

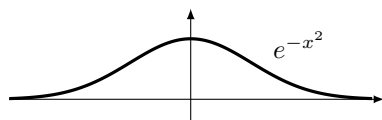
Miksei funktiota e^{-x^2} voi integroida? (Osa 1/2)

Milo Orlich

Matematiikan ja systeemianalyysin laitos, Aalto-yliopisto

milo.orlich@alumni.aalto.fi

Moni tuntee funktion e^{-x^2} niin sanottuna Gaussin kellokäyränä, jota käytetään tilastotieteessä normaalijakauman tiheysfunktiona. Sillä on symmetrinen, kellomainen muoto ja kauniita ominaisuuksia.



Mutta yllätys odottaa opiskelijaa, joka yrittää laskea sen integraalia: funktiolla e^{-x^2} ei ole alkeisintegraalifunktiota.

Tässä artikkelissa selvitämme, mitä tämä tarkoittaa ja miksi näin on. Ensimmäisessä osassa tutustumme algebran käsitteisiin, kuten kuntiin ja kuntalaajennuksiin, joita käytetään esittelemään Liouvillen lause. Mukana on lauseen seuraus, jonka avulla todistetaan, ettei funktiolla e^{-x^2} ole alkeisintegraalifunktioita.

Artikkelin toinen osaa koostuu Liouvillen lauseen pitkästä todistuksesta.

Ongelman esittely ja artikkelin rakenne

Yliopiston fuksina osallistut heti alusta differentiaali- ja integraalilaskennan kurssille. Siellä opit, miten reaaliuuttujan funktion derivaatta ja integraali lasketaan.

Tässä kirjoituksessa oletetaan, että nämä käsitteet ovat jo jotenkin tuttuja.

Muistetaan kuitenkin varmuuden vuoksi, että funktion f derivaatta määritellään pisteessä $x_0 \in \mathbb{R}$ seuraavasti:

$$f'(x_0) = \lim_{x \rightarrow x_0} \frac{f(x) - f(x_0)}{x - x_0}$$

(jos raja-arvo on olemassa). Funktion f integraalifunktio on funktio, jonka derivaatta on f , ja sitä merkitään

$$\int f(x) dx.$$

Määritelmä 1. Reaaliuuttujan reaaliarvoista funktiota kutsutaan **alkeisfunktioiksi**, jos se on

- *rationaalifunktio* (eli kahden polynomin osamäärä, esimerkiksi polynomi),
- *algebrallinen funktio* (esim. neliöjuuri, kuutiojuuri, ..., ja yleisemmin polynomisen yhtälön ratkaisu),
- *eksponentti- tai logaritmifunktio*,
- *trigonometrinen funktio tai sen käänteisfunktio*,

tai äärellinen summa, tulo, osamäärä tai kompositio yllä olevista funktioista.

Esimerkki 2. Esimerkiksi funktiot

$$x^{\cos(x-1)} - e^{x^2}, \quad \frac{\sqrt{x} + \arcsin(x^2)}{\sqrt[3]{e^{\sin(x)}} - \arccos(x)} \quad \text{ja}$$

$$\frac{\cos(1 + e^{5x^3 - \ln(x^4 + 2)} - \cos(x)^{\sin(x)}) \cdot (x^3 + 2x^2 + 17)}{5x^5 + 3x^2 - 5\sqrt{x} - 17\sqrt[5]{\tan(x)^3} + e^{-x}}$$

ovat alkeisfunktioita.

Derivointi on mekaaninen prosessi: jokaisen alkeisfunktion derivaatan voi laskea tulon säännön tai ketjusäännön jne. avulla, ja äärellisen monen askelen jälkeen derivaatan voi kirjoittaa eksplisiittisesti. Jokaisen alkeisfunktion derivaatta on itse alkeisfunktio, esimerkiksi:

$f(x)$	$f'(x)$
x^n	nx^{n-1}
e^x	e^x
$\log(x)$	$1/x$
$\sin(x)$	$\cos(x)$
$\cos(x)$	$-\sin(x)$

Muiden alkeisfunktioiden derivaatta lasketaan yhdistelemällä sopivasti taulukossa olevia funktioita.

Toisaalta integrointi ei ole niin yksinkertaista. (Matemaatikkoja ja insinöörejä ärsyttää, kun symmetria puuttuu...) On olemassa alkeisfunktioita joiden integraalifunktiot eivät ole alkeisfunktioita!

Tehtävä 3. Yritä laskea $\int e^{-x^2} dx$. (Mutta älä yritä liian pitkään. Tätä ei pysty laskemaan.) Kokeile vaan osittaisintegrointia tai sijoitusmenettelyä.

