曲線のヤコビ多様体における群演算の幾何的様相
～曲線でLet's 足し算～

楫研究室 石川 大蔵

概 要

代数曲線のヤコビ多様体の元は, 適当な linearly equivalent を経由して種数以下の点の形式和で表せることが知られている. 2 つの因子の形式的な和を種数以下の点で生成される元として表す際に, 経由する linearly equivalent がどのような有理射によって与えられるかを調べ, かつ具体的に記述した.

1 序

楕円曲線には加法群の構造が定義されることがよく知られている. 例えば, 平面上 $\{y^2 = x^3 - x\} \cup \{\infty\}$ で与えられる楕円曲線 C の 2 点 P, Q の和 $P+Q$ は, P, Q を通る直線 L_1 と C とのもう一つの交点 R の involution $\overline{R}$ によって, $P + Q \sim \overline{R}$ であった. 楕円曲線の場合, 曲線とそのヤコビ多様体は同一視できるので, 楕円曲線の加法群の構造はそのヤコビ多様体での群演算として見なすことができる.

一方で曲線のヤコビ多様体の元は適当な linearly equivalent によって種数以下の点で生成できることが知られている. 上の例では, linearly equivalent を与える rational function ϕ は, L_2 を involution を与える直線, L_i $(i = 1, 2)$ の定義方程式を l_i とすれば, $\phi = l_1/l_2 \in \mathrm{K}(C)$ として与えられる. しかし, 種数が 2 以上のとき, 群演算に現れる ϕ の具体的な形はあまり知られていないように思われる. 本修士論文は, ヤコビ多様体の 2 元の和を linearly equivalent を通じて種数以下の点の和として表す際に, その linearly equivalent を与える rational function ϕ がどのようなものかを考察し, かつ具体的に記述したものである.

2 諸定義

まず始めに, 全体を通じて使う概念を定義する:

Definition 2.1. 非特異な代数曲線 C について,

$$\mathrm{Jac}(C) := \mathrm{Cl}^0(C) = \ker\{\deg : \mathrm{Cl(C)} \longrightarrow \mathbb{Z}\},$$

を C の**ヤコビ多様体**という. ここで,

$$\mathrm{Cl}(C) = \{ \sum_i^{finite} n_i P_i \ ; n_i \in \mathbb{Z},\ P_i \in C\}/\sim ;$$

$$D_1 \sim D_2 \Longleftrightarrow D_1 - D_2 = (f)\ ;\ \text{for } \exists f \in \mathrm{K}(C).$$

特にこの同値類を linearly equivalent という.

Remark 2.2. $\mathrm{Jac}(C)$ の任意の元は, $P_0 \in C$ を固定して,

$$\sum_i^{finite} n_i P_i - (\sum_i^{finite} n_i) P_0\ ;\ n_i \in \mathbb{N},\ \sum_i n_i \leq g,\ P_i \in C$$

と表せる. すなわち, C 上の点 P に対応する $\mathrm{Jac}(C)$ の元 $(P - P_0)$ の高々種数個の和となる.

$\mathrm{Jac}(C)$ の 2 つの元 $D_1,\ D_2$ の和 $D_1 + D_2$ が形式的に種数より大なる個数の点での和となったとき, ある rational function による principal divisor を経由して, 種数以下の個数の点での和に書き直せる. このときの rational function がどのようなものかを考察する. すなわち問題は以下のようになる:

Question 2.3. $D_1,\ D_2 \in \mathrm{Jac}(C)$ について,

$$D_1 + D_2 = \sum_{i=1}^{h} n_i P_i - (\sum n_i) P_0 \ \ s.t.\ h \gneq g(C)$$

とする. 適当な linearly equivalent によって,

$$D_1 + D_2 = \sum_{j=1}^{h'} m_i Q_i - (\sum m_i) P_0 + (\phi) \ \ s.t.\ h' \leq g(C)$$

となるが, このときの $\phi \in K(C)$ はどのようなものか.

