TAMPEREEN YLIOPISTO
Pro gradu -tutkielma

Jori Mäntysalo

Resolventtimenetelmästä

Informaatiotieteiden yksikkö
Matematiikka
Kesäkuu 2013

Tampereen yliopisto

Informaatiotieteiden yksikkö

MÄNTYSALO, JORI: Resolventtimenetelmästä

Pro gradu -tutkielma, 52 s.

Matematiikka

Kesäkuu 2013

Tiivistelmä

Resolventtimenetelmä on eräs tapa määritellä polynomin Galois'n ryhmä.

Jokaista ryhmää G kohti voidaan muodostaa resolventti, joka kertoo onko Galois'n ryhmä G tai sen aliryhmä. Oikea ryhmä määritetään yhdistämällä useamman resolventin tulokset.

Resolventti on polynomi, josta tutkitaan rationaalijuurien olemassaoloa. Resolventin kertoimet voidaan esittää tutkittavan polynomin kertoimien avulla. Kokonaislukukertoimisen polynomin tapauksessa resolventin kertoimet ovat kokonaislukuja, jolloin ne voidaan myös laskea numeerisesti tutkittavan polynomin juurista ja pyöristää kokonaislukuun.

Resolventin ydin on osasymmetrinen monen muuttujan resolventtipolynomi. Esimerkiksi $f(a, b, c, d) = ab + cd$ on tällainen: jotkin permutoinnit, kuten muuttujien a ja b vaihto, eivät muuta sen arvoa. Tämä resolventtipolynomi vastaa 8-alkioista ryhmää D_4, ja vastaavasti polynomin f neljää muuttujaa voi permutoida 8 tavalla säilyttäen polynomi samana.

Tutkielmassa resolventtimenetelmän käyttö selostetaan rationaalikertoimisille polynomeille. Konkreettisena esimerkkinä laaditaan tarvittavat resolventit viidennen asteen polynomin Galois'n ryhmän selvittämiseen ja sovelletaan niitä.

Asiasanat: Galois'n ryhmä, resolventti.

Sisältö

1 Johdanto

Melko abstrakti Galois'n teoria syntyi konkreettisesta ongelmasta: viidennen asteen yhtälölle ei löytynyt samantyyppistä ratkaisukaavaa kuin 2.–4. asteen yhtälöille tunnettiin. Galois'n oivallus oli tutkia polynomin yhden juuren sijaan kaikkien juurten permutaatioita.

Nämä permutaatiot tunnetaan nimellä Galois'n ryhmä. Annetun polynomin Galois'n ryhmän voi määrittää usealla tavalla, joista resolventtimenetelmä on yksi. Ilmeisesti ensimmäisenä menetelmän esitti täsmällisesti Richard Stauduhar vuonna 1973[11].

Tutkielman voi ajatella kolmitasoisena: esitietojen jälkeen esitämme ensin resolventtimenetelmän periaatteen luvussa 3, sitten konkretisoimme sen viidennen asteen polynomeille luvussa 4, ja lopuksi luvussa 5 konkretisoimme tätä edelleen määrittämällä muutaman esimerkkipolynomin Galois'n ryhmät.

Esitiedoista luvut 2.1, 2.2 ja 2.3 kertaavat taustatietoja. Niiden tärkein tulos on rajata mahdollisuudet: Jaottoman asteen n polynomin Galois'n ryhmä on S_n tai sen transitiivinen aliryhmä. Aliryhmillä voi olla edelleen aliryhmiä, ja ryhmä voi olla useammankin ryhmän aliryhmä. Näin aliryhmät muodostavat suunnatun verkon, jota resolventeilla haarukoidaan.

Luku 2.4 käsittelee symmetrisiä polynomeja, ja on olennainen avain koko menetelmään. Luvun 2.5 sen sijaan voi hyvin ohittaa ensimmäisellä lukukerralla, sillä se koskee vain erästä erikoistilannetta.

Lopuksi luvussa 6 hahmottelemme menetelmän yleistämistä toisaalta muille kuin rationaalikertoimisille polynomeille ja toisaalta menetelmän käytännön toteutettavuutta korkeamman asteen polynomeille.

2 Taustatietoa

Tarvittava taustatieto löytyy olennaisesti samanlaisena mistä tahansa algebran oppikirjasta. Eräs vaihtoehto paperilla on [12] ja verkossa [8].

Oletamme lukijan tuntevan käsitteet kunta ja kuntalaajennus. Kertaamme muut määritelmät tiiviisti ja vain siltä osin kuin tämän tutkielman ymmärtämiseksi on tarpeen.

Käytämme merkintää $G \subset H$ kun G on ryhmän H aito aliryhmä tai vastaavasti kunnan aito alikunta. Jos voi olla myös $G = H$, merkitsemme $G \subseteq H$.

2.1 Ryhmäteoriaa

Myöhemmin määriteltävä Galois'n ryhmä voidaan tulkita juurten permutaatioryhmän transitiiviseksi aliryhmäksi. Siksi aloitamme ryhmäteorialla ja määrittelemme nämä käsitteet.

Muistin virkistykseksi esitämme oikealla Kleinin neliryhmän, jota merkitään V. Se on kuvattu abstraktina ryhmänä. Tutkimme sitten kahta ryhmän S_4 aliryhmää:

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$G_1 = \{(), (12), (34), (12)(34)\}$
$G_2 = \{(), (12)(34), (13)(24), (14)(23)\}$

Abstraktiksi ryhmäksi tulkittuna edelliset ovat Kleinin neliryhmän kanssa isomorfisia: $G_1 \cong G_2 \cong V$. Ryhmillä on silti eroa, jonka nyt määrittelemme.

Määritelmä 2.1. ([4, s. 155]) Olkoon $G \subseteq S_n$ ryhmä ja aliryhmät $H, H' \subset G$. Jos on olemassa sellainen $g \in G$, että $gHg^{-1} = H'$, niin H ja H' ovat *konjugaatteja ryhmässä* G.

Esimerkki 2.1. Ryhmä $\{(), (13), (24), (13)(24)\}$ on konjugaatti edellisen esimerkin ryhmälle G_1 ryhmässä S_4. Edellisen lauseen konjugoiva alkio g on tässä permutaatio (23).

Vapaasti kuvaten konjugaatti tarkoittaa saman asian kuvausta eri tavoin numeroituna, ja konjugoiva alkio kuvaa tätä (uudelleen)numerointia; edellä siis uudelleennumerointi tarkoitti alkioiden 2 ja 3 keskinäistä vaihtoa.

Määritelmä 2.2. ([4, s. 134]) Olkoon ryhmä $G \subseteq S_n$. Jos kaikilla $a, b \in \{1, 2, \ldots, n\}$ on olemassa $\sigma \in G$ siten, että $\sigma(a) = b$, niin aliryhmä G on *transitiivinen*.

Edellisistä esimerkeistä ryhmä G_1 ei ole transitiivinen, koska esimerkiksi alkio 1 ei siirry alkion 3 paikalle millään ryhmään kuuluvalla permutaatiolla. Ryhmä G_2 on transitiivinen.

On olennaista havaita transitiivisuuden olevan jonkin ryhmän S_n aliryhmän ominaisuus, ei abstraktin ryhmän ominaisuus.

Vapaasti kuvaten transitiivisuus tarkoittaa, että ryhmässä mikä tahansa alkio siirtyy minkä tahansa toisen alkion paikalle. Jos ryhmä ei ole transitiivinen, se voidaan jakaa osiin joiden välillä siirtymiä ei tapahdu; esimerkkiryhmässä G_1 nämä osat ovat $\{1, 2\}$ ja $\{3, 4\}$.

Havaitsimme edellä, etteivät kaksi keskenään isomorfista ryhmää välttämättä ole konjugaatteja. Palaamme tähän Galois'n ryhmien yhteydessä.

2.2 Kuntateoriaa

Tässä työssä tutkimme vain rationaalikertoimisia polynomeja. Tällöin vastaavat juurikunnat ovat tietyntyyppisiä rationaali- ja kompleksilukujen välikuntia. Kertaamme näistä muutamia määritelmiä ja lauseita. Palautamme aluksi mieleen merkinnän $K(a_1, a_2, \ldots, a_n)$: tämä tarkoittaa suppeinta kunnan K laajennusta, johon kuuluvat alkiot $a_1, a_2, \ldots, a_n$.

Määritelmä 2.3 (Kuntalaajennuksen aste)**.** (Vrt. [4, s. 88])

Olkoon L kunta, joka voidaan esittää n-ulotteisena vektoriavaruutena, jonka kerroinkunta on K.

Tällöin L on *kunnan K äärellinen laajennus* jonka *aste* on n. Aste merkitään $[L : K]$.

Määritelmä siis tarkoittaa, että kunnan L kaikkien alkioiden esittämiseksi tarvitaan vähintään n alkiota $k_1 = 1, k_2, \ldots, k_n \in L$:

$$L = \{a_1 + a_2k_2 + a_3k_3 + \cdots + a_nk_n \mid a_1, a_2, \ldots, a_n \in K\}.$$

Tällainen kunta saadaan liittämällä K-kertoimisten polynomien juuria kuntaan K. Erikoistapaus tästä on kunnan $\mathbb{Q}$ äärellinen laajennus.

Lause 2.1. (Vrt. [4, s. 78])

Olkoot $r_1, r_2, \ldots, r_n$ rationaalikertoimisten polynomien juuria.

Tällöin $\mathbb{Q}(r_1, r_2, \ldots, r_n)$ on rationaalilukujen äärellinen laajennus.

Todistus: Sivuutetaan.

Teemme edellisistä esimerkin

Esimerkki 2.2. Luvut $\sqrt{2}$ ja $\sqrt{3}$ ovat selvästi eräiden polynomien juuria. Tällöin joukko

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a_1 + a_2\sqrt{2} + a_3\sqrt{3} + a_4\sqrt{6} \mid a_1, a_2, a_3, a_4 \in \mathbb{Q}\}$$

on kunta. Se on kunnan $\mathbb{Q}$ äärellinen laajennus ja $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=4$.

Kuntalaajennuksia voidaan laajentaa edelleen.

Lause 2.2 (Tornilause)**.** ([4, s. 91])

Olkoot M/L ja L/K kuntalaajennuksia.

Tällöin $[M:K]=[M:L][L:K]$.

Todistus: sivuutetaan.

Esimerkki 2.3. Joukko $\mathbb{Q}(\sqrt{2})=\{a_1+a_2\sqrt{2}\mid a_1,a_2\in\mathbb{Q}\}$ on kunta ja $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$. Edellä todettiin $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=4$. Siis laajennuksen $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}(\sqrt{2})$ aste on $4/2=2$. Auki purettuna tämä laajennus on

$$\mathbb{Q}(\sqrt{2},\sqrt{3})=\{a_1+a_2\sqrt{3}\mid a_1,a_2\in\mathbb{Q}(\sqrt{2})\}.$$

Edellä esitetyn perusteella polynomille voidaan määritellä juurikunta, suppein — ja erityisesti äärellinen — kuntalaajennus joka sisältää kaikki juuret. Algebran peruslauseen nojalla kompleksilukukertoimisen polynomin kaikki juuret ovat kompleksilukuja (vrt. [4, s. 62–66]). Näin rationaalikertoimisen polynomin juurikunta on rationaalilukujen äärellinen laajennus ja kompleksilukujen aito alikunta.

Määritelmä 2.4. (Vrt. esim. [8, s. 341]) Olkoon $P\in\mathbb{Q}[x]$ polynomi, jonka juuret ovat $r_1,r_2,\ldots,r_n\in\mathbb{C}$. Kunta

$$\mathbb{Q}(r_1,r_2,\ldots,r_n)\subset\mathbb{C}$$

on polynomin P *juurikunta*.

Ennen esimerkkiä määrittelemme lisää.

Määritelmä 2.5. (vrt. [8, s. 373])

Olkoon $L/\mathbb{Q}$ kuntalaajennus ja f bijektio $L\to L$ siten, että

- $\forall a,b\in L\colon f(a+b)=f(a)+f(b)$,
- $\forall a,b\in L\colon f(ab)=f(a)f(b)$ ja
- $\forall x\in\mathbb{Q}\colon f(x)=x$.

Tällöin f on $\mathbb{Q}$-*automorfismi*.

Teemme edellisistä esimerkin.

Esimerkki 2.4. Tutkitaan polynomin $P(x) = x^2 - 2$ juurikuntaa $\mathbb{Q}(\sqrt{2})$.

Olkoon funktio

$$f(a_1 + a_2\sqrt{2}) = a_1 - a_2\sqrt{2}.$$

Selvästi $\forall x, y \in \mathbb{Q}(\sqrt{2})$ pätee $f(x + y) = f(x) + f(y)$, ja helpolla laskutoimituksella nähdään $f(xy) = f(x)f(y)$. Jos x on rationaaliluku, niin $f(x) = x$.

Siis f on $\mathbb{Q}$-automorfismi kunnassa $\mathbb{Q}(\sqrt{2})$.

Määritimme siis edellä polynomin juurikunnan $\mathbb{Q}$-automorfismin; itse asiassa Galois'n ryhmän alkion, johon palaamme seuraavassa luvussa.

Tarvitsemme vielä polynomien jaollisuuteen liittyvän lauseen. Seuraava ei liity aiemmin esitettyyn.

Lause 2.3. (Vrt. [4, s. 110])

Rationaalikertoiminen polynomi, jolla on moninkertainen juuri, on jaollinen.

Todistus:

Tehdään vastaoletus: $P \in \mathbb{Q}[x]$ on jaoton polynomi, jolla on moninkertainen juuri r.

Lasketaan ensin derivaatta pisteessä r. Vastaoletuksen nojalla P on muotoa $(x - r)^2Q$, jossa Q on jokin polynomi. Tämän derivaatta on $(2x - 2r)Q + (x - r)^2Q'$. Siis r on myös derivaatan P' nollakohta.

Lasketaan polynomien P ja P' suurin yhteinen tekijä. Olkoon $R \in \mathbb{Q}[x]$ jokin polynomi, joka jakaa polynomit P ja P'. Koska vastaoletuksen mukaan P on jaoton, on R vakio tai P kerrottuna vakiolla. Viimeksimainitussa tapauksessa polynomin R aste on sama kuin polynomin P, jolloin se ei voi jakaa pienempää astetta olevaa polynomia P'.

Siis polynomin R on oltava vakio. Tällöin on Bézoutin lemmana tunnetun lauseen (lähde [8, s. 271–272]; lähde ei nimeä lausetta) perusteella olemassa polynomit $S \in \mathbb{Q}[x]$ ja $T \in \mathbb{Q}[x]$ siten, että

$$SP + TP' = 1.$$

Sijoittamalla tähän $x = r$ saadaan $0 = 1$. Tämä on ristiriita ja todistaa alkuperäisen väitteen.

2.3 Galois'n ryhmä

Tässä työssä tutkimme erästä tapaa määritellä polynomin Galois'n ryhmä. Aloitamme määritelmästä ja pohdimme sitten millä tarkkuudella Galois'n ryhmä on mielekästä kertoa.

Määritelmä 2.6. ([8, s. 373], [4, s. 134])

Olkoon $L/\mathbb{Q}$ äärellinen kuntalaajennus.

Kunnan L kaikki $\mathbb{Q}$-automorfismit muodostavat ryhmän laskutoimituksena funktioiden yhdistäminen. Tämä on *kuntalaajennuksen Galois'n ryhmä* ja se merkitään $\mathrm{Gal}(L/\mathbb{Q})$.

Jos L on polynomin $P \in \mathbb{Q}[x]$ juurikunta, on tämä myös *polynomin P Galois'n ryhmä* ja se merkitään $\mathrm{Gal}(P)$.

Teemme ensin esimerkin kuntalaajennuksen Galois'n ryhmästä.

Esimerkki 2.5. Tutkitaan kuntaa $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Tällä on tunnetusti (esim. [8, s. 373–374]) neljä $\mathbb{Q}$-automorfismia:

$f_0(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$
$f_1(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$
$f_2(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$
$f_3(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}.$

Nämä funktiot muodostavat Kleinin neliryhmän kanssa isomorfisen ryhmän, kun laskutoimitukseksi otetaan funktioiden yhdistäminen.

Polynomin Galois'n ryhmää voidaan ajatella toisinkin. Tässä palaamme tapaan, jolla Galois itse käsitteli nykyään hänen nimeään kantavaa ryhmää[4, s. 135].

Lause 2.4. ([8, s. 374])

Polynomin Galois'n ryhmän alkio kuvaa juuren juurelle.

Todistus: Olkoon $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ rationaalikertoiminen polynomi. Olkoon r polynomin P juuri ja f jokin joukon $\mathrm{Gal}(P)$ alkio. Tällöin

$0 = f(0) \Leftrightarrow$ (automorfismissa nolla kuvautuu aina nollaan)
$0 = f(P(r)) \Leftrightarrow$ (oletuksen mukaan $P(r) = 0$)
$0 = f(a_n r^n + a_{n-1}r^{n-1} + \cdots + a_0) \Leftrightarrow$ (polynomi purettu)
$0 = f(a_n r^n) + f(a_{n-1}r^{n-1}) + \cdots + f(a_0) \Leftrightarrow$ (summan automorfismi)
$0 = f(a_n)f(r)^n + f(a_{n-1})f(r)^{n-1} + \cdots + f(a_0) \Leftrightarrow$ (tulon automorfismi)
$0 = a_n f(r)^n + a_{n-1}f(r)^{n-1} + \cdots + a_0$ (koska $a_i \in \mathbb{Q}$, niin $f(a_i) = a_i$)
$0 = P(f(r))$ (polynomi koottu)

Jokainen Galois'n ryhmän automorfismi siis permutoi juuret jollain tavalla.

Lause 2.5. ([4, s. 133])

Olkoon $P \in \mathbb{Q}[x]$ astetta n ja $r_1, r_2, \ldots, r_n$ sen juuret.

Tällöin voidaan muodostaa injektiivinen homomorfismi $\mathrm{Gal}(P) \to S_n$.

