Iwasawa-elmélet
Egyéni kutatómunka 1

Márton Dénes

1. Bevezetés

Egyéni kutatómunkám során az Iwasawa-elmélet legfontosabb eszközeit értettem meg John Coates és Sujatha Ramdorai Cyclotomic Fields and Zeta Values c. könyve [1] második és harmadik fejezete alapján. A téma érdekesebb és fontosabb tételeinek kimondása és bizonyításának megértése, - mint például a fő sejtés, Iwasawa tétel vagy hogy létezik a Riemann-féle zéta-függvénynek egy p-adikus megfelelője, - az egyéni kutatómunka 2 tantárgy során lesz a célom.

Kezdjük azzal, hogy hogyan tudunk számolni:

2. Hatványsorok, egységek

Legyen p páratlan prímszám. Legyen n természetes szám, $\mathcal{K}_n = \mathbb{Q}_p(\mu_{p^{n+1}})$, ahol $\mu_{p^{n+1}}$ a p^{n+1}-dik egységgyökök halmaza. $\mathbb{Q}_p$ abszolútértéke egyértelműen kiterjed $\mathcal{K}_n$-re, legyen $\mathcal{U}_n = \{u \in \mathcal{K}_n \ : \ |u|_p = 1\}$ a $\mathcal{K}_n$ egészeinek gyűrűjének egységei. Legyenek ζ_n egységgyökök a $\mu_{p^{n+1}}$ valamilyen fix generátorai, melyekre $\zeta_{n+1}^p = \zeta_n$ és legyen $\pi_n = \zeta_n - 1$.

Legyen $N_{n,m} : \mathcal{K}_n \to \mathcal{K}_m$ a norma $n \geq m$-re. Ekkor $N_{n+1,n}(\mathcal{U}_{n+1}) \subseteq \mathcal{U}_n$, mert ha $u_{n+1} \in \mathcal{U}_{n+1}$ egység, akkor minden $\sigma \in \mathrm{Gal}(\mathcal{K}_{n+1}/\mathcal{K}_n)$-ra $|\sigma(u_{n+1})|_p = |u_{n+1}|_p$ és $N_{n+1,n}(u_{n+1}) = \prod_\sigma \sigma(u_{n+1})$, tehát $|N_{n+1,n}(u_{n+1})|_p = |u_{n+1}|_p^p = 1$.

Legyen $\mathcal{U}_\infty = \varprojlim \mathcal{U}_n$, ahol az inverz limesznél az áttérési leképezéseket a norma adja meg. Jelöljük még a $\mathbb{Z}_p$-együtthatós formális hatványsorokat $R = \mathbb{Z}_p[[T]]$-vel. Az egyik fontos tétel a következő:

2.1. Tétel. *Minden $\boldsymbol{u} = (u_n) \in \mathcal{U}_\infty$ egységre egyértelműen létezik $f_{\boldsymbol{u}}(T) \in R$, amire $f(\pi_n) = u_n$ minden $n \geq 0$-ra.*

2.2. Példa. Legyenek a és b egészek és relatív prímek p-hez, ekkor $\mathbf{u} = (u_n) \in \mathcal{U}_\infty$, ahol $u_n = \frac{\zeta_n^{-a/2} - \zeta_n^{a/2}}{\zeta_n^{-b/2} - \zeta_n^{b/2}}$.

Ennek a bizonyítása nem szerepel Coates és Sujatha könyvében, így ezt bizonyítom:

Bizonyítás. Először megmutatjuk, hogy $u_0 \in \mathcal{U}_0$. Definíció szerint

$$|u_0|_p = \sqrt[p-1]{|N_{\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p}(u_0)|_p},$$

mert $|\mathbb{Q}_p(\mu_p) : \mathbb{Q}_p| = p - 1$, hiszen ζ_0 mininmálpolinomja $\mathbb{Q}_p$ fölött $\Phi_p(x)$, ami $(p-1)$-edfokú. A normát számolhatjuk úgy, mint a Galois-konjugáltak szorzata, így

$$N_{\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p}(u_0) = \prod_{k=1}^{p-1} \frac{\zeta_0^{-ak/2 - \zeta_0^{ak/2}}}{\zeta_0^{-bk/2} - \zeta_0^{bk/2}},$$

hiszen $\sigma_k \in \mathrm{Gal}(\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p) = (\mathbb{Z}/p\mathbb{Z})^\times$ olyan, hogy $\sigma_k(\zeta_0) = \zeta_0^k$.

$$\prod_{k=1}^{p-1}(\zeta_0^{-ak/2} - \zeta_0^{ak/2}) = \prod_{k=1}^{p-1}\zeta_0^{-ak/2}(1-\zeta_0^{ak}) = \zeta_0^{-\frac{a}{2}\cdot\frac{p(p-1)}{2}}\prod_{k=1}^{p-1}(1-\zeta_0^k)$$

$\prod_{k=1}^{p-1}(x-\zeta_0^k) = \frac{x^p-1}{x-1} = \Phi_p(x) = x^{p-1}+\cdots+x+1$, tehát $\Phi_p(1) = p$. Mivel $\zeta_0^p = 1$, ezért a számláló egyenlő p-vel, hasonlóan a nevező is, vagyis $N_{\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p(u_0)} = 1$ és így $|u_0|_p = 1$, u_0 egység.

