2020年7月15日 15:37

内容：证明弱 Mordell-Weil 定理：$\forall n \in \mathbb{N}$ $E(K)/nE(K)$ 有限群

方法1

Kummer 序列

$E[n] = E[n](\bar{K})$

$$0 \to E[n] \to E(\bar{K}) \xrightarrow{[n]} E(\bar{K}) \to 0$$

G-module. 短正合列 $G = Gal(\bar{K}/K)$

$$\cdots \to E(K) \xrightarrow{[n]} E(K) \to H^1(K, E[n]) \to H^1(K, E) \xrightarrow{[n]} H^1(K, E) \to \cdots$$

$v \in \Omega$ K_v, $G_v = Gal(\bar{K}_v/K_v)$

$$0 \to E(K)/nE(K) \to H^1(K, E[n]) \to H^1(K, E)[n] \to 0$$

$$0 \to \prod_{v\in\Omega} E(K_v)/nE(K_v) \to \prod_{v\in\Omega} H^1(K_v, E[n]) \to \prod_{v\in\Omega} H^1(K_v, E)[n] \to 0$$

Selmer 群：

$$Sel^{(n)}(E/K) := \{ \gamma \in H^1(K, E[n]) \mid \forall v \in \Omega_K \quad \gamma_v \text{ 在 } E(K_v)/nE(K_v) \text{ 的像之中} \}$$

($\gamma_v \in H^1(K_v, E[n])$)

$$= \{ \gamma \in H^1(K, E[n]) \mid \forall v \in \Omega_K \quad \gamma_v \text{ 在 } H^1(K_v, E) \text{ 中的像为 } 0 \}$$

$$= \ker\left(H^1(K, E[n]) \to \prod_{v\in\Omega} H^1(K_v, E) \right)$$

Lem Abel 群之间的同态 $A \xrightarrow{\alpha} B \xrightarrow{\beta} C$（不必正合，不必是复形）

则有长正合列：

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

把它用到

$$H^1(K, E[n]) \xrightarrow{\alpha} H^1(K, E)[n] \xrightarrow{\beta} \prod_{v\in\Omega} H^1(K_v, E)[n]$$

$$0 \to E(K)/nE(K) \hookrightarrow Sel^{(n)}(E/K) \to Ш(E/K)[n] \to 0$$

要证 $Sel^{(n)}(E/K)$ 有限 $(\Rightarrow |Ш(E/K)[n]| < +\infty)$

↳ 要用到 E 在 K_v（有 $\mathbb{Q}_p$）上的性质

$E(K_v)$ 的部可以分出一些层次. cf. Milne 讲义.

（Silverman GTM 106）

方法2 $E(K)/nE(K) \hookrightarrow H^1(K, E[n])$ (Silverman GTM 1.6)

$\mathrm{Gal}(\bar{K}/K)$ 有限 ↑ 无限

$\bar{K} \subseteq \mathbb{C}$

$E[n](\bar{K}) \subset E[n](\mathbb{C})$ 在 $\mathbb{C}$ 上 $E(\mathbb{C}) \cong \mathbb{C}/\mathbb{Z}\oplus\mathbb{Z} \cong \mathbb{R}/\mathbb{Z} \oplus \mathbb{R}/\mathbb{Z}$

$E[n](\mathbb{C}) \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$

$n=2$

总之有: $H^1(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \mu_2(\bar{\mathbb{Q}})) \cong \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ 含有无穷个元素

$2, 3, 5, 7, 11, \cdots \bmod \mathbb{Q}^{\times 2}$

但在某些特定情况之下 $H^1(K, E[n])$ 有限。

* 如果 $E[n] = E[n](K)$ 的全部点都在 K 中, $\mathrm{Gal}(\bar{K}/K)$ 作用平凡.

$M = E[n]$ 和 G-模 $H^1(G, E[n]) = \mathrm{Hom}_c(G, E[n])$

$\forall \varphi \in \mathrm{Hom}_c(G, E[n])$

分解 $G \xrightarrow{\varphi} E[n]$, $G \to G/N \xrightarrow{\bar{\varphi}}$

$N \trianglelefteq G$ 开正规子群. G/N 有限群

$\bar{\varphi}$: 有限开可能

这里唯一的问题是: N 依赖 φ. 如果对所有的 φ 都一样 N. OK.

