Algebra II

Jokke Häsä

Matematiikan ja tilastotieteen laitos, kevät 2010

Helsingin yliopisto

Sisältö

Peruskäsitteet

0. Kertausta

Tässä luvussa käydään läpi sellaiset peruskäsitteet ja merkinnät, joiden oletetaan olevan tuttuja aiemmalta algebran kurssilta.

0.1. Laskutoimitukset. Olkoon X joukko. Joukon X *laskutoimitus* on kuvaus $* : X \times X \to X$, joka liittää jokaiseen pariin (x, y) yksikäsitteisen alkion joukosta X. Tätä alkiota kutsutaan laskutoimituksen *tulokseksi* ja merkitään tavalliseen tapaan $x*y$. Laskutoimituksella varustettu joukko tarkoittaa paria $(X, *)$. Tämä on yksinkertaisin algebrallinen struktuuri, ja sitä nimitetään toisinaan *magmaksi*.

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. (Todistetaan 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. Jos laskutoimitus on lisäksi vaihdannainen, ei alkioiden järjestyksellä lausekkeessa ole väliä, joten voidaan ottaa käyttöön tulomerkintä

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

tai yleisemmin, jos I on jokin äärellinen indeksijoukko:

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

Laskutoimituksen *neutraalialkioksi* kutsutaan alkiota e, jolle pätee

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

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

$$x * y = y * x = e,$$

missä e on neutraalialkio. Alkion x käänteisalkiota merkitään yleensä x^{-1}.

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

$$e = e * e' = e',$$

joten $e = e'$. 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 $y = y'$.

Jos laskutoimituksella on neutraalialkio, voidaan määritellä alkion x *kertaluku.* Jos 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.

Neutraalialkio mahdollistaa nollapotenssin ja tyhjän tulon määrittelyn. Jos $m < n$, niin

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

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

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

(Potenssin kirjoittamisessa vaaditaan tietysti laskutoimituksen liitännäisyyttä.) Näistä määritelmistä seuraavat tutut potenssilait:

$$x^m * x^n = x^{m+n} \qquad \text{ja} \qquad (x^m)^n = x^{m \cdot n},$$

missä m ja n voivat olla mitä tahansa kokonaislukuja; negatiivisten potenssien tapauksessa vaaditaan alkion x kääntyvyyttä.

Tavallisesti laskutoimituksia merkitään joko *multiplikatiivisesti* kertolaskun tapaan, tai *additiivisesti* yhteenlaskun tapaan. (Jälkimmäisessä tapauksessa oletetaan käytännössä aina, että laskutoimitus on vaihdannainen.) Oheisesta taulukosta selviävät eri merkintätapojen yksityiskohdat.

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

Joukko X saatetaan myös varustaa useammalla kuin yhdellä laskutoimituksella, tavallisimmin kahdella. Tällöin toinen laskutoimitus on yleensä vaihdannainen, ja sitä merkitään additiivisesti; toista laskutoimitusta merkitään puolestaan multiplikatiivisesti. Koko rakenne on siis kolmikko $(X, +, \cdot)$. Laskulausekkeissa kertolaskut ajatellaan laskettavaksi ennen yhteenlaskuja, joten esim. $x + y \cdot z$ tarkoittaa lauseketta $x + (y \cdot z)$. Lisäksi sanotaan, että tällaiset laskutoimitukset toteuttavat *osittelulain*, mikäli

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

kaikilla $x, y, z \in X$.

0.2. Perusrakenteet. Tavallisimpiin algebrallisiin rakenteisiin kuuluu ryhmä.

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

(G0) G on suljettu laskutoimituksen suhteen, eli $x * y \in G$ kaikilla $x, y \in G$.
(G1) Laskutoimitus on liitännäinen.
(G2) Laskutoimituksella on neutraalialkio joukossa G.
(G3) Jokaisella $x \in G$ on käänteisalkio joukossa G.

Huomataan, että ehto (G0) sisältyy itse asiassa jo laskutoimituksen määritelmään. Käänteisalkiot ovat yksikäsitteisiä, koska laskutoimitus on liitännäinen. Mikäli laskutoimitus on lisäksi vaihdannainen, rakennetta nimitetään *vaihdannaiseksi* eli *Abelin*[1] *ryhmäksi*. Eräitä esimerkkejä ryhmistä ovat

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

Ryhmälaskutoimituksen tärkein ominaisuus on *sievennyssääntö*. Jos x, y ja z ovat ryhmän alkioita ja e on neutraalialkio, niin

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

Sievennyssääntö käyttää hyväkseen kaikkia ryhmäaksioomia. Tästä säännöstä saadaan myös seuraava aputulos.

LEMMA 0.2. *Olkoon $(G, *)$ ryhmä, neutraalialkiona e. Tällöin kaikilla $x, y \in G$ pätee*

$$x * y = y \qquad \Rightarrow \qquad x = e.$$

Tarkastelemalla kontrapositiota "jos $x \neq e$, niin $x * y \neq y$" voidaan saatu tulos tulkita niin, että ryhmässä millä tahansa neutraalialkiosta poikkeavalla alkiolla kertominen muuttaa kaikkia muita alkioita.

Rakennetta, joka toteuttaa edellisestä määritelmästä vain ehdot (G0) ja (G1), nimitetään *puoliryhmäksi*. (Puoliryhmä on siis liitännäinen magma.) Jos rakenne toteuttaa ehdot (G0)–(G2), sitä kutsutaan *monoidiksi*. Esimerkkejä monoideista ovat luonnollisten lukujen vaihdannainen monoidi $(\mathbb{N}, +)$ (neutraalialkiona 0), sekä kaikkien $n \times n$-reaalimatriisien muodostama joukko varustettuna matriisikertolaskulla (neutraalialkio yksikkömatriisi). Esimerkkejä puoliryhmistä ovat $(\mathbb{Z}_+, +)$ (positiiviset kokonaisluvut), sekä minkä tahansa renkaan ideaali (määritelmä seuraa myöhemmin), laskutoimituksena kyseisen renkaan kertolasku.

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

Kahden laskutoimituksen rakenteista yleisimpiä 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) Osittelulaki pätee.

Rengasta nimitetään *vaihdannaiseksi*, mikäli kertolasku on vaihdannainen.

Esimerkkejä renkaista:

- $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$
- $(\mathbb{Z}_n, +, \cdot)$ (modulaariaritmetiikka)
- $n \times n$-reaalimatriisit
- Abelin ryhmän G endomorfismit (homomorfismit $G \to G$) varustettuna pisteittäisellä yhteenlaskulla: $(f + g)(x) = f(x) + g(x)$, ja kuvausten yhdistämisellä.

Renkaan R kääntyvien alkioiden joukkoa merkitään usein R^*. Tämä tulee erityisesti kyseeseen tuttujen lukurenkaiden, kuten renkaiden $\mathbb{Q}$, $\mathbb{R}$ ja $\mathbb{Z}_n$, kohdalla. Esim. $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$.

Osittelulaista seuraa, että renkaassa R pätee $0 \cdot x = x \cdot 0 = 0$ kaikilla $x \in R$, nimittäin

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

josta yhteenlaskuryhmän sievennyssääntöä 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. *triviaalirengas*).

Olkoon jatkossa R vaihdannainen rengas, jossa $0 \neq 1$. On mahdollista, että $x \cdot y = 0$, vaikka $x \neq 0 \neq y$ (vrt. matriiseihin). Mikäli kuitenkin kaikilla $x, y \in R$ pätee

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

vaihdannaista rengasta R nimitetään *kokonaisalueeksi*. 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 $(K \setminus \{0\}, \cdot)$ muodostaa vaihdannaisen ryhmän.

Vaihdannainen epätriviaali rengas on siis kunta, jos ja vain jos se sisältää kaikkien nollasta poikkeavien alkioidensa käänteisalkiot. Jokainen kunta on kokonaisalue, sillä jos $x \cdot y = 0$ joillain $x, y \in K$, ja $x \neq 0$, niin

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

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. Mahdollisimman yleisesti muotoiltuna laskutoimitusstruktuurin X *alistruktuurilla* tarkoitetaan osajoukkoa $Y \subset X$, jolle pätevät seuraavat ehdot:

- Y on suljettu kaikkien X:n laskutoimitusten suhteen.
- 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 realisoituvat hieman eri muodoissa eri rakenteiden yhteydessä. Ehdoista seuraa, että alistruktuuri on aina samaa tyyppiä kuin ympäröivä struktuuri, esim. alirengas on aina itsekin rengas. Kuitenkaan mikä tahansa renkaan ehdot täyttävä toisen renkaan osajoukko ei välttämättä ole alirengas.

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 seuraa että $g^{-1} \in H$ sekä edelleen $e = g \cdot g^{-1} \in H$. Pienellä päättelyllä saadaan seuraava toisinaan kätevä tulos.

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

(H1) $H \neq \emptyset$
(H2) $gh^{-1} \in H$ *kaikilla* $g, h \in H$.

Toinen aliryhmiin liittyvä erikoisuus mainitaan seuraavassa lauseessa.

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 olla esimerkiksi eri neutraalialkio kuin ryhmällä G. Voisi siis päteä $e' \cdot g = g$ kaikilla $g \in H$, vaikka e' ei olisikaan koko ryhmän G neutraalialkio. Ryhmässä kuitenkin millä tahansa varsinaisesta neutraalialkiosta poikkeavalla alkiolla kertominen muuttaa kaikkia muita alkioita, joten edellä kuvailtuja pienemmässä joukossa toimivia neutraalialkioita ei löydy. Tulos seuraa tästä sekä ympäröivän ryhmän G käänteisalkioiden yksikäsitteisyydestä.

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

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

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.[2] Tästä seuraa ryhmäteorian kenties tärkein tulos.

LAUSE 0.8 (Lagrange[3]). *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 yleisemmässä (ja kompaktimmassa) muodossa: $[G : H] = G/H$.

Yleisistä alistruktuuriehdoista saadaan kriteerit myös alirenkaana tai alikuntana olemiselle.

LAUSE 0.9 (Alirengaskriteeri.). *Renkaan R osajoukko A on alirengas, jos ja vain jos*

(AR1) $x - y \in A$ *kaikilla* $x, y \in A$
(AR2) $xy \in A$ *kaikilla* $x, y \in A$
(AR3) $1 \in A$ *(kertolaskun neutraalialkio renkaassa R).*

Ehdon (AR1) muotoilussa on käytetty yllä mainittua aliryhmäkriteeriä; kolmas ehto nimittäin takaa, että A on epätyhjä.

LAUSE 0.10 (Alikuntakriteeri.). *Kunnan K osajoukko L on alikunta, jos ja vain jos*

(AK1) $L^* \neq \emptyset$
(AK2) $x - y \in L$ *kaikilla* $x, y \in L$
(AK3) $xy^{-1} \in L$ *kaikilla* $x \in L$ *ja* $y \in L^*$.

Mikä tahansa struktuurin X osajoukko S ei ole välttämättä alistruktuuri, mutta se voidaan aina täydentää alistruktuuriksi lisäämällä siihen sopivasti alkioita. Pienintä alistruktuuria, joka sisältää joukon S nimitetään *S:n virittämäksi* alistruktuuriksi ja merkitään $\langle S \rangle$. Voidaan osoittaa, että $\langle S \rangle$ on kaikkien niiden alistruktuurien 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

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

Yhden alkion x virittämää aliryhmää voidaan merkitä $\langle x \rangle$. Jos $G = \langle x \rangle$ jollain x, eli koko ryhmä on yhden alkionsa virittämä, ryhmää kutsutaan *sykliseksi*. Syklistä ryhmää merkitään yleensä C_n, missä n on alkion x kertaluku (voi olla myös ääretön). Ryhmän C_n alkioiden lukumäärä on n. Esimerkiksi $\mathbb{Z}$ on ääretön syklinen ryhmä. Sykliset ryhmät ovat yksinkertaisimpia vaihdannaisia ryhmiä. Niiden kaikki ali- ja tekijäryhmät ovat myös syklisiä.

[2]Myös äärettömän aliryhmän sivuluokat ovat yhtä mahtavia.

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

0.4. 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 $f : (X, *) \to (Y, \circ)$ kuvaa mahdolliset käänteisalkiot käänteisalkioiksi kaikkien struktuurien tapauksessa. Tämä seuraa yhtälöketjusta

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

joiden perustella $f(x)^{-1} = f(x^{-1})$. Induktiolla saadaan lopulta osoitettua, että

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

kaikilla kokonaisluvuilla n.

Homomorfismien merkitys on siinä, että ne säilyttävät algebralliset ominaisuudet. Esimerkiksi alistruktuurin kuva homomorfismissa on vastaavanlainen alistruktuuri maalistruktuurissa. Myös liitännäisyys-, vaihdannaisuus- ja ositteluominaisuudet säilyvät. Erityisesimerkki homomorfismista on bijektiivinen eli kääntyvä homomorfismi, jota nimitetään *isomorfismiksi*. Koska se kuvaa struktuurit toisikseen säilyttäen algebralliset ominaisuudet molempiin suuntiin, ovat nämä ns. *isomorfiset struktuurit* täysin samankaltaiset toistensa kanssa, alkioiden ja laskutoimitusten nimeämistä vaille identtiset.

Ryhmien tapauksessa myös homomorfismin kohdalla saadaan muutamia yksinkertaistuksia. Ensinnäkin ryhmien välisen kuvauksen $f : (G, *) \to (H, \circ)$ tapauksessa jälkimmäistä homomorfismiehtoa (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 sievennyssäännön avulla tulee $e_H = f(e_G)$. Toinen seikka liittyy homomorfismin *ytimeen*

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

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 osoittaa injektiivisyyden.

Ryhmähomomorfismia koskien voidaan tässä yhteydessä mainita seuraava helposti muistettava sääntö.

LAUSE 0.11. *Homomorfismi f ryhmältä G ryhmään H on*

- *injektiivinen* $\iff$ $\operatorname{Ker} f = \{e_G\}$

- *surjektiivinen* $\iff$ $\operatorname{Im} f = H$.

Rengashomomorfismin $f : R \to S$ 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 triviaali.

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

LAUSE 0.12. *Jokainen kuntahomomorfismi $f : K \to L$ on injektiivinen.*

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

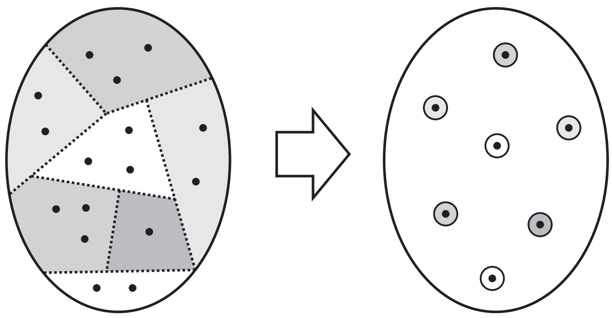
1. Tekijärakenteet

Tässä osassa tarkastellaan tekijärakenteita, kuten tekijäryhmiä ja tekijärenkaita, lähtien liikkeelle mahdollisimman yleisistä periaatteista. Tekijärakenteiden ajatuksena on päästä tarkastelemasta yksityiskohtia silloin, kun se ei ole välttämätöntä. Esimerkiksi annetun kokonaisluvun parillisuuden päättelemiseen tarvitsee tarkastella vain viimeistä numeroa. Yhteenlaskusta puolestaan tiedämme, että kahden luvun summa on parillinen, jos ja vain jos luvut ovat joko molemmat parillisia tai molemmat parittomia. Silloin kun parillisuus on ainoa kiinnostava ominaisuus, selviämme hyvin mistä tahansa yhteenlaskuun liittyvästä ongelmasta tarkkailemalla vain yhteenlaskettavien parillisuutta. Esimerkiksi summan

$$102738471029348 + 1723841702893740 + 172389471029347$$

selvittäminen on työlästä, mutta pelkkä vilkaisu kertoo, että tulos on pariton.

1.1. Ekvivalenssirelaatiot. Minkä tahansa tekijärakenteen taustalla on *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.



Kuva 1. Tekijärakenteessa samaan osaan kuuluvat alkiot samastetaan.

Toinen tapa ymmärtää tekijärakennetta on, että ajatellaan *samastettavaksi* samaan osaan sisältyvät alkiot. Tällöin niiden väliset erot ikään kuin tahallisesti unohdetaan. Tämä johtaa luonnollisella tavalla *ekvivalenssirelaation* käsitteeseen. Jos R on jokin kaksipaikkainen relaatio, niin merkintä xRy tarkoittaa, että x on relaatiossa alkion y kanssa.[4] Intuitio antaa olettaa, että kuvatakseen ekvivalenssia (tai "samastamista") kaksipaikkaisen relaation R on toteutettava alla olevat ehdot kaikilla alkioilla x, y, z:

1. R on *refleksiivinen*, eli xRx.
2. R on *symmetrinen*, eli jos xRy, niin yRx.
3. R on *transitiivinen*, eli jos xRy ja yRz, niin xRz.

Nämä ehdot voidaan ottaa ekvivalenssirelaation määritelmäksi.

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

MÄÄRITELMÄ 1.1. Kaksipaikkaista relaatiota R joukossa X kutsutaan *ekvivalenssirelaatioksi*, jos se on refleksiivinen, symmetrinen ja transitiivinen. Alkion x sanotaan olevan *ekvivalentti* alkion y kanssa, jos xRy. Alkion x *ekvivalenssiluokaksi relaation R suhteen* nimitetään joukkoa, joka sisältää kaikki x:n kanssa ekvivalentit alkiot:

$$[x]_R = \{y \in X \mid xRy\}.$$

Ekvivalenssiluokkaa voidaan merkitä myös $[x]$ tai $\overline{x}$, jos relaatio on asiayhteydestä selvä. Relaation R kaikkien ekvivalenssiluokkien joukkoa merkitään X/R.

Tietyn ekvivalenssirelaation ekvivalenssiluokat muodostavat aina osituksen. Toisaalta jokainen ositus antaa aiheen määritellä ekvivalenssirelaatio, jossa samaan osaan kuuluvat alkiot ovat keskenään ekvivalentteja. Kaksi ekvivalenssiluokkaa $[x]$ ja $[y]$ ovat samat, jos ja vain jos x on ekvivalentti y:n kanssa. Sanotaan, että sekä x että y ovat tämän ekvivalenssiluokan *edustajia*.

Olkoon nyt $(X, *)$ jokin algebrallinen struktuuri, 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 $*'$, joka vastaa luonnollisella tavalla alkuperäistä laskutoimitusta:

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

Tässä määritelmässä on eräs ongelma. Laskutoimituksen $*'$ täytyisi liittää jokaiseen pariin $([x], [y])$ yksikäsitteinen kolmas alkio $[x] *' [y]$. Kaavan antama tulos $[x * y]$ riippuu kuitenkin näennäisesti joukon X alkioista x ja y. Kukin ekvivalenssiluokka voi sisältää monia eri alkioita $x_1, x_2, x_3, \dots$, ja tällöin $[x_1] = [x_2] = [x_3]$, jne. Jotta laskutoimituksen $[x] *' [y]$ tulos olisi yksikäsitteinen, on siis pidettävä huoli siitä, että se ei riipu joukon X alkioista vaan ainoastaan niiden edustamista luokista. Toisinaan sanotaan, että tällöin kaavan antama laskutoimitus on *hyvin määritelty*. Määrittelyn onnistuminen yleisessä tapauksessa vaatii, että laskutoimitus ja ekvivalenssirelaatio ovat tietyllä tavalla yhteensopivat.

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 $*'$, jolle pätee*

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

kaikilla $x, y \in X$.

TODISTUS. Jotta lauseessa annettu kaava määrittelisi laskutoimituksen $*'$ 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 $*'$ 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 sekaantumisen vaaraa ei ole.

Mikäli laskutoimituksella on rakenteessa X neutraalialkio, sen ekvivalenssiluokka $[e]$ toimii neutraalialkiona tekijärakenteessa. Tämä nähdään siitä, että $[e] * [x] = [e * x] = [x]$ kaikilla $x \in X$.

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 $m + m' = 2k$ 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, ts. parillisen luvun lisääminen säilyttää parillisuuden ja parittomuuden. Saatu kaksialkioinen tekijämonoidi on itse asiassa ryhmä, sillä $[1]$ on oma vasta-alkionsa.

Voitaisiin myös tarkastella luonnollisten lukujen 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 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.

Esimerkki 1.5. *Erotusmonoidit.* Olkoon $(M, +)$ vaihdannainen monoidi, esim. $(\mathbb{N}, +)$. Yritetään luoda monoidia M vastaava rakenne, jossa kaikki alkiot olisivat kääntyviä. Ideana on muodostaa symbolisia erotuksia $a - b$, joista sitten samastetaan ne, joiden voi ajatella vastaavan samaa alkiota.

Erotuksien muodostamiseksi tarkastellaan tulomonoidia $(M \times M, +)$, jossa yhteenlasku määritellään pisteittäin: $(a, b) + (c, d) = (a + c, b + d)$, ja neutraalialkiona toimii $(0, 0)$. Paria (a, b) voidaan nyt pitää symbolisena erotuksena. Tulomonoidissa määritellään relaatio

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

Relaatiota voidaan verrata kokonaislukujen laskusääntöihin, joiden mukaan $a - b = a' - b'$, jos ja vain jos $a + b' = a' + b$. Alkio c voidaan jättää ehdosta pois, jos jokainen alkio on *supistuva*, eli jos ehdosta $x + c = y + c$ seuraa $x = y$ (kuten luonnollisilla luvuilla).

On helppo osoittaa, että relaatio $\sim$ on yhteenlaskun kanssa yhteensopiva ekvivalenssirelaatio. Saatavaa tekijärakennetta $M \times M/\sim$ kutsutaan *erotusmonoidiksi.*

Kanoninen kuvaus $a \mapsto [(a, 0)]$ liittää alkuperäisen monoidin M erotusmonoidiinsa. Mikäli jokainen alkio on supistuva, kanoninen kuvaus on injektio, ja alkuperäinen monoidi voidaan ajatella erotusmonoidin osajoukkona (esim. $(\mathbb{N}, +) \subset (\mathbb{Z}, +)$). Erotusmonoidissa jokaisella alkiolla $[(a, b)]$ on vasta-alkio, sillä

$$[(b, a)] + [(a, b)] = [(a + b, a + b)] = [(0, 0)].$$

Erotusmonoidin konstruktiota voidaan hieman yleistää valitsemalla aluksi jokin laskutoimituksen suhteen suljettu osajoukko S, jonka alkioista halutaan kääntyviä. Tällöin ekvivalenssin ehdoksi tulomonoidissa tulee

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

Tällainen yleisempi konstruktio on tarpeen esimerkiksi silloin, kun monoidista $(\mathbb{Z}, \cdot)$ halutaan konstruoida murtoluvut. Joukoksi S on tässä tapauksessa valittava $\mathbb{Z} \setminus \{0\}$. (Multiplikatiivisen merkinnän tapauksessa erotusmonoidia kutsutaan *jakomonoidiksi.*)

1.2. Homomorfismien hajottaminen. Oletetaan, että on määritelty algebrallinen struktuuri $(X, *)$ ja sen tekijästruktuuri X/R ekvivalenssirelaation R suhteen. Kuvausta $\pi : X \to X/R$, $\pi(x) = [x]$, joka liittää jokaiseen alkioon sen edustaman ekvivalenssiluokan, nimitetään *kanoniseksi surjektioksi.* Tekijärakenteen määritelmästä seuraa suoraan, että kanoninen surjektio on aina homomorfismi.

Oletetaan nyt, että on lisäksi määritelty homomorfismi $f : (X, *) \to (Y, \cdot)$. Herää kysymys, voidaanko määritellä sellaista homomorfismia $\overline{f}$ tekijärakenteesta X/R joukkoon Y, joka toteuttaisi ehdon

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

Tämän ehdon toteutuessa sanotaan, että alla oleva kaavio *kommutoi.*

$$\begin{tikzcd} X \arrow[rr, "f"] \arrow[dr, "\pi"'] & & Y \\ & X/R \arrow[ur, dashed, "\overline{f}"'] & \end{tikzcd}$$

Kommutointiehdon merkitys on siinä, että sen toteutuessa voitaisiin kirjoittaa

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

jolloin homomorfismin $\overline{f}$ ominaisuudet olisivat suoraan johdettavissa kuvauksen f ominaisuuksista. Ongelma puolestaan on se, että kuvaus f voi saada eri arvoja sellaisillakin alkioilla, jotka kuuluvat samaan ekvivalenssiluokkaan, kun taas $\overline{f} \circ \pi$ kuvaa tällaiset alkiot aina samalle alkiolle. Ongelma ratkaistaan samalla tavoin kuin tekijärakenteen määrittelyssä.

MÄÄRITELMÄ 1.6. Olkoon X joukko, jossa on määritelty ekvivalenssirelaatio $\sim$. Olkoon f lisäksi 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.

LAUSE 1.7 (Homomorfismin hajottaminen). *Olkoon f homomorfismi struktuurilta $(X, *)$ struktuuriin $(Y, \cdot)$, ja olkoon $\sim$ joukossa X määritelty laskutoimituksen kanssa yhteensopiva ekvivalenssirelaatio. Jos f on yhteensopiva ekvivalenssirelaation $\sim$ kanssa, niin on olemassa yksikäsitteinen homomorfismi $\overline{f} : X/\sim \to Y$, 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 on struktuurin Y neutraalialkio. Kuvauksen $\overline{f}$ yksikäsitteisyys seuraa suoraan siitä, että sen on toteutettava kaava $\overline{f}([x]) = f(x)$. □

HUOMAUTUS 1.8. 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 1.9. Jatketaan esimerkin 1.4 tarkastelua. Niin sanottu *inkluusiokuvaus* $\iota : (\mathbb{N}, +) \to (\mathbb{Z}, +)$, $\iota(n) = n$, 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 mahdotonta: kyseisen homomorfismin kuvassa voisi siis olla korkeintaan kaksi alkiota, mutta toisaalta sen pitäisi olla sama kuin $\operatorname{Im} \iota$, joka on ääretön.

Tarkastellaan sitten kuvausta $g : (\mathbb{N}, +) \to (\{1, -1\}, \cdot)$, $g(n) = (-1)^n$, joka on myös homomorfismi. Jos $n \sim n'$, 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 $\overline{g} : \mathbb{N}/\sim \to \{1, -1\}$, jolle pätee $[0] \mapsto 1$ ja $[1] \mapsto -1$. Tämä homomorfismi on itse asiassa ryhmäisomorfismi: surjektiivisuus seuraa g:n surjektiivisuudesta ja injektiivisyys esim. siitä, että lähtö- ja maalijoukko ovat samankokoisia.

1.3. Tekijäryhmät. Olkoon G multiplikatiivinen ryhmä. Tekijäryhmään liittyvä ekvivalenssirelaatio saadaan aina ns. normaalin aliryhmän avulla.

MÄÄRITELMÄ 1.10. 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 $H \trianglelefteq G$.

Algebra I:ssä on todistettu seuraava lause.

LAUSE 1.11 (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 $g \in gH$ kaikilla g, alkiot x ja x' kuuluvat samaan sivuluokkaan, jos ja vain jos $x \in x'H$. Kun aliryhmä on normaali, tämä relaatio on yhteensopiva laskutoimituksen kanssa, mikä seuraavassa todistetaan.

LAUSE 1.12. *Oletetaan, että $H \trianglelefteq G$. Tällöin ekvivalenssirelaatio*

$$x \sim x' \iff x \in x'H$$

on yhteensopiva laskutoimituksen kanssa.

TODISTUS. Olkoot $x, x', y, y' \in G$ sellaiset, että $x \in x'H$ ja $y \in y'H$. Erityisesti $x = x'h_1$ ja $y = y'h_2$ joillain $h_1, h_2 \in H$. Nyt $h_1y' \in Hy'$, ja koska H on normaali, $Hy' = y'H$. Täten $h_1y' = y'h_3$ jollain $h_3 \in H$. Lopulta saadaan

$$xy = x'h_1 \cdot y'h_2 = x'y' \cdot h_3h_2 \in (x'y')H,$$

eli $xy \sim x'y'$. □

Normaalin aliryhmän N suhteen voidaan siis muodostaa tekijäryhmä, jossa samastetaan samaan sivuluokkaan kuuluvat alkiot. Tätä tekijäryhmää merkitään G/N. Kääntäen, jokainen ryhmälaskutoimituksen kanssa yhteensopiva ekvivalenssirelaatio liittyy aina johonkin normaaliin aliryhmään.

LAUSE 1.13. *Oletetaan, että $\sim$ on ryhmässä G määritelty, laskutoimituksen kanssa yhteensopiva ekvivalenssirelaatio. Tällöin neutraalialkion luokka $N = [e]$ on normaali aliryhmä G:ssä, ja kaikilla $g, g' \in G$ pätee $g \sim g'$ jos ja vain jos $g' \in gN$.*

TODISTUS. Osoitetaan ensin, että N on aliryhmä. Selvästi $e \in N$. Olkoot sitten $g, h \in N$. Tällöin $g \sim e$ ja $h \sim e$, joten $gh \sim ee = e$, koska laskutoimitus on yhteensopiva relaation $\sim$ kanssa. Näin ollen $gh \in N$. Lisäksi

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

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

Olkoot sitten $g, g' \in G$ sellaiset, että $g \sim g'$. Tällöin $g^{-1}g' \sim g^{-1}g = e$, joten $g^{-1}g' \in N$. Näin ollen

$$g' = g \cdot \underbrace{g^{-1}g'}_{\in N} \in gN.$$

Toisaalta, jos $g' \in gN$, niin $g^{-1}g' \in N$, eli $g^{-1}g' \sim e$. Täten $g' = g \cdot g^{-1}g' \sim ge = g$.

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

Tästä eteenpäin oletetaan aina ryhmistä puhuttaessa, että tekijärakenteeseen liittyvä ekvivalenssirelaatio on muotoa $g \in g'N$.

Ryhmähomomorfismin hajotukselle saadaan seuraava ehto.

Lause 1.14. *Olkoon $f : G \to H$ ryhmähomomorfismi, ja olkoon $N \trianglelefteq G$. Tällöin on olemassa yksikäsitteinen homomorfismi $\overline{f} : G/N \to H$, jolle pätee $\overline{f}([g]) = f(g)$ kaikilla $g \in G$, jos ja vain jos $N \subset \operatorname{Ker} f$.*

Todistus. Oletetaan ensin, että $N \subset \operatorname{Ker} f$. Jos $g' \sim g$ eli $g' \in gN$, niin $g^{-1}g' \in N$. Oletuksen perusteella

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

joten $f(g) = f(g')$. Kuvauksen $\overline{f}$ olemassaolo seuraa nyt lauseesta 1.7.

Oletetaan sitten, että $N \not\subset \operatorname{Ker} f$. Tällöin löytyy jokin $h \in N$, jolle $f(h) \neq 1_H$. Toisaalta $[h] = [1_G]$ ja $f(1_G) = 1_H$, joten millään kuvauksella ei voi päteä $[g] \mapsto f(g)$ kaikilla $g \in G$. □

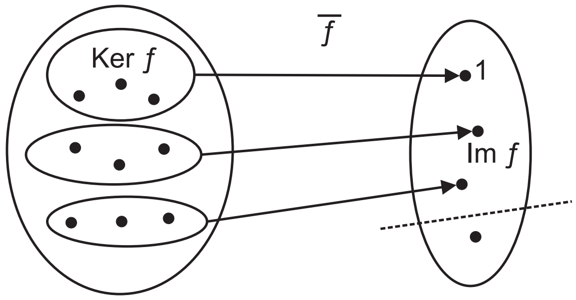
Tunnetusti ryhmähomomorfismin ydin on normaali aliryhmä. Yllä olevasta lauseesta saadaan siten erityistapauksessa $\operatorname{Ker} f = N$ tuttu homomorfialause.

Korollaari 1.15 (Ryhmien homomorfialause). *Olkoon $f : G \to H$ ryhmähomomorfismi. Tällöin ryhmät $G/\operatorname{Ker} f$ ja $\operatorname{Im} f$ ovat isomorfiset.*

$$\begin{tikzcd}
G \arrow[r, "f"] \arrow[d, "\pi"'] & H \\
G/\operatorname{Ker} f \arrow[r, dashed, "\cong"] & \operatorname{Im} f \arrow[u, hook, "\iota"']
\end{tikzcd}$$

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

Todistus. Lauseen nojalla löytyy homomorfismi $\overline{f} : G/\operatorname{Ker} f \to H$. Olkoon $g \in G$. Jos $g \not\sim 1_G$, niin $g \notin \operatorname{Ker} f$, joten $\overline{f}([g]) = f(g) \neq 1_H$. Näin ollen $\operatorname{Ker} \overline{f} = \{[1_G]\}$, mistä seuraa kuvauksen $\overline{f}$ injektiivisyys. Rajoittamalla maalijoukko aliryhmään $\operatorname{Im} f$, saadaan kuvauksesta $\overline{f}$ edelleen bijektiivinen homomorfismi $\tilde{f} : G/\operatorname{Ker} f \to \operatorname{Im} f$. □



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

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

MÄÄRITELMÄ 1.16. Renkaan $(R, +, \cdot)$ yhteenlaskuryhmän aliryhmää A kutsutaan *ideaaliksi*, jos kaikilla $r \in R$ ja $a \in A$ pätee

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

Ensimmäisen ehdon toteuttavia aliryhmiä kutsutaan *vasemmanpuoleisiksi* ideaaleiksi ja toisen ehdon toteuttavia *oikeanpuoleisiksi*.

HUOMAUTUS 1.17. Ideaalisuusehdot muuttuvat ymmärrettäviksi, kun pohditaan kysymystä: “Minkälainen luokka voidaan ottaa tekijärenkaan nolla-alkioksi?” Koska renkaassa pätee aina $r \cdot 0 = 0 \cdot r = 0$, täytyy tämän luokan myös toteuttaa $[r]A = A[r] = A$.

Ideaalin sivuluokat muodostavat osituksen.

LAUSE 1.18. *Olkoon A ideaali renkaassa R. Tällöin ekvivalenssirelaatio*

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

on yhteensopiva renkaan kertolaskun kanssa.

TODISTUS. Olkoot $x, x', y, y' \in R$ sellaiset, että $x \in x' + A$ ja $y \in y' + A$. Erityisesti $x = x' + a_1$ ja $y = y' + a_2$ joillain $a_1, a_2 \in A$. Koska A on ideaali, tulot $x'a_2$, a_1y' ja a_1a_2 sisältyvät A:han. Näin ollen

$$xy = (x' + a_1)(y' + a_2) = x'y' + \underbrace{x'a_2 + a_1y' + a_1a_2}_{\in A} \in x'y' + A,$$

joten $xy \sim x'y'$. □

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

LAUSE 1.19. *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 $r \in r' + A$.*

TODISTUS. Lauseesta 1.13 seuraa, että A on aliryhmä ja sen sivuluokat vastaavat täsmälleen relaation $\sim$ ekvivalenssiluokkia. Tarvitsee siis vain todistaa, että A on ideaali. Olkoot $r \in R$ ja $a \in A$ eli $a \sim 0$. Koska laskutoimitus on yhteensopiva relaation $\sim$ kanssa, niin

$$ra \sim r \cdot 0 = 0 \qquad \text{ja} \qquad ar \sim 0 \cdot r = 0.$$

Tämä tarkoittaa, että $r \in A$. □

Algebra I:ssä on osoitettu, että rengashomomorfismin ydin on aina ideaali. Seuraavien rengashomomorfismien hajotukseen liittyvien lauseiden todistukset sivuutetaan, koska ne ovat aivan samanlaiset kuin ryhmähomomorfismien tapauksessa.

LAUSE 1.20. *Olkoon* $f : R \to S$ *rengashomomorfismi, ja olkoon* A *renkaan* R *ideaali. Tällöin on olemassa yksikäsitteinen rengashomomorfismi* $\overline{f} : R/A \to S$, *jolle pätee* $\overline{f}([r]) = f(r)$ *kaikilla* $r \in R$, *jos ja vain jos* $A \subset \operatorname{Ker} f$.

KOROLLAARI 1.21 (Renkaiden homomorfialause). *Olkoon* $f : R \to S$ *rengashomomorfismi. Tällöin renkaat* $R/\operatorname{Ker} f$ *ja* $\operatorname{Im} f$ *ovat isomorfiset.*

Ryhmäteoriaa

2. Ryhmän toiminta

Permutaatiot kuvaavat jonkin perusjoukon alkioita toisikseen. Eräät permutaatiot jättävät joitain alkioita paikalleen, toiset liikuttavat kaikkia joukon alkioita. Kaikki permutaatiot muodostavat ryhmän, jossa neutraalialkiona on kaikki alkiot paikallaan pitävä identtinen permutaatio.

Ryhmän toiminta yleistää permutaation käsitettä. Kaikille ryhmän alkioille voidaan määritellä tapa, jolla niiden oletetaan vaikuttavan jonkin joukon alkioihin. Tämän tavan tulee olla sopusoinnussa ryhmän rakenteen kanssa; esimerkiksi neutraalialkion tulisi pitää kaikki alkiot paikallaan. Toimintojen avulla saadaan tietoa ryhmän rakenteesta ainakin kahdella tavalla. Ensinnäkin ryhmän toiminnan kautta voidaan saada ryhmälle esitys esimerkiksi vektoriavaruuden lineaarikuvauksina, jolloin ryhmää päästään tutkimaan helposti käsiteltävien matriisien avulla. Toisaalta ryhmällä voi olla erilaisia toimintoja myös itsessään, ja näiden toimintojen tutkiminen ratkaisee suoraan monia ryhmän rakenteeseen liittyviä kysymyksiä.

2.1. Toiminnan määritelmä. Oletetaan seuraavassa, että G on ryhmä ja X jokin joukko. Merkitään symbolilla X^X kaikkien kuvausten $X \to X$ joukkoa.

MÄÄRITELMÄ 2.1. Kuvausta $\varphi : G \to X^X$, $g \mapsto f_g$, nimitetään ryhmän G *vasemmanpuoleiseksi toiminnaksi joukossa* X, jos se toteuttaa seuraavat ehdot:

(T1) $f_e = \mathrm{id}_X$, missä e on neutraalialkio
(T2) $f_{gh} = f_g \circ f_h$ kaikilla $g, h \in G$.

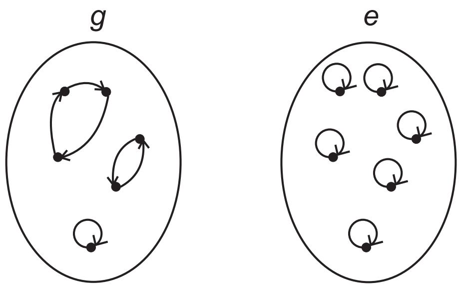
Vastaavasti voidaan määritellä *oikeanpuoleinen toiminta* korvaamalla jälkimmäinen ehto ehdolla (T2') $f_{gh} = f_h \circ f_g$.

Yllä oleva määritelmä soveltuu sellaisenaan myös monoidille. Käänteisalkioiden olemassaolosta kuitenkin seuraa, että $f_g \circ f_{g^{-1}} = f_{g \cdot g^{-1}} = f_e = \mathrm{id}$, joten jokainen f_g on kääntyvä. Jokainen ryhmän alkio vastaa siis jotain bijektiota $X \to X$, eli kuvauksen φ maalijoukko voidaan rajoittaa permutaatioryhmään $\mathrm{Sym}(X)$. Tällöin φ:stä tulee homomorfismi.

Yleensä on tapana merkitä vasemmanpuoleista toimintaa yksinkertaisemmin kertolaskun tapaan: $f_g(x) = gx$. (Joskus saatetaan käyttää selvyyden vuoksi merkintää $g.x$.) Tällöin vasemmanpuoleisen toiminnan ehdoiksi tulee

(T1) $ex = x$ kaikilla $x \in X$
(T2) $(gh)x = g(hx)$ kaikilla $g, h \in G$ ja $x \in X$.

Oikeanpuoleinen toiminta kirjoitetaan vastaavasti oikeanpuoleiseksi kertolaskuksi $f_g(x) = xg$. Tällöin $x(gh) = (xg)h$.



KUVA 3. Ryhmän alkiot vastaavat permutaatioita

Esimerkkejä toiminnoista:

- Joukon X permutaatioryhmä toimii joukossa X luonnollisella tavalla: $\sigma x = \sigma(x)$ kaikilla permutaatioilla σ.
- Vektoriavaruuden kerroinkunnan kertolaskuryhmä $(K^*, \cdot)$ toimii vektoriavaruudessa skaalarikertolaskulla.
- Kääntyvien $n \times n$-reaalimatriisien ryhmällä $GL_n(\mathbb{R})$ on matriisikertolaskun määrittelemä toiminta avaruudessa $\mathbb{R}^n$.
- Jos G on ryhmä, kaava $f_g : h \mapsto gh$ määrittelee G:n vasemmanpuoleisen toiminnan itsessään. Vastaavasti kaava $h \mapsto hg$ määrittelee oikeanpuoleisen toiminnan.
- Jos $H \leq G$, kaava $xH \mapsto (gx)H$ määrittelee G toiminnan H:n sivuluokkien joukossa.
- Jos G on ryhmä, kaava $f_g : h \mapsto ghg^{-1}$ määrittelee myös toiminnan joukossa G. Tätä toimintaa kutsutaan *konjugoinniksi*. Tällä toiminnalla on se ominaisuus, että jokainen f_g on homomorfismi.
- Jos $x \mapsto gx$ on jonkin ryhmän vasemmanpuoleinen toiminta, niin kaava $xg = g^{-1}x$ määrittelee erään oikeanpuoleisen toiminnan. Tämä seuraa siitä, että $x(gh) = (gh)^{-1}x = h^{-1}(g^{-1}x) = (xg)h$.

Joukkoa, jossa on määritelty ryhmän G toiminta, voidaan kutsua *G-joukoksi*. Kahden G-joukon välinen kuvaus $f : X \to Y$ on *G-morfismi*, jos

$$g.f(x) = f(g.x) \quad \text{kaikilla } g \in G \text{ ja } x \in X.$$

Esimerkiksi K-kertoimisten vektoriavaruuksien väliset lineaarikuvaukset ovat K^*-morfismeja.

2.2. Radat ja vakauttajat. Oletetaan, että on määritelty ryhmän G toiminta joukossa X. Osajoukkoa Y kutsutaan *vakaaksi*, jos $gy \in Y$ kaikilla $g \in G$ ja $y \in Y$. Jos osajoukko on vakaa, voidaan siinä määritellä G:n toiminta rajoittamalla alkuperäistä toimintaa. Minimaalisia vakaita osajoukkoja kutsutaan radoiksi.

MÄÄRITELMÄ 2.2. Alkion $x \in X$ *rata* on joukko

$$Gx = \{gx \mid g \in G\}.$$

Jos toimivia ryhmiä on useita, rataa voi kutsua täsmällisemmin *G-radaksi*.

Radat muodostavat joukon X osituksen; vastaava ekvivalenssirelaatio on

$$x \sim x' \iff x = gx' \quad \text{jollain } g \in G.$$

Jokainen ratojen yhdiste on vakaa osajoukko. Ratojen joukkoa merkitään X/G (tai joskus $G\backslash X$, jos halutaan tehdä ero vasemman- ja oikeanpuoleisten toimintojen välillä).

Mikä tahansa osajoukko saadaan vakaaksi, kun rajoitutaan tarkastelemaan sopivaa aliryhmää.

MÄÄRITELMÄ 2.3. Osajoukon $Y \subset X$ *vakauttaja* on

$$G_Y = \{g \in G \mid gy \in Y \text{ kaikilla } y \in Y\}.$$

Jos $Y = \{y\}$, merkitään myös $G_Y = G_y$ ja puhutaan alkion y *kiinnittäjästä.*

Alkioiden kiinnittäjät[5] ovat aina G:n aliryhmiä, mutteivät välttämättä normaaleja. Kiinnittäjä voi vakauttaa suurempiakin osajoukkoja: esimerkiksi ryhmän kertolaskutoiminta itsessään ($g.h = gh$) on sellainen, että jokaisen neutraalialkiosta poikkeavan alkion h kiinnittäjä on $G_h = \{e\}$, joka tietysti kiinnittää kaikki ryhmän alkiot.

