2020年6月17日 13:42

椭圆曲线选讲

Ref: $E/\mathbb{Q}$

① Rational points on elliptic curves Silverman-Tate 本科生教材

② The arithmetic of elliptic curves Silverman GTM 106

③ Advanced topics in the arithmetic of elliptic curves Silverman GTM151

④ Arithmétique Marc Hindry 法语 → 他的个网页 pdf.

⑤ Elliptic curves Milne 讲义 → 他的个主页

0. 综述

Mordell-Weil 定理.

Th (Mordell-Weil) K 数域. E_K 定义在 K 上的椭圆曲线. 那么

$E(K) = \{E$ 在 K 上的有理点$\}$ 构成一个有限生成 Abel 群.

K 数域. 域 $K/\mathbb{Q}$ 有限扩张 —— 代数数论的研究对象

特殊: $K=\mathbb{Q}$

* 什么是椭圆曲线?
* 什么叫有理点?
* 如何定义 $E(K)$ 上的群结构?
* 如何证明 $E(K)$ 有限生成 → 高度函数 —— 描述有理点的算术复杂性.
  → 群的上同调: Galois 上同调

抽象代数:

有限域

Abel 群的结构定理: A: 有限生成 Abel 群

那么 $A \cong \mathbb{Z}^r \oplus F$ finite group.

$E(K) \cong \mathbb{Z}^r \oplus F$. $F = E(K)_{tor}$

r 称作椭圆曲线 E_K 的秩.

r 称作椭圆曲线 E_K 的秩.

难问题 $r = ?$ (代数量)

BSD 猜想(的一部分): r 可以用一个解析的公式来表达.

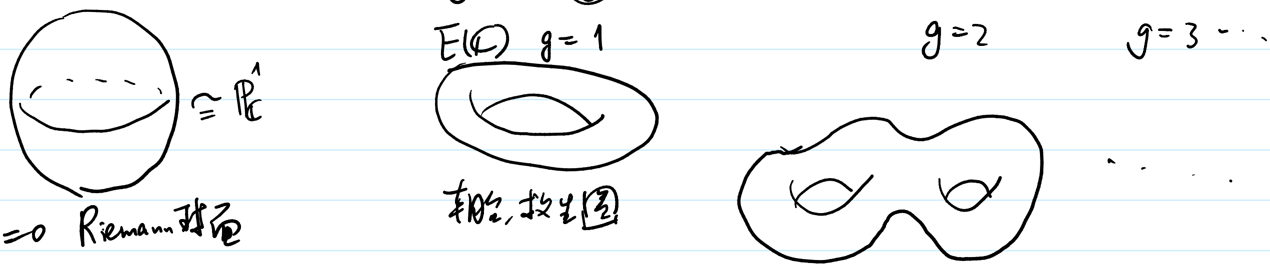
B: Birch, SD: Swinnerton-Dyer

椭圆曲线在现代数学中的位置

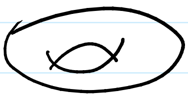
E: 是一个(交换的) Lie 群 (微分流形 + 群)

代数群 (代数簇 + 群)

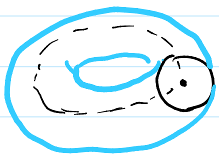
复结构 $E(\mathbb{C})$ ⟶ 1维光滑复流形, 即复曲线, Riemann面 (亏格为1的) genus (g)



亏格 g = 洞的个数(直观)

$E(\mathbb{C})$ =  $= S^1 \times S^1$ 交换群

其他域 K: E(K) Abel群?



亏格 g=0.

线性代数中: 二次型分类 ⟶ 平面二次曲线分类 (conic 圆锥曲线)

抛物线/双曲线/椭圆、+ 若干退化类

亏格0的曲线

⚠ 椭圆 ≠ 椭圆曲线

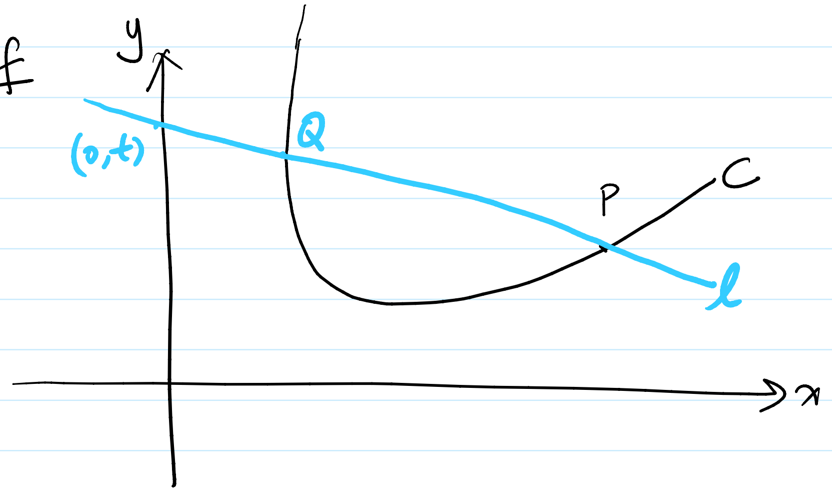
求椭圆周长、椭圆积分. ∈ 椭圆曲线的函数域.

