Eötvös Loránd Tudományegyetem
Természettudományi Kar

Iwasawa-elmélet

Pálffy Patrik Dániel

Témavezető:
Zábrádi Gergely, egyetemi docens

Bsc diplomamunka
Algebra és Számelmélet Tanszék

Budapest, 2024.

Köszönetnyílvánítás

Szeretném kifejezni köszönetemet témavezetőmnek, Zábrádi Gergelynek, akinek az óráinak hatására döntöttem amellett, hogy elméleti matematikus legyek és az algebra, algebrai számelmélet iránt érdeklődjek.
Köszönöm családomnak és barátaimnak a támogatást.

Tartalomjegyzék

0. fejezet

Bevezetés

A számelmélet a görögökig visszamenő ága a matematikának, viszont egésszen Gaussig az állításokat különállónak gondolták. Gauss Disquisitiones című könyve összefoglalta a számelmélet számos eredményét, ami sok neves matematikust inspirált későbiekben, mint E.Kummer, L.Dirichlet és R.Dedekind. Az algebrai számelmélet első nagy felfedezését Dirichlet-nek köszönhetjük, aki belátta az első osztályszám formulát. A 20. század elején kutatott a témában Hilbert, akinek köszönhetünk sok osztálytestelméleti tételt. A terület magába foglalja az elliptikus görbék és moduláris formák közti kapcsolat tanulmányozását, ami segítségre volt A.Wilesnak, aki bebizonyította a Nagy Fermat sejtést. A század második felében kutatott K.Iwasawa, akinek az elmélete a modulusok elméletével probálja megmagyarázni a testbővítések láncának tulajdonságát.
A szakdolgozat során belátást adok a p-adikus számok fölötti testbővítések tulajdonságára és az Iwasawa Fősejtésére. A dolgozat Washington [6] könyvét követi.
Az 1. fejezetben a dolgozathoz szükséges definíciókat sorolom fel. A 2. fejezetben körosztási bővítésekről szól és végül megemlítem, hogy mekkora hatványon oszthatja a p prím az osztályszámot. A 3. fejezetben az Iwasawa-elmélethez szükséges moduluselméletet ismertetem és belátjuk a Λ-modulusok struktúra tételét. A 4. fejezetben a 2. fejezetben említett tétel általánosítását látjuk be úgy, hogy nem tesszük fel, hogy körosztási bővítésünk van. Az 5. fejezetben számos következményét bizonyítom be a 4. fejezet tételének. A 6. fejezetben említésre kerül az Iwasawa Fősejtés és a hozzátartozó Mazur-Wiles tétel, amit felületesen be is lát a dolgozat.

1. fejezet

Alapozás

1.1. Dirichlet karakterek

1.1.1. Definíció. χ-t Dirichlet karakternek hívjuk, ha egy multiplikatív homomorfizmus és $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$.

Ha $n|m$ akkor χ indukál egy $(\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ homomorfizmust úgy, hogy komponáljuk a $(\mathbb{Z}/m\mathbb{Z}) \to (\mathbb{Z}/n\mathbb{Z})$ természetes leképzéssel. Ezért amikor χ-ről beszélünk akkor érdemes a minimális n-ről beszélni, hiszen ugyanazt a leképzést indukálják.
Példák

1. Legyen $\chi : (\mathbb{Z}/8\mathbb{Z})^\times \to \mathbb{C}^\times$ úgy hogy $\chi(1) = 1, \chi(3) = -1, \chi(5) = 1, \chi(7) = -1$. Mivel $\chi(a + 4) = \chi(a)$ elég lenne mod 4 definiálni.
2. $\chi : (\mathbb{Z}/6\mathbb{Z})^\times \to \mathbb{C}^\times$ úgy, hogy $\chi(1) = 1, \chi(5) = -1$. Ekkor definiálhatnánk $\chi : (\mathbb{Z}/3\mathbb{Z})^\times \to \mathbb{C}^\times$ $\chi(1) = 1, \chi(2) = -1$.

1.1.2. Definíció. Egy Dirichlet karaktert párosnak hívunk, ha $\chi(-1) = 1$. Egy Dirichlet karaktert páratlannak hívunk, ha $\chi(-1) = -1$

1.2. L-függvények

1.2.1. Definíció. Legyen χ egy dirichlet karakter. Ekkor

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \quad \mathrm{Re}(s) > 1,$$

a χ átlal indukált L-függvény.

Vegyük észre, hogy ha $\chi = 1$ akkor megkapjuk a Riemann zeta függvényt. Ahogyan a Riemann zeta függvényről úgy az L-függvényekről is tudjuk, hogy analitikusan folythatható kivéve $s = 1$-ben amikor $\chi = 1$.

1.2.2. Definíció. Bernulli számoknak hívjuk a következő hatványsor együtthatóit

$$\frac{t}{e^t - 1} = \sum_{n=1}^{\infty} B_n \frac{t^n}{n!},$$

ahol B_n az n-ik Bernulli szám.

A Bernulli számokat általánosíthatjuk úgy, hogy

$$\sum_{a=1}^{f} \frac{\chi(a) t e^{at}}{e^{ft} - 1} = \sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!},$$

ahol f a minimális szám, ami indukálja χ-t.
Másik általánosítása a Bernulli polinomok, ahol $B_n(X)$-t úgy definiáljuk, hogy

$$\frac{te^{Xt}}{e^t-1} = \sum_{n=1}^{\infty} B_n(X)\frac{t^n}{n!}.$$

1.3. p-adikus Számok

Ebben a szekcióban egyetlen egy állítást sem bizonyítunk, a bizonyítás itt olvasható [4].

1.3.1. Definíció. Legyen $|.| : \mathbb{K} \to \mathbb{R}_{\geq 0}$ egy abszolútérték $\mathbb{K}$-n, ami kielégíti a következőket

1. $|x| = 0$ akkor és csak akkor, ha $x = 0$
2. $|xy| = |x||y|$
3. $|x + y| \leq |x| + |y|$
4. $|x + y| \leq \max\{|x|, |y|\}$.

Az utolsót nem-Arkimédeszi tulajdonságnak hívjuk.

1.3.2. Definíció. Egy metrikus teret, amit egy nem-Arkhemédeszi abszolút érték indukált, ultrametrikus térnek hívjuk.

1.3.3. Lemma. *Legyen $\mathbb{K}$ egy ultrametrikus tér. Ha $|x| \neq |y|$ akkor $|x + y| = max\{|x|, |y|\}$*

1.3.4. Definíció. A p-adikus kiértékelés $\mathbb{Q}$-n úgy definiáljuk, hogy $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$. Legyen $x \in \mathbb{Q}$ ahol $x \neq 0$. Ha $x \in \mathbb{Z}$, akkor $v_p(x)$ legyen olyan, hogy

$$x = p^{v_p(x)}x', \quad \text{ahol } p \nmid x'.$$

Minden $x \in \mathbb{Q}$-ra, ahol $x = \frac{a}{b}, a, b \in \mathbb{Z}$

$$v_p(x) = v_p(a) - v_p(b).$$

Végül $v_p(0) = \infty$.

1.3.5. Lemma. *A következő állítások igazak minden $x, y \in \mathbb{Q}$:*

1. $v_p(xy) = v_p(x) + v_p(y)$
2. $v_p(x + y) \geq min\{v_p(x), v_p(y)\}$.

1.3.6. Definíció. Legyen a p-adikus abszolút érték úgy definiálva, hogy

$$|x|_p = \begin{cases} p^{-v_p(x)}, & \text{if } x \neq 0 \\ 0, & \text{x=0.} \end{cases}$$

1.3.7. Állítás. *A p-adikus abszolút érték nem-Arkimédeszi abszolút érték $\mathbb{Q}$-n.*

1.3.8. Definíció. Legyen $\mathbb{Q}_p$ a p-adikus számok teste, amit úgy kapunk, hogy $\mathbb{Q}$-t teljessé tesszük a p-adikus abszolút értékre.

1.3.9. Definíció. Legyen $\mathbb{Z}_p$ a p-adikus egészek gyűrűje és

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p | |x|_p \leq 1\}.$$

1.4. Inverz Limesz

1.4.1. Definíció. Legyen I egy rendezett halmaz úgy, hogy minden $i, j \in I$-re létezik egy $k \in I$, hogy $i \leq k, j \leq k$. Minden $i \in I$-re legyen A_i egy halmaz és tegyük fel, hogy ha $i \leq j$ akkor létezik egy leképzés $\phi_{ji} : A_j \to A_i$, hogy $\phi_{ii} =$id és $\phi_{jk}\phi_{ij} = \phi_{ik}$, ha $i \leq j \leq k$. Ezt egy inverz rendszernek nevezzük.
Legyen $A = \prod A_i$ és definiáljuk az inverz limeszt, hogy

$$\varprojlim A_i = \{(\dots, a_i, \dots) \in A | \phi_{kj}(ak) = a_j, \text{ ha } j \leq k\}.$$

A $A \to A_i$ projekció indukál egy leképzést $\phi_i : \varprojlim A_i \to A_i$.

Példák:

1. Legyen I a pozitív egészek, $A_i = \mathbb{Z}/p^i\mathbb{Z}, \phi_{ji} : a \bmod p^j \mapsto a \bmod p^i$. Ekkor $\varprojlim \mathbb{Z}/p^i\mathbb{Z} = \mathbb{Z}_p$. A ϕ_i leképzés az a leképzés, ami a p-adikus szám első i tagját nézi.

2. Legyen I rendezett egészek úgy, hogy $m \leq n$, ha $m|n$. Létezik egy természetes leképzés $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. Legyen $\hat{Z} = \varprojlim \mathbb{Z}/n\mathbb{Z}$. A kínai maradék tételből kövezkezik, hogy $\hat{Z} \simeq \prod_{p \text{ prím}} \mathbb{F}_p$.

Azok, akik jobban érdeklődnek az inverz limesz iránt itt olvashatnak róla többet [5].

1.5. Elágazáselmélet

1.5.1. Definíció. Legyen R egy gyűrű. R prím gyűrű, ha minden $A, B \lhd R$ $AB = 0 \iff A = 0$ vagy $B = 0$.
Az $I \lhd R$ ideált prím ideálnak hívjuk, ha R/I prím gyűrű.

1.5.2. Definíció. Legyen A egy Dedekind gyűrű és K a törtek teste A felett. Legyen B az algebrai egészek A-nak L fölött, ahol L egy véges szeparábilis bővítése K-nak. Ekkor a prím ideál $\mathfrak{p}$ felbomlik B-ben

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}, \quad e_i \geq 1.$$

Ha bármely i-re $e_i > 1$ akkor a $\mathfrak{p}$ prím elágazik B-ben, különben azt mondjuk, hogy nem ágazik el. Az e_i számot az elágazás számának hívjuk. Azt mondjuk, hogy $\mathfrak{P}$ osztja $\mathfrak{p}$-t ($\mathfrak{P}|\mathfrak{p}$), ha $\mathfrak{P}$ megjelenik a felbontásban. Az elágazás számát $e(\mathfrak{P}/\mathfrak{p})$-vel is jelöljük és $f(\mathfrak{P}/\mathfrak{p})$ a mellékosztályok foka (a $[B/\mathfrak{P} : A/\mathfrak{p}]$ testbővítés rendje). Ha $e_i = f_i = 1$ minden i-re akkor azt mondjuk, hogy $\mathfrak{p}$ bomlik L-ben.

1.5.3. Lemma. *Legyen $\mathfrak{P}$ egy prím ideálja B-nek, ami osztja $\mathfrak{p}$-t $\iff$ $\mathfrak{p} = \mathfrak{P} \cap K$.*

1.5.4. Tétel. *Legyen m a L/K bővítés rendje és $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ a prímek, amik osztják $\mathfrak{p}$-t. Ekkor*

$$\sum_{i=1}^{g} e_i f_i = m.$$

Ha L/K Galois akkor az elágazás számok és mellégosztályok rendjei is egyenlőek ekkor

$$efg = m.$$

1.5.5. Definíció. Egy k test tökéletes, ha minden véges bővítése szeparábilis.

1.5.6. Definíció. Azt mondjuk, hogy $\mathfrak{p}$ teljesen elágazik B fölött, ha

$$\mathfrak{p}B = \mathfrak{P}^n$$

alakú.

1.5.7. Definíció. Legyen R egy gyűrű, azt mondjuk, hogy R lokális, ha R-nek egy darab maximális bal ideálja van.

1.5.8. Definíció. Legyen R egy lokális gyűrű és M a maximális bal ideálja. Ekkor R/M testet a maradéktestnek nevezik.

1.5.9. Definíció. Legyen L egy véges Galois bővítése K-nak és tegyük fel, hogy a maradékteste k tökéletes. Legyen Π egy prím L-ben ($\mathfrak{p} = (\Pi)$). A definiáljuk a következő részcsoport sorozatot $G \supset G_0 \supset G_1 \supset \dots$ úgy, hogy

$$\sigma \in G_i \iff |\sigma\alpha - \alpha| < |\Pi|^i, \text{ minden } \alpha \in B.$$

A G_0 csoportot inercia csoportnak hívjuk, a G_1 csoportot az elágazás csoportnak, a G_i $i > 1$ csoportokat a magasabb elágazás csoportoknak.

1.5.10. Lemma. *A G_i csoportok normál részcsoportok G-ben és G_i stabilizálódik.*

1.5.11. Definíció. Azt mondjuk, hogy L/K nem ágazik el, ha minden prím K-ban nem ágazik el.

A lemmák bizonyatásai megtalálhatóak a [2] jegyzetben.

1.6. Osztálytestelmélet

1.6.1. Definíció. Legyen I a törtideálok csoportja K-ban és legyen $i : K^\times \to I$ egy leképezés, ami $a \in K^\times$-t elküldi egy főideálban. Ekkor $C = I/i(K^\times)$-t K osztály csoportjának hívjuk. A $H \leq C$ részcsoport megfelel egy $i(K^\times) \supset \tilde{H} \leq I$ részcsoporttal.

1.6.2. Definíció. Legyen H egy részcsoportja C osztály csoportnak K fölött. Legyen L egy véges nem elágazó Abel bővítése K-nak, azt mondjuk, hogy az osztályteste H-nak, ha minden $\mathfrak{p}$ prím ideál az algebrai egészekben bomlik L-ben akkor és csak akkor, ha $\mathfrak{p} \in \tilde{H}$.

1.6.3. Definíció. Legyen I a törtideálok csoportja és $i(K^\times)$ a tört főideálok csoportja. Ekkor $[I : i(K^\times)] = h$ véges és K osztály számának hívjuk.

1.6.4. Definíció. Azt mondjuk, hogy egy számtest teljesen valós, ha minden $\mathbb{C}$-be menő beágyazása $\mathbb{R}$ beli. Hasonlóan egy számtest teljesen képzestes, ha egyetlen egy $\mathbb{C}$ beágyazása sem $\mathbb{R}$ beli.

1.6.5. Definíció. Egy számtestet CM-testnek (komplex szorzás testnek) hívunk, ha teljesek képzetes és egy teljesen valós testnek a másod fokú bővítése.