Esimerkkejä:

- Vektoriavaruuden V skalaarikertolaskussa jokaisen nollasta poikkeavan vektorin rata on origon kautta kulkeva suora. Joukko $V \setminus \{\overline{0}\}$ on vakaa ryhmän K^* toiminnassa. Ositusta $P(V) = (V \setminus \{\overline{0}\})/K^*$ kutsutaan vektoriavaruuden V *projektiiviseksi avaruudeksi.*
- Ryhmän $GL_n(\mathbb{R})$ toiminnassa aliavaruuden $\langle v \rangle \subset \mathbb{R}^n$ (origon kautta kulkeva suora) vakauttaja on niiden matriisien joukko, joilla on ominaisvektorina v. Toisaalta esim. origokeskisen ympyrän vakauttaja on ns. *ortogonaalinen ryhmä* $O_n(\mathbb{R})$. Tähän aliryhmään kuuluvat ne matriisit, joiden sarakkeet muodostavat ortonormaalin vektorijoukon.
- Ajatellaan ryhmän $GL_2(\mathbb{R})$ toimintaa tasossa. Origokeskisen tasasivuisen kolmion vakauttaja on kolmion *symmetriaryhmä.* Voidaan osoittaa, että tämä on isomorfinen ryhmän S_3 kanssa. Tällä tavoin saadaan ryhmän S_3 esitys tason lineaarikuvauksina.
- Merkitään $N_n = \{1, 2, \ldots, n\}$. Määritellään permutaatioryhmän S_n toiminta pareilla $\{a, b\}$, missä $a \neq b$, seuraavasti: $\sigma\{a, b\} = \{\sigma a, \sigma b\}$. Jos parien joukko E tulkitaan jonkin verkon särmiksi, niin E:n vakauttaja on kyseisen verkon automorfismiryhmä.

Kiinnittäjän G_x alkiot pitävät x:n paikallaan, ja kukin kiinnittäjän sivuluokka vastaa jotain alkiota x:n radalla. Tämä todistetaan seuraavassa.

LAUSE 2.4 (Rata-vakauttajalause). *Olkoon X jokin G-joukko, ja $x \in X$. Tällöin on olemassa bijektio $f : G/G_x \to Gx$, jolle pätee $gG_x \mapsto gx$.*

TODISTUS. Osoitetaan ensin, että mainittu f on hyvin määritelty. Jos g ja g' ovat samassa sivuluokassa, niin $g = g'h$ jollain $h \in G_x$. Alkio h kiinnittää

[5] Yleisen osajoukon kiinnittäjä on alimonoidi, muttei välttämättä aliryhmä, ellei osajoukko tai kiinnittäjä itse ole äärellinen.

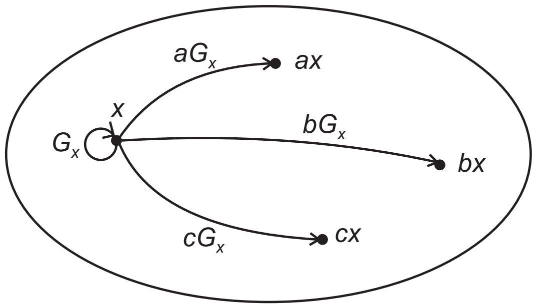
x:n, joten $gx = g'(hx) = g'x$. Siispä voidaan määritellä kuvaus $f : gG_x \mapsto gx$. Selvästikin f on surjektio radalle Gx.

Osoitetaan vielä, että f on injektio. Jos $gx = hx$ joillain $g, h \in G$, niin

$$h^{-1}gx = h^{-1}hx = ex = x,$$

eli alkio $h^{-1}g$ kiinnittää x:n. Näin ollen $h^{-1}g \in G_x$, mistä seuraa, että g ja h kuuluvat samaan kiinnittäjän sivuluokkaan. □

Huomautus 2.5. Jos määritellään G:n luonnollinen toiminta $g.hG_x = (gh)G_x$ kiinnittäjän G_x sivuluokkien joukossa, voidaan osoittaa, että edellisen lauseen bijektio f on itse asiassa G-joukkojen isomorfismi.



Kuva 4. Kiinnittäjän sivuluokat vastaavat yksi yhteen radan alkioita

Määritelmä 2.6. Ryhmän G toimintaa joukossa X sanotaan *transitiiviseksi*, jos kaikilla $x, y \in X$ löytyy jokin $g \in G$, jolle $gx = y$. Tällöin sanotaan myös, että G-joukko X on *homogeeninen*.

Jokainen rata on homogeeninen joukko. Toisaalta ryhmä toimii transitiivisesti, jos ja vain jos joukko X on jokaisen alkionsa rata. Transitiivisen toiminnan tapauksessa rata-vakauttajalauseesta saadaan hyödyllinen seuraus.

Lause 2.7. *Oletetaan, että ryhmä G toimii transitiivisesti joukossa X. Olkoon H jonkin alkion kiinnittäjä. Tällöin*[6]

$$|X| = [G : H].$$

Todistus. Merkitään H:n kiinnittämää alkiota x. Rata-vakauttajalauseesta 2.4 saadaan bijektio $Gx \to G/H$. Koska toiminta on transitiivista, pätee $Gx = X$, josta väite seuraa. □

Korollaari 2.8. *Oletetaan, että G toimii joukossa X (ei välttämättä transitiivisesti). Olkoon T kaikkien G-ratojen* edustajisto, *eli joukko, joka sisältää jokaisesta radasta täsmälleen yhden alkion. Tällöin pätee*

$$|X| = \sum_{x \in T} [G : G_x].$$

[6]Aliryhmän indeksi on määritelty vain äärellisessä tapauksessa. Lauseen todistus kuitenkin toimii sellaisenaan myös äärettömillä mahtavuuksilla.

TODISTUS. Jokainen rata Gx on homogeeninen joukko, joten edellisen lauseen mukaan $|Gx| = [G : G_x]$. Tulos seuraa siitä, että radat muodostavat joukon X osituksen. $\square$

ESIMERKKI 2.9. Ryhmät S_3 ja S_2 toimivat luonnollisesti joukoissa $\{1,2,3\}$ ja $\{1,2\}$. Näiden toimintojen avulla voidaan tuloryhmälle $S_3 \times S_2$ määritellä toiminta joukossa $N_5 = \{1,2,3,4,5\}$ seuraavasti:

$$(\sigma_1, \sigma_2)n = \begin{cases} \sigma_1(n), & \text{jos } n \in \{1,2,3\}, \\ \sigma_2(n-3)+3, & \text{jos } n \in \{4,5\}. \end{cases}$$

Ryhmän S_3 alkiot siis toimivat tavalliseen tapaan joukossa $\{1,2,3\}$, ja ryhmän S_2 ainoa 2-sykli (12) vaihtaa alkiot 4 ja 5 keskenään. Tämä toiminta ei ole transitiivista: alkion 1 rata on joukko $\{1,2,3\}$, ja alkion 4 rata on joukko $\{4,5\}$.

Alkion 1 kiinnittäjä on aliryhmä

$$G_1 = \{(\mathrm{id}, \mathrm{id}),\ (\mathrm{id}, (12)),\ ((23), \mathrm{id}),\ ((23), (12))\},$$

joka on isomorfinen Kleinin neliryhmän kanssa. Sen kolme sivuluokkaa ovat G_1, $((12), \mathrm{id})G_1$ ja $((132), \mathrm{id})G_1$, jotka vastaavat radan alkioita 1, 2 ja 3.

Koska jokainen muotoa $(\sigma, (12))$ oleva pari liikuttaa alkiota 4, tämän alkion kiinnittäjä G_4 sisältyy aliryhmään $S_3 \times \{\mathrm{id}\}$. Toisaalta edellisen lauseen mukaan

$$|N_5| = [G : G_1] + [G : G_4] = 12/4 + 12/|G_4| = 3 + 12/|G_4|,$$

joten kiinnittäjässä G_4 on kuusi alkiota. Siispä $G_4 = S_3 \times \{\mathrm{id}\}$.

2.3. Konjugointi. Ryhmässä G voidaan määritellä G:n konjugointitoiminta $f_g : h \mapsto ghg^{-1}$. Koska jokainen kuvaus f_g on homomorfismi, aliryhmät kuvautuvat konjugoitaessa aliryhmiksi. Näin ollen konjugointitoiminta voidaan määritellä myös ryhmän aliryhmien joukossa. Molemmissa tapauksissa alkion kuvia toiminnassa nimitetään sen *konjugaateiksi*. Konjugaatit ovat siis joko muotoa ${}^g h = ghg^{-1}$ (alkioiden konjugointi) tai ${}^g H = gHg^{-1}$ (aliryhmien konjugointi).

Jos G toimii konjugoimalla itsessään, ratoja kutsutaan *konjugaattiluokiksi* ja alkioiden kiinnittäjiä *keskittäjiksi*. Alkion x konjugaattiluokkaa merkitään ${}^G x$. Kaksi alkiota kuuluvat samaan konjugaattiluokkaan, jos ne ovat toistensa konjugaatteja. Neutraalialkio muodostaa aina oman konjugaattiluokkansa. Seuraava tulos kertoo konjugaattiluokkien tärkeydestä; todistus jätetään harjoitustehtäväksi.

LAUSE 2.10. *Jokainen normaali aliryhmä on konjugaattiluokkien yhdiste.*

Alkion x keskittäjää ryhmässä G merkitään

$$C_G(x) = \{g \in G \mid gxg^{-1} = x\}.$$

Konjugointitoiminnan symmetrian vuoksi $g \in C_G(h)$ jos ja vain jos $h \in C_G(g)$. Koska

$$C_G(x) = \{g \in G \mid gx = xg\},$$

alkion x keskittäjää voidaan luonnehtia myös niin, että se koostuu täsmälleen niistä alkioista, jotka kommutoivat x:n kanssa. Keskittäjien leikkausta

$$Z(G) = \bigcap_{x \in G} C_G(x) = \{g \in G \mid gxg^{-1} \text{ kaikilla } x \in G\}$$

nimitetään *keskukseksi.* Keskuksen alkiot kommutoivat kaikkien ryhmän alkioiden kanssa, niillä konjugoiminen pitää kaikki alkiot paikallaan, eivätkä ne itse liiku mihinkään muilla alkioilla konjugoitaessa. Tästä seuraa muun muassa, että $Z(G)$ on ryhmän G normaali aliryhmä.

Jos G toimii konjugoimalla omien aliryhmiensä joukossa, ratoja kutsutaan edelleen (aliryhmien) *konjugaattiluokiksi.* Aliryhmien kiinnittäjiä sen sijaan *normalisoijiksi*, ja merkitään

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\} = \{g \in G \mid gH = Hg\}.$$

Nimitys selviää määritelmästä: Jos g on normalisoijan alkio, niin g:hen liittyvät vasen ja oikea H:n sivuluokka yhtyvät. Tästä saadaan normalisoijalle luonnehdinta, jonka mukaan aliryhmän H normalisoija on *suurin aliryhmä, jossa H on normaali.* Esimerkiksi $N_G(H) = G$ täsmälleen silloin, kun $H \trianglelefteq G$.

Edellä todistetuista lauseista 2.7 ja 2.8 saadaan nyt seuraavat versiot.

LAUSE 2.11. *Alkion x konjugaattiluokan koko on*

$$\left|{}^{G}x\right| = [G : C_G(x)].$$

LAUSE 2.12 (Luokkayhtälö). *Olkoon C jokin ryhmän G konjugaattiluokkien edustajisto. Tällöin*

$$|G| = \sum_{x \in C} [G : C_G(x)].$$

3. Symmetriaryhmiä

Symmetrioita käytetään usein helpottamaan monimutkaiseen struktuuriin liittyviä ongelmia. Symmetriaryhmät koostuvat permutaatioista, jotka säilyttävät jonkin tietyn rakenteen. Tällainen yleinen määritelmä voi oikeastaan kuvata mitä tahansa ryhmää (kaikki ryhmät ovat isomorfisia jonkin permutaatioryhmän kanssa), ja joskus sanotaankin, että ryhmäteoria on nimenomaan symmetrioiden tutkimista. Lisäksi se, mitä rakennetta symmetrioiden sallitaan muuttaa, vaihtelee hyvin paljon. Esimerkiksi neliön symmetriaryhmään lasketaan sellaisetkin permutaatiot, jotka peilaavat neliön jonkin lävistäjän suhteen, vaikka tällaista muunnosta varten neliö täytyy "nostaa tasosta irti" ja kääntää ympäri.[7] Sen sijaan kuution symmetriaryhmään ei lasketa muita kuin kolmiulotteisessa avaruudessa tapahtuvia kiertoja; kuutiota ei saa peilata poikkileikkaavan tason suhteen, niin että etusivu ja takasivu vaihtuisivat päittäin.

Tässä luvussa tarkastellaan esimerkinomaisesti, mitä symmetrioista saadaan tietää ja mihin niitä voidaan käyttää. Koska symmetriat ovat permutaatioita, aloitetaan tutustumalla tarkemmin permutaatioihin.

3.1. Symmetriset ryhmät ja permutaation etumerkki. Merkitään n ensimmäisen positiivisen kokonaisluvun joukkoa $N_n = \{1, 2, \dots, n\}$. *Symmetrinen ryhmä* S_n on tämän joukon kaikkien permutaatioiden muodostama ryhmä. Sopivalla alkioiden numeroinnilla voidaan määritellä ryhmän S_n luonnollinen toiminta missä tahansa äärellisessä joukossa $X = \{x_1, \dots, x_n\}$ kaavalla $\sigma x_n = x_{\sigma(n)}$.

Symmetrisen ryhmän alkioita on yleensä kätevintä merkitä syklien avulla. Jos $a_1, \dots, a_m$ ovat joukon N_n eri alkioita, niin *m-sykli* $\rho = \begin{pmatrix} a_1 & \dots & a_m \end{pmatrix}$ on sellainen permutaatio, että

$$\rho(a_i) = \begin{cases} a_{i+1}, & \text{jos } i < m, \\ a_1, & \text{jos } i = m. \end{cases}$$

Muut alkiot ρ pitää paikallaan. On helppo nähdä, että jokainen permutaatio voidaan kirjoittaa erillisten syklien tulona, esimerkiksi

$$S_6 \ni \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 6 & 4 & 5 \end{pmatrix} = (12)(3)(465).$$

Tämä esitys on syklien järjestystä sekä kirjoitusasua vaille yksikäsitteinen, esimerkiksi $(123)(45) = (54)(231)$. Usein yhden alkion syklit jätetään merkitsemättä.

Kahden alkion syklejä nimitetään *vaihdoiksi* tai *transpositioiksi*. Jokainen sykli voidaan kirjoittaa vaihtojen tulona, sillä

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_m \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \end{pmatrix} \begin{pmatrix} a_2 & a_3 \end{pmatrix} \cdots \begin{pmatrix} a_{m-1} & a_m \end{pmatrix}.$$

Tästä seuraa, että mielivaltainen permutaatio voidaan kirjoittaa vaihtojen tulona. Tällainen esitys ei ole millään muotoa yksikäsitteinen, mutta osoittautuu, että saman permutaation esityksessä vaihtojen lukumäärä on aina joko parillinen tai pariton. Tämän osoittamiseksi määritellään ensin permutaation etumerkki.

[7] Tarkemmin sanoen, jos L on peilaus, ei ole olemassa jatkuvasti parametrisoitua tason etäisyydet säilyttävien lineaarikuvausten perhettä (A_t), missä $t \in [0, 1]$ ja $A_0 = \mathrm{id}$, $A_1 = L$. Tämä johtuu siitä, että peilauksen determinantti on -1.

Määritelmä 3.1. Oletetaan, että permutaation $\sigma \in S_n$ esityksessä erillisten syklien tulona on t sykliä (1-syklit mukaanluettuina). Tällöin permutaation σ *etumerkki* on

$$\operatorname{sgn}(\sigma) = (-1)^{n-t}.$$

Määritelmän perusteella esimerkiksi m-syklin etumerkki on 1, jos ja vain jos m on pariton. Vaihdon etumerkki on siis -1. Osoitetaan seuraavaksi, että etumerkkikuvaus on ryhmähomomorfismi.

Lemma 3.2. *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). Jos a ja b esiintyvät samassa syklissä, esim. $\rho_1 = \begin{pmatrix} a & c_1 & \dots & c_k & b & d_1 & \dots & d_l \end{pmatrix}$, niin

$$\tau\rho_1 = \begin{pmatrix} a & c_1 & \dots & c_k \end{pmatrix} \begin{pmatrix} b & d_1 & \dots & d_l \end{pmatrix}.$$

Tässä tapauksessa permutaatiolla $\tau\beta$ on sykliesitys $(\tau\rho_1)\rho_2 \cdots \rho_t$, jossa on yhteensä $t+1$ sykliä. Etumerkin määritelmän mukaan $\operatorname{sgn}(\tau\beta) = (-1)^{n-(t+1)} = -\operatorname{sgn}(\beta)$. Toisaalta, jos a ja b esiintyvät eri sykleissä, esim. $\rho_1 = \begin{pmatrix} a & c_1 & \dots & c_k \end{pmatrix}$ ja $\rho_2 = \begin{pmatrix} b & d_1 & \dots & d_l \end{pmatrix}$, niin

$$\tau\rho_1\rho_2 = \begin{pmatrix} a & c_1 & \dots & c_k & b & d_1 & \dots & d_l \end{pmatrix}.$$

Tällöin permutaation $\tau\beta$ sykliesityksessä on yksi sykli vähemmän kuin β:n esityksessä, joten $\operatorname{sgn}(\tau\beta) = (-1)^{n-(t-1)} = -\operatorname{sgn}(\beta)$. □

Lause 3.3. *Kaikilla $\alpha, \beta \in S_n$ pätee*

$$\operatorname{sgn}(\alpha\beta) = \operatorname{sgn}(\alpha)\operatorname{sgn}(\beta),$$

eli kuvaus $\operatorname{sgn} : S_n \to (\{1,-1\}, \cdot)$ *on ryhmähomomorfismi.*

Todistus. Oletetaan, että α voidaan kirjoittaa vaihtojen tulona $\tau_1 \cdots \tau_m$, missä m on pienin mahdollinen. Käytetään induktiota tulon pituuden m suhteen. Jos $m = 1$, niin α on itse vaihto, jolloin tulos seuraa edellisestä lemmasta. Oletetaan sitten, että $m > 1$ ja väite pätee kaikilla m:ää pienemmillä luvuilla. Nyt $\tau_2 \cdots \tau_m$ on erään permutaation minimaalinen esitys vaihtojen tulona. Jos nimittäin $\tau_2 \cdots \tau_m = \sigma_1 \cdots \sigma_r$, missä $r < m-1$, niin $\alpha = \tau_1\sigma_1 \cdots \sigma_r$, mikä on ristiriidassa luvun m minimaalisuuden kanssa. Näin ollen edellisestä lemmasta ja induktio-oletuksesta seuraa

$$\begin{aligned}
\operatorname{sgn}(\alpha\beta) &= \operatorname{sgn}(\tau_1 \cdots \tau_m\beta) = -\operatorname{sgn}(\tau_2 \cdots \tau_m\beta) \\
&\overset{\text{i.o.}}{=} -\operatorname{sgn}(\tau_2 \cdots \tau_m)\operatorname{sgn}(\beta) \\
&= \operatorname{sgn}(\tau_1 \cdots \tau_m)\operatorname{sgn}(\beta) \\
&= \operatorname{sgn}(\alpha)\operatorname{sgn}(\beta).
\end{aligned}$$

Tämä todistaa induktioaskeleen. □

Yllä olevan lauseen mukaan permutaation etumerkki voidaan selvittää kirjoittamalla permutaatio vaihtojen tulona: etumerkki on 1, jos ja vain jos vaihtojen lukumäärä on parillinen, sillä $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\tau_1) \cdots \operatorname{sgn}(\tau_m) = (-1)^m$. Tällöin permutaatiota kutsutaan *parilliseksi*, muuten *parittomaksi*. Parilliset permutaatiot muodostavat tärkeän normaalin aliryhmän.

MÄÄRITELMÄ 3.4. Etumerkkihomomorfismin ydintä

$$\operatorname{Ker}(\operatorname{sgn}) = \{\sigma \in S_n \mid \sigma \text{ on parillinen}\}$$

kutsutaan *alternoivaksi ryhmäksi* ja merkitään A_n.

LAUSE 3.5. *Jos $n \geq 2$, niin $[S_n : A_n] = 2$.*

TODISTUS. Koska $n \geq 2$, niin vaihto (12) kuuluu ryhmään S_n. Täten sgn on surjektio kahden alkion joukolle $\{1, -1\}$. Homomorfialauseen nojalla löytyy bijektio $S_n/A_n \to \{1, -1\}$. □

3.2. Konjugointi symmetrisessä ryhmässä. Symmetrisessä ryhmässä alkion konjugaatit löydetään helpoiten sykliesityksen avulla. Konjugointi yksinkertaisesti permutoi sykliesityksen symboleja.

LAUSE 3.6. *Olkoot $\sigma, \tau \in S_n$. Oletetaan, että τ:n esitys erillisten syklien tulona on*

$$\tau = \begin{pmatrix} a_{1,1} & \dots & a_{1,k_1} \end{pmatrix} \cdots \begin{pmatrix} a_{m,1} & \dots & a_{m,k_m} \end{pmatrix}.$$

Merkitään $\sigma(a_{i,j}) = a'_{i,j}$ kaikilla i ja j. Tällöin τ:n konjugaatille pätee

$$^{\sigma}\tau = \begin{pmatrix} a'_{1,1} & \dots & a'_{1,k_1} \end{pmatrix} \cdots \begin{pmatrix} a'_{m,1} & \dots & a'_{m,k_m} \end{pmatrix}.$$

TODISTUS. Merkitään väitteessä esiintyvää tuloa

$$\tau' = \begin{pmatrix} a'_{1,1} & \dots & a'_{1,k_1} \end{pmatrix} \cdots \begin{pmatrix} a'_{m,1} & \dots & a'_{m,k_m} \end{pmatrix}$$

ja osoitetaan, että $\sigma\tau\sigma^{-1} = \tau'$. Olkoon sitä varten $b \in N_n$ mielivaltainen. Koska σ on bijektio, löydetään jokin $a \in N_n$, jolle $b = a'$. Jos τ pitää a:n paikallaan, niin τ' pitää puolestaan b:n paikallaan. Tällöin $\sigma\tau\sigma^{-1}(b) = \sigma\tau(a) = \sigma(a) = b = \tau'(b)$.

Oletetaan sitten, että a esiintyy jossain syklissä, jonka pituus on suurempi kuin 1. Järjestelemällä syklejä tarvittaessa uudestaan, voidaan valita, että $a = a_{1,1}$. Tällöin pätee

$$\tau\sigma^{-1}(b) = \tau(a) = \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,k_1} \end{pmatrix} . a_{1,1} = a_{1,2}.$$

Lisäksi nähdään, että $b = a'_{1,1}$, joten

$$\tau'(b) = \begin{pmatrix} a'_{1,1} & a'_{1,2} & \dots & a'_{1,k_1} \end{pmatrix} . a'_{1,1} = a'_{1,2} = \sigma(a_{1,2}).$$

Saatiin, että mielivaltaisella alkiolla $b \in N_n$ pätee $\tau'(b) = \sigma(a_{1,2}) = \sigma\tau\sigma^{-1}(b)$. Siispä väite on todistettu. □

Symmetrisessä ryhmässä samaan konjugaattiluokkaan kuuluvat siis täsmälleen ne alkiot, joilla on sama *syklityyppi*, eli joiden sykliesityksessä on sama lukumäärä samanpituisia syklejä. Syklityyppiä voidaan merkitä jonolla $(t_1, t_2, \dots, t_m)$, missä $t_1 \geq t_2 \geq \cdots t_m$ ja $\sum_i t_i = n$. Tällaista jonoa nimitetään luvun n ositukseksi. Esimerkiksi permutaation $(12)(345)(6)$ syklityyppi on $(3, 2, 1)$.

ESIMERKKI 3.7. Tarkastellaan ryhmää S_3, joka koostuu 1-, 2- ja 3-sykleistä. Sen konjugaattiluokat ovat

$$C_1 = \{\mathrm{id}\}, \quad C_2 = \{(12), (23), (13)\} \quad \text{ja} \quad C_3 = \{(123), (132)\}.$$

Ainoastaan konjugaattiluokkien yhdiste voi olla normaali aliryhmä. Toisaalta aliryhmän täytyy aina sisältää neutraalialkio, joten epätriviaaleja normaaleja aliryhmiä voivat olla ainoastaan yhdisteet $C_1 \cup C_2$ ja $C_1 \cup C_3$. Ensimmäisessä on 4 alkiota, joten se ei voi olla aliryhmä, koska $4 \nmid 6$. Jälkimmäinen yhdiste on alternoiva ryhmä A_3, joka on tunnetusti normaali aliryhmä.

Alternoivassa ryhmässä tilanne on monimutkaisempi. Esimerkiksi A_3 on vaihdannainen, mistä seuraa, että sen jokainen konjugaattiluokka on yksiö. Edellisen esimerkin luokka $C_3 \subset A_3$ siis jakautuu A_3:n toiminnassa kahdeksi eri luokaksi. Tämä johtuu siitä, että ainoa alkio, joka konjugoisi alkion (123) alkiolle (132), sattuu olemaan transpositio. Seuraavan lauseen avulla voidaan päätellä, milloin jokin konjugaattiluokka jakautuu siirryttäessä alternoivaan ryhmään. Oletetaan, että alkiolla $\sigma \in S_n$ on esitys $\rho_1 \cdots \rho_m$ erillisten syklien tulona, ja että syklit on järjestetty pituuden mukaan laskevaan järjestykseen.

Lause 3.8. *Olkoon K_S alkion σ konjugaattiluokka ryhmässä S_n ja vastaavasti K_A saman alkion konjugaattiluokka ryhmässä A_n. Nyt $K_S \neq K_A$, jos ja vain jos*

$$(*) \qquad \textit{syklien } \rho_i \textit{ pituudet ovat parittomia ja erillisiä.}$$

Tällöin $|K_A| = \frac{1}{2}|K_S|$.

Todistus. Tarkastellaan alkion σ keskittäjiä. Merkitään $C_S = C_{S_n}(\sigma)$ ja $C_A = C_{A_n}(\sigma) = C_S \cap A_n$. Koska $C_A \leq C_S$, löytyy Lagrangen lauseen jokin positiivinen kokonaisluku k, jolle $k \cdot |C_A| = |C_S|$. Lauseen 2.11 mukaan taas

$$n! = |C_S| \cdot |K_S| \qquad \text{ja} \qquad \frac{n!}{2} = |C_A| \cdot |K_A|.$$

Näistä yhtälöistä voidaan lopulta päätellä, että $|K_A| = k/2 \cdot |K_S|$. Toisaalta, koska $K_A \subset K_S$, niin k on joko 1 tai 2.

Tarvitsee siis vain todistaa, että ehto $(*)$ pätee, jos ja vain jos $C_A = C_S$. Oletetaan, että $\alpha \in C_S$. Lauseen 3.6 perusteella jokaisella i löytyy jokin sellainen j, että ${}^{\alpha}\rho_i = \rho_j$. Jos ehto $(*)$ pätee, täytyy olla $i = j$, koska syklit ovat eri pituisia ja ne on järjestetty pituuden mukaan. Tällöin $\alpha = \rho_i^k$ jollain k. Koska syklin ρ_i pituus on pariton, sen etumerkki on 1. Edelleen $\operatorname{sgn}(\alpha) = 1$, joten $\alpha \in C_A$.

Oletetaan sitten, että ehto $(*)$ ei päde. Tällöin voidaan löytää sellainen $\alpha \in C_S$, että $\operatorname{sgn}(\alpha) = -1$ (harjoitustehtävä). Näin ollen $C_S \neq C_A$, ja väite on todistettu. □

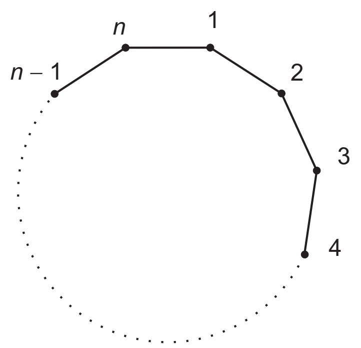
3.3. Diedriryhmät. Tarkastellaan joukosta $N_n = \{1, 2, \ldots, n\}$ muodostettujen järjestämättömien parien joukkoa

$$X = \{\{a, b\} \mid a, b \in N_n,\ a \neq b\}.$$

Määritellään tässä joukossa ryhmän S_n toiminta kaavalla $\sigma.\{a, b\} = \{\sigma(a), \sigma(b)\}$. Joukon X osajoukkoja voidaan ajatella *verkkoina*, joissa solmuina ovat joukon N_n alkiot ja särminä parit $\{a, b\}$. Verkkoa

$$E_n = \{\{1, 2\},\ \{2, 3\},\ \ldots,\ \{n-1, n\},\ \{n, 1\}\}.$$

nimitetään *monikulmioksi.*



KUVA 5. Monikulmio E_n

Etsitään monikulmion E_n vakauttaja G. Tämä koostuu kaikista mahdollisista verkon solmujen permutaatioista, jotka säilyttävät särmärakenteen, joten se on monikulmion symmetriaryhmä. Vakauttaja G toimii nyt vakauttamassaan monikulmiossa samalla tavalla kuin S_n.

Särmän $\{1, n\}$ kiinnittäjä aliryhmän G toiminnassa sisältää kaksi permutaatiota: identtisen kuvauksen ja *peilauksen*

$$\sigma = \begin{pmatrix}1 & n\end{pmatrix}\begin{pmatrix}2 & n-1\end{pmatrix}\dots\begin{pmatrix}k & n-k\end{pmatrix},$$

missä $k = [n/2]$ (kokonaisosa). Toiminta on selvästi transitiivista, joten lauseen 2.7 perusteella $|G| = |G_{\{1,n\}}||E_n| = 2n$. Etsitään nuo $2n$ symmetriaryhmän alkiota. Sykli $\rho = (1\ 2\ \dots\ n)$ eli *kierto* on vakauttajassa G, ja sen potensseista saadaan jo n alkiota. Koska mikään kierron positiivinen potenssi ei kiinnitä särmiä, σ ei kuulu aliryhmään $\langle\rho\rangle$, ja täten kyseinen aliryhmä ja sen sivuluokka $\sigma\langle\rho\rangle$ ovat erillisiä. Näistä saadaan jo yhteensä $2n$ alkiota, joten jokainen symmetriaryhmän alkio on joko muotoa ρ^j tai $\sigma\rho^j$ jollain $j \in \{0, 1, \dots, n-1\}$.

MÄÄRITELMÄ 3.9. *Diedriryhmä*[8] D_{2n} on monikulmion E_n vakauttaja.

Edellä todettiin, että alkiot ρ ja σ virittävät diedriryhmän, ja jokainen diedriryhmän alkio voidaan kirjoittaa muodossa ρ^j tai $\sigma\rho^j$. Suoraviivaisella laskulla nähdään, että

$$^{\sigma}\rho = \begin{pmatrix}n & n-1 & \dots & 2 & 1\end{pmatrix} = \rho^{-1},$$

josta sitten seuraa, että $^{\sigma}(\rho^j) = \rho^{-j}$. Erityisesti $\rho\sigma = \sigma\rho^{-1}$. Tämän tiedon avulla voidaan rekonstruoida koko ryhmän laskutoimitustaulu, mikä johtaa seuraavaan havaintoon.

LAUSE 3.10. *Jos ryhmän G virittää kaksi alkiota r ja s, joille pätee*

$$r^n = 1, \qquad s^2 = 1 \qquad \text{ja} \qquad srs = r^{-1},$$

niin $G \cong D_{2n}$.

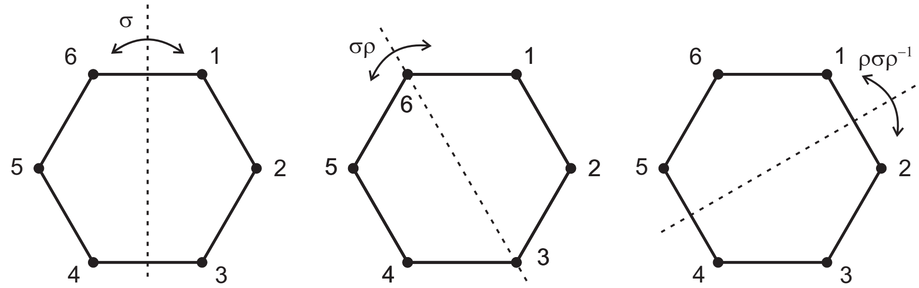
Diedriryhmässä $(\sigma\rho)^2 = \sigma\rho\sigma\rho = \rho^{-1}\rho = \mathrm{id}$, ja toisaalta $\sigma \cdot \sigma\rho = \rho$. Näin ollen diedriryhmän virittää kaksi *involuutiota* eli kertalukua kaksi olevaa alkiota, joiden tulon kertaluku on n. Osoittautuu, että myös tämä ominaisuus karakterisoi diedriryhmän täydellisesti. Seuraavan lauseen todistus sivuutetaan (ks. esim. Rotman: An Introduction to the Theory of Groups).

[8] diedri = kaksitahokas (kr.)

LAUSE 3.11. *Jos ryhmän G virittää kaksi alkiota a ja b, joille pätee*

$$a^2 = 1, \qquad b^2 = 1 \qquad ja \qquad (ab)^n = 1,$$

niin $G \cong D_{2n}$.



KUVA 6. Peilauksia eräässä diedriryhmässä. Huomaa, että peilauksen konjugaatille pätee $\rho\sigma\rho^{-1} = \sigma\rho^{-1}\rho^{-1} = \sigma\rho^{-2}$.

Diedriryhmät ovat säännöllisten monikulmioiden symmetriaryhmiä. Kiinnittämällä säännöllinen monikulmio keskipisteestään tason origoon ja valitsemalla sopivat lineaarikuvaukset kuvaamaan kiertoa ja peilausta, voidaan helposti näyttää, että diedriryhmä on isomorfinen erään äärellisen lineaarikuvausryhmän kanssa. Koska $D_6 = S_3$ (niissä on yhtä monta alkiota), tällä tavoin saadaan jo aiemmin mainittu ryhmän S_3 esitys tason lineaarikuvausten joukkona. Voidaan osoittaa, että sellaisia äärellisiä tason lineaarikuvausten ryhmän aliryhmiä, jotka säilyttävät pisteiden väliset etäisyydet, ovat ainoastaan sykliset ryhmät C_n ja diedriryhmät D_{2n}.

3.4. "Burnsiden" kaava. Esimerkkinä symmetriaryhmien sovelluksista esitetään seuraavassa niin sanottu Burnsiden lemma. William Burnside (1852–1927) oli huomattava brittimatemaatikko, joka loi perustan ryhmäteorian tutkimukselle Englannissa. Hän todisti lukuisia keskeisiä ryhmäteorian lauseita, mutta Burnsiden lemmaksi nimitettävä lause ei itse asiassa kuulu niihin. Burnside esittää kyseisen lemman kirjassaan "The Theory of Groups of Finite Order" mainiten sen löytäjäksi saksalaisen Ferdinand Frobeniuksen, mutta myöhemmistä painoksista lähdeviite on jostain syystä poistettu. Traditioon on sittemmin iskostunut viitata tulokseen Burnsiden lemmana, mutta erityisesti ryhmäteoreetikot tapaavat vitsailla aiheesta kutsuen lausetta "Ei-Burnsiden lemmaksi".

MÄÄRITELMÄ 3.12. Oletetaan, että G toimii joukossa X. Alkion $g \in G$ *kiintopistejoukko* on

$$\mathrm{Fix}(g) = \{x \in X \mid gx = x\}.$$

LAUSE 3.13 (Ratojenlaskentalause eli Burnsiden lemma). *Oletetaan, että G toimii äärellisessä joukossa G. Tällöin*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |\,\mathrm{Fix}(g)|.$$

Todistus. Se lukumäärä, kuinka monta kertaa jokin tietty $x \in X$ luetellaan summassa $\sum_g |\operatorname{Fix}(g)|$, on täsmälleen $|G_x|$, sillä x on kiintopistejoukossa $\operatorname{Fix}(g)$ jos ja vain jos $g \in G_x$. Täten

$$\sum_{g \in G} |\operatorname{Fix}(g)| = \sum_{x \in X} |G_x|,$$

ja rata-vakauttajalauseen seurauslauseen 2.7 perusteella

$$\sum_{x \in X} |G_x| = |G| \sum_{x \in X} \frac{1}{|Gx|}.$$

Oikeanpuoleisessa summassa tietty termi $1/|Gx|$ luetellaan yhtä monta kertaa, kuin radassa Gx on alkioita. Näistä termeistä koostuva osasumma on selvästi $|Gx| \cdot 1/|Gx| = 1$, ja koska radat muodostavat osituksen, kokonaissummaksi tulee ratojen lukumäärä $|X/G|$. Siispä

$$\sum_{x \in X} |G_x| = |G| \cdot |X/G|,$$

josta väite seuraa. □

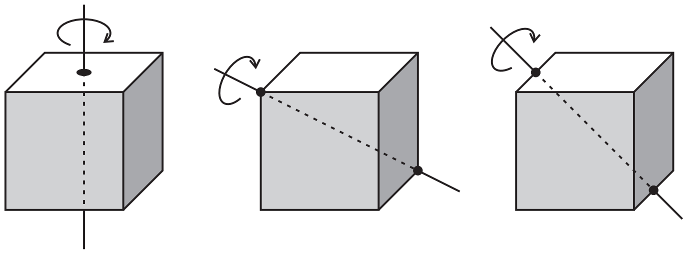
Esimerkki 3.14. Lasketaan, kuinka monella tavalla kuution tahkot voidaan värittää n eri väriä käyttämällä. Väritykset lasketaan samaksi, jos ne saadaan toisistaan kuutiota kiertämällä.

Värityskysymys voidaan formalisoida seuraavasti. Numeroidaan kuution tahkot yhdestä kuuteen ja käytettävät värit yhdestä n:ään. Tällöin jokainen väritys on kuuden alkion jono $(a_1, a_2, a_3, a_4, a_5, a_6)$, missä $a_i \in N_n$ kaikilla i, ja kaikkien väritysten joukko on N_n^6. Kuution symmetriaryhmä G toimii tässä joukossa luonnollisella tavalla: jos $g \in G$ tuottaa kuution tahkojen permutaation $\sigma \in S_6$ ja $a \in N_n^6$ on jokin väritys, niin $(g.a)_i = a_{\sigma(i)}$ kaikilla i.

Kaksi väritystä a ja b samastetaan, jos pätee $g.a = b$ jollain kuution kierrolla $g \in G$. Tämä tarkoittaa sitä, että a ja b kuuluvat samaan rataan. Kysymyksessä halutaan siis selvittää ratojen lukumäärä. Ratojenlaskentalauseen perusteella riittää selvittää kaikki kiintopistejoukot.

Tehtävää helpottaa, jos jaetaan symmetriat konjugaattiluokkiin. “Samantyyppiset” kierrot kuuluvat samaan konjugaattiluokkaan, ja jos g ja h ovat konjugaatteja, niin $|\operatorname{Fix}(g)| = |\operatorname{Fix}(h)|$. Tarkastellaan esimerkiksi neljännesympyrän kiertoa vastakkaisten tahkojen keskipisteiden kautta kulkevan akselin ympäri. Tällaisia akseleita on yhteensä 3, ja kierto voidaan tehdä joko myötä- tai vastapäivään. Kyseiseen konjugaattiluokkaan kuuluu siis 6 kiertoa. Jokainen tällainen kierto kiinnittää täsmälleen ne väritykset, joissa akselin suuntaiset tahkot ovat samanväriset. Näitä värityksiä on tuloperiaatteen mukaan n^3 kappaletta, sillä akselin lävistämille tahkoille voidaan valita mitkä tahansa värit, ja muille tahkoille valitaan jokin kolmas väri.

Alla olevassa taulukossa esitetään kaikki tarpeelliset laskelmat konjugaatioluokittain. Symmetriat on ilmoitettu kiertoakselin ja kiertokulman avulla.



KUVA 7. Kuution symmetria-akselit

symmetria $g \in G$	$\lvert {}^G g \rvert$	$\lvert \operatorname{Fix}(g) \rvert$
identtinen kuvaus	1	n^6
tahkojen keskipisteiden ympäri 90°	6	n^3
tahkojen keskipisteiden ympäri 180°	3	n^4
nurkan ympäri 120°	8	n^2
särmän keskipisteen ympäri 180°	6	n^3

Tuloksena saadaan nyt ratojenlaskentalauseen mukaan

$$|X/G| = \frac{1}{24} \sum_{g \in G} |\operatorname{Fix}(g)| = \frac{1}{24}\left(n^6 + 3 \cdot n^4 + 12 \cdot n^3 + 8 \cdot n^2\right).$$

Jos värejä on esimerkiksi kolme, saadaan $1368/24 = 57$ erilaista väritystä.

3.5. Sisäiset symmetriat. Kuution väritysesimerkissä 3.14 tarkasteltiin yksittäisten alkioiden sijaan niiden konjugaattiluokkia ja todettiin, että konjugaattiluokkia vastaavat luonnollisella tavalla erityyppiset kiertoakselit ja eri kiertokulmat. Tarkastellaan vielä lähemmin tätä konjugointia.

Otetaan esimerkiksi kaksi eri kiertoakselia A ja B, joista kumpikin kulkee eräiden vastakkaisten nurkkien kautta. Kierto B:n ympäri saadaan kääntämällä kuutio ensin symmetrialla g niin, että B siirtyy akselin A paikalle, suorittamalla sitten kierto h akselin A ympäri, ja kääntämällä kuutio lopuksi takaisin. Nähdään, että kierto B:n ympäri on itse asiassa $g^{-1}hg$, eli A:n ympäri tapahtuvan kierron konjugaatti.

Ryhmän alkiolla $g \in G$ konjugointi tuottaa ryhmän sisäisen isomorfismin $h \mapsto {}^g h$, eli niin sanotun *automorfismin.* Automorfismit ovat ryhmän symmetrioita: ne ovat permutaatioita, jotka säilyttävät ryhmän laskutoimitusrakenteen. Konjugoinnista saatavia automorfismeja kutsutaan *sisäisiksi*, ja ne muodostavat ryhmän $\mathrm{Inn}(G)$.

Ryhmällä voi olla muitakin kuin sisäisiä automorfismeja. Kaikkien automorfismien ryhmää merkitään $\mathrm{Aut}(G)$. Sisäiset automorfismit ovat kuitenkin sellaisia, jotka säilyttävät myös ryhmän toiminnan ominaisuudet. Väritysesimerkissä todettiin, että esimerkiksi $\mathrm{Fix}(g) = \mathrm{Fix}(h)$, jos g ja h ovat samassa konjugaattiluokassa eli saadaan toisistaan jotain sisäistä symmetriaa käyttämällä.

On mahdollista osoittaa, että kuution symmetriaryhmän kaikki automorfismit ovat sisäisiä. Kaikille ryhmille tämä ei kuitenkaan päde. Helppo esimerkki saadaan Kleinin neliryhmästä V_4. Koska se on vaihdannainen, millä tahansa alkiolla konjugointi pitää kaikki alkiot paikallaan, joten $\mathrm{Inn}(V_4) = \{\mathrm{id}\}$. Toisaalta kaikki ryhmän V_4 neutraalialkiosta poikkeavat alkiot ovat keskenään täysin samanarvoisia, ja mikä tahansa niiden permutaatio on kyseisen ryhmän automorfismi. Täten $\mathrm{Aut}(V_4) = S_3$.

4. Ryhmien sisäinen rakenne

Tässä luvussa tarkastellaan joitakin tapoja päästä käsiksi ryhmien sisäiseen rakenteeseen. Useimmat tuloksista ovat erityisen käyttökelpoisia äärellisten ryhmien tapauksessa.