Elég már csak azt megmutatni, hogy $N_{n+1,n}(u_{n+1}) = u_n$ teljesül minden $n \geq 0$-ra, mert akkor ha $u_n \in \mathcal{U}_n$, akkor $u_{n+1} \in \mathcal{U}_{n+1}$ az $|u_{n+1}|_p$ képletéből. $\mathrm{Gal}(\mathcal{K}_{n+1}/\mathcal{K}_n)$ p-elemű csoport, mert $|\mathcal{K}_{n+1} : \mathcal{K}_n| = p$, hiszen ζ_k minimálpolinomja $\mathbb{Q}_p$ felett $\Phi_{p^{k+1}}$, ami $p^k(p-1)$-edfokú és $|\mathcal{K}_{n+1} : \mathbb{Q}_p| = |\mathcal{K}_{n+1} : \mathcal{K}_n| \cdot |\mathcal{K}_n : \mathbb{Q}_p|$. A Galois csoport tetszőleges σ_k $(k = 0, \ldots, p-1)$ elemére $\sigma_k(\zeta_{n+1}) = \zeta_{n+1}\zeta_0^k$, mert a Galois-konjugáltjai ζ_{n+1}-nek a $\mathcal{K}_n$ feletti minimálpolinomjának gyökei, ami pedig $x^p - \zeta_n$.

$$\prod_{k=0}^{p-1}\left((\zeta_{n+1}\zeta_0^k)^{-a/2} - (\zeta_{n+1}\zeta_0^k)^{a/2}\right) = \prod_{k=0}^{p-1}\zeta_{n+1}^{-a/2}\zeta_0^{-ak/2}(1-\zeta_{n+1}^a\zeta_0^{ak}) =$$

$$= \zeta_{n+1}^{-ap/2}\zeta_0^{-\frac{a}{2}\cdot\frac{p(p-1)}{2}}\prod_{k=0}^{p-1}(1-\zeta_{n+1}^a\zeta_0^{ak})$$

$\prod_{k=0}^{p-1}(x-\zeta_{n+1}^a\zeta_0^{ak}) = x^p - \zeta_n^a$, tehát a számláló $\zeta_n^{-a/2}(1-\zeta_n^a) = \zeta_n^{-a/2} - \zeta_n^{a/2}$. Hasonlóan számolható a nevező is, így $N_{n+1,n}(u_{n+1}) = u_n$. Tehát $\mathbf{u} \in \mathcal{U}_\infty$. □

A példát folytatva legyen

$$w_k(T) = \frac{(1+T)^{-k/2} - (1+T)^{k/2}}{T},$$

ami $R^\times$-ben van ha $(k,p) = 1$. Tehát $f_{\mathbf{u}}(T) = w_a(T)/w_b(T) \in R$ és $f_{\mathbf{u}}(\pi_n) = u_n$.

2.3. Megjegyzés. Az R-beli hatványsorok konvergensek $\mathbb{Q}_p$ algebrai lezártjának egészeinek gyűrűjének maximális ideálján, tehát $f_{\mathbf{u}}(\pi_n)$ értelmes. ($|\pi_n|_p < 1$, mert π_n minimálpolinomja $\mathbb{Q}_p$ felett $\Phi_{p^{n+1}}(x+1)$ és $\Phi_{p^{n+1}}(1) = p$, tehát $|N_{\mathcal{K}_n/\mathbb{Q}_p}(\pi_n)|_p = |p|_p < 1$.) A következő tételből pedig az is látszik, hogy R egy elemének véges sok gyöke van ebben az ideálban, mert az egységeknek nincs gyökük.

A 2.1. Tétel egyértelműségi része közvetlenül következik a Weierstrass előkészítési tételből:

2.4. Tétel (Weierstrass). *Minden $f(T) \in R$ egyértelműen írható $f(T) = p^m g(T)w(T)$ alakba, ahol m nemnegatív egész, $g(T)$ egy olyan polinom, ami főegyütthatós, de a többi együtthatója $p\mathbb{Z}_p$-ben van, illetve $w(T) \in R^\times$.*

A létezéshez deiniáljuk a következő leképezéseket. Legyen $f \in R$ hatványsorra $\varphi(f)(T) = f((1+T)^p - 1)$. Ekkor φ egy injektív $\mathbb{Z}_p$-algebra endomorfizmus. Látszik, hogy $\varphi(T) = (1+T)^p - 1$, tehát $\varphi(f)(T) = f(\varphi(T))$.

2.5. Állítás. *Léteznek folytonos $\mathcal{N} : R \to R$, $\psi : R \to R$ leképezések, melyekre*

$$(\varphi \circ \mathcal{N})(f)(T) = \prod_{\xi \in \mu_p} f(\xi(1+T) - 1)$$

$$(\varphi \circ \psi)(f)(T) = \frac{1}{p} \cdot \sum_{\xi \in \mu_p} f(\xi(1+T) - 1),$$

ahol ψ $\mathbb{Z}_p$-modulus homomorfizmus, $\psi \circ \varphi = 1_R$ az identitás, illetve $\mathcal{N}(fg) = \mathcal{N}(f)\mathcal{N}(g)$. Speciálisan $\mathcal{N}(R^\times) \subseteq R^\times$

2.6. Megjegyzés. R-en a topológiát az $\mathfrak{m} = (p, T)$ maximális ideál hatványai indukálják. Az $\mathcal{N}$ leképezést normának, a ψ leképezést nyomnak hívjuk.

