ALGEBRALLISTEN FUNKTIOKUNTIEN ζ-FUNKTIOT

Katsaus Riemannin ζ-funktioon

Klassinen Riemannin ζ-funktio määritellään sarjana

$$\zeta(s) = \sum_{n=0}^{\infty} \frac{1}{n^s}. \tag{1}$$

Tälle voidaan johtaa Eulerin tuloesitys

$$\zeta(s) = \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{1}{p^s}}. \tag{2}$$

Riemannin ζ-funktion määrittelevät sarja (1) ja tulo (2) suppenevat, kun $\mathrm{Re}s > 1$, mutta ζ-funktio voidaan jatkaa koko kompleksitasoon meromorfifunktioksi, jolla on ainoa napa pisteessä $s = 1$ ja siinä residy 1.

Riemannin ζ-funktiolla on triviaalit nollakohdat pisteissä $s = -2, -4, -6, \ldots$, mutta ei muita nollakohtia puolitasossa $\mathrm{Re}s < 0$ eikä lainkaan nollakohtia puolitasossa $\mathrm{Re}s > 1$. Kuuluisan, yhä todistamattoman Riemannin hypoteesin mukaan vyöhykkeessä $0 \leq \mathrm{Re}s \leq 1$ olevat nollakohdat sijaitsevat suoralla $\mathrm{Re}s = \frac{1}{2}$. Riemannin ζ-funktion nollakohtien määrämisellä on mittava merkitys alkulukujen jakautumisen teoriassa; ζ-funktion nollakohdat määräävät täydellisesti alkulukujen jakautumisen.

Riemannin ζ-funktion välitön yleistys algebralliselle lukukunnalle F on Dedekindin ζ-funktio, joka määritellään sarjana

$$\zeta_F(s) = \sum_{\mathfrak{A}} \frac{1}{\mathrm{N}(\mathfrak{A})^s}. \tag{3}$$

Myös tälle saadaan tuloesitys

$$\zeta_F(s) = \prod_{\mathfrak{P}} \frac{1}{1 - \frac{1}{\mathrm{N}(\mathfrak{P})^s}}. \tag{4}$$

Summassa (3) $\mathfrak{A}$ käy läpi kaikki lukukunnan F kokonaiset ihanteet ja tulossa (4) $\mathfrak{P}$ käy kaikki alkuihanteet. Summassa ja tulossa esiintyy *ihanteen normi*, joka määritellään seuraavasti:

$$\mathrm{N}(\mathfrak{A}) = |\mathcal{O}/\mathfrak{A}|. \tag{5}$$

Ylläolevassa merkinnässä $\mathcal{O}$ on lukukunnan kokonaislukujen rengas. Kun asetetaan $F = \mathbb{Q}$, saadaan erikoistapauksena klassinen Riemannin ζ-funktio. Riemannin hypoteesi algebrallisten lukukuntien ζ-funktioille on myös edelleen avoin probleema.

Funktiokunnat yli äärellisten kuntien.

Olkoon $\mathbb{F}_q$ kertalukua q oleva äärellinen kunta ja $\mathcal{F} = F/\mathbb{F}_q$ sukua g oleva funktiokunta. Olkoon vielä $\tilde{\mathbb{F}}_q$ funktiokunnan täysi vakioiden kunta. Jos $\tilde{\mathbb{F}}_q \neq \mathbb{F}_q$, on kuitenkin seurauksen I.1.15 mukaan laajennus $[\tilde{\mathbb{F}}_q : \mathbb{F}_q]$ äärellinen, joten on olemassa sellainen r, että $\tilde{\mathbb{F}}_q = \mathbb{F}_{q^r}$. Tällöin myös $g(F/\mathbb{F}_{q^r}) = g(F/\mathbb{F}_q)$, joten korvaamalla pohjakunta $\mathbb{F}_q$ tarvittaessa kunnalla $\mathbb{F}_{q^r}$ voidaan ainakin aluksi olettaa, että $\mathbb{F}_q$ on täysi vakioiden kunta.

Olkoon P jokin funktiokunnan $F/\mathbb{F}_q$ paikka. Määritellään paikan absoluuttinen normi

$$\mathrm{N}(P) = |\mathcal{O}_P/P| = q^{\deg P},$$

ja yleistetään tämä välittömästi divisoreille

$$\mathrm{N}(A) = q^{\deg A}.$$

Määritellään funktiokunnalle $\mathcal{F} = F/\mathbb{F}_q$ ζ-funktio

$$\zeta_{\mathcal{F}}(s) = \sum_{\substack{A \in \mathcal{D}_{\mathcal{F}} \\ A \geq 0}} \frac{1}{\mathrm{N}(A)^s}. \tag{6}$$

Merkitään

$$A_n = |\{A \in \mathcal{D}_{\mathcal{F}} \mid \deg A = n,\ A \geq 0\}|.$$

Lemma V.1.1. *Jokaiselle luonnolliselle luvulle n on voimassa $A_n < \infty$.*

Todistus. Jokainen astetta n oleva positiivinen divisori voidaan esittää korkeintaan n alkudivisorin summana yksikäsitteisellä tavalla. Näinollen riittää todistaa että joukko

$$S_n = \{P \in \mathbb{P}_{\mathcal{F}} \mid \deg P \leq n\}$$

on äärellinen. Tämän joukon sijasta voidaan tarkastella rationaalisen funktiokunnan $\mathbb{F}_q(x)/\mathbb{F}_q$ alkudivisoreja. Merkitään

$$S_n^0 = \{P \in \mathbb{P}_{\mathbb{F}_q(x)} \mid \deg P \leq n\}.$$

Selvästi on $P \cap \mathbb{F}_q(x) \in S_n^0$ aina kun $P \in S_n$. Toisaalta jokaisen paikan $P \in S_n^0$ yllä on vain äärellisen monta paikkaa $P' \in S_n$. Tämän vuoksi riittää osoittaa, että joukko S_n^0 on äärellinen. Tämä puolestaan johtuu siitä että astetta n olevat paikat vastaavat bijektiivisesti kunnan $\mathbb{F}_q$ astetta n olevien jaottomien polynomien ekvivalenssiluokkia. □

Nyt ζ-funktio saa muodon

$$\zeta_{\mathcal{F}}(s) = \sum_{n=0}^{\infty} \frac{A_n}{q^{ns}}.$$

Merkitään

$$Z_{\mathcal{F}}(t) = \sum_{n=0}^{\infty} A_n t^n, \tag{7}$$

jolloin $\zeta_{\mathcal{F}}(s) = Z_{\mathcal{F}}(q^{-s})$. Jatkossa funktiota $Z_{\mathcal{F}}(t)$ kutsutaan funktiokunnan $F/\mathbb{F}_q$ Z-funktioksi.