Joskus sanotaan jotenkin epämääräisesti, että funktiota e^{-x^2} ”ei voi integroida”, ja tämän lauseen voi vahingossa ymmärtää niin, että integraalifunktioita ei ole olemassa ollenkaan. Itse asiassa integraalifunktio voidaan kyllä kirjoittaa vaikka sarjana, kun muistetaan, että $e^y = \sum_{k=0}^{+\infty} \frac{y^k}{k!}$. Saadaan siis

$$\begin{aligned} \int e^{-x^2} dx &= \int \sum_{k=0}^{+\infty} \frac{(-x^2)^k}{k!} dx \\ &= \sum_{k=0}^{+\infty} \int \frac{(-x^2)^k}{k!} dx \\ &= \sum_{k=0}^{+\infty} (-1)^k \frac{x^{2k+1}}{(2k+1) \cdot k!} + c, \quad c \in \mathbb{R}. \end{aligned}$$

Sarja ei kuitenkaan ole alkeisfunktio.

Tässä kirjoituksessa esitetään Liouvillen lauseen kautta todistus, ettei funktiolle e^{-x^2} ole olemassa alkeisintegraalifunktioita.

Artikkelin rakenne

Aluksi kootaan ne käsitteet, jotka tarvitaan kompleksianalyysistä. Sitten siirrytään algebraan: määritellään

kunnat, sen jälkeen keskustellaan polynomeista ja kuntalaajennuksista. Kun kaikki työkalut ovat saatavilla, esitetään lopulta Liouvillen lause, jota ”sovelletaan” siihen ongelmaan, että funktion e^{-x^2} integraalifunktiot eivät ole alkeisfunktioita. Lopuksi esitetään lisää tähän ongelmaan liittyvää kirjallisuutta.

Meromorfitiset funktiot

Tässä artikkelissa oletetaan, että kompleksilukujen kunta

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$$

on jonkin verran tuttu. Tässä i on niin sanottu *imaginaariyksikkö*, jolle pätee $i^2 = -1$. Vaikka meidän alkuperäinen ongelmamme koskee reaaliuuttujan funktiota e^{-x^2} , on itse asiassa hyödyllistä tutkia kompleksimuuttujan kompleksiarvoisia funktioita. Sellaisia funktioita tutkitaan funktioteoriassa eli kompleksianalyysissä.

Huomautus 4. Käytämme heti kompleksilukuja hyväksemme huomaten, että trigonometriset funktiot ja niiden käänteisfunktiot voidaan poistaa Määritelmässä 1 olevasta alkeisfunktioiden listasta. Eulerin kaavalla $e^{iz} = \cos z + i \sin z$ on helppo todistaa, että jokaisella kompleksiluvulla $z \in \mathbb{C}$ pätee

$$\cos z = \frac{e^{iz} + e^{-iz}}{2} \quad \text{ja} \quad \sin z = \frac{e^{iz} - e^{-iz}}{2i}.$$

Myös muut trigonometriset funktiot ja niiden käänteisfunktiot voidaan kirjoittaa eksponentti- ja logaritmifunktioiden avulla, esimerkiksi

$$\arcsin z = -i \ln(iz + \sqrt{1 - z^2}).$$

Ks. esimerkiksi kirjan [7] Luku II.

Toinen pääpointti on se, että kompleksilukujen joukossa $\mathbb{C}$ millä tahansa m -asteisella kompleksikertoimisella polynomilla on m juurta. Tämä on algebrallisempi fakta, ja sitä käytetään artikkelin toisessa osassa. Nyt jatketaan analyysin parissa.

Määritelmä 5. Kompleksimuuttujan kompleksiarvoiselle funktiolle f ja kompleksiluvulle z_0 määritellään derivaatta samalla tavalla kuin reaalitapauksessa:

$$f'(z_0) = \lim_{z \rightarrow z_0} \frac{f(z) - f(z_0)}{z - z_0},$$

missä z voi lähestyä kompleksilukua z_0 kuinka tahansa kompleksitasossa. Funktiota f sanotaan **holomorfin** **seksi pisteessä** z_0 , jos f on derivoituva (eli derivaatta on olemassa (äärellisenä!)) jonkin pisteen z_0 ympäristön jokaiselle pisteelle.¹

¹Esimerkiksi kirjassa [7] käytetään sanaa ”säännöllinen” sanan ”holomorfinen” sijaan. Joskus käytetään myöskin sanaa ”analyytinen” synonyymina.

Esimerkiksi polynomit, eksponenttifunktio, sini ja kosini ovat holomorfisia funktioita koko kompleksitasossa. Kompleksiderivaatta toteuttaa samanlaisia ehtoja kuin reaaliderivaatta, esimerkiksi $(f + g)' = f' + g'$ ja $(fg)' = f'g + fg'$. Toisaalta kompleksitapauksessa paljon enemmän pätee kuin reaalissa. (Ks. kirjan [7] Luku I.)

