Transkendenttiluvut ja Hermiten lause

Esa V. Vesalainen
Matematik och statistik, Åbo Akademi

Matematiikassa erittäin usein esiintyvä *Neperin vakio* eli *luonnollisen logaritmin kanta* on luku

$$e = \sum_{\mu=0}^{\infty} \frac{1}{\mu!} = \frac{1}{0!} + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + \dots$$
$$= 1 + 1 + \frac{1}{2} + \frac{1}{6} + \frac{1}{24} + \dots \approx 2{,}718281828459\dots$$

Yllä esiintyvät kertomat ovat $0! = 1$, $1! = 1$, $2! = 1 \cdot 2$, $3! = 1 \cdot 2 \cdot 3$, $4! = 1 \cdot 2 \cdot 3 \cdot 4$, ja niin edelleen. Tässä artikkelissa tarkoituksena on esittää yksityiskohtainen ja alkeellinen todistus Hermiten lauseelle:

Lause 1 (Hermiten lause)**.** *Luku e on transkendenttinen. Toisin sanoen, jos $P(x)$ on kokonaislukukertoiminen polynomi, joka ei ole nollapolynomi, niin $P(e) \neq 0$.*

Samalla yritämme taustoittaa tätä hieman vertailemalla kokonaislukukertoimisten polynomien nollakohtiin, ja kertoa hieman yleistyksistä.

Ennen aloittamista lienee syytä kertoa, että differentiaali- ja integraalilaskentaa tuntemattoman lukijan ei ole syytä pelästyä myöhemmin esiintyviä lukuisia derivaattalausekkeita. Nimittäin, seuraavassa käsitellään vain polynomien derivaattoja, jotka voi tässä määritellä suoraan alkeellisella tavalla, jolloin niiden tarvittavat perusominaisuudet ovat myös helppoja todistaa. Matemaattisesta analyysistä ei tarvita juuri mitään muita tietoja, kuin että eksponenttifunktiolla on Taylor-kehitelmä

$$e^x = \sum_{\mu=0}^{\infty} \frac{x^\mu}{\mu!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots,$$

mikä pätee ja on kaikin puolin matemaattisesti mielekäs kaikilla reaaliluvuilla x. Käytännön kannalta voimme käsitellä tätä ääretöntä sarjaa varsin samaan tapaan kuin äärellistä summaakin.

Algebralliset luvut

Reaaliluku, ja yleisemmin kompleksiluku, α on *algebrallinen luku*, jos on olemassa kokonaislukukertoiminen polynomi $P(x)$, joka ei ole nollapolynomi, ja jolle $P(\alpha) = 0$. Pienintä mahdollista polynomin $P(x)$ astetta kutsutaan algebrallisen luvun α *asteeksi*. Jos α ei ole algebrallinen, niin se on *transkendenttinen*.

Rationaaliluvut ovat aina algebrallisia. Nimittäin, jos a on kokonaisluku ja b positiivinen kokonaisluku, niin rationaaliluku a/b on aina kokonaislukukertoimisen polynomin $bx - a$ nollakohta, ja siten ensimmäisen asteen algebrallinen luku. Kääntäen, kokonaislukukertoimisen ensimmäisen asteen polynomin $bx - a$ nollakohta on aina rationaaliluku, nimittäin a/b. Siis ensimmäisen asteen algebrallisia lukuja ovat täsmälleen rationaaliluvut.

Mielenkiintoisempi esimerkki on luku $\sqrt{2}$, joka on algebrallinen luku, koska se on polynomin $x^2 - 2$ nollakohta. Kompleksiluku i on myös algebrallinen luku, koska se on polynomin $x^2 + 1$ nollakohta. Koska $\sqrt{2}$ on tunnetusti irrationaalinen, ja koska i ei ole edes reaaliluku, ja siten ei myöskään rationaaliluku, eivät $\sqrt{2}$ ja i voi olla ensimmäisen asteen algebrallisia lukuja, joten ne ovat toisen asteen algebrallisia lukuja.

Esimerkkejä tunnetuista transkendenttisistä luvuista ovat e, π, e^π, $2^{\sqrt{2}}$, tai vaikkapa luku

$$0{,}123456789101112131415\dots$$

Lisää esimerkkejä annetaan tämän artikkelin lopussa, kun keskustellaan Hermiten lauseen yleistyksistä.

Algebrallisten lukujen perusominaisuuksia

Kuvailemme tässä ensiksi algebrallisten lukujen perusominaisuuksia. Ensimmäiseksi on luonnollista kysyä, mitä tapahtuu algebrallisille luvuille peruslaskutoimituksissa? On mahdollista todistaa, että lopputuloksena saadaan aina algebrallisia lukuja:

Lause. *Jos α ja β ovat algebrallisia lukuja, niin silloin myös luvut $\alpha + \beta$, $\alpha - \beta$ ja $\alpha\beta$ ovat algebrallisia lukuja. Jos lisäksi $\beta \neq 0$, niin myös α/β on algebrallinen luku.*

Syvällisempi kysymys olisi, millaisia ratkaisuita saadaan polynomiyhtälöistä, joissa kertoimet ovat algebrallisia lukuja. Jälleen kaikki toimii mukavasti:

Lause. *Jos α on reaaliluku (tai yleisemmin kompleksiluku), jos $P(x)$ on polynomi, jonka kertoimet ovat algebrallisia lukuja, jos $P(x)$ ei ole nollapolynomi, ja jos $P(\alpha) = 0$, niin itse asiassa α on myös algebrallinen luku.*

Tämä motivoi kauniisti transkendenttilukujen nimen: transkendenttiluvut ovat kaikkien algebrallis-

ten operaatioiden (peruslaskutoimitusten ja polynomiyhtälöiden ratkaisun) ulottumattomissa. Tai toisin sanoen, jos lähdetään liikkeelle vaikkapa rationaaliluvuista, niin peruslaskutoimituksilla ja ratkaisemalla polynomiyhtälöitä jo konstruoiduista luvuista voi aina konstruoida vain algebrallisia lukuja.

Esimerkkejä algebrallisten lukujen teorian sovellutuksista

Emme voi mitenkään tehdä tässä oikeutta algebrallisille luvuille, mutta ehkäpä muutama valaiseva esimerkki niiden esiintymisestä matematiikassa olisi kuitenkin paikallaan.

Konstruktiot harpilla ja viivaimella. Algebrallisten lukujen motivaatioksi annamme joitakin esimerkkejä niiden sovelluksista. Aloitetaan seuraavista kuuluisista kolmesta konstruktio-ongelmasta:

- *Kulman kolmijako:* Jaettava annettu kulma harpilla ja viivaimella kolmeen yhtä suureen osaan.
- *Kuution kahdentaminen:* Jos on annettu kuution särmän mittainen jana, konstruoitava siitä harpilla ja viivaimella sellainen jana, jonka pituus on yhtä pitkä kuin sellaisen kuution särmä, jonka tilavuus on kaksi kertaa niin iso kuin alkuperäisen kuution tilavuus oli.
- *Ympyrän neliöinti:* Jos on annettu ympyrä, on konstruoitava harpilla ja viivaimella sellainen neliö, jolla on sama ala kuin annetulla ympyrällä.

Nämä kaikki kolme ongelmaa osoittautuvat mahdottomiksi, ja nämä mahdottomuudet näkee konseptuaalisesti miellyttävällä tavalla algebrallisten lukujen teorian kautta. Nimittäin, jos lähdetään liikkeelle jostakin yhdestä yksikön mittaisesta janasta, niin on mahdollista todistaa, että kaikkien siitä harpilla ja viivaimella konstruoitavien janojen pituudet ovat aina algebrallisia lukuja, joiden asteet ovat luvun 2 potensseja.

Kulman kolmijaon mahdottomuus seuraa nyt vaikkapa siitä, että jos kulman voisi jakaa kolmeen osaan, niin erityisesti $60°$ kulman voisi jakaa kolmeen osaan, jolloin voisi konstruoida $20°$ asteen suuruisen kulman, ja siten esimerkiksi janan, jonka pituus olisi $\cos 20°$. Kuitenkin tämä luku on yhtälön $8x^3 - 6x - 1 = 0$ ratkaisu, ja osoittautuu, että $\cos 20°$ on kolmannen asteen algebrallinen luku. Koska 3 ei ole luvun 2 potenssi, on kulman kolmijako siis mahdotonta.

