Algebra 2

Syksy 2016

Kerkko Luosto
Informaatiotieteiden yksikkö, Tampereen yliopisto

I Johdanto: algebra ja yhtälöt

1. Koulualgebrasta algebraan

Koulun matematiikan opetuksen suurimpia abstraktiohyppäyksiä on siirtymä aritmetiikasta algebraan – tai kuten yliopistolla tarkemmin asia ilmaistaisiin, alkeisaritmetiikasta koulualgebraan. Hyppäyksen keskeinen piirre on symbolisten merkintöjen käyttöönotto: lukuihin ruvetaan viittaamaan kirjaimilla, mikä mahdollistaa yhtälömuotoisten ongelmien sujuvan ratkaisemisen. Koulualgebra onkin paitsi lausekkeiden manipulointia mitä suurimmassa määrin yhtälöiden ratkaisemista.

Tutkimusalgebrassa koulualgebran päälle tulee uusi abstraktiokerros, nimittäin algebralliset rakenteet, ja algebran alasta riippuu vahvasti, missä määrin yhtälöt ovat enää varsinaisia kiinnostuksen kerroksia. Kun siirtymää alkeisaritmetiikasta koulualgebraan voi perustella yhtälönratkaisun sujuvuudella, niin on syytä vastaavasti pohtia, ovatko algebralliset rakenteet yhtä helposti motivoitavissa. Naiivi vastaus olisi, että kun reaalilukujen tai kompleksilukujen järjestelmissä on käytettävissä algebrallisia menetelmiä tietynlaisten yhtälöiden ratkaisemiseksi, niin oltaisiin kiinnostuneita siitä, miten nämä tulokset yleistyvät muihin rakenteisiin.

Kouluopetuksen siirtymällä alkeisaritmetiikasta koulualgebraan on vastineensa matematiikan historiallisessa kehityskulussa, vaikkakaan kehitys ei ollut aivan suoraviivaista. Sen sijaan matematiikan historia ei lainkaan tue naiivia motivaatiota algebrallisten rakenteiden käyttöönotolle, vaan taustalla on syvällisempiä ja monisyisempiä tavoitteita, jotka paljastuvat vähitellen kurssin kuluessa. Toistaiseksi kehittelemme kuitenkin teoriaa naiivin selityksen näkökulmasta.

Jotta totutut tekniikat yhtälöiden ratkaisemiseksi onnistuisivat, algebrallisen rakenteen, jossa toimimme, pitää yleensä olla kunta.

1.1. Määritelmä. Kahden laskutoimituksen rakenne $(\mathsf{K}, +, \cdot)$ on *kunta*, jos

1) $(\mathsf{K}, +)$ on Abelin ryhmä, ns. *kunnan yhteenlaskuryhmä*,
2) $(\mathsf{K}^*, \cdot)$, jossa $\mathsf{K}^* = \mathsf{K} \setminus \{0\}$ ja 0 on yhteenlaskun neutraalialkio, on Abelin ryhmä (*kunnan kertolaskuryhmä*) ja

3) Yhteen- ja kertolasku osittelevat eli

$$\begin{aligned} &(x+y)z = xz + yz \qquad \text{(oikealta osittelu)} \\ \text{ja} \quad &x(y+z) = xy + xz \qquad \text{(vasemmalta osittelu).} \end{aligned}$$

kun $x, y, z \in K$.

Ensimmäisen asteen yhtälöt ratkeavat kunnissa totutulla tavalla, mutta heikommissa järjestelmissä eteen tulee kaikenlaisia ongelmia: yhtälöillä ei välttämättä ole ratkaisuja tai niitä voi olla useampia.

Tarkastellaan erityisesti toisen asteen perusmuotoisen yhtälön ratkaisemista reaalilukujen kunnassa. Olkoot $a, b \in \mathbb{R}$. Ratkaisu perustuu tunnetusti neliöksi täydentämiseen:

$$\begin{aligned} & x^2 + ax + b = 0 \\ \iff & x^2 + ax + a^2/4 = a^2/4 - b \\ \iff & (x + a/2)^2 = a^2/4 - b. \end{aligned}$$

Jo reaalilukujen kunnassa törmätään nyt siihen ongelmaan, että reaaliluvun neliö on epänegatiivinen, joten jos $a^2/4 - b < 0$, niin yhtälöllä ei ole ratkaisuja. Jos sen sijaan $a^2/4 - b \geqslant 0$, niin on olemassa jopa epänegatiivinen $u \in \mathbb{R}$, jolle $u^2 = a^2/4 - b$ (nimittäin $u = \sqrt{a^2/4 - b}$), ja ratkaisut ovat $x = -a/2 \pm u$. Edellä esitetty diskrimaatin positiivisuusongelma selittää mitä suurimmassa määrin tarvetta kompleksilukujen käyttöön matematiikassa.