Määritelmä 6. *Meromorfinen funktio on kompleksiarvoinen funktio, joka on määritelty kompleksitason avoimessa osajoukossa U ja on holomorfinen joukossa U paitsi mahdollisessa osajoukossa, joka koostuu eristetyistä pisteistä.*

Seuraavaksi kootaan hyvin tuttuja faktoja (ks. [4, 7]):

- Meromorfinen funktio voidaan aina esittää kahden holomorfinen funktion osamääränä. Ja toisinpäin kahden holomorfinen funktion osamäärä

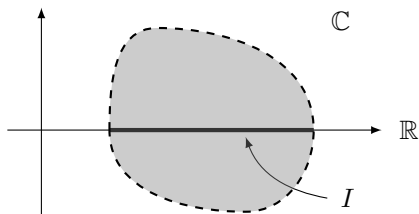
$$m(x) = \frac{f(x)}{g(x)},$$

jossa $g(x) \neq 0$, on meromorfinen.

- Jos f ja g ovat eri meromorfit, niin joukko $\{z \in \mathbb{C} \mid f(z) = g(z)\}$ koostuu eristetyistä pisteistä. Varsinkin siinä tapauksessa, että $f(x) = g(x)$ jokaisella alkiolla x jossain reaalivälissä I (kuten Määritelmässä 7), niin $f = g$.

Lopuksi meidän tutkituin funktiolajimme tässä kirjoituksessa:

Määritelmä 7. *Olko I reaaliväli ja olko f kompleksiarvoinen funktio, joka on määritelty välissä I paitsi mahdollista joukkoa erillisiä pisteitä. Silloin f :ää sanotaan **reaalisesti meromorfiseksi funktioksi**, jos f on jonkin (standardi)meromorfinen funktion g rajoittuma väliin I , missä g on määritelty jossain välin I kompleksiympäristössä.*



Kunnat (ja renkaat)

Kunta on algebrallinen rakenne, jota käytetään monella matematiikan alalla.

Määritelmä 8. *Kunta on joukko $\mathbb{K}$, jossa määritellään kaksi sellaista laskutoimitusta $+$ ja $\cdot$, että:*

- $+$ ja $\cdot$ ovat assosiatiivisia, eli jokaisille alkiolle $a, b, c \in \mathbb{K}$ pätee $(a + b) + c = a + (b + c)$ ja $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,

- $+$ ja $\cdot$ ovat vaihdannaisia, eli jokaisille alkiolle $a, b \in \mathbb{K}$ pätee $a + b = b + a$ ja $a \cdot b = b \cdot a$,
- distributiivisuus pätee, eli $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ kaikille $a, b, c \in \mathbb{K}$,
- on olemassa neutraali-alkio 0 laskutoimitukselle $+$ ja neutraali-alkio $1 \neq 0$ laskutoimitukselle $\cdot$, eli $0 + a = a$ ja $1 \cdot a = a$ kaikille $a \in \mathbb{K}$,
- jokaiselle alkiolle a on olemassa sellainen alkio $-a$, että $(-a) + a = 0$,
- jokaiselle alkiolle $a \neq 0$ on olemassa sellainen käänteisalkio $\frac{1}{a}$, että $\frac{1}{a} \cdot a = 1$.

Meidän pitäisi itse asiassa täsmällisemmin sanoa, että kunta on tripla $(\mathbb{K}, +, \cdot)$, mutta laskutoimitukset $+$ ja $\cdot$ ymmärretään tavallisesti kontekstista, ja siksi kirjoitamme vain "kunta $\mathbb{K}$ ". Tässä kirjoituksessa summa ja kertolasku ovat aina "tavalliset" summa ja kertolasku, luvuille tai funktioille.

Esimerkki 9. 1. $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$ on rationaalilukujen kunta.

2. $\mathbb{R}$ on reaalilukujen kunta, joka sisältää kunnan $\mathbb{Q}$. Esimerkiksi π ja e kuuluvat kuntaan $\mathbb{R}$, mutteivät kuntaan $\mathbb{Q}$.

3. $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}$ on kompleksilukujen kunta, joka sisältää kunnan $\mathbb{R}$.

4. Joukko $\mathbb{Z}_2 = \{0, 1\}$ on pienin mahdollinen kunta, jos määritellään laskutoimitukset näin:

$+$	0	1	$\cdot$	0	1
0	0	1	0	0	0
1	1	0	1	0	1

5. Olkoot I reaaliväli ja $\mathbb{K}$ kunta reaalisesti meromorfinen funktioita (ks. Määritelmä 7). Jatkoa tällaista kuntaa $\mathbb{K}$ sanotaan **kunnaksi meromorfinen funktioita välissä I** .

Kokonaisluvut $\mathbb{Z}$ eivät muodosta kuntaa: viimeinen ehto kunnan määritelmässä ei pidä paikkaansa, koska ainoat alkiot, joille on olemassa käänteisalkio, ovat 1 ja -1 . Kaikki muut ehdot kuitenkin pätevät, ja triplaa $(\mathbb{Z}, +, \cdot)$ kutsutaan **(vaihdannaiseksi) renkaaksi**. Rengas on siis kunnan yleistys. Samalla tavalla reaalikertoimiset polynomit toteuttavat kaikki kunnan ehdot paitsi viimeistä, ja siksi nekin ovat rengas, jota merkitään symbolilla $\mathbb{R}[x]$.