Kuution kahdentamisen mahdottomuus sujuu samassa hengessä: Jos kuution kahdentaminen olisi aina mahdollista, niin silloin yksikkökuution kahdentaminen olisi mahdollista. Mutta tämä tarkoittaisi sellaisen janan konstruointia, jonka pituus olisi $\sqrt[3]{2}$. Ei ole kovin yllättävää, että tämä luku, joka on yhtälön $x^3 - 2 = 0$ ratkaisu, osoittautuu myös kolmannen asteen algebralliseksi luvuksi, ja on siten myös harpin ja viivaimen ulottumattomissa.

Ympyrän neliöinnin mahdottomuus on hieman kimurantimpi todistaa. Jos alkuperäisen ympyrän säde on vaikkapa 1, niin silloin ympyrän ala on π, ja halutun neliön ala olisi myös π, jolloin oleellisesti ottaen pitäisi konstruoida neliön sivuksi jana, jonka pituus olisi $\sqrt{\pi}$. Tällöin $\sqrt{\pi}$ olisi algebrallinen luku, ja koska algebrallisten lukujen tulot ovat algebrallisia, myös $\sqrt{\pi} \cdot \sqrt{\pi} = \pi$ olisi algebrallinen luku. Mutta osoittautuu, että π on transkendenttinen, ja siten ympyrän neliöinti ei ole mahdollista.

Mainittakoon vielä yksi tulos, jonka ymmärtämisessä tietynlaiset algebralliset luvut — nimittäin yhtälöiden $x^n = 1$ ratkaisut — näyttelevät tärkeää osaa: Jos $n \geqslant 3$ on kokonaisluku, niin harpilla ja viivaimella voi piirtää säännöllisen n-kulmion täsmälleen silloin, kun $n = 2^\nu p_1 p_2 \cdots p_r$, missä ν on epänegatiivinen kokonaisluku, r epänegatiivinen kokonaisluku, ja p_1, p_2, …, p_r ovat Fermat'n alkulukuja, joista mitkään kaksi eivät ole yhtä suuria. *Fermat'n alkuluvulla* tarkoitetaan alkulukua, joka on yhtä suuri kuin $2^{2^\alpha} + 1$ jollakin epänegatiivisella kokonaisluvulla α. Tunnetut Fermat'n alkuluvut ovat 3, 5, 17, 257 ja 65537.

Lukuteoria. Algebrallisten lukujen teoria on lukuteorian suuri ja tärkeä osa-alue, jolle emme myöskään voi tehdä tässä oikeutta. Yksi tapa, jolla algebralliset luvut tekevät elämän helpommaksi, on se, että kun kokonaislukuja laajentaa sopivilla algebrallisilla luvuilla, saadaan näin lisää tekijöihinjakoja, jolloin on enemmän työkaluja käytettävissä kokonaisluku- ja rationaalilukuratkaisuiden etsimiseen erilaisille Diofantoksen yhtälöille. Esimerkiksi, jos tavallisia kokonaislukuja laajentaa yhtälön $x^2 + x + 1 = 0$ ratkaisulla ω, ja muilla siitä ja kokonaisluvuista peruslaskutoimituksilla saatavilla luvuilla, niin Fermat'n suuren lauseen yhtälö eksponentilla 3, eli yhtälö $x^3 + y^3 = z^3$ voidaan kirjoittaa muodossa

$$z^3 = \left(x + y\right)\left(x + \omega y\right)\left(x + \omega^2 y\right).$$

Tästä on hyötyä sen osoittamisessa, että kyseisellä kolmannen asteen Diofantoksen yhtälöllä ei ole ratkaisuita positiivisten kokonaislukujen joukossa. Nimittäin, oikean puolen tekijöillä voi olla enimmillään vain hyvin pieni suurin yhteinen tekijä, jolloin ne kaikki ovat jotain mahdollisia hyvin pieniä lisätekijöitä vaille kuutiolukuja, mikä rajoittaa mahdollisia ratkaisuita merkittävästi.

Algebrallisten lukujen teoria on luonnollisella tavalla hyödyllistä myös tutkittaessa neliömuotojen teoriaa, kuten mitkä alkuluvut ovat muotoa $x^2 + 2y^2$ tai mitkä kokonaisluvut ovat kahden neliön summia. Myös kauniin neliönjäännösten teorian yleistäminen on ollut algebrallisen lukuteorian suuria teemoja.

Algebralliset yhtälöt. Ei ole yllättävää, että algebrallisten yhtälöiden ymmärtämisessä algebralliset luvut ovat tärkeitä. Eräs kuuluisa esimerkki on se seikka, joka usein muotoillaan jotenkin näin: yleiset viidennen ja korkeamman asteen yhtälöt eivät ole algebrallisesti ratkeavia. Erityisesti, on olemassa rationaalilukukertoimisia viidennen ja korkeamman asteen yhtälöitä, joiden juuret eivät ole mitään rationaaliluvuista peruslaskutoimituksilla ja juurenotoilla saatavia lukuja.

Kertomat ja binomikertoimet

Tarvitsemme useita eri työkaluja Hermiten lauseen todistusta varten. Ensinnäkin on tarpeen palauttaa mieleen, mitä ovat kertomat ja binomikertoimet. Jos n on positiivinen kokonaisluku, niin luvun n *kertoma* on yksinkertaisesti tulo

$$n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n.$$

Lisäksi asetamme $0! = 1$. Esimerkiksi $5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120$.

Jos n on epänegatiivinen kokonaisluku ja k on jokin luvuista 0, 1, 2, …, n, niin *binomikerroin* $\binom{n}{k}$ kertoo, kuinka monella eri tavalla n eri olion joukosta voi valita k olion osajoukon. Eräs kombinatoriikan perustulos sanoo, että itse asiassa

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!} = \frac{n\,(n-1)\,(n-2)\cdots(n-k+1)}{k!}.$$

Eräs toinen kombinatoriikan perustulos sanoo, että kun lisäksi $k < n$, niin

$$\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}.$$

Tällä seikalla on varsin havainnollinen merkitys: binomikertoimet voi asettaa kolmioksi, jossa jokainen binomikerroin (reunoilla olevia lukuun ottamatta) on kahden yläpuolella olevan summa:

$$\begin{array}{ccccccccccc}
\binom{0}{0} & & & & & & & & & & \\
\binom{1}{0} & & \binom{1}{1} & & & & & & & & \\
\binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & & & & \\
\binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & & & \\
\binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & & \\
\binom{5}{0} & & \binom{5}{1} & & \binom{5}{2} & & \binom{5}{3} & & \binom{5}{4} & & \binom{5}{5} \\
\binom{6}{0} & & \binom{6}{1} & & \binom{6}{2} & & \binom{6}{3} & & \binom{6}{4} & & \binom{6}{5} & & \binom{6}{6} \\
\binom{7}{0} & & \binom{7}{1} & & \binom{7}{2} & & \binom{7}{3} & & \binom{7}{4} & & \binom{7}{5} & & \binom{7}{6} & & \binom{7}{7} \\
\binom{8}{0} & & \binom{8}{1} & & \binom{8}{2} & & \binom{8}{3} & & \binom{8}{4} & & \binom{8}{5} & & \binom{8}{6} & & \binom{8}{7} & & \binom{8}{8} \\
\binom{9}{0} & & \binom{9}{1} & & \binom{9}{2} & & \binom{9}{3} & & \binom{9}{4} & & \binom{9}{5} & & \binom{9}{6} & & \binom{9}{7} & & \binom{9}{8} & & \binom{9}{9}
\end{array}$$

……

Näin syntyy kuvio nimeltä *Pascalin kolmio*:

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
 & 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 \\
 & & 1 & & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & & 1 \\
 & & & 1 & & 8 & & 28 & & 56 & & 70 & & 56 & & 28 & & 8 & & 1 \\
 & & & & 1 & & 9 & & 36 & & 84 & & 126 & & 126 & & 84 & & 36 & & 9 & & 1 \\
 & & & & & 1 & & 10 & & 45 & & 120 & & 210 & & 252 & & 210 & & 120 & & 45 & & 10 & & 1
\end{array}$$

……

Lemma 2. *Olkoot ℓ, q ja m positiivisia kokonaislukuja, joille $\ell \geqslant q$. Tällöin*

$$q! \mid m\,(m+1)\,(m+2)\cdots(m+\ell-1).$$

Tai toisin sanoen, $q!$ jakaa aina ℓ peräkkäisen positiivisen kokonaisluvun tulon.

