Iwasawa-elmélet
Egyéni kutatómunka 2

Márton Dénes

1. Bevezetés, előzmények

A kutatómunkám az első folytatása volt, azaz John Coates és Sujatha Ramdorai Cyclotomic Fields and Zeta Values c. könyvének [1] folytatása a negyedik, ötödik és hatodik fejezetekkel. Az egész könyv legfontosabb célja a fő sejtés "legegyszerűbb" bizonyításának prezentálása, amire a hatodik fejezetben kerül sor. Ehhez szükséges Euler rendszerek használta, - amik definiálása és tanulmányozása az ötödik fejezetet teszik ki, - illetve Iwasawa tétele, aminek a kimondásához és bizonyításához a módszereket az első kutatómunkám során taglalt második és harmadik fejezetek tartalmazzák.

A legfontosabb jelöléseket, definíciókat és tételt megismétlem a második és harmadik fejezetekből, azaz az első kutatómunkámból.

Rögzítsünk egy p páratlan prímet az egész beszámoló során és az n természetes számokra jelöljék $\mathcal{K}_n = \mathbb{Q}_p(\mu_{p^{n+1}})$ lokális testeket, ahol $\mu_{p^{n+1}}$ a p^{n+1}-dik egységgyökök halmaza. Hasonlóan $\mu_{p^\infty} = \bigcup \mu_{p^{n+1}}$ a p-hatványadik egységgyökök halmaza. Rögzítsük a $\mu_{p^{n+1}}$ csoportok olyan ζ_n generátorait, melyekre $\zeta_{n+1}^p = \zeta_n$ és legyen $\pi_n = \zeta_n - 1$. A $\mathcal{K}_n$ test egészeinek gyűrűjének egységeit jelölje $\mathcal{U}_n$. Vezessük még be továbbá az

$$\mathcal{U}_\infty = \varprojlim \mathcal{U}_n \text{ és } \mathcal{G} = \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p) = \varprojlim \mathrm{Gal}(\mathcal{K}_n/\mathbb{Q}_p)$$

jelöléseket.

A $\mathfrak{G}$ provéges Abel csoport *Iwasawa algebrájának* hívjuk a $\Lambda(\mathfrak{G}) = \varprojlim \mathbb{Z}_p[\mathfrak{G}/\mathfrak{H}]$ $\mathbb{Z}_p$-algebrát, ahol $\mathfrak{H}$ a $\mathfrak{G}$ nyílt részcsoportjain fut végig. Jelölje $Q(\mathfrak{G})$ a $\Lambda(\mathfrak{G})$ Iwasawa algebra teljes hányadosgyűrűjét. Azt mondjuk, hogy $\lambda \in Q(\mathfrak{G})$ egy *pszeudomérték* $\mathfrak{G}$-n, ha $(g-1)\lambda \in \Lambda(\mathfrak{G})$ minden $g \in \mathfrak{G}$-re.

Iwasawa tételének bizonyításához szükséges legfontosabb tétel az első kutatómunkámból:

1.1. Tétel. *Léteznek leképezések, melyekkel*

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

egzakt sorozat, ahol $T_p(\mu) = \varprojlim \mu_{p^{n+1}}$.

2. Iwasawa tétele

Vezessük be a jelöléseket a lokális eset után a globális esetre is. Legyen $\mathcal{F}_\infty = \mathbb{Q}(\mu_{p^\infty})$ és $F_\infty = \mathcal{F}_\infty^+$ a legnagyobb valós részteste. Legyen

$$\mathcal{G} = \mathrm{Gal}(\mathcal{F}_\infty/\mathbb{Q}) \text{ és } G = \mathrm{Gal}(F_\infty/\mathbb{Q}).$$

