はじめに

本書は大沢温泉 (岩手県) にて, 2007 年 8 月 20 日 から 24 日までの 5 日間に渡り, 「種数の高い代数曲線と Abel 多様体」 をテーマに開催された第 15 回 整数論サマースクールの報告です. 本サマースクールには大変大勢の方に参加していただき, 感謝に堪へません. 心より御礼申し上げます.

楕円曲線の非常に深い定理を高い種数の代数曲線やその Jacobi 多様体, さらには Abel 多様体へと一般化するには, ある程度の具体的な計算のできる素材が必要だと思はれますが, その様なことを記述した文献は極めて少ないか, あまり知られてゐない様なので, この企画をいたしました. 内容はいくつかのまとまりになつてゐます:

(1) 前半の吉富さん, 小川さん, 軍司さん, 尾崎さん·梅垣さん, 山内さん, 大西, 中屋敷さんの記事は連続して読まれることを想定してゐます. これらは, 今日, 知られてゐる楕円函数論に匹敵する Abel 函数論の具体的な解説になつてゐると信ずるものです.
(2) 中でも Abel-Jacobi の定理は特に重要なので, 軍司さんの記事と尾崎さん・梅垣さんの記事で, それぞれが別々の方法によりその証明を記述してゐます.
(3) 後半の梅垣さん, 小川さん, 西来路さん, 安田さんの部分は, ある程度の知識をお持ちの方に向けて, それぞれに独立した topics を扱つたものです.
(4) 暗号理論への応用といふ最近の傾向を重視し, 志村さんと松尾さんの記事も連続して読まれることを想定して書かれてゐます.
(5) 小林さんの記事を (1) の部分を参照しながら読んでいただくと, Abel 多様体の抽象論を具体例を踏まへて理解するのに便利なのではないかと思ひます.

このテーマの方面にはもつと具体的な計算をして調べなければならないことが, 非常に多いと思ひます. 本書がこのテーマの方面でその様な研究したいと感じてをられる方にとつて, 参考になつたならこれ以上の喜びはありません.

ただ, 各記事の間には重複してゐることがらがある一方で, 記事と記事の関連に不親切な面もあります. これは時間的制約もありやむを得なかつた面もありますが, 総じて世話人である大西の至らぬ所為です. どうかお許しいただきたく存じます.

講演者の小川さん, 梅垣さん, 軍司さん, 西来路さん, 志村さんはこのスクールの企画当初から, 未熟な世話人を親身になつて支へて下さいました. 本研究集会の講師の旅費の一部を科学研究費補助金 基盤研究 (C) “堅牢なアーベル函数論の構築の研究” (研究代表者 大西) 課題番号 16540002 から支給し, 本報告集の印刷費と郵送費を基盤研究 (B) “概均質ベクトル空間のゼータ関数と保型形式の関連” (研究代表者 佐藤文広先生) 課題番号 16340012 から援助していただきました. 参加者の中で本スクールの開催を陰で支へて下さつた多くの方, これらの方の支へがなかつたら, このスクールは有り得ませんでした. 本当に有難うございました.

2008 年 1 月 20 日
ss2007 世話人, 大西良博/尾台喜孝

第 15 回整数論サマースクール

「種数の高い代数曲線と Abel 多様体」

楕円曲線, 楕円函数については新しくて詳細な多くの文献がありますが, 種数の高い代数曲線について類似のことを例を作って調べたい場合に, 困難を感じたことはありませんか. 最近は, かなり詳しい計算が可能になってきていますが, まとまった文献がないので, 独力での実行は難しいかも知れません. そこで今回のサマースクールでは, どうすれば, 楕円函数, 楕円曲線の場合の様に計算 (自分で例を作るなど) ができるかを中心に話題をしぼりました.

日程　2007 年 8 月 20 日 (月) – 8 月 24 日 (金)
会場　大沢温泉（岩手県花巻市）　`http://www.oosawaonsen.com/`
住所：〒 025-0244　岩手県花巻市湯口字大沢 181　電話：0198-25-2021
世話人　大西 良博 (岩手大学),　尾台 喜孝 (岩手大学)

プログラム

8 月 20 日 (月)

15:30 – 16:10　受け付け
16:30 – 17:00　大西 良博 (岩手大学)
このサマースクール全体の概括
17:10 – 18:00　吉富 賢太郎 (大阪府立大学)
Riemann 面, 代数曲線, 函数体の対応
18:20 – 19:10　小川 裕之 (大阪大学)
Riemann-Roch の定理 – 計算例を中心に – (1)
19:10 – 20:10　夕食
20:20 – 21:10　小川 裕之 (大阪大学)
Riemann-Roch の定理 – 計算例を中心に – (2)

8 月 21 日 (火)

7:30 – 8:50　朝食
9:00 – 9:50　軍司 圭一 (東京大学)
Abel-Jacobi の定理 ([Tata I] の最終章から) (1)
10:10 – 11:00　軍司 圭一 (東京大学)
Abel-Jacobi の定理 ([Tata I] の最終章から) (2)
11:20 – 12:10　尾崎 学 (近畿大学), 梅垣 敦紀 (立教大学)
Abel-Jacobi の定理 ([Iw] から) (1)
12:10 – 13:50　昼食
14:00 – 14:50　尾崎 学 (近畿大学), 梅垣 敦紀 (立教大学)
Abel-Jacobi の定理 ([Iw] から) (2)
15:10 – 16:00　志村 真帆呂 (東海大学)
暗号理論の準備 ([Tata II] 式に因子の加法の計算法)
16:20 – 17:10　山内 卓也 (広島大学)
genus 1 の理論の復習 (ここまでの話しと対応させて) (1)
17:30 – 18:20　山内 卓也 (広島大学)
genus 1 の理論の復習 (ここまでの話しと対応させて) (2)
18:30 – 19:30　夕食

8 月 22 日 (水)

7:30 – 8:50	朝食
9:00 – 9:50	大西 良博 (岩手大学) 高種数の場合の sigma 函数と $\wp$ 函数
10:10 – 11:00	大西 良博 (岩手大学) Jacobi 多様体の具体的な定義方程式とそれに対応する加法公式
11:20 – 12:10	難波 誠 (追手門学院大学) Inversions of abelian integrals
12:20 –	昼食 午後は自由時間
18:00 –	懇親会

8 月 23 日 (木)

7:30 – 8:50	朝食
9:00 – 9:50	梅垣 敦紀 (立教大学) CM 型の種数 2 の代数曲線とアーベル曲面
10:10 – 11:00	松尾 和人 (中央大学) 代数曲線暗号とその安全性
11:20 – 12:10	小川 裕之 (大阪大学) アーベル多様体の有理等分点について
12:10 – 13:50	昼食
14:00 – 14:50	小林 真一 (名古屋大学) Algebraic theory via schemes ([AV] から) (1)
15:10 – 16:00	小林 真一 (名古屋大学) Algebraic theory via schemes ([AV] から) (2)
16:20 – 17:10	西来路 文朗 (広島国際大学) 超楕円曲線のヤコビ多様体の形式群 (1)
17:30 – 18:20	西来路 文朗 (広島国際大学) 超楕円曲線のヤコビ多様体の形式群 (2)
18:30 – 19:30	夕食

8 月 24 日 (金)

7:30 – 8:50	朝食
9:00 – 9:50	中屋敷 厚 (九州大学) シグマ関数の代数的表示
10:10 – 11:00	安田 正大 (京都大学) アーベル多様体の Birch Swinnerton-Dyer 予想についての話題 (1)
11:20 – 12:10	安田 正大 (京都大学) アーベル多様体の Birch Swinnerton-Dyer 予想についての話題 (2)
12:20 –	昼食 , 解散

(注) 文献表

[Iw]	岩澤 健吉 : 代数函数論
[Tata I]	D. Mumford : Tata lectures on theta I
[Tata II]	D. Mumford : Tata lectures on theta II
[AV]	D. Mumford : Abelian varieties

参加者一覧 (所属は参加当時のもの)

青木 宏樹 (東京理科大学)
天野 勝利 (日本工業大学)
飯島 努 (中央大学)
石井 卓 (千葉工業大学)
石毛 利昌 (千葉大学)
伊東 杏希子 (名古屋大学院)
伊吹山 知義 (大阪大学)
井原 健太郎 (大阪大学)
市原 由美子 (広島大学)
内田 幸寛 (名古屋大学大学院)
内海 和樹 (広島大学大学院)
梅垣 敦紀 (立教大学)
江上 繁樹 (富山大学)
太田 雄介 (上智大学大学院)
大坪 紀之 (千葉大学)
大西 良博 (岩手大学)
大場 彦浄 (東北大学大学院)
岡崎 武生 (京都大学)
岡野 恵司 (早稲田大学)
岡本 亮彦 (早稲田大学院)
小川 裕之 (大阪大学)
萩原 啓 (東京大学)
尾崎 学 (近畿大学)
小澤 信太郎 (中央大学院)
尾台 喜孝 (岩手大学)
小野寺 一浩 (慶應義塾大学院)

加川 貴章 (立命館大学)
加塩 朋和 (京都大学)
金子 元 (京都大学)
川島 誠 (大阪府立大学)
河本 史紀 (学習院大学)
金城 謙作 (東北大学大学院)
倉繁 章 (上智大学院)
軍司 圭一 (東京大学大学院)
幸田 英希 (早稲田大学院)
児島 道隆 (早稲田大学院)
後藤 丈志 (東京理科大学)
小林 真一 (名古屋大学)
小牟田 綾 (大阪府立大学)
小松 亨 (上智大学)
今野 大悟 (東北大学大学院)

齋藤 恆和 (早稲田大学)
西来路 文朗 (広島国際大学)
酒井 祐貴子 (早稲田大学)
坂田 裕 (早稲田大学)
佐藤 篤 (東北大学院)
佐藤 文広 (立教大学)
志賀 元明 (東北大学)
志村 真帆呂 (東海大学)
鈴木 譲 (大阪大学)
鈴木 良雄 (千葉大学院)
須田 智彦 (北海道大学)
諏訪 紀幸 (中央大学)
曽根 寿久 (名古屋大学院)

高橋 直樹 (東北大学院)
竹本 隆 (九州大学院)
田谷 久雄 (宮城教育大学)
趙 晋輝 (中央大学)
対馬 龍司 (明治大学)
土屋 和由 (株式会社光電製作所)
津野 祐司 (中央大学)
角皆 宏 (上智大学)
富永 健介 (広島大学)

中屋敷 厚 (九州大学院)
並川 健一 (大阪大学院)
難波 誠 (追手門学院大学)
西村 直人 (大阪大学院)

長谷川 武博 (都留文科大学)
原 隆 (東京大学大学院)
坂内 健一 (名古屋大学大学院)
平之内 俊郎 (九州大学)
広中 由美子 (早稲田大学)
星 明考 (早稲田大学)

松尾 和人 (情報セキュリティ大学院大学)
松波 周一 (北海道大学院)
南出 大樹 (神戸大学院)
宮坂 宥憲 (東北大学院)
宮崎 直 (東京大学大学院)
村上 弘 (首都大学東京)
水澤 靖 (東京理科大学)
百瀬 文之 (中央大学院)

安田 正大 (京都大学)
谷戸 光昭 (神奈川工科大学・明星大学)
山内 卓也 (広島大学)
山上 敦士 (京都産業大学)
山崎 義徳 (九州大学大学院)
山田 智宏 (京都大学院)
山田 裕二 (立教大学)
吉冨 賢太郎 (大阪府立大学)
吉村 俊介 (大阪府立大学)

若林 功 (成蹊大学)
若林 徳子 (近畿大学大学院)

目 次

第 15 回 整数論サマースクール 報告集, pp.1-13

リーマン面と代数曲線

吉冨 賢太郎*

1 リーマン面

1.1 定義

まず, 正則性と調和性について復習しておく.

定義 1.1. $\boldsymbol{C}$ (の開集合) 上の複素数値函数 $f = u + iv$ で, 定義されている各点で微分可能なものを正則函数という (ただし, u, v は f の実部・虚部). 正則な 1 対 1 写像を等角写像という. f が正則ならば コーシーリーマンの関係式

$$\frac{\partial f}{\partial x} = -i\frac{\partial f}{\partial x} \iff \frac{\partial u}{\partial x} = \frac{\partial v}{\partial y}, \quad \frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x}.$$

を満たす. さらに, u, v は $\Delta u = \Delta v = 0$ をみたす (ただし, $\Delta f = \dfrac{\partial^2 f}{\partial x^2} + \dfrac{\partial^2 f}{\partial y^2}$). 一般に, $\Delta u = 0$ を満たす実数値函数を調和函数という. $\overline{u}$ が正則のとき, u は反正則という.

リーマン面とは 1 次元の複素解析多様体であるが, 以下に再定義しておく.

定義 1.2. 位相空間 S において, 次の条件をみたす族 $\mathcal{A}$ のことを S の上の等角構造という.

(i) $\mathcal{A}$ の元 ϕ は S の開集合 U_ϕ から $\boldsymbol{C}$ の開集合への位相同型である.

(ii) $\cup_{\phi\in\mathcal{A}} U_\phi = S$.

(iii) $U_\phi \cap U_\psi \neq \emptyset$ ならば $\psi \circ \phi^{-1}$ は $\phi(U_\phi \cap U_\psi)$ から $\psi(U_\phi \cap U_\psi)$ への全射等角写像である.

(iv) S の開集合 U_ψ から $\boldsymbol{C}$ の開集合への位相同型 ψ で $U_\phi \cap U_\psi \neq \emptyset$ であるようなすべての $\phi \in \mathcal{A}$ に対して (iii) をみたすならば $\psi \in \mathcal{A}$ である (極大性).

注: ここでは境界つきリーマン面は除外して考える.

定義 1.3. 連結 *Hausdorff* 空間 S とその上の等角構造 $\mathcal{A}$ からなる対 $R = (S, \mathcal{A})$ のことをリーマン面という. $\mathcal{A}$ の元 ϕ を局所座標 (*local coordinate*), S を基底空間という. ここでは, S は基底空間を表わすのに用い, R と書いたときはリーマン面の構造も含め考えているものとする.

*大阪府立大学 総合教育研究機構

リーマン面 R の基底空間の部分集合 U が連結開集合のとき, U は相対位相で連結 Hausdorff であり, R の等角構造から誘導される等角構造が入る. これを R の領域という.

S がコンパクトのとき $R = (S, \mathcal{A})$ を閉 (closed) リーマン面といい, そうでないとき開 (open) リーマン面という. 射影的で滑らかな完備代数曲線 (complete projective smooth algebraic curve) は閉リーマン面と対応する (cf. §2).

リーマン面は複素 1 次元であるから' 面' である. ただし, ' 面' とはここでは可算基底を持つ連結な二次元位相多様体を言う (リーマン面の基底空間には連結を仮定している).

可算基底とは, 可算個の開集合の族で任意の開集合がこの族の和集合として表わせるようなものを言う. このような基底があるときこの空間は countable (第 2 可算公理をみたす) という.

次が成り立つ.

定理 1.1. リーマン面は可算基底を持つ. また, リーマン面には三角形分割が存在し, 向きづけ可能である.

したがって, リーマン面は実際この意味で "面" であり, 向きづけ可能である (したがって, メビウスの帯にはリーマン面の構造は入らないことがわかる). また逆に閉リーマン面について次が成り立つ ([1] 定理 4.9).

定理 1.2. コンパクト *Hausdorff* 位相空間 S があるリーマン面 R の基底空間となるためには S が向きづけ可能な閉曲面であることが必要十分である.

リーマン面の三角形分割より得られる複体のオイラー数を χ とする. すなわち, 三角形の数を n_2, 辺の数を n_1, 頂点の数を n_0 とするとき, $\chi = n_2 - n_1 + n_0$ であたえられるものである. このとき, $\chi = 2 - 2g$ によって定まる g をリーマン面の種数という. コンパクト (可算) 向きづけ可能な 2 次元位相多様体の同相類は種数によって決まる.

リーマン球面の場合は $g = 0$, 楕円曲線は $g = 1$ である. 直感的には "穴の数" となるが, これは標準切断によって説明される (後述 cf.1.6).

リーマン面の例をいくつか (証明なしに) あげる.

例 1.1. 複素平面全体は開リーマン面である. また, 複素平面内の開円板も開リーマン面である. 球面 S^2 は $\boldsymbol{C} \cup \{\infty\}$ と位相同型であり (cf. [5]), 局所座標の近傍として, $U_0 = \boldsymbol{C}^2, U_\infty = \boldsymbol{C}^2 \setminus \{0\} \cup \{\infty\}$ をとり, $\phi_0(z) = z$, $\phi_\infty(z) = 1/z$ とすることにより等角構造が入る. このようにして得られるリーマン面をリーマン球面と呼び, $\boldsymbol{P}^1$ または $\boldsymbol{P}^1(\boldsymbol{C})$ で表す.

例 1.2. 複素平面 $\boldsymbol{C}$ の格子 $L = \{m_1\omega_1 + m_2\omega_2 | m_1, m_2 \in \boldsymbol{Z}\}$ による商空間はトーラス ("一人乗り浮き輪") と見なせ自然にリーマン面の構造が入る. これは, 楕円函数の基本領域であり, 楕円曲線と言われる代数曲線 E の $\boldsymbol{C}$ 値点全体 $E(\boldsymbol{C})$ と同一視される. この同一視 *(*同型*)* はワイエルシュトラスの $\mathscr{P}$ 函数とその微分によって与えられる.

この他にも, 上半平面の合同部分群による商空間などがある. 一般に既存のリーマン面からリーマン面を構成する方法として, 貼り合わせ, 被覆リーマン面, 等角写像の不連続群 (離散群) による商空間, などの手法がある (cf. [2] pp.46).

1.2 解析写像

リーマン面の間の写像については以下のように定義する.

定義 1.4. 2 つのリーマン面 R, R' の間の写像 $f : R \to R'$ は $z \in R$ のまわりの局所座標 U_ϕ と $f(z) \in R'$ のまわりの局所座標 V_ψ に対して, $\psi(f(\phi^{-1}(x)))$ が $x = 0$ の近傍で正則であるとき解析写像という. 全単射な解析写像を同型写像 (または等角同値) という. R と R' の間に同型写像が存在するとき, R と R' は同型であるといい, $R \cong R'$ と記す.

リーマン面の間の写像の性質を考えるのに, 局所変数 (local parameter) を考えるのが便利である. これは, 後述の解析写像の分岐指数や解析函数の位数を定義するのに便利である.

定義 1.5. リーマン面 R の領域 U から $\boldsymbol{C}$ の領域 U' への全単射解析写像 f が存在するとき, U を R の解析的領域と呼び,

$$f(z) = t = x + iy$$

によって与えられる $t = f(z)$ を U における解析的変数, $(x(z), y(z))$ を解析的座標とよぶ. 特に U が 点 z_0 の近傍で $f(z_0) = 0 \in \boldsymbol{C}$ となるように正規化されているとき, t を z_0 のまわりの局所変数という.

例 1.3. $R = \boldsymbol{P}^1$ の場合, $z_0 \in \boldsymbol{C}$ ならば, $f(z) = z - z_0$, $z_0 = \infty$ ならば $f(z) = 1/z$ とすればこれは $\boldsymbol{P}^1$ の局所座標 (局所変数) を与える.

解析写像について次が成り立つ.

定理 1.3. リーマン面 R から R' への写像 f が点 z において解析的であるとする. z と $z' = f(z)$ における局所変数 t, t' を適当にとると z の近傍で

$$t' = f(t) \equiv 0 \qquad or \qquad t' = f(t) = t^n \quad (n \geqq 1)$$

とできる. $t' = t^n$ となるとき, n は局所定数のとりかたによらず, f の z における分岐指数という. $n > 1$ ならば z は分岐点, $n = 1$ ならば不分岐点と呼ばれる.

また, 上の定理から次が言える.

定理 1.4. リーマン面 R の領域 U からリーマン面 R' への解析写像 f に対し, $f(U)$ は一点であるかまたは R' の領域である. 特に f が R の一点 z_0 の近傍で一定の値 $w_0 \in R'$ をとるならば f は U 上で一定, すなわち $f(z) = w_0$ である.

1.3 被覆リーマン面と基本群

定義 1.6. 連結 n 次元多様体 S' から連結 n 次元多様体 S の上への写像 f が次の条件をみたすとき S' を S の被覆多様体, f をその被覆写像 (*covering map*) という. 即ち: S の各点 P に対し ある P の近傍 U が存在して $f^{-1}(U)$ の各連結成分への f への制限は位相同型写像になる.

被覆多様体を $S' \overset{f}{\twoheadrightarrow} S$ などと表わす. 2 つの被覆多様体 $S'_1 \overset{f_1}{\twoheadrightarrow} S_1$, $S'_2 \overset{f_2}{\twoheadrightarrow} S_2$ は位相同型 $g' : S'_1 \to S'_2$ と $g : S_1 \to S_2$ が存在して $g' \circ f_2 = f_1 \circ g$ をみたすとき同型であるという. ただし, $S_1 = S_2$ のときは, g としては恒等写像と定める. このときは g' を同型写像と呼ぶ. さらに $S'_1 = S'_2 = S'$, $f'_1 = f'_2 = f'$ のとき, g' は自己同型写像で, これら全体は S' の位相変換群をなす. これを $S' \overset{f}{\twoheadrightarrow} S$ の自己同型群とよび $A(S' \overset{f}{\twoheadrightarrow} S)$ と書く.

任意の位相多様体 S は自明な被覆多様体 $S \overset{\mathrm{Id}_S}{\twoheadrightarrow} S$ をもつ. これ以外に被覆多様体を持たないとき, S は単連結であるという. S の被覆多様体には必ず単連結なものが存在し, 同型を除いて一意的に定まる. その一つを $S^* \overset{f^*}{\twoheadrightarrow} S$ とするとき, $G = A(S^* \overset{f^*}{\twoheadrightarrow} S)$ を S の基本群という.

P^* を S^* の点とすると, 適当な P^* の近傍 U^* をとると, G の異なる 2 つの元 g, g' に対して $g(U^*) \cap g'(U^*) = \emptyset$ とできる. したがって, G の元は忠実に作用する. また, このような変換群を不連続変換群という. S^* の任意の不連続変換群はある S の S^* に関する基本群となる. S として, G による S^* の商空間 $S^*(G) = G\backslash S^*$ を考えればよい

補題 1.1. 連結多様体 S の単連結被覆多様体を S^* とし, $S^* \overset{f^*}{\twoheadrightarrow} S$ の基本群を G とすれば S^* の点 P^*, Q^* が G に関して同値であるためには, $f^*(P^*) = f^*(Q^*)$ であることが必要十分であり, $Q^* = g(P^*)$ となる $g \in G$ が一意的に存在する. これにより $S^*(G)$ と S は同相になる. また, G_1, G_2 を不連続群とするとき, $S^*(G_1)$ と $S^*(G_2)$ が同相であるためには, G_1, G_2 が共役であることが必要十分である.

また, G の部分群 H に被覆多様体 $S^*(H)$ が対応し, $S^*(H_1) \cong S^*(H_2) \leftrightarrow H_1$ と H_2が共役などガロア理論と類似のことが成り立つ.

S の上の単連結被覆多様体は, S の道 (曲線) のホモトピー類の全体のなす群を考えることによってうる. すなわち, $I = [t_0, t_1]$ を $\boldsymbol{R}$ の閉区間とする. $\gamma : I \to X$ を X における道とよぶ. $\gamma(t_0)$ を始点, $\gamma(t_1)$ を終点という. また, 始点と終点が同じときループまたは閉曲線といい, そうでないと開曲線という. 道 γ, γ' を' つなげたもの' を $\gamma\gamma'$ と書いて積を定義する. 点 P_0 を基点とする曲線のホモトピークラス $[\gamma]$ 全体は群をなし, P_0 によらず同型である. これもよく知られた基本群の定義である. 基本群の元 $[\gamma]$ に対しその終点を対応させることにより, 被覆多様体 S^* をうる.

次にリーマン面の場合に考えると

定理 1.5. 被覆多様体 $S' \overset{f'}{\twoheadrightarrow} S$ において S があるリーマン面 R の基底空間のとき, S' にも f' が解析写像となるようなリーマン面の構造が入り, リーマン面 R' の基底空間となる.

このとき, R' を R の被覆リーマン面という. 被覆多様体の同型や自己同型群などは位相写像のかわりに解析写像として同様に定義される. このようにして (閉) リーマン面を分類するには単連結リーマン面を考え, その自己同型群の不連続部分群の共役類を求め, その代表系に対応するリーマン面を考えればよいことがわかる.

而して, リーマン面は以下のように分類される.

定理 1.6. リーマン面 R は以下のいずれかと同型である. それぞれ, 普遍被覆リーマン面が 楕円型, 放物型, 双曲型であるという.

(1) 複素球面 $\boldsymbol{P}^1(\boldsymbol{C})$
(2) 複素平面 $\boldsymbol{C}$ を被覆リーマン面とする以下のもの.
(2-1) $\boldsymbol{C} = \boldsymbol{P}^1(\boldsymbol{C}) \setminus \{\infty\}$
(2-2) $\boldsymbol{C} \setminus \{0\} = \boldsymbol{P}^1(\boldsymbol{C}) \setminus \{0, \infty\}$
(2-3) $\boldsymbol{C}/L$, L は 2 次元格子群 $\boldsymbol{Z}\omega_1 + \boldsymbol{Z}\omega_2$, $\omega_1/\omega_2 \in \boldsymbol{H}$.
(3) 上半平面 $\boldsymbol{H}$ を合同部分群でわったもの.

注: (2-3) は楕円曲線である.
注: (3) はモジュラー曲線などがその典型的な例である.

上の分類から, 閉リーマン面となるのは, リーマン球面か, 楕円曲線, もしくは, 上半平面の一次分数変換群の離散部分群による商空間 (のコンパクト化) となる. これらの基本領域を考えると, 最初の 2 つについては明白であり, 楕円曲線の場合は格子の内部と接する辺が基本領域となる. この場合, 後述の標準切断はこの 2 本の辺の像である閉曲線によるものである. 一方, (3) の場合も基本領域は 2n 角形になることがわかり, 基本群の元は, この基本領域 Ω の各辺をとなりあう基本領域の接しない 1 辺に写すただ一つの変換によって生成されることがわかる.

上の定理から実際リーマン面が三角形分割可能であることがわかるが, この三角形を貼り合わせてえられる凸多角形が $2g$ 角形になる. ここで, g は種数である. 一般に次が成り立つ.

定理 1.7. 連結な 2 次元位相多様体は 2 辺ずつ組になった正 $2n$ 角形の辺を次の文字の列に従って同一視したものと同相である.
(1) aa^{-1}
(2) $a_1b_1a_1^{-1}b_1^{-1}a_2b_2a_2^{-1}b_2^{-1}\cdots a_hb_ha_h^{-1}b_h^{-1}$
(3) $a_1a_1a_2a_2\cdots a_ha_h$.
ただし, 向きづけ可能な場合は (1), (2) の場合である.

リーマン面は向きづけ可能であるから, リーマン球面と位相同型でなければ, (2) のような変形で得られることになる. 逆に;

定理 1.8. 球面と同相でない向きづけ可能なリーマン面 R には次の性質を持った単純閉曲線 $\alpha_k, \beta_k, \quad k = 1, \ldots g$ が存在する. すなわち, これらは基点 P_0 を持ち, 任意の 2 つは P_0 以外に共通を持たず, さらに $4g$ 角形から上の (2) の形の接着を行なって得られる面と同相であり, 接着された a_k, b_k に対応する曲線の像が α_k, β_k $(k = 1, \ldots, p)$ となる.

この定理の α_k, β_k を P_0 を基点とする S の標準切断という. なお, 標準切断の交差の仕方は 2 通りあるが, どちらにとるかは [4] を参照されたい. 交点数などの説明もこの稿では割愛する.

標準切断によって基本群は生成される. すなわち次が成り立つ.

定理 1.9. 球面と位相同型ではない向きづけ可能なコンパクトな面 S の点 P_0 を基点とする標準切断を $\alpha_1, \beta_1, \ldots, \alpha_g, \beta_g$ とする. このとき, 基本群 $\pi_1(S, P_0)$ は標準切断のホモト

ピー類 $[\alpha_k], [\beta_k]$ $(k = 1, \ldots, g)$ によって生成され基本関係 $\prod_{k=1}^{g} [\alpha_k][\beta_k][\alpha_k]^{-1}[\beta_k]^{-1} = 1$ が成り立つ.

前述のように g は種数であり, これを種数の定義とすることができる. 即ち :

定義 1.7. (種数の再定義) 上の標準切断で定まる g を R もしくは基底空間 S の種数という. g は S の位相不変量であるが, さらに, g によって 2 次元位相多様体としての同型類が完全に定まる.

これで種数がいわゆる穴の数であることが幾何的に明確になった. 種数が標準切断や三角形分割によらないことは, Betti 数 $(= 2g)$ や (調和 or 正則) 微分形式の空間の次元などが種数によって表わされる $(= 2g$ or g となる) ことから実際わかる.

このようにして, 閉リーマン面の基底空間の位相不変量である種数が定まるが, 種数 1 以上の面に対してリーマン面の同型類は無限に存在することが知られる. すなわち, 解析構造が入ることによって, リーマン面は確かに"ただの面"でないのである (種数 0 のリーマン面はすべてリーマン球面にリーマン面として同型である).

1.4 解析函数と微分形式

定義 1.8. リーマン面 R に対し, R から $\boldsymbol{P}^1$ への解析写像を解析函数と呼ぶ. 解析函数全体は体をなすがこれを $K(R)$ で表わし, R の解析函数体という. $f \in K(R)$ が $f(z) \neq \infty$ のとき, f は z で正則であるという. すなわち, $z \in U_\phi$ であるような局所座標 ϕ に対して, $f \circ \phi^{-1}$ が点 $\phi(z)$ で正則であることである.

解析函数 (正則函数) と同様に R 上の調和函数も同様に定義される. u が調和函数のとき, コーシーリーマンの関係式を満たすような調和函数 v が定数を除いて定まる. これを共役といい, u^* であらわす.

リーマン面 R 上の正則函数や調和函数についても複素平面上と同様の次のようなことが成り立つ.

定理 1.10 (除去可能性定理). R の点 z に対し, f を $R - \{z\}$ 上の正則 (調和) 函数とする. もし, ある近傍 U で f が $U - \{z\}$ で有界となるものが存在するならば, f は R 上の正則 (調和) 函数に拡張できる.

定理 1.11 (最大値の原理). リーマン面 R 上の正則 (調和) 函数 f の絶対値がある点において最大値をとるならば f が定数値函数である. 特に閉リーマン面上の正則函数は定数しかない.

注: 開リーマン面のときは, 必ず非定値の正則函数が存在する (cf. [2] p.11).

定理 1.12 (一致の定理). リーマン面 R 上の正則函数 f, g が R 上の収束点列 (または集積点を持つ点列) $\{p_n\}$ に対して $f(p_n) = g(p_n)$ をみたすならば, $f = g$ である.

