Yhtälöiden ratkaisemisesta

Pro gradu-tutkielma
Antti Pekkala
1988723
Matemaattisten tieteiden laitos
Oulun yliopisto
Syksy 2014

Sisältö

Johdanto

Tulevana matematiikan aineenopettajana yhtälöiden ratkaisemista käsittelevä tutkielma tuntui itselle juuri sopivalta. Tutkielma käsittelee toisen, kolmannen ja neljännen asteen yhtälöitä ja niiden ratkaisemista. Vaikka tämä on huomattavasti lukiomatematiikkaakin haastavampaa, uskon siitä olevan hyötyä jatkossa. Aihe on hyvää lisätietoa, sillä toisen asteen yhtälön ratkaisukaava on yksi käytetyimpiä työkaluja lukion matematiikassa.

Tutkielmassa joudutaan käsittelemään pääasiassa polynomeja, minkä vuoksi rakennetaan polynomirenkaan käsite. Tätä varten joudutaan määrittämään renkaan ja kunnan käsitteet, sekä niihin liittyvä peruskäsitteistö kappaleessa 1. Myös polynomirenkaille rakennetaan peruskäsitteistö ja niiden yhteyteen tarvittavat määritelmät ja työkalut. Nämä käsitellään sekä yleisille polynomirenkaille kappaleessa 2, että rationaalilukukertoimisille polynomirenkaille kappaleessa 3. Näiden jälkeen on mahdollista muodostaa toisen, kolmannen ja neljännen asteen yhtälöiden ratkaisukaavat kappaleessa 4. Näitä ratkaisukaavoja käytetään ja sovelletaan reilusti ja niihin liittyviä apukeinoja käytetään hyväksi. Lisäksi todetaan ettei viidennen asteen yhtälöille ole ratkaisukaavaa olemassa.

Koska yhtälöiden ratkaiseminen ja ratkaisukaavojen löytäminen on ollut historiallisesti merkittävää matematiikalle ja koska ratkaisukaavojen muodostaminen suoritetaan osittain historialliseen tyyliin, on tutkielmaan lisätty vielä historiaa käsittelevä osuus, kappale 5. Tässä käydään läpi yhtälöiden ratkaisemiseen liittyvää historiaa ja sen merkitystä matematiikalle.

Tutkielmassa on käytetty lähteinä Markku Niemenmaan luentoihin pohjautuvaa luentomonistetta ja siihen liittyviä luentoja (Lähde [1]) peruskäsittestön luomiseen, J. J. Rotmanin teosta (Lähde [2]) ja O. E. Nicodemin teosta (Lähde [3]) kolmannen ja neljännen asteen yhtälöiden ratkaisukaavan ja esimerkkien tekemiseen, sekä C. B. Boyerin teosta (Lähde [4]) historiaosuuden muodostamiseen. Muut osiot mukailevat pääosin luentomuistiinpanoja (Lähde [1]).

1 Renkaista ja kunnista

Tässä kappaleessa määritellään ryhmän, renkaan ja kunnan käsitteet, joita tarvitaan polynomirenkaan muodostamiseen. Sisältöä on muotoiltu luentomonistetta ja luentomuistiinpanoja [1] mukaillen niiltä osin kuin on tarvittu.

Määritelmä 1.1. Pari $(G, *)$ on *ryhmä*, jos seuraavat ehdot täyttyvät:
1° *Assosiaatio:* Alkioille $x, y, z \in G$ pätee

$$x * (y * z) = (x * y) * z.$$

2° *Ykkösalkio:* On olemassa sellainen alkio $1 \in G$, jolle kaikilla $x \in G$ pätee

$$1 * x = x = x * 1.$$

3° *Vasta-alkio:* Jokaiselle alkiolle x on olemassa alkio $x' \in G$, jolle pätee

$$x' * x = 1 = x * x'.$$

Lisäksi ryhmää $(G, *)$ kutsutaan *Abelin ryhmäksi*, jos sille on seuraava ehto voimassa:
4° *Kommutaatio:* Alkioille $x, y \in G$ pätee

$$x * y = y * x.$$

Esimerkki 1.2. Pari $(\mathbb{Z}, +)$ ja pari $(\mathbb{Q} \setminus \{0\}, \cdot)$ ovat ryhmiä. Huomattavaa on, että ryhmän $(\mathbb{Z}, +)$ ykkösalkio on 0 ja kun taas ryhmällä $(\mathbb{Q} \setminus \{0\}, \cdot)$ ykkösalkio on 1. Todistetaan tämä:
1° Assosiaatio on voimassa kokoneislukujen ja rationaalilukujen joukossa sekä yhteen- että kertolaskun suhteen.
2° Yhteenlaskussa $0 + x = x = x + 0$ ja kertolaskussa $1 \cdot y = y = y \cdot 1$ pätevät kaikilla $x \in \mathbb{Z}$ ja $y \in \mathbb{Q}$.
3° Yhteenlaskussa alkion x vasta-alkio on $-x$ ja kertolaskussa $\frac{1}{x} = x^{-1}$. Koska alkiota $\frac{1}{0}$ ei voida määritellä, on kertolaskun joukko $(\mathbb{Q} \setminus \{0\}, \cdot)$ jouduttu muodostamaan ilman tätä alkiota 0.

Kaikille alkioille $x, y \in \mathbb{Z}$ pätee $x + y = y + x$ ja kaikille alkioille $x, y \in \mathbb{Q}$ pätee $x \cdot y = y \cdot x$. Tällöin siis myös ehto 4° toteutuu, joten molemmat ryhmät ovat Abelin ryhmiä.

Määritelmä 1.3. Ryhmän $(G, *)$ epätyhjä osajoukko H on *aliryhmä*, mikäli seuraavat ehdot täyttyvät:
1° Ryhmän G ykkösalkio kuuluu joukkoon H eli $1 \in H$.
2° Alkioille $x, y \in H$ pätee $x * y \in H$.
3° Jos alkio $x \in H$, niin silloin myös vasta-alkio $x' \in H$.

Lause 1.4. *Ryhmän $(G, *)$ aliryhmä $(H, *)$ on ryhmä.*

Todistus. Osoitetaan ryhmän ehtojen täyttyvän aliryhmän H alkioille.
1° Koska aliryhmän H alkiot kuuluvat myös ryhmään G, pätee niille assosiaatio $x * (y * z) = (x * y) * z$ myös aliryhmässä H.
2° Aliryhmän määritelmä sanoo, että ryhmän G ykkösalkio $1 \in H$. Tämä ykkösalkio on nyt myös aliryhmän H ykkösalkio, sillä operaatio $*$ on sama.
3° Aliryhmän määritelmässä todetaan jokaiselle aliryhmän H alkiolle olevan vasta-alkio. Koska nämä alkiot kuuluvat ryhmään G, pätevät niiden säännöt myös aliryhmässä H. □

Huomautus 1.5. Tapauksissa, missä ryhmän osajoukko tulee osoittaa ryhmäksi on helpompi osoittaa aliryhmän käsitteen kautta. Tällöin assosiaatiota ei tarvitse erikseen todistaa, vaan se periytyy ryhmältä aliryhmälle.
Ryhmän G aliryhmiin kuuluvat triviaalit tapaukset $\{1\}$ ja ryhmä G itse. Kun puhutaan ei-triviaaleista aliryhmistä, käytetään termiä *aito* aliryhmä.

Esimerkki 1.6. Ryhmän $(\mathbb{Z}, +)$ aliryhmä $\{x \in \mathbb{Z} | x = 2k, k \in \mathbb{Z}\}$ samalla yhteenlaskuoperaatiolla on myös ryhmä, sillä aliryhmän edellytykset toteutuvat.
1° Ryhmän $\mathbb{Z}$ ykkösalkio 0 on nyt myös aliryhmän ykkösalkio, sillä $2 \cdot 0 = 0$
2° Aliryhmän alkioilla $2m$ ja $2n$ muodostettu alkio $2m + 2n = 2(m + n)$ kuuluu aliryhmään, sillä kokonaislukujen summa on kokonaisluku.
3° Aliryhmän alkion $2m$ vasta-alkio on $2(-m) = -2m$, koska $2m + (-2m) = 0$. Tämä alkio kuuluu nyt aliryhmään, sillä kokonaisluvun vastaluku on myös kokonaisluku.

Määritelmä 1.7. Kolmikko $(R, +, \cdot)$ on *rengas*, jos seuraavat ehdot täyttyvät:
1° Pari $(R, +)$ on Abelin ryhmä (eli kommutatiivinen ryhmä).
2° Operaatio $(\cdot\ )$ on assosiatiivinen operaatio joukossa R, eli $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
3° On olemassa ykkösalkio $1 \in R$, jolle $1a = a = a1$ kaikilla $a \in R$.
4° $a \cdot (b + c) = a \cdot b + a \cdot c$ ja $(a + b) \cdot c = a \cdot c + b \cdot c$ kaikilla $a, b, c \in R$.
Lisäksi sanotaan, että rengas on *kommutatiivinen*, mikäli kertolaskuoperaatio $(\cdot)$ on kommutatiivinen, eli seuraava ehto on voimassa.
5° $a \cdot b = b \cdot a$ kaikilla $a, b \in R$

Huomautus 1.8. Renkaan määrittelyssä käytetyt operaatiot $+$ ja $\cdot$ merkitään juuri näillä symboleilla, koska niitä tullaan jatkossa käyttämään yhteen- ja kertolasku operaattoreina. Annettu määritelmä ei kuitenkaan rajoita näitä operaatioita olemaan juuri yhteenlaskua ja kertolaskua, vaan ne voivat olla jotain muutakin. Merkitään jatkossa kertolasku ilman operaattorimerkintää, eli $a \cdot b = ab$.

Esimerkki 1.9. Rationaalilukujen joukko $\mathbb{Q}$ varustettuna yhteen- ja kertolaskulla on rengas:
1° $(\mathbb{Q}, +)$ on Abelin ryhmä, sillä yhteenlasku on assosiatiivinen ja kommutatiivinen rationaaliluvuilla ja tässä joukossa on ykkösalkio 0 sekä käänteisalkio $-a$.
2° Rationaalilukujen välinen kertolasku on tunnetusti assosiatiivinen, kuten myös esimerkissä 1.2 todettiin.
3° On olemassa ykkösalkio $1_{\mathbb{Q}} = 1$, jolle $1a = a = a1$ kaikilla $a \in \mathbb{Q}$
4° Selvästi myös ehdot $a(b+c) = ab+ac$ ja $(a+b)c = ac+bc$ pätevät kaikilla $a, b, c \in \mathbb{Q}$.

