Elliptikus görbék artimetikája

Csahók Tímea

Témavezető: Zábrádi Gergely

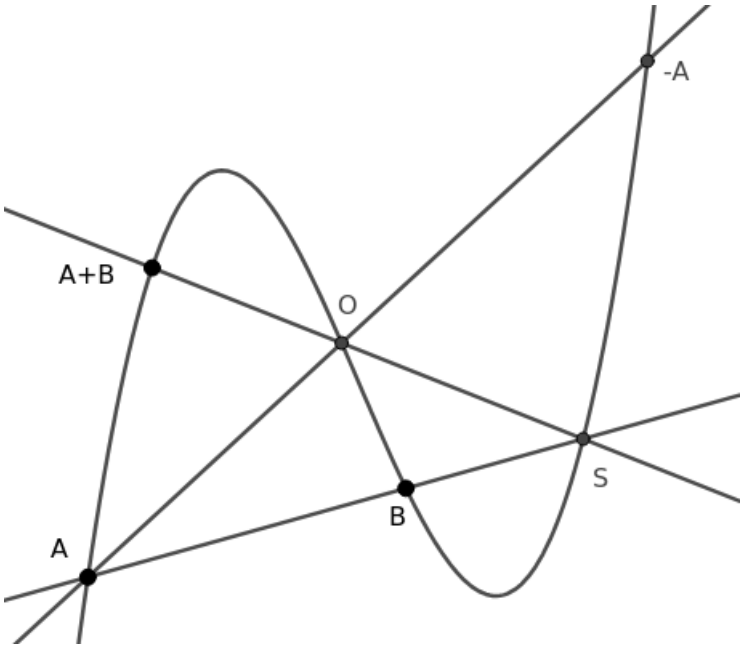
1 Bevezetés

Szakdolgozatomban a csoportkohomológiával foglalkoztam, majd a mesterképzés első félévében többek között algebrai számelméletről és algebrai görbékről tanultam. Az elliptikus görbék témaköre – amely egy sokat kutatott része az algebrai számelméletnek – így jól illeszkedett a tanulmányaimba. James Milne jegyzetéből többek között a komplex számok feletti elliptikus görbékről is sok mindent tanultam, azonban ebben az összefoglalóban az elliptikus görbék aritmetikájáról írok részletesebben, a végső cél a véges bázis-tétel belátása a racionális számok teste felett.

2 Elliptikus görbék csoportstruktúrája

Definíció 2.1. Egy **elliptikus görbe** a k tökéletes test felett egy 1 génuszú görbe, amelyen ki van jelölve egy $O \in E(k)$ pont.

A görbe pontjain a következő műveletet tudjuk definiálni: Az A és B pontok összegéhez legyen S az AB egyenes harmadik metszéspontja a görbével, ekkor $A+B$ legyen az SO egyenes harmadik metszéspontja a görbével. (Ha $P = Q$, akkor a PQ egyenes a görbe P pontbeli érintőjét jelöli.)



Világos, hogy ez a művelet kommutatív. Egységelem lesz az O pont, egy A pont inverze pedig az OA egyenes görbével vett harmadik metszéspontja lesz. A művelet asszociativitása a Bézout-tételből következik.

Jelölés 2.2. *Az E/k görbe n-edrendű pontjainak csoportja $E_n(k)$.*

3 Kohomológiai emlékeztető

Definíció 3.1. Ha G csoport, M pedig $\mathbb{Z}G$-modulus, akkor az $f : G \to M$ leképezést **keresztezett homomorfizmusnak** hívjuk, ha minden $\sigma, \tau \in G$ esetén

$$f(\sigma\tau) = f(\sigma) + \sigma f(\tau) \quad \text{teljesül.}$$

A keresztezett homomorfizmusok közül **principálisnak** nevezzük azokat, amelyekre

$$f(\sigma) = \sigma m - m \quad \text{valamely } m \in M \text{ elemre.}$$

Definíció 3.2. Ha G csoport, M pedig $\mathbb{Z}G$-modulus, akkor a **nulladik csoportkomomológia** $H^0(G, M) = M^G$, ahol $M^G = \{m \in M \mid gm = m\}$. Az **első kohomológia** pedig

$$H^1(G, M) = \frac{\{G \to M \text{ keresztezett hom.}\}}{\{G \to M \text{ princ. keresztezett hom.}\}}.$$