Todistus. Tämä seuraa suoraan siitä tiedosta, että binomikertoimet ovat kokonaislukuja. Nimittäin, voimme laskea, että

$$\binom{m+\ell-1}{\ell} = \frac{(m+\ell-1)\,(m+\ell-2)\cdots(m+1)\,m}{\ell!},$$

eli itse asiassa $\ell!$ jakaa tulon $m\,(m+1)\cdots(m+\ell-1)$, jolloin myös luvun $q!$ on jaettava se. □

Myöhemmin esitettävä Hermiten lauseen todistus perustuu oleellisella tavalla siihen, että kertoma $n!$ kasvaa nopeammin kuin mikään eksponenttifunktio B^n, kun positiivinen kokonaisluku n kasvaa rajatta:

Lemma 3. *Olkoot A, B ja ε positiivisia reaalilukuja. Tällöin löytyy (luvuista A, B ja ε riippuva) positiivinen kokonaisluku Ξ niin, että*

$$\frac{A \cdot B^n}{n!} < \varepsilon$$

kaikilla kokonaisluvuilla $n \geqslant \Xi$.

Todistus. Olkoon ensin $M = \lceil B \rceil$ pienin kokonaisluku, jolle $M \geqslant B$, ja tarkastellaan kokonaislukua n, jolle $n > 2M$. Tällöin

$$\begin{aligned}
\frac{A \cdot B^n}{n!} &= \frac{A \cdot B^{2M} \cdot B^{n-2M}}{(2M)! \cdot (2M+1)\,(2M+2)\cdots(n-1)\,n} \\
&= \frac{A \cdot B^{2M}}{(2M)!} \cdot \frac{B}{2M+1} \cdot \frac{B}{2M+2} \cdot \ldots \cdot \frac{B}{n-1} \cdot \frac{B}{n}.
\end{aligned}$$

Asian ydin on, että viimeiset tekijät $B/(2M+1)$, …, B/n ovat kaikki pienempiä kuin $1/2$ ja voimme siten arvioida

$$\frac{A \cdot B^n}{n!} < \frac{A \cdot B^{2M}}{(2M)!} \left(\frac{1}{2}\right)^{n-2M} = \frac{A \cdot B^{2M} \cdot 2^{2M}}{(2M)!} \cdot \left(\frac{1}{2}\right)^{n}.$$

Nyt varmasti pätee

$$\frac{A \cdot B^n}{n!} < \varepsilon,$$

jos pätee

$$\frac{A \cdot B^{2M} \cdot 2^{2M}}{(2M)!} \cdot \left(\frac{1}{2}\right)^n < \varepsilon.$$

Mutta tämän viimeisen voi kirjoittaa muodossa

$$2^n > \frac{A \cdot B^{2M} \cdot 2^{2M}}{\varepsilon \cdot (2M)!}.$$

Riittää siis valita haluttu kokonaisluku Ξ niin, että

$$2^{\Xi} > \frac{A \cdot B^{2M} \cdot 2^{2M}}{\varepsilon \cdot (2M)!} \quad \text{ja} \quad \Xi > 2M. \qquad \square$$

Polynomien derivaatat

Tarkastellaan polynomia

$$P(x) = \sum_{\nu=0}^{d} c_\nu \, x^\nu,$$

missä d on epänegatiivinen kokonaisluku, ja c_0, c_1, $\ldots$, c_d ovat reaalilukuja. Tavalliseen tapaan x^0 tarkoittaa vakiota 1, koska se on niin käytännöllistä. Tällöin määrittelemme polynomin $P(x)$ *derivaatan* $P'(x)$ asettamalla

$$P'(x) = \sum_{\nu=1}^{d} c_\nu \, \nu \, x^{\nu-1}.$$

Jos $d = 0$, summassa ei ole termejä ja $P'(x) = 0$. Merkitsemme derivaattaa myös

$$\frac{\mathrm{d}}{\mathrm{d}x} P(x) = P^{(1)}(x) = P'(x).$$

Esimerkiksi, suoraan määritelmän nojalla

$$\frac{\mathrm{d}}{\mathrm{d}x}\left(3x^3 - 4x^2 + 7x - 5\right) = 9x^2 - 8x + 7.$$

Samoin

$$\frac{\mathrm{d}}{\mathrm{d}x} 1 = 0, \ \frac{\mathrm{d}}{\mathrm{d}x} x = 1, \ \frac{\mathrm{d}}{\mathrm{d}x} x^2 = 2x, \ \frac{\mathrm{d}}{\mathrm{d}x} x^3 = 3x^2, \ \ldots,$$

ja yleisesti

$$\frac{\mathrm{d}}{\mathrm{d}x} x^\nu = \nu \, x^{\nu-1}$$

jokaisella epänegatiivisella kokonaisluvulla ν. Tässä $0\,x^{-1}$ tarkoittaa nollapolynomia.

Voimme luonnollisesti derivoida polynomia useampaan kertaan, ja merkitsemme toista derivaattaa

$$\frac{\mathrm{d}^2}{\mathrm{d}x^2} P(x) = P''(x) = P^{(2)}(x),$$

ja yleisemmin ℓ. derivaattaa, kun ℓ on epänegatiivinen kokonaisluku,

$$\frac{\mathrm{d}^\ell}{\mathrm{d}x^\ell} P(x) = P^{(\ell)}(x).$$

Erityisesti

$$\frac{\mathrm{d}^0}{\mathrm{d}x^0} P(x) = P^{(0)}(x) = P(x).$$

Esimerkiksi, aiemman polynomin $3x^3 - 4x^2 + 7x - 5$ toinen derivaatta on

$$\begin{aligned}\frac{\mathrm{d}^2}{\mathrm{d}x^2}\left(3x^3 - 4x^2 + 7x - 5\right) &= \frac{\mathrm{d}}{\mathrm{d}x}\left(9x^2 - 8x + 7\right) \\ &= 18x - 8,\end{aligned}$$

ja sen kolmas derivaatta on

$$\frac{\mathrm{d}^3}{\mathrm{d}x^3}\left(3x^3 - 4x^2 + 7x - 5\right) = \frac{\mathrm{d}}{\mathrm{d}x}\left(18x - 8\right) = 18.$$

Sen neljäs ja kaikki korkeammat derivaatat ovat nollapolynomeja.

Jos ν on epänegatiivinen kokonaisluku ja ℓ on positiivinen kokonaisluku, niin

$$\frac{\mathrm{d}^\ell}{\mathrm{d}x^\ell} x^\nu = \nu\,(\nu-1)\,(\nu-2)\cdots(\nu-\ell+1)\,x^{\nu-\ell},$$

jos $\ell \leqslant \nu$, ja

$$\frac{\mathrm{d}^\ell}{\mathrm{d}x^\ell} x^\nu = 0,$$

jos $\ell > \nu$. Yleisemminkin pätee, että jos $P(x)$ on reaalikertoiminen polynomi, joka on vakio, tai jonka aste on pienempi kuin ℓ, niin

$$\frac{\mathrm{d}^\ell}{\mathrm{d}x^\ell} P(x) = 0.$$

On mielenkiintoista huomata, että positiivisilla kokonaisluvuilla ν lausekkeella $x^\nu/\nu!$ on se ominaisuus, että

$$\frac{\mathrm{d}}{\mathrm{d}x}\,\frac{x^\nu}{\nu!} = \frac{\nu\,x^{\nu-1}}{\nu!} = \frac{\nu\,x^{\nu-1}}{\nu\cdot(\nu-1)!} = \frac{x^{\nu-1}}{(\nu-1)!}.$$

Tästä seuraa, että yleisemmin

$$\frac{\mathrm{d}^\ell}{\mathrm{d}x^\ell}\,\frac{x^\nu}{\nu!} = \frac{x^{\nu-\ell}}{(\nu-\ell)!},$$

kun $\ell \leqslant \nu$, ja

$$\frac{\mathrm{d}^\ell}{\mathrm{d}x^\ell}\,\frac{x^\nu}{\nu!} = 0,$$

kun $\ell > \nu$.

