2020年7月1日 13:53

K上的椭圆曲线：平面3次光滑射影曲线 且带有一个有理点.

3. Weierstrass 方程

$(X:Y:Z)$. $Y^2Z = X^3 + aXZ^2 + bZ^3$ $a,b \in K$.

$E \subseteq \mathbb{P}^2$ $\Delta = 4a^3 + 27b^2$

$O = (0:1:0) \in \mathbb{P}^2 = \mathbb{A}^2 \sqcup \mathbb{P}^1$ ($Z \neq 0$) ($Z = 0$) 三重点.(光滑点) → Jacobi 判别.

$C \cap \mathbb{P}^1 = \{O\}$ Bézout ↑ $Z=0$ 是 C 于 O 处切线.

$C \cap \mathbb{A}^2$ 去齐次化 $y^2 = x^3 + ax + b$ ($\Delta \neq 0$)

光滑点? Jacobi $\left(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\right) = (-3x^2 - a, 2y) = (0,0)$

$\Leftrightarrow$ $y = 0$ $x = \sqrt{\frac{-a}{3}}$

落在 $C \cap \mathbb{A}^2$ 的方程

从而

$P(x,y)$ 处光滑 $\Leftrightarrow$ $\Delta = 4a^3 + 27b^2 \neq 0$

当 $\Delta \neq 0$ 时 上述方程定义了 $\mathbb{P}^2$ 中一条椭圆曲线.

加法零: $O = (0:1:0) \in E(K)$

Rk. 定义 $j(E) = \frac{1728 \cdot (4a^3)}{\Delta}$ (j 不变量)

E_K 与 E'_K 在 K 上同构 $\Leftrightarrow$ $j(E) = j(E')$

问题 $\forall j \in K$ $\exists E_K$ 椭圆曲线使 $j(E) = j$ $\Delta = 4a^3 + 27b^2$

① $y^2 = x^3 + 1$ ($j = 0$)

② $y^2 = x^3 + x$ ($j = 1728$)

③ $j \neq 0$, $j \neq 1728$, $j \in K$ $y^2 = x^3 - \frac{27}{4} \frac{j}{j-1728} x - \frac{27}{4} \frac{j}{j-1728}$

椭圆曲线往往在以下定义：

① Weierstrass 方程定义的曲线

②

① Weierstrass 给定义的曲线

② 第一个有理生的 3 次平面光滑射影曲线. (我们今主业)

③ 第一个有理生的 3 格为 1 的平面光滑射影曲线 $(g=\frac{(d-1)(d-2)}{2})$

① ⇒ ③ ✓ ③ ⇒ ① ?

如果 $\mathrm{char}K\neq 2,3$. ③ ⇒ ① ✓

若 $\mathrm{char}K=2$ 或 3. 把 ① 换成 ①' 后上述仍是等价的.

①': $E: Y^2Z+a_1XYZ+a_3YZ^2=X^3+a_2X^2Z+a_4XZ^2+a_6Z^3$

$(y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6)$

$E\cap\mathbb{P}^1=\{O\}$ 3重切点. $O=(0:1:0)\in E(K)$

Jacobi 判别法 ⟶ $\Delta=?$

若 $\mathrm{char}K\neq 2,3$ 时 可把 ①' ⟶ ①

变量代换: $\begin{cases} Y'=Y+\frac{a_1X+a_3}{2} \\ X'=X+\frac{4a_2+a_1^2}{12}Z \\ Z'=Z \end{cases}$

目标: 希望证明 ③ ⇒ ①'

⟶ 代数曲线 / Riemann 面 最基本的结果: Riemann-Roch 定理.

↳ 紧致函数的推广 $\mathbb{C}$. $\mathbb{P}^1(\mathbb{C})=\mathbb{C}\sqcup\{\infty\}$

$\mathbb{C}$ 上 $\mathbb{P}^1$

复平面上, 最美妙的"亚纯函数"即有理分式函数 $\frac{P(x)}{Q(x)}=f(x)$

使 $Q(x)=0$ 而 $P(x)\neq 0$ 的 $x\in\mathbb{C}$ 称作 f 的极点.

零点

Riemann 面/代数曲线 上面都有类似的亚纯函数.

$\mathbb{C}$ K

Riemann-Roch 定理回答了"有多少亚纯函数"这个问题.