Vegyük észre, hogy $\mathcal{G}$ izomorf a bevezetésben definiált csoporttal. Ha

$$J = \{1, \iota\} = \mathrm{Gal}(\mathcal{F}_\infty / F_\infty),$$

azaz ι a konjugálás, akkor

$$\Lambda(\mathcal{G}) = \Lambda(\mathcal{G})^+ \oplus \Lambda(\mathcal{G})^-,$$

ahol $\Lambda(\mathcal{G})^+ = \frac{1+\iota}{2}\Lambda(\mathcal{G})$ és $\Lambda(\mathcal{G})^- = \frac{1-\iota}{2}\Lambda(\mathcal{G})$, mert p páratlan, így 2-vel oszthatunk $\mathbb{Z}_p$-ben. A természetes $\Lambda(\mathcal{G}) \twoheadrightarrow \Lambda(G)$ szürjekció megszorítása $\Lambda(\mathcal{G})^+$-ra indukál egy $\Lambda(\mathcal{G})^+ \simeq \Lambda(G)$ izomorfizmust, ezért tekinthetjük $\Lambda(G)$-t a $\Lambda(\mathcal{G})$ $\Lambda(\mathcal{G})^+$-nak megfelelő részalgebrájának. Hasonlóan

$$Q(\mathcal{G}) = Q(\mathcal{G})^+ \oplus Q(\mathcal{G})^-$$

és a pszeudomértékeket G-n megfeleltethetjük azon pszeudomértékeknek $\mathcal{G}$-n, melyek $Q(\mathcal{G})^+$-ban vannak.

2.1. Tétel. *Létezik egyetlen $\boldsymbol{\zeta}_p$ pszeudomérték G-n, amire*

$$\int_G \chi(g)^k d\boldsymbol{\zeta}_p = (1 - p^{k-1})\boldsymbol{\zeta}(1-k)$$

teljesül minden páros $k \geq 2$ számra, ahol $\boldsymbol{\zeta}$ a Riemann-féle zéta-függvény.

Iwasawa tételének másik feléhez körosztási egységek kellenek. Legyenek a természetes számokra $\mathcal{F}_n = \mathbb{Q}(\mu_{p^{n+1}})$ és $F_n = \mathcal{F}_n^+$ a legnagyobb valós részteste. Jelölje $\mathcal{D}_n$ az $\mathcal{F}_n$ egészeinek gyűrűjében az egységek metszetét $\mathcal{F}_n^\times$ azon részcsoportjával, amit a $\sigma(\pi_n)$-ek generálnak, ahol σ végigfut $\mathrm{Gal}(\mathcal{F}_n/\mathbb{Q})$ elemein. Továbbá legyen $D_n = \mathcal{D}_n \cap F_n$. Ekkor D_n-et generálják $\pm c_n(e, 1)$ Galois-konjugáltjai, ahol

$$c_n(e,1) = \frac{\zeta_n^{-e/2} - \zeta_n^{e/2}}{\zeta_n^{-1/2} - \zeta_n^{1/2}},$$

ahol e olyan primitív gyök modulo p, melyre $e^{p-1} \not\equiv 1 \mod p^2$.

