椭圆曲线

回顾 射影空间 K 域 $\mathbb{F}_p, \mathbb{F}_q, \mathbb{Q}, \mathbb{Q}_p, \mathbb{R}, \mathbb{C}$

n 维仿射空间 $\mathbb{A}^n$ $\quad \mathbb{A}^n(K)=K^n \quad 0=(0,0,\dots,0)$

n 一 射影 一 $\mathbb{P}^n$ $\quad \mathbb{P}^n(K)=(K^{n+1}\setminus 0)/\sim$

$(x_0,x_1,\dots,x_n)\sim(y_0,y_1,\dots,y_n)$

若 $\exists\lambda\in K^*$ $(y_0,\dots,y_n)=\lambda(x_0,\dots,x_n)$

$\to$ 记 $(x_0:x_1:\dots:x_n)$ 齐次坐标

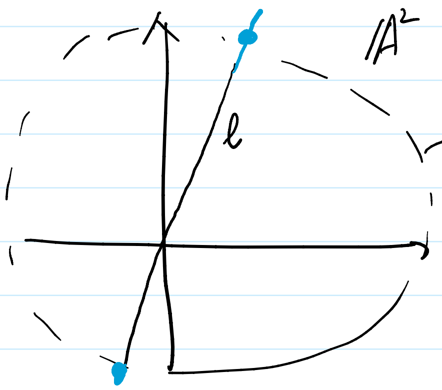
若 $x_0\neq0$ $\quad (x_0:x_1:\dots:x_n)=(\underset{\sim}{1}:\underbrace{x_1':\dots:x_n'})$ $\quad x_i'=x_i/x_0$

$\cong \mathbb{A}^n \quad (x_1',\dots,x_n')$

若 $x_0=0$ $\quad (x_0:x_1:\dots:x_n)=(0:\underbrace{x_1:\dots:x_n}_{\mathbb{P}^{n-1}})$

$$\mathbb{P}^n(K)=\underset{x_0\neq0}{A}\sqcup\underset{x_0=0}{B}=\underbrace{\mathbb{A}^n}_{有限部分}\sqcup\underbrace{\mathbb{P}^{n-1}}_{\to 无穷远点}$$

例 $n=2$ $\quad \underset{(x:y:z)}{\mathbb{P}^2}=\underbrace{\mathbb{A}^2}_{z\neq0}\sqcup\underbrace{\mathbb{P}^1}_{z=0}$



沿 l 方向的 ∞ 远处对应 $\mathbb{P}^1_{(x:y)}$ 中的点

$\to$ 无穷远直线 $\mathbb{P}^1$ 恰对应于是 l 的斜率 $\frac{y}{x}$ 的倒数.

l 的斜率 $\in K\sqcup\{\infty\}$

$\mathbb{P}^1(K)=\mathbb{A}^1(K)\sqcup\mathbb{P}^0(K)$

$\mathbb{P}^n$ 中的几何对象. 齐次多项式所定义的零点 = 射影代数集.

Def $\quad F(\lambda X_0,\dots,\lambda X_n)=\lambda^m F(X_0,\dots,X_n)$ $\quad$ m次齐次

$F(X_0,\dots,X_n)=0 \Leftrightarrow F(\lambda X_0,\dots,\lambda X_n) \quad \forall\lambda\in K^*$

$$X(K)=\{(x_0:\cdots:x_n)\in\mathbb{P}^n(K)\mid \forall i\ F_i(x_0,\cdots,x_n)=0\}\subset\mathbb{P}^n(K)$$

$$F_i\in K[X_0,\cdots,X_n]\quad(\mathbb{Z})$$

Rk. $K=\mathbb{Q}$

X 射影簇 $\quad X(\mathbb{Z})=X(\mathbb{Q})$

$\mathbb{Z}_p\quad\mathbb{Q}_p$

$\mathcal{O}_K\quad K$

例 平面射影曲线（d次）$\quad\mathbb{P}^2$ 中由一个方程定义的（d次齐次）

"Def" $C\subset\mathbb{P}^2$ d次射影曲线，光滑

称 $g(C)=\frac{1}{2}(d-1)(d-2)\in\mathbb{Z}$ 为 C 的亏格 (genus)

