

Márton Dénes

Matematika MSc

Coates és Wiles tétele

Szakdolgozat

Témavezető: Zábrádi Gergely
Algebra és Számelmélet Tanszék



Budapest, 2025

Tartalomjegyzék

1. Bevezetés	3
2. Elliptikus görbék	3
2.1. Elliptikus görbék a komplex számok felett	7
2.2. Elliptikus görbék lokális testek felett	9
2.3. Elliptikus görbék számtestek felett	13
3. Komplex szorzás	15
3.1. A komplex szorzás főtétele	16
3.2. Az elliptikus görbe Hecke karaktere	18
4. Selmer csoport	21
4.1. A nagyított Selmer csoport	21
4.2. A valódi Selmer csoport	23
5. Elliptikus egységek	25
5.1. Definíció és alaptulajdonságok	25
5.2. Elliptikus görbék K felett	29
5.3. Értelmezés a tóruszon	30
5.4. A Hecke L -függvény	31
5.5. p -adikus értelmezés	33
6. Euler rendszerek	35
6.1. Elliptikus egységek	35
6.2. Kolyvagin konstrukciója	36
7. Az osztálycsoport mérete	40
8. Coates és Wiles tétele	43

1. Bevezetés

A Clay Matematikai Intézet egyik megoldatlan millenniumi problémája a Birch és Swinnerton-Dyer-sejtés, ami egy elliptikus görbe analitikus viselkedését kapcsolja össze egy algebrai tulajdonságával. Egészen pontosan a következő formában [Mil06] 10.5:

1.1. Sejtés (BSD). Legyen $E/\mathbb{Q}$ elliptikus görbe, amire az $E(\mathbb{Q})$ Mordell-Weil csoport rangja r és $P_1, \dots, P_r$ lineárisan független elemei $E(\mathbb{Q})$ -nak. Ekkor

$$L(E, s) \sim \left(\Omega \prod_{p \text{ rossz}} c_p \right) \frac{|\text{III}(E/\mathbb{Q})| \det(\langle P_i, P_j \rangle)}{|E(\mathbb{Q}) : \sum \mathbb{Z}P_i|^2} (s-1)^r \quad \text{ha } s \rightarrow 1,$$

ahol $L(E, s)$ az elliptikus görbe Hasse-Weil L -függvénye, $\Omega = \int_{E(\mathbb{R})} |\omega_E|$, a szorzat azon p prímeiken megy végig, ahol E redukciója $\bmod p$ szinguláris, $c_p = |E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)|$, $\text{III}(E/\mathbb{Q})$ a Tate-Safarevics csoport és $\langle \cdot, \cdot \rangle : E(\mathbb{Q}) \times E(\mathbb{Q}) \rightarrow \mathbb{R}$ a Néron-Tate párosítás.

Nem tudjuk, hogy a Tate-Safarevics csoport véges-e, így nem meglepő, hogy a BSD-sejtés sem bizonyított még. A Tate-Safarevics csoport végenségét külön sejtésként is megfogalmazhatnánk. Viszont Birch és Swinnerton-Dyer már első cikkükben rengeteg számításra alapozták sejtésüket, azonban jelenleg is csak nagyon speciális esetekben léteznek bizonyított állítások a témában. Egyik első eredmény Coates és Wiles tétele 1977-ből [CW77], aminek megértése a célja a szakdolgozatomnak Rubin jegyzete [Rub99] alapján.

1.2. Tétel (Coates, Wiles). *Tegyük fel, hogy az E elliptikus görbe K fölött van definiálva, ahol K egy képzetes kvadratikus test és E -n van komplex szorzás a K test $\mathcal{O}_K$ egészeinek gyűrűjével. Ha $L(E, 1) \neq 0$, akkor $E(K)$ véges csoport.*

Ha a BSD-sejtésben eltekintünk egy pillanatra $\lim_{s \rightarrow 1} \frac{L(E, s)}{(s-1)^r}$ -től, akkor az azt is mondja, hogy az 1 éppen annyiszoros gyöke $L(E, s)$ -nek, mint a Mordell-Weil csoport rangja. Coates és Wiles tétele pedig abban a ritka esetben, amikor E -n van komplex szorzás, akkor megmondja, hogy ha $E(K)$ -nak van szabad része, akkor $L(E, s)$ -nek gyöke van 0-ban, megerősítve a várakozásainkat a BSD-sejtés igazságára.

A bizonyítás rengeteg elméletet felhasznál, mint például természetesen az elliptikus görbékét [Mil06, Sil09], algebrai számelméletet [Zá20], osztálytestelméletet [Mil20], csoportkohomológiát [Sha] vagy például reprezentáció elméletet, karakter elméletet [Shu22]. Ezekre csak hivatkozni fogunk amikor szükséges, mert a fókusz Coates és Wiles tételének bizonyítása.

2. Elliptikus görbék

2.1. Definíció. F test felett definiált *elliptikus görbének* mondjuk a következőket:

- (a) egy E harmadfokú nemszinguláris projektív síkgörbe F felett és egy $O \in E(F)$ pont;
- (b) ugyanaz, mint (a), de feltesszük, hogy O inflexiós pont;
- (c) egy harmadfokú nemszinguláris projektív síkgörbe F felett

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \quad (2.1)$$

alakban;

(d) egy 1 génuszú nonszinguláris projektív síkgörbe F felett és egy $O \in E(F)$ pont.

Belátható, hogy ezek mind ugyanazokat az objektumokat definiálják izomorfizmus erejéig. A (c)-ben szereplő egyenletet az elliptikus görbe egy *Weierstraß egyenletének* mondjuk. A harmadfokú nonszinguláris projektív síkgörbék elláthatók Abel-csoport struktúrával, ahol a nullelem tetszőlegesen választható. Elliptikus görbe esetén a nullelem szerepét O tölti be. Szokás áttanszformálni O -t a $(0 : 1 : 0)$ pontba és a görbe $\{Z = 1\}$ -be eső affin részét tekinteni, ahol O -nak az egyetlen görbén lévő végtelen távoli pont felel meg, amit szintén O -val jelölünk. Az $E(F)$, - azaz azon pontok halmaza, melyek a görbén vannak és minden koordinátájuk F -ben van - jelölésbe beleértjük a csoportstruktúrát, így azt végig csoportként értelmezzük.

Tehát innentől gondolhatunk egy F fölötti elliptikus görbére, mint

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (2.2)$$

nullhelyeire, ahol $a_1, a_2, a_3, a_4, a_6 \in F$, kiegészítve egy végtelen távoli ponttal és ellátva egy Abel-csoport struktúrával, ahol a végtelen távoli pont a nullelem. [Sil09] §III.2.3 megmondja, hogy hogyan számolható ki két pont összege. Ha F karakterisztikája se nem 2, se nem 3, akkor az egyszerűbb

$$y^2 = x^3 + ax + b$$

alakra hozható az elliptikus görbe. Azonban mivel például egy $\mathbb{Q}$ fölötti elliptikus görbét miután változcserével olyan alakra hozzuk, ahol az együtthatók egészek, és azt mod p vizsgáljuk, akkor előfordulhat, hogy egy 2 vagy 3 karakterisztikájú test fölött kell ismerünk az elliptikus görbe viselkedését. Hasonlóan igaz ez egy tetszőleges számtest fölött is.

Definiáljuk a következő mennyiségeket az általános esetben:

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 & c_4 &= b_2^2 - 24b_4 \\ b_4 &= a_1a_3 + 2a_4 & c_6 &= -b_2^3 + 36b_2b_4 - 216b_6 \\ b_6 &= a_3^2 + 4a_6 & \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\ b_8 &= b_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 & j &= c_4^3/\Delta \end{aligned}$$

Azt mondjuk, hogy Δ az elliptikus görbe *diszkriminánsa*, j pedig a j -*invariánsa*.

2.2. Állítás. (i) Egy (2.1) Weierstraß egyenlettel megadott görbe pontosan akkor nonszinguláris, ha $\Delta \neq 0$.

Ha szinguláris, akkor egyetlen szinguláris pontja van.

(ii) Két elliptikus görbe pontosan akkor izomorf $\bar{F}$ felett, ha j -invariánsuk megegyezik.

Bizonyítás. [Sil09] III. 1.4 állítás. □

2.3. Állítás. Tegyük fel, hogy az E elliptikus görbe egy (2.2) Weierstrass egyenlet által van definiálva. Ekkor az E -n értelmezett F feletti holomorf differenciálok tere egy 1-dimenziós vektortér F felett, aminek bázisa

$$\omega_E = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}.$$

Továbbá ω_E invariáns az $E(\bar{F})$ -beli pontokkal való eltolásokra. (Differenciálok: ld. [Sil09] II.4 fejezet.)

Bizonyítás. [Rub99] 1.2 állítás, [Sil09] III. 1.5 állítás és III. 5.1 állítás. $\square$

2.4. Definíció. Azt mondjuk, hogy ω_E az E elliptikus görbe *invariáns differenciálja*.

2.5. Definíció. Tegyük fel, hogy E elliptikus görbe. Azt mondjuk, hogy egy $E \rightarrow E$ morfizmus, - mint algebrai görbe - *endomorfizmus*, ha O -t O -ba viszi.

Általában azt mondjuk, hogy egy (E, O) és (E', O') elliptikus görbék közötti morfizmus *izogénia*, ha O -t O' -be viszi. Ha létezik az (E, O) és (E', O') görbék között izogénia, aminek a képe nem csak az O' pont, akkor azt mondjuk, hogy a két görbe *izogén*. [Sil09] III. 6.1 tétel szerint ez egy ekvivalenciareláció.

[Sil09] III. 4.8 tétel szerint egy izogénia homomorfizmus is az Abel csoportstruktúrákra nézve. Speciálisan egy endomorfizmus is homomorfizmus.

Ha $F(E)$ -vel jelöljük a racionális függvényeket egy E elliptikus görbén, és $\phi : E \rightarrow E'$ izogénia elliptikus görbék között nem a konstans O' , akkor

$$\phi^* : \bar{F}(E') \rightarrow \bar{F}(E), f \mapsto f \circ \phi$$

beágyazás. A $\bar{F}(E')/\phi^*\bar{F}(E)$ testbővítés véges (ld. [Sil09] II. 2.4 tétel), fokát ϕ *fokának* hívjuk és $\deg(\phi)$ -vel jelöljük. Azt mondjuk, hogy ϕ *szeparábilis*, *inszeparábilis*, *tisztán inszeparábilis*, ha a testbővítés rendre szeparábilis, inszeparábilis, tisztán inszeparábilis.

2.6. Példa. Minden m egész számra $[m] : E \rightarrow E, P \mapsto mP$ (az Abel-csoportban összeadjuk m -szer P -t, vagy $|m|$ -szer $(-P)$ -t) endomorfizmus, aminek foka m^2 . Továbbá, ha $m \neq 0$, F karakterisztikája 0 vagy F karakterisztikája nem 0, de nem osztja m -et, akkor $[m]$ maga izomorf $(\mathbb{Z}/m\mathbb{Z})^2$ -tel. (ld. [Sil09] III. 6.4 tétel.)

2.7. Példa. Ha F véges, $\#(F) = q$, akkor $\varphi_q : (X, Y, Z) \mapsto (X^q, Y^q, Z^q)$ tisztán inszeparábilis endomorfizmusa E -nek, foka q és *Frobenius endomorfizmusnak* hívjuk. (ld. [Sil09] II. 2.11 állítás.)

2.8. Definíció. Ha F elliptikus görbe F felett van definiálva, akkor $\text{End}_F(E)$ -vel jelöljük E F feletti endomorfizmusainak gyűrűjét. Ekkor $\text{End}_F(E)$ nullosztómentes (ld. [Sil09] III. 4.2 állítás) és 2.6. példa szerint létezik egy $\mathbb{Z} \hookrightarrow \text{End}_F(E)$ beágyazás.

2.9. Definíció. Jelöljük $\mathcal{D}(E/F)$ -fel az E F feletti holomorf differenciáljainak 2.3. állítás szerint 1-dimenziós vektorterét. [Sil09] III. 5.2 tétel szerint a $\phi \mapsto \phi^*$ leképezés ad egy

$$\iota = \iota_F : \text{End}_F(E) \rightarrow \text{End}_F(\mathcal{D}(E/F)) \cong F$$

Abel-csoport homomorfizmust. [Sil09] III.5.6 következmény szerint ι maga az inszeparábilis endomorfizmusok ideálja. Speciálisan ha F karakterisztikája 0, akkor ι injektív.

2.10. Lemma. Tegyük fel, hogy $\text{char}(F) = 0$, L test tartalmazza F -et, $\phi \in \text{End}_L(E)$. Ha $\iota_L(\phi) \in F$, akkor $\phi \in \text{End}_F(E)$.

Bizonyítás. Ha $\sigma \in \text{Aut}(\bar{L}/F)$, akkor

$$\iota_L(\phi^\sigma) = \sigma(\iota_L(\phi)) = \iota_L(\phi).$$

Mivel L karakterisztikája 0, ezért ι_L injektív, tehát $\phi^\sigma = \phi$. $\square$

2.11. Definíció. Ha $\phi \in \text{End}_F(E)$, akkor $E[\phi] \subset E(\bar{F})$ jelöli ϕ magját $\bar{F}$ felett. $F(E[\phi])$ jelöli F testbővítését $E[\phi]$ pontjainak koordinátaival.

Vegyük észre, hogy $F(E[\phi])$ független az F feletti Weierstraß egyenlet választásától. [Sil09] III. 4.10 tétel következményeként $\#(E[\phi])$ osztja $\deg(\phi)$ -t, és pontosan akkor egyeznek meg, ha ϕ szeparábilis.

2.12. Definíció. Ha ℓ egy racionális prím, akkor definiáljuk az ℓ -adikus Tate modulusát E -nek, mint

$$T_\ell(E) = \varprojlim_n E[\ell^n],$$

ahol $\varprojlim$ az inverz limeszt jelöli, (ld. [Zá20] 4.3.1. definíció) $[\ell] : E[\ell^{n+1}] \rightarrow E[\ell]$ összekötő leképezésekkel. Ha $\text{char}(F) \neq \ell$, akkor 2.6. példa szerint

$$T_\ell(E) \cong \mathbb{Z}_\ell^2.$$

A G_F abszolút Galois csoport $\mathbb{Z}_\ell$ -lineárisan hat $T_\ell(E)$ -n, ezzel adva egy

$$\rho_\ell : G_F \rightarrow \text{Aut}(T_\ell(E)) \cong \text{GL}_2(\mathbb{Z}_\ell)$$

reprezentációt, ha $\ell \neq \text{char}(F)$.

2.13. Definíció. Legyen $\mathcal{K}$ egy $\mathbb{Q}$ -algebra, ami végesen generált $\mathbb{Q}$ felett. Azt mondjuk, hogy $\mathcal{R}$ egy *rend* (angolul *order*) $\mathcal{K}$ -ban, ha részgyűrű $\mathcal{K}$ -ban, végesen generált $\mathbb{Z}$ -modulus és $\mathcal{R} \otimes \mathbb{Q} = \mathcal{K}$.

2.14. Példa. Legyen $\mathcal{K}$ képzetes kvadratikus test és $\mathcal{O}$ az egészeinek gyűrűje. Minden $f \geq 1$ egészre $\mathbb{Z} + f\mathcal{O}$ rend $\mathcal{K}$ -ban. Sőt, ez az összes rendje $\mathcal{K}$ -nak. (Ld. [Sil09] III.9.1 példa.)

2.15. Tétel. Ha E egy elliptikus görbe, akkor $\text{End}_F(E)$ a következők közül valamelyik:

(i) $\mathbb{Z}$,

(ii) egy rend egy képzetes kvadratikus testben,

(iii) egy rend egy $\mathbb{Q}$ feletti kvaternióalgebrában.

Ha $\text{char}(F) = 0$, akkor csak az első kettő lehetséges.

Bizonyítás. [Sil09] III. 9.4 következmény. □

2.16. Lemma. Tegyük fel, hogy E elliptikus görbe az $y^2 = x^3 + ax + b$ Weierstraß egyenlettel van megadva. Ha $\text{Aut}(E)$ tartalmaz egy 4-edrendű (vagy 3-adrendű) elemet, akkor $b = 0$ (vagy $a = 0$).

Bizonyítás. [Rub99] 1.13 lemma. □

2.1. Elliptikus görbék a komplex számok felett

Ha egy elliptikus görbe egy 0 karakterisztikájú test fölött definiált, akkor azt értelmezhetjük egy $\mathbb{Q}(a_1, a_2, a_3, a_4, a_6)$ felett definiált elliptikus görbének is. Ez a test beágyazható $\mathbb{C}$ -be, tehát érdemes megvizsgálni a $\mathbb{C}$ feletti elliptikus görbéket az általánosabb 0 karakterisztikájú testek feletti elliptikus görbékhez is.

2.17. Definíció. Tegyük fel, hogy L egy rács $\mathbb{C}$ -ben. Definiáljuk az L -hez rendelt Weierstraß $\wp$ -függvényt, a Weierstraß σ -függvényt és az Eisenstein sorokat, mint

$$\begin{aligned}\wp(z; L) &= \frac{1}{z^2} + \sum_{0 \neq \omega \in L} \left(\frac{1}{(z + \omega)^2} - \frac{1}{\omega^2} \right), \\ \sigma(z; L) &= z \prod_{0 \neq \omega \in L} \left(1 - \frac{z}{\omega} \right) e^{(z/\omega) + \frac{(z/\omega)^2}{2}}, \\ G_k(L) &= \sum_{0 \neq \omega \in L} \frac{1}{\omega^k} \quad \text{minden páros } k \geq 4\text{-re.}\end{aligned}$$

A függvények konvergencia és egyéb tulajdonságaihoz ld. [Sil09] VI. 3.1 tétel, VI. 3.3 lemma, VI. 3.5 tétel.

2.18. Tétel. (i) Ha L egy rács $\mathbb{C}$ -ben, akkor a

$$\xi : z \mapsto (\wp(z; L), \wp'(z; L)/2)$$

leképezés egy biholomorfizmus (mint Riemann-felületek) és csoporthomomorfizmus $\mathbb{C}/L$ -ről $E(\mathbb{C})$ -re, ahol E az $y^2 = x^3 - 15G_4(L)x - 35G_6(L)$ által definiált elliptikus görbe.

(ii) Ha E elliptikus görbe $\mathbb{C}$ felett az $y^2 = x^3 + ax + b$ egyenlet által van definiálva, akkor létezik egy egyértelmű $L \subset \mathbb{C}$ rács, amire $15G_4(L) = -a$ és $35G_6(L) = -b$. Tehát (i) ad egy izomorfizmust $\mathbb{C}/L$ és $E(\mathbb{C})$ között.

(iii) Az előző megfeleltetésnél az ω_E holomorf differenciál a dz differenciálnak felel meg $\mathbb{C}/L$ -en.

Bizonyítás. [Sil09] VI. 3.6 állítás az (i), [Shi71] 4.2 fejezetben bizonyított (ii). A (iii) egyszerű számolásból következik:

$$\omega_E = \frac{dx}{2y} = \frac{d(\wp(z))}{\wp'(z)} = dz.$$

□

2.19. Definíció. Ha $L \subset \mathbb{C}$ rács, akkor legyen

$$\begin{aligned}\Delta(L) &= (60G_4(L))^3 - 27(140G_6(L))^2 \\ j(L) &= \frac{-1728(60G_4(L))^3}{\Delta(L)}.\end{aligned}$$

Éppen úgy definiáltuk, hogy $\Delta(L)$ a diszkriminánsa, $j(L)$ pedig a j -invariánsa a 2.18. tétel megfeleltetésénél kapott elliptikus görbének.

2.20. Állítás. Tegyük fel, hogy az E elliptikus görbe $\mathbb{C}$ felett az L rácshoz tartozik a 2.18. tétel megfeleltetésénél. Ekkor a 2.9. definíció ι leképezése ad egy

$$\text{End}_{\mathbb{C}}(E) \xrightarrow{\sim} \{\alpha \in \mathbb{C} : \alpha L \subset L\}$$

izomorfizmust.

Bizonyítás. [Sil09] VI. 4.1 tétel szerint adottak az

$$\begin{aligned} \{\alpha \in \mathbb{C} : \alpha L \subset L\} &\rightarrow \{\phi : \mathbb{C}/L \rightarrow \mathbb{C}/L \text{ holomorf, } \phi(0) = 0\} \\ \alpha &\mapsto \phi_{\alpha}, \text{ ahol } \phi_{\alpha}(z) = \alpha z \pmod{L} \end{aligned}$$

és

$$\begin{aligned} \text{End}_{\mathbb{C}}(E) &\rightarrow \{\phi : \mathbb{C}/L \rightarrow \mathbb{C}/L \text{ holomorf, } \phi(0) = 0\} \\ \phi &\mapsto \tilde{\phi} = \xi^{-1} \circ \phi \circ \xi \end{aligned}$$

bijekciók. Legyen $\phi \in \text{End}_{\mathbb{C}}(E)$. Ekkor egyrészt ι -nál vett képét úgy kapjuk meg, hogy $\phi^*(\omega_E) = a_{\phi}\omega_E$, ahol $a_{\phi} \in \mathbb{C}$ és $\iota(\phi) = a_{\phi}$. A 2.18. tétel (iii) része szerint a megfeleltetésnél ω_E -nek dz felel meg, tehát $\mathbb{C}/L$ -ben az előző egyenlőséget úgy fordíthatjuk le, hogy $\tilde{\phi}^*(dz) = a_{\phi}dz$.

Másrészt a bijekciókat használva látjuk, hogy létezik egy $\alpha \in \mathbb{C}$, $\alpha L \subset L$, amire $\tilde{\phi} = \phi_{\alpha}$, tehát

$$\tilde{\phi}^*(dz) = d(\tilde{\phi}^*z) = d(z \circ \tilde{\phi}) = d(z \circ \phi_{\alpha}) = d(\alpha z) = \alpha dz,$$

vagyis $\phi^*(\omega_E) = \alpha\omega_E$, használva a 2.3. állítást $a_{\phi} = \alpha$, azaz $\iota(\phi) = \alpha$. Tehát ι tényleg a megfelelő részhalmazába képez $\mathbb{C}$ -nek, injektív, mert $\mathbb{C}$ karakterisztikája 0 és szürjektív is, mert egy α -hoz a bijekciókat használva választhatjuk $\phi = \xi \circ \phi_{\alpha} \circ \xi^{-1} \in \text{End}_{\mathbb{C}}(E)$ endomorfizmust, amire $\iota(\phi) = \alpha$. $\square$

2.21. Következmény. Ha E elliptikus görbe egy 0 karakterisztikájú F test felett, akkor $\text{End}_F(E)$ vagy $\mathbb{Z}$, vagy egy rend egy képzetes kvadratis testben.

Bizonyítás. 2.15. tétel vagy 2.20. állításból már bizonyítani is tudjuk, hogy ha E elliptikus görbe $\mathbb{C}$ egy részteste felett definiált, akkor $\text{End}_{\mathbb{C}}(E) \cong \{\alpha \in \mathbb{C} : \alpha L \subset L\}$ egy diszkrét részgyűrűje $\mathbb{C}$ -nek, mert a részgyűrűség világos, és diszkrét, mert ha $\alpha \neq \beta$, $\alpha, \beta \in \{\alpha \in \mathbb{C} : \alpha L \subset L\}$, akkor legyen $\omega \in L$ olyan, hogy $|\omega| = \delta := \min_{0 \neq \omega \in L} |\omega| \neq 0$. Ekkor $0 \neq (\alpha - \beta)\omega = \alpha\omega - \beta\omega \in L$, tehát $|\alpha - \beta| \cdot |\omega| \geq \delta$, amit osztva δ -val $|\alpha - \beta| \geq 1$.

Belátjuk, hogy nem triviális diszkrét részgyűrű $\mathbb{C}$ -ben csak a következményben felsorolt lehet. Tegyük fel, hogy $0 \neq R \subset \mathbb{C}$ diszkrét részgyűrű. Speciálisan diszkrét részcsoporthoz. Legyen $\omega_1 \in R$, amire $|\omega_1| = \min_{0 \neq \omega \in R} |\omega|$. Teljesül $R \cap \mathbb{R}\omega_1 = \mathbb{Z}\omega_1$ az ω_1 definíciója miatt. Ha $R \neq \mathbb{Z}\omega_1$, akkor legyen $\omega_2 \in R \setminus \mathbb{Z}\omega_1$ olyan, amire $|\omega_2| = \min_{\omega \in R \setminus \mathbb{Z}\omega_1} |\omega|$. Az előzőek miatt ω_1 és ω_2 $\mathbb{R}$ -függetlenek. Tegyük fel, hogy $R \neq \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. Legyen $\omega \in R \setminus (\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2)$. Mivel $\{\omega_1, \omega_2\}$ egy $\mathbb{R}$ -bázis $\mathbb{C}$ -ben, ezért valamilyen $\alpha, \beta \in \mathbb{R}$ számokra $\omega = \alpha\omega_1 + \beta\omega_2$. Ehhez hozzáadva egy $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ rácshoz lévő számot $\omega' = a\omega_1 + b\omega_2$, ahol $a, b \in (-1/2, 1/2]$ és továbbra is $\omega' \in R \setminus (\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2)$. A háromszög-egyenlőtlenséget használva

$$|\omega'| = |a\omega_1 + b\omega_2| \leq \frac{1}{2}(|\omega_1| + |\omega_2|) \leq |\omega_2|.$$

Egyenlőség csak akkor lehet, ha ω_1 és ω_2 párhuzamosak, ami nem lehet, mert bázist alkotnak, tehát $|\omega'| < |\omega_2|$, ellentmondva ω_2 definíciójának. Vagyis R additív csoportja 1 vagy 2 rangú szabad csoport.

Tegyük fel, hogy R gyűrűben $n\omega = 1$, ahol $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$ és $\omega \in R$. Ekkor $\omega = 1/n$ és $\omega^k = 1/n^k \in R$, ami nem lehet, mert 0 torlódási pont lenne, de R diszkrét. Ha R 1 rangú, ω_1 generátorral, akkor $n\omega_1 = 1$ valamilyen n egészre, mert $1 \in R$. Azonban az előzőek miatt $n = \pm 1$, tehát $\omega_1 = \pm 1$, vagyis $R = \mathbb{Z}$. Ha R 2 rangú, akkor legyenek ω_1, ω_2 generátorok, és $1 = n_1\omega_1 + n_2\omega_2$ valamilyen n_1, n_2 egészekre. Tegyük fel, hogy egyik sem 0. Ha nem relatív prímek, akkor $1 = n\omega$ teljesül $n > 1$, $\omega \in R$ számokkal, ami a korábbiak miatt nem lehet. Ha relatív prímek, akkor valamilyen a, b egészekre $bn_1 - an_2 = 1$. Legyen $u = a\omega_1 + b\omega_2 \in R$. Ezekkel a választásokkal teljesül

$$\begin{aligned}\omega_1 &= b \cdot 1 - n_2 u \\ \omega_2 &= -a \cdot 1 + n_1 u.\end{aligned}$$

Vagyis 1 és u is generátorok. Ha n_1 vagy n_2 közül valamelyik 0, akkor a korábbi torlódási pontos érvelés miatt szintén feltehető, hogy 1 az egyik generátor. Legyen tehát 1 és u két generátora R -nek, vagyis $R = \mathbb{Z} + \mathbb{Z}u$. Mivel 1 és u bázist alkotnak, ezért u nem valós. Az $u^2 \in R$ elem felírható $u^2 = au + b$ alakban a, b egészekkel, tehát $\mathbb{Q}(u) \geq \mathbb{Q}$ másodfokú bővítés, vagyis $\mathbb{Q}(u) = \mathbb{Q} + \mathbb{Q}u = R \otimes \mathbb{Q}$ valóban egy képzetes kvadratikus test, és így R egy rend egy képzetes kvadratikus testben.

Tehát $\text{End}_{\mathbb{C}}(E)$ valóban $\mathbb{Z}$ vagy egy rend egy képzetes kvadratikus testben, és a 2.1. fejezet elején írtak szerint ez minden 0 karakterisztikájú testre is igaz $\mathbb{C}$ helyett. $\square$

Az alábbi táblázat összehasonlítja egy tetszőleges F test feletti elliptikus görbét és egy $\mathbb{C}$ feletti elliptikus görbén a ξ megfeleltetést.