定理 1.13. 正則函数列 $\{f_n\}$ が R 上の函数 f にコンパクト一様収束するならば, f は正則である.

定義 1.9. R 上の解析函数 f の $z_0 \in R$ における位数を以下のように定義する. z_0 における局所変数を t として, $a_0 = f(z_0) \neq \infty$ のとき、$f(z) - a_0 = a_1 t + a_2 t^2 + \cdots, a_0 = f(z_0)$ となる. このとき, $a_j \neq 0$ となる最小の j を f の $z = z_0$ における位数といい, $\nu_{z_0}(f)$ で表わす. ただし, 恒等的に 0 のときは ∞ と定める. また, $a_0 = \infty$ のときは, $\dfrac{1}{f(z)} = a_1 t + a_2 t^2 + \cdots \neq 0$ となる. $a_j \neq 0$ となる最小の j を m とするとき, $\nu_{z_0}(f) = -m$ とかき, m 位の極を持つという.

次に微分形式を定義しよう. 微分形式は不変形式とも言い, リーマン面上での積分をする場合に函数のかわりに必要となるものである.

函数のかわりになぜ不変形式を考えるか理由を述べておく. $z = z_0, w = w_0 = \psi(\phi^{-1}(z_0))$ において

$$\frac{d}{dz} f(\phi^{-1}(z)) = \frac{d}{dw} f(\psi^{-1}(w)) \cdot \frac{dw}{dz}$$

が成り立つから, 函数の微分係数は局所座標に依存する. そこで, 代わりに微分形式を考えるのである.

リーマン面 R においてすべての局所座標 $\phi \in \mathcal{A}$ に $\phi(U_\phi)$ で定義された複素数値函数 a_ϕ, b_ϕ を対応させる. この対応 $\omega : \phi \mapsto (a_\phi, b_\phi)$ で, $U_\phi \cap U_\psi \neq \emptyset$ であるような ϕ, ψ に対して

$$a_\phi(z) = a_\psi(\psi(\phi^{-1}(z)))(\psi \circ \phi^{-1})'(z)$$

$$b_\phi(z) = a_\psi(\psi(\phi^{-1}(z)))\overline{(\psi \circ \phi^{-1})'(z)}$$

が成り立つものを 1 位微分形式 (1-form) といい, $\omega = a dz + b\overline{dz}$ で表わす. $b_\phi \equiv 0$ となるもの正則微分形式という. すなわち $\omega = a dz$ が正則微分である. f が正則函数のとき, $a_\phi(z) = (f \circ \phi^{-1})'(z)$, $b_\phi \equiv 0$ で定義すればこれは 1-form になる. これを f の微分といい, df で表わす. R 上の C^1 級函数に対しても同様に du が定義され, $du = \dfrac{\partial u}{\partial z} dz + \dfrac{\partial u}{\partial \overline{z}} \overline{dz}$ となる. f が正則ならば df も正則微分形式である.

ω を 1-form として, 複素共役 $\overline{\omega}$ を $\phi \mapsto (\overline{b_\phi}, \overline{a_\phi})$ によって定まるものと定義する. $\mathrm{Re}\,\omega = \dfrac{1}{2}(\omega + \overline{\omega})$, $\mathrm{Im}\,\omega = \dfrac{1}{2i}(\omega - \overline{\omega})$ を ω の実部・虚部という. $\overline{\omega} = \overline{b} dz + \overline{a}\overline{dz}$ である. ${}^*\omega = -ia dz + ib\overline{dz}$ とおいて, ω の共役という. 1-form ω で 正則微分 ω_1, ω_2 によって $\omega = \omega_1 + \overline{\omega_2}$ とかけるものを調和微分という. u が調和函数ならば $du + i\,{}^*du = 2\dfrac{\partial u}{\partial z} = \left(\dfrac{\partial u}{\partial x} - i\dfrac{\partial u}{\partial y}\right) dz$ も正則微分である.

正則微分 $a dz$ の零点と位数は $a = \{a_\phi\}_{\phi \in \mathcal{A}}$ の零点と位数として局所座標のとり方によらず定まる.

また, a が有理型函数であるとき, (すなわち, a_ϕ が有理型函数であるとき), $\omega = a dz$ を有理型微分という. ω の極とその位数も同様に定義される. また留数も局所座標に依らない数として同様に定義することができ, ω の z における留数を $\mathrm{Res}(\omega, z)$, $z \in R$ のように

表わす. 複素平面の領域 D 上では有理型函数と有理型微分, 正則函数と正則微分は同一視して考えられる.

有理型函数 f と有理型微分 ω の積 $f\omega$ は有理型微分である. 局所座標での商をはりあわせることによって有理型函数 ω_1/ω_2 が定義される.

例 1.4. $\boldsymbol{P}^1(\boldsymbol{C})$ の領域 D で $\infty \in D$ のときを考える. 局所座標として, $U_0 = (D\backslash\{\infty\}, \phi_0 = Id)$ と $U_\infty = (D \setminus \{0\}, \zeta = \phi_\infty : z \mapsto 1/z)$ がとれる. $\omega = a\ dz$ を正則微分とする. $f = a_{\phi_0}$ は正則函数であるが, $U_0 \cap U_\infty$ 上 $f(z) = a_{\phi_0}(z) = a_{\phi_\infty}(\zeta(z))\dfrac{d\zeta}{dz} = -a_{\phi_\infty}\left(\dfrac{1}{z}\right)\dfrac{1}{z^2}$ となり, ∞ におけるローラン展開は $f(z) = \dfrac{c_2}{z^2} + \dfrac{c_3}{z^3} + \cdots$, となる. つまり, 2 位の零点を持つ. 逆に ∞ で 2 位の零点を持つような函数 f に正則微分が対応するのでこれらを同一視することができる.

有理型微分のことを Abel 微分ともいう. また, 正則なものを第 1 種微分 (DFK, differential of first kind), 正則でなく 極における留数が 0 のものを第 2 種微分 (DSK), その他を第 3 種微分 (DTK) などとも呼ぶ. ただし, これらの定義は文献や他の講演によって違うので注意されたい.

以下のような問題を考える.

問題 R の疎な点 $p_1, \ldots, p_m$ と各点 p_n における主要部が与えられたときに $\{p_n\}$ 以外で正則で, $\{p_n\}$ で与えられた主要部を持つような有理型 (解析) 函数または有理型微分が存在するか.

これについていくつかの定理を述べておく ([1] pp. 170-171).

定理 1.14. z_1, z_2 を リーマン面 R の異なる 2 点とする. z_1 において 1 位の零点を持ち, z_2 において 1 位の極を持つ解析函数 $f \in K(R)$ が存在する.

定理 1.15. z をリーマン面 R の任意の点とするとき, z において $n(\geq 2)$ 位の極を持ち, 他では正則な R の微分形式 $\omega_{z,m}$ が存在する.

定理 1.14 の応用として次が成り立つ.

定理 1.16. リーマン面 R, R' の基底空間 S, S' の間の写像 $f : S \to S'$ が R' 上の解析函数から R 上の解析函数を誘導するならば, f は解析写像である.

これより, 2 つのリーマン面の同型について次が成り立つ.

定理 1.17. R, R' をリーマン面, S, S' をそれぞれの基底空間とする. $f : S \to S'$ が全単射で f により $f^{\#}K(R') \ni g' \mapsto g \in K(R)$ を $g(z) = g(f(z))$ で定めるとき, $f^{\#}$ が同型を与えるならば R, R' は同型である.

また, 閉リーマン面については次が成り立つ.

定理 1.18. R, R' を閉リーマン面とする. $K(R) \cong K(R')$ ならば, $R \cong R'$ である.

すなわち閉リーマン面の場合には 函数体が同型であれば対応するリーマン面も同型である. このことは次節で解説する.

また, 閉リーマン面 R 上では, R の異なる 2 点 z_1, z_2 に対して z_1, z_2 以外で正則で, z_1 に留数 1 の 1 位の極, z_2 に留数 -1 の 1 位の極を持ち, Re ω_{z_1,z_2} は z_1, z_2 の外で完全となるような微分形式 ω_{z_1,z_2} が存在することが知られる. 一方一般のリーマン面上の微分形式について次が知られている ([2] p.121):

定理 1.19. リーマン面 R において, 任意に与えられた有限個の点で, 任意に与えられた局所座標に対し, 任意に与えられた主要部 (ただし, 閉リーマン面のときは留数の和が 0) の極を持ち, 他では正則な有理型微分が存在する.

1.5 その他の微分形式と外微分

定義 1.10. リーマン面 S において, 各局所座標 ϕ に対し $\phi(U_\phi)$ 上の複素数値函数 c_ϕ を対応させる対応 $\Omega : \phi \mapsto c_\phi$ で

$$c_\phi(z) = c_\psi(\psi(\phi^{-1}(z)))|(\psi \circ \phi^{-1})'(z)|^2$$

が $z \in \phi(U_\phi \cap U_\psi)$ に対して成り立つとき, S の 2 位微分形式または *2-form* という.

2-form Ω を $c|dz|^2$, $cdz\overline{dz}$, $c\ dx\ dy$, $cdx \wedge dy$, $\dfrac{i}{2}cdz \wedge \overline{dz}$ などと表わす.

1-form のなすベクトル空間の外積代数を考えて 2-form は 次数 2 部分加群に属すると考えられる. すなわち, 2-form の表示式の最後の 2 つの $\wedge$ は外積を表わしその意味で等しい. 実際, $dz \wedge \overline{dz} = (dx + idy) \wedge (dx - idy) = -2idx \wedge dy$ となる.

一般に 1-form $\omega_j = a_j dz + b_j \overline{dz}$, j = 1, 2 に対して $\omega_1 \wedge \omega_2$ を 2-form $(a_1 b_2 - a_2 b_1) dz \wedge \overline{dz}$ で定義し, ω_1 と ω_2 の外積という.

また, ω の外微分 $d\omega$ を

$$d\omega = \left(\frac{\partial b}{\partial z} - \frac{\partial a}{\partial \bar{z}} \right) dz \wedge \overline{dz}.$$

で定義する. これは, $\omega = adz + b\overline{dz}$ のとき $d\omega = da \wedge dz + db \wedge \overline{dz}$ と定義してもよい. ω が正則微分ならば, $d\omega = 0$ である.

1.6 アーベル積分

区分的に解析的な曲線とは, 解析的な曲線 (C^1 級) の有限個の積をいう. 次のような性質で特徴づけられる微分形式が区分的に解析的な曲線 α に対して一意的に定まることが証明される (cf. [2] p.143).

定理 1.20. α を閉リーマン面 R 上の区分的に解析的な曲線とする. α に対して以下の性質を持つ R 上の微分形式 ω'_α が一意的に定まる.
(1) α が閉曲線のとき, ω'_α は R で正則で R 上の任意の閉形式 ω に対し,

$$\int_S (\mathrm{Re}\, \omega'_\alpha) \wedge \omega = 2\pi \int_\alpha \omega.$$

(2) α が開曲線のとき, ω'_α は α の始点 z_0 に留数 i の *1* 位の極, z_1 に留数 $-i$ の *1* 位の極を持ち, $R\setminus\{z_0,z_1\}$ で正則であり, R 上の任意の閉形式 ω に対し, 上の積分等式をみたす.

リーマン面 R 上のなめらかな曲線 γ とこの曲線上で連続な 1-form ω があるとき, ω の γ に沿う積分が定義される (アーベル積分). ω が第 1 種 (第 2 種, 第 3 種) であるにしたがってこのアーベル積分も第 1 種 (第 2 種, 第 3 種) であるという.

区分的になめらかな曲線に対しても積分が定義される. γ を覆う局所座標近傍を考えて γ を分割し, $\displaystyle\int_{\phi_j\circ\gamma}\left(a_{\phi_j}dz+b_{\phi_j}\overline{dz}\right)$ の和とすればよい.

定義 1.11. R 上の *1-form* ω は R で C^1 級のある函数 u に対して $\omega=du$ となるとき, 完全であるという. また, C^1-級 *1-form* ω は $d\omega=0$ をみたすとき, 閉形式 (*closed form*) であるという.

定理 1.21. R 上の連続な *1-form* に対して以下は同値.
(1) 完全形式である.
(2) 始点・終点が同じ任意の *2* つの曲線 γ_0,γ_1 に対し $\displaystyle\int_{\gamma_0}\omega=\int_{\gamma_1}\omega$ である.
(3) 区分的になめらかな任意のループ γ に対し $\displaystyle\int_\gamma\omega=0$.

$d(du)=0$ より, 完全形式は閉形式である. 逆は一般には成り立たないが上の定理より 次が成り立つ.

定理 1.22. R が単連結であれば閉形式は完全形式である. すなわち, $d\omega=0$ ならばある C^1-級函数 u があって $\omega=du$ となる. 特に ω が正則 (調和) ならば, 正則 (調和) 函数 f があって $\omega=df$ となる.

完全な ω にたいして, $u(z)=\displaystyle\int_{z_0}^{z}\omega$ で定義すると, $du=\omega$ をみたす.
次のグリーンの定理 (または Stokes の定理) が成り立つ.

定理 1.23. 閉リーマン面 R の C^1 級 *1-form* ω に対し, $\displaystyle\int_R d\omega=0$ が成り立つ.

注: 境界つきの場合は, $\displaystyle\int_S d\omega=\int_{\partial S}\omega$ が成り立つ.
次はリーマン面の Cauchy の積分定理である.

定理 1.24. リーマン面 R の (区分的に) 滑らかな閉曲線 γ が $[\gamma]=0$ をみたすならば, R 上の任意の閉形式 ω に対し, $\displaystyle\int_\gamma\omega=0$ が成り立つ. 特に ω が正則微分形式ならば成り立つ.

Cauchy の積分定理から次の留数定理が成り立つ.

定理 1.25. 閉リーマン面の有理型微分の極は有限個しかなく留数の和は 0 である.

定理 1.26. R を種数 g のリーマン面とし, $\alpha_1, \beta_1, \ldots, \alpha_g, \beta_g$ を R の標準切断とする. R 上の 正則微分 ω_1, ω_2 に対し,

$$\sum_{k=1} g\left\{\int_{\alpha_k}\omega_1\int_{\beta_k}\omega_2-\int_{\alpha_k}\omega_2\int_{\beta_k}\omega_1\right\}=0,$$

$$i\sum_{k=1} g\left\{\int_{\alpha_k}\omega_1\int_{\beta_k}\overline{\omega_2}-\int_{\alpha_k}\overline{\omega_2}\int_{\beta_k}\omega_1\right\}=(\omega_1,\omega_2)=\int_S\omega_1\wedge{}^*\overline{\omega_2}.$$

閉曲線 γ に対して定まる 1-from ω'_γ を前の通りとする.

定理 1.27. 種数 $g \geqq 1$ の閉リーマン面 R において区分的に解析的な標準切断 $\alpha_1, \beta_1, \ldots, \alpha_g, \beta_g$ に関して次が成り立つ.
(1) ω'_{α_k}, $k = 1, \ldots, g$ は $A(R)$ の基底である.
(2) $A(R) \ni \omega \mapsto {}^t\left(\int_{\alpha_1}\omega, \cdots \int_{\alpha_k}\omega\right) \in \boldsymbol{C}^g$ は線型同型である.

このことから, $\int_{\alpha_j}\theta_k = \delta_{jk}$ となる $\theta_1, \ldots, \theta_g$ が存在する. これを正規正則微分という.

定義 1.12. θ_k $(k = 1, \ldots, g)$ を正則微分とする. T を (i, j) 成分が $\left(\int_{\beta_j}\theta_i\right)$ であるような行列とすると, $\omega \in A(R)$ に対し, $\left(\int_{\beta_1}\omega, \ldots, \int_{\beta_g}\omega\right) = \left(\int_{\alpha_1}\omega, \ldots, \int_{\alpha_g}\omega\right)T$ がなりたつ. この T を R の標準切断 $\{\alpha_1, \beta_1, \ldots, \alpha_g, \beta_g\}$ に関する周期行列という.

$T = {}^tT$, $\operatorname{Im} T$ は正定値である.

2 代数曲線と閉リーマン面

代数曲線の一般論, 基本的な用語などについてはこの稿では略す. [3] に詳しいのでそちらを参照されたい.

2.1 代数函数体

$k = \boldsymbol{C}$ または 一般の体とする.

定義 2.1. k 上の (1 変数) 代数函数体 K とは
(1) K の k 上超越的な元 x があって, $K/k(x)$ は有限次拡大である.
(2) k は K の中で代数的に閉じている.

$K/k(x)$ が有限次分離的であるような x を分離元とよぶ. このとき次が成り立つ.

定理 2.1 (Schmidt). k が完全体ならば, k の上の代数函数体には常に分離元が存在する.

定義 2.2. k の任意の元 α に対し, $\nu_P(\alpha) = 0$ となるような K の素因子 *(*付値の同値類*)* P を K の素点あるいは単に点と言う.

定理 2.2. k に含まれない K の任意の元 x に対し, $\nu_P(x) \neq 0$ となる K の素点が少なくとも *2*つ, かつ有限個存在する. したがって特に $x \in K$ が $x \in k \Longleftrightarrow \nu_P(x) = 0(\forall P)$ である.

$\nu_P(x)$ を x の P における位数という. $m = \nu_P(x) > 0$ のとき x は m 位の零点, $-m = \nu_P(x) < 0$ のとき x は m 位の極を持つという.

定理 2.3. K の素点 P の剰余体は k の有限次拡大である. したがって $k = \boldsymbol{C}$ のときは剰余体はすべて $\boldsymbol{C}$ である.

2.2 代数函数体のリーマン面

$\boldsymbol{C}$ 上の代数函数体に対し閉リーマン面が一意的に対応する, というのが代数函数論の重要な主張である.

K を $k = \boldsymbol{C}$ 上の代数函数体とする. P を K の素点, u を K の元とする. u の P における値 $\bar{u}(P)$ を以下のように定める. すなわち $\mathfrak{p}$ を P に対応する局所環の極大イデアルとし, $u \equiv a \mod (\mathfrak{p})$ となる $a \in \boldsymbol{C}$ を u の P における値とする. $\tilde{K} = \{\bar{u}(P) | u \in K\}$ は K と同型になる.

このとき, 次が成り立つ ([1] 定理 4.2).

定理 2.4. K を複素数体上の *1* 変数代数函数体とするとき, K の素点全体 S を基底空間とするリーマン面 R で解析函数体が $\tilde{K}$ と一致するような閉リーマン面が一意的に存在する. これを K に属するリーマン面とよび, $\mathfrak{R}(K)$ と書く. $K(\mathfrak{R}(K)) \cong K$ である.

素点の集合 S に解析構造が入り, それによってリーマン面となりその解析函数体が $\tilde{K}$ となるのである. すなわち,

定理 2.5. $\boldsymbol{C}$ 上の代数函数体 K に対し, K の素点を基底空間とするようなリーマン面 R で解析函数体 $K(R)$ が K と同型となるものが一意的に存在する. これを K に対応するリーマン面とよび, $\mathfrak{R}(K)$ で表わす.

2.3 閉リーマン面との対応

上では, 代数函数体, すなわち代数曲線の函数体から出発してリーマン面が構成され, 閉リーマン面となることを見た. 逆に閉リーマン面 R に対し次が成り立つ.

定理 2.6. 閉リーマン面 R 上の解析函数体 $K(R)$ は複素数体 $\boldsymbol{C}$ 上の代数函数体であって, それに対して上の対応で定まる閉リーマン面は R と同型である.

これより, 前節で述べた定理 1.18 が従う.

また, これらの対応についてはガロア理論と類似の性質があることが知られる ([1] pp.222-223). 特に, 代数函数体 K の $\boldsymbol{C}$-自己同型群と $R = R(K)$ の自己同型群は同型となる.

このようにして解析的に定義されたリーマン面と代数的に定義された代数曲線乃至その代数函数体とは密接に関連づけられることが知られる.

参考文献

[1] 岩澤健吉, 代数函数論, 岩波書店

[2] 及川廣太郎, リーマン面, 共立出版社

[3] 小川裕之, Riemann-Roch の定理, SS2007

[4] 軍司圭一, Abel-Jacobi の定理 I, SS2007

[5] 田村一郎, トポロジー, 岩波全書

第 15 回 整数論サマースクール 報告集, pp.15-60

代数曲線の Riemann-Roch の定理

小川 裕之*

§1 代数多様体

§1.1 アフィン代数多様体

(a) k を代数閉体とする.

$$\mathbb{A}^n = \mathbb{A}^n(k) = \{(x_1, \cdots, x_n) \,|\, x_1, \cdots, x_n \in k\}$$

を**アフィン空間** (affine space) という. $\mathbb{A}^1$ を**アフィン直線**, $\mathbb{A}^2$ を**アフィン平面**という. $k[X] = k[X_1, \cdots, X_n]$ を n 変数 k-係数多項式環とする. 変数の組 $X = (X_1, \cdots, X_n)$ を $\mathbb{A}^n$ の**座標系**という. 多項式 $f(X) \in k[X]$ の変数に, 点 $\boldsymbol{x} \in \mathbb{A}^n$ の座標を代入することで, f の $\boldsymbol{x}$ での値 $f(\boldsymbol{x})$ が定義される. $k[X]$ のイデアル I に対して,

$$V = V(I) = \{\boldsymbol{x} \in \mathbb{A}^n \,|\, f(\boldsymbol{x}) = 0 \ (\forall f \in I)\}$$

を I によって定まる**アフィン代数的集合** (affine algebraic set) という. $k[X]$ のイデアル

$$I(V) = \{f \in k[X] \,|\, f(\boldsymbol{x}) = 0 \ (\forall \boldsymbol{x} \in V)\}$$

を V の**定義イデアル**という. 一般に $I(V(I)) \supset I$ である. 剰余環 $k[V] = k[X]/I(V)$ を V の**座標環** (coordinate ring) という. $f \in k[V]$ の定める写像 $f : V \ni \boldsymbol{x} \longmapsto f(\boldsymbol{x}) \in k$ を V の**多項式函数** (polynomial function) という. $\mathbb{A}^n$ の座標系 $X_1, \cdots, X_n$ で代表される多項式函数を**座標函数** (coordinate function) という.

命題 1.1 (1) 有限個の点からなる $\mathbb{A}^n$ の部分集合も, $\mathbb{A}^n$ 全体もアフィン代数的集合である.
(2) アフィン代数的集合の有限個の和集合も, 任意個の共通部分もアフィン代数的集合である.

定理 1.2 $\mathbb{A}^n$ に, アフィン代数的集合の全体を閉集合系とする位相 (**Zariski 位相**という) が定義できる.

問 1 $\mathbb{A}^n$ の部分空間としてのアフィン代数的集合 V の位相を, 座標環 $k[V]$ を使って定義せよ.

(b) $I(V)$ が素イデアルのとき, V を**アフィン代数多様体** (affine algebraic variety) という. 座標環の商体 $k(V)$ を V の**函数体** (function field) といい, その元を V の**有理函数** (rational function) という. 函数体 $k(V)$ は k 上の有限生成体なので, k 上有限次の超越次数をもつ. $k(V)$ の k 上の超越次数を V の**次元** (dimension) といい, $\dim V$ で表す.

$f_1, \cdots, f_m$ を $I(V)$ の生成系とする. $P \in V$ に対して, $m \times n$ 行列 $(\partial f_i/\partial X_j(P))_{i,j}$ の階数が丁度 $n - \dim V$ であるとき, P を**非特異点** (non-singular point) あるいは**単純点** (simple point) という. 階数が $n - \dim V$ より小さいとき, P を**特異点** (singular point) という.

アフィン代数的集合 V がアフィン代数的集合 V_1 を部分集合として含むとき, $V_1 \subset V$ と書き, V_1 を V のアフィン代数的部分集合という. このとき $I(V_1) \supset I(V)$ となる. V_1 がアフィン代数多様体なら次元 $\dim V_1$ が定まる. アフィン代数多様体 V に含まれるアフィン代数多様体 $V_1 \subset V$ の次元の最大値を V の**次元**とい

*大阪大学大学院 理学研究科

い, $\dim V$ と書く. アフィン代数的集合 V の部分集合 U が**十分に大きい**とは, $V \smallsetminus U$ が V より次元の小さい代数的部分集合に含まれるときをいう.

(c) φ を有理函数とする. $P \in V$ について, 多項式函数 p, q で $\varphi = p/q$, $q(P) \neq 0$ となるものが取れるとき, φ は P で**正則** (regular) であるといい, P を φ の**正則点**という. φ の正則点全体の集合を $\mathrm{dom}\,\varphi$ とおき, φ の**定義域**という. φ の正則点 P において φ の値が $\varphi(P) = p(P)/q(P)$ により定まるので, 有理函数はその定義域から $k\ (= \mathbb{A}^1)$ への写像となる. $\varphi(P) = 0$ となるとき P を φ の**零点** (zero) という.

定理 1.3 アフィン代数多様体において, すべての点で正則な有理函数は多項式函数である.

$P \in V$ で正則な有理函数の全体を $k[V]_P$ とおくと, $k[V]_P$ は多項式函数の全体 $k[V]$ を含む整域である. $k[V]_P$ の商体もまた函数体 $k(V)$ なので, 有理函数は P で正則な有理函数の比で表せる. P が $1/\varphi$ の零点であるとき, P を φ の**極** (pole) という.

命題 1.4 $k[V]_P$ は, P を零点にもつ有理函数の全体を唯一つの極大イデアルとする局所環である.

問 2 有理函数の定義域は, 十分に大きい部分集合であることを示せ.

§1.2 射影多様体

(a) $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{A}^{n+1} \smallsetminus \{0\}$ とする. $\boldsymbol{a} = c\boldsymbol{b}$ なる $c \in k^\times$ が取れるとき $\boldsymbol{a} \sim \boldsymbol{b}$ と書く. 同値類の全体 $\mathbb{P}^n = \mathbb{A}^{n+1} \smallsetminus \{0\}/\sim$ を $\boldsymbol{n}$ **次元射影空間** (n-projective space) という. $\mathbb{P}^1$ を**射影直線**, $\mathbb{P}^2$ を**射影平面**という. $(x_0, x_1, \cdots, x_n) \in \mathbb{A}^n \smallsetminus \{0\}$ で代表される射影空間の点を連比 $[x_0 : x_1 : \cdots : x_n]$ で表し, **斉次座標**という. アフィン空間 $\mathbb{A}^{n+1}$ の座標系 $X_0, X_1, \cdots, X_n$ の連比 $X_0 : X_1 : \cdots : X_n$ を $\mathbb{P}^n$ の**斉次座標系**という. 多項式環 $k[X] = k[X_0, X_1, \cdots, X_n]$ の元 $f(X)$ が $f(\lambda X) = \lambda^d f(X)$ $(\forall \lambda \in k)$ を満たすとき, f を $\boldsymbol{d}$ **次斉次多項式**という. d を斉次多項式 f の**次数**といい, $\deg f$ と書く. 斉次多項式で生成されたイデアルを**斉次イデアル**という. 斉次イデアル I に対して,

$$V = V(I) = \{\boldsymbol{x} \in \mathbb{P}^n \mid f(\boldsymbol{x}) = 0 \ \forall f \in I \text{ は斉次多項式 }\}$$

を I によって定まる**射影代数的集合** (projective algebraic set) という.

$$I(V) = (f \in kX \mid f \text{ は斉次}, \ f(\boldsymbol{x}) = 0 \ (\forall \boldsymbol{x} \in V))$$

を V の**定義イデアル**という. 剰余環 $k[V] = k[X]/I(V)$ を V の**斉次座標環** (homogeneous coordinate ring) という. 定義イデアルが素イデアルのとき, V を**射影多様体** (projective variety) という.

命題 1.5 (1) 有限個の点からなる $\mathbb{P}^n$ の部分集合も, $\mathbb{P}^n$ 全体もアフィン代数的集合である.
(2) 射影代数的集合の有限個の和集合も, 任意個の共通部分もアフィン代数的集合である.

定理 1.6 $\mathbb{P}^n$ に, 射影代数的集合の全体を閉集合系とする位相が定義できる.

問 3 $\mathbb{P}^n$ の部分空間としての射影代数的集合 V の位相を, 斉次座標環 $k[V]$ を使って定義せよ.

(b) $X_0 : X_1 : \cdots : X_n$ を射影空間 $\mathbb{P}^n$ の斉次座標系とする. 斉次イデアル (X_j) によって定まる射影代数的集合 $V(X_j)$ の補集合を U_j とおくと, $U_j = \{[x_0 : \cdots] \in \mathbb{P}^n \mid x_j \neq 0\}$ と表せる. $V(X_j)$ は $\mathbb{P}^{n-1}$ に同型で, U_j は $\mathbb{A}^n$ に同型である. V を射影代数的集合とする. $V_j = V \cap U_j$ はアフィン空間 $(U_j \simeq \mathbb{A}^n)$ に含まれるアフィン代数的集合になる. また $V_j^\infty = V \cap V(X_j)$ は射影空間 $(V(X_j) \simeq \mathbb{P}^{n-1})$ に含まれる射影代数的集合で, 集合として $V = V_j \cup V_j^\infty$ と書ける. V_j を座標 X_j に関する**アフィン部分集合**といい, V_j^∞ を**無限遠集合**, V_j^∞ に属する点を**無限遠点**という.

(c) n 変数 d 次多項式 f に対して

$$\bar{f}(X_0, X_1, \cdots, X_n) = X_0^d\, f(X_1/X_0, \cdots, X_n/X_0)$$

は d 次斉次多項式で, f の**斉次化**という. V をアフィン代数的集合とし, $I(V)$ をその定義イデアルとする. $I(V)$ の元を斉次化したもので生成される斉次イデアルを $\overline{I(V)}$ とおく. $\overline{I(V)}$ によって定まる射影代数的集合 $\bar{V}$ を V の**射影閉包**という. $\bar{V} \smallsetminus V$ の点を V の**無限遠点**という.

(d) 1 次斉次多項式で生成された斉次イデアルによって定まる代数的集合 $\ell \subset \mathbb{P}^n$ は**超平面**と呼ばれ, $\mathbb{P}^{n-1}$ に同型である. また $U = \mathbb{P}^n \smallsetminus \ell$ はアフィン空間 $\mathbb{A}^n$ に同型である. $\bar{V} \subset \mathbb{P}^n$ を射影代数的集合とする. 超平面 ℓ で $\bar{V}$ のどの既約成分も含まないものをとり, $U = \mathbb{P}^n \smallsetminus \ell$ とおく. $V = \bar{V} \cap U$ はアフィン空間 $U \simeq \mathbb{A}^n$ に含まれるアフィン代数的集合で, 空ではない. V の射影閉包は $\bar{V}$ に等しい. V を $\bar{V}$ の**アフィン部分集合**といい, $V \cap \ell$ を V の**無限遠集合**, $V \cap \ell$ に属する点を**無限遠点**という. 射影代数的集合 $\bar{V}$ の任意の点 P に対して, P を通らない超平面 ℓ をとることで, P を含むアフィン部分多様体 V が存在する. このとき V を P の**アフィン近傍**という. $\bar{V}$ が射影代数多様体なら, アフィン部分集合 V はアフィン代数多様体になる. このとき V を $\bar{V}$ の**アフィン部分多様体**という. 射影多様体 $\bar{V}$ が ℓ に含まれないなら, $\bar{V}$ はアフィン部分多様体 V の射影閉包である.