Palautetaan mieleen seuraavat merkinnät:

(1) $\mathcal{D}_{\mathcal{F}}$ on funktiokunnan divisoriryhmä,

(2) $\mathcal{P}_{\mathcal{F}}$ on päädivisorien muodostama aliryhmä,

(3) $A \sim B$ merkitsee, että $A - B \in \mathcal{P}_{\mathcal{F}}$ ja

(4) $\mathcal{C}_{\mathcal{F}} = \mathcal{D}_{\mathcal{F}}/\mathcal{P}_{\mathcal{F}}$ on divisoriluokkaryhmä.

Tekijäryhmä $\mathcal{C}_{\mathcal{F}}$ on algebrallisten lukukuntien ihanneluokkaryhmän analogia algebrallisten funktiokuntien teoriassa.

Käytetään divisoriluokkaryhmän alkiosta $A + \mathcal{P}_{\mathcal{F}}$ merkintää $[A]$, jolloin siis

$$[A] = \{B \in \mathcal{D}_{\mathcal{F}} \mid B \sim A\}.$$

Divisoreilla, jotka ovat ekvivalentteja modulo päädivisorit, on sama dimensio ja sama aste. Näinollen voidaan myös divisoriluokille määritellä dimensio ja aste.

$$\dim [A] = \dim A$$
$$\deg [A] = \deg A$$

Merkitään

$$\mathcal{D}^0_{\mathcal{F}} = \{A \in \mathcal{D}_{\mathcal{F}} \mid \deg A = 0\}, \text{ astetta 0 olevat divisorit ja}$$

$$\mathcal{C}^0_{\mathcal{F}} = \{[A] \in \mathcal{C}_{\mathcal{F}} \mid \deg [A] = 0\}, \text{ astetta 0 olevat divisoriluokat.}$$

Määritellään myös ihanneluokkaluvun analogia funktiokunnille.

MÄÄRITELMÄ. Funktiokunnan $F/\mathbb{F}_q$ luokkaluku h on

$$h = h_{\mathcal{F}} = \left|\mathcal{C}^0_{\mathcal{F}}\right|.$$

Propositio V.1.3. *Luokkaluku h on äärellinen.*

Todistus. Merkitään yleisesti astetta $n \in \mathbb{N}$ olevia divisoriluokkia

$$\mathcal{C}^n_{\mathcal{F}} = \{[A] \in \mathcal{C}_{\mathcal{F}} \mid \deg [A] = n\}.$$

Valitaan jokin sellainen luku $n > g$, että on olemassa n-asteinen divisori B. Silloin kuvaus $\mathcal{C}^0_{\mathcal{F}} \mapsto \mathcal{C}^n_{\mathcal{F}}$, $[A] \mapsto [A+B]$ on selvästi bijektio, joten riittää osoittaa että luku $|\mathcal{C}^n_{\mathcal{F}}|$ on äärellinen. Tämän osoittamiseksi väitetään, että jokaisessa divisoriluokassa $[C] \in \mathcal{C}^n_{\mathcal{F}}$ on *positiivinen* astetta n oleva divisori. Tällöin alkuperäinen väite seuraa, sillä teoreeman V.1.1 mukaan kutakin lukua n kohti on vain äärellinen määrä astetta n olevia positiivisia divisoreja.

Kun merkitään W = funktiokunnan $F/\mathbb{F}_q$ kanoninen divisori, on Riemannin-Rochin lauseen mukaan

$$\dim [C] = \dim C = \deg C + 1 - g + \dim (W - C) \geq n + 1 - g \geq 1.$$

Tällöin, huomautuksen I.4.5 (b) mukaan, luokassa $[C]$ on positiivinen divisori. □

HUOMAUTUS. Edellisen lauseen todistuksesta nähdään, että on aina joko $\mathcal{C}_{\mathcal{F}}^n = \emptyset$ tai $|\mathcal{C}_{\mathcal{F}}^n| = |\mathcal{C}_{\mathcal{F}}^0|$.

MÄÄRITELMÄ. $\partial = \min\{\deg A \mid A \in \mathcal{D}_{\mathcal{F}},\ \deg A > 0\}$.

Kuvaus $\deg\ : \mathcal{D}_{\mathcal{F}} \mapsto \mathbb{Z}$ on ryhmähomomorfismi ja kuva $\mathrm{Im}(\deg\ )$ on luvun ∂ generoima. Tällöin ∂ jakaa jokaisen divisorin asteen.

Tarkastellaan lukuja

$$A_n = |\{A \in \mathcal{D}_{\mathcal{F}} \mid A \geq 0,\ \deg A = n\}|\,.$$

Lemma V.1.4.