Polynomien derivaattojen perusominaisuuksia

Tarvitsemme hieman perustietoja siitä, miten derivointi käyttäytyy, kun polynomeista otetaan summia ja tuloja, tai kun niissä tehdään muuttujanvaihtoja $x \longmapsto x + a$ reaalivakioilla a.

Lause 4. *Jos $P(x)$ ja $Q(x)$ ovat reaalilukukertoimisia polynomeja, ja jos a on reaaliluku, niin*

$$\frac{\mathrm{d}}{\mathrm{d}x}\left(P(x) + Q(x)\right) = P'(x) + Q'(x)$$

ja

$$\frac{\mathrm{d}}{\mathrm{d}x}\left(a\,P(x)\right) = a\,P'(x).$$

Todistus. Täydentämällä polynomeja $P(x)$ ja $Q(x)$ tarvittaessa termeillä, jotka ovat muotoa $0\,x^\nu$ epänegatiivisilla kokonaisluvuilla ν, voimme kirjoittaa ne summina

$$P(x) = \sum_{\nu=0}^{d} p_\nu\,x^\nu \quad \text{ja} \quad Q(x) = \sum_{\nu=0}^{d} q_\nu\,x^\nu,$$

missä d on positiivinen kokonaisluku ja p_0, p_1, …, p_d, q_0, q_1, …, q_d ovat reaalilukuja. Nyt

$$\begin{aligned}\frac{\mathrm{d}}{\mathrm{d}x}\left(P(x) + Q(x)\right) &= \frac{\mathrm{d}}{\mathrm{d}x}\left(\sum_{\nu=0}^{d} p_\nu\,x^\nu + \sum_{\nu=0}^{d} q_\nu\,x^\nu\right)\\ &= \frac{\mathrm{d}}{\mathrm{d}x}\sum_{\nu=0}^{d}\left(p_\nu + q_\nu\right)x^\nu = \sum_{\nu=1}^{d}\left(p_\nu + q_\nu\right)\nu\,x^{\nu-1}\\ &= \sum_{\nu=1}^{d} p_\nu\,\nu\,x^{\nu-1} + \sum_{\nu=1}^{d} q_\nu\,\nu\,x^{\nu-1} \;= P'(x) + Q'(x).\end{aligned}$$

Samassa hengessä voimme laskea

$$\begin{aligned}\frac{\mathrm{d}}{\mathrm{d}x}\left(a\,P(x)\right) &= \frac{\mathrm{d}}{\mathrm{d}x}\sum_{\nu=0}^{d} a\,p_\nu\,x^\nu\\ &= \sum_{\nu=1}^{d} a\,p_\nu\,\nu\,x^{\nu-1} = a\,P'(x).\end{aligned}$$ □

Lause 5. *Jos $P(x)$ ja $Q(x)$ ovat reaalilukukertoimisia polynomeja, niin*

$$\frac{\mathrm{d}}{\mathrm{d}x}\left(P(x)\,Q(x)\right) = P'(x)\,Q(x) + P(x)\,Q'(x).$$

Todistus. Olkoot

$$P(x) = \sum_{\nu=0}^{a} p_\nu\,x^\nu \quad \text{ja} \quad Q(x) = \sum_{\mu=0}^{b} q_\mu\,x^\mu,$$

missä luonnollisesti a ja b ovat epänegatiivisia kokonaislukuja, ja p_0, p_1, …, p_a, q_0, q_1, …, q_b ovat reaalilukuja. Tällöin edellisen tuloksen nojalla

$$\begin{aligned}&\frac{\mathrm{d}}{\mathrm{d}x}\left(P(x)\,Q(x)\right) = \frac{\mathrm{d}}{\mathrm{d}x}\left(\sum_{\nu=0}^{a} p_\nu\,x^\nu \sum_{\mu=0}^{b} q_\mu\,x^\mu\right)\\ &= \sum_{\nu=0}^{a}\sum_{\mu=0}^{b} p_\nu\,q_\mu\,\frac{\mathrm{d}}{\mathrm{d}x}\,x^{\nu+\mu}\\ &= \sum_{\nu=0}^{a}\sum_{\mu=0}^{b} p_\nu\,q_\mu\,(\nu+\mu)\,x^{\nu+\mu-1}\\ &= \sum_{\nu=0}^{a}\sum_{\mu=0}^{b} p_\nu\,\nu\,x^{\nu-1}\,q_\mu\,x^\mu + \sum_{\nu=0}^{a}\sum_{\mu=0}^{b} p_\nu\,x^\nu\,q_\mu\,\mu\,x^{\mu-1}\\ &= P'(x)\,Q(x) + P(x)\,Q'(x).\end{aligned}$$ □

Lause 6. *Jos $P(x)$ ja $Q(x)$ ovat reaalilukukertoimisia polynomeja siten, että $P(x) = Q(x+a)$ jollakin reaalivakiolla a, niin silloin*

$$P^{(\ell)}(x) = Q^{(\ell)}(x+a),$$

jokaisella positiivisella kokonaisluvulla ℓ.

Todistus. Ei ole vaikea havaita, että riittää osoittaa tämä arvolla $\ell = 1$, jolloin väite suuremmilla luvun ℓ arvoilla seuraa soveltamalla tapauksen $\ell = 1$ tulosta toistuvasti. Ei ole myöskään vaikea vakuuttua siitä, että riittää osoittaa väite yhdelle monomille. Loppujen lopuksi meidän riittää osoittaa, että

$$\frac{\mathrm{d}}{\mathrm{d}x}\left(x+a\right)^\nu = \nu\left(x+a\right)^{\nu-1}$$

jokaisella positiivisella kokonaisluvulla ν. Tämä onnistuu näppärästi induktiolla. Ensinnäkin,

$$\frac{\mathrm{d}}{\mathrm{d}x}\left(x+a\right) = 1 = 1\cdot\left(x+a\right)^0,$$

joten väite pätee, kun $\nu = 1$. Jos ν sitten on sellainen positiivinen kokonaisluku, että

$$\frac{\mathrm{d}}{\mathrm{d}x}\left(x+a\right)^\nu = \nu\left(x+a\right)^{\nu-1},$$

niin tulon derivoimiskaavalla

$$\begin{aligned}&\frac{\mathrm{d}}{\mathrm{d}x}\left(x+a\right)^{\nu+1} = \frac{\mathrm{d}}{\mathrm{d}x}\left(\left(x+a\right)^\nu\left(x+a\right)\right)\\ &= \left(x+a\right)\frac{\mathrm{d}}{\mathrm{d}x}\left(x+a\right)^\nu + \left(x+a\right)^\nu\frac{\mathrm{d}}{\mathrm{d}x}\left(x+a\right)\\ &= \left(x+a\right)\nu\left(x+a\right)^{\nu-1} + \left(x+a\right)^\nu\cdot 1\\ &= \left(\nu+1\right)\left(x+a\right)^\nu,\end{aligned}$$

ja induktioaskel on valmis. □

Polynomien korkeamman kertaluvun derivaattojen ominaisuuksia

Binomikaava sanoo, että jos a ja b ovat reaalilukuja, ja jos ℓ on positiivinen kokonaisluku, niin

$$(a+b)^\ell = \sum_{m=0}^{\ell} \binom{\ell}{m} a^m\, b^{\ell-m},$$

mikä selittääkin binomikertoimien nimen. Tulon ℓ. derivaatalle pätee varsin samanhenkinen kaava:

Lemma 7. *Olkoot $P(x)$ ja $Q(x)$ reaalilukukertoimisia polynomeja, ja olkoon ℓ positiivinen kokonaisluku. Tällöin*

$$\frac{\mathrm{d}^\ell}{\mathrm{d}x^\ell}\left(P(x)\,Q(x)\right) = \sum_{m=0}^{\ell} \binom{\ell}{m} P^{(m)}(x)\,Q^{(\ell-m)}(x).$$

Todistus. Todistamme tämän induktiolla parametrin ℓ suhteen. Kun $\ell = 1$, kaava sanoo vain, että

$$\frac{\mathrm{d}}{\mathrm{d}x}\left(P(x)\,Q(x)\right) = P'(x)\,Q(x) + P(x)\,Q'(x),$$

mikä onkin aiemmin mainittu derivaatan perusominaisuus. Oletetaan sitten, että positiivinen kokonaisluku ℓ on sellainen, että pätee

$$\frac{\mathrm{d}^\ell}{\mathrm{d}x^\ell}\left(P(x)\,Q(x)\right) = \sum_{m=0}^{\ell} \binom{\ell}{m} P^{(m)}(x)\,Q^{(\ell-m)}(x).$$

