Symmetriset polynomit ja resultantti

Pro gradu -tutkielma
Pauliina Pigg
Matematiikan ja tilastotieteen laitos
Helsingin yliopisto
Tammikuu 2014

HELSINGIN YLIOPISTO — HELSINGFORS UNIVERSITET — UNIVERSITY OF HELSINK

Tiedekunta/Osasto — Fakultet/Sektion — Faculty	Laitos — Institution — Department
Matemaattis-luonnontieteellinen	Matematiikan ja tilastotieteen laitos

Tekijä — Författare — Author
Pauliina Pigg

Työn nimi — Arbetets titel — Title

Symmetriset polynomit ja resultantti

Oppiaine — Läroämne — Subject		
Matematiikka		
Työn laji — Arbetets art — Level	Aika — Datum — Month and year	Sivumäärä — Sidoantal — Number of pages
Pro gradu -tutkielma	Tammikuu 2014	40 s.

Tiivistelmä — Referat — Abstract

Tutkielma jakautuu otsikon mukaisesti kahteen osaan, jotka ovat symmetriset polynomit ja resultantti. Osiot eivät ole täysin erillisiä, sillä resultanttia laskiessa voidaan hyödyntää symmetristen polynomien ominaisuuksia.

Aluksi määritellään symmetrisen polynomin käsite sekä esitellään symmetriset perusfunktiot. Symmetrinen polynomi käytännössä tarkoittaa polynomia, joka pysyy muuttumattomana, vaikka sen muuttujien järjestystä vaihdettaisiin mielivaltaisesti. "Symmetriset polynomit- osuuden ydin on symmetristen funktioiden peruslause, joka kiteytettynä tarkoittaa, että jokainen symmetrinen polynomi voidaan yksikäsitteisesti esittää symmetristen perusfunktioiden avulla. Lisäksi esitellään polynomiyhtälön kertoimien ja kyseisen yhtälön juurien symmetristen perusfunktioiden välinen yhteys.

Resultantti on eräs kahdesta polynomiyhtälöstä muodostettu matemaattinen lauseke. Työssä esitellään resultantin lause sekä osoitetaan se todeksi kahdella eri tapaa. Toinen todistustavoista pohjautuu symmetrisiin perusfunktioihin, ja toinen tapa polynomiyhtälöistä muodostettavien determinanttien käyttöön. Resultantille voidaan laskea arvo suoraan sijoittamalla resultantin lausekkeeseen lukuarvot, jotka saadaan annetuista polynomiyhtälöistä. Resultantin parhaimpia käyttöominaisuuksia kuitenkin on, että sen avulla voidaan selvittää kahden polynomin yhteiset nollakohdat sekä mahdollinen tuntematon muuttuja. Tämän mahdollistaa muuan muassa se, että resultantin arvo on nolla, kun se muodostetaan yhteisen juuren omaaville polynomiyhtälöille. Resultanttia on hyödynnetty jopa todistettaessa RSA-salauksen luotettavuutta. Työn lopussa esitetään myös algoritmi, jolla resulantin arvo voidaan laskea.

Avainsanat — Nyckelord — Keywords
Symmetriset polynomit, polynomit, resultantti, RSA-salaus, algoritmi resultantille

Säilytyspaikka — Förvaringsställe — Where deposited
Kumpulan tiedekirjasto

Muita tietoja — Övriga uppgifter — Additional information

Sisältö

Johdanto

Tutkielman alussa määritellään symmetrisen polynomin käsite muutamalla esimerkillä varustettuna. Symmetrinen polynomi tarkoittaa käytännössä sitä, että se säilyy muuttumattomana, vaikka sen muuttujia järjesteltäisiin uudelleen mielivaltaisesti. Lisäksi esitetään määritelmät polynomin homogeenisuudesta ja epähomogeenisuudesta, jonka jälkeen käsitellään "Symmetriset polynomit" -osuuden ydintä eli symmetristen funktioiden peruslausetta se todeksi osoittaen. Symmetristen polynomien peruslause sanoo, että jokainen symmetrinen polynomi, jonka toisistaan riippumattomat muuttujat ovat x_1, x_2, ..., x_n, voidaan esittää muuttujien x_1, x_2, ..., x_n symmetristen perusfunktioiden avulla. Symmetrinen perusfunktio $p_k(x_1, x_2, \ldots, x_n)$, missä $1 \leq k \leq n$, on sen muuttujien summa tai muuttujista muodostettujen tulojen summa, jossa kunkin tulon tulontekijöiden määrä on k. Jokaisessa tulossa tulontekijöillä pitää olla eri indeksit. Summa ei voi sisältää kahta samanlaista termiä. Lisäksi kaikilla termeillä on kertoimena luku 1. Summan pitää sisältää kaikki mahdolliset termit, jotka täyttävät nämä edellä esitetyt ehdot.
Tämän jälkeen on pari esimerkkiä siitä, kuinka peruslauseen todistuksen ideaa hyväksikäyttäen voidaan symmetriselle funktiolle löytää muoto, jossa se on esitettynä perusfunktioiden avulla. Luvussa kaksi tarkastellaan, millainen yhteys yhtälön juurien symmetrisillä perusfunktioilla ja yhtälön kertoimilla on. Nämä ensimmäiset kaksi lukua olen kirjoittanut luonnontieteiden kandidaantin tutkimelmaani. Olen liittänyt ne myös tähän työhön mukaan esityksen täydellisyyden ja helppolukuisuuden vuoksi, sillä resultanttia käsitellessäni olen käyttänyt apuna symmetrisiä polynomeja.
Kolmas luku, tämän työn ydin, käsittelee resultanttia. Resultantin lauseen mukaan kahden polynomiyhtälön A ja B resultantti R voidaan esittää polynomin A kertoimien suhteen polynomin B astetta olevana ja polynomin B kerrointen suhteen polynomin A astetta olevana homogeenisena polynomina, jonka kertoimet ovat kokonaislukuja. Resultantti $R = 0$, jos ja vain jos yhtälöillä on yhteinen juuri. Resultantin lause todistetaan symmetrisiin funktioihin perustuen sekä johdetaan se yhtälöistä muodostettavan determinantin avulla. Todistettaessa kahden polynomiyhtälön resultantti symmetrisiin perusfunktioihin perustuen jäsennellään resultantin lauseketta niin, että kertoimiksi muodostuu toisen polynomiyhtälön juurien symmetrisiä polynomeja. Kun tässä hyödynnetään luvussa 2 todettua polynomiyhtälön kerrointen, symmetristen perusfunktioiden ja yhtälön juurien symmetristen polynomien välistä yhteyttä, on saatu resultantin lauseke esitettyä muodossa, joka on täsmälleen resultantin lauseen mukainen. Esimerkin avulla esitetään, kuinka tapauksissa, joissa yhtälöillä on yhteinen juuri, voidaan resultanttia apuna käyttäen selvittää mahdollinen tuntematon tekijä sekä yhteisten juurien arvot. Johdettaessa resultantti determinanttien avulla pyritään to-

teamaan, että polynomiyhtälöistä A ja B muodostetun yhtälön kerroinmatriisin determinantti D on täsmälleen sama kuin resultantti R. Lopputulokseen päädytään esittämällä kahdella eri tapaa tulo $a_0^n b_0^m DM$, missä a_0 ja b_0 ovat polynomien korkeimpien termien kertoimet, luku n polynomin B aste, luku m polynomin A aste sekä determinantti M polynomien A ja B juurista muodostettu Vandermonden determinantti. Kolmannen luvun loppuosassa esitellään algoritmi resultantin laskemiselle sekä lasketaan algoritminkäyttöä selventävä esimerkkitehtävä sekä todistetaan algoritmin pitävän paikkansa.
Esitys on tehty siten, että kirjoittaja olettaa lukijan hallitsevan algebran alkeet. Lähteinä on käytetty pääosin teoksia [1] ja [2].

1 Symmetriset polynomit

Määritelmä 1. Olkoon s_n joukon $\{1, 2, \ldots, n\}$ permutaatioiden joukko. Polynomi $p(x_1, x_2, \ldots, x_n)$ on *symmetrinen*, jos

$$p^{\Pi}(x_1, x_2, \ldots, x_n) = p(x_{\Pi(1)}, x_{\Pi(2)}, \ldots, x_{\Pi(n)}) = p(x_1, \ldots, x_n)$$

kaikilla $\Pi \in s_n$. ($Kts.$[3])

Symmetriseksi funktioksi kutsutaan siis toisistaan riippumattomien muuttujien funktiota, jos funktio ei muutu, vaikka muuttujien paikkoja vaihdeltaisiin keskenään kuinka tahansa. Olkoot x_1, x_2, …, x_n yhtälön

$$A(x) = (x - x_1)(x - x_2)\cdots(x - x_n) \tag{1}$$

toisistaan riippumattomat muuttujat. Kehittämällä yhtälön (1) oikea puoli muuttujan x polynomiksi saadaan

$$A(x) = x^n - p_1 x^{n-1} + p_2 x^{n-2} - \cdots + (-1)^n p_n, \tag{2}$$

missä jokainen $p_i = p_i(x_1, \ldots, x_n)$ on muuttujien x_1, x_2, …, x_n symmetrinen polynomi.

Näitä ovat

$$\begin{aligned}
p_1(x_1, x_2, \ldots, x_n) &= x_1 + x_2 + \cdots + x_n, \\
p_2(x_1, x_2, \ldots, x_n) &= x_1x_2 + \cdots + x_1x_n + x_2x_3 + \cdots + x_2x_n + \cdots + x_{n-1}x_n, \\
p_3(x_1, x_2, \ldots, x_n) &= x_1x_2x_3 + \cdots + x_1x_{n-1}x_n + \cdots + x_{n-2}x_{n-1}x_n, \\
&\vdots \\
p_n(x_1, x_2, \ldots, x_n) &= x_1x_2\cdots x_n, \\
p_{n+1}(x_1, x_2, \ldots, x_n) &= p_{n+2}(x_1, x_2, \ldots, x_n) = \ldots = 0.
\end{aligned}$$

Siis, kun $1 \leq k \leq n$, niin $p_k(x_1, x_2, \ldots, x_n)$ on kaikkien niiden muuttujista $x_1, x_2, \ldots, x_n$ saatujen tulojen summa, joissa on k tekijää ja jokaisella tekijällä on eri indeksi. Polynomin $p_k(x_1, x_2, \ldots, x_n)$ kaikilla termeillä on kertoimenaan luku 1. Polynomeja $p_1, p_2, \ldots, p_n$ kutsutaan muuttujien $x_1, x_2, \ldots, x_n$ symmetrisiksi perusfunktioiksi.

Määritelmä 2. *Homogeeninen polynomi* on polynomi, jonka termien asteet ovat samat. Termin asteluku määräytyy sen sisältämän muuttujan potenssista. Useamman muuttujan sisältävän termin asteluku (kokonaisaste) saadaan summaamalla muuttujien potenssit.

Esimerkki 1. $x^5 + 2x^2y^3 + 9xy^4$ on homogeeninen polynomi, jonka aste on 5.

Määritelmän 2. perusteella voidaan todeta, että symmetrinen perusfunktio $p_k(x_1, x_2, \ldots, x_n)$, missä $1 \leq k \leq n$, on homogeeninen polynomi, jonka aste on k.

Määritelmä 3. Polynomi on *epähomogeeninen*, jos se ei ole homogeeninen. Siis epähomogeenisen polynomin termien kokonaisaste ei ole kaikilla termeillä sama.

Muuttujien $x_1, x_2, \ldots, x_n$ symmetrisiksi polynomeiksi kutsutaan myös funktioita, jotka eivät ole edellä mainittujen symmetristen perusfunktioiden muodossa, mutta voidaan esittää symmetristen perusfunktioiden polynomeina. Helposti nähdään, että myös tuntemattomien neliöiden summa $x_1^2 + x_2^2 + \ldots + x_n^2$ on symmetrinen. Erityisesti kahden symmetrisen polynomin summa, erotus ja tulo ovat symmetrisiä.

Esimerkki 2. Olkoon $n = 3$ ja polynomina symmetrisistä perusfunktioista koostuva polynomi $p_1p_2 + 2p_3$. Korvataan p_1, p_2 ja p_3 niiden lausekkeilla, jotka koostuvat muuttujista $x_1, x_2, \ldots, x_n$. Tällöin saadaan

$$\begin{aligned}(p_1p_2 + 2p_3)(x_1, x_2, x_3) &= (x_1 + x_2 + x_3)(x_1x_2 + x_1x_3 + x_2x_3) + 2(x_1x_2x_3) \\ &= x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_2^2x_3 + x_1x_3^2 + x_2x_3^2 + 5x_1x_2x_3.\end{aligned}$$

Saatu polynomi on selvästi symmetrinen. Tämä nähdään seuraavasti.

Olkoon $\pi \in s_3$ mielivaltainen. Tällöin

$$\begin{aligned}(p_1p_2 + 2p_3)(x_{\pi(1)}, x_{\pi(2)}, x_{\pi(3)}) =& p_1(x_{\pi(1)}, x_{\pi(2)}, x_{\pi(3)})p_2(x_{\pi(1)}, x_{\pi(2)}, x_{\pi(3)}) \\ &+ 2p_3(x_{\pi(1)}, x_{\pi(2)}, x_{\pi(3)}) \\ =& p_1(x_1, x_2, x_3)p_2(x_1, x_2, x_3) + 2p_3(x_1, x_2, x_3) \\ =& (p_1p_2 + 2p_3)(x_1, x_2, x_3).\end{aligned}$$

Esimerkki 3. (Muuttujien uudelleenjärjestäminen)

Vaihdetaan edellisessä määritelmässä esiintyvän polynomin

$$(p_1p_2 + 2p_3)(x_1, x_2, x_3) = (x_1 + x_2 + x_3)(x_1x_2 + x_1x_3 + x_2x_3) + 2(x_1x_2x_3)$$

muuttujat x_1 ja x_2 keskenään.

Tällöin saadaan

$$(p_1p_2 + 2p_3)(x_2, x_1, x_3) = (x_2 + x_1 + x_3)(x_2x_1 + x_2x_3 + x_1x_3) + 2(x_2x_1x_3).$$

Järjestämällä muuttujat uudelleen saadaan jälleen

$$(p_1p_2 + 2p_3)(x_2, x_1, x_3) = (x_1 + x_2 + x_3)(x_1x_2 + x_1x_3 + x_2x_3) + 2(x_1x_2x_3).$$

Huomataan, että lauseke ei muutu, vaikka muuttujien x_1, x_2, x_3 järjestystä vaihdettaisiin kuinka tahansa. Siispä ko.polynomi on symmetrinen.

