhteen (tai yhtä hyvin π laajennoksen $\mathbb{Q}(e)$ suhteen) eli onko olemassa polynomia, jonka kertoimissa saa hyödyntää piin potensseja ja jolla on juurena e.

8.4. Algebrallinen sulkeuma. Algebrallisia kuntalaajennoksia voidaan rakentaa jaottomista polynomeista esimerkin 7.1 tapaan. Jos polynomi f ei jakaannu kunnan K suhteen ensimmäisen asteen tekijöihin, sillä on jokin jaoton vähintään toista astetta oleva tekijä g, ja tämän avulla voidaan tuottaa kuntalaajennos L, josta löytyy juuri jaottomalle tekijälle g. Tällöin L/K on algebrallinen laajennos, sillä se sisältyy polynomien f juurten virittämään laajennokseen. Jatkamalla samaan tapaan saadaan mille tahansa äärelliselle polynomijoukolle konstruoitua algebrallinen laajennos, jossa kaikki joukon polynomit jakautuvat ensimmäisen asteen tekijöihin.

Toisaalta on myös olemassa kuntia, joissa jokainen polynomi jakautuu ensimmäisen asteen tekijöihin. Tällaista kuntaa ei voi laajentaa algebrallisesti, sillä se sisältää jo kaikkien polynomiensa juuret.

MÄÄRITELMÄ 8.14. Kunta K on *algebrallisesti suljettu*, jos jokainen polynomi $f \in K[X]$, joka ei ole vakio, jakautuu 1. asteen tekijöihin renkaassa $K[X]$.

Algebrallisesti suljetut kunnat voidaan karakterisoida monella tapaa.

LAUSE 8.15. *Olkoon K kunta. Seuraavat ehdot ovat yhtäpitäviä.*

a) Kunta K on algebrallisesti suljettu.
b) Jokaisella polynomilla $f \in K[X]$, joka ei ole vakio, on juuri kunnassa K.
c) Kunnalla K ei ole aitoja algebrallisia laajennoksia.
d) Kunnalla K ei ole aitoja äärellisiä laajennoksia.
e) Jos L on kunnan K laajennos, niin K koostuu täsmälleen niistä kunnan L alkioista, jotka ovat algebrallisia kunnan K suhteen.

TODISTUS. Harjoitustehtävä. □

Algebrallisesti suljettua kuntaa ei voi laajentaa algebrallisesti, mutta jos siihen lisää jonkin transkendenttialkion, kunta lakkaa olemasta algebrallisesti suljettu. Tällöin sitä voidaan edelleen laajentaa algebrallisesti, kunnes mahdollisesti saavutetaan uusi algebrallisesti suljettu kunta. Kuntaa, joka on algebrallisesti suljettu ja jota on laajennettu ainoastaan algebrallisesti jonkin lähtökunnan suhteen, nimitetään lähtökunnan algebralliseksi sulkeumaksi.

MÄÄRITELMÄ 8.16. Kunnan K *algebrallinen sulkeuma* $\overline{K}$ on kunnan K laajennos, joka on algebrallisesti suljettu ja algebrallinen.

Kunnan algebrallinen sulkeuma on sen suurin mahdollinen algebrallinen laajennos, koska sulkeuma on algebrallisesti suljettu eikä sillä itsellään siis voi olla

aitoja algebrallisia laajennoksia. Algebrallinen sulkeuma on toisaalta myös pienin algebrallisesti suljettu kunta, joka sisältää alkuperäisen kunnan. Jos nimittäin sulkeumasta poistaa yhdenkin alkion, poistuu samalla jonkin polynomin juuri, koska jokainen sulkeuman alkio on algebrallinen.

Algebrallisen sulkeuman määritelmä ja merkintätapa antavat ymmärtää, että jokaisella kunnalla olisi yksikäsitteinen algebrallinen sulkeuma. Tämä pitääkin paikkansa, mutta todistaminen vaatii Zornin lemmaa. Olemassaolo todistetaan lauseessa 8.19, mutta yksikäsitteisyyden todistaminen sivuutetaan.

Esimerkki 8.17. Kompleksilukujen kunta $\mathbb{C}$ on algebrallisesti suljettu. Tämä tulos, jonka Gauss todisti vuonna 1799[1], tunnetaan *algebran peruslauseen* nimellä. Sille on lukuisia todistuksia, jotka yleensä nojautuvat kompleksianalyysiin tai algebralliseen topologiaan. On olemassa myös Galois'n teoriaa käyttävä todistus, jossa tarvitaan algebrallisten menetelmien lisäksi vain väliarvolausetta. Pelkästään kompleksilaskennan perusteille rakentuva todistus on julkaistu Solmu-lehden numerossa 3/2011. Koska $\mathbb{C}$ on algebrallisesti suljettu ja algebrallinen reaalilukujen kunnan $\mathbb{R}$ suhteen, se on tämän kunnan algebrallinen sulkeuma.

Kompleksilukujen kunta ei kuitenkaan ole rationaalilukujen kunnan algebrallinen sulkeuma. Tarkastellaan luvussa 8.3 esiteltyä algebrallisten lukujen joukkoa

$$\mathbb{A} = \{\alpha \in \mathbb{C} \mid \alpha \text{ on algebrallinen kunnan } \mathbb{Q} \text{ suhteen}\}.$$

Melko helposti voidaan näyttää, että $\mathbb{Q}(\mathbb{A}) = \mathbb{A}$ ja toisaalta $\overline{\mathbb{A}} = \mathbb{A}$. Kunta $\mathbb{A}$ on siis rationaalilukujen algebrallinen laajennos ja lisäksi algebrallisesti suljettu. Algebralliset luvut muodostavat siis kunnan $\mathbb{Q}$ algebrallisen sulkeuman.

Näytetään vielä luvun lopuksi, että jokaisella kunnalla K on algebrallinen sulkeuma. Olemassaolotodistuksen perusidea on käyttää Zornin lemmaa kaikkien lähtökunnan K algebrallisten laajennosten kokoelmassa. Kyseinen kokoelma on kuitenkin lähtökohdaksi liian laaja, koska kunnalla K voi olla määrättömästi keskenään isomorfisia algebrallisia laajennoksia, joiden alkioita vain merkitään eri tavoin. Tämän korjaamiseksi todistuksessa lähdetään liikkeelle jostakin kiinnitetystä kunnan K ylijoukosta, joka on kuitenkin tarpeeksi suuri sisältääkseen algebrallisen sulkeuman. Koon varmistamiseksi käytetään seuraavaa joukko-opillista lemmaa. Lukija, joka ei tunne mahtavuuksien teoriaa, voi sivuuttaa todistuksen yksityiskohdat.

Lemma 8.18. *Jos L/K on algebrallinen laajennos, niin $|L| \leq \max\{|K|, |\mathbb{N}|\}$.*

Todistus. Jokainen polynomi $f = a_0 + a_1X + \cdots + a_nX^n \in K[X]$ voidaan samastaa äärellisen jonon $(a_0, \ldots, a_n)$ kanssa. Astetta n olevien K-kertoimisten polynomien joukon $K_n[X]$ mahtavuus on siis $|K^{n+1}|$. Jos K on äärellinen, tämä mahtavuus on $|K|^{n+1}$, muuten $|K^{n+1}| = |K|$. Koska $K[X]$ on numeroituva yhdiste joukoista $K_n[X]$, joukko-opin perustuloksista seuraa, että $|K[X]| \leq \max\{|K|, |\mathbb{N}|\}$.

Koska L/K on algebrallinen, jokainen kunnan L alkio on jonkin K-kertoimisen polynomin juuri. Indeksöidään jokaisen K-kertoimisen polynomin juuret $\alpha_1, \ldots, \alpha_r$ jossain mielivaltaisessa järjestyksessä, jolloin kutakin kunnan L alkiota α vastaa

[1]Oikeastaan Gaussin väitöskirjassaan esittämä todistus sisältää aukon. Jean-Robert Argand esitti täydellisen todistuksen vuonna 1806, ja Gauss julkaisi myöhemmin useitakin erilaisia aukottomia versioita.

yksikäsitteinen pari $(p, i) \in K[X] \times \mathbb{N}$, missä $p = \min(K, \alpha)$ ja alkion α indeksi polynomin p juurten joukossa on i. Näiden parien muodostaman joukon mahtavuus on korkeintaan $\max\{|K[X]|, |\mathbb{N}|\} = \max\{|K|, |\mathbb{N}|\}$. □

LAUSE 8.19. *Jokaisella kunnalla on algebrallinen sulkeuma.*

TODISTUS. Olkoon K mielivaltainen kunta. Olkoon S jokin joukko, joka sisältää kunnan K ja jolle pätee $|S| > \max\{|K|, |\mathbb{N}|\}$. Joillekin joukon S osajoukoille voidaan määritellä kuntarakenne, jonka suhteen niistä tulee kunnan K algebrallisia laajennoksia. Olkoon $\mathcal{A}$ nyt kaikkien tällaisten joukkoon S sisältyvien kunnan K algebrallisten laajennosten kokoelma. (Sama osajoukko voi esiintyä kokoelmassa useamman kerran erilaisilla kuntarakenteilla varustettuna.) Selvästi $K \in \mathcal{A}$, joten $\mathcal{A} \neq \emptyset$. Merkitään $L_1 \leq L_2$, kun L_2 on kunnan L_1 laajennos. Tämä relaatio tekee kokoelmasta $\mathcal{A}$ osittaisjärjestyksen.

On suoraviivaista tarkistaa, että osittaisjärjestyksessä $(\mathcal{A}, \leq)$ jokaisen ketjun yhdiste kuuluu edelleen joukkoon $\mathcal{A}$. Tämä yhdiste on ketjun yläraja. Zornin lemmasta seuraa nyt, että joukossa $\mathcal{A}$ on maksimaalinen alkio M, joka on siis algebrallinen kunnan K suhteen. On vielä osoitettava, että M on algebrallisesti suljettu.

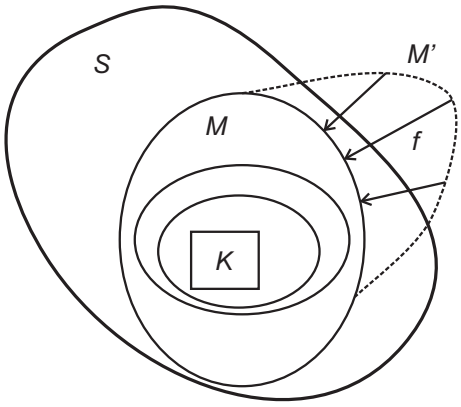
Olkoon M' jokin kunnan M algebrallinen laajennos. Koska sekä M'/M että M/K ovat algebrallisia laajennoksia, edellisestä lemmasta saadaan

$$|M'| \leq \max\{|M|, |\mathbb{N}|\} \leq \max\{|K|, |\mathbb{N}|\} < |S|.$$

Näin ollen löytyy jokin injektio $f\colon M' \to S$, jolle lisäksi pätee $f|_M = \mathrm{id}$. Kun määritellään kuvajoukossa fM' laskutoimitukset kaavoilla

$$f(a) + f(b) = f(a + b) \quad \text{ja} \quad f(a)f(b) = f(ab),$$

myös joukosta fM' tulee kunnan M algebrallinen laajennos, joka sisältyy joukkoon S. Nyt alkion M maksimaalisuudesta seuraa, että $fM' = M$, joten $M' = M$, koska $f|_M = \mathrm{id}$ ja f on injektio. Siispä M on algebrallisesti suljettu ja kunnan K algebrallinen sulkeuma.



KUVA 13. Maksimaalinen algebrallinen laajennos M on kunnan K algebrallinen sulkeuma.

□

Algebrallisen sulkeuman yksikäsitteisyyden todistaminen sivuutetaan.

Ryhmäteoriaa

Materiaalin viimeinen osa käsittelee ryhmiä. Ensimmäisessä luvussa tarkastellaan ryhmiä edustamassa symmetriaa. Abstraktien rakenteiden symmetrian mallintaminen johti alun perin ryhmän määrittelyyn Galois'n ja muiden tutkimuksissa, ja yhä nykyäänkin se on ryhmäteorian pääasiallinen sovelluskohde mitä erilaisimmilla matematiikan ja muiden tieteiden aloilla. Symmetrioiden teoreettisessa tarkastelussa on apua ryhmän toiminnan käsitteestä.

Symmetrioiden jälkeen perehdytään hieman tuloksiin, joiden avulla voidaan selvittää ryhmien sisäistä rakennetta. Viimeisessä luvussa tutustutaan vapaisiin ryhmiin.

9. Symmetriat ja ryhmän toiminta

Usein kuulee sanottavan, että ryhmät kuvaavat symmetrioita, mutta mitä tällä oikeastaan tarkoitetaan? Mitä symmetria ylipäätään on? Tällä kurssilla määrittelemme yksinkertaisesti, että joukon symmetrialla tarkoitetaan sellaista bijektiivistä kuvausta joukolta itselleen, joka säilyttää joukossa määritellyn rakenteen. Tällaiset kuvaukset muodostavat luonnollisella tavalla kaikkien annetun joukon bijektioiden aliryhmän. Bijektiota joukolta itselleen kutsutaan myös permutaatioksi, joten jokainen symmetriaryhmä on itse asiassa jonkin symmetrisen ryhmän aliryhmä.

Symmetriat ovat siis permutaatioita. Toisaalta minkä tahansa ryhmän alkiot voidaan toisinaan tulkita jonkin joukon symmetrioiksi, ja tällöin sanotaan, että ryhmä toimii tuossa joukossa. Toiminnan myötä ryhmän alkiot voidaan samastaa tiettyjen permutaatioiden kanssa, ja silloin puhutaan ryhmän permutaatioesityksestä. Ryhmän toiminnan teorian avulla voidaan tutkia tarkemmin symmetrioiden ominaisuuksia.

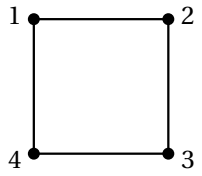
9.1. Esimerkkejä symmetriaryhmistä. Symmetrialla ei ole yleispätevää täsmällistä määritelmää, joten niihin täytyy tutustua esimerkkien kautta.

Esimerkki 9.1. Neliön symmetriaryhmä D_4 lienee tuttu aiemmista algebran opinnoista. Tarkastellaan tässä erästä tapaa määritellä kyseinen ryhmä. Esimerkkiin palataan myöhemmin.

Ajatellaan neliötä verkkona eli graafina. Neliön nurkat muodostavat verkon solmut ja neliön sivut verkon särmät. Numeroidaan nurkat kuvan 14 osoittamalla tavalla, jolloin verkon solmujen joukko on $N = \{1, 2, 3, 4\}$. Verkon symmetriat ovat ne joukon N permutaatiot, jotka säilyttävät verkon särmät. Toisin sanoen D_4 on symmetrisen ryhmän S_4 aliryhmä, ja σ kuuluu aliryhmään D_4, jos seuraava ehto on voimassa kaikilla $m, n \in N$:

> solmujen m ja n välillä on särmä jos ja vain jos solmujen $\sigma(m)$ ja $\sigma(n)$ välillä on särmä.

Esimerkiksi $\tau = (12)$ ei kuulu aliryhmään D_4, sillä solmujen 1 ja 3 välillä ei ole särmää, mutta solmujen $\tau(1) = 2$ ja $\tau(3) = 3$ välillä on.



KUVA 14. Neliö verkkona.