Siinä tapauksessa, että osaat vähän matriisilaskentaa: neliömatriisit muodostavat epävaihdannaisen renkaan (eli kertolaskun vaihdannaisuus ei päde), mutteivät kuntaa.

Polynomit ja rationaalifunktiot

Määritelmä 10. Olkoon R vaihdannainen rengas. Tällöin R -kertoiminen polynomi on jokin, joka näyttää tältä:

$$a_d X^d + a_{d-1} X^{d-1} + \cdots + a_2 X^2 + a_1 X + a_0,$$

missä $a_0, \dots, a_d \in R$ kutsutaan **kertoimiksi**. Tällaisen polynomien joukkoa (itse asiassa rengasta) merkitään symbolilla $R[X]$.

Jos et ole tyytyväinen tähän ”määritelmään”, voit tarkistaa kirjan [3] pykälän 21.2. Ymmärtääksesi yksityiskohdat paremmin voit myös yrittää todistaa, että jos R on vaihdannainen rengas, niin on $R[X]$ myöskin.

Määritelmä 11. Jos P on polynomi

$$a_d X^d + a_{d-1} X^{d-1} + \cdots + a_2 X^2 + a_1 X + a_0$$

ja $a_d \neq 0$, luonnollista lukua d kutsutaan polynomin P **asteeksi** (engl. degree) ja sitä merkitään symbolilla $\deg(P)$. Jos $\deg(P) = 0$ eli $P = a_0 \neq 0$, niin polynomia P kutsutaan **vakio(polynomi)ksi**. Nollapolynomille (eli sille polynomille, jonka kaikki kertoimet ovat nolla) emme määrittele astetta tässä kirjoituksessa, vaikka sitäkin sanotaan vakioksi.

Esimerkiksi $\deg(X^2 + 1) = 2$ ja $\deg(X^4 - X^3) = 4$.

Kokonaislukujen jakoyhtälö on varmaan tuttu: kokonaisluvuille a ja b on olemassa yksikäsitteiset q ja r niin, että voidaan kirjoittaa $a = qb + r$ ja $0 \leq r < |b|$. Lukua r kutsutaan **jakojäännökseksi** (engl. remainder). Käyttämällä tätä lausetta uudestaan ja uudestaan voi laskea lukujen a ja b suurimman yhteisen tekijän, ja tätä prosessia kutsutaan *Eukleideen algoritmiksi*.

Samalla tavalla huomioi, että voidaan jakaa polynomi P polynomilla Q , eli löytää sellainen jakoyhtälö

$$P = UQ + V,$$

jossa $\deg(V) < \deg(Q)$ tai $V = 0$, ja laskea sillä kahden polynomin suurin yhteinen tekijä $\text{syt}(P, Q)$. (Ks. kirjan [3] pykälät 7 ja 22.)

Jatkossa käytämme seuraavaa kuuluisaa lausetta.

Lause 12 (Bézout’n yhtälö). Olkoot $\mathbb{K}$ kunta, $P, Q \in \mathbb{K}[X]$ kaksi polynomia ja $M = \text{syt}(P, Q)$. Silloin on olemassa kaksi sellaista polynomia $S, T \in \mathbb{K}[X]$, että

$$PS + QT = M,$$

$\deg S < \deg Q - \deg M$, $\deg T < \deg P - \deg M$ tai $S = 0$ tai $T = 0$.

Esimerkiksi jos $P = X^2 - 1$ ja $Q = X^4 - X^3$, niin niiden suurin yhteinen tekijä renkaassa $\mathbb{R}[X]$ on $M = X - 1$. Voidaan kirjoittaa

$$(X^2 - 1)(X^2 - X + 1) + (X^4 - X^3)(-1) = X - 1,$$

eli $S = X^2 - X + 1$ ja $T = -1$.

Määritelmä 13. Olkoon R vaihdannainen rengas. Tällöin R -kertoiminen **rationaalifunktio** on kahden R -kertoimisen polynomin osamäärä, eli

$$f(X) = \frac{P(X)}{Q(X)}, \quad P, Q \in R[X], \quad Q \neq 0.$$

Rationaalifunktioiden joukkoa (itse asiassa kuntaa) merkitään symbolilla $R(X)$.

Polynomi Q ei siis ole nollapolynomi, mutta voi kyllä olla, että jollakin $r \in R$ pätee $Q(r) = 0$. Jos $P \neq 0$, niin rationaalifunktion $\frac{P}{Q}$ käänteisalkio on $\frac{Q}{P}$.

Huomautus 14. Renkaan R alkioita r voidaan ajatella vakio-polynomina, ja polynomia $P \in R[X]$ voidaan ajatella triviaalina rationaalifunktiona $\frac{P}{1}$. Meillä on siis inklusiot

$$R \subset R[X] \subset R(X).$$

Esimerkiksi $\mathbb{R} \subset \mathbb{R}[X] \subset \mathbb{R}(X)$ ja $\mathbb{C} \subset \mathbb{C}[X] \subset \mathbb{C}(X)$.