Kun toisen asteen yhtälön ratkaisemista yritetään yleistää muihin kuntiin, paljastuu toinenkin ongelma: Kunnassa on mahdollista, että $1 + 1 = 0$; tällaisia kuntia kutsutaan karakteristikaa 2 oleviksi kunniksi. Tällöin kaikille kunnan alkioille x ja t pätee

$$(x + t)^2 = x^2 + xt + tx + t^2 = x^2 + (1 + 1)xt + t^2 = x^2 + 0 \cdot xt + t^2 = x^2 + t^2.$$

Tällaisissa kunnissa neliöksi täydentäminen on siis mahdotonta muissa kuin triviaalissa tapauksessa $a = 0$.

Korkeampiasteisiin yhtälöihin siirryttäessä tilanne muuttuu edelleen monimutkaisemmaksi. Monivuosisatainen tavoite oli johtaa näille yhtälöille juurtamiseen perustuvia ratkaisukaavoja. Renessanssin aikana tämä onnistuikin kolmannen ja neljännen asteen yhtälöille ja johdettuja kaavoja kutsutaan Cardanon kaavoiksi. Jo nämä kaavat paljastivat mielenkiintoisia asioita, nimittäin että reaalilukuyhtälöiden ratkaisussa tarvitaan kompleksisia välituloksia. Kolmannen asteen yhtälön ratkaisukaava on selvästi ja neljännen asteen kaava huomattavasti vaikeampi kuin toisen asteen vastaava, mutta toive, että yhä korkeampiin asteisiin siirryttäessä samanlaisen, mutta vain monimutkaisemman kaavan voisi esittää, eli vuosisatoja.

1800-luvulla matemaatikot olivat kypsyneet siihen ajatukseen, että viidennen asteen yhtälön ratkaisemisen vaikeudet saattoivat johtua halutunlaisen ratkaisun mahdottomuudestakin. Vuonna 1824 norjalainen Niels Henrik Abel vihdoin onnistui todistamaan, että juurtamiseen perustuvaa ratkaisukaavaa ei ole olemassa viidennen asteen yhtälölle. Muutamaa vuotta myöhemmin ranskalainen Évariste Galois analysoi ratkaisuongelmaa pidemmälle, ja osoitti nykyaikaisin termein kuvailtuna, että kuhunkin polynomiyhtälöön voidaan liittää permutaatioryhmä, joka eräällä tavalla kuvaa, miten vaikea yhtälö on ratkaista. Abelin ja Galois'n

töissä algebralliset rakenteet esiintyvät vain implisiittisesti, mutta modernille matemaatikoille näiden tulosten esittäminen ilman kuntia ja ryhmiä olisi yhtä turhauttavaa kuin matematiikan soveltajalle yhtälönratkaisu ilman symbolista esitystä kirjaimien avulla. Nämä työt siis motivoivat algebrallisten rakenteiden käyttöä syvällisellä tavalla.

Tässä pitkässä johdannossa käydään aluksi läpi kuntateorian perustuloksia nimenomaisesti yhtälönratkaisemisen näkökulmasta, jonka jälkeen Cardanon kaavat käydään kevyesti läpi. Myöhemmissä osioissa siirrytään modernimpaan asetelmaan. Ensin poiketaan renkaiden jaollisuusteoriaan, sitten palataan jälleen kuntateoriaa ja käsitellään mm. Galois'n teoriaa siinä määrin, kun se on tällaisella kurssilla mahdollista.

2. Kuntateorian perustuloksia

Esitellään ensin kunnan karakteristika ja tutkitaan sen vaikutusta kunnan kokoon. Aloitetaan kokonaisluvuilla kertomisesta, joka voidaan määritellä missä tahansa renkaassa.