Tällöin

$$\begin{aligned}
\frac{\mathrm{d}^{\ell+1}}{\mathrm{d}x^{\ell+1}}\left(P(x)\,Q(x)\right) &= \frac{\mathrm{d}}{\mathrm{d}x}\,\frac{\mathrm{d}^\ell}{\mathrm{d}x^\ell}\left(P(x)\,Q(x)\right) \\
&= \frac{\mathrm{d}}{\mathrm{d}x}\sum_{m=0}^{\ell} \binom{\ell}{m} P^{(m)}(x)\,Q^{(\ell-m)}(x) \\
&= \sum_{m=0}^{\ell} \binom{\ell}{m} P^{(m+1)}(x)\,Q^{(\ell-m)}(x) \\
&\quad + \sum_{m=0}^{\ell} \binom{\ell}{m} P^{(m)}(x)\,Q^{(\ell-m+1)}(x) \\
&= \sum_{m=1}^{\ell+1} \binom{\ell}{m-1} P^{(m)}(x)\,Q^{(\ell+1-m)}(x) \\
&\quad + \sum_{m=0}^{\ell} \binom{\ell}{m} P^{(m)}(x)\,Q^{(\ell+1-m)}(x) \\
&= \sum_{m=0}^{\ell+1} \binom{\ell+1}{m} P^{(m)}(x)\,Q^{(\ell+1-m)}(x),
\end{aligned}$$

missä käytämme viimeisessä yhtäsuuruudessa niitä seikkoja, että

$$\binom{\ell}{0} = \binom{\ell+1}{0} = \binom{\ell}{\ell} = \binom{\ell+1}{\ell+1} = 1,$$

ja

$$\binom{\ell}{m-1} + \binom{\ell}{m} = \binom{\ell+1}{m},$$

kun $m \in \{1, 2, \ldots, \ell\}$. □

Lemma 8. *Olkoon a reaaliluku, olkoon r positiivinen kokonaisluku, olkoon $R(x)$ reaalilukukertoiminen polynomi, ja tarkastellaan polynomia*

$$Q(x) = (x-a)^r\,R(x).$$

Tällöin

$$Q(a) = Q'(a) = Q''(a) = \ldots = Q^{(r-1)}(a) = 0$$

ja

$$Q^{(r)}(a) = r!\,R(a).$$

Todistus. On ilmeistä, että $Q(a) = 0$. Olkoon siis $\ell \in \{1, 2, \ldots, r\}$, ja tarkastellaan lauseketta $Q^{(\ell)}(a)$. Lemman 7 mukaan

$$\begin{aligned}
Q^{(\ell)}(x) &= \sum_{m=0}^{\ell} \binom{\ell}{m} \left(\frac{\mathrm{d}^m}{\mathrm{d}x^m}\,(x-a)^r\right) R^{(\ell-m)}(x) \\
&= \sum_{m=0}^{\ell} \binom{\ell}{m}\, r\,(r-1)\cdots(r-m+1) \\
&\qquad \cdot (x-a)^{r-m}\; R^{(\ell-m)}(x).
\end{aligned}$$

Jos $\ell < r$, niin silloin jokaisessa termissä esiintyy ainakin yksi tekijä $x-a$, ja on oltava $Q^{(\ell)}(a) = 0$. Jos taas $\ell = r$, niin silloin tekijä $x-a$ esiintyy jokaisessa termissä, jossa $m < \ell$, ja jäljelle jää vain se termi, jossa $m = \ell$, ja

$$Q^{(r)}(a) = r!\,R(a),$$

kuten pitikin. □

Epäyhtälöitä

Tarvitsemme hieman työkaluja epäyhtälöistä. Ensimmäinen on kolmioepäyhtälö, johon törmää matematiikassa varsin monissa tilanteissa varsin usein.

Lemma 9 (Kolmioepäyhtälö)**.** *Olkoon n positiivinen kokonaisluku, ja olkoot a_1, a_2, …, a_n reaalilukuja. Tällöin on aina*

$$|a_1 + a_2 + \ldots + a_n| \leqslant |a_1| + |a_2| + \ldots + |a_n|\,.$$

Todistus. Käytämme jälleen induktiota, nyt lukumäärän n suhteen. Tapauksessa $n = 1$ epäyhtälön molemmat puolet ovat yhtä kuin $|a_1|$, ja asia on selvä. Tapauksessa $n = 2$ väite seuraa siitä, että on oltava

$$2a_1a_2 \leqslant |2a_1a_2| = 2\,|a_1| \cdot |a_2|\,,$$

jolloin

$$\begin{aligned}|a_1 + a_2|^2 &= (a_1 + a_2)^2 = a_1^2 + a_2^2 + 2a_1a_2\\ &\leqslant a_1^2 + a_2^2 + 2\,|a_1| \cdot |a_2|\\ &= |a_1|^2 + |a_2|^2 + 2\,|a_1| \cdot |a_2|\\ &= (|a_1| + |a_2|)^2\,.\end{aligned}$$

ja muistaen, että luvut $|a_1 + a_2|$ ja $|a_1| + |a_2|$ ovat molemmat epänegatiivisia, voimme ottaa neliöjuuret puolittain, jolloin saadaan haluttu kolmioepäyhtälö

$$|a_1 + a_2| \leqslant |a_1| + |a_2|\,.$$

Lopuksi, jos n on positiivinen kokonaisluku, $n \geqslant 2$, ja a_1, a_2, …, a_n, a_{n+1} ovat reaalilukuja siten, että

$$|a_1 + a_2 + \ldots + a_n| \leqslant |a_1| + |a_2| + \ldots + |a_n|\,,$$

niin soveltamalla tätä ja kahden muuttujan kolmioepäyhtälöä saadaan

$$\begin{aligned}&|a_1 + a_2 + \ldots + a_n + a_{n+1}|\\ &\leqslant |a_1 + a_2 + \ldots + a_n| + |a_{n+1}|\\ &\leqslant |a_1| + |a_2| + \ldots + |a_n| + |a_{n+1}|\,,\end{aligned}$$

ja olemme valmiita. □

Itse asiassa käytämme kolmioepäyhtälöä myös erääseen äärettömään sarjaan:

Korollaari 10 (Kolmioepäyhtälö sarjoille)**.** *Olkoon a_1, a_2, … jono reaalilukuja, jolle ääretön sarja*

$$\sum_{\mu=1}^{\infty} a_\mu$$

suppenee. Tällöin

$$\left|\sum_{\mu=1}^{\infty} a_\mu\right| \leqslant \sum_{\mu=1}^{\infty} |a_\mu|\,.$$

Emme perustele tätä sen kummemmin tässä, mutta tulos seuraa suoraan äärettömien sarjojen määritelmistä osasummien raja-arvojen kautta.

Toinen epäyhtälötulos, jota tarvitsemme, on varsin erityislaatuinen polynomien derivaattoihin ja eksponenttifunktioon liittyvä arvio. Hermiten lauseen todistuksessa konstruoitavan luvun N määritelmässä esiintyvät korkeamman kertaluvun derivaatat ovat hyödyllisiä mm. siksi, että seuraavan lemman todistuksessa rivillä $(*)$ supistuu eksponenttifunktion Taylorkehitelmästä alku pois.