Thm. 定在 K (任何域) 上 光滑二次曲线 C ($C(K) \neq \emptyset$) 一旦有一个 K-点

Th K (代数域) 上 光滑二次曲线 C ($g(C)=0$) 一旦有一个 K-点,

则 它的K点与 K 一一对应 (更准确: 与 $\mathbb{P}^1(K)$ 一一对应)

Pf



已知 $P \in C(K)$

$P(x_0, y_0)$ $x_0, y_0 \in K$

$C: F(x,y)=0$

二次曲线 $\deg F = 2$

定义 $\phi: K \longrightarrow C(K)$

$t \longmapsto Q(x,y)$

ϕ 良好定义? $t \in K$, $P(x_0,y_0)$, $\in K$ $\Big\} \Rightarrow$ l 斜率 $\in K$ $l: y = ax+b$, $\in K$

$l \cap C$, $0 = F(x,y) = F(x, ax+b)$ 关于 x 的二次方程

P是一个解, Q另一个解

韦达定理 $\Rightarrow$ $Q(x,y)$ $x, y \in K$. #

Rk ① "双射" 验证, 映射 ϕ (用韦达写出来之后) 是由多项式/分式函数定义,

这不仅是一个"双射", 还是一个代数几何里的同构.

② 相似的办法 可用于定义 亏格 1 的椭圆曲线上的群结构.

③ 用线性代数/解析 二次曲线分类 了事, 那是在 $\mathbb{R}^3$ 中的分类

$\mathbb{P}^3$ 中只有一类 $\cong \mathbb{P}^1 \subset \mathbb{P}^3$

Th (Faltings 的 Fields 奖工作, Mordell 猜想) K 数域. 曲线 C_K 亏格 ≥ 2

那么 $C(K)$ 有限

Rk. 剩下 亏格 1 的算术性质 由 Mordell-Weil 定理

$E(K)$ — $r=0$ 有限群; $r>0$ 无限群

$r>0$ 无限群

椭圆曲线与代数数论的对比

经典的代数数论，两个重要定理。

K 数域 $K/\mathbb{Q}$ 有限扩张

$\mathcal{O}_K=\{\alpha\in K \mid \alpha$ 的首一相伴多项式 $\in\mathbb{Q}[x]$ 的系数是整数$\}\subset K$

↳ K 的代数整数环

$K=\mathbb{Q}$ $\mathcal{O}_K=\mathbb{Z}$

$K=\mathbb{Q}(i)$, $\mathcal{O}_K=\mathbb{Z}[i]$

$K=\mathbb{Q}(\sqrt{5})$, $\mathcal{O}_K=\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$

} PID

$K=\mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_K=\mathbb{Z}[\sqrt{-5}]$ not PID, not UFD

$(1+\sqrt{-5})(1-\sqrt{-5})=6=2\times 3$

$\mathcal{O}_K$: Dedekind 整环：元素不一定可以一分解，但理想可以唯一分解.

$0\neq I\subset\mathcal{O}_K$ ideal. $I=\mathfrak{p}_1^{\alpha_1}\mathfrak{p}_2^{\alpha_2}\cdots\mathfrak{p}_r^{\alpha_r}$，其中 $\mathfrak{p}_i\subset\mathcal{O}_K$ 素理想，$\alpha_i\in\mathbb{N}$

理这些理想在乘法之下成为一个（交换）幺半群，单位元：$\mathcal{O}_K$

它给出一个交换群 I_K：K 的分式理想群（即允许 $\alpha_i\in\mathbb{Z}$）

它是一个自由 Abel 群，基：$\{\mathfrak{p}\mid \mathfrak{p}\subset\mathcal{O}_K$ 素理想$\}$

$$\varphi: K\longrightarrow I_K,\quad \alpha\longmapsto(\alpha)=(r_1)\cdot(r_2)^{-1}$$

$\alpha=\frac{r_1}{r_2}$, $r_1,r_2\in\mathcal{O}_K$

一般 φ 不是满射（因 $\mathcal{O}_K$ 不是 PID）

为满射等价于？

理想类群 $Cl(K):=\mathrm{Coker}(\varphi)=I_K/I_{\mathrm{Im}(\varphi)}$ 衡量了 $\mathcal{O}_K$ 与 PID 的差距.