2.1. Merkintä. Olkoon $(R, +, \cdot)$ rengas, jonka nolla-alkiota merkitään tässä selvyyden vuoksi symbolilla 0_R, siis jotta se erottuisi kokonaisluvusta 0. Määritellään kaikille $n \in \mathbb{Z}$ ja $x \in R$ induktion avulla $n \cdot x$:

$$\begin{aligned} 0 \cdot x &= 0_R, \\ (n+1) \cdot x &= n \cdot x + x, \text{ kun } n \in \mathbb{N}, \\ n \cdot x &= (-n) \cdot (-x), \text{ kun } n \in \mathbb{Z}_- = \mathbb{Z} \setminus \mathbb{N}. \end{aligned}$$

Kun $n \in \mathbb{N}$, tämä merkitsee epämuodollisesti, että

$$n \cdot x = \underbrace{x + \cdots + x}_{n \text{ kpl}}.$$

Kokonaiskerronnalle voidaan osoittaa tuttuja perusominaisuuksia: Kun $m, n \in \mathbb{Z}, x, y \in R$, niin

1) $(mn)x = m(nx)$,
2) $(mn) \cdot (xy) = (mx)(ny)$,
3) $(m+n) \cdot x = m \cdot x + n \cdot x$ ja
4) $m \cdot (x+y) = m \cdot x + m \cdot y$.

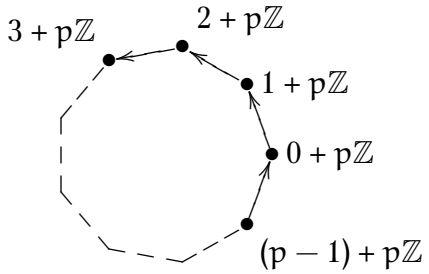
2.2. Määritelmä. Kunnan $\boldsymbol{K} = (K, +, \cdot)$ *karakteristika* on pienin $p \in \mathbb{Z}_+$, jolle pätee $p \cdot 1 = 0$ kunnassa $\boldsymbol{K}$, mikäli tällainen on olemassa, muuten 0.

Huomattakoon, että jos kunnan $\boldsymbol{K}$ karakteristika on p, niin kaikilla $x \in K$ pätee $p \cdot x = 0$, nimittäin

$$p \cdot x = p \cdot (1 \cdot x) = (p \cdot 1) \cdot x = 0 \cdot x = 0 \quad (0 \in K, 1 \in \mathbb{Z}).$$

2.3. Esimerkki. a) Rationaali-, reaali- ja kompleksilukujen kuntien karakteristikat ovat nollia, sillä kaikilla $n \in \mathbb{Z}_+$ pätee $n \cdot 1 = n \neq 0$.

b) Kun p on alkuluku, $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ on kunta, jonka karakteristika on p. Siis $p \cdot (1+p\mathbb{Z}) = 0+p\mathbb{Z}$.



Kelloaritmetiikka

2.4. Lause. *Kunnan* $\boldsymbol{K} = (K, +, \cdot)$ *karakteristika on joko* 0 *tai alkuluku.*

Todistus. Oletetaan vastoin väitettä, että kunnan $\boldsymbol{K}$ karakteristika olisi yhdistetty luku $p \neq 0$, ts. $p = qr$ joillakin $q, r \in \mathbb{N}$, $q < p$ ja $r < p$. Tällöin

$$0 = p \cdot 1 = (qr) \cdot 1 = (qr) \cdot (1 \cdot 1) = (q \cdot 1)(r \cdot 1).$$

Kunnat ovat kokonaisalueita, joten niissä ei ole epätriviaaleja nollantekijöitä. Ylläolevasta yhtälöstä seuraa siis $q \cdot 1 = 0$ tai $r \cdot 1 = 0$. Nämä ovat molemmat ristiriidassa sen kanssa, että p on pienin $m \in \mathbb{Z}_+$, jolle $m \cdot 1 = 0$. □

2.5. Lause. *Karakteristikaa* 0 *olevat kunnat ovat äärettömiä.*

Todistus. Jos $(K, +, \cdot)$ on tällainen kunta, niin kaikki ykkösen monikerrat ovat eri lukuja. Jos nimittäin olisi $m \cdot 1 = n \cdot 1$ joillakin $m, n \in \mathbb{Z}$, $m > n$, niin

$$0 = (m \cdot 1) - (n \cdot 1) = (m \cdot 1) + ((-n) \cdot 1) = \underbrace{(m - n)}_{>0} \cdot 1,$$

mikä on ristiriidassa sen kanssa, että kunnan $\boldsymbol{K}$ karakteristika on nolla. Siis $K \supseteq \{ n \cdot 1 \mid n \in \mathbb{Z} \}$ on ääretön. □

Huomautus. Itse asiassa on olemassa kaiken kokoisia äärettömiä karakteristikaa nolla olevia kuntia. Tämä perustuu yleiseen malliteoreettiseen faktaan, mutta on todistettavissa myös algebrallisesti ns. transkendenttikantojen avulla.