A 2.1. tétel bizonyításának egyik ötlete, hogy $f \in R^\times$, $\mathcal{N}(f) = f$ hatványsort keresünk. Ugyanis ha $f(T) = a_0 + a_1 T + \dots$ ilyen, akkor $a_0 \in \mathbb{Z}_p^\times$, $|\pi_n| < 1$, így $|a_k \pi_n^k| < 1$, ha $k \geq 1$. Tehát

$$|a_0 + a_1\pi_n + \dots + a_k\pi_n^k| = \max(|a_0|, |a_1\pi_n + \dots + a_k\pi_n^k|) = 1$$

mert

$$|a_0| = 1 > \max(|a_1\pi_n|, \dots, |a_k\pi_n^k|) \geq |a_1\pi_n + \dots + a_k\pi_n^k|.$$

Tudjuk, hogy $\mathcal{U}_n$ zárt, ezért $f(\pi_n) \in \mathcal{U}_n$ minden $n \geq 0$-ra. Ha megmutatjuk, hogy $N_{n+1,n}(f(\pi_{n+1})) = f(\pi_n)$, akkor $(f(\pi_n)) \in \mathcal{U}_\infty$. A ζ_{n+1} Galois-konjugáltjait használva

$$N_{n+1,n}(f(\zeta_{n+1} - 1)) = \prod_{\xi \in \mu_p} f(\xi\zeta_{n+1} - 1),$$

illetve $\mathcal{N}(f) = f$-et $\mathcal{N}$ definíciójába beírva

$$\varphi(f)(T) = \prod_{\xi \in \mu_p} f(\xi(1+T) - 1),$$

ugyanakkor φ definíciója miatt viszont $\varphi(f)(\pi_{n+1}) = f(\pi_n)$, azaz valóban $(f(\pi_n)) \in \mathcal{U}_\infty$.

2.7. Lemma. *Tegyük fel, hogy $f \in R^\times$. Ekkor $g = \lim_{k\to\infty} \mathcal{N}^k(f)$ létezik, $g \in R^\times$ és $\mathcal{N}(g) = g$ teljesül.*

Ezt bizonyítani lehet úgy, hogy megmutatjuk, hogy $\mathcal{N}^k(f)$ Cauchy és R teljes topologikus tér. Ezzel már bizonyítani lehet a 2.1. tételt, mert egy $\mathbf{u} \in \mathcal{U}_\infty$-hez választunk minden $n \geq 0$-ra egy $f_n \in R^\times$ hatványsort, amire $f_n(\pi_n) = u_n$. Ekkor a $g_n(T) = \mathcal{N}^n(f_{2n})$ sorozatnak létezik torlódási pontja, mert R kompakt tér, ezt választjuk $f_{\mathbf{u}}(T)$-nek.

A 2.1. tételnél többet is mondhatunk. Legyen $\mathcal{K}_\infty = \mathbb{Q}_p(\mu_{p^\infty})$ és $\mathcal{G} = \mathrm{Gal}(\mathcal{K}_\infty/\mathbb{Q}_p)$. A körosztási karakter $\chi : \mathcal{G} \to \mathbb{Z}_p^\times$, amire $\sigma(\zeta) = \zeta^{\chi(\sigma)}$ teljesül minden $\sigma \in \mathcal{G}$ és $\zeta \in \mu_{p^\infty}$ esetén. $\mathcal{G}$-nek a hatása R-en a következő: legyen $\sigma \in \mathcal{G}$ és $f \in R$, ekkor $(\sigma f)(T) = f((1+T)^{\chi(\sigma)} - 1)$, ahol ha $a \in \mathbb{Z}_p$, akkor egyértelműen írható $a = \sum_{i=0}^\infty a_i p^i$, $a_i \in \{0, 1, \dots, p-1\}$ alakba és $(1+T)^a = \prod_{i=0}^\infty (1+T)^{a_i p^i}$. Ez a csoporthatás $R^\times$-et önmagába képezi, $\varphi(\sigma f) = \sigma(\varphi f)$, és $\mathcal{G}$ hatása felcserélhető az $\mathcal{N}$ és ψ operátorokkal.

Legyen $W = \{f \in R^\times \ : \ \mathcal{N}(f) = f\}$.

2.8. Tétel. *Az $\boldsymbol{u} \mapsto f_{\boldsymbol{u}}(T)$ leképezés egy $\mathcal{G}$-izomorfizmus $\mathcal{U}_\infty$ és W között.*

Definiáljuk a következő részhalmazait R-nek: $R^{\psi=1} = \{f \in R \ : \ \psi(f) = f\}$, $R^{\psi=0} = \{f \in R \ : \ \psi(f) = 0\}$. Teljesül $(1-\varphi)R = TR$. Ebből és ψ definíciójából következik, hogy van egy egzakt sorozatunk:

2.9. Lemma.

$$0 \longrightarrow \mathbb{Z}_p \longrightarrow R^{\psi=1} \xrightarrow{\theta} R^{\psi=0} \longrightarrow \mathbb{Z}_p \longrightarrow 0$$

egzakt sorozat, ahol $\theta(f) = (1-\varphi)(f)$, *a baloldali leképezés a természetes beágyazás, a jobboldali pedig a hatványsor* 0*-beli kiértékelése.*

2.10. Definíció. Legyen $f \in R^{\times}$-re

$$\Delta(f) = (1+T)\frac{f'(T)}{f(T)},$$

ahol $f'(T)$ a formális deriváltat jelöli. Látszik, hogy Δ egy csoporthomomorfizmus $R^{\times}$-ről R additív csoportjába.