F	$\mathbb{C}$
(E, ω_E)	$(\mathbb{C}/L, dz)$
x, y	$\wp(z; L), \wp'(z; L)/2$
izomorfizmus osztálya E -nek	$\{\alpha L : \alpha \in \mathbb{C}^\times\}$
$\text{End}_F(E)$	$\{\alpha \in \mathbb{C} : \alpha L \subset L\}$
$\text{Aut}_F(E)$	$\{\alpha \in \mathbb{C}^\times : \alpha L = L\}$
$E[m]$	$m^{-1}L/L$

2.2. Elliptikus görbék lokális testek felett

Rögzítsük erre a fejezetre a következőket:

- p egy racionális prím,
- F véges bővítése $\mathbb{Q}_p$ -nek,
- $\mathcal{O}$ az F egészeinek gyűrűje,
- $\mathfrak{p}$ a maximális ideálja $\mathcal{O}$ -nak,
- π egy generátora $\mathfrak{p}$ -nek,
- $\mathbb{k} = \mathcal{O}/\mathfrak{p}$ a maradékteste $\mathcal{O}$ -nak,
- $v : F \rightarrow \mathbb{Z} \cup \{\infty\}$ értékelése F -nek, amire $v(\pi) = 1$.

Rögzítsünk egy F felett definiált E elliptikus görbét.

2.22. Definíció. Azt mondjuk, hogy E egy (2.2) Weierstraß egyenlete *minimális*, ha $a_1, a_2, a_3, a_4, a_6 \in \mathcal{O}$ és $v(\Delta)$ minimális az összes olyan E -t definiáló Weierstraß egyenlet közül, melyeknek együttthatói $\mathcal{O}$ -ban vannak.

Minden E elliptikus görbének van minimális Weierstraß egyenlete és *minimális diszkriminánsnak* hívjuk E egy minimális Weierstraß egyenletének diszkriminánsa által generált ideált $\mathcal{O}$ -ban.

E redukciójának mondjuk azt az $\tilde{E}$ görbét, amit $\mathbb{k}$ fölött definiál az

$$y^2 + \tilde{a}_1 xy + \tilde{a}_3 y = x^3 + \tilde{a}_2 x^2 + \tilde{a}_4 x + \tilde{a}_6$$

Weierstraß egyenlet, ahol (2.2) egy minimális Weierstraß egyenlete E -nek és $\tilde{a}_i$ a képe a_i -nek $\mathbb{k}$ -ban. Az $\tilde{E}$ redukció izomorfizmus erejéig független E konkrét minimális egyenletének választásától (ld. [Sil09] VII.2 fejezet első bekezdése).

Az $\tilde{E}$ görbe nem feltétlenül elliptikus görbe, hiszen lehet szinguláris, viszont mindeképpen legfeljebb 1 szinguláris pontja van (ld. 2.2. állítás). Ha szinguláris, akkor legyen

$$\tilde{E}_{\text{ns}} = \tilde{E} - \{\tilde{E} \text{ szinguláris pontja}\},$$

amin szintén van egy Abel-csoport struktúra, csakúgy, mint egy elliptikus görbén (ld. [Sil09] III. 2.5 állítás).

Ha Δ jelöli a minimális diszkriminánsát E -nek, akkor egészen pontosan a következő 3 lehetőség valamelyike fordul elő (ld. 2.2. állítás és [Sil09] III. 2.5 állítás):

- (i) $\Delta \in \mathcal{O}^\times$, $\tilde{E}$ nemszinguláris, azaz $\tilde{E} = \tilde{E}_{\text{ns}}$ egy elliptikus görbe;
- (ii) $\Delta \notin \mathcal{O}^\times$, $\tilde{E}$ szinguláris, és $\tilde{E}_{\text{ns}}(\mathbb{k}) \cong \mathbb{k}^\times$;
- (iii) $\Delta \notin \mathcal{O}^\times$, $\tilde{E}$ szinguláris, és $\tilde{E}_{\text{ns}}(\mathbb{k}) \cong \mathbb{k}$.

Azt mondjuk, hogy E -nek rendre *sima*, *multiplikatív* vagy *additív* a redukciója, ha (i), (ii) vagy (iii) teljesül.

Továbbá ha létezik egy F' véges bővítése F -nek, amire E -nek sima redukciója van F' fölött nézve, akkor azt mondjuk, hogy E -nek *potenciálisan sima* redukciója van.

2.23. Lemma. (i) E -nek akkor és csak akkor van potenciálisan sima redukciója, ha $j(E) \in \mathcal{O}$.

(ii) Ha E -nek potenciálisan sima redukciója van, akkor E -nek sima vagy additív a redukciója.

Bizonyítás. [Sil09] VII. 5.4 és 5.5 állítás. □

2.24. Definíció. Létezik egy természetes

$$\mathbb{P}^2(F) \rightarrow \mathbb{P}^2(\mathbb{k})$$

redukció leképezés. Ennek a megszorítása ad egy $E(F) \rightarrow \tilde{E}(\mathbb{k})$ leképezést. Legyen az ősképe $\tilde{E}_{\text{ns}}(\mathbb{k})$ -nak $E_0(F) \subset E(F)$, $\tilde{O} \in \tilde{E}_{\text{ns}}(\mathbb{k})$ ősképe pedig $E_1(F) \subset E(F)$.

2.25. Állítás. *Létezik Abel-csoportoknak egy*

$$0 \rightarrow E_1(F) \rightarrow E_0(F) \rightarrow \tilde{E}_{ns}(\mathbb{k}) \rightarrow 0$$

egzakt sorozata, ahol a jobboldali leképezés a redukció. Ha E -nek sima a redukciója, akkor a redukció leképezés indukál egy injektív

$$\text{End}_F(E) \rightarrow \text{End}_{\mathbb{k}}(\tilde{E})$$

homomorfizmust.

Bizonyítás. [Sil09] VII. 2.1 állítás. □

Ha E -nek sima a redukciója és $\phi \in \text{End}_F(E)$, akkor legyen ϕ redukciója $\tilde{\phi} \in \text{End}_{\mathbb{k}}(\tilde{E})$.

2.26. Lemma. *Ha E egy minimális Weierstraß egyenlettel van definiálva, akkor*

$$E_1(F) = \{(x, y) \in E(F) : v(x) < 0\} = \{(x, y) \in E(F) : v(y) < 0\}.$$

Ha $(x, y) \in E_1(F)$, akkor $3v(x) = 2v(y) < 0$.

Bizonyítás. [Rub99] 3.5 lemma. □

2.27. Lemma. *Tegyük fel, hogy E -nek sima a redukciója, $\phi \in \text{End}_F(E)$, $\tilde{\phi}$ tisztán inszeparábilis. Ekkor*

(i) $\tilde{\phi}$ injektív $\tilde{E}(\mathbb{k})$ -n,

(ii) $\ker(\phi) \subset E_1(F)$.

Bizonyítás. [Rub99] 3.6 lemma. □

2.28. Tétel. *Rögzítsük egy (2.2) minimális Weierstraß egyenletét E -nek. Létezik egy $\hat{E}$ formális csoport egy $\mathcal{F}_E \in \mathcal{O}[[Z, Z']]$ formális csoport szabállyal, illetve egy*

$$w(Z) = Z^3 + a_1 Z^4 + (a_1^2 + a_2) Z^5 + \cdots \in \mathcal{O}[[Z]]$$

hatványsor, amire ha

$$x(Z) = \frac{Z}{w(Z)} \in Z^{-2}\mathcal{O}[[Z]], \quad y(Z) = -\frac{1}{w(Z)} \in Z^{-3}\mathcal{O}[[Z]],$$

akkor

(i) $(x(Z), y(Z)) \in E(\mathcal{O}((Z)))$,

(ii)

$$(x(Z), y(Z)) + (x(Z'), y(Z')) = (x(\mathcal{F}_E(Z, Z')), y(\mathcal{F}_E(Z, Z')))$$

mint pontok E -n az $F((Z, Z'))$ hányadostestbeli koordinátákkal,

(iii) *létezik egy $\text{End}_F(E) \rightarrow \text{End}(\hat{E})$ leképezés (amit majd $\phi \mapsto \phi(Z) \in \mathcal{O}[[Z]]$ -vel jelölünk), amire minden $\phi \in \text{End}_F(E)$ -re*

$$\phi((x(Z), y(Z))) = (x(\phi(Z)), y(\phi(Z)))$$

teljesül $E(F((Z)))$ -ben.

Bizonyítás. Ld. [Sil09] IV.1 fejezet. □

Minden $n \geq 1$ -re legyen $\hat{E}(\mathfrak{p}^n)$ az a kommutatív csoport $\mathfrak{p}^n$ -en, amin az összeadás $(z, z') \mapsto \mathcal{F}_E(z, z')$.

2.29. Következmény. *A 2.28. tétel jelöléseivel*

$$Z \mapsto \left(\frac{Z}{w(Z)}, -\frac{1}{w(Z)} \right) : \hat{E}(\mathfrak{p}) \xrightarrow{\sim} E_1(F)$$

izomorfizmus, aminek az inverze

$$(x, y) \mapsto -\frac{x}{y}.$$

Bizonyítás. Ld. [Sil09] VII. 2.2 állítás és [Rub99] 3.8 következmény. □

2.30. Következmény. *Tegyük fel, hogy a $\mathbb{k}$ test q elemű, E -nek sima a redukciója és $\phi \in \text{End}_F(E)$ redukciója a $\varphi_q \in \text{End}_{\mathbb{k}}(\bar{E})$ Frobenius endomorfizmus. Ekkor*

$$\phi(Z) \equiv Z^q \pmod{\mathfrak{p}\mathcal{O}[[Z]]}.$$

Bizonyítás. [Rub99] 3.9 következmény. □

2.31. Definíció. Legyen

$$\hat{\omega}(Z) = \frac{\frac{d}{dZ}x(Z)}{2y(Z) + a_1x(Z) + a_3} \in 1 + Z\mathcal{O}[[Z]],$$

továbbá $\lambda_{\hat{E}}(Z) \in Z + Z^2F[[Z]]$ az az egyértelmű hatványsor, amire $\frac{d}{dZ}\lambda_{\hat{E}}(Z) = \hat{\omega}(Z)$.

2.32. Lemma. *(i) A $\lambda_{\hat{E}}$ hatványsor a logaritmus leképezése $\hat{E}$ -nak, azaz az az izomorfizmus $\hat{E}$ -ről a $\hat{\mathbb{G}}_a$ additív formális csoportba (ld. [Sil09] IV. 2.2.1 példa), amire $\lambda'_{\hat{E}}(0) = 1$.*

(ii) A $\lambda_{\hat{E}}$ hatványsor konvergál $\mathfrak{p}$ -n. Ha $\text{ord}_{\mathfrak{p}}(p) < p - 1$, akkor $\lambda_{\hat{E}}$ egy izomorfizmus $\hat{E}(\mathfrak{p})$ -ről $\mathfrak{p}$ additív csoportjába.

Bizonyítás. [Rub99] 3.11 lemma. □

2.33. Definíció. Legyen $\lambda_E : E_1(F) \rightarrow F$ a kompozíciója a 2.29. következmény izomorfizmusának inverzének és $\lambda_{\hat{E}}$ -nak.

2.34. Következmény. *Ha $\text{ord}_{\mathfrak{p}}(p) < p - 1$, akkor $\lambda_E : E_1(F) \rightarrow \mathfrak{p}$ izomorfizmus.*

Bizonyítás. A 2.32. lemma (ii) részéből és a 2.29. következményből triviális. □

2.35. Állítás. *Minden $\phi \in \text{End}_F(E)$ -re $\phi(Z) = \iota(\phi)Z + O(Z^2)$. ($O(Z^2)$ azt jelöli, hogy Z^2 -tel osztható hatványsor.)*

Bizonyítás. [Rub99] 3.14 állítás. □

2.36. Tétel. *Tegyük fel, hogy $\phi \in \text{End}_F(E)$ és $\iota(\phi) \in \mathcal{O}^\times$.*

(i) ϕ egy automorfizmusa $E_1(F)$ -nek.

(ii) Ha E -nek sima a redukciója, akkor az $E[\phi] \cap E(F) \rightarrow \tilde{E}(\mathbb{k})$ redukció leképezés injektív.

Bizonyítás. [Rub99] 3.15 tétel. □

2.37. Következmény. Tegyük fel, hogy E -nek sima a redukciója, $\phi \in \text{End}_F(E)$ és $\iota(\phi) \in \mathcal{O}^\times$. Ha $P \in E(\bar{F})$ és $\phi(P) \in E(F)$, akkor $F(E[\phi], P)/F$ elágazásmentes.

Bizonyítás. [Rub99] 3.17 következmény. □

2.38. Következmény. Tegyük fel, hogy $\ell \neq p$ és I jelölje az inerciárészcsoporthát $G_F = \text{Gal}(\bar{F}/F)$ abszolút Galois csoportnak.

(i) Ha E -nek sima a redukciója, akkor I triviálisan hat $T_\ell(E)$ -n.

(ii) Ha E -nek potenciálisan sima redukciója van, akkor I egy véges faktoron keresztül hat $T_\ell(E)$ -n.

Bizonyítás. Következik a 2.37. következményből. □

2.39. Tétel (Néron-Ogg-Safarevics kritérium). Legyen $I \subset G_F$ az inerciárészcsoport.

(i) Ha $\ell \neq p$ és I triviálisan hat $T_\ell(E)$ -n, akkor E -nek sima a redukciója.

(ii) Ha $\ell \neq p$ és $T_\ell(E)^I \neq 0$, akkor E -nek sima vagy multiplikatív redukciója van.

Bizonyítás. Ld. [Sil09] VII. 7.1 tétel és [Rub99] 3.19 tétel. □

2.3. Elliptikus görbék számtestek felett

Legyen ebben a fejezetben F egy számtest és E egy elliptikus görbe F felett definiálva. A cél az $E(F)$ Mordell-Weil csoport vizsgálata.

Ha $\mathfrak{q}$ egy prímje F -nek, akkor azt mondjuk, hogy E -nek rendre *sima*, *potenciálisan sima*, *additív*, *multiplikatív* redukciója van $\mathfrak{q}$ -ban, ha E -t $F_{\mathfrak{q}}$ (F teljessé téve $\mathfrak{q}$ szerint) feletti elliptikus görbeként nézve sima, potenciálisan sima, additív, multiplikatív redukciója van. Jelöljük $\Delta(E)$ -vel E minimális diszkriminánsát, azaz $\mathcal{O}_F$ azon ideálját, melyet úgy kapunk, hogy minden $\mathfrak{q}$ prímre összeszorozzuk E $F_{\mathfrak{q}}$ feletti minimális diszkriminánsát. Ez jóldefiniált, mert E (minden Weierstraß egyenletének) sima redukciója van majdnem minden prímre.

Mivel F karakterisztikája 0, ezért a 2.9. definíció $\iota : \text{End}_F(E) \rightarrow F$ leképezése injektív. Azonosítsuk mostantól $\text{End}_F(E)$ -t az $\mathcal{O} \subset F$ képével. A 2.21. következmény értelmében $\mathcal{O}$ vagy $\mathbb{Z}$ vagy egy rend egy képzetes kvadratikus testben.

Ha $\alpha \in \mathcal{O}$, akkor α -t írunk a megfelelő endomorfizmusra is, tehát $E[\alpha] \subset E(\bar{F})$ a magja α -nak és $F(E[\alpha])$ az F bővítése $E[\alpha]$ pontjainak koordinátaival.

2.40. Definíció. Tegyük fel, hogy $0 \neq \alpha \in \mathcal{O}$. Az α -val való szorzás szürjektív $E(\bar{F})$ -on (ld. [Sil09] II. 2.3 tétel), tehát van egy

$$0 \longrightarrow E[\alpha] \longrightarrow E(\bar{F}) \xrightarrow{\alpha} E(\bar{F}) \longrightarrow 0$$

egzakt sorozat. A G_F -kohomológia hosszú egzakt sorozata

$$E(F) \xrightarrow{\alpha} E(F) \longrightarrow H^1(F, E[\alpha]) \longrightarrow H^1(F, E) \xrightarrow{\alpha} H^1(F, E),$$

mert $E(\bar{F})^{G_F} = E(F)$, ahol $H^1(F, E) = H^1(F, E(\bar{F}))$ rövidítést vezettünk be. Ezt máshogy felírva

$$0 \longrightarrow E(F)/\alpha E(F) \longrightarrow H^1(F, E[\alpha]) \longrightarrow H^1(F, E)_\alpha \longrightarrow 0, \quad (2.3)$$

ahol $H^1(F, E)_\alpha$ jelöli α magját $H^1(F, E)$ -n. Az $E(F)/\alpha E(F) \hookrightarrow H^1(F, E[\alpha])$ leképezés a "Kummer elmélet" leképezés, azaz

$$P \mapsto (\sigma \mapsto \sigma Q - Q),$$

ahol $Q \in E(\bar{F})$ -re teljesül $\alpha Q = P$.

Ugyanígy, ha $\mathfrak{q}$ egy (véges vagy végtelen) prímje F -nek, akkor F helyettesíthető $F_{\mathfrak{q}}$ -val (2.3)-ban, ami a

$$\begin{array}{ccccccc} 0 & \longrightarrow & E(F)/\alpha E(F) & \longrightarrow & H^1(F, E[\alpha]) & \longrightarrow & H^1(F, E)_\alpha \longrightarrow 0 \\ & & \downarrow & & \downarrow \text{res}_{\mathfrak{q}} & & \downarrow \text{res}_{\mathfrak{q}} \\ 0 & \longrightarrow & E(F_{\mathfrak{q}})/\alpha E(F_{\mathfrak{q}}) & \longrightarrow & H^1(F_{\mathfrak{q}}, E[\alpha]) & \longrightarrow & H^1(F_{\mathfrak{q}}, E)_\alpha \longrightarrow 0 \end{array} \quad (2.4)$$

diagramhoz vezet. Defináljuk az (α) -Selmer csoportot, mint

$$\mathcal{S}_\alpha(E) = \mathcal{S}(E/F) \subset H^1(F, E[\alpha])$$

$$\begin{aligned} \mathcal{S}_\alpha(E) &= \{c \in H^1(F, E[\alpha]) : \text{res}_{\mathfrak{q}}(c) \in \text{im}(E(F_{\mathfrak{q}})/\alpha E(F_{\mathfrak{q}})) \text{ minden } \mathfrak{q}\} \\ &= \{c \in H^1(F, E[\alpha]) : \text{res}_{\mathfrak{q}}(c) = 0 \in H^1(F_{\mathfrak{q}}, E) \text{ minden } \mathfrak{q}\}. \end{aligned}$$

2.41. Állítás. *Tegyük fel, hogy $0 \neq \alpha \in \mathcal{O}$. A (2.3) egzakt sorozatban $E(F)/\alpha E(F)$ Kummer elmélet leképezésénél vett képe benne van $\mathcal{S}_\alpha(E)$ -ben.*

Bizonyítás. Triviális abból, hogy (2.4) kommutatív. □

2.42. Állítás. *Tegyük fel, hogy $0 \neq \alpha \in \mathcal{O}$. Ekkor $\mathcal{S}_\alpha(E)$ véges.*

Bizonyítás. [Rub99] 4.4 állítás vagy [Sil09] X. 4.2 tétel. □

2.43. Következmény (Gyenge Mordell-Weil tétel). *Tegyük fel, hogy $0 \neq \alpha \in \mathcal{O}$. Ekkor $E(F)/\alpha E(F)$ véges.*

Bizonyítás. A 2.41. és 2.42. állításokból triviális. □

2.44. Tétel (Mordell-Weil). *$E(F)$ végesen generált.*

Bizonyítás. [Sil09] VIII. 6.7 tétel. □

2.45. Definíció. A $\text{III}(E)$ Tate-Safarevics csoportja E -nek F felett a következő részcsoportja $H^1(F, E(\bar{F}))$ -nek:

$$\text{III}(E) = \ker \left(H^1(F, E(\bar{F})) \rightarrow \prod_{\substack{v \text{ (véges vagy végtelen)} \\ \text{prímje } F\text{-nek}}} H^1(F_v, E) \right).$$

2.46. Állítás. *Ha $0 \neq \alpha \in \mathcal{O}$, akkor (2.3) megszorítható egy*

$$0 \longrightarrow E(F)/\alpha E(F) \longrightarrow \mathcal{S}_\alpha(E) \longrightarrow \text{III}(E)_\alpha \longrightarrow 0$$

egzakt sorozatra, ahol $\text{III}(E)_\alpha$ a $\text{III}(E)$ azon elemeinek részcsoportja, amiket α annulál.

Bizonyítás. [Sil09] X. 4.2 tétel. □

3. Komplex szorzás

Rögzítsük $\mathbb{C}$ egy F résztestét és egy F felett definiált E elliptikus görbét.

3.1. Definíció. Azt mondjuk, hogy E -n van komplex szorzás F fölött, ha $\text{End}_F(E) \neq \mathbb{Z}$, azaz $\text{End}_F(E)$ egy rend egy képzetes kvadratikus testben.

Tegyük fel inntől, hogy E -n van komplex szorzás és legyen

$$\mathcal{O} = \iota(\text{End}_F(E)) \subset F.$$

Ahogy 2.3. fejezetben, megfeleltetjük $\text{End}_F(E)$ -t $\mathcal{O}$ -nak. Legyen $K = \mathbb{Q}\mathcal{O} \subset F$ a képzetes kvadratikus test, ami tartalmazza $\mathcal{O}$ -t, és jelöljük $\mathcal{O}_K$ -val K egészeinek gyűrűjét. Ha $\mathfrak{a}$ ideálja $\mathcal{O}$ -nak, akkor legyen $E[\mathfrak{a}] = \bigcap_{\alpha \in \mathfrak{a}} E[\alpha]$.

Rögzítsük F egy beágyazását $\mathbb{C}$ -be. Ha E -t egy $\mathbb{C}$ feletti elliptikus görbeként vizsgáljuk, akkor 2.20. állítás szerint

$$E(\mathbb{C}) \cong \mathbb{C}/L, \text{ ahol } L \subset K \subset \mathbb{C} \text{ és } \mathcal{O}L = L. \quad (3.1)$$

(Eredetileg csak annyit tudunk, hogy L egy rács, de L -et lecserélve λL -re, ahol $\lambda^{-1} \in L$, feltehető, hogy $L \subset K$.) Tehát ha $\mathcal{O} = \mathcal{O}_K$, akkor L egy törtideál K -ban.

3.2. Állítás. *Létezik egy E' elliptikus görbe F felett definiálva, ami izogén E -vel F felett, és $\text{End}_F(E') \cong \mathcal{O}_K$.*

Bizonyítás. [Rub99] 5.3 állítás. □

Mostantól feltesszük, hogy $\mathcal{O} = \mathcal{O}_K$.

3.3. Állítás. *Ha $\mathfrak{a}$ nemnulla ideál $\mathcal{O}$ -ban, akkor $E[\mathfrak{a}] \cong \mathcal{O}/\mathfrak{a}$, mint $\mathcal{O}$ -modulusok.*

Bizonyítás. A (3.1) azonosítást használva $E[\mathfrak{a}] \cong \mathfrak{a}^{-1}L/L$, ahol L egy törtideálja K -nak. Mivel L törtideál, ezért $\mathfrak{a}^{-1}L/L \cong \mathcal{O}/\mathfrak{a}$. □

3.4. Következmény. *Ha $\mathfrak{a}$ nemnulla ideál $\mathcal{O}$ -ban, akkor G_F hatása $E[\mathfrak{a}]$ -n indukál egy*

$$\text{Gal}(F(E[\mathfrak{a}])/F) \hookrightarrow (\mathcal{O}/\mathfrak{a})^\times$$

injektív leképezést. Speciálisan $F(E[\mathfrak{a}])/F$ Abel bővítés.

Bizonyítás. Ha $\beta \in \mathcal{O}$, $\sigma \in G_F$ és $P \in E(\bar{F})$, akkor β endomorfizmus F felett van definiálva, tehát $(\beta P)^\sigma = \beta^\sigma(P^\sigma) = \beta(P^\sigma)$. Ez ad egy

$$\text{Gal}(F(E[\mathfrak{a}])/F) \hookrightarrow \text{Aut}_{\mathcal{O}}(E[\mathfrak{a}])$$

beágyazást, hiszen az előbbiek szerint egy $\sigma \in \text{Gal}(F(E[\mathfrak{a}])/F)$ hatása $E[\mathfrak{a}]$ -n felcserélhető tetszőleges $\mathcal{O}$ -beli endomorfizmussal. A 3.3. állítás miatt pedig

$$\text{Aut}_{\mathcal{O}}(E[\mathfrak{a}]) \cong \text{Aut}_{\mathcal{O}}(\mathcal{O}/\mathfrak{a}) = (\mathcal{O}/\mathfrak{a})^\times.$$

□

Ha $\mathfrak{a}$ nemnulla ideál $\mathcal{O}$ -ban, akkor legyen $E[\mathfrak{a}^\infty] = \bigcup_n E[\mathfrak{a}^n]$.

3.5. Következmény. G_F hatása $E[\mathfrak{a}^\infty]$ -en indukál egy

$$\mathrm{Gal}(F(E[\mathfrak{a}^\infty])/F) \hookrightarrow (\varprojlim_n \mathcal{O}/\mathfrak{a}^n)^\times$$

injektív leképezést. Speciálisan minden p racionális prímre

$$\mathrm{Gal}(F(E[p^\infty])/F) \hookrightarrow (\mathcal{O} \otimes \mathbb{Z}_p)^\times.$$

Bizonyítás. Triviálisan következik 3.4. következményből és hogy

$$\mathrm{Gal}(F(E[\mathfrak{a}^\infty])/F) \cong \varprojlim_n \mathrm{Gal}(F(E[\mathfrak{a}^n])/F).$$

□

3.6. Tétel. Tegyük fel, hogy F véges bővítése $\mathbb{Q}_\ell$ -nek valamilyen ℓ -re.

(i) E -nek potenciálisan sima redukciója van.

(ii) Tegyük fel, hogy $\mathfrak{p}$ egy prímje $\mathcal{O}$ -nak és $n \in \mathbb{Z}^+$ olyan, hogy az $1 + \mathfrak{p}^n \mathcal{O}_\mathfrak{p}$ multiplikatív csoport torziómentes. ($\mathcal{O}_\mathfrak{p} = \varprojlim_n \mathcal{O}/\mathfrak{p}^n$ az $\mathcal{O}$ teljessé tétele $\mathfrak{p}$ -nél.) Ha $\mathfrak{p} \nmid \ell$, akkor E -nek sima redukciója van $F(\varprojlim_n E[\mathfrak{p}^n])$ felett minden olyan prímnél, amik nem osztják $\mathfrak{p}$ -t.

Bizonyítás. [Rub99] 5.7 tétel. □

3.7. Megjegyzés. A 3.6. tétel (ii) részének feltétele teljesül $n = 1$ -re, ha a $\mathfrak{p}$ alatti racionális prím 3-nál nagyobb.

3.8. Állítás. Tegyük fel, hogy $\mathfrak{q}$ egy prímje F -nek, ahol E -nek sima redukciója van és $q = N_{F/\mathbb{Q}}\mathfrak{q}$. Létezik egy $\alpha \in \mathcal{O}$ endomorfizmus, aminek a redukciója modulo $\mathfrak{q}$ az éppen a φ_q Frobenius endomorfizmusa $\tilde{E}$ -nek.

Bizonyítás. [Rub99] 5.9 állítás. □

3.1. A komplex szorzás főtétele

3.9. Definíció. Legyen k számtest és legyen S véges halmaza prímeknek, ami tartalmazza az összes végtelen prímet (azaz a beágyazásokat egy arkhimédieszi lokális testbe: $\mathbb{R}$ vagy $\mathbb{C}$). Ekkor definiáljuk

$$\mathbf{A}_S^\times = \prod_{v \in S} k_v^\times \times \prod_{v \notin S} \mathcal{O}_v^\times.$$

(k_v jelöli a k test teljessé tételét a v prím szerint, $\mathcal{O}_v$ pedig ebben az egészek gyűrűjét a véges prímekre.) Legyen továbbá

$$\mathbf{A}_k^\times = \varinjlim_S \mathbf{A}_S^\times$$

az *idèlek csoportja*, ahol $\varinjlim$ a direkt limeszt jelöli, ld. [Zá20] 4.2.1. definíció.

Hecke karakternek mondjuk egy

$$\chi : \mathbf{A}_k^\times \rightarrow \mathbb{C}^\times$$

folytonos karakterét az idèle csoportnak, ami triviális $k^\times$ -en. ($k^\times$ beágyazható diszkrét részcsoportként az idèlek csoportjába az $x \mapsto (x, x, \dots)$ leképezéssel, ld. [CF67] II.16 fejezet.)