Az érdeklödő olvasú Milne "Class Field Theory" könyvében olvashatnak jobban utána a témának. [3]

2. fejezet

Körosztási bővítések

2.1. Csoportgyűrűk és hatványsorok

Legyen $\mathcal{O}$ az algebrai egészek gyűrűje egy véges bővítésének $\mathbb{Q}_p$-nek. Legyen $\mathfrak{p}$ a maximális ideálja $\mathcal{O}$-nak és π a generátora $\mathfrak{p}$-nek. Legyen Γ egy multiplikatív csoport, ami izomorf $\mathbb{Z}_p$-vel és γ ennek a generátora. Mivel $\mathbb{Z}_p$ zárt részcsoportjai $p^n\mathbb{Z}_p$ alakúak, ezért Γ zárt részcsoportjai Γ^{p^n} alakúak. Legyen $\Gamma_n = \gamma/\gamma^{p^n}$, ez ciklikus és p^n rendű. Vegyük a $\mathcal{O}[\Gamma_n]$ csoportgyűrűt. Ha $m \geq n \geq 0$ akkor létezik egy természetes leképzés $\phi_{m,n} : \mathcal{O}[\Gamma_m] \to \mathcal{O}[\Gamma_n]$, amit a $\Gamma_m \to \Gamma_n$ leképzés indukál. Ha vesszük az inverze limeszét $\mathcal{O}[\Gamma_n]$-nak a $\phi_{m,n}$ lekézések mellett akkor a $\mathcal{O}[[\Gamma]]$ csoportgyűrűjét kapjuk Γ-nak. Világos, hogy

$$\mathcal{O}[\Gamma_n] \simeq \mathcal{O}/((1+T)^{p^n} - 1),$$

ahol az izomorfizmus

$$\gamma \bmod \Gamma^{p^n} \mapsto 1 + T \bmod((1+T)^{p^n} - 1).$$

Ezért elég a polinom gyűrűt vizsgálnunk, hogy meg értsük $\mathcal{O}[[\Gamma]]$-t, hiszen

$$\mathcal{O}[[\Gamma]] \simeq \varprojlim \mathcal{O}[T]/((1+T)^{p^n} - 1).$$

2.1.1. Tétel. *$\mathcal{O}[[\Gamma]] \simeq \mathcal{O}[[T]]$, ahol $\gamma \mapsto 1 + T$ indukálja az izomorfizmust.*

A tétel bizonyításához szükségünk lesz más eredményekhez, amit nézzünk meg előtte.

2.1.2. Állítás. *Legyen $f, g \in \mathcal{O}[[T]]$ és tegyük fel, hogy $f = a_0 + a_1T + \ldots$, ahol $a_i \in \mathfrak{p}$ minden $0 \leq i \leq n-1$ és $a_n \in \mathcal{O}^\times$, Ekkor egyértelmű g maradékos osztása f-el, azaz*

$$g = qf + r,$$

ahol $q \in \mathcal{O}[[T]]$ és $r \in \mathcal{O}[T]$ legfeljebb $n-1$ fokú polinom.

Bizonyítás. Elsőnek lássuk be a függetlenséget, amihez elég $qf + r = 0$ egyenletet nézni. Ha $q, r \neq 0$ feltehetjük, hogy $\pi \nmid r$ vagy $\pi \nmid q$. Tudjuk, hogy $\pi | r$ és $\pi | fq \bmod \pi$. Mivel $\mathfrak{p}$ egy maximális ideál és $a_n \in \mathcal{O}^\times$, ezért nem lehet $\mathfrak{p}$-ben a_n, hiszen akkor $\mathfrak{p}$ triviálisan az egész gyűrű lenne. Ezzel ellenmondásra jutottunk.
Definiáljuk az τ operátort $\tau = \tau_n : \mathcal{O}[[T]] \to \mathcal{O}[[T]]$ ugy, hogy

$$\tau\left(\sum_{i=0}^{\infty} b_i T^i\right) = \sum_{i=n}^{\infty} b_i T^{i-n}.$$

Ezzel τ egy fajta "shift operator". Világos, hogy τ $\mathcal{O}$-lineáris és teljesíti a következőket

1. $\tau(T^n h(T)) = h(T)$ minden $h(T) \in \mathcal{O}[[T]]$,
2. $\tau(h(T)) = 0 \iff h(T) \in \mathcal{O}[T]$ és a foka kisebb mint n.

Ekkor

$$f(T) = \pi P(T) + T^n U(T),$$

ahol $P(T)$ legfeljebb $n-1$ fokú és $U(T) = a_n + a_{n+1}T + \cdots = \tau(f(T))$. Mivel $a_n \in \mathcal{O}^\times$, $U(T)$ egy egység elem a hatványsor gyűrűben. Legyen

$$q(T) = \frac{1}{U(T)} \sum_{i=0}^{\infty} (-1)^j \pi^j \left(\tau \circ \frac{P}{U}\right)^j \circ \tau(g).$$

Itt a $(X \circ Y)^k$ jelölés ezt jelenti, hogy

$$(X \circ Y)^2 \circ Z = X(Y(X(Y(Z)))).$$

Lehetséges, hogy minden tag hozzáadodik egy q_i-hez, viszon π^j tagok miatt konvergálni fognak. Tehát $q(T)$ egy jól definiát hatványsor $\mathcal{O}[[T]]$-ben. Mivel

$$qf = \pi qP + T^n qU,$$

ezért

$$\tau(qf) = \pi\tau(qP) + \tau(T^n qU) = \pi\tau(qP) + qU,$$

viszont ez csak eltolja így

$$\pi\tau(qP) = \tau(g) - qU.$$

Ebből már kövezkezik, hogy

$$\tau(qf) = \tau(g)$$

és a második pontból megkaptuk, hogy $g = qf + r$, ahol r legfeljebb $n-1$ fokú. □

2.1.3. Definíció. P(T)$\in \mathcal{O}[T]$ polinomot megkülönböztetettnek hívjuk, ha

$$P(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0, \text{ahol } a_i \in \mathfrak{p}.$$

2.1.4. Tétel. *(p-adikus Weierstrass Előkészítési Tétel)*

$$f(T) = \sum_{i=0}^{\infty} a_i T^i \in \mathcal{O}[[T]],$$

Tegyük fel, hogy létezik egy n, amire $a_i \in \mathfrak{p}, 0 \leq i \leq n-1$, de $a_n \notin \mathfrak{p}$. Ekkor f egyértelműen írható f(T)=P(T)U(T) alakban, ahol U(T)$\in \mathcal{O}[[T]]$ egység eleme és P(T) egy megkülönböztetett n-ed rendű polinom.
Még általánosabban ha f(T)$\in \mathcal{O}[[T]]$ nem nulla, akkor egyértelműen írható

$$f(T) = \pi^\mu P(T)U(T)$$

P és U, ahogy fent definiáltuk és μ egy nemnegatív egész.

Bizonyítás. A második verzió könnyen megkapható az elsőből, ha kiemeljük a legnagyobb együtthatón a π-t $f(T)$-ből. Legyen $g(T) = T^n$ ekkor

$$T^n = q(T)f(T) + r(T), \quad \text{ahol deg } r \leq n-1.$$

Mivel

$$q(T)f(T) \equiv q(T)(a_n T^n + \dots) \bmod \pi$$

megkaptuk, hogy $r(T) \equiv 0 \bmod \pi$.Ezért $P(T) = T^n - r(T)$ egy n-ed fokú megkülönböztetett polinom. Legyen q_0 a konstans tagja $q(T)$-nek. Mivel $1 \equiv q_0 a_n \bmod \pi$, ezért $q_0 \in \mathcal{O}^\times$, tehát $q(T)$ egy egység. Legyen $U(T) = 1/q(T)$, ekkor $f(T) = P(T)U(T)$. Mivel minden megkülönböztetett polinom felírható $P(T) = T^n - r(T)$ alakban, ezért kész vagyunk. Hiszen

$$T^n = U(T)^{-1} f(T) + r(T)$$

egyértelműen meghatározza $U(T)$-t és $r(T)$-t az előző lemma miatt. □

2.1.5. Lemma. *Tegyük fel, hogy $P(T) \in \mathcal{O}[T]$ egy megkülönböztett polinom és legyen $g(T) \in \mathcal{O}[T]$ tetszőleges. Ha $g(T)/P(T) \in \mathcal{O}[[T]]$ akkor $g(T)/P(T) \in \mathcal{O}[T]$.*

Bizonyítás. Tegyük fel, hogy $g(T) = f(T)P(T)$ valamilyen $f(T) \in \mathcal{O}[[T]]$. Legyen $x \in \mathbb{C}_p$ egy gyöke $P(T)$-nek. Ekkor

$$0 = P(x) = x^n + (\text{többszöröse } \pi\text{-nek}),$$

tehát $|x| < 1$, tehát $f(x)$ konvergál és $g(x) = 0$. Ha osztjuk $T - x$-el és szükségszerűen nagyobb gyűrűben vizsgáljuk, akkor ez előző lépések ismétlésével azt kapjuk, hogy $P(T)|g(T)$ mint polinom, ezért $\mathcal{O}[T]$ beli. □

Most térjünk vissza a tétel bizonyításához. Elgéséges belátni, hogy

$$\mathcal{O}[[T]] \simeq \varprojlim \mathcal{O}[T]/((1+T)^{p^n} - 1).$$

Vegyük észre, hogy $P_n(T) = (1+T)^{p^n} - 1$ egy megkülönböztett polinom, sőt $(\pi, T) \supseteq (p, T)$ egy maximális ideálja $\mathcal{O}[T]$-nek. Világos, hogy $P_0 \in (p, T)$, ezért

$$\frac{P_{n+1}(T)}{P_n(T)} = (1+T)^{p^n(p-1)} + (1+T)^{p^n(p-2)} + \cdots + 1 \in (p, T)$$

indukcióból következik, hogy $P_n(T) \in (p, T)^n$. 2.1.2-es állítás miatt létezik egy természetes leképzés $\mathcal{O}[[T]]$-ból $\mathcal{O}[T]$ mod $P_n(T)$-be minden n-re. Nevezetesen $f(T) \mapsto f_n(T)$, ahol $f(T) = q_n(T)P_n(T) + f_n(T)$, ahol $\deg f_n < p^n$. Ha $m \geq n \geq 0$, akkor

$$f_m(T) - f_n(T) - \left(q_n - \frac{P_m}{P_n} q_m\right) P_n.$$

A 2.1.5 lemma szerint $f_m \equiv f_n \bmod P_n$, ezért

$$(f_0, f_1, \dots) \in \varprojlim \mathcal{O}[T]/(P_n(T)).$$

Ez meghatározza a leképzésünket a hatványsor gyűrűből az inverz limeszbe. Ha $f_n = 0$ minden n-re akkor $P_n | f$ minden n-re, ezért $f \in \bigcap_{n=0}^{\infty} (p, T)^{n+1} = 0$, tehát injektív a leképzés.
Most lássuk be a szürjektivitást. Tegyük fel, hogy $(f_0, f_1, \dots)$ egy eleme az inversz limesznek. Ekkor minden $m \geq n \geq 0$-ra $f_m \equiv f_n \bmod P_n$, ezért mod $(p, T)^{n+1}$ is. Így a konstansok kongurensek mod p^{n+1}, a lineáris tagok kongurensek mod p^n és így tovább. Ekkor az együtthatók egy Cauchy sorozatot alkotnak. Legyen $f = \lim f_n(T) \in \mathcal{O}[[T]]$. Meg kell mutatnunk, hogy $f \mapsto (f_0, f_1, \dots)$. Ha $m \geq n \geq 0$ akkor $f_m - f_n = q_{m,n} P_n$ valamilyen $q_{m,n} \in \mathcal{O}[T]$. Engedjük m-t a végtelenbe ekkor

$$q_{m,n} = \frac{f_m - f_n}{P_n} = \frac{f - f_n}{P_n},$$

mivel $q_{m,n} \in \mathcal{O}[T]$, ezért a határértéknek $\mathcal{O}[[T]]$-ben van és

$$f = (P_n)(\lim_m q_{m,n}) + f_n.$$

Így $f \mapsto (f_0, f_1, \dots)$.

2.2. p-adikus L-függvények és alkalmazásaik

Ebben a fejezetben ezeket a jelöléseket használjuk, ha máshogy nincsen jelezve. $q = p$ ha $p \neq 2$ és $q = 4$ ha $p = 2$. Legyen $q_n = qp^n d$, ahol $(d, p) = 1$ és $K_n = \mathbb{Q}(\zeta_{q_n})$,és $K_\infty = \bigcup_{n \geq 0} \mathbb{Q}(\zeta_{q_n})$. Ekkor $K_n = K_n(\zeta_{qp^n})$ és $K_\infty = K_0(\zeta_{qp^\infty})$ és

$$\mathrm{Gal}(K_\infty/\mathbb{Q}) \simeq \Delta \times \Gamma,$$

ahol

$$\Delta = \mathrm{Gal}(K_0/\mathbb{Q}) \quad \text{és} \quad \Gamma = \mathrm{Gal}(K_\infty/K_0) \simeq \mathbb{Z}_p.$$

2.2.1. Definíció. Nevezzük ξ_n-nek a következő kifejezést

$$\xi_n = -\frac{1}{q_n} \sum_{\substack{0 < a < q_n \\ (a, q_0) = 1}} a\delta(a)^{-1}\gamma_n(a)^{-1},$$

ahol $\gamma_n(a) \in \Gamma_n$ és $\delta(a) \in \Delta$, Legyen η_n a következő

$$\eta_n = (1 - (1+q_0)\gamma_n(1+q_0)^{-1})\xi_n = -\sum_a \left(\left\{ \frac{a(1+q_0)}{q_n} \right\} - (1+q_0)\left\{ \frac{a}{q_n} \right\} \right) \delta(a)^{-1}\gamma_n(a)^{-1}\gamma_n(1+q_0)^{-1}.$$

2.2.2. Definíció. Legyen θ egy páros karakter és $\theta^* = \omega\theta^{-1}$ egy páratlan karakter. Legyen

$$\varepsilon_{\theta^*} = \tfrac{1}{|\Delta|} \sum_{\delta\in\Delta} \theta^*(\delta)\delta^{-1}$$

idempotens θ^*-ra. Ekkor $\varepsilon_{\theta^*}\xi_n = \xi_n(\theta)\varepsilon_{\theta^*}$ és $\varepsilon_{\theta^*}\eta_n = \eta_n(\theta)\varepsilon_{\theta^*}$, ahol

$$\xi_n(\theta) = -\frac{1}{q_n}\sum_a a\theta\omega^{-1}(a)\gamma_n(a)^{-1} \in K_\theta[\Gamma_n]$$

és

$$\eta_n(\theta) = (1-(1+q_0)\gamma_n(1+q_0)^{-1})\xi_n(\theta) = \sum_a \left((1+q_0)\left\{\frac{a}{q_n}\right\} - \left\{\frac{a(1+q_0)}{q_n}\right\}\right)\times\theta\omega^{-1}(a)\gamma_n(a)^{-1}\gamma_n(1+q_0)^{-1} \in \mathcal{O}_\theta[\Gamma_n].$$

2.2.3. Tétel. *Legyen $\chi = \theta\psi$ egy páros Dirichlet karakter és $\zeta_\psi = \psi(1+q_0)^{-1} = \chi(1+q_0)^{-1}$. Ekkor*

$$L_p(s,\chi) = f(\zeta_\psi(1+q_0)^s - 1, \theta)$$

Bizonyítás. Vegyük észre, hogy ha $|s| < qp^{\frac{-1}{p-1}}$ akkor

$$|(1+q_0)^s - 1| = |p^{s\log_p(1+q_0)} - 1| < 1$$

és mivel ζ_ψ p-hatvány rendű, ezért $|\zeta_\psi(1+q_0)^s - 1| < 1$. Így a jobb oldal konvergál és analitikus függvény s-n. Ezért elég csak a $s = 1-m$ helyeken vizsgálni, ahol m egy egész. Legyen $i(a) = \log_p < a > /\log_p(1+q_0)$, ahol $< a >= \omega(a)^{-1}a$. Legyen γ_n Γ_n egy eleme. Mivel $\gamma_n(1+q_0)$ megfelel $1+T$-nek, ezért $\gamma_n(a) = \gamma_n(1+q_0)^{i(a)}$ megfelel $(1+T)^{i(a)} \bmod (1+T)^{p^n} - 1$-nek. Létezik olyan hatványsor $g \in \mathcal{O}[[T]]$, hogy

$$g(T,\theta) \equiv \sum_{\substack{0<a<q_n\\(a,q_0)=1}} \left((1+q_0)\left\{\frac{a}{q_n}\right\} - \left\{\frac{(1+q_0)a}{q_n}\right\}\right) \times \theta\omega^{-1}(a)(1+T)^{-i(a)-1} \bmod (1+T)^{p^n} - 1.$$