Seuraava tulos jätetään harjoitustehtäväksi:

2.6. Lemma. *(Cauchyn lause Abelin ryhmille) Olkoon* $(G, +)$ *äärellinen Abelin ryhmä ja* p *sellainen alkuluku, että* $p \mid |G|$. *Tällöin on olemassa* $x \in G$, *jolle* $\operatorname{ord}(x) = p$. □

2.7. Lause. *Äärellisen kunnan koko on alkulukupotenssi, ts.* p^k *jollakin alkuluvulla* p *ja* $k \in \mathbb{Z}_+$.

Todistus. Olkoon $\boldsymbol{K} = (K, +, \cdot)$ äärellinen kunta ja p sen karakteristika. Edellisten lauseiden mukaan $p \neq 0$ ja p on alkuluku. Tarkastellaan kunnan $\boldsymbol{K}$ yhteenlaskuryhmää $(K, +)$ ja se

kertalukua m, joka on tietysti myös kunnan $\boldsymbol{K}$ koko. Cauchyn lauseen mukaan pätee, että jos on olemassa alkuluku $q \neq p$, jolle $q \mid m$, niin ryhmässä $(K, +)$ on alkio x, jonka kertaluku on q, ts. $q \cdot x = 0$, mutta $m \cdot x \neq 0$, kun $m \in \mathbb{Z}_+$, $m < q$.

Toisaalta $p \cdot x = 0$. Näistä yhdistelemällä saadaan, että kaikilla $\alpha, \beta \in \mathbb{Z}$ pätee

$$(\alpha p + \beta q)x = (\alpha p)x + (\beta q)x = \alpha(px) + \beta(qx) = \alpha \cdot 0 + \beta \cdot 0 = 0 + 0 = 0.$$

Koska $\operatorname{syt}(p, q) = 1$, on olemassa $\alpha, \beta \in \mathbb{Z}$, joille $\alpha p + \beta q = 1$, jolloin $x = 1 \cdot x = (\alpha p + \beta q)x = 0$, mikä on mieletöntä.

On siis päätelty, että p on luvun m ainoa alkutekijä, joten $n = p^k$, missä $k \in \mathbb{N}$. Koska kunnassa on vähintään kaksi alkiota, $k > 0$. □

Huomautus. Kaikkien äärellisten kuntien karakteristika on alkuluku, mutta kaikki alkulukukarakteristikaiset kunnat eivät ole äärellisiä.

3. Yhtälönratkaiseminen kunnissa

Jokaiseen kuntaan $(K, +, \cdot)$ voidaan liittää polynomirengas $(K[x], +, \cdot)$ eli K-kertoimisten polynomien rengas, joka on yksiköllinen vaihdannainen rengas. Esimerkiksi pätee

$$(ax + b)(cx + d) = acx^2 + (ad + bc)x + bd.$$

Yleisemmin polynomirenkaassa $(K[x], +, \cdot)$ pätee Cauchyn kertosääntö:
Kun $p = \sum_{i=0}^{m} a_i x^i$, $q = \sum_{j=0}^{n} b_j x^j \in K[x]$, niin

$$pq = \sum_{k=0}^{m+n} \left(\sum_{i=\max\{0,k-n\}}^{\min\{k,m\}} a_i b_{k-i} \right) x^k = \sum_{k=0}^{m+n} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) x^k,$$

missä jälkimmäiset, yksinkertaisemmat indeksirajat tulevat voimaan, kun sovitaan kertoimista, että $a_i = 0$ ja $b_j = 0$, kun $i, j \in \mathbb{N}$, $i > m$ ja $j > n$. Polynomin $p = \sum_{i=0}^{m} a_i x^i$, missä $a_m \neq 0$, aste on m, mitä merkitään $\deg(p) = m$. Polynomien tulolle pätee

$$\deg(pq) = \deg(p) + \deg(q),$$

nimittäin tässä kuntakertoimisten polynomien tapauksessa. Nollapolynomeille määritellään $\deg(p) = -\infty$ (useissa esityksissä tämä jätetään määrittelemättä).

