椭圆曲线的理论

——以 Mordell 定理为例

周潇翔

University of Science and Technology of China

2019 年 10 月 28 日

摘要

在这份报告中, 我们给出

- 对象: 椭圆曲线;
- 定理:Mordell 定理;
- 介绍:BSD 猜想.

由于是简要的报告, 本人不会具体地深入定理的证明细节, 如有需要请参考附件.

这份报告只花了 3-4 小时的准备, 必有诸多谬误与不当之处, 还请谅解.

目录

目录

理想类群与单位群

定理

设 K 为数域, 对代数整数环 $\mathcal{O}_K$, 其理想类群 $Cl(K)$ 为有限群, 且单位群 $\mathcal{O}_K^\times$ 为有限生成群.

用正合列表示其中的关系.

$$0 \longrightarrow \mathcal{O}_K^\times \longrightarrow K^\times \xrightarrow{v} \bigoplus_{\mathfrak{p}\in M_K^0} \mathbb{Z} \longrightarrow Cl(K) \longrightarrow 0$$

赋值理论

设 L/K 为数域的扩张, 则自然有对应环素谱之间的满射:$\pi : \mathrm{Spec}\,\mathcal{O}_L \longrightarrow \mathrm{Spec}\,\mathcal{O}_K$. 设 $\mathfrak{p} \in \mathrm{Spec}\,\mathcal{O}_K \setminus \{(0)\}$, 则我们对 $\mathcal{O}_L$ 的素理想 $\mathfrak{p}\mathcal{O}_L$ 有唯一的**素理想分解**:

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_g^{e_g} \quad \text{where } \mathfrak{q}_i \in \pi^{-1}(\mathfrak{p})$$

其中

- e_i 称为 $\mathfrak{q}_i$ 的**分歧指数**;
- $f_i := [\mathcal{O}_L/\mathfrak{q}_i : \mathcal{O}_K/\mathfrak{p}]$ 称为 $\mathfrak{q}_i$ 的**剩余类域次数**;
- g 称为域扩张 L/K 的**分裂次数**;

另外我们还有分解群与 Inertia 子群来刻画域扩张的分歧性质.

类数公式

设 K 为数域, 记 $r := \mathrm{rank}(\mathcal{O}_K^\times) = r_1 + r_2 - 1$, 其中 r_1, r_2 分别为 K 的实嵌入个数与复嵌入对数, 则 **Dedekind ζ-函数**

$$\zeta_K(s) := \sum_{0 \neq \mathfrak{a} \lhd \mathcal{O}_K} \frac{1}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p} \in \mathrm{MaxSpec}\,\mathcal{O}_K} \frac{1}{1 - N(\mathfrak{p})^{-s}} \qquad \text{当} Re(s) > 1$$

可亚纯延拓至全空间, 在 $s = 0$ 处的零点阶数为 r, 且有

$$\zeta_K(s) = -h_K \frac{R_K}{w_K} s^r + O(s^{r+1})$$

其中

- $h_K := \#Cl(K)$ 为 K 的**类数**;
- $w_K := \#(\mathcal{O}_K^\times)_{\mathrm{tor}}$ 为 K 的单位根数目;
- R_K 为 $\mathcal{O}_K/(\mathcal{O}_K^\times)_{\mathrm{tor}}$ 作为格点时对应的体积.

目录

对象: 椭圆曲线

Definition

设 K 为域, 则 K 上的椭圆曲线 $E(K)$ 是一个指定原点、亏格为 1、几何不可约的 1 维光滑 K-射影簇.

Definition (Naive)

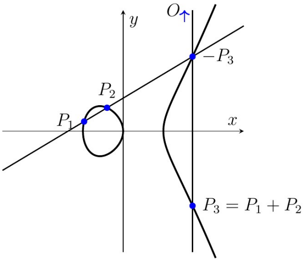
设 K 为域, 假设 $\operatorname{char} K \neq 2, 3$. 则 K 上的椭圆曲线 $E(K)$ 是方程

$$y^2 = 4x^3 + g_2 x + g_3 \qquad g_2, g_3 \in K$$

在 $K\mathbb{P}^2$ 中的解空间.

椭圆曲线上的结构

- 概型结构;
- 群结构: 如右图所示
- 实椭圆曲线: 流形结构;
- 复椭圆曲线: 黎曼面结构 (= 复环面 = 亏格为 1 的黎曼面).



$$y^2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$$

目录

陈述

定理 (Mordell 定理)

设 K 为数域, 则椭圆曲线 $E(K)$

$$E/K : y^2 = 4x^3 + g_2x + g_3 \qquad g_2, g_3 \in K$$

关于上述群运算构成有限生成 *Abel* 群.

对 Abel 簇, 同样有相同的结论:

定理 (Mordell-Weil 定理)

设 K 为数域, 则 K 上的 *Abel* 簇为有限生成 *Abel* 群.

证明概述

Mordell 定理

$\uparrow$ descent lemma

高的性质

- $\#\{P \mid H(P) < M\} < +\infty$
- $H(P+Q) \leqslant C_1 H(P)^2$
- $H(P)^4 \leqslant C_2 H(2P)$

弱 Mordell 定理

$$\#E(K)/mE(K) < +\infty$$

$$\uparrow$$

$$[K([m]^{-1}E(K)) : K] < +\infty$$

$$\uparrow$$

$$\#T_S < +\infty$$

$$\uparrow$$

$R_S^\times$ 为有限生成群

弱 Modell 定理

定理 (高的性质)

设 K 为数域, 则 $E(K)/2E(K)$ 为有限群.

