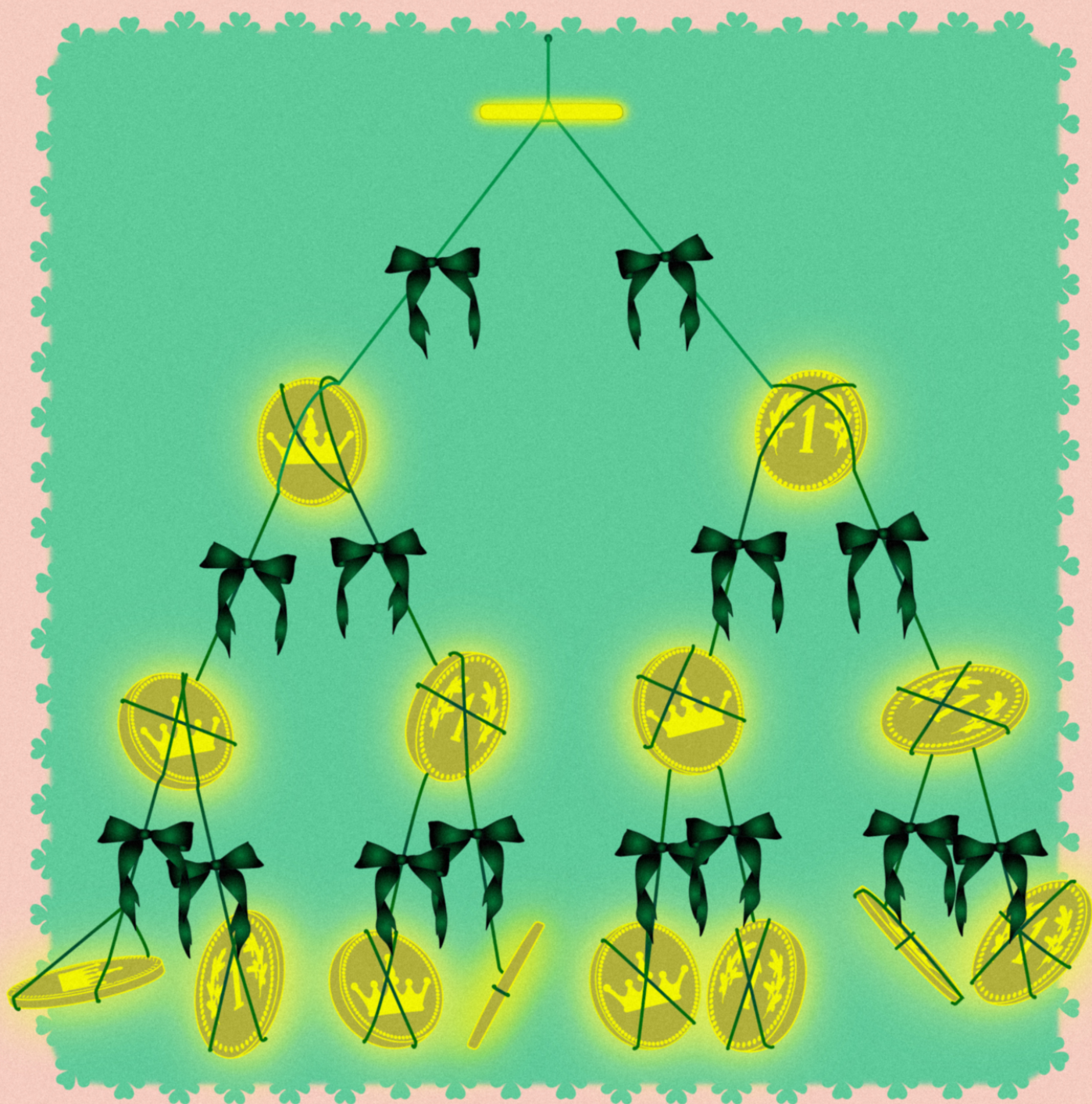


S&LMU

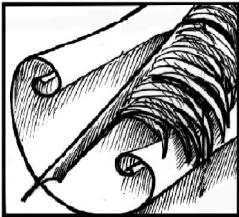
MATEMATIIKKALEHTI 3/2025

matematiikkalehtisolmu.fi



Sisällys

Pääkirjoitus: Matematiikan kertauskurssit ja osaaminen yliopisto-opintojen alussa (Anne-Maria Ernvall-Hytönen)	3
Pupujussin kuolema (Markku Halmetoja)	5
Miksei funktiota e^{-x^2} voi integroida? (Osa 2/2) (Milo Orlich)	7
Topologiasta ja matematiikan soveltamisesta (Marjatta Näätänen)	17
Rahapeliongelma (Jukka Liukkonen)	19
Ympyrän neliöiminen (Reijo Hautakangas)	24



Matematiikan kertauskurssit ja osaaminen yliopisto-opintojen alussa

Pääkirjoitus

Matematiikan osaamisesta on puhuttu paljon eri yhteyksissä. Yliopistoilla on erityisesti huomattu tarve lukiomatematiikan kertauskursseille. Tällaisia ovatkin eri yliopistot kehittäneet hiukan eri lähtökohdista ja hiukan eri kohderyhmille. On nimittäin melko eri tilanne, pitääkö varmistaa, että jokainen pitkän matematiikan kurssi on riittävän hyvin hallussa, jotta ensimmäisen vuoden matematiikan opinnot sujuvat, vai onko varmistettava se, että matematiikkaa lähinnä menetelmänä opiskelevalla ihmisellä on riittävä hallinta lukiomatematiikan perusteista.

Kertauskursseihin liittyy periaatteellinen dilemma: voidaanko yliopistossa antaa opintopisteitä kurssista, joka ei sisällä sen erityisempää yliopistosisältöä, vaan jossa vain kerrataan jo toivottavasti aiemmin opiskeltuja sisältöjä? Jos voidaan, niin mihin kokonaisuuteen tällaiset opintopisteet voidaan hyväksyä?

Toinen puoli tietenkin on pohdinta siitä, että ei myöskään ole hyvä, jos ihmiset tulevat kursseille vajavaisella osaamisella. He eivät todennäköisesti saa niin paljon kurseista irti kuin pitäisi, eikä tilanne välttämättä ole hyvä muillekaan kurssilaisille.

Moniin kieliin verrattuna matematiikan tilanne on kuitenkin varsin lohdullinen. Yle raportoi joulukuussa 2025 [1], että jatkossa joidenkin yliopistojen joihinkin kielten tutkinto-ohjelmiin voi päästä, vaikka kieltä ei olisi opiskellut aiemmin. Ylen artikkeli kertoo, että tällöin opiskelijan on tarkoitus ensimmäisen opiskeluvuoden aikana saada sellainen kielitaito, joka vastaa lukion

lyhyttä oppimäärää. Tämän jälkeen voi jatkaa perusopintoihin. Ratkaisun takana on se, että useita vieraita kieliä opiskellaan nykyään hyvin vähän. Tämä näkyy myös esimerkiksi eri kielten kirjoittajamäärissä ylioppilaskokeessa. Siinä missä kevään 2026 pitkän ja lyhyen matematiikan kokeisiin on ilmoittautunut yhteensä 29340 kokeilasta, esimerkiksi pitkän ja lyhyen saksan kokeisiin tänä keväänä on ilmoittautunut yhteensä 1341 kokeilasta ja pitkän ja lyhyen ranskan kokeisiin 852 kokeilasta [2].

Ylioppilaskokeiden kielten kirjoittajien laskutrendistä olen itsekin kirjoittanut Solmun pääkirjoituksessa 3/23 näkökulmana se, että alamäki alkoi jo merkittävästi ennen korkeakoulujen yhteisvalinnan pisteuudistusta, jossa pitkän matematiikan kokeesta sai reilusti pisteitä. Pisteytystä on itse asiassa jälleen uudistettu: ensi syksystä alkaen pitkä matematiikka ei enää anna niin paljon pisteitä kaikilla aloilla. Toistaiseksi tämän uudistuksen merkitys kirjoittajamäärien kannalta näyttää pieneltä: edelliseen kevääseen verrattuna pitkän matematiikan kokeeseen on ilmoittautunut 390 kokeilasta eli 2,69 % vähemmän kuin vuotta aiemmin ja lyhyen matematiikan kokeeseen on ilmoittautunut 1024 kokeilasta enemmän [2]. Pitkän matematiikan kokeilasmäärän väheneminen on siis hyvin vähäistä, eikä todennäköisesti vaikuta mitenkään siihen, millaisilla esitiedoilla opiskelijat tulevat yliopistolle.

Anne-Maria Ernvall-Hytönen

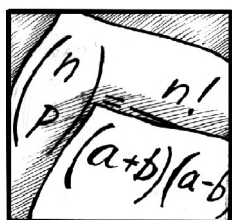
Viitteet

- [1] Minna Matintupa. Yliopistojen kieliopinnot avataan ummikoille – professori syyttää peruskoulua suomalaisten kielitaidon näivettymisestä. Yle 12.12.2025.

<https://yle.fi/a/74-20199131>

- [2] Ylioppilastutkintoon osallistujat kokeittain (kaikki kokelaslajit) tutkintokerrat kevät 2025 ja kevät 2026.

<https://tiedostot.ylioppilastutkinto.fi/ext/stat/FB2026KT2001.pdf>



Pupujussin kuolema

Markku Halmetoja

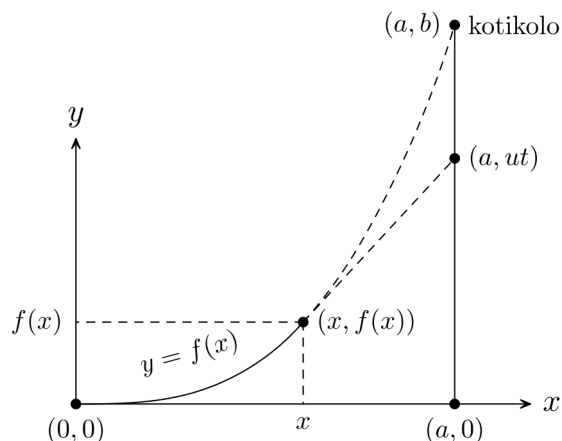
Katselin hiljattain ikkunastani takapihalle säätilaa arvioidakseni ja havaitsin pensasaidan vieressä vilkasta liikehdintää. Joukko harakoita ja variksia näytti pitävän kiivaanpuoleista torikokousta. Ihmettelin, mitä nämä kaksi eivät aivan ystävällisissä väleissä olevaa heimoa keskenään puuhaavat, kunnes näin, että ne olivat yhteisellä aterialla. Ruokalistalla oli edesmennyt pupujussi, jota linnut kilvan näykkivät terävillä nokillaan. Linnut eivät elävän pupun kimppuun kävisi; kuolinsyy lienee ollut loukkaantuminen tai vanhuus. Luonnossa mikään ei mene hukkaan: toisen kuolema on toisen elämä. Tätä kiertokulkua siinä miettiessäni muistin, että olin parikymmentä vuotta sitten ratkaissut aiheetta sivuavan tehtävän. Kyseessä oli Helsingin yliopiston matematiikan laitoksen sivulta löytämäni differentiaaliyhtälöitä sisältäneen kurssin laskuharjoituksen tehtävä:

Petolintu lentää 50 metrin korkeudella ja havaitsee suoraan alapuolellaan pupujussin. Lintu lähtee syöksymään vakiovauhdilla v kohti pupua, joka samalla hetkellä lähtee loikkimaan nopeudella 10 m/s kohti sadan metrin päässä olevaa kotikoloaan. Lintu suuntaa syöksynsä joka hetki pupua kohti. Mikä on pienin v , jolla lintu tavoittaa pupujussin?

Laadin tuolloin tilanteesta erilaisia yhtälöitä, mutta jokin tuntui aina estävän ratkaisuun pääsyn. Aikani veivattuani kysyin neuvoa laskuharjoituksen tekijältä Petri Olalta (hänelle kiitos), ja hän opastikin asettamaan tilanteen koordinaatistoon kuvion osoittamalla tavalla. Kun vielä merkitään $a = 50$ m, $b = 100$ m ja $u = 10$ m/s, päästään todella kauniisiin yhtälöihin.

Alkakoon linnun syöksy hetkellä $t = 0$ ja olkoon $y =$

$f(x)$ linnun ratakäyrän yhtälö. Lintu lähtee origosta ja syöksy alkaa kohtisuoraan alas, joten $f(0) = 0$ ja $f'(0) = 0$. Linnun syöksymisnopeus $v(> u)$ on pienin mahdollinen silloin, kun se tavoittaa pupun sen kotikolon edustalla. Siis $f(a) = b$.



Jos lintu on hetkellä t pisteessä $(x, f(x))$, niin se on aikavälillä $[0, t]$ kulkenut matkan vt ja toisaalta matka on käyrän $y = f(x)$ välillä $[0, x]$ olevan osan pituus. Siis

$$vt = \int_0^x \sqrt{1 + [f'(\xi)]^2} d\xi. \quad (1)$$

Hetkellä t pupu on pisteessä (a, ut) . Koska linnun syöksy suuntautuu jatkuvasti pupua kohti, saamme sen lentoradan kohdassa x olevan tangentin kulmakertoimen

eli funktion f derivaatan esitettyä pupun sijainnin avulla,

$$f'(x) = \frac{f(x) - ut}{x - a},$$

mistä seuraa

$$ut = f(x) + f'(x)(a - x). \quad (2)$$

Eliminoimalla t :n yhtälöistä (1) ja (2) saamme yhtälön, josta ratkaistaan ratakäyrä $y = f(x)$, ja sen avulla v . Aluksi paljasta näytettävä yhtälö

$$\frac{u}{v} \int_0^x \sqrt{1 + [f'(\xi)]^2} d\xi = f(x) + f'(x)(a - x)$$

siistiyytään derivoimalla muotoon

$$\frac{u}{v} \sqrt{1 + [f'(x)]^2} = f''(x)(a - x). \quad (3)$$

Merkitsemällä $p = f'(x)$, jolloin $f''(x) = \frac{dp}{dx}$, saamme (3):sta

$$\frac{u}{v} \sqrt{1 + p^2} = \frac{dp}{dx}(a - x),$$

mistä muuttujat erottamalla tulee

$$\frac{dp}{\sqrt{1 + p^2}} = \frac{u}{v} \frac{dx}{a - x},$$

ja edelleen integroimalla

$$\ln(p + \sqrt{1 + p^2}) = -\frac{u}{v} \ln(a - x) + A.$$

Koska $p(0) = f'(0) = 0$, saamme $A = \frac{u}{v} \ln a$, ja yhtälö sievenee muotoon

$$\ln(p + \sqrt{1 + p^2}) = \frac{u}{v} \ln\left(\frac{a}{a - x}\right).$$

Huomaamalla, että tämän yhtälön vasen puoli on hyperbolisen sinin^{*)} käänteisfunktio, saamme

$$\begin{aligned} p &= \sinh\left(\ln\left(\frac{a}{a - x}\right)^{u/v}\right) \\ &= \frac{1}{2}\left(\frac{a}{a - x}\right)^{u/v} - \frac{1}{2}\left(\frac{a - x}{a}\right)^{u/v} \\ &= f'(x). \end{aligned}$$

Kirjoittamalla derivaatta muotoon

$$f'(x) = \frac{1}{2}\left(1 - \frac{x}{a}\right)^{-u/v} - \frac{1}{2}\left(1 - \frac{x}{a}\right)^{u/v}$$

saadaan integroimalla

$$\begin{aligned} f(x) &= \frac{av}{2(v + u)}\left(1 - \frac{x}{a}\right)^{1+u/v} \\ &\quad - \frac{av}{2(v - u)}\left(1 - \frac{x}{a}\right)^{1-u/v} + B. \end{aligned}$$

Ehdosta $f(0) = 0$ seuraa

$$B = \frac{a}{2}\left(\frac{v}{v - u} - \frac{v}{v + u}\right) = \frac{auv}{v^2 - u^2},$$

joten ratakäyrän yhtälö on

$$\begin{aligned} f(x) &= \frac{av}{2(v + u)}\left(1 - \frac{x}{a}\right)^{1+u/v} \\ &\quad - \frac{av}{2(v - u)}\left(1 - \frac{x}{a}\right)^{1-u/v} + \frac{auv}{v^2 - u^2}. \end{aligned}$$

Ehdosta $f(a) = b$ saamme v :n ratkaisemiseksi yhtälön

$$f(a) = \frac{auv}{v^2 - u^2} = b,$$

mikä annettujen numeeristen arvojen sijoittamisen jälkeen pelkistyy muotoon

$$v^2 - 5v - 100 = 0.$$

Haukalta vaadittava nopeus on siis

$$v = \frac{1}{2}\sqrt{5 + 5\sqrt{17}} \text{ m/s} \approx 12,81 \text{ m/s}.$$

Seuraavana aamuna linnut olivat poissa eikä pupusta näkynyt suolen pätkääkään. Ilmeisesti kettu oli yön pimeydessä käynyt kuitaamassa oman osansa saaliista.