3.1. Lause. *(Jakoyhtälö) Olkoot $p, s \in K[x]$, missä $(K, +, \cdot)$ on kunta. Oletetaan, että $s \neq 0$. Tällöin on olemassa yksikäsitteiset polynomit $q, r \in K[x]$, joille pätee $p = qs + r$, missä $\deg(r) < \deg(s)$.*

Todistus. Todistetaan ensin polynomien q ja r olemassaolo induktiolla polynomin p asteen suhteen.

1) Jos $\deg(p) < \deg(s)$, niin $p = 0 \cdot s + p$, jossa $\deg(p) < \deg(s)$.

2) Oletetaan, että $\deg(p) \geqslant \deg(s)$ ja induktio-oletus pätee kaikille polynomeille $\widetilde{p}$, joille $\deg(\widetilde{p}) < \deg(p)$. Merkitään $p = \sum_{i=0}^{m} a_i x^i$, $s = \sum_{j=0}^{n} b_j x^j$, missä $m = \deg(p) \geqslant n = \deg(s)$. Merkitään edelleen $\widetilde{p} = p - (a_m b_n^{-1})x^{m-n}s$. Tällöin $(a_m b_n^{-1})x^{m-n}s$ on astetta $m - n + \deg(s) = m - n + n = m$, joten

$$\deg(\widetilde{p}) \leqslant \max\{\deg(p), \deg(-(a_m b_n^{-1})x^{m-n}s)\} = m.$$

Koska polynomin $\widetilde{p}$ m. asteen kerroin on $a_m - (a_m b_n^{-1})b_n = 0$, niin $\deg(\widetilde{p}) < m$. Siis polynomiin $\widetilde{p}$ voidaan soveltaa induktio-oletusta: Kun $\widetilde{p}$ jaetaan polynomilla s, niin saadaan sellainen (vaillinainen) osamäärä $\widetilde{q}$ ja jakojäännös $\widetilde{r}$, että $\widetilde{p} = \widetilde{q} \cdot s + \widetilde{r}$, missä $\deg(\widetilde{r}) < \deg(s)$. Tästä seuraa

$$\begin{aligned} p &= \widetilde{p} + (a_m b_n^{-1})x^{m-n}s = \widetilde{q} \cdot s + \widetilde{r} + (a_m b_n^{-1})x^{m-n}s \\ &= (\widetilde{q} + (a_m b_n^{-1})x^{m-n}) \cdot s + \widetilde{r}. \end{aligned}$$

Tässä $\deg(\widetilde{r}) < \deg(s)$, joten voidaan valita $q = \widetilde{q} + (a_m b_n^{-1})x^{m-n}$ ja $\widetilde{r} = r$.

Yksikäsitteisyyden todistamiseksi oletetaan, että $p = q_0 s + r_0 = q_1 s + r_1$, missä $\deg(r_0) < \deg(s)$ ja $\deg(r_1) < \deg(s)$. Tällöin

$$0 = (q_0 s + r_0) - (q_1 s + r_1) = (q_0 - q_1)s + (r_0 - r_1).$$

Jos olisi $q_0 \neq q_1$, niin pätisi

$$\begin{aligned} \deg((q_0 - q_1)s) &= \deg(q_0 - q_1) + \deg(s) \\ &\geqslant 0 + \deg(s) = \deg(s) \\ &> \max\{\deg(r_1), \deg(-r_0)\} \geqslant \deg(r_1 - r_0), \end{aligned}$$

mikä on ristiriita, sillä $r_1 - r_0 = (q_0 - q_1)s$. Siis $q_0 = q_1$ ja $0 = (q_0 - q_1)s + (r_0 - r_1) = 0 \cdot s + r_0 - r_1 = r_0 - r_1$, joten $r_0 = r_1$. □

Edellä olevasta induktio-oletuksesta voidaan tunnistaa myös *jako-algoritmi*: Kun polynomia p jaetaan polynomilla s, niin alussa jakojäännoksen puolella on p kokonaan ja osamäärän puolella 0. Ensimmäisessä vaiheessa jakojäännöksestä poistetaan $(a_m b_n^{-1})x^{m-n}s$ ja osamäärään lisätään $(a_m b_n^{-1})x^{m-n}$, jolloin jakojäännökseen jää $\widetilde{p} = p - (a_m b_n^{-1})x^{m-n}s$. Prosessia jatketaan, kunnes jakojäännöksen aste on pienempi kuin jakajan.

