

可積分有理写像の歩数は離散対数である

—全等位集合上の軌道の完全な理論とその形式検証—

Yuta Ogura

Independent researcher

第 1 版 — 2026 年 10 月

概要

体 K 上の有限次元空間の有理写像 σ と二つの状態 s, t について、歩数の集合 $\text{Id}(s, t) = \{n \in \mathbb{Z} : \sigma^n s = t\}$ (力学系の作用歪群における s から t への射の集合) を、写像を反復せずに決定する。Lyness 写像、Euler のコマの Kahan–Hirota–Kimura 離散化、面積を保つ線形写像、双曲測地線の Kahan 離散化について、任意の体 (必要な場合は標数 $\neq 2$) 上で、保存量の各等位集合において写像がその等位集合に付随するアーベル群 A の固定された元 P による平行移動として表され、それを実現する単射な座標 ψ が存在することを、Lean 4 と Mathlib を用いて証明する。したがって $\sigma^n s = t$ は $\psi(t) - \psi(s) = nP$ と同値である。よって歩数は離散対数として求まり、 $\text{Id}(s, t)$ は空集合か P の位数を法とする剰余類である。また $\psi(s)$ の $\langle P \rangle$ を法とする類は軌道の完全不変量となる。定理は退化した等位集合 (結節点を持つ曲線、可約な曲線、Euler のコマで座標が消える等位集合) も扱う。さらに次の二つの結果により、この理論は決定手続きとなる。第一に、写像が定義されない状態は各等位の有限個の明示的な状態なので、軌道が零除算に至るかどうかが (状態の正則性) は、正則・非正則のいずれの場合も数個の離散対数で判定でき、正則でない状態の有限な連鎖も同じ対数から読める。第二に、部分有理写像についての還元定理により、正則性と道のないことは素数を法とする還元から $\mathbb{Q}$ に引き戻され、 $\mathbb{Q}$ 上の歩数は還元でも歩数であるので、 $\mathbb{Q}$ 上の問いは上界の範囲で有限個の素数と一回の厳密な反復で決まり、ある素数で道がなければ否定の答え「決して」が無条件に得られる。力学はまた、道の定数 $\text{path} : \Pi x. \text{Id}(x, \text{step } x)$ を持つ Martin-Löf 型理論の小さな理論として公理化され、HoTTLean の歪群モデルで解釈される。そこで s と t の間の恒等型はちょうど集合 $\text{Id}(s, t)$ である。開発は定理 1,146 個からなり、sorry はなく標準の公理だけを使い、健全性を Lean で証明した実行可能な証明書検査器を含む。これは、これらの問いに独立に検査できる証明書つきで答える Structure Computer の数学的基礎である。2 コアの機械で、 $\mathbb{F}_{2^{61}-1}$ 上で 7.9×10^{15} 歩先にある状態の歩数が 0.4 秒で求まる (反復では約 96 年かかる)。

目次

1	序論	2
1.1	問い	2
1.2	平行移動としての可積分写像	3
1.3	貢献	3
2	設定	4
2.1	部分流と正則状態	4
2.2	答えの三つの形	4

2.3	作用歪群	5
3	位相：群上の平行移動流	5
4	Lyness 写像	5
4.1	写像と積分	6
4.2	楕円的な等位	6
4.3	結節点を持つ等位	6
4.4	可約な等位 $k = 0$ と $k = a - 1$	7
5	Euler のコマの Kahan–Hirota–Kimura 離散化	8
5.1	写像と保存量	8
5.2	普遍コマとその等位	8
5.3	楕円的な等位	8
5.4	すべての等位：場合 A、B、Z	9
6	線形流、離散化した振動子、E2	9
7	位相による正則性	10
8	有理数への還元	11
9	型理論的な内容	12
10	形式化	12
10.1	範囲と統計	12
10.2	証明の技法	12
10.3	非空性	13
10.4	健全性を証明した証明書検査器	13
11	関連研究	13
12	範囲と今後	14
A	例題	14

1 序論

1.1 問い

離散力学系とは、状態空間 X と写像 $\sigma : X \rightarrow X$ の組である。二つの状態 s, t について、 s から t にそもそも到達するか、到達するなら何歩でか。 σ が可逆なら完全な答えは集合

$$\text{Id}(s, t) = \{ n \in \mathbb{Z} : \sigma^n s = t \}$$

であり、空か、軌道の周期 $M \geq 0$ の剰余類 $r + M\mathbb{Z}$ である（無限軌道では $M = 0$ ）。記法は型理論のものである。 $\text{Id}(s, t)$ は作用歪群 $X//\mathbb{Z}$ における s から t への射の集合であり、9 節でその対応を正確にする。

$q \approx 2^{61}$ として σ が $\mathbb{F}_q$ 上の有理写像なら、典型的な軌道は約 q 個の状態を持ち、たどれない。「 t には決して着かない」は軌道全体をたどらなければ確かめられない。 $\mathbb{Q}$ 上では軌道は一般に無限で、反復だけでは否定の答えは得られない。必要なのは、所属と歩数が直接読み取れる軌道の記述である。

1.2 平行移動としての可積分写像

可積分写像では、等位曲線上の平行移動の構造がそのような記述を与える。QRT 型の平面写像 [23, 24] は双二次曲線のペンシルを保ち、その滑らかなファイバー（楕円曲線）の上では、群の固定された元による平行移動として作用する [8]。Lyness 写像 $(x, y) \mapsto (y, (a + y)/x)$ はもっとも簡単な例で、等位曲線 $(x + 1)(y + 1)(x + y + a) = kxy$ によって実数上の力学が記述され [3]、Hone [10, 11] は $\mathbb{Z}/N$ 上の平行移動の構造を楕円曲線法による素因数分解に用いた。Euler のコマの Kahan–Hirota–Kimura 離散化 [9, 13] は独立な二つの有理保存量を持つ可積分写像で [4, 19, 20]、その等位曲線も楕円曲線である。等位を、一步が P による平行移動になる群 A と同一視すれば、問い $\text{Id}(s, t)$ は離散対数であり、有限体上では Pohlig–Hellman 法 [21] により群の位数の最大素因数の平方根程度の時間で計算できる。線形写像ではこれが Kannan と Lipton の軌道問題 [6, 14] であり、楕円可除列については、添字の復元が楕円離散対数問題と同値であることを Lauter と Stange [15] が示した。

1.3 貢献

本稿は四つの族について、平行移動の構造をもとに決定手続きを構成し、その正しさを形式的に証明する。

- (i) **すべての等位、すべての体（4–6 節）。** 四つの族についてすべての等位集合で群 A 、平行移動の点 P 、座標 ψ を特定し、 ψ が単射になる正確な領域とともに平行移動の定理を証明する。曲線が結節点を持つ等位や直線と円錐曲線に分かれる等位（判別式が非平方のときは二次拡大の固有座標、放物的な場合は加法的な座標）、座標が一つまたは二つ消える Euler のコマの等位、固定点と平衡点を含む。主張は任意の体の上で、Mathlib の Weierstrass 曲線とその群法則 [1, 26] を基礎として証明される。
- (ii) **位相による正則性（7 節）。** 有理写像は特異集合の上で定義されない。各等位で一步またはその逆が定義されない状態が明示的に書けて少数であること（Lyness 写像では高々二つ、Euler のコマでは等位の乗数について次数 3 以下と 4 以下の二つの多項式の根から定まる高々 56 個の候補）を示す。したがって状態が正則であることと、それらのどれも剰余類 $\psi(s) + \langle P \rangle$ にないことは同値である。状態が正則か否かは反復なしに判定でき、正則でない状態についても同じ対数とその有限な連鎖と、あれば t への唯一の歩数を与える。
- (iii) **$\mathbb{Q}$ への還元（8 節）。** 有理数のデータについて、素数を法とする正則性が $\mathbb{Q}$ に引き戻ること、 $\mathbb{Q}$ 上の歩数が p を法とする還元でも歩数であること、 p を法として道がなければ $\mathbb{Q}$ 上にもないことを証明する。少数の素数と中国剰余定理、一回の有理数の厳密な反復で $\mathbb{Q}$ 上の