問 4 (1) 射影代数的集合 $\bar{V}$ において, 任意のアフィン部分集合は開集合であることを示せ.
(2) 射影閉包は, アフィン代数的集合の射影空間における位相閉包であることを示せ.

§1.3 射影多様体の有理函数

(a) 有理式 $f(X) \in k(X) = k(X_0, X_1, \cdots, X_n)$ が $f(\lambda X) = \lambda^d f(X)$ $(\lambda \in k)$ を満たすとき, f を ***d* 次斉次有理式**といい, d を f の**次数**という. このとき f は次数の差が d の斉次多項式の比で表すことができる. 特に 0 次斉次有理式 f は, 次数の同じ斉次多項式 p, q で $f = p/q$ と表すことができる.

(b) $\bar{V} \subset \mathbb{P}^n$ を射影多様体とし, $I(\bar{V})$ をその定義イデアルとする. 0 次 $n{+}1$ 変数斉次有理式 p/q で $q \notin I(\bar{V})$ なるものの全体を $k[X;\bar{V}]_0$ と書く. $p_1/q_1, p_2/q_2 \in k[X;\bar{V}]_0$ が $p_1\, q_2 - p_2\, q_1 \in I(\bar{V})$ をみたすとき, $p_1/q_1 \sim p_2/q_2$ と定義する. $k(\bar{V}) = k[X;\bar{V}]_0/\sim$ とおき, $\bar{V}$ の**函数体**という. 函数体の元を**有理函数**という. 函数体 $k(\bar{V})$ の k 上の超越次数を $\bar{V}$ の**次元** (dimension) といい $\dim \bar{V}$ で表す.

定理 1.7 射影多様体の有理函数は自然にアフィン部分多様体の有理函数とみなせる. この意味で, 射影多様体の函数体はアフィン部分多様体の函数体に同型で, 射影多様体の次元はアフィン部分多様体の次元に等しい.

(c) φ を $\bar{V}$ の有理函数とする. $P \in \bar{V}$ に対して, 次数の同じ斉次多項式 p, q で $\varphi = p/q$, $q(P) \neq 0$ となるものが取れるとき, φ は P で**正則**であるといい, P を φ の**正則点**という. $\varphi(P) = p(P)/q(P)$ により φ の正則点 P での値が定まる.

命題 1.8 $V \subset \bar{V}$ を $P \in \bar{V}$ のアフィン近傍とする. $\bar{V}$ の有理函数が P で正則であることと, V の有理函数として P で正則であることとは同値である. 従って P で正則な $\bar{V}$ の有理函数の全体は $k[V]_P$ に等しい.

φ の正則点全体の集合を $\mathrm{dom}\,\varphi$ とおき, φ の**定義域**という. φ の正則点 P において φ の値が定まるので, 有理函数はその定義域から k $(= \mathbb{A}^1)$ への写像となる. $\varphi(P) = 0$ となるとき P を φ の**零点**という. 写像の定義域には含まれない点 $P \in \bar{V} \smallsetminus \mathrm{dom}\,\varphi$ で, $1/\varphi$ が P で定義され $(1/\varphi)(P) = 0$ となるとき P を φ の**極**という.

定理 1.9 射影代数多様体において, すべての点で正則な有理函数は定数函数である.

(d) $f_1, \cdots, f_m$ を $I(\bar{V})$ の斉次多項式からなる生成系とする. $P \in \bar{V}$ において, $m \times n$ 行列 $(\partial f_i/\partial X_j(P))_{i,j}$ の階数が $n - \dim \bar{V}$ であるとき P を**非特異点**といい, 階数が $n - \dim \bar{V}$ より小さいとき P を**特異点**という.

命題 1.10 P が射影多様体 $\bar{V}$ の特異点であることと, P のアフィン近傍での特異点であることとは同値である.

§1.4 有理写像・正則写像

(a) V をアフィン多様体とする. n 個の有理函数 $f_1, \cdots, f_n$ に対して,

$$\varphi = (f_1, \cdots, f_n) : V \ni P \longmapsto (f_1(P), \cdots, f_n(P)) \in \mathbb{A}^n$$

を V から $\mathbb{A}^n$ への**有理写像**という. φ は $f_1, \cdots, f_n$ の定義域の共通部分で写像として定義される. φ の像がアフィン代数多様体 V_1 に含まれるとき, $\varphi : V \to V_1$ と書き V から V_1 への有理写像という. 函数体の準同型写像

$$\varphi^* : k(V_1) \ni f \longmapsto f \circ \varphi \in k(V)$$

が引き起こされる. φ の像が V_1 の中で十分に大きいなら, φ^* は単射になり, $k(V_1)$ は $k(V)$ の部分体に同型である. 更に $k(V)$ が $\varphi^* k(V_1)$ 上有限次拡大となるとき, その拡大次数を φ の**写像度** (degree) といい $\deg \varphi$ と書く. このとき, 有限次拡大 $k(V)/\varphi^* k(V_1)$ のノルム写像 $N_{k(V)/\varphi^* k(V_1)} : k(V)^\times \to \varphi^* k(V_1)^\times$ に, 中への同型 φ^* の逆写像を合成した

$$\varphi_* = (\varphi^*)^{-1} \circ N_{k(C)/\varphi^* k(C')} : k(C)^\times \to k(C')^\times$$

が定義される. 乗法群の準同型写像 φ_* を φ の**ノルム写像**という.

命題 1.11 (1) φ の像が V_1 の中で十分に大きいなら, φ^* は体の埋め込みで, $\dim V_1 \le \dim V$ となる.
(2) $\dim V = \dim V_1 = 1$ とする. φ が定数写像でなければ φ^* は単射で, $k(V)/\varphi^* k(V_1)$ は有限次拡大である.

(b) V をアフィン代数的集合とし, $f_0, f_1, \cdots, f_n$ を有理函数とする.

$$\varphi = [f_0 : f_1 : \cdots : f_n] : V \ni P \longmapsto [f_0(P) : f_1(P) : \cdots : f_n(P)] \in \mathbb{P}^n$$

を V から $\mathbb{P}^n$ への有理写像という. $P \in V$ に対して, 有理写像 g を $g f_0, g f_1, \cdots, g f_n$ が P で正則で少なくともひとつ P で零にならないように取れるとき, φ は P で**正則**であるといい, P を φ の**正則点**という. φ の正則点の全体を $\mathrm{dom}\,\varphi$ と書き, φ の**定義域**という. すべての点で正則な有理写像を**正則写像**という. 有理写像 φ の像が射影多様体 $\bar{V}_1$ に含まれるとき, $\varphi : V \to \bar{V}_1$ と書き V から $\bar{V}_1$ への有理写像という.

射影多様体からアフィン空間へ, 射影多様体からアフィン多様体へ, 射影多様体から射影空間へ, 射影多様体から射影多様体への有理写像を同様に定義し, それらについて正則点, 定義域なども同様に定めることができる.

V の有理函数 φ に対して, 有理写像 $[1 : \varphi] : V \to \mathbb{P}^1$ を考える. φ の定義域において $[1 : \varphi]$ は明らかに写像として定義される. また φ の極 P においても $[1 : \varphi](P) = [1/\varphi : 1](P) = [0 : 1]$ だから, $[1 : \varphi]$ は P で正則である.

命題 1.12 (1) 有理函数 φ に対して, $[1 : \varphi]$ の定義域は φ の正則点と極の全体に等しい.
(2) φ が定数函数でないなら, $[1 : \varphi]$ の像は $\mathbb{P}^1$ から有限個の点を除いたものとなる.

(c) $\bar{V}_1, \bar{V}_2$ を射影多様体とする. 正則写像 $\varphi : \bar{V}_1 \to \bar{V}_2$, $\psi : \bar{V}_2 \to \bar{V}_1$ で, $\varphi \circ \psi$, $\psi \circ \varphi$ が恒等写像であるものが取れるとき, $\bar{V}_1$ と $\bar{V}_2$ は**同型** (isomorphic) であるといい $\bar{V}_1 \simeq \bar{V}_2$ と書く. φ, ψ を**同型写像** (isomorphism) という. アフィン多様体に対しても同様に同型, 同型写像が定義される.

V_1, V_2 をアフィン多様体または射影多様体とする. 像が十分に大きい有理写像 $\varphi : V_1 \to V_2$, $\psi : V_2 \to V_1$ で, $\varphi \circ \psi$, $\psi \circ \varphi$ が殆どの点で恒等写像に等しいとき, φ, ψ を**双有理写像** (birational map) といい, V_1 と

V_2 は**双有理同値** (birational equivalent) という. アフィン多様体 V とその射影閉包 $\bar{V}$ は双有理同値である. またそれらの函数体は同型であった. $\mathbb{A}^n$ の函数体も, $\mathbb{P}^n$ の函数体も, n 個の射影直線の直積 $\mathbb{P}^1 \times \cdots \times \mathbb{P}^1$ の函数体も n 変数有理函数体に同型で, $\mathbb{A}^n$, $\mathbb{P}^n$, $\mathbb{P}^1 \times \cdots \times \mathbb{P}^1$ は双有理同値である.

定理 1.13　双有理同値であるための必要十分条件は, 函数体が同型であることである.

§2　代数曲線

§2.1　射影直線・射影平面

射影空間の中でも 1 次元の射影直線と 2 次元の射影平面をこれからよく使う. アフィン直線, 射影直線は有理函数などの値の属する空間として, アフィン平面, 射影平面は 1 変数代数函数体のモデルとしての平面曲線を描くキャンパスとして.... 特に断らない限り以下の記号を固定して使う.

射影直線 $\mathbb{P}^1$ の斉次座標系 $X_0 : X_1$ を固定し, アフィン直線と同型な部分集合 $U_0 = \{[x_0 : x_1] \in \mathbb{P}^1 \,|\, x_0 \neq 0\}$ をとる. 集合として $\mathbb{P}^1 = U_0 \cup \{[0:1]\}$ と書ける. アフィン直線 U_0 の座標系として $z = X_1/X_0$ が取れ, $U_0 \subset \mathbb{P}^1$ の点はこの座標で表す. $[0:1]$ は z に関する無限遠点なので ∞ と書く. こうして $\mathbb{P}^1 = \mathbb{A}^1 \cup \{\infty\}$ と書ける. 別のアフィン部分集合 $U_\infty = \{[x_0 : x_1] \in \mathbb{P}^1 \,|\, x_1 \neq 0\}$ の座標として $w = X_0/X_1$ が取れる. U_0 と U_∞ の共通部分 ($U_0 \cap U_\infty = \mathbb{P}^1 \smallsetminus \{0, \infty\}$) において $w = 1/z$ と書けるので, ∞ の近傍での解析にはアフィン部分空間 U_∞ と座標 $w = 1/z$ を使えばよい.

射影平面 $\mathbb{P}^2$ の斉次座標系 $X : Y : Z$ を固定する. $U = \{[a:b:1] \in \mathbb{P}^2 \,|\, (a, b) \in \mathbb{A}^2\}$ は $x = X/Z$, $y = Y/Z$ を座標系とするアフィン平面 $\mathbb{A}^2$ と同一視できる. x-座標は $\{[x_0 : 0 : 1] \,|\, x_0 \in \mathbb{A}^1\}$ で, y-座標は $\{[0 : y_0 : 1] \,|\, y_0 \in \mathbb{A}^1\}$ で表される. $\ell_\infty = \{[a:b:0] \in \mathbb{P}^2 \,|\, [a:b] \in \mathbb{P}^1\}$ を**無限遠直線**とよぶ. 集合として $\mathbb{P}^2 = \mathbb{A}^2 \cup \ell_\infty$ と書ける.

§2.2　平面曲線・代数曲線

(a)　k を代数閉体とする. 1 次元アフィン代数多様体を**アフィン代数曲線** (affine algebraic curve), 1 次元射影多様体を**射影曲線** (projective curve) という. アフィン代数曲線を貼り合わせた, 連結な代数多様体を**代数曲線** (algebraic curve) という. この解説での対象は非特異完備代数曲線なので, 殆どの場合, アフィン平面曲線の非特異完備化を考えれば十分である. 非特異完備化はその手続きに応じていろいろな物が現れるが, 代数曲線ではすべて同型になるので, 結局のところどの手順を選んでも構わない. §2.6 で非特異完備化の具体的な例を与える. そこでは幾つかの平面曲線について, 射影閉包をとり無限遠点などの特異点を具体的に解消してみせる. 正統的な議論とは少し離れてしまい, 十分に満足のいく例ではないかもしれないが, それらを見知っておくことで, 代数曲線により親しく接する機会になればと思います.

(b)　2 変数の多項式 $f(x, y) \in k[x, y]$ に対して, イデアル (f) によって定まるアフィン代数的集合 C を**アフィン平面曲線** (affine plane curve) という. f を C の**定義多項式**, $f = 0$ を**定義方程式**という. 定義多項式が既約のとき C を**既約アフィン平面曲線**という. このとき C は 1 次元アフィン代数多様体である. $f = f_1 f_2 \cdots f_r$ と既約多項式の積に分解するとき, C は $f_1, \cdots, f_r$ のそれぞれで定義された既約アフィン平面曲線 $C_1, \cdots, C_r$ の和集合となる. $C_1, \cdots, C_r$ を C の**既約成分**という. 斉次多項式 $f(X, Y, Z) \in k[X, Y, Z]$ に対して, 斉次イデアル (f) によって定まる射影代数的集合 C を**射影平面曲線** (projective plane curve) という. f を C の**定義多項式**, $F = 0$ を**定義方程式**という. 定義多項式が既約のとき C を**既約射影平面曲線**という. アフィン平面曲線, 射影平面曲線を**平面曲線** (plane curve) という. 平面曲線 C の定義多項式の次数 m を, C の**次数**といい, C を $\boldsymbol{m}$ **次曲線**という. 1 次曲線を**直線**という.

(c) $C : f(x, y) = 0$ をアフィン平面曲線とする. $\partial f/\partial x(P) = \partial f/\partial y(P) = 0$ を満たす $P = (a, b) \in C$ を**特異点**といい, そうでないとき**非特異点**という. 非負整数 $j \geq 0$ に対して, u, v の j 次斉次多項式 $f_P^{(j)}(u, v)$ を

$$f_P^{(j)}(u, v) = (u\frac{\partial}{\partial x} + v\frac{\partial}{\partial y})^j f(P) = \sum_{i=0}^{j} \binom{j}{i} \frac{\partial^j}{\partial x^i \partial y^{j-i}} f(P)\, u^i\, v^{j-i}$$

で定義する. $f_P^{(r)}(u, v)$ が恒等的に 0 ならない最小の r を P の**重複度** (multiplicity) といい, このとき P を ***r*-重点**という. 特異点は重複度が 2 以上で, 非特異点は重複度が 1 である. r-重点 P において, $f_P^{(r)}(x - a, y - b) = 0$ で定義されるアフィン平面曲線を**接錐** (tangent cone) という. 接錐は重複度を込めて丁度 r 個の直線の和で, それぞれの直線は C に P で接する. r-重特異点 P $(r \geq 2)$ の接錐が異なる r 個の直線の和となる (丁度 r 個の接線が引ける) とき, P を**通常特異点** (ordinary singular point) という. 通常 2 重点を**結節点** (node) という. $P \in C$ が結節点のとき, 平行移動で P をアフィン平面の原点に移し, 2 つの異なる接線を $y = x$, $y = -x$ に移す線形変換により C の定義方程式は $y^2 - x^2 + (x, y$ の 3 次以上の項$) = 0$ と書ける. 接線が 1 本しか引けない 2-重点では, 接線を $y = 0$ に移すことで $y^2 + (x, y$ の 3 次以上の項$) = 0$ となる. 適当な同型変換で $y^2 - x^3 + (x, y$ の 4 次以上の項$) = 0$ となるとき, P を**尖点** (cusp) という.

問 5 $f(x, y)$ を斉次 3 次多項式とする. 既約なアフィン代数曲線 $C : y^2 = f(x, y)$ は尖点をもつことを示せ.

問 6 $F(X, Y, Z)$ を m 次斉次多項式とし, $\overline{C} : F(X, Y, Z) = 0$ を射影平面曲線とする. 次を示せ.

(1) $X\frac{\partial F}{\partial X}(X, Y, Z) + Y\frac{\partial F}{\partial Y}(X, Y, Z) + Z\frac{\partial F}{\partial Z}(X, Y, Z) = m\,F(X, Y, Z)$ が成り立つ.

(2) $P \in \overline{C}$ が特異点であるための必要十分条件は, $\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0$ である.

(3) $P \in \overline{C}$ が特異点でないとき, P での接線は $X\frac{\partial F}{\partial X}(P) + Y\frac{\partial F}{\partial Y}(P) + Z\frac{\partial F}{\partial Z}(P) = 0$ で与えれらる.

(4) Z-座標が 0 でない $P \in \overline{C}$ が $\overline{C}$ の特異点であることと, $\overline{C} \cap \{Z \neq 0\}$ の特異点であることは同値である.

(d) C を平面曲線とし, $P \in C$ を非特異点とする. P における C の接線 ℓ_P は, P での C との交点数 $I_P(C, \ell_P)$ が 2 以上の直線である. P での交点数が 3 以上になるとき P を**変曲点** (point of inflextion, flex) という. 多項式 $f(x, y)$, 斉次多項式 $F(X, Y, Z)$ に対して,

$$H_f(x, y) = \det \begin{vmatrix} f_{xx} & f_{xy} & f_x \\ f_{yx} & f_{yy} & f_y \\ f_x & f_y & f \end{vmatrix} \qquad H_F(X, Y, Z) = \det \begin{vmatrix} F_{XX} & F_{XY} & F_{XZ} \\ F_{YX} & F_{YY} & F_{YZ} \\ F_{ZX} & F_{ZY} & F_{ZZ} \end{vmatrix}$$

とおく. ここで添え字はその変数に関する偏微分を表すものとする. アフィン平面曲線 $C : f(x, y) = 0$ に対して, $H_f(x, y) = 0$ で表されるアフィン平面曲線を C の **Hesse 曲線** (Hessian) という. 射影平面曲線 $\overline{C} : F(X, Y, Z) = 0$ に対して, $H_F(X, Y, Z) = 0$ で表される射影平面曲線を $\overline{C}$ の **Hesse 曲線**という.

定理 2.1 平面曲線の非特異点が変曲点であるための必要十分条件は, Hesse 曲線上にあることである.

問 7 上の定理を示せ.

§2.3 代数函数体

(a) K を体 k の拡大体とする. $y \in K$ が $k(x_1, \cdots, x_r)$ 上代数的であるとき, y は $x_1, \cdots, x_r$ に k 上**代数的従属**であるという. k 上代数的でないとき, $x \in K$ は k 上**超越的** (transcendental) であるという. K の部分集合 S が k 上**代数的独立**であるとは, 任意の $y \in S$ が, y を除く S の有限個の元の組すべてに対して代数的従属でないときをいう. K の部分集合 S が代数的独立で, K が $k(S)$ の代数拡大であるとき, S を k 上の K の**超越基**という. 体 k の拡大 K に対して超越基 S は必ず存在し, S の濃度は一意に定まる. この濃度を K の k 上の**超越次数** (transcendence degree) といい $\mathrm{tr.deg}_k K$ で表す. $K = k(S)$ となる超越基 S が取れるとき, K を k の**純超越拡大**という.

(b) 体 k の超越次数 n の純超越拡大を k 上の $\boldsymbol{n}$ **変数有理函数体** (rational function field) といい, その様な体の有限次代数拡大を k 上の $\boldsymbol{n}$ **変数代数函数体** (algebraic function field) という. また k を K の**係数体**という. K を k 上の 1 変数代数函数体とする. このとき k 上超越的な元 $x \in K$ で K が $k(x)$ 上有限次拡大となるものが取れる. K が $k(x)$ の分離拡大となるとき, x を**分離元**という.

定理 2.2 (F.K.Schmidt) 係数体が完全体の 1 変数代数函数体は, 常に分離元をもつ.

以下, 係数体 k は代数閉体とする. x を 1 変数代数函数体 K の分離元とすると, K は $k(x)$ の単純拡大になる. $K = k(x, y)$ と書ける. K の超越次数は 1 なので, x と y は k 上代数的従属である. 0 でない多項式 $f(X, Y) \in k[X, Y]$ で $f(x, y) = 0$ なるのもが存在する. アフィン平面曲線 $C : f(X, Y) = 0$ をとると, C の函数体 $k(C)$ は K に一致する.

定理 2.3 係数体が代数閉体のとき, 1 変数代数函数体は適当なアフィン平面曲線の函数体になる.

§2.4 局所環と局所助変数

(a) C を代数曲線とする. $P \in C$ で正則な有理函数全体を $k[C]_P$ とし, P を零点にもつものの全体を M_P とおく.

命題 2.4 $k[C]_P$ は, M_P を唯一つの極大イデアルとする局所環である. 特に $P \in C$ が非特異点のとき整閉である.

定理 2.5 P が特異点でないとき, $k[C]_P$ は離散付値環である.

(b) P を非特異点とする. 離散付値環 $k[C]_P$ から誘導された $k(C)$ の加法的正規付値を ord_P とおく. 付値体 $k(C)$ の完備化を $k(C)_P$ とおく. 有理函数を含む完備化の元 f に対して $\mathrm{ord}_P(f)$ を f の P での**位数** (order) という. 位数が非負のとき f は P で**正則**であるという. 位数が正のとき P を f の**零点**といい, 位数が負のとき P を f の**極**という. $k[C]_P$ が整閉なので, これらは §1.1 (c), §1.3 (c) の定義と同値になる. P が特異点のときは少し煩雑になる. $k[C]_P$ の整閉包 $k[C]'_P$ は有限個の極大イデアルをもつ環である. 各極大イデアルは, 特異点解消の後に新たに付け加わる非特異点に対応する. 各極大イデアルごとに $k[C]'_P$ に離散付値が定まり, $k(C)$ が離散付値体になる. 以下, 非特異点の場合と同様の議論ができるが, 極大イデアルの選び方で付値など異なることを注意しておく.

(c) 完備付値体 $k(C)_P$ の素元 (位数が丁度 1 の元) を P における**局所助変数** (local parameter) という. P での局所助変数 t_P で $k(C)_P$ の元を Laurent 級数展開することで, $k(C)_P = k((t_P))$ と書ける. $P \in C$ が非特異点のとき局所助変数を P で正則な有理式に表せる有理函数を取ることができる. 特異点 P では一般に $k[C]_P$ が整閉でないので, 局所助変数を P で正則な有理式に表せる有理函数で取ることはできない.

定理 2.6 非特異点での局所助変数 (となる有理函数) は函数体の分離元である. 即ち, $t_P \in k(C)$ を非特異点 $P \in C$ の局所助変数とするとき, $k(C)$ は $k(t_P)$ 上の有限次分離拡大体である.

定理 2.7 代数曲線の函数体は 1 変数代数函数体である. 代数曲線はあるアフィン平面曲線に双有理同値である.

定理 2.8 双有理同値な代数曲線において, それらの非特異完備化は互いに同型である.

問 8 (1) 代数曲線 $C_1 : y^2 = x^2(x+1)$, $C_2 : y^2 = x^3$, $C_3 : y^2 = x^4(x-1)$ に関して, 特異点を求めよ.
(2) 各特異点における局所環が整閉であるかどうか調べ, 整閉包における極大イデアルを求めよ.
(3) それら代数曲線の函数体が有理函数体であることを示せ.

(d) 射影直線における局所環, 局所助変数をまとめておく. 射影直線 $\mathbb{P}^1$ の斉次座標系を $X_0 : X_1$ とすると, $\mathbb{P}^1$ の有理函数は X_0, X_1 の 0 次斉次有理式の全体に等しい. 0 次斉次有理式は, 分母分子を X_0 の適当なベキで割ることで, $z = X_1/X_0$ の有理式として表せる. 函数体 $k(\mathbb{P}^1)$ は有理函数体 $k(z)$ になる. z は $U_0 = \{X_0 \neq 0\} \simeq \mathbb{A}^1$ の座標系なので, $\mathbb{P}^1$ の函数体は $\mathbb{A}^1$ の函数体に等しい. $a = [1 : a] \in \mathbb{A}^1 \subset \mathbb{P}^1$ をとる. 有理函数 $f \in k(\mathbb{P}^1) = k(z)$ が a で正則であるためには, 有理式としての f の分母が $z = a$ で零にならなければよい. 局所環は $k[\mathbb{P}^1]_a = \{f = p/q \,|\, p, q \in k[z], q(a) \neq 0\}$ となる. $k[\mathbb{P}^1]_a$ は $u_a = z - a$ を素元とする離散付値環で, u_a で割り切れる回数で付値が定まる. 函数体の完備化 $K(\mathbb{P}^1)_a$ は $k((u_a)) = k((z - a))$ で, 有理式を $z = a$ の近傍で Laurent 級数展開することに対応する.

無限遠点 $\infty = [0 : 1] \in \mathbb{P}^1$ はアフィン部分直線 $U_\infty = \{X_1 \neq 0\} \simeq \mathbb{A}^1$ の点と思い, 座標 $w = X_0/X_1 = 1/z$ を使って上と同様に考えることができる. 結論を w でなく z の言葉でまとめる. ∞ での局所環 $k[\mathbb{P}^1]_\infty$ は $\{f = p/q \,|\, p, q \in k[z], \deg p \leq \deg q\}$ に等しく, 次数の差 $\deg q - \deg q$ を $f = p/q$ の付値とする離散付値環をなす. ∞ の局所助変数として $u_\infty = 1/z$ がとれ, 函数体の ∞ での完備化は $k((1/z))$ に等しい.

§2.5 Bézout の定理

(a) 斉次多項式 f, g で定義された射影平面曲線をそれぞれ C, D とおく. $m = \deg f, n = \deg g$ とし, C, D は共通の既約成分をもたないとする. C と D の両方に属する点 P を, C, D の**交点**という. P を原点として含むアフィン部分平面 $\mathbb{A}^2 \subset \mathbb{P}^2$ をとる. このアフィン部分平面 $\mathbb{A}^2$ の座標系を x, y とし, $C \cap \mathbb{A}^2$, $D \cap \mathbb{A}^2$ の定義多項式を $f(x, y)$, $g(x, y)$ と書く. 形式的ベキ級数環 $k[[x, y]]$ において, 剰余環 $k[[x, y]]/(f, g)$ は有限次元 k 線形空間になる. その次元を P における C と D の**局所交点数**といい, $I_P(C, D)$ $(= \dim_k k[[x, y]]/(f, g))$ とおく. このとき,

定理 2.9 (Bézout) $$\sum_{P \in C \cap D} I_P(C, D) = m\,n$$

(b) C と D の交点 P は $f(P) = 0, g(P) = 0$ を満たすので, 連立方程式 $f = g = 0$ の根として得られる. 局所交点数は, 少しわかり難いが, 特異点で交わる場合を除いて, 連立方程式における根の重複度と考えてよい. C と D が普通に交わる場合の局所交点数は 1 で, 接する場合は 2 (以上), 接する度合いが増す毎にその値は増えていく. 多くの場合に局所交点数は 1 になるので, 大雑把には C と D の交点の個数は $m\,n$ 個といってもいいだろう.

定理 2.10 (簡易版) 共通の既約成分をもたない 2 つの射影平面曲線は必ず交点をもつ. 更にそれら射影平面曲線の次数を m, n とおくとき, 交点の個数は高々 $m\,n$ 個で, 接するなど特別な場合を除いて丁度 $m\,n$ 個である.

§2.6 アフィン平面曲線の完備化

(a) 2 次アフィン平面曲線は, 定義方程式が可約であるなら, 2 つの直線の和となり, その交点は特異点になる. アフィン平面上で平行であるならアフィン平面内に交点はもたないが, 射影閉包をとると無限遠点で交わり, 無限遠点を特異点にもつ. 既約な 2 次アフィン平面曲線は非特異で, その射影閉包も非特異である. 既約な 2 次射影平面曲線は非特異で, 射影直線に同型である. この同型は Bézout の定理を使って具体的に書くことができる.

問 9 アフィン平面内の円, 楕円, 双曲線, 放物線を定義する方程式を与え, それらが特異点をもたないことを確かめよ. それぞれの射影閉包もまた特異点をもたず, すべて同型であることを同型写像を具体的に書いて確かめよ.

(b) k の標数が 2 でないとする. 3 次多項式 $f(x) \in k[x]$ に対して, アフィン平面曲線

$$C : y^2 = f(x)$$

を考える. f が重根をもたないとき, C は非特異アフィン平面曲線である. このとき C を**楕円曲線** (elliptic curve) という. 楕円曲線 C の射影閉包は $\overline{C} : Y^2 Z = Z^3 f(X/Z)$ で定義される 3 次射影平面曲線である. 無限遠点は $[0:1:0] \in \overline{C}$ の 1 点で, $[0:1:0]$ でも非特異なので, $\overline{C}$ は非特異 3 次射影平面曲線である.

$O = [0:1:0] \in \overline{C}$ とおく. 2 点 $P, Q \in \overline{C}$ をとる. Bézout の定理より, P, Q を通る直線 ($P = Q$ のときは P での接線) は第 3 の点 R で C と交わる. R と O を通る直線も R' で C と交わる. ここで $P \oplus Q := R'$ と定める. C は $\oplus$ に関して O を零元とする加法群の構造をもつ.

問 10 (1) アフィン平面曲線 $C : y^2 = f(x)$ ($\deg f = 3$) が非特異であることと, $f(x) = 0$ が重根をもたないことが同値であることを示せ. C の射影閉包 $\overline{C}$ が無限遠点で非特異であることを示せ.

(2) $\oplus$ が O を零元とする加法を C の上に定めることを確かめよ.

(3) P, P', O が同一直線上にあるとき, P と P' の座標の関係を記せ.

(c) $a_1, a_2, a_3, a_4, a_6 \in k$ をとり, 3 次アフィン平面曲線

$$C : y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

を考える. k の標数が 2 と異なるとき, 定義方程式の左辺を y に関して平方完成することで, C はアフィン平面曲線

$$C_1 : y^2 = 4x^3 + b_2 x^2 + 2 b_4 x + b_6$$

と同型である. ただし $b_2 = a_1^2 - 4a_2$, $b_4 = 2a_4 + a_1 a_3$, $b_6 = a_3^2 + 4a_6$ とおいた. 更に $c_4 = b_2^2 - 24 b_4$, $c_6 = -b_2^3 + 36 b_2 b_4 - 216 b_6$ とおく. k の標数が 3 と異なるなら, C および C_1 は

$$C_2 : y^2 = x^3 - 27 c_4 x - 54 c_6$$

に同型である. C_1 および C_2 を (b) で扱ったもので, C はそれらと同型なアフィン平面曲線である. C の定義方程式を **Weierstrass 方程式**という. C の射影閉包を $\overline{C}$ における無限遠点は $[0:1:0]$ の唯一つの点で, 非特異点である. C あるいは $\overline{C}$ が特異点をもたないとき, C を**楕円曲線**という.

$$\Delta = -b_2^2 b_8 - 8 b_4^3 - 27 b_6^2 + 9 b_2 b_6 b_6 = (c_4^3 - c_6^2)/1728$$

$$b_8 = a_1^2 a_6 + 4 a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2$$

とおく. Δ を C の**判別式**という. $\Delta \neq 0$ のとき

$$j = j(C) = c_4^3/\Delta = 1728\, c_4^3/(c_4^3 - c_6^2)$$

とおき, C の ***j*-不変量**という.