Térjünk vissza az elliptikus görbénkhez.

3.10. Definíció. Ha K egy prímje $\mathfrak{p}$ és egy törtideálja $\mathfrak{a}$, akkor legyen $\mathfrak{a}_{\mathfrak{p}} = \mathfrak{a}\mathcal{O}_{\mathfrak{p}}$. Ekkor

$$K/\mathfrak{a} = \mathfrak{a} \otimes (K/\mathcal{O}) = \mathfrak{a} \otimes \left(\bigoplus_{\mathfrak{p}} K_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}} \right) = \bigoplus_{\mathfrak{p}} K_{\mathfrak{p}}/\mathfrak{a}_{\mathfrak{p}}. \quad (3.2)$$

Ha $x = (x_{\mathfrak{p}}) \in \mathbf{A}_K^{\times}$, akkor létezik egyértelműen egy $\mathfrak{b}$ törtideálja K -nak, amire $\mathfrak{b}_{\mathfrak{p}} = x_{\mathfrak{p}}\mathfrak{a}_{\mathfrak{p}}$. Jelöljük ezt mostantól $x\mathfrak{a}$ -val, azaz $(x\mathfrak{a})_{\mathfrak{p}} = x_{\mathfrak{p}}\mathfrak{a}_{\mathfrak{p}}$ teljesül minden $\mathfrak{p}$ -re. Az $x_{\mathfrak{p}}$ -vel való szorzás ad egy $K_{\mathfrak{p}}/\mathfrak{a}_{\mathfrak{p}} \xrightarrow{\sim} K_{\mathfrak{p}}/x_{\mathfrak{p}}\mathfrak{a}_{\mathfrak{p}} = K_{\mathfrak{p}}/(x\mathfrak{a})_{\mathfrak{p}}$ izomorfizmust. Ha koordinátáinként összerakjuk ezeket a leképezéseket (3.2)-ben, akkor kapunk egy

$$x : K/\mathfrak{a} \xrightarrow{\sim} K/x\mathfrak{a}$$

izomorfizmust. (Ld. [Shi71] 116. oldal, [Rub99] 5.10 definíció.)

A következő fontos tételhez még definiáljuk a következőket. Jelölje K^{ab} a maximális Abel bővítést K -nak, és legyen $[\cdot, K^{ab}/K]$ az Artin leképezése a globális osztálytest-elméletnek. (Ld. [Mil20] V.3 fejezet.) Ha σ egy automorfizmusa $\mathbb{C}$ -nek, akkor jelölje E^{σ} azt az elliptikus görbét, amit úgy kapunk, hogy E egyenletének együtthatóira alkalmazzuk σ -t.

3.11. Tétel (A komplex szorzás főtétele). *Rögzítsük egy $\mathfrak{a}$ törtideálját K -nak és egy*

$$\xi : \mathbb{C}/\mathfrak{a} \rightarrow E(\mathbb{C})$$

biholomorfizmust, mint (3.1)-ben. Tegyük fel, hogy $\sigma \in \text{Aut}(\mathbb{C}/K)$ -ra és $x \in \mathbf{A}_K^{\times}$ -re $[x, K^{ab}/K] = \sigma|_{K^{ab}}$. Ekkor létezik egy egyértelmű $\xi' : \mathbb{C}/x^{-1}\mathfrak{a} \rightarrow E^{\sigma}(\mathbb{C})$, amire a

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\xi} & E_{tors} \\ x^{-1} \downarrow & & \downarrow \sigma \\ K/x^{-1}\mathfrak{a} & \xrightarrow{\xi'} & E_{tors}^{\sigma}, \end{array}$$

ahol E_{tors} a torzió részét jelöli $E(\mathbb{C})$ -nek és E_{tors}^{σ} pedig $E^{\sigma}(\mathbb{C})$ -nek.

Bizonyítás. [Shi71] 5.4 tétel. □

Jelölje H a K Hilbert osztálytestét.

3.12. Következmény. (i) $K(j(E)) = H \subset F$.

(ii) $j(E)$ egy egész eleme H -nak.

Bizonyítás. Használjuk a 3.11. tétel jelöléseit. Egy $\sigma \in \text{Aut}(\mathbb{C}/K)$ automorfizmusra

$$j(E) = j(E)^{\sigma} \Leftrightarrow E \cong E^{\sigma} \Leftrightarrow \mathbb{C}/\mathfrak{a} \cong \mathbb{C}/x\mathfrak{a} \Leftrightarrow x\mathfrak{a} = \lambda\mathfrak{a} \text{ valamilyen } \lambda \in \mathbb{C}\text{-re}$$

$$\Leftrightarrow x \in K^{\times} \prod_{\mathfrak{p} \nmid \infty} \mathcal{O}_{\mathfrak{p}}^{\times} \prod_{\mathfrak{p} \mid \infty} K_{\mathfrak{p}}^{\times} \Leftrightarrow [x, H/K] = 1 \Leftrightarrow \sigma|_H \text{ identitás.}$$

Ez bizonyítja (i)-t. Ha a 3.6. tétel (i) részét és a 2.23. lemma (i) részét alkalmazzuk F összes prímjére, akkor megkapjuk, hogy $j(E) \in \mathcal{O}_F$, illetve az (i) részből, hogy $j(E) \in H$, tehát valóban egész eleme H -nak. □

3.13. Következmény. *Létezik egy elliptikus görbe H felett definiálva, aminek az endomorfizmus gyűrűje $\mathcal{O} = \mathcal{O}_K$.*

Bizonyítás. [Rub99] 5.13 következmény. □

3.2. Az elliptikus görbe Hecke karaktere

Mostantól tegyük fel, hogy F egy számtest.

3.14. Tétel. *Létezik egy*

$$\psi = \psi_E : \mathbf{A}_F^\times / F^\times \rightarrow \mathbb{C}^\times$$

Hecke karakter, amire teljesülnek a következők.

(i) *Ha $x \in \mathbf{A}_F^\times$ és $y = N_{F/K}x \in \mathbf{A}_K^\times$, akkor*

$$\psi(x)\mathcal{O} = y_\infty^{-1}(y\mathcal{O}) \subset \mathbb{C}.$$

(ii) *Ha $x \in \mathbf{A}_F^\times$ véges idèle (azaz az arkhimédieszi komponense 1) és $\mathfrak{p}$ egy prímje K -nak, akkor $\psi(x)(N_{F/K}x)_\mathfrak{p}^{-1} \in \mathcal{O}_\mathfrak{p}^\times$ és minden $P \in E[\mathfrak{p}^\infty]$ pontra*

$$[x, F^{\text{ab}}/F]P = \psi(x)(N_{F/K}x)_\mathfrak{p}^{-1}P.$$

(iii) *Ha $\mathfrak{q}$ egy prímje F -nek és $U_\mathfrak{q}$ jelöli a lokális egységeit F -nek $\mathfrak{q}$ -ban, akkor*

$$\psi(U_\mathfrak{q}) = 1 \Leftrightarrow E\text{-nek sima redukciója van } \mathfrak{q}\text{-ban.}$$

Bizonyítás. Tegyük fel, hogy $x \in \mathbf{A}_F^\times$, $y = N_{F/K}x$, $\sigma = [x, F^{\text{ab}}/F]$. Ekkor σ megszorítása K^{ab} -ra $[y, K^{\text{ab}}/K]$, tehát a 3.11. tétel alkalmazható σ -val és y -nal. Mivel σ fixálja F -et, ezért $E = E^\sigma$ (hiszen E F felett definiált), tehát a 3.11. tétel diagramjában $\xi : \mathbb{C}/\mathfrak{a} \rightarrow E(\mathbb{C})$ és $\xi' : \mathbb{C}/y^{-1}\mathfrak{a} \rightarrow E(\mathbb{C})$ izomorfizmusok vannak. Tekintsük a $\xi^{-1} \circ \xi' : \mathbb{C}/y^{-1}\mathfrak{a} \rightarrow \mathbb{C}/\mathfrak{a}$ izomorfizmust. Ez mindenképpen egy elemmel való szorzás, ami az $y^{-1}\mathfrak{a}$ törtideált az $\mathfrak{a}$ törtideálba viszi, tehát erre a $\psi_{\text{fin}}(x) \in K^\times$ elemre $\psi_{\text{fin}}(x)\mathcal{O} = y\mathcal{O}$. Defináljuk a Hecke karakterünk, mint

$$\psi(x) = y_\infty^{-1}\psi_{\text{fin}}(x).$$

Ekkor ψ triviális $F^\times$ -en és homomorfizmus, illetve teljesíti (i)-t. Ha $\mathfrak{p}$ egy prímje K -nak és $k > 0$, akkor a 3.11. tétel szerint a

$$\begin{array}{ccccc} \mathfrak{p}^{-k}\mathfrak{a}_\mathfrak{p}/\mathfrak{a}_\mathfrak{p} & \xrightarrow{\sim} & \mathfrak{p}^{-k}\mathfrak{a}/\mathfrak{a} & \xrightarrow{\xi} & E[\mathfrak{p}^k] \\ y_\mathfrak{p}^{-1} \downarrow & & y^{-1} \downarrow & & \downarrow \sigma \\ \mathfrak{p}^{-k}y_\mathfrak{p}^{-1}\mathfrak{a}_\mathfrak{p}/y_\mathfrak{p}^{-1}\mathfrak{a}_\mathfrak{p} & \xrightarrow{\sim} & \mathfrak{p}^{-k}y^{-1}\mathfrak{a}/y^{-1}\mathfrak{a} & \xrightarrow{\psi_{\text{fin}}(x)\xi} & E[\mathfrak{p}^k] \end{array}$$

diagram kommutatív, ahol a baloldali négyzetet az y hatása adja $K/\mathfrak{a}$ -n. (Ld. 3.10. definíció.) Ez bizonyítja (ii)-t, hiszen egy x véges idélere $y_\infty = 1$ és a $P \in E[\mathfrak{p}^k]$ pont képét a jobboldalon nézhetjük közvetlenül (azaz σP) vagy körbemenve, ahogy viszont $\psi_{\text{fin}}(x)y_\mathfrak{p}^{-1}P$.

(iii) Tegyük fel, hogy $\mathfrak{q}$ egy prímje F -nek és p egy racionális prím, ami nincs $\mathfrak{q}$ alatt. Ha $u \in U_\mathfrak{q}$, akkor minden p feletti $\mathfrak{p}$ prímjére F -nek $(N_{F/K}u)_\mathfrak{p} = 1$, tehát (ii) szerint $[u, F^{\text{ab}}/F]$ úgy hat $T_p(E)$ -n, mint a $\psi(u)$ -val való szorzás. Az $[U_\mathfrak{q}, F^{\text{ab}}/F]$ éppen az inerciárészecsoporthoz $\mathfrak{q}$ -ban, tehát a 2.38. következmény (i) része és a Néron-Ogg-Safarevics kritérium (2.39. tétel (i)) miatt ebből következik a (iii).

Még meg kell mutatni, hogy ψ folytonos, hogy Hecke karakter legyen. A 3.6. tétel (i) része szerint E -nek minden prímben potenciálisan sima redukciója van, tehát a 2.38. következmény (ii) része miatt minden prímnél $[U_q, F^{ab}/F]$ egy véges faktoron keresztül hat $T_p(E)$ -n. A (iii) rész bizonyításánál látottak szerint ez a hatás olyan, mint a $\psi(u)$ -val való szorzás ($u \in U_q$), és a (iii) miatt majdnem minden $\mathfrak{q}$ prímre ez triviális. A maradék véges sok prímre tehát található egy nyílt részcsoportha U_q -nak, amin ψ triviális. Tehát ψ folytonos. $\square$

A 3.14. tétel ψ Hecke karakterének konduktorát jelölje $\mathfrak{f} = \mathfrak{f}_E$. Tekinthejtük ψ -t, mint a karakterét az F $\mathfrak{f}$ -hez relatív prím törtideáljainak. (Ld. [Shu22].) A 3.14. tétel (iii) része miatt látjuk, hogy $\mathfrak{f}$ osztói éppen azok a prímek, ahol E -nek nincs sima redukciója.

3.15. Következmény. *Mint ideálokon definiált karakter, ψ teljesíti a következőket:*

- (i) ha $\mathfrak{b}$ ideálja F -nek relatív prím $\mathfrak{f}$ -hez, akkor $\psi(\mathfrak{b})\mathcal{O} = N_{F/K}\mathfrak{b}$;
- (ii) ha $\mathfrak{q}$ egy prímje F -nek, ami nem osztja $\mathfrak{f}$ -et és $\mathfrak{b}$ egy $\mathfrak{q}$ -hoz relatív prím ideálja $\mathcal{O}$ -nak, akkor $[\mathfrak{q}, F(E[\mathfrak{b}])/F]$ úgy hat $E[\mathfrak{b}]$ -n, mint a $\psi(\mathfrak{q})$ -val való szorzás;
- (iii) ha $\mathfrak{q}$ egy prímje F -nek, ahol E -nek sima a redukciója és $q = N_{F/\mathbb{Q}}\mathfrak{q}$, akkor $\psi(\mathfrak{q}) \in \mathcal{O}$ redukciója modulo $\mathfrak{q}$ a φ_q Frobenius endomorfizmusa $\tilde{E}$ -nak.

Bizonyítás. Az első kettő a 3.14. tétel (i) és (ii) átfogalmazása ideálokon értelmezett Hecke karakterre.

A (iii)-hez tegyük fel, hogy $P \in E_{\text{tors}}$ pont rendje $\mathfrak{b}$, relatív prím $\mathfrak{q}$ -hoz, jelölje $\tilde{P}$ a redukcióját modulo $\bar{F}$ egy $\mathfrak{q}$ feletti prímje, és $\sigma_{\mathfrak{q}} = [\mathfrak{q}, F(E[\mathfrak{b}])/F]$. Ekkor

$$\widetilde{\psi(\mathfrak{q})}\tilde{P} = \widetilde{\sigma_{\mathfrak{q}}P} = \varphi_q\tilde{P},$$

ahol az első egyenlőség a (ii), a második pedig a $[\mathfrak{q}, F(E[\mathfrak{b}])/F]$ Artin szimbólum definíciója. A 2.36. tétel (ii) része szerint a redukció leképezés injektív a $\mathfrak{q}$ -hoz relatív prím torzió részen, ami bizonyítja (iii)-t. $\square$

3.16. Megjegyzés. Látjuk, hogy 3.15. (iii) ad egy konkrét endomorfizmust, amit a 3.8. állítás is kimond, azonban a 3.8. állítás a 3.11. komplex szorzás főtételenek bizonyításának egy fontos eleme, aminek 3.15. egy következménye, tehát a 3.8. állításra szükség van.

3.17. Következmény. *Tegyük fel, hogy $F = K$ és legyen $\mathfrak{p}$ egy olyan prím, amire $\mathcal{O}^\times \rightarrow (\mathcal{O}/\mathfrak{p})^\times$ nem szürjektív. Ekkor $E[\mathfrak{p}] \not\subset E(K)$.*

Bizonyítás. A 3.14. tétel (ii) része miatt $[\mathcal{O}_{\mathfrak{p}}^\times, K^{ab}/K]$ úgy hat $E[\mathfrak{p}]$ -n, mint $\mathcal{O}_{\mathfrak{p}}^\times$ $\psi(x)x^{-1}$ karakterével való szorzás. A 3.14. tétel (i) része miatt pedig $\psi(\mathcal{O}_{\mathfrak{p}}^\times) \subset \mathcal{O}^\times$.

Tegyük fel indirekt, hogy $E[\mathfrak{p}] \subset E(K)$. Ekkor G_K triviálisan hat $E[\mathfrak{p}]$ -n, speciálisan $[\mathcal{O}_{\mathfrak{p}}^\times, K^{ab}/K]$ triviálisan hat $E[\mathfrak{p}]$ -n. Az előzőek miatt $x \in \mathcal{O}_{\mathfrak{p}}^\times$ és $P \in E[\mathfrak{p}]$ pontra $\psi(x)P = xP$. Belátjuk, hogy $r : \mathcal{O}^\times \rightarrow (\mathcal{O}/\mathfrak{p})^\times$ szürjektív.

Tegyük fel, hogy $x + \mathfrak{p} \in (\mathcal{O}/\mathfrak{p})^\times$ valamilyen $x \in \mathcal{O} - \mathfrak{p}$. (Hiszen $\mathcal{O}/\mathfrak{p}$ test, tehát elég annyi, hogy $x + \mathfrak{p}$ ne legyen 0, azaz $x \notin \mathfrak{p}$.) Tekinthező $x \in \mathcal{O}_{\mathfrak{p}}^\times$. Megmutatjuk, hogy $\psi(x) \in \mathcal{O}^\times$ képe r -nél x . Legyen $P \in E[\mathfrak{p}]$ az a pont, aminek a képe az $E[\mathfrak{p}] \cong \mathcal{O}/\mathfrak{p}$ (3.3. állítás) $\mathcal{O}$ -modulus izomorfizmusnál $1 + \mathfrak{p}$. A $\psi(x)P = xP$ egyenlőség $\mathcal{O}/\mathfrak{p}$ -ben megfelel a $\psi(x) + \mathfrak{p} = x + \mathfrak{p}$ egyenlőségnek, de ez pont azt jelenti, hogy az $\mathcal{O}^\times$ -beli $\psi(x)$ képe r -nél $x + \mathfrak{p}$, tehát r szürjektív. $\square$

3.18. Következmény. Tegyük fel, hogy $F = K$. Ekkor $\mathcal{O}^\times \rightarrow (\mathcal{O}/\mathfrak{f})^\times$ injektív. Speciálisan, E -nek nem lehet sima redukciója K minden prímjében.

Bizonyítás. Legyen $u \in \mathcal{O}^\times$, $u \neq 1$ és x az az idèle, amire $x_\infty = 1$ és $x_p = u$ minden véges prímrre. Ekkor $\psi(x) = \psi(u^{-1}x) = u \neq 1$. Az $\{y \in \mathbf{A}_K^\times \text{ véges} : y_p \in 1 + \mathfrak{f}\mathcal{O}_p\}$ halmazon triviális ψ az $\mathfrak{f}$ konduktor definíciója miatt, ami emiatt nem tartalmazhatja x -et. Tehát $u \not\equiv 1 \pmod{\mathfrak{f}}$. Ez bizonyítja az injektivitást, a második állítás pedig következik a 3.14. tétel (iii)-ből: tegyük fel, hogy $\mathfrak{f} = \prod_p \mathfrak{p}^{e_p}$ véges szorzat véges prímekekre. Legyen $\psi = \bigotimes_p \psi_p$ a $\psi_p : K_p^\times \rightarrow \mathbb{C}^\times$ lokális karakterekkel. A kínai maradéktételt használva

$$\mathcal{O}^\times \hookrightarrow (\mathcal{O}/\mathfrak{f})^\times \cong \prod_p (\mathcal{O}/\mathfrak{p}^{e_p})^\times \cong \prod_p (\mathcal{O}_p/\mathfrak{p}^{e_p}\mathcal{O}_p)^\times \cong \prod_p \mathcal{O}_p^\times / (1 + \mathfrak{p}^{e_p}\mathcal{O}_p).$$

Tehát $u \in \mathcal{O}^\times$, $u \neq 1$ képe a szorzatban nem triviális, azaz valamilyen $\mathfrak{p} \mid \mathfrak{f}$ -re $u \not\equiv 1 \pmod{\mathfrak{p}^{e_p}\mathcal{O}_p}$. Az $\mathfrak{f}$ konduktor definíciója szerint $\psi_p(u) \neq 1$, hiszen e_p a legnagyobb kitevő, amire ψ_p triviális $(1 + \mathfrak{p}^{e_p}\mathcal{O}_p)$ -n. Legyen $x \in \mathbf{A}_K^\times$ idèle olyan, hogy $x_p = u$ és $x_q = 1$ minden más prímrre. Ekkor $x \in \mathcal{O}_p^\times \subset \mathbf{A}_K^\times$ és $\psi(x) = \psi_p(u) \neq 1$, vagyis 3.14. tétel (iii) szerint E -nek nem sima a redukciója $\mathfrak{p}$ -ben. $\square$

Ha $\mathfrak{a}$ egy ideálja K -nak, akkor jelölje $K(\mathfrak{a})$ a sugár osztály testét K -nak modulo $\mathfrak{a}$. (Ld. [Mil20] V. 3.6 tétel utáni bekezdést.)

3.19. Következmény. Tegyük fel, hogy E a K felett van definiálva, $\mathfrak{a}$ egy $6\mathfrak{f}$ -hez relatív prím ideálja K -nak és $\mathfrak{p}$ egy prímjé K -nak, ami nem osztja $6\mathfrak{f}$ -et.

- (i) $E[\mathfrak{a}\mathfrak{f}] \subset E(K(\mathfrak{a}\mathfrak{f}))$.
- (ii) A $\text{Gal}(K(E[\mathfrak{a}])/K) \rightarrow (\mathcal{O}/\mathfrak{a})^\times$ leképezése a 3.4. következménynek izomorfizmus.
- (iii) Ha $\mathfrak{b} \mid \mathfrak{a}$, akkor a természetes $\text{Gal}(K(\mathfrak{a}\mathfrak{f})/K(\mathfrak{b}\mathfrak{f})) \rightarrow \text{Gal}(K(E[\mathfrak{a}])/K(E[\mathfrak{b}]))$ leképezés izomorfizmus.
- (iv) $K(E[\mathfrak{a}\mathfrak{p}^n])/K(E[\mathfrak{a}])$ teljesen elágazik $\mathfrak{p}$ felett.
- (v) Ha az $\mathcal{O}^\times \rightarrow (\mathcal{O}/\mathfrak{a})^\times$ leképezés injektív, akkor $K(E[\mathfrak{a}\mathfrak{p}^n])/K(E[\mathfrak{a}])$ elágazásmentes $\mathfrak{p}$ -n kívül.

Bizonyítás. [Rub99] 5.20 következmény. $\square$

3.20. Következmény. Tegyük fel, hogy $\mathfrak{q}$ egy prímjé F -nek. Létezik egy E' elliptikus görbe F felett definiálva, amire

- E' izomorf E -hez $\bar{F}$ felett,
- E' -nek sima redukciója van $\mathfrak{q}$ -ban.

Bizonyítás. [Rub99] 5.22 következmény. $\square$

4. Selmer csoport

Legyen E elliptikus görbe a 0-karakterisztikájú F test felett definiálva, melyen van komplex szorzás a képzetes kvadratikus K test egészeinek gyűrűjével, azaz $\mathcal{O} = \mathcal{O}_K$ -val.

4.1. Lemma. *Tegyük fel, hogy $\mathfrak{p}$ prímje K -nak a $p > 3$ racionális prím felett és $n \geq 0$. Legyen C részcsoportha $(\mathcal{O}/\mathfrak{p}^n)^\times$, ami szorzásként hat $\mathcal{O}/\mathfrak{p}^n$ -en. Ha C ciklikus vagy nem p -csoport, akkor minden $i > 0$ -ra*

$$H^i(C, \mathcal{O}/\mathfrak{p}^n) = 0.$$

Bizonyítás. [Rub99] 6.1 lemma. □

4.2. Lemma. *Tegyük fel, hogy $\mathfrak{p}$ prímje K -nak a $p > 3$ racionális prím felett és $n \geq 0$.*

(i) *Ha $\mathcal{O}_{\mathfrak{p}} = \mathbb{Z}_p$ vagy ha $E[\mathfrak{p}] \not\subset E(F)$, akkor a megszorítás leképezés ad egy*

$$H^1(F, E[\mathfrak{p}^n]) \cong H^1(F(E[\mathfrak{p}^n]), E[\mathfrak{p}^n])^{Gal(F(E[\mathfrak{p}^n])/F)}$$

izomorfizmust.

(ii) *Tegyük fel, hogy F egy véges bővítése $\mathbb{Q}_\ell$ -nek, ahol $\ell \neq p$. Ekkor a megszorítás leképezés ad egy*

$$H^1(F, E)_{\mathfrak{p}^n} \hookrightarrow H^1(F(E[\mathfrak{p}^n])/F)_{\mathfrak{p}^n}$$

injektív függvényt.

Bizonyítás. Vezessük be az $F_n = F(E[\mathfrak{p}^n])$ jelölést. A 3.3. állítás szerint $E[\mathfrak{p}^n] \cong \mathcal{O}/\mathfrak{p}^n$ és a 3.4. következmény miatt megfeleltethető $Gal(F_n/F)$ az $(\mathcal{O}/\mathfrak{p}^n)^\times$ egy C részcsoporthjának. Ha $\mathcal{O}_{\mathfrak{p}} = \mathbb{Z}_p$, akkor C ciklikus, mert

$$(\mathcal{O}/\mathfrak{p}^n)^\times \cong (\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^n \mathcal{O}_{\mathfrak{p}})^\times \cong (\mathbb{Z}_p/p^n \mathbb{Z}_p)^\times \cong (\mathbb{Z}/p^n \mathbb{Z})^\times$$

és $p > 3$ miatt van primitív gyök modulo p^n . Ha $E[\mathfrak{p}] \not\subset E(F)$, akkor $Gal(F_1/F)$ nem hat triviálisan $E[\mathfrak{p}]$ -n, speciálisan nem triviális csoport. Viszont $n = 1$ -re is $Gal(F_1/F)$ megfeleltethető $(\mathcal{O}/\mathfrak{p})^\times$ egy részcsoporthjának, tehát p -hez relatív prím rendű. Ekkor azonban $Gal(F_n/F)/Gal(F_n/F_1) \cong Gal(F_1/F)$ miatt a véges C csoportnak a rendje nem p -hatvány, így nem p -csoport. A 4.1. lemma miatt minden $i > 0$ -ra $H^i(C, E[\mathfrak{p}^n]) = 0$. A csoportkohomológiából ismert Inf-Res sorozat (angolul: inflation-restriction sequence) ad egy

$$0 \rightarrow H^1(C, E[\mathfrak{p}^n]^{G_{F_n}}) \rightarrow H^1(F, E[\mathfrak{p}^n]) \rightarrow H^1(F_n, E[\mathfrak{p}^n])^{G_{F_n}} \rightarrow H^2(C, E[\mathfrak{p}^n]^{G_{F_n}})$$

egzakt sorozatot, ahol $E[\mathfrak{p}^n]^{G_{F_n}} = E[\mathfrak{p}^n]$, tehát a második és az utolsó tag 0, ami bizonyítja (i)-t.

A (ii)-hez ld. [Rub99] 6.2 lemma (ii). □

4.1. A nagyított Selmer csoport

A továbbiakban tegyük fel, hogy F egy számtest.

4.3. Definíció. Ha $\alpha \in \mathcal{O}$, akkor legyen $\mathcal{S}'_\alpha(E) = \mathcal{S}'_\alpha(E/F) \subset H^1(F, E[\alpha])$ a következő:

$$\begin{aligned}\mathcal{S}'_\alpha(E) &= \{c \in H^1(F, E[\alpha]) : \text{res}_{\mathfrak{q}}(c) \in \text{im}(E(F_{\mathfrak{q}})/\alpha E(F_{\mathfrak{q}})) \text{ minden } \mathfrak{q} \nmid \alpha\} \\ &= \{c \in H^1(F, E[\alpha]) : \text{res}_{\mathfrak{q}}(c) = 0 \in H^1(F_{\mathfrak{q}}, E(\bar{F}_{\mathfrak{q}})) \text{ minden } \mathfrak{q} \nmid \alpha\}\end{aligned}$$

a (2.4) diagramban. Nyilván $\mathcal{S}_\alpha(E) \subset \mathcal{S}'_\alpha(E)$.

4.4. Lemma. *Tegyük fel, hogy $\mathfrak{p}$ egy prímjel K -nak, ami nem osztja 6-ot, $n \geq 1$, $E[\mathfrak{p}^n] \subset E(F)$ és $\mathfrak{p}^n = \alpha\mathcal{O}$. Ekkor*

$$\mathcal{S}'_\alpha(E/F) = \text{Hom}(\text{Gal}(M/F), E[\mathfrak{p}^n]),$$

ahol M a maximális Abel p -bővítése F -nek, ami elágazásmentes a $\mathfrak{p}$ feletti prímeken kívül.