$\text{Id}(s, t)$ が決まり、ある素数で道がなければ、反復では決して得られない無条件の答え「決して」が返る。

- (iv) **型理論的な内容 (9 節)**。力学は五つの定数からなる Martin-Löf 型理論の理論であり、HoTTLean [17] の垂群モデルで解釈される。閉じた項 s, t の間の恒等型は $\text{Id}(s, t)$ で、ループ空間は周期の部分群で解釈され、解釈の健全性から、別の軌道にある状態の間の恒等型の閉じた項は構成できないことが従う。
- (v) **検証済みの検査器 (10.4 節)**。定理に加えて、開発は $\mathbb{F}_q$ 上の Lyness 写像の証明書の実行可能な検査器を含む。検査器は Mathlib に依存しない Lean で書かれ、受理した主張が Lean での定義について真であるという健全性定理を伴う。

すべてが形式化されている。Lean 4 [7] の定理 1,146 個、sorry なし、公理は `propext · Classical.choice · Quot.sound` のみ、そしてすべての主要な定理について、全仮定を Lean の中で示した具体的な状態に適用し、空虚でないことを確かめた (10.3 節)。この理論は、 $\text{Id}(s, t)$ と関連する構造の問いに独立の検査器が確かめる証明書つきで答えるシステム Structure Computer [18] の基礎である。一例： $a = 3$ の Lyness 写像を $\mathbb{F}_q$ 、 $q = 2^{61} - 1$ の上で考えると、状態 $t = (813066766938016773, 992646061924517494)$ には、 $s = (2, 5)$ からちょうど $n \equiv 7,863,588,611,074,867 \pmod{576,460,752,629,115,698}$ を満たす歩数で着く。計算と検査で 0.4 秒。実測した毎秒 2.6×10^6 歩で反復すれば約 96 年かかる (付録 A)。

2 設定

2.1 部分流と正則状態

有理写像はいたるところで定義されるわけではない。Lyness 写像は $x = 0$ または $a + y = 0$ で、その逆写像は $y = 0$ または $a + x = 0$ で未定義である。そこで**部分流**を扱う。

定義 2.1 (部分流). 集合 S 上の部分流とは、定義されるところで互いに逆になる二つの部分写像 $f, g : S \rightarrow S$ の組である。 $f(x) = y$ なら $g(y) = x$ 、またその逆。

定義 2.2 (正則状態). 状態 s は、すべての前向きな反復 $f^n(s)$ と後ろ向きな反復 $g^n(s)$ ($n \in \mathbb{N}$) が定義されるとき**正則**という。

正則状態は f, g で閉じ、 f はその上で g を逆とする置換 σ に制限される。これを**正則な流れ**と呼び、整数べきを σ^n と書く。有限の状態空間では正則と周期的は同じなので、小さい q では正則性は閉路の検出である。7 節では反復なしにそれを判定する。正則でない状態は有限の**連鎖**の上であり、 f の反復は f が未定義の**前向きに詰まる状態**で、 g の反復は後ろ向きに詰まる状態で止まる。連鎖上の状態から目標の状態 t に着くのは高々一度である。

2.2 答えの三つの形

状態 s, t について、 $\text{Id}(s, t)$ の答えは次のちょうど一つである。

- **歩数** $(r, M) : s, t$ は正則で、 $\{n : \sigma^n s = t\} = r + M\mathbb{Z}$ 、 $M \geq 0$ (軌道が無限になりうる $\mathbb{Q}$ 上

では、 $|n|$ の上界 B の範囲での答え)。

- **道なし** : s は正則で、すべての $n \in \mathbb{Z}$ について $\sigma^n s \neq t$ (t が正則でない場合を含む)。
- **正則でない** : s は正則でない。答えは前向きの連鎖の長さ t と、 $f^n s = t$ ($n \geq 0$) または $g^{-n} s = t$ ($n < 0$) となる高々一つの n を与える。

2.3 作用亜群

流れ (S, σ) は $\mathbb{Z}$ -集合であり、その**作用亜群** $S//\mathbb{Z}$ は状態を対象とし、 $\sigma^n s = t$ となる整数 n を s から t への射とする。射の集合 $\text{Hom}(s, t) = \text{Id}(s, t)$ が研究の対象であり、 s の自己同型群は周期の部分群 $M\mathbb{Z}$ 、軌道の基本群である。

3 位相：群上の平行移動流

定義 3.1 (位相). $\Phi = (S, \sigma)$ を流れ、 A をアーベル群、 $P \in A$ 、 $\psi : S \rightarrow A$ 、 $R \subseteq S$ を $\sigma x \in R \iff x \in R$ を満たす部分集合とする。 (ψ, P) が R 上の**位相座標**であるとは、すべての $x \in R$ について $\psi(\sigma x) = \psi(x) + P$ であり、 ψ が R 上で単射であることをいう。

定理 3.2 (平行移動流). (ψ, P) を R 上の位相座標、 $s, t \in R$ とする。すべての $n \in \mathbb{Z}$ について

$$\sigma^n s = t \iff \psi(t) - \psi(s) = nP.$$

したがって $\text{Id}(s, t) = \{n \in \mathbb{Z} : \psi(t) - \psi(s) = nP\}$ であり、 $\psi(t) - \psi(s) \notin \langle P \rangle$ なら空、そうでなければ P の位数を法とする剰余類である。また s, t が同じ軌道にあることと $\psi(s) \equiv \psi(t) \pmod{\langle P \rangle}$ は同値である。

Proof. 帰納法と R の両向きの不変性から、 $x \in R$ 、 $n \in \mathbb{Z}$ について $\psi(\sigma^n x) = \psi(x) + nP$ 。 $\sigma^n s = t$ なら $\psi(t) = \psi(s) + nP$ 。逆に $\psi(t) = \psi(s) + nP$ なら R 上の単射性で $t = \sigma^n s$ 。 n の P の位数を法とする一意性は位数の定義である。 $\square$

$\psi(x)$ の $A/\langle P \rangle$ における類が x の**位相**である。位相は σ で保存され、定理 3.2 により軌道の完全不変量である。位相は保存量の等位集合を $A/\langle P \rangle$ の元ごとに細分し、有限体上では等位集合上の軌道の高々 $|A/\langle P \rangle|$ である。例 A.7 の二つの状態は Euler のコマの保存量の値が等しいのに別の軌道にあり、位相がそれを分ける。

巡回群 $A = \langle g \rangle$ 、 $P = eg$ 、 $\psi(t) - \psi(s) = jg$ では条件は $en \equiv j \pmod{\text{ord } g}$ と読み、 $\gcd(e, \text{ord } g) \mid j$ のとき解ける。位数と対数は Pohlig–Hellman で計算し、剰余類は素数べき部分から中国剰余定理で組み立てる。巡回でない A (楕円曲線 $\mathbb{Z}/n_1 \times \mathbb{Z}/n_2$ 、 $(\mathbb{Z}/2)^r$ との積) でも成分ごとに同じであり、 $\psi(t) - \psi(s) \notin \langle P \rangle$ であることは、ある素数べき成分で確かめられる。部分的な平行移動も同様に扱う。禁止集合 $B \subseteq A$ について、部分写像 $a \mapsto a + P$ ($a, a + P \notin B$ のとき定義) に関し、 a が正則であることは剰余類 $a + \langle P \rangle$ が B と交わらないことと同値である。これが 7 節の抽象形である。

4 Lyness 写像

以下 K は体、 $a \in K$ とする。

4.1 写像と積分

パラメータ a の Lyness 写像は部分流

$$T(x, y) = \left(y, \frac{a+y}{x}\right) (x \neq 0, a+y \neq 0), \quad T^{-1}(x, y) = \left(\frac{a+x}{y}, x\right) (y \neq 0, a+x \neq 0)$$

であり、漸化式 $x_{n+1}x_{n-1} = a + x_n$ を一階の系に書き直したものである。条件 $a+y \neq 0$ は像で T^{-1} が定義されるためのものである。積分は

$$I(x, y) = \frac{(x+1)(y+1)(x+y+a)}{xy}$$

で、 T が定義されるところで $I(Tx) = I(x)$ 。状態が等位 k 上にあるとは $xy \neq 0$ かつ $kxy = (x+1)(y+1)(x+y+a)$ であること。異なる等位の状態は決して結ばれない。