Tétel 3.3 (A kohomológia hosszú egzakt sorozata)**.** *Ha $0 \to A \to B \to C \to 0$ $\mathbb{Z}G$-modulusok egzakt sorozata, akkor a következő sorozat egzakt:*

$$0 \to H^0(G, A) \to H^0(G, B) \to H^0(G, C) \to H^1(G, A) \to H^1(G, B) \to \dots$$

Az Inf és Res leképezésekből kapjuk a következőt:

Állítás 3.4. *Ha $H \leq G$ részcsoport, M pedig $\mathbb{Z}G$-modulus, akkor a*

$$0 \to H^1\left({}^{G}\!/_{H}, M^H\right) \xrightarrow{\text{Inf}} H^1(G, M) \xrightarrow{\text{Res}} H^1(H, M)$$

sorozat egzakt.

A csoportkohomológiát végtelen csoportokra is tudjuk definiálni.

Definíció 3.5. Ha k test, $G = \text{Gal}(k^{al}/k)$, akkor legyen

$$H^1(G, M) = \varinjlim_{H \lhd G} H^1\left({}^{G}\!/_{H}, M^H\right).$$

Jelölés 3.6. *Ha E elliptikus görbe k felett, akkor legyen*

$$H^i\left(\text{Gal}(k^{al}/k), E(k^{al})\right) = H^i(k, E).$$

4 A véges bázis-tétel a racionálisok felett

Az elliptikus görbék csoportjainak vizsgálatánál az egyik alapvető tétel a Mordell-Weil-tétel, amely azt mondja ki, hogy $E(K)$ végesen generált minden K számtestre. Itt most csak $K = \mathbb{Q}$-ra vázolom a bizonyítást, azoban ez kisebb módosításokkal hamar általánosodik tetszőleges számtestre.

Először azt fogjuk belátni, hogy ${}^{E(\mathbb{Q})}\!/_{nE(\mathbb{Q})}$ véges. Ez ugyan gyengébb állítás a véges bázis-tételnél, azonban a bizonyítás ezen része igényel több munkát és (algebrai számelméleti) tudást, utána már rövid úton adódik a véges bázis-tétel is.

Lemma 4.1. *Ha a K test algebrailag zárt és E/K elliptikus görbe, akkor az n-nel való szorzás, azaz $\varphi : E(K) \to E(K)$, $\varphi(P) = nP$ szürjektív.*

Ebből kapjuk, hogy a

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

sorozat egzakt, majd a kohomológia hosszú egzakt sorozatából

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

egzakt, vagyis az n-nel való szorzásoknál képet, illetve magot véve kapjuk, hogy

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

is egzakt.

Ha a görbét $\mathbb{Q}$ helyett $\mathbb{Q}_p$ felett tekintjük, akkor a következő kommutatív diagramot kapjuk:

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

$H^1(\mathbb{Q}, E_n)$-t szeretnénk egy olyan részcsoportjára lecserélni, amely még tartalmazza ${}^{E(\mathbb{Q})}\!/_{nE(\mathbb{Q})}$ képét, de be lehet róla látni, hogy véges. Ha egy $\gamma \in H^1(\mathbb{Q}, E_n)$ benne van a képben, akkor a redukáltja, γ_p pedig az alsó sorbeli képben van benne. A sorozat egzaktsága miatt az ${}^{E(\mathbb{Q}_p)}\!/_{nE(\mathbb{Q}_p)} \to H^1(\mathbb{Q}_p, E_n)$ leképezés képe megegyezik a $H^1(\mathbb{Q}_p, E_n) \to H^1(\mathbb{Q}_p, E)_n$ leképezés magjával, így definiálhatjuk a következő csoportokat:

Definíció 4.2. Az $E/\mathbb{Q}$ elliptikus görbe **Selmer-csoportja**

$$S^{(n)}(E/\mathbb{Q}) = \{\gamma \in H^1(\mathbb{Q}, E_n) \mid \forall p\ \gamma_p \in H^1(\mathbb{Q}_p, E_n) \text{ a lenti képben van benne}\} =$$

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

Tate-Safarevics-csoportja pedig

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

A

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

egzakt sorozatra a kígyó-lemmából azt kapjuk, hogy

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

egzakt, vagyis ${}^{E(\mathbb{Q})}\!/_{nE(\mathbb{Q})}$ végességéhez elegendő azt megmutatni, hogy $S^{(n)}(E/\mathbb{Q})$ véges.