Esimerkki 1.10. Myös kokonaislukujen joukko $\mathbb{Z}$ varustettuna yhteen- ja kertolaskulla on rengas. Alla olevia ehtoja osoitettiin osittan esimerkissä 1.2.
1° $(\mathbb{Z}, +)$ on Abelin ryhmä esimerkin 1.2 perusteella.
2° Kokonaislukujen välinen kertolasku on assosiatiivinen, kuten esimerkissä 1.2 todettiin.
3° Kokonaislukujen kertolaskun ykkösalkio on 1, sillä $1x = x = x1$ kaikille $x \in \mathbb{Z}$.
4° Myös ehdot $a(b + c) = ab + ac$ ja $(a + b)c = ac + bc$ pätevät joukossa $\mathbb{Z}$, jos ne kerran pätevät esimerkin 1.9 mukaan joukossa $\mathbb{Q}$.

Määritelmä 1.11. Rengas $(K, +, \cdot)$ on *kunta*, jos seuraavat ehdot täyttyvät:
1° K on kommutatiivinen rengas.
2° Pari $(K \setminus \{0\}, \cdot)$ on ryhmä.

Tässä yhteydessä alkiolla 0 tarkoitetaan kunnan alkiota, jolle $(+)$ operaation suhteen on voimassa $a + 0 = a = 0 + a$.

Huomautus 1.12. Kunnan määritelmästä seuraa välittömästi, että ryhmä $(K \setminus \{0\}, \cdot)$ on Abelin ryhmä, sillä kommutatiivinen rengas edellyttää operaation $(\cdot)$ kommutatiivisuutta.

Esimerkki 1.13. Rationaalilukujen joukko $\mathbb{Q}$ varustettuna yhteen- ja kertolaskulla on kunta:
1° Nyt Esimerkin 1.9 mukaan $\mathbb{Q}$ on rengas, ja koska kertolasku on kommutatiivinen rationaalilukujen kesken, on $\mathbb{Q}$ kommutatiivinen rengas.
2° Nyt on jo todettu, että kertolasku on assosiatiivinen, joten riittää löytää ykkösalkio ja käänteisalkio. Ne ovat $1_{\mathbb{Q}} = 1$ ja $a^{-1} = n/m$, kun $a = m/n$. Huomattavaa on, ettei alkiolle $0 \in \mathbb{Q}$ löydy käänteisalkiota, mitä tosin ei vaaditakaan.

Esimerkki 1.14. Toisin kuin rationaaliluvuille, kokonaislukujen renkaasta $\mathbb{Z}$ ei voi muodostaa kuntaa. Tämä johtuu siitä, että $(\mathbb{Z} \setminus \{0\}, \cdot)$ ei ole ryhmä. Se täyttää muut ryhmän ehdot, muttei vasta-alkion ehtoa. Vasta-alkio kokonaisluvulle x olisi $\frac{1}{x}$, mikä on rationaaliluku, muttei kokonaisluku.

2 Polynomit renkaassa K[x]

Tässä kappaleessa esitetään polynomirenkaan määritelmä ja siihen liittyviä hyödyllisiä apuvälineitä. Sisältöä on muotoiltu luentomonistetta ja luentomuistiinpanoja [1] mukaillen.

2.1 Peruskäsitteistöä

Määritelmä 2.1. Kolmikkoa $(K[x], +, \cdot)$, missä
$K[x] = \{a_0 + a_1x + \ldots + a_nx^n \mid n \geq 0, a_i \in K, K \text{ on kunta}\}$ ja operaatiot $(+)$ ja $(\cdot)$ ovat polynomien yhteen- ja kertolasku, kutsutaan *polynomirenkaaksi.*

Lause 2.2. *Polynomirengas on kommutatiivinen rengas.*

Todistus. Tarkastellaan renkaan ehdot ja katsotaan lopuksi, että rengas on kommutatiivinen:
1°Olkoon $f(x), g(x)$ ja $h(x)$ joukon $K[x]$ polynomeja. Nyt tiedetään, että $(+)$ on assosiatiivinen operaatio. Lisäksi kunnan K ykkösalkio $1_K \in K[x]$ on selvästi ryhmän $(K[x], +)$ ykkösalkio. Ja koska käänteisalkio $-f(x)$, missä $-f(x) = (-1)f(x)$, on olemassa, ja polynomien summa on kommutatiivinen, on $(K[x], +)$ Abelin ryhmä.
2°Polynomien kertolasku $(\cdot)$ on selvästi assosiatiivinen
3°Kunnan K ykkösalkio 1_K on myös renkaan ykkösalkio, jolloin $1_Kf(x) = f(x) = f(x)1_K$.
4°Nyt seuraavat yhtälöt pitävät paikkaansa

$$f(x)(g(x)+h(x)) = f(x)g(x)+f(x)h(x) \text{ ja } (f(x)+g(x))h(x) = f(x)h(x)+g(x)h(x)$$

kaikilla $f(x), g(x)$ ja $h(x) \in K[x]$ polynomien laskusääntöjen nojalla.
Lisäksi kommutatiivisuus $f(x)g(x) = g(x)f(x)$ on myös voimassa polynomien laskusääntöjen nojalla. □

Määritelmä 2.3. Polynomin *asteeksi* sanotaan polynomin korkeinta astetta olevan termin eksponenttia, eli polynomin $f(x) = a_0 + a_1x + \ldots + a_nx^n$ aste on n. Tätä merkitään seuraavasti: $\deg f(x) = n$. Jos polynomi on nollasta poikkeava vakiopolynomi, eli muotoa $f(x) = a_0 \neq 0$, niin sen aste on 0. Mikäli $f(x) = 0$, niin sen aste on $-\infty$.

Määritelmä 2.4. Jos $f(x) = q(x)g(x)$, niin sanotaan, että $g(x)$ jakaa polynomin $f(x)$. Merkitään $g(x) \mid f(x)$.

Määritelmä 2.5. Polynomi $f(x) \in K[x]$ on *jaoton*, mikäli $\deg f(x) \geq 1$ ja polynomia $f(x)$ ei voi esittää kahden positiivista astetta olevan polynomin tulona.

Määritelmä 2.6. Jos $f(x) = a_0 + a_1x + \ldots + a_nx^n, \alpha \in K$ ja $f(\alpha) = a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$, niin α on polynomin $f(x)$ *nollakohta*. Voidaan myös sanoa, että α on polynomin $f(x)$ *juuri*.

Esimerkki 2.7. Nyt kunnasta $(\mathbb{Q}, +, \cdot)$ muodostettu rengas $\mathbb{Q}[x]$ on polynomirengas. Tämä rengas sisältää muun muassa polynomit $0, 1, f(x) = 3/4x^3 + 6$ ja $p(x) = x^2 - 2$, joista $p(x)$ on jaoton kunnassa $\mathbb{Q}$, eli ei ole olemassa kunnan $\mathbb{Q}$ alkiota α, jolle $p(\alpha) = 0$ (Lemman 2.9 perusteella). Huomattavaa kuitenkin on, että reaalilukujen kunnassa $\mathbb{R}$ tälläinen löytyy, eli $p(x) = x^2 - 2 = 0$, kun $x = \sqrt{2}$.

2.2 Jakoalgoritmi

Osoitetaan seuraavaksi tärkeä polynomeihin liittyvä lause.

Lause 2.8 (Jakoalgoritmi)**.** *Jos polynomit $f(x) \in K[x]$ ja $g(x) \in K[x]$ ja $g(x) \neq 0$, niin*

$$f(x) = q(x)g(x) + r(x)$$

missä $q(x) \in K[x]$ ja $r(x) \in K[x]$ ovat yksikäsitteiset ja $\deg r(x) < \deg g(x)$.

Todistus. Muodostetaan joukko $S = \{f(x) - g(x)s(x) \mid s(x) \in K[x]\}$. Nyt Joukossa S on pienintä astetta oleva termi, merkitään sitä polynomilla $r(x)$. Tällöin $r(x) = f(x) - g(x)s(x)$, joten

$$f(x) = q(x)g(x) + r(x)$$

jollain polynomilla $q(x) \in K[x]$.
Osoitetaan seuraavaksi, että polynomin $r(x)$ aste on pienempää kuin polynomin $g(x)$ aste. Merkitään

$$g(x) = b_0 + b_1x + \ldots + b_mx^m \text{ ja } r(x) = c_0 + c_1x + \ldots + c_tx^t,$$

jolloin $\deg g(x) = m$ ja $\deg r(x) = t$. Tehdään nyt vastaoletus, että $t \geq m$. Muodostetaan uusi polynomi

$$h(x) = f(x) - q(x)g(x) - (c_t/b_m)x^{t-m}g(x) = r(x) - (c_t/b_m)x^{t-m}g(x)$$

jonka jälkimmäinen osa on muotoa $r(x) - (c_t x^t + \ldots)$, eli polynomin $h(x)$ aste on pienempää kuin polynomin $r(x)$ aste t. Kirjoittamalla polynomi $h(x)$ uuteen muotoon, saadaan kuitenkin $h(x) = f(x) - g(x)(q(x) + (c_t/b_m)x^{t-m})$, eli $h(x) \in S$. Tämä on kuitenkin ristiriidassa sen olettamuksen kanssa, jonka mukaan $r(x) \in S$ on joukon pienintä astetta oleva polynomi. Tällöin vastaoletus on väärä ja $t < m$ eli $\deg r(x) < \deg g(x)$.
Vielä täytyy osoittaa polynomien $q(x)$ ja $r(x) \in K[x]$ yksikäsitteisyys. Olkoot

$$f(x) = q_1(x)g(x) + r_1(x)$$

ja

$$f(x) = q_2(x)g(x) + r_2(x)$$

josta toisistaan vähentämällä saadaan

$$g(x)[q_1(x) - q_2(x)] = r_2(x) - r_1(x).$$

Koska polynomien $r_1(x)$ ja $r_2(x)$ aste on pienempää kuin polynomin $g(x)$ aste, on myös niiden erotuksen $r_2(x) - r_1(x)$ aste pienempää kuin polynomin $g(x)$ aste. Tällöin on oltava $q_1(x) - q_2(x) = 0$ eli $q_1(x) = q_2(x)$ ja edelleen $r_2(x) - r_1(x) = 0$ eli $r_1(x) = r_2(x)$. Tällöin polynomit $q(x)$ ja $r(x)$ ovat yksikäsitteiset. □