Legyen $(1+q_0)a = a_1 + a_2q_n$, ahol $0 \le a_1 < q_n$. Ekkor $i(a)+1 = i((1+q_1)a) \equiv i(a_1) \bmod p^n$ és

$$g(T,\theta) \equiv \sum_a a_2\theta\omega^{-1}(a_1)(1+T)^{i(a_1)} \bmod (1+T)^{p^n} - 1.$$

Ha m egy pozitív egész és n elég nagy akkor

$$g(\zeta_\psi(1+q_0)^{1-m} - 1, \theta) \equiv \sum_a a_2\theta\omega^{-1}(a_1)(\zeta_\psi^{-1}(1+q_0)^{m-1})^{i(a_1)} \bmod q_n,$$

mivel

$$\begin{aligned}(1+T)^{p^n} - 1 &= (\zeta_\psi(1+q_0)^{1-m})^{p^n} - 1\\ &= (1+q_0)^{(1-m)p^n} - 1 \equiv 0 \bmod q_n.\end{aligned}$$

De $\zeta_\psi^{-i(a_1)} = \psi(1+q_0)^{i(a_1)} = \psi(a_1)$ és $(1+q_0)^{i(a_1)} =< a_1 >$, ezért

$$\begin{aligned}g(\zeta_\psi(1+q_0)^{1-m} - 1, \theta) &\equiv \sum_a a_2\theta\omega^{-1}(a_1)\psi(a_1) < a_1 >^{m-1}\\ &\equiv \sum_a a_2\chi\omega^{-m}(a_1)a_1^{m-1} \bmod q_n.\end{aligned}$$

Ha n olyan nagy, hogy $f_\chi | q_n$ akkor $\chi\omega^{-m}((1+q_0)a) = \chi\omega^{-m}(a_1)$. Azonban

$$((1+q_0)a)^m \equiv a_1^m + ma_1^{m-1}q_na_2 \bmod q_n^2,$$

szóval

$$\chi\omega^{-m}(1+q_0)(1+q_0)^m\sum_a \chi\omega^{-m}(a)a^m \equiv \sum_{a_1}\chi\omega^{-m}(a_1)a_1^m + mq_n\sum_{a_2} a_2\chi\omega^{-m}(a_1)a_1^{m-1} \bmod q_n^2.$$

Azonban $\chi\omega^{-m}(1+q_0) = \chi(1+q_0)$. Azt kapjuk, hogy

$$g(\zeta_\psi(1+q_0)^{1-m}-1,\theta) =$$

$$= ((1+q_0)^m\chi(1+q_0)-1)\frac{1}{m}\lim_{n\to\infty}\frac{1}{q_n}\sum_{\substack{0<a<q_n\\(a,q_n)=1}}\chi\omega^{-m}(a)a^m$$

$$= -h(\zeta_\psi(1+q_0)^{1-m}-1)\frac{1}{m}\lim_{n\to\infty}\frac{1}{q_n}\sum_a\chi\omega^{-m}(a)a^m.$$

A következő lemma befejezi a bizonyítást.

2.2.4. Lemma.

$$\lim_{n\to\infty}\frac{1}{q_n}\sum_{\substack{0<a<q_n\\(a,q_0)=1}}\chi\omega^{-m}(a)a^m = (1-\chi\omega^{-m})(p)p^{m-1}B_{m,\chi\omega^{-m}}$$

Bizonyítás. Emlékezzünk a Bernulli függvényekre

$$B_m(X) = \sum\binom{m}{i}B_iX^{m-i} \quad \text{ahol } B_i \text{ az i-dik Bernulli szám,}$$

$$B_{m,\chi\omega^{-m}} = \frac{1}{q_n}\sum_{j=1}^{q_n}\chi\omega^{-m}(j)q_n^mB_m\left(\frac{j}{q_n}\right)$$
$$= \frac{1}{q_n}\sum_j\chi\omega^{-m}(j)\left(j^m - \frac{m}{2}j^{m-1}q_n\right) \bmod \frac{1}{p}q_n$$

Mivel

$$\chi\omega^{-m}(q_n-j)(q_n-j)^{m-1} \equiv -\chi\omega^{-m}(j)j^{m-1} \bmod q_n.$$

így ha párosítjuk az elemeket azt kapjuk, hogy

$$\sum_j\chi\omega^{-m}(j)j^{m-1} \equiv 0 \bmod q_n,$$

Így azt kaptuk, hogy

$$B_{m,\chi\omega^{-m}} = \lim_{n\to\infty}\frac{1}{q_n}\sum_{j=1}^{q_n}\chi\omega^{-m}(j)j^m$$

tehát

$$(1-\chi\omega^{-m}(p)p^{m-1})B_{m,\chi\omega^{-m}} = \lim\frac{1}{q_n}\sum_{j=1}^{q_n}\chi\omega^{-m}(j)j^m - \lim\frac{1}{q_n}\sum_{j=1}^{q_n}\chi\omega^{-m}(pj)(pj)^m$$
$$= \lim\frac{1}{q_n}\sum_{\substack{j=1^{q_n}\\p\nmid j}}\chi\omega^{-m}(j)j^m = \lim\frac{1}{q_n}\sum_{\substack{j=1\\(j,q_0)=1}}^{q_n}\chi\omega^{-m}(j)j^m.$$

Ezzel a lemmát és a tételt is beláttuk. □

□

2.2.5. Lemma. *Ha $\theta = 1$ akkor $\frac{1}{2}g(T,\theta)$ egység $\mathbb{Z}_p[[T]]$-ben.*

Bizonyítás. Az 2.2.3 tétel alapján

$$f(0,1) = -B_{1,\omega^{-1}} = -\frac{1}{q}\sum_{\substack{a=1\\ n\nmid a}}^{q} \omega^{-1}(a)a \equiv \frac{1}{p} \bmod \mathbb{Z}_p,$$

mivel $\omega(a) \equiv a \bmod q$. Azonban

$$h(0,1) = -q \quad \text{ahol } h \text{ asszimptotikus lim } \eta_n\text{-hoz.}$$

Valamint

$$f(T,\theta) = \frac{g(T,\theta)}{h(T,\theta)},$$

ha az olvasót több részlet érdekel f, g, h-ról akkor megtalálhatja a Whasington könyv [6] 123 oldalán. Ezért

$$\frac{1}{2}g(0,1) = \frac{1}{2}f(0,1)h(0,1) \equiv \frac{-q}{2p} \bmod \frac{q}{2}\mathbb{Z}_p.$$

Így azt kaptuk, hogy $\frac{1}{2}g(0,1) \not\equiv 0 \bmod p$, tehát a konstans része $\frac{1}{2}g$-nek egy egység. □

A következő három tételt a dolgozatban nem bizonyítjuk, de az érdeklödő olvasó megtalálja a Whasington könyv [6] 126 és 131 oldalán.

2.2.6. Tétel. *Legyen (d,p)=1, $q_n = qdp^n$ és $h_n^- = h^-(\mathbb{Q}(\zeta_{q_n}))$. Tegyük fel, hogy $d \not\equiv 2(mod 4)$, ekkor*

$$\frac{h_n^-}{h_0^-} = \prod_{\substack{\theta\neq 1\\ f_\theta | q_0\\ \theta \text{ páros}}} \prod_{\substack{\zeta^{p^n}=1\\ \zeta\neq 1}} \frac{1}{2}f(\zeta - 1, \theta) \times \textit{(p-adikus egység)}$$

2.2.7. Tétel. *Legyen $p^{e_n^-}$ egy p hatávny, ami osztja h_n^--t (lásd 7.13). Ekkor léteznek λ, μ, ν n-től független számok, amikre teljesül, hogy $\lambda \geqslant 0, \mu \geqslant 0$, ekkor*

$$e_n^- = \lambda n + \mu p^n + \nu$$

minden n-re.

2.2.8. Tétel. *Legyen K egy Abel bővítése $\mathbb{Q}$, legyen p egy prím és K_∞/K egy körosztási $\mathbb{Z}_p$bővítése K-nak, ekkor μ=0.*

Belátjuk, hogy minden számtestnek létezik legalább egy darab $\mathbb{Z}_p$-bővítése.

Legyen $\mathbb{B}_n$ egy különböző résztestei $\mathbb{Q}(\zeta_{qp^n})$-nek, amik p^n rendű ciklikusak $\mathbb{Q}$ felett. Nézzük a $(\mathbb{Z}/qp^n\mathbb{Z})^\times \simeq (\mathbb{Z}/q\mathbb{Z})^\times \times$ (ciklikus p^n-ed rendű) izomorfizmust és vegyük $\mathbb{B}_n$-t $(\mathbb{Z}/q\mathbb{Z})^\times$ fix testének. Ekkor $\mathbb{Q} = \mathbb{B}_0$ és $\mathbb{B}_\infty/\mathbb{Q}$ egy $\mathbb{Z}_p$-bővítés. Legyen K egy tetszőleges számtest és $K_\infty = K\mathbb{B}_\infty$. Azt állítjuk, hogy K_∞/K is egy $\mathbb{Z}_p$-bővítés. Legyen $\mathbb{B}_e = K \cap \mathbb{B}_\infty$. Ekkor a Galois csoportja K_∞/K-nak izomorf $\mathbb{B}_\infty/\mathbb{B}_\infty \cap K$ Galois csoportjával, ami $p^e\mathbb{Z}_p \simeq \mathbb{Z}_p$. Ekkor K_∞/K-t K-nak a körosztási $\mathbb{Z}_p$-bővítésének hívjuk. Ha K tartalmazza $\mathbb{Q}(\zeta_q)$-t akkor elég a p egységgyököket hozzávenni K-hoz.

3. fejezet

Iwasawa-elmélet alapozás

3.1. Szükséges állítások a $\mathbb{Z}_p$-bővítésekről

3.1.1. Állítás. *Legyen K_∞/K egy $\mathbb{Z}_p$-bővítés. Ekkor minden $\boldsymbol{n} \geq 0$ létezik egyértelműen egy K_n, p^n rendű test K fölött. K_n és K_∞ az egyetlen testek, K és K_∞ között.*

Bizonyítás. Minden köztes testhez tartozik egy részcsoportja $\mathbb{Z}_p$-nek. Legyen ez S$\neq$0 zárt részcsoport és legyen $x \in S$ úgy, hogy ν_p(x) minimális. Ekkor $x\mathbb{Z}$, így $x\mathbb{Z}_p$ is része S-nek, x választásából adódik, hogy S=x$\mathbb{Z}_p$=$p^n\mathbb{Z}_p$ valamely n-re. □

3.1.2. Állítás. *Legyen K_∞/K egy $\mathbb{Z}_p$-bővítés és legyen $\tilde{l}$ egy prímje (esetleg arkhimédeszi) K-nak, ami nem helyezkedik p fölött. Ekkor K_∞/K nem ágazik el $\tilde{l}$-ben, azaz $\mathbb{Z}_p$-bővítések csakis p-ben ágaznak el.*

Bizonyítás. Legyen $I \subseteq \mathrm{Gal}(K_\infty/K) \simeq \mathbb{Z}_p$ az inercia csoportja $\tilde{l}$-nek, mivel I zárt így, vagy I=0 vagy I=$p^n\mathbb{Z}_p$ minden n-re. Ha I=0 akkor kész vagyunk. Tegyük fel, hogy I=$p^n\mathbb{Z}_p$, sőt legyen végtelen is. I-nek a rendje 1-nek vagy 2-nek kell legyen végtelen prímekre, így feltehető, hogy $\tilde{l}$ nem arkhemédeszi. Teljes indukcióval válasszunk egy $\tilde{l}_n$ helyét K_n-nek, ami $\tilde{l}_{n-1}$ felett helyezkedik el és $\tilde{l}_0$=$\tilde{l}$. Legyen $\bar{K}_n$ a teljesététele K_n-nek és legyen $\bar{K}_\infty$=$\bigcup \bar{K}_n$. Ekkor

$$I \subseteq \mathrm{Gal}(\bar{K}_\infty/\bar{K}).$$

Legyen U egy egysége $\bar{K}$-nak. A lokális osztálytestelmélet szerint létezik egy folytonos szürjektív homomorfizmus

$$U \to I \simeq p^n\mathbb{Z}_p.$$

Viszont

$$U \simeq (\text{véges csoport}) \times \mathbb{Z}_l^a, \quad \mathrm{a} \in \mathbb{Z},$$

ahol l egy racionális prím, ami osztható $\tilde{l}$-el. Mivel $p^n\mathbb{Z}_p$ nincs torzió eleme és csinálnunk kell egy szürjektív folytonos leképzést

$$\mathbb{Z}_l^a \to p^n\mathbb{Z}_p \to p^n\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p.$$

$\mathbb{Z}_l^a$-nek nincs zárt részcsoportja, aminek az indexe p, szóval ellentmondásra jutottunk. □

3.1.3. Lemma. *Legyen K_∞/K egy $\mathbb{Z}_p$-bővítés. Legyen legalább egy prím, ami elágazik a bővítésben és létezik egy nem negatív egész n, amire ha egy prím elágazik K_∞/K_n-ben akkor az teljesen elágazik.*

Bizonyítás. K osztályszáma véges és a maximális nem elágazó Abel bővítése K-nak véges, így létezik prím aminek el kell ágaznia K_∞/K-ban. Előző állításban beláttuk, hogy csak véges sok ilyen létezik. Legyenek ezek $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ és $I_1, \ldots, I_s$ a hozzájuk tartozó inercia csoport. Ekkor

$$\bigcap I_j = p^n\mathbb{Z}_p$$

valamely n-re, $p^n\mathbb{Z}_p$ fixteste K_n és $\mathrm{Gal}(K_\infty/K)$⊆I_j minden $0 \leq \mathrm{j} \leq \mathrm{s}$. Tehát minden prím, ami $\mathfrak{p}_j$ felett helyezkedik el teljesen elágazik K_∞/K-ban. □

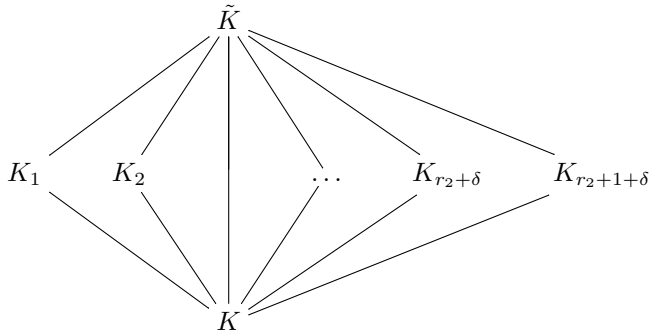
Korábban beláttuk az 2.fejezetben, hogy minden K számtestnek van $\mathbb{Z}_p$-bővítése, névlegesen a körosztási $\mathbb{Z}_p$-bővítés. Ezt kibővítve legyen E_1 azon egységek K-ban, amik 1-gyel kongurensek modulo minden $\mathfrak{p}$ prím, ami p fölötti. Legyen $U_1, \mathfrak{p}$ lokális egységek kongurens 1 modulo $\mathfrak{p}$. Ekkor létezik egy beágyazás

$$E_1 \to U_1 = \prod_{\mathfrak{p}|\mathrm{p}} U_1, \mathfrak{p}$$

$$\varepsilon \mapsto (\varepsilon, \ldots, \varepsilon).$$

$\bar{E}$ lezárt egy $\mathbb{Z}_p$-modulus és a Leopoldt sejtés azt jósolja, hogy $\mathbb{Z}_p$-rangja $\mathrm{r}_1 + \mathrm{r}_2 - 1$, ahol r_1 a valós beágyazásainak a száma és r_2 a komplex beágyazásainak a száma. Abel számtestekre ez az állítás tudott.