4.2 楕円的な等位

等位 k に対し $W_k: Y^2 = X^3 + A_2X^2 + A_4X + A_6$ 、

$$A_2 = (a-k)^2 - 4a + 2k + 4, \quad A_4 = 4k((a-k)^2 - 2a + k), \quad A_6 = 4k^2((a-k)^2 + 2k)$$

を Weierstrass 曲線とする。判別式は $\Delta(W_k) = 4096k^3(a-k-1)^2(a^3 - 2a^2k - 6a^2 + ak^2 - 10ak + 12a + k - 8)$ であり、 $\Delta \neq 0$ の等位を楕円的という ($k \neq 0, k \neq a-1, \text{char } K \neq 2$ が従う)。

$$U = -2(k + 2xy + 2x + 2y + 2), \quad V = -4(a(x+1)(y+1) - k(xy + x - y) + 2y(x+1)(y+1))$$

とおき、 $\varphi(x, y) = (U, V)$ 、 $Q = (2k, 4k(a-k-1))$ とする。

定理 4.1 (楕円的な等位). $\Delta(W_k) \neq 0$ なら、 φ は等位 k を $W_k(K)$ に写し、 $Q \in W_k(K)$ 、 $T(x, y)$ が定義されるとき W_k の群法則で $\varphi(T(x, y)) = \varphi(x, y) + Q$ 、 φ は等位上で単射である。したがって等位の正則状態 s, t とすべての $n \in \mathbb{Z}$ について

$$T^n s = t \iff \varphi(t) - \varphi(s) = nQ$$

であり、 $\varphi(s)$ の $W_k(K)/\langle Q \rangle$ における類は等位上の軌道の完全不変量である。

初めの三つの主張は等位の式を仮定とする多項式恒等式に帰着し、Mathlib の加法公式を用いて証明される。 $\mathbb{F}_q$ 上では $\text{Id}(s, t)$ は位数 $\approx q$ の群における楕円曲線の離散対数であり、 $q = 2^{61} - 1$ では位数が約 2^{40} を超える素因数を持たない限り 1 秒を大きく下回る時間で答えが出る (2^{45} 程度の素因数を持つ例 A.2 では 18 秒)。

4.3 結節点を持つ等位

$\Delta(W_k) = 0$ だが $k \neq 0, k \neq a-1, 2 \neq 0$ のとき、 W_k はちょうど一つの特異点を持ち、非特異点は同じ加法公式で群をなす。等位上にあつて $\varphi(x, y)$ が W_k の非特異点である状態を良いという。

定理 4.2 (結節点を持つ等位). この仮定の下で良い状態は不変な領域をなし、その上で $\varphi \circ T = \varphi + Q$ 、 φ は単射である。したがって W_k の非特異点の群について定理 3.2 が良い状態の上で成り立つ。等位上の良くない状態は T の固定点である。

4.4 可約な等位 $k = 0$ と $k = a - 1$

判別式が除く二つの等位では曲線は可約で、 T は成分を置換し、 T のべきが各成分に Möbius 変換として働く。群は、固有座標の乗法群または加法群と $\mathbb{Z}$ の積を、一つの元が生成する部分群で割った商である。

■ $k = 0$ ：三本の直線。 等位は $x = -1$ 、 $x + y + a = 0$ 、 $y = -1$ で、 T が巡回させる。 $x = -1$ 上で T^3 は固定点 $y = 1 - a$ と $y = -1$ を持ち、 $\ell = (y + 1)/(y + a - 1)$ を $(a - 1)^{-1}$ 倍する。頂点を除く状態 $(x, y \neq 1 - a, (x, y) \neq (-1, -1))$ で、等位から $K^\times \times \mathbb{Z}$ への写像 v を、 $x = -1$ 上で $(\frac{y+1}{y+a-1}, 0)$ 、 $y = -1$ 上で $(\frac{x+a-1}{x+1}, 2)$ 、それ以外で $(\frac{x+1}{x+a-1}, 1)$ と定める。

定理 4.3. $a \neq 1, 2$ のとき、 $G = (K^\times \times \mathbb{Z})/\langle((a - 1)^{-1}, -3)\rangle$ における類 $\psi = [v]$ は $\psi(Tx) = \psi(x) + [(1, 1)]$ を満たし頂点の外で単射である。頂点の外で、 $A = G$ 、 $P = [(1, 1)]$ として定理 3.2 が成り立つ。

$\mathbb{F}_q$ 上の群の位数は $3(q - 1)$ で、頂点は長さ高々 3 の軌道をなす。 $a = 2$ では三本の直線が一点で交わり Möbius 写像は放物的で、座標 $c = 1/(y + 1)$ は加法的、群は $(K \times \mathbb{Z})/\langle(1, -3)\rangle$ ($\mathbb{F}_q$ 上の位数 $3q$) である。

■ $k = a - 1$ ：直線と円錐曲線。 $(x + 1)(y + 1)(x + y + a) - (a - 1)xy = (x + y + 1)((x + 1)(y + 1) + a - 1)$ なので、等位は直線 $x + y + 1 = 0$ と円錐曲線 $(x + 1)(y + 1) = 1 - a$ で、 T が入れ替える。直線上で T^2 は $z \mapsto (a - 1 - z)/z$ で、固定点 x_1, x_2 は $z^2 + z + 1 - a$ の根。 $\ell(z) = (z - x_1)/(z - x_2)$ とおくと T^2 は ℓ を x_2/x_1 倍する。固有座標は $L = K(x_1, x_2)$ に値をとる。

定理 4.4. $L \supseteq K$ が $x_1 + x_2 = -1$ 、 $x_1 x_2 = 1 - a$ を満たす $x_1 \neq x_2$ を含み、 $a \neq 1$ とする。 $x \neq x_1, x_2$ の等位上の状態について、直線上で $[(\ell(x), 0)]$ 、円錐曲線上で $[(\ell(-1 - x), 1)]$ で定まる $(L^\times \times \mathbb{Z})/\langle(x_2/x_1, -2)\rangle$ への写像 ψ は $P = [(1, 1)]$ とする位相座標である。さらに $2 \neq 0$ で $4a - 3$ が K で非平方なら、 $L = K(\sqrt{4a - 3})$ として除外される状態はなく、位相は等位全体で完全である。

$\mathbb{F}_q$ 有理な状態の位相座標が値をとる部分群の位数は $2(q - 1)$ (分裂) または、 $L^\times$ のノルム 1 の部分で $2(q + 1)$ (非分裂)。接する場合 $4a = 3$ は放物的で群は $(K \times \mathbb{Z})/\langle(-2, -2)\rangle$ 、二つの可約な等位が一致する $a = 1$ ではすべての軌道の周期が 5 で、 $\text{Id}(s, t)$ は五歩から読める。表 1 に等位をまとめる。結節点と放物的な場合には $\text{char } K \neq 2$ が要る。

等位	条件	群 A	P
楕円的	$\Delta(W_k) \neq 0$	$W_k(K)$	$(2k, 4k(a - k - 1))$
結節点	$k \neq 0, a - 1; 2 \neq 0; \Delta = 0$	W_k の非特異点	同じ
$k = 0$	$a \neq 1, 2$	$(K^\times \times \mathbb{Z})/\langle((a - 1)^{-1}, -3)\rangle$	$[(1, 1)]$
$k = 0, a = 2$		$(K \times \mathbb{Z})/\langle(1, -3)\rangle$	$[(0, 1)]$
$k = a - 1$	$a \neq 1; L$ で $x_1 \neq x_2$	$(L^\times \times \mathbb{Z})/\langle(x_2/x_1, -2)\rangle$	$[(1, 1)]$
$k = a - 1, 4a = 3$		$(K \times \mathbb{Z})/\langle(-2, -2)\rangle$	$[(0, 1)]$