Kuntalaajennukset, algebralliset ja transkendentit alkio

Määritelmä 15. Kunnan $\mathbb{K}$ (kunta)laajennus on sellainen kunta $\mathbb{L}$, että $\mathbb{K} \subseteq \mathbb{L}$ ja kunnan $\mathbb{K}$ laskutoimitukset ovat samat kuin kunnassa $\mathbb{L}$.

Esimerkki 16. 1. Esimerkiksi $\mathbb{C}$ on kunnan $\mathbb{R}$ laajennus, ja $\mathbb{R}$ on kunnan $\mathbb{Q}$ laajennus. Siten $\mathbb{C}$ on myös kunnan $\mathbb{Q}$ laajennus.

2. Rationaalifunktioiden kunta $\mathbb{K}(X)$, jossa $\mathbb{K}$ on mikä tahansa kunta, on kunnan $\mathbb{K}$ laajennus.

Tässä kirjoituksessa tärkeimmät kunnat koostuvat funktioista. Mutta seuraavat määritelmät sopivat yleisimmille kunnille.

Määritelmä 17. Olkoot $\mathbb{K}$ kunta ja $\mathbb{L} \supseteq \mathbb{K}$ kuntalaajennus. Olkoon $\alpha \in \mathbb{L}$.

- Alkiota α kutsutaan **algebralliseksi alkioksi kunnan $\mathbb{K}$ suhteen**, jos on olemassa sellainen epäolopoliinomi $Q \in \mathbb{K}[X]$, että $Q(\alpha) = 0$. Tässä tapauksessa voidaan todistaa, että on olemassa yksikäsitteinen pienimmän asteen polynomi $P \in \mathbb{K}[X]$, jonka korkeimman asteen termin kerroin on 1 siten, että $P(\alpha) = 0$. Tätä polynomia P kutsutaan alkion α **minimipolynomiksi kunnan $\mathbb{K}$ suhteen**.

- Alkiota α kutsutaan **transkendenttiseksi alkioksi kunnan $\mathbb{K}$ suhteen**, jos α ei ole algebrallinen, toisin sanoen jos ainoa polynomi $Q \in \mathbb{K}[X]$, jolle pätee $Q(\alpha) = 0$, on nollapolynomi $Q \equiv 0$.

Esimerkki 18. 1. Otetaan laajennus $\mathbb{R} \subset \mathbb{C}$. Kompleksiluku i on algebrallinen kunnan $\mathbb{R}$ suhteen, koska polynomi $Q = X^2 + 1 \in \mathbb{R}[X]$ toteuttaa $Q(i) = 0$.

2. Otetaan laajennus $\mathbb{Q} \subset \mathbb{R}$. Irrationaaliluku $\sqrt{2}$ on algebrallinen kunnan $\mathbb{Q}$ suhteen, koska polynomi $Q = X^2 - 2 \in \mathbb{Q}[X]$ toteuttaa $Q(\sqrt{2}) = 0$.

3. Triviaalitapauksessa $\mathbb{L} = \mathbb{K}$ jokainen kunnan $\mathbb{K}$ alkio α on algebrallinen sen sisältävän kunnan suhteen, koska polynomi $Q = X - \alpha \in \mathbb{K}[X]$ toteuttaa $Q(\alpha) = 0$.

Kaikissa yllä olevissa esimerkeissä annettu polynomi Q on itse asiassa minimipolynomi.

4. Lindemann ja Hermite todistivat, että reaaliuvut π ja e ovat transkendenttisia kunnan $\mathbb{Q}$ suhteen. Ei ole olemassa mitään polynomia $Q \in \mathbb{Q}[x]$ siten, että $Q(\pi) = 0$ tai $Q(e) = 0$.

Kunnan $\mathbb{K}$ laajennus $\mathbb{K}(\alpha)$

Määritelmä 19. Olkoot $\mathbb{K}$ kunta ja $\alpha \in \mathbb{L} \setminus \mathbb{K}$. Määritellään nyt kunnan $\mathbb{L}$ pienin alikunta $\mathbb{K}(\alpha)$, joka sisältää sekä kunnan $\mathbb{K}$ että ”uuden” alkion α .

- Jos α on algebrallinen kunnan $\mathbb{K}$ suhteen, olkoon $P \in \mathbb{K}[X]$ sen minimipolynomi ja $m := \deg P$. Silloin $m > 1$, tai muuten α olisi kunnan $\mathbb{K}$ alkio. Määritellään

$$\mathbb{K}(\alpha) := \{Q(\alpha) \mid Q \in \mathbb{K}[X], \deg Q \leq m-1\}.$$

