Lukijalle

> Matematiikan opetuksessa käsiteltävä aines voidaan järjestää ainakin seuraavien kolmen periaatteen mukaan: matematiikan historiallinen kehitysjärjestys, matematiikan looginen esitysjärjestys ja matematiikan pedagoginen oppimisjärjestys. Etenkin viimeksi mainitun erottaminen kahdesta edellisestä on tärkeää. Joskus tuntuu, että kaksi viimeksi mainittua ovat vaarassa sekoittua suunniteltaessa matematiikan opetusta. Historiallisen kehitysjärjestyksen liittäminen rinnalle saattaa auttaa kokonaisuuden hallitsemisessa. [Juha Oikkonen: [9]]

Modernin algebran alkeita on yleensä tapana opettaa tiukan aksiomaattis–abstraktilla tavalla käyttäen ryhmiä, renkaita ja kuntia lukuteorian perusteiden esittelyyn ja toisinaan lukualueiden **Z**, **Q**, **R** ja **C** konstruoimiseen luonnollisista luvuista **N** lähtien. Vaikka tämä tarjoaa asiasta kiinnostuneille hauskaa puuhaa, on olemassa vaara, että algebra alkaa tuntua muusta tosiolevaisesta kovin irralliselta asialta.

Siksi uskon, että peruskurssia seuraavan algebrakurssilla on oltava runsaammin yhteyksiä muuhun matematiikkaan ja sen ulkopuolellekin. Modernin algebran syntyhistoria tukee tällaista pyrkimystä, sillä sen lähtökohtana on ollut toisaalta klassinen algebra, esimerkiksi toisen ja kolmannen asteen polynomiyhtälön ratkaisukaavat, ja toisaalta myös geometriset ongelmat, kuten vanha kysymys kulman kolmijaon mahdottomuudesta.

Algebralla, etenkin ryhmän käsitteellä, on merkitystä lähes kaiken matematiikan taustalla. Felix Kleinin kuuluisa *Erlanger Programm* vuodelta 1872 asetti tavoitteeksi matematiikan ymmärtämisen invarianssien, symmetrian ja näihin liittyvien ryhmien pohjalta. Tässä Klein itse ja vielä suuremmassa määrässä myöhempien sukupolvien matemaatikot ovat pitkälti onnistuneetkin. Kleinin ohjelma korostaa ryhmien käyttöä geometrisluonteisten teorioiden yhdistävänä tekijänä, mutta mainitsee lopuksi mallina ja lähtökohtana myös puhtaasti algebrallisen *Galois'n teorian.*

Tämän monisteen rungon muodostaa luvuissa 2 ja 4 esitettävä kuntalaajennusten teoria, joka huipentuu Galois'n päälauseeseen. Teorialla todistetaan alkajaisiksi, että algebralliset luvut muodostavat kunnan ja luvussa 3 osoitetaan mahdottomiksi muutamia geometrisia konstruktioprobleemoita. Viidennen asteen yhtälön ratkaisukaavan mahdottomuus todistetaan Galois'n teoriaa käyttäen vasta luvussa 6. Luvut 1 ja 5 on tarkoitettu antamaan tarvittavia esitietoja ennen kaikkea polynomien jaollisuudesta ja ryhmistä. Kaiken kaikkiaan luvut 1–6 muodostavat

yhtenäisen kokonaisuuden, joka sisältää suurimman osan algebran oppikirjoissa tavallisesti käsiteltävistä asioista.

Luvut 0, 7 ja 8 ovat pääteoriasta aika irrallisia. Prologiluku 0 sisältää perusteellisen esityksen π:n transkendenttisuustodistuksesta, joka käyttää yhden muuttujan integraalilaskennan keinoja. Todistus tarjoaa samalla tilaisuuden symmetristen polynomien esittelyyn. π:n transkendenttisuus ratkaisee viime kädessä luvussa 3 kysymyksen ympyrän neliöimisestä.

Lukuihin 7 ja 8 olen koonnut esimerkkejä ryhmistä. Toivon monien valitsemieni esimerkkien olevan lukijalle jossakin muodossa ennestään tuttuja ja pyrin lähinnä Kleinin hengessä kiinnittämään huomiota ryhmäkäsitteen monipuolisiin käyttökohteisiin. Nämä osat on kirjoitettu aika kevyeen tyyliin eivätkä ne sisällä edes kaikkien lauseiden todistuksia. Tarkoituksena on vain kertoa hieman siitä, mitä muuta kuin Galois'n teoriaa algebra on, ja antaa intoa jatko-opiskeluun. Luku 8 vihjaa samalla, että moderni fysiikka on yllättävän algebrallista.

Loppuun liittämäni pieni algebran historia on oikeastaan vain luettelo joistakin tärkeimmistä vuosiluvuista ja nimistä. Historiallissävyisiä kommentteja on toisaalta ripoteltu sopivilta osin muuallekin tekstiin, lähinnä lukujen alkuihin.

Kiitoksia

Tämä moniste on syntynyt keväällä 1991 pitämäni algebran jatkokurssin sivutuotteena, oppilaitteni aktiivisuuden ja kiinnostuksen innoittamana.

Pekka Kekäläinen, Lassi Kurittu, Osmo Pekonen ja Vesa Ruuska tarkastivat käsikirjoituksen löytäen runsaasti virheitä ja tekivät myös sisältöön liittyviä olennaisia parannusehdotuksia. Mikko Saarimäki antoi käyttööni algebraseminaarinsa aineiston historialiitteineen. Ari Lehtoselta olen saanut TEX-apua ja luvan käyttää stereografista projektiota esittävää kuvaa.

Kiitos kaikille.

Mattilanniemessä 22.10.1991

Lisää kiitoksia

Sotamies Pasi Huovinen on aivotoimintoja ylläpitääkseen lukenut tätä monistetta ja löytänyt kymmenkunta virhettä. Olen kiitollisin mielin korjannut ne uuteen painokseen.

Mattilanniemessä 17.9.1993

Lauri Kahanpää

Sisällys

Jotkut asiat herättävät omituista, järjenvastaista ja ironista iloa henkilön päässä. Aikoinaan piti päntätä koulussa algebraa. Ja päntätessä oli vuorenvarma siitä, ettei tule aikuisena algebraa tarvitsemaan. Aikuisena sitten huomaa A) ettei todellakaan ole tarvinnut algebraa ja B) että lapsille opetetaan edelleen algebraa, C) jota he eivät todennäköisesti tule aikuisina milloinkaan tarvitsemaan. (Poikkeuksena tietenkin ne lapset, joista tulee **algebranopettajia**.) [Markus Kajo: Kettusen kirja. 1990]

00. Esitiedot:

Tämä moniste edellyttää lukijaltaan joitakin tietoja algebran perusasioista. Kaikki tarvittava esitetään jokaisella algebran peruskurssilla ja jokaisessa modernin algebran oppikirjassa sekä esim. Lauri Myrbergin monisteessa Algebra. Seuraavia käsitteitä pidämme tunnettuina:

(1) **Joukot:** yhdiste, leikkaus, osajoukko, joukkojen erotus, tulojoukko, kuvaus, kuvajoukko, alkukuvajoukko, rajoittuma, insur- ja bijektio, käänteiskuvaus, ekvivalenssirelaatio, mahtavuus, numeroituvuus, $\mathbf{R}$:n ylinumeroituvuus,
(2) **Ryhmät:** aliryhmä, homomorfismi, iso- ja automorfismi, ydin, sivuluokat, normaali aliryhmä, tekijäryhmä, kertaluku, alkion kertaluku, Lagrangen lause kertaluvuista, $\mathbf{Z}_k$,
(3) **Renkaat:** esimerkit $\mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}, k\mathbf{Z}, \mathbf{Z}_k$, alirengas, rengashomomorfismi, ideaali, tekijärengas, pääideaali,
(4) **Kunnat:** Kokonaisalue, kunta, esimerkit $\mathbf{Q}, \mathbf{R}, \mathbf{C}, \mathbf{Z}_p$, alikunta.
(5) **Kokonaislukujen jaollisuus:** jakolaskualgoritmi, suurin yhteinen tekijä, Eukleideen algoritmi, alkulukuhajoitelma.
(6) **Polynomit**: laskutoimitukset polynomeille, rengas $R[X]$, jakolaskualgoritmi, juuria on korkeintaan asteen määrä, algebran peruslause.

Olisi hyvä myös osata rationaalilukujen konstruktio kokonaislukuparien ekvivalenssiluokkina. Kompleksilukujen analyysistä käytetämme toistuvasti algebran peruslausetta.

Prologi transkendenttiluvuista nojaa yhden muuttujan integraalilaskentaan ja käyttää myös kompleksista eksponenttifunktiota. Klassisia Lien ryhmiä käsittelevä luku 8 sisältää monenlaisia vittauksia algebran ulkopuolelle, sillä tarkoituksena on esitellä joitakin algebran yhteyksiä kompleksianalyysiin, differentiaaligeometriaan ja ennen kaikkea fysiikkaan.

0. Prologi: e ja π

0.1. Lause (Hermite 1873). *e on transkendenttinen.*

0.2. Lause (Lindemann 1882). *π on transkendenttinen.*

Aloitamme algebran jatko-opiskelun kahdella kuuluisalla lauseella.

Luvussa 3 tulemme näkemään, että π:n transkendenttisuus ratkaisee yhden matematiikan historian pitkäaikaisimmista ongelmista, ympyrän neliöimisprobleeman.

Määrittelemme kohta, mitä transkendenttisella luvulla tarkoitetaan. Lause 0.2. saattaa olla tämän kirjasen hankalin todistettava eikä oikeastaan algebraa ollenkaan. Siksi tämä onkin prologi. Todistamme ensin harjoituksen vuoksi kaksi helpompaa ja vanhempaa tulosta:

0.3. Lause (Lambert 1768). *π on irrationaalinen.*

0.4. Lause (Legendre 1794). *π^2 on irrationaalinen.*

π:n irrationaalisuus. Tehdään vastaoletus: $\pi = \frac{a}{b}$ joillekin kokonaisluvuille a ja b. Olkoon n luonnollinen luku ja $\alpha = \frac{\pi}{2} = \frac{a}{2b} > 0$. Lasketaan osittaisintegroimalla palautuskaava integraalille

$$\begin{aligned}
I_n &= \int_{-1}^{1} (1-x^2)^n \cos(\alpha x)\, dx = \\
&= \Big|_{-1}^{1} (1-x^2)^n \frac{1}{\alpha}\sin(\alpha x) + \int_{-1}^{1} 2nx(1-x^2)^{n-1}\frac{1}{\alpha}\sin(\alpha x)\, dx = \\
&= \frac{2n}{\alpha}\Bigg(\Big|_{-1}^{1} x(1-x^2)^{n-1}\frac{1}{\alpha}(-\cos(\alpha x)) + \\
&\quad + \int_{-1}^{1} 2(n-1)x^2(1-x^2)^{n-2}\frac{1}{\alpha}(-\cos(\alpha x)) - \\
&\quad - (1-x^2)^{n-1}\frac{1}{\alpha}(-\cos(\alpha x))\, dx\Bigg) = \\
&= \frac{1}{\alpha^2}(2n(2n-1)I_{n-1} - 4n(n-1)I_{n-2}),
\end{aligned}$$

kun $n \geq 2$. Näin on saatu palautuskaava

$$I_n = \frac{1}{\alpha^2}(2n(2n-1)I_{n-1} - 4n(n-1)I_{n-2}).$$

Tällä integraalin laskeminen palautuu tapauksiin $n = 0$ ja $n = 1$, jotka

laskemme erikseen.

$$
\begin{aligned}
I_0 &= \int_{-1}^{1} \cos(\alpha x)\,dx = \frac{2}{\alpha}\sin\alpha \\
I_1 &= \int_{-1}^{1} (1-x^2)\cos(\alpha x)\,dx = I_0 + \int_{-1}^{1} (-x^2)\cos(\alpha x)\,dx = \\
&= I_0 - \left(\Big|_{-1}^{1} x^2 \frac{1}{\alpha}\sin(\alpha x) - \int_{-1}^{1} 2x \frac{1}{\alpha}\sin(\alpha x)\,dx \right) = \\
&= I_0 - I_0 + \frac{2}{\alpha}\int_{-1}^{1} x\sin(\alpha x)\,dx = \\
&= \frac{2}{\alpha}\left(- \Big|_{-1}^{1} x\frac{1}{\alpha}\cos(\alpha x) + \int_{-1}^{1} \frac{1}{\alpha}\cos(\alpha x)\,dx \right) = \\
&= \frac{2}{\alpha^3}\Big|_{-1}^{1} \frac{1}{\alpha}\sin(\alpha x) = \frac{4}{\alpha^3}\sin\alpha.
\end{aligned}
$$

Näistä lähtien palautuskaava johtaa tulokseen

$$I_n = n!\big(\frac{k_1}{\alpha} + \cdots + \frac{k_{2n+1}}{\alpha^{2n+1}}\big)\sin\alpha,$$

missä jokainen k_j on kokonaisluku. Näin ollen

$$\frac{\alpha^{2n+1}}{n!} I_n = P_n(\alpha)\sin\alpha,$$

missä P_n on enintään asteen $2n+1$ kokonaislukukertoiminen polynomi. Kun muistetaan, että $\alpha = \frac{\pi}{2} = \frac{a}{2b}$, jolloin $\sin\alpha = 1$, niin huomataan, että

$$\frac{a^{2n+1}}{n!} I_n = (2b)^{2n+1} P_n\big(\frac{a}{2b}\big)$$

on kokonaisluku kaikilla n. Tämä on mahdotonta, sillä $\frac{a^{2n+1}}{n!} \to 0$, kun $n \to \infty$ ja $|I_n| \le 2$, joten $\frac{a^{2n+1}}{n!} I_n \to 0$, mikä on **kokonaislukujonolle mahdollista vain, jos se on tasan** 0 **suurilla** n. Näinkään ei tässä käy, sillä selvästi integraali I_n eroaa nollasta kaikilla n. Olemme saavuttaneet ristiriidan ja siis todistaneet vastaoletuksen vääräksi. π on todella irrationaalinen.

π^2:n irrationaalisuus. π^2:n irrationaalisuustodistus on periaatteessa samantapainen kuin edellinenkin, mutta hieman mutkikkaampi. Vastaoletamme: $\pi^2 = \frac{a}{b}$, missä $a, b \in \mathbf{Z}$. Olkoon

$$f(x) = \frac{1}{n!} x^n (1-x)^n,$$

jolloin sen kaikkien kertalukujen derivaatat kohdissa 0 ja 1 ovat kokonaislukuja. Muodostetaan funktio

$$G(x) = b^n\bigg(\pi^{2n}f(x) - \pi^{2n-2}f''(x) + \pi^{2n-4}f^{(4)}(x) - \ldots (-1)^n f^{(2n)}(x)\bigg).$$

Edellä sanotun nojalla $G(0)$ ja $G(1)$ ovat kokonaislukuja, ja tätä on tarkoitus käyttää hyväksi samaan tapaan kuin edellisessä todistuksessa, siis konstruoimalla nollaan suppeneva jono integraaleja, jotka ovat toisaalta kokonaislukuja. Olennaisesti tällaiseksi osoittautuu

$$I_n = \int_0^1 a^n \sin(\pi x) f(x)\, dx,$$

sillä $\pi I_n \in \mathbf{Z}$. Derivoimalla G saadaan

$$G'(x) = b^n\bigg(\pi^{2n}f'(x) - \pi^{2n-2}f'''(x) + \pi^{2n-4}f^{(5)}(x) - \ldots (-1)^n f^{(2n+1)}(x)\bigg)$$

$$G''(x) = b^n\bigg(\pi^{2n}f''(x) - \pi^{2n-2}f^{(4)}(x) + \pi^{2n-4}f^{(6)}(x) - \ldots (-1)^n f^{(2n+2)}(x)\bigg),$$

joten lauseke

$$(G''(x) + \pi^2 G(x))\sin(\pi x)$$

on toisaalta yhtä kuin

$$b^n\pi^{2n+2}f(x)\sin(\pi x),$$

ja toisaalta yhtä kuin

$$\frac{d}{dx}\bigg(G'(x)\sin(\pi x) - \pi G(x)\cos(\pi x)\bigg).$$

Siksi

$$\begin{aligned} I_n &= \int_0^1 \pi^{2n} b^n \sin(\pi x) f(x)\, dx = \\ &= \pi^{-2}\int_0^1 \frac{d}{dx}\bigg(G'(x)\sin(\pi x) - \pi G(x)\cos(\pi x)\bigg)\, dx = \\ &= \pi^{-1}(G(0) + G(1)), \end{aligned}$$

ja siis itse asiassa $\pi I_n \in \mathbf{Z}$, mikä myös kelpaa tarkoitukseemme. On tietysti selvää, että I_n ei voi olla 0 millään n. Sen toteamiseksi, että $I_n \to 0$, riittää yksinkertainen arvio

$$\begin{aligned} |I_n| = |a^n| \int_0^1 \sin(\pi x)\frac{1}{n!}x^n(1-x)^n\, dx \leq \\ \leq \frac{|a^n|}{n!}\int_0^1 x^n(1-x)^n\, dx \leq \frac{|a^n|}{n!} \to 0. \end{aligned}$$

Näin on saatu samantapainen ristiriita kuin edellisessä todistuksessakin, ja siis myös π^2 on irrationaaliluku.

e:n transkendenttisuus.

0.5. Määritelmä.

(1) *Kompleksiluku z on algebrallinen, mikäli on olemassa nollasta eroava kokonaislukukertoiminen polynomi*

$$P(z) = a_m z^m + a_{m-1} z^{m-1} + \cdots + a_0, \qquad a_0 \neq 0,\ a_m \neq 0,$$

jonka jokin nollakohta luku z on.

(2) *Kompleksiluku z on transkendenttinen, mikäli se ei ole algebrallinen*[1]*.*

Ryhdymme todistamaan lausetta 0.3., jonka mukaan e on transkendenttinen. Tehdään vastaoletus: e ei ole *transkendenttinen,* vaan *algebrallinen* luku. On siis olemassa nollasta eroava kokonaislukukertoiminen polynomi P siten, että

$$0 = P(e) = a_m e^m + a_{m-1} e^{m-1} + \cdots + a_0. \tag{1}$$

Todistamme nyt kaavan (1) mahdottomaksi saman tapaisella tekniikalla kuin edellisissäkin todistuksissa. Laskemme integraalien summia

$$S_p = \sum_{j=0}^{m} (a_j e^j \int_0^j e^{-x} f(x)\, dx),$$

missä p on **alkuluku** ja funktio f on

$$f(x) = \frac{1}{(p-1)!}(x^{p-1}(x-1)^p(x-2)^p \ldots (x-m)^p).$$

Summan nollas termi on kylläkin 0, mutta kirjoitamme sen kauneussyistä mukaan myöhempää tarvetta varten. Varsinainen vaiva on siinä, että osoitetaan S_p:n olevan nollasta eroava kokonaisluku. Ainakin f on polynomi, jonka aste on $mp + p - 1$, ja siis derivaatta $f^{(mp+p)}$ on nolla.

[1]Samaan algebrallisen ja transkendenttisen luvun käsitteeseen päädytään, jos annetaan kertoimien a_j olla rationaalilukuja. Tämän huomaa helposti kertomalla sellaisen polynomin P kertoimiensa nimittäjien tulolla.

Olkoon

$$F(x) = f(x) + f'(x) + \cdots + f^{(mp+p-1)}(x), \text{ jolloin}$$

$$\frac{d}{dx}(e^{-x}F) = e^{-x}(F' - F) = -e^{-x}f, \text{ ja siis kaikilla } j$$

$$a_j \int_0^j e^{-x} f(x)\, dx = a_j \Big|_0^j - e^{-x}F = a_j F(0) - a_j e^{-j} F(j).$$

Siispä:

$$S_p = \underbrace{\left(\sum_{j=0}^{m} a_j e^j \right)}_{0} F(0) - \sum_{j=0}^{m} a_j \underbrace{F(j)}_{\sum_{i=0}^{mp+p-1} f^{(i)}(j)}$$

$$= -\sum_{j=0}^{m} \sum_{i=o}^{mp+p-1} a_j f^{(i)}(j).$$

Tämä pitäisi todistaa nollasta eroavaksi kokonaisluvuksi. Ainakin $a_j \in \mathbf{Z}$ oletuksemme nojalla. Osoitetaan, että myös esiintyvät f:n derivaatat ovat kokonaislukuja, eli että

$$f^{(i)}(j) \in \mathbf{Z} \quad \forall j = 0, \ldots, m; i = 0, \ldots, mp + p - 1.$$

Muistamme aluksi, että

$$f(x) = \frac{1}{(p-1)!}(x^{p-1}(x-1)^p \ldots (x-m)^p), \text{ ja siis}$$

$$f(j) = \frac{1}{(p-1)!}\Big(j^{p-1}(j-1)^p \ldots (j-m)^p\Big) = 0,$$

koska $j \in \{0, \ldots, m\}$ ja $p \geq 2$.

$$f'(j) = \frac{1}{(p-1)!}\Big((p-1)j^{p-2}(j-1)^p \ldots (j-m)^p + \ldots$$

$$+ j^{p-1}(j-1)^p \ldots p(j-m)^{p-1})\Big) = 0,$$

tulon derivointikaavalla , kun $j \neq 0$ tai $p > 2$.

(Kun $j = 0$ ja $p = 2$, niin 1. termi on $(m!)^2$.)

Toistamalla derivointia ja käyttämällä Leibnitzin kaavaa tulon korkeammille derivaatoille:

$$(uv)^{(i)} = \sum_{k=0}^{i} \binom{i}{k} u^{(k)} v^{(i-k)}$$

saadaan:

$$f(x) = \frac{1}{(p-1)!} \underbrace{x^{p-1}}_{u_0(x)} \underbrace{(x-1)^p \dots (x-m)^p}_{v_0(x)}$$

$$\text{siis } f^{(i)}(x) = \frac{1}{(p-1)!} \sum_{k=0}^{i} \binom{i}{k} u_0^{(k)}(x) v_0^{(i-k)}(x),$$

josta sijoituksella $x = j = 0$ kukin termi antaa nollan, paitsi termi $k = p-1$, jossa $u_0^{(p-1)}(0) = (p-1)!$ ja siis kaiken kaikkiaan:

$$f^{(i)}(0) = \binom{i}{p-1} v_0^{i-p+1}(0),$$

missä v_0 on yllä määritelty. Tulos on kokonaisluku ja lisäksi p:llä jaollinen, kun $i \neq p-1$.

Tapauksessa $j \in \{1, 2, \dots, m\}$ on mukavampi jakaa f tuloksi kahdesta tekijästä hieman toisin (hakasulkeissa oleva termi on poistettu):

$$f(x) = \frac{1}{(p-1)!} \underbrace{(x-j)^p}_{u_j(x)} \underbrace{x^{p-1}(x-1)^p \dots [(x-j)^p] \dots (x-m)^p}_{v_j(x)}.$$

Derivointi ja sijoitus $x = j$ antavat taas kustakin termistä nollan, paitsi siitä, jossa $k = p$, ja se tuottaa u_j:n derivaataksi $u_j(p)(j) = p!$, joka kumoaa nimittäjän $(p-1)!$:n ja jättää vielä kertoimen p. Siis

$$f^{(i)}(j) = \binom{i}{p} p v_j^{i-p}(j),$$

missä v_j on yllä määritelty. Tulos on p:llä jaollinen kokonaisluku.

Näin on kaikki esiintyvät derivaatat laskettu ja voidaan koota:

$$(*) \qquad S_p = -\sum_{j=0}^{m} \sum_{i=0}^{mp+p-1} a_j f^{(i)}(j) \in \mathbf{Z},$$

kuten väitettiinkin. Itse asiassa nyt on samalla myös selvää, että luku S_p ei ole 0, eipä edes jaollinen alkuluvulla p. Kehitelmässä $(*)$ on nimittäin kaksinkertaisen summan jokainen termi jaollinen p:llä, paitsi mahdollisesti ensimmäinen nollasta eroava, siis termi $j = 0$, $i = p-1$. Tämä termi puolestaan on yksinkertaisesti

$$a_0 f^{(p-1)}(0) = a_0 \binom{p-1}{p-1} v_0^0(0) = a_0((-1)^m(m!))^p.$$

Tässä a_0 ja myös $(-1)^m(m!)$ on p:stä riippumaton luku. Valitaan alkuluku p suuremmaksi kuin $a_0(m!)$. Nyt ei $a_0((-1)^m(m!))^p$, eikä siis myöskään sen ja p:n monikerran summa S_p voi olla jaollinen p:llä, saati nolla. ((tässä tarvittiin oletustamme $a_0 \neq 0$).

Lopuksi varmistaudumme siitä, että kuitenkin $S_p \to 0$, kun $p \to \infty$. f:n määritelmästä näkee, että

$$|f(x)| \leq \frac{m^{mp+p-1}}{(p-1)!},$$

sillä $0 \leq x \leq m$. Sijoittamalla tämän S_p:n määritelmään saamme arvion

$$\begin{aligned} |S_p| &= |\sum_0^m a_j e^j \int_0^j e^{-x} f(x)\, dx| \leq \\ &\leq \sum_0^m |a_j e^j| \int_0^j \frac{m^{mp+p-1}}{(p-1)!}\, dx \leq \\ &\leq \sum_0^m |a_j e^j| j \frac{m^{mp+p-1}}{(p-1)!} \to 0. \end{aligned}$$

π:n transkendenttisuus. Todistaaksemme, että myös π on transkendenttinen, joudumme edellisten kikkojen lisäksi turvautumaan vielä kahteen muuhun apuvälineeseen, nimittäin kompleksilukuihin ja symmetrisiin polynomeihin.

Kompleksiluvuista. Kompleksiluvuista tarvitaan tässä seuraavia tietoja

(1) Kompleksiluvut muodostavat kunnan $\mathbf{C}$, jonka alikuntana on $\mathbf{R}$.
(2) Kompleksiluvun i neliö on -1.
(3) Kompleksinen *eksponenttifunktio*

$$e^z = \sum_{k=o}^{\infty} \frac{z^k}{k!}$$

on määritelty kaikilla $z \in \mathbf{C}$ ja noudattaa tavanomaisia laskulakeja.
(4) *Eulerin kaava:* reaaliselle α pätee

$$e^{\alpha i} = \cos\alpha + i \sin\alpha,$$

erityisesti $e^{\pi i} = -1$.

Kompleksiluvun algebrallisuus ja transkendenttisuus määriteltiin edellä tutkittaessa lukua e. Todetaan, että $iz \in \mathbf{C}$ on algebrallinen aina, kun z on sitä: Olettakaamme että on olemassa kokonaisluvut $a_0, \ldots, a_m$ siten, että $a_m \neq 0$ ja

$$P(z) = a_0 + a_1 z + a_2 z^2 + \cdots + a_m z^m = 0.$$

Koska $i^2 = -1$, niin $P(-i(iz)) = P(z) = 0$, ja toisaalta

$$\begin{aligned} P(-i(iz)) &= a_0 + a_1(-i(iz)) + a_2(-i(iz))^2 + \cdots + a_m(-i(iz))^m = \\ &= a_0 - ia_1(iz) - a_2(iz)^2 + \cdots + (-i)^m a_m (iz)^m. \end{aligned} \tag{1}$$

Kaikki $-i$:n potenssit ovat ± 1 tai $\pm i$, joten kaava (1) on muotoa

$$0 = Q(iz) + iR(iz) = P(z), \tag{2}$$

missä Q ja R ovat kokonaislukukertoimisia polynomeja, joista ainakin toinen eroaa nollasta. Kerrotaan yhtälö (2) puolittain lausekkeella $Q(iz) - iR(iz)$. (Se ei muuten yleensä ole $P(z)$:n kompleksikonjugaatti, koska $Q(iz)$ ei yleensä ole reaalinen, vaikka z olisi.) Saadaan

$$0 = (Q(iz) + iR(iz))(Q(iz) - iR(iz)) = Q^2(iz) + R^2(iz).$$

On löydetty kokonaislukukertoiminen nollapolynomista eroava polynomi $Q^2 + R^2$, jonka nollakohta iz on. iz on siis algebrallinen[2].

Symmetrisistä polynomeista tarvittavat tiedot ovat vähemmän yleisesti tunnettuja. Siksi esitellään niitä tässä hiukan tarkemmin.

Symmetrisistä polynomeista.

0.6. Määritelmä.

(1) *Yhden muuttujan X polynomi* on lauseke[3]

$$P = P(X) = \sum_{k=0}^{\infty} a_k X^k = a_0 + a_1 X + a_2 X^2 + \cdots + a_m X^m + \ldots$$

missä *kertoimet* ovat kompleksilukuja ja kaikki paitsi äärellisen moni niistä on 0. Kaksi polynomia yhtyy, jos niillä on samat kertoimet.

[2]Todistamme myöhemmin, että algebrallisten lukujen joukko on $\mathbf{C}$:n alikunta. Erillinen perustelumme tässä on siten periaatteessa tarpeeton.

[3]Vrt. määr. 1.9.

(2) *Kahden muuttujan* X ja Y *polynomi* on lauseke

$$\begin{aligned} P = P(X,Y) &= \sum_{j=0,k=0}^{\infty} a_{jk} X^j Y^k = \\ &= a_{00} + \\ &+ a_{10}X + a_{01}Y + \\ &+ a_{20}X^2 + a_{11}XY + a_{02}Y^2 + \\ &+ a_{30}X^3 + a_{21}X^2Y + a_{12}XY^2 + a_{03}Y^3 + \\ &+ \dots, \end{aligned}$$

jossa vain äärellisen moni kertoimista a_{jk} on nollasta eroava. (Kehitelmän vaakarivit ovat nimeltään P:n *homogeeniset osat.* Asteen r *homogeeninen polynomi* on polynomi, jossa vain sillä vaakarivillä esiintyy nollasta eroavia kertoimia, jolla ensimmäinen termi on $a_{r0}X^r$. Asteen nolla homogeenipolynomi on *vakiopolynomi,* asteen yksi *lineaarinen* polynomi eli *lineaarimuoto,* asteen kaksi *kvadraattinen* jne.)

(3) Vastaavasti määritellään n:*n muuttujan polynomi* (homogeeniosineen).

$$\begin{aligned} P(X_1,\dots,X_n) &= \sum_{\nu_1,\dots,\nu_n \in \mathbf{N}} a_{\nu_1,\dots,\nu_n} X_1^{\nu_1} \dots X_n^{\nu_n} = \\ &= \sum_{k \in \mathbf{N}} \sum_{|\nu|=k} a_\nu X^\nu, \end{aligned}$$

missä on käytetty (ainoan kerran tässä monisteessa) mukavia *multi-indeksimerkintöjä:*

$$\begin{aligned} X &= (X_1,\dots,X_n) \\ \nu &= (\nu_1,\dots,\nu_n) \in \mathbf{N}^n \\ X^\nu &= X_1^{\nu_1} \dots X_n^{\nu_n} \\ |\nu| &= \nu_1 + \dots + \nu_n. \end{aligned}$$

(4) (Usean muuttujan) polynomi $P = P(X_1,\dots,X_n)$ on *symmetrinen,* jos se ei muutu, kun sen tuntemattomia X_j vaihdetaan keskenään, ts. on oltava

$$P(X_1,\dots,X_n) = P(X_{\sigma(1)},\dots,X_{\sigma(n)})$$

kaikilla n:n alkion permutaatioilla eli bijektioilla

$$\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}.$$

(5) *Symmetriset alkeispolynomit* ovat polynomit

$$\begin{aligned}
s_0(X_1, \ldots, X_n) &= 1 \\
s_1(X_1, \ldots, X_n) &= X_1 + \cdots + X_n \\
s_2(X_1, \ldots, X_n) &= X_1X_2 + \cdots + X_1X_n + X_2X_n + \cdots + +X_{n-1}X_n \\
&= \{\text{kaikki kahden } X_j\text{:n tulot}\} \\
s_3(X_1, \ldots, X_n) &= \{\text{kaikki kolmen } X_j\text{:n tulot}\} \\
s_n(X_1, \ldots, X_n) &= X_1 \ldots X_n.
\end{aligned}$$

Myös näiden tulot ja niiden lineaarikombinaatiot ovat selvästi symmetrisiä polynomeja. Jos Q on polynomi, on siis

$$P(X_1, \ldots, X_n) = Q(s_0(X_1, \ldots, X_n), \ldots, s_n(X_1, \ldots, X_n))$$

symmetrinen polynomi.

0.7. Lemma. *Muita n:n muuttujan symmetrisiä polynomeja kuin edellä mainitut ei ole olemassa.*

Ennen todistusta on mukava huomata, että symmetriset alkeispolynomit esiintyvät luonnossa: Jos kompleksilukukertoimisen polynomin

$$P = a_0 + a_1X + a_2X^2 + \cdots + X^n,$$

korkeimman asteen termin kerroin on 1, eli P on *perusmuotoinen,* niin se voidaan algebran peruslauseen mukaan aina kirjoittaa tulona 1-asteisista polynomeista:

$$P = (X - \alpha_1)(X - \alpha_2) \ldots (X - \alpha_n),$$

missä $\alpha_1, \ldots, \alpha_n$ ovat P:n nollakohdat eli juuret. Kertomalla tulo auki huomataan, että P:n kertoimet ovat merkkiä vaille samoja kuin symmetriset alkeispolynomit sen juurista:

$$\begin{aligned}
a_0 &= s_n(\alpha_1, \ldots, \alpha_n)(-1)^n \\
&\ldots \\
a_{n-1} &= s_1(\alpha_1, \ldots, \alpha_n)(-1)^1 \\
a_n &= s_0(\alpha_1, \ldots, \alpha_n) = 1.
\end{aligned}$$

Lemman 0.7. todistus. Olkoon

$$P = P(X_1, \ldots, X_n)$$

symmetrinen polynomi astetta k. Tehtävänä on löytää polynomi

$$Q = Q(Y_0, \ldots, Y_n)$$

siten, että

$$P(X_1, \ldots, X_n) = Q(s_0(X_1, \ldots, X_n), \ldots, s_n(X_1, \ldots, X_n)).$$

Esitämme algoritmin, jolla Q voidaan löytää. Koska merkintätavat monine indekseineen ovat hankalia lukea, kokeilemme algoritmia ensin johonkin esimerkkiin ja esitämme vasta sen jälkeen yleisen version. Esimerkki olkoon symmetrinen polynomi

$$\begin{aligned} P = P(X_1, X_2, X_3) = \\ = X_1 + X_2 + X_3 + 2X_1^2X_3 + 6X_1X_2X_3 + 2X_1^2X_2 + \\ + 2X_1X_2^2 + 2X_1X_3^2 + 2X_2X_3^2 + 2X_2^2X_3. \end{aligned}$$

Algoritmin aluksi järjestämme P:n termit "sanakirjajärjestykseen" eli *leksikografisesti,* ts. otetaan ensin ne termit, joissa X_1:llä on korkein esiintyvä potenssi, siis termit

$$2X_1^2X_3 \quad \text{ja} \quad 2X_1^2X_2.$$

Nämä järjestetään keskenään X_2:n potenssin mukaan, ensin $2X_1^2X_2$, sitten $2X_1^2X_3$. Näin jatketaan. Leksikografinen järjestys merkitsee siis sitä, että termit järjestetään vain esiintyvien eksponenttien mukaan kertoimista välittämättä ja että eksponenttijonoa $(\nu_1, \ldots, \nu_n)$ vastaava termi (tai yhtälailla itse jono) on ennen jonoa $(\mu_1, \ldots, \mu_n)$ vastaavaa termiä, jos jollakin $1 \leq k \leq n$ on voimassa:

$$\nu_1 = \mu_1, \ \ldots, \nu_{k-1} = \mu_{k-1} \quad \text{ja} \quad \nu_k > \mu_k.$$

P:n termit tulevat siten järjestykseen

$$\begin{aligned} P = 2X_1^2X_2 + 2X_1^2X_3 + 2X_1X_2^2 + 6X_1X_2X_3 + 2X_1X_3^2 + X_1 + \\ + 2X_2^2X_3 + 2X_2X_3^2 + X_2 + X_3. \end{aligned}$$

Algoritmin varsinainen askel on, että **vähennetään tästä haluttua muotoa oleva symmetrinen polynomi** P_V, jolla on – leksikografisesti

järjestettynä – sama ensimmäinen termi kuin P:llä, esimerkissämme siis $2X_1^2X_2$ ja joka on korkeintaan samaa astetta kuin P. Tällainen on olemassa, nimittäin

$$\begin{aligned} P_V &= 2s_1s_2 = 2(X_1+X_2+X_3)(X_1X_2+X_1X_3+X_2X_3) = \\ &= 2X_1^2X_2 + 2X_1^2X_3 + 2X_1X_2^2 + 6X_1X_2X_3 + 2X_1X_3^2 + \\ &+ 2X_2^2X_3 + 2X_2X_3^2. \end{aligned}$$

Erotuksesta $P - P_V$ putoaa halutun ensimmäisen termin lisäksi ilahduttavasti pois myös jokainen siitä vain muuttujia permutoimalla saatu termi, sillä symmetrian takia ne kaikki esiintyvät molemmissa polynomeissa. Erotus on

$$P - P_V = X_1 + X_2 + X_3,$$

joka jo onkin symmetrinen alkeispolynomi s_1. Siis

$$P = Q(s_0, s_1, s_2),$$

missä $Q = Q(Y_0, Y_1, Y_2) = 2Y_1Y_2 + Y_3$. Esimerkissä siis algoritmin yksi askel ratkaisi probleeman. Olisi voinut käydä niin, että erotus $P - P_V$ ei olisi ollut mikään polynomeista s_k. Tällöin olisi erotuspolynomiin sovellettu algoritmin askelta uudelleen, siis vähennetty uudelleen halutunlainen polynomi siten, että leksikografisesti ensimmäinen termi saadaan pois astetta nostamatta.

Lemma on todistettu, kunhan vielä vakuutudumme siitä, että halutunlainen vähennettävä aina löytyy ja algoritmi päättyy äärellisen monen askeleen jälkeen polynomista P riippumatta. Vähennettävän löytäminen on helppoa. Jos nimittäin P:n leksikografisesti 1. termi on vaikkapa

$$aX_1^{\nu_1} \dots X_n^{\nu_n},$$

niin vähennetään

$$P_V = as_1^{\nu_1-\nu_2}s_2^{\nu_2-\nu_3} \dots s_n^{\nu_n}.$$

Tällä on todella halutut ominaisuudet, minkä voi päätellä siitä, että polynomien tulon leksikografisesti 1. termi tietysti on tekijöiden 1. termien tulo ja toisaalta muodostamamme P_V:n kaikkien termien aste on sama, siis sama kuin P:n 1. termin aste ja näinollen $\leq k$.

Toisaalta algoritmi päättyykin aikanaan. Vähennystoimenpide poistaa nimittäin leksikografisesti varhaisempia termejä lisäten vain mahdollisesti myöhempiä, mutta on olemassa vain äärellisen monta mahdollista tapaa muodostaa annettua indeksiä leksikografisesti myöhempiä ja samalla annettua lukua k alemmanasteisia indeksejä. Lemma on todistettu. □

Algoritmin konstruktiotavasta ilmenee vielä enemmän:

Vähennettävien polynomien kertoimet ovat kokonaislukuja kerrottuina P:n kertoimilla, siis itsekin **kokonais- tai rationaalilukuja**, jos P on kokonais- tai rationaalilukukertoiminen.

Itse asiassa löydetty polynomi Q on myös yksikäsitteinen. Todistamme tämänkin täydellisyyden vuoksi: Olkoon siis em. merkinnöin $Q_1(s_0, \ldots, s_n) = Q_2(s_0, \ldots, s_n)$. Osoitetaan, että $Q_1 = Q_2$. Tarkastelemalla erotusta $Q_1 - Q_2$ palaudutaan heti tilanteeseen, jossa $Q_2 = 0$, joten riittää olettaa, että $Q(s_0, \ldots, s_n) = 0$ ja todistaa, että $Q = 0$. Vastaoletamme, että Q:lla on nollasta eroavia termejä – ainakin yksi. Olkoon

$$aY_0^{\nu_0} \ldots Y_n^{\nu_n}$$

näistä se, jolla indeksi

$$\alpha = (\alpha_0, \ldots, \alpha_n), \text{ missä } \alpha_k = \sum_{j=k}^{n} \nu_j$$

on leksikografisesti mahdollisimman varhainen. α:n määritelmän mukaan

$$\alpha_n = \nu_{n-1} + \alpha_{n-1}, \text{ paitsi } \alpha_n = \nu_n.$$

Polynomin $Q(s_0, \ldots, s_n)$ leksikografisesti ensimmäinen termi on nyt

$$aX_1^{\alpha_1} \ldots X_n^{\alpha_n} \neq 0,$$

joten $Q \neq 0$ vasten oletusta.

Päätodistus. Todistettaessa π:n transkendenttisuutta tulemme tarvitsemaan lemmaa 0.7. ensisijaisesti tilanteessa, jossa tutkittavana on nollakohtiensa avulla esitetty polynomi

$$\begin{aligned} P &= a_0 + a_1 X + a_2 X^2 + \cdots + X^n = \\ &= (X - \alpha_1)(X - \alpha_2) \ldots (X - \alpha_n). \end{aligned}$$

Joudumme tarkastelemaan symmetristä polynomia P:n juurista $\alpha_1, \ldots, \alpha_n$. Olennainen havainto on, että tällainen on lemman 0.7. nojalla lausuttavissa polynomina juurten symmetrisistä alkeispolynoimeista

$$s_0(\alpha_0, \ldots, \alpha_n), \ldots, s_n(\alpha_1, \ldots, \alpha_n),$$

jotka ovat merkkejä vaille P:n kertoimet $a_0, \ldots, a_{n-1}$.

Näiden pitkien valmistelujen jälkeen palaamme π:n transkendenttisuustodistukseen, jota emme itse asiassa ole vielä varsinaisesti aloittaneetkaan. Ideana on jälleen rakentaa jono funktioita, joiden integraali yli sopivan välin on toisaalta kokonaislukuarvoinen, toisaalta $\to 0$. Rakennuspalikoina ovat edelleen – nyt erityisesti symmetriset – polynomit ja eksponenttifunktio, tällä kertaa kompleksisena versionaan.

Apupolynomin konstruktio: Teemme vastaoletuksen, jonka mukaan π on algebrallinen. Siis myös $i\pi$ on algebrallinen ja on olemassa rationaalilukukertoiminen, perusmuotoinen polynomi $P_1(z) = a_0 + a_1 z + \cdots + z^n$, jolla $P_1(i\pi) = 0$. Olkoot sen juuret $\alpha_1 = i\pi, \alpha_2, \alpha_3, \ldots, \alpha_n \in \mathbf{C}$, jolloin

$$P(z) = (z - \alpha_1)(z - \alpha_2)\ldots(z - \alpha_n)$$

Tarkastelemme myös lukua

$$L = (e^{\alpha_1} + 1)(e^{\alpha_2} + 1)\ldots(e^{\alpha_n} + 1),$$

joka on 0, koska ensimmäinen tekijä Eulerin kaavan mukaan on 0. Kerrotaan L auki ja ryhmitellään:

$$\begin{aligned}
L = {} & e^0 + \\
& + e^{\alpha_1} + e^{\alpha_2} + \cdots + e^{\alpha_n} + \\
& + e^{\alpha_1+\alpha_2} + e^{\alpha_1+\alpha_3} + \cdots + e^{\alpha_{n-1}+\alpha_n} + \ldots \qquad \text{(kaikki aidot parit)} \\
& + e^{\alpha_1+\alpha_2+\alpha_3} + \ldots \qquad \text{(kaikki aidot kolmikot)} \\
& \ldots \\
& + e^{\alpha_1+\cdots+\alpha_n}.
\end{aligned}$$

Rakennamme rationaalilukukertoimisen polynomin, jonka nollakohtina ovat kaikki tässä esiintyvät eksponentit. Teemme sen rivi kerrallaan:

(1) Nollannella rivillä on eksponenttina vain luku 0.
(2) Ensimmäisellä rivillä ovat eksponentteina P_1:n nollakohdat.
(3) Toisella rivillä ovat eksponentteina P_1:n nollakohtien parien summat. Polynomi P_2, jonka nollakohtina ne esiintyvät, on:

$$P_2(z) = b_0 + b_1 z + \cdots + z^d, \text{ missä } d = \binom{n}{2},$$

ja kertoimet b_j ovat mahdollisesti merkkejä vaille samoja kuin symmetriset alkeispolynomit sen juurista:

$$b_j = \pm s_{d-j}(\alpha_1 + \alpha_2, \ldots \alpha_{n-1} + \alpha_n)$$

Nämä luvut b_j ovat rationaalisia. Ne ovat nimittäin symmetrisiä polynomeja luvuista α_j ja siis lemman 0.7. algoritmin nojalla kokonaislukukertoimisia polynomeja lausekkeista $s_j(\alpha_1, \ldots, \alpha_n)$, jotka ovat alkuperäisen polynomin P_1 kertoimet, ja siis rationaalilukuja.

(4) Kolmannen rivin voimme hoidella samalla tavalla.

(5) Samoin kaikki muutkin.

Näin on saatu kutakin riviä kohti rationaalilukukertoiminen polynomi P_k, jonka nollakohdat ovat täsmälleen rivillä esiintyvät eksponentit. Tulo

$$P_L = P_0 \ldots P_n$$

on rationaalilukukertoiminen polynomi, jolla on nollakohtinaan kaikki L:n kehitelmässä esiintyneet eksponentit.

Olkoot $\beta_1, \ldots, \beta_r$ em. listan nollasta eroavat eksponentit. Nollaan yhtyvien eksponenttien lukumäärä k on ainakin 1, sillä nollannen rivin eksponentti on 0. L:n kehitelmä voidaan näillä merkinnöillä kirjoittaa lyhyeen muotoon

$$L = e^{\beta_1} + \cdots + e^{\beta_r} + k = 0.$$

Myös polynomia P_L kannattaa vähän muotoilla. Jaetaan se ensin z^k:lla, jolloin nollakohta 0 poistuu ja muut jäävät. Kertomalla riittävän suurella kokonaisluvulla c_r saamme kokonaislukukertoimisen polynomin P, jolla on täsmälleen nollakohdat $\beta_1, \ldots, \beta_r$. Sen aste olkoon r:

$$P(z) = c_0 + c_1 X + \cdots + c_r X^r,$$

missä sekä c_0 että c_r ovat nollasta eroavia.

Integraalin konstruktio: Jäljittelemme pitkälti e:n transkendenttisuustodistusta. Olkoon p alkuluku, $s = rp - r$ ja

$$f(x) = \frac{c_r^s x^{p-1} (P(x))^p}{(p-1)!}$$

polynomi astetta $p - 1 + rp = s + p + r - 1$. Olkoon lisäksi

$$F(x) = \sum_{k=0}^{\infty} f^{(k)}(x) = \sum_{k=0}^{s+p+r-1} f^{(k)}(x).$$

Tuttuun tapaan:

$$\frac{d}{dx}(e^{-x} F(x)) = -e^{-x} f(x)$$

$$e^{-x} F(x) - F(0) = -\int_0^x e^{-y} f(y)\, dy$$

$$F(x) - e^x F(0) = -x \int_0^1 e^{(1-\lambda)x} f(\lambda x)\, d\lambda.$$

Päästäksemme käsiksi polynomeihin annamme x:lle kaikki arvot β_j ja summaamme käyttäen sieventämiseen tietoa $L = 0$:

$$\sum_{j=1}^{r} F(\beta_j) + kF(0) = -\sum_{j=1}^{r} \beta_j \int_0^1 e^{(1-\lambda)\beta_j} f(\lambda\beta_j)\, d\lambda.$$

Konstruktiot on tehty. Nyt osoitetaan, että tulos on saavutettu, eli että vasen puoli on nollasta eroava kokonaisluku.

Tarkistamme ensin, että vasemman puolen 1. termi on p:llä jaollinen kokonaisluku. Tutkittavana on

$$\sum_{j=1}^{r}\sum_{k=0}^{\infty} f^{(k)}(\beta_j) = \sum_{j=1}^{r}\sum_{k=0}^{s+p+r-1} f^{(k)}(\beta_j).$$

Ainakin

$$\sum_{j=1}^{r} f^{(t)}(\beta_j) = 0 \quad \forall t = 0, \ldots, p$$

Myöhemmissä derivaatoissa ($t > p$) esiintyy kerroin $p!$ G. Näille t on

$$\sum_{j=1}^{r} f^{(t)}(\beta_j)$$

lukujen β_j symmetrinen polynomi astetta $\leq s$. Siis se voidaan lemman 0.7. algoritmin avulla lausua symmetrisenä kokonaislukukertoimisena polynomina polynomin $\frac{P}{c_r}$ kertoimista $\frac{c_j}{c_r}$. Luvulla c_r^s kertominen määritelmässä tekee siten $\sum_{j=1}^{r} f^{(t)}(\beta_j)$:stä kokonaisluvun. Myös kerroin p on käyttämättä. $\sum_{j=1}^{r} f^{(t)}(\beta_j)$ on peräti jaollinen p:llä. Ensimmäinen termi on tutkittu.

Toinen termi on helpompi.

$$f^{(t)} = \begin{cases} 0, \quad (t \leq p-2) \\ c_r^s c_0^p, \quad (t = p-1) \\ \text{ jaollinen } p\text{:llä muuten.} \end{cases}$$

Siksi

$$kF(0) = \sum_{k=0}^{s+p+r-1} f^{(k)}(0) = k(c_r^s c_0^p + mp)$$

jollekin $m \in \mathbf{Z}$.

Kaiken kaikkiaan vasen puoli on muotoa

$$kc_r^s c_0^p + \ell p \quad \text{jollekin } \ell \in \mathbf{Z}.$$

Riittävän suurelle p tämä on p:llä jaoton eikä siis voi olla ainakaan 0.