Ha A egy részhalmaza $\mathcal{K}_n$-nek vagy $K_n = \mathcal{K}_n^+$-nak, ahol $\mathcal{K}_n^+$ az a részteste $\mathcal{K}_n$-nek, amin a konjugálás triviálisan hat, akkor $\overline{A}$ jelölje a lezártját a p-adikus topológiában. Legyen $\mathcal{C}_n = \overline{\mathcal{D}}_n$ és $C_n = \overline{D}_n$. A $\mathcal{K}_n$ egészeinek gyűrűjének maximális ideálja legyen $\mathfrak{p}_n$, a K_n egészeinek gyűrűjének egységei pedig U_n. Az $\mathcal{U}_n$ és U_n nem $\mathbb{Z}_p$-modulusok, ezért bevezetjük azt a jelölést, hogy $\mathcal{U}_n^1 = \{x \in \mathcal{U}_n : x \equiv 1 \mod \mathfrak{p}_n\}$, illetve általában egy $Z \leq \mathcal{U}_n$ részcsoportra $Z^1 = Z \cap \mathcal{U}_n^1$. Így $\mathcal{U}_n^1$ és U_n^1 csoportok (a művelet a szorzás) már $\mathbb{Z}_p$-modulusok, ahol $a \in \mathbb{Z}_p$ hatása egy $x \in \mathcal{U}_n^1$ vagy $x \in U_n^1$ elemen az x^a hatványozás. (Ez értelmes, mert $x = 1 + y$, ahol $y \in \mathfrak{p}_n$ és $x^a = (1+y)^a = \sum_{k=0}^\infty \binom{a}{k} y^k$ konvergens, mert $|y|_p < 1$ és $|\binom{a}{k}|_p \leq 1$. Mivel a hatványsor $k = 0$-ra 1-gyel kezdődik, ezért minden véges összegre $|\sum_{k=0}^N \binom{a}{k} y^k|_p = \max\{|1|_p, |\sum_{k=1}^N \binom{a}{k} y^k|_p\} = 1$, mert a második tagból y kiemelhető, így annak abszolútértéke 1-nél kisebb. Tehát $\sum_{k=0}^N \binom{a}{k} y^k$ egység, amiknek a halmaza zárt, vagyis x^a is egység. Továbbá az is igaz, hogy $x^a - 1 = \sum_{k=1}^\infty \binom{a}{k} y^k = y \lim_{N\to\infty} \sum_{k=0}^N \binom{a}{k+1} y^k$, ahol $|\sum_{k=0}^N \binom{a}{k+1} y^k|_p \leq 1$, azaz benne van az egészek gyűrűjében, ami szintén zárt, vagyis $\sum_{k=0}^\infty \binom{a}{k+1} y^k$ is benne van. De mivel $y \in \mathfrak{p}_n$, ezért szintén $x^a - 1 \in \mathfrak{p}_n$, vagyis $x^a \in \mathcal{U}_n^1$ vagy $x \in U_n^1$.)

Hasonlóan C_n^1 is $\mathbb{Z}_p$-modulus, ráadásul U_n^1 és C_n^1 is kompaktak. Tehát

$$U_\infty^1 = \varprojlim U_n^1 \text{ és } C_\infty^1 = \varprojlim C_n^1,$$

- ahol az összekötő leképezéseket a norma függvények adják, - szintén kompakt $\mathbb{Z}_p$-modulusok. A $G = \varprojlim \mathrm{Gal}(F_n/\mathbb{Q}) = \varprojlim \mathrm{Gal}(K_n/\mathbb{Q}_p)$ csoport folytonosan hat U^1_∞-en és C^1_∞-en. Ekkor U^1_∞ és C^1_∞ ellátható egy $\Lambda(G)$-modulus struktúrával a következőképpen:

Legyen M kompakt $\mathbb{Z}_p$-modulus, amin G folytonosan hat. Jelölje a *Pontrjagin duálisát* $M^D = \{M \to \mathbb{Q}_p/\mathbb{Z}_p$ folytonos homomorfizmus$\}$, ahol $\mathbb{Q}_p/\mathbb{Z}_p$ diszkrét $\mathbb{Z}_p$-modulus. Egy $H \leq G$ nyílt részcsoportra legyen a *H-invariánsok* halmaza M^H, azaz a legnagyobb részmodulusa M-nek, amit H fixen hagy és a *H-koinvariánsok* halmaza M_H, azaz a legnagyobb faktora M-nek, amit H fixen hagy. Ekkor

$$M^D = \bigcup_{H \leq G \text{ nyílt}} (M^D)^H,$$

mert M^D diszkrét G-modulus. Ennek Pontrjagin duálisát véve és felhasználva, hogy $(M^D)^H$ duálisa M_H-nak és azt, hogy a Pontrjagin dualitás megcseréli a direkt limeszt és az inverz limeszt, kapjuk hogy

$$M = \varprojlim M_H.$$

Ezen már tudjuk definiálni $\Lambda(G) = \varprojlim \mathbb{Z}_p[G/H]$ hatását.