Lemma 2.9. *Olkoon $f(x) \in K[x]$ ja $\alpha \in K$. Nyt $f(\alpha) = 0$ tarkalleen silloin, kun $(x - \alpha) \mid f(x)$.*

Todistus. Todistetaan väite molempiin suuntiin. Jos $(x - \alpha) \mid f(x)$, niin $f(x) = (x - \alpha)q(x)$ ja $f(\alpha) = (\alpha - \alpha)q(\alpha) = 0$.
Jos taas $f(\alpha) = 0$, niin sovelletaan jakoalgoritmia polynomeihin $f(x)$ ja $(x - \alpha)$. Silloin

$$f(x) = (x - \alpha)q(x) + r(x),$$

missä $\deg r(x) < \deg (x - \alpha) = 1$. Tällöin $r(x) = c \in K$, eli $f(x) = (x - \alpha)q(x) + c$. Koska $f(\alpha) = (\alpha - \alpha)q(x) + c = 0$, on polynomin $r(x)$ edelleen oltava 0. Nyt siis $f(x) = (x - \alpha)q(x)$, eli $(x - \alpha) \mid f(x)$. □

Lemma 2.10. *Olkoon $f(x) \in K[x]$ ja $\deg f(x) = n$. Tällöin polynomilla $f(x)$ on korkeintaan n nollakohtaa kunnassa K.*

Todistus. Olkoot $a_1, a_2, \ldots, a_m$ polynomin $f(x)$ kaikki nollakohdat kunnassa K. Nyt Lemman 2.9 perusteella $q(x) = (x - a_1) \ldots (x - a_m) \mid f(x)$, jolloin jakoalgoritmin perusteella $\deg q(x) = m \leq n$ □

3 Polynomeista renkaassa $\mathbb{Q}[x]$

Rationaalilukukertoiminen rengas on polynomirenkaan $K[x]$ erikoistapaus. Tässä kappaleessa on tarkoitus luoda työkaluja kokonaislukukertoimisten polynomien käsittelyyn renkaassa $\mathbb{Q}[x]$. Määritelmät ja lauseet noudattavat luentomonistetta ja luentomuistiinpanoja [1].

Määritelmä 3.1. Polynomin $f(x) = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x]$ yhteinen kerroin, eli $syt(a_0, a_1, \ldots, a_n)$ on 1, niin polynomia $f(x)$ kutsutaan silloin *alkeispolynomiksi.*

Lemma 3.2. *Kahden alkeispolynomin tulo on alkeispolynomi.*

Todistus. Olkoot
$f(x) = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x]$ ja
$g(x) = b_0 + b_1x + \ldots + b_mx^m \in \mathbb{Z}[x]$ alkeispolynomeja.
Tarkastellaan niiden tuloa $f(x)g(x)$ ja tehdään vastaoletus: $f(x)g(x)$ ei ole alkeispolynomi. Tällöin on olemassa ainakin sellainen alkuluku $p \in \mathbb{Z}$ joka jakaa polynomin $f(x)g(x)$ kaikki kertoimet. Koska polynomit $f(x)$ ja $g(x)$ ovat alkeispolynomeja, on olemassa sellaiset kertoimet a_j ja b_k, joita p ei jaa. Oletetaan lisäksi, että nämä kertoimet ovat polynomien ensimmäiset tälläiset kertoimet, jolloin $p \mid a_0, p \mid a_1, \ldots, p \mid a_{j-1}$ ja $p \mid b_0, p \mid b_1, \ldots, p \mid b_{k-1}$. Nyt polynomin $f(x)g(x)$ termin x^{j+k} kerroin c_{j+k} on muotoa

$$c_{j+k} = a_jb_k + [a_{j+1}b_{k-1} + a_{j+2}b_{k-2} + \ldots + a_{j+k}b_0] + [a_{j-1}b_{k+1} + a_{j-2}b_{k+2} + \ldots + a_0b_{j+k}].$$

Merkitään

$$c_{j+k} = a_jb_k + A + B.$$

Koska $f(x)g(x)$ on alkeispolynomi, pätee $p \mid c_{j+k}$. Nyt myös $p \mid a_0, p \mid a_1, \ldots, p \mid a_{j-1}$, joten $p \mid B$. Vastaavasti myös $p \mid b_0, p \mid b_1, \ldots, p \mid b_{k-1}$, joten myös $p \mid A$. Tästä seuraa se, että myös $p \mid a_jb_k$, eli joko $p \mid a_j$ tai $p \mid b_k$, mistä seuraa ristiriita. Tällöin vastaoletus on väärä ja polynomi $f(x)g(x)$ on alkeispolynomi. □

Lemma 3.3. *Jos alkeispolynomi $f(x)$ voidaan esittää kahden rationaalikertoimisen polynomin tulona, niin $f(x)$ voidaan esittää kahden kokonaislukukertoimisen polynomin tulona.*

Todistus. Olkoon $f(x) = u(x)v(x)$, missä $u(x), v(x) \in \mathbb{Q}[x]$. Tällöin $f(x) = \frac{a}{b}t(x)d(x)$, missä $a, b \in \mathbb{Z}$ ja $t(x)$ ja $d(x)$ ovat alkeispolynomeja. Täten

$$bf(x) = at(x)d(x).$$

Koska $f(x)$ on alkeispolynomi, on sen yhteinen kerroin 1 ja polynomin $bf(x)$ yhteinen kerroin b. Polynomi $t(x)d(x)$ on alkeispolynomi oletuksen ja Lemman [3.2] nojalla. Tällöin polynomin $at(x)d(x)$ yhteinen kerroin on a. Koska

$bf(x) = at(x)d(x)$, on tällöin oltava $a = b$. Tällöin polynomi $f(x)$ supistuu muotoon $f(x) = \frac{a}{a}t(x)d(x) = t(x)d(x)$. Tämä tarkoittaa sitä, että alkeispolynomi $f(x)$ on esitetty kahden kokonaislukukertoimisen polynomin tulona. □

Esimerkki 3.4. Polynomi $f(x) = 7x^3 + 37x^2 + 31x + 6$ on alkeispolynomi, sillä $syt(7, 37, 31, 6) = 1$. Tiedetään, että polynomi $f(x)$ voidaan esittää rationaalilukukertoimisen polynomin tulona, sillä

$$7x^3 + 37x^2 + 31x + 6 = (\frac{3}{5}x^2 + 3x + \frac{9}{5})(\frac{35}{3}x + \frac{10}{3}).$$

Tällöin polynomi voidaan esittää myös lemman 3.3 nojalla myös kokonaislukukertoimisten polynomien tulona. Tällöin

$$f(x) = (\frac{3}{5}x^2 + 3x + \frac{9}{5})(\frac{35}{3}x + \frac{10}{3}) = \frac{3}{5}(x^2 + 5x + 3)\frac{5}{3}(7x + 2)$$

$$f(x) = (x^2 + 5x + 3)(7x + 2).$$

Lause 3.5 (Eisensteinin kriteeri)**.** *Olkoon $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ ja olkoon p sellainen alkuluku, että $p \nmid a_n, p|a_{n-1}, \ldots, p|a_1, p|a_0$, mutta $p^2 \nmid a_0$. Tällöin polynomi $f(x)$ on jaoton renkaassa $\mathbb{Q}[x]$.*

Todistus. Jos polynomi $f(x)$ ei ole alkeispolynomi, niin tästä muodostettu polynomi $f(x)/syt(a_0 \ldots a_n)$ on. Koska $p \nmid a_n$, niin $p \nmid syt(a_0 \ldots a_n)$. Tällöin voidaan merkitä polynomia $f(x)/syt(a_0 \ldots a_n) = g(x)$. Tälle polynomille pätee samat ehdot kuin polynomille $f(x)$. Tämän vuoksi voidaan olettaa, että polynomi $f(x)$ on alkeispolynomi, sillä todistus voidaan suorittaa myös polynomille $g(x)$.

Tehdään vastaoletus; polynomi $f(x)$ on jaollinen polynomirenkaassa $\mathbb{Q}[x]$. Tällöin polynomi voidaan kirjoittaa muodossa $f(x) = u(x)v(x)$, missä polynomit $u(x)$ ja $v(x) \in \mathbb{Q}[x]$ sekä $\deg u(x)$ ja $\deg v(x) \geq 1$. Lemman [3.3] nojalla polynomi $f(x)$ voidaan esittää kahden kokonaislukukertoimisen polynomin tulona. Olkoon siis

$$f(x) = (b_r x^r + \ldots + b_1 x + b_0)(c_s x^s + \ldots + c_1 x + c_0),$$

missä $b_i, c_i \in \mathbb{Z}$ ja $r, s \geq 1$. Tällöin $n = r + s, a_n = b_r c_s$ ja $a_0 = b_0 c_0$. Koska $p|a_0$, mutta $p^2 \nmid a_0$, niin alkuluku p jakaa joko luvun b_0 tai c_0, muttei molempia. Oletetaan, että $p|b_0$, jolloin $p \nmid c_0$. Tarkastellaan nyt joukkoa $b_0, b_1, \ldots, b_r$. Tässä joukossa on ainakin yksi termi, jolle pätee $p \nmid b_i$, sillä $p \nmid a_n = b_r c_s$. Oletetaan, että termi b_k on näistä ensimmäinen, jota alkuluku p ei jaa, eli $p|b_0, \ldots p|b_{k-1}$, mutta $p \nmid b_k$. Koska $n = r + s \geq k + s \geq k + 1$, niin $k < n$. Tästä seuraa, että $p|a_k$ oletuksen nojalla. Nyt termi a_k on muotoa $a_k = b_k c_0 + b_{k-1} c_1 + b_{k-2} c_2 + \ldots$. Tässä termeille $b_{k-1}, b_{k-2}, \ldots$ pätee

ehto $p|b_i$ vakion k valinnan perusteella. Tästä seuraa siis, että myös ehdot $p|b_{k-1}c_1, p|b_{k-2}c_2, \ldots$ pätevät. Tämän perusteella alkuluku p jakaa myös termin $b_k c_0$, jolloin joko $p|b_k$ tai $p|c_0$. Tämä on kuitenkin edellisen perusteella mahdotonta, jolloin vastaoletuksemme on väärä ja väitteemme totta. □

Esimerkki 3.6. Polynomi $7x^3 + 8x^2 + 4x + 2$ on jaoton, sillä alkuluku $p = 2$ jakaa luvut $8, 4$ ja 2, mutta $2 \nmid 7$ ja $4 \nmid 2$.
Vastaavasti polynomi $x^{11} - 3$ on myös jaoton, sillä nollakertoimisille termeille ehto pätee, onhan $0 \cdot 3 = 0$ kokonaisluku eli $3|0$. Itse asiassa kaikille polynomeille, jotka ovat muoto $x^n - p$, missä $n \geq 2$, ovat jaottomia.