Rk（$\Rightarrow$ $g(C)\neq 2$，但 亏格2的曲线，但非平面曲线）

例 $d=2$ 二次曲线 $g=0$，圆锥曲线，若光滑

得来：抛物线，椭圆，双曲线。

（二次型的分类）

$F\in K[X,Y,Z]$ 齐次 $\quad$ 定义 $C\subset\mathbb{P}^2\quad F(X,Y,Z)=0$

$\mathbb{A}^2\subset\mathbb{P}^2\qquad C\cap\mathbb{A}^2\subset\mathbb{A}^2$

$(Z\neq 0)$

$Z=1,\quad x=\frac{X}{Z},\ y=\frac{Y}{Z}$

$$F(X,Y,Z)=0$$
$$\Updownarrow$$
$$f(x,y)=F(x,y,1)=0$$

$f(x,y)\in k[x,y]$ 不必齐次。 $\quad$ 仿射曲线

例 $F(X,Y,Z)=3X^3+4Y^3+5Z^3=0\quad C\subset\mathbb{P}^2$

$\mathbb{A}^2\cap C$：$\quad 3\left(\frac{X}{Z}\right)^3+4\left(\frac{Y}{Z}\right)^3+5=0$

$(Z\neq 0)$

$\mathbb{P}^2=\mathbb{A}^2\sqcup\mathbb{P}^1\quad f(x,y)=3x^3+4y^3+5=0\ (\mathbb{A}^2\cap C)$

无穷远处 $C\cap\mathbb{P}^1\quad(Z=0)\qquad 3X^3+4Y^3+0=0$ 3个点 $\subset\mathbb{P}^1$

$\mathbb{P}^2 = \mathbb{A}^2 \sqcup \mathbb{P}^1$

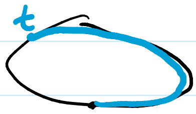
无穷远处 $C \cap \mathbb{P}^1$ $(Z=0)$ $3X^3+4Y^3+0=0$ 齐次 $\subset \mathbb{P}^1$

f 为 F 的去齐次化 $x=\frac{X}{Z}$, $y=\frac{Y}{Z}$.

F 为 f 的齐次化

Def 椭圆曲线 (elliptic curve) 是至少有一个 K-有理点的 3次 (⟺ 亏格 1) 光滑平面射影曲线.

Rk. 椭圆?



$\int_p^t \cdots$ = 椭圆函数.

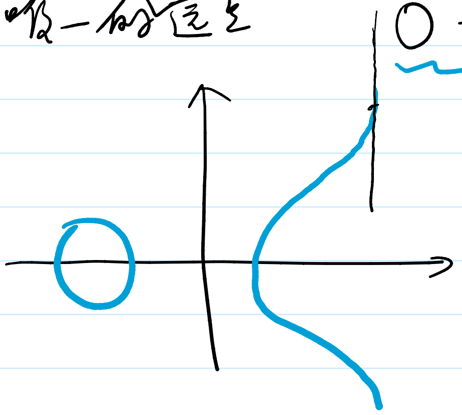
Prop char $K \neq 2,3$ 任一条椭圆曲线 E 都同构于以下形式的椭圆曲线. (Weierstrass 方程)

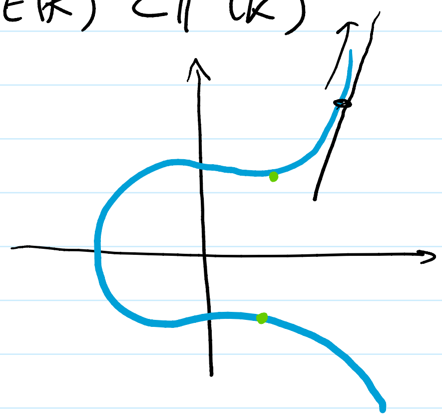
$$F(X,Y,Z)=Y^2Z-(X^3+aXZ^2+bZ^3)=0 \quad \subset \mathbb{P}^2$$

