Elliptikus görbék artimetikája

Csahók Tímea

Témavezető:
Zábrádi Gergely

2020. december 18.

Áttekintés

- Csoportstruktúra elliptikus görbéken

Áttekintés

- Csoportstruktúra elliptikus görbéken
- Gyenge véges-bázis tétel

Áttekintés

- Csoportstruktúra elliptikus görbéken
- Gyenge véges-bázis tétel
- A véges-bázis tétel bizonyítása

Áttekintés

- Csoportstruktúra elliptikus görbéken
- Gyenge véges-bázis tétel
- A véges-bázis tétel bizonyítása
- Kitekintés

Elliptikus görbék

Definíció

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

Elliptikus görbék

Definíció

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

Ekvivalensen egy harmadfokú projektív nemszinguláris k feletti síkgörbe egy $O \in E(k)$ ponttal.

Elliptikus görbék

Definíció

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

Ekvivalensen egy harmadfokú projektív nemszinguláris k feletti síkgörbe egy $O \in E(k)$ ponttal.

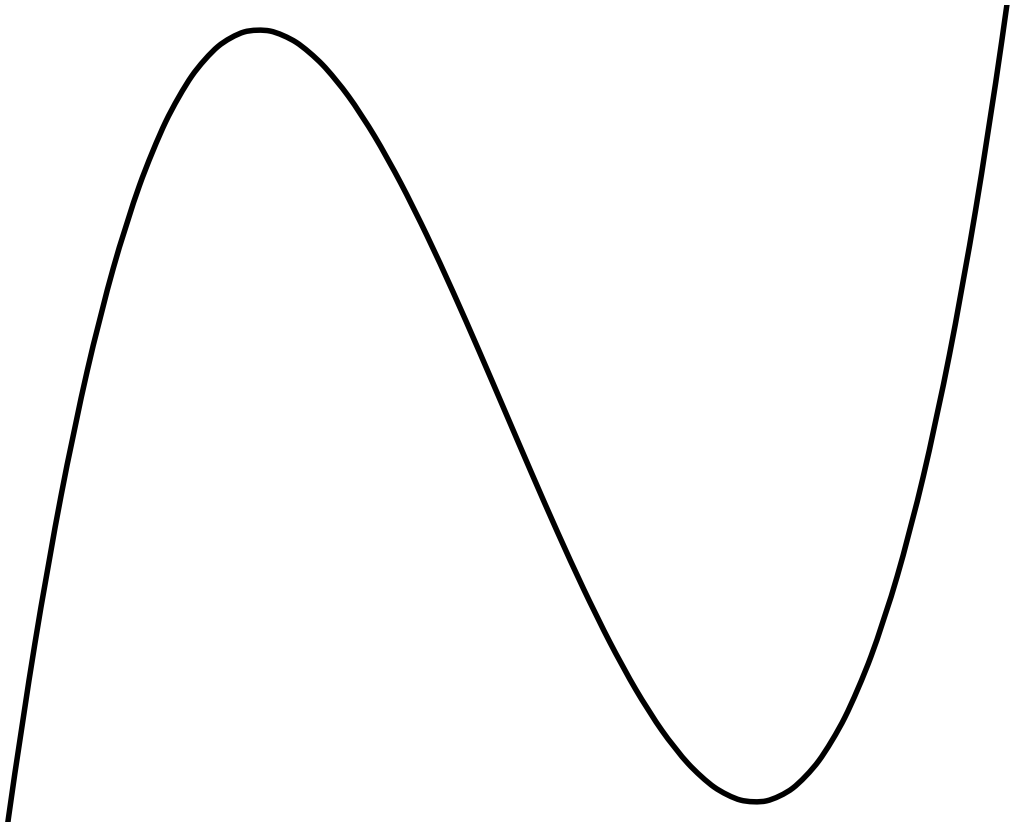
Állítás

$E(k)$-n létezik Abel-csoportstruktúra, amely független O választásától.