3 Hyperelliptic curves

種数 g の hyperelliptic curve C を, $\{y^2 = p(x)\} \cup \{\infty\}$, 但し $p(x)$ は $2g+1$ 次の多項式として与える. 以下の定義を与える:

Definition 3.1. $C \ni P := (a, b)$ の involution を $\overline{P} := (a, -b)$
で定義する. 特に $\overline{\infty} := \infty$.
また, $Jac(C) \ni D$ が reduced form とは, $D := \sum n_i P_i - (\sum n_i)\infty$ という形で書け, 以下のすべての条件を満足するものとする.

(1) $\sum n_i \leq g$,

(2) $P_i \neq P_j, \overline{P_j}, \infty$ if $i \neq j$,

(3) P_i; branch point $\Rightarrow n_i = 1$.

Remark 3.2. (1) $\mathrm{Jac}(C)$ の任意の元に対し, linearly equivalent で reduced form な元が存在する.

(2) ある代数曲線 C' に対し, $C' \cap C = \{P_1, \ldots, P_h\} \Rightarrow P_1 + \cdots + P_h \sim h\infty$

(3) $(P - \infty) \sim (\overline{P} - \infty)$

このとき 2 つの reduced form,

$$D_1 := \sum_i^{h_1} P_i - h_1\infty,\ D_2 := \sum_j^{h_2} Q_j - h_2\infty \in \mathrm{Jac}(C);\ P_i \neq Q_j$$

について, $D_1 + D_2$ の reduced form がどのような principal divisor を経由して得られるかを考える. 上の Remark から, $P_i \neq \overline{Q_j}$ $(1 \leq \forall i \leq h_1,\ 1 \leq \forall j \leq h_2)$ として良い. 実際, $P + \overline{P} \sim 2\infty$ ゆえ, P_i と Q_j に involution の関係があれば, その 2 点を除いた点でも同じ元を生成できるからである.
$D_1 + D_2$ の reduced form を与えるような rational function は, F. Leitenberger によって以下の 2 つの関数を与えることで良いことが示されている：

$$\deg b(x) = (h_1 + h_2 + g - \varepsilon)/2,\ \deg c(x) = (h_1 + h_2 - g - 2 + \varepsilon)/2.$$

但し, $\varepsilon = \begin{cases} 0 & (h_1 + h_2 + g:\ \text{even}) \\ 1 & (h_1 + h_2 + g:\ \text{odd}) \end{cases}$
なる次数の $b(x),\ c(x) \in \mathbb{C}[x]$ において, $P_i,\ Q_j$ が

$$b(x) - y \cdot c(x) = 0$$

を満たすものを考えれば良い. 実際,
$(b(x) - y \cdot c(x)) \cdot (b(x) + y \cdot c(x)) = b^2(x) - y^2 \cdot c^2(x) = 0$ を満たす C 上の点は, $b^2(x) - p(x) \cdot c^2(x) = 0$ を満たす.
$\deg(b^2(x) - p(x) \cdot c^2(x)) \leq h_1 + h_2 + g$ より, 新たに g 個以下の解 x_k を得る. この各 x_k に対し, $b(x_k) - y \cdot c(x_k) = 0$ となるような y_k によって $R_k = (x_k, y_k)$ とおけば,

$$D_1 + D_2 \sim -\sum(R_k - \infty) \sim \sum(\overline{R_k} - \infty)$$

従って linearly equivalent を与える rational function ϕ は, $b(x) - y \cdot c(x)$ と各 R_i における involution を与える直線とで与えられることになるが, 本質的なのは $b(x) - y \cdot c(x)$ であるゆえ, $b(x), c(x)$ を定められれば良い.
Leitenberger は論文の中で, $g = 2$ のときの特に $h_1,\ h_2 = 2$ の場合について上の $b(x), c(x)$ を具体的に与えている. (次数を見ると, $\deg b(x) = 3, \deg c(x) = 0$ ゆえ, 実際には $b(x)$ のみを与えている.) それが次の定理である：