Vastaavalla tavalla voidaan määritellä minkä tahansa verkon symmetriaryhmä. Verkkojen symmetrioita kutsutaan myös niiden *automorfismeiksi*. Monikulmioiden symmetriaryhmiä kutsutaan puolestaan *diedriryhmiksi*, ja niistä käytetään merkintää D_n, missä n on monikulmion kärkien lukumäärä.

Kun ryhmän alkiot kirjoitetaan permutaatioina, kyseessä on ryhmän *permutaatioesitys*. Neliön symmetriaryhmä voitaisiin määritellä täysin abstraktisti esimerkiksi laskutoimitustaulun avulla, mutta permutaatioesitystä käytettäessä voidaan tukeutua permutaatioryhmien teoriaan.

ESIMERKKI 9.2. Olkoon $f \in \mathbb{Q}[X]$ jokin polynomi. Tämän polynomin kompleksijuuret virittävät jonkin rationaalilukujen laajennoksen L. Kunnan L automorfismit, eli isomorfismit kunnalta itselleen, muodostavat polynomin f *Galois'n ryhmän* $\mathrm{Gal}(f)$. Ei ole vaikea osoittaa, että Galois'n ryhmän alkiot kuvaavat polynomin juuret toisikseen. Jos juuret numeroidaan, voidaan Galois'n ryhmä tällä tavoin esittää jonkin symmetrisen ryhmän S_n aliryhmänä. Tässä esityksessä ei myöskään menetetä informaatiota: koska polynomin f juuret virittävät laajennoksen L, voidaan osoittaa, että laajennoksen L automorfismit riippuvat täysin siitä, miten juuret kuvautuvat.

Tarkastellaan esimerkkinä polynomia

$$f = X^2 - 2.$$

Tämän juuret $x_1 = \sqrt{2}$ ja $x_2 = -\sqrt{2}$ virittävät laajennoksen $\mathrm{Gal}(f) = \mathbb{Q}(\sqrt{2})$. Laajennoksen automorfismit kuvaavat juuret toisilleen, joten ainoat mahdolliset automorfismit ovat $\sigma_1 = \mathrm{id}$ ja

$$\sigma_2 \colon a + b\sqrt{2} \mapsto a - b\sqrt{2}.$$

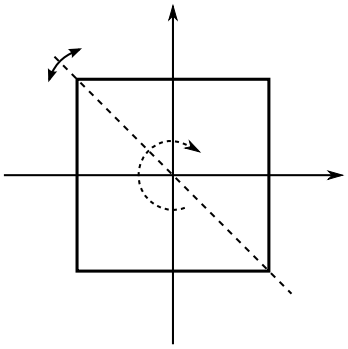
Tarkempi tarkastelu osoittaa, että σ_2 on todellakin kunnan $\mathbb{Q}(\sqrt{2})$ automorfismi.

Käyttämällä juurten numerointia hyväksi voidaan Galois'n ryhmää ajatella ryhmänä S_2. Tällä tavoin saadaan Galois'n ryhmän permutaatioesitys. Galois'n ryhmät on nimetty ranskalaisen Évariste Galois'n mukaan, joka todisti, että polynomin f juurille on olemassa algebrallinen ratkaisukaava, jos ja vain jos $\mathrm{Gal}(f)$ voidaan purkaa tietynlaiseksi vaihdannaisten ryhmien ketjuksi.

Polynomien kerroinkuntana voidaan käyttää muutakin kuntaa kuin rationaalilukuja. Tällöin Galois'n ryhmään otetaan vain ne automorfismit, jotka kiinnittävät kerroinkunnan. Lisäksi Galois'n ryhmä määritellään vain, jos polynomi f on *separoituva*, eli jos sen juuret kerroinkunnan algebrallisessa sulkeumassa ovat erillisiä. Separoituvia kuntia ovat muun muassa kaikki äärelliset kunnat sekä ne, joiden karakteristika on 0.

Esimerkki 9.3. Neliötä voidaan ajatella, paitsi verkkona esimerkin 9.1 tapaan, myös tasokuviona eli pistejoukkona $X \subset \mathbb{R}^2$. Tasokuvioista puhuttaessa symmetrioina pidetään yleensä sellaisia kuvauksia, jotka säilyttävät kaikkien pisteiden väliset etäisyydet. Näitä kutsutaan *isometrioiksi*.

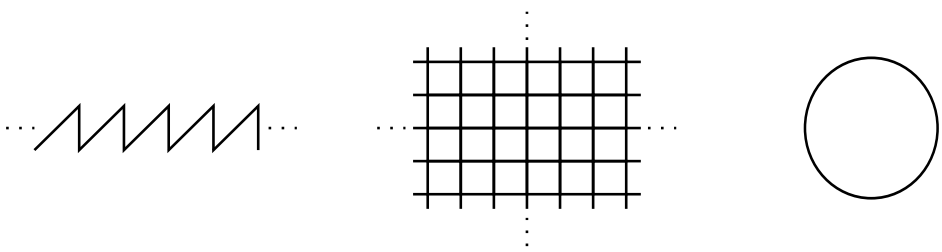
Neliö on rajoitettu tasokuvio, joten sillä voi olla symmetrioinaan ainoastaan kiertoja ja peilauksia. Sijoitetaan origo neliön keskipisteeseen, jolloin mahdolliset kiertosymmetriat ovat origokeskisiä ja peilaussymmetriat tapahtuvat origon kautta kulkevien suorien suhteen (ks. kuva 15). Nämä kuvaukset muodostavat tason *ortogonaalisen ryhmän* $\mathrm{O}_2(\mathbb{R})$, joten neliön symmetriaryhmää D_4 voidaan ajatella ortogonaalisen ryhmän aliryhmänä. Ortogonaalinen ryhmä on puolestaan aliryhmänä yleisessä lineaarisessa ryhmässä $\mathrm{GL}_2(\mathbb{R})$, johon kuuluvat kaikki tason kääntyvät lineaarikuvaukset. Esimerkiksi kiertomatriisi $\left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$ kuuluu ryhmään D_4.



Kuva 15. Neliö tasokuviona. Symmetriat ovat origokeskisiä kiertoja ja peilauksia.

Kun neliön symmetriat määritellään lineaarikuvauksina, saadaan ryhmän D_4 *matriisiesitys* eli *lineaarinen esitys*. Tällainen esitys mahdollistaa lineaarialgebran keinot ryhmän tutkimisessa. Ryhmien *esitysteoria* tutkii nimenomaan lineaarisia esityksiä.

Neliön symmetriaryhmä on äärellinen, mutta tasokuvioiden symmetriaryhmät voivat olla myös äärettömiä. Kuvan 16 kahdella ensimmäisellä kuviolla on symmetrioinaan siirtoja, jotka virittävät aina äärettömän ryhmän. Ensimmäisen kuvion symmetriaryhmä kuuluu niin kutsuttuihin *friisiryhmiin* ja toisen niin kutsuttuihin *tapettiryhmiin*. Kolmas kuvio, ympyrä, on rajoitettu, mutta sillä on silti ääretön symmetriaryhmä. Itse asiassa kyseessä on koko ortogonaalinen ryhmä $\mathrm{O}_2(\mathbb{R})$. Ympyrän symmetriaryhmä kuuluu niin kutsuttuihin *Lien ryhmiin*.



Kuva 16. Tasokuvioita, joiden symmetriaryhmät ovat äärettömiä.

Esimerkki 9.4. Myös ryhmillä on omat symmetriaryhmänsä. Koska symmetria on bijektiivinen kuvaus joukolta itselleen, joka säilyttää joukossa määritellyn rakenteen, ryhmän symmetriat ovat yksinkertaisesti isomorfismeja ryhmältä itselleen eli ryhmän *automorfismeja*. Ryhmän G automorfismiryhmää merkitään $\mathrm{Aut}(G)$.

Tarkastellaan esimerkiksi syklistä ryhmää $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$. Sen neutraalialkio on $\overline{0}$ ja virittäjiä alkiot $\overline{1}$ ja $\overline{2}$. Intuitiivisesti tuntuu siltä, että alkioilla $\overline{1}$ ja $\overline{2}$ ei pitäisi olla ryhmän rakenteen mielessä mitään eroa: jos ne vaihtaa toisin päin, mikään olennainen ei muutu. Voidaankin määritellä kuvaus

$$\sigma\colon \mathbb{Z}_3 \to \mathbb{Z}_3, \quad \sigma(x) = -x.$$

Suoraviivainen tarkistus osoittaa, että σ on ryhmän $\mathbb{Z}_3$ automorfismi.

Kuvauksen σ ja identtisen kuvauksen lisäksi muita automorfismeja ryhmällä $\mathbb{Z}_3$ ei voi olla. Automorfismin on nimittäin kuvattava virittäjäalkiot virittäjäalkioille, joten sen on joko vaihdettava $\overline{1}$ ja $\overline{2}$ keskenään tai kiinnitettävä ne. Toisaalta virittäjäalkioiden kuvat määrittävät homomorfismin täysin, jolloin tuloksena saadaan juuri edellä mainitut symmetriat. Automorfismiryhmäksi saadaan siis $\mathrm{Aut}(\mathbb{Z}_3) = \{\mathrm{id}, \sigma\}$.

9.2. Ryhmän toiminta. Joukon permutaatiot liikuttelevat joukon alkioita ympäriinsä. Permutaatiot muodostavat joukon symmetrisen ryhmän, jonka eri aliryhmät liikuttelevat alkioita hieman eri tavoin. Ryhmän toiminta yleistää tätä ilmiötä. Ideana on valita permutaatioryhmän sijaan mikä tahansa ryhmä ja määritellä, miten tuon ryhmän alkiot liikuttavat jonkin annetun joukon alkioita. Liikuttelun on jollain tapaa tapahduttava ryhmän ehdoilla: esimerkiksi neutraalialkio ei saa liikuttaa mitään alkiota.

Ryhmän toiminnan määritelmä ja merkintätapa muistuttavat skalaarikertolaskua.

Määritelmä 9.5. Olkoon G ryhmä ja X joukko. Kuvausta $\varphi\colon G \times X \to X$, $(g, x) \mapsto gx$, nimitetään ryhmän G *toiminnaksi joukossa* X, jos se toteuttaa seuraavat ehdot:

(T1) $ex = x$ kaikilla $x \in X$
(T2) $(gh)x = g(hx)$ kaikilla $x \in X$ ja $g, h \in G$.

Toiminnan määritelmä soveltuu sellaisenaan myös monoidin toiminnan määrittelyyn, koska määritelmässä ei oteta kantaa käänteisalkioihin. Toisinaan käytetään selvyyden vuoksi toiminnalle merkintää $g.x$ tai $g(x)$. Tarkalleen ottaen yllä on määritelty ryhmän *vasemmanpuoleinen* toiminta. Oikeanpuoleinen toiminta $(g, x) \mapsto xg$ määritellään vastaavasti ehdoin $xe = x$ ja $x(gh) = (xg)h$.

Esimerkki 9.6. Seuraavassa on esimerkkejä toiminnoista.

- Joukon X symmetrinen ryhmä $S(X)$ toimii joukossa X permutoimalla: $\sigma x = \sigma(x)$. Kyseessä on toiminta, sillä kaikilla $x \in X$ ja $\sigma, \tau \in S(X)$ pätee $ex = \mathrm{id}(x) = x$ ja $(\sigma\tau)x = (\sigma \circ \tau)(x) = \sigma(\tau(x)) = \sigma(\tau x)$.
- Olkoon V vektoriavaruus, jonka skalaarikunta on K. Kertolaskuryhmä K^* toimii joukossa V skalaarikertolaskulla. Kaikilla $\mathbf{v} \in V$ ja $a, b \in K^*$ nimittäin pätee $1\mathbf{v} = \mathbf{v}$ ja $(ab)\mathbf{v} = a(b\mathbf{v})$ vektoriavaruuden määritelmän mukaisesti.

- Olkoon K jokin kunta. Kääntyvät $n \times n$ -matriisit muodostavat yleisen lineaarisen ryhmän $\mathrm{GL}_n(K)$. Tämä ryhmä toimii vektoriavaruudessa K^n matriisikertolaskulla.
- Jos G on ryhmä, kaava $g.h = gh$ määrittelee ryhmän G vasemmanpuoleisen toiminnan itsessään. Tätä toimintaa kutsutaan (vasemmaksi) *siirtotoiminnaksi* eli *translaatioksi*.
- Myös kaava $g.h = ghg^{-1}$ määrittelee ryhmän G toiminnan itsessään. Tätä toimintaa kutsutaan *konjugoinniksi*. Konjugointitoimintaan palataan myöhemmin.
- Olkoon X jokin joukko, jossa on määritelty ryhmän G toiminta. Kaikkien kuvausten $X \to X$ joukossa $\mathcal{F}(X)$ voidaan nyt määritellä ryhmän G vasen toiminta kaavalla $(gf)(x) = f(g^{-1}x)$. Tämän tarkistaminen jätetään harjoitustehtäväksi.

Esimerkki 9.7. Sama ryhmä voi toimia samassa joukossa monella eri tavalla. Tarkastellaan kahta ryhmän $\mathbb{Z}$ toimintaa joukossa $\mathbb{R}$.

Ensimmäinen toiminta on siirtotoiminta: $n.x = n + x$ kaikilla $n \in \mathbb{Z}$ ja $x \in \mathbb{R}$. Jos $m, n \in \mathbb{Z}$ ja $x \in \mathbb{R}$, nähdään, että $0.x = 0 + x = x$ ja

$$(m + n).x = (m + n) + x = m + (n + x) = m.(n + x) = m.(n.x).$$

Täten kyseessä on ryhmän toiminta.

Toinen toiminta on eräänlainen peilaus. Määritellään $n.x = (-1)^n x$ kaikilla $n \in \mathbb{Z}$ ja $x \in \mathbb{R}$. Myös tämä on ryhmän toiminta, sillä $0.x = (-1)^0 x = 1 \cdot x = x$ ja

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

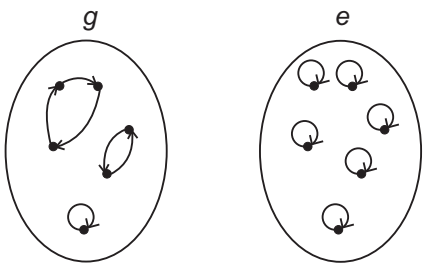
kaikilla $x \in \mathbb{R}$ ja $m, n \in \mathbb{Z}$.

Kun ryhmä toimii jossain joukossa, jokainen ryhmän alkio tuottaa joukon permutaation. Tällä tavoin toiminnat yleistävät permutaatioryhmiä.

Lause 9.8. *Olkoon G ryhmä, joka toimii joukossa X. Määritellään jokaisella $g \in G$ kuvaus $\sigma_g \colon X \to X$ kaavalla $\sigma_g(x) = gx$. Tällöin σ_g on joukon X permutaatio jokaisella $g \in G$, ja kuvaus $\Phi \colon G \to S(X)$, $\Phi(g) = \sigma_g$, on ryhmähomomorfismi.*

Todistus. Suoraviivainen todistus jätetään harjoitustehtäväksi. □

Koska ryhmän toiminnassa jokainen ryhmän alkio vastaa jotakin permutaatiota, toimintaa kutsutaan myös ryhmän *permutaatioesitykseksi* (vrt. esim. 9.1). Tämä ajatus on esitetty kuvassa 17. Permutaatioesitykseksi kutsutaan toisinaan myös kuvausta Φ tai kuvaryhmää $\Phi(G)$.