Jos $cx_1^{v_1}x_2^{v_2}\cdots x_n^{v_n}$ on sellaisen symmetrisen polynomin, jossa samanmuotoiset muuttujat on yhdistetty, termi, niin polynomin täytyy sisältää myös kaikki termit, jotka saadaan äsken mainitusta termistä vaihtamalla eri tavoin muuttujien $x_1, \ldots, x_n$ järjestystä. Nämä jäsenet muodostavat yhdessä oman symmetrisen polynominsa, joka on lisäksi homogeeninen. Sitä merkitään symbolilla

$$S(cx_1^{v_1}x_2^{v_2}\cdots x_n^{v_n}).$$

Esimerkki 4. Jos $n = 3$ ja $x_1^4x_2$ on jokin symmetrisen polynomin termi, niin symmetrinen polynomi sisältää myös osasumman

$$S(x_1^4x_2) = x_1^4x_2 + x_1^4x_3 + x_2^4x_1 + x_2^4x_3 + x_3^4x_1 + x_3^4x_2.$$

Siispä jokainen symmetrinen polynomi voidaan esittää symmetristen osasummien summana. Tästä seuraa, että *epähomogeeninen symmetrinen polynomi voidaan aina esittää homogeenisten symmetristen polynomien summana.*

Esimerkki 5. Olkoon $n = 3$. Symmetrisistä perusfunktioista koostuva polynomi $p_1(x_1, x_2, x_3) + p_2(x_1, x_2, x_3) = x_1 + x_2 + x_3 + x_1x_2 + x_1x_3 + x_2x_3$ on symmetrinen. Polynomi ei selvästikään ole homogeeninen, mutta se voidaan lausua homogeenisten polynomien p_1 ja p_2 summana.

Lause 1 (Peruslause). *Olkoon R kommutatiivinen ykkösellinen rengas ja $R[x_1, x_2, \ldots, x_n]$ R-kertoimisten polynomien rengas. Jokainen symmetrinen polynomi $P(x_1, x_2, \ldots, x_n) \in R[x_1, x_2, \ldots, x_n]$ voidaan lausua symmetristen perusfunktioiden polynomina $Q(p_1, p_2, \ldots, p_n) \in R[p_1, p_2, \ldots, p_n]$. Polynomi Q on yksikäsitteisesti määrätty ja sen kokonaisaste perusfunktoiden $p_1, p_2, \ldots, p_n$ suhteen on yhtäsuuri kuin polynomin P aste muuttujan x_1 suhteen.*

Todistus. Koska epähomogeeninen symmetrinen polynomi voidaan esittää homogeenisten symmetristen polynomien summana, niin todistuksessa riittää käsitellä vain tapausta, jossa P on homogeeninen.

Käsittelemme seuraavassa polynomin korkeinta termiä, sillä symmetrisen funktion korkein termi määrää polynomin asteen muuttujan x_1 suhteen.

Olkoon $P(x_1, x_2, \ldots, x_n)$ astetta t oleva symmetrinen polynomi. Jos

$$M = c_i x_1^{i_1} x_2^{i_2} \cdots, x_n^{i_n} \qquad \text{ja} \qquad \mathrm{N} = c_j x_1^{j_1} x_2^{j_2} \cdots, x_n^{j_n}$$

ovat kaksi polynimin P termiä ja ensimmäinen erotuksista

$$i_1 - j_1,\ i_2 - j_2,\ \ldots,\ i_n - j_n,$$

joka on nollasta eroava, on positiivinen, niin sanotaan, että M on *korkeampi* kuin N ja vastaavasti N on *matalampi* kuin M. Voidaan olettaa, että polynomissa P samanmuotoiset termit on aina yhdistetty. Tällöin polynomissa P jokin jäsen on *korkein*, sillä sen kahdesta termistä toinen on aina korkeampi. Olkoon tämä korkein termi

$$a_0 x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}. \tag{3}$$

Polynomi P on homogeeninen, joten korkeimmalle termille pätee

$$k_1 + k_2 + \cdots + k_n = t \qquad \text{ja} \qquad \mathrm{k}_1 \geq k_2 \geq \cdots \geq k_n.$$

Nimittäin, jos olisi $k_i < k_{i+1}$ jollakin i, niin polynomi $P(x_1, x_2, \ldots, x_n)$ symmetrisenä polynomina sisältäisi termin

$$a_0 x_1^{k_1} x_2^{k_2} \cdots x_{i+1}^{k_i} x_i^{k_{i+1}} \cdots x_n^{k_n} = a_0 x_1^{k_1} x_2^{k_2} \cdots x_i^{k_{i+1}} x_{i+1}^{k_i} \cdots x_n^{k_n}, \tag{4}$$

missä yhtälön oikea puoli on saatu vasemmasta vaihtamalla keskenään tekijöiden $x_i^{k_{i+1}}$ ja $x_{i+1}^{k_i}$ paikkaa. Vertaamalla muuttujan x_i potensseja termien (3) ja (4) kesken huomataan, että (4) on korkeampi kuin (3), sillä oletettiin, että $k_i < k_{i+1}$. Tämä on ristiriita, sillä oletuksena oli, että termi (3) on korkein.

Muodostetaan peruslauseen todistusta varten symmetristen perusfunktioiden tulosta muodostuva polynomi

$$Q_1 = a_0 p_1^{k_1 - k_2} p_2^{k_2 - k_3} \cdots p_{n-1}^{k_{n-1} - k_n} p_n^{k_n}. \tag{5}$$

Tämä on homogeeninen symmetrinen polynomi muuttujien $x_1, x_2 \ldots x_n$ suhteen, ja sen kaikki potenssit ovat ei-negatiivisia kokonaislukuja. Perusfunktioiden

$p_1, p_2 \dots p_n$ korkeimmat termit ovat $x_1, x_1x_2, x_1x_2x_3, \dots, x_1x_2 \cdots x_n$. Koska homogeenisten symmetristen polynomien tulon korkein termi on yhtäsuuri kuin tekijöiden korkeimpien termien tulo, saadaan polynomin Q_1 korkeimmaksi termiksi

$$a_0 x_1^{k_1-k_2}(x_1x_2)^{k_2-k_3}(x_1x_2x_3)^{k_3-k_4}\cdots(x_1x_2\cdots x_{n-1})^{k_{n-1}-k_n}(x_1x_2\cdots x_n)^{k_n} =$$
$$a_0\frac{x_1^{k_1}}{x_1^{k_2}}\cdot\frac{x_1^{k_2}x_2^{k_2}}{x_1^{k_3}x_2^{k_3}}\cdot\frac{x_1^{k_3}x_2^{k_3}x_3^{k_3}}{x_1^{k_4}x_2^{k_4}x_3^{k_4}}\cdots\frac{x_1^{k_{n-1}}x_2^{k_{n-1}}x_3^{k_{n-1}}\cdots x_{n-1}^{k_{n-1}}}{x_1^{k_n}x_2^{k_n}x_3^{k_n}\cdots x_{n-1}^{k_n}}\cdot x_1^{k_n}x_2^{k_n}x_3^{k_n}\cdots x_n^{k_n} =$$
$$a_0 x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n},$$

joka on ekvivalentti polynomin P korkeimman termin kanssa.

Koska siis polynomien P ja Q_1 korkeimmat termit ovat samat, vähennettäessä polynomi Q_1 polynomista P korkein termi häviää. Muodostuneen, edelleen muuttujien $x_1, x_2 \dots x_n$ suhteen astetta t olevan, homogeenisen symmetrisen polynomin $P - Q_1 = P_1$ korkein termi on täten matalampi kuin termi (3), sillä vain yksi termeistä voi olla korkein symmetrisessä polynomissa, jossa samanmuotoiset termit on yhdistetty. Olkoon tämä polynomin P_1 korkein termi

$$b_0 x_1^{l_1}x_2^{l_2}\cdots x_n^{l_n}$$

ja merkitään

$$Q_2 = b_0 p_1^{l_1-l_2}p_2^{l_2-l_3}\cdots p_{n-1}^{l_{n-1}-l_n}p_n^{l_n}.$$

Toistamalla edellä mainittu prosessi polynomille Q_2, huomataan, että sen korkein termi on sama kuin polynomin P_1 korkein termi. Tällöin vastaavasti saadaan

$$P_1 - Q_2 = P_2,$$

jossa polynomin P_2 korkein termi on taas matalampi kuin polynomin P_1. Tähän sijoittamalla $P - Q_1 = P_1$ saadaan yhtälö

$$P - Q_1 - Q_2 = P_2,$$

josta saadaan polynomille P esitys

$$P = Q_1 + Q_2 + P_2.$$

Jatkamalla tätä prosessia saadaan lopulta $P_s = 0$ jollakin s ja voimme näin ollen ilmaista polynomin P polynomien $Q_1, Q_2, \dots, Q_s$ summana:

$$P(x_1, x_2, \dots, x_n) = Q_1 + Q_2 + \cdots + Q_s = Q(p_1, p_2, \dots, p_n),$$

missä polynomin Q kertoimet ovat polynomin P kertoimien määräämän renkaan lukuja.

Polynomin Q_1 aste symmetristen perusfunktioiden suhteen on

$$(k_1 - k_2) + (k_2 - k_3) + \cdots + (k_{n-1} - k_n) + k_n = k_1.$$

Vastaavasti saadaan polynomin Q_2 aste symmetristen perusfunktioiden suhteen on $l_1 \leq k_1$ jne. Polynomien $Q_1, Q_2, \ldots, Q_n$ summasta muodostuvan polynomin Q aste symmetristen perusfunktioiden $p_1, p_2, \ldots, p_n$ suhteen määräytyy luonnollisesti sen symmetristen perusfunktioiden suhteen korkeinta astetta (kokonaisastetta) olevan termin mukaan. Äskettäin todettiin, että polynomin Q_1 symmetristen perusfunktioiden suhteen muodostuva asteluku k_1 oli korkeampi tai yhtäsuuri kuin muiden osasummien $Q_2, Q_3, \ldots, Q_n$ asteluvut symmetristen perusfunktioiden suhteen. Täten myös polynomin Q asteluku symmetristen perusfunktioiden suhteen on k_1. Myös polynomin P korkeimman jäsenen aste muuuttujan x_1 suhteen on k_1. Täten polynomin Q aste perusfunktoiden $p_1, p_2, \ldots, p_n$ suhteen on yhtäsuuri kuin polynomin P aste muuttujan x_1 suhteen.

Todistamme vielä, että polynomi Q on määrätty yksikäsitteisesti. Suoritamme todistuksen tekemällä vastaoletuksen, että polynomia P esittää vielä toinen symmetristen perusfunktioiden $p_1, p_2, \cdots, p_n$ polynomi. Olkoon tämä $Q'(p_1, p_2 \cdots, p_n)$. Tällöin näiden erotus on

$$Q - Q' = 0 = \sum g_i p_1^{i_1} p_2^{i_2} \ldots p_n^{i_n}.$$

Tässä kertoimet g_i ovat nollasta eroavia. Yhtälö muuttuu identtiseksi lausuttaessa polynomit $p_1, p_2, \ldots, p_n$ muuttujien $x_1, x_2, \ldots, x_n$ avulla. Summan termit ilmaistuna yleisessä muodossa ovat muuttujien $x_1, x_2, \ldots, x_n$ homogeenisia symmetrisiä polynomeja. Olkoon summan yleisen termin korkein jäsen $g_i x_1^{\lambda_1} x_2^{\lambda_2} \ldots x_n^{\lambda_n}$. Koska homogeenisten symmetristen polynomien tulon korkein termi on yhtäsuuri kuin kuin tulon tekijöiden korkeimpien termien tulo, niin tulon $g_i x_1^{\lambda_1} x_2^{\lambda_2} \ldots x_n^{\lambda_n}$ korkein termi on sen tekijöiden $p_1^{i_1}, p_2^{i_2}, \ldots, p_n^{i_n}$ korkeimpien termien tulo. Koska

$$\begin{aligned}
&\text{tekijän } p_1^{i_1} \text{ korkein termi on } x_1^{i_1}, \\
&\text{tekijän } p_2^{i_2} \text{ korkein termi on } x_1^{i_2} x_2^{i_2}, \\
&\qquad\qquad \vdots \\
&\text{tekijän } p_n^{i_n} \text{ korkein termi on } x_1^{i_n} x_2^{i_n} \cdots x_n^{i_n},
\end{aligned}$$

niin tulon $g_i p_1^{i_1} p_2^{i_2} \cdots p_n^{i_n}$ korkein termi on $g_i x_1^{i_1+i_2+\cdots+i_n} x_2^{i_2+\cdots+i_n} \cdots x_n^{i_n}$. Jotta tämä

olisi yhtäsuuri termin $g_i x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_n^{\lambda_n}$, saadaan yhtälöryhmä

$$\begin{cases} i_1 + i_2 + \cdots + i_n & = \lambda_1, \\ \quad i_2 + \cdots + i_n & = \lambda_2, \\ \qquad \vdots & \\ \qquad i_n & = \lambda_n. \end{cases}$$

Tästä yhtälöryhmästä saamme

$$i_1 = \lambda_1 - \lambda_2, i_2 = \lambda_2 - \lambda_3, \cdots, i_{n-1} = \lambda_{n-1} - \lambda_n, i_n = \lambda_n.$$

Summan eri termeillä ei voi olla samaa korkeinta jäsentä. Eli koko summan korkein termi esiintyy vain yhdessä summan termissä $g_i x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$. Tämä on kuitenkin mahdotonta, sillä yllä oleva yhtälö ei olisikaan muuttujien $x_1, x_2, \ldots, x_n$ sijoittamisen jälkeen identtisesti nolla.

□

Sovellettaessa edellä esiteltyä keinoa polynomin Q muodostamiseksi voidaan menetellä seuraavaan tapaan. Muodostetaan polynomin P korkeimmasta jäsenestä $a_0 x_1^{k_1'} x_2^{k_2'} \cdots x_n^{k_n'}$ askel askeleelta madaltaen kaikki tulot

$$x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n},$$

joissa

$$\begin{aligned} &k_1 + k_2 + \cdots + k_n = k_1' + k_2' + \cdots + k_n' = t, \\ &k_1 \geq k_2 \geq \cdots \geq k_n \geq 0. \end{aligned}$$

Esimerkiksi, jos x_1^4 on jonkin homogeenisen symmetrisen polynomin korkein jäsen, niin tätä madaltamalla saadaan tulot $x_1^4, x_1^3 x_2, x_1^2 x_2^2, x_1^2 x_2 x_3, x_1 x_2 x_3 x_4$.

Polynomien $P, P_1, P_2, \ldots$ korkeimmat jäsenet ovat nämä tulot varustettuina asianomaisilla kertoimilla. Tämä nähdään myös seuraavassa esimerkissä.

Esimerkki 6. Olkoon n=3 ja $P(x_1, x_2, x_3) = S(x_1^2 x_2) = x_1^2 x_2 + x_1^2 x_3 + x_2^2 x_1 + x_2^2 x_3 + x_3^2 x_1 + x_3^2 x_2$. Tämän polynomin korkein termi on $x_1^2 x_2$.

Muodostetaan edellä mainitulla tavalla korkeimmasta jäsenestä tulot, joiden tulisi olla sopivilla kertoimilla varustettuina polynomien $P, P_1, \ldots$ korkeimmat jäsenet. Nämä ovat $x_1^2 x_2$ ja $x_1 x_2 x_3$.