Lopuksi näytetään, että oikea puoli

$$-\sum_{j=1}^{r} \beta_j \int_0^1 e^{(1-\lambda)\beta_j} f(\lambda\beta_j)\, d\lambda$$

lähenee nollaa p:n kasvaessa rajatta. Koska $0 \le \lambda \le 1$, niin

$$\begin{aligned} |f(\lambda\beta_j)| &= \Big| \frac{c_r^s (\lambda\beta_j)^{p-1} (P(\lambda\beta_j))^p}{(p-1)!} \Big| \le \\ &\le \frac{|c_r^s||\beta_j|^{p-1}}{(p-1)!} \Big[\underbrace{\sup_{0\le\lambda\le 1} |P(\lambda\beta_j)|}_{m_j<\infty} \Big]^p \le \\ &\le \frac{|c_r^s||\beta_j|^{p-1}}{(p-1)!} m_j^p \end{aligned}$$

Siispä tutkittava summa on itseisarvoltaan enintään

$$\begin{aligned} &\sum_{j=1}^{r} \frac{|c_r^s||\beta_j|^p}{(p-1)!} m_j^p \underbrace{\max_{j=1,\dots,r} \Big| \int_0^1 e^{(1-\lambda)\beta_j}\, d\lambda \Big|}_{B<\infty} = \\ &= \frac{B|c_r|^s}{(p-1)!} \sum_{j=1}^{r} |\beta_j|^p m_j^p \to 0, \text{ kun } p \to \infty. \end{aligned}$$

□

On olemassa paljon muitakin transkendettilukuja kuin e ja π. Ensimmäiset löysi J. LIOUVILLE. Eräs Liouvillen luvuista on

$$\sum_{\nu=1}^{\infty} 10^{-\nu!},$$

jonka transkendenttisuustodistus on helppo ja esiintyy algebrankirjoissa vihjein varustettuna harjoitustehtävänä. Liouvillen lause vuodelta 1844 tuottaa saman tien paljon transkendenttilukuja. Lauseen muotoilussa käytetään algebrallisen luvun korkeuden käsitettä, joka määritellään seuraavasti.

0.8. Määritelmä. Olkoon α jaottoman nollasta eroavan kokonaislukukertoimisen polynomin

$$P_\alpha(z) = a_m z^m + a_{m-1} z^{m-1} + \cdots + a_0, \qquad a_m > 0,$$

nollakohta ja olkoon P_α sievennetty niin, että sen kertoimilla ei ole yhteisiä tekijöitä[4]. α:n *korkeus* on luku $H(\alpha) = \max\{|a_0|, \ldots, |a_n|\}$.

Liouvillen lause sanoo, että **irrationaaliluku** ξ on transkendenttinen, mikäli on olemassa $c > 0$ ja $n \in N = \{1, 2, \ldots\}$ siten, että

$$\inf\{H(\alpha)^n |\xi - \alpha| \big| \alpha \in \mathbf{Q}\} > c.$$

Nykyisin tiedetään, että on on olemassa muitakin transkendenttilukuja kuin Liouvillen ehdon toteuttavat (K. MAHLER 1937), mm. $0,123456789101112131415\ldots$ on sellainen.

Melkein kaikki kompleksiluvut ovat transkendenttisia, sillä kompleksilukujen joukko on G. CANTORIN kuuluisan lauseen (1874) mukaan ylinumeroituva, mutta algebrallisten lukujen joukko on numeroituva, koska kokonaislukukertoimisia polynomeja on vain numeroituva joukko ja kullakin on vain äärellisen monta nollakohtaa. Tämä havainto ei kuitenkaan auta konstruoimaan yksittäisiä transkendettilukuja.

Ei tunneta yleistä mentettelytapaa, jolla luvusta voisi testata, onko se algebrallinen vai transkendenttinen. Esimerkiksi Eulerin vakiosta

$$C = \lim_{n\to\infty} (1 + \frac{1}{2} + \cdots + \frac{1}{n} - \log n)$$

ei tiedetä onko se transkendenttinen, eipä edes onko se mahdollisesti rationaalinen.

[4]Todistamme kohdassa 2.6., että P_α on yksikäsitteinen.

1. Polynomit

Perusasioita.

1.1. Määritelmä. Renkaassa $R = (R, +, \cdot)$ pätevät kaikilla $a, b \in R$ aksioomat:

(1) $(R, +)$ on abelin ryhmä
(2) $a(bc) = (ab)c$
(3) $a(b + c) = ab + ac$
(4) $(a + b)c = ac + bc$.

Esimerkiksi $\mathbf{Z}$, $k\mathbf{Z}$ ja $\mathbf{Z}_k$ = tekijärengas $\mathbf{Z}/k\mathbf{Z}$ ovat renkaita.
Kokonaisalueessa R on lisäksi voimassa

(5) $ab = ba$
(6) $\exists 1 : 1 \neq 0$ ja $\forall a \in R : 1a = a$
(7) $ab = 0 \implies a = 0$ tai $b = 0$.

Esimerkkejä kokonaisalueista ovat $\mathbf{Z}$, *polynomirenkaat* $\mathbf{Z}[X] = \{P \mid P$ on yhden muuttujan X kokonaislukukertoiminen polynomi $\}$, $\mathbf{Q}[X], \mathbf{R}[X]$ ja $\mathbf{C}[X]$, sekä tekijärengas $\mathbf{Z}_p$ aina ja vain kun p on alkuluku.
Kunnaksi kokonaisalue tulee, jos on voimassa käänteisalkiota koskeva aksiooma:

(8) $\forall a \in R^* = R \setminus \{0\}\ \exists a^{-1} \in R$ siten että $aa^{-1} = 1$.

R^* on kunnan R *multiplikatiivinen ryhmä.* Kuntia ovat mm. $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ ja äärellinen kunta $\mathbf{Z}_p$ aina ja vain, kun p on alkuluku.

1.2. Huom. Renkaiden välinen kuvaus on *(rengas-)homomorfismi*, jos se säilyttää summat ja tulot. Ollessaan lisäksi bijektio se on *isomorfismi.* Renkaan epätyhjä osajoukko on *alirengas*, jos se sisältää alkioidensa summat, erotukset ja tulot. Kunnan alirengas on *alikunta*, jos se sisältää myös nollasta eroavien alkioidensa käänteiset sekä nollan ja ykkösen. Esimerkiksi $\mathbf{Q}, \mathbf{R}$ ja $\mathbf{C}$ ovat toistensa alikuntia.

Kun I on renkaan R alirengas, niin voidaan muodostaa tekijäjoukko $R/I = \{[a] = a + I \mid a \in R\}$ ja varustaa se ryhmän struktuurilla luonnollisella tavalla (luokkien edustajia yhteen laskemalla), koska *additiivinen ryhmä* $(R, +)$ on kommutatiivinen ja sen aliryhmänä I siis normaali aliryhmä. Yleensä ei kuitenkaan kertolasku periydy tähän tekijäryhmään. Tilanne korjaantuu, jos I on R:n *ideaali,* eli

$$IR \subset I \text{ ja } RI \subset I.$$

Tällöin on olemassa tekijärengas R/I. On hyvä huomata, että alikunta ei ole ideaali, kuten esimerkki $\mathbf{Q} \subset \mathbf{R}$ osoittaa. (Kunnalla K ei ole muita ideaaleja kuin triviaalit K ja $\{0\}$. Mieti miksi.)

Alkukunta ja karakteristika.

1.3. Määritelmä. Kunnan K *alkukunta* on sen kaikkien alikuntien leikkaus

$$P = \cap_{I \text{ on } K\text{:n alikunta}} I.$$

1.4. Lause. *K:n alkukunta P on sen suppein alikunta. Lisäksi P on isomorfinen joko $\mathbf{Q}$:n tai $\mathbf{Z}_p$:n kanssa, missä p on alkuluku.*

Todistus. Ensimmäinen väite seuraa siitä, että alikuntien leikkaukset ovat alikuntia. Erityisesti P sisältää nolla- ja ykkösalkion.

Toisen väitteen todistamiseksi tarkastellaan rengashomomorfismia $^\bullet$, (jolla "$\mathbf{Z}$ upotetaan kuntaan K"):

$$^\bullet : \mathbf{Z} \to K : n \mapsto n^\bullet = \begin{cases} 1 + \cdots + 1 \, (n \text{ kpl.}), & \text{jos } n \geq 0 \\ -(-n)^\bullet, & \text{jos } n < 0. \end{cases}$$

Tässä on kaksi vaihtoehtoa. Homomorfismi $^\bullet$ saattaa olla injektio tai sitten ei.

Jos $^\bullet$ on injektio, niin sen kuvajoukko on $\mathbf{Z}$:n kanssa isomorfinen K:n alirengas ja erityisesti $m^\bullet \neq 0$ kaikille kokonaisluvuille $m \neq 0$. Tämä antaa mahdollisuuden laajentaa kuvauksen $^\bullet$ kuvaukseksi $\mathbf{Q} \to K$ asettamalla

$$(\frac{n}{m})^\bullet = \frac{n^\bullet}{m^\bullet}$$

kaikille $\frac{n}{m} \in \mathbf{Q}$. Näin tulee määritellyksi injektiivinen rengas- ja siis kuntahomomorfismi $\mathbf{Q} \to K$, jonka kuvajoukko on $\mathbf{Q}$:n kanssa isomorfinen K:n alikunta, jonka samaistamme $\mathbf{Q}$:hun. Alkukunta P on lauseen alkuosan mukaan tämän osajoukko ja siis myös $\mathbf{Q}$:n alikunta. Mutta $\mathbf{Q}$:lla ei (tietenkään!) ole muita alikuntia kuin se itse. Siksi $P = \mathbf{Q}$.

Toinen vaihtoehto on, että $^\bullet$ ei ole injektio, jolloin puhe $\mathbf{Z}$:n upottamisesta K:hon on aika kyseenalaista. Tällöin on olemassa $n \in \mathbf{Z} \setminus \{0\}$ siten, että $n^\bullet = 0$, jolloin myös $(-n)^\bullet = 0$, ja koska ainakin toinen luvuista n ja $-n$ on luonnollinen, on olemassa pienin luonnollinen luku p, jolla $p^\bullet = 0$. Tämä p on alkuluku, sillä muuten olisi olemassa sitä pienemmät luonnolliset luvut m ja n, joille $p = mn$ ja siis kunnassa K

$$m^\bullet n^\bullet = (mn)^\bullet = p^\bullet = 0,$$

jolloin joko $m^\bullet = 0$ tai $n^\bullet = 0$ vastoin p:n määritelmää. Koska p siis on alkuluku, niin $\mathbf{Z}_p$ on kunta. Toisaalta se on renkaana isomorfinen kuvajoukon $(\mathbf{Z})^\bullet \subset K$ kanssa, joka siis myös on kunta ja näin ollen K:n alikunta. Siis – samaistaen isomorfiset – $\mathbf{Z}_p$ on K:n alikunta. Nytpä on

helppo todeta, että ei myöskään $\mathbf{Z}_p$:llä ole aitoa alikuntaa, ei edes aliryhmää (kertaluku!) ja siksi samoin kuin edellisessä tapauksessa voidaan päätellä, että K:n alkukunta P on löydetty $\mathbf{Z}_p$.[5] $\square$

1.5. Määritelmä. Sanomme, että kunnan K *karakteristika* on luku 0, jos sen alkukunta on $\mathbf{Q}$. Jos taas sen alkukunta on $\mathbf{Z}_p$, niin sen *karakteristika* on alkuluku p,

Esimerkiksi kunnilla $\mathbf{Q}$, $\mathbf{R}$ ja $\mathbf{C}$ on karakteristika 0 ja kunnilla $\mathbf{Z}_p$ karakteristika p. (Muita kuntia ei ole tainnut vielä esiintyäkään.)

1.6. Lause. *Kaikilla kunnan K alikunnilla on sama karakteristika kuin K:lla.*

Todistus. Niillä on sama alkukunta. $\square$

1.7. Lause. *Olkoon K:n karakteristika alkuluku p. Jos $k \in K^* = K \setminus \{0\}$ ja $nk = k + \cdots + k = 0$, niin n on jaollinen p:llä.*

Todistus. $nk = n^\bullet k$ lauseen 1.4. todistuksen mielessä. $n^\bullet$ ja k ovat kunnan – siis kokonaisalueen – alkioita, joiden tulo on 0. Siis toinen niistä on 0, eikä se ole k, vaan siis $n^\bullet$. Tämä $n^\bullet$ on siis paitsi K:n myös sen alkukunnan $P \sim \mathbf{Z}_p$ nolla-alkio, eli $[n]$ on $\mathbf{Z}_p$:n nolla, eli $n \in p\mathbf{Z}$. $\square$

Tarkastelumme antavat aiheen merkitä kunnan K alkiota $n^\bullet$ lyhyesti n. Sekaannusta ei synny, kun muistetaan, että kun kunnan karakteristika on alkuluku p, tämä pitää tulkita modulo p.

Jakokunta.

1.8. Lause. *Rengas R on kokonaisalue aina ja vain ollessaan (isomorfiaa vaille, kuten aina tällaisissa yhteyksissä) jonkin kunnan $K = K(R)$ alirengas, joka sisältää K:n ykkösalkion, vieläpä niin, että kaikki K:n alkiot ovat muotoa*

$$k = \frac{a}{b}, \quad a \in R,\, b \in R^*.$$

[5] Kaiken kaikkiaan olemme tulleet määritelleeksi mielivaltaiselle renkaalle R ulkoisen kertolaskutoimituksen

$$\bullet : \mathbf{Z} \times R \to R : (n, k) \mapsto n \bullet k := n^\bullet k,$$

jonka suhteen rengas R on "melkein vektoriavaruus": kaikki vektoriavaruuden aksioomat pätevät $(R, +, ^\bullet)$:lle, paitsi että kertoimien rengas $\mathbf{Z}$ ei ole kunta, kuten vektoriavaruudelle kuuluu. Tällaista struktuuria sanotaan ($\mathbf{Z}$-kertoimiseksi) *moduliksi*. Moduleilla on oma "lineaarialgebransa", joka suuresti muistuttaa vektoriavaruuksien teoriaa. Matkimalla lineaarialgebraa voi näin mukavasti keksiä vaikkapa yleisiä renkaita, eli $\mathbf{Z}$-moduleita koskevia lauseita.

Tämä kunta – R:n jakokunta – on yksikäsitteinen.

Todistus. Tietysti jokainen kunnan ykkösellinen alirengas on kokonaisalue. Lauseen väite on siis toinen puoli. Olkoon R kokonaisalue.

Jakokunta K on helppo konstruoida jäljittelemällä sitä tapaa, jolla rationaaliluvut rakennetaan kokonaisluvuista, siis tekijäjoukkona joukosta

$$K = \{(a, b) \mid a \in R, b \in R^*\}$$

ekvivalenssirelaation

$$(a, b) \sim (c, d) \iff ad = bc$$

suhteen. Tunnetulla tavalla todetaan, että laskutoimitukset on mahdollista määritellä parien ekvivalenssiluokille

$$[(a, b)] = \{(x, y) \mid x \in R, y \in R^*, (x, y) \sim (a, b)\}$$

edustajittain. Näin saadaan kunta $K = R \times R^* / \sim$. Kuvaus $a \mapsto [a, 1]$ on injektiivinen homomorfismi, mikä antaa aiheen samaistaa a:n ja $[a, 1]$:n. Yleisesti $[a, b] = \frac{[a,1]}{[b,1]}$, ja siis todella $K = \{\frac{a}{b} \mid a \in R, b \in R^*\}$. Yksikäsitteisyyden todistaminen on sekin helppoa. □

Polynomeista.

1.9. Määritelmä. Määrittelemme tässä polynomin käsitteen uudelleen hieman yleistäen – prologissahan polynomeilla jo laskeskeltiinkin. Olkoon R kommutatiivinen rengas. *Yhden muuttujan X n-asteinen R-(kertoiminen) polynomi* on lauseke[6]

$$P = P(X) = a_0 + a_1 X + \cdots + a_n X^n,$$

missä jokainen $a_\nu \in R$ ja $a_n \neq 0$. *Nollapolynomi* on lauseke 0. Sen *aste* on $-\infty$.

Kaksi polynomia yhtyvät, jos ja **vain** jos niillä on samat kertoimet.

Havaintoja.

(1) Muuttujan X kaikenasteisten R-polynomien joukko $R[X]$ on luonnollisin **kertoimiin kohdistuvin** laskutoimituksin itsekin kommutatiivinen rengas, *polynomirengas* ja – ilmeistä isomorfiaa vaille – riippumaton muuttujan X nimestä.

(2) Polynomia ei pidä harkitsemattomasti samaistaa määrittelemäänsä renkaan R (tai muunkaan struktuurin) funktioon

$$x \mapsto a_0 + a_1 x + \cdots + a_n x^n,$$

[6]"Lauseke" ei ole hyvin määritelty käsite, vaikka toivottavasti vetoaakin intuitioon ja lukijan aikaisempaan kokemukseen paremmin kuin täsmällinen määritelmä, jonka voisimme asettaa esim. siten, että polynomi samaistetaan *kertoimiensa* jonoon $(a_0, a_1, \dots)$, missä vaaditaan, että jokainen paitsi äärellisen moni a_ν on nolla.

sillä eri polynomeja saattaa vastata sama funktio, kun R ei ole esim. reaaliluvut. (Keksi esimerkki kunnassa Z_2.)

(3) Vastaavasti voidaan määritellä usean muuttujan $X_1, \ldots, X_m$ polynomit. Tällaisen polynomin

$$P(X_1, \ldots, X_m) = \sum_{\nu_1,\nu_2,\ldots,\text{ja } \nu_m=0}^{n} a_{\nu_1,\nu_2,\ldots,\nu_m} X_1^{\nu_1} X_2^{\nu_2} \ldots X_m^{\nu_m},$$

aste on

$$\max\{\nu_1 + \cdots + \nu_m \,|\, a_{\nu_1,\nu_2,\ldots,\nu_m} \neq 0\}.$$

Näin muodostuu usean muuttujan polynomirengas

$$R[X_1, \ldots, X_m].$$

Sen voi pienellä vaivannäöllä todistaa olevan isomorfinen yhden muuttujan kerrallaan lisäämällä saadun renkaan $R[X_1] \ldots [X_m]$ kanssa.

1.10. Lause. *Jos R on kokonaisalue, vaikkapa kunta, niin myös polynomirengas $R[X]$ on kokonaisalue, samoin siis jokainen $R[X_1][X_2] \ldots [X_m]$.*

Todistus. Olkoon R kokonaisalue ja

$$P = a_0 + a_1 X + \cdots + a_n X^n,\ a_n \neq 0$$

ja

$$Q = b_0 + b_1 X + \cdots + b_m X^m,\ b_m \neq 0$$

kaksi sen nollasta eroavaa polynomia. Tulon PQ korkeimman asteen termi on $a_n b_m X^{n+m}$, missä kerroin $a_n b_m$ on nollasta eroava. Siksi tulo PQ ei ole nollapolynomi. Kommutatiivisuus on ilmeistä. Ykkönen on vakiopolynomi 1. □

Tämä lause antaa mahdollisuuden määritellä:

1.11. Määritelmä. Olkoon R kokonaisalue. Kokonaisalueen $R[X]$ *jakokunta* on kunta, jota merkitsemme (hämäävän samankaltaisesti!!) $R(X)$. Sen alkiot, *rationaalilausekkeet,* ovat siis muotoa $\frac{P}{Q}$ – muodollisesti siis parit (P, Q) – missä P ja Q ovat R-polynomeja ja Q ei ole nollapolynomi.

Polynomien jaollisuus ja suurin yhteinen tekijä.

1.12. Huomautus. Tarkastelemme tämän luvun loppuosasssa yleensä **kunnan K** polynomeja. Niillä voi pitkälti laskea kuten kokonaisluvuilla. Erityisesti on syytä muistaa, että polynomin P voi jakaa toisella, vaikkapa Q:lla, tunnettua jakolaskualgoritmia käyttäen, jolloin jää jakojäännös: $\forall P, Q \in K[X]\, \exists A, B \in K[X]$:

$$P = AQ + B,$$

siten että B:n aste on aidosti pienempi kuin Q:n aste.

Jakolaskualgoritmin avulla voi esim. todistaa, että kunnan polynomirenkaan kaikki ideaalit ovat ns. *pääideaaleja*, eli ne muodostuvat yhden polynomin kaikista tuloista muiden kanssa, ts. sillä *jaollisista* polynomeista.[7]

Kerroinrenkaan ollessa kunta K toimii myös *Eukleideen algoritmi,* jolla löydetään annetuille nollasta eroaville polynomeille $P_1, \ldots, P_n$ jaollisuuden mielessä (Ks. määr. 1.14.) *suurin yhteinen tekijä* $D = \text{syt}\,(P_1, \ldots, P_n)$. Samalla saadaan myös lause, jonka mukaan D voidaan lausua muodossa

$$D = B_1P_1 + \cdots + B_nP_n,$$

missä $B_1, \ldots$ ja $B_n \in K[X]$.

Suurin yhteinen tekijä ei ole edes kerroinrenkaan ollessa kunta aivan yksikäsitteinen, sillä jos D_1 ja D_2 ovat samojen polynomien $P_1, \ldots$ ja P_n suurimpia yhteisiä tekijöitä, niin ne määritelmän mukaan ilmeisesti ovat kylläkin jaollisia toinen toisillaan, mutta tästä ei vielä seuraa, että ne yhtyisivät. (Esim. $\mathbf{R}-$polynomit P ja $2P$ ovat todella jaollisia toisillaan, ovathan $2X^0$ ja $\frac{1}{2}X^0 \in \mathbf{R}[X]$.) Suurin yhteinen tekijä on siis enintään "vakiotekijää vaille yksikäsitteinen". Mutta tätä se sitten onkin. Olkoot nimittäin D_1 ja D_2 nollasta eroavia ja jaollisia toisillaan

$$D_1 = AD_2 \text{ ja } D_2 = BD_1.$$

Tällöin $D_1 = AD_2 = ABD_1$, eli $D_1(1 - AB) = 0$ ja siis kokonaisalueominaisuuden perusteella $AB = 1$. Todistakaamme, että tällöin A ja B ovat astetta 0 eli oleellisesti vain K:n alkioita. Itse asiassa tämä väite on seuraava lemma:

[7] Todistus on helppo ja esitetään kohdassa 2.6. puhuttaessa algebrallisista kuntalaajennuksista.

1.13. Lemma. *Olkoon K kunta. Polynomirenkaan $K[X]$ ykkösen tekijät eli kääntyvät alkiot eli yksiköt* ovat täsmälleen nollasta eroavat *vakiopolynomit* eli asteen 0 polynomit aX^0, $a \in K^*$.

Todistus. Kun kerroinrengas on kunta (riittää kokonaisalue), niin polynomien asteelle $\deg(P)$ pätee korkeimman asteisia kertoimia vertaamalla saatava yhtälö

$$\deg(PQ) = \deg P + \deg Q.$$

Siksi kahden polynomin tulo voi olla 0-asteinen vain kun molemmat tekijät ovat sitä. □

Tämä antaa aiheen sanoa, että polynomi $P(X) = a_0 + \cdots + a_n X^n$ on *perusmuotoinen* (engl. monic), jos $a_n = 1$. Jokainen nollasta eroava polynomi saadaan täsmälleen yhdestä perusmuotoisesta kertomalla vakiolla (joka on a_n). Erityisesti vakiopolynomia vastaava perusmuotoinen polynomi on 1.

Polynomien jaollisuutta tarkasteltaessa tulevat alkulukuja vastaamaan jaottomat polynomit. Tilanne on samantapainen kuin kokonaisluvuillakin, mutta on syytä heti huomata, että polynomin jaollisuus tai jaottomuus riippuu ratkaisevasti siitä, missä kerroinkunnassa sitä tarkastellaan. Sekaannuksen vaara olisi etenkin silloin, kun tarkastellaan jotakin kuntaa L, sen alikuntaa K ja polynomia $P \in K[X] \subset L[X]$. Virheiden välttämiseksi kerrataan jaollisuuden muodollinen määritelmä, jonka voimme asettaa myös silloin, kun kerroinrengas ei ole kunta[8]:

1.14. Määritelmä.

(1) Polynomi $P \in R[X]$ on *renkaassa R jaollinen* polynomilla $A \in R[X]$, eli *A jakaa P*:n, eli A on P:n *tekijä*, mikäli on olemassa $B \in R[X]$ siten, että

$$P = AB.$$

(2) Polynomi $P \in R[X]$ on *renkaassa R jaollinen* mikäli on olemassa A ja $B \in R[X]$ siten, että sekä A että B ovat **aidosti** alempaa astetta kuin P ja

$$P = AB.$$

(3) Muuten P on *jaoton renkaassa R*.

(4) Polynomi $D \in R[X]$ on polynomien $Q_1, \ldots$ ja Q_n *suurin yhteinen tekijä*– lyhyesti syt – jos se jakaa kaikki annetut $Q_1, \ldots$ ja Q_n ja D itse on jaollinen jokaisella sellaisella polynomilla P, joka myös jakaa polynomit $Q_1, \ldots$ ja Q_n.

[8] Joissakin tärkeissä esimerkeissämme kerroinrengas tulee olemaan $\mathbf{Z}$.

Esimerkin polynomista, joka on jaoton renkaassa Z ja kunnasssa $\mathbf{Q}$, mutta jaollinen kunnassa $\mathbf{R}$ tarjoaa vaikkapa

$$P(X) = X^2 - 2.$$

Vältämme seuraavassa näitä kunnan vaihtoon liittyviä "hankaluuksia" (jotka myöhemmin ovat suurenkin mielenkiinnon kohteena) kiinnittämällä kerta kaikkiaan kunnan K.

Polynomin hajoitelma jaottomien tuloksi. Todistamme, että kokonaisluvun yksikäsitteisellä alkulukuhajoitelmalla on vastine kunnan polynomeille.

1.15. Lause. *(1) Nollasta eroava polynomi $P \in K[X]$ voidaan esittää tulona jaottomista polynomeista:*

$$(*) \qquad P = aP_1P_2 \dots P_k,$$

missä $a \in K$ ja polynomit $P_1, P_2, \dots$ ja P_k ovat perusmuotoisia, jaottomia ja ei vakioita.

(2) Edellä mainittu jako on tekijöiden järjestystä lukuun ottamatta yksikäsitteinen.

Todistus. Osoitetaan ensin hajoitelman $(*)$ olevan olemassa. Se onkin helppoa induktiolla asteen suhteen. Olkoon tutkittava polynomi $P \in K[X]$ astetta k. Jos P on jaoton, on hajoitelma löytynyt. Jos P on jaollinen, niin $P = AB$, missä A ja B ovat aidosti alempaa astetta. Jatketaan tutkimalla A:n ja B:n jaollisuutta samalla tavalla. Viimeistään k askelen jälkeen jäljellä on vain vakioita ja jaottomia polynomeja, sillä viimeistään 1-asteinen polynomi on jaoton.

Toiseksi näytetään hajoitelman yksikäsitteisyys. Olkoon samalla polynomilla P kaksi hajoitelmaa jaottomien perusmuotoisten polynomien tuloksi:

$$P = aP_1P_2 \dots P_k = bQ_1Q_2 \dots Q_l.$$

ainakin a on P:n korkeimman asteen kerroin , siis $a = b$.Voimme siis olettaa, että $a = b = 1$. Jaoton P_1 jakaa siis tulon jaottomista polynomeista $Q_1 \dots Q_l$. Se jakaa siis jonkin tekijöistä Q_j (!?) (Tämä johtopäätös – niin luonnolliselta kuin se tuntuukin – on todistuksen arka kohta ja vaatii erillisen perustelun, joka jää seuraavaksi lemmaksi.) Olkoon se vaikkapa Q_1; järjestystähän voi tarvittaessa vaihtaa. P_1 jakaa siis jaottoman polynomin Q_1! Tämä on mahdollista vain, jos P_1 olisi vakio – mitä se ei ole – tai sitten Q_1 on vakio kertaa P_1 – miten asia siis on.

Vakio on 1, koska P_1 ja Q_1 ovat perusmuotoisia. Siis $Q_1 = P_1$. Koska polynomirengas on kokonaisalue, voidaan yhtälö

$$P = P_1 P_2 \dots P_k = P_1 Q_2 \dots Q_l$$

sieventää jakamalla puolittain yhteisellä tekijällä P_1, eihän se ole 0. Jatketaan induktiolla, kunnes jommalle kummalle puolelle jää pelkkä

ykkönen. Silloin toisellakin puolella on vain ykkösiä, sillä nämä ovat ainoita perusmuotoisia ykkösen tekijöitä. □

Muistetaanpa, että vielä puuttuu:

1.16. Lemma. *Jos jaoton $P \in K[X]$ jakaa polynomien tulon $Q_1 \dots Q_l$, niin se jakaa jonkin tekijöistä.*

Todistus. Riittää tarkastella kahden polynomin tuloa, (induktio!) ja voidaan vielä olettaa, että kaikki polynomit ovat perusmuotoisia. Jakakoon siis P tulon QS, mutta ei Q:ta. Tällöin P:n ja Q:n syt. on 1, sillä P:llä ei ole muita perusmuotoisia tekijöitä kuin 1 ja P, joka ei ole Q:n tekijä. Kohdassa 1.12. saatiin Eukleideen algoritmin avulla tieto, että koska $\mathrm{syt}(P, Q) = 1$ ja K on kunta, niin on olemassa sellaiset polynomit A ja $B \in K[X]$, että

$$1 = AP + BQ.$$

Tämä ratkaiseekin asian, sillä nyt

$$S = APS + BQS$$

ja P jakaa siis S:n, koska P jakaa APS:n ja oletuksen mukaan myös QS:n. □

Polynomin jakaminen alkutekijöihinsä on eräs algebran klassisia ongelmia, eikä yleensä ollenkaan helppoa. Tämähän pitää sisällään mm. kaikki **R**- tai **C**-kertoimisen polynomin juurten löytämiseen liittyvät probleemat, erityisesti kuuluisan viidennen asteen yhtälön ratkaisemisen. Yhteys hajoitelman ja juurten välillä on seuraava:

Polynomin juuret.

1.17. Määritelmä. Olkoon R kommutatiivinen rengas. Polynomin $P \in R[X]$ *juuri* eli *nollakohta* (R:ssä) on R:n alkio x, jolle $P(x) = 0$, missä $x \to P(x)$ on P:n tunnetulla tavalla määrittelemä *polynomifunktio* R:ssä. (Vrt. 1.9.(2).)

Jakolaskualgoritmin avulla on kunnan tapauksessa helppo todistaa seuraavan lauseen kohta (1) ja siitä induktiolla ja alkutekijähajoitelmalla kohta (2) ja triviaalisti (3):

1.18. Lause. *Olkoon K kunta ja $P \in K[X] \setminus \{0\}$. Olkoon k P:n aste.*

(1) *K:n alkio a on P:n juuri aina ja vain, kun P on jaollinen 1. asteen polynomilla $X - a$.*
(2) *P on muotoa*

$$P(X) = a_k(X - \alpha_1)^{\nu_1}(X - \alpha_2)^{\nu_2} \dots (X - \alpha_n)^{\nu_n} Q(X),$$

missä Q:lla ei ole yhtään juurta K:ssa. $\alpha_1, \ldots$ ja α_n ovat P:n juuret ja a_k P:n korkeimman asteen termin kerroin. Lukuja ν_j sanotaan P:n juurten α_j kertaluvuiksi.

(3) P:n nollakohtien lukumäärä kertaluvut huomioiden, eli summa

$$\nu_1 + \cdots + \nu_n$$

on enintään P:n aste k. Sama pätee sitä suuremmalla syyllä nollakohtien lukumäärälle tavallisessa mielessä: $n \leq k$.

"Algebran peruslauseen" mukaan jokaisella $\mathbf{C}$-kertoimisella polynomilla on kunnassa $\mathbf{C}$ ainakin yksi juuri. Edellinen lause takaa siis jo prologissa käyttämämme esitystavan tällaiselle polynomille 1. kertaluvun tekijöiden tulona. Alkutekijähajoitelma on siis tässä tapauksessa perin yksinkertainen rakenteeltaan (joskin silti vaikea löytää). Kuten jo aikaisemmin on todettu, voi esim. kunnassa $\mathbf{R}$ esiintyä korkean kertaluvun nollakohdattomia polynomeja: vaikkapa $X^{20000} + 1$ on sellainen.

Jaottomuuskriteereitä. Päätämme tämän luvun kahdella lauseella, joiden avulla voi (yrittää) päätellä polynomin jaottomuutta kunnassa $\mathbf{Q}$.

1.19. Lause (Gauss). *Olkoon $\mathbf{Z}$-kertoiminen polynomi P jaoton renkaassa $\mathbf{Z}[X]$. Silloin se on jaoton myös renkaassa $\mathbf{Q}[X]$.*

Todistus. Olkoon

$$P(X) = a_0 + a_1 X + \cdots + a_n X^n$$

$\mathbf{Z}$-kertoiminen polynomi, joka on jaollinen $\mathbf{Q}[X]$:ssä. On siis olemassa $\mathbf{Q}$-kertoimiset alempiasteiset polynomit $B(X)$ ja $C(X)$ joille $P = BC$. Kertomalla nimittäjien tulolla s saamme yhtälön

$$(*) \qquad sP = BC,$$

missä

$$B(X) = b_0 + b_1 X + \cdots + b_m X^m \quad \text{ja}$$
$$C(X) = c_0 + c_1 X + \cdots + c_k X^k$$

ovat $\mathbf{Z}-$polynomeja. Yhtälö $(*)$ voidaan nyt jakaa puolittain s:n alkutekijöillä kokonaiskertoimisuuden kärsimättä. Tämän todistamme seuraavasti: Olkoon p jokin s:n alkutekijä. Tällöin s ja siis myös p jakaa kaikki sP:n kertoimet, siis myös yhtälön oikean puolen kertoimet. Jos p

jakaa kaikki polynomin B kertoimet tai kaikki C:n kertoimet, niin sievennys voidaan suorittaa. Jollei, niin on olemassa pienimmät indeksit $i \in \{1, \ldots, m\}$ ja $j \in \{1, \ldots, k\}$, joilla b_i ja c_j ovat p:llä jaottomat. Oikealla puolella on X^{i+j}:n kertoimena

$$b_0 c_{i+j} + b_1 c_{i+j-1} + \cdots + b_i c_j + \cdots + b_{i+j} c_0,$$

ja tämä on siis jaollinen p:llä. Koska i ja j ovat pienimmät indeksit lajissaan, niin tässä summassa kaikki tekijät, paitsi $b_i c_j$ ovat jaollisia p:llä. Erotuksena vasemman puolen kertoimesta ja muiden oikean puolen termien summasta on siis myös $b_i c_j$ jaollinen alkuluvulla p. p jakaa siis joko b_i:n tai c_j:n vastoin oletusta. A tai B voidaan siis jakaa luvulla p renkaassa $\mathbf{Z}[X]$. Toistamalla päättelyä kaikille s:n tekijöille saadaan lauseen väite. □

1.20. Lause (Eisensteinin ehto). *Olkoon*

$$P(X) = a_0 + a_1 X + \cdots + a_n X^n$$

Z*-kertoiminen polynomi. Riittävää P:n jaottomuudelle* **Z***:ssa – ja siis* **Q***:ssa – on, että on olemassa alkuluku p, jolle*

(1) *kertoimet $a_0, \ldots, a_{n-1}$ ovat jaollisia p:lla,*
(2) *kerroin a_n ei ole jaollinen p:lla ja*
(3) *kerroin a_0 ei ole jaollinen p^2:lla.*

Todistus. Oletetaan, että kuitenkin

$$P = BC$$

missä

$$B(X) = b_0 + b_1 X + \cdots + b_m X^m \text{ ja}$$
$$C(X) = c_0 + c_1 X + \cdots + c_k X^k$$

ovat alempiasteisia ja **Z**-kertoimisia. P:n aste on

$$n = m + k$$

ja sen vakiotermi on

$$a_0 = b_0 c_0,$$

joten oletuksen (1) nojalla alkuluku p jakaa b_0:n tai c_0:n, mutta (3):n nojalla ei molempia. Jakakoon se vaikkapa b_0:n. Jokin kertoimista b_i on joka tapauksessa jaoton p:lla, sillä muuten p jakaisi kaikki P:nkin kertoimet vastoin oletusta (2). Olkoon i pienin indeksi, jolla p ei jaa b_i:tä. Nyt

$$a_i = b_i c_0 + \cdots + b_0 c_i,$$

joten a_i on jaoton p:lla, koska oikean puolen summassa tasan yksi termi on p:lla jaoton. Mutta $i \leq m < n$ vastoin oletusta (1). Eisensteinin ehto on siis riittävä polynomin jaottomuudelle. □

oo

2. Kunnan laajentaminen

Kuntalaajennukset ovat tämän monisteen keskeinen tarkastelun kohde. Kaikki jäljempänä esittelemämme mahdottomuustodistukset perustuvat algebrallisten kuntalaajennuksien ominaisuuksiin. Kuntalaajennuksilla on läheinen yhteys polynomeihin. Tässä luvussa käsittelemme perusasiat kuntalaajennuksista.

Kuntalaajennus. Seuraava määritelmä ilmaisee, että isomorfiaa vaille kunta L on **k**unnan K **l**aajennus, jos K on L:n alikunta.

2.1. Määritelmä. *Kuntalaajennus* $L : K$ on injektiivinen rengashomomorfismi kunnalta K kunnalle L.

Huomautus. Yleensä samaistamme kunnan K kuvaansa L:ssä, jonka kanssa se on isomorfinen.

2.2. Määritelmä.

(1) Olkoon L kunta ja $\emptyset \neq A \subset L$. Joukon A *virittämä* L:n alikunta on kaikkien A:n sisältävien L:n alikuntien leikkaus

$$\cap\{I \mid I \text{ on } L\text{:n alikunta ja } A \subset I\ \}.$$

(2) Olkoon $L : K$ kuntalaajennus ja $M \subset L$ osajoukko. Joukon $M \cup K$ virittämä L:n alikunta (ja vastaava kuntalaajennus $K(M) : K$) on saatu K:sta *lisäämällä* eli *adjungoimalla* siihen joukko M (M:n alkiot). Tätä alikuntaa merkitsemme

$$K(M),$$

tai, kun M on äärellinen $M = \{a_1, \ldots, a_n\}$:

$$K(M) = K(a_1, \ldots, a_n).$$

(3) Erityisesti yhden alkion adjungoimisella saatu kuntalaajennus $K(a) : K$ on *yksinkertainen* laajennus.

2.3. Esimerkkejä. Joukon A virittämä alikunta on suppein L:n alikunta, joka sisältää joukon A. Se muodostuu kaikista alkiosta, jotka saadaan A:n alkioista ja ykkösestä toistamalla niihin kunnan neljää (!) laskutoimitusta äärellisen monta kertaa. Esim. L:n alkukunta on sen kaikkien alikuntien leikkaus $P = \cap_{I \text{ on } K\text{:n alikunta}} I$. Se on siis joukon $\{0, 1\}$ virittämä L:n alikunta. Toisena esimerkkinä voi todeta, että $\{0, i\}$:n virittämä $\mathbf{C}$:n alikunta muodostuu kaikista kompleksiluvuista $a + ib$, joilla a ja $b \in \mathbf{Q}$.

Emme ota omaa merkintää mielivaltaisen joukon $M \subset L$ virittämälle alikunnalle, sillä jatkossa tärkeä on vain kuntalaajennukseen liittyvä erikoistapaus (2). Esimerkkejä tästäkin tarjoavat kompleksiluvut: laajennuksen $\mathbf{C} : \mathbf{R}$ mielessä on

(a) $$\mathbf{R}(i) = \mathbf{C}.$$

Laajennuksen $\mathbf{R} : \mathbf{Q}$ tai $\mathbf{C} : \mathbf{Q}$ mielessä

(b) $$\mathbf{Q}(\sqrt{2}) = \{a + b\sqrt{2} \,|\, a, b \in \mathbf{Q}\},$$

(c) $$\mathbf{Q}(\sqrt[3]{2}) = \{a + b(\sqrt[3]{2}) + c(\sqrt[3]{2})^2 | a, b, c \in \mathbf{Q}\},$$

ja

(d) $$\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\sqrt{2} + \sqrt{3}).$$

Todista, että näin on! Huomaa, että esimerkki (c) osoittaa, että alikunnan K yksinkertainen laajennus $K(\alpha)$ ei aina eikä edes yleensä, muodostu pelkästään lausekkeista $a + b\alpha$, vaikka nämä tietysti ovat mukana. Ilmiö johtuu siitä, että ne eivät välttämättä muodosta kuntaa. Esimerkki (d) näyttää vastaavasti, että laajennuksen yksinkertaisuus ei välttämättä heti erotu tavasta, jolla se on kirjoitettu näkyviin.

Kuntalaajennus $K(M)$ riippuu tietysti alkuperäisestä suurimmasta kunnasta L, sillä L määrää M:n alkioiden laskutoimitukset keskenään ja K:n alkioiden kanssa eivätkä näiden tulokset yleensä ole edes $K \cup M$:n alkiota, vaan muualla L:ssa. Jätämme L:n usein kuitenkin pois merkinnöistä, koska L on useimmiten kiinnitetty – usein se on $\mathbf{C}$. Ryhdymme tutkiskelemaan yksinkertaisten laajennusten mahdollista rakennetta. Samalla pääsemme lähemmäs yhteyttä polynomeihin ja niiden juuriin. Tulemme myös todistamaan, että (prologissa esiintyneet) algebralliset luvut muodostavat kunnan.

Algebrallisuus ja transkendenttisuus.

2.4. Määritelmä. Olkoon $L : K$ kuntalaajennus ja $a \in L$. Sanomme, että a on *algebrallinen* (K:n suhteen), mikäli a on jonkin nollasta eroavan $K-$kertoimisen polynomin juuri. Myös yksinkertaista kuntalaajennusta $K(a)$ sanomme tällöin *algebralliseksi*. Muuten a ja $K(a)$ ovat *transkendenttisia.*

2.5. Esimerkki. Kunnan K rationaalilausekkeiden kunta on K:n transkendenttinen kuntalaajennus $K(X) : K$. Tämä on helppo todeta. Ainakin K laajenee rationaalilausekkeiden kunnaksi adjungoimalla yksi

elementti, nimittäin polynomi, siis rationaalilauseke X. Huomaamme, että aikaisemmin eri yhteyksissä käyttöön ottamamme täsmälleen saman näköiset merkinnät $K(X)$ ja $K(X)$ (ks. määritelmät 1.11. ja 2.1.) eivät sittenkään esitä eri asioita. Laajennus $K(X) : K$ on toisaalta myös transkendenttinen. Olkoon nimittäin X jonkin $K-$kertoimisen polynomin P juuri $K(X)$:ssä. Määritelmän mukaan tämä tarkoittaa, että $K(X)$:n alkio $P(X)$ on $K(X)$:n nolla-alkio, eli rationaalilauseke 0, eli nollapolynomi. Siis P on nollapolynomi ja X transkendenttinen K:n suhteen.

Huomautus. Tässä olikin isomorfiaa vaille ainoa K:n transkendenttinen yksinkertainen laajennus. (Tämän todistaminen on sopiva harjoitustehtävä. Helpommaksi se käy, kun kohta todistamme vastaavan, joskin hankalamman tuloksen algebrallisille laajennuksille.) Algebrallisia kuntalaajennuksia on mutkikkaampi kokoelma. Koska algebrallinen alkio on usean eri polynomin nollakohta, on syytä valita näiden joukosta mahdollisimman siisti. Luonnollisia ehdokkaita ovat asteeltaan pienin tai jaoton polynomi, jos sellainen on olemassa.

Minimaalipolynomi.

2.6. Lause ja määritelmä. *Olkoon yksinkertainen kuntalaajennus $K(a) : K$ algebrallinen.*

(1) *On olemassa tasan yksi alimman mahdollisen asteen perusmuotoinen polynomi $P \in K[X]$, jolle $P(a) = 0$.*
(2) *Sanomme, että P on a:n minimaalipolynomi K:ssa.*
(3) *Minimaalipolynomi P on jaoton.*
(4) *Kaikki polynomit $Q \in K[X]$, joilla $Q(a) = 0$, ovat jaollisia minimaalipolynomilla P. Erityisesti minimaalipolynomi on ainoa jaoton perusmuotoinen polynomi, jolla on juurena a.*

Todistus. (1) Oletuksen mukaan joukossa

$$I_a = \{Q \in K[X] \,|\, Q(a) = 0\}$$

on muitakin polynomeja kuin vakio 0. Joillakin niistä – olkoon P eräs sellainen – on alin mahdollinen aste. Jakamalla P tarvittaessa korkeimman asteen terminsä kertoimella voimme huolehtia siitä, että P on myös perusmuotoinen. Jos tällaisia polynomeja olisivat vaikkapa P ja Q, niin niiden erotus olisi aidosti alemman asteinen ja $\in I_a$. Erotus olisi siis 0, koska muita alemman asteisia polynomeja ei I_a:ssa ole.

(3) On samaan tapaan helppo todeta, että P on jaoton. Jos ei se sitä olisi, niin se olisi tulo kahdesta aidosti alemman asteisesta polynomista,

$P = RS$, jolloin $P(a) = R(a)S(a)$ ja siis joko $R(a)$ tai $S(a)$ on 0 vastoin P:n määritelmää.

(4) Lopuksi jokainen joukkoon I_a kuuluva polynomi Q on tosiaan jaollinen minimaalipolynomilla P. Olkoon nimittäin $Q \in I_a \setminus \{0\}$, jolloin $Q(a) = 0$ ja Q:n aste on vähintään P:n aste. Jaetaan Q P:llä jakolaskualgoritmia käyttäen. Saadaan jakojäännös R, jonka aste on **aidosti** pienempi kuin P:n. On siis olemassa polynomi A siten, että

$$\begin{aligned} Q &= AP + R, \text{ jolloin erityisesti} \\ Q(a) &= A(a)P(a) + R(a), \text{ ja siis} \\ R(a) &= 0, \text{ eli} \\ R &\in I_a \end{aligned}$$

Koska P on I_a:n alimman asteinen nollasta eroava alkio, on siis jäännös $R = 0$, eli Q jaollinen P:llä, kuten pitikin[9]. $\square$

Edellinen lause voidaan melkein kääntää:

2.7. Lause. *Jokainen kunnan K jaoton perusmuotoinen polynomi $P \in K[X]$ on jonkin kuntalaajennuksen $K(\alpha) : K$ minimaalipolynomi.*

Todistus. Tarkastellaan polynomirengasta $K[X]$. Itse kunta K on sen alirengas. Olkoon I P:llä jaollisten polynomien ideaali ja S tekijärengas

$$S = K[X]/I; \text{ kanonista surjektiota merkitsemme } \nu\text{:llä.}$$

Otamme todistaaksemme, että

(1) S on kunta,

[9] On helppo huomata, että

$$I_a = \{Q \in K[X] \mid Q(a) = 0\}$$

on polynomirenkaan $K[X]$ ideaali. Edellä todistimme, että on olemassa sellainen $P \in K[X]$, että

$$\{Q \in K[X] \mid Q(a) = 0\} = \{Q \in K[X] | Q \text{ on jaollinen } P\text{:llä }\},$$

eli I_a on P:llä jaollisten alkioiden joukko, P:n virittämä **pääideaali**, jota on tapana merkitä (P). Itse asiassa kohdan (4) todistus kelpaa lähes sellaisenaan näyttämään, että jokainen muukin polynomirenkaan $K[X]$ ideaali on pääideaali. Polynomirengas on siis ns. **pääideaalirengas**. Samaan tapaan – siis jakolaskualgoritmilla – voi todeta, että myös $\mathbf{Z}$ on pääideaalirengas. Tee se! Tämä selittää osaltaan nimitystä ideaali. Tunnetuimmassa renkaassa $\mathbf{Z}$ ideaalit vastaavat edellä sanotun mukaan lukuja: kukin pääideaali on jonkin luvun virittämä. Yleisemmässä renkaassa on muitakin ideaaleja kuin pääideaalit eli "luvut". On siten perusteltua sanoa näitä "ideaalisiksi luvuiksi", mistä nykyinen nimi on lyhenne.

(2) ν:n rajoittuma K:hon on injektio ja siis kuvaansa samaistettuna K on S:n alikunta ja
(3) P on kuntalaajennuksen $S : K$ minimaalipolynomi.

(1) Ainakin kyseessä on kommutatiivinen rengas, jolla on ykkösenä $1 = \nu(1)$. Olkoon $[Q] = Q + I \in S \setminus \{0\}$. Tehtävänä on löytää sille käänteisalkio $[R] = R + I \in S \setminus \{0\}$, jolle olisi voimassa

$$\begin{aligned} [Q][R] &= [1], \text{ eli} \\ QR &\in 1 + I, \text{ eli} \\ QR - 1 &\text{ on jaollinen } P\text{:llä.} \end{aligned}$$

Oletuksemme mukaan P on jaoton eikä jaa Q:ta (koska $[Q] \neq 0$), ja on siis voimassa Eukleideen algoritmiin (1.12.) perustuva kaava

$$AP + BQ = 1$$

sopiville polynomeille A ja B. Tämäpä ratkaisikin asian, sillä R:ksi kelpaa selvästikin B.
(2) Jokainen nollasta eroava rengashomomorfismi kunnalta renkaalle on injektio! (Syy: homomorfismin ydin on $\{0\}$ tai ideaali, siis kunnan tapauksessa $\{0\}$ tai koko kunta.)
(3) Kuntalaajennus $S : K$ on ensinnäkin yksinkertainen, sillä $S = K([X]) = K(X + I)$, joten väitteen α:ksi kelpaa polynomin X luokka. Osoitamme, että P on α:n eli $[X]$:n minimaalipolynomi. Ensinnäkin todella $P(\alpha) = 0$, eli $P([X]) = [P(X)] = [0]$. Toiseksi P on jaoton ja perusmuotoinen. Lause on todistettu. □

Tässä luomaamme tekijäavaruutta S on syytä vielä kerran vilkaista (ja verrata esim $\mathbf{Z}_p$:hen). S:n alkioita ovat polynomien luokat $Q + I$. Kutakin niistä edustaa jakolaskualgoritmin takia tasan yksi Q, jonka aste on alle I:n virittäjän P asteen. S:n laskutoimitukset näille Q ovat muuten tavanomaiset, mutta saataessa (polynomeja kertoessa) asteeltaan liian korkeita suoritetaan reduktio modulo P eli huomataan luokan edustajaksi kelpaavan jakojäännöksen.