Huomautus 3.7. Huomattavaa on, että lause 3.5 toimii vain yhteen suuntaan. Esimerkiksi polynomi $f(x) = x^3 - 4$ on jaoton mutta lauseen ehtoja täyttävää alkulukua p ei ole olemassa. Joissain tapauksissa tämä ongelma voidaan kuitenkin kiertää tekemällä polynomiin lineaarinen muunnos. Esimerkiksi polynomi $g(x) = f(x + 1) = x^3 + 3x^2 + 3x - 3$ on Eisensteinin kriteerien perusteella jaoton, jolloin myös polynomi $f(x)$ on jaoton.

4 Polynomien nollakohdista ja yhtälöiden juurista

Käsiteltäessä tässä kappaleessa polynomeja oletetaan, että ne kuuluvat polynomirenkaaseen $\mathbb{C}[x]$. Tämä johtuu neliöjuuren käytöstä, sillä neliöjuuritermiä sisältävät juuret voivat olla irrationaalisia tai kompleksisia. Usein kuitenkin käsiteltävät polynomit ovat kokoneislukukertoimisia.

4.1 Toinen aste

Tämä kappale on muotoiltu luentomonistetta ja luentomuistiinpanoja [1] mukaillen.

Toisen asteen polynomi on yleisesti muotoa $ax^2 + bx + c = 0$. Yhtälön ratkaisemisen kannalta epäolennainen kerroin a voidaan jättää pois, sillä se voidaan jakaa yhtälöstä pois, jolloin yhtälö on muotoa $x^2 + \frac{b}{a}x + \frac{c}{a} = 0$. Käytetään siis muotoa $x^2 + bx + c = 0$ yksinkertaisuuden vuoksi.

Mikäli yhtälöön sijoitetaan muuttujan x paikalle termi $y - b/2$, saadaan ensimmäisen asteen termi supistettua pois, eli

$$y^2 - by + \frac{b^2}{4} + by - \frac{b^2}{2} + c = 0$$

$$y^2 = \frac{b^2}{4} - c$$

$$y = \pm\sqrt{\frac{b^2 - 4c}{4}}.$$

Kun tämä sijoitetaan takaisin alkuperäiseen yhtälöön, saadaan

$$x = -\frac{b}{2} \pm \frac{\sqrt{b^2 - 4c}}{2}.$$

Tätä kutsutaan nyt toisen asteen yhtälön *klassiseksi ratkaisukaavaksi*. Tällaisiksi kutsutaan ratkaisukaavoja, joihin on käytetty peruslaskutoimituksia $(+, -, \cdot, /)$, juuri- ja potenssilausekkeita, sekä polynomin kertoimia. Näitä saatuja kahta ratkaisua kutsutaan nyt yhtälön juuriksi ja yhtälöä vastaavan toisen asteen polynomin $f(x) = x^2 + bx + c$ nollakohdiksi, jolloin

$$f(-\frac{b}{2} + \frac{\sqrt{b^2 - 4c}}{2}) = 0 = f(-\frac{b}{2} - \frac{\sqrt{b^2 - 4c}}{2}).$$

Toisen asteen yhtälön juuria on siis kaksi. Neliöjuurilausekkeen arvosta riippuen ratkaisut voivat kuitenkin olla reaalisia tai kompleksisia. Mikäli neliöjuuren sisällä olevan lauseen arvo on positiivinen, ovat ratkaisut reaalisia ja mikäli negatiivinen, ovat ratkaisut kompleksisia. Tätä varten määritellään diskriminatin käsite.

Määritelmä 4.1. Olkoon toisen asteen polynomin $f(x) = x^2 + bx + c$ juuret u_1 ja u_2. Merkitään nyt

$$\Delta = u_1 - u_2 = -\frac{b}{2} + \frac{\sqrt{b^2 - 4c}}{2} - \left[-\frac{b}{2} - \frac{\sqrt{b^2 - 4c}}{2}\right] = \sqrt{b^2 - 4c},$$

jolloin $\Delta^2 = b^2 - 4c$. Lukua Δ^2 kutsutaan nyt polynomin $f(x)$ *diskriminantiksi*.

Nyt siis edelliset perustelut pätevät diskriminantille. Toisen asteen yhtälön diskrimantin ollessa positiivinen eli $\Delta^2 \geq 0$, ovat polynomin juuret reaalisia ja diskriminantin ollessa negatiivinen juuret ovat kompleksisia. Huomattava erikoistapaus on $\Delta^2 = 0$, jolloin juuret ovat reaalisia, mutta myös samoja. Tälläistä tapausta kutsutaan tuplajuureksi, eli $u_1 = u_2 = -b/2$.

Esimerkki 4.2. Lasketaan polynomin $f(x) = 3x^2 - 6x + 1$ nollakohdat ja diskriminantti. Jaetaan ensin polynomi kolmella saaden uusi polynomi $g(x) = x^2 - 2x + 1/3$, jonka juuret ovat samat kuin alkuperäisen polynomin $f(x)$. Nyt juuret polynomille ovat

$$u_1 = -\frac{2}{2} + \frac{\sqrt{2^2 - 4/3}}{2} = \sqrt{\frac{2}{3}} - 1$$

$$u_2 = -\frac{2}{2} - \frac{\sqrt{2^2 - 4/3}}{2} = -\sqrt{\frac{2}{3}} - 1.$$

Juuret ovat siis reaalisia, mikä nähdään myös diskriminantin arvosta $\Delta^2 = 2^2 - 4/3 = 8/3 > 0$.

4.2 Kolmas aste

Tämän kappaleen muotoilu noudattaa pääosin teoksessa[2] noudatettua esitystapaa.

Kolmannen asteen polynomi on muotoa $f(y) = ay^3 + by^2 + cy + d$ ja siitä johdettu kolmannen asteen yhtälö on muotoa $y^3 + by^2 + cy + d = 0$. Kerroin a on tässä nyt jätetty pois, sillä yksinkertaisesti jakamalla se voidaan supistaa yhtälöstä pois. Edelleen sijoittamalla $y = x - b/3$ yhtälöstä saadaan

$$(x - b/3)^3 + b(x - b/3)^2 + c(x - b/3) + d = 0$$

$$x^3 - \frac{3bx^2}{3} + \frac{3b^2x}{9} - \frac{b^3}{27} + bx^2 - \frac{2b^2x}{3} + \frac{b^3}{9} + cx - \frac{cb}{3} + d = 0$$

$$x^3 + \frac{9c - 3b^2}{9}x + \frac{2b^3 - 9bc + 27d}{27} = 0,$$

eli toisen asteen termi supistui pois. Tällöin riittää tarkastella kolmannen asteen yhtälöistä tapausta, jotka ovat muotoa

$$x^3 + qx + r = 0.$$

Olkoon nyt u eräs tämän yhtälön juuri. Valitaan nyt sellaiset luvut g ja h joille pätevät ehdot

$$1^\circ \; g + h = u$$

$$2^\circ \; gh = -q/3.$$

Valinta on mahdollinen, sillä ratkaistaessa tämä yhtälöpari luvun g suhteen saadaan toisen asteen yhtälö, joka voidaan ratkaista. Sijoittamalla $h = u - g$ alempaan yhtälöön saadaan siis $g(u - g) = -q/3$ eli $g^2 - ug + q/3 = 0$, joten tälläiset luvut g ja h ovat olemassa.

Sijoitetaan nyt $u = g + h$ tarkasteltavaan kolmannen asteen yhtälöön.

$$(g + h)^3 + q(g + h) + r = 0$$

$$g^3 + 3g^2h + 3gh^2 + h^3 + q(g + h) + r = 0$$

$$g^3 + h^3 + (g + h)(3gh + q) + r = 0$$

Tästä muodosta voidaan nyt poistaa termi $(g+h)(3gh+q)$, sillä lukujen g ja h valinnan perusteella $3gh+q=0$. Tällöin

$$g^3+h^3+r=0,$$

johon edelleen sijoittamalla ehdosta 2° saatu $h=-\frac{q}{3g}$ päästään muotoon

$$g^3-\frac{q^3}{27g^3}+r=0$$

$$g^6+rg^3-\frac{q^3}{27}=0.$$

Tämä on nyt toisen asteen yhtälö luvun g^3 suhteen. Ratkaisemalla saadaan

$$g^3=1/2(-r\pm\sqrt{r^2+4q^3/27}).$$

Koska $h^3=-r-g^3$, niin vastaavasti

$$h^3=1/2(-r\mp\sqrt{r^2+4q^3/27}).$$

Tällöin alkuperäisen kolmannen asteen yhtälön eräs juuri on

$$u=\sqrt[3]{1/2(-r+\sqrt{r^2+4q^3/27})}+\sqrt[3]{1/2(-r-\sqrt{r^2+4q^3/27})}.$$

Esimerkki 4.3. Ratkaistaan polynomin $f(y)=-2y^3+6y^2-4y-2$ nollakohta.
Ensiksi muutetaan polynomi muotoon x^3+qx+r, mihin voidaan käyttää askeen saatua ratkaisukaavaa. Nyt polynomin $-\frac{1}{2}f(y)$ nollakohta on sama kuin polynomin $f(y)$, joten tarkastellaan tätä polynomia ja merkitään sitä tähdellä. Tällöin $f^*(y)=y^3-3y^2+2y+1$. Käytetään nyt tähän polynomiin sijoitusta $y=x-b/3=x+1$, jolloin saadaan uusi polynomi $g(x)=f^*(x+1)$, joka on muotoa

$$g(x)=(x+1)^3-3(x+1)^2+2(x+1)+1=x^3+3x^2+3x+1-3x^2-6x-3+2x+2+1$$

$$g(x)=x^3-x+1$$

Nyt tähän muotoon voidaan käyttää edellä muodostettua ratkaisukaavaa, jolloin polynomin nollakohta on

$$u=\sqrt[3]{1/2(-r+\sqrt{r^2+4q^3/27})}+\sqrt[3]{1/2(-r-\sqrt{r^2+4q^3/27})}$$

$$u=\sqrt[3]{1/2(-1+\sqrt{-23/27})}+\sqrt[3]{1/2(-1-\sqrt{-23/27})}.$$

Tämän likiarvo voidaan laskea laskimella, jolloin saadaan $u \approx -1,32$. Nyt tämä on siis vasta polynomin $g(x)$ nollakohta. Tällöin polynomin $f^*(y)$ nollakohdat ovat polynomin $g(x)$ nollakohdat, joihin on lisätty 1, eli tapaus $u+1$. Koska alkuperäisen polynomin $f(y)$ nollakohdat ovat samat kuin polynomin $f^*(y)$, on polynomin $f(y)$ yksi nollakohta

$$y_1 = 1 + \sqrt[3]{1/2(-1+\sqrt{-23/27})} + \sqrt[3]{1/2(-1-\sqrt{-23/27})}$$

ja sen likiarvo $y_1 \approx -0,32$.