Prop 1 L/K 有限 Galois 扩张, 若 $E(L)/nE(L)$ 有限则 $E(K)/nE(K)$ 也有限.

(从而可推出 $E[n](\bar{K}) \subseteq E[n](K)$)

Prop 2 若 $E[n](\bar{K}) \subseteq E(K)$, 则存在有限 Galois 扩张 L/K, 使

$\mathrm{Hom}_c(\mathrm{Gal}(\bar{K}/K), E[n]) = \mathrm{Hom}_c(\mathrm{Gal}(L/K), E[n])$

$\| \qquad\qquad\qquad\qquad \|$

$H^1(K, E[n]) \qquad\qquad H^1(\mathrm{Gal}(L/K), E[n])$

Pf of Prop 1

Pf of Prop 1

$$E(K) \hookrightarrow E(L)$$

$$0 \to Ш \to \frac{E(K)}{nE(K)} \longrightarrow \frac{E(L)}{nE(L)}$$

(左侧有限 ⇐ 右侧有限)

要证 $Ш$ 是有限的

$$Ш = \frac{E(K) \cap nE(L)}{nE(K)} \subseteq \frac{E(K)}{nE(K)}$$

$\forall P \pmod{nE(K)} \in Ш$

可取一个 $Q_P \in E(L)$ 使 $[n]Q_P = P$

(Q_P 不唯一，但至多 n^2 种取法，对每个 P，先取定一个 Q_P)

定义 $\delta_P : Gal(L/K) \longrightarrow E[n]$

$$\sigma \longmapsto \sigma Q_P - Q_P$$

(这是用点)

这像在 $E[n]$ 中：$[n](\sigma Q_P - Q_P) = \sigma([n]Q_P) - [n]Q_P = \sigma P - P \overset{P \in E(K)}{=} P - P = O$

我们又需要证 $Ш \longrightarrow Map(Gal(L/K), E[n])$ 是单射

$$P \longmapsto \delta_P$$

若 $\delta_P = \delta_{P'}$ 即 $\sigma Q_P - Q_P = \sigma Q_{P'} - Q_{P'}$

$$\sigma(Q_P - Q_{P'}) = Q_P - Q_{P'} \quad \forall \sigma \in Gal(L/K)$$

故 $Q_P - Q_{P'} \in E(K)$

$P - P' = [n](Q_P - Q_{P'}) \in nE(K)$ 即 $P = P' \bmod nE(K) \in Ш$ #

为证明 Prop 2，找到结论中的 L，需要承认以下类域论中的结果.

Prop K：数域 给定 $S \subset \Omega_K$ 为有限子集，$S \supset \Omega_K^\infty$，给定 $n \in \mathbb{Z}$，$n \geq 2$.

存在 L/K 满足以下条件的域扩张

① L/K 是 Galois 扩张，而且 $Gal(L/K)$ 是 Abel 群且 $n\,Gal(L/K) = 0$

② L/K 在 S 外非分歧.

那么 L/K 是有限扩张。

③ L/K 在 ... 外非分歧.

那么 L/K 是有限扩张。

（证明利用到类域论中由 L/K 的有限性，归结为代数数论中 K 的理想类群的有限性和 O_K^* 的有限生成性）

Prop 2 $E[n](\bar{K}) \subseteq E(K)$ 那么 $\exists\, L/K$ 有限 使

$$Hom_c(Gal(\bar{K}/K), E[n]) = Hom_c(Gal(L/K), E[n])$$

我们将取 L 为 K 加入以下集合中的全部坐标

$$\Sigma = \{Q \in E(\bar{K}) \mid [n]Q \in E(K)\}$$

简记为 $L = K([n]^{-1}E(K))$

$\forall \sigma \in Gal(\bar{K}/K)$ 若 $Q \in \Sigma$ $[n]Q \in E(K)$

$$[n](\sigma Q) = \sigma([n]Q) = [n]Q \in E(K) \Rightarrow \sigma Q \in \Sigma$$

即 Σ 在 σ 作用下是稳定的，

L 由 Σ 中坐标生成的，在 σ 的作用下也稳定

$\Rightarrow L/K$ 是正规扩张，是 Galois 扩张.