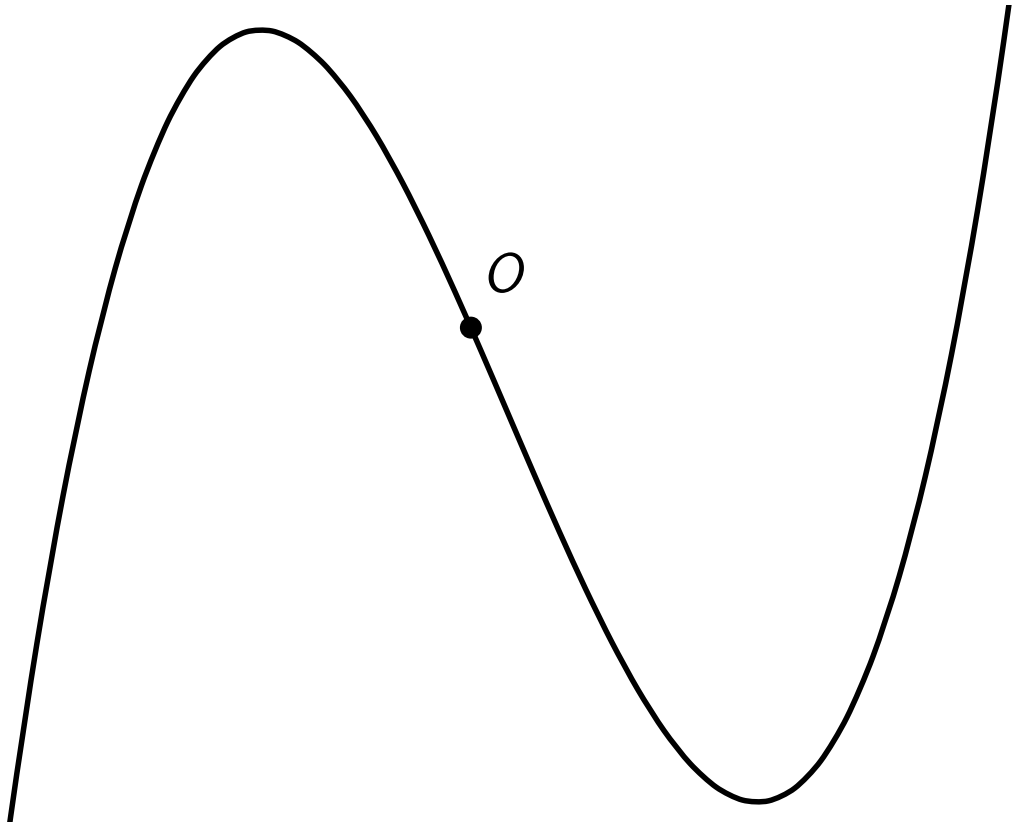
Tétel (Véges bázis)

$E(K)$ végesen generált minden K számtestre.