Kuva 17. Ryhmän alkiot vastaavat permutaatioita.

Lauseessa 9.8 määritelty ryhmän G permutaatioesitys $\Phi(G)$ ei ole välttämättä isomorfinen alkuperäisen ryhmän G kanssa. Mille tahansa ryhmälle voidaan esimerkiksi määritellä triviaali toiminta, jossa kaikki ryhmän alkiot kiinnittävät kaikki joukon alkiot, jolloin $\Phi(G) = \{\mathrm{id}\}$. Jos $\Phi(G) \cong G$, esitystä kutsutaan *uskolliseksi*. Seuraavan lauseen todistus perustuu siihen, että jokaisella ryhmällä on uskollinen permutaatioesitys.

LAUSE 9.9 (Cayleyn lause). *Jokainen ryhmä on isomorfinen jonkin permutaatioryhmän kanssa.*

TODISTUS. Olkoon G ryhmä. Ryhmän G vasen siirtotoiminta itsessään määritellään kaavalla $g.h = gh$. Tätä vastaava permutaatioesitys $\Phi\colon G \to S(G)$ on injektiivinen (todistus jätetään lukijalle). Ryhmien homomorfialauseesta seuraa, että G on isomorfinen kuvaryhmän $\Phi(G)$ kanssa. □

9.3. Radat ja vakauttajat. Oletetaan tässä alaluvussa, että G on ryhmä, joka toimii joukossa X. Joukon X alkion rata saadaan liikuttamalla sitä kaikilla ryhmän alkioilla.

MÄÄRITELMÄ 9.10. Alkion $x \in X$ *rata* on joukko

$$Gx = \{gx \mid g \in G\}.$$

Radat muodostavat joukon X osituksen. Vastaava ekvivalenssirelaatio on

$$x \sim y, \quad \text{jos } y = gx \text{ jollain } g \in G.$$

Kaikkien ratojen joukkoa merkitään X/G. Jos joukossa X on vain yksi rata, toimintaa kutsutaan *transitiiviseksi*.

Radat määrittävät, millä tavoin annettu alkio liikkuu ryhmän toiminnassa. Vastaavasti voidaan tutkia, mitkä ryhmän alkiot eivät liikuta annettua alkiota.

MÄÄRITELMÄ 9.11. Alkion $x \in X$ *kiinnittäjä* on joukko

$$G_x = \{g \in G \mid gx = x\}.$$

Kiinnittäjiä kutsutaan myös *pistevakauttajiksi*. Kiinnittäjät ovat ryhmän G aliryhmiä (todistus jätetään harjoitustehtäväksi). Yleisemmin osajoukon $Y \subset X$ *vakauttaja* voidaan määritellä joukkona

$$G_Y = \{g \in G \mid gy \in Y \text{ kaikilla } y \in Y\}.$$

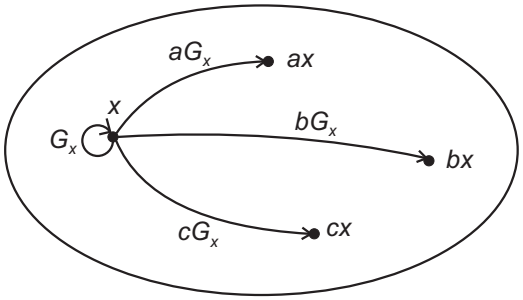
Tällöin $G_x = G_{\{x\}}$. Yleiset vakauttajat eivät välttämättä ole aliryhmiä.

ESIMERKKI 9.12. Tarkastellaan kertolaskuryhmän $\mathbb{R}^*$ toimintaa reaalikertoimisessa vektoriavaruudessa V. Olkoon $\mathbf{v} \in V$ mikä tahansa nollasta poikkeava vektori. Rata $\mathbb{R}^*\mathbf{v} = \{a\mathbf{v} \mid a \in \mathbb{R}^*\}$ on origon kautta kulkeva suora, jolta on poistettu origo itse. Nollavektorin rata puolestaan sisältää pelkästään nollavektorin.

Nollavektorista poikkeavien vektorien radat skalaaritoiminnassa muodostavat niin kutsutun *projektiivisen avaruuden* $\mathrm{P}(V) = (V \setminus \{\mathbf{0}\})/\mathbb{R}^*$.

ESIMERKKI 9.13. Tarkastellaan yleisen lineaarisen ryhmän $\mathrm{GL}_n(\mathbb{R})$ toimintaa vektoriavaruudessa $\mathbb{R}^n$. Olkoon $\mathbf{v} \in \mathbb{R}^n$ jokin nollasta poikkeava vektori. Yhtälö $A\mathbf{v} = \mathbf{v}$, missä $A \in \mathrm{GL}_n(\mathbb{R})$, voidaan tulkita niin, että vektori $\mathbf{v}$ on matriisin A ominaisvektori ominaisarvolla 1. Vektorin $\mathbf{v}$ kiinnittäjä $G_{\mathbf{v}}$ koostuu siis kaikista sellaisista matriiseista, joilla on ominaisvektorinaan $\mathbf{v}$ ominaisarvolla 1.

Radat ja kiinnittäjät eli pistevakauttajat liittyvät toisiinsa seuraavasti. Alkion x kiinnittäjä G_x koostuu niistä alkioista, jotka eivät liikuta alkiota x. Kiinnittäjä on aliryhmä, joten voidaan tarkastella jotain sivuluokkaa aG_x. Jos $b \in aG_x$, niin $b = ag$ jollain $g \in G_x$. Alkiot b ja a siis eroavat ainoastaan alkion g verran. Toisaalta alkio g kiinnittää alkion x, joten alkiot a ja b liikuttavat alkiota x täsmälleen samalla tavalla. Toisin sanoen alkion x radalla alkiot ax ja $bx = agx$ ovat sama alkio. Voidaan siis päätellä, että kaikki alkiot, jotka kuuluvat samaan kiinnittäjän sivuluokkaan, vastaavat samaa radan alkiota (ks. kuva 18).



KUVA 18. Kiinnittäjän sivuluokat vastaavat yksi yhteen radan alkioita.

LAUSE 9.14 (Rata–vakauttajalause). *Olkoon G ryhmä, joka toimii joukossa X. Oletetaan, että $x \in X$. Tällöin on olemassa bijektio $\varphi\colon G/G_x \to Gx$, jolle pätee $\varphi(aG_x) = ax$ kaikilla $a \in G$.*

TODISTUS. Koska kuvauksen φ arvot halutaan määritellä sivuluokan edustajien avulla, täytyy ensin tarkistaa, että edustajan valinta ei vaikuta kuvauksen arvoihin.

Oletetaan, että $aG_x = bG_x$ joillain $a, b \in G$. Tällöin pätee $a^{-1}b \in G_x$, joten $a^{-1}b = g$ jollain $g \in G_x$. Koska $gx = x$, tästä seuraa, että

$$bx = agx = ax.$$

Näin ollen alkiot ax ja bx ovat samat, joten kuvaus φ voidaan määritellä kaavalla $\varphi(aG_x) = ax$.

Koska maalijoukoksi on valittu alkion x rata, nähdään suoraan, että kuvaus φ on surjektio. Osoitetaan, että se on injektio. Oletetaan siis, että $\varphi(aG_x) = \varphi(bG_x)$ pätee joillain $a, b \in G$. Tällöin $ax = bx$, mistä seuraa, että $x = a^{-1}bx$. Siispä alkio $a^{-1}b$ kiinnittää alkion x, joten a ja b kuuluvat samaan kiinnittäjän sivuluokkaan. Tämä todistaa injektiivisyyden. □

Huomautus. Huomaa, ettei rata–vakauttajalauseen todistuksessa voitu käyttää luvun 1.4 tuloksia, sillä rata Gx ei ole samantyyppinen rakenne kuin ryhmä G eikä niiden välillä ole määritelty homomorfismia. Toisaalta voitaisiin kyllä määritellä ryhmän vasen siirtotoiminta joukossa G, jolloin sekä G että Gx olisivat niin kutsuttuja *G-joukkoja*. Tällaisten rakenteiden välille voitaisiin edelleen määritellä homomorfismit. Sen jälkeen voitaisiin tarkistaa, että samaan kiinnittäjän sivuluokkaan kuuluminen on G-toiminnan kanssa yhteensopiva ekvivalenssirelaatio. Tällä tavoin päästäisiin käyttämään hyväksi aiempia tuloksia, mutta tässä yhteydessä oli yksinkertaisempaa todistaa kuvauksen olemassaolo suoraan.

ESIMERKKI 9.15. Käytetään rata-vakauttajalausetta esimerkissä 9.1 määritellyn neliön diedriryhmän $G = D_4$ kertaluvun selvittämiseen. Esimerkin mukaan ryhmä $G \leq S_4$ toimii kuvan 14 verkossa permutoimalla sen solmuja.

Ensinnäkin nähdään helposti, että sykli (1234) kuuluu ryhmään G. Tämä sykli vie solmun 1 solmulle 2. Käyttämällä samaa sykliä uudestaan saadaan solmu 1 solmulle 3 ja lopulta solmulle 4. Täten jokainen verkon solmu kuuluu solmun 1 rataan eli ryhmän G toiminta joukossa $N = \{1, 2, 3, 4\}$ on transitiivista. Rata–vakauttajalauseesta seuraa nyt, että $[G : G_1] = |N| = 4$.

Tarkastellaan sitten solmun 1 kiinnittäjää G_1. Koska solmu 3 on ainoa, joka ei ole yhteydessä solmuun 1, jokainen joukon G alkio, joka kiinnittää solmun 1, kiinnittää myös solmun 3. Toisaalta solmut 2 ja 4 voidaan vaihtaa keskenään permutaatiolla (24) solmun 1 pysyessä paikallaan. Tästä seuraa, että kiinnittäjä on aliryhmä $G_1 = \{(1), (24)\}$. Lagrangen lauseen perusteella $[G : G_1] = |G|/|G_1|$. Yhdistämällä tämä tieto aiempiin voidaan päätellä, että $|G| = 8$.

Vastaavalla tavalla voidaan päätellä, että n-kulmion symmetriaryhmän D_n kertaluku on aina $2n$. Tämän vuoksi tällaiselle ryhmälle käytetäänkin toisinaan merkintää D_{2n}.

10. Ryhmien sisäisestä rakenteesta

Tähän lukuun on koottu eräitä keskeisiä ryhmäteorian käsitteitä ja työkaluja, jotka liittyvät ryhmän sisäisten rakenteen tutkimiseen. Ryhmät ovat erittäin monimuotoisia olioita, ja yksinkertaisetkin kysymykset niiden rakenteeseen liittyen voivat osoittautua erittäin vaikeiksi ratkaista. Luvussa esitettävät menetelmät auttavat hahmottamaan ryhmien rakennetta, mutta mikään niistä ei anna kaikenkattavaa kuvaa ryhmien olemuksesta.

10.1. Konjugointi. Konjugointi on eräs tapa, jolla ryhmä toimii itsessään. Konjugoinnin valttina on, että sen ominaisuudet liittyvät suoraan moniin ryhmän ominaisuuksiin. Esimerkiksi radat liittyvät normaaleihin aliryhmiin (lause 10.4) ja kiinnittäjät vaihdannaisuuteen (lause 10.5). Lisäksi konjugoinnin tuottamat permutaatioesitykset ovat ryhmän symmetrioita (lause 10.7). Oletetaan koko alaluvussa, että G on jokin ryhmä.

MÄÄRITELMÄ 10.1. Merkitään $gxg^{-1} = {}^g x$ kaikilla $g, x \in G$. Saatavaa kuvausta $G \times G \to G$, $(g, x) \mapsto {}^g x$ kutsutaan *konjugoinniksi*.

On suoraviivaista tarkistaa, että konjugointi on ryhmän toiminta. Alkiota ${}^g x$ kutsutaan alkion x *konjugaatiksi*. Konjugoinnissa radoilla ja kiinnittäjillä on omat nimityksensä.

MÄÄRITELMÄ 10.2. Olkoon $x \in G$.

- Alkion x rataa konjugoinnissa kutsutaan alkion x *konjugaattiluokaksi* ja merkitään ${}^G x$.
- Alkion x kiinnittäjää konjugoinnissa kutsutaan alkion x *keskittäjäksi* ja merkitään $C_G(x)$.

Neutraalialkion konjugaattiluokka on yksiö ja keskittäjä puolestaan koko ryhmä. Toisaalta neutraalialkio myös kuuluu kaikkien alkioiden keskittäjiin, sillä ne ovat aliryhmiä. Jokainen alkio g kuuluu myös itse omaan keskittäjäänsä $C_G(g)$, sillä $ggg^{-1} = g$. Myös käänteisalkio g^{-1} kuuluu keskittäjään $C_G(g)$, koska keskittäjä on aliryhmä.

ESIMERKKI 10.3. Etsitään ryhmän S_3 konjugaattiluokat. Neutraalialkio muodostaa oman luokkansa. Kokeilemalla selvää, että

$$\begin{aligned} {}^{(12)}(123) &= (12)(123)(12)^{-1} = (132), \\ {}^{(23)}(12) &= (23)(12)(23)^{-1} = (13) \quad \text{ja} \\ {}^{(12)}(13) &= (12)(13)(12)^{-1} = (23). \end{aligned}$$

Tämä osoittaa, että molemmat 3-syklit kuuluvat samaan konjugaattiluokkaan A, ja kaikki 2-syklit kuuluvat myös yhteen konjugaattiluokkaan B.

Tarkistetaan vielä, että konjugaattiluokat A ja B eivät ole sama luokka. Tätä varten on konjugoitava esimerkiksi 3-sykliä (123) kaikilla ryhmän alkioilla, jotta voidaan todeta, että se ei voi päätyä luokkaan B. Työ helpottuu, kun huomataan, että neutraalialkio keskittää minkä tahansa alkion ja että lisäksi alkion (123) keskittäjään kuuluvat ainakin alkio itse samoin kuin käänteisalkio (132). Tarkistetaan muut konjugoinnit käsin:

$$^{(12)}(123) = (12)(123)(12)^{-1} = (132),$$
$$^{(13)}(123) = (13)(123)(13)^{-1} = (132),$$
$$^{(23)}(123) = (23)(123)(23)^{-1} = (132).$$

Nähdään, että (123) ei konjugoidu joukkoon B. Koska konjugaattiluokat muodostavat osituksen, luokat A ja B ovat erillisiä. Ryhmällä S_3 on siis kolme konjugaattiluokkaa: $\{(1)\}$, $\{(123), (132)\}$ ja $\{(12), (13), (23)\}$.

Normaalisuuskriteerin nojalla ryhmän G aliryhmä H on normaali, jos ja vain jos $ghg^{-1} \in H$ kaikilla $g \in G$ ja $h \in H$. Konjugoinnin avulla muotoiltuna tämä tarkoittaa, että aliryhmä on normaali, jos ja vain jos aliryhmän alkioiden konjugaatit säilyvät aliryhmässä. Sanotaan, että aliryhmä on *vakaa* konjugoinnissa. Toinen tapa ilmaista sama asia on sanoa, että aliryhmän alkioiden radat sisältyvät aliryhmään. Tästä saadaan seuraava tulos.

LAUSE 10.4. *Olkoon H ryhmän G aliryhmä. Tällöin H on normaali, jos ja vain jos se on konjugaattiluokkien yhdiste.*

Keskittäjän alkiot voidaan karakterisoida seuraavasti.