Tässä on vasta ratkaistu yksi kaikkiaan kolmesta yhtälön juuresta. Loput kaksi juurta voidaan kuitenkin johtaa tästä ensimmäisestä juuresta. Tarkastellaan tätä varten yhtälön $x^3 - 1 = 0$ juuria. Nyt yksi näistä juurista on 1, mikä voidaan tarkastaa sijoittamalla se yhtälöön. Jakamalla yhtälö tällä juurella saadaan toisen asteen yhtälö $x^2 + x + 1 = 0$, jonka juuret ovat

$$x = 1/2[-1 \pm \sqrt{1-4}] = -\frac{1}{2} \pm i\frac{\sqrt{3}}{2}.$$

Koska näistä juurista toinen saadaan korottamalla toinen sen neliöön, merkitään näitä kahta muuta juurta symbolein ω ja ω^2. Tällöin

$$\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$$

$$\omega^2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}.$$

Näiden termien valinta perustuu niiden ominaisuuksiin. Korottaessa termi ω kolmanteen potenssiin saadaan

$$\omega^3 = (-\frac{1}{2} - i\frac{\sqrt{3}}{2})(-\frac{1}{2} + i\frac{\sqrt{3}}{2}) = \frac{1}{4} + i\frac{\sqrt{3}}{4} - +i\frac{\sqrt{3}}{4} + \frac{3}{4} = 1.$$

Valittaessa termeja g ja h tuli päteä ehdot 1° ja 2°. Ehto 2° toteutuu myös käyttämällä termien g ja h tilalta termejä ωg ja $\omega^2 h$ tai $\omega^2 g$ ja ωh, sillä $gh = \omega^3 gh = (\omega g)(\omega^2 h) = (\omega^2 g)(\omega h)$. Samoin ehto 1° pätee, sillä ratkaisussa käytetyt termit $g = \sqrt[3]{g^3} = \sqrt[3]{(\omega g)^3} = \sqrt[3]{(\omega^2 g)^3}$ ja $h = \sqrt[3]{h^3} = \sqrt[3]{(\omega h)^3} = \sqrt[3]{(\omega^2 h)^3}$ voidaan korvata nyt käytetyillä termeillä. Tästä voidaan siis muodostaa yhtälön kaksi muuta juurta. Merkitään juuria nyt termeillä u, v ja w, jolloin vastaavasti

$$u = g + h$$

$$v = \omega g + \omega^2 h$$
$$w = \omega^2 g + \omega h.$$

Otetaan esimerkki, missä ratkaistaan nämä kaikki kolme juurta.

Esimerkki 4.4. Esimerkki teoksesta [3], sivulta 148.
Ratkaistaan yhtälön $x^3 + 3x^2 + 9x + 14 = 0$ juuret. Jotta voimme käyttää ratkaisukaavaamme, tulee yhtälö ensin muuttaa muotoon $x^3 + qx + r = 0$. Tehdään sijoitus $x = y - b/3 = y - 1$, jolloin saadaan

$$(y-1)^3 + 3(y-1)^2 + 9(y-1) + 14 = 0$$
$$y^3 + 6y + 7 = 0.$$

Tämä yhtälö on nyt halutussa muodossa, missä $q = 6$ ja $r = 7$. Tällöin yksi ratkaisu yhtälöön on

$$u = \sqrt[3]{1/2(-r + \sqrt{r^2 + 4q^3/27})} + \sqrt[3]{1/2(-r - \sqrt{r^2 + 4q^3/27})}$$

$$u = \sqrt[3]{1/2(-7 + \sqrt{49 + 32})} + \sqrt[3]{1/2(-7 - \sqrt{49 + 32})} = \sqrt[3]{1} + \sqrt[3]{-8} = -1.$$

Tämä ratkaisu on helppo saada myös kokeilemalla tai yhtälöä tutkimalla. Edellisten tietojen perusteella voidaan nyt myös muodostaa kaksi muuta juurta. Nyt $g = 1$, $h = -2$, $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ ja $\omega^2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$, jolloin yhtälön juuret v ja w ovat

$$v = \omega g + \omega^2 h = -\frac{1}{2} + i\frac{\sqrt{3}}{2} + 1 + i\sqrt{3}$$
$$v = \frac{1}{2} + \frac{3}{2}\sqrt{3}i$$

$$w = \omega^2 g + \omega h = -\frac{1}{2} - i\frac{\sqrt{3}}{2} + 1 - i\sqrt{3}$$
$$w = \frac{1}{2} - \frac{3}{2}\sqrt{3}i.$$

Nämä ovat siis juuret yhtälöön $y^3 + 6y + 7 = 0$, jolloin alkuperäisen yhtälön $x^3 + 3x^2 + 9x + 14 = 0$ juuret saadaan takaisin sijoittamalla $(y - 1 = x)$:

$$u_x = -1 - 1 = -2$$
$$v_x = \frac{1}{2} + \frac{3}{2}\sqrt{3}i - 1 = -\frac{1}{2} + \frac{3}{2}\sqrt{3}i$$

$$w_x = \frac{1}{2} - \frac{3}{2}\sqrt{3}i - 1 = -\frac{1}{2} - \frac{3}{2}\sqrt{3}i.$$

Nyt kun yhtälön juuret ovat selvillä, voidaan toisen asteen yhtälön tavoin määrittää sille diskriminantti.

Määritelmä 4.5. Olkoon yhtälön $x^3 + qx + r = 0$ juuret u, v ja w. Lisäksi olkoon

$$\Delta = (u - v)(u - w)(v - w).$$

Tällöin termiä Δ^2 kutsutaan kolmannen asteen yhtälön *diskriminantiksi*.

Koska kolmannen asteen yhtälö on hieman haastavampaa käsitellä ja ymmärtää, niin osoitetaan kolmannen asteen yhtälön diskriminantin arvo lauseen avulla.

Lause 4.6. *Olkoon yhtälön $x^3 + qx + r = 0$ juuret u, v ja w. Tällöin yhtälön diskrimantti on*

$$\Delta^2 = -27r^2 - 4q^3.$$

Todistus. Todistus luentomonisteesta [1] sivulta 27.
Määritelmän 4.5 perusteella $\Delta = (u - v)(u - w)(v - w)$. Lasketaan tulon termit erikseen. Siis ensimmäinen termi on

$$\begin{aligned} u - v &= g + h - \omega g - \omega^2 h \\ &= g(1 - \omega) - \omega^2 h(1 - \omega) \\ &= (1 - \omega)(g - \omega^2 h), \end{aligned}$$

toinen termi on

$$\begin{aligned} u - w &= g + h - \omega^2 g - \omega h \\ &= g(1 - \omega^2) - \omega h(1 - \omega^2) \\ &= (1 - \omega^2)(g - \omega h) \\ &= -\omega^2(1 - \omega)(g - \omega h) \end{aligned}$$

ja kolmas termi on

$$\begin{aligned} v - w &= \omega g + \omega^2 h - \omega^2 g - \omega h \\ &= \omega[g + \omega h - \omega g - h] \\ &= \omega(1 - \omega)(g - h). \end{aligned}$$

Yhdistämällä nämä, saadaan

$$\Delta = (1-\omega)(g-\omega^2 h)(-\omega^2(1-\omega)(g-\omega h))(\omega(1-\omega)(g-h))$$

$$= -\omega^3(1-\omega)^3(g-h)(g-\omega h)(g-\omega^2 h)$$

$$= -(1-3\omega+3\omega^2-\omega^3)(g-h)(g-\omega h)(g-\omega^2 h)$$

$$= -[1-3(-\frac{1}{2}-i\frac{\sqrt{3}}{2})+3(-\frac{1}{2}+i\frac{\sqrt{3}}{2})-1](g-h)(g-\omega h)(g-\omega^2 h)$$

$$= 3\sqrt{3}i(g-h)(g-\omega h)(g-\omega^2 h).$$

Nyt termin ω ominaisuuksien vuoksi $g^3-h^3 = (g-h)(g-\omega h)(g-\omega^2 h)$. Tämä voidaan myös ajatella kolmannen asteen yhtälönä luvun g suhteen, jolla on juuret $g_1 = h$, $g_2 = \omega h$ ja $g_3 = \omega^3 h$. Tästä seuraa

$$\Delta = 3\sqrt{3}i(g^3-h^3)$$

$$\Delta = 3\sqrt{3}i\sqrt{r^2+\frac{4q^3}{27}},$$

jolloin edelleen

$$\Delta^2 = -27r^2 - q^3.$$

□

Kuten toisen asteen tapauksessa, diskriminantin arvo on yhteydessä juurien arvoihin. Kolmannen asteen yhtälö kuitenkin poikkeaa toisesta asteesta; kolmannen asteen yhtälöllä on aina vähintään yksi reaalinen juuri, riippumatta diskriminantin arvosta. Osoitetaan kolmannen asteen yhtälön diskriminantin arvoon liittyvä lause:

Lause 4.7. *Polynomin x^3+qx+r kaikki nollakohdat ovat reaalisia, jos ja vain jos diskriminantti on positiivinen eli $\Delta^2 \geq 0$.*

Todistus. Todistus luentomonisteesta [1] sivulta 27.
Mikäli kaikki juuret u, v ja w ovat reaalisia, niin silloin $\Delta = (u-v)(u-w)(v-w)$ on reaalinen ja siten myös $\Delta^2 \geq 0$. Tarkastellaan siis tapausta, missä jokin juurista ei ole reaalinen. Olkoon yhtälön juuri w muotoa $w = s+ti$, missä $t, s \in \mathbb{R}$ ja $t \neq 0$. Tällöin toinen juurista on muotoa $v = s-ti$ ja kolmas juuri u on reaalinen, sillä kuten aiemmin todettiin, on kolmannen asteen polynomilla aina vähiintään yksi reaalinen juuri. Lasketaan nyt diskriminantin arvo.

$$\Delta = (u-v)(u-w)(v-w) = [u-(s-ti)][u-(s+ti)](-2ti)$$

$$\Delta = [(u-s)+ti][(u-s)-ti](-2ti) = [(u-s)^2-(ti)^2](-2ti),$$

jolloin saadaan

$$\Delta^2 = [(u-s)^2 + t^2]^2(-2ti)^2.$$

Nyt nähdään, että kaikki neliötermit viimeistä lukuunottamatta ovat positiivisia, sillä ne sisältävät vain reaalisia lukuja. Viimeinen termi on kuitenkin negatiivinen, sillä $i^2 = -1$. Tällöin siis $\Delta^2 \leq 0$.