(1) *Jos* $\partial \nmid n$, *niin* $A_n = 0$

(2) *Jokaiselle divisoriluokalle* $[C] \in \mathcal{C}_{\mathcal{F}}$ *pätee*

$$|A \in [C] \mid A \geq 0\}| = \frac{1}{q-1}\left(q^{\dim [C]} - 1\right).$$

(3) *Jos* $\partial \mid n$ *ja* $n > 2g-2$, *niin*

$$A_n = \frac{h}{q-1}\left(q^{n+1-g} - 1\right).$$

Todistus. Kohta (1) on triviaali. Kohta (2) varten havaitaan, että ehdot $A \in [C]$ ja $A \geq 0$ ovat yhtäpitäviä ehtojen $A = (x) + C$ ja $(x) \geq -C$ Kanssa. Jos taas nämä ehdot ovat voimassa, on $x \in \mathcal{L}(C) \setminus \{0\}$. Toisaalta $\mathbb{F}_q$-avaruudessa on $q^{\dim [C]} - 1$ nollasta eroavaa alkiota, ja kahta eri alkiota vastaa sama divisori tarkalleen silloin kun ne ovat $\mathbb{F}_q$-riippuvia. Tämä todistaa väitteen (2)

Jos $\partial \mid n$, on olemassa astetta n oleva divisori, ja edelläolleen huomautuksen mukaan astetta n olevia divisoriluokkia on tarkalleen h kappaletta. Olkoot nämä $[C_1]$, $[C_2]$, …, $[C_h]$. Kohdan (b) ja Riemannin-Rochin lauseen mukaan

$$|\{A \in [C_j] \mid A \geq 0\}| = \frac{1}{q-1}\left(q^{\dim C_j} - 1\right) = \frac{1}{q-1}\left(q^{n+1-g} - 1\right).$$

Toisaalta, jokainen astetta n oleva divisori on tarkalleen yhdessä luokista $[C_1]$, $[C_2]$, …, $[C_h]$, joten

$$A_n = \sum_{j=1}^{h} |\{A \in [C_j] \mid A \geq 0\}| = \frac{h}{q-1}\left(q^{n+1-g} - 1\right).$$

Tämä todistaa kohdan (3). □

Propositio V.1.6. *Potenssisarja* $Z_{\mathcal{F}}(t) = \sum_{n=0}^{\infty} A_n t^n$ *suppenee, kun* $|t| < \frac{1}{q}$. *Tällöin on myös voimassa*

(1) *Jos funktiokunnan* $F/\mathbb{F}_q$ *suku* $g = 0$, *on*

$$Z_{\mathcal{F}}(t) = \frac{1}{q-1}\left(\frac{q}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}}\right).$$

(2) *Jos* $g \geq 1$, *on* $Z(t) = F(t) + G(t)$, *esityksessä*

$$F(t) = \frac{1}{q-1} \sum_{\substack{[C]\in \mathcal{C}_{\mathcal{F}} \\ 0 \leq \deg\,[C] \leq 2g-2}} q^{\dim\,[C]} t^{\deg\,[C]}$$

on holomorfinen osa ja

$$G(t) = \frac{h}{q-1}\left(q^{1-g}(qt)^{2g-2+\partial}\frac{1}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}}\right).$$

Todistus. Näytetään aluksi, että sukua nolla olevan funktiokunnan luokkaluku $h = 1$, toisin sanoen näytetään että jokainen astetta nolla oleva divisori on päädivisori. Valitaan jokin nolla-asteinen divisori A. Koska $\deg A = 0 > 2g-2$ on Riemannin-Rochin lauseen nojalla $\dim A = \deg A + 1 - g = 1$ ja siis $Ł(A) \neq \{0\}$. Nyt voidaan valita nollasta eroava alkio $x \in Ł(A)$, jolle siis pätee $(x) \geq -A$. Koska molemmat divisorit (x) ja A ovat astetta nolla, on tämä mahdollista vain jos $(x) = -A$ ja siis $A = -(x) = (x^{-1}) \in \mathcal{P}_{\mathcal{F}}$. Lemman V.1.4 mukaan

$$\begin{aligned}\sum_{n=0}^{\infty} A_n t^n &= \sum_{n=0}^{\infty} A_{\partial n} t^{\partial n} = \sum_{n=0}^{\infty} \frac{1}{q-1}\left(q^{\partial n+1} - 1\right) t^{\partial n} \\ &= \frac{1}{q-1}\left(q\sum_{n=0}^{\infty}(qt)^{\partial n} - \sum_{n=0}^{\infty} t^{\partial n}\right) \\ &= \frac{1}{q-1}\left(\frac{q}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}}\right).\end{aligned}$$

Viimeisestä muodosta nähdään suoraan että sarja suppenee aina kun $|qt| < 1$.

Yleisessä tapauksessa

$$\sum_{n=0}^{\infty} A_n t^n = \sum_{\deg\,[C]\geq 0} |\{A \in [C] \mid A \geq 0\}| \cdot t^{\deg\,[C]}$$

$$= \sum_{\deg\,[C]\geq 0} \frac{q^{\dim\,[C]} - 1}{q-1} \cdot t^{\deg\,[C]}$$

$$= \frac{1}{q-1} \sum_{\deg\,[C]\geq 0} q^{\dim\,[C]} t^{\deg\,[C]} - \frac{1}{q-1} \sum_{\deg\,[C]\geq 0} t^{\deg\,[C]}$$

$$= \underbrace{\frac{1}{q-1} \sum_{0 \leq \deg\,[C] \leq 2g-2} q^{\dim\,[C]} t^{\deg\,[C]}}_{F(t)}$$

$$+ \underbrace{\frac{1}{q-1} \sum_{\deg\,[C] > 2g-2} q^{\deg\,[C]+1-g} t^{\deg\,[C]} - \frac{1}{q-1} \sum_{\deg\,[C] \geq 0} t^{\deg\,[C]}}_{G(t)}.$$

Todetaan vielä että

$$\begin{aligned}
(q-1)G(t) &= \sum_{n=\frac{2g-1}{\partial}+1}^{\infty} h q^{n\partial+1-g} \cdot t^{n\partial} - \sum_{n=0}^{\infty} h t^{\partial n} \\
&= h q^{1-g} \sum_{n=\frac{2g-1}{\partial}+1}^{\infty} (qt)^{n\partial} - h\frac{1}{1-t^{\partial}} \\
&= h q^{1-g} \sum_{n=0}^{\infty} (qt)^{n\partial+2g-2+\partial} - \frac{h}{1-t^{\partial}} \\
&= h q^{1-g} (qt)^{2g-2+\partial} \frac{1}{1-(qt)^{\partial}} - \frac{h}{1-t^{\partial}}. \quad \square
\end{aligned}$$

Seuraus V.1.7. *Funktiolla $Z(t)$ on yksinkertainen napa pisteessä $t = 1$. Tämä johtuu siitä, että funktiolla $\frac{1}{1-t^{\partial}}$ on yksinkertainen napa pisteessä $t = 1$.*

ärettömistä tuloista.