Lemma 11. *Tarkastellaan reaalilukukertoimista asteen $d \in \mathbb{Z}_+$ polynomia*

$$P(x) = \sum_{\nu=0}^{d} c_\nu\, x^\nu,$$

ja olkoon z reaaliluku. Tällöin polynomille

$$P^*(x) = P(x) + P'(x) + P''(x) + \ldots + P^{(d)}(x)$$

pätee

$$|P^*(z) - e^z\, P^*(0)| \leqslant |z|\, e^{|z|} \sum_{\nu=0}^{d} |c_\nu| \cdot |z|^\nu\,.$$

Todistus. Kirjoitamme polynomin kertoimet $P(x)$ hieman toisella tavalla asettamalla

$$c_\nu = \frac{\gamma_\nu}{\nu!}$$

jokaiselle $\nu \in \{0, 1, 2, \ldots, d\}$, jolloin siis

$$P(x) = \sum_{\nu=0}^{d} \frac{\gamma_\nu\, x^\nu}{\nu!}.$$

Tämän notaation taustalla on se ajatus, että kun $\nu \in \mathbb{Z}_+$, niin termin $x^\nu/\nu!$ derivaatta on yksinkertaisesti $x^{\nu-1}/(\nu-1)!$. Nyt voimme laskea, että

$$\begin{aligned}P^*(x) &= P(x) + P'(x) + P''(x) + \ldots + P^{(d)}(x)\\ &= \sum_{\nu=0}^{d} \frac{\gamma_\nu\, x^\nu}{\nu!} + \sum_{\nu=1}^{d} \frac{\gamma_\nu\, x^{\nu-1}}{(\nu-1)!} + \sum_{\nu=2}^{d} \frac{\gamma_\nu\, x^{\nu-2}}{(\nu-2)!}\\ &\qquad + \ldots + \sum_{\nu=d}^{d} \frac{\gamma_\nu\, x^{\nu-d}}{(\nu-d)!}\\ &= \sum_{\nu=0}^{d} \gamma_\nu \sum_{\mu=0}^{\nu} \frac{x^\mu}{\mu!}.\end{aligned}$$

Erityisesti siis

$$P^*(0) = \sum_{\nu=0}^{d} \gamma_\nu.$$

Nyt voimme arvioida eksponenttifunktion Taylorkehitelmällä, että

$$\begin{aligned}&|P^*(z) - P^*(0)\, e^z|\\ &\quad= \left|\sum_{\nu=0}^{d} \gamma_\nu \sum_{\mu=0}^{\nu} \frac{z^\mu}{\mu!} - \sum_{\nu=0}^{d} \gamma_\nu \sum_{\mu=0}^{\infty} \frac{z^\mu}{\mu!}\right|\\ &\quad= \left|-\sum_{\nu=0}^{d} \gamma_\nu \sum_{\mu=\nu+1}^{\infty} \frac{z^\mu}{\mu!}\right| \qquad (*)\\ &\quad\leqslant \sum_{\nu=0}^{d} |\gamma_\nu| \sum_{\mu=\nu+1}^{\infty} \frac{|z|^\mu}{\mu!},\end{aligned}$$

missä viimeisessä askeleessa käytettiin kolmio-

epäyhtälöä. Viimeistä sarjaa voimme lisäksi arvioida

$$\begin{aligned}
&\sum_{\mu=\nu+1}^{\infty} \frac{|z|^\mu}{\mu!} \\
&= \frac{|z|^{\nu+1}}{\nu!} \left(\frac{1}{\nu+1} + \frac{|z|}{(\nu+1)(\nu+2)} \right. \\
&\qquad\qquad \left. + \frac{|z|^2}{(\nu+1)(\nu+2)(\nu+3)} + \ldots \right) \\
&\leqslant \frac{|z|^{\nu+1}}{\nu!} \left(1 + \frac{|z|}{1!} + \frac{|z|^2}{2!} + \ldots \right) \\
&= \frac{|z|^{\nu+1}}{\nu!}\, e^{|z|}.
\end{aligned}$$

Yhdistämällä tämä aiempaan arvioomme saamme siis

$$\begin{aligned}
|P^*(z) - P^*(0)\, e^z| &\leqslant \sum_{\nu=0}^{d} |\gamma_\nu| \, \frac{|z|^{\nu+1}}{\nu!}\, e^{|z|} \\
&= |z|\, e^{|z|} \sum_{\nu=0}^{d} |c_\nu| \cdot |z|^\nu .
\end{aligned}$$

kuten pitikin. □

Vietan kaavat ja eräs niiden seuraus

Ei ole hankala laskea, että millä tahansa reaaliluvuilla a, b, c ja d pätee

$$(x-a)(x-b) = x^2 - (a+b)\,x + ab,$$

ja

$$\begin{aligned}
(x-a)(x-b)(x-c) &= x^3 - (a+b+c)\,x^2 \\
&\quad + (ab+bc+ca)\,x - abc,
\end{aligned}$$

ja vielä

$$\begin{aligned}
&(x-a)(x-b)(x-c)(x-d) \\
&\quad = x^4 - (a+b+c+d)\,x^3 \\
&\qquad + (ab+ac+ad+bc+bd+cd)\,x^2 \\
&\qquad - (abc+abd+acd+bcd)\,x + abcd.
\end{aligned}$$

Yleisessä tapauksessa näitä yhteyksiä polynomin nollakohtien ja sen kertoimien välillä kutsutaan *Vietan kaavoiksi*:

Lause 12 (Vietan kaavat)**.** *Olkoon d positiivinen kokonaisluku, ja olkoot a, a_1, a_2, …, a_d, c_0, c_1, c_2, …, c_d reaalilukuja siten, että*

$$\begin{aligned}
&a\,(x-a_1)\,(x-a_2)\cdots(x-a_d) \\
&\qquad = c_0 + c_1\,x + c_2\,x^2 + \ldots + c_d\,x^d.
\end{aligned}$$

Tällöin jokaisella $\nu \in \{0, 1, 2, \ldots, d-1\}$ pätee

$$c_\nu = a \cdot (-1)^{d-\nu} \sum_{\substack{I \subseteq \{1,2,\ldots,d\},\ i \in I \\ \#I = d-\nu}} \prod a_i,$$

missä siis viimeisessä summassa I käy läpi kaikki joukon $\{1, 2, \ldots, d\}$ täsmälleen $d-\nu$ lukua sisältävät osajoukot ja $\prod$-lausekkeessa otetaan yhtä sellaista joukkoa I vastaavien lukujen a_i tulo. Toisin sanoen, $\sum\prod$-lausekkeessa otetaan luvuista a_1, …, a_d kaikkien $d-\nu$ luvun osajoukkojen tulojen summa.

Vietan kaavat ovat tarpeen seuraavan lemman vuoksi. Sovellettaessa kolmioepäyhtälöä vastaan tulee polynomi, joka on saatu eräästä toisesta polynomista ottamalla jokaisesta kertoimesta itseisarvot. On oleellista, että seuraavassa lemmassa nollakohdat a_1, …, a_d ovat juuri epänegatiivisia reaalilukuja.

Lemma 13. *Olkoon d positiivinen kokonaisluku, olkoon a nollasta poikkeava reaaliluku, olkoot a_1, a_2, …, a_d epänegatiivisia reaalilukuja, ja olkoot c_0, c_1, …, c_d reaalilukuja niin, että*

$$\begin{aligned}
&c_0 + c_1\,x + c_2\,x^2 + \ldots + c_{d-1}x^{d-1} + c_d\,x^d \\
&\qquad = a\,(x-a_1)\,(x-a_2)\cdots(x-a_d).
\end{aligned}$$

Tällöin

$$\begin{aligned}
&|c_0| + |c_1|\,x + |c_2|\,x^2 + \ldots + |c_d|\,x^d \\
&\qquad = |a|\,(x+a_1)\,(x+a_2)\cdots(x+a_d).
\end{aligned}$$

Todistus. Ensinnäkin $c_d = a$, ja Vietan kaavojen mukaan jokaisella $\nu \in \{0, 1, \ldots, d-1\}$ pätee

$$\frac{c_\nu}{a} = (-1)^{d-\nu} \sum_{\substack{I \subseteq \{1,2,\ldots,d\},\ i \in I \\ \#I = d-\nu}} \prod a_i.$$

