曲线知识

2024年10月11日　20:46

1. 一些概念

下设 $E/k:\ y^2=f(x)$

1° E/k 表示 E 定义在 k 上 (def. over k). 基本等同于 $f\in k[x]$

2° $E=E(\bar{k})=\{(x,y)\in \bar{k}^2:\ y^2=f(x)\}\cup\{\infty\}$

$E(k)\ =\{(x,y)\in E:\ x,y\in k\}.\cup\{\infty\}$

任取扩域 L/k，$E(L)$ 都是群.

EX. $E/\mathbb{R}:\ y^2=x^3+x$，$\bar{\mathbb{R}}=\mathbb{C}$. $P=(i,0)\notin E(\mathbb{R})$，但 $P\in E$.

3° DEF.(同构)

$\varphi: E_1 \xrightarrow{\sim} E_2$ 是同构，若 φ 是定义良好的有理映射，且 φ 是群同构.

若存在 φ，则 $E_1\cong E_2$.

若 $\varphi=(\varphi_x,\varphi_y)$、$\varphi_x,\varphi_y\in L(x)$. 则 E_1, E_2 是 L-同构的，或在域 L 上同构 (isomorphic over L). $E_1\cong_L E_2$

特别地，若 $E_1\not\cong_k E_2$，但 $E_1\cong_L E_2$，$[L:k]=2$. 则 E_1 是 E_2 的二次扭曲 (quadratic twist). $E_1\cong_2 E_2$.

2. Montgomery 曲线

1° 方程

$E_{A,B}:By^2=x^3+Ax^2+x$.　　$(A\neq\pm 2)$

(非扭曲) $E_A:=E_{A,1}:\ y^2=x^3+Ax^2+x$

2° 二次扭曲

FACT. 设 $E_A/\mathbb{F}_p:\ y^2=x^3+Ax^2+x$.　$p\equiv 3\ (4)$ (意味着 -1 是二次非剩余)

记 $i\in\overline{\mathbb{F}_p}$ 满足 $i^2=-1$. 取 $\mathbb{F}_{p^2}=\mathbb{F}_p(\sqrt{-1})=\mathbb{F}_p(i)$，则

(a) $E_A\cong_{\mathbb{F}_{p^2}}E_{A,-1}$，即 $E_A\cong_2 E_{A,-1}$. 而且 $E_A(\mathbb{F}_p)\to\{(x,iy)\in E_{A,-1}:x,y\in\mathbb{F}_p\}$；$(x,y)\mapsto(x,iy)$ 是群同构.

(b) $E_{-A}\cong_{\mathbb{F}_p}E_{A,-1}$，　$(-x,y)\mapsto(x,y)$　. 也是 $E_{-A}(\mathbb{F}_p)$ 到 $E_{A,-1}$ 间的同构

Pf. (a) $E_{A,-1}:\ -y^2=x^3+Ax^2+x\ \xrightarrow{\sim_2}\ E_A: y^2=x^3+Ax^2+x$.

$(x,iy)\ \mapsto\ (x,y)$

(b) $y^2=(-x)^3-A(-x)^2+(-x)=-(x^3+Ax^2+x)\ \Rightarrow\ -y^2=x^3+Ax^2+x$. 故 $(-x,y)\in E_{-A}\Rightarrow(x,y)\in E_{A,-1}$.

所以. $(-x,y)\mapsto(x,y)$.

3°. 一个 CSIDH 使用的结论.

FACT. CSIDH 使用某些超奇异曲线的 $\mathbb{F}_p$-同构类. 每个同构类中有且仅有一条 Montgomery 曲线 E_A，因此它可以作为代表元.

Proposition 8. *Let $p\geq 5$ be a prime such that $p\equiv 3 \pmod 8$, and let $E/\mathbb{F}_p$ be a supersingular elliptic curve. Then $\mathrm{End}_p(E)=\mathbb{Z}[\pi]$ if and only if there exists $A\in\mathbb{F}_p$ such that E is $\mathbb{F}_p$-isomorphic to the curve $E_A\colon y^2=x^3+Ax^2+x$. Moreover, if such an A exists then it is unique.*

证明中使用了 Riemann-Roch 定理.

要么 { 你不想知道
GTM106 第3章里学过. 就是在Weierstrass方程间的关系的思路.
证 同一曲线的不同

Ref. CSIDH: An Efficient Post-Quantum Commutative Group Action

3. 什么是超奇异 (supersingular)

$E/\mathbb{F}_p$ 超奇异 $:\Leftrightarrow$ $\#E(\mathbb{F}_p)=p+1$.