Peruslauseen todistuksen mukaan

$$\begin{aligned} Q_1 = p_1^{2-1}p_2^{1-0} = p_1p_2 &= (x_1+x_2+x_3)(x_1x_2+x_1x_3+x_2x_3) \\ &= x_1^2x_2 + x_1^2x_3 + x_2^2x_1 + x_2^2x_3 + x_3^2x_1 + x_3^2x_2 + 3x_1x_2x_3 \end{aligned}$$

ja

$$\begin{aligned} P_1 = P - Q_1 =& x_1^2x_2 + x_1^2x_3 + x_2^2x_1 + x_2^2x_3 + x_3^2x_1 + x_3^2x_2 - (x_1^2x_2 + x_1^2x_3 + x_2^2x_1 \\ &+ x_2^2x_3 + x_3^2x_1 + x_3^2x_2 + 3x_1x_2x_3) \\ =& -3x_1x_2x_3. \end{aligned}$$

Tästä nähdään, että polynomin P_1 korkein jäsen on $-3x_1x_2x_3$. Tämä todellakin on polynomin P korkeimmasta jäsenestä madaltamalla saatu tulo varustettuna kertoimella -3.

Polynomi P voidaan nyt esittää symmetristen perusfunktioiden polynomina

$$P = p_1p_2 - 3p_3.$$

Koska $P = Q_1 + Q_2 + \ldots + Q_s$ ja polynomit $Q_1, Q_2, \ldots, Q_s$ muodostettiin polynomien $P, P_1, \ldots$ korkeinten jäsenten avulla, saadaan

$$P = \sum_{\substack{k_1+k_2+\ldots+k_n=t \\ k_1\geq k_2\geq\ldots\geq k_n}} c_k p_1^{k_1-k_2}p_2^{k_2-k_3}\cdots p_{n-1}^{k_{n-1}-k_n}p_n^{k_n}.$$

Kertoimet c_k voidaan määrätä sijoittamalla muuttujien $x_1, x_2, \ldots, x_n$ paikalle sopivia kokonaislukuja ja laskemalla näin saatavista lineaarisista yhtälöistä kertoimien arvot.

Jos $n > t$, niin $k_{t+1} = \cdots = k_n = 0$, joten voidaan kirjoittaa

$$P = \sum_{\substack{k_1+k_2+\ldots+k_n=t \\ k_1\geq k_2\geq\ldots\geq k_n}} c_k p_1^{k_1-k_2}p_2^{k_2-k_3}\cdots p_{t-1}^{k_{t-1}-k_t}p_t^{k_t}.$$

Tällöin voidaan kertoimia c_k määrätessä asettaa $x_{t+1} = \cdots = x_n = 0$. Toisin sanoen, *kun $n > t$, polynomi P voidaan muodostaa ikään kuin $n = t$.*

Esimerkki 7. Lausu symmetristen perusfunktioiden polynomina $P(x_1, x_2, x_3) = S(x_1^3x_2x_3)$.

Ratkaisu. Voidaan olettaa, että $n \geq 5$. Tällöin mahdolliset korkeimmat jäsenet ovat

$$x_1^3 x_2 x_3,\ x_1^2 x_2^2 x_3,\ x_1^2 x_2 x_3 x_4,\ x_1 x_2 x_3 x_4 x_5.$$

Peruslauseen todistuksen perusteella tiedetään, että halutun polynomin $Q(p_1, p_2, \ldots, p_n)$ osasummat $Q_1, Q_2, \ldots$ määräytyvät symmetristen polynomien $P, P_1, P_2, \ldots$ korkeimpien termien mukaan. Siispä korkeimmista jäsenistä saadaan

$$\begin{aligned}
Q_1 &= p_1^{3-1} p_2^{1-1} p_3^{1-0} = p_1^2 p_3, \\
Q_2 &= A p_1^{2-2} p_2^{2-1} p_3^{1-0} = A p_2 p_3, \\
Q_3 &= B p_1^{2-1} p_2^{1-1} p_3^{1-1} p_4^{1-0} = B p_1 p_4 \qquad \text{ja} \\
Q_4 &= C p_1^{1-1} p_2^{1-1} p_3^{1-1} p_4^{1-1} p_5^{1-0} = C p_5.
\end{aligned}$$

Termin Q_1 muodostamisessa on otettu huomioon polynomin P korkeimman jäsenen $x_1^3 x_2 x_3$ kerroin, joka on 1. Näin saadaan

$$P = Q_1 + Q_2 + Q_3 + Q_4 = p_1^2 p_3 + A p_2 p_3 + B p_1 p_4 + C p_5. \tag{a}$$

Polynomi P voidaan muodostaa ikään kuin $n = 5$, sillä kertoimia A, B ja C määrättäessä voidaan sijoittaa $x_6 = x_7 = \ldots = 0$.

Tällöin

$$\begin{aligned}
S(x_1^3 x_2 x_3) =& x_1^3 x_2 x_3 + x_1^3 x_2 x_4 + x_1^3 x_2 x_5 + x_1^3 x_3 x_4 + x_1^3 x_3 x_5 + x_1^3 x_4 x_5 + x_2^3 x_1 x_3 + \\
& x_2^3 x_1 x_4 + x_2^3 x_1 x_5 + x_2^3 x_3 x_4 + x_2^3 x_3 x_5 + x_2^3 x_4 x_5 + x_3^3 x_1 x_2 + x_3^3 x_1 x_4 + \\
& x_3^3 x_1 x_5 + x_3^3 x_2 x_4 + x_3^3 x_2 x_5 + x_3^3 x_4 x_5 + x_4^3 x_1 x_2 + x_4^3 x_1 x_3 + x_4^3 x_1 x_5 + \\
& x_4^3 x_2 x_3 + x_4^3 x_2 x_5 + x_4^3 x_3 x_5 + x_5^3 x_1 x_2 + x_5^3 x_1 x_3 + x_5^3 x_1 x_4 + x_5^3 x_2 x_3 + \\
& x_5^3 x_2 x_4 + x_5^3 x_3 x_4
\end{aligned}$$

ja

$$\begin{aligned}
p_1 =& x_1 + x_2 + x_3 + x_4 + x_5, \\
p_2 =& x_1 x_2 + x_1 x_3 + x_1 x_4 + x_1 x_5 + x_2 x_3 + x_2 x_4 + x_2 x_5 + x_3 x_4 + x_3 x_5 + x_4 x_5, \\
p_3 =& x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_2 x_5 + x_1 x_3 x_4 + x_1 x_3 x_5 + x_1 x_4 x_5 + x_2 x_3 x_4 + \\
& x_2 x_3 x_5 + x_2 x_4 x_5 + x_3 x_4 x_5, \\
p_4 =& x_1 x_2 x_3 x_4 + x_1 x_2 x_3 x_5 + x_1 x_2 x_4 x_5 + x_1 x_3 x_4 x_5 + x_2 x_3 x_4 x_5 \qquad \text{ja} \\
p_5 =& x_1 x_2 x_3 x_4 x_5.
\end{aligned}$$

Kertoimien määräämiseksi

1) sijoitetaan $x_1 = x_2 = x_3 = 1$ ja $x_4 = x_5 = \ldots x_n = 0$.

Tällöin saadaan

$$\begin{aligned} P = S(x_1^3 x_2 x_3) =& x_1^3 x_2 x_3 + x_2^3 x_1 x_3 + x_3^3 x_1 x_2 \\ =& 1 + 1 + 1 = 3, \end{aligned}$$

$$\begin{aligned} p_1 =& x_1 + x_2 + x_3 = 1 + 1 + 1 = 3, \\ p_2 =& x_1 x_2 + x_1 x_3 + x_2 x_3 = 1 + 1 + 1 = 3, \\ p_3 =& x_1 x_2 x_3 = 1 \qquad \text{ja} \\ p_4 =& p_5 = 0. \end{aligned}$$

Näin ollen yhtälöksi (a) saadaan

$$P = 3^2 + 3A = 3,$$

josta saadaan

$$A = -2. \tag{b}$$

2) Sijoitetaan $x_1 = x_2 = x_3 = 1$, $x_4 = x_5 = -1$ ja $x_6 = \cdots = x_n = 0$.

Tällöin on $S = -6$, $p_1 = 1$, $p_2 = -2$, $p_3 = -2$, $p_4 = 1$ ja $p_5 = 1$, joten yhtälöksi (a) saadaan

$$P = -2 + 4A + B + C = -6,$$

johon sijoittamalla (b) saadaan

$$C = -B + 4. \tag{c}$$

3) Sijoitetaan $x_1 = x_2 = x_3 = x_4 = 1$ ja $x_5 = x_6 = \cdots = x_n = 0$.

Tällöin $S = 12$, $p_1 = 4$, $p_2 = 6$, $p_3 = 4$, $p_4 = 1$ ja $p_5 = 0$.

Kun nämä ja yhtälö (b) sijoitetaan yhtälöön (a), saadaan

$$P = 16 \cdot 4 - 12 \cdot 4 + 4B = 12,$$

josta

$$B = -1.$$

Edelleen sijoittamalla $B = -1$ yhtälöön (c) saadaan

$$C = 5.$$

Siispä $S(x_1^3 x_2 x_3)$ voidaan lausua symmetristen perusfunktioiden polynomina seuraavasti:

$$P = p_1^2 p_3 - 2p_2 p_3 - p_1 p_4 + 5p_5.$$

2 Yhtälön juurien symmetriset polynomit

Lause 2. *Jos yhtälön*

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0 \tag{A}$$

juuret ovat $x_1, x_2, \ldots, x_n$*, niin*

$$a_1 = -p_1, a_2 = p_2, a_3 = -p_3, \ldots, a_n = (-1)^n p_n,$$

jossa $p_1, p_2, \ldots, p_n$ *merkitsevät juurien symmetrisiä perusfunktioita.*

Todistus. Jos $x_1, x_2, \ldots, x_n$ ovat yhtälön

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

juuret, niin voidaan kirjoittaa

$$x^n + a_1 x^{n-1} + \cdots + a_n = (x - x_1)(x - x_2) \cdots (x - x_n).$$

Kertomalla sulut auki saadaan yhtälö

$$x^n + a_1 x^{n-1} + \cdots + a_n = x^n - p_1 x^{n-1} + \cdots + (-1)^n p_n,$$

mistä seuraa haluttu tulos.

□

Olkoon $P(x_1, x_2, \ldots, x_n)$ yhtälön (A) juurien symmetrinen polynomi. Tällöin edellisten lauseiden nojalla voidaan kirjoittaa

$$P(x_1, x_2, \ldots, x_n) = Q(p_1, p_2, \ldots, p_n) = Q(-a_1, a_2, \ldots, (-1)^n a_n).$$

Koska Lauseen 1 mukaan polynomin Q kertoimet ovat polynomin P kertoimien määräämässä renkaassa, niin on siis voimassa lauseet:

Lause 3. *Yhtälön* (A) *juurien symmetrinen polynomi P on yhtälön* (A) *ja polynomin P kertoimien määräämän renkaan luku. (Katso perustelut [2, s. 162])*

Lause 4. *Jos yhtälön $a_0x^m + a_1x^{m-1} + \cdots + a_m = 0$, missä $a_0 \neq 0$, juurien symmetrisen polynomin $P(x_1, x_2 \ldots, x_m)$ aste muuttujan x_1 suhteen on t, niin lauseke $a_0^t P$ voidaan lausua yhtälön kertoimien suhteen astetta t olevana homogeenisena polynomina $R(a_0, a_1 \ldots, a_m)$, missä polynomin R kertoimet ovat polynomin P kertoimien määräämän renkaan lukuja.*

Todistus. Tarkastellaan yhtälöä

$$a_0x^m + a_1x^{m-1} + \cdots + a_m = 0. \tag{B}$$

Tämä saadaan yhtälön (A) muotoon jakamalla yhtälön molemmat puolet kertoimella $a_0 \neq 0$:

$$x^m + \frac{a_1}{a_0}x^{m-1} + \cdots + \frac{a_m}{a_0} = 0.$$

Olkoon $P(x_1, x_2, \ldots, x_m)$ nyt juurien symmetrinen polynomi. Peruslauseen (Lause 1) mukaan symmetrinen polynomi $P(x_1, x_2, \ldots, x_n)$ voidaan lausua symmetristen perusfunktioiden polynomina $Q(p_1, p_2, \ldots, p_n)$. Tällöin voidaan kirjoittaa

$P(x_1, x_2, \ldots, x_m) = Q(p_1, p_2, \ldots, p_m) = Q(-\frac{a_1}{a_0}, \frac{a_2}{a_0}, \ldots, (-1)^m\frac{a_m}{a_0})$.

Olkoon polynomin P aste muuttujan x_1 suhteen t. Tällöin Lauseen 1 mukaan myös polynomin Q kokonaisaste muuttujien $\frac{a_1}{a_0}, \frac{a_2}{a_0}, \ldots, \frac{a_m}{a_0}$ suhteen on t. Kun tämä polynomi kerrotaan luvulla a_0^t, luvut a_0 supistuvat pois nimittäjistä ja tulokseksi saadaan kertoimien $a_0, a_1, \ldots, a_m$ polynomi. Koska polynomin Q jokainen jäsen on nollatta astetta näiden suhteen, niin polynomi $a_0^t P$ on näiden kertoimien $a_0, a_1, \ldots, a_m$ t. asteen homogeeninen polynomi. □

3 Resultantti

3.1 Resultantti symmetristen funktioiden avulla

Tutkimme, millä ehdolla kahdella polynomiyhtälöllä

$$A(x) = a_0x^m + a_1x^{m-1} + \cdots + a_m = 0 \qquad (a_0 \neq 0), \tag{1}$$

$$B(x) = b_0x^n + b_1x^{n-1} + \cdots + b_n = 0 \qquad (b_0 \neq 0) \tag{1'}$$

on yhteinen juuri. Olkoot yhtälön (1) juuret $\alpha_1, \alpha_2, \ldots, \alpha_m$ ja yhtälön (1') juuret $\beta_1, \beta_2, \ldots, \beta_n$. Silloin pätee

$$A(x) = a_0(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_m), \tag{2}$$
$$B(x) = b_0(x-\beta_1)(x-\beta_2)\cdots(x-\beta_n). \tag{2'}$$

Tuloa

$$\begin{aligned} R = a_0^n b_0^m &(\alpha_1-\beta_1)(\alpha_1-\beta_2)\cdots(\alpha_1-\beta_n) \\ &(\alpha_2-\beta_1)(\alpha_2-\beta_2)\cdots(\alpha_2-\beta_n) \\ &\vdots \\ &(\alpha_m-\beta_1)(\alpha_m-\beta_2)\cdots(\alpha_m-\beta_n) \end{aligned} \tag{3}$$

kutsutaan yhtälöiden *resultantiksi*. Kohdan (2) avulla havaitaan, että

$$R = a_0^n B(\alpha_1)B(\alpha_2)\cdots B(\alpha_m). \tag{4}$$

Kohdan (2') avulla taas saadaan lauseke

$$R = (-1)^{mn} b_0^m A(\beta_1)A(\beta_2)\cdots A(\beta_n). \tag{4'}$$

Lause 5. *Yhtälöiden* (1) *ja* (1') *resultantti* R *voidaan esittää kertoimien* $a_0, a_1 \ldots, a_m$ *suhteen* n*. asteen ja kertoimien* $b_0, b_1 \ldots, b_n$ m*. asteen homogeenisena polynomina, jonka kertoimet ovat kokonaislukuja. Resultantti* $R = 0$*, jos ja vain jos yhtälöillä on yhteinen juuri.*

Todistus. Ajatellaan $B(x)$ muodossa $B(x) = b_0x^n + b_1x^{n-1} + \cdots + b_n$. Tällöin havaitaan, että tulo

$$\begin{aligned} B(\alpha_1)B(\alpha_2)\cdots B(\alpha_m) =&(b_0\alpha_1^n + b_1\alpha_1^{n-1}\cdots + b_n)(b_0\alpha_2^n + b_1\alpha_2^{n-1}\cdots + b_n) \\ &\cdots(b_0\alpha_m^n + b_1\alpha_m^{n-1}\cdots + b_n), \end{aligned}$$

missä muuttujat $\alpha_1, \alpha_2, \ldots, \alpha_m$ ovat polynomin

$$A(x) = a_0x^m + a_1x^{m-1} + \cdots + a_m$$

nollakohdat, on kertoimien $b_0, b_1, \ldots, b_n$ suhteen homogeeninen m. asteen polynomi.