3.2. Seuraus. *Jos* $a \in K$ *on polynomiyhtälön* $p(x) = 0$ *ratkaisu, niin* $p = (x - a)q$ *jollakin* $q \in K[x]$.

Todistus. Kun jakoyhtälössä valitaan jakajaksi $x - a$, niin huomataan, että jakojäännöksen c täytyy olla vakiopolynomi ($\deg(r) < \deg(x - a) = 1$), ts. $p = (x - a)q + c$ jollakin $q \in K[x]$ ja $c \in K$. Koska $p(a) = 0$, niin $0 = p(a) = (a - a) \cdot q(a) + c = 0 \cdot q(a) + c = c$. Siis $p = (x - a)q$ jollakin $q \in K[x]$. □

3.3. Seuraus. *Kunnassa kirjoitetulla polynomiyhtälöllä on korkeintaan asteensa verran ratkaisuja.*

Todistus. Olkoon $p \in K[x] \setminus \{0\}$, $n = \deg(p)$. Olkoot $a_0, \ldots, a_{m-1} \in K$ polynomiyhtälön $p(x) = 0$ eri ratkaisuja. Osoitetaan induktiolla luonnollisen luvun $k \leqslant m$ suhteen, että on olemassa $q_k \in K[x]$, jolle

$$p = (x - a_0) \cdots (x - a_{k-1}) q_k. \qquad (*)$$

Tapauksessa $k = 0$ voidaan triviaalisti valita $q_0 = p$. Oletetaan nyt, että (*) pätee ja $k < m$. Koska

$$0 = p(a_k) = \underbrace{(a_k - a_0)}_{\neq 0} \cdots \underbrace{(a_k - a_{k-a})}_{\neq 0} q_k(a_k)$$

ja $(K, +, \cdot)$ on kuntana kokonaisalue, niin $q_k(a_k) = 0$. Edellisen seurauksen mukaan on olemassa $q_{k+1} \in K[x]$, jolle $q_k = (x - a_k) q_{k+1}$. Siis $p = (x - a_0) \cdots (x - a_{k-1})(x - a_k) q_{k+1}$.

Erityisesti $p = (x - a_0) \cdots (x - a_{m-1}) q_m$. Tästä seuraa helppo astetarkastelu

$$\deg(p) = \deg(x - a_0) + \ldots + \deg(x - a_{m-1}) + \deg(q_m) = m + \deg(q_m) \geqslant m. \quad \square$$

4. Cardanon kaavat

Toisen asteen yhtälön muotoisia ongelmia osattiin ratkaista jo vanhalla ajalla, kolmannen ja neljännen asteen renessanssiajalla (vuosina 1515 ja n. 1540). Kolmannen asteen kompleksikertoiminen yhtälö on muotoa ($a, b, c, d \in \mathbb{C}$, $a \neq 0$)

$$\begin{aligned} & ax^3 + bx^2 + cx + d = 0 \\ \iff & x^3 + \frac{b}{a}x^2 + \frac{c}{a}x + \frac{d}{a} = 0. \end{aligned}$$

Sijoittamalla $t = x + \frac{b}{3a} \iff x = t - \frac{b}{3a}$ yhtälö saadaan muotoon

$$\begin{aligned} & \left(t - \frac{b}{3a}\right)^3 + \frac{b}{a}\left(t - \frac{b}{3a}\right)^2 + \frac{c}{a}\left(t - \frac{b}{3a}\right) + \frac{d}{a} = 0. \\ \iff & t^3 - 3 \cdot \frac{b}{3a}t^2 + 3\left(\frac{b}{3a}\right)^2 t - \left(\frac{b}{3a}\right)^3 + \frac{b}{a}t^2 - \frac{2b^2}{3a^2}t + \frac{b^3}{9a^3} + \frac{c}{a}t - \frac{bc}{3a^2} + \frac{d}{a} = 0 \\ \iff & t^3 - \textcircled{\frac{b}{a}t^2} + \frac{b^2}{3a^2}t - \frac{b^3}{27a^3} + \textcircled{\frac{b}{a}t^2} - \frac{2b^2}{3a^2}t + \frac{b^3}{9a^3} + \frac{c}{a}t - \frac{bc}{3a^2} + \frac{d}{a} = 0 \\ \iff & t^3 + \left(\frac{c}{a} - \frac{b^2}{3a^2}\right)t + \frac{2b^3}{27a^3} - \frac{bc}{3a^2} + \frac{d}{a} = 0 \\ \iff & t^3 + qt + r = 0, \end{aligned}$$

missä $q = \frac{c}{a} - \frac{b^2}{3a^2}$ ja $r = \frac{2b^3}{27a^3} - \frac{bc}{3a^2} + \frac{d}{a}$.