3.1.4. Állítás. *Tegyük fel, hogy $\bar{E}_1$ $\mathbb{Z}_p$-rangja $r_1 + r_2 - 1 - \delta$, és $0 \leq \delta$. Ekkor $r_2 + 1 + \delta$ darab független $\mathbb{Z}_p$-bővítése van K-nak. Más szóval a legkisebb testnek, ami tartalmazza az összes $\mathbb{Z}_p$-bővítéseket legyen $\tilde{K}$, a Galois csoportja izomorf $\mathbb{Z}_p^{r_1+1+\delta}$-vel.*



3.1.5. Következmény. *Legyen H egy Hilbert osztályteste K-nak és legyen F a maximális Abel bővítése K-nak ami nem ágazik el p kivételével. Ekkor*

$$Gal(F/K) \simeq (\prod_{\mathfrak{p}|p} U_{\mathfrak{p}}/\bar{E}).$$

ahol $\bar{E}$ jelöli E lezártját és diagonálisan be van ágyazva $\prod U_{\mathfrak{p}}$-be.

3.2. Λ-modulus struktúrák

Legyen $\Lambda = \mathbb{Z}_p[[T]]$. Emlékezzünk a megkülönböztetett polinomok definíciójára. A p-adikus Weierstrass előkészítési tétel szerint minden nem nulla $f(T) \in \Lambda$ polinom felírható egyértelműen, illetve állítás szerint $U(T)$ is polinom, ha $f(T)$ az. Az osztási-algoritmus is működik, ha deg(0)=-∞-nek definiáljuk.

$$f(T) = q(T)P(T) + r(T)$$

Ezekkel teljesül, hogy Λ egy UFD, aminek az irreducibilus elemei p és a megkülönböztetett irreducibilis polinomok, az egységek pedig azok a hatványsorok, amik $\mathbb{Z}_p^\times$-ben vannak.

3.2.1. Lemma. *Tegyük fel, hogy $f, g \in \Lambda$ relatív prímek. Ekkor (f, g) ideál véges indexű.*

Bizonyítás. Legyen $h \in (f, g)$ egy minimális rendű elem. Ekkor $h = p^s H$ alakba írható, ahol $H = 1$ vagy H megkülönböztetett polinom. Tegyük fel, hogy $H \neq 1$, mivel f és g relatív prímek, ezért feltehetjük, hogy H nem osztja f-t. osztási-algoritmus szerint

$$f = Hq + r, \quad \deg \mathrm{r} < \deg \mathrm{H} = \deg \mathrm{h},$$

$$p^s f = hq + p^s r.$$

A $p^s r$ foka kisebb, mint h foka, ezért $p^s r \in (f,g)$, így ellentmondásra jutottunk. Tehát $H=1$ és h=p^s. Általánosság elvesztése nélkül feltehetjük, hogy f nem osztható p-vel és megkülönböztetett polinom, ha nem az akkor használjuk g-t vagy osszuk el egy egységgel. Tudjuk, hogy

$$(f,g) \supseteq (p^s, f)$$

Az osztási-algoritmus miatt minden eleme Λ-nak kongurens egy f-nél kisebb fokú polinommal modulo f. Ezekből véges sok van mod p^s, így az ideál (p^s, f) véges rendű. □

3.2.2. Lemma. *Tegyük fel, hogy $f, g \in \Lambda$ relatív prímek. Ekkor*
(1)

$$\Lambda/(fg) \mapsto \Lambda/(f) \oplus \Lambda/(g)$$

természetes leképzés egy injektív leképzés véges komaggal.
(2) létezik egy természetes leképzés,

$$\Lambda/(f) \oplus \Lambda/(g) \mapsto \Lambda/(fg)$$

aminek véges a komagja.

Bizonyítás. (1) Korábbiakban beláttuk, hogy Λ egy UFD, tehát a leképzés injektív. Az kell, hogy a komag véges. Vegyünk egy (a mod f, b mod g) ideált, ha $a-b \in (f,g)$, akkor $a-b = fA+gB$, valamely $A, B \in \Lambda$. Legyen

$$c = a - fA = b + gB.$$

Ekkor

$$c \equiv a \text{ mod f}, \quad c \equiv b \text{ mod g},$$

tehát (a,b) része a képtérnek. Legyen $r_1, \ldots, r_n \in \Lambda$ reprezentatívjai $\Lambda/(f,g)$-nek. Ekkor

$$\{(0 \text{ mod f}, r_j \text{ mod g}) | 1 \leq j \leq n\}$$

halmaz reprezentatívja a komagnak.
(2) Az első részből tudjuk,hogy

$$\Lambda/(fg) \simeq M \subseteq \Lambda/(f) \oplus \Lambda/(g) = N$$

és M véges indexű részgyűrűje N-nek. Legyen P egy megkülönböztetett polinom Λ-ban, ami relatív prím fg-hez. Ha (x,y)∈N, akkor

$$(P^i)(x,y) \equiv (P^j)(x,y) \text{mod M}$$

valamely i<j-re. Mivel

$$1 - P^{j-i} \in \Lambda^\times,$$

ezért

$$P^i(x,y) \in \text{M}.$$

Ezekből következik, hogy $P^k N \subseteq$M valamely k-ra. Tegyük fel, hogy P^k(x,y)=0 N-ben, tehát f|P^kx,g|P^ky. Mivel gcd(P,fg)=1, ezért f|x és g|y, szóval (x,y)=0 N-ben. Ezekből követően

$$N \xrightarrow{P^k} M \twoheadrightarrow (fg)$$

injektív. A képtér tartalmazza (P^k,fg) ideált, ami véges indexű az előző lemme szerint. □

3.2.3. Állítás. *A prím ideáljai Λ-nak a 0,(p,T),(p),(P(T)), ahol P(T) irreducibilis és megkülönböztetett.*
A (p,T) ideál az egyetlen maximális ideál Λ-ban.

Bizonyítás. Az, hogy a felsoroltak prím ideálok könnyen belátható, ha felidézzük a definíciót. Legyen $\mathfrak{p} \neq 0$ egy prím ideál és h∈ $\mathfrak{p}$ egy minimális rendű elem. Ekkor h=p^sH úgy, hogy H=1 vagy H megkülönböztetett. Mivel $\mathfrak{p}$ prím, ezért p∈ $\mathfrak{p}$ vagy H∈ $\mathfrak{p}$. Ha 1≠H akkor H irreducubilisnek kell lennie h rendjének minimalitása miatt. Tehát (f)⊆ $\mathfrak{p}$, ahol f=p vagy f egy irreducibilis megkülönböztetett polinom. Ha (f)=$\mathfrak{p}$ ez egyike a listán lévőknek, tehát kész vagyunk. Szóval tegyük fel, hogy (f)≠ $\mathfrak{p}$, tehát létezik egy $g \in \mathfrak{p}$, amit nem oszt f. Mivel f irreducibilis, ezért f és g relatív prímek. Az előző lemma szerint $\mathfrak{p}$ véges indexű Λ-ban. Mivel $\Lambda/\mathfrak{p}$ véges $\mathbb{Z}_p$-modulus,ezért $p^N \in \mathfrak{p}$ valamilyen nagy N-re, így p∈ $\mathfrak{p}$ is, mivel $\mathfrak{p}$ prím, úgyanakkor $T^i \equiv T^j$ mod $\mathfrak{p}$ valamely i<j-re. Mivel $1 - T^{j-i} \in \Lambda^\times$, ezért T^i és p-hez hasonlóan $T \in \mathfrak{p}$ is, tehát $(p,T) \subseteq \mathfrak{p}$. Ezzel befejeztük a bizonyítást, mivel $\Lambda/(p,T) \simeq \mathbb{Z}/p\mathbb{Z}$, tehát (p,T) maximális ideál és $\mathfrak{p} = (p,T)$.
Minden ideált tartalmaz (p,T), ezért ez az egyetlen maximális ideál. □

3.2.4. Lemma. *Legyen $f \in \Lambda$ ekkor $\Lambda/(f)$ véges.*

Bizonyítás. Tegyük fel, hogy $f \neq 0$. Az általánosság elvesztése nélkül feltehető, hogy $f = p$ vagy f megkülönböztetett. Ha $f = p$ akkor $\Lambda/(f) \simeq \mathbb{Z}_p[[T]]/p\mathbb{Z}_p[[T]]$. Ha f megkülönböztetett akkor az osztási-algoritmussal készen vagyunk. □

3.2.5. Lemma. *Λ egy Noether gyűrű.*

Bizonyítás. A lemma könnyen belátható a Hilbert bázis tétel használatával, mivel elégséges belátni, hogy ha A noether akkor A[[T]] is noether. □

3.2.6. Definíció. Két Λ-modulus, M és M' pszeudo-izomorf, jelöljük

$$M \sim M',$$

ha létezik egy homomorfizmus M→M' véges maggal és komaggal. Más szóval létezik egy egzakt sorozata Λ-modulusoknak

$$0 \to A \to M \to M' \to B \to 0$$

ahol A és B véges Λ-modulus.

3.2.7. Észrevétel. *$M \sim M'$-ből nem következik, hogy $M' \sim M$. Például, $(p,T) \sim \Lambda$. Vegyünk egy $\Lambda \to (p,T)$ homomorfizmust, legyen $f(T)$ az $1 \in \Lambda$ képe. Ekkor Λ képe $(f) \subseteq (p,T)$, de $\Lambda/(f)$ végtelen, tehát $(p,T)/(f)$ is végtelen és a komag is végtelen, viszont megmutatható, hogy végesen generált Λ-torzió Λ-modulusokra $M \sim M' \iff M' \sim M$.*
Korábbi lemma szerint, ha $(f,g) = 1$ akkor

$$\Lambda/(fg) \sim \Lambda/(f) \oplus \Lambda/(g) \quad \text{és} \quad \Lambda/(f) \oplus \Lambda/(g) \sim \Lambda/(fg)$$

Tudni szeretnék a struktúráját a végesen generált Λ-modulusoknak. Erről szól a következő tétel.

3.2.8. Tétel. *Legyen M egy végesen generált Λ-modulus. Ekkor*

$$M \sim \Lambda^r \oplus \left(\bigoplus_{i=1}^{s} \Lambda/(p^{n_i}) \right) \oplus \left(\bigoplus_{j=1}^{l} \Lambda/(f_j(T)^{m_j}) \right),$$

ahol $r, s, t, n_i, m_j \in \mathbb{Z}$ és f_j egy megkülönböztetett irreducibilis polinomok.

Bizonyítás. Legyenek M generátorai $u_1, \ldots, u_n$, és köztük különböző összefüggésekkel

$$\lambda_1 u_1 + \cdots + \lambda_n u_n = 0 \quad \lambda_i \in \Lambda.$$

Mivel az összefüggések halmaza R részmodulusa Λ^n, és Λ noether, tehát az összefüggések végesen generáltak. Így M-t reprezentálhatjuk egy mártrixnak, aminek a sorai $(\lambda_1, \ldots, \lambda_n)$, ahol $\sum \lambda_i u_i = 0$ egy összefüggés. Ezt a mártixot is jelöljük R-rel.
Elsőnek nézzük meg a sorok és oszlopok közti műveleteket, amik az R és M generátorait módosítják.

Művelet A. Sorokat vagy oszlopokat fel lehet cserélni.

Művelet B. Egyik sorhoz vagy oszlophoz hozzáadhatunk egy mások sor vagy oszlop többszörösét. Például: ha $\lambda' = q\lambda + r$ akkor

$$\begin{pmatrix} \vdots & & \vdots & \\ \lambda & \cdots & \lambda' & \cdots \\ \vdots & & \vdots & \end{pmatrix} \to \begin{pmatrix} \vdots & & \vdots & \\ \lambda & \cdots & r & \cdots \\ \vdots & & \vdots & \end{pmatrix}.$$

Művelet C. Egy sort vagy oszlopot megszorozni $\Lambda^\times$ egy elemével.

Ezek a műveletek megtartják az izomorfizmust is. A következőkben olyan műveleteket nézünk, amik csak pszeudo-izomorfizmust tartják meg.

Művelet 1. Ha R tartalmaz olyan sort, hogy $(\lambda_1, p\lambda_2, \dots, p\lambda_n)$ és $p \nmid \lambda_1$. Ekkor az R mátrixot az R' mátrixá alakíthatjuk úgy, hogy az első sora $(\lambda_1, \lambda_2, \dots, \lambda_n)$ legyen és az első oszlop minden eleme p-vel szorzódik. Lásd:

$$\begin{pmatrix} \lambda_1 & p\lambda_2 & \dots \\ \alpha_1 & \alpha_2 & \dots \\ \beta_1 & \beta_2 & \dots \end{pmatrix} \to \begin{pmatrix} \lambda_1 & \lambda_2 & \dots \\ p\alpha_1 & \alpha_2 & \dots \\ p\beta_1 & \beta_2 & \dots \end{pmatrix}.$$

Speciálisan, ha minden λ nulla akkor $\alpha_1, \beta_1, \dots$ mindegyikét megszorozhatjuk p egy hatványával.

Bizonyítás. Legyen R-ben egy összefüggés a következő

$$\lambda_1 u_1 + p(\lambda_2 u_2 + \dots + \lambda_n u_n) = 0.$$

Legyen $M' = M \oplus v\Lambda$ a v új generátorral és modulo a következő összefüggések

$$(-u_1, pv) = 0 \quad (\lambda_2 u_2 + \dots + \lambda_n u_n, \lambda_1 v) = 0$$

Ekkor létezik egy természetes leképzés $M \to M'$. Tegyük fel, hogy $m \mapsto 0$, ekkor m eleme az összefüggések modulusának, tehát

$$(m, 0) = a(-u_1, pv) + b(\lambda_2 u_2 + \dots + \lambda_n u_n, \lambda_1 v)$$

valamely $a, b \in \Lambda$, így

$$ap = -b\lambda_1.$$

Mivel $p \nmid \lambda_1$ a feltétel szerint, ezért $p|b$, ugyanakkor, $\lambda_1|a$. Az M részben,

$$\begin{aligned} m &= -\frac{a}{\lambda_1}(\lambda_1 u_1) - \frac{a}{\lambda_1} p(\lambda_2 u_2 + \dots + \lambda_n u_n) \\ &= -\frac{a}{\lambda_1}(0) = 0. \end{aligned}$$

Mivel pv és $\lambda_1 v$ képei benne van M képében, ezért (p, λ_1) annullálja M'/M-et. Mivel $\Lambda/(p, \lambda_1)$ véges, ezért M' is végesen generált, tehát M'/M is véges, így

$$M \sim M'.$$

Az új modulus M' generátorai $v, u_2, \dots, u_n$. Minden $\alpha_1 u_1 + \dots + \alpha_n u_n = 0$ alakú összefüggésből, $p\alpha_1 u_1 + \dots + \alpha_n u_n = 0$ alakú lesz. Ezzel az állítást beláttuk. □

Művelet 2. Ha az első oszlop minden eleme osztható p^k-nal és ha van egy sora a mátrixnak $(p^k\lambda_1, \dots, p^k\lambda_n)$ alakban és $p \nmid \lambda_1$, akkor azt a sort kicserélhetjük $(\lambda_1, \dots, \lambda_n)$-ra. Lásd:

$$\begin{pmatrix} p^k\lambda_1 & p^k\lambda_2 & \dots \\ p^k\alpha_1 & \alpha_2 & \dots \end{pmatrix} \to \begin{pmatrix} \lambda_1 & \lambda_2 & \dots \\ p^k\alpha_1 & \alpha_2 & \dots \end{pmatrix}.$$

Bizonyítás. Legyen $M' = M \oplus \Lambda v$ moduló a következő összefüggések

$$(p^k u_1, -p^k v) = 0 \quad (\lambda_2 u_2 + \dots + \lambda_n u_n, \lambda_1 v) = 0.$$

M szintén beágyazható M'-be, mivel $p \nmid \lambda_1$ és (p^k, λ_1) ideál annullálja M'/M-et, tehát a hányados véges. Ezekből következik, hogy $M \sim M'$.
Tudjuk, hogy $p^k(u_1 - v) = 0$ és p^k osztja az első oszlopot, ezért M' felboklik,

$$M' = M'' \oplus (u_1 - v)\Lambda,$$

ahol M'' generátorai $v, u_2, \dots, u_n$ és az összefüggéseit $(\lambda_1, \dots, \lambda_n)$ és R generálja. Vegyük észre, hogy

$$(u_1 - v)\Lambda \simeq \Lambda/(p^k),$$

ez már a tételnek megfelelő alakban van, így a továbbiakban M''-vel fogunk foglalkozni. □

Művelet 3. Ha R egy sora $(p^k\lambda_1, \dots, p^k\lambda_n)$ alakú és valamilyen $p \nmid \lambda$-ra, $(\lambda\lambda_1, \dots, \lambda\lambda_n)$ is egy összefüggés, akkor R-t R'-re cserélhetjük, ahol R' minden sora ugyanaz, mint R-nek kivéve $(p^k\lambda_1, \dots, p^k\lambda_n)$ helyett $(\lambda_1, \dots, \lambda_n)$-t írunk.

