NYILATKOZAT

Név: Nagygyörgyi Bálint
ELTE Természettudományi Kar, szak: Matematikus MSc
NEPTUN azonosító: HE20WC
Diplomamunka címe: A Selmer- és Tate-Safarevich csoport

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

Budapest, 2023. 06. 07

a hallgató aláírása

Eötvös Loránd Tudományegyetem

Természettudományi Kar

Mogyorósi Bálint

A Selmer- és a Tate-Safarevich csoport

Diplomamunka

Matematikus MSc

Témavezető:

dr. Zábrádi Gergely

Algebra és Számelmélet Tanszék

Budapest, 2023

Köszönet nyilvánítás

Szeretnék ezúton is köszönetet mondani a témavezetőmnek, dr. Zábrádi Gergelynek, hogy megismertette velem ezt a témát, a rendszeres konzultációkat valamint, hogy hasznos észrevételekkel, tanácsokkal látott el a szakdolgozatom elkészítése során.

Tartalomjegyzék

Jelölések **4**

Bevezetés **5**

1. Elliptikus görbék bevezető elmélete avagy Geometria és Aritmetika **6**
1.1. Racionális pontok 6
1.2. Harmadfokú görbék geometriája 7
1.3. Weierstrass Normalizált alak 8
1.4. Explicit képletek elliptikus görbén a csoport szabályra 8
1.5. Elliptikus görbék redukciója modulo p 10

2. Elliptikus görbék aritmetikája **13**
2.1. Csoport kohomológia 13
2.2. Végtelen Galois csoportok kohomológiája 16
2.3. A Selmer és Tate-Shafarevich csoportok 20

3. Selmer csoport végessége **22**
3.1. Előkészületek 22
3.2. Végesség egy speciális esetben 24
3.3. Az általános eset bizonyítása 25
3.4. Magasságok; a véges bázis tétel bizonyításának befejezése 29

4. A rang számolása **42**
4.1. Rang számítása általános esetben 42
4.2. Rang explicit számolása 44

Jelölések

E	Elliptikus görbe
$\bar{E}$	mod p redukált elliptikus görbe
$\bar{E}^{ns}$	redukált elliptikus görbe nemszinguláris része
$\mathbb{Q}_p$	p-adikus számok teste
$K, \mathbb{K}$	$\mathbb{Q}$ véges testbővítése, számtest
$\mathcal{O}_K$	K számtestben az egészek gyűrűje
$S^{(n)}(E/\mathbb{Q})$	Selmer csoport
$Ш(E/\mathbb{Q})$	Tate-Shafarevich csoport
$H^1(G, M)$	Első csoport-kohomológia csoport
$\mathbb{P}^n(K)$	K test feletti projektív n-dimenziós tér

Bevezetés

Diophantikus egyenleteknek a racionális (vagy egész) együtthatós polinomegyenleteket nevezzük, melyeknek racionális (vagy egész) megoldásait keressük. Ezek megoldása mindig is foglalkoztatta a matematikus társadalmat. Bevezető számelméleten megtanuljuk, hogy az $ax + by = c$ típusú egyenleteknek mikor van megoldása az egészek között; ezt követően lineáris algebrából, hogy egyenletrendszereket mikor tudunk megoldani. A következő nehézségi szint, amikor homogén másodfokú egyenleteknek keressük a megoldását. Ezek a kúpszeletek, azaz a 0-génuszú görbék, amikre a Hasse-Minkowski tétel ad választ, mely szerint akkor és csak akkor létezik racionális megoldás, ha a valós és p-adikus számtestek felett mind létezik megoldás. Ezt nevezik globális-lokális elvnek is. Speciálisan ha egy 0 génuszú görbének van racionális pontja, akkor végtelen sok racionális pontja van. A másik extrém esetet, mikor a görbe génusza 1-nél nagyobb. Erre vonatkozik Faltings (híres és mély) tétele, mely szerint ezen görbéken mindig csak véges sok racionális pont van. A közbülső esettel elérkeztünk az elliptikus görbékhez, amik az 1 génuszú görbék, melyeken van racionális pont. Itt létezik ellenpélda, ahol a globális-lokális elv sérül, ezért más eszközökhöz kell fordulnunk. Viszont ebben az 1-génuszú esetben van egy csoportstruktúra a görbén, ami egy természetes eszköz a megoldások megadására, ennek megértése alapvető fontosságú. Diplomamunkámban ezzel foglalkozom: belátom a Mordell–Weil tételt, azaz, hogy tetszőleges számtest felett a megoldáshalmazunk egy végesen generált Abel-csoport.

1. fejezet

Elliptikus görbék bevezető elmélete avagy Geometria és Aritmetika

1.1. Racionális pontok

A síkunkon egy pontot racionálisnak nevezünk, ha mindkét koordinátája racionális szám. Egy egyenest racionális egyenesnek hívunk, ha az egyenes egyenletét fel tudjuk írni racionális számokkal, azaz:

$$ax + by + c = 0$$

$a, b, c \in \mathbb{Q}$. Azt a tényt könnyen láthatjuk, hogyha van két racionális pontunk, akkor a rajtuk átmenő egyenes racionális egyenes lesz, egyszerűen csak fel kell írni az egyenes egyenletét. Ha van két racionális egyenesünk és nekik van közös pontjuk, akkor ez a pont racionális lesz: ezt abból láthatjuk, hogy egy egyenletrendszert oldunk meg, aminek racionális együtthatói vannak, így csak racionális eredményt kaphatunk.

Minket a görbéken lévő racionális pontok fognak érdekelni, az előzőekhez hasonlóan definiáljuk a racionális kúpot, legyen

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

a kúpunk egyenlete, akkor hívjuk racionálisnak, ha minden együtthatója racionális. A kúpnak szeretnénk nézni a metszetét egy racionális egyenessel. Ekkor az egyenletek megoldása során egy másodfokú egyenletet kapunk, aminek két megoldása lesz, de nem szükségszerűen lesznek a megoldásai racionálisak. Azonban ha tudjuk, hogy az egyik az, akkor a

másik is, ez a Viéte formulák miatt van.

1.2. Harmadfokú görbék geometriája

Harmadfokú görbének hívjuk a következőt

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + jx + iy + j = 0.$$

Azt mondjuk, hogy a harmadfokú görbe racionális ha az együtthatói racionálisak.
Egy egyenes a görbénket 3 pontban fogja metszeni, ezt kihasználva ha tudunk két racionális pontot a görbénken akkor az őket összekötő egyenesen lesz még egy harmadik racionális pont ami a görbénken is rajta van. Ez azért van így, mert amikor felírjuk az egyenleteket egy harmadfokú polinomunk lesz, aminek két gyökéről tudjuk, hogy racionális így a harmadik is az kell, hogy legyen.
Ezzel egy műveletet kapunk a görbénk racionális pontjainak halmazán ami két ponthoz rendel egy harmadikat amit $P*Q$ jelölünk, de ez még önmagában nem lesz csoportművelet mert nem szükségszerűen lesz egységelemünk.

Ahhoz, hogy ebből csoportműveletet csináljunk kicsit módosítanunk kell illetve kelleni fog találni egy racionális pontot a görbénken amit rögzítünk. A rögzített racionális pontunkat jelölje $\mathfrak{O}$. Ekkor P és Q pontunkhoz rendeljük hozzá $P * Q$ pontot, ezután nézzük a $(P * Q) * \mathfrak{O}$ pontot, ezt definiáljuk $P + Q$-nak. Ezzel már egy csoportműveletet definiáltunk aminek egységeleme $\mathfrak{O}$, valamint kommutatív is. Az inverzét a következő képpen kapjuk meg, vegyük $\mathfrak{O} * \mathfrak{O}$ pontot, ez legyen S. Q inverze a $-Q = Q * S$ pont lesz, hiszen $-Q + Q = (-Q * Q) * \mathfrak{O} = (S) * \mathfrak{O} = \mathfrak{O}$, első lépésben a $-Q$ Q egyenesen a 3.pont S lesz a konstrukció miatt, de S és a kitüntetett pontunk egyenesén megint a kitüntetett pont lesz a 3. hisz S-et így definiáltuk.
Az asszociativitás is hasonló geometriai okoskodással kijön.

1.3. Weierstrass Normalizált alak

1.3.1. Definíció. A K test projektív síkját, az $(a : b : c) \in K^3$ hármasok halmazának definiáljuk azokkal a kitételekkel, hogy
(1) két pont ekvivalensnek tekintünk $(a : b : c) \sim (a' : b' : c')$, ha $\exists t \in K^\times : a' = at$, $b' = bt$, $c' = ct$
(2) $(0 : 0 : 0)$ pontot nem vesszük be a projektív síkunkba.

1.3.2. Definíció. Egy nemszinguláris projektív harmad fokú egy génuszú görbét aminek van legalább egy racionális pontja, elliptikus görbének nevezzük.

Tegyük fel, hogy van egy harmadfokú görbénk a projektív síkon valamint a kitüntetett $\mathfrak{O}$ pont, azt fogjuk megvalósítani, hogy úgy választjuk meg a tengelyeinket, hogy a görbénk egyenlete minél egyszerűbb legyen.
A $Z = 0$ tengelyt válasszuk a görbe $\mathfrak{O}$-beli érintőjének ez az egyenes még egy pontban metszi a görbénket, az itt lévő érintő lesz az $X = 0$ tengely, végül $Y = 0$ egy tetszőleges $\mathfrak{O}$-en átmenő egyenes ami nem a $Z = 0$.
Ezután ha áttérünk affin koordinátákra az $x = X/Z$ és $y = Y/Z$ megfeleltetésekkel, az egyenletünk a következő alakot ölti:

$$xy^2 + (ax + b)y = cx^2 + dx + e$$

ezután végig szorozva x-szel valamint az $y = xy$ helyettesítéssel élve:

$$y^2 + (ax + b)y = f(x)$$

ahol, $deg(f(x)) = 3$, ha $f(x)$ főegyütthatója nem 1 akkor helyettesítsük az x és y változókat λx illetve $\lambda^2 y$ változókkal, így az egyenletünk Weierstrass alakja:

$$y^2 = x^3 + ax^2 + bx + c$$

.

1.4. Explicit képletek elliptikus görbén a csoport szabályra

$$E : y^2 = x^3 + ax^2 + bx + c$$

A fenti egyenletet szeretnénk homogenizálni, $x = X/Z$ és $y = Y/Z$:

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3$$

Keressük a görbénk és a $Z = 0$ (végtelen beli) egyenes metszetét, vagyis a $X^3 = 0$ egyenlet megoldásait. Vagyis a görbénknek pontosan egy pontja lesz a végtelenben, az a pont ahol a függőleges egyenesek metszik egymást, ezt a pontot fogjuk mi $\mathfrak{O}$ pontnak választani.
Össze szeretnénk adni $P_1 = (x_1, y_1)$ illetve $P_2 = (x_2, y_2)$ pontokat. Első lépésben húzunk rajta egy egyenest és megkeressük a 3. metszéspontot, ez lesz $P_1 * P_2 = (x_3, y_3)$. Az $\mathfrak{O}$ választása miatt $P_1 + P_2$ a $P_1 * P_2$-nak az $x = 0$ egyenesre vett tükörképe lesz, mert $\mathfrak{O}$-ban a függőleges egyenesek találkoznak vagyis 3.metszépont az $\mathfrak{O}$ és $P_1 * P_2 = (x_3, y_3)$ által feszített egyenesen és a görbe metszete lesz de a görbénk szimmetrikus $x = 0$-ra így valóban a tükörképe lesz, koordinátákkal kifejezve $P_1 + P_2 = (x_3, -y_3)$. Tehát, hogy tudjuk számolni $P_1 + P_2$ elég $P_1 * P_2$ koordinátáját tudni.
A P_1 és P_2 pontok által feszített egyenes egyenlete:

$$y = \lambda x + \nu \text{ , ahol } \lambda = \frac{y_2 - y_1}{x_2 - x_1} \text{ és } \nu = y_1 - \lambda x_1 = y_2 - \lambda x_2.$$

A konstrukció miatt tudjuk, hogy a görbénk P_1-ben és P_2-ben metszi az egyenesünket, a harmadik pontot úgy kaphatjuk meg, hogy az egyenes egyenletét be helyettesítjük a görbénk egyenletébe:

$$y^2 = (\lambda x + \nu)^2 = x^3 + ax^2 + bx + c$$

Tudjuk, hogy van két racionális gyöke így a harmadik is az kell legyen vagyis van gyöktényezős alakja $\mathbb{Q}$ test felett, rendezve az egyenletet kapjuk:

$$0 = x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2) = (x - x_1)(x - x_2)(x - x_3).$$

Nézzük meg mindkét oldalt x^2 együtthatóját, ebből kapjuk, hogy:

$$a - \lambda^2 = -x_1 - x_2 - x_3$$

ezt rendezve valamint felhasználva az egyenes egyenletét:

$$x_3 = \lambda^2 - a - x_1 - x_2 \qquad y_3 = \lambda x_3 + \nu.$$

Ezzel a $P_1 + P_2$ koordinátái:

$$(\lambda^2 - a - x_1 - x_2, -\lambda(\lambda^2 - a - x_1 - x_2) - \nu)$$

1.5. Elliptikus görbék redukciója modulo p

Vegyünk egy elliptikus görbét:

$$E : Y^2Z = X^3 + aX^2Z + bXZ^2 + bZ^3, \quad a, b \in \mathbb{Q}, \quad \Delta = 4a^3 + 27b^2 \neq 0.$$

Változók cseréje után $X \mapsto X/c^2$, $Y \mapsto Y/c^3$ ahol $c \in \mathbb{Q}$ számot úgy választjuk, hogy az új a, b együtthatók egészek legyenek ezután vehetjük őket modulo p így kapunk egy görbét $\overline{E}$ az $\mathbb{F}_p$ test felett.

Egy dimenziós algebrai csoportok

Legyen k egy tökéletes test. A következő az irreducibilis algebrai görbék listája melyek rendelkeznek csoport struktúrával amit reguláris leképezések definiálnak.