4.1. Sylowin[9] lauseet. Lagrangen lause kertoo, että äärellisen ryhmän jokaisen aliryhmän kertaluku jakaa ryhmän kertaluvun. Voidaanko sitten jokaista ryhmän kertaluvun tekijää p kohti löytää aliryhmä, jonka kertaluku olisi p? Vastaus on yleisessä tapauksessa kielteinen, sillä esimerkiksi ryhmällä A_4 ei ole kuuden alkion aliryhmää, vaikka $|A_4| = 12$. Kuitenkin, jos p sattuu olemaan alkuluku, tällainen aliryhmä löytyy. Tämän tuloksen todisti Augustin Louis Cauchy vuonna 1845. Peter Sylow paransi tulosta vuonna 1872 osoittamalla, että itse asiassa jokaista sellaista p:n potenssia kohti, joka jakaa ryhmän kertaluvun, löytyy kyseistä kertalukua oleva aliryhmä, ja suurimmat niistä ovat kaikki keskenään isomorfisia, jopa konjugaatteja.

[9]Peter Ludwig Mejdell Sylow (1832–1918), norjalainen ryhmäteoreetikko.

Sylowin lauseet liittyvät aliryhmiin, joiden kertaluku on jonkin alkuluvun potenssi. Tällaisilla ryhmillä on muutenkin monia kiinnostavia ominaisuuksia; esimerkiksi niillä on aina epätriviaali keskus.

MÄÄRITELMÄ 4.1. Olkoon p alkuluku. Äärellistä ryhmää sanotaan *p-ryhmäksi*, jos sen kertaluku on p^m jollain $m \geq 1$.

MÄÄRITELMÄ 4.2. Oletetaan, että ryhmän kertaluku on $p^k m$, missä p on alkuluku, $k \geq 1$, ja m ei ole jaollinen p:llä. Sellaista aliryhmää, jonka kertaluku on p^k, kutsutaan *Sylowin p-aliryhmäksi.*

Sylow käytti lauseidensa todistamisessa yllä mainittua Cauchyn tulosta, mutta sittemmin lauseet on todistettu uudestaan monellakin eri tavalla. Tässä luvussa seurataan Helmut Wielandtin kombinatoriseen havaintoon perustuvaa esitystä, jota varten tarvitaan ensin yksinkertainen aputulos.

LEMMA 4.3. *Oletetaan, että p on alkuluku, joka ei jaa lukua $m \in \mathbb{N}$, ja k on positiivinen kokonaisluku. Tällöin binomikerroin $\binom{p^k m}{p^k}$ ei ole jaollinen luvulla p.*

TODISTUS. Tarkasteltava binomikerroin on

$$\binom{p^k m}{p^k} = \frac{p^k m(p^k m-1)\cdots(p^k m-i)\cdots(p^k m-p^k+1)}{p^k(p^k-1)\cdots(p^k-i)\cdots(p^k-p^k+1)}.$$

Koska luku m ei sisällä yhtään tekijää p, riittää tutkia osoittajan termejä $p^k m - i$, missä $1 \leq i < p^k$. Olkoon $i = p^l q$, missä $l \in \mathbb{N}$ ja $p \nmid q$. Nyt

$$p^k m - i = p^l(p^{k-l} m - q),$$

ja p ei jaa lukua $p^{k-l}m - q$, koska $k - l > 0$. Siispä korkein p:n potenssi, joka jakaa termin $p^k m - i$, on p^l. Samalla päättelyllä p^l jakaa kuitenkin myös nimittäjän termin $p^k - i$. Koska osoittajassa ja nimittäjässä on yhtä monta termiä, jokainen tekijä p supistuu pois, joten binomikertoimeen ei jää yhtään tekijää p. $\square$

LAUSE 4.4 (Sylow). *Oletetaan, että $|G| = p^k m$, missä $k \geq 1$, ja p on alkuluku, joka ei jaa lukua m. Tällöin*

(i) *Ryhmällä G on Sylowin p-aliryhmä.*
(ii) *Ryhmän G Sylowin p-aliryhmät ovat keskenään konjugaatteja.*
(iii) *Jos s_p on Sylowin p-aliryhmien lukumäärä, niin $s_p \equiv 1 \pmod p$, ja s_p jakaa luvun m.*

TODISTUS. (i) Olkoon $\mathcal{A}_p = \{A \subset G : |A| = p^k\}$. Määritellään G:n toiminta tässä joukossa kertolaskulla: $gA = \{ga \mid a \in A\}$ kaikilla $A \in \mathcal{A}_p$. Lemman 4.3 perusteella joukon $\mathcal{A}_p$ koko ei ole jaollinen p:llä. Tämän vuoksi jollekin radalle GB pätee $p \nmid |GB|$. Toisaalta B:n kiinnittäjälle pätee $|G_B| = |G|/|GB|$, joten $|G_B|$ on jaollinen luvulla p^k. Olkoon sitten $b_0 \in B$. Jos $g \in G_B$, niin $gb_0 \in B$. Näin saadaan kuvaus $g \mapsto gb_0$ kiinnittäjältä G_B joukolle B. Tämä kuvaus on injektio, joten $|G_B| \leq p^k$. Siispä $|G_B| = p^k$, ja G_B on vaadittu Sylowin aliryhmä.

(ii) Olkoon P jokin Sylowin p-aliryhmä, ja Q mikä tahansa p-aliryhmä. Tarkastellaan ryhmän Q kertolaskutoimintaa P:n sivuluokkien joukossa. Näiden sivuluokkien määrä on m, joka ei ole jaollinen p:llä. Koska jokaisen radan koko kuitenkin jakaa ryhmän Q kertaluvun (jälleen lause 2.7) eli on p:n potenssi, täytyy ratojen joukossa olla jokin yksiö $\{aP\}$. Tällöin $QaP = aP$, joten $a^{-1}Qa \subset P$. Täten jokaisella p-aliryhmällä on konjugaatti, joka sisältyy annettuun Sylowin p-aliryhmään. Jos Q on itse Sylowin aliryhmä eli $|Q| = |P|$, täytyy olla $a^{-1}Qa = P$.

(iii) Olkoon P edelleen jokin Sylowin p-aliryhmä. Nyt P toimii konjugoimalla kaikkien Sylowin p-aliryhmien joukossa $\{P, Q_1, \ldots, Q_r\}$. Kuten aikaisemmin, ratojen (eli konjugaattiluokkien) koot jakavat toimivat ryhmän kertaluvun $|P| = p^k$. Koska ${}^P P = P$, ryhmän P rata on yksiö. Osoitetaan, että jokaisen muun radan ${}^P Q_i$ koko on jaollinen p:llä. Tällöin nimittäin

$$s_p = 1 + \sum_i p^{k_i},$$

missä i käy läpi kaikki radat ja $k_i \geq 1$ kaikilla i. Tästä seuraa ensimmäinen väite.

Jos $\left|{}^P Q_i\right| = 1$, niin P sisältyy normalisoijaan $N_G(Q_i)$. Selvästi sekä P että Q_i ovat tämän normalisoijan Sylowin p-aliryhmiä. Toisaalta $Q_i \trianglelefteq N_G(Q_i)$, joten Q_i ja P eivät ole konjugaatteja ryhmässä $N_G(Q_i)$. Tämä on ristiriidassa kohdan (ii) kanssa, joten $\left|{}^P Q_i\right| > 1$, mikä oli todistettava.

Viimeinen väite seuraa siitä, että ryhmän G konjugointitoiminta kaikkien Sylowin p-aliryhmien joukossa on transitiivista. Tällöin nimittäin $s_p = [G : N_G(P)]$, joten s_p jakaa ryhmän G kertaluvun $p^k m$. Koska $s_p \equiv 1 \pmod p$, niin Eukleideen lemman perusteella $s_p \mid m$. □

Kaikki Sylowin p-aliryhmät ovat keskenään konjugaatteja, mistä seuraa, että ne ovat myös keskenään isomorfisia. Toisaalta jokainen Sylowin p-aliryhmän konjugaatti on itse Sylowin p-aliryhmä. Jos tällaisia löytyy vain yksi, kyseinen aliryhmä on silloin väistämättä normaali. Sylowin lauseet auttavat tällä tavoin ns. *yksinkertaisten* ryhmien löytämisessä. Ryhmää sanotaan yksinkertaiseksi, jos sillä ei ole aitoja epätriviaaleja normaaleja aliryhmiä.

Esimerkki 4.5. Oletetaan, että ryhmä, jonka kertaluku on 30, ei voi olla yksinkertainen. Kertaluvun alkutekijähajotelma on $2 \cdot 3 \cdot 5$. Tarkastellaan ensin Sylowin 5-aliryhmiä. Niitä löytyy Sylowin lauseen mukaan s_5 kappaletta, missä

$$s_5 \equiv 1 \pmod 5 \qquad \text{ja} \qquad s_5 \mid 6.$$

Täytyy siis päteä joko $s_5 = 1$ tai $s_5 = 6$. Ensimmäisessä tapauksessa aliryhmä olisi normaali, joten tarkastellaan jälkimmäistä. Viiden alkion aliryhmät leikkaavat toisiaan vain neutraalialkion kohdalla, joten näihin ryhmiin sisältyy neutraalialkio poisluettuna yhteensä 24 alkiota.

Tarkastellaan sitten Sylowin 3-aliryhmiä. Niitä on s_3 kappaletta, missä $s_3 \equiv 1 \pmod 3$ ja $s_3 \mid 10$. Näin ollen $s_3 = 1$ tai $s_3 = 10$. Keskitytään jälleen jälkimmäiseen tapaukseen, jolloin näistä kolmen alkion aliryhmistä saadaan yhteensä 20 neutraalialkiosta poikkeavaa alkiota. Lisäksi mikään näistä ei voi sisältyä Sylowin 5-aliryhmään, joten yhteensä on löydetty jo $24 + 20 = 44$ alkiota. Tämä on ristiriita, joten ryhmällä on normaali aliryhmä.

Sylowin lauseet auttavat muutenkin ryhmien rakenteen selvittämisessä.

Esimerkki 4.6. Tarkastellaan ryhmiä, joiden kertaluku on $35 = 5 \cdot 7$. Niiden Sylowin 5-aliryhmien lukumäärälle pätee $s_5 \equiv 1 \pmod 5$ ja $s_5 \mid 7$, joten näitä ryhmiä on vain yksi. Merkitään sitä kirjaimella P. Samalla tavoin Sylowin 7-aliryhmiä on vain yksi; olkoon se Q. Sekä P että Q ovat normaaleja aliryhmiä, ja niiden leikkaus on triviaali. Tästä seuraa, että koko ryhmä on isomorfinen tuloryhmän $P \times Q \cong \mathbb{Z}_5 \times \mathbb{Z}_7$ kanssa (todistetaan myöhemmin). Lisäksi $\mathbb{Z}_5 \times \mathbb{Z}_7 \cong \mathbb{Z}_{35}$, joten ryhmä on itse asiassa syklinen.

Sylowin lauseesta saadaan seurauksena Cauchyn lause.

LAUSE 4.7 (Cauchy). *Olkoon p jokin ryhmän G kertaluvun alkutekijä. Tällöin G:ssä on alkio, jonka kertaluku on p.*

TODISTUS. Harjoitustehtävä. □

Ääretön p-ryhmä määritellään niin, että sen jokaisen alkion kertaluku on jaollinen p:llä. Äärellisessä tapauksessa tämä määritelmä on yhtäpitävä aiemman kanssa. Lagrangen lauseesta nimittäin seuraa, että p-ryhmän jokaisen alkion kertaluku on jaollinen p:llä. Toisaalta, jos ryhmän kertaluvulla on alkutekijä $q \neq p$, niin Cauchyn lauseen perusteella se sisältää alkion, jonka kertaluku on q.

4.2. Tuloryhmät. Olkoot A ja B ryhmän G aliryhmiä. Tutkitaan, milloin niiden *tulojoukko*

$$AB = \{ab \mid a \in A, b \in B\}$$

on aliryhmä. Tulojoukon alkioiden $g_1 = a_1b_1$ ja $g_2 = a_2b_2$ tulo on $g_1g_2 = a_1b_1a_2b_2$. Jos tämä tulo on joukossa AB, niin

$$b_1a_2 = a_1^{-1} \underbrace{(g_1g_2)}_{\in AB} b_2^{-1} \in AB.$$

Siispä vähimmäisvaatimus sille, että tulojoukko olisi aliryhmä, on että b_1a_2 on muotoa $a'b'$ joillain $a' \in A$ ja $b' \in B$. Koska tämän täytyy päteä kaikille alkioille, ehdoksi tulee $AB = BA$. Tämä toteutuu esimerkiksi silloin, kun jokainen A:n alkio kommutoi jokaisen B:n alkion kanssa. Vähempikin kuitenkin riittää.

LEMMA 4.8. *Olkoot H ja N ryhmän G aliryhmiä. Jos N on normaali G:ssä, niin $HN \leq G$.*

TODISTUS. Käytetään aliryhmäkriteeriä. Selvästi HN on epätyhjä. Olkoot $a_1, a_2 \in H$ ja $b_1, b_2 \in N$. Koska N on normaali, niin $Na_2^{-1} = a_2^{-1}N$, joten $b_1b_2^{-1}a_2^{-1} = a_2^{-1}b'$ jollain $b' \in N$. Tällöin

$$a_1b_1(a_2b_2)^{-1} = a_1b_1b_2^{-1}a_2^{-1} = (a_1a_2^{-1})b' \in HN.$$

Siispä HN on aliryhmä. □

Keskitytään jatkossa siihen tapaukseen, missä molemmat aliryhmät ovat normaaleja.

LAUSE 4.9. *Oletetaan, että H ja K ovat ryhmän G normaaleja aliryhmiä. Jos $HK = G$ ja $H \cap K = \{1\}$, niin $G \cong H \times K$.*

TODISTUS. Näytetään ensin, että H:n ja K:n alkiot ovat keskenään vaihdannaisia. Olkoot $a \in H$ ja $b \in K$. Nyt $(aba^{-1})b^{-1} \in K$, koska K on normaali. Samoin kuitenkin $a(ba^{-1}b^{-1}) \in H$, joten $aba^{-1}b^{-1} \in H \cap K = \{1\}$. Tästä seuraa, että $ba = ab$.

Harjoitustehtävänä on osoittaa, että jokaisella G:n alkiolla on yksikäsitteinen tuloesitys $g = ab$, missä $a \in H$ ja $b \in K$. Tällöin on mahdollista määritellä kuvaus $f : G \to H \times K$ kaavalla $f(ab) = (a, b)$. Kuvaus on selvästi bijektio. Olkoot $a_1, a_2 \in H$ ja $b_1, b_2 \in K$, jolloin

$$\begin{aligned} f(a_1b_1 \cdot a_2b_2) &= f(a_1a_2 \cdot b_1b_2) = (a_1a_2,\, b_1b_2) \\ &= (a_1, b_1) \cdot (a_2, b_2) = f(a_1a_2) \cdot f(b_1b_2). \end{aligned}$$

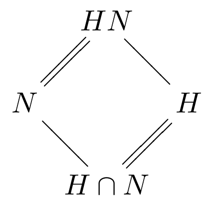
Täten f on homomorfismi. □

Jos edellisen lauseen ehdot pätevät, sanotaan, että G on aliryhmiensä H ja K *sisäinen suora tulo*. Tällöin ei yleensä erotella sisäistä tuloa HK ja ulkoista tuloa $H \times K$, koska nämä ovat keskenään isomorfiset.

4.3. Isomorfialauseet. Seuraavat Emmy Noetherin muotoilemat tulokset selvittävät tekijäryhmien välisiä suhteita. Niiden todistukset nojaavat vahvasti homomorfialauseeseen. Vastaavat tulokset pätevät myös renkaille.

LAUSE 4.10 (1. isomorfialause[10]). *Olkoot H ja N ryhmän G aliryhmiä, ja olkoon N normaali. Tällöin $H \cap N \trianglelefteq H$, ja $H/(H \cap N) \cong HN/N$.*

Huomaa, että lemman 4.8 nojalla HN on ryhmä. Lisäksi N on normaali ryhmässä HN, koska $HN \leq G$ ja N on normaali G:ssä. Alla oleva Hassen kaavio voi helpottaa lauseen muistamista. Kaksinkertainen viiva viittaa normaaliin aliryhmään. Yhdensuuntaiset kaksoisviivat viittaavat isomorfisiin tekijäryhmiin.



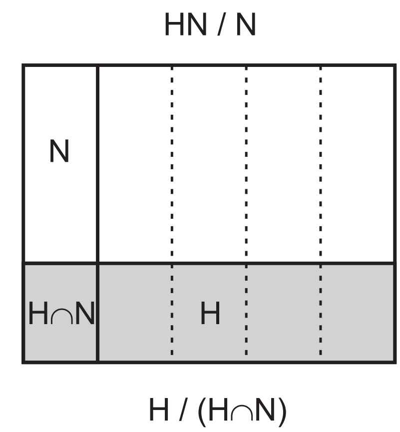
TODISTUS. Olkoon $\pi : G \to G/N$ kanoninen surjektio, ja olkoon π' sen rajoittuma ryhmään H. Kuvauksen π' arvot ovat siis sivuluokkia hN, missä $h \in H$. Tällaiset sivuluokat kuuluvat tekijäryhmään HN/N, koska $hn \in HN$ jokaisella $n \in N$.

Selvästi

$$\operatorname{Ker} \pi' = \{g \in H \mid g \in N\} = H \cap N,$$

joten $H \cap N$ on normaali, ja homomorfialauseen perusteella $H/(H \cap N) \cong \operatorname{Im} \pi'$. Toisaalta, jos $gN \in HN/N$, niin $g = hn$ joillain $h \in H$ ja $n \in N$. Nyt saadaan $\pi'(h) = hN = gN$, joten $\operatorname{Im} \pi' = HN/N$. □

[10]Monissa lähteissä homomorfialausetta nimitetään ensimmäiseksi isomorfialauseeksi. Tällöin ensimmäisestä isomorfialauseesta tuleekin toinen isomorfialause, ja toisesta kolmas.

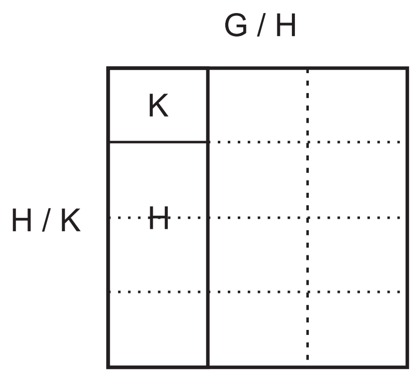


Kuva 8. Noetherin 1. isomorfialause

Lause 4.11 (2. isomorfialause). *Olkoot H ja K ryhmän G normaaleja aliryhmiä, joille pätee $K \leq H$. Tällöin H/K on normaali ryhmässä G/K, ja*

$$(G/K)/(H/K) \cong G/H.$$

Todistus. Olkoon $\pi : G \to G/H$ kanoninen surjektio. Koska $K \subset H$, kaikilla $k \in K$ pätee $\pi(k) = H$. Lauseen 1.14 perusteella on olemassa homomorfismi $f : G/K \to G/H$, jolle pätee $f(gK) = gH$. Tämä kuvaus ikään kuin laajentaa sivuluokkia ja on selvästi surjektio. Lisäksi $f(gK) = gH = H$ jos ja vain jos $g \in H$, ja tämä on yhtäpitävää sen kanssa, että $gK \in H/K$. Täten $\operatorname{Ker} f = H/K$, ja tulos seuraa homomorfialauseesta. □



Kuva 9. Noetherin 2. isomorfialause

5. Ryhmän kompositiotekijät

Ratkeavan ryhmän käsite kuuluu historiallisesti ensimmäisiin varsinaisen ryhmäteorian käsitteisiin. Évariste Galois todisti vuonna 1831, että polynomiyhtälöön liittyy aina tietty symmetriaryhmä, joka permutoi polynomin juuria, ja mahdollinen ratkaisukaava saadaan tietynlaisesta jonosta tuon symmetriaryhmän aliryhmiä. Ryhmää, jolla on tällainen jono, kutsutaan ratkeavaksi juuri tästä syystä.

5.1. Ratkeavat ryhmät.

MÄÄRITELMÄ 5.1. 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+1}/G_i kutsutaan jonon *tekijöiksi.* Jonon *pituus* on jonon aitojen inkluusioiden lukumäärä, joka on sama kuin epätriviaalien tekijöiden määrä.

Huom. Tässä ja muissakin yhteyksissä tyydytään yleensä merkitsemään triviaalia ryhmää symbolilla 1, jättämällä siis joukkosulkeet pois. Samaten normaalin jonon tekijöitä merkitään yleensä vain isomorfiatyypin mukaan; ei siis tehdä eroa esimerkiksi ryhmien A_3 ja $\mathbb{Z}_3$ välillä.

Ryhmällä voi olla useita erilaisia normaaleja jonoja, joissa voi myös olla eri tekijät. Esimerkiksi ryhmällä S_4 on muun muassa normaalit jonot $S_4 \triangleright A_4 \triangleright 1$ ja $S_4 \triangleright V_4 \triangleright 1$. Edellisen tekijät ovat (isomorfiaa vaille) C_2 ja A_4, jälkimmäisen S_3 ja V_4.

Kaikkien normaalin jonon jäsenten ei tarvitse olla normaaleja ryhmässä G. Normaalius ei nimittäin ole transitiivinen ominaisuus: esimerkiksi

$$D_8 \triangleright \langle \rho^2, \sigma \rangle \triangleright \langle \sigma \rangle \triangleright 1$$

on normaali jono, mutta $\langle \sigma \rangle$ ei ole normaali ryhmässä D_8.

ESIMERKKI 5.2. Normaalin jonon tekijät ovat tietyssä mielessä tulon tekijöiden yleistys. Jos nimittäin G on aliryhmiensä H ja K suora tulo, eli $G \cong H \times K$, niin G:llä on normaali jono $G \triangleright H \triangleright 1$. Lisäksi $G/H \cong K$ (1. isomorfialauseen nojalla), 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 $G \triangleright N \triangleright 1$ tekijät ovat H ja N.

Jonon tekijät eivät kuitenkaan aina vastaa mitään tuloa. Esimerkiksi neljän alkion syklisellä ryhmällä $C_4 = \langle g \rangle$ on normaali jono $C_4 \triangleright \langle g^2 \rangle \triangleright 1$, jonka molemmat tekijät ovat isomorfisia ryhmän C_2 kanssa. Ryhmä C_4 kuitenkin sisältää vain yhden C_2:n kanssa isomorfisen aliryhmän, joten se ei voi olla kahden tällaisen tekijän tulo.

Ratkeavalla ryhmällä täytyy olla tietyntyyppinen normaali jono.

MÄÄRITELMÄ 5.3. Ryhmää sanotaan *ratkeavaksi*, jos sillä on normaali jono, jonka kaikki tekijät ovat vaihdannaisia ryhmiä.

Selvästi kaikki vaihdannaiset ryhmät ovat ratkevia, koska triviaalin jonon $G \trianglelefteq 1$ ainoa tekijä on vaihdannainen. Myös kaikki diedriryhmät ja kaikki äärelliset p-ryhmät ovat ratkeavia. Symmetriset ryhmät S_3 ja S_4 ovat ratkeavia, sillä niillä on normaalit jonot $S_3 \triangleright A_3 \triangleright 1$ ja $S_4 \triangleright A_4 \triangleright V_4 \triangleright 1$, joiden tekijät ovat vaihdannaisia. Sen sijaan S_n ja A_n eivät ole ratkeavia, mikäli $n \geq 5$. Tähän palataan myöhemmin.

5.2. Kompositiojonot. Koska normaalius ei ole transitiivinen ominaisuus, normaalin jonon osajono ei välttämättä ole normaali. Alkuperäisen jonon jäsenten väliin voidaan kuitenkin usein lisätä sopivia alkioita niin, että saadaan uusi normaali jono.

Määritelmä 5.4. Normaalia jonoa (H_i) sanotaan jonon (G_i) *hienonnukseksi*, mikäli se sisältää kaikki jonon (G_i) jäsenet, eli (G_i) on jonon (H_i) osajono.

Määritelmä 5.5. Jos ryhmän normaalilla jonolla ei ole triviaaleja tekijöitä, mutta kaikilla sen hienonnuksilla on, jonoa kutsutaan ryhmän *kompositiojonoksi*.

Kompositiojono on siis tietyllä tavalla maksimaalinen normaali jono. Aiemmin mainittu jono $S_4 \rhd A_4 \rhd V_4 \rhd 1$ ei ole kompositiojono, sillä ryhmällä V_4 on epätriviaali normaali aliryhmä C_2. Jonon loppupäätä voidaan siis hienontaa seuraavasti: $\cdots \rhd V_4 \rhd C_2 \rhd 1$. Toisaalta jono $S_3 \rhd A_3 \rhd 1$ on kompositiojono, sillä sitä ei voida hienontaa ottamatta mukaan triviaaleja tekijöitä.

Normaalin jonon tekijöitä voidaan verrata kokonaisluvun tekijöihin. Oletetaan, että $n = m_1 \cdot m_2$. Jos jompikumpi tekijöistä ei ole alkuluku, se voidaan edelleen jakaa pienempiin tekijöihin. Lopulta saavutetaan kyseisen luvun alkutekijähajotelma $n = p_1 p_2 \ldots p_r$, jonka tekijöitä ei voi enää jakaa epätriviaalilla tavalla. Kompositiojono vastaa tällaista alkutekijähajotelmaa. Osoittautuu nimittäin, että ryhmän kompositiotekijät ovat järjestystä vaille yksikäsitteiset. On kuitenkin huomattava, että toisin kuin kokonaislukujen tapauksessa, kahdella ryhmällä voi olla samat kompositiotekijät, vaikka ryhmät eivät olisi isomorfiset.

Osoitetaan seuraavaksi, että alkutekijähajotelman alkulukuja vastaavat normaalin jonon *yksinkertaiset* tekijät. Ryhmää kutsutaan yksinkertaiseksi, jos se on epätriviaali eikä sillä ole aitoja epätriviaaleja normaaleja aliryhmiä.

Lause 5.6. *Ryhmän G normaali jono (G_i) on kompositiojono, jos ja vain jos sen tekijät ovat yksinkertaisia.*

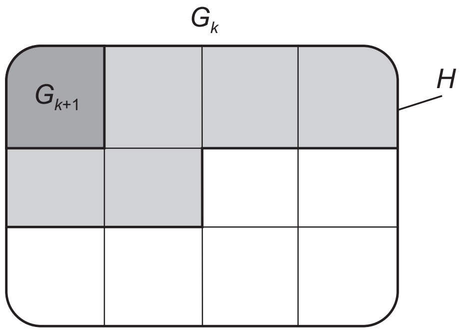
Todistus. Oletetaan ensin, että normaali jono (G_i) ei ole kompositiojono eli että $G_k \rhd H \rhd G_{k+1}$ jollain k. Noetherin toisesta isomorfialauseesta seuraa tällöin, että $H/G_{k+1} \lhd G_k/G_{k+1}$, ja koska H/G_{k+1} ei ole triviaali, tekijä G_k/G_{k+1} ei ole yksinkertainen.

Oletetaan sitten, että jokin tekijä G_k/G_{k+1} ei ole yksinkertainen eli että pätee $H \lhd G_k/G_{k+1}$ jollain $H \neq \{1\}$. Olkoon $\pi : G_k \to G_k/G_{k+1}$ kanoninen surjektio. Tarkastellaan alkukuvaa $H' = \pi^{-1}H$ (ks. kuva 10). Tämä on normaali ryhmässä G_k, koska H on normaali maalijoukossa. Toisaalta ryhmä G_{k+1} on normaali H':ssa, koska se on normaali suuremmassa ryhmässä G_k. Siispä $G_k \trianglerighteq H' \trianglerighteq G_{k+1}$. Lisäksi, koska π on surjektio, pätee $\pi H' = H$. Tällöin nähdään helposti, että $H' \neq G_k$, koska $H \neq G_k/G_{k+1}$, ja $H' \neq G_{k+1}$, koska $H \neq \{1\}$. Näin ollen jono (G_i) ei ole kompositiojono. □

Aiemmin hienonnettu jono

$$S_4 \rhd A_4 \rhd V_4 \rhd C_2 \rhd 1$$

on kompositiojono, sillä sen tekijät ovat C_2, C_3, C_2 ja C_2, jotka ovat kaikki yksinkertaisia.



Kuva 10. Tekijän normaalista aliryhmästä saadaan uusi aliryhmä jonon jäsenten G_k ja G_{k+1} väliin.

Epätriviaalilla äärellisellä ryhmällä on aina kompositiojono. Tämä löydetään lähtemällä hienontamaan normaalia jonoa $G \rhd 1$. Jokaisesta uudesta syntyvästä tekijästä H etsitään aito epätriviaali normaali aliryhmä K. Tämä aliryhmä nostetaan kanonisen surjektion avulla alkuperäisen jonon jäseneksi, ja uusiksi tekijöiksi saadaan K ja siihen liittyvä tekijäryhmä H/K. Hienonnusta jatketaan niin kauan kuin tekijöistä löytyy normaaleja aliryhmiä. Lopulta tekijät ovat kaikki yksinkertaisia, jolloin saatu jono on kompositiojono. Koska ryhmä on äärellinen, prosessi päättyy varmasti.

Jos vaihdannaisella ryhmällä on kompositiojono, sen tekijät ovat yksinkertaisia vaihdannaisia ryhmiä. On melko helppo nähdä, että tällaiset ryhmät ovat äärellisiä syklisiä ryhmiä, joiden kertaluku on alkuluku. Koska alkuperäisen ryhmän kertaluku on tekijöiden kertalukujen tulo, tämä osoittaa, että äärettömällä vaihdannaisella ryhmällä ei voi olla kompositiojonoa. Myös jokaisella äärellisellä ratkeavalla ryhmällä on jokin kompositiojono, jonka tekijät ovat muotoa C_p, sillä vaihdannaisia tekijöitä pilkkomalla on päädyttävä lopulta yksinkertaisiin vaihdannaisiin ryhmiin.

Epävaihdannaisella äärettömällä ryhmällä voi olla tai olla olematta kompositiojono. Esimerkiksi ryhmän $\mathbb{Z}$ jokainen aliryhmä on muotoa $n\mathbb{Z}$. Viimeistä edelliseksi kompositiotekijäksi jäisi siis väistämättä jokin tällainen aliryhmä, ja koska $n\mathbb{Z}$ ei ole yksinkertainen, tämä on ristiriita. Toisaalta esimerkiksi reaalitason lineaarikuvaukset, joiden determinantti on 1, muodostavat ryhmän $SL_2(\mathbb{R})$, ja tällä on kompositiojono $SL_2(\mathbb{R}) \rhd \{I, -I\} \rhd \{I\}$. Jonon ensimmäinen tekijä on *projektiivisten* kuvausten ryhmä $PSL_2(\mathbb{R})$, joka on yksinkertainen (todistus sivuutetaan).

5.3. Kompositiotekijöiden yksikäsitteisyys. Ranskalainen matemaatikko Camille Jordan todisti vuonna 1868, että äärellisen ryhmän kompositiotekijöiden kertaluvut ovat yksikäsitteiset, ja saksalainen Otto Hölder täydensi tulosta vuonna 1889 näyttämällä, että itse tekijät ovat isomorfiaa vaille samat. Tulos pätee myös sellaisille äärettömille ryhmille, joilla on kompositiojono. Ryhdytään seuraavaksi osoittamaan tätä tulosta.

Määritelmä 5.7. Ryhmän kaksi normaalia jonoa ovat *ekvivalentit*, jos niiden kompositiotekijöiden välillä on bijektio φ, jolle pätee $\varphi(A) \cong B$.

Sen osoittamiseksi, että tietyn ryhmän kaikki kompositiojonot ovat keskenään ekvivalentteja, näytetään, että kahdella normaalilla jonolla on aina ekvivalentit hienonnukset. Koska kompositiojonoilla ei ole epätriviaaleja hienonnuksia, niiden on itse oltava toistensa kanssa ekvivalentteja. Ensin on kuitenkin todistettava seuraava tekninen aputulos.

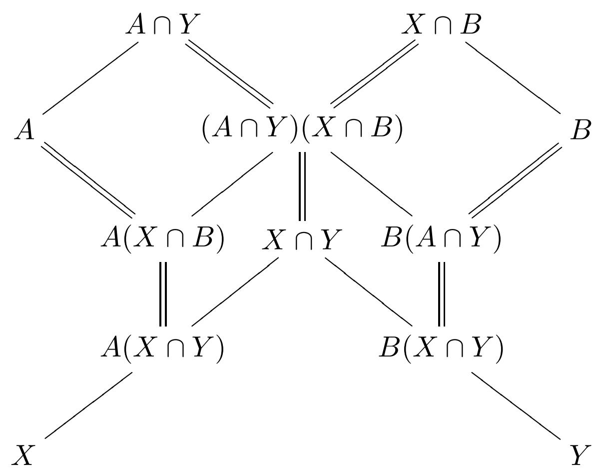
Lemma 5.8 (Zassenhausin perhoslemma). *Olkoot A, B, X ja Y ryhmän G aliryhmiä. Oletetaan, että $A \trianglelefteq X$ ja $B \trianglelefteq Y$. Tällöin*

$$A(X \cap B) \trianglelefteq A(X \cap Y) \quad \textit{ja} \quad B(A \cap Y) \trianglelefteq B(X \cap Y),$$

ja lisäksi tekijäryhmille pätee

$$\frac{A(X \cap Y)}{A(X \cap B)} \cong \frac{B(X \cap Y)}{B(A \cap Y)}.$$

Oheisessa Hassen kaaviossa näkyvät lemmaan liittyvien ryhmien keskinäiset sisältyvyyssuhteet (ryhmät suurenevat ylhäältä alaspäin). Kaksoisviiva merkitsee normaalia aliryhmää, ja yhdensuuntaiset kaksoisviivat viittaavat isomorfisiin tekijäryhmiin. Ylemmät suunnikkaat (etusiivet) perustuvat suoraan 1. isomorfialauseeseen. Alemmat suunnikkaat (takasiivet) puolestaan vastaavat lemman sisältöä.



Kuva 11. Zassenhausin perhonen

Todistus. Merkitään $D = (A \cap Y)(X \cap B)$ ja osoitetaan, että

$$\frac{A(X \cap Y)}{A(X \cap B)} \cong \frac{X \cap Y}{D}.$$

Ensin todetaan, että koska $A \trianglelefteq X$, niin $A \cap Y \trianglelefteq X \cap Y$. Samoin $X \cap B \trianglelefteq X \cap Y$. Tästä seuraa helposti, että myös tulo $(A \cap Y)(X \cap B)$ on normaali ryhmässä $X \cap Y$.

Määritellään $f : A(X \cap Y) \to (X \cap Y)/D$ kaavalla $f(az) = zD$, missä $a \in A$ ja $z \in X \cap Y$. Tämä f on selvästi surjektiivinen. Homomorfisuuden osoittamiseksi otetaan alkiot $a_1, a_2 \in A$ ja $z_1, z_2 \in (X \cap Y)$. Koska $A \trianglelefteq X$ ja $z_1 \in X$, nähdään, että $z_1 a_2 = a' z_1$ jollain $a' \in A$. Nyt

$$f(a_1 z_1 \cdot a_2 z_2) = f(a_1 a' \cdot z_1 z_2) = (z_1 z_2)D,$$

joten f on homomorfismi.

Osoitetaan vielä, että kuvauksen f ydin on $A(X \cap B)$, jolloin haluttu tulos seuraa homomorfialauseesta. Jos $a \in A$ ja $z \in X \cap B$, niin erityisesti $z \in D$, joten $f(az) = D$ eli $az \in \operatorname{Ker} f$. Toisaalta, jos $f(az) = D$ eli $z \in D$, niin $z = yx$ joillain $y \in A \cap Y$ ja $x \in X \cap B$. Tällöin $ay \in A$, joten $az = ayx \in A(X \cap B)$. Näin ollen $\operatorname{Ker} f = A(X \cap B)$.

Samalla tavoin voidaan osoittaa, että $B(X \cap Y)/B(A \cap Y) \cong (X \cap Y)/D$, ja lemman väite seuraa isomorfian transitiivisuudesta. □

LAUSE 5.9 (Schreierin hienonnuslause). *Ryhmän G millä tahansa kahdella normaalilla jonolla on ekvivalentit hienonnukset.*

TODISTUS. Oletetaan, että G:llä on normaalit jonot

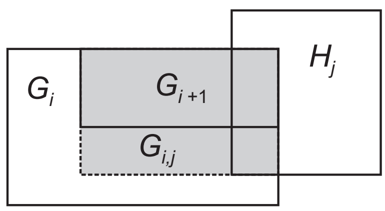
$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = 1$$

ja

$$G = H_0 \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq H_m = 1.$$

Edetään lisäämällä ensimmäisessä jonossa aina kahden jonon peräkkäisen jäsenen väliin "kopio" koko toisesta jonosta. Tarkemmin sanottuna, määritellään aliryhmät $G_{i,j} = G_{i+1}(G_i \cap H_j)$ kaikilla $i \leq n$ ja $j \leq m$. Nyt

$$G_{i,j+1} = G_{i+1}(G_i \cap H_{j+1}) \leq G_{i+1}(G_i \cap H_j) = G_{i,j}.$$



KUVA 12. Hienonnuksen alkio

Asettamalla $A = G_{i+1}$, $X = G_i$, $B = H_{j+1}$ ja $Y = H_j$, saadaan Zassenhausin lemmasta, että $G_{i,j+1} \trianglelefteq G_{i,j}$. Lisäksi

$$G_{i,0} = G_{i+1}(G_i \cap G) = G_i \qquad \text{ja} \qquad G_{i,m} = G_{i+1}(G_i \cap \{1\}) = G_{i+1},$$

joten jono

$$G_{0,0} \trianglerighteq G_{0,1} \trianglerighteq \cdots \trianglerighteq G_{0,m-1} \trianglerighteq G_{1,0} \trianglerighteq \cdots \trianglerighteq G_{n-1,0} \trianglerighteq \cdots \trianglerighteq G_{n-1,m-1} \trianglerighteq 1$$

on jonon (G_i) hienonnus. Samalla tavoin voidaan määritellä $H_{i,j} = H_{j+1}(H_j \cap G_i)$, jolloin saadaan jonon (H_j) hienonnus

$$H_{0,0} \trianglerighteq H_{1,0} \trianglerighteq \cdots \trianglerighteq H_{n-1,0} \trianglerighteq H_{0,1} \trianglerighteq \cdots \trianglerighteq H_{0,m-1} \trianglerighteq \cdots \trianglerighteq H_{n-1,m-1} \trianglerighteq 1.$$

Molemmat hienonnukset sisältävät nm tekijää. Tekijöiden välille voidaan määritellä bijektio $G_{i,j}/G_{i,j+1} \mapsto H_{i,j}/H_{i+1,j}$, ja Zassenhausin lemman avulla nähdään, että toisiaan vastaavat tekijät ovat isomorfiset. □

KOROLLAARI 5.10 (Jordanin-Hölderin lause). *Saman ryhmän kaksi kompositiojonoa ovat aina keskenään ekvivalentit.*

Todistus. Edellisen lauseen mukaan kompositiojonoilla on ekvivalentit hienonnukset. Kompositiojonon määritelmän perusteella näiden hienonnusten uudet tekijät ovat kaikki triviaaleja, joten alkuperäiset jonot olivat jo keskenään ekvivalentit. □

Esimerkiksi syklisellä ryhmällä $\mathbb{Z}_{30}$ on muun muassa kompositiojonot

$$\mathbb{Z}_{30} \rhd \langle\overline{3}\rangle \rhd \langle\overline{15}\rangle \rhd 1 \qquad \text{ja} \qquad \mathbb{Z}_{30} \rhd \langle\overline{5}\rangle \rhd \langle\overline{10}\rangle \rhd 1.$$

Ensimmäisen jonon kompositiotekijät ovat järjestyksessä C_3, C_5 ja C_2, ja toisen jonon tekijät ovat C_5, C_2 ja C_3. Molemmissa on siis samat tekijät.

Jordanin-Hölderin lauseen avulla saadaan uusi karakterisointi äärellisen ryhmän ratkeavuudelle. Ratkeavalla ryhmällä on normaali jono, jonka tekijät ovat vaihdannaisia. Aiemmin todettiin, että jos ryhmä on äärellinen, sen vaihdannaisia tekijöitä pilkkomalla saatava kompositiojono sisältää vain syklisiä tekijöitä, joiden kertaluku on alkuluku. Toisaalta Jordanin-Hölderin lauseen perusteella millä tahansa tavalla tuotettu kompositiojono sisältää samat tekijät.

Lause 5.11. *Äärellinen ryhmä on ratkeava, jos ja vain jos sillä on normaali jono, jonka tekijät ovat syklisiä ryhmiä, joiden kertaluku on alkuluku.*

5.4. Äärelliset yksinkertaiset ryhmät. Koska jokaisella äärellisellä ryhmällä on kompositiojono, äärellisten ryhmien teoriaa voidaan lähestyä kompositiotekijöiden kautta. Tämä lähestymistapa johtaa kahteen erilliseen kysymykseen: minkälaisia ovat äärelliset yksinkertaiset ryhmät, ja millä tavalla kompositiotekijöistä voidaan saada selville koko ryhmän rakennetta koskevia asioita. Jälkimmäistä kysymystä tutkii niin sanottu *ryhmälaajennosten* teoria. Tarkastellaan erästä tähän liittyvää esimerkkiä.

Esimerkki 5.12. Ryhmillä S_3 ja $\mathbb{Z}_6$ on kompositiojonot

$$S_4 \rhd A_3 \rhd 1 \qquad \text{ja} \qquad \mathbb{Z}_6 \rhd \langle\overline{2}\rangle \rhd 1.$$

Molempien jonojen tekijät ovat C_2 ja C_3. Pelkästään kompositiotekijöistä ei voida siis päätellä, mikä ryhmä on kyseessä. Tässä suhteessa ryhmän kompositiojono poikkeaa kokonaisluvun alkutekijähajotelmasta.

Tekijöiden perusteella voidaan kuitenkin päätellä ryhmästä jotakin. Oletetaan, että ryhmällä G on kompositiojono $G \rhd H \rhd 1$, jonka tekijät ovat C_2 ja C_3. Tämä tarkoittaa sitä, että $H = C_3$ ja $C_3 \lhd G$. Koska $\mathrm{syt}(2,3) = 1$, aliryhmä C_3 ei voi sisältää alkiota, jonka kertaluku on 2. Tällainen alkio kuitenkin löytyy (esimerkiksi Cauchyn lauseen perusteella), joten $C_2 \leq G$ ja $C_2 \cap C_3 = 1$. Nyt on kaksi mahdollisuutta: voi olla $C_2 \lhd G$, jolloin $G \cong C_2 \times C_3 \cong \mathbb{Z}_6$, tai sitten $C_2 \ntrianglelefteq G$.

Vaikka C_2 ei olisi normaali ryhmässä G, niin joka tapauksessa $G = C_2C_3$. Koska C_3 on normaali, tämä rakenne on niin sanottu *puolisuora tulo*. Puolisuorassa tulossa jokainen alkio voidaan esittää yksikäsitteisessä muodossa ab, missä $a \in C_2$ ja $b \in C_3$. Lisäksi mikä tahansa tulo saadaan kaavasta

$$(a_1b_1)(a_2b_2) = (a_1a_2)\left({}^{a_2^{-1}}b_1b_2\right).$$

Koko puolisuoran tulon rakenne riippuu siis tekijöiden rakenteen lisäksi siitä, millä tavalla ensimmäisen ryhmän alkioilla konjugointi toimii toisessa. Triviaali konjugointi johtaa takaisin suoraan tuloon.

Esimerkin tapauksessa ei ole vaikea osoittaa, että mahdollisia epätriviaaleja konjugointeja on vain yksi: jos $1 \neq a \in C_2$ ja $b \in C_3$, niin ${}^a b = b^{-1}$. Ratkaisemalla tästä ryhmän kertotaulu nähdään, että kyseessä on itse asiassa S_3; esimerkiksi ${}^{(12)}(123) = (132)$. Näin on löydetty kaikki mahdolliset ryhmät, joiden kompositiotekijät ovat C_2 ja C_3.