Kimondhatjuk Iwasawa tételét:

2.2. Tétel (Iwasawa)**.** *Az U^1_∞/C^1_∞ $\Lambda(G)$-modulus kanonikusan izomorf a $\Lambda(G)/I(G)\boldsymbol{\zeta}_p$ modulussal, ahol $I(G)$ az augmentációs ideál.*

2.3. Megjegyzés. Az augmentációs ideált $\{g - 1 : g \in G\}$ generálja, tehát $I(G)\boldsymbol{\zeta}_p$ valóban ideál, mert $\boldsymbol{\zeta}_p$ pszeudomérték.

A bizonyítás vázlata az 1.1. tételben szereplő egzakt sorozat átírása

$$0 \longrightarrow T_p(\mu) \longrightarrow \mathcal{U}^1_\infty \longrightarrow \Lambda(\mathcal{G}) \longrightarrow T_p(\mu) \longrightarrow 0$$

alakba, mert $\mathcal{U}_\infty = \mu_{p-1} \times \mathcal{U}^1_\infty$. Ezután J-invariánsokat véve kapunk egy $U^1_\infty \simeq \Lambda(G)$ izomorfizmust. C^1_∞-et és $I(G)\boldsymbol{\zeta}_p$-t az segít összehasonlítani, hogy a $c_n(e,1)$-ek segítségével megmutatható, hogy C^1_∞ ciklikus modulus és $\boldsymbol{\zeta}_p$ is ezek segítségével volt definiálva.

3. Fő sejtés

Térjünk át a fő sejtésre, amit valójában már bizonyítottak. Legyen M_∞ a maximális kommutatív p-bővítése F_∞-nek, ami elágazásmentes a p fölötti egyetlen prímideálon kívül. Legyen

$$X_\infty = \mathrm{Gal}(M_\infty/F_\infty).$$

X_∞ definíció szerint egy kommutatív *pro-p csoport*, azaz véges p-csoportok inverz limesze. X_∞ egy kompakt $\mathbb{Z}_p$-modulus, amit el tudunk látni egy folytonos G-hatással. Legyen $g \in G$ és $x \in X_\infty$. Válasszunk egy tetszőleges $\tilde{g} \in \mathrm{Gal}(M_\infty/\mathbb{Q})$ felemeltet g-hez, majd definiáljuk g hatását x-en úgy, mint

$$g.x = \tilde{g}x\tilde{g}^{-1}.$$

Ez független $\tilde{g}$ választásától. Ahogy már korábban is volt, G hatása X_∞-en kiterjed lineárisan és folytonosan és így X_∞ egy $\Lambda(G)$-modulus lesz.

Bár a fő sejtés kimondásához nincs rá szükség, de a bizonyításához igen, ezért definiálunk egy másik modulust is. Legyen L_∞ a maximális kommutatív p-bővítése F_∞-nek, ami mindenhol elágazásmentes. Hasonlóan

$$Y_\infty = \mathrm{Gal}(L_\infty/F_\infty)$$

szintén ellátható egy $\Lambda(G)$-modulus struktúrával.

Legyen V_n az F_n egészeinek gyűrűjének egységei, illetve $E_n = \overline{V}_n$. Hasonlóan a korábbiakhoz, $E^1_\infty = \varprojlim E^1_n$ szintén $\Lambda(G)$-modulus.

Globális osztálytest-elméletre hivatkozva bizonyítható, hogy

$$0 \longrightarrow E^1_\infty \longrightarrow U^1_\infty \longrightarrow \mathrm{Gal}(M_\infty/L_\infty) \longrightarrow 0 \tag{3.1}$$

egzakt sorozat, amiből következik, hogy:

3.1. Tétel (Fundamentális egzakt sorozat)**.** *$\Lambda(G)$-modulusok egzakt sorozata a következő:*

$$0 \longrightarrow E^1_\infty/C^1_\infty \longrightarrow U^1_\infty/C^1_\infty \longrightarrow X_\infty \longrightarrow Y_\infty \longrightarrow 0.$$

A fő sejtés kimondásához még szükség van a (G-)karakterisztikus ideál fogalmára. Azt mondjuk, hogy egy M $\Lambda(G)$-modulus $\Lambda(G)$*-torzió*, ha M minden elemét annulálja $\Lambda(G)$ egy olyan eleme, ami nem nullosztó.