Koska tässä summassa kaikki termit ovat epänegatiivisia, on siis oltava

$$\begin{aligned}
|c_\nu| &= |a| \sum_{\substack{I \subseteq \{1,2,\ldots,d\},\ i \in I \\ \#I = d-\nu}} \prod a_i \\
&= |a|\,(-1)^{d-\nu} \sum_{\substack{I \subseteq \{1,2,\ldots,d\},\ i \in I \\ \#I = d-\nu}} \prod (-a_i),
\end{aligned}$$

missä hyödynnämme sitä tietoa, että jokaisessa $\prod$-tulossa on täsmälleen $d-\nu$ tekijää. Mutta Vietan kaavojen mukaan siis

$$\begin{aligned}
&\sum_{\nu=0}^{d} |c_\nu|\, x^\nu \\
&\qquad = |a|\,(x-(-a_1))\,(x-(-a_2))\cdots(x-(-a_d)),
\end{aligned}$$

kuten pitikin. □

Hermiten lauseen todistus

Alku ja strategia. Aloitamme tekemällä sen vastaoletuksen, että e on algebrallinen. Tällöin on olemassa positiivinen kokonaisluku n ja kokonaisluvut a_0, a_1, $\ldots$, a_n niin, että

$$a_0 + a_1\, e + a_2\, e^2 + \ldots + a_n\, e^n = 0,$$

ja $a_n \neq 0$. Voimme luonnollisesti olettaa, että n on pienin tällainen luku. Nyt $a_0 \neq 0$, sillä jos olisi $k \in \{0, 1, \ldots, n-1\}$, jolle

$$a_0 = a_1 = \ldots = a_k = 0 \quad \text{ja} \quad a_{k+1} \neq 0,$$

niin voisimme jakaa luvun e toteuttaman yhtälön luvulla e^{k+1}, saaden uuden yhtälön

$$a_{k+1} + a_{k+2}\, e + a_{k+3}\, e^2 + \ldots + a_n\, e^{n-k-1} = 0,$$

minkä aste olisi pienempi kuin n.

Valitsemme alkuluvun p, jolle $p > n$ ja $p > |a_0|$. Tulemme aivan lopuksi vielä vaatimaan, että p on isompi kuin jokin $\Xi + 1$, missä Ξ tulee lemmasta 3.

Määrittelemme rationaalilukukertoimisen polynomin $P(x)$ asettamalla

$$P(x) = \frac{1}{(p-1)!}\, x^{p-1}\, (x-1)^p\, (x-2)^p \cdots (x-n)^p\,.$$

Tämän polynomin aste on $d = (n+1)\, p - 1$.

Seuraavaksi määrittelemme luvuista p ja n riippuvan rationaaliluvun N asettamalla

$$N = \sum_{\ell=0}^{d} \sum_{k=0}^{n} a_k\, P^{(\ell)}(k).$$

Tavoitteemme on osoittaa ensin, että $N \neq 0$, ja sitten että $N = 0$, kunhan vain p on riittävän iso. Tämä ristiriita osoittaa luvun e transkendenttisuuden.

Miksi $N \neq 0$? Osoittaaksemme, että $N \neq 0$, osoitamme, että itse asiassa N on kokonaisluku, joka ei ole jaollinen luvulla p. Tämä saavutetaan osoittamalla, että itse asiassa jokainen termi luvun N määrittelevässä summassa on kokonaisluku, ja että termiä $a_0\, P^{(p-1)}(0)$ lukuun ottamatta ne kaikki ovat jaollisia luvulla p.

Lemman 8 nojalla

$$P(0) = P'(0) = \ldots = P^{(p-2)}(0) = 0,$$

ja samoin

$$P(k) = P'(k) = \ldots = P^{(p-1)}(k) = 0$$

jokaisella $k \in \{1, 2, \ldots, n\}$. Saman lemman mukaan

$$\begin{aligned} P^{(p-1)}(0) &= \frac{1}{(p-1)!}\, (p-1)!\, (-1)^p\, (-2)^p \cdots (-n)^p \\ &= (-1)^{pn}\, (n!)^p\,. \end{aligned}$$

Tiedämme siis, että $a_0\, P^{(p-1)}(0)$ on kokonaisluku, ja koska $p > n$ ja $p > |a_0|$, sen on oltava alkuluvulla p jaoton kokonaisluku.

Meidän on vielä käsiteltävä termit $a_k\, P^{(\ell)}(k)$, missä $\ell \in \{p, p+1, \ldots, d\}$ ja $k \in \{0, 1, 2, \ldots, n\}$. Kirjoitetaan tätä varten

$$P(x) = \frac{1}{(p-1)!} \sum_{\nu=p-1}^{d} c_\nu\, x^\nu,$$

missä luvut c_{p-1}, c_p, $\ldots$, c_d ovat kokonaislukuja. Voimme laskea, että

$$P^{(\ell)}(k) = \frac{1}{(p-1)!} \sum_{\nu=\ell}^{d} c_\nu\, \nu\, (\nu-1) \cdots (\nu-\ell+1)\, k^{\nu-\ell}.$$

Koska lemman 2 nojalla tulo $\nu \cdots (\nu - \ell + 1)$ on $\ell > p-1$ peräkkäisen kokonaisluvun tulona jaollinen luvulla $(p-1)!$, on luvun $P^{(\ell)}(k)$ oltava kokonaisluku. Lisäksi, koska $\ell \geqslant p$, on tulossa vähintään p peräkkäistä tekijää, joten ainakin yksi tekijöistä on jaollinen luvulla p. Koska p on alkuluku, ei nimittäjä $(p-1)!$ ole jaollinen luvulla p. Täten luvun $P^{(\ell)}(k)$ on oltava jaollinen luvulla p.

Olemme siis todistaneet, että N on kokonaisluku, joka ei ole jaollinen luvulla p, joten on oltava $N \neq 0$.

Miksi $N = 0$? Yritetään seuraavaksi arvioida luvun N kokoa. Kirjoittamalla

$$P^*(x) = P(x) + P'(x) + P''(x) + \ldots + P^{(d)}(x),$$

voimme kirjoittaa

$$\begin{aligned} N &= a_0\, P^*(0) + a_1\, P^*(1) + a_2\, P^*(2) + \ldots + a_n\, P^*(n) \\ &= a_0\, P^*(0) + a_1\, P^*(1) + \ldots + a_n\, P^*(n) \\ &\qquad - P^*(0)\, (a_0 + a_1\, e + \ldots + a_n\, e^n) \\ &= a_1\, (P^*(1) - e\, P^*(0)) + a_2\, \big(P^*(2) - e^2\, P^*(0)\big) \\ &\qquad + \ldots + a_n\, (P^*(n) - e^n\, P^*(0))\,. \end{aligned}$$

Siten voimme arvioida kolmioepäyhtälöllä ja lemman 11 nojalla, että

$$\begin{aligned} |N| &\leqslant \sum_{k=1}^{n} |a_k| \cdot \big|P^*(k) - e^k\, P^*(0)\big| \\ &\leqslant \sum_{k=1}^{n} |a_k|\, k\, e^k\, \frac{1}{(p-1)!} \sum_{\nu=p-1}^{d} |c_\nu|\, k^\nu. \end{aligned}$$

Lemman 13 nojalla voimme arvioida viimeistä summaa

$$\begin{aligned} \sum_{\nu=p-1}^{d} |c_\nu|\, k^\nu &= k^{p-1}\, (k+1)^p\, (k+2)^p \cdots (k+n)^p \\ &\leqslant ((2n)!)^p\,. \end{aligned}$$

Siten saamme arvion

$$|N| \leqslant n\, e^n \sum_{k=1}^{n} |a_k|\, \frac{((2n)!)^p}{(p-1)!}.$$

Valitsemalla lemmassa 3

$$\varepsilon = 1, \quad A = n\,e^n \sum_{k=1}^{n} |a_k|\,(2n)!, \quad \text{ja} \quad B = (2n)!,$$

löytyy positiivinen kokonaisluku Ξ siten, että $|N| < 1$ kunhan vain alkuluvun p valinnassa pidetään huolta, että $p-1 > \Xi$. Koska N oli kokonaisluku, on epäyhtälö $|N| < 1$ mahdollinen vain silloin, kun $N = 0$, ja olemme valmiit.