Theorem 3.3 (F. Leitenberger)**.** $D_1 := \sum_{i=1}^{2} n_i P_i - 2\infty,\ D_2 := \sum_{i=3}^{4} n_i P_i - 2\infty$
$P_i := (x_i, y_i)$ とする.

$$x_i \neq x_j \ (\text{if } i \neq j) \Rightarrow b(x) = \sum_{i=1}^{4} y_i \cdot \prod_{j \neq i} \frac{x - x_j}{x_i - x_j}$$

よって

$$\phi = (y - b(x))/(l_1 \cdot l_2)\ ;\ \text{但し } l_i \text{は involution を与える直線の定義方程式}$$

となる.

これに対し, 任意の種数 g かつ $h_1 + h_2 = g + s;\ (1 \leq s \leq g)$ としたまったく一般の場合の $b(x), c(x)$ を与えた次の定理が, 本修士論文の主結果の一つである.
$D_1 + D_2$ が $g+s\ (1 \leq s \leq g)$ 個の点で生成されているとき, $n = [(g+s+1)/2]$ とすると, $\deg b(x) = 2g - n,\ \deg c(x) = n - 1$ である. すると, この n を用いて $b(x), c(x)$ は以下のように表せる:

Theorem 3.4. $D_1 + D_2 := \sum_{i=1}^{g+s} n_i P_i - (g+s)\infty,\ (1 \leq s \leq g)$ とし, 各 $P_i := (x_i, y_i)$ はすべて相異なるもので, branch point の個数は $g + s - n$ 以下とする. このとき,

$$b(x) = \sum_{1 \leq i_1 \lneq i_2 \lneq \cdots \lneq i_n \leq g+s} y_{i_1} \cdots y_{i_n} \cdot \frac{\prod_{k \neq i_1, i_2, \cdots, i_n} (x - x_k)}{\prod_{k \neq i_1, i_2, \cdots, i_n} (x_{i_1} - x_k) \cdots (x_{i_n} - x_k)},$$

$$c(x) = \sum_{i \leq i_1 \lneq i_2 \lneq \cdots \lneq i_{n-1} \leq g+s} y_{i_1} \cdots y_{i_{n-1}} \cdot \frac{\prod_{l=1}^{n-1} (x_{i_l} - x)}{\prod_{k \neq i_1, i_2, \cdots, i_{n-1}} (x_{i_1} - x_k) \cdots (x_{i_{n-1}} - x_k)}.$$

特に,

$$\phi = (b(x) - y \cdot c(x))/(\prod_{i=1}^{g} l_i); \text{但し各 } l_i \text{は involution を与える直線の定義方程式.}$$

proof. $P_j\ (1 \leq \forall j \leq 2g)$ が, $b(x) - y \cdot c(x) = 0$ を満たせば良い. 各項で見ると, $c(x_j)$ は, $j \in \{i_k\}_{k=1}^{l-1}$ の項では 0 になるので,

$$c(x_j) = \sum_{\substack{1 \leq i_1 \lneq i_2 \lneq \cdots \lneq i_{n-1} \leq 2g \\ i_1, i_2, \cdots, i_{n-1} \neq j}} \frac{y_{i_1} y_{i_2} \cdots y_{i_{n-1}}}{\prod_{k \neq j, i_1, i_2, \cdots i_{n-1}} (x_{i_1} - x_k) \cdots (x_{i_{n-1}} - x_k)}$$

一方 $b(x)$ は, $j \notin \{i_k\}_{k=1}^n$ の項では 0 となるゆえ,

$$\begin{aligned} b(x_j) &= \sum_{1\le i_1\lneq i_2\lneq\cdots\lneq i_{n-1}\le 2g} \frac{y_j y_{i_1} y_{i_2}\cdots y_{i_{n-1}}}{\prod_{k\neq j,i_1,i_2,\cdots i_{n-1}} (x_{i_1}-x_k)\cdots(x_{i_{n-1}}-x_k)} \\ &= y_j \cdot c(x_j) \end{aligned}$$