3.2. Állítás. *Legyen M egy végesen generált $\Lambda(G)$-torzió $\Lambda(G)$-modulus. Ekkor létezik egy egzakt sorozat*

$$0 \longrightarrow \bigoplus_{i=1}^{h} \frac{\Lambda(G)}{\Lambda(G)f_i} \longrightarrow M \longrightarrow Q \longrightarrow 0,$$

ahol $f_1, \ldots, f_h$ nem nullosztók $\Lambda(G)$-ben, Q pedig egy véges számosságú $\Lambda(G)$-modulus.

Az M modulus *G-karakterisztikus ideáljának* hívjuk az $f_1 \ldots f_h$ szorzat által generált főideált $\Lambda(G)$-ben, amit $\mathrm{ch}_G(M)$-mel jelölünk. Ez az ideál csak M-től függ, az egzakt sorozattól nem.

3.3. Állítás. *Az összes $\Lambda(G)$-modulus, ami a fundamentális egzakt sorozatban szerepel végesen generált és torzió.*

3.4. Tétel (Fő sejtés)**.** *Teljesül*

$$ch_G(X_\infty) = I(G)\boldsymbol{\zeta}_p.$$

Felhasználva, hogy a karakterisztikus ideál multiplikatív abban az értelemben, hogy ha végesen generált torzió $\Lambda(G)$-modulusok egzakt sorozata

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0,$$

akkor $\mathrm{ch}_G(M_2) = \mathrm{ch}_G(M_1)\mathrm{ch}_G(M_3)$, illetve a fundamentális egzakt sorozatot, megkaphatjuk, hogy a fő sejtés ekvivalens azzal, hogy $\mathrm{ch}_G(E^1_\infty/C^1_\infty) = \mathrm{ch}_G(Y_\infty)$, mivel Iwasawa tétele miatt $U^1_\infty/C^1_\infty \simeq \Lambda(G)/I(G)\boldsymbol{\zeta}_p$. A bizonyítása a fő sejtésnek ez utóbbi egyenlőség igazolása. A már kiszámolt esetekben valójában több is igaz.

3.5. Állítás. *Ha $F_0 = \mathbb{Q}(\mu_p)^+$ osztályszáma relatív p-hez, akkor*

$$E^1_\infty/C^1_\infty = Y_\infty = 0.$$

Ez minden ismert esetben teljesül és ekkor természetesen a G-karakterisztikus ideáljuk is megegyezik (mindkettő az egész $\Lambda(G)$), illetve a fundamentális egzakt sorozat és Iwasawa tétele miatt $X_\infty \simeq \Lambda(G)/I(G)\boldsymbol{\zeta}_p$ is igaz.

Felvázoljuk $\mathrm{ch}_G(E^1_\infty/C^1_\infty) = \mathrm{ch}_G(Y_\infty)$ bizonyítását. Legyen $\mathcal{L}^1 : U^1_\infty \simeq \Lambda(G)$ az Iwasawa tétel bizonyításában szereplő izomorfizmus. Bizonyítható, hogy $\mathcal{L}^1(E^1_\infty)$ főideál $\Lambda(G)$-ben, felhasználva a (3.1) egzakt sorozatot, és Iwasawa azon eredményét, hogy X_∞-nek nincs nemnulla véges $\Lambda(\Gamma_0)$-részmodulusa, ahol $\Gamma_0 = \mathrm{Gal}(F_\infty/F_0)$. Tehát valamilyen $\alpha \in \Lambda(G)$-re $\mathcal{L}^1(E^1_\infty) = \alpha\Lambda(G)$. Mivel C^1_∞ ciklikus modulus, ezért $\mathcal{L}^1(C^1_\infty) = I(G)\boldsymbol{\zeta}_p$ főideál. C^1_∞ részhalmaza E^1_∞-nek, tehát $\mathcal{L}^1(C^1_\infty) = I(G)\boldsymbol{\zeta}_p$ is részhalmaza $\mathcal{L}^1(E^1_\infty) = \alpha\Lambda(G)$-nek, így $I(G)\boldsymbol{\zeta}_p$ generátora előáll $\alpha\beta$ alakban valamilyen $\beta \in \Lambda(G)$-re. De ekkor az Iwasawa tétel $U^1_\infty/C^1_\infty \simeq \Lambda(G)/I(G)\boldsymbol{\zeta}_p$ izomorfizmusa ad egy