LAUSE 10.5. *Olkoot $g, h \in G$. Tällöin $h \in C_G(g)$ pätee, jos ja vain jos alkiot g ja h kommutoivat eli $hg = gh$.*

TODISTUS. Harjoitustehtävä. □

Keskittäjien leikkaus on aliryhmien leikkauksena aliryhmä. Edellisen lauseen nojalla se sisältää sellaiset alkiot, jotka kommutoivat kaikkien ryhmän alkioiden kanssa. Tämä aliryhmä on ryhmäteoriassa keskeinen.

MÄÄRITELMÄ 10.6. Ryhmän G *keskus* on joukko
$$Z(G) = \{g \in G \mid gh = hg \text{ kaikilla } h \in G\}.$$

Ryhmän keskus on paitsi aliryhmä, myös normaali sellainen, mikä voidaan helposti todistaa suoraan normaalisuuskriteerillä. Se voidaan kuitenkin nähdä myös hyödyntämällä edellä esitettyjä lauseita seuraavasti. Jokaisen keskuksen alkion g keskittäjä on keskuksen määritelmän perusteella koko ryhmä. Tällöin rata–vakauttajalauseesta seuraa, että alkion g konjugaattiluokka on yksiö. Koska siis keskuksen alkioiden konjugaattiluokat ovat yksiöitä, ne sisältyvät kokonaan keskukseen. Täten keskus on normaali lauseen 10.4 nojalla.

Konjugoinnin tuottama permutaatioesitys on tärkeä, sillä se tuottaa ryhmän symmetrioita. Seuraavan lauseen suoraviivainen todistus on harjoitustehtävä.

LAUSE 10.7. *Jokaisella $g \in G$ kuvaus $f_g \colon G \to G$, $f_g(x) = {}^g x$, on ryhmäisomorfismi.*

Kuvauksia f_g nimitetään ryhmän *sisäisiksi* symmetrioiksi. Ne muodostavat ryhmän $\mathrm{Inn}(G)$, joka on automorfismiryhmän $\mathrm{Aut}(G)$ aliryhmä. Voidaan osoittaa, että kyseinen aliryhmä on vieläpä normaali, ja vastaavaa tekijäryhmää merkitään $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$. Tekijäryhmän alkioita nimitetään *ulkoisiksi* symmetrioiksi.

10.2. Konjugointi permutaatioryhmissä. Moni ryhmä esiintyy permutaatioryhmänä, joko sellaisenaan tai permutaatioesityksen välityksellä. Tällaisten ryhmien tutkimiseen on erityistyökaluja. Esimerkiksi permutaatioita konjugoitaessa ei tarvitse suorittaa työläitä kertolaskuja, vaan konjugoinnin tulos voidaan päätellä suoraan konjugoitavan alkion sykliesityksestä. Yksinkertaisesti sanottuna permutaatiota konjugoitaessa permutoidaan sykliesityksen alkioita.

LAUSE 10.8. *Olkoot $\sigma, \tau \in S_n$. Oletetaan, että permutaation τ esitys erillisten syklien tulona on*

$$\tau = (a_{1,1} \quad \dots \quad a_{1,k_1}) \cdots (a_{m,1} \quad \dots \quad a_{m,k_m}).$$

Merkitään $\sigma(a_{i,j}) = b_{i,j}$ kaikilla i ja j. Tällöin alkion τ konjugaatti on

$${}^{\sigma}\tau = (b_{1,1} \quad \dots \quad b_{1,k_1}) \cdots (b_{m,1} \quad \dots \quad b_{m,k_m}).$$

TODISTUS. Merkitään väitteessä esiintyvää jälkimmäistä tuloa kirjaimella τ'. On osoitettava, että $\sigma\tau\sigma^{-1}$ ja τ' ovat sama permutaatio. Olkoon sitä varten $y \in N_n$ mielivaltainen. Koska σ on bijektio, löydetään jokin $x \in N_n$, jolle $y = \sigma(x)$. Jos τ pitää alkion x paikallaan, alkio x muodostaa permutaation τ sykliesityksessä 1-syklin (joka voidaan jättää merkitsemättä). Tällöin y muodostaa 1-syklin permutaation τ' sykliesityksessä, joten τ' kiinnittää alkion y. Saadaan

$$\sigma\tau\sigma^{-1}(y) = \sigma\tau(x) = \sigma(x) = y = \tau'(y).$$

Oletetaan sitten, että x esiintyy permutaatiossa τ jossain syklissä, jonka pituus on suurempi kuin yksi. Järjestelemällä syklejä tarvittaessa uudestaan voidaan valita, että $x = a_{1,1}$. Tällöin pätee

$$\tau\sigma^{-1}(y) = \tau(x) = (a_{1,1} \quad a_{1,2} \quad \dots \quad a_{1,k_1})\,[a_{1,1}] = a_{1,2}. \tag{1}$$

(Funktion argumentti on kirjoitettu hakasulkeisiin, jotta se erottuisi syklimerkinnästä.) Permutaation τ' konstruktion perusteella pätee $y = \sigma(a_{1,1}) = b_{1,1}$, josta saadaan

$$\tau'(y) = (b_{1,1} \quad b_{1,2} \quad \dots \quad b_{1,k_1})\,[b_{1,1}] = b_{1,2} = \sigma(a_{1,2}). \tag{2}$$

Yhtälöistä (1) ja (2) seuraa, että $\tau'(y) = \sigma(a_{1,2}) = \sigma\tau\sigma^{-1}(y)$. Koska y oli mielivaltainen, nähdään, että $\tau' = \sigma\tau\sigma^{-1}$. Väite on todistettu. □

ESIMERKKI 10.9. Tarkastellaan ryhmän S_7 permutaatioita $\sigma = (1254)$ ja $\tau = (16)(247)$. Jos halutaan konjugoida alkiota τ alkiolla σ, riittää kuvata permutaation τ sykliesityksen alkiot permutaatiolla σ. Kuvat ovat

$$\sigma(1) = 2, \quad \sigma(6) = 6, \quad \sigma(2) = 5, \quad \sigma(4) = 1 \quad \text{ja} \quad \sigma(7) = 7,$$

joten konjugaatiksi saadaan ${}^{\sigma}\tau = {}^{\sigma}((16)(247)) = (26)(517)$.

Symmetrisen ryhmän konjugaattiluokat voidaan johtaa edellisestä lauseesta. Konjugointi ei nimittäin lauseen mukaan voi muuttaa permutaation *syklityyppiä*, eli sitä, kuinka monesta minkäkin pituisesta syklistä permutaatio koostuu. Toisaalta symmetrisessä ryhmässä mikä tahansa permutointi on mahdollinen, joten kaikki saman syklityypin permutaatiot saadaan konjugoimalla toisistaan. Konjugaattiluokat vastaavat siis yksi yhteen syklityyppejä.

KOROLLAARI 10.10. *Symmetrisessä ryhmässä kaksi permutaatiota kuuluvat samaan konjugaattiluokkaan, jos ja vain jos niillä on sama syklityyppi.*

Syklityyppiä voidaan merkitä syklien pituuksien jonona $(t_1, t_2, \ldots, t_m)$, joka on järjestetty pisimmästä lyhimpään, 1-syklit mukaan lukien. Esimerkiksi ryhmän S_8 permutaation $(12)(345)(67)$ syklityyppi on $(3, 2, 2, 1)$.

Esimerkki 10.11. Tarkastellaan ryhmää S_3. Ryhmän alkioiden mahdolliset syklityypit ovat $(1, 1, 1)$ (neutraalialkio) $(2, 1)$ (2-syklit) ja (3) (3-syklit). Edellisen korollaarin mukaan ryhmän konjugaattiluokat ovat

$$E = \{\mathrm{id}\}, \quad A = \{(123), (132)\} \quad \text{ja} \quad B = \{(12), (23), (13)\}.$$

Nämä löydettiin jo esimerkissä 10.3.

Lauseen 10.4 mukaan ainoastaan konjugaattiluokkien yhdiste voi olla normaali aliryhmä. Toisaalta aliryhmän täytyy aina sisältää neutraalialkio, joten aitoja epätriviaaleja normaaleja aliryhmiä voivat olla ainoastaan yhdisteet $E \cup A$ ja $E \cup B$. Jälkimmäisessä on 4 alkiota, joten se ei voi olla aliryhmä Lagrangen lauseen nojalla. Sen sijaan $E \cup A$ on tunnetusti normaali aliryhmä.

Esimerkki 10.12. Korollaaria 10.10 voi käyttää sellaisenaan vain koko symmetrisessä ryhmässä. Tarkastellaan esimerkiksi ryhmää $A_3 = \{(1), (123), (132)\}$, joka on ryhmän S_3 aliryhmä. Ryhmä A_3 on vaihdannainen, joten konjugointi on tämän ryhmän sisällä triviaali kuvaus. Jokainen alkio kuuluu siis omaan konjugaattiluokkaansa eivätkä nämä muotoudu syklityyppien mukaan. Ryhmän S_3 konjugaattiluokka $\{(123), (132)\}$ jakautuu ryhmässä A_3 kahdeksi luokaksi $\{(123)\}$ ja $\{(132)\}$. Tämä johtuu siitä, että alkiot, jotka voisivat konjugoida 3-syklit toisikseen, ovat itse 2-syklejä, eivätkä siksi mukana ryhmässä A_3.

Esimerkki 10.13. Tutkitaan vielä konjugointia neliön symmetriaryhmässä, tarkemmin sanoen sen permutaatioesityksessä, joka esiteltiin esimerkissä 9.1.

Etsitään neliön symmetriaryhmän D_4 alkiot aikaisemman esimerkin kuvaan 14 viitaten. Ryhmään D_4 kuuluvat ainakin neliön kierto $\rho = (1234)$ sekä peilaus pystyakselin suhteen $\sigma = (12)(34)$. Alkio ρ virittää aliryhmän $\langle\rho\rangle$, johon kuuluvat

$$(1), \quad \rho = (1234), \quad \rho^2 = (13)(24), \quad \rho^3 = (1432).$$

Koska σ ei kuulu tähän aliryhmään, sivuluokka $\sigma\langle\rho\rangle$ sisältää neljä alkiota lisää:

$$\sigma = (12)(34), \quad \sigma\rho = (24), \quad \sigma\rho^2 = (14)(23), \quad \sigma\rho^3 = (13).$$

Esimerkin 9.15 nojalla $|D_4| = 8$, joten enempää alkioita ryhmässä ei ole.

Lauseen 10.8 perusteella eri syklityypin alkiot eivät voi kuulua samaan konjugaattiluokkaan. Kun ryhmän D_4 alkiot jaetaan syklityypin mukaan, saadaan seuraava alustava osittelu:

- (1)
- $\rho = (1234)$, $\rho^3 = (1432)$
- $\rho^2 = (13)(24)$, $\sigma\rho = (14)(23)$, $\sigma\rho^3 = (12)(34)$
- $\sigma = (24)$, $\sigma\rho^2 = (13)$.

Kukin rivi sisältää siis permutaatiot, jotka saattavat kuulua samaan konjugaattiluokkaan syklityyppinsä perusteella. Toisaalta voidaan laskea

$${}^{\sigma}\rho = {}^{(12)(34)}(1234) = (2143) = \rho^3.$$

Molemmat 4-syklit ρ ja ρ^3 kuuluvat siis samaan konjugaattiluokkaan.

Edelleen koska $\sigma^{-1} = \sigma$, niin $\rho\sigma = \sigma \cdot {}^{\sigma}\rho = \sigma\rho^3$. Tämän avulla saadaan

$${}^{\rho}\sigma = \rho\sigma\rho^{-1} = \sigma\rho^3\rho^{-1} = \sigma\rho^2$$

ja

$$^{\rho}(\sigma\rho) = {}^{\rho}\sigma^{\rho}\rho = \sigma\rho^2 \cdot \rho = \sigma\rho^3.$$

Nähdään siis, että myös alkiot σ ja $\sigma\rho^2$ kuuluvat samaan luokkaan, samoin kuin alkiot $\sigma\rho$ ja $\sigma\rho^3$.

Entä alkio ρ^2? Huomataan, että aliryhmän $\langle\rho\rangle$ indeksi ryhmässä D_4 on 2, joten $\langle\rho\rangle$ on normaali aliryhmä. Lauseen 10.4 nojalla alkiota ρ^2 ei voi konjugoida ulos aliryhmästä $\langle\rho\rangle$. Toisaalta mikään muu saman aliryhmän alkio ei ole samaa syklityyppiä kuin ρ^2, joten kyseinen alkio on yksin omassa konjugaattiluokassaan. Ryhmän D_4 konjugaattiluokat ovat siis seuraavat:

$$\{1\}, \quad \{\rho, \rho^3\}, \quad \{\rho^2\}, \quad \{\sigma, \sigma\rho^2\} \quad \text{ja} \quad \{\sigma\rho, \sigma\rho^3\}.$$

10.3. Permutaation etumerkki. Tässä alaluvussa tarkastellaan, miten permutaatiot jaetaan kahteen joukkoon, parillisiin ja parittomiin permutaatioihin. Näiden joukkojen permutaatiot eroavat toisistaan etumerkiltään, joka on parillisilla 1 ja parittomilla -1.

Kahden alkion syklejä nimitetään *vaihdoiksi* tai *transpositioiksi*. Jokainen sykli voidaan kirjoittaa vaihtojen tulona:

$$(a_1 \quad a_2 \quad \cdots \quad a_m) = (a_1 \quad a_2)\,(a_2 \quad a_3) \cdots (a_{m-1} \quad a_m)\,.$$

Koska jokainen permutaatio voidaan puolestaan kirjoittaa syklien tulona, saadaan seuraava tulos.

LAUSE 10.14. *Ryhmässä S_n jokainen alkio voidaan kirjoittaa vaihtojen tulona.*

Huomautus. Jos $n = 1$, ryhmässä S_n ei ole lainkaan vaihtoja. Voidaan kuitenkin ajatella, että identtinen kuvaus, joka on ryhmän S_1 ainoa alkio, on vaihtojen tyhjä tulo.

Permutaation esitys vaihtojen tulona ei ole millään muotoa yksikäsitteinen, sillä esimerkiksi

$$(1234)(567) = (14)(12)(23)(56)(67),$$
$$(1234)(567) = (13)(34)(42)(14)(42)(57)(56),$$
$$\text{jne.}$$

Osoittautuu kuitenkin, että saman permutaation esityksissä vaihtojen lukumäärä on aina joko parillinen tai pariton. Tämän mukaan permutaatioita kutsutaan parillisiksi tai parittomiksi. Todistusta varten määritellään ensin permutaation etumerkki.

MÄÄRITELMÄ 10.15. Oletetaan, että permutaation $\sigma \in S_n$ esityksessä erillisten syklien tulona on t sykliä (1-syklit mukaan luettuina). Tällöin permutaation σ *etumerkki* on

$$\operatorname{sgn}(\sigma) = (-1)^{n-t}.$$

Permutaation etumerkki voidaan määritellä monella tavalla. Tähän valittu määritelmä on kätevä, koska sen esittämiseen ei tarvita ylimääräisiä käsitteitä eikä aputuloksia. Se ei kuitenkaan ole kovin intuitiivinen. Seuraavassa esitetään tuloksia, joiden avulla etumerkkiä on helpompi käsitellä ja hahmottaa.