表 1 Lyness 写像の等位集合とその位相座標。

5 Euler のコマの Kahan–Hirota–Kimura 離散化

以下 $\text{char } K \neq 2$, $h a_1 a_2 a_3 \neq 0$ とする。

5.1 写像と保存量

Euler のコマは $\dot{x}_1 = a_1 x_2 x_3$, $\dot{x}_2 = a_2 x_3 x_1$, $\dot{x}_3 = a_3 x_1 x_2$ 。その Kahan 離散化 [4, 13] は Hirota と Kimura のもの [9] に一致し、各積を極化で置き換える：

$$\tilde{x} - x = h B(x, \tilde{x}), \quad B(x, y) = (a_1(x_2 y_3 + x_3 y_2), a_2(x_3 y_1 + x_1 y_3), a_3(x_1 y_2 + x_2 y_1))$$

(h は Hirota–Kimura の ϵ)。方程式は $\tilde{x}$ について線形で、 $B(x, \tilde{x}) = J(x)\tilde{x}$ となる行列 $J(x)$ を用いて $(1 - hJ(x))\tilde{x} = x$ と書け、行列式は $D_h(x) = 1 - h^2(a_2 a_3 x_1^2 + a_3 a_1 x_2^2 + a_1 a_2 x_3^2) - 2h^3 a_1 a_2 a_3 x_1 x_2 x_3$ 。したがって時間発展写像は有理写像 $T_h(x) = \text{adj}(1 - hJ(x))x / D_h(x)$ で、可逆、 $T_h^{-1} = T_{-h}$ 。Hirota–Kimura の三つの保存量は

$$I_{12} = \frac{a_2 x_1^2 - a_1 x_2^2}{1 - h^2 a_1 a_2 x_3^2}, \quad I_{23} = \frac{a_3 x_2^2 - a_2 x_3^2}{1 - h^2 a_2 a_3 x_1^2}, \quad I_{31} = \frac{a_1 x_3^2 - a_3 x_1^2}{1 - h^2 a_3 a_1 x_2^2}$$

であり、定義された一步に沿ってすべての分子と分母が共通の因子倍されるので、三つの比は保存される（独立なものは二つ）。

5.2 普遍コマとその等位

$u_i = \lambda_i x_i$, $\lambda_1^2 = h^2 a_2 a_3$, $\lambda_3^2 = h^2 a_1 a_2$, $\lambda_1 \lambda_3 = h a_2 a_1$ の縮尺変換（そのような λ_i は二つの二次拡大の塔 $L \supseteq K$ に存在する）によって、すべてのコマが**普遍コマ** $a = (1, 1, 1)$, $h = 1$ と共役になる。そこで $D(u) = 1 - u_1^2 - u_2^2 - u_3^2 - 2u_1 u_2 u_3$, $y(u) = (1 - u_1^2, 1 - u_2^2, 1 - u_3^2)$ とおくと、 y は各一步でスカラー倍されるので、状態の**等位**は点 $\alpha = [y(u)] \in \mathbb{P}^2(K)$ である ($y(u) \neq 0$ のとき。 $y(u) = 0$ の状態は 5.4 節で扱う)。

5.3 楕円的な等位

等位 α の代表 $(\alpha_1, \alpha_2, \alpha_3)$ を一つ固定し、その基本対称式を c_1, c_2, c_3 として、

$$W_\alpha: \quad Y^2 - 2c_1 XY - 4c_3 Y = X^3 - (c_1^2 - c_2)X^2 - 3c_1 c_3 X - 3c_3^2$$

とする。判別式は $16(\alpha_1 \alpha_2 \alpha_3)^2 \prod_{i < j} (\alpha_i - \alpha_j)^2$ で、等位が楕円的なのは α_i がすべて非零で相異なるとき。等位上の u について $y(u) = m\alpha$ と書き (m を u の**乗数**と呼ぶ)、 $\varphi_\alpha(u) = (N(u)/m^2, R(u)/m^3)$ とおく。ここで $\pi = (1 + u_1)(1 + u_2)(1 + u_3)$ として

$$N = \pi(u_1 + u_2 + u_3 - 1), \quad R = -\pi \left(\sum_i (u_i^3 - u_i^2 - u_i) - 2(u_1 u_2 + u_1 u_3 + u_2 u_3) + 1 \right)$$

であり、 $Q = (0, c_3)$ とする。

定理 5.1 (コマの楕円的な等位). $\Delta(W_\alpha) \neq 0$ なら、 φ_α は等位を $W_\alpha(K)$ に写し、 $Q \in W_\alpha(K)$ 、 Tu が定義されるとき $\varphi_\alpha(Tu) = \varphi_\alpha(u) + Q$ 、 φ_α は二歩が定義される状態の上に明示的な有理逆写

像を持つ。したがって定理 3.2 が普遍コマの等位の正則状態の上で成り立ち、縮尺変換を通じてすべてのコマについても成り立つ。そのとき位相座標は拡大 L 上の曲線に値をとる。

恒等式は u の次数 12 以下の無条件の多項式恒等式である。

5.4 すべての等位：場合 A、B、Z

普遍コマのすべての等位は、座標の巡回置換の後、三つの場合のどれかに入るか空虚である。

場合 A：すべての $\alpha_i \neq 0$ 。 二つの α_i が一致すると W_α は結節点や尖点を持ちうる。 W_α の定義式の二つの偏導関数は $\varphi_\alpha(u)$ でいずれも $\pi(u_1 + u_2)(u_1 + u_3)(u_2 + u_3)$ の倍数であり（たとえば Y についての偏導関数 $2Y - 2c_1X - 4c_3$ の値は $2\pi(u_1 + u_2)(u_1 + u_3)(u_2 + u_3)/m^3$ ）、 $\varphi_\alpha(u)$ が非特異であることと対ごとの和 $u_i + u_j$ が非零であることは同値である。偶数個の符号変換は群 $V \cong (\mathbb{Z}/2)^2$ をなして写像と可換であり、二つの座標が消えない限り、四つの像 gu ($g \in V$) のうち少なくとも一つで φ_α の値が非特異になる。位相座標は、選んだ元を g_u として $(\varphi_\alpha(g_u u), g_u) \in W_\alpha^{\text{ns}} \times V$ 、 $P = (Q, 0)$ 。

場合 B： $\alpha_3 = 0$ 、 $\alpha_1 \neq \alpha_2$ は非零。 $u_3 = \pm 1$ で、写像は等位の二つの成分 $u_3 = 1$ と $u_3 = -1$ を入れ替え、 $u_3 = -1$ を $u_3 = 1$ に写してから φ_α をとると $P' = (\alpha_2(\alpha_2 - \alpha_1), \alpha_2(\alpha_2 - \alpha_1)(2\alpha_2 + \alpha_1))$ だけ平行移動される。位相座標は $W_\alpha^{\text{ns}} \times \mathbb{Z}/2$ に値をとり、 $P = (P', 1)$ 。

場合 Z： $\alpha_2 = \alpha_3 = 0$ 。 $u_2, u_3 = \pm 1$ で、写像は $(u_1, u_2, u_3) \mapsto (u_1 - 2u_2u_3, -u_2, -u_3)$ 。 $[\pm 1] \in \mathbb{Z}/2$ を符号の類として、位相座標は $(u_1u_2u_3, [u_2], [u_2u_3]) \in K \times (\mathbb{Z}/2)^2$ 、 $P = (-2, 1, 0)$ 。

正則状態のない等位。 $\alpha = (c, c, 0)$ の等位と $y(u) = 0$ となる状態では二歩続けて進める状態がなく、正則状態はない。平衡点（二つの座標が零）は固定点である。

定理 5.2 (すべてのコマのすべての等位). $\text{char } K \neq 2$, $ha_1a_2a_3 \neq 0$ とし、等位を一つ固定する。アーベル群 A , $P \in A$ 、正則状態の上の写像 ψ があって、その等位上の平衡点でないすべての正則状態 s, t について、すべての $n \in \mathbb{Z}$ で $\sigma^n s = t \iff \psi(t) - \psi(s) = nP$ 。 s, t が同じ軌道にあることと $\psi(t) - \psi(s) \in \langle P \rangle$ は同値。 $\psi(t) - \psi(s) \notin \langle P \rangle$ なら 9 節の意味で s, t の間の恒等型の閉じた項は構成できない。