$E\cap\mathbb{A}^2$ $f(x,y)=y^2-(x^3+ax+b)=0$ $\subset\mathbb{A}^2$

$y^2=x^3+ax+b$ Rk 光滑即要求 $\Delta=4a^3+27b^2 \neq 0$

唯一的无穷远点 $O=(0:1:0)\in E(K)\subset\mathbb{P}^2(K)$





Rk. 注: Riemann-Roch 定理

Rk 光滑 ⟺ $\Delta \neq 0$

Def 任一点 $\bar{K}$-点 $P=(x:y:z)\in C(\bar{K})\subseteq\mathbb{P}^2(\bar{K})$ 处有切线

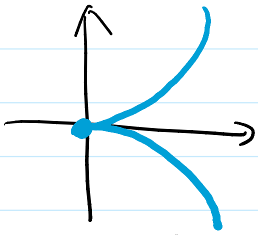
⟺ $\left(\frac{\partial F}{\partial X}(P), \frac{\partial F}{\partial Y}(P), \frac{\partial F}{\partial Z}(P)\right)\neq(0,0,0)$

反例: ① $Y^2=X^3$ $(0:0:1)\in C(\bar{K})$ 不光滑

$(2)\ (\partial x \cdots,\ \partial y \cdots,\ \partial z \cdots)$

直观：① $y^2=x^3$ $\quad(0:0:1)\in C(\bar{K})$ 不光滑

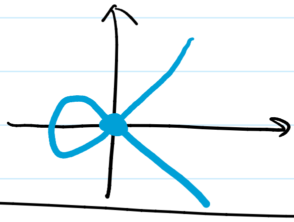
$(Y^2Z=X^3)$



尖点.

② $y^2=x^2(x+1)$ $\quad(0:0:1)$ 不光滑

$Y^2Z=X^2(X+Z)$



结点.

Th (Bézout) $K=\bar{K}$ $\quad\mathbb{P}^2$ $\quad C_1$ m次

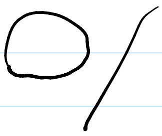
C_2 n次

则 $C_1\cap C_2$ 共有 mn 个交点(计重数)

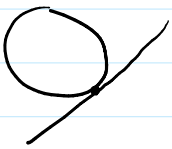
Rk

* 射影

* $K=\bar{K}$ 否则 $K=\mathbb{R}$



* 计重数

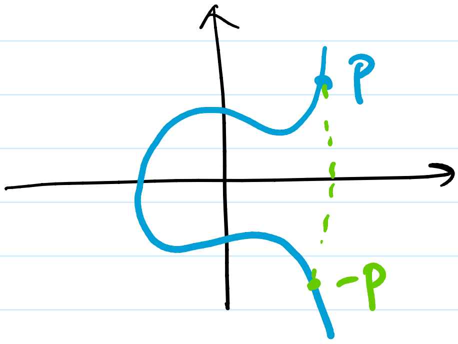


椭圆曲线的Abel群结构

$E(K)$ 是一个Abel群.