Elliptikus görbék

Ezek az egyetlen irreducibilis projektív görbék amiknek a csoport struktúráját polinomok adják meg.

Additív csoport

Legyen $\mathbb{A}^1$ az affin egyenes, ez egy csoport az összeadásra nézve,

$$\mathbb{A}^1(k) = k, \quad (x, y) \mapsto x + y : k \times k \to k.$$

$\mathbb{A}^1$ teret ezzel a csoportstruktúrával ellátva $\mathbb{G}_a$ jelöljük.

Multiplikatív csoport

Vegyük az affin egyenest az origó nélkül, ez egy csoport lesz a szorzásra nézve:

$$\mathbb{A}^1(k)\backslash\{0\} = k^\times, \quad (x, y) \mapsto x \cdot y : k^\times \times k^\times \to k^\times.$$

$\mathbb{G}_m$ jelöljük $\mathbb{A}^1(k)\backslash\{0\}$ halmazt ellátva ezzel a csoport struktúrával. Az $x \mapsto (x, x^{-1})$ azonosítja a $\mathbb{G}_m$ csoportot az $XY = 1$ affin görbével.

Csavart multiplikatív csoport

Legyen a egy nemnégyzet elem $k^\times$ testben, és legyen $L = k[\sqrt{a}]$. Ekkor létezik egy algebrai csoport $\mathbb{G}_m[a]$ k felett, amire:

$$\mathbb{G}_m[a](k) = \{\gamma \in L^\times | \mathrm{Nm}_{L/k}\gamma = 1\}.$$

Legyen $\alpha = \sqrt{a}$, így $\{1, \alpha\}$ egy bázisa L testnek mint k vektortér. Ekkor

$$(x + \alpha y)(x' + \alpha y') = xx' + ayy' + \alpha(xy' + x'y)$$

és

$$\mathrm{Nm}(x + \alpha y) = (x + \alpha y)(x - \alpha y) = x^2 - ay^2.$$

$\mathbb{G}_m[a]$ csoportot az $X^2 - aY^2 = 1$ affin síkgörbének definiáljuk a:

$$(x, y) \cdot (x', y') = (xx' + ayy', xy' + x'y)$$

csoport struktúrával.

Elliptikus görbék redukciója

Vegyünk egy elliptikus görbét:

$$E : Y^2Z = X^3 + aX^2Z + bXZ^2 + bZ^3, \quad a, b \in \mathbb{Q}, \quad \Delta = 4a^3 + 27b^2 \neq 0.$$

Változók cseréje után $X \mapsto X/c^2$, $Y \mapsto Y/c^3$ ahol c számot úgy választjuk, hogy az új a, b együtthatók egészek legyenek és $|\Delta|$ minimális; ekkor az egyenletet minimálisnak nevezzük. Ekkor E redukciója egy p prímre:

$$\overline{E} : Y^2Z = X^3 + \overline{a}XZ^2 + \overline{b}Z^3$$

ahol $\overline{a}, \overline{b}$ az a és b egészek képei $\mathbb{F}_p$ testben. Három esetet különböztetünk meg:

(a) **Jó redukció.** Ha $p \neq 2$ és p nem osztja Δ, ekkor $\overline{E}$ egy elliptikus görbe $\mathbb{F}_p$ test felett. Egy $P = (x : y : z) \in E$ ponthoz választhatunk olyan reprezentáns hogy $x, y, z \in \mathbb{Z}$ és nincs közös osztójuk, ekkor $\overline{P} \overset{\text{def}}{=} (\overline{x} : \overline{y} : \overline{z})$ egy jóldefiniált pont $\overline{E}$ görbén. Mivel $(0 : 1 : 0)$ a $(0 : 1 : 0)$ pontba képződik és egyenesek redukciója egyenes, így a $E(\mathbb{Q}) \to \overline{E}(\mathbb{F}_p)$ egy homomorfizmus.

(b) **Csúcsos, vagy additív redukció.** Ebben az esetben $\overline{E}$ van egy csúcsa, és $\overline{E}^{\text{ns}} \cong \mathbb{G}_a$. Ha $p \neq 2, 3$ ez pontosan akkor fordul elő ha $p|4a^3 + 27b^2$ és $p| - 2ab$.

(c) **Csomó ponti, vagy multiplikatív redukció.** Ha $p \neq 2, 3$ pontosan akkor fordul elő, ha $p|4a^3 + 27b^2$ és p nem osztja $-2ab$. A tangensek a csomópontban racionálisak $\mathbb{F}_p$ felett akkor és csak akkor ha $-2ab$ négyzet $\mathbb{F}_p$ testben és ebben az esetben $\overline{E}^{\text{ns}} \cong \mathbb{G}_m$ és azt mondjuk, hogy E görbének hasadó multiplikatív redukciója van. Másfelől ha $-2ab$ nem négyzet, akkor $\overline{E}^{\text{ns}} \cong \mathbb{G}_m[-2\overline{ab}]$ és E elliptikus görbének ekkor nemhasadó multiplikatív redukciója van.

2. fejezet

Elliptikus görbék aritmetikája

A következő két fejezetben belátjuk az általános véges bázis tételt Elliptikus görbékre.

2.0.1. Tétel. *Legyen E elliptikus görbe a K számtest felett ekkor $E(K)$ egy végesen generált csoport lesz.*

2.1. Csoport kohomológia

2.1.1. Definíció. Véges csoport kohomológiája:
Legyen G véges csoport, és legyen M Abel csoport. A G csoport hatása M-en egy leképezés $G \times M \to M$, úgy hogy:
(a) $\sigma(m + m') = \sigma m + \sigma m'$ minden $\sigma \in G$, $m, m' \in M$
(b) $\sigma(\tau m) = \sigma(\tau m)$ minden $\sigma, \tau \in G$, $m \in M$
(c) $1_G m = m$ minden $m \in M$

2.1.2. Példa. Legyen L egy véges Galois bővítése a K testnek G Galois csoporttal, és legyen E egy elliptikus görbe K felett. Ekkor L, $L^\times$ és $E(L)$ mind rendelkezik egy természetes G-hatással.
Egy M G-modulusra, definiáljuk

$$H^0(G, M) = M^G = \{m \in M | \sigma m = m, \forall \sigma \in G\}.$$

A fenti példákra,

$$H^0(G, L) = K,\ H^0(G, L^\times) = K^\times \text{ és } H^0(G, E(L)) = E(K).$$

2.1.3. Definíció. Egy $f : G \to M$ homomorfizmust keresztezett homomorfizmusnak hívunk ha teljesül rá a következő azonosság:

$$f(\sigma\tau) = f(\sigma) + \sigma f(\tau), \forall \sigma, \tau \in G$$

Vegyük észre, hogy a feltétel implikálja $f(1) = f(1 \cdot 1) = f(1) + f(1)$, azaz $f(1) = 0$. Minden $m \in M$ elemhez hozzárendelhetünk egy keresztezett homomorfizmust a következő képpen:

$$f(\sigma) = \sigma m - m, \ \forall \sigma \in G.$$

Ilyen típusú keresztezett homomorfizmusokat principálisnak nevezzük. Összege és különbsége keresztezett és principális homomorfizmusoknak keresztezett illetve principális homomorfizmus. Így definiálhatjuk a következő csoportot:

$$H^1(G, M) = \frac{\{\text{keresztezett homomorfizmus}\}}{\{\text{principális keresztezett homomorfizmus}\}}$$

2.1.4. Példa. Ha G triviálisan hat M Abel csoporton, azaz $\sigma m = m$ minden $\sigma \in G$ és $m \in M$, akkor a keresztezett homomorfizmus egyszerűen egy homomorfizmus és minden principális keresztezett homomorfizmus nulla. Így a $H^1(G, M) = \mathrm{Hom}(G, M)$ csoportok azonosak.

2.1.5. Állítás. *Legyen L egy véges Galois bővítése K testnek G Galois csoporttal. Ekkor $H^1(G, L^\times) = 0$, azaz minden $G \to L^\times$ principális.*

Bizonyítás. Legyen f egy $G \to L^\times$ keresztezett homomorfizmus. Multiplikatív jelölésmódot használva, a következőt jelenti:

$$f(\sigma\tau) = f(\sigma) \cdot \sigma(f(\tau)), \quad \sigma, \tau \in G.$$

Kell egy $\gamma \in L^\times$ hogy $f(\sigma) = \sigma(\gamma)/\gamma$ minden $\sigma \in G$. Mivel $f(\tau)$ nem nulla, Dedekind karakterek lineáris függetlenségéről szóló tétele mutatja, hogy:

$$\sum_{\tau \in G} f(\tau)\tau : L \to L$$

egy nem nulla leképezés, azaz létezik egy $\alpha \in L$, hogy:

$$\beta \stackrel{def}{=} \sum_{\tau \in G} f(\tau) \cdot \tau(\alpha) \neq 0$$

Ekkor tetszőleges $\sigma \in G$ Galois hatásra:

$$\sigma(\beta) = \sum_{\tau \in G} \sigma(f(\tau)) \cdot (\sigma\tau)(\alpha)$$

$$= \sum_{\tau \in G} f(\sigma)^{-1} \cdot f(\sigma\tau) \cdot (\sigma\tau)(\alpha)$$

$$= f(\sigma)^{-1} \cdot \sum_{\tau \in G} f(\sigma\tau) \cdot (\sigma\tau)(\alpha)$$

$$= f(\sigma)^{-1} \cdot \beta$$

Ezt átrendezve kapjuk, hogy $f(\sigma) = \beta/\sigma(\beta) = \sigma(\beta^{-1})/\beta^{-1}$. $\square$

2.1.6. Következmény. *Egy $P = (x_0 : ... : x_n) \in \mathbb{P}^n(L)$ pontot a G Galois csoport fixen hagy akkor és csak akkor ha reprezentálható egy K-beli $n+1$-essel.*

Bizonyítás. Tegyük fel, hogy $\sigma P = P$ minden $\sigma \in G$. Ekkor:

$$\sigma(x_0, ..., x_n) = c(\sigma)(x_0, .., x_n).$$

Valamilyen $c(\sigma) \in L^\times$, ez ad egy $\sigma \mapsto c(\sigma)$ hozzárendelést ami egy keresztezett homomorfizmus lesz:

$$\sigma(\tau(x_0, ..., x_n)) = \sigma(c(\tau)(x_0, ..., x_n)) = \sigma(c(\tau))\sigma(x_0, ..., x_n) = \sigma(c(\tau))c(\sigma)(x_0, ..., x_n),$$

azaz $c(\sigma\tau) = \sigma(c(\tau))c(\sigma)$. Ezek mind principálisak így $c(\sigma) = c/\sigma(c)$ valami $c \in L^\times$, ezzel:

$$\sigma(cx_0, ..., cx_n) = c(\sigma)\sigma(c)(x_0, .., x_n) = c(x_0, .., x_n) = (cx_0, ..., cx_n).$$

A feltétel miatt $cx_i \in K$. $\square$

2.1.7. Állítás. *Tetszőleges G-modulusok egzakt sorozatára:*

$$0 \to M \to N \to P \to 0,$$

létezik egy kanonikus egzakt sorozat:

$$0 \to H^0(G, M) \to H^0(G, N) \to H^0(G, P) \xrightarrow{\delta}$$

$$H^1(G, M) \to H^1(G, N) \to H^1(G, P)$$

Bizonyítás. Elsőnek definiáljuk a δ leképezést a következő képpen: legyen $p \in P^G$, ehhez létezik egy $n \in N$ elem ami p-be képződik, és $\sigma n - n \in M$ minden $\sigma \in G$ csoportelemre. A $\sigma \mapsto \sigma n - n : G \to M$ egy keresztezett homomorfizmus, aminek az osztályát $\delta(p)$ definiáljuk. Egy másik n' ami p elembe képződik ugyan úgy indukál egy kersztezett homomorfizmust, ami az előzőtől $\sigma \mapsto \sigma(n - n') - (n - n^1)$ principális keresztezett homomorfizmusban tér el, így $\delta(p)$ osztály jól definiált. A bizonyítás hátralévő része hasonló módszerekkel bizonyítható. □

2.1.8. Állítás. *Ha G csoport rendje m, akkor $mH^1(g, M) = 0$.*

Bizonyítás. Általánosan ha G egy véges m indexű részcsoport, akkor létezik egy komegszorítás leképezés $Cor : H^1(H, M) \to H^1(G, M)$, hogy $Cor \circ Res = m$. Alkalmazzuk ezt a $H = 1$ részcsoportra. □

2.2. Végtelen Galois csoportok kohomológiája

Legyen k egy tökéletes test, és legyen k^{al} egy algebrai lezártja k testnek. k^{al} azon automorfizmusainak G csoportja melyek k résztestet fixen hagyják elláthető egy természetes topológiával, ahol egy részcsoport pontosan akkor nyílt ha létezik k testnek egy olyan véges bővítése melyet fixen hagy, ezt a topológiát Krull topológiának nevezzük. G csoportot együtt a Krull topológiával k^{al} k feletti Galois csoportjának hívjuk. A nyílt részcsoportok egy környezetbázisát adják 1_G csoportelemnek. Nyílt részcsoportok zártak, így nyíltak tetszőleges metszete zárt, valamint minden zárt részcsoport nyíltak metszete. A szokásos Galois elmélet végtelen Galois csoportokra is igaz marad, azaz létezik bijektív megfeleltetés K köztes testek $k \subset K \subset k^{al}$ és G zárt részcsoportjai között, miszerint k minden véges bővítésének megfelel egy nyílt részcsoport G csoportban.

Egy M G-modulust diszkrétnek nevezünk ha a $G \times M \to M$ leképezés folytonos az M moduluson a diszkrét topológiát, a G csoporton pedig a Krull topológiát véve. Ez ekvivalens a következővel:

$$M = \bigcup_H M^H \quad H \text{ nyílt } G \text{ csoportban},$$

azaz, M minden eleméjhez létezik egy G-beli részcsoport, amik fixen hagyják k valamelyik véges bővítését. Például, $M = k^{al}$, $M = k^{al\times}$ és $M = E(k^{al\times})$ mind diszkrét G-modulusok,

mert

$$k^{al} = \bigcup K, \quad {}^{al\times} = \bigcup K^{\times}, \quad E(k^{al\times}) = \bigcup E(K)$$

ahol K végigfut k összes véges bővítésén melyeket k^{al} tartalmaz.