4.1. Lemma. *Kaikilla $u, v \in \mathbb{C}$ on olemassa sellaiset $\alpha, \beta \in \mathbb{C}$, että*

$$\begin{cases} \alpha + \beta = u \\ \alpha \cdot \beta = v \end{cases}.$$

Pari $\{\alpha, \beta\}$ on yksikäsitteinen.

Todistus. Harjoitustehtävä. □

Lemman perusteella yhtälön tuntemattoman t voi hajottaa kahdeksi tuntemattomaksi α ja β, joille

$$\begin{cases} \alpha + \beta = t \\ \alpha \cdot \beta = -q/3. \end{cases}$$

Sijoittamalla tämä kolmannen asteen yhtälöön saadaan

$$\begin{aligned} 0 = t^3 + qt + r &= (\alpha + \beta)^3 + q(\alpha + \beta) + r \\ &= \alpha^3 + 3\alpha^2\beta + 3\alpha\beta^2 + \beta^3 + q(\alpha + \beta) + r \\ &= \alpha^3 + \beta^3 + \underbrace{(3\alpha\beta + q)}_{0}(\alpha + \beta) + r \\ &= \alpha^3 + \beta^3 + r. \end{aligned}$$

Uusien muuttujien tulee siis toteuttaa

$$\begin{cases} \alpha^3 + \beta^3 = -r \\ \alpha^3 \cdot \beta^3 = (\alpha\beta)^3 = (-q/3)^3 = -q^3/27 \end{cases},$$

mutta tämähän on lemman mukainen vaatimus lausekkeille $\gamma = \alpha^3$ ja $\delta = \beta^3$.

Kääntäen tietenkin havaitaan, että jos α ja β toteuttavat edellisestä yhtälöparista jälkimmäisen ja jälkimmäisestä ensimmäisen eli

$$\begin{cases} \alpha \cdot \beta = -q/3 \\ \alpha^3 + \beta^3 = -r, \end{cases}$$

niin $t = \alpha + \beta$ on tarkasteltavan kolmannen asteen yhtälön ratkaisu. Kaikkien ratkaisujen etsimiseksi saadaan siis seuraava menetelmä.

Kolmannen asteen yhtälön ratkaiseminen

1) Yhtälö muuntuu sijoituksella $t = x + \frac{b}{3a}$ muotoon $t^3 + qt + r = 0$.
2) Lemman perustella yhtälöparin
$$\begin{cases} \gamma + \delta = -r \\ \gamma \cdot \delta = -\frac{q^3}{27} \end{cases}$$

voi ratkaista parin γ, δ suhteen ja pari $\{\gamma, \delta\}$ on yksikäsitteinen.

3) Lasketaan kuutiojuuret:

$$\begin{cases} \alpha^3 = \gamma \\ \beta^3 = \delta \\ \alpha\beta = -q/3. \end{cases}$$

Viimeinen yhtälö voidaan aina toteuttaa, sillä kahdesta ensimmäisestä yhtälöstä seuraa $(\alpha\beta)^3 = \gamma\delta = -\frac{q^3}{27} = \left(-\frac{q}{3}\right)^3$. Jos (α, β) on yhtälöryhmän ratkaisu, niin muut ratkaisut ovat $(\omega\alpha, \omega^2\beta)$, $(\omega^2\alpha, \omega\beta)$, missä $\omega = e^{2\pi i/3}$.

4) Yksinkertaistetun kolmannen asteen yhtälön $t^3 + qt + r = 0$ ratkaisut ovat siis $t = \alpha + \beta$, $t = \omega\alpha + \omega^2\beta$ ja $t = \omega^2\alpha + \omega\beta$.