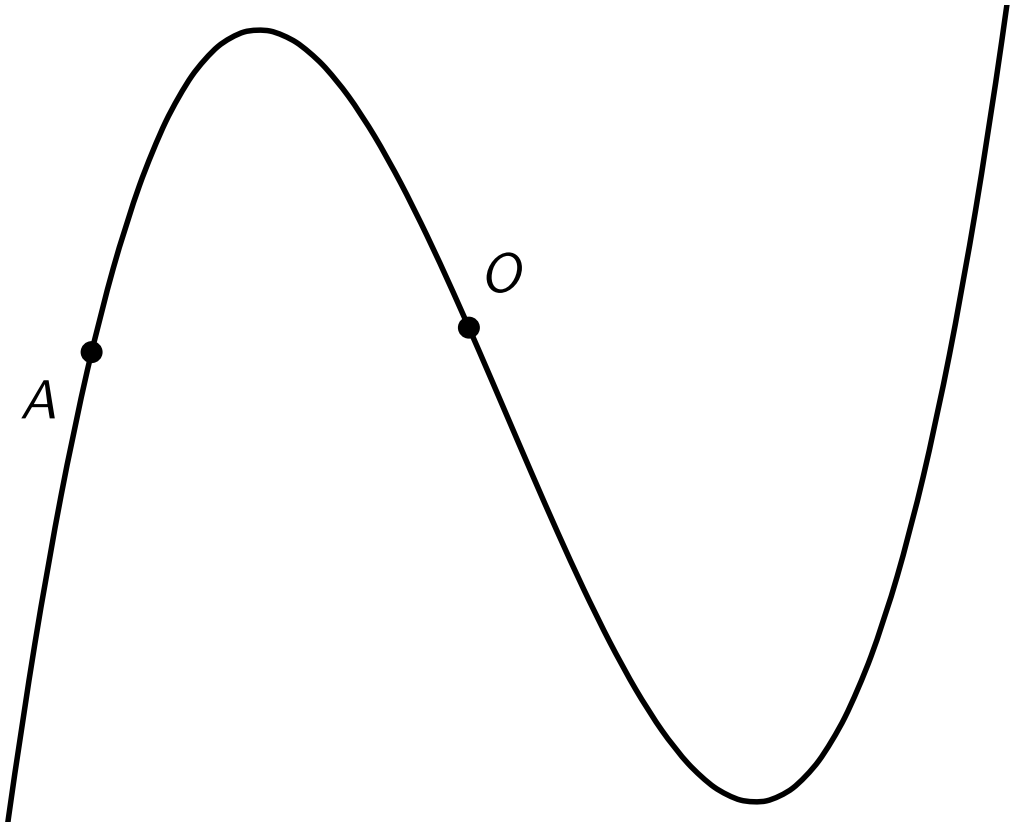
Elliptikus görbék csoportstruktúrája



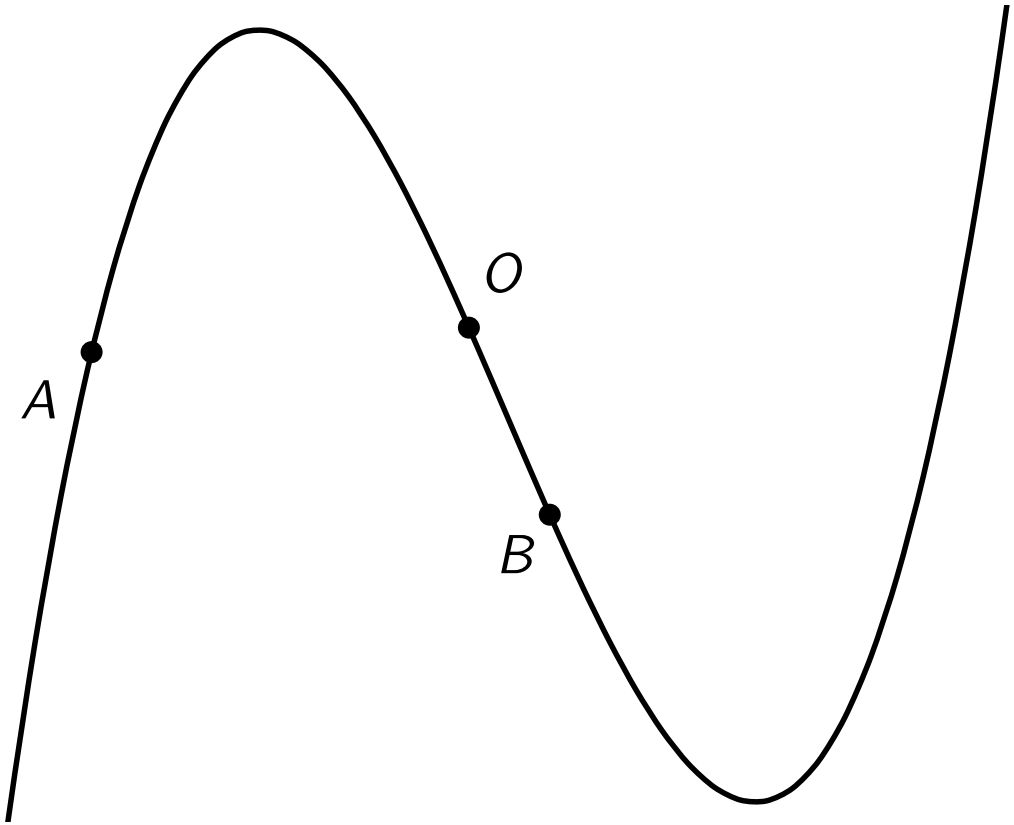
Elliptikus görbék csoportstruktúrája