Olemme nyt jo pitkälti selvittäneet, miten kunnan K yksinkertaiset algebralliset laajennukset ja sen jaottomat perusmuotoiset polynomit vastaavat toisiaan, sillä tiedämme nyt, että jokaisella algebrallisella laajennuksella $K(a) : K$ on yksi ja vain yksi minimaalipolynomi P, jolla

$P(a) = 0$,[10] ja toisaalta jokainen jaoton perusmuotoinen polynomi on jonkin algebrallisen laajennuksen minimaalipolynomi. Todistamme nyt vielä, että kaksi laajennusta, joilla on sama minimaalipolynomi, yhtyvät. Tämä voi tietenkin olla totta vain "isomorfiaa vaille".

2.8. Lause. *Olkoot $K(\alpha) : K$ ja $K(\beta) : K$ kunnan K yksinkertaisia laajennuksia, joilla on sama minimaalipolynomi P. Silloin ne ovat isomorfisia laajennuksia*[11], ts. on olemassa kuntaisomorfismi

$$\varphi : K(\alpha) \to K(\beta), \quad \text{jolla}$$
$$\varphi|_K = I_K (= K\text{:n identtinen kuvaus.})$$

Itse asiassa voimme lisäksi valita isomorfismin φ siten, että $\varphi(\alpha) = \beta$.

Todistus. Tehtävänä on määritellä $\varphi(x)$ kaikille $x \in K(\alpha)$ ja todistaa $\varphi(x)$ kuntalaajennusisomorfismiksi $K(\beta)$:lle. Määrittelyä varten on tarpeen lausua laajan kunnan alkio $x \in K(\alpha)$ **standardimuodossa**, johon antaa vihjeen edellisen lauseen konstruktio, nimittäin muodossa

$$x = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n,$$

missä n on (P:n aste -1) ja kertoimet $a_0, \ldots, a_n \in K$. Tämä esitys on olemassa ja vieläpä yksikäsitteinenkin, mutta lykätään sen tarkastelua hetken tuonnemmaksi ja määritellään

$$\varphi(x) = a_0 + a_1\beta + a_2\beta^2 + \cdots + a_n\beta^n.$$

Tämä toimii, sillä ainakin em. esityksen yksikäsitteisyys ja olemassaolo $K(\alpha)$:ssa takaavat, että näin saadaan kuvaus $K(\alpha) \to K(\beta)$ ja vastaavasti yksikäsitteisyys ja olemassaolo $K(\beta)$:ssa, että saadaan injektio ja surjektio. $\varphi(x)$ on siis bijektio $K(\alpha) \to K(\beta)$. Testataan, että se on rengashomomorfismi ja kuvaa K:n alkiot itselleen. Olkoot

$$x = A(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n \text{ ja}$$
$$y = B(\alpha) = b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_n\alpha^n \in K(\alpha).$$

[10] Sama yksinkertainen laajennus voidaan tuottaa adjungoimalla K:hon **eri** alkioita, esim. $\mathbf{Q}(\sqrt{2}) = \mathbf{Q}(\sqrt{2}+1)$ ja näihin liittyy eri minimaalipolynomit, onhan niillä eri juuret. Älä hämäänny tästä!

[11] Riittäisi tarkastella kahden isomorfisen kunnan K ja K' laajennuksia $K(\alpha)$ ja $K'(\beta)$. Minimaalipolynomien pitäisi olettaa olevan tätä isomorfiaa vaille samat. Tuloksena olisi, että laajennuksetkin ovat isomorfiaa vaille samat siinä mielessä, että saadaan kuntaisomorfismi $\varphi : K(\alpha) \to K'(\beta)$, jolla rajoittuma $\varphi|_K$ on alkuperäinen isomorfismi $K \to K'$ ja voisimme huolehtia siitä, että $\varphi(\alpha) = \beta$. Tulemme itse asiassa tarvitsemaan lausetta 2.8. juuri tässä näennäisesti yleisemmässä muodossa.

Silloin selvästikin

$$\begin{aligned}&\varphi(x+y)=\\&=(a_0+b_0)+(a_1+b_1)\alpha+(a_2+b_2)\alpha^2+\cdots+(a_n+b_n)\alpha^n=\\&=\varphi(x)+\varphi(y)\end{aligned}$$

ja lisäksi vastaava pätee tulollekin: Myös tulo xy on muotoa

$$xy=C(\alpha)=c_0+c_1\alpha+c_2\alpha^2+\cdots+c_n\alpha^n.$$

Polynomeja A, B ja C yhdistää tieto, että

$$\begin{aligned}A(\alpha)B(\alpha)&=C(\alpha)\text{ eli}\\(AB-C)(\alpha)&=0,\end{aligned}$$

mutta tämä merkitsee, että α:n minimaalipolynomi P jakaa $(AB-C)$:n. C **on siis jakojäännös, joka saadaan jaettaessa** AB**:tä** P**:llä**, onhan C:n aste $\leq n = P$:n aste -1. Vastaava päättely voidaan tehdä kuvapuolella: kuvien tuloa esittää sama polynomi C. Juuri tätä väitetäänkin. □

Todistettavaksi jäi lemma:

2.9. Lemma. *Olkoon P laajennuksen $K(\alpha) : K$ minimaalipolynomi ja $x \in K(\alpha)$. On olemassa tasan yksi asteeltaan P:tä alempi polynomi $A \in K[X]$, jolle*

$$x=A(\alpha)=a_0+a_1\alpha+a_2\alpha^2+\cdots+a_n\alpha^n.$$

Todistus. Todistetaan aluksi yksikäsitteisyys. Olkoon

$$\begin{aligned}&x=A(\alpha)=a_0+a_1\alpha+a_2\alpha^2+\cdots+a_n\alpha^n \quad \text{ja}\\&x=B(\alpha)=b_0+b_1\alpha+b_2\alpha^2+\cdots+b_n\alpha^n, \quad n=P\text{:n aste } -1.\end{aligned}$$

Silloin selvästikin $(A-B)(\alpha)=0$ ja $A-B$ on asteeltaan aidosti alempi kuin α:n minimaalipolynomi P. Siis $A-B=0$.

Olemassaolopuolen todistus alkaa havainnolla, että jokainen $K(\alpha)$:n alkio on muotoa $\frac{S(\alpha)}{T(\alpha)}$, missä S ja $T \in K[X]$, sillä tällaisten alkioiden joukko on selvästikin jo $K(\alpha)$:n alikunta, joka sisältää sekä K:n että alkion α.

Pyritään laventamaan $\frac{S}{T}$ jollakin polynomilla siten, että nimittäjä saisi kohdassa α arvon 1. Ehto $T(\alpha)\neq 0$ takaa, että nimittäjäpolynomi

T ei ole jaollinen minimaalipolynomilla P, vaan on olemassa polynomit F ja $G \in K[X]$ siten, että

$$\begin{aligned} FT + GP &= 1, && \text{jolloin erityisesti} \\ F(\alpha)T(\alpha) + G(\alpha)P(\alpha) &= 1, && \text{ja siis} \\ F(\alpha)T(\alpha) &= 1. \end{aligned}$$

Laventamalla polynomilla F saa $K(\alpha)$:n alkio $x = \frac{S(\alpha)}{T(\alpha)}$ siis muodon

$$x = \frac{(FS)(\alpha)}{1} = (FS)(\alpha),$$

joka on muuten halutunlainen esitys, paitsi että polynomin FS asteesta ei tiedetä mitään. Jos aste ei valmiiksi ole pienempi kuin P:n aste niin korjataan asia jakamalla FS P:llä ja huomaamalla, että jakojäännöksellä on oikeanlainen aste ja pistessä α sama arvo x kuin FS:llä. $\square$

Kuntalaajennuksen aste. Jokainen kunta K on $1-$ulotteinen $K-$kertoiminen vektoriavaruus. Itse asiassa myös jokainen kunnan K laajennus on $K-$vektoriavaruus. Koska asia on tärkeä, esitämme muodollisen määritelmän:

2.10. Määritelmä. Olkoon $L : K$ kuntalaajennus. Laskutoimitukset

$$+ : L \times L \to L : (x, y) \mapsto x + y$$
$$\cdot : K \times L \to L : (\alpha, y) \mapsto \alpha y$$

tekevät L:stä $K-$vektoriavaruuden. Sen dimensio on kuntalaajennuksen $L : K$ **aste**. Astetta merkitään

$$[L : K] = \dim_K(L).$$

Esimerkkejä.

$$[\mathbf{C} : \mathbf{R}] = 2$$
$$[\mathbf{C}(X) : \mathbf{C}] = \infty$$
$$[\mathbf{R} : \mathbf{Q}] = \infty$$
$$[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2.$$

Seuraava lause antaa laskuapua asteen määräämiseen.

2.11. Lause. *Olkoot K, L ja M toistensa alikuntia siten, että:*

$$K \subset L \subset M.$$

Nyt:

$$[M : K] = [M : L][L : K]$$

Todistus[12]*.* Olkoon

$$K - \text{vektoriavaruudella } L \text{ kanta } (e_i)_{i \in I} \text{ ja}$$
$$L - \text{vektoriavaruudella } M \text{ kanta } (f_j)_{j \in J}.$$

Osoitamme, että

$$K-\text{vektoriavaruudella } M \text{ on kanta } (e_i f_j)_{i \in I, j \in J}.$$

[12]Todistamme lauseen tapauksessa, jossa dimensiot ovat äärellisiä. Symbolille ∞ tai kardinaaliluvuille todistus on samantapainen.

(1) Todistetaan, että vektorit $e_i f_j, \quad i \in I, j \in J$ virittävät M:n. Tarkastellaan alkiota $x \in M$.

$$x = \sum_{j \in J} \mu_j f_j$$

joillekin $\mu_j \in L$ ja siis, koska jokainen μ_j vastaavasti on muotoa

$$\mu_j = \sum_{i \in I} \lambda_{ij} e_i, \quad \lambda_{ij} \in K,$$

saadaan haluttu kehitelmä

$$x = \sum_{i \in I, j \in J} \lambda_{ij} e_i f_j.$$

(2) Todistetaan lineaarinen riippumattomuus. Olkoon

$$\begin{aligned} 0 = \sum_{i \in I, j \in J} \lambda_{ij} e_i f_j = \\ = \sum_{j \in J} (\sum_{i \in I} \lambda_{ij} e_i) f_j \end{aligned}$$

Koska f_j:t ovat lineaarisesti riippumattomia ja $\sum_{i \in I} \lambda_{ij} e_i \in L$, on jokainen

$$\sum_{i \in I} \lambda_{ij} e_i = 0$$

ja siis, koska e_i:t ovat lineaarisesti riippumattomia ja $\lambda_{ij} \in K$, on jokainen

$$\lambda_{ij} = 0.$$

□

Esimerkki.

$$[\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}] = \underbrace{[\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}(\sqrt{2})]}_{2} \underbrace{[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}]}_{2} = 4.$$

Lause antaa jopa kannan $(1, \sqrt{2}, \sqrt{3}, \sqrt{2}\sqrt{3})$.

2.12.Lause. *Olkoon $K(\alpha) : K$ yksinkertainen kuntalaajennus.*

(1) *Jos α on transkendenttinen, niin $[K(\alpha) : K] = \infty$.*
(2) *Jos α on algebrallinen, niin $[K(\alpha) : K]$ on α :n* **minimaalipolynomin aste** ja siis erityisesti äärellinen!

Todistus.

(1) Isomorfismia vaille $K(\alpha)$ on $K(X)$, jossa lineaarisesti riippumattomia ovat ainakin $1, X, X^2, \ldots$.
(2) Olkoon minimaalipolynomin aste n. Lemman 2.9. mukaan $K(\alpha)$:n kannaksi kelpaa $(1, \alpha, \alpha^2 \ldots, \alpha^{n-1})$. □

Tarkastelemme seuravassa myös muita kuin yksinkertaisia laajennuksia.

2.13. Määritelmä.

(1) Kuntalaajennus $L : K$ on *äärellinen*, jos $[L : K] < \infty$.
(2) Kuntalaajennus $L : K$ on *algebrallinen*, jos jokainen $a \in L$ on algebrallinen, so. jonkin $K-$kertoimisen polynomin juuri.

Näiden käsitteiden välillä vallitsee tärkeä yhteys, jonka olemme itse asiassa jo löytäneet.

2.14. Lause. *Kuntalaajennus $L : K$ on äärellinen aina ja vain kun*

(1) *$L : K$ on algebrallinen ja*
(2) *$L = K(\alpha_1, \ldots, \alpha_s)$ joillekin äärellisen monelle $\alpha_1, \ldots, \alpha_s \in L$.*

Todistus. Ehtojen riittävyys seuraa induktiopäättelyllä lauseista 2.11. ja 2.12. Välttämättömyys todetaan seuraavasti:

Olkoon $L : K$ äärellinen, jolloin on olemassa $K-$vektoriavaruuden L kanta $(e_1, \ldots, e_n)$. Jokainen L:n alkio on siten muotoa

$$x = a_1 e_1 + \cdots + a_n e_n, \quad a_i \in K$$

ja kuuluu siis varmasti kuntalaajennukseen $K(e_1, \ldots, e_n)$. Tämä todistaa jälkimmäisen väitteen. Todistetaan vielä, että $L : K$ on algebrallinen. Sitä varten valitaan mielivaltainen $x \in L$. Jonossa $(1, x, x^2, \ldots, x^n)$ on $n + 1$ jäsentä, siis enemmän kuin L:n kannassa on kantavektoreita. Siksi jono on lineaarisesti riippuva eli on olemassa nollasta eroavat kertoimet $\lambda_1, \ldots, \lambda_n$, joille

$$\sum_{i=0}^{n} \lambda_i x^i = 0.$$

Nyt x on polynomin $P(X) = \sum_{i=0}^{n} \lambda_i X^i$ nollakohta, siis algebrallinen. □

Algebrallisten lukujen kunta. Muistamme aluksi, että kompleksiluku z on määritelmän mukaan algebrallinen aina ja vain kun on olemassa rationaalilukukertoiminen, perusmuotoinen polynomi $P_1 = a_0 + a_1 + \cdots +^n$, jolla $P_1(z) = 0$. Lukija on hyvinkin jo saattanut kokeilla algebrallisten lukujen joukon osoittamista kunnaksi tai edes ryhmäksi ja huomata, että se ei suoraan määritelmästä lähtemällä ole helppoa. Nyt käytämme edellä kehiteltyjä apuvälineitä ja onnistumme.

2.15. Lause. *Algebrallisten lukujen joukko* $\mathbf{A}$ *on* $\mathbf{C}$*:n alikunta.*

Todistus. Todistimme edellä , että kompleksiluku α on algebrallinen aina ja vain, kun yksinkertainen kuntalaajennus $\mathbf{Q}(\alpha) : \mathbf{Q}$ on äärellinen.

Olkoot α ja β kaksi algebrallista lukua. Osoitetaan, että niiden summakin on algebrallinen. Oletuksen mukaan

$$\begin{aligned} & [\mathbf{Q}(\alpha) : \mathbf{Q}] < \infty \\ \text{ja} \quad & [\mathbf{Q}(\beta) : \mathbf{Q}] < \infty \end{aligned}$$

ja edelleen 2.14.:n nojalla

$$[\mathbf{Q}(\alpha)(\beta) : \mathbf{Q}(\alpha)] \leq [\mathbf{Q}(\beta) : \mathbf{Q}] < \infty,$$

kelpaahan $\mathbf{Q}-$kertoiminen polynomi nollaamaan β:n myös sen algebrallisuuden toteamiseksi kunnassa $\mathbf{Q}(\alpha)$. Nytpä

$$\mathbf{Q}(\alpha + \beta) \subset \mathbf{Q}(\alpha, \beta) = \mathbf{Q}(\alpha)(\beta),$$

ja siis

$$\begin{aligned} [\mathbf{Q}(\alpha + \beta) : \mathbf{Q}] &\leq [\mathbf{Q}(\alpha, \beta) : \mathbf{Q}] = \\ &= [\mathbf{Q}(\alpha)(\beta) : \mathbf{Q}(\alpha)][\mathbf{Q}(\alpha) : \mathbf{Q}] \\ &< \infty. \end{aligned}$$

Luku $\alpha + \beta$ on siis alussa tehdyn huomautuksen nojalla algebrallinen.

Vastaavanlainen päättely antaa myös tiedon, että $\alpha - \beta$, $\alpha\beta$ ja α:n ollessa nollasta eroava myös α^{-1} ovat algebrallisia. $\square$

3. Harppi ja viivoitin

Kreikkalaisten geometria ja klassiset ongelmat. Aksiomaattinen ja yleisemminkin deduktiivinen matematiikka, siis teoreemojen todisteleminen tiukkojen sääntöjen puitteissa on tunnetusti peräisin muinaisesta Kreikasta. Klassisen geometrian perusprobleemoita oli geometristen konstruktioiden tekeminen harpilla ja viivoittimella. Näillä voidaankin saada aikaan monenlaista. Janan voi jakaa haluttuun määrään yhtä pitkiä osia, pisteen kautta voi piirtää annetun suoran suuntaisen suoran, kulman voi puolittaa, annettua neliötä pinta-alaltaan kaksinkertaisen neliön voi piirtää, annetun monikulmion kokoisen neliön voi piirtää. Kolmea kuuluisaa konstruktiota ei kuitenkaan osata tehdä, vaikka aikojen kuluessa on nähty paljon vaivaa ratkaisuyrityksien eteen

(1) mielivaltaisen kulman jakoa kolmeen yhtä suureen osaan
(2) annetun ympyrän kokoisen neliön piirtämistä
(3) annettua kuutiota tilavuudeltaan kaksinkertaisen kuution konstruoimista.

Kreikkalaiset ja heidän seuraajansa eivät ilmeisesti tulleet ajatelleeksi, että saattaisi olla mahdollista todistaa tehtävät mahdottomiksi. Sen teemme tässä luvussa käyttäen algebrallisia menetelmiä pisteiden koordinaatteihin. Vaikka mahdottomuus voidaan todistaa, on vieläkin olemassa harrastelijamatemaatikoita, jotka tosissaan yrittävät esim. kulmien kolmijakoa.[13]

Muilla työkaluilla em. ongelmat on kyllä mahdollista ratkaista. Tähän riittää esimerkiksi jo Arkhimedeen käyttämä kahdella merkillä varustettu viivain ja harppi. Ironista iloa aiheuttaa meidän jälkeentulleiden päässä tieto siitä, että kaikki konstruktiot, joita kreikkalaseen tyyliin voi tehdä harpilla ja viivoittimella on mahdollista suorittaa vielä vähemmillä työkaluilla. Viivoittimesta voi luopua (Mohr 1672), tai sitten harpista, jos on annettu yksi kiinteä ympyrä ja sen keskipiste (Steiner 1832) tai kaksi toisiaan sivuavaa ympyrää (Cauer 1912).

Konstruoituvat pisteet ja luvut.

3.1. Määritelmä. Olkoon J_0 joukko tason $\mathbf{R}^2$ pisteitä.

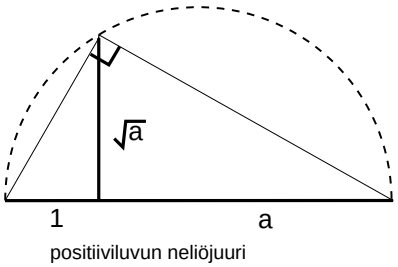
(1) Suora s **saadaan joukosta** J_0, jos se kulkee ainakin kahden s:n eri pisteen kautta. Ympyrä y **saadaan joukosta** J_0, jos sen keskipiste kuuluu joukkoon ja sen säde on kahden joukkoon kuuluvan pisteen etäisyys.

[13] Ks. esim. U.Dudley: What To Do, When the Trisector Comes. The Mathematical Intelligencer Vol.5 No. 1 (1983).

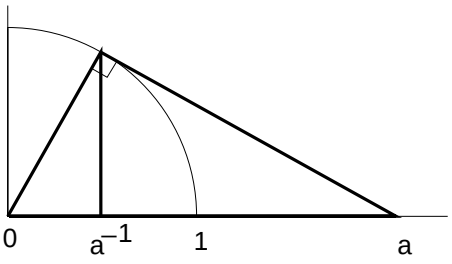
(2) Piste $z = (x, y) \in \mathbf{R}^2$ on joukosta J_0 **yhdellä askelella konstruoituva**, mikäli se on kahden joukosta J_0 saatavan eri ympyrän tai suoran leikkauspiste.
(3) Piste $z = (x, y)$ on joukosta J_0 **konstruoituva**, mikäli on olemassa pisteet $z_1, \ldots, z_n \in \mathbf{R}^2$ siten, että $z = z_n$ ja kukin z_j on yhdellä askelella konstruoituva joukosta $J_0 \cup \{z_1, \ldots, z_{j-1}\}$ — tapauksessa $j = 1$ joukosta J_0.
(4) Piste $z \in \mathbf{R}^2$ on **konstruoituva**, mikäli se on konstruoituva joukosta $\{(0, 0), (0, 1)\} \subset \mathbf{R}^2$
(5) Luku $x \in \mathbf{R}$ on **konstruoituva**, mikäli se on jonkin konstruoituvan pisteen $x-$ tai $y-$koordinaatti.

3.2. Huomautus. *Konstruoituvien lukujen joukko* $\mathbf{K}$ *on* $\mathbf{R}$*:n alikunta.*

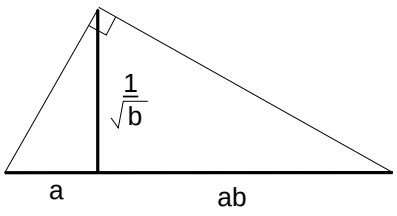
Todistus. Olkoot x_1 ja x_2 reaalilukuja. Niiden summa ja erotus ovat tietysti konstruoituvia, käänteisluvutkin on helppo konstruoida oheisen piirroksen mukaan. Tulon konstruointi käy konstruoimalla ensin neliöjuuri.



positiiviluvun neliöjuuri



positiiviluvun käänteinen



positiivilukujen tulo

□

Seuraus: Kaikki rationaaliluvut ja niiden parilliset juuret ovat konstruoituvia.

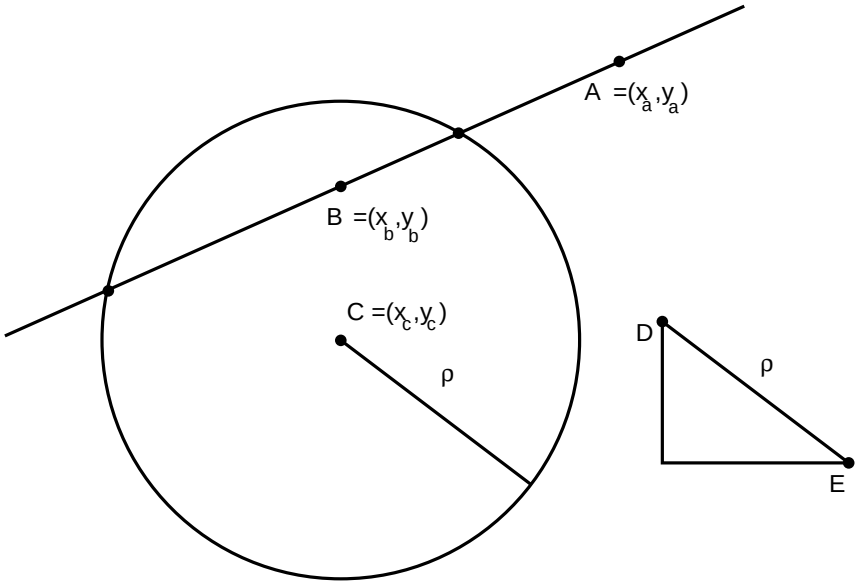
3.3. Merkintöjä. Olkoon J_0 joukko tason pisteitä ja $z = (x, y)$ joukosta J_0 konstruoituva piste. Olkoot pisteet $z_1 = (x_1, y_1), \ldots, z_n = (x_n, y_n)$ sellaiset, että $z = z_n$ ja kukin z_j on yhdellä askelella konstruoituva joukosta $J_0 \cup \{z_1, \ldots, z_{j-1}\}$; tapauksessa $j = 1$ joukosta J_0.

$\mathbf{K}_0$ olkoon J_0:aan kuuluvien pisteiden koordinaattien virittämä $\mathbf{R}$:n alikunta ja

$$\begin{aligned} \mathbf{K}_1 &= \mathbf{K}_0(x_1, y_1) \\ &\ldots \\ \mathbf{K}_n &= \mathbf{K}_{n-1}(x_n, y_n) \end{aligned}$$

3.4. Lause. *x_j ja y_j ovat $\mathbf{K}_{j-1}-$mielessä algebrallisia, vieläpä niin, että kumpikin on jonkin $\mathbf{K}_{j-1}$–kertoimisen toisen asteen polynomin nollakohta. Vastaavien minimaalipolynomin aste on siis 1 tai 2.*

Todistus. Konstruktion mukaan x_j ja y_j ovat



kuvan mukaisesti erään suoran ja ympyrän (tai kahden suoran tai ympyrän) leikkauspisteen koordinaatit, missä pisteiden A, B, C, D ja E koordinaatit kuuluvat kuntaan $\mathbf{K}_{j-1}$, kuten Pythagoraan lauseen nojalla myös ρ^2. Suoran yhtälö on

$$y = y_a + \frac{y_b - y_a}{x_b - x_a}(x - x_a), \text{ kun } x_b \neq x_a$$

ja ympyrän yhtälö on

$$(x - x_c)^2 + (y - y_c)^2 = \rho^2.$$

Sijoittamalla y:n lauseke ylemmästä alempaan yhtälöön saadaan x:lle toisen asteen yhtälö

$$(x - x_c)^2 + \left(y_a + \frac{y_b - y_a}{x_b - x_a}(x - x_a) - y_c\right)^2 = \rho^2,$$

jonka kertoimet ovat kunnassa $\mathbf{K}_{j-1}$. Tämän olemassaolo merkitsee, että x_j on $\mathbf{K}_{j-1}-$algebrallinen ja sen minimaalipolynomi on korkeintaan astetta 2. Vastaava pätee y_j:lle. Saman tapaisella laskulla voi todeta, että myös kahden ympyrän tapaus, joka johtaa kahden toisen asteen yhtälön pariin, sievenee toisen asteen yhtälöiksi x:lle ja y:lle. Kahden suoran tapaus on vielä helpompi; leikkauspiste kuuluu samaan reaalilukujen alikuntaan, $\mathbf{K}_{j-1}$ kuin suorat määräävien neljän pisteen koordinaatitkin. □

3.5. Lause. *Olkoon $z = (x, y)$ konstruoituva joukosta J_0. Asteet $[\mathbf{K}_0(x) : \mathbf{K}_0]$ ja $[\mathbf{K}_0(y) : \mathbf{K}_0]$ ovat luvun 2 potensseja.*

Todistus. Olkoon $z = (x, y)$ konstruoitu J_0:sta lisäämällä siihen konstruktion eri vaiheissa pisteet $z_1, z_2, \ldots, z_n = z$, koordinaatein $z_j = (x_j, y_j)$. Edellisen lauseen mukaan asteet

$$[\mathbf{K}_{j-1}(x_j) : \mathbf{K}_{j-1}] \text{ ja}$$
$$[\mathbf{K}_{j-1}(y_j) : \mathbf{K}_{j-1}]$$

ovat ykkösiä tai kakkosia. Koska tietysti

$$[\mathbf{K}_{j-1}(x_j)(y_j) : \mathbf{K}_{j-1}(x_j)] \leq [\mathbf{K}_{j-1}(y_j) : \mathbf{K}_{j-1}],$$

on tämäkin enintään kaksi. Siksi

$$[\mathbf{K}_j : \mathbf{K}_{j-1}] = [\mathbf{K}_{j-1}(x_j)(y_j) : \mathbf{K}_{j-1}(x_j)][\mathbf{K}_{j-1}(x_j) : \mathbf{K}_{j-1}]$$

on 1,2 tai 4. Induktiolla tästä seuraa, että

$$[\mathbf{K}_n : \mathbf{K}_0] = [\mathbf{K}_n : \mathbf{K}_{n-1}] \ldots [\mathbf{K}_1 : \mathbf{K}_0]$$

on kakkosen potenssi. Tästä seuraa alkuperäinen väittemme, jonka mukaan $[\mathbf{K}_0(x) : \mathbf{K}_0]$ on kakkosen potenssi, sillä

$$[\mathbf{K}_n : \mathbf{K}_0] = [\mathbf{K}_n : \mathbf{K}_0(x)][\mathbf{K}_0(x) : \mathbf{K}_0]$$

missä edellä todetun mukaan vasemman puolen luvulla ei ole muita alkutekijöitä kuin kakkosia. □

Harjoitustehtävä. Olkoon $\mathbf{K}(\alpha) : \mathbf{K}$ algebrallinen kuntalaajennus. Osoita, että seuraavat ovat yhtäpitäviä:

(1) Laajennuksen $\mathbf{K}(\alpha) : \mathbf{K}$ aste on kakkosen potenssi.
(2) On olemassa kuntalaajennus $\mathbf{K}(\beta) : \mathbf{K}$, jonka aste on kakkosen potenssi ja jolle $\alpha \in \mathbf{K}(\beta)$.

Kolme ratkaisua.

3.6. Lause. *Annetusta ympyrästä ei voi harpilla ja viivoittimella konstruoida alaltaan saman kokoista neliötä.*

Todistus. Valitaan ympyrän säde pituuden yksiköksi. Tehtävänä on siis konstruoida luku $\sqrt{\pi}$ lähtemällä ympyrän keskipisteestä ja säteestä, siis joukosta $J_0 = \{(0,0),(1,0)\}$, jolloin $\mathbf{K}_0 = \mathbf{Q}$. Nytpä olemme prologissa todistaneet, että π ei ole edes algebrallinen, eikä siis myöskään $\sqrt{\pi}$ kuulu algebrallisten lukujen kuntaan. Se ei siis edellisen lauseen ja lauseen 2.14. vuoksi voi myöskään olla konstruoituva. □

3.7. Lause. *Ei ole mahdollista konstruoida harpilla ja viivoittimella annetusta kuutiosta tilavuudeltaan kaksi kertaa suurempaa kuutiota.*

Todistus. Tämä merkitsisi luvun $\sqrt[3]{2}$ konstruoitavuuta rationaaliluvuista, mutta $\sqrt[3]{2}$:n minimaalipolynomi on tietysti x^3-2 ja sen aste 3 ei ole kakkosen potenssi. □

3.8. Lause. 60 *asteen kulmaa ei voi kolmijakaa harpilla ja viivoittimella.*

Todistus. Jos voisi, niin luku $cos\frac{\pi}{9}$ olisi konstruoituva rationaaliluvuista. Osoittautuu, että $cos\frac{\pi}{9}$ on kyllä algebrallinen ja sen minimaalipolynomin löytää, kun muistaa trigonomeriasta kaavan kolminkertaisen kulman kosinille

$$\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta).$$

Sijoittamalla tähän $\theta = \frac{\pi}{9}$ ja katsomalla tasasivuisesta kolmiosta, että $\cos\frac{\pi}{3} = \frac{1}{2}$ saa yhtälön

$$8\cos^3\frac{\pi}{9} - 6\cos\frac{\pi}{9} - 1 = 0,$$

eli lyhenteitä $x = 2\cos\frac{\pi}{9}$ käyttämällä

$$x^3 - 3x - 1 = 0. \tag{1}$$

Joka on lukenut lauseen 3.6. todistuksen tietää, että nyt riittää todeta tämä polynomi jaottomaksi $\mathbf{Q}$:ssa. Asian voi tarkastaa suoraan. Tutkittava kolmijako on siis mahdoton. □

Yksi vastaesimerkki. Lauseen 3.5. ehto konstruoituvuudelle on kyllläkin välttämätön, mutta **ei riittävä**. Annamme täydellisyyden vuoksi vastaesimerkin:

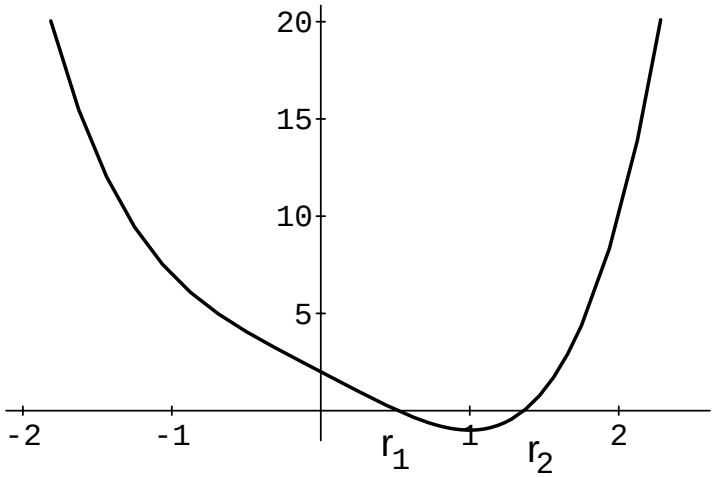
3.9. Esimerkki (Kalmanson)[14]. Jaottomalla polynomilla

$$P = X^4 - 4X + 2$$

on reaalinen juuri x, joka ei ole konstruoituva, vaikka

$$[\mathbf{Q}(x) : \mathbf{Q}] = 4.$$

Todistus. Eisensteinin ehdolla on helppo todeta polynomi jaottomaksi, joten aste ainakin on 4. Piirtämällä kuvaajan huomaa, että P:llä on tasan kaksi reaalista juurta, r_1 ja r_2, ja ne ovat välillä [0,2].



P hajoaa ensimmäisen ja toisen asteen tekijöihin, joten varmasti on olemassa kertoimet a, b, c ja d, joilla

$$(*) \qquad \begin{aligned} X^4 - 4X + 2 &= (X^2 + aX + b)(X^2 + cX + d) \\ &= (X - r_1)(X - r_2)(X^2 + cX + d). \end{aligned}$$

Kertoimia vertailemalla saadaan kaavasta $(*)$ yhtälöryhmä

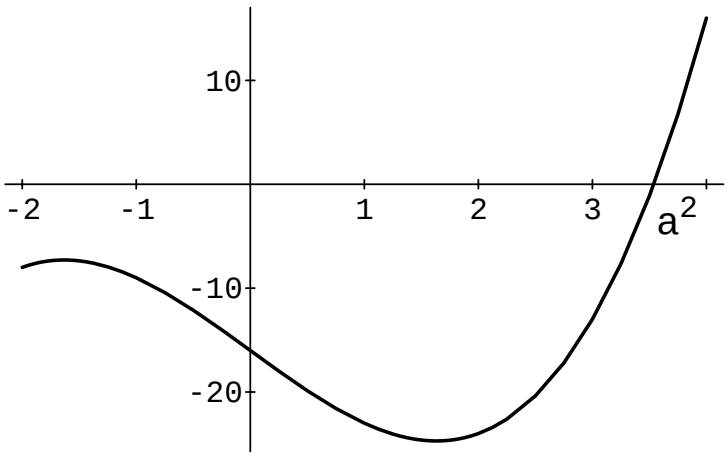
$$(**) \qquad \begin{aligned} a + c &= 0 \\ b + ac + d &= 0 \\ bc + ad &= -4 \\ bd &= 2, \end{aligned}$$

josta seuraa, merkitsemällä $X = a^2$:

$$16 = a^2((b + d)^2 - 4bd) = X(X^2 - 8) = X^3 - 8X.$$

[14]American Mathematical Monthly, **79**, 227-278 (1972)

Tämä on tuntemattomalle X kolmannen asteen yhtälö. Piirtämällä kuvaajan huomaa, että sillä on tasan yksi reaalinen juuri, ja se ei ole kokonaisluku, vaan $3 < a^2 < 4$.



Gaussin lauseen 1.19. nojalla polynomilla $X^3 - 8X - 16$ ei siis ole rationaalisia juuria, joten se on jaoton kolmannen asteen polynomi ja sen juuret siis konstruoitumattomia. Eritoten a^2 on siten konstruoitumaton, samoin siis a. Toisaalta $a = -r_1 - r_2$, joten ainakin toinen juurista r_1 ja r_2 on konstruoitumaton.

□

4. Galois'n teoria

Evariste Galois ... selvitti probleeman, johon eivät aikaisempien sukupolvien suuret matemaatikot olleet pystyneet yrityksistään huolimatta. Ajan myötä on käynyt selväksi, että hänen kehittämänsä **menetelmät** ovat monin verroin tärkeämpiä kuin ongelma, jonka ratkaisemaksi ne keksittiin. Galois otti käyttöön ratkeavan, yksinkertaisen ja normaalin ryhmän käsitteet, jotka ovat oleellisia ryhmien teoriassa. Lisäksi hän ratkaisi kuntia koskevan probleeman muuntamalla sen ryhmiä koskevaksi ja näin tehden ilmeisesti ensimmäisenä ...tutki matemaattista objektia liittämällä siihen rakenteeltaan yksinkertaisemman matemaattisen objektin. Liioittelematta voi sanoa, että Galois'n teoria on välttämätöntä ainakin suurelle osalle lukuteorian ja algebrallisen geometrian modernia tutkimusta. [J. BASTIDA [1]]

Luvussa 3 havaitsimme, että kuntalaajennukset ovat tehokkaita todistettaessa eräitä geometrisia tehtäviä mahdottomiksi ratkaista. Tuntuu sitäkin luontevammalta kokeilla niitä myös algebrallisiin ongelmiin. 1800–luvun alussa N.H. ABEL ja E. GALOIS onnistuivatkin tässä ja ratkaisivat mm. kysymyksen korkeamman kuin neljännen asteen algebrallisten yhtälöiden ratkaisukaavan olemassolosta. Palaamme tähän aiheeseen vasta luvussa 6, sillä osoittautuu, että tarvitsemme kuntalajennuksistamme tarkempaa tietoa kuin pelkän asteen, jonka hyväksi käyttöön edellä esitetyt geometriset mahdottomuustodistukset perustuivat. Tarkoitukseen sopivaa tarkempaa tietoa kuntalaajennuksen rakenteesta antaa sen Galois'n ryhmä. Seuraavassa kerromme, mikä Galois'n ryhmä on ja todistamme Galois'n teorian päälauseen, joka viime kädessä antaa yhteyden tämän ryhmän ja polynomin nollakohtien ominaisuuksien välille.

Galois loi teoriansa kompleksilukujen alikunnille ja välttyi siten erikseen pohtimasta mm. karakteristikaa ja separoituvuutta. Normaalin kuntalaajennuksen käsite on alkuperäinen. Seuraamamme vakiintunut esitystapa on olennaisesti peräisin E. ARTINilta (1898-1962).

Galois'n ryhmä.

4.1. Määritelmä. Olkoon $K \subset L$ alikunta .

(1) Kuntaisomorfismi $\alpha : L \to L$ eli L:n automorfismi on $K-$*automorfismi*, jos
$$\alpha(k) = k \quad \forall k \in K.$$

(2) L:n automorfismit muodostavat tunnetusti ryhmän kuvausten yhdistämisen ollessa laskutoimituksena. $K-$automorfismien joukko
$$\Gamma(L : K)$$

on sen aliryhmä. Kutsumme sitä kuntalaajennuksen $L : K$ *Galois'n ryhmäksi.*

4.2. Esimerkkejä.

Galois'n ryhmä $\Gamma(\mathbf{C} : \mathbf{R})$ muodostuu kaikista kuntaisomorfismeista

$$\alpha : \mathbf{C} \to \mathbf{C},$$

joilla

$$\alpha(x) = x \quad \forall x \in \mathbf{R}.$$

Määräämme kaikki tällaiset α. Olkoon $\alpha \in \Gamma(\mathbf{C} : \mathbf{R})$. Tunnemme jo α:n arvot $\mathbf{R}$:ssä. Myös kompleksisista arvoista voidaan sanoa jotakin. Koska α on kuntaisomorfismi ja siis säilyttää summat ja tulot, niin on esimerkiksi oltava voimassa

$$-1 = \alpha(-1) = \alpha(i^2) = \alpha(ii) = \alpha(i)\alpha(i) = (\alpha(i))^2,$$

eli myös $\alpha(i)$ on –1:n neliöjuuri, joko i tai $-i$. Tutkimme kummankin vaihtoehdon erikseen.

(1) Jos $\alpha(i) = i$, niin kaikille kompleksiluvuille $z = x + iy$ pätee

$$\alpha(z) = \alpha(x + iy) = \alpha(x) + \alpha(i)\alpha(y) = x + iy = z,$$

ja α on siis $\mathbf{C}$:n identtinen kuvaus, joka tietysti todella kuuluu Galois'n ryhmään $\Gamma(\mathbf{C} : \mathbf{R})$ ja on sen neutraalialkio.

(2) Jos $\alpha(i) = -i$, niin kaikille kompleksiluvuille $z = x + iy$ pätee

$$\alpha(z) = \alpha(x + iy) = \alpha(x) + \alpha(i)\alpha(y) = x - iy = \overline{z},$$

ja α on siis niin sanottu kompleksikonjugointi, eli $\mathbf{C}$:n heijastus $\mathbf{R}-$akselissa. Sekin todella kuuluu Galois'n ryhmään $\Gamma(\mathbf{C} : \mathbf{R})$. Tarkistamme vielä tämän: kaikilla z_1 ja $z_2 \in \mathbf{C}$ on

$$\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}, \text{ ja}$$
$$\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}.$$

Kaikille $z = x + 0i \in \mathbf{R}$ on lisäksi $\overline{z} = x - 0i = z$, kuten pitääkin. Galois'n ryhmä $\Gamma(\mathbf{C} : \mathbf{R})$ on siis kaksialkioinen ryhmä.

Toisena esimerkkinä määrätään samantapaisella menettelyllä Galois'n ryhmä $\Gamma(\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q})$. (Kuutiojuuri on tässä reaalinen.) Olkoon taas $\alpha \in \Gamma(\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q})$.

$$\alpha(x) = x \quad \forall x \in \mathbf{Q}, \text{ ja}$$
$$2 = \alpha(2) = \alpha((\sqrt[3]{2})^3) = (\alpha(\sqrt[3]{2}))^3,$$

joten $\alpha(\sqrt[3]{2})$ on se (todella ainoa) luku $s \in \mathbf{Q}(\sqrt[3]{2})$, jolle $s^3 = 2$, eli myös

$$\alpha(\sqrt[3]{2}) = \sqrt[3]{2}.$$

Koska jokainen $x \in \mathbf{Q}(\sqrt[3]{2})$ on muotoa $x = a + b\sqrt[3]{2} + c(\sqrt{2})^2$, missä a, b ja c ovat rationaalilukuja, on tullut todistetuksi että α on identtinen kuvaus. Galois'n ryhmä $\Gamma(\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q})$ on siis yksialkioinen eli triviaali.

Havaintoja. Yksinkertaisen algebrallisen kuntalaajennuksen Galois'n ryhmä liittyy esimerkkien valossa ilmeisesti sen minimaalipolynomin nollakohtiin. Löysimme Galois'n ryhmän nimen omaan käyttämällä hyväksi seuraavia periaatteita, jotka lukijan olisi mielellään todistettava oikeiksi.

(1) Olkoon $L : K$ kuntalaajennus, $P = a_0 + a_1X + a_2X^2 + \cdots + a_mX^m$ $K-$polynomi ja $x \in L$ sen nollakohta. Tällöin jokainen $K-$automorfismi α kuvaa x:n joksikin P:n nollakohdista: $P(\alpha(x)) = 0$. Koska $K-$automorfismi on injektio, niin se siis yksinkertaisesti **permutoi** P:n nollakohtia keskenään, onhan näiden joukko äärellinen.

(2) Erityisesti, jos P on yksinkertaisen algebrallisen kuntalaajennuksen $L : K$ minimaalipolynomi, niin $K-$automorfismi α määräytyy täysin vaikutuksestaan P:n nollakohtiin, koska L saadaan K:sta adjungoimalla ne, ja α:n rajoittuma K:hon on identtinen kuvaus. Yksinkertaisen algebrallisen kuntalaajennuksen Galois'n ryhmä voidaan siten samaistaa sen minimaalipolynomin nollakohtien joukon joidenkin permutaatioiden muodostamaan ryhmään.

(3) Sama idea toimii yleisemminkin, kun L on saatu K:sta adjungoimalla siihen jonkin $K-$polynomin juuria, vaikkapa "kaikki". Tämä johtaa meidät määrittelemään **normaalin** kuntalaajennuksen käsitteen ja tutkimaan nimen omaan sellaisen Galois'n ryhmää.[15]

Galois'n relaatio.

4.3. Määritelmä. Olkoot $K \subset M \subset L$ toistensa alikuntia. Merkitsemme tähän tilanteeseen liittyviä Galois'n ryhmiä lyhyesti

$$\Gamma(L : M) = M^*.$$

Erityisesti

$$\Gamma(L : K) = K^*. \quad \square$$

[15] Näin Galois itse luonnollisestikin menetteli Lagrangen ideaa seuraten. Permutaatioryhmistä lisää luvussa 5.

4.4. Huomautus. On hyvä huomata, että operaatio * kääntää inkluusiot: Jos $K \subset M_1 \subset M_2 \subset L$ ovat toistensa alikuntia, niin $M_2^* \subset M_1^*$.

Pohdimme seuraavassa miten — jos ollenkaan — M voitaisiin rekonstruoida $L : K$:sta ja ryhmästä M^*. Ainakin on varmaa, että M muodostuu pelkästään sellaisista L:n alkioista, jotka jokainen M^*:een kuuluva L:n automorfismi kuvaa itselleen. On ehkä jopa toivoa, että niiden joukko olisi itse M. Tähän varautuen on syytä määritellä

4.5. Määritelmä. Olkoon

$$H \subset K^* = \Gamma(L : K)$$

aliryhmä. Asetamme:

$$H^\dagger = \{x \in L \,|\, \alpha(x) = x \,\forall \alpha \in H\}.$$

On helppo todeta, että $H^\dagger$ on L:n alikunta ja sisältää K:n alikuntanaan. $H^\dagger$ on nimeltään *H:n kiintopistekunta.*

4.6. Lause.

(1) *Olkoot $H \subset G \subset \Gamma(L : K)$ aliryhmiä. Silloin*

$$G^\dagger \subset H^\dagger.$$

(2) *Olkoot $K \subset M \subset L$ alikuntia. Silloin*

$$M \subset (M^*)^\dagger.$$

(3) *Olkoon $H \subset \Gamma(L : K)$ aliryhmä. Silloin*

$$H \subset (H^\dagger)^*.$$

Todistus.

(1) Olkoon $h \in G^\dagger = \{x \in L \,|\, \alpha(x) = x \,\forall \alpha \in G\}$. Silloin $h \in L$ ja erityisesti $\alpha(h) = h$ kaikilla $\alpha \in H$.
(2) Olkoon $m \in M$. On osoitettava, että $m \in (M^*)^\dagger = \{x \in L \,|\, \alpha(x) = x \,\forall \alpha \in M^*\}$. Tämäpä seuraa suoraan M^*:n määritelmästä.
(3) Olkoon $\alpha \in H$. On osoitettava, että $\alpha \in (H^\dagger)^* = \{\alpha \in \Gamma(L : K) \,|\, \alpha(x) = x \,\forall x \in H^\dagger\}$. Tämäpä seuraa suoraan $H^\dagger$:n määritelmästä. □

Edellä esittämämme kysymys siitä, miten M:n voisi rekonstruoida vastaavasta ryhmästä M^* olisi ratkennut, jos edellä kohdassa (2) olisi voimassa yhtäsuuruus. Asiaa voi kokeilla esimerkkeihin. Tarjolla on esimerkki 4.2. ja siinä on helppo huomata, että

(1) kuntalaajennuksessa $\mathbf{C} : \mathbf{R}$ on $(\mathbf{R}^*)^\dagger = \mathbf{R}$, kuten saattaisi arvatakin, mutta
(2) kuntalaajennuksessa $\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}$ ei ole $(\mathbf{Q}^*)^\dagger = \mathbf{Q}$, vaan $(\mathbf{Q}^*)^\dagger = \mathbf{Q}(\sqrt[3]{2})$.

Joudumme siis pohtimaan, mistä kiikastaa, että toisinaan arvauksemme näyttää toimivan, toisinaan taas ei. Asia tulee ratkeamaan tyydyttävästi, kun ensin on määritelty tarvittavat normaalin ja separoituvan kuntalaajennuksen käsitteet, joihin esimerkin 4.2. yhteydessä jo vihjaistiinkin. Tulos on kuuluisa *Galois'n päälause.*

Hajoituskunta. Edellä esimerkissä (1) esiintynyt kompleksilukujen kunta $\mathbf{C}$ on *algebrallisesti täydellinen,* onhan voimassa algebran peruslause, jonka mukaan jokaisella $\mathbf{C}-$polynomilla on nollakohta $\mathbf{C}$:ssä, ja siitä seuraa tunnetusti, että kompleksilukujen kunnassa jokainen polynomi voidaan lausua tulona ensimmäisen asteen tekijöistä, eli *hajoaa* $\mathbf{C}$*:ssä.* Määrätessämme $\mathbf{R}$:n Galois'n ryhmää $\mathbf{C}$:ssä oli oleellista, että -1:n molemmat neliöjuuret kuuluvat $\mathbf{C}$:hen. Esimerkissä (2) olennainen ero edelliseen oli, että luvun 2 kuutiojuurista, eli $\sqrt[3]{2}$:n minimaalipolynomin nollakohdista vain yksi kuului tutkittavaan laajaan kuntaan $\mathbf{Q}(\sqrt[3]{2})$ ja minimaalipolynomi $x^3 - 2$ jakautuu siinä vain tuloksi 2. asteen ja 1. asteen polynomista. Tämä antaa aiheen seuraavaan määritelmään.

4.7. Määritelmä.

(1) Olkon $L : K$ kuntalaajennus. n:nnen asteen polynomi $P \in K[X]$ *hajoaa kunnassa* L, mikäli sillä on L:ssä täydet n nollakohtaa, eli

$$P(X) = k(X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_n)$$

joillekin $\alpha_1, \dots, \alpha_n \in L$. Sama nollakohta saa toistua. Luonnollisesti $k \in K$.

(2) K-polynomin P *hajoituskunta* on minimaalinen K:n laajennus Σ, jossa P hajoaa. Tämä tarkoittaa, että
   - i Σ on K:n laajennus.
   - ii P hajoaa Σ:ssa.
   - iii Jos $K \subset \Xi \subset \Sigma$ ja P hajoaa Ξ:ssä, niin $\Xi = \Sigma$.

4.8. Huomautus. Kohdan iii voi lausua myös näin:

iii' $\Sigma = K(\sigma_1, \dots, \sigma_n)$,
missä $\sigma_1, \dots, \sigma_n$ ovat P:n nollakohdat Σ:ssa.