5) Alkuperäisen yhtälön ratkaisut saadaan tekemällä palauttava sijoitus $x = t - \frac{b}{3a}$. Ne ovat siten $x = \alpha + \beta - \frac{b}{3a}$, $x = \omega\alpha + \omega^2\beta - \frac{b}{3a}$ ja $x = \omega^2\alpha + \omega\beta - \frac{b}{3a}$.

Neljännen asteen yhtälön ratkaiseminen

1) Yhtälö $ax^4 + bx^3 + cx^2 + dx + e = 0$ muuttuu sijoituksella $t = x + \frac{b}{4a}$ muotoon $t^4 + qt^2 + rt + s = 0$. (Yksityiskohdat ovat hyvin samankaltaisia kuin kolmannen asteen yhtälön tapauksessa.)

2) Jos $r = 0$, niin yo. yhtälö on toisen asteen yhtälö lausekkeelle t^2, joten se ratkeaa toisen asteen ratkaisukaavalla.

3) Oletetaan jatkossa $r \neq 0$. Pyritään jakamaan polynomi $t^4 + qt^2 + rt + s$ kahdeksi toisen asteen polynomiksi, mikä palauttaisi yhtälönratkaisun toisen asteen yhtälöiden ratkaisemiseen:

$$\begin{aligned} t^4 + qt^2 + rt + s &= (t^2 + jt + l)(t^2 + kt + m) \\ &= t^4 + (j + k)t^3 + (m + jk + l)t^2 + (jm + kl)t + lm. \end{aligned}$$

Jotta tämä olisi identtisesti totta, täytyy olla

$$\begin{cases} j + k = 0 \\ m + jk + l = q \\ jm + kl = r \\ lm = s \end{cases} \iff \begin{cases} k = -j \\ m - j^2 + l = q \\ j(m - l) = r \\ lm = s \end{cases}$$

Koska $r \neq 0$, täytyy päteä myös $j \neq 0$. Tarkastellaan yhtälöryhmän keskimmäisiä

yhtälöitä.

$$\begin{aligned}
&\begin{cases} m - j^2 + l = q \\ \quad j(m - l) = r \end{cases} \\
\iff &\begin{cases} m + l = q + j^2 \\ m - l = r/j \end{cases} \\
\iff &\begin{cases} 2m = j^2 + q + r/j \\ \quad 2l = j^2 + q - r/j \end{cases}
\end{aligned}$$

Neljän yhtälön ryhmän alimmasta yhtälöstä seuraa siis

$$\begin{aligned}
4s = 4lm &= (2m)(2l) = (j^2 + q + r/j)(j^2 + q - r/j) \\
&= (j^2 + q)^2 - (r/j)^2 = j^4 + 2qj^2 + q^2 - r^2/j^2 \\
\iff 4sj^2 &= j^6 + 2qj^4 + q^2j^2 - r^2 \\
\iff j^6 + 2qj^4 &+ (q^2 - 4s)j^2 - r^2 = 0 \\
\iff (j^2)^3 + 2q(j^2)^2 &+ (q^2 - 4s)j^2 - r^2 = 0.
\end{aligned}$$

4) Tämä on kolmannen asteen yhtälö lausekkeelle j^2, joka ratkeaa edellä esitetyin menetelmin ja josta saadaan neliöjuurtamalla j. Tämän jälkeen saadaan laskettua myös k, l, m ja neljännen asteen yhtälö palautuu toisen asteen yhtälöiden ratkaisemiseksi:

$$t^4 + qt^2 + rt + s = 0 \iff t^2 + jt + l = 0 \vee t^2 + kt + m = 0.$$

Neljännen asteen yhtälön ratkaiseminen on tietenkin selvästi työläämpää kuin kolmannen, koska tehtävä sisältää osatehtävänään tietyn kolmannen asteen yhtälön ratkaisemisen. Kaikki polynomiyhtälöt ovat silti luonteeltaan samanlaisia neljänteen asteeseen saakka – erityisesti ne ratkeavat klassisin menetelmin. Kuten Abel ja Galois 1800-luvulla osoittivat, klassiset juurtamiseen perustuvat menetelmät eivät kuitenkaan pure korkeampiasteisiin yhtälöihin. Aikoinaan nämä tulokset merkitsivät osaltaan paradigmaattista murrosta matematiikkaan, mutta nykymatemaatikolle tämänkaltaiset tulokset ovat arkipäivää: Matematiikan tutkimukseen kuuluu oleellisena osana erilaisten menetelmien rajoitusten tutkiminen.