Amikor M diszkrét, egy keresztezett homomorfizmus $f : G \to M$ folytonos akkor és csak akkor f konstans valamely H nyílt részcsoport által meghatározott mellékosztályokon, vagyis f leképezés egy inflációs leképezés azaz egy $G/H \to M$ keresztezett homomorfizmus. Minden principális keresztezett homomorfizmus folytonos ugyanis M minden eleme invariáns egy nyílt G normálosztóra.

Legyen G egy végtelen Galois csoport és M egy diszkrét G-modulus, ekkor definiálhatjuk $H^1(G, M)$ azon $f : G \to M$ azon keresztezett homomorfizmusok csoportjának amit principális keresztezett homomorfizmus faktorizálásával kapunk. Ezzel a definícióval:

$$H^1(G, M) = \varinjlim_{H \lhd G} H^1(G/H, M^H)$$

ahol H végigfut G csoport összes nyílt normálosztóján. Expliciten ez a következőt jelenti:

(a) $H^1(G, M)$ az Inf:$H^1(G/H, M^H) \to H^1(G, M)$ inflációs leképezések képeinek uniója ahol H végigfut G csoport összes nyílt normálosztóján.

(b) Egy $\gamma \in H^1(G/H, M^H)$ elem képe nulla lesz $H^1(G, M)$ csoportban akkor és csak akkor ha létezik olyan H' G-beli nyílt normálosztó, hogy $H' \subset H$ és $H^1(G/H', M^H)$ csoportban a γ képe nulla.

Speciálisan a $H^1(G, M)$ csoport torziós.

2.2.1. Példa. (a) 1.1.5 állítás miatt:

$$H^1(G, k^{al\times}) = \varinjlim_{K/k} H^1(Gal(K/k), K^{\times}) = 0$$

(b) Legyen L egy test és $n \geq 1$ egész, valamint

$$\mu_n(L) = \{\xi \in L^{\times} \xi^n = 1\}.$$

$$1 \to \mu_n(k^{al}) \to k^{al} \xrightarrow{\cdot n} k^{al} \to 1$$

A fenti egzakt sorozatból származtathatjuk a kohomológia csoportoknak a következő egzakt sorozatát:

$$1 \to \mu_n(k) \to k^\times \xrightarrow{\cdot n} k^\times \to H^1(G, \mu_n(k^{al})) \to 1$$

ami szolgáltat egy kanonikus izomorfizmust:

$$H^1(G, \mu_n(k^{al})) \cong k^\times / k^{\times n}.$$

Ha k egy szám test és $n > 1$, akkor ez a csoport végtelen. Például, a

$$(-1)^{\varepsilon(\infty)} \prod_{p \text{ prím}} p^{\varepsilon(p)}$$

ahol minden kitevő 0 vagy 1 értéket veszi fel és csak véges sok nemnulla kitevő szerepel a szorzatban, reprezentáns rendszerét adják $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, ami egy végtelen dimenziós vektortér lesz $\mathbb{F}_2$ felett.

(c) Ha a G csoport triviálisan hat az M moduluson, akkor $H^1(G, M)$ a folytonos $\alpha : G \to M$ morfizmusok halmaza. Mivel M diszkrét, a magja ezen leképezéseknek nyílt. Ha K egy rögzített test, akkor α definiál egy injektív homomorfizmust $\mathrm{Gal}(K/k) \to M$.

Egy E elliptikus görbére k test felett, $H^i(\mathrm{Gal}(k^{al}/k), E(k^{al}))$ helyett $H^i(k, E)$ rövidítést használjuk.

2.2.2. Példa. Legye E egy elliptikus görbe $\mathbb{Q}$ felett, és $\mathbb{Q}^{al}$ pedig legyen a $\mathbb{Q}$ test algebrai lezártja $\mathbb{C}$ testben, valamint válasszunk $\mathbb{Q}_p^{al}$ algebrai lezártját a $\mathbb{Q}_p$ testnek. A $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ beágyazás kiterjed egy $\mathbb{Q}^{al} \hookrightarrow \mathbb{Q}_p^{al}$ beágyazássá,

$$\begin{array}{ccc} \mathbb{Q}^{al} & \to & \mathbb{Q}_p^{al} \\ \uparrow & & \uparrow \\ \mathbb{Q} & \to & \mathbb{Q}_p \end{array}$$

$\mathrm{Gal}(\mathbb{Q}_p^{al}/\mathbb{Q}_p)$ csoport hatása a $\mathbb{Q}^{al} \subset \mathbb{Q}_p^{al}$ moduluson definiál egy

$$\mathrm{Gal}(\mathbb{Q}_p^{al}/\mathbb{Q}_p) \to \mathrm{Gal}(\mathbb{Q}^{al}/\mathbb{Q})$$

homomorfizmust.
Így tetszőleges $\mathrm{Gal}(\mathbb{Q}^{al}/\mathbb{Q}) \to E(\mathbb{Q}^{al})$ keresztezett homomorfizmus definiál egy $\mathrm{Gal}(\mathbb{Q}_p^{al}/\mathbb{Q}) \to$

$E(\mathbb{Q}_p^{al})$ keresztezett homomorfizmust. Ez az első kohomológia csoportokon is indukál egy homomorfizmust:

$$H^1(\mathbb{Q}, E) \to H^1(\mathbb{Q}_p, E)$$

ami független lesz a $\mathbb{Q}^{al} \hookrightarrow \mathbb{Q}_p^{al}$ beágyazás választásától.

2.3. A Selmer és Tate-Shafarevich csoportok

Bevezetem a következő jelölést $\mathbb{Q}_\infty = \mathbb{R}$, valamint ∞ is beleértem ha prímekre hivatkozok.

2.3.1. Lemma. *Legyen E elliptikus görbe egy k algebrailag zárt test felett, és $n \in \mathbb{Z}$ ekkor a $P \mapsto nP : E(k) \to E(k)$ leképezés szürjektív.*

Bizonyítás. A bizonyítás megtalálható [3] jegyzetben a 4. fejezetének 2.1 lemmája. □

A fenti lemma miatt a következő sorozat egzakt lesz:

$$0 \to E_n(\mathbb{Q}^{al}) \to E(\mathbb{Q}^{al}) \xrightarrow{\cdot n} E(\mathbb{Q}^{al}) \to 0$$

és ebből kapjuk a kohomológiák egzakt sorozatát:

$$0 \to E(\mathbb{Q}) \xrightarrow{\cdot n} E(\mathbb{Q}) \to H^1(\mathbb{Q}, E_n) \to H^1(\mathbb{Q}, E) \xrightarrow{\cdot n} H^1(\mathbb{Q}, E).$$

Ezt felhasználva kapjuk alábbi rövid egzakt sorozatot:

$$0 \to E(\mathbb{Q})/nE(\mathbb{Q}) \to H^1(\mathbb{Q}, E_n) \to H^1(\mathbb{Q}, E)_n \to 0.$$

$H^1(\mathbb{Q}, E)_n$ csoport $H^1(\mathbb{Q}, E)$ n. torzió csoportja. Ha a $H^1(\mathbb{Q}, E_n)$ csoport véges, akkor tudnánk hogy $E(\mathbb{Q})/nE(\mathbb{Q})$ is véges, de ez nem szükségszerű. Például ha az E összes másodrendű pontjának koordinátája $\mathbb{Q}$ testbeli, akkor $\mathrm{Gal}(\mathbb{Q}^{al}/\mathbb{Q})$ triviálisan hat $E_2(\mathbb{Q}^{al}) \cong (\mathbb{Z}/2\mathbb{Z})^2$ moduluson. Ekkor

$$H^1(\mathbb{Q}, E_2) \cong H^1(\mathbb{Q}, \mu_2 \times \mu_2) \cong (\mathbb{Q}^\times/\mathbb{Q}^{\times 2}) \times (\mathbb{Q}^\times/\mathbb{Q}^{\times 2}),$$

ami végtelen. Ehelyett a következőek szerint járunk el. Ha az E elliptikus görbénket $\mathbb{Q}_p$ felett nézzük kapunk egy hasonló egzakt sorozatot és egy kommutatív diagrammot:

$$\begin{array}{ccccccccc} 0 \to & E(\mathbb{Q})/nE(\mathbb{Q}) & \to & H^1(\mathbb{Q}, E_n) & \to & H^1(\mathbb{Q}, E)_n & \to 0 \\ & \downarrow & & \downarrow & & \downarrow & \\ 0 \to & E(\mathbb{Q}_p)/nE(\mathbb{Q}_p) & \to & H^1(\mathbb{Q}_p, E_n) & \to & H^1(\mathbb{Q}_p, E)_n & \to 0 \end{array}$$

$H^1(\mathbb{Q}, E_n)$ csoportot akarjuk helyettesíteni egy részhalmazával ami tartalmazza a $E(\mathbb{Q})/nE(\mathbb{Q})$ képét úgy hogy erről a részhalmazról be tudjuk látni, hogy véges. Következő képpen tehetjük ezt meg ha $\gamma \in H^1(\mathbb{Q}, E_n)$ egy $E(\mathbb{Q})$ csoport elem, akkor a képe $\gamma_p \in H^1(\mathbb{Q}_p, E_n)$ egy $E(\mathbb{Q}_p)$ csoport elem. Ez alapján bevezethetjük a következő definíciót:

$$S^{(n)}(E/\mathbb{Q}) = \{\gamma \in H^1(\mathbb{Q}, E_n) : \forall p, \gamma_p \ E(\mathbb{Q}_p) \text{ csoportból jön}\}$$

$$= \mathrm{Ker}\left(H^1(\mathbb{Q}, E_n) \to \prod_{\text{p prím}} H^1(\mathbb{Q}_p, E) \right)$$

Az $S^{(n)}$ csoportot Selmer csoportnak hívjuk. Ennek mintájára definiálhatjuk a Tate-Shafarevich csoportot:

$$Ш(E/\mathbb{Q}) = \mathrm{Ker}\left(H^1(\mathbb{Q}, E) \to \prod_{\text{p prím}} H^1(\mathbb{Q}_p, E) \right)$$

Ez egy torziós csoport lesz. A $Ш(E/\mathbb{Q})$ csoportnak van egy geometriai értelmezése is, amiből látható, hogy 1 génuszú görbék esetén méri a Hasse elv sérülését. Valamint látható hogy a fenti definíciók kiterjednek tetszőleges számtestek esetére.

2.3.2. Lemma. *Tetszőleges Abel csoport homomorfizmus párokra*

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C$$

létezik egy egzakt sorozat:

$$0 \to \mathrm{Ker}(\alpha) \to \mathrm{Ker}(\beta \circ \alpha) \xrightarrow{\alpha} \mathrm{Ker}(\beta) \to$$

$$\to \mathrm{Koker}(\alpha) \to \mathrm{Koker}(\beta \circ \alpha) \xrightarrow{\alpha} \mathrm{Koker}(\beta) \to 0$$

Ezt a lemmát alkalmazhatjuk az alábbi leképezésekre:

$$E(\mathbb{Q})/nE(\mathbb{Q}) \to H^1(\mathbb{Q}, E_n) \to \prod_{\text{p prím}} H^1(\mathbb{Q}_p, E)_n$$

ami a következő rövid egzakt sorozatot adja:

$$0 \to E(\mathbb{Q})/nE(\mathbb{Q}) \to S^{(n)}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q}) \to 0$$

3. fejezet

Selmer csoport végessége

Ezen fejezetben belátjuk a következő tételt:

3.0.1. Tétel. *Minden $\mathbb{Q} \leq \mathbb{K}$ számtest feletti E elliptikus görbére, és tetszőleges $n \in \mathbb{Z}$ egészre a $S^{(n)}(E/\mathbb{K})$ Selemer csoport véges.*

3.1. Előkészületek

3.1.1. Lemma. *Legyen E egy elliptikus görbe a $\mathbb{Q}_p$ test felett jó redukcióval, és legyen $n \in \mathbb{Z}\backslash p\mathbb{Z}$. Egy $E(\mathbb{Q}_p)$ modulusbeli P pont nQ alakú valamilyen $Q \in E(\mathbb{Q}_p)$ elemre akkor és csak akkor ha a képe $\overline{P} \in E(\mathbb{F}_p)$ $n\overline{Q}$ alakú valamilyen $\overline{Q} \in E(\mathbb{F}_p)$ elemre.*

Bizonyítás. Mivel $P \mapsto \overline{P}$ egy homomorfizmus, a szükségesség egyértelmű, az elégségességet pedig diagram vadászattal látjuk be:

$$\begin{array}{ccccccc} 0 \to & E^1(\mathbb{Q}_p) & \to & E(\mathbb{Q}_p) & \to & \overline{E}(\mathbb{F}_p) & \to 0 \\ & \downarrow^n & & \downarrow^n & & \downarrow^n & \\ 0 \to & E^1(\mathbb{Q}_p) & \to & E(\mathbb{Q}_p) & \to & \overline{E}(\mathbb{F}_p) & \to 0 \end{array}$$

használjuk hogy, függőleges nyilak izomorfizmusok. Részletesebben, legyen $P \in E(\mathbb{Q}_p)$ olyan pont aminek a képére teljesül: $\overline{P} = n\overline{Q}$, ekkor a $P - nQ$ $\overline{E}(\mathbb{F}_p)$ null elemébe képződik, ami egy $E^1(\mathbb{Q}_p)$ modulusbeli elem. Ezért, $P - nQ = nQ'$ valamilyen $Q' \in E^1(\mathbb{Q}_l)$ elemre azaz $P = n(Q + Q')$ $\square$

A következőkben szükségünk lesz egy kis algebrai számelméletre. Legyen K $\mathbb{Q}_p$ egy véges

bővítése, a $\mathbb{Z}_p$ egészlezártja $\mathcal{O}_K$ K testben szintén egy főideál gyűrű lesz ami lokális is azaz, (π) az egyetlen maximális ideálja. Ezért, $p = \text{egység} \times \pi^e$ valamilyen $e \in \mathbb{Z}$ elemre, ezt az egészet hívjuk a K elágazási indexének $\mathbb{Q}_p$ felett. Ha $e = 1$ akkor a maximális ideál (p), ekkor K nem elágazó $\mathbb{Q}_p$ felett.