Jos $\sigma \in S_n$ on m-sykli, sen esityksessä erillisten syklien tulona on yksi m-sykli ja $n - m$ kappaletta 1-syklejä. Määritelmän perusteella pätee täten

$$\operatorname{sgn}(\sigma) = (-1)^{n-(1+n-m)} = (-1)^{m-1}.$$

Syklin etumerkki on siis 1, jos ja vain jos sen pituus on pariton. Esimerkiksi jokaisen vaihdon etumerkki on -1. Identtistä kuvausta voidaan pitää 1-syklinä, ja sen etumerkki on 1.

Osoitetaan seuraavaksi, että etumerkkikuvaus on ryhmähomomorfismi ryhmälle $(\{1,-1\},\cdot)$. Tähän tarvitaan pieni aputulos.

LEMMA 10.16. *Jos $\beta \in S_n$ ja τ on jokin vaihto, niin* $\operatorname{sgn}(\tau\beta) = -\operatorname{sgn}(\beta)$.

TODISTUS. Merkitään $\tau = (a\ b)$. Olkoon $\rho_1 \cdots \rho_t$ permutaation β esitys erillisten syklien tulona (1-syklit mukana). Oletetaan ensin, että a ja b esiintyvät samassa syklissä. Järjestämällä syklejä tarvittaessa uudelleen voidaan olettaa, että

$$\rho_1 = \begin{pmatrix} a & c_1 & \dots & c_k & b & d_1 & \dots & d_l \end{pmatrix}.$$

On suoraviivaista tarkistaa, että

$$\tau\rho_1 = (a\ c_1\ \dots\ c_k)(b\ d_1\ \dots\ d_l).$$

Permutaation $\tau\beta$ sykliesityksessä on siis yhteensä $t+1$ sykliä, joten sen etumerkki on $\operatorname{sgn}(\tau\beta) = (-1)^{n-(t+1)} = -\operatorname{sgn}(\beta)$.

Oletetaan sitten, että a ja b esiintyvät eri sykleissä, esimerkiksi

$$\rho_1 = \begin{pmatrix} a & c_1 & \dots & c_k \end{pmatrix} \quad \text{ja} \quad \rho_2 = \begin{pmatrix} b & d_1 & \dots & d_l \end{pmatrix}.$$

Tällöin pätee

$$\tau\rho_1\rho_2 = \begin{pmatrix} a & c_1 & \dots & c_k & b & d_1 & \dots & d_l \end{pmatrix}.$$

Nyt permutaation $\tau\beta$ sykliesityksessä on yksi sykli vähemmän kuin permutaation β esityksessä, joten $\operatorname{sgn}(\tau\beta) = (-1)^{n-(t-1)} = -\operatorname{sgn}(\beta)$. □

LAUSE 10.17. *Kaikilla $\alpha, \beta \in S_n$ pätee*

$$\operatorname{sgn}(\alpha\beta) = \operatorname{sgn}(\alpha)\operatorname{sgn}(\beta),$$

eli kuvaus $\operatorname{sgn}\colon S_n \to (\{1,-1\},\cdot)$ *on ryhmähomomorfismi.*

TODISTUS. Olkoot $\alpha, \beta \in S_n$. Jokainen permutaatio voidaan kirjoittaa vaihtojen tulona, joten voidaan kirjoittaa $\alpha = \tau_1 \cdots \tau_m$, missä jokainen τ_i on vaihto. Valitaan vaihdot siten, että niiden lukumäärä m on pienin mahdollinen. Käytetään induktiota tulon pituuden m suhteen.

Jos $m = 0$, permutaatio α on identtinen kuvaus. Tämän permutaation etumerkki on 1, ja toisaalta

$$\operatorname{sgn}(\alpha\beta) = \operatorname{sgn}(\beta) = \operatorname{sgn}(\alpha)(\beta).$$

Tulos siis pätee tapauksessa $m = 0$.

Oletetaan sitten, että $m > 0$ ja että väite pätee kaikilla α' ja β, missä α' voidaan kirjoittaa vähemmän kuin m vaihdon tulona. Tällöin edellisestä lemmasta ja induktio-oletuksesta seuraa

$$\begin{aligned} \operatorname{sgn}(\tau_1 \cdots \tau_m\beta) &= -\operatorname{sgn}(\tau_2 \cdots \tau_m\beta) \\ &\overset{\text{i.o.}}{=} -\operatorname{sgn}(\tau_2 \cdots \tau_m)\operatorname{sgn}(\beta) \\ &= \operatorname{sgn}(\tau_1 \cdots \tau_m)\operatorname{sgn}(\beta). \end{aligned}$$

Näin ollen väite pätee myös luvulla m. Induktioperiaatteen nojalla väite pätee kaikilla luonnollisilla luvuilla. □

Yllä olevan lauseen nojalla permutaation etumerkki voidaan selvittää kirjoittamalla permutaatio vaihtojen tulona: etumerkki on 1, jos ja vain jos vaihtojen lukumäärä on parillinen, sillä $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\tau_1)\cdots\operatorname{sgn}(\tau_m) = (-1)^m$. Tästä seuraa myös, että vaihtojen lukumäärä on saman permutaation kaikissa esityksissä aina joko parillinen tai pariton. Permutaatioita, jotka koostuu parillisesta määrästä vaihtoja, kutsutaan *parillisiksi* permutaatioiksi ja muita *parittomiksi*. Parilliset permutaatiot muodostavat tärkeän normaalin aliryhmän.

MÄÄRITELMÄ 10.18. Etumerkkihomomorfismin ydintä

$$\operatorname{Ker}(\operatorname{sgn}) = \{\sigma \in S_n \mid \sigma \text{ on parillinen}\}$$

kutsutaan *alternoivaksi ryhmäksi* ja merkitään symbolilla A_n.

LAUSE 10.19. *Jos $n \geq 2$, niin $[S_n : A_n] = 2$.*

TODISTUS. Koska $n \geq 2$, vaihto (12) kuuluu ryhmään S_n. Tällöin kuvaus sgn on surjektio kahden alkion ryhmälle $\{1, -1\}$. Homomorfialauseen nojalla löytyy bijektio $S_n/A_n \to \{1, -1\}$. □

10.4. Cauchyn lause. Lagrangen lauseen mukaan äärellisen ryhmän aliryhmän kertaluku jakaa ympäröivän ryhmän kertaluvun. Käänteisesti voidaan esittää kysymys, vastaako jokaista ryhmän kertaluvun tekijää jokin aliryhmä, jonka kertaluku kyseinen tekijä on. Tiedetään, että äärellisellä syklisellä ryhmällä on täsmälleen yksi aliryhmä kutakin ryhmän kertaluvun tekijää kohti. Itse asiassa kaikilla äärellisillä vaihdannaisilla ryhmillä on aliryhmiä kutakin kertalukua kohden, joskin niitä voi olla useita. Tämän väitteen todistamiseen voidaan käyttää esimerkiksi jäljempänä esitettävää äärellisviritteisten vaihdannaisten ryhmien peruslausetta (lause 11.11).

Epävaihdannaisilla ryhmillä Lagrangen lauseen käänteistulos pätee vain ryhmän kertaluvun alkutekijöillä. Seuraava todistus käyttää hyväksi erästä ryhmän toimintaa varsin elegantilla tavalla.

LAUSE 10.20 (Cauchyn lause). *Olkoon G äärellinen ryhmä, jonka kertaluku on n. Jos p on luvun n alkutekijä, ryhmällä G on aliryhmä, jonka kertaluku on p.*

TODISTUS. Olkoon p jokin alkuluku, joka jakaa kertaluvun n. Tarkastellaan seuraavaa joukkoa:

$$X = \{(x_1, \ldots, x_p) \mid x_i \in G \text{ kaikilla } i \text{ ja } x_1 x_2 \cdots x_p = e\}.$$

Toisin sanoen joukko X koostuu kaikista ryhmän G alkioiden p-jonoista, joiden tulo on neutraalialkio. Jos on annettu $p-1$ alkiota $x_1, \ldots, x_{p-1} \in G$ ja asetetaan $x_p = x_{p-1}^{-1} \cdots x_1^{-1}$, nähdään, että $(x_1, \ldots, x_p) \in X$. Toisaalta jos $(x_1, \ldots, x_p) \in X$, täytyy päteä $x_p = x_{p-1}^{-1} \cdots x_1^{-1}$. Tämä osoittaa, että p-jonojen lukumäärä joukossa X saadaan laskemalla eri tavat, joilla alkiot $x_1, \ldots, x_{p-1}$ voidaan valita ryhmästä G. Näin ollen $|X| = n^{p-1}$.

Jos $x_1 x_2 \cdots x_p = e$ pätee joillain $x_1, \ldots, x_p \in G$, myös $x_2 \cdots x_p x_1 = e$ pätee. Siten mikä tahansa joukon X jonon syklinen permutaatio kuuluu myös joukkoon X. Voidaan siis määritellä ryhmän $\mathbb{Z}_p$ toiminta joukossa X asettamalla

$$[k]_p(x_1, x_2, \ldots, x_p) = (x_{k+1}, x_{k+2}, \ldots, x_p, x_1, \ldots, x_k)$$

kaikilla $k \in \{0, \ldots, p-1\}$. On suoraviivaista tarkistaa, että kyseessä todella on ryhmän toiminta.

Rata–vakauttajalauseen nojalla yllä määritellyn toiminnan ratojen koot jakavat ryhmän $\mathbb{Z}_p$ kertaluvun. Koska p on alkuluku, kunkin radan koko on joko 1 tai p. Olkoon a niiden ratojen lukumäärä, joiden koko on 1, ja b niiden ratojen lukumäärä, joiden koko on p. Alkion rata on yksiö täsmälleen silloin, kun alkio on muotoa $(x, \ldots, x)$. Tiedetään, että $(e, \ldots, e) \in X$, joten $a \geq 1$.

Radat muodostavat joukon X osituksen, ja joukon X koko on n^{p-1}, joten voidaan kirjoittaa

$$n^{p-1} = a \cdot 1 + b \cdot p.$$

Koska p jakaa luvun n, yhtälöstä nähdään, että p jakaa myös luvun a. Koska $a \geq 1$ ja 1 ei ole jaollinen luvulla p, täytyy päteä $a > 1$. Siispä on olemassa jokin $x \neq e$, jolle pätee $(x, \ldots, x) \in X$. Tällöin $x^p = 1$, mistä seuraa, että alkion x kertaluku on p. □

10.5. Isomorfialauseet. Seuraavassa esiteltävät tulokset helpottavat tekijäryhmien käsittelyä. Ne ovat peräisin Emmy Noetheriltä. Samoin kuin homomorfialause, vastaavat tulokset pätevät myös renkaille ja moduleille. Ennen tulosten esittelyä tarkastellaan hieman aliryhmien tuloja.

Olkoot A ja B ryhmän G aliryhmiä. Tulojoukko

$$AB = \{ab \mid a \in A, b \in B\}$$

ei ole välttämättä aliryhmä. Esimerkiksi tulojoukon alkioiden $b = e \cdot b$ ja $a = a \cdot e$ tulo on ba. Jotta AB olisi aliryhmä, tämän tulon on oltava joukossa AB. Tämä tarkoittaa, että ba on muotoa $a'b'$ joillain $a' \in A$ ja $b' \in B$. Siispä vähimmäisehto sille, että AB on aliryhmä, on että tulojoukot BA ja AB ovat sama joukko. Tämä toteutuu esimerkiksi silloin, kun jokainen aliryhmän A alkio kommutoi jokaisen aliryhmän B alkion kanssa. Vähempikin kuitenkin riittää, kuten nähdään seuraavasta lemmasta.

LEMMA 10.21. *Olkoot H ja N ryhmän G aliryhmiä, ja olkoon N lisäksi normaali. Tällöin tulo HN on ryhmän G aliryhmä.*

TODISTUS. Joukko HN sisältää neutraalialkion. Oletetaan, että $a_1, a_2 \in H$ ja $b_1, b_2 \in N$. Koska N on normaali, konjugointi ei kuvaa alkioita pois joukosta N. Täten $a_2^{-1} b_1 a_2 = b'$ jollain $b' \in N$. Nyt $b_1 a_2 = a_2 b'$, joten

$$a_1 b_1 \cdot a_2 b_2 = a_1 a_2 b' b_2 \in HN.$$

Joukko HN on siis suljettu kertolaskun suhteen. Samalla tavoin $a_1 b_1^{-1} a_1^{-1} = b''$ jollain $b'' \in N$, mistä seuraa

$$(a_1 b_1)^{-1} = b_1^{-1} a_1^{-1} = a_1^{-1} b'' \in HN.$$

Siispä HN on aliryhmä. □

Toisen aliryhmän normaalius on riittävä ehto siihen, että tulojoukko HN on aliryhmä, mutta ei välttämätön. Jos tulojoukko HN on koko ryhmä G, aliryhmä N on normaali ja $H \cap N = \{e\}$, ryhmää G kutsutaan aliryhmien H ja N *puolisuoraksi tuloksi*. Jos molemmat aliryhmät ovat normaaleja, G on aliryhmiensä suora tulo. Kirjataan tämä tulos ylös seuraavassa lauseessa.

LAUSE 10.22. *Oletetaan, että H ja K ovat ryhmän G normaaleja aliryhmiä. Jos $HK = G$ ja $H \cap K = \{e\}$, niin $G \cong H \times K$.*

TODISTUS. Harjoitustehtävä. □

Ensimmäinen isomorfialause koskee aliryhmien H ja N tuloa. Jos N on normaali aliryhmä, tulojoukko HN on lemman 10.21 nojalla aliryhmä. Se koostuu tuloista hn. Tekijäryhmässä HN/N aliryhmän N alkiot samastetaan. Tällöin siis $[hn] = [he] = [h]$, joten voisi ajatella, että tekijäryhmä olisi isomorfinen aliryhmän H kanssa. Tämä ei kuitenkaan ole aivan totta, sillä aliryhmässä H saattaa olla samoja alkioita kuin aliryhmässä N, jolloin nämäkin samastetaan. Kun tämä otetaan huomioon, lauseesta tulee seuraavanlainen.

LAUSE 10.23 (1. isomorfialause[1]). *Olkoot H ja N ryhmän G aliryhmiä, ja olkoon N normaali. Tällöin $N \trianglelefteq HN$, $H \cap N \trianglelefteq H$, ja*

$$HN/N \cong H/(H \cap N).$$

TODISTUS. Aliryhmä N on normaali ryhmässä HN, koska kaikki ryhmän HN konjugoivat alkiot sisältyvät ryhmään G ja N on normaali ryhmässä G. Olkoon $\pi\colon G \to G/N$ kanoninen surjektio, ja olkoon π' sen rajoittuma ryhmään H.

Selvitetään kuvauksen π' kuva ja ydin. Ensinnäkin kuvauksen arvot ovat sivuluokkia hN, missä $h \in H$. Tällaisen sivuluokan alkiot ovat aliryhmässä HN, joten sivuluokat kuuluvat tekijäryhmään HN/N. Toisaalta jos $gN \in HN/N$, niin $g = hn$ joillain $h \in H$ ja $n \in N$. Nyt saadaan $\pi'(h) = hN = (gn^{-1})N = gN$, joten $\operatorname{Im}\pi' = HN/N$.