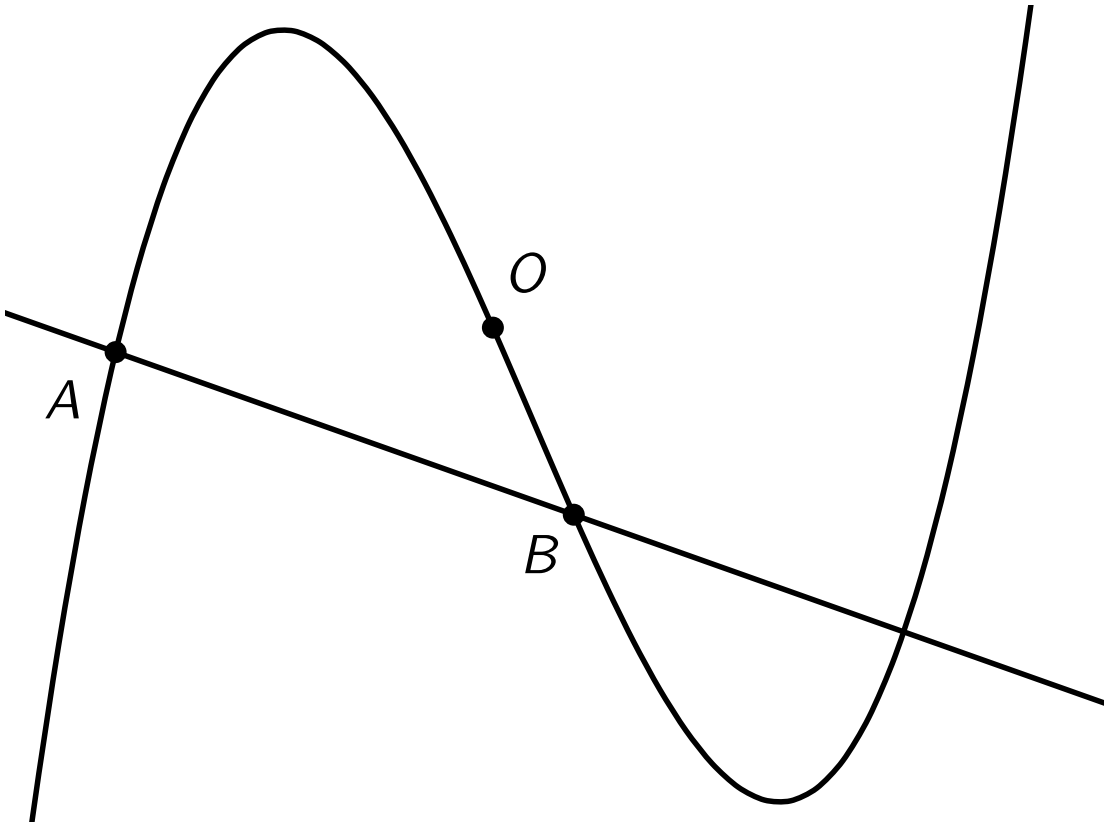
Elliptikus görbék csoportstruktúrája



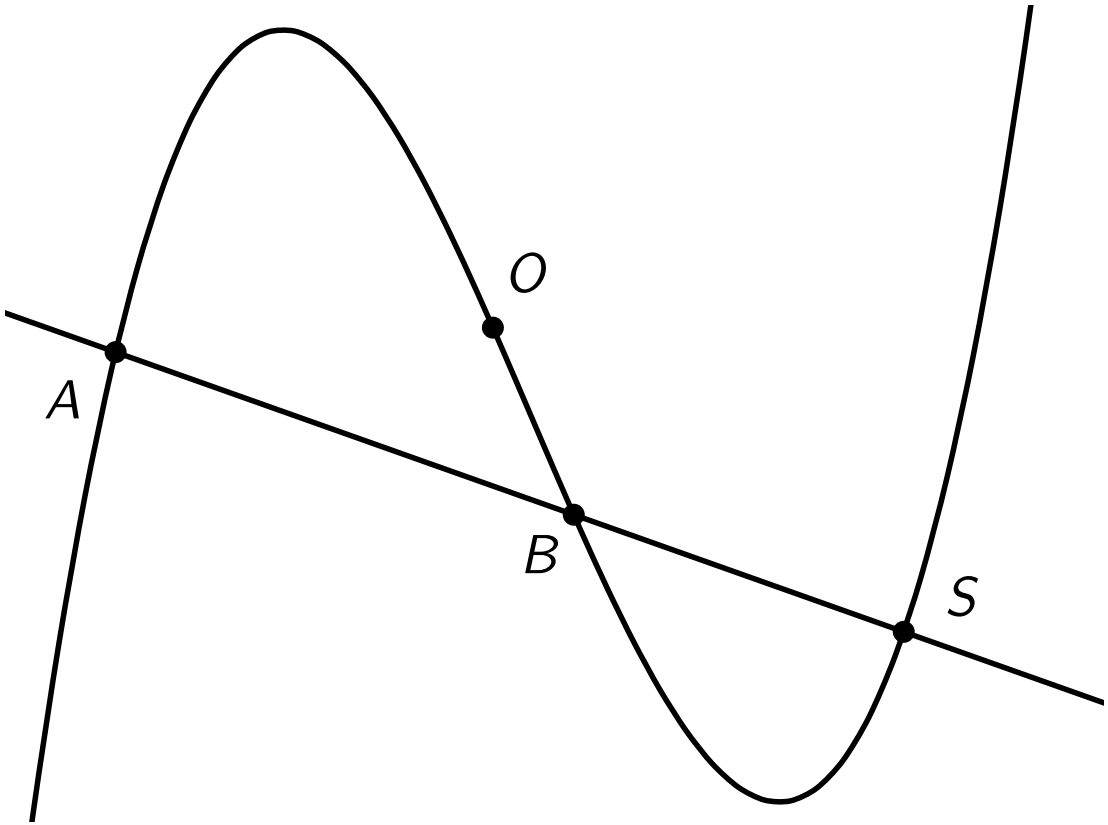
Elliptikus görbék csoportstruktúrája