定理 2.11 (1) 判別式 Δ は k の標数によらず $a_1, \cdots, a_6$ の式で表される. C の射影閉包 $\overline{C}$ が特異点をもたないことと $\Delta \neq 0$ であることは, k の標数によらず, 必要かつ十分である.

(2) Weierstrass 方程式で定義された楕円曲線 C, C' が同型であるための必要十分条件は $j(C) = j(C')$ である.

少し補足する. 本来, **楕円曲線**とは 1 次元アーベル多様体, 非特異完備代数曲線で代数的に定義された群演算をもつもののことをいう. (b) の代数曲線には, 無限遠点 $O = [0:1:0]$ を零元とする加法が有理写像の形で定義され, 1 次元アーベル多様体になるので楕円曲線と呼んだ. Weierstrass 方程式で定義された C に関しても, 無限遠点 $O = [0:1:0]$ を零元とする加法が全く同じ手続きで定義される. C も 1 次元アーベル多様体, 即ち楕円曲線である. 1 次元アーベル多様体としての楕円曲線に同型を考えるなら, 単に曲線としての同型ではなく, 加法も込めて同型をいうべきである. 実際には, 代数曲線の同型写像が零元を保つなら加法演算も保たれるので, Weierstrass 方程式で定義された楕円曲線の場合には無限遠点を保つ同型写像を考えればよい. アフィン曲線間の同型写像 (座標変換に過ぎない) と j-不変量の関係を計算したのが, 定理の (2) である. j-不変量は楕円曲線の不変量であって, 代数曲線の不変量ではないことを注意しておく.

(d) k の標数が 2 でないとする. 4 次多項式 $f(x) \in k[x]$ をとる. 4 次アフィン曲線 $C : y^2 = f(x)$ は, $f(x) = 0$ が重根をもたないなら非特異である. C の射影閉包 $\overline{C} : Y^2\,Z^2 = Z^4\,f(X/Z)$ は, 無限遠点 $[0:1:0]$ を特異点にもつ. 3 通りの手順で, C の非特異完備化を構成する.

まずは, 標準的なブローアップを行う. $\overline{C}$ は唯一つの無限遠点 $P_0 = [0:1:0]$ を特異点にもつので, P_0 のアフィン近傍を P_0 でブローアップしたアフィン代数曲線 C_0 と C との貼り合わせを作れば良い. 4 次式 f を $f(x) = a_0\,x^4 + a_1\,x^3 + a_2\,x^2 + a_3\,x + a_4$ と書く. P_0 を含むアフィン近傍

$$C_0' : z^2 = a_0\,x^4 + a_1\,x^3\,z + a_2\,x^2\,z^2 + a_3\,x\,z^3 + a_4\,z^4$$

をとる. 特異点 $(0,\,0) \in C_0'$ を解消したアフィン代数曲線を C_0 とおく. $(0,\,0) \in C_0'$ は 2 つの接線をもつ 2 重点 (結節点) なので, C_0 上の 2 つの点に分かれる. より具体的に C_0 は

$$C_0 : v^2 = a_0 + a_1\,u + a_2\,u^2 + a_3\,u^3 + a_4\,u^4 \quad (= u^4\,f(1/u))$$

で定義されるアフィン平面曲線で, f が重根をもたないので, 非特異である. 有理写像

$$\varphi_0 : C \ni (x,\,y) \longmapsto (1/x,\,y/x^2) \in C_0$$

により, C と C_0 は双有理同値になる. φ_0 は, $C \smallsetminus \{(0,\,\pm\sqrt{a_4})\}$ から $C_0 \smallsetminus \{(0,\,\pm\sqrt{a_0})\}$ への同型写像である. φ_0 で C と C_0 を貼り合わせた代数曲線を $\hat{C}$ とおく. このとき $\hat{C}$ は非特異完備代数曲線になる. 従って $\hat{C}$ が C の非特異完備化にあたる. $u = 1/x$ より, $\hat{C}$ における C の無限遠点は u-座標が 0 の C_0 の点 $(0 \pm \sqrt{a_0})$ の 2 点である. $(0,\,\sqrt{a_0})$ に対応する無限遠点を P_∞ とし, $(0,\,-\sqrt{a_0})$ に対応する無限遠点を P_∞' とする. このとき P_∞ の u-座標は 0 で v-座標は $\sqrt{a_0}$ である. また P_∞' の u-座標は 0 で v-座標は $-\sqrt{a_0}$ である. $k(C) = k(\hat{C}) = k(C_0) = k(u,\,v)$ なので, C の有理函数の無限遠点での値は, 有理函数を u, v で展開し, u, v-座標の値を代入すれば良い.

アフィン平面の平行移動と, ブローアップを組み合わせて非特異完備化を与える. $f(x) = 0$ の根 $\alpha \in k$ をとる.

$$f(x) = a_0\,(x-\alpha)^4 + a_1\,(x-\alpha)^3 + a_2\,(x-\alpha)^2 + a_3\,(x-\alpha)$$

となる. $f(x) = 0$ は重根をもたないので $a_3 \neq 0$ である. ここで

$$C_\alpha : v^2 = a_3\,u^3 + a_2\,u^2 + a_1\,u + a_0$$

は非特異 3 次アフィン平面曲線, つまり楕円曲線である. 有理写像

$$\psi : C \ni (x,\,y) \longmapsto (1/(x-\alpha),\,y/(x-\alpha)^2) \in C_\alpha$$

は, C から C_α への双有理同値を与える. C_α の射影閉包 $\overline{C}_\alpha$ は (b) より非特異射影平面曲線である. ψ の $\overline{C}_\alpha$ への延長を再び ψ と書くと,

$$\psi : C \ni (x,\,y) \longmapsto [x-\alpha : y : (x-\alpha)^2] \in \overline{C}_\alpha$$

ψ は C の $\overline{C}_\alpha$ への埋め込みなので, $\overline{C}_\alpha$ は C の非特異完備化である. またこのとき, 射影閉包 $\overline{C}$ における C の無限遠点 $[0:1:0]$ は, 2 点 $(0,\,\pm\sqrt{a_0}) \in C_\alpha$ に対応する.

最後のものは, 少し技巧的だが..... 4 次多項式 $f(x)$ の平方根 $\sqrt{f(x)}$ をベキ級数体 $k((1/x))$ で開平する.

$$\sqrt{f(x)} = \sqrt{a_0\,x^4 + a_1\,x^3 + a_2\,x^2 + a_3\,x + a_4} = b_0\,x^2 + b_1\,x + b_2 + b_3/x + \cdots$$

有理函数 $u = y - (b_0\,x^2 + b_1\,x)$, $v = x\,y - (b_0\,x^3 + b_1\,x^2 + b_2\,x)$, $w = x^2\,y - (b_0\,x^4 + b_1\,x^3 + b_2\,x^2 + b_3\,x)$ は,

$$u^2 + 2\,b_0\,w + 2\,b_1\,v - a_4 = 0\ , \quad u\,w - v^2 - b_2\,w + b_3\,v = 0$$

を満たす. どちらも w の 1 次式なので w を消去して, u と v の関係式を得る.

$$2\,b_0\,v^2 + 2\,b_1\,u\,v - a_3\,v = -u^3 + b_2\,u^2 + a_4\,u - a_4\,b_2$$

$a_0 = b_0^2$ に注意して $(u_0,\,v_0) = (-2\,b_0\,u,\,4\,b_0\,v)$ とおくと, u_0, v_0 は次を満たす.

$$v_0^2 - 2\,b_1\,u_0\,v_0 - 2\,b_0\,a_3\,v_0 = u_0^3 + 2\,b_0\,b_2\,u_0^2 - 4\,a_0\,a_4\,u_0 - 8\,a_0\,a_4\,b_0\,b_2$$

このままでも良いがさらに $(u_2,\,v_2) = (u_1,\,v_1 - b_1\,u_0 - b_0\,a_3) = (-2\,b_0\,u,\,4\,a_0\,v + 2\,b_0\,b_1\,u - b_0\,a_3)$ とおくと,

$$v_2^2 = u_2^3 + a_2\,u_2^2 + (-4\,a_0\,a_4 + a_1\,a_3)\,u_2 + (a_0\,a_3^2 - 4\,a_0\,a_2\,a_4 + a_1^2\,a_4)$$

なる関係式を得る. すべての係数がもともとの C の定義方程式の係数で書けていることを注意しておく.

$$C_\infty : y^2 = x^3 + a_2\,x^2 + (-4\,a_0\,a_4 + a_1\,a_3)\,x + (a_0\,a_3^2 - 4\,a_0\,a_2\,a_4 + a_1^2\,a_4)$$
$$\varphi_\infty : C \ni P \longmapsto (u_2(P),\, v_2(P)) \in C_\infty$$

φ_∞ は C から C_∞ への双有理写像になり, C_∞ の射影閉包 $\overline{C}_\infty$ は C の非特異完備化になる. 射影閉包 $\overline{C}$ における C の無限遠点 $[0:1:0]$ に対応する点は少し見え難くなっているが, C_∞ の唯一つの無限遠点と $(-2b_0b_2,\, 3b_0^2b_3) \in C_\infty$ の 2 点である.

問 11 (1) C の非特異完備化 $\hat{C}$, $\overline{C}_\alpha$, $\overline{C}_\infty$ は互いに同型であることを確かめよ.

(2) $\overline{C}_\alpha$ の加法を, 上の同型写像を通して $\hat{C}$ の上に描くことができる. その演算手続きを図形的に説明せよ.

(3) $\overline{C}_\infty$ の加法を, 上の同型写像を通して $\hat{C}$ の上に描くことができる. その演算手続きを図形的に説明せよ.

(e) k の標数が 2 でないとし, (b), (d) を次数に関して一般化したものを扱う. 重根をもたない多項式 $f(x) \in k[x]$ に対して, アフィン平面曲線 $C : y^2 = f(x)$ を考える. このとき C は非特異アフィン平面曲線になる. C (の非特異完備化) を**超楕円曲線** (hyperelliptic curve) という. 正しくは後で定義する種数によって呼び名が変わる (§3.5, §4.5). この曲線 C については f の次数 $n = \deg f$ で区別できる. $n \le 2$ のとき **2 次曲線** (conic), $n = 3,\, 4$ のとき**楕円曲線** (elliptic curve), $n \ge 5$ のとき**超楕円曲線**という. 2 次曲線は (a) で, $n = 3$ の楕円曲線は (b) で, $n = 4$ のものは (d) で扱った. 以下ここでは $n \ge 5$ の超楕円曲線 $C : y^2 = f(x)$ について非特異完備化を構成する.

4 次のときのブローアップと同じ手続きでをとる. $n = \deg f$, $m = [(n+1)/2]$ とおく. n が奇数のとき $n = 2\,m - 1$ で, n が偶数のとき $n = 2\,m$ である. C の射影閉包 $\overline{C}$ は唯一つの無限遠点 $[0:1:0]$ を特異点にもつ. その特異点を解消したアフィン代数曲線として,

$$C_0 : v^2 = u^{2m}\,f(1/u)$$

を取ることができる. C が非特異なので (従って f は重根をもたないので), C_0 もまた非特異アフィン平面曲線である. C_0 も超楕円曲線で, 次数は $2\,m$ を超えない. $f(x)$ の定数項が 0 でないなら次数は $2\,m$ で, 0 なら次数は $2\,m - 1$ である. 有理写像

$$\varphi_0 : C \ni (x,\, y) \longmapsto (1/x,\, y/x^m) \in C_0$$

により, C と C_0 は双有理同値になる. φ_0 で C と C_0 を貼り合わせた代数曲線を $\hat{C}$ とおく.

命題 2.12 $\hat{C}$ は C の非特異完備化で, 無限遠点は, 次数が奇数のとき 1 点で, 次数が偶数のとき 2 点である.

次数 $n = \deg f$ が偶数の超楕円曲線 $C : y^2 = f(x)$ において, $f(x) = 0$ の根 $\alpha \in k$ をとる. このとき $f(x) = a_0\,(x-\alpha)^n + a_1\,(x-\alpha)^{n-1} + \cdots + a_{n-1}\,(x-\alpha)$ と書ける.

$$C' : v^2 = a_{n-1}\,u^{n-1} + \cdots + a_1\,u + a_0$$

とおくと, C' は非特異アフィン平面曲線で, 特に次数が奇数の超楕円曲線である. C を C' は双有理同値で, 貼り合わせ $C \cup C'$ もまた C の非特異完備化である. $C \cup C'$ は C' の非特異完備化でもあるので, C と C' のどちらから始めても同じ非特異完備代数曲線 $C \cup C'$ を扱うことになる. 閉体上で扱う限り, 超楕円曲線として $\deg f$ が奇数のものをとり, 無限遠点は唯一つと考えても十分である.

超楕円曲線 $C : y^2 = f(x)$ において, 有理写像 $\iota : C \ni (x,\, y) \longmapsto (x,\, -y) \in C$ が定義される. ι は自分自身への同型写像で, 2 回繰り返すと恒等写像になる. ι を**超楕円対合** (hyperelliptic involution) という. C の非特異完備化は, C と双有理同値な超楕円曲線を貼り合せて作ったので, 無限遠点においても超楕円対合が定義される. f が奇数次のとき無限遠点は唯一つで, ι で不変である. f が偶数次のときは無限遠点は 2 つあり, ι で互いに移りあう. 無限遠点以外の点で ι で不変なものは, y-座標が 0 となるので, x-座標が $f(x) = 0$

の根になる n $(=\deg f)$ 個である. 無限遠点も含めて ι で不変な点は, f が奇数次のときは $n+1$ 個で, f が奇数次のときは n 個である. まとめて $m=[(n+1)/2]$ で表すと, 超楕円曲線 $C: y^2=f(x)$ の超楕円対合で不変な点は丁度 $2m$ 個である.

問 12 (1) アフィン平面曲線 $C: y^2=f_1(x)\,f_2(x)^2$ は $C': v^2=f_1(u)$ に双有理同値であることを示せ.
(2) アフィン平面曲線 $C: y^2=f(x)$ が非特異であることと, $f(x)=0$ が重根をもたないことは同値である.

(f) k の標数が 2 でも 3 でもないとする. $\overline{C}: F(X, Y, Z)=0$ を既約な 3 次射影平面曲線とする.

問 13 $\overline{C}$ が特異点をもつとする. 特異点は丁度 1 つで, $\overline{C}$ は射影直線に双有理同値であることを示せ.

$\overline{C}: F(X, Y, Z)=0$ を非特異 3 次射影平面曲線とし, $H_F(X, Y, Z)=0$ を C の Hesse 曲線とする. F は 3 次斉次多項式なので H_F も 3 次斉次多項式になる.

命題 2.13 C は丁度 9 個の変曲点をもつ.

P_∞ を $\overline{C}$ の変曲点とし, P_∞ での接線を ℓ とおく. 射影平面の斉次座標変換により (新しい斉次座標系を再び $X:Y:Z$ と書く), P_∞ を $[0:1:0]$ に ℓ を $\{Z=0\}$ に移すことができる. このとき

命題 2.14 $\overline{C}$ は Weierstrass 方程式で定義される射影平面曲線に同型である.

問 14 命題 2.12 を示せ. また, $\overline{C}$ が特異点をもつときにも, 上と同様の手続きで命題 2.12 が成り立つことを示せ.

(g) 簡単のため k の標数は 0 とする. 重根をもたない 4 次多項式 $f(x)\in k[x]$ をとる. アフィン平面曲線

$$C: y^3=f(x)$$

は特異点をもたない. 射影平面における C の射影閉包は

$$\overline{C}: Y^3\,Z=f(X/Z)\,Z^4$$

と表される. $\overline{C}$ における C の無限遠点は $[0:1:0]$ の 1 点で, 特異点ではない. 従って $\overline{C}$ は非特異射影曲線, つまり C の非特異完備化にあたる.

(h) 少し一般の場合を考える. ここでも簡単のため k の標数は 0 とする. アフィン平面曲線

$$C: y^3=f(x)\qquad (f(x)\in k[x])$$

をとる. C は, f の次数 $\deg f$ が 1 以下なら有理曲線, 2 次なら楕円曲線になり, 3 次のものは (f) で, 4 次のものは (g) で扱った. ここでは $\deg f\geq 5$ とする.

命題 2.15 (1) 多項式 $f_1, f_2, f_3\in k[x]$ で, $f=f_1\,f_2^2\,f_3^3$ を満たし $f_1\,f_2$ は重根をもたないものが存在する.
(2) アフィン平面曲線 $C_1: f_2(x)\,y^3=f_1(x)$, $C_2: f_1(x)\,y^3=f_2(x)$ は特異点をもたない.
(3) C_1, C_2 は $C: y^3=f(x)$ に双有理同値である.

n_1 次と n_2 次の多項式 $f_1, f_2\in k[x]$ は互いに素で重根をもたないとする. アフィン平面曲線 $C_1: f_2(x)\,y^3=f_1(x)$ の射影閉包を $\overline{C}_1$ とおく. 先に (f) や (g) で扱ったものを省くために, $n_1\geq 5$ または $n_2\geq 1$ とする.

命題 2.16 $s=n_1-n_2-3$ とおく. $\overline{C}_1$ における C_1 の無限遠点は,
(1) $s>0$ のとき, $[0:1:0]$ の 1 点で, 特異点である.
(2) $s=0$ のとき, $[0:1:0]$ と $[1:a:0]$ (a は $a^3=$ (f_1 の最高次の係数)/(f_2 の最高次の係数) なる k の元) の 4 点で, $[1:a:0]$ は非特異点である. $[0:1:0]$ は $\deg f_2>1$ のとき特異点で, $n_2=1$ のとき非特異点である.
(3) $s<0$ のとき, $[0:1:0]$ と $[1:0:0]$ の 2 点で, $[1:0:0]$ は特異点である. $[0:1:0]$ は $n_2>1$ のとき特異点で, $n_2=1$ のとき非特異点である.

簡単に, 特異点の様子を調べてみる. $s=0$, $s<0$ の場合も本質的に何も変わらないが, 並べて書くと煩雑になるので演習問題として省略し, ここでは $s>0$ の場合のみ述べる. $m=n_1-3$ とおく. (f) や (g) で扱ったものを除くと $m\geq 2$ としてよい.

命題 2.17 $\overline{C}_1$ の唯一つの特異点 $[0:1:0]$ は重複度 m の特異点である. $f_2(x)=\sum b_j\,x^j$ と書くとき接錐の定義方程式は $Z^s\,(\sum j!\,(m-j)!\,b_j\,X^j\,Z^{n_2-j})=0$ である.

問 15 $s\leq 0$ の場合に, 無限遠特異点における接錐を求めよ.

特異点を一つずつ解消していってもいいが, この曲線に対しては双有理同値な 4 つのアフィン代数曲線を貼り合わせればよい. $r=0$, ± 1 を $r\equiv n_1-n_2 \bmod 3$ にとる. $r=-1$ のとき $\tilde{f}_1(x)=x^{n_1+1}\,f_1(1/x)$, $\tilde{f}_2(x)=x^{n_2}\,f_2(1/x)$ とおき, $r=0$, 1 のとき $\tilde{f}_1(x)=x^{n_1}\,f_1(1/x)$, $\tilde{f}_2(x)=x^{n_2+1}\,f_2(1/x)$ とおく.

命題 2.18 $C_1: f_2(x)\,y^3=f_1(x)$, $C_2: f_1(x)\,y^3=f_2(x)$, $\tilde{C}_1: \tilde{f}_2(x)\,y^3=\tilde{f}_1(x)$, $\tilde{C}_2: \tilde{f}_1(x)\,y^3=\tilde{f}_2(x)$ は非特異アフィン平面曲線で, 互いに双有理同値である. 双有理写像で貼り合わせた代数曲線 $\hat{C}_1=C_1\cup C_2\cup\tilde{C}_1\cup\tilde{C}_2$ は非特異完備代数曲線で, C_1 の非特異完備化である.

問 16 双有理写像 $C_1\ni(x,\,y)\longmapsto(x,\,*)\in C_2$, $C_1\ni(x,\,y)\longmapsto(1/x,\,*)\in\tilde{C}_1$, $C_1\ni(x,\,y)\longmapsto(1/x,\,*)\in\tilde{C}_2$ を具体的に書き表せ. C_1 の座標函数 x, y を非特異完備化 $\hat{C}_1=C_1\cup C_2\cup\tilde{C}_1\cup\tilde{C}_2$ の有理函数に延ばしたとき, 有理写像としての x, $y:\hat{C}\to\mathbb{P}^1$ が全射正則写像であることを確かめよ.

問 17 非特異完備化 $\hat{C}_1$ における C_1 の無限遠点の個数を求めよ. (上の問いにも関係するが, $\hat{C}_1\smallsetminus C_1$ には x-座標函数の値が無限大の点だけでなく, 有限の値をとる点もある. それらすべてを "無限遠点" と呼ぶのは少し気が引けるが, x-座標函数の値ごとに "無限遠点" の個数を数えてみよ.)

(i) 簡単のため k の標数は 0 とする. $d>1$ とし, n_1 次と n_2 次の多項式 f_1, $f_2\in k[x]$ は互いに素で重根をもたないとする. このとき, アフィン平面曲線

$$C: f_2(x)\,y^d=f_1(x)$$

は特異点をもたない. C の射影閉包を $\overline{C}$ とおく.

命題 2.19 $s=n_1-n_2-d$, $m=n_1-d$ とおく. $s>0$ とする. $\overline{C}$ における C の無限遠点は $[0:1:0]$ の唯一つで, 重複度は m である. $f_2(x)=\sum b_j\,x^j$ と書くとき接錐は $Z^s\,(\sum j!\,(m-j)!\,b_j\,X^j\,Z^{n_2-j})=0$ で定義される.

問 18 $s\leq 0$ のとき, $\overline{C}$ における C の無限遠点を求め, 特異点であるかどうか調べよ. また, 接錐を計算せよ.

$|r|\leq d/2$ を $r\equiv n_1-n_2 \bmod d$ となるようにとる. $r=0$, ± 1 のとき, C の非特異完備化は (h) の命題 2.18 と全く同様にできる. $r\neq 0$, ± 1 のときは, 簡単ではないが標準的な手続きで特異点を解消することができる. 煩雑になるのと, ここまでで十分に例を挙げたと思うので, 以下は省略する. 冗長になるかもしれないが, $r=-1$ のとき $\tilde{f}_1(x)=x^{n_1+1}\,f_1(1/x)$, $\tilde{f}_2(x)=x^{n_2}\,f_2(1/x)$ とおき, $r=0$, 1 のとき $\tilde{f}_1(x)=x^{n_1}\,f_1(1/x)$, $\tilde{f}_2(x)=x^{n_2+1}\,f_2(1/x)$ とおくと, 命題 2.18 と全く同じ (y のベキ指数のみ異なる) 次の命題が成り立つ.

命題 2.20 $C_1: f_2(x)\,y^d=f_1(x)$, $C_2: f_1(x)\,y^d=f_2(x)$, $\tilde{C}_1: \tilde{f}_2(x)\,y^d=\tilde{f}_1(x)$, $\tilde{C}_2: \tilde{f}_1(x)\,y^d=\tilde{f}_2(x)$ は非特異アフィン平面曲線で, 互いに双有理同値である. 双有理写像で貼り合わせた代数曲線 $\hat{C}=C_1\cup C_2\cup\tilde{C}_1\cup\tilde{C}_2$ は非特異完備代数曲線で, それぞれのアフィン平面曲線の非特異完備化である.

問 19 $r\neq 0$, ± 1 とする.

(1) $C: f_2(x)\,y^d=f_1(x)$ の非特異完備化 $\hat{C}$ を 4 つの非特異アフィン平面曲線の貼り合わせで与えよ.

(2) C の座標函数 x, y を $\hat{C}$ の有理函数に延ばしたとき, x, $y:\hat{C}\to\mathbb{P}^1$ が全射正則写像であることを示せ.

(3) 非特異完備化 $\hat{C}$ における C の無限遠点の個数を求めよ.

§3　分岐被覆と Riemann-Hurwitz の公式

§3.1　代数曲線の有理写像

(a)　C を代数曲線とし, f を有理函数とする. $[1:f]:C\ni P\longmapsto[1:f(P)]\in\mathbb{P}^1$ は C から $\mathbb{P}^1$ への有理写像である. 有理写像 $\varphi=[f:g]:C\to\mathbb{P}^1$ は, f が零写像なら, $\varphi=[0:g]=[0:1]=\infty$ なので, ∞ に値をもつ定数写像である. f が零写像でないなら, f の零点を除いたところで $\varphi=[f:g]=[1:g/f]$ なので, φ は有理函数 g/f に対応する. 従って, C から $\mathbb{P}^1$ への有理写像の全体は, $k(C)\cup\{\infty\}$ に 1 対 1 に対応する.

(b)　代数曲線の非定数有理写像 $\varphi:C\to C'$ はほとんど全射なので, C' の有理函数 $f\in k(C')$ に対して $f\circ\varphi$ は C の有理函数になる. 体の準同型写像 $\varphi^*:k(C')\ni f\longmapsto f\circ\varphi\in k(C)$ が引き起こされる.

命題 3.1　(1)　非定数有理写像 $\varphi:C\to C'$ に対して, $k(C)$ は $\varphi^*k(C')$ の有限次拡大である.
(2)　体の中への k-同型 $\psi:k(C')\to k(C)$ に対して, $\varphi^*=\psi$ なる有理写像 $\varphi:C\to C'$ が唯一つ存在する.
(3)　k を含む $k(C)$ 部分体 K を $[k(C):K]<\infty$ にとる. このとき, 代数曲線 C_0 と有理写像 $\varphi:C\to C_0$ で $\varphi^*k(C_0)=K$ を満たすものが存在する.

(c)　C を代数曲線とし, $\varphi:C\to\mathbb{P}^n$ を射影空間への有理写像とする.

定理 3.2　非特異点 $P\in C$ において φ は正則である.

系 3.3　(1)　非特異代数曲線から射影空間への有理写像は, 正則写像である.
(2)　非特異完備代数曲線の間の有理写像は, 定数写像であるか全射である.
(3)　非特異完備代数曲線の間の写像度が 1 の有理写像は同型写像である.

問 20　(1)　非特異点の局所助変数をうまく使って, 定理 3.2 を示せ.
(2)　非特異完備代数曲線は射影空間に射影曲線として埋め込まれることを使って, 系 3.3 を示せ.

(d)　C, C' を非特異完備代数曲線とし, $\varphi:C\to C'$ を有理写像とする. φ が定数写像でないとき, 有限次拡大 $k(C)/\varphi^*k(C')$ の拡大次数を φ の**写像度**といい $\deg\varphi$ と書く. φ が非零定数写像のとき $\deg\varphi=0$ と定義し, 零写像に対して $\deg 0=-\infty$ とおく. $k(C)/\varphi^*k(C')$ が分離的拡大体のとき φ を**分離的** (separable) といい, $k(C)/\varphi^*k(C')$ が (純) 非分離的拡大体のとき φ を (**純**) **非分離的** ((purely) inseparable) という. $k(C)/\varphi^*k(C')$ の分離次数, 非分離次数を φ の**分離次数**, **非分離次数**といい, $\deg_s\varphi$, $\deg_i\varphi$ と書く.

(e)　k の標数が $p\ (>0)$ の場合を考える. $q=p^r$ に対して, **q-乗 Frobenius 写像** π を, 体 k 上では体の同型写像 $\pi:k\ni x\longmapsto x^q\in k$ として, 多項式環上では係数への作用 $\pi:k[X]\ni f\longmapsto f^\pi\in k[X]$ として, アフィン空間 $\mathbb{A}^n$, 射影空間 $\mathbb{P}^n$ 上では各成分への作用として定義する. 代数曲線 C に対して, $I(C)^\pi$ によって定まる代数曲線を C^π とおく. 自然な有理写像 $\pi:C\ni P\to C^\pi$ を, 代数曲線の **q-乗 Frobenius 写像**という.

命題 3.4　拡大 $k(C)/\pi^*k(C^\pi)$ は q 次純非分離的である. 従って π は q 次の純非分理的有理写像である.

命題 3.5　k の標数を $p>0$ とする. $\varphi:C\to C'$ を非特異代数曲線の非定数有理写像とする. $q=\deg_i\varphi$ とおき, π を q-上 Frobenius 写像とする. このとき, 分離的有理写像 $\psi:C^\pi\to C'$ で $\varphi=\psi\circ\pi$ となるものが存在する.

§3.2　有理写像の分岐点

(a) $\tilde{C}$, C を非特異完備代数曲線とし, $\varphi : \tilde{C} \to C$ を非定数有理写像とする. $P \in \tilde{C}$ とする. $\varphi(P) \in C$ は非特異点なので, 局所助変数 $t_{\varphi(P)} \in k(C)_{\varphi(P)}$ を Q で正則な有理式に表せる有理函数に取ることができる. $e_\varphi(P) = \mathrm{ord}_P(\varphi^* t_{\varphi(P)})$ を P での φ の**分岐指数** (ramification index) という. $k(C)_{\varphi(P)} = k((t_{\varphi(P)}))$ なので, 完備離散付値体 $k(\tilde{C})_P$ の中での $\varphi^* k(C)$ の閉包は $k((\varphi^* t_{\varphi(P)}))$ である. 分岐指数は完備体 $k(\tilde{C})_P / k((\varphi^* t_{\varphi(P)}))$ の拡大次数に等しい. 分岐指数が 2 以上のとき P を φ の**分岐点** (branch point) といい, φ は P で**分岐する** (ramified) という. 分岐指数が 1 のとき P を φ の**不分岐点** (unbranch point) といい, φ は P で**不分岐である** (unramified) という. φ が**不分岐**であるとは, $\tilde{C}$ のすべての点で不分岐なときをいう. $Q \in C$ に対して, $\varphi(P) = Q$ なる $P \in \tilde{C}$ を Q の上にある点という. Q の上のすべての点で $\varphi : \tilde{C} \to C$ が不分岐であるとき φ は Q で**不分岐であるといい**, そうでないとき Q で**分岐する**という. 分岐点 P での分岐指数が k の標数で割れるとき, **野性的分岐** (wild ramification) といい, k の標数で割れないとき, **順な分岐** (tame ramification) という.

命題 3.6 (1) すべての $Q \in C$ で, $\sum_{P \in \varphi^{-1}(Q)} e_\varphi(P) = \deg \varphi$ が成り立つ.
(2) 有限個の点を除く殆どすべての $Q \in C$ で, $\sharp \varphi^{-1}(Q) = \deg_s \varphi$ が成り立つ.
(3) 非定数有理写像の合成に関して, $e_{\psi \circ \varphi}(P) = e_\varphi(P)\, e_\psi(\varphi(P))$ が成り立つ.