Huomioi, että jokaisella alkiolla $b \in \mathbb{K}(\alpha)$ on sellainen yksikäsitteinen polynomi Q , että $Q(\alpha) = b$ ja $\deg Q \leq m-1$. Tai muuten, jos olisi olemassa kaksi eri sellaista polynomia Q ja T , niin

$$(Q - T)(\alpha) = Q(\alpha) - T(\alpha) = b - b = 0,$$

mutta $\deg(Q - T) \leq m-1$, ja tämä on ristiriita sen kanssa, että m on minimipolynomin aste. Siten $Q = T$. Seuraavassa tehtävässä 21 merkitään alkion $b \in \mathbb{K}(\alpha)$ polynomia Q symbolilla Q_b , eli

$$Q_b(\alpha) = b.$$

Meidän pitää vielä määritellä summa ja kertolasku. Alkioiden $Q(\alpha)$ ja $T(\alpha)$ summa on yksinkertaisesti

$$Q(\alpha) + T(\alpha) = (Q + T)(\alpha)$$

kunnan $\mathbb{L}$ alkiona. Tätä varten huomioi, että $\deg(Q + T) \leq m-1$. Jos otetaan polynomit Q ja T , joiden asteet ovat korkeintaan $m-1$, ei voida määritellä heti kertolaskua $Q(\alpha)T(\alpha) = (QT)(\alpha)$, koska voi olla, että $\deg(QT) \geq m$. Jaetaan ensin alkion α minimipolynomilla P : olkoon

$$QT = UP + V$$

sellainen jakoyhtälö, jossa $\deg(V) \leq m-1$ tai $V = 0$. Nyt määritellään

$$Q(\alpha)T(\alpha) := V(\alpha).$$

- Jos α on transkendenttinen kunnan $\mathbb{K}$ suhteen, määritellään

$$\mathbb{K}(\alpha) := \left\{ \frac{P(\alpha)}{Q(\alpha)} \mid P, Q \in \mathbb{K}[X] \right\}.$$

Operaatiot toimivat tässä intuition mukaan.

Huomautus 20. Molemmissa tapauksissa $\mathbb{K}(\alpha)$ on pienin kunta, joka sisältää sekä kunnan $\mathbb{K}$ että alkion α . Lisäksi kunnan $\mathbb{K}$ laskutoimitukset ovat samat kuin kunnassa $\mathbb{K}(\alpha)$.

Tehtävä 21. Todista, että $\mathbb{K}(\alpha)$ on todellakin kunta, kun α on algebrallinen alkio kunnan $\mathbb{K}$ suhteen.

Vihje: Olkoot $a, b \in \mathbb{K}(\alpha)$ ja $Q_a, Q_b \in \mathbb{K}[X]$ niiden vastaavat polynomit. On helppo osoittaa, että $a+b \in \mathbb{K}(\alpha)$. Olkoon P alkion α minimipolynomi. Jos $\deg(Q_a Q_b) > \deg(P)$, kirjoita

$$Q_a Q_b = \tilde{Q}P + T$$

joillakin polynomeilla $\tilde{Q}$ ja T , joille pätee $\deg(T) < \deg(P)$. Kun pitää todistaa, että jokainen epänolla alkio on kääntyvä, huomioi, että koska $\deg(Q) < \deg(P)$ ja P on jaoton, $\text{syt}(P, Q) = 1$. Lauseen 12 avulla kirjoita $PS + QT = 1$ joillakin polynomeilla S ja T .

Esimerkki 22. 1. $\mathbb{R} \subsetneq \mathbb{R}(i) = \mathbb{C}$.

2. $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{2}) \subsetneq \mathbb{R}$.

3. Notatio $\mathbb{K}(X)$ rationaalifunktioiden kunnalle on itse asiassa järkevä kuntalaajennuksien kannalta: X on jokin ”uusi” transkendenttinen alkio, joka lisätään saaden laajennus $\mathbb{K}(X)$.

Tehtävä 23. Käy määritelmä läpi ja osoita, että $\mathbb{R}(i) = \mathbb{C}$. Miten kompleksiluvun $a + bi$ käänteisalkio kirjoitetaan muodossa $c + di$, jossa $c, d \in \mathbb{R}$? Samalla tavalla, miten kunnan $\mathbb{Q}(\sqrt{2})$ alkion $a + b\sqrt{2}$ käänteisalkio kirjoitetaan muodossa $c + d\sqrt{2}$, jossa $c, d \in \mathbb{Q}$?

Liouvillen lauseen väite

On aika yhdistää algebraa ja analyysia.

Muistetaan, että Määritelmässä 7 ja Esimerkissä 9 tuli esiin funktioita, jotka määritellään reaalivälissä I ja ovat rajoittumia joistain funktioista, jotka ovat meromorfisia jossain välin I kompleksiympäristössä. Sellaisista funktioista koostuu kunta $\mathbb{K}$ jatkossa.