Bizonyítás. Vegyük a következő szürjektív leképzést

$$M \to M' = M/(\lambda_1 u_1 + \dots + \lambda_n u_n)\Lambda.$$

A magot annillálja a (λ, p^k) ideál, micel M végesen generált, ezért a mag is. A $\Lambda/(\lambda, p)$ modulus véges, ezért a mag is az, tehát $M \sim M'$. □

Ezzel beláttuk, hogy a műveleteink megtartják a pszeudo-izomorfizmust, a következőkben $A, B, C, 1, 2, 3$-mal fogunk hivatkozni ezekre.
Most elkezdhetjük a tétel bizonyítását. Ha $0 \neq f \in \Lambda$, akkor

$$f(T) = p^\mu P(T)U(T)$$

, ahol $P(T)$ megkülönböztetett és $U \in \Lambda^\times$. Legyen

$$deg_w f = \begin{cases} \infty, & \mu > 0 \\ degP(T), & \mu = 0; \end{cases}$$

ez f Weierstrass foka. Adott R mátrixra definiálhatjuk a

$$deg^{(k)}(R) = \min \deg_w(a_{ij}) \quad \text{minden } i, j \geq k,$$

ahol (a'_{ij}) végig fut az összes olyan mátrixon, amit a műveleteinkkel kaphatubk és az első $(k-1)$ sort megtartja. Ha az R mátrix a következő alakú

$$\begin{pmatrix} \lambda_{11} & & 0 & 0 & \dots \\ & \ddots & & & \\ 0 & & \lambda_{r-1r-1} & 0 & \dots \\ * & \dots & * & * & \dots \\ * & \dots & * & * & \dots \end{pmatrix} = \begin{pmatrix} D_{r-1} & 0 \\ A & B \end{pmatrix}$$

ahol λ_{kk} megkülönböztetett és

$$deg\lambda_{kk} = deg_w\lambda_{kk} = deg^{(k)}(R), \quad \text{minden} 1 \leq k \leq r-1,$$

akkor azt mondjuk, hogy R $(r-1)$ normál alakban van.

3.2.9. Állítás. *Ha egy részmártrix $B \neq 0$ akkor R átalakítható a műveleteinkkel R'-vé úgy, hogy R' r-normál formájú és az első $r-1$ diagonális ellen ugyanaz.*

Az állítást nem bizonyítjuk, viszont a következőkben fel fogjuk tenni. [6]
Egy R mátrixot és indukcióval a következő alakba alakíthatjuk

$$\begin{pmatrix} \lambda_{11} & & & 0 \\ & \ddots & & \\ & & \lambda_{rr} & \\ A & & & 0 \end{pmatrix}$$

ahol minden λ_{jj} megkülönböztetett és $deg\lambda_{jj} = deg^{(j)}(R) \text{minden} j \leq r$. Az euklideszi algoritmus miatt feltehetjük, hogy λ_{ij} egy polinom és

$$deg\lambda_{ij} \leq deq\lambda_{jj}. \quad \text{minden} i \neq j.$$

Tegyük fel, hogy $\lambda_{ij} \neq 0$ valamely $i \neq j$-re. Mivel $deg_w\lambda_{jj}$ minimális, ezért $p|\lambda_{jj}$, tehát minden nemnulla összefüggés $(\lambda_{i1}, \dots, \lambda_{ir}, 0, \dots, 0)$, ami osztható p-vel. Legyen $\lambda = \lambda_{11} \dots \lambda_{rr}$., ekkor $p \nmid \lambda$, mivel minden λ_{jj} megkülönböztetett. Ekkor

$$(\lambda\frac{1}{p}\lambda_{i1}, \dots, \lambda\frac{1}{p}\lambda_{ir}, 0, \dots, 0)$$

egy összefüggés, mivel $\lambda_{jj}u_j = 0$. A 3-s művelet miatt feltehetjük, hogy p nem osztja egyetlen λ_{ij} valamely j-re, tehát

$$deg_w\lambda_{ij} \leq deg\lambda_{ij} < deg\lambda_{jj} = deg^{(j)}(R).$$

Ez lehetetlen $deg^{(j)}(R)$ minimalitása miatt, ezért $\lambda_{ij} = 0$ minden $i, j, i \neq j$. Modulusokként felírva

$$\Lambda/(\lambda_{11}) \oplus \cdots \oplus \Lambda/(\lambda_{rr}) \oplus \Lambda^{n-r}.$$

Ha a 2. műveletben lévő $\Lambda/(p^k)$ modulusokat hozzáadva megkaptuk a tételt. □

Megjegyzés: a diagonális elemek nem feltétlen irreducibilisok, de ezt megoldja a (13.8) lemma.

4. fejezet

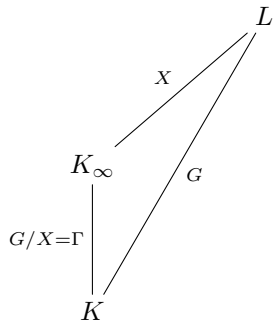
Iwasawa-elmélet

Ebben a fejezetben az második fejezetben belátott 2.2.8 tételt fogjuk általánosítani.

4.0.1. Tétel. *Legyen K_∞/K egy $\mathbb{Z}_p$-bővítés. Legyen p^{e_n} egy hatványa p-nek, ami osztja K_n osztályszámát. Ekkor léteznek olyan egészek, $\lambda \geq 0$,$\mu \geq 0$, és ν függetlenek n-től, hogy létezik egy n_0, hogy*

$$e_n = \lambda n + \mu p^n + \nu \quad \textit{minden } n \geq n_0.$$

Bizonyítás. Legyen $\Gamma = \mathrm{Gal}(K_\infty/K) \simeq \mathbb{Z}_p$, és legyen γ_0 topologiai generátora Γ-nak. Legyen L_n a maximális nem elágazó Abel p-bővítése K_n-nek, azaz $X_n = \mathrm{Gal}(L_n/K_n) \simeq A_n$, ami egy p-Sylow-ja K_n ideál osztály csoportjának. Legyen $L = \bigcup_{n\geq 0}^{n} L_n$ és $X = \mathrm{Gal}(L/K_\infty)$. Minden L_n Galois K felett, mivel L_n maximális, ezért ezeknek az uniója is Galois. Legyen $G = \mathrm{Gal}(L/K)$. Tujduk venni a következő diagrammot.



A bizonyítás lényege az lesz, hogy X-t egy Γ-modulusként($\mathbb{Z}_p$-modulus) írjuk fel, ami egyben Λ-modulus is, amiről beláttuk, hogy végesen generált és Λ-torziós, tehát pszeudo-izomorf $\Lambda/(p^k)$ és $\Lambda/(P(T)^k)$ alakú Λ-modulusok direkt összegével.

Egy speciális esettel fogunk kezdeni.

Feltétel. *Minden prím, ami elágazik K_∞/K fölött az teljesen elágazik.*
3.1.3 lemma beláttuk, hogy ez megtehető, ha K-t kicseréljük egy K_n-re vamilyen n-re. Feltétel szerint,

$$K_{n+1} \cap L_n = K_n,$$

tehát

$$\mathrm{Gal}(L_n/K_n) \simeq \mathrm{Gal}(L_nK_{n+1}/K_{n+1}),$$

ami része X_{n+1}=Gal(L_{n+1}/K_{n+1}). Van egy leképzésünk X_{n+1}, X_n között

$$X_{n+1} \to X_n.$$

Ez megfelel egy norma leképzésnek $A_{n+1} \to A_n$ ideál osztály csoportok között. Vegyük észre, hogy

$$X_n \simeq \mathrm{Gal}(L_nK_\infty/K_\infty),$$

tehát

$$\varprojlim X_n \simeq \varprojlim \mathrm{Gal}((\bigcup L_n K_\infty)/K_\infty) = \mathrm{Gal}(L/K_\infty) = X.$$

Legyen $\gamma \in \Gamma_n = \Gamma/\Gamma^{p^n}$. Bővítsük γ-t $\tilde{\gamma} \in \mathrm{Gal}(L_n/K)$. Legyen $x \in X_n$. Ekkor γ hat x-en a következő képpen

$$x^\gamma = \tilde{\gamma} x (\tilde{\gamma})^{-1}.$$

Mivel $\mathrm{Gal}(L_n/K_n) = X_n$ Abel, ezért x^γ jól definiált, ezzel X_n egy $\mathbb{Z}_p[\Gamma_n]$-modulus. Most tekintsük X-t, mint $X \simeq \varprojlim X_n$ végtelen dimenziós vektorteret és egy eleme $(x_0, x_1, \dots)$. $\mathbb{Z}_p[\Gamma_n]$ hat az n-edik elemen.

4.0.2. Állítás. *X egy Λ-modulus.*

Bizonyítás. Tudjuk, hogy X_n egy Γ-modulus, mivel γ_0 a generátora és $(\gamma_0 - 1)X_n$ egy nem triviális részcsoportja, ezért X_n elő áll, mint $\Gamma \simeq \mathbb{Z}_p[T]$-fölötti modulus. Ekkor X_n modulus $\mathbb{Z}_p[T]/(p_n^a, T_n^b) \simeq \mathbb{Z}_p[[T]]/(p_n^a, T_n^b)$ fölött,tehát X_n egy Λ-modulus, amit annullál az (p_n^a, T_n^b) ideál. Legyen $t_n = a_n + b_n$ ekkor $(p,T)^{t_n} \subseteq (p_n^a, T_n^b)$, így X_n-t nézhetjük, mint $\Lambda/(p,T)^{t_n}$ fölötti modulus. Ezzel beláttuk az állítást. □

Legyenek $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ prímek, amik elágaznak K_∞/K fölött és $\tilde{\mathfrak{p}_i}$ $\mathfrak{p}_i$ fölötti fix prímje L-nek. Legyen $I_i \subseteq G$ az inercia csoportok. Mivel L/K_∞ nem ágazik el, ezt

$$I_i \cap X = 1.$$

Valamint K_∞/K teljesen elágazik $\mathfrak{p}_i$ fölött, ezért

$$I_i \hookrightarrow G/X = \Gamma,$$

szürjektív, így bijektív is. Tehát

$$G = I_i X = X I_i, \quad i = 1, \dots, s.$$

Legyen $\sigma_i \in I_i$ γ_i-ba képződik. Ekkor σ_i-nak szükséges I_i topologiai generátorának lennie. Tudjuk, hogy

$$I_i \subseteq X I_1,$$

tehát

$$\sigma_i = a_i \sigma_1$$

valamilyen $a_i \in X$.

4.0.3. Lemma. *(A korábban feltett feltétel mellett). Legyen G' a lezártja G kommutátor csoportjának. Ekkor*

$$G' = X^{\gamma_0 - 1} = TX.$$

Bizonyítás. Mivel $\Gamma \simeq I_1 \subseteq G$ ráképez $\Gamma = G/X$-re, ezért felemelhetjük $\gamma \in \Gamma$ egy megfelelő elembe I_1-ben, így tudjuk definiálni Γ hatását X-n. Következőkben Γ-t és I_1-t megfeleltetjük egymásnak, tehát $x^\gamma = \gamma x \gamma^{-1}$. Legyen

$$a = \alpha x, b = \beta y, \quad \alpha, \beta \in \Gamma, x, y \in X,$$

szabadon választott elemei $G = \Gamma X$-nek. Ekkor

$$\begin{aligned} aba^{-1}b^{-1} &= \alpha x \beta y x^{-1} \alpha^{-1} x^{-1} \beta^{-1} \\ &= x^\alpha \alpha \beta y x^{-1} \alpha^{-1} y^{-1} \beta^{-1} = x^\alpha (yx^{-1})^{(\alpha\beta)} (\alpha\beta) \alpha^{-1} y^{-1} \beta^{-1} \\ &= x^\alpha (yx^{-1})^{(\alpha\beta)} (y^{-1})^\beta \quad \text{(Mivel } \Gamma \text{ Abel)} \\ &= (x^\alpha)^{1-\beta} (y^\beta)^{\alpha - 1}. \end{aligned}$$

Legyen $\beta = 1, \alpha = \gamma_0$. Azt kapjuk, hogy $y^{\gamma_1 - 1} \in G'$, tehát

$$X^{\gamma_0 - 1} \subseteq G'.$$

Minden β-ra létezik egy $c \in \mathbb{Z}_p$, hogy $\beta = \gamma_0^c$, tehát

$$1 - \beta = 1 - \gamma_0^c = 1 - (1+T)^c = 1 - \sum_{n=0}^{\infty} \binom{c}{n} T^n \in T\Lambda.$$

Mivel $\gamma_0 - 1 = T, (x^\alpha)^{1-\beta} \in X^{\gamma_0 - 1}$. Hasonlóan $(y^\beta)^{1-\alpha} \in X^{\gamma_0 - 1}$. Mindezek után, mivel $X^{\gamma_0 - 1} = TX$ zárt (hiszen egy kompakt halmaz képe), így $G' \subseteq X^{\gamma_0 - 1}$. Ezzel a lemmát beláttuk. □

4.0.4. Lemma. *(A korábban feltett feltétel mellett). Legyen Y_0 egy $\mathbb{Z}_p$-részmodulusa X-nek a következő generátorokkal $\{a_i | 2 \le i \le s\}$ és $X^{\gamma_0 - 1} = TX$ által. Legyen $Y_n = \nu_n Y_0$, ahol*

$$\nu_n = 1 + \gamma_0 + \gamma_0^2 + \cdots + \gamma_0^{p^n - 1} = \frac{(1+T)^{p^n} - 1}{T}.$$