2.11. Tétel. *Teljesül* $\Delta(W) = R^{\psi=1}$ *és* $W \cap Ker(\Delta) = \mu_{p-1}$.

Ennek a tételnek a neheze a $\Delta(W) \supseteq R^{\psi=1}$ tartalmazás, amit azzal a trükkel lehet igazolni, hogy modulo p vizsgáljuk a hatványsorokat, azaz áttérünk az $R/pR = \mathbb{F}_p[[T]]$ gyűrűre.

2.12. Lemma. *Minden* $f \in W$ *hatványsorra az*

$$\mathcal{L}(f) := \frac{1}{p}\log\left(\frac{f(T)^p}{\varphi(f)(T)}\right)$$

sorozat R*-ben, sőt* $R^{\psi=0}$*-ban van. Az* $\mathcal{L} : W \to R^{\psi=0}$ *leképezés egy* $\mathcal{G}$*-homomorfizmus.*

2.13. Megjegyzés. Ahogy máskor is, log a hatványsorát jelenti, azaz

$$\log(1+T) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} T^n.$$

Legyen $A = \{\xi(1+T)^a \in R^{\times} \ : \ \xi \in \mu_{p-1}, \ a \in \mathbb{Z}_p\}$ és $D(f) = (1+T)f'(T)$ differenciál operátor.

2.14. Tétel.

$$0 \longrightarrow A \longrightarrow W \xrightarrow{\mathcal{L}} R^{\psi=0} \xrightarrow{\alpha} \mathbb{Z}_p \longrightarrow 0$$

$\mathcal{G}$*-modulusok egzakt sorozata, ahol* $\alpha(f) = (Df)(0)$.

A 2.1. tétel segítségével definiálhatjuk $\mathcal{U}_\infty$ egy elemének logaritmikus deriváltját.

2.15. Definíció. Minden $k \geq 1$-re legyen $\delta_k : \mathcal{U}_\infty \to \mathbb{Z}_p$ logaritmikus derivált homomorfizmus a

$$\delta_k(\mathbf{u}) = \left(D^{k-1}\left(\frac{(1+T)f'_{\mathbf{u}}(T)}{f_{\mathbf{u}}(T)}\right)\right)_{T=0}$$

leképezés, ahol $f_{\mathbf{u}}(T)$ a 2.1. tételből nyert egyértelmű hatványsor, $T=0$ pedig azt jelenti, hogy a 0-ban felvett értékét vesszük. (Ez egy értelmes definíció, mert tudjuk, hogy $f_{\mathbf{u}}(T)$ egység R-ben.)

2.16. Lemma. *Minden $k \geq 1$-re δ_k egy csoporthomomorfizmus, melyre minden $\boldsymbol{u} \in \mathcal{U}_\infty$ és $\sigma \in \mathcal{G}$ esetén $\delta_k(\sigma(\boldsymbol{u})) = \chi(\sigma)^k \delta_k(\boldsymbol{u})$.*

Összekötjük az eddigieket a Riemann-féle zéta-függvénnyel, amit a következő állítás mutat. Legyen $\boldsymbol{\zeta}$ a Riemann-féle zéta-függvény és legyen $\mathbf{c}(a,b) = (c_n(a,b))$, ahol $c_n(a,b) = \frac{\zeta_n^{-a/2} - \zeta_n^{a/2}}{\zeta_n^{-b/2} - \zeta_n^{b/2}}$. Már megmutattuk, hogy $\mathbf{c}(a,b) \in \mathcal{U}_\infty$.

2.17. Állítás. *(i) $\delta_k(\boldsymbol{c}(a,b)) = 0$ ha $k = 1,3,5,\dots$*

(ii) $\delta_k(\boldsymbol{c}(a,b)) = (b^k - a^k)\boldsymbol{\zeta}(1-k)$ ha $k = 2,4,6,\dots$

A bizonyítást egy egyszerű számolás adja a $T = e^z - 1$ változócsere után, mert akkor $D = \frac{d}{dz}$; illetve felhasználva a Bernoulli számok definícióját és hogy $\boldsymbol{\zeta}(1-k) = -\frac{\mathcal{B}_k}{k}$ ha $k = 2,4,6,\dots$.

2.18. Tétel. *$\delta_k(\mathcal{U}_\infty) = \mathbb{Z}_p$ ha $k = 1,2,\dots,p-1$.*

A δ_k homomorfizmus képe egy ideál $\mathbb{Z}_p$-ben, mert ha $\mathbf{u}$, $\mathbf{v} \in \mathcal{U}_\infty$, akkor

$$\delta_k(\mathbf{u}) + \delta_k(\mathbf{v}) = \delta_k(\mathbf{uv}) \in \delta_k(\mathcal{U}_\infty),$$

illetve ha $a \in \mathbb{Z}_p$, akkor létezik egy m pozitív egész szám, amire $m^{-1}a = b \in \mathbb{Z}_p^\times$ és $b \equiv 1 \pmod p$. Létezik b-nek k-dik gyöke $\mathbb{Z}_p^\times$-ben, mert $(1+T)^{1/k}$ hatványsor konvergens $p\mathbb{Z}_p$-n. Mivel $\chi : \mathcal{G} \to \mathbb{Z}_p^\times$ bijekció, ezért létezik $\sigma \in \mathcal{G}$, amire $\chi(\sigma)^k = b$. Ekkor