Kun tulot $B(\alpha_1)B(\alpha_2)\cdots B(\alpha_m)$ esitetään muuttujien $b_1, b_2, \ldots, b_n$ polynomina, kertoimet ovat yhtälön (1) juurien α_1, α_2, ..., α_m kokonaislukukertoimisia symmetrisiä polynomeja, joiden asteet muuttujan α_1 suhteen ovat korkeintaan n.

Edellä olevaa lauseketta selventää seuraava esimerkki, jossa $n = 3$ ja $m = 2$. Tällöin

$$\begin{aligned}
B(\alpha_1)B(\alpha_2) =&(b_0\alpha_1^3 + b_1\alpha_1^2 + b_2\alpha_1 + b_3)(b_0\alpha_2^3 + b_1\alpha_2^2 + b_2\alpha_2 + b_3)\\
=&b_0^2(\alpha_1^3\alpha_2^3) + b_0b_1(\alpha_1^3\alpha_2^2 + \alpha_2^3\alpha_1^2) + b_0b_2(\alpha_1^3\alpha_2 + \alpha_2^3\alpha_1) + b_0b_3(\alpha_1^3 + \alpha_2^3)\\
&+ b_1^2(\alpha_1^2\alpha_2^2) + b_1b_2(\alpha_1^2\alpha_2 + \alpha_2^2\alpha_1) + b_1b_3(\alpha_1^2 + \alpha_2^2) + b_2^2(\alpha_1\alpha_2)\\
&+ b_2b_3(\alpha_1 + \alpha_2) + b_3^2\\
=&b_0^2S(\alpha_1^3\alpha_2^3) + b_0b_1S(\alpha_1^3\alpha_2^2) + b_0b_2S(\alpha_1^3\alpha_2) + b_0b_3S(\alpha_1^3) + b_1^2S(\alpha_1^2\alpha_2^2)\\
&+ b_1b_2S(\alpha_1^2\alpha_2) + b_1b_3S(\alpha_1^2) + b_2^2S(\alpha_1\alpha_2) + b_2b_3S(\alpha_1) + b_3^2.
\end{aligned}$$

Tämä polynomi on kertoimien b_0, b_1, b_2 suhteen homogeeninen ja sen aste näiden suhteen on $m = 2$. Lisäksi tulon $B(\alpha_1)B(\alpha_2)$ kertoimet ovat muuttujien α_1 ja α_2 suhteen kokonaislukukertoimisia homogeenisia symmetrisiä polynomeja, joiden asteet muuttujan α_1 suhteen ovat pienempiä tai yhtäsuuria kuin $n = 3$.

Koska tulon $B(\alpha_1)B(\alpha_2)\cdots B(\alpha_m)$ kertoimet ovat juurien α_1, α_2, ..., α_m symmetrisiä polynomeja, ne voidaan lausua Lauseen 1 mukaan symmetristen perusfunktioiden polynomeina, ja edelleen lauseen 4 mukaan yhtälön (1) kertoimien $a_0, a_1, \ldots, a_m$ polynomeina. Kun nämä polynomit kerrotaan yhtälössä (4) esiintyvällä tekijällä a_0^n, niin saadut tulot ovat kertoimien $a_0, a_1, \ldots, a_m$ homogeenisia n. asteen polynomeja, joiden kertoimet ovat kokonaislukuja. Resultantin muodosta näkyy, että $R = 0$, jos ja vain jos yhtälöillä (2) ja (2') on yhteinen juuri.

□

Esimerkki 8. Olkoot

$$A(x) = a_0x^2 + a_1x + a_2 = 0, \tag{5}$$

$$B(x) = b_0x^2 + b_1x + b_2 = 0. \tag{5'}$$

Muodostetaan näiden kahden toisen asteen yhtälöin resultantti käyttämällä hyväksi resultantin R esitysmuotoa (4):

$$\begin{aligned}
R &= a_0^2B(\alpha_1)B(\alpha_2)\\
&= a_0^2(b_0\alpha_1^2 + b_1\alpha_1 + b_2)(b_0\alpha_2^2 + b_1\alpha_2 + b_2)\\
&= a_0^2[b_0^2\alpha_1^2\alpha_2^2 + b_0b_1\alpha_1\alpha_2(\alpha_1 + \alpha_2) + b_0b_2(\alpha_1^2 + \alpha_2^2) + b_1^2\alpha_1\alpha_2 + b_1b_2(\alpha_1 + \alpha_2) + b_2^2].
\end{aligned}$$

Lauseen 2 mukaisesti saadaan

$$\frac{a_1}{a_0} = -p_1 = -(\alpha_1 + \alpha_2) \qquad ja \qquad \frac{a_2}{a_0} = p_2 = \alpha_1\alpha_2.$$

Täten voidaan sijoittaa

$$\alpha_1 + \alpha_2 = -\frac{a_1}{a_0} \qquad ja \qquad \alpha_1\alpha_2 = \frac{a_2}{a_0},$$

ja saadaan

$$R = b_0^2 a_2^0 - b_0 b_1 a_1 a_2 + b_0 b_2 (a_1^2 - 2a_0 a_2) + b_1^2 a_0 a_2 - b_1 b_2 a_0 a_1 + b_2^2 a_0^2.$$

Tämä voidaan saattaa muotoon

$$R = (a_0 b_2 - a_2 b_0)^2 - (a_1 b_2 - a_2 b_1)(a_0 b_1 - a_1 b_0). \tag{6}$$

3.2 Resultantti determinantin avulla

Johdamme nyt resultantin käyttämällä symmetristen funktioiden sijasta determinanttia apuna. Oletetaan, että yhtälöillä (1) ja (1') on yhteinen juuri γ. Tällöin voidaan kirjoittaa

$$A(x) = a_0(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_m) = (x - \gamma)A_1(x), (*)$$
$$B(x) = -b_0(x - \beta_1)(x - \beta_2)\cdots(x - \beta_n) = -(x - \gamma)B_1(x), (**)$$

missä

$$A_1(x) = u_0 x^{m-1} + u_1 x^{m-2} + \cdots + u_{m-1},$$
$$B_1(x) = v_0 x^{n-1} + v_1 x^{n-2} + \cdots + v_{n-1},$$

ja kertoimet $u_0, \ldots, u_{m-1}, v_0 \ldots, v_{n-1}$ ovat vakioita. Edellisistä yhtälöistä seuraa identiteetti

$$A(x)B_1(x) + B(x)A_1(x) = 0. \tag{6}$$

Tehdään sijoitukset tähän yhtälöön sijoittamalla $A(x)$ ja $B(x)$ yhtälöiden (1) ja (1') muodossa sekä suoritetaan kertomiset yhtälön vasemmalla puolella:

$$\begin{aligned}A(x)B_1(x)+B(x)A_1(x) =&(a_0x^m+a_1x^{m-1}+\cdots+a_m)(v_0x^{n-1}+v_1x^{n-2}+\cdots+v_{n-1})+\\ &(b_0x^n+b_1x^{n-1}+\cdots+b_n)(u_0x^{m-1}+u_1x^{m-2}+\cdots+u_{m-1})\\ =&(a_0v_0+b_0u_0)x^{m+n-1}+(a_1v_0+a_0v_1+b_1u_0+b_0u_1)x^{m+n-2}+\\ &(a_2v_0+a_1v_1+a_0v_2+b_2u_0+b_1u_1+b_0u_2)x^{m+n-3}+\\ &\cdots+(a_mv_{n-2}+a_{m-1}v_{n-1}+b_nu_{m-2}+b_{n-1}u_{m-1})x+\\ &(a_mv_{n-1}+b_nu_{m-1})\\ =&0.\end{aligned}$$

Jotta edellinen yhtälö pätisi identtisesti, on kunkin muuttujan x potenssin kertoimen oltava 0. Saadaan seuraava yhtälöryhmä, jonka avulla voidaan määrätä kertoimet $u_0,\ldots,u_{m-1},v_0\ldots,v_{n-1}$:

$$\begin{cases} a_0v_0 & +b_0u_0 & =0,\\ a_1v_0+a_0v_1 & +b_1u_0+b_0u_1 & =0,\\ a_2v_0+a_1v_1+a_0v_2 & +b_2u_0+b_1u_1+b_0u_2 & =0,\\ \cdots\cdots\cdots\cdots\cdots\cdots, & & \\ a_mv_{n-2}+a_{m-1}v_{n-1} & +b_nu_{m-2}+b_{n-1}u_{m-1} & =0,\\ a_mv_{n-1} & +b_nu_{m-1} & =0. \end{cases} \tag{8}$$

Yhtälöryhmä voidaan ilmaista matriisien avulla:

$$\begin{bmatrix} a_0 & & & & b_0 & & & \\ a_1 & a_0 & & & b_1 & b_0 & & \\ a_2 & a_1 & a_0 & & b_2 & b_1 & b_0 & \\ \vdots & & & & \vdots & & & \\ & & & a_m & & & & b_n \end{bmatrix} \begin{bmatrix} v_0 \\ \vdots \\ v_{n-1} \\ u_0 \\ \vdots \\ u_{m-1} \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ \vdots \\ \vdots \\ 0 \end{bmatrix}.$$

Muodostetaan tämän yhtälöryhmän kerroinmatriisin determinantti D. Osoitetaan, että determinantti $D=0$, jos ja vain jos yhtälöillä (1) ja (1') on yhteinen juuri. Eli tällöin on osoitettu determinantilla D olevan resultantin R ominaisuus. Jotta determinantti voidaan todeta olevan täsmälleen sama kuin resultantti R, muodostamme kahdella eri tavalla tulon $a_0^nb_0^mDM$, missä M on kokoa $(m+n)\times(m+n)$ oleva Vandermonden determinantti. Vertaamalla näitä kahta saatua tuloa $a_0^nb_0^mDM$ voidaan lopulta todeta determimantin D olevan juuri sama kuin yhtälöistä (1) ja (1') muodostettu resultantti $R(A,B)$.
Kirjoitetaan determinantin D pystyrivit vaakariveiksi ja vaakarivit pystyriveiksi. Näin voidaan tehdä, sillä determinantin arvo ei muutu tässä toimeenpiteessä. Siispä saadaan

$$D = \begin{vmatrix} a_0 & a_1 & \cdots\cdots & a_m & & \\ & a_0 & a_1 & \cdots\cdots & a_m & \\ & & \cdots\cdots\cdots & & & \\ & & a_0 & a_1 & \cdots\cdots & a_m \\ b_0 & b_1 & \cdots\cdots & b_n & & \\ & b_0 & b_1 & \cdots\cdots & b_n & \\ & & \cdots\cdots\cdots & & & \\ & & b_0 & b_1 & \cdots\cdots & b_n \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \text{ riviä} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m \text{ riviä} \end{matrix}. \tag{9}$$

Tässä homogeenisten lineaaristen yhtälöiden yhtälöryhmässä on sekä yhtälöiden että tuntemattomien lukumäärä $m+n$. Lisäksi yhtälöryhmällä on juuret, jotka kaikki eivät ole nollia. Nyt tarvisemme seuraavaa apulausetta:

Lemma 6. *Jos homogeenisessa lineaarisessa yhtälöryhmässä on yhtälöitä yhtä monta kuin tuntemattomia, niin yhtälöryhmän determinantin häviäminen on välttämätön ja riittävä ehto, jotta yhtälöryhmällä olisi muitakin ratkaisuja kuin triviaali ratkaisu.*

Todistus. Kts. [2, s. 132]. □

Tämän lauseen nojalla on todistettu, että $D = 0$.

Oletamme nyt kääntäen, että $D = 0$. Silloin edellä mainitun Lemman 1 mukaan yhtälöryhmällä (8) on juuret $u_0, \ldots, u_{m-1}, v_0 \ldots, v_{n-1}$, jotka eivät kaikki ole nollia. Identtisyys (6) voidaan kirjoittaa muotoon

$$A(x)B_1(x) = -B(x)A_1(x).$$

Tässä emme oleta, että polynomit $A_1(x)$ ja $B_1(x)$ olisivat samat kuin kaavoissa (*) ja (**). Eli nämä polynomit on muodostettu vastaavalla tavalla kuin kyseisessä kohdassa, mutta ne saattavat sisältää yhteisen juuren.

Ajattelemme molemmat puolet jaetuiksi nollakohtiensa avulla lineaarisiin tekijöihin eli

$$a_0(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_m)B_1(x) = -B(x)u_0(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{m-1}).$$

Koska polynomin $A(x)$ aste m on suurempi kuin polynomin $A_1(x)$ aste $m-1$, niin ainakin yksi polynomin $A(x)$ lineaarisista tekijöistä on polynomin $B(x)$ tekijä. Tämä nähdään, kun jaetaan yhtälön molemmat puolet tulolla $-u_0(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{m-1})$, jolloin saadaan yhtälö

$$B(x) = -\frac{a_0}{u_0}(x-\alpha_m)B_1(x).$$

Täten yhtälöillä (1) ja (1') on yhteinen juuri.

Näin olemme todistaneet, että determinantilla D on Lauseessa 5 esitetty resultantin R ominaisuus.