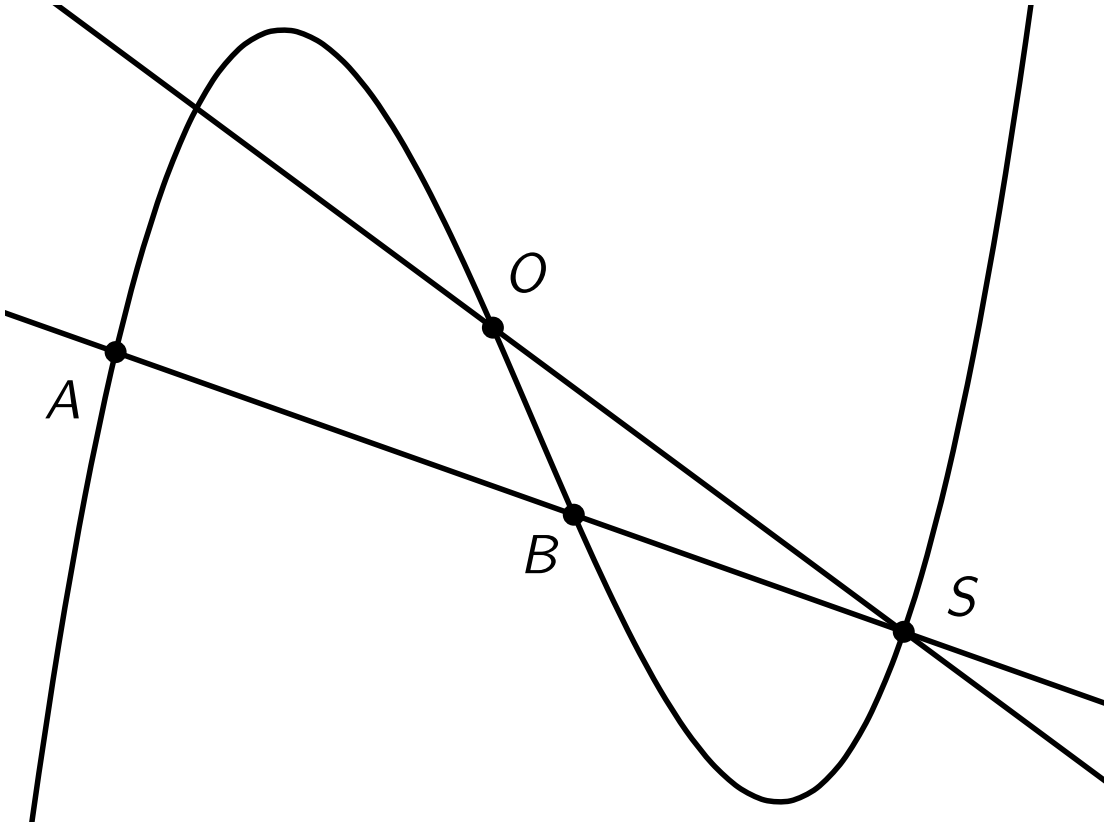
Elliptikus görbék csoportstruktúrája



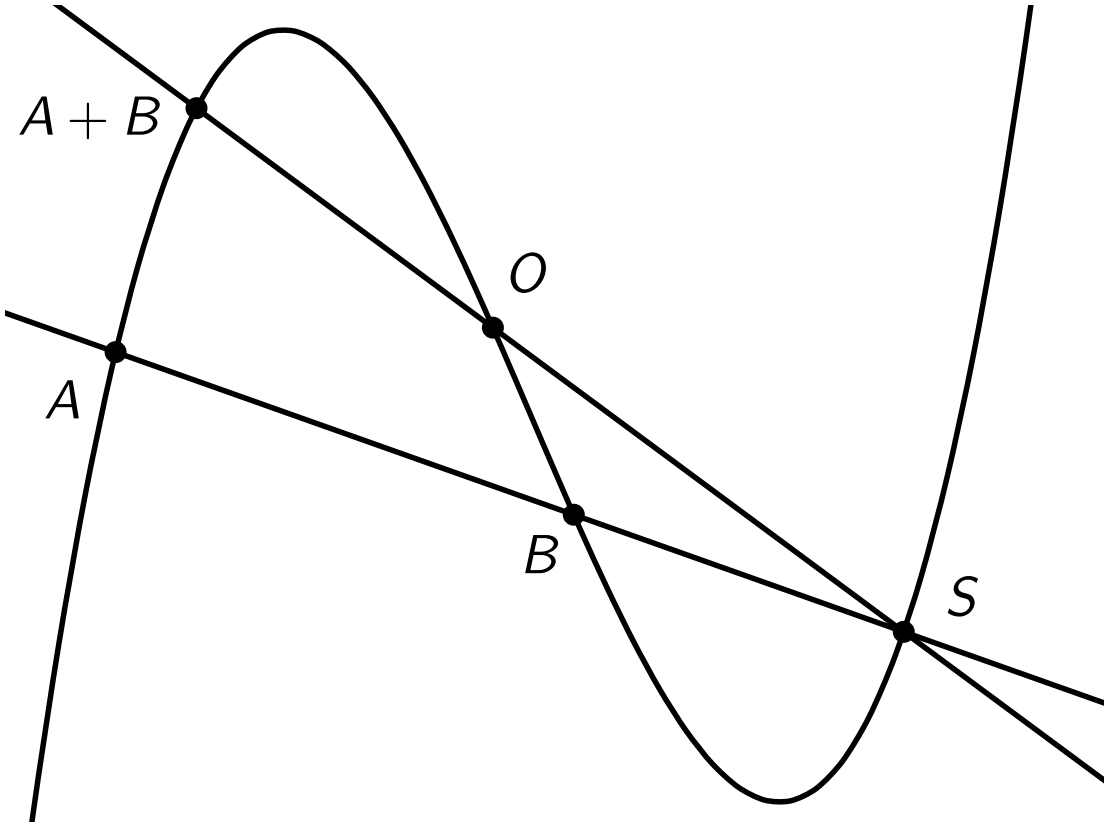
Elliptikus görbék csoportstruktúrája