Sanotaan että tulo

$$\prod_{i=1}^{\infty} (1 + a_i)$$

suppenee kohti lukua $a \in \mathbb{C}$, jos $a \neq 0$ ja

$$\lim_{n \mapsto \infty} \prod_{i=1}^{n} (1 + a_i) = a. \tag{8}$$

Lisäksi sanotaan, että tulo (8) suppenee *itseisesti*, jos sarja

$$\sum_{i=1}^{\infty} |a_i| \tag{9}$$

suppenee. Tunnetusti itseisestä suppenemisesta seuraa suppeneminen, ja tällöin raja-arvo (8) on riippumaton tekijöiden järjestyksestä. Lisäksi, jos tulo (8) suppenee itseisesti, niin myös tulo

$$\prod_{i=1}^{\infty} (1 + a_i)^{-1}$$

suppenee itseisesti kohti raja-arvoa a^{-1}.

Propositio V.1.8 (Eulerin tuloesitys). *Funktiokunnan $\mathcal{F} = F/\mathbb{F}_q$ Z-funktiolla on esitys*

$$Z(t) = \prod_{P \in \mathbb{P}_\mathcal{F}} \frac{1}{1 - t^{\deg P}}. \tag{10}$$

Tulo suppenee itseisesti, kun $|t| \leq \frac{1}{q}$.

Todistus. Tulo $\prod_{P \in \mathbb{P}_\mathcal{F}} \left(1 - t^{\deg P}\right)^{-1}$ suppenee itseisesti, sillä

$$\sum_{P \in \mathbb{P}_\mathcal{F}} \left|t^{\deg P}\right| \leq \sum_{n=0}^{\infty} A_n \left|t\right|^n \leq \infty$$

Proposition V.1.6 mukaan. Tarkastellaan nyt tuloja

$$\prod_{\substack{P \in \mathbb{P}_\mathcal{F} \\ \deg P \leq n}} \left(1 - t^{\deg P}\right)^{-1} = \prod_{\substack{P \in \mathbb{P}_\mathcal{F} \\ \deg P \leq n}} \sum_{i=0}^{\infty} \left(t^{\deg P}\right)^i.$$

Oikealla puolella olevat sarjat suppenevat itseisesti, joten Cauchyn kertolaskusäännön mukaan saadaan

$$\prod_{\substack{P \in \mathbb{P}_\mathcal{F} \\ \deg P \leq n}} \left(1 - t^{\deg P}\right)^{-1} = \prod_{\substack{P \in \mathbb{P}_\mathcal{F} \\ \deg P \leq n}} \sum_{i=0}^{\infty} t^{i \deg P} = \sum_{\substack{A \in \mathcal{D}_\mathcal{F}^{(n)} \\ A \geq 0}} t^{\deg A}. \tag{11}$$

Summassa (11) esiintyvä merkintä $\mathcal{D}_\mathcal{F}^{(n)}$ tarkoittaa niiden divisorien joukkoa, joiden alkudivisoritekijöiden aste ei ylitä lukua n. Selvästi on $\mathcal{D}_\mathcal{F}^{(\infty)} = \mathcal{D}_\mathcal{F}$. Antamalla luvun n lähestyä ääretöntä saadaan

$$\prod_{P \in \mathbb{P}_\mathcal{F}} \left(1 - t^{\deg P}\right)^{-1} = \sum_{\substack{A \in \mathcal{D}_\mathcal{F} \\ A \geq 0}} t^{\deg A} = \sum_{n=0}^{\infty} A_n t^n = Z(t).$$

□

Luovutaan nyt oletuksesta, jonka mukaan vakiokunta $\mathbb{F}_q$ on täysi vakioiden kunta. Tällöin on huomattava, että edellä saadut tulokset *eivät päde* sellaisenaan. Palautetaan mieleen, että Riemannin-Rochin lauseen mukaan Tässä tapauksessa

$$\dim A = \deg A + (1 - g)[\tilde{\mathbb{F}}_q : \mathbb{F}_q] + \dim (W - A).$$

Kiinnitetään jokin kunnan $\mathbb{F}_q$ algebrallinen sulkeuma $\overline{\mathbb{F}}_q$ ja tarkastellaan vakiokuntalaajennusta $\overline{F} = F\overline{\mathbb{F}}_q$. Tunnetun tuloksen mukaan kutakin luonnollista lukua r kohti on olemassa yksikäsitteinen r-asteinen laajennus $\mathbb{F}_{q^r}/\mathbb{F}_q$,jolle pätee $\mathbb{F}_{q^r} \subseteq \overline{\mathbb{F}}$. Määritellään kunnat F_r seuraavasti: $F_r = F\mathbb{F}_{q^r} \subseteq \overline{F}$.

Lemma V.1.9.

