楕円曲線と代数幾何

JP3BGY

2021/11/21

Table of Contents

1. 自己紹介
2. Motivation
3. 代数多様体の定義
4. 次元
5. 特異点・非特異
6. 種数
7. 発展について
8. 最後に

Table of Contents

1. 自己紹介
2. Motivation
3. 代数多様体の定義
4. 次元
5. 特異点・非特異
6. 種数
7. 発展について
8. 最後に

自己紹介

- 名前：JP3BGY
- 所属：東京大学理学部数学科 4 年
- Crypto を研究したくて数学を頑張っている Pwner

Table of Contents

1. 自己紹介
2. Motivation
3. 代数多様体の定義
4. 次元
5. 特異点・非特異
6. 種数
7. 発展について
8. 最後に

初等的な楕円曲線の定義

定義

標数が 2,3 でない体 k 上の x,y 二次元空間において

$$\Delta := -16(4a^3 + 27b^2) \neq 0$$

を満たす係数 $a, b \in k$ を用いて以下の等式を満たす曲線 $(x, y) \in k^2$ を楕円曲線と呼ぶ。

$$y^2 = x^3 + ax + b$$

事実

楕円曲線上の点に無限遠点を加えたものに対して、直線の交点によって群構造が定まる。詳細は『クラウドを支えるこれからの暗号技術』などを参照

初等的な定義に残る疑問点

- 突然出てきた Δ と多項式はいったい何？
- ほかに楕円曲線と似た性質を持つ曲線はないの？
- 標数 2,3 の体はどこ行った？
- 突然出てきた無限遠点とは？有限体の無限遠...?

⇒代数幾何による抽象的な定義によって解決する！

代数多様体を用いた定義

定義

体 k の 1 次元非特異射影代数多様体で、種数が 1 であるようなものを楕円曲線と呼ぶ。

代数多様体を用いた定義

定義

体 k の 1 次元非特異射影代数多様体で、種数が 1 であるようなものを楕円曲線と呼ぶ。

注意事項

時間の関係でより深い理解に必要な複素解析、代数、位相・解析多様体、代数的トポロジーの話は前提とします。
興味があれば数学科か工学部の該当授業を受けましょう。

また、証明を一切載せてないうえに、かなり端折っています。
参考・関連資料も後ろに載せておきますので詳細はそちらに。

Table of Contents

1. 自己紹介
2. Motivation
3. **代数多様体の定義**
4. 次元
5. 特異点・非特異
6. 種数
7. 発展について
8. 最後に

affine 多様体の定義

定義

体 k の n タプル $\mathbf{A}_k^n := \prod_{i=1}^n k$ の集合に n 変数多項式の集合 (イデアル) の共通零点の集合を閉とする位相を入れる（ザリスキー位相という)。この位相上で閉となる集合を代数的集合といい、代数的集合かつ真部分閉集合二つの和集合とならない（既約位相という）ものを affine 多様体という。

定義

$T \subset A_K^n$ に対して、その集合全体を零点に含む多項式全体を $Z(T)$ と書き (これはイデアルとなる)、T が代数的集合の時 $k[X_i]_{i=1}^n / Z(T)$ をその代数的集合の座標環という。

射影代数多様体の定義

定義

体 k の原点を除いた $n+1$ タプルにスカラー倍による同値類 $\forall \lambda \in k.(a_i)_{i=0}^n \sim (\lambda a_i)_{i=0}^n$ をとった $\mathbf{P}_k^n := \prod_{i=0}^n k - \{(0)\}/\sim$ の集合に $n+1$ 変数斉次多項式の集合の共通零点（0 か 0 でないかは well-def）の集合を閉とする位相を入れ、この位相上で閉となる集合を代数的集合といい、代数的集合かつ既約なものを射影代数多様体という。

定義

$T \subset A_K^n$ に対して、その集合全体を零点に含む斉次多項式全体から生成されるイデアルを $Z(T)$ と書き、T が代数的集合の時 $k[X_i]_{i=0}^n/Z(T)$ をその代数的集合の座標環という。

代数多様体

事実

既約位相上の開部分集合は既約かつ稠密 (閉包が全体になる)