□

Kuten toisen asteen yhtälöissä, on kolmannen asteen yhtälöissä diskriminantin arvo $\Delta^2 = 0$ poikkeuksellinen. Tällöin polynomilla on moninkertainen nollakohta. Tämä ei kuitenkaan kerro, onko nollakohta kaksin- vai kolminkertainen, kuten seuraava esimerkki näyttää.

Esimerkki 4.8. Polynomin $f(x) = (x-1)(x-1)(x+2) = x^3 - 3x + 2$ diskriminantti on $\Delta^2 = -27 \cdot 2^2 - 4 \cdot (-3)^3 = 0$. Tulomuodosta nähdään, että nollakohta $x = 1$ on kaksinkertainen.
Polynomin $g(x) = (x-0)(x-0)(x-0) = x^3$ diskriminantti on myös $\Delta^2 = -27 \cdot 0^2 - 4 \cdot 0^3 = 0$. Tulomuodosta nähdään, että nollakohta $x = 0$ on kolminkertainen.

4.3 Neljäs aste

Tässä kappaleessa mukaillaan pääasiassa teoksen [2] esitystapaa.

Neljännen asteen polynomi on muotoa $f(y) = ay^4 + by^3 + cy^2 + dy + e$ ja siitä johdettu neljännen asteen yhtälö on muotoa $y^4 + by^3 + cy^2 + dy + e = 0$. Kerroin a on tässä nyt jätetty pois, sillä yksinkertaisesti jakamalla se voidaan supistaa yhtälöstä pois. Edelleen sijoittamalla $y = x - b/4$ yhtälöstä saadaan

$$(x-b/4)^4 + b(x-b/4)^3 + c(x-b/4)^2 + d(x-b/4) + e = 0$$

$$x^4 - bx^3 + \frac{3b^2x^2}{8} - \frac{b^3x}{16} + \frac{b^4}{256} + bx^3 - \frac{3b^2x^2}{4} + \frac{3b^3x}{16} - \frac{b^4}{64} + cx^2 - \frac{bcx}{2} + \frac{b^2c}{16} + dx - \frac{bd}{4} + e = 0$$

$$x^4 + \frac{8c - 3b^2}{8}x^2 + \frac{3b^2 - b^3 - 8bc + 16d}{16}x + \frac{16b^2c - 3b^4 - 64bd + 256e}{256} = 0,$$

eli kolmannen asteen termi supistui pois. Tällöin riittää tarkastella neljännen asteen yhtälöistä tapausta, jotka ovat muotoa

$$x^4 + qx^2 + rx + s = 0.$$

Pyritään jakamaan tämä vaillinnainen neljännen asteen polynomi tekijöihin. Merkitään

$$x^4 + qx^2 + rx + s = (x^2 + jx + l)(x^2 + jx + m)$$

$$= x^4 + (m + l - j^2)x^2 + (jm - jl)x + ml,$$

jolloin vertaamalla termejä saadaan yhtälöryhmä

$$\begin{cases} m + l - j^2 = q \\ jm - jl = r \\ ml = s, \end{cases} \tag{1}$$

josta termit m, l ja j on mahdollista ratkaista annettujen termien q, r ja s suhteen. Ratkaistaan kahdesta ylemmästä yhtälöstä termi m, jotka yhteenlaskemalla saadaan:

$$\begin{cases} m = q - l + j^2 \\ m = l + r/j \\ \hline 2m = q + j^2 + r/j \end{cases} \tag{2}$$

Vastaavasti myös muuttujan l suhteen:

$$\begin{cases} l = q - m + j^2 \\ l = m - r/j \\ \hline 2l = q + j^2 - r/j \end{cases} \tag{3}$$

Sijoittamalla tämän nyt yhtälöryhmän alimpaan yhtälöön saadaan

$$s = ml$$

$$4s = 2m2l$$

$$4s = (q + j^2)^2 - (r/j)^2$$

$$q^2 + 2qj^2 + j^4 - 4s - \frac{r^2}{j^2} = 0$$

$$j^6 + 2qj^4 + (q^2 - 4s)j^2 - r^2 = 0.$$

Tämän kolmannen asteen yhtälön ratkaisuna saadaan selville j^2 ja sitä kautta j sekä yhtälöryhmän muuttujat m ja l. Tämän jälkeen yhtälön ratkaisuun tarvitsee ratkaista vain toisen asteen yhtälöt $x^2+jx+l = 0$ ja $x^2-jx+m = 0$.

Koska kolmannenkin asteen yhtälön ratkaisu on pitkä, tulisi neljännen asteen yhtälön ratkaisusta vielä moninkerroin pidempi. Tämän vuoksi yhtälön eksplisiittistä ratkaisua ei esitetä. Näytetään kuitenkin esimerkillä, miten ratkaisu saataisiin tehtyä.

Esimerkki 4.9. Esimerkki teoksesta [2], sivulta 358.
Tarkastellaan yhtälöä $x^4 - 2x^2 + 8x - 3 = 0$, missä kolmannen asteen termi on jo hävitetty yhtälöstä. Jaetaan tämä yhtälö nyt kahteen toisen asteen termiin, kuten aiemmin, jolloin saadaan

$$x^4 - 2x^2 + 8x - 3 = (x^2 + jx + l)(x^2 + jx + m)$$

$$= x^4 + (m + l - j^2)x^2 + (jm - jl)x + ml,$$

mistä voidaan muodostaa yhtälöryhmä. Se on nyt muotoa

$$\begin{cases} m + l - j^2 = -2 \\ jm - jl = 8 \\ ml = -3, \end{cases}$$

mistä edelleen voidaan muodostaa, kuten aiemmin, kolmannen asteen yhtälö muuttujan j^2 suhteen.

$$j^6 + 2qj^4 + (q^2 - 4s)j^2 - r^2 = 0$$

$$j^6 - 4j^4 + 16j^2 - 64 = 0$$

Nyt voitaisiin ensin poistaa toisen asteen termi suorittamalla muuttujan vaihto $j^2 = y + 4/3$, jolloin yhtälö olisi muotoa

$$y^3 + \frac{32}{3}y - \frac{1280}{27}$$

ja josta edelleen saataisiin, diskriminantin $\Delta^2 = -27r^2 - 4q^3 = -65536$ ollessa negatiivinen, saadaan ainoaksi reaalijuureksi

$$u = \sqrt[3]{1/2\left(\frac{1280}{27} + \sqrt{\frac{1280^2}{27^2} - \frac{4 \cdot 32^3}{27 \cdot 3^3}}\right)} + \sqrt[3]{1/2\left(\frac{1280}{27} - \sqrt{\frac{1280^2}{27^2} - \frac{4 \cdot 32^3}{27 \cdot 3^3}}\right)}$$

$$u = 8/3,$$

joka takaisinvaihdon kautta antaa tulokseksi $j^2 = 8/3 + 4/3 = 4$. Tämä vastaus saadaan kuitenkin ehkä helpommin kokeilemalla.

Nyt sijoittamalla tämä arvo yhtälöryhmään saadaan yhtälöpari

$$\begin{cases} m + l - 4 = -2 \\ ml = -3, \end{cases}$$

mistä edelleen muodostuu toisen asteen yhtälö $l^2 - 2l - 3 = 0$, josta $l = 1 \pm 2$. Valitsemalla $l = 3$ seuraa, että $m = -1$, kun taas toisinpäin tehty valinta

tuottaa päinvastaisen tuloksen. Valinnasta riippuen j on joko positiivinen tai negatiivinen. Valinta $l = 3$ tekee yhtälöryhmän keskimmäisen yhtälön perusteella muuttujasta j negatiivisen, jolloin

$$\begin{cases} m = -1 \\ l = 3 \\ j = -2. \end{cases}$$

Tällöin alkuperäinen yhtälö saa muodon

$$x^4 - 2x^2 + 8x - 3 = (x^2 - 2x + 3)(x^2 + 2x - 1) = 0,$$

mistä toisen asteen yhtälöt voidaan ratkaista helposti.
Yhtälöstä $x^2-2x+3 = 0$ saadaan ratkaisuiksi $x_1 = 1+\sqrt{2}i$ ja $x_2 = 1-\sqrt{2}i$ ja yhtälöstä $x^2+2x-1 = 0$ saadaan ratkaisuiksi $x_3 = -1+\sqrt{2}$ ja $x_4 = -1-\sqrt{2}$. Nämä neljä juurta ovat siis alkuperäisen yhtälön neljä nollakohtaa.

Myös neljännen asteen yhtälölle on mahdollista määrittää diskriminantti, mutta koska emme määrittäneet eksplisiittistä ratkaisua neljännen asteen yhtälölle, jätämme myös diskriminantin määrityksen pois.

4.4 Trigonometriaan perustuva ratkaisu

Tämä kappaleen mukailee teoksen [2] esitystapaa.

Kolmannen asteen yhtälön juuret ovat joskus hyvin hankalia, jos ne ratkaistaan klassisella ratkaisukaavalla. Seuraava on tästä hyvä esimerkki.