Def Riemann 面 C 上的全体的集合生成一个自由 Abel 群 (即 $\mathbb{Z}$-系数的有限形式和)

Def Riemann面 C 上的点 作为基 生成一个自由Abel群（即Z-系数的有限形式和）称作 C 的除子群 Div(C)，其元素称作除子 divisor.

即 $P_1, \cdots, P_n$ 为 C 上的点，$D = a_1P_1 + \cdots + a_nP_n$　$a_i \in \mathbb{Z}$
C上除子.

$\deg: \mathrm{Div}(C) \longrightarrow \mathbb{Z}$
$D \longmapsto \deg(D) = \sum_{i=1}^{n} a_i$

（↳ 两者作推广，可定义在一般代数曲线上（即 $K \neq \overline{K}$））

$\mathbb{P}^1(\mathbb{C}) \supseteq \mathbb{A}^1(\mathbb{C}) = \mathbb{C}$
$x_i = P_i \in \mathbb{C}$
$\prod_{i=1}^{n}(x-x_i)^{a_i} = f(x)$
$D = a_1P_1 + \cdots + a_nP_n$ ←

从 C上一个非零的亚纯函数 φ 出发，我们可定义一个除子
$\mathrm{div}(\varphi) = \sum n_P P$　其中 P 为 φ 零点或极点
n_P = P对应的重数 <　+ : P是零点　− : P是极点

Rk　C 是射影曲线 ⟹ $\deg(\mathrm{div}(\varphi)) = 0$（即 极点个数 = 零点个数）

D：除子.

定义　$L(D) = \{0\} \cup \{\varphi$ 为C上非零亚纯函数 而且 $\mathrm{div}(\varphi) + D$ 的所有系数 $\geq 0\}$
是一个K-向量空间.

例　$D = P + 2Q$　　$P, Q \in C(K)$
$\varphi \in L(D) \Leftrightarrow \varphi$ 在除了 P 与 Q 之外无其他极点，而且在P处极点重数至多为 1
在Q - - - 2

$l(D) = \dim_K L(D)$ 描述 满足给定极点条件的亚纯函数的多少.

Th（Riemann-Roch 定理）　C：射影光滑代数曲线，亏格为 g，则
$l(D) - l(\Delta - D) = \deg D + 1 - g.$
其中 D为C上一个除子，Δ 称作C的典范除子 是由 C上的微分形式定义的.
$\deg \Delta = 2g - 2.$

Cor　$l(D) \geq \deg D + 1 - g$，而且当 $\deg D > 2g-2$ 时可取 = 。

Cor $l(D) \geq \deg D + 1 - g$，而且当 $\deg D > 2g-2$ 时可取 $=$。

Pf. $l(\Delta - D) \geq 0$

$\deg D > 2g-2 \Rightarrow \deg(\Delta - D) < 0$

$\deg(\mathrm{div}(\varphi)) = 0$ 从而 $\deg(\underbrace{\mathrm{div}(\varphi) + \Delta - D}_{\text{系数不可能全是 }+}) < 0$

$\Rightarrow L(\Delta - D) = 0$

$l(\Delta - D) = 0$ #

Cor 当 $g=1$ 时，$\deg D \geq 1 \rightarrow l(D) = \deg D$

③ $\Rightarrow$ ①'

$g(E)=1$. E 光滑，且有 $O \in E(K)$

$\forall m \in \mathbb{Z}, m \geq 1$, cor $\Rightarrow \dim L(mO) = m$

而且 $L(O) \subseteq L(2O) \subseteq L(3O) \subseteq \cdots$

$L(O)$ 1维，于是常值函数 1 是 $L(O)$ 的基.

$L(2O)$ 2维，把 1 扩充为 $L(2O)$ 的基 $\{1, x\}$ （x 为 C 上某个亚纯函数）

$L(3O)$ 3维. 一组基为 $\{1, x, y\}$

若 O 不是 x 的极点 或 若 O 是 x 的 1 阶极点 则有 $x \in L(O) = \mathrm{Vect}(1)$ 矛盾.

$\Rightarrow$ O 是 x 的 2 阶极点（因 $x \in L(2O)$）$\Rightarrow$ O 是 x^2 是 4 阶极点

同理 O 是 y 的 3 阶极点.

$\{1, x, y, x^2\} \subseteq L(4O)$ 而且 x^2 不可能是 $1, x, y$ 的线性组合（看 O 处极点）

$\longrightarrow$ 是基

同理 $\{1, x, y, x^2, xy\}$ 必是 $L(5O)$ 的基.