注意 5.3. 拡大 L は一般には避けられない。 $h^2a_2a_3$ が非平方なら $\mathbb{F}_q$ 有理な状態の位相座標は位数 $\approx q^2$ の $W_\alpha(\mathbb{F}_{q^2})$ に値をとる。そこで点の位数を Hasse の区間で baby-step giant-step により求めるには約 $q^{1/2}$ 回の演算が要り、 $\mathbb{F}_q$ 上の曲線の $q^{1/4}$ 回と対照的である。実用上の上限が Euler のコマで $q \approx 2^{45}$ 、Lyness 写像で $q \approx 2^{61}$ と異なるのはこのためである。

6 線形流、離散化した振動子、E2

■振動子。 離散化した調和振動子 $\sigma(x, y) = (y, -x + 2cy)$ は保存量 $x^2 + y^2 - 2cxy$ を持つ。 $l \in L^\times$ が $l + l^{-1} = 2c$, $l \neq l^{-1}$ を満たすなら固有座標 $x - ly$ と $x - l^{-1}y$ は $l^{\pm 1}$ 倍され、合わせて単射なので、歩数は $\langle l \rangle \leq L^\times$ の対数である ($L = K$ または K の二次拡大)。 $c = \pm 1$ では Jordan の閉形式 $\sigma^n(x, y) = l^n(x + \frac{n}{l}w, y + nw)$ 、 $w = y - lx$ により歩数は線形方程式になる。 $\det C = 1$ のスカラーでない線形写像 C ($2 \neq 0$) は $2c = \text{tr } C$ の振動子に共役であり、 $\det C = 1$ で孤立した

固定点を持つアフィン写像 $v \mapsto Cv + b$ はその点を原点とする座標で線形になる。 $\text{tr } C = 2$ で固定点を持たないアフィン写像は標準形 $(x, y) \mapsto (x + y, y + 1)$ と $(x, y) \mapsto (x, y + 1)$ を持つ。

■E2。 [18] で E2 と呼ぶ系は、二次形式 Q (双線形式 B) について $-\log Q$ の Hessian 計量の測地流の Kahan 離散化である。 $Q = x^2 - y^2 - z^2$ では $Q = 1$ 上の測地線が双曲平面のものである。写像は $Q(p)Q(x) \neq 0$ の状態 (p, x) 上で $(p, x) \mapsto (x, (2B(x, p)x - Q(x)p)/Q(p))$ で、決して特異にならない。 $r = Q(x)/Q(p)$ 、 $b = B(p, x)/Q(p)$ 、任意の交代双線形式 ω についての $\omega(p, x)/Q(p)$ が保存され、軌道は $x_{k+1} = 2bx_k - rx_{k-1}$ を満たすので、 σ^k は同伴行列 C の k 乗であり、独立な p, x について作用重群における状態の自己同型群は $\text{ord}(C)\mathbb{Z}$ 。位相座標は $\lambda^2 - 2b\lambda + r$ の根の固有座標か Jordan 形で与えられる。

■共役。 部分流の同型 ($f(x) = y \iff f'(ex) = ey$ の全単射 e) は正則性、歩数、道のないこと、部分軌道を保つ。 Lyness 型 $(x, y) \mapsto (y, (a + by)/x)$ とその反転は縮尺の後パラメータ a/b^2 の Lyness 写像である。全単射な座標変換で式が Lyness 写像の式になる系は Lyness の流れに同型である。Kahan 離散化はアフィン座標変換と可換なので、アフィン座標で Euler のコマになる二次のベクトル場の Kahan 離散化はコマのものに同型である。例 A.8–A.10 はこれらの定理による。見慣れない有理写像やベクトル場も、Lyness 写像や Euler のコマとして認識すれば答えが得られる。定理が要求するのは多項式恒等式の検証だけである。

7 位相による正則性

ここまでの主張はすべて正則状態についてのものであり、この仮定は実際に効いてくる。約 8.8×10^{17} 歩進んでから零除算に至る状態もある (例 A.2)。しかし位相座標を持つ等位では、詰まる状態は明示的で少数であり、正則性の判定は群の部分群への所属の判定に帰着する。

定理 7.1. (f, g) を部分流、 R を定義された一步に沿って不変な領域、 $\psi : R \rightarrow A$ を $f(x) = y$ のとき $\psi(y) = \psi(x) + P$ を満たす写像とし、 $s \in R$ とする。

- (a) f または g が未定義のすべての $z \in R$ が $\psi(z) - \psi(s) \notin \langle P \rangle$ を満たすなら、 s は正則。
- (b) ψ が R 上単射で、そのような z のどれかが $\psi(z) - \psi(s) \in \langle P \rangle$ を満たすなら、 s は正則でない。
- (c) (連鎖) (b) の仮定の下、 $n \geq 0$ について $f^n(s) = t$ であることと、 $t \in R$ 、 $\psi(t) = \psi(s) + nP$ 、かつ $0 \leq m < n$ で $\psi(y) = \psi(s) + mP$ となる前向きに詰まる $y \in R$ がないことは同値。 g と $-P$ 、後ろ向きに詰まる状態についても同様。

Proof. (a) $f^m(s)$ が詰まる状態 z なら $\psi(z) = \psi(s) + mP$ となり、仮定に反する。 g についても同様。(b) $\psi(z) = \psi(s) + nP$ 、 f が z で未定義、 $n \geq 0$ とすると、 s が正則なら $f^n(s)$ は定義され R にあり z と同じ ψ の値を持つので、単射性で z に等しい。(c) $f^n(s) = t$ なら $m < n$ のすべての $f^m(s)$ が定義されるので、それらと同じ ψ の値を持つ前向きに詰まる状態はない。逆に $m < n$ について ψ の値が $\psi(s) + mP$ である前向きに詰まる状態 y がなければ、(a) の議論で $f^n(s)$ までの反復はすべて定義され、単射性により $f^n(s) = t$ である。 $\square$

■Lyness 写像。 等位 k 上で T は $a + y = 0$ で未定義。 $y = -a$ を等位の式に代入すると $(1 - a)x = -(ka + 1 - a)$ 。したがって $a \neq 1$ なら等位には高々一つの前向きに詰まる状態 $F = (-\frac{ka+1-a}{1-a}, -a)$ と一つの後ろ向きに詰まる状態 $G = (-a, -\frac{ka+1-a}{1-a})$ があり、状態が正則であることと $\varphi(F) - \varphi(s)$ 、 $\varphi(G) - \varphi(s)$ のどちらも $\langle Q \rangle$ にないことは同値である。したがって判定は離散対数二つ（または非所属の証拠二つ）で済み、そうでなければ連鎖と t への歩数は $\varphi(F) - \varphi(s)$ 、 $\varphi(G) - \varphi(s)$ 、 $\varphi(t) - \varphi(s)$ の対数から読める。結節点の等位と可約な等位でもそれぞれの群で同じことが成り立つ。

■Euler のコマ。 普遍コマでは写像は $D(u)D(-u) = 0$ のところ、または一步で y に掛かるスカラー因子かその鏡像 ($T^{-1} = T_{-h}$ についての同じ因子) が消えるところで未定義。乗数 m の状態 ($y(u) = m\alpha$) について $r_i = 1 - m\alpha_i$ とおくと

$$P_D(m) = (1 - \sum r_i)^2 - 4r_1r_2r_3,$$

$$P_P(m) = ((1 + r_3 - r_1 - r_2)^2 + 4r_3 - 4r_1r_2)^2 - 16(1 + r_3 - r_1 - r_2)^2r_3$$

は次数 ≤ 3 、 ≤ 4 で、 $r_i = u_i^2$ のとき $P_D(m) = D(u)D(-u)$ であり、 $P_P(m)$ は T のスカラー因子と T^{-1} のその積である。したがって詰まる状態は P_DP_P の根 m について $u_i = \pm\sqrt{1 - m\alpha_i}$ となる u の中にある。高々 $7 \times 8 = 56$ 個の候補で、根の抽出で見つかる。詰まる候補のどれも $\psi(s)$ の剰余類になれば s は正則（縮尺変換ですべてのコマに）。剰余類にある候補が詰まっていて、しかも反対向きに二歩進めるなら、 s は正則でない。