3.1.2. Lemma. *k test $\mathbb{F}_p$ egy véges bővítése, ekkor létezik egy nem elágazó bővítése $\mathbb{Q}_p$ testnek K aminek a foka $[k : \mathbb{F}_p]$ valamint $\mathcal{O}_K/p\mathcal{O}_K = k$.*

Bizonyítás. Legyen α egy primitív eleme k testnek $\mathbb{F}_p$ felett, és legyen $f_0(X)$ az α minimál polinomja $\mathbb{F}_p$ felett, ezzel

$$k = \mathbb{F}_p[\alpha] \cong \mathbb{F}_p/(f_0(X)).$$

Minden $f(X) \in \mathbb{Z}_p[X]$ normált polinomra ami teljesíti $f_0(X) = f(X) \bmod p$ egyenletet, a test $K = \mathbb{Q}_p[X]/(f(X))$ rendelkezik a megkövetelt tulajdonságokkal. □

3.1.3. Megjegyzés. Legyen $K \supset \mathcal{O}_K \to k$ mint a lemmában. Legyen q k rendje, ekkor $X^q - X$ gyökei k testben lesznek. A Hensel lemma igaz $\mathcal{O}_K$ gyűrűre is, így $X^q - X$ minden gyöke felemelhető $\mathcal{O}_K$ gyűrűbe. Ezért K az $X^q - X$ polinom felbontási testét tartalmazza, sőt azonos vele.

Legyen K mint a lemmában. Mivel $\mathcal{O}_K$ egy főideál gyűrű és p az egyetlen prím eleme, így minden $\alpha \in K^\times$ felírható egyértelműen up^m alakban ahol $u \in \mathcal{O}_K^\times$ és $m \in \mathbb{Z}$. Definiáljuk egy elem rendjét a következő képpen $\text{ord}_p(\alpha) = m$. Ekkor ord_p egy $K^\times \to \mathbb{Z}$ homomorfizmus, ami az $\text{ord}_p : \mathbb{Q}_p^\times \to \mathbb{Z}$ kiterjesztése.

3.1.4. Lemma. *Legyen E egy elliptikus görbe $\mathbb{Q}_p$ felett jó redukcióval, és legyen $n \in \mathbb{Z}\backslash p\mathbb{Z}$. Minden $p \in E(\mathbb{Q})_p$ pontra, létezik K $\mathbb{Q}_p$ egy véges bővítése amire $P \in nE(K)$.*

3.1.5. Állítás. *Legyen E egy elliptikus görbe $\mathbb{Q}_p$ felett és Δ diszkriminánssal, valamint legyen T azon prímszámok halmaza amik osztják $2n\Delta$ számot. Minden $\gamma \in S^{(n)}(\mathbb{Q})$ és $p \notin T$ páros hoz létezik egy véges nemelágazó K bővítése $\mathbb{Q}_p$ testnek úgy, hogy γ a $H^1(K, E_n)$ csoport null elemébe képződik.*

Bizonyítás. A Selmer csoport definíciójából tudjuk, hogy létezik $P \in E(\mathbb{Q}_p)$ ami γ_p elemre képződik a $\gamma \in H^1(\mathbb{Q}_p, E_n)$ képére. Mivel p nem osztja $2n\Delta$ számot így létezik egy

nemelágazó K bővítése $\mathbb{Q}_p$ testnek amire $P \in nE(K)$, és így γ_p a $H^1(\mathbb{Q}, E_n)$ null elemébe képződik:

$$\begin{array}{ccccc} E(\mathbb{Q}) & \stackrel{n}{\to} & E(\mathbb{Q}) & \to & H^1(\mathbb{Q}, E_n) \\ \downarrow & & \downarrow & & \downarrow \\ E(\mathbb{Q}_p) & \stackrel{n}{\to} & E(\mathbb{Q}_p) & \to & H^1(\mathbb{Q}_p, E_n) \\ \downarrow & & \downarrow & & \downarrow \\ E(K) & \stackrel{n}{\to} & E(K) & \to & H^1(K, E_n) \end{array}$$

□

3.2. Végesség egy speciális esetben

Ebben a részben belátjuk, hogy $S^{(2)}(E/\mathbb{Q})$ véges ha E minden másodrendű pontjainak koordinátája $\mathbb{Q}$ testbeliek. Ez a feltétel azt jelenti, hogy E egyenlete a következő képpen írható fel:

$$Y^2Z = (X - \alpha Z)(X - \beta Z)(X - \gamma Z), \quad \alpha, \beta, \gamma \in \mathbb{Q}.$$

Ez implikálja a következőt:

$$E_2(\mathbb{Q}^{\mathrm{al}}) = E_2(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2 = (\mu_2)^2,$$

ezekhez hozzávéve a $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$ triviális hatását, és így

$$H^1(\mathbb{Q}, E_2) \cong H^1(\mathbb{Q}, \mu_2)^2 \cong (\mathbb{Q}^\times/\mathbb{Q}^{\times 2})^2.$$

Legyen $\gamma \in S^{(2)}(E/\mathbb{Q}) \subset H^1(\mathbb{Q}, E_2)$. Minden p_0 prímre ami nem osztja 2Δ, létezik egy véges nemelágazó K bővítése $\mathbb{Q}_{p_0}$ testnek amire γ a nullába képződik a függőleges nyilak mentén:

$$\begin{array}{ccc} H^1(\mathbb{Q}, E_n) & \stackrel{\cong}{\to} & (\mathbb{Q}^\times/\mathbb{Q}^{\times 2})^2 \\ \downarrow & & \downarrow \\ H^1(K, E_n) & \stackrel{\cong}{\to} & (K^\times/K^{\times 2})^2 \end{array}$$

Tegyük fel, hogy:

$$\gamma \leftrightarrow \left((-1)^{\varepsilon(\infty)} \prod_{\text{p prím}} p^{\varepsilon(p)}, (-1)^{\varepsilon'(\infty)} \prod_{\text{p prím}} p^{\varepsilon'(p)} \right), \quad 0 \le \varepsilon(p), \varepsilon'(p) \le 1,$$

a fenti nyíl menti megfeleltetés. Most $\mathrm{ord}_{p_0}\left((-1)^{\varepsilon(\infty)} \prod_{\text{p prím}} p^{\varepsilon(p)}\right) = \varepsilon(p_0)$, és így ha $(-1)^{\varepsilon(\infty)} \prod_{\text{p prím}} p^{\varepsilon(p)}$ egy négyzet K testben, akkor $\varepsilon(P_0) = 0$. Ebből adódóan az egyetlen p ami megjelenhet a faktorizációban azok a prímek amik osztják 2Δ. Ez véges sok lehetőséget ad γ elemre.

3.3. Az általános eset bizonyítása

Tudjuk [2]-ből, hogy $\mathbb{Q}$ testnek egy értékelése van és így egy telítése $\mathbb{Q}_p$ minden (p) prímideálra $\mathbb{Z}$ gyűrűben. Valamint van még egy telítése $\mathbb{R}$ ezeken kívül, amit az egyszerűség kedvéért $\mathbb{Q}_\infty$ jelölünk. Ehhez hasonlóan ha L egy számtest akkor van egy telítése így értékelése is minden $\mathcal{O}_L$ gyűrűbeli prímideálra és további telítések minden $\mathbb{R}$ testbe való különböző beágyazásra vagy különböző komplex-konjugált beágyazás párokra $\mathbb{C}$ testbe. Jelöljük $\mathcal{P}(p)$-vel azon értékelések halmazát amik kiterjesztik $|\cdot|_p$ értékelést. Ekkor

$$L \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \prod_{\nu \in \mathcal{P}(p)} L_\nu$$

ahol L_ν az L telítése ν értékelésre nézve. Legyen $\mathcal{P} = \bigcup_{\text{p prím}} \mathcal{P}(p)$. Minden E elliptikus görbére L felett, definiáljuk a következőt:

$$S^{(n)}(E/L) = \text{Ker}\left(H^1(L, E_n) \to \prod_{\nu \in \mathcal{P}} H^1(L_\nu, E) \right).$$

Adott n egészre, ahelyett hogy belátnánk $S^{(n)}(E/\mathbb{Q})$ végességét egyszerűbb belátni $S^{(n)}(E/L)$ végességét elegendően nagy L számtestre. Következő lemmából látható hogy valóban elégséges ezt az esetet vizsgálni:

3.3.1. Lemma. *Tetszőleges $L|\mathbb{Q}$ Galois bővítésére és $n \geq 1$ egészre, a*

$$S^{(n)}(E/\mathbb{Q}) \to S^{(n)}(E/L)$$

leképezés magja véges.

Bizonyítás. Mivel $S^{(n)}(E/\mathbb{Q})$ illetve $S^{(n)}(E/L)$ a $H^1(\mathbb{Q}, E_n)$ és $H^1(L, E_n)$ csoportok megfelelő részcsoportjai, így elégséges hogy a magja a

$$H^1(\mathbb{Q}, E_n) \to H^1(L, E_n)$$

leképezésnek véges. Ez a mag valójában a $H^1(\text{Gal}(L/\mathbb{Q}), E_n(L))$ csoport, ami véges hisz mind $\text{Gal}(L/\mathbb{Q})$ és $E_n(L)$ is véges. □

A speciális eset bizonyításánál a következő tényeket használtuk ki:

(a) $\mathbb{Q}$ tartalmaz egy primitív egységgyököt

(b) $E(\mathbb{Q})_2 = E(\mathbb{Q}^{\mathrm{al}})_2$ (feltétel szerint)

(c) minden véges T prímek részhalmazára, a

$$r \mapsto (ord_p(r) \mod 2) : \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \to \bigoplus_{p\notin T} \mathbb{Z}/2\mathbb{Z}$$

leképezés magja véges.

Valamely L véges Galois bővítésére $\mathbb{Q}$ testnek, L tartalmazni fog egy n-edik primitív egységgyököt és így $E(L)$ tartalmazni fogja az $E(\mathbb{Q}^{\mathrm{al}})$ modulus n-ed rendű elemeit. Ahogy majd a következőkben belátjuk, (c) analogonja számtestekre három algebrai számelméleti tételből fog következni, és így a speciális eset bizonyítása átvihető lesz az általános esetre.

Algebrai Számelméleti kitérő

Következőkben L a $\mathbb{Q}$ test egy véges bővítése lesz és $\mathcal{O}_L$ az algebrai egészek gyűrűje L testben. Tételek nagyrésze csak kimondására kerül és ezek bizonyítását csak hivatkozni fogom.

3.3.2. Tétel (Dedekind)**.** *Minden $\mathcal{O}_L$ gyűrű beli ideál felírható prímideálok szorzataként.*

Bizonyítás. Ennél általánosabb tételt fogunk belátni: Minden $\mathfrak{A}$ Dedekind gyűrűben egy tetszőleges valódi nem nulla ideál $\mathfrak{a}$ felírható a következő alakban:

$$\mathfrak{a} = \mathfrak{p}_1^{r_1}\mathfrak{p}_2^{r_2}\cdots\mathfrak{p}_n^{r_n}$$

3.3.3. Lemma. *Legyen A egy Noether gyűrű, ekkor minden $\mathfrak{a}$ ideál tartalmazza nemnulla prímideálok szorzatát.*

Bizonyítás. Tegyük fel, hogy az állítás nem teljesül és válaszunk egy maximális ideált az ellenpéldákból. Ekkor $\mathfrak{a}$ maga sem lehet prímideál, így léteznek $x, y \notin A$, hogy $xy \in \mathfrak{a}$ de sem x sem y nem eleme $\mathfrak{a}$ ideálnak. $\mathfrak{a} + (x)$ és $\mathfrak{a} + (y)$ ideálok valódi részhalmaza $\mathfrak{a}$, de a szorzatukat $\mathfrak{a}$ tartalmazza. Azonban $\mathfrak{a}$ maximális volt ami nem tartalmaz prímszorzatot ezért $\mathfrak{a} + (x)$ és $\mathfrak{a} + (y)$ ideálok tartalmaznak de ekkor $\mathfrak{a}$ is tartalmaz ami ellentmondás. Ezzel igazolva állításunk. $\square$

3.3.4. Állítás. *Ha* $\mathfrak{p}$ *egy maximális ideál az* R *gyűrűben akkor,* $R/\mathfrak{p}^n \cong R_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}^n$ *minden* $n \geq 1$.