Jos kompositiotekijöiden kertaluvut eivät ole keskenään jaottomia, on myös sellainen vaihtoehto, että ryhmä ei ole lainkaan tekijöidensä tulo. Tästä nähtiin jo aiemmin esimerkki. Tällaisessa tapauksessa ryhmän rakenteen selvittäminen johtaa hankaliin laajennosteoreettisiin kysymyksiin.

Äärellisten yksinkertaisten ryhmien tunteminen on ensiaskel kaikkien äärellisten ryhmien rakenteen selvittämisessä. Tämän askeleen ottamisen aloitti jo Galois todistamalla seuraavan tuloksen.

LAUSE 5.13. *Alternoivat ryhmät A_n ovat yksinkertaisia, kun $n \geq 5$ tai $n = 3$.*

TODISTUS. (Hahmotelma.) Tapaus A_3 on selvä, joten oletetaan, että $n \geq 5$. Tällöin 3-syklien konjugaattiluokka ei jakaudu ryhmässä A_n, joten kaikki 3-syklit ovat keskenään konjugaatteja. Lisäksi, jos $H \trianglelefteq A_n$, niin H sisältää kaikkien alkioidensa konjugaatit. Jos siis H sisältää jonkin 3-syklin, sen täytyy sisältää kaikki 3-syklit. Toisaalta ei ole vaikea nähdä, että 3-syklit virittävät ryhmän A_n, kun $n \geq 3$. Lauseen tulos saadaan nyt käymällä läpi erilaiset mahdolliset syklityypit ja osoittamalla, että jos H sisältää tietyn syklityypin permutaatioita, se sisältää myös jonkin 3-syklin. □

KOROLLAARI 5.14. *Alternoiva ryhmä A_n on ratkeava, jos ja vain jos $n < 5$.*

TODISTUS. Olemme nähneet, että pienet alternoivat ryhmät ovat ratkeavia. Toisaalta, jos $n \geq 5$, niin ryhmän A_5 kompositiojonossa on vain yksi tekijä, ja se ei ole vaihdannainen. □

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. Gorenstein, Lyons ja Solomon ovat aloittaneet projektin, jossa he kokoavat todistusta yksiin kansiin, ja kyseisestä projektista on muodostumassa yksitoistaosainen kirjasarja.

LAUSE 5.15 (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, tai oikeammin näiden ryhmien yksinkertaisia kompositiotekijöitä. Esimerkiksi ortogonaaliset tai unitaariset ryhmät kuuluvat näihin. Poikkeukselliset Lie-tyypin ryhmät ovat samanlaisella konstruktiolla saatavia matriisiryhmiä, mutta niihin liittyvän vektoriavaruuden dimensio on rajoitettu. Sporadiset ryhmät ovat ryhmiä, jotka eivät kuulu mihinkään muista luokista. Niistä suurinta nimitetään "hirviöryhmäksi", ja sen kertaluku on kertaluokkaa $8 \cdot 10^{53}$.

Renkaat ja modulit

Tässä osassa käsiteltävät renkaat ovat vaihdannaisia, ellei toisin mainita.

6. Ideaalit

Kuten aikaisemmin on todettu, tekijärenkaassa nollan ekvivalenssiluokkaa vastaa renkaan *ideaali.* Ideaalin käsitteen otti käyttöön Richard Dedekind (1831–1916), ja se pohjautuu Ernst Kummerin (1810–1893) keksimiin "ideaalisiin lukuihin". Käsitteen synty on siis lukuteoriassa: monissa lukualueissa kokonaislukujen yksikäsitteinen alkutekijöihin jako ei onnistu, mutta toisinaan tämä voidaan korvata jakamalla luvun virittämä ideaali niin sanottuihin alkuideaaleihin.

6.1. Määritelmä ja virittäminen. Ideaali on määritelmän mukaan renkaan additiivisen ryhmän aliryhmä A, jolle pätee $rA = A$ kaikilla renkaan alkioilla r. Jos rengas ei ole vaihdannainen, puhutaan erikseen vasemman- ja oikeanpuoleisista ideaaleista (joille pätee $rA = A$ tai $Ar = A$), ja ideaalilla tarkoitetaan sellaista aliryhmää, joka on sekä vasemman- että oikeanpuoleinen ideaali. Yhdistämällä aliryhmäkriteeri sekä ideaalisuusehto saadaan seuraava tulos.

LAUSE 6.1 (Ideaalisuuskriteeri). *Renkaan R osajoukko A on ideaali, jos ja vain jos*

(I1) $A \neq \emptyset$
(I2) $a - b \in A$ *kaikilla* $a, b \in A$
(I3) $ra \in A$ *kaikilla* $a \in A$ *ja* $r \in R$.

Renkaan osajoukon X virittämä ideaali on pienin ideaali, joka sisältää joukon X, ja sitä merkitään $\langle X \rangle$. Yhden alkion virittämää ideaalia nimitetään *pääideaaliksi.* Pääideaalit ovat aina muotoa $\langle x \rangle = \{rx \mid r \in R\}$.

MÄÄRITELMÄ 6.2. Rengas R on *pääideaalirengas*, jos se on kokonaisalue ja kaikki sen ideaalit ovat pääideaaleja.

Esimerkiksi kokonaislukujen rengas $(\mathbb{Z}, +, \cdot)$ on pääideaalirengas, sillä sen kaikki aliryhmät ovat muotoa $n\mathbb{Z} = \langle n \rangle$. Toinen esimerkki saadaan yhden muuttujan polynomeista, joiden kertoimet ovat kunnassa K. Nämä muodostavat renkaan, jota merkitään $K[X]$. Kyseinen rengas on kokonaisalue, sillä kahden polynomin tulo on nolla, jos ja vain jos jompikumpi tekijöistä on nolla.

LAUSE 6.3. *Polynomirengas $K[X]$ on pääideaalirengas.*

TODISTUS. Oletetaan, että A on renkaan $K[X]$ ideaali. Jos A sisältää jonkin vakiopolynomin $a \neq 0$, niin $a^{-1}a = 1 \in A$, jolloin $A = R = \langle 1 \rangle$. Toisaalta, jos

$A = \{0\}$, niin $A = \langle 0 \rangle$. Voidaan siis olettaa, että $A \neq \{0\}$ ja A ei sisällä nollasta poikkeavia vakiopolynomeja. Valitaan A:sta polynomi $g \neq 0$, jonka aste on pienin mahdollinen (välttämättä siis positiivinen). Jos nyt $f \in A$, niin polynomien jakoalgoritmin perusteella $f = gq + r$, missä r:n aste on pienempi kuin g:n. Toisaalta $r = f - gq \in A$, mutta g:n aste on pienin A:n nollasta poikkeavien polynomien joukossa, joten $r = 0$. Näin ollen $f = gq$, ja koska tämä pätee kaikilla $f \in K[X]$, voidaan päätellä, että $A = \langle g \rangle$. Täten $K[X]$ on pääideaalirengas. $\square$

Useamman kuin yhden muuttujan polynomeille edellinen lause ei päde: esimerkiksi renkaassa $K[X, Y]$ ideaali $\langle X, Y \rangle$ ei ole yhden alkion virittämä, koska X ja Y ovat jaottomia, mutta kumpikaan ei ole toisen tekijä. Lause ei myöskään päde, jos K ei ole kunta: renkaassa $\mathbb{Z}[X]$ ideaali $\langle 2, X \rangle$ ei ole pääideaali. Todistuksessa ongelma tulee vastaan siinä, että vaikka 2 on vakiopolynomi, silti $1 \notin \langle 2, X \rangle$.

6.2. Alkuideaalit ja maksimaaliset ideaalit. Alkuideaalin käsite on keskeinen monissa renkaiden sovelluksissa. Oletetaan seuraavassa, että R rengas ja A sen ideaali.

Määritelmä 6.4. Oletetaan, että $A \neq R$ ja kaikilla $x, y \in R$ pätee:

jos $xy \in A$, niin $x \in A$ tai $y \in A$.

Ideaalia A kutsutaan tällöin *alkuideaaliksi.*

Määritelmä 6.5. Ideaalia A kutsutaan *maksimaaliseksi*, jos $A \neq R$ ja millään ideaalilla B ei päde $A \subsetneq B \subsetneq R$.

Alkuideaalin määritelmä muistuttaa läheisesti kokonaisalueen määritelmää. Yhteys paljastuu seuraavassa lauseessa.

Lause 6.6. *Olkoon R rengas ja A sen ideaali. Tällöin*

(a) *A on alkuideaali, jos ja vain jos tekijärengas R/A on kokonaisalue*
(b) *A on maksimaalinen, jos ja vain jos tekijärengas R/A on kunta.*

Todistus. Harjoitustehtävä. $\square$

Lauseesta saadaan nyt suoraan seuraava tulos.

Korollaari 6.7. *Jokainen maksimaalinen ideaali on alkuideaali.*

Seuraavassa esimerkkejä alkuideaaleista:

- Kokonaislukujen renkaassa ideaali $\langle p \rangle$ on alkuideaali, jos ja vain jos p on alkuluku tai nolla. Toisaalta, jos p on alkuluku, tekijärengas $\mathbb{Z}/\langle p \rangle = \mathbb{Z}_p$ on äärellinen kokonaisalue. Siksi se on kunta, joten ideaali $\langle p \rangle$ on myös maksimaalinen. Siispä ainoa $\mathbb{Z}$:n alkuideaali, joka ei ole maksimaalinen, on nollaideaali $\{0\}$.
- Yleisemmin, pääideaalirenkaassa R jokainen nollasta poikkeava alkuideaali on maksimaalinen. Jos nimittäin $\langle x \rangle \neq \{0\}$ on alkuideaali ja lisäksi $\langle x \rangle \subsetneq \langle y \rangle$, niin $x \in \langle y \rangle$ eli $x = ry$ jollain $r \in R$. Tällöin $ry \in \langle x \rangle$, mutta $y \notin \langle x \rangle$, joten alkuideaalin määritelmän perusteella $r \in \langle x \rangle$. Edelleen

$r = sx$ jollain $s \in R$, joten $x = ry = sxy$ eli $(1 - sy)x = 0$. Koska R on kokonaisalue, nähdään että $sy = 1$, mistä seuraa $R = \langle y \rangle$.

- Polynomirenkaassa $R[X_1, \ldots, X_n]$ pääideaali $\langle f \rangle$ on alkuideaali, jos f on jaoton polynomi.

Todistetaan seuraavaksi tulos, joka varmistaa alkuideaalien riittävän saatavuuden.

LAUSE 6.8 (Krull). *Jokaisella epätriviaalilla renkaalla on maksimaalinen ideaali.*

Lauseen todistus on perusesimerkki *Zornin*[11] *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 ei-mitallisen joukon olemassaoloon tai joukkojen välisten mahtavuuksien vertailuun. Aksiooman mukaan mille tahansa epätyhjien joukkojen kokoelmalle voidaan määritellä kuvaus, joka antaa joukon arvoksi aina jonkin sen sisältämän alkion. Tällaista kuvausta kutsutaan yleensä *valintafunktioksi.* 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-aksiooman on sen naiivin joukko-opin perussäännön vastainen, että jokaisesta alkiosta pitäisi pystyä sanomaan, kuuluuko se annettuun joukkoon vai ei. Muun muassa[12] sen vuoksi on yleensä tapana mainita erikseen, jos todistuksessa nojaudutaan johonkin valinta-aksioomasta riippuvaan tulokseen.

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

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

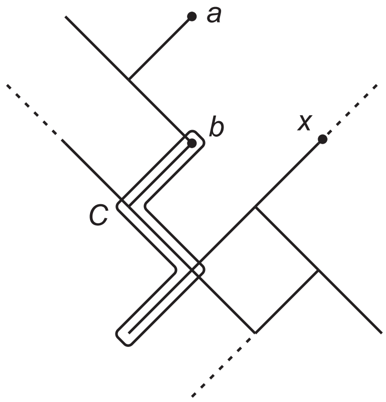
Jos relaatio $\leq$ on transitiivinen ja antisymmetrinen, niin paria $(\mathcal{P}, \leq)$ kutsutaan *osittaisjärjestykseksi.* Jos myös ehto (J3) toteutuu, niin pari on *täydellinen järjestys* eli *lineaarijärjestys.* Jos sekaannuksen vaaraa ei ole, osittaisjärjestykseksi tai lineaariseksi järjestykseksi 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 $m \leq a$.

LEMMA 6.9 (Zornin lemma). *Oletetaan, että $\mathcal{P}$ on epätyhjä osittaisjärjestys, jossa jokaisella ketjulla on yläraja. Tällöin $\mathcal{P}$ sisältää maksimaalinen alkion.*

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

[12] 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.

Todistus. Zornin lemma on yhtäpitävä joukko-opillisen valinta-aksiooman kanssa. Tämän todistus sivuutetaan (ks. esim. Enderton: Elements of Set Theory). □



Kuva 13. Osa erästä osittaisjärjestystä. Tässä järjestyksessä pätee $b \leq a$, mutta alkiota x ei voi vertailla a:n tai b:n kanssa. Sekä a että b ovat molemmat ketjun C ylärajoja, ja a on maksimaalinen alkio.

Lauseen 6.8 todistus. Olkoon R epätriviaali rengas. Tarkastellaan kaikkien R:n aitojen ideaalien muodostamaa kokoelmaa $\mathcal{P}$. Tämä on osittaisjärjestys sisältymisrelaation $\subset$ suhteen. Lisäksi $\mathcal{P}$ on epätyhjä, koska se sisältää vähintään nollaideaalin $\{0\}$. Osoitetaan, että jokaisella ketjulla on yläraja tässä osittaisjärjestyksessä.

Olkoon $\mathcal{A}$ jokin ketju. Selvästi jokainen $\mathcal{A}$:n alkio sisältyy yhdisteeseen $\cup\mathcal{A}$, joten riittää osoittaa, että $\cup\mathcal{A} \in \mathcal{P}$ eli että $\cup\mathcal{A}$ on aito ideaali. Ensinnäkin se on epätyhjä, koska $0 \in \{0\} \in \mathcal{A}$. Oletetaan, että $r \in R$ ja $a, b \in \cup\mathcal{A}$. 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 $a - b \in B$ ja $ra \in B$. Näin ollen

$$a - b \in \cup\mathcal{A} \qquad \text{ja} \qquad ra \in \cup\mathcal{A},$$

joten ideaalikriteerin perusteella $\cup\mathcal{A}$ on ideaali. Lisäksi $\cup\mathcal{A} \neq R$, koska kaikilla $B \in \mathcal{P}$ pätee $1 \notin B$. Yhdiste $\cup\mathcal{A}$ on siis eräs ketjun $\mathcal{A}$ yläraja.

Zornin lemman perusteella joukossa $\mathcal{P}$ on maksimaalinen alkio, joka on samalla haluttu maksimaalinen ideaali. □

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

Korollaari 6.10. *Jos $A \neq \{0\}$ on renkaan R ideaali, niin on olemassa R:n maksimaalinen ideaali, joka sisältää A:n.*

Jos rengas R ei ole vaihdannainen, alkuideaalin määritelmä muuttuu hieman. Tässä tapauksessa sanotaan, että ideaali A on alkuideaali, jos $A \neq R$ ja kaikilla ideaaleilla B ja C pätee

$$BC \subset A \quad \Rightarrow \quad B \subset A \quad \text{tai} \quad C \subset A.$$

Tämä ehto voidaan lausua alkioiden avulla niin, että jos $bRc \subset A$, niin $b \in A$ tai $c \in A$, kun b ja c ovat mitä tahansa renkaan R alkioita. Vaihdannaisella renkaalla tämä palautuu aiempaan määritelmään, sillä jos $bc \in A$, niin $brc = bcr \in A$ kaikilla $r \in R$.

6.3. Jakorenkaat ja lokalisointi. Jakorengas on rengas, johon on lisätty käänteisalkioita, jotta jakolasku tulisi mahdolliseksi. Menetelmä tuli osin tutuksi jo erotusmonoidiesimerkin 1.5 yhteydessä. Tällä kertaa tarkastellaan yleisempää tapausta, jossa käänteisalkiot lisätään vain valituille alkioille.

Olkoon R vaihdannainen rengas ja S jokin kertolaskun suhteen suljettu osajoukko, joka sisältää ykkösalkion. Tarkoitus on lisätä renkaaseen R kaikkien S:n alkioiden käänteisalkiot. Tarkastellaan karteesisen tulon $R \times S$ (joka ei yleensä itse ole rengas) kaksipaikkaista relaatiota

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

Tämä on sama ekvivalenssirelaatio kuin erotusmonoidiesimerkissä, nyt vain kirjoitettu eri muotoon renkaan laskutoimitusten avulla. Tekijärakennetta $(R \times S)/\sim$ nimitetään renkaan *jakorenkaaksi joukon S suhteen* ja merkitään $S^{-1}R$. Jakorenkaan alkiota $[(a, b)]_\sim$ voidaan merkitään murtolukumuodossa a/b. Jakorenkaaseen liittyy kanoninen kuvaus $\eta : R \to S^{-1}R$, missä $a \mapsto a/1$.

Lause 6.11. *Seuraavat väitteet pätevät renkaan R jakorenkaalle $S^{-1}R$:*

(a) *$S^{-1}R$ on vaihdannainen rengas, laskutoimituksina $a/b \cdot c/d = (ac)/(bc)$ ja $a/b + c/d = (ad + bc)/(bd)$.*
(b) *Kanoninen kuvaus η on rengashomomorfismi.*
(c) *Jos $s \in S$, kuva-alkiolla $\eta(s) \in S^{-1}R$ on käänteisalkio.*
(d) *Kanoninen kuvaus η on injektio, jos ja vain jos S ei sisällä nollanjakajia.*
(e) *$S^{-1}R$ on nollarengas, jos ja vain jos $0 \in S$.*

Todistus. Harjoitustehtävä. □

Edellisestä lauseesta seuraa erityisesti, että jos $S = R \setminus \{0\}$, jakorengas $S^{-1}R$ on kunta. Jos lisäksi R on kokonaisalue, kuntaa $S^{-1}R$ nimitetään R:n *osamääräkunnaksi*. Esimerkiksi $\mathbb{Q}$ on $\mathbb{Z}$:n osamääräkunta.

Ryhdytään seuraavaksi tarkastelemaan jakorenkaisiin liittyvää prosessia, jota nimitetään renkaan *lokalisoinniksi*.

Määritelmä 6.12. Rengasta, jolla on vain yksi maksimaalinen ideaali, kutsutaan *lokaaliksi* tai *paikalliseksi* renkaaksi.

Alkuideaalin avulla voidaan tuottaa paikallinen jakorengas.

Lause 6.13 (Lokalisointi). *Olkoon R rengas ja P sen jokin alkuideaali. Tällöin $S = R \setminus P$ on kertolaskun suhteen suljettu joukko, joka sisältää ykkösalkion, ja jakorengas $R_P = S^{-1}R$ on paikallinen rengas.*

Todistus. Koska $P \neq R$, nähdään että $1 \in S$. Olkoot $a, b \in S$. Jos tulo ab ei olisi joukossa S, se kuuluisi alkuideaaliin P. Alkuideaalin määritelmän mukaan joko $a \in P$ tai $b \in P$, mikä on mahdotonta. Täten S on kertolaskun suhteen suljettu.

Osoitetaan sitten, että joukko $M = \{a/b \mid a \in P, b \in S\}$ on ideaali renkaassa R_P. Koska $0 \in P$, nähdään että $M \neq \emptyset$. Olkoot sitten $a/b, c/d \in M$ ja $r/s \in R_P$. Tällöin $ac - bd \in P$, koska P on ideaali, ja $bd \in S$, koska S on kertolaskun suhteen suljettu. Näin ollen

$$\frac{a}{b} - \frac{c}{d} = \frac{ac - bd}{bd} \in M.$$

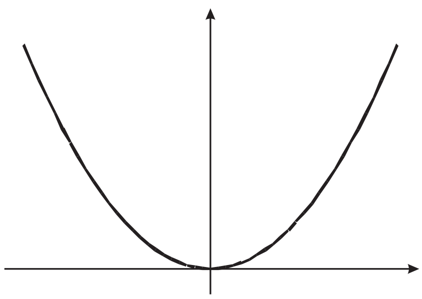
Samoin $ra \in P$ ja $sb \in S$, joten

$$\frac{r}{s} \cdot \frac{a}{b} = \frac{ra}{sb} \in M.$$

Ideaalikriteerin perusteella M on ideaali.

Näytetään lopuksi, että M on renkaan R_P ainoa maksimaalinen ideaali. Jos $A \not\subset M$ jollain ideaalilla A, niin löytyy alkio $a/b \in A \setminus M$. Tällöin $a \notin P$, joten $a \in S$, mistä seuraa, että a/b on kääntyvä alkio renkaassa R_P. Koska ideaali A sisältää kääntyvän alkion, se sisältää automaattisesti myös ykkösalkion, ja on siksi koko rengas. Tästä seuraa, että jokainen aito ideaali sisältyy ideaaliin M, joten M on ainoa maksimaalinen ideaali. □

Esimerkki 6.14. Lokalisointi-nimitys tulee algebrallisesta geometriasta. Tarkastellaan reaalikertoimisen polynomin $p = X^2 - Y$ nollakohtien joukkoa tasossa. Tämä joukko on paraabelin muotoinen algebrallinen käyrä. Koska f on jaoton renkaassa $\mathbb{R}[X,Y]$, sen virittämä ideaali $\langle p \rangle$ on alkuideaali. Lokalisoimalla voidaan muodostaa paikallinen rengas $\mathbb{R}[X,Y]_{\langle p \rangle}$. Se koostuu rationaalifunktioista f/g, missä f ja g ovat polynomeja ja $g \notin \langle p \rangle$.



Kuva 14. Polynomin $X^2 - Y$ nollakohtien joukko on paraabeli.

Renkaalla $\mathbb{R}[X,Y]_{\langle p \rangle}$ on sellainen ominaisuus, että sen sisältämät funktiot ovat määriteltyjä melkein kaikissa paraabelin pisteissä. Nimittäin, olkoon g sellainen polynomi, että $g(x,y) = 0$ äärettömän monessa paraabelin pisteessä. Tällöin voidaan osoittaa muun muassa, että g saa arvon nolla kaikissa paraabelin pisteissä ja että p jakaa polynomin g. Näin ollen $g \in \langle p \rangle$, joten kaikilla f pätee $f/g \notin \mathbb{R}[X,Y]_{\langle p \rangle}$. Voidaan ajatella, että lokalisoinnin avulla huomio on keskitetty kaikkien rationaalifunktioiden sijaista sellaiseen alueeseen, jonka funktiot on määritelty melkein koko paraabelilla. Vastaava konstruktio toimii myös korkeammissa ulottuvuuksissa.

Jos rengas ei ole vaihdannainen, tämän luvun menetelmät eivät sovellu sellaisinaan käytettäviksi. Itse asiassa ei ole edes selvää, että epävaihdannaisen renkaan alkioille ylipäätään voidaan lisätä käänteisalkioita. Jakorengas-nimitystä käytetään kuitenkin myös epävaihdannaisessa tapauksessa sellaisesta renkaasta, jossa jakolasku on mahdollinen. Tällaista rakennetta voidaan toisaalta ajatella epävaihdannaisena kuntana, ja silloin sitä nimitetään *vinokunnaksi*.

7. Modulit

Vektoriavaruudet ovat vaihdannaisia ryhmiä, joissa on määritelty jonkin kunnan skalaaritoiminta. Hyväksymällä kerroinrakenteeksi rengas kunnan sijaan rakenne nimeltä *moduli*. Modulin käsite on siis vektoriavaruuden yleistys, mutta modulien teoria poikkeaa melko paljon vektoriavaruuksien teoriasta. Yleisellä modulilla ei esimerkiksi välttämättä ole kantaa, ja vaikka olisikin, kannan pituus ei ole välttämättä yksikäsitteinen, jolloin dimensiota käsitettä ei voida määritellä. Toisaalta jokaiselle vaihdannaiselle ryhmälle voidaan määritellä luonnollinen modulirakenne, ja siksi modulien teoria on myös suurelta osin vaihdannaisten ryhmien teoriaa.

7.1. Modulit ja lineaarikuvaukset.

MÄÄRITELMÄ 7.1. Olkoon R rengas. Vaihdannaista ryhmää $(M,+)$, jossa on määritelty renkaan R toiminta, nimitetään *moduliksi*. Renkaan toiminta on renkaan kertolaskumonoidin $(R,\cdot)$ toiminta, joka toteuttaa seuraavat ehdot 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 *kerroinrenkaaksi*, ja sen toimintaa *skalaarikertolaskuksi.*

Aksioomat (M1) ja (M2) määrittelevät kertolaskumonoidin toiminnan, ja loput aksioomat määrittävät, miten renkaan ja modulin yhteenlaskut suhtautuvat tuohon toimintaan. Modulin aksioomista voidaan helposti johtaa tuttuja laskusääntöjä, kuten $0.x = 0$, $(-1).x = -x$ jne. Yleensä toimintaa merkitään yksinkertaisesti kertolaskuna jättämällä alkioiden välistä piste pois.

Tässä määritelty renkaan toiminta on oikeastaan renkaan *vasen* toiminta, ja siksi tällaista modulia nimitetään joskus *vasemmaksi* R-moduliksi. Vastaavasti voitaisiin määritellä oikeat modulit renkaan oikean toiminnan avulla.

Esimerkkejä moduleista:

- Jos K on kunta, jokainen K-vektoriavaruus on samalla K-moduli, sillä modulin aksioomat ovat täsmälleen samat kuin vektoriavaruuden aksioomat.
- Rengas R on itse R-moduli, kun skalaarikertolaskuksi otetaan renkaan oma kertolasku.
- Jokainen vaihdannainen ryhmä on $\mathbb{Z}$-moduli, kun skalaarikertolaskuksi määritellään monikerran ottaminen: $n.x = nx = x + \cdots + x$ (n kertaa). Tämä on itse asiassa ainoa tapa, jolla $\mathbb{Z}$ voi toimia vaihdannaisessa ryhmässä, sillä $\mathbb{Z}$ on additiivisena ryhmänä alkion 1 virittämä, jolloin toiminta määräytyy täysin aksioomista (M1) ja (M3).
- Jäännösluokkarenkaiden $\mathbb{Z}_n$ toiminta ryhmässä M on myös yksikäsitteisesti määrätty: $[k]_n.x = kx$ (monikerta). Jotta tällainen toiminta olisi hyvin määritelty, täytyy ryhmässä M päteä $nx = 0$, eli jokaisen alkion

kertaluvun täytyy jakaa luku n. 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 vektoriavaruus.

- Olkoon K kunta. K-kertoimiset $n \times n$-matriisit muodostavat renkaan $M_n(K)$, joka ei ole vaihdannainen. Tämä rengas toimii matriisikertolaskulla vasemmalta sarakevektorien avaruudessa K^n ja oikealta vastaavassa rivivektorien avaruudessa. Vektoriavaruutta K^n voidaan siis tarkastella joko vasempana tai oikeana $M_n(K)$-modulina.
- Renkaan R ideaalit ovat R-moduleja, kun kertolaskuna on renkaan oma kertolasku. Ideaalit ovat samalla rengasmodulin R alimoduleja (määritelmä seuraa).

Olkoot M ja N jotain R-moduleja. Kuvausta $f : M \to N$ 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 ryhmähomorfismin ydin, eli nollan alkukuva.

Kaikkien R-modulihomomorfismien $M \to N$ joukko on itse R-moduli, jos laskutoimitukset määritellään pisteittäin:

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

Tätä modulia merkitään $\mathrm{Hom}_R(M, N)$, tai jos kerroinrengas on selvä asiayhteydestä, yksinkertaisemmin $\mathrm{Hom}(M, N)$.

7.2. Ali- ja tekijämodulit. R-modulin M *alimoduli* N on ryhmän M aliryhmä, joka on vakaa kertolaskutoiminnan suhteen. Kaikilla $x, y \in N$ ja $a \in R$ täytyy siis päteä

(AM1) $N \neq \emptyset$
(AM2) $x - y \in N$
(AM3) $a.x \in N$.

Ehdot (AM1) ja (AM2) tulevat aliryhmäkriteeristä. Ehdoista (AM1) ja (AM3) seuraa $0 = 0.x \in N$ jollain $x \in N$.

Mielivaltaisten alimodulien leikkaus on aina alimoduli. Lineaarikuvausten kuvat ja ytimet ovat myös alimoduleja.

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

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

Tämä määritelmä on additiivinen versio aliryhmien tulon määritelmästä. Koska modulit ovat vaihdannaisia ryhmiä, alimodulien summa on aina aliryhmä. Se on samalla pienin aliryhmä, joka sisältää summattavansa, eli $A + B = \langle A \cup B \rangle$. Lisäksi alimodulien summa on itse alimoduli, koska $r(a + b) = ra + rb \in A + B$ kaikilla $a \in A$ ja $b \in B$.

Summaa voidaan yleistää äärettömän monelle alimodulille edellä mainitun viritysominaisuuden avulla. Olkoon $(M_i)_{i\in I}$ perhe[13] 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, jotka sisältyvät johonkin alimoduleista M_i. Sen alkiot ovat siis muotoa $\sum_{i\in I} x_i$, missä $x_i \in M_i$ kaikilla i, ja $x_i = 0$ lukuunottamatta äärellistä määrää indeksejä i. Alimodulien yleinen summa on aina alimoduli.

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

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

on automaattisesti hyvin määritelty. Jos nimittäin $x = y + n$ jollain $n \in N$, niin $ax = ay + an \in ay + N$, sillä $an \in N$. Tekijämodulia merkitään tavalliseen tapaan M/N.

Tekijämoduleille pätee samanlainen homomorfialause kuin ryhmille ja renkaille. Lisäksi Noetherin isomorfialauseet pätevät myös modulien tapauksessa.

7.3. Modulien suorat summat ja tulot. Useimpien algebrallisten rakenteiden tapauksessa kahden rakenteen karteesinen tulo on myös samantyyppinen rakenne (kunnat ovat poikkeus tästä). 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 $(m_1, m_2, \dots, m_n)$, missä $m_i \in M_i$ kaikilla i. Äärettömän indeksijoukon tapauksessa suoran summan määritelmä poikkeaa karteesisen tulon määritelmästä. Molemmat ovat kuitenkin R-moduleja, ja jälkimmäistä nimitetään *suoraksi tuloksi.*

MÄÄRITELMÄ 7.2. 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 $\prod_{i\in I} M_i$.

Suoraan tuloon liittyvät *kanoniset projektiokuvaukset* $\pi_j : \prod_{i\in I} M_i \to M_j$, joille pätee $\pi_j(x) = x_j$. Projektiokuvaukset ovat modulihomomorfismeja.

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

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

Määritelmä 7.3. 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.* Suoraan summaan liittyvät *kanoniset injektiot* $\iota_j : M_j \to \bigoplus_{i\in I} M_i$, missä $\iota_j(y) = (x_i)_{i\in I}$ ja

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

Esimerkiksi jos indeksijoukko on $I = \{1,2,3,4\}$ ja $a \in M_2$, voidaan kirjoittaa $\iota_2(a) = (0,a,0,0)$. Kanoniset injektiot ovat modulihomomorfismeja. Jokainen suoran summan alkio (x_i) voidaan kirjoittaa muodossa $\sum_i \iota_i(x_i)$. Tämä summa on äärellinen (oikeammin äärelliskantajainen), koska $x_i = 0$ äärellistä indeksijoukkoa lukuunottamatta. Kanonisille injektioille pätee seuraava lause, jota nimitetään suoran summan *universaaliominaisuudeksi.*

Lause 7.4. *Olkoon (M_i) 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 $\theta : \bigoplus_i M_i \to N$, jolle pätee*

$$\varphi_i = \theta \circ \iota_i \tag{7.5}$$

kaikilla i, eli seuraava kaavio kommutoi:

$$\begin{tikzcd} M_i \arrow[rr, "\varphi_i"] \arrow[dr, "\iota_i"'] & & N \\ & \bigoplus_i M_i \arrow[ur, dashed, "\theta"'] & \end{tikzcd}$$

Todistus. Jokainen suoran summan alkio $x = (x_i)$ voidaan kirjoittaa muodossa $x = \sum_i \iota_i(x_i)$. Näin ollen, mikäli θ toteuttaa ehdon (7.5), täytyy kaikilla $x \in \bigoplus_i M_i$ päteä

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

Tämä kaava määrittelee kuvauksen θ yksikäsitteisesti.

Osoitetaan sitten, että yllä määritelty θ toteuttaa lauseessa mainitut ehdot. On helppo nähdä, että θ on R-lineaarinen. Lisäksi, jos $y \in M_j$, niin $(\iota_j(y))_i = 0$ kaikilla $i \neq j$. Täten kaikilla j pätee

$$\theta(\iota_j(y)) = \sum_i \varphi_i\big((\iota_j(y))_i\big) = \varphi_j(y),$$

eli kuvaus θ toteuttaa ehdon (7.5). $\square$

Universaalisuudella tarkoitetaan sitä, että aina kun käsillä on perhe lineaarikuvauksia johonkin tiettyyn moduliin, tämä perhe voidaan korvata yhdellä kuvauksella suorasta summasta kyseiseen moduliin. Modulien suora summa on ikäänkuin "universaali" lineaarikuvausperhe (ι_i), joka voidaan täydentää lineaarikuvauksella θ vastaamaan mitä tahansa lineaarikuvausperhettä (φ_i). Vastaavanlainen tulos pätee myös suoralle tulolle.

Lause 7.6. *Olkoon (N_i) 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 $\theta : M \to \prod_i N_i$, jolle pätee $\varphi_i = \pi_i \circ \theta$ kaikilla i, eli oheinen kaavio kommutoi.*

$$\begin{tikzcd} M \arrow[rr, "\varphi_i"] \arrow[dr, dashed, "\theta"'] & & N_i \\ & \prod_i N_i \arrow[ur, "\pi_i"'] & \end{tikzcd}$$

Todistus. Sivuutetaan. □

Ryhmiä tutkittaessa oli hyödyllistä tietää, milloin tietty ryhmä sattui olemaan isomorfinen jonkin tuloryhmän kanssa. Koska modulit ovat vaihdannaisia ryhmiä, myös moduleille saadaan vastaava tulos.

Lause 7.7. *Olkoon $(M_i)_{i\in I}$ perhe R-modulin M alimoduleja. Jos $\sum_i M_i = M$ ja $M_i \cap \sum_{j\neq i} M_j = \{0\}$ kaikilla i, niin M on isomorfinen suoran summan $\bigoplus_i M_i$ kanssa.*

Todistus. Jokaisella i voidaan määritellä inkluusiokuvaus $\varphi_i : M_i \to M$, missä $\varphi_i(x) = x$. Suoran summan universaalisuusominaisuuden perusteella löytyy R-lineaarinen kuvaus $\theta : \bigoplus_i M_i \to M$, jolle pätee $\theta(\iota_i(x)) = \varphi_i(x) = x$ kaikilla i ja $x \in M_i$. Osoitetaan, että θ on bijektio.

$$\begin{tikzcd} M_i \arrow[rr, "\varphi_i"] \arrow[dr, "\iota_i"'] & & \sum_i M_i \\ & \bigoplus_i M_i \arrow[ur, "\theta"'] & \end{tikzcd}$$

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 $\theta(x) = \theta(y)$ joillain $x, y \in \bigoplus_i M_i$. Tämä tarkoittaa sitä, että $\sum_i x_i = \sum_i y_i$, eli toisin sanoen $\sum_i (x_i - y_i) = 0$. Edelleen, jokaisella i pätee

$$(x_i - y_i) = -\sum_{i\neq j}(x_j - y_j).$$

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 erityisesti

$x_i - y_i = 0$. Koska tämä pätee kaikilla i, saadaan $x_i = y_i$ kaikilla i, joten $x = y$. Tämä todistaa injektiivisyyden. $\square$

Huomautus. Ryhmäteoriassa vaihdannaisten ryhmien $(G_i, +)$ suora summa konstruoidaan samalla tavoin kuin modulien suora summa. Suoraksi tuloksi kuitenkin nimitetään täsmälleen samaa konstruktiota siinä tapauksessa, että ryhmän laskutoimitusta merkitään multiplikatiivisesti. Kummassakin rakenteessa siis alkioina ovat perheet (g_i), joissa $g_i = 0$ lukuunottamatta äärellistä määrää indeksejä. Jos viimeksi mainittu rajoitus jätetään pois (kuten modulien suorassa tulossa), ryhmien tuloa tai summaa kutsutaan *rajoittamattomaksi* suoraksi tuloksi tai summaksi.

8. Modulikonstruktioita

8.1. Vapaat modulit. Vektoriavaruuden tärkeimpiä ominaisuuksia on, että sen vektorit voidaan ilmaista yksikäsitteisesti kantavektorien yhdistelminä. Tässä luvussa tarkastellaan moduleja, joilla on vastaava ominaisuus.

Olkoon X osajoukko R-modulissa M. Mitä tahansa äärellistä summaa $\sum_i r_i x_i$, missä $r_i \in R$ ja $x_i \in X$ kaikilla i, kutsutaan joukon X *lineaarikombinaatioksi.* Jos jokainen modulin M alkio voidaan ilmaista joukon X lineaarikombinaationa, sanotaan, että X *virittää* modulin M. Edelleen, jos kullakin lineaarikombinaatiolla pätee $\sum_i r_i x_i = 0$ ainoastaan siinä tapauksessa, että $r_i = 0$ kaikilla i, sanotaan, että osajoukko X on *lineaarisesti riippumaton* eli *vapaa.* Jos osajoukko ei ole vapaa, se on *sidottu.*

MÄÄRITELMÄ 8.1. Olkoon M jokin R-moduli. Osajoukkoa $B \subset M$ kutsutaan modulin M *kannaksi*, jos B virittää modulin M ja on lineaarisesti riippumaton. Tällöin modulia M kutsutaan *vapaaksi.*

Vapaassa modulissa jokainen alkio voidaan esittää kannan 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 joukko B on vapaa, tästä seuraa, että $r_i = r_i'$ kaikilla i.

Esimerkkejä vapaista moduleista:

- Lineaarialgebran peruskurssilla on osoitettu, että jokaisella äärellisellä $\mathbb{R}$-vektoriavaruudella on kanta, joten jokainen tällainen vektoriavaruus on vapaa $\mathbb{R}$-moduli. Sama todistus pätee millä tahansa kerroinkunnalla. Myös äärettömillä vektoriavaruuksilla on kanta, mutta sen todistamiseen tarvitaan Zornin lemmaa.
- Mikä tahansa rengas R on vapaa R-moduli, kantana yksiö $\{1\}$. Yleisemmin, tulomoduli R^n on vapaa, ja sen luonnollinen kanta koostuu alkioista $e_i = (0, \dots, 0, 1, 0, \dots, 0)$ (ykkösalkio i:nnellä paikalla).
- Vaihdannaista ryhmää kutsutaan vapaaksi, jos se on vapaa $\mathbb{Z}$-modulina. $\mathbb{Q}$ ei ole vapaa ryhmä. Myöskään $\mathbb{Z}_n$ ei ole vapaa, mikä seuraa erityisesti myöhemmin todistettavasta lauseesta 8.4. Tuo lause osoittaa, että jokainen vapaa ryhmä on isomorfinen ryhmien $\mathbb{Z}$ suoran summan kanssa; erityisesti jokainen vapaa ryhmä on ääretön.

Vapaisiin moduleihin liittyy seuraava universaaliominaisuus. Sen mukaan jokainen vapaassa modulissa määritelty lineaarikuvaus määräytyy täysin kannan alkioiden kuvien perusteella.

LAUSE 8.2. *Olkoon M vapaa R-moduli, jolla on kanta B, ja olkoon $\iota : B \to M$ inkluusiokuvaus. Oletetaan lisäksi, että N on jokin toinen R-moduli ja $f : B \to N$ on mikä tahansa kuvaus. Tällöin on olemassa yksikäsitteinen R-lineaarinen kuvaus $\varphi : M \to N$, jolle pätee $f = \varphi \circ \iota$, eli oheinen kaavio kommutoi.*

$$\begin{tikzcd} B \arrow[rr, "f"] \arrow[dr, hook, "\iota"'] & & N \\ & M \arrow[ur, dashed, "\varphi"'] & \end{tikzcd}$$

Lisäksi

i) φ *on injektiivinen, jos ja vain jos kuvajoukko* fB *on vapaa*
ii) φ *on surjektiivinen, jos ja vain jos kuvajoukko* fB *virittää modulin* N.

TODISTUS. Jokaisella vapaan modulin alkiolla on yksikäsitteinen esitys kannan alkioiden lineaarikombinaationa. Määritellään $\varphi : M \to N$ kaavalla

$$\sum_i r_i b_i \;\mapsto\; \sum_i r_i f(b_i). \tag{8.3}$$

On helppo nähdä, että näin saatu kuvaus on R-lineaarinen ja että $\varphi(b) = f(b)$ kaikilla kannan alkioilla b. Yksikäsitteisyys seuraa siitä, että lineaarikuvauksen on kuvattava lineaarikombinaatiot juuri kaavan (8.3) määräämällä tavalla.

Muiden väitteiden todistaminen jätetään harjoitustehtäväksi. □

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

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

Kannan alkiot ovat siis ykkösalkion kuvia kanonisissa injektioissa $\iota_i : R \to \bigoplus_i R$. Osoittautuu, että kaikki vapaat modulit ovat isomorfisia tällaisen suoran summan kanssa.

LAUSE 8.4. *Jos* M *on vapaa* R*-moduli, niin* $M \cong R^{(I)}$ *jollain* I.

TODISTUS. Olkoon $B = \{b_i\}_{i\in I}$ vapaan modulin M kanta. Määritellään kuvaus $f : B \to R^{(I)}$ kaavalla $f(b_i) = e_i$. Universaaliominaisuuden 8.2 nojalla on olemassa R-lineaarinen kuvaus $\varphi : M \to R^{(I)}$, jolle pätee $\varphi(b_i) = e_i$ kaikilla i. Saman lauseen loppuosan perusteella φ on bijektiivinen, koska joukko $\{e_i\}$ on modulin $R^{(I)}$ kanta. □

Nyt vapaan modulin universaaliominaisuus voidaan tulkita uudella tavalla: Jokaista joukkoa I kohti voidaan konstruoida "universaali" R-moduli $R^{(I)}$. Tässä modulissa joukon I alkio i samastetaan yleensä luonnollisen kannan alkion e_i kanssa. Tällöin mikä tahansa kuvaus f joukolta I johonkin R-moduliin N voidaan laajentaa homomorfismiksi $\varphi : R^{(I)} \to N$.

ESIMERKKI 8.5. Olkoon R rengas, ja X jokin joukko. Samastetaan kukin alkio $x \in X$ vapaan modulin $R^{(X)}$ kanta-alkion e_x kanssa. Tällöin vapaan modulin alkiot voidaan kirjoittaa formaalin lineaarikombinaation muodossa

$$\sum_x r_x x = \sum_x r_x e_x.$$

Tällä tavoin minkä tahansa joukon X päälle voidaan konstruoida modulirakenne, jota kutsutaan *joukon* X *virittämäksi vapaaksi moduliksi.*

Erityisesti, jos $R = \mathbb{Z}$ ja $n \in R$, alkiota nx voidaan pitää x:n formaalina monikertana. Tällä tavoin saadaan joukon X virittämä vapaa vaihdannainen ryhmä. Tässä ryhmässä joukon X alkioita voidaan lisätä yhteen ja vähentää toisistaan.

Esimerkiksi algebrallisessa topologiassa törmätään tilanteeseen, jossa joukko X koostuu jonkin topologisen avaruuden eräänlaisista yleistetyistä kolmioista (tarkemmin sanoen kolmioiden ja niiden n-ulotteisten vastineiden kuvista jatkuvissa kuvauksissa). Vapaassa ryhmässä $\mathbb{Z}^{(X)}$ voidaan näistä kolmioista luoda erilaisia lineaarikombinaatioita. Tämän ryhmän rakennetta tutkimalla saadaan tietoa avaruuden rakenteesta.

8.2. Tensoritulot. Monet 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

$$(x+y) \otimes z = x \otimes z + y \otimes z, \qquad (ax) \otimes y = a(x \otimes y)$$

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

Esimerkiksi tavallinen pistetulo $x \cdot y$ ja kolmiulotteisen reaaliavaruuden ristitulo $x \times y$ ovat bilineaarisia tuloja. Seuraavassa yleistetään bilineaarisen tulon käsite mielivaltaisille moduleille, ja tarkastellaan modulien *tensorituloa*, jossa voidaan määritellä eräänlainen universaali bilineaarinen tulo.