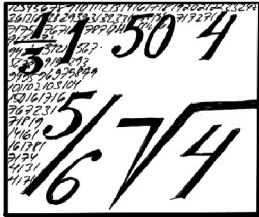
*) Hyperbolisia funktioita $\sinh$ ja $\cosh$ ei ehkä näy nykylukion oppimäärässä. Niiden määritelmät ovat kuitenkin perin yksinkertaiset:

$$\cosh x = \frac{1}{2}(e^x + e^{-x}) \quad \text{ja} \quad \sinh x = \frac{1}{2}(e^x - e^{-x}).$$

Välittömästi nähdään, että funktiot ovat toistensa derivaattoja ja että $\cosh x \geq 1$ kaikilla $x \in \mathbb{R}$. Täten hyperbolinen sini on aidosti kasvava ja sillä on käänteisfunktio:

$$\begin{aligned} y &= \sinh x = \frac{1}{2}(e^x - e^{-x}) \\ &\iff \\ x &= \sinh^{-1} y = \ln(y + \sqrt{1 + y^2}). \end{aligned}$$

Hyperbolisten funktioiden nimet muistuttavat trigonometristen funktioiden sinin ja kosinin nimiä. Funktioilla onkin mielenkiintoinen ja syvällinen yhteys, mikä paljastuu, kun nämä funktiot määritellään kompleksiluvuille. Sitä kannattaa matematiikasta kiinnostuneen lukijalaisen odottaa ja tehdä ahkerasti töitä, jotta pääsee matematiikan syventäviin opintoihin yliopistossa.



Miksei funktiota e^{-x^2} voi integroida? (Osa 2/2)

Milo Orlich

milo.orlich@alumni.aalto.fi

Tämä on artikkelin [3] jatko. Tässä osassa todistetaan Liouvillen lause. Tätä lausetta ja Lausetta 29 lukuun ottamatta artikkelin ensimmäisen osan tuloksia ja määritelmiä ei toisteta.

Jatkossa käytetään seuraavaa notaatiota.

Määritelmä 1. Jos laajennusta $\mathbb{K}(\alpha)$ halutaan laajentaa lisää alkiolla β , niin merkinnän $\mathbb{K}(\alpha)(\beta)$ sijaan kirjoitetaan $\mathbb{K}(\alpha, \beta)$. Ja samoin jos on monta alkiota $\alpha_1, \dots, \alpha_n$, kirjoitetaan $\mathbb{K}(\alpha_1, \dots, \alpha_n)$.

Toistetaan Liouvillen lauseen (eli artikkelin ensimmäisen osan Lauseen 29) väite:

Lause 2 (Liouville). Olkoot $\mathbb{K}$ derivaatan suhteen suljettu kunta meromorfinen funktioita ja $\alpha \in \mathbb{K}$. On olemassa kunnan $\mathbb{K}$ alkeislaajennus $\mathbb{L}$ ja sellainen $y \in \mathbb{L}$, että $y' = \alpha$, jos ja vain jos on olemassa sellaiset $u_1, \dots, u_n, v \in \mathbb{K}$ ja $c_1, \dots, c_n \in \mathbb{C}$, että

$$\alpha = \sum_{i=1}^n c_i \frac{u'_i}{u_i} + v'. \quad (1)$$

Liouvillen lauseen muoto on ”jotain $\Leftrightarrow$ jotain”, joten pitää todistaa, että implikaatio pätee molempiin suuntiin. Aloitetaan yksinkertaisemmasta implikaatiosta.

Implikaation ” $\Leftarrow$ ” todistus. Oletetaan, että on olemassa sellaiset $u_1, \dots, u_n, v \in \mathbb{K}$ ja $c_1, \dots, c_n \in \mathbb{C}$, että yhtälö (1) pätee. Jos on olemassa sellaiset $i_0 \in \{1, \dots, n\}$ ja $a \in \mathbb{K}$, että

$$\frac{u'_{i_0}}{u_{i_0}} = a',$$

niin määritellään $\bar{v} := v + c_{i_0}a$. Jos tämä tapahtuu uudelleen, niin määritellään $\bar{v}$ kunnan $\mathbb{K}$ alkioiden derivaattoja vastaavien yhtälön (1) termien summaksi. Voidaan siis olettaa, että jokaisella indeksillä i ei ole olemassa sellaista $a \in \mathbb{K}$, että $u'_i/u_i = a'$. Lisäksi voidaan olettaa, että välissä I , jossa v ja kaikki funktiot u_j on määritetty, pätee $u_i(x) \neq 0$ jokaisella alkiolla $x \in I$ ja indeksillä $i \in \{1, \dots, n\}$, tai muuten otetaan osaväli $J \subsetneq I$.

Määritellään nyt $a_i := \log u_i$ jokaisella $i \in \{1, \dots, n\}$. Voidaan olettaa, että $a_i \notin \mathbb{K}(a_1, \dots, a_{i-1})$, tai muuten a_i yksinkertaisesti ohitetaan. Sitten $\mathbb{L} := \mathbb{K}(a_1, \dots, a_n)$ on kunnan $\mathbb{K}$ alkeislaajennus. Koska kaikki funktiot a_i sekä v kuuluvat kuntaan $\mathbb{L}$, saadaan myös

$$y := \sum_{i=1}^n c_i a_i + v \in \mathbb{L}.$$

Derivoimalla tämä saadaan

$$y' = \sum_{i=1}^n c_i a'_i + v' = \sum_{i=1}^n c_i \frac{u'_i}{u_i} + v' = \alpha.$$

□

Huomautus 3. Jos etsitään integraalifunktiota kunnan $\mathbb{K}$ ulkopuolelta, ainoa mahdollisuus saada se on lisäämällä äärettömän monta logaritmifunktiota! Esimerkiksi rationaalifunktiolla $\frac{1}{x}$ ei ole integraalifunktiota kunnassa $\mathbb{C}(x)$, mutta kyllä on laajennuksessa $\mathbb{C}(x)(\ln x) = \mathbb{C}(x, \ln x)$.

Liouville'n lauseen implikaation " $\Rightarrow$ " todistus tulee olemaan melko pitkä ja tehdään eri tapauksissa. Ensin kerätään paljon apulauseita seuraavassa luvussa. Liouville'n lauseen implikaation " $\Rightarrow$ " todistus alkaa sivulla 12. Todistus jatkuu eri tavalla riippuen siitä, onko kyseessä oleva funktio transkendenttinen eksponenttifunktio (niin kuin kirjoituksen otsikossa) vai algebrallinen.

Todistuksen perusaineekset

Tehtävä 4. Tarkista, että seuraava yhtälö pitää paikkansa:

$$\frac{(f_1 f_2 \cdots f_n)'}{f_1 f_2 \cdots f_n} = \frac{f_1'}{f_1} + \cdots + \frac{f_n'}{f_n}. \quad (2)$$

Tulemme käyttämään sitä ja erikoistapausta

$$\frac{(fg)'}{fg} = \frac{f'}{f} + \frac{g'}{g} \quad (3)$$

pari kertaa jatkossa.

Meromorfinen funktion poolit

Määritelmä 5. Olkoot f ja g holomorfinen funktioita jossain kompleksitason avoimessa osajoukossa U . Meromorfinen funktion $\frac{f(x)}{g(x)}$ **poolit** (eli navat) ovat funktion g nollakohdat.

Huomautus 6. Ainoa poolien sovellus, jota käytämme jatkossa, on siinä tapauksessa, että kyseessä oleva meromorfinen funktio on rationaalifunktio eli kahden polynomin osamäärä $\frac{P(x)}{Q(x)}$. Oletetaan, että P ja Q ovat keskenään jaottomat, ja jaetaan nimittäjä tekijöihin:

$$\frac{P(x)}{Q(x)} = \frac{P(x)}{\omega(x - z_1)^{a_1}(x - z_2)^{a_2} \cdots (x - z_n)^{a_n}}.$$

Tässä $z_1, \dots, z_n$ ovat eri kompleksilukuja, $\omega \in \mathbb{C}$ ja $a_1, \dots, a_n$ ovat positiivisia kokonaislukuja. Tietysti $P(z_i) \neq 0$ kaikilla i . Sanotaan, että z_i on funktion $\frac{P(x)}{Q(x)}$ a_i -**kertainen pooli**, toisin sanoen poolin z_i **kertaluku** on a_i . Huomaamme nyt, että rationaalifunktion derivaatta on sekin rationaalifunktio, ja sen poolien kertaluvut ovat välttämättä > 1 : jos siis kirjoitetaan

$$\frac{P(x)}{Q(x)} = \frac{f(x)}{(x - z_i)^{a_i}},$$

jossa rationaalifunktio $f(x)$ sisältää kaikki muut termit $(x - z_j)^{a_j}$, niin

$$\begin{aligned} \frac{d}{dx} \frac{P(x)}{Q(x)} &= \frac{(x - z_i)^{a_i} f'(x) - a_i (x - z_i)^{a_i-1} f(x)}{(x - z_i)^{2a_i}} \\ &= \frac{(x - z_i) f'(x) - a_i f(x)}{(x - z_i)^{a_i+1}}, \end{aligned}$$

eikä z_i ole viimeisen osoittajan nollakohta.

Transkendenttisuudesta

Lemma 7. Olkoon α transkendenttinen alkio ja olkoot P ja Q kaksi eri polynomia. Tällöin $P(\alpha) \neq Q(\alpha)$.

Todistus. Jos $P(\alpha) = Q(\alpha)$, niin α on polynomin $P - Q$ juuri. Transkendenttisuuden takia tämä tarkoittaa, että $P - Q$ on nollapolynomi, eli $P = Q$. $\square$

Lemma 8. Olkoon $g(x) \in \mathbb{C}(x)$ rationaalifunktio, joka ei ole vakio. Tällöin funktio $e^{g(x)}$ on transkendenttinen kunnan $\mathbb{C}(x)$ suhteen.

Todistus. Oletetaan, että e^g on algebrallinen kunnan $\mathbb{K} := \mathbb{C}(x)$ suhteen. Silloin on olemassa sen minimipolynomi

$$P = X^n + f_{n-1}X^{n-1} + \cdots + f_1X + f_0 \in \mathbb{K}[X].$$

Derivoidaan yhtälö $P(e^g) = 0$ eli

$$e^{ng} + f_{n-1}e^{(n-1)g} + \cdots + f_1e^g + f_0 = 0$$

saaden

$$ng'e^{ng} + (f'_{n-1} + (n-1)f_{n-1}g')e^{(n-1)g} + \cdots + (f'_1 + g'f_1)e^g + f'_0 = 0.$$

On siis olemassa toinen n -asteinen polynomi, jonka arvo funktiolle e^g on nolla. Tämä on välttämättä polynomin P kerrannainen, ja korkeimman ja pienimmän asteen kertoimet ovat verrannolliset:

$$ng' = \frac{f'_0}{f_0}. \quad (4)$$

Kirjoitetaan rationaalifunktio $f_0 \in \mathbb{C}(x)$ osoittajan ja nimittäjän tulona lineaarisia, pareittain erillisiä tekijöitä:

$$f_0 = \prod_{i=1}^m (x - z_i)^{\alpha_i}, \quad m \in \mathbb{N}, \quad z_i \in \mathbb{C}(x), \quad \alpha_i \in \mathbb{Z} \setminus \{0\}.$$

Sen derivaatta on

$$\begin{aligned} f'_0 &= [\alpha_1(x - z_1)^{\alpha_1-1}(x - z_2)^{\alpha_2} \cdots (x - z_m)^{\alpha_m}] + \cdots \\ &\quad + [\alpha_m(x - z_1)^{\alpha_1} \cdots (x - z_{m-1})^{\alpha_{m-1}}(x - z_m)^{\alpha_m-1}] \\ &= \sum_{i=1}^m \alpha_i \frac{f_0}{x - z_i} = f_0 \sum_{i=1}^m \frac{\alpha_i}{x - z_i}. \end{aligned}$$

Tämän ja yhtälön (4) avulla saamme, että

$$ng' = \sum_{i=1}^m \frac{\alpha_i}{x - z_i}.$$

Huomaamme nyt, että oikealla puolella olevan funktion poolien kertaluku on 1, kun taas ng' on rationaalifunktion derivaatta, jonka poolien kertaluku on aina suurempi kuin 1 (ks. Huom 6). Tämä on ristiriita. $\square$

Osamurtokehiteelmä

Seuraava apulaus on se, jota käytetään eniten Liouvil-
len lauseen todistuksessa. Siinä tapauksessa, että ky-
seessä oleva funktio on transkendenttinen (niin kuin
artikkelin otsikossa), käytetään pelkästään seuraavaa
lausetta.

Lause 9. *Olko $\mathbb{K}$ kunta ja $f \in \mathbb{K}(X)$ rationaalifunk-
tio, jonka nimittäjä ei ole vakio. Tällöin on olemassa*

- *luonnollinen luku $N \in \mathbb{Z}_{>0}$,*
- *N pareittain erillistä jaotonta polynomia $V_1, \dots, V_N \in \mathbb{K}[X]$, joiden korkeimman asteen ter-
min kerroin on 1,*
- *N luonnollista lukua $m_1, \dots, m_N \in \mathbb{Z}_{>0}$,*
- *jokaisilla $i \in \{1, \dots, N\}$ ja $k \in \{1, \dots, m_i\}$, polyno-
mi $S_{k,i} \in \mathbb{K}[X]$, jolle $\deg S_{k,i} < \deg V_i$,*
- *polynomi $S_0 \in \mathbb{K}[X]$*

siten, että

$$f = S_0 + \sum_{i=1}^N \sum_{k=1}^{m_i} \frac{S_{k,i}}{V_i^k}.$$

Todistus. Kirjoitetaan $f = P/Q$, missä $P, Q \in \mathbb{K}[X]$
ovat keskenään jaottomat ja $\deg Q \geq 1$. Olkoon

$$Q = V_1^{\nu_1} V_2^{\nu_2} \dots V_N^{\nu_N}$$

alkutekijähajotelma (eli $V_i \neq V_j$, ja kaikki V_i :t ovat
jaottomat). Jos $N = 1$, niin funktio on jo yhtälön (5)
muodossa. Jos $N > 1$, polynomit $V_1^{\nu_1}$ ja

$$\tilde{Q} := V_2^{\nu_2} \dots V_N^{\nu_N}$$

ovat keskenään jaottomat. Bézout'n yhtälön (ks. artik-
kelin osa 1) mukaan on olemassa $S, T \in \mathbb{K}[X]$ siten,
että $SV_1^{\nu_1} + T\tilde{Q} = 1$. Nyt voidaan kirjoittaa

$$f = \frac{P}{Q} = \frac{P(SV_1^{\nu_1} + T\tilde{Q})}{V_1^{\nu_1}\tilde{Q}} = \frac{PS}{\tilde{Q}} + \frac{PT}{V_1^{\nu_1}},$$

missä jälkimmäisen yhteenlaskettavan nimittäjä on
jaottoman polynomin potenssi. Jos $N - 1 > 1$, tois-
tetaan sama prosessi, jolloin saadaan

$$f = \frac{*}{\tilde{\tilde{Q}}} + \frac{*}{V_2^{\nu_2}} + \frac{PT}{V_1^{\nu_1}},$$

missä $\tilde{\tilde{Q}} = V_3^{\nu_3} \dots V_N^{\nu_N}$ ja pikku tähdet esittävät sopivia
polynomeja. Äärellisen monen askelen jälkeen saadaan

$$f = \frac{R_1}{V_1^{\nu_1}} + \dots + \frac{R_N}{V_N^{\nu_N}} = \sum_{i=1}^N \frac{R_i}{V_i^{\nu_i}} \quad (5)$$

joillain polynomeilla $R_1, \dots, R_N \in \mathbb{K}[X]$. Mikäli
 $\deg R_i > \deg V_i$ tietyllä indeksillä i , Eukleideen algo-
ritmin avulla saadaan sellaiset Q_i ja S_i , että $R_i =$

$Q_i V_i + S_i$ ja $\deg S_i < \deg V_i$. Silloin summan (5) i :s
yhteenlaskettava voidaan kirjoittaa muotoon

$$\frac{R_i}{V_i^{\nu_i}} = \frac{Q_i V_i + S_i}{V_i^{\nu_i}} = \frac{Q_i}{V_i^{\nu_i-1}} + \frac{S_i}{V_i^{\nu_i}}.$$

Mikäli $\deg(Q_i) > \deg(V_i)$, sama prosessi toistetaan,
kunnes

$$\frac{R_i}{V_i^{\lambda_i}} = S_{0,i} + \sum_{k=1}^{m_i} \frac{S_{k,i}}{V_i^k}, \quad (6)$$

missä $\deg S_{k,i} < \deg V_i$ jokaisella $k \in \{1, \dots, m_i\}$.