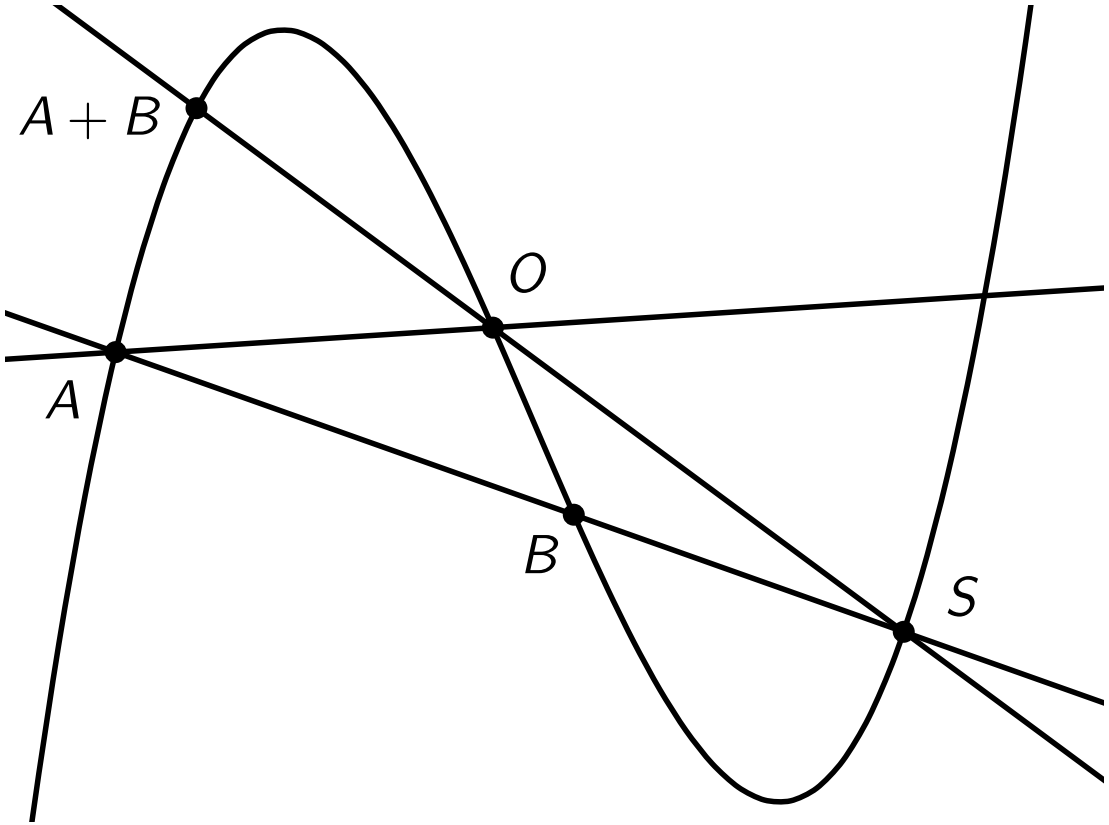
Elliptikus görbék csoportstruktúrája



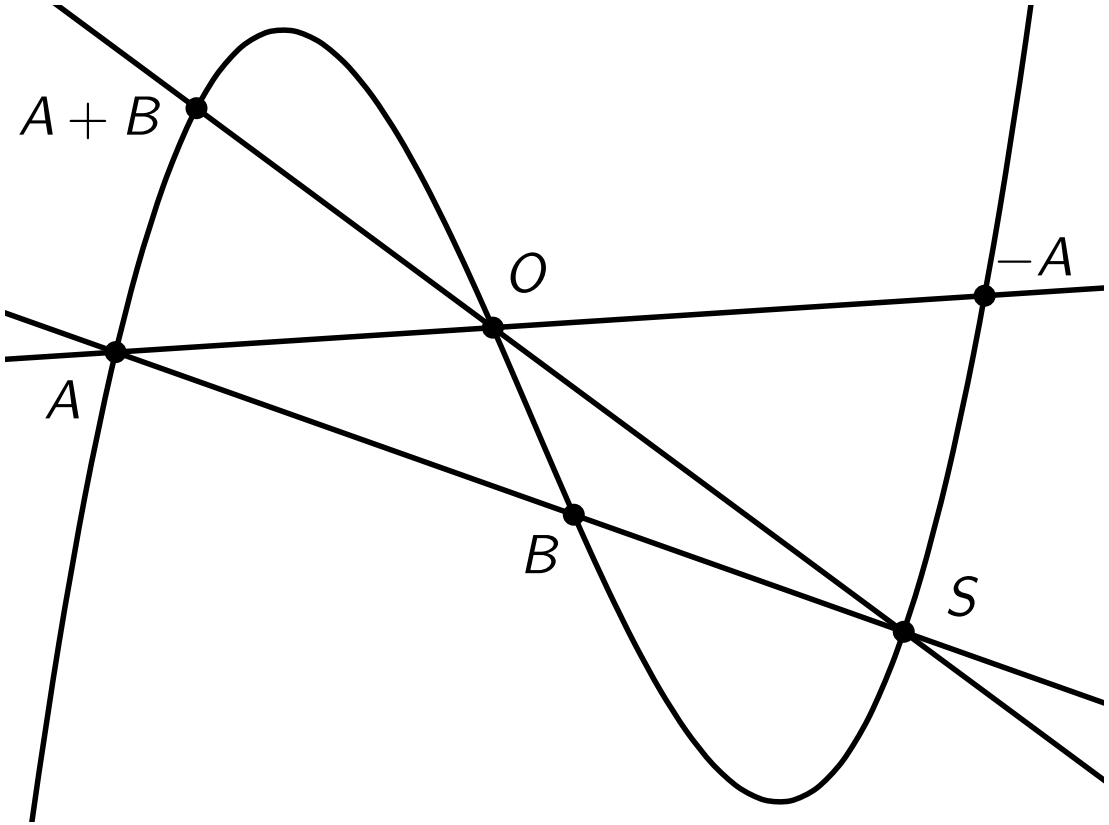
Elliptikus görbék csoportstruktúrája



Elliptikus görbék csoportstruktúrája



Elliptikus görbék csoportstruktúrája



A gyenge véges-bázis tétel

Cél:

A gyenge véges-bázis tétel

Cél: $E(\mathbb{Q})/nE(\mathbb{Q})$ véges.