□

Remark 3.5. (1) 種数が 3 以上のとき, $b(\alpha)=c(\alpha)=0$ の場合, $b(x)-y\cdot c(x)=0$ からは y 座標が定まらないが, C 上の点で, $T:=(\alpha,\sqrt{p(\alpha)})$ とすれば, $\overline{T}$ も C 上 $b(x)-y\cdot c(x)=0$ を満たす点なので,

$$D_1+D_2 \sim \sum(R_i-\infty)+(T+\overline{T}-2\infty)=\sum(R_i-\infty)+(l_1/l_\infty)\ ;$$

但し, l_1 は T の involution を与える直線の定義方程式, l_∞ は無限遠直線の定義方程式となる.

(2) branch point が $g+s-n+1$ 点以上あるとき, D_1+D_2 に現れる branch point の和は C のそれ以外の $g-s+n$ 点以下の branch point の和になるので, この linearly equivalent のみで g 点以下の点で生成されている自明な場合である.

4 Space curves

空間曲線に対しても, 同様に群演算を与えるような rational function を考える. 始めに次の値を定める：

$$N_m := \binom{m+3}{3} - 1$$

N_m は m 次曲面がなす族の次元である. これを用いて lemma を与える:

Lemma 4.1. $\mathbb{P}^3 \ni P_i$ $(1\le i\le N_m)$ を general にとる. $\mathbb{C}[x,y,z,w]$ の m 次単項式を $M_1, M_2, \ldots, M_{N_m+1}$ とおく. このとき, $\{P_i\}_{i=1}^{N_m} \subset H_m$ なる m 次曲面 H_m の定義方程式は,

$$F_m(P_1,P_2,\ldots,P_{N_m}) = \sum_{i=1}^{N_m+1} \det(\boldsymbol{v_1}\cdots\overbrace{-\boldsymbol{v_{N_m+1}}}^{i}\cdots\boldsymbol{v_{N_m}})\cdot M_i + \det A\cdot M_{N_m+1}.$$

ここで, $\boldsymbol{v_i} = {}^t(M_i(P_1),\ldots,M_i(P_{N_m}))$; $(1\le\forall i\le N_m)$, $A=(\boldsymbol{v_1}\cdots\boldsymbol{v_{N_m}})$ として, $F_m=0$ で与えられる.

proof. P_j $(1 \leq j \leq N_m)$ に対して,

$$\sum_{i=1}^{N_m+1} \det(\boldsymbol{v_1} \cdots \overbrace{-\boldsymbol{v_{N_m+1}}}^{i} \cdots \boldsymbol{v_{N_m}}) \cdot M_i(P_j) = -\det A \cdot M_{N_m+1}(P_j)$$

を示せば良い. 左辺を $\boldsymbol{v_{N_m+1}}$ において余因子展開する. A の (k,i) 成分における余因子を $\Delta_{k,i}$ とすれば,

$$\sum_{k=1}^{N_m} -M_{N_{m+1}}(P_k) \sum_{i=1}^{N_m} (-1)^{k+i} M_i(P_j) \cdot \Delta_{k,i}$$

ここで, $\sum_{i=1}^{N_m}(-1)^{i+k} M_i(P_j) \cdot \Delta_{k,i}$ は, A の k 行ベクトルを j 行ベクトルに入れ替えたものの行列式だから,

$$\sum_{i=1}^{N_m}(-1)^{i+k} M_i(P_j) \cdot \Delta_{k,i} = \begin{cases} 0 & (\text{if } k \neq j), \\ \det A & (\text{if } k = j). \end{cases}$$

以上より, (左辺)$= -M_k(P_j) \cdot \det A =$(右辺).