Kuvauksen $\pi'\colon H \to G/N$ määritelmän perusteella nähdään, että

$$\operatorname{Ker}\pi' = \{h \in H \mid h \in N\} = H \cap N.$$

Ydin on normaali aliryhmä, joten $H \cap N$ on normaali ryhmässä H. Lopulta homomorfialauseen perusteella $H/(H \cap N) \cong \operatorname{Im}\pi'$. Tämä todistaa viimeisen väitteen. □

Toinen isomorfialause koskee tekijäryhmiä saman aliryhmän suhteen. Jos H ja K ovat ryhmän G normaaleja aliryhmiä, ja $K \subset H$, voidaan muodostaa tekijäryhmät G/K ja H/K. Molemmat koostuvat aliryhmän K sivuluokista. Tekijäryhmässä $(G/K)/(H/K)$ samastetaan ne aliryhmän K sivuluokat, jotka kuuluvat aliryhmään H. Osoittautuu, että saman tuloksen saa yksinkertaisesti samastamalla suoraan ryhmässä G aliryhmän H alkiot.

LAUSE 10.24 (2. isomorfialause). *Olkoot H ja K ryhmän G normaaleja aliryhmiä, joille pätee $K \leq H$. Tällöin tekijäryhmä H/K on normaali ryhmässä G/K, ja*

$$(G/K)/(H/K) \cong G/H.$$

TODISTUS. Olkoon $\pi\colon G \to G/H$ kanoninen surjektio. Koska $K \subset H$, kaikilla $k \in K$ pätee $\pi(k) = H$. Aliryhmä K siis sisältyy kuvauksen π ytimeen, joten lauseen 1.15 perusteella on olemassa homomorfismi $f\colon G/K \to G/H$, jolle pätee $f(gK) = \pi(g) = gH$. Tämä kuvaus laajentaa sivuluokkia ja on surjektiivinen, koska myös π on. Lisäksi $f(gK) = gH = H$, jos ja vain jos $g \in H$, ja tämä on yhtäpitävää sen kanssa, että $gK \in H/K$. Täten $\operatorname{Ker} f = H/K$, joten H/K on ryhmän G/K normaali aliryhmä. Viimeinen väite seuraa homomorfialauseesta. □

[1]Monissa lähteissä homomorfialausetta nimitetään ensimmäiseksi isomorfialauseeksi. Tällöin ensimmäisestä isomorfialauseesta tuleekin toinen isomorfialause ja toisesta kolmas.

10.6. Kompositiojonot. Jos ryhmästä löydetään normaali aliryhmä, sen suhteen voidaan muodostaa tekijäryhmä, jolla saattaa olla yksinkertaisempi rakenne kuin alkuperäisellä ryhmällä. Ryhmä voidaan ikään kuin pilkkoa kahteen "tekijään", joiden ominaisuuksia voi tutkia erikseen. Pilkkomista voidaan myös jatkaa edelleen niin kauan kuin uusia normaaleja aliryhmiä löytyy.

MÄÄRITELMÄ 10.25. Ryhmän G *normaali jono* on jono aliryhmiä G_i, joille pätee
$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_n = 1.$$
Tekijäryhmiä G_i/G_{i+1} kutsutaan jonon *tekijöiksi*.

Huomautus. Tässä merkitään triviaalia ryhmää symbolilla 1, sillä se on yleinen tapa ryhmäteoriassa. Samaten normaalin jonon tekijöitä merkitään yleensä vain isomorfiatyypin mukaan; esimerkiksi ryhmät A_3 ja $\mathbb{Z}_3$ ovat molemmat syklisiä kolmen alkion ryhmiä, joten niitä voidaan merkitä yksinkertaisesti C_3.

ESIMERKKI 10.26. Symmetrisellä ryhmällä S_4 on normaali jono
$$S_4 \rhd A_4 \rhd 1,$$
jonka tekijät ovat C_2 ja A_4. Samalla ryhmällä on muitakin normaaleja jonoja.

Neliön symmetriaryhmällä on muun muassa seuraava normaali jono:
$$D_4 \rhd \langle \rho^2, \sigma \rangle \rhd \langle \sigma \rangle \rhd 1.$$
Tässä on käytetty esimerkin 10.13 merkintöjä, joissa ρ on neliön kierto ja σ peilaus. Jonon kaikkien tekijöiden kertaluku on 2. Huomaa, että normaalius ei ole transitiivinen ominaisuus: yllä aliryhmä $\langle \sigma \rangle$ ei ole normaali koko ryhmässä D_4.

ESIMERKKI 10.27. Normaalin jonon tekijän käsite on tietyssä mielessä tulon tekijän yleistys. Jos nimittäin G on aliryhmiensä H ja K suora tulo eli $G \cong H \times K$, ryhmällä G on normaali jono $G \rhd H \rhd 1$. Lisäksi $G/H \cong K$, joten normaalin jonon tekijät ovat samat kuin tulon tekijät H ja K. Sama pätee yleisemminkin: jos $G = HN$, missä $H \cap N = 1$ ja $N \trianglelefteq G$, niin jonon $G \rhd N \rhd 1$ tekijät ovat H ja N (vrt. lemmaan 10.21).

Jonon tekijät eivät kuitenkaan aina vastaa mitään tuloa. Esimerkiksi neljän alkion syklisellä ryhmällä $C_4 = \langle g \rangle$ on normaali jono $C_4 \rhd \langle g^2 \rangle \rhd 1$, jonka molemmat tekijät ovat isomorfisia ryhmän C_2 kanssa. Ryhmä C_4 kuitenkin sisältää vain yhden tyyppiä C_2 olevan aliryhmän, joten se ei voi olla kahden tällaisen aliryhmän tulo.

Évariste Galois osoitti vuonna 1830, että polynomin juurille voidaan esittää juurenottoihin perustuva kaava, jos ja vain jos polynomin Galois'n ryhmällä (ks. esim. 9.2) on normaali jono, jonka kaikki tekijät ovat vaihdannaisia. Tämän tuloksen vuoksi tällaista ryhmää kutsutaan ratkeavaksi. Vaihdannaiset ryhmät ovat ratkeavia, ja jo Abel huomasi, että Galois'n ryhmän vaihdannaisuudesta seuraa polynomin ratkeavuus. Tämän vuoksi Camille Jordan alkoi nimittää vaihdannaisia ryhmiä Abelin ryhmiksi.

MÄÄRITELMÄ 10.28. Ryhmää sanotaan *ratkeavaksi*, jos sillä on normaali jono, jonka kaikki tekijät ovat vaihdannaisia ryhmiä.

Normaalin jonon (G_i) *hienonnus* on sellainen normaali jono (G_i'), joka sisältää osajononaan alkuperäisen jonon. Hienonnus on *aito*, mikäli se poikkeaa alkuperäisestä. Annettua normaalia jonoa voidaan hienontaa, mikäli sen tekijöiltä löydetään normaaleja aliryhmiä. Tutustutaan hienontamiseen seuraavan esimerkin avulla.

Esimerkki 10.29. Tarkastellaan normaalia jonoa

$$G \rhd H \rhd \{0\},$$

missä $G = \mathbb{Z}_{30}$ ja $H = \langle\overline{6}\rangle$. Jonon ensimmäinen tekijä on $G/H = \{[\overline{0}], [\overline{1}], \ldots, [\overline{5}]\}$. Sivuluokkia merkitään tässä hakasulkeilla: $[a] = a + \langle\overline{6}\rangle$.

Tekijäryhmä G/H on kuuden alkion syklinen ryhmä, joten sillä on kolmen alkion normaali aliryhmä $N = \{[\overline{0}], [\overline{2}], [\overline{4}]\}$. Tästä saadaan ryhmälle G uusi aliryhmä ottamalla alkukuva kanonisessa surjektiossa $\pi\colon G \to G/H$. Prosessia kutsutaan *nostamiseksi*. Esimerkiksi sivuluokan $[\overline{2}]$ alkukuva on $\{\overline{2}, \overline{8}, \overline{14}, \overline{20}, \overline{26}\}$, sillä kaikki nämä kuvautuvat kuvauksessa π sivuluokalle $[\overline{2}]$. Näin saadaan lopulta aliryhmä

$$\begin{aligned}\hat{N} = \pi^{-1}N = \{\ & \overline{0},\ \overline{6},\ \overline{12},\ \overline{18},\ \overline{24},\\ & \overline{2},\ \overline{8},\ \overline{14},\ \overline{20},\ \overline{26},\\ & \overline{4},\ \overline{10},\ \overline{16},\ \overline{22},\ \overline{28}\ \} = \langle\overline{2}\rangle.\end{aligned}$$

Tämän esimerkin ryhmät ovat vaihdannaisia, joten kaikki aliryhmät ovat normaaleja. Nostamalla saadut aliryhmät ovat kuitenkin aina normaaleja, sillä normaalin aliryhmän alkukuva homomorfismissa on normaali. Saatu normaali aliryhmä $\hat{N}$ sijoittuu normaalissa jonossa termien G ja H väliin. Alkuperäistä jonoa voidaan siis hienontaa jonoksi

$$G \rhd \hat{N} \rhd H \rhd \{0\}.$$

Uuden jonon kaksi ensimmäistä tekijää ovat C_2 ja C_3. Nämä saatiin pilkkomalla alkuperäinen tekijä $G/H = C_6$ osiin $N = C_3$ ja $(G/H)/N = C_2$ ja nostamalla sen jälkeen alkuperäiseen jonoon.

Jos ryhmä on äärellinen, hienontamista ei voida jatkaa loputtomiin. Maksimaalista normaalia jonoa nimitetään kompositiojonoksi.

Määritelmä 10.30. Jos ryhmän normaalilla jonolla

$$G = G_1 \rhd G_2 \rhd \cdots \rhd 1$$

ei ole aitoja hienonnuksia (lukuun ottamatta sellaisia, jotka saadaan toistamalla jotakin jonon jäsentä peräkkäin), jonoa kutsutaan ryhmän G *kompositiojonoksi*.

Jos tekijöiltä löydetään normaaleja aliryhmiä, aito hienonnus löytyy esimerkin 10.29 nostamistekniikalla. Tämä antaa aiheen määritellä sellaiset ryhmät, joilla ei ole aitoja normaaleja aliryhmiä.

Määritelmä 10.31. Epätriviaali ryhmä G on *yksinkertainen*, jos sillä ei ole aitoa epätriviaalia normaalia aliryhmää.

Esimerkkiä 10.29 imitoimalla voidaan todistaa seuraava tulos. Tarkka todistus jätetään lukijalle.

LAUSE 10.32. *Ryhmän normaali jono on kompositiojono, jos ja vain jos sen tekijät ovat yksinkertaisia.*

Kompositiojonoihin liittyy tärkeä ominaisuus, jota voidaan pitää ryhmien "alkutekijähajotelmana". Jos ryhmällä on kompositiojono, niitä on tyypillisesti useita. Esimerkiksi ryhmällä $\mathbb{Z}_6$ on kompositiojonot

$$\mathbb{Z}_6 \rhd \langle\overline{2}\rangle \rhd \{\overline{0}\} \qquad \text{(tekijät } C_2 \text{ ja } C_3\text{)}$$

ja

$$\mathbb{Z}_6 \rhd \langle\overline{3}\rangle \rhd \{\overline{0}\} \qquad \text{(tekijät } C_3 \text{ ja } C_2\text{)}.$$

Ranskalainen matemaatikko Camille Jordan todisti vuonna 1868, että äärellisen ryhmän kompositiotekijöiden kertaluvut ovat järjestystä vaille yksikäsitteiset, ja saksalainen Otto Hölder täydensi tulosta vuonna 1889 näyttämällä, että itse tekijät ovat isomorfiaa vaille samat. Todistus sivuutetaan, mutta se löytyy monista ryhmäteorian oppikirjoista.

LAUSE 10.33 (Jordanin–Hölderin lause). *Jos ryhmällä on kompositiojono, sen tekijät ovat järjestystä ja isomorfiaa vaille yksikäsitteiset.*

Mainitaan lopuksi vielä muutama sana kompositiojonoista ja yksinkertaisista ryhmistä. Kuten aiemmin on jo todettu, äärellisellä ryhmällä on aina kompositiojono, sillä jonon hienontamista ei voida jatkaa mielivaltaisen pitkälle. Äärettömällä ryhmällä voi olla tai olla olematta kompositiojono. Ryhmällä $\mathbb{Z}$ ei ole kompositiojonoa, mutta esimerkiksi erityisellä lineaarisella ryhmällä $\mathrm{SL}_2(\mathbb{R})$ on (todistus sivuutetaan).

Ratkeavien ryhmien normaaleissa jonoissa tekijät ovat määritelmän mukaan vaihdannaisia. Ei ole vaikea näyttää, että vaihdannainen ryhmä on yksinkertainen, jos ja vain jos se on syklinen ryhmä C_p, missä p on alkuluku. Tästä nähdään, että äärettömällä ratkeavalla ryhmällä ei voi olla kompositiojonoa, koska sen kompositiotekijät olisivat äärellisiä. Toisaalta äärelliselle ratkeavalle ryhmälle voidaan aina löytää kompositiojono pilkkomalla sen vaihdannaisia tekijöitä. Lisäksi äärellisille ratkeaville ryhmille saadaan seuraava karakterisointi.

LAUSE 10.34. *Äärellinen ryhmä on ratkeava, jos ja vain jos sillä on kompositiojono, jonka tekijät ovat syklisiä ryhmiä, joiden kertaluku on alkuluku.*

TODISTUS. Todistus jätetään harjoitustehtäväksi. □

Kompositiotekijöiden olemassaolo ja yksikäsitteisyys antavat mahdollisuuden lähestyä äärellisten ryhmien teoriaa kompositiojonojen kautta. Tällainen lähestymistapa vaatii, että ensinnäkin tunnetaan kaikki äärelliset yksinkertaiset ryhmät, jotka siis voivat olla kompositiojonon tekijöinä, ja toisaalta niistä osataan koota takaisin alkuperäinen ryhmä. Eri ryhmillä voi nimittäin olla samat kompositiotekijät. Jälkimmäinen kysymys on hyvin monimutkainen ja siihen on vain osittaisia ratkaisuja, jotka hyödyntävät muun muassa ryhmien kohomologiateoriaa. Ensimmäinen kysymys on sen sijaan ratkaistu viime vuosisadan lopulla.

Jo Galois aloitti äärellisten yksinkertaisten ryhmien tutkimuksen todistamalla, että alternoiva ryhmä A_n on yksinkertainen, kun $n \geq 5$. Tämä liittyy polynomien ratkaisukaavojen olemassaoloon sillä tavoin, että mikään ryhmä, joka sisältää normaalissa jonossaan tekijän A_n jollain $n \geq 5$, ei voi olla ratkeava. Polynomeilla, joiden aste on vähintään 5, esiintyy tällaisia Galois'n ryhmiä, mistä seuraa, että niillä ei ole yleistä ratkaisukaavaa.

Galois'n jälkeen yksinkertaisia ryhmiä löydettiin lisää, ja erinäisten vaiheiden jälkeen 1980-luvulla alettiin uskoa, että kaikki äärelliset yksinkertaiset ryhmät olisi löydetty. Tuloksen todistamiseksi koottiin yhteen satoja artikkeleja, joita jouduttiin korjailemaan ja paikkailemaan, mutta nykyisin näyttää siltä, että todistuksessa ei pitäisi olla aukkoja. Kukaan yksittäinen ihminen ei ole sitä kuitenkaan pystynyt tarkistamaan. Daniel Gorenstein, Richard Lyons ja Ronald Solomon ovat aloittaneet projektin, jossa he kokoavat todistusta yksiin kansiin, ja kyseisestä projektista on muodostumassa yksitoistaosainen kirjasarja.