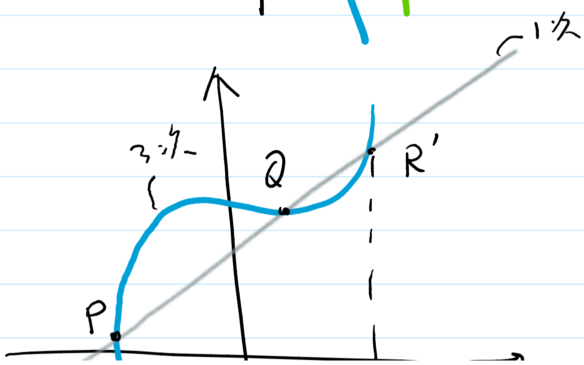
零元：无穷远点 $O=(0:1:0)\in E(K)$

逆元：



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

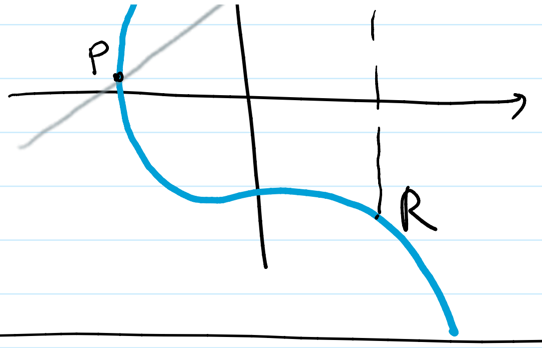
加法：



$Q+P$
$\|$
$P+Q:=R$

$E(K)\times E(K)\to E(K)$

$\ \ \ \ \ \ P\ \ ,\ \ \ \ Q$



难：群的结合律
（Bézout 定理）

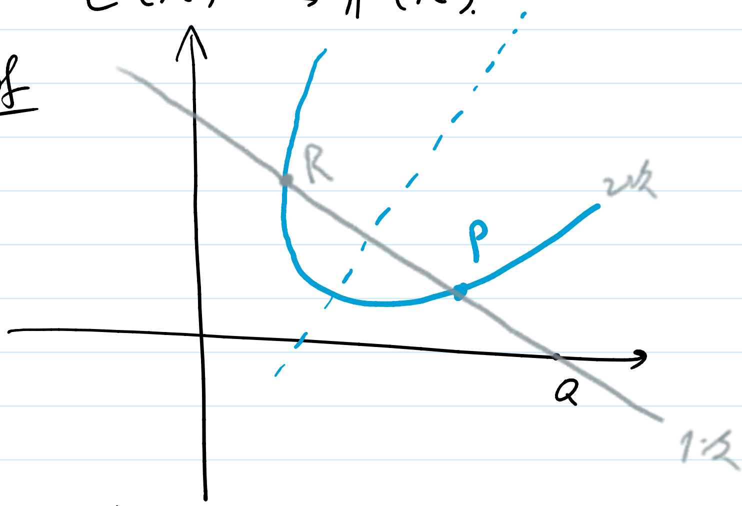
几何决定算术的几个定理：

Th1 C：亏格 0 光滑射影曲线．若 $C(K)\neq\varnothing$，则有自然的双射
$\ni P$

$C(K)\xrightarrow{\sim}\mathbb{P}^1(K)$

$\mathbb{P}^1=\mathbb{A}^1\sqcup\{\infty\}$

Pf



$\varphi:\mathbb{P}^1(K)\xrightarrow{\sim}C(K)$

$Q\longmapsto R$

#

Th2 (Faltings，Mordell 猜想)

C 光滑射影曲线．$g(C)\geq 2$ K 数域 则 $C(K)<+\infty$

Th3 (Mordell-Weil) $C=E$ $g(C)=1$，$C(K)\neq\varnothing$，椭圆曲线．

则 $E(K)$ 是有限生成的 Abel 群

$E(K)\cong F\oplus\mathbb{Z}^r$ F 有限群

$r\in\mathbb{N}$ $r=rk(E)$ E_K 的秩．

$=?$

小结：几何决定算术．

$K=\mathbb{Q}$ $E(\mathbb{Z})=E(\mathbb{Q})$

$E(\mathcal{O}_K)=E(K)$ $\mathbb{G}_m=GL_1$

代数群

$\mathcal{O}_K^\times=\mathbb{G}_m(\mathcal{O}_K)$ Dirichlet 单位定理

有限生成 Abel 群 秩 $r+s-1$

代数中

$$\mathcal{O}_K^\times = \mathrm{Tor}(\mathcal{O}_K) \quad \text{Dirichlet 单位定理}$$

有限生成 Abel 群 rk $r+s-1$

$\mathbb{Z}^\times$

Th3 证明策略：

① 弱 Mordell-Weil $\boxed{E(K)/nE(K)}$ 有限群 → 某上同调中

用 Galois 上同调

② Fermat 递降法

需要

$x^4+y^4=z^4$ 互素 $(x,y,z)\in\mathbb{Z}^3$ 取 $|z|$ 最小的一组解

$\leadsto$ 构造一个新解 (x',y',z') 使 $|z'|<|z|$ 标准

③ "高度" —— 衡量有理点的算术复杂度.

Def A Abel群 $(A=E(K))$

称 $q: A\longrightarrow \mathbb{R}$ $(\mathbb{R}^+)$ 为 A 上的二次型 若 $\forall x,y\in A$

有 $q(x+y)+q(x-y)=2q(x)+2q(y)$

（平行四边形法则 $\|x+y\|^2+\|x-y\|^2=2\|x\|^2+2\|y\|^2$）

Rk 取 $x=y=0 \Rightarrow q(0)=0$

$x=y \Rightarrow q(2x)=4q(x)$

$x=-y \Rightarrow q(-x)=q(x)$

$x=2y \Rightarrow q(3x)=9q(x)$

归纳 $\Rightarrow q(nx)=n^2q(x)$ 二次型

$\forall n\in\mathbb{Z}$

Def 称函数 $f: A\longrightarrow\mathbb{R}$ 有 Northcott 性质 若 $\forall B\in\mathbb{R}$

$\{x\in A \mid f(x)\le B\}$ 有限集.