定義

affine/射影多様体の開部分集合をそれぞれ quasi-affine/射影多様体といい、affine/射影/quasi-(affine/射影) 代数多様体を (古典的) 代数多様体と呼ぶ。

定義

代数多様体 X の座標環は整域となり、その商体を関数体といい、$K(X)$ とかく。また、点 P に対して P を零点に持つ多項式 (斉次多項式) 全体から生成されるイデアルは素イデアルとなり、この素イデアルによる局所化 $K(X)_P$ を P の局所環という。

代数多様体間の射

定義

affine 代数多様体 X に対して、その上の正則関数とは写像 $f : X \to k$ で、任意の点 $p \in X$ に対して開近傍 $p \in U$ と多項式 g, h が存在して、h は U 上で零点を持たず $f|_U = g/h$ となるものをいう。射影代数多様体は g, h を次数が等しい斉次多項式として同様に定義する (次数が同じなので写像として well-def である)。

定義

代数多様体 X, Y 間の射とは連続写像 $f : X \to Y$ で、任意の開集合 $U \subset Y$ とその開集合上の正則関数 ϕ に対して $\phi \circ f$ が $f^{-1}(U) \subset X$ 上の正則関数となるものをいう。

代数多様体間の rational map

事実

代数多様体間の射 $\phi, \psi : X \to Y$ がある開集合 $U \subset X$ において一致していたら、$\phi = \psi$ である。

定義

代数多様体 X, Y 間の rational map$\phi : X \to Y$ とは、開集合 U とその上の射 $f : U \to Y$ のタプル (U, f) に対する同値類で、$(U, f) \sim (V, g) := f|_{U \cap V} = g|_{U \cap V}$ となるようなものである。逆写像が存在するものを双有理写像といい、この時定義域 X と値域 Y は双有理同値という。

無限遠点の解決 1

事実

楕円曲線は双有理同値による変形によって 2 次射影代数多様体 $\mathbf{P}_k^2$ 上で以下の形の斉次多項式の零点によりあらわされる。

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

無限遠点と呼ばれていたものは $[X : Y : Z] := [0 : 1 : 0]$ である。
また、この射影代数多様体の部分空間
$U_Z := \{[a : b : c] \in \mathbf{P}_k^2 | c = 1\}$ は相対位相として *affine* 多様体となり、そこでの楕円曲線は次の多項式の零点であらわされる。

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

無限遠点の解決 2

事実

楕円曲線における群構造は、射影代数多様体の直線 $aX + bY + cZ = 0$ との交点を考えることで初等的な場合と同様に定義・証明をすることができる。接線等は代数的微分 $x^n \mapsto nx^{n-1}$ を考える。

楕円曲線の表示

事実

標数が *2,3* でなければ楕円曲線は二次射影代数多様体 $\mathbf{P}^2_k$ 上の以下の多項式で表示される楕円曲線と双有理同値である。

$$y^2z = x^3 + axz^2 + bz^3$$

これは、部分 *affine* 代数多様体 U_Z 上では以下の式であらわされる。

$$y^2 = x^3 + ax + b$$

標数が 2,3 である場合については、それぞれ 2,3 で割ることができない関係上場合分けが発生するが、簡易的な表示が存在しないわけではない。詳細は参考資料にて。

Table of Contents

1. 自己紹介
2. Motivation
3. 代数多様体の定義
4. 次元
5. 特異点・非特異
6. 種数
7. 発展について
8. 最後に

代数多様体の次元

離散位相で濃度が有限な場合とかがあるので位相多様体のような次元の定義は難しい……

定義

代数多様体 X に対して、X の次元を閉部分集合かつ既約となる狭義昇鎖列 $\emptyset \neq Z_0 \subsetneq \cdots \subsetneq Z_n \subset X$ で最長となるような n とする