Bizonyítás. Mivel $E[\mathfrak{p}^n] \subset E(F)$, ezért G_F triviálisan hat $E[\mathfrak{p}^n]$ -en, tehát

$$H^1(F, E[\mathfrak{p}^n]) = \text{Hom}(G_F, E[\mathfrak{p}^n]), \quad H^1(F_{\mathfrak{q}}, E[\mathfrak{p}^n]) = \text{Hom}(G_{F_{\mathfrak{q}}}, E[\mathfrak{p}^n]),$$

ahol $\mathfrak{q}$ egy prímjel F -nek, ami nem osztja $\mathfrak{p}$ -t. A 3.6. tétel (ii) része E -nek sima redukciója van $\mathfrak{p}$ -ben. A 2.37. következmény miatt a (2.4) diagramban $E(F_{\mathfrak{q}})/\alpha E(F_{\mathfrak{q}})$ képe benne van $\text{Hom}(G_{F_{\mathfrak{q}}}/I_{\mathfrak{q}}, E[\mathfrak{p}^n])$ -ban, ahol $I_{\mathfrak{q}}$ az inerciarészcsoport $G_{F_{\mathfrak{q}}}$ -ban, és adottak a

$$\text{Hom}(G_{F_{\mathfrak{q}}}/I_{\mathfrak{q}}, E[\mathfrak{p}^n]) \cong E[\mathfrak{p}^n] \cong \mathcal{O}/\mathfrak{p}^n$$

$\mathcal{O}$ -modulus izomorfizmusok. Másrészt ha $\mathbb{k}$ -val jelöljük $F_{\mathfrak{q}}$ maradéktestét és használjuk a 2.36. tételt, akkor

$$E(F_{\mathfrak{q}})/\alpha E(F_{\mathfrak{q}}) \cong \tilde{E}(\mathbb{k})/\alpha \tilde{E}(\mathbb{k}) \cong \mathcal{O}/\mathfrak{p}^n.$$

Tehát az $E(F_{\mathfrak{q}})/\alpha E(F_{\mathfrak{q}}) \hookrightarrow H^1(F_{\mathfrak{q}}, E[\mathfrak{p}^n])$ képe a (2.4) diagramban $\text{Hom}(G_{F_{\mathfrak{q}}}/I_{\mathfrak{q}}, E[\mathfrak{p}^n])$. $\mathcal{S}'_\alpha$ definíciójából következik a lemma. $\square$

4.5. Tétel. *Tegyük fel, hogy E K felett definiált, $\mathfrak{p}$ prímjel K -nak nem osztja 6-ot, $n \geq 1$ és $\mathfrak{p}^n = \alpha\mathcal{O}$. Legyen $K_n = K(E[\mathfrak{p}^n])$. Ekkor*

$$\mathcal{S}'_\alpha(E/K) = \text{Hom}(\text{Gal}(M_n/K_n), E[\mathfrak{p}^n])^{Gal(K_n/K)},$$

ahol M_n a maximális Abel p -bővítése K_n -nek, ami elágazásmentes a $\mathfrak{p}$ feletti prímeken kívül.

Bizonyítás. Legyen $G = \text{Gal}(K_n/K)$. A 3.17. következmény szerint $E[\mathfrak{p}] \not\subset E(F)$, tehát a 4.2. lemma (i) része miatt a megszorítás leképezés ad egy

$$H^1(K, E[\mathfrak{p}^n]) \cong H^1(K_n, E[\mathfrak{p}^n])^G$$

izomorfizmust. Az $\mathcal{S}'_\alpha(E/K)$ képe ennél az izomorfizmusnál benne van $\mathcal{S}'_\alpha(E/K_n)$ -ben. És fordítva is, ha egy $H^1(K, E[\mathfrak{p}^n])$ -beli osztály képe benne van $\mathcal{S}'_\alpha(E/K_n)$ -ben, akkor az az osztály benne volt $\mathcal{S}'_\alpha(E/K)$ -ban, mert 4.2. lemma (ii) része miatt a

$$H^1(K_{\mathfrak{q}}, E(\bar{K}_{\mathfrak{q}})) \rightarrow H^1(K_{\mathfrak{q}}(E[\mathfrak{p}^n]), E(\bar{K}_{\mathfrak{q}}))$$

megszorítás leképezés injektív minden olyan $\mathfrak{q}$ prímjelre, amik nem osztják $\mathfrak{p}$ -t. Tehát $\mathcal{S}'_\alpha(E/K) = \mathcal{S}'_\alpha(E/K_n)^G$ és a tétel következik a 4.4. lemmából. $\square$

4.2. A valódi Selmer csoport

Mostantól tegyük fel, hogy $F = K$, azaz E K felett definiált. A 3.12. következmény miatt K osztályszáma 1, azaz $\mathcal{O}$ főideálgyűrű. Rögzítsük egy $\mathfrak{p}$ prímtét K -nak, ami nem osztja 6f-et és egy π generátorát $\mathfrak{p}$ -nek. Legyen $\lambda_E : E_1(K_{\mathfrak{p}}) \rightarrow \mathfrak{p}\mathcal{O}_{\mathfrak{p}}$ a 2.33. definíció logaritmus függvénye.

4.6. Lemma. *A λ_E leképezés egyértelműen kiterjed egy $E(K_{\mathfrak{p}}) \rightarrow \mathfrak{p}\mathcal{O}_{\mathfrak{p}}$ szűrjekcióvá, aminek a magja véges és nincs $\mathfrak{p}$ -torziója.*

Bizonyítás. Legyen p a $\mathfrak{p}$ alatti racionális prím. Ekkor $p > 3$ és $\text{ord}_{\mathfrak{p}}(p) \leq 2$, ezért a 2.34. következmény szerint $\lambda_E : K_{\mathfrak{p}} \rightarrow \mathfrak{p}\mathcal{O}_{\mathfrak{p}}$ izomorfizmus. Mivel $\mathfrak{p}$ nem osztja f -et, ezért E -nek sima redukciója van $\mathfrak{p}$ -ben. A 2.25. állítás szerint $E(K_{\mathfrak{p}})/E_1(K_{\mathfrak{p}}) \cong \tilde{E}(\mathbb{k})$, ahol $\mathbb{k}$ a maradékteste $K_{\mathfrak{p}}$ -nek. Speciálisan $E(K_{\mathfrak{p}})/E_1(K_{\mathfrak{p}})$ véges. A 3.15. következmény (iii) része szerint $\psi(\mathfrak{p})$ redukciója modulo $\mathfrak{p}$ a φ_p Frobenius endomorfizmus, tehát tisztán inszeparábilis. Vagyis használhatjuk a 2.27. lemmát, azaz $\widehat{\psi(\mathfrak{p})} = \varphi_p$ injektív $\tilde{E}(\mathbb{k})$ -n és $\ker(\psi(\mathfrak{p})) \subset E_1(F)$. Belátjuk, hogy $E(K_{\mathfrak{p}})/E_1(K_{\mathfrak{p}})$ -nek nincs $\mathfrak{p}$ -torziója. Tegyük fel, hogy $P \in E(K_{\mathfrak{p}})$, $P \notin E_1(K_{\mathfrak{p}})$. Az előzőek miatt $\psi(\mathfrak{p})P \neq O$. Ha $\psi(\mathfrak{p})P \in E_1(K_{\mathfrak{p}})$, akkor definíció szerint $\tilde{O} = \widehat{\psi(\mathfrak{p})P} = \varphi_p \tilde{P}$, de φ_p injektív, ezért $\tilde{P} = \tilde{O}$, ami ellentmond P választásának. Így $\psi(\mathfrak{p})P \notin E_1(K_{\mathfrak{p}})$. Akárhányszor megcsinálhatjuk ezt, vagyis minden $k \geq 0$ -ra $\psi(\mathfrak{p})^k P \notin E_1(K_{\mathfrak{p}})$, azaz $E(K_{\mathfrak{p}})/E_1(K_{\mathfrak{p}})$ -nek nincs $\mathfrak{p}$ -torziója 3.15. következmény (i) része miatt. $\square$

4.7. Definíció. Minden $n \geq 1$ -re legyen $K_{n,\mathfrak{p}} = K_{\mathfrak{p}}(E[\mathfrak{p}^n])$ és definiáljunk egy Kummer párosítást:

$$\begin{aligned} \langle \cdot, \cdot \rangle_{\pi^n} : E(K_{\mathfrak{p}}) \times K_{n,\mathfrak{p}}^{\times} &\rightarrow E[\mathfrak{p}^n] \\ \langle P, x \rangle_{\pi^n} &= [x, K_{n,\mathfrak{p}}^{\text{ab}}/K_{n,\mathfrak{p}}]Q - Q, \end{aligned}$$

ahol $[\cdot, K_{n,\mathfrak{p}}^{\text{ab}}/K_{n,\mathfrak{p}}]$ a lokális Artin leképezés és $Q \in E(\bar{K}_{\mathfrak{p}})$ teljesíti, hogy $\pi^n Q = P$.

4.8. Lemma. *Minden n -re létezik egy egyértelmű Galois-ekvivariáns $\delta_n : K_{n,\mathfrak{p}}^{\times} \rightarrow E[\mathfrak{p}^n]$ homomorfizmus, ami teljesíti, hogy ha $P \in E(K_{\mathfrak{p}})$ és $x \in K_{n,\mathfrak{p}}^{\times}$, akkor*

$$\langle P, x \rangle_{\pi^n} = (\pi^{-1}\lambda_E(P))\delta_n(x).$$

Továbbá, ha $\mathcal{O}_{n,\mathfrak{p}}$ jelöli $K_{n,\mathfrak{p}}$ egészeinek gyűrűjét, akkor $\delta_n(\mathcal{O}_{n,\mathfrak{p}}^{\times}) = E[\mathfrak{p}^n]$.

Bizonyítás. Legyen $\delta_n(x) = \langle R, x \rangle_{\pi^n}$, ahol $R \in E(K_{\mathfrak{p}})$ -ra $\lambda_E(R) = \pi$. Az egyetlen nem triviális része a lemmának a szűrjektivitás.

A 3.14. tétel (ii) része miatt, ha $x \in \mathcal{O}_{\mathfrak{p}}^{\times}$, akkor az $[x, K_{n,\mathfrak{p}}/K_{\mathfrak{p}}]$ úgy hat $E[\mathfrak{p}^n]$ -en, mint az x^{-1} -zel való szorzás. Tehát $E(K_{\mathfrak{p}})$ -nek nincs $\mathfrak{p}$ -torziója és $E[\mathfrak{p}]$ -nek nincs valódi $G_{K_{\mathfrak{p}}}$ -stabil részcsoportha.

A 4.6. lemma ad egy $E(K_{\mathfrak{p}})/\mathfrak{p}^n E(K_{\mathfrak{p}}) \xrightarrow{\sim} \mathcal{O}/\mathfrak{p}^n$ izomorfizmust. Mivel

$$E(K_{\mathfrak{p}})/\mathfrak{p}^n E(K_{\mathfrak{p}}) \hookrightarrow H^1(K_{\mathfrak{p}}, E[\mathfrak{p}^n]) \hookrightarrow \text{Hom}(K_{n,\mathfrak{p}}^{\times}, E[\mathfrak{p}^n])$$

injektív (az első (2.4) miatt, míg a másik a 4.2. lemma (ii) és 4.6. lemma miatt), ezért a δ_n képe nincs benne $E[\mathfrak{p}^{n-1}]$ -ben. Mivel δ_n képe $G_{K_{\mathfrak{p}}}$ -stabil, ezért ez az egész $E[\mathfrak{p}^n]$. De $\delta_n(K_{n,\mathfrak{p}}^{\times})/\delta_n(\mathcal{O}_{n,\mathfrak{p}}^{\times})$ egy faktora $E[\mathfrak{p}^n]$ -nek, amin $G_{K_{\mathfrak{p}}}$ triviálisan hat, tehát ahogy előbb, ennek a faktornak triviálisnak kell lennie, azaz úgyszintén $\delta_n(\mathcal{O}_{n,\mathfrak{p}}^{\times}) = E[\mathfrak{p}^n]$. $\square$

4.9. Tétel. Legyen $K_n = K(E[\mathfrak{p}^n])$ és $\mathcal{O}_n$ az egészeinek gyűrűje, illetve legyen

$$W_n = K_n^\times \prod_{v|\infty} K_{n,v}^\times \prod_{v \nmid \mathfrak{p}\infty} \mathcal{O}_{n,v}^\times \cdot \ker(\delta_n) \subset \mathbf{A}_{K_n}^\times.$$

Ekkor

$$\mathcal{S}_{\pi^n}(E/K) = \text{Hom}(\mathbf{A}_{K_n}^\times/W_n, E[\mathfrak{p}^n])^{\text{Gal}(K_n/K)}.$$

Bizonyítás. Definíció szerint van egy

$$E(K_{\mathfrak{p}})/\pi^n E(K_{\mathfrak{p}}) \hookrightarrow \text{Hom}(K_{n,\mathfrak{p}}^\times/\ker(\delta_n), E[\mathfrak{p}^n])^{\text{Gal}(K_{n,\mathfrak{p}}/K_{\mathfrak{p}})} \quad (4.1)$$

injektív leképezés. A 4.6. lemmából következik, hogy $E(K_{\mathfrak{p}})/\pi^n E(K_{\mathfrak{p}}) \cong \mathcal{O}/\mathfrak{p}^n$. A 4.8. lemmából pedig, hogy $K_{n,\mathfrak{p}}^\times/\ker(\delta_n) \cong E[\mathfrak{p}^n]$, illetve 3.14. tétel (ii)-ből, hogy

$$\text{Hom}(E[\mathfrak{p}^n], E[\mathfrak{p}^n])^{\text{Gal}(K_{n,\mathfrak{p}}/K_{\mathfrak{p}})} \cong \text{Hom}_{\mathcal{O}}(E[\mathfrak{p}^n], E[\mathfrak{p}^n]) \cong \mathcal{O}/\mathfrak{p}^n.$$

Vagyis (4.1) egy izomorfizmus. A tétel következik a 4.5. tételből és osztálytestelméletből. $\square$

Jelölje A az ideál osztálycsoportját $K(E[\mathfrak{p}])$ -nek, illetve $\mathcal{E}$ a $K(E[\mathfrak{p}])$ globális egységeinek csoportját.

4.10. Következmény.

$$\mathcal{S}_{\pi}(E) = 0 \Leftrightarrow \left(\text{Hom}(A, E[\mathfrak{p}])^{\text{Gal}(K(E[\mathfrak{p}])/K)} = 0 \text{ és } \delta_1(\mathcal{E}) \neq 0 \right).$$

Bizonyítás. A 3.19. következmény (iv) része miatt $K(E[\mathfrak{p}])/K$ teljesen elágazik $\mathfrak{p}$ -ben ($n = 1$, $\mathfrak{a} = \mathcal{O}$ választással). A bővítés foka $\mathbf{N}\mathfrak{p} - 1$ a 3.19. következmény (ii) része miatt. Jelölje $K_{1,\mathfrak{p}}$ a $K(E[\mathfrak{p}])$ teljessé tételét a $\mathfrak{p}$ feletti prímben. Legyen $\mathcal{O}_{1,\mathfrak{p}}$ az egészeinek gyűrűje és $\bar{\mathcal{E}}$ a lezártját $\mathcal{E}$ -nek $\mathcal{O}_{1,\mathfrak{p}}$ -ben. Legyen még továbbá $V = \ker(\delta_1) \cap \mathcal{O}_{1,\mathfrak{p}}^\times$ és $\Delta = \text{Gal}(K(E[\mathfrak{p}])/K)$. Létezik egy

$$0 \rightarrow \mathcal{O}_{1,\mathfrak{p}}^\times/\bar{\mathcal{E}}V \rightarrow \mathbf{A}_{K_1}^\times/W_1 \rightarrow A' \rightarrow 0$$

egzakt sorozat, ahol W_1 halmaz a 4.9. tételből van és A' a faktora A -nak a $\mathfrak{p}$ feletti $\mathcal{P}$ prím osztályának egy hatványával faktorizálva. Feltettük, hogy $F = K$, így $\mathcal{O}$ főideálgyűrű, tehát $\mathcal{P}^{\mathbf{N}\mathfrak{p}-1} = \mathfrak{p}$ főideál, azaz $\mathcal{P}^{\mathbf{N}\mathfrak{p}-1}$ osztálya triviális A -ban. Ha $h : A \rightarrow E[\mathfrak{p}]$ homomorfizmus, akkor $h(\mathcal{P}^{\mathbf{N}\mathfrak{p}-1}) = (\mathbf{N}\mathfrak{p} - 1)h(\mathcal{P}) = \mathcal{O}$ és $\mathbf{N}\mathfrak{p} - 1$ relatív prím $\mathfrak{p}$ -hez $\mathcal{O}$ -ban, tehát invertálható $\mathcal{O}/\mathfrak{p}$ -ben, azaz $h(\mathcal{P}) = \mathcal{O}$ ($E[\mathfrak{p}] \cong \mathcal{O}/\mathfrak{p}$). Tehát $\text{Hom}(A, E[\mathfrak{p}]) = \text{Hom}(A', E[\mathfrak{p}])$. Ekkor

$$0 \rightarrow \text{Hom}(\mathcal{O}_{1,\mathfrak{p}}^\times/\bar{\mathcal{E}}V, E[\mathfrak{p}])^\Delta \rightarrow \text{Hom}(\mathbf{A}_{K_1}^\times/W_1, E[\mathfrak{p}])^\Delta \rightarrow \text{Hom}(A', E[\mathfrak{p}])^\Delta$$

egzakt, mert $\text{Hom}(-, E[\mathfrak{p}])$ balegzakt funktor. Tehát a 4.9. tétel miatt

$$\begin{aligned} \mathcal{S}_{\pi}(E) = 0 &\Leftrightarrow \text{Hom}(A_{K_1}^\times/W_1, E[\mathfrak{p}])^\Delta = 0 \Leftrightarrow \\ &\Leftrightarrow \left(\text{Hom}(A, E[\mathfrak{p}])^\Delta = 0 \text{ és } \text{Hom}(\mathcal{O}_{1,\mathfrak{p}}^\times/\bar{\mathcal{E}}V, E[\mathfrak{p}])^\Delta = 0 \right). \end{aligned}$$

A 4.8. lemma szerint $\delta_1 : \mathcal{O}_{1,\mathfrak{p}}^\times/V \rightarrow E[\mathfrak{p}]$ izomorfizmus. A 3.19. következmény (ii) része miatt $\Delta \cong (\mathcal{O}/\mathfrak{p})^\times$, tehát $E[\mathfrak{p}]$ -nek nincs valódi Galois-stabil részmodulusa. Ha

adott egy nemnulla $\mathcal{O}_{1,\mathfrak{p}}^\times/\bar{\mathcal{E}}V \rightarrow E[\mathfrak{p}]$ Δ -ekvivariáns leképezés, akkor a képe Galois-stabil, tehát a leképezés szűrjektív. Vagyis δ_1^{-1} -zel komponálva kapunk egy $\mathcal{O}_{1,\mathfrak{p}}^\times/\bar{\mathcal{E}}V \rightarrow \mathcal{O}_{1,\mathfrak{p}}^\times/V$ szűrjekciót. Létezik azonban a természetes $\mathcal{O}_{1,\mathfrak{p}}^\times/V \rightarrow \mathcal{O}_{1,\mathfrak{p}}^\times/\bar{\mathcal{E}}V$ szűrjekció is, azaz a két csoport elemszáma megegyezik, vagyis $\bar{\mathcal{E}}V \subset V$. Ha $\bar{\mathcal{E}}V \subset V$, akkor $\delta_1 : \mathcal{O}_{1,\mathfrak{p}}^\times/\bar{\mathcal{E}}V \rightarrow E[\mathfrak{p}]$ nemnulla Δ -ekvivariáns leképezés. Összefoglalva

$$\mathrm{Hom}(\mathcal{O}_{1,\mathfrak{p}}^\times/\bar{\mathcal{E}}V, E[\mathfrak{p}])^\Delta = 0 \Leftrightarrow \bar{\mathcal{E}}V \not\subset V \Leftrightarrow \delta_1(\mathcal{E}) \neq 0,$$

ami az előzőekkel együtt bizonyítja a következményt. $\square$

5. Elliptikus egységek

Rögzítsünk egy K képzetes kvadratikus testet, aminek egészeinek gyűrűjét jelöljük $\mathcal{O}$ -val. Legyen továbbá E egy elliptikus görbe $\mathbb{C}$ felett, amin van komplex szorzás $\mathcal{O}$ -val. Legyen $\mathfrak{a}$ egy 6-hoz relatív prím, nemtriviális ideálja $\mathcal{O}$ -nak. Az egyszerűség kedvéért tegyük fel, hogy K osztályszáma 1, azaz $\mathcal{O}$ főideálgyűrű.

5.1. Definíció és alaptulajdonságok

5.1. Definíció. Válasszunk egy (2.2) Weierstraß egyenletet E -nek. Defináljuk a következő racionális függvényt E -n:

$$\Theta_{E,\mathfrak{a}} = \alpha^{-12} \Delta(E)^{\mathbf{N}\mathfrak{a}-1} \prod_{P \in E[\mathfrak{a}] - \mathcal{O}} (x - x(P))^{-6},$$

ahol α egy tetszőleges generátora $\mathfrak{a}$ -nak, x pedig a behelyettesített pont x -koordinátája. Mivel $\mathcal{O}^\times = \mathrm{Aut}(E)$ 2, 4 vagy 6 elemű [Sil09] III.10.1 tétel szerint, ezért a definíció nem függ α választásától.

5.2. Lemma. (i) $\Theta_{E,\mathfrak{a}}$ nem függ a Weierstraß egyenlet választásától.

(ii) Ha $\phi : E' \xrightarrow{\sim} E$ egy izomorfizmus elliptikus görbéknek, akkor $\Theta_{E',\mathfrak{a}} = \Theta_{E,\mathfrak{a}} \circ \phi$.

(iii) Ha E F felett van definiálva, akkor $\Theta_{E,\mathfrak{a}}$ is F felett definiált.

Bizonyítás. Minden másik Weierstraß egyenlet megkapható egy

$$x' = u^2x + r, \quad y' = u^3y + su^2x + t$$

helyettesítéssel, ahol $u \in \mathbb{C}^\times$ (ld. [Sil09] III. 3.1 (b) állítás). Ekkor $\Delta(E') = u^{12} \Delta(E)$ (ld. [Sil09] III. 1.3 megjegyzés). A 3.3. állítás szerint $E[\mathfrak{a}] \cong \mathcal{O}/\mathfrak{a}$, tehát $\#(E[\mathfrak{a}]) = \mathbf{N}\mathfrak{a}$. Az új koordinátákkal felírva $\Theta_{E,\mathfrak{a}}$ -t látjuk, hogy megegyezik a kettő, vagyis ez bizonyítja (i)-t, (ii) pedig csak egy másik megfogalmazása (i)-nek. A (iii)-hez vegyük észre, hogy $\alpha \in F$, mert $\mathcal{O} \subset F$ és $\Delta(E) \in F$. A G_F abszolút Galois csoport hat az $E[\mathfrak{a}] - \mathcal{O}$ halmazon, mint a 3.4. következményben. Tehát G_F permutálja az $\{x(P) : P \in E[\mathfrak{a}] - \mathcal{O}\}$ halmazt, vagyis ha a

$$\prod_{P \in E[\mathfrak{a}] - \mathcal{O}} (x - x(P)) \in \bar{F}[x]$$

polinomon együtthatónként hat egy $\sigma \in G_F$ automorfizmus, akkor az fixen hagyja. Vagyis az együtthatók F -ben is vannak, tehát $\Theta_{E,\mathfrak{a}}$ F felett definiált. $\square$

5.3. Lemma. Tegyük fel, hogy E K felett definiált és $\mathfrak{p}$ egy olyan prímje K -nak, ahol E -nek sima a redukciója. Rögzítsük E egy olyan Weierstraß egyenletét, ami minimális $\mathfrak{p}$ -ben. Legyenek $\mathfrak{b}, \mathfrak{c}$ nemtriviális relatív prím ideáljai $\mathcal{O}$ -nak, és $P \in E[\mathfrak{b}]$, $Q \in E[\mathfrak{c}]$ pontjai $E(\bar{K})$ -nak, amik rendje rendre $\mathfrak{b}$ és $\mathfrak{c}$. Fixáljuk egy kiterjesztését a $\mathfrak{p}$ -adikus értékelésnek $\bar{K}$ -ra, amire $\text{ord}_{\mathfrak{p}}(\mathfrak{p}) = 1$.

(i) Ha $n > 0$ és $\mathfrak{b} = \mathfrak{p}^n$, akkor $\text{ord}_{\mathfrak{p}}(x(P)) = -\frac{2}{N\mathfrak{p}^{n-1}(N\mathfrak{p}-1)}$.

(ii) Ha $\mathfrak{b}$ nem hatványa $\mathfrak{p}$ -nek, akkor $\text{ord}_{\mathfrak{p}}(x(P)) \geq 0$.

(iii) Ha $\mathfrak{p} \nmid \mathfrak{bc}$, akkor $\text{ord}_{\mathfrak{p}}(x(P) - x(Q)) = 0$.

Bizonyítás. (i) Tegyük fel, hogy $\mathfrak{b} = \mathfrak{p}^n$ valamilyen $n \geq 1$ -re. Legyen $\hat{E}$ a 2.28. tétel szerinti formális csoportja E -nek. Legyen $\pi = \psi_E(\mathfrak{p})$ és $[\pi^m](X) \in \mathcal{O}[[X]]$ a π^m -hez tartozó endomorfizmusa $\hat{E}$ -nak minden m -re. Definiáljuk az

$$f(X) = \frac{[\pi^n](X)}{[\pi^{n-1}](X)} \in \mathcal{O}[[X]]$$

hatványsort. A $\pi \in \mathcal{O}$ redukciója modulo $\mathfrak{p}$ éppen a Frobenius endomorfizmusa $\tilde{E}$ -nak a 3.15. következmény (iii) része miatt. Tehát a 2.30. következmény miatt $[\pi](X) \equiv X^{N\mathfrak{p}} \pmod{\mathfrak{p}}$, ahonnan

$$f(X) \equiv X^{N\mathfrak{p}^n - N\mathfrak{p}^{n-1}} \pmod{\mathfrak{p}}.$$

A 2.35. állításból pedig következik, hogy

$$f(X) \equiv \pi \pmod{X}.$$

Használjuk a Weierstraß preparációs tételt, ami ad egy $f(X) = e(X)u(X)$ felbontást, ahol $e(X)$ egy $(N\mathfrak{p}^n - N\mathfrak{p}^{n-1})$ -fokú Eisenstein polinom és $u(X) \in \mathcal{O}[[X]]^\times$ egység. Mivel a Frobenius endomorfizmusa $\tilde{E}$ -nek tisztán inszeparábilis endomorfizmusa, ezért a 2.27. lemma (ii) részéből következik, hogy $E[\mathfrak{p}^n] \subset E_1(\bar{K}_{\mathfrak{p}})$. Tehát a P pontnak vehetjük a képét a 2.29. következmény inverzénél, ami $z = -x(P)/y(P)$. De a P pontra definíció szerint teljesül $\pi^n P = O$, $\pi^{n-1} P \neq O$, tehát z gyöke $f(X)$ -nek. Mivel egy egység hatványsornak nem lehet gyöke, ezért $e(z) = 0$. Könnyen számolható, hogy $\text{ord}_{\mathfrak{p}}(x(P)/y(P)) = 1/N\mathfrak{p}^{n-1}(N\mathfrak{p} - 1)$, mert $e(X)$ egy Eisenstein polinom. A 2.26. lemma szerint a $P \in E_1(K_{\mathfrak{p}})$ pontra $3\text{ord}_{\mathfrak{p}}(x(P)) = 2\text{ord}_{\mathfrak{p}}(y(P))$, azaz $\text{ord}_{\mathfrak{p}}(x(P)) = -2\text{ord}_{\mathfrak{p}}(x(P)/y(P))$. Ezzel (i) kész van.

(ii) Ha $\mathfrak{b}$ nem $\mathfrak{p}$ hatványa, akkor létezik $\mathfrak{q} \neq \mathfrak{p}$ prím, ami osztja $\mathfrak{b}$ -t. A $\psi(\mathfrak{q}) \in \mathcal{O}$ endomorfizmusra $\text{ord}_{\mathfrak{p}}(\psi(\mathfrak{q})) = 0$, tehát $\psi(\mathfrak{q}) \in \mathcal{O}_{\mathfrak{p}}^\times$. Vagyis a 2.36. tétel (i) része szerint $\psi(\mathfrak{q})$ automorfizmus $E_1(\bar{K}_{\mathfrak{p}})$ -n.