另一方面，它也衡量了“局部-整体”的差距：

对 $\mathcal{O}_K$ 素，其完备化 $(\mathcal{O}_K)_p$ 总是一个 PID，但整 $\mathcal{O}_K$ 不是 PID.

$p\in\mathbb{Z}$ $\mathbb{Z}_p$

$0 \neq p \in \mathbb{Z}$ …… $\mathbb{Z}_p$

Th $Cl(K)$ 是一个有限(Abel)群.
$h_K = |Cl(K)|$ 称作类数

Th (Dirichlet 单位定理) $\mathcal{O}_K^\times = \{可逆元\}$ 是一个有限生成 Abel 群
其自由部分的秩 $r = r_1 + r_2 - 1$
其中 r_1 是 $K \hookrightarrow \mathbb{R}$ 不同实嵌入的个数
r_2 是 $K \hookrightarrow \mathbb{C}$ 不同的复嵌入的个数(且相差一个复共轭的看作同一个复嵌入)

$K = \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{R}$ $\quad r_1 = 2$, $r_2 = 0$.
$a + \sqrt{2}b \overset{\iota_1}{\longmapsto} a + \sqrt{2}b$
$a + \sqrt{2}b \overset{\iota_2}{\longmapsto} a - \sqrt{2}b$

$K = \mathbb{Q}(i) \longrightarrow \mathbb{C}$ $\quad r_1 = 0$, $r_2 = 1$
$a + bi \overset{\iota_1}{\longmapsto} a + bi$
$a + bi \overset{\iota_2}{\longmapsto} a - bi$
$\iota_1 = \overline{\iota_2}$

Mordell-Weil 是 Dirichlet 单位定理的一个类比:

GL_n 可逆矩阵群, $\det M \neq 0$ $\quad GL_n \subseteq Mat_{n\times n} \cong K^{n^2}$
自动带流形/代数簇结构,
Lie 群/代数群

$n=1$ $\quad GL_1$ 是交换代数群
Dirichlet $\quad GL_1(\mathbb{Z}) = \mathbb{Z}^\times = \{\pm 1\}$
$GL_1(\mathcal{O}_K) = \mathcal{O}_K^\times$ 有限生成 Abel 群
$r = rk(\mathcal{O}_K^\times)$ 可算.

$GL_1 \rightsquigarrow E$ 交换代数群 射影曲线(整数解=有理解)
Mordell-Weil: $E(\mathcal{O}_K) = E(K)$ 有限生成 Abel 群.
$rk(E/K) = ?$ BSD Conj.

"类群有限"?
衡量椭圆曲线的"局部-整体"差距时:
Tate-Shafarevich 群 $Ш(E/K) = \mathrm{Ker}\left(H^1(K, E) \to \prod_{v \in \Omega} H^1(K_v, E) \right)$ (K: $\mathbb{Q}$; K_v: $\mathbb{Q}_p$, $\mathbb{Q}_\infty = \mathbb{R}$)

Tate-Shafarevich 群 $Ш(E/K) = \mathrm{Ker}\left(H^1(\mathbb{Q}, E) \to \prod_{v\in\Omega} H^1(\mathbb{Q}_p, E)\right)$, $\mathbb{Q}_\infty = \mathbb{R}$

Conj $Ш(E/K)$ 有限

代数数论中 类数: h_K 可由类数公式计算(与数域的 ζ-函数解析性质有紧密联系)

$E \rightsquigarrow |Ш|$ 也与 $L(E/K)$ 的解析性质相关.
BSD·猜想 — 个公式

复习 1. 射影空间 $(\mathbb{A}^n(\mathbb{R}) = \mathbb{R}^n)$ Euclid空间. $\mathbb{A}^n(\mathbb{C}) = \mathbb{C}^n$

K 域 $\mathbb{A}^n$: n维 仿射空间, $\mathbb{A}^n(K) = K^n$

$\mathbb{P}^n$: n维射影空间, 定义为:

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

$(x_0, x_1, \cdots, x_n) \sim (y_0, \cdots, y_n)$ 当 $\exists \lambda \in K^*$ 使 $(y_0, \cdots, y_n) = \lambda(x_0, \cdots, x_n)$

其中的等价类常写成 $(x_0 : x_1 : \cdots : x_n)$ (只关心比例)

若 $x_0 \neq 0$ $(x_0 : x_1 : \cdots : x_n) = (1 : x_1' : \cdots : x_n')$ $x_i' = \frac{x_i}{x_0}$

若 $x_0 \neq 0$ $(x_0 : \cdots : x_n) = (0 : x_1 : \cdots : x_n)$ $x_1, \cdots, x_n$ 不全为0