Määritelmä 8.6. Olkoot M, N ja P kolme R-modulia. Kuvausta f joukolta $M \times N$ moduliin P kutsutaan R-*bilineaariseksi*, 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 bilineaarinen kuvaus $\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$. Yleisessä tapauksessa modulien M ja N ei kuitenkaan tarvitse olla samat. Huomaa, että bilineaarisessa kuvauksessa pätevät kaavat $f(x, 0) = 0$ ja $f(0, y) = 0$, sillä esimerkiksi $f(x, 0) = f(x, 0.0) = 0.f(x, 0) = 0$.

Olkoot M ja N mielivaltaisia R-moduleja. Ryhdytään konstruoimaan modulia T, jolle voidaan määritellä bilineaarinen kuvaus $M \times N \to T$, $(x, y) \mapsto x \otimes y$. Ideana on lähteä liikkeelle modulista, jonka alkioita ovat parien (x, y) muodostamat lineaarikombinaatiot. Näitä pareja voidaan pitää muodollisina tuloina. Sen jälkeen samastetaan alkioita niin, että bilineaarisuusehdot täyttyvät: esimerkiksi jokainen pari $(x+y, z)$ samastetaan lineaarikombinaation $(x, z) + (y, z)$ kanssa.

Olkoon C vapaa R-moduli $R^{(M \times N)}$. 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 C:n alimoduli, jonka virittävät yllä mainitut lineaarikombinaatiot.

MÄÄRITELMÄ 8.7. R-modulien M ja N *tensoritulo* $M \otimes_R N$ on tekijämoduli C/D, missä $C = R^{(M\times N)}$ ja D on edellä määritelty alimoduli. Jos kerroinrengas on asiayhteydestä selvä, tensorituloa voidaan merkitä myös $M \otimes N$.

Parin (x, y) ekvivalenssiluokkaa tekijämodulissa C/D merkitään $x \otimes y$. (Tämä on oikeastaan perheen $e_{(x,y)}$ ekvivalenssiluokka, mutta tämä perhe samastettiin parin (x, y) kanssa.) Koska parit (x, y) virittävät vapaan modulin C, niiden ekvivalenssiluokat virittävät modulin C/D. Jokainen tensoritulon $M \otimes N$ alkio voidaan siis esittää alkioiden $x \otimes y$ lineaarikombinaationa. Tensorituloon liittyy kanoninen kuvaus $\eta : M \times N \to M \otimes N$, jolle pätee $\eta(x, y) = x \otimes y$. Kanoninen kuvaus on R-bilineaarinen.

ESIMERKKI 8.8. 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 $am+bn = 1$. Tällöin alkiolle $\overline{x} \otimes \overline{y} \in \mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n$ pätee

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

Koska tensoritulon jokainen virittäjäalkio on nolla, tensoritulo on triviaali moduli.

Tensoritulon ominaisuuksia todistettaessa ei ole yleensä tarpeellista palata tensoritulon määritelmään, vaan voidaan käyttää seuraavaa universaaliominaisuutta.

LAUSE 8.9. *Olkoot M, N ja P jotain R-moduleja, ja olkoon $f : M \times N \to P$ jokin R-bilineaarinen kuvaus R-modulille P. Tällöin on olemassa yksikäsitteinen R-lineaarinen kuvaus $\varphi : M \otimes_R N \to P$, jolle pätee $\varphi(x \otimes y) = f(x, y)$ kaikilla $x \in M$ ja $y \in N$, eli oheinen kaavio kommutoi.*

$$\begin{tikzcd} M \times N \arrow[rr, "f"] \arrow[dr, "\eta"'] & & P \\ & M \otimes_R N \arrow[ur, dashed, "\varphi"'] & \end{tikzcd}$$

TODISTUS. Koska parit (x, y), missä $x \in M$ ja $y \in N$, muodostavat vapaan modulin $C = R^{(M\times N)}$ kannan, kuvaus f voidaan laajentaa lineaarikuvaukseksi $g : C \to P$ 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 D:n virittäjällä u, niin $D \subset \operatorname{Ker} f$. Siispä on olemassa yksikäsitteinen R-modulien homomorfismi $\varphi : C/D \to P$, jolle pätee $g = \varphi \circ \pi$, missä π on kanoninen surjektio. Nyt kaikilla $(x, y) \in M \times N$ pätee $x \otimes y = \pi(x, y)$, joten

$$\varphi(x \otimes y) = \varphi(\pi(x, y)) = g(x, y) = f(x, y).$$

□

$$
\begin{tikzcd}
M \times N \arrow[r, "f"] \arrow[d, "\iota"'] & P \\
C \arrow[r, "\pi"'] \arrow[ur, dashed, "g"] & C/D \arrow[u, dashed, "\varphi"']
\end{tikzcd}
$$

Kuva 15. Lauseen 8.9 todistukseen liittyvä kommutoiva kaavio. Yläkolmio saadaan vapaan modulin universaaliominaisuudesta ja alakolmio modulien homomorfialauseesta. Kuvaus ι on inkluusiokuvaus, ja $\eta = \pi \circ \iota$.

Esimerkki 8.10. Universaaliominaisuuden perusteella ei ole olemassa mitään epätriviaalia $\mathbb{Z}$-bilineaarista kuvausta joukolta $\mathbb{Z}_m \times \mathbb{Z}_n$ annetulle modulille P. Jos näet $f : \mathbb{Z}_m \times \mathbb{Z}_n \to P$ on bilineaarinen, täytyy olla olemassa lineaarikuvaus $\varphi : \mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n \to P$, jolle $\varphi \circ \eta = f$. Aiemmin nähtiin, että $\mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n = 0$, joten kuvauksen φ täytyy olla nollakuvaus. Tästä seuraa, että myös f on nollakuvaus.

Seuraavassa lauseessa luetellaan joitakin tensoritulon ominaisuuksia.

Lause 8.11. *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* $(x \otimes y) \otimes z \mapsto x \otimes (y \otimes x)$

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* $a \otimes x \mapsto a.x$.

Viimeisessä kohdassa rengasta R ajatellaan R-modulina.

Todistus. Todistetaan kohta (i) ja jätetään muut harjoitustehtäviksi. Määritellään kuvaukset $f : M \times N \to N \otimes M$ ja $g : N \times M \to M \otimes N$ kaavoilla

$$f(x, y) = y \otimes x \qquad \text{ja} \qquad g(y, x) = x \otimes y.$$

Nämä kuvaukset ovat selvästi bilineaarisia, joten lauseen 8.9 perusteella on olemassa yksikäsitteiset lineaarikuvaukset $\varphi : M \otimes N \to N \otimes M$ ja $\psi : N \otimes M \to M \otimes N$, joille pätee $\varphi(x \otimes y) = f(x, y) = y \otimes x$ ja $\varphi(y \otimes x) = g(y, x) = x \otimes y$ kaikilla $x \in M$ ja $y \in N$. Lisäksi $\varphi \circ \psi = \mathrm{id}$ ja $\psi \circ \varphi = \mathrm{id}$, joten φ ja ψ ovat toistensa käänteiskuvauksia ja siten isomorfismeja. $\square$

Huomautus. Edellistä lausetta voi tulkita siten, että R-modulit muodostavat ikäänkuin oman algebrallisen struktuurinsa, joiden laskutoimitukset $\oplus$ ja $\otimes$ toteuttavat lauseessa mainitut kohdat (i)–(iv). Kertolaskun $\otimes$ "neutraalialkio" on kerroinrengas R.

Osoittautuu, että universaaliominaisuus määrittelee tensoritulon isomorfiaa vaille täydellisesti. Universaaliominaisuutta voidaan tämän vuoksi käyttää määritelmän sijasta tensorituloon liittyvissä todistuksissa.

Lause 8.12. *Olkoot M, N, Q kolme R-modulia, ja olkoon g jokin R-bilineaarinen kuvaus $M \times N \to Q$. Oletetaan, että* $\operatorname{Im} g$ *virittää modulin Q ja että seuraava* *sääntö on voimassa: jos f on mikä tahansa R-bilineaarinen kuvaus tulolta $M \times N$ modulille P, niin on olemassa sellainen R-lineaarinen kuvaus $\psi : Q \to P$, että $f = \psi \circ g$. Tällöin $Q \cong M \otimes_R N$, ja isomorfismille pätee $g(x, y) \mapsto x \otimes y$.*

Todistus. Koska kuvaus g on bilineaarinen, tensoritulon universaaliominaisuuden perusteella löytyy lineaarikuvaus $\varphi : M \otimes N \to Q$, jolle $\varphi \circ \eta = g$. Toisaalta kanoninen kuvaus η on bilineaarinen, joten oletuksen nojalla löytyy lineaarikuvaus $\psi : Q \to M \otimes N$, jolle pätee $\psi \circ g = \eta$.

$$\begin{tikzcd} M \times N \arrow[rr, "g"] \arrow[dr, "\eta"'] & & Q \\ & M \otimes N \arrow[ur, dashed, "\varphi"'] & \end{tikzcd} \qquad \begin{tikzcd} M \times N \arrow[rr, "\eta"] \arrow[dr, "g"'] & & M \otimes N \\ & Q \arrow[ur, dashed, "\psi"'] & \end{tikzcd}$$

Osoitetaan, että φ on kuvauksen ψ käänteiskuvaus. Selvästi $\mathrm{id} = \mathrm{id}_{M \otimes N}$ on R-lineaarinen kuvaus, jolle pätee $\mathrm{id} \circ \eta = \eta$. Toisaalta myös $\psi \circ \varphi$ on R-lineaarinen, ja

$$(\psi \circ \varphi) \circ \eta = \psi \circ g = \eta.$$

Tensoritulon universaaliominaisuuden mukaan tällaisia kuvauksia voi olla vain yksi, joten $\mathrm{id} = \psi \circ \varphi$.

$$\begin{tikzcd} M \times N \arrow[rr, "\eta"] \arrow[dr, "\eta"'] & & M \otimes N \\ & M \otimes N \arrow[ur, shift left, "\mathrm{id}"] \arrow[ur, shift right, "\psi \circ \varphi"'] & \end{tikzcd}$$

Olkoon sitten $u \in Q$ mielivaltainen. Koska kuvajoukko $\operatorname{Im} g$ virittää modulin Q, voidaan kirjoittaa $u = \sum_i g(x_i, y_i)$ joillain $x_i \in M$ ja $y_i \in N$. Toisaalta nähdään, että

$$(\varphi \circ \psi) \circ g = \varphi \circ \eta = g,$$

joten

$$(\varphi \circ \psi)(u) = \sum_i (\varphi \circ \psi)(g(x_i, y_i)) = \sum_i g(x_i, y_i) = u.$$

Näin ollen $\varphi \circ \psi = \mathrm{id}$, ja φ on kuvauksen ψ käänteiskuvaus. Siispä $\psi : Q \to M \otimes N$ on R-modulien isomorfismi, jolle pätee $\psi(g(x, y)) = \eta(x, y) = x \otimes y$. $\square$

Esimerkki 8.13. Olkoon R jokin rengas. Tarkastellaan vapaita tulomoduleja R^n ja R^m. Merkitään symbolilla $R^{n \times m}$ joukkoa, jonka alkioita ovat R-kertoimiset $n \times m$-matriisit. Nämä matriisit muodostavat vapaan R-modulin. Sen luonnollisena kantana ovat alkeismatriisit E_{ij}, joissa rivin i sarakkeessa j on ykkösalkio ja muualla 0. Alkioiden $x = (x_1, \ldots, x_m)$ ja $y = (y_1, \ldots, y_m)$ *dyaditulo* tai *ulkotulo* $g(x, y)$ määritellään matriisina

$$g(x, y) = \begin{bmatrix} x_1 y_1 & x_1 y_2 & \cdots & x_1 y_m \\ x_2 y_1 & x_2 y_2 & \cdots & x_2 y_m \\ \vdots & & & \vdots \\ x_n y_1 & x_n y_2 & \cdots & x_n y_m \end{bmatrix}.$$

Kuvaus $g : R^n \times R^m \to R^{n \times m}$ on R-bilineaarinen.

Osoitetaan, että $R^{n\times m} \cong R^n \otimes R^m$ käyttämällä lausetta 8.12. Selvästi $\operatorname{Im} g$ virittää modulin $R^{n\times m}$, sillä $g(e_i, e_j) = E_{ij}$. Olkoon sitten $f : R^n \times R^m \to P$ bilineaarinen kuvaus jollekin R-modulille P. Määritellään kuvaus φ alkeismatriiseilta moduliin P seuraavasti:

$$\varphi(E_{ij}) = f(e_i, e_j).$$

Vapaan modulin universaaliominaisuuden nojalla φ voidaan laajentaa yksikäsitteisellä tavalla koko modulin $R^{n\times m}$ lineaarikuvaukseksi. Jos $A = (a_{ij}) \in R^{n\times m}$, niin

$$\varphi(A) = \varphi\left(\sum_{i,j} a_{ij} E_{ij}\right) = \sum_{i,j} a_{ij} f(e_i, e_j).$$

Täten

$$\varphi(g(x, y)) = \sum_{i,j} x_i y_j f(e_i, e_j) = f\left(\sum_i x_i e_i, \sum_j y_j e_j\right) = f(x, y)$$

kaikilla $(x, y) \in R^n \times R^m$. Siispä $f = \varphi \circ g$, joten lauseesta 8.12 saadaan, että $R^{n\times m} \cong R^n \otimes R^m$. Dyadituloa $g(x, y)$ vastaa tensoritulo $x \otimes y$.

Nyt nähdään, että reaaliavaruuksien tensoritulo tosiaan yleistää tavallisia piste- ja ristituloja. Pistetulo $x \cdot y$ saadaan matriisista $A = x \otimes y$ lineaarisella kuvauksella $A \mapsto \sum_i A_{ii}$, joka summaa yhteen kaikki lävistäjäalkiot. Ristitulo puolestaan saadaan kuvauksella

$$A \mapsto (A_{23} - A_{32},\ A_{31} - A_{13},\ A_{12} - A_{21}),$$

joka myös on $\mathbb{R}$-lineaarinen.

Tarkastellaan lopuksi erästä tensoritulojen sovellusta, jota nimitetään *skalaarien laajennukseksi.* Olkoot R ja S renkaita ja olkoon $f : R \to S$ rengashomomorfismi. Nyt rengasta S voidaan ajatella R-modulina, kun skalaarikertolasku määritellään kaavalla $a.b = f(a) \cdot b$. Jos M jokin R-moduli, niin voidaan muodostaa tensoritulo

$$M_S = S \otimes_R M.$$

Tämä tensoritulo on S-moduli, kun määritellään $b'.(b \otimes x) = (b'b) \otimes x$ kaikilla alkioilla $b, b' \in S$ ja $x \in M$. Sanotaan, että M_S on saatu modulista M *skalaareja laajentamalla.* Usein R on itse asiassa renkaan S alirengas, ja $f : R \to S$ on inkluusiokuvaus. Jos $S = R$ ja f on identtinen kuvaus, niin $M_R \cong M$ lauseen 8.11 perusteella.

LEMMA 8.14. *Jos $M = R^n$, missä $n \in \mathbb{N}$, niin M_S ja S^n ovat isomorfisia S-moduleina.*

TODISTUS. Harjoitustehtävä. □

LAUSE 8.15. *Jokaisella vaihdannaisella renkaalla R pätee, että jos R^m ja R^n ovat isomorfisia R-moduleja, niin $m = n$.*

TODISTUS. Merkitään $M = R^m$ ja $N = R^n$, ja oletetaan, että $M \cong N$. Olkoon K renkaan R osamääräkunta. (Osamääräkunta on R:n jakorengas joukon $R \setminus \{0\}$

suhteen. Tämä on kunta, koska R on vaihdannainen.) Kunnasta K saadaan R-moduli kanonisen kuvauksen $\eta : R \to K$ avulla. Edellisen lemman perusteella

$$K^m \cong M_K \cong N_K \cong K^n.$$

Yllä olevat isomorfismit ovat K-vektoriavaruuksien isomorfismeja. Koska vektoriavaruuden dimensio on yksikäsitteinen, $m = n$. $\square$

9. Algebrat

Monissa sovelluksissa törmätään moduleihin, joissa on modulirakenteen lisäksi määritelty 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. Tässä materiaalissa oletukset pidetään kuitenkin minimissään.

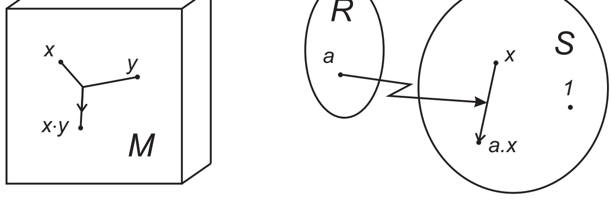
9.1. Perusominaisuudet.

Määritelmä 9.1. Olkoon R vaihdannainen rengas, ja olkoon A jokin R-moduli, jossa on määritelty R-bilineaarinen kertolasku $(x, y) \mapsto x \cdot y$ kaikilla $x, y \in A$. Tällöin 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 kertolaskua merkitään yksinkertaisesti xy jättämällä piste pois. Samoin skalaarikertolaskua voidaan merkitä $a.x = ax$. Jos skalaarikertolaskun ja algebran sisäisen kertolaskun sekoittuminen halutaan välttää, voidaan niille käyttää eri merkintöjä. Esimerkiksi seuraavat laskulait 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 16. Algebra on moduli M, jossa on määritelty bilineaarinen kertolasku. Liitännäinen ja ykkösellinen algebra voidaan nähdä myös renkaana S, jossa on määritelty toisen renkaan skalaarikertolasku.

Esimerkkejä algebroista:

- Olkoon R rengas. R-kertoimisten neliömatriisien modulissa $R^{n \times n}$ voidaan määritellä tuttu matriisikertolasku, joka tekee kyseisestä modulista *matriisialgebran.*
- Polynomirenkaassa $R[X_1, \ldots, X_n]$ rengas R voidaan samastaa vakiopolynomien kanssa. Tällöin skalaarikertolasku voidaan määritellä samalla säännöllä kuin polynomikertolasku, jolloin polynomirenkaasta tulee *polynomialgebra.*
- Olkoon R mikä tahansa rengas, ei välttämättä vaihdannainen. Niin kuin ryhmien tapauksessa, R voidaan varustaa renkaan $\mathbb{Z}$ skalaarikertolaskulla $n.a = a + \cdots + a$ (n kertaa). Jokainen rengas on siis $\mathbb{Z}$-algebra. Kuten ryhmillä, tämä on ainoa tapa, jolla $\mathbb{Z}$ voi toimia renkaassa R, joten $\mathbb{Z}$-algebrojen teoria vastaa renkaiden teoriaa.
- Yleisemmin, jos R ja S ovat renkaita ja $f : R \to S$ on rengashomomorfismi, niin S voidaan varustaa skalaarikertolaskulla $a.b = f(a) \cdot b$. Tällöin renkaasta S tulee R-algebra.
- Jos K on kunta, jokainen K-algebra A on vektoriavaruus. Tällöin voidaan puhua muun muassa algebran *dimensiosta.* Jos vektoriavaruudessa on lisäksi määritelty ylimääräistä rakennetta, 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 homomorfismien joukko $\mathrm{End}_R(M) = \mathrm{Hom}_R(M, M)$ on R-algebra, jota kutsutaan M:n *endomorfismialgebraksi.*

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

Määritelmä 9.2. R-algebran A alimoduli B on *R-alialgebra*, jos se on modulin A alimoduli ja toteuttaa ehdon

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

Alimodulia I kutsutaan *R-ideaaliksi*, jos

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

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

Määritelmä 9.3. Olkoot A ja B kaksi R-algebraa. R-lineaarista kuvausta $\varphi : A \to B$ kutsutaan *R-algebrahomomorfismiksi*, jos

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

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 kuten moduleille yleensä.

9.2. 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 koko algebran kertolaskun täysin.

LAUSE 9.4. *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) *Algebralla A on ykkösalkio 1, jos ja vain jos $1 \cdot a = a$ 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

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

Huomaa, että yllä käytetään hyväksi kerroinrenkaan vaihdannaisuutta. Muut väitteet todistetaan samalla tavalla. □

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

$$b_i \cdot b_j = \sum_k c_{ij}^k b_k.$$

Vakioita $c_{ij}^k \in R$ (tässä k on yläindeksi, ei potenssi) kutsutaan algebran *rakennevakioiksi kannan B suhteen.* Kertolaskun bilineaarisuudesta seuraa, että rakennevakioiden tunteminen riittää algebran kertolaskun tuntemiseksi, sillä

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

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

LAUSE 9.5. *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 9.6. 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

Tämä $\mathbb{R}$-algebra on selvästi ykkösellinen, liitännäinen ja vaihdannainen. Tällä tavoin määritellään *kompleksilukualgebra*, joka on siis kaksiulotteinen reaalikertoiminen algebra. Kompleksialgebran rakennevakiot on lueteltu alla olevassa taulukossa, missä on merkitty $c_{xy}^z = c_{xy}(z)$.

(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 9.7. *Kvaterniot.* William Hamilton[14] löysi vuonna 1843 kertotaulun neliulotteiselle reaalikertoimiselle algebralle $\mathbb{H}$, jonka hän risti kvaternioiksi[15]. Erityistä kvaternioalgebrassa on se, että kaikilla alkioilla on käänteisalkiot, joten jakolasku on mahdollista. Hamilton oli työskennellyt kauan tietynlaisen kolmiulotteisen algebran löytämiseksi, kun hän ollessaan kävelyllä Dublinissa äkkiä tajusi saavansa ideansa toimimaan, jos lisäisi mukaan neljännen ulottuvuuden. Hän innoistui keksinnöstään niin, että kaiversi siltä seisomalta kvaterniokannan kertolaskusäännöt Broughamin sillan kiveykseen. Jos algebran kantaa merkitään symboleilla 1, i, j ja k, kertotaulu näyttää tältä:

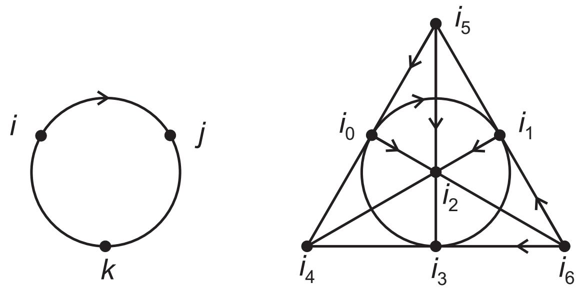
$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Kertotaulusta nähdään, että kvaternioalgebra on liitännäinen ja ykköselliinen. Lisäksi jokaisella nollasta poikkeavalla alkiolla on käänteisalkio: esimerkiksi $(1 + j) \cdot \frac{1}{2}(1 - j) = 1$. Kvaternioalgebra ei kuitenkaan ole vaihdannainen, joten se ei ole kunta. Sen sijaan sitä nimitetään *jakoalgebraksi* (vrt. jakorengas). Kuten kompleksialgebrassa, jokainen ykkösalkiosta poikkeava kanta-alkio on luvun -1 neliöjuuri. Kvaternioita käytettiin kolmiulotteisen reaaliavaruuden geometrian hahmottamiseen ennen vektoriavaruuden käsitteen muotoilua; kvaternioiden avulla voidaan muun muassa muotoilla piste- ja ristitulot sekä kolmiulotteisen avaruuden kierrot.

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

[15]quaternio = nelikkö (lat.)

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 17. 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 $j \cdot i = -k$, ja oktonioilla on voimassa $i_0 \cdot i_1 = i_3$ ja $i_1 \cdot i_4 = -i_2$.

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

Määritelmä 9.8. *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 9.4. Samanlainen konstruktio voidaan tehdä lähtien liikkeellä ryhmän sijaan monoidista, jolloin tuloksena on monoidialgebra.

Esimerkki 9.9. Esitysteoriassa tutkitaan homomorfismeja annetulta ryhmältä G jonkin vektoriavaruuden V kääntyvien lineaarikuvausten ryhmään $GL(V)$. Tällainen kuvaus määrittelee ryhmän G lineaarisen toiminnan avaruudessa V, ja sitä kutsutaan ryhmän *esitykseksi* avaruudessa V. Esityksistä — kuten toiminnoista yleensäkin — on se hyöty, että niitä tutkimalla saadaan paljon tietoa ryhmän rakenteesta.

Nykyisin on tapana sisällyttää esitysteoria modulien teoriaan käyttämällä hyväksi ryhmäalgebran käsitettä. Olkoon V jokin K-kertoiminen vektoriavaruus, ja olkoon $\varphi : G \to GL(V)$ ryhmähomomorfismi, jolloin $\varphi(g)$ on kääntyvä lineaarikuvaus jokaisella $g \in G$. Koska ryhmäalgebra KG on liitännäinen ja ykköselli-nen, sitä voidaan pitää renkaana, joka ei kuitenkaan ole vaihdannainen, ellei G ole vaihdannainen. Avaruuteen V voidaan nyt määritellä renkaan KG kanta-alkioiden vasemmanpuoleinen toiminta kaavalla

$$g.x = \varphi(g)(x).$$

Laajentamalla tämä toiminta lineaarisesti koko renkaan KG vasemmaksi toiminnaksi avaruudesta V tulee vasen KG-moduli.

Jokaista esitystä φ vastaa nyt yksikäsitteisesti jokin KG-moduli, ja esitysteoriasta tutut käsitteet voidaan ilmaista yksinkertaisesti modulikäsitteiden avulla. Esimerkiksi esitys on jaoton, jos ja vain jos vastaavalla modulilla ei ole aitoja epätriviaaleja alimoduleita, ja kaksi esitystä ovat keskenään ekvivalentit, jos ja vain jos vastaavat modulit ovat isomorfiset.

9.4. Polynomialgebrat. Polynomit muodostavat renkaita, joissa voidaan määritellä luonnollinen skalaarikertolasku. Tähän asti polynomeja on käsitelty tässä materiaalissa varsin epämuodollisesti ja niihin on sovellettu koulussa opittuja tietoja. Esitetään tässä yhteydessä eräs tapa konstruoida formaalisti R-kertoiminen polynomialgebra.

Olkoon R rengas ja $I = \{1, 2, \ldots, n\}$ äärellinen indeksijoukko. Ruvetaan määrittelemään polynomialgebraa $R[X_1, \ldots, X_n]$, joka koostuu R-kertoimisista n:n muuttujan 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 muuttujan X_i muodollinen eksponentti. Jos jokin ν_i on nolla, voidaan vastaava X_i^0 jättää merkitsemättä tuloon. 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 vastaa nyt muodollista vaihdannaista tuloa:

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

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

Tarkastellaan sitten monoidialgebraa $P_R(I) = RM_n$. Sen alkioina ovat monoidin M_n alkioiden R-kertoimiset lineaarikombinaatiot

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

Kanta-alkioiden kertolasku saadaan monoidin M_n laskutoimituksesta:

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

ja kahden yleisen alkion tulo on

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

Huomaa, että algebraan siirryttäessä monoidin yhteenlasku muuttuu algebran kertolaskuksi ja samalla monoidin nolla-alkiosta $X^0 = (0, \dots, 0)$ tulee algebran ykkösalkio.

Määritelmä 9.10. Monoidialgebra $P_R(I)$ on *R-kertoiminen n:n muuttujan polynomialgebra.* Se on liitännäinen, vaihdannainen ja ykkösellinen R-algebra, ja sitä merkitään $R[X_1, \dots, X_n]$. Monoidin M_n alkioita 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 $X_2^5 X_3$ aste on $5 + 1 = 6$.

Polynomia, jonka aste on 0, nimitetään *vakiopolynomiksi* tai *vakioksi.* Kuvaus $\eta : a \mapsto aX^0$ 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 vakiopolynomien kertolaskuun. Erityisesti η kuvaa renkaan ykkösalkion algebran ykkösalkioksi.

Polynomialgebralle pätee seuraava universaaliominaisuus.

Lause 9.11. *Olkoon R 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 $\varphi : R[X_1, \dots, X_n] \to A$, jolle pätee $\varphi(X_i) = x_i$ jokaisella i.*

Todistus. Koska algebra A on liitännäinen ja ykkösellinen, se on kertolaskunsa suhteen monoidi. Määritellään kuvaus $f : M_n \to A$ kaavalla

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

Kuvaus f on monoidihomomorfismi monoidilta M_n algebran A multiplikatiiviselle monoidille, sillä

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

ja $f(X^0) = x_1^0 \cdots x_n^0 = 1_A$. (Tässä käytettiin hyväksi A:n vaihdannaisuutta.)

Koska $R[X_1, \dots, X_n]$ on vapaa moduli, jonka kanta on M_n, vapaan modulin universaaliominaisuudesta seuraa, että on olemassa yksikäsitteinen R-lineaarinen kuvaus $\varphi : R[X_1, \dots, X_n] \to A$, jolle pätee $\varphi(X^\nu) = f(X^\nu)$ kaikilla $X^\nu \in M_n$. Tämä lineaarikuvaus säilyttää lisäksi algebran kertolaskurakenteen, sillä kannan alkioilla pätee

$$\varphi(X^\nu \cdot X^\mu) = f(X^\nu \cdot X^\mu) = f(X^\nu) \cdot f(X^\mu) = \varphi(X^\nu) \cdot \varphi(X^\mu),$$

ja yleinen tapaus seuraa kuvauksen φ sekä algebrakertolaskun lineaarisuusominaisuuksista. Kuvaus φ on siis algebrahomomorfismi, ja lisäksi $\varphi(X_i) = f(X^{e_i}) = x_i$ kaikilla 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 φ:n yksikäsitteisyydestä seuraa, että $\varphi' = \varphi$. $\square$

MÄÄRITELMÄ 9.12. Edellisen lauseen kuvausta φ kutsutaan *sijoitushomomorfismiksi.* Polynomin $f = \sum_\nu a_\nu X^\nu$ arvo sijoitushomomorfismissa on

$$\varphi(f) = \sum_\nu a_\nu x^{\nu_1} \cdots x^{\nu_n},$$

ja sitä merkitään $f(x_1, \dots, x_n)$.

Sijoitushomomorfismin avulla voidaan määritellä algebran A *polynomifunktio* $(x_1, \dots, x_n) \mapsto f(x_1, \dots, x_n)$. 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.

Tässä luvussa määriteltiin polynomit äärellisen muuttujajoukon 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.

9.5. Lien algebrat. Lien algebrat tarjoavat tärkeän esimerkin epäliitännäisistä algebroista. Yleensä Lien algebrat liitetään vastaaviin Lien ryhmiin, jotka kuvaavat jatkuvia symmetrioita; eräs esimerkki on reaalitason ympyrän symmetriaryhmä. Näillä ryhmillä on paljon käyttöä paitsi matematiikan puolella, myös teoreettisessa fysiikassa. Lien algebroja voidaan myös käyttää muun muassa yksinkertaisten Lie-tyypin ryhmien luokitteluun ja analysointiin.

Määritelmä 9.13. Olkoon $\mathfrak{L}$ jokin K-vektoriavaruus. Oletetaan, että avaruudessa $\mathfrak{L}$ on määritelty bilineaarinen tulo $(x, y) \mapsto [xy]$, jolle pätee

(LA1) $[xx] = 0$ kaikilla $x \in \mathfrak{L}$
(LA2) $[x[yz]] + [y[zx]] + [z[xy]] = 0$ kaikilla $x, y, z \in \mathfrak{L}$.

Tällöin avaruutta $\mathfrak{L}$ kutsutaan *Lien algebraksi.*

Ehtoa (LA1) nimitetään *alternoivuudeksi* ja ehtoa (LA2) *Jacobin identiteetiksi.* Lien algebran kertolasku ei yleensä ole liitännäinen eikä vaihdannainen; sen sijaan ehdon (LA1) ja kertolaskun bilineaarisuuden perusteella pätee

$$0 = [(x + y)(x + y)] = [xx] + [xy] + [yx] + [yy] = [xy] + [yx],$$

mistä seuraa

(LA1′) $[xy] = -[yx]$ kaikilla $x, y \in V$.

Jos kerroinkunnan karakteristika ei ole 2, ehdot (LA1) ja (LA1′) ovat yhtäpitäviä: tällöin nimittäin ehto (LA1) saadaan asettamalla $x = y$ yhtälössä $[xy] + [yx] = 0$.

Liitännäisten algebrojen avulla voidaan tuottaa runsaasti esimerkkejä Lien algebroista. Olkoon A jokin liitännäinen K-algebra, esimerkiksi K-kertoimisten neliömatriisien muodostama algebra. *Lien kommutaattori* määritellään kaavalla

$$[x, y] = xy - yx \qquad \text{kaikilla } x, y \in A.$$

Algebrasta A tulee Lien algebra kertolaskun $(x, y) \mapsto [x, y]$ suhteen. Tämä kertolasku on nimittäin selvästi bilineaarinen, ja sille pätee ehto (LA1). Jacobin identiteetin tarkistamiseksi todetaan, että

$$\begin{aligned}
[x, [y, z]] &= [x, yz - zy] = (xyz - xzy) - (yzx - zyx) \\
[y, [z, x]] &= [y, zx - xz] = (yzx - yxz) - (zxy - xzy) \\
[z, [x, y]] &= [z, xy - yx] = (zxy - zyx) - (xyz - yxz).
\end{aligned}$$

Kun lasketaan yllä olevat lausekkeet yhteen, saadaan tulokseksi 0. Liitännäisyyttä käytettiin siihen, että kolminkertaiset tulot voitiin kirjoittaa ilman sulkeita.

Esimerkki 9.14. Palautetaan mieleen, että matriisin x *jälki* on sen diagonaalialkioiden summa: $\operatorname{tr} x = \sum_i x_{ii}$. Tarkastellaan joukkoa

$$\mathfrak{sl}_n(\mathbb{R}) = \{x \in \mathbb{R}^{n\times n} \mid \operatorname{tr} x = 0\}.$$

On helppo nähdä, että $\mathfrak{sl}_n(\mathbb{R})$ on liitännäisen algebran $\mathbb{R}^{n\times n}$ aliavaruus (se on lineaarikuvauksen $\operatorname{tr} : \mathbb{R}^{n\times n} \to \mathbb{R}$ ydin), mutta kyseinen aliavaruus ei ole suljettu matriisikertolaskun suhteen. Toisaalta, jos tarkastellaan avaruutta $\mathbb{R}^{n\times n}$ Lien algebrana kertolaskun $[x, y]$ suhteen, voidaan osoittaa, että $\mathfrak{sl}_n(\mathbb{R})$ on Lien alialgebra. Kaikille matriiseille $x, y \in \mathbb{R}^{n\times n}$ nimittäin pätee

$$\begin{aligned}\operatorname{tr}(xy - yx) &= \sum_{i=1}^{n}\left(\sum_{k=1}^{n} x_{ik}y_{ki} - \sum_{k=1}^{n} y_{ik}x_{ki}\right)\\ &= \sum_{i,k=1}^{n} x_{ik}y_{ki} - \sum_{i,k=1}^{n} x_{ki}y_{ik} = 0.\end{aligned}$$

Lien algebraa $\mathfrak{sl}_n(\mathbb{R})$ nimitetään *erityiseksi lineaariseksi algebraksi.*

Jos liitännäinen algebra A on myös vaihdannainen, niin kommutattori $[x, y]$ on nolla kaikilla $x, y \in A$. Tämä ominaisuus otetaan Lien algebran vaihdannaisuuden määritelmäksi.

MÄÄRITELMÄ 9.15. Lien algebraa $\mathfrak{L}$ kutsutaan *vaihdannaiseksi*, jos $[xy] = 0$ kaikilla $x, y \in \mathfrak{L}$.

Huomaa, että Lien algebran vaihdannaisuus ei ole sama asia kuin yleisen algebran vaihdannaisuus. Jos kerroinkunnan karakteristika ei ole 2, niin Lien algebra $\mathfrak{L}$ on vaihdannainen, jos ja vain jos $[xy] = [yx]$ pätee kaikilla $x, y \in \mathfrak{L}$ eli $\mathfrak{L}$ on vaihdannainen algebra. Kuitenkin karakteristikan ollessa 2 ehto $[xy] = [yx]$ seuraa suoraan ehdosta (LA1′) eikä $\mathfrak{L}$ silti ole välttämättä vaihdannainen Lien algebra.

LAUSE 9.16. *Jokainen yksiulotteinen Lien algebra on vaihdannainen.*

TODISTUS. Oletetaan, että $\mathfrak{L}$ on yksiulotteinen K-kertoiminen Lien algebra. Olkoon v jokin nollasta poikkeava vektori. Avaruus $\mathfrak{L}$ on nyt vektorin v virittämä, joten jokainen alkio on muotoa av, missä $a \in K$. Alternoivuudesta seuraa $[(av)(bv)] = ab[vv] = 0$ kaikilla $a, b \in K$, joten $\mathfrak{L}$ on vaihdannainen. □

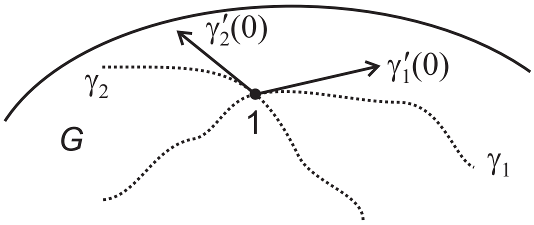
ESIMERKKI 9.17. Lien algebrat liittyvät läheisesti *Lien ryhmiin.* Tarkastellaan esimerkkinä Lien ryhmästä jotain reaalikertoimista matriisiryhmää $G \leq GL_n(\mathbb{R})$. Tämän ryhmän matriiseja voidaan ajatella avaruuden $\mathbb{R}^{n^2}$ pisteinä, jolloin esimerkiksi ryhmässä määritellyille funktioille ja poluille voidaan määritellä raja-arvot ja derivaatat tavalliseen tapaan.

Olkoon $\gamma : \mathbb{R} \to G$ derivoituva funktio, jolle pätee $\gamma(0) = 1$ (ykkösmatriisi). Tämä γ on neutraalialkion kautta kulkeva *polku.* Derivaatta $\gamma'(0) \in \mathbb{R}^{n\times n}$ määrää polun *tangenttivektorin* neutraalialkion kohdalla. Voidaan osoittaa, että kaikkien neutraalialkion kautta kulkevien polkujen tangenttivektorit muodostavat avaruuden $\mathbb{R}^{n\times n}$ aliavaruuden $\mathfrak{g}$. Tämä *tangenttiavaruus* on lisäksi suljettu Lien kommutaattorin suhteen, joten se on Lien algebra. Sitä kutsutaan *ryhmän G Lien algebraksi.* Kommutaattorilla on läheinen yhteys konjugointiin ryhmässä G.

Jos $x \in \mathfrak{g}$, eli x on jonkin neutraalialkion kautta kulkevan polun γ derivaatta, pätee derivaatan määritelmän mukaan

$$\gamma(t) = 1 + tx + t\epsilon(t),$$

missä $|\varepsilon(t)| \to 0$, kun $t \to 0$. Polulla γ olevia ryhmän alkioita voidaan siis approksimoida Lien algebran alkion tx avulla, kun t on riittävän pieni. Tämän vuoksi Lien algebraa nimitetään joskus ryhmän *generoivaksi* algebraksi. Yllä olevan kaavan perusteella alkiota tx voidaan pitää infinitesimaalisena ryhmän alkiona, ja



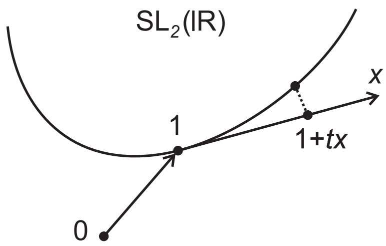
Kuva 18. Lien ryhmän G tangenttivektoreita

Lien algebraa nimitetäänkin joskus *infinitesimaaliseksi ryhmäksi*, vaikka todellisuudessa Lien algebralla ei ole ryhmän rakennetta.

Esimerkiksi erityinen lineaarinen algebra $\mathfrak{sl}_n(\mathbb{R})$ (ks. esimerkki 9.14) on erityisen lineaarisen ryhmän $SL_n(\mathbb{R})$ Lien algebra. Ryhmään $SL_n(\mathbb{R})$ kuuluvat sellaiset $n \times n$-matriisit, joiden determinantti on 1. Jos $x \in \mathfrak{sl}_2(\mathbb{R})$, niin x on muotoa $\left[\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right]$, ja

$$\det(1 + tx) = \begin{vmatrix} 1 + ta & tb \\ tc & 1 - ta \end{vmatrix} = 1 - t^2(a^2 + bc).$$

Jos parametri t on infinitesimaalisen pieni, toisen potenssin t^2 sisältävä termi voidaan jättää huomiotta. Tällöin huomataan, että matriisin $1 + tx$ determinantti on erittäin lähellä ykköstä, joten kyseinen matriisi approksimoi jotain ryhmän $SL_2(\mathbb{R})$ alkiota.



Kuva 19. Matriisi $1 + tx$ on lähellä ryhmää $SL_2(\mathbb{R})$.

Yleisessä tapauksessa Lien ryhmät voivat olla mitä tahansa derivoituvia monistoja. Tällöin tangenttivektorit voidaan määritellä samaan tapaan kuin matriisien tapauksessa. Kertolaskua ei kuitenkaan saada suoraan matriisialgebran kommutaattorina vaan se on johdettava muulla tavalla.

Kuntalaajennokset

10. Esimerkki: Äärelliset kunnat

Ennen kuin ruvetaan käsittelemään kuntalaajennoksia yleisesti, tarkastellaan hieman äärellisten kuntien rakennetta ja konstruktiota. Samalla tutustutaan niihin menetelmiin, joita teorian kehittämisessä tullaan tarvitsemaan.

Palautetaan aluksi mieleen kunnan karakteristikan ja alkukunnan käsitteet.

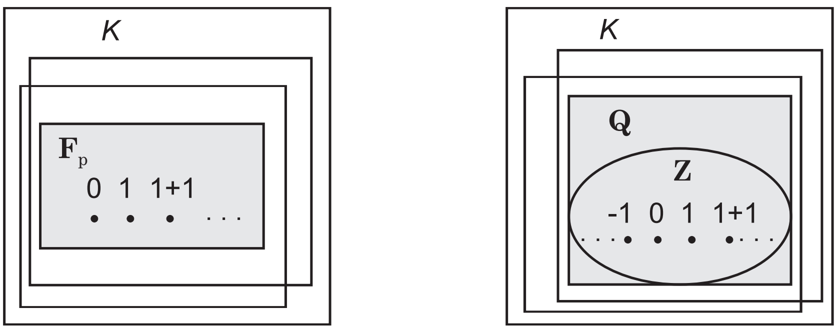
Määritelmä 10.1. Olkoon K kunta. Pienintä positiivista kokonaislukua n, jolle pätee

$$\underbrace{1+\cdots+1}_{n \text{ kpl}} = 0,$$

kutsutaan K:n *karakteristikaksi* ja merkitään $\operatorname{char}(K)$. Jos tällaista lukua ei ole olemassa, sanotaan että karakteristika on nolla.

Kunnan karakteristika on aina alkuluku, jos se ei ole nolla. Jos karakteristika on $p > 0$, niin minkä tahansa alkion p:s monikerta on nolla, sillä $(a + \cdots + a) = a(1 + \cdots + 1) = 0$ kaikilla a.

Jos K on kunta, mikä tahansa alikunta sisältää kaikki ykkösalkion monikerrat. Toisaalta karakteristikan ollessa $p > 0$ ykkösalkion monikerrat muodostavat renkaan $\mathbb{Z}_p$ kanssa isomorfisen alistruktuurin, joka on kunta. Tätä kuntaa merkitään symbolilla $\mathbb{F}_p$ ja nimitetään kunnan K *alkukunnaksi*. Toisaalta, jos K:n karakteristika on 0, niin ykkösalkion monikerrat muodostavat rakenteen, joka on isomorfinen renkaan $\mathbb{Z}$ kanssa. Jokainen K:n alikunta sisältää paitsi nämä monikerrat, myös niiden käänteisalkiot. Täten alikunnan täytyy sisältää $\mathbb{Z}$:n osamääräkunta $\mathbb{Q}$. Näistä havainnoista saadaan seuraava lause.