Ekkor

$$X_n \simeq X/Y_n \quad \textit{minden } n \ge 0.$$

Bizonyítás. Nézzük az $n = 0$ esetet. Tudjuk, hogy $K \subseteq L_0 \subseteq L$. Mivel L_0 egy maximális elágazásmentes Abel p-bővítése K-nak és L/K is egy p-bővítés, ezért L_0/k is egy maximális elágazásmentes Abel p-bővítése L/K-nak. Tehát $\mathrm{Gal}(L/L_0)$ egy zárt részcsoportja G-nek, amit G' és az inercia csoportok generálnak, azaz $X^{\gamma_0 - 1}, I_1, a_2, \ldots, a_s$, szóval

$$\begin{aligned} X_0 = \mathrm{Gal}(L_0/K) &= G/\mathrm{Gal}(L/L_0) = XI_1/\mathrm{Gal}(L/L_0) \\ &\simeq X/\overline{\langle X^{\gamma_0 - 1}, a_2, \ldots, a_s \rangle} = X/Y_0, \end{aligned}$$

Tegyük fel, hogy $n \ge 1$. K-t cseréljük ki K_n-re és γ_0-t $\gamma_0^{p^n}$-ra. Ekkor σ_i-ből $\sigma_i^{p^n}$ lesz. Vegyük észre, hogy

$$\begin{aligned} \sigma_i^{k+1} &= (a_i \sigma_1)^{k+1} = a_i \sigma_1 a_i \sigma_1^{-1} \sigma_1^2 a_i \sigma_i^{-2} \ldots \sigma_1^k a_i \sigma_1^{-k} \sigma_1^{k+1} \\ &= a_i^{1 + \sigma_1 + \cdots + \sigma_1^k} \sigma_1^{k+1}. \end{aligned}$$

Így tudjuk, hogy

$$\sigma_i^{p^n} = (\nu_n a_u) \sigma_1^{p^n},$$

tehát a_i-t kicseréltük $\nu_n a_i$-re. Végezetük cseréljük ki $X^{\gamma_0 - 1}$-t $(\gamma_0^{p^n} - 1)X = \nu_n X^{\gamma_0 - 1}$, tehát Y_0-ból $\nu_n Y_0$, amivel a lemmát beláttuk. □

4.0.5. Lemma. *(Nakayama Lemma). Legyen X egy kompakt Λ-modulus. Akkor*

$$X \textit{ végesen generált } \Lambda \textit{ fölött} \iff X/(p,T)X \textit{ véges.}$$

Ha $x_1, \ldots, x_n$ generálja $X/(p,T)X$-t $\mathbb{Z}$ fölött, akkor generálják X-t Λ fölött. Speciálisan:

$$X/(p,T)X = 0 \iff X = 0.$$

Bizonyítás. Vegyünk egy kis környezetét a 0-nak X-ben, legyen U. Mivel $(p,T)^n \to 0$ Λ-ban, így minden $z \in X$ létezik egy U_z környezete, hogy $(p,T)^n U_z \subseteq U$ nagy n-re. Mivel X kompakt, ezért véges sok U_z lefedi X-t, tehát van olyan n, hogy $(p,T)^n X \subseteq U$. Tehát $\bigcap((p,T)^n X) = 0$ minden kompakt Λ-modulusra.
Tegyük fel, hogy $x_1, \ldots, x_n$ generálja $X/(p,T)X$-t. Legyen $Y = \Lambda x_1 + \cdots + \Lambda x_n \subseteq X$. Ekkor Y kompakt, mivel Λ^n képe, tehát X/Y is kompakt Λ-modulus. A feltétel miatt $Y + (p,T)X = X$, ezért

$$(p,T)(X/Y) = (Y + (p,T)X)/Y = X/Y,$$

szóval

$$(p,T)^n (X/Y) = X/Y \quad \text{minden } n \ge 0.$$

A fentiekből következik, hogy $X/Y = 0$, tehát $X = Y$ és $\{x_i\}$ generálja X-t. □

4.0.6. Lemma. *(A korábban feltett feltétel mellett). $X = Gal(L/K_\infty)$ végesen generált Λ-modulus,*

Bizonyítás. Vegyük észre, hogy $\nu_1 \in (p,T)$, tehát $Y_0/(p,T)Y_0$ része $Y_0/\nu_1 Y_0 = Y_0/Y_1 \subseteq X/Y_1 = X_1$-nek, ami véges. Ebből már következik, hogy Y_0 is véges, szóval X is véges, mivel $X/Y_0 = X_0$ véges. □

Megjegyzés. A feltétel elhagyásával általánosan is beláthatjuk. Legyen K_∞/K egy $\mathbb{Z}_p$-bővítés és válassunk egy $e \ge 0$, amire K_∞/K_e fölött minden elágazó prím teljesen elágazik. Ekkor a 4.0.4 lemmát és 4.0.6 lemmát felhasználva K_∞/K_e-re azt kapjuk, hogy az az X modulus, ami megegyezik K_e-re és K-ra az végesen generált Λ-modulus. Ekkor minden $n \ge e$

$$1 + \gamma_0^{p^e} + \gamma_0^{2p^e} + \cdots + \gamma_0^{p^n - p^e} = \frac{\nu_n}{\nu_e} \overset{\text{def}}{=} \nu_{n,e}.$$

Ezzel a jelöléssel Y_e-t vehetjük, mint K_e Y_0-ja. Ekkor

$$Y_n = \nu_{n,e} Y_e, \quad \text{és} \quad X_n \simeq X/Y_n, \quad \text{minden } n \geq e.$$

Ezzel beláttuk a következő lemmát.

4.0.7. Lemma. *Legyen K_∞/K egy $\mathbb{Z}_p$-bővítés. Ekkor X végesen generált Λ-modulus és létezik egy $e \geq 0$, hogy*

$$X_n \simeq X/\nu_{n,e} Y_e, \quad \textit{minden } n \geq e.$$

Most használjuk X-re a végesen generált Λ-modulusok struktúra tételét, ezt megtehetjük Y_e-re is mivel X/Y_e véges. Tehát

$$Y_e \sim X \sim \Lambda^r \oplus (\bigoplus \Lambda/(p^{k_i})) \oplus (\bigoplus \Lambda/(f_j(T)^{m_j})).$$

Most nézzük meg milyen tagok szerepelhetnek a jobb oldalt, ha a $V/\nu_{n,e}V$ hányadost nézzük.

1. $V = \Lambda$. Ez végtelen az 3.2.4 lemma miatt. Mivel $V/\nu_{n,e}V$ véges, ezért ez nem lehet.

2. $V = \Lambda/(p^k)$. Ebben az esetben
$$V/\nu_{n,e}V \simeq \Lambda/(p^k \nu_{n,e}).$$
Két megkülönböztetett polinom hányadosa egy polinom, akkor az is megkülönbőztetett, vagy konstant. Tegyük fel, hogy nem az lenne, akkor azaz $\frac{f}{g} = h$, ahol f, g megkülönbőztetett, de h nem az. Akkor $f = gh$, ami ellent mond annak, hogy f megkülönbőztetett, mert létezik $i \geq \deg(g)$, hogy f_i, f i-edik együtthatója nem lenne $\mathfrak{p}$-beli. Hiszen h_j nem $\mathfrak{p}$-beli, tehát $f_{i+j} = \mathfrak{p} + h_j$. Ezt tudva
$$\nu_{n,e} = \frac{\nu_n}{\nu_e} = \frac{((1+T)^{p^n} - 1)/T}{((1+T)^{p^e} - 1)/T}$$
is megkülönböztetett. Az osztási algoritmusból kapjuk, hogy $\Lambda/\nu_{n,e}$ elemei legfeljebb $\nu_{n,e}$-ed fokú polinom mod p^k. Tehát
$$|V/\nu_{n,e}V| = p^{k(p^n - p^e)} = p^{kp^n + c},$$
valamilyen c konstansra.

3. $V = \Lambda/(f(T)^m)$. Legyen $g(T) = f(T)^m$ és a foka d. Ekkor
$$T^d \equiv pQ(T) \bmod g$$
valamilyen $Q(T)$ polinomra, ezelből
$$T^k \equiv (p)(\text{polinom}) \bmod g \quad k \geq d.$$
Ha $p^n \geq$ akkor
$$\begin{aligned}(1+T)^{p^n} &= 1 + (p)(\text{polinom}) + T^{p^n} \\ &\equiv 1 + (p)(\text{polinom}) \bmod g.\end{aligned}$$
Tehát
$$(1+T)^{p^n} \equiv 1 + p^2 \text{polinom} \bmod g.$$
Ezekből következik
$$\begin{aligned}P_{n+2} &= (1+T)^{p^{n+2}} - 1 \\ &= ((1+T)^{(p-1)p^{n+1}} + \cdots + (1+T)^{p^{n+1}} + 1)(((1+T)^{p^{n+1}} - 1) \\ &= (1 + \cdots + 1 + (p^2)(\text{polinom}))(P_{n+1}(T)) \\ &= p(1 + (p)(\text{polinom}))P_{n+1}(T) \bmod g.\end{aligned}$$

Mivel 1+(p)(polinom)$\in \Lambda^\times$,

$$\frac{P_{n+2}}{P_{n+1}} \text{ ami } (p) \times \text{(egységként) hat } V = \Lambda/(g)\text{-n},$$

minden $p^n \geq d$. Tegyük fel, hogy $n_0 > e, p^{n_0} \geq d$, és $n \geq n_0$. Ekkor

$$\frac{\nu_{n+2,e}}{\nu_{n+1,e}} = \frac{\nu_{n+2}}{\nu_{n+1}} = \frac{P_{n+2}}{P_{n+1}},$$

és

$$\nu_{n+2,e}V = \frac{P_{n+2}}{P_{n+1}}(\nu_{n+1,e}V) = p\nu_{n+1,e}V.$$

Tehát

$$|V/\nu_{n+2,e}V| = |V/pV||pV/p\nu_{n+1,e}V|$$

minden $n \geq n_0$. Mivel $(g,p) = 1$, ezért a p-vel való szorzás injektív, szóval

$$|pV/p\nu_{n+1,e}V| = |V/\nu_{n+1,e}V|.$$

Tudjuk, hogy

$$V/pV \simeq \Lambda/(p,g) = \Lambda/(p,T^d),$$

ezért $|V/pV| = p^d$. Indunkcióval beláthatjuk, hogy

$$|V/\nu_{n,e}V| = p^{d(n-n_0-1)}|V/\nu_{n_0+1,e}V|$$

minden $n \geq n_0 + 1$. Ha $V/\nu_{n,e}V$ véges minden n-re, akkor

$$|V/\nu_{n,e}V| = p^{dn+c}, \quad n \geq n_0 + 1$$

valamely c konstansra. Ha végtelen akkore nem lehet az összegben, ami akkor lehet, ha $(\nu_{n,e}, f) \neq 1$. Ezzek kapjuk a következő állítást.

4.0.8. Állítás. *Legyen*

$$E = \Lambda^r \oplus \bigoplus_{i=1}^{s} \Lambda/(p^{k_i}) \oplus \bigoplus_{j=1}^{t} \Lambda/(g_j(T)),$$

ahol minden $g_j(T)$ megkülönbőztetett (nem feltétlen irreducibilis). Legyen $m = \sum k_i$ és $l = \sum degg_j$. Ha $E/\nu_{n,e}E$ véges minden n-re akkore $r = 0$ és letezik egy n_0 és c konstans, hogy

$$E/\nu_{n,e}E = p^{mp^n+ln+c}, \quad \textit{minden } n > n_0.$$

Vegyük a következő egzakt sorozatot

$$0 \to A \to Y_e \to E \to B \to 0$$

ahol A, B végesel és E, ahogyan az előző állításban definiáltuk. Y_e rendjét szeretnénk megtudni, amihez a következő lemmára lesz szükségünk.

4.0.9. Lemma. *Tegyük fel, hogy Y és E Λ-modulusok úgy, hogy $Y \sim E$ és $Y/\nu_{n,e}Y$ véges minden n-re. Ekkor léteziknek konstansok c, n_0, hogy*

$$|Y/\nu_{n,e}Y| = p^c|E/\nu_{n,e}E \quad \textit{minden } n \geq n_0.$$

Bizonyítás. Nézzük a következő kommutatív diagrammot

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \nu_{n,e}Y & \xrightarrow{f} & Y & \xrightarrow{g} & Y/\nu_{n,e}Y & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi'_n} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi''_n} & & \\ 0 & \longrightarrow & \nu_{n,e}E & \xrightarrow{f'} & E & \xrightarrow{g'} & E/\nu_{n,e}E & \longrightarrow & 0 \end{array}$$

A következő egyenlőtlenségek teljesülnek

1. $|\text{Ker}\phi'_n| \leq |\text{Ker}\phi|$
2. $|\text{Coker}\phi'_n| \leq |\text{Coker}\phi|$
3. $|\text{Coker}\phi''_n| \leq |\text{Coker}\phi|$
4. $|\text{Ker}\phi''_n| \leq |\text{Ker}\phi||\text{Coker}\phi|$.

Tudjuk, hogy $f\phi = \phi'_n f'$. Tudjuk, hogy f és f' egy-egy monomorfizmus. Ebből a kettőből következik az első egyenlőtlenség, mivel ϕ és ϕ'_n vehető, mint $\nu_{n,e}Y \xrightarrow{\phi,\phi'_n} \nu_{n,e}E$ függvények és itt megegyezik a magjuk. Vegyük Coker(ϕ)-nek reprezentásait, ha ezt beszorozzuk $\nu_{n,e}$-vel akkor reprezentánsok lesznek Coker(ϕ'_n)-nek. Hasonlóan, mivel $E/\nu_{n,e}E \subseteq E$, ezért Coker(ϕ''_n)$\subseteq$Coker(ϕ). Már csak a 4.-t kell bizonyítanunk. A Kígyó lemma [7] alapján létezik egy hosszú egzakt sorozat

$$0 \to \text{Ker } \phi'_n \to \text{Ker}\phi \to \text{Ker } \phi''_n \to \text{Coker } \phi'_n \to \text{Coker } \phi \to \text{Coker } \phi''_n \to 0.$$

Ebből következik is, hogy

$$|\text{Ker } \phi''_n| \leq |\text{Ker } \phi||\text{Coker } \phi'_n| \leq |\text{Ker } \phi||\text{Coker } \phi|,$$

utolsó lépésben használjuk a 2-est, ezzel beláttuk a 4-est is.
Tegyük fel, hogy $m \geq n \geq 0$. A következő egyenlőtlenségek teljesülnek

1. $|\text{Ker } \phi'_n| \geq |\text{Ker } \phi'_m|$
2. $|\text{Coker } \phi'_n| \geq |\text{Coker } \phi'_m|$
3. $|\text{Ker } \phi''_n| \leq |\text{Ker } \phi''_m|$.

Tudjuk, hogy $\nu_{m,e}Y \subseteq \nu_{n,e}Y$, tehát Ker $\phi'_, \subseteq$ Ker ϕ'_n. Legyen $\nu_{m,e}y \in \nu_{m,e}E$ és $z \in \nu_{n,e}E$ egy reprezentánsa $\nu_{n,e}y$-nak Cokerϕ'_n-ben. Ekkor

$$\nu_{n,e}y - z = \phi(\nu_{n,e}x) \quad \text{valamilyen } x \in Y.$$

Beszorozva $\frac{\nu_{m,e}}{\nu_{n,e}}$-vel ezt kapjuk

$$\nu_{m,e}y - (\frac{\nu_{m,e}}{\nu_{n,e}})z = \phi(\nu_{m,e}x) = \phi'_m(\nu_{m,e}x).$$

Tehát $(\frac{\nu_{m,e}}{\nu_{n,e}})$-val szorozva Coker ϕ'_n reprezentásait akkor Cokert ϕ'_m reprezentánsait kapjuk. Mivel $\nu_{m,e}E \subseteq \nu_{n,e}E$, ezért az utolsó egyenlőtkenség is igaz.
Az előző 7 darab egyenlőtlenséggel Ker ϕ'_n,Coker ϕ'_n és Coker ϕ''_n rendjei konstansok valamilyen $n \geq n_0$. Egyetlen egy dolog maradt, belátni, hogy Ker ϕ''_n is konstant. A Kígyó lemma alapján

$$|\text{Ker } \phi'_n||\text{Ker } \phi''_n||\text{Coker } \phi| = |\text{Ker } \phi||\text{Coker } \phi'_n||\text{Coker } \phi''_n|.$$

Ebből következik, hogy $|\text{Ker } \phi''_n|$ konstans $n \geq n_0$. □

Vegyük E-t, $\lambda \geq 0, \mu \geq 0$,$\nu, n_0$ egészek, hogy

$$\begin{aligned} p^{e_n} = |X_n| &= |X/Y_e||Y_e/\nu_{n,e}Y_e \\ &= (\text{konstans})|E/\nu_{n,e}E| \\ &= p^{\lambda n + \mu p^n + \nu}, \quad \text{minden } n > n_0. \end{aligned}$$

Ezzel a tételt beláttuk. □

5. fejezet

Következmények

Ebben a fejezetben az előző fejezet tételének egyes következményet fogjuk vizsgálni.