Esimerkki 4.10. Esimerkki teoksesta [2], sivulta 355.
Ratkaistaan yhtälö $x^3 - 7x + 6 = 0$ ratkaisukaavalla. Nyt $q = -7$ ja $r = 6$, mistä edelleen

$$g^3 = 1/2(-r+\sqrt{r^2 + 4q^3/27}) = 1/2(-6+\sqrt{36 - 1372/27}) = -3+\sqrt{-100/27}$$

$$h^3 = 1/2(-r - \sqrt{r^2 + 4q^3/27}) = -3 - \sqrt{-100/27})$$

jolloin ratkaisut ovat

$$u = g + h = \sqrt[3]{-3 + \sqrt{-100/27}} + \sqrt[3]{-3 - \sqrt{-100/27}}.$$

$$v = \omega g+\omega^2 h = (-\frac{1}{2}+i\frac{\sqrt{3}}{2})\sqrt[3]{-3 + \sqrt{-100/27}}+(-\frac{1}{2}-i\frac{\sqrt{3}}{2})\sqrt[3]{-3 - \sqrt{-100/27}}$$

$$w = \omega^2 g + \omega h = (-\frac{1}{2} - i\frac{\sqrt{3}}{2})\sqrt[3]{-3 + \sqrt{-100/27}} + (-\frac{1}{2} + i\frac{\sqrt{3}}{2})\sqrt[3]{-3 - \sqrt{-100/27}}$$

Nämä ratkaisut ovat hyvin monimutkaisen näköisiä, mutta todellisuudessa ne ovat kokonaislukuja. Tämä johtuu siitä, että yhtälö voidaan kirjoittaa sen tulomuodossa seuraavasti:

$$x^3 - 7x + 6 = (x - 1)(x - 2)(x + 3) = 0$$

Tällöin juuret u, v ja w vastaavat lukuja 1, 2 ja -3, ei tosin välttämättä tässä järjestyksessä.

Yksi tapa kiertää tälläiset hankalat kompleksiluvut on käyttää trigonometrista lähestymistapaa. Mikäli kolmannen asteen yhtälön kaikki juuret ovat reaalisia, voidaan juurien arvoa approksimoida lauseen 4.12 avulla. Todistetaan tätä lausetta varten ensin seuraava lemma. Trigonometriset lauseet otetaan todistamatta käyttöön.

Lemma 4.11. *Olkoon kolmannen asteen polynomi* $f(y) = y^3 - 3/4y - 1/4cos(3\theta)$. *Tämän polynomin juuret ovat* $cos\theta$, $cos(\theta{+}120°)$ *ja* $cos(\theta{+}240°)$.

Todistus. Tiedetään, että

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

Tästä seuraa suoraan, että yksi polynomin juurista on $cos\theta$, sillä sijoitus $y = cos\theta$ tuottaa yhtälön $cos^3\theta - 3/4cos\theta - 1/4cos(3\theta) = 0$ joka on yhtäpitävä yhtälön 4 kanssa. Koska

$$cos(3\theta) = cos(3\theta + 360°) = cos(3(\theta + 120°)) = cos(3(\theta + 240°)),$$

niin myös $cos(\theta + 120°)$ ja $cos(\theta + 240°)$ kelpaavat juuriksi. □

Nyt voidaan muotoilla trigonometriset juuret antava lause.

Lause 4.12. *Olkoon* $f(x) = x^3 + qx + r$ *kolmannen asteen polynomi, jonka kaikki juuret ovat reaalisia, eli* $27r^2 + 4q^3 \leq 0$. *Mikäli* $t = \sqrt{-4q/3}$ *ja* $cos3\theta = -4r/t^3$, *niin yhtälön juuret ovat* $tcos\theta$, $tcos(\theta + 120°)$ *ja* $tcos(\theta + 240°)$.

Todistus. Olkoon v eräs polynomin $f(x)$ juurista. Jos merkitään $v = tu$, niin voidaan annettu polynomi muuttaa yhtälöksi

$$u^3 + \frac{q}{t^2}u + \frac{r}{t^3} = 0.$$

Jos nyt voimme valita muuttujan t siten, että

$$\frac{q}{t^2} = -\frac{3}{4}$$

ja

$$\frac{r}{t^3} = -\frac{1}{4}cos(3\theta)$$

jollakin θ arvolla, niin silloin Lemman 4.11 nojalla yhtälön juuret ovat $cos\theta$, $cos(\theta + 120°)$ ja $cos(\theta + 240°)$. Lisäksi, koska $v = tu$, on alkuperäisen polynomin juuret silloin $v = tcos\theta$, $tcos(\theta + 120°)$ ja $tcos(\theta + 240°)$.
Ensimmäisestä muuttujan t ehdosta seuraa nyt

$$t = \sqrt{\frac{-4q}{3}}.$$

Tämä luku on nyt reaaliluku, sillä oletuksen ehdosta $27r^2 + 4q^3 \leq 0$ seuraa se, että $q \leq 0$ ja $-\frac{4q}{3} \geq 0$.
Toinen muuttujan t ehto muokkautuu muotoon

$$\frac{-4r}{t^3} = cos(3\theta),$$

mikä on määritelty vain ja ainoastaan, kun $|-4r/t^3| \leq 1$. Osoitetaan se siis todeksi. Oletuksesta saadaan $27r^2 \leq -4q^3$ eli $9r^2/q^2 \leq -4q/3$. Tästä edelleen voidaan johtaa

$$\left|\frac{3r}{q}\right| \leq \sqrt{\frac{-4q}{3}} = t,$$

koska $t^2 = -4q/3$ ja $t = \sqrt{-4q/3}$. Tällöin

$$\left|\frac{-4r}{t^3}\right| = \left|\frac{-4r}{(-4q/3)t}\right| = \left|\frac{3r}{qt}\right| \leq \frac{t}{t} = 1,$$

kuten pyrittiinkin osoittamaan. Nyt siis on löydetty sellainen t joka muuttaa yhtälön muotoon, jonka juuret saadaan Lemman 4.11 nojalla. □

Kokeillaan tätä lausetta nyt esimerkkiin 4.10.

Esimerkki 4.13. Esimerkki teoksesta [2], sivuilta 360 ja 361.
Ratkaistaan kolmannen asteen yhtälön $x^3 - 7x + 6 = 0$ juuret trigonometrisesti. Lasketaan ensin t ja θ, käyttäen likiarvoja. Nyt

$$t = \sqrt{-4q/3} = \sqrt{28/3} \approx 3,055$$

ja tätä likiarvoa hyväksikäyttäen voimme laskea likiarvon $cos(3\theta)$

$$cos(3\theta) = -\frac{4r}{t^3} \approx -\frac{24}{3,055^3} \approx -0,842,$$

mistä edelleen voimme laskea likiarvon muuttujalle θ

$$3\theta \approx 148°$$

$$\theta \approx 49°.$$

Koska tiedämme esimerkistä 4.10 yhtälön juurien olevan reaalisia, voimme lauseen 4.12 perusteella ilmoittaa juurien likiarvot.

$$u \approx 3,055cos49° \approx 2,00$$

$$v \approx 3,055cos169° \approx -3,00$$

$$w \approx 3,055cos289° \approx 1,00$$

Trigonometrinen approksimointi on siis huomattavan näppärä tapa selvittää juurien arvot verrattuna klassiseen ratkaisukaavaan.

4.5 Viides aste

Tämä kappale noudattaa luentomonisteen ja luentomuistiinpanojen [1] esitystapaa.
Viidennen asteen yhtälö voidaan merkitä tutussa muodossa $ax^5+bx^4+cx^3+dx^2+ex+f = 0$. Tästä muodosta voidaan jälleen poistaa jakamalla kerroin a ja sitten toiseksi korkeinta astetta oleva termi sijoituksella $x = y-b/5$, jolloin yhtälö saadaan muotoon $x^5+px^3+qx^2+rx+s = 0$. Edellisten ratkaisukaavojen muodostamisen perusteella voisi olettaa, että ratkaisu löytyy nyt jollakin ovelalla sijoittamisella tai yhtälön pyörittelyllä, mutta todellisuudessa näin ei voida tehdä. Viidennen asteen yhtälölle ei ole olemassa klassista ratkaisukaavaa. Myöskään korkeammille kuin viidennen asteen yhtälöille ei yleisiä ratkaisukaavoja ole olemassa. Tämän pätevä perusteleminen vaatii Galois'n teoriaa, mitä tähän tutkielmaan ei ole tarkoitus sisällyttää. Todettakoon asia kuitenkin lyhyesti.

Klassinen ratkaisukaava polynomille on mahdollista tuottaa, jos polynomi $f(x)$ on juuriratkeava. Tätä varten täytyy olla mahdollista tehdä polynomin $f(x)$ Galois'n ryhmälle aliryhmien ketju, jossa peräkkäisten aliryhmien tekijäryhmä on aina syklinen. Jaottomilla viidennen asteen polynomeilla syntyy tekijäryhmä $A_5/(1)$, mikä ei alternoivien ryhmien teorian perusteella ole syklinen. Tämän takia polynomi $f(x)$ ei ole juuriratkeava, eikä näin ollen viidennen asteen yhtälöille ole mahdollista muodostaa klassista ratkaisukaavaa.

Esimerkki 4.14. Polynomi $f(x) = x^5 - 6x + 3$ on Eisensteinin kriteerin (lause 3.5) nojalla jaoton, sillä alkuluku $p = 3$ jakaa luvun 6 ja 3, muttei lukua 1 ja lisäksi $p^2 = 9 \nmid 3$. Osoittautuu, että polynomin $f(x)$ Galois'n ryhmä on symmetrinen ryhmä S_5. Tämän vuoksi polynomi $f(x)$ ei ole juuriratkeava.

Kolmannen ja neljännen asteen polynomeilla tälläinen Galois'n ryhmälle muodostuva aliryhmien ketju, jonka tekijäryhmät ovat syklisiä on mahdollista muodostaa, siksi kolmannen ja neljännen asteen polynomeille oli mahdollista muodostaa ratkaisukaava.

5 Yhtälöiden historiaa

Tämä kappale etenee teoksen [4] mukaisesti.

5.1 Ensimmäinen ja toinen aste

Yhtälöiden ratkaisemisella on pitkä historia. Ensimmäisen asteen yhtälöitä on ratkottu jo ainakin muinaisessa Egyptissä, 5000 vuotta sitten. Kyseiset yhtälöt ovat yleisesti olleet typpiä $x + ax = b$ tai $x + ax + bx = c$. Tälläisiin tehtäviin on aina liittynyt jokin käytännön ongelma tai sanallinen selitys. Esimerkiksi yhtälö $x + \frac{1}{7}x = 19$ on sanallisesti esitetty 'Mikä on kasan arvo, jos kasa ja sen seitsemäsosa on 19'. Ratkaisua on haettu ensin väärällä arvolla arvaamalla, jonka jälkeen yhtälön vasenta puolta on verrattu yhtälön oikeaan puoleen. Tämän jälkeen vasenta puolta on kerrottu sopivalla luvulla jotta päästään haluttuun arvoon, jolloin myös arvausta on kerrottu samalla luvulla, saaden näin oikea vastaus. Myös toisen asteen yhtälöitä voidaan egyptiläisten ajatella ratkaisseen, tosin vain vaillinnaisia sellaisia. Tehtävät olivat geometrisia, yleensä neliöiden ja ympyröiden pinta-alojen laskemista missä esiintyi neliötermejä.