問 21 代数体の拡大における素点の分岐指数と, 非特異完備代数曲線の間の非定数有理写像における曲線上の点の分岐指数は, 全く同等の概念であることを後者を函数体の言葉で書き直すことで説明せよ. 代数体の拡大での惰性にあたるものが, 代数曲線の場合に現れないことを説明せよ.

(b) $\varphi : \tilde{C} \to C$ を非特異完備代数曲線の非定数有理写像とする. 代数閉体 k 上の 1 変数代数函数体の有限次分離拡大 $k(\tilde{C}) / \varphi^* k(C)$ は単純拡大である. $k(\tilde{C}) / \varphi^* k(C)$ の生成元の最小多項式 $F(X) \in \varphi^* k(C)[X]$ をとる.

定理 3.7 $F(X)$ を完備離散付値体 $k((\varphi^* u_Q))$ 係数の多項式として既約元分解を $F(X) = F_1(X) \cdots F_r(X)$ とする. このとき $\varphi^{-1}(Q) = \{P_1, \cdots, P_r\}$ で, 適当に並べ替えて $e_\varphi(P_j) = \deg F_j$ となるようにできる.

$P \in \tilde{C}$, $Q = \varphi(P) \in C$ とする. t_P を P での局所助変数とし, $e = e_\varphi(P)$ とおく. Q での局所助変数 $u_Q \in k(C)$ の $k(\tilde{C}) \subset k((t_P))$ への持ち上げは, $\varphi^* u_Q = t_P^e + * t_P^{e+1} + \cdots$ と書ける. t_P^e の項の係数は, t_P か u_Q に織り込んで 1 になるようにした.

命題 3.8 分離的な非零有理函数 $f \in k(\tilde{C})$ に対して, $\mathrm{ord}_P(\varphi^* f) = e_\varphi(P)\, \mathrm{ord}_{\varphi(P)}(f)$ が成り立つ.

定理 3.9 f を非特異完備代数曲線 C の分離的非定数有理函数とする. 有理写像 $[1 : f] : C \to \mathbb{P}^1$ に関する $P \in C$ の分岐指数を $e_f(P)$ とおく. P が f の極なら $\mathrm{ord}_P(f) = -e_f(P)$ で, 極でないなら $\mathrm{ord}_P(f - f(P)) = e_f(P)$ である. f のすべての極の位数の和と f のすべての零点の位数の和は一致し, $\sum_P \mathrm{ord}_P(f) = 0$ が成り立つ.

(c) e が k の標数で割れない (野性的分岐でない) なら, $(\varphi^* u_Q)^{1/e} = (t_P^e + * t_P^{e+1} + \cdots)^{1/e} = t_P + * t_P^2 + \cdots \in k((t_P))$ と二項展開できる. 右辺は $k(C_1)_P$ の素元なので P での局所助変数になる. それを改めて t_P と置き直せば,

定理 3.10 P での分岐が野性的でないなら, 局所助変数 $t_P \in k(C)_P$ で, $t_P^e = \varphi^* u_Q$ なるものが取れる.

P での分岐が野性的 (分岐指数が k の標数で割り切れる) とする. u_Q の持ち上げの展開 $\varphi^* u_Q = t_P^e + \cdots \in k((t_P))$ に現れる t_P のすべてのベキ指数が k の標数 p (> 0) で割り切れるなら, 右辺は t_P のベキ級数の p 乗の形に表せるので, 拡大 $k((t_P)) / k((\varphi u_Q))$ は非分離的である. 同じことだが, 拡大 $k((t_P)) / k((\varphi^* u_Q))$ が分離的なら, $\varphi^* u_Q$ の t_P での展開に p と素なベキ指数の項が現れる. §4.2 で定義する局所微分の言葉での

言うと, 局所微分 $(du_Q)_Q$ の引き戻し $(\varphi^*(du_Q)_Q)_P$ は, $k((t_P))/k((\varphi^*))$ が分離的なら非零で, 非分離的なら零になる.

§3.3 局所助変数の具体的な形

(a) 与えられた代数曲線の特異点を無くし完備なものに取り替えることは重要である. 前節で具体的に計算したようにその様な操作は可能であった. そこでは, 特異点や無限遠点の近傍を双有理写像で非特異なものに貼りかえていく作業を行った. 代数曲線の場合には, 有限回の貼りかえで非特異完備なものに到達し, また非特異完備化された代数曲線は手順によらず同型であった.

双有理写像のもとで函数体は変わらない (体として同型である). 函数体から眺めると, 非特異完備化は与えられた函数体をもつ非特異完備代数曲線が同型を除いて唯一つ存在することを具体的な構成とともに保障する. 特異点であろうと無限遠点であろうと, 局所助変数を与えて, 任意の有理函数の Laurent 級数展開が計算できれば十分であろう. 話しを簡単にする (野性的分岐が現れないようにする) ため, この節で k の標数は 0 とする.

(b) C を代数曲線とし, C の非特異完備化を $\tilde{C}$ とおく. C の非特異点は自然に $\tilde{C}$ の (非特異) 点と思え, C の有理函数もまた $\tilde{C}$ の有理函数と思える. $P \in C$ を非特異点とし, $f \in k(C)$ を分離的非定数有理函数とする. 分離的有理写像 $f : \tilde{C} \to \mathbb{P}^1$ における P の分岐指数を e とおき, $a = f(P) \in \mathbb{P}^1$ とおく. 射影直線 $\mathbb{P}^1 = \mathbb{A}^1 \cup \{\infty\}$ のアフィン座標系 z をとり, $a \in \mathbb{A}^1$ のとき $u_a = z - a$ とし, $a = \infty$ のとき $u_\infty = 1/z$ とすると, u_a は $a \in \mathbb{P}^1$ の局所助変数である. 定理 3.10 より, $P \in \tilde{C}$ の局所助変数 $t \in k(\tilde{C})_P$ として, $t^e = f^* u_a$ となるものが取れる. ここで $k(C) = k(\tilde{C})$ だから, 局所助変数 t は $P \in C$ における局所助変数と思うことができる. 以上をまとめて

定理 3.11 代数曲線 C の非特異点 $P \in C$ をとる. C の有理函数 f に対し, $a = f(P)$ とおき, 分岐被覆 f における P の分岐指数を e とおく. このとき P の局所助変数 $t \in k(C)_P$ として, P が f の極でないとき $t^e = f - a$ で, P が f の極のとき $t^e = 1/f$ なるものが取れる.

問 22 超楕円曲線 $C : y^2 = f(x)$ (f は重根をもたない) に関して, $P_a = (a, *) \in C$ ($a \in \mathbb{A}^1 \subset \mathbb{P}^1$) における局所助変数を与えよ. また, 座標函数 x, y をその局所助変数で展開するにはどのようにすればよいか.

(c) 特異点にしろ無限遠点にしろ, 適当なアフィン近傍を取って考えればよい.

m, n を 2 以上の整数とする. k の標数は 0 であったので, m も n も標数で割り切れない. アフィン平面曲線

$$C : y^m = x^n f_0(x) \qquad (f_0(x) \in k(x),\ f_0(0) \neq 0, \infty)$$

を考える. $P = (0, 0) \in C$ は特異点である. 特異点 $P \in C$ の近傍の様子を知るには, P を除いた近傍を非特異なものに貼りかえればよい. 最も簡単な場合として n が m の倍数のときには, 定義方程式を $(y/x^{n/m})^m = f_0(x)$ と変形できる. $v = y/x^{n/m}$ と置けば, C は P に対応する点で非特異なアフィン平面曲線 $C' : v^m = f_0(x)$ に双有理同値になる. C と C' で x-座標函数は共通なので, P に対応する C' の点は x-座標函数の値が 0 の点になる. このとき v-座標函数の値は $f_0(0)$ の m 乗根だけ現れるので, P に対応する C' の点は丁度 m 個である.

次に易しい $n \equiv 1 \mod m$ のとき, 定義方程式は $(y/x^*)^m = x\, f_0(x)$ と書ける. C は P に対応する点で非特異な $C' : v^m = x\, f_0(x)$ に双有理同値である. この場合も C と C' で x-座標函数は共通なので, P に対応する C' の点は x-座標函数の値が 0 の点になる. v-座標函数の値は 0 なので, P に対応する C' の点は唯一つである.

これら 2 つの場合, C の特異点 P を解消した代数曲線 C' において, 定理 3.10 を有理函数 x に対して使うことができる. P に対応する非特異点での局所助変数 $t \in k(C)_P$ として, 最初の例では $t = x$, 次の例では

$t^m = x$ なるものが取れる. 座標函数 v を局所助変数 t で展開すると, 最初の例では $v = \sqrt[m]{f_0(t)} \in k[[t]]$, 次の例では $v = t\,\sqrt[m]{f_0(t^m)} \in k[[t]]$ と展開される. $\sqrt[m]{f_0(t^*)}$ は二項展開により t のベキ級数に表すことは簡単で, m 乗根の選び方により m 通りの展開をもつ. $t = 0$ での v の値は, 最初の例では $f_0(t)$ の m 乗根の選び方に従って m 個現れ, 次の例では $f_0(t^m)$ の m 乗根の取り方によらず値は 0 である. $P \in C$ に対応する C' の非特異点が, 最初の例では m 個, 次の例ではただ 1 個であったことを, 函数体の言葉で述べたものになっている.

(d) 特異点 $P \in C$ における函数体の解析を特異点解消を経ずに行う. 局所環 $k[C]_P$ の整閉包における極大イデアルごとに, 函数体の完備化と一意化元としての局所助変数が定まる. 結局のところ, 函数体のベキ級数体への稠密な埋め込みを与えればよい. 函数体 $k(C)$ は座標函数 x, y で生成される体で, P での局所環 $k[C]_P$ は, k 上 x, y で生成される環である. $a\,m + b\,n = d$ ($d = \gcd(m, n)$, a, $b \in \mathbb{Z}$) とし $t = x^a\,y^b \in k(C)$ とおく.

$$t^m = (x^a\,y^b)^m = x^{am}\,y^{bm} = x^{am}\,(x^n\,f_0(x))^b = x^{am+bn}\,f_0(x)^b = x^d\,f_0(x)^b$$
$$t^n = (x^a\,y^b)^n = x^{an}\,y^{bn} = (y^m/f_0(x))^a\,y^{bn} = y^{am+bn}\,f_0(x)^{-a} = y^d\,f_0(x)^{-a}$$

従って t は $k[C]_P$ 上整である. $f_0(0) \neq 0, \infty$ なので, 二項展開により $\sqrt[d]{f_0(x)} \in k[[x]]^\times$ となる.

$$t^{m/d} = x\,\sqrt[d]{f_0(x)}^{\,b}, \quad t^{n/d} = y\,\zeta\,\sqrt[d]{f_0(x)}^{\,-a} \quad (\text{ただし } \zeta^d = 1 \text{ とする})$$

と書けるので x, $y \in k[[t]]$ を得る. 座標函数が t で展開されたので, 埋め込み $k(C) = k(x, y) \hookrightarrow k((t))$ が定まる. 完備離散付値体 $k((t))$ の素元 t は $k(C)$ に属するので $k(C)$ は $k((t))$ で稠密である. 稠密な埋め込み $k(C) \hookrightarrow k((t))$ は, y を展開する際に現れた d 乗根 ζ の選び方に依存し, 丁度 d 個現れる. このそれぞれが, 局所環の整閉包における極大イデアルに対応し, C の非特異完備化における P の上の点に対応する. 以上まとめて

定理 3.12 m, n を 2 以上の整数とする. $a\,m + b\,n = d$ ($d = \gcd(m, n)$, a, $b \in \mathbb{Z}$) とし $t = x^a\,y^b \in k(C)$ とおく. このとき t は $P = (0, 0) \in C$ での局所助変数で $\mathrm{ord}_P(x) = m/d$, $\mathrm{ord}_P(y) = n/d$ となる. t による y の展開は丁度 d 通りあり, それぞれに対して函数体のベキ級数体への稠密な埋め込みが定まる. このことは, 非特異完備化により P が局所的に同相な丁度 d 個の非特異点に分かれることを意味する.

問 23 m, p, $q \geq 2$ で $\gcd(m, p, q) = 1$ とする. アフィン平面曲線 $y^m = x^p\,(1 - x)^q$ の特異点を求め, 各特異点での局所助変数を与えよ. また, 各特異点での座標函数 x, y の位数を計算し, 非特異完備化したときに幾つの非特異点に分かれるか調べよ.

問 24 超楕円曲線 $C : y^2 = f(x)$ (f は重根をもたない) の射影閉包において, 無限遠点の局所助変数を定理 3.12 に従って与えよ. また §2.6 (e) で与えた非特異完備化 $\hat{C} = C \cup C_0$ において, C の無限遠点の局所助変数を与えよ.

問 25 代数曲線 $C : y^d = f(x)$ ($f \in k[x]$, $d \in \mathbb{N}$) の射影閉包を $\overline{C}$ とおく. $P \in \overline{C}$ の局所助変数を与えよ.

§3.4 分岐被覆

(a) 非特異完備代数曲線の非定数有理写像 $\varphi : \tilde{C} \to C$ は全射正則写像である. $\varphi : \tilde{C} \to C$ を**分岐被覆** (branched covering) あるいは単に**被覆** (covering) という. φ を**被覆写像** (covering map) といい, $\tilde{C}$ を**被覆曲線** (covering curve), C を**基礎曲線** (base curve) という. 写像度 $\deg\varphi$ を**被覆次数** (covering degree) あるいは**葉数**という. φ が分離的 ($k(\tilde{C})/\varphi^*k(C)$ が分離拡大) のとき, $\tilde{C}$ は C を重複を込めて $\deg\varphi$ 重に覆っている. φ が分岐点をもたないとき**不分岐被覆** (unbranched covering) という. 被覆 $\varphi : \tilde{C} \to C$ が不分岐であるための必要十分条件は, C のすべての点の上に丁度 $\deg\varphi$ 個ずつ $\tilde{C}$ の点があることである. このとき $\tilde{C}$ は C を丁度 $\deg\varphi$ 重に覆う.

(b) 非特異完備代数曲線 C から自分自身への同型写像を C の**自己同型写像** (automorphism) という. それら全体のなす群を**自己同型群**といい $\mathrm{Aut}(C)$ で表す. 被覆 $\varphi : \tilde{C} \to C$ に対して, $\tilde{C}$ の自己同型 σ で $\varphi \circ \sigma = \varphi$ となるものを φ の**被覆変換** (covering transformation) という. それら全体のなす $\mathrm{Aut}(\tilde{C})$ の部分群を φ の**被覆変換群** (covering transformation gruop) といい G_φ で表す. G_φ は有限群で, その位数は $\deg\varphi$ を超えない. $\sharp G_\varphi = \deg\varphi$ となる被覆 φ を **Galois 被覆**といい, G_φ をその **Galois 群**という.

命題 3.13 $\varphi : \tilde{C} \to C$ が Galois 被覆であることと, 函数体の拡大 $k(\tilde{C})/\varphi^* k(C)$ が Galois 拡大であることとは同値である. 更にこのとき G_φ は $\mathrm{Gal}(k(\tilde{C})/\varphi^*\bar{k}(C))$ に同型である.

$\varphi : \tilde{C} \to C$ を Galois 被覆とする. $Q \in C$ の上のすべての点 $P \in \tilde{C}$ で分岐指数 $e_\varphi(P)$ は等しいので, $e_\varphi(Q) = e_\varphi(P)$ を Q での分岐指数とよぶ. 分岐指数は写像度 $\deg\varphi$ の約数になる.

定理 3.14 C を非特異完備代数曲線とし, G を有限群とする. このとき Galois 被覆 $\varphi : \tilde{C} \to C$ で $G_\varphi \simeq G$ となるものが存在する.

問 26 代数体の Galois 拡大における Hilbert の理論を, Galois 被覆に対して考えてみよ. (分解群, 惰性群, 分岐群にあたるものを定義してみよ.)

問 27 $\varphi : \tilde{C} \to C$ を Galois 被覆とする. 被覆曲線 $\tilde{C}$ の有理函数 $\tilde{h}$ が Galois 不変 (G_f 不変 : $\forall\sigma \in G_f$ に対して $\sigma^*\tilde{h} = \tilde{h}$) なら, 基礎曲線 C の有理函数 h で $\varphi^* h = \tilde{h}$ となるものが存在することを示せ.

(c) C を非特異完備代数曲線とする. 定数でない有理函数の写像度 (被覆 $C \to \mathbb{P}^1$ の葉数) の最小値 $d = \mathrm{gon}\,(C)$ を C の**最小被覆葉数** (gonality) という. このとき C を d-gonal 曲線という. 最小被覆葉数は射影直線 $\mathbb{P}^1$ の被覆としての最小の被覆次数なので, 1-gonal 曲線は射影直線と同型である. C が射影直線の 2 次の被覆であるとき, **超楕円的** (hyperelliptic) という. 2-gonal 曲線を**超楕円曲線** (hyperelliptic curve) という. 正確には (後で定義する) 種数も勘案し, 種数が 0 の非特異射影曲線を**有理曲線**, 種数が 1 の非特異射影曲線を**楕円曲線** (elliptic curve) といい, 種数が 2 以上の 2-gonal 曲線を**超楕円曲線**という. Riemann-Roch の定理の応用で述べるが, 有理曲線は 1-goanl になる (射影直線と同型になる) ので, 2-gonal 曲線の種数は 1 以上である. 2-gonal 曲線 C について, $\varphi : C \to \mathbb{P}^1$ を葉数 2 の被覆 (有理函数) とする. 函数体 $k(C)$ は有理函数体 $k(\mathbb{P}^1)$ の 2 次 (Galois) 拡大なので, 2 次の被覆は Galois 被覆になる. G_φ の生成元 $\iota : C \to C$ を C の**超楕円対合** (hyperelliptic involution) という.

C を位数 2 の自己同型 ι をもつ非特異射影曲線とする. ι は函数体 $k(C)$ の位数 2 の自己同型写像を引き起こす. その不変体 K に対応する非特異射影曲線を C' とすると, 2 次 Galois 被覆 $C \to C'$ が定まる. K が有理函数体であったなら C' として $\mathbb{P}^1$ がとれ, C は 2-gonal 曲線となる.

§3.5 Riemann 面と Riemann-Hurwitz の公式

(a) $k = \mathbb{C}$ 複素数体の場合を考える. 連結な複素 1 次元複素多様体 R を **Riemann 面**という. コンパクトな Riemann 面を**閉 Riemann 面**, コンパクトでない Riemann 面を**開 Riemann 面**という. 単位開円板や複素平面 $\mathbb{C}$, 複素上半平面は開 Riemann 面で, Riemann 球面 $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ や複素トーラス $T = \mathbb{C}/\Lambda$ ($\Lambda \subset \mathbb{C}$ は格子) は閉 Riemann 面である. Riemann 面は向きづけ可能な実 2 次元実解析的多様体で, 距離づけ可能で第二加算公理を満たすので, 三角形分割可能である. Riemann 面の三角形分割における単体の個数の交代和を **Euler 標数**といい $\chi(R)$ と書く. 閉 Riemann 面は幾つか穴の開いた閉じた曲面に位相同相である. 位相不変量である穴の個数を, 閉 Riemann 面 R の**種数** (genus) といい $g(R)$ と書く.

(b) $\mathbb{C}$ で定義された非特異完備代数曲線 R は, 連結かつコンパクトな複素 1 次元複素多様体, すなわち閉 Riemann 面である. 閉 Riemann 面としての種数を R の**種数**といい $g(R)$ で表す. また Euler 標数を $\chi(R)$ で表す. 複素射影直線は複素平面 $\mathbb{C}$ を 2 枚貼り合わせた Riemann 球面 $\hat{\mathbb{C}}$ なので, 種数は 0 である.

命題 3.15 (1) 閉 Riemann 面 $\hat{\mathbb{C}}$ の種数は 0 で, Euler 標数は 2 である.
(2) 複素トーラスの種数は 1 で, Euler 標数は 0 である.

閉曲面の 1 次整係数ホモロジー群の階数 (1 次 Betti 数 $b_1(R)$) は, 種数の 2 倍に等しい. 1 次元複素多様体 R 上の正則微分全体なす複素線形空間の次元は, 種数に等しい. Euler 標数は Betti 数の交代和に等しく,

定理 3.16 $\chi(R) = 2 - 2\,g(R)$

(c) Riemann 面の全射正則写像 $\pi : \tilde{R} \to R$ を**被覆**という. π を**被覆写像**, $\tilde{R}$ を**被覆面**, R を**基礎面**という. $Q \in R$ に対して, $\pi(P) = Q$ なる $P \in \tilde{R}$ を Q の上にある点という. Q の局所円板 (U, φ) ($U \subset R$ は Q の開近傍, $\varphi : U \to \mathbb{C}$ は埋め込み) と, P の開円板 $(\tilde{U}, \tilde{\varphi})$ を適当に選んで, $\varphi \circ \pi \circ \tilde{\varphi}^{-1}(z) = z^{e_P}$ と表すことができる. この自然数 e_P を P における π の**重複度** (multiplicity) あるいは**分岐指数**という. $e_P > 1$ となるとき P を π の**分岐点**とよぶ. 被覆 π が分岐点をもたないとき, φ は**不分岐**であるという. 分岐点の全体は高々加算個の孤立点からなる集合である. $\tilde{R}$ が閉 Riemann 面ならば R も閉 Riemann 面で, 分岐点の個数は有限である. $Q \in R$ の上にある点の個数は有界になるが, より詳しく $Q \in R$ の上にある点の重複度の和は一定である. その数 n_π を R 上の $\tilde{R}$ の**葉数**という.

定理 3.17 (Riemann-Hurwitz) $\chi(\tilde{R}) = n_\pi\,\chi(R) - \sum_{P \in \tilde{R}} (e_P - 1)$

系 3.18 (1) 被覆 $\pi : R \to \hat{\mathbb{C}}$ の葉数が 2 なら, 分岐点の個数は $4 - \chi(R)$ 個である.
(2) 被覆 $\pi : \tilde{R} \to R$ の葉数が 2 以上なら, $\chi(\tilde{R}) \le \chi(R)$ である. $\chi(R)$ が負なら, $\chi(\tilde{R}) < \chi(R)$ である.
(3) 葉数が 2 以上の $\hat{\mathbb{C}}$ の被覆は, 少なくとも 2 点で分岐する.

問 28 すべての分岐点を頂点に含む, 基礎面の三角形分割を, 被覆面の三角形分割に持ち上げることで, Riemann-Hurwitz の公式を示せ. 更にその系 3.18 を示せ.

問 29 $m, p, q \ge 2$ で $\gcd(m, p, q) = 1$ とする. アフィン平面曲線 $C/\mathbb{C} : y^m = x^p\,(1-x)^q$ の非特異完備化を $\hat{C}$ とおく. C の座標函数 x を $\hat{C}$ に延ばした有理函数を再び $x : \hat{C} \to \hat{\mathbb{C}}$ と書く. 次の問いに答えよ.
(1) $x^*\mathbb{C}(\mathbb{P}^1) = \mathbb{C}(x)$ を示し, 函数体の拡大次数 $[\mathbb{C}(\hat{C}) : \mathbb{C}(x)]$ を求めよ.
(2) 任意の $a \in \hat{\mathbb{C}}$ に対して $\sum_{P \in x^{-1}(a)} e_x(P) = m$ となることを確かめよ.
(3) 分岐被覆 x の分岐点と分岐指数を求めよ.
(4) $\chi(\hat{C})$ (あるいは $\hat{C}$ の種数) を m, p, q で表せ.
(5) $\chi(\hat{C}) = 2$ (あるいは $g(\hat{C}) = 0$) となる m, p, q を求めよ.
(6) $\chi(\hat{C}) = 0$ (あるいは $g(\hat{C}) = 1$) となる m, p, q を求めよ.

§4 Riemann-Roch の定理

§4.1 因子・因子類

(a) C を代数曲線とする. C のすべての点で生成された自由アーベル群を**因子群** (divisor group) といい $\mathrm{Div}(C)$ と書く. $\mathrm{Div}(C)$ の元を**因子**という. 因子 D は C の有限個の点の $\mathbb{Z}$-係数の形式和

$$D = n_1\,P_1 + \cdots + n_m\,P_m \quad (P_1, \cdots, P_m \text{ は相異なる点})$$

で表される. 係数 $n_1, \cdots, n_m$ が 0 でないとき, 上を因子 D の**被約表示**という. また, すべての C の点を渡る和

$$D = \sum_{P \in C} n_P\,P \quad (n_P \in \mathbb{Z} \text{ で, 有限個の } P \text{ を除いて } n_P = 0)$$

で表すこともできる. $n_P \neq 0$ となる $P \in C$ 全体の集合を D の**台** (support) といい $\mathrm{supp}(D)$ と書く. 因子群の零元はすべての係数が 0 の因子で 0 と書く. $\mathrm{supp}(0)$ は空集合である. 因子 D の係数の和 $\deg(D) = \sum n_P$ を因子 D の**次数**という. $\deg : \mathrm{Div}(C) \to \mathbb{Z}$ は準同型写像で, その核を $\mathrm{Div}^0(C)$ とおく. $P \in C$ に対して $\nu_P : \mathrm{Div}(C) \ni D \longmapsto n_P \in \mathbb{Z}$ とおくと, ν_P も準同型写像である. すべての $P \in C$ に対して $\nu_P(D) \geq 0$ となる因子 D を**整因子** (positeve (or effective) divisor) といい $D \geq 0$ と書く. D_0 を因子 D の**零因子** (zero divisor) といい, D_∞ を**極因子** (polar divisor) という.

(b) C を非特異完備代数曲線とする. C の零でない有理函数 $f \in k(C)^\times$ に対して,

$$\mathrm{div}(f) = \sum_P \mathrm{ord}_P(f)\, P$$

を f の**因子**という. 位数が正の項のみ集めた $\mathrm{div}(f)_0$ を f の**零因子**といい, 位数が負の項のみ集めて符号を変えた $\mathrm{div}(f)_\infty$ を f の**極因子**という. ord_P は加法的付値なので,

$$\mathrm{div} : k(C)^\times \longrightarrow \mathrm{Div}(C)$$

は準同型写像である. 函数の因子の次数は 0 なので, div の像は $\mathrm{Div}^0(C)$ に含まれる. 因子が 0 の函数は, 零点も極ももたないので, 非零定数函数である. div の核は $k^\times$ に等しい.

有理函数の因子を**主因子** (principal divisor) という. 主因子全体のなす群を**主因子群**といい $\mathrm{Div}^\ell(C)$ と書く. 因子 D_1, D_2 の差が主因子になるとき, D_1 と D_2 は**線形同値** (linearly equivalent) といい, $D_1 \sim D_2$ と書く. $\sim$ は因子全体の上に同値関係を定める. $\sim$ に関する因子の同値類を**因子類** (divisor class) という. 因子 D の属する因子類を $[D]$ と書く. 因子類全体のなす群 $\mathrm{Pic}(C) = \mathrm{Div}(C)/\mathrm{Div}^\ell(C)$ を C の**因子類群** (divisor class group) または **Picard 群**という. 主因子は次数が 0 なので因子類にも自然に次数を定義できる. 次数が 0 の因子類全体のなす群を $\mathrm{Pic}^0(C)$ と書く. 次の完全列を得る.

$$1 \longrightarrow k^\times \longrightarrow k(C)^\times \xrightarrow{\mathrm{div}} \mathrm{Div}^0(C) \longrightarrow \mathrm{Pic}^0(C) \longrightarrow 0$$

参考までに, 代数体 K における次の完全列との比較すれば, 因子類群は函数体のイデアル類群と言える.

$$1 \longrightarrow O_K^\times \longrightarrow K^\times \longrightarrow I_K \longrightarrow C_K = I_K/P_K \longrightarrow 0$$

因子は (分数) イデアル, 整因子は整イデアル, 主因子は単項イデアルに対応する. 代数体のイデアルは有限生成 (有限個の $K^\times$ の元で生成される) であることに対応して, 整因子は有限個の有理函数の共通零点で表すことができる. 特に 2-gonal 曲線 (楕円曲線, 超楕円曲線) は 2 次体に対応するので, 任意の整因子は 2 個の有理函数の共通零点で表すことができる. 代数曲線の点は代数函数体における加法的離散付値を定め, 代数体の素イデアルもまた代数体における加法的離散付値を定める. **素点**という意味から, 代数曲線の点は代数体の素イデアルに対応する. 本来, 代数多様体の (非特異) 点は座標環の極大イデアルに対応するべきものであるが, 代数閉体上定義された 1 次元の代数曲線の場合には座標環の自明でない素イデアルは極大イデアルになる. 代数体の整数環においても同様である. 以上をひと言でいえば, 非特異代数曲線の座標環も有限次代数体の整数環も **Dedekind 整域**である.

問 30 主因子の全体は因子群の部分群をなすこと, 線形同値は因子群の加法を保つ同値関係を定めることを示せ.

問 31 超楕円曲線 $C : y^2 = f(x)$ (f は重根をもたない) について, 有理函数 x, y, $x - a$, $f'(x)$ の因子を求めよ.

(c) $\varphi : C_1 \to C_2$ を非特異完備代数曲線の間の非定数有理写像とする.

$$C_2 \ni Q \longmapsto \varphi^*(Q) = \sum_{\varphi(P)=Q} e_\varphi(P)\, P \in \mathrm{Div}(C_1)$$

を, $\mathrm{Div}(C_2)$ へ線形に拡張したものを $\varphi^* : \mathrm{Div}(D_2) \to \mathrm{Div}(D_1)$ とおく. また

$$C_1 \ni P \longmapsto \varphi_*(P) = \varphi(P) \in C_2$$

を線形に拡張したものを $\varphi_* : \mathrm{Div}(C_1) \to \mathrm{Div}(C_2)$ とおく.

命題 4.1 非特異完備代数曲線 C の有理函数 f を有理写像 $f : C \to \mathbb{P}^1$ と思うと, f の零因子は $\mathrm{div}(f)_0 = f^*(0)$ で極因子は $\mathrm{div}(f)_\infty = f^*(\infty)$ に等しい. よって $\mathrm{div}(f) = f^*(0-\infty)$ である.

命題 4.2 $\varphi : C_1 \to C_2$ を非特異完備代数曲線の非定数有理写像とする. $D_j \in \mathrm{Div}(C_j)$, $f_j \in k(C_j)^\times$ に対して,

(1) $\deg(\varphi^* D_2) = (\deg \varphi)\,(\deg(D_2))$ (2) $\varphi^*\mathrm{div}(f_2) = \mathrm{div}(\varphi^* f_2)$

(3) $\deg(\varphi_* D_1) = \deg D_1$ (4) $\varphi_*\mathrm{div}(f_1) = \mathrm{div}(\varphi_* f_1)$

(5) $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*, \quad (\psi \circ \varphi)_* = \psi_* \circ \varphi_*$ (6) $\varphi_* \circ \varphi^* = \deg \varphi$

定理 4.3 非特異完備代数曲線の非定数有理写像 $\varphi : C_1 \to C_2$ は, 因子類群の準同型写像 $\varphi^* : \mathrm{Pic}^0(C_2) \to \mathrm{Pic}^0(C_1)$ と, $\varphi_* : \mathrm{Pic}^0(C_1) \to \mathrm{Pic}^0(C_2)$ を引き起こす. また $\varphi_* \circ \varphi^* : \mathrm{Pic}^0(C_2) \to \mathrm{Pic}^0(C_2)$ は $\deg(\varphi)$ 倍写像になる.