通过"x 坐标" 映射

$$E(K) \xrightarrow{\tilde{\varphi}_i} K^\times \xrightarrow{\hat{\pi}} (K^\times/(K^\times)^2)^3 \xrightarrow{\hat{\eta}} (P_K/(P_K)^2)^3$$

得到证明.

- 用到理想类群与单位群的有限性.
- 某些证明中用到了歧化理论.(局部与整体)
- 引出:
  - Galois 上同调;
  - Tamagawa 数 $c_v := \#E(K_v)/E^0(K_v)$;
  - m-Selmer 群 $S^{(m)}(E/K)$ 与 Shafarevich-Tate 群 $\text{Ш}(E/K)$.

高的性质

Definition (Naive height)

设 $P = [x_0, \ldots, x_N] \in \mathbb{P}^N(K)$, 定义 P 相对于 K 的高

$$H_K(P) = \prod_{v \in M_K} \max\{|x_0|_v, \ldots, |x_N|_v\}^{n_v}$$

与椭圆曲线 E/K 上的高 $H_x(P) = H(x(P))$

- 用到多项式的估计与乘积公式 (定义);
- 引出:
  - **Néron-Tate height**: 实线性空间 $E(K) \otimes_{\mathbb{Z}} \mathbb{R}$ 上的一个内积;
  - 无挠部分 $\Lambda := E(K)/E(K)_{\mathrm{tor}}$ 作为 $E(K) \otimes_{\mathbb{Z}} \mathbb{R}$ 上的格点;
  - 环面 $E(K) \otimes_{\mathbb{Z}} \mathbb{R}/\Lambda$ 所对应的体积 $R_{E/K}$. ($r = 0$ 时令 $R_{E/K} = 1$.)

目录

同类数公式类比

- $\mathcal{O}_K^\times \longleftrightarrow E(\mathbb{Q})$: 格点, 对应的环面体积分别为 R_K 与 $R_{E/\mathbb{Q}}$.

$$\mathcal{O}_K^\times = H^0(K, \mathcal{O}_{\bar{K}}^\times) \qquad E(K) = H^0(K, E(\bar{K})).$$

- $Cl(K) \longleftrightarrow \text{Ш}(E/\mathbb{Q})$: 由于

$$Cl(K) := \mathrm{Ker}\left\{H^1(K, \mathcal{O}_{\bar{K}}^\times) \longrightarrow \prod_v H^1(K_v, \mathcal{O}_{\bar{K}_v}^\times)\right\}$$

$$\text{Ш}(E/\mathbb{Q}) := \mathrm{Ker}\left\{H^1(\mathbb{Q}, E(\bar{\mathbb{Q}})) \longrightarrow \prod_v H^1(\mathbb{Q}_v, E(\bar{\mathbb{Q}}_v))\right\}$$

类群 $Cl(K)$ 有限,$\text{Ш}(E/\mathbb{Q})$ 有限?

- $\zeta_K(s) \longleftrightarrow L(E, s)$

L 函数

Definition (Hesse-Weil L 函数)

对素数 p, 考虑 E 模 p 的解的个数 N_p(包含 O), 记 $t_p := p + 1 - N_p$, 定义 *Hesse-Weil* L 函数

$$L(E,s) := \prod_{p|\Delta} \frac{1}{1 - t_p p^{-s}} \prod_{p\nmid\Delta} \frac{1}{1 - t_p p^{-s} + p^{1-2s}}$$

猜想陈述

Conjecture (Birch and Swinnerton-Dyer Conjecture)

对 $\mathbb{Q}$ 上的椭圆曲线 $E : y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$, 我们有

- *Hesse-Weil L* 函数在 1 点处的阶为椭圆曲线的秩 r_E;
- *Sha* 群 $Ш(E/\mathbb{Q})$ 有限;
- $$L(E,s) = \Omega(E) \prod_{p\ prime} c_p(E) \cdot \# Ш(E/\mathbb{Q}) \frac{R_{E//\mathbb{Q}}}{(\# E(\mathbb{Q})_{\mathrm{tor}})^2} (s-1)^r + O((s-1)^{r+1})$$

其中 $\Omega(E) := \int_{E(\mathbb{R})} \frac{dx}{2|y|}$ 为 $E(\mathbb{R})$ 上的 ***Néron* 周期**.

进展

- Coates 与 Wiles(1977): 对带复乘的椭圆曲线证明了了 L-函数零点阶数为 0(无零点) 的情形.
- Benedict Gross 与 Don Zagier 使用 Gross-Zagier 公式描绘了 L-函数零点阶数为 1 的情形, 随后被 Kolyvagin 用来说明

$$\operatorname{ord}_{s=1} L(E,s) = 1 \Longrightarrow r_E = 1$$

  对部分秩为 0 或 1 的椭圆曲线 (带有复乘且导子较小) 证明了 BSD 猜想.
- 张伟与 Christophe Skinner 等人通过对椭圆曲线的 “计数” 证明 “至少有约 $\frac{2}{3}$ 的椭圆曲线满足 BSD 猜想” .

Thank you!