Perustelu. iii $\implies$ iii', sillä P hajoaa kunnassa $K(\sigma_1, \ldots \sigma_n) \subset \Sigma$.

iii' $\implies$ iii, sillä selvästikin jokainen kunta $\Xi \subset K(\sigma_1, \ldots, \sigma_n)$, jossa P hajoaa, sisältää nollakohdat $\sigma_1, \ldots, \sigma_n$ ja siis koko $K(\sigma_1, \ldots \sigma_n)$:n.

4.9. Lause (Olemassaolo ja **Y**ksikäsitteisyys). *Jokaisella vakiosta eroavalla polynomilla $P \in K[X]$ on kuntalaajennusten isomorfiaa vaille tasan yksi hajoituskunta.*[16]

Todistus. Aloitamme konstruktiolla. Jos alkuperäinen kunta K olisi $\mathbf{C}$:n alikunta, niin P:n hajoituskunta saataisiin siitä adjungoimalla P:n kompleksiset juuret ja olisi siis $\mathbf{C}$:n alikunta. Myös yleisen kunnan K tapauksessa osaamme adjungoida polynomin juuren kuntaan, ainakin kun polynomi on jaoton ja kelpaa siis yksinkertaisen laajennuksen minimaalipolynomiksi. Tätä tietoa ja induktiota P:n asteen suhteen käytämme seuraavasti.

(1) Jos P on 1. astetta, K on sen hajoituskunta.

(2) Oletamme, että jokaisella enintään asteen n polynomilla on hajoituskunta, olipa alkuperäinen kunta mikä tahansa. Olkoon P asteen $n+1$ polynomi. Jos P hajoaa kunnassa K, on hajoituskunta löytynyt. Muuten on olemassa sen jaoton tekijä P_1, joka on vähintään toista astetta. Laajennetaan K adjungoimalla siihen (lauseen 2.7. mukaisesti) jokin jaottoman polynomin P_1 juuri α. Nyt α on myös P:n nollakohta kunnassa $K(\alpha)$. Tässä kunnassa siis

$$P(X) = (X - \alpha)Q(X),$$

ja Q on astetta n. Induktio-oletuksen mukaan $K(\alpha)-$polynomilla Q on olemassa hajoituskunta Σ. Se on selvästi myös P:n hajoituskunta.

Myös yksikäsitteisyys palautuu induktiolla vastaavaan jaottomia polynomeja koskevaan tulokseen. Todistamme itse asiassa hieman enemmän kuin lauseessa väitetään:[17]

Olkoon $i : K \to \widetilde{K}$ kuntaisomorfismi ja $P(X) = a_0 + \cdots + a_n X^n \in K[X]$ polynomi. Sanomme polynomia $\widetilde{P}(X) = i(a_0) + \cdots + i(a_n)X^n \in \widetilde{K}[X]$ sen isomorfiseksi vastineeksi $\widetilde{K}[X]$:ssa. Olkoon Σ P:n ja $\widetilde{\Sigma}$ $\widetilde{P}$:n hajoituskunta.

[16] Yleistämme tässä lauseen 2.8. tilanteen koskemaan mielivaltaisen polynomin P kaikkia nollakohtia.

[17] Näennäisesti yleisempi muoto on helpompi todistaa. Tähän tarkoitukseen sopii lauseen 2.8. yleisempi muoto.

Väitämme, että on olemassa kuntaisomorfismi

$\varphi : \Sigma \to \widetilde{\Sigma}$, jolla

$\varphi|_K = i$ ja

φ kuvaa P:n nollakohdat Σ:ssa $\widetilde{P}$:n nollakohdiksi $\widetilde{\Sigma}$:ssa kertaluvut huomioiden.

Teemme induktion P:n asteen suhteen.

(1) Jos P on 1. astetta, on K tietysti sen sen ainoa hajoituskunta.

(2) Oletamme, että lause on tosi jokaisella asteen enintään n polynomilla. Olkoon P:n aste $n+1$. Asianomaisissa hajoituskunnissa P ja sen vastine $\widetilde{P}$ hajoavat 1. asteen tekijöiksi:

$$P(X) = k(X - \sigma_1) \dots (X - \sigma_{n+1})$$
$$\widetilde{P}(X) = i(k)(X - \widetilde{\sigma}_1) \dots (X - \widetilde{\sigma}_{n+1})$$

Pudottaaksemme P:n astetta induktiota varten huomaamme, että P on jaollinen σ_1:n minimaalipolynomilla P_1, joka minimaalipolynomin määritelmän mukaan on perusmuotoinen, jaoton ja hävittää σ_1:n. Sen isomorfinen vastine $\widetilde{P}_1$ on myös perusmuotoinen ja jaoton, siis nollakohtiensa minimaalipolynomi. Toisaalta $\widetilde{P}_1$ on $\widetilde{P}$:n tekijä, joten sen nollakohdat kunnassa $\widetilde{\Sigma}$ ovat myös $\widetilde{P}$:n nollakohtia ja kuuluvat siis joukkoon $\{\widetilde{\sigma}_1, \dots, \widetilde{\sigma}_{n+1}\}$. Numerointia tarvittaessa muuttaen voimme olettaa, että $\widetilde{P}(\widetilde{\sigma}_1) = 0$, jolloin $\widetilde{P}_1$ on $\widetilde{\sigma}_1$:n minimaalipolynomi. Tilanne on siis sellainen, että meillä on kahdessa kunnassa K ja $\widetilde{K}$ tarkasteltavana isomorfiaa $i : K \to \widetilde{K}$ vaille sama jaoton perusmuotoinen polynomi ja kummassakin siihen liittyvä yksinkertainen algebrallinen laajennus. Tämmöinen laajennus on lauseen 2.8. yleisemmän version mukaan isomorfiaa vaille yksikäsitteinen: on olemassa kuntaisomorfismi

$$\varphi_1 : K(\sigma_1) \to \widetilde{K}(\widetilde{\sigma}_1) \quad \text{siten, että}$$
$$\varphi_1|_K = i : K \to \widetilde{K} \text{ ja}$$
$$\varphi_1(\sigma_1) = \widetilde{\sigma}_1.$$

Nyt $\frac{P}{X-\sigma_1} \in K(\sigma_1)[X]$ on asteen n polynomi ja $\frac{\widetilde{P}}{X-\widetilde{\sigma}_1} \in \widetilde{K}(\widetilde{\sigma}_1)[X]$ on sen isomorfinen vastine isomorfiana φ_1. Induktio-oletuksen nojalla näiden hajoituskunnat — nimittäin Σ ja $\widetilde{\Sigma}$ — ovat isomorfiset halutulla tavalla, eli on olemassa isomorfismi

$$\varphi : \Sigma \to \widetilde{\Sigma} \quad \text{siten, että}$$
$$\varphi|_{K(\sigma_1)} = \varphi_1 \quad \text{ja}$$
$$\varphi(\sigma_j) = \widetilde{\sigma}_j \quad \forall j = 1, \dots, n+1.$$

φ toteuttaa lauseen vaatimukset. $\square$

4.10. Esimerkkejä.

(a) $$K = \mathbf{Q} \text{ ja } P(X) = (X^2 - 3)(X^3 + 1)$$

Konstruoidaan hajoituskunta Σ. Se on helppoa, koska P:llä on $\mathbf{C}$:ssä nollakohdat $\pm\sqrt{3}$ ja -1:n kuutiojuuret $-1, \frac{1+i\sqrt{3}}{2}$ ja $\frac{1-i\sqrt{3}}{2}$. Siis $\Sigma = \mathbf{Q}(\sqrt{3}, -\sqrt{3}, -1, \frac{1+i\sqrt{3}}{2}, \frac{1-i\sqrt{3}}{2}) = \mathbf{Q}(\sqrt{3}, i)$.

(b) $$K = \mathbf{Q},\ P_1(X) = X^2 - 3,\ P_2(X) = X^2 - 2X - 2.$$

P_1:lla ja P_2:lla on sama hajoituskunta $\Sigma = \mathbf{Q}(\sqrt{3})$. Tästä näkee, että eri polynomeilla, jopa jaottomilla, voi olla sama hajoituskunta.

(c) $$K = \mathbf{Z}_2 \text{ ja } P(X) = X^2 + X + 1.$$

Nyt emme voi käyttää $\mathbf{C}$:n algebrallista täydellisyyttä oikotienä hajoituskunnan Σ löytämiseen, vaan joudumme konstruoimaan sen suoraan määritelmän nojalla. Ainakin $\mathbf{Z}_2$:n alkiot, siis 0 ja 1 kuuluvat siihen. Lisäksi on muitakin alkioita, koska P ei hajoa vielä $\mathbf{Z}_2$:ssa, vaan on jopa jaoton. Hajoituskunnassa P:llä on siis ainakin vielä nollakohtansa. Olkoon ζ sellainen. Kunnassa Σ pätee siis

$$0 = P(\zeta) = \zeta^2 + \zeta + 1,$$

ja siis, koska Σ:n karakteristika on 2:

$$\zeta^2 = \zeta + 1.$$

Alkio $\zeta + 1$ ei ole mikään aikaisemmista, koska jokainen yhtälöistä

$$\begin{aligned} \zeta + 1 &= 0 \\ \zeta + 1 &= 1 \text{ ja} \\ \zeta + 1 &= \zeta \end{aligned}$$

johtaa ristiriitaan sen kanssa, että 0, 1 ja ζ ovat eri alkioita. Toisaalta muita Σ:an välttämättä kuuluvia uusia alkioita on vaikea keksiä, ovathan ainakin kaikki ζ:n $\mathbf{Z}_2-$polynomit ilmeisesti joukossa $\{0, 1, \zeta, \zeta + 1\}$ jo mukana. Koetamme, muodostuisiko tästä joukosta haluttu kunta. Laskutoimitukset ovat välttämättä seuraavat:

$+$	0	1	ζ	$\zeta+1$
0	0	1	ζ	$\zeta+1$
1	1	0	$\zeta+1$	ζ
ζ	ζ	$\zeta+1$	0	1
$\zeta+1$	$\zeta+1$	ζ	1	0

$\cdot$	0	1	ζ	$\zeta+1$
0	0	0	0	0
1	0	1	ζ	$\zeta+1$
ζ	0	ζ	$\zeta+1$	1
$\zeta+1$	0	$\zeta+1$	1	ζ

Saatiin todella kuntalaajennus ja P:lle siinä juuret ζ ja $\zeta+1$. Pienin mahdollinen tämä tietysti myös on. $\square$

Normaalit kuntalaajennukset.

4.11. Määritelmä. Kuntalaajennus $L : K$ on *normaali*[18], mikäli jokainen **jaoton** polynomi $P \in K[X]$ joko hajoaa L:ssä tai on siinä nollakohdaton, toisin sanoen L sisältää joko kaikki P:n nollakohdat tai ei ainoatakaan.

4.12. Esimerkkejä. $\mathbf{C} : \mathbf{R}$ on normaali laajennus, mutta $\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}$ ei.

Seuraava lause **samaistaa toisiinsa hajoituskunnan ja normaalin kuntalaajennuksen käsitteet**.

4.13. Lause. *Kuntalaajennukselle $L : K$ seuraavat ovat yhtäpitäviä:*

(1) *$L : K$ on äärellinen ja normaali*
(2) *On olemassa polynomi $P \in K[X]$ siten, että L on sen hajoituskunta.*

Todistus. (1) $\implies$ (2). Olkoon $L : K$ äärellinen ja normaali. Lauseen 2.14. mukaan äärellisyys merkitsee, että

(i) $L : K$ on algebrallinen ja
(ii) $L = K(\alpha_1, \ldots, \alpha_s)$ joillekin äärellisen monelle $\alpha_1, \ldots, \alpha_s \in L$.

Olkoon P_j minimaalipolynomi α_j:lle ja

$$P = P_1 \ldots P_s.$$

Normaaliusoletuksen mukaan kaikki (jaottomat!) P_j:t hajoavat kunnassa L, ja siis myös P hajoaa siinä. Toisaalta $L = K(\alpha_1, \ldots, \alpha_s)$ on varmasti minimaalinen kunta, jossa P hajoaa. Tätä väitettiin.

(2) $\implies$ (1). Olkoon L polynomin P hajoituskunta $K(\sigma_1, \ldots, \sigma_n)$. Lauseen 2.14. mukaan L on äärellinen. Jää todettavaksi normaalius. Normaaliuden määritelmä antaa aiheen ottaa tarkasteltavaksi jaottoman polynomin $Q \in K[X]$, jolla on nollakohta $\alpha \in L$. Se pitää hajoittaa L:ssä. Tietysti Q hajoaa omassa hajoituskunnassaan, mutta tämä ei johda helppoon todistukseen, vaan on sopivampaa tutkiskella polynomin PQ hajoituskuntaa, joka olkoon M.

[18] Muuten *paranormaali*

M sisältää kaikki Q:n nollakohdat ja myös P:n nollakohdat, joten $L \subset M$. Lauseen väitteen todistamiseksi riittää osoittaa, että jokaiselle Q:n nollakohdalle $\beta \in M$ pätee

$$[L(\beta) : L] = [L(\alpha) : L],$$

joka on 1, koska oletimme, että $\alpha \in L$.

Olkoon siis β sellainen. Tutkittavat kunnat ovat toistensa laajennuksia seuraavasti:

$$\begin{array}{ccccc} & K(\alpha) & \subset & L(\alpha) & \\ K & \subset & L & \subset & M \\ & K(\beta) & \subset & L(\beta) & \end{array},$$

joten

$$[L(\alpha) : L][L : K] = [L(\alpha) : K(\alpha)][K(\alpha) : K] \text{ ja}$$
$$[L(\beta) : L][L : K] = [L(\beta) : K(\beta)][K(\beta) : K].$$

Koska yksinkertaisilla laajennuksilla $K(\alpha)$ ja $K(\beta)$ on sama minimaalipolynomi Q, niin $[K(\alpha) : K] = [K(\beta) : K] (= Q$:n aste). Lisäksi $L(\alpha)$ on $K(\alpha)-$polynomin P (näin!) hajoituskunta, samoin $L(\beta)$ $K(\beta)-$polynomin P. Lauseen 2.8. yleisemmän version nojalla kuntalaajennukset $L(\alpha) : K(\alpha)$ ja $L(\beta) : K(\beta)$ ovat isomorfiset. Erityisesti niillä on sama aste.

Sijoittamalla nämä tiedot yllä olevaan yhtälöpariin saadaan

$$[L(\alpha) : L] = [L(\beta) : L],$$

joka oli enää todistettava. □

Separoituvuus.

4.14. Määritelmä. **Jaotonta** polynomia $P \in K[X]$ sanotaan *separoituvaksi,* mikäli sillä ei ole moninkertaisia nollakohtia (isomorfiaa vaille yksikäsitteisessä!) hajoituskunnassaan, eli mikäli $P(X) = k(X-\sigma_1)\dots(X-\sigma_n)$ missä kaikki nollakohdat $\sigma_1, \dots, \sigma_n$ ovat eri alkioita.

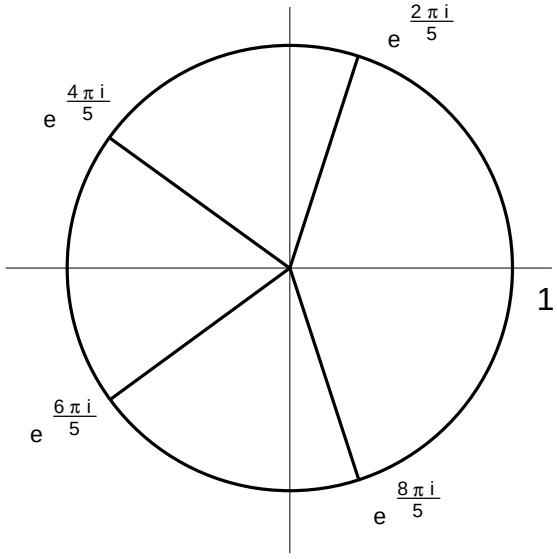
4.15 Esimerkki. (a) Separoituva on esim. $\mathbf{Q}-$polynomi

$$X^4 + X^3 + X^2 + X + 1,$$

sillä se on jaoton ja sen juuret $\mathbf{C}$:ssä ovat

$$e^{\frac{2\pi i}{5}}, e^{\frac{4\pi i}{5}}, e^{\frac{6\pi i}{5}}, \text{ ja } e^{\frac{8\pi i}{5}},$$

jotka ovat eri kompleksilukuja.



(b) Separoitumattoman polynomin tekemisessä on hieman vaivaa. Olkoon p pariton alkuluku ja $K = \mathbf{Z}_p(u)$ transkendenttinen laajennus. $K-$kertoiminen polynomi

$$P(X) = X^p - u$$

osoittautuu separoitumattomaksi. Todistamme tämän. Ensin tarkistetaan eräiden (itse asiassa kaikkien) nollakohtien yhtyminen:

Olkoon σ P:n nollakohta sen hajoituskunnassa Σ. Silloin

$$\begin{aligned} P(\sigma) = \sigma^p - u = 0, \text{ eli} \\ \sigma^p = u. \end{aligned}$$

$$\text{Toisaalta } (X-\sigma)^p = X^p + \binom{p}{1} X^{p-1}(-\sigma) + \cdots + (-\sigma)^p.$$

Koska ensimmäistä ja viimeistä lukuunottamatta binomikertoimet ovat jaollisia p:llä, ja kunnassa $\mathbf{Z}_p(u)$, jonka alkioita ne ovat, on $p = 0$, on

$$\begin{aligned} (X-\sigma)^p = X^p - \sigma^p, \text{ ja siis} \\ (X-\sigma)^p = P(X). \end{aligned}$$

Olkoon α toinen P:n nollakohta. Sijoittamalle α X:n paikalle saadaan

$$(\alpha - \sigma)^p = P(\alpha) = 0,$$

josta seuraa

$$\alpha = \sigma.$$

Kaikki P:n nollakohdat yhtyvät siis ja hajoituskunnassaan P on muotoa

$$P(X) = (X - \sigma)^p.$$

Osoitetaan seuraavaksi, että P on jaoton alkuperäisessä polynomirenkaassa $\mathbf{Z}_p(u)[X]$. Jos ei olisi, niin olisi olemassa $\mathbf{Z}_p(u)-$polynomit Q ja R, joille

$$P = QR$$

ja joiden aste ainakin 1 ja enintään $p-1$. Kunnassa Σ on

$$Q(X)R(X) = P(X) = (X - \sigma)^p.$$

Siksi

$$Q(X) = (X - \sigma)^n, \text{ missä } 1 \leq n \leq p-1.$$

Q:n kertoimet ovat oletuksen mukaan kunnan $\mathbf{Z}_p(u)$ alkioita. Erityisesti siis vakiotermi

$$\sigma^n \in \mathbf{Z}_p(u).$$

Myös itse σ kuuluu samaan kuntaan, sillä alkuluvun p ja sitä pienemmän luonnollisen luvun n suurin yhteinen tekijä on 1, ja on siis olemassa kokonaisluvut a ja b, joille

$$1 = ap + bn, \text{ jolloin}$$
$$\sigma = \sigma^1 = \sigma^{ap+bn} = (\sigma^p)^a(\sigma^n)^b = u^a(\sigma^n)^b \in \mathbf{Z}_p(u).$$

On nyt helppo nähdä, että tämä on mahdotonta, koska P:llä ei ole lainkaan nollakohtia (sitä ainoaa) kerroinkunnassaan, joka u:n transkendenttisuuden takia on

$$\mathbf{Z}_p(u) = \{\frac{A(u)}{B(u)} \mid A \text{ ja } B \text{ polynomeja } \in \mathbf{Z}_p[u], B \neq 0\}.$$

Sellaisellehan olisi voimassa

$$A(u)^p = uB(u)^p,$$

mikä on mahdotonta, koska molemmat puolet ovat u:n polynomeja, vasemmanpuoleisen aste on jaollinen p:llä ja oikeanpuoleisen ei.

Tulemme seuraavassa mm. todistamaan, että kunnassa $\mathbf{C}$ jokainen jaoton polynomi on separoituva. Moninkertaisten nollakohtien tunnistamisessa hyödyllinen apuväline on polynomin (muodollinen) derivaatta:

4.16. Määritelmä. Polynomin

$$P(X) = a_0 + a_1X + \cdots + a_nX^n$$

derivaatta on polynomi

$$\mathcal{D}P(X) = a_1 + 2a_2X + \cdots + na_nX^{n-1}.$$

Vakiopolynomin derivaatta on 0: $D(a) = 0$.

4.17. Huomautus. Ilmeisesti polynomien derivointi toteuttaa differentiaalilaskennasta tutut laskulait — kunnasta riippumatta.

$$\begin{aligned}\mathcal{D}(P+Q) &= \mathcal{D}P + \mathcal{D}Q\\ \mathcal{D}(PQ) &= \mathcal{D}(P)Q + P\mathcal{D}(Q)\end{aligned}$$

Tulon derivointikaava antaa vakiopolynomiin a sovellettuna:

$$\mathcal{D}(aP) = \mathcal{D}(a)P + a\mathcal{D}(P) = a\mathcal{D}(P),$$

joten $\mathcal{D}$ on erityisesti $K-$lineaarikuvaus $K[X] \to K[X]$.

Tavallisesta yhden muuttujan differentiaalilaskennasta tunnemme lauseen, jonka mukaan funktiolla on moninkertainen nollakohta täsmälleen itse funktion ja sen derivaatan yhteisessä nollakohdassa. Muodollisen derivaatan avulla tälle saadaan algebrallinen vastine.

4.18. Lause. *Nollasta eroavalla polynomilla $P \in K[X]$ on moninkertainen nollakohta hajoituskunnassaan Σ jos ja vain jos P:llä ja sen derivaatalla $P' = \mathcal{D}P$ on vakiosta eroava yhteinen tekijä $\in K[X]$.*

Todistus. Oletetaan aluksi, että P:llä on monikertainen nollakohta Σ:ssa:

$$P = (X-\sigma)^2Q(X).$$

$$\begin{aligned}P'(X) &= 2(X-\sigma)(Q(X) + (X-\sigma)^2Q'(X) =\\ &= (X-\sigma)(2Q(X) + (X-\sigma)Q'(X))\end{aligned}$$

Yhteiseksi tekijäksi käy siis $K[X]$:ssa σ:n minimaalipolynomi.

Oletamme seuraavaksi, että P:llä ja sen derivaatalla P' on yhteinen vakiosta eroava tekijä. Todistamme induktiolla P:n asteen n suhteen, että tämä implikoi, että P:llä on moninkertainen nollakohta. Jos $n = 1$, niin implikaatio on triviaalisti voimassa.

Induktioaskel suoritetaan seuraavasti. Yhteisen tekijän nollakohta hajoituskunnassa Σ on myös P:n ja P':n yhteinen nollakohta, olkoon se $\sigma_1 \in \Sigma$. P on $\Sigma[X]$:n alkiona muotoa

$$P(X) = \underbrace{\text{vakio} \cdot (X-\sigma_1)(X-\sigma_2)\dots(X-\sigma_{n-1})}_{\text{Olkoon tm } Q(X)}(X-\sigma_n).$$

Tarkoituksenamme on todistaa, että jokin nollakohdista $\sigma_1, \dots, \sigma_n$ on moninkertainen. Jos näin ei olisi, niin olisi $\sigma_i \neq \sigma_j$ kaikilla $i \neq j$. Derivoimalla saadaan

$$\begin{aligned} P'(X) &= Q'(X)(X-\sigma_n) + Q(X), \text{ eli} \\ Q'(X)(X-\sigma_n) &= P'(X) - Q(X). \end{aligned}$$

Koska σ_1 on P:n ja P':n yhteinen nollakohta, P' on jaollinen $(X-\sigma_1)$:llä, kuten määritelmänsä mukaan myös Q. Tulo $Q'(X)(X-\sigma_n) = P'(X) - Q(X)$ on näin ollen jaollinen $(X-\sigma_1)$:llä. Mutta vastaoletuksen mukaan $\sigma_1 \neq \sigma_n$, joten nimen omaan $Q'(X)$ on jaollinen $(X-\sigma_1)$:llä. Q:lla ja Q':lla on siis yhteinen nollakohta $\sigma_1 \in \Sigma$. $K[X]$:ssa Q ja Q' ovat jaollisia σ_1:n minimaalipolynomilla.

Olemme löytäneet polynomin Q, jolla on — kuten P:llä — yhteinen vakiosta eroava tekijä derivaattansa kanssa, ja toisistaan eroavat nollakohdat $\sigma_1, \dots, \sigma_n \in \Sigma$. Mutta Q on astetta $n-1$. Tämä on induktio-oletuksen vastaista. Lause on todistettu. □

4.19. Lause.

(1) *Kunnassa, jonka karakteristika on 0, jokainen nollasta eroava jaoton polynomi on separoituva.*

(2) *Kunnassa, jonka karakteristika on alkuluku $p \neq 0$, jokainen jaoton polynomi on separoituva,* **paitsi että** täsmälleen muotoa

$$P(X) = a_0 + a_1 X^p + \dots + a_r X^{rp}$$

olevat jaottomat polynomit ovat separoitumattomia.

Todistus. (1) Teemme vastaoletuksen, että jaoton polynomi $P \in K[X]$ on separoitumaton, eli sillä on moninkertainen nollakohta hajoituskunnassaan. Edellisen lauseen mukaan sillä on yhteinen vakiosta eroava tekijä derivaattansa kanssa. Koska P:llä ei jaottomana ole aidosti alempiasteisia vakiosta eroavia tekijöitä, mutta derivaatta on alempiasteinen kuin P itse, on tämä mahdollista vain, mikäli derivaatta on nolla, ts.

$$\begin{aligned} \mathcal{D}P(X) = a_1 + 2a_2 X + \dots + n a_n X^{n-1} &= 0, \text{ eli} \\ j a_j &= 0 \quad \forall\, j = 1, \dots, n. \end{aligned}$$

Karakteristikan ollessa 0 $j \neq 0 \quad \forall j = 1, \ldots, n$, ja siis itse kertoimet $a_1, \ldots, a_n$ häviävät. P on siis vakio, mikä on mahdotonta, koska P:llä on vakiosta eroava tekijä.

(2) Sama päättely toimii karakteristikan p tapauksessa niille kertoimille a_j, joilla j ei ole p:llä jaollinen. Tätä väitetäänkin. □

4.20. Määritelmä. Olkoon $L : K$ kuntalaajennus.

(1) Alkio $\alpha \in L$ on *separoituva*, mikäli se on algebrallinen ja sen minimaalipolynomi on separoituva.
(2) Kuntalaajennus on *separoituva,* mikäli L:n jokainen alkio on separoituva.

Näytämme lopuksi, että laajennuksen separoituvuus periytyy välikuntiin:

4.21. Lause. *Olkoon $L : K$ separoituva laajennus ja M kunta K:n ja L:n välissä. Tällöin laajennukset $M : K$ ja $L : M$ ovat separoituvia.*

Todistus. Voimme olettaa, että

$$K \subset M \subset L.$$

$M : K$ on tietysti separoituva. Olkoon sitten $\alpha \in L$. α:lla on separoituva minimaalipolynomi $P_K \in K[X]$. α:n minimaalipolynomi M:n suhteen, $P_M \in M[X]$ on P_K:n tekijä $M[X]$:ssä. Siksi senkin nollakohdat hajoituskunnassa ovat yksinkertaisia. Tätä väitettiinkin. □

Puolet Galois'n päälauseesta. "$(H^\dagger)^* = H$". Tavoitteena on seuraavassa todistaa, että kun

$$L : K$$

on äärellinen, separoituva, normaali kuntalaajennus ja H sen Galois'n ryhmän $K^* = \Gamma(L : K)$ aliryhmä, niin

$$(H^\dagger)^* = H.$$

Tämä tehdään osoittamalla, että kummassakin on yhtä monta alkiota. Sehän riittääkin, koska jo tiedämme, että $H \subset (H^\dagger)^*$. Osoitamme ensin, että H:n alkioiden lukumäärä $\#H$ on

$$\#H = [L : H^\dagger],$$

ja myöhemmin, että myös

$$\#((H^\dagger)^*) = [L : H^\dagger].$$

Tarvitsemme joitakin apuvälineitä.

4.22. Huomautus. Olkoot L ja K mitä tahansa kuntia. Joukko

$$Kuv(K,L) = \{\alpha : K \to L \,|\, \alpha \text{ on kuvaus } \}$$

on luonnollisella tavalla L-vektoriavaruus. Seuraavassa tarkastelemme sen osajoukkoa (vaan ei aliavaruutta)

$$Mon(K,L) = \{\alpha : K \to L \,|\, \alpha \text{ on kuntahomomorfismi ja injektio } \}$$

Injektiivistä homomorfismia on tapana sanoa *monomorfismiksi.* Siitä lyhenne.

4.23. Lause (Dedekindin lemma). *Olkoot K ja L kuntia ja*

$$\begin{aligned} &\alpha_j \in Mon(K,L) \quad \forall\, j = 1,\dots,n, \\ &\alpha_{j_1} \neq \alpha_{j_2},\ \textit{kun}\ j_1 \neq j_2 \end{aligned}$$

Tällöin $\alpha_1, \dots$ ja α_n ovat $L-$lineaarisesti riippumattomia.

Saman voi ilmaista nykyaikaisemmin sanomalla, että "mikä tahansa joukko eri monomorfismeja $K \to L$ on vapaa".

Todistus. Olkoot $\lambda_1, \dots, \lambda_n \in L$ siten, että

$$\lambda_1\alpha_1 + \cdots + \lambda_n\alpha_n = 0, \quad \text{eli}$$

$$\lambda_1\alpha_1(x) + \cdots + \lambda_n\alpha_n(x) = 0 \quad \forall\, x \in K. \tag{1}$$

Osoitetaan, että kertoimet λ_j ovat nollia. Tehdään vastaoletus, että jokin niistä on nollasta eroava ja että kaavassa (1) esiintyvä n on **pienin positiivinen kokonaisluku, jolla tämä ilmiö voi tapahtua.** Tällainen n on olemassa, koska jokaisessa epätyhjässä luonnollisten lukujen joukossa on pienin luku. Selvästi $n \geq 2$. Tässä minimitilanteessa jokainen λ_j eroaa nollasta. Ristiriidan tuottamiseksi pyrimme muodostamaan häviävän lineaarikombinaation $n-1$:stä monomorfismista $\alpha_2, \dots, \alpha_n$. Koska $\alpha_1 \neq \alpha_n$, on olemassa $y \in K$, jolla $\alpha_1(y) \neq \alpha_n(y)$. Tietysti $y \neq 0$. Sijoitetaan (1):een xy.

$$\lambda_1\alpha_1(xy) + \cdots + \lambda_n\alpha_n(xy) = 0, \text{ eli}$$

$$\lambda_1\alpha_1(x)\alpha_1(y) + \cdots + \lambda_n\alpha_n(x)\alpha_n(y) = 0 \quad \forall\, x \in K.$$

Toisaalta kertomalla (1) $\alpha_1(y)$:llä

$$\lambda_1\alpha_1(x)\alpha_1(y) + \cdots + \lambda_n\alpha_n(x)\alpha_1(y) = 0 \quad \forall\, x \in K.$$

Erotuksena saadaan kaikille $x \in K$

$$\lambda_2(\alpha_2(x)\alpha_1(y) - \alpha_2(x)\alpha_2(y)) + \cdots + \lambda_n(\alpha_n(x)\alpha_1(y) - \alpha_n(x)\alpha_n(y)) = 0,$$
$$\text{eli} \quad \lambda_2(\alpha_1(y) - \alpha_2(y))\alpha_2 + \cdots + \lambda_n(\alpha_1(y) - \alpha_n(y))\alpha_n = 0$$

Tässä häviää $L-$lineaarikombinaatio $n-1$:stä monomorfismista α_j, ja ainakin yksi kertoimista, nimittäin $\lambda_n(\alpha_1(y) - \alpha_n(y))$ on y:n valinnan takia nollasta eroava. Tämä on vastoin n:n määritelmää. $\square$

4.24. Lause (Lineaarialgebraa). *Homogeenisella yhtälöryhmällä*

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= 0 \\ &\cdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n &= 0 \end{aligned}$$

on missä tahansa kunnassa nollasta eroava ratkaisu $(x_1, \ldots, x_n)$, *kun* $n > m$.

Todistus. Lause kuuluu lineaarialgebran alkeisiin. Täydellisyyden vuoksi hahmotellaaan todistus.

On osoitettava, että matriisia (a_{ij}) (esim. standardikannassa) vastaavan lineaarikuvauksen $A : K^n \to K^m$ ydin $Ker(A)$ ei ole pelkkä nolla. Lineaarikuvaukselle A pätee isomorfialause:

$$K^n/Ker(A) \sim Im(A) \subset K^m,$$

joten

$$n - \dim Ker(A) \leq m,$$

jonka oletettiin olevan aidosti alle n. Ytimen dimensio ei siis tosiaankaan ole 0. □

Seuraavassa tarkastelemme Galois'n ryhmän aliryhmiä. Lukijaa kehotetaan verestämään tietojaan äärellisistä ryhmistä sopivaksi katsomallaan tavalla. Joka tapauksessa on hyvä muistaa seuraava periaate, joka seuraa suoraan ryhmän määritelmästä:

4.25. Huomautus. Olkoon G ryhmä ja $h \in G$. Silloin

$$hG = \{hg \,|\, g \in G\} = G,$$

sillä h:lla kertominen on tietysti jopa bijektio ryhmältä itselleen. Jos

$$G = \{g_1, \ldots, g_n\}$$

on äärellinen, ja sen alkioiden lukumäärä eli G:n *kertaluku* on $\#G = n$, niin tämä merkitsee, että

$$hG = \{hg_1, \ldots, hg_n\} = \{g_1, \ldots, g_n\} = G.$$

ja erityisesti # (hG)=# G.

4.26. Lause (Artin; Galois'n päälauseen 1. puoli.). *Olkoon G kunnan K automorfismiryhmän äärellinen aliryhmä ja olkoon $G^\dagger$ sen kiintopistekunta. Tällöin*

$$[K : G^\dagger] = \#G.$$

Todistus. Olkoon $G = \{e = g_1, g_2, \ldots, g_n\}$, $n = \#G$ ja $m = [K : G^\dagger]$.

Osoitetaan aluksi, että $n \leq m$. Tehdään vastaoletus: $n > m$. Erityisesti $m < \infty$. On olemassa $m-$alkioinen kanta $G^\dagger-$vektoriavaruudelle K, olkoon se $(x_1, \ldots, x_m)$. Tämän avulla on mahdollista johtaa sellainen ristiriita Dedekindin lemman kanssa, että $e = g_1, g_2, \ldots$ ja g_n ovat $K-$lineaarisesti riippuvia. Pitää ilmeisesti löytää nollasta eroava $(\lambda_1, \ldots, \lambda_n) \in K^n$ siten, että

$$\lambda_1 g_1(x) + \cdots + \lambda_n g_n(x) = 0 \quad \forall\, x \in K.$$

Koska mikä tahansa $x \in K$ voidaan lausua kannassamme

$$x = \sum_{j=1}^{m} \mu_j x_j, \quad \mu_j \in G^\dagger,$$

niin λ_j:den valinnalla on nollaksi kaikilla $\mu_j \in G^\dagger$ saatava lauseke

$$\begin{aligned}\lambda_1 g_1(x) + \cdots + \lambda_n g_n(x) &= \lambda_1 g_1(\sum_{j=1}^{m} \mu_j x_j) + \cdots + \lambda_n g_n(\sum_{j=1}^{m} \mu_j x_j) = \\ &= \sum_{j,k=1}^{m,n} \lambda_k g_k(\mu_j x_j) = \sum_{j,k=1}^{m,n} \mu_j \lambda_k g_k(x_j) = \\ &= \sum_{j=1}^{m} \mu_j (\lambda_1 g_1(x_j) + \cdots + \lambda_n g_n(x_j)).\end{aligned}$$

Onnistumme jopa valitsemaan $\lambda-$kertoimet siten, että

$$\lambda_1 g_1(x_j) + \cdots + \lambda_n g_n(x_j) = 0 \quad \forall\, j = 0, \ldots, m,$$

sillä lineaarialgebrallisen lauseen 4.24. mukaan on olemassa $\lambda = (\lambda_1, \ldots, \lambda_n) \neq 0 \in K^n$ siten, että

$$\begin{aligned} g_1(x_1)\lambda_1 + \cdots + g_n(x_1)\lambda_n &= 0, \\ &\cdots \\ g_1(x_m)\lambda_1 + \cdots + g_n(x_m)\lambda_n &= 0. \end{aligned}$$

mitä juuri tarvitaankin.

Todistuksen toisena puolena osoitetaan, että myös $n \geq m$. Vastaoletus on nyt: $n < m = [K : G^\dagger]$. Tällä kertaa on siis olemassa $G^\dagger-$lineaarisesti riippumattomat

$$x_1, \ldots, x_{n+1} \in K.$$

Lineaarialgebrallisen lemman 4.24. mukaan on nyt olemassa

$$\lambda_1, \ldots, \lambda_{n+1} \in K$$

siten, että jokin niistä eroaa nollasta ja

$$\begin{aligned} g_1(x_1)\lambda_1 + \cdots + g_1(x_{n+1})\lambda_{n+1} &= 0, \\ &\cdots \\ g_n(x_1)\lambda_1 + \cdots + g_n(x_{n+1})\lambda_{n+1} &= 0. \end{aligned}$$

g_j käy tässä läpi koko ryhmän G. Voimme olettaa, että kertoimet λ_j on valittu siten, että **mahdollisimman moni niistä on nolla**. Indeksien numerointi olkoon tehty siten, että aluksi tulevat nollasta eroavat λ_j:t, siis

$$\begin{aligned} &\lambda_1, \ldots, \lambda_r \neq 0, \text{ ja} \\ &\lambda_{r+1}, \ldots, \lambda_{n+1} = 0, \text{ jolloin yhtälöryhmä on} \\ (*) \qquad &g_j(x_1)\lambda_1 + \cdots + g_j(x_r)\lambda_r = 0 \in K \quad \forall j = 1, \ldots, n. \end{aligned}$$

Kuten Dedekindin lemman todistuksessa yritetään taas tuottaa $(*)$:stä samanlainen kaava, jossa on vähemmän termejä. Sitä varten valitaan mielivaltainen automorfismi $g \in G$ ja operoidaan sillä $(*)$:een

$$\begin{aligned} g(g_j(x_1)\lambda_1 + \cdots + g_j(x_r)\lambda_r) &= g(0) = 0 \\ gg_j(x_1)g(\lambda_1) + \cdots + gg_j(x_r)g(\lambda_r) &= 0 \quad \forall j = 1, \ldots n \\ (**) \qquad g_j(x_1)g(\lambda_1) + \cdots + g_j(x_r)g(\lambda_r) &= 0 \quad \forall j = 1, \ldots n. \end{aligned}$$

Jälkimmäinen johtopäätös perustuu siihen, että huomautuksen 4.25. mukaan gg_j käy läpi koko ryhmän G, kun g_j tekee niin. Kaksi alinta riviä ovat siten sama yhtälöryhmä. Kertomalla $(*)$ $g(\lambda_1)$:llä ja $(**)$ λ_1:llä ja vähentämällä ne toisistaan saadaan ensimmäiset termit kumoutumaan ja jää:

$$g_j(x_2)(\lambda_2 g(\lambda_1) - g(\lambda_2)\lambda_1) + \cdots + g_j(x_r)(\lambda_r g(\lambda_1) - g(\lambda_r)\lambda_1) = 0,$$

joka on kaavan $(*)$ kaltainen yhtälöryhmä, mutta sisältää vähemmän termejä kussakin yhtälössä. Koska $(*)$:n termien määrä on minimaalinen, on oltava

$$\lambda_i g(\lambda_1) - \lambda_1 g(\lambda_i)) = 0 \quad \forall i = 2, \ldots, r \text{ jokaisella } g \in G.$$

Tällöin

$$\begin{aligned} \lambda_i g(\lambda_1) &= \lambda_1 g(\lambda_i) \quad \text{, ja siis} \\ \lambda_i \lambda_1^{-1} &= g(\lambda_i \lambda_1^{-1}) \quad \forall i = 2, \ldots, r. \end{aligned}$$

Mutta koska näin käy kaikilla $g \in G$, niin tämä merkitsee, että

$$\begin{aligned} \lambda_i \lambda_1^{-1} &\in G^\dagger \quad \text{eli} \\ \lambda_i &= \underbrace{(\lambda_i \lambda_1^{-1})}_{z_i \in G^\dagger} \lambda_1 \quad \forall i = 2, \ldots, r. \end{aligned}$$

Yhtälöryhmän $(*)$ ensimmäiseen (ts. $j = 1$, muistaen, että g_1 on neutraalialkio) yhtälöön sijoitettuna tämä antaa

$$x_1 \lambda_1 z_1 + \cdots + x_r \lambda_1 z_r = 0.$$

Jaamme puolittain λ_1:llä, joka ei ole 0, ja huomaamme että $x_1, \ldots$ ja x_r ovat lineaarisesti $G^\dagger-$riippuvat, samoin siis $x_1, \ldots$ ja x_n. Näin ei voi olla, koska ne muodostavat kannan. Todistus on valmis. $\square$

4.27. Lause. *Äärellisen kuntalaajennuksen $L : K$ Galois'n ryhmän äärelliselle aliryhmälle $H \subset \Gamma(L : K)$ pätee:*

$$[H^\dagger : K] = \frac{[L : K]}{\#H}.$$

Todistus.

$$[H^\dagger : K] = \frac{[L : K]}{[L : H^\dagger]} = \frac{[L : K]}{\#H}. \quad \square$$

4.28. Esimerkki. (a) Muistetaan, että $\mathbf{C}$:n $\mathbf{R}-$automorfismien ryhmä $G = \Gamma(\mathbf{C} : \mathbf{R})$ on 2-alkioinen jäseninään identtinen kuvaus ja kompleksikonjugointi. Tässä kiintopistekunta $G^\dagger$ on $\mathbf{R}$. $\mathbf{C}$ on todella 2-ulotteinen $\mathbf{R}-$vektoriavaruus.

(b) Olkoon $\omega = e^{\frac{2\pi i}{5}}$ ja $K = \mathbf{Q}(\omega)$. Ilmeisesti $\omega^5 = 1$ ja

$$\mathbf{Q}(\omega) = \{p + q\omega + r\omega^2 + s\omega^3 + t\omega^4 \,|\, p, q, r, s, t \in \mathbf{Q}\}. \tag{1}$$

Määrätään $\Gamma(\mathbf{Q}(\omega) : \mathbf{Q})$. Galois'n ryhmä muodostuu kaikista $\mathbf{Q}(\omega)$:n $\mathbf{Q}-$automorfismeista α. α:n vaikutus rationaalilukuihin tiedetään. Sen vaikutus ω:aan voidaan päätellä siitä, että

$$\alpha(\omega)^5 = \alpha(\omega^5) = \alpha(1) = 1.$$

$\alpha(\omega)$ on siis jokin ykkösen viidensistä kompleksisista juurista, jotka ovat $1, \omega, \omega^2, \omega^3$ ja ω^4. Ykkönen itse ei tule kysymykseen, koska α on isomorfismina injektio. Jää 4 vaihtoehtoa. On helppo todeta, että ne kaikki todella johtavat $Q-$automorfismeihin ja siis tässä $\#G = 4$. Todistamamme lauseen mukaan on siis kuntalaajennuksemme aste myös 4, eikä 5, niinkuin kaavaa (1) äkkisiltään silmäilemällä voisi luulla. Asia näyttää vielä pahemmalta, jos huomaa, että ω on polynomin $X^5 - 1$ nollakohta ja muistelee lisää unohtamiaan lauseita. Iloksemme voimme kuitenkin todeta, että tämä $X^5 - 1$ ei ole ω:n minimaalipolynomi, vaan jaollinen $\mathbf{Q}$:ssa. Minimaalipolynomi on $X^4 + X^3 + X^2 + X + 1$, siis astetta 4, kuten kuuluu. Kaavan (1) vektorit $1, \omega, \omega^2, \omega^3$ ja ω^4 ovat siis nähtävästi $\mathbf{Q}-$lineaarisesti riippuvia! Totta kai ovatkin; niiden summa on 0.

$K-$monomorfismit.

4.29. Määritelmä. Olkoon K kuntien L ja M yhteinen alikunta. Kuntahomomorfismia

$$\phi : M \to L$$

sanotaan *$K-$monomorfismiksi*, jos se on injektio ja jos

$$\phi(k) = k \quad \forall k \in K.$$

4.30. Huomautus. Erityisesti, kun $K \subset M \subset L$ ovat toistensa alikuntia, niin jokaisen $K-$automorfismin $L \to L$ rajoittuma M:ään on $K-$monomorfismi $M \to L$. Onko olemassa muitakin? Riittävän ehdon niiden puuttumiselle antaa seuraava lause.

4.31. Lause. *Olkoon $L : K$ äärellinen, normaali kuntalaajennus ja $K \subset M \subset L$ toistensa alikuntia. Silloin jokainen $K-$monomorfismi $M \to L$ on jonkin $K-$automorfismin $L \to L$ rajoittuma M:ään.*

Todistus. Olkoon

$$\alpha : M \to L$$

$K-$monomorfismi. Se on kuntaisomorfismi

$$\alpha : M \to \alpha(M) \quad \subset L.$$

Ideana on käyttää hajoituskunnan yksikäsitteisyyslausetta 4.9. — isomorfismiversionaan — α:n jatkamiseen isomorfismiksi $\beta : L \to L$. Jotta tämä onnistuisi, pitäisi L:n olla jonkin $M-$polynomin hajoituskunta ja samalla myös sitä isomorfismissa α vastaavan $\alpha(M)-$polynomin hajoituskunta. Tällainen polynomi onkin tarjolla, sillä olemme olettaneet, että L on K:n äärellinen, normaali laajennus ja sellainen on lauseen 4.13. mukaan nimen omaan jonkin $K-$polynomin P hajoituskunta. Koska $K \subset M$, niin P on myös $M-$polynomi ja L on siis $M-$polynomin P hajoituskunta. Isomorfismissa $\alpha : M \to \alpha(M)$ P:tä vastaa se itse, koska P:n kertoimet ovat K:n alkioita ja $\alpha(k) = k$ $\forall k \in K$. Yksikäsitteisyyslauseen ehdot ovat siis voimassa, ja on olemassa isomorfismi $\beta : L \to L$, eli L:n automorfismi, jonka rajoittuma todellakin on

$$\beta|_M = \alpha.$$

Tällaista haluttiin. □

4.32. Lause (Konstruktioperiaate). *Olkoon kuntalaajennus $L{:}K$ äärellinen ja normaali. Olkoon $P \in K[X]$ jaoton polynomi ja α ja β sen nollakohtia L:ssä. Silloin on olemassa L:n $K-$automorfismi σ, jolle $\sigma(\alpha) = \beta$.*

Todistus. Koska α:lla ja β:lla on sama minimaalipolynomi P, niin ne adjungoimalla saadaan K:sta lauseen 2.8. mukaan isomorfiset laajennukset, eli on olemassa isomorfismi

$$i : K(\alpha) \to K(\beta),$$

jolle $i(\alpha) = (\beta)$ ja $i|_K = id_K$. Tulkittuna kuvaukseksi $K(\alpha) \to L$ i on $K-$monomorfismi ja sille on siis edellisen lauseen mukaan olemassa halutunlainen jatko. □

Normaali sulkeuma. Paranormaali laajennus on siitä huono, että se ei sisällä "riittävästi nollakohtia". Asiaa voi yrittää korjata suurentamalla sitä.

4.33. Määritelmä. Olkoon $L : K$ algebrallinen kuntalaajennus. Sen *normaali sulkeuma* on L:n laajennus N, jolle:

(1) $N : K$ on normaali

(2) $L \subset M \subset N$, ja $M : K$ normaali $\implies M = N$.

L:n normaali sulkeuma on siis minimaalinen K:n normaali laajennus, joka sisältää L:n.

4.34. Lause. *Olkoon $L : K$ äärellinen kuntalaajennus. On olemassa isomorfiaa vaille tasan yksi L:n normaali sulkeuma. Se on K:n äärellinen laajennus.*

Todistus. **Olemassaolo**: Olkoon $\{x_1, \ldots, x_n\}$ L:n kanta. Osoitetaan, että etsityksi normaaliksi laajennukseksi kelpaa alkioiden $x_1, \ldots, x_n \in L$ minimaalipolynomien tulon

$$P = P_{x_1} \ldots P_{x_n} \in K[X] \quad \text{tässä nimen omaan } K[X]$$

hajoituskunta N. Tarkistetaan, että tulos on saatu:

(1) $K \subset L \subset N$ ovat toistensa alikuntia.

(2) Laajennus $N : K$ on normaali ja äärellinen, koska N on P:n hajoituskunta myös, kun P tulkitaan $K-$polynomiksi (selvästi P hajoaa siinä ja toisaalta jokainen kunta, joka sisältää K:n ja P:n nollakohdat sisältää alkiot $x_1, \ldots, x_n$ ja siis niiden virittämän $K-$vektoriavauuden L.) ja lause 4.13. sanoo, että juuri tämä takaa kuntalaajennuksen normaaliuden ja äärellisyyden.

(3) N on myös minimaalinen. Olkoon nimittäin

$$L \subset M \subset N,$$

missä myös M on K:n normaali laajennus. Silloin em. minimaalipolynomien $P_{x_1}, \ldots, P_{x_n}$ nollakohdat $x_1, \ldots, x_n$ kuuluvat L:ään ja siis myös M:ään, joka oletettiin K:n normaaliksi laajennukseksi. Koska minimaalipolynomit ovat $K-$kertoimisia ja laajennus $M : K$ on normaali, ne hajoavat M:ssä, ja siis koko P hajoaa M:ssä. Mutta N on P:n hajoituskunta. Siis $M = N$.