問 32 命題 4.2 を示せ.

§4.2 局所微分

(a) C を非特異完備代数曲線とする. 函数体の $P \in C$ での完備化 $k(C)_P$ は, P での局所助変数 $t \in k(C)_P$ をとって $k(C)_P = k((t))$ と展開できる. $f = \sum a_i t^i \in k(C)_P$ に対して, 通常のベキ級数の微分 $df/dt = \sum i\, a_i\, t^{i-1}$ を f の t に関する微分という. 微分の線形性や, 積の微分の公式などが成り立つ. $P \in C$ の別の局所助変数 t' に関する f の微分 df/dt' も定義され, 合成関数の微分により $df/dt = (df/dt')\,(dt'/dt)$ が成り立つ.

(b) $k(C)_P$ の元の組 $(g,\, f)$, $(g',\, f')$ が $g\, df/dt = g'\, df'/dt$ を満たすとき, $(g,\, f) \underset{P}{\sim} (g',\, f')$ と定義する. $\underset{P}{\sim}$ は ${k(C)_P}^2$ の同値関係をなす. $(g,\, f)$ で代表される同値類を**局所微分**といい, $(g\, df)_P$ で表す. 局所微分 $(g\, df)_P$ と $h \in k(C)_P$ の積を $f\,(g\, df)_P = (h\, g\, df)_P$ で定義することができる. ここで

$$(g\, df)_P = (g\, df/dt)\,(dt)_P\ , \quad g\, df/dt \in k(C)_P$$

となるので, 局所微分の全体は $k(C)_P\,(dt)_P$ に等しい.

定理 4.4 P での局所微分の全体は, $(dt)_P$ で生成される 1 次元 $k(C)_P$ 線形空間をなす.

(c) P の局所助変数 t, t' について $\mathrm{ord}_P(dt'/dt) = 0$ なので, $\mathrm{ord}_P(g\, df/dt)$ は局所助変数の取り方によらない. $\mathrm{ord}_P((g\, df)_P) = \mathrm{ord}_P(g\, df/dt)$ を局所微分の**位数**という. 位数が非負のとき, $(g\, df)_P$ は P で**正則**という. 位数が正のとき P を $(g\, df)_P$ の**零点**, 位数が負のとき P を $(g\, df)_P$ の**極**という. 局所微分 $(g\, df)_P$ の t での展開

$$(g\, df)_P = (g\, df/dt)\,(dt)_P = (\textstyle\sum a_i\, t^i)\,(dt)_P$$

を考える. t^{-1} の展開係数を**留数** (residue) といい $\mathrm{Res}_P((g\, df)_P)$ で表す.

定理 4.5 留数の定義は, 局所助変数 t の取り方によらない.

問 33 上の定理を示せ.

(d) 分離的非零有理函数 $f \in k(C)^\times$ をとり P での局所微分 $(df)_P$ を考える. P の分岐指数 $e = e_f(P)$ が k の標数で割れない (野性的分岐でない) とする. 定理 3.10 より, P での局所助変数 $t_P \in k(C)_P$ で $t_P^e = f^* u_a$ $(a = f(P) \in \mathbb{P}^1)$ なるものが取れる. u_a は $\mathbb{P}^1$ における a での局所助変数で, $\mathbb{P}^1 = \mathbb{A}^1 \cup \{\infty\}$ のアフィン座標 z をとり, $a \in \mathbb{A}^1$ のとき $u_a = z - a$ とおき, $a = \infty$ のとき $u_\infty = 1/z$ とおいた.

$$f = \begin{cases} a + t^e & (a \in \mathbb{A}^1) \\ t^{-e} & (a = \infty) \end{cases} \qquad (df)_P = df/dt\,(dt)_P = \begin{cases} e\, t^{e-1}\,(dt)_P & (a \in \mathbb{A}^1) \\ -e\, t^{-e-1}\,(dt)_P & (a = \infty) \end{cases}$$

定理 4.6　f を分離的非零有理函数とし, P での分岐指数 e は k の標数で割れないとする. このとき $df \neq 0$ で, $(df)_P$ の P での位数は, P が f の極なら $-e-1$ に, 極でないなら $e-1$ に等しい.

問 34　k の標数が 2 でないとする. 超楕円曲線 $C : y^2 = f(x)$　(f は重根をもたない) をとる. $P \in C$ において $\mathrm{ord}_P(dx)$, $\mathrm{ord}_P(dy)$ を計算せよ.

§4.3　微分

(a)　C の函数体 $k(C)$ の 2 元の組 (g, f), (g', f') が同値 $(g, f) \sim (g', f')$ であるとは, すべての $P \in C$ に対して局所微分が一致する ($(g\,df)_P = (g'\,df)_P$) ときをいう. (g, f) で代表される同値類を $g\,df$ で表し, C の**微分**という. C の微分の全体を Ω_C とおく. $h \in k(C)$ に対し, $h\,(g\,df) = hg\,df$ で微分と有理函数の積が定義される. すべての P に対して $(g\,df)_P = 0$ のとき $g\,df$ を零微分といい 0 で表す.

定理 4.7　$x \in k(C)$ とする. $dx \neq 0$ となるための必要十分条件は, x が $k(C)$ の分離元 ($k(C)/k(x)$ が分離拡大) となることである. 更にこのとき, すべての $P \in C$ に対して局所微分 $(dx)_P$ は零ではない.

定理 4.8　$dx \neq 0$ なる $x \in k(C)$ をとる. このとき C のすべての微分は $y\,dx$ ($y \in k(C)$) なる形に一意的に表される. 従って, 微分の全体 Ω_C は 1 次元 $k(C)$ 線形空間をなす.

(b)　$\varphi : C_1 \to C_2$ を非特異完備代数曲線の非定数有理写像とする.

$$\varphi^* : \Omega_{C_2} \ni g\,df \longmapsto \varphi^*(g\,df) = \varphi^* g\, d(\varphi^* f) \in \Omega_{C_1}$$

は k-線形写像である. $k(C_1)$ の部分体としての $k(C_2)$ を係数とする線形空間の線形写像ということもできる. どちらの意味においても,

定理 4.9　$\varphi : C_1 \to C_2$ が分離的ならば, 線形写像 $\varphi^* : \Omega_{C_2} \to \Omega_{C_1}$ は単射である.

(c)　$y\,dx$ を C の微分とする. $P \in C$ における局所微分 $(y\,dx)_P$ の留数 $\mathrm{Res}_P((y\,dx)_P)$ を $y\,dx$ の P での**留数**といい, $\mathrm{Res}_P(y\,dx)$ と書く.

定理 4.10 (留数定理)　微分 $y\,dx$ の留数は, 有限個の P を除いて 0 である. 更に留数の総和は 0 に等しい.

$$\sum_P \mathrm{Res}_P(y\,dx) = 0$$

(d)　$y\,dx$ を代数曲線 C の微分とする. $P \in C$ における局所微分 $(y\,dx)_P$ の位数 $\mathrm{ord}_P((y\,dx)_P)$ を $y\,dx$ の P での**位数**といい, $\mathrm{ord}_P(y\,dx)$ と書く. 位数が正のとき P を $y\,dx$ の**零点**, 位数が負のとき P を $y\,dx$ の**極**という. $\mathrm{div}(y\,dx) = \sum_P \mathrm{ord}_P(y\,dx)\,P$ は, 次の定理より C の因子となる. **微分因子**あるいは**標準因子** (canonical divisor) という. 定理 4.8 より, 微分因子の全体はひとつの因子類をなす. これを**微分因子類**あるいは**標準因子類**という. 極をもたない (C のすべての点で正則な) 微分を**第一種微分**あるいは**正則微分**という. 唯一つの点でのみ極をもつ微分を**第二種微分**という. 相異なる 2 点でのみ 1 位の極をもつ微分を**第三種微分**という. 零微分も第一種微分である. 第一種微分 (正則微分) の全体は, k 線形空間をなす. 留数定理より, 第二種微分は唯一つの極の位数が丁度 1 位のものは存在しない. 微分が丁度 1 位の極をもつためには, 少なくとも 2 点以上で極をもつ必要がある. 以下の 3 つの定理は, Riemann-Roch の定理の応用として得られる (§5.2) ものであるが, ここにまとめておく.

定理 4.11　(1)　任意の $P \in C$ と $m \geq 2$ に対して, P で丁度 m 位の極をもつ第二種微分 ω_{mP} が存在する.
(2)　P で高々 m 位の極をもつ第二種微分の全体は, 第一種微分と $\omega_{2P}, \cdots, \omega_{mP}$ の一次結合で表される.

定理 4.12 (1) $P, Q \in C$ で 1 位の極をもち, P, Q での留数がそれぞれ 1, -1 の第三種微分 ω_{PQ} が存在する.

(2) $P, Q \in C$ で高々 1 位の極をもつ第三種微分の全体は, 第一種微分と ω_{PQ} の一次結合で表される.

定理 4.13 代数曲線の零でない微分において, 零点と極の個数は高々有限個である.

(e) 野性的分岐をもたない分離元 $x \in k(C)$ をとる. 定理 4.6 より C のすべての点で, 微分 dx $(\neq 0)$ の位数が計算できる. 有理函数 (写像) が野性的分岐をもたないことを調べるのは面倒に思えるかもしれないが, k の標数が 0 ならすべての有理函数 (写像) は野性的分岐をもたないし, 有理函数 (写像) の写像度が k の標数より小さい場合も野性的分岐をもたないことを注意しておく. 有理函数としての x の極を $Q_1, \cdots, Q_s$ とし, その位数をそれぞれ e'_1 $(= -\mathrm{ord}_{Q_1}(x)), \cdots, e'_s$ とおく. 分岐被覆 $x : C \to \mathbb{P}^1$ の, 極を除く分岐点を $P_1, \cdots, P_r$ とし, 分岐指数をそれぞれ $e_1, \cdots, e_r$ とする. 極の位数はその点での分岐指数に等しいので, 2 位以上の極は分岐点でもある.

命題 4.14 $\mathrm{div}(dx) = \sum_j (e_j - 1)P_j - \sum_i (e'_i + 1)Q_i$ 従って, $\deg \mathrm{div}(dx) = \sum_j (e_j - 1) - \sum_i (e'_i + 1)$

全く同じものであるが, 少し書き換えてみる.

命題 4.15 $\mathrm{div}(dx) = \sum (e_x(P) - 1)\, P - 2\,(x)_\infty$ 従って, $\deg \mathrm{div}(dx) = \sum (e_x(P) - 1) - 2 \deg x$

§4.4 射影直線の微分

射影直線 $\mathbb{P}^1$ のアフィン部分直線 $\mathbb{A}^1$ のアフィン座標 z は函数体 $k(\mathbb{P}^1)$ を生成する. z の極は $\infty \in \mathbb{P}^1$ のみで, 位数は 1 である. 1 次被覆 $z : \mathbb{P}^1 \to \mathbb{P}^1$ は分岐点をもたない. 特に野性的分岐をもたないので, 命題 4.14 (4.15) より,

$$\mathrm{div}(dz) = -2\,\infty$$

となる. 標準因子の次数は -2 なので, $\mathbb{P}^1$ は零以外に正則な微分 (第一種微分) をもたない. また dz の極は ∞ のみなので dz は第二種微分である. 命題 4.14 より, 分離的な有理函数 f から得られる微分 df の極での位数は -2 以下なので, 第三種微分はこの形では得られない. $z \in k(C)$ は ∞ で 1 位の極をもつ. 任意の $a \in \mathbb{A}^1$ に対して $\mathrm{div}(z - a) = a - \infty$ となる. 従って

$$\mathrm{div}(dz/(z-a)) = \mathrm{div}(dz) - \mathrm{div}(z-a) = -2\,\infty - (a - \infty) = -\infty - a$$

となる. 微分 $dz/(z-a)$ は a, ∞ で 1 位の極をもつ第三種微分である. ∞ の局所助変数 $w = 1/z$ で

$$\frac{dz}{z-a} = \frac{1}{1/w - a}\,\frac{d(1/w)}{dw}\,dw = \frac{w}{1-aw}\,(-w^{-2})\,dw = (-w^{-1} - a - a^2\,w - a^3\,w^2 - \cdots)\,dw$$

より, ∞ での $dz/(z-a)$ の留数は -1 である. a の局所助変数 $t = z - a$ で展開して

$$\frac{dz}{z-a} = \frac{1}{t}\,\frac{d(t+a)}{dt}\,dt = t^{-1}\,dt$$

a での $dz/(z-a)$ の留数は 1 である. 以上まとめて,

命題 4.16 (1) 射影直線 $\mathbb{P}^1$ の標準因子の次数は -2 である. 特に $\mathbb{P}^1$ は零でない第一種微分をもたない.

(2) $a \in \mathbb{P}^1$ をとる. $x \in k(\mathbb{P}^1)$ を a を ∞ に移す一次分数変換とする. このとき a でのみ極をもつ第二種微分の全体は dx の $k[x]$ 倍 $(k[x]\,dx)$ に等しい.

(3) 2 点 $a, b \in \mathbb{P}^1$ をとる. $x \in k(\mathbb{P}^1)$ を a を ∞ に b を 0 に移す一次分数変換とする. このとき a と b でのみ 1 位の極をもつ第三種微分は dx/x の定数倍で表される. また $\mathrm{Res}_a(dx/x) = -1$, $\mathrm{Res}_b(dx/x) = 1$ である.

問 35 z を射影直線 $\mathbb{P}^1 = \mathbb{A}^1 \cup \{\infty\}$ のアフィン座標とする. 多項式 $f \in k[z] \subset k(x) = k(\mathbb{P}^1)$ に関して, df, $d(\frac{1}{f})$, $\frac{dz}{f}$ を第一種微分, 第二種微分, 第三種微分の和で表せ.

§4.5 $L(D)$ と種数

(a) 非特異完備代数曲線 C の因子 D に対して, 函数体 $k(C)$ の部分集合

$$L(D) = \{f \in k(C)^\times \,|\, \mathrm{div}(f) + D \geq 0\} \cup \{0\}$$

を考える. $f \in L(D)$ とすると, $P \in C$ に対して $\mathrm{ord}_P(f) + \nu_P(D) \geq 0$ なので $\mathrm{ord}_P(f) \geq -\nu_P(D)$ となる. f は $\nu_P(D) > 0$ となる点 P でのみ, 位数が $\nu_P(D)$ を超えない極をもつ. また $\nu_P(D) < 0$ なら f は P で少なくとも $\nu_P(D)$ 位の零をもたなくてはならない. 例えば $D = P$ のとき, $L(P)$ は P でのみ高々 1 位の極をもつ有理函数の全体で, $L(2\,P)$ は P でのみ高々 2 位の極をもつ有理函数の全体, $L(P - Q)$ は P でのみ高々 1 位の極をもち Q で少なくとも 1 位の零点をもつ有理函数の全体で, $L(P - 2Q)$ は P でのみ高々 1 位の極をもち Q で少なくとも 2 位の零点をもつ有理函数の全体である. 函数の因子の次数は 0 なので, 最後のもの ($L(P - 2Q)$) に含まれる有理函数は 0 に限る. $L(P - 2Q) = 0$ となる. また $L(P - Q)$ に含まれる函数の因子は $Q - P$ に限るので, $L(P - Q)$ に含まれる有理函数の比は定数になる. $L(P - Q)$ の次元は 1 を超えない. 定数函数はすべての点で正則なので $L(P)$ に含まれる. $f \in L(P) \smallsetminus k$ が存在するなら, f は P の外で正則で, P で 1 位の極をもつので, f の写像度は 1 である. 従って f は C から $\mathbb{P}^1$ への同型写像となる.

命題 4.17 $L(P) \supsetneqq k$ なる $P \in C$ が存在するなら, $C \simeq \mathbb{P}^1$ である.

命題 4.18 (1) $L(D)$ は k 線形空間をなす.
(2) $\deg(D) < 0$ のとき $L(D) = \{0\}$ である.
(3) $L(0) = k$ である. 従って $\mathrm{div}(f) = \mathrm{div}(g)$ $(f, g \in k(C))$ ならば $g = c\,f$ $(c \in k)$ となる.
(4) $D_1 \leq D_2$ ならば $L(D_1) \subset L(D_2)$ である.
(5) $D_1 - D_2 = \mathrm{div}(f)$ $(f \in k(C))$ ならば $L(D_2) \ni g \longmapsto g\,f \in L(D_1)$ は k 線形空間の同型写像である.
(6) 商空間 $L(D + P)/L(D)$ は k 線形空間として高々 1 次元である.

定理 4.19 $L(D)$ は有限次元 k 線形空間である.

k 線形空間 $L(D)$ の次元を $\ell(D)$ とおく. 命題 4.18 より $\deg(D) < 0$ のとき $\ell(D) = 0$ である. $\ell(0) = 1$ で, $\ell(D + P) \leq \ell(D) + 1$ が成り立つ. また $\deg(D) = 0$ のとき $\ell(D) \leq 1$ であるが, D が主因子のとき $\ell(D) = 1$ で, そうでないなら $\ell(D) = 0$ である.

定理 4.20 C を非特異完備代数曲線とする. すべての因子 D において $\deg D - \ell(D)$ は上に有界である.

問 36 命題 4.18, 定理 4.19, 定理 4.20 を示せ.

(b) C の微分 ω をとり, C の標準因子のひとつとして $K_C = \mathrm{div}(\omega)$ とおく. 因子 D に対して, 微分の全体 Ω_C の部分集合 $\Omega_C(D) = \{\omega \in \Omega_C \smallsetminus \{0\} \,|\, \mathrm{div}(\omega) \geq D\} \cup \{0\}$ をとる.

定理 4.21 $L(K_C - D) \ni f \longmapsto f\omega \in \Omega_C(D)$ は k 線形空間の同型写像である.

系 4.22 $\Omega_C(D)$ は有限次元 k 線形空間で, その次元は $\ell(K_C - D)$ に等しい.

第一種微分 (正則微分) 全体のなす k 線形空間 $\Omega_C(0)$ は, 標準因子 K_C の取り方によらず, $L(K_C)$ と同型である. このことからも, すべての標準因子は線形同値で, 微分の全体が 1 次元 $k(C)$ 線形空間をなすことがわかる. $P \in C$ で $m \geq 0$ 位の極をもつ第二種微分の全体 $\Omega_C(-m\,P)$ は $L(K_C + m\,P)$ と同型なので, P でのみ極をもつ第三種微分の全体 $\cup_m \Omega_C(-m\,P)$ は $\cup_m L(K_C + m\,P)$ に同型である. $P, Q \in C$ で高々 1 位の極をもつ第三種微分の全体 $\Omega_C(-P - Q)$ は $L(K_C + P + Q)$ に同型である.

問 37 $\ell(K_C + P) = \ell(K_C)$, $\ell(K_C + P + Q) \leq \ell(K_C) + 1$ となることを示せ.

(c) 第一種微分全体のなす k 線形空間 $\Omega_C(0)$ の次元 $(\ell(K_C))$ を C の**種数** (genus) といい $g(C)$ と書く. $k=\mathbb{C}$ とするとき, ここでの種数 (第一種微分全体の次元) は, 向きづけ可能な閉曲面の位相不変量であるところの穴の個数に一致する. また 命題 4.16 (1) より,

命題 4.23 射影直線の種数は 0 である.

(d) 種数は別の手続きによって定義されることがある. 定理 4.20 より $\deg(D)-\ell(D)+1$ は上に有界なので, その最大値 g' を C の**種数**という. $r(D)=g'-(\deg(D)-\ell(D)+1)$ を因子 D の**特異指数**といい, $r(D)=0$ となる因子を**正常因子**という.

定理 4.24 自然数 m を適当に取れば, $\deg(D)\geq m$ なる任意の因子 D は正常因子となる.

正常因子において $\ell(D)=\deg(D)-g'+1$ となるので, $L(D)$ の次元 $\ell(D)$ が簡単な式で与えられる. ここでの種数 g' と, 第一種微分全体の次元としての種数 $g(C)$ の関係を見ることは容易ではない. 次節の Riemann-Roch の定理により, 両者が等しい $(g'=g(C))$ ことが示される.

問 38 射影直線の任意の整因子 D に対して $\ell(D)=\deg D+1$ であることを示せ. 従って, ここでの種数の定義でも, 射影直線の種数は 0 である.

§4.6 Riemann-Roch の定理

定理 4.25 (Riemann-Roch) C を非特異完備代数曲線, K_C を標準因子とする. 次を満たす定数 g が存在する.

$$\ell(D)-\ell(K_C-D)=\deg D-g+1 \qquad (D \text{ は } C \text{ の任意の因子})$$

系 4.26 (1) $\ell(D)\geq \deg D-g+1$
(2) $\ell(K_C)=g$
(3) $\deg K_C=2g-2$
(4) $\deg D>2g-2$ ならば, $\ell(D)=\deg D-g+1$

系 (2) より定理の g は, 第一種微分全体のなす k 線形空間の次元に等しい. 系 (1) より $\deg D-\ell(D)+1$ は有界で g を超えず, (4) より $\deg D-\ell(D)+1=g$ なる因子 D がある. つまり g は $\deg D-\ell(D)+1$ の最大値にも等しい. Riemann-Roch の定理の定数 g は C の種数であり, §4.5 (c), (d) で定義した種数は同じ値になることがわかった. また, 系 (4) より定理 4.24 は $m=2\,g(C)-1$ に対して成り立つ.

問 39 Riemann-Roch の定理を使って, 系 4.26 を示せ.

問 40 (1) $\ell(D)>0$ ならば $\deg D\geq 0$ である. さらに $\deg D=0$ ならば D は主因子である.
(2) $\deg D=2\,g-2$ で $\ell(D)\geq g$ ならば D は標準因子である.
(3) $\ell(D)>0$ で $\ell(K_C-D)>0$ ならば $\ell(D)-1\leq \deg D/2$ である. (Cliford の定理)

§4.7 Riemann-Hurwitz の公式

(a) $\varphi: C_1\to C_2$ を非特異完備代数曲線の間の分離的な非定数有理写像とする. 線形写像 $\varphi^*:\Omega_{C_2}\to\Omega_{C_1}$ は単射である. $P\in C_1$ を取り, $Q=\varphi(P)\in C_2$ とおく. Q での局所助変数 u_Q の微分 du_Q の引き戻しを, P での局所助変数 t_P と有理函数 f で $\varphi^*\,du_Q=f\,dt_P$ と表す. $m_\varphi(P)=\mathrm{ord}_P(f)$ を P での φ の**微分指数** (differntial exponent) という. 微分指数は局所助変数 u_Q, t_P に依らない. 因子 $\sum_P m(P)\,P$ を φ の**分岐因子** (ramification divisor) という.

定理 4.27 (1) C_2 の微分 ω に対して, $\mathrm{ord}_P(\varphi^*\omega) \geq e_\varphi(P)\,\mathrm{ord}_Q(\omega) + m_\varphi(P)$ が成り立つ.
(2) P での分岐が野性的なら $m_\varphi(P) \geq e_\varphi(P)$ で, 不分岐または順な分岐のなら $m_\varphi(P) = e_\varphi(P) - 1$ である.

系 4.28 (1) C_2 の第一種微分 ω に対して $\varphi^*\omega$ も C_1 の第一種微分である. 従って $g(C_1) \geq g(C_2)$ が成り立つ.
(2) $C_1 \simeq C_2$ なら $g(C_1) = g(C_2)$ である.

(b) §3 で Riemann 面に関する Riemann-Hurwitz の公式に触れた. 三角形分割を被覆写像で持ち上げることで, Euler 標数の関係式としての Riemann-Hurwitz の公式が得た. Euler 標数が種数で表されるので, Riemann-Hurwitz の公式は種数の関係式に書き換えることもできる. 一般の体における代数曲線の場合, 微分を被覆写像で持ち上げる (定理 4.27) ことで, 標準因子の次数の関係式が得られる. 標準因子の次数を種数で表す (系 4.26 (3)) ことで, Riemann 面のときと全く同じ, 種数の関係式としての Riemann-Hurwitz の公式が得られる.

定理 4.29 (Riemann-Hurwitz) $\varphi : C_1 \to C_2$ を非特異完備代数曲線の分離的な非定数有理写像とする.

$$2\,g(C_1) - 2 \;=\; (2\,g(C_2) - 2)\,\deg\varphi + \sum_{P \in C_1} m_\varphi(P)$$

系 4.30 φ が同型写像でないとき, $g(C_1) \geq g(C_2)$ である. 特に $g(C_2) \geq 2$ のとき $g(C_1) > g(C_2)$ である.

問 41 Riemann-Hurwitz の公式を示せ.

問 42 C を種数が 2 以上の非特異完備代数曲線とする. 有理写像 $\varphi : C \to C$ が, 任意の第一種微分 ω について $\varphi^*\omega = \omega$ となるとき, $\varphi = \mathrm{id}$ であることを示せ.

問 43 自然数 d が k の標数で割り切れないとする. 代数曲線 $C : y^d = f(x)$ (の非特異完備化) の種数を求めよ.

問 44 k の標数が 2 でも 3 でもないとする. 代数曲線 $C : y^2 = x^3 + a\,x + b$ が特異点をもたないとする. 分岐被覆 $x : C \to \mathbb{P}^1$ と $y : C \to \mathbb{P}^1$ に対して Riemann-Hurwitz の公式を使って, C の種数が 1 であることを確かめよ.

§5 Riemann-Roch の定理の応用

§5.1 因子類群と基準写像

(a) C を種数 g の非特異完備代数曲線とする. C の因子 D の属する因子類を $[D]$ で表す. $P_\infty \in C$ に対して,

$$\Phi_{P_\infty} : C \ni P \longmapsto [P - P_\infty] \in \mathrm{Pic}^0(C)$$

を P_∞ を基点とする**基準写像** (canonical map) という. d を正の整数とし, $\mathrm{Sym}^g(C)$ を C の点の d 次の対称積 $C^d/\mathfrak{S}_d$ とする. 次数 d の整因子は対称積 $\mathrm{Sym}^d(C)$ の元と思える. この意味で, d 次対称積 $\mathrm{Sym}^d(C)$ は次数 d の整因子の全体に等しい. 次数 d の因子 D_∞ をとる.

$$\Phi_{D_\infty} : \mathrm{Sym}^d(C) \ni D \longmapsto [D - D_\infty] \in \mathrm{Pic}^0(C)$$

を D_∞ を基点とする**基準写像**という. Riemann-Roch の定理を使って, 次を示す.

定理 5.1 (1) $g=0$ ならば, $\mathrm{Div}^0(C)=\mathrm{Div}^\ell(C)$, $\mathrm{Pic}^0(C)=0$ である.
(2) $g\geq 1$ のとき, $\Phi_{P_\infty}: C\to \mathrm{Pic}^0(C)$ は単射である.
(3) $g\geq 1$ のとき, 次数 g の任意の因子 D_∞ に対して $\Phi_{D_\infty}: \mathrm{Sym}^g(C)\to \mathrm{Pic}^0(C)$ は全射である.

(b) 種数 $g=0$ のとき, 次数が -1 以上の因子 D に対して $\ell(D)=\deg(D)-g+1=\deg(D)+1$ が成り立つ. 次数が 0 の因子 $D\in\mathrm{Div}^0(C)$ に対して, $\ell(-D)=0+1=1>0$ より, 零でない有理函数 $f\in L(-D)$ が取れる. $\mathrm{div}(f)+(-D)\geq 0$ より $\mathrm{div}(f)\geq D$ となる. 両者の次数は 0 なので $\mathrm{div}(f)=D$ を得る. 従って D は主因子である. $\mathrm{Div}^0(C)=\mathrm{Div}^\ell(C)$ なので $\mathrm{Pic}^0(C)=0$ である.

(c) $\Phi_{P_\infty}(P)=\Phi_{P_\infty}(Q)$ なる $P, Q\in C$ をとる. $[P-Q]=[P-P_\infty]-[Q-P_\infty]=\Phi_{P_\infty}(P)-\Phi_{P_\infty}(Q)=0$ より, $\mathrm{div}(f)=P-Q$ となる有理函数 $f\in k(C)^\times$ が存在する. f の極因子は Q なので $f\in L(Q)$ となる. 命題 4.17 より $L(Q)=k$ なので, f は定数函数である. $\mathrm{div}(f)=0$ なので $P=Q$ となる. つまり Φ_{P_∞} は単射である.

(d) D_∞ を次数が g の因子とする. 任意の $D\in\mathrm{Div}^0(C)$ に対して,

$$\ell(D_\infty+D)\geq \deg(D_\infty+D)-g+1=g-g+1$$

となるので, 零でない $f\in L(D_\infty+D)$ が存在する. $D_0=\mathrm{div}(f)+(D_\infty+D)$ は次数が g の整因子なので, $D_0\in\mathrm{Sym}^g(C)$ である. $\Phi_{D_\infty}(D_0)=[D_0-D_\infty]=[\mathrm{div}(f)+D_\infty+D-D_\infty]=[D]$ より, $\Phi_{D_\infty}: \mathrm{Sym}^g(C)\to\mathrm{Pic}^0(C)$ は全射である.

§5.2 第一種, 第二種, 第三種微分

(a) C を種数 g の非特異完備代数曲線とする. C の種数は, 第一種微分全体のなす有限次元 k 線形空間の次元で定義した. 第二種微分, 第三種微分に関する定理 4.11, 4.12 を証明し, 定理 4.13 の成り立つことを確かめる. $k(C)$ の分離元 x をとり, $K_C=\mathrm{div}(dx)$ とおく.

(b) $P\in C$ で $m\geq 1$ 位の極をもつ第二種微分の全体 $\Omega(-m\,P)$ は, $L(K_C+m\,P)\ni y\longmapsto y\,dx\in\Omega(-m\,P)$ より, $L(K_C+m\,P)$ と同型である.

$$\ell(K_C+m\,P)=\deg(K_C+m\,P)-g+1=2g-2+m-g+1=g+m-1$$

なので, $m\geq 2$ とするとき, $\ell(K_C+m\,P)>\ell(K_C+(m-1)\,P)$ より有理函数 $y_m\in L(K_C+m\,P)\smallsetminus L(K_C+(m-1)P)$ が取れる. 微分 $y_m\,dx$ は P で丁度 m 位の極をもつ第二種微分である.