8 有理数への還元

$\mathbb{Q}$ 上では軌道は一般に無限で、離散対数は使えない。代わりに素数を法とする還元を用いる。

定義 8.1 (還元). 部分流 Φ から Ψ への還元とは、 $\rho(x) = x'$ かつ $f_\Psi(x') = y'$ のとき $f_\Phi(x) = y$ 、 $\rho(y) = y'$ となる y があり、 g についても同様な部分写像 ρ である。

p 整なデータを持つ有理写像の p を法とする還元はこの意味の還元である。還元した分母が非零なら、もとの分母は p 進単数だからである。

定理 8.2 (還元). $\rho(s) = s'$ 、 $\rho(t) = t'$ とする。(a) s' が正則なら s も正則。(b) s' が正則なら、すべての n について $\rho(\sigma^n s) = \sigma'^n s'$ 、特に $\sigma^n s = t$ なら $\sigma'^n s' = t'$ 。(c) s' が正則で、すべての n で $\sigma'^n s' \neq t'$ なら、すべての n で $\sigma^n s \neq t$ 。

四つの族について $\mathbb{Q} \rightarrow \mathbb{Q}_p \supseteq \mathbb{Z}_p \rightarrow \mathbb{Z}/p$ に沿って合成すると： p 整な a, x, y について、 $(\bar{x}, \bar{y})$ が $\mathbb{Z}/p$ 上の正則な Lyness の状態なら (x, y) は $\mathbb{Q}$ 上で正則。 $\mathbb{Q}$ 上の歩数は p を法とする還元でも歩数である。 $\bar{s}$ と $\bar{t}$ が p を法として決して結ばれないなら s と t は $\mathbb{Q}$ 上で決して結ばれない。Euler のコマ、振動子、対角形式の E2 も同様である。

■ $\mathbb{Q}$ 上の決定手続き。 $|n|$ の上界 B が与えられたとき、ある下限より大きい素数を順に、データが p 整でないか $\bar{s}$ が正則でないものを飛ばして選び、各素数で正則性を含めて $\text{Id}(\bar{s}, \bar{t})$ を計算する。どれかの素数での「道なし」は (c) により $\mathbb{Q}$ 上で道なしであり、無条件で B によらない。そうでなければ剰余類を法が $2B$ を超えるまで中国剰余定理で合わせる。 $|n| \leq B$ の候補は高々一つ残り、

有理数の厳密な反復で確かめるか除外する。素数での $\bar{s}$ の正則性が本質的である。これがなければ $\mathbb{Q}$ 上の道が零除算に還元される状態を通りうる。例 A.4 と A.6 はこの手続きによる。 $\bar{s}$ と $\bar{t}$ の位相が異なる素数が一つあれば、 $a = 3$ の Lyness 写像が $\mathbb{Q}$ 上で $(3, 7)$ を $(7, 3)$ に決して運ばないこと (両方とも正で同じ等位曲線上にあるにもかかわらず)、および $\mathbb{F}_q$ 上で結ばれる Euler のコマの二つの状態が $\mathbb{Q}$ 上では決して結ばれないことが示される。

9 型理論的な内容

HoTTLean/SynthLean [17] の構文で、Martin-Löf 型理論の理論

$$X : \mathcal{U}_0, \quad s, t : X, \quad \text{step} : X \rightarrow X, \quad \text{path} : \prod_{x:X} \text{Id}_X(x, \text{step } x)$$

を考える。この理論ではすべての m, n について $\text{Id}(\text{step}^m s, \text{step}^n s)$ の項が構成できる (path、 J 、反射律)。任意の流れ (S, σ) と状態 s_0, t_0 について、理論は HoTTLean の亜群モデルで $X \mapsto S // \mathbb{Z}$ 、 $s, t \mapsto s_0, t_0$ 、 $\text{step} \mapsto \sigma$ ($\mathbb{Z}$ 作用と可換なので関手)、 $\text{path} \mapsto (x \mapsto 1 : x \rightarrow \sigma x)$ ($\mathbb{Z}$ が可換なので自然) と解釈される。

定理 9.1. 亜群モデルで恒等型 $\text{Id}_X(s, t)$ は $\text{Hom}_{S // \mathbb{Z}}(s_0, t_0) = \{n : \sigma^n s_0 = t_0\}$ 、項 $\text{step}^n s$ は $\sigma^n s_0$ 、ループ空間 $\text{Id}(s, s)$ は周期の部分群で解釈される。解釈の健全性により、 t_0 が s_0 の軌道上にないなら (特に保存量または位相が異なるなら)、恒等型 $\text{Id}(\text{step}^m s, \text{step}^n t)$ の閉じた項は構成できない。

3-8 節の結果は、この意味で**恒等型を計算している**。作用亜群の射の集合と位相方程式の解集合の間の同値は、反復に関する主張を経由せず、集合の同値として直接証明されている。流れの共役 e は作用亜群の同型を与え、それに沿った輸送は $\text{Id}(s, t)$ を歩数を保って $\text{Id}(es, et)$ に運び、保存量と周期も移る。これは、6 節の共役と、システムが検査済みの結果を共役な系へ「輸送」する操作を型理論で定式化したものである。

10 形式化

10.1 範囲と統計

開発は Lean 4 [7] で Mathlib [26] と HoTTLean の上に書かれ、1,146 個の定理が、抽象的な位相の定理、四つの族の等位ごとの定理、正則性、還元、共役と座標変換、式で与えた系の意味、型理論的な解釈、実行可能な検査器とその健全性の証明にわたる。sorry、admit、axiom、native_decide はなく、カーネルでの計算は decide による。全定理の使用公理を自動で監査し、propext、Classical.choice、Quot.sound 以外が使われていないことを確かめた。

10.2 証明の技法

Lyness 写像の楕円的な恒等式は等位の式を仮定とする多項式恒等式 (コマのものは無条件) で、明示的な係数を与えた linear_combination により Mathlib のアフィンな加法公式を用いて証明され、群法則の退化した分岐は場合分けで扱う。形式証明の前後に数式処理で記号的・数値的に照合した。群論には Mathlib のものを、還元の補題には Mathlib の p 進整数を、退化した等位には二次拡大のための AdjoinRoot と群 $(K^\times \times \mathbb{Z}) / \langle \cdot \rangle$ のための商群を使う。

10.3 非空性

仮定の多い定理は気づかれずに空虚になりうる。そこですべての主要な定理を、全仮定を Lean の中で証明した具体的な状態に適用する。 $\mathbb{F}_{13}$ 上 $a = 2$ 、等位 $k = 11$ の Lyness 写像（正則状態、連鎖 $(11, 8) \rightarrow (8, 8) \rightarrow (8, 11)$ ）を持つ非正則状態、二つの可約な等位。 $\mathbb{F}_{17}$ 上の Euler のコマ $(2, 2, 16, 10)$ の正則状態と非正則状態。 $\mathbb{Q}$ 上の状態 $(2, 5)$ (Lyness、 $a = 3$) と $(1/3, 1/5, 1/7)$ (Euler のコマ $(1, 2, -3, 1/2)$) が 13 を法とする閉路から還元で正則。Jordan 形と非分裂の振動子。猫写像 ($\mathbb{F}_{13}$ 上で周期 14) とアフィンな猫写像を含む共役の項目。可能な場合は同じ事実を直接の計算でも確かめ、定理の帰結と一致することを確認した。