Todistus:

Olkoon $f \in \mathrm{Gal}(P)$. Edellisen lauseen perusteella se kuvaa juuren juurelle. Koska Galois'n ryhmän alkio on automorfismi, se on bijektio. Tällöin kaksi eri juurta eivät voi kuvautua samalle juurelle. Funktio f voidaan siis kuvata juurten yhtenä permutaationa:

$$\mathrm{Gal}(P) \to S_n \colon f \mapsto \sigma$$

jossa

$$f(r_i) = r_j \Leftrightarrow \sigma(i) = j.$$

Todistamme kuvauksen homomorfismiksi. Kuvautukoot $f, g \in \mathrm{Gal}(P)$ permutaatioiksi siten, että $f \mapsto \sigma$ ja $g \mapsto \tau$. Tällöin

$$(f \circ g)(i) = f(g(i)) = j \Rightarrow \sigma(\tau(i)) = (\sigma \circ \tau)(i).$$

Siis Galois'n ryhmää voidaan tarkastella ryhmänä funktioita laskutoimituksena funktioiden yhdistäminen tai ryhmänä juurien permutaatioita laskutoimituksena permutaatioiden yhdistäminen. Viimeksimainittu näkökulma kertoo enemmän. Palaamme edelliseen esimerkkiin.

Esimerkki 2.6. Tutkitaan polynomeja $P, Q \in \mathbb{Q}[x]$:

$P(x) = x^4 - 10x^2 + 1 = (x - \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x + \sqrt{2} - \sqrt{3})(x + \sqrt{2} + \sqrt{3})$
$Q(x) = x^4 - 5x^2 + 6 = (x - \sqrt{2})(x + \sqrt{2})(x - \sqrt{3})(x + \sqrt{3})$

Molempien juurikunta on $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ ja siis $\mathrm{Gal}(P) \cong \mathrm{Gal}(Q) \cong V$, kuten edellä totesimme.

Numeroidaan juuret:
P: $r_1 = -\sqrt{2} - \sqrt{3}$, $r_2 = +\sqrt{2} - \sqrt{3}$, $r_3 = -\sqrt{2} + \sqrt{3}$, $r_4 = +\sqrt{2} + \sqrt{3}$
Q: $r_1 = -\sqrt{2}$, $r_2 = +\sqrt{2}$, $r_3 = -\sqrt{3}$, $r_4 = +\sqrt{3}$.

Tutkitaan mihin edellisen esimerkin $\mathbb{Q}$-automorfismit kuvaavat juuret.

f_0: $P\colon (r_1, r_2, r_3, r_4) \to (r_1, r_2, r_3, r_4)$ $Q\colon (r_1, r_2, r_3, r_4) \to (r_1, r_2, r_3, r_4)$
f_1: $P\colon (r_1, r_2, r_3, r_4) \to (r_2, r_1, r_4, r_3)$ $Q\colon (r_1, r_2, r_3, r_4) \to (r_2, r_1, r_3, r_4)$
f_2: $P\colon (r_1, r_2, r_3, r_4) \to (r_3, r_4, r_1, r_2)$ $Q\colon (r_1, r_2, r_3, r_4) \to (r_1, r_2, r_4, r_3)$
f_3: $P\colon (r_1, r_2, r_3, r_4) \to (r_4, r_3, r_2, r_1)$ $Q\colon (r_1, r_2, r_3, r_4) \to (r_2, r_1, r_4, r_3)$

Tiivistäen Galois'n ryhmät vastaavat seuraavia juurien permutaatioryhmiä:
P: $\{(), (r_1\ r_2)(r_3\ r_4), (r_1\ r_3)(r_2\ r_4), (r_1\ r_4)(r_2\ r_3)\}$.
Q: $\{(), (r_1\ r_2), (r_3\ r_4), (r_1\ r_2)(r_3\ r_4)\}$.

Havaitsemme, että polynomin P Galois'n ryhmä vastaa muodoltaan edellä ryhmäteorian yhteydessä esimerkkinä ollutta ryhmää G_2, polynomin Q Galois'n ryhmä vastaavasti ryhmää G_1.

Numeroimalla juuret toisin olisi ryhmän $\{(), (r_1\ r_2), (r_3\ r_4), (r_1\ r_2)(r_3\ r_4)\}$ sijaan edellä voinut olla esimerkiksi $\{(), (r_1\ r_3), (r_2\ r_4), (r_1\ r_3)(r_2\ r_4)\}$ tai muu tämän aliryhmän konjugaatti. Jokainen juurien uudelleennimeäminen voidaan esittää sarjana kahden juuren keskinäisiä vaihtoja. Tällainen vaihto $(r_i\ r_j)$ vastaa ryhmän kertomista vasemmalta permutaatiolla $(r_i\ r_j)$ ja oikealta permutaatiolla $(r_j\ r_i)$, jolloin tuloksena on konjugaatti.

On siis kolme tapaa kuvata Galois'n ryhmä:

1. Abstrakti ryhmä. Esimerkki: Polynomin Q Galois'n ryhmä on V, niin myös polynomin P.
2. Konjugointia vaille yksikäsitteinen permutaatioryhmä. Esimerkki: Polynomin Q Galois'n ryhmän muoto on $\{(), (12), (34), (12)(34)\}$, polynomin P ei ole.
3. Juuret nimettynä yksikäsitteinen permutaatioryhmä. Esimerkki: Polynomin P Galois'n ryhmän alkiot ovat $()$, $(+\sqrt{2}, -\sqrt{2})$, $(+\sqrt{3}, -\sqrt{3})$ ja $(+\sqrt{2}, -\sqrt{2})(+\sqrt{3}, -\sqrt{3})$.

Edellisen esimerkin polynomi P on jaoton ja sitä vastaava Galois'n ryhmä transitiivinen. Sen sijaan Q on jaollinen, $Q(x) = (x^2 - 2)(x^2 - 3)$, ja vastaava Galois'n ryhmä ei ole transitiivinen. Tämä on yleinen sääntö[4, 134], josta tässä todistamme implikaation toiseen suuntaan.

Todistuksen olennainen idea on se, että liittämällä rationaalilukuihin mikä tahansa jaottoman polynomin juurista päädytään samanlaiseen kuntaan. Esimerkiksi $\sqrt[4]{2}$ ja $i\sqrt[4]{2}$ ovat jaottoman polynomin $x^4 - 2$ juuria, joten $\mathbb{Q}(\sqrt[4]{2}) \cong \mathbb{Q}(i\sqrt[4]{2})$.

Isomorfismi lasketaan kaksivaiheisesti. Esimerkiksi pisteelle $2\sqrt[4]{2} - 3\sqrt{2}$ etsitään ensin polynomi, jonka arvo juuressa $\sqrt[4]{2}$ on haettu luku. Se on $-3x^2 + 2x$. Sitten tähän sijoitetaan juuri $i\sqrt[4]{2}$ ja saadaan $3\sqrt{2} + 2i\sqrt[4]{2}$. Siis tässä kuvauksessa esimerkiksi $2\sqrt[4]{2} - 3\sqrt{2} \in \mathbb{Q}(\sqrt[4]{2}) \mapsto 2i\sqrt[4]{2} + 3\sqrt{2} \in \mathbb{Q}(i\sqrt[4]{2})$.

Varsinaista todistusta varten palautamme ensin mieleen rengasteoriasta ideaalien ja homomorfismien yhteyden. Homomorfismin ydin on ideaali, ja kääntäen renkaan R ideaalia I vastaa yksikäsitteinen homomorfismi, joka kuvaa kunkin alkion jäännösluokalleen. Jos R ja R' ovat renkaita ja f homomorfismi $R \to R'$, niin $R/\ker f \cong \operatorname{Im} f$ — siis tekijärengas on isomorfinen homomorfismin kuvan kanssa.[8, s. 249–251]

Toiseksi tarvitsemme kuntien isomorfian laajennuslausetta. Sen mukaan kunnan K isomorfismi voidaan laajentaa kunnan $K(a)$ isomorfismiksi, kun a on algebrallinen[12, s. 44].

Lause 2.6. (Vrt. [4, s. 77, 105])

Olkoon polynomi $P \in \mathbb{Q}[x]$ jaoton. Tällöin $\mathrm{Gal}(P)$ on transitiivinen.

Todistus: Olkoot r ja r' mielivaltaisesti valitut polynomin P juuret. Todistukseksi riittää osoittaa, että jokin Galois'n ryhmän alkio kuvaa juuren r juurelle r'.

Osoitamme ensin, että on olemassa isomorfismi $\mathbb{Q}(r) \cong \mathbb{Q}[x]/\langle P \rangle$.

Olkoon f sijoitushomomorfismi $\mathbb{Q}[x] \to \mathbb{C}$, joka laskee polynomin P pisteessä r; siis $f(P) = P(r)$.

Määritelmän mukaan tällöin $\mathrm{Im}\, f = \mathbb{Q}(r)$.

Osoitamme $\ker f = \langle P \rangle$ osoittamalla ensin $\langle P \rangle \subseteq \ker f$ ja sitten $\ker f \subseteq \langle P \rangle$.

Olkoon mielivaltainen polynomi $Q \in \mathbb{Q}[x]$. Tällöin $f(QP) = f(Q)f(P) = Q(r)P(r) = Q(r)0 = 0$, eli $\langle P \rangle \subseteq \ker f$.

Oletetaan sitten, että polynomi $Q \in \ker f$, eli $Q(r) = 0$. Koska P on minimipolynomi, pitää olla $Q = PQ'$, jossa $Q' \in \mathbb{Q}[x]$. Siis $\ker f \subseteq \langle P \rangle$.

Edellämainitun renkaiden isomorfialauseen perusteella on olemassa haluttu isomorfia $\mathbb{Q}[x]/\langle P \rangle \cong \mathbb{Q}(r)$. Tämä isomorfia on identiteettifunktio rationaaliluvuille ja kuvaa jäännösluokan $x + \langle P \rangle$ alkiolle r.

Vastaava päättely voidaan tietysti toistaa juurelle r'. Näin saadaan isomorfiaketju $\mathbb{Q}(r) \cong \mathbb{Q}[x]/\langle P \rangle \cong \mathbb{Q}(r')$.

Haluttu Galois'n ryhmän alkio saadaan yhdistämällä edelliset isomorfiat. Joukkojen $\mathbb{Q}(r)$ ja $\mathbb{Q}[x]/\langle P \rangle$ välillä on bijektio, jossa rationaaliluku $q \in \mathbb{C}$ kuvautuu vakiopolynomille $q \in \mathbb{Q}[x]$ ja juuri $r \in \mathbb{C}$ 1. asteen polynomille $x \in \mathbb{Q}[x]$. Tämä ja vastaava bijektio juurelle r' yhdistämällä saadaan bijektio, jossa rationaaliluvut kuvautuvat itselleen ja juuri r juurelle r'.

Isomorfian laajennuslauseen perusteella isomorfia $\mathbb{Q}(r) \to \mathbb{Q}(r')$ voidaan laajentaa isomorfiaksi $\mathbb{Q}(r, s) \to \mathbb{Q}(r', s_1)$ jossa s on jokin kuntaan $\mathbb{Q}(r)$ kuulumaton polynomin juuri. Tätä laajennusta voidaan jatkaa juuri kerrallaan koko juurikuntaan saakka.

Näin päädyimme työn lähtöpisteeseen: astetta n olevan jaottoman rationaalikertoimisen polynomin Galois'n ryhmä on jokin ryhmän S_n transitiivinen aliryhmä.

Myös jaottomien polynomien Galois'n ryhmät voivat olla keskenään isomorfisia olematta silti konjugaatteja.

Esimerkki 2.7. Tutkitaan ryhmän S_6 aliryhmiä Sage-ohjelmistolla:

```
def t(g): return PermutationGroup(g.gens())
G=Set(map(t, TransitiveGroups(6))).subsets(2)
[ (g[0], g[1]) for g in G if g[0].is_isomorphic(g[1])]
```

tulostaa

```
. . . [(1,3,5)(2,4,6), (1,4)(2,5), (1,5)(2,4)]
. . . [(1,3,5)(2,4,6), (1,4)(2,5), (1,5)(2,4)(3,6)]
```

Siis ryhmän S_6 transitiiviset aliryhmät $\langle(1,3,5)(2,4,6),(1,4)(2,5),(1,5)(2,4)\rangle$ ja $\langle(1,3,5)(2,4,6),(1,4)(2,5),(1,5)(2,4)(3,6)\rangle$ ovat keskenään isomorfisia mutta eivät konjugaatteja.

Myöhemmin havaitsemme, että jaottomilla viidennen asteen polynomeilla näin ei käy: jos ryhmän S_5 transitiiviset aliryhmät jaetaan konjugaattityyppeihin, on jokainen tyyppi erilainen myös abstraktina ryhmänä. Siksi tulemme käyttämään esimerkiksi muotoa $\mathrm{Gal}(P) \cong D_5$.

Jatkoon tarvitsemme Galois'n teoriasta yhden lauseen.

Lause 2.7. ([4, s. 130])

Olkoon $P \in K[x] \subseteq \mathbb{C}[x]$ jaoton polynomi, jonka juurikunta on L.

Tällöin $[L : K] = |\,\mathrm{Gal}(P)|$.

Todistus: sivuutetaan.

Esimerkki tästä saatiin jo aiemmin: $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = 4$ ja esimerkissä 2.5 esitimme kunnan $\mathbb{Q}(\sqrt{2},\sqrt{3})$ neljä $\mathbb{Q}$-automorfismia.

Todistamme edellisen perusteella, että Galois'n ryhmän alkiot ovat täsmällisesti $\mathbb{Q}$-automorfismeja, eivätkä kiinnitä laajempaa alikuntaa.

Lause 2.8. ([4, s. 148])

Olkoon L polynomin $P \in \mathbb{Q}[x]$ juurikunta.

Jos $x \in L\backslash\mathbb{Q}$, niin on olemassa sellainen $f \in \mathrm{Gal}(P)$ että $f(x) \neq x$.

Todistus:

Olkoon $\mathbb{Q}' \subseteq L$ alikunta, jonka $\mathrm{Gal}(P)$ kiinnittää. Osoitetaan $\mathbb{Q}' = \mathbb{Q}$.

Selvästi L on polynomin P juurikunta myös kun P tulkitaan $\mathbb{Q}'$-kertoimiseksi.

Edellisen lauseen perusteella $[L : \mathbb{Q}'] = |\,\mathrm{Gal}(L/\mathbb{Q}')|$ ja $[L : \mathbb{Q}] = |\,\mathrm{Gal}(L/\mathbb{Q})|$. Toisaalta $[L : \mathbb{Q}] = [L : \mathbb{Q}'][\mathbb{Q}' : \mathbb{Q}]$. Nämä yhdistämällä saadaan

$$|\,\mathrm{Gal}(L/\mathbb{Q})| = |\,\mathrm{Gal}(L/\mathbb{Q}')|[\mathbb{Q}' : \mathbb{Q}] \tag{1}$$

Osoitetaan $\mathrm{Gal}(L/\mathbb{Q}') = \mathrm{Gal}(L/\mathbb{Q})$. Koska $\mathbb{Q} \subseteq \mathbb{Q}'$, niin $\mathbb{Q}'$-automorfismi on aina $\mathbb{Q}$-automorfismi eli $\mathrm{Gal}(L/\mathbb{Q}') \subseteq \mathrm{Gal}(L/\mathbb{Q})$. Toisaalta oletuksen mukaan $\mathrm{Gal}(P)$ kiinnittää kunnan $\mathbb{Q}'$ eli $\mathrm{Gal}(L/\mathbb{Q}') \supseteq \mathrm{Gal}(L/\mathbb{Q})$.

Siis $\mathrm{Gal}(L/\mathbb{Q}') = \mathrm{Gal}(L/\mathbb{Q})$ eli erityisesti $|\,\mathrm{Gal}(L/\mathbb{Q}')| = |\,\mathrm{Gal}(L/\mathbb{Q})|$. Sijoittamalla tämä kaavaan 1 saadaan $[\mathbb{Q}' : \mathbb{Q}] = 1$ eli $\mathbb{Q}' = \mathbb{Q}$.

Tämä on keskeisin pohja työn päälauseelle, joten toistamme tuloksen.

Seuraus 2.1. Galois'n ryhmä jakaa polynomin juurikunnan alkiot täsmällisesti kahteen joukkoon.

$x \in \mathbb{Q} \quad \Leftrightarrow$ Kaikki Galois'n ryhmän automorfismit kiinnittävät alkion x.
$x \notin \mathbb{Q} \quad \Leftrightarrow$ Jokin Galois'n ryhmän automorfismi "siirtää" alkiota x.

2.4 Symmetriset polynomit

Mitä on polynomin $x^3 + ax^2 + bx + c$ juurien neliöiden summa?

Vastaus, $a^2 - 2b$, on helppo osoittaa oikeaksi: juurien summa on $-a$, juurien pareittaisten tulojen summa on b ja $(r_1 + r_2 + r_3)^2 - 2(r_1r_2 + r_1r_3 + r_2r_3) = r_1^2 + r_2^2 + r_3^2$. Symmetriset polynomit kertovat miten vastaus löydetään.

Tulemme myöhemmin havaitsemaan, että tämän työn keskeisin käsite eli resolventti on nimenomaan symmetrinen polynomi. Kuten edellä juurien neliösumma, myös resolventit voidaan osoittaa oikeiksi helposti, mutta symmetristen polynomien teoriaa tarvitaan niiden muodostamiseen.

Edellä oli jo hyvä esimerkki *alkeis*symmetrisestä polynomista, $r_1r_2+r_1r_3+r_2r_3$. Määrittelemme käsitteen täsmällisesti.

Määritelmä 2.7. ([4, s. 27]) Lukujen $y_1, y_2, \ldots, y_n$ *alkeissymmetrinen polynomi* on tulojen summa, jossa kerrotaan aina k lukua kerrallaan. Se merkitään e_k.

$$e_k(y_1, y_2, \ldots, y_n) = \sum_{1 \le j_1 < j_2 < \cdots < j_k \le n} y_{j_1} y_{j_2} \cdots y_{j_k}$$

Esimerkiksi neljän luvun alkeissymmetriset polynomit ovat siis
$e_1(y_1, y_2, y_3, y_4) = y_1 + y_2 + y_3 + y_4$
$e_2(y_1, y_2, y_3, y_4) = y_1y_2 + y_1y_3 + y_1y_4 + y_2y_3 + y_2y_4 + y_3y_4$
$e_3(y_1, y_2, y_3, y_4) = y_1y_2y_3 + y_1y_2y_4 + y_1y_3y_4 + y_2y_3y_4$
$e_4(y_1, y_2, y_3, y_4) = y_1y_2y_3y_4$.