Osoitamme nyt, että determinantti D on identtinen resultantin R kanssa. Todistaaksemme väitteen muodostamme kahdella tavalla tulon $a_0^n b_0^m DM$, missä M on kokoa $(m+n) \times (m+n)$ oleva Vandermonden determinantti

$$M = \begin{vmatrix} \beta_1^{m+n-1} & \beta_2^{m+n-1} & \cdots & \beta_n^{m+n-1} & \alpha_1^{m+n-1} & \alpha_2^{m+n-1} & \cdots & \alpha_m^{m+n-1} \\ \beta_1^{m+n-2} & \beta_2^{m+n-2} & \cdots & \beta_n^{m+n-2} & \alpha_1^{m+n-2} & \alpha_2^{m+n-2} & \cdots & \alpha_m^{m+n-2} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ \beta_1^2 & \beta_2^2 & \cdots & \beta_n^2 & \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_m^2 \\ \beta_1 & \beta_2 & \cdots & \beta_n & \alpha_1 & \alpha_2 & \cdots & \alpha_m \\ 1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 \end{vmatrix}.$$

Determinantti M voidaan Vandermonden determinanttina kirjoittaa sen toiseksi viimeisen rivin alkioiden erotusten tulona. Tulontekijöinä ovat kaikki erotukset, jotka saadaan vähennettäessä kukin alkio edeltävistä alkioistaan. Niinpä

$$M = \prod_{1 \le i < j \le n} (\beta_i - \beta_j) \cdot \prod_{j=1}^{n} \prod_{i=1}^{m} (\beta_j - \alpha_i) \cdot \prod_{1 \le i < j \le m} (\alpha_i - \alpha_j).$$

Merkitään aiemmin esiintynyttä resultantin lauseketta (3) symbolilla $R(A, B)$, jolloin

$$\begin{aligned} R(B, A) = a_0^n b_0^m &(\beta_1 - \alpha_1)(\beta_1 - \alpha_2) \cdots (\beta_1 - \alpha_m) \\ &(\beta_2 - \alpha_1))(\beta_2 - \alpha_2) \cdots (\beta_2 - \alpha_m) \\ &\vdots \\ &(\beta_n - \alpha_1)(\beta_n - \alpha_2) \cdots (\beta_n - \alpha_m) = a_0^n b_0^m \prod_{j=1}^{n} \prod_{i=1}^{m} (\beta_j - \alpha_i). \end{aligned} \tag{10}$$

Täten saadaan yhtälö

$$\begin{aligned} a_0^n b_0^m DM &= D \cdot a_0^n b_0^m \prod_{j=1}^{n} \prod_{i=1}^{m} (\beta_j - \alpha_i) \cdot \prod_{1 \le i < j \le n} (\beta_i - \beta_j) \cdot \prod_{1 \le i < j \le m} (\alpha_i - \alpha_j) \\ &= D \cdot R(B, A) \cdot \prod_{1 \le i < j \le n} (\beta_i - \beta_j) \cdot \prod_{1 \le i < j \le m} (\alpha_i - \alpha_j). \end{aligned} \tag{11}$$

Muodostetaan nyt toisella tavalla tulo $a_0^n b_0^m DM$. Yleisesti pätee, että tulon determinantti on determinanttien tulo. Toisin sanoen $det(DM) = det(D)det(M)$. Siispä matriisitulon DM determinantti voidaan laskea matriisien D ja M determinanttien kertolaskuna, ja on seuraavanlainen

$$DM = \begin{vmatrix} \beta_1^{n-1}A(\beta_1) & \beta_2^{n-1}A(\beta_2) & \cdots & \beta_n^{n-1}A(\beta_n) & 0 & 0 & \cdots & 0 \\ \beta_1^{n-2}A(\beta_1) & \beta_2^{n-2}A(\beta_2) & \cdots & \beta_n^{n-2}A(\beta_n) & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ \beta_1 A(\beta_1) & \beta_2 A(\beta_2) & \cdots & \beta_n A(\beta_n) & 0 & 0 & \cdots & 0 \\ A(\beta_1) & A(\beta_2) & \cdots & A(\beta_n) & 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & \alpha_1^{m-1}B(\alpha_1) & \alpha_2^{m-1}B(\alpha_2) & \cdots & \alpha_m^{m-1}B(\alpha_m) \\ 0 & 0 & \cdots & 0 & \alpha_1^{m-2}B(\alpha_1) & \alpha_2^{m-2}B(\alpha_2) & \cdots & \alpha_m^{m-2}B(\alpha_m) \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & \alpha_1 B(\alpha_1) & \alpha_2 B(\alpha_2) & \cdots & \alpha_m B(\alpha_m) \\ 0 & 0 & \cdots & 0 & B(\alpha_1) & B(\alpha_2) & \cdots & B(\alpha_m) \end{vmatrix}.$$

Determinantin DM alkio, joka sijaitsee ensimmäisen sarakkeen ylimmällä rivillä, on laskettu noudattaen determinanttien kertolaskusääntöä, ja näyttää tältä:

$a_0 \cdot \beta_1^{m+n-1} + a_1 \cdot \beta_1^{m+n-2} + a_2 \cdot \beta_1^{m+n-3} + \cdots + a_m \cdot \beta_1^{m+n-(m+1)} + 0 \cdot \beta_1^{m+n-(m+2)} +$
$\cdots + 0 \cdot \beta_1^{m+n-(m+n)}$
$= \beta_1^{n-1} \cdot (a_0\beta_1^m + a_1\beta_1^{m-1} + \cdots + a_m)$
$= \beta_1^{n-1}A(\beta_1).$

Toisen sarakkeen ylimmällä rivillä sijaitseva alkio on muodostettu kertomalla determinantin D ylin rivi ja determinantin M toinen sarake keskenään:

$a_0 \cdot \beta_2^{m+n-1} + a_1 \cdot \beta_2^{m+n-2} + a_2 \cdot \beta_2^{m+n-3} + \cdots + a_m \cdot \beta_2^{m+n-(m+1)} + 0 \cdot \beta_2^{m+n-(m+2)} +$
$\cdots + 0 \cdot \beta_2^{m+n-(m+n)}$
$= \beta_2^{n-1} \cdot (a_0\beta_2^m + a_1\beta_2^{m-1} + \cdots + a_m)$
$= \beta_2^{n-1}A(\beta_2).$

Ensimmäisen rivin $(n+1)$. alkio on laskettu vastaavasti näin:

$a_0 \cdot \alpha_1^{m+n-1} + a_1 \cdot \alpha_1^{m+n-2} + \cdots + a_m \cdot \alpha_1^{m+n-(m+1)}$
$= \alpha_1^{n-1} \cdot (a_0\alpha_1^m + a_1\alpha_1^{m-1} + \cdots + a_m)$
$= \alpha_1^{n-1}A(\alpha_1)$

Koska polynomi $A(\alpha_1)$ voidaan jakaa nollakohtiensa avulla lineaarisiin tekijöihin, se tulee muotoon $\alpha_0(\alpha_1 - \alpha_1)(\alpha_1 - \alpha_2)\cdots(\alpha_1 - \alpha_n)$.

Tästä selvästi nähdään, että toinen tulontekijöistä $(\alpha_1 - \alpha_1)$ on nolla, joten myös $\alpha_1^{n-1}A(\alpha_1) = 0$.

Ensimmäisen rivin $(n+2)$ alkio on myös nolla, sillä sen lauseke on muotoa $\alpha_2^{n-1}A(\alpha_2)$, jolloin polynomin $A(\alpha_2)$ kolmas tekijä on nolla, kun $A(\alpha_2)$ on jaettu

lineaarisiin tekijöihin nollakohtiensa avulla kuten edellä. Myös loput matriisitulossa DM esiintyvät nollat voidaan perustella vastaavalla tavalla.

Sovelletaan Laplacen teoreemaa, ja otetaan nyt determinantin DM sarakkaiden yhteiset tekijät $A(\beta_1), A(\beta_2), \cdots, A(\beta_n)$ sekä $B(\alpha_1), B(\alpha_2), \cdots, B(\alpha_m)$ determinantin eteen kertoimiksi ja jäljellä oleva determinantti lasketaan Vandermonden determinanttina. Saadaan yhtälö

$$a_0^n b_0^m DM = a_0^n b_0^m \prod_{j=1}^{n} A(\beta_j) \cdot \prod_{1 \le i < j \le n} (\beta_i - \beta_j) \cdot \prod_{i=1}^{n} B(\alpha_i) \cdot \prod_{1 \le i < j \le m} (\alpha_i - \alpha_j). \quad (12)$$

Yhtälö (10) voidaan kirjoittaa myös muotoon

$$R(B, A) = a_0^n b_0^m \prod_{j=1}^{n} \prod_{i=1}^{m} (\beta_j - \alpha_i) = b_0^m \prod_{j=1}^{n} A(\beta_j)$$

ja samoin yhtälö (3) muotoon

$$R(A, B) = a_0^n b_0^m \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j) = a_0^n \prod_{i=1}^{m} B(\alpha_i).$$

Sijoittamalla nämä yhtälöön (12) saadaan

$$a_0^n b_0^m DM = R(A, B) \cdot R(B, A) \prod_{1 \le i < j \le n} (\beta_i - \beta_j) \cdot \prod_{1 \le i < j \le m} (\alpha_i - \alpha_j) \quad (13)$$

Vertaamalla keskenään yhtälöitä (11) ja (13) saadaan tulos $D = R(A, B)$.

Esimerkki 9. Millä arvolla k yhtälöillä $3x^2 - kx - 6 = 0$ ja $6x^2 + kx + 2 = 0$ on yhteinen juuri? Määrää juurien yhteiset arvot.

Ratkaisu.

Symmetristen funktioiden avulla muodostetun resultantin (kts. yhtälö 3) muodosta nähdään, että jos yhtälöillä on jokin yhteinen juuri, niin juurien sijoittamisen jälkeen jokin tulontekijöistä on nolla. Tällöin myös resultantin arvo on nolla. Siispä resultantti $R = 0$, jos ja vain jos yhtälöillä on yhteinen juuri.

Ratkaistaan tehtävä käyttäen näistä yhtälöistä saadun yhtälöryhmän determinantista muodostettua resultanttia. Perustelut yhtäsuuruudelle $R = D$ on esitetty Luvussa 3.2.

Muodostetaan aluksi yhtälöistä yhtälöryhmä $\begin{cases} 3x^2 & -kx & -6 & = 0 \\ 6x^2 & +kx & +2 & = 0 \end{cases}$

Determinantin (9) mukaisesti voidaan kirjoittaa

$$D = R = \begin{vmatrix} 3 & -k & -6 & 0 \\ 0 & 3 & -k & -6 \\ 6 & k & 2 & 0 \\ 0 & 6 & k & 2 \end{vmatrix}.$$

Kehitetään tämä determinantti ensimmäisen pystyrivin mukaan, jolloin

$$R = 3 \begin{vmatrix} 3 & -k & -6 \\ k & 2 & 0 \\ 6 & k & 2 \end{vmatrix} + 6 \begin{vmatrix} -k & -6 & 0 \\ 3 & -k & -6 \\ 6 & k & 2 \end{vmatrix}.$$

Kun näin saaduista kolmirivisistä determinanteista ensimmäinen kehitetään keskimmäisen vaakarivin mukaan ja jälkimmäinen determinantti ylimmän vaakarivin mukaan, saadaan

$$R = 3(-k) \begin{vmatrix} -k & -6 \\ k & 2 \end{vmatrix} + 3 \cdot 2 \begin{vmatrix} 3 & -6 \\ 6 & 2 \end{vmatrix} + 6 \cdot (-k) \begin{vmatrix} -k & -6 \\ k & 2 \end{vmatrix} - 6 \cdot (-6) \begin{vmatrix} 3 & -6 \\ 6 & 2 \end{vmatrix}$$

$$\begin{aligned} &= (-3 \cdot k - 6 \cdot k) \begin{vmatrix} -k & -6 \\ k & 2 \end{vmatrix} + (3 \cdot 2 - (-6 \cdot 6)) \begin{vmatrix} 3 & -6 \\ 6 & 2 \end{vmatrix} \\ &= -9k \cdot (-2k - (-6k)) + (6 + 36)(6 - (-36)) \\ &= -36k^2 + 42. \end{aligned}$$

Koska $R = D = 0$, saadaan

$$\begin{aligned} D = -36k^2 + 42 &= 0 \\ \Leftrightarrow k &= \pm 7 \end{aligned}$$

Kun ratkaistaan
$f(x) = 0$ arvolla $k = 7$, saadaan $x = 3$ tai $x = -2/3$, ja
$g(x) = 0$ arvolla $k = 7$, saadaan $x = -1/2$ tai $x = -2/3$.

Näin ollen yhteinen juuri arvolla $k = 7$ on $x = -2/3$.

Kun ratkaistaan
$f(x) = 0$ arvolla $k = -7$, saadaan $x = 2/3$ tai $x = 1/2$, ja
$g(x) = 0$ arvolla $k = -7$, saadaan $x = -3$ tai $x = 2/3$.

Joten yhteinen juuri arvolla $k = -7$ on $x = 2/3$.

Vastaus: Yhtälöillä on olemassa yhteiset juuret, jos ja vain jos $k = \pm 7$. Tällöin yhteiset juuret ovat $x = \mp 2/3$.

Jos kyseessä on homogeeninen lineaarinen yhtälöryhmä, jossa yhtälöiden määrä on yhtä pienempi kuin tuntemattomien määrä, on helpompi tapa ratkaista tehtävä löytämällä resultantti ja samalla mahdollinen yhteinen juuri seuraavan lauseen (Lause 7) avulla.

Lause 7. *Jos $D', D'', \ldots$ merkitsevät niitä yhtälöryhmän* (15) *matriisin $(n-1)$-rivisiä determinantteja, jotka saadaan pyyhkimällä matriisista pois vuorotellen ensimmäinen, toinen,... pystyrivi, ja jos nämä determinantit eivät kaikki häviä, niin yhtälöryhmä määrää tuntemattomien x_1, x_2, ... , x_n suhteet seuraavasti*

$$x_1 : x_2 : \cdots : x_n = D' : -D'' : \cdots : (-1)^{(n-1)} D^{(n)}$$

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n & = 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n & = 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots & \\ a_{n-1,1}x_1 + a_{n-1,2}x_2 + \cdots + a_{n-1,n}x_n & = 0 \end{cases} \tag{15}$$

Esimerkiksi muuttujien x, y ja z yhtälöryhmä

$$\begin{cases} a_0 x & + a_1 y & + a_2 z & = 0 \\ b_0 x & + b_1 y & + b_2 z & = 0 \end{cases}$$

määrää suhteet

$$x : y : z = \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} : (-1) \begin{vmatrix} a_0 & a_2 \\ b_0 & b_2 \end{vmatrix} : \begin{vmatrix} a_0 & a_1 \\ b_0 & b_1 \end{vmatrix}.$$

Se, että tällä tavoin menettelemällä saadaan selville yhtälöiden resultantti näkyy parhaiten ottamalla esimerkkitapaukseksi yhtälöryhmä

$$\begin{cases} a_0 x^2 & + a_1 x & + a_2 & = 0 \\ b_0 x^2 & + b_1 x & + b_2 & = 0, \end{cases}$$

jossa tuntemattomien paikalla ovat muuttujat x^2, x ja luku 1.
Yhtälöryhmän matriisi on

$$\begin{vmatrix} a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 \end{vmatrix}.$$

Nyt muuttujien x^2, x ja 1 suhteet määräävät suhteen determinanteille, jotka on saatu pyyhkimällä vuorotellen pois matriisista ensimmäinen, toinen ja kolmas pystyrivi

$$x^2 : x : 1 = \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} : (-1) \begin{vmatrix} a_0 & a_2 \\ b_0 & b_2 \end{vmatrix} : \begin{vmatrix} a_0 & a_1 \\ b_0 & b_1 \end{vmatrix}.$$

Tästä saadaan

$$x = \frac{x^2}{x} = (-1) \frac{\begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix}}{\begin{vmatrix} a_0 & a_2 \\ b_0 & b_2 \end{vmatrix}}.$$

Ja toisaalta saadaan

$$x = \frac{x}{1} = (-1) \frac{\begin{vmatrix} a_0 & a_2 \\ b_0 & b_2 \end{vmatrix}}{\begin{vmatrix} a_0 & a_1 \\ b_0 & b_1 \end{vmatrix}}.$$

Näistä voidaan tehdä verranto

$$\begin{vmatrix} a_0 & a_2 \\ b_0 & b_2 \end{vmatrix}^2 = \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} \begin{vmatrix} a_0 & a_1 \\ b_0 & b_1 \end{vmatrix}.$$

$\Leftrightarrow (a_0b_2 - a_2b_0)^2 = (a_1b_2 - a_2b_1)(a_0b_1 - a_1b_0)$
$\Leftrightarrow (a_0b_2 - a_2b_0)^2 - (a_1b_2 - a_2b_1)(a_0b_1 - a_1b_0) = 0$

Tämä on juuri sama lauseke, joka Esimerkissä 8 saatiin kyseisen yhtälöryhmän resultantin esitysmuodoksi.