3.15. következmény (i) része szerint $\psi(\mathfrak{q})\mathcal{O} = \mathfrak{q}$, tehát $\psi(\mathfrak{q})P \in E[\mathfrak{b}/\mathfrak{q}]$, vagyis valamilyen $\alpha \in \mathfrak{b}/\mathfrak{q} \subset \mathcal{O}$ endomorfizmusra $\alpha(\psi(\mathfrak{q})P) = O$. De mivel $\mathcal{O}$ kommutatív, ezért $\psi(\mathfrak{q})\alpha P = O$. Mivel P rendje pontosan $\mathfrak{b}$, ezért $\alpha P \neq O$.

Tegyük fel, hogy $P \in E_1(\bar{K}_{\mathfrak{p}})$. Ekkor $\widetilde{\alpha P} = \tilde{\alpha}\tilde{P} = \tilde{\alpha}\tilde{O} = \tilde{O}$, tehát $\alpha P \in E_1(\bar{K}_{\mathfrak{p}})$. Mivel $\psi(\mathfrak{q})$ automorfizmus $E_1(\bar{K}_{\mathfrak{p}})$ -nek, ezért $\psi(\mathfrak{q})\alpha P \neq O$, ami ellentmondás. Tehát $P \notin E_1(\bar{K}_{\mathfrak{p}})$, és ezért 2.26. lemma miatt $\text{ord}_{\mathfrak{p}}(x(P)) \geq 0$.

(iii) Jelöljük a P és Q pontok redukcióját modulo $\mathfrak{p}$ $\tilde{P}$ -vel és $\tilde{Q}$ -val. Ekkor

$$\begin{aligned} \text{ord}_{\mathfrak{p}}(x(P) - x(Q)) > 0 &\Leftrightarrow x(\tilde{P}) = x(\tilde{Q}) \Leftrightarrow \tilde{P} = \pm\tilde{Q} \Leftrightarrow \\ &\Leftrightarrow \widetilde{P \mp Q} = \tilde{O} \Leftrightarrow P \mp Q \in E_1(\bar{K}_{\mathfrak{p}}). \end{aligned}$$

Mivel $\mathfrak{b}$ és $\mathfrak{c}$ relatív prímek, ezért $P \pm Q$ rendje nem lehet $\mathfrak{p}$ -hatvány, tehát hasonlóan a (ii) részhez $P \pm Q \notin E_1(\bar{K}_{\mathfrak{p}})$. $\square$

Minden $\mathfrak{b}$ ideáljára $\mathcal{O}$ -nak jelöljük $K(\mathfrak{b})$ -vel a sugár osztálytestét K -nak modulo $\mathfrak{b}$.

5.4. Tétel. *Legyen $\mathfrak{b}$ egy nemtriviális, $\mathfrak{a}$ -hoz relatív prím ideálja $\mathcal{O}$ -nak és $Q \in E[\mathfrak{b}]$ egy $\mathcal{O}$ -generátora $E[\mathfrak{b}]$ -nek (ld. 3.3. állítás).*

(i) $\Theta_{E,\mathfrak{a}}(Q) \in K(\mathfrak{b})$.

(ii) *Ha $\mathfrak{c}$ egy $\mathfrak{b}$ -hez relatív prím ideálja $\mathcal{O}$ -nak, c egy generátora $\mathfrak{c}$ -nek, $\sigma_{\mathfrak{c}} = [\mathfrak{c}, K(\mathfrak{b})/K]$, akkor*

$$\Theta_{E,\mathfrak{a}}(Q)^{\sigma_{\mathfrak{c}}} = \Theta_{E,\mathfrak{a}}(cQ).$$

(iii) *Ha $\mathfrak{b}$ nem prímhatalvány, akkor $\Theta_{E,\mathfrak{a}}(Q)$ egy globális egység. Ha $\mathfrak{b}$ egy $\mathfrak{p}$ prím hatványa, akkor $\Theta_{E,\mathfrak{a}}(Q)$ egység azon prímeknél, amik nem osztják $\mathfrak{p}$ -t.*

Bizonyítás. Mivel feltettük, hogy K osztályszáma 1, ezért az 5.2. lemma (i) és a 3.13. következmény miatt feltehetjük, hogy E K felett van definiálva egy (2.2) Weierstraß egyenlettel. Tehát 5.2. lemma (iii) miatt $\Theta_{E,\mathfrak{a}} \in K(E)$.

Tegyük fel, hogy $x \in \prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^{\times} \subset \mathbf{A}_K^{\times}$ és $x \equiv 1 \pmod{\mathfrak{b}}$, illetve legyen $\sigma_x = [x, K^{\text{ab}}/K]$. A 3.14. tétel szerint $\psi(x) \in \mathcal{O}^{\times} = \text{Aut}(E)$ és $\sigma_x Q = \psi(x)Q$, tehát

$$\Theta_{E,\mathfrak{a}}(Q)^{\sigma_x} = \Theta_{E,\mathfrak{a}}(Q^{\sigma_x}) = \Theta_{E,\mathfrak{a}}(\psi(x)Q) = \Theta_{E,\mathfrak{a}}(Q),$$

ahol az első egyenlőség azért van, mert $\Theta_{E,\mathfrak{a}}$ K felett definiált, a harmadik pedig az 5.2. lemma (ii) része miatt. Osztálytestelméletből következik, hogy a σ_x -ek generálják $\text{Gal}(\bar{K}/K(\mathfrak{b}))$ -t, azaz $\Theta_{E,\mathfrak{a}}(Q)$ -t fixálja, vagyis (i) kész van.

Tegyük fel, hogy $x \in \mathbf{A}_K^{\times}$ idèle olyan, hogy $x\mathcal{O} = \mathfrak{c}$ és $x_{\mathfrak{p}} = 1$ minden olyan $\mathfrak{p}$ prímre, ami osztja $\mathfrak{b}$ -t. Ekkor a 3.14.tétel szerint $\psi(x) \in c\mathcal{O}^{\times}$ és $\sigma_{\mathfrak{c}}Q = \psi(x)Q$. Megint az 5.2. lemma (ii) részét használva

$$\Theta_{E,\mathfrak{a}}(Q)^{\sigma_{\mathfrak{c}}} = \Theta_{E,\mathfrak{a}}(\psi(x)Q) = \Theta_{E,\mathfrak{a}}(cQ).$$

Ez a (ii).

Legyen $\mathfrak{p}$ egy prímje K -nak, aminek $\mathfrak{b}$ nem a hatványa. A 3.20. következmény és az 5.2. lemma miatt feltehető, hogy E Weierstraß egyenletének sima redukciója van $\mathfrak{p}$ -ben. Vagyis ez azt jelenti, hogy $\Delta(E)$ és $\mathfrak{p}$ relatív prímek. Legyen $n = \text{ord}_{\mathfrak{p}}(\mathfrak{a})$. Ekkor

$$\begin{aligned} \text{ord}_{\mathfrak{p}}(\Theta_{E,\mathfrak{a}}(Q)) = -12n - 6 \sum_{P \in E[\mathfrak{a}] - E[\mathfrak{p}^n]} \text{ord}_{\mathfrak{p}}(x(Q) - x(P)) - \\ - 6 \sum_{P \in E[\mathfrak{p}^n] - \mathcal{O}} \text{ord}_{\mathfrak{p}}(x(Q) - x(P)) \end{aligned} \quad (5.1)$$

Használjuk az 5.3. lemmát. Ha P rendje $\mathfrak{p}^m$ valamilyen $m > 0$ -ra, akkor

$$\text{ord}_{\mathfrak{p}}(x(P)) = -2/\mathbf{N}\mathfrak{p}^{m-1}(\mathbf{N}\mathfrak{p} - 1) \text{ és } \text{ord}_{\mathfrak{p}}(x(Q)) \geq 0.$$

Ha P rendje nem $\mathfrak{p}$ -hatvány, akkor $P \pm Q$ rendje sem lehet $\mathfrak{p}$ -hatvány, tehát ahogy az 5.3. lemmában, $\text{ord}_{\mathfrak{p}}(x(Q) - x(P)) = 0$. Vagyis

$$\text{ord}_{\mathfrak{p}}(x(Q) - x(P)) = \begin{cases} -\frac{2}{\mathbf{N}\mathfrak{p}^m - \mathbf{N}\mathfrak{p}^{m-1}}, & \text{ha } P \text{ rendje } \mathfrak{p}^m, m > 0 \\ 0, & \text{ha } P \text{ rendje nem } \mathfrak{p}\text{-hatvány.} \end{cases}$$

(5.1)-be beírva látjuk, hogy az első szumma 0, a második szummában pedig a $\mathfrak{p}^m$ -rendű pontok éppen $E[\mathfrak{p}^m] - E[\mathfrak{p}^{m-1}]$ pontjai, tehát $\mathbf{N}\mathfrak{p}^m - \mathbf{N}\mathfrak{p}^{m-1}$ darab van belőle, azaz a második szumma n darab -2 összege. Tehát $\text{ord}_{\mathfrak{p}}(\Theta_{E,\mathfrak{a}}(Q)) = 0$, amiből következik (iii). $\square$

5.5. Lemma. *A $\Theta_{E,\mathfrak{a}}$ racionális függvény divizora*

$$12\mathbf{N}\mathfrak{a}[O] - 12 \sum_{P \in E[\mathfrak{a}]} [P].$$

Bizonyítás. Az $x - x(P)$ függvénynek E -n legfeljebb 2 gyöke lehet, ami van is: P és $-P$ (ld. [Sil09] III. 2.3 (a)). Multiplikatíván számolva ugyanannyi gyöke és pólusa van $(x - x(P))$ -nek (ld. [Sil09] II. 3.1 (b) állítás), pólusa pedig csak O -ban lehet, tehát $x - x(P)$ divizora $[P] + [-P] - 2[O]$. Ebből következik az állítás. $\square$

5.6. Tétel. *Tegyük fel, hogy $\mathfrak{b}$ egy $\mathfrak{a}$ -hoz relatív prím ideálja $\mathcal{O}$ -nak és β egy generátora $\mathfrak{b}$ -nek. Ekkor minden $P \in E(\bar{K})$ pontra*

$$\prod_{R \in E[\mathfrak{b}]} \Theta_{E,\mathfrak{a}}(P + R) = \Theta_{E,\mathfrak{a}}(\beta P).$$

Bizonyítás. Mindkét oldal K felett definiált racionális függvény E -n az 5.2. lemma (iii) része szerint. Számoljuk ki a divizorukat, felhasználva az 5.5. lemmát.

$$\begin{aligned} \text{div} \left(\prod_{R \in E[\mathfrak{b}]} \Theta_{E,\mathfrak{a}}(P + R) \right) &= \sum_{R \in E[\mathfrak{b}]} \text{div}(\Theta_{E,\mathfrak{a}}(P + R)) = \\ &= \sum_{R \in E[\mathfrak{b}]} (12\mathbf{N}\mathfrak{a}[-R] - 12 \sum_{Q \in E[\mathfrak{a}]} [Q - R]) = 12\mathbf{N}\mathfrak{a} \sum_{R \in E[\mathfrak{b}]} [-R] - 12 \sum_{R \in E[\mathfrak{b}]} \sum_{Q \in E[\mathfrak{a}]} [Q - R] = \\ &= 12\mathbf{N}\mathfrak{a} \sum_{R \in E[\mathfrak{b}]} [R] - 12 \sum_{R \in E[\mathfrak{b}]} \sum_{Q \in E[\mathfrak{a}]} [Q + R], \end{aligned}$$

mert $-R \in E[\mathfrak{b}] \Leftrightarrow R \in E[\mathfrak{b}]$. Illetve

$$\text{div}(\Theta_{E,\mathfrak{a}}(\beta P)) = 12\mathbf{N}\mathfrak{a} \sum_{P \in E[\mathfrak{b}]} [P] - 12 \sum_{P \in E[\mathfrak{a}\mathfrak{b}]} [P],$$

mert $\beta P = O \Leftrightarrow P \in E[\mathfrak{b}]$ és $\beta P \in E[\mathfrak{a}] \Leftrightarrow \alpha\beta P = 0 \Leftrightarrow P \in E[\mathfrak{a}\mathfrak{b}]$. A két divizor megegyezik, mivel a 3.3. állítás és a kínai maradéktétel szerint $E[\mathfrak{a}\mathfrak{b}] \cong E[\mathfrak{a}] \times E[\mathfrak{b}]$.

Tehát a két racionális függvény hányadosa egy konstans $\lambda \in K^\times$ [Sil09] II. 3.1 (a) része szerint. Legyen $w_K = \#(\mathcal{O}^\times)$ és számítsuk ki a két függvény hányadosát a $P = O$ pontban. Szükség van a $\Theta_{E,\mathfrak{a}}(P)/\Theta_{E,\mathfrak{a}}(\beta P)$ értékére a $P = O$ pontban.

$$\frac{\Theta_{E,\mathfrak{a}}(P)}{\Theta_{E,\mathfrak{a}}(\beta P)} = \prod_{Q \in E[\mathfrak{a}] - O} \left(\frac{x(P) - x(Q)}{x(\beta P) - x(Q)} \right)^{-6}$$

Ha használjuk a 2.18. tétel azonosítását, akkor

$$\lim_{z \rightarrow 0} \frac{\wp(z) - \wp(w)}{\wp(\beta z) - \wp(w)}$$

értékét kell kiszámolnunk valamilyen $w \notin L$ pontra (ez felel meg Q -nak). [Sil09] III. 3.5 tétel szerint $\wp(z)$ Laurent sora $z = 0$ -ban

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1)G_{2k+2}z^{2k},$$

tehát

$$\lim_{z \rightarrow 0} \frac{\wp(z) - \wp(w)}{\wp(\beta z) - \wp(w)} = \lim_{z \rightarrow 0} \frac{1 + \sum_{k=1}^{\infty} (2k+1)G_{2k+2}z^{2k+2} - \wp(w)z^2}{\beta^{-2} + \sum_{k=1}^{\infty} (2k+1)G_{2k+2}\beta^{2k}z^{2k+2} - \wp(w)z^2} = \beta^2.$$

Azaz $\Theta_{E,\mathfrak{a}}(P)/\Theta_{E,\mathfrak{a}}(\beta P)$ a $P = O$ pontban $\beta^{-12(\mathbf{N}\mathfrak{a}-1)}$. Már könnyű kiszámolni, hogy

$$\lambda = \beta^{-12(\mathbf{N}\mathfrak{a}-1)} \prod_{R \in E[\mathfrak{b}] - O} \Theta_{E,\mathfrak{a}}(R) = \frac{\Delta(E)^{(\mathbf{N}\mathfrak{a}-1)(\mathbf{N}\mathfrak{b}-1)}}{\alpha^{12(\mathbf{N}\mathfrak{b}-1)}\beta^{12(\mathbf{N}\mathfrak{a}-1)}} \prod_{\substack{R \in E[\mathfrak{b}] \\ R \neq O}} \prod_{\substack{P \in E[\mathfrak{a}] \\ P \neq O}} (x(R) - x(P))^{-6}$$

Legyen

$$\mu = \frac{\Delta(E)^{(\mathbf{N}\mathfrak{a}-1)(\mathbf{N}\mathfrak{b}-1)/w_K}}{\alpha^{12(\mathbf{N}\mathfrak{b}-1)/w_K}\beta^{12(\mathbf{N}\mathfrak{a}-1)/w_K}} \prod (x(R) - x(P))^{-12/w_K},$$

ahol a szorzat az $R \in E[\mathfrak{b}] - O$ és $P \in (E[\mathfrak{a}] - O)/\pm 1$ pontpárokon fut végig, mert $x(P) = x(-P)$ és $\mathfrak{a}$ relatív prím 6-hoz, a kitevők pedig jóldefiniált egész számok, mert w_K a 12 osztója. Teljesül $\mu^{w_K} = \lambda$. Ugyanúgy bizonyítható, hogy $\mu \in \mathcal{O}^\times$, mint az 5.4. tétel (iii) része. Tehát $\lambda = 1$ Lagrange véges csoportokra vonatkozó tétele miatt. $\square$

5.7. Következmény. Tegyük fel, hogy $\mathfrak{b}$ egy $\mathfrak{a}$ -hoz relatív prím ideálja $\mathcal{O}$ -nak, $Q \in E[\mathfrak{b}]$ rendje $\mathfrak{b}$, $\mathfrak{p}$ egy $\mathfrak{b}$ -t osztó prím, π egy generátora $\mathfrak{p}$ -nek, $\mathfrak{b}' = \mathfrak{b}/\mathfrak{p}$ szintén ideálja $\mathcal{O}$ -nak. Ha $\mathcal{O}^\times \rightarrow (\mathcal{O}/\mathfrak{b}')^\times$ injektív, akkor

$$N_{K(\mathfrak{b})/K(\mathfrak{b}')} \Theta_{E,\mathfrak{a}}(Q) = \begin{cases} \Theta_{E,\mathfrak{a}}(\pi Q) & \text{ha } \mathfrak{p} \mid \mathfrak{b}' \\ \Theta_{E,\mathfrak{a}}(\pi Q)^{1 - \text{Frob}_{\mathfrak{p}}^{-1}} & \text{ha } \mathfrak{p} \nmid \mathfrak{b}' \end{cases}$$

ahol $\text{Frob}_{\mathfrak{p}}$ a $\mathfrak{p}$ -hez tartozó Frobenius $\text{Gal}(K(\mathfrak{b}')/K)$ -ban.

Bizonyítás. [Rub99] 7.7 következmény. $\square$

5.2. Elliptikus görbék K felett

Legyen mostantól E K felett definiált, $\mathfrak{a}$ relatív prím $6\mathfrak{f}$ -hez. Jelöljük egy $P \in E(\bar{K})$ pontra τ_P -vel a P -vel való eltolást E -n. Tehát τ_P egy racionális függvény a $K(P)$ test fölött.

Rögzítsünk egy $S \in E[\mathfrak{f}]$ $\mathcal{O}$ -generátort. Ekkor $S \in E(K(\mathfrak{f}))$ a 3.19. következmény (i) része miatt ($\mathfrak{a} = \mathcal{O}$ választással) és legyen

$$\Lambda_{E,\mathfrak{a}} = \Lambda_{E,\mathfrak{a},S} = \prod_{\sigma \in \text{Gal}(K(\mathfrak{f})/K)} \Theta_{E,\mathfrak{a}} \circ \tau_{S^\sigma}.$$

5.8. Állítás. (i) $\Lambda_{E,\mathfrak{a}}$ racionális függvény K felett definiált.

(ii) Ha B ideálok egy halmaza $\mathcal{O}$ -ban, amik relatív prímek $\mathfrak{a}\mathfrak{f}$ -hez és a $\mathfrak{b} \mapsto [\mathfrak{b}, K(\mathfrak{f})/K]$ Artin leképezés bijekció B és $\text{Gal}(K(\mathfrak{f})/K)$ között, akkor

$$\Lambda_{E,\mathfrak{a}}(P) = \prod_{\mathfrak{b} \in B} \Theta_{E,\mathfrak{a}}(\psi(\mathfrak{b})S + P).$$

(iii) Ha $\mathfrak{r}$ egy ideálja $\mathcal{O}$ -nak és $Q \in E[\mathfrak{r}]$, $Q \notin E[\mathfrak{f}]$, akkor $\Lambda_{E,\mathfrak{a}}(Q)$ egy globális egység $K(E[\mathfrak{r}])$ -ben.

Bizonyítás. (i) triviális, (ii) közvetlenül következik a 3.15. következmény (ii) részéből és (iii) pedig következik az 5.4. tétel (iii) részéből. $\square$

5.3. Értelmezés a tóruszon

Továbbra is legyen E K felett definiált. Rögzítsük E egy K feletti Weierstraß egyenletét. Legyen $L \subset \mathbb{C}$ rács, amit a 2.18. tétel (ii) része ad. Ekkor $\mathcal{O}L = L$ (2.20. állítás), tehát létezik $\Omega \in \mathbb{C}^\times$, amire $L = \Omega\mathcal{O}$. A $\xi(z) = (\wp(z; L), \wp'(z; L)/2)$ egy $\mathbb{C}/L \xrightarrow{\sim} E(\mathbb{C})$ izomorfizmus. Definiáljuk $\Theta_{L,\mathfrak{a}} = \Theta_{E,\mathfrak{a}} \circ \xi$ -t:

$$\Theta_{L,\mathfrak{a}}(z) = \alpha^{-12} \Delta(L)^{\mathbf{N}\mathfrak{a}-1} \prod_{u \in \mathfrak{a}^{-1}L/L-0} (\wp(z; L) - \wp(u; L))^{-6}.$$

5.9. Definíció. Legyenek

$$A(L) = \pi^{-1} \text{area}(\mathbb{C}/L),$$

$$s_2(L) = \lim_{s \rightarrow 0+} \sum_{0 \neq \omega \in L} \omega^{-2} |\omega|^{-2s},$$

$$\eta(z; L) = A(L)^{-1} \bar{z} + s_2(L)z,$$

$$\theta(z; L) = \Delta(L) e^{-6\eta(z; L)z} \sigma(z; L)^{12}.$$

($\Delta(L)$ -hez ld. 2.19. definíció, $\sigma(z; L)$ -hez ld. 2.17. definíció.)

5.10. Lemma. $\Theta_{L,\mathfrak{a}}(z) = \frac{\theta(z; L)^{\mathbf{N}\mathfrak{a}}}{\theta(z; \mathfrak{a}^{-1}L)}.$

Bizonyítás. Ld. [Rub99] 7.10 lemma. A bizonyítás gondolatmenete, hogy

$$\mathbf{N}\mathfrak{a} \cdot A(L)^{-1} = A(\mathfrak{a}^{-1}L)^{-1}$$

miatt $\theta(z; L)^{\mathbf{N}\mathfrak{a}}/\theta(z; \mathfrak{a}^{-1}L)$ holomorf függvény, sőt periodikus L szerint és divizora $\mathbb{C}/L$ -en $12\mathbf{N}\mathfrak{a}[0] - 12 \sum_{v \in \mathfrak{a}^{-1}L/L} [v]$. Vagyis csak konstanszorosban térhet el $\Theta_{L,\mathfrak{a}}$ -tól. Azonban mindkét függvénynek a Laurent sora a $z = 0$ -ban $\alpha^{-12} \Delta(L)^{\mathbf{N}\mathfrak{a}-1} z^{12(\mathbf{N}\mathfrak{a}-1)}$ -vel kezdődik. $\square$

5.11. Definíció. Definiáljuk $k \geq 1$ -re az *Eisenstein sorokat*:

$$E_k(z; L) = \lim_{s \rightarrow k} \sum_{\omega \in L} \frac{(\bar{z} + \bar{\omega})^k}{|z + \omega|^{2s}},$$

ahol a limesz azt jelenti, hogy az analitikus folytatását értékeljük ki $s = k$ -ban. Ha $k \geq 3$, akkor

$$E_k(z; L) = \sum_{\omega \in L} \frac{1}{(z + \omega)^k}$$

teljesül.

5.12. Állítás. $E_1(z; L) = \log(\sigma(z; L))' - s_2(L)z - A(L)^{-1}\bar{z}$,

$$E_2(z; L) = \wp(z; L) + s_2(L),$$

$$E_k(z; L) = \frac{(-1)^k}{(k-1)!} \left(\frac{d}{dz}\right)^{(k-2)} \wp(z; L) \quad \text{ha } k \geq 3.$$

Bizonyítás. Az első kettőhöz ld. [CW77] 242-243. oldal. A harmadik következik $\wp(z; L)$ definíciójából indukcióval. $\square$

5.13. Tétel. Minden $k \geq 1$ -re

$$\left(\frac{d}{dz}\right)^k \log \Theta_{L,\mathfrak{a}}(z) = 12(-1)^{k-1}(k-1)!(\mathbf{N}\mathfrak{a}E_k(z; L) - E_k(z; \mathfrak{a}^{-1}L)).$$

Bizonyítás. Az 5.10. lemmát használva

$$\log(\Theta_{L,\mathfrak{a}}(z)) = \mathbf{N}\mathfrak{a} \log(\theta(z; L)) - \log(\theta(z; \mathfrak{a}^{-1}L)). \quad (5.2)$$

A θ és η definíciója szerint

$$\begin{aligned} \log(\theta(z; L)) &= \log(\Delta(L) - 6\eta(z; L)z + 12\log(\sigma(z; L))) = \\ &= \log(\Delta(L)) - 6A(L)^{-1}z\bar{z} - 6s_2(L)z^2 + 12\log(\sigma(z; L)), \end{aligned}$$

tehát

$$\frac{d}{dz} \log(\theta(z; L)) = -6A(L)^{-1}\bar{z} - 12s_2(L)z + 12\log(\theta(z; L))' = 12E_1(z; L) + 6A(L)^{-1}\bar{z}$$

az 5.12. állítás szerint. Hasonlóan

$$\frac{d}{dz} \log(\theta(z; \mathfrak{a}^{-1}L)) = 12E_1(z; \mathfrak{a}^{-1}L) + 6A(\mathfrak{a}^{-1}L)^{-1}\bar{z}.$$

Mivel $\mathbf{N}\mathfrak{a} = \alpha \cdot \bar{\alpha} = |\alpha|^2$, ezért $\mathbf{N}\mathfrak{a} \cdot A(\mathfrak{a}^{-1}L) = A(L)$, tehát (5.2) deriváltjába beírva az előbb kiszámoltakat az A -t tartalmazó tagok éppen kiesnek és $k = 1$ -re megkapjuk a tételt.

[Sil09] VI. 3.3 lemma (b) része szerint $\left(\frac{d}{dz}\right)^2 \log(\sigma(z; L)) = -\wp(z; L)$, tehát

$$\frac{d}{dz} E_k(z; L) = -kE_{k+1}(z; L)$$

teljesül minden $k \geq 1$ -re az 5.12. állítás miatt. Innen már indukcióval következik a tétel állítása minden $k \geq 1$ -re. $\square$

5.4. A Hecke L -függvény

5.14. Definíció. Defináljuk minden $k \geq 1$ -re a Hecke L -függvényét $\bar{\psi}^k$ -nak, mint a következő Dirichlet-sor analitikus folytatása:

$$L(\bar{\psi}^k, s) = \sum \frac{\bar{\psi}^k(\mathfrak{b})}{\mathbf{N}\mathfrak{b}^s},$$

ahol az összegzés a $\bar{\psi}^k$ konduktorához relatív prím $\mathfrak{b}$ ideáljain fut végig $\mathcal{O}$ -nak. Ha $\mathfrak{m}$ ideálja $\mathcal{O}$ -nak, amit oszt $\mathfrak{f}$ és $\mathfrak{c}$ pedig egy $\mathfrak{m}$ -hez relatív prím ideál, akkor definiáljuk $L_{\mathfrak{m}}(\bar{\psi}^k, s, \mathfrak{c})$ -t ugyanezzel a képlettel, viszont megszorítva továbbá azokra az ideálokra, amik relatív prímei $\mathfrak{m}$ -hez és $[\mathfrak{b}, K(\mathfrak{m})/K] = [\mathfrak{c}, K(\mathfrak{m})/K]$.

Legyen $\Omega \in \mathbb{C}^\times$, amire $L = \Omega\mathcal{O}$.

5.15. Állítás. Tegyük fel, hogy $v \in KL$ rendje KL/L -ben $\mathfrak{m}$, ahol $\mathfrak{f} \mid \mathfrak{m}$. Ekkor minden $k \geq 1$ -re

$$E_k(v; L) = v^{-k} \psi(\mathfrak{c})^k L_{\mathfrak{m}}(\bar{\psi}^k, k, \mathfrak{c}),$$

ahol $\mathfrak{c} = \Omega^{-1}v\mathfrak{m}$.