Bizonyítás. Bizonyítás megtalálható [2] 37.oldalán 3.7.3 állítás. □
Fenti lemma értelmében tetszőleges $\mathfrak{a}$ ideálja A gyűrűnek tartalmazza nemnulla prímek szorzatát:

$$\mathfrak{b} = \mathfrak{p}_1^{r_1}\mathfrak{p}_2^{r_2}\cdots\mathfrak{p}_m^{r_m}$$

Azt is feltehetjük, hogy a fenti felírásban a $\mathfrak{p}_i$ prímideálok mind különbözőek. Ekkor:

$$A/\mathfrak{b} \cong A/\mathfrak{p}_1^{r_1} \times A/\mathfrak{p}_2^{r_2} \times \cdots \times A/\mathfrak{p}_n^{r_n} \cong A_{\mathfrak{p}_1}/\mathfrak{q}_1^{r_1} \times A_{\mathfrak{p}_2}/\mathfrak{q}_2^{r_2} \times \cdots \times A_{\mathfrak{p}_m}/\mathfrak{q}_m^{r_m}$$

Ahol $\mathfrak{q}_i = \mathfrak{p}_i A_{\mathfrak{p}_i}$ az $A_{\mathfrak{p}_i}$ lokalizált gyűrű maximális ideálja. Az első izomorfizmust a Kínai maradék tétel adja, a második izomorfizmust pedig a fenti állítás adja. Ez az izomorfizmus mutatja, hogy $\mathfrak{a}/\mathfrak{b}$ ideálnak $\mathfrak{q}_1^{s_1}/\mathfrak{q}_1^{r_1} \times \mathfrak{q}_2^{s_2}/\mathfrak{q}_2^{r_2} \times \cdots \times \mathfrak{q}_m^{s_m}/\mathfrak{q}_n^{r_n}$ valamilyen $s_i \leq r_i$ egészekre. Ez az ideál a $\mathfrak{p}_1^{s_1}\cdots\mathfrak{p}_1^{s_m}$ képe az izomorfizmusnál, így :

$$\mathfrak{a} = \mathfrak{p}_1^{s_1}\cdots\mathfrak{p}_1^{s_m} \text{ in } A/\mathfrak{b}.$$

Mivel mindkét ideál tartalmazza $\mathfrak{b}$ ideált így kapjuk, hogy:

$$\mathfrak{a} = \mathfrak{p}_1^{s_1}\cdots\mathfrak{p}_1^{s_m}$$

Azaz valóban felírható egy ideál prímideálok szorzataként már csak az egyértelműség van hátra.
Tegyük fel hogy van két faktorizációnk, nulla kitevős tényezőket hozzávéve a szorzatunkhoz feltehetjük, hogy ugyanazok a prímek jelennek meg a faktorizációnkban csak más kitevővel:

$$\mathfrak{p}_1^{s_1}\cdots\mathfrak{p}_1^{s_m} = \mathfrak{a} = \mathfrak{p}_1^{t_1}\cdots\mathfrak{p}_1^{t_m}$$

A fenti bizonyításban láttuk, hogy $\mathfrak{q}^{s_i} = \mathfrak{a}A_{\mathfrak{p}_i} = \mathfrak{q}_i^{t_i}$ ahol $\mathfrak{q}_i$ maximális ideál $A_{\mathfrak{p}_i}$ gyűrűben így szükségszerűen $s_i = t_i$. □

3.3.5. Definíció. Legyen $a \in \mathcal{O}_L$ és $\mathfrak{p}$ egy prímideálja, legyen az $ord_{\mathfrak{p}}$ a $\mathfrak{p}$ kitevője az (a) faktorizációjában, azaz

$$(a) = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(a)}.$$

$x = \frac{a}{b} \in L$ testelem rendje legyen $\mathrm{ord}_{\mathfrak{p}}(a) - \mathrm{ord}_{\mathfrak{p}}(b)$. Az $\mathcal{O}_L$ osztálycsoportja C, amit következő homomorfizmus komagjaként definiálunk:

$$L^{\times} \to \bigoplus_{\mathfrak{p}\subset\mathcal{O}_L,\mathfrak{p}\text{ prím}} \mathbb{Z} \to C \to 0$$

3.3.6. Tétel. *Ha L test a $\mathbb{Q}$ egy véges bővítése akkor a bővítés osztály csoportja véges.*

Bizonyítás. Bizonyítás megtalálható [2] 32.oldalán 3.5.9 Tétel. □

3.3.7. Definíció. U az egységek csoportja $\mathcal{O}_L$ gyűrűben.

3.3.8. Tétel. *Az U csoport végesen generált.*

Bizonyítás. [3] 5.1 Tétel. □

Tetszőleges kommutatív gyűrűben a egység $\mathcal{O}$ gyűrűben akkor és csak akkor, ha $(a) = \mathcal{O}$. A mi esetünkben, ez ekvivalens azzal, hogy $\mathrm{ord}_{\mathfrak{p}}(a) = 0$, vagyis kapjuk a következő egzakt sorozatot:

$$0 \to U \to L^{\times} \to \bigoplus_{\mathfrak{p} \subset \mathcal{O}_L, \mathfrak{p} \text{ prím}} \mathbb{Z} \to C \to 0$$

végesen generált U egység csoporttal és véges C osztálycsoporttal. Ennek segítségével az előbbi tételeket valamivel általánosabban is kimondhatjuk:

3.3.9. Következmény. *Ha T prímideálok egy véges halmaza az L testbővítésben, akkor az U_T, C_T csoportok a következő egzakt sorozat által definiálva:*

$$0 \to U_T \to L^{\times} \xrightarrow{a \mapsto \mathrm{ord}_{\mathfrak{p}}(a)} \bigoplus_{\mathfrak{p} \notin T} \mathbb{Z} \to C_T \to 0$$

végesen generált illetve véges.

Bizonyítás.

$$L^{\times} \xrightarrow{a \mapsto \mathrm{ord}_{\mathfrak{p}}(a)} \bigoplus_{\mathfrak{p}} \mathbb{Z} \xrightarrow{\text{projekció}} \bigoplus_{\mathfrak{p} \notin T} \mathbb{Z}$$

A fenti leképezés sorozat, kernel kokernel sorozata ad egy egzakt sorozatot:

$$0 \to U \to U_T \to \bigoplus_{\mathfrak{p} \in T} \mathbb{Z} \to C \to C_T \to 0$$

□

Selmer csoport végességének a bizonyítása

A fentiek alapján a következő lemma bizonyítja az $S^n(E/L)$ csoport végességét és így $S^n(E/\mathbb{Q})$ csoport végességét is.

3.3.10. Lemma. *Legyen $T \subset \mathcal{P}$ véges részhalmaz ami tartalmazza $\mathcal{P}(\infty)$ prímet, legyen N a magja a következő leképezésnek:*

$$a \mapsto (\mathrm{ord}_{\mathfrak{p}}(a) \bmod n) : L^{\times}/L^{\times n} \to \bigoplus_{\mathfrak{p} \notin T} \mathbb{Z}/\mathbb{Z}n.$$

Ekkor létezik egy egzakt sorozat:

$$0 \to U_T/U_T^n \to N \to (C_T)_n$$

Bizonyítás. Diagramm vadászattal bizonyítjuk

$$\begin{array}{ccccccccccc}
0 & \longrightarrow & U_T & \longrightarrow & L^{\times} & \longrightarrow & \bigoplus_{\mathfrak{p}\notin T}\mathbb{Z} & \longrightarrow & C_T & \longrightarrow & 0 \\
 & & \downarrow^n & & \downarrow^n & & \downarrow^n & & \downarrow^n & & \\
0 & \longrightarrow & U_T & \longrightarrow & L^{\times} & \longrightarrow & \bigoplus_{\mathfrak{p}\notin T}\mathbb{Z} & \longrightarrow & C_T & \longrightarrow & 0 \\
 & & & & \downarrow & & \downarrow & & & & \\
 & & & & L^{\times} & \longrightarrow & \bigoplus_{\mathfrak{p}\notin T}\mathbb{Z}/\mathbb{Z} & & & &
\end{array}$$

Legyen $\alpha \in L^{\times}$ egy N-beli elem reprezentánsa. Ekkor $n|\mathrm{ord}_{\mathfrak{p}}(\alpha)$ minden $\mathfrak{p} \notin T$, így α elemünket leképezhetjük $(\frac{\mathrm{ord}_{\mathfrak{p}}(\alpha)}{n})$ elem c osztályába C_T csoportban. Ekkor $nc = 0$. Ha $c = 0$, akkor létezik egy $\beta \in L^{\times}$, hogy $\mathrm{ord}_{\mathfrak{p}}(\beta) = \mathrm{ord}_{\mathfrak{p}}(\alpha)/n$ minden $\mathfrak{p} \notin T$ prímideálra. Most α/β egy U_T beli elem, és jól definiált egy U_T^n beli elem erejéig. $\square$

3.4. Magasságok; a véges bázis tétel bizonyításának befejezése

Legyen $P = (a_0 : ... : a_n) \in \mathbb{P}^n(\mathbb{Q})$. Azt mondjuk hogy, $(a_0 : ... : a_n)$ egy primitív reprezentánsa P pontnak, ha:

$$a_i \in \mathbb{Z},\ \gcd(a_0, ..., a_n) = 1.$$

A magasságát, $H(P)$ P pontnak a következő képpen definiáljuk:

$$H(P) = \max_i |a_i|$$

A logaritmikus magasságot $h(P)$ a P pontnak $\log H(P)$ értékeként definiáljuk.

Magasság $\mathbb{P}^1$ téren

Legyen $F(X,Y)$ és $G(X,Y)$ m-fokú homogén polinomok a $\mathbb{Q}[X,Y]$ gyűrűben, és legyen $V(\mathbb{Q})$ a közös nullhelyeik halmaza. Ekkor F és G meghatároznak egy leképezést:

$$\varphi : \mathbb{P}^1(\mathbb{Q})\backslash V(\mathbb{Q}) \to \mathbb{P}^1(\mathbb{Q}),\ (x:y) \mapsto (F(x,y) : G(x,y))$$

3.4.1. Állítás. *Ha $F(X,Y)$ és $G(X,Y)$ m-fokú homogén polinomok nincs közös nullhelyük $\mathbb{P}^1(\mathbb{Q}^{\mathrm{al}})$ téren, akkor létezik egy B konstans, hogy*

$$|h(\varphi(P)) - m \cdot h(P)| \leq B,\ \text{minden } P \in \mathbb{P}^1(\mathbb{Q}).$$

Bizonyítás. F és G polinomokat tetszőleges konstanssal szorozva nem változtatjuk φ értékét, így feltehetjük, hogy egész együtthatósak. Legyen $(a:b)$ egy primitív reprezentánsa P pontnak. Ekkor tetszőleges cX^iY^{m-i} monomra:

$$|ca^ib^j| \leq |c| \max(|a^m|, |b^m|),$$

és ezzel:

$$|F(a,b)|, |G(a,b)| \leq C \cdot (max(|a|,|b|))^m$$

ahol $C = (m+1)\max(|F \text{ vagy } G \text{ együtthatója}|)$. Fentiekből kapjuk:

$$H(\varphi(P)) \leq \max(|F(a,b)|, |G(a,b)|) \leq C \cdot \max(|a|,|b|)^m = C \cdot H(P)^m$$

Ha vesszük a logaritmusát az egyenlőtlenségünknek a következőt kapjuk:

$$h(\varphi(P)) \leq mh(P) + \log C$$

Feltételünk szerint az F és G rezultánsa R (mint homogén polinomok rezultánsa) nem nulla. Vegyük az $Y^{-m}F(X,Y) = F(\frac{X}{Y}, 1)$ és az $Y^{-m}G(X,Y) = G(\frac{X}{Y}, 1)$. Hogyha ezekere úgy tekintünk, mint egyváltozós polinomokra az $\frac{X}{Y}$ változóban, akkor ugyan az lesz a rezultánsuk, mint $F(X,Y)$ és $G(X,Y)$ polinomoknak. Valamint léteznek $U(\frac{X}{Y}), V(\frac{X}{Y}) \in \mathbb{Z}[\frac{X}{Y}]$ $m-1$ fokú polinomok, hogy

$$U(\frac{X}{Y})F(\frac{X}{Y}, 1) + V(\frac{X}{Y})G(\frac{X}{Y}, 1) = R$$

egyenlőség teljesül. Ezután ha végig szorozzuk az azonosságunkat Y^{2m-1} változóval és $Y^{m-1}U(\frac{X}{Y}) = U(X,Y)$ valamint $Y^{m-1}V(\frac{X}{Y}) = V(X,Y)$ jelölésekkel élve kapjuk:

$$U(X,Y)F(X,Y) + V(X,Y)G(X,Y) = RY^{2m-1}$$

egyenletet. A fenti gondolatmenet hasonlóan végig vihető X változóval ekkor a polinomjainkat $\frac{Y}{X}$ változó polinomjaiként tekintjük homogenizálás után kapunk $U^{'}(X,Y)$ és $V^{'}(X,Y)$ $m-1$ változós polinomokat valamint a következő egyenletet:

$$U^{'}(X,Y)F(X,Y)+V^{'}(X,Y)G(X,Y)=RX^{2m-1}.$$

Helyettesítsük (a,b) értékeket (X,Y) helyére:

$$U(a,b)F(a,b)+V(a,b)G(a,b)=Rb^{2m-1}$$

$$U^{'}(a,b)F(a,b)+V^{'}(a,b)G(a,b)=Ra^{2m-1}.$$

Fenti egyenletekből láthatjuk, hogy:

$$\gcd(F(a,b),G(a,b)) \text{ osztja } \gcd(Rb^{2m-1},Rb^{2m-1})=R.$$

A bizonyítás első feléhez hasonlóan, létezik egy $C>0$ konstans amire

$$U(a,b),U^{'}(a,b),V(a,b),V^{'}(a,b)\leq C\cdot(\max(|a|,|b|))^{m-1}$$

$$2C\cdot(\max(|a|,|b|))^{m-1}\cdot\max(|F(a,b)|,|G(a,b)|)\leq\max(|Ra^{2m-1}|,|Rb^{2m-1}|).$$

Ezt összevetve azzal, hogy $\gcd(F(a,b),G(a,b))|R$, kapjuk:

$$H(\varphi(P))\leq\frac{1}{|R|}\max(|F(a,b)|,|G(a,b)|)\leq\frac{1}{2C}H(P)^m.$$

Logaritmust véve adódik az állítás

$$h(\varphi(P))\leq mh(P)-log(2C).$$

□

3.4.2. Megjegyzés. Létezik egy jól definiált leképezés:

$$V:\mathbb{P}^1\times\mathbb{P}^1\to\mathbb{P}^2$$

$$(a:b),(c:d)\mapsto(ac:ad+bc:bd)$$

ezt a leképzést Veronese leképezésnek hívjuk.