Määrittelemme sitten symmetrisen polynomin.

Määritelmä 2.8. ([4, s. 30]) Olkoon polynomi $P \in \mathbb{Q}[y_1, y_2, \ldots, y_n]$. Jos

$$\forall \sigma \in S_n \colon P(y_1, y_2, \ldots, y_n) = P(y_{\sigma(1)}, y_{\sigma(2)}, \ldots, y_{\sigma(n)})$$

niin P on *symmetrinen polynomi*.

Epämuodollisesti kuvaten alkeissymmetrinen polynomi on polynomifunktio, joka ei välitä parametriensa järjestyksestä. Esimerkiksi luvun alussa ollut

juurien neliöiden summa on juurien symmetrinen polynomi, mutta ei alkeissymmetrinen.

Alun esimerkissä esitimme symmetrisen polynomin alkeissymmetristen polynomien avulla. Osoitamme, että vastaava esitystapa on aina mahdollinen.

Todistus on algoritminen. Symmetrisen polynomin termeistä valitaan kussakin suoritusaskeleessa "suurin" tutkimalla ensin muuttujan y_1 eksponenttia, sitten muuttujan y_2 eksponenttia ja niin edelleen. Tämä termi korvataan alkeissymmetristen polynomien tulolla siten, että tämän tulon sivutuotteina syntyy käsiteltävää termiä "pienempiä" termejä. Näin algoritmi väistämättä päättyy joskus.

Lause 2.9 (Symmetristen polynomien päälause)**.** (Vrt. [4, s. 30–32])

Jokainen symmetrinen polynomi voidaan esittää alkeissymmetristen polynomien yhteen-, vähennys- ja kertolaskujen avulla.

Todistus:

1: Määritelmät

Määritellään ensin järjestysrelaatio $\succ$ monen muuttujan polynomin termeille. Merkitään polynomin muuttujat $y_1, y_2, \ldots, y_n$.

$$\begin{aligned} c_a y_1^{a_1} y_2^{a_2} \cdots y_n^{a_n} \succ c_b y_1^{b_1} y_2^{b_2} \cdots y_n^{b_n} \iff\ & a_1 > b_1 \text{ tai} \\ & a_1 = b_1 \text{ ja } a_2 > b_2 \text{ tai} \\ & a_1 = b_1 \text{ ja } a_2 = b_2 \text{ ja } a_3 > b_3 \text{ tai} \\ & \quad \ldots \end{aligned}$$

Sanotaan "A on suurempi kuin B" kun $A \succ B$ ja tämän vastakohtaa sanotaan "pienempi kuin". Termiä, jota suurempaa termiä polynomissa ei ole, kutsutaan nimellä "johtava termi".

2: Johtavassa termissä muuttujien eksponentit ovat väheneviä

Olkoon johtava termi

$$A = y_1^{a_1} y_2^{a_2} \cdots y_k^{a_k} y_{k+1}^{a_{k+1}} \cdots y_n^{a_n}.$$

Tehdään vastaoletus: johtavassa termissä on

$$a_1 \geq a_2 \geq \cdots \geq a_{k-1} \geq a_k, \text{ mutta } a_k < a_{k+1}.$$

Oletuksen nojalla polynomi on symmetrinen, jolloin siinä on myös termi

$$A' = y_1^{a_1} y_2^{a_2} \cdots y_k^{a_{k+1}} y_{k+1}^{a_k} \cdots y_n^{a_n}.$$

Määritellyn järjestysrelaation perusteella A' on suurempi kuin A. Tämä on ristiriita.

3: Johtavaa termiä pienempiä termejä on äärellinen määrä

Olkoon johtava termi

$$A = y_1^{a_1} y_2^{a_2} \cdots y_k^{a_k} \cdots y_n^{a_n}.$$

Osoitetaan, että mikään eksponenteista $a_2, a_3, \ldots, a_n$ ei voi olla suurempi kuin a_1. Tehdään vastaoletus: $a_k > a_1$. Tällöin on symmetrian nojalla olemassa termi

$$A' = y_1^{a_k} y_2^{a_2} \cdots y_k^{a_1} \cdots y_n^{a_n}$$

ja jälleen saadaan ristiriita $A' \succ A$.

Kun jokaisen termin eksponentti on rajoitettu, on erilaisia termejä äärellinen määrä.

4: Algoritmin korvausaskeleen kuvaus

Kussakin suoritusaskeleessa johtava termi korvataan alkeissymmetristen polynomien tulolla:

$$c y_1^{i_1} y_2^{i_2} \cdots y_{n-1}^{i_{n-1}} y_n^{i_n} \;\rightarrow\; c e_1^{i_1 - i_2} e_2^{i_2 - i_3} \cdots e_{n-1}^{i_{n-1} - i_n} e_n^{i_n}.$$

Kohdan 2 perusteella eksponentit $i_1 - i_2, i_2 - i_3, \ldots, i_{n-1} - i_n$ ovat ei-negatiivisia ja korvaus on tehtävissä.

4.1: Korvaus tuottaa johtavan termin

Alkeissymmetristen polynomien $e_1, e_2, \ldots, e_n$ johtavat termit ovat $y_1, y_1 y_2, \ldots, y_1 y_2 \cdots y_n$. Korvattava termi syntyy näiden tulosta

$$(y_1)^{i_1 - i_2} (y_1 y_2)^{i_2 - i_3} \cdots (y_1 y_2 \cdots y_k)^{i_k - i_{k+1}} \cdots (y_1 y_2 \cdots y_n)^{i_n}$$

sillä muuttujan y_k eksponentiksi tulee

$$(i_k - i_{k+1}) + (i_{k+1} - i_{k+2}) + \cdots + (i_{n-1} - i_n) + i_n = i_k.$$

4.2: Korvaus ei tuota johtavaa termiä suurempia termejä

Korvaus tuottaa myös muita termejä. Tehdään vastaoletus: jokin näistä on johtavaa termiä suurempi termi

$$A' = (y_1)(y_1 y_2) \cdots (y_1 y_2 \cdots y_{k-1}) E_k E_{k+1} \cdots E_n$$

jossa E_i kuvaa alkeissymmetrisen polynomin e_i termiä ja jossa erityisesti $E_k \neq y_1 y_2 \cdots y_k$. Olkoon $l \leq k$ pienin sellainen indeksi, että termi E_k ei sisällä muuttujaa y_l. Tällöin A' on pienempi kuin johtava termi

$$A = ce_1^{i_1 - i_2} e_2^{i_2 - i_3} \cdots e_{n-1}^{i_{n-1} - i_n} e_n^{i_n}$$

sillä muuttujien $y_1, y_2, \ldots, y_{l-1}$ eksponentit ovat tulossa A' enintään yhtäsuuria kuin tulossa A, ja muuttujan y_l eksponentti on suurempi tulossa A.

5: Algoritmin kuvaus

Tehdään polynomin termeistä lista T ja alustetaan lista S tyhjäksi.

Kohdan 4 mukaisia korvauksia toistetaan johtavalle termille, kunnes lista T on tyhjä. Jokaisella askeleella listalle S lisätään kohdan 4 mukainen alkeissymmetristen polynomien tulo, ja listalta T poistetaan sillä olleet termit, jotka korvausaskel tuotti. Listalle T lisätään ne termit, jotka korvausaskel tuotti ja joita siinä ei entuudestaan ollut.

Kohdan 4.2 perusteella algoritmin suoritusaskel tuottaa johtavan termin lisäksi ainoastaan sellaisia muita termejä, jotka ovat johtavaa termiä pienempiä.

Symmetristen polynomien tulo on selvästi symmetrinen, ja kun tämä vähennetään toisesta symmetrisestä polynomista, on erotuskin symmetrinen. Näin lista T säilyy symmetrisenä ja korvauksia voidaan jatkaa. Kohdan 3 perusteella johtavaa termiä pienempiä termejä on olemassa äärellinen määrä. Täten algoritmi päättyy äärellisessä ajassa.

Alun esimerkissä eli juurien neliöiden summassa johtava termi oli $r_1^2 r_2^0 r_3^0$, ja korvaava alkeissymmetristen polynomien tulo siis $e_1^{2-0} e_2^{0-0} e_3^0$. Havainnollistamme algoritmin yhtä askelta hieman monimutkaisemmassa tilanteessa:

Esimerkki 2.8. Olkoon johtava termi

$$y_1^9 y_2^6 y_3^2.$$

Tällöin tarvittava alkeissymmetristen polynomien tulo on

$$e_1^{9-6} e_2^{6-2} e_3^2 = e_1^3 e_2^4 e_3^2 = (y_1 + y_2 + y_3)^3 (y_1 y_2 + y_1 y_3 + y_2 y_3)^4 (y_1 y_2 y_3)^2.$$

Johtava termi saadaan tulon tekijöistä

$$(y_1 + \cdots)^3 (y_1 y_2 + \cdots)^4 (y_1 y_2 y_3)^2.$$

Pitkähkön tulon muut termit ovat

$$4y_1^9y_2^5y_3^3 \succ 6y_1^9y_2^4y_3^4 \succ \cdots \succ 3y_1^8y_2^7y_3^2 \succ 19y_1^8y_2^6y_3^3 \succ \cdots \succ y_1^2y_2^6y_3^9.$$

Tässä suurinkin termi siis on käsiteltyä termiä myöhemmin — muuttujan y_1 eksponentti on sama ja muuttujan y_2 eksponentti yhtä pienempi kuin käsitellyssä termissä.

Havaitsemme lisäksi, että kukin korvausaskel voi korvata useampia termejä. Tässä esimerkissä termin $y_1^9y_2^6y_3^2$ lisäksi symmetrisessä polynomissa on symmetrian nojalla oltava termi $y_3^9y_2^6y_1^2$, joka näkyy edellä tulon pienimpänä terminä.

Monen muuttujan symmetriset polynomit liittyvät läheisesti yhden muuttujan polynomin juuriin.

Lause 2.10. Kokonaislukukertoimisen pääpolynomin juurien symmetrisen polynomin arvo on kokonaisluku.

Todistus:

Olkoon $P(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$ pääpolynomi, jolla on juuret $r_1, r_2, \ldots, r_n$.

Polynomin kertoimet ovat sen juurien symmetrisiä polynomeja tai niiden vastalukuja:

$$\begin{aligned} a_{n-1} &= -e_1(r_1, r_2, \ldots, r_n) \\ a_{n-2} &= +e_2(r_1, r_2, \ldots, r_n) \\ a_{n-3} &= -e_3(r_1, r_2, \ldots, r_n) \\ &\ldots \end{aligned}$$

Kokonaislukujen alkeissymmetriset polynomit ovat kokonaislukujen tulojen summia, siis kokonaislukuja.

Lauseen 2.9 perusteella symmetrinen polynomi voidaan esittää alkeissymmetristen polynomien yhteen-, vähennys ja kertolaskujen avulla. Tällöin symmetrisen polynomin arvo on kokonaisluku.

Tämän lauseen merkitys tulee ilmi numeerisessa laskennassa.

Esimerkki 2.9. Lasketaan polynomin $x^3 + 2x^2 - 3x - 5$ juurien neliöiden summa käyttämättä luvun alussa esitettyä kaavaa.

Juuret ovat noin $-2{,}38$, $-1{,}27$ ja $1{,}65$, niiden neliöt noin 5,66, 1,61 ja 2,72 ja näiden summa noin 9,99. Jos laskutarkkuus oli riittävä, on oikea vastaus tasan 10.

2.5 Tschirnhausin muunnos

Myöhemmin luvussa 4.2 esiintyvä 19-terminen diskriminantti olisi 59-terminen ilman Tschirnhausin muunnosta. Esittelemme muunnoksen siksi jo nyt, vaikka välttämättä sitä tarvitsemme vasta työn lopussa.

Määritelmä 2.9. (Vrt. [7, s. 141])

Olkoon polynomi $P \in \mathbb{Q}[x]$ astetta $n > 2$ ja $r_1, r_2, \ldots, r_n$ sen juuret. Olkoon polynomi $t \in \mathbb{Q}[x]$ astetta 1 tai 2. Tällöin polynomin

$$\prod_{i=1}^{n}(x - t(r_i))$$

muodostaminen on *Tschirnhausin muunnos*, jossa P on *muunnettava polynomi* ja t on *muuntava polynomi*.

Tutuin esimerkki tästä on polynomin muuntaminen lineaarisella polynomilla siten, että toiseksi korkeinta astetta oleva kerroin katoaa; juuri tämä muunnos yksinkertaistaa mm. myöhemmin esitettävää diskriminantin kaavaa.

Esimerkki 2.10. Olkoon muunnettava polynomi

$$x^5 + ax^4 + bx^3 + cx^2 + dx + e$$

ja muuntava polynomi

$$t(x) = x + \frac{a}{5}.$$

Tämä muunnos saadaan yksinkertaisesti sijoittamalla polynomiin $x - \frac{a}{5}$, ja tuloksena on

$$x^5 + px^3 + qx^2 + rx + s$$

jossa

$$\begin{array}{rcccccc}
p & = & & & & -\frac{2}{5}a^2 & +b \\
q & = & & & +\frac{4}{25}a^3 & -\frac{3}{5}ab & +c \\
r & = & & -\frac{3}{125}a^4 & +\frac{3}{25}a^2b & -\frac{2}{5}ac & +d \\
s & = & +\frac{4}{3125}a^5 & -\frac{1}{125}a^3b & +\frac{1}{25}a^2c & -\frac{1}{5}ad & +e.
\end{array}$$

Sopiva muunnos säilyttää polynomin kokonaislukukertoimisena pääpolynomina:

Lause 2.11. Olkoot $P, t \in \mathbb{Z}[x]$ pääpolynomeja.

Polynomin P Tschirnhausin muunnos polynomilla t tuottaa kokonaislukukertoimisen pääpolynomin, jonka aste on sama kuin muunnettavalla polynomilla.

Todistus:

Muunnetun polynomin asteluku on selvästi sama kuin muunnettavalla polynomilla.

Muunnetun polynomin kertoimet ovat muunnettavan polynomin juurien symmetrisiä polynomeja, siis lauseen 2.10 perusteella kokonaislukuja.

Esimerkin tällaisesta Tschirnhausin muunnoksesta näemme vasta lopun esimerkeissä.

Varsinainen ydinasia Tschirnhausin muunnoksessa on se, että muunnos säilyttää Galois'n ryhmän. Tulemme päätymään työn lopussa tilanteeseen, jossa Galois'n ryhmä ei suoraan selviä käyttämällämme menetelmällä. Tällöin polynomia on muunnettava.

On tietysti mahdollista, että muunnos ei säilytä Galois'n ryhmää: polynomin $x^4 - 2$ muuntaminen polynomilla $t(r) = r^2$ selvästi tuottaa jaottomasta polynomista jaollisen. Tämä on huomioitu seuraavassa:

Lause 2.12. Olkoon muunnettava polynomi $P \in \mathbb{Q}[x]$ jaoton. Olkoon muuntava polynomi $t(r) = r^2 + pr + q \in \mathbb{Q}[x]$.

Jos Tschirnhausin muunnos tuottaa jaottoman polynomin, on sen Galois'n ryhmä sama kuin polynomilla P.

Todistus:

Oletuksen mukaan muunnettu polynomi on jaoton, joten lauseen 2.3 nojalla sen kaikki juuret ovat erisuuria.

Olkoot r ja r' polynomin P juuria. Olkoon $f \in \mathrm{Gal}(P)$ sellainen, että $f(r) = r'$. Tutkitaan mihin $t(r)$ kuvautuu automorfismissa f.

$f(t(r)) =$	(Puretaan polynomi)
$f(r^2 + pr + q) =$	(Summan automorfismi)
$f(r^2) + f(pr) + f(q) =$	(Tulon automorfismi)
$f(r)f(r) + pf(r) + f(q) =$	($f(r) = r'$)
$r'r' + pr' + q =$	(Kootaan polynomi)
$t(r')$.	

Siis Galois'n ryhmät juurten permutaatioiksi tulkittuna ovat samat alkuperäisellä ja muunnetulla polynomilla. Erityisesti tällöin niiden kertaluku on sama.

Osoitetaan sitten alkuperäisen ja muunnetun polynomin juurikunnat samaksi.

Olkoot $r_1, r_2, \ldots, r_n$ polynomin P juuret ja P' muunnettu polynomi. Olkoot näiden juurikunnat $L = \mathbb{Q}(r_1, r_2, \ldots, r_n)$ ja $L' = \mathbb{Q}(t(r_1), t(r_2), \ldots, t(r_n))$. Selvästi $L \supseteq L'$.

Galois'n teorian perusteella $[L/\mathbb{Q}] = |\operatorname{Gal}(P)|$ ja $[L'/\mathbb{Q}] = |\operatorname{Gal}(P')|$. Edellä osoitettiin $|\operatorname{Gal}(P)| = |\operatorname{Gal}(P')|$, joten $[L/\mathbb{Q}] = [L'/\mathbb{Q}]$. Tornilauseen perusteella $[L/\mathbb{Q}] = [L/L'][L'/\mathbb{Q}]$, jolloin $[L/L'] = 1$ eli $L = L'$.

Yleinen rationaalikertoiminen polynomi voidaan helposti muuntaa kokonaislukukertoimiseksi *pää*polynomiksi, jolla on sama Galois'n ryhmä. Polynomi kerrotaan ensin sopivalla vakiolla, jotta tulos on kokonaislukukertoiminen. Olkoon tuloksessa johtavan termin kerroin a. Polynomiin sijoitetaan $\frac{x}{a}$ ja tulos kerrotaan luvulla a^{n-1}, jossa n on polynomin asteluku.

Galois'n ryhmän säilyminen tässä muunnoksessa todistettaisiin samoin kuin edellisessä todistuksessa. Sivuutamme tämän.

Jatkossa voimme siis olettaa käsiteltävien 5. asteen polynomien olevan kokonaislukukertoimisia pääpolynomeja ilman 4. asteen termiä.

3 Resolventti

Työmme pääsisältö on resolventtilause, johon etenemme hitaasti johdatellen. Aloitamme diskriminantista, joka kertoo meille onko Galois'n ryhmä ryhmän A_n aliryhmä. Sitten uudelleentulkitsemme diskriminantin resolventin erikoistapauksena.