(c) $P, Q\in C$ でのみ高々 1 位の極をもつ第三種微分の全体 $\Omega_C(-P-Q)$ は, $L(K_C+P+Q)\ni y\longmapsto y\,dx\in\Omega_C(-P-Q)$ より, $L(K_C+P+Q)$ と同型である.

$$\ell(K_C+P+Q)=\deg(K_C+P+Q)-g+1=2g-g+1=g+1>g=\ell(K_C)$$

なので, 有理函数 $y_{PQ}\in L(K_C+P+Q)\smallsetminus L(K_C)$ が取れる. 微分 $y_{PQ}\,dx$ は P, Q で丁度 1 位の極をもつ第三種微分で, 適当に定数倍することで, P での留数を 1 に取れる. 留数定理より Q での留数が -1 になるので, $y_{PQ}\,dx$ は P, Q でそれぞれ留数が $1, -1$ の第三種微分である.

(d) ω を C の任意の微分とする. ω の因子 $\mathrm{div}(\omega)$ の極に現れる点 $P\in C$ とし, その位数を $m=-\mathrm{ord}_P(\omega)$ とする. t を P での局所助変数とする. 定理 4.12 の第二種微分 ω_{jP} は T^{-j} の項から始まる Laurent 級数に展開される. $b_2, \cdots, b_m\in k$ を適当に選んで, $\omega-(b_m\,\omega_{mP}+\cdots+b_2\,\omega_{2P})$ の Laurent 級数展開の t^{-m} の項から t^{-2} の項までを打ち消すように取れる. このとき ω' は P で高々 1 位の極をもつ. これを繰り返して, $\omega'=\omega-$(第二種微分の有限和) の極 $P_1, \cdots, P_r$ がすべて 1 位の極とすることができる. P_j における ω' の留数を c_j とおく. 留数定理より $c_1+\cdots+c_r=0$ である. P_j, P_r においてそれぞれ留数 $1, -1$ をもつ第三

種微分を ω_j とし, $\omega'' = \omega' - (c_1\,\omega_1 + \cdots + c_{r-1}\,\omega_{r-1})$ とおく. ω'' は $P_1, \cdots, P_{r-1}$ での留数が 0 なので, $P_1, \cdots, P_{r-1}$ で正則である. P_r での留数も $c_1 + \cdots + c_r = 0$ なので, P_r でも正則である. ω'' は第一種微分である.

§5.3 種数 0 の代数曲線

(a) C を種数 0 の非特異完備代数曲線とする. すべての因子 D に対して $\ell(D) = \deg D + 1$ が成り立つ. $P_\infty \in C$ をとる. $\ell(P_\infty) = 2 > \ell(0) = 1$ より $x \in L(P_\infty) \smallsetminus k$ なる非定数有理函数 x が取れる. x の極因子は P_∞ なので, $\deg(x) = 1$ である. $x : C \to \mathbb{P}^1$ は同型写像になるので $C \simeq \mathbb{P}^1$ である.

(b) x^2 の極因子は $2\,P_\infty$ なので, $L(2\,P_\infty)$ に属する. $\ell(2\,P_\infty) = 3$ より, $L(2\,P_\infty)$ は $1, x, x^2$ を基底にもつ. 同様にして $L(m\,P_\infty)$ は m 次以下の x の多項式の全体に等しい. 従って $\cup_{m\geq 0} L(m\,P_\infty) = k[x]$ が成り立つ.

$a \in \mathbb{A}^1 \subset \mathbb{P}^1$ に対して, $x(P_a) = a$ なる $P_a \in C$ をとる. $x(P_\infty) = \infty$ なので, 記号 P_a は $a \in \mathbb{P}^1$ に対して定まる. $a \mapsto P_a$ は同型写像 $x : C \simeq \mathbb{P}^1$ の逆写像にあたるので, $C = \{P_a \,|\, a \in \mathbb{P}^1\}$ である. $x(P_0) = 0$ より P_0 は x の零点である. $\mathrm{div}(x) = P_0 - P_\infty$ なので特に $1/x \in L(P_0)$ である. また $(x-a)(P_a) = x(P_a) - a = 0$ で $x - a \in L(P_\infty)$ なので, $\mathrm{div}(x-a) = P_a - P_\infty$ となる. $1/(x-a) \in L(P_a)$ を得る.

$a \in \mathbb{A}^1 \subset \mathbb{P}^1$ に対して $t_a = x - a$ は P_a で 1 位の零点をもつので P_a の局所助変数である. $a = \infty$ のとき $t_a = 1/x$ は P_∞ の局所序変数である. $a \in \mathbb{A}^1$ に対して $u_a = t_a = x - a$ をおき, $a = \infty$ に対して $u_a = 1$ とおく. このとき $a, b \in \mathbb{P}^1$ に対して, $\mathrm{div}(u_b/u_a) = P_b - P_a$ が成り立つ.

有理函数 $f \in k(C)$ をとる. $\mathrm{div}(f) = P_{b_1} + \cdots + P_{b_r} - P_{a_1} - \cdots - P_{a_r}$ と書く. 有理函数 $f_0 = u_{b_1} \cdots u_{b_r}/u_{a_1} \cdots u_{a_r}$ の因子は $\mathrm{div}(f)$ に等しいので f は f_0 の定数倍である. $k(C) = k(x)$ を得る.

(c) C の自己同型写像は, 函数体 $k(C) = k(x)$ の自己同型写像を引き起こす. $k(x)$ の自己同型写像は一次分数変換で表せるので, 結局 $\mathrm{Aut}(C) \simeq \mathrm{Aut}(k(x)/k) \simeq \mathrm{PSL}_2(k)$ が成り立つ.

簡単のため $k = \mathbb{C}$ とする. $\sigma : x \longmapsto 1/x$, $\tau : x \longmapsto (x-1)/x$ によって生成される $\mathrm{PSL}_2(\mathbb{C})$ の部分群は 3 次対称群 $\mathfrak{S}_3$ に同型である. $\mathbb{C}(C) = \mathbb{C}(x)$ における $\mathfrak{S}_3$ の固定体を $K = \mathbb{C}(x)^{\mathfrak{S}_3}$ とおく. K に対応する代数曲線を C_0 とおくと, C_0 の函数体を K に対応させる写像度 6 の有理写像 $C \to C_0$ がとれる. 従って C_0 の種数も 0 でなければならない. $u = x + \tau^* x + \tau^{*2} x \in k(x)$ をとる. u は τ の作用で不変なので $u \in \mathbb{C}(x)^{\langle\tau\rangle}$ となる. $[\mathbb{C}(x) : \mathbb{C}(u)] = 3$ なので $\mathbb{C}(x)^{\langle\tau\rangle} = \mathbb{C}(u)$ となる. $\mathbb{C}(x) = \mathbb{C}(u)(x)$ と思うと, x は $\mathbb{C}(u)$ 係数の 3 次多項式

$$X^3 - u\,X^2 + (u-3)\,X + 1 = 0$$

の根となる. この方程式は Shanks の最単純 3 次巡回方程式と呼ばれるもので, 3 次巡回拡大の生成的方程式系である. $u + \sigma^* u$, $u\,\sigma^* u$ は $\mathfrak{S}_3$-不変なので $\mathbb{K} = \mathbb{C}(x)^{\mathfrak{S}_3}$ に属する. $u + \sigma^* u = 3$ (定数) だが, $w = u\,\sigma^* u$ は $\mathbb{C}$ 上超越的で $[\mathbb{C}(x) : \mathbb{C}(w)] = 6$ となる. 従って $\mathbb{K} = \mathbb{C}(w)$ をえる. $\mathbb{C}(x) = \mathbb{C}(w)(x)$ とみれば, x は $\mathbb{C}(w)$ 上

$$X^6 - 3\,X^5 + (w-3)\,X^4 - (2\,w-11)\,X^3 + (w-3)\,X^2 - 3\,X + 1 = 0$$

で定義される. $\mathfrak{S}_3$-拡大に関する生成的方程式系である. u は $\mathbb{C}(w)$ 上 $U^2 - 3\,U + w = 0$ で定義され, $\mathbb{C}(u)$ 上の x の方程式から u にあたる部分を消去する (終結式を取ればよい) ことでも, 同じ 6 次方程式が得られる.

問 45 $\sigma : x \longmapsto 2/x$, $\tau : x \longmapsto 2\,(x-1)/x$ によって生成される $\mathrm{PSL}_2(\mathbb{C})$ の部分群は 4 次二面体群 D_4 に同型である. D_4-拡大 $\mathbb{C}(x)/\mathbb{C}(x)^{D_4}$ の定義方程式を求めよ.

問 46 射影直線 $\mathbb{P}^1$ の 4 点 $\{0, 1, -1, \infty\}$ を置換する一次分数変換全体のなす $\mathrm{PSL}_2(\mathbb{C})$ の部分群 G を求め, $\mathbb{C}(\mathbb{P}^1)/\mathbb{C}(\mathbb{P}^1)^G$ の定義方程式を求めよ. G の指数 2 の部分群 H に対して $\mathbb{C}(\mathbb{P}^1)/\mathbb{C}(\mathbb{P}^1)^H$ の定義方程式を求めよ.

§5.4 種数 1 の代数曲線

(a) C を種数 1 の非特異完備代数曲線とし, $P_\infty \in C$ をとる. $\ell(0)=1$, $\ell(n\,P_\infty)=n$ $(n\geq 1)$ となる. 従って, $L(0)=L(P_\infty)=k$ で $L(2\,P_\infty)\supsetneqq k$ である. $\ell(2\,P_\infty)=2$ なので, 非定数有理函数 $x\in L(2\,P_\infty)\smallsetminus k$ が取れ $L(2\,P_\infty)$ は 1, x を基底にもつ. x の極因子は $2\,P_\infty$ に等しい.

$\ell(3\,P_\infty)=3$ なので, $y\in L(3\,P_\infty)\smallsetminus L(2\,P_\infty)$ が取れ $L(3\,P_\infty)$ は 1, x, y を基底にもつ. y の極因子は $3\,P_\infty$ に等しい. x^2 の極因子は $4\,P_\infty$ なので, $L(4\,P_\infty)$ に含まれる函数として 1, x, y, x^2 が取れる. それぞれの極因子は 0, $2\,P_\infty$, $3\,P_\infty$, $4\,P_\infty$ なので k 上独立である. 1, x, y, x^2 は 4 次元 k 線形空間 $L(4\,P_\infty)$ の基底をなす. $L(5\,P_\infty)$ の基底として 1, x, y, x^2, $x\,y$ が取れ, $L(6\,P_\infty)$ の基底として 1, x, y, x^2, xy, x^3 が取れる. 以下同様にして, $\cup_{m\geq 0}L(m\,P_\infty)=k[x]+k[x]\,y$ となる.

(b) y^2 の極因子は $6\,P_\infty$ なので $y^2\in L(6\,P_\infty)$ である. 6 次元 k 線形空間 $L(6\,P_\infty)$ の基底は 1, x, x^2, x^3, y, xy なので, y^2 はそれら基底の線形結合で表せる. 適当に並べ替えて $y^2+a_1\,x\,y+a_3\,y=a_0\,x^3+a_2\,x^2+a_4\,x+a_6$ なる a_0, a_1, $\cdots$, $a_6\in k$ が存在する. 両辺に現れる項で極因子が $6\,P_\infty$ となるのは y^2 と x^3 のみなので, x^3 の係数 a_0 は消えない. 有理函数 x, y は線形空間の基底として選んだものであったので, 適当に (0 でない) 定数倍して取り替えても構わない. x, y をともに a_0 倍すると, 上の線形関係式は x^3 の係数を 1 にすることができる.

(c) C の有理函数 x, y の関係式に対応する, 3 次アフィン平面曲線

$$E: Y^2+a_1\,X\,Y+a_3\,Y=X^3+a_2\,X^2+a_4\,X+a_6$$

をとる. 一般に, 上の形の方程式を **Weierstrass 方程式**という. 係数の取り方によれば特異点をもつ場合もあるが, 特異点をもたないとき E を Weierstrass 方程式で定義された**楕円曲線**という.

命題 5.2 (1) C の有理函数 x, y の関係式で定義された E は特異点をもたない. つまり楕円曲線である.

(2) 有理写像 $\varphi: C\ni P\longmapsto (x(P),\,y(P))\in E$ は, C から $\bar{E}$ (E の射影閉包) への同型を引き起こす. 従って, 定義方程式 $Y^2+a_1\,X\,Y+a_3\,Y=X^3+a_2\,X^2+a_4\,X+a_6$ を C の (あるいは E の) **Weierstrass 標準形**という.

楕円曲線 E の函数体は座標函数 X, Y で生成される. 上の命題より C の函数体は E の函数体と同型で $\varphi^*X=x$, $\varphi^*Y=y$ なので, $k(C)$ は x, y で生成される. 以上のことをまとめると,

命題 5.3 C を種数が 1 の非特異完備代数曲線とする.

(1) 任意の $P_\infty\in C$ に対して, 極因子が $2\,P_\infty$ の有理函数 x と, $3\,P_\infty$ の有理函数 y が存在する.

(2) $L(m\,P_\infty)$ の基底として 1, x, $\cdots$, $x^{[m/2]}$, y, xy, $\cdots$, $x^{[(m-3)/2]}y$ が取れる.

(3) x, y を適当に定数倍して $y^2+a_1\,x\,y+a_3\,y=x^3+a_2\,x^2+a_4\,x+a_6$ なる a_1, $\cdots$, $a_6\in k$ が取れる.

(4) C の函数体は k 上 x, y で生成される. つまり $k(C)=k(x,\,y)$ である.

§5.5 種数 1 の代数曲線の加法

(a) 基準写像 $\Phi: C\ni P\longmapsto [P-P_\infty]\in \mathrm{Pic}^0(C)$ は, 定理 5.1 (2) より単射で, (3) より全射である. Φ を通して, 因子類群 $\mathrm{Pic}^0(C)$ の群構造を C の上に展開することができる. P, $Q\in C$ に対して $\Phi(P)+\Phi(Q)=\Phi(R)$ なる $R\in C$ が取れる. $P\oplus Q:=R$ により C の上に演算 $\oplus$ が定義され, C は P_∞ を零元とする加法群の構造をもつ.

$D=P+Q-P_\infty$ とおく. $\deg(D)=1$ なので $\ell(D)=1$ である. 零でない $f\in L(D)$ が存在する. $\mathrm{div}(f)+D$ は次数 1 の整因子なので, $\mathrm{div}(f)+D=R$ $(R\in C)$ と書ける. $R-P_\infty\sim D-P_\infty\sim P+Q-2P_\infty=P-P_\infty+Q-P_\infty$ より, $\Phi(R)=\Phi(P)+\Phi(Q)$ が成り立つ. 加法 $\oplus$ を計算するには $L(P+Q-P_\infty)$ に属する函数を求めればよい.

(b) $L(P+Q-P_\infty)$ に属する函数は P, Q で高々 1 位の極をもつ函数の全体 $L(P+Q)$ に含まれる. $\ell(P+Q)=2$ なので, $L(P+Q)$ の基底となる函数をもとめ, P_∞ で零点となるように係数の組を連立方程式を解く要領で決めればよい. 適当に与えた P, Q に対して $L(P+Q)$ を計算するのは少しコツが要る. 加法の定義を少し見直して, $P\oplus Q=R$ なる R を求める少し異なった手続きを与える.

$x\in L(2\,P_\infty)\smallsetminus k$ は 2 次の Galois 被覆 $x:C\to\mathbb{P}^1$ である. Galois 群 G_x の生成元を ι とおく. $P\in C$ に対して $P'=\iota(P)$ と書くことにする. $P\in C$ $(P\neq P_\infty)$ とする. 有理函数 $x-x(P)$ は P を零点にもつ. $x(P')=x(P)$ なので P' も $x-x(P)$ の零点である. P が x の分岐点でない $(P'\neq P)$ とき, $\mathrm{div}(x-x(P))=P+P'-2\,P_\infty$ が成り立つ. P が x の分岐点のとき, P での分岐指数が 2 なので $x-x(P)$ は P で 2 位の零点となる. よって $\mathrm{div}(x-x(P))=2\,P-2\,P_\infty$ となる. どちらにせよ $\mathrm{div}(x-x(P))=P+P'-2\,P_\infty$ となる. $[P'-P_\infty]=-[P-P_\infty]$ なので $\Phi(P')=-\Phi(P)$ を得る. P が x の分岐点のとき $2\Phi(P)=0$ となる. $\Phi(P)+\Phi(Q)=\Phi(R)$ ということは, $\Phi(R')=-\Phi(R)$ なので $\Phi(P)+\Phi(Q)+\Phi(R')=0$ に同等である. このとき $P+Q+R'-3\,P_\infty\sim 0$ なので $f\in L(3\,P_\infty)$ で $\mathrm{div}(f)=P+Q+R'-3\,P_\infty$ となるものが取れる. $L(3\,P_\infty)$ の基底は 1, x, y なので f は x, y の 1 次式である. 同型 $C\simeq\bar{E}$ により C は射影平面に埋め込まれる. このとき x, y はアフィン座標系 X, Y に対応するので, x, y の 1 次方程式 $f=0$ は射影平面内の直線に対応する. この意味で $f=0$ は直線の方程式ということができ, f の零点 P, Q, R' は直線 $f=0$ の上の点といえる.

以上まとめる. P, $Q\in C$ とする. ℓ を P と Q を通る直線とする. $P=Q$ のときは ℓ として P での C の接線をとる. ℓ は C と P, Q, R で交わる. このとき $\Phi(P)+\Phi(Q)=\Phi(R')$ となるので, $P\oplus Q=R'$ である. ここで R' は $x(R')=x(R)$ なので, 直線 $x-x(R)=0$ と C との交点として計算できる.

(c) $x(P)\neq x(Q)$ の場合に $L(P+Q-P_\infty)$ を直接与えてみる. P', Q' を通る直線の方程式を $a+b\,x+c\,y=0$ とおくと, $\mathrm{div}(f)>P'+Q'-3\,P_\infty$ である.

$$\mathrm{div}\Big(\frac{a+b\,x+c\,y}{(x-x(P))\,(x-x(Q))}\Big)>P_\infty-P-Q$$

なので, $h=(a+b\,x+c\,y)/(x-x(P))(x-x(Q))\in L(P+Q-P_\infty)$ である. 実際 P が分岐点でないとき, P の局所助変数として $t=x-x(P)$ がとれる. 有理函数 h を t で展開すると

$$h=\frac{a+b\,x(P)+c\,y(P)}{x(P)-x(Q)}\,t^{-1}+\cdots$$

P が分岐点のとき, P の局所助変数として $t^2=x-x(P)$ がとれる. $y=y(P)+b_1\,t+\cdots$ と t で展開すると,

$$h=\frac{c\,b_1}{x(P)-x(Q)}\,t^{-1}+\cdots$$

どちらの場合も t^{-1} の係数は零でないので, h が P で丁度 1 位の極をもつが局所助変数で計算できる.

問 47 $x(P)=x(Q)$ となる P, Q のすべての組み合わせに対して, $L(P+Q-P_\infty)$ を求めよ.

問 48 基準写像の基点を取り替えることで, C の上に引き起こされる加法演算はどの様に変わるか.

(d) 基準写像の引き戻しにより定義される, 種数 1 の代数曲線上の加法演算は, 基準写像の基点の選び方によって演算としては異なる. 基点は加法の零元なので, 零元を指定することで種数 1 の代数曲線上に加法演算が定義される. これまで少し曖昧に使っていたが, 楕円曲線とは 1 次元アーベル多様体のことで, 種数 1 の代数曲線のことではない. 種数が 0 か 2 以上の代数曲線の上には, 有理写像としての加法演算が定義できないので, 1 次元アーベル多様体となりうる代数曲線は種数が 1 のものに限る. 種数 1 の代数曲線 E には $O\in E$ を零元とする加法演算が定義できるので, 組 (E,O) を**楕円曲線**という. E が Weierestrass 方程式で定義されるときに限り, 無限遠点 $O=[0:1:0]$ を零元とする加法演算を暗黙のうちに仮定し, 単に E を楕円曲線と呼ぶ.

§5.6 種数 1 の代数曲線の微分

(a) Riemann-Roch の定理, あるいは種数の定義より, 第一種微分が存在しその全体は 1 次元 k 線形空間をなす. 命題 5.2 で得た, Weierstrass 方程式で定義された楕円曲線 (種数 1 の非特異完備代数曲線) に対して, 第一種, 第二種, 第三種微分を具体的に微分を計算してみる.

$$E : y^2 + a_1\,x\,y + a_3\,y = x^3 + a_2\,x^2 + a_4\,x + a_6$$

とする. $x : E \to \mathbb{P}^1$ は 2 次 Galois 被覆で, Galois 群 G_x の生成元を ι とおく. 簡単のため $\iota(P) = P'$ と書く. $x \circ \iota = x$ なので $x(P') = x(P)$ が成り立つ. $y(P), y(P')$ は y の 2 次方程式 $y^2 + a_1\,x(P)\,y + a_3\,y = x(P)^3 + \cdots$ の 2 根になるので, $y(P) + y(P') = -a_1\,x(P) - a_3$ となる. $y(P') = -y(P) - a_1\,x(P) - a_3$ なので,

$$\iota : E \ni P = (x,\, y) \longmapsto P' = (x,\, -y - a_1\,x - a_3) \in E$$

と表せる. P が x の分岐点 ($P' = P$) となるとき, $y(P) = y(P')$ なので y の 2 次方程式 $y^2 + a_1\,x(P)\,y + a_3\,y = x(P)^3 + \cdots$ が重根をもつときである. k の標数が 2 と異なるとき, 分岐点 P の x-座標は $(a_1\,x + a_3)^2 - 4(x^3 + a_2\,x^2 + a_4\,x + a_6) = 0$ の根で, y-座標は $y = -(a_1\,x(P) + a_3)/2$ で表される. k の標数が 2 のときは, 分岐点の x-座標は $a_1\,x + a_3 = 0$ を満たす. 以下簡単のため k の標数が 2 と異なるとする. 定義多項式の右辺の y の項を平方の形にまとめると, (y の式)^2 = (x の 3 次多項式) と書ける. x の分岐点は, この右辺の 3 次方程式の根を x 座標とする 3 点 (P_1, P_2, P_3 とおく) と, $P_\infty = [0:1:0]$ である.

問 49 Riemann-Hurwitz の公式を使って, 2 次被覆 $x : E \to \mathbb{P}^1$ の分岐点の個数が, k の標数が 2 と異なるとき 4 個で, k の標数が 2 のとき 2 個であることを示せ.

(b) 暫く k の標数が 2 と異なる場合を考える. 有理函数 x の極は P_∞ のみで, その位数は 2 である. 被覆 $x : C \to \mathbb{P}^1$ の, 極以外の分岐点は P_1, P_2, P_3 の 3 点で分岐指数はすべて 2 である. §4.2, §4.3 に従って, E の微分 dx の因子を計算すると,

$$(dx) = P_1 + P_2 + P_3 - 3\,P_\infty$$

となる. 標準因子を直接計算することで, 種数が 1 の場合の $\deg \mathrm{div}(dx) = 0 = 2\,g(E) - 2$ が確かめられた.

さて, $y_0 = 2\,y + a_1\,x + a_3 \in L(3\,P_\infty)$ を考える. y_0 は E の定義方程式を y で偏微分したものであるが, E の定義方程式の y を含む項を平方の形にまとめたときに現れる項でもある. y_0 の零点は無限遠点を除く x の分岐点になるので, $\mathrm{div}(y_0) = P_1 + P_2 + P_3 - 3\,P_\infty$ である.

$\omega_E = dx/y_0$ とおく. ω_E を E の**不変微分**あるいは **Néron 微分**という.

$$\mathrm{div}(\omega_E) = \mathrm{div}(dx) - \mathrm{div}(y_0) = 0$$

なので, E の微分因子類は主因子類に等しい. ω_E は極をもたないので E の第一種微分である. 他の第一種微分 ω についても $\mathrm{div}(\omega) = 0$ なので, ω/ω_E は定数函数になる. E の第一種微分の全体は 1 次元 k 線形空間をなす.

$f \in k(E)^\times$ を取ると $\mathrm{div}(f\,\omega_E) = \mathrm{div}(f)$ である. P_∞ でのみ極をもつ第二種微分は, P_∞ でのみ極をもつ有理函数 f をとって $f\,\omega_E$ と表せる. P_∞ でのみ極をもつ有理函数の全体は $\cup_{m\geq 0} L(m\,P_\infty) = k[x] + k[x]\,y$ なので, P_∞ でのみ極をもつ第二種微分の全体は $(k[x] + k[x]\,y)\,\omega_E$ に等しい. 一般の $P \in E$ に対しても同様に P でのみ極をもつ有理函数の全体を求めればよい. $\ell(0) = \ell(P) = 1 < \ell(2\,P) = 2 < \ell(3\,P) = 3$ なので, P でのみ極をもつ有理函数 x_P, y_P で, それぞれの P での位数が丁度 2 と 3 のものが存在する. P_∞ のときと同様に, P でのみ極をもつ第二種微分の全体は $(k[x_P] + k[x_P]\,y_P)\,\omega_E$ となる.

$P, Q \in C$ ($P \neq Q$) で 1 位の極をもつ第三種微分は, $L(P + Q)$ に属する有理函数に ω_E をかければよい. $L(P + Q)$ は §5.5 (c) で作ってあるので, P, Q でのみ 1 位の極をもつ第三種微分の全体は $L(P + Q)\,\omega_E$ で表される. $\ell(P + Q) = 2$ なので, P, Q でのみ 1 位の極をもつ第三種微分の全体は k 線形空間として 2 次元である.

問 50 $P \neq P_\infty$ とする. $x_P = 1/(x - x(P)) \in L(2\,P)$, $y_P = (y_0 - y_0(P'))/(x - x(P))^2 \in L(3\,P)$ を示せ.

(c) k 標数が 3 と異なる (標数が 2 の場合も含む) とする. 写像度 3 の有理函数 y から微分 dy を考える. $x_0 = 3x^2 + 2a_2\,x + a_4 - a_1\,y$ (E の定義方程式を x で偏微分したもの) とおく. 上と同様にして

$\mathrm{div}(dy) = \mathrm{div}(x_0)$ が計算できる．従って dy/x_0 は第一種微分で, (標数が 2 でないとき) ω_E の定数倍である．実際には E の定義方程式の全微分を計算することで $dx/y_0 = dy/x_0$ が示される．標数が 2 のとき $\omega_E = dy/x_0$ で不変微分を定義することができる．

問 51　(1)　k の標数が 2, 3 と異なるとき $dx/y_0 = dy/x_0$ であることを確かめよ．
(2)　不変微分 ω_E は, E の加法に関して不変であることを示せ．

(d)　以上, E の微分についてまとめる．

命題 5.4　E を Weierstrass 方程式で定義された種数 1 の非特異完備代数曲線とする．
(1)　$dx/(2y + a_1\,x + a_3)$, $dy/(3\,x^2 + 2\,a_2\,x + a_4 - a_1\,y)$ が E の微分として零でないなら, 両者は等しい．
(2)　上の微分を ω_E とおく．このとき $\mathrm{div}(\omega_E) = 0$ である．
(3)　E の第一種微分の全体は $k\,\omega_E$ に等しい．特に第一種微分の全体は 1 次元 k 線形空間をなす．
(4)　x_P, y_P を $P \in E$ でのみ極をもつ有理函数で, それぞれの P での位数が丁度 2, 3 のものとする ($P = P_\infty$ のとき, $x_P = x$, $y_P = y$ と取れる)．このとき P における第二種微分の全体は $(k[x_P] + k[x_P]\,y_P)\,\omega_E$ に等しい．
(5)　$P, Q \in C$ $(P \neq Q)$ でのみ 1 位の極をもつ第三種微分の全体は $L(P + Q)\,\omega_E$ に等しい．特に P, Q でのみ高々 1 位の極をもつ第三種微分の全体は 2 次元 k 線形空間をなす．

§5.7　Weierstrass 点

(a)　C を種数 g の非特異代数曲線とし, $P \in C$ をとる．P の外で正則で, P で n 位の極をもつ函数の全体は $L(n\,P)$ なので, P でのみ極をもつ函数の全体は $\cup_n L(n\,P)$ で与えられる．P で丁度 n 位の極をもつ函数は, $L(n\,P) \setminus L((n-1)\,P)$ に属するので, $\ell(n\,P) > \ell((n-1)\,P)$ のときに限り存在する．種数 $g = 0$ のとき P で任意の位数の極をもつ函数が存在する．種数 $g = 1$ のとき, $n \geq 2$ に対して, P で丁度 n 位の極をもつ函数が存在する．

定理 5.5 (Weierstrass)　C を種数 g が 2 以上 $(g \geq 2)$ の非特異完備代数曲線とし, $P \in C$ とする．
(1)　P でのみ極をもつ有理函数が存在する．
(2)　g 個の異なる自然数 $n_1, \cdots, n_g$ があって, それらと異なる任意の自然数 n に対して, P の外で正則で, P で丁度 n 位の極をもつ有理函数が存在する．

(b)　$\ell((g+1)\,P) \geq g + 1 - g + 1 = 2$ となる．$\ell((g+1)\,P) \geq 2$ なので, 定数函数でない $f \in L((g+1)\,P)$ が存在する．f は極をもたねばならないが, f の極因子に台は P だけなので, f は P でのみ極をもつ．

(c)　P でのみ丁度 n 位の極をもつ有理函数は, $\ell(n\,P) > \ell((n-1)\,P)$ のとき存在し, $\ell(n\,P) = \ell((n-1)\,P)$ のとき存在しない．$\ell(n\,P) = n - g + 1$ $(n > 2g - 2)$ なので, $n \geq 2g$ に対して $\ell(n\,P) > \ell((n-1)\,P)$ となる．P で丁度 n $(\geq 2g)$ 位の極をもつ有理函数が存在する．
$\ell((2g-1)\,P) = 2g - 1 - g + 1 = g$ なので,

$$1 = \ell(0) \leq \ell(P) \leq \ell(2\,P) \leq \cdots \leq \ell((2g-2)\,P) \leq \ell((2g-1)\,P) = g$$

となる．隣り合う項の差 $\ell(n\,P) - \ell((n-1)\,P)$ は 0 か 1 なので, $2g-1$ 個の隣り合う項の差のうち $g-1$ 個が 1 で g 個が 0 である．$\ell(n\,P) = \ell((n-1)\,P)$ となる n を順に並べた $n_1, \cdots, n_g$ が, 定理 5.5 (2) の自然数の組である．

(d)　$\ell(n\,P) = \ell((n-1)\,P)$ となる自然数 n を P の**空隙値** (gap value) といい, 小さい順に並べた $\{n_1, \cdots, n_g\}$ $(n_1 < \cdots < n_g)$ を P の **空隙値列** (gap sequence) という．空隙値列は P に固有の数の

集合であるが, 殆どの場合 $\{1, \cdots, g\}$ になる. 空隙値列が $\{1, \cdots, g\}$ と異なる $P \in C$ を **Weierstrass 点**という. 種数 $g = 0$ のとき C のすべての点で空隙値列は空集合で, $g = 1$ のときすべての点で空隙値列は $\{1\}$ である. 種数が 0 か 1 の非特異完備代数曲線は Weierstrass 点をもたない. 以下 C の種数は 2 以上とする.

命題 5.6 C の Weierstrass 点は高々有限個である.