3.4.3. Lemma. *Legyen R a (P,Q) képe a Veronese leképezésnél. Ekkor:*

$$\frac{1}{2}\leq\frac{H(R)}{H(P)H(Q)}\leq 2.$$

Bizonyítás. Válasszunk P és Q pontoknak egy egy primitív reprezentánst, ezek legyenek $(a : b)$ és $(c : d)$. Ekkor

$$H(R) \geq \max(|ac|, |ad + bc|, |bd|) \geq 2 \max(|a|, |b|) \max(|c|, |d|) = 2H(P)H(Q).$$

Ha egy p prím osztja ac és bd egészeket is, akkor vagy osztja a és d de b és c nem osztja, vagy pont fordítva. Bármelyik is legyen, biztosan nem osztja $ad + bc$, és ezzel $(ac, ad + bc, bd)$ egy primitív reprezentánsa lesz R pontnak. Már csak a következő egyenlőtlenséget kell belátnunk:

$$\max(|ac|, |ad + bc|, |bd|) \leq \frac{1}{2} \max(|a|, |b|) \max(|c|, |d|)$$

ez könnyen látszik bármelyik két elem is legyen a jobb oldalon a maximum legalább a szorzatuk megtalálható a bal oldalt. □

Magasság az elliptikus görbéken

Legyen E egy elliptikus görbe

$$E : Y^2Z = aXZ^2 + bZ^3,\ a, b \in \mathbb{Q},\ \Delta = 4a^3 + 27b^2 \neq 0.$$

Egy $P \in E(\mathbb{Q})$ pontra, definiáljuk

$$H(P) = H((x(P) : z(P))) \text{ ha } z(P) \neq 0$$

$$H(P) = 1 \text{ ha } P = (0 : 1 : 0)$$

és

$$h(P) = \log(H(P))$$

3.4.4. Lemma. *Minden $B > 0$ konstansra a $\{P \in E(\mathbb{Q}) : h(P) < B\}$ egy véges halmaz.*

Bizonyítás. Az egyértelmű, hogy B konstansra a $\{P \in \mathbb{P}^1(\mathbb{Q}) : h(P) < B\}$ halmaz véges, de minden $(x_0, z_0) \in \mathbb{P}^1$, maximum két pont van amikre $(x_0, y, z_0) \in E(\mathbb{Q})$, és így $\{P \in E(\mathbb{Q}) : h(P) < B\}$ szintén véges. □

3.4.5. Állítás. *Létezik egy A konstans:*

$$|h(2P) - 4H(P)| \leq A.$$

Bizonyítás. Legyen $P = (x : y : z)$ és $2P = (x_2 : y_2 : z_2)$. A duplikációs formula szerint:

$$(x_2 : z_2) = (F(x) : G(x))$$

ahol $F(X, Z)$ és $G(X, Z)$ homogén 4-ed fokú polinomok, amiket a következő formula ad meg:

$$F(X, 1) = (3X^2 + a)^2 - 8X(X^3 + aX + b)$$

$$G(X, 1) = 4(X^3 + aX + b).$$

Mivel $X^3 + aX + b$ és a deriváltja $3X^2 + a$ polinomnak nincs közös gyöke, így $F(X, 1)$ és $G(X, 1)$ polinomoknak sem lesz így használhatjuk a 2.4.1 Állításunkat ahol φ a duplikációs formula és $m = 4$ ezzel kapjuk, hogy valóban létezik ilyen A konstans:

$$|h(2P) - 4h(P)| \leq A.$$

□

3.4.6. Állítás. *Létezik maximum egy $\overline{h} : E(\mathbb{Q}) \to \mathbb{R}$ ami kielégíti a következő feltételeket:*

1. *(a) $\overline{h}(P) - h(P)$ korlátos $E(\mathbb{Q})$ halmazon;*
2. *(b) $\overline{h}(2P) = 4\overline{h}(P)$.*

Bizonyítás. Ha $\overline{h}$ kielégíti az (a) feltételt B korláttal, akkor:

$$|\overline{h}(2^n P) - h(2^n P)| \leq B.$$

Ha ezenfelül a (b) feltételt is kielégíti akkor,

$$\left|\overline{h}(P) - \frac{h(2^n P)}{4^n}\right| \leq \frac{B}{4^n},$$

azaz $h(2^n P)/4^n$ konvergál $\overline{h}(P)$ függvényhez. □

3.4.7. Megjegyzés. Tetszőleges $\overline{h} : E(\mathbb{Q}) \to \mathbb{R}$ függvényt mely kielégíti az (a) és (b) feltételeket kanonikusnak, Néron-Tatenek vagy magasság függvénynek nevezzük. A bizonyítás szerint ha $\overline{h}$ létezik akkor biztosan a $h(2^n P)/4^n$ határértéke.

3.4.8. Lemma. *Minden $P \in E(\mathbb{Q})$, a $h(2^n P)/4^n$ sorozat Cauchy $\mathbb{R}$ testben.*

Bizonyítás. A 2.4.5 állítás értelmében létezik A konstans:

$$|h(2P) - 4h(P)| \leq A$$

minden P pontra. Legyen $N \geq M \geq 0$ és $P \in E(\mathbb{Q})$,

$$\begin{aligned}\left|\frac{h(2^N P)}{4^N} - \frac{h(2^M P)}{4^M}\right| &= \left|\sum_{n=M}^{N-1} \frac{h(2^{n+1}P)}{4^{n+1}} - \frac{h(2^n P)}{4^n}\right| \\ &\leq \sum_{n=M}^{N-1} \frac{1}{4^{n+1}} |h(2^{n+1}P) - 4h(2^n P)| \\ &\leq \sum_{n=M}^{N-1} \frac{1}{4^{n+1}} A \\ &\leq \frac{A}{4^{M+1}} \left(1 + \frac{1}{4} + \frac{1}{4^2} + \frac{1}{4^3} + ...\right) \\ &\leq \frac{A}{3 \cdot 4^M}.\end{aligned}$$

Azaz $h(2^n P)/4^n$ Cauchy. □

3.4.9. Definíció. A fenti lemma miatt értelmes a következő definíció

$$\overline{h}(P) = \lim_{n \to \infty} \frac{h(2^n P)}{4^n}$$

minden $P \in E(\mathbb{Q})$ pontra.

3.4.10. Tétel. *Az $\overline{h}(P) : E \to \mathbb{R}$ egy Néron-Tate függvény; továbbá,*

- *(a) minden $C \leq 0$, a $\{P \in E(\mathbb{Q}) | \overline{h}(P) \leq C\}$ halmaz véges;*
- *(b) $\overline{h}(P) \leq 0$, és ez egyenlőséggel teljesül, akkor és csak akkor ha P véges rendű.*

Bizonyítás. (a):Az előző tétel bizonyításából felhasználhatjuk az egyenlőtlenséget $M = 0$ helyettesítéssel:

$$\left|\frac{h(2^N P)}{4^N} - \frac{h(P)}{1}\right| \leq \frac{A}{3}$$

ezután vegyük a határértékét $N \to \infty$, azaz $\overline{h}(P) - h(P)$ korlátos. Azon P pontok halmaza amire $\overline{h}(P) \leq C$ teljesül véges ugyanis h magasságfüggvényre ez teljesül és $\overline{h}(P) - h(P)$ korlátos.
(b): $H(P) \geq 1$ és egész így $h(P) \geq 0$ és $\overline{h}(P) \geq 0$. Ha P torziós pont akkor $\{2^n P | n \geq 0\}$ véges, így $\overline{h}(P)$ korlátos rajta, legyen ez a korlát D és $\overline{h}(P) = \overline{h}(2^n P)/4^n \leq D/4^n$ minden

n nemnegatív egészre. Másfelől ha P nem véges rendű pont, akkor $\{2^n P | n \geq 0\}$ végtelen és így $\overline{h}$ nem korlátos rajta. Ekkor $\overline{h}(2^n P) > 1$ valamilyen n egészre és így $\overline{h}(P) > 4^{-n} > 0$.
□

3.4.11. Megjegyzés. Legyen $f : M \to K$, egy M Abel csoportból egy K, char$K \neq 2$ testbe menő függvény. Egy ilyen f függvényt kvadratikusnak nevezünk, ha $f(2x) = 4f(x)$ és

$$B(x, y) \xrightarrow{\text{def}} f(x + y) - f(x) - f(y)$$

bi-additív. Ekkor B szimmetrikus és ez az egyetlen szimmetrikus bi-additív forma $B : M \times M \to K$, hogy $f(x) = \frac{1}{2}B(x, x)$ teljesül. Szükségünk lesz a következő lemmára:

3.4.12. Lemma. *Az $f : M \to K$ M Abel csoportból K, char$K \neq 2$ testbe menő függvény kvadratikus ha teljesíti a paralelogramma egyenlőséget:*

$$f(x + y) + f(x - y) = 2f(x) + 2f(y) \ \forall x, y \in M.$$

Bizonyítás. f teljesítse a paralelogramma egyenlőséget. Legyen $x = y = 0$, ezzel kapjuk, hogy $f(0) = 0$, $x = y$ választással a $f(2x) = 4f(x)$ azonosságot kapjuk. Ha $x = 0$ akkor $f(-y) = f(y)$. Szimmetria miatt elég az egyik oldali additivitást megmutatni, azaz $B(x + y, z) = B(x, z) + B(y, z)$ azonosságot:

$$f(x + y + z) - f(x + y) - f(z) = f(x + z) - f(x) - f(z) + f(y + z) - f(y) - f(z)$$

ezt nullára rendezve kapjuk:

$$f(x + y + z) - f(x + y) - f(x + z) - f(y + z) + f(x) + f(z) + f(y) = 0.$$

A paralelogramma egyenlőséget használva kapjuk a következő négy azonosságot:

$$f(x + y + z) + f(x + y - z) - 2f(x + y) - 2f(z) = 0$$

$$f(x + y - z) + f(x - y + z) - 2f(x) - 2f(y - z) = 0$$

$$f(x + y + z) + f(x - y + z) - 2f(x + z) - 2f(y) = 0$$

$$2f(y + z) + 2f(y - z) - 4f(y) - 4f(z) = 0$$

Az elsőtől kezdve összeadva őket váltakozó előjellel és az elsőt pozitívval véve:

$$2f(x + y + z) - 2f(x + y) - 2f(x + z) - 2f(y + z) + 2f(x) + 2f(z) + 2f(y) = 0$$

□

3.4.13. Állítás. *A $\overline{h} : E(\mathbb{Q}) \to \mathbb{R}$ magasság függvény egy kvadratikus forma.*

Ennek belátásához a paralelogramma egyenlőséget fogjuk használni.

3.4.14. Lemma. *Létezik egy C konstans amire:*

$$H(P_1 + P_2)H(P_1 - P_2) \leq H(P_1)^2 H(P_2)^2$$

minden $P_1, P_2 \in E(\mathbb{Q})$ pontra.

Bizonyítás. Legyen $P_3 = P_1 + P_2$ és $P_4 = P_1 - P_2$ és $P_i = (x_i : y_i : z_i)$
Ekkor $(x_3x_4 : x_3z_z + x_4z_3 : z_3z_4) = (w_0, w_1, w_2)$, ahol

$$w_0 = (x_2z_1 - x_1z_2)^2$$

$$w_1 = 2(x_1x_2 + az_1z_2)(x_1z_2 + x_2z_1) + 4b(z_1z_2)^2$$

$$w_2 = (x_1x_2)^2 - 2ax_1x_2z_1z_2 - 4b(x_1z_1z_2^2 + x_2z_1^2z_2) + a(z_1z_2)^2.$$

Ebből következik, hogy:

$$H(w_0 : w_1 : w_2) \leq C \cdot H(P_1)^2 \cdot H(P_2)^2.$$

□

3.4.15. Lemma. *A kanonikus magasság függvény $\overline{h} : E(\mathbb{Q}) \to \mathbb{R}$ teljesíti a parelallogarmma egyenlőséget:*

$$\overline{h}(P + Q) + \overline{h}(P - Q) = 2\overline{h}(P) + 2\overline{h}(Q).$$

Bizonyítás. Az előző lemma beli egyenlőtlenség logaritmusát véve kapjuk az alábbit:

$$h(P + Q) + h(P - Q) \leq 2h(P) + 2h(Q) + B.$$

P és Q helyére 2^nP és 2^nQ írva és végig osztva 4^n, valamint $n \to \infty$:

$$\overline{h}(P + Q) + \overline{h}(P - Q) \leq 2\overline{h}(P) + 2\overline{h}(Q).$$

Legyen $P' = P + Q$ és $Q' = P - Q$ ez fogja adni a másik irányú egyenlőtlenséget:

$$\overline{h}(P') + \overline{h}(Q') \leq 2\overline{h}\left(\frac{P' + Q'}{2}\right) + 2\overline{h}\left(\frac{P' - Q'}{2}\right) = \frac{1}{2}\overline{h}(P' + Q') + \frac{1}{2}\overline{h}(P' - Q')$$

□

3.4.16. Megjegyzés. Legyen K egy számtest. Ha $\mathcal{O}_K$ nem egy principális tartomány, akkor előfordulhat, hogy nem létezik primitív reprezentánsa egy $P \in \mathbb{P}^n(K)$ pontnak és ekkor a pont magasságának definíciója nem terjed ki egyből számtestekre. Ehelyett kissé különböző megközelítést választunk ilyenkor. Egy $c \in \mathbb{Q}^\times$ elmere:

$$\prod_{2,\ldots,\infty} |c|_p = 1.$$

Itt $|.|_p$ a szokásos abszolút érték ha $p = \infty$ egyébként pedig a p-adikus értékelés. Ekkor egy $P = (a_0 : a_1 : \ldots : a_n) \in \mathbb{P}^n(\mathbb{Q})$ pontra a magasságot definiáljuk a következő képpen:

$$H(P) = \prod_{2,\ldots,\infty} \max_i(|a_i|_p)$$

ez független P reprezentánsának a választásától. Továbbá $(a_0, \ldots, a_n)$ egy primitív reprezentáns minden $p \neq \infty$ $\max_i |a_i|_p = 1$, azaz $H(P) = \max_i |a_i|_\infty$ ami megegyezik a korábbi definícióval. Egy K számtest esetén, lehetséges normalizálni az értékelést így a $\mathbb{Q}$ esetén bevezetett szorzatformula érvényben marad így:

$$H(P) \overset{def}{=} \prod_{\nu} \max_i(|a_i|_\nu), \;\; P = (a_0 : a_1 : \ldots : a_n)$$

megadja nekünk a jó jelölését a magasságnak $\mathbb{P}(K)$ projektív téren. Ezzel a definícióval ezen szakasz minden eredménye kiterjeszthető számtestek feletti elliptikus görbékre.