Bizonyítás. Legyen μ egy generátora $\mathfrak{m}$ -nek, tehát $v = \alpha\Omega/\mu$ valamilyen $\alpha \in \mathcal{O}$ -val, ami relatív prím $\mathfrak{m}$ -hez. A $\beta = \alpha + \mu\omega/\Omega \in \mathcal{O}$ ($\omega \in L$) jelöléssel elég nagy s -re (hogy a sorok konvergensek legyenek)

$$\sum_{\omega \in L} \frac{(\bar{v} + \bar{\omega})^k}{|v + \omega|^{2s}} = \frac{\mathbf{N}\mu^s}{\bar{\mu}^k} \frac{\bar{\Omega}^k}{|\Omega|^{2s}} \sum_{\substack{\beta \in \mathcal{O} \\ \beta \equiv \alpha \pmod{\mathfrak{m}}}} \frac{\bar{\beta}^k}{|\beta|^{2s}}.$$

A 3.15. következmény (i) szerint $\psi(\beta\mathcal{O})$ és β ugyanazt az ideált generálja $\mathcal{O}$ -ban, tehát hányadosuk egység. Definiáljuk az

$$\epsilon(\beta) = \frac{\psi(\beta\mathcal{O})}{\beta},$$

ami így egy multiplikatív leképezést ad $\{\beta \in \mathcal{O} : \beta \text{ relatív prím } \mathfrak{f}\text{-hez}\}$ -ről $\mathcal{O}^\times$ -be. ψ konduktorának definíciója szerint ϵ keresztülvezethető $(\mathcal{O}/\mathfrak{f})^\times$ -en az

$$\hat{\epsilon} : (\mathcal{O}/\mathfrak{f})^\times \rightarrow \mathcal{O}^\times, \quad \hat{\epsilon}(\beta + \mathfrak{f}) = \epsilon(\beta)$$

képlettel. Tehát $\alpha \equiv \beta \pmod{\mathfrak{m}}$ esetén

$$\bar{\beta} = \bar{\psi}(\beta\mathcal{O}) \frac{\psi(\alpha\mathcal{O})}{\alpha},$$

mert $\mathcal{O}^\times$ elemei egység-hosszúak. Írjuk be az előző szummába

$$\sum_{\substack{\beta \in \mathcal{O} \\ \beta \equiv \alpha \pmod{\mathfrak{m}}}} \frac{\bar{\beta}^k}{|\beta|^{2s}} = \frac{\psi(\alpha\mathcal{O})^k}{\alpha^k} \sum_{\substack{\mathfrak{b} \in \mathcal{O}, \\ [\mathfrak{b}, K(\mathfrak{m})/K] = [\alpha\mathcal{O}, K(\mathfrak{m})/K]}} \frac{\bar{\psi}(\mathfrak{b})^k}{\mathbf{N}\mathfrak{b}^s}$$

Definíció szerint $\mathfrak{c} = \Omega^{-1}v\mathfrak{m} = \Omega^{-1}\alpha\Omega\mathfrak{m}/\mu = \alpha\mathcal{O}$. Összerakva mindent

$$\lim_{s \rightarrow k} \sum_{\omega \in L} \frac{(\bar{v} + \bar{\omega})^k}{|v + \omega|^{2s}} = \lim_{s \rightarrow k} \frac{\mathbf{N}\mu^s}{\bar{\mu}^k} \frac{\bar{\Omega}^k}{|\Omega|^{2s}} \frac{\psi(\mathfrak{c})^k}{\alpha^k} L_{\mathfrak{m}}(\bar{\psi}^k, s, \mathfrak{c}) = v^{-k} \psi(\mathfrak{c})^k L_{\mathfrak{m}}(\bar{\psi}^k, k, \mathfrak{c}).$$

□

5.16. Definíció. Rögzítsük $\mathfrak{f}$ egy f generátorát és egy B halmazát $\mathcal{O}$ ideáljainak, amik $\mathfrak{a}\mathfrak{f}$ -hez relatív prímekek úgy, hogy a $\mathfrak{b} \mapsto [\mathfrak{b}, K(\mathfrak{f})/K]$ Artin leképezés bijekció B és $\text{Gal}(K(\mathfrak{b})/K)$ között. Legyen $u = \Omega/f \in \mathfrak{f}^{-1}L$ és definiáljuk a

$$\Lambda_{L,\mathfrak{a}}(z) = \Lambda_{L,\mathfrak{a},f}(z) = \Lambda_{L,\mathfrak{a},\xi(u)}(\xi(z)) = \prod_{\mathfrak{b} \in B} \Theta_{L,\mathfrak{a}}(\psi(\mathfrak{b})u + z)$$

függvényt. Az 5.8. állítás (ii) része miatt $\Lambda_{L,\mathfrak{a}} = \Lambda_{E,\mathfrak{a}} \circ \xi$.

5.17. Tétel. Minden $k \geq 1$ -re

$$\left(\frac{d}{dz}\right)^k \log \Lambda_{L,\mathfrak{a}}(z) \big|_{z=0} = 12(-1)^{k-1}(k-1)! f^k(\mathbf{N}\mathfrak{a} - \psi(\mathfrak{a})^k) \Omega^{-k} L(\bar{\psi}^k, k).$$

Bizonyítás. Használjuk az 5.13. tételt

$$\begin{aligned} \left(\frac{d}{dz}\right)^k \log \Lambda_{L,\mathfrak{a}}(z) \big|_{z=0} &= \sum_{\mathfrak{b} \in B} \left(\frac{d}{dz}\right)^k \log \Theta_{L,\mathfrak{a}}(z) \big|_{z=\psi(\mathfrak{b})u} = \\ &= 12(-1)^{k-1}(k-1)! \left(\mathbf{N}\mathfrak{a} \sum_{\mathfrak{b} \in B} E_k(\psi(\mathfrak{b})u; L) - \sum_{\mathfrak{b} \in B} E_k(\psi(\mathfrak{b})u; \mathfrak{a}^{-1}L) \right). \end{aligned} \quad (5.3)$$

Használjuk az 5.15. állítást is. Mivel $\psi(\mathfrak{b})u$ rendje $\mathfrak{f}$ KL/L -bn és a 3.15. következmény (i) része miatt $\psi(\mathfrak{b})\mathcal{O} = \mathfrak{b}$, ezért $E_k(\psi(\mathfrak{b})u; L) = (\psi(\mathfrak{b})u)^{-k} \psi(\mathfrak{b})^k L_{\mathfrak{f}}(\bar{\psi}^k, k, \mathfrak{b})$. Összeadva

$$\sum_{\mathfrak{b} \in B} E_k(\psi(\mathfrak{b})u; L) = \sum_{\mathfrak{b} \in B} u^{-k} L_{\mathfrak{f}}(\bar{\psi}^k, k, \mathfrak{b}) = u^{-k} L(\bar{\psi}^k, k).$$

Az Eisenstein sorok definíciójából és $\psi(\mathfrak{a})\mathcal{O} = \mathfrak{a}$ miatt $E_k(z; \mathfrak{a}^{-1}L) = \psi(\mathfrak{a})^k E_k(\psi(\mathfrak{a})z; L)$. Ezt használva

$$\sum_{\mathfrak{b} \in B} E_k(\psi(\mathfrak{b})u; \mathfrak{a}^{-1}L) = \psi(\mathfrak{a})^k \sum_{\mathfrak{b} \in B} E_k(\psi(\mathfrak{a})\psi(\mathfrak{b})u; L) = u^{-k} \psi(\mathfrak{a})^k L(\bar{\psi}^k, k).$$

Beírva a két összegre kiszámoltakat (5.3)-ba kapjuk az állítást. □

5.18. Következmény (Damerell tétele). Minden $k \geq 1$ -re

$$\Omega^{-k} L(\bar{\psi}^k, k) \in K.$$

Bizonyítás. Az 5.8. állítás (i) része szerint $\Lambda_{L,\mathfrak{a}} \in K(\wp(z; L), \wp'(z; L))$, azaz racionális függvénye $\wp(z; L)$ -nek és $\wp'(z; L)$ -nek K -beli együtthatókkal. A 2.18. tétel szerint teljesül az ottani jelölésekkel

$$\wp'(z; L)^2 = 4\wp(z; L)^3 + 4a\wp(z; L) + 4b.$$

Deriválva az összefüggést és indukciót használva látszik, hogy az egyre nagyobb deriváltak csak a bal oldalon jelennek meg és első hatványon, tehát mindig átrendezve az egyenlőséget $\wp^{(k)}(z; L) \in K(\wp(z; L), \wp'(z; L), \dots, \wp^{(k-1)}(z; L))$, amiből következik, hogy $\wp^{(k)}(z; L) \in K(\wp(z; L), \wp'(z; L))$. Tehát szintén $\Lambda_{L,\mathfrak{a}}^{(k)} \in K(\wp(z; L), \wp'(z; L))$, és így $\left(\frac{d}{dz}\right)^k \log \Lambda_{L,\mathfrak{a}}(z) \in K(\wp(z; L), \wp'(z; L))$, amiből az 5.17. tételt használva következik Damerell tétele. □

5.5. $\mathfrak{p}$ -adikus értelmezés

Rögzítsük K egy $\mathfrak{p}$ prímjét, aminél E -nek sima redukciója van, $\mathfrak{p} \nmid 6$. Tegyük fel, hogy a választott Weierstraß egyenletünkre $\mathfrak{p} \nmid \Delta(E)$ és $\mathfrak{a}$ relatív prím $\mathfrak{p}$ -hez és $6\mathfrak{f}$ -hez is. Legyen $\hat{E}$ az E -hez rendelt formális csoport $\mathcal{O}_{\mathfrak{p}}$ felett. (Azaz $K_{\mathfrak{p}}$ egészeinek gyűjűje.) Legyenek továbbá $x(Z), y(Z) \in \mathcal{O}_{\mathfrak{p}}[[Z]]$ a 2.28. tétel hatványsorai.

5.19. Definíció. Legyen $\lambda_{\hat{E}}(Z) \in Z + Z^2 K_{\mathfrak{p}}[[Z]]$ a 2.31. definíció logaritmus függvénye. Tehát $\lambda'_{\hat{E}}(Z) \in \mathcal{O}_{\mathfrak{p}}[[Z]]^{\times}$. Defináljuk a következő operátort $\mathcal{O}_{\mathfrak{p}}[[Z]]$ -n:

$$D = \frac{1}{\lambda'_{\hat{E}}(Z)} \frac{d}{dZ}.$$

5.20. Állítás. Az (x, y) pont megfeleltetése $(\wp(z; L), \frac{1}{2}\wp'(z; L))$ -nek, illetve $(x(Z), y(Z))$ -nek a következő kommutatív diagramot adja:

$$\begin{array}{ccccccc} K(\wp(z), \wp'(z)) & \xleftarrow{\sim} & K(E) & \xrightarrow{\sim} & K(x(Z), y(Z)) & \hookrightarrow & K_{\mathfrak{p}}((Z)) \\ \frac{d}{dz} \downarrow & & \downarrow & & \downarrow D & & \downarrow D \\ K(\wp(z), \wp'(z)) & \xleftarrow{\sim} & K(E) & \xrightarrow{\sim} & K(x(Z), y(Z)) & \hookrightarrow & K_{\mathfrak{p}}((Z)). \end{array}$$

Bizonyítás. Mivel minden függőleges leképezés deriválás, ezért elég belátni, hogy $\frac{d}{dz}\wp(z)$ és $D(x(Z))$, illetve $\frac{d}{dz}\wp'(z)$ és $D(y(Z))$ egymás megfelelői. A 2.18. tétel szerint teljesül

$$\wp'(z)^2 = 4\wp(z)^3 + 4a\wp(z) + b.$$

Deriválva az összefüggést

$$2\wp'(z)\wp''(z) = 12\wp(z)^2\wp'(z) + 4a\wp'(z),$$

amiből

$$\wp''(z) = 6\wp(z)^2 + 2a.$$

A $K(\wp(z), \wp'(z))$ testben tehát teljesül

$$\frac{d}{dz}\wp(z) = 2 \cdot \frac{1}{2}\wp'(z) \text{ és } \frac{d}{dz}\left(\frac{1}{2}\wp'(z)\right) = 3\wp(z)^2 + a,$$

vagyis azt kell ellenőrizni, hogy $K(x(Z), y(Z))$ -ben teljesül

$$D(x(Z)) = 2y(Z) \text{ és } D(y(Z)) = 3x(Z)^2 + a.$$

Az első triviálisan következik a definíciókból, mert $\lambda'_{\hat{E}}(Z) = (\frac{d}{dZ}x(Z))/2y(Z)$, tehát

$$D(x(Z)) = \frac{1}{\lambda'_{\hat{E}}} \frac{d}{dZ}x(Z) = 2y(Z).$$

A második pedig következik abból, hogy $x(Z)$ és $y(Z)$ is teljesíti az $y^2 = x^3 + ax + b$ egyenletet, tehát

$$y(Z)^2 = x(Z)^3 + ax(Z) + b,$$

amire alkalmazva D -t

$$2y(Z)D(y(Z)) = 3x(Z)^2D(x(Z)) + aD(x(Z)).$$

Behelyettesítve $D(x(Z)) = 2y(Z)$ -t

$$2y(Z)D(y(Z)) = 6x(Z)^2y(Z) + 2ay(Z),$$

amit osztva $2y(Z)$ -vel

$$D(y(Z)) = 3x(Z)^2 + a.$$

□

5.21. Definíció. Legyen $\Lambda_{\mathfrak{p},\mathfrak{a}}(Z)$ a $\Lambda_{E,\mathfrak{a}}$ képe a 5.20. állítás felső soránál.

5.22. Tétel. (i) $\Lambda_{\mathfrak{p},\mathfrak{a}}(Z) \in \mathcal{O}_{\mathfrak{p}}[[Z]]^{\times}$.

(ii) Minden $k \geq 1$ -re

$$D^k \log(\Lambda_{\mathfrak{p},\mathfrak{a}}(Z))|_{Z=0} = 12(-1)^{k-1}(k-1)! f^k(\mathbf{N}\mathfrak{a} - \psi(\mathfrak{a})^k) \Omega^{-k} L(\bar{\psi}^k, k).$$

Bizonyítás. Rögzítsünk egy $\bar{K} \hookrightarrow \bar{K}_{\mathfrak{p}}$ beágyazást, hogy $R \in E[\mathfrak{f}]$ pontra értelmezhesük $x(R) \in \bar{K}_{\mathfrak{p}}$. Jelölje $\bar{K}_{\mathfrak{p}}$ egészeinek gyűrűjét $\mathcal{R}$.

Tekintsük az 5.8. állítás (ii) részénél lévő egyik $x(\psi(\mathfrak{b})S + P) - x(Q)$ tagot, ahol $Q \in E[\mathfrak{a}] - \mathcal{O}$. Írjuk fel az explicit képletet az x -koordinátára (ld. [Sil09] III. 2.3)

$$x(\psi(\mathfrak{b})S + P) - x(Q) = \frac{(y(P) - y(\psi(\mathfrak{b})S))^2}{(x(P) - x(\psi(\mathfrak{b})S))^2} - x(P) - x(\psi(\mathfrak{b})S) - x(Q).$$

Az 5.3. lemma (ii) szerint $\text{ord}_{\mathfrak{p}}(x(Q)) \geq 0$, mert $\mathfrak{a}$ és $\mathfrak{p}$ relatív prímekek és hasonlóan $\text{ord}_{\mathfrak{p}}(x(\psi(\mathfrak{b})S)) \geq 0$, mert S egy $\mathcal{O}$ -generátora $E[\mathfrak{f}]$ -nek. Illetve a 2.26. lemma miatt $\text{ord}_{\mathfrak{p}}(y(\psi(\mathfrak{b})S)) \geq 0$. Tehát $x(\psi(\mathfrak{b})S), y(\psi(\mathfrak{b})S), x(Q) \in \mathcal{R}$. Helyettesítsük be $x(P)$ és $y(P)$ helyére $x(Z)$ -t és $y(Z)$ -t. Ez ad egy

$$x(\psi(\mathfrak{b})S + P) \mapsto g_{\mathfrak{b},Q}(Z) \in \mathcal{R}[[Z]]$$

hozzárendelést, ahol $g_{\mathfrak{b},Q}$ -ra teljesül

$$g_{\mathfrak{b},Q}(0) = x(\psi(\mathfrak{b})S) - x(Q) \in \mathcal{R}^{\times},$$

mert az 5.3. lemma (iii) része használható $\mathfrak{p} \nmid \mathfrak{af}$ miatt. Tehát $g_{\mathfrak{b},Q}(Z) \in \mathcal{R}[[Z]]^{\times}$. A $\mathfrak{p}$ választása miatt $\Delta(E), \alpha \in \mathcal{O}_{\mathfrak{p}}^{\times}$. Az 5.8. állítás (ii) részét és $\Theta_{E,\mathfrak{a}}$ definícióját használva

$$\Lambda_{\mathfrak{p},\mathfrak{a}}(Z) = \alpha^{-12\#(B)} \Delta(E)^{(\mathbf{N}\mathfrak{a}-1)\#(B)} \prod_{\mathfrak{b} \in B, Q \in E[\mathfrak{a}] - \mathcal{O}} g_{\mathfrak{b},Q}(Z)^{-6} \in \mathcal{R}[[Z]]^{\times}.$$

Tudjuk azonban definíció szerint, hogy $\Lambda_{\mathfrak{p},\mathfrak{a}}(Z) \in K_{\mathfrak{p}}((Z))$, tehát (i) teljesül, mert $\mathcal{R}[[Z]]^{\times} \cap K_{\mathfrak{p}}((Z)) = \mathcal{O}_{\mathfrak{p}}[[Z]]^{\times}$. A (ii) triviálisan következik az 5.17. tételből és az 5.20. állításból. $\square$

6. Euler rendszerek

Rögzítsük K -nak egy $\mathfrak{p}$ prímjét, ami nem osztja $6\mathfrak{f}$ -et, és minden $n \geq 1$ -re legyen $K_n = K(E[\mathfrak{p}^n])$. Legyen p a racionális prím $\mathfrak{p}$ alatt. Rögzítsük $\mathcal{O}$ egy nemtriviális $\mathfrak{a}$ ideálját, ami relatív prím $6\mathfrak{f}\mathfrak{p}$ -hez. Jelölje $\mathcal{R} = \mathcal{R}(\mathfrak{a})$ az $\mathcal{O}$ -nak azon négyzetmentes ideáljait, melyek relatív prímekek $6\mathfrak{af}\mathfrak{p}$ -hez, és ha $\mathfrak{r} \in \mathcal{R}$, akkor $K_n(\mathfrak{r}) = K_n(E[\mathfrak{r}]) = K(E[\mathfrak{r}\mathfrak{p}^n])$. A későbbiekben $\mathfrak{q}$ mindig $\mathcal{R}$ egy prím elemét jelöli majd.

6.1. Elliptikus egységek

6.1. Definíció. Ha $\mathfrak{r} \in \mathcal{R}$ és $n \geq 0$, akkor legyen

$$\eta_n(\mathfrak{r}) = \eta_n^{(\mathfrak{a})}(\mathfrak{r}) = \Lambda_{E,\mathfrak{a},\xi(\Omega/\mathfrak{f})}(\xi(\psi(\mathfrak{p}^n\mathfrak{r})^{-1}\Omega)) = \Lambda_{L,\mathfrak{a}}(\psi(\mathfrak{p}^n\mathfrak{r})^{-1}\Omega),$$

ahol $\Lambda_{L,\mathfrak{a}}$ a 5.16. definícióból van.

6.2. Állítás. Tegyük fel, hogy $\mathfrak{r} \in \mathcal{R}$ és $n \geq 1$.

(i) $\eta_n(\mathfrak{r})$ globális egység $K_n(\mathfrak{r})$ -ben.

(ii) Ha $\mathfrak{q}$ prím és $\mathfrak{r}\mathfrak{q} \in \mathcal{R}$, akkor

$$N_{K_n(\mathfrak{r}\mathfrak{q})/K_n(\mathfrak{r})}\eta_n(\mathfrak{q}\mathfrak{r}) = \eta_n(\mathfrak{r})^{1-\text{Frob}_{\mathfrak{q}}^{-1}}.$$

(iii) $N_{K_{n+1}(\mathfrak{r})/K_n(\mathfrak{r})}\eta_{n+1}(\mathfrak{r}) = \eta_n(\mathfrak{r})$.

Bizonyítás. Az 5.8. állítás (iii) részéből következik (i) és az 5.7. következményből pedig (ii) és (iii). $\square$

6.2. Kolyvagin konstrukciója

6.3. Definíció. Legyen $G_{\mathfrak{r}} = \text{Gal}(K_n(\mathfrak{r})/K_n)$. A 3.19. következmény (ii) része miatt $G_{\mathfrak{r}}$ független $n \geq 1$ választásától és adottak a természetes izomorfizmusok

$$\begin{array}{ccc} G_{\mathfrak{r}} & \xlongequal{\quad} & \prod_{\mathfrak{q}|\mathfrak{r}} G_{\mathfrak{q}} \\ \downarrow \sim & & \downarrow \sim \\ (\mathcal{O}/\mathfrak{r})^{\times} & \xlongequal{\quad} & \prod_{\mathfrak{q}|\mathfrak{r}} (\mathcal{O}/\mathfrak{q})^{\times}. \end{array}$$

Ha $\mathfrak{q} \mid \mathfrak{r}$, akkor $G_{\mathfrak{q}}$ tekinthető $G_{\mathfrak{r}}$ faktorának és részcsoporthoz tartozó is. A 3.19. következmény miatt ha $\mathfrak{q}\mathfrak{r} \in \mathcal{R}$, akkor $K_n(\mathfrak{q}\mathfrak{r})/K_n(\mathfrak{r})$ ciklikus, $N_{\mathfrak{q}} - 1$ fokú, és teljesen elágazik minden $\mathfrak{q}$ feletti prímekben, illetve nem ágazik el minden minden más prímekben. (A 3.19. következmény (iv) és (v) részéhez $\mathfrak{a} := \mathfrak{r}\mathfrak{p}^n$, $\mathfrak{p} := \mathfrak{q}$, $n := 1$ választással.)

Minden $\mathfrak{r} \in \mathcal{R}$ -re legyen

$$N_{\mathfrak{r}} = \sum_{\sigma \in G_{\mathfrak{r}}} \sigma \in \mathbb{Z}[G_{\mathfrak{r}}],$$

speciálisan

$$N_{\mathfrak{r}} = \prod_{\mathfrak{q}|\mathfrak{r}} N_{\mathfrak{q}}.$$

Legyenek minden $n \geq 1$ és $\mathfrak{r} \in \mathcal{R}$ -re $x_{n,\mathfrak{r}}$ változók. Legyen $X_{n,\mathfrak{r}} = Y_{n,\mathfrak{r}}/Z_{n,\mathfrak{r}}$ egy $\text{Gal}(K_n(\mathfrak{r})/K)$ -modulus, ahol

$$Y_{n,\mathfrak{r}} = \bigoplus_{\mathfrak{s}|\mathfrak{r}} \mathbb{Z}[\text{Gal}(K_n(\mathfrak{s})/K)]x_{n,\mathfrak{s}},$$

$$Z_{n,\mathfrak{r}} = \sum_{\mathfrak{q}\mathfrak{s}|\mathfrak{r}} \mathbb{Z}[\text{Gal}(K_n(\mathfrak{r})/K)](N_{\mathfrak{q}}x_{n,\mathfrak{q}\mathfrak{s}} - (1 - \text{Frob}_{\mathfrak{q}}^{-1})x_{n,\mathfrak{s}}) \subset Y_{n,\mathfrak{r}}.$$

Vagy másképpen megfogalmazva $X_{n,\mathfrak{r}}$ a szabad $\text{Gal}(K_n(\mathfrak{r})/K)$ -modulus az $\{x_{n,\mathfrak{s}} : \mathfrak{s} \mid \mathfrak{r}\}$ szimbólumokon kifaktorizálva azokkal a relációkkal, hogy

- $G_{\mathfrak{r}/\mathfrak{s}}$ triviálisan hat $x_{n,\mathfrak{s}}$ -en, és
- $N_{\mathfrak{q}}x_{n,\mathfrak{q}\mathfrak{s}} = (1 - \text{Frob}_{\mathfrak{q}}^{-1})x_{n,\mathfrak{s}}$, ha $\mathfrak{q}\mathfrak{s} \mid \mathfrak{r}$.

Minden $\mathfrak{q} \in \mathcal{R}$ prímre rögzítsük egy $\sigma_{\mathfrak{q}}$ generátorát $G_{\mathfrak{q}}$ -nak és legyen

$$D_{\mathfrak{q}} = \sum_{i=1}^{\mathbf{N}\mathfrak{q}-2} i\sigma_{\mathfrak{q}}^i \in \mathbb{Z}[G_{\mathfrak{q}}],$$

illetve tetszőleges $\mathfrak{r} \in \mathcal{R}$ -re

$$D_{\mathfrak{r}} = \prod_{\mathfrak{q}|\mathfrak{r}} D_{\mathfrak{q}} \in \mathbb{Z}[G_{\mathfrak{r}}].$$

Ha M egy p -hatvány, akkor jelöljük $\mathcal{R}_{n,M}$ -mel azon $\mathfrak{r} \in \mathcal{R}$ ideálok halmazát, melyekre még az is teljesül, hogy minden $\mathfrak{q} \mid \mathfrak{r}$ prímosztóra

- $\mathfrak{q}$ teljesen felbomlik K_n/K -ban,
- $\mathbf{N}\mathfrak{q} \equiv 1 \pmod{M}$.

6.4. Állítás. *Tegyük fel, hogy M p -hatvány, $n \geq 1$ és $\mathfrak{r} \in \mathcal{R}_{n,M}$.*

(i) $X_{n,\mathfrak{r}}$ -nek nincs $\mathbb{Z}$ -torziója.

(ii) $D_{\mathfrak{r}}x_{n,\mathfrak{r}} \in (X_{n,\mathfrak{r}}/MX_{n,\mathfrak{r}})^{G_{\mathfrak{r}}}$.

Bizonyítás. Minden $\mathfrak{q} \in \mathcal{R}$ és $\mathfrak{s} \mid \mathfrak{r}$ -re legyenek

$$\begin{aligned} B_{\mathfrak{q}} &= G_{\mathfrak{q}} - \{1\}, \\ B_{\mathfrak{s}} &= \prod_{\mathfrak{q}|\mathfrak{s}} B_{\mathfrak{q}} = \left\{ \prod_{\mathfrak{q}|\mathfrak{s}} g_{\mathfrak{q}} : g_{\mathfrak{q}} \in B_{\mathfrak{q}} \right\} \subset G_{\mathfrak{r}}, \\ B &= \bigcup_{\mathfrak{s}|\mathfrak{r}} B_{\mathfrak{s}}x_{n,\mathfrak{s}} \subset X_{n,\mathfrak{r}}. \end{aligned}$$

Ekkor $X_{n,\mathfrak{r}}$ egy szabad $\mathbb{Z}$ -modulus B bázissal. (Ld. [Rub91] 2.1 lemma.)