Rk 若二次型 q 有 Northcott 性质, 则 q 是半正定的 $\forall x\in A$ $q(x)\ge 0$

记号：记 $|x|=\sqrt{q(x)}$ $\left(|x|=0 \Leftarrow x=0\right)$ $\not\Rightarrow$

$x\in\mathfrak{g}$: x $|x|=\sqrt{q(x)}$ $\left(|x|=0 \Leftrightarrow x=0\right)$

Prop (弱 Mordell-Weil $\Rightarrow$ Mordell-Weil)

A : Abel群. 若存在二次型 $q: A\to\mathbb{R}^+$ 有Northcott性质.

则 $A/2A$ 有限 $\Rightarrow$ A 有限生成.

证: 若 S 为 $A/2A$ 的一组代表元. $|S|<+\infty$

$B=\max_{x\in S} q(x)$ $(\overset{\text{可设}}{B}\geq 1)$

则 $S\subset F=\{x\in A\mid q(x)\leq B\}$ 有限集 生成了 A.

Pf: $\forall x\in A$ 若 $\underbrace{q(x)>B}_{|x|>\sqrt{B}}$ 希望把 x 写成 F 中元素的 $\mathbb{Z}$-线性组合.

$x_0:=x$ $\quad x_0=y_1+2x_1$ $\begin{pmatrix} y_1\in S\\ x_1\in A\end{pmatrix}$

同理 $\quad x_1=y_2+2x_2$ $(y_2\in S,\ x_2\in A)$

$x_2=\cdots\cdots$

$(|x|=\sqrt{q(x)})$

$$|x_1|=\frac12|x_0-y_1|\leq\frac12\left(|x_0|+|y_1|\right)\leq\frac12\left(|x_0|+\sqrt{B}\right)<|x_0|$$

同理, 只要 $\underbrace{|x_n|>\sqrt{B}}$ 则 $\underbrace{|x_n|<|x_{n-1}|<\cdots<|x_1|<|x_0|}$

Northcott: 比 $|x_0|$ 小的至多有限个 $\quad\downarrow$ 不会一直下去.

从而 $\exists n$ $|x_n|\leq\sqrt{B}$ $(\Rightarrow x_n\in F)$

此时 $x=x_0$ 是 $y_i\in S\subset F$ 及 $\underset{F}{\overset{\cap}{x_n}}$ 的 $\mathbb{Z}$-线性组合

\#.

Rk 这是以 $|\cdot|=\sqrt{q(\cdot)}$ 为指标的 Fermat 递降法.

如何构造这样的二次型 $q: E(K)\to\mathbb{R}^+$?

baby case : $K=\mathbb{Q}$ $\quad\mathbb{P}^n$ $\quad(E\hookrightarrow\mathbb{P}^2)$

定义 $H_{\mathbb{Q}}: \mathbb{P}^n(\mathbb{Q})\to\mathbb{R}$

$P=(x_0:x_1:\cdots:x_n)$ $\quad x_i\in\mathbb{Z}$ $\quad\gcd(x_0,\cdots,x_n)=1$

设 $P \in \mathbb{P}^n(\mathbb{Q})$

$$\begin{array}{c} \Downarrow \\ P = (x_0 : x_1 : \cdots : x_n) \end{array} \qquad x_i \in \mathbb{Z} \qquad \gcd(x_0, \dots, x_n) = 1$$

$$H_{\mathbb{Q}}(P) := \max(|x_0|, \dots, |x_n|) \qquad h_{\mathbb{Q}}(P) = \log(H_{\mathbb{Q}}(P))$$

<u>高度 height</u>.

Rk $\to$ 利用了 $\mathbb{Z}$: UFD 不易推广到 K

<u>数域:有理:</u>

例 $\mathbb{Q} = \mathbb{A}^1(\mathbb{Q}) \subset \mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \sqcup \{\infty\}$

$$x \longmapsto (x : 1) = P$$

$$H_{\mathbb{Q}}(x) := H_{\mathbb{Q}}(P)$$

$$x = \pi = 3.14159\cdots \approx \frac{22}{7} = \pi_1 \qquad \underset{\substack{\| \\ 22}}{H_{\mathbb{Q}}(\pi_1)} \quad \left(\overset{\pi_1}{\overset{\|}{\tfrac{22}{7}}} : 1\right) = (22 : 7)$$

$$\approx \frac{355}{113} = \pi_2 \qquad H_{\mathbb{Q}}(\pi_2) = 355.$$

Rk.