LAUSE 10.35 (Äärellisten yksinkertaisten ryhmien luokittelulause). *Jokainen äärellinen yksinkertainen ryhmä kuuluu johonkin seuraavista luokista.*

1. *sykliset ryhmät C_p, missä p on alkuluku (ainoat vaihdannaiset ryhmät)*
2. *alternoivat ryhmät A_n, missä $n \geq 5$*

3.a. *klassiset Lie-tyypin ryhmät*

3.b. *poikkeukselliset Lie-tyypin ryhmät*

4. *26 sporadista ryhmää (ainoa äärellinen luokka)*

Klassiset Lie-tyypin ryhmät ovat äärellisten vektoriavaruuksien erityyppisten lineaarikuvausten muodostamia ryhmiä, siis matriisiryhmiä, tai oikeammin näiden ryhmien yksinkertaisia kompositiotekijöitä. Esimerkiksi ortogonaaliset ja unitaariset ryhmät kuuluvat mainittuihin lineaarikuvausryhmiin. Klassiset ryhmät voidaan konstruoida myös yksinkertaisten Lien algebrojen avulla, ja tällöin saadaan sivutuotteena joitakin ylimääräisiä yksinkertaisia ryhmiä, joita kutsutaan poikkeuksellisiksi Lie-tyypin ryhmiksi. Sporadiset ryhmät ovat ryhmiä, jotka eivät kuulu mihinkään muista luokista. Niistä suurinta nimitetään sen koon vuoksi "Hirviöryhmäksi". Hirviöryhmän kertaluku on kertaluokkaa $8 \cdot 10^{53}$.

11. Vapaat ryhmät

Vapailla moduleilla on virittäjäjoukko, jonka alkioilla ei ole keskenään mitään lineaarista riippuvuutta. Vastaavasti vapaat ryhmät ovat ryhmiä, joiden virittäjät ovat toisistaan riippumattomia. Vapaan ryhmän rakenne riippuu siis ainoastaan virittäjien lukumäärästä. Jokainen ryhmä saadaan jostakin vapaasta ryhmästä ilmoittamalla ne relaatiot, jotka virittäjien on toteutettava. Tällaista tapaa kuvailla ryhmää kutsutaan ryhmän esitykseksi virittäjien ja relaatioiden avulla.

Tässä materiaalin viimeisessä luvussa tutustutaan aluksi ryhmän esittämiseen virittäjien ja relaatioiden avulla ja sen jälkeen näytetään, miten tällainen ryhmä voidaan konstruoida. Konstruktio on jälleen esimerkki universaalikonstruktiosta.

Jos virittäjistä oletetaan vain, että ne kommutoivat keskenään, päädytään vapaaseen vaihdannaiseen ryhmään. Osoittautuu, että nämä ryhmät ovat täsmälleen samoja kuin vapaat $\mathbb{Z}$-modulit. Kaikki vaihdannaiset ryhmät saadaan vapaiden vaihdannaisten ryhmien tekijäryhminä. Kun virittäjien lukumäärä on äärellinen, näiden tekijäryhmien rakenne voidaan selvittää, ja tällä tavoin selviää siis kaikkien äärellisviritteisten vaihdannaisten ryhmien rakenne. Nämä tulokset esitetään viimeisessä alaluvussa.

11.1. Virittäjät ja relaatiot. Ryhmiä voidaan määritellä abstraktisti ilmoittamalla virittäjien lukumäärä sekä se, mitä ehtoja virittäjien on toteutettava. Lähdetään tutustumaan aiheeseen seuraavan esimerkin avulla, jossa annetaan uusi karakterisointi tutuille diedriryhmille.

Esimerkki 11.1. Etsittäessä neliön symmetriaryhmän konjugaattiluokkia esimerkissä 10.13 huomattiin, että konjugointikaava ${}^{\sigma}\rho = \rho^{-1}$ pätee, kun σ on peilaus ja ρ kierto. On helppo tarkistaa, että tämä kaava pätee muissakin diedriryhmissä. Tässä esimerkissä on tarkoitus osoittaa, että kyseinen konjugointiehto yhdessä eräiden alkioiden kertalukuja koskevien ehtojen kanssa riittää itse asiassa karakterisoimaan diedriryhmät täydellisesti.

Oletetaan, että ryhmä G on kahden eri alkion r ja s virittämä, joista alkion r kertaluku on $n > 1$ ja alkion s kertaluku 2. Oletetaan lisäksi, että ${}^{s}r = r^{-1}$. Osoitetaan, että tällöin ryhmä G on isomorfinen ryhmän D_n kanssa.

Ensinnäkin ryhmä sisältää alkion r virittämän aliryhmän $\langle r \rangle$, jossa on n alkiota. Toisaalta s ei kuulu ryhmään $\langle r \rangle$, mikä nähdään seuraavasti. Jos $n = 2$, aliryhmässä $\langle r \rangle$ on vain alkiot 1 ja r, eikä s oletuksien perusteella ole kumpikaan niistä. Jos taas $n > 2$, niin konjugointiehdon mukaan ${}^{s}r = r^{-1} \neq r$. Kuitenkin jokainen ryhmän $\langle r \rangle$ alkio keskittää alkion r, joten $s \notin \langle r \rangle$. Alkiota s vastaava sivuluokka $s\langle r \rangle$ sisältää siis n alkiota, jotka poikkeavat aliryhmän $\langle r \rangle$ alkioista.

Seuraavaksi näytetään, että kaikki ryhmän G alkiot ovat joko aliryhmässä $\langle r \rangle$ tai sivuluokassa $s\langle r \rangle$. Koska G on alkioiden r ja s virittämä, jokainen sen alkio voidaan esittää tulona alkioista r ja s. Konjugointiehdosta $srs^{-1} = r^{-1}$ ja alkioiden kertaluvuista seuraa, että $rs = sr^{n-1}$. Näin ollen alkioiden r ja s tulot voidaan järjestää niin, että kaikki alkion s esiintymät ovat vasemmassa päädyssä. Esimerkiksi

$$rrsrrrr = r(sr^{n-1})rrrr = (sr^{n-1})r^{n-1}rrrr = sr^{2n+2} = sr^2.$$

Koska s on oma käänteisalkionsa, vasemmasta päädystä voidaan lisäksi supistaa alkioita s pareittain. Näin ollen jokainen ryhmän alkio on joko muotoa r^j tai sr^j

jollain $j \in \mathbb{Z}$, joten se kuuluu joko aliryhmään $\langle r \rangle$ tai sivuluokkaan $s\langle r \rangle$. Tämä osoittaa myös, että ryhmässä on tasan $2n$ alkiota.

Lopulta isomorfian tarkistamiseksi määritetään ryhmän G kertotaulu. Käyttäen toistuvasti kaavaa $rs = sr^{n-1}$ voidaan laskea alkioiden tulot:

$$\begin{aligned} r^j \cdot r^k &= r^{j+k} \\ sr^j \cdot r^k &= sr^{j+k} \\ r^j \cdot sr^k &= sr^{j(n-1)}r^k = sr^{k-j} \\ sr^j \cdot sr^k &= s(sr^{k-j}) = r^{k-j}. \end{aligned}$$

Käyttämällä esimerkiksi diedriryhmän permutaatioesitystä ja asettamalla r vastaamaan kiertoa $(12\ldots n)$ ja s mitä tahansa peilausta voidaan tarkistaa, että yllä laskettu ryhmän G kertotaulu on sama kuin ryhmän D_n. Näin ollen ryhmät ovat isomorfiset.

Edellisessä esimerkissä diedriryhmä määriteltiin antamalla ryhmän virittäjät, näiden kertaluvut sekä eräs yhtälö, joka virittäjien on toteutettava. Tällaista tapaa määritellä ryhmä kutsutaan ryhmän *esitykseksi virittäjien ja relaatioiden avulla.* Relaatioesitystä merkitään

$$G = \langle s_1, \ldots, s_n \mid w_1, \ldots, w_m \rangle,$$

missä $s_1, \ldots, s_n$ ovat ryhmän virittäjät ja $w_1, \ldots, w_m$ ovat relaatioyhtälöt, jotka ryhmän alkioiden on toteutettava. Virittäjien oletetaan olevan erillisiä. Lisäksi oletetaan, että virittäjien välillä ei ole mitään ylimääräisiä relaatioita, jotka eivät seuraisi relaatioista $w_1, \ldots, w_m$. Relaation w sanotaan seuraavan relaatioista $w_1, \ldots, w_m$, mikäli w pätee jokaisessa ryhmässä, joka toteuttaa relaatiot $w_1, \ldots, w_m$.

Relaatioyhtälöt on tapana merkitä niin, että yhtälön toisella puolella on pelkkä neutraalialkio, ja usein tämäkin jätetään merkitsemättä. Tällöin edellisen esimerkin konjugointiehdosta tulisi $srsr = e$, tai pelkästään $(sr)^2$. Diedriryhmän tapauksessa voidaan siis merkitä

$$D_n = \langle r, s \mid r^n, s^2, (sr)^2 \rangle.$$

Tämä merkintä luetaan niin, että diedriryhmä on sellainen ryhmä, jolla on kaksi virittäjää r ja s, joille pätee $r^n = e$, $s^2 = e$ ja $(sr)^2 = e$.

Relaatioesitys on toisinaan käyttökelpoinen, mutta siihen liittyy myös hankaluuksia. Esimerkiksi yllä mainitussa diedriryhmän esityksessä vaaditaan, että $r^n = e$, mutta edeltävän esimerkin 11.1 todistuksessa oletettiin vahvemmin, että alkion r *kertaluku* on n. Diedriryhmän tapauksessa ongelmaa ei kuitenkaan synny. Esimerkin todistus nimittäin osoittaa joka tapauksessa, että annetut relaatiot pätevät diedriryhmässä D_n. Koska $r^m = e$ ei päde ryhmässä D_n millään $m < n$, kyseinen relaatio ei ole annettujen relaatioiden seuraus. Relaatioesityksessä oletetaan aina, että tällaiset relaatiot, jotka eivät seuraa annetuista relaatioista, eivät myöskään ole voimassa. Näin ollen alkion r kertaluku todellakin on n.

Toisinaan käy kuitenkin niin, että relaatioista seuraa jotakin odottamatonta.

Esimerkki 11.2. Tarkastellaan ryhmää

$$G = \langle a, b \mid aba^{-1} = b^2, bab^{-1} = a^2 \rangle.$$

Ryhmän virittää siis kaksi alkiota, jotka toteuttavat ristikkäiset konjugointirelaatiot. Alkioiden kertaluvuista ei tiedetä mitään, joten ryhmä voi ensi näkemältä olla äärellinen tai ääretön. Pienellä kokeilulla huomataan kuitenkin, että

$$(aba^{-1})b^{-1} = b^2b^{-1} = b \tag{1}$$

ja toisaalta, koska konjugointi on automorfismi,

$$a(ba^{-1}b^{-1}) = aa^{-2} = a^{-1}. \tag{2}$$

Yhtälöistä (1) ja (2) seuraa, että $a^{-1} = b$. Soveltamalla tätä ensimmäiseen konjugointiehtoon nähdään, että

$$b^2 = aba^{-1} = ab^2,$$

josta $a = e$. Tällöin edelleen

$$b^2 = aba^{-1} = ebe = b,$$

joten $b = e$. Nähtiin siis, että molemmat virittäjät ovat itse asiassa neutraalialkio, joten kyseessä on triviaalin ryhmän esitys.

Edellinen esimerkki osoittaa, että relaatioiden seurauksia voi olla vaikea ennakoida. Itse asiassa ei ole olemassa yleistä menetelmää, jolla voisi selvittää kuvaako jokin virittäjien ja relaatioiden avulla annettu ryhmän esitys jotain tiettyä ryhmää vai ei. Tämän osoittivat toisistaan tietämättä armenialainen Sergei Adian vuonna 1955 ja israelilainen Michael Rabin vuonna 1958. Toinen relaatioesityksiin ratkeamaton ongelma on niin kutsuttu ”sanaongelma” (engl. word problem). Se tarkoittaa kysymystä, voiko jollain algoritmilla selvittää, esittääkö annettu virittäjien tulo (eli *sana*) ryhmän neutraalialkiota vai ei. Sanaongelman ratkeamattomuuden yleisessä tapauksessa osoittivat venäläinen Pjotr Novikov vuonna 1955 ja amerikkalainen William Boone vuonna 1958.

11.2. Vapaan ryhmän konstruktio. Tässä alaluvussa tarkastellaan, miten virittäjien ja relaatioiden avulla esitetyt ryhmät voidaan konstruoida. Samalla tullaan osoittaneeksi, että mikä tahansa tällä tavalla esitetty ryhmä on itse asiassa olemassa. Konstruktio on universaalikonstruktio, jossa ensin määritellään kaikki mahdolliset annettujen virittäjien tuloina saatavat alkiot ja sen jälkeen samastetaan alkioita annettujen relaatioiden mukaan.

Olkoon S jokin symbolijoukko, joka sisältää symbolin e. Joukko F_S koostuu äärellisistä merkkijonoista

$$t_1t_2\cdots t_n,$$

missä jokainen t_i on joko muotoa s tai s^{-1} jollain $s \in S$. Näitä merkkijonoja kutsutaan *sanoiksi*. Laskutoimituksena on merkkijonojen yhteenliittäminen eli konkatenointi:

$$(t_1\cdots t_m)\cdot(t'_1\cdots t'_n) = t_1\cdots t_m t'_1\cdots t'_n.$$

Lisäksi merkkijonoja samastetaan seuraavien sääntöjen mukaan:

(1) $t_1\cdots ss^{-1}\cdots t_n = t_1\cdots e\cdots t_n$
(2) $t_1\cdots s^{-1}s\cdots t_n = t_1\cdots e\cdots t_n$
(3) $t_1\cdots e\cdots t_n = t_1\cdots t_n$.

Esimerkiksi alkioiden $s_1s_2s_3^{-1}$ ja $s_3s_2^{-1}s_1$ tulo voidaan laskea seuraavasti:

$$s_1s_2s_3^{-1}\cdot s_3s_2^{-1}s_1 = s_1s_2s_3^{-1}s_3s_2^{-1}s_1 = s_1s_2es_2^{-1}s_1 = s_1s_2s_2^{-1}s_1 = s_1es_1 = s_1s_1.$$

Tavalliseen tapaan merkitään $ss\cdots s = s^n$, jolloin edellisen laskun tulos kirjoitettaisiin s_1^2.

Seuraavan lauseen helpohko todistus sivuutetaan.

LAUSE 11.3. *Yllä kuvattu joukko F_S laskutoimituksineen ja samastuksineen on ryhmä, jonka neutraalialkiona toimii e. Symbolit s_i ja s_i^{-1} ovat toistensa käänteisalkioita kaikilla i ja sanan $t_1 \cdots t_n$ käänteisalkio on $t_n^{-1} \cdots t_1^{-1}$. Joukko S virittää ryhmän F_S.*

Ryhmää F_s nimitetään *vapaaksi ryhmäksi*. Se on ryhmä, jonka virittäjinä toimivat joukon S alkiot, ja näiden virittäjien välillä ei ole mitään relaatioita.

Jos joukossa S on n alkiota, vastaavaa vapaata ryhmää merkitään F_n. Vapaat ryhmät ovat aina äärettömiä, sillä minkä tahansa virittäjäalkion s kaikki potenssit poikkeavat toisistaan. Yhden alkion virittämä vapaa ryhmä on täten ääretön syklinen ryhmä, joten se on isomorfinen ryhmän $\mathbb{Z}$ kanssa. Yhden alkion virittämä vapaa ryhmä on ainoa vaihdannainen vapaa ryhmä, sillä jos s_1 ja s_2 ovat kaksi eri virittäjäalkiota, niin $s_1 s_2 \neq s_2 s_1$.