A gyenge véges-bázis tétel

Cél: $E(\mathbb{Q})/nE(\mathbb{Q})$ véges. Később:

A gyenge véges-bázis tétel

Cél: $E(\mathbb{Q})/nE(\mathbb{Q})$ véges. Később: $E(\mathbb{Q})$ végesen generált.

A gyenge véges-bázis tétel

Cél: ${}^{E(\mathbb{Q})}\!/_{nE(\mathbb{Q})}$ véges. Később: $E(\mathbb{Q})$ végesen generált.

Lemma

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.

A gyenge véges-bázis tétel

Cél: $E(\mathbb{Q})/nE(\mathbb{Q})$ véges. Később: $E(\mathbb{Q})$ végesen generált.

Lemma

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.

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

A gyenge véges-bázis tétel

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

A gyenge véges-bázis tétel

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

Kohomológia hosszú egzakt sorozatából:

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

A gyenge véges-bázis tétel

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

Kohomológia hosszú egzakt sorozatából:

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

Vagyis

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

A gyenge véges-bázis tétel

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

A gyenge véges-bázis tétel

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

Definíció

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

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

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

A gyenge véges-bázis tétel

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

Definíció

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

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

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

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 gyenge véges-bázis tétel

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

A gyenge véges-bázis tétel

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

Kígyó-lemmából:

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

A gyenge véges-bázis tétel

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

Kígyó-lemmából:

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

Lemma

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.

A gyenge véges-bázis tétel

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

Kígyó-lemmából:

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

Lemma

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 elég belátni, hogy $S^{(n)}(E/K)$ véges valamely K-ra.

Magasságfüggvények

Definíció

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.

Magasságfüggvények

Definíció

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

Magasságfüggvények

Definíció

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

Definíció

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

Magasságfüggvények

Definíció

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

Definíció

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

Magasságfüggvények

Definíció

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

Definíció

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

Állítás

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.

A bizonyítás vége

Állítás

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.

A bizonyítás vége

Állítás

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.

Állítás

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.

Kitekintés

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{tors} \times \mathbb{Z}^r$$

Kitekintés

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{tors} \times \mathbb{Z}^r$$

$$E : Y^2Z = X^3 - XZ^2 \rightsquigarrow E(\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$$

Kitekintés

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{tors} \times \mathbb{Z}^r$$

$$E : Y^2Z = X^3 - XZ^2 \rightsquigarrow E(\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$$

Sejtés

Tetszőlegesen nagy r-re létezik r rangú elliptikus görbe $\mathbb{Q}$ felett.

Kitekintés

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{tors} \times \mathbb{Z}^r$$

$$E : Y^2Z = X^3 - XZ^2 \rightsquigarrow E(\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$$

Sejtés

Tetszőlegesen nagy r-re létezik r rangú elliptikus görbe $\mathbb{Q}$ felett.

$$Y^2 + XY + Y = X^3 - X^2 -$$
$$-244537673336319601463803487168961769270757573821859853707X +$$
$$+961710182053183034546222979258806817743270$$
$$6820289644342389578309898984381511214999310$$

Kitekintés

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{tors} \times \mathbb{Z}^r$$

$$E : Y^2Z = X^3 - XZ^2 \rightsquigarrow E(\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$$

Sejtés

Tetszőlegesen nagy r-re létezik r rangú elliptikus görbe $\mathbb{Q}$ felett.

$$Y^2 + XY + Y = X^3 - X^2 -$$
$$-2445376733363196014638034871689617692707575738218598537 07X +$$
$$+961710182053183034546222979258806817743 27$$
$$0682028964434238957830989898438151121499931$$

Sejtés

$Ш(E/\mathbb{Q})$ mindig véges.

Köszönöm a figyelmet!