



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 merkin $\mathbb{K}(\alpha)(\beta)$ 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 määritelty, 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! Esi-merkiksi rationaalifunktiolla $\frac{1}{x}$ ei ole integraalifunktiota kunnassa $\mathbb{C}(x)$, mutta kyllä on laajennuksessa $\mathbb{C}(x)(\ln x) = \mathbb{C}(x, \ln x)$.

Liouvilien lauseen implikaation ” $\Rightarrow$ ” todistus tulee olemaan melko pitkä ja tehdään eri tapauksissa. Ensin kerätään paljon apulauseita seuraavassa luvussa. Liouvilien 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.

Meromorfin funktion poolit

Määritelmä 5. Olkoot f ja g holomorfin funktiona jossain kompleksitason avoimessa osajoukossa U . Meromorfin 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 meromorfin 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. Olkoot $\mathbb{K}$ 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 epävakioilla 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. *Olko 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. $\square$

Olko $m \in \mathbb{Z}_{>0}$. Kirjoittamalla jatkossa $\mathbb{C}_w^m$ tarkoittamme, 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). *Olko $m, n \in \mathbb{Z}_{>0}$ ja $\mathcal{A}$ tulon $\mathbb{C}^{n+m} = \mathbb{C}_z^n \times \mathbb{C}_w^m$ avoin joukko. Olko $F = (F_1, \dots, F_n): \mathcal{A} \rightarrow \mathbb{C}^n$ holomorfinen funktio. Olko $(z^0, w^0) = (z_1^0, \dots, z_n^0, w_1^0, \dots, w_m^0) \in \mathcal{A}$ 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 kääntyvä. 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. *Olko $\mathbb{K}$ kunta meromorfisia funktioita reaalivälissä I ja olko $P \in \mathbb{K}[X]$ m -asteinen jaoton polynomi. Tällöin jollekin osavälille $J \subseteq I$ on olemassa sellaiset pareittain erilliset meromorfiset 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 $i \in \{1, \dots, m\}$.

Olko 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^3y .

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

$$\begin{aligned} s_1 &:= x_1 + x_2 + \dots + x_n, \\ s_2 &:= x_1x_2 + x_1x_3 + \dots + x_{n-1}x_n, \\ &\vdots \\ s_n &:= x_1x_2 \dots x_n. \end{aligned}$$

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 peruspolut 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 parittain 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

$$\begin{aligned} P(X) &= (X - z_1)(X - z_2) \dots (X - z_m) \\ &= X^m - a_1X^{m-1} + a_2X^{m-2} - \dots \pm a_m \end{aligned}$$

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' alkioiden 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 meromorfisia 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 yhtälösä (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, jotta 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 $a'_i mb' = ia_i b' + a'_i$, 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

$$L := V_1^{m_1+1} \dots V_N^{m_N+1} M_{i_1} \dots M_{i_s},$$

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

$$\frac{\mathcal{P}(f_1)}{V_1^{m_1}(f_1) V_2^{m_2+1}(f_1) \dots V_N^{m_N+1}(f_1) M_{i_1}(f_1) \dots M_{i_s}(f_1)}$$

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

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

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

$$\cdot V_2^{m_2+1}(f_1) \dots V_N^{m_N+1}(f_1)$$

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

Koska f_1 on transkendenttinen, Lemmasta 7 seuraa, että

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

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 $v := \frac{1}{m} S(z_1, \dots, z_k) = \frac{1}{m} \sum_{k=1}^m Q(z_k)$ 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, määriteltyt 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

$$S_0(X) = s_1 X + s_0$$

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

$$\begin{aligned} f e^g &= \sum_{i=1}^N c_i \frac{u'_i}{u_i} + (s_1 e^g + s_0)' + \varepsilon_1 g' \\ &= \sum_{i=1}^N c_i \frac{u'_i}{u_i} + s'_1 e^g + s_1 g' e^g + s'_0 + \varepsilon_1 g'. \end{aligned}$$

Kirjoittamalla eri tavalla saamme

$$(f - s'_1 - s_1 g') e^g = \sum_{i=1}^N c_i \frac{u'_i}{u_i} + s'_0 + \varepsilon_1 g',$$

missä oikea puoli ei sisällä funktiota e^g . Jos funktion e^g kerroin vasemmalla puolella olisi epänolla, saisimme ristiriidan transkendenttisuuden kanssa, joten $f - s'_1 - s_1 g' = 0$ eli

$$f = s'_1 + s_1 g'.$$

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 differentiaali-algebra (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.