A Selmer-csoportot $\mathbb{Q}$ helyett tetszőleges K számtestre is definiálni tudjuk.

Lemma 4.3. *Minden véges $K/\mathbb{Q}$ Galois-bővítésre és $n \geq 1$ egészre az*

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

leképezés magja véges.

Tehát a homomorfizmustétel miatt ha $S^{(n)}(E/K)$ véges valamely K-ra, akkor $S^{(n)}(E/\mathbb{Q})$ is az. A $S^{(n)}(E/K)$ csoport végességének bizonyításakor két fontos algebrai számelméleti állítást használunk fel:

Tétel 4.4. *Ha $K/\mathbb{Q}$ véges bővítés, akkor az osztályszáma véges.*

Tétel 4.5 (Dedekind)**.** *Ha $K/\mathbb{Q}$ véges bővítés, akkor az algebrai egészek között az egységek csoportja végesen generált.*

Most pedig azt fogjuk belátni, hogy $E(\mathbb{Q})$ végesen generált, ehhez magasságfüggvényekre lesz szükségünk. A magasságfüggvény az abszolút értékre hasonlít, először definiáljuk a projektív tér racionális pontjain:

Definíció 4.6. Ha $P = (a_0 : \ldots : a_n) \in \mathbb{P}^n(\mathbb{Q})$, akkor $(a_0, \ldots, a_n)$ **primitív reprezentánsa** P-nek, ha $a_i \in \mathbb{Z}$ és legnagyobb közös osztójuk 1. Ekkor legyen $H(P) = \max_i |a_i|$.

Ehhez hasonlóan tudunk magasságfüggvényt definiálni E racionális pontjain is, a következőképpen:

Definíció 4.7. Egy $P \in E(\mathbb{Q})$ pont esetén legyen $H(P) = H(x(P) : z(P))$ ha $z(P) \neq 0$, és 1 ha $z(P) = 0$. Legyen $h(P) = \log H(P)$.

Az E-n lévő magasságfüggvényt többféleképpen is lehet definiálni, ezek különbsége korlátos. Két tulajdonságot megkövetelve már egyértelműen fog létezni egy kanonikus magasságfüggvény, erről szól a következő állítás.

Tétel 4.8. *Pontosan egy olyan $\hat{h} : E(\mathbb{Q}) \to \mathbb{R}$ függvény létezik, amelyre $\hat{h}(P) - h(P)$ korlátos $E(\mathbb{Q})$-n és $\hat{h}(2P) = 4\hat{h}(P)$, ezt hívjuk a* ***kanonikus magasságfüggvénynek****. Konkrétan megadva*

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

ráadásul $\hat{h}$ kvadratikus alak is.

Állítás 4.9. *Minden $C \geq 0$ esetén $\{P \in E(\mathbb{Q}) \mid \hat{h}(P) \leq C\}$ véges, valamint $\hat{h}(P) \geq 0$, egyenlőség pedig pontosan akkor teljesül, ha P rendje véges.*

Innen a következő állításból már következik, hogy $E(\mathbb{Q})$ végesen generált:

Állítás 4.10. *Legyen C olyan, hogy $S = \{P \in E(\mathbb{Q}) \mid \hat{h}(P) \leq C\}$ tartalmazza ${}^{E(\mathbb{Q})}\!/_{2E(\mathbb{Q})}$ mellékosztályainak egy-egy reprezentánsát. (Ilyen C létezik, hiszen ${}^{E(\mathbb{Q})}\!/_{2E(\mathbb{Q})}$ véges.) Ekkor S generálja $E(\mathbb{Q})$-t.*

Felhasznált irodalom

- Milne, James S. *Elliptic curves*. World Scientific, 2020.