Újabb Algebrai Számelméleti kitérő

Következőkben belátjuk, hogy a fenti megjegyzésben említett normalizálás valóban elvégezhető számtestek esetén.

3.4.17. Tétel (Szorzat formula)**.** *$p = 2, 3, 5, 7, \ldots, \infty$, legyen $|.|_p$ a megfelelő normalizálás abszolút érték $\mathbb{Q}$ testen. Minden nemnulla racionális számra:*

$$\prod_{p \text{ prím}} |a|_p = 1$$

Bizonyítás. Legyen $\alpha = \frac{a}{b}$ $a, b \in \mathbb{Z}$. Ekkor $|\alpha|_v = 1$ hacsak $p|a$ vagy $p|b$. Ekkor $|\alpha|_v = 1$ kivéve véges sok v prímre, azaz a szorzat véges így jóldefiniált.
Legyen $\pi(a) = \prod_v |a|_v$. Ekkor π egy $\mathbb{Q}^\times \to \mathbb{R}^\times$ homomorfizmus, így elég belátni hogy

$\pi(-1) = 1$ és $\pi(p) = 1$ minden prímre. Ez első egyértlemű hisz, $|-1| = 1$ minden abszolút értékre. A második tulajdonság sem nehéz:

$$|p|_p = 1/p,\ |p|_q = 1, \text{ ha } q \neq p, \text{ és } |p|_\infty = p$$

ezen számok szorzata 1 és ezzel be is láttuk hogy az állítás beli szorzat minden racionális számra egy. $\square$
A következő állítást csak kimondom a bizonyítása megtalálható [3] jegyzetben 7.38 tétel.

3.4.18. Tétel. *Legyen K egy diszkrét $|.|_K$ abszolút értékkel telített test, és L legyen egy véges szeparábilis n fokú bővítése. Ekkor $|.|_K$ kiterjeszthető egyértelműen L testre egy abszolút értékének $|.|_L$, és L teljes lesz erre az abszolút értékre nézve. Minden $\beta \in L$:*

$$|\beta|_L = |\mathrm{Nm}_{L/K}\beta|_K^{\frac{1}{n}}$$

3.4.19. Megjegyzés. A $|\beta|_L = |\mathrm{Nm}_{L/K}\beta|_K^{\frac{1}{n}}$ azonosságból látszik hogy $|.|_L$ diszkrét akkor és csak akkor, ha $|.|_K$ diszkrét.

Legyen K egy test $|.|$ abszolút értékkel (ez lehet arkhimédészi vagy diszkrét nem-arkhimédészi), és legyen L egy véges szeparábilis bővítése. Ha K teljes, tudjuk, hogy létezik $|.|$ egy egyértelmű kiterjesztése L testre előző tétel miatt. Legyen $L = K[\alpha]$ és legyen $f(X)$ az α minimál polinomja K test felett. Legyen $|.|'$ $|.|$ kiterjesztése L testre. Ezután vehetjük $\hat{L}$ az L teljessé tételét $|.|'$ abszolútértékkel, ezzel kapjuk a következő diagrammot:

$$\begin{array}{ccc} L & \to & \hat{L} \\ \uparrow & & \uparrow \\ K & \to & \hat{K} \end{array}$$

Ekkor $\hat{L} = \hat{K}[\alpha]$ mivel $\hat{K}[\alpha]$ teljes és véges $\hat{K}$ felett és tartalmazza L testet. Legyen $g(X)$ az α minimál polinomja $\hat{K}$ felett. Mivel $f(\alpha) = 0$ és $g(X)|f(X)$ így $|.|$ minden kiterjesztéséhez hozzá tudunk rendelni $f(X)$ egy irreducibilis faktorát $\hat{K}[x]$ polinomgyűrűben.
Ha pedig $g(X)$ egy normált irreducibilis faktora $f(X)$ polinomnak $\hat{K}[X]$ polinomgyűrűben és $\hat{K}[x] = \hat{K}[X]/(g(X))$ a következő diagrammot kapjuk:

$$\begin{array}{ccc} L & \xrightarrow{\alpha \mapsto x} & \hat{K}[x] \\ \uparrow & & \uparrow \\ K & \to & \hat{K} \end{array}$$

A kiterjesztési tétel szerint $\hat{K}$ abszolút értéke egyértelműen kiterjed $\hat{K}[x]$ testre és ez indukál egy abszolút értéket L testen ami $|.|$ kiterjesztése. A fenti két művelet egymás inverzei ezzel a következő állítást be is láttuk:

3.4.20. Állítás. *Legyen $L = K[\alpha]$ egy véges szeparábilis bővítése K testnek, és legyen $f(X)$ α minimál polinomja K felett. Ekkor létezik egy bijekció $f(X)$ $\hat{K}[X]$ beli faktorai és $|.|$ abszolútérték L kiterjesztései között.*

Van egy kanonikusabb módja L telítéseinek származtatására a különböző $|.|$ kiterjesztései esetén.

3.4.21. Állítás. *Legyen $|.|$ egy abszolútérték (arkhimédészi vagy diszkrét nem arkhimédészi) K testen és L legyen a K egy vége szeparábilis bővítése, $\hat{K}$ pedig a K telítése. Ekkor $|.|$ csak véges sok $|.|_1, ..., |.|_g$ kiterjesztése van az L testre. L_i jelölje L telítését az $|.|_i$ abszolútértékre nézve, ekkor*

$$L \otimes_K \hat{K} \cong \prod_{i=1}^{g} L_i.$$

Bizonyítás. Mivel L szeparábilis K felett, így $L = K[\alpha] \cong K[X]/(f(X))$ minden $\alpha \in L$ primitív elemre és $f(X)$ minimál polinomjára. Tegyük fel, hogy $f(X)$ faktoraira bomlik $\hat{K}[X]$ felett:

$$f(X) = f_1(X) \cdot f_2(X) \cdot ... \cdot f_g(X)$$

ahol $f_i(X)$ normált és irreducibilis. Ekkor

$$L \otimes_K \hat{K} = K[\alpha] \otimes_K \hat{K} \cong \hat{K}[X]/(f(X)) \cong \prod_i \hat{K}[X]/(f_i(X))$$

így az bizonyítás következik az előző állításunkból. Megjegyezendő, hogy a kanonikus leképezés L testből a telítésébe $a \mapsto a_i$, és a kanonikus kiterjesztését $K \to L_i$ $\hat{K}$ testre $b \mapsto b$ adja. Ezzel az állításunk beli izomorfizmus $a \otimes b \mapsto (a_1 b, ..., a_g b)$. $\square$

3.4.22. Állítás. *Az előző állítás feltételeivel, minden $\alpha \in L$ elemre:*

$$\mathrm{Nm}_{L/K}(\alpha) = \prod_i \mathrm{Nm}_{L_i/\hat{K}}(\alpha), \qquad \mathrm{Tr}_{L/K}(\alpha) = \sum_i \mathrm{Tr}_{L_i/\hat{K}}(\alpha)$$

Bizonyítás. α normája és nyoma definíció szerint a determinánsa és nyoma az $x \mapsto \alpha x : L \to L$ K-lineáris leképezésnek. Ezek nem változnak amikor L testet tenzorszorozzuk $\hat{K}$-val, és a tenzorszorzás definíciójából könnyen látszik, hogy a norma és nyom a szorzatban szorzatra és összegre esik szét. $\square$

Mielőtt belátnánk a szorzat formulát számtestekre, szükségünk van a lokális testek egy tulajdonságára. Legyen K egy lokális test $|.|$ normalizált abszolútértékkel. Ha $K = \mathbb{R}$ akkor kapjuk a szokásos abszolút értékünket, ha $K = \mathbb{C}$ akkor a szokásos abszolútérték négyzetét, és $|a| = \left(\frac{1}{\mathbb{N}\mathfrak{p}}\right)^{\mathrm{ord}(a)}$ ha az abszolútértéke egy $\mathfrak{p}$ prímideál definiálja.

Legyen L a K teste egy véges szeparábilis bővítése, és legyen $|.|$ az egyértelmű kiterjesztése a K test abszolút értékének L bővítésre. Legyen $\|.\|$ a $|.|$ abszolútérték normalizáltja L testen. Szeretnénk megérteni a kapcsolatot $\|.\|$ és $|.|$ között.

3.4.23. Lemma. *A fenti esetben, $\|a\| = |a|^n$, ahol $n = |L : K|$.*

Bizonyítás. Ha K arkhimédészi, akkor csak két eset lehet és ezek egyértelműek. Így tegyük fel, hogy K nemarkhimédészi. Mivel normalizált abszolút értékünk van létezik c: $\|.\| = |.|^c$, és elég megnézünk hogy az azonosság teljesül $\pi \in K$ prímekre. Legyen Π L egy prímje, és legyen $\mathfrak{P} = (\Pi)$ valamint $\mathfrak{p} = (\pi)$, akkor $\pi = (\text{egység}) \times \Pi^e$, és így

$$\|\pi\| = \|\Pi^e\| = \left(\frac{1}{\mathbb{N}\mathfrak{P}}\right)^e = \left(\frac{1}{\mathbb{N}\mathfrak{p}}\right)^{ef} = |\pi|^n$$

azaz $c = n$. $\square$

3.4.24. Állítás. *Legyen L/K egy véges bővítése számtesteknek. Minden $v \in K$ prímre és $\alpha \in L$:*

$$\prod_{w|v} \|\alpha\|_w = \prod_v \|\mathrm{Nm}_{K/\mathbb{Q}}\alpha\|_v.$$

$\|.\|_w$ és $\|.\|_v$ a normalizált abszolút értékek w és v prímekre.

Bizonyítás. Legyen $|.|_i$, $i = 1, 2, ..., g$ $\|.\|_v$ kiterjesztése L testre, és legyen $\|.\|_i$ a $|.|_i$ abszolútértéknek megfelelő normalizált abszolút érték. Ekkor:

$$\|\mathrm{Nm}_{L/K}\alpha\|_v = \|\prod_{i=1}^{g} \mathrm{Nm}_{L_i/\hat{K}}\alpha\|_v = \prod_{i=1}^{g} \|\mathrm{Nm}_{L_i/\hat{K}}\alpha\|_v = \prod_{i=1}^{g} |\alpha_i|^{n_i} = \prod_{i=1}^{g} \|\alpha\|_w$$

Ahol első egyenlőségnél azt használtuk ki, hogy a norma szorzatra bomlik a bővítésnek megfelelően ahogy a bekezdés elején láttuk. Utolsó előtti egyenlőségnél kiterjesztési tételt használtuk, valamint az utolsó egyenlőségnél az előző lemmát használtuk. $\square$

3.4.25. Tétel (Szorzat formula számtestekre)**.** *Legyen K egy algebrai számtest; minden nemnulla $\alpha \in K$ esetén:*

$$\prod_w \|\alpha\|_w = 1$$

Bizonyítás.

$$\prod_w \|\alpha\|_w = \prod_v \left(\prod_{w|v} \|\alpha\|_w \right) = \prod_v \|\mathrm{Nm}_{K/\mathbb{Q}}\alpha\|_v,$$

ahol v végigfut $\mathbb{Q}$ összes prímjén $2, 3, 5, 7, ..., \infty$. A második egyenlőséget az előző állításunk adja és utolsó szorzata 1 lesz a $\mathbb{Q}$ testre vonatkozó szorzatformula miatt. □

Véges bázis tétel bizonyításának befejezése

3.4.26. Állítás. *Legyen $C > 0$ alkalmasan megválasztott konstans amire $S = \{P \in E(\mathbb{Q}) | \overline{h}(p) \leq C\}$ tartalmazza $2E(\mathbb{Q})$ $E(\mathbb{Q})$ beli reprezentánsainak egy halmazát, ekkor S generálja $E(\mathbb{Q})$ csoportot.*

Bizonyítás. Tegyük fel, hogy $\exists Q \in E(\mathbb{Q})$ ami nincs benne az S által generált részcsoportban. Mivel $\overline{h}$ diszkrét értékeket vesz fel megválaszthatjuk Q pontunkat úgy, hogy $\overline{h}(Q)$ a lehető legkisebb legyen. S definíciójából adódóan $\exists P \in S$ amire $Q = P + 2R$ valamilyen $R \in E(\mathbb{Q})$. R nem lehet az S által generált részcsoportban hisz Q nincs benne, így $\overline{h}(R) \geq \overline{h}(Q)$. Így,

$$2\overline{h}(P) = \overline{h}(P+Q) + \overline{h}(P-Q) - 2\overline{h}(Q) \geq$$

$$\geq 0 + \overline{h}(2R) - 2\overline{h}(Q) =$$

$$= 4\overline{h}(R) - 2\overline{h}(Q) \geq 2\overline{h}(Q)$$

ami ellentmondás hiszen $\overline{h}(P) \leq C$ és $\overline{h}(Q) > C$. □

Mivel a magasság függvényt kiterjeszthettük számtestekre így ugyan ez a bizonyítás működik változtatás nélkül tetszőleges számtestre. Tehát ezzel beláttuk a következő tételt is:

3.4.27. Tétel. *Minden $\mathbb{Q} \leq \mathbb{K}$ számtest feletti E elliptikus görbére, és tetszőleges $n \in \mathbb{Z}$ egészre a $S^{(n)}(E/\mathbb{K})$ Selemer csoport véges.*

4. fejezet

A rang számolása

Most már tudjuk, hogy a csoportunk $E(\mathbb{Q})$ végesen generált, így a végesen generált Abel csoportokra vonatkozó alaptétel alapján:

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{torzió}} \oplus \mathbb{Z}^r,$$

valamilyen $r \geq 0$, ez az egész számot hívjuk $E(\mathbb{Q})$ rangjának. $E(\mathbb{Q})_{\text{torzió}}$ csoportot tudjuk, hogy kell kiszámolni hisz csak véges sok csoport realizálódhat elliptikus görbe torziós csoportjaként. Szeretnénk r rangot meghatározni, másképpen $E(\mathbb{Q})/E(\mathbb{Q})_{\text{torzió}}$ egy bázisát.