Table of Contents

1. 自己紹介
2. Motivation
3. 代数多様体の定義
4. 次元
5. **特異点・非特異**
6. 種数
7. 発展について
8. 最後に

特異点・非特異の定義

定義

r 次元の (quasi-)affine 代数多様体 $X \subset \mathbf{A}_k^n$ に対してイデアル $Z(X)$ の生成元を $f_i (i = 1, \cdots, m)$ とする ($k[X_i]$ はネーター環なのでイデアルはすべて有限生成)。この時代数多様体が点 P で非特異であるとは、$\left[\frac{\partial f_j}{\partial x_i}(P)\right]$ のランクが $n - r$ である点のことであり、代数多様体上すべての点が非特異な多様体を非特異代数多様体という。(quasi-) 射影代数多様体上ではある部分 (quasi-)affine 多様体 U_{X_i} 上で点が非特異であれば非特異といい (一つの U_{X_i} で非特異なら点を含むすべての U_{X_i} で非特異であることが言える)、すべての点が非特異なものを非特異代数多様体と呼ぶ。

判別式 Δ の謎の解明

事実

$f(x,y) = y^2 - x^3 - ax - b$ で表示される曲線が非特異となる条件は、$f(x,y) = 0$ となる点において $2y = 3x^2 - a = 0$ となる点が存在しないことであり、これは判別式 Δ が 0 でないことと同値。実は射影代数多様体で考えても非特異になる条件は同じ。

位相多様体との関係

事実

$\mathbb{C}, \mathbb{R}$ 上の非特異な r 次元代数多様体は r 次元位相多様体である
*(*陰函数定理・逆関数定理の位相多様体への一般化である *Constant Rank Theorem* を使って示せる*)*。

Table of Contents

1. 自己紹介
2. Motivation
3. 代数多様体の定義
4. 次元
5. 特異点・非特異
6. **種数**
7. 発展について
8. 最後に

注意

以降は体は代数閉であるとする。代数閉でない体上の代数多様体においては、その体の代数閉包によって同様の定義を行う。また、一次元代数多様体を以降代数曲線と書く。

因子

定義

代数曲線の P 上の局所環 $(O_P, \mathfrak{m})$ の元 f に対して、$\max_{d \in \mathbb{N} \cup \{\infty\}} f \in \mathfrak{m}^d$ を $\mathrm{ord}_P f$ とする関数 $\mathrm{ord}_P : O_P \to \mathbb{N} \cup \{\infty\}$ を定義し、これを $\mathrm{ord}_P f/g = \mathrm{ord}_P f - \mathrm{ord}_P g$ のようにして関数体に一般化する。これを P での位数という。$\mathrm{ord}_P f = 1$ となる f を P の uniformizer という。

定義

代数曲線 X に対して、$\coprod_{x \in X} \mathbb{Z}$ をその因子といい、$\mathrm{Div}(X)$ とかく。因子 $D \in \mathrm{Div}(X)$ に対して x での射影を D_x と書き、$\deg D = \sum_{x \in X} D_x$ とする。また、代数曲線 X とその関数体 $K(X)$ の可逆元 f に対して $\mathrm{div} : K(X)^* \to \mathrm{Div}(X)$ を $\mathrm{div}(f) = \sum_{P \in X} \mathrm{ord}_P(f)(P)$ とする

微分形式

定義

体 K 上の代数曲線 X 上の関数体 $K(X)$ に対して、$f \in K(X)$ に対して df を基底とする $K(X)$ ベクトル空間を
$\{d(f+f') - df - df', d(ff') - fdf' - f'df, da | f, f' \in K(X), a \in K\}$
で生成される部分空間で割ったものを X の微分形式といい、Ω_X とかく。

事実

代数曲線 X 上の微分形式は $K(X)$ の 1 次元ベクトル空間となる。

代数曲線上の因子群 1

定義

一次元代数多様体 X に対して $\mathrm{Im}\, d$ は $\mathrm{Div}(X)$ の部分群 (因子群は可換なので特に正規部分群) となり、この部分群の元を主因子とよび、$\mathrm{Div}(X)/\mathrm{Im}\, d$ をピカール群と呼ぶ。また、ピカール群上で同じ同値類になる因子を線形同値という。