Yksikäsitteisyys: Olkoot M ja N kumpikin $L : K$:n normaaleja sulkeumia. Silloin kumpikin niistä sisältää em. polynomin P hajoituskunnan, olkoot ne Σ ja Ξ. Mutta Σ ja Ξ ovat edellisen konstruktion nojalla $L : K$:n normaaleja sulkeumia, sitäpaitsi saman polynomin hajoituskuntina keskenään isomorfisia ja sisältävät L:n. Normaalin sulkeuman minimaalisuuden nojalla ne yhtyvät M:ään ja N:ään. □

4.35. Esimerkki. Esimerkissä 4.2. määrättiin Galois'n ryhmä

$$\Gamma(\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}),$$

joka osoittautui yksialkioiseksi, vaikka kuntalaajennuksen $\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}$ aste on 3. Tämä laajennus ei toisaalta selvästikään ole normaali. Normaali sulkeuma saadaan lauseen 4.34. todistuksen mukaisesti $\mathbf{Q}(\sqrt[3]{2})$:n-kanta-alkioiden minimaalipolynomeista. Kannaksi käy esim. $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\}$.

Kanta-alkioilla on minimaalipolynomit $X-1$, $P(X)=X^3-2$ ja $R(X)=X^3-4$. Normaali sulkeuma on niiden tulon hajoituskunta, siis $\mathbf{Q}(\sqrt[3]{2},\ \omega(\sqrt[3]{2}),\ \omega^2(\sqrt[3]{2}\ ))=\mathbf{Q}(\sqrt[3]{2},\ \omega)$, missä $\omega=e^{\frac{2\pi i}{3}}$ on ykkösen kompleksinen kuutiojuuri.

4.36. Lemma. *Olkoot*

$$K\subset L\subset N\subset M$$

toistensa alikuntia siten, että $N:K$ on äärellisen algebrallisen laajennuksen $L:K$ normaali sulkeuma.

Olkoon lisäksi

$$\alpha:L\to M$$

$K-$monomorfismi. Silloin $\alpha(L)\subset N$.

Todistus. Olkoon $x\in L$ ja $P\in K[X]$ sen minimaalipolynomi.

$$0=P(x)=\alpha(P(x))=P(\alpha(x)),$$

ja siis myös $\alpha(x)$ on P:n nollakohta. Sellaiset kuuluvat kaikki normaaliin sulkeumaan N. □

4.37. Lause (Normaaliuden karakterisointi). *Olkoon $L:K$ äärellinen kuntalaajennus. Seuraavat ovat yhtäpitäviä:*

(1) *$L:K$ on normaali*
(2) *K:lla on olemassa normaali laajennus $N\supset L$, jolla jokainen $K-$monomorfismi*

$$\alpha:L\to N$$

on L:n $K-$automorfismi.
(3) *kaikilla K:n normaaleilla laajennuksilla M, joilla $M\supset L$, jokainen $K-$monomorfismi*

$$\alpha:L\to M$$

on L:n $K-$automorfismi.

Todistus.

(1) $\Longrightarrow$ (3). Olkoon $L:K$ normaali laajennus. Lemma 4.36. sovellettuna tilanteeseen $K\subset L\subset L\subset M$ sanoo, että $\alpha(L)\subset L$. Toisaalta α on $K-$monomorfismina $K-$lineaarikuvaus äärellisulotteiselta $K-$vektoriavaruudelta L itselleen ja sitä paitsi injektio. Se on siis bijektiokin.

(3) $\Longrightarrow$ (2). Selvä. Huomaa, että tarvitaan sentään tietoa, että normaali laajennus $N \supset L$ on olemassa. Sen takaa lause 4.34.

(2) $\Longrightarrow$ (1). Olkoon

$$K \subset L \subset N,$$

kuten (2):ssa vaaditaan, ja olkoon $P \in K[X]$ jaoton polynomi, jolla on nollakohta $x \in L$. Normaalissa laajennuksessa N se hajoaa. Olkoon $y \in N$ sen nollakohta. Konstruktioperiaatteen 4.32. mukaan on olemassa $K-$automorfismi $\sigma : N \to N$, jolle $\sigma(x) = y$. Kohdan (2) mukaan σ:n rajoittuma L:ään on L:n $K-$automorfismi. Siis $y \in L$. $\square$

Toinen puolisko Galois'n päälauseesta. "$(K^*)^\dagger = K$".

4.38. Lause. *Olkoon $L : K$ äärellinen, astetta n oleva separoituva kuntalaajennus ja $N \supset L$ K:n normaali laajennus, esimerkiksi $L : K$:n normaali sulkeuma.*

Silloin on olemassa täsmälleen $n = [L : K]$ eri $K-$monomorfismia $L \to N$.

Todistus. Tehdään induktio asteen $[L : K]$ suhteen. Tapaus $[L : K] = 1$ on triviaali, onhan identtinen kuvaus ainoa $K-$monomorfismi $K \to K$. Induktio-oletamme, että lause pätee kaikille kuntalaajennuksille, joiden aste on enintään n, ja että $[L : K] = n+1$. Asteen alentamiseksi valitaan jokin $\alpha \in L \setminus K$. α:n minimaalipolynomi P on jaoton ja oletuksen mukaan myös separoituva, joten sillä on N:ssä asteensa r määrä eri nollakohtia

$$\alpha = \alpha_1, \ldots, \alpha_r.$$

Induktio-oletus tepsii nyt kuntalaajennuksiin $K(\alpha) \subset L \subset N$. $K(\alpha)-$monomorfismeja $L \to N$ on olemassa tasan $[L : K(\alpha)]$ kappaletta, eli niiden lukumäärä s on

$$[L : K(\alpha)] = \frac{[L : K]}{[K(\alpha) : K]} = \frac{n+1}{r}.$$

Olkoot ne vaikkapa

$$\varphi_1, \varphi_2, \ldots, \varphi_s : L \to N.$$

Ainakin nämä ovat hakemiamme $K-$monomorfismeja, mutta lisäksi voi olla olemassa sellaisiakin, jotka eivät ole $K(\alpha)$:ssa identtisiä kuvauksia. K:n alkioiden tulee toki kuvautua itselleen, mutta α voi periaatteessa $K-$monomorfismissa kuvautua muuksikin kuin itsekseen, nimittäin **joksikin muuksi P:n nollakohdista** $\alpha = \alpha_1, \ldots, \alpha_r$. Tällaisia $K-$monomorfismeja voi kullekin α_j konstruoida. Konstruktioperiaatteen 4.32. mukaan on nimittäin olemassa $K-$automorfismit

$$\sigma_1, \ldots, \sigma_r : N \to N,$$

joille

$$\sigma_j(\alpha) = \alpha_j.$$

Kuvaukset

$$\psi_{ij} = \sigma_j \varphi_i : L \to N$$

ovat selvästi eri $K-$monomorfismeja. Koska niiden lukumäärä on $rs = n + 1$, riittää osoittaa, että muita ei ole. Tämä onkin suoraviivaista. Olkoon ψ $K-$automorfismi $L \to N$. Silloin $\psi(\alpha)$ on P:n nollakohta ja siis jokin α_j. Kuvaus

$$\varphi = \sigma_j^{-1} \psi$$

on $K(\alpha)-$monomorfismi $L \to N$ ja siis jokin φ_i. Näin ollen

$$\psi = \sigma_j \varphi_i,$$

kuten väitettiinkin. □

4.39. Lause. *Olkoon $L : K$ äärellinen, separoituva normaali kuntalaajennus. Tällöin*

$$\#\Gamma(L : K) = [L : K].$$

Todistus. Edellisen lauseen mukaan on olemassa tasan $[L : K]$ kappaletta $K-$monomorfismeja $L \to L$. Lause 4.37. osoittaa, että ne ovat automorfismeja. □

4.40. Lause (Galois'n päälauseen 2. puoli). *Olkoon $L : K$ äärellinen, separoituva normaali kuntalaajennus. Silloin K on Galois'n ryhmän $\Gamma(L : K)$ kiintopistekunta, eli*

$$(K^*)^\dagger = K.$$

Todistus. Olkoon K_0 Galois'n ryhmän $\Gamma(L : K)$ kiintopistekunta. Silloin

$$\begin{aligned} K \subset K_0. &\quad \text{(Lause 4.6.(2))} \\ [L : K_0] = \#\Gamma(L : K) &\text{ (Lause 4.26.)} \\ [L : K] = \#\Gamma(L : K) &\text{ (Lause 4.39.)} \\ [K_0 : K] = \frac{[L : K]}{[L : K_0]} &= 1 \end{aligned}$$

□

Normaalius ja separoituvuus eivät ole pelkkiä teknisiä oletuksia, vaan tarpeellisia, jotta edellinen lause pätisi.

4.41. Lause (Ehtojen välttämättömyys). *Olkoon $L : K$ äärellinen kuntalaajennus, jolle on voimassa edellisen lauseen johtopäätös:*

$$K = \Gamma(L : K)^{\dagger}.$$

Silloin ovat voimassa myös edellisen lauseen oletukset: $L : K$ on normaali ja separoituva.

Todistus. Merkitään $n = \#\Gamma(L : K)$. Tämä on äärellinen seuraavan lemman 4.42. mukaan. On siis olemassa ainakin n $K-$monomorfismia $L \to L$, nimittäin $K-$automorfismit. Toisaalta on helppo todeta — ja todistetaan seuravana lemmana — että niitä on enintään n kappaletta, ja **separoitumattomassa tapauksessa aidosti vähemmän**. Toisaalta $n = [L : K]$, sillä Lause 4.27. ei edellytä separoituvuutta eikä normaaliutta, mutta antaa kuitenkin tämän tiedon. Separoitumattomuus on siis mahdotonta.

Myös normaaliustodistus perustuu samaan lemmaan. Osoitamme, että $L : K$ toteuttaa normaaliuden takaavan lauseen 4.37. ehdon (3). Olkoon $M \supset L$ K:n normaali laajennus ja

$$\alpha : L \to M$$

$K-$monomorfismi. Galois'n ryhmän alkiot eli L:n $K-$automorfismit ovat myös $K-$monomorfismeja $L \to M$, ja niitä on n kappaletta. Seuraavan lemman mukaan muita ei ole, vaan α on jokin niistä, siis L:n automorfismi, kuten pitääkin. □

4.42. Lemma. *Olkoot*

$$K \subset L \subset M$$

toistensa alikuntia, $M : K$ äärellinen ja $[L : K] = n$.

Tällöin on olemassa korkeintaan n $K-$monomorfismia $L \to M$. Jos $L : K$ ei ole separoituva, niin niitä on aidosti vähemmän.

Todistus. Käsitellään ensin tapaus, jossa M on K:n normaali laajennus. Tällöin voimme nimittäin jäljitellä lauseen 4.38. todistusta. Separoituvuudesta luopuminen aiheuttaa vain sen, että haettujen $K-$monomorfismien määrä kasvaa kussakin induktioaskelessa korkeintaan $m-$kertaiseksi, missä m on alkion α minimaalipolynomin **eri** nollakohtien lukumäärä sen hajoituskunnassa ja siis enintään, mutta ei välttämättä tasan sen aste. Jos $L : K$ ei ole separoituva, niin jollakin $\alpha \in L \setminus K$ niitä on aidosti vähemmän.

Yleinen tapaus palautuu jo käsiteltyyn huomaamalla, että M voidaan korvata normaalilla sulkeumallaan N, koska sekin on OY-lauseen 4.34. mukaan äärellinen ja koska jokainen $K-$monomorfismi $L \to M$ sitä suuremmalla syyllä on $K-$monomorfismi $L \to N$. □

Galois'n päälause.

4.43. Lause (Galois'n pää-). *Olkoon kuntalaajennus $L : K$ äärellinen, separoituva ja normaali. Merkitään*

$$\begin{aligned} G &= K^* = \Gamma(L : K) \\ n &= [L : K] \\ \mathcal{G} &= \{H \mid H \text{ on } G\text{:n aliryhmä } \} \\ \mathcal{F} &= \{M \mid K \subset M \subset L \text{ ovat toistensa alikuntia } \} \end{aligned}$$

Seuraavat väitteet ovat tosia:

(1) $\#G{=}n$
(2) *Kuvaukset* $* : \mathcal{F} \to \mathcal{G}$ *ja* $^\dagger : \mathcal{G} \to \mathcal{F}$ *ovat toistensa käänteiskuvauksia.*
(3) $\forall M \in \mathcal{F}$*:*

$$[L : M] = \#M^*$$
$$[M : K] = \frac{\#G}{\#M^*}$$

(4) *Kunta* $M \in \mathcal{F}$ *on* K*:n normaali laajennus aina ja vain, kun* M^* *on* G*:n normaali aliryhmä.*
(5) *Kun kunta* $M \in \mathcal{F}$ *on* K*:n normaali laajennus, niin Galois'n ryhmä* $\Gamma(M : K)$ *ja tekijäryhmä* $\frac{G}{M^*} = \frac{\Gamma(L:K)}{\Gamma(L:M)}$ *ovat isomorfiset.*

Todistus.

(1) on lause 4.39.

(2) seuraa kaikesta tähänastisesta yhdistelemällä näin: Olkoon ensin $M \in \mathcal{F}$. Lauseen 4.40. mukaan

$$M^{*\dagger} = M,$$

kunhan $L : M$ on äärellinen, normaali ja separoituva. Nämä asiat olemme olettaneet laajennuksesta $L : K$, mutta äärellisyys ja lauseen 4.21 mukaan myös separoituvuus periytyvät $L : M$:lle, joka on normaaliuden ensimmäisen karakterisoinnin 4.13. mukaan myös normaali, onhan L jonkin $K-$polynomin ja siis myös $M-$polynomin hajoituskunta.

Olkoon sitten $H \in \mathcal{G}$. Ainakin $H \subset H^{\dagger *}$, tämä helppo puolihan selvitettiin lauseessa 4.6. Lisäksi voimme soveltaa edellistä tulosta kuntaan $H^\dagger$, jolloin saamme

$$H^{\dagger *\dagger} = H^\dagger.$$

Artinin lauseen 4.26. mukaan siis

$$\#H = [L : H^\dagger] = [L : H^{\dagger *\dagger}] = \#H^{\dagger *}.$$

Siinäpä se!

(3) seuraa – kuten (1) – siitä, että myös $[L : M]$ on äärellinen, separoituva ja normaali. Lauseen 4.39. mukaan nimittäin tällöin

$$\#\Gamma(L : M) = [L : M],$$

kuten väitetäänkin. Väitteen jälkimmäinen yhtälö merkitsee tämän huomioiden, että

$$[M : K][L : M] = \#G,$$

joka on väite (1). Huomaa muuten, että kun M^* on G:n normaali aliryhmä, niin

$$\frac{\#G}{\#M^*} = \#(\frac{G}{M^*}) = \ M^*\text{:n } \textit{indeksi } G\text{:n suhteen.}$$

(4) ja (5) edellyttävät vielä pientä lemmaa:

4.44. Lemma. *Olkoon $L : K$ äärellinen, separoituva ja normaali kuntalaajennus ja*

$$K \subset M \subset L$$

toistensa alikuntia sekä $\varphi \in \Gamma(L : K) = K^*$. Pätee

$$(\varphi(M))^* = \varphi M^* \varphi^{-1}.$$

Todistus. Tämä seuraa suoraan määritelmistä. L:n automorfismi α kuuluu joukkoon $\varphi M^* \varphi^{-1}$ täsmälleen silloin, kun

$$\begin{aligned} \exists \beta \in M^* : \quad & \alpha = \varphi\beta\varphi^{-1}, \\ \text{eli} \quad & \varphi^{-1}\alpha\varphi = \beta \in M^*, \\ \text{eli} \quad & \varphi^{-1}\alpha\varphi(x) = x \quad \forall x \in M. \end{aligned}$$

Toisaalta myös ehto $\alpha \in (\varphi(M))^*$ merkitsee, että

$$\begin{aligned} & \alpha\varphi(x) = \varphi(x) \quad \forall x \in M, \\ \text{eli} \quad & \varphi^{-1}\alpha\varphi(x) = x \quad \forall x \in M. \end{aligned}$$

□

Päälauseen todistuksen loppuosa. Muistetaan väitteet:

(4) Kunta $M \in \mathcal{F}$ on K:n normaali laajennus aina ja vain, kun M^* on G:n normaali aliryhmä.

(5) Kun näin käy, niin Galois'n ryhmä $\Gamma(M : K)$ ja tekijäryhmä $\frac{G}{M^*}$ ovat isomorfiset.

Todistaaksemme kohdan (4) oletamme aluksi, että $M : K$ on normaali laajennus. On osoitettava, että $\varphi M^* \varphi^{-1} = M^*$ kaikille $\varphi \in G$. Olkoon siis φ L:n $K-$automorfismi. Edellisen lemman mukaan

$$\varphi M^* \varphi^{-1} = (\varphi(M))^*,$$

joten riittää todistaa, että $\varphi(M) = M$. Tämä taas on normaaliuden karakterisoinnin 4.37.(3) mukaan selvää, onhan rajoittuma

$$\varphi|_M : M \to L$$

$K-$monomorfismi.

Toisen puolen todistamiseksi oletetaan, että M^* on normaali aliryhmä Galois'n ryhmässä $G = \Gamma(L : K)$. Käytetään nyt karakterisointia 4.37.(2) kuntalaajennuksen $M : K$ normaaliuden testaamiseen. Otetaan siis $K-$monomorfismi $\sigma : M \to L$. Koska $L : K$ on oletuksen mukaan äärellinen ja normaali, niin lause 4.31. takaa, että σ on jonkin $K-$automorfismin $\tau : L \to L$ rajoittuma. M^* on normaali aliryhmä, joten edellisen lemman nojalla

$$(\tau(M))^* = \tau M^* \tau^{-1} = M^*,$$

mistä kohdan (2) nojalla seuraa $\tau M = M$, eli $\sigma M = M$.

Lopuksi todistetaan kohta (5). Olkoon todella M^* normaali aliryhmä, jolloin on ainakin olemassa tekijäryhmä $\frac{G}{M^*}$. Ryhdytään sitten tarkastelemaan väitetyn isomorfian toista osapuolta, joka on Galois'n ryhmä $\Gamma(M : K)$. Keksitään aluksi homomorfismi

$$h : G \to \Gamma(M : K) : \quad \varphi \mapsto \varphi|_M.$$

Tämä on todella kuvaus asianomaisten joukkojen välillä, sillä $L : K$ on normaali ja $\varphi|_M$ siis jälleen karakterisoinnin 4.37. mukaan M:n automorfismi. Ryhmähomomorfisuus on ilmeinen asia. Ryhmien homomorfismilauseen mukaan h:n kuvaryhmä $h(G)$ ja $\frac{G}{Ker(h)}$ ovat isomorfiset. Riittää siis osoittaa, että h on surjektio ja huomata, että ydin on M^*. Lause 4.31. varmistaa surjektiivisuuden ja viimeistelee todistuksen. □

Malliesimerkki.

4.45. Esimerkki. Olkoon

$$P(X) = X^4 - 2 \in \mathbf{Q}[X].$$

Merkitään $\omega = \sqrt[4]{2} > 0$.

(1) Määrätään P:n hajoituskunta: Juuret $\mathbf{C}$:ssä ovat $\pm\omega$ ja $\pm i\omega$:

$$P(X) = (X - \omega)(X + \omega)(X - i\omega)(X + i\omega).$$

Hajoituskunnaksi kelpaa siis $K = \mathbf{Q}(\omega, i)$. Lauseiden 4.13. ja 4.19. mukaan kuntalaajennus $K : \mathbf{Q}$ on äärellinen, normaali ja separoituva.

(2) Määrätään aste

$$[K : \mathbf{Q}] = [\mathbf{Q}(\omega, i) : \mathbf{Q}(\omega)][\mathbf{Q}(\omega) : \mathbf{Q}].$$

i:n minimaalipolynomi on $X^2+1 \in \mathbf{Q}(\omega)[X]$. ω:n minimaalipolynomi on alkuperäinen $P(X) \in \mathbf{Q}[X]$, sillä P on todella $\mathbf{Q}$:ssa jaoton. (Käytä Eisensteinin ehtoa tai muodosta parittain tuloja P:n 1. asteen tekijöistä.) Etsitty aste on siis 8.

(3) Määrätään Galois'n ryhmä $\Gamma[K : \mathbf{Q}]$. K:n $\mathbf{Q}-$automorfismeissa voivat em. polynomin P juuret kuvautua vain permutoitumalla toisikseen, erityisesti

(1) i:n kuva on $\pm i$.
(2) ω:n kuva on $\pm\omega$ tai $\pm i\omega$.

Kokeilemalla huomaa, että nämä kaikki 8 mahdollisuutta tulevat kysymykseen. Galois'n ryhmän laskutoimitukset voi taulukoida kahdeksi $8\times 8-$talukoksi. Vähemmällä pääsee, kun huomaa, että muut kuvaukset saadaan tuloina kahdesta "generaattorista" α ja β, joille

$$\begin{aligned} \alpha(i) &= i, \quad \alpha(\omega) = i\omega \\ \beta(i) &= -i, \quad \beta(\omega) = \omega. \end{aligned}$$

$$\Gamma(K : \mathbf{Q}) = \{1, \alpha, \alpha^2, \alpha^3, \beta, \alpha\beta, \alpha^2\beta, \alpha^3\beta\}$$

Laskutoimitusten luettelemisen sijasta voi ryhmän esittää mukavasti antamalla **generaattorit ja niiden väliset relaatiot**. (Näistä lisää seuraavassa luvussa.)

$$\Gamma(K : \mathbf{Q}) = \langle \alpha, \beta : \alpha^4 = \beta^2 = 1, \beta\alpha = \alpha^3\beta \rangle.$$

(4) $\Gamma(K : \mathbf{Q})$:n aliryhmät on mahdollista löytää kokeilemalla. Ne ovat:

$$\begin{aligned} G =& \Gamma(K : \mathbf{Q}), \\ S =& \{1, \alpha, \alpha^2, \alpha^3\}, \\ T =& \{1, \alpha^2, \beta, \alpha^2\beta\}, \\ U =& \{1, \alpha^2, \alpha\beta, \alpha^3\beta\}, \\ A =& \{1, \alpha^2\}, \\ B =& \{1, \beta\}, \\ C =& \{1, \alpha\beta\}, \\ D =& \{1, \alpha^2\beta\}, \\ E =& \{1, \alpha^3\beta\} \text{ ja} \\ I =& \{1\}. \end{aligned}$$

Näiden inkluusiot ovat:

$$\begin{array}{ccccc} & & G & & \\ & T & S & U & \\ D & B & A & C & E \\ & & I. & & \end{array}$$

Tästä seuraa, että Galois'n päälauseen mukaan vastaaville kiintopistekunnille pätevät käänteiset inkluusiot:

$$\begin{array}{ccccc} & & K = I^\dagger & & \\ D^\dagger & B^\dagger & A^\dagger & C^\dagger & E^\dagger \\ & T^\dagger & S^\dagger & U^\dagger & \\ & & \mathbf{Q} = G^\dagger. & & \end{array}$$

(5) Määrätään kiintopistekunnat. Työtä helpottaa, että tiedämme niiden asteet. $\mathbf{Q}$:n suhteen asteen 2 välikunnat $\mathbf{Q}(i), \mathbf{Q}(\sqrt{2})$ ja $\mathbf{Q}(i\sqrt{2})$ ovat $S^\dagger$, $T^\dagger$ ja $U^\dagger$ — tässä järjestyksessä, kuten voi helposti todeta. Huomaa: $\mathbf{Q}$:n suhteen asteen 2 välikunnalle M on $[K : M] = 4$, ja edellä esiintyivät 4-alkioiset aliryhmät.

Loput 5 välikuntaa ovat astetta 4. Määrätään esimerkiksi $C^\dagger$. Se ei ole aivan triviaalia. $C = \{1, \alpha\beta\}$. On siis löydettävä ne K:n alkiot

$$x = a + b\omega + c\omega^2 + d\omega^3 + ei + fi\omega + gi\omega^2 + hi\omega^3, \quad a, \ldots, h \in \mathbf{Q},$$

joille $\alpha\beta(x) = x$. Soveltamalla α:aa ja β:aa saadaan

$$\alpha\beta(x) = a + f\omega - c\omega^2 - h\omega^3 - ei + bi\omega + gi\omega^2 - di\omega^3,$$

mistä saadaan 8 yhtälöä:

$$\begin{aligned} a &= a, \\ b &= f, \\ c &= -c, \\ d &= -h, \\ e &= -e, \\ f &= b, \\ g &= g \quad \text{ja} \\ h &= -d. \end{aligned}$$

Siis kertoimet $a, \ldots, h \in \mathbf{Q}$ ovat mielivaltaisia, paitsi että: $c = 0, e = 0, f = b$ ja $h = -d$.

$$C^\dagger = \{x = a + b(1+i)\omega + gi\omega^2 + d(1-i)\omega^3 \mid a, b, g, d \in \mathbf{Q}\}.$$

Tästä aste 4 näkyy. $C^\dagger$:n lauseke kuntalaajennuksena sievenee vielä: Koska $(1+i)^2 = 2i$ ja $(1+i)^3 = -2(1-i)$, niin

$$C^\dagger = \mathbf{Q}((1+i)\omega).$$

Vastaavalla tavalla voi todeta, että

$$\begin{aligned} A^\dagger &= \mathbf{Q}(i, \sqrt{2}), \\ B^\dagger &= \mathbf{Q}(\omega), \\ D^\dagger &= \mathbf{Q}(i\omega) \text{ ja} \\ E^\dagger &= \mathbf{Q}((1-i)\omega). \end{aligned}$$

(6) Tarkastetaan vastaavatko normaalit aliryhmät ja välikunnat toisiaan. Normaaleja aliryhmiä ovat G, S, T, U, A ja I. Niiden kiintopistekunnat osoittautuvat sopivien polynomien $P(X)$ hajoituskunniksi:

$$\begin{aligned} G^\dagger &: P(X) = X \\ S^\dagger &: P(X) = X^2 + 1 \\ T^\dagger &: P(X) = X^2 - 2 \\ U^\dagger &: P(X) = X^2 + 2 \\ A^\dagger &: P(X) = X^4 - X^2 - 2 \\ I^\dagger &: P(X) = X^4 - 2 \end{aligned}$$

ja ovat siis $\mathbf{Q}$:n normaaleja laajennuksia. Muut eivät saa sitä ollakaan, vaan kullekin on olemassa polynomi $Q(X)$, jolla on vain osa nollakohdistaan ao. laajennuksessa: Lukija täydentäköön taulukon.

$$\begin{aligned} B^\dagger &: Q(X) = X^2 - 2, \\ C^\dagger &: Q(X) = \\ D^\dagger &: Q(X) = \\ E^\dagger &: Q(X) = \quad . \end{aligned}$$

(7) Testataan lopuksi Galois'n päälauseen viimeistä väitettä normaaliin aliryhmään A. Pitäisi todeta isomorfisiksi ryhmät $\Gamma(A^\dagger : \mathbf{Q})$ ja $\frac{G}{A}$. Tekijäryhmä on ainakin 4-alkioinen

$$\begin{aligned}\langle \alpha, \beta : \alpha^4 = \beta^2 = 1, \beta\alpha = \alpha^3\beta, \alpha^2 = 1\rangle \\ = \langle \alpha, \beta : \alpha^2 = \beta^2 = 1, \beta\alpha = \alpha\beta\rangle \\ = (\mathbf{Z}_2, +) \times (\mathbf{Z}_2, +).\end{aligned}$$

Sama pitäisi saada laskemalla $\Gamma(A : \mathbf{Q})$ suoraan. Koska $A^\dagger = \mathbf{Q}(i\sqrt{2})$, niin sen $\mathbf{Q}-$automorfismit saadaan valitsemalla i:n kuvaksi $\pm i$ ja $\sqrt{2}$:n kuvaksi $\pm\sqrt{2}$, mistä saadaan 4 alkiota Galois'n ryhmään. Tässä $\alpha^2 = \beta^2 = 1$ ja $\alpha\beta = \beta\alpha$, joten ryhmä on

$$(\mathbf{Z}_2, +) \times (\mathbf{Z}_2, +).$$

5. RYHMÄTERAPIAA

Galois'n päälauseen mielenkiinto perustuu pitkälti sen sovelluksiin, joissa yleensä saadaan tietoa välikunnista lähtemällä Galois'n ryhmää koskevista tiedoista. Tätä varten tarvitaan tuntumaa ryhmiin, erityisesti permutaatioryhmiin ja niiden normaaleihin aliryhmiin. Vapaita ja äärellisesti generoituja ryhmiä koskevia tarkasteluja ei tarvita monisteen loppuosan ymmärtämiseksi, mutta muita tämän luvun kohtia tarvitaan.

Generaattorit ja kommutaattorit.

5.1. Määritelmä. Olkoon G ryhmä. Laskutoimitusta merkitsemme multiplikatiivisesti, ykköstä e:llä, aliryhmänä olemista merkillä $\Subset$, normaalina aliryhmänä olemista $\lhd$.

(1) Joukko $J \subset G$ *generoi* aliryhmän $M \subset G$, mikäli

$$M = \bigcap_{J \subset L \Subset G} L,$$

eli M on pienin joukon J sisältävä aliryhmä. Kun $J \neq \emptyset$, niin M muodostuu kaikista joukon J alkioiden ja niiden käänteisten äärellisistä tuloista.

(2) aliryhmän M generoiva joukko J on *minimaalinen*, jos mikään sen aito osajoukko ei generoi M:ää.

5.2. Esimerkki. (1) Additiivisen ryhmän $\mathbf{Z}$ generoi mm. jokainen seuraavista joukoista:

$$\mathbf{Z}, \mathbf{N}, \{1\}, \{-1\}.$$

Näistä $\{1\}$ ja $\{-1\}$ ovat minimaalisia.

(2) ryhmän G alkioiden x ja y *kommutaattori* on

$$xyx^{-1}y^{-1}.$$

G:n *kommutaattorialiryhmä* on kaikkien kommutaattorien generoima aliryhmä G'. G on kommutatiivinen, eli abelin ryhmä aina ja vain kun kommutaattorialiryhmä G' on pelkkä $\{e\}$.

5.3. Lause. *Jokainen kommutaattorialiryhmää G' laajempi aliryhmä $H \Subset G$ on normaali. Erityisesti G' itse on normaali.*

Todistus. Olkoon $h \in H$ ja $x \in G$. Silloin

$$xhx^{-1} = xhx^{-1}h^{-1}h \in G'H \subset H. \quad \square$$

5.4. Lause. *Tekijäryhmä $\frac{G}{H}$ on kommutatiivinen aina ja vain, kun normaali aliryhmä $H \lhd G$ sisältää kommutaattorialiryhmän G'.*

Todistus. Olkoot

$$X = xH \quad \text{ja} \quad Y = yH.$$

tekijäryhmän $\frac{G}{H}$ alkioita. Silloin $XYX^{-1}Y^{-1}$ on sen alkio $xyx^{-1}y^{-1}H$. Se on $\frac{G}{H}$:n neutraalialkio H aina ja vain, kun $xyx^{-1}y^{-1} \in H$. $\frac{G}{H}$ on siis kommutatiivinen aina ja vain, kun H sisältää kaikki kommutaattorit ja siis koko G':n. $\square$

Symmetriset ryhmät.

5.5. Määritelmä. Symmetrinen ryhmä $\mathcal{S}_n$ muodostuu kaikista $n-$alkioisen joukon $E_n = \{1, 2, \ldots, n\}$ permutaatioista. Vakiintuneen tavan mukaisesti merkitsemme permutaatiota, joka kuvaa kunkin luvun $j \in E_n$ luvuksi n_j symbolilla

$$\tau = \begin{pmatrix} 1 & 2 & \ldots & n \\ n_1 & n_2 & \ldots & n_n \end{pmatrix}$$

eli

$$\tau = \begin{pmatrix} i_1 & i_2 & \ldots & i_n \\ n_{i_1} & n_{i_2} & \ldots & n_{i_n} \end{pmatrix},$$

missä i on mielivaltainen E_n:n permutaatio. Laskutoimituksena on kuvausten yhdistäminen. Permutaatioita yhdistettäessä on oppikirjoissa usein tapana merkitä **ensiksi sovellettava permutaatio vasemmalle. Me käytämme kuitenkin kuvausten yhdistämisessä tavanomaista järjestyskonventiota ja laskemme siis esimerkiksi:**

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Symmetrisen ryhmän aliryhmiä sanotaan *permutaatioryhmiksi.*

On hyvä huomata, että $\mathcal{S}_n$:n määritelmässä olennaista on vain joukon E_n mahtavuus, ei sen alkioiden nimet. Symmetristen ryhmien merkitys perustuu paljolti siihen, että kaikki ryhmät ovat permutaatioryhmien kanssa isomorfisia:

5.6. Lause (Cayley). [19] *Jokainen äärellinen ryhmä $G = \{a_1, \ldots, a_n\}$ on isomorfinen jonkin permutaatioryhmän $M \Subset \mathcal{S}_n$ kanssa.*

[19] Myös äärettömän joukon E permutaatiot eli bijektiot itselleen muodostavat ryhmän, *symmetrisen ryhmän* $\mathcal{S}_E$. Cayleyn lause todistuksineen pätee tässäkin. Asiasta lisää luvuissa 7 ja 8.

Todistus. Isomorfismiksi kelpaa kuvaus, joka alkioon $a \in G$ liittää $n-$alkioisen joukon G permutaation

$$s_a : x \mapsto ax,$$

ns. vasemman siirron alkiolla a. $\square$

Määritelmä. Transpositio eli vaihto on permutaatio, joka kuvaa kaksi E_n:n eri alkiota toisikseen ja muut itselleen. Merkintöjä:

$$\tau_{i,j} = \tau_{j,i} = (i,j) = (j,i) = \begin{pmatrix} 1 & \dots & i & \dots & j & \dots & n \\ 1 & \dots & j & \dots & i & \dots & n \end{pmatrix}.$$

5.7. Lause.

(1) *$\mathcal{S}_n$:ssä on $n!$ alkiota.*
(2) *$\mathcal{S}_n$:ssä on $\frac{1}{2}n(n-1)$ transpositiota.*
(3) *Transpositiot generoivat ryhmän $\mathcal{S}_n$.*
(4) *Transpositiot $(1,2),(2,3),\dots$ ja $(n-1,n)$ ovat minimaalinen ryhmän $\mathcal{S}_n$ generoiva joukko.*
(5) *Jokainen transpositio (i,j), $i<j$, voidaan lausua tulona*

$$(i,j) = (i,i+1)\dots(j-2,j-1)(j-1,j)(j-2,j-1)\dots(i,i+1).$$

(6) *Transpositio $(1,2)$ ja kiertävä permutaatio*

$$\begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 2 & 3 & \dots & n & 1 \end{pmatrix}$$

ovat minimaalinen ryhmän $\mathcal{S}_n$ generoiva joukko.

Todistus. Induktio. $\square$

Huomaa, että permutaation esitys transpositioiden tulona ei ole yksikäsitteinen. Esimerkiksi E_4:ssä

$$(1,2) = (3,4)(2,1)(3,4).$$

Kuitenkin esiintyvien transpositioiden **lukumäärä on modulo 2 riippumaton niiden valinnasta**. Tämän perustelemme:

5.8. Määritelmä. Permutaation $\beta \in \mathcal{S}_n$ *merkki* on

$$\epsilon_\beta = (-1)^{\nu_\beta},$$

missä

$$\nu_\beta = \#\{(i,j) \in E_n \times E_n \mid i<j \text{ ja } \beta(j) < \beta(i)\}$$

on *järjestyskääntöjen* eli *inversioiden* lukumäärä permutaatiossa β. Sanomme, että β on *parillinen*, jos sen merkki on 1 ja *pariton*, jos sen merkki on -1.

5.9. Lause.

(1) *Kahden permutaation tulon merkki on niiden merkkien tulo. Merkkikuvaus ϵ on siis ryhmähomomorfismi $\mathcal{S}_n$:ltä multiplikatiiviselle ryhmälle $\{1, -1\}$.*
(2) *Transpositio on pariton.*
(3) *Parillinen permutaatio voidaan esittää tulona vain parillisen monesta transpositiosta, pariton vain parittoman monesta.*

Todistus. (1) Koska β on bijektio joukolta $\{1, \ldots, n\}$ itselleen, niin tulo

$$P_\beta = \prod_{1 \le i < j \le n} \frac{\beta(i) - \beta(j)}{i - j}$$

on ± 1, sillä merkkiä vaille sekä osoittaja että nimittäjä käyvät läpi kertaalleen kaikki erotukset $i - j$, missä $i < j$. Toisaalta tulon tekijä $\frac{\beta(i)-\beta(j)}{i-j}$ on positiivinen tai negatiivinen sen mukaan, vaihtaako β i:n ja j:n keskinäisen järjestyksen vai ei. Siksi koko tulon merkkikin on sama kuin permutaation β merkki ja yllättäen

$$P_\beta = \epsilon_\beta.$$

Tästä väite seuraakin, sillä jos σ on toinen E_n:n permutaatio, niin

$$\begin{aligned} P_{\beta\sigma} &= \prod_{1 \le i < j \le n} \frac{\beta(\sigma(i)) - \beta(\sigma(j))}{i - j} \\ &= \prod_{1 \le i < j \le n} \frac{\beta(\sigma(i)) - \beta(\sigma(j))}{\sigma(i) - \sigma(j)} \prod_{1 \le i < j \le n} \frac{\sigma(i) - \sigma(j)}{i - j} \\ &= \prod_{1 \le \sigma(i) < \sigma(j) \le n} \frac{\beta(\sigma(i)) - \beta(\sigma(j))}{\sigma(i) - \sigma(j)} \prod_{1 \le i < j \le n} \frac{\sigma(i) - \sigma(j)}{i - j} \\ &= P_\beta P_\sigma, \end{aligned}$$

koska σ on bijektio.

(2) Väite on triviaali, kun transpositio τ vaihtaa kaksi peräkkäistä lukua. Toisaalta lause 5.7. (5) kertoo, että jokainen permutaatio voidaan lausua parittoman monen ($2(i - j) - 1$ kpl.) tällaisen tulona.

(3) Seuraa edellisistä kohdista. □

Kiertohajoitelma. Hajoitimme edellä mielivaltaisen permutaation tuloksi transpositioista. Toinen hyödyllinen hajoitelma on permutaation esittäminen tulona erillisistä syklisistä permutaatioista eli kierroista.

5.10. Määritelmä. Permutaatio $\beta \in \mathcal{S}_n$ on *syklinen permutaatio*, tarkemmin sanoen $k-$*kierto*, jos se permutoi syklisesti k kpl. luvuista $1, \ldots, n$ ja kuvaa muut $n-k$ kpl. itselleen. Merkintöjä:

$$\beta = (i_1, i_2, \ldots, i_{k-1}, i_k) = \begin{pmatrix} i_1 & i_2 & \ldots & i_{k-1} & i_k & i_{k+1} & \ldots & i_n \\ i_2 & i_3 & \ldots & i_k & i_1 & i_{k+1} & \ldots & i_n \end{pmatrix}.$$

Huomaa, että erityisesti transpositiot ovat kiertoja ja että niille käyttämämme merkintätapa on tämän standardin mukainen. Kannattaa varoa algebran kirjoja lukiessaan sitä mahdollisuutta, että mielivaltaista permutaatiota saatetaan merkitä kirjoittamalla näkyviin meidän määritelmämme 5.5. kaksirivisen matriisin alempi rivi. Esimerkiksi permutaatio

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

on eri asia kuin kierto $(3, 1, 2)$, joka on permutaatio

$$(3, 1, 2) = (2, 3, 1) = (1, 2, 3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

5.11. Lause. *$k-$kierto β voidaan lausua transpositioiden tulona esimerkiksi seuraavasti*

$$\beta = (i_1, i_2, \ldots, i_{k-1}, i_k) = (i_1, i_2)(i_2, i_3) \ldots (i_{k-1}, i_k).$$

Tästä näkyy, että sen merkki on $(-1)^{k-1}$. Erityisesti jokainen $3-$kierto β on parillinen permutaatio.

Todistus. Helppo $\square$

5.12. Lause. *Mikä tahansa permutaatio $\beta \in \mathcal{S}_n$ paitsi identtinen kuvaus voidaan esittää tulona* **erillisistä** *ei identtisistä kierroista – siis sellaisista, jotka permutoivat eri lukuja. Tämä esitys on järjestystä vaille yksikäsitteinen ja järjestyksen saa valita vapaasti.*

Todistus. Perustelemme ensin esityksen olemassaolon. Olkoon $\beta \in \mathcal{S}_n$. Tehtävänä on jakaa joukko $E_n = \{1, 2, \ldots, n\}$ luokkiin, eli erillisiin osajoukkoihin, joita kutakin β permutoi syklisesti. Tämän luokkajaon antaa sopiva ekvivalenssirelaatio, nimittäin *transitiivisuusekvivalenssi*:

$$a \sim_{\mathcal{T}} b \iff a = \beta^m(b) \quad \text{jollekin } m \in \mathbf{Z}.$$

Tämä on selvästikin ekvivalenssirelaatio joukossa E_n: refleksiivinen, symmetrinen ja transitiivinen.

Merkitään luvun a luokkaa, sen *transitiivisuusluokkaa*

$$[a] = \{\dots \beta^{-1}a, a, \beta a, \beta^2 a, \dots\}.$$

Nytpähän $[a]$ on äärellisen joukon E_n osajoukkona itsekin äärellinen. Olkoon siinä j alkiota: $j = \#[a]$. Itse asiassa luokan $[a]$ alkiot ovat täsmälleen

$$a, \beta a, \beta^2 a, \dots \text{ ja } \beta^{j-1}(a),$$

sillä

$$\{a, \beta a, \beta^2 a, \dots, \beta^j a\} \subset [a] \implies$$
$$\implies \#\{a, \beta a, \beta^2 a, \dots, \beta^j a\} \leq \#[a] = j,$$

joten on olemassa luvut $0 \leq \mu < \nu \leq j$ siten, että

$$\beta^\mu = \beta^\nu,$$

jolloin

$$\beta^{\nu-\mu}a = a.$$

On näin ollen olemassa nollasta eroava **luonnollinen** luku k, jolla

$$\beta^k a = a.$$

Olkoon k pienin tällainen. Nyt

$$[a] = \{a, \beta a, \beta^2 a, \dots, \beta^{k-1}a\},$$

missä kaikki alkiot eroavat toisistaan. Erityisesti $k = j$.

Permutaation β rajoittuma luokkaan $[a]$ on selvästi kierto

$$s_a = (a, \beta a, \beta^2 a, \dots, \beta^{j-1}a).$$

Koska transitiivisuusluokat ovat erillisiä ja niiden yhdiste on koko E_n, niin β on tulo näin saatavista kierroista. Mahdolliset yksialkioiset transitiivisuusluokat tuottavat identtisen kierron, joka tarpeettomana jätetään pois tulosta.

Osoitetaan kehitelmän yksikäsitteisyys. Olkoon

$$\beta = s_1 s_2 \dots s_\nu$$

hajoitelma erillisten kiertojen tuloksi. β:n useampialkioiset transitiivisuusluokat ovat s_j:den transitiivisuusluokat, koska ne on oletettu erillisiksi. β:n rajoittumat näihin ovat kierrot s_j. $\square$

5.13. Esimerkki.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 4 & 8 & 3 & 1 & 6 & 2 & 5 \end{pmatrix} = (1,7,2,4,3,8,5).$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 4 & 6 & 1 & 3 & 9 & 2 & 8 & 5 \end{pmatrix} = (1,7,2,4)(3,6,9,5).$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 5 & 2 & 7 & 1 & 6 & 9 & 3 & 4 \end{pmatrix} = (1,8,3,2,5)(4,7,9).$$

Sykliset ryhmät.

5.14. Määritelmä. ryhmä G on *syklinen*, mikäli on olemassa $a \in G$, s.e. $\{a\}$ generoi G:n. Tällöin

$$G = \{a^n \mid n \in \mathbf{Z}\}.$$

Sanomme, että a on G:n *virittäjä*. Syklinen ryhmä on aina kommutatiivinen eli abelin ryhmä. Se voi olla ääretön tai äärellinen:

5.15. Lause. *Ääretön syklinen ryhmä on isomorfinen kokonaislukujen additiivisen ryhmän* $(\mathbf{Z}, +)$ *kanssa.* $m-$*alkioinen syklinen ryhmä on isomorfinen additiivisen ryhmän* $(\mathbf{Z}_m, +)$ *kanssa.*

Todistus. Jos jokainen a^n on eri alkio, niin isomorfismi on kuvaus $a^k \mapsto k \in \mathbf{Z}$. Muuten se on

$$a^k \mapsto k \in \mathbf{Z}_m,$$

missä $m = \min\{n \in \{1,2,\dots\} \mid a^n = e\}$. □

Itse asiassa tietenkin minkä tahansa ryhmän G mikä tahansa alkio $a \in G$ generoi kommutatiivisen aliryhmän

$$\{a^n \mid n \in \mathbf{Z}\} \Subset G$$

Sitä sanotaan a:n generoimaksi G:n sykliseksi aliryhmäksi ja sen kertalukua eli alkioiden lukumäärää, äärellisessä tapauksessa

$$\min\{n \in \mathbf{N} \mid a^n = e\},$$

sanotaan alkion $a \in G$ *kertaluvuksi.*

5.16. Lause. *Ryhmä* G*, jonka kertaluku on alkuluku, on syklinen ja siis kommutatiivinen.*

Todistus. Jos G on pelkkä $\{e\}$, on asia selvä. Muuten G:llä on e:stä eroava alkio a. Sen virittämä syklinen aliryhmä on kommutatiivinen, mutta yhtyy koko G:hen, koska sen kertaluku jakaa G:n kertaluvun, joka on kuitenkin oletettu jaottomaksi. □

Alternoivat ryhmät.

5.17. Määritelmä. Totesimme edellä, että kuvaus ϵ on ryhmähomomorfismi $\mathcal{S}_n$:ltä multiplikatiiviselle ryhmälle $\{1, -1\}$. Sen ydin muodostuu kaikista parillisista permutaatioista ja on symmetrisen ryhmän normaali aliryhmä, *alternoiva ryhmä* $\mathcal{A}_n$. Selvästi $\#\mathcal{A}_n = \frac{1}{2}n!$

5.18. Lause. *Alternoiva ryhmä* $\mathcal{A}_n$ *(*$n > 2$*) operoi transitiivisesti joukossa* E_n*, toisin sanoen kaikille* a *ja* $b \in E_n$ *on olemassa parillinen permutaatio* $\beta \in \mathcal{A}_n$*, jolle*

$$b = \beta(a).$$

Todistus. Olkoon $c \in E_n \setminus \{a, b\}$. Valitse $\beta = (a, c)(c, b)$. $\square$

5.19. Lause. *Alternoivan ryhmän* $\mathcal{A}_n$ *(*$n > 2$*) virittävät* $3-$*kierrot*

$$(1, 2, 3), (1, 2, 4), \ldots, (1, 2, n).$$

Todistus. Olkoon $p \in \mathcal{A}_n$. p voidaan esittää tulona parillisen monesta transpositioista

$$\begin{aligned} p &= t_1 t_2 t_3 t_4 \ldots t_{2m} \\ &= t_1(1,2)(1,2)t_2 t_3(1,2)\ldots(1,2)t_{2m}. \end{aligned}$$

Väite on siis todistettu, mikäli jokainen muotoa $t(1, 2)$ tai muotoa $(1, 2)t$ oleva permutaatio on esitettävissä äärellisenä tulona väitteen $3-$kierroista ja niiden käänteisistä. Näin onkin. Olkoon $i, j \in E_n \setminus \{1, 2\}$.

$$\begin{aligned} (1,2)(1,2) &= id = (1,2,3)^3 \\ (1,i)(1,2) &= (1,2,i) \\ (2,i)(1,2) &= (1,i,2) = (1,2,i)^{-1} \\ (i,j)(1,2) &= (1,2,j)(1,i,2)(1,2,j) \\ (1,2)(i,j) &= \text{ sama kuin edellinen} \\ (1,2)(1,i) &= (1,i,2) = (1,2,i)^{-1} \\ (1,2)(2,i) &= (1,2,i). \end{aligned}$$

Muita ei ole. $\square$

Alternoivien ryhmien normaaleilla aliryhmillä – oikeastaan niiden puutteella – tulee olemaan ratkaiseva osa todistettaessa, että yleisen polynomin juuria ei voi ”löytää algebrallisesti”.

Äärellisesti generoidut ryhmät.

5.20. Määritelmä. ryhmä G on *äärellisesti generoitu* , jos sillä on äärellinen generoiva joukko. Esimerkiksi sykliset ryhmät ja äärelliset ryhmät ovat äärellisesti generoituja.

5.21. Lause.

(1) *Äärellisesti generoitu ryhmä on enintään numeroituva.*
(2) *Äärellisesti generoidun ryhmän homomorfinen kuva on äärellisesti generoitu.*
(3) *Jokainen äärellinen generoiva joukko sisältää minimaalisen generoivan joukon, joka sekin on äärellinen.*

Todistus.

(1) Se muodostuu generoivien alkioiden ja niiden käänteisten äärellisistä tuloista.
(2) Sen generoivat generaattorien kuvat.
(3) Jätä turhat pois! □

Vapaat ryhmät.

5.22. Määritelmä. Olkoon I joukko ja $J = I \bigcup (I \times \{-1\})$. Sanomme I:tä *aakkostoksi* ja sen alkioita *kirjaimiksi.* Kirjaimet $a \in I$ ja $b = a^{-1} \in (I \times \{-1\})$ ovat *toistensa vastineet.* Muodostetaan I*:n virittämä vapaa ryhmä* G seuraavasti: Joukko G muodostuu niistä äärellisen monen kirjaimen järjestetyistä jonoista $(a_1, \ldots, a_n)$, joissa ei esiinny peräkkäisinä kirjaimina toistensa vastineita. Näitä jonoja sanotaan *sievennetyisi sanoiksi.* Erityisesti tyhjä sana, jossa ei ole yhtään kirjainta, on sievennetty sana. Laskutoimituksena G:ssä on sievennettyjen sanojen asettaminen peräkkäin ja sen jälkeen sieventäminen:

$$(a_1, \ldots, a_n) \circ (b_1, \ldots, b_m)$$

muodostetaan siis jonosta

$$(a_1, \ldots, a_n, b_1, \ldots, b_m),$$

poistamalla kirjaimet a_n ja b_1, mikäli ne sattuvat olemaan toistensa vastineita, tämän jälkeen poistamalla tarvittaessa a_{n-1} ja b_2 jne. kunnes jää sievennetty sana.