Esimerkki 10. Lasketaan nyt Esimerkki 9 äsken esitetyn tuloksen avulla. Yhtälöistä $3x^2 - kx - 6 = 0$ ja $6x^2 + kx + 2 = 0$ muodostetun yhtälöryhmän kerroinmatriisin determinantti on siis

$$\begin{vmatrix} 3 & -k & -6 \\ 6 & k & 2 \end{vmatrix}.$$

Tästä saadaan suhteet

$$x^2 : x : 1 = \begin{vmatrix} -k & -6 \\ k & 2 \end{vmatrix} : (-1) \begin{vmatrix} 3 & -6 \\ 6 & 2 \end{vmatrix} : \begin{vmatrix} 3 & -k \\ 6 & k \end{vmatrix}.$$

Tästä saadaan

$$x = \frac{x^2}{x} = (-1) \frac{\begin{vmatrix} -k & -6 \\ k & 2 \end{vmatrix}}{\begin{vmatrix} 3 & -6 \\ 6 & 2 \end{vmatrix}}.$$

Toisaalta saadaan

$$x = \frac{x}{1} = (-1)\frac{\begin{vmatrix} 3 & -6 \\ 6 & 2 \end{vmatrix}}{\begin{vmatrix} 3 & -k \\ 6 & k \end{vmatrix}}.$$

Näistä voidaan tehdä verranto

$$\begin{vmatrix} 3 & -6 \\ 6 & 2 \end{vmatrix}^2 = \begin{vmatrix} -k & -6 \\ k & 2 \end{vmatrix} \begin{vmatrix} 3 & -k \\ 6 & k \end{vmatrix}$$

$\Leftrightarrow (3 \cdot 2 - (-6) \cdot 6)^2 = ((-k) \cdot 2 - (-6) \cdot k)(3k - (-k)6)$
$\Leftrightarrow 42^2 = -4k \cdot 9k$
$\Leftrightarrow 42^2 = -36k^2$
$\Leftrightarrow k = \pm\sqrt{\frac{42^2}{36}} = \pm 7.$
Yhtälöillä $3x^2 - kx - 6 = 0$ ja $6x^2 + kx + 2 = 0$ on siis yhteinen juuri, jos ja vain jos $k = \pm 7$.

Lasketaan vielä nämä yhteiset nollakohdat sijoittamalla vuorotellen saadut kertoimen k arvot muuttujan x lausekkeeseen

$$x = -\frac{\begin{vmatrix} 3 & -6 \\ 6 & 2 \end{vmatrix}}{\begin{vmatrix} 3 & -k \\ 6 & k \end{vmatrix}} = -\frac{-2k+6k}{6+36} = -\frac{4k}{42}.$$

Sijoittamalla tähän $k = 7$ saadaan

$x = -\frac{4 \cdot 7}{42} = -\frac{2}{3}$,

ja sijoittamalla $k = -7$ saadaan
$x = -\frac{4 \cdot (-7)}{42} = \frac{2}{3}$.

3.3 Muuttujan eliminoiminen resultantin avulla

Yksi resultantin mahtavimpia ominaisuuksia on käyttää sitä ratkaistaessa yhteistä nollakohtaa yhtälöryhmän polynomeille, jotka ovat kahden toisistaan riippumattoman muuttujan polynomeja. Tämä tapahtuu eliminoimalla resultantin avulla toinen muuttujista. Jos toisistaan riippumattomia muuttujia on enemmän kuin kaksi, voidaan resultanttia hyödyntää, kunhan ensin eliminoidaan muuttujia muilla keinoin.

Tätä keinoa on tässä työssä käytettykin jo esimerkissä 9. Tarkastellaan prosessia vielä hieman yleisessä muodossa.

Kahden muuttuujan x ja y polynomiyhtälöryhmä voidaan aina saattaa muotoon

$$\begin{cases} A(x,y) &= a_0(y)x^m + a_1(y)x^{m-1} + \cdots + a_m(y) = 0, \\ B(x,y) &= b_0(y)x^n + b_1(y)x^{n-1} + \cdots + b_n(y) = 0, \end{cases}$$

jossa $a_0, b_0, \cdots$ ovat muuttujan y polynomeja. Ajatellaan yhtälöryhmän polynomit muuttujan x polynomeina, jolloin niistä determinantin 9 mukaisesti muodostettu resultantti $R(y)$ on muuttujan y polynomi. Resultantin lausekkeessa ei näin ollen esiinny enää muuttujaa x, vaan se on elimoinoitunut. Jotta polynomeilla $A(x,y)$ ja $B(x,y)$ olisi yhteinen juuri, määrätään $R(y) = 0$. Ratkaistaan saatu muuttujan y polynomiyhtälö. Merkitään tämän yhtälön ratkaisua y_0. Koska yhtälöillä $A(x,y) = 0$ ja $B(x,y) = 0$ on yksi tai useampia yhteisiä juuria x, ne voidaan löytää ratkaisemalla polynomiyhtälöt $A(x,y_0) = 0$ ja $B(x,y_0) = 0$ ja etsimällä ne ratkaisut, jotka saadaan molemmista polynomiyhtälöistä.

Esimerkki 11. Yhtälöiden $\begin{cases} yx^2 + 1 = 0, \\ yx^2 + x = 0, \end{cases}$

resultantti on

$$D = R(y) = \begin{vmatrix} y & 0 & 1 & 0 \\ 0 & y & 0 & 1 \\ y & 1 & 0 & 0 \\ 0 & y & 1 & 0 \end{vmatrix} = y \begin{vmatrix} y & 0 & 1 \\ 1 & 0 & 0 \\ y & 1 & 0 \end{vmatrix} + y \begin{vmatrix} 0 & 1 & 0 \\ y & 0 & 1 \\ y & 1 & 0 \end{vmatrix} = y^2 \begin{vmatrix} 0 & 0 \\ 1 & 0 \end{vmatrix} + y \begin{vmatrix} 1 & 0 \\ y & 1 \end{vmatrix}$$

$$= (-y) \begin{vmatrix} y & 1 \\ y & 0 \end{vmatrix} = 0 + y + (-y)(-y) = y^2 + y.$$

Voidaan merkitä $R(y_0) = y_0^2 + y_0 = 0$, jolloin saadaan
$y_0 = 0$ tai $y_0 = -1$.

Ratkaisemalla

$A(x,-1) = 0$ saadaan $x = \pm 1$ ja laskemalla
$B(x,-1) = 0$ saadaan $x = 0$ tai $x = 1$.

Näin ollen polynomeilla $A(x,y)$ ja $B(x,y)$ on yhteinen tekijä, kun $x = 1$ ja $y = -1$.

Ratkaisemalla

$B(x,0) = 0$ saadaan $x = 0$, mutta yhtälö
$A(x,0) = 0$ ei ole ratkeava millään muuuttujan x arvolla.

Näin ollen polynomeilla $A(x,y)$ ja $B(x,y)$ ei ole yhteistä tekijää muuttujan y arvolla 0.

3.3.1 Resultantti RSA-salauksessa

RSA on yksi yleisimmin käytetyistä julkisen avaimen salakirjoitusjärjestelmistä. RSA-salaus perustuu siihen, että salaus tehdään kertomalla kaksi erittäin suurta alkulukua keskenenään, mikä on varsin helppoa, mutta salauksen purkaminen on sen sijaan hyvin vaikeaa ja hidasta, sillä purkaminen tapahtuu jakamalla tämä saatu tulo tekijöihin. RSA on käsiteltynä hyvin seikkaperäisesti Pekka Larjan tekemässä gradussa RSA-salaus ja sen lukuteoreettinen pohja [4].

Seuraavassa esitellään, kuinka resultanttia on voitu hyödyntää todistettaessa RSA-salauksen luotettavuutta. Käydään kuitenkin ensin läpi hieman salauksen matemaattista rakennetta.

Olkoon

$$n = pq,$$

missä valitut erisuuret alkuluvut p ja q ovat hyvin suuria, jotta salauksen purkaminen tulisi vaikeaksi. Salaus voidaan ilmaista kongruenssina

$$ed \equiv 1 \pmod{\Phi(n)},$$

jossa lukua n kutusutaan *kertoimeksi*, lukua e *salauseksponentiksi* ja lukua d *salauksen purkueksponentiksi*. Tässä $mod(\Phi(n)) = mod(\Phi(pq)) = (p-1)(q-1)$, ja lisäksi luku d on valittu siten, että $\text{syt}(d, \Phi(n)) = 1$. Suurin yhteinen tekijä voidaan määrittää Eukleideen algoritmia käyttämällä. Luku e, jolle pätee $1 < e < \Phi(n)$ on saatu myös Eukleideen algoritmin yhtälöketjuista.

Resultantin avulla ollaan kyetty osoittamaan, että RSA-salaus ei ole luotettava, jos purkueksponentti d on pienempi kuin $n^{0,292}$. Aiemmin jo kauan valloilla ollut todisettu tieto oli Wienerin tulos, jonka mukaan RSA-salaus katsotaan epävarmaksi, jos luku d on pienempi kuin $n^{0,25}$. Eli vanhan tiedon mukaisesti luotettavana on saatettu pitää salausta, joka tämän todistuksen myötä onkin osoitettu epävarmaksi.

3.4 Algoritmi resultantille

Seuraava algoritmi ja sen todistus on tehty pohjautuen lähteeseen [5].

Algoritmi 1. Olkoon K rengas. Olkoot A ja B polynomeja, jotka kuuluvat polynomirenkaaseen $K[x]$ sekä niiden termien kertoimet kokonaisalueeseen, jossa on olemassa yksikäsitteinen tekijöihinjako. Käytetään tällaisesta alueesta lyhennettä UFD (Unique Factorization Domain).

1. Tarkoitetaan merkinnällä $cont(A)$ polynomin A kerrointen suurinta yhteistä tekijää, vastaavasti merkinnällä $cont(B)$) polynomin B kerrointen suurinta yhteistä tekijää, ja merkinnöillä $deg(A)$ ja $deg(B)$ polynomien A ja B asteita. Jos $A = 0$ tai $B = 0$, tulos on 0 ja algoritmi päättyy. Muutoin aseta $a \leftarrow cont(A)$, $b \leftarrow cont(B)$, $A \leftarrow A/a$, $B \leftarrow B/b$, $g \leftarrow 1$, $h \leftarrow 1$, $s \leftarrow 1$ ja $t \leftarrow a^{deg(B)-deg(A)}$. Jos polynomin A aste on pienempi kuin polynomin B aste, niin korvaa polynomi A polynomilla B ja toisin päin. Lisäksi, jos polynominen A ja B asteet ovat parittomia lukuja, aseta $s \leftarrow -1$.

2. Aseta $\delta \leftarrow deg(A) - deg(B)$. Jos $deg(A)$ ja $deg(B)$ ovat parittomia lukuja, aseta $s \leftarrow -s$.

3. Olkoon $l(B)$ polynomin B johtavan termin kerroin. Aseta $d \leftarrow l(B)$. Laske kohtien $4 - 6$ mukaan polynomit Q ja R siten, että $d^{\delta+1}A = BQ + R$ ja $deg(R) < deg(B)$.

4. Aseta $R \leftarrow A$, $Q \leftarrow 0$ ja $e \leftarrow \delta + 1$.

5. Jos $deg(R) < deg(B)$, aseta $q \leftarrow d^e$, $Q \leftarrow qQ$, $R \leftarrow qR$, ja näin ollen olet ratkaissut polynomit Q ja R siten, että $d^{\delta+1}A = BQ + R$, missä $deg(R) < deg(B)$. Siirry kohtaan 7. Muutoin siirry kohtaan 6.

6. Aseta $S \leftarrow l(R)x^{deg(R)-deg(B)}$, $Q \leftarrow dQ + S$, $R \leftarrow dR - SB$, $e \leftarrow e - 1$. Siirry kohtaan 5.

7. Aseta $A \leftarrow B$, $B \leftarrow R/gh^{\delta}$.

8. Aseta $g \leftarrow l(A)$, $h \leftarrow h^{1-\delta}g^{\delta}$. Jos $deb(B) > 0$, siirry kohtaan 2. Muutoin aseta $h \leftarrow h^{1-deg(A)}l(B)^{deg(A)}$ ja päätä algoritmi tulostamalla sth.

Esimerkki 12. Laske algoritmin mukaisesti resultantti polynomeille

$$A(x) = x^4 - 2x^2 + 1 \tag{14}$$

ja

$$B(x) = x^3 - 3x^2 - 2x + 6. \tag{15}$$

Polynomin (14) juuret ovat kaksinkertaiset juuret $x = \pm 1$ ja polynomin (15) juuret ovat $x = \pm\sqrt{2}$ ja $x = 3$. Jos polynomeilla olisi yhteinen nollakohta, niin

lauseen 5 mukaan resultantti olisi 0. Mutta, kun näin ei ole, niin lasketaan resultantti noudattaen kohta kohdalta algoritmia sen numerointia mukaillen

1. Asetetaan $a \leftarrow cont(A) = 1$, $b \leftarrow cont(B) = 1$. Merkitään $A = A_{k-1}$, ja asetetaan $A_{k-1} \leftarrow \frac{A_{k-1}}{a} = x^4 - 2x^2 + 1$, $B \leftarrow \frac{B}{b} = x^3 - 3x^2 - 2x + 6$, $g_{k-1} \leftarrow 1$, $h_{k-1} \leftarrow 1$, $s \leftarrow 1$ ja $t \leftarrow a^{deg(B)} b^{deg(A_{k-1})} = 1^3 \cdot 1^4 = 1$.

2. Merkitään $d_k = deg(A_k)$. Asetetaan $\delta_{k-1} = d_{k-1} - d_k = deg(A_{k-1}) - deg(A_k) = 4 - 3 = 1$.

3. Olkoon $l(B)$ polynomin B johtavan termin kerroin. Asetetaan $d \leftarrow l(B)$. Lasketaan kohtien $4-6$ mukaan polynomit Q ja R siten, että $d^{\delta_{k-1}+1} A_{k-1} = BQ + R$ ja $deg(R) < deg(B)$.

4. Asetetaan $R_{k+1} \leftarrow A_{k-1}$, $Q \leftarrow 0$ ja $e \leftarrow \delta_{k-1}+1 = d_{k-1}-d_k+1 = 4-3+1 = 2$.

5. Koska $deg(R_{k+1}) = 4 > deg(B) = 3$, siirrytään kohtaan 6.

6. Asetetaan
   $S \leftarrow l(R_{k+1}) x^{deg(R_{k+1})-deg(B)} = l_{k-1} x^{d_{k-1}-d_k} = 1x^{4-3} = x$,
   $Q \leftarrow dQ + S = 1 \cdot 0 + x = x$,
   $R_{k+1} \leftarrow dR_{k+1} - SB = dA_{k-1} - SA_k = 1 \cdot (x^4 - 2x^2 + 1) - x(x^3 - 3x^2 - 2x + 6) = 3x^3 - 6x + 1$ ja
   $e \leftarrow e - 1 = 2 - 1 = 1$.
   Siirrytään takaisin kohtaan 5.