$$E^1_\infty/C^1_\infty \simeq \Lambda(G)/\beta\Lambda(G) \tag{3.2}$$

izomorfizmust. Speciálisan $\mathrm{ch}_G(E^1_\infty/C^1_\infty) = \beta\Lambda(G)$.

Ha Γ csoport izomorf $\mathbb{Z}_p$ additív csoportjával, M pedig egy végesen generált torzió $\Lambda(\Gamma)$-modulus, akkor ha M^Γ és M_Γ végesek (eml.: a Γ-invariánsok és Γ-koinvariánsok halmaza), akkor definiáljuk M Γ-*Euler karakterisztikáját* a

$$\chi(\Gamma, M) = \#(M_\Gamma)/\#(M^\Gamma)$$

képlettel, ahol $\#A$ jelöli egy véges A halmaz számosságát.

3.6. Állítás. *Legyenek M_1 és M_2 végesen generált torzió $\Lambda(\Gamma)$-modulusok, melyekre*

(i) $ch_\Gamma(M_1) \supset ch_\Gamma(M_2)$ és

(ii) $\chi(\Gamma, M_1) = \chi(\Gamma, M_2)$.

Ekkor $ch_\Gamma(M_1) = ch_\Gamma(M_2)$.

Ennek az állításnak a használatában az (i), azaz "$\mathrm{ch}_G(Y_\infty)$ osztja $\mathrm{ch}_G(E^1_\infty/C^1_\infty)$" bizonyítása Euler rendszerek használatával lehetséges, amiknek definiálása a 4. fejezetre marad. A (ii) igazolása pedig $\Gamma = \Gamma_0$-ra lehetséges.

4. Euler rendszerek

Az Euler rendszerek motivációja az egyetlen ismert konkrét példája is. Legyen $r \geq 2$ egész, $a_1, \ldots, a_r$ nemnulla egészek és $n_1, \ldots, n_r$ olyan egész számok, amire $\sum_{j=1}^r n_j = 0$. Definiáljuk

$$\alpha(T) = \prod_{j=1}^r (T^{-a_j/2} - T^{a_j/2})^{n_j}$$

hatványsort a $T^{1/2}$ változóban. Legyen $S = \{2\} \cup \{p \text{ prím} \mid \exists j : \ p \text{ osztja } a_j\text{-t}\}$ és

$$W_S = \{\zeta \in \overline{\mathbb{Q}} : \zeta^m = 1 \text{ valamilyen } m \geq 1 \text{ egészre, amire } (m, S) = 1\} = \bigoplus_{q \notin S \text{ prím}} \mu_{q^\infty}. \tag{4.1}$$

Mivel $2 \in S$, ezért minden $\zeta \in W_S$ számnak egyértelműen létezik négyzetgyöke W_S-ben, jelölje ezt $\zeta^{1/2}$. Definiáljuk a következő

$$\phi_\alpha : W_S \to \overline{\mathbb{Q}}^\times$$

leképezést:

$$\phi_\alpha(\zeta) = \alpha(\zeta) \text{ ha } \zeta \neq 1, \text{ és } \phi_\alpha(1) = \prod_{j=1}^{r} a_j^{n_j}.$$

4.1. Lemma. *Minden $\zeta \in W_S$ egységgyökre*

(i) teljesül $\phi_\alpha(\zeta^{-1}) = \phi_\alpha(\zeta)$ és $\phi_\alpha(\zeta^\sigma) = \phi_\alpha(\zeta)^\sigma$ minden $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$-ra;

(ii) ha q prím nincs S-ben, akkor

$$\prod_{\rho \in \mu_q} \phi_\alpha(\rho\zeta) = \phi_\alpha(\zeta^q);$$

(iii) ha q prím nincs S-ben és ζ rendje relatív prím q-hoz, akkor

$$\phi_\alpha(\rho\zeta) \equiv \phi_\alpha(\zeta) \mod \mathfrak{q}$$

minden $\rho \in \mu_q$-ra és minden q fölötti $\mathfrak{q}$ prímre.