Lopuksi, mikäli polynomin V_i korkeimman asteen ter-
min kerroin on $a \neq 1$, voidaan määritellä $\bar{V}_i := \frac{V_i}{a}$ ja
 $\bar{S}_{k,i} := \frac{S_{k,i}}{a^k}$. Tällöin polynomin $\bar{V}_i$ korkeimman asteen
termin kerroin onkin 1, ja $\frac{S_{k,i}}{V_i^k} = \frac{\bar{S}_{k,i}}{\bar{V}_i^k}$. $\square$

Esimerkki 10. *Edellistä lausetta käytetään jatkossa
"teoreettisena" tuloksena, emmekä ole kiinnostuneita
erityisistä rationaalifunktioista. Voi olla kuitenkin hyö-
dyllistä käydä todistus läpi ymmärtääksesi, miten se
toimii. Esimerkiksi siinä tapauksessa, että annettu ra-
tionaalifunktio on $\frac{P}{Q} = \frac{x^3}{x+1}$, niin $N = 1$ ja ainoa ni-
mittäjän jaoton tekijä on $V_1 = x + 1$. Voit tarkistaa,
että lauseen todistus tuottaa osamurtokehiteelmän*

$$\begin{aligned} \frac{x^3}{x+1} &= \frac{(x^2 - 1 + 1)(x+1)}{x+1} - \frac{1}{x+1} \\ &= x^2 - x + 1 - \frac{1}{x+1}. \end{aligned}$$

*Tämä onkin helppo rationaalifunktio. Voit kokeilla itse
vaikeampia esimerkkejä.*

Polynomin juuret

Alkio r on polynomin P **juuri**, jos $P(r) = 0$. Toisin
sanoen r on polynomiyhtälön $P(x) = 0$ ratkaisu. Al-
gebran pääongelma on löytää tällaisia juuria. Jos ker-
roinjoukko on liian pieni, on vaikeaa löytää niitä, joten
joukkoa laajennetaan:

- Polynomilla $X + 1$ ei ole juurta joukossa $\mathbb{N}$, mutta
sillä on juuri -1 joukossa $\mathbb{Z}$.
- Polynomilla $2X - 1$ ei ole juurta joukossa $\mathbb{Z}$, mutta
sillä on juuri $\frac{1}{2}$ joukossa $\mathbb{Q}$.
- Polynomilla $X^2 - 2$ ei ole juurta joukossa $\mathbb{Q}$, mutta
sillä on juuri $\sqrt{2}$ joukossa $\mathbb{R}$.
- Polynomilla $X^2 + 1$ ei ole juurta joukossa $\mathbb{R}$, mutta
sillä on juuri i joukossa $\mathbb{C}$.

Kuten näimme, $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ on ketju kuntalaajennuk-
sia. Juuri tämän takia kuntalaajennuksia tutkitaan: ha-
luamme laajentaa kuntaa niin, että juuria löytyy. Huo-
maa, ettei tarvitse ottaa kuntaa $\mathbb{R}$ juuren löytämiseksi
polynomille $X^2 - 2 \in \mathbb{Q}[X]$: laajennus $\mathbb{Q}(\sqrt{2})$ riittää.

Lause 11 (algebran peruslause). *Jokaisella epävakio-
lla polynomilla $P \in \mathbb{C}[X]$ on jokin juuri joukossa $\mathbb{C}$.*

Itse asiassa tätä lausetta voi käyttää todistamaan, että m -asteisella kompleksikertoimisella polynomilla on täsmälleen m juurta, jos lasketaan kertalukuja. Toisin sanoen, m -asteinen polynomi $P \in \mathbb{C}[X]$ voidaan kirjoittaa tulona lineaarisia termejä

$$P(X) = (X - z_1)(X - z_2) \cdots (X - z_m),$$

missä jotkut juuret $z_i \in \mathbb{C}$ voivat toistua. (Vaikka edellistä lausetta kutsutaan ”peruslauseeksi”, se ei ole mikään triviaali tulos.) Tämä seuraa edellisestä lauseesta ja siitä, että r on polynomin P juuri jos ja vain jos $X - r$ jakaa polynomin P , eli $P = (X - r)Q$ jollakin polynomilla Q . (Ks. kirjan [2] Lause 22.9.)

Määritelmä 12. Olkoot P polynomi ja r sen juuri. Juuren r **kertaluku** on korkein n , jolle $(X - r)^n$ jakaa polynomin P , eli korkein n , jolle voidaan kirjoittaa

$$P = (X - r)^n Q,$$

jossa $Q(r) \neq 0$.

Lemma 13. Polynomille $P \in \mathbb{C}[X]$ seuraavat ehdot ovat yhtäpitävät:

- kaikkien P :n juurien kertaluvut ovat $= 1$,
- P ja P' ovat keskenään jaottomat.

Todistus. Oletetaan, että polynomilla P on juuri r , jonka kertaluku on $n > 1$. Tällöin $P(X) = (X - r)^n Q(X)$ jollain sopivalla Q , jolle pätee $Q(r) \neq 0$. Tällöin

$$P'(X) = n(X - r)^{n-1}Q(X) + (X - r)^n Q'(X),$$

joten $P'(r) = 0$. Tämä tarkoittaa, että $X - r$ jakaa myös polynomin P' . Jos sen sijaan $n = 1$, niin $P'(r) \neq 0$, eli r ei ole derivaatan juuri. Mutta koska polynomin P voi jakaa lineaarisiin tekijöihin, niin jos kaikkien juurien kertaluvut ovat $= 1$, niin P ja P' ovat keskenään jaottomat. $\square$

Olkoon $m \in \mathbb{Z}_{>0}$. Kirjoittamalla jatkossa $\mathbb{C}_w^m$ tarkoitamme, että karteesiselle tulolle $\mathbb{C}^m = \mathbb{C} \times \cdots \times \mathbb{C}$ otetaan koordinaatit $(w_1, \dots, w_m)$. Seuraavakin lause on melko kuuluisa.

Lause 14 (Implisiittisen funktion lause). Olkoot $m, n \in \mathbb{Z}_{>0}$ ja $\mathcal{A}$ tulon $\mathbb{C}^{n+m} = \mathbb{C}_z^n \times \mathbb{C}_w^m$ avoin joukko. Olkoon $F = (F_1, \dots, F_n): \mathcal{A} \rightarrow \mathbb{C}^n$ holomorfinen funktio. Olkoon $(z^0, w^0) = (z_1^0, \dots, z_n^0, w_1^0, \dots, w_m^0) \in \mathcal{A}$ sellainen piste, että $F(z^0, w^0) = 0$ ja Jacobin matriisi siinä pisteessä, eli

$$\begin{pmatrix} \frac{\partial F_1(z^0, w^0)}{\partial z_1} & \cdots & \frac{\partial F_n(z^0, w^0)}{\partial z_1} \\ \vdots & \ddots & \vdots \\ \frac{\partial F_1(z^0, w^0)}{\partial z_n} & \cdots & \frac{\partial F_n(z^0, w^0)}{\partial z_n} \end{pmatrix},$$

on kääntövä. Tällöin on olemassa pisteen $z^0 \in \mathbb{C}^n$ avoin ympäristö U , pisteen $w^0 \in \mathbb{C}^m$ avoin ympäristö V ja holomorfinen funktio $h: V \rightarrow U$ siten, että

- $U \times V \subseteq \mathcal{A}$,
- $F(h(w), w) = 0$ kaikilla $w \in V$,
- $h(w^0) = z^0$.

Lause 15. Olkoon $\mathbb{K}$ kunta meromorfinen funktioita reaalivälissä I ja olkoon $P \in \mathbb{K}[X]$ m -asteinen jaoton polynomi. Tällöin jollekin osavälille $J \subseteq I$ on olemassa sellaiset pareittain erilliset meromorfiniset funktiot

$$f_1, \dots, f_m: J \rightarrow \mathbb{C},$$

että $P(f_i) = 0$ jokaisella $i = 1, \dots, m$.

Todistus. Olkoon

$$Q(x) = x^m + c_{m-1}x^{m-1} + \cdots + c_1x + c_0 \in \mathbb{C}[x]$$

sellainen polynomi, jolla on m parittain erillistä juurta $z_1, \dots, z_m \in \mathbb{C}$. Lemmasta 13 seuraa, että polynomeilla Q ja

$$Q'(x) = \sum_{i=1}^m ic_i x^{i-1}$$

ei ole yhteisiä tekijöitä, joten $Q'(z_i) \neq 0$ kaikilla i . Määritellään holomorfinen funktio

$$F: \mathbb{C}^{m+1} \rightarrow \mathbb{C},$$

$$(x, a_0, \dots, a_{m-1}) \mapsto x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0.$$

Haluamme nyt käyttää Lauseita 14, ja päätelläksemme Jacobin matriisin kääntyvyyden riittää huomata, että

$$\frac{\partial F}{\partial x}(z_i, c_0, \dots, c_{m-1}) = Q'(z_i) \neq 0$$

jokaisella $i \in \{1, \dots, m\}$. Käytämme Lauseita 14 m kertaa, yhden kerran jokaisella z_i . On olemassa pisteen $(c_0, \dots, c_{m-1})$ avoin ympäristö $V \subseteq \mathbb{C}^m$, pisteiden z_i avoimet ympäristöt $U_i \subseteq \mathbb{C}$ ja m holomorfinen funktiota $h_i: V \rightarrow U_i$ niin, että

- jokaisella $(a_0, \dots, a_{m-1}) \in V$

$$F(h_i(a_0, \dots, a_{m-1}), a_0, \dots, a_{m-1}) = 0,$$

eli $h_i(a_0, \dots, a_{m-1})$ on polynomin $x^m + a_{m-1}x^{m-1} + \cdots + a_0$ juuri;

- $h_i(c_0, \dots, c_{m-1}) = z_i$ jokaisella $i \in \{1, \dots, m\}$.

Olkoon nyt

$$P(X) = \sum_{i=0}^m g_i X^i \in \mathbb{K}[X]$$

polynomi kuten lauseen väitteessä. Voimme olettaa, että kaikki funktiot g_i ovat määritellyt välissä I , tai muuten otetaan sellainen osaväli. Voimme myös olettaa, että funktio g_m ei ole koskaan nolla välissä I . Toisin sanoen, voimme jakaa funktiolla g_m , tai itse asiassa olettaa alusta alkaen, että polynomin P korkeimman asteen termin kerroin on $g_m = 1$.

Jokaisella reaaliluvulla $t \in I$ määritellään polynomi

$$P_t(x) := \sum_{i=0}^m g_i(t)x^i \in \mathbb{C}[x].$$

Etsimme sellaisen $t_0 \in I$, että polynomilla P_{t_0} on m parittain erillistä juurta. Koska P on jaoton, P ja P' ovat keskenään jaottomat. Bézout'n lauseen mukaan (ks. artikkelin osa 1) on olemassa sellaiset $S, T \in \mathbb{K}[X]$, että

$$SP + TP' = 1. \quad (7)$$

Voimme olettaa, että polynomien S ja T kaikki kertoimet — jotka ovat kunnan $\mathbb{K}$ alkioita, eli funktioita — ovat määritellyt välissä I , tai muuten otetaan osaväli. Jokaisella $t \in I$ voimme siis määritellä polynomit P'_t , S_t ja T_t samalla tavalla kuin polynomin P_t . Yhtälöstä 7 saamme yhtälön

$$S_t P_t + T_t P'_t = 1,$$

joka pätee renkaassa $\mathbb{C}[x]$. Tästä seuraa, että P_t ja P'_t ovat keskenään jaottomat, ja Lemman 13 nojalla tämä tarkoittaa, että polynomilla P_t on m erillistä juurta. Tämä pitää paikkansa jokaisella reaaliluvulla t välissä I , tai osavälissä J , jos sitä tarvitaan. Sellaiset polynomit P_t ovat niin kuin polynomi Q todistuksen alussa. Olkoon siis $t_0 \in J$ ja olkoot $z_1, \dots, z_m$ polynomin P_{t_0} juuret. Voimme käyttää funktioita $h_1, \dots, h_m$ saadaksemme väitteen funktiot

$$f_i(t) = h_i(g_0(t), \dots, g_{m-1}(t))$$

pisteen t_0 ympäristössä. Huomaa, että funktiot f_i ovat holomorfin välin J kompleksiympäristössä. $\square$

Symmetriset polynomit

Määritelmä 16. Funktiota $\sigma: A \rightarrow B$ kutsutaan **bijektioksi**, jos σ on sekä injektio että surjektio, eli

- jos $a \neq a'$, niin $\sigma(a) \neq \sigma(a')$,
- jokaisella alkiolla $b \in B$ on olemassa sellainen $a \in A$, että $\sigma(a) = b$.

Jos $A = B$, niin bijektiota $\sigma: A \rightarrow A$ kutsutaan **permutaatioksi**.

Huomautus 17. Joukon $\{1, 2, \dots, n\}$ permutaatio on siis bijektio $\sigma: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$. Toisin sanoen σ on ”järjestyksen sekoittaminen”. Joukon $\{1, 2\}$ kaksi mahdollista permutaatiota ovat σ_1 ja σ_2 , missä

$$\sigma_1(1) = 1, \sigma_1(2) = 2 \quad \text{ja} \quad \sigma_2(1) = 2, \sigma_2(2) = 1.$$

Joukon $\{1, 2, 3\}$ mahdolliset permutaatiot ovat funktiot $\sigma_1, \dots, \sigma_6$, joiden arvot $\sigma_i(1)$, $\sigma_i(2)$ ja $\sigma_i(3)$ ovat

$$1, 2, 3, \quad 2, 1, 3, \quad 3, 2, 1, \quad 1, 3, 2, \quad 2, 3, 1 \quad \text{ja} \quad 3, 1, 2.$$

Määritelmä 18. Polynomia $P \in \mathbb{K}[x_1, \dots, x_n]$ kutsutaan **symmetriseksi polynomiksi**, jos

$$P(x_1, \dots, x_n) = P(x_{\sigma(1)}, \dots, x_{\sigma(n)})$$

millä tahansa indeksien permutaatiolla σ .

Jos kirjoitetaan x ja y $x_1:n$ ja $x_2:n$ sijaan, esimerkiksi renkaassa $\mathbb{K}[x, y]$ polynomit $x^2 + y^2$ ja xy ovat symmetriset, mutteivät polynomit $x^2 + y$ ja $x^3 y$.

Jokaisella luonnollisella luvulla n renkaassa $\mathbb{K}[x_1, \dots, x_n]$ on olemassa tärkeitä symmetrisiä polynomeja, nimittäin niin kutsutut **symmetriset peruspolynomit**:

$$\begin{aligned} s_1 &:= x_1 + x_2 + \dots + x_n, \\ s_2 &:= x_1 x_2 + x_1 x_3 + \dots + x_{n-1} x_n, \\ &\vdots \\ s_n &:= x_1 x_2 \dots x_n. \end{aligned}$$

Nämä ovat symmetristen polynomien ”atomit”, sillä jokainen symmetrinen polynomi voidaan esittää niiden polynomeina seuraavan kuuluisan lauseen mukaan.