Seuraava suuri edistysaskel algebrassa ja yhtälöiden ratkaisemisessa sijoittuu Babyloniaan, aikakaudelle 2000-600 eKr. Babylonialaiset olivat nimittäin onnistuneet selvittämään toisen asteen yhtälön ratkaisukaavan. Babylonialaisten tapa lähestyä algebraa, kuten egyptiläistenkin, oli puhtaan käytännöllinen. Vastaukset ongelmiin katsottiin taulukoista, joihin oli ennalta laskettu tulokset eri muuttujan arvoilla. Mikäli vastaus oli taulukon arvojen välistä, käytettiin interpolointia. Myös likiarvot olivat babylonialaisten suosiossa, sillä toisin kuin egyptiläisillä, heidän 60-paikkajärjestelmänsä salli myös desimaalien käytön.

Koska Babyloniassa, kuten ei vielä pitkään aikaan yleisestikkään, hyväksytty negatiivisia lukuja, olivat toisen asteen yhtälöt jotakin seuraavista kol-

mesta muodosta (lukujen p ja q ollessa positiivisia):

$$x^2 + px = q$$

$$x^2 = px + q$$

$$x^2 + q = px$$

Babylonialaiset olivat kehittäneet näille yhtälöille ratkaisukaavan. Meidän merkintätavallamme ratkaisu on $x = \sqrt{(p/2)^2 + q} + p/2$, joka vastaa edellisistä yhtälöistä keskimmäistä tapausta. Babylonialaiset olivat myös taitavia yhtälöiden pyörittäjiä. Sellaiset tapaukset kuten $11x^2 + 7x = a$ eivät tuottaneet ongelmia, vaan niistä selvittiin hämmästyksellisesti muuttujan vaihdon avulla. Yhtälö ensin kerrottiin toisen asteen termin kertoimella, jonka jälkeen termi $11x$ korvattiin muuttujalla y, joka ratkaistiin.

$$(11x)^2 + 7 \cdot 11x = 11a \Leftrightarrow y^2 + 7y = 11a$$

Tämän jälkeen alkuperäinen x voitiin ratkaista yhtälöstä $11x = y$.

Babylonialaiset osasivat myös ratkoa vaillinnaisia kolmannen asteen yhtälöitä. Yhtälöihin $x^3 = a$ ja $x^3 + x^2 = a$ voitiin katsoa ratkaisut valmiista taulukoista. Kuten aiemmin todettiin, eivät termien kertoimet olleet ongelmallisia, vaan niistä päästiin sijoitusmenetelmällä eroon. Vaikkakin babylonialaiset osasivat käyttää sijoitusmenetelmäänsä hyvin, ei ole varmuutta siitä, että he olisivat osanneet hyödyntää sitä täydelliseen kolmannen asteen yhtälöön. Periaatteessa ei ole vaikeaa sijoittaa sopivaa termiä nelitermiseen yhtälöön muodostaen siitä kolmitermisen, jonka he selvästi osasivat ratkaista. Sijoitusmenetelmää osattiin kuitenkin soveltaa myös esimerkiksi yhtälöön $x^8 + px^4 = q$, muuttaen se toisen asteen yhtälöksi sijoituksella $y = x^4$. Tälläinen korkeampien asteiden yhtälöiden ratkaiseminen, millä ei ollut tuohon aikaan mitään käytännön sovellutusta, kertoo korkeasta matematiikan osaamisesta ja kiinnostuksesta.

5.2 Kolmas ja nejäs aste

Yhtälöiden ratkaisemisen taito pysyi tällä tasolla pitkään. Vasta 1500-luvulla otettiin seuraava edistysaskel, nimittäin kolmannen asteen yhtälön ratkaisukaavan löytyminen. Tämän ratkaisun esitti julkisesti ensimmäisen kerran italialainen Geronimo Cardano (1501-1576) teoksessaan *Ars Magna* vuonna 1545, yhdessä neljännen asteen yhtälön ratkaisukaavan kanssa. Cardano ei itse keksinyt näitä ratkaisuja, kuten hän itsekkin teoksessaan ilmoittaa, vaikkakin kolmannen asteen yhtälön ratkaisu

$$u = \sqrt[3]{1/2(-r + \sqrt{r^2 + 4q^3/27})} + \sqrt[3]{1/2(-r - \sqrt{r^2 + 4q^3/27})}.$$

tunnetaan nykyäänkin nimellä *Cardanon kaava*. Kappaleissa 4.2 ja 4.3 esitetyt ratkaisut mukailevat tuon ajan ratkaisutapaa löyhästi.

Kolmannen asteen yhtälön ratkaisukaavan uskotaan löytäneen ensimmäisenä Scipione del Ferro (1465-1526), joka toimi Bolognan yliopiston matematiikan professorina. Hän ei julkaissut ratkaisuaan, mutta paljasti sen eräälle oppilaistaan, Antonio Maria Fiorille, ennen kuolemaansa. Sana kiiri kolmannen asteen yhtälön ratkaisemisesta, mikä innoitti myös Niccolo Tartagliaa (1500-1557) ratkaisun löytämiseen. Hän saikin, ei välttämättä täysin omin avuin, mutta kuitenkin sai muodostettua itsekin ratkaisun. Myös tästä alkoi sana leviämään, mikä innoitti Fiorin ja Tartaglian kisaamaan aiheesta. He muodostivat toisilleen kolmannen asteen yhtälöitä ratkaistaviksi, mitkä heidän tuli tietyssä ajassa ratkaista. Tartaglia voitti kisan ylivoimaisesti, johtuen hänen erilaisesta ratkaisukaavastaan. Fior osasi ratkaista vain muotoa $x^3 + qx = r$ olevat yhtälöt, kun taas Tartaglia hallitsi myös yhtälöt, jotka olivat muodossa $x^3 + qx^2 = r$. Mahdollisesti Tartaglia osasi muuttaa kappaleessa 4.2 olevan esityksen tavoin yhtälön muotoon, missä toisen asteen termiä ei ole. Cardanon kuultua Tartaglian menestyksestä, hän kutsui hänet luokseen. Cardano oli menestyvä lääkäri, joka oli taitava usealla tieteen alalla, kun taas Tartaglia oli, lapsena saadun vamman vuoksi, puhevikainen ja heikommassa sosiaalisessa asemassa. Erinäisten lupausten saattelemana Cardano sai kolmannen asteen yhtälön ratkaisun Tartaglialta, minkä Tartaglia aikoi myöhemmin sisällyttää algebralliseen tutkimukseensa. Cardano kuitenkin rikkoi lupauksensa ja julkaisi ratkaisun ennen Tartagliaa.

Neljännen asteen yhtälön ratkaisun Cardano sai apulaiseltaan Ludovico Ferrarilta (1522-1565). Ars Magnassa hän kertoo Ferrarin keksineen sen hänen pyynnöstään. Näillä ratkaisuilla oli suuri merkitys matematiikkaan. Ne olivat uutta edistystä tuhansia vuosia askarruttaneiden asioiden parissa. Erityisesti neljännen asteen yhtälöllä ei ollut enää käytännön sovellutusta kolmiulotteisessa maailmassamme, joten siksi tätä kutsutaankin nykyaikaisen matematiikan aluksi. Tästä alkanut algebran tutkimisen kiihko toikin paljon uutta matematiikkaa. Esimerkin 4.10 antamat ratkaisut ovat tästä hyvä esimerkki. Cardano ei voinut ymmärtää, miten aikasemmin epätodellisina hylätyt tapaukset neliöjuuren sisällä olevista negatiivisista luvuista saattoivatkin tuotaa kokonaislukuja. Negatiivisten lukujen ja imaginäärilukujen kehitys pääsi etenemään tällaisen huomion kautta.

5.3 Viides aste ja Galois'n teoria

Luonnollisesti useat matemaatikot yrittivät tästä innottuneina löytää viidennen asteen yhtälön ratkaisukaavaa, turhaan. Kuten totesimme, viidennen asteen yhtälöille ei ratkaisukaavaa ole olemassa. Tämän todisti ensimmäisenä

riittävän tarkasti Niels Abel vuonna 1824, yrittäessään ratkaista viidennen asteen yhtälöä. Myös aikaisempi todistus tästä löytyy vuodelta 1799, joka oli Paolo Ruffinin käsialaa, mutta mitä ei kelpuutettu riittäväksi todistukseksi. Tästä löydöstä innostuneena Évariste Galois (1812-1832) intoutui tutkimaan abstraktia algebraa. Useat vastoinkäymiset kuitenkin varjostivat Galois'n elämää; hänen opiskeluhakemuksensa hylättiin toistuvasti, hänen julkaistaviksi tarkoitetut tutkimukset joko hävisivät tai ne palautettiin julkaisukelvottomina, hänen isänsä teki itsemurhan ja hän joutui viettämään useita kuukausia vankilassa. Vuonna 1832 hänet haastettiin kaksintaisteluun, joka johti hänen kuolemaansa, Galois'n ollessa vasta kahdenkymmenen vuoden iässä. Hänen tutkimuksensa olivat, yhdessä muiden matematikkojen kanssa, hyvin merkittäviä 1800-luvun algebran kehitykselle. Galois'n mukaan nimetty teoria pystyikin todistamaan yleisesti ratkeavuuden ja sitä kautta ratkaisukaavan olemassaolon, yhtälön asteesta riippumatta. Hänen teoriat saivatkin ansaitsemansa arvostuksensa vasta kauan hänen kuolemansa jälkeen; ensimmäinen hänen työstämänsä teoria julkaistiinkin vasta 1846.

Lähdeluettelo

[1] J. Kauppi (toim.): *Algebra II*. Oulu: Oulun yliopiston Matemaattisten tieteiden laitoksen julkaisuja, 2008.

[2] J. J. Rotman: *A First Course In Abstract Algebra*, second edition. Upper Saddle River, New Jersey, USA: Prentice Hall, 2000.

[3] O. E. Nicodemi, M. E. Sutherland, G. W. Towsley: *An Introduction To Abstract Algebra With Notes To The Future Teacher*. Upper Saddle River, New Jersey, USA: Prentice Hall, 2007.

[4] C. B. Boyer: *A History Of Mathematics*. Princeton, New Jersey, USA: Princeton University Press, 1985.