Yleistyksiä seurauksineen

Itse asiassa yllä annettu Hermiten lauseen todistus on voimallisempi kuin voisi ajatella. Nimittäin, samassa hengessä pystyy todistamaan huomattavasti yleisempiä ja vahvempia tuloksia, vaikka emme olekaan tehneet tässä niin. Eräs oleellisesti vahvempi tulos, jonka voi todistaa varsin samanlaisilla työkaluilla, jos lisäksi käytettävissä on hieman symmetristen polynomien ominaisuuksia ja algebrallisten lukujen perusominaisuuksia, on tällainen:

Lause (Hermiten–Lindemannin lause)**.** *Jos α on algebrallinen luku ja $\alpha \neq 0$, niin e^α on transkendentaalinen luku.*

Vaikka emme todista tätä lausetta tässä, on kenties valaisevaa nähdä, mitä kaikkea siitä seuraa:

Korollaari. *Luku e on transkendentaalinen.*

Todistus. Koska luku 1 on selvästi nollasta poikkeava ja algebrallinen, on luvun $e = e^1$ oltava transkendentaalinen. □

Korollaari. *Luku π on transkendentaalinen.*

Todistus. Jos luku π olisi algebrallinen, olisi myös luku $i\pi$ kahden algebrallisen luvun tulona algebrallinen. Se on myös selvästi nollasta poikkeava. Siten luvun $e^{i\pi}$ pitäisi olla transkendentaalinen. Mutta Eulerin kauniin kaavan nojalla $e^{i\pi} = -1$ ja -1 ei ole transkendentaalinen luku. Siten π on transkendentaalinen luku. □

Korollaari. *Jos α on algebrallinen luku, $\alpha \neq 0$ ja $\alpha \neq 1$, niin $\log\alpha$ on transkendentaalinen.*

Todistus. Jos olisi $\log\alpha = \beta$, jollakin algebrallisella luvulla β, niin olisi toisaalta $\beta \neq 0$, ja toisaalta luku $e^\beta = \alpha$ olisi algebrallinen vastoin Hermiten–Lindemannin lausetta. □

Korollaari. *Jos α on algebrallinen luku ja $\alpha \neq 0$, niin $\sin\alpha$ ja $\cos\alpha$ ovat transkendentaalisia lukuja.*

Todistus. Koska tunnetusti

$$\sin^2\alpha + \cos^2\alpha = 1,$$

seuraa tästä, että jos toinen luvuista $\sin\alpha$ ja $\cos\alpha$ on algebrallinen, niin toinen on ratkaisu sellaiselle polynomiyhtälölle, jonka kertoimet ovat algebrallisia lukuja, ja siten myös algebrallinen. Jos $\sin\alpha$ ja $\cos\alpha$ ovat transkendenttisia, niin olemme valmiita. Oletetaan siis, että $\sin\alpha$ ja $\cos\alpha$ ovat algebrallisia. Tällöin myös luku

$$i\sin\alpha + \cos\alpha$$

olisi algebrallinen. Mutta toisaalta

$$i\sin\alpha + \cos\alpha = i \cdot \frac{e^{i\alpha} - e^{-i\alpha}}{2i} + \frac{e^{i\alpha} + e^{-i\alpha}}{2} = e^{i\alpha},$$

ja viimeksi mainitun luvun on oltava transkendenttinen. Tämä ristiriita osoittaa, että $\sin\alpha$ ja $\cos\alpha$ eivät voi olla algebrallisia. □

Korollaari. *Jos α on algebrallinen luku ja $\alpha \neq 0$, niin $\tan\alpha$ on transkendentaalinen luku.*

Todistus. Huomautetaan, että $\cos\alpha \neq 0$, koska muutoin α olisi luvun π monikerran puolikkaana transkendenttinen. Samasta syystä on oltava $\sin\alpha \neq 0$. Oletetaan siis, että olisi $\tan\alpha = \beta$, jollakin algebrallisella luvulla $\beta \neq 0$. Tällöin olisi

$$\beta = \tan\alpha = \sin\alpha \cdot \frac{1}{\cos\alpha} = \frac{e^{i\alpha} - e^{-i\alpha}}{2i} \cdot \frac{2}{e^{i\alpha} + e^{-i\alpha}},$$

ja edelleen

$$i\beta e^{i\alpha} + i\beta e^{-i\alpha} = e^{i\alpha} - e^{-i\alpha},$$

ja vielä sieventämällä

$$(1 - i\beta)\,e^{i\alpha} = (1 + i\beta)\,e^{-i\alpha}.$$

Jos $1 - i\beta = 0$, niin $1 + i\beta = 0$, koska eksponenttifunktion kaikki arvot ovat nollasta poikkeavia, ja tällöin olisi

$$\beta = \frac{1 + i\beta}{2i} - \frac{1 - i\beta}{2i} = 0 - 0 = 0.$$

Siten on oltava $1 - i\beta \neq 0$, ja voimme sieventää vielä kerran saadaksemme

$$e^{2i\alpha} = \frac{1 + i\beta}{1 - i\beta}.$$

Tässä $2i\alpha$ on nollasta poikkeava algebrallinen luku, ja yhtälön oikea puoli on algebrallinen, ja siten olemme saavuttaneet ristiriidan. □

Samanlaisia transkendentaalisuustuloksia voisi esittää myös muille tutuille transkendentaalisille funktioille, kuten sinh, cosh, tanh, arcsin, arccos, arctan, arsinh, arcosh ja artanh, mutta sivuutamme yksityiskohdat tässä.

Mainittakoon lopuksi vielä yksi vahvempi tulos, jonka voi todistaa varsin samassa hengessä ja samoin työkaluin kuin Hermiten–Lindemannin lauseen:

Lause (Lindemannin–Weierstrassin lause)**.** *Jos n on positiivinen kokonaisluku, jos α_1, α_2, …, α_n ovat algebrallisia lukuja, joista mitkään kaksi eivät ole yhtä suuria, ja jos β_1, β_2, …, β_n ovat nollasta poikkeavia algebrallisia lukuja, niin*

$$\beta_1 e^{\alpha_1} + \beta_2 e^{\alpha_2} + \ldots + \beta_n e^{\alpha_n} \neq 0.$$

Kirjallisuudesta

Hermiten lause todistetaan monissa eri teoksissa, kuten vaikkapa [1, 3, 5, 7]. Tällaisissa transkendenttitodistuksissa yleinen integraalien tai väliarvolauseen soveltaminen on korvattu eksponenttifunktion Taylorkehitelmän käytöllä kirjan [5] lukujen e ja π transkendenttisuuksien todistuksia seuraten.

Hermiten–Lindemannin ja Lindemannin–Weierstrassin lauseen todistuksia löytyy vaikkapa teoksista [1, 3, 7], joista löytyy myös algebrallisten lukujen perusteoriaa. Algebrallisista luvuista perustietoa löytyy myös mainiosta kirjasta [6]. Vanha klassikoteos [8] sisältää helposti lähestyttävässä muodossa materiaalia niin algebrallisista luvuista kuin sovellutuksista mm. yhtälöön $x^3 + y^3 = z^3$, yhtälöiden algebralliseen ratkeavuuteen ja harpilla ja viivaimella tehtäviin konstruktioihin.

Solmunkin sivuilla on aiemmin ilmestynyt aiheeseen liittyviä artikkeleita. Artikkelissa [2] irrationaalisista, algebrallisista ja transkendentaalisista luvuista löytyy todistukset luvun e irrationaalisuudelle ja Liouvillen kauniille lauseelle, joka on yksinkertaisin tapa konstruoida konkreettisia transkendenttisia lukuja. Artikkelissa [4] on esitetty todistus lukujen π ja π^2 irrationaalisuudelle. Hermiten lauseen todistusta voi halutessaan verrata näihin lukujen e ja π irrationaalisuuksien todistuksiin.

Viitteet

[1] Burger, E. B., ja R. Tubbs: *Making Transcendence Transparent. An intuitive approach to classical transcendental number theory*, Springer, 2004.

[2] Ernvall-Hytönen, A.-M.: *Rationaalisia, irrationaalisia, algebrallisia ja transkendenttisiä otuksia*, Solmu, 3/2014, 12–15.

[3] Гельфонд, А. О.: *Трансцендентные и алгебраические числа*, URSS, 2015.

[4] Lehtinen, M.: *Miksi π on irrationaalinen?*, Solmu, 2/2001, 6–8.

[5] Perron, O.: *Irrationalzahlen*, Göschens Lehrbücherei, Reine und angewandte Mathematik, 1, Walter de Gruyter & Co, 1960.

[6] Pollard, H., ja H. G. Diamond: *The Theory of Algebraic Numbers*, Dover Publications, 1998.

[7] Шидловский, А. Б.: *Диофантовы приближения и трансцендентные числа*, Fizmatlit, 2007.

[8] Väisälä, K.: *Lukuteorian ja korkeamman algebran alkeet*, Tiedekirjasto, 17, Otava, 1961.