Lause 19 (Newton). Olkoot R rengas ja $S \in R[x_1, \dots, x_n]$ symmetrinen polynomi. On olemassa yksikäsitteinen polynomi $Q \in R[y_1, \dots, y_n]$ siten, että

$$S(x_1, \dots, x_n) = Q(s_1, \dots, s_n).$$

Esimerkki 20. Renkaassa $R[x, y]$ symmetriset peruspolynomit ovat $x + y$ ja xy . Esimerkiksi $x^2 + y^2$ on symmetrinen ja

$$x^2 + y^2 = (x + y)^2 - 2(xy).$$

Eli lauseen vastaava polynomi $Q \in R[y_1, y_2]$ on $y_1^2 - 2y_2$.

Lause 21. Olkoot $\mathbb{K}$ kunta, $m \in \mathbb{N}$ ja $P \in \mathbb{K}[x]$ m -asteinen polynomi, jolla on pareittain erilliset juuret $z_1, \dots, z_m$ jossakin sopivassa kunnan $\mathbb{K}$ laajennuksessa. Jos $S \in \mathbb{K}[x_1, \dots, x_m]$ on symmetrinen polynomi, niin $S(z_1, \dots, z_m) \in \mathbb{K}$.

Todistus. Lauseen 19 avulla voi kirjoittaa

$$S(x_1, \dots, x_m) = Q(s_1, \dots, s_m)$$

sopivalla polynomilla $Q \in \mathbb{K}[y_1, \dots, y_m]$. Eksplisiittisesti

$$\begin{aligned} P(X) &= (X - z_1)(X - z_2) \dots (X - z_m) \\ &= X^m - a_1 X^{m-1} + a_2 X^{m-2} - \dots \pm a_m \end{aligned}$$

joillain $a_1, \dots, a_m \in \mathbb{K}$. Huomaa, että $a_i = s_i(z_1, \dots, z_m)$ jokaisella $i \in \{1, \dots, m\}$. Joten $S(z_1, \dots, z_m) = Q(a_1, \dots, a_m)$, ja tämä on kunnan $\mathbb{K}$ alkio. $\square$

Algebralliset alkio, joilla on sama minimipolynomi

Olkoot $\mathbb{K}$ kunta ja $\mathbb{L}$ sen laajennus. Olkoot $f, g \in \mathbb{L} \setminus \mathbb{K}$ kaksi algebrallista alkioita, joilla on sama minimipolynomi P kunnan $\mathbb{K}$ suhteen. Tämän pykälän päätulos on Lause 24: siinä tapauksessa, että $\mathbb{K}$ on kunta, jossa voidaan ottaa derivaatta, niin voidaan sijoittaa f ja f' alkoiden g ja g' paikalle tietyllä tavalla.

Tehtävä 22. Oletetaan, että algebralliset alkio f ja g ovat niin kuin edellä, ja olkoon P niiden minimipolynomi kunnan $\mathbb{K}$ suhteen. Olkoon $n := \deg(P) - 1$. Silloin kunnan $\mathbb{K}(f)$ alkio on muotoa $a = \sum_{i=0}^n a_i f^i$ joillain $a_i \in \mathbb{K}$. Määritellään nyt funktio

$$\pi: \mathbb{K}(f) \longrightarrow \mathbb{K}(g), \quad \sum_{i=0}^n a_i f^i \longmapsto \sum_{i=0}^n a_i g^i,$$

joka sijoittaa alkion g alkion f paikalle. Osoita, että

$$\pi(a + b) = \pi(a) + \pi(b) \quad \text{ja} \quad \pi(ab) = \pi(a)\pi(b)$$

jokaisella $a, b \in \mathbb{K}(f)$. (Toisin sanoen tämä funktio π on kuntien välinen isomorfismi.)

Lemma 23. Samalla notaatiolla $\pi(f') = g'$.

Todistus. Samalla tavalla kuin artikkelin ensimmäisen osan Lemman 27 todistuksessa voi osoittaa, että

$$f' = -\frac{\sum_{i=0}^n a'_i f^i}{\sum_{i=1}^n i a_i f^{i-1}} \quad \text{ja} \quad g' = -\frac{\sum_{i=0}^n a'_i g^i}{\sum_{i=1}^n i a_i g^{i-1}}.$$

Edellisen tehtävän nojalla,

$$\pi(f') = -\frac{\sum_{i=0}^m a'_i \pi(f)^i}{\sum_{i=1}^m i a_i \pi(f)^{i-1}}.$$

Tämä on yhtä kuin g' , koska $\pi(f) = g$. $\square$

Lause 24. Olkoot $\mathbb{K}$ kunta meromorfsia funktioita ja f, g kaksi algebrallista alkioita kunnan $\mathbb{K}$ suhteen. Oletetaan, että alkioilla f ja g on sama minimipolynomi $P \in \mathbb{K}[X]$. Olkoon $Q \in \mathbb{K}[Y, Z]$ kahden muuttujan polynomi, ja oletetaan, että $Q(f, f') \in \mathbb{K}$. Tällöin

$$Q(f, f') = Q(g, g').$$

Todistus. Koska funktion π rajoittuma kuntaan $\mathbb{K}$ on identiteetti,

$$Q(f, f') = \pi(Q(f, f')).$$

Edellisen tehtävän nojalla

$$\pi(Q(f, f')) = Q(\pi(f), \pi(f')).$$

Lopuksi tiedetään, että $\pi(f) = g$ suoraan määritelmästä ja $\pi(f') = g'$ edellisestä lemmasta. $\square$

Tätä pykälää voi varmaan lähestyä helpommin, jos niin sanotun tekijärenkaan käsite ja ensimmäinen homomorfismin lause ovat tutut. (Ks. kirjan [2] pykälät 16 ja 20.) Tästä näkökulmasta olisi ilmeistä, että $\mathbb{K}(f)$ ja $\mathbb{K}(g)$ ovat ”likimain sama asia”.

Implikaation ” $\Rightarrow$ ” todistuksen alku

Oletetaan, että on olemassa alkeislaajennus $\mathbb{L}$ niin kuin lauseen väitteessä. Eli $\mathbb{L} = \mathbb{K}(f_1, \dots, f_N)$ joillakin alkeisfunktioilla $f_1, \dots, f_N$. Todistus tehdään induktiolla N :n suhteen. Jos $N = 0$, niin $\mathbb{L} = \mathbb{K}$, ja on olemassa funktion α integraalifunktio $y \in \mathbb{L}$. Siis $v := y$ kelpaa. Kun $N > 0$, kirjoitetaan

$$\mathbb{K}(f_1, \dots, f_N) = \mathbb{K}(f_1)(f_2, \dots, f_N)$$

ja oletetaan, että väite pitää paikkansa kunnalle $\mathbb{K}(f_1)$, eli on olemassa sellaiset $t_1, \dots, t_n, w \in \mathbb{K}(f_1)$ ja $d_1, \dots, d_n \in \mathbb{C}$, että

$$\alpha = \sum_{i=1}^n d_i \frac{t'_i}{t_i} + w'. \quad (8)$$

Jatkossa etsimme funktioita $u_1, \dots, u_n, v$ funktioiden $t_1, \dots, t_n, w$ kautta ja kompleksilukuja $c_1, \dots, c_n$ kompleksilukujen $d_1, \dots, d_n$ kautta.

Riippuen siitä, onko f_1 transkendenttinen (eksponentti- tai logaritmifunktio) vai algebrallinen alkio kunnan $\mathbb{K}$ suhteen, todistus sujuu eri tavalla. Tässä kirjoituksessa käymme läpi ne tapaukset, että f_1 on transkendenttinen eksponenttifunktio tai algebrallinen, ja transkendenttisen logaritmifunktion tapaus jätetään tehtäväksi.

Implikaation ” $\Rightarrow$ ” todistuksen jatko: jos f_1 on transkendenttinen

Koska f_1 on transkendenttinen alkio, jokainen yhtälössä (8) oleva funktio $t_i \in \mathbb{K}(f_1)$ voidaan esittää osamääränä

$$t_i = \frac{P_i(f_1)}{Q_i(f_1)}$$

sopivilla keskenään jaottomilla polynomeilla $P_i, Q_i \in \mathbb{K}[X]$. Koska

$$\left(\frac{a}{b}\right)' = \frac{a'}{a} - \frac{b'}{b},$$

identiteetistä (8) tulee

$$\alpha = \sum_{i=1}^n d_i \frac{(P_i(f_1))'}{P_i(f_1)} - \sum_{i=1}^n d_i \frac{(Q_i(f_1))'}{Q_i(f_1)} + w'. \quad (9)$$

Olkoot $R_1, \dots, R_N$ kaikkien polynomien P_i ja Q_i kaikki jaottomat tekijät, toistaen mahdollisesti monta kertaa ne, jotka esiintyvät eri polynomeissa ja korkealla potenssilla. (Eli voi olla, että $R_i = R_j$, vaikka $i \neq j$.) Huomaa, että $N \geq n$. Identiteetin (2) nojalla voidaan kirjoittaa (9) muodossa

$$\alpha = \sum_{i=1}^N e_i \frac{(R_i(f_1))'}{R_i(f_1)} + w'$$

joillain sopivilla kompleksiluvuilla e_i . Olkoon $u_i \in \mathbb{K}$ polynomin R_i korkeimman asteen termin kerroin, joten voimme kirjoittaa $R_i = u_i M_i$, missä polynomin M_i vastaava kerroin on 1. Identiteetin (3) avulla

$$\alpha = \sum_{i=1}^N e_i \frac{u'_i}{u_i} + \sum_{i=1}^N e_i \frac{(M_i(f_1))'}{M_i(f_1)} + w'.$$

Voi olla, että jälkimmäisessä summassa $M_i = M_j$ vaikka $i \neq j$. Kirjoitetaan sitten yhteen ne polynomit M_i , jotka toistuvat niin, että

$$\alpha = \sum_{i=1}^N e_i \frac{u'_i}{u_i} + \sum_{i=1}^{\tilde{N}} \varepsilon_i \frac{(M_i(f_1))'}{M_i(f_1)} + w' \quad (10)$$

sopivilla uusilla kertoimilla ε_i ja luonnollisella luvulla $\tilde{N} \leq N$.

Loppusilaukseksi, koska w on kunnan $\mathbb{K}(f_1)$ alkio, on olemassa sellainen $g \in \mathbb{K}(X)$, että $w = g(f_1)$. Sovelletaan tälle funktiolle g Lausetta 9 saaden

$$w = S_0(f_1) + \sum_{i=1}^{\tilde{N}} \sum_{k=1}^{m_i} \frac{S_{k,i}(f_1)}{V_i^k(f_1)}.$$

Yhtälöstä (10) tulee siis

$$\begin{aligned} \alpha &= \sum_{i=1}^N e_i \frac{u'_i}{u_i} + \sum_{i=1}^{\tilde{N}} \varepsilon_i \frac{(M_i(f_1))'}{M_i(f_1)} + (S_0(f_1))' \\ &+ \sum_{i=1}^{\tilde{N}} \sum_{k=1}^{m_i} \frac{(S_{k,i}(f_1))'}{V_i^k(f_1)} - \sum_{i=1}^{\tilde{N}} \sum_{k=1}^{m_i} k \frac{S_{k,i}(f_1)(V_i(f_1))'}{V_i^{k+1}(f_1)}. \end{aligned} \quad (11)$$

Jos f_1 on eksponenttifunktio

Olkoon f_1 transkendenttinen eksponenttifunktio kunnan $\mathbb{K}$ suhteen.

Lemma 25. *Olkoon*

$$P(X) = a_m X^m + \cdots + a_0 = \sum_{i=0}^m a_i X^i, \quad (a_m \neq 0)$$

m -asteinen polynomi renkaassa $\mathbb{K}[X]$. Tällöin polynomille

$$\tilde{P}(X) := \sum_{i=0}^m (ia_i b' + a'_i) X^i \in \mathbb{K}[X]$$

pätee $(P(f_1))' = \tilde{P}(f_1)$.

Todistus. Koska f_1 on eksponenttifunktio kunnan $\mathbb{K}$ suhteen, on olemassa sellainen $b \in \mathbb{K}$, että $f'_1 = b' f_1$.

Silloin

$$\begin{aligned} (P(f_1))' &= \sum_{i=0}^m a'_i f_1^i + \sum_{i=1}^m ia_i f_1^i f_1^{i-1} \\ &= a'_0 + \sum_{i=1}^m a'_i f_1^i + \sum_{i=1}^m ia_i \frac{f'_1}{f_1} f_1^i \\ &= a'_0 + \sum_{i=1}^m (a'_i + ia_i b') f_1^i \\ &= \sum_{i=0}^m (a'_i + ia_i b') f_1^i = \tilde{P}(f_1). \end{aligned}$$

□

Lemma 26. *Käyttäen samaa notaatiota kuin edellä $ma_m b' + a'_m \neq 0$, eli*

$$\deg \tilde{P} = \deg P = m.$$

Todistus. Jos päinvaistoin olisi $ma_m b' + a'_m = 0$, niin

$$\begin{aligned} (a_m f_1^m)' &= a'_m f_1^m + ma_m f_1^m f_1^{m-1} \\ &= a'_m f_1^m + ma_m b' f_1^m \\ &= (a'_m + ma_m b') f_1^m = 0. \end{aligned}$$

Eli $a_m f_1^m$ olisi vakiofunktio, toisin sanoen kompleksiluku. Tämä on ristiriita, koska $a_m \neq 0$ ja f_1 on transkendenttinen. □

Lemma 27. *Jos a_m on vakiofunktio ja P jakaa polynomin $\tilde{P}$, niin P on monomi.*

Todistus. Koska asteet ovat yhtä suuret, P jakaa polynomin $\tilde{P}$ jos ja vain jos on olemassa sellainen $k \in \mathbb{K}$, että $kP = \tilde{P}$. Korkeimman asteen (eli m) termeille tämä tarkoittaa

$$ka_m = ma_m b' + a'_m = ma_m b',$$

missä toinen yhtälö pätee, koska a_m on vakio. Koska $a_m \neq 0$ seuraa, että $k = mb'$. Tällöin $a'_m b' = ia_i b' + a'_i$, eli $a'_i - a_i(m-i)b' = 0$ kaikille $i \in \{0, \dots, m-1\}$. Mutta sitten jokaisella indeksillä i

$$\begin{aligned} \left(\frac{a_i}{f_1^{m-i}} \right)' &= \frac{a'_i f_1^{m-i} - a_i(m-i) f_1^{m-i} b'}{(f_1^{m-i})^2} \\ &= \frac{a'_i - a_i(m-i)b'}{f_1^{m-i}} = 0, \end{aligned}$$

eli a_i/f_1^{m-i} on jokin vakio $c_i \in \mathbb{C}$. Yhtälöstä $a_i = c_i f_1^{m-i}$ ja siitä, että f_1 on transkendenttinen, seuraa, että $a_i = c_i = 0$ jokaisella $i \in \{0, \dots, m-1\}$. Toisin sanoen P on monomi $a_m X^m$. □

Sovelletaan nyt edelliset huomautukset yhtälöön (11). Jokaisella $i \in \{1, \dots, n\}$ on olemassa polynomit $\tilde{M}_i, \tilde{V}_i \in \mathbb{K}[X]$ niin, että

$$(M_i(f_1))' = \tilde{M}_i(f_1) \quad \text{ja} \quad (V_i(f_1))' = \tilde{V}_i(f_1).$$

Samalla tavalla on olemassa polynomit $\tilde{S}_0$ ja $\tilde{S}_{k,i}$. Yhtälöstä (11) tulee sitten

$$\alpha = \sum_{i=1}^N e_i \frac{u'_i}{u_i} + \sum_{i=1}^{\tilde{N}} \varepsilon_i \frac{\tilde{M}_i(f_1)}{\tilde{M}_i(f_1)} + \tilde{S}_0(f_1) \quad (12)$$

$$+ \sum_{i=1}^{\tilde{N}} \sum_{k=1}^{m_i} \frac{\tilde{S}_{k,i}(f_1)}{V_i^k(f_1)} - \sum_{i=1}^{\tilde{N}} \sum_{k=1}^{m_i} k \frac{S_{k,i}(f_1) \tilde{V}_i(f_1)}{V_i^{k+1}(f_1)}.$$