(1) *Laajennus F_r/F on astetta r oleva Galois'n laajennus jonka Galois'n ryhmä on syklinen. Ryhmän $Gal(F_r/F)$ generoi Frobenius-automorfismi σ, jolle pätee $\sigma(\alpha) = \alpha^q$ kaikille kunnan $\mathbb{F}_{q^r}$ alkioille α.*

(2) *Kunta $\mathbb{F}_{q^r}$ on kunnan F_r täysi vakioden kunta.*

(3) *Funktiokuntien $F_r/\mathbb{F}_{q^r}$ ja $F/\mathbb{F}_q$ suvut ovat samat.*

(4) *Olkoon $P \in \mathbb{P}_{\mathcal{F}}$ astetta m oleva paikka. Merkitään $d = syt(m, r)$. Silloin $Con_{F_r/F}(P) = P_1 + P_2 + \ldots P_d$. Esityksessä on $P_i \neq P_j$ aina kun $i \neq j$ ja deg $P_i = \frac{m}{d}$.*

Todistus. Kohta (1). Tunnetusti laajennus $\mathbb{F}_{q^r}/\mathbb{F}_q$ on syklinen astetta r oleva Galois'n laajennus, jonka Galois'n ryhmän generoi Frobenius-automorfismi. Lemman III.6.2 nojalla on voimassa $[F_r : F] = [\mathbb{F}_{q^r} : \mathbb{F}_q]$. Esityksestä $F_r = F\mathbb{F}_{q^r}$ seuraa tunnetusti, että kukin ryhmän $\mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ automorfismi voidaan nostaa Laajennuksen F_r/F automorfismeiksi. Kyseisiä automorfismeja saadaan siis r kappaletta, mikä on mahdollista vain silloin kun kysymyksessä on Galois'n laajennus. Suoraviivaisesti voidaan todeta että Frobenius-automorfismi Generoi ryhmän $\mathrm{Gal}(F_r/F)$.

Kohdat (2) ja (3) seuraavat suoraan Propositiosta III.6.1 ja Teoreemasta III.6.3.

Kohta (4). Teoreeman III.6.3 mukaan vakiokuntalaajennuksessa F_r/F kaikki paikat P säilyvät haaroittumattomina. Olkoon nyt P' jokin paikan P yllä oleva paikka. Edelleen lauseen III.6.3 (g) mukaan paikan P' jäännösluokkakunta on kuntien $F_P = \mathcal{O}_P/P$ ja $\mathbb{F}_{q^r}$ kompositum. Merkitään $l = \mathrm{pyj}(m, r)$. Koska $F_P = \mathbb{F}_{q^m}$, on kyseinen kompositum

$$\mathbb{F}_{q^m}\mathbb{F}_{q^r} = \mathbb{F}_{q^l}.$$

Tämän vuoksi

$$\deg P' = [\mathbb{F}_{q^l} : \mathbb{F}_{q^r}] = \frac{l}{r} = \frac{\mathrm{pyj}(m, r)}{r} = \frac{m}{d}.$$

Toisaalta deg $\left(\mathrm{Con}_{F_r/F}(P)\right)$ = deg $P = m$ (Teoreema III.6.3. (c)). Tällöin on oltava

$$\mathrm{Con}_{F_r/F}(P) = P_1 + P_2 + \ldots P_d,$$

ja jokaisen paikan P_i aste on $\frac{m}{d}$. □

Jatkossa tarvitaan seuraava yksinkertainen polynomi-identiteetti: Olkoot m ja r luonnollisia lukuja ja $d = \mathrm{syt}(m, r)$. Käytetään r:nsien ykkösenjuurien joukosta merkintää $\mathbb{U}_r$. Silloin

$$\left(X^{\frac{r}{d}} - 1\right)^d = \prod_{\zeta \in \mathbb{U}_r} \left(X - \zeta^m\right). \tag{12}$$

Identiteetti (12) on helppo havaita oikeaksi: Koska $|\mathbb{U}_r| = r$, on yhtälön kumpikin puoli astetta r oleva pääpolynomi. Lisäksi kyseisillä polynomeilla on tarkalleen samat nollakohdat; kertalukua $\frac{r}{d}$ olevat ykkösenjuuret ovat kummankin polynomin d-kertaisia nollakohtia.

Sijoitetaan yhtälöön (12) $X = t^{-m}$ ja kerrotaan puolittain luvulla t^{mr}, jolloin saadaan

$$\left(1 - t^{\frac{mr}{d}}\right)^d = \prod_{\zeta \in \mathbb{U}_r} \left(1 - (\zeta t)^m\right). \tag{13}$$

Propositio V.1.10. *Olkoot $Z(t)$ funktiokunnan $\mathcal{F} = F/\mathbb{F}_q$ ja $Z_r(t)$ funktiokunnan $\mathcal{F}_r = F_r/\mathbb{F}_{q^r}$ Z-funktiot. Silloin*

$$Z_r(t^r) = \prod_{\zeta \in \mathbb{U}_r} Z(\zeta t).$$

Todistus. Tunnetun funktioteorian tuloksen mukaan riittää todistaa väitetty funktionaaliyhtälö oikeaksi ympyräalueessa $|t| < \frac{1}{q}$. Tässä alueessa on voimassa Eulerin tuloesitys

$$Z_r(t^r) = \prod_{P' \in \mathbb{P}_{\mathcal{F}_r}} \left(1 - t^{r \cdot \deg P'}\right)^{-1} = \prod_{P \in \mathbb{P}_{\mathcal{F}}} \prod_{P' | P} \left(1 - t^{r \cdot \deg P'}\right)^{-1}. \tag{14}$$

Kiinteällä m-asteisella paikalla $P \in \mathbb{P}_{\mathcal{F}}$ saa sisemmän tulon käänteisluku (Lemman V.1.9 mukaan) muodon

$$\prod_{P' | P} \left(1 - t^{r \cdot \deg P'}\right) = \left(1 - t^{\frac{rm}{d}}\right)^d$$

$$= \prod_{\zeta \in \mathbb{U}_r} (1 - (\zeta t)^m) = \prod_{\zeta \in \mathbb{U}_r} \left(1 - (\zeta t)^{\deg P}\right).$$

Sijoittamalla tämä esitykseen (14) saadaan

$$Z_r(t^r) = \prod_{\zeta \in \mathbb{U}_r} \prod_{P \in \mathbb{P}_{\mathcal{F}}} \left(1 - (\zeta t)^{\deg P}\right)^{-1} = \prod_{\zeta \in \mathbb{U}_r} Z(\zeta t).$$

□

Seuraus V.1.11 (F.K. Schmidt). $\partial = 1$.