□

Remark 4.2. $P_1, \ldots, P_{N_m} \in \mathbb{P}^3$ を general にとると, $P_1, \ldots, P_{N_m} \in H_m$ となるような m 次曲面 H_m はただ一つである.

すると, この F_m を用いれば rational function を具体的に与えることができる. それが次の定理である:

Theorem 4.3. $P_1, \ldots, P_{g+1} \in C$ を general にとる.

$$D_1 + D_2 = \sum_{i=1}^{g+1} P_i - (g+1)P_0 \sim \sum_{i=1}^{g} R_i - gP_0$$

を与える rational function ϕ は, $P_1, \ldots, P_{g+1}$ に対して $\{Q_i\}_{i=1}^{md-(g+1)}$, $\{R_i\}_{i=1}^{g} \subset C$, $\{S_i\}_{i=1}^{N_m-md}$, $\{T_i\}_{i=1}^{N_m-md} \subset \mathbb{P}^3 \setminus C$ が存在して,

$$\phi = \frac{F_m(P_1, \ldots, P_{g+1}, Q_1, \ldots, Q_{md-(g+1)}, S_1, \ldots, S_{N_m-md})}{F_m(Q_1, \ldots, Q_{md-(g+1)}, P_0, R_1, \ldots, R_g, T_1, \ldots, T_{N_m-md})}.$$

proof. $N_m \geq md \geq g+1$ となるように $m \in \mathbb{N}$ とし,

$$H_m = Z(F_m(P_1, \ldots, P_{g+1}, Q_1, \ldots, Q_{md-(g+1)}, S_1, \ldots, S_{N_m-md})),$$

$$H'_m = Z(F_m(Q_1, \ldots, Q_{md-(g+1)}, P_0, R_1, \ldots, R_g, T_1, \ldots, T_{N_m-md}))$$

とおくと, $\{P_i\}_{i=1}^{g+1}, \{Q_i\}_{i=1}^{md-(g+1)} \in H_m$ ゆえ

$$H_m.C = \sum_{i=1}^{g+1} P_i + \sum_{i=1}^{md-(g+1)} Q_i.$$

次に $\{Q_i\}_{i=1}^{md-(g+1)}, \{R_i\}_{i=1}^{g}, \{P_0\} \in H'_m$ ゆえ

$$H'_m.C = \sum_{i=1}^{md-(g+1)} Q_i + P_0 + \sum_{i=1}^{g} R_i.$$

すると, $H_m.C - H'_m.C = (F_m/F'_m)$ なので,

$$D_1 + D_2 = \sum_{i=1}^{g} R_i - gP_0 + (F_m/F'_m)$$

となり, 求める rational function $\phi = F_m/F'_m$ となる. □

Remark 4.4. 上はすべて $\mathbb{P}^3$ 限り記したが, $\mathbb{P}^n$ での曲線においても全く同様の議論により rational function を与えられる.

5 謝辞

何よりもまず, 指導教官の楫 元先生には大変お世話になりました. 結果を得る過程も含め, 先生には多大なお時間を割いていただき, 私の拙い研究にお付き合い頂きました. ありがとうございます.
そして, 楫研の先輩である網谷 泰治氏, 深澤 知氏, 古川 勝久氏からも多岐にわたるアドバイスを適時いただき, 大いに助けていただきました. また, 同期の渡辺 究氏, 齋藤 恆和氏, 生駒 典久氏, 須田 庄氏の研究に対する姿勢に大いに励まされました. 最後に, 一緒にゼミを行ってくれた後輩の伊藤 達哉氏, 権業 善範氏にもこの場を借りてお礼申し上げます.

参考文献

[1] R. Hartshorne, *Algebraic Geometry*, GTM52, Springer, 1977

[2] F. Leitenberger, *About the group law for the Jacobi variety of a hyperelliptic curve*, Beiträge Algebra Geom. 46 (2005), no. 1, 125–130

[3] 佐武一郎, 線型代数学, 裳華房, 1974