5.23. Lause. *Vapaa ryhmä on ryhmä.*

Todistus. Laskemalla voi osoittaa, että määrittelemämme $\circ$ on assosiatiivinen laskutoimitus. Neutraalialkiona toimii tyhjä sana. Sievennetyn

sanan $(a_1, \ldots, a_k)$ käänteisalkio on sana $(a'_k, \ldots, a'_1)$, missä a'_j on a_j:n vastine.

Merkintöjä voi hieman yksinkertaistaa jättämällä turhat sulkeet pois.

$$(a) = a,$$
$$(a_1, \ldots, a_k) = a_1, \ldots, a_k,$$
$$(a)^{-1} = a^{-1}.$$

Tarvittaessa voidaan G:n alkioita merkitä myös sieventämättöminä sanoina, kunhan muistetaan samaistaa sanat, joista sieventämällä tulee sama.

5.24. Lause.

(1) *Aakkosto generoi vapaan ryhmänsä.*
(2) *Vapaa ryhmä G määräytyy isomorfiaa vaille yksikäsitteisesti aakkostonsa mahtavuudesta.*
(3) *Erityisesti vastinaakkostot I ja $I \times \{-1\}$ generoivat isomorfiset ryhmät.*

Todistus. Selvä. □

5.25. Lause. *Jokainen ryhmä on isomorfinen jonkin vapaan ryhmän tekijäryhmän kanssa.*

Todistus. Olkoon I ryhmän G generoiva joukko. Sellainen on olemassa, kelpaahan esim. koko G. Osoitetaan, että G on I:n generoiman vapaan ryhmän Γ tekijäryhmä(n kanssa isomorfinen). Riittää löytää surjektiivinen homomorfismi

$$h : \Gamma \to G.$$

Sellainen on tarjolla: kuvataan

$$a = (a_1, \ldots, a_n) \mapsto a_1 \ldots a_n \in G.$$

Homomorfisuus ja surjektiivisuus ovat ilmeisiä. Väite seuraa heti: $G \sim \frac{\Gamma}{\text{Ker } h}$. □

Edellinen lause sellaisenaan ei vielä paljoa sano, riippuuhan esitys joukon I valinnasta eikä h:n ytimestäkään ole vielä sanottu mitään. Sanotaan:

5.26. Huomautus (ryhmän virittäjä-relaatioesitys).
Edellisen lauseen tilanteessa homomorfismin h ydin on

$$N = \text{Ker } h$$
$$= \{a = a_1^{\mu_1} \ldots a_n^{\mu_n} \in \Gamma \mid a_1, \ldots, a_n \in I (\subset G), a_1^{\mu_1} \ldots a_n^{\mu_n} = e \in G\}.$$

Ytimen alkioita $a_1^{\mu_1} \dots a_n^{\mu_n} (= e)$ sanotaan generaattoreiden $a_k \in I$ välisiksi *relaatioiksi.* Selvästi G määräytyy generaattoreistaan ja näiden välisistä relaatioista, mutta niitä voi olla ja yleensä on kovin paljon. Tilannetta voi yrittää yksinkertaistaa. Tämä onnistuu, kun huomaa, että N on Γ:n aliryhmä, jonka tuntemiseksi riittää tuntea sen generoiva joukko, *ryhmän G määrittelevien relaatioiden joukko* (generoivan joukon I suhteen). Generoiva joukko I ja määrittelevät relaatiot määräävät aliryhmän $N \Subset \Gamma$ ja siis ryhmän $G = \frac{\Gamma}{N}$ täysin.

G muodostuu aakkoston I kirjainten ja niiden muodollisten käänteisten jonoista, eli sanoista, jotka sievennetään poistamalla alkio-vastaalkioparit, jolloin saadaan vapaa ryhmä, ja jatkamalla sieventelyä poistamalla myös kaikki sanassa mahdollisesti esiintyvät määrittelevät relaatiot. Tämä ryhmän G esittämistapa **saattaa** olla melko yksinkertainen, kun määritteleviä relaatioita on kohtuullisen vähän. Edes äärellisesti generoidun ryhmän tapauksessa ei kuitenkaan tarvittavien relaatioiden joukko ole aina äärellinen. Äärellisen monen relaation tapauksessakaan ei sieventely yleensä ole mikään helppo rutiinitehtävä.

Olemme todenneet, että mikä tahansa ryhmä voidaan lausua generaattoreiden ja relaatioiden avulla. Toisaalta mikä tahansa joukko I kelpaa vapaan ryhmän generaattoreiksi ja mikä tahansa joukko R vapaan ryhmän G alkioita määrää jonkin tekijäryhmän sen relaatioina. (Ne samaistetaan siis neutraalialkioon.) Tämä tekijäryhmä on $\frac{G}{N}$, missä N on suppein G:n normaali aliryhmä, joka sisältää joukon R. (Suppein on olemassa, nimittäin kaikkien leikkaus.)

Jos näin esitetyn ryhmän määritteleviin relaatioihin lisätään uusi relaatio, niin saatava uusi ryhmä on aikaisemman tekijäryhmä. Tämä järkeenkäypä lause (von Dyck) todistetaan periaatteessa samalla tavalla kuin edellä ollut erikoistapaus, mielivaltaisen ryhmän esittäminen vapaan ryhmän tekijäryhmänä.

Ratkeavat ryhmät.

5.27. Määritelmä. ryhmä G on *ratkeava,* mikäli on olemassa äärellisen monta sen sisäkkäistä aliryhmää

$$\{e\} = G_0 \Subset G_1 \Subset \cdots \Subset G_n = G$$

siten, että

(1) $\quad G_i \lhd G_{i+1} \quad \forall i = 0, \dots, n-1,$

(2) $\quad \frac{G_{i+1}}{G_i}$ on kommutatiivinen $\quad \forall i = 0, \dots, n-1.$

Huomaa, että aliryhmät $G_i \Subset G$ eivät yleensä ole normaaleja, koska

$$H \lhd K \lhd G \not\Rightarrow H \lhd G.$$

Ratkeavan ryhmän käsitteen merkitys piilee siinä, että polynomiin liittyvä Galois'n ryhmä tulee osoittautumaan ratkeavaksi täsmälleen silloin, kun "nollakohdille on olemassa algebrallinen kaava".

5.28. Esimerkkejä.

(1) Abelin ryhmät ovat ratkeavia, jonona $\{e\} \Subset G$.
(2) Symmetrinen ryhmä $\mathcal{S}_3$ on ratkeava; sillä on normaalina aliryhmänä 3−alkioinen syklinen ryhmä, jonka generoi permutaatio $(1,2,3) \in \mathcal{S}_3$ ja tekijäryhmä on $\mathcal{S}_2$.
(3) Myös $\mathcal{S}_4$ on ratkeava; sillä on aliryhmäjono

$$\{e\} \Subset \mathcal{V} \Subset \mathcal{A}_4 \Subset \mathcal{S}_4,$$

missä $\mathcal{A}_4$ on alternoiva ryhmä ja $\mathcal{V}$ on *Kleinin neliryhmä*[20]

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

tekijäryhmät ovat itse asiassa

$$\frac{\mathcal{V}}{\{e\}} \sim \mathcal{V}$$
$$\frac{\mathcal{A}_4}{\mathcal{V}} \sim (\mathbf{Z}_3, +)$$
$$\frac{\mathcal{S}_4}{\mathcal{A}_4} \sim (\mathbf{Z}_2, +).$$

Kaikki ovat kommutatiivisia.
(4) Symmetrinen ryhmä $\mathcal{S}_5$ ei ole ratkeava. Perusteluksi tarvitaan melkein koko tämä luku.

5.29. Lause (Ratkeavuuden perinnöllisyyslause).

(1) *Ratkeavan ryhmän aliryhmät ovat ratkeavia.*
(2) *Ratkeavan ryhmän tekijäryhmät ovat ratkeavia.*
(3) *Jos ryhmän G normaali aliryhmä H ja tekijäryhmä $\frac{G}{H}$ ovat ratkeavia, niin myös G itse on ratkeava.*

Todistus. Nämä kaikki perustuvat **ryhmien isomorfialauseisiin**: □

[20] $a = (12)(34)$, $b = (13)(24)$, $c = (14)(23)$. Neliryhmästä hieman lisää lauseen 5.35. todistuksessa.

5.30. Lause (Isomorfialauseet).

(1)
$$\frac{H}{N \cap H} \sim \frac{HN}{N},$$
kun $N \lhd G$ *ja* $H \leqslant G$.

(2)
$$\frac{G/N}{H/N} \sim \frac{G}{H}, \qquad \textit{"supistussääntö"}$$
kun $N \lhd G$ *ja* $N \leqslant H \lhd G$.

Todistus. (1) Tarkastellaan kanonista surjektiota

$$\theta : G \to \frac{G}{N}.$$

aliryhmän $H \leqslant G$ kuva on $\theta(H) \leqslant \frac{G}{N}$. Sen alkukuva $\theta^{-1}(\theta(H))$ sisältää tietysti H:n, mutta on yleensä sitä aidosti laajempi, sillä se sisältää kaikkien alkioidensa sivuluokatkin:

$$\theta g \in \theta(H) \iff \theta(gN) \subset \theta(H).$$

Alkukuva on siis G:n aliryhmä $HN = \{hn \mid h \in H,\, g \in N\}$. θ:n rajoittumina on saatu kaksi surjektiota ryhmälle $\theta(H)$, nimittäin

$$\theta' : H \to \theta(H)$$
$$\text{ja} \quad \theta'' : HN \to \theta(H).$$

Ryhmien homomorfismilauseen mukaan

$$\frac{H}{\text{Ker } \theta'} \sim \frac{HN}{\text{Ker } \theta''} (\sim \theta(H)).$$

Väitteen todistamiseksi riittää näin ollen todistaa, että ytimet ovat oikeat. Tässä ei ole mitään ongelmaa:

$$\text{Ker } \theta' = \text{Ker } \theta \cap H = N \cap H.$$
$$\text{Ker } \theta'' = \text{Ker } \theta \cap HN = N \cap HN = N.$$

(2) Jo osan (1) oletuksin on $N \cap H \lhd H$, joten lisäehdolla $N \leqslant H$ tekijäryhmä H/N on olemassa ja luonnollisella tavalla isomorfinen $G/N =$

$\theta(G)$:n aliryhmän $\theta(H)$ kanssa. **Surjektiivisessa** homomorfismissa normaalin aliryhmän kuva on normaali aliryhmä, joten $H/N \lhd G/N$. Nyt kanoniset surjektiot yhdistämällä saadaan surjektiivinen homomorfismi

$$G \xrightarrow{\theta} G/N \xrightarrow{\varphi} \frac{G/N}{H/N}.$$

Homomorfismilause antaa isomorfian

$$\frac{G/N}{H/N} = \frac{G}{Ker(\varphi\theta)},$$

mutta esiintyvä ydin on H. $\square$

Lauseen 5.29. Todistus. (1) Olkoon

$$\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_r = G,$$

missä kukin tekijäryhmä $\frac{G_{j+1}}{G_j}$ on kommutatiivinen. Jos $H \Subset G$, niin valitaan

$$H_i = G_i \cap H$$

ja saadaan

$$\{e\} = H_0 \lhd H_1 \lhd \cdots \lhd H_r = H,$$

missä kukin tekijäryhmä

$$\frac{H_{j+1}}{H_j} = \frac{G_{j+1} \cap H}{G_j \cap H} = \frac{G_{j+1} \cap H}{G_j \cap (G_{j+1} \cap H)} \sim$$
$$\sim \frac{G_j(G_{j+1} \cap H)}{G_j} \Subset \frac{G_{j+1}}{G_j}$$

on kommutatiivinen.

(2) Jos $N \lhd G$, niin saadaan

$$\{e\} = \frac{N}{N} = \frac{G_0N}{N} \lhd \frac{G_1N}{N} \lhd \cdots \lhd \frac{G_rN}{N} = \frac{GN}{N} = \frac{G}{N},$$

missä kukin tekijäryhmä

$$\frac{G_{j+1}N/N}{G_jN/N} \sim \frac{G_{j+1}N}{G_jN} = \frac{G_{j+1}(G_jN)}{G_jN} \sim$$
$$\sim \frac{G_{j+1}}{G_{j+1} \cap (G_jN)} \sim \frac{G_{j+1}/G_j}{(G_{j+1} \cap (G_jN))/G_j},$$

on kommutatiivinen, koska osoittaja on sitä.

(3) Olkoon lopuksi

$$\{e\} = N_0 \lhd N_1 \lhd \cdots \lhd N_r = N, \text{ ja}$$
$$\{e\} = \frac{N}{N} = \frac{G_0}{N} \lhd \frac{G_1}{N} \lhd \cdots \lhd \frac{G_s}{N} = \frac{G}{N},$$

missä asianomaiset tekijäryhmät ovat kommutatiivisia. Itse G:lle saadaan jono

$$\{e\} = N_0 \lhd N_1 \lhd \cdots \lhd N_r = N = G_0 \lhd G_1 \lhd \cdots \lhd G_s = G,$$

mistä tekijäryhmiksi saadaan joko kommutatiiviseksi jo tiedettyjä $\frac{N_{j+1}}{N_j}$ tai

$$\frac{G_{j+1}}{G_j} \sim \frac{G_{j+1}/N}{G_j/N},$$

nekin abel. □

Yksinkertaiset ryhmät.

5.31 Määritelmä. Ryhmä, jolla ei ole yhtään epätriviaalia normaalia aliryhmää, on *yksinkertainen.*

5.32. Esimerkki. Äärellisellä ryhmällä, jonka kertaluku on alkuluku, ei ole edes yhtään epätriviaalia aliryhmää. Se on siis yksinkertainen. Näin käy, vaikka ryhmä lauseen 5.16. mukaan on syklinen ja siis kommutatiivinen ja sellaisena ratkeava.

Yksinkertaisuus on ratkeavuudelle tavallaan vastakkainen ominaisuus. Juuri mikään ryhmä ei ole molempia. Ainoan poikkeuksen muodostaa itse asiassa edellinen esimerkki, sillä pätee

5.33. Lause. *Ryhmä G on samalla sekä yksinkertainen että ratkeava aina ja vain ollessaan alkulukukertalukua, lauseen 5.16. mukaan siis syklinenkin.*

Todistus. Jos G on ratkeava, niin on olemassa sen sisäkkäiset aliryhmät

$$\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G.$$

Poistamalla mahdolliset toistot jonosta voimme olettaa, että $G_{n-1} \neq G$. Tapaus $G = \{e\}$ on triviaali ja sivuutetaan. Yksinkertaisuusoletuksen takia G_{n-1} on $\{e\}$. Ryhmä $G = \frac{G}{\{e\}} = \frac{G_n}{G_{n-1}}$ on siis abel.

Abelin ryhmän kaikki aliryhmät ovat normaaleja, joten G:llä ei nyt saa olla edes yhtään epätriviaalia aliryhmää. Kuitenkin jokainen alkio

$g \in G\backslash\{e\}$ virittää aliryhmän, nimittäin syklisen aliryhmän $\{g^n \mid n \in Z\}$. Tämä on siis koko G, joka näin ollen on syklinen. Syklisellä ryhmällä on kuitenkin epätriviaaleja aliryhmiä — esimerkiksi g^j:n virittämä syklinen aliryhmä, missä j on kertaluvun $\#G$ tekijä, tapauksessa $\#G = \infty$ mikä tahansa kokonaisluku — ellei sen kertaluku ole alkuluku, mikä jää ainoana mahdollisuutena jäljelle. Lauseen käänteinen puoli on helppo todistaa. □

Todistamme pian korkeamman asteen yhtälöiden tutkimisessa olennaisella tavalla tarvittavan lauseen, jonka mukaan alternoiva ryhmä $\mathcal{A}_n$ on yksinkertainen kaikilla $n \geq 5$ — toisin kuin $\mathcal{A}_4$, jonka edellä totesimme olevan suorastaan ratkeava.

Sen sijaan emme tarvitse jatkossa seuraavaa äärellisten ryhmien rakennetta selvittävää lausetta, jolla siis tässä on "vain yleissivistävä arvo":

5.34. Lause (Jordan–Hölder). *Mielivaltaisella äärellisellä ryhmällä on aliryhmät*

$$\{e\} = G_0 \Subset G_1 \Subset \cdots \Subset G_n = G$$

siten, että (vrt. 5.27.)

(1) $\quad G_i \lhd G_{i+1} \quad \forall i = 0, \ldots, n-1,$

(2) $\quad \dfrac{G_{i+1}}{G_i}$ *on* **yksinkertainen** $\quad \forall i = 0, \ldots, n-1.$

Tekijäryhmien $\frac{G_{i+1}}{G_i}$ jono riippuu, järjestystä lukuunottamatta, vain ryhmästä G, ei normaalien aliryhmien valinnoista.

Todistus. Ideana on alkaa tilanteesta $\{e\} \lhd G$ ja lisätä väliin maksimaalinen määrä normaaleja aliryhmiä, induktiivisesti yksi kerrallaan. Isomorfialauseita tarvitaan. □

5.35. Lause. *Alternoiva ryhmä $\mathcal{A}_n$ on yksinkertainen kaikilla $n \geq 5$.*

Todistus. Olkoon $\{e\} \neq N \lhd \mathcal{A}_n = \mathcal{A}$, $n \geq 5$. Osoitamme, että $\mathcal{A} \subset N$. Riittää, että N sisältää $\mathcal{A}$:n virittäjät, esimerkiksi lauseen 5.19 kierrot

$$(1,2,3), (1,2,4), \ldots, (1,2,n).$$

Itse asiassa riittää osoittaa, että N sisältää edes yhden 3−kierron (a,b,c). Riittävyyden voi todeta seuraavasti: Merkintöjä tarvittaessa muuttaen voi olettaa, että $(1,2,3) \in N$. On osoitettava, että $(1,2,k) \in N$, kun $k > 3$. Nytpä

$$(1,2,k) = (1,k,2)^2$$

ja $\quad (1,k,2) = (3,2,k)(1,2,3)(3,2,k)^{-1} \in (3,2,k)N(3,2,k)^{-1} \subset N,$

koska N on normaali ja $(3,2,k)$ on parillinen permutaatio, siis $(3,2,k) \in \mathcal{A}$.

Ongelmaksi jää löytää N:stä 3−kierto. Tarkastellaan millaisia alkioita N:ssä ylimalkaan voi olla. Ainakin jokainen $x \in N$ on muotoa

$$x = s_1 s_2 \dots s_m,$$

missä s_j:t ovat erillisiä kiertoja. Todistus jakautuu tapauksiin (1) – (4) sen mukaan kuinka monia alkioita kierrot s_j permutoivat. Voimme olettaa, että x:n muodostavat kierrot $s_1, s_2, \dots, s_m$ on lueteltu pituusjärjestyksessä, pisin ensin.

(1) **"s_1 on pitkä kierto."** Oletetaan, että jollakin $x \in N$ s_1 on muotoa

$$s_1 = (a_1, \dots, a_k)$$

missä $k \geq 4$. Lohkaistaan s_1:stä alkupää

$$t = (a_1, a_2, a_3)$$

ja osoitetaan, että

$$t^{-1}xtx^{-1}$$

on toisaalta N:n alkio, toisaalta 3−kierto (a_1, a_3, a_4).

$(t^{-1}xt)x^{-1}$ kuuluu todella normaaliin aliryhmään N , koska $x \in N$ ja t on 3−kiertona parillinen eli $\mathcal{A}$:n alkio. Kiertojen tulon laskemiseksi yksinkertaistetaan merkintöjä. Nimeämällä E_n:n alkiot uudelleen korvaamme jokaisen a_j:n yksinkertaisesti j:llä, jolloin siis esimerkiksi $t = (1,2,3)$. Käyttämällä aluksi kiertojen t ja s_j $j \neq 1$ erillisyyttä, joka takaa niiden vaihdannaisuuden, ja sitten suoraan laskemalla saamme todella:

$$\begin{aligned} t^{-1}xtx^{-1} &= t^{-1}s_1 s_2 \dots s_m t (s_1 s_2 \dots s_m)^{-1} = \\ &= t^{-1}s_1 t (s_2 \dots s_m)(s_2 \dots s_m)^{-1} s_1^{-1} = \\ &= t^{-1}s_1 t s_1^{-1} = \\ &= (1,2,3)^{-1}(1,2,\dots,k)(1,2,3)(1,2,\dots,k)^{-1} = \\ &= (3,2,1)(1,2,\dots,k)(1,2,3)(k,\dots,2,1) = \\ &= (3,2,1)(1,2,\dots,k)(1,2,3)(k,\dots,2,1) = (1,3,4). \end{aligned}$$

(2) **"s_1 ja s_2 ovat 3−kiertoja".** Oletamme, että jollakin $x \in N$

$$x = (1,2,3)(4,5,6)y,$$

missä on taas lyhennetty merkintöjä kirjoittamalla $s_3 \dots s_m = y$. Olkoon nyt $t = (2, 3, 4)$. Silloin

$$(t^{-1}xt)x^{-1} = (1, 5, 2, 4, 3) \in N,$$

joten tapaus (2) palautuu tapaukseen (1).

(3) **"s_1 on ainoa 3−kierto."** Oletamme, että jollakin $x \in N$

$$x = (1, 2, 3)y,$$

missä $s_2 \dots s_m = y$ muodostuu erillisistä 2−kierroista eli transpositioista, jolloin $y^2 = y$ ja siis, muistaen s_j:den vaihdannaisuuden:

$$x^2 = ((1, 2, 3)y)^2 = (1, 2, 3)^2 y^2 = (1, 2, 3)^2 = (1, 3, 2)$$

on N:ään kuuluva 3−kierto.

(4) **"s_1 on transpositio."** Jäljellä on tapaus, jossa jokainen N:n alkio on pelkkien erillisten transpositioiden tulo, parillisen monen tottakai! N:ssä on siis alkio

$$x = (1, 2)(3, 4)y,$$

missä $y^2 = y$. Muokkaamalla tätä edellä opitulla tavalla kiertoa $t = (2, 3, 4)$ käyttäen saadaan N:ään kuuluvaksi kahden transposition tulo

$$t^{-1}xtx^{-1} = (1, 3)(2, 4).$$

Alternoivan ryhmän $\mathcal{A}_4$ tapauksessa tämä tilanne todella esiintyy ja tuottaa edellä mainitun Kleinin neliryhmän $\mathcal{V} \lhd \mathcal{A}_4$. Mutta tässä on oletettu, että $m \geq 5$, joten on olemassa vielä alkio 5 ja siis esimerkiksi $(5, 3, 1) \in \mathcal{A}$. Toistetaan temppu vielä kerran: N:ssä on alkio

$$\begin{aligned}(5,3,1)^{-1}(1,3)(2,4)(5,3,1)((1,3)(2,4))^{-1} &= \\ &= (1,3,5)(1,3)(2,4)(5,3,1)(2,4)(1,3) = \\ &= (1,3,5)(1,3)(5,3,1)(2,4)(2,4)(1,3) = \\ &= (1,3,5)(1,3)(5,3,1)(1,3) = \\ &= (1,5,3)\end{aligned}$$

vastoin tämän kohdan oletusta. □

Täydellisyyden vuoksi mainitaan, että tapauksissa $m = 1, 2, 3$ ja 4 käy seuraavasti:

(1) $\mathcal{A}_2$ on yksialkioinen, siis $\sim \{e\}$. Tätä ei ole tapana pitää yksinkertaisena ryhmänä.

(2) $\mathcal{A}_3$ on kolmialkioinen, joten sillä ei ole ei triviaaleja aliryhmiä ollenkaan. Se on yksinkertainen abelin ryhmä.

(3) $\mathcal{A}_4$ ei ole yksinkertainen, koska Kleinin neliryhmä on sen normaali aliryhmä. Muita ei olekaan, mikä todistetaan oleellisesti kuten edellinen lause, mutta helpommalla vaivalla.

Jo Galois todisti, että $\mathcal{A}_5$ on pienin yksinkertainen epäkommutatiivinen ryhmä. Välittömänä seurauksena lauseesta 5.35. saadaan:

5.36. Lause. *Symmetrinen ryhmä $\mathcal{S}_n$ ei ole ratkeava, kun $n \geq 5$.*

Todistus. Muuten sen aliryhmä $\mathcal{A}_n$ olisi lauseen 5.29. mukaan ratkeava, mutta sitä se ei ole, vaan yksinkertainen. □

$p-$ryhmät.

5.37. Määritelmä.

(1) ryhmän G alkiot a ja b ovat *konjugoidut,* mikäli

$$a = g^{-1}bg$$

jollekin $g \in G$.

(2) Konjugointi on ekvivalenssirelaatio. Ekvivalenssiluokkia sanotaan G:n *konjugointiluokiksi* $G_1, G_2, \ldots$.

5.38. Lause.

(1) *Ykkösalkion sisältävä konjugointiluokka on $G_1 = \{e\}$.*
(2) $\#G = 1 + \#G_2 + \#G_3 + \#G_4 + \ldots$ *(G:n luokkayhtälö)*

5.39. Määritelmä. Alkion $x \in G$ *keskittäjä* on G:n aliryhmä

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

5.40. Lause.

$$\overbrace{\#\{G{:}n\ C_G(x){-}sivuluokat\}}^{C_G(x)\text{:n indeksi}} = \#\ \overbrace{\{g^{-1}xg \,|\, g \in G\}}^{x{:}nkonjugointiluokka}\ .$$

Todistus. Alkiot g ja $h \in G$ kuuluvat samaan oikeanpuoleiseen sivuluokkaan $\in \frac{G}{C_G(x)}$ jos ja vain jos

$$\begin{aligned} hg^{-1} &\in C_G(x), \\ hg^{-1}x &= xhg^{-1} \text{ , eli} \\ g^{-1}xg &= h^{-1}xh \in \{g^{-1}xg \,|\, g \in G\}. \end{aligned}$$

Tunnetusti aliryhmän vasempia ja oikeita sivuluokkia on yhtä monta. Keskittäjän oikeanpuoliset sivuluokat ja konjugointiluokan eri alkiot vastaavat siis toisiaan bijektiivisesti. □

Huomaa, että konjugointiluokat voivat olla eri kokoisia, mutta edellinen lause takaa, että kunkin konjugointiluokan alkioiden lukumäärä on koko G:n kertaluvun tekijä.

5.41. Määritelmä. Olkoon p alkuluku. Ryhmä G on *$p-$ryhmä,* mikäli sen kertaluku on p:n potenssi.

5.42. Esimerkki.

(1) Kleinin neliryhmä $\mathcal{V}$ on $2-$ryhmä.
(2) Symmetrinen ryhmä S_n, ei ole $p-$ryhmä millekään p kun $n \geq 3$.

5.43. Määritelmä. Ryhmän G *keskus* on normaali kommutatiivinen aliryhmä

$$Z(G) = \{x \in G \,|\, xg = gx \ \forall g \in G\}.$$

5.44. Lause.

(1) *Abelin ryhmän keskus on koko ryhmä.*
(2) $Z(\mathcal{S}_3) = \{e\}$.
(3) $x \in Z(G) \iff$ *x:n konjugointiluokka on pelkkä* $\{x\}$.
(4) *$p-$ryhmän* $G \neq \{e\}$ *keskus ei ole pelkkä* $\{e\}$.

Todistus. Kaksi ensimmäistä väitettä ovat triviaaleja. Väitettä (3) varten huomataan, että

$$\begin{aligned} \{x\} = \{g^{-1}xg \,|\, g \in G\} &\text{ merkitsee, että} \\ x = g^{-1}xg \quad &\forall g \in G. \end{aligned}$$

Kohta (4) on varsinainen asia. G:n luokkayhtälö on

$$p^n = \#G = 1 + \#G_2 + \cdots + \#G_r.$$

Toisaalta konjugointiluokkien kertaluvut ovat p^n:n tekijöitä, siis itsekin muotoa

$$\#C_j = p^{n_j}, \quad n_j \in \mathbf{N} \cup \{0\}.$$

Oikealla puolella täytyy siis esiintyä yksialkioisia konjugointiluokkia, itse asiassa ainakin $p-1$ kappaletta; joka tapauksessa siis ainakin yksi neutraalista eroava $x \in G$ kuuluu tällaiseen. Mutta tällöin kohdan (3) nojalla $x \in Z(G) \setminus \{e\}$. $\square$

5.45. Lause. *Olkoon G $p-$ryhmä kertalukua p^n. Silloin G:llä on jono* **G:n normaaleja** *aliryhmiä*

$$\{e\} = G_0 \lhd G_1 \lhd G_2 \cdots \lhd G_n = G,$$

siten, että

$$\#G_j = p^j$$

kaikilla $j = 0, \ldots, n$. Erityisesti $p-$ryhmä siis on ratkeava.

Todistus. Tehdään induktio. Tapaus $n = 0$ on selvä. Yleisessä tapauksessa tarkastellaan G:n keskusta

$$\{e\} \neq Z(G) \lhd G.$$

Se on kertaluvun p^m abelin ryhmä. Sellaisessa on aina kertaluvun p alkio, ts. on olemassa $x \in Z(G)$, jonka generoima aliryhmä K on tasan $p-$alkioinen, sillä mikä tahansa sellaisen abelin ryhmän alkio y generoi **syklisen** aliryhmän, jonka kertaluku myös on p:n potenssi. Keskuksen aliryhmänä myös K on G:n normaali aliryhmä. Ryhmä $\frac{G}{K}$ on $p-$ryhmä, jonka kertaluku on p^{n-1}. Induktio-oletuksen nojalla tilanne on siis tämä:

$$\frac{K}{K} \lhd \frac{G_1}{K} \lhd \cdots \lhd \frac{G_{n-1}}{K} = \frac{G}{K},$$

vieläpä siten, että kaikki ovat $\frac{G}{K}$:n normaaleja aliryhmiä ja

$$\#\frac{G_j}{K} = p^j$$

kaikilla $j = 1, \ldots, n-1$.

Näin ollen $\#G_j = p^{j+1}\, \forall j = 1, \ldots, n-1$, ja myös jokainen G_j on G:n normaali aliryhmä. Lisäämällä jonon alkuun $G_0 = \{e\}$ saadaan haluttu jono.

Viimeinen väite seuraa siitä, että esiintyvät tekijäryhmät $\frac{G_{j+1}}{G_j}$ovat alkulukukertalukua p, siis syklisinä abelin ryhmiä. $\square$

Sylowin lause.

5.46 Lause (L. Sylow[21] 1872). *Olkoon ryhmän G kertaluku $\#G = p^\alpha r$, missä p on alkuluku, mutta ei r:n tekijä. Tällöin*

(1) *Jossakin G:n aliryhmässä on tasan p^α alkiota. Tällaista sanotaan $p-$Sylow–aliryhmäksi.*
(2) *Kaikki $p-$Sylow–aliryhmät saadaan toisistaan konjugoimalla.*
(3) *Jokainen G:n $p-$alkioinen aliryhmä sisältyy johonkin $p-$Sylow–aliryhmään.*
(4) $\#\{A \Subset G \,|\, \#A = p^\alpha\} \equiv 1 \,(mod p)$

[21] On olemassa muitakin samaan aihepiiriin liittyviä Sylowin lauseita. Ludwig Sylow (1832-1918), oli norjalainen kuten Abel ja hänen maanmiehensä Sophus Liekin.

Todistus. Todistamme induktiolla vain kohdan (1), jota jatkossa tarvitaan. $\#G = n$. Lause pätee, kun $n = 1$ tai 2. Yleisessä tapauksessa tarkastelemme luokkayhtälöä

$$\#G = \#G_1 + \cdots + \#G_s, \text{ eli lyhyesti}$$
$$(*) \qquad p^\alpha r = c_1 + \cdots + c_s.$$

Olkoon $x_j \in G_j$, $Z_j = x_j$:n keskittäjä, ja $n_j = \#Z_j$ kullekin $j = 1, \ldots, s$. Indeksiä koskevan lauseen 5.40. mukaan

$$(**) \qquad n_j = \frac{p^\alpha r}{c_j} \, \forall j = 1, \ldots, s.$$

Voimme olettaa, että jokainen c_j on joko 1 tai p:n monikerta. Jos näin ei olisi, niin olisi nimittäin jokin $c_j > 1$ p:llä jaoton. Kaavan $(**)$ mukaan olisi siis

$$\#Z_j = n_j = p^\alpha \frac{r}{c_j} < p^\alpha r = n, \text{ ja}$$
$$\frac{r}{c_j} \text{ jaoton } p\text{:llä.}$$

Induktio-oletuksen mukaan tällainen Z_j sisältäisi $p^\alpha-$alkioisen aliryhmän, joka siis olisi G:n $p-$Sylow–aliryhmä ja lause olisi todistettu. Jää tapaus, jossa luokkayhtälön $(*)$ oikealla puolella on summa vain ykkösistä ja p:n monikerroista. Olkoon ykkösiä z kappaletta. Lauseen 5.44.(3) mukaan $z = \#(Z(G))$. Luokkayhtälö $(*)$ saa muodon

$$p^\alpha r = 1 + \cdots + 1 + kp = z + kp$$

jollekin $k \in \mathbf{N}$. z on siis jaollinen p:llä, joten keskus $Z(G)$ ei ole yksialkioinen, vaan jopa p jakaa sen kertaluvun $z = \#(Z(G))$. Nytpä pätee, että abelin ryhmällä, jonka kertaluvun jakaa alkuluku p, on aina olemassa kertaluvun p alkio, siis sellainen, joka generoi $p-$alkioisen syklisen aliryhmän. Perustelemme tämän kohta, mutta käytämme sitä ensin. Sen mukaan $Z(G)$:llä on $p-$alkioinen syklinen aliryhmä P. Keskuksen määritelmän nojalla $P \lhd G$. Nyt

$$\#\frac{G}{P} = p^{\alpha-1} r,$$

joten induktio-oletus sanoo, että $\#\frac{G}{P}$:llä on olemassa kertaluvun $p^{\alpha-1}$ aliryhmä $\#\frac{S}{P}$. Tällöin S on G:n aliryhmä, jolle $\#S = p^\alpha$.

Lause on todistettu, kun vielä todistetaan yllä käyttämämme abelin ryhmien syklisiä aliryhmiä koskeva väite, eli

5.47. Lemma. *Olkoon G abelin ryhmä ja sen kertaluku $\#G$ jaollinen alkuluvulla p. Silloin G:ssä on kertaluvun p alkio.*

Todistus. Teemme jälleen kerran induktiopäättelyn kertaluvun $n = \#G$ suhteen. Tapaukset $n = 1, 2$, ja 3 ovat triviaaleja, päteehän lause tietysti aina, kun n itse on alkuluku. Jos n ei ole alkuluku, niin G:llä on epätriviaali aliryhmä, sillä G on joko epäsyklinen tai sitten syklinen kertalukua, joka ei ole alkuluku. Olkoon kertaluvultaan suurin epätriviaali aliryhmä $M \Subset G$, $m = \#M$. Olkoon $t \in G \setminus M$ ja olkoon T sen generoima syklinen aliryhmä. Silloin MT on abelin ryhmän G aliryhmä, ja aidosti maksimaalista aliryhmää M suurempana siis koko G. Ensimmäisen isomorfialauseen 5.30.(1) nojalla

$$\frac{M}{M \cap T} \sim \frac{MT}{T} = \frac{G}{T} \quad \text{ja siis}$$
$$m\#(T) = n\#(M \cap T), \quad p\text{:llä jaollinen.}$$

Siispä p on joko m:n tai $\#T$:n alkutekijä. Koska $m < n$, niin induktio-oletus kertoo, että ensin mainitussa tapauksessa on olemassa kertaluvun p alkio $g \in M \subset G$, kuten halutaankin. Jälkimmäisessä tapauksessa taas T:n alkiolla $t^{\frac{\#T}{p}}$ on kertaluku p. □

Tämän lemman oletuksista voi sen avulla todistetun Sylowin lauseen avulla jälkiviisaasti karsia kommutatiivisuuden[22].

5.48. Lause (Cauchy). *Olkoon G mikä tahansa ryhmä ja p sen kertaluvun $\#G$ alkutekijä. Silloin G:ssä on kertaluvun p alkio.*

Todistus. Sylowin lauseen mukaan on olemassa G:n $p-$Sylow-aliryhmä. Olkoon se $H \neq \{0\}$. Sylowin lauseen 5.46. mukaan H:lla on mm. $p-$alkioinen aliryhmä. Koska p on alkuluku, aliryhmä on syklinen. □

5.49. Esimerkki Sylowin lauseen tilanteesta. Tarkastellaan symmetristä ryhmää $\mathcal{S}_4$. Sen kertaluku on $\#\mathcal{S}_4 = 4! = 24 = 2^3 \times 3 = 3^1 \times 8$. Sylowin aliryhmien kertalukuina esiintyvät siis lauseen mukaan 3 ja 8. Tällaisia voikin suoraan löytää: mikä tahansa $3-$kierto, vaikkapa $(1, 2, 3) \in \mathcal{S}_4$ generoi sellaisen. Kertaluku 8 on vähemmän itsestäänselvä. Kleinin neliryhmä $\mathcal{V}$ on $\mathcal{S}_4$:n normaali aliryhmä. Olkoon $t \in \mathcal{S}_4$ transpositio. Sen generoimassa aliryhmässä T on kaksi alkiota ja sen ja $\mathcal{V}$:n yhdessä generoimassa ryhmässä $\mathcal{V}T$ 8.

Sylowin lause ei päde ilman oletusta, että p on alkuluku. Esimerkin tästä antaa alternoiva ryhmä $\mathcal{A}_5$, jolla ei itse asiassa ole kertaluvun 15 aliryhmää, vaikka $\#\mathcal{A}_5 = \frac{1}{2}5! = 60$ ja $15 = 15^1$.

[22] Cauchyn tulos on Sylowin lausetta vanhempi ja siis alun perin todistettu eri tavalla.

Cardanon kaava. Polynomiyhtälön

$$a_n x^n + \cdots + a_1 x + a_0 = 0$$

ratkaiseminen on algebran klassinen ongelma. Muinaiset egyptiläiset ja babylonialaiset selvisivät ensimmäisen, pitkälti myös toisen asteen yhtälöistä. Cardanon kaavana tunnettu kolmannen asteen yhtälön ratkaisu on peräisin renessanssin Italiasta, varsinaisena keksijänään ilmeisesti bolognalainen matemaatikko Scipione del FERRO ja tästä lähes riippumatta Niccolo Fontana, lisänimeltä TARTAGLIA. Girolamo CARDANO puolestaan oli monipuolinen luonnontieteilijä ja "lääkäri", joka Tartaglian harmiksi julkaisi kaavan kirjassaan "Ars Magna" (1545), väittämättä sentään sitä itse keksineensä. Neljännen asteen yhtälö palautuu kolmannen asteen yhtälöön, minkä huomasi samassa yhteydessä Cardanon oppilas Ludovico FERRARI. Myös tämän idea julkaistiin Ars Magnassa lupaa kysymättä.

Ratkaisukaavat antavat lausekkeen juurille kertoimien funktioina, ja muodostuvat äärellisestä määrästä kunnan laskutoimituksia **ja n:nsien juurten ottoja**. Esimerkiksi kolmannen asteen yhtälö palautuu muotoon

$$x^3 + px + q = 0$$

siirtämällä aluksi origo kuutioparabelin käännepisteen alle, siis kohtaan joka löytyy ratkaisemalla ensimmäisen asteen yhtälö. Nyt ratkaisun antaa kaava[23]

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}},$$

missä eri vaihtoehdot syntyvät kompleksisten kuutiojuurten valinnoista. Neljännen asteen yhtälön ratkaisu tapahtuu tämän jälkeen huomaamalla, että myös sen toiseksi korkein termi on melko helppo eliminoida, jolloin saadaan

$$x^4 + px^2 + qx + r = 0,$$

joka on yhtäpitävää sen kanssa, että kaikille $t \in \mathbf{R}$

$$(x^2 + t)^2 = (2t - p)x^2 - qx + (t^2 - r).$$

[23] Cardanon kaava johdetaan mm. Tapani Kuusalon monisteessa Kompleksianalyysi. Klinen historiankirjassa kaavojen alkuperäisiä muotoja käsitellään seikkaperäisesti.

Tämän oikea puoli on muotoa $(x-a)^2$ – jolloin yhtälö ratkeaakin helposti – kunhan diskriminantti häviää:

$$(*) \qquad 4(2t-p)(t^2-r)-q^2=0.$$

Viimeisin yhtälö on kolmatta astetta t:lle.

Viidennen ja korkeamman asteen yhtälöiden ratkaisukaavaa etsittiin lähes kolmesataa vuotta, kunnes norjalainen Niels Henrik ABEL vuonna 1824 LAGRANGEn esitöiden pohjalta todisti, että sellaista ei ole olemassa. (RUFFINIn hyvää yritystä Abel ei tuntenut.) Ongelmaksi jäi löytää yhtenäinen tapa saada selville, mitkä yhtälöt ovat "algebrallisesti ratkeavia", mitkä eivät. Evariste GALOIS selvitti täydellisesti tämän puolen kolme vuotta sen jälkeen kun Abel oli kuollut tuberkuloosiin vuonna 1829, mutta hänen lauseensa, jonka mukaan yhtälö on ratkeava aina ja vain, kun polynomin hajoituskunnan Galois'n ryhmä on ratkeava[24], tuli julki vasta 1843, yksitoista vuotta Galois'n ennenaikaisen kuoleman[25] jälkeen.

Esitämme todistuksen Abelin tulokselle käyttäen Galois'n menetelmiä. Aloitamme sanomalla täsmällisesti, mitä ovat algebrallisesti ratkeavat polynomiyhtälöt. **Seuraavassa on kaikkien tarkasteltavien kuntien karakteristika yksinkertaisuuden vuoksi 0.**

Juurilaajennus.

6.1. Määritelmä. Kuntalaajennus $L:K$ on *radikaali–,* eli *juurilaajennus*, mikäli

$$L=K(\alpha_1,\ldots,\alpha_m) \text{ ja on olemassa } n_2,\ldots,n_m\in\mathbf{N}, \textit{ joilla}$$
$$(\alpha_j)^{n_j}\in K(\alpha_1,\ldots,\alpha_{j-1}) \quad \forall j\in\{2,\ldots,m\}.$$

Jono $\alpha_1,\ldots,\alpha_m$ on juurilaajennuksen $L:K$ *juurijono.*

Määritelmä merkitsee, että L saadaan K:sta adjungoimalla siihen yksi kerrallaan äärellinen määrä aikaisempien alkioiden n:nsiä juuria. Kunnan L alkiot ovat siis etsimiemme kaavojen kaltaisia lausekkeita K:n alkioista.

[24] Aina-puoli edellyttää, että kunnan karakteristika on 0. On jopa olemassa toisen asteen ratkeamaton yhtälö, jonka Galois'n ryhmä on peräti kommutatiivinen.

[25] Evariste Galois oli **radikaali** tasavaltalainen ja kuoli 20–vuotiaana mahdollisesti poliittiseksi epäillyssä hämärissä olosuhteissa käydyssä kaksintaistelussa. Hänen elämästään on muodostunut legenda; kauneimmillaan se on esitettynä E.T. Bellin kirjassa Matematiikan miehiä. Tarinan takana olevia tosiasioita ruoditaan Rothmanin artikkelissa [10].

6.2. Määritelmä. Polynomi $P \in K[X]$ on *juurin ratkeava*, mikäli on olemassa K:n juurilaajennus M, joka sisältää P:n hajoituskunnan Σ.

Määritelmä merkitsee, että P:n kaikki juuret ovat lausuttavissa halutunlaisina kaavoina. Kunnan M ei tietenkään tarvitse olla itse Σ. Juurilaajennuksen välikunnat eivät aina ole juurilaajennuksia. Todistamme seuraavassa, että juurin ratkeavan polynomin hajoituskunnan Galois'n

ryhmä $\Gamma(\Sigma : K)$ on ratkeava. Todistuksen pääkohdat sisältyvät seuraavaan lauseeseen:

6.3. Lause. *Olkoon $L : K$ normaali juurilaajennus. Galois'n ryhmä $\Gamma(L : K)$ on ratkeava.*

Todistus. Todistus on **idealtaan** suoraviivainen: Juurilaajennus muodostuu jonosta laajennuksia, joissa kussakin lisätään yksi k:n n:s juuri. Sellaisella on kommutatiivinen Galois'n ryhmä. Ratkeava ryhmä taas koostuu jonosta kommutatiivisia ryhmiä. Yksityiskohdissa on kuitenkin näpertämistä; joudumme käyttämään tehokkaasti ratkeavuuden säilymisominaisuuksia.

Juurilaajennusoletus merkitsee, että

$$\begin{aligned} &L = K(\alpha_1, \ldots, \alpha_m) \text{ ja on olemassa } n_1, \ldots, n_m \in \mathbf{N}, \text{ joilla} \\ &(\alpha_1)^{n_1} \in K \text{ ja} \\ &(\alpha_j)^{n_j} \in K(\alpha_1, \ldots, \alpha_{j-1}) \quad \forall j \in \{2, \ldots, m\}. \end{aligned}$$

Tässä jonossa voi ilman muuta olettaa, että jokainen luku n_j on alkuluku, sillä tähän päästään lisäämällä juurijonoon tarvittaessa α:n alempia juuria, onhan esimerkiksi

$$\sqrt[6]{x} = \sqrt[3]{\sqrt{x}}.$$

Erityisesti siis on olemassa alkuluku p, jolle $\alpha_1^p \in K$. Joudumme ottamaan käyttöön apukunnat

$$\begin{aligned} \Omega_L &= L(\omega_0, \ldots, \omega_{p-1}) \text{ ja} \\ \Omega_K &= K(\omega_0, \ldots, \omega_{p-1}), \end{aligned}$$

missä $\omega_0, \ldots, \omega_{p-1}$ ovat polynomin $X^p - 1$ nollakohdat eli ykkösen n:nnet juuret. Tarkastelemme kahta kaksivaiheista kuntalaajennusta.

$$\begin{array}{ccc} & \Omega_L & \\ L & & \Omega_K \\ & K & \end{array}$$

Tavoitteena on todistaa, että $\Gamma(L : K)$ on ratkeava. Käytämme periytymislauseita 5.29. ja Galois'n päälauseen 4.43. mukaisia yhteyksiä

$$\Gamma(L : K) = \frac{\Gamma(\Omega_L : K)}{\Gamma(\Omega_L : L)}, \tag{1}$$

$$\Gamma(\Omega_K : K) = \frac{\Gamma(\Omega_L : K)}{\Gamma(\Omega_L : \Omega_K)}, \tag{2}$$

jotka pätevät, koska oletuksen mukaan $L : K$ ja hajoituskuntana $\Omega_K : K$ ovat normaaleja kuntalaajennuksia. Yhtälö (1) osoittaa, että riittää todistaa $\Gamma(\Omega_L : K)$ ratkeavaksi. Yhtälön (2) mukaan taas tälle riittää, että $\Gamma(\Omega_K : K)$ ja $\Gamma(\Omega_L : \Omega_K)$ ratkeavat. Todistamme sen.

Osoitamme aluksi, että $\Gamma(\Omega_K : K)$ on jopa abelin ryhmä: Ω_K saadaan K:sta adjungoimalla siihen ykkösen juuret $\omega_0, \ldots, \omega_{p-1}$. Kuten klassisessa tapauksessa $K = \mathbf{Q}$ ovat ne lauseen 4.18. mukaisesti yleisessäkin karakteristikan 0 tapauksessa erillisiä, eihän polynomilla $X^p - 1$ ja sen derivaatalla pX^{p-1} ole yhteisiä tekijöitä. Ykkösen juuret muodostavat kunnassa Ω_K multiplikatiivisen aliryhmän. Juurten erillisyyden vuoksi tämä ryhmä on alkulukukertalukua p ja siis syklinen: ykkösen juuret ovat $\omega_1, \omega_1^2, \ldots, \omega_1^{p-1}$ ja $\omega_1^p = \omega_p = \omega_0 = 1$. Kunnan $\Omega_K = K(\omega_1)$ $K-$automorfismi $A_k \in \Gamma(\Omega_K : K)$ määräytyy vaikutuksestaan juureen ω_1, jonka kuva on jokin juurista $\omega_1, \ldots, \omega_1^p = 1$.

$$A_k(\omega_1) = \omega_k \,\forall\, k = 1, \ldots, p.$$

Tällaiset automorfismit A_k kommutoivat.

Jää todistettavaksi, että myös $\Gamma(\Omega_L : \Omega_K)$ on ratkeava. Muistetaan merkinnät:

$$\begin{aligned} L &= K(\alpha_1, \ldots, \alpha_m), \\ \Omega_K &= K(\omega_0, \ldots, \omega_{p-1}), \\ \Omega_L &= L(\omega_0, \ldots, \omega_{p-1}). \end{aligned}$$

Tutkittava laajennus $\Omega_L : \Omega_K$ jakautuu vaiheiksi

$$\Omega_K \quad \subset \quad \Omega_K(\alpha_1) \quad \subset \quad \Omega_L.$$

Koska $L : K$ on äärellinen ja normaali, on L lauseen 4.13. mukaan jonkin polynomin $P \in K[X]$ hajoituskunta. $\Omega_L = \Omega_K(\alpha_1)(\alpha_2, \ldots, \alpha_m)$ on saman polynomin $P \in \Omega_K(\alpha_1)[X]$ hajoituskunta, joten laajennus $\Omega_L : \Omega_K(\alpha_1)$ on normaali. Koska separoituvuus on automaattista karakteristikan 0 tapauksessa on Galois'n päälauseen 4.43. mukaan

$$\Gamma(\Omega_K(\alpha_1) : \Omega_K) = \frac{\Gamma(\Omega_L : \Omega_K)}{\Gamma(\Omega_L : \Omega_K(\alpha_1))}.$$

$\Gamma(\Omega_L : \Omega_K)$ on siis ratkeava, mikäli molemmat Galois'n ryhmät $\Gamma(\Omega_L : \Omega_K(\alpha_1))$ ja $\Gamma(\Omega_K(\alpha_1) : \Omega_K)$ ovat ratkeavia. Osoitamme, että ne sitä ovat.

$\Gamma(\Omega_L : \Omega_K(\alpha_1))$:n ratkeavuustodistus on induktio jonon pituuden m suhteen. Voimme tehdä induktio-oletuksen, että todistettavana olevan lauseen 6.3. väite pätee, kun tutkittavan normaalin kuntalaajennuksen juurijonossa on enintään $m-1$ termiä α_j. Laajennus $\Omega_L = \Omega_K(\alpha_1)(\alpha_2, \ldots, \alpha_m) : \Omega_K(\alpha_1)$ on juurilaajennus, jonka juurijono on alkuperäistä yhdellä lyhempi, sitä paitsi normaali. Induktio-oletuksen mukaan sen Galois'n ryhmä $\Gamma(\Omega_L : \Omega_K(\alpha_1))$ siis on ratkeava.