$E[n](\bar{K}) \subset E(K)$ $\quad (0 \to E[n] \to E(\bar{K}) \xrightarrow{[n]} E(\bar{K}) \to 0)$

$$E(K) \xrightarrow{\delta} H^1(Gal(\bar{K}/K), E[n]) = Hom_c(Gal(\bar{K}/K), E[n](\bar{K}))$$ 定义

$\forall P \in E[n] \subset E(\bar{K})$ 取 $Q \in E(\bar{K})$, $[n]Q = P$

定义 $\delta_P : Gal(\bar{K}/K) \to E[n]$

$\sigma \mapsto \sigma Q - Q$

exer 验证 δ_P 不依赖 Q 的选取，且是一个同态

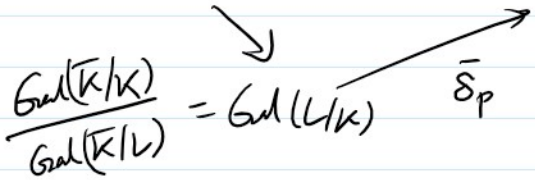
若 $\sigma \in Gal(\bar{K}/L) = N$ 由于 $Q \in \Sigma$, $Q \in E(L)$

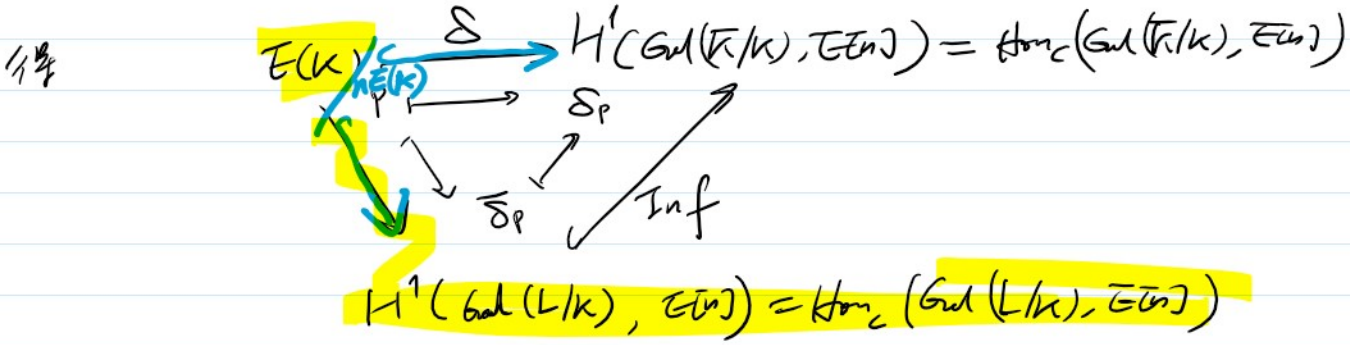
$\sigma Q - Q = 0$ 即 δ_P 在正规子群 $N = Gal(\bar{K}/L)$ 上是平凡的

从而 δ_P 是一个连续映射，定义了 $H^1(Gal(\bar{K}/K), E[n])$ 中一个同调类.

且有交换图 $Gal(\bar{K}/K) \xrightarrow{\delta_P} E[n]$

$Gal(\bar{K}/K) \searrow \quad \nearrow \bar{\delta}_P$





得

$$E(K)/nE(K) \xrightarrow{\delta} H^1(Gal(\bar{K}/K), E[n]) = Hom_c(Gal(\bar{K}/K), E[n])$$

$$H^1(Gal(L/K), E[n]) = Hom_c(Gal(L/K), E[n])$$

$\Rightarrow E(K)/nE(K)$ 有限.

若现在固定 $\sigma \in Gal(\bar{K}/K)$

考虑 $E(K) \to E[n]$

$P \mapsto \sigma Q - Q$.

其中 $Q \in E(\bar{K})$ 使 $[n]Q = P$

exer 这是一个well-defined同态.