Kuva 20. Jokainen kunta sisältää yksikäsitteisen minimaalisen alikunnan.

Lause 10.2. *Jokainen kunta sisältää yksikäsitteisen minimaalisen alikunnan, jota nimitetään* alkukunnaksi. *Jos kunnan karakteristika on alkuluku p, tämä alkukunta on isomorfinen jäännösluokkakunnan $\mathbb{F}_p$ kanssa. Jos karakteristika on nolla, alkukunta on isomorfinen rationaalilukujen kunnan $\mathbb{Q}$ kanssa.*

Jokaisen äärellisen kunnan karakteristika on välttämättä positiivinen, mutta äärettömän kunnan karakteristika voi olla yhtä hyvin positiivinen tai nolla. Osoittautuu, että äärellisen kunnan rakenne on muutenkin hyvin tarkoin määrätty. Seuraava lause antaa rajoituksen äärellisen kunnan alkioiden lukumäärälle.

Lause 10.3. *Jos K on äärellinen kunta, niin $|K| = p^n$, missä p on K:n karakteristika ja n jokin positiivinen kokonaisluku.*

Todistus. Samastetaan kunnan K alkukunta ja $\mathbb{F}_p$. Nyt K on $\mathbb{F}_p$-algebra, kun skalaarikertolaskuna on kunnan sisäinen kertolasku. Erityisesti K on siis äärellinen $\mathbb{F}_p$-vektoriavaruus, joten sillä on äärellinen dimensio. Merkitään K:n kantaa $\{b_1, \dots, b_n\}$. Jokainen K:n alkio voidaan nyt kirjoittaa yksikäsitteisessä muodossa

$$x_1 b_1 + x_2 b_2 + \cdots x_n b_n,$$

missä $x_i \in \mathbb{F}_p$ kaikilla i. Tällaisia lineaarikombinaatioita on tuloperiaatteen mukaan p^n kappaletta, joten $|K| = p^n$. $\square$

Myöhemmin tullaan osoittamaan, että jokaista alkulukupotenssia p^n kohti on olemassa kunta, jonka koko on p^n, ja että tämä kunta on isomorfiaa vaille yksikäsitteinen. Tarkastellaan seuraavaksi, miten tällaisia kuntia voidaan periaatteessa konstruoida.

Lähdetään liikkeelle alkukunnasta $\mathbb{F}_p$. Oletetaan, että $f \in \mathbb{F}_p[X]$ on jaoton polynomi, jonka aste on $n > 0$. Polynomien jakoyhtälöstä seuraa (todistus jätetään harjoitustehtäväksi), että polynomin f virittämä ideaali $\langle f \rangle$ on alkuideaali. Edelleen sivulla 48 olevan esimerkin perusteella $\langle f \rangle$ on maksimaalinen. Näin ollen tekijärengas $\mathbb{F}_p[X]/\langle f \rangle$ on kunta. Se koostuu sivuluokista $\overline{g} = g + \langle f \rangle$. Nolla- ja ykkösalkiot ovat vastaavasti vakiopolynomien 0 ja 1 sivuluokat; näitä luokkia merkitään yksinkertaisesti $\overline{0} = 0$ ja $\overline{1} = 1$.

Lause 10.4. *Kunnan $\mathbb{F}_p[X]/\langle f \rangle$ alkioiden lukumäärä on p^n.*

Todistus. Merkitään $\mathbb{F}_p[X]/\langle f \rangle = K$. Huomataan, että $\langle f \rangle$ on $\mathbb{F}_p$-modulin $\mathbb{F}_p[X]$ alimoduli, sillä $ag \in \langle f \rangle$ kaikilla $g \in \langle f \rangle$ ja $a \in \mathbb{F}_p$. Näin ollen K on $\mathbb{F}_p$-tekijämoduli. Edellisen lauseen todistuksen perusteella riittää osoittaa, että K:lla on kanta, jonka pituus on n.

Tarkastellaan monomeja X^i, missä $i \in \{0, \dots, n-1\}$, ja näistä muodostettua lineaarikombinaatiota

$$g = \sum_{i=0}^{n-1} a_i X^i, \qquad \text{missä } a_i \in \mathbb{F}_p \text{ kaikilla } i.$$

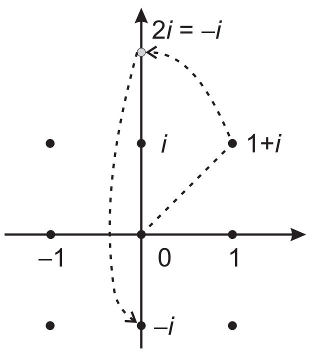
Sivuluokka $\overline{g}$ on joukon $B = \{1, \overline{X} \dots, \overline{X}^{n-1}\}$ lineaarikombinaatio, kertoiminaan skalaarit a_i. Oletetaan, että $\overline{g} = 0$, jolloin $g \in \langle f \rangle$. Nyt f jakaa g:n, mutta g:n aste on pienempi kuin n, joten g:n on oltava nollapolynomi. Siispä $a_i = 0$ kaikilla i, mistä seuraa, että joukko B on vapaa.

Oletetaan sitten, että $h \in \mathbb{F}_p[X]$ on mielivaltainen. Jakoyhtälöstä seuraa, että $h = fq+r$, missä r:n aste on pienempi kuin n. Tällöin $h-r \in I$ eli $\overline{h} = \overline{r}$. Toisaalta r on muotoa $a_0 + a_1X + \cdots + a_{n-1}X^{n-1}$, joten $\overline{h} = \overline{r}$ voidaan esittää lineaarikombinaationa joukon B alkioista. Kyseinen joukko on siis $\mathbb{F}_p$-vektoriavaruuden K kanta. □

Esimerkki 10.5. Toisen asteen polynomi $f = X^2 + 1$ on jaoton kunnassa $\mathbb{F}_3 = \{-1, 0, 1\}$, koska mikään kunnan alkioista ei ole sen juuri. Tekijärengas $K = \mathbb{F}_3[X]/\langle f\rangle$ on kunta, joka koostuu alkioiden 1 ja $\overline{X}$ lineaarikombinaatioista:

$$K = \Big\{0,\ 1,\ -1,\ \overline{X},\ \overline{X}+1,\ \overline{X}-1,\ -\overline{X},\ -\overline{X}+1,\ -\overline{X}-1,\Big\}.$$

K on siis 9 alkion kunta. Lisäksi $\overline{X}^2 = (\overline{X}^2+1) - 1 = 0 - 1 = -1$, eli alkio $\overline{X}$ on luvun -1 (oikeastaan ykkösalkion $1+I$ vasta-alkion) neliöjuuri. Kuten algebroissa yleensä, kannan alkioiden kertotaulu määrittää koko kunnan K:n kertolaskun. Merkitään vielä $\overline{X} = i$, jolloin K:n kertolaskua voidaan ajatella “modulaarisena” kompleksilukujen kertolaskuna. Esimerkiksi $(1+i)^2 = 1 + 2i - 1 = 2i = -i$.



Kuva 21. Kunnan $\mathbb{F}_3$ kaksiulotteinen laajennos. Kertolasku toimii kuten kompleksiluvuilla.

11. Jaollisuudesta

Kuntalaajennosten yhteydessään käytetään usein apuna jaottomia polynomeja. Tarkastellaan seuraavaksi hieman jaollisuuskäsitettä yleensä ja todistetaan joitain kriteerejä erityisesti polynomien jaottomuudelle.

11.1. Jaollisuus kokonaisalueissa. Olkoon R kokonaisalue[16]. Jaollisuuteen liittyvät käsitteet määritellään R:ssä samalla tavoin kuin kokonaisluvuilla. Alkio $a \in R$ *jakaa* alkion $b \in R$, jos $b = ac$ jollain $c \in R$. Tällöin merkitään $a|b$, ja sanotaan myös, että b on a:n *tekijä*. Jos $a|b$ ja $b|a$, niin a ja b ovat toistensa *liittoalkioita*. Kääntyviä alkioita kutsutaan *yksiköiksi*, ja ne jakavat kaikki R:n alkiot, sillä jos a on yksikkö, niin $b = a(a^{-1}b)$. Seuraavan lemman helppo todistus jätetään harjoitustehtäväksi.

LEMMA 11.1. *Oletetaan, että $a, b \in R$.*

a) *Alkiot a ja b ovat liittoalkioita, jos ja vain jos $a = bc$, missä c on yksikkö.*
b) *Jos $a, b \in R \setminus \{0\}$ ovat liittoalkioita ja $a = bc$, niin c on yksikkö.*
c) *Kaikki yksiköt ovat toistensa liittoalkioita.*

Koska jokainen alkio on jaollinen kaikilla yksiköillä sekä omilla liittoalkioillaan, niitä voidaan pitää alkion *triviaaleina tekijöinä*. Yleisessä kokonaisalueessa voi olla kahdentyyppisiä jaottomia alkioita. Koska nolla-alkio on joka tapauksessa jaollinen kaikilla alkioilla, se jätetään tarkastelun ulkopuolelle.

MÄÄRITELMÄ 11.2. Oletetaan, että $a \in R \setminus \{0\}$ ei ole yksikkö. Tällöin a:ta sanotaan *jaottomaksi*, jos sen jokainen tekijä on joko yksikkö tai a:n liittoalkio.

MÄÄRITELMÄ 11.3. Oletetaan, että $a \in R \setminus \{0\}$ ei ole yksikkö. Alkiota a sanotaan *alkualkioksi*, jos aina kun a jakaa tulon bc, niin a jakaa jomman kumman alkioista b ja c.

Kokonaislukujen renkaassa $\mathbb{Z}$ on vain kaksi yksikköä: 1 ja -1. Luvun $n \in \mathbb{Z}$ liittoalkioita on siis samoin kaksi: n ja $-n$. Kokonaisluku p on jaoton, jos ja vain jos se on jonkin alkuluvun liittoalkio, sillä tällöin p:llä on tekijöinä vain luvut 1, -1, p ja $-p$, jotka ovat kaikki joko yksiköitä tai p:n liittoalkioita.

LAUSE 11.4. *Jos $a \in R$ on alkualkio, se on jaoton.*

TODISTUS. Oletetaan, että $a \in R$ on alkualkio ja $a = bc$ joillain $b, c \in R$. Tällöin sekä b että c jakavat a:n. Toisaalta a jakaa triviaalisti tulon bc, joten koska a on alkualkio, a jakaa b:n tai c:n. 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. □

Käänteinen väite ei päde: jaoton alkio ei välttämättä ole alkualkio, vaikka tämä onkin totta kokonaislukujen tapauksessa. Esimerkiksi kompleksilukujen alirenkaassa $\mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\}$ pätee

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

[16]Monet esiteltävistä käsitteistä voidaan määritellä myös renkaissa, mutta yksinkertaisuuden vuoksi tarkastellaan tässä yhteydessä vain kokonaisalueita.

Pienellä laskulla voidaan osoittaa, että luvut 2, 3 sekä $1 \pm i\sqrt{5}$ ovat kaikki jaottomia. Esimerkiksi 2 kuitenkin jakaa tulon $(1+i\sqrt{5})(1-i\sqrt{5})$, muttei kumpaakaan sen tekijöistä, joten se ei ole alkuluku.

Lukujen suurin yhteinen tekijä määritellään myös tutulla tavalla.

MÄÄRITELMÄ 11.5. Olkoot $a, b \in R$. Alkiota $d \in R$ nimitetään alkioiden a ja b *suurimmaksi yhteiseksi tekijäksi*, jos seuraavat ehdot pätevät:

i) $d|a$ ja $d|b$, eli d on a:n ja b:n yhteinen tekijä.
ii) Jos $c|a$ ja $c|b$, niin $d|c$.

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

Kaikissa kokonaisalueissa kahdella alkiolla ei välttämättä ole suurinta yhteistä tekijää. Lisäksi alkioiden a ja b suurin yhteinen tekijä ei yleensä ole yksikäsitteinen, mistä syystä tuttu merkintä $d = \mathrm{syt}(a, b)$ ei periaatteessa ole käyttökelpoinen. Määritelmän ehdoista kuitenkin seuraa, että kaikki kahden alkion suurimmat yhteiset tekijät ovat toistensa liittoalkioita. Merkinnän $d = \mathrm{syt}(a, b)$ voidaankin ajatella 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.

Esimerkiksi renkaassa $\mathbb{Z}$ lukujen 30 ja 12 suurimpia yhteisiä tekijöitä ovat määritelmän mukaan luvut 6 ja -6. Positiivisista luvuista puhuttaessa kuitenkin yleensä määritellään, että luvun $\mathrm{syt}(m, n)$ on myös oltava positiivinen. Tällöin sanan "suurin" voidaan ajatella tarkoittavan myös suurinta kokonaislukujen tavallisen järjestyksen suhteen.

11.2. Erilaiset jaollisuusalueet. Kunnassa jaollisuuskysymykset ovat triviaaleja, koska jokainen nollasta poikkeava alkio on yksikkö ja siksi jokaisen alkion tekijä. Toisaalta yleisessä kokonaisalueessa ei välttämättä voida esimerkiksi löytää kahden alkion suurinta yhteistä tekijää tai kirjoittaa alkiota jaottomien alkioiden tulona. Seuraavassa esitellään muutamia kokonaisalueiden tyyppejä, joissa on toinen toistaan paremmat jaollisuusominaisuudet. Todistuksia ei käsitellä, mutta ne löytyvät monista algebran perusoppikirjoista, esimerkkinä Nathan Jacobsonin *Lectures in Abstract Algebra I. Basic Concepts.*

Tekijöihinjakorenkaat. Kokonaisaluetta, jossa jokainen nollasta poikkeava alkio voidaan hajottaa yksikäsitteisellä tavalla jaottomien alkioiden tuloksi, kutsutaan *tekijöihinjakorenkaaksi*[17] (TJR) tai *faktoriaaliseksi renkaaksi.* Jaon on oltava yksikäsitteinen sillä rajoituksella, että tekijöiden järjestyksellä ei ole väliä ja jokainen alkio voidaan korvata liittoalkiollaan. Kokonaislukujen rengas on TJR: esimerkiksi $60 = 2 \cdot 2 \cdot 3 \cdot 5$; tätä jakoa pidetään samana kuin $60 = -5 \cdot 2 \cdot 3 \cdot (-2)$. Tekijöihinjakorenkaassa jokainen jaoton alkio on alkualkio. Lisäksi kahden alkion

[17] englanniksi *unique factorisation domain* eli UFD

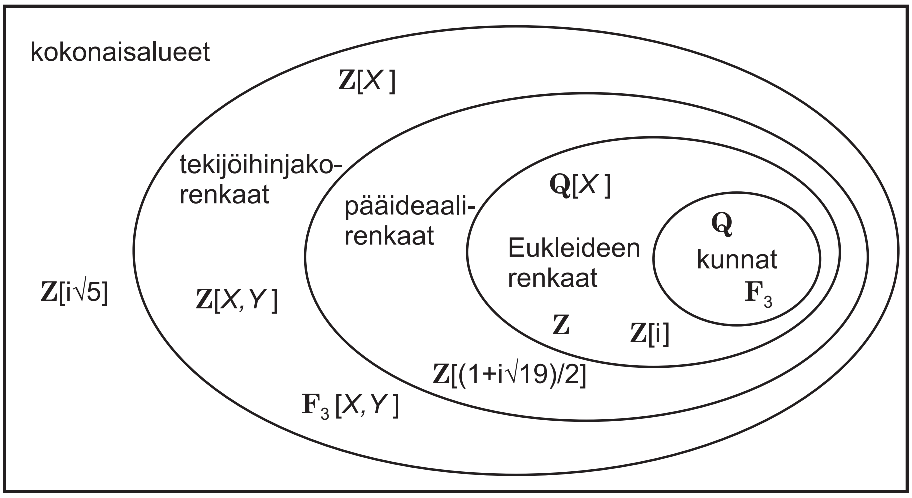
suurin yhteinen tekijä on aina mahdollista löytää vertailemalla alkioiden tekijöihinjakoja. Hieman hankalampaa on osoittaa, että jos R on TJR, niin myös polynomirengas $R[X]$ on TJR. Tästä voidaan edelleen induktiolla päätellä, että rengas $R[X_1, \ldots, X_n]$ on TJR kaikilla n.

Pääideaalirenkaat. Pääideaalirenkaassa (PIR) jokainen ideaali on yhden alkion virittämä. Tästä seuraa, että minkä tahansa kahden alkion a ja b suurin yhteinen tekijä on olemassa ja se voidaan kirjoittaa muodossa $xa + by$. Lisäksi pääideaalirenkaassa jokainen pääideaaleista muodostettu aidosti nouseva ketju $\langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \cdots$ on äärellisen pituinen. Tämän ominaisuuden avulla voidaan osoittaa, että jokainen PIR on myös TJR. Kuitenkaan esimerkiksi polynomirengas $\mathbb{Z}[X]$ ei ole PIR vaikka onkin TJR.

Eukleideen renkaat. Eukleideen renkaaksi kutsutaan kokonaisaluetta R, jossa voidaan määritellä ns. *Eukleideen funktio* $\varepsilon : R \to \mathbb{N}$. Eukleideen funktion on toteutettava seuraava ehto:

> 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 $\varepsilon(r) < \varepsilon(b)$.

Tämän määritelmän merkitys on siinä, että Eukleideen renkaassa on mahdollista käyttää Eukleideen algoritmia kahden alkion suurimman yhteisen tekijän löytämiseksi. Tästä seuraa, että jokainen Eukleideen rengas on PIR (vrt. lauseen 6.3 todistus). Kokonaisluvuilla voidaan määritellä Eukleideen funktio kaavalla $\varepsilon(a) = |a|$, ja jos K on kunta, niin polynomirenkaassa $K[X]$ Eukleideen funktion arvo saadaan polynomin asteesta. Tämä on myös polynomien jakoyhtälön perustana.



Kuva 22. Erilaisia jaollisuusalueita

11.3. Polynomien jaottomuus. Tarkastellaan nyt polynomien jaollisuuteen liittyviä tuloksia, jotta voidaan todistaa muutama hyödyllinen jaottomuuskriteeri. Aloitetaan kirjoittamalla virallisesti ylös polynomien jakoyhtälö, jota on jo käytetty monissa todistuksissa.

LAUSE 11.6 (Jakoyhtälö). *Olkoon K kunta, ja olkoot $f, g \in K[X]$. Oletetaan, että $g \neq 0$. Tällöin löytyy yksikäsitteiset $q, r \in K[X]$, joille pätee $f = qg + r$ ja* $\deg(r) < \deg(g)$.

TODISTUS. Jakoyhtälö osoitetaan samalla tavoin kuin kokonaisluvuilla. 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 $r = 0$, väite pätee, 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 $\deg(r) \geq \deg(g)$, niin 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 $\deg(r) < \deg(g)$.

Yksikäsitteisyyden osoittamiseksi oletetaan, että polynomit q_1, q_2, r_1 ja r_2 toteuttavat 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 $r_1 = r_2$. □

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

Jakoyhtälön olemassaolo osoittaa, että yhden muuttujan polynomit muodostavat Eukleideen renkaan, jos kerroinrengas on kunta. Tämän avulla voidaan helposti osoittaa, että polynomirenkaassa on yksikäsitteinen tekijöihinjako. Seuraavaa lemmaa on jo käytetty muun muassa luvussa 10, kun konstruoitiin kunnan $\mathbb{F}_p$ laajennos jaottoman polynomin avulla.

LEMMA 11.7. *Olkoon K kunta ja $f, g, h \in K[X]$. Oletetaan, että f on jaoton ja $f|(gh)$. Tällöin $f|g$ tai $f|h$.*

TODISTUS. Harjoitustehtävä. □

LAUSE 11.8. *Jos K on kunta, polynomirengas $K[X]$ on tekijöihinjakorengas.*

TODISTUS. Tämä todistus on jälleen samanlainen kuin kokonaisluvuilla. Oletetaan, että $f \in K[X]$ 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 $f = f_1 f_2 \cdots f_r$, missä jokainen f_i on jaoton.

Oletetaan sitten, että $f = f_1 \cdots f_r = g_1 \cdots g_s$, missä jokainen f_i ja g_i on jaoton. Nyt f_1 jakaa tulon $g_1 \cdots g_s$, ja koska f_1 on jaoton, seuraa edellisestä lemmasta, että f_1 jakaa jonkin polynomeista g_i. Järjestystä vaihtamalla voidaan olettaa, että $f_1 \mid g_1$. Toisaalta g_1 on jaoton, joten f_1 ja g_1 ovat liittoalkioita. Tästä seuraa, että

$f_2 \cdots f_r = ug_2 \cdots g_s$, missä u on yksikkö. Induktion avulla voidaan päätellä, että $r = s$ ja että f_i ja g_i ovat liittoalkioita kaikilla i. □

Osoitetaan tässä välissä eräs hyödyllinen tekijöihinjakorenkaan ominaisuus.

LEMMA 11.9. *Tekijöihinjakorenkaassa jokainen jaoton alkio on alkualkio.*

TODISTUS. Oletetaan, että p on jaoton alkio, joka jakaa tulon ab. Kirjoitetaan a ja b jaottomien alkioiden tulona muodossa $a = a_1 a_2 \cdots a_r$ ja $b = b_1 b_2 \cdots b_s$. Koska p on tulon ab jaoton tekijä, sen täytyy olla mukana tulon ab hajotelmassa jaottomiin tekijöihin. Eräs tällainen hajotelma on $a_1 \cdots a_r b_1 \cdots b_s$. Hajotelman yksikäsitteisyydestä seuraa nyt, että p on jokin alkioista a_i tai b_i tai niiden liittoalkio. Täten $p|a$ tai $p|b$. □

Lopuksi osoitetaan joitakin käytännöllisiä jaottomuuskriteerejä. Ensimmäinen on monelle tuttu lukiosta.

LAUSE 11.10 (Rationaalijuuritesti). *Olkoon R tekijöihinjakorengas, jonka osamääräkunta on K. Oletetaan, että polynomilla $f = a_0 + \cdots + a_n X^n \in R[X]$ on juuri $p/q \in K$, missä* $\operatorname{syt}(p, q) = 1$. *Tällöin p jakaa kertoimen a_0, ja q jakaa kertoimen a_n.*

TODISTUS. Kerrotaan yhtälö $f(p/q) = 0$ puolittain luvulla q^n, jolloin saadaan

$$a_0 q^n + a_1 p q^{n-1} + a_2 p^2 q^{n-2} + \cdots + a_n p^n = 0.$$

Ottamalla p yhteiseksi tekijäksi ja siirtelemällä termejä saadaan

$$a_0 q^n = -p(a_1 q^{n-1} + a_2 p q^{n-2} + \cdots + a_n p^{n-1}).$$

Yllä olevasta yhtälöstä nähdään, että p jakaa tulon $a_0 q^n$. Lemman 11.9 mukaan p on alkualkio, joten p jakaa a_0:n tai q^n:n. Oletuksen mukaan p:llä ei ole yhteisiä epätriviaaleja tekijöitä alkion q^n kanssa, joten $p|a_0$. Vastaavasti yhtälöstä

$$q(a_0 q^{n-1} + a_1 p q^{n-2} + \cdots + a_{n-1} p^{n-1}) = -a_n p^n$$

nähdään, että $q|a_n$. □

Rationaalijuuritesti soveltuu korkeintaan kolmannen asteen polynomien jaottomuustestiksi, kuten seuraava esimerkki osoittaa.

ESIMERKKI 11.11. Tarkastellaan polynomia $f = 3X^3 + 3X - 1 \in \mathbb{Z}[X]$. Jos se ei ole jaoton, se on muotoa $f = (aX + b)g$, missä $g \in \mathbb{Z}[X]$ on toisen asteen polynomi. Tällöin f:llä on rationaalijuuri $-b/a$. Rationaalijuuritestin perusteella f:n rationaalijuuret ovat joukossa $\{\pm 1, \pm 1/3\}$. Mikään näistä luvuista ei kuitenkaan ole f:n juuri, joten f on jaoton.

Muita kriteerejä varten tarvitaan hieman aputuloksia. Seuraava yksinkertainen havainto on usein käyttökelpoinen, ja siksi se mainitaan tässä erikseen. Helppo todistus sivuutetaan.

LEMMA 11.12. *Olkoon R rengas, ja olkoon I renkaan R ideaali. Tällöin kuvaus $R[X] \to (R/I)[X]$, missä $\sum_i a_i X^i \mapsto \sum_i (a_i + I) X^i$ on surjektiivinen rengashomomorfismi.*

Jatkossa merkitään polynomin $f \in R[X]$ kuvaa yllä olevan lemman kuvauksessa $\overline{f}$. Polynomi $\overline{f} \in (R/I)[X]$ saadaan siis korvaamalla f:n kertoimet sivuluokillaan. Tyypillisesti ideaali I valitaan alkuideaaliksi, jotta syntyvästä tekijärenkaasta tulisi kokonaisalue.

MÄÄRITELMÄ 11.13. Olkoon R tekijöihinjakorengas, ja olkoon $f \in R[X]$. Jos polynomin f kertoimilla on suurimpana yhteisenä tekijänä 1, sanotaan että f on *primitiivinen.*

LEMMA 11.14. *Olkoon R tekijöihinjakorengas, ja olkoot $f, g \in R[X]$. Jos f ja g ovat primitiivisiä, niin fg on primitiivinen.*

TODISTUS. Oletetaan vastoin väitettä, että f ja g ovat primitiivisiä mutta fg ei ole. Tällöin löytyy jaoton alkio $p \in R$, joka jakaa kaikki tulopolynomin fg kertoimet. Koska R on TJR, tiedetään, että p on alkualkio. Täten tekijärengas $R/\langle p\rangle$ on kokonaisalue, mistä seuraa, että myös $R/\langle p\rangle[X]$ on kokonaisalue.

Olkoot $\overline{f}, \overline{g} \in R/\langle p\rangle[X]$ ne polynomit, jotka saadaan polynomeista f ja g vaihtamalla kertoimet sivuluokkiinsa ideaalin $\langle p\rangle$ suhteen (vrt. lemma 11.12). Koska f ja g ovat primitiivisiä, alkio p ei jaa niiden kaikkia kertoimia. Tästä nähdään, että $\overline{f} \neq 0$ ja $\overline{g} \neq 0$. Koska $R/\langle p\rangle[X]$ on kokonaisalue, niin $\overline{fg} = \overline{f} \cdot \overline{g} \neq 0$. Tämä taas tarkoittaa sitä, että p ei jaa kaikkia tulon fg kertoimia, mikä on ristiriita. Siispä fg on primitiivinen. □

LAUSE 11.15 (Gaussin lemma[18]). *Olkoon R tekijöihinjakorengas, jonka osamääräkunta on K. Tällöin $f \in R[X]$ on jaoton, jos ja vain jos f on primitiivinen ja jaoton renkaassa $K[X]$.*

TODISTUS. Oletetaan ensin, että f on primitiivinen ja jaoton renkaassa $K[X]$. Jos f ei ole jaoton renkaassa $R[X]$, niin $f = gh$ joillain $g, h \in R[X]$, missä g ja h eivät kumpikaan ole yksiköitä. Koska f on jaoton $K[X]$:ssä, niin joko g tai h on vakio. Tämä vakio kuitenkin jakaa kaikki polynomin $gh = f$ kertoimet, mikä on mahdotonta, koska f on primitiivinen. Täten f on jaoton renkaassa $R[X]$.

Oletetaan sitten, että f on jaoton renkaassa $R[X]$. Se voidaan kuitenkin kirjoittaa muodossa $f = cf_1$, missä c on f:n kertoimien suurin yhteinen tekijä ja f_1 on primitiivinen. Jaottomuudesta seuraa nyt, että c on yksikkö $R[X]$:ssä, joten f on primitiivinen.

Tehdään vastaoletus, että f ei ole jaoton renkaassa $K[X]$. Tällöin $f = gh$ joillain $g, h \in K[X]$, missä g ja h eivät kumpikaan ole vakioita. Laventamalla tulon gh kertoimet samannimisiksi, kyseinen tulo voidaan kirjoittaa muodossa $gh = a/b \cdot g_1 h_1$, missä $g_1, h_1 \in R[X]$ ovat primitiivisiä ja $a, b \in R$ ovat jaottomia toistensa suhteen. Tällöin $bf = ag_1 h_1$. Edellisen lemman perusteella tulo $g_1 h_1$ on primitiivinen. Nyt b on polynomin bf kertoimien suurin yhteinen tekijä, ja a on polynomin $ag_1 h_1$ kertoimien suurin yhteinen tekijä, joten b ja a ovat liittoalkioita. Koska $\mathrm{syt}(a, b) = 1$, tämä on mahdotonta, elleivät a ja b ole R:n yksiköitä. Viimeksi mainitussa tapauksessa voidaan kirjoittaa $f = (ag_1)(b^{-1}h_1)$, jolloin f ei olekaan jaoton renkaassa $R[X]$. Tämä on ristiriita, joten f on jaoton renkaassa $K[X]$. □

[18]Myös lemmaa 11.14 nimitetään toisinaan Gaussin lemmaksi.

Lause 11.16 (Eisensteinin kriteeri). *Olkoon R tekijöihinjakorengas, jonka osamääräkunta on K, ja olkoon $f = a_0 + \cdots + a_n X^n \in R[X]$. Polynomi f on jaoton renkaassa $K[X]$, jos jompikumpi seuraavista ehdoista on voimassa:*

a) *Jokin alkualkio $p \in R$ jakaa kertoimet $a_0, \ldots, a_{n-1}$ mutta ei kerrointa a_n, ja p^2 ei jaa kerrointa a_0.*
b) *Jokin alkualkio $p \in R$ jakaa kertoimet $a_1, \ldots, a_n$ mutta ei kerrointa a_0, ja p^2 ei jaa kerrointa a_n.*

Todistus. Oletetaan, että ehto (a) pätee. Voidaan olettaa, että f on primitiivinen. (Muuten jaetaan f kertoimiensa suurimmalla yhteisellä tekijällä, mikä ei vaikuta jaottomuuteen kunnan K suhteen.) Olkoon $\overline{f}$ se renkaan $R/\langle p\rangle[X]$ polynomi, joka saadaan f:stä muuttamalla kertoimet sivuluokikseen ideaalin $\langle p\rangle$ suhteen (ks. lemma 11.12). Ehdon (a) perusteella pätee $\overline{f} = \overline{a}_n X^n \neq 0$. Oletetaan, että f ei ole jaoton renkaassa $K[X]$. Gaussin lemman perusteella $f = gh$, missä $g, h \in R[X]$. Koska f on primitiivinen, kumpikaan g:stä ja h:sta ei ole vakio. Nyt $\overline{g} \cdot \overline{h} = \overline{f} = \overline{a}_n X^n$, mistä seuraa, että sekä $\overline{g}$ että $\overline{h}$ ovat muotoa cX^i. Jos kumpikaan polynomeista $\overline{g}$ ja $\overline{h}$ ei ole vakio, niin p jakaa polynomien g ja h vakiotermit. Tällöin kuitenkin p^2 jakaa a_0:n, mikä on vastoin oletusta. Siispä voidaan olettaa, että esimerkiksi $\overline{g}$ on vakio. Kuitenkaan g ei ole vakio, joten p jakaa g:n korkeimman asteen kertoimen. Tällöin p jakaa myös kertoimen a_n, mikä on jälleen vastoin oletusta. Polynomi f on siis jaoton renkaassa $K[X]$. Ehdon (b) tapaus todistetaan samalla tavalla. □

Esimerkki 11.17. Polynomi $X^5 - 12X^3 + 2X + 2$ nähdään jaottomaksi renkaassa $\mathbb{Q}[x]$, kun valitaan Eisensteinin kriteerissä $p = 2$. Aikaisemman esimerkin polynomi $3X^3 + 3X - 1$ on myös jaoton, mikä huomataan valitsemalla $p = 3$. Sen sijaan esimerkiksi polynomista $X^4 + 2X + 4$ Eisensteinin kriteeri ei sano mitään.

Lause 11.18. *Olkoon R tekijöihinjakorengas, jonka osamääräkunta on K, ja olkoon $f \in R[X]$ primitiivinen polynomi. Oletetaan, että $p \in R$ on alkualkio, joka ei jaa f:n korkeimman asteen termin kerrointa. Jos $\overline{f}$ on jaoton renkaassa $R/\langle p\rangle[X]$, niin f on jaoton renkaassa $K[X]$.*

Todistus. Jos f ei ole jaoton renkaassa $K[X]$, niin Gaussin lemman mukaan se jakautuu tekijöihin myös renkaassa $R[X]$. Jos $f = gh$, missä $g, h \in R[X]$, niin $\overline{f} = \overline{g} \cdot \overline{h}$ lemman 11.12 perusteella. Lisäksi kumpikaan g:stä ja h:sta ei ole vakio, koska f on primitiivinen. Jos $\overline{f}$ on jaoton, niin $\overline{g}$ tai $\overline{h}$ on yksikkö kokonaisalueessa $R/\langle p\rangle[X]$. Polynomirenkaan yksiköt ovat vakioita, joten koska g ja h eivät ole vakioita, p jakaa joko g:n tai h:n korkeimman asteen kertoimen. Tämä on mahdotonta, koska f:n korkeimman asteen kerroin ei ole jaollinen p:llä. Näin ollen f on jaoton renkaassa $K[X]$. □

Yllä oleva lause ei päde käänteisessä muodossa: esimerkiksi $X^3 + X + 1 \in \mathbb{Z}[X]$ on jaoton, mutta renkaassa $\mathbb{F}_3[X]$ se jakautuu tuloksi $(X-1)(X^2+X-1)$.

Esimerkki 11.19. Tarkastellaan polynomia $f = 3 + 2X - X^3 + 7X^4 \in \mathbb{Z}[X]$. Kirjoittamalla kertoimet modulo 2, saadaan polynomi $\overline{f} = 1 + X^3 + X^4 \in \mathbb{F}_2[X]$. Oletetaan, että $f = (X^2 + aX + b)(X^2 + cX + d)$ joillain $a, b, c, d \in \mathbb{F}_2$. Kertomalla tulo auki ja vertailemalla kertoimia nähdään, että

$$a + c = 1, \quad ac + b + d = 0, \quad ad + bc = 0 \quad \text{ja} \quad bd = 1.$$

Ensimmäisestä ehdosta seuraa, että täsmälleen yksi luvuista a ja c on nolla. Viimeisestä ehdosta nähdään, että $b = d = 1$. Tällöin kuitenkin $ad + bc = 1$, mikä on ristiriita. Siispä $\overline{f}$ on jaoton, joten myös f on jaoton kunnan $\mathbb{Q}$ suhteen. Samalla vaivalla on myös osoitettu, että mikä hyvänsä neljännen asteen polynomi $\sum_{i=0}^{4} a_i X^i$ on jaoton $\mathbb{Q}$:n suhteen, kunhan kertoimista a_0, a_3 ja a_4 ovat parittomia ja muut parillisia.

12. Yleiset laajennokset

Tässä luvussa tutustutaan kuntalaajennoksiin liittyviin peruskäsitteisiin.

12.1. Kuntalaajennos ja sen aste.

MÄÄRITELMÄ 12.1. Kunnan K *laajennos* L on mikä tahansa kunnan K ylikunta eli kunta, joka sisältää K:n alikuntanaan. Laajennosta merkitään L/K (lausutaan "L yli K:n"), ja kuntaa K kutsutaan laajennoksen *lähtökunnaksi.*

Luvussa 10 nähtiin, että kunnan K ylikunta L on myös K-algebra, skalaarikertolaskuna L:n kertolasku. Kunnan K laajennos voidaan itse asiassa määritellä hieman yleisemmin niin, että se on mikä tahansa K-algebra, joka on samalla kunta. Tällainen laajennos kuitenkin sisältää K:n kanssa isomorfisen alikunnan, jolloin tilanne käytännössä palautuu tässä esitettyyn.

Koska kunnan K laajennos on K-vektoriavaruus, sillä on hyvin määritelty dimensio.

MÄÄRITELMÄ 12.2. Kuntalaajennoksen L/K *aste* on L:n dimensio K-vektoriavaruutena. Astetta merkitään $[L : K]$, ja se voi olla joko positiivinen kokonaisluku tai ääretön.

Jos $[L : K]$ on äärellinen, laajennosta nimitetään *äärelliseksi laajennokseksi*, muuten kyseessä on *ääretön laajennos.*

Esimerkkejä kuntalaajennoksista:

- Kompleksilukujen kunta $\mathbb{C}$ on reaalilukujen $\mathbb{R}$ äärellinen laajennos. Pari $\{1, i\}$ muodostaa $\mathbb{C}$:n kannan, joten $[\mathbb{C} : \mathbb{R}] = 2$.
- Kunta $\mathbb{R}$ on $\mathbb{Q}$:n ääretön laajennos: esimerkiksi joukko $\{2^{1/n} \mid n \in \mathbb{N}\}$ on vapaa $\mathbb{Q}$:n suhteen, joten laajennoksella $\mathbb{R}/\mathbb{Q}$ ei ole äärellistä kantaa. Samoin $\mathbb{C}$ on $\mathbb{Q}$:n ääretön laajennos.
- Luvussa 10 käsiteltiin laajennoksia $K/\mathbb{F}_p$, missä $K = \mathbb{F}_p[X]/\langle f\rangle$ ja f oli jokin jaoton polynomi. Huomattiin, että tällaisen laajennoksen aste on sama kuin polynomin f aste.
- Jos K on kunta, polynomialgebra $K[X]$ on ääretönulotteinen K-algebra, joka sisältää K:n (samastettuna vakiopolynomien kanssa). Polynomialgebra ei kuitenkaan ole kunta, joten se ei ole K:n laajennos. Sen osamääräkunta on K-kertoimisten *rationaalilausekkeiden* joukko $K(X)$. Tämä joukko, joka koostuu osamääristä f/g, missä $f, g \in K[X]$ ja $g \neq 0$, on kunta ja sellaisena kunnan K laajennos. Kunta $K(X)$ sisältää alirenkaan $K[X]$, joten $[K(X) : K] = \infty$.

Seuraava lause koskee peräkkäisten laajennoksien asteita.

LAUSE 12.3. *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.

Ensinnäkin jokainen $x \in M$ on muotoa $\sum_j y_j b_j$ oleva lineaarikombinaatio, missä $y_j \in L$ kaikilla j. Toisaalta jokainen y_j on muotoa $\sum_i x_{ij} a_i$, missä $x_{ij} \in K$ kaikilla i. Täten $x = \sum_{i,j} x_{ij} a_i b_j$, joten joukko B virittää M:n K-vektoriavaruutena.

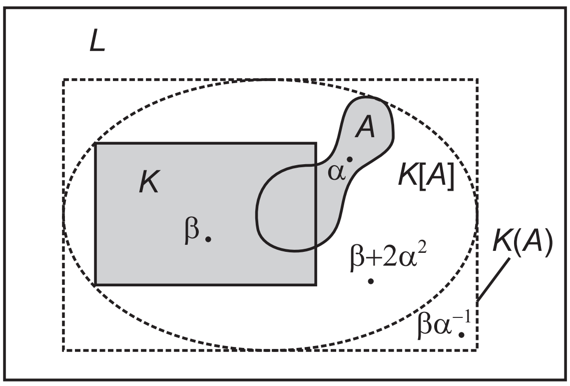
Osoitetaan sitten, että B on vapaa. Oletetaan, että $\sum_{i,j} x_{ij} a_i b_j = 0$, missä $x_{ij} \in K$ kaikilla i. Joukko $\{b_j\}$ on vapaa L-avaruudessa M, ja $\sum_i x_{ij} a_i \in L$ kaikilla j, joten $\sum_i x_{ij} a_i = 0$ kaikilla j. Edelleen joukko $\{a_i\}$ on vapaa K-avaruudessa L, joten $x_{ij} = 0$ 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 $i \neq k$ ja $j \neq l$. Näin saadaan lopulta $[M : K] = |B| = |I| \cdot |J| = [L : K][M : L]$. Tämä sisältää myös sen tapauksen, että $[L : K]$ tai $[M : L]$ on ääretön. □

Edellisestä lauseesta seuraa muun muassa, että jos $K \subset L \subset M$ ovat kuntia ja $[M : K] = n$, niin asteet $[M : L]$ ja $[L : K]$ ovat luvun n tekijöitä. Erityisesti, jos n on alkuluku, niin laajennoksella M/K ei ole epätriviaaleja alilaajennoksia L/K.

12.2. Virittäminen. Kuntalaajennoksen käsittelyä helpottaa huomattavasti, jos tiedetään sen olevan joidenkin tiettyjen alkioiden virittämä. Kuntalaajennoksen virittäminen ei tässä yhteydessä tarkoita samaa kuin sen virittäminen vektoriavaruutena. Erityisesti äärellisviritteisen kuntalaajennoksen asteen ei tarvitse välttämättä olla äärellinen.

Määritelmä 12.4. Olkoon L kunnan K laajennos, ja A joukko L:n alkioita. *Joukon A virittämä laajennoksen L/K alirengas* $K[A]$ on pienin L:n alirengas, joka sisältää sekä kunnan K että osajoukon A. *Joukon A virittämä laajennoksen L/K alilaajennos* $K(A)$ on puolestaan pienin L:n alikunta, joka sisältää sekä kunnan K että osajoukon A. Jos $A = \{a_1, \ldots, a_n\}$ on äärellinen, merkitään $K[A] = K[a_1, \ldots, a_n]$ ja $K(A) = K(a_1, \ldots, a_n)$. Tässä tapauksessa kuntaa $K(a_1, \ldots, a_n)$ nimitetään K:n *äärellisviritteiseksi* laajennokseksi.

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, mikä ei seuraa suoraan määritelmästä.



Kuva 23. Joukon A virittämät laajennoksen K/L alirengas $K[A]$ ja alilaajennos $K(A)$

Polynomialgebrat ovat vapaita äärellisviritteisiä algebroja. Sijoitushomomorfismista saadaan merkittävä yhteys K-kertoimisten polynomialgebrojen ja K:n äärellisviritteisten kuntalaajennosten välille. Seuraava lause konkretisoi tätä yhteyttä.

LAUSE 12.5. *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 $\varphi : K[X] \to L$ alkioihin $a_1, \ldots, a_n$ liittyvä sijoitushomomorfismi. Tämän algebrahomomorfismin kuva on $\{f(a_1, \ldots, a_n) \mid f \in K[X]\}$, ja se on algebran L alialgebra, siis alirengas. Toisaalta mikä tahansa L:n alirengas M, joka sisältää kunnan K lisäksi alkiot $a_1, \ldots, a_n$, sisältää myös kaikki näistä alkioista muodostettujen tulojen K-lineaariset kombinaatiot, joten $f(a_1, \ldots, a_n) \in M$ kaikilla $f \in K[X]$. Näin ollen $\operatorname{Im} \varphi \subset M$, mistä seuraa, että $K[a_1, \ldots, a_n] = \operatorname{Im} \varphi$. Renkaan $K[a_1, \ldots, a_n]$ osamääräkunta Q puolestaan koostuu alkioista p/q, missä $p, q \in K[a_1, \ldots, a_n]$ ja $q \neq 0$. Jokainen L:n alikunta, joka sisältää alkiot a_i, sisältää myös renkaan $K[a_1, \ldots, a_n]$ ja edelleen edellä mainitut osamäärät p/q. Täten $K(a_1, \ldots, a_n) = Q$. □

ESIMERKKI 12.6. Laajennoksen $\mathbb{C}/\mathbb{Q}$ alilaajennos $\mathbb{Q}(i)$ koostuu osamääristä $f(i)/g(i)$, missä $f, g \in \mathbb{Q}[X]$ ja $g \neq 0$. Koska $i^2 = -1$, voidaan rajoittua ensimmäisen asteen polynomeihin. Tällöin

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

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

$$\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\} = \mathbb{Q}[i].$$

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

Toisaalta voidaan osoittaa, että $\mathbb{Q}$:n laajennoksella $\mathbb{Q}(\pi) \subset \mathbb{R}$ ei ole äärellistä kantaa. Äärellisviritteinen ei siis välttämättä tarkoita samaa kuin äärellinen.