3.1 Polynomin diskriminantti

Diskriminantti on polynomin juurien pareittaisten erotusten neliöiden tulo:

Määritelmä 3.1. ([4, s. 46])

Olkoon $P \in \mathbb{Q}[x]$ polynomi, jolla on juuret $r_1, r_2, \ldots, r_n$. Olkoon

$$\delta(r_1, r_2, \ldots, r_n) = \prod_{i=1}^{n-1} \prod_{j=i+1}^{n} (r_i - r_j).$$

Tällöin luku $\delta(r_1, r_2, \ldots, r_n)^2$ on polynomin *diskriminantti*. Se merkitään ΔP.

Diskriminantin erikoistapaus on tuttu:

Esimerkki 3.1. Toisen asteen polynomissa diskriminantti supistuu muotoon $(r_1 - r_2)^2$. Lukiossa opitun kaavan perusteella $\Delta(x^2 + ax + b) = a^2 - 4b$. Sijoittamalla $a = -e_1(r_1, r_2) = -(r_1 + r_2)$ ja $b = e_2(r_1, r_2) = r_1 r_2$ saadaan $\Delta = (-(r_1 + r_2))^2 - 4r_1 r_2 = r_1^2 + 2r_1 r_2 + r_2^2 - r_1 r_2 = r_1^2 - 2r_1 r_2 + r_2^2 = (r_1 - r_2)^2$ eli oikea tulos.

Diskriminantti on juurien symmetrinen polynomi, joten lauseen 2.9 perusteella se voidaan aina esittää tutkittavan polynomin kertoimien avulla siten kuin edellä toisen asteen tapauksessa. Esitämme viidennen asteen resolventin luvussa 4.2.

Diskriminantti on rationaaliluku, erikoistapauksessa kokonaisluku:

Lause 3.1. Jos $P \in \mathbb{Z}[x]$ on pääpolynomi, niin $\Delta P \in \mathbb{Z}$.

Todistus: Diskriminantti on juurien symmetrinen polynomi. Lauseen 2.10 perusteella kokonaislukukertoimisen pääpolynomin juurien symmetrisen polynomin arvo kokonaisluku.

Teemme tästä numeerisen esimerkin.

Esimerkki 3.2. Tutkitaan polynomia $P(x) = x^3 + 2x + 1$.

Juuret ovat noin $r_1 \approx -0{,}453$, $r_2 \approx 0{,}227 - 1{,}47i$ ja $r_3 \approx 0{,}227 + 1{,}47i$. Diskriminantti on $(r_1 - r_2)^2(r_1 - r_3)^2(r_2 - r_3)^2 \approx -59{,}0078$.

Olettaen että laskutarkkuus oli riittävä on diskriminantti täsmälleen -59.

Diskriminantti kertoo koostuuko Galois'n ryhmä pelkästään parillisista permutaatioista:

Lause 3.2. [6, s. 7–8] Olkoon $P \in \mathbb{Q}[x]$ astetta n oleva jaoton polynomi.

Tällöin $\mathrm{Gal}(P) \subseteq A_n$ jos ja vain jos ΔP on rationaaliluvun neliö.

Todistus:

Olkoot polynomin juuret $r_1, r_2, \ldots, r_n$. Tällöin väite on yhtäpitävä sen kanssa, että $\delta(r_1, r_2, \ldots, r_n)$ on rationaaliluku jos ja vain jos $\mathrm{Gal}(P) \subseteq A_n$.

Osoitetaan, että mielivaltainen kahden juuren keskinäinen vaihto muuttaa juuriparien erotusten tulon δ arvon vastaluvukseen.

Permutaatio voidaan esittää yhdistelmänä transpositioita. Jokainen transpositio voidaan esittää yhdistelmänä kahden peräkkäisen alkion vaihtoja: transpositio $(i\ j)$ saadaan yhdistämällä $(i\ i{+}1), (i{+}1\ i{+}2), \ldots, (j{-}1\ j)$ ja $(j{-}1\ j{-}2), (j{-}2\ j{-}3), \ldots, (i{+}1\ i)$. Siksi riittää tarkastella peräkkäisten juurien r_a ja r_{a+1} vaihtoja.

Jokainen tällainen vaihto selvästi vaihtaa tulossa δ tekijän $r_a - r_{a+1}$ vastaluvukseen, eikä vaikuta tulon δ muihin tekijöihin. Näin koko tulo δ vaihtuu vastaluvukseen. Parillinen määrä vaihtoja ei siis muuta tuloa δ.

Se, että $\mathrm{Gal}(P) \subseteq A_n$ tarkoittaa, että Galois'n ryhmässä on vain permutaatioita, jotka koostuvat parillisesta määrästä vaihtoja. Osoitetaan tämä ekvivalentiksi sen kanssa, että δ on rationaaliluku.

1) $\mathrm{Gal}(P) \not\subseteq A_n \Rightarrow \delta \notin \mathbb{Q}$: Jos jokin $f \in \mathrm{Gal}(P)$ on juurien permutaatioksi tulkittuna pariton permutaatio, niin edellä esitetyn perusteella $f(\delta) \neq \delta$. Tällöin $\delta \notin \mathbb{Q}$, koska määritelmän mukaan $\mathbb{Q}$-automorfismi kuvaa rationaaliluvut itselleen.

2) $\mathrm{Gal}(P) \subseteq A_n \Rightarrow \delta \in \mathbb{Q}$: Lauseen 2.8 perusteella vain rationaaliluvut kuvautuvat itselleen kaikilla Galois'n ryhmän automorfismeilla.

Nolla on itsensä vastaluku, joten se on käsiteltävä erikseen. Koska P on jaoton, ei sillä lauseen 2.3 nojalla voi olla kahta yhtäsuurta juurta, joten tulo δ ei voi olla nolla.

3.2 Diskriminantti on resolventin erikoistapaus

Resolventin ideaa kuvaamme parhaiten sanalla *osasymmetria*. Luvussa 2.4 tarkastelimme (täysin) symmetrisiä polynomeja. Laajennamme määritelmää:

Määritelmä 3.2. Olkoon polynomi $f \in \mathbb{Q}[y_1, y_2, \ldots, y_n]$ ja ryhmä $G \subseteq S_n$. Jos

$$\forall \sigma \in G\colon\ f(y_1, y_2, \ldots, y_n) = f(y_{\sigma(1)}, y_{\sigma(2)}, \ldots, y_{\sigma(n)})$$

niin polynomi f on *G-invariantti*.

Jos ei ole olemassa ryhmää $H \supset G$ siten, että f olisi H-invariantti, niin polynomi f on *tiukasti G-invariantti*.

Tällä käsitteellä voimme kuvailla diskriminanttia:

Esimerkki 3.3. Diskriminantti on juurien (täysin) symmetrinen polynomi eli S_n-invariantti.

Diskriminantin neliöjuuri δ on juurien A_n-invariantti mutta ei S_n-invariantti polynomi. Jotta voisi olla ryhmä G siten, että $A_n \subset G \subset S_n$, pitäisi ryhmän G kertaluvun olla ryhmän A_n kertaluvun monikerta ja jakaa tasan ryhmän S_n kertaluku. Tämä on mahdotonta, koska $|S_n|/|A_n| = 2$. Siispä δ on tiukasti A_n-invariantti.

Resolventti on yhden muuttujan polynomi, jonka rationaalijuurien olemassaoloa tutkitaan. Diskriminantti on tietysti helppo kääntää polynomiksi:

$$\begin{gathered}\text{"Onko diskriminantti } \Delta \text{ rationaaliluvun neliö?"} \\ \Leftrightarrow \\ \text{"Onko polynomilla } x^2 - \Delta \text{ rationaalijuuria?"}\end{gathered}$$

Etenemme nyt diskriminanttiin toista reittiä. Otamme malliksi kolmannen asteen polynomin, jolla tietenkin on kolme juurta.

Näiden juurien permutaatiot vastaavat ryhmää S_3, jonka asteluku on 6. Ryhmän A_3 asteluku on 3, joten erilaisia sivuluokkia S_3/A_3 saadaan $6/3 = 2$ — siis parilliset ja parittomat permutaatiot.

Auki kirjoitettuna kolmannen asteen diskriminantin neliöjuuri on

$$\delta(r_1, r_2, r_3) = (r_1 - r_2)(r_1 - r_3)(r_2 - r_3).$$

Kun tämä tiukasti A_3-invariantti polynomi evaluoidaan kaikilla kuudella permutaatiolla, saadaan kaksi erilaista arvoa:

$$\begin{gathered}\delta(r_1, r_2, r_3) = \delta(r_2, r_3, r_1) = \delta(r_3, r_1, r_2) \\ \neq \\ \delta(r_1, r_3, r_2) = \delta(r_2, r_1, r_3) = \delta(r_3, r_2, r_1).\end{gathered}$$

Kukin sivuluokka siis vastaa yhtä mahdollista polynomin arvoa.

Muodostetaan sitten polynomi, jonka juuriksi tulee yksi kummastakin sivuluokasta. Muistamme, että kahden juuren keskinäinen vaihto muuttaa polynomin δ etumerkin.

$$
\begin{gathered}
(x - \delta(r_1, r_2, r_3))(x - \delta(\boldsymbol{r_2}, \boldsymbol{r_1}, r_3)) = \\
(x - \delta(r_1, r_2, r_3))(x + \delta(r_1, r_2, r_3)) = \\
(x^2 - (\delta(r_1, r_2, r_3))^2) = \\
x^2 - \Delta.
\end{gathered}
$$

Edellä olleen voi ajatella eräänlaisena osittamisena ja kokoamisena. Jaoimme ryhmän S_n kahteen sivuluokkaan, ja sopivalla kertolaskulla kokosimme sivuluokat. Tuloksena saimme polynomin, jonka kertoimet ovat alkuperäisen polynomin juurten (täysin) symmetrisiä polynomeja.

Tämä on resolventin olennainen idea. Ryhmä G jaetaan ryhmän H mukaisesti sivuluokkiin käyttämällä jotain tiukasti H-invarianttia polynomia. Osat kerrotaan yhteen.

Diskriminantin neliöjuuri oli esimerkissämme A_3-invariantti polynomi. Väärinkäsitysten välttämiseksi teemme vielä yhden esimerkin:

Esimerkki 3.4. Polynomi $y_1y_2^2 + y_2y_3^2 + y_3y_1^2$ on tiukasti A_3-invariantti.

Ryhmää G kohti voi siis olla erilaisia G-invariantteja polynomeja. Tästä seuraa, että myös resolventteja voi olla erilaisia.

3.3 Resolventtilause

Tämä luku on työmme ydin. Aloitamme täsmällisestä määritelmästä.

Määritelmä 3.3. ([6, s. 7–8], [4, s. 387])

Olkoon polynomi $P \in \mathbb{Q}[x]$ astetta n ja $r_1, r_2, \ldots, r_n$ sen juuret. Olkoon ryhmät $H \subset G \subseteq S_n$. Olkoon polynomi $f \in \mathbb{Q}[y_1, y_2, \ldots, y_n]$ tiukasti H-invariantti.

Polynomin f ryhmää H vastaava *resolventti* ryhmässä G on

$$
\mathrm{Res}_G(P, f)(x) = \prod_{\sigma \in G//H} (x - f(r_{\sigma(1)}, r_{\sigma(2)}, \ldots, r_{\sigma(n)}))
$$

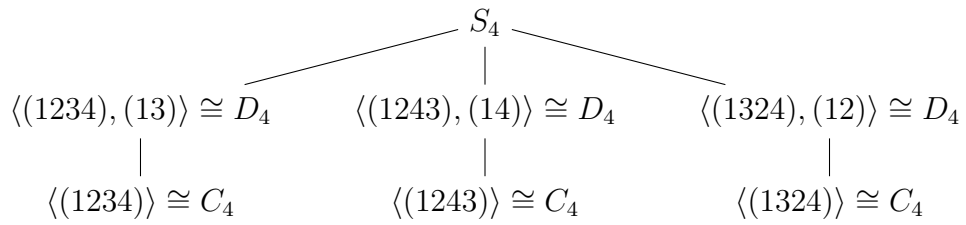
jossa $\sigma \in G//H$ tarkoittaa, että σ käy läpi jokaisen sivuluokan yhden edustajan.

Jos $G = S_n$, resolventti on *absoluuttinen*. Jos $G \subset S_n$, resolventti on *suhteellinen*.

Käytämme tässä ja seuraavassa luvussa esimerkkinä neljännen asteen polynomeja ja ryhmiä $S_4 \supset D_4 \supset C_4$. Tutkimme ensin ryhmiä itsessään.

Ryhmä C_4 kuvaa tässä tapauksessa neljän juuren kierroksen määräämää ryhmää. Tällaisia kierroksia on selvästi kuusi: juuri 1 voi siirtyä minkä tahansa kolmen juuren paikalle, ja tämä toiseen jäljellä olevasta kahdesta juuresta. Kuudesta kierroksesta saadaan kolme ryhmää, koska
$\langle(1234)\rangle = \langle(1432)\rangle$
$\langle(1243)\rangle = \langle(1342)\rangle$
$\langle(1324)\rangle = \langle(1432)\rangle$

Yleisesti diedriryhmässä D_n on $2n$ alkiota, ja sillä on aliryhmä C_n. Laajennamme ylläolevat C_4-ryhmät D_4-ryhmiksi. Tällöin ketju $S_4 \supset D_4 \supset C_4$ konkreettisina ryhminä on puu:



Esimerkki 3.5. Laaditaan tiukasti D_4-invariantti polynomi f:

$$f(y_1, y_2, y_3, y_4) = y_1y_2 + y_3y_4.$$

Diedriryhmään kuuluva kierto $y_1 \to y_3 \to y_2 \to y_4 \to y_1$ antaa polynomin f arvoksi $y_3y_4 + y_2y_1$, vaihto $y_1 \leftrightarrow y_2$ taas $y_2y_1 + y_3y_4$. Nämä kierto ja vaihto generoivat ryhmän D_4, joten f on D_4-invariantti.

Jotta voisi olla ryhmä G siten, että $D_4 \subset G \subset S_4$, pitäisi ryhmän G kertaluvun olla ryhmän D_4 kertaluvun monikerta ja jakaa tasan ryhmän S_4 kertaluku. Tämä on mahdotonta, koska $|S_4|/|D_4| = 3$. Jos siis f on invariantti jonkin laajemman ryhmän suhteen, se on S_4-invariantti eli täysin symmetrinen. Näin ei ole, koska $f(y_1, y_2, y_3, y_4) \neq f(y_1, \boldsymbol{y_3}, \boldsymbol{y_2}, y_4)$.

Koska $|S_4|/|D_4| = 24/8 = 3$, jakaa D_4 ryhmän S_4 kolmeen sivuluokkaan ja kussakin sivuluokassa on kahdeksan alkiota. Yksi näistä kolmesta sivuluokasta tarkoittaa polynomiin f sijoitettuna seuraavia:

$$\begin{array}{cccc} r_1r_2 + r_3r_4 & r_1r_2 + r_4r_3 & r_2r_1 + r_3r_4 & r_2r_1 + r_4r_3 \\ r_3r_4 + r_1r_2 & r_3r_4 + r_2r_1 & r_4r_3 + r_1r_2 & r_4r_3 + r_2r_1. \end{array}$$

Kullekin sivuluokalle saadaan edustaja valitsemalla juurelle r_1 pari tuloon, jolloin summan toiselle puolelle jää kahden jäljelle jääneen juuren tulo. Edustajat ovat esimerkiksi

$$r_1r_2 + r_3r_4, \;\; r_1r_3 + r_2r_4, \;\; r_1r_4 + r_2r_3.$$

Näin siis

$$\mathrm{Res}_{S_4}(f,P)(x) = \prod_{\sigma\in S_4//D_4}(x - f(r_{\sigma(1)}, r_{\sigma(2)}, \ldots, r_{\sigma(n)})) =$$
$$[x-(r_1r_2+r_3r_4)]\cdot[x-(r_1r_3+r_2r_4)]\cdot[x-(r_1r_4+r_2r_3)].$$

Konkretisoimme tätä pidemmälle. Tutkimme polynomia

$$x^4 - 2$$

jonka juuret numeroimme

$$r_1 = \sqrt[4]{2},\ r_2 = i\sqrt[4]{2},\ r_3 = -\sqrt[4]{2},\ r_4 = -i\sqrt[4]{2}.$$

Resolventti on

$$[x-(i\sqrt{2}+i\sqrt{2})]\cdot[x-(-\sqrt{2}+\sqrt{2})]\cdot[x-(-i\sqrt{2}+(-i\sqrt{2}))]$$
$$=$$
$$(x-2i\sqrt{2})\cdot(x-0)\cdot(x-(-2i\sqrt{2})).$$

Tällä on yksinkertainen rationaalijuuri nolla; siis

$$\begin{array}{lcl}(r_1r_2+r_3r_4) & \neq & 0,\\ (r_1r_3+r_2r_4) & = & 0\in\mathbb{Q},\\ (r_1r_4+r_2r_3) & \neq & 0.\end{array}$$

Myöhemmin osoitamme tästä seuraavan, että $\mathrm{Gal}(x^4-2)\subseteq D_4$.

Tämä oli absoluuttinen resolventti. Suhteellisesta resolventista teemme esimerkin seuraavassa luvussa.

Toistamme vielä, ettei resolventtipolynomi ole yksikäsitteinen. Esimerkiksi $f(r_1,r_2,r_3,r_4) = (r_1+r_2)(r_3+r_4)$ on toinen tiukasti D_4-invariantti polynomi.

Edellä päädyimme neljännen asteen polynomista kolmannen asteen resolventtiin, ja korkeintaan neljännen asteen polynomeille tunnetaan yleinen ratkaisukaava juurtamalla. Palaamme seuraavassa luvussa kysymykseen korkeamman asteen polynomien ja/tai resolventtien käsittelystä. Sitä ennen todistamme työn keskeisimmän lauseen.

Lähtötietomme tämän lauseen käyttöön on tutkittavan polynomin Galois'n ryhmän kuuluminen ryhmään G. Haluamme tietää kuuluuko Galois'n ryhmä myös ryhmään $H\subset G$. Resolventtilause antaa meille jonkin kolmesta vastauksesta: kyllä, ei, ehkä.