FACT. 设 $p=4\ell_1\ell_2\cdots\ell_n-1$，$\ell_i$ 是不同的奇素数. E 是超奇异曲线，则 $E(\mathbb{F}_p)$ 是循环群.

Pf. $\#E(\mathbb{F}_p)=p+1\Rightarrow E(\mathbb{F}_p)\cong\mathbb{Z}/4\times\mathbb{Z}/\ell_1\cdots\mathbb{Z}/\ell_n$ 显然循环，生成元 $(1,1,\cdots,1)$. □

同源知识

2024年10月10日 15:06

同源 (isogeny)

以下默认曲线定义在 $\mathbb{F}_p$ 上. $p>3$.

1. 定义

DEF. $E_1 \xrightarrow{\varphi} E_2$ 是同源 :⟺ φ 是满同态且为(非常值的)有理映射. E_2 称为值域曲线 (codomain curve)

FACT. 曲线方程形如 $y^2=f(x)$ 时, 可写为 $\varphi(x,y)=\left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right)$, $u(x), v(x), s(x), t(x) \in \mathbb{F}_p[x]$

EX. ① $[2]: E \to E$, $P \mapsto 2P$ 是同源. 也是自同态 ~~实际上值域曲线是 $E/E[2]$, $E[2]:=\{P\in E: 2P=\infty\}$. 见下~~

↑ E/E[2]其实就是E，注意同源都是满的

② $\pi: E \to E$, $(x,y) \mapsto (x^p, y^p)$ ··········

③ 同构是同源

④ 见后.

2. 同源 ⟷ 子群

FACT. 给定(可分)同源的起点 E, 有如下的一一对应.

$$\{\text{可分同源 } E \xrightarrow{\varphi} E'\} \longleftrightarrow \{G \subseteq E : |G| < \infty\}, \qquad E \xrightarrow{\varphi} E/G \mapsto G.$$

"$E'=E/G$" 表示 E' 作为群同构于 E/G, 这样的 E' 存在且唯一 (在同构的意义下)

Proposition 25. *Let E be an elliptic curve, and let G be a finite subgroup of E. There are a unique elliptic curve E', and a unique separable isogeny ϕ, such that* $\ker\phi = G$ *and* $\phi : E \to E'$.

Ref: [Mathematics of Isogeny Based Cryptography - Luca De Feo]

3. 次数 (degree)

可分同源 φ 的次数 $= |G| = \#\varphi^{-1}(\infty) = \varphi^{-1}(Q)$ $(\forall Q \in E_2)$

EX. 同构次数为 1.

4. 计算同源的方法和复杂度.

求同源指求值域曲线方程和点的像 $\varphi(P)$

通常计算 $E \to E/G$, $G=\langle P \rangle$.

Vélu公式: $O(\#G)$

$\sqrt{\text{é}}$lu算法: $\tilde{O}(\sqrt{\#G})$

5. 同源像点的阶

设 $\varphi: E \to E/\langle P \rangle$, 且 $P \in \langle Q \rangle$, 则 $\operatorname{ord}(\varphi(Q)) = \dfrac{\operatorname{ord}(Q)}{\deg\varphi}$.

推完后会杀掉阶的因子 $\deg\varphi = \operatorname{ord}(P)$

EX. 一个完整的同源例子.

$p=7$, E_0, E_1 定义在 $\mathbb{F}_7$ 上, 皆为超奇异. $P=(0,0) \in E_0$. 有如下同源.

$$\varphi: E_0 \to E_1 = E_0/\langle P \rangle ;\ (x,y) \mapsto \left(\frac{x^2+2x+1}{x}, \frac{-x^2+1}{x^2}y\right). \quad \deg(\varphi) = |\langle P \rangle| = \operatorname{ord}(P) = 2.$$

```
sage: p=7
sage: E = EllipticCurve(GF(p), [0, 0, 0, 1, 0])
sage: E
Elliptic Curve defined by y^2 = x^3 + x over Finite Field of size 7
sage: E.order()
8
```

```
sage: P = E(0,0)
sage: P.order()
2
sage: phi = E.isogeny(kernel=P, model='montgomery')
sage: phi.codomain()
Elliptic Curve defined by y^2 = x^3 + x^2 + x over Finite Field of size 7
sage: phi.degree()
2
sage: phi.rational_maps()
((x^2 + 2*x + 1)/x, (-x^2*y + y)/x^2)
sage: for Q in E.points():
....:     print(f'Q = {Q}, phi(Q) = {phi(Q)}')
....:
Q = (0 : 0 : 1), phi(Q) = (0 : 1 : 0)
Q = (0 : 1 : 0), phi(Q) = (0 : 1 : 0)
Q = (1 : 3 : 1), phi(Q) = (4 : 0 : 1)
Q = (1 : 4 : 1), phi(Q) = (4 : 0 : 1)
Q = (3 : 3 : 1), phi(Q) = (3 : 2 : 1)
Q = (3 : 4 : 1), phi(Q) = (3 : 5 : 1)
Q = (5 : 2 : 1), phi(Q) = (3 : 2 : 1)
Q = (5 : 5 : 1), phi(Q) = (3 : 5 : 1)
```