A fő sejtés bizonyításához elég a 4.1. lemma állításait használni, így ez alapján definiálhatjuk az Euler rendszereket.

4.2. Definíció. Legyen S véges halmaza prímeknek, ami tartalmazza a 2-t. Legyen W_S a (4.1) által definiált halmaz. Azt mondjuk, hogy $\phi : W_S \to \overline{\mathbb{Q}}^\times$ egy *Euler rendszer*, ha teljesül minden $\zeta \in W_S$ egységgyökre a 4.1. lemma három állítása ϕ_α helyett ϕ-re.

Térjünk vissza a fő sejtés bizonyítására. Legyen $F = F_m = \mathbb{Q}(\mu_{p^{m+1}})^+$ test valamilyen $m \geq 0$ egészre. Jelölje $A = A_m$ az F egészeinek gyűrűjének ideál osztálycsoportjának a p-hatványrendű elemei által alkotott részcsoportot, illetve $\Pi = \mathrm{Gal}(F/\mathbb{Q})$ és $R = R_m = \mathbb{Z}_p[\Pi]$. A 3.2. állítás szerint van egy

$$0 \longrightarrow \bigoplus_{i=1}^{h} \frac{\Lambda(G)}{\Lambda(G)f_i} \longrightarrow Y_\infty \longrightarrow Q \longrightarrow 0$$

egzakt sorozat. Legyen $\delta \in \Lambda(G)$ annulátora Q-nak, amire még az is teljesül, hogy $R/\mathrm{pr}(\delta)R$ véges, ahol $\mathrm{pr} : \Lambda(G) \to R$ a természetes vetítés. Bizonyítható, hogy $R/\mathrm{pr}(\beta)R$ véges. Legyen s egy fix p-hatvány, ami annulálja mind $R/\mathrm{pr}(\delta)R$-t, mind $R/\mathrm{pr}(\beta)R$-t. Ekkor definiáljuk a $t = (\#A)(\#Q)p^m s^{h+1}$ p-hatványt, illetve $\mathcal{R} = (\mathbb{Z}/t\mathbb{Z})[\Pi]$ csoportgyűrűt. Ha $x \in \Lambda(G)$, akkor jelölje a képét $x^\star$ a $\Lambda(G) \twoheadrightarrow \mathcal{R}$ természetes szürjekciónál. Rögzítsük még G-nek egy γ topologikus generátorát, azaz a γ által generált részcsoport lezártja G-ben az egész G csoport.

Az Euler rendszerek elméletével és teljes indukcióval bizonyítható az alábbi tétel.

4.3. Tétel. *Teljesül $i = 1, \ldots, h$-ra, hogy $f_1^\star \ldots f_i^\star$ osztja $((\gamma - 1)\beta\delta^{i+1})^\star$-t $\mathcal{R}$-ben.*

Ebből következik, hogy a megfelelő oszthatóság teljesül $(\mathbb{Z}/p^{m+1}\mathbb{Z})[\mathrm{Gal}(F_m/\mathbb{Q})]$-ban is $i = h$-ra, mert t többszöröse p^{m+1}-nek. Mivel minden $m \geq 0$-ra teljesül és

$$\Lambda(G) = \varprojlim (\mathbb{Z}/p^m\mathbb{Z})[\mathrm{Gal}(F_m/\mathbb{Q})],$$

ezért kompaktságra hivatkozva $f_1 \ldots f_h$ osztja $(\gamma - 1)\beta\delta^{h+1}$-t $\Lambda(G)$-ben. Innen már megmutatható, hogy $f_1 \ldots f_h$ osztja β-t, azaz éppen azt, ami a fő sejtéshez kellett.

Hivatkozások

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