Lause 3.3. ([6, s. 7–8], [4, s. 387])

Olkoon polynomi $P \in \mathbb{Q}[x]$ astetta n ja $\mathrm{Gal}(P) \subseteq G \subseteq S_n$.

Olkoot ryhmät $H = H_1, H_2, \ldots, H_m \subset G$ konjugaatteja ja resolventtipolynomi $f \in \mathbb{Q}[y_1, y_2, \ldots, y_n]$ tiukasti H-invariantti.

Tällöin, jos resolventilla $\mathrm{Res}_G(f, P)$

1. on yksinkertainen rationaalijuuri, niin $\mathrm{Gal}(P) \subseteq H_i$ jollain i ja
2. ei ole rationaalijuuria lainkaan, niin $\mathrm{Gal}(P) \not\subseteq H_i$ millään i.

Todistus, kohta 1

Olkoon r resolventin $\mathrm{Res}_G(f, P)$ yksinkertainen rationaalijuuri. Voidaan olettaa ryhmät $H = H_1, H_2, \ldots, H_m$ ja polynomin P juuret $r_1, r_2, \ldots, r_n$ numeroiduksi niin, että rationaalijuuri r vastaa resolventin tekijöistä ryhmän H identiteettipermutaation määräämää sivuluokkaa.

Resolventin juuret ovat tällöin

$f(r_1, r_2, \ldots, r_n) = r \in \mathbb{Q}$
$f(r_{\sigma_2(1)}, r_{\sigma_2(2)}, \ldots, r_{\sigma_2(n)}) \neq r$
$f(r_{\sigma_3(1)}, r_{\sigma_3(2)}, \ldots, r_{\sigma_3(n)}) \neq r$
$\ldots$
$f(r_{\sigma_l(1)}, r_{\sigma_l(2)}, \ldots, r_{\sigma_l(n)}) \neq r$

jossa $l = |G|/|H|$ ja $\sigma_2, \sigma_3, \ldots, \sigma_l$ ovat ryhmän H muiden sivuluokkien edustajat.

Teemme vastaoletuksen $\mathrm{Gal}(P) \not\subseteq H$. Tiedämme, että $\mathrm{Gal}(P) \subseteq G$. Näistä seuraa, että on olemassa jokin Galois'n ryhmän automorfismi $\tau \in G \backslash H$. Viimeksimainittu tarkoittaa, että $\tau f \neq f$. Tällöin resolventissa on ainakin tekijä $(x - f(r_1, r_2, \ldots, r_n))$ ja tästä eroava tekijä $(x - \tau f(r_1, r_2, \ldots, r_n))$.

Viimeksimainittu tekijä voidaan kirjoittaa $(x - f(r_{\tau(1)}, r_{\tau(2)}, \ldots, r_{\tau(n)}))$. Koska toisaalta juuri $f(r_1, r_2, \ldots, r_n)$ on rationaalinen ja toisaalta Galois'n ryhmän alkio kuten τ on määritelmän mukaan $\mathbb{Q}$-invariantti, täytyy resolventilla olla kaksinkertainen juuri: $f(r_1, r_2, \ldots, r_n) = f(r_{\tau(1)}, r_{\tau(2)}, \ldots, r_{\tau(n)})$. Tämä on mahdotonta, koska oletimme resolventilla olevan *yksinkertaisen* juuren. Vastaoletus on väärä, joten kohta 1 on todistettu.

Todistus, kohta 2

Käännetään implikaatio. Oletetaan $\mathrm{Gal}(P) \subseteq H_i$ ja osoitetaan siitä seuraavan, että resolventilla on ainakin yksi rationaalijuuri.

Voidaan olettaa ryhmät $H_1, H_2, \ldots, H_m$ numeroiduksi niin, että $\mathrm{Gal}(P) \subseteq H$. Yksi resolventin juurista vastaa identiteettialkion määräämää aliryhmän H sivuluokkaa eli ryhmää H itsessään. Koska f on H-invariantti ja $\mathrm{Gal}(P) \subseteq H$, niin f on $\mathrm{Gal}(P)$-invariantti. Lauseen 2.8 perusteella tämä resolventin juuri on rationaalinen.

Edellinen lause jättää avoimen kysymyksen: entä jos resolventilla on rationaalijuuria, mutta ei yksinkertaisia? Lopun esimerkeissä esitämme kaksi polynomia, joiden resolventeilla on kaksinkertainen juuri toisen Galois'n ryhmän ollessa C_5 ja toisen D_5. Resolventtilause ei siis kerro mitään Galois'n ryhmästä, jos kaikki rationaalijuuret ovat moninkertaisia.

Todistus on hieman tikkuinen, joten jatkamme esimerkillä.

Esimerkki 3.6. Olkoon polynomi $P \in \mathbb{Q}[x]$ astetta 4 ja r_1, r_2, r_3 ja r_4 sen juuret. Oletetaan ensin $\mathrm{Gal}(P) = C_4 \subset D_4$.

Kuten edellä kuvattiin, tarkoittaa $\mathrm{Gal}(P)$ tällöin jotain kolmesta mahdollisesta permutaatioryhmästä: $\langle (r_1, r_2, r_3, r_4) \rangle$, $\langle (r_1, r_3, r_2, r_4) \rangle$ tai $\langle (r_1, r_2, r_4, r_3) \rangle$.

Käytetään jälleen resolventtipolynomia $f(y_1, y_2, y_3, y_4) = y_1y_2 + y_3y_4$. Kierrätetään juuria $r_1 \to r_2 \to r_3 \to r_4 \to r_1$ ja tutkitaan miten resolventin tekijät käyttäytyvät:

$$\begin{gathered}
[x - (r_1r_2 + r_3r_4)] \cdot [x - (\mathbf{r_1r_3} + \mathbf{r_2r_4})] \cdot [x - (r_1r_4 + r_2r_3)] \\
\Downarrow \\
[x - (r_2r_3 + r_4r_1)] \cdot [x - (r_2r_4 + r_3r_1)] \cdot [x - (r_2r_1 + r_3r_4)] \\
= \\
[x - (r_1r_4 + r_2r_3)] \cdot [x - (\mathbf{r_1r_3} + \mathbf{r_2r_4})] \cdot [x - (r_1r_2 + r_3r_4)]
\end{gathered}$$

Siis resolventin juuri $r_1r_3 + r_2r_4$ kuvautuu itselleen, juuret $r_1r_2 + r_3r_4$ ja $r_1r_4 + r_2r_3$ kuvautuvat toisilleen. Siis $r_1r_3 + r_2r_4 \in \mathbb{Q}$ ja $r_1r_2 + r_3r_4, r_1r_4 + r_2r_3 \notin \mathbb{Q}$.

Oletetaan sitten, että Galois'n ryhmä sisältää kierroksen $r_1 \to r_2 \to r_3 \to r_1$. Tällöin

$$\begin{gathered}
[x - (r_1r_2 + r_3r_4)] \cdot [x - (r_1r_3 + r_2r_4)] \cdot [x - (r_1r_4 + r_2r_3)] \\
\Downarrow \\
[x - (r_2r_3 + r_1r_4)] \cdot [x - (r_2r_1 + r_3r_4)] \cdot [x - (r_2r_4 + r_3r_1)] \\
= \\
[x - (r_1r_4 + r_2r_3)] \cdot [x - (r_1r_2 + r_3r_4)] \cdot [x - (r_1r_3 + r_2r_4)]
\end{gathered}$$

Eli yksikään resolventin juurista ei kuvaudu itselleen. Vastaavin mekaanisin laskuin nähdään, että sama pätee aina, kun Galois'n ryhmä sisältää ryhmään D_4 kuulumattoman permutaation.

3.4 Resolventin muodostaminen

Jäljellä on kysymys siitä, miten resolventit käytännössä muodostetaan. Tutkimme ensin millainen resolventista tulee.

Absoluuttisen resolventin kertoimet ovat tutkittavan polynomin juurten symmetrisiä polynomeja ja näin lauseen 2.10 nojalla kokonaislukuja. Sama pätee myös suhteelliseen resolventtiin:

Lause 3.4. ([11, s. 984])

Olkoot $H \subset G \subseteq S_n$ ryhmiä ja f tiukasti H-invariantti polynomi. Olkoon $P \in \mathbb{Z}[x]$ pääpolynomi jolla $\mathrm{Gal}(P) \subseteq G$.

Tällöin resolventin $\mathrm{Res}_G(f, P)$ kertoimet ovat kokonaislukuja.

Todistus:

Resolventti auki purettuna on

$$\begin{gathered}(x - f(r_{\sigma_1(1)}, r_{\sigma_1(2)}, \ldots, r_{\sigma_1(n)}))\cdot \\ (x - f(r_{\sigma_2(1)}, r_{\sigma_2(2)}, \ldots, r_{\sigma_2(n)}))\cdot \\ \ldots \\ (x - f(r_{\sigma_l(1)}, r_{\sigma_l(2)}, \ldots, r_{\sigma_l(n)}))\end{gathered}$$

jossa $l = |G|/|H|$ ja $\sigma_1, \sigma_2, \ldots, \sigma_l \in G$ ovat sivuluokkien $G//H$ edustajat.

Valitaan mielivaltainen $\tau \in \mathrm{Gal}(P)$. Oletuksen mukaan $\mathrm{Gal}(P) \subseteq G$ joten $\tau \in G$. Tällöin $\tau G = G$, joten myös ryhmän H mukaiset sivuluokat ovat samat: $G/H = (\tau G)/H$. Kertomalla vasemmalta permutaatiolla τ^{-1} nähdään, että $\tau\sigma$ ja $\tau\sigma'$ kuuluvat samaan sivuluokkaan vain, jos σ ja σ' kuuluvat samaan sivuluokkaan.

Siis juurten permutointi mielivaltaisella Galois'n ryhmän automorfismilla ei muuta resolventin tekijöitä, ainoastaan permutoi niitä keskenään. Koska resolventti ei muutu millään Galois'n ryhmän alkiolla, sen kertoimet ovat lauseen 2.8 nojalla rationaalilukuja.

Luku, joka on kokonaislukukertoimisen pääpolynomin juuri, on algebrallinen kokonaisluku. Nämä luvut muodostavat renkaan, eli ovat suljettu joukko yhteen- ja kertolaskun suhteen. Kokonaisluvut ovat ainoita rationaalilukuja, jotka ovat algebrallisia kokonaislukuja. [10, s. 3–6]

Koska resolventin kertoimet muodostuvat kokonaislukukertoimisten polynomien juurista ja ovat rationaalilukuja, ne edellisen perusteella ovat kokonaislukuja.

Käytämme tässä luvussa esimerkkinä neljännen asteen polynomia

$$P(x) = x^4 - x^3 - 3x^2 + x + 1$$

jonka juuret numeroimme

$$r_1 \approx -1{,}356, \;\; r_2 \approx -0{,}4773, \;\; r_3 \approx 0{,}7376, \;\; r_4 \approx 2{,}095.$$

Selvitämme ensin onko $\mathrm{Gal}(P) \subseteq D_4$. Resolventtipolynomi on edellisestä luvusta tuttu $f(y_1, y_2, y_3, y_4) = y_1y_2 + y_3y_4$, jolloin resolventti siis on $(x - (r_1r_2 + r_3r_4))(x - (r_1r_3 + r_2r_4))(x - (r_1r_4 + r_2r_3))$.

Galois'n ryhmän määritys alkaa aina absoluuttisella resolventilla, koska ainoa lähtötietomme on Galois'n ryhmän kuuluminen ryhmään S_n. On kolme tapaa selvittää absoluuttisen resolventin juuret.

Tapa 1: Resolventin juuret polynomin juurista

Ensimmäinen tapa on suoraviivainen: ei lähdetä muodostamaan resolventtia, vaan suoraan tutkittavan polynomin juurien likiarvoista lasketaan resolventin juurten likiarvot.

Esimerkki 3.7. Resolventin $\mathrm{Res}_{S_4}(f, P)$ juuret ovat

$$\begin{array}{lcl} r_1r_2 + r_3r_4 & \approx & +2{,}19249 \\ r_1r_3 + r_2r_4 & \approx & \mathbf{-2{,}00013} \\ r_1r_4 + r_2r_3 & \approx & -3{,}19287 \end{array}$$

Resolventilla näyttää olevan yksinkertainen rationaalijuuri -2. Jos oletamme näin olevan, tiedämme Galois'n ryhmän tarkasti. Tällä juurien numeroinnilla se on $\langle (r_1, r_2, r_3, r_4), (r_1, r_3) \rangle$ eikä esimerkiksi $\langle (r_1, r_2, r_4, r_3), (r_1, r_4) \rangle$.

Voi olla, että edellä resolventin juuri oli vain sattumalta lähellä kokonaislukua -2. Jatkamme varmaan menetelmään.

Tapa 2: Resolventin kertoimet polynomin juurista

Resolventin kertoimet ovat kokonaislukuja. Lasketaan siis resolventin kertoimien likiarvot tutkittavan polynomin juurten likiarvoista ja pyöristetään kokonaislukuihin.

Esimerkki 3.8. Merkitään

$$\begin{array}{lcl} T_1 = r_1r_2 + r_3r_4 & \approx & +2{,}19249 \\ T_2 = r_1r_3 + r_2r_4 & \approx & -2{,}00013 \\ T_3 = r_1r_4 + r_2r_3 & \approx & -3{,}19287 \end{array}$$

Tällöin resolventti on

$$x^3 - (T_1 + T_2 + T_3)x^2 + (T_1T_2 + T_1T_3 + T_2T_3)x - (T_1T_2T_3)$$

josta sijoittamalla saadaan noin

$$x^3 + 3{,}00051x^2 - 4{,}99945x - 14{,}00161.$$

Jos laskutarkkuus oli riittävä, tämä on todellisuudessa

$$x^3 + 3x^2 - 5x - 14.$$

Rationaalijuurilauseen perusteella polynomin mahdolliset rationaalijuuret ovat muotoa $\pm\frac{p}{q}$, jossa p jakaa tasan vakiotermin ja q jakaa tasan korkeimman asteen termin kertoimen. Tähän soveltaen mahdolliset resolventin juuret ovat ±1, ±2, ±7 ja ±14. Osoittautuu, että -2 todella on yksinkertainen rationaalijuuri. Siis $\mathrm{Gal}(P) \subseteq D_4$.

Jos olisimme aloittaneet tavalla kaksi, olisimme saaneet selville Galois'n ryhmän varmasti, mutta ei yksikäsitteisesti vaan konjugointia vaille yksikäsitteisesti. Yhdistämällä tavat yksi ja kaksi saimme varman ja täsmällisimmän mahdollisen tuloksen.

Tapa 3: Resolventin kertoimet polynomin kertoimista

Lauseen 2.9 perusteella voidaan lausua absoluuttisen resolventin kertoimet tutkittavan polynomin kertoimien avulla, tutkittavan polynomin juuria ei siis tarvitse laskea. Saman lauseen todistuksen algoritmi kertoo miten tämä tehdään. Tämä on vaihtoehto tavalle kaksi.

Esimerkki 3.9. Lasketaan polynomille $x^4 + ax^3 + bx^2 + cx + d$ resolventti resolventtipolynomilla f. Esimerkiksi termin x kertoimeksi saadaan

$$(r_1r_2+r_3r_4)(r_1r_3+r_2r_4)+(r_1r_2+r_3r_4)(r_1r_4+r_2r_3)+(r_1r_3+r_2r_4)(r_1r_4+r_2r_3).$$

Purkamalla tämä auki saadaan polynomi, jonka johtava termi on $r_1^2r_2r_3$. Lauseen 2.9 mukaisesti tehdään ensimmäisessä askeleessa korvaus

$$r_1^2r_2^1r_3^1r_4^0 \to e_1^{2-1}e_2^{1-1}e_3^{1-0}e_4^0$$

eli tutkittavan polynomin kertoimien avulla esitettynä ac. Jatkamalla tämä loppuun ja käymällä kaikki kertoimet läpi saadaan

$$\mathrm{Res}_{S_4}(f, x^4 + ax^3 + bx^2 + cx + d) = x^3 - bx^2 + (ac - 4d)x - (a^2d - 4bd + c^2).$$

Polynomille P tämä resolventti on $x^3+3x^2-5x-14$, eli edellisessä esimerkissä laskutarkkuus oli riittävä.

Tästä tietenkin jatketaan kuten edellä tutkimalla rationaalijuurilauseen perusteella mahdolliset juuret. Tuloksena saadaan konjugointia vaille yksikäsitteinen tulos.

Numeerisesta laskennasta

Laskimme tavassa kaksi resolventin vakiotermin olevan *noin* -14. On mahdollista laskea juuren likiarvon sijaan väli, jonka sisällä juuri *varmasti* on; juuren arvo olisi esimerkiksi $(1{,}23 + 4{,}56i) + h$, jossa $|h| < 10^{-8}$. Tällaisista juurien arvoista voidaan laskea resolventin kertoimelle vastaava väli. Jos tulos on esimerkiksi reaalilukuväli [2,1; 3,9], on haettu luku täsmälleen 3. Laskutarkkuutta kasvattamalla päädytään aina varmaan lopputulokseen.

Jos resolventin juuria lasketaan suoraan, sama toimii vain puoliksi. Jos kokonaislukukertoimisen pääpolynomin resolventilla on rationaalijuuri, se on kokonaisluku. Jos lasketaan jonkin resolventin juuren olevan esimerkiksi $1{,}3+h$ jossa $|h| < 0{,}1$, tämä juuri ei ole rationaalinen.

Jos resolventin juuri on esimerkiksi $3 + h$ jossa $|h| < 10^{-20}$, on epävarmaa onko juuri rationaalinen: sehän voi olla esimerkiksi $3 + 10^{-30}$. Riippuu sovelluksesta voimmeko tyytyä vastaukseen joka ei ole varma vaan vain erittäin todennäköinen.

Jos haluamme varman vastauksen ja lisäksi tietää tarkasti Galois'n ryhmän, voimme yhdistää tavan yksi tapaan kaksi tai kolme. Tämän voimme tehdä kahdessa eri järjestyksessä.

Voimme laskea ensin numeerisesti resolventin juuret. Jos jokin niistä näyttää olevan suurella tarkkuudella yksinkertainen rationaalijuuri, voimme varmistaa tämän tavalla kaksi tai kolme. Näin teimme edellä.