$$\delta_k(\sigma(\mathbf{u})^m) = m\delta_k(\sigma(\mathbf{u})) = m\chi(\sigma)^k\delta_k(\mathbf{u}) = mb\delta_k(\mathbf{u}) = a\delta_k(\mathbf{u}),$$

azaz $a\delta_k(\mathbf{u}) \in \delta_k(\mathcal{U}_\infty)$ minden $a \in \mathbb{Z}_p$ és $\mathbf{u} \in \mathcal{U}_\infty$-re. Tehát elég egy olyan $\mathbf{u} \in \mathcal{U}_\infty$ egységet mutatni, aminek δ_k-képe egység $\mathbb{Z}_p$-ben. Ezt úgy lehet megmutatni, ha áttérünk az R/pR gyűrűre ahogy ez már korábban egyszer volt.

3. Iwasawa algebrák, p-adikus mértékek

Provéges csoportnak hívunk egy olyan topologikus csoportot, ami diszkrét véges csoportok inverz limesze, vagy ezzel ekvivalensen egy olyan topologikus csoport, ami kompakt, totálisan összefüggéstelen (az összefüggőségi komponensei egyeleműek) és T_0. Ilyenre példa $\mathcal{G} = \mathrm{Gal}(\mathbb{Q}_{\mu_{p^\infty}}/\mathbb{Q}_p) = \varprojlim \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p)$ és $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ additív csoportja. Legyen $\mathfrak{G}$ provéges Abel csoport és $\mathcal{T}_{\mathfrak{G}}$ a nyílt részcsoportjainak halmaza. Mivel $\mathfrak{G}$ kompakt, ezért minden $\mathfrak{H} \in \mathcal{T}_{\mathfrak{G}}$ véges indexű.

3.1. Definíció. Iwasawa algebrának mondjuk a következőt:

$$\Lambda(\mathfrak{G}) = \varprojlim \mathbb{Z}_p[\mathfrak{G}/\mathfrak{H}],$$

ahol $\mathfrak{H}$ végigfut $\mathcal{T}_{\mathfrak{G}}$ elemein. $\mathbb{Z}_p[\mathfrak{G}/\mathfrak{H}]$ a $\mathfrak{G}/\mathfrak{H}$ véges csoport $\mathbb{Z}_p$ feletti csoportgyűrűje. Az áttérési leképezéseket $\mathfrak{H}_1 \supseteq \mathfrak{H}_2$ részcsoportokra a $\mathfrak{G}/\mathfrak{H}_1 \to \mathfrak{G}/\mathfrak{H}_2$, $g + \mathfrak{H}_1 \mapsto g + \mathfrak{H}_2$ szürjektív leképezés lineáris kiterjesztése adja. A $\Lambda(\mathfrak{G})$ Iwasawa algebra egy kompakt topologikus $\mathbb{Z}_p$-algebra ($\mathbb{Z}_p$-modulus és gyűrű), ahol a topológiát a csoportgyűrűkön lévő p-adikus topológia indukálja. (A $\mathbb{Z}_p[\mathfrak{G}/\mathfrak{H}]$ tekinthető a $\mathbb{Q}_p^{|\mathfrak{G}:\mathfrak{H}|}$ végesdimenziós vektortér zárt egységkockájának, a végesdimenziós vektortéren pedig minden norma által indukált topológia megegyezik.)

Legyen $\mathbb{Q}_p$ algebrai lezártjának teljessé tétele $\mathbb{C}_p$. Jelöljük $C(\mathfrak{G}, \mathbb{C}_p)$-vel a folytonos $\mathfrak{G} \to \mathbb{C}_p$ függvények $\mathbb{C}_p$-algebráját. Lássuk el $C(\mathfrak{G}, \mathbb{C}_p)$ teret a szuprémum normával, azaz legyen $\|f\| = \sup_{g \in \mathfrak{G}} |f(g)|_p$, így $C(\mathfrak{G}, \mathbb{C}_p)$ egy $\mathbb{C}_p$-Banach-tér. Azt mondjuk, hogy $f \in C(\mathfrak{G}, \mathbb{C}_p)$ lokálisan konstans, ha létezik $\mathfrak{H}$ részcsoportja $\mathfrak{G}$-nek, amire $f(g) = f(h)$ ha $g - h \in \mathfrak{H}$, jelöljük ezen függvények halmazát $\mathrm{Step}(\mathfrak{G})$-vel. Tehát az ilyen függvények adnak egy $\mathfrak{G}/\mathfrak{H} \to \mathbb{C}_p$ függvényt. Teljesül, hogy $\mathrm{Step}(\mathfrak{G})$ mindenhol sűrű $C(\mathfrak{G}, \mathbb{C}_p)$-ben, azaz minden $f \in C(\mathfrak{G}, \mathbb{C}_p)$ és $\varepsilon > 0$-ra létezik $g \in \mathrm{Step}(\mathfrak{G})$, hogy $\|f - g\| < \varepsilon$.