Számítsuk ki a következőt

$$\begin{aligned} (\sigma_{\mathfrak{q}} - 1)D_{\mathfrak{q}} &= (\sigma_{\mathfrak{q}} - 1) \sum_{i=1}^{\mathbf{N}\mathfrak{q}-2} i\sigma_{\mathfrak{q}}^i = \sum_{i=1}^{\mathbf{N}\mathfrak{q}-2} i\sigma_{\mathfrak{q}}^{i+1} - \sum_{i=1}^{\mathbf{N}\mathfrak{q}-2} i\sigma_{\mathfrak{q}}^i = \\ &= (\mathbf{N}\mathfrak{q} - 2)\sigma_{\mathfrak{q}}^{\mathbf{N}\mathfrak{q}-1} + \sum_{i=2}^{\mathbf{N}\mathfrak{q}-2} (i-1)\sigma_{\mathfrak{q}}^i - \sigma_{\mathfrak{q}} - \sum_{i=2}^{\mathbf{N}\mathfrak{q}-2} i\sigma_{\mathfrak{q}}^i = (\mathbf{N}\mathfrak{q} - 2) - \sigma_{\mathfrak{q}} - \sum_{i=2}^{\mathbf{N}\mathfrak{q}-2} \sigma_{\mathfrak{q}}^i = \\ &= \mathbf{N}\mathfrak{q} - 1 - \sum_{i=1}^{\mathbf{N}\mathfrak{q}-1} \sigma_{\mathfrak{q}}^i = \mathbf{N}\mathfrak{q} - 1 - N_{\mathfrak{q}}. \end{aligned}$$

Indukcióval bizonyítjuk (ii)-t az $\mathfrak{r}$ prímosztóinak számára. Tegyük fel, hogy $\mathfrak{q} \mid \mathfrak{r}$, azaz $\mathfrak{r} = \mathfrak{q}\mathfrak{s}$ valamilyen kevesebb osztójú $\mathfrak{s}$ -re. Ekkor

$$\begin{aligned} (\sigma_{\mathfrak{q}} - 1)D_{\mathfrak{r}}x_{n,\mathfrak{r}} &= (\sigma_{\mathfrak{q}} - 1)D_{\mathfrak{q}}D_{\mathfrak{s}}x_{n,\mathfrak{r}} = \\ &= (\mathbf{N}\mathfrak{q} - 1)D_{\mathfrak{s}}x_{n,\mathfrak{r}} - (1 - \text{Frob}_{\mathfrak{q}}^{-1})D_{\mathfrak{s}}x_{n,\mathfrak{s}}, \end{aligned} \tag{6.1}$$

hiszen $X_{n,\mathfrak{r}}$ -en igaz az a reláció, hogy $N_{\mathfrak{q}}x_{n,\mathfrak{q}\mathfrak{s}} = (1 - \text{Frob}_{\mathfrak{q}}^{-1})x_{n,\mathfrak{s}}$ ha $\mathfrak{q}\mathfrak{s} \mid \mathfrak{r}$. Mivel $\mathfrak{q} \in \mathcal{R}_{n,M}$, ezért $M \mid \mathbf{N}\mathfrak{q} - 1$ és $\text{Frob}_{\mathfrak{q}} \in G_{\mathfrak{s}}$. Az indukciós feltevés miatt $D_{\mathfrak{s}}x_{n,\mathfrak{s}} \in (X_{n,\mathfrak{s}}/MX_{n,\mathfrak{s}})^{G_{\mathfrak{s}}}$, tehát $(1 - \text{Frob}_{\mathfrak{q}}^{-1})D_{\mathfrak{s}}x_{n,\mathfrak{s}} \in MX_{n,\mathfrak{s}}$. De emiatt (6.1)-ből látjuk, hogy

$$(\sigma_{\mathfrak{q}} - 1)D_{\mathfrak{r}}x_{n,\mathfrak{r}} \in MX_{n,\mathfrak{r}}.$$

Ha tetszőlegesen sokszor szorozzuk ezt a kongruenciát σ_q -val, akkor azt kapjuk, hogy

$$D_{\mathfrak{r}}x_{n,\mathfrak{r}} \equiv \sigma_q D_{\mathfrak{r}}x_{n,\mathfrak{r}} \equiv \sigma_q^2 D_{\mathfrak{r}}x_{n,\mathfrak{r}} \equiv \cdots \equiv \sigma_q^{N_q-2} D_{\mathfrak{r}}x_{n,\mathfrak{r}} \pmod{M},$$

azaz $D_{\mathfrak{r}}x_{n,\mathfrak{r}} \in (X_{n,\mathfrak{r}}/MX_{n,\mathfrak{r}})^{G_q}$, mert σ_q generálja G_q -t. Ebből következik (ii), mert ez elmondható $\mathfrak{r}$ minden prímosztójára és $G_{\mathfrak{r}} = \prod_{q|\mathfrak{r}} G_q$. $\square$

6.5. Definíció. *Euler rendszernek* mondjuk globális egységek egy

$$\{\eta(n, \mathfrak{r}) \in K_n(\mathfrak{r})^\times : n \geq 1, \mathfrak{r} \in \mathcal{R}\}$$

halmazát, ami teljesíti az

$$N_{K_n(q\mathfrak{r})/K_n(\mathfrak{r})}\eta(n, q\mathfrak{r}) = \eta(n, \mathfrak{r})^{1-\text{Frob}_q^{-1}} \quad (6.2)$$

$$N_{K_{n+1}(\mathfrak{r})/K_n(\mathfrak{r})}\eta(n+1, \mathfrak{r}) = \eta(n, \mathfrak{r}) \quad (6.3)$$

egyenleteket.

Ezzel ekvivalens definíció, hogy Euler rendszer egy Galois-ekvivariáns

$$\eta : \varinjlim_{n,\mathfrak{r}} X_{n,\mathfrak{r}} \rightarrow \bigcup_{n,\mathfrak{r}} K_n(\mathfrak{r})^\times$$

leképezés, ahol $\eta(x_{n,\mathfrak{r}})$ globális egység minden n -re és $\mathfrak{r}$ -re.

Euler rendszerre példa a 6.2. állítás miatt az $\eta(n, \mathfrak{r}) = \eta_n(\mathfrak{r})$ elliptikus egységek rendszere.

6.6. Állítás. *Tegyük fel, hogy η Euler rendszer és $q \in \mathcal{R}$ egy prím. Legyen $Nq-1 = dp^k$, ahol $p \nmid d$. Ekkor minden $n \geq 1$ -re és q -hoz relatív prím $\mathfrak{r} \in \mathcal{R}$ -re*

$$\eta(n, q\mathfrak{r})^d \equiv \eta(n, \mathfrak{r})^{d\text{Frob}_q^{-1}}$$

modulo minden q feletti prím.

Bizonyítás. [Rub99] 8.6 állítás. $\square$

6.7. Definíció. Tegyük fel, hogy η Euler rendszer, $n \geq 1$, M p -hatvány, $\mathfrak{r} \in \mathcal{R}_{n,M}$. Az Euler rendszer második definícióját használva definiálható egy $c = c_{\eta,n,\mathfrak{r}} : G_{\mathfrak{r}} \rightarrow K_n(\mathfrak{r})^\times$ 1-kociklus:

$$c(\sigma) = \eta\left(\frac{(\sigma-1)D_{\mathfrak{r}}x_{n,\mathfrak{r}}}{M}\right) \quad \text{minden } \sigma \in G_{\mathfrak{r}}.$$

A 6.4. állítás (ii) része miatt ez egy értelmes definíció. Mivel $H^1(G_{\mathfrak{r}}, K_n(\mathfrak{r})^\times) = 0$, ezért létezik $\beta \in K_n(\mathfrak{r})^\times$, amire $c(\sigma) = \beta^\sigma/\beta$ teljesül minden $\sigma \in G_{\mathfrak{r}}$ -re. Mivel $G_{\mathfrak{r}}$ fixen hagyja $\eta(x_{n,\mathfrak{r}})^{D_{\mathfrak{r}}}/\beta^M$ -t, ezért $\eta(x_{n,\mathfrak{r}})^{D_{\mathfrak{r}}}/\beta^M \in K_n^\times$ és legyen

$$\kappa_{n,M}(\mathfrak{r}) = \eta(x_{n,\mathfrak{r}})^{D_{\mathfrak{r}}}/\beta^M \in K_n^\times/(K_n^\times)^M.$$

β választása egyértelmű modulo $K_n^\times$, hiszen $G_{\mathfrak{r}}$ minden eleme pontosan azokat hagyja fixen $K_n(\mathfrak{r})^\times$ -ben, amik $K_n^\times$ elemei is. Ezért $\kappa_{n,M}(\mathfrak{r})$ független β választásától.

6.8. Definíció. Rögzítsünk egy $n \geq 1$ számot, egy M p -hatványt, és az egyszerűség kedvéért ideiglenesen legyen $F = K_n$, $\mathcal{R}_{F,M} = \mathcal{R}_{n,M}$. Jelölje $\mathcal{O}_F$ az F egészeinek gyűrűjét és

$$\mathcal{I}_F = \mathcal{I} = \bigoplus_{\Omega} \mathbb{Z}\Omega$$

F törtideáljainak csoportját additívan írva. Ennek részcsoporthaként legyen

$$\mathcal{I}_{F,\mathfrak{q}} = \mathcal{I}_{\mathfrak{q}} = \bigoplus_{\Omega|\mathfrak{q}} \mathbb{Z}\Omega$$

a K -beli $\mathfrak{q}$ prímeál feletti ideálok által generált részcsoporth. Ha $y \in F^\times$, akkor legyen $(y) \in \mathcal{I}$ az y által generált törtfőideál, illetve $(y)_{\mathfrak{q}}$, $[y]$ és $[y]_{\mathfrak{q}}$ az (y) projekciói rendre $\mathcal{I}_{\mathfrak{q}}$ -ban, $\mathcal{I}/M\mathcal{I}$ -ben és $\mathcal{I}_{\mathfrak{q}}/M\mathcal{I}_{\mathfrak{q}}$ -ban. Vegyük észre, hogy $[y]$ és $[y]_{\mathfrak{q}}$ jóldefiniáltak, ha $y \in F^\times/(F^\times)^M$.

Tegyük fel, hogy $\mathfrak{q} \in \mathcal{R}_{F,M}$, Ω egy prím $\mathfrak{q}$ felett F -ben és $\bar{\Omega}$ egy prím Ω felett $\bar{K}$ -ban. Tudjuk, hogy $\mathfrak{q}$ teljesen felbomlik F/K -ban, hiszen $\mathcal{R}_{F,M}$ -nek ez volt az egyik feltétele, illetve Ω teljesen elágazik $F(\mathfrak{q})/F$ -ben $\mathbf{N}\Omega - 1 = \mathbf{N}\mathfrak{q} - 1$ elágazási indexszel a 3.19. következmény miatt. Legyen σ_{Ω} egy felemeltje $\sigma_{\mathfrak{q}}$ -nak G_K -ba, ami benne van $\bar{\Omega}$ inerciarészcsoporthjában. Ekkor van egy

$$a \mapsto (\pi^{a/M})^{1-\sigma_{\Omega}} : \mathbb{Z}/M\mathbb{Z} \xrightarrow{\sim} \mu_M$$

izomorfizmus, ahol π egy generátora $\mathfrak{q}$ -nak. Legyen $\text{Frob}_{\Omega} \in G_{F_{\Omega}}$ egy Frobenius leképezése Ω -nak, illetve

$$\phi_{\Omega} : F_{\Omega}^{\times}/(F_{\Omega}^{\times})^M \rightarrow \mathbb{Z}/M\mathbb{Z}$$

a képe Frob_{Ω} -nak a

$$G_{F_{\Omega}} \rightarrow \text{Hom}(F_{\Omega}^{\times}, \mu_M) \xrightarrow{\sim} \text{Hom}(F_{\Omega}^{\times}, \mathbb{Z}/M\mathbb{Z})$$

kompozíciónál, ahol az első leképezés a Kummer leképezés, a második pedig a korábbi izomorfizmusból jön. (A Kummer leképezés egy $\sigma \in G_{F_{\Omega}}$ -hoz az $x \mapsto (x^{1/M})^{\sigma-1}$ homomorfizmust rendeli.) Tehát mivel σ_{Ω} az inerciarészcsoporthoz tartozik, ezért $\phi_{\Omega}(\alpha) = a$, ahol

$$(\alpha^{1/M})^{\text{Frob}_{\Omega}-1} = (\pi^{a/M})^{1-\sigma_{\Omega}} \equiv (\beta^{1/M})^{1-\sigma_{\Omega}} \quad (6.4)$$

modulo $\bar{F}_{\Omega}$ maximális ideálja, ahol $\beta \in \bar{F}_{\Omega}^{\times}$ egy olyan elem, amire $\text{ord}_{\Omega}(\beta) = a$.

Ezeket egy globális leképezéssé összerakva kapunk egy

$$\phi_{\mathfrak{q}} : F^{\times}/(F^{\times})^M \rightarrow \mathcal{I}_{\mathfrak{q}}/M\mathcal{I}_{\mathfrak{q}}$$

függvényt a $\phi_{\mathfrak{q}}(\alpha) = \sum_{\Omega|\mathfrak{q}} \phi_{\Omega}(\alpha)\Omega$ képlettel. Ekkor $\phi_{\mathfrak{q}}$ egy $\text{Gal}(F/K)$ -ekvivariáns leképezés és indukál egy ugyanígy jelölt

$$\phi_{\mathfrak{q}} : (\mathcal{O}_F/\mathfrak{q}\mathcal{O}_F)^{\times}/((\mathcal{O}_F/\mathfrak{q}\mathcal{O}_F)^{\times})^M \xrightarrow{\sim} \mathcal{I}_{\mathfrak{q}}/M\mathcal{I}_{\mathfrak{q}}$$

izomorfizmust.

6.9. Állítás. Tegyük fel, hogy η egy Euler rendszer, $n \geq 1$, $\mathfrak{r} \in \mathcal{R}_{n,M}$ és $\mathfrak{q}$ egy prím K -ban.

(i) Ha $\mathfrak{q} \nmid \mathfrak{r}$, akkor $[\kappa_{n,M}(\mathfrak{r})]_{\mathfrak{q}} = 0$.

(ii) Ha $\mathfrak{q} \mid \mathfrak{r}$, akkor $[\kappa_{n,M}(\mathfrak{r})]_{\mathfrak{q}} = \phi_{\mathfrak{q}}(\kappa_{n,M}(\mathfrak{r}/\mathfrak{q}))$.

Bizonyítás. Tegyük fel, hogy $\mathfrak{q} \nmid \mathfrak{r}$. Ekkor $\mathfrak{q}$ nem ágazik el $K_n(\mathfrak{r})/K_n$ -ben. A $\kappa_{n,M}(\mathfrak{r})$ definíció szerint egy globális egység és egy M -dik hatvány szorzata $K_n(\mathfrak{r})^\times$ -ben. Tehát $\text{ord}_{\Omega}(\kappa_{n,M}(\mathfrak{r})) \equiv 0 \pmod{M}$ minden $\mathfrak{q}$ feletti Ω prímjére K_n -nek, mert ha Ω' egy prímjé $K_n(\mathfrak{r})$ -nek Ω felett, akkor $\text{ord}_{\Omega} = \text{ord}_{\Omega'}$, hiszen $\mathfrak{q}$ nem ágazik el. Ebből következik (i).

Tegyük fel, hogy $\mathfrak{q} \mid \mathfrak{r}$, például $\mathfrak{r} = \mathfrak{q}\mathfrak{s}$. Definíció szerint

$$\kappa_{n,M}(\mathfrak{r}) = \eta(x_{n,\mathfrak{r}})^{D_{\mathfrak{r}}} / \beta_{\mathfrak{r}}^M, \quad \kappa_{n,M}(\mathfrak{s}) = \eta(x_{n,\mathfrak{s}})^{D_{\mathfrak{s}}} / \beta_{\mathfrak{s}}^M,$$

ahol $\beta_{\mathfrak{r}} \in K_n(\mathfrak{r})^\times$, $\beta_{\mathfrak{s}} \in K_n(\mathfrak{s})^\times$, és teljesül

$$\beta_{\mathfrak{r}}^{\sigma-1} = \eta((\sigma-1)D_{\mathfrak{r}}x_{n,\mathfrak{r}}/M), \quad \beta_{\mathfrak{s}}^{\sigma-1} = \eta((\sigma-1)D_{\mathfrak{s}}x_{n,\mathfrak{s}}/M)$$

minden $\sigma \in G_{\mathfrak{r}}$ -re. Rögzítsük egy $\mathfrak{q}$ feletti Ω prímjét K_n -nek, és legyen σ_{Ω} olyan, mint a 6.8. definícióban, és jelölje d a p -hez relatív prím részét $(\mathbf{N}\mathfrak{q} - 1)$ -nek. Modulo minden Ω feletti prím

$$\begin{aligned} (\kappa_{n,M}(\mathfrak{r})^{d/M})^{1-\sigma_{\Omega}} &= ((\eta(x_{n,\mathfrak{r}})^{D_{\mathfrak{r}}})^{1/M} / \beta_{\mathfrak{r}})^{d(1-\sigma_{\Omega})} \stackrel{(1)}{\equiv} \beta_{\mathfrak{r}}^{d(\sigma_{\mathfrak{q}}-1)} \\ &= \eta((\sigma_{\mathfrak{q}}-1)D_{\mathfrak{r}}x_{n,\mathfrak{r}}/M)^d \\ &= \eta((\mathbf{N}\mathfrak{q}-1-N_{\mathfrak{q}})D_{\mathfrak{s}}x_{n,\mathfrak{r}}/M)^d \\ &= \eta((\mathbf{N}\mathfrak{q}-1)D_{\mathfrak{s}}x_{n,\mathfrak{r}}/M)^d \eta((\text{Frob}_{\mathfrak{q}}^{-1}-1)D_{\mathfrak{s}}x_{n,\mathfrak{s}}/M)^d \\ &= (\eta(x_{n,\mathfrak{r}})^{D_{\mathfrak{s}}})^{d(\mathbf{N}\mathfrak{q}-1)/M} / \beta_{\mathfrak{s}}^{d(1-\text{Frob}_{\mathfrak{q}}^{-1})} \\ &= (\eta(x_{n,\mathfrak{r}})^{D_{\mathfrak{s}}})^{d\text{Frob}_{\mathfrak{q}}\text{Frob}_{\mathfrak{q}}^{-1}(\mathbf{N}\mathfrak{q}-1)/M} / \beta_{\mathfrak{s}}^{d(1-\text{Frob}_{\mathfrak{q}}^{-1})} \\ &\equiv (\eta(x_{n,\mathfrak{r}})^{D_{\mathfrak{s}}})^{d\text{Frob}_{\mathfrak{q}}(1-\text{Frob}_{\mathfrak{q}}^{-1})/M} / \beta_{\mathfrak{s}}^{d(1-\text{Frob}_{\mathfrak{q}}^{-1})} \\ &\stackrel{(2)}{\equiv} (\eta(x_{n,\mathfrak{s}})^{D_{\mathfrak{s}}})^{d(1-\text{Frob}_{\mathfrak{q}}^{-1})/M} / \beta_{\mathfrak{s}}^{d(1-\text{Frob}_{\mathfrak{q}}^{-1})} \\ &\equiv (\eta(x_{n,\mathfrak{s}})^{D_{\mathfrak{s}}})^{d(1-\text{Frob}_{\Omega}^{-1})/M} / \beta_{\mathfrak{s}}^{d(1-\text{Frob}_{\Omega}^{-1})} \\ &= ((\eta(x_{n,\mathfrak{s}})^{D_{\mathfrak{s}}} / \beta_{\mathfrak{s}}^M)^{1/M})^{d(1-\text{Frob}_{\Omega}^{-1})} \\ &\equiv ((\kappa_{n,M}(\mathfrak{s})^{d/M})^{\text{Frob}_{\Omega}-1}), \end{aligned}$$

ahol használtuk az (1) kongruenciánál, hogy $\eta(x_{n,\mathfrak{r}})$ globális egység és a (2) kongruenciánál a 6.6. állítást. A (6.4) kongruenciát használva $\alpha = \kappa_{n,M}(\mathfrak{s})^d$ és $\beta = \kappa_{n,M}(\mathfrak{r})^d$ választással adódik, hogy

$$d\phi_{\Omega}(\kappa_{n,M}(\mathfrak{s})) = \phi_{\Omega}(\alpha) = \text{ord}_{\Omega}(\beta) = d\text{ord}_{\Omega}(\kappa_{n,M}(\mathfrak{r})),$$

amiből következik (ii), mert M p -hatvány és d relatív prím p -hez, tehát d invertálható modulo M . $\square$

7. Az osztálycsoport mérete

Legyen a jelöléshalmazok elkerülése végett $F = K_1 = K(E[\mathfrak{p}])$, μ_F az egységgyökök F -ben és $\Delta = \text{Gal}(F/K)$, azaz $\Delta \cong (\mathcal{O}/\mathfrak{p})^\times$ ciklikus $p-1$ vagy p^2-1 renddel.

A Maschke tétel miatt $\mathbb{F}_p[\Delta]$ félegyszerű, mivel $p \nmid \#(\Delta)$. Tehát előáll ferdetest feletti mátrixgyűrűk direktösszegeként a Wedderburn-Artin tétel szerint. Itt azonban

$\mathbb{F}_p[\Delta]$ kommutatív, tehát a mátrixgyűrűk 1-dimenziósak és a ferdetestek testek. $\mathbb{F}_p[\Delta]$ véges is, tehát a testek végesek, és p -hatvány eleműek, mert $\mathbb{F}_p[\Delta]$ p -karakterisztikájú. Vagyis

$$\mathbb{F}_p[\Delta] \cong \bigoplus_{j=1}^r \mathbb{F}_{p^{n_j}}. \quad (7.1)$$

Tehát Δ $\mathbb{F}_p$ feletti reprezentációi olyanok, hogy $\mathbb{F}_{p^{n_j}}^\times$ egy elemét rendeljük a csoportelemekhez. Azonban Δ elemszáma $p^2 - 1$ osztója, tehát a csoportelemek képe $(p^2 - 1)$ -edik egységgyökök, amik benne vannak $\mathbb{F}_{p^2}$ -ben. Azaz feltehetjük, hogy (7.1)-ben $1 \leq n_j \leq 2$.

Egyértelműen létezik $\mathbb{Q}_p$ -nek egy $\mathbb{Q}_{p^2}$ -tel jelölt, másodfokú, elágazásmentes bővítése $\mathbb{F}_{p^2}$ maradéktesttel, méghozzá az $x^2 - \tilde{u}$ felbontási teste, ahol $\tilde{u} \in \mathbb{Z}_p$ tetszőleges felemeltje az $u \in \mathbb{F}_p$ tetszőleges kvadratikus nemmaradéknak. Legyen $\mathbb{Z}_{p^2}$ a $\mathbb{Q}_{p^2}$ egészeinek gyűrűje, melynek az elemei karakterizálhatók az egyértelmű $\varepsilon_0 + p\varepsilon_1 + p^2\varepsilon_2 + \dots$, ($\varepsilon_j \in \{0\} \cup \mu_{p^2-1}$) végtelen sorukkal.

Az (7.1) felbontáshoz tartoznak $e_1, \dots, e_r \in \mathbb{F}_p[\Delta]$ ortogonális idempotensek. Felemelhetőek $\mathbb{Z}_p[\Delta]$ -ba ortogonális idempotensekké, és így kapunk egy

$$\mathbb{Z}_p[\Delta] \cong \bigoplus_{\chi \in \Xi} R_\chi \quad (7.2)$$

felbontást, ahol Ξ a Δ irreducibilis $\mathbb{F}_p$ -reprezentációinak halmaza, R_χ pedig $\mathbb{Z}_p[\Delta]$ megfelelő direkt összeadandója. Az előzőek szerint $\dim(\chi) \leq 2$ és $R_\chi \cong \mathbb{Z}_{p^{\dim(\chi)}}$.

Ha $\chi \in \Xi$ és M egy $\mathbb{Z}[\Delta]$ -modulus, akkor jelölje $M^{(p)} = \varprojlim_n M/p^n M = M \otimes_{\mathbb{Z}} \mathbb{Z}_p$ a p -adikus telítését M -nek, illetve

$$M^\chi = M^{(p)} \otimes_{\mathbb{Z}_p[\Delta]} R_\chi.$$

A tenzorszorzás és direktösszeg felcserélhetősége miatt $M^{(p)} = \bigoplus_{\chi \in \Xi} M^\chi$, ezért M^χ tekinthető a faktorának és részmodulusának is $M^{(p)}$ -nek. Ha $m \in M$, akkor m^χ jelöli a projekcióját M^χ -re.

7.1. Lemma. Minden nemtriviális $\chi \in \Xi$ reprezentációra $(\mathcal{O}_F^\times/\mu_F)^\chi$ szabad 1-rangú modulus R_χ felett.

Bizonyítás. Nincs valós beágyazása F -nek, mert már K -nak sincs, ezért összesen

$$s = |F : \mathbb{Q}|/2 = |F : K||K : \mathbb{Q}|/2 = \#(\Delta)$$

komplex beágyazása van F -nek. A Dirichlet egységtétel szerint $\mathcal{O}_F^\times/\mu_F \cong \mathbb{Z}^{s-1}$, tehát létezik egy

$$0 \rightarrow (\mathcal{O}_F^\times/\mu_F) \otimes_{\mathbb{Z}} \mathbb{Q} \rightarrow \mathbb{Q}[\Delta] \rightarrow \mathbb{Q} \rightarrow 0$$

egzakt sorozat. Mivel $\mathbb{Z}_p$ lapos $\mathbb{Z}$ -modulus, ezért $- \otimes_{\mathbb{Z}} \mathbb{Z}_p$ funktor megtartja az egzakt-ságot, ezért χ -komponenseket véve következik az állítás. $\square$

Jelölje A az ideál osztálycsoportját F -nek. Legyen M p -hatványra $F_M = F(\mu_M)$ a jelölés egyszerűsítéséért.

7.2. Lemma.

$$\text{Hom}(A, \mathbb{Z}/M\mathbb{Z}) \rightarrow \text{Hom}(G_F, \mathbb{Z}/M\mathbb{Z}) \rightarrow \text{Hom}(G_{F_M}, \mathbb{Z}/M\mathbb{Z})$$

injektív leképezés, ahol $A \cong \text{Gal}(H_F/F) \cong G_F/\text{Gal}(\bar{F}/H_F)$ (H_F az F Hilbert osztálytest) indukálja az első leképezést, és a megszorítás a másodikat.

Bizonyítás. [Rub99] 9.2 lemma. □

7.3. Lemma.

$$F^\times / (F^\times)^M \rightarrow F_M^\times / (F_M^\times)^M$$

injektív leképezés.

Bizonyítás. [Rub99] 9.3 lemma. □

7.4. Állítás. *Tegyük fel, hogy $\kappa \in F^\times / (F^\times)^M$ és $\alpha \in \text{Hom}(A, \mathbb{Z}/M\mathbb{Z})$, $\alpha \neq 0$. Ekkor létezik egy $\mathfrak{q} \in \mathcal{R}_{F,M}$ prím, és egy $\mathfrak{Q}$ prímje F -nek $\mathfrak{q}$ felett, amikre*

(i) $\alpha(\mathfrak{c}) \neq 0$, ahol $\mathfrak{c}$ a $\mathfrak{Q}$ osztálya F -ben,

(ii) $[\kappa]_{\mathfrak{q}} = 0$ és minden $d \in \mathbb{Z}$ -re $d\phi_{\mathfrak{q}}(\kappa) = 0 \Leftrightarrow \kappa^d \in (F^\times)^M$.

Bizonyítás. [Rub99] 9.4 állítás. □

Legyen η Euler rendszer és $\mathcal{C} = \mathcal{C}_\eta \subset \mathcal{O}_F$ a $\mathbb{Z}[\Delta]$ felett generált részcsoportha $\mu_F \cup \{\eta(1, \mathcal{O})\}$ -nak.

7.5. Tétel. *Ha η Euler rendszer, $\chi \in \Xi$, akkor*

$$\#(A^\chi) \leq \#((\mathcal{O}_F^\times / \mathcal{C}_\eta)^\chi).$$

Bizonyítás. Ha χ a triviális karakter, akkor A^χ a p -része K ideál osztálycsoportjának, ami triviális, mert K -ról feltettük, hogy főideálgyűrű. Tegyük fel, hogy $\chi \neq 1$.

A 7.1. lemma szerint $(\mathcal{O}_F^\times / \mathcal{C})^\chi \cong R_\chi / mR_\chi$ valamilyen $m \in R_\chi$ -re. Ha $m = 0$, akkor triviális a tétel állítása. Tegyük fel, hogy $m \neq 0$ és ekkor valamilyen p -hatvány. Legyen M olyan nagy p -hatvány, hogy annullálja A -t. Minden $\mathfrak{r} \in \mathcal{R}_{F,M}$ -re vezessük be a $\kappa(\mathfrak{r})$ rövidítést $\kappa_{1,M}(\mathfrak{r}) \in F^\times / (F^\times)^M$ helyett. Indexeljük meg $\text{Hom}(A^\chi, \mathbb{Z}/M\mathbb{Z}) \subset \text{Hom}(A, \mathbb{Z}/M\mathbb{Z})$ elemeit, mint

$$\text{Hom}(A^\chi, \mathbb{Z}/M\mathbb{Z}) = \{\alpha_1, \dots, \alpha_k\}.$$

Használjuk a 7.4. állítást és gyártsuk le induktívan a következő sorozatát prímeknek: $\mathfrak{q}_1, \dots, \mathfrak{q}_k \in \mathcal{R}_{F,M}$, $\mathfrak{Q}_i$ prímje F -nek $\mathfrak{q}_i$ felett, $\mathfrak{c}_i$ a $\mathfrak{Q}_i$ osztálya A -ban és $\mathfrak{r}_i = \prod_{j \leq i} \mathfrak{q}_j$ minden $0 \leq i \leq k$ -ra,

$$\alpha_i(\mathfrak{c}_i) \neq 0 \tag{7.3}$$

$$d\phi_{\mathfrak{q}_i}(\kappa(\mathfrak{r}_{i-1})^\chi) = 0 \Leftrightarrow (\kappa(\mathfrak{r}_{i-1})^\chi)^d = 0 \in F^\times / (F^\times)^M \tag{7.4}$$

(alkalmazzuk 7.4. állítást $\kappa = \kappa(\mathfrak{r}_{i-1})^\chi$ és $\alpha = \alpha_i$ választásokkal, hogy megkapjuk $\mathfrak{q}_i$ -t és $\mathfrak{Q}_i$ -t).