Äärettönviritteisten laajennosten ominaisuudet voidaan useimmiten palauttaa äärellisviritteiseen tapaukseen seuraavan lauseen avulla.

LAUSE 12.7. *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*

$$K(A) = \bigcup \{K(a_1, \ldots, a_n) \mid n \in \mathbb{N},\ a_1, \ldots, a_n \in A\}.$$

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, täytyy sen 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 ovat kunnassa $F(a_1, \ldots, a_n, b_1, \ldots, b_m)$, ja tämä kunta puolestaan sisältyy yhdisteeseen F. Siispä F on kunta, ja $K(A) = F$. $\square$

13. Algebralliset laajennokset

Vanhoina aikoina algebran tutkimuksen päämääränä oli oppia ratkaisemaan polynomiyhtälöitä. Niinpä erityisen tärkeää osaa klassisessa kuntalaajennosten teoriassa näyttelevät sellaiset laajennokset, joiden kaikki alkiot ovat joidenkin lähtökunnan polynomien juuria. Esimerkiksi jokainen kompleksiluku on jonkin korkeintaan toisen asteen polynomiyhtälön ratkaisu.

13.1. Algebrallisuus ja minimipolynomit.

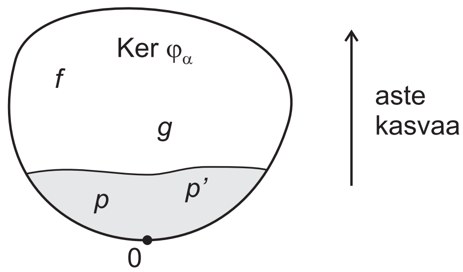
MÄÄRITELMÄ 13.1. Olkoon L kunnan K laajennos. Alkiota $\alpha \in L$ kutsutaan *algebralliseksi* kunnan K suhteen, jos on olemassa nollasta poikkeava polynomi $f \in K[X]$, jolle pätee $f(\alpha) = 0$. Jos tällaista polynomia ei ole, sanotaan, että α on *transkendenttinen* K:n suhteen. Jos kaikki L:n alkiot ovat algebrallisia K:n suhteen, sanotaan, että L on algebrallinen K:n suhteen, ja laajennosta L/K kutsutaan *algebralliseksi laajennokseksi*.

Oletetaan, että L on kunnan K laajennos ja $\alpha \in L$. Jos α on transkendenttinen K:n suhteen, niin kaikilla nollasta poikkeavilla polynomeilla $f \in K[X]$ pätee $f(\alpha) \neq 0$. Tämä tarkoittaa, että alkioon α liittyvän 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, ideaali $\operatorname{Ker} \varphi_\alpha$ on jonkin yhden polynomin p virittämä, eli $\operatorname{Ker} \varphi_\alpha = \langle p \rangle$. Koska jokainen ideaalin $\langle p \rangle$ polynomi on jaollinen p:llä, nähdään että p:n aste on minimaalinen joukon $\operatorname{Ker} \varphi_\alpha$ nollasta poikkeavien polynomien keskuudessa. Lisäksi myös kaikki p:n kanssa samanasteiset joukon $\operatorname{Ker} \varphi_\alpha$ polynomit ovat jaollisia p:llä, joten ne voivat erota tästä vain vakiokertoimella, ja jokainen niistä virittää saman ideaalin. Polynomin p määräämiseksi yksikäsitteisesti riittää siis viritysominaisuuden lisäksi vaatia esimerkiksi, että korkeimman asteen kerroin on 1 eli että p on *pääpolynomi*. Tätä polynomia nimitetään alkion α *minimipolynomiksi*.



KUVA 24. Sijoitushomomorfismin ytimen virittää mikä tahansa minimaalisen asteen omaava nollasta poikkeava polynomi. Nämä ovat kaikki toistensa liittoalkioita.

MÄÄRITELMÄ 13.2. Oletetaan, että $\alpha \in L$ on algebrallinen kunnan K suhteen. Alkion α *minimipolynomi* K:n suhteen on sellainen nollasta poikkeava pääpolynomi $p \in K[X]$, jolle pätee $p(\alpha) = 0$ ja jonka aste on pienin mahdollinen. Alkion α minimipolynomia kunnan K suhteen merkitään $p = \min(K, \alpha)$.

Huom. Koska määritelmän mukaan $p(\alpha) = 0$, niin $p \in \operatorname{Ker}\varphi_\alpha$. Määritelmää edeltävän päättelyn perusteella alkion α minimipolynomi voidaan karakterisoida niin, että se on *se pääpolynomi, joka virittää alkioon α liittyvän sijoitushomomorfismin ytimen.*

Esimerkki 13.3. 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 polynomin juuri. Näin ollen $\min(\mathbb{Q}, \sqrt{2}) = X^2 - 2$. Toisaalta $\min(\mathbb{R}, \sqrt{2}) = X - \sqrt{2}$.

Alkion α minimipolynomin hyödyllisyys piilee siinä, että sen aste kertoo laajennoksen $K(\alpha)$ asteen. Seuraavassa lauseessa tämä seikka on koottu yhteen muiden hyödyllisten ominaisuuksien kanssa.

Lause 13.4. *Olkoon L kunnan K laajennos, ja olkoon $\alpha \in L$ algebrallinen kunnan K suhteen. Tällöin*

i) *Minimipolynomi* $\min(K, \alpha)$ *on jaoton renkaassa $K[X]$.*
ii) *Jos $f \in K[X]$, niin $f(\alpha) = 0$, jos ja vain jos* $\min(K, \alpha)$ *jakaa f:n.*
iii) *$K[\alpha]$ on kunta, ja $K[\alpha] = K(\alpha)$.*
iv) *Jos n on polynomin* $\min(K, \alpha)$ *aste, niin alkiot $1, \alpha, \ldots, \alpha^{n-1}$ muodostavat laajennoksen $K(\alpha)/K$ kannan. Erityisesti $[K(\alpha) : K] = n < \infty$.*

Todistus. Merkitään $\min(K, \alpha) = p$. Aloitetaan kohdasta (ii). Jos $f(\alpha) = 0$ jollain $f \in K[X]$, niin $f \in \operatorname{Ker}\varphi_\alpha$. Koska p virittää ideaalin $\operatorname{Ker}\varphi_\alpha$, f on jaollinen p:llä. Toisaalta, jos $f = pg$ jollain $g \in K[X]$, niin $f(\alpha) = p(\alpha)g(\alpha) = 0$.

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

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

Lauseen 12.5 perusteella $f(\alpha)$ ja $g(\alpha)$ ovat renkaassa $K[\alpha]$. Tämä rengas on kokonaisalue, koska se on kunnan L alirengas, joten $f(\alpha) = 0$ tai $g(\alpha) = 0$. Nyt p:n asteen minimaalisuudesta seuraa, että $\deg(f) \geq \deg(p)$ tai $\deg(g) \geq \deg(p)$. Toisaalta p on jaollinen sekä f:llä että g:llä, joten joko f tai g on vakio. Vakiot ovat yksiköitä renkaassa $K[X]$, joten p on jaoton.

iii) Lauseen 12.5 mukaan $K[\alpha] = \operatorname{Im}\varphi_\alpha$, ja toisaalta $\langle p \rangle = \operatorname{Ker}\varphi_\alpha$. Algebrojen homomorfialauseesta seuraa täten, että $K[X]/\langle p \rangle \cong K[\alpha]$. Koska $K[\alpha] \subset L$ on kokonaisalue, $\langle p \rangle$ on alkuideaali. Toisaalta $K[X]$ on pääideaalirengas, joten sen jokainen nollasta poikkeava alkuideaali on maksimaalinen. Tästä seuraa, että $K[\alpha]$ on kunta. Lisäksi $K[\alpha] = K(\alpha)$, koska $K[\alpha] \subset K(\alpha)$ ja $K(\alpha)$ on pienin kunta, joka sisältää sekä K:n että alkion α.

iv) Olkoon $x \in K(\alpha)$. Kohdan (iii) nojalla $x = f(\alpha)$ jollain $f \in K[X]$. Jakoyhtälöstä nähdään, että $f = qp + r$, missä $\deg(r) < \deg(p) = n$. Nyt $f(\alpha) = r(\alpha)$, koska $p(\alpha) = 0$. Alkio $x = r(\alpha)$ voidaan siis kirjoittaa lineaarikombinaationa alkioista $1, \alpha, \ldots, \alpha^{n-1}$. Oletetaan sitten, että $\sum_{i=0}^{n-1} a_i\alpha^i = 0$ joillain $a_i \in K$. Tällöin polynomi $g = \sum_{i=0}^{n-1} a_i X_i$ on ytimessä $\operatorname{Ker}\varphi_\alpha = \langle p \rangle$, joten p jakaa f:n. Kuitenkin f:n aste on pienempi kuin n, joten f:n on oltava nollapolynomi. Tämä tarkoittaa sitä, että $a_i = 0$ kaikilla i, ja joukko $\{1, \alpha, \ldots, \alpha^{n-1}\}$ on vapaa. Kyseinen joukko muodostaa siis laajennoksen $K(\alpha)$ kannan kerroinkunnan K suhteen. $\square$

Esimerkki 13.5. Tarkastellaan laajennosta $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Polynomille $f = X^3-2$ pätee $f(\sqrt[3]{2}) = 0$, joten luvun $\sqrt[3]{2}$ minimipolynomi jakaa f:n. Toisaalta f on jaoton Eisensteinin kriteerin perusteella, joten se on luvun $\sqrt[3]{2}$ minimipolynomi. Täten laajennoksen $\mathbb{Q}(\sqrt[3]{2})$ aste on 3. Lisäksi $\mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q}(\sqrt[3]{2})$, joten jokainen laajennoksen alkio on muotoa $a + b\sqrt[3]{2} + c\sqrt[3]{4}$. Tämä koskee myös käänteislukuja x^{-1}, missä $x \in \mathbb{Q}[\sqrt[3]{2}]$.

Esimerkki 13.6. Kompleksiluku $\omega = e^{i\pi/3}$ on polynomin $X^3 - 1$ juuri. Tämä polynomi ei kuitenkaan ole ω:n minimipolynomi, sillä se jakautuu tekijöihin seuraavasti: $X^3 - 1 = (X - 1)(X^2 + X + 1)$. Näistä tekijöistä jälkimmäinen on jaoton rationaalijuuritestin perusteella, ja 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. Aiemmin todettiin, että sama ei päde toisinpäin: äärellisviritteinen laajennos ei ole välttämättä aina äärellinen. Käsitteet ovat kuitenkin yhtäpitäviä, mikäli laajennos on algebrallinen. Lisäksi äärellinen laajennos on aina algebrallinen. Nämä ajatukset on ilmaistu seuraavissa kahdessa lauseessa.

Lause 13.7. *Olkoon L kunnan K äärellinen laajennos. Tällöin L on äärellisviritteinen ja algebrallinen K:n suhteen.*

Todistus. Harjoitustehtävä. $\square$

Lause 13.8. *Olkoon L kunnan K laajennos. Oletetaan, että $\alpha_i \in L$ on algebrallinen K:n suhteen kaikilla i. 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 n:n suhteen. Tapaus $n = 1$ seuraa lauseesta 13.4. Oletetaan, että väite pätee renkaalle $K_1 = K[\alpha_1, \ldots, \alpha_{n-1}]$. Tällöin K_1 on kunta. Koska α_n on algebrallinen K:n ja siis myös K_1:n suhteen, lauseesta 13.4 seuraa, että $K[\alpha_1, \ldots, \alpha_n] = K_1[\alpha_n]$ on kunta. Edelleen saman lauseen mukaan $\min(K_1, \alpha_n)$ jakaa polynomin $\min(K, \alpha_n)$, joten

$$[K_1[\alpha_n] : K_1] \leq [K(\alpha_n) : K].$$

Induktio-oletuksen ja lauseen 12.3 perusteella

$$[K_1[\alpha_n] : K] = [K_1[\alpha_n] : K_1] \cdot [K_1 : K] \leq \prod_{i=1}^{n} [K(\alpha_i) : K].$$

$\square$

Edellisistä lauseista saadaan suoraan seuraava ehto alkion algebrallisuudelle.

Korollaari 13.9. *Olkoon L kunnan K laajennos. Tällöin $\alpha \in L$ on algebrallinen K:n suhteen, jos ja vain jos $[K(\alpha) : K]$ on äärellinen. Lisäksi L on algebrallinen, jos $[L : K]$ on äärellinen.*

Korollaarin jälkimmäisen väitteen implikaatiota ei voi kääntää. Esimerkiksi joukko $\{2^{1/n} \mid n \in \mathbb{N}\}$ virittää $\mathbb{Q}$:n algebrallisen laajennoksen, jonka aste on ääretön.

Nyt voidaan todistaa, että laajennoksen algebrallisuus on transitiivinen ominaisuus.

Lause 13.10. *Olkoot $K \subset L \subset M$ kuntia. Jos L/K ja M/L ovat algebrallisia laajennoksia, niin M/K on algebrallinen.*

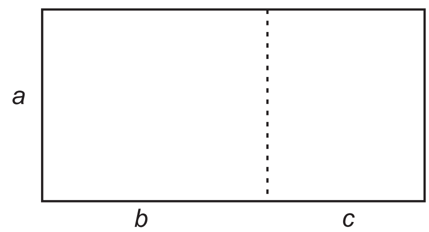
Todistus. Oletetaan, että $m \in M$. Olkoon $p = a_0 + a_1X + \cdots + a_nX^n$ alkion m minimipolynomi kunnan L suhteen. Merkitään $K_1 = K(a_0, \ldots, a_n)$. Koska L on algebrallinen K:n suhteen ja $a_i \in L$ jokaisella i, laajennos K_1 on äärellinen lauseen 13.8 perusteella. Nyt $p \in K_1[X]$, joten m on algebrallinen kunnan K_1 suhteen. Täten $[K_1(m) : K_1]$ on äärellinen, ja

$$[K_1(m) : K] = [K_1(m) : K_1] \cdot [K_1 : K] < \infty.$$

Edelleen $K(m) \subset K_1(m)$, joten $[K(m) : K] < \infty$. Lauseesta 13.7 seuraa, että $K(m)$ on algebrallinen K:n suhteen. Erityisesti siis m on algebrallinen K:n suhteen, ja koska m oli mielivaltainen, koko laajennos M/K on algebrallinen. □

13.2. Sovellus: Harppi–viivainkonstruktiot. Edellä opittua teoriaa voidaan käyttää tiettyjen klassisten geometristen konstruktioiden tutkimiseen. Nämä konstruktiot, joista ehkä tunnetuin kulkee nimellä ympyrän neliöinti, ovat askarruttaneet matemaatikkojen mieltä antiikista 1800-luvulle saakka, jolloin niiden toteuttaminen saatiin viimein saatiin osoitettua mahdottomaksi algebrallisten menetelmien avulla.

Antiikin Kreikassa geometrialla oli erityisen tärkeä sija matemaattisessa kirjallisuudessa. Algebrallisten merkintöjen puuttuessa geometriaa käytettiin kaikkien matemaattisten (eli lähinnä geometristen ja lukuteoreettisten) tulosten todistamiseen. Luvut esitettiin eripituisina janoina: yhteenlasku tulkittiin kahden janan liittämiseksi peräkkäin, ja kahden luvun tulo tarkoitti sellaisen suorakulmion muodostamista, jonka sivut vastasivat kerrottavia lukuja. Näin voitiin todistaa 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 25. Geometrinen konstruktio osittelulain todistamiseksi

Perinteisen tarinan mukaan filosofi Platon[19] vaati, että geometriset konstruktiot olisi toteutettava vain harppia ja viivainta hyväksikäyttäen. Viivaimella sai

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

piirtää rajattoman pitkän suoran kahden tunnetun pisteen kautta, ja harpilla oli sallittua piirtää ympyrä, jonka keskipiste ja säde tunnettiin. (Oikeastaan säännöt olivat vielä tiukemmat, mutta yhtäpitävät tässä esitettyjen kanssa.) Pian esiin nousi 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. kostruktio 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 kielelle. Tarkasteltavana ovat pistejoukot $G \subset \mathbb{R}^2$, joita nimitetään *kuvioksi.* Kuvion G *suora* on suora, joka kulkee G:n kahden pisteen kautta. Kuvion G *ympyrä* taas on ympyrä, jonka keskipiste on G:ssä ja säde kahden G:n pisteen välinen etäisyys.

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 $G_{i+1} = G_i \cup \{P_{i+1}\}$ 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 $G_n = G$. Kuvion G *kunta* K_G on laajennos $\mathbb{Q}(A)$, missä A sisältää kaikkien G:n pisteiden x- ja y-koordinaatit.

Seuraava lause antaa algebrallisen ehdon kuvion konstruoitavuudelle.

LAUSE 13.11. *Jos kuvio G voidaan konstruoida kuviosta G_0, niin*

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

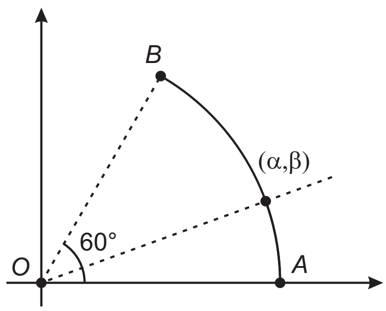
jollain $n \in \mathbb{N}$.

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 12.3. □

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

ESIMERKKI 13.12. *Kulman kolmiajako.* Osoitetaan, että $60°$ 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 $B = (1/2, \sqrt{3}/2)$. 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).



KUVA 26. Kulman kolmiajako

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

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

Koska $\cos 60° = 1/2$, tästä seuraa, että α on polynomin $8X^3 - 6X - 1$ juuri. Koska tämä polynomi on lisäksi jaoton $\mathbb{Q}$:n suhteen esimerkiksi rationaalijuuritestin perusteella, se on minimipolynomin $\min(\mathbb{Q}, \alpha)$ liittoalkio. Siispä kyseisen minimipolynomin aste on 3, ja edelleen $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Lauseiden 13.11 ja 12.3 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.

Tämä esimerkki osoittaa, että mielivaltaisen kulman kolmiajakamiseksi 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.

13.3. Transkendenttisuudesta. Luvun todistamiseksi algebralliseksi riittää löytää polynomi, jonka juuri kyseinen luku on. Transkendenttisuuden todistaminen on sen sijaan työläämpää. Jotkut tapaukset ovat kuitenkin selkeitä: Oletetaan esimerkiksi, että K on kunta, ja tarkastellaan polynomialgebran $K[X]$ jakokuntaa $K(X)$. Tämä kunta on K:n laajennos, ja alkio $X \in K(X)$ on selvästi transkendenttinen K:n suhteen. Kaikkien K-kertoimisten polynomien joukko $K[X]$ nimittäin 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 $f = 0$.

Useimmiten transkendenttisista luvuista puhuttaessa tarkoitetaan reaali- tai kompleksilukuja, jotka ovat transkendenttisia rationaalilukujen kunnan suhteen. Nykyään on selvää, 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 14.11). Siispä *algebrallisten lukujen joukko*

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

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. Tämän todisti Georg Cantor vuonna 1878. Kuitenkin jo ennen sitä — tarkemmin sanoen vuonna 1844 — Joseph Liouville oli osoittanut, että hänen nimeään kantavat Liouvillen luvut ovat transkendenttisia reaalilukuja. Tämä oli ensimmäinen osoitus transkendenttiseten 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 on jäänyt muun muassa se, onko e algebrallinen vai transkendenttinen laajennoksen $\mathbb{Q}(\pi)$ suhteen eli onko olemassa polynomia, jonka kertoimissa saa hyödyntää piin potensseja ja jolla on juurena e.

14. Juurikunnat

Mielivaltaisella polynomilla ei välttämättä ole juuria tarkasteltavassa kunnassa. Tässä luvussa tutkitaan sellaisia algebrallisia laajennoksia, jotka saadaan lisäämällä polynomeille juuria. Ääritapauksessa voidaan muodostaa laajennos, johon lisätään kaikkien polynomien kaikki mahdolliset juuret.

14.1. Määritelmä ja olemassaolo. Tarkastellaan aluksi esimerkkiä. Oletetaan, että K on kunta ja $f \in K[X]$ jokin polynomi, jolla on juuria kunnan K laajennoksessa L. Jos $\alpha_1, \ldots, \alpha_n \in L$ ovat polynomin f juuret, voidaan määritellä, että $K(\alpha_1, \ldots, \alpha_n)$ on f:n *juurikunta* laajennoksessa L. Juurikunta on siis pienin L:n alilaajennos, joka sisältää polynomin f juuret. Määritelmä on kuitenkin hieman kömpelö, koska siinä viitataan ympäröivään laajennokseen L, jossa polynomilla jo tiedetään olevan juuria. Lisäksi jää avoimeksi, sisältääkö L kaikki f:n juuret vai jääkö osa juurista mahdollisesti juurikunnan ulkopuolelle.

Seuraava tuttu lemma antaa juurten olemassaololle kriteerin, joka perustuu vain polynomin jaollisuusominaisuuksiin.

LEMMA 14.1. *Olkoon K kunta, ja $f \in K[X]$ nollasta poikkeava polynomi.*

a) *Alkio α on polynomin f juuri, jos ja vain jos $X - \alpha$ jakaa f:n.*
b) *Polynomin f juurten lukumäärä missä tahansa K:n laajennoksessa on korkeintaan* $\deg(f)$.

TODISTUS. a) Jakoyhtälöstä saadaan $f = (X - \alpha) \cdot g + r$, missä r on vakio. Nyt $f(\alpha) = r$, joten $f(\alpha) = 0$, jos ja vain jos $X - \alpha$ jakaa f:n.

b) Olkoon L kunnan K laajennos. Käytetään induktiota polynomin f asteen suhteen. Jos $\deg(f) = 0$, niin väite pätee selvästi. Oletetaan sitten, että väite pätee astetta n olevilla polynomeilla ja että f:n aste on $n + 1$. Jos f:llä ei ole juuria laajennoksessa L, niin väite pätee. Muussa tapauksessa voidaan valita juuri $\alpha \in L$ ja kirjoittaa $f = (X - \alpha) \cdot g$. Jokainen f:n juuri on nyt joko α tai jokin g:n juurista. Jälkimmäisiä on induktio-oletuksen mukaan korkeintaan n kappaletta, joten yhteensä juuria on korkeintaan $n + 1$. □

Lemman avulla päästään juurikunnan määritelmässä eroon viittauksesta ympäröivään kuntaan. Mikäli ympäröivää kuntaa ei ole, ei voida tietää, minkälaisia juuria annetulla polynomilla on eri laajennoksissa. Kuitenkin sellainen laajennos, jonka suhteen polynomi jakautuu ensimmäisen asteen tekijöihin, sisältää joka tapauksessa maksimaalisen määrän kyseisen polynomin juuria.

MÄÄRITELMÄ 14.2. Olkoon $f \in K[X]$ jokin polynomi. Kunnan K laajennos L on f:n *juurikunta* kunnan K suhteen, jos seuraavat ehdot toteutuvat:

(JK1) Polynomi f jakautuu 1. asteen polynomien tuloksi renkaassa $L[X]$.
(JK2) $L = K(\alpha_1, \dots, \alpha_n)$, missä $\alpha_1, \dots, \alpha_n \in L$ ovat polynomin f juuret.

Huomaa, että ehto (JK1) takaa, että polynomilla on suurin mahdollinen määrä juuria laajennoksessa L. Ehdolla (JK2) puolestaan varmistetaan, että L ei sisällä mitään ylimääräistä kyseisten juurten lisäksi.

Yleisemmin, jos $S \subset K[X]$ on joukko polynomeja, sanotaan, että L on joukon S juurikunta, jos jokainen $f \in S$ jakautuu ensimmäisen asteen tekijöihin L:n suhteen ja lisäksi $L = K(A)$, missä A koostuu kaikkien S:n polynomien juurista.

Polynomijoukon juurikunta ei ole yksikäsitteinen. Myöhemmin tullaan kuitenkin osoittamaan, että kaikki tietyn joukon juurikunnat ovat keskenään isomorfiset.

ESIMERKKI 14.3. Kompleksilukujen kunta $\mathbb{C}$ on polynomin $X^2 + 1$ juurikunta $\mathbb{R}$:n suhteen, sillä $\mathbb{C} = \mathbb{R}(i) = \mathbb{R}(i, -i)$. Yleisesti, jos L on kunnan K laajennos ja $\alpha^2 \in K$ jollain $\alpha \in L$, niin laajennos $K(\alpha) \subset L$ on polynomin $X^2 - \alpha^2$ juurikunta K:n suhteen. Toisaalta esimerkiksi $\mathbb{Q}(\sqrt[3]{2})$ ei ole polynomin $X^3 - 2$ juurikunta $\mathbb{Q}$:n suhteen, sillä

$$X^3 - 2 = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + \sqrt[3]{4})$$

eikä polynomilla $X^2 + \sqrt[3]{2}X + \sqrt[3]{4}$ ole reaalisia juuria; siis erityisesti sillä ei ole juuria kunnassa $\mathbb{Q}(\sqrt[3]{2})$.

Esimerkki 14.4. Olkoon $f = X^2 + X + 1 \in \mathbb{F}_2[X]$. Koska f on jaoton, tekijärengas $K = \mathbb{F}_2[X]/\langle f\rangle$ on kunnan $\mathbb{F}_p$ laajennos. Merkitään $\alpha = \overline{X}$. Nyt $\alpha^2 + \alpha = 1$, sillä $\alpha^2 + \alpha + 1 = 0$, ja $1 = -1$ kunnassa K. Täten

$$\begin{aligned}(X + \alpha)(X + (\alpha + 1)) &= X^2 + (2\alpha + 1)X + \alpha^2 + \alpha \\ &= X^2 + X + \alpha^2 + \alpha = X^2 + X + 1.\end{aligned}$$

Siispä f jakautuu renkaassa $K[X]$ ensimmäisen asteen tekijöihin $X+\alpha$ ja $X+\alpha+1$. Lisäksi $K = \mathbb{F}_2[\alpha] = \mathbb{F}_2[\alpha, \alpha+1]$, joten K on polynomin f juurikunta alkukunnan $\mathbb{F}_2$ suhteen.

Voidaan osoittaa, että millä tahansa polynomilla on olemassa juurikunta. Se löydetään jo tutuksi tulleella menetelmällä.

Lause 14.5. *Olkoon K kunta, ja olkoon $f \in K[X]$ jokin polynomi, joka ei ole vakio. Tällöin löytyy K:n äärellinen laajennos L, jonka suhteen f jakautuu ensimmäisen asteen tekijöihin.*

Todistus. Käytetään induktiota polynomin f asteen suhteen. Jos $\deg(f) = 1$, tapaus on selvä. Oletetaan sitten, että väite pätee tapauksessa n. Olkoon $f \in K[X]$ polynomi, jonka aste on $n+1$. Valitaan jokin f:n jaoton tekijä p, ja konstruoidaan kunta $K_1 = K[X]/\langle p\rangle$. Lähtökunta K voidaan samastaa K_1:n alikunnan kanssa, jolloin K_1 on K:n laajennos.

Merkitään $\alpha = \overline{X}$. Sijoitettaessa muuttujan X paikalle $\overline{X}$ polynomi p muuttuu polynomiksi $\overline{p}$. Täten $p(\alpha) = \overline{p} = 0$, eli α on polynomin p juuri ja siten myös f:n juuri. Näin ollen $f = (X-\alpha)\cdot g$ jollain $g \in K_1[X]$. Nyt polynomin g aste on n, joten induktio-oletuksen perusteella löytyy K_1:n äärellinen laajennos L, jonka suhteen g jakautuu 1. asteen tekijöihin. Siispä myös f jakautuu M:n suhteen ensimmäisen asteen tekijöihin, ja lisäksi $[L : K] = [L : K_1] \cdot \deg(p) < \infty$. □

Korollaari 14.6. *Jokaisella polynomilla $f \in K[X]$ on juurikunta kunnan K suhteen.*

Todistus. Edellisen lauseen avulla löydetään K:n laajennos L, jonka suhteen f jakautuu ensimmäisen asteen tekijöihin. Olkoot $\alpha_1, \ldots, \alpha_n \in L$ polynomin f juuret. Nyt $K(\alpha_1, \ldots, \alpha_n) \subset L$ on etsitty juurikunta. □

Mielivaltaisen äärellisen polynomijoukon $\{f_1, \ldots, f_n\}$ juurikunta löydetään soveltamalla edellistä lausetta tuloon $f_1 \cdots f_n$. Jos polynomeja on ääretön määrä, todistus on vaikeampi, ja se jätetään myöhemmäksi.

14.2. Algebrallinen sulkeuma. Tarkastellaan seuraavaksi niitä laajennoksia, jotka sisältävät kaikkien polynomiensa juuret.

Määritelmä 14.7. Kunta K on *algebrallisesti suljettu*, jos jokainen polynomi $f \in K[X]$ jakautuu ensimmäisen asteen tekijöihin renkaassa $K[X]$.

Algebrallisesti suljetut kunnat voidaan karakterisoida monella tapaa.

Lause 14.8. *Olkoon K kunta. Seuraavat ehdot ovat yhtäpitäviä.*

a) *K on algebrallisesti suljettu.*

b) *Jokaisella polynomilla $f \in K[X]$ on juuri K:ssa.*
c) *K:lla ei ole aitoja algebrallisia laajennoksia.*
d) *K:lla ei ole aitoja äärellisiä laajennoksia.*
e) *Jos L on K:n laajennos, niin K koostuu täsmälleen niistä L:n alkioista, jotka ovat algebrallisia K:n suhteen.*

Todistus. Harjoitustehtävä. □

Määritelmä 14.9. Kunnan K laajennosta L nimitetään K:n *algebralliseksi sulkeumaksi*, jos se on algebrallisesti suljettu ja algebrallinen K:n suhteen.

Kunnan algebrallinen sulkeuma on pienin algebrallisesti suljettu kunta, joka sisältää alkuperäisen kunnan. Jos nimittäin algebrallisesta sulkeumasta poistaa yhdenkin alkion, poistuu samalla jonkin polynomin juuri, koska jokainen sulkeuman alkio on algebrallinen. Toisaalta algebrallinen sulkeuma on algebrallisista laajennoksista suurin, koska se on algebrallisesti suljettu.

Esimerkki 14.10. Kompleksilukujen kunta $\mathbb{C}$ on algebrallisesti suljettu. Tämä tulos, jonka Gauss todisti vuonna 1799, tunnetaan *algebran peruslauseen* nimellä.[20] Sille on lukuisia todistuksia, jotka yleensä perustuvat kompleksianalyysiin. On olemassa myös Galois'n teoriaa käyttävä todistus, jossa tarvitaan algebrallisten menetelmien lisäksi vain väliarvolausetta. Koska $\mathbb{C}$ on algebrallisesti suljettu ja algebrallinen reaalilukujen suhteen, se on $\mathbb{R}$:n algebrallinen sulkeuma.

Tarkastellaan algebrallisten lukujen joukkoa

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

On helppo nähdä, että jokaisen $\mathbb{A}$-kertoimisen polynomin kaikki kompleksijuuret löytyvät $\mathbb{A}$:sta. Koska $\mathbb{C}$ on algebrallisesti suljettu, myös $\mathbb{A}$ on täten algebrallisesti suljettu. Lisäksi $\mathbb{A}$ on kunnan $\mathbb{Q}$ algebrallinen laajennos. Algebralliset luvut muodostavat siis $\mathbb{Q}$:n algebrallisen sulkeuman.

Voidaan osoittaa, että mielivaltaisella kunnalla K on algebrallinen sulkeuma ja että tämä sulkeuma on isomorfiaa vaille yksikäsitteinen. Tässä esitettävän olemassaolotodistuksen perusidea on käyttää Zornin lemmaa kaikkien K:n algebrallisten laajennosten kokoelmassa. Kyseinen kokoelma on kuitenkin liian laaja ollakseen joukko, joten sitä on rajoitettava jollain tapaa. Samalla on silti pidettävä huolta siitä, että kokoelma sisältää riittävän määrän kuntia, jotta todistus menee läpi. Tähän käytetään seuraavaa joukko-opillista lemmaa.

Lemma 14.11. *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 $|K^n|$. Jos K on äärellinen, tämä mahtavuus on $|K|^n$, muuten $|K^n| = |K|$. Koska $K[X]$ on numeroituva yhdiste joukoista $K_n[X]$, joukko-opin perustuloksista seuraa, että $|K[X]| \leq \max\{|K|, |\mathbb{N}|\}$.

[20]Oikeastaan Gaussin väitöskirjassaan esittämä todistus sisältää aukon. Jean-Robert Argand esitti täydellisen todistuksen vuonna 1814, ja Gauss julkaisi myöhemmin useitakin erilaisia aukottomia versioita.

Koska L/K on algebrallinen, jokainen L:n alkio on jonkin K-kertoimisen polynomin juuri. Indeksöidään jokaisen K-kertoimisen polynomin juuret $\alpha_1, \ldots, \alpha_r$ jossain mielivaltaisessa järjestyksessä, jolloin kutakin L:n alkiota α vastaa yksikäsitteinen pari $(p, i) \in K[X] \times \mathbb{N}$, missä $p = \min(K, \alpha)$ ja α:n indeksi polynomin p juurten joukossa on i. Näiden parien muodostaman joukon mahtavuus on korkeintaan $\max\{|K[X]|, |\mathbb{N}|\} = \max\{|K|, |\mathbb{N}|\}$. □

Lause 14.12. *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 S:n osajoukoille voidaan määritellä kuntarakenne, jonka suhteen niistä tulee K:n algebrallisia laajennoksia. Olkoon $\mathcal{A}$ nyt kaikkien tällaisten joukkoon S sisältyvien K:n 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 L_1:n laajennos. Tämä relaatio tekee kokoelmasta $\mathcal{A}$ osittaisjärjestyksen.

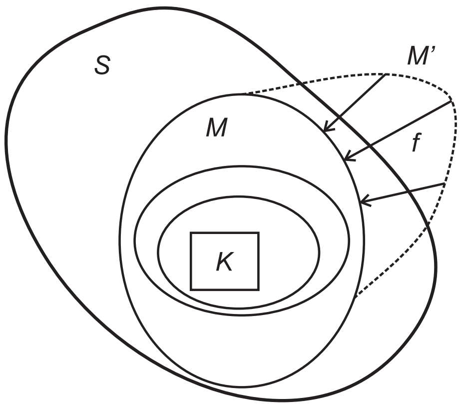
On helppo nähdä, että osittaisjärjestyksessä $(\mathcal{A}, \leq)$ jokaisella ketjulla on yläraja. Zornin lemmasta seuraa tällöin, että $\mathcal{A}$:ssa on maksimaalinen alkio M. Riittää osoittaa, että M on algebrallisesti suljettu. Olkoon sitä varten M' jokin M:n algebrallinen laajennos. Edellisen lemman perusteella

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

koska sekä M'/M että M/K ovat algebrallisia laajennoksia. Näin ollen löytyy jokin injektio $f : M' \to S$, jolle lisäksi pätee $f|_M = \mathrm{id}$. Kun määritellään kuvassa $f(M')$ laskutoimitukset kaavoilla

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

joukosta $f(M') \subset S$ tulee M:n algebrallinen laajennos. Nyt M:n maksimaalisuudesta seuraa, että $f(M') = M$, joten $M' = M$, koska $f|_M = \mathrm{id}$ ja f on injektio. Siispä M on algebrallisesti suljettu ja kunnan K algebrallinen sulkeuma.



Kuva 27. Maksimaalinen algebrallinen laajennos M on kunnan K algebrallinen sulkeuma.

□

KOROLLAARI 14.13. *Jokaisella polynomijoukolla* $S \subset K[X]$ *on juurikunta kunnan* K *suhteen.*

TODISTUS. Olkoon M kunnan K algebrallinen sulkeuma. Tällöin jokainen polynomi $f \in S$ jakautuu ensimmäisen asteen tekijöihin M:n suhteen. Olkoon A joukko, joka sisältää kaikki S:n polynomien juuret. Nyt $K(A)$ on etsitty juurikunta. $\square$

15. Laajennosten väliset homomorfismit

Rakenteiden väliset homomorfismit auttavat selvittämään rakenteiden suhteita toisiinsa. Rakenteen sisäiset isomorfismit — eli niin sanotut automorfismit — auttavat vastaavasti rakenteen omien ominaisuuksien selvittämisessä. Automorfismit muodostavat aina ryhmän, ja tällä tavoin ryhmäteoriasta tuttuja tuloksia päästään käyttämään hyväksi uusilla alueilla. Kuntalaajennosten yhteydessä automorfismien tutkiminen johtaa Galois'n teoriaan, jolla on lukemattomia sovelluksia lukuteoriassa ja yleisten kuntien teoriassa.

15.1. Homomorfismin määritelmä ja Galois'n ryhmä.

Määritelmä 15.1. Kunnan K laajennosten välistä kuntahomomorfismia σ kutsutaan *K-laajennosten homomorfismiksi* tai lyhyemmin *K-homomorfismiksi*, jos $\sigma(a) = a$ kaikilla $a \in K$.

Kuntalaajennosten välinen kuntahomomorfismi σ on siis K-homomorfismi, jos se kiinnittää lähtökunnan K. Tämä on yhtäpitävää se kanssa, että σ on samalla K-algebrahomomorfismi, jolloin se säilyttää skalaarikertolaskun. Jos nimittäin σ on K-algebrojen välinen homomorfismi, niin kaikilla $a \in K$ pätee $\sigma(a) = \sigma(a.1) = a.\sigma(1) = a$. Toisaalta, jos σ on mielivaltainen K:n kiinnittävä kuntahomomorfismi, niin $\sigma(ab) = \sigma(a)\sigma(b) = a\sigma(b)$.

Koska kuntahomomorfismit ovat aina injektioita, myös laajennosten väliset homomorfismit ovat injektioita. Lisäksi, jos $[L_1 : K] = [L_2 : K] < \infty$, niin laajennosten L_1 ja L_2 välinen homomorfismi on surjektio, koska se on injektio kahden samanulotteisen vektoriavaruuden välillä. Erityisesti äärellisen laajennoksen K-homomorfismit ovat aina bijektioita: niin sanottuja *K-automorfismeja*.

Määritelmä 15.2. Kunnan K laajennoksen L *Galois'n ryhmä* $\mathrm{Gal}(L/K)$ on kaikkien K-automorfismien $\sigma : L \to L$ muodostama ryhmä.

Galois'n ryhmä on siis kaikkien L:n automorfismien ryhmässä $\mathrm{Aut}(L)$ se aliryhmä, joka kiinnittää lähtökunnan K.

Tarkastellaan joukon X virittämää kunnan K laajennosta $K(X)$. Koska jokainen K-automorfismi säilyttää alkioiden tulot ja K-kertoimiset lineaarikombinaatiot, nähdään, että virittäjäalkioiden kuvat määrittävät automorfismin täysin. Puetaan tämä havainto täsmälliseen muotoon seuraavassa lemmassa.

Lemma 15.3. *Olkoon $K(X)$ joukon X virittämä K:n laajennos, ja olkoot $\sigma, \tau \in \mathrm{Gal}(K(X)/K)$. Jos $\sigma|_X = \tau|_X$, niin $\sigma = \tau$.*

15.2. Juurten kuvautuminen. Osoittautuu, että kuntalaajennosten väliset homomorfismit kuvaavat polynomien juuria toisikseen. Tämä tarjoaa erittäin hyödyllisen tavan päästä käsiksi erityisesti algebrallisten laajennosten välisiin homomorfismeihin.

Lause 15.4. *Olkoon $\sigma : L_1 \to L_2$ jokin K-laajennosten homomorfismi, ja olkoon $\alpha \in L_1$ algebrallinen lähtökunnan K suhteen. Jos polynomille $f \in K[X]$ pätee $f(\alpha) = 0$, niin $f(\sigma(\alpha)) = 0$. Lisäksi* $\min(K, \alpha) = \min(K, \sigma(\alpha))$.

Todistus. Merkitään $f = b_0 + b_1X + \cdots + b_nX^n$. Koska $b_i \in K$ kaikilla i ja σ on K-homomorfismi, nähdään että $\sigma(b_i) = b_i$ kaikilla i. Täten

$$f(\sigma(\alpha)) = \sum_i b_i\sigma(\alpha)^i = \sum_i \sigma(b_i)\sigma(\alpha)^i = \sigma(f(\alpha)) = \sigma(0) = 0.$$

Lisäksi, jos $p = \min(K, \alpha)$, niin $p(\sigma(\alpha)) = 0$, joten alkion $\sigma(\alpha))$ minimipolynomi jakaa p:n. Toisaalta p on jaoton pääpolynomi, joten täytyy olla $p = \min(K, \sigma(\alpha))$. □

Korollaari 15.5. *Jos L on kunnan K äärellinen laajennos, niin* $\mathrm{Gal}(L/K)$ *on äärellinen ryhmä.*

Todistus. Laajennos on äärellinen, jos ja vain jos se on äärellisen monen algebrallisen alkion virittämä. Olkoon $L = K(\alpha_1, \ldots, \alpha_n)$, ja olkoon p_i alkion α_i minimipolynomi kaikilla i. Jokainen K-automorfismi määräytyy täysin sen mukaan, mihin virittäjäalkiot kuvautuvat. Toisaalta edellisen lauseen mukaan jokainen α_i voi kuvautua vain jollekin polynomin p_i juurista, joita on äärellinen määrä. Yhteensä erilaisia automorfismeja on siis vain äärellisen monta. □

Esimerkki 15.6. Tarkastellaan laajennosta $\mathbb{C}/\mathbb{R}$. Voidaan helposti osoittaa, että kuvaukset id sekä $\sigma : a + bi \mapsto a - bi$ ovat $\mathbb{R}$-automorfismeja. Koska lisäksi $\mathbb{C} = \mathbb{R}(i)$, jokainen $\mathbb{R}$-automorfismi määräytyy sen perusteella, miten se kuvaa alkion i. Tämän alkion minimipolynomi on $p = X^2 + 1$, ja sillä on juurina i ja $-i$. Lauseen 15.4 perusteella jokainen $\mathbb{R}$-automorfismi τ permutoi p:n juuria, joten täytyy päteä joko $\tau(i) = i$ tai $\tau(i) = -i$. Edellisessä tapauksessa $\tau = \mathrm{id}$, jälkimmäisessä $\tau = \sigma$. Täten $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, \sigma\}$.

Lauseen 15.4 tulos voidaan myös kääntää: jos α ja α' ovat jonkin jaottoman polynomin juuria, niin löytyy sellainen automorfismi, joka kuvaa alkion α alkiolle α'. Tämän tuloksen todistaminen jätetään myöhemmäksi.

15.3. Galois'n teorian peruslause. Kuntalaajennoksen automorfismiryhmän rakenteen selvittäminen auttaa laajennoksen ominaisuuksien tutkimisessa. Tärkeä vastaavuus saadaan liittämällä automorfismiryhmän aliryhmät niihin kuntiin, jotka niiden alkiot kiinnittävät. Tutkitaan seuraavaksi tätä niin kutsuttua *Galois'n yhteyttä*.

Jokaiseen K:n laajennokseen L liittyy automorfismiryhmä $\mathrm{Gal}(K/L)$. Toisaalta jokaiseen L:n kunta-automorfismien joukkoon $S \subset \mathrm{Aut}(L)$ voidaan liittää *kiintokunta*

$$\mathrm{Fix}(S, L) = \{a \in L \mid \sigma(a) = a \text{ kaikilla } \sigma \in S\}.$$

On helppo nähdä, että kiintokunta todellakin on kunta, jolloin se on kunnan L alikunta. Lisäksi, jos S sisältää vain K-automorfismeja eli $S \subset \mathrm{Gal}(L/K)$, niin $K \subset \mathrm{Fix}(S, L)$ eli $\mathrm{Fix}(S, L)$ on kunnan K laajennos.

Oletetaan seuraavassa, että L on kunta, ja yksinkertaistetaan merkintöjä kirjoittamalla $\mathrm{Gal}(L/K) = \mathrm{Gal}(K)$ ja $\mathrm{Fix}(S, L) = \mathrm{Fix}(S)$. Kiintokuntien ja Galois'n ryhmien välille saadaan seuraavan lauseen mukainen vastaavuus.