Toisaalta voimme ensin selvittää tarkan tuloksen antavilla tavoilla onko resolventilla rationaalijuurta. Jos on, voimme tavalla yksi etsiä mistä resolventin tekijästä tämä tulos saatiin ja siitä päätellä mikä Galois'n ryhmä tarkalleen on. Tarvittava laskutarkkuus voi tällöin olla pienempi: esimerkiksi edellä riittää tietää $r_1r_2 + r_3r_4 = 2 + h$, jossa $|h| < 3$, jotta tiedetään ettei tämä ole resolventin rationaalijuuri -2.

Tapaa, jossa likiarvojen sijaan lasketaan lukuväleillä, kutsutaan intervallilaskennaksi. Sen käytännön toteutusta emme tässä käsittele.

Suhteellinen resolventti ryhmien D_4 ja C_4 erottajana

Palaamme polynomiin P. Tiedämme $\mathrm{Gal}(P) \subseteq \langle (r_1, r_2, r_3, r_4), (r_1, r_3) \rangle \cong D_4$, eli tämä on esimerkki suhteellisesta resolventista. Selvitämme onko $\mathrm{Gal}(P) \subseteq C_4$, siis käytännössä onko $\mathrm{Gal}(P) = \langle (r_1, r_2, r_3, r_4) \rangle$.

Aluksi tarvitaan resolventtipolynomi. Olkoon se

$$f(y_1, y_2, y_3, y_4) = y_1 y_2^2 + y_2 y_3^2 + y_3 y_4^2 + y_4 y_1^2$$

Koska $|D_4|/|C_4| = 8/4 = 2$, jakautuu D_4 kahteen sivuluokkaan:
$\{(), (1234), (13)(24), (1432)\}$
$\{(13), (24), (12)(34), (14)(23)\}$.

Sijoittamalla polynomiin f sivuluokkien edustajista esimerkiksi identiteetti-permutaatio ja $(14)(23)$ saadaan resolventiksi

$$\begin{gathered}[x - f(r_1, r_2, r_3, r_4)] \cdot [x - f(r_4, r_3, r_2, r_1)] \\ = \\ [x - (r_1 r_2^2 + r_2 r_3^2 + r_3 r_4^2 + r_4 r_1^2)] \cdot [x - (r_4 r_3^2 + r_3 r_2^2 + r_2 r_1^2 + r_1 r_4^2)].\end{gathered}$$

Resolventtipolynomi on selvästi C_4-invariantti. Ryhmien kertalukujen perusteella on jälleen selvää, ettei ole väliryhmää G siten, että $C_4 \subset G \subset D_4$. Koska $f(r_1, r_2, r_3, r_4) \neq f(r_4, r_3, r_2, r_1)$, polynomi f on tiukasti C_4-invariantti.

Suhteellisen resolventin juuret polynomin juurista

Esimerkki 3.10. Resolventin juuret ovat

$$\begin{aligned} r_1 r_2^2 + r_2 r_3^2 + r_3 r_4^2 + r_4 r_1^2 &\approx +6{,}5209 \\ r_4 r_3^2 + r_3 r_2^2 + r_2 r_1^2 + r_1 r_4^2 &\approx -5{,}5213 \end{aligned}$$

Näyttää selvältä, että rationaalijuuria ei ole eli $\mathrm{Gal}(P) \not\subseteq C_4$.

Suhteellisen resolventin kertoimet polynomin juurista

Edellisen esimerkin likiarvoilla laskettuna resolventti on

$$\begin{gathered}(x - 6{,}5209)(x - (-5{,}5213)) \\ \approx \\ x^2 - 0{,}9996x - 36{,}004\end{gathered}$$

joka tietysti pyöristyy muotoon

$$x^2 - x - 36.$$

Mahdolliset rationaalijuuret ovat ± 1, ± 6 ja ± 36. Mikään niistä ei ole juuri, joten edellisen esimerkin päättelymme osui oikeaan: $\mathrm{Gal}(P) \not\subseteq C_5$.

Suhteellisen resolventin kertoimet polynomin kertoimista

Vielä voi pohtia kolmatta tapaa suhteellisen resolventin tapauksessa. Koska resolventin kertoimet eivät ole tutkittavan polynomin juurien symmetrisiä polynomeja, ei niitä voi esittää tutkittavan polynomin kertoimien avulla.

Sivuhuomiona toteamme, että hieman vastaavanlainen tapa olisi olemassa. Olkoon tutkittava polynomi $x^4 + ax^3 + bx^2 + cx + d$, sen juuret r_1, r_2, r_3 ja r_4 sekä edellä löydetty rationaalijuuri $R = r_1r_2 + r_3r_4 \in \mathbb{Q}$.

Tällöin resolventin termin x kerroin

$$(r_1r_2^2 + r_2r_3^2 + r_3r_4^2 + r_4r_1^2) + (r_4r_3^2 + r_3r_2^2 + r_2r_1^2 + r_1r_4^2)$$

voidaan esittää kertoimien ja luvun R avulla muodossa

$$-a(b - R) - 2c.$$

Sivuutamme resolventin vakion esittämisen vastaavalla tavalla.

Neljäs tapa

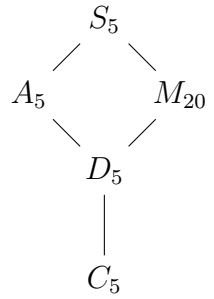
Teoriassa olisi kenties vielä yksi tapa: juuret voi laskea tarkasti. Ratkaisua ei löydy juurtamalla, mutta muilla funktioilla löytyy. Tätä tapaa ei ilmeisesti käytännössä käytetä missään.

4 Galois'n ryhmä 5. asteen polynomille

Tämä ja seuraava luku ovat laaja esimerkki resolventtimenetelmän käytöstä. Menetelmä jakautuu esi- ja työvaiheeseen. Esivaiheessa etsitään ryhmän S_n transitiiviset aliryhmät ja muodostetaan sopivat resolventit. Työvaiheessa transitiivisten aliryhmien verkkoa haarukoidaan resolventeilla kunnes vain yksi ryhmä jää mahdolliseksi. Tämä luku kertoo esivaiheesta.

4.1 Ryhmän S_5 transitiiviset aliryhmät

Ryhmällä S_5 on isomorfialuokittain laskettuna viisi transitiivista aliryhmää ja kuhunkin isomorfialuokkaan kuuluvat aliryhmät ovat keskenään konjugaatteja. Kuvaamme ensin niiden väliset suhteet. Lähteenä tälle luvulle on [4, s. 369].

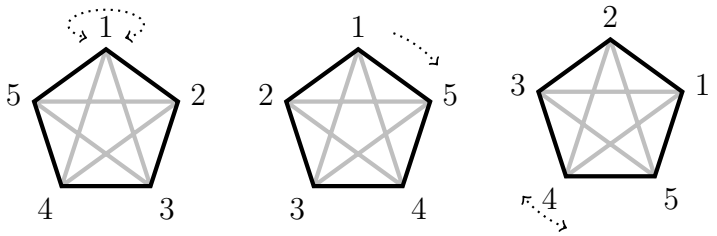


Kaaviona aliryhmät muodostavat helposti muistettavan kuvion, vieressä näkyvän "liikennemerkin". Ryhmän S_5 maksimaaliset aliryhmät ovat A_5 ja M_{20}, joiden molempien aliryhmä on D_5, jolla taas on aliryhmänään C_5.

Ryhmistä vaikeimmin kuvailtava on 20-alkioinen ryhmä M_{20}. Etenemme siihen vaiheittain ja hyödynnämme grafiikkaa.

Ryhmä C_5 kuvaa viisikulmion kiertoa ja sen generoi 5-sykli: $C_5 \cong \langle(\text{abcde})\rangle$. Ryhmässä S_5 on $4! = 24$ eri 5-sykliä: alkio 1 voi siirtyä johonkin neljästä vaihtoehdosta, tämä johonkin kolmesta jäljellä olevasta ja niin edelleen. Yhden 5-syklin generoima ryhmä sisältää kolme muuta 5-sykliä, joten erilaisia C_5-aliryhmiä on $4!/4 = 6$.

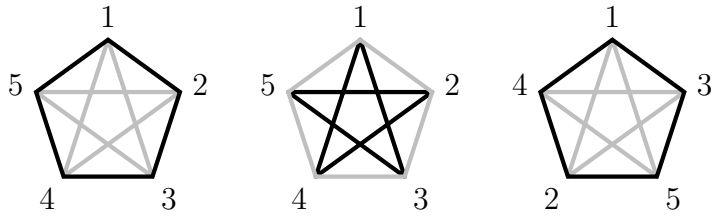
Diedriryhmässä D_5 mukaan tulee viisikulmion kääntö. Diedriryhmän voi ajatella sisältävän permutaatiot, joissa ensin joko tehdään kääntö pitäen kulma 1 paikallaan tai ei tehdä, ja sitten kierretään viisikulmiota 0-4 askelta. Toinen tapa on ajatella viittä mahdollista kiertoa ja viittä kääntöä. Alla kuvataan miten kääntö alkion 1 suhteen ja yhden askeleen kierto vastaa kääntöä alkion 4 suhteen.



"käännä 1:n suhteen"+"kierrä kerran"="käännä 4:n suhteen"

Jokainen D_5-aliryhmä voidaan ajatella C_5-aliryhmäksi, jota on laajennettu käännöllä. Näin myös erilaisia D_5-aliryhmiä on kuusi. Permutaationa ryhmä on muotoa $D_5 \cong \langle (\text{abcde}), (\text{be})(\text{cd}) \rangle$.

Ryhmä M_{20} suhtautuu ryhmään D_5 hieman kuten D_5 ryhmään C_5. Viisikulmion kierto ja kääntö säilyttävät kunkin kulman naapurit entisellään. Ryhmässä M_{20} mukaan tulee vielä täydellinen naapurien vaihto. Tämä voidaan kuvata joko vaihtamalla kulmien numerointia sopivasti tai vaihtamalla ulkokehä ja sisätähti keskenään.

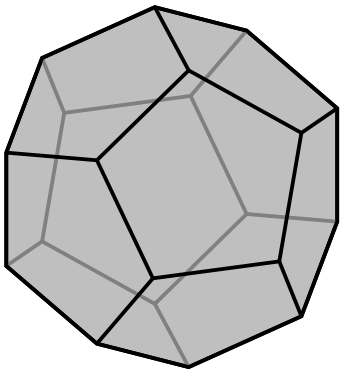


Ryhmä M_{20} sisältää viisikulmion kiertojen ja kääntöjen lisäksi vaihdon, jossa jokaisen kulman naapuripisteet vaihtuvat.

Permutaatioina ajatellen ryhmän M_{20} generoivat 5-sykli ja sopiva 4-sykli: $M_{20} \cong \langle (\text{abcde}), (\text{bced}) \rangle$. Ainoat 4-syklin (bced) generoiman ryhmän aidot aliryhmät ovat $\langle (\text{be})(\text{cd}) \rangle$ ja triviaaliryhmä; vastaavasti aliryhmäketju on $\langle (\text{abcde}), (\text{bced}) \rangle \cong M_{20} \supset \langle (\text{abcde}), (\text{be})(\text{cd}) \rangle \cong D_5 \supset \langle (\text{abcde}) \rangle \cong C_5$ ja erilaisia M_{20}-aliryhmiä on kuusi.

Tasokuvioin ei voi havainnollistaa kahta jäljellä olevaa ryhmää. Käytämme kolmiulotteista mielikuvaa perustelematta tarkemmin miksi se on oikea.

Ryhmä A_5 kuvaa kahdestatoista viisikulmiosta muodostuvan dodekaedrin kiertoja[2, s. 247]. Sen kuusi syklistä viiden alkion aliryhmää vastaavat pyörittämistä vastakkaisten sivujen pysyessä paikallaan.



Dodekaedri

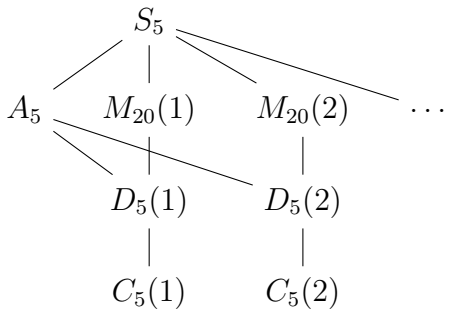
Visuaalisesti ajatteleva havaitsee, että kaikki dodekaedrin asennot saadaan toistamalla esimerkiksi mitä tahansa kahta jonkin sivun suuntaista kääntöä. Vastaavasti kaksi 5-sykliä generoivat ryhmän A_5.

Ryhmää S_5 helposti vastaavaa kolmiulotteistakaan kuviota ei ole. Lähimmäksi pääsemme ajattelemalla dodekaedria, josta voi vaihtaa sisäpuolen ulkopuoleksi. Tällöin ryhmä A_5 vastaisi niitä permutaatioita, joissa sisäpuoli jää sisäpuoleksi.

Ryhmän M_{20} mieltäminen ryhmän S_5 aliryhmäksi ei ole graafisesti helppoa. Voimme ehkä ajatella tasolla olevaa dodekaedria, jonka voi kiertää viiteen asentoon (vrt. C_5), kääntää ylä- ja alapuolet (vrt. ryhmän D_5 kääntö) tai vaihtaa sisäpuolen ulkopuoleksi (vrt. ryhmän M_{20} vaihto).

Mielikuvaa jatkaen ryhmät C_5 ja D_5 eivät vaihda sisä- ja ulkopuolta, eli kuuluvat ryhmään A_5. Sen sijaan ryhmän M_{20} permutaatioista puolet vaihtaa. Vastaavasti ryhmän A_5 aliryhmiä ovat C_5 ja D_5 mutta ei M_{20}.

Vielä on korostettava, että tilanne on monimutkaisempi kun ryhmiä ei yhdistetä konjugaateittain. Merkitsemme seuraavassa konkreettiset aliryhmät $M_{20}(1)$, $M_{20}(2)$ jne. Tällöin kuvioksi saadaan seuraava:



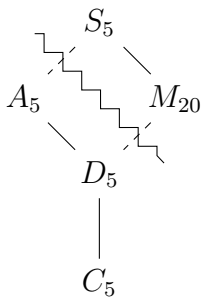
Miten transitiiviset aliryhmät etsitään? Kysymys on puhtaasti ryhmäteoriaan kuuluva, ja ohitamme sen tässä lyhyesti.

Voidaan todistaa, että ryhmän S_5 transitiivisessa aliryhmässä on ainakin yksi 5-sykli. Tähän voidaan lisätä erilaisia permutaatioita ja tutkia millainen ryhmä saadaan. Voidaan olettaa 5-sykli numeroiduksi (12345) ja tutkia ryhmiä $\langle(12345), (123)\rangle$, $\langle(12345), (12)(34)\rangle$ jne.

Olennainen oikotie on havainto
$\langle(12345)\rangle = \langle(13524)\rangle = \langle(14253)\rangle = \langle(15432)\rangle$.
Tämän ansiosta riittää tutkia sellaisten permutaatioiden lisäämistä, jotka alkavat "(12", siis esimerkiksi 4-sykleistä (1234), (1235), (1243), (1245), (1253) ja (1254). Löydettyihin ryhmiin lisätään uusia permutaatioita, kunnes generoituva ryhmä on A_5 tai S_5. Lisäksi esimerkiksi kaksi 5-sykliä generoivat ryhmän A_5, kuten edellä todettiin. Laskenta voidaan aina lopettaa kun päädytään tällaiseen tilanteeseen, jossa lopputulos on jo selvä.

Täysin toisenlainen lähestymistapa on ottaa annettuna transitiivisten aliryhmien lista ja todistaa, ettei muita aliryhmiä ole. Tämä esitetään esimerkiksi lähteessä[4, s. 369].

4.2 Diskriminantti 5. asteen polynomille



Lauseen 3.2 perusteella Galois'n ryhmä on ryhmän A_n aliryhmä, eli siihen kuuluu vain parillisia permutaatioita, jos ja vain jos diskriminantti on rationaaliluvun neliö. Viidennen asteen polynomilla siis

$$\mathrm{Gal}(P) \cong \begin{cases} S_5 \text{ tai } M_{20} & \sqrt{\Delta P} \notin \mathbb{Q} \\ A_5 \text{ tai } D_5 \text{ tai } C_5 & \sqrt{\Delta P} \in \mathbb{Q} \end{cases}$$

Esitämme diskriminantin auki purettuna tapauksessa, jossa 4. asteen termiä ei ole; Tschirnhausin muunnoksella yleinen muoto voidaan aina muuntaa tällaiseksi.

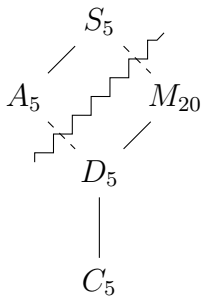
$$\begin{aligned}
&\Delta x^5 + ax^3 + bx^2 + cx + d = \\
&+ 108a^5d^2 - 72a^4bcd + 16a^4c^3 + 16a^3b^3d - 4a^3b^2c^2 - 900a^3cd^2 + 825a^2b^2d^2 \\
&+ 560a^2bc^2d - 128a^2c^4 - 630ab^3cd + 144ab^2c^3 - 3750abd^3 + 2000ac^2d^2 \\
&+ 108b^5d - 27b^4c^2 + 2250b^2cd^2 - 1600bc^3d + 256c^5 + 3125d^4.
\end{aligned}$$

Kaava voidaan periaatteessa muodostaa lauseen 2.9 todistuksen algoritmilla, mutta se olisi erittäin hidasta. Käytännössä toimiva tapa on esimerkiksi lähteessä[6, s. 7].

Palautamme vielä mieleen, että polynomilla $x^2 - \Delta$ ei voi olla moninkertaista juurta. Ainoa mahdollisuus olisi $\Delta = 0$, jolloin tutkittavalla polynomilla olisi moninkertainen juuri, eikä se olisi jaoton.

4.3 Ryhmän M_{20} resolventti

Siirrymme työn monimutkaisimpaan resolventtiin. Tiedämme $\mathrm{Gal}(P) \subseteq S_5$, selvitämme onko $\mathrm{Gal}(P) \subseteq M_{20}$. Tämä resolventti on siis absoluuttinen.