$\{1, x, y, x^2, xy, y^2, x^3\} \subseteq L(6O)$ 7个元素. $\dim L(6O) = 6$ （y^2：6阶）

$\Rightarrow$ 线性相关/K.

$a_0 y^2 + a_1 xy + a_3 y = a_0' x^3 + a_2 x^2 + a_4 x + a_6$ 且 a_0, a_0' 不为 0.

作 $(x, y, z) \rightsquigarrow (\alpha x, \alpha y, \alpha z)$ 可不妨设 $a_0 = a_0' = 1$

$\cdots = x^3 + a_2 x^2 + a_4 x + a_6$

作 $(x,y,z) \rightsquigarrow (\alpha x, \alpha y, \alpha z)$ 可以使得 $a_0 = a_0' = 1$

从而得 $\mathbb{A}^2$ 中 $C: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

$\varphi: E\setminus\{O\} \xrightarrow{\simeq} C$

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

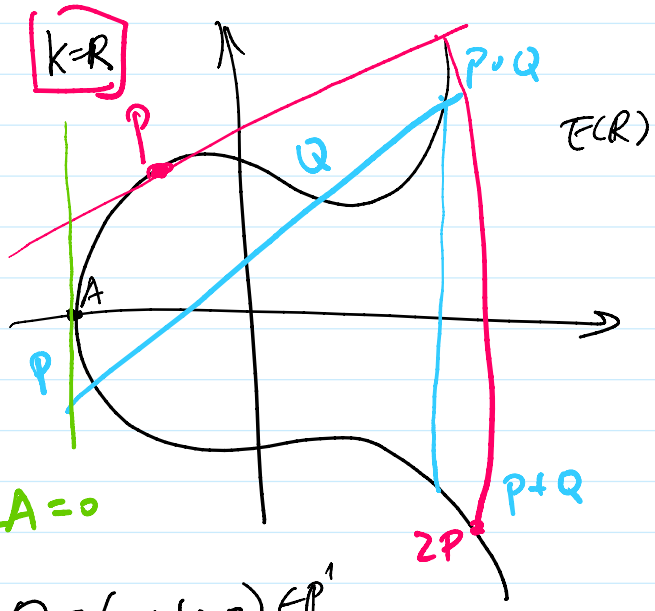
x, y 是两个有理函数仅在 O 处有极点

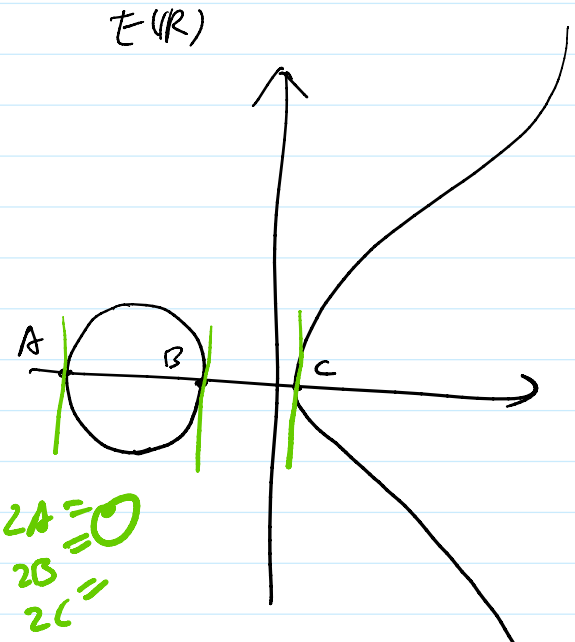
$x(P) \in K$, $y(P) \in K$ 重要的定义.

从而得 ①' 中的 Weierstrass 方程 #.

本课程常见讨论 $\mathrm{char} K \neq 2, 3$.

$E: \quad y^2 = x^3 + ax + b \qquad \Delta = 4a^3 + 27b^2 \neq 0$





$O = (0:1:0) \in \mathbb{P}^1$

$[2]: E \to E$

$\ker: \ker[2] = \{A, O\} \cong \mathbb{Z}/2\mathbb{Z}$

2-torsion 点

$\ker[2] = E[2] = E[2](\bar{K})$

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

$E[2](\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z} = \{A, O\}$

$f(x) = x^3 + ax + b = 0$ 有 1 个/3 个 实根.