Todistus. Olkoon $\zeta \in \mathbb{U}_\partial$, jolloin siis $\zeta^\partial = 1$. Koska ∂ jakaa jokaisen divisorin asteen, on voimassa

$$Z(\zeta t) = \prod_{P \in \mathbb{P}_{\mathcal{F}}} \left(1 - (\zeta t)^{\deg P}\right)^{-1} = \prod_{P \in \mathbb{P}_{\mathcal{F}}} \left(1 - t^{\deg P}\right)^{-1} = Z(t).$$

Proposition V.1.10 mukaan on

$$Z_\partial(t^\partial) = \prod_{\zeta \in \mathbb{U}_\partial} Z(\zeta t) = Z(t)^\partial. \tag{15}$$

Seurauksen V.1.7 mukaan rationaalifunktiolla $Z_\partial(t^\partial)$ on yksinkertainen napa pisteessä $t = 1$, toisaalta taas funktiolla $Z(t)^\partial$ on kertalukua ∂ oleva napa tässä pisteessä. Väite seuraa nyt laskemalla yhtälöstä (15) napojen kertaluvut pisteessä $t = 1$. □

Seuraus V.1.12.

(1) *Sukua* 0 *oleva funktiokunta* $F/\mathbb{F}_q$ *on rationaalinen ja sen* Z*-funktio on*

$$Z(t) = \frac{1}{(1-t)(1-qt)}.$$

(2) *Jos funktiokunnan* $F/\mathbb{F}_q$ *suku* $g \geq 1$ *ja täysi vakioiden kunta on* F_q*, voidaan sen* Z*-funktio kirjoittaa muodossa* $Z(t) = F(t) + G(t)$*. Tässä esityksessä on*

$$F(t) = \frac{1}{q-1} \sum_{0 \leq \deg\,[C] \leq 2g-2} q^{\dim\,[C]} t^{\deg\,[C]} \text{ ja}$$

$$G(t) = \frac{h}{q-1}\left(q^g t^{2g-1} \frac{1}{1-qt} - \frac{1}{1-t}\right).$$

Todistus. Luvut A_n merkitsevät astetta n olevien positiivisten divisorien määrää. Sijoitetaan Lemmaan V.1.4 (c) $n = 1$, jolloin saadaan $A_1 = \frac{h}{q-1}(q^2-1) = h(q+1) \geq 3$, josta nähdään, että funktiokunnalla $F/\mathbb{F}_q$ on astetta 1 oleva divisori. Propositiosta I.6.3 seuraa nyt, että funktiokunta $F/\mathbb{F}_q$ on rationaalinen. Väitteen loppuosa saadaan Propositiosta V.1.6 sijoittamalla $\partial = 1$.

Propositio V.1.13 (*Z*-funktion funktionaaliyhtälö). *Olkoon* F_q *funktiokunnan* $F/\mathbb{F}_q$ *täysi vakioiden kunta. Funktiokunnan* Z*-funktio toteuttaa tällöin funktionaaliyhtälön*

$$Z(t) = q^{g-1} t^{2g-2} Z(\frac{1}{qt}).$$

Todistus. Sukua 0 olevalle funktiokunnalle yhtälö saadaan suoraan seurauksesta V.1.12:

$$Z(\frac{1}{qt}) = \frac{1}{(1-\frac{1}{qt})(1-q\cdot\frac{1}{qt})}$$

$$= \frac{qt^2}{(qt-1)(t-1))} = \frac{qt^2}{(1-t)(1-qt)} = qt^2 Z(t).$$

Tapauksessa $g \geq 1$ esitetään Z-funktio seurauksen V.1.12 (2) muodossa $Z(t) = F(t) + G(t)$. Olkoon W funktiokunnan $F/\mathbb{F}_q$ kanoninen divisori. Tämän aste

deg $[W] = 2g - 2$. Saadaan

$$\begin{aligned}
(q-1)F(t) &= \sum_{0\le \deg\,[C]\le 2g-2} q^{\dim\,[C]} t^{\deg\,[C]} \\
&= \sum_{0\le \deg\,[C]\le 2g-2} q^{\deg\,[C]+1-g+\dim\,[W-C]} t^{\deg\,[C]} \\
&= q^{g-1}t^{2g-2} \sum_{0\le \deg\,[C]\le 2g-2} q^{\deg\,[C]-(2g-1)+\dim\,[W-C]} t^{\deg\,[C]-(2g-2)} \\
&= q^{g-1}t^{2g-2} \sum_{0\le \deg\,[C]\le 2g-2} q^{\deg\,[C]-\deg\,[W]+\dim\,[W-C]} \cdot t^{\deg\,[C]-\deg\,[W]} \\
&= q^{g-1}t^{2g-2} \sum_{0\le \deg\,[W-C]\le 2g-2} q^{\dim\,[W-C]} \cdot \left(\frac{1}{qt}\right)^{\deg\,[W-C]} \\
&= q^{g-1}t^{2g-2}(q-1)F(\frac{1}{qt}).
\end{aligned}$$

Funktiolle $G(t)$ saadaan suoralla laskulla

$$\begin{aligned}
&q^{g-1}t^{2g-2}G(\frac{1}{qt}) \\
&\qquad = \frac{h}{q-1} q^{g-1}t^{2g-2} \left(q^g \left(\frac{1}{qt}\right)^{2g-1} \frac{1}{1-q\frac{1}{qt}} - \frac{1}{1-\frac{1}{qt}} \right) \\
&\qquad = \frac{h}{q-1} \left(\frac{1}{t}\frac{1}{1-\frac{1}{t}} - \frac{q^g t^{2g-1}}{qt\left(1-\frac{1}{qt}\right)} \right) \\
&\qquad = G(t).
\end{aligned}$$

Väite saadaan yhdistämällä tulokset. □

MÄÄRITELMÄ. Polynomia $L(t) = L_{\mathcal{F}}(t) = (1-t)(1-qt)Z_{\mathcal{F}}(t)$ Kutsutaan funktiokunnan $\mathcal{F} = F/\mathbb{F}_q$ *L-polynomiksi.*

Seurauksen V.1.12 mukaan polynomi $L(t)$ on enintään astetta $2g$. Lisäksi havaitaan, että

$$L(t) = (1-t)(1-qt)\sum_{n=0}^{\infty} A_n t^n. \tag{16}$$

Esityksestä (16) nähdään L-polynomin avulla voidaan saada informaatiota luvuista A_n.