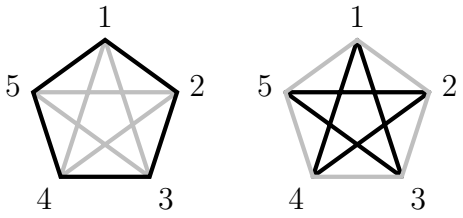


Tarvitsemme tiukasti M_{20}-invariantin polynomin. Koska $|S_5|/|M_{20}| = 120/20 = 6$, tulee kuhunkin sivuluokkaan 20 alkiota ja resolventti tulee olemaan kuudetta astetta.

Määrittelemme ensin D_5-invariantin apupolynomin g:

$$\begin{aligned}
&g(y_1, y_2, y_3, y_4, y_5) = \\
&+ y_1y_2 + y_2y_3 + y_3y_4 + y_4y_5 + y_5y_1 \\
&- y_1y_3 - y_3y_5 - y_5y_2 - y_2y_4 - y_4y_1.
\end{aligned}$$

Havainnollistamme apupolynomia sivulta 37 tutulla kuviolla.



Alkutila Vaihdettu

Polynomi g siis käy läpi kaikki tulot $y_i y_j$, $i \neq j$. Etumerkki on valittu siten, että ylläolevassa kuviossa plus-merkkiset tulot muodostavat reunan viisikulmion, miinus-merkkiset taas sisällä olevan tähden.

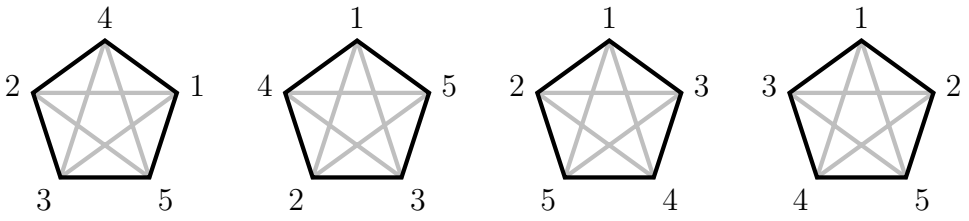
Polynomi g on D_5-invariantti. Tämän voi laskea, mutta sen näkee helposti myös kuviosta: ryhmä D_5 kiertää tai kääntää, ja naapurikulmat säilyvät naapurikulmina.

Jos tehdään ryhmään M_{20} kuuluva vaihto, jokaisen kulman naapurit vaihtuvat. Polynomissa g vaihtuu tällöin jokaisen termin etumerkki, eli koko polynomin arvo vaihtuu vastaluvukseen. Vastalukujen neliöt ovat tietysti samoja, joten M_{20}-invariantti polynomi saadaan neliöimällä:

$$f(y_1, y_2, y_3, y_4, y_5) = g(y_1, y_2, y_3, y_4, y_5)^2.$$

Vielä on todistettava, että polynomi f ei ole invariantti minkään aidosti laajemman ryhmän suhteen. Ainoa mahdollisuus olisi S_5, koska ei ole transitiivista ryhmää G s.e. $M_{20} \subset G \subset S_5$. Esimerkiksi $f(1, 2, 3, 0, 0) = 25$ mutta $f(2, 1, 3, 0, 0) = 1$. Siis f ei ole invariantti permutaation (12) suhteen, eikä siis S_5-invariantti, joten f on tiukasti M_{20}-invariantti.

Havainnollistamme sivuluokat graafisesti. Mikä tahansa viisikulmio voidaan kiertää tilanteeseen, jossa kulma 1 on ylimpänä. Edelleen tekemällä tarvittaessa kääntö ja/tai vaihto saadaan kulma 2 tästä oikealle. Sivuluokat määräytyvät siis kulmien 3, 4 ja 5 sijainnin perusteella; näitä on kuusi kuten pitääkin, koska kolme alkiota voidaan järjestää $3! = 6$ tavalla.



Alkutila Kierto Vaihto Kääntö

Permutaation (35) määräämä sivuluokka: $f(4, 1, 5, 3, 2) = f(1, 2, \mathbf{5}, 4, \mathbf{3})$

Resolventti on siis

$$[x - f(r_1, r_2, \boldsymbol{r_3}, \boldsymbol{r_4}, \boldsymbol{r_5})] \cdot [x - f(r_1, r_2, \boldsymbol{r_4}, \boldsymbol{r_3}, \boldsymbol{r_5})] \cdots [x - f(r_1, r_2, \boldsymbol{r_5}, \boldsymbol{r_4}, \boldsymbol{r_3})].$$

Tämä voidaan kertoa auki ja lauseen 2.9 todistuksen algoritmilla hakea sille kaava tutkittavan polynomin kertoimien avulla siten kuin esimerkissä 3.9 hahmottelimme. Osoittautuu, että resolventti supistuu yllättävän tiiviiseen muotoon[4, s. 373–374]. Polynomin $P(x) = x^5 + ax^3 + bx^2 + cx + d$ kertoimilla se on

$$\mathrm{Res}_{S_5}(P, f) = (x^3 + px^2 + qx + r)^2 - 2^{10}\Delta x$$

jossa Δ on diskriminantti ja

$$\begin{aligned}
p &= -3a^2 - 20c \\
q &= +3a^4 - 8a^2c + 16ab^2 - 400bd + 240c^2 \\
r &= -a^6 + 28a^4c - 16a^3b^2 - 80a^2bd - 176a^2c^2 + 224ab^2c + 4000ad^2 - 64b^4 \\
&\quad - 1600bcd + 320c^3.
\end{aligned}$$

Todistamme lähteen [5, s. 389] pohjalta, ettei resolventilla voi olla kaksinkertaista juurta. Idea on se, että jos yksi resolventin juuri on rationaalinen, niin Galois'n ryhmän alkio kierrättää viittä muuta juurta. Todistus pätee kaikille ryhmät M_{20} ja S_5 erottaville resolventeille.

Lause 4.1. Olkoon P jaoton 5. asteen polynomi. Olkoon f tiukasti M_{20}-invariantti polynomi.

Tällöin resolventilla $\mathrm{Res}_{S_5}(P, f)$ ei ole yhtä useampaa rationaalijuurta.

Todistus:

Jos $\mathrm{Gal}(P) \not\subseteq M_{20}$, ei resolventtilauseen nojalla resolventilla ole rationaalijuuria lainkaan.

Jos $\mathrm{Gal}(P) \subseteq M_{20}$, niin Galois'n ryhmä sisältää yhden syklisen viiden alkion aliryhmän. Voidaan olettaa juuret numeroiduksi niin, että tämä aliryhmä on $\langle(r_1\ r_2\ r_3\ r_4\ r_5)\rangle$. Tällöin rationaalijuuri saadaan resolventin tekijästä $x - f(r_1, r_2, r_3, r_4, r_5)$.

Tutkitaan mihin edellämainitun aliryhmän permutaatiot kuvaavat resolventin tekijän $x - f(r_1, r_2, r_3, \boldsymbol{r_5}, \boldsymbol{r_4})$. Tämä tehdään yksinkertaisesti kierrättämällä tutkittavan polynomin juuria:

$$\begin{aligned}
&f(r_1, r_2, r_3, r_5, r_4) \to f(r_2, r_3, r_4, r_1, r_5) \to f(r_3, r_4, r_5, r_2, r_1) \to \\
&f(r_4, r_5, r_1, r_3, r_2) \to f(r_5, r_1, r_2, r_4, r_3) \to f(r_1, r_2, r_3, r_5, r_4).
\end{aligned}$$

Käännetään nämä tekijät tutumpaan muotoon:

$$f(r_1, r_2, r_3, r_5, r_4) \to f(r_1, r_2, r_4, r_5, r_3) \to f(r_1, r_2, r_5, r_4, r_3) \to$$
$$f(r_1, r_2, r_5, r_3, r_4) \to f(r_1, r_2, r_4, r_3, r_5) \to f(r_1, r_2, r_3, r_5, r_4).$$

Siis resolventin viisi muuta juurta kuvautuvat kukin toisilleen jollain Galois'n ryhmän alkiolla. Jos jokin niistä olisi rationaalinen, kaikkien viiden juuren arvo olisi sama rationaaliluku. Tällöin tutkittavan polynomin juuret olisivat yhtäsuuria, eikä se olisi jaoton.

Yhdistettynä diskriminanttiin tilanne on siis seuraava:

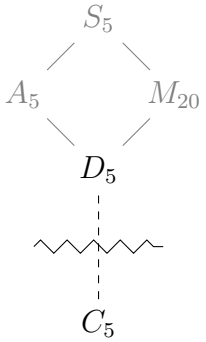
$$\mathrm{Gal}(P) \cong \begin{cases} S_5 & \sqrt{\Delta P} \notin \mathbb{Q} \text{ ja resolventilla ei ole rationaalijuuria} \\ A_5 & \sqrt{\Delta P} \in \mathbb{Q} \text{ ja resolventilla ei ole rationaalijuuria} \\ M_{20} & \sqrt{\Delta P} \notin \mathbb{Q} \text{ ja resolventilla on rationaalijuuri} \\ D_5 \text{ tai } C_5 & \sqrt{\Delta P} \in \mathbb{Q} \text{ ja resolventilla on rationaalijuuri} \end{cases}$$

4.4 Suhteellinen resolventti erottaa ryhmät D_5 ja C_5

Voimme jatkaa loppuun kahdella tavalla: absoluuttinen resolventti erottaa suoraan ryhmän C_5 ryhmässä S_5, suhteellinen resolventti erottaa ryhmän C_5 ryhmässä D_5.

Koska $|S_5|/|C_5| = 120/5 = 24$, on absoluuttinen resolventti 24. asteen polynomi. Ohitamme sen muodostamisen.

Yleisesti voimme käyttää suhteellista resolventtia, kun jo tiedämme Galois'n ryhmän olevan jokin ryhmän S_n aito aliryhmä. Tässä tapauksessa tämä ryhmä on D_5.



Ryhmässä S_5 ei ole vain yhtä ryhmää D_5, vaan kuusi. Tämän vuoksi suhteellisen resolventin käyttö edellyttää aliryhmän täsmällistä selvittämistä. Se puolestaan tarkoittaa, että oikea D_5-aliryhmä on etsittävä numeerisesti.

On luultavasti helpointa ajatella tämä juurien uudelleennumerointina: vaihdetaan numerointi niin, että C_5-aliryhmä on $\langle (r_1\ r_2\ r_3\ r_4\ r_5) \rangle$. Jos esimerkiksi D_5-aliryhmä jollain juurien numeroinnilla on $\langle (r_1\ \boldsymbol{r_3}\ \boldsymbol{r_2}\ r_4\ r_5), (r_3\ r_5)(r_2\ r_4) \rangle$, tehdään vaihto $r_2 \leftrightarrow r_3$.

Ryhmät D_5 ja C_5 erottavaksi resolventtipolynomiksi, joka on symmetrinen "kierron" mutta ei "käännön" suhteen, sopii

$$f(y_1, y_2, y_3, y_4, y_5) = y_1y_2^2 + y_2y_3^2 + y_3y_4^2 + y_4y_5^2 + y_5y_1^2.$$

Tämä on selvästi tiukasti C_5-invariantti, tarkemmin sanoen $\langle(y_1\ y_2\ y_3\ y_4\ y_5)\rangle$-invariantti. Laskemme resolventin auki; sivuluokkia on nyt vain kaksi, koska $|D_5|/|C_5| = 2$.

$$\mathrm{Res}_{D_5}(P, f) =$$
$$(x - r_1r_2^2 + r_2r_3^2 + r_3r_4^2 + r_4r_5^2 + r_5r_1^2)(x - r_5r_4^2 + r_4r_3^2 + r_3r_2^2 + r_2r_1^2 + r_1r_5^2).$$

Todistimme aiemmin, ettei diskriminantilla resolventiksi tulkittuna eikä kuudennen asteen resolventilla voi olla moninkertaista juurta. Valitettavasti sama ei päde viimeiseen resolventtiin. Ratkaisu on Tschirnhausin muunnos, jonka käyttö selviää esimerkeistä.

Suhteellisen resolventin kertoimet eivät ole tutkittavan polynomin juurien symmetrisiä polynomeja. Niinpä suhteellista resolventtia emme voi esittää tutkittavan polynomin kertoimien avulla samalla tavalla kuin absoluuttisen resolventin esitimme.

Lauseen 3.4 nojalla resolventin kertoimet ovat kokonaislukuja. Laskemme siis kertoimien likiarvot numeerisesti ja pyöristämme kokonaisluvuiksi.

Lopuksi optimoimme vähän.

Lause 4.2. Ryhmät D_5 ja C_5 erottavalla suhteellisella resolventilla ei voi olla täsmälleen yhtä rationaalijuurta.

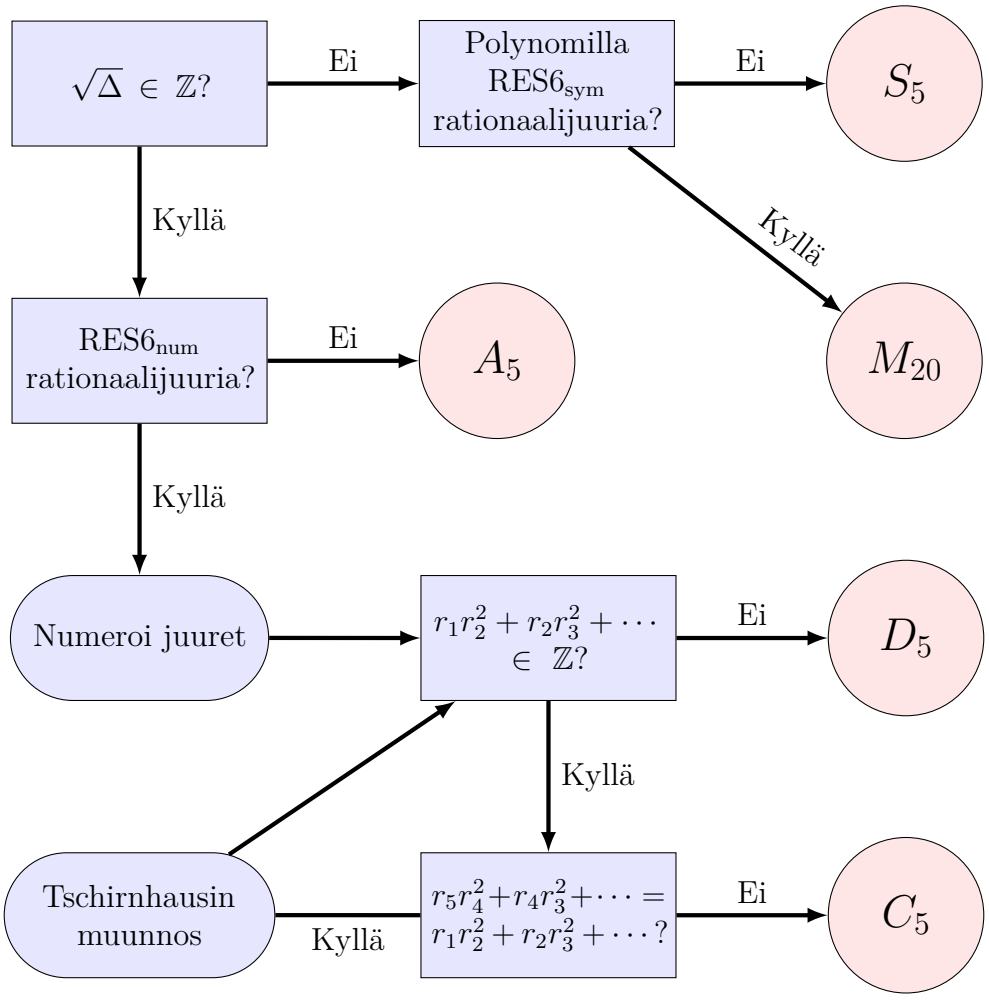
Todistus: Selvästi $\langle(r_1\ r_2\ r_3\ r_4\ r_5)\rangle = \langle(r_5\ r_4\ r_3\ r_2\ r_1)\rangle$ eli molemmat permutaatiot kuuluvat samaan ryhmään. Siispä jos Galois'n ryhmä on C_5, sekä $f(r_1, r_2, r_3, r_4, r_5) \in \mathbb{Q}$ että $f(r_5, r_4, r_3, r_2, r_1) \in \mathbb{Q}$.

Jos siis resolventin juurista yksi ei ole rationaalinen, ei toista tarvitse laskea vaan ryhmän tiedetään olevan D_5.

5 Esimerkkejä

Kokoamme palat yhteen algoritmiksi. Tuloksena tämä antaa ryhmän M_{20} vain konjugaattityyppinä, ryhmät D_5 ja C_5 juuret numeroituna tarkkana ryhmänä. Käytännössä varmaankin myös M_{20} haluttaisiin juuret numeroituna, mutta tässä tarkoitus on vain havainnollistaa resolventteja.

Tässä $\mathrm{RES6}_{\mathrm{sym}}$ on 6. asteen resolventti polynomin kertoimista laskettuna ja $\mathrm{RES6}_{\mathrm{num}}$ sama laskettuna numeerisesti polynomin juurten likiarvoista. Viimeksimainittu siis selvittää Galois'n ryhmästä tietoa tarkasti juuret numeroituna, ensinmainittu vain konjugaattityyppinä.



Havainnollistamme resolventtimenetelmää neljällä polynomilla. Oletamme kaikissa esimerkeissä tunnetuksi sen, että tutkittavat polynomit ovat jaottomia.

Esimerkki 5.1. Tutkitaan polynomia $x^5 - x + 1$.

Diskriminantti muotoa $x^5 + ax + b$ olevalle polynomille on yksinkertaisesti $256a^5 + 3125b^4$, siis tässä tapauksessa $256 \cdot (-1)^5 + 3125 \cdot 1^4 = 2869$. Se ei ole rationaaliluvun neliö, joten Galois'n ryhmä on S_5 tai M_{20}.

Myös kuudennen asteen resolventti on yksinkertaisempi kun osa kertoimista on nollia, tässä tapauksessa $(x^3 + 20x^2 + 240x - 320)^2 - 2937856x$. Mikään luvun 320^2 tasan jakava luku ole resolventin juuri, joten ryhmä on S_5.

Seuraavat kaksi esimerkkiä on valittu tahallisen hankaliksi, jotta näemme resolventin kaksoisjuuren ja sen ratkaisun Tschirnhausin muunnoksella.