10.4 健全性を証明した証明書検査器

[18] で述べるシステムはすべての答えに証明書（等位、平行移動の点、素因数分解付きの位数、対数または非所属の証拠、正則性のデータ）を付け、独立のプログラムが検査する。 $\mathbb{F}_q$ 上の Lyness 写像についてはその検査器が第二の形でも存在する。実行時に Mathlib を使わない Lean で書かれ、受理したものは真であるという定理を伴う。検査器が証明書を受理するなら q は素数で、 $\mathbb{Z}/q$ 上で、開発で定義された Lyness の流れについて主張が成り立つ。すなわち、**歩数** (r, M) については正則状態について $\sigma^n s = t \iff n \equiv r \pmod{M}$ 、**道なし**についてはすべての n で $\sigma^n s \neq t$ 、**正則でない**については s が正則でなく述べられた連鎖の長さを持ち、 t に述べられた n でちょうど着くこと。実行部は証明済みの Lucas 判定で Pratt の素数性証明書 [22] を検証し、Mathlib の群演算と一致することを証明したアフィンな加法公式を使い、 $NP = 0$ と N のすべての素因数 ℓ について $(N/\ell)P \neq 0$ であることで位数を確かめ、証拠の確認に必要な有界回だけ反復する。楕円的な等位と結節点を持つ等位を、正則性のすべての判定結果と非正則状態の部分軌道も含めて扱う。系として 9 節の型理論的な結論が得られる。受理された**歩数**の証明書は作用垂群における同値 $\text{Id}(s, t) \simeq \{n : n \equiv r \pmod{M}\}$ を与え、受理された**道なし**の証明書からは、恒等型の閉じた項が構成できないことが従う。

11 関連研究

QRT 写像の平行移動の構造は Quispel, Roberts, Thompson [23, 24] によるもので、特異ファイバーを含めて Duistermaat [8] が網羅的に扱った。Bastien と Rogalski [3] は Lyness 写像の等位曲線上の実数の力学を記述し、Hone [10, 11] は Lyness の反復をスカラー倍として因数分解に使った。Hirota–Kimura 離散化 [9] とその保存量は Petrera と Suris [19] が Kahan の方法の一般論 [4, 20] の中で研究した。本稿はこれらの上に築く。すべての等位の明示的な Weierstrass モデルと平行移動の点 (W_α とすべてのコマの普遍コマへの縮約を含む)、退化した等位の完全な扱い、正則性の判定法と還元定理、およびそれらすべての形式証明を与える。線形写像の軌道問題は Kannan–Lipton [14] と Chonev–Ouaknine–Worrell [6]、楕円可除列の添字の復元と楕円離散対数の関係は Lauter と Stange [15] による。Roberts と Vivaldi [25]、Jogia, Roberts, Vivaldi [12] は $\mathbb{F}_p$ 上の可積分写像を周期の統計とファイバーの群の位数を通して研究した。本稿は個々の軌道を計算する。Mathlib の Weierstrass 曲線 [1] が形式化の基礎であり、我々の知る限り、QRT 写像や Kahan 写像の形式化、力学の道具としての楕円離散対数の形式化は証明支援系でこれが初めてである。垂群モデルと検

証済みの解釈は HoTTLean/SynthLean [17]、Awodey と Hua [2] がプロジェクトの型理論的な出発点に示唆を与えた。信頼できないソルバが出す証明書を検証済みの検査器で確かめる手法は確立しており [5, 16]、10.4 節はそれを軌道の証明書に持ち込む。

12 範囲と今後

理論が扱うのは四つの族とそのアフィン共役である。一般の QRT 写像は楕円曲線のペンシルを保つので 4 節は拡張の雛形であり、十分な数の保存量を持つ高次元の Kahan 離散化が自然な次の対象である。点の数え上げを実装すれば、Euler のコマ ($h^2 a_2 a_3$ が非平方の場合) の実用上の上限 $q \approx 2^{45}$ を引き上げられる見込みである。Lean で検証した検査器を Lyness 写像から他の族と $\mathbb{Q}$ に広げることが形式面の次の一步である。

AI の利用について

この研究は AI アシスタント (Claude、Anthropic) が中心的な役割を担って行われた。目標の設定、何を作り何を証明するかを選択、設計上の決定、結果の確認は著者が行い、著者の指示の下で AI アシスタントが Lean の開発の大部分、姉妹システム、本稿の本文を書き、文献を照合し、付録 A の実測を行った。内容の責任は著者にある。数学の正しさは Lean のカーネルと Mathlib に立脚し、公理は監査され、主要な定理は具体的なデータで実体化されている。

謝辞

開発は Lean 4、Mathlib、HoTTLean の上に築かれている。その貢献者に感謝する。

A 例題

以下はシステムのサイトの「高度な例題」で、2026 年 10 月 22 日に 2 コアの Intel Xeon 2.1 GHz で計算し直した。時間は問いに答える一つのコマンドの壁時計時間 (起動、計算、独立の検査を含む。3 回の中央値)。比較のため、同じ機械は $\mathbb{F}_{2^{61}-1}$ 上の Lyness 写像を毎秒 2.6×10^6 歩、 $\mathbb{F}_{2^{40}+15}$ 上の Euler のコマを毎秒 2.4×10^6 歩で反復する。 $q_{61} = 2^{61} - 1$ 、 $q_{40} = 1,099,511,627,791$ 。

例 A.1 (Lyness、 $\mathbb{F}_{q_{61}}$: 7.9×10^{15} 歩先の状態)。 $a = 3$ 、 $s = (2, 5)$ 、 $t = (813066766938016773, 992646061924517494)$ 。等位 $k = 18$ 。 Q の位数は $576,460,752,629,115,698 = 2 \cdot 6673 \cdot 3612179 \cdot 11957747$ 、 $\log_Q(\varphi(t) - \varphi(s)) = 7,863,588,611,074,867$ 。
答え : $t = \sigma^n s \iff n \equiv 7,863,588,611,074,867 \pmod{576,460,752,629,115,698}$ 、両状態とも位相の判定で正則。0.39 秒。 7.86×10^{15} 歩の反復は約 96 年、法を反復で確立するにはその約 73 倍。

例 A.2 (Lyness、 $\mathbb{F}_{q_{61}}$: 長さ 8.8×10^{17} の連鎖)。 $a = 3$ 、

$$\begin{aligned} s &= (652450593252319644, 397870522539971473), \\ t &= (557047722706213665, 1530465154515367894). \end{aligned}$$

楕円的な等位 $k = 1031421348935828000$ で Q の位数は 2,305,843,011,612,193,701、前向きに詰ま

る状態の s に対する対数は 881,059,717,639,816,779. s は正則でなく、前向きの軌道はその歩数の後に零除算に当たり、 t にはちょうど $n = 403,567,694,157,578,575$ で着く。18.4 秒。時間は約 2^{45} の素数位数成分の算術に費やされる。

例 A.3 (Lyness、 $\mathbb{F}_{q_{61}}$: 同じ等位、決して着かない). $a = 3$ 、

$$s = (1473736884130421033, 1913329524460333331), \\ t = (1744307874685056163, 461811991117244972).$$

s, t は同じ等位 $k = 471089872214466856$ 上にある。 Q の位数は $192,153,584,192,171,886 = 2 \cdot 3^2 \cdot 47 \cdot 17203 \cdot 70957 \cdot 186071$. $\varphi(t) - \varphi(s) \notin \langle Q \rangle$ 、2 準素成分で確かめられる。答え：道なし。0.48 秒。 s の軌道を一周する反復は約 2,300 年。

例 A.4 ($\mathbb{Q}$ 上の Lyness : $(3, 7)$ と $(7, 3)$). $a = 3$ 、上界 30。両状態とも正で同じ等位曲線上にあり、似た組 $(2, 5), (5, 2)$ は 3 歩戻ると結ばれる。 $p = 10009$ で $\bar{s}$ は正則で位相が異なるので、 $\mathbb{Q}$ 上で $T^n(3, 7) = (7, 3)$ となる整数 n はない。0.19 秒。

例 A.5 (Euler のコマ、 $\mathbb{F}_{q_{40}}$: 周期の半分). $(a_1, a_2, a_3, h) = (1, 2, -3, 1/2)$ 、 $s = (3, 1, 4)$ 、 $t = (3, -1, -4)$ 。場合 A. Q の位数は $274,877,781,052 = 2^2 \cdot 7 \cdot 61 \cdot 7901 \cdot 20369$ 、対数 137,438,890,526。二つの符号を変えた状態にはちょうど周期の半分で着く。0.35 秒。

例 A.6 ($\mathbb{Q}$ 上の Euler のコマ : 同じ組). 同じデータ、上界 30。 $p = 10039$ で位相が異なる。 $\mathbb{F}_{q_{40}}$ 上で結ばれ、独立な二つの保存量の値が等しいこの二つの状態は、 $\mathbb{Q}$ 上では決して結ばれない。0.26 秒。

