Nagell–Lutz-tétel

Szőri Vajk

1. Bevezetés

A Nagell-Lutz-tétel azt állítja, hogy ha $E/\mathbb{Q}$ egy elliptikus görbe akkor a nem nulla torzió pontjainak egész koordinátái vannak, és vagy 2 a rendjük, vagy az y koordinátájuk négyzete osztja a görbe diszkriminánsát.
Ez a tétel megkönnyíti a görbe torzió pontjainak megtalálását. Ugyanakkor a tétel megfordítása nem igaz. Tehát a tétel megadja az összes lehetséges véges rendű pontot, de ahoz hogy biztos legyünk egy pont rendjének végességében találnunk kell egy n-t, hogy $nP = 0$. De a tételt lehet arra is használni hogy bebizonyosodjuk arról hogy egy pont nem véges rendű. Számítsuk ki $P, 2P, 4P, ...$ x-koordinátáját amíg egyszer nem egész számot kapunk.
Az állítások és tételek bizonyításai megtalálhatóak [1]-ben. Elliptikus görbékkel és formális csoportokkal kapcsolatos alap állítások megtalálhatóak az előző egyéni kutatómunkámban.

2. Formális csoportokkal kapcsolatos állítások

2.1. Definíció. Egy invariáns differenciál az F/R formális csoporton egy differenciál forma

$$\omega(T) = P(T)dT \in R[[T]]dt$$

amire teljesül

$$\omega \circ F(T,S) = \omega(T).$$

Kiírva $\omega(T) = P(T)dT$ egy invariáns differenciál, ha teljesül rá

$$P(F(T,S))F_X(T,S) = P(T),$$

ahol $F_X(X,Y)$ F első változó szerinti parciális deriváltja. Egy invariáns differenciál normált, ha $P(0) = 0$.

2.2. Állítás. *Legyen F/R egy formális csoport. Egyértelműen létezik egy normált invariáns differenciál F/R-en. Ezt meghatározza az alábbi formula:*

$$\omega = F_X(0,T)^{-1}dT.$$

Minden invariáns differneciál $a\omega$ alakú F/R-en valamilyen $a \in R$-re.

2.3. Következmény. *Legyen F/R és G/R két formális csoport amelyek normált invariáns differenciáljai ω_F és ω_G. Legyen $f : F \to G$ egy homomorfizmus.Ekkor*

$$\omega_G \circ f = f'(0)\omega_F.$$

2.4. Következmény. *Legyen F/R egy formális csoport és legyen $p \in \mathbb{Z}$ egy prím. Ekkor léteznek $f(T), g(T) \in R[[T]]$ hatványsorok hogy $f(0) = g(0) = 0$ és teljesül az alábbi:*

$$[p](T) = pf(T) + g(T^p).$$

2.5. Tétel. *Legyen R egy DVR ami teljes a maximális ideáljára, M-re, nézve, legyen $p = char(R/M)$, és legyen v az értékelés R-en. Legyen F/R egy formális csoport, és tegyük fel hogy $x \in F(M)$ rendje p^n valamilyen $n \geq 1$-re, tehát:*

$$[p^n](x) = 0 \text{ és } [p^{n-1}](x) \neq 0.$$

Ekkor

$$v(x) \leq \tfrac{v(p)}{p^n - p^{n-1}}.$$

3. Nagell-Lutz-tétel

3.1. Tétel. *Legyen K lokális test, teljes egy v diszkrét értékelésre, R az egészek gyűrűje, M R maximális idálja, π: $M = \pi R$ és $k = R/M$ az R-hez tartozó maradéktest. Tegyük fel hogy $char(K) = 0$ és $p = char(k) > 0$. Legyen E/K egy elliptikus görbe, amit az alábbi Weierstrass egyenlet határoz meg:*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

ahol minden $a_i \in R$. Legyen $P \in E(K)$ egy pont aminek a rendje $m \geq 2$. Ekkor

1. *Ha m nem p-nek a hatványa, akkor $x(P), y(P) \in R$.*
2. *He $m = p^n$, akkor*

$$\pi^{2r}x(P), \pi^{3r}y(P) \in R \text{ ahol } r = \left[\frac{v(p)}{p^n - pn - 1}\right]$$

Mivel egy K feletti elliptikus görbét tekinthetünk egy K_v felett definiált elliptikus görbének, ahol K_v K telítése valamilyen $v \in M_K^0$-re (M_K^0 a K-beli nemarkhimédészi értékelések halmaza). Ezért az előző tételt lokális testekre összefonhatjuk a következő tétellé.

3.2. Tétel. *Legyen K egy számtest, R az egészek gyűrűje és E/K egy elliptikus görbe amit az alábbi Weierstrass-egyenlet határoz meg:*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

ahol minden $a_i \in R$. Legyen $P \in E(K)$ egy pont aminek a rendje $m \geq 2$. Ekkor

1. *Ha m nem prím hatvány, akkor $x(P), y(P) \in R$.*
2. *He $m = p^n$ prím hatvány, akkor legyen minden $v \in M_K^0$-re*

$$r_v = \left[\frac{v(p)}{p^n - pn - 1}\right]$$

Ekkor

$$ord_v(x(P)) \geq -2r_v \text{ és } ord_v(y(P)) \geq -3r_v, \text{ ahol } ord_v \text{ a } v \text{ normált értékelés(azaz } ord_v(v) = 1).$$

Vagyis ha $ord_v(p) = 0$, akkor $x(P)$ és $y(P)$ is v-egész.

3.3. Következmény (Nagell-Lutz-tétel)**.** *Legyen $E/\mathbb{Q}$ egy elliptikus görbe, amit az alábbi Weierstrass-egyenlet határoz meg*

$$y^2 = x^3 + Ax + B, A, B \in \mathbb{Z}.$$

Tegyük fel hogy $P \in E(\mathbb{Q})$ egy nem nulla torzió pont. Ekkor:

1. $x(P), y(P) \in \mathbb{Z}$.
2. *És $[2]P = 0$ vagy $y(P)^2$ osztja $4A^2 + 27B^2$-et.*

Hivatkozások

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