Teoreema V.1.15.

(1) *$L(t)$-polynomi on kokonaiskertoiminen ja sen aste deg $L(t) = 2g$.*

(2) *On voimassa funktionaaliyhtälö $L(t) = q^g t^{2g} L(\frac{1}{qt})$.*

(3) *Jos h on funktiokunnan $F/\mathbb{F}_q$ luokkaluku, on voimassa $L(1) = h$*

(4) *Jos käytetään astetta 1 olevien paikkojen määrästä merkintää N ja merkitään $L(t) = a_0 + a_1 t + \ldots + a_{2g}t^{2g}$, niin*

(a) $a_0 = 1$ *ja* $a_{2g} = q^g$,

(b) $a_{2g-i} = q^{g-i}a_i$ *aina kun* $i \in \{0, 1, \ldots, g\}$, *ja*

(c) $a_1 = N - (q + 1)$

(5) *Polynomilla* $L(t)$ *on renkaassa* $\mathbb{C}[t]$ *hajotelma*

$$L(t) = \prod_{i=1}^{2g}(1 - \alpha_i t). \tag{17}$$

Kompleksiluvut α_1, α_2, ..., α_{2g} *ovat algebrallisia kokonaislukuja. Lisäksi ne voidaan numeroida siten että* $\alpha_i\alpha_{g+i} = q$ *pätee aina kun* $i \in \{1, 2, \ldots, g\}$.

(6) *Jos* $L_r(t) = (1 - t)(1 - q^r t)Z_r(t)$ *on vakiokuntalaajennuksen* $F_r = F\mathbb{F}_{q^r}$ *L-polynomi, niin*

$$L_r(t) = \prod_{i=1}^{2g}(1 - \alpha_i^r t).$$

Luvut α_i *ovat samat kuin yhtälössä (17).*

Todistus. Jos funktiokunnan suku on nolla, on $L(t) = 1$ ja kaikki väittämät ovat triviaaleja. Oletetaan siksi että $g \geq 1$.

Kohta (1). L-polynomin määritelmän mukaan on selvä, että deg $(L) \leq 2g$. Asteen alarajaa koskeva väittämä tulee todistettua kohdassa (4). Väittämä $L(t) \in \mathbb{Z}[t]$ seuraa nyt esityksestä (16).

Kohta (2) seuraa suoraan Z-funktion funktionaaliyhtälöstä.

Seurauksen V.1.12 (b) mukaan on

$$L(t) = (1 - t)(1 - qt)F(t) + \frac{h}{q - 1}\left(q^g t^{2g-1}(1 - t) - (1 - qt)\right).$$

Sijoittamalla tähän $t = 1$ nähdään että $L(1) = h$.

Kohtaa (4) varten merkitään

$$L(t) = a_0 + a_1 t + \ldots + a_{2g}t^{2g}.$$

Kohdan (2) funktionaaliyhtälöstä saadaan nyt

$$L(t) = q^g t^{2g} L(\frac{1}{qt}) = \frac{a_{2g}}{q^g} + \frac{a_{2g-1}}{q^{g-1}}t + \ldots + q^g a_0 t^{2g}.$$

Tästä seuraa (b), sillä vertailemalla kertoimia nähdään että $a2g - 1 = q^{g-i}a_i$ aina kun $i \in \{0, 1, \ldots, g\}$. Esityksestä (16) nähdään että L-polynomin vakiokerroin $a_0 = A_0$ ja ensimmäistä astetta olevan termin kerroin $a_1 = (-1 - q)A_0 + A_1 = A_1 - (q + 1)A_0$. Astetta 0 olevia positiivisia divisoreja on vain yksi, joten $A_0 = 1$. Helposti todetaan myös että $A_1 = N$, joten saadaan kohta (c) ja (a)-kohdan ensimmäinen väittämä. Toinen väittämä saadaan asettamalla kohdassa (b) $i = 0$. Tästä saadaan myös kohta (1), sillä astetta $2g$ olevan termin kerroin on $q^g \neq 0$.

Kohtaa (5) varten tarkastellaan polynomin L *resiprookkipolynomia*

$$L^{\perp}(t) = t^{2g}L(\frac{1}{t}) = a_0t^{2g} + a_1t^{2g-1} + \ldots + a_{2g} = t^{2g} + a_1t^{2g-1} + \ldots + q^g. \quad (18)$$

Polynomi $L^{\perp}(t)$ on $\mathbb{Z}$-kertoiminen pääpolynomi, joten sen nollakohdan α_1, α_2, …, α_{2g} ovat algebrallisia kokonaislukuja. Polynomi $L^{\perp}(t)$ jakautuu tekijöihin:

$$L^{\perp}(t) = \prod_{i=1}^{2g}(t - \alpha_i).$$

Tällöin

$$L(t) = t^{2g}L^{\perp}(\frac{1}{t}) = \prod_{i=1}^{2g}(1 - \alpha_i t).$$

Välittömästi havaitaan että polynomin $L^{\perp}(t)$ juuret α_i ovat polynomin $L(t)$ jurien käänteislukuja. Kohdan (2) funktionaaliyhtälöstä saadaan $L^{\perp}(\frac{q}{\alpha}) = q^gL(\frac{1}{\alpha})$, joten $L^{\perp}(\alpha) = 0$ tarkalleen silloin kun $L^{\perp}(\frac{q}{\alpha}) = 0$. Järjestetään polynomin $L^{\perp}(t)$ nollakohdat jonoon seuraavalla tavalla:

$$\alpha_1, \frac{q}{\alpha_1}, \ldots, \alpha_k, \frac{q}{\alpha_k}, \underbrace{q^{\frac{1}{2}}, \ldots, q^{\frac{1}{2}}}_{m \text{ kpl}}, \underbrace{-q^{\frac{1}{2}}, \ldots, -q^{\frac{1}{2}}}_{n \text{ kpl}}.$$