例 A.7 (Euler のコマ、 $\mathbb{F}_{q_{40}}$: 保存量が同じでも決して着かない). $s = (3, 1, 4)$ 、 $t = (-3, -1, 4)$ は独立な二つの保存量の値が等しい。 $\langle Q \rangle$ に属さないことは楕円曲線の成分で確かめられる。答え：道なし。0.42 秒。

例 A.8 (平面の有理写像、 $\mathbb{F}_{q_{61}}$). $x' = -\frac{3x^2-5xy+x+2y^2-3y-2}{3x-2y+5}$ 、 $y' = -\frac{3x^2-5xy-19x+2y^2+10y-33}{3x-2y+5}$ 、 $s = (21, 33)$ 、 $t = (492515881573357819, 1485161943497875320)$ 。アフィンな座標変換 $u = (3x - 2y + 5, -x + y - 7)$ が式を $a = 3$ の Lyness 写像に変え、状態は例 A.1 のものになり、答えは同じ剰余類である。0.44 秒。

例 A.9 (同じ写像を $\mathbb{Q}$ 上で). $s = (26, 40)$ 、 $t = (22, 32)$ 、上界 30。新しい座標での例 A.4。道なし。0.26 秒。

例 A.10 (三変数の二次のベクトル場、Kahan 離散化 $h = 1/2$ 、 $\mathbb{F}_{q_{40}}$). 分数係数の完全な二次式三つ (例題ページに掲載)、 $s = (6, 4, 14)$ 、 $t = (4, -6, -2)$ 。中心 (すべての偏導関数が消える点) と三つの軸 (斉次部分の $\mathbb{P}^2$ における零点) から Euler のコマ $(-3, 2, 1)$ 、 $h = 1/2$ (座標の順を逆にした例 A.5 のコマ) へのアフィン写像が得られ、答えは例 A.5 のものである。0.41 秒。

参考文献

- [1] David Kurniadi Angdinata and Junyan Xu. An elementary formal proof of the group law on Weierstrass elliptic curves in any characteristic. In *14th International Conference on Interactive Theorem Proving (ITP 2023)*, volume 268 of *LIPIcs*, pages 6:1–6:19. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2023. doi: 10.4230/LIPIcs.ITP.2023.6.
- [2] Steve Awodey and Joseph Hua. Path types in algebraic type theory. arXiv:2601.06567, 2026.
- [3] G. Bastien and M. Rogalski. Global behavior of the solutions of Lyness’ difference equation $u_{n+2}u_n = u_{n+1} + a$. *Journal of Difference Equations and Applications*, 10(11):977–1003, 2004. doi: 10.1080/10236190410001728104.
- [4] Elena Celledoni, Robert I. McLachlan, Brynjulf Owren, and G. R. W. Quispel. Geometric properties of Kahan’s method. *Journal of Physics A: Mathematical and Theoretical*, 46(2): 025201, 2013. doi: 10.1088/1751-8113/46/2/025201.
- [5] Krishnendu Chatterjee, Tim Quatmann, Maximilian Schöffeler, Maximilian Weininger, Tobias Winkler, and Daniel Zilken. Fixed point certificates for reachability and expected rewards in MDPs. arXiv:2501.11467, 2025.
- [6] Ventsislav Chonev, Joël Ouaknine, and James Worrell. On the complexity of the orbit problem. *Journal of the ACM*, 63(3):23, 2016. doi: 10.1145/2857050.
- [7] Leonardo de Moura and Sebastian Ullrich. The Lean 4 theorem prover and programming language. In *Automated Deduction – CADE 28*, volume 12699 of *Lecture Notes in Computer Science*, pages 625–635. Springer, 2021. doi: 10.1007/978-3-030-79876-5_37.
- [8] J. J. Duistermaat. *Discrete Integrable Systems: QRT Maps and Elliptic Surfaces*. Springer Monographs in Mathematics. Springer, New York, 2010. ISBN 978-1-4419-7116-6.
- [9] Ryogo Hirota and Kinji Kimura. Discretization of the Euler top. *Journal of the Physical Society of Japan*, 69(3):627–630, 2000. doi: 10.1143/JPSJ.69.627.
- [10] Andrew N. W. Hone. Efficient ECM factorization in parallel with the Lyness map. arXiv:2002.03811, 2020.
- [11] Andrew N. W. Hone. ECM factorization with QRT maps. In *Advances in Software Engineering, Education, and e-Learning*, Transactions on Computational Science and Computational Intelligence. Springer, 2021. doi: 10.1007/978-3-030-70873-3_28. arXiv:2001.09076 (2020).
- [12] Danesh Jogia, John A. G. Roberts, and Franco Vivaldi. An algebraic geometric approach to integrable maps of the plane. *Journal of Physics A: Mathematical and General*, 39(5): 1133–1149, 2006.
- [13] William Kahan. Unconventional numerical methods for trajectory calculations. Unpublished lecture notes, University of California, Berkeley, 1993.
- [14] R. Kannan and R. J. Lipton. Polynomial-time algorithm for the orbit problem. *Journal of the ACM*, 33(4):808–821, 1986. doi: 10.1145/6490.6496.

- [15] Kristin E. Lauter and Katherine E. Stange. The elliptic curve discrete logarithm problem and equivalent hard problems for elliptic divisibility sequences. In *Selected Areas in Cryptography (SAC 2008)*, volume 5381 of *Lecture Notes in Computer Science*, pages 309–327. Springer, 2009. doi: 10.1007/978-3-642-04159-4_20. arXiv:0803.0728.
- [16] Ross M. McConnell, Kurt Mehlhorn, Stefan Näher, and Pascal Schweitzer. Certifying algorithms. *Computer Science Review*, 5(2):119–161, 2011. doi: 10.1016/j.cosrev.2010.09.009.
- [17] Wojciech Nawrocki, Joseph Hua, Mario Carneiro, Yiming Xu, Spencer Woolfson, Shuge Rong, Sina Hazratpour, and Steve Awodey. A certifying proof assistant for synthetic mathematics in Lean. In *Proceedings of the 15th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2026)*. ACM, 2026.
- [18] Yuta Ogura. Structure Computer: certified structure computation for discrete dynamical systems. Companion paper, same site, 2026.
- [19] Matteo Petrera and Yuri B. Suris. On the Hamiltonian structure of Hirota–Kimura discretization of the Euler top. *Mathematische Nachrichten*, 283(11):1654–1663, 2010. doi: 10.1002/mana.200711162. arXiv:0707.4382.
- [20] Matteo Petrera, Andreas Pfadler, and Yuri B. Suris. On integrability of Hirota–Kimura type discretizations. *Regular and Chaotic Dynamics*, 16(3–4):245–289, 2011. doi: 10.1134/S1560354711030051.
- [21] Stephen C. Pohlig and Martin E. Hellman. An improved algorithm for computing logarithms over $\text{GF}(p)$ and its cryptographic significance. *IEEE Transactions on Information Theory*, 24(1):106–110, 1978. doi: 10.1109/TIT.1978.1055817.
- [22] Vaughan R. Pratt. Every prime has a succinct certificate. *SIAM Journal on Computing*, 4(3):214–220, 1975. doi: 10.1137/0204018.
- [23] G. R. W. Quispel, J. A. G. Roberts, and C. J. Thompson. Integrable mappings and soliton equations. *Physics Letters A*, 126(7):419–421, 1988. doi: 10.1016/0375-9601(88)90803-1.
- [24] G. R. W. Quispel, J. A. G. Roberts, and C. J. Thompson. Integrable mappings and soliton equations II. *Physica D*, 34(1–2):183–192, 1989. doi: 10.1016/0167-2789(89)90233-9.
- [25] John A. G. Roberts and Franco Vivaldi. Arithmetical method to detect integrability in maps. *Physical Review Letters*, 90(3):034102, 2003. doi: 10.1103/PhysRevLett.90.034102.
- [26] The mathlib Community. The Lean mathematical library. In *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020)*, pages 367–381. ACM, 2020. doi: 10.1145/3372885.3373824.