Legyen $\lambda \in \Lambda(\mathfrak{G})$ tetszőleges elem, $f \in \mathrm{Step}(\mathfrak{G})$ lokálisan konstans a $\mathfrak{H}$ részcsoporttal. Legyen $\lambda_{\mathfrak{H}}$ a λ képe $\mathbb{Z}_p[\mathfrak{G}/\mathfrak{H}]$-ban, tehát valamilyen $c_{\mathfrak{H}}(x) \in \mathbb{Z}_p$ együtthatókra

$$\lambda_{\mathfrak{H}} = \sum_{x \in \mathfrak{G}/\mathfrak{H}} c_{\mathfrak{H}}(x) x.$$

Vezessük be a következő jelölést:

$$\int_{\mathfrak{G}} f d\lambda = \sum_{x \in \mathfrak{G}/\mathfrak{H}} c_{\mathfrak{H}}(x) f(x).$$

Ez a definíció független $\mathfrak{H}$ választásától és mivel $c_{\mathfrak{H}}(x) \in \mathbb{Z}_p$, ezért

$$\left| \int_{\mathfrak{G}} f d\lambda \right| \leq \|f\|.$$

Ha ε_x a karakterisztikus függvénye az $x \in \mathfrak{G}/\mathfrak{H}$ mellékosztálynak, akkor

$$\int_{\mathfrak{G}} \varepsilon_x d\lambda = c_{\mathfrak{H}}(x).$$

Ha f nem lokálisan konstans, akkor választható egy f_n függvénysorozat $\mathrm{Step}(\mathfrak{G})$-ben, ami f-hez tart és ekkor $\int_{\mathfrak{G}} f_n d\lambda$ Cauchy sorozat $\mathbb{C}_p$-ben, tehát konvergens, legyen

$$\int_{\mathfrak{G}} f d\lambda = \lim_{n \to \infty} \int_{\mathfrak{G}} f_n d\lambda.$$

Használva azt a jelölést, hogy $M_\lambda(f) = \int_{\mathfrak{G}} f d\lambda$ egy olyan lineáris funkcionált kapunk $C(\mathfrak{G}, \mathbb{C}_p)$-n, amire teljesül $|M_\lambda(f)|_p \leq \|f\|$. A karakterisztikus függvényre vonatkozó megjegyzésből következik, hogy ha $M_{\lambda_1} = M_{\lambda_2}$, akkor $\lambda_1 = \lambda_2$, illetve ha $f(\mathfrak{G}) \subseteq \mathbb{Q}_p$, akkor $M_\lambda(f) \in \mathbb{Q}_p$. Egy fontos gondolat ennek a megfordítása. Tegyük fel, hogy $L(f)$ lineáris funkcionál $C(\mathfrak{G}, \mathbb{C}_p)$-n, amire $|L(f)|_p \leq \|f\|$ és ha $f(\mathfrak{G}) \subseteq \mathbb{Q}_p$, akkor $L(f) \in \mathbb{Q}_p$. Minden $\mathfrak{H}$ részcsoportra és $x \in \mathfrak{G}/\mathfrak{H}$ mellékosztályra legyen $c_{\mathfrak{H}}(x) = L(\varepsilon_x)$. Az ezekkel az együtthatókkal felépített λ olyan Iwasawa-algebrabeli elem lesz, amire $M_\lambda = L$.

Néhány további tulajdonsága ennek az integrálásnak:

- Ha $\lambda = g \in \mathfrak{G}$, akkor dg a Dirac mérték, azaz $\int_{\mathfrak{G}} f dg = f(g)$.
- $\int_{\mathfrak{G}} f(x) d(\lambda_1 \lambda_2)(x) = \int_{\mathfrak{G}} (\int_{\mathfrak{G}} f(x + y) d\lambda_1(x)) d\lambda_2(y)$, ahol $\lambda_1 \lambda_2$ a szorzat a $\Lambda(\mathfrak{G})$ Iwasawa-algebrában.
- Ha $\nu : \mathfrak{G} \to \mathbb{C}_p^\times$ folytonos csoporthomomorfizmus, akkor ν kiterjeszthető egy folytonos $\Lambda(\mathfrak{G}) \to \mathbb{C}_p$ algebra homomorfizmussá a $\nu(\lambda) = \int_{\mathfrak{G}} \nu d\lambda$ képlettel.

Legyen S a $\Lambda(\mathfrak{G})$ azon elemeinek halmaza, amik nem nullosztók. Ekkor S multiplikatívan zárt, legyen $Q(\mathfrak{G}) = S^{-1}\Lambda(\mathfrak{G})$ lokalizáltja az Iwasawa-algebrának. Azt mondjuk, hogy $\lambda \in Q(\mathfrak{G})$ pszeudomérték $\mathfrak{G}$-n, ha $(g-1)\lambda \in \Lambda(\mathfrak{G})$ minden $g \in \mathfrak{G}$-re. Tegyük fel, hogy λ pszeudomérték és legyen $\nu : \mathfrak{G} \to \mathbb{C}_p^\times$ folytonos csoporthomomorfizmus, ami nem a konstans 1 függvény. Legyen

$$\int_{\mathfrak{G}} \nu d\lambda = \frac{\int_{\mathfrak{G}} \nu d((g-1)\lambda)}{\nu(g)-1},$$

ahol g tetszőleges olyan eleme $\mathfrak{G}$-nek, amire $\nu(g) \neq 1$. (Független g választásától.)

Mostantól konkrét provéges csoportokat vizsgálunk, amiket összekötünk a korábbi hatványsorokkal. Legyen $\binom{x}{n} = 1$, ha $n = 0$ és $\binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!}$ ha $n \geq 1$.

3.2. Tétel (Mahler). *Legyen $f : \mathbb{Z}_p \to \mathbb{C}_p$ folytonos függvény. Ekkor f egyértelműen írható*

$$f(x) = \sum_{n=0}^{\infty} a_n \binom{x}{n}$$

alakba, ahol $a_n \in \mathbb{C}_p$ és $\lim_{n\to\infty} a_n = 0$.