4.1. Rang számítása általános esetben

$S^2(E/\mathbb{Q})$ tekinthetjük a rang egy kiszámolható felső határának $Ш(E/\mathbb{Q})_2$ hibataggal. $E(\mathbb{Q})$ képét kell meghatároznunk $S^2(\mathbb{Q})$ csoportban.

$$\begin{array}{ccccccccc} 0 \to & E(\mathbb{Q})/2^n E(\mathbb{Q}) & \to & H^1(\mathbb{Q}, E_{2^n}) & \to & H^1(\mathbb{Q}, E)_{2^n} & \to 0 \\ & \uparrow & & \uparrow & & \uparrow & \\ 0 \to & E(\mathbb{Q})/2^{n+1} E(\mathbb{Q}) & \to & H^1(\mathbb{Q}, E_{2^{n+1}}) & \to & H^1(\mathbb{Q}, E)_{2^{n+1}} & \to 0 \end{array}$$

Ez alapján konstruálhatjuk a következő kommutatív diagrammot:

$$\begin{array}{ccccccccc}
0 & \to & E(\mathbb{Q})/2E(\mathbb{Q}) & \to & S^{(2)}(E/\mathbb{Q}) & \to & Ш(E/\mathbb{Q})_2 & \to & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \to & E(\mathbb{Q})/4E(\mathbb{Q}) & \to & S^{(4)}(E/\mathbb{Q}) & \to & Ш(E/\mathbb{Q})_4 & \to & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & \cdots & & \cdots & & \cdots & & \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \to & E(\mathbb{Q})/2^nE(\mathbb{Q}) & \to & S^{(2^n)}(E/\mathbb{Q}) & \to & Ш(E/\mathbb{Q})_{2^n} & \to & 0
\end{array}$$

A bal oldali függőleges leképezések a természetes hányados leképezések. Legyen $S^{(2,n)}(E/\mathbb{Q})$ az $S^{(2^n)}(E/\mathbb{Q})$ csoport képe $S^{(2)}(E/\mathbb{Q})$ csoportban.

4.1.1. Állítás. *Az $E(\mathbb{Q})/2E(\mathbb{Q})$ csoportot tartalmazza $\bigcap_n S^{(2,n)}(E/\mathbb{Q})$, és ezek egyenlőek ha nem létezik egy nem nulla elem $Ш(E/\mathbb{Q})$ csoportban ami osztható lenne 2 minden hatványával.*

Bizonyítás. Mivel a baloldali függőleges leképezések mind szürjektívek, $E(\mathbb{Q})/2E(\mathbb{Q})$ képe $S^{(2)(E/\mathbb{Q})}$ csoportban egyenlő $E(\mathbb{Q})/2^nE(\mathbb{Q})$ képével, amit tartalmaz $S^{(2,n)}(E/\mathbb{Q})$ a diagramm kommutativitása miatt. Másik irány, legyen $\gamma \in \bigcap_n S^{(2,n)}(E/\mathbb{Q})$, az az minden n egészre létezik egy elem $\gamma_n \in S^{(2^n)}$ ami γ elembe képződik. Legyen δ_n γ_n képe $Ш(E/\mathbb{Q})_{2^n}$ csoportban. Ekkor $2^{n-1}\delta_n = \delta_1$ minden n egészre, és így δ_1 osztható kettő minden hatványával. Ha az egyetlen ilyen elem $Ш(E/\mathbb{Q})$ csoportban 0, akkor γ benne van $E(\mathbb{Q})/2E(\mathbb{Q})$ képében. □

4.1.2. Megjegyzés. Mivel $Ш(E/\mathbb{Q})$ torziós csoport és $Ш(E/\mathbb{Q})_2$ véges, ha nem létezik nemnulla elem $Ш(E/\mathbb{Q})$ csoportban ami osztható lenne 2 minden hatványával, akkor a 2-csoport komponense $Ш(E/\mathbb{Q})$ csoportnak véges. Ha $2^{n_0-1}Ш(E/\mathbb{Q})_{2^{n_0}} = 0$, ekkor diagramm vadászattal kaphatjuk a következőt: $S^{(2,n_0)}(E/\mathbb{Q}) = S^{(2,n_0+1)}(E/\mathbb{Q}) = ... \cong E(\mathbb{Q})/2E(\mathbb{Q})$. Ez ad egy lehetséges stratégiát rang kiszámítására. Számoljuk ki $S^{(2)}$ csoportot, továbbá számoljuk ki $E(\mathbb{Q})$ $T(1)$ részcsoportját amiket a $h(P) \leq 10$ pontok generálnak. Ha $T(1)$ fedi $S^{(2)}$ csoportot akkor készen is vagyunk megtaláltuk az r rangot ezen felül még $E(\mathbb{Q})$ generátorait is. Ha nem számoljuk ki S^{2^2} csoportot, és a $T(2)$ részcsoportot amit a $h(P) \leq 10^2$ pontok generálnak. Ha $T(2)$ képe $S^{(2)}$ csoportban $S^{(2,2)}$ akkor megtaláltuk a csoportunk rangját. Ha nem tovább iterálhatjuk ezt a folyamatot. Legrosszabb eshetőség: A Tate-Shaferevich csoport tartalmaz egy nemnulla elemet amit kettő minden hatványa oszt, amikor is a fenti számítást örökké valóságig kéne folytatnunk.

Ez akkor történne meg ha például Ш$(E/\mathbb{Q})$ a $\mathbb{Q}/\mathbb{Z}$ csoportot tartalmazná. Széles körben sejtett hogy ez sohasem fordul elő.

4.1.3. Sejtés. *A Tate-Shafarevich csoport mindig véges.*

Ha a sejtés igaznak bizonyul a fenti stratégia algoritmussá válna $E(\mathbb{Q})$ csoport számításához.

4.1.4. Megjegyzés. 1987-ig nem volt ismert egyetlen elliptikus görbére sem $\mathbb{Q}$ feletti hogy a Tate-Shafarevich csoportja véges. Kolyvagin és Rubin bizonyította speciális esetben 1987 környékén. Azonban a sejtésnek még közel sem teljes a bizonyítása.

4.2. Rang explicit számolása

Előzőekben már láttuk, hogy a rang számítása lehet igen hosszadalmas folyamat, de esetenként vannak egyszerűbb módszerek. Hogy elkerüljük a $\mathbb{Q}$ testtől különböző L számtestekkel való számolást tegyük fel, hogy minden másodrendű pontunk racionális $\mathbb{Q}$ felett:

$$E : Y^2Z = (X - \alpha Z)(X - \beta Z)(X - \gamma Z)$$

ahol α, β, γ különböző egészek. $(X - \alpha Z)(X - \beta Z)(X - \gamma Z)$ diszkriminánsa:

$$\Delta = (\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \alpha)^2.$$

4.2.1. Állítás. *$E(\mathbb{Q})$ rangja r teljesíti a következő egyenlőtlenséget:*

$$r \leq \{p | p \text{ osztja } 2\Delta\}$$

Bizonyítás. Mivel $E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{torzió}} \oplus \mathbb{Z}^r$, ezért $E(\mathbb{Q})/2E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{torzió}}/2E(\mathbb{Q})_{\text{torzió}} \oplus (\mathbb{Z}/2\mathbb{Z})^r$. Mivel $E(\mathbb{Q})_{\text{torzió}}$ véges, a $E(\mathbb{Q})_{\text{torzió}} \xrightarrow{\cdot 2} E(\mathbb{Q})_{\text{torzió}}$ leképezés magjának és komagjának ugyan az a rendje, azaz $E(\mathbb{Q})_{\text{torzió}}/2E(\mathbb{Q})_{\text{torzió}} \cong (\mathbb{Z}/2\mathbb{Z})^2$. Van egy:

$$E(\mathbb{Q})/2E(\mathbb{Q}) \to (\mathbb{Q}^\times/\mathbb{Q}^{2\times})^2$$

egy beágyazás és a képét tartalmazza a $\mathbb{Q}^\times/\mathbb{Q}^{2\times}$ két részcsoportjának szorzata; -1 és azon prímek melyekre E elliptikus görbének rossz redukciója van, azaz azok amik osztják 2Δ által generált részcsoportok. □

Lehetséges ezt a becslést javítani. Legyen T_1 azon prímek halmaza, amik osztják Δ és a redukció csomóponti, és legyen T_2 azon prímek halmaza amik osztják Δ és a redukció csúcsos. Az az T_1 azon prímek halmaza amikre modulo két gyöke egybeesik $(X-\alpha)(X-\beta)(X-\gamma)$ polinomnak, és T_2 azon prímek melyekre modulo mind a három gyök egybe esik. Legyen t_1 és t_2 a T_1 és T_2 halmazok elemszáma.

4.2.2. Állítás. *$E(\mathbb{Q})$ r rangja kielégíti $r \leq t_1 + 2t_2 - 1$ egyenlőtlenséget.*

Bizonyítás. Legyen $\varphi_\alpha : E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathbb{Q}^\times/\mathbb{Q}^{2\times}$

$$\varphi_\alpha((x:y:z)) = \begin{cases} (\frac{x}{z} - \alpha)\mathbb{Q}^{\times 2} & \text{ha } z \neq 0, x \neq \alpha z \\ (\alpha-\beta)(\alpha-\gamma)\mathbb{Q}^\times & \text{ha } z \neq 0, x = \alpha z \\ \mathbb{Q}^\times & \text{ha } (x:y:z) = (0:1:0) \end{cases}$$

φ_β leképezést definiálhatjuk ugyan így, ekkor

$$P \mapsto (\varphi_\alpha(P), \varphi_\beta(P)) : E(\mathbb{Q})/2E(\mathbb{Q}) \to (\mathbb{Q}^\times/\mathbb{Q}^{2\times})^2$$

leképezés injektív. Minden p prímre, legyen $\varphi_p(P)$ a $(\mathbb{Z}/2\mathbb{Z})^2$ egy eleme aminek a koordinátái:

$$\mathrm{ord}_p(\varphi_\alpha(P)) \bmod 2, \text{ és } \mathrm{ord}_p(\varphi_\beta(P)) \bmod 2$$

valamint $\varphi_\infty(P)$ legyen eleme a $\{\pm 1\}^2$ halmaznak és koordinátái:

$$\mathrm{sign}(\varphi_\alpha(P)), \text{ és } \mathrm{sign}(\varphi_\beta(P))$$

Bizonyítás következő lépéseke keresztül végezzük:

1. (a) ha p nem osztja Δ, akkor $\varphi_p(P) = 0$ minden P pontra;
2. (b) ha $p \in T_1$, akkor $\varphi_p(P)$ tartalmazza az $\mathbb{F}_2^2$ diagonálisa minden P pontra;
3. (c) amikor α, β, γ rendezettek, azaz $\alpha < \beta < \gamma$, $\varphi_\infty(P)$ egyenlő $(+1,+1)$ vagy $(+1,-1)$.

A $p = 2$ esetet kivéve (a) pontot már beláttuk. (b) esetet csak $\alpha \equiv \beta \bmod p$ és $P = (x : y : 1)$, $x \neq \alpha, \beta, \gamma$. Legyen

$$a = \mathrm{ord}_p(x-\alpha),\ b = \mathrm{ord}_p(x-\beta),\ c = \mathrm{ord}_p(x-\gamma).$$

Mivel

$$(x-\alpha)(x-\beta)(x-\gamma)$$

egy négyzet (elliptikus görbénk egy pontja), így $a+b+c \equiv \bmod 2$. Ha $a<0$, akkor p^{-a} megjelenik mint x nevező faktora, mert $\alpha \in \mathbb{Z}$, és ebből következik hogy $b=a=c$. Hisz $a+b+c \equiv \bmod 2$ ez implikálja, hogy $a \equiv b \equiv c \equiv 0 \bmod 2$ és így $\varphi_p(P)=0$. Ugyanez az érvelés elmondható $b<0$ és $c<0$ esetén. Ha $a>0$, akkor p osztja az $x-\alpha$ számlálóját. Mivel p nem osztja $\alpha-\gamma$, így $(\alpha-\gamma)+(x-\alpha)=(x-\gamma)$ sem osztja ezzel $c=0$. Most $a+b \equiv 0 \bmod 2$ következik, hogy $\varphi_p(P)$ az $\mathbb{F}_2^2$ diagonálisában van. Hasonló érvelés elmondható $b>0$ és $c>0$ esetén. (b) további alesetei hasonló számolásokkal bizonyíthatók.

Végezetül lássuk be (c) pontot. Legyen $P=(x:y:1)$, $x \neq \alpha, \beta, \gamma$. Feltehetjük, hogy $\alpha<\beta<\gamma$, és így $(x-\alpha)>(x-\beta)>(x-\gamma)$. Ekkor $\varphi_\infty(P)=(+1,+1)$,$(+1,-1)$ vagy $(-1,-1)$. Azonban

$$(x-\alpha)(x-\beta)(x-\gamma)$$

egy négyzet $\mathbb{Q}$ testben így a $(-1,-1)$ pár nem fordulhat elő. Az $x=\alpha$, $x=\beta$ és $x=\gamma$ esetek ehhez hasonlóan egyszerűen beláthatók. $\square$

4.2.3. Példa. Vegyük a következő elliptikus görbét:

$$E: Y^2Z = X^3 - XZ^2$$

erre a görbére $(\alpha,\beta,\gamma)=(-1,0,1)$. Az egyetlen rossz prím 2, amire a redukciónk csomóponti. Ezért $r=0$, és E görbének nincs végtelen rendű pontja:

$$E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

Irodalomjegyzék

[1] J.S. Milne, *Elliptic Curves*, World Scientific, 2020

[2] G. Zábrádi, *Algebraic Number Theory*, 2020, [Online], https://zabradi.web.elte.hu/Jegyzetek/algszamjegyzet.pdf

[3] J.S. Milne, *Algebraic Number Theory*, 2020, [Online], https://www.jmilne.org/math/CourseNotes/ANT.pdf

[4] J.S. Milne, *Fields and Galois Theory*, Kea Books, 2022

[5] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, 2009

[6] Joseph H. Silverman, Jhon T. Tate, *Rational Points on Elliptic Curves*, Springer, 2015