Määritelmä 24. Olkoot nyt I reaaliväli ja $\mathbb{K}$ kunta, joka koostuu funktioista, jotka ovat meromorfisia välissä I . Olkoon funktio f meromorfinen funktio jossain välin I osavälissä J . Funktiota f kutsutaan

- **eksponenttifunktioksi** (kunnan $\mathbb{K}$ suhteen), jos on olemassa funktio $g \in \mathbb{K}$, joka on määritelty välissä J ja jolle pätee

$$f' = g'f,$$

- **logaritmifunktioksi** (kunnan $\mathbb{K}$ suhteen), jos on olemassa funktio $g \in \mathbb{K}$, joka on määritelty välissä J , jossa se on aina epänulla, ja jolle pätee

$$f' = g'/g.$$

Huomautus 25. ”Tavalliset” eksponentti- ja logaritmifunktiot ovat tietysti eksponentti- ja logaritmifunktiot tämän ”algebrallisen” määritelmän mukaan. Sen pääpointti on, että ainoat eksponentti- ja logaritmifunktion ominaisuudet, joita käytetään Liouvillen lauseen todistuksessa, ovat juuri ne, jotka ovat yllä olevassa määritelmässä.

Määritelmä 26. Kunta $\mathbb{K}$ meromorfisia funktioita on **derivaatan suhteen suljettu**, jos jokaisen funktion $f \in \mathbb{K}$ derivaatta kuuluu kuntaan $\mathbb{K}$.

Lemma 27. Olkoon $\mathbb{K}$ derivaatan suhteen suljettu kunta meromorfisia funktioita, ja olkoon f joko algebrallinen funktio tai eksponentti- tai logaritmifunktio. Silloin laajennus $\mathbb{K}(f)$ on derivaatan suhteen suljettu.

Todistus. Periaatteessa pitää todistaa, että jokaisen funktion $h \in \mathbb{K}(f)$ derivaatta h' kuuluu laajennukseen $\mathbb{K}(f)$. Mutta koska h voidaan kirjoittaa funktion f polynomina tai rationaalifunktiona, riittää todistaa, että f' kuuluu laajennukseen $\mathbb{K}(f)$. Jos f on eksponentti- tai logaritmifunktio, tämä on helppo tarkistaa. Olkoon siis f algebrallinen, mikä tarkoittaa, että on olemassa minimipolynomi

$$P = a_0 + a_1X + \cdots + a_mX^m = \sum_{i=0}^m a_iX^i$$

funktiolle f . Silloin $P(f) = 0$. Ota derivaatta saaden

$$f' \sum_{i=1}^m ia_i f^{i-1} + \sum_{i=0}^m a'_i f^i = 0.$$

Osoita, ettei $\sum_{i=1}^m ia_i f^{i-1}$ ole nollapolynomi, joten voit kirjoittaa

$$f' = - \frac{\sum_{i=0}^m a'_i f^i}{\sum_{i=1}^m ia_i f^{i-1}}$$

ja päätellä, että $f' \in \mathbb{K}(f)$. $\square$

Määritelmä 28. Olkoon $\mathbb{K}$ kunta meromorfisia funktioita. Kunnan $\mathbb{K}$ laajennusta $\mathbb{L}$ kutsutaan **alkeislaajennukseksi**, jos on olemassa sellaiset funktiot $f_1, \dots, f_n$, että jos merkitään

$$\begin{aligned} \mathbb{K}_0 &:= \mathbb{K}, \\ \mathbb{K}_{i+1} &:= \mathbb{K}_i(f_{i+1}), \quad i = 0, \dots, n-1, \end{aligned}$$

niin f_{i+1} on joko algebrallinen funktio tai eksponentti- tai logaritmifunktio kunnan $\mathbb{K}_i$ suhteen, ja $\mathbb{K}_n = \mathbb{L}$. Funktiota f kutsutaan **alkeisfunktioksi**, jos f kuuluu johonkin kunnan $\mathbb{C}(x)$ alkeislaajennukseen.

Toisin sanoen, ehkä eksplisiittisemmin, yllä olevassa määritelmässä on kuntalaajennuksien ”ketju”

$$\mathbb{K} = \mathbb{K}_0 \subseteq \mathbb{K}_1 \subseteq \mathbb{K}_2 \subseteq \cdots \subseteq \mathbb{K}_{n-1} \subseteq \mathbb{K}_n = \mathbb{L}.$$

Lisäksi muistetaan, että huomautuksessa 4 sanottiin, että

$$\cos z = \frac{e^{iz} + e^{-iz}}{2}, \quad \sin z = \frac{e^{iz} - e^{-iz}}{2i},$$

ja myös muut trigonometriset funktiot ja niiden käänteisfunktiot voidaan kirjoittaa eksponentti- ja logaritmifunktioiden termeistä.

Lause 29 (Liouville). Olkoot $\mathbb{K}$ derivaatan suhteen suljettu kunta meromorfisia funktioita ja $\alpha \in \mathbb{K}$. Seuraavat ehdot ovat yhtäpitävät:

- On olemassa kunnan $\mathbb{K}$ alkeislaajennus $\mathbb{L}$ ja sellainen $y \in \mathbb{L}$, että $y' = \alpha$.
- On olemassa sellaiset $u_1, \dots, u_n, v \in \mathbb{K}$ ja $c_1, \dots, c_n \in \mathbb{C}$, että

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

Artikkelissa [6] Rosenlicht kirjoitti:

Thus the original loosely worded analytic problem, when formulated as a precise analytic problem, becomes algebraic.