Lause 15.7. *Olkoon L kunta. Tällöin seuraavat ehdot pätevät:*

a) *Jos $K_1 \subset K_2$ ovat L:n alikuntia, niin* $\mathrm{Gal}(K_2) \leq \mathrm{Gal}(K_1)$.

b) *Jos* $S_1 \subset S_2 \subset \mathrm{Aut}(L)$*, niin* $\mathrm{Fix}(S_2) \subset \mathrm{Fix}(S_1)$*.*
c) *Jos* $S \subset \mathrm{Aut}(L)$*, niin* $\mathrm{Fix}(S) = \mathrm{Fix}(\mathrm{Gal}(\mathrm{Fix}(S)))$*.*
d) *Jos* K *on jokin kunnan* L *alikunta, niin* $\mathrm{Gal}(K) = \mathrm{Gal}(\mathrm{Fix}(\mathrm{Gal}(K)))$*.*

Todistus. Väitteet (a) ja (b) seuraavat suoraan kiintokunnan ja Galois'n ryhmän määritelmistä. Todistetaan väitteet (c) ja (d).

Oletetaan ensin, että S on jokin kunnan L automorfismien joukko, ja merkitään $K = \mathrm{Fix}(S)$. Koska S:n alkiot kiinnittävät K:n, niin $S \subset \mathrm{Gal}(K)$. Kohdasta (b) seuraa, että $\mathrm{Fix}(\mathrm{Gal}(K)) \subset \mathrm{Fix}(S) = K$. Toisaalta jokainen ryhmän $\mathrm{Gal}(K)$ alkio kiinnittää K:n, joten $K \subset \mathrm{Fix}(\mathrm{Gal}(K))$.

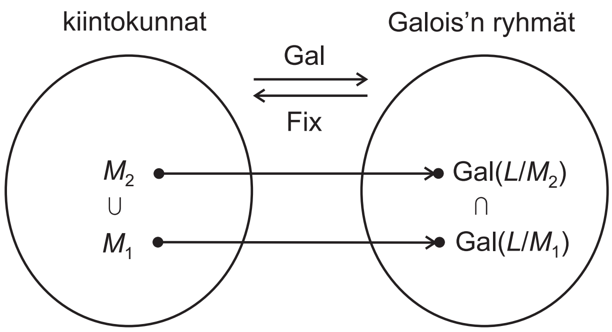
Oletetaan sitten, että K on kunnan L alikunta, ja merkitään $H = \mathrm{Gal}(K)$. Nyt $K \subset \mathrm{Fix}(\mathrm{Gal}(K))$, joten kohdan (a) mukaan

$$\mathrm{Gal}(\mathrm{Fix}(\mathrm{Gal}(K))) \subset \mathrm{Gal}(K) = H.$$

Toisaalta jokainen H:n alkio kiinnittää kunnan $\mathrm{Fix}(H)$, joten $H \subset \mathrm{Gal}(\mathrm{Fix}(H))$. □

Yllä olevan lauseen sanoma on, että on olemassa bijektiivinen, inkluusiosuunnan kääntävä vastaavuus Galois'n ryhmien $\mathrm{Gal}(L/M) \leq \mathrm{Gal}(L/K)$ ja kiintokuntien $\mathrm{Fix}(S, L) \subset L$ välillä, missä $K \subset M \subset L$ ja S on ryhmän $\mathrm{Gal}(L/K)$ osajoukko. Tämän vastaavuuden antaa kuvaus $M \mapsto \mathrm{Gal}(L/M)$, ja sen käänteisvastaavuus on muotoa $H \mapsto \mathrm{Fix}(H, L)$. Vastaavuuden bijektiivisisyys seuraa lauseen kohdista (c) ja (d): Jos $M_1, M_2 \subset L$ ovat kaksi kiintokuntaa, joille pätee $\mathrm{Gal}(M_1) = \mathrm{Gal}(M_2)$, niin $M_1 = \mathrm{Fix}(\mathrm{Gal}(M_1)) = \mathrm{Fix}(\mathrm{Gal}(M_2)) = M_2$. Toisaalta, jos $H \leq \mathrm{Gal}(L)$ on mikä hyvänsä Galois'n ryhmä, niin $\mathrm{Fix}(H)$ on kiintokunta, jolle pätee $\mathrm{Gal}(\mathrm{Fix}(H)) = H$.

Lauseen ehdot toteuttavaa vastaavuutta kutsutaan yleisesti *Galois'n vastaavuudeksi* tai *Galois'n yhteydeksi*. Sellainen esiintyy monilla muillakin aloilla, esimerkiksi algebrallisessa geometriassa polynomijoukkojen ja niiden sisältämien polynomien yhteisten nollakohtien joukkojen välillä.



Kuva 28. Galois'n yhteys liittää toisiinsa kiintokunnat ja niiden Galois'n ryhmät

Määritelmä 15.8. Olkoon L kunnan K laajennos. Kuntaa M, jolle pätee $K \subset M \subset L$, kutsutaan laajennoksen L/K *välikunnaksi*.

Jos S on joukko K-automorfismeja, niin kiintokunta $\mathrm{Fix}(S, L)$ sisältää K:n. Täten $\mathrm{Fix}(S, L)$ on laajennoksen L/K välikunta.

Olisi hyödyllistä, jos lauseen 15.7 määrittelemä bijektiivinen vastaavuus voitaisiin ulottaa *kaikkien* ryhmän $\mathrm{Gal}(L/K)$ aliryhmien ja *kaikkien* laajennoksen L/K välikuntien välille. Erityisesti jos laajennos L/K on äärellinen, pystyttäisiin tällöin löytämään kaikki kyseisen laajennoksen välikunnat tutkimalla laajennoksen äärellistä Galois'n ryhmää.

Haluttaisiin siis osoittaa, että jokainen ryhmän $\mathrm{Gal}(L/K)$ aliryhmä olisi Galois'n ryhmä ja jokainen L/K:n välikunta olisi kiintokunta. Kuitenkin voi käydä esimerkiksi niin, että $\mathrm{Gal}(L/K)$ kiinnittää muutakin kuin lähtökunnan K. Tällöin triviaali välikunta K ei ole minkään aliryhmän $H \leq \mathrm{Gal}(L/K)$ kiintokunta. Tämä antaa aiheen seuraavaan määritelmään.

MÄÄRITELMÄ 15.9. Algebrallista laajennosta L/K kutsutaan *Galois'n laajennokseksi*, jos $K = \mathrm{Fix}(\mathrm{Gal}(L/K), L)$.

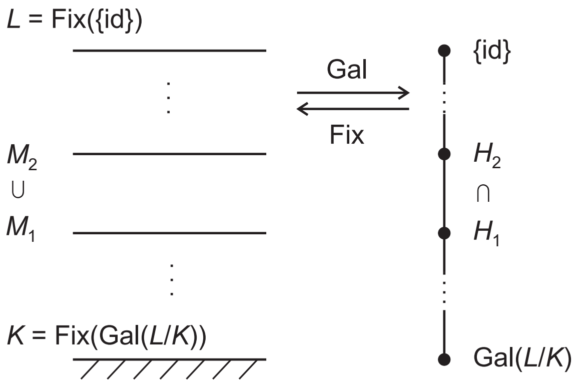
Kunnan K algebrallinen laajennos on siis Galois'n laajennos (tai lyhyemmin, predikatiivina: Galois), jos kaikkien K-automorfismien kiinnittämä joukko on täsmälleen K.

ESIMERKKI 15.10. Laajennoksen $\mathbb{C}/\mathbb{R}$ Galois'n ryhmä on $\{\mathrm{id}, \sigma\}$, missä σ on kompleksikonjugointi $a + bi \mapsto a - bi$. Kompleksikonjugoinnille pätee $\sigma(x) = x$ jos ja vain jos $x \in \mathbb{R}$, joten $\mathbb{C}$ on $\mathbb{R}$:n Galois'n laajennos.

Osoittautuu, että jos laajennos L/K on Galois'n laajennos, niin jokainen laajennos L/M, missä M on L/K:n välikunta, on myös Galois. Tästä seuraa puolestaan, että jokainen välikunta on kiintokunta (nimittäin $M = \mathrm{Fix}(\mathrm{Gal}(L/M))$) ja lopulta jokainen Galois'n ryhmän aliryhmä on Galois'n ryhmä.

LAUSE 15.11 (Galois'n teorian peruslause). *Oletetaan, että L on kunnan K äärellinen Galois'n laajennos. Tällöin kuvaus $M \mapsto \mathrm{Gal}(L/M)$ antaa bijektiivisen, inkluusiosuunnan kääntävän vastaavuuden laajennoksen L/K välilaajennosten sekä ryhmän $\mathrm{Gal}(L/K)$ aliryhmien välillä. Tämän vastaavuuden käänteisvastaavuus on $H \mapsto \mathrm{Fix}(H, L)$.*

TODISTUS. Sivuutetaan. $\square$



KUVA 29. Galois'n laajennokseen liittyvän Galois'n ryhmän jokainen aliryhmä vastaa jotain välikuntaa

16. Valikoituja aiheita

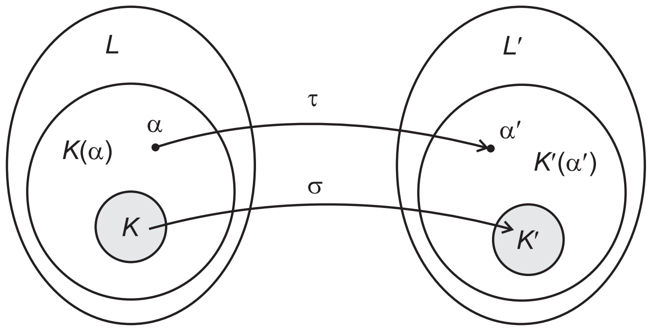
Materiaalin viimeisessä luvussa käydään läpi väliinjääneitä kuntalaajennoksiin liittyviä tuloksia ja tutustutaan vielä hieman tarkemmin Galois'n teoriaan.

16.1. Isomorfismien jatkaminen. On hyödyllistä tietää, millaisessa tilanteessa kuntien välinen isomorfismi voidaan laajentaa algebrallisten laajennosten väliseksi isomorfismiksi.

Kuntien välistä homomorfismia $\sigma : K \to K'$ vastaa polynomirenkaiden homomorfismi $K[X] \to K'[X]$, joka kuvaa polynomin $\sum_i a_i X^i$ polynomille $\sum_i \sigma(a_i) X^i$. Myös tätä johdettua homomorfismia merkitään kirjaimella σ, mikäli sekaantumisen vaaraa ei ole. Seuraava lemma kertoo, millä tavalla annettua kuntaisomorfismia voidaan jatkaa yksinkertaiseen algebralliseen laajennokseen.

LAUSE 16.1. *Oletetaan, että $\sigma : K \to K'$ on kuntaisomorfismi. Olkoon f jokin jaoton K-kertoiminen polynomi, olkoon α polynomin f juuri jossain K:n laajennoksessa L, ja olkoon α' vastaavasti polynomin $\sigma(f)$ juuri jossain K':n laajennoksessa L'. Tällöin on olemassa isomorfismi $\tau : K(\alpha) \to K'(\alpha)$, jolle pätee*

$$\tau|_K = \sigma \quad ja \quad \tau(\alpha) = \alpha'.$$



KUVA 30. Isomorfismi voidaan jatkaa yksinkertaiseen laajennokseen.

TODISTUS. Merkitään $g = \sigma(f)$. Koska f on jaoton ja $f(\alpha) = 0$, alkion α minimipolynomi on f:n liittoalkio. Täten f virittää alkioon α liittyvän sijoitushomomorfismin ytimen. Vastaava pätee polynomille $g \in K'[X]$, sillä se on myös jaoton. Algebrojen homomorfialauseesta saadaan K-algebrojen isomorfismit

$$\varphi : K[X]/\langle f \rangle \to K(\alpha) \qquad \text{ja} \qquad \psi : K'[X]/\langle g \rangle \to K'(\alpha).$$

Toisaalta kaava $h \mapsto \sigma(h) + \langle g \rangle$ määrittelee surjektiivisen rengashomomorfismin $\chi : K[X] \to K'[X]/\langle g \rangle$. Tämän homomorfismin ydin on $\langle f \rangle$, joten algebrojen homomorfialauseesta saadaan isomorfismi $\overline{\chi} : K[X]/\langle f \rangle \to K'[X]/\langle g \rangle$. Nyt yhdistetty kuvaus $\tau = \psi \circ \overline{\chi} \circ \varphi^{-1} : K(\alpha) \to K(\alpha')$ on kuntaisomorfismi, jolle pätee

$$\tau : \alpha \overset{\varphi^{-1}}{\mapsto} X + \langle f \rangle \overset{\overline{\chi}}{\mapsto} X + \langle g \rangle \overset{\psi}{\mapsto} \alpha'.$$

Lisäksi $\tau|_K = \sigma$, sillä φ ja ψ kuvaavat vakiopolynomit vastaavasti kuntien K ja K' alkioille. $\square$

Esimerkki 16.2. Yllä olevaa lausetta voidaan käyttää myös tilanteessa, jossa K ja K' ovat sama kunta ja $\sigma = \mathrm{id}_K$. Jos tällöin α ja α' ovat saman jaottoman polynomin juuria, niin on olemassa isomorfismi $K(\alpha) \cong K(\alpha')$, joka kuvaa $\alpha \mapsto \alpha'$ ja joka kiinnittää lähtökunnan K. Esimerkiksi polynomi $X^4 - 2$ on jaoton $\mathbb{Q}$:n suhteen, ja sillä on kompleksijuuret $\pm\sqrt[4]{2}$ ja $\pm i\sqrt[4]{2}$. On siis olemassa muun muassa $\mathbb{Q}$-isomorfismi $\sigma : \mathbb{Q}(\sqrt[4]{2}) \to \mathbb{Q}(i\sqrt[4]{2})$, jolle pätee $\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$, sekä automorfismi $\tau \in \mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q})$, jolle pätee $\sigma(\sqrt[4]{2}) = -\sqrt[4]{2}$.

Osoittautuu, että kuntaisomorfismi voidaan aina laajentaa jopa juurikuntien isomorfismiksi. Tämän tuloksen todistus perustuu Zornin lemmaan. Oletetaan, että $\sigma : K \to K'$ on jokin K-isomorfismi. Olkoon $S = \{f_i\}_{i\in I}$ joukko K-kertoimisia polynomeja, ja olkoon $S' = \{\sigma(f_i)\}$ vastaava joukko K'-kertoimisia polynomeja. Olkoon lisäksi L polynomijoukon S jokin juurikunta K:n suhteen, ja L' vastaavasti S':n jokin juurikunta kunnan K' suhteen.

Lause 16.3 (Isomorfismien jatkaminen). *Olkoon $\alpha \in L$, ja olkoon p alkion α minimipolynomi K:n suhteen. Olkoon lisäksi $\alpha' \in L'$ mikä tahansa polynomin $\sigma(p)$ juuri. Tällöin löytyy isomorfismi $\tau : L \to L'$, jolle pätee $\tau|_K = \sigma$ ja $\tau(\alpha) = \alpha'$.*

Todistus. Olkoon $\mathcal{F}$ kaikkien parien (F, φ) joukko, missä F on kunnan L alikunta ja $\varphi : F \to L'$ on kuntahomomorfismi, jolle pätee $\varphi|_K = \sigma$. Tämä joukko sisältää parin (K, σ), joten $\mathcal{F} \neq \emptyset$. Joukko $\mathcal{F}$ voidaan varustaa osittaisjärjestyksellä määrittelemällä $(F, \varphi) \leq (F', \varphi')$ silloin, kun $F \subset F'$ ja $\varphi'|_F = \varphi$. Olkoon $\{(F_i, \varphi_i)\}_{i\in I}$ jokin ketju osittaisjärjestyksessä $\mathcal{F}$. Määrittelemällä

$$F = \bigcup_{i\in I} F_i \quad \text{ja} \quad \varphi(a) = \varphi_i(a), \quad \text{kun } a \in F_i,$$

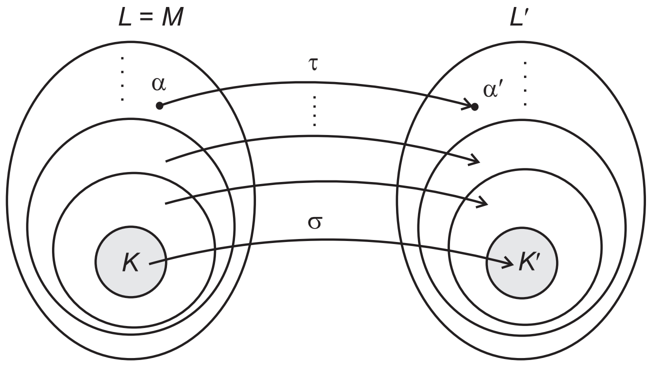
saadaan hyvin määritelty pari $(F, \varphi) \in \mathcal{F}$, joka on ketjun $\{(F_i, \varphi_i)\}_{i\in I}$ yläraja. Zornin lemman perusteella joukossa $\mathcal{F}$ on maksimaalinen alkio (M, τ).

Osoitetaan, että $M = L$ ja $\tau(M) = L'$. Jos $M \subsetneq L$, niin löytyy jokin polynomi $f \in S$, jonka kaikki juuret eivät ole kunnassa M. Olkoon α jokin tällainen juuri, ja olkoon $p = \min(K, \alpha)$. Merkitään $q = \sigma(p) \in S'$. Koska L' on joukon S' juurikunta, löytyy jokin $\alpha' \in L'$, jolle pätee $q(\alpha) = 0$. Lauseen 16.1 perusteella on olemassa isomorfismi $\varphi : M(\alpha) \to \tau(M)(\alpha')$, jolle pätee $\varphi|_M = \tau$. Tämä on ristiriidassa parin (M, τ) maksimaalisuuden kanssa, joten $M = L$. Lisäksi on helppo osoittaa, että juurikunnan kuva $\tau(L)$ on puolestaan polynomijoukon S' juurikunta kunnan K' suhteen, mistä seuraa, että $\tau(L) = L'$. □

Isomorfismien jatkamislausetta käytetään usein konstruoimaan annetun laajennoksen automorfismeja eli Galois'n ryhmän alkioita. Lisäksi siitä seuraa suoraan juurikuntien ja algebrallisten sulkeumien yksikäsitteisyys.

Korollaari 16.4. *Olkoon K kunta, ja olkoon S joukko K-kertoimisia polynomeja. Kaikki S:n juurikunnat kunnan K suhteen ovat isomorfisia K:n laajennoksina. Erityisesti kaikki K:n algebralliset sulkeumat ovat isomorfisia.*

Todistus. Koska $\mathrm{id} : K \to K$ on kuntaisomorfismi, isomorfismien jatkamislauseesta saadaan K-laajennosten isomorfismi minkä tahansa kahden S:n juurikunnan välille. Toinen väite seuraa tästä suoraan, sillä kunnan K algebrallinen sulkeuma on samalla kaikkien K-kertoimisten polynomien joukon juurikunta. □



Kuva 31. Isomorfismi voidaan jatkaa juurikuntien isomorfismiksi.

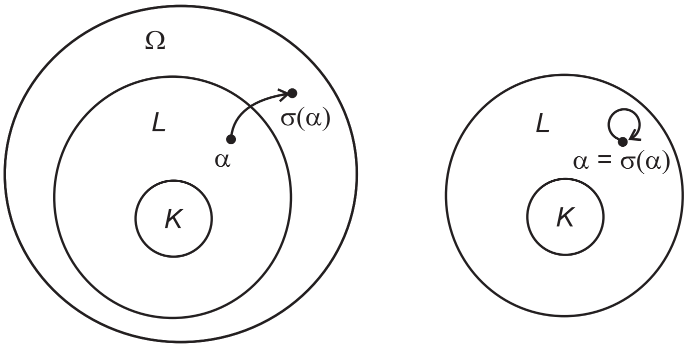
Nyt kun on todistettu algebrallisen sulkeuman olemassaolo ja yksikäsitteisyys isomorfiaa vaille, voidaan algebrallisista laajennoksista puhuttaessa aina rajoittua sopivan alkukunnan algebrallisen sulkeuman alikuntiin. Mikä tahansa algebrallinen laajennos nimittäin sisältyy johonkin algebralliseen sulkeumaan, ja kahden sulkeuman välinen isomorfismi kuvaa myös kyseisen laajennoksen tuon ennalta valitun sulkeuman alilaajennokseksi.

16.2. Galois'n laajennosten karakterisoinnista. Algebrallinen laajennos L/K on Galois, jos K on suurin L:n alikunta, jonka kaikki K-automorfismit kiinnittävät. Mitä enemmän K-automorfismeja on, sitä suuremman joukon ne kiinnittävät. Voidaan siis päätellä intuitiivisesti, että laajennos on Galois, jos siinä voidaan määritellä mahdollisimman suuri määrä K-automorfismeja.

Olkoon L kunnan K algebrallinen laajennos, ja olkoon Ω jokin K:n algebrallinen sulkeuma (jotka ovat siis kaikki keskenään isomorfisia). Isomorfismien jatkamislauseen perusteella jokainen L:n K-automorfismi voidaan jatkaa Ω:n K-automorfismiksi. Mutta mitkä Ω:n automorfismeista rajoittuvat L:n automorfismeiksi? Koska jokaisen K-kertoimisen jaottoman polynomin juuri voidaan isomorfismien jatkamislauseen perusteella kuvata toiselle saman polynomin juurelle, täytyisi L:n sisältää kaikki nämä juuret, jos se sisältää niistä yhdenkin, muuten joukko L ei ole vakaa kyseisessä kuvauksessa. Laajennoksen L täytyisi siis olla jonkin polynomijoukon juurikunta. Tätä ehtoa kutsutaan *normaalisuusehdoksi*: kunnan L kuvaa jossakin Ω:n K-automorfismissa σ kutsutaan L:n konjugaatiksi, ja normaalisuus takaa, että jokaiselle L:n konjugaatille pätee $\sigma(L) \subset L$. (Vertaa tätä aliryhmän normaalisuuden käsitteeseen.)

Laajennoksen automorfismien määrä voi rajoittua toisellakin tavalla. Jaottoman polynomin jokaisen juuren voi kuvata mille tahansa toiselle juurelle, mutta joskus käy niin, että erillisten juurien lukumäärä on pienempi kuin polynomin aste. Toisin sanoen jotkin polynomin ensimmäisen asteen tekijöistä ovat samoja. Tämä vähentää myös erilaisten automorfismien määrää.

Määritelmä 16.5. Olkoon K kunta, ja olkoon $p \in K[X]$ jokin jaoton polynomi. Oletetaan, että L on K:n laajennos ja $\alpha \in L$. Jos p on jaollinen polynomilla $(X - \alpha)^n$ jollain $n > 1$, sanotaan, että α on polynomin p *moninkertainen juuri*. Jos p:llä ei ole lainkaan moninkertaisia juuria juurikunnassaan K:n suhteen, sanotaan, että p on K:n suhteen *separoituva*.



KUVA 32. Algebrallisen laajennoksen automorfismeja menetetään, jos juuret kuvautuvat laajennoksen ulkopuolelle tai itselleen.

Polynomia f kutsutaan separoituvaksi, jos sen jokainen jaoton tekijä on separoituva. Polynomin separoituvuuden selvittämiseksi on olemassa näppärä testi, joka hyödyntää polynomin derivaatan käsitettä. Vaikka polynomialgebrassa ei voidakaan yleensä määritellä metriikkaa eikä raja-arvoja, polynomeja voidaan silti derivoida muodollisesti tutuilla derivointikaavoilla.

LEMMA 16.6. *Olkoon K kunta, ja olkoon $f \in K[X]$ polynomi, joka ei ole vakio. Tällöin f on separoituva, jos ja vain jos* $\mathrm{syt}(f, f') = 1$.

TODISTUS. Osoitetaan ensin, että jos $f, g \in K[X]$ ja L on K:n laajennos, niin f ja g ovat keskenään jaottomia renkaassa $L[X]$, jos ja vain jos ne ovat keskenään jaottomia renkaassa $K[X]$. Toinen suunta on selvä, joten oletetaan, että $\mathrm{syt}(f, g) = 1$ renkaassa $K[X]$. Tällöin $af + bg = 1$ joillain $a, b \in K[X]$. Tämä yhtälö pätee myös renkaassa $L[X]$, joten $\mathrm{syt}(f, g) = 1$ myös renkaassa $L[X]$.

Oletetaan nyt, että $\mathrm{syt}(f, f') = 1$, ja tarkastellaan f:n jakokuntaa L. Jos $\alpha \in L$ on sellainen, että $f = (X - \alpha)^2 \cdot g$, niin

$$f' = 2(X - \alpha) \cdot g + (X - \alpha)^2 \cdot g' = (X - \alpha)(2g + (X - \alpha)g'),$$

joten $X - \alpha$ jakaa myös polynomin f'. Tämä on ristiriita sen kanssa, että f ja f' ovat keskenään jaottomia renkaassa $L[X]$.

Oletetaan sitten, että polynomi f jakautuu juurikunnassaan L erillisiksi ensimmäisen asteen tekijöiksi, ja merkitään $f = \prod_{i=1}^n (X - \alpha_i)$, missä luvut $\alpha_i \in L$ ovat erillisiä. Tulon derivointisäännön nojalla

$$f' = \sum_{i=1}^n \prod_{i \neq j} (X - \alpha_j).$$

Nyt jokaisella k pätee $f'(\alpha_k) = \prod_{k \neq j} (X - \alpha_j) \neq 0$, joten polynomeilla f ja f' ei ole yhteisiä juuria. Olkoon nyt $d \in K[X]$ jokin polynomien f ja f' yhteinen tekijä. Koska L on polynomin f juurikunta ja d on f:n tekijä, myös d:n kaikki juuret löytyvät kunnasta L. Lisäksi jokainen näistä juurista on polynomien f ja f' yhteinen juuri, koska d jakaa molemmat polynomit. Tällaisia juuria ei ole, joten polynomin d täytyy olla vakio. Täten polynomien f ja f' suurin yhteinen tekijä on yksikkö. □

Laajennoksen alkiota nimitetään separoituvaksi, jos sen minimipolynomi on separoituva. Koko laajennos on separoituva, jos sen jokainen alkio on separoituva. Seuraava lause, jonka todistuksen perusideaa hahmoteltiin yllä, esittää tärkeimmän tavan karakterisoida Galois'n laajennokset.

LAUSE 16.7. *Oletetaan, että L on kunnan K algebrallinen laajennos. Seuraavat ehdot ovat yhtäpitäviä:*

i) *L/K on Galois'n laajennos.*
ii) *L/K on normaali ja separoituva.*
iii) *L on jonkin separoituvista polynomeista koostuvan joukon juurikunta kunnan K suhteen.*

Jos lähtökunnan karakteristika on nolla, derivaattatestin perusteella jokainen laajennos on separoituva. Jos nimittäin f on jaoton polynomi ja polynomeilla f ja f' on yhteinen tekijä g, joka ei ole vakio, niin g:n täytyy olla f:n liittoalkio. Silloin $\deg(f) = \deg(g)$, mutta koska $\deg(f') = \deg(f) - 1$, niin g ei voi olla polynomin f' tekijä. Näin saadaan vielä eräs karakterisointi Galois'n laajennoksille siinä tapauksessa, että separoituvuutta ei tarvitse erikseen mainita.

LAUSE 16.8. *Oletetaan, että L on kunnan K algebrallinen laajennos ja K:n karakteristika on nolla. Tällöin L/K on Galois, jos ja vain jos se on jonkin polynomijoukon juurikunta K:n suhteen.*

16.3. Äärelliset kunnat. Luvussa 10 nähtiin, että jokaisen äärellisen kunnan koko on p^n, missä p on alkuluku ja n positiivinen kokonaisluku. Nyt voidaan lopulta osoittaa, että jokaista tällaista lukua p^n kohti on olemassa kyseistä kertalukua oleva kunta. Lisäksi kaikki samaa kertalukua olevat kunnat ovat keskenään isomorfisia.

LAUSE 16.9. *Olkoon p alkuluku ja n positiivinen kokonaisluku. On olemassa kunta K, jonka koko on p^n. Lisäksi tämä kunta on isomorfiaa vaille yksikäsitteinen.*

TODISTUS. Olkoon Ω kunnan $\mathbb{F}_p$ algebrallinen sulkeuma. Tarkastellaan polynomia $f = X^{p^n} - X$, ja merkitään sen juurten joukkoa $L \subset \Omega$. On helppo nähdä, että joukko L on kunnan Ω alikunta. Tällöin L myös sisältää välttämättä alkukunnan $\mathbb{F}_p$. Lisäksi $f' = p^n \cdot X^{p^n-1} - 1 = -1$, joten derivaattatestin perusteella f on separoituva kunnan $\mathbb{F}_p$ suhteen. Siispä kaikki f:n juuret ovat erillisiä, joten kunnan L koko on p^n.

Olkoon sitten M mikä tahansa kunta, jonka koko on p^n. Tämä kunta sisältää alkukuntanaan kunnan K, joka on isomorfinen kunnan $\mathbb{F}_p$ kanssa. Koska $|M^*| = p^n - 1$, niin $a^{p^n-1} = 1$ kaikilla $a \in M^*$. Täten jokainen kunnan M alkio on polynomin f juuri (sillä myös 0 on f:n juuri). Toisaalta polynomilla f on korkeintaan p^n juurta, joten M on f:n juurikunta kunnan K suhteen. Isomorfismien jatkamislauseesta seuraa, että kaikki tällaiset juurikunnat ovat keskenään isomorfisia. □

Äärellisten kuntien multiplikatiivisilla ryhmillä on sellainen merkittävä ominaisuus, että ne ovat kaikki syklisiä. Tämän osoittamiseksi käytetään ryhmän *eksponentin* käsitettä. Ryhmän G eksponentti $\exp(G)$ on pienin positiivinen kokonaisluku m, jolle pätee $g^m = 1$ kaikilla $g \in G$. Toisin sanoen eksponentti on ryhmän alkioiden kertalukujen pienin yhteinen jaettava.

LEMMA 16.10. *Olkoon G vaihdannainen ryhmä. Tällöin löytyy alkio $g \in G$, jonka kertaluku on* $\exp(G)$.

TODISTUS. Koska K^* on vaihdannainen, se voidaan kirjoittaa p-ryhmien suorana tulona $G_1 \times \cdots \times G_n$, missä $|G_i| = p_i^{k_i}$ kaikilla i (todistus harjoitustehtävä). Olkoon $g_i \in G_i$ se alkio, jonka kertaluku ryhmässä G_i on suurin, ja olkoon tämä kertaluku m_i. Ryhmän G_i jokaisen alkion kertaluku on jokin p_i:n potenssi, mistä seuraa, että $h^{m_i} = 1$ kaikilla $h \in G_i$.

Olkoon nyt $g = (g_1, g_2, \ldots, g_n) \in G$, ja olkoon g:n kertaluku m, jolloin erityisesti $\exp(G) \geq m$. Toisaalta jokaisella i pätee nyt $g_i^m = 1$, mistä seuraa, että $m_i | m$. Jos siis $h = (h_1, \ldots, h_n) \in G$, niin

$$h^m = (h_1^m, \ldots, h_n^m) = (1, \ldots, 1).$$

Täten myös epäyhtälö $\exp(G) \leq m$ pätee, joten g on alkio, jonka kertaluku on $\exp(G)$. $\square$

LAUSE 16.11. *Jos kunta K on äärellinen, niin $(K^*, \cdot)$ on syklinen ryhmä.*

TODISTUS. Merkitään $m = \exp(K^*)$. Jokaisella $g \in K^*$ pätee $g^m = 1$, joten jokainen ryhmän K^* alkio on polynomin $X^m - 1$ juuri. Tällä polynomilla on kuitenkin korkeintaan m juurta, joten $|K^*| \leq m$. Toisaalta edellisen lemman mukaan m on jonkin alkion $g \in K^*$ kertaluku, joten $|K^*| = m$, ja g virittää ryhmän $|K^*|$. $\square$

16.4. Polynomien ratkeavuus. Galois pystyi nimeään kantavan teorian avulla lopulta selvittämään täsmälleen, mitkä rationaalikertoimiset polynomit voidaan ratkaista kuntalaskutoimitusten ja juurenoton avulla. Tämä tulos riippuu vahvasti siitä, että tiettyihin kuntalaajennosten ketjuihin liittyy Galois'n ryhmän normaali jono, minkä osoittamiseksi puolestaan täytyy tuntea seuraava Galois'n teorian peruslauseen jatko-osa.

LAUSE 16.12 (Galois'n teorian peruslause, 2. osa). *Oletetaan, että L/K on äärellinen Galois'n laajennos, ja merkitään $G = \mathrm{Gal}(L/K)$. Jos $H = \mathrm{Gal}(L/M)$, missä M on jokin laajennoksen K/L välikunta, niin*

$$[L : M] = |H| \quad \text{ja} \quad [M : K] = [G : H].$$

Lisäksi H on normaali G:ssä, jos ja vain jos M/K on Galois'n laajennos. Tässä tapauksessa $G/H \cong \mathrm{Gal}(M/K)$.

$$\begin{tikzcd}
L \arrow[r, leftrightarrow] \arrow[d, dash, "{[L:M]}"] & \{\mathrm{id}\} \arrow[d, dash, "H"] \\
M \arrow[r, leftrightarrow] \arrow[d, dash, "{[M:K]}"] & H \arrow[d, dash, "G/H"] \\
K \arrow[r, leftrightarrow] & G
\end{tikzcd}$$

Todistus. Sivuutetaan. □

Tutustutaan seuraavaksi polynomin ratkeavuuden määritelmään. Se muistuttaa huomattavasti geometrisen konstruoituvuuden ehtoa.

Määritelmä 16.13. Kunta L on kunnan K *juurilaajennos*, jos on olemassa jono kuntia

$$K = K_0 \subset K_1 \subset \cdots \subset K_r = L,$$

missä $K_{i+1} = K_i(a_i)$ jollain $a_i \in K_{i+1}$, ja lisäksi $a_i^{n_i} \in F_i$ jollain $n_i \in \mathbb{N}$.

Jos $n = \max\{n_i\}$, missä luvut n_i ovat kuten edellisessä määritelmässä, sanotaan, että L/K on *kertaluvun n* juurilaajennos.

Oletetaan, että $f \in K[X]$. Jos on olemassa juurilaajennos L/K, jossa f jakautuu ensimmäisen asteen tekijöihin, sanotaan, että f on *juurtamalla ratkeava*. Käytännössä tämä tarkoittaa sitä, että f:n juuret voidaan kirjoittaa lausekkeina, joissa esiintyy yhteen-, vähennys-, kerto- ja jakolaskun lisäksi mielivaltaisia juurilausekkeita. Seuraava Évariste Galois'n todistama lause julkaistiin vasta hänen kuolemansa jälkeen vuonna 1843.

Lause 16.14 (Galois). *Olkoon K kunta, jonka karakteristika on 0, ja olkoon $f \in K[X]$. Olkoon L polynomin f juurikunta K:n suhteen. Tällöin f on juurtamalla ratkeava, jos ja vain jos* $\mathrm{Gal}(L/K)$ *on ratkeava ryhmä.*

Todistus. (Hahmotelma.) Oletetaan, että f on juurtamalla ratkeava, jolloin on olemassa kertaluvun n juurilaajennos M/K, joka sisältää juurikunnan L. Nyt M/K ei välttämättä ole Galois'n laajennos, mutta se on separoituva, koska $\mathrm{char}(K) = 0$. Olkoon $\overline{M}$ laajennoksen M/K *normaali sulkeuma* eli pienin normaali laajennos, joka sisältää kunnan M. Tällöin laajennos $\overline{M}/K$ on Galois. Teknisistä syistä asetetaan $K_1 = K(\omega)$, missä ω on $e^{2\pi i/n}$, ykkösen n:s juuri. Voidaan osoittaa, että $\overline{M}/K_1$ on edelleen kertaluvun n juurilaajennos, joten on olemassa kuntien jono

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_r = \overline{M},$$

missä $K_{i+1} = K_i(a_i)$ ja $a_i^n \in K_i$. Tässä kuntajonossa jokainen laajennos K_{i+1}/K_i on Galois, ja jokainen $\mathrm{Gal}(K_{i+1}/K_i)$ on vaihdannainen ryhmä.

Merkitään $G = \mathrm{Gal}(\overline{M}/K)$ ja $H_i = \mathrm{Gal}(\overline{M}/K_i)$. Galois'n teorian peruslauseen perusteella on olemassa aliryhmien jono

$$G = H_0 \geq H_1 \geq \cdots \geq H_r = 1. \tag{$*$}$$

Peruslauseen toisen osan mukaan H_{i+1} on normaali ryhmässä H_i kaikilla i, sillä K_{i+1}/K_i on Galois'n laajennos. Jono $(*)$ on siis normaali jono. Koska lisäksi tekijä $H_i/H_{i+1} \cong \mathrm{Gal}(K_{i+1}/K_i)$ on vaihdannainen ryhmä kaikilla i, nähdään, että G on ratkeava ryhmä. Ratkeavien ryhmien teorian perusteista seuraa, että myös $\mathrm{Gal}(L/K) \cong G/\,\mathrm{Gal}(\overline{M}/L)$ on ratkeava.

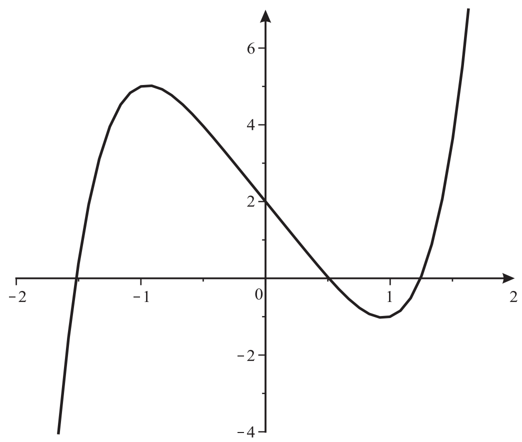
Toinen suunta etenee samalla periaatteella mutta vaatii vielä enemmän teknisiä aputuloksia. □

Voidaan kysyä, mitä hyötyä Galois'n lauseesta oikeastaan on. Näyttää nimittäin siltä, että sen selvittämiseksi, onko jokin polynomi juurtamalla ratkeava, on tunnettava sen juurikunnan Galois'n ryhmä. Tämän juurikunnan tunteminen taas tuntuu edellyttävän sitä, että juuret on jo löydetty. Käytännössä kuitenkin voidaan vähäisistä juurten luonnetta koskevista tiedoista päätellä ryhmien teorian avulla yhtä ja toista juurikunnan Galois'n ryhmästä, vaikka itse juuria ei tunnettaisi. Seuraavassa tästä eräs esimerkki.

Esimerkki 16.15. Tarkastellaan polynomia $f = X^5 - 4X + 2$. Tämä polynomi on Eisensteinin kriteerin perusteella jaoton $\mathbb{Q}$:n suhteen, joten sillä ei ole rationaalijuuria. Toisaalta piirtämällä polynomifunktion $x \mapsto f(x)$ kuvaaja voidaan päätellä, että f:llä on kolme reaalijuurta, joten se voidaan jakaa tuloksi

$$f = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3) \cdot g,$$

missä $\alpha_i \in \mathbb{R}$ kaikilla i, ja g on toisen asteen reaalikertoiminen polynomi.



Kuva 33. Polynomifunktion $f(x) = x^5 - 4x + 2$ kuvaaja.

Olkoon $L \subset \mathbb{C}$ polynomin f juurikunta, jolloin L/K on Galois'n laajennos. Polynomilla f on yhteensä viisi kompleksijuurta, ja jokainen juurikunnan $\mathbb{Q}$-automorfismi määräytyy siitä, miten se permutoi näitä juuria. Voidaan siis päätellä, että $\mathrm{Gal}(L/K)$ on isomorfinen jonkin ryhmän S_5 aliryhmän kanssa. Polynomi f on jaoton, joten se on itse jokaisen juurensa minimipolynomi. Tästä nähdään, että

$$[L : K] = [L : \mathbb{Q}(\alpha_1)] \cdot [\mathbb{Q}(\alpha_1) : \mathbb{Q}] = [L : \mathbb{Q}(\alpha_1)] \cdot 5.$$

Galois'n peruslauseen toisen osan perusteella $|\,\mathrm{Gal}(L/K)| = [L : K]$, joten ryhmän $\mathrm{Gal}(L/K)$ kertaluku on jaollinen viidellä. Cauchyn lauseesta seuraa, että $\mathrm{Gal}(L/K)$ sisältää alkion, jonka kertaluku on 5. Ryhmässä S_5 kaikki tällaiset alkiot ovat 5-syklejä. Toisaalta tiedetään, että toisen asteen polynomin g juuret ovat toistensa kompleksikonjugaatteja, joten kompleksikonjugoinnin rajoittuma juurikuntaan L on $\mathbb{Q}$-automorfismi, joka vaihtaa keskenään polynomin f ei-reaaliset juuret ja pitää reaaliset paikallaan. Ryhmässä S_5 tämä alkio on transpositio.

On varsin suoraviivaista osoittaa, että 5-sykli ja transpositio riittävät virittämään koko ryhmän S_5, mistä seuraa, että $\mathrm{Gal}(L/K) \cong S_5$. Koska S_5 ei ole ratkeava, myöskään polynomi f ei ole juurtamalla ratkeava.

Jo ennen Galois'ta oli tunnettua, että n:nnen asteen polynomiyhtälöllä ei ole yleistä ratkaisukaavaa, mikäli $n \geq 5$. Sen olivat nimittäin todistaneet itsenäisesti Ruffini[21] vuonna 1799 ja Abel vuonna 1824. Galois'n lause tarkentaa tätä tulosta näyttämällä täsmälleen, millä yksittäisillä polynomeilla on ratkaisukaava ja millä ei. Tulos voidaan myös johtaa Galois'n lauseesta, kun muistetaan, että S_n ei ole ratkeava millään $n \geq 5$.

LAUSE 16.16 (Abelin–Ruffinin lause). *Olkoon K kunta, jonka karakteristika on nolla. Jos $n \geq 5$, niin n:nnen asteen K-kertoimisella polynomilla ei ole yleistä kaavaa juurten löytämiseksi.*

TODISTUS. Yleinen n:nnen asteen polynomi on muotoa

$$f = (X - Y_1)(X - Y_2) \cdots (X - Y_n) = X^n - s_1 X^{n-1} + \cdots + (-1)^n s_n,$$

missä jokainen Y_i on tuntematon parametri ja jokainen $s_i \in K[Y_1, \ldots, Y_n]$ on ns. *symmetrinen polynomi*. Esimerkiksi

$$\begin{aligned} s_1 &= Y_1 + Y_2 + \cdots + Y_n \\ s_2 &= Y_1 Y_2 + Y_1 Y_3 + \cdots + Y_2 Y_3 + \cdots + Y_{n-1} Y_n \\ &\vdots \\ s_n &= Y_1 Y_2 \cdots Y_n. \end{aligned}$$

Polynomin f kertoimet ovat siis kunnassa $K_0 = K(s_1, \ldots, s_n) \subset K(Y_1, \ldots, Y_n)$. Jos on olemassa ratkaisukaava yleiselle n:nnen asteen polynomille, täytyy polynomin f olla juurtamalla ratkeava kunnan K_0 suhteen.

Polynomin f juurikunta on $L = K(Y_1, \ldots, Y_n)$. Galois'n ryhmän $\mathrm{Gal}(L/K_0)$ alkiot määräytyvät siitä, miten ne permutoivat virittäjiä Y_i, joten $\mathrm{Gal}(L/K_0)$ on isomorfinen jonkin symmetrisen ryhmän S_n aliryhmän kanssa. Toisaalta mikä tahansa tuntemattomien permutaatio kiinnittää jokaisen symmetrisen polynomin s_i, joten $\mathrm{Gal}(L/K_0) \cong S_n$. Koska S_n ei ole ratkeava, kun $n \geq 5$, myöskään f ei ole juurtamalla ratkeava. Tämä todistaa väitteen. $\square$

LOPPU

[21]Paolo Ruffini (1765–1822), italialainen filosofi ja matemaatikko