5.0.1. Állítás. *Tegyük fel, hogy E olyan mint a xy lemmában úgy, hogy $r = 0$. Ekkor*

$$m = 0 \iff p - rang(E/\nu_{n,e}E) \text{ korlátos, ahogyan } n \to \infty.$$

Bizonyítás. Emlékezzünk, hogy egy véges Abel csoport $p-$rangja a csoport ciklikusokra való direkt felbontásában szereplő p hatvány rendú csoportok száma. Ez megegyezik a következővel

$$\dim_{\mathbb{Z}/p\mathbb{Z}}(A/pA).$$

Tudjuk, hogy $\nu_{n,e}$ megkülönböztetett polonom és a foka $p^n - p^e$. Ha deg $\nu_{n,e} \geq \max$ deq g_j, akkor

$$\begin{aligned} E/(p,\nu_{n,e})E &= \left(\bigoplus_{j=1}^{s} \Lambda/(p,\nu_{n,e})\right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(p,g_j,\nu_{n,e}))\right) \\ &= \left(\bigoplus_{j=1}^{s} \Lambda/(p,T^{p^n-p^e})\right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(p,T^{\deg g_j}))\right) \\ &\simeq (\mathbb{Z}/p\mathbb{Z})^{s(p^n-p^e)+l}. \end{aligned}$$

Tehát a rang akkor és csak akkor korlátos, ha $s = 0$. □

5.0.2. Állítás. *Tegyük fel, hogy K_∞/K egy $\mathbb{Z}_p$-bővítés, amiben pontosen egy prím ágazik el és ez teljesen elágazik. Ekkor*

$$A_n \simeq X_n \simeq X/((1+T)^{p^n} - 1)X$$

és

$$p \nmid h_0 \iff p \nmid h_n \quad \text{minden } n \geq 0.$$

Bizonyítás. Mivel K_∞/K kielégíti a 4.0.1 tétel feltételét, így használhatjuk a 4.0.4 lemmát. Tudjuk, hogy $s = 1$, tehát $Y_0 = TX$ és $Y_n = ((1+T)^{p^n} - 1)X$. Ezzel az első felével kész is vagyunk. Ha $p \nmid h_0$, akkor $X/TX = 0$, tehát $X/(p,T)X = 0$. Nakayama lemma miatt $X = 0$. Ezzel az állítást beláttuk. □

5.0.3. Állítás. $\mu = 0 \iff p - rang(A_n) korlátos, ahogyan\ n \to \infty$.

Bizonyítás. Tudjuk, hogy $Y_e \sim E$, ahol E olyan mint 4.0.8 lemmában. Az itteni első lemma szerint $\mu = 0 \iff p - \text{rang}(E/\nu_{n,e}E)$ korlátos. Vegyük az 4.0.9 lemma bizonyításában használt egzakt sorozatot

$$0 \to C_n \to Y_e/\nu_{n,e}Y \to E/\nu_{n,e}E \to B_n \to 0$$

ahol $|C_n|, |B_n|$ n-től függetlenül korlátosak. Ebből következik, hogy

$$\mu = 0 \iff p - \text{rang}(Y/\nu_{n,e}Y) \text{ korlátos},$$

de

$$A_n \simeq X_n \simeq X/\nu_{n,e}Y_e.$$

Mivel X/Y_e véges, ezért az állítást beláttuk. □

Megjegyzés:
Tegyük fel, hogy K_n CM-testek. Ekkor K_∞^+/K^+ egy $\mathbb{Z}_p$-bővítés (Ha igaz a Leopoldt sejtés, akkor az 3.1.4 Tételből következik). Ha p páratlan, akkor felbonthatjuk A_n-t, ami K_n osztálycsoportjának egy p-Sylow-ja, A következő alakot kapjuk

$$A_n = A_n^+ \oplus A_n^-.$$

Hasonlóan,

$$X_n = X_n^+ \oplus X_n^-,$$

így

$$X = X^+ \oplus X^-.$$

Megkaphatjuk az 4.0.1 tételhez hasonló állításokat,

$$A_n^\pm \simeq X_n^\pm \simeq X^\pm/\nu_{n,e}Y^\pm.$$

Ha $p^{e_n^\pm}$ egy hatványa p-nek, ami osztja $h_n^\pm$-t, akkor

$$e_n = e_n^+ + e_n^-.$$

Végül,

$$e_n^\pm = \lambda^\pm n + \mu^\pm p^n + \nu^\pm \quad \text{minden } n \geq n_n^\pm,$$

ahol

$$\lambda = \lambda^+ + \lambda^-, \quad \mu = \mu^+ + \mu^-, \quad \nu = \nu^+ + \nu^-.$$

A 4.0.1 állítás analógjaként kapjuk, hogy

$$\mu^\pm = 0 \iff p - \text{rang}(A^\pm) \text{ korlátos.}$$

Ha $p = 2$ akkor nem tudjuk A_n-t felbontani, viszont ha

$$A_n^- = \{a | Ja = -a\} \quad (\text{ahol } J \text{ a komplex konjugálás}).$$

Ekkor az előző fejezet főtétele igaz lesz A_n^-, X_n^--re. Meg tudjuk adni e^+-t is, ha A_n^+ helyett $A_n(K_n^+)$-t nézzük. Ekkor a következőt kapjuk

$$e_n^\pm = \lambda^\pm n + \mu^\pm 2^n + \nu^\pm.$$

Az egzat sorozatból

$$0 \to A_n^- \to A_n \xrightarrow{1+J} A(K_n^+) \to 0$$

a következőt kapjuk

$$\begin{aligned} \mu &= \mu^+ + \mu^- \quad \text{és} \\ \mu^+ = 0 &\iff 2 - \text{rang } A(K_n^+) \text{ korlátos} \\ \mu^- = 0 &\iff 2 - \text{rang } A_n^- \text{ korlátos} \end{aligned}$$

5.0.4. Tétel. *Legyen p egy páratlan prím. Legyen L egy CM-test és $\zeta_p \in L$. Legyen A a p-Sylow részcsportja L osztálycsoportjának. Ekkor*

$$p - rang A^+ \leq 1 + p - rang A^-.$$

Legyen W az L beli egységgyökök. Ha $L(W^{1/p})/L$ (teljesen) elágazik, akkor

$$p - rang A^+ \leq p - rang A^-.$$

($A^\pm = \{x \in A | \bar{x} = x^{\pm 1}\}$ és $A^+ \simeq A(L^+)$).

5.0.5. Állítás. *Legyen L egy CM-test és A_L, A_{L^+} a 2-Sylow részcsoportja L, L^+-nek. Ekkor*

$$2 - rang A_{L^+} \leq 1 + 2 - rang A_L^-.$$

Ennek a tételnek és állításnak a bizonyítása megtalálható a Whashinton könyv 192-n oldalán.

5.0.6. Állítás. *Legyen p prím. Tegyük fel, hogy K egy CM-test és $\zeta_p \in K$, illetve legyen K_∞/K egy körosztási $\mathbb{Z}_p$-bővítés. Ekkor*

$$\mu = 0 \iff \mu^- = 0.$$

Bizonyítás. "$\Rightarrow$" triviális, hiszen $\mu = \mu^+ + \mu^-$. Tegyük fel, hogy $\mu^- = 0$ ekkor $p-$rang A_n^- korlátos. A használva az előző tételt és állítást azt kapjuk, hogy $p-$rangA_n^+(2-rang $A(K_n^+)$) korlátos, amiből következik, hogy $\mu^+ = 0$. Ezzel beláttuk az állítást. □

5.0.7. Állítás. *Tegyük fel, hogy K_∞/K egy $\mathbb{Z}_p$-bővítés és $\mu = 0$. Ekkor*

$$X \simeq \varprojlim A_n \simeq \mathbb{Z}_p^\lambda \oplus \textit{(véges p-csoport)}$$

mint $\mathbb{Z}_p$-modulusok.

Bizonyítás. Tudjuk, hogy

$$X \sim E = \bigoplus_j \Lambda/(g_j(T))$$

ahol minden g_j megkülönbőztetett és $\sum g_j = \lambda$. Az osztási algoritmus szerint

$$\Lambda/(g_j(T)) \simeq \mathbb{Z}_p^{\deg g_j}.$$

Így azt kapjuk, hogy

$$E \simeq \mathbb{Z}_p^p.$$

Mivel X egy $\mathbb{Z}_p$-modulus, ami végesen generált, ezért a struktúra tételből következik az állítás. □

5.0.8. Állítás. *Legyen p egy páratlan prím. Legyen K egy CM-test és K_∞/K egy körosztási $\mathbb{Z}_p$-bővítése K-nak. Ekkor a következő leképzés injektív*

$$A_n^- \to A_{n+1}^-.$$

Megjegyzés: Szükséges feltennünk, hogy p páratlan, illetve A^+-ra nem feltétlen igaz az állítás.

Bizonyítás. Legyen I egy ideálja A_n-nek, ami főideál K_{n+1}-ben, tehát

$$I = (\alpha).$$

Legyen σ a generátora $\mathrm{Gal}(K_{n+1}/K)$-nak. Ekkor

$$(\alpha^{\sigma-1}) = \frac{I^\sigma}{I} = (1).$$

Következik, hogy

$$\alpha^{\sigma-1} = \varepsilon \in E_{n+1} = K_{n+1} \text{ egységei.}$$

Legyen N egy norma K_{n+1}/K_n-n. Ekkor

$$N\epsilon = (N\alpha)^{\sigma-1} = 1.$$

Tegyük fel, hogy I reprezentálja A_n^- egy osztályát. Jelöljük J-vel a komplex konjugálást. Ekkor

$$I^{1+J} = (\beta), \quad \beta \in K_n \quad (\text{azaz } \beta^\sigma = \beta),$$

tehát

$$\alpha^{1+J} = \beta\eta \quad \eta \in E_{n+1}.$$

Legyen

$$\alpha_1 = \frac{\alpha^2}{\eta},$$

és

$$\varepsilon_1 = \alpha_1^{\sigma-1} = \frac{\varepsilon^2}{\eta^{\sigma-1}} \in E_{n+1}.$$

Ekkor

$$\varepsilon_1^{1+J} = (\alpha_1^{1+J})^{\sigma-1} = (\beta^2)^{\sigma-1}(\eta^{\sigma-1})^{1-J} = (\eta^{\sigma-1})^{1-J} \in E_{n+1}^-,$$

de

$$E_{n+1}^- = W_{n+1} = \text{egységgyökök } K_{n+1}\text{-ben.}$$

Vegyük észre, hogy

$$N\varepsilon_1 = (N\alpha_1)^{\sigma-1} = 1.$$

5.0.9. Lemma. *Ha $\varepsilon_1 \in W_{n+1}$ és $N\varepsilon_1 = 1$ akkor $\varepsilon_1 = \varepsilon_2^{\sigma-1}$, ahol $\varepsilon_2 \in W_{n+1}$*

Bizonyítás. Hilbert 90 tétele [1] szerint $\varepsilon_1 = y^{\sigma-1}$,ahol $y \in K_{n+1}$, de ezt tudjuk, hiszen $y = \alpha_1$. Azt szeretnénk, hogy $y \in W_{n+1}$. Nézzük a következő két sorozatot

$$1 \to W_n \to W_{n+1} \xrightarrow{\sigma-1} W_{n+1}^{\sigma-1} \to 1$$

$$1 \to W_{n+1} \cup \mathrm{Ker}N \to W_{n+1} \xrightarrow{N} W_n \to 1.$$

Az első egyértelműen egzakt. A másodikről is be szeretnénk látni ezt. Ha $\zeta_p \not\in K_0$ akkor $\zeta_p \not\in K_m$ minden m-re. Ha ez nem teljesülne akkor létezne egy nem triviális részcsoportja $(\mathbb{Z}/p\mathbb{Z})^\times$ $\mathrm{Gal}(K_\infty/K)$-ben, ami nem lehet. Mivel $N : W_n \to W_n$ a p hatvány leképezés, ez szürjektív, ezért $N : W_{n+1} \to W_n$ is szürjektív. Ha $\zeta_p \in K_0$ akkor $K_{n+1} = K_n(\zeta)$, ahol $\zeta = \zeta_{p^m}$,minden $m \geq n+1$. Azonban $W_{n+1} = \langle\zeta\rangle \times \langle\zeta_t\rangle$ valamilyen $t \quad (p,t) = 1$, és $W_n = \langle\zeta^p\rangle \times \langle\zeta_t\rangle$. Könnyű látni, hogy $N\zeta = \zeta^p$ és $N\zeta_t = \zeta_t^p$, szóval $\langle N\zeta_t\rangle = \langle\zeta_t\rangle$. Ekkor N szürjektív és a második sorozat is egzakt. Megkaptuk, hogy

$$|W_{n+1}^{\sigma-1}| = \frac{|W_{n+1}|}{|W_n|} = |W_{n+1} \cap \mathrm{Ker}\ N|.$$

Mivel $W_{n+1}^{\sigma-1}$ része $W_{n+1} \cap N$, ezért egyenlőnek is kell lennie. Ezzel a lemmát beláttuk. □

Lemmaból azt kapjuk, hogy

$$\alpha_1^{\sigma-1} = \varepsilon_1 = \varepsilon_2^{\sigma-1} \quad \text{,ahol } \varepsilon_2 \in W_{n+1}.$$

Tehát

$$\left(\frac{\alpha_1}{\varepsilon_2}\right)^\sigma = \frac{\alpha_1}{\varepsilon_2},$$

azaz

$$\frac{\alpha_1}{\varepsilon_2} \in K_n.$$

Viszont

$$\frac{\alpha_1}{\varepsilon_2} = (\alpha_1) = (\alpha^2) = I^2 \quad K_{n+1}\text{-ben},$$

és az ideálok egyértelmű felbontásából

$$\frac{\alpha_1}{\varepsilon_2} = I^2 \quad K_{n+1}\text{-ben},$$

Mivel p páratlan és I p hatvány rendű A_n^--ben, ezért I egy főideál. □

5.0.10. Állítás. *Legyen p páratlan és K egy CM-test. Legyen K_∞/K egy körosztási $\mathbb{Z}_p$-bővítés. Ekkor $X^- = \varprojlim A_n^-$ nem tartalmaz véges Λ-modulust, tehát létezik egy injektív leképzés véges komaggal,*

$$X^- \hookrightarrow \bigoplus_i \Lambda/(p^{k_i}) \oplus \bigoplus_j \Lambda/(g_j(T)).$$

Bizonyítás. Tegyük fel, hogy $F \subseteq X^-$ véges Λ-modulus. Legyen $\mathrm{Gal}(K_\infty/K)$ generátora γ_0. Mivel F véges, ezért létezik $n_0 \in \mathbb{N}$, hogy minden $n \geq n_0$-ra $\gamma_0^{p^n}$ triviálisan hat F-n. Tegyük fel, hogy

$$0 \neq x = (\dots, x_m, x_{m+1}, \dots) \in F \subseteq \varprojlim A_n^-.$$

Ekkor $x_{m+1} \to x_m$ a megfelelő norma leképzés mellett és $x_m \neq 0$ minden elég nagy m-re (letezik m_0,hogy $m \geq m_0$). Legyen m nagyon m_0-nál és n_0-nál. Az 5.0.8 állítás szerint $x_m \neq 0$, amikor felemeljük A_{m+1}^--be, Nézzük a következő elem hatását x-re

$$1 + \gamma_0^{p^m} + \gamma_0^{2p^m} + \dots + \gamma_0^{(p-1)p^m}.$$

Mivel $m \geq n_0$ az előbbi elem úgy hat x-n, mint p és ez legy a norma leképzés K_{m+1}-ből K_m-be. Tehát

$$pX_{m+1} = x_m \neq 0 \quad A_{m+1}\text{-ben.}$$

Mivel F egy véges p-csoport és p injektíven hat, ezért $F = 0$. □

5.0.11. Következmény. *Legyen p páratlan és K egy CM-test, illetve K_∞/K egy körosztási $\mathbb{Z}_p$-bővítés. Ha $\mu^- = 0$ akkor*

$$X \simeq \mathbb{Z}_p^{\lambda^-}.$$

Bizonyítás. Az előző tétel és a 5.0.7 tétel bizonyításához hasonlóan belátható. □

6. fejezet

A Fősejtés

Ebben a fejezetben feltesszük, hogy $p \neq 2$. Nézzük a következő $\mathbb{Z}_p$-bővítést $\mathbb{Q}(\zeta_\infty)/\mathbb{Q}(\zeta_p)$. A kövezkező tételt segítségével meg tudjuk mutatni, hogy $\varepsilon_i X$, mivel izomorf.