Liouvillen lauseen sovelluksia

Artikkelin toisessa osassa todistamme sekä Liouvillen lauseen että seuraavan.

Lause 30. Olkoot $f, g \in \mathbb{C}(x)$, missä f ei ole nolla eikä g ole vakio, määriteltyt jossakin reaalivälissä J . Silloin 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

$$f = a' + ag'.$$

Tässä ensimmäisessä osassa todistamme vain sen, että edellisestä lauseesta seuraa seuraava.

Seuraus 31. Funktiolla e^{-x^2} ei ole alkeisintegraalifunktioita.

Todistus. Tässä tapauksessa Lauseen 30 funktiot f ja g ovat $f(x) = 1$ ja $g(x) = -x^2$. Oletetaan, että on olemassa sellainen rationaalifunktio $a \in \mathbb{C}(x)$, että $f = a' + ag'$, eli

$$1 = a'(x) - 2xa(x). \quad (1)$$

Kirjoitetaan $a(x) = \frac{P(x)}{Q(x)}$, missä $P, Q \in \mathbb{C}[x]$ ovat keskenään jaottomat, mikä voidaan tehdä, jos Q ei ole vakiopolynomi. Yhtälöstä (1) tulee sitten

$$\frac{P'(x)Q(x) - P(x)Q'(x)}{Q(x)^2} - 2x \frac{P(x)}{Q(x)} = 1,$$

mistä seuraa, että

$$P'(x)Q(x) - P(x)Q'(x) - 2xP(x)Q(x) = Q(x)^2,$$

ja järjestämällä oikealle puolelle kaikki termit, joissa Q esiintyy, saadaan että Q jakaa polynomin PQ' . Mutta koska P ja Q ovat keskenään jaottomat, Q jakaa polynomin Q' . Tästä seuraa, että $\deg Q' \geq \deg Q$, mikä on mahdollista vain, jos Q on vakiopolynomi. Rationaalifunktion $a = \frac{P(x)}{Q(x)}$ pitää siis olla polynomi. Yhtälöstä (1) tulee $P'(x) - 2xP(x) = 1$, eli

$$2xP(x) = P'(x) - 1. \quad (2)$$

Polynomi P ei voi olla nollapolynomi, tai muuten $0 = -1$. Olkoon sitten $m = \deg(P) > 0$. Yhtälön (2) vasemman puolen polynomin aste on $m+1$, mutta oikean puolen polynomin aste on varmasti sitä pienempi. Tämä on ristiriita. $\square$

Tehtävä 32. Osoita, ettei seuraavilla funktioilla ole alkeisintegraalifunktioita: e^{x^2} , e^x/x , e^{e^x} , $1/\log x$, $\log(\log x)$. Vihje: Osoita, että

$$\int \frac{e^x}{x} dx = \int e^{e^t} dt = \int \frac{1}{\log u} du$$

ja

$$\int \log(\log x) dx = x \log(\log x) - \int \frac{1}{\log x} dx.$$

Lisää kirjallisuutta

Ensimmäinen, joka todisti tämän kirjoituksen päätöksen, oli Liouville artikkelissa [5] (ranskaksi). Opin itse tästä teemasta artikkeleista [2] (italiaksi) ja [6] (englanniksi). Tämä kirjoitus on enimmäkseen artikkelin [2] inspiroima.

Tämän kirjoituksen pointtina (erityisesti toisessa osassa) on, kuinka paljon algebraa käytetään analyttisessä ongelmassa. Jos aiot lukea enemmän algebrasta, kirja [3] (suomeksi) on todella ystävällinen johdatus. Toisaalta jos kiinnostavat esimerkiksi vaikeat yksityiskohdat kuntalaaajennuksista, niin suositellaan kirjan [1] lukua 15. Tässä kirjoituksessa käytettiin myös vähän kompleksianalyysia, ja siitä voi lukea suomeksi erinomaisista klassikoista [4, 7].

Viitteet

- [1] M. Artin. *Algebra, Second Edition*. Pearson Education Asia Ltd. (2014).
- [2] 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.
- [3] J. Hästö, J. Rämö. *Johdatus abstraktiin algebraan*. Gaudeamus (2015).
- [4] E. Lindelöf. *Johdatus funktioteoriaan*. Helsinki (1936).
- [5] J. Liouville. *Mémoire sur les Transcendentes Elliptiques et sur l'impossibilité d'exprimer les racines de certaines équations en fonction finie explicite des coefficients*. J Math. Pures Appl. 2 pp. 124–193 (1837).
- [6] M. Rosenlicht. *Integration in finite terms*. Amer. Math. Monthly **79** (9) pp. 963–972 (1972).
- [7] K. Väisälä. *Matematiikka IV. Jälkimmäinen osa*. Teknillinen korkeakoulu. Moniste n:o 141 (1956).