Muistetaan, että jos $i \neq j$, niin $M_i \neq M_j$ ja $V_i \neq V_j$. Olkoot $M_{i_1}, \dots, M_{i_s}$ ne polynomit joukosta $\{M_i\}$, jotka eivät ole yhtä kuin mikään polynomi V_j . Kun määritellään

$$L := V_1^{m_1+1} \dots V_{\tilde{N}}^{m_{\tilde{N}}+1} M_{i_1} \dots M_{i_s},$$

niin $L(f_1)$ on suurin yhteinen nimittäjä identiteetissä (12). Se osamäärä, jonka nimittäjä on korkein alkion $V_1(f_1)$ potenssi, löytyy viimeisestä (tupla)summasta indeksiarvoilla $i = 1$ ja $k = m_1$. Voidaan siis kirjoittaa

$$\frac{\mathcal{P}(f_1)}{V_1^{m_1}(f_1) V_2^{m_2+1}(f_1) \dots V_{\tilde{N}}^{m_{\tilde{N}}+1}(f_1) M_{i_1}(f_1) \dots M_{i_s}(f_1)}$$

$$= -m_1 \frac{S_{m_1,1}(f_1) \tilde{V}_1(f_1)}{V_1^{m_1+1}(f_1)}$$

jollain sopivalla polynomilla $\mathcal{P} \in \mathbb{K}[X]$. Kerrotaan molemmat puolet alkioilla $-\frac{1}{m_1} L(f_1)$, jolloin saadaan

$$-\frac{1}{m_1} \mathcal{P}(f_1) V_1(f_1) = S_{m_1,1}(f_1) \tilde{V}_1(f_1)$$

$$\cdot V_2^{m_2+1}(f_1) \dots V_{\tilde{N}}^{m_{\tilde{N}}+1}(f_1)$$

$$\cdot M_{i_1}(f_1) \dots M_{i_s}(f_1).$$

Koska f_1 on transkendenttinen, Lemmasta 7 seuraa, että

$$-\frac{1}{m_1} \mathcal{P} V_1 = S_{m_1,1} \tilde{V}_1 V_2^{m_2+1} \dots V_{\tilde{N}}^{m_{\tilde{N}}+1} M_{i_1} \dots M_{i_s}.$$

Jaoton polynomi V_1 on selvästi vasemman puolen tekijä. Ainoa tapa, jolla V_1 voi jakaa oikean puolen, on että V_1 jakaa polynomin $\tilde{V}_1$. Koska polynomin V_1 korkeimman asteen termin kerroin on 1, Lemman 27 nojalla saadaan, että V_1 on itse asiassa monomi ja välttämättä monomi X .

Jos sama prosessi tehdään muille polynomeille V_i , ja koska $V_i \neq V_1$, huomaamme, ettei V_i esiinny yhtälössä (12). Samanlaisella tavalla voi päätellä, että $M_1 = X$, eivätkä muut polynomit M_i esiinny. Lopuksi Lauseesta 9 seuraa, että $\deg S_{k,1} < \deg V_1 = 1$ jokaisella $k \in \{1, \dots, m_1\}$, joten $S_{k,1} = S_{k,1}(f_1) = \sigma_k$ jollakin $\sigma_k \in \mathbb{K}$. Yhtälöstä (12) tulee sitten

$$\alpha = \sum_{i=1}^N e_i \frac{u'_i}{u_i} + \varepsilon_1 \frac{f'_1}{f_1} + \tilde{S}_0(f_1) + \sum_{k=1}^{m_1} \frac{\sigma'_k}{f_1^k} - \sum_{k=1}^{m_1} k \frac{\sigma_k f'_1}{f_1^{k+1}}$$

$$= \sum_{i=1}^N e_i \frac{u'_i}{u_i} + \varepsilon_1 b' + \sum_{k=1}^{m_1} \frac{\sigma'_k - kb' \sigma_k}{f_1^k} + \tilde{S}_0(f_1).$$

Jos yksikin termeistä $\sigma'_k - kb' \sigma_k$ olisi epänolla, niin kerromalla molemmat puolet alkioilla $f_1^{m_1}$ saisimme epäollan polynomin, jolle f_1 on juuri. Tämä on ristiriita, koska f_1 on transkendenttinen, joten kaikki nuo termit ovat nollija ja

$$\alpha = \sum_{i=1}^N e_i \frac{u'_i}{u_i} + \varepsilon_1 b' + \tilde{S}_0(f_1).$$

Polynomin $\tilde{S}_0$ määritelmästä ja Lemmasta 26 seuraa, että $\deg(\tilde{S}_0) = 0$, eli $S_0 = S_0(f_1) = s_0 \in \mathbb{K}$. Voi siis kirjoittaa

$$\alpha = \sum_{i=1}^N e_i \frac{u'_i}{u_i} + \varepsilon_1 b' + s'_0,$$

ja määrittelemällä $v := \varepsilon_1 b + s_0$ saamme yhtälön (1).

Jos f_1 on logaritmifunktio

Tehtävä 28. Tee todistus itse seuraten suunnilleen samaa strategiaa kuin eksponenttifunktion tapauksessa.

Vihje: Lemmat 25, 26 ja 27 pitää muokata. Esimerkiksi uusi polynomi $\tilde{P}$ on

$$\tilde{P}(X) := a'_m X^m + \sum_{i=0}^{m-1} \left(a'_i + (i+1) a_{i+1} \frac{b'}{b} \right) X^i.$$

Huomaa, että

- jos a_m on vakio, niin $\deg(\tilde{P}) < \deg(P)$,
- jos a_m ei ole vakio, niin $\deg(\tilde{P}) = \deg(P)$.

Implikaation ” $\Rightarrow$ ” todistuksen jatko: jos f_1 on algebrallinen

Aloitetaan taas yhtälöstä (8) eli

$$\alpha = \sum_{i=1}^n d_i \frac{t'_i}{t_i} + w',$$

missä $t_1, \dots, t_n, w \in \mathbb{K}(f_1)$. Koska nyt oletetaan, että f_1 on algebrallinen, on olemassa sellaiset polynomit $P_1, \dots, P_n, Q \in \mathbb{K}[X]$, että $t_i = P_i(f_1)$ ja $w = Q(f_1)$ jokaisella $i \in \{1, \dots, n\}$. Koska $\mathbb{K}(f_1)$ on kunta, on olemassa polynomit $R_1, \dots, R_n \in \mathbb{K}[X]$ niin, että

$$\frac{1}{P_i(f_1)} = R_i(f_1). \quad (13)$$

Yhtälöstä (8) tulee

$$\alpha = \sum_{i=1}^n d_i (P_i(f_1))' R_i(f_1) + (Q(f_1))'. \quad (14)$$

Olkoon $M \in \mathbb{K}[X]$ alkion f_1 minimipolynomi kunnan $\mathbb{K}$ suhteen, ja olkoon $m := \deg(M)$. Lemman 15 avulla

polynomilla M on m pareittain erillistä meromorfasta juurta $z_1, \dots, z_m$, ja yksi niistä on f_1 . Jollekin sopivalle polynomille $\mathcal{T} \in \mathbb{K}[X, Y]$ yhtälön (14) oikea puoli on yhtä kuin $\mathcal{T}(f_1, f_1')$. Koska $z_1, \dots, z_m$ ovat saman jaotoman polynomin juuret, voimme käyttää Lausetta 24 saaden

$$\alpha = \sum_{i=1}^n d_i (P_i(z_k))' R_i(z_k) + (Q(z_k))'$$

jokaisella $k \in \{1, \dots, m\}$. Jos otetaan summa kaikkien indeksien $k \in \{1, \dots, m\}$ suhteen, saamme

$$m\alpha = \sum_{k=1}^m \left(\sum_{i=1}^n d_i (P_i(z_k))' R_i(z_k) + (Q(z_k))' \right).$$

Tästä ja yhtälöstä (13) seuraa, että

$$\alpha = \frac{1}{m} \sum_{i=1}^n \sum_{k=1}^m d_i \frac{(P_i(z_k))'}{P_i(z_k)} + \frac{1}{m} \left(\sum_{k=1}^m Q(z_k) \right)'.$$

Sovelletaan yhtälöä (2) ensimmäisessä termissä esiintyvään summaan saaden

$$\begin{aligned} \alpha &= \frac{1}{m} \sum_{i=1}^n d_i \frac{(P_i(z_1)P_i(z_2) \cdots P_i(z_m))'}{P_i(z_1)P_i(z_2) \cdots P_i(z_m)} \\ &\quad + \frac{1}{m} \left(\sum_{k=1}^m Q(z_k) \right)'. \end{aligned}$$

Jokaisella $i \in \{1, \dots, n\}$ määritellään polynomi

$$S_i(X_1, \dots, X_m) := P_i(X_1) \cdots P_i(X_m)$$

renkaassa $\mathbb{K}[X_1, \dots, X_m]$. Polynomi S_i on symmetrinen, joten siihen voidaan soveltaa Lausetta 21, kun määritellään

$$u_i := S_i(z_1, \dots, z_m) = P_i(z_1) \cdots P_i(z_m),$$

jolloin saadaan, että u_i on kunnan $\mathbb{K}$ alkio. Samalla tavalla voimme ottaa toisen symmetrisen polynomin

$$S(X_1, \dots, X_m) := \sum_{k=1}^m Q(X_k),$$

jolloin $v := \frac{1}{m} S(z_1, \dots, z_m) = \frac{1}{m} \sum_{k=1}^m Q(z_k)$ on kunnan $\mathbb{K}$ alkio. Eli voimme kirjoittaa

$$\alpha = \frac{1}{m} \sum_{i=1}^n d_i \frac{u_i'}{u_i} + v',$$

ja saamme yhtälön (1), kun määritellään $c_i := d_i/m$.

Seurauksen todistus

Todistetaan lopuksi artikkelin ensimmäisen osan Lause 30 eli seuraava lause.

Lause 29. Olkoot $f, g \in \mathbb{C}(x)$, missä f ei ole nolla eikä g ole vakio, määritellyt jossakin reaalivälissä J . Tällöin funktiolla

$$\begin{aligned} J &\longrightarrow \mathbb{C}, \\ x &\longmapsto f(x)e^{g(x)} \end{aligned}$$

on alkeisintegraalifunktio, jos ja vain jos on olemassa sellainen rationaalifunktio $a \in \mathbb{C}(x)$, että

$$f = a' + ag'. \quad (15)$$

Todistus. ($\Leftarrow$) Oletetaan, että jokin rationaalifunktio $a \in \mathbb{C}(x)$ toteuttaa $f = a' + ag'$. Määritellään

$$h(x) := a(x)e^{g(x)}, \quad \mathbb{K} := \mathbb{C}(x).$$

Koska e^g on eksponenttifunktio kunnan $\mathbb{K}$ suhteen, $\mathbb{K}(e^g)$ on kunnan $\mathbb{C}(x)$ alkeislaajennus. Joten h , joka on tämän laajennuksen alkio, on alkeisfunktio. Lopuksi otetaan derivaatta:

$$h' = a'e^g + ag'e^g = (a' + ag')e^g = fe^g.$$

($\Rightarrow$) Olkoot f epänolla ja g epävakio. Olkoon $\mathbb{L}$ kunnan $\mathbb{C}(x)$ sellainen alkeislaajennus, johon kuuluu funktion fe^g integraalifunktio y . Silloin kuntaan $\mathbb{L}$ kuuluu myös $y' = fe^g$ sekä e^g , joten $\mathbb{L}$ on kunnan $\mathbb{C}(x)(e^g)$ alkeislaajennus. Olkoon

$$\alpha := fe^g, \quad \mathbb{K} := \mathbb{C}(x)(e^g).$$

Liouvillen lauseen mukaan on olemassa sellaiset $t_1, \dots, t_n, w \in \mathbb{K}$ ja $d_1, \dots, d_n \in \mathbb{C}$, että

$$\alpha = \sum_{i=1}^n d_i \frac{t_i'}{t_i} + w'.$$

Tämän voi kirjoittaa eri tavalla Lauseen 9 nojalla, ja niin kuin Liouvillen lauseen todistuksessa saamme yhtälön

$$\begin{aligned} \alpha &= \sum_{i=1}^N e_i \frac{u_i'}{u_i} + \sum_{i=1}^{\tilde{N}} \varepsilon_i \frac{(M_i(f_1))'}{M_i(f_1)} + (S_0(f_1))' \\ &\quad + \sum_{i=1}^{\bar{N}} \sum_{k=1}^{m_i} \frac{(S_{k,i}(f_1))'}{V_i^k(f_1)} - \sum_{i=1}^{\bar{N}} \sum_{k=1}^{m_i} k \frac{S_{k,i}(f_1)(V_i(f_1))'}{V_i^{k+1}(f_1)}. \end{aligned} \quad (16)$$

Lauseen 8 mukaan, e^g on transkendenttinen kunnan $\mathbb{C}(x)$ suhteen, joten voimme käyttää samaa strategiaa kuin Liouvillen lauseen todistuksen osassa, joka koskee transkendenttisiä eksponenttifunktioita. Lisäksi kirjoitetaan α eli fe^g renkaan $\mathbb{C}(x)[X]$ jonakin polynomina pistessä e^g , eli

$$\alpha = fe^g = P(e^g), \quad P(X) := fX.$$

Samalla tavalla kuin yllä mainitussa todistuksen osassa yhtälöstä (16) tulee

$$P(e^g) = \sum_{i=1}^N c_i \frac{u_i'}{u_i} + (S_0(e^g))' + \varepsilon_1 g'. \quad (17)$$

Koska vasemmalla puolella oleva polynomi on ensimmäistä astetta, niin pitää myöskin olla polynomin S'_0 . Ja transkendenttisen eksponenttifunktion tapauksen huomausten mukaan pätee myös $\deg(S_0) = 1$, joten

$$S_0(X) = s_1X + s_0$$

joillakin sopivilla $s_1, s_0 \in \mathbb{C}(x)$. Niinpä yhtälöstä (17) tulee

$$\begin{aligned} fe^g &= \sum_{i=1}^N c_i \frac{u'_i}{u_i} + (s_1e^g + s_0)' + \varepsilon_1g' \\ &= \sum_{i=1}^N c_i \frac{u'_i}{u_i} + s'_1e^g + s_1g'e^g + s'_0 + \varepsilon_1g'. \end{aligned}$$

Kirjoittamalla eri tavalla saamme

$$(f - s'_1 - s_1g')e^g = \sum_{i=1}^N c_i \frac{u'_i}{u_i} + s'_0 + \varepsilon_1g',$$

missä oikea puoli ei sisällä funktiota e^g . Jos funktion e^g kerroin vasemmalla puolella olisi epänolla, saisimme ristiriidan transkendentisuuden kanssa, joten $f - s'_1 - s_1g' = 0$ eli

$$f = s'_1 + s_1g'.$$

Koska $s_1 \in \mathbb{C}(x)$, saamme halutun yhtälön (15). $\square$

Viimeisiä kommentteja

Niin kuin sanottu ensimmäisessä osassa on tämä kirjoitus artikkelin [1] inspiroima, paitsi että tässä teemme

kaiken tavallisen derivaatan ”perus”tapauksessa. Periaatteessa on mahdollista analysoida mikä vaan derivaatta seuraavan määritelmän mukaan.

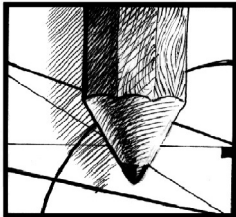
Määritelmä 30. *Differentiaalikunta* on kunta $\mathbb{K}$, jossa määritellään sellainen funktio $D: \mathbb{K} \rightarrow \mathbb{K}$, jota kutsutaan **derivaataksi**, että jokaisilla alkioilla $a, b \in \mathbb{K}$ pätee

$$D(a+b) = D(a) + D(b) \quad \text{ja} \quad D(ab) = D(a)b + aD(b).$$

Esimerkiksi tavallinen derivaatta on derivaatta edellisen määritelmän mukaan. Jos D on derivaatta, niin on $-D$ myöskin. Tämän kirjoituksen tulokset pitävät paikkansa yleisemmässä tapauksessa, että kyseessä on yleinen derivaatta. Matematiikan osa-alue, joka käsittelee tällaisia käsitteitä ja tuloksia on differentiaalialgebra (engl. *differential algebra*).