Az a_n együtthatókat $a_n = (\nabla^n f)(0)$ adja meg, ahol $\nabla f(x) = f(x+1) - f(x)$. Mivel $\left|\binom{x}{n}\right|_p \leq 1$ minden $x \in \mathbb{Z}_p$-re, ezért $\|f\| = \sup|a_n|_p$ és minden $\lambda \in \Lambda(\mathbb{Z}_p)$-re $c_n(\lambda) = \int_{\mathbb{Z}_p} \binom{x}{n} d\lambda$ $\mathbb{Z}_p$-ben van.

3.3. Definíció. A Mahler transzformált a következő $\mathcal{M} : \Lambda(\mathbb{Z}_p) \to R$ leképezés

$$\mathcal{M}(\lambda) = \sum_{n=0}^{\infty} c_n(\lambda) T^n.$$

3.4. Tétel. *$\mathcal{M} : \Lambda(\mathbb{Z}_p) \to R$ egy $\mathbb{Z}_p$-algebra izomorfizmus.*

A Mahler transzformált inverzének megkonstruálásánál azt a fontos gondolatot használjuk, hogy bizonyos lineáris funkcionálokhoz egyértelműen létezik Iwasawa-algebrabeli elem, amivel az integrálás éppen a funkcionál.

3.5. Lemma. *$\mathcal{M}(1_{\mathbb{Z}_p}) = 1 + T$, ahol $1_{\mathbb{Z}_p}$ a $\mathbb{Z}_p$ egységeleme.*

$\mathbb{Z}_p^\times$ nem részcsoportja $\mathbb{Z}_p$ additív csoportjának, mégis beágyazzuk $\Lambda(\mathbb{Z}_p^\times)$-t $\Lambda(\mathbb{Z}_p)$-be. Vegyük észre, hogy $\mathbb{Z}_p^\times$ nyílt és zárt is $\mathbb{Z}_p$-ben, ezért kompakt, mert kompakt zárt része, és totálisan összefüggéstelen is, mert nyílt. Illetve ha ε a $\mathbb{Z}_p^\times$ karakterisztikus függvénye, akkor ε folytonos és minden $\lambda \in \Lambda(\mathbb{Z}_p)$-re definiálhatunk egy $L(f) = \int_{\mathbb{Z}_p} f\varepsilon d\lambda$ funkcionált $C(\mathbb{Z}_p, \mathbb{C}_p)$-n, amire $|L(f)|_p \leq \|f\|$. Tehát egyértelműen létezik $\#(\lambda) \in \Lambda(\mathbb{Z}_p)$, amire $L = M_{\#(\lambda)}$. Ahhoz, hogy ez a leképezés érthetőbb, sőt számolható legyen, definiáljuk a következő $\mathcal{S} : R \to R$ operátort:

$$\mathcal{S}(g(T)) = g(T) - \frac{1}{p} \sum_{\xi \mu_p} g(\xi(1+T) - 1),$$

azaz $\mathcal{S} = 1_R - \varphi \circ \psi$, ahol 1_R az identikus leképezés.

3.6. Lemma. *Minden $\lambda \in \Lambda(\mathbb{Z}_p)$-re $\mathcal{S}(\mathcal{M}(\lambda)) = \mathcal{M}(\#(\lambda))$. Speciálisan $\#(\lambda) = \lambda$ akkor és csak akkor, ha $\mathcal{S}(\mathcal{M}(\lambda)) = \mathcal{M}(\lambda)$, vagy ekvivalensen, ha $\mathcal{M}(\lambda) \in R^{\psi=0}$.*

Definiálhatjuk az $i : \Lambda(\mathbb{Z}_p^\times) \to \Lambda(\mathbb{Z}_p)$ beágyazást az

$$\int_{\mathbb{Z}_p} f d(i(\eta)) = \int_{\mathbb{Z}_p^\times} f|_{\mathbb{Z}_p^\times} d\eta$$

egyenlőséggel, ahol f végigfut az összes $C(\mathbb{Z}_p, \mathbb{C}_p)$ függvényen és $f|_{\mathbb{Z}_p}$ az f megszorítása $\mathbb{Z}_p^\times$-re, hiszen a jobboldali formula egy olyan $C(\mathbb{Z}_p, \mathbb{C}_p) \to \mathbb{C}_p$ funkcionált ad meg, amihez egyértelműen létezik $i(\eta) \in \Lambda(\mathbb{Z}_p)$.

3.7. Lemma. *Teljesül $i(\Lambda(\mathbb{Z}_p^\times)) = \{\lambda \in \Lambda(\mathbb{Z}_p) \ : \ \#(\lambda) = \lambda\}$. Speciálisan ezért $\mathcal{M}(i(\Lambda(\mathbb{Z}_p^\times))) = R^{\psi=0}$.*

Emiatt élhetünk azzal a konvencióval, hogy $\Lambda(\mathbb{Z}_p^\times)$ az a részhalmaza $\Lambda(\mathbb{Z}_p)$-nek, amelyekre $\#(\lambda) = \lambda$.