5. Koska $deg(R_{k+1}) = 3 = deg(B)$, siirrytään kohtaan 6.

6. Asetetaan
   $S \leftarrow l(R_{k+1}) x^{deg(R_{k+1})-deg(B)} = 3x^{3-3} = 3$,
   $Q \leftarrow dQ + S = 1x + 3 = x + 3$,
   $R_{k+1} \leftarrow dR_{k+1} - SB = 1 \cdot (3x^3 - 6x + 1) - 3(x^3 - 3x^2 - 2x + 6) = 9x^2 - 17$ ja
   $e \leftarrow e - 1 = 1 - 1 = 0$.
   Siirrytään takaisin kohtaan 5.

5. Koska $deg(R_{k+1}) = 2 < deg(B) = 3$, asetetaan
   $q \leftarrow d^e = 1^0 = 1$,
   $Q \leftarrow qQ = x + 3$ ja
   $R \leftarrow qR_{k+1} = 9x^2 - 17$.

Ja näin ollen on saatu ratkaistua polynomit Q ja R, ja yhtälöksi $d^{\delta_{k-1}+1}A_{k-1} = BQ+R$ saatiin $1^{4-3+1}(x^4-2x^2+1) = (x^3-3x^2-2x+6)(x+3)+(9x^2-17)$. Nyt voidaan siirtyä kohtaan 7.

7. Asetetaan
$A_k \leftarrow B = x^3 - 3x^2 - 2x + 6$ ja
$B \leftarrow \frac{R_{k+1}}{g_{k-1}^{\delta_{k-1}} g_{k-1}}$.

8. Asetetaan
$g_k \leftarrow l(A_k) = 1$ ja
$h_k \leftarrow h_{k-1}^{1-\delta_{k-1}} g_k^{\delta_{k-1}} = 1^{1-1} \cdot 1^{4-3} = 1$.
Koska $deg(B) = 2 > 0$, niin siirrytään kohtaan 2.

2. Merkitään $d_k = deg(A_k)$. Asetetaan $\delta_k = deg(A_k) - deg(B) = 3 - 2 = 1$.

3. Asetetaan $d \leftarrow l(B) = 9$. Lasketaan kohtien $4-6$ mukaan polynomit Q ja R siten, että $d^{\delta_k+1}A_k = BQ + R$ ja $deg(R) < deg(B)$.

4. Asetetaan
$R_{k+2} \leftarrow A_k = x^3 - 3x^2 - 2x + 6$, $Q \leftarrow 0$ ja $e \leftarrow \delta_k + 1 = 1 + 1 = 2$.

5. Koska $deg(R_{k+2}) = 3 > deg(B) = 2$, siirrytään kohtaan 6.

6. Asetetaan
$S \leftarrow l(R_{k+2})x^{deg(R_{k+2})-deg(B)} = 1x^{3-2} = x$,
$Q \leftarrow dQ + S = 1 \cdot 0 + x = 9 \cdot 0 + x = x$,
$R_{k+2} \leftarrow dR_{k+2} - SB = 9\cdot(x^3-3x^2-2x+6) - x(9x^2-17) = -9\cdot 3x^2 - x + 6\cdot 9$
ja
$e \leftarrow e - 1 = 2 - 1 = 1$.
Siirrytään takaisin kohtaan 5.

5. Koska $deg(R_{k+2}) = 2 = deg(B) = 2$, siirrytään kohtaan 6.

6. Asetetaan
$S \leftarrow l(R_{k+2})x^{deg(R_{k+2})-deg(B)} = -9 \cdot 3x^2x^{2-2} = -9 \cdot 3$,
$Q \leftarrow dQ + S = 9x + (-9 \cdot 3)$,
$R_{k+2} \leftarrow dR_{k+2} - SB = 9(-9\cdot 3x^2 - x + 6\cdot 9) - (-9\cdot 3)(9x^2-17) = -9x + 27$
ja
$e \leftarrow e - 1 = 1 - 1 = 0$.
Siirrytään takaisin kohtaan 5.

5. Koska $deg(R_{k+2}) = 1 < deg(B) = 2$, asetetaan
$q \leftarrow d^e = 9^0 = 1$,
$Q \leftarrow qQ = 9x + 9 \cdot 3 = 9x - 27$ ja
$R \leftarrow qR_{k+2} = -9x + 27$.
Ja näin saatiin ratkaistua polynomit Q ja R, ja yhtälöksi $d^{\delta_k+1}A_k = BQ+R$ saatiin $9^2(x^3 - 3x^2 - 2x + 6) = (9x^2 - 17)(9x - 27) + (-9x + 27)$.
Nyt voidaan siirtyä kohtaan 7.

7. Asetetaan
$A_{k+1} \leftarrow B = 9x^2 - 17$ ja
$B \leftarrow \frac{R_{k+2}}{g_k h_k^{\delta_k}} = \frac{R_{k+2}}{1 \cdot 1^1} = -9x + 27$.

8. Asetetaan
$g_{k+1} \leftarrow l(A_{k+1}) = 9$ ja
$h_{k+1} \leftarrow h_k^{1-\delta_k} g_{k+1}^{\delta_k} = 1 \cdot 9^{3-2} = 9$.
Koska $deg(B) = 1 > 0$, niin siirrytään kohtaan 2.

2. Asetetaan $\delta_{k+1} = deg(A_{k+1}) - deg(B) = 2 - 1 = 1$.

3. Asetetaan $d \leftarrow l(B) = -9$. Lasketaan kohtien $4 - 6$ mukaan polynomit Q ja R siten, että $d^{\delta_{k+1}+1}A_{k+1} = BQ + R$ ja $deg(R) < deg(B)$.

4. Asetetaan
$R_{k+3} \leftarrow A_{k+1} = 9x^2 - 17$, $Q \leftarrow 0$ ja $e \leftarrow \delta_{k+1} + 1 = 1 + 1 = 2$.

5. Koska $deg(R_{k+3}) = 2 > deg(B) = 1$, siirrytään kohtaan 6.

6. Asetetaan
$S \leftarrow l(R_{k+3})x^{deg(R_{k+3})-deg(B)} = 9x^{2-1} = 9x$,
$Q \leftarrow dQ + S = (-9) \cdot 0 + 9x = 9x$,
$R_{k+3} \leftarrow dR_{k+3} - SB = (-9)(9x^2 - 17) - 9x(-9x + 27) = -27 \cdot 9x + 9 \cdot 17$
ja
$e \leftarrow e - 1 = 2 - 1 = 1$.
Siirrytään takaisin kohtaan 5.

5. Koska $deg(R_{k+3}) = 1 = deg(B)$, siirrytään kohtaan 6.

6. Asetetaan
$S \leftarrow l(R_{k+3})x^{deg(R_{k+3})-deg(B)} = (-27 \cdot 9)x^{1-1} = -27 \cdot 9$,
$Q \leftarrow dQ + S = (-9)9x - 27 \cdot 9$,

$R_{k+3} \leftarrow dR_{k+3} - SB = (-9)(-27 \cdot 9x + 9 \cdot 17) - (-27 \cdot 9)(-9x + 27) = 5184$
ja
$e \leftarrow e - 1 = 1 - 1 = 0$.
Siirrytään takaisin kohtaan 5.

5. Koska $deg(R_{k+3}) = 0 < deg(B) = 1$, asetetaan

$q \leftarrow d^e = (-9)^0 = 1$, $Q \leftarrow dQ = -9^2x - 27 \cdot 9$ ja
$R \leftarrow qR_{k+3} = 5184$.
Näin ollen yhtälöksi $d^{\delta_{k+1}+1}A_{k+1} = BQ + R$ saadaan
$(-9)^2(9x^2 - 17) = (-9x + 27)(-9^2x - 27 \cdot 9) + 5184$
Siirrytään kohtaan 7.

7. Asetetaan
$A_{k+2} \leftarrow B = -9x + 27$ ja
$B \leftarrow \frac{R_{k+3}}{g_{k+1}h_{k+1}^{\delta_{k+1}}} = \frac{5184}{9 \cdot 9^{2-1}} = \frac{5184}{81} = 64$.

8. Asetetaan
$g_{k+2} \leftarrow l(A_{k+2}) = -9$ ja
$h_{k+2} \leftarrow h_{k+1}^{1-\delta_{k+1}} g_{k+2}^{\delta_{k+1}} = 9^{1-1} \cdot (-9)^1 = -9$.
Koska $deg(B) = 0$, asetetaan
$h_{k+3} \leftarrow h_{k+2}^{1-deg(A)} l(B)^{deg(A)} = -9^{1-1} \cdot 64^1 = 64$
ja päätetään algoritmi tulostamalla
$sth_{k+2} = 1 \cdot 1 \cdot 64 = 64$,
mikä on algoritmin antama resultantin arvo tehtävässä annetuille polynomeille A ja B.

Esimerkki 13. Lasketaan vielä esimerkin (11) polynomeille

$$A(x) = x^4 - 2x^2 + 1$$

ja

$$B(x) = x^3 - 3x^2 - 2x + 6$$

resultantti resultantin lausekkeen $(4')$ eli lausekkeen

$$R = (-1)^{mn} b_0^m A(\beta_1)A(\beta_2) \cdots A(\beta_n)$$

avulla. Saadaan

$$\begin{aligned} R &= (-1)^{4\cdot 3}1^4((\sqrt{2})^4 - 2(\sqrt{2})^2 + 1)((\sqrt{-2})^4 - 2(\sqrt{-2})^2 + 1)(3^4 - 2\cdot 3^2 + 1) \\ &= (9\cdot(\sqrt{2})^2 - 17)(9\cdot(\sqrt{-2})^2 - 17)(9\cdot 3^2 - 17) \\ &= 64. \end{aligned}$$

Algoritmin todistus. Olkoot polynomit A_i algoritmin kohdassa 7 asetettuja polynomeja ja jakojäännökset R_i kohdassa 5 saatuja jakojäännöksiä. Algoritmin voidaan ajatella olevan monivaiheinen siten, että kunkin vaiheen päätyttyä eli siirryttäessä kohtaan 7 on saatu suoritettua polynomin jako. Vaiheiden määrä riippuu alkuperäisistä polynomeista, ja algoritmi päättyy, kunhan ollaan päädytty tilanteeseen, jossa $deg(B) = 0$. Olkoon t sellainen indeksi, että $deg(A_{t+1}) = 0$. Olkoot algoritmissa annetut polynomit $A = A_0$ ja $B = A_1$. Voidaan ajatella, että kohdassa 7 asetettavan polynomin A_i, missä $i = k-1, k, k+1, ..., t+1 \leq i$, alaindeksi i kertoo, monesko vaihe algoritmissa aloitetaan. Koska merkittiin $A = A_0$, täytyy olla $k \geq 1$. Varustetaan kunkin vaiheen omaavat vakiot g ja h alaindeksillä i. Siispä $g_0 = h_0 = 1$. Merkitään kunkin vaiheen vakioita g_i ja h_i. Käytetään esimerkin (11) merkintöjä $deg(A_i) = d_i$ ja $\delta_i = d_i - d_{i+1}$ sekä merkintää $l(A_i) = l_i$. Tarkastellaan tässä polynomia A_k jollakin annetulla k. Koska k voi olla kuitenkin, mikä tahansa annettu k, niin tarkastelu pätee kaikille k Merkitään polynomin A_k nollakohtia symboleilla β_j, missä $1 \leq j \leq d_k$. Yhtälön (4') muodossa ilmaistun resultantin lausekkeen avulla saadaan polynomien A_{k-1} ja A_k resultantiksi

$$\begin{aligned} R(A_{k-1}, A_k) &= (-1)^{d_{k-1}d_k} {l_k}^{d_{k-1}} A_{k-1}(\beta_1)A_{k-1}(\beta_2)\cdots A_{k-1}(\beta_{d_k}) \\ &= (-1)^{d_{k-1}d_k} {l_k}^{d_{k-1}} \prod_{1\leq j\leq d_k} A_{k-1}(\beta_j). \end{aligned} \tag{15}$$

Osoitetaan, että

$$\prod_{1\leq j\leq d_k} A_{k-1}(\beta_j) = \prod_{1\leq j\leq d_k} \frac{R_{k+1}(\beta_j)}{{l_k}^{\delta_{k-1}+1}}. \tag{Väite 1}$$

Ratkaistaessa algoritmin mukaisesti yhtälön

$$d_k^{\delta_{k-1}+1} A_{k-1} = BQ + R_{k+1}$$

polynomeja Q ja R_{k+1} kohdassa 2 asetetaan

$\delta_{k-1} \leftarrow d_{k-1} - d_k$ ja kohdissa 3 ja 4
$d \leftarrow l(B)$,

$R_{k+1} \leftarrow A_{k-1}$ ja
$e \leftarrow \delta_{k-1} + 1 = d_{k-1} - d_k + 1$.

Jos nyt $deg(R_{k+1}) < deg(B)$, niin asetetaan

$q \leftarrow d^e = l(B)^{\delta_{k-1}+1}$ ja
$R_{k+1} \leftarrow qR_{k+1} = l(B)^{\delta_{k-1}+1} A_{k-1}$.

Näin ollen

$$\prod_{1 \le j \le d_k} R_{k+1}(\beta_j) = (l(B)^{\delta_{k-1}+1} A_{k-1}(\beta_1))(l(B)^{\delta_{k-1}+1} A_{k-1}(\beta_2)) \cdots (l(B)^{\delta_{k-1}+1} A_{k-1}(\beta_{d_k}))$$
$$= l(B)^{d_k(\delta_{k-1}+1)} \prod_{1 \le j \le d_k} A_{k-1}(\beta_j).$$

Tästä saadaan edelleen

$$\prod_{1 \le j \le d_k} A_{k-1}(\beta_j) = \frac{\prod_{1 \le j \le d_k} R_{k+1}(\beta_j)}{l(B)^{d_k(\delta_{k-1}+1)}} = \prod_{1 \le j \le d_k} \frac{R_{k+1}(\beta_j)}{l(B)^{\delta_{k-1}+1}},$$

ja tämä oli todistuksen väite 1.

Jos kohdissa $2-4$ tehtyjen sijoitusten jälkeen ei päde $deg(R_{k+1}) < deg(B)$, niin siirrytään kohtaan 6 ja asetetaan

$S \leftarrow l(R_{k+1}) x^{deg(R_{k+1}) - deg(B)} = l_{k-1} x^{d_{k-1} - d_k}$,
$R'_{k+1} \leftarrow d \cdot R_{k+1} - S \cdot B = l(B) A_{k-1} - l_{k-1} x^{d_{k-1} - d_k} \cdot B$ ja
$e \leftarrow e - 1 = d_{k_1} - d_k + 1 - 1 = d_{k-1} - d_k = \delta_{k-1}$.

Näiden sijoitusten jälkeen siirrytään kohtaan 5. Oletetaan, että ollaan tilanteessa, jossa $deg(R_{k+1}) < deg(B)$. Täten asetetaan

$q \leftarrow d^e = l(B)^{\delta_{k-1}}$
$R_{k+1} \leftarrow qR'_{k+1} = l(B)^{\delta_{k-1}} \cdot R'_{k+1}$.