Viitteet

- [1] C. De Lellis. *Il teorema di Liouville ovvero perché “non esiste” la primitiva di e^{x^2}* . La Matematica nella Società e nella Cultura. Rivista dell’Unione Matematica Italiana 7.1 (2014): 55–97.
- [2] J. Häsä, J. Rämö. *Johdatus abstraktiin algebraan*. Gaudeamus (2015).
- [3] M. Orlich. *Miksei funktiota e^{-x^2} voi integroida?* (Osa 1/2). Solmu 2/2025.



Topologiasta ja matematiikan soveltamisesta

Marjatta Näättänen

Matematiikka on menetelmätiede, joka on aina ollut vuorovaikutuksessa luonnontieteiden ja tekniikan kanssa. Näiden alojen ongelmat ovat johtaneet uusien matemaattisten teorioiden luomiseen, ja toisaalta hyvinkin abstrakteille matemaattisille teorioille on, usein myöhemmin ja yllättäenkin, ilmaantunut sovelluksia. Moderni, tekniikkaa laajasti käyttävä yhteiskuntamme perustuu matematiikalle – joka ei ole luonnontieteiden ja tekniikan kaavakokoelma, vaan koko ajan kehittyvä, itsenäinen tiede. Nykymatematiikan laaja-alaisuuden vuoksi yliopisto-opetus perustutkintovaiheessa tyytyykin tarjoamaan matemaattisen pohjan, jolta voi jatkaa.

Monien matemaatikkojen mielestä matematiikkaa tulisi opettaa koulutasolla tuomalla esiin sen kauneus ja sen tarjoamien älyllisten haasteiden mielihyvä. Tärkeintä on kuitenkin oikean päättelytavan oppiminen – tätähän tarvittaisiin yhteiskunnan kaikilla aloilla, politiikasta alkaen, ongelmien kunnolliseen analysointiin. Matematiikan opiskelu edesauttaa selkeän, järkevän ja luotettavan ajattelutavan kehittymistä. Kuten lihaksia, on aivojakin harjoitettava. ”Use it or lose it” pätee tässäkin.

Matematiikkadiplomin X tehtävissä¹ pääset kurkistamaan muutamiin sellaisiin matematiikan aloihin, kuten lukuteoria, solmuteoria, kombinatoriikka, topologia, joihin koulukursseillasi tuskin törmäät.

Esimerkiksi topologiasta tarjottavat tehtävät ovat askartelua. Toivottavasti ne herättävät kiinnostusta ja poistavat valitettavan yleistä käsitystä, että matema-

tiikka on lähinnä luvuilla laskemista. Matematiikan yhtenäisyys tulee myös esille tehtävissä, joissa eri alat kietoutuvat toisiinsa ja ratkaisutavat voivat olla monenlaisia.

Kiinnostuneille on reittejä jatkoon Solmunkin tiedostojen avulla. Yksi esimerkki topologian käytöstä löytyy Solmusta 1/2025², suomeksi yliopistotason oppikirjoja on kirjoittanut mm. Jussi Väisälä.

Hyvin abstraktin teorian käyttömahdollisuuksia on tutkinut prof. Eero Hyry, joka kuvailee seuraavassa lyhyesti tutkimustaan:

Tässä lyhyt yleistajuinen kuvaus topologisesta data-analyysistä.

Big datan kasvava merkitys edellyttää myös uusia matemaattisia menetelmiä sen käsittelemiseksi. Topologinen data-analyysi on suhteellisen uusi matematiikan osa-alue, joka hyödyntää algebrallista topologiaa datan muodon tutkimiseen ja analysointiin. Topologia tutkii muotoja ilman tarkkoja mittauksia. Homologia on algebrallisen topologian työkalu, jonka avulla voidaan löytää datasta yhtenäisiä komponentteja, reikiä, onkaloita ja näiden korkeampiulotteisia vastineita.

Topologinen data-analyysi on yllättävä käytännön sovellus algebralliselle topologialle, jota pidettiin aikaisemmin täysin teoreettisena matematiikan osa-alueena. Se soveltuu erityisesti korkeampiulotteisen ja ei-lineaarisen datan tutkimiseen, ja pystyy näin usein

¹<https://matematiikkalehtisolmu.fi/2008/diplomi/diplomitehtavat10.pdf>

²<https://matematiikkalehtisolmu.fi/2025/1/talutushihna.pdf>

havaitsemaan piirteitä, jotka jäävät perinteisiltä tilastollisilta menetelmiltä piiloon. Topologisen data-analyysin avulla voidaan dataa tutkia eri mittakaavoissa. Mittakaavan muuttuessa datan todelliset ominaisuudet erottuvat kohinasta.

Tämä aihe on todellakin kiinnostanut tiedetoimittajia. Esimerkkeinä

Precision Problem Solving: Topological Data Analysis Driving Advances in Medicine and Biology | Department of Mathematics

The Mathematical Shape of Things to Come | Quanta

Magazine

Ayasdi Analyzes Shape Of Big Data | InformationWeek

How Mathematicians Use Homology to Make Sense of Topology | Quanta Magazine

Prof. Hyry on työskennellyt vain topologisen data-analyysin teorian parissa. Mutta Tampereella 2021 väitellyt Henri Riihimäki, joka kirjoitti väitöskirjan KTH:ssa ja sen jälkeen toiminut tutkijana Tukholmassa ja Aberdeenissa, on soveltanut sitä biologisiin neuroverkkoihin.



Rahapeliongelma

Jukka Liukkonen

Mat. yo. evp.

Pythonin kanssa peliongelman kimp- puun

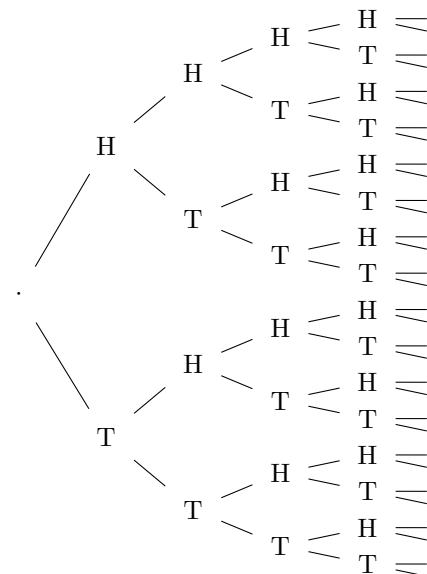
Professori Daniel Litt tutkii leipätyönään algebrallista geometriaa Toronton yliopistossa. Hän kertoo löytäneensä hyödyllisiä välineitä toiselta matematiikan osa-alueelta, lukuteoriasta. Vapaa-aikaansa Litt viettää kolmannen matematiikan osa-alueen, todennäköisyyslaskennan parissa. Hän keksii huvikseen todennäköisyysprobleemoita, jotka johtavat ihmisen intuition helposti harhaan. Tässä on yksi Littin probleemoista:

Kolikko heitetään sata kertaa. Alice saa pisteen aina, kun kaksi kruunaa tulee peräkkäin. Bob saa pisteen aina, kun kruunaa seuraa klaava. Eniten pisteitä kerännyt pelaaja voittaa pelin. Kumpi on todennäköisempi voittaja?

Siis hetkinen: kaikki neljä mahdollista kruunan ja klaavan järjestettyä paria ovat yhtä todennäköisiä, joten Alice ja Bob saavat sadan heittokerran pelissä kumpikin keskimäärin saman määrän pisteitä, ja tuo määrä on $99/4 = 24,75$, sillä sadan kolikon jonossa on vain 99 kolikkoväliä ja saman verran kahden peräkkäisen kolikon muodostamia pareja. Tällöinhän Alice on yhtä todennäköinen voittaja kuin Bob? Varmistetaanpa asia kirjoittamalla pieni kolikonheittoa simuloiva Python-ohjelma.

No, Python-ohjelma kirjoitettiin, mutta siinä vaikutti olevan jokin bugi, sillä onnetar suosi säännöllisesti Bobia, jolla voiton todennäköisyys oli aina kolmisen prosenttiyksikköä suurempi kuin Alicella. Bugia ei sit-

keistä etsinnöistä huolimatta löydetty. Heräsi epäily, että vika on jossain muualla, esimerkiksi aritmeettislogisessa yksikössä otsaluun takana. Hoksattiin tutkia miten käy, jos heittosarja on paljon lyhyempi, vaikkapa neljä heittoa? Oheisesta puukaaviosta, jossa H tarkoittaa kruunaa (*heads*) ja T tarkoittaa klaavaa (*tails*), nähdään huolellisesti katsomalla, että neljän kolikonheiton tapauksessa kaikista mahdollisista 16 pelistä Alice voittaa neljä ja Bob kuusi. Jäljelle jäävät kuusi ovat tasapelejä. Python-ohjelma taisi olla kunnossa alun alkaenkin.



Peli ja peliavaruus

Kolikonheiton *tulosjonoa* mallinnetaan yhtä pitkällä kirjainten H ja T muodostamalla jonolla. Alice saa pisteen jokaisesta HH-esiintymästä ja Bob jokaisesta HT-esiintymästä. Esimerkiksi kirjainjono HTTHHTH vastaa erästä seitsemän kolikonheiton tulosjonoa. Siitä tulee Alicelle yksi piste ja Bobille kaksi. Täydellisyyden vuoksi otetaan mukaan myös pelaajat Cheryl, joka saa pisteen jokaisesta TH-esiintymästä, ja Dustin, joka saa pisteen jokaisesta TT-esiintymästä. Yleisyyttä tavoitellen sovitaan, että kolikkoa heitetään n kertaa. Tällöin puhutaan **n -pelistä**. Kaikkien mahdollisten n -peliin joukkoa kutsutaan **n -peliavaruudeksi**. Pelaajien nimet lyhennetään muotoon A, B, C ja D. Toisesta heittokerrasta alkaen joku nelikosta saa pisteen jokaisella heittokerralla.

Oheinen suunnattu verkko esittää pelin kulkua sen jälkeen, kun kolikkoa on heitetty kaksi kertaa. Verkon solmujen nimet A, B, C ja D kertovat, kuka saa pisteen kyseiseen solmuun tultaessa. Kaaret tai nuolet

AA, AB, BC, BD, CA, CB, DC, DD

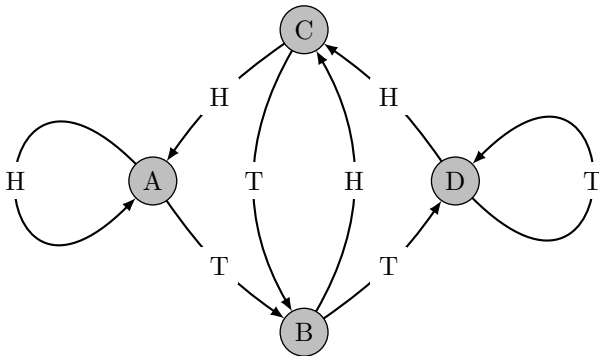
vastaavat siirtymiä *pelitilanteesta* seuraavaan kolikonheiton myötä. Esimerkiksi tulosjonoa

HHTHTTTT

vastaa pelitilanne

ABDCBDD,

jossa Alicella ja Cherylillä on yksi piste kummallakin, Bobilla on kaksi pistettä ja Dustinilla kolme pistettä. Tulosjonot ja pelitilanteet vastaavat toisiaan kääntäen yksikäsitteisesti. Huomaa, että kaikki kirjaimista A, B, C ja D muodostetut jonot eivät edusta pelitilannetta: esimerkiksi AC ei voi toteutua. Vain verkkokaavion mukaiset jonot ovat pelitilanteita.



Kun verkon solmut kootaan matriisiksi

$$\mathbf{G} = \begin{bmatrix} A & B \\ C & D \end{bmatrix},$$

kaikki kaaret saadaan neliöstä

$$\mathbf{G}^2 = \begin{bmatrix} A & B \\ C & D \end{bmatrix}^2 = \begin{bmatrix} AA + BC & AB + BD \\ CA + DC & CB + DD \end{bmatrix},$$

mutta mikä parasta, kaikki n kolikonheittoa vastaavat $n - 1$ kaaren reitit saadaan matriisipotenssista $\mathbf{G}^{n-1}$. Lukija voi tulla vakuuttuneeksi tästä laskemalla potenssin $\mathbf{G}^3$ ja vertaamalla sitä verkkokaavioon. On tärkeää huomata, että toistaiseksi matriisialkiot ovat vain symboleja, joille tulon vaihdantalaki ei ole voimassa, joten laskutoimituksissa kannattaa olla huolellinen. Symbolin tai symbolijonojen tulo tarkoittaa vain niiden asettamista peräkkäin. Plusmerkki symbolijonojen välissä toimii erottimenä, jolla kaksi jonoa erotetaan toisistaan. Tällainen “yhteenlasku” on vaihdannainen. Matriiseilla laskemisen säännöt voidaan tarvittaessa opiskella Wikipedian sivulta [6].

Huomautus. Merkkijonoilla laskeminen ei välttämättä ole epämääräistä puuhastelua. Siitä tulee aivan oikeaa matematiikkaa, kun otetaan käyttöön *vapaan algebran* käsite (ks. [4]). Nyt on kysymys aakkostosta $\{A, B, C, D\}$ muodostettujen merkkijonojen virittämästä vapaasta $\mathbb{Z}$ -algebrasta.

Pelitilanteesta pistetilanteeseen

Pistelaskentaan päästään käsiksi korvaamalla vaihdantalakia noudattamattomat symbolit A, B, C ja D vaihdantalakia noudattavilla symboleilla a, b, c ja d mainitussa järjestyksessä. Esimerkiksi Bobin pisteet pelitilanteessa ABDCBDD saadaan muodostamalla vastaava pistetilannetermi ab^2cd^3 ja katsomalla symbolin b eksponentti: sehän on kaksi. Siirtymällä pelitilanteista pistetilanteisiin menetetään tieto siitä, missä järjestyksessä pisteet ovat kullekin kertyneet. Pelimatriisin $\mathbf{G}$ tilalle astuu tällöin pistematriisi

$$\mathbf{S} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Kaikkien mahdollisten 3-peliin pistetilanteet nähdään matriisista

$$\mathbf{S}^2 = \begin{bmatrix} a^2 + bc & ab + bd \\ ac + cd & bc + d^2 \end{bmatrix}.$$

Matriisialkioiden summasta

$$\mathbf{1}^T \mathbf{S}^2 \mathbf{1} = a^2 + bc + ab + bd + ac + cd + bc + d^2,$$

missä

$$\mathbf{1} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad \mathbf{1}^T = \begin{bmatrix} 1 & 1 \end{bmatrix},$$

havaitaan Alicen saavan yhdestä pelistä keskimäärin $(2 + 0 + 1 + 0 + 1 + 0 + 0 + 0)/8 = 1/2$ pistettä, ja Bobin vastaava keskiarvo on $(0 + 1 + 1 + 1 + 0 + 0 + 1 + 0)/8 = 1/2$. Keskiarvojen yhtäsuuruus ei ole yllätys. Ensimmäisen kappaleen lukemisen jälkeen ei enää yllätä sekään, että Alice voittaa Bobin kahdessa pelissä, kun

taas Bob voittaa Alicen kolmessa pelissä. Miten käy, kun kolikkoa heitetään kolmen heiton sijaan sata kertaa? Tulostulokset on aika monta. Niiden lukumäärä on 31-numeroinen kokonaisluku.

Huomautus. Siirtyminen pelitilanteista pistetilanteisiin merkitsee siirtymistä vapaasta $\mathbb{Z}$ -algebrasta vastaavaan polynomialgebraan $\mathbb{Z}[a, b, c, d]$ (ks. [7]).

Fokus Aliceen ja Bobiin

Kuten lukija varmaan jo huomasi, parivaljakoiden (Alice, Bob) ja (Dustin, Cheryl) kesken vallitsee symmetria; toisin sanoen, kun verkkokaaviossa A ja D, B ja C sekä H ja T vaihdetaan keskenään, kaavion informaation sisältö ei muutu lainkaan. Sama vaikutus, siis ei vaikutusta ollenkaan, saadaan aikaan kiertämällä kaaviota 180° .