Mutatunk egy nagyon fontos egzakt sorozatot, ami a 2.14. tétel átfogalmazása a Mahler transzformált és $\Lambda(\mathbb{Z}_p^\times)$ segítségével. Először definiáljuk $\mathcal{G}$ hatását $\Lambda(\mathbb{Z}_p)$-n: $g \cdot (a_{\mathbb{Z}_p}) = (\chi(g) \cdot a)_{\mathbb{Z}_p}$ minden $a \in \mathbb{Z}_p$-re, ahol $a_{\mathbb{Z}_p}$ azt jelöli, hogy $\mathbb{Z}_p \subset \Lambda(\mathbb{Z}_p)$-ben tekintjük a-t. Linearitással és folytonossággal ez a hatás kiterjed $\Lambda(\mathbb{Z}_p)$-re, és ekkor $\Lambda(\mathbb{Z}_p^\times)$ egy $\mathcal{G}$-részmodulus. Mivel $\mathcal{M}(1_{\mathbb{Z}_p}) = 1 + T$, ezért $\mathcal{M}$ egy $\mathcal{G}$-izomorfizmus $\Lambda(\mathbb{Z}_p)$ és R között. A $\chi : \mathcal{G} \simeq \mathbb{Z}_p^\times$ körosztási karakter kiterjed egy

$$\tilde{\chi} : \Lambda(\mathcal{G}) \simeq \Lambda(\mathbb{Z}_p^\times)$$

$\mathcal{G}$-izomorfizmussá. Összerakva a két izomorfizmust, adódik egy

$$\tilde{\mathcal{M}} = \mathcal{M} \circ \tilde{\chi} : \Lambda(\mathcal{G}) \simeq R^{\psi=0}$$

$\mathcal{G}$-izomorfizmus. Szükség van még a következő $\tilde{\mathcal{L}} : \mathcal{U}_\infty \to \Lambda(\mathcal{G})$ leképezésre is:

$$\tilde{\mathcal{L}}(\mathbf{u}) = \tilde{\mathcal{M}}^{-1}(\mathcal{L}(f_\mathbf{u})),$$

ahol $f_\mathbf{u}$ a 2.1. tételbeli hatványsor. Használva a $\tilde{\chi}$ izomorfizmust adódik, hogy

$$\int_{\mathcal{G}} \binom{\chi(g)}{n} d\tilde{\mathcal{L}}(\mathbf{u}) = \int_{\mathbb{Z}_p^\times} \binom{x}{n} d(\tilde{\chi}(\tilde{\mathcal{L}}(\mathbf{u})),$$

tehát a Mahler transzformált definíciója miatt

$$\mathcal{L}(f_\mathbf{u}) = \mathcal{M}(\tilde{\chi}(\tilde{\mathcal{L}}(\mathbf{u}))) = \sum_{n=0}^{\infty} T^n \int_{\mathcal{G}} \binom{\chi(g)}{n} d\tilde{\mathcal{L}}(\mathbf{u}).$$

3.8. Tétel. *Egzakt sorozata $\mathcal{G}$-modulusoknak a következő:*

$$0 \longrightarrow \mu_{p-1} \times T_p(\mu) \longrightarrow \mathcal{U}_\infty \xrightarrow{\tilde{\mathcal{L}}} \Lambda(\mathcal{G}) \xrightarrow{\beta} T_p(\mu) \longrightarrow 0,$$

ahol $T_p(\mu) = \varprojlim \mu_{p^{n+1}}$ és az áttérési leképezések a p-edik hatványra emelés. A baloldali leképezés a természetes beágyazás, ami egy $(x, a) \in \mu_{p-1} \times T_p(\mu)$ párhoz $xa \in \mathcal{U}_\infty$-t rendeli. A β leképezést pedig a $\beta(\lambda) = (\zeta_n)^{\int_{\mathcal{G}} \chi d\lambda}$ képlet adja.

A 2.14. tételbeli α és az itteni β leképezéseket a következő lemma segít összehasonlítani:

3.9. Lemma. *Minden $g \in R$ hatványsorra és $k \geq 0$ egészre teljesül*

$$\int_{\mathbb{Z}_p} x^k d(\mathcal{M}^{-1}(g(T))) = (D^k g(T))_{T=0}.$$

Ezt a lemmát ugyancsak azzal a trükkel lehet bizonyítani, hogy bizonyos lineáris funkcionálok valamilyen Iwasawa-algebrabeli elemek szerinti integrálások. A lemmának következménye a következő állítás is:

3.10. Állítás. *Minden $k \geq 1$ és $\boldsymbol{u} \in \mathcal{U}_\infty$-re*

$$\int_{\mathcal{G}} \chi(g)^k d\tilde{\mathcal{L}}(\boldsymbol{u}) = (1 - p^{k-1})\delta_k(\boldsymbol{u}).$$

Megmutatható a lemma használatával a következő javítása is a 2.18. tételnek.

3.11. Állítás. *Legyen $k \geq 1$ egész.*

$$\delta_k(\mathcal{U}_\infty) = \begin{cases} \mathbb{Z}_p, & \text{ha } k = 1 \text{ vagy } k \not\equiv 1 \pmod{p-1}, \\ p^m \mathbb{Z}_p, & \text{ha } k > 1 \text{ és } k \equiv 1 \pmod{p-1}, \text{ ahol } m = 1 + ord_p(k-1). \end{cases}$$

$ord_p(k-1)$ a $k-1$ szám rendje modulo p.

Hivatkozások

[1] J. Coates and R. Sujatha. *Cyclotomic Fields and Zeta Values.* Springer Monographs in Mathematics. Springer Berlin Heidelberg, 2006.