6.0.1. Tétel. *Tegyük fel, hogy $p \nmid h(\mathbb{Q}(\zeta_p)^+)+$. Legyen $P_n(T) = (1+T)^{p^n} - 1$. Ekkor minden $i = 3, 5, \ldots, p-2$-re,*

$$\varepsilon_i A_n \simeq \mathbb{Z}_p[[T]]/(P_n(T), f(T, \omega^{1-i}))$$

és

$$\varprojlim \varepsilon_i A \simeq \mathbb{Z}_p[[T]/(f(T, \omega^{1-i}))$$

mint $\mathbb{Z}_p[[T]]$-modulus, ahol $f(T, \omega^{1-i})$ hatványsora kielégiti a következőt

$$f((1+p)^s, \omega^{1-i}) = L_p(s, \omega^{1-i}).$$

Bizonyítás. A bizonyítás megtalálható a Whasington könyvének 199 oldalán. □

A tétel szerint

$$\varepsilon_i X \simeq \Lambda/(f(T, \omega^{1-i})) \quad \text{minden } i = 3, 5 \ldots, p-2\text{-re},$$

ahol

$$f((1+p)^p - 1, \omega^{1-i}) = L_p(s, \omega^{1-i}).$$

Tudjuk, hogy f faktorizálható a Weirstrass előkészítési tétel szerint, A 2.2.8 tétel szerint $\mu_i = 0$,tehát

$$\varepsilon_i X \simeq \Lambda/(g_i(T)),$$

ami teljesítia 3.2.8 tételt. Ebben az esetben a megkülönböztetett polinom megegyezik a p-adikus L-függvénnyel. A sejtés szerint ez általánosabban is igaz.
Legyen F teljesen valós test és legyen $K_0 = F(\zeta_0), K_\infty = F(\zeta_{p^\infty})$. Legyen

$$\Delta = \mathrm{Gal}(K_0/F) \subseteq (\mathbb{Z}/p\mathbb{Z})^\times.$$

Legyen $\chi \in \hat{\Delta}$ páratlan Dirichlet karakter. Ekkor

$$\varepsilon_\chi X \hookrightarrow \bigoplus_i \Lambda/(p^{k_i^\chi}) \oplus \bigoplus_j \Lambda/(g_j^\chi(T))$$

véges comaggal. Legyen $\mu_\chi = \sum k_i^\chi$ és legyen

$$g^\chi(T) = p^{\mu_\chi} \prod_j g_j^\chi(T).$$

Be lett bizonyítva (lásd. 296 oldal [6]), hogy létezik egy p-adikus L-függvény, $L_p(s, \omega\chi^{-1})$ minden $\omega\chi^{-1}$ páros Dirichlet karakterre. Ha $F = \mathbb{Q}$ akkor ez a szokásos p-adikus L-függvény. Ez nagyobb F-ekre nehezebb belátni.

Legyen $\mathrm{Gal}(K_\infty/K_0)$ generátora $\gamma_0 = 1+T$. Definuáljuk $\kappa_0 \in 1+p\mathbb{Z}_p$ úgy, hogy $\gamma_0\zeta_{p^n} = \zeta_{p^n}^{\kappa_0}$ minden $n \geq 1$. Be lett bizonyítva, hogy létezik egy hatványsor $f_\chi \in \Lambda$, hogy

$$L_p(s, \omega\chi^{-1}) = f_\chi(\kappa_0^s - 1), \quad \chi \neq \omega.$$

A Főtétel (első alakja). $f_\chi(T) = g^\chi(T)U_\chi(T)$ *ahol* $U_\chi \in \Lambda^\times$.

A főtételt más alakban is kimondhatjuk. Az egyszerűség kedvéért legyen $F = \mathbb{Q}$, ez nem szükséges, mivel a fősejtés igaz minden teljesen valós test fölött. Legyen $\chi \neq \omega$ egy első rendű páratlan Dirichlet karakter, és legyen $K_0 = K_\chi(\zeta_p), K_\infty = (\zeta_{p^\infty})$. Legyen $\mathcal{O}$ olyan, hogy tartalmazza χ értékeit és $\mathbb{Z}_p \subseteq \mathcal{O}$ és legyen $f_\chi \in \mathcal{O}[[T]]$ kielégíti a következőt

$$f_\chi(\kappa_0^s - 1) = L_p(s.\omega\chi^{-1}),$$

ahogyan a 2.2.3 tételben. Ekkor

$$f_\chi(T) = p^{\mu_\chi}\tilde{f}_\chi(T)U_\chi(T),$$

ahol $U_\chi \in \mathcal{O}[[T]]^\times, \tilde{f}_\chi(T)$ megkülönbőztetett és $\mu_\chi \geq 0$.
Vegyük a

$$V = X \otimes_{\mathbb{Z}_p} \mathbb{C}_p$$

$\mathbb{C}_p$ fölötti vektorteret és legyen $g_\chi(T)$ a karakterisztikus polinoma $\gamma_0 - 1$-nek, ami hat $V_\chi = \varepsilon_\chi V$.

A Főtétel (második alakja). $\tilde{f}_\chi(T) = g_\chi(T)$.

A második alak előnye, hogy több fajta karakteret nézhetünk vele. Ellenben elveszítjük azt, hogy $\mu = \mu_\chi$ (μ-t $\varepsilon\chi X$-ből, μ_χ-t f_χ-ből kaptuk). $\mathbb{Q}$ fölötti Abel bővítésekre egyenlőek, hiszen mindkettő 0.
A fősejtést megalkotását a véges testek fölötti görbék tanulmányozása motiválta. Legyen C egy görbe és a nemszáma(genus) g k fölött. Legyen k karakterisztikája $l \neq p$ és legyen J a Jacobi varietánsa. Legyen J_p a p rendű pontok halmaza J-n k lezártja fölött. Ekkor

$$J_p \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^{2g}, \text{mint Abel csoportok.}$$

Ekkor

$$\mathrm{Hom}_{\mathbb{Z}_p}(J_p, \mathbb{Q}_p/\mathbb{Z}_p) \simeq \mathbb{Z}_p^{2q}$$

és

$$\mathrm{Hom}_{\mathbb{Z}_p}(J_p, \mathbb{Q}_p/\mathbb{Z}_p) \otimes \mathbb{Q}_p \simeq \mathbb{Q}_p^{2g}.$$

A Frobenius automorfizmus $\bar{k}$-nak k fölött hat ezen a teren és Weil tétele szerint a karakterisztukus polinom a C zeta függvényének a számláloja. Így a főtétel egy eszköz, hogy ezt kibővítsük a fügvénytestekre.
A főtételt (első alak) Mazur és Wiles bebizonyította $F = \mathbb{Q}, K_0 = \mathbb{Q}(\zeta_p)$, Ennel egy kicsit erősebbet bizonyítottak be, amit körbejárunk kicsit.
Legyen R egy kommutatiív gyűrű és M egy végesen generált R-modulus. Minden $r \in \mathbb{Z}$ és $B \subseteq R^r$ létezik egy egzakt sor

$$0 \to B \xrightarrow{\Phi} R^r \xrightarrow{\Psi} M \to 0.$$

Vegyük azokat az $r \times r$ mátrixokat, amik kielégítik a következőt

$$\Phi = \begin{pmatrix} \Phi(b_1) \\ \vdots \\ \Phi(b_r) \end{pmatrix}$$

ahol $(b_1, \ldots, b_r) \in B^r$. A Fitting ideál $F_R(M)$ úgy van definiálva, hogy legyen az az ideál R-ben, amit $\det(\Phi)$ elemei generálnak. Megmutatható, hogy $F_R(M)$ nem függ r-től és Ψ-től, tehát csak M-től függ.

Példák.

1. $R = \mathbb{Z}, M =$ végesen generált csoport. Ekkor $F_R(M) = |M|\mathbb{Z}$.

2. $M = R/I$, ahol I egy ideálja R-nek. Ekkor $F_R(M) = I$.
3. $R = \Lambda$ és M kielégíti a következőt
$$0 \to M \to \bigoplus_j \Lambda/(g_j(T)) \to (\text{véges}) \to 0.$$
Ekkor
$$F_\Lambda(M) = (\prod g_j)\Lambda.$$
4. Ha $M \to N$ egy szürjektív leképzés és M, N R-modulusok, akkor $F_R(M) \subseteq F_R(N)$.
5. Ha I egy ideálja R-nek akkor
$$F_{R/I}(M/IM) = F_R(M) \bmod I.$$

Legyen $i \neq 1 \bmod p-1$ és páratlan. Ekkor $f_{\omega^i}(T) \in \Lambda$ létezik és
$$f_{\omega^i}((1+p)^s - 1) = L_p(-s, \omega^{1-i}).$$
Legyen ε_i egy idempontens elem és
$$\varepsilon_i A_\infty = \lim \varepsilon_i A_n = \bigcup \varepsilon_i A_n.$$
Definiáljuk
$$X_\infty^{(i)} = \mathrm{Hom}_{\mathbb{Z}_p}(\varepsilon_i A_\infty, \mathbb{Q}_p/\mathbb{Z}_p).$$
Megmutatható, hogy ha $\varepsilon_i X \sim \bigoplus \Lambda/(g_j(T))$ akkor $X_\infty^{(i)} \sim \bigoplus \Lambda/(\tilde{g}_j(T))$, ahol
$$\tilde{g}_j(T) = g_j((1+T)^{-1} - 1).$$

6.0.2. Tétel. *(Mazur-Wiles). Legyen $i \neq 1$ mod $p-1$ páratlan. Ekkor*

1. $F_\Lambda X_\infty^{(i)} = (f_{\omega^i}(T))$,
2. $F_{\Lambda/(P_n(T))}(\varepsilon_i A_n) = F_{\Lambda/(P_n(T))}(X_\infty^{(i)}/P_n(T)X_\infty^{(i)}) = (f_{\omega^i}(T) \bmod P_n(T))$,

ahol $P_n(T) = (1+T)^{p^n} - 1$.

A harmadik példa alapján az első rész adja a főtételt. Ha feltesszük a Vandiver sejtést, akkor a második példa alapján megoldhatjuk, viszont sokszor van, hogy egy nem ciklikus modulusnak a fitting ideálja megegyezik egy ciklikus moduluséval. Így a tételből nem következik a Vandiver sejtés vagy a ciklikussága az osztálycsoportnak, mint modulus a csoport gyűrű felett.
A bizonyítás algebrai geometriát és moduláris formák elméletét használja, hogy nem elágazó bővítését kontruálja $\mathbb{Q}(\zeta^{p^{n+1}})$-nek. Ezért $X_\infty^{(i)}$ elég nagy, hogy $F_\Lambda(X_\infty^{(i)}) \subseteq (f_{\omega^i}(T))$ minden i-re. Ha
$$X_\infty^{(i)} \hookrightarrow \bigoplus \Lambda/(\tilde{g}_j(T))$$
véges komaggal rendelkezik, akkor
$$F_\Lambda(X_\infty^{(i)}) = (\prod \tilde{g}_j(T)) = (\tilde{g}_{\omega^i}(T)).$$
Ezért
$$f_{\omega^i}(T) | \tilde{g}_{\omega^i}(T)$$
és $\deg_w f_{\omega^i} \leq \deg_w \tilde{g}_{\omega^i}$, ahol $\deg_w$ a Weierstrass fok. A 2.2.7 tétel szerint $\lambda^- = \sum_i \deg_w \tilde{g}_{\omega^i}$, szóval
$$f_{\omega^i} = (\tilde{g}_{\omega^i})(\text{egység}).$$
Ezzel az első részt beláttuk. Természetesen a bizonyítás nehezebbik része olyan bővítést konstruálni, ami megfelel. Egy felhasználása a tételnek a következő eredmény
$$|\varepsilon_i A_0| = p - \text{része } B_{1,\omega^{-i}}\text{-nek.}$$
Ez következik a második részből, hiszen $\Lambda/(P_0(T)) = \mathbb{Z}_p$, a Fitting ideál meghatározza a rendjét, és
$$f_{\omega^i}(T) \equiv f_{\omega^i}(0) = L_p(0, \omega^{1-i}) = -B_{1,\omega^{-i}} \bmod P_0(T),$$
ezzel beláttuk.

Irodalomjegyzék

[1] Lucas Lingle. Galois theory and hilbert's theorem 90, 2013. Elérhető:`https://math.uchicago.edu/~may/REU2013/REUPapers/Lingle.pdf`.

[2] James S. Milne. Algebraic number theory (v3.08), 2020. Elérhető:`www.jmilne.org/math/`.

[3] J.S. Milne. Class field theory (v4.03), 2020. Elérhető:`www.jmilne.org/math/`.

[4] Alexa Pomerantz. An introduction to the p-adic numbers. 2020. Elérhető:`https://math.uchicago.edu/~may/REU2020/REUPapers/Pomerantz.pdf`.

[5] Shatz S. *Profinite Groups, Arithmetic, and Geometry*. Princeton University Press, 1972.

[6] Lawrence C. Washington. *Introduction to Cyclotomic Fields*. Springer, 1982.

[7] Charles A. Weibel. An introduction to homological algebra. 1994. Elérhető:`https://people.math.rochester.edu/faculty/doug/otherpapers/weibel-hom.pdf`.

NYILATKOZAT

Név: Pálffy Patrik Dániel

ELTE Természettudományi Kar, szak: Matematika Bsc

NEPTUN azonosító: XPT02Q

Szakdolgozat címe:
Iwasawa-elmélet

A **szakdolgozat** szerzőjeként fegyelmi felelősségem tudatában kijelentem, hogy a dolgozatom önálló szellemi alkotásom, abban a hivatkozások és idézések standard szabályait következetesen alkalmaztam, mások által írt részeket a megfelelő idézés nélkül nem használtam fel.

Budapest, 2023.06.04.

a hallgató aláírása