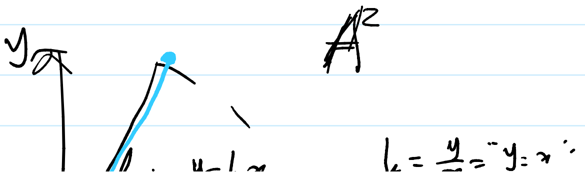
按 $x_0 \neq 0, = 0$ 分类 $\mathbb{P}^n(K) = \underset{x_0\neq 0}{A} \sqcup \underset{x_0 = 0}{B}$

A 与 $\mathbb{A}^n(K)$ 一一对应
B 与 $\mathbb{P}^{n-1}(K)$ 一一对应 $\Rightarrow \mathbb{P}^n = \underbrace{\mathbb{A}^n}_{\text{有限部分}} \sqcup \underbrace{\mathbb{P}^{n-1}}_{\text{无穷远部分}}$

$$\mathbb{P}^n = \mathbb{A}^n \sqcup \mathbb{A}^{n-1} \sqcup \underbrace{\mathbb{A}^{n-2} \sqcup \cdots \sqcup \underbrace{\mathbb{A}^1 \sqcup \mathbb{A}^0}_{\mathbb{P}^1}}_{\mathbb{P}^2}$$

$(x:y:z)$

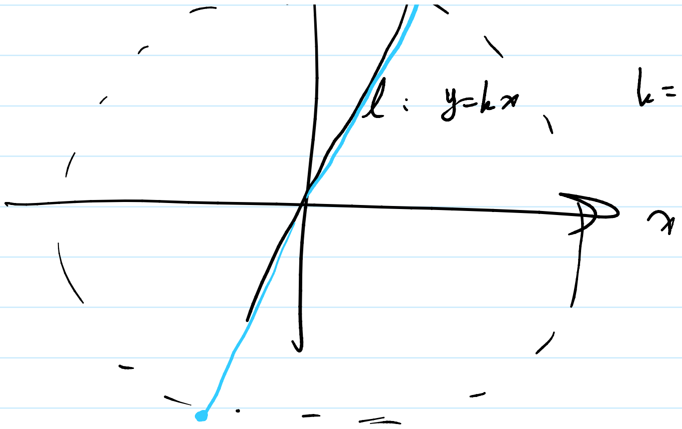
$\mathbb{P}^2 = \mathbb{A}^2 \sqcup \mathbb{P}^1$



$(x:y:\cdot)$

$\mathbb{P}^2 = \underset{(z\neq 0)}{\mathbb{A}^2} \sqcup \underset{(z=0)}{\mathbb{P}^1}$

$(0:1:0) = \ell \cap \mathbb{P}^1$



$k = \frac{y}{x} = "y:x"$

即 $x:y$ 是 ℓ 的斜率的倒数

$k=\infty$ (即 $\ell\perp x$轴) $\ell\cap\mathbb{P}^1$ 对应于 $0\in\mathbb{P}^1$

$k\in K$ $\ell \not\perp x$轴 $\mathbb{P}^1\cap\ell$ 对应于 $(1:k)\in\mathbb{P}^1$

$\mathbb{P}^2=\mathbb{A}^2\sqcup\mathbb{A}^1\sqcup\mathbb{A}^0$　　在n维中 考虑开覆盖.

$\underset{(x:y:z)}{\mathbb{P}^2} = \underset{(x\neq 0)}{\mathbb{A}^2}\cup\underset{(y\neq 0)}{\mathbb{A}^2}\cup\underset{(z\neq 0)}{\mathbb{A}^2}$

考虑 $\mathbb{P}^n$ $(x_0:\cdots:x_n)$ 上的n维对象 (射影) 代数簇 = (齐次) 多项式方程的零点.

$F(x_0,\cdots,x_n)\in K[X_0,X_1,\cdots,X_n]$

$\mathbb{P}^n$ 中的点差一个λ倍 是同一个点, 因此考虑 F 为齐次多项式.

Def 称 F 称作为齐次 n次多项式 若 $F(\lambda X_0,\lambda X_1,\cdots,\lambda X_n)=\lambda^n F(X_0,\cdots,X_n)$

(即 F 是若干 n次单项式之和)

若齐次 则 $F(x_0,\cdots,x_n)=0 \iff F(\lambda x_0,\cdots,\lambda x_n)=0$

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

↳ 有理点的集合.

X: 射影代数簇　　　平面射影曲线: $\mathbb{P}^2$ 一个 F 定义的.

⇓

"整点 = 有理点" (代n: proper 则 $X(\mathcal{O}_K)=X(K)$)

$E(\mathbb{Q})$　$E(\mathbb{C})$　$E(\mathbb{R})$ → Lie group.

$E(\mathbb{Q}) \subset E(\mathbb{C}) \quad E(K))$