从而得到 $Gal(\bar{K}/K) \xrightarrow{\varphi} Hom(E(K), E[n])$

$\sigma \longmapsto$ " $P \mapsto \sigma Q - Q$ "

φ 是群同态: $\tau\sigma Q - Q = \tau(\sigma Q - Q) + \tau Q - Q$ ($\sigma Q - Q \in E[n](\bar{K}) \subset E(K)$)

$= (\sigma Q - Q) + (\tau Q - Q)$

又已经知道 $Gal(\bar{K}/L) = N$ 在 φ 下的像是平凡的

即 $Gal(\bar{K}/L) = N \subset \ker\varphi$

反之, 若 $\sigma Q - Q = 0$ 对 $\forall P \in E(K)$ ($[n]Q = P$) 成立. 即 σ 固定了所有 $Q \in \Sigma$

从而 σ 固定了 L.

即 $\sigma \in Gal(\bar{K}/L)$

即 $Gal(\bar{K}/L) = \ker\varphi$.

于是 $Gal(L/K) = \dfrac{Gal(\bar{K}/K)}{Gal(\bar{K}/L)} \hookrightarrow Hom(E(K), E[n](\bar{K}))$

Abel群 $\Leftarrow$ Abel群

$N \cap Gal(L/K) = 0$

得证 ① ✓

证 ① ✓

为了证②. 我们修取定 S 以及证明 L/K 在 S 外都好约.

取 $S = \Omega_K^\infty \cup \{ v \in \Omega_K^f \mid v(\Delta) \neq 0$ 或 $v(n) \neq 0$. 即 $p \mid n$ 或 $p \mid \Delta \}$

其中 $v(\Delta) \neq 0$. 即 $p \mid \Delta$

E/K $y^2 = x^3 + ax + b$ $a, b \in K$ 总可设 $a, b \in \mathcal{O}_K$ $p \mid \Delta$.

$y^2 - (x^3 + \bar{a}x + \bar{b}) \in \underbrace{\mathcal{O}_K/p}_{\text{记: 有限域 } \mathbb{F}_v}[x, y]$

$\bar{\Delta} = 0 \in \mathbb{F}_v$ 即约化后不光滑 (同样的 $\mathcal{X}_p$ 不光滑)

称为 坏约化 bad reduction, 绝大部分 p 是好约化.

考虑 $v \in \Omega_K \setminus S$, 取 $Q \in E(\bar{K})$ 使 $[n]Q = P \in E(K)$

令 $K' = K(Q)$ 是 Galois 扩张

只要证明 K'/K 在 v 处好约即可.

取 $v' \in \Omega_{K'}$ 在 v 上的延拓, 剩余类域扩张 $\mathbb{F}_{v'}/\mathbb{F}_v$

E 在 v' 和 v 处有好约化.

$\mathrm{Red}_{v'} : E(K'_{v'}) = E(\mathcal{O}_{K'_{v'}}) \longrightarrow \bar{E}_{v'}(\mathbb{F}_{v'})$

* 当 $p \nmid n$ 时 $\mathrm{Red}_{v'}$ 的限制 $E(K'_{v'})[n] \hookrightarrow \bar{E}_{v'}(\mathbb{F}_{v'})$

令 $I_{v'|v} \subset \mathrm{Gal}(K'_{v'}/K_v) \subset \mathrm{Gal}(K'/K)$ 在 v' 处的惯性群子 (inertia group)

$\mathrm{Gal}(K'_{v'}/K_v) = G_{v'|v}$

$\mathrm{Gal}(\mathbb{F}_{v'}/\mathbb{F}_v) = G_{v'|v} / I_{v'|v}$

于是 $\forall \sigma \in I_{v'|v}$

$\overline{E[n](K) \subset E(K)}$

$\overline{\sigma Q - Q} = \sigma\bar{Q} - \bar{Q} = \bar{Q} - \bar{Q} = \bar{O}$ 即 $\sigma Q - Q \in E(K) \cap \ker(\mathrm{Red}_{v'})$

$\overline{\sigma Q - Q} = \sigma\overline{Q} - \overline{Q} = \overline{Q} - \overline{Q} = \overline{O}$ 即 $\overbrace{\sigma Q - Q}^{\cdot} \in E(K) \cap Ker(Red_{v'})$

又 $[n](\sigma Q - Q) = \sigma([n]Q) - [n]Q = \sigma P - P = P - P = 0$

从而 $\sigma Q - Q \in E[n] \cap Ker(Red_{v'}) = \{0\}$

即 $\sigma \in I_{v'/v}$ 平凡作用于 Q 上

—— 平凡作用于 K' 上 $\Rightarrow$ K'/K 在 v 处是非分歧的 #

Rk. 同样方法，若 A 是 Abel 簇，可证明 $A(K)/nA(K)$ 有限。

IV. Fermat 大定理 与 BSD 猜想

$K = \mathbb{Q}$.