Toinen puolisko $\Omega_K(\alpha_1) : \Omega_K$ on sekin normaali laajennus, sillä $X^p - 1$ hajoaa Ω_K:ssä ja siis $X^p - \alpha_1^p$ hajoaa $\Omega_K(\alpha_1)$:ssä, joka näin ollen on Ω_K-polynomin $X^p - \alpha_1^p$ hajoituskunta, ovathan sen nollakohdat $\alpha_1\omega_1, \ldots, \alpha_1\omega_1^{(p-1)}$ ja $\alpha_1\omega_1^p = \alpha_1$. Samaa havaintoa käyttäen voi todistaa, että $\Gamma(\Omega_K(\alpha_1) : \Omega_K)$ on kommutatiivinen: $\Omega_K(\alpha_1)$:n Ω_K-automorfismi määräytyy nimittäin vaikutuksestaan α_1:een, jonka se kuvaa joksikin $X^p-\alpha_1^p$:n nollakohdaksi $\alpha_1\omega_1^k$. Kommutointi seuraa kuten edellä Galois'n ryhmää $\Gamma(\Omega_K, K)$ tutkittaessa.

$\Gamma(\Omega_L : \Omega_K)$ on siis ratkeava, mikä enää todistuksesta puuttuikin. $\square$

Päästäksemme polynomin hajoituskuntaa koskevaan tulokseen tarvitsemme pari lemmaa:

6.4. Lemma. *Olkoon $L : K$ äärellinen kuntalaajennus ja M sen normaali sulkeuma. Silloin on olemassa sellaiset $M : K$:n välikunnat*

$$L_1, \ldots, L_s,$$

että

(1) $M = K(L_1 \cup \cdots \cup L_s)$
(2) *Kaikki laajennukset $L_j : K$ ja $L : K$ ovat isomorfisia.*

Todistus. Todistus on helppo, koska käytettävissä on normaalin sulkeuman konstruktio 4.34. jonka samalla kertaamme. Äärellisenä laajennuksena L on vektoreiden $\alpha_1, \ldots, \alpha_r$ virittämä $K-$vektoriavaruus, missä alkiot $\alpha_1, \ldots, \alpha_r$ ovat algebrallisia. Merkitään α_k:n minimaalipolynomia $P_{\alpha_k} \in K[X]$. Kuntalaajennuksen $L : K$ normaali sulkeuma on polynomien tulon $P = P_{\alpha_1} \ldots P_{\alpha_r}$ hajoituskunta N. Saman laajennuksen normaaleina sulkeumina laajennukset $M : K$ ja $N : K$ ovat isomorfiset, ja voimme siis samaistaa ne: $M = N$. Hajoituskunnan yksikäsitteisyyttä koskevan lauseen 4.9. todistus osoittaa, että kun β_j on P_j:n nollakohta, niin laajennukset

$$K(\alpha_1, \ldots, \alpha_j, \ldots, \alpha_r) : K = L : K \text{ ja}$$
$$K(\alpha_1, \ldots, \beta_j, \ldots, \alpha_r) : K$$

ovat isomorfiset. Jälkimmäiset generoivat N:n, eli M:n, kun j ja β_j käyvät läpi kaikki mahdolliset arvot. $\square$

6.5. Lemma. *Juurilaajennuksen $L : K$ normaali sulkeuma M on juurilaajennus.*

Todistus. Tämä seuraa edellisestä Lemmasta: $M = K(L_1 \cup \cdots \cup L_s)$, missä kaikki laajennukset $L_j : K$ ja $L : K$ ovat isomorfisia, siis juurilaajennuksia. Riittää siis ilmeisesti todistaa, että kahden juurilaajennuksen $R : K$ ja $S : K$ yhdessä virittämä laajennus $K(R \cup S)$ on juurilaajennus. Olkoon niillä juurijonot $(\alpha_1, \ldots, \alpha_m)$ ja $(\beta_1, \ldots, \beta_n)$. Tällöin

$$(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n)$$

on juurijono $K(R \cup S)$:lle. $\square$

6.6. Lause. *Olkoon $M : K$ juurilaajennus ja Σ sen välikunta: $K \subset \Sigma \subset M$. Galois'n ryhmä $\Gamma(\Sigma : K)$ on ratkeava.*

Todistus. Palautamme väitteen lauseen 6.3. tilanteeseen. Suoraan määritelmän mukaan

$$\Gamma(\Sigma : K) = \Gamma(\Sigma : K_0),$$

missä K_0 on $\Gamma(\Sigma : K)$:n kiintopistekunta

$$K_0 = \{\sigma \in \Sigma \,|\, A(\sigma) = \sigma \forall A \in \Gamma(\Sigma : K)\}.$$

Todistammekin, että $\Gamma(\Sigma : K_0)$ on ratkeava. Tilanne on hieman alkuperäistä helpompi, sillä $\Sigma : K_0$ on **normaali** laajennus, koska K_0 on $\Gamma(\Sigma : K_0)$:n eli $\Gamma(\Sigma : K)$:n kiintopistekunta, ja normaalius on lauseen 4.41. mukaan välttämätöntä tälle Galois'n relaatiolle. Koska $K \subset K_0$, niin tietysti myös $M : K_0$ on juurilaajennus ja Σ sen välikunta:

$$K_0 \subset \Sigma \subset M.$$

Olkoon N kuntalaajennuksen $M : K_0$ normaali sulkeuma. Lemman 6.5. nojalla se on normaaliutensa ohella myös juurilaajennus, ja lause 6.3. soveltuu siis siihen, koska karakteristika 0 takaa separoituvuuden:

$$\Gamma(N : K_0) \text{ on ratkeava.}$$

Tutkittava Galois'n ryhmä $\Gamma(\Sigma : K_0)$ on Galois'n päälauseen 4.43 mukaan sen tekijäryhmä ja siis myös ratkeava. $\square$

Viidennen asteen yhtälö. Tarkoituksena on nyt antaa esimerkki viidennen asteen $\mathbf{Q}-$kertoimisesta polynomista, joka ei ole juurin ratkeava. Edellisen lauseen mukaan riittää, että sen hajoituskunnan Σ Galois'n ryhmä $\mathbf{Q}$:n suhteen ei ole ratkeava. Ratkeamattomksi tiedämme ainakin symmetriset ja alternoivat ryhmät, kun $n \geq 5$.

6.7. Lause. *Olkoon p alkuluku ja P jaoton asteen p $\mathbf{Q}-$kertoiminen polynomi. Jos P:llä on tasan kaksi ei reaalista juurta $\mathbf{C}$:ssä, niin sen hajoituskunnan Σ Galois'n ryhmä $\mathbf{Q}$:n suhteen on symmetrinen ryhmä $\mathcal{S}_p$.*

Todistus. Algebran peruslauseen mukaan P:llä on $\mathbf{C}$:hen sisältyvä hajoituskunta Σ. Koska P on jaoton ja karakteristika on 0, niin P:n nollakohdat ovat yksinkertaisia. Galois'n ryhmän $G = \Gamma(\Sigma : \mathbf{Q})$ alkiot määräytyvät vaikutuksistaan näihin nollakohtiin, joita ne permutoivat. Tässä mielessä Galois'n ryhmä on symmetrisen ryhmän $\mathcal{S}_p$ aliryhmä. Osoitamme, että se sisältää alkiot $(1, 2)$ ja $(1, 2, \ldots, p)$, jotka lauseen 5.7.(6) mukaan generoivat koko ryhmän $\mathcal{S}_p$.

Transposition löytämiseksi riittää huomata, että kompleksikonjugointi on $\mathbf{C}$:n $\mathbf{Q}-$automorfismi. P:n reaaliset juuret ovat sen kiintopisteitä. Kompleksiset juuret, joita on kaksi, kuvautuvat toisikseen, sillä reaalikertoimisen polynomin juuret ovat reaalisia tai parittain toistensa kompleksikonjugaatteja. Juurten kompleksikonjugointi on siten pelkkä transpositio ja numeroimalla juuret alkaen kompleksisista samaistamme sen transpositioon $(1, 2)$.

$p-$kierron $(1, 2, \ldots, p)$ löytämiseksi muistetaan, että lauseen 4.9. mukaisesti P:n hajoituskuntaa Σ konstruoitaessa kuntaan $\mathbf{Q}$ adjungoidaan aluksi P:n juuri α, jolloin laajennuksen $\mathbf{Q}(\alpha) : \mathbf{Q}$ aste on p ja koko laajennuksen $\Sigma : \mathbf{Q}$ aste siis sekin p:llä jaollinen. Galois'n päälauseen 4.43. mukaan tämä aste on Galois'n ryhmän kertaluku ja siis p jakaa $\#G$:n. Cauchyn lause 5.48. takaa nyt, että G:llä on $p-$alkioinen syklinen aliryhmä. Symmetrisen ryhmän ainoat kertaluvun p alkiot ovat $p-$kierrot. G:ssä on siis $p-$kierto. $(a1, a_2, \ldots, a_p)$, jossa voidaan valita $a_1 = 1$, jolloin $2 = a_\mu$ jollekin $\mu \in \{2, \ldots, p\}$. G:ssä on siis kierto

$$(1, a_2, \ldots, a_\mu = 2, \ldots, a_p)$$

ja näin ollen myös kierto

$$(1, a_2, \ldots, a_\mu = 2, \ldots, a_p)^{(\mu-1)} = (1, 2, b_3, \ldots, b_p),$$

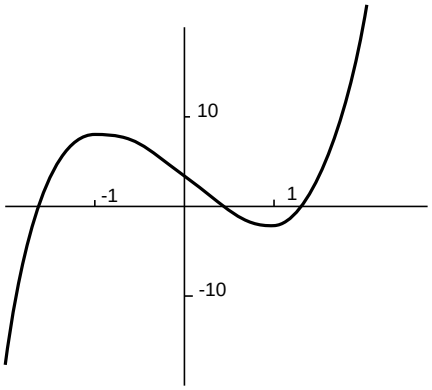
joka alkiot $b_3, \ldots, b_p$ uudelleen nimeämällä on haluttu kierto $(1, 2, \ldots, p)$. $\square$

6.8. Esimerkki (TÄTÄ ON ODOTETTU). Q−*polynomi*

$$P(X) = X^5 - 6X + 3$$

ei ole juurin ratkeava.

Todistus. Riittää tarkistaa, että P toteuttaa edellisen lemman 6.9. ehdot, sillä silloin sen hajoituskunnan Galois'n ryhmä $\mathbf{Q}$:n suhteen on $\mathcal{S}_5$, joka lauseen 5.36. mukaan ei ole ratkeava. Lause 6.6. estää tällöin P:n hajoituskuntaa olemasta juurilaajennus, mitä juuri väitetäänkin. P **on Q−polynomina jaoton**: Tämän näkee Eisensteinin ehdosta 1.20. mutta asian voi pienellä vaivannäöllä tarkistaa suoraankin kertoimia vertailemalla.



(2) P:llä on **tasan kaksi** kompleksista juurta, sillä reaalisia on kolme, kaikki yksinkertaisia. Sen derivaatalla $P'(X) = 5X^4 - 6$ on nimittäin kaksi reaalista nollakohtaa, $\pm\sqrt[4]{\frac{6}{5}}$, mikä takaa että itse reaalifunktiolla P ei ole kolmea enempää nollakohtia. Koska P:llä ei ole nollakohtia derivaattansa nollakohdissa, ovat reaaliset nollakohdat yksinkertaisia. Toisaalta niitä on ainakin kolme, koska $P(-2) = -17 < 0$, $P(-1) = 8 > 0$, $P(1) = -2 < 0$ ja $P(2) = 23 > 0$. Loput kaksi nollakohtaa ovat aidosti kompleksisia ja toistensa konjugaatteina eri kohtia. □

Symmetria ja ryhmä. Tutkiskellessamme algebrallisten yhtälöiden ratkeavuutta kiinnitimme huomiota polynomin juurien tuottamiin kuntalaajennuksiin ja niiden Galois'n ryhmiin. Ryhmät kuvaavat **symmetriaa**. Tämä ei ehkä heti ole ilmeistä ja siksi tässä kappaleessa on tarkoitus silmäillä millaisia ryhmiä liittyy aivan tavallisiin paperille piirrettyihin symmetrisiin kuvioihin.

Tasokuvioista.

7.1. Määritelmä. Olkoon $\mathcal{M}$ metrisen avaruuden $\mathbf{R}^2$, **euklidisen tason**, isometristen bijektioiden eli *(jäykkien) liikkeiden* joukko.

7.2. Lause. *$\mathcal{M}$ on ryhmä.*

Todistus. Isometrioista yhdistetty kuvaus on isometria, samoin isometrisen bijektion käänteinen.

□

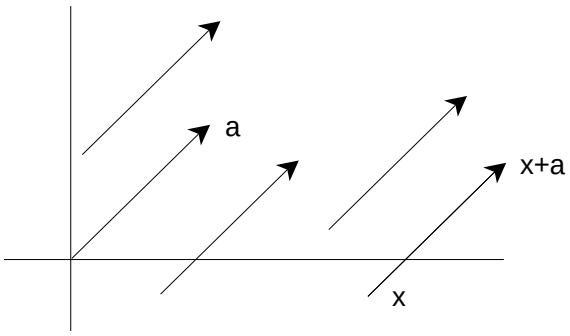
7.3. Huomautus. Euklidinen geometria käsittelee niitä tasokuvioiden ominaisuuksia, jotka ovat invariantteja ryhmän $\mathcal{M}$ kuvauksissa[26]. Tämä asia saa lisävalaistusta, kun ensin luokittelemme $\mathcal{M}$:n alkiot.

7.4. Lause. *Ainakin seuraavat ovat liikkeitä:*

(1) *Translaatiot eli siirrot*

$$T_a : x \mapsto x + a,$$

missä $a \in \mathbf{R}^2$.



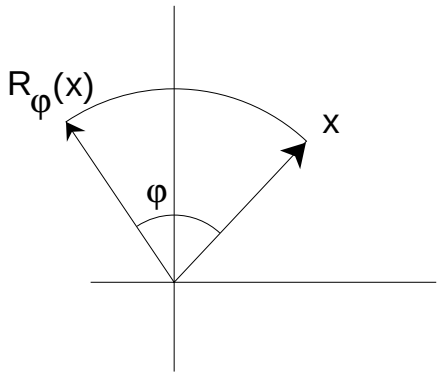
[26]Itse asiassa myös mittakaavan muutokset, homotetiat sallitaan.

(2) *Rotaatiot eli kierrot*

$$R_\varphi : x = (x_1, x_2) \mapsto R_\varphi x,$$

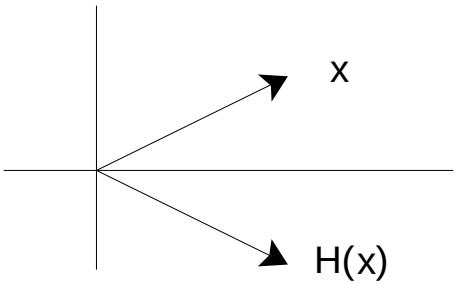
missä matriisi R_φ *on muotoa*

$$R_(\varphi) = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}.$$



(3) *Reflektio eli heijastus*

$$H : x = (x_1, x_2) \mapsto (x_1, -x_2)$$



(4) *Näistä yhdistetyt kuvaukset, joita ovat mm. heijastukset mielivaltaisten suorien suhteen ja kierrot mielivaltaisten pisteiden ympäri. (Katso lisäksi lause 7.7.)*

(5) *Muita ei ole.*

Todistus. Vain kohta (5) on hieman epätriviaali. Todistamme siitä saman tien n-ulotteisen version. Olkoon $f : \mathbf{R}^n \to \mathbf{R}^n$ isometrinen bijektio, siis

$$||f(x) - f(y)|| = ||x - y|| \quad \forall x, y \in \mathbf{R}^n.$$

Yhdistetään siihen translaatio $T_{-f(0)}$. Näin saadaan isometrinen bijektio $T_{-f(0)} \circ f$, jolle 0 on kiintopiste. Riittää todistaa, että **se** on yhdistetty

kuvaus kierrosta ja heijastuksesta H. Voimme siis olettaa, että $f(0) = 0$, jolloin erityisesti

$$||f(x)|| = ||x|| \quad \forall x \in \mathbf{R}^n.$$

Lineaarialgebrasta muistamme määritelmän, jonka mukaan $\mathbf{R}^n$:n **lineaarikuvaus**, joka säilyttää normin, on *ortogonaalinen*. Yhdistämällä kuvaukseen tarvittaessa heijastus saadaan sille determinantiksi positiiviluku, itse asiassa $+1$, jolloin kuvaus säilyttää suunnistuksen. 2–, ja 3–ulotteisia suunnistuksen säilyttätäviä ortogonaalikuvauksia sanotaan kierroiksi; 2–ulotteisessa tilanteessa kierto on lauseessamme väitettyä muotoa[27].

Todistettavaksi jää siten vain se, että jokainen origon kiinnittävä isometrinen kuvaus $f : \mathbf{R}^n \to \mathbf{R}^n$ on lineaarinen. Tämä seuraa siitä, että se ensinnäkin säilyttää sisätulon $\mathbf{R}^n$:ssä, koska

$$\begin{aligned} ||x-y||^2 &= (x-y, x-y) = ||x||^2 - 2(x,y) + ||y||^2 \quad \forall x, y \in \mathbf{R}^n \\ \implies (f(x), f(y)) &= \frac{1}{2}(||f(x) - f(y)||^2 - ||f(x)||^2 - ||f(y)||^2) \\ &= \frac{1}{2}(||x-y||^2 - ||x||^2 - ||y||^2) \\ &= (x, y), \end{aligned}$$

ja toisekseen tällöin jokainen $f(\alpha x + \beta y) - \alpha f(x) - \beta f(y)$ on nolla, koska sen sisätulo mielivaltaisen alkion $f(z) \in \mathbf{R}^2$ (todella, kaikki R^n:n vektorit ovat tätä muotoa, koska f on surjektio.) kanssa häviää, onhan

$$\begin{aligned} &(f(\alpha x + \beta y) - \alpha f(x) - \beta f(y), f(z)) = \\ &= (f(\alpha x + \beta y), f(z)) - (f(\alpha x), f(z)) - (f(\beta y), f(z)) = \\ &= (\alpha x + \beta y, z) - (\alpha x, z) - (\beta y, z) = 0. \end{aligned}$$

□Olemme kiinnostuneita tasokuvioiden symmetriaominaisuuksista. Yhteyden ryhmiin antaa seuraava havainto:

7.5. Huomautus ja määritelmä. Olkoon $T \subset \mathbf{R}^2$ *tasokuvio*. Niiden liikkeiden $f \in \mathcal{M}$ joukko, joille T on *invariantti*,

$$G_T = \{f \in \mathcal{M} \big| \, f(T) = T\},$$

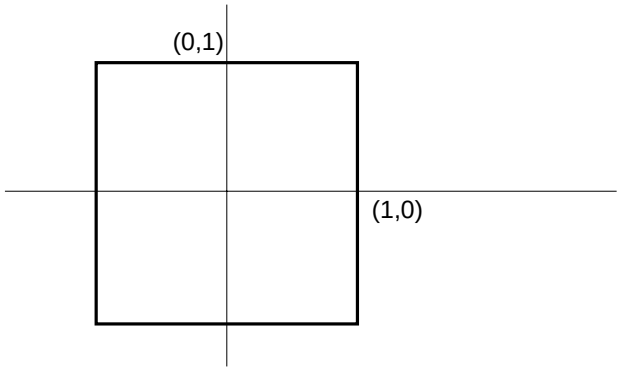
on ryhmän $\mathcal{M}$ aliryhmä. Se on nimeltään T:n *symmetriaryhmä*[28] G_T.

[27] 3–ulotteinen kiertomatriisi esitellään luvussa 8.

[28] Eri asia kuin symmetrinen ryhmä.

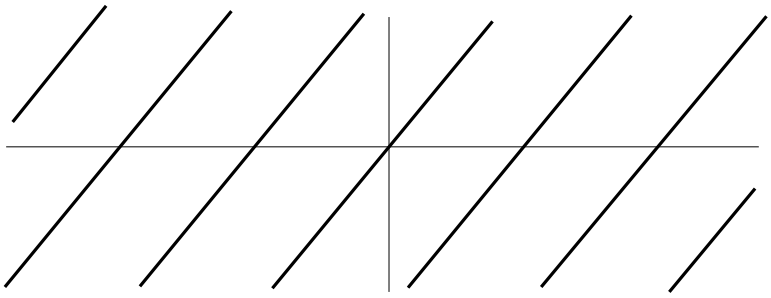
7.6. Esimerkkejä. (1) Olkoon T origokeskinen ympyrä. G_T muodostuu selvästikin kaikista niistä liikkeistä, joissa origo ei liiku. Se on siis ylinumeroituvasti ääretön ryhmä, jonka virittävät rotaatiot ja heijastus H.

(2) Olkoon T kuvan mukainen origokeskinen neliö. $T = [-1, 1]^2$.



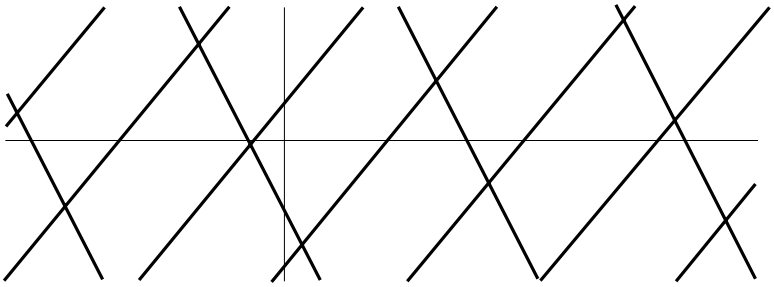
G_T muodostuu nyt vain rotaatioista $R_{\frac{\pi}{2}}, R_\pi, R_{\frac{3\pi}{2}}$, identtisestä kuvauksesta ja edellämainituista yhdistettynä heijastukseen. Se on siis äärellinen ryhmä, jonka virittävät rotaatio $R_{\frac{\pi}{2}}$ ja heijastus H.

(3) Olkoon T kuvan mukainen ääretön suoraparvi.



Ylinumeroituvasti ääretön ryhmä G_T muodostuu nyt kaikista suoraparven suuntaisista siirroista, niitä vastaan kohtisuorasta raidan leveyden pituisesta siirrosta, heijastuksesta parveen kuuluvan origon kautta kulkevan suoran suhteen, kierrosta R_π ja näistä yhdistetyistä kuvauksista.

(4) Olkoon T kuvan mukainen ääretön verkko.



Numeroituvasti ääretön ryhmä G_T muodostuu nyt kumpienkin suoraparvien suuntaisista verkkosuunnikkaan ao. sivun monikertojen mittaisista siirroista, kulman π suuruisista kierroista verkon solmukohtien suhteen ja näistä yhdistetyistä kuvauksista.

Esimerkeistä näkyy, että melko samankaltaisten kuvioiden symmetriaryhmät saattavat olla kovin erilaisia. Osoittautuu kuitenkin, että mahdollisia tasokuvioiden symmetriaryhmiä on olemassa vain vähän. Aluksi huomataan, että itse asiassa tason liikkeitäkin on vähemmän kuin saattaisi lauseen 7.4. valossa äkkisiltään luulla.

7.7. Lause. *Jokainen tason liike on jokin seuraavista*

(1) *Kierto jonkin pisteen ympäri*
(2) *Siirto*
(3) *Siirtoheijastus, eli siirto ja sen jälkeen heijastus siirron suuntaisen suoran, akselin suhteen.*

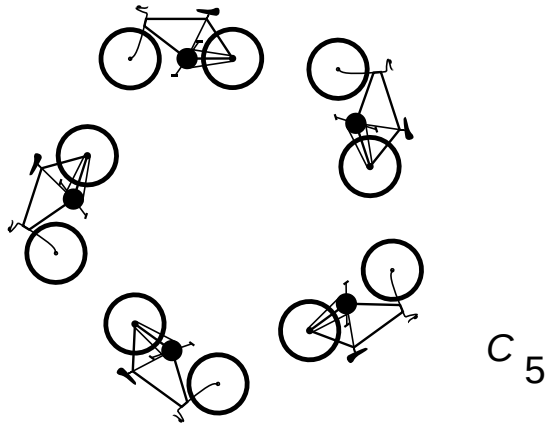
Erityisesti kierron ja heijastuksen yhdistelmä on aina siirtoheijastus

Todistus. Perustuu lauseeseen 7.4.(5). Kannattaa aluksi piirrellä kuvioita vakuuttuakseen lauseen todenperäisyydestä. Liikkeet voi heti jakaa suunnistuksen säilyttäviin ja kääntäviin.

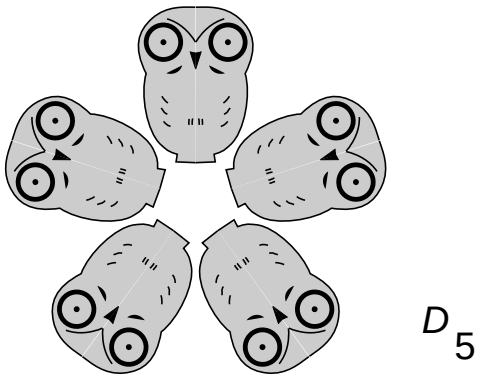
Kukat. Luokitellaan äärelliset tasokuvioiden symmetriaryhmät:

7.8. Lause (Leonardo da Vinci[29]). *Tasokuvion äärellinen symmetriaryhmä on aina jokin seuraavista*

(1) *syklinen ryhmä $\mathcal{C}_n$, joka muodostuu kierroista saman pisteen. kuvion symmetriakeskuksen suhteen, siis origon ollessa symmetriakeskuksena kuvauksista $R_\alpha, R_{2\alpha}, \ldots, R_{n\alpha} = R_0$, missä $\alpha = \frac{2\pi}{n}$. $\#(\mathcal{C}_n) = n$.*



(2) *dihedraalinen ryhmä $\mathcal{D}_n$, joka muodostuu edellä mainittujen lisäksi n:stä heijastuksesta symmetriakeskuksen kautta sopivasti sijoitetun säännöllisen n–kulmion kärkiin ja sivujen keskipisteisiin kulkevien suorien suhteen. $\#(\mathcal{D}_n) = 2n$. Huomaa pöllö-ja pyöräkuvioiden ero: pöllö on symmetrisempi.*



Todistus. Kuten edellinen.

□

[29]Leonardo keksi tämän lauseen suunnitellessaan symmetrisiä kirkkoja. Todistus ja ryhmäkäsite ovat tietysti myöhempiä.

Lukijan tehtäväksi jää – kuten moni muukin hauska asia tässä luvussa – muodostaa kertolaskutaulut joillekin dihedraalisille ryhmille. Siinä yhteydessä voi huomata esimerkiksi, että syklinen ryhmä $\mathcal{C}_2$ ja dihedraalinen ryhmä $\mathcal{D}_1$ ovat isomorfisia, mutta muodostuvat eri kuvauksista.

Näin on äärelliset tasokuvioiden symmetriaryhmät luokiteltu. Huomiota herättää, että niillä kaikilla on symmetriakeskus eli invariantti piste. Siksi niitä sanotaan tavallisesti *pisteryhmiksi*.

Sen 17 seinäpaperia. Alamme tarkastella äärettömiä tasokuvioiden symmetriaryhmiä. Nämä on tapana jakaa **diskreetteihin** ja **jatkuviin**.

7.9. Määritelmä.

(1) Olkoon $G \subset \mathcal{S}_E$ ryhmä joukon E bijektioita itselleen, laskutoimituksena kuvausten yhdistäminen. Alkion $x \in E$ *rata* on joukko

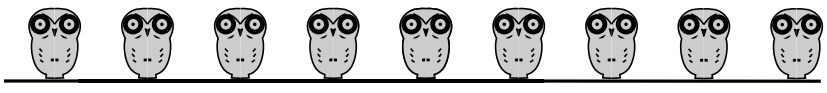
$$G(x) = \{g(x) \big| g \in G\}.$$

(2) Ryhmä avaruuden R^n bijektioita itselleen on *diskreetti*, mikäli mikään piste $x \in R^n$ ei ole ratansa kasautumispiste.

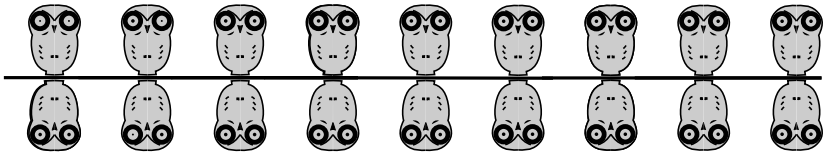
7.10. Esimerkkejä.

(1) Jokainen äärellinen ryhmä avaruuden R^n bijektioita itselleen on diskreetti. Koko symmetrinen ryhmä $\mathcal{S}_{R^n}$ ei ole diskreetti, ei liioin tason symmetriaryhmä $G_{\mathbf{R}^2}$.

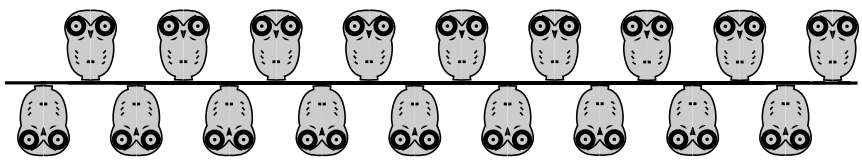
(2) Seuraavat ovat esimerkkejä tasokuvioista, joiden symmetriaryhmä on diskreetti, mutta ääretön:



(1)

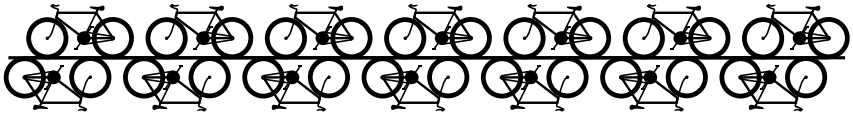


(2)

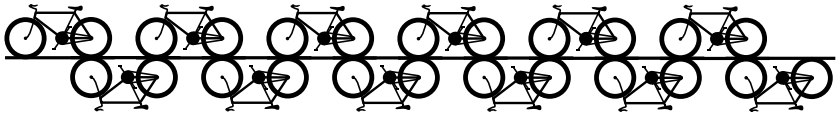


(3)

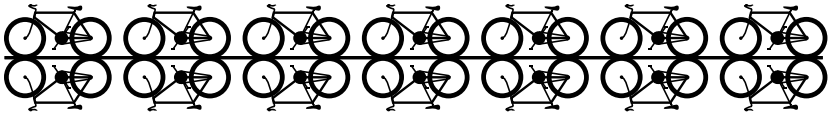
(4)



(5)



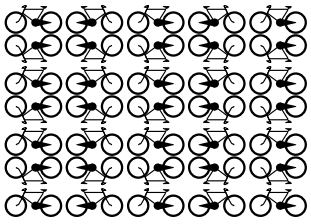
(6)



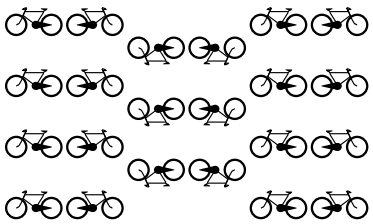
(7)

Kuvioiden (1) - (7) symmetriaryhmät jättävät erään suoran invariantiksi. Näitä sanotaan *friisiryhmiksi*. On olemassa täsmälleen yllä kuvatut 7 friisiryhmää. Seuraavien sivujen kuvioiden symmetriaryhmät eivät jätä mitään suoraa invariantiksi. Näitä ryhmiä sanomme *tapettiryhmiksi*. On olemassa vain kuvatut 17 tapettiryhmää (Fedorov 1891). Kaikkia on käytetty runsaasti ornamentiikassa[30].

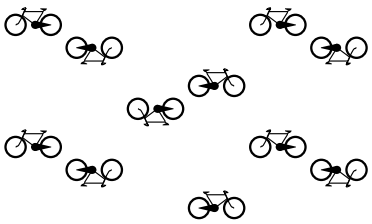
[30]Alhambran mosaiikeissa on 13 eri symmetriaa, Toledosta löytyy vielä kaksi lisää.



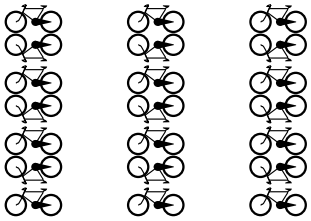
1. p2mm



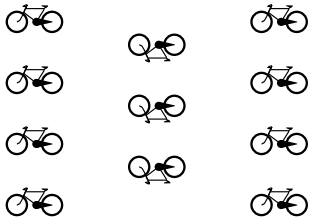
2. p2gm



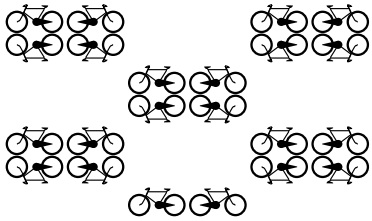
3. p2gg



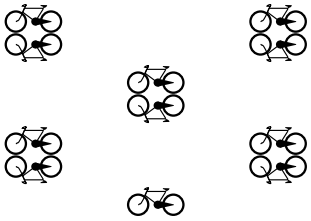
4. p11m



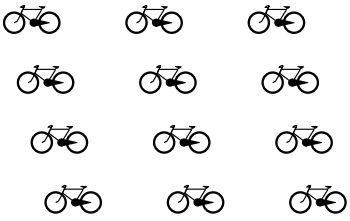
5. p1g



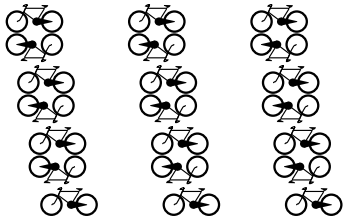
6. c2mm



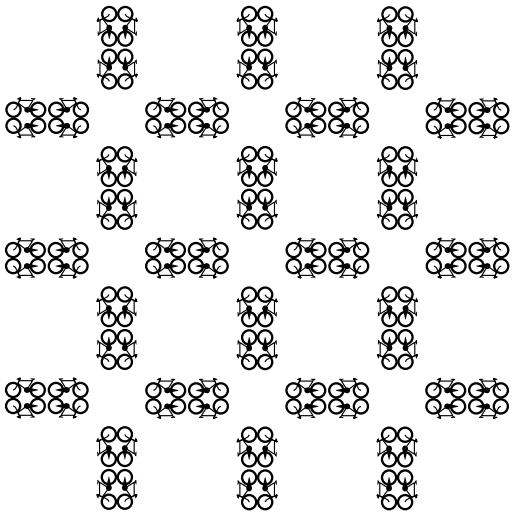
7. c11m



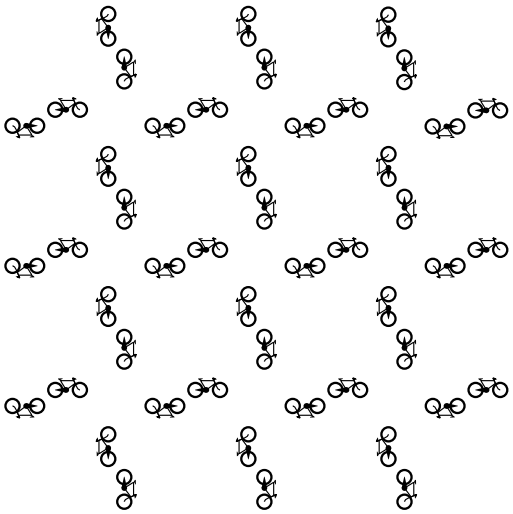
8. p1



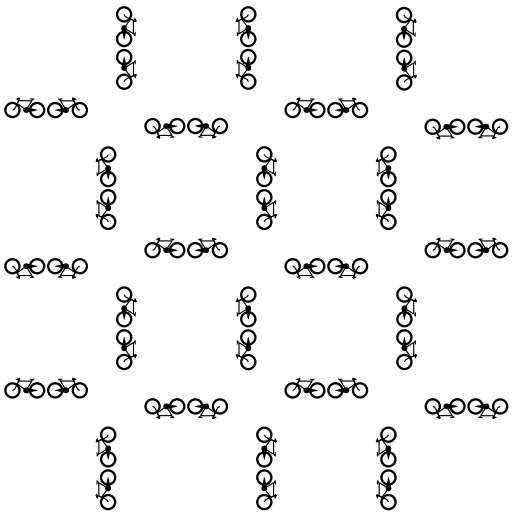
9. p2



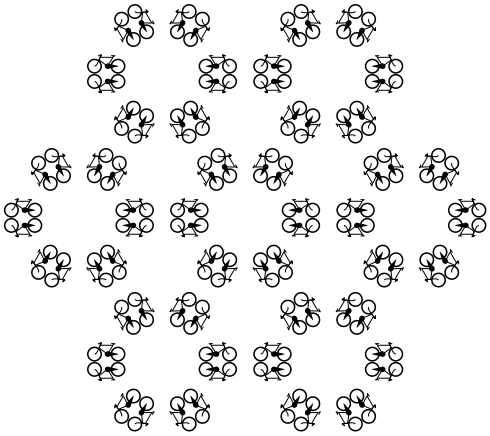
10. p4m



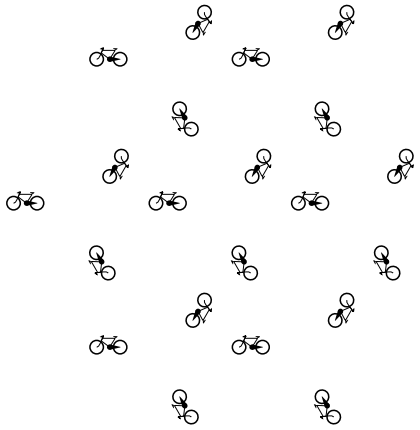
11. p4



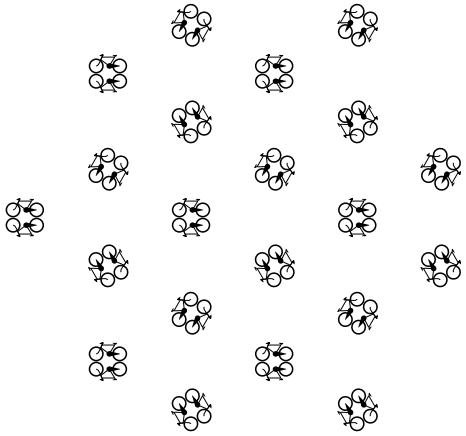
12. p4gm



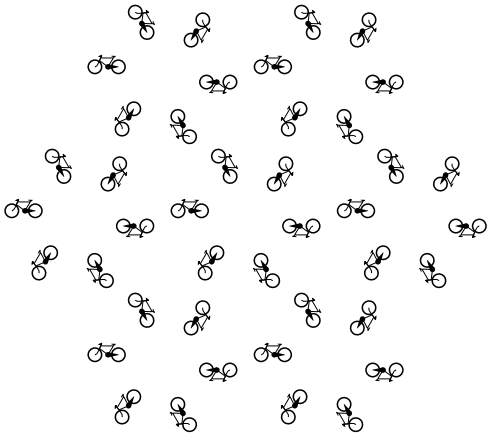
13. p6mm



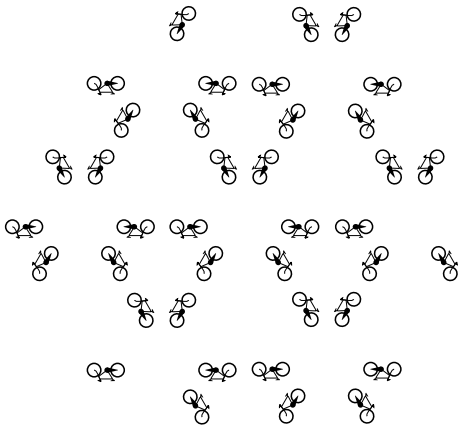
14. p3



15. p31m



16. p6



17. p3m1

Irti tasosta. On mahdollista luokitella saman tapaisin menetelmin myös useampiulotteisten kappaleiden symmetriaryhmiä. Esimerkiksi säännöllisillä monitahokkailla on verrattain yksinkertaiset äärelliset symmetriaryhmät. Tapettiryhmien vastineina syntyy kolmiulotteisessa avaruudessa ryhmiä, jotka kuvaavat esimerkiksi kemiassa ja kiinteän olomuodon fysiikassa tärkeitä mahdollisia kidehilarakenteita. Äärellisiä on 32 ja varsinaisia äärettömiä kristallografisia ryhmiä on 230 erilaista. Neljännessä ulottuvuudessa ryhmiä saadaan 4783 kpl ja ylemmissä ulottuvaisuuksissa vielä enemmän, kuitenkin aina äärellinen määrä.

Euklidisen avaruuden ohella myös muiden metristen avaruuksien,

vaikkapa pallon pinnan isometriset bijektiot muodostavat kauniita ja mielenkiintoisia – itse asiassa hyvinkin merkityksellisiä ryhmiä. Seuraavassa luvussa toteamme sitä paitsi, että myös edellä sivuuttamillamme jatkuvilla ryhmillä on samantapainen merkitys symmetrian kuvaajina.

oo

8. Klassiset Lien ryhmät

Klassiset Lien ryhmät ovat vektoriavaruuden lineaarikuvausten – yhtälailla matriisien – muodostamia topologisia ryhmiä. Ne ovat esimerkki matematiikan eri alojen, tässä lineaarialgebran, ryhmäteorian ja differentioituvien pintojen sekä useampiulotteisten monistojen[31] teorian synteesistä. Lisäksi niillä on merkitystä modernin fysiikan perustana.

Lien ryhmät.

8.1 Määritelmä.

(1) *Topologinen ryhmä* on ryhmä G, joka on varustettu sellaisella topologialla, että laskutoimitus on jatkuva kuvaus $G \times G \to G$ ja alkion kääntäminen on jatkuva $G \to G$.
(2) *Reaalinen Lien ryhmä* eli *jatkuva ryhmä* on ryhmä G, joka on samalla varustettu differentioituvalla struktuurilla, siis monisto, jossa ryhmän laskutoimitus ja kääntäminen ovat differentioituvia kuvauksia[32].
(3) *Kompleksinen Lien ryhmä* on ryhmä G, joka on samalla kompleksianalyyttinen monisto, jossa laskutoimitus ja kääntäminen ovat analyyttisiä kuvauksia.

Topologisten ryhmien merkitys perustuu suureksi osaksi siihen, että niissä on — kuten ryhmässä $(R^n, +)$ — mielekästä puhua **translaatioista**, tosin erikseen vasemman- ja oikeanpuoleisista, siis kuvauksista $x \mapsto hx$ ja $x \mapsto xh$. Translaatiot ovat homeomorfismeja. Jos ryhmän topologia on "lokaalisti kompakti", kuten yleensä onkin, niin topologisessa ryhmässä on olemassa Lebesguen mitan vastine, *Haarin mitta*, joka on translaatioinvariantti. Tämä tekee mahdolliseksi harrastaa integraalilaskentaa. Ilmiö on tuttu esimerkiksi ympyrän kehältä, joka on topologinen ryhmä luonnollisella topologiallaan ja laskutoimituksellaan, joka on kulmien yhteenlasku modulo 2π. Haarin mitta on tällöin kaaren pituus eli tasainen jakauma välillä $[0, 2\pi]$. **Fourier-analyysi** ja yleisem-

[31] Liite M

[32] On yhdentekevää, minkä kertaluvun differentioituvuuden asetamme pohjaksi Lien ryhmän määritelmälle. Vuonna 1900 maailman matemaatikoiden kongressissa Pariisissa DAVID HILBERT esitti kuuluisat 23 probleemaansa, joista viides koski tätä asiaa. Hilbert tiesi jo, että jokainen $\mathcal{C}^k-$mielessä $(0 < k)$ Lien ryhmä voidaan varustaa yhteensopivalla $\mathcal{C}^\infty-$Lien ryhmän struktuurilla, itse asiassa jopa reaalianalyyttisen eli $\mathcal{C}^\omega-$ryhmän struktuurilla. Avoimena oli kysymys siitä, voidaanko samaa sanoa tapauksessa C^0. Myönteisen vastauksen todistivat oikeaksi J. v.Neumann kompakteille ryhmille 1933 ja Montgomery ja Zippin yleisessä tapauksessa 1952. Heidän lauseensa sanoo: Kaikki äärellisulotteiset, lokaalikompaktit separoituvat metriset lokaalisti yhtenäiset topologiset ryhmät ovat Lien ryhmiä.

min **harmoninen analyysi** tutkii näitä ilmiöitä. Emme syvenny tähän aiheeseen, vaan keskitymme esittelemään klassisia Lien ryhmiä.

Klassiset Lien ryhmät.

8.2. Esimerkkejä.

(1) Topologisia ryhmiä ovat kaikki Lien ryhmät.

(2) Reaalisia Lien ryhmiä ovat mm. $(\mathbf{R}^n, +)$, kaikki kompleksiset – erityisesti alla kohdassa (3) mainitut – Lien ryhmät ja seuraavat ryhmät, jotka ovat $n \times n-$matriisien avaruuden $\mathbf{R}^{n\times n} = \mathbf{R}^{n^2}$ osajoukkoja, itse asiassa alimonistoja:

$$\begin{aligned}
GL(n,\mathbf{R}) &= \text{ Aut}(\mathbf{R}^n) = \text{ kääntyvät } n\times n-\text{matriisit}\\
&= \text{ lineaariset bijektiot } \mathbf{R}^n \to \mathbf{R}^n \quad (\mathbf{G}\text{eneral } \mathbf{L}\text{inear })\\
&\text{Erityisesti } \mathbf{R}\text{:n multiplikatiivinen ryhmä on } GL(1,\mathbf{R})\\
SL(n,\mathbf{R}) &= \text{ } n\times n-\text{matriisit, joiden determinantti on 1}\\
&(\mathbf{S}\text{pecial } \mathbf{L}\text{inear })\\
O(n,\mathbf{R}) &= \text{ ortogonaaliset } n\times n-\text{matriisit}\\
&= \text{sisätuloavaruusisomorfismit } \mathbf{R}^n \to \mathbf{R}^n \quad (\mathbf{O}\text{rthogonal })\\
SO(n,\mathbf{R}) &= O(n,\mathbf{R}) \cap SL(n,\mathbf{R}) \quad (\mathbf{S}\text{pecial } \mathbf{O}\text{rthogonal })\\
U(n,\mathbf{C}) &= \text{ unitaariset } n\times n-\text{matriisit}\\
&= \text{ sisätuloavaruusisomorfismit } \mathbf{C}^n \to \mathbf{C}^n \quad (\mathbf{U}\text{nitary })\\
SU(n,\mathbf{C}) &= U(n,\mathbf{C}) \cap SL(n,\mathbf{C}) \quad (\mathbf{S}\text{pecial } \mathbf{U}\text{nitary })
\end{aligned}$$

(3) Kompleksisia Lien ryhmiä ovat samaan tapaan itse $(\mathbf{C}^n, +)$ ja kompleksiset matriisiryhmät

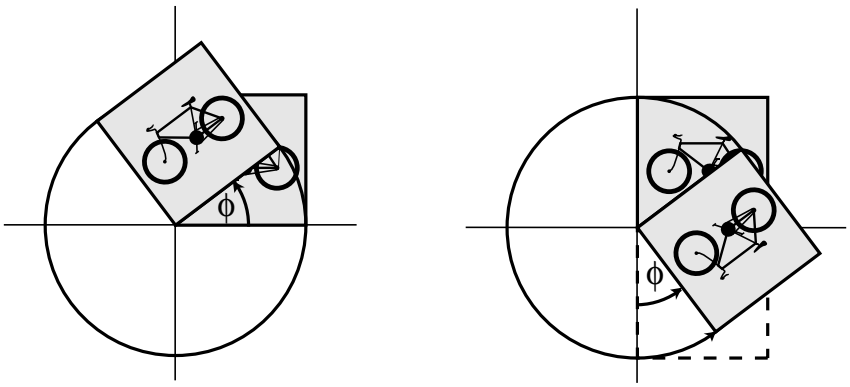
$$\begin{aligned}
GL(n,\mathbf{C}) &= \text{ Aut}(\mathbf{C}^n) = \text{ kääntyvät } n\times n-\text{matriisit}\\
&= \mathbf{C}-\text{lineaariset bijektiot } \mathbf{C}^n \to \mathbf{C}^n\\
SL(n,\mathbf{C}) &= \text{ } n\times n-\text{matriisit, joiden determinantti on 1.}
\end{aligned}$$

Näitä sanomme klassisiksi Lien ryhmiksi. Seuraavassa käsittelemme vain reaalisia.

Tunnemme lineaarialgebrasta klassisten Lien ryhmien algebrallisia ominaisuuksia. Kiinnitämme huomiota differentioituvaan puoleen esimerkkeinä ortogonaaliryhmät $SO(2,\mathbf{R})$, $O(2,\mathbf{R})$, $SO(3,\mathbf{R})$, ja $O(3,\mathbf{R})$.

8.3. Esimerkki ($SO(2,\mathbf{R})$ ja $O(2,\mathbf{R})$). Sisätuloavaruusisomorfismit, eli isometriat $R^2 \to R^2$, joilla origo on kiintopisteenä, ovat lauseen 7.7.

mukaan täsmälleen kierrot origon ympäri, heijastus $x-$akselin suhteen ja näistä yhdistetyt kuvaukset. Kierrot muodostavat täsmälleen ryhmän $SO(2,\mathbf{R})$, kierrot ja heijastus yhdessä virittävät ryhmän $O(2,\mathbf{R})$.



Tarkastellaan aluksi pelkkiä kiertoja. Kierron voi ilmaista antamalla kiertokulman $\phi \in \mathbf{R}/2\pi\mathbf{Z} = S^1$, ja ryhmänä onkin

$$SO(2,\mathbf{R}) = S^1 = \text{ ympyrä,}$$

samoin topologisena avaruutena ja monistona. Asian voi perustella seuraavasti. Kulman ϕ kierron matriisi on

$$\text{kiertomat}(\phi) = \begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix}.$$

Kuvaus "kiertomat" on jatkuva $\mathbf{R} \to \mathbf{R}^{2\times 2}$, koska sen komponentit, **matriisielementit** $\pm\cos\phi$ ja $\pm\sin\phi$ ovat sitä. Samasta syystä se on differentioituvakin. Kuvaus "kiertomat" voidaan tulkita kuvaukseksi myös ympyrältä matriisiryhmälle, koska se vie 2π:n monikerralla eroavat pisteet yhteen. Itse asiassa "kiertomat" on homeo- jopa diffeomorfismi ympyrältä kuvajoukolleen $SO(2,\mathbf{R})$, joka siis on monistona ympyrän kanssa isomorfinen.