Näin ollen

$$\prod_{1 \le j \le d_k} R_{k+1}(\beta_j) = (l(B)^{\delta_{k-1}} {R_{k+1}}'(\beta_1))(l(B)^{\delta_{k-1}} {R_{k+1}}'(\beta_2)) \cdots (l(B)^{\delta_{k-1}} {R_{k+1}}'(\beta_{d_k}))$$
$$= l(B)^{d_k(\delta_{k-1})}(l(B)A_{k-1}(\beta_1) - l_{k-1} x^{\delta_{k-1}} B(\beta_1))(l(B)A_{k-1}(\beta_2) - l_{k-1} x^{\delta_{k-1}} B(\beta_2))$$
$$\cdots (l(B)A_{k-1}(\beta_{d_k}) - l_{k-1} x^{\delta_{k-1}} \cdot B(\beta_{d_k}).$$

Koska $B(\beta_j) = 0$ kaikilla $1 \leq j \leq d_k$, niin saadaan

$$\prod_{1\leq j\leq d_k} R_{k+1}(\beta_j) = l(B)^{d_k(\delta_{k-1})} l(B)^{d_k} \prod_{1\leq j\leq d_k} A_{k-1}(\beta_j) = l(B)^{d_k(\delta_{k-1}+1)} \prod_{1\leq j\leq d_k} A_{k-1}(\beta_j). \tag{16}$$

Koska kohdassa 7 asetetaan $A_k \leftarrow B$, voimme todeta $l(B) = l_k$. Siispä yhtälö (16) saadaan muotoon

$$\prod_{1\leq j\leq d_k} \frac{R_{k+1}(\beta_j)}{l_k^{(\delta_{k-1}+1)d_k}} = \prod_{1\leq j\leq d_k} A_{k-1}(\beta_j).$$

Näin on todistettu väite 1.

Jos tehtävässä aikana toistamiseen joudutaan siirtymään kohtaan 6, todistuksessa sijoitetaan

$S \leftarrow l(R'_{k+1})x^{deg(R'_{k+1})-deg(B)}$,
$R''_{k+1} \leftarrow dR'_{k+1} - SB = l(B)R'_{k+1} - SB$ ja
$e \leftarrow e - 1 = \delta_{k-1} - 1$.

Tämän jälkeen siirrytään kohtaan 5. Jos nyt $deg(R_{k+1}) < deg(B)$, asetetaan

$q \leftarrow d^e = l(B)^{\delta_{k-1}-1}$ ja
$R_{k+1} \leftarrow qR''_{k+1} = l(B)^{\delta_{k-1}-1}(l(B)R'_{k+1} - SB)$
$= l(B)^{\delta_{k-1}}R'_{k+1} - l(B)^{\delta_{k-1}-1}SB.$

Näin ollen

$$\prod_{1\leq j\leq d_k} R_{k+1}(\beta_j) = (l(B)^{\delta_{k-1}}R'_{k+1}(\beta_1) - l(B)^{\delta_{k-1}-1}SB(\beta_1))(l(B)^{\delta_{k-1}}R'_{k+1}(\beta_2) - l(B)^{\delta_{k-1}-1}SB(\beta_2))$$
$$\cdots (l(B)^{\delta_{k-1}}R'_{k+1}(\beta_{d_k}) - l(B)^{\delta_{k-1}-1}SB(\beta_{d_k})).$$

Koska $B(\beta_j) = 0$, kaikilla $1 \leq j \leq d_k$, niin saadaan

$$\prod_{1\leq j\leq d_k} R_{k+1}(\beta_j) = (l(B)^{\delta_{k-1}}R'_{k+1}(\beta_1)(l(B)^{\delta_{k-1}}R'_{k+1}(\beta_2)\cdots(l(B)^{\delta_{k-1}}R'_{k+1}(\beta_{d_k}).$$

Nyt ollaan päädytty tilanteeseen, joka jo todistettiin.

Sijoitetaan väitteen 1 yhtälö yhtälöön 15, jolloin saadaan

$$\begin{aligned} R(A_{k-1}, A_k) &= (-1)^{d_{k-1}d_k} {l_k}^{d_{k-1}} \prod_{1 \le j \le d_k} \frac{R_{k+1}(\beta_j)}{{l_k}^{(\delta_{k-1}+1)d_k}} \\ &= (-1)^{d_{k-1}d_k} {l_k}^{d_{k-1}} {l_k}^{-d_k(\delta_{k-1}+1)} \prod_{1 \le j \le d_k} R_{k+1}(\beta_j) \\ &= (-1)^{d_{k-1}d_k} {l_k}^{d_{k-1}-d_k(\delta_{k-1}+1)} \prod_{1 \le j \le d_k} R_{k+1}(\beta_j). \end{aligned} \tag{17}$$

Todistetaan seuraavaksi, että

$$\prod_{1 \le j \le d_k} R_{k+1}(\beta_j) = {l_k}^{-dk+1} R(A_k, g_{k-1} h_{k-1}^{\delta_{k-1}} A_{k+1}). \qquad \text{(Väite 2)}$$

Lähdetään liikkeelle muodostamalla resultantti $R(A_k, g_{k-1}{h_{k-1}}^{\delta_{k-1}} A_{k+1})$ resultantin lausekkeen (4) mukaisesti. Tässä luvut β_j ovat polyonimin A_k nollakohdat.

$$R(A_k, g_{k-1} h_{k-1}^{\delta_{k-1}} A_{k+1}) = {l_k}^{d_{k+1}} \prod_{1 \le j \le d_k} g_{k-1}{h_{k-1}}^{\delta_{k-1}} A_{k+1}(\beta_j). \tag{18}$$

Koska resultantin algoritmissa (kohta 7) tehdään korvaus $R(A_{k+1}) \leftarrow \frac{R_{k+1}}{g_{k-1}{h_{k-1}}^{\delta_{k-1}}}$, saadaan $g_{k-1}{h_{k-1}}^{\delta_{k-1}} A_{k+1} = R_{k+1}$. Tämä voidaan sijoittaa yhtälöön (18) ja saadaan

$$\begin{aligned} R(A_k, g_{k-1}{h_k}^{\delta_{k-1}} A_{k+1}) &= {l_k}^{d_{k+1}} \prod_{1 \le j \le d_k} R_{k+1}(\beta_j) \\ \Leftrightarrow {l_k}^{-d_{k+1}} R(A_k, g_{k-1}{h_k}^{\delta_{k-1}} A_{k+1}) &= \prod_{1 \le j \le d_k} R_{k+1}(\beta_j). \end{aligned}$$

Ilmaistaan reusultantti $R(A_k, g_{k-1}{h_k}^{\delta_{k-1}} A_{k+1})$ säännön $R(A, cB) = c^{deg(A)} R(A, B)$ mukaisesti, jolloin yhtälö (17) saa muodon

$$R(A_{k-1}, A_k) = (-1)^{d_{k-1}d_k} {l_k}^{d_{k-1}-d_k(\delta_{k-1}+1)-d_{k+1}} {g_{k-1}}^{d_k} {h_{k-1}}^{d_k(d_{k-1}-d_k)} R(A_k, A_{k+1}).$$

Tähän voidaan sijoittaa $l_k = g_k$, sillä algoritmissa kohdassa 8 tehdään korvaus $g \leftarrow l(A)$. Näin ollen saadaan

$$R(A_{k-1}, A_k) = (-1)^{d_{k-1}d_k} {g_k}^{d_{k-1}-\delta_{k-1}d_k-d_k-d_{k+1}} {g_{k-1}}^{d_k} {h_{k-1}}^{d_k(d_{k-1}-d_k)} R(A_k, A_{k+1}).$$

Kohdassa 8 suoritettavan korvauksen mukaan

$$\begin{aligned} h_k &= {h_{k-1}}^{1-\delta_{k-1}} {g_k}^{\delta_{k-1}} \\ \Leftrightarrow {g_k}^{d_k(\delta_{k-1})} &= \frac{{h_k}^{d_k}}{{h_{k-1}}^{d_k(1-\delta_{k-1})}}, \end{aligned}$$

ja lisäksi $\delta_{k-1} = d_{k-1} - d_k$, joten saadaan edelleen

$$\begin{aligned} R(A_{k-1}, A_k) &= (-1)^{d_{k-1}d_k} {g_k}^{-\delta_{k-1}d_k} {g_k}^{-d_{k+1}} {g_k}^{\delta_{k-1}} {g_{k-1}}^{d_k} {h_{k-1}}^{\delta_{k-1}d_k} R(A_k, A_{k+1}) \\ &= (-1)^{d_{k-1}d_k} \frac{{g_k}^{\delta_{k-1}} {h_{k-1}}^{d_k(1-\delta_{k-1})} {g_{k-1}}^{d_k} {h_{k-1}}^{\delta_{k-1}d_k}}{{h_k}^{d_k} {g_k}^{d_{k+1}}} R(A_k, A_{k+1}). \end{aligned}$$

Edelleen kohdan 8 mukaan

$$\begin{aligned} h_k &= {h_{k-1}}^{1-\delta_{k-1}} {g_k}^{\delta_{k-1}} \\ \Leftrightarrow {g_k}^{(\delta_{k-1})} &= \frac{h_k}{{h_{k-1}}^{1-\delta_{k-1}}}, \end{aligned}$$

joten tämä sijoittamalla saadaan

$$\begin{aligned} R(A_{k-1}, A_k) &= (-1)^{d_{k-1}d_k} \frac{h_k g_{k-1}^{d_k} h_{k-1}^{\delta_{k-1}d_k} h_{k-1}^{d_k(1-\delta_{k-1})}}{h_{k-1}^{1-\delta_{k-1}} g_k^{d_{k+1}} {h_k}^{d_k}} R(A_k, A_{k+1}) \\ &= (-1)^{d_{k-1}d_k} \frac{g_{k-1}^{d_k} h_{k-1}^{\delta_{k-1}d_k - \delta_{k-1}d_k + d_k - 1 + d_{k-1} - d_k}}{g_k^{d_{k+1}} h_k^{d_k - 1}} R(A_k, A_{k+1}) \\ &= (-1)^{d_{k-1}d_k} \frac{g_{k-1}^{d_k} h_{k-1}^{d_{k-1}-1}}{g_k^{d_{k+1}} h_k^{d_k-1}} R(A_k, A_{k+1}). \end{aligned} \tag{19}$$

Kirjoitetaan resultantin $R(A_{k-1}, A_k)$ lauseke kuten kohdassa 19. Näin ollen

$$R(A_{k-1}, A_k) = (-1)^{d_{k-1}d_k} \frac{g_{k-1}^{d_k} h_{k-1}^{d_{k-1}-1}}{g_k^{d_{k+1}} h_k^{d_k-1}} R(A_k, A_{k+1}).$$

Kirjoitetaan vastaavalla tavalla kyseisessä resultantin lausekkeessa esiintyvä resultantti $R(A_k, A_{k+1})$ eli

$$R(A_k, A_{k+1}) = (-1)^{d_k d_{k+1}} \frac{g_k^{d_{k+1}} h_k^{d_k-1}}{g_{k+1}^{d_{k+2}} h_{k+1}^{d_{k+1}-1}} R(A_{k+1}, A_{k+2}).$$

Esitetään samalla tavoin kaikki resultantin lausekkeet $R(A_{k-1}, A_k)$, missä $1 \leq k \leq t$. Sijoittamalla kukin resultantin lauseke kutakin edeltävään reusultantin lausekkeesseen saadaan

$$R(A_k, A_{k+1}) = (-1)^{\sum_{1\leq k\leq t} d_{k-1}d_k} \frac{g_{k-1}^{d_k} g_k^{d_{k+1}} g_{k+1}^{d_{k+2}} \cdots g_{t-1}^{d_t} h_{k-1}^{d_{k-1}-1} h_k^{d_k-1} h_{k+1}^{d_{k+1}-1} \cdots h_{t-1}^{d_{t-1}-1}}{g_k^{d_{k+1}} g_{k+1}^{d_{k+2}} g_{k+2}^{d_{k+3}} \cdots g_t^{d_{t+1}} h_k^{d_k-1} h_{k+1}^{d_{k+1}1} h_{k+2}^{d_{k+2}-1} \cdots h_t^{d_t-1}} \cdot R(A_t, A_{t+1}).$$

Supistetaan, jolloin saadaan

$$R(A_k, A_{k+1}) = (-1)^{\sum_{1\leq k\leq t} d_{k-1}d_k} \frac{g_{k-1}^{d_k} h_{k-1}^{d_{k-1}}}{g_t^{d_{t+1}} h_t^{d_t-1}} R(A_t, A_{t+1}).$$

Koska asetettiin $g_{k-1} = 1$ ja $h_{k-1} = 0$, ja koska $g_t^{d_{t+1}} = g_t^0 = 1$, niin saadaan

$$\begin{aligned} R(A_k, A_{k+1}) &= (-1)^{\sum_{1\leq k\leq t} d_{k-1}d_k} \frac{1}{h_t^{d_t-1}} R(A_t, A_{t+1}) \\ &= (-1)^{\sum_{1\leq k\leq t} d_{k-1}d_k} h_t^{1-d_t} R(A_t, A_{t+1}). \end{aligned}$$

Olkoon c vakio ja A polynomi. Tällöin pätee $R(A, c) = c^{deg(A)}$. Sovelletaan tätä resultanttiin $R(A_t, A_{t+1})$, missä siis A_{t+1} on nollatta astetta oleva polynomi eli vakio, jolloin saadaan

$$R(A_k, A_{k+1}) = (-1)^{\sum_{1\leq k\leq t} d_{k-1}d_k} h_t^{1-d_t} A_{t+1}^{d_t}.$$

Koska A_{t+1} on vakiopolynomi, se sisältää vain yhden termin, joka on luonnollisesti myös kyseisen poynomin johtava termi l_{t+1}. Siispä

$$R(A_k, A_{k+1}) = (-1)^{\sum_{1\leq k\leq t} d_{k-1}d_k} h_t^{1-d_t} l_{t+1}^{d_t}.$$

Algoritmin kohdassa 8 asetetaan $h_{i+1} \leftarrow h_i^{1-d_i} l_{i+1}^{d_i}$, missä $i = k-1, k, k+1, ..., t+1 \leq i$, joten tällöin asetetaan $h_{t+1} \leftarrow h_t^{1-d_t} l_{t+1}^{d_t}$. Näin saadaan

$$R(A_k, A_{k+1}) = (-1)^{\sum_{1\leq k\leq t} d_{k-1}d_k} h_{t+1}.$$

□

Lähdeluettelo

[1] A. Kurosh: *Higher algebra,* MIR Publishers, Moskova, 1980.

[2] K. Väisälä: *Lukuteorian ja korkeamman algebran alkeet,* Otava, Helsinki, 1950.

[3] K. Väänänen: *Lukuteorian luentomoniste,* Oulun yliopisto, 2008.

[4] P. Larja: *RSA-salaus ja sen lukuteoreettinen pohja,* http://tampub.uta.fi/bitstream/handle/10024/82542/gradu05032.pdf?sequence=1/

[5] H. Cohen: *A course in Computational Algebraic Number Theory,* Springer, Fourth Printing 2000.