1. 椭圆曲线 mod p 约化

$E/\mathbb{Q}$ (广义) Weierstrass 方程

$$a_i \in K = \mathbb{Q}.$$

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

唯一保持方程保持相同形式的(仿射)坐标变换是

$$\begin{cases} x = u^2 x' + r \\ y = u^3 y' + u^2 s x' + t \end{cases}$$

$u, r, s, t \in \mathbb{Q}$ (若还要 $O \mapsto O'$ 则 $r = s = t = 0$)

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

$$\Delta = -16\,\Delta(A,B) = -16\,(4A^3 + 27B^2) \qquad \Delta \neq 0 \Leftrightarrow E_{\mathbb{Q}} \text{ 光滑}.$$

$$\Delta' = u^{-12} \Delta$$

取适当 $A, B \in \mathbb{Z}$ 使 Δ 中不含整数的 12 次方.

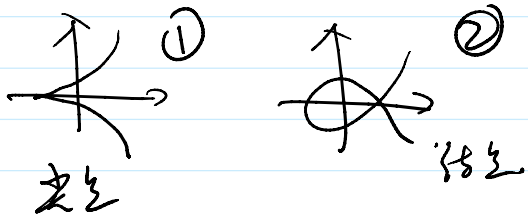
此时 Δ 绝对值是整数且达最小，记 Δ_E

此时称作 Weierstrass 极小方程

mod p 约化. 若 $p \nmid \Delta_E$ $\overline{\Delta_E} \in \mathbb{F}_p^*$ 从而 E_p 仍是光滑的.
是椭圆曲线.

是椭圆曲线.

当 $p \mid \Delta_E$. $\overline{\Delta}_E = 0 \in \mathbb{F}_p$. E_p 有奇异点, 事实上只有一个奇异点.
在 $\mathbb{F}_p$ 上



去掉此点, 剩下 E_p^{ns} (ns = non-singular)

光滑3次曲线: Bezout: 一切割法 $E_p^{ns}(\mathbb{F}_p)$ 仍是 Abel 群
$E_p^{ns}(\overline{\mathbb{F}}_p)$

在①中: $E_p^{ns}(\mathbb{F}_p) \cong G_a(\mathbb{F}_p) = \mathbb{F}_p$ 称 加性约化.

②: $E_p^{ns}(\overline{\mathbb{F}}_p) \cong GL_1(\mathbb{F}_p) = G_m(\overline{\mathbb{F}}_p) = \overline{\mathbb{F}}_p^*$ 乘性约化

} 正则约化

semi-stable 约化 (半稳定) $\begin{cases} \text{乘性} \\ \text{加性} \end{cases}$

Def 定义 $E/\mathbb{Q}$ 的 conductor 为 $N_E = \prod_p p^{n(E,p)}$ 其中

$$n(E,p) = \begin{cases} 0, & E \text{ 在 } p \text{ 处好约化} \\ 1, & \text{乘性} \\ 2+\delta_{E,p}, & \text{加性} \end{cases}$$

$$\delta_{E,p} = \begin{cases} 0, & p \neq 2,3 \\ \leq 8, & p=2 \\ \leq 5, & p=3 \end{cases}$$

当 E 在 p 处有好约化时, 记"误差":

$$a_p = p+1-|E_p(\mathbb{F}_p)| = |\mathbb{P}^1(\mathbb{F}_p)| - |E_p(\mathbb{F}_p)|$$

Th (Hasse-Weil) 当 $E_{/\mathbb{F}_q}$ ($q=p^r$) 为椭圆曲线时 (亏格 $g=1$)

Th (Hasse-Weil) 若 $E/\mathbb{F}_q$ 为椭圆曲线 (亏格 $g=1$)

$$\Big|\, 1+q - |E(\mathbb{F}_q)| \,\Big| \le 2\sqrt{q}\cdot g$$

(即 $|a_p| \le 2\sqrt{p}$.)

星期三 ⟶ 很可能晚上.