Polynomi $L^{\perp}(t)$ on parillista astetta, joten sen vakiotermi q^g on yhtäsuuri kuin juurten tulo. Saadaan yhtälö

$$\alpha_1 \cdot \frac{q}{\alpha_1} \cdot \ldots \alpha_k \frac{q}{\alpha_k} \cdot \left(q^{\frac{1}{2}}\right)^m \cdot \left(-q^{\frac{1}{2}}\right)^n = q^g.$$

Tästä nähdään että n on parillinen. Toisaalta $n + m + 2k = 2g$, josta nähdään että myös m on parillinen. Näin on todistettu väite (5).

Proposition V.1.10 mukaan

$$\begin{aligned} L_r(t^r) &= (1 - t^r)(1 - q^rt^r)Z_r(t^r) \\ &= (1 - t^r)(1 - q^rt^r) \prod_{\zeta \in \mathbb{U}_r} Z(\zeta t) \\ &= (1 - t^r)(1 - q^rt^r) \prod_{\zeta \in \mathbb{U}_r} \frac{L(\zeta t)}{(1 - \zeta t)(1 - q\zeta t)} = \prod_{\zeta \in \mathbb{U}_r} L(\zeta t) \\ &= \prod_{i=1}^{2g} \prod_{\zeta \in \mathbb{U}_r} (1 - \alpha_i \zeta t) = \prod_{i=1}^{2g}(1 - \alpha_i^r t^r). \end{aligned}$$

Tästä nähdään, että $L_r(t) = \prod_{i=1}^{2g}(1 - \alpha_i^r t)$. □

Edelläolevan teoreeman todistuksesta nähdään, että luku

$$N(F) = N = |\{P \in \mathbb{P}_{\mathcal{F}} \mid \deg P = 1\}| = A_1$$

voidaan laskea, jos kunnan $F/\mathbb{F}_q$ L-polynomi tunnetaan. Merkitään $F_r = F\mathbb{F}_r$ ja tarkastellaan myös lukuja

$$N_r = N(F_r) = |\{P \in \mathbb{P}_{F_r} \mid \deg P = 1\}|.$$

Näiden lukujen arviointi on oleellisessa asemassa Hassen-Weilin teoreeman todistuksessa.

Seuraus V.1.16. *Olkoot α_1, α_2, ..., α_{2g} polynomin $L(t)$ nollakohtien käänteisluvut. Jokaiselle luonnolliselle luvulle r on voimassa*

$$N_r = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r.$$

Erityisesti tapauksessa $r = 1$ saadaan

$$N(F) = q + 1 - \sum_{i=1}^{2g} \alpha_i.$$

Todistus. Teoreeman V.1.15 (d) mukaan $N_r - (q^r + 1)$ on kunnan F_r L-polynomin ensimmäisen asteen termin kerroin. Toisaalta

$$L_r(t) = \prod_{i=1}^{2g} (1 - \alpha_i^r t),$$

josta nähdään suoraan että tämä kerroin on $-\sum_{i=1}^{2g} \alpha_i^r$.

Mikäli luvut N_r tunnetaan kyllin monella arvolla r, voidaan L-polynomin kertoimet laskea.

Seuraus V.1.17. *Olkoon $L(t) = \sum_{i=0}^{2g} a_i t^i$ funktiokunnan $F/\mathbb{F}_q$ L-polynomi ja $S_r = N_r - (q^r + 1)$. Silloin on voimassa*

(1) $\dfrac{L'(t)}{L(t)} = \sum_{r=1}^{\infty} S_r t^{r-1}$

(2) $a_0 = 1$ *ja*

$$i a_i = S_i a_0 + s_{i-1} a_1 + \ldots + S_1 a_{i-1} \tag{19}$$

aina kun $i \in \{1, 2, \ldots, g\}$.

Jos siis luvut N_1, N_2, ..., N_g ovat tunnetut, voidaan kertoimet a_1, a_2, ..., a_g määrätä yhtälöstä (19) ja muut kertoimet yhtälöstä $a_{2g-i} = q^{g-i} a_i$ Teoreeman V.1.15 (d) mukaisesti.

Todistus. Kun merkitään $L(t) = \prod_{i=1}^{2g} (1 - \alpha_i t)$, on

$$L'(t) = \sum_{i=1}^{2g} \prod_{\substack{j=1 \\ j \neq i}}^{2g} (-\alpha_i)(1 - \alpha_j t).$$

Seurauksen V.1.16 ja lukujen S_r määritelmien mukaan saadaan

$$\begin{aligned} \frac{L'(t)}{L(t)} &= \sum_{i=1}^{2g} \frac{-\alpha_i}{(1 - \alpha_i t)} = \sum_{i=1}^{2g} (-\alpha_i) \cdot \sum_{r=0}^{\infty} (\alpha_i t)^r \\ &= \sum_{r=1}^{\infty} \left(\sum_{i=1}^{2g} -\alpha_i^r \right) t^{r-1} = \sum_{r=1}^{\infty} S_r t^{r-1}. \end{aligned}$$

Lauseen V.1.15 mukaan $a_0 = 1$. Kohdasta (1) seuraa suoraan että

$$a_1 + 2a_2 t + \ldots 2g a_{2g} t^{2g-1} = (a_0 + a_1 t + \ldots + a_{2g} t^{2g}) \cdot \sum_{r=1}^{\infty} S_r t^{r-1}. \tag{20}$$

Väite (2) saadaan nyt vertailemalla puolittain kertoimia yhtälössä (20). □