Ryhmä $O(2,\mathbf{R})$ sisältää myös heijastuksen. Sekä ryhmänä että topologisena avaruutena ja monistonakin on

$$O(2,\mathbf{R}) = S^1 \times \{-1,1\}.$$

Tämäkin on heuristisesti uskottavaa asiaa , koska tason ortogonaalikuvaus epäilemättä muodostuu kierrosta ja mahdollisesti sen alla yhdestä

heijastuksesta, jonka mukanaoloa tai olemattomuutta voi merkitä esim. indeksillä 1 tai -1. Asiaa voi perustella tarkemmin laskemalla matriiseja. Kierretyn heijastuksen matriisi on

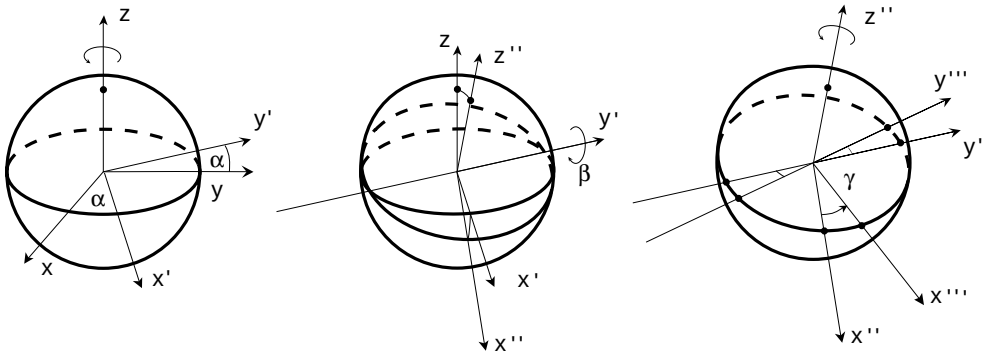
$$\text{peilikiertomat}(\phi) = \begin{pmatrix} \cos\phi & \sin\phi \\ \sin\phi & -\cos\phi \end{pmatrix}.$$

Myös kuvaus "peilikiertomat" on jatkuva ja jopa differentioituva lokaali injektio $\mathbf{R} \to \mathbf{R}^{2\times 2}$. Sekin voidaan tulkita injektioksi ympyrältä matriisiryhmälle, ja on diffeomorfismi ympyrältä kuvajoukolleen, joka muodostuu kaikista kierroista yhdistettynä yhteen heijastukseen. Kuvausten "kiertomat" ja "peilikiertomat" kuvajoukot ovat erillisiä, sillä determinanttifunktio det on jatkuva $\mathbf{R}^{2\times 2} \to \mathbf{R}$, mutta saa $O(2,\mathbf{R})$:ssä vain arvot 1 ja -1, ensin mainitun kierroille ja jälkimmäisen heijastuskierroille. Topologisena avaruutena ryhmällä $O(2,\mathbf{R})$ on siten kaksi yhtenäistä komponenttia, joista kumpikin on ympyrän kanssa isomorfinen, toisin sanoen

$$O(2,\mathbf{R}) = S^1 \times \{-1, 1\}.$$

ja neutraalialkion sisältävä komponentti on aliryhmä $SO(2,\mathbf{R})$.

8.4. Esimerkki ($SO(3,\mathbf{R})$ ja $O(3,\mathbf{R})$). $SO(3,\mathbf{R})$ muodostuu kolmiulotteisen avaruuden kierroista origon kautta kulkevien akseleiden ympäri. Kunkin kierron voi karakterisoida kolmella reaaliluvulla, esimerkiksi kiertoakselin suunnan määrittelevillä kahdella kulmalla ja kierron suuruudella tai – kuten seuraavassa tehdään – *Eulerin kulmilla*



$$\alpha \in [0, 2\pi),\ \beta \in [0, \pi) \text{ ja } \gamma \in [0, 2\pi),$$

jolloin vastaava matriisi on tulo

$$\begin{pmatrix} \cos\gamma & \sin\gamma & 1 \\ -\sin\gamma & \cos\gamma & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \cos\beta & 1 & -\sin\beta \\ 0 & 1 & 0 \\ \sin\beta & 0 & \cos\beta \end{pmatrix} \begin{pmatrix} \cos\alpha & \sin\alpha & 1 \\ -\sin\alpha & \cos\alpha & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Kuten tason kiertojen tapauksessa muodostuu nytkin kaikkien isometristen lineaarikuvausten ryhmä $O(\mathbf{R}, 3)$ tällaisista kierroista ja heijastuksesta, jossa determinantti vaihtuu 1:stä -1:een. Topologisella ryhmällä $O(3, \mathbf{R})$ on kaksi yhtenäistä komponenttia, jotka ovat diffeomorfisia keskenään ja joista toinen on aliryhmä $SO(3, \mathbf{R})$.

Lokaali isomorfia. Edellisissä esimerkeissä näkyy, että kaksi Lien ryhmää voivat olla "lokaalisti isomorfisia" olematta isomorfisia. Asetamme tarvittavan määritelmän:

8.5. Määritelmä. Lien ryhmät G ja H ovat *lokaalisti* isomorfisia, mikäli niiden neutraalialkioilla e ja e' on ympäristöt U ja V, ja näiden välillä on diffeomorfismi, joka säilyttää kaikki kysymykseen tulevat ryhmätulot.

8.6. Esimerkki. Lien ryhmät $SO(3, \mathbf{R})$ ja $O(3, \mathbf{R})$ ovat lokaalisti isomorfiset, käyhän etsityksi ympäristöksi itse $SO(3, \mathbf{R})$ ja diffeomorfismiksi sen upotus $O(3, \mathbf{R})$:ään.

$O(3, \mathbf{R})$ on **epäyhtenäinen**, nimittäin kahdesta yhtenäisestä komponentista muodostuva ryhmä, joka osoittautuu lokaalisti isomorfiseksi toisen komponenttinsa kanssa. Ei pidä kuitenkaan luulla, etteivät kaksi lokaalisti isomorfista Lien ryhmää voisi olla kumpikin yhtenäisiä olematta isomorfisia:

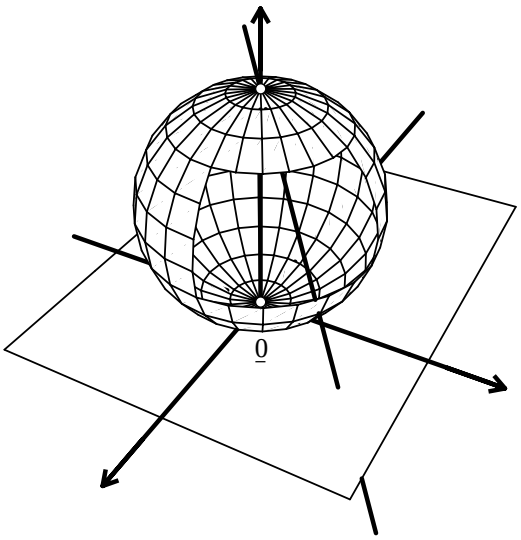
8.7. Esimerkki. Lien ryhminä ympyrä $S^1 = SO(2, \mathbf{R})$ ja suora $\mathbf{R}$ ovat lokaalisti isomorfiset, käyhän etsityksi ympäristöksi esimerkiksi väli $]-\pi, \pi[\subset \mathbf{R}$ ja diffeomorfismiksi

$$(*) \qquad \varphi \mapsto e^{i\varphi}.$$

Kaava $(*)$ määrittelee itse asiassa lokaalisti injektiivisen reaalianalyyttisen surjektion, *peitekuvauksen* $\mathbf{R} \to S^1$. $\mathbf{R}$ on S^1:n $\infty-$kertainen *peite*.

Seuraava esimerkki samasta asiasta on vähän vähemmän triviaali.

8.8. Esimerkki. Lien ryhmät $SO(3, \mathbf{R})$ ja $SU(2, \mathbf{C})$ ovat lokaalisti isomorfiset. Tämän asian ymmärtää parhaiten tulkitsemalla ortogonaalikuvausryhmän $SO(3, \mathbf{R})$ $\mathbf{R}^3$:n yksikköpallon S^2 suunnistuksen säilyttävien isometrioiden eli pallon kiertojen ryhmäksi. Toisaalta pallolla on luonnollinen yhteys kompleksilukuihin, samaistaahan stereografinen projektio **Riemannin pallon** S^2 kompleksilukujen tasoon $\widehat{\mathbf{C}}$, johon on otettu mukaan äärettömyyspiste vastaamaan projektiokeskusta eli pallon pohjoisnapaa.



Ei ole kovin vaikeaa kompleksianalyysiä[33] osoittaa, että pallon kiertoja vastaavat kompleksitasossa $\mathbf{C}$ täsmälleen ne ensimmäisen kertaluvun rationaalikuvaukset, jotka ovat muotoa

$$(*) \qquad w : z \mapsto w = w(z) = \frac{az + \overline{b}}{-bz + \overline{a}} \quad ,$$

missä a ja $b \in \mathbf{C}$ ja ainakin toinen niistä on nollasta eroava. Sanomme näitä *Möbius-kierroiksi*. Laventamalla rationaalilauseketta $(*)$ tarvittaessa voidaan olettaa, että $|a|^2 + |b|^2 = 1$. Näin teemmekin, ja nimitämme matriisia

$$(**) \qquad \begin{pmatrix} a & \overline{b} \\ -b & \overline{a} \end{pmatrix}$$

Möbius-kierron $w : z \mapsto w(z) = \frac{az+\overline{b}}{-bz+\overline{a}}$ matriisiksi $Mat(w)$.

Toisaalta $SU(2, \mathbf{C})$:n alkiot, unitaariset $2 \times 2-$matriisit, ovat täsmälleen muotoa $(**)$, missä determinantti $|a|^2 + |b|^2 = 1$. Laskemalla kahden Möbius-kierron yhdistetyn kuvauksen huomaa heti, että kuvaus, joka $SU(2, \mathbf{C})-$matriisiin liittää vastaavan Möbius-kierron, on ryhmähomomorfismi ja tietysti surjektio Möbius-kiertojen ryhmälle, joka on $SO(3, \mathbf{R})$, koska Möbius-kierrot ovat bijektiota vaille samoja kuin pallon kierrot. Saatu surjektiivinen ryhmähomomorfismi

$$\varphi : SU(2, \mathbf{C}) \to SO(3, \mathbf{R})$$

[33]Ks. esim Nevanlinna–Paatero: Funktioteoria § 3.14.

ei ole aivan injektio, vaan matriisit $M \in SU(2,\mathbf{C})$ ja $-M$ esittävät samaa kiertoa: $\varphi(M) = \varphi(-M)$. Muut esittävätkin sitten eri kiertoja – homomorfismin φ ydin on $\{I, -I\}$, missä I on $2 \times 2-$yksikkömatriisi. Olemme löytäneet isomorfismin tekijäryhmälle

$$SO(3,\mathbf{R}) = SU(2,\mathbf{C})/\{I, -I\}.$$

$SU(2,\mathbf{C})$ on $SO(3,\mathbf{R})$:n kaksinkertainen peite. Löytämämme peitekuvaus φ on jatkuva, jopa lokaali diffeomorfismi.[34] Tässä esimerkissä varsinaisesti etsimäksemme lokaaliksi isomorfismiksi Lien ryhmien $SU(2,\mathbf{C})$ ja $SO(3,\mathbf{R})$ välille kelpaa siten kuvaus φ, kunhan se rajoitetaan sopivaan neutraalialkion $I \in SU(2,\mathbf{C})$ ympäristöön.

Kaikki neljä edellisen esimerkin Lien ryhmää ovat tosin yhtenäisiä, mutta eivät kaikki yhdesti yhtenäisiä. Suora on yhdesti yhtenäinen, mutta ympyrä S^1 ei. $SU(2,\mathbf{C})$ on homeomorfinen $\mathbf{C}^2$:n eli $\mathbf{R}^4$:n yksikköpallon pinnan eli S^3:n kanssa ja siis yhdesti yhtenäinen. Siitä antipodaaliset pisteet samaistamalla saatu ortogonaaliryhmä $SO(3,\mathbf{R})$ on homeomorfinen ns. projektiivisen avaruuden P^3 kanssa eikä yhdesti yhtenäinen. Tämän voi todeta huomaamalla, että yhdesti yhtenäisyyden estäväksi kutistumattomaksi lenkiksi kelpaa meridiaani, joka yhdistää pohjoisnavan etelänapaan, joka on samaistettu pohjoisnapaan.

Ryhmän topologia, erityisesti sen yhtenäisyysominaisuudet ovat lokaaleista isomorfismeista puhuttaessa tärkeä asia, sillä pätee

8.9. Lause. *Kaksi* **yhdesti yhtenäistä** *Lien ryhmää ovat isomorfisia aina ja vain ollessaan lokaalisti isomorfisia.*

Tällä lauseella on merkitystä kaikille Lien ryhmille – kuten esimerkkiemme valossa saattaa arvata.

8.10. Lause. *Jokainen Lien ryhmä on jonkin yhdesti yhtenäisen Lien ryhmän Lien tekijäryhmä.*

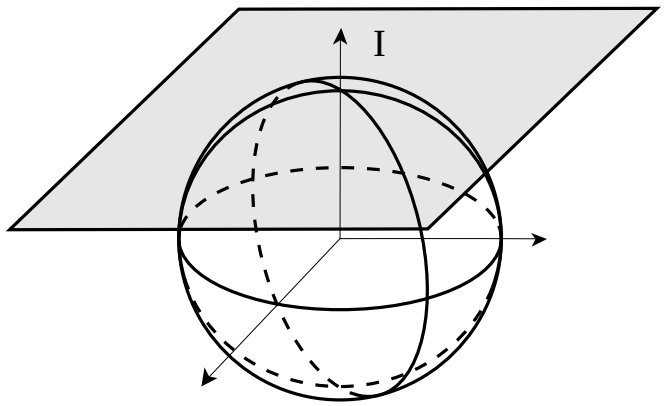
Emme todista kumpaakaan näistä lauseista, emmekä edes ole määritelleet, mitä tarkoitetaan Lien ryhmän Lien tekijäryhmällä.

Lien ryhmän Lien algebra.

8.11. Johdanto. Mielivaltaisen pieni neutraalialkion e ympäristö määrää edellä sanotun mukaan yhdesti yhtenäisen Lien ryhmän G isomorfismia

[34] SU(2)-matriisien tulkinnan avaruuden kiertoina voi esittää hieman toisinkin. Liitetään SU(2)-matriisiin M $\mathbf{R}^3$:n kuvaus $(x,y,z) \mapsto H = \begin{pmatrix} x & z-iy \\ z+iy & -x \end{pmatrix} \mapsto K = MHM^{-1} \mapsto (K_{11}, Im(K_{21}), Re(K_{21}))$. Osoittautuu, että se on yllä konstruoitu kierto.

vaille ja määritelmän mukaan jokaisen Lien ryhmän lokaalia isomorfiaa vaille. Mielivaltaisen pientä alkion e ympäristöä on differentiaalilaskennassa totuttu edustamaan tangenttiavaruudella T_e, jota yritämme havainnollistaa puutteellisella 2-ulotteisina kuvalla:



Tässä tämä ei kuitenkaan sellaisenaan riitä, sillä esimerkiksi Lien ryhmät $SO(3,\mathbf{R})$ ja $\mathbf{R}^3$, ovat kumpikin 3-ulotteisia, mikä merkitsee, että kummankin tangenttiavaruuskin on 3-ulotteinen – ja siis vektoriavaruutena sama. Sopivasti paranneltuna tangenttiavaruus kuitenkin saadaan kantamaan koko neutraalialkion ympäristöä kuvaavaa informaatiota. Kikka on siinä, että siinä otetaan käyttöön vektoriavaruussääntöjen lisäksi uusi laskutoimitus, Lien sulkeet kuvaamaan **ryhmän** laskutoimitusta. Vaikka konstruktio tehdään neutraalialkion kohdalla, se kuvaa ryhmän rakennetta kaikissa pisteissä, sillä koko asetelma voidaan siirtää mielivaltaisen pisteen $a \in G$ kohdalle translaatiolla $V_a : G \to G : x \mapsto ax$, joka on diffeomorfismi, jolloin sen derivaatta DV_a on isomorfismi $T_e \to T_a$.[35]

8.12. Määritelmä. Tarkastelemme aluksi erikoistapauksena klassisisia Lien ryhmiä, jotka ovat matriisiryhmiä, siis $GL(\mathbf{R},n)$:n aliryhmiä[36].

[35]Tällä on mielenkiintoinen seuraus. Olkoon $X_e \in T_e \setminus \{0\}$. Tällöin $X_a = DV_a(X_e)$ on kaikkialla nollasta eroava differentioituva vektorikenttä monistolla G. Lien ryhmä G voidaan siis "kammata ilman jakausta tai pyörrettä" toisin kuin esim. tavallinen pallo $S^2 \subset \mathbf{R}^3$. Erityisesti S_2 ei ole varustettavissa Lien ryhmän rakenteella, mikä selittää seuraavilla sivuilla esiintyvien tangenttiavaruutta esittävien kuviemme vajavaisuutta.

[36]ja alimonistoja

Neutraalialkiona on ykkösmatriisi

$$I = \begin{pmatrix} 1\,0\,\ldots\,0 \\ 0\,1\,\ldots\,0 \\ \vdots\,\vdots\,\ddots\,\vdots \\ 0\,0\,\ldots\,1 \end{pmatrix}$$

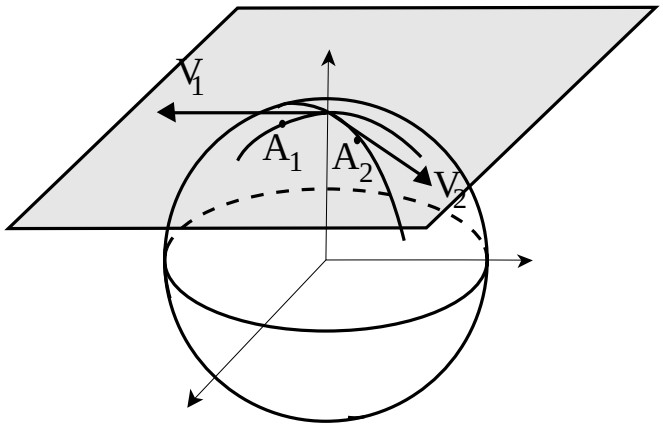
Klassissen Lien ryhmän G tangenttiavaruus neutraalialkion I kohdalla[37] $\mathfrak{g}$ muodostuu kaikista I:n kautta kulkevista moniston G differentioituvista käyristä samaistaen käyrät, joilla on sama derivaatta I:n kohdalla.

Tangenttivektoreita ovat siis viime kädessä nämä derivaatat, jotka klassisen Lien ryhmän tapauksessa ovat matriiseja. Tangenttiavaruus on monistosta G periytyvine laskutoimituksineen vektoriavaruus, jonka laskutoimitukset ovat tavalliset matriisien yhteenlasku ja luvulla kertominen.

Neutraalialkion ympäristössä tangenttiavaruus $\mathfrak{g}$ sivuaa monistoa G ja ympäristössä olevat matriisit ovat muotoa

$$A_i = I + \epsilon\, V_i,$$

missä ϵ on pieni luku ja V, on matriisi, jolle $\|V\| = 1$.[38]



V ei yleensä kuulu ryhmään G, mutta kuuluu ainkin rajalla $\epsilon \to 0$ tangenttiavaruuteen $\mathfrak{g}$. Ryhmätoimitus – matriisien kertolasku – antaa

[37] Liite M.

[38] Matriisien vektoriavaruus $\mathbf{R}^{n^2}$ on varustettu jollakin normilla, esimerkiksi operaattorinormilla tai euklidisella normilla. Emme sano mitä normia käytämme, koska kaikki normit äärellisulotteisessa avaruudessa $\mathbf{R}^{n^2}$ kuitenkin antavat saman topologian.

kahteen tällaiseen sovellettuna

$$(I + \epsilon_1 V_1)(I + \epsilon_2 V_2) = I + \epsilon_1 V_1 + \epsilon_2 V_2 + \epsilon_1\epsilon_2 V_1 V_2$$

Ensimmäisen kertaluvun (yksi epsilon) tarkkuudella eli tangenttiavaruudessa se siis vastaa matriisien yhteenlaskua, mutta toisessa kertaluvussa on G:n ryhmätoimituksen epäkommutatiivisuutta heijasteleva matriisitulotermi $V_1 V_2$, josta teemme kaipaamamme lisästruktuurin tangenttiavaruuteen.

8.14. Määritelmä. Klassisen Lien ryhmän G *Lien algebra* $\mathfrak{g}$ on tangenttiavaruus T_I varustettuna vektorilaskutoimitustensa lisäksi laskutoimituksella

$$[X, Y] = XY - YX,$$

jota sanotaan *Lien tuloksi, Lien sulkeiksi,* tai *kommutaattoriksi.*

Olemme tangenttivektoreita tutkiessamme ajautuneet algebrasta differentiaaligeometriaan, jota tarvittaisiin lisää, jos haluaisimme määritellä Lien algebran mielivaltaiselle Lien ryhmälle. Tarkoitus ei kuitenkaan ole laajasti ruveta pohtimaan tätä, vaan valaista asiaa tarkastelemalla lähemmin klassisia esimerkkejä.

8.15. Esimerkki. Palaamme tilanteeseen, jossa Lien ryhmä on jokin edellä esitellyistä $GL(n, \mathbf{R})$:n aliryhmistä. G:n tangenttiavaruus $\mathfrak{g}$ neutraalialkion $e = I$ kohdalla koostuu kaikista matriiseista

$$X = \frac{dA(t)}{dt}\Big|_{t=0},$$

missä $t \to A(t)$ on käyrä G:ssä, siis kuvaus janalta G:lle, ja lisäksi $A(0) = I$. $\mathfrak{g}$ on äärellisulotteinen vektoriavaruus ja sille voidaan muodostaa kanta seuraavasti: G muodostuu joukosta matriiseja, joiden elementit riippuivat differentioituvasti joistakin (minimaalisen monesta) parametreistä $x_1, \ldots, x_n$. $\mathfrak{g}$:n vektoriavaruuskanta saadaan derivoimalla G:n yleinen alkio

$$A(x_1 \ldots, x_k) = \begin{pmatrix} a_{11}(x_1, \ldots, x_k) & \ldots & a_{1n}(x_1, \ldots, x_k) \\ \vdots & \ddots & \vdots \\ a_{n1}(x_1, \ldots, x_k) & \ldots & a_{nn}(x_1, \ldots, x_k) \end{pmatrix}$$

kunkin parametrin x_j suhteen kohdassa $I = A(0 \ldots, 0)$. Kutakin parametria x_j tulee siis vastaamaan tangenttivektori $X_j = \dfrac{\partial A}{\partial x_j}\Big|_{x=0}$. $\mathfrak{g}$ on

näiden virittämä vektoriavaruus. Lukija laskekoon tämän tapauksessa $SO(3, \mathbf{R})$. Tuloksena on:

Lien ryhmä	Tangenttiavaruus
$GL(n, \mathbf{R})$	$gl(n, \mathbf{R}) = R^{n \times n}$
$SL(n, \mathbf{R})$	$sl(n, \mathbf{R}) = \{M \in R^{n \times n} \mid \text{jälki}(M) = 0\}$
$O(n, \mathbf{R})$	$o(n, \mathbf{R}) = \{M \in R^{n \times n} \mid M : \text{n transpoosi on } -M\}$
$SO(n, \mathbf{R})$	$so(n, \mathbf{R}) = o(n, \mathbf{R}) \cap sl(n, \mathbf{R})$
$U(n, \mathbf{C})$	$u(n, \mathbf{C}) = \{M \in R^{n \times n} \mid M : \text{n transpoosi on } -\overline{M}\}$
$SU(n, \mathbf{C})$	$su(n, \mathbf{C}) = u(n, \mathbf{C}) \cap sl(n, \mathbf{C})$

Sen sijaan että todistelisimme näitä asioita, katsomme mitä hyötyä Lien algebrasta voisi olla. Ainakin Lien algebra on alkuperäistä ryhmää sikäli miellyttävämpi objekti, että se on **vektoriavaruus**. Tätä voi käyttää alkuperäisen ryhmän tutkimiseen, sillä **Lien ryhmä määräytyy lokaalia isomorfiaa vaille Lien algebrastaan**. Erityisesti kommutatiivinen Lien ryhmä, jolla ilmeisestikin on triviaali Lien tulo $[X, Y] = 0$, määräytyy lokaalia isomorfismia vaille pelkästä dimensiostaan.

Tämä yksikäsitteinen määräytyminen ei ole pelkkä teoreettinen olemassaolo- ja yksikäsitteisyyslause, vaan klassisen Lien ryhmän neutraalialkion ympäristö voidaan laskemalla rekonstruoida Lien algebrasta eksponenttifunktion avulla:

8.16. Määritelmä. Olkoon $X \in R^{n \times n} = gl(n, \mathbf{R})$. Määrittelemme:

$$e^X = \sum_{j=0}^{\infty} \frac{1}{j!} X^j.$$

Sarja suppenee, kun $\|X\| < 1$.

8.17. Lause.

(1) $\det e^X = e^{\text{jlki}X}$.
(2) *Jos* $XY = YX$, *niin* $e^{XY} = e^X e^Y$
(3) *Eksponenttifunktion* $exp : gl(n, \mathbf{R}) \to GL(n, \mathbf{R})$ *derivaatta origossa on identtinen kuvaus.*
(4) *Eksponenttifunktion* $exp : \mathfrak{g} \to G$ *derivaatta origossa on identtinen kuvaus. Se kuvaa siis Lien algebran origon ympäristön vastaavan Lien ryhmän origon ympäristöksi.*

Yhteys Lien ryhmien ja niiden Lien algebrojen välillä on siis läheinen. Itse asiassa tilanne on vielä parempi. Lien algebrat voi nimittäin karakterisoida aksiomaattisesti.

Lien algebrat.

8.18. Määritelmä. Äärellisulotteinen vektoriavaruus V varustettuna lisäksi laskutoimituksella [X,Y] on *Lien algebra*, jos pätevät laskulait

$$X \mapsto [X,Y] \quad \text{on lineaarinen} \quad \forall\, Y$$
$$[X,Y] = -[Y,X]$$
$$[X,[Y,Z]] + [Y,[Z,X]] + [Z,[X,Y]] = 0 \quad \text{(Jacobin identiteetti)}$$

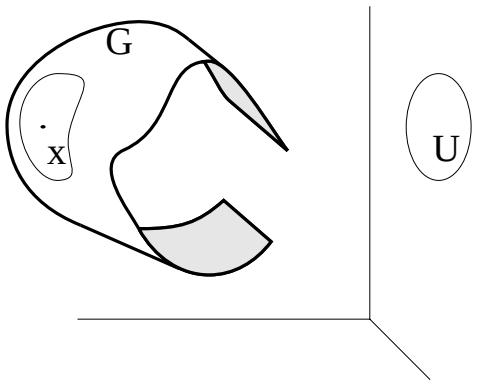
Osoittautuu, että jokaiseen äärellisulotteiseen abstraktiin Lien algebraan liittyy Lien ryhmä, jonka Lien algebra se on. Toisaalta Lien algebrat tunnetaan lähes kaikki – ns. puoliyksinkertaiset on luokiteltu.

Kun huomaamme, että Lien ryhmät olennaiselta osin pitävät sisällään kaiken, mitä tarkoitamme äärettömällä eli jatkuvalla symmetrialla, on ymmärrettävää, että Lien ryhmät ja algebrat ovat paras työkalu, jolla fysiikassa kuvataan luonnossa esiintyviä säännönmukaisuuksia, invariansseja eli symmetrioita. Erityisen tärkeitä ovat Minkowskin avaruuden isometrisista isomorfismeista eli *Lorentz–muunnoksista* muodostuvat ryhmät, ovathan luonnonlait erikoisen suhteellisuusteorian mukaan tässä mielessä invariantteja.

Liite M: Pari sanaa monistoista

M.1. Johdanto. Klassisissa Lien ryhmissä voi harrastaa differentiaalilaskentaa – ne ovat monistoja. Monistojen teoria on se laaja matematiikan ala, jota sanotaan differentiaaligeometriaksi. Esitämme luvun 8 tarpeisiin määritelmän reaaliselle monistolle – oikeastaan vain R^n:n alimonistolle – ja sen tangenttiavaruudelle. Yleinen määritelmä löytyy luonnollisestikin kaikista differentiaaligeometrian tai Lien ryhmien kirjoista.

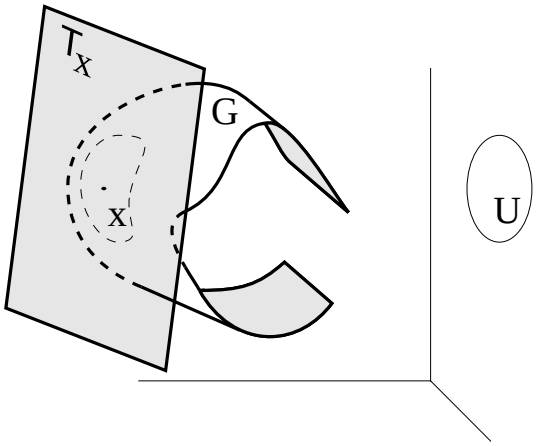
M.2. Määritelmä. Euklidisen avaruuden $\mathbf{R}^3$ *sileä pinta* eli *2-ulotteinen alimonisto* on joukko $G \subset \mathbf{R}^3$, joka lokaalisti – siis jokaisen pisteensä x ympäristössä – on jonkin jatkuvasti derivoituvan kuvauksen $f : U \to \mathbf{R}$ kuvaaja, missä U on avoin joukko jossakin $\mathbf{R}^3$:n kolmesta koordinaattitasosta.



Useampaan ulotteisuuteen kaavamaisesti yleistäen saadaan edellisestä

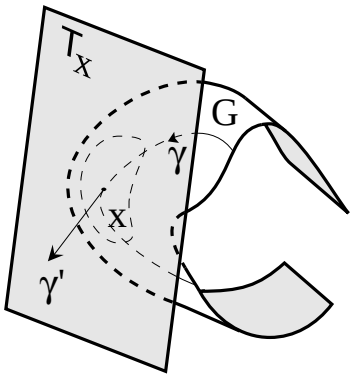
M.3. Määritelmä. Euklidisen avaruuden $\mathbf{R}^{n+m}$ *n-ulotteinen alimonisto* on joukko $G \subset \mathbf{R}^n$, joka lokaalisti – siis jokaisen pisteensä x ympäristössä – on jonkin jatkuvasti derivoituvan kuvauksen $f : U \to \mathbf{R}^m$ kuvaaja, missä U on avoin joukko jossakin $\mathbf{R}^{n+m}$:n $n-$ulotteisista "koordinaattitasoista".

M.4. Määritelmä. Euklidisen avaruuden $\mathbf{R}^{n+m}$ n-ulotteisen alimoniston G *tangenttiavaruus* T_x kohdassa $x \in G$ on edellisessä määritelmässä esiintyneen funktion f derivaatan kuvaaja. Se on mukavinta ajatella siirretyksi origosta kulkemaan pisteen $x \in G \subset \mathbf{R}^{n+m}$ kautta.



M.5. Huomautus. G:n tangenttiavaruus T_x ei riipu funktion f valinnasta.

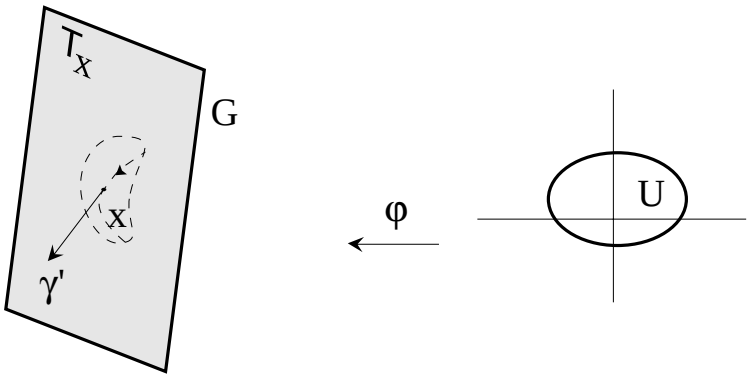
M.6. Huomautus. G:n tangenttiavaruus T_x sivuaa monistoa G pisteessä x. Tämä tarkoittaa sitä, että jokaisen sileän käyrän $\gamma :]a, b[\to G$ derivaatta $\gamma'(t_0)$ kohdassa, jossa $\gamma(t_0) = x$, on tangenttiavaruuden T_x suuntainen.



Tangenttiavaruus yhtyy näiden derivaattavektoreiden joukkoon

$$\{\gamma'(t_0) | \gamma :]a, b[\to G \text{ on sileä käyrä, } \gamma(t_0) = x\},$$

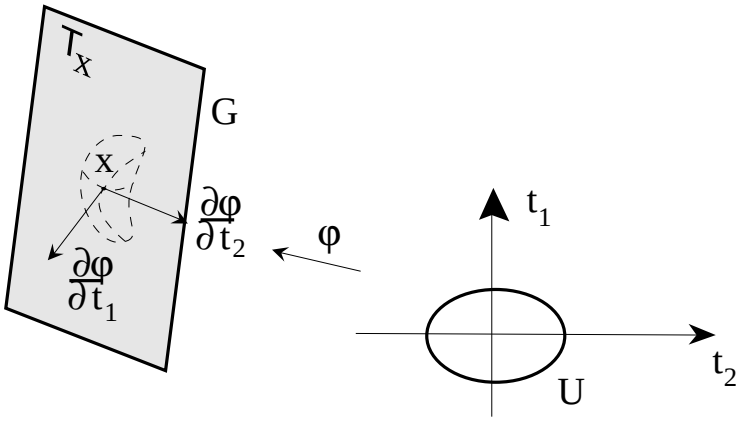
jona sen voisi määritelläkin. Tällaisella määritelmällä on se etu, että se kelpaa myös silloin, kun monisto G esitetään jossakin muussa muodossa, esimerkiksi jonkin sileän funktion $F : \mathbf{R}^{n+m} \to \mathbf{R}^m, (\text{ rank} F'(x) = m)$ tasa-arvopintana tai – kuten klassiset Lien ryhmät luvussa 8 – pisteen x ympäristö jonkin sileän funktion $\varphi : U \to \mathbf{R}^{n+m}$, kuvajoukkona , missä U on avoin joukko $\mathbf{R}^n$:ssä.



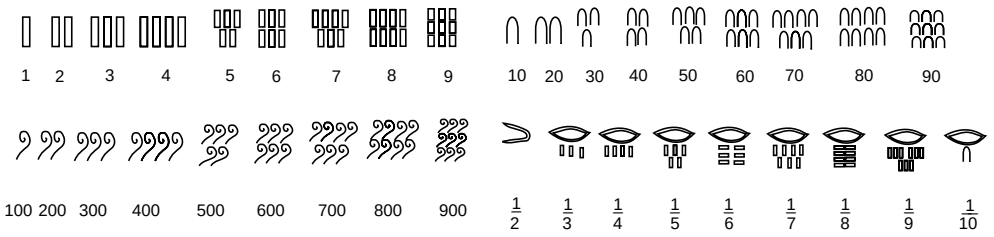
Tokihan n lineaarisesti riippumatonta tangenttiavaruuden vektoria jo virittää sen. Jos $x = \varphi(0)$, niin näiksi voidaan valita koordinaattiakselien kuvien muodostamien käyrien

$$t_i \mapsto \varphi(t_1, \ldots, t_n)$$

derivaatat kohdassa $t = 0$.



Klassisen Lien algebran kantavektorit muodostetaan näin.



Hieroglyyfien numerot

Babylonialaiset käyttivät neljätuhatta vuotta sitten jo varsin kehittynyttä aritmetiikkaa nuolenpääkirjoituksissaan ja osasivat ratkaista joitakin toisen asteen yhtälöitä. Muinaisesta Egyptistä on säilynyt kirjuri Ahmosen laatima matematiikan oppikirja, ns. Rhindin papyrus. Siitä voi päätellä, että egyptiläiset eivät tunteneet toisen asteen yhtälön ratkaisukaavaa. Deduktiivisen matematiikan kehdossa, Kreikassa, pääasiallinen kehitys tapahtui geometrian alalla, mutta algebraakin harrastettiin, etenkin lukuteoriaa. Pythagoras (n. 585-500 e.Kr.) käsitteli kokonaislukujen neliöiden summia ja pythagoralaiset kehittivät itse asiassa uskontofilosofian, jossa kokonaislukuja palvottiin kaiken olevaisen alkuna. Eukleideen (n. 300 e.Kr.) Alkeet käsittelee algebraa sekä geometrisesti että myös lukuteoreettisesti; alkulukuja todistetaan olevan äärettömän paljon. Antiikin etevin matemaatikko, Arkhimedes (287-212 e.Kr.) määräsi π:lle likiarvon ($3\frac{10}{71} < \pi < 3\frac{1}{7}$), "tyhjennysmenetelmällä", eli approksimoimalla ympyrän alaa sisä- ja ulkopuolelle piirrettyjen säännöllisten monikulmioiden avulla ja todisti integraalilaskentaa ennakoiden, että molemmat antavat saman raja-arvon. Samoihin aikoihin Diophantos laski symbolein, harrasti lukuteoriaa ilman geometrista taustaa ja etsi kokonaislukuratkaisuja kokonaislukukertoimisille yhtälöille.

Numerojärjestelmämme, "arabialaiset luvut", on tosiasiassa alkujaan intialainen. Hindulaiset matemaatikot (n. 200–1200) ottivat käyttöön paikkajärjestelmän, johon kuului nollamerkki, negatiiviset luvut (velat) ja muita uusia symbolisia merkintätapoja. He osasivat myös laskea neliö- ja kuutiojuurilla. Noin 600-luvulta alkaen hindulaista ja kreikkalaista traditiota jatkettiin etenkin arabiankielisessä kulttuuripiirissä. Arabit hyväksyivät irrationaaliluvut, mutta eivät negatiivisia. He käsittelivät sujuvasti 1., 2. ja eräissä erikoistapauksessa jopa 3. asteen yhtälöitä. Tarkkoja todistuksia kreikkalaiseen tyyliin ei kuitenkaan an-

nettu. Algoritmi (nimestä Mohammed ibn Musa al-Khowârizmî (830)) ja algebra (edellä mainitun teoksesta "Al-jabr w'al muqâbala"; al-jabr = palauttaminen.) ovat alkujaan arabian kieltä. Suomeksikin käännetyn "Viisaan viinin" ja muiden runoteosten tekijänä tunnettu Omar al–Khaijam (1048?–1122) oli myös aikansa etevin matemaatikko[39].

Euroopassa keskiaika oli matematiikan kannalta hiljaista. Kannattaa mainita arabialaisten numeroiden yleistyminen soveltavalla puolella ja Pisan Leonardon eli Fibonaccin (n. 1170–1250) lukuteoreettiset tarkastelut.

Renessanssin aluksi eurooppalaiset kiinnittivät huomionsa kreikkalaisten saavutuksiin, mutta 1500-luvulta alkaen myös algebran kehitys jatkui, aluksi vieläpä voimakkaasti. Cardanon kaava 3. asteen yhtälön ratkaisemiseksi tuli julki vuonna 1545. (Asiasta lisää luvussa "Radikaalia".) Negatiivisten lukujen neliöjuuria alettiin käyttää symbolisena laskuapuna. Nykyiset merkinnät laskutoimituksille, neliöjuurille, yhtälöille ja epäyhtälöille sekä muuttujille ja tuntemattomalle x otettiin käyttöön.

1600-luvulle tultaessa oli geometria edelleen dominoiva matematiikan ala, mutta algebra – etenkin lukuteoria – tuli nyt sen rinnalle ennen kaikkea siitä syystä, että Descartes'in (1596–1650) suorakulmaisten koordinaattien järjestelmällinen käyttö kytki luvut ja geometrian toisiinsa luoden samalla pohjan derivaatan ja integraalin keksimiselle ja raja-arvojen tutkimiselle. Samalla alkoi todennäköisyyslaskenta ja sen myötä kombinatoriikka. Pascal esitti binomikertoimet vuonna 1654, Fermat jätti jälkipolville kuuluisan probleemansa kuollessaan v. 1665. Girard muotoili algebran peruslauseen v. 1629 ja Leibnitz merkitsi $3 \times 3-$matriiseita indeksiparein 1693.

Lukujärjestelmäämme alettiin ymmärtää 1700-luvulla, kun toisaalta negatiiviset, irrationaaliset ja kompleksiset, toisaalta algebralliset ja transkendenttiset luvut löysivät paikkansa. Euler todisti 1737 e:n ja e^2:n irrationaalisuuden ja yritti 1749 todistaa algebran peruslauseen. d'Alembert kirjoitti v. 1747 kompleksilukuja muodossa $a + b\sqrt{-1}$. Lambertin todistus π:n irrationaalisuudelle on peräisin vuodelta 1761 ja Lagrangen uraauurtavat tutkimukset polynomin juurten permutaatioista vuodelta 1770. Lineaarialgebraa ennakoivat "suorakulmalaskusäännöt" lineaaristen yhtälöryhmien ratkaisemiseksi. Tällaisia laativat mm. McLaurin, Cramer ja Vandermonde. Karakteristisen yhtälön ottivat käyttöön Laplace, Lagrange ja Euler. Vuosisadan lopussa tapahtui geometristen konstruktioiden alalla ratkaiseva käänne. Gauss (1777–1855) todisti v. 1796 algebrallisin menetelmin, että säännölli-

[39]Hänen algebrankirjansa suomennosta saanemme kuitenkin vielä odottaa.

nen 17-kulmio on konstruoitavissa harpilla ja viivoittimella ja löysi pari vuotta myöhemmin riittävän ehdon $n-$kulmion konstruoituvuudelle, joka oli eräs muinaisten kreikkalaisten avoimista ongelmista. Vuonna 1837 Wantzel todisti Gaussin ehdon myös välttämättömäksi ja sivutuotteena tästä ratkesi myös kulman kolmiajakoa koskeva ongelma. Ympyrän neliöintiongelma jäi tässä vaiheessa ratkaisematta, koska tieto π:n transkendenttisuudesta puuttui vielä lähes sadan vuoden ajan.

Abstraktin algebran alku sijoittuu vasta 1800-luvulle, jolloin määriteltiin ryhmä, kunta ja algebra ja selvitettiin transkendenttilukujen olemassaolo ja ylemmän asteen polynomiyhtälön ratkeavuus. Determinantti- ja matriisioppi kehittyi. 1800-luvun edistysaskelten luettelo on pitkä:

Gauss keksi algebran peruslauseen todistuksen 1799 reaalisille ja 1848 kompleksisille kertoimille, Abel (1802–1829) todisti Lagrangen ja Ruffinin töiden pohjalta erään viidennen asteen yhtälön ratkeamattomaksi ja otti käyttöön lukukunnan käsitteen. Galois (1811–1832) loi täydellisen teorian polynomiyhtälöiden ratkeavuudesta ja tähän tarvittavista kerroinkunnan laajennuksista. Myös normaali aliryhmä ja isomorfia ovat Galois'n keksintöjä. Galois'n teoriaa kehitti edelleen Jordan (1838–1922), jolta on peräisin Abelin ryhmä-nimitys, Jordan-Hölderin lause ryhmille (Hölder 1859–1937), ja matriisien normaalimuoto. Sylow, joka tutki kertalukua p^n – missä p on alkuluku – olevien aliryhmien olemassaoloa, eli vuosina 1832–1918. Abstraktin ryhmän käsite on nykyisessä muodossa peräisin Cayleyltä (1821–1895), joka myös todisti, että kaikki ryhmät ovat realisoitavissa permutaatioryhminä ja otti käyttöön nimeään kantavat luvut. Matriisi–nimityksen (1850) isä on Sylvester. Hamilton (1805–1865) selvensi lopullisesti lukujärjestelmän rakenteen esittämällä kompleksiluvut reaalilukupareina (1837, Gaussin esitys v.1831 ei tullut julki); yleistyksenä kompleksiluvuista Hamilton loi kvaterniot, kunnan, jonka laskutoimitus ei kommutoi. Tämän suuntainen tutkimus tuli tavallaan tiensä päähän vuonna 1878, kun Frobenius (1849–1917) todisti, että R^n voidaan varustaa vinokunnan struktuurilla vain, kun $n = 1, 2$ tai 4. Frobeniukselta ovat peräisin myös minimaalipolynomi (1878) (yksikäsitteisyystodistus on Henselin, vuodelta 1904), matriisin ranki ja Cayley-Hamiltonin lauseen todistus. Ensimmäisen transkendenttiluvun löysi Liouville (1889–1913) vuonna 1844. Cantor (1845–1918) on keksinyt joukkojen mahtavuuden ja siitä seuraavan irrationaali- ja jopa transkendenttilukujen runsauden lisäksi nimeään kantavan fraktaalisen joukon ja myös reaalilukujen esittämisen Cauchyn jonojen ekvivalenssiluokkina. Dedekind (1831–1916) puolestaan esitti tämän kanssa ekvivalentin tavan reaalilukujen konstruoimiseksi rationaaliluvuista – Dedekindin leikkaukset – vuosina 1871–72. Hän konstruoi myös kokonaisluvut joukko-opin avulla. Dedekind ja

Weber tutkivat algebrallisin metodein kompleksimuuttjien algebrallisten funktioiden muodostamia kuntia ja niiden avulla Riemannin pintoja jatkaen näin Abelin tutkimuksia. Tässä yhteydessä he ottivat käyttöön kunta-nimen. Kroneckerin algebrallisten lukujen teoria vuodelta 1887 esittää algebralliset luvut aidon algebrallisesti polynomirenkaan $\mathbf{Q}[X]$ pääideaalien avulla käyttämättä kompleksi- tai edes reaalilukuja. Tästä oli enää lyhyt askel aksiomaattiseen kunnan käsitteeseen, joka esiintyy ensimmäisen kerran Weberin (1842–1913) Galois'n teorian perusteita käsittelevässä kirjoituksessa vuodelta 1893. Hilbert (1862–1934) esitti 1897 algebrallisten lukujen teorian ja 1899 reaalilukujen postulaatit. Hermite (1822–1901) todisti 1855, että hermiitisen matriisin ominaisarvot ovat reaalisia ja 1873, että e on transkendenttinen. Samaa menetelmää täydentäen Lindemann (1852–1901) esitti π:n transkendenttisuustodistuksen 1882. Kokonaislukujen Peanon (1858–1939) aksioomat ovat peräisin vuodelta 1889 ja joukko-opin Zermelon (1871–1953) aksioomat vuodelta 1908.

Algebran kehitys ei tietenkään ole päättynyt vuosisatamme alkuun, vaan 1900-luku on ollut uusien keksintöjen aikaa. Katsausluontoinen yhteenveto nykyalgebran historiasta on Encyclopedia Britannicassa, joka omistaa hakusanalle algebra parikymmentä sivua.

Lähteistä

Tämä moniste perustuu lähes kokonaan kirjaluettelossa mainittuihin teoksiin. Päälähteenä olen käyttänyt Stewartia [11], jota miellyttävän tyylinsä vuoksi suosittelen luettavaksi monisteen rinnalla. Kirja sisältää juuri sopivan määrän harjoitustehtäviä, jotka on maltettu myös pitää riittävän helppoina Galois'n teorian aloittelijan ratkaistaviksi. Stewart esittelee lisäksi Galois'n teorian käyttöä mm. säännöllisten monikulmioiden konstruoitavuuden tutkimiseen ja äärellisten kuntien teoriaa. Laajempi ja uudempi esitys Galois'n teoriasta on Bastidan kirjassa [1]. Huhut kertovat Rothmaninkin julkaisseen kirjan samasta aiheesta. Van der Waerdenin klassista algebrankirjaa [13] olen pitänyt pohjana symmetrisiä polynomeja käsittelevälle luvulle. Ryhmäteoriaa ja luvut 7 ja 8 olen haalinut kokoon vaihtelevista lähteistä. Historialiite perustuu Mikko Saarimäen kokoamiin muistiinpanoihin kirjoista Kline [7] ja Struik [12]. Erityisesti Galois'n henkilöstä kiinnostuneille Bellin [2] lähinnä kaunokirjallista elämäkertaa tarkempi on Rothmanin kriittinen artikkeli [10]. Siisti ja lyhyt kertomus on Stewartin kirjassa. Trisektoreita ei esiinny ainoastaan jutussa [4] vaan olen kohdannut sellaisen elävässä elämässä....

1. Bastida, J.R., *Field extensions and Galois theory*, Addison-Wesley, 1984.
2. Bell, E.T., *Matematiikan miehiä*, Werner Söderström OY, 1963.
3. Cabric, B., *A Device for Angle Trisectioning*, Arkhimedes **43** (1991), Helsinki, 24–27.
4. Dudley, U., *What To Do When the Trisector Comes*, Mathematical Intelligencer **5** (1983), 20–24.
5. Hall, F.M., *An Introduction to Abstract Algebra*, Cambridge University Press, 1969.
6. Klein, *Gesammelte mathematische Abhandlungen*, Springer, reprint 1973.
7. Kline, *Mathematical Thought from Ancient to Modern Times*.
8. Myrberg, L., *Algebra*, Kirjayhtymä, 1978.
9. Oikkonen, J. (toim.), *Katsauksia matematiikan historiaan*, Gaudeamus, 1982.
10. Rothman, T., *Genius and Biographers: The Fictionalization of Evariste Galois.*, The American Mathematical Monthly **89** (1982), 84-107.
11. Stewart, I., *Galois Theory*, Chapman & Hall, 1973.
12. Struik, *A Source book in Mathematics,1200-1800.*.
13. van der Waerden, B.L., *Algebra*, Springer, 1966.
14. Varadarajan, V.S., *Lie groups, Lie algebras, and their representations*, Prentice-Hall, 1974.