Esimerkki 5.2. Tutkitaan polynomia $x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$.

Sijoitetaan polynomiin $x - \frac{1}{5}$ eli tehdään Tschirnhausin muunnos jolla 4. asteen termi katoaa. Tulos on

$$x^5 - \frac{22}{5}x^3 - \frac{11}{25}x^2 + \frac{462}{125}x + \frac{979}{3125}.$$

Diskriminantin kaava antaa tälle tulokseksi 121 eli 11^2. Galois'n ryhmä on siis A_5, D_5 tai C_5.

Tutkittavan polynomin juuret neljän desimaalin tarkkuudella ovat

$$r_1 \approx -1{,}9190,\ r_2 \approx -1{,}3097,\ r_3 \approx -0{,}2846,\ r_4 \approx 0{,}8308,\ r_5 \approx 1{,}6825.$$

Laskemme kuudennen asteen resolventin juuret, siis polynomin

$$f(y_1, y_2, y_3, y_4, y_5) = \\ (+y_1y_2 + y_2y_3 + y_3y_4 + y_4y_5 + y_5y_1 - y_1y_3 - y_3y_5 - y_5y_2 - y_2y_4 - y_4y_1)^2$$

arvon kuudella eri tulokset antavalla permutaatiolla:

$f(r_1, r_2, r_3, r_4, r_5) \approx 31{,}780$
$f(r_1, r_2, r_3, r_5, r_4) \approx 70{,}920$
$f(r_1, r_2, r_4, r_3, r_5) \approx 1{,}077$
$f(r_1, r_2, r_4, r_5, r_3) \approx 95{,}661$
$f(r_1, r_2, r_5, r_3, r_4) \approx \mathbf{0{,}000}$
$f(r_1, r_2, r_5, r_4, r_3)$ ei lasketa

Resolventille näytti löytyvän rationaalijuuri nolla, ja koska lauseen 4.1 nojalla moninkertaisia juuria ei voi olla, lopetimme laskennan tähän. Galois'n ryhmä on tämän perusteella luultavasti M_{20}, D_5 tai C_5, ja koska diskriminantti oli rationaaliluvun neliö, ryhmä on siis D_5 tai C_5.

Varmistetaan tulos sivun 41 kaavalla. Koska mahdollinen rationaalijuuri on nolla, riittää laskea resolventin vakiotermi. Sijoitetaan siis $a = -\frac{22}{5}$, $b = -\frac{11}{25}$ jne. Mainitulla kaavalla saadaan vakiotermiksi odotetusti nolla.

Edellä kuudennen asteen resolventin juuri oli $f(r_1, r_2, r_5, r_3, r_4)$, joten Galois'n ryhmän sisältämä 5-sykli on $(r_1\ r_2\ r_5\ r_3\ r_4)$. Haluamme sykliksi $(r_1\ r_2\ r_3\ r_4\ r_5)$ ja numeroimme juuret tämän mukaan uudelleen:

$$r_1 \approx -1{,}9190,\ r_2 \approx -1{,}3097,\ r_3 \approx 1{,}6825,\ r_4 \approx -0{,}2846,\ r_5 \approx 0{,}8308.$$

Laskemme ryhmät D_5 ja C_5 erottavan suhteellisen resolventin juuret.

$r_1r_2^2 + r_2r_3^2 + r_3r_4^2 + r_4r_5^2 + r_5r_1^2 \approx -3{,}99988$
$r_5r_4^2 + r_4r_3^2 + r_3r_2^2 + r_2r_1^2 + r_1r_5^2 \approx -3{,}99993$

Päädyimme siis ilmeisesti kaksinkertaiseen rationaalijuureen -4, eikä resolventtilause kerro Galois'n ryhmää.

Tehdään Tschirnhausin muunnos $t(r) = r^2 + 2r + 1$.

Muunnetut juuret ovat

$$r_1 \approx 0{,}8446,\ r_2 \approx 0{,}0959,\ r_3 \approx 7{,}1958,\ r_4 \approx 0{,}5118,\ r_5 \approx 3{,}3518.$$

Resolventin juuriksi saadaan nyt noin 14,999 ja 37,002. Galois'n ryhmä todennäköisesti on C_5. Resolventti on, jos laskutarkkuus oli riittävä,

$$x^2 - 52x + 555.$$

Arvioimme vielä hetken tarvittavaa tarkkuutta. Muunnetut juuret ovat kymmentä pienempiä. Oletetaan, että niiden tarkkuus 0,00005. Tällöin muotoa $r_ir_j^2$ olevien tulojen tarkkuus on noin 0,001. Näitä tuloja summataan viisi, jolloin tarkkuus on 0,005. Resolventin termin x kertoimeen lasketaan yhteen kaksi tällä tarkkuudella tiedettyä juurta, jolloin sen tarkkuus on 0,01. Ainakin kerroin 52 on siis oikein.

Seuraavassa esimerkissä vaihtelun vuoksi laskemme enemmän numeerisesti.

Esimerkki 5.3. Tutkitaan polynomia $x^5 - x^4 - 5x^3 + 4x^2 + 3x - 1$.

Juuret ovat

$$r_1 \approx -2{,}0245,\ r_2 \approx -0{,}6768,\ r_3 \approx 0{,}2702,\ r_4 \approx 1{,}2238,\ r_5 \approx 2{,}2074.$$

Diskriminantin neliöjuuri suoraan juurista laskettuna on noin 400,9922. Tulos näyttää epävarmalta, mutta oletamme tämän olevan kokonaisluku 401. Galois'n ryhmä on siis A_5, D_5 tai C_5.

Laskemme kuudennen asteen resolventin numeerisesti. Aloitamme sen juurien likiarvosta:

$T_1 = f(r_1, r_2, r_3, r_4, r_5) \approx 20{,}2582$
$T_2 = f(r_1, r_2, r_3, r_5, r_4) \approx 81{,}2711$
$T_3 = f(r_1, r_2, r_4, r_3, r_5) \approx \mathbf{0{,}9997}$
$T_4 = f(r_1, r_2, r_4, r_5, r_3) \approx 134{,}2211$
$T_5 = f(r_1, r_2, r_5, r_3, r_4) \approx 2{,}7270$
$T_6 = f(r_1, r_2, r_5, r_4, r_3) \approx 94{,}5259$

Nyt emme voineet pysähtyä rationaalijuurelta 1 näyttävään tulokseen, koska laskemme resolventin kertoimia. Kertomalla tästä polynomin auki saamme

$$(x - T_1)(x - T_2) \cdots (x - T_6) =$$
$$x^6 - (T_1 + \cdots + T_6)x^5 + (T_1T_2 + T_1T_3 + \cdots + T_5T_6)x^4 + \cdots + (T_1 \cdots T_6) \approx$$
$$x^6 - 334{,}0030x^5 + 38791{,}8661x^4 - 1805619{,}2087x^3 + \cdots .$$

Laskutarkkuus oli siis aivan liian pieni. Toistamalla laskut tutkittavan polynomin juurien etsimisestä lähtien riittävän suurella tarkkuudella saisimme kuitenkin resolventin, jolla on rationaalijuuri 1. Siis Galois'n ryhmä on D_5 tai C_5.

Edellisen esimerkin tapaan järjestämme polynomin juuret numeerisesti löydetyn resolventin juuren perusteella. Juurien numeroinniksi tulee $r_1 \approx -2{,}0245$, $r_2 \approx 0{,}2702$, $r_3 \approx -0{,}6768$, $r_4 \approx 2{,}2074$ ja $r_5 \approx 1{,}2238$.

Ryhmät D_5 ja C_5 eivät nytkään erotu: viimeisellä resolventilla on kolmen desimaalin tarkkuudella kaksinkertainen rationaalijuuri 5. Tarvitsemme taas Tschirnhausin muunnosta.

Käytämme samaa muunnosta $t(r) = r^2 + 2r + 1$ ja saamme juuret 1,0496, 1,6134, 0,1045, 10,2874 ja 4,9453.

Välitarkistuksena puramme muunnetun polynomin auki. Saamme tulokseksi $x^5 - 18{,}0002x^4 + 95{,}0024x^3 - 171{,}0060x^2 + 103{,}0048x - 9{,}0029$ eli kertoimet näyttävät olevan lähellä kokonaislukuja.

Resolventin juureksi saamme noin $270{,}846 \notin \mathbb{Q}$. Lauseen 4.2 perusteella toista resolventin juurta ei tarvitse laskea. Galois'n ryhmä on D_5.

Viimeisessä esimerkissä yhtenä kertoimena on parametri.

Esimerkki 5.4. Tutkitaan polynomia $x^5 - a$ oletuksella $\sqrt[5]{a} \notin \mathbb{Q}$.

Diskriminantti on 5^5a^4, eli ei neliö. Ryhmä on siis S_5 tai M_{20}.

Kuudennen asteen resolventti supistuu muotoon $x^6 - 3200000a^4x$. Sillä on rationaalijuuri nolla, eli Galois'n ryhmä on M_{20}, D_5 tai C_5.

Siis Galois'n ryhmä tätä muotoa oleville jaottomille polynomeille on M_{20}.

Avoimeksi esimerkeistä jää, olisiko Tschirnhausin muunnos voinut tuottaa uuden kaksoisjuuren. Vastaus on valitettavasti myönteinen, mutta onneksi käytännössä harvinainen. Tschirnhausin muunnos voidaan toistaa sattumanvaraisilla parametreilla. Käytännössä monet Galois'n ryhmän laskevat tietokoneohjelmat tekevätkin juuri niin, vaikka algoritmin päättymistä ei silloin voidakaan todistaa.

6 Tulosten yleistämisestä

Hahmottelemme vielä pintapuolisesti resolventtimenetelmää yleisemmässä tapauksessa.

6.1 Kerroinkunnista

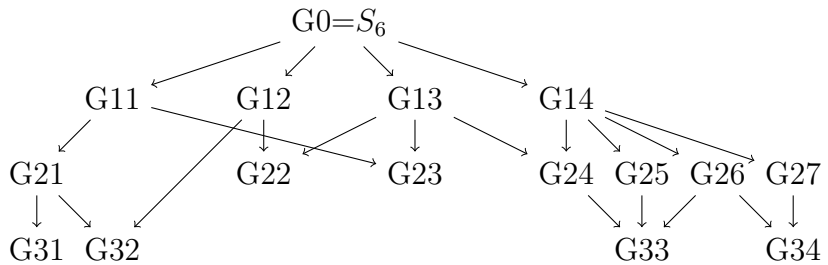
Galois'n ryhmä voidaan määritellä missä tahansa kerroinkunnassa, vaikka tässä työssä käsittelimme vain rationaalikertoimisia polynomeja. Esityksen ydin, resolventtilause, pätee kerroinkunnasta riippumatta. Sen sijaan resolventin kertoimien etsiminen approksimoimalla juuria riittävällä numeerisella tarkkuudella ei tietenkään mielivaltaisessa kerroinkunnassa ole mahdollista.

Muista muutoksista toteamme esimerkkinä, että kerroinkunnan karakteristikan ollessa 2 on jokainen alkio itsensä vastaluku. Tällöin diskriminantin sijaan tarvitaan muu resolventti tunnistamaan onko Galois'n ryhmä alternoivan ryhmän aliryhmä; kolmannen asteen polynomille tällainen on esimerkissä 3.4.[3, s. 2–3].

6.2 Transitiivisten aliryhmien etsintä

Esitämme malliksi ryhmän S_6 transitiivisten aliryhmien verkon, joka Sagella saadaan komennolla

```
G=TransitiveGroups(6);
print join([str(i)+": "+join([str(j)
for j in range(i-1,0,-1) if G[j].is_subgroup(G[i])])
for i in range(len(G),0,-1)], "\n")
```



Transitiiviset aliryhmät on luetteloitu ryhmään S_{32} saakka. Jos n on alkuluku, ei ryhmässä S_n ole kovin paljon transitiivisia aliryhmiä, esimerkiksi ryhmällä S_7 seitsemän ja ryhmällä S_{11} kahdeksan. Toisaalta yllä kuvatusta ryhmästä S_6 niitä löytyy 16, ryhmästä S_8 jo 50.[9]

Ryhmän S_p, jossa p on alkuluku, transitiivinen aliryhmä sisältää p-syklin ja se on hyvä lähtöpiste aliryhmien luettelointiin. Sama ei päde yleisesti ryhmille S_n, vaan esimerkiksi $\{(), (12)(34), (13)(24), (14)(23)\}$ on ryhmän S_4 transitiivinen aliryhmä, joka ei sisällä 4-sykliä. Muun muassa tämän vuoksi transitiivisten aliryhmien luettelointi on monimutkainen tehtävä.

Teoriassa transitiiviset aliryhmät ovat aina etsittävissä, koska hakuavaruus on äärellinen.

6.3 Resolventtien käyttöjärjestys

Selvää on, että kaikkia mahdollisia resolventteja ei tarvita. Esimerkiksi viidennen asteen tapauksessa ei koskaan selvitetä suoraan onko Galois'n ryhmä ryhmän D_5 aliryhmä, vaan tämä selviää ryhmät A_5 ja M_{20} tunnistavilla resolventeilla.

Luonteva tapa on aloittaa ryhmän S_n maksimaalisista aliryhmistä, oikean aliryhmän löydyttyä käydä läpi sen maksimaaliset aliryhmät ja niin edelleen. Maksimaalisista aliryhmistä kannattanee ensimmäiseksi valita suurin, koska tällöin resolventin asteluku on pienin. Toinen vaihtoehto on valita se, joka jakaa jäljellä olevan hakuavaruuden mahdollisimman samankokoisiin osiin, koska tällöin resolventteja tarvitaan vähiten.

Jos mahdollisia Galois'n ryhmiä on n, ovat teoreettiset rajat $n-1$ ja $\lceil \log_2 n \rceil$ resolventtia. Yläraja syntyy, kun kaikki mahdolliset aliryhmät ovat "rinnakkain", saman ryhmän maksimaalisia aliryhmiä. Alaraja saavutetaan kun mahdolliset aliryhmät ovat "ketjussa", siten että jokaisella ryhmällä on vain yksi maksimaalinen aliryhmä ja jokainen resolventti jakaa ketjun kahtia.

Yleisesti tietokoneohjelmia optimoidaan kahdella kriteerillä: pahimman ja keskimääräisen tapauksen mukaan. Keskimääräinen tapaus on vaikeasti määriteltävissä Galois'n ryhmien yhteydessä — tulisiko esimerkiksi olettaa kaikki ryhmät yhtä todennäköisiksi, vai polynomien kertoimet tasajakautuneiksi kokonaisluvuiksi jollain välillä?

6.4 Resolventtipolynomien muodostaminen

On olemassa teoreettisesti yksinkertainen ratkaisu resolventtipolynomiksi[1, s. 4]: summataan aliryhmän H mukaiset permutaatiot nousevin potenssein kerrottuna, siis $\sum_{\sigma \in H} \sigma(y_1 y_2^2 \cdots y_n^n)$.

Esimerkiksi ryhmän D_4 mukaisesti neljää juurta voi permutoida kahdeksalla tavalla; eräs sivuluokka sisältää esimerkiksi permutaatiot $(r_1\ r_2\ r_3\ r_4)$, $(r_2\ r_1\ r_4\ r_3)$ ja kuusi muuta permutaatiota. Resolventtipolynomissa summattaisiin tällöin yhteen näitä vastaavasti $r_1 r_2^2 r_3^3 r_4^4$, $r_2 r_1^2 r_4^3 r_3^4$ ja kuusi muuta

tuloa. Näin ratkaisu on huomattavasti monimutkaisempi kuin tässä työssä esimerkkinä ollut $f(r_1, r_2, r_3, r_4) = r_1r_2 + r_3r_4$.

Parhaiden, tai edes käytännössä järkevästi laskettavissa olevien, resolventtipolynomien etsimiseen ei ilmeisesti ole yksinkertaista tapaa[1].

Absoluuttinen resolventti on esitettävissä tutkittavan polynomin kertoimien avulla, mutta se monimutkaistuu ja sen asteluku kasvaa polynomin asteluvun kasvaessa. Numeerisessa laskennassa puolestaan vaadittava laskentatarkkuus kasvaa. Nämä ongelmat ovat ilmeisesti väistämättömiä.

Rationaalikertoimisen polynomin Galois'n ryhmän määrittäminen on siis periaatteellisesti aina ratkaistavissa oleva ongelma. Käytännössä resolventtimenetelmää tässä esitettyyn tapaan käytetään ainoastaan matalaa, 3.–5. astetta oleviin polynomeihin.

[1]Tätä työtä tehtäessä ei kuitenkaan ole tutkittu Claus Fiekerin ja Jürgen Klünersin tuoretta julkaisua Computational Galois Theory: Invariants and Computations over $\mathbb{Q}$.

Viitteet

[1] Cangelmi, L. *Resolvents and Galois Groups*. Number Theory 53(3) (1995).

[2] Carter, N. *Visual Group Theory*. Mathematical Association of America, 2009.

[3] Conrad, Keith. *Galois Groups of Cubics and Quartics (All Characteristics)*. `http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/cubicquarticallchar.pdf`.

[4] Cox, David A. *Galois theory*. John Wiley & Sons, 2004.

[5] Dummit, D. S. *Solving Solvable Quintics*. Mathematics of Computation 57(195), ss. 387–401.

[6] Healy, Alexander D. *Resultants, Resolvents and the Computation of Galois Groups*. `http://www.alexhealy.net/papers/math250a.pdf`.

[7] Jensen, Christian U., Ledet, Arne ja Yui, Noriko. *Generic Polynomials, Constructive Aspects of the Inverse Galois Problem*. Cambridge University Press, 2002.

[8] Judson, Thomas W. *Abstract Algebra / Theory and Applications*. Verkkokirja `http://abstract.ups.edu/`, vuoden 2011 versio.

[9] OEIS-sarja A002106. `http://oeis.org/A002106`.

[10] Shurman, Jerry. *Algebraic Numbers and Algebraic Integers*. `http://people.reed.edu/~jerry/361/lectures/lec09.pdf`.

[11] Stauduhar, Richard P. *The Determination of Galois Groups*. Mathematics of Computation 27(124) (1973)

[12] Stewart, Ian. *Galois Theory*. Chapman and Hall, 1973.

Viittaukset verkkosivustoihin on tarkistettu 6.5.2013.