事実

代数閉体上の一次元代数多様体 X において、任意の微分形式 $\omega \in \Omega_X$ と $uniformizert \in K(X)$ に対して $\omega = gdt$ となる $g \in K(C)$ が一意に存在する。さらに $\mathrm{div}(g)$ は t によらずに一意となる。これを $\mathrm{div}(\omega)$ とかく。

代数曲線上の因子群 2

定義

零出ない $\omega_1, \omega_2 \in \Omega_X$ に対して $\mathrm{div}(\omega_1) = \mathrm{div}(f) + \mathrm{div}(\omega_2)$ となる関数体の元 f が存在するため、$\mathrm{div}(\omega_1)$ のピカード群への像は ω_1 の値によらず一意となる。この像の同値類を標準因子類、その元を標準因子という。

事実

因子 D_1, D_2 に対して $D_1 \geq D_2$ であるとは、任意の点での射影においてその不等号が成り立つことである。因子 D に対して $\mathcal{L}(D) := \{f \in K(X)^* : \mathrm{div}(f) \geq -D\} \cup \{0\})$ は K ベクトル空間であり、その次元を $l(D)$ とかく。

種数

定義

代数曲線 X に対してある定数整数 g が存在して、任意の標準因子 K_X と因子 D に対して以下の等式が成り立つ。

$$l(D) - l(K_X - D) = \deg D - g + 1$$

このような g を代数曲線の次数という。

事実

複素数の場合、この種数は閉リーマン面の種数と一致する。

Table of Contents

1. 自己紹介
2. Motivation
3. 代数多様体の定義
4. 次元
5. 特異点・非特異
6. 種数
7. **発展について**
8. 最後に

群構造を持つ物の一般化

楕円曲線のような群構造を持つ代数多様体を考える方向で一般化・抽象化はできないか
⇒アーベル多様体

事実

楕円曲線は 1 次元のアーベル多様体

暗号への応用

定義

楕円曲線間の射が楕円曲線上の群において群準同型となっているとき、その射を同種写像という。

超特異楕円曲線という特殊な楕円曲線間上の特定の同種写像の計算困難性を用いた耐量子計算機暗号の研究が進められており、超特異同種写像ディフィー・ヘルマンなどがその例にあたる。

スキーム論

今までやってきた古典的代数多様体の話のうち

- 多項式環をもっと一般の可換環にできないか
- 射や rational map とかいうやつもう少し見通しが良くならないか

⇒スキーム論
層や圏論を用いてより見通しの良い一般化となり、また代数多様体の現代的な定義はスキーム論によって行われる。

Table of Contents

1. 自己紹介
2. Motivation
3. 代数多様体の定義
4. 次元
5. 特異点・非特異
6. 種数
7. 発展について
8. 最後に

代数幾何をやる意味とは

こんないろんな分野にまたがる上にやたらめったらややこしいものをやる必要あるのか？
⇒代数だけを使って数式をごちゃごちゃやるような天才的で意味が分からず、ほかに応用の利きにくい発想を、位相・圏・層を用いて見通しをよくし、さらに他への応用ができるようにしたものが代数幾何である。
暗号への応用として Rigid Cohomology による楕円曲線の群の位数計算方法の導出などがある。

参考資料

- https://arxiv.org/ftp/arxiv/papers/1103/1103.4560.pdf
  楕円曲線の分類について、標数 2,3 の場合分けについても書かれてる
- https://link.springer.com/book/10.1007/978-0-387-09494-6
- https://link.springer.com/book/10.1007/978-1-4757-3849-0
- https://www.cambridge.org/core/books/commutative-ring-theory/0281983075056 8B06C16E6199F3562C1

その他おすすめの資料

- 雪江代数・整数：群・可換環・体および数論に関して基礎を一通り網羅しており、行間も少ない
- アティマク可換代数：可換環に関して基礎からじっくりやる本、簡単すぎたら前ページの松村先生の本がよいです
- 坪井幾何学 I,II,III：解析多様体や代数的トポロジーについての資料、代数幾何だけをやる場合はそこまで必要はないが、解析多様体と深くかかわるため、余裕があればやっておくのが良い。
- アールフォース複素解析：複素上の代数幾何は複素解析とも関連があるので、余裕があればやっておくとよい。