Vapaille ryhmille pätee seuraava universaaliominaisuus, jonka todistus sivuutetaan.

LAUSE 11.4 (Vapaan ryhmän universaaliominaisuus). *Olkoon F_S vapaa ryhmä virittäjäjoukkonaan S, ja olkoon $\iota\colon S \to F_S$ inkluusiokuvaus. Oletetaan lisäksi, että H on jokin ryhmä ja $f\colon S \to H$ on mikä tahansa kuvaus. Tällöin on olemassa yksikäsitteinen ryhmähomomorfismi $\varphi\colon F_S \to H$, jolle pätee $\varphi \circ \iota = f$.*

KOROLLAARI 11.5. *Jokainen ryhmä on jokin vapaan ryhmän tekijäryhmä.*

TODISTUS. Olkoon H jokin ryhmä. Universaaliominaisuudesta seuraa, että on olemassa homomorfismi $\varphi\colon F_H \to H$, jolle pätee $\varphi(h) = h$ kaikilla $h \in H$. Ryhmien homomorfialauseesta seuraa, että $F_H / \operatorname{Ker}\varphi \cong H$. □

Tarkastellaan nyt ryhmän esitystä $G = \langle S \mid W \rangle$, missä joukko S sisältää ryhmän virittäjät ja W relaatiot. Vapaa ryhmä F_S sisältää kaikki virittäjistä ja niiden käänteisalkioista muodostettavat sanat. Joukon W alkiot, eli annetun esityksen relaatiot, ovat vapaan ryhmän F_S alkioita. Nämä alkiot halutaan samastaa neutraalialkion kanssa. Ideana on muodostaa tekijäryhmä joukon W virittämän aliryhmän suhteen, mutta joukkoa W on ensin laajennettava, jotta aliryhmästä saadaan normaali.

Määritellään joukko

$$Z = \{{}^t w \mid w \in W, t \in F_S\}.$$

Joukko Z sisältää siis joukon W kaikkien alkioiden konjugaatit. Merkitään tämän joukon virittämää aliryhmää $N = \langle Z \rangle$. Tätä aliryhmää kutsutaan joukon W *normaaliksi sulkeumaksi*. Näillä merkinnöillä voidaan esittää seuraava lause.

LAUSE 11.6. *Aliryhmä N on normaali vapaassa ryhmässä F_S, ja tekijäryhmä F_S/N on isomorfinen ryhmän $G = \langle S \mid W \rangle$ kanssa.*

TODISTUS. Oletetaan, että $g \in F_S$, ja tarkastellaan alkion $n \in N$ konjugaattia ${}^g n$. Alkio n on tulo joistakin joukon Z alkioista ja näiden käänteisalkioista. Koska alkiolla g konjugointi on ryhmän F_S automorfismi, se säilyttää tulot ja käänteisalkiot, joten riittää tarkastella jotain alkiota $z \in Z$. Tämä puolestaan on muotoa ${}^t w$ joillain $t \in F_S$ ja $w \in W$. Nyt

$${}^g z = {}^g({}^t w) = {}^{gt} w \in Z \subset N.$$

Aliryhmä N sisältää siis joukon Z alkioiden konjugaatit, ja koska N on aliryhmä, se sisältää myös näistä ja näiden käänteisalkioista saatavat tulot, joten N sisältää kaikki konjugaattinsa. Näin ollen se on normaali.

Osoitetaan sitten jälkimmäinen väite. Käyttämällä vapaan ryhmän universaaliominaisuutta inkluusiokuvaukseen $\iota\colon S \to G$ saadaan ryhmähomomorfismi $\varphi\colon F_S \to G$, jolle pätee $\varphi(s) = s$ kaikilla $s \in S$. Koska joukko S virittää ryhmän G ja vapaa ryhmä F_S sisältää kaikki virittäjistä ja näiden käänteisalkioista saatavat muodolliset tulot, nähdään helposti, että homomorfismi φ on surjektiivinen. Tarkastellaan ydintä $\operatorname{Ker}\varphi$.

Oletetaan, että $t \in \operatorname{Ker}\varphi$ jollain $t \in F_S$. Kirjoittamalla t virittäjien avulla nähdään, että $\varphi(t) = e$ on jokin relaatio, joka on voimassa joukon S alkioiden välillä ryhmässä G. Se on siis seuraus joukon W relaatioista, mikä tarkoittaa sitä, että se pätee missä tahansa ryhmässä, joka sisältää joukon W alkiot. Koska $W \subset N$, nähdään, että $t \in N$, mistä seuraa $\operatorname{Ker}\varphi \subset N$.

Toisaalta jokaisella $w \in W$ pätee $\varphi(w) = e$ ryhmässä G, joten $w \in \operatorname{Ker}\varphi$. Koska $\operatorname{Ker}\varphi$ on normaali aliryhmä, se sisältää alkioidensa konjugaatit. Määritelmänsä nojalla N on pienin aliryhmä, joka sisältää kaikki joukon W alkioiden konjugaatit, joten $N \subset \operatorname{Ker}\varphi$. Näin ollen $\operatorname{Ker}\varphi = N$, joten tulos seuraa ryhmien homomorfialauseesta. □

Korollaari 11.7. *Jokainen ryhmä voidaan esittää virittäjien ja relaatioiden avulla.*

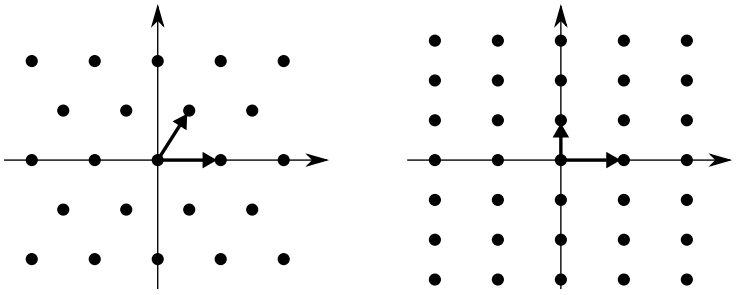
Todistus. Olkoon H jokin ryhmä. Vapaan ryhmän universaaliominaisuuden nojalla löytyy homomorfismi $\varphi\colon F_H \to H$, jolle pätee $\varphi(h) = h$ kaikilla $h \in H$. Homomorfialauseen nojalla $H \cong F_H/\operatorname{Ker}\varphi$. Edellisen lauseen perusteella ryhmällä H on esitys $\langle H \mid \operatorname{Ker}\varphi\rangle$. □

11.3. Vapaat vaihdannaiset ryhmät. Vapaaksi vaihdannaiseksi ryhmäksi kutsutaan ryhmää, jolla on virittäjäjoukko, jonka alkiot ovat muuten riippumattomia paitsi että ne kommutoivat keskenään. Tästä seuraa, että koko ryhmä on vaihdannainen. Modulien yhteydessä todettiin, että jokainen vaihdannainen ryhmä on $\mathbb{Z}$-moduli (vrt. esim. 2.2), ja siksi vaihdannaisten ryhmien teoria on myös $\mathbb{Z}$-modulien teoriaa. Vapaat vaihdannaiset ryhmät ovat puolestaan vapaita $\mathbb{Z}$-moduleja (vrt. esim. 2.6). Ryhmän virittäjäjoukko S muodostaa $\mathbb{Z}$-modulin kannan, ja ryhmä on modulina isomorfinen suoran summan $\mathbb{Z}^{(S)}$ kanssa (vrt. esim. 3.4).

Esimerkki 11.8. Matematiikassa *hila* määritellään ryhmän $\mathbb{R}^n$ aliryhmänä, joka on isomorfinen äärellisviritteisen vapaan vaihdannaisen ryhmän $\mathbb{Z}^n$ kanssa. Hila on samalla vektoriavaruuden $\mathbb{R}^n$ osajoukko. Tämän vektoriavaruuden kanta voidaan valita niin, että hilaan kuuluvat täsmälleen ne kantavektorien lineaarikombinaatiot, joiden kertoimet ovat kokonaislukuja. Kuvassa 19 on esitetty kaksi hilaa avaruudessa $\mathbb{R}^2$. Algebran lisäksi hiloilla on sovelluksia muun muassa lukuteoriassa, koodausteoriassa ja materiaalifysiikassa.

Vapaat modulit toteuttavat universaaliominaisuuden (lause 2.7), joten sama universaaliominaisuus pätee myös vapailla vaihdannaisilla ryhmillä. Ryhmien kielelle käännettynä lause kuuluu seuraavasti.

Lause 11.9. *Olkoon G vapaa vaihdannainen ryhmä virittäjäjoukkonaan S, ja olkoon $\iota\colon S \to G$ inkluusiokuvaus. Oletetaan lisäksi, että H on jokin toinen*



KUVA 19. Kaksi tasohilaa kantavektoreineen.

vaihdannainen ryhmä ja $f\colon S \to H$ on mikä tahansa kuvaus. Tällöin on olemassa yksikäsitteinen ryhmähomomorfismi $\varphi\colon G \to H$, jolle pätee $\varphi \circ \iota = f$.

Universaaliominaisuudesta saadaan seurauslause samaan tapaan kuin vapaiden ryhmien tapauksessa.

KOROLLAARI 11.10. *Jokainen vaihdannainen ryhmä on jonkin vapaan vaihdannaisen ryhmän tekijäryhmä.*

Jos vaihdannaisella ryhmällä on äärellinen virittäjäjoukko, se voidaan edellisten tulosten perusteella esittää suoran summamodulin $\mathbb{Z}^n$ tekijämodulina. Tällaisten modulien rakenne tunnetaan hyvin.

LAUSE 11.11 (Äärellisviritteisten vaihdannaisten ryhmien peruslause). *Olkoon G vaihdannainen ryhmä, jolla on äärellinen virittäjäjoukko. Tällöin G on isomorfinen suoran summan*

$$\mathbb{Z}_{p_1^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{k_s}} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$$

kanssa, missä jokainen p_i on alkuluku ja jokainen k_i positiivinen kokonaisluku. Lisäksi esitys on summattavien järjestystä vaille yksikäsitteinen.

Huomautus. Jotkin lauseen alkuluvuista p_i ja eksponenteista k_i voivat olla keskenään samoja. Muotoa $\mathbb{Z}$ olevien summattavien lukumäärää kutsutaan ryhmän G *asteeksi* (engl. rank) tai *Bettin luvuksi*.

TODISTUKSEN HAHMOTELMA. Käydään läpi todistuksen pääideat ja sivuutetaan täsmälliset yksityiskohdat.

Olkoon G vaihdannainen ryhmä, jolla on äärellinen virittäjäjoukko, jonka koko on n. Vapaiden modulien universaaliominaisuuden nojalla on olemassa modulihomomorfismi $\varphi\colon \mathbb{Z}^n \to G$. Ideana on löytää vapaalle modulille $\mathbb{Z}^n$ kanta $X = \{x_1, \ldots, x_n\}$, jolla on sellainen ominaisuus, että joukosta $\{m_1 x_1, \ldots, m_s x_s\}$ tulee alimodulin $\operatorname{Ker}\varphi$ kanta joillain kokonaisluvuilla $m_1, \ldots, m_s$, missä $s \leq n$. Kun modulin alkiot kirjoitetaan tässä kannassa, ydin on

$$\operatorname{Ker}\varphi = \{(a_1 m_1, \ldots, a_s m_s, 0, \ldots, 0) \mid a_1, \ldots, a_s \in \mathbb{Z}\}.$$

Modulien homomorfialauseesta seuraa tällöin, että

$$G \cong \mathbb{Z}^{(X)} / \operatorname{Ker}\varphi = \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_s} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}.$$

Kun G on esitetty syklisten ryhmien $\mathbb{Z}_{m_i}$ ja $\mathbb{Z}$ suorana summana, voidaan äärelliset sykliset ryhmät purkaa sellaisiksi, joiden kertaluvut ovat alkulukujen potensseja. Purkamiseen käytetään tulosta (nk. kiinalainen jäännöslause), jonka mukaan $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \oplus \mathbb{Z}_n$, jos $\operatorname{syt}(m, n) = 1$. Esimerkiksi $\mathbb{Z}_{20} \cong \mathbb{Z}_4 \oplus \mathbb{Z}_5$.

Lopuksi on osoitettava hajotelman yksikäsitteisyys. Bettin luvun $n - s$ yksikäsitteisyys seuraa vapaan modulin kannan pituuden yksikäsitteisyydestä (vrt. esim. 3.15) seuraavasti. Olkoon T ryhmän G osajoukko, johon kuuluvat kaikki alkiot, joiden kertaluku on äärellinen. Tämä joukko on aliryhmä, jota kutsutaan ryhmän G *torsioaliryhmäksi*. Tekijäryhmä G/T on vapaa $\mathbb{Z}$-moduli, ja $G/T \cong \mathbb{Z}^{n-s}$. Kannan pituuden yksikäsitteisyys takaa nyt Bettin luvun yksikäsitteisyyden.

Alkulukupotenssien yksikäsitteisyyksien todistaminen onnistuu vertailemalla alkioiden kertalukuja. Esimerkiksi ryhmät $\mathbb{Z}_2 \oplus \mathbb{Z}_8$ ja $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ sisältävät kumpikin 16 alkiota, mutta ne eivät ole isomorfisia, sillä ensimmäinen sisältää alkion, jonka kertaluku on 8 ja jälkimmäinen ei.

Koko todistus löytyy esimerkiksi John Fraleighin kirjasta A First Course in Abstract Algebra, jossa osa yksityiskohdista on jaettu harjoitustehtäviksi. □

Sovelluksena äärellisviritteisten vaihdannaisten ryhmien peruslauseesta voidaan todistaa kuntien aliryhmiä koskeva tulos.

LAUSE 11.12. *Minkä tahansa kunnan kertolaskuryhmän jokainen äärellinen aliryhmä on syklinen.*

TODISTUS. Olkoon K jokin kunta, ja olkoon G ryhmän K^* äärellinen aliryhmä, jonka kertaluku on n. Äärellisviritteisten vaihdannaisten ryhmien peruslauseen nojalla G on isomorfinen syklisten ryhmien tulon $C_{m_1} \times \cdots \times C_{m_s}$ kanssa. Jos $\text{syt}(m_i, m_j) = 1$ kaikilla i ja j, ryhmä G on syklinen, sillä $G \cong C_{m_1 \cdots m_s}$. Oletetaan siis, että $\text{syt}(m_i, m_j) > 1$ joillain i ja j.

Olkoon $d > 1$ sellainen, että $d \mid m_i$ ja $d \mid m_j$. Tällöin ryhmällä C_{m_i} on aliryhmä, jonka kertaluku on d, ja tämän aliryhmän kaikkien alkioiden kertaluku jakaa luvun d. Sama koskee ryhmää C_{m_j}. Tästä seuraa, että ryhmässä G on yhteensä vähintään d^2 alkiota, joiden kertaluku on luvun d tekijä. Merkitään näiden alkioiden joukkoa D. Kunnassa K jokainen joukon D alkio on polynomin $X^d - 1$ juuri. Tällä polynomilla on kuitenkin korkeintaan d juurta, mikä on ristiriita. Täten ryhmä G on syklinen. □

KOROLLAARI 11.13. *Äärellisten kuntien kertolaskuryhmät ovat syklisiä.*

LOPPU