A $\{\mathfrak{c}_i^\chi\}$ osztályok generálják A^χ -t, mert ha nem generálnák, akkor létezne nemtriviális $\alpha \in \text{Hom}(A^\chi, \mathbb{Z}/M\mathbb{Z})$, amire $\alpha(\mathfrak{c}_j) = 0$ minden j -re, de $\alpha = \alpha_i$ valamilyen i -re, tehát (7.3) miatt ez nem lehet.

Jelölje $1 \leq i \leq k$ -ra s_i a $\mathfrak{c}_i^\chi$ rendjét $A^\chi / \langle \mathfrak{c}_1^\chi, \dots, \mathfrak{c}_{i-1}^\chi \rangle$ -ben. Teljesül

$$|\langle \mathfrak{c}_1^\chi, \dots, \mathfrak{c}_i^\chi \rangle : \langle \mathfrak{c}_1^\chi, \dots, \mathfrak{c}_{i-1}^\chi \rangle| = |R_\chi : s_i R_\chi|,$$

így

$$\#(A) = \prod_{i=1}^k |R_\chi : s_i R_\chi|.$$

Ha $1 \leq i \leq k-1$, akkor jelölje t_i a $\kappa(\mathfrak{r}_i)^\chi$ rendjét $F^\times/(F^\times)^M$ -ben. A 6.9. állítás (ii) része és (7.4) miatt $[\kappa(\mathfrak{r}_i)^\chi]_{\mathfrak{q}_i}$ rendje t_{i-1} , speciálisan $t_{i-1} \mid t_i$. Mivel $\kappa(\mathfrak{r}_0)$ a képe $\eta(1, \mathcal{O})$ -nak $\mathcal{O}_F^\times/(\mathcal{O}_F^\times)^M$ -ben, ezért a

$$0 \rightarrow R_\chi \kappa(\mathfrak{r}_0)/(\mu_F \cap R_\chi \kappa(\mathfrak{r}_0)) \rightarrow (\mathcal{O}_F^\times/\mu_F(\mathcal{O}_F^\times)^M)^\chi \rightarrow (\mathcal{O}_F^\times/\mathcal{C})^\chi \rightarrow 0$$

egzakt sorozat mutatja, hogy $M \mid t_0 m$.

Minden i -re válasszunk egy $\nu_i \in F^\times/(F^\times)^M$ -t, amire $\nu_i^{M/t_i} = \kappa(r_i)^\chi \zeta$, ahol $\zeta \in \mu_F$. Tehát

$$(M/t_i)[\nu_i]_{\mathfrak{q}_i} = [\kappa(\mathfrak{r}_i)^\chi]_{\mathfrak{q}_i},$$

amiből látszik, hogy $[\nu_i]_{\mathfrak{q}_i}$ rendje $(\mathcal{I}_{\mathfrak{q}_i}/M\mathcal{I}_{\mathfrak{q}_i})^\chi$ -ben $t_{i-1}M/t_i$. Az

$$\begin{aligned} \mathcal{I}_{\mathfrak{q}_i} &\rightarrow \mathbb{Z}[\Delta] \\ \sum_{\sigma \in \Delta} e_\sigma(\mathfrak{Q}_i)^\sigma &\mapsto \sum_{\sigma \in \Delta} e_\sigma \sigma \end{aligned}$$

izomorfizmus indukál egy $(\mathcal{I}_{\mathfrak{q}_i}/M\mathcal{I}_{\mathfrak{q}_i})^\chi \cong R_\chi/MR_\chi$ izomorfizmust, hiszen M p -hatvány és így $\mathbb{Z}/M\mathbb{Z} \cong \mathbb{Z}_p/M\mathbb{Z}_p$. A 6.9. állítás miatt létezik egy $u \in R_\chi^\times$ egység, amire

$$(\nu_i) \equiv u(t_i/t_{i-1})\mathfrak{q}_i^\chi \pmod{\mathcal{I}_{\mathfrak{q}_1}, \dots, \mathcal{I}_{\mathfrak{q}_{i-1}}, t_i\mathcal{I}}.$$

Tudjuk, hogy $t_0 \mid t_i$ és $(M/m) \mid t_0$, tehát M választása miatt t_i annulálja A -t és így

$$(t_i/t_{i-1})\mathfrak{c}_i^\chi = 0 \quad A^\chi/\langle \mathfrak{c}_1^\chi, \dots, \mathfrak{c}_{i-1}^\chi \rangle\text{-ben.}$$

Tehát $s_i \mid (t_i/t_{i-1})$ minden $i \geq 1$ -re, tehát

$$\#(A) = \prod_{i=1}^k |R_\chi : s_i R_\chi| \text{ osztja } \prod_{i=1}^k |R_\chi : \frac{t_i}{t_{i-1}} R_\chi| = \prod_{i=1}^k |t_{i-1} : t_i R_\chi| = |t_0 R_\chi : t_k R_\chi|.$$

Mivel $t_k \mid M$ és $M \mid t_0 m$, ezért $t_k \mid t_0 m$, vagyis $|t_0 R_\chi : t_k R_\chi|$ osztja $|R_\chi : m R_\chi|$ -t, ami bizonyítja a tételt, hiszen $(\mathcal{O}_F^\times/\mathcal{C})^\chi \cong R_\chi/mR_\chi$. $\square$

7.6. Következmény. Legyen $\mathcal{C}_a = \mathcal{C}_\eta$, ahol $\eta(n, \mathfrak{r}) = \eta_n^{(a)}(\mathfrak{r})$ a 6.1. definíció elliptikus Euler rendszere. Ha $\chi \in \Xi$, akkor

$$\#(A^\chi) \text{ osztja } \#((\mathcal{O}_F^\times/\mathcal{C}_a)^\chi)\text{-t.}$$

Bizonyítás. Következik a 7.5.tételből. $\square$

7.7. Következmény. Ha $(\eta_1^\eta)^\chi \notin \mu_F^\chi((\mathcal{O}_F^\times)^\chi)^p$, akkor $A^\chi = 0$.

Bizonyítás. A 7.1. lemmából következik, hogy $(\mathcal{O}_F^\times/\mathcal{C}_a)^\chi$ triviális, amiből a 7.6. következmény miatt következik, hogy $A^\chi = 0$. $\square$

8. Coates és Wiles tétele

Tegyük fel, hogy $\mathfrak{p}$ ideálja K -nak nem osztja $\mathfrak{f}$ -et és a $p > 7$ racionális prím felett van. Továbbra is $F = K(E[\mathfrak{p}])$, $\Delta = \text{Gal}(F/K)$ és A az ideál osztálycsoportja F -nek.

8.1. Lemma. *Létezik $\mathfrak{a}$ ideálja $\mathcal{O}$ -nak, ami relatív prím $6\mathfrak{p}\mathfrak{f}$ -hez és $\mathbf{N}\mathfrak{a} \not\equiv \psi(\mathfrak{a}) \pmod{\mathfrak{p}}$.*

Bizonyítás. A 3.17. következmény miatt $E[\bar{\mathfrak{p}}] \not\subset E(K)$, mert $\mathcal{O}^\times$ legfeljebb 6 elemű (ld. [Sil09] III. 10.1 tétel). Legyen $\mathfrak{q}$ egy prímje K -nak, ami nem osztja $6\mathfrak{p}\mathfrak{f}$ -et és $[\mathfrak{q}, K(E[\bar{\mathfrak{p}}])/K] \neq 1$. Ha $\psi(\mathfrak{q}) \equiv 1 \pmod{\bar{\mathfrak{p}}}$, akkor $\psi(\mathfrak{q})$ triviális $E[\bar{\mathfrak{p}}]$ -n (3.3. állítás), tehát a 3.15. következmény (ii) miatt $[\mathfrak{q}, K(E[\bar{\mathfrak{p}}])/K]$ is triviálisan hat $E[\bar{\mathfrak{p}}]$ -n, ami nem lehet. Tehát $\psi(\mathfrak{q}) \not\equiv 1 \pmod{\bar{\mathfrak{p}}}$, amit konjugálva $\bar{\psi}(\mathfrak{q}) \not\equiv 1 \pmod{\mathfrak{p}}$. A 3.15. következmény (i) része miatt $\psi(\mathfrak{q})\mathcal{O} = \mathfrak{q}$, tehát $\psi(\mathfrak{q})\bar{\psi}(\mathfrak{q}) = \mathbf{N}\psi(\mathfrak{q}) = \mathbf{N}\mathfrak{q}$. Vagyis $\mathfrak{a} = \mathfrak{q}$ választással teljesül a lemma. $\square$

A 3.19. következmény (iv) része miatt ($\mathfrak{a} = \mathcal{O}$ és $n = 1$ választással) F/K teljesen elágazik $\mathfrak{p}$ -ben. Jelölje $\mathcal{P}$ a $\mathfrak{p}$ feletti prímjét F -nek. A 2.27. lemma és a 3.15. következmény miatt $E[\mathfrak{p}] \subset E_1(F_{\mathcal{P}})$ (2.27.-ben $\phi = \psi(\mathcal{P})$ választással $\tilde{\phi}$ tisztán inszeparábilis 3.15. (iii) miatt, és $\psi(\mathcal{P}) \in \mathfrak{p}$ 3.15. (i) miatt, tehát $E[\mathfrak{p}] \subset \ker(\psi(\mathcal{P})) = \ker(\phi) \subset E_1(F_{\mathcal{P}})$), tehát a 2.29. következmény izomorfizmusának megszorítása ad egy

$$E[\mathfrak{p}] \xrightarrow{\sim} \hat{E}[\mathfrak{p}] \subset \hat{E}(F_{\mathcal{P}})$$

izomorfizmust, ahol $\hat{E}$ az E -hez rendelt formális csoport. Jelölje $\mathcal{O}_{F,\mathcal{P}}$ az $\mathcal{O}_F$ teljessé tételét $\mathcal{P}$ szerint.

8.2. Lemma.

$$E[\mathfrak{p}] \xrightarrow{\sim} \hat{E}[\mathfrak{p}] \xrightarrow{1+} (1 + \mathcal{P}\mathcal{O}_{F,\mathcal{P}})/(1 + \mathcal{P}^2\mathcal{O}_{F,\mathcal{P}})$$

egy Δ -ekvivariáns izomorfizmus.

Bizonyítás. A formális csoportok definíciója miatt $\mathcal{F}_E(z, z') = z + z' + (\geq 2\text{-fokú tagok})$, tehát valóban homomorfizmus a lemma leképezése, mert modulo $1 + \mathcal{P}^2\mathcal{O}_{F,\mathcal{P}}$ nem számítanak a ≥ 2 -fokú tagok.

Értsük meg jobban a leképezést. A 2.29. következmény izomorfizmusa $F_{\mathcal{P}}$ -re a következő

$$\begin{aligned} E_1(F_{\mathcal{P}}) &\cong \hat{E}(\mathcal{P}\mathcal{O}_{F,\mathcal{P}}) \\ (x, y) &\mapsto -\frac{x}{y}. \end{aligned}$$

Ennek megszorítása adja az $E[\mathfrak{p}] \xrightarrow{\sim} \hat{E}[\mathfrak{p}]$ izomorfizmust. Vegyünk egy $P \in E[\mathfrak{p}]$, $O \neq P = (x, y)$ pontot. A 2.26. lemma szerint $3\text{ord}_{\mathcal{P}}(x) = 2\text{ord}_{\mathcal{P}}(y)$. Használhatjuk az 5.3. lemma (i) részét, mert $P \neq O$, miszerint $\text{ord}_{\mathfrak{p}}(x) = -2/(\mathbf{N}\mathfrak{p} - 1)$. Mivel $\mathfrak{p}$ teljesen elágazik, ezért $\text{ord}_{\mathcal{P}}(x) = (\mathbf{N}\mathfrak{p} - 1)\text{ord}_{\mathfrak{p}}(x)$, és így

$$\text{ord}_{\mathcal{P}}\left(-\frac{x}{y}\right) = \text{ord}_{\mathcal{P}}(x) - \text{ord}_{\mathcal{P}}(y) = -\frac{1}{2}\text{ord}_{\mathcal{P}}(x) = 1.$$

A P pont képe a lemma leképezésénél éppen $1 - x/y$, ami így nincs benne $(1 + \mathcal{P}^2\mathcal{O}_{F,\mathcal{P}})$ -ben, azaz a lemma leképezése injektív. A $\mathcal{P}$ -adikus logaritmus és exponenciális leképezések miatt

$$(1 + \mathcal{P}\mathcal{O}_{F,\mathcal{P}})/(1 + \mathcal{P}^2\mathcal{O}_{F,\mathcal{P}}) \cong \mathcal{P}\mathcal{O}_{F,\mathcal{P}}/\mathcal{P}^2\mathcal{O}_{F,\mathcal{P}} \cong \mathcal{O}_{F,\mathcal{P}}/\mathcal{P}\mathcal{O}_{F,\mathcal{P}} \cong \mathcal{O}_F/\mathcal{P} \cong \mathcal{O}/\mathfrak{p},$$

ahol az utolsó lépésben kihasználtuk, hogy $\mathfrak{p}$ teljesen elágazik. Vagyis (3.3. állítás miatt) mindkét oldal rendje $\mathbf{N}\mathfrak{p}$, tehát izomorfizmus a lemma leképezése. A Δ -ekvivariancia világos a definícióból. $\square$

8.3. Definíció. Defináljuk a

$$\delta : \mathcal{O}_{F,\mathcal{P}}^\times \rightarrow E[\mathfrak{p}]$$

leképezést, mint az

$$\mathcal{O}_{F,\mathcal{P}}^\times \cong \mathbb{F}_{p^k}^\times \times (1 + \mathcal{P}\mathcal{O}_{F,\mathcal{P}}) \rightarrow (1 + \mathcal{P}\mathcal{O}_{F,\mathcal{P}})$$

természetes vetítés és a 8.2. lemma izomorfizmusának inverzének kompozíciója, ahol $\mathbb{F}_{p^k}$ az $\mathcal{O}_{F,\mathcal{P}}$ maradékteste.

Legyen $\mathfrak{a}$ egy 8.1. lemmát teljesítő ideál, $\Omega \in \mathbb{C}^\times$ -re legyen $L = \Omega\mathcal{O}$, f egy generátora az $\mathfrak{f}$ konduktornak. Ezekkel a választásokkal legyen $\eta_n(\mathfrak{r})$ 6.1. definíció elliptikus egységei. Legyen $\eta = \eta_1(\mathcal{O})$ globális egysége F -nek, ami függ $\mathfrak{a}$ -tól.

8.4. Állítás. $\text{ord}_{\mathfrak{p}}(L(\bar{\psi}, 1)/\Omega) \geq 0$ és

$$L(\bar{\psi}, 1)/\Omega \equiv 0 \pmod{\mathfrak{p}} \Leftrightarrow \delta(\eta) = 0.$$

Bizonyítás. Legyen $P = (\wp(\Omega/\psi(\mathfrak{p}); L), \wp'(\Omega/\psi(\mathfrak{p}); L)/2)$. Ekkor $P \in E[\mathfrak{p}]$, hiszen $E[\mathfrak{p}] \cong \mathfrak{p}^{-1}L/L$ és $\psi(\mathfrak{p})\mathcal{O} = \mathfrak{p}$. Legyen $z = -x(P)/y(P) \in \mathcal{P}$ a P képe $\hat{E}[\mathfrak{p}]$ -ben. Ekkor $\eta = \eta_1(\mathcal{O}) = \Lambda_{E,\mathfrak{a}}(P) = \Lambda_{\mathfrak{p},\mathfrak{a}}(z)$, ahol $\Lambda_{\mathfrak{p},\mathfrak{a}}$ az 5.21. definíció hatványsora.

Az 5.22. tétel szerint $\Lambda_{\mathfrak{p},\mathfrak{a}}(0) \in \mathcal{O}_{\mathfrak{p}}^\times$ és $D \log \Lambda_{\mathfrak{p},\mathfrak{a}}(Z) \big|_{Z=0} = 12f(\mathbf{N}\mathfrak{a} - \psi(\mathfrak{a}))(L(\bar{\psi}, 1)/\Omega)$. Mivel $\lambda'_{\hat{E}}(0) = 1$, ezért

$$\begin{aligned} D \log \Lambda_{\mathfrak{p},\mathfrak{a}}(Z) \big|_{Z=0} &= \frac{1}{\lambda'_{\hat{E}}(Z)} \frac{d}{dZ} \log \Lambda_{\mathfrak{p},\mathfrak{a}}(Z) \big|_{Z=0} = \frac{\frac{d}{dZ} \Lambda_{\mathfrak{p},\mathfrak{a}}(Z)}{\Lambda_{\mathfrak{p},\mathfrak{a}}(Z)} \bigg|_{Z=0} = \\ &= \frac{\Lambda_{\mathfrak{p},\mathfrak{a}} \text{ hatványsorban } Z \text{ együtthatója}}{\Lambda_{\mathfrak{p},\mathfrak{a}}(0)}. \end{aligned}$$

Tehát $\Lambda_{\mathfrak{p},\mathfrak{a}}(z)$ modulo $\mathcal{P}^2$ könnyen számolható, mert csak az első két tag számít, azaz

$$\begin{aligned} \eta &\equiv \Lambda_{\mathfrak{p},\mathfrak{a}}(0) + z \frac{d}{dZ} \Lambda_{\mathfrak{p},\mathfrak{a}}(Z) \big|_{Z=0} = \Lambda_{\mathfrak{p},\mathfrak{a}}(0)(1 + z D \log \Lambda_{\mathfrak{p},\mathfrak{a}}(Z) \big|_{Z=0}) = \\ &= \Lambda_{\mathfrak{p},\mathfrak{a}}(0)(1 + 12f(\mathbf{N}\mathfrak{a} - \psi(\mathfrak{a}))(L(\bar{\psi}, 1)/\Omega)z) \pmod{\mathcal{P}^2}. \end{aligned}$$

Tehát mivel hasonlóan $\eta \equiv \Lambda_{\mathfrak{p},\mathfrak{a}}(0) \pmod{\mathcal{P}}$, ezért

$$\delta(\eta) = 12f(\mathbf{N}\mathfrak{a} - \psi(\mathfrak{a}))(L(\bar{\psi}, 1)/\Omega)P.$$

Az $\mathfrak{a}$ ideál választása miatt $\text{ord}_{\mathfrak{p}}(12f(\mathbf{N}\mathfrak{a} - \psi(\mathfrak{a}))) = 0$. $P \neq \mathcal{O}$, mert $\Omega/\psi(\mathfrak{p}) \notin \Omega\mathcal{O} = L$, tehát ha $\delta(\eta) = 0$, akkor $1 \leq \text{ord}_{\mathfrak{p}}(12f(\mathbf{N}\mathfrak{a} - \psi(\mathfrak{a}))(L(\bar{\psi}, 1)/\Omega)) = \text{ord}_{\mathfrak{p}}(L(\bar{\psi}, 1)/\Omega)$, mert $P \in E[\mathfrak{p}]$. Ha $\delta(\eta) \neq 0$, akkor

$$0 = \pi\delta(\eta) = 12f(\mathbf{N}\mathfrak{a} - \psi(\mathfrak{a})) \left(\pi \frac{L(\bar{\psi}, 1)}{\Omega} \right) P,$$

ahol π generátora $\mathfrak{p}$ -nek, tehát

$$1 \leq \text{ord}_{\mathfrak{p}}(12f(\mathbf{N}\mathfrak{a} - \psi(\mathfrak{a}))(\pi L(\bar{\psi}, 1)/\Omega)) = 1 + \text{ord}_{\mathfrak{p}}(L(\bar{\psi}, 1)/\Omega),$$

mert $P \in E[\mathfrak{p}]$, tehát $L(\bar{\psi}, 1)/\Omega \in \mathcal{O}_{\mathfrak{p}}$, és ha $\delta(\eta) \neq 0$, akkor

$$0 = \text{ord}_{\mathfrak{p}}(12f(\mathbf{N}\mathfrak{a} - \psi(\mathfrak{a}))(L(\bar{\psi}, 1)/\Omega)) = \text{ord}_{\mathfrak{p}}(L(\bar{\psi}, 1)/\Omega)$$

is teljesül. □

8.5. Definíció. Legyen χ_E a Δ reprezentációja $E[\mathfrak{p}]$ -n. A 3.19. következmény (ii) része miatt χ_E $\mathbb{F}_p$ -irreducibilis (mert $\mathcal{O}/\mathfrak{p}$ testnek nincs $(\mathcal{O}/\mathfrak{p})^\times$ -invariáns nemtriviális altere), tehát $E[\mathfrak{p}] \cong R_{\chi_E}/\mathfrak{p}R_{\chi_E}$, mint Δ -modulusok.

8.6. Tétel. Tegyük fel, hogy $L(\bar{\psi}, 1)/\Omega$ egység $\mathfrak{p}$ -nél. Ekkor

$$A^{\chi_E} = 0.$$

Bizonyítás. Mivel δ Δ -ekvivariáns és $E[\mathfrak{p}]^\chi = 0$ minden $\chi_E \neq \chi \in \Xi$ reprezentációra, ezért

$$\delta(\eta^{\chi_E}) = \delta(\eta)^{\chi_E} = \delta(\eta) \neq 0,$$

ahol az utolsó lépésben kihasználtuk 8.4. állítást. A binomiális tétel miatt teljesül $(1 + \mathcal{P}\mathcal{O}_{F,\mathcal{P}})^p \subset (1 + \mathcal{P}^2\mathcal{O}_{F,\mathcal{P}})$, tehát $((\mathcal{O}_{F,\mathcal{P}}^\times)^{\chi_E})^p \subset \ker \delta$, speciálisan

$$\eta^{\chi_E} \notin ((\mathcal{O}_F^\times)^{\chi_E})^p.$$

Tegyük fel, hogy $\mu_F^{\chi_E}$ nemtriviális. Ekkor létezik G_K -ekvivariáns $E[p] \rightarrow \mu_p$ homomorfizmus. A Weil párosítás (ld. [Sil09] III. 8.1 állítás) ad egy $E[p] \cong \text{Hom}(E[p], \mu_p)$ Galois-ekvivariáns izomorfizmust. Tehát $E[p]^{G_K}$ nemtriviális, ami azonban ellentmond a 3.17. következménynek, tehát $\mu_F^{\chi_E}$ triviális. A tétel következik a 7.7. következményből. $\square$

8.7. Lemma. Tegyük fel, hogy p két prímre bomlik fel K -ban és $\text{Tr}_{K/\mathbb{Q}}\psi(\mathfrak{p}) \neq 1$. Ekkor

$$(i) \mu_p \not\subset F_{\mathcal{P}},$$

$$(ii) (\mathcal{O}_{F,\mathcal{P}}^\times)^\chi \text{ szabad 1-rangú } R_{\chi_E} \text{ felett.}$$

Bizonyítás. [Rub99] 10.9 lemma. $\square$

8.8. Tétel. Tegyük fel, hogy $L(\bar{\psi}, 1)/\Omega$ egység $\mathfrak{p}$ -nél, p két prímre bomlik fel K -ban és $\text{Tr}_{K/\mathbb{Q}}\psi(\mathfrak{p}) \neq 1$. Ekkor a természetes (injektív)

$$(\mathcal{O}_F^\times)^{\chi_E} \rightarrow (\mathcal{O}_{F,\mathcal{P}}^\times)^{\chi_E}$$

leképezés szürjektív is.

Bizonyítás. Mint ahogy a 8.6. tételnél, így itt is $\delta(\eta^{\chi_E}) = \delta(\eta)$ és $\eta^{\chi_E} \notin ((\mathcal{O}_{F,\mathcal{P}}^\times)^{\chi_E})^p$, tehát $(\mathcal{O}_F^\times)^{\chi_E} \not\subset ((\mathcal{O}_{F,\mathcal{P}}^\times)^{\chi_E})^p$. A 7.1. lemma szerint $(\mathcal{O}_F^\times/\mu_F)^{\chi_E}$ szabad 1-rangú R_{χ_E} -modulus és $\mu_F^{\chi_E}$ triviális, tehát $(\mathcal{O}_F^\times)^{\chi_E}$ is szabad 1-rangú R_{χ_E} -modulus. Az

$$(\mathcal{O}_F^\times)^{\chi_E} \rightarrow (\mathcal{O}_{F,\mathcal{P}}^\times)^{\chi_E}$$

leképezés képe valamilyen m p -hatványra izomorf mR_{χ_E} -vel. De 8.7. lemma (ii) része és $(\mathcal{O}_F^\times)^{\chi_E} \not\subset ((\mathcal{O}_{F,\mathcal{P}}^\times)^{\chi_E})^p$ miatt $m = 1$, azaz a beágyazás szürjektív. $\square$

8.9. Tétel (Coates, Wiles). Ha $L(\bar{\psi}, 1) \neq 0$, akkor $E(K)$ véges.

Bizonyítás. A Csebotarev sűrűségi tétel miatt található végtelen sok prím, amik teljesen felbomlanak K -ban és $\text{Tr}_{K/\mathbb{Q}}\psi(\mathfrak{p}) \neq 1$. Válasszunk egy olyat, ami nem osztja $2 \cdot 3 \cdot 5 \cdot 7 \cdot \mathfrak{f} \cdot L(\bar{\psi}, 1)$ -et. A 4.10. következményt akarjuk használni. Egyrészt 8.6. tétel szerint $A^{\chi_E} = 0$, amiből következik, hogy $\text{Hom}(A, E[\mathfrak{p}])^\Delta = 0$. Másrészt δ_1 egy Δ -ekvivariáns leképezés, tehát $\delta_1((\mathcal{O}_{F,\mathcal{P}}^\times)^{\chi_E}) = E[\mathfrak{p}]$. A 8.8. tétel szerint $(\mathcal{O}_F^\times)^{\chi_E} \cong (\mathcal{O}_{F,\mathcal{P}}^\times)^{\chi_E}$, azaz $\delta_1((\mathcal{O}_F^\times)^{\chi_E}) = E[\mathfrak{p}]$, speciálisan $\delta_1(\mathcal{O}_F^\times) \neq 0$. Tehát $\mathcal{S}_{\psi(\mathfrak{p})}(E) = 0$, vagyis a 2.46. állítás miatt $E(K)/\mathfrak{p}E(K) = 0$. A 2.44. Mordell-Weil tételből következik, hogy $E(K)$ véges. $\square$

Hivatkozások

- [CF67] J.W.S. Cassels and A. Fröhlich. *Algebraic Number Theory: Proceedings of an Instructional Conference organized by the London Mathematical Society*. Thompson Book Company, 1967.
- [CW77] J Coates and A Wiles. On the conjecture of Birch and Swinnerton-Dyer. *Inventiones mathematicae*, 39(3):223–251, October 1977.
- [Dao17] Alexandre Daoud. The Coates-Wiles Theorem. Master’s thesis, University of Cambridge, 2017. <http://www.p-adic.com/Coates-Wiles.pdf>.
- [Mil06] J.S. Milne. *Elliptic Curves*. BookSurge Publishers, 2006. <https://jmilne.org/math/Books/ectext6.pdf>.
- [Mil20] J.S. Milne. Class field theory (v4.03), 2020. <https://jmilne.org/math/CourseNotes/CFT.pdf>.
- [Rub91] Karl Rubin. The "main conjectures" of Iwasawa theory for imaginary quadratic fields. *Inventiones mathematicae*, 103(1):25–68, 1991.
- [Rub99] Karl Rubin. *Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer*, pages 167–234. Springer Berlin Heidelberg, Berlin, Heidelberg, 1999. <https://swc-math.github.io/aws/1999/99RubinCM.pdf>.
- [Sha] Romyar T. Sharifi. Group and Galois cohomology. <https://www.math.ucla.edu/~sharifi/groupcoh.pdf>.
- [Shi71] Gorō Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions*. Princeton University Press, 1971.
- [Shu22] Jerry Shurman. Hecke characters classically and idèlically, 2022. <https://people.reed.edu/~jerry/361/lectures/heckechar.pdf>.
- [Sil09] Joseph H Silverman. *The Arithmetic of Elliptic Curves*. Graduate texts in mathematics. Springer, Dordrecht, 2009.
- [Zá20] Gergely Zábrádi. Algebrai számelmélet jegyzet, 2020. <https://zabradi.web.elte.hu/Jegyzetek/algyszamjegyzet.pdf>.

Nyilatkozat mesterséges intelligencia használatáról

Alulírott Márton Dénes nyilatkozom, hogy szakdolgozatom elkészítése során nem használtam MI alapú eszközöket.

Kelt:.....2025.06.02.

Aláírás:.....Márton Dénes