Kun ollaan kiinnostuneita pelkästään Alicen ja Bobin keskinäisestä taistosta, pistetilannetermeissä c ja d korvataan ykkösillä. Silloin

$$S = \begin{bmatrix} a & b \\ 1 & 1 \end{bmatrix}, \quad S^2 = \begin{bmatrix} a^2 + b & ab + b \\ a + 1 & b + 1 \end{bmatrix},$$

ja kahden muuttujan a ja b pistetilannepolynomi saa muodon

$$\mathbf{1}^T S^2 \mathbf{1} = a^2 + b + ab + b + a + 1 + b + 1 = a^2 + ab + a + 3b + 2.$$

Tästä riisutustakin versiosta nähdään Alicen ja Bobin pisteet sekä heidän kaksintaistelussa voittamiensa pelien määrät.

Huomautus. Kun c ja d korvataan ykkösillä, polynomialgebra $\mathbb{Z}[a, b, c, d]$ samalla projisoidaan alialgebraksi $\mathbb{Z}[a, b]$.

Fokus voitettujen pelien lukumäärään

Jos kiinnostuksen kohteena on pelkästään artikkelin alussa mainittu kysymys siitä, kumpi on todennäköinen voittaja, Alice vai Bob, pistetilannetermejä modifioidaan edelleen sopimalla, että $ab = 1$, jolloin tasapelit redusoituvat ykkösiksi. Esimerkiksi peliin ABDCBDD liittyvä pistetilannetermi ab^2cd^3 , joka on jo degeneroitunut muotoon ab^2 , pelkistyy sopimuksen jälkeen pelkäksi alkioksi b . Tästä nähdään, että Bob voittaa Alicen yhdellä pisteellä kyseisessä pelissä. Polynomi

$$\begin{aligned} \mathbf{1}^T S^2 \mathbf{1} &= a^2 + ab + a + 3b + 2 \\ &= a^2 + 1 + a + 3b + 2 \\ &= a^2 + a + 3b + 3 \end{aligned}$$

kertoo meille, että kolmesta kolikonheitosta voi syntyä kaikkiaan $8 = 1^2 + 1 + 3 \cdot 1 + 3 = 2^3$ (sijoita $a = b = 1$) erilaista peliä. Niistä Alice voittaa yhden kahdella pisteellä (a^2) ja yhden yhdellä pisteellä (a), kun Bob puolestaan voittaa kolme peliä yhdellä pisteellä ($3b$). Alicen

ja Bobin keskinäisessä kisassa tasapelejä on kolme (3). Degeneroitunutkin polynomi on täten sangen informatiivinen.

Huomautus. Sopimus $ab = 1$ merkitsee, että polynomialgebra $\mathbb{Z}[a, b]$ ensin projisoidaan polynomialgebraksi $\mathbb{Z}[a]$ ja sen jälkeen lokalisoidaan Laurentin polynomialgebraksi $\mathbb{Z}[a, a^{-1}]$ (ks. [5]).

Heittojen lukumäärä $n + 1$

Polynomi $\mathbf{1}^T S^n \mathbf{1}$ monimutkaistuu vauhdikkaasti, kun n kasvaa. Sen aste kasvaa lineaarisesti, mutta kertoimet eksponentiaalisesti, minkä todistaminen jätetään lukijalle. Esimerkiksi

$$\begin{aligned} \mathbf{1}^T S^6 \mathbf{1} &= a^6 + a^5 + 2a^4 + 8a^3 + 12a^2 \\ &\quad + 18a + 30 + 32b + 19b^2 + 5b^3. \end{aligned}$$

Tässä termit on kirjoitettu alkion a alenevien potenssien mukaan, kun otetaan huomioon sopimus eli yhtälö $ab = 1$, jonka mukaan $b = a^{-1}$ on alkion a käänteisalkio. Matriisipotenssien laskemista on mahdollista helpottaa diagonalisoimalla. Menetelmään tarkemmin puuttumatta todetaan, että matriisi S voidaan esittää hajotelmana

$$S = P \Lambda P^{-1},$$

missä P^{-1} on matriisin P käänteismatriisi, so.

$$P P^{-1} = P^{-1} P = I, \quad I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

ja Λ on lävistäjämatriisi eli muotoa

$$\begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}.$$

Silloin on voimassa

$$S^n = P \Lambda^n P^{-1},$$

ja keskimäinen matriisipotenssi on helppoa laskea, sillä

$$\Lambda^n = \begin{bmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{bmatrix}.$$

Lukija voi verifioida nämä kaksi yhtälöä harjoitustehtävänä. Osoittautuu, että hajotelma $S = P \Lambda P^{-1}$ toteutuu, kun lävistäjäalkioina ovat

$$\begin{aligned} \lambda_1 &= \frac{1}{2} \left(a + 1 + \sqrt{(a-1)^2 + 4b} \right), \\ \lambda_2 &= \frac{1}{2} \left(a + 1 - \sqrt{(a-1)^2 + 4b} \right), \end{aligned}$$

ja kerroinmatriisit ovat esimerkiksi

$$\begin{aligned} P &= \begin{bmatrix} \lambda_1 - 1 & \lambda_2 - 1 \\ 1 & 1 \end{bmatrix}, \\ P^{-1} &= \frac{1}{\lambda_1 - \lambda_2} \begin{bmatrix} 1 & 1 - \lambda_2 \\ -1 & \lambda_1 - 1 \end{bmatrix}. \end{aligned}$$

Tämänkin toteen näyttäminen normaaliin tapaan laskemalla jätetään lukijalle harjoitustehtäväksi.

Huomautus. Symbolien a ja b olemuksesta tiedetään vain, että $ab = 1$. Ei ole tarkoituksenmukaista esitellä uusia algebrallisia struktuureja aikaisemmissa huomautuksissa esiteltyjen lisäksi, joten edellä mainittujen neliöjuurten olemus ja olemassaolo jäävät hämärän peittoon. Kun tavoitteena on matriisitulon $\mathbf{1}^T \mathbf{S}^n \mathbf{1}$ esittäminen kokonaislukukertoimisena polynomina, ja neliöjuuret lopulta supistuvat lausekkeista pois, tällainen formaali eli muodollinen kaavojen pyörittely nähtäkään pelkästään keinona päästä lopputulokseen. Menettely voidaan hyväksyä ainakin silloin, kun lopputuloksen pätevyys on mahdollista verifioida laillisin keinoin. Monesti jonkin lausekkeen keksiminen on hyvin vaikeaa, mutta kun lauseke lopulta tavalla tai toisella keksitään, sen todistaminen päteväksi esimerkiksi induktiolla on hyvin yksinkertaista. Sitä paitsi: eikös joku ole joskus sanonut, että ”tarkoitus pyhittää keinot”.

Yleiseen $(n+1)$ -peliin liittyvän tehtävän ratkaisun vaikeus piilee siinä, että potenssien λ_1^n ja λ_2^n ja lopulta polynomin $\mathbf{1}^T \mathbf{S}^n \mathbf{1}$ laskeminen johtaa monimutkaisiin lausekkeisiin. Kun kyseinen polynomi on jollain keinolla saatu laskettua, se voidaan esittää kanonisessa muodossa

$$p(a, b) = \sum_{i=1}^I \alpha_i a^i + \gamma + \sum_{j=1}^J \beta_j b^j.$$

Tasapeliin lukumäärä on

$$p(0, 0) = \gamma.$$

Alicen ja Bobin voittamien pelien lukumäärät ovat vastaavasti

$$p(1, 0) - \gamma = \sum_{i=1}^I \alpha_i \text{ ja } p(0, 1) - \gamma = \sum_{j=1}^J \beta_j.$$

Huomautus. Nollan sijoittaminen muuttujan a tai b paikalle saattaa tuntua oudolta, kun muistetaan sopimus $ab = 1$. Idea on siinä, että tuota sopimusta käytetään saatettaessa polynomin lauseketta edellä esitettyyn kanoniseen muotoon. Tämän jälkeen on enää kysymys polynomin kertoimista ja niiden summista. Jos ne saadaan selville sijoittamalla nolla muuttujan paikalle, tälle polynomin syntyhistoriaan nähden laittomalle sijoitukselle ei ole mitään estettä. Kun kanonisointiin liittyvät laskut ovat vielä kesken, nollan sijoittaminen muuttujan paikalle johtaa väärään lopputulokseen. Esimerkiksi jos yhtälöketjun

$$(a+b)^2 = a^2 + 2ab + b^2 = a^2 + 2 + b^2$$

ensimmäiseen yhtälöön sijoitetaan $a = b = 0$ vakio-termin paljastamiseksi, saadaan väärä tulos 0. Sijoitus sopii tehdä vasta loppuun asti laskettuun kanoniseen muotoon. Silloin saadaan oikea tulos 2.

Eräs keino mutkikkaiden lausekkeiden hallitsemiseksi on käyttää laskentaan jotakin symbolisen laskennan ohjelmistoa. Näin on tehty mm. artikkelissa [1], vaikkakin eri lähtökohdista kuin edellä esitetty. Symbolisen laskennan lisäksi todistusvoimaa saadaan kompleksianalyysistä kuten artikkelissa [3]. Itse asiassa polynomi $p(a, b)$ voidaan kirjoittaa vastaavaksi kompleksimuuttujan z Laurentin sarjaksi

$$L(z) = \sum_{i=1}^I \alpha_i z^i + \gamma + \sum_{j=1}^J \beta_j z^{-j},$$

joka tässä tapauksessa, kun termejä on vain äärellinen määrä, on pelkkä Laurentin polynomi. Jos funktion L lauseketta ei tunneta sarjamuodossa, sarjan tuntemattomat kertoimet saadaan joskus selville kompleksista integrointia käyttäen. Vaikka se ei onnistuisikaan, integraalit saattavat kuitenkin kertoa jotain oleellista informaatiota kertoimista.

Tuloksia

Vaikka kolikonheittoprobleema johtaa pitkiin laskuihin, sitä on hyvin helppoa tutkia kokeellisesti. Sadan heiton kisaa Alicen ja Bobin välillä simuloitiin tätä artikkelia varten yksinkertaisella Python-ohjelmalla, joka käytti heittotulosten arpomiseen satunnaislukugeneraattoria. Kymmenestä miljoonasta pelistä Alice voitti 4 574 682, Bob voitti 4 859 895, ja tasapelejä tuli 565 423 kappaletta. Tämän kokeen valossa Alice voittaa pelin noin 45,7 %:n todennäköisyydellä, Bob voittaa noin 48,6 %:n todennäköisyydellä, ja peli päättyy tasan noin 5,7 %:n todennäköisyydellä. Artikkelissa [1] lasketut teoreettiset arvot ovat vastaavasti 0,4576402592, 0,4858327983 ja 0,0565269425.

Eräs kollega laski Mathematica-ohjelmalla polynomin $p(a, b) = \mathbf{1}^T \mathbf{S}^{99} \mathbf{1}$ arvot $p(1, 0)$, $p(0, 1)$ ja $p(0, 0)$, kun

$$\mathbf{S} = \begin{bmatrix} a & b \\ 1 & 1 \end{bmatrix},$$

ja sai sitä kautta selville, miten monta 2^{100} :sta mahdollisesta pelistä päättyy Alicen tai Bobin voittoon tai tasapeliin:

Bob voittaa	615 866 238 418 960 422 359 689 555 420
Alice voittaa	580 127 949 239 420 834 381 088 427 404
Tasapeli	71 656 412 569 848 144 755 925 222 552
Yhteensä	1 267 650 600 228 229 401 496 703 205 376

Artikkelissa [3] todistetaan, että Bob voittaa n -pelin todennäköisemmin kuin Alice, kun $n \geq 3$. Toisin sanoen Bob voittaa suuremman osan n -peliavaruuden peleistä kuin Alice, kun $n \geq 3$. Artikkelissa todistetaan myös, että kumpikin todennäköisyys lähestyy raja-arvoaan lukua $1/2$, kun n kasvaa rajatta, ja todennäköisyyksien erotus

$$\mathbb{P}(\{\text{Bob voittaa}\}) - \mathbb{P}(\{\text{Alice voittaa}\})$$

vieläpä käyttäytyy asympotoottisesti kuin

$$\frac{1}{2\sqrt{n\pi}} + \mathcal{O}\left(n^{-3/2}\right).$$

Pohdintaa

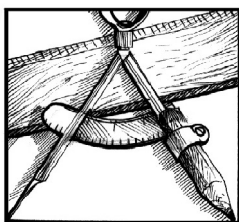
Alicelle pisteen tuovia pareja HH on tasan yhtä monta kuin Bobille pisteen tuovia pareja HT, kun kaikki n -pelit otetaan mukaan laskentaan. Siksi on ehkä yllättävää, että Bob kuitenkin voittaa suuremman osan yksittäisistä n -peleistä kuin Alice. Koska tarkastelu käsittelee koko peliavaruuden, mukana ovat myös sellaiset pelit, joissa Alice saa yli $n/2$ pistettä. Tällaisiin peleihin sisältyvät Alicen pisteet ovat poissa muihin peleihin sisältyvistä Alicen pisteistä. Bobin sen sijaan on mahdollonta saada yhdestäkään pelistä enempää kuin $n/2$ pistettä. Näin ollen Bobin pisteet ovat tasaisemmin jakautuneet n -pelien kesken. Kärjistäen voidaan sanoa, että Alice voittaa pienen määrän pelejä isolla pistemäärällä, jolloin Bob saa tilaisuuden voittaa suuren määrän pelejä pienellä pistemäärällä. Tällainen heuristiikka tukee Bobin onnekkautta, mutta kokonaan toinen asia on siihen pohjautuvan todistuksen kirjoittaminen, jos se ylipäänsä on mahdollista.

Daniel Litt haluaisi nähdä Bobin onnekkauudelle todistuksen, jossa intuitio ei peittyisi teknisten yksityiskohden taakse. Joskus todistukset ovat sellaisia, että väite kyllä putkahtaa monimutkaisen päättelyketjun ja hirmuisten laskelmien jälkeen ulos, ja kaikki pystyvät verifoimaan todistuksen päteväksi vaihe vaiheelta, mutta kukaan ei oikeastaan ymmärrä, mitä todistuksessa tapahtuu. Littin problema yleiselle n -pelille on sen luontoinen, että joku aiheesta kiinnostunut nuori opiskelija, jolla ei vielä ole kokemuksen painolastia harteillaan, saattaisi onnistua keksimään omintakeisen ratkaisun, johon urautuneiden ammattilaisten mielikuvitus ei ole

riittänyt. Quanta Magazine -verkkolehdestä [2] on professori Littin haastattelu.

Viitteet

- [1] Shalosh B. Ekhad & Doron Zeilberger: *How to Answer Questions of the Type: If you toss a coin n times, how likely is HH to show up more than HT?*
Kirjoitus arXiv-julkaisualustalla 22.5.2024.
<https://arxiv.org/abs/2405.13561>
- [2] Erica Klarreich: *Perplexing the Web, One Probability Puzzle at a Time.*
Kirjoitus Quanta Magazine -verkkolehdestä 29.8.2024.
<https://www.quantamagazine.org/perplexing-the-web-one-probability-puzzle-at-a-time-20240829/>
- [3] Simon Segert: *A proof that HT is more likely to outnumber HH than vice versa in a sequence of n coin flips.*
Kirjoitus arXiv-julkaisualustalla 26.5.2024.
<https://arxiv.org/abs/2405.16660>
- [4] Wikipedia: *Free algebra.*
https://en.wikipedia.org/wiki/Free_algebra
- [5] Wikipedia: *Laurent polynomial.*
https://en.wikipedia.org/wiki/Laurent_polynomial
- [6] Wikipedia: *Matrix (mathematics).*
[https://en.wikipedia.org/wiki/Matrix_\(mathematics\)](https://en.wikipedia.org/wiki/Matrix_(mathematics))
- [7] Wikipedia: *Polynomial ring.*
https://en.wikipedia.org/wiki/Polynomial_ring



Ympyrän neliöiminen

Reijo Hautakangas

Tarkastellaan kysymystä siitä, voidaanko piirtää neliö, jonka pinta-ala on sama kuin annetun ympyrän pinta-ala. Neliön sivun pituuden pystyy tietenkin laskemaan helposti. Sen sijaan harpilla ja viivaimella tällaista neliötä ei voi piirtää, sillä esimerkiksi yksikköympyrää vastaavan neliön piirtäminen edellyttäisi erään transkendenttiluvun mittaisen pituuden konstruoimisen harpilla ja viivaimella. Sen sijaan likiarvotarkaisuja voi tehdä harpilla ja viivaimella.