取 G 为 $\#E(\mathbb{F}_p)$ 生成元，$\mathrm{ord}(G)=8$.

有 $P=4G$，$\mathrm{ord}(\varphi(G)) = \dfrac{\mathrm{ord}(G)}{\deg(\varphi)} = \dfrac{8}{2} = 4$.

$P_2 = 2G \Rightarrow \mathrm{ord}(P_2) = \dfrac{4}{2} = 2$

```
sage: G = E.gens()[0]
sage: G.order()
8
sage: 4*G == P
True
sage: G
(3 : 4 : 1)
sage: phi(G)
(3 : 5 : 1)
sage: phi(G).order()
4
sage: P2 = 2*G
sage: P2.order()
4
sage: phi(P2).order()
2
```

群作用

2024年10月11日 17:24

1. 定义.

定义 1.1 (群作用、G-集合). 设 G 是群, X 是集合.

- G 于 X 上的**左作用** (或**作用**) 指映射

$$* : G \times X \to X,\quad (g, x) \mapsto g * x,$$

满足以下条件:

- 单位元 $1 \in G$ 的作用是恒同映射, 也就是说对任何 $x \in X$,

$$1 * x = x.$$

- 对任何 $g, h \in G$ 和 $x \in X$, 有

$$(gh) * x = g \cdot (h * x).$$

此时, 我们说 G **左作用** (或**作用**) 于 X, 并将此群作用记为

$$G \curvearrowright X,$$

称带有该左作用的集合 X 为 **G-集合**.

Ref: [群作用 - 香蕉空间]

2. 例子

EX1. (置换密码).

$X = \{$"abc", "acb", "cab", ...$\}$ 字符串, $|X| = A_3^3 = 6$

置换群 $G = S_3$. 有一种显然的群作用: 改变字符串中字符排列顺序.

比如 $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} *$ "abc" $=$ "bca"

EX2 (左平移作用)

设 $(G, \cdot)$ 是群. 取 $X = G$. 那么

$$* : G \times X \longrightarrow X :$$
$$(g_1, g_2) \mapsto g_1 \cdot g_2.$$ 或者说定义 $g_1 * g_2 := g_1 \cdot g_2$

是一个群作用.

EX3:

设 $V = \mathbb{R}^3$. 取 $X = \{B = (\beta_1, \beta_2, \beta_3) : \{\beta_1, \beta_2, \beta_3\}$ 为一组基$\}$

$$GL_3(\mathbb{R}) \curvearrowright X : (P, B) \mapsto BP$$

记 $C = BP = (\nu_1, \nu_2, \nu_3)$, 那么 P 是基 B 到基 C 的过渡阵.

必是一组基, $\mathrm{rank}(C) = \mathrm{rank}(B)$.

3. 自由、可迁 / 传递

DEF. 设 $* : G \times X \to X$.

若 $\forall x \in X$, $\forall g \in G$ $g * x = x \Rightarrow g = 1$, 则称群作用 $*$ 自由 (free)

若 $\forall x_1 \in X$ ($\forall x_2 \in X$, $\exists g \in G$ s.t. $g * x_1 = x_2$.), 则称 $*$ 可迁 (transitive).

EX. 上面三个例子中群作用自由且可迁.

$G \curvearrowright X$ 自由且可迁时称为 G-挠子 (G-torsor) 或 G 的主齐性空间 (principal homogenous space).

THM. 对于 G-挠子, 有 $|G| = |X|$.

Pf. 固定 $x_0 \in X$, 有双射 $G \to X : g \mapsto g * x_0$. 可迁 ⇒ 满; 自由 ⇒ 单. □