高度用于描述有理点的算术复杂度.

$$\Omega = \Omega_{\mathbb{Q}} = \{p\} \cup \{\infty\}$$

Prop $P \in \mathbb{P}^n(\mathbb{Q})$ <u>任取</u>齐次坐标 $P = (x_0 : x_1 : \cdots : x_n)$ (不必 $\in \mathbb{Z}$ 不必 $\gcd = 1$)

那么 (*) $$H_{\mathbb{Q}}(P) = \prod_{v \in \Omega} \max(|x_0|_v, \dots, |x_n|_v)$$

(只有 $p \mid x_i$ 分子分母时才会出现非1的项)

Rk 右边不依赖于 $\mathbb{Z}$ 是 UFD $\rightsquigarrow$ 推广到一般 K.

Pf

① 先验证乘积公式: $\forall x \in \mathbb{Q} \quad \prod_{v \in \Omega} |x|_v = 1$

② 由①可知 (*) 右边不依赖于 P 的坐标选取

③ 取 $x_i \in \mathbb{Z}$ $\gcd = 1$ 的 P 坐标, 计算知 (*) ✓ #

Def $H_K : \mathbb{P}^n(K) \longrightarrow \mathbb{R}$ $\qquad K$ 数域

Def $H_K: \mathbb{P}^n(K) \longrightarrow \mathbb{R}$ $\quad K$ 数域

$$P \longmapsto \prod_{v\in\Omega_K} \max(|x_0|_v, \cdots, |x_n|_v)$$

Lem K'/K $\quad \forall P\in \mathbb{P}^n(K)\subset \mathbb{P}^n(K')$

则有 $H_{K'}(P) = H_K(P)^{[K':K]}$ $\quad (\overline{\mathbb{Q}}=\overline{K}=\overline{K'})$

Def $\forall P\in\mathbb{P}^n(\overline{\mathbb{Q}})$ $\quad \exists K/\mathbb{Q}$ 有限扩张，使 $P\in\mathbb{P}^n(K)$

$H(P) := H_K(P)^{\frac{1}{[K:\mathbb{Q}]}}$ $\quad$ Lem $\Rightarrow$ 良定义，与 K 取法无关.

Th (Northcott)

$\{P\in\mathbb{P}^n(\overline{\mathbb{Q}}) \mid [\mathbb{Q}(P):\mathbb{Q}]\le d$ 且 $H(P)\le B\}$ 是有限集合.

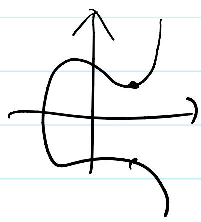
$h = \log\circ H$ 也有此性质.

$E\subset\mathbb{P}^2$

$$\begin{tikzcd} E(\overline{\mathbb{Q}}) \subset \mathbb{P}^2(\overline{\mathbb{Q}}) \arrow[r, "h"] & \mathbb{R} \end{tikzcd}$$

不太实用.
另一方法:

$$\begin{tikzcd} E\setminus O \subset \mathbb{A}^2 \arrow[r] & \mathbb{A}^1 \subset \mathbb{P}^1 \arrow[r, "h"] & \mathbb{R} \\ (x,y) \arrow[r, mapsto, "2:1"'] & x & \end{tikzcd}$$



$\forall P\in(E\setminus O)(\overline{\mathbb{Q}})$

$P=(x(P),\, y(P))$

定义 $h(P)=h(x(P))=\log H(x(P))$

再规定 $h(O)=0$

Th (Weil 高度) $h: E(\overline{\mathbb{Q}})\longrightarrow\mathbb{R}$ 几乎是一个二次型!

$\exists\, c$ 常数 $\quad \forall P\in E(\overline{\mathbb{Q}})$ $\quad -c\le h(2P)-4h(P)\le c$

c_1 $\quad \forall P,Q\in$ $\quad -c_1\le h(P+Q)+h(P-Q)-2h(P)-2h(Q)\le c_1$

Th (Néron–Tate 高度) E/K 椭圆曲线 $\forall P\in E(\overline{K})$

Th (Néron-Tate 高度) E/K 椭圆曲线 $\forall P \in E(\bar{K})$

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

满足平行四边形法则

以及 Northcott 性质. ✓