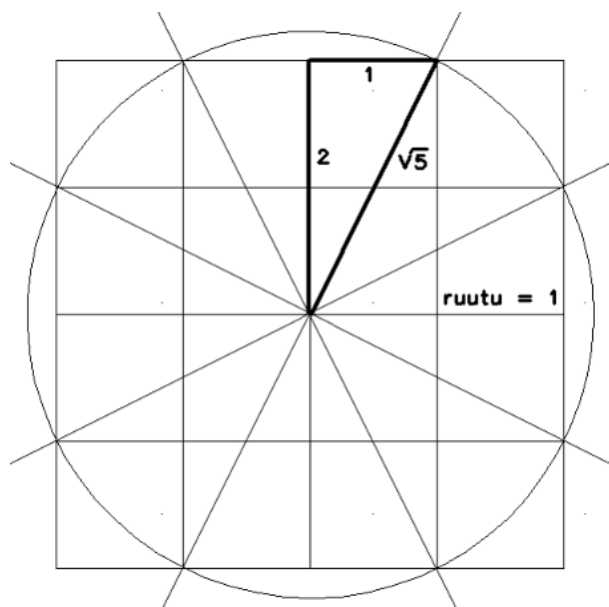
Voidaan esimerkiksi löytää niin tarkka ratkaisu, että kun otetaan huomioon harppiviivainmenetelmän luontainen piirustusepätarkkuus, niin itse ratkaisumenetelmän epätarkkuus ei juuri huononna tulosta.

Lähdetään aluksi ratkaisemaan toista tehtävää: Neliön ympyröiminen. Tämäkin on mahdotonta ratkaista tarkasti harpilla ja viivaimella, sillä tämänkin ratkaiseminen antaisi transkendenttiluvun mittaisen pituuden konstruktion. Neliön ja ympyrän pinta-alojen yhtäsuuruus on tavoitteena tässäkin.

Jaetaan piirretty neliö aluksi kuuteentoista ruutuun. Ruudun sivun pituus on 1. Kuvaan piirretään ympyrä neliön keskipisteeseen. Sen säteeksi otetaan $\sqrt{5}$ kuvan mukaisesti. Ympyrän ja neliön leikkauspisteiden kautta kulkevat sädesuorat lisätään kuvaan (niiden ja neliön sivujen väliset kulmat määräävät ympyrän ja neliön pinta-alojen suhteen).

Neliön pinta-ala on

$$s^2 = 4 \cdot 1 = 4$$



ja ympyrän

$$\pi r^2 = \pi(\sqrt{5})^2 = \pi 5 = 15,70 \dots$$

Pinta-alavirhesuhde on

$$16/15,70 \dots = 1,018 \dots$$

ja viivavirhesuhde

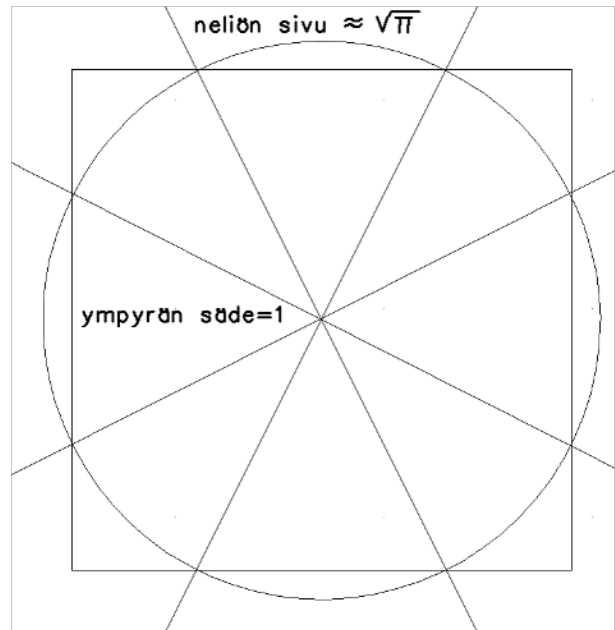
$$\sqrt{1,018 \dots} = 1,0092 \dots$$

Ympyrän säde on siis hiukan liian lyhyt ($< 1\%$).

Nyt voidaan lähteä ratkomaan alkuperäistä tehtävää: ympyrän neliöiminen.

Siirretään neliöitävä ympyrä samaan keskipisteeseen edellisen tehtävän ympyrän kanssa. Sädesuorien kanssa syntyy 8 uutta leikkauspistettä, jotka määrittävät piirrettävän uuden neliön sivut. Neliöitävän ympyrän säteeksi merkitään 1 ja uuden neliön sivuksi $\approx \sqrt{\pi}$. Nämä uudet tekstit ja viivat voidaan piirtää leveämpinä tai erivärisinä, jotta ne erottuisivat vanhasta kuviosta.

Käytännössä näiden kuvien piirtäminen on huomattavan yksinkertaista ruutupaperia käyttäen, mitä harpiviivainmenetelmä ei kuitenkaan salli. Tällöin voitaisiin käyttää sädesuorien tangentille tarkempia kokonaislukujen (ruutujen) osamääriä kuin tuo $1/2$, joita löytyykin runsaasti. Esimerkiksi $23/44$ on jo turhanakin tarkka. Oikea arvo on $\sqrt{(4-\pi)/\pi}$ ($= 0,52272\dots$), josta neliön sivujen ja sädesuorien väliseksi kulmaksi saadaan $27,597\dots^\circ$. Tässä ratkaisussa neliön sivu on kuitenkin hiukan liian pitkä ($< 1\%$).



Solmu 3/2025

ISSN-L 1458-8048

ISSN 1459-0395 (Painettu)

ISSN 1458-8048 (Verkkolehti)

Julkaisija:

Suomen matemaattinen yhdistys ry

PL 68 (Pietari Kalmin katu 5)

00014 Helsingin yliopisto

Päätoimittaja:

Anne-Maria Ernvall-Hytönen, professori, Matematiikan ja tilastotieteen osasto, Helsingin yliopisto

Toimitussihteeri:

Juha Ruokolainen, FT

Sähköposti:

toimitus@matematiikkalehtisolmu.fi

Verkkosivu:

matematiikkalehtisolmu.fi

Toimittajat:

Pekka Alestalo, dosentti, Matematiikan ja systeemianalyysin laitos, Aalto-yliopisto

Sirkka-Liisa Eriksson, dosentti, Matematiikan ja tilastotieteen osasto, Helsingin yliopisto

Aapo Halko, FT, Matematiikan ja tilastotieteen osasto, Helsingin yliopisto

Olli Järvinen, jatko-opiskelija, Matematiikan ja tilastotieteen laitos, Turun yliopisto

Jyrki Lahtonen, yliopistonlehtori, Matematiikan ja tilastotieteen laitos, Turun yliopisto

Heikki Pokela, tuntiopettaja, Tapiolan lukio

Antti Rasila, Associate Professor, Guangdong Technion - Israel Institute of Technology

Mikko Sillanpää, professori, Matemaattisten tieteiden laitos ja Biologian laitos, Oulun yliopisto

Samuli Siltanen, professori, Matematiikan ja tilastotieteen osasto, Helsingin yliopisto

Kimmo Vehkalahti, vanhempi yliopistonlehtori, Yhteiskuntatieteiden keskus, Helsingin yliopisto

Tieteelliset asiantuntijat:

Heikki Apiola, dosentti, Matematiikan ja systeemianalyysin laitos, Aalto-yliopisto

Mika Koskenoja, dosentti, Matematiikan ja tilastotieteen osasto, Helsingin yliopisto

Liisa Näveri, FT, Opettajankoulutuslaitos, Helsingin yliopisto

Matematiikkadiplomit:

Juha Ruokolainen, juha piste ruokolainen 'at' yahoo piste com

Marjatta Näätänen, dosentti, Matematiikan ja tilastotieteen osasto, Helsingin yliopisto

Yliopistojen ja korkeakoulujen yhteyshenkilöt:

Ari Koistinen, FM, Metropolia Ammattikorkeakoulu

Juha Lehtinen, yliopistonlehtori, Matematiikan ja tilastotieteen laitos, Jyväskylän yliopisto

Jorma Merikoski, emeritusprofessori, Tietotekniikan yksikkö, Tampereen yliopisto

Antti Viholainen, yliopistonlehtori, Fysiikan ja matematiikan laitos, Itä-Suomen yliopisto

Kansikuva:

Noora Isoeskelä

Painopaikka:

Painosalama Oy

Numeroon 1/2026 tarkoitetut kirjoitukset pyydämme lähettämään 1.2.2026 mennessä.

Kiitämme taloudellisesta tuesta Jenny ja Antti Wihurin rahastoa.

Laaja-alainen projektiosaaminen matematiikan opetuksessa

Matematiikkalehti Solmun matematiikkadiplomien tehtävistä kerättyjä tehtäväpaketteja voi käyttää laaja-alaisen osaamisen opetuksessa. Eri aihepiireihin liittyviä matematiikan tehtäviä ratkomalla oppilaat huomaavat, että matematiikan osaamista tarvitaan monissa eri yhteyksissä. Matematiikan kumuloituva rakenne vaatii ennen matemaattisten työkalujen käyttöä aineen sisäistä (eli vertikaalista) eheyttämistä, vasta tämän jälkeen voidaan pyrkiä eri oppiaineiden väliseen (horisontaaliseen) eheyttämiseen. Tarvittavien matematiikan sisältöjen on siis oltava hallinnassa ennen niiden käyttöä. Opettajan ratkaistavaksi jää eri oppiaineiden erilainen etenemistähti, esimerkiksi käsite mittakaava voi tulla esille maantiedossa eri luokka-asteella kuin matematiikassa.

Käytettävissä on 10 tehtäväpakettia. Alla annetaan neljästä paketista esimerkkejä niiden sisällöistä. Tehtävät voi tulostaa Matematiikkalehti Solmun (matematiikkalehtisolmu.fi) Matematiikkadiplomi-sivulta ja pyytää vastaukset osoitteesta juha.ruokolainen@yahoo.com

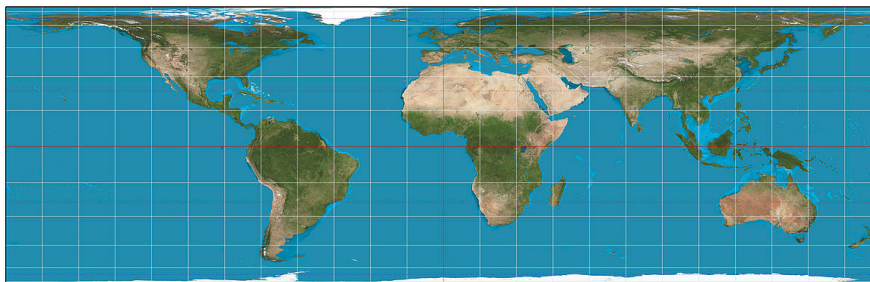
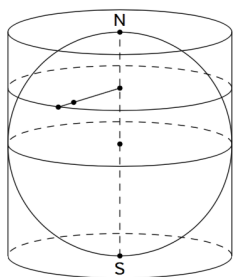
Koululle ei aiheudu muita kuin mahdollisia monistus/tulostuskustannuksia.

Tehtäväpaketit

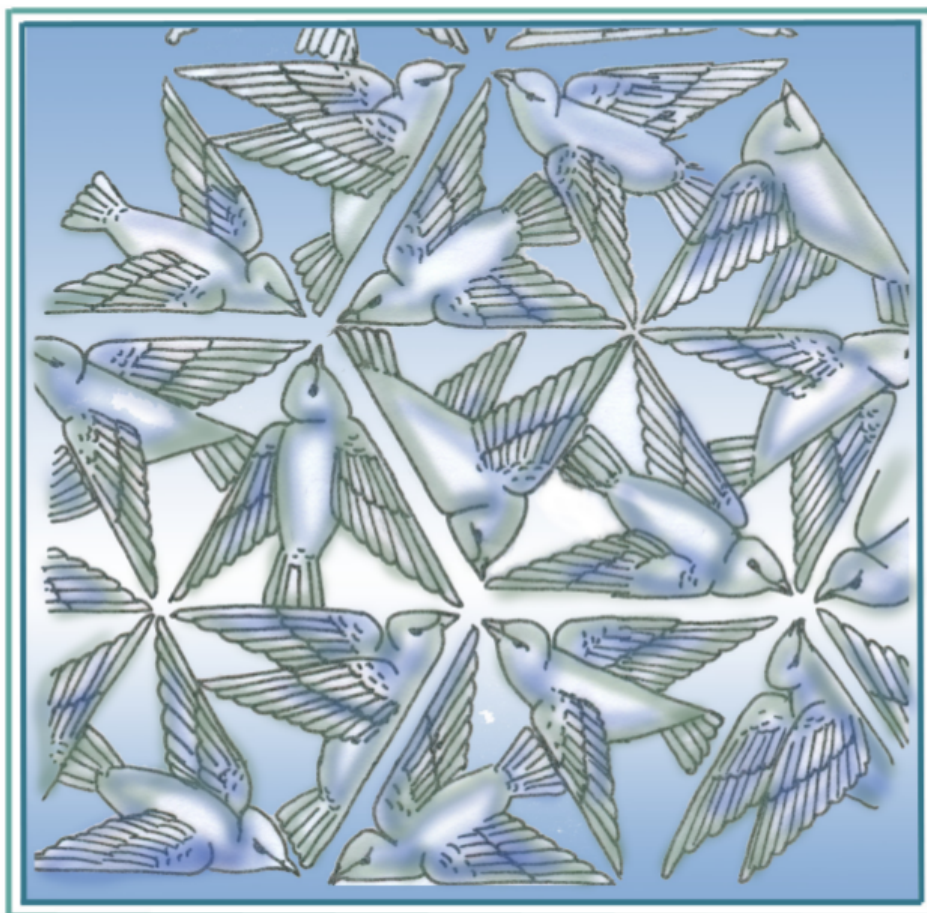
Peruskoulua, ehkä osittain myös lukiota, varten koottujen tehtäväpakettien aiheet ovat:

- **Maapallo** (Sisältöjä: maapallo, etäisyyksiä luonnossa ja kartalla, tasokartta, ihminen Aurion ja vetyatomien välissä. Matemaattisia sisältöjä: suuruussuhteet, mittakaava, etäisyydet, myös pallolla, maapallon pyöriminen, projektio, suuret luvut.)
- **Suomen historia** (Sisältöjä: väkiluvun kehitys keskiajalta, kaupungit, kansakoulu, tytöt ja pojat opetuksessa, taiteilijoita, radioaktiivinen hajoaminen, Pisa-tulokset. Matemaattisia sisältöjä: ajan yksiköt, prosenttilaskenta ja prosenttipisteet, kaavioiden laatiminen ja tulkitseminen, lineaarinen approksimaatio, murtoluvut, päättely.)
- **Terveys ja ravinto** (Matemaattisia ym. sisältöjä: suhteet, prosentit, perusaineenvaihdunta, liikkuminen, painoindeksi, energian tarve, kalorit, ajankäyttö, lääkeannostus, alkoholi ja hormonit)
- **Talous** (Sisältöjä: kauppa- ja hinnanalennuslaskuja, remonttikustannuslaskuja, brutto- ja nettopalkka, verotus, korot, pörssi, valtion budjetti, luonnonvarojen tuottavuus eri EU-maissa)
- **Todennäköisyys**
- **Matematiikka ja taide** (2 tasoa)
- **Mittaaminen** (2 tasoa)
- **Koodauksen (tai ohjelmoinnin) pohjustus**, jossa on eri vaihtoehtoja tutkivia tehtäviä.

Alaluokille sopivia tehtäviä on kolmen viimeisen aiheen paketeissa.



Kuva: Strebe (Oma teos) [CC BY-SA 3.0], lähde: Wikimedia Commons



 SOLMU
MATEMATIIKKALEHTI

matematiikkalehtisolmu.fi