$\mathbb{Z}: \quad \ker[2] = \{A, B, C, O\}$

$\cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

~~$\mathbb{Z}/4\mathbb{Z}$~~

$E[2](\mathbb{R}) = \{O, A, B, C\} = (\mathbb{Z}/2\mathbb{Z})^2$.

此时，还可以计算出具体 $P+Q$ 的加法公式.

Prop $\mathrm{char} K \neq 2, 3$, $P_1(x_1, y_1)$, $P_2(x_2, y_2) \in E(K)\setminus\{O\}$

Prop $\mathrm{char}\, K \neq 2,3$，$P_1(x_1,y_1)$，$P_2(x_2,y_2) \in E(K)\setminus\{O\}$

记 $-P_1=(x_1,-y_1)$，则 P_1+P_2 的坐标由以下公式给出

① 若 $P_2=-P_1$（$x_1=x_2$，$y_1=-y_2$）则 $P_1+P_2=O$

② 若 $P_1=P_2$，令 $\lambda=\dfrac{3x_1^2+a}{2y_1}$，$\mu=y_1-\lambda x_1$，则

$$P_1+P_2=P_1+P_2=\left(\lambda^2-x_1-x_2,\ -\lambda^3+\lambda(x_1+x_2)-\mu\right)$$

③ 若 $P_1\neq\pm P_2$（即 $x_1\neq x_2$），令 $\lambda=\dfrac{y_1-y_2}{x_1-x_2}$，$\mu=y_1-\lambda x_1$

P_1+P_2 公式同②.

（提示：计算时利用韦达定理） #

Rk. 运算 $\phi: E\times E \to E$，$(P_1,P_2)\mapsto P_1+P_2$ 在 Zariski 拓扑意义下是连续的.

- 由有理公式定义
- 分母处处非零时连续（例如 $P_1\neq\pm P_2$ 即 $x_1-x_2\neq 0$）
- $P_1=P_2$ 时，且它仍为不在 x 轴上时. （$y_1=\pm y_2\neq 0$）

$$(y_1-y_2)(y_1+y_2)=y_1^2-y_2^2=(x_1^3+ax_1+b)-(x_2^3+ax_2+b)$$
$$=(x_1-x_2)(x_1^2+x_1x_2+x_2^2+a)$$

$$\lambda=\frac{y_1-y_2}{x_1-x_2}=\frac{x_1^2+x_1x_2+x_2^2+a}{y_1+y_2}\neq 0 \quad \checkmark$$

- 当 $P_1=-P_2$（$x_1=x_2$，$y_1=-y_2$ 时）$P_1+P_2=O=(0:1:0)$ 不在 "$z\neq 0$" 这个仿射平面 $\mathbb{A}^2$ 中.

要找到 "$Y\neq 0$" 这个仿射平面，把公式限制在 "$Y\neq 0$" 这个 $\mathbb{A}^2$ 中. $\rightsquigarrow$ ✓

Rk 用 $x(P)$ 来表示 $P(x,y)$ 的 x 坐标，由上述计算知：

$$x(P+Q)+x(P-Q)=\frac{2(x(P)+x(Q))(a+x(P)x(Q))+4b}{(x(P)-x(Q))^2}$$

$$x(P+Q)\cdot x(P-Q)=\frac{(x(P)x(Q)-a)^2-4b(x(P)+x(Q))}{(x(P)-x(Q))^2}$$

$$x(P+Q)\cdot x(P-Q) = \frac{(x(P)x(Q)-a)^2 - 4b(x(P)+x(Q))}{(x(P)-x(Q))^2}$$

$$x(2P) = \frac{x(P)^4 - 2ax(P)^2 - 8bx(P) + a^2}{4(x(P)^3 + ax(P) + b)}$$

II. Mordell-Weil 定理

Th (MW) K: 数域, E/K 椭圆曲线.
$\forall K$ 则 $E(K)$ 是有限生成的 Abel 群.

$\Downarrow$

$(E(K) \cong F \oplus \mathbb{Z}^r)$

Th (弱 MW) K, E 同上. $\forall m \in \mathbb{Z}$ $m > 0$
则 $E(K)/mE(K)$ 是有限群

证明 MW 的策略: 先证明 弱MW. 引入 "高度"函数(用于度量 E 上有理点的算术复杂度). 加上 "Fermat 递降法" $\Rightarrow$ MW.