この命題は, 次の Hurwitz の定理でより定量的に示される. 不正確ではあるが, 直観的に Weierstrass 点が有限個であることを描いてみる. 全射な基準写像 $\Phi_{D_\infty} : \mathrm{Sym}^g(C) \to \mathrm{Pic}^0(C)$ は, 殆どの点で 1 対 1 となる. 単射にならない所は, $\mathrm{Sym}^g(C)$ の (真に小さい) 部分多様体の有限和集合 ($\mathcal{E}$ とおく) で表せる. $\mathrm{Sym}^g(C)$ に C を対角に埋め込んだものを自然に C と同一視すると, Weierstrass 点は C と $\mathcal{E}$ の共通部分に含まれる. また Weierstrass 点でない点が存在するので C は $\mathcal{E}$ に含まれない. Bézout の定理の拡張により C と $\mathcal{E}$ の共通部分は有限集合になるので, Weierstrass 点は高々有限個である.

(e) 以下 k の標数は 0 とする. C の第一種微分全体のなす線形空間の基底 $\omega_1, \cdots, \omega_g$ に対して, **Wronski 行列** (Wronskian) $W(\omega_1, \cdots, \omega_g)$ を定義する. $P \in C$ の局所助変数 t をとり, $\omega_i = f_i\, dz$ と表す. $m = g(g+1)/2$ とおき, $f_i^{(j)}$ を f_i の t に関する j 階微分とする. $W(\omega_1, \cdots, \omega_g)_P = \det(f_i^{(j)})_{i,j}\, (dt)_P^m$ は m 重の局所微分 (局所微分の m 回テンソル積) として意味をもつ. ここで $W(\omega_1, \cdots, \omega_g) = (W(\omega_1, \cdots, \omega_g)_P)$ とおくと, 微分の Wronski 行列が m 重の微分 (微分の m 回テンソル積) として定義される. Wronski 行列 $W(\omega_1, \cdots, \omega_g)$ の因子を W_C とかき, **Weierstrass 因子**とよぶ.

命題 5.7 (1) Weierstrass 因子 W_C は第一種微分の基底の取り方によらない.
(2) $\deg(W_C) = g(g^2-1)$ で, $P \in C$ で $\nu_P(W_C) = n_1 + \cdots + n_g - m$ が成り立つ.
(3) W_C は整因子 ($W_C \geq 0$) で, その台集合は Weierstrass 点の全体に等しい.

系 5.8 種数が 2 以上なら Weierstrass 点が存在し, その個数は高々 $g(g^2-1)$ 個である. 個数が丁度 $g(g^2-1)$ 個のとき, 空隙値列はすべて $\{1, 2, \cdots, g-1, g+1\}$ である.

Weierstrass 点の個数の下限も具体的に与えることができる. 函数の積を考えることで, 自然数全体から空隙値列を除いた集合が自然数全体の部分半群になることがわかる. 空隙値は $2\,g$ より小さいので次の補題より, 空隙値の和は g^2 以下になる.

補題 5.9 $\mathbb{N} - \{n_1, \cdots, n_g\}$ $(1 \leq n_1 < \cdots < n_g < 2\,g)$ が加法について半群なら, $n_1 + \cdots + n_g \leq g^2$ が成り立つ.

さて Weierstrass 因子の P での位数 $\nu_P(W_C)$ は空隙値の和から $m = g(g+1)/2$ を引いたものであったので, $\nu_P(W_C) \leq g(g-1)/2$ となる. 従って, Weierstrass 点は少なくとも $2g+2$ 個存在する.

定理 5.10 (Hurwitz) Weierstrass 点の個数は $2g+2$ 個以上, $g(g^2-1)$ 個以下である.

殆どの代数曲線で Weierstrass 点の個数は最大値の $g(g^2-1)$ 個となり, 最小値の $2g+2$ 個になるのは超楕円曲線に限る. 種数 $g = 2$ のとき $2g+2 = 6$, $g(g^2-1) = 6$ なので, これらのことは種数が 2 の非特異完備代数曲線は超楕円曲線であることを示唆する. このことは Riemann-Roch の定理を使って, すぐ後で確かめる. (§5.12)

問 52 命題 5.7, 補題 5.9 を示せ.

§5.8 代数曲線の自己同型群

(a) C を種数 g (≥ 2) の非特異完備代数曲線とし, Weierstrass 点の個数を w とおく. C の自己同型群 $\mathrm{Aut}(C)$ は, C から自分自身への同型写像全体のなす群である. 自己同型写像は Weierstrass 点の間の置換を引き起こす.

定理 5.11　k の標数が 2 と異なるとする. 超楕円曲線 C の Weierstrass 点を固定する自己同型写像は, 恒等写像か超楕円対合に限る.

定理 5.12 (Hurwitz)　$2\,g+3$ 個以上の点を固定する自己同型写像 $\varphi : C \to C$ は恒等写像である.

系 5.13　群の準同型写像 $\mathrm{Aut}(C) \to \mathfrak{S}_w$ は, C が超楕円曲線でないとき単射である. C が超楕円曲線のとき, その核は超楕円対合の生成する位数 2 の部分群である.

定理 5.14　種数が 2 以上の非特異完備代数曲線の自己同型群は有限群である.

問 53　次の様にして定理 5.12 を示せ: f を定理 5.12 の自己同型写像とする. $P \in C$ に対して $h \in L((g+1)\,P) \smallsetminus k$ をとる. $h_0 = h - \varphi^* h$ の因子を計算し, $h_0 = 0$ であることを示せ. 従って $f(P) = P$ となることを示せ.

(b)　C の自己同型写像は C の函数体 $k(C)$ の自己同型写像を引き起こすので, $\mathrm{Aut}(C)$ は自然に $k(C)$ に作用する. G を $\mathrm{Aut}(C)$ の位数 d の有限部分群とする. $k(C)$ における G-不変体 $k(C)^G$ は $k(C)/k$ の中間体で, $[k(C) : k(C)^G] = \sharp G < \infty$ となる. このとき $\varphi^*(C_G) = k(C)^G$ なる非特異完備代数曲線 C_G と有理写像 $\varphi : C \to C_G$ が存在する. C_G を G による C の**商代数曲線** (quotient curve) という. $\varphi : C \to C_G$ は Galois 群が G に等しい Galois 分岐被覆である. 分岐被覆 φ の分岐点を $P_1, \cdots, P_s \in C_G$ とする. φ は Galois 被覆なので, P_j の上の点における φ の分岐指数 (e_j とおく) はすべて等しく, e_j は φ の写像度 d の約数である. Riemann-Hurwitz の公式

$$2\,g-2 \;\geq\; d\,(2\,g(C_G)-2+(1-\tfrac{1}{e_1})+\cdots+(1-\tfrac{1}{e_s}))$$

を得る. k の標数が 0 ならば, 野性的分岐が現れないので上は常に等号が成り立つ. このとき, 与えられた種数 g (≥ 2) に対して $g(C_G)$, $e_1, \cdots, e_s$ の不定方程式と思って解くと, 自己同型群の上限が得られる.

定理 5.15 (Hurwitz)　k の標数は 0 とする. $g \geq 2$ のとき, 自己同型群 $\mathrm{Aut}(C)$ の位数は $84\,(g-1)$ を超えない.

問 54　k の標数は 0 とする. 自己同型群の位数は, $84\,(g-1)$, $48\,(g-1)$, $40\,(g-1)$, $\cdots$ となることを示せ. (注) すべての可能性を計算する必要はない. 上記のものを与える分岐指数の組を求め, 可能であれば, 被覆写像を具体的に表して C の定義方程式を与えてみよ.

問 55　k の標数は 0 とする. C の種数が 2 ならば, 自己同型群の位数は 48 を超えないことを示せ. (上の演習問題を考慮すれば, 位数が 84 にならないことを示せばよい)

§5.9　超楕円曲線

(a)　種数 g (≥ 2) の非特異完備代数曲線 C で $\mathbb{P}^1$ への 2 次の分離的被覆 (写像度が 2 の分離的有理函数) をもつものを**超楕円曲線**という. $x : C \to \mathbb{P}^1$ を 2 次の分離的被覆とする. x は C の有理函数であるがその極因子を D とおく. D は 2 次の整因子なので $\ell(D) \leq 2$ である. $L(D)$ は一次独立な有理函数 1, x を含むので, $\ell(D) = 2$ で 1, x が基底となる. $m \geq g$ のとき $\ell(m\,D) = \deg(m\,D) - g + 1 = 2m - g + 1$ なので, 特に $\ell(g\,D) = g+1$ となる. $x^m \in L(m\,D) \smallsetminus L((m-1)\,D)$ ($m \geq 1$) なので,

$$\ell(0) = 1 < \ell(D) = 2 < \ell(2\,D) < \ell(3\,D) < \cdots < \ell((g-1)\,D) < \ell(g\,D) = g+1$$

となる. 従って $1 \leq m \leq g$ に対して $\ell(m\,D) = m+1$ となり $L(m\,D)$ は m 次以下の x の多項式全体に等しい. $\ell((g+1)\,D) = g+3 = \ell(g\,D)+2$ なので, $L((g+1)\,D)$ には $g+1$ 次以下の x の多項式全体とは一次独立な有理函数 $y \in L((g+1)\,D)$ がとれる. 以上より,

命題 5.16 $L(m\,D) = \begin{cases} k + k\,x + \cdots + k\,x^m & (1 \le m \le g) \\ k + k\,x + \cdots + k\,x^m + k\,y + k\,xy + + \cdots + k\,x^{m-g-1}y & (m \ge g+1) \end{cases}$

さてここで y^2 の極因子は $2(g+1)\,D$ を超えないので $y^2 \in L(2(g+1)\,D)$ となる. $g+1$ 次以下の多項式 $a_1 \in k[x]$ と $2g+2$ 次以下の多項式 $a_2 \in k[x]$ で $y^2 + a_1(x)\,y + a_2(x) = 0$ とかける.

定理 5.17 C は, $C_0 : y^2 + a_1(x)\,y + a_2(x) = 0$ で定義されるアフィン平面曲線の非特異完備化に同型である.

問 56 簡単のため k の標数は 2 と異なるとする.

(1) アフィン平面曲線 $C_0 : y^2 + a_1(x)\,y + a_2(x) = 0$ が特異点をもたない条件を与えよ.

(2) 種数 g の超楕円曲線 C の函数 x, y から作ったアフィン平面曲線 C_0 は非特異であることを示せ.

(b) $a_1,\, a_2 \in k[x]$ を $\deg a_1 \le g+1$, $\deg a_2 \le 2g+2$ とし, アフィン平面曲線 $C : y^2 + a_1(x)\,y + a_2(x) = 0$ が特異点をもたないとする. $\tilde{C} : v^2 + (u^{g+1}a_1(1/u))\,v + u^{2g+2}a_2(1/u) = 0$ とおくと, $\tilde{C}$ も非特異アフィン平面曲線である. 有理写像 $\varphi : C \ni (x,\, y) \longmapsto (1/x,\, y/x^{g+1}) \in \tilde{C}$ は双有理的で, φ で C と $\tilde{C}$ を貼り合わせた代数曲線 $\hat{C} = C \cup \tilde{C}$ は C の非特異完備化である. C の無限遠点は x-座標が ∞ なので, $\tilde{C}$ において u-座標が 0 の点である. $a_1(x)$ の x^{g+1} 次の項の係数を c_1, $a_2(x)$ の x^{2g+2} の項の係数を c_2 とおく. このとき $\tilde{C}$ の u-座標が 0 の点の v-座標は $v^2 + c_1\,v + c_2 = 0$ の根である. k の標数によらず, C の無限遠点は $c_1^2 - 4c_2 = 0$ のとき 1 点で, $c_1^2 - 4c_2 \ne 0$ のとき 2 点である.

2 次 Galois 被覆 $x : C \longmapsto \mathbb{P}^1$ の Galois 群は $\iota : C \ni P = (x,\, y) \longmapsto P' = (x,\, -y - a_1(x)) \in C$ で生成される. ι を**超楕円対合**という. u-座標が 0 の点 $P_\infty = (0,\, v_0) \in \tilde{C}$ は, ι により $P'_\infty = (0,\, -v_0 - c_1) \in \tilde{C}$ に移る.

(c) 少し細かい計算をするために, k の標数は 2 と異なるとする. 超楕円曲線 C は, 重根をもたない多項式 $f(x) \in k[x]$ で $y^2 = f(x)$ で定義することができる. このとき C の無限遠点は, f の次数が奇数のとき 1 点で, f の次数が偶数のとき 2 点である. アフィン部分曲線上の d 個分岐点を $Q_1, \cdots, Q_d$ とおく. これらの点の x-座標 $x(Q_1), \cdots, x(Q_d)$ は $f(x) = 0$ の根であり, 順に $\alpha_1, \cdots, \alpha_d$ と書く. このとき Q_j の局所助変数として $t_j^2 = x - \alpha_j$ $(t_j \in k(C)_P)$ がとれる. Q_j において座標函数 y の値は 0 である. 定義方程式の右辺 $f(x)$ を t_j で展開すると, $f(x) = b_1\,t_j^2 + b_2\,{}^4_j + \cdots$ $(b_1 \ne 0)$ と書ける. $y^2 = f(x)$ より $y = \sqrt{b_1}\,t_j + (\text{高次の項})$ と展開される. 最初の項に $\pm$ をつけ忘れているように見えるが, t_j の取り方に $\pm$ の不確定さがあるので, y の展開に $\pm$ をつける必要は無い. ともかく $\mathrm{ord}_{Q_j}(x - \alpha_j) = 2$, $\mathrm{ord}_{Q_j}(y) = 1$ である.

アファイン部分曲線 (x の正則点) 上の点 $P \in C$ をとり, $a = x(P) \in \mathbb{A}^1$ とおく. x-座標の値が a となる点は P と P' である. x-座標の値を明記するときには P, P' をそれぞれ P_a, P'_a と書く. x が P_a で不分岐であるなら P_a の局所助変数として $t_{P_a} = x - a$ がとれる. P_a において y-座標函数の値 $y(P_a)$ は 0 でない. 定義方程式の右辺 $f(x)$ を t_{P_a} で展開すると, $f(x) = b_0 + b_1\,t_{P_a} + \cdots$ $(b_0 \ne 0)$ と書ける. $(y(P_\infty))^2 = f(x(P_\infty) = f(a) = b_0$ より, $y = y(P_a) + (\text{高次の項})$ と展開される. 従って $\mathrm{ord}_{P_a}(x - a) = 1$, $\mathrm{ord}_{P_a}(y) = 0$ である.

d が奇数のとき無限遠点 P_∞ は唯一つの点で, u, v-座標で表すと $(0,\, 0)$ となる. つまり $x(P_\infty) = (1/u)(P_\infty) = 1/u(P_\infty)$ より P_∞ は函数 x の極で, $(y/x^m)(P_\infty) = u(P_\infty) = 0$ より, y の P_∞ での位数 $\mathrm{ord}_{P_\infty}(y)$ は x^m の P_∞ での位数 $m\,\mathrm{ord}_{P_\infty}(x)$ より大きい. もう少し精密に, P_∞ は 2 次被覆 x の分岐点なので, P_∞ の局所助変数として $t_\infty^2 = 1/x$ $(t_\infty \in k(C)_{P_\infty})$ がとれる. $y^2 = f(x) = a_0\,t_\infty^{-2d} + \cdots$ $(a_0 \ne 0)$ より, $y = \sqrt{a_0}\,t_\infty^{-d} + (\text{高次の項})$ となる. 従って $\mathrm{ord}_{P_\infty}(x) = -2$, $\mathrm{ord}_{P_\infty}(y) = -d$ である.

d が偶数のとき無限遠点は 2 つあるが, u, v-座標で表すと $(0, \pm\sqrt{a_0})$ と書ける. $(0,\, \sqrt{a_0})$ に対応する無限遠点を P_∞ とし, $(0,\, -\sqrt{a_0})$ に対応する無限遠点を P'_∞ とする. 函数 $u = y/x^m$ は, P_∞ において $\sqrt{a_0}$ を値にもち, P'_∞ において $-\sqrt{a_0}$ を値にもつ. もう少し精密に, P_∞ は 2 次被覆 x の不分岐点なので,

P_∞ の局所助変数として $t_\infty = 1/x$ ($t_\infty \in k(C)_{P_\infty}$) がとれる. $y^2 = f(x) = a_0\, t_\infty^{-d} + \cdots$ ($a_0 \neq 0$) より, $y = \sqrt{a_0}\, t_\infty^{-d/2} +$ (高次の項) となる. 従って $\mathrm{ord}_{P_\infty}(x) = -1$, $\mathrm{ord}_{P_\infty}(y) = -d/2$ である.

命題 5.18 (1) $d = \deg f$ が奇数のとき, $\mathrm{div}(x) = P_0 + P_0' - 2\,P_\infty$, $\mathrm{div}(y) = Q_1 + \cdots + Q_d - d\,P_\infty$
(2) $d = \deg f$ が偶数のとき, $\mathrm{div}(x) = P_0 + P_0' - (P_\infty + P_\infty')$, $\mathrm{div}(y) = Q_1 + \cdots + Q_d - (d/2)\,(P_\infty + P_\infty')$

(d) 空隙値列の計算をする. $d = \deg f$ が奇数 (このとき $d = 2g+1$) のとき, 無限遠点 P_∞ は分岐点であった. P_∞ の外で正則な有理函数は, アフィン部分曲線上で正則な有理函数なので, 座標函数で生成された多項式函数 $k[x, y]$ になる. 関係式 $y^2 = f(x)$ に注意すれば, $k[x] + k[x]\,y$ と書ける. $y \in L((2g+1)\,P_\infty)$ なので $n \leq 2g$ とすると $L(n\,P_\infty) \subset k[x]$ である. $x \in L(2\,P_\infty)$ なので $L(0) = L(P_\infty) = k$, $L(2\,P_\infty) = L(3\,P_\infty) = k + k\,x$, $\cdots$, $L((2g-2)\,P_\infty) = k + k\,x + \cdots + k\,x^{g-1}$, $L(g\,P_\infty) = k + k\,x + \cdots + k\,x^g$ となる. 極因子が $n\,P_\infty$ ($n \geq 2g+1 = d$) の函数として, n が偶数のときは $x^{n/2}$ を, n が奇数のときは $x^{(n-d)/2}y$ をとることができる. 従って P_∞ の空隙値列は $\{1, 3, 5, \cdots, 2g-1\}$ である.

$d = \deg f$ が偶数 (このとき $d = 2g+2$) のとき, 無限遠点 P_∞ は分岐点ではない. $L(n\,P_\infty)$ の次元 $\ell(n\,P_\infty)$ を計算したいのだが, 先に $L(n(P_\infty + P_\infty'))$ ($\supset L(n\,P_\infty)$) の次元を計算する. P_∞ と P_∞' の外で正則な有理函数は, アフィン部分曲線の正則な有理函数なので, 座標函数 x, y で生成された多項式函数 $k[x, y]$ である. 関係式 $y^{=} f(x)$ により, $k[x] + k[x]\,y$ と書ける. $y \in L((g+1)(P_\infty + P_\infty'))$ より, $L(n\,(P_\infty + P_\infty')) \subset k[x]$ ($n \leq g$) となる. $k[x]$ の元は超楕円対合 ι で不変なので, $k[x]$ の元に対する P_∞ の位数と P_∞' の位数は等しい. 従って P_∞' で正則な $k[x]$ の元は P_∞ でも正則である. よって $L(n\,P_\infty) = k$ ($n \geq g$) を得る. 空隙値列は丁度 g 個の自然数の組なので, P_∞ の空隙値列は $\{1, 2, 3, \cdots, g\}$ である. C の分岐点での空隙値列は d が奇数の場合の P_∞ の, 不分岐点での空隙値列は d が偶数の場合の P_∞ の空隙値列の計算と同様にできる.

命題 5.19 2 次被覆 x の分岐点 $P \in C$ の空隙値列は $\{1, 3, 5, \cdots, 2g-1\}$ である. その他の点の空隙値列は $\{1, 2, \cdots, g\}$ である. 従って超楕円曲線 C の Weierstrass 点は $2g+2$ 個である.

定理 5.11 あるいは系 5.13 より, 超楕円曲線の自己同型写像は超楕円対合と可換である. 自己同型群を超楕円対合で割った剰余類群 $\mathrm{RAut}(C) = \mathrm{Aut}(C)/\langle\iota\rangle$ を C の**被約自己同型群** (reduced automorphism group) という.

命題 5.20 被約自己同型群 $\mathrm{RAut}(C)$ は, 自然に射影直線の一次分数変換の部分群になり, また, 対称群 $\mathfrak{S}_{2g+2}$ の部分群に同型である.

(e) k の標数が 2 と異なるとする. C を種数 g (≥ 2) の超楕円曲線で, $x : C \to \mathbb{P}^1$ を射影直線の 2 次被覆とする. (a) で $L(m\,D)$ ($m \geq 1$, D は x の極因子) の基底の計算から, C のアフィン平面曲線としての定義方程式を与えた. 超楕円曲線の Weierstrass 点について調べたことを用いると, 定義方程式を次の様に与えることができる. x は 2 次の Galois 被覆なので, 分岐指数は 1 または 2 となる. Riemann-Hurwitz の公式より, 分岐点の個数は $2g+2$ 個である. $a_1, \cdots, a_{2g+2} \in \mathbb{P}^1$ を x の分岐点とする.

定理 5.21 C は $C_0 : y^2 = (x - a_1)\,(x - a_2) \cdots (x - a_{2g+2})$ に同型である. (右辺の積で $a_j = \infty$ となる項は除く)

§5.10 超楕円曲線の微分

(a) k の標数は 2 と異なるとし, $C : y^2 = f(x)$ を種数 g (≥ 2) の超楕円曲線とする. $f \in k[x]$ は重根をもたず, 次数は $d = 2g+1, 2g+2$ である. 微分 dx の因子を計算する. 2 次 Galois 被覆 $x : C \to \mathbb{P}^1$ のアファイン部分曲線上の分岐点は $Q_1, \cdots, Q_d$ で, d が奇数のとき無限遠点 P_∞ も分岐点になる. 有理函数 x の極は, d が奇数のときは無限遠点 P_∞ 唯一つで位数は -2 である. d が偶数のときは 2 つの無限遠点 P_∞, P_∞' で位数は -1 である.

命題 5.22
$$\mathrm{div}(dx) = \begin{cases} Q_1 + \cdots + Q_d - 3\,P_\infty & (d \text{ は奇数}) \\ Q_1 + \cdots + Q_d - 2\,P_\infty - 2\,P'_\infty & (d \text{ は偶数}) \end{cases}$$

d が奇数 (P_∞ が分岐点) のとき, $Q_{d+1} = P_\infty$ とおく. d が奇数のとき $d+1 = 2g+2$ で, d が偶数のとき $d = 2g+2$ である. 従って d の偶奇によらず $Q_1, \cdots, Q_{2g+2}$ が x のすべての分岐点を表す. また d が奇数のとき $P'_\infty = P_\infty$ なので, 微分 dx の因子を d の偶奇によらない形で表せる.

$$\mathrm{div}(dx) = Q_1 + \cdots + Q_{2g+2} - 2\,P_\infty - 2\,P'_\infty$$

(b) 有理函数 y の因子は $\mathrm{div}(y) = Q_1 + \cdots + Q_{2g+2} - (g+1)\,(P_\infty + P'_\infty)$ なので,

$$\mathrm{div}(\frac{dx}{y}) = (g-1)\,(P_\infty + P'_\infty)$$

である. また $\mathrm{div}(x) = P_0 + P'_0 - P_\infty - P'_\infty$ なので, $0 \le n \le g-1$ に対して

$$\mathrm{div}(x^n\,\frac{dx}{y}) = n(P_0 + P'_0) + (g-1-n)\,(P_\infty + P'_\infty)$$

命題 5.23 C の第一種微分の全体は, $\frac{dx}{y}$, $x\,\frac{dx}{y}$, $\cdots$, $x^{g-1}\,\frac{dx}{y}$ で生成される g 次元 k-線形空間である.

(c) P_∞ が分岐点 ($P'_\infty = P_\infty$) のとき, P_∞ でのみ極をもつ有理函数の全体は $k[x] + k[x]\,y$ であった. ω を P_∞ でのみ極をもつ微分とすると, $\omega/\frac{dx}{y}$ は P_∞ でのみ極をもつ有理函数である. 従って P_∞ でのみ極をもつ第二種微分の全体は $(k[x] + k[x]\,y)\,\frac{dx}{y}$ である.

P_∞ が不分岐点 ($P'_\infty \ne P_\infty$) のとき, P_∞ でのみ極をもつ第二種微分 ω をとる. $\mathrm{ord}_{P_\infty}(\omega) = n$ ($n \ge 1$) とおくと, $f_\omega = \omega/\frac{dx}{y}$ は極因子が $n\,P_\infty + (g-1)\,(P_\infty + P'_\infty)$ である. $n = 1$ のとき, f_ω の極因子は $g\,(P_\infty + P'_\infty)$ に含まれる. ところが $L(g\,(P_\infty + P'_\infty)) \subset k[x]$ なので, f_ω の P_∞ の位数と P'_∞ の位数は等しい. 従って P_∞ での位数が丁度 1 の第二種微分は存在しない. このことは留数の計算からすでにわかっていたことだが, 有理函数や微分の因子を具体的に計算することでもわかる. $n = 2$ のとき, f_ω の極因子は $(g+1)\,P_\infty + (g-1)\,P'_\infty$ なので, f_ω は $L((g+1)\,(P_\infty + P'_\infty)) = k + k\,x + \cdots + k\,x^{g+1} + k\,y$ に含まれる. 無限遠点 P_∞ と P'_∞ の区別は $u = 1/x$, $v = y/x^{g+1}$ 座標で $(0, \sqrt{a_0})$ になるのが P_∞ で $(0, -\sqrt{a_0})$ となるが P'_∞ と定めた. 従って P'_∞ の近傍で $y \ne -\sqrt{a_0}\,x^{g+1}$ となる. P'_∞ の局所助変数 $t_\infty = 1/x$ で有理函数 y を Laurent 級数展開すると

$$y = -\sqrt{a_0}\,t_\infty^{-g-1} + b_1\,t_\infty^{-g} + b_2\,t_\infty^{-g+1} + \cdots$$

となる. $f_P = y + \sqrt{a_0}\,t_\infty^{-g-1} - b_1\,t_\infty^{-g}$ とおくと, $h \in L(2\,P_\infty + (g-1)\,(P_\infty + P_\infty))$ なので $f_P\,\frac{dx}{y}$ は P_∞ で 2 位の極をもつ第二種微分である. $n \ge 2$ に対して $\ell(n\,P_\infty + (g-1)\,(P_\infty + P'_\infty)) = g + n - 1$ である. $\ell((g-1)\,(P_\infty + P'_\infty)) = \ell(P_\infty + (g-1)\,(P_\infty + P'_\infty)) = g$ なので, どの n (≥ 2) に対しても, P_∞ で丁度 n 位の極をもつ第二種微分が存在する. P_∞ で高々 n 位の極をもつ第二種微分の全体は $g + n - 1$ 次元 k-線形空間をなす.

(d) 異なる 2 点 P, $Q \in C$ をとる. $\ell(P + Q + (g-1)\,(P_\infty + P'_\infty)) = 2g - g + 1 = g + 1$ である. $\ell((g-1)(P_\infty + P'_\infty)) = g$ より, $f_{PQ} \in L(P + Q + (g-1)\,(P_\infty + P'_\infty)) \setminus L((g-1)\,(P_\infty + P'_\infty))$ がとれる. このとき $\omega_{PQ} = f_{PQ}\,\frac{dx}{y}$ は P, Q で高々 1 位の極をもつ第三種微分である. また P, Q で高々 1 位の極をもつ第三種微分の全体は $g+1$ 次元 k-線形空間をなす.

$p = x(P)$, $q = x(Q)$ とおく. P, Q は分岐点でなく, $p \ne q$, $p \ne \infty$, $q \ne \infty$ の場合に, ω_{PQ} をもう少し具体的に与える. f_{PQ} を与えればよいのだが, $h_{PQ} = f_{PQ}\,(x-p)(x-q)$ とおくと, $\mathrm{div}(h_{PQ}) \ge -P' - Q' + (g+1)(P_\infty + P'_\infty)$ である. h_{PQ} は $L((g+1)\,(P_\infty + P'_\infty)) = k + k\,x + \cdots + k\,x^{g+1} + k\,y$ に属する有理函数で P', Q' を零点にもつものである. P', Q' を通る直線の方程式を $h_{PQ} = a + b\,x + c\,y = 0$ とおく. $f_{PQ} = h_{PQ}/(x-p)(x-q)$ とおくと $f_{PQ} \in L(P + Q - (g-1)(P_\infty + P'_\infty))$ となり, $\omega_{PQ} = f_{PQ}\,\frac{dx}{y}$ は P, Q で高々 1 位の極をもつ第三種微分である.

問 57 適当に場合分けして (上に書いたものも含む), P, Q で高々 1 位の極をもつ第三種微分を求めよ. 更に P, Q での留数を計算し, 留数定理が成り立つことを確かめよ.

§5.11　超楕円曲線の因子類群

(a)　C を種数 g の超楕円曲線とする. 話を簡単にするため, k の標数は 2 と異なるとし, C の無限遠点 P_∞ は Weierstrass 点 ($P'_\infty = P_\infty$) とする. C は, 次数が $2g+1$ の重根をもたない多項式 $f(x) \in k[x]$ により, $C : y^2 = f(x)$ で定義される. $g\,P_\infty$ に関する基準写像 $\Phi = \Phi_{gP_\infty} : \mathrm{Sym}^g(C) \to \mathrm{Pic}^0(C)$ は定理 5.1 (3) より全射である.

命題 5.24　Φ は殆ど単射である.

(b)　もう少し精密に述べる. $P \in C$ に対して $P \neq P_\infty$ のとき $u_P = x - x(P)$ とおき, $u_{P_\infty} = 1$ とおく. 因子 $D = \sum n_P\,P$ に対して, $D' = \sum n_P\,P'$ とおく. また $u_D = \prod u_P^{n_P}$ とおく. D の次数を d とすると,

命題 5.25　$\mathrm{div}(u_D) = D + D' - 2d\,P_\infty$

$D_1,\ D_2 \in \mathrm{Sym}^g(C)$ とする. $\Phi(D_1) = \Phi(D_2)$ となるための必要十分条件は $\ell(D_1 - D_2) > 0$ である. $L(D_1 - D_2) \ni h \longmapsto h\,u_{D_1} \in L(2g\,P_\infty - D'_1 - D_2)$ より, $\ell(2g\,P_\infty - D'_1 - D_2) = \ell(D_1 - D_2)$ である. $L(2g\,P_\infty - D'_1 - D_2) \subset L(2g\,P_\infty) = k + k\,x + \cdots + k\,x^g \subset k[x]$ なので,

定理 5.26　$D_1,\ D_2 \in \mathrm{Sym}^g(C)$ が $\Phi(D_1) = \Phi(D_2)$ となるための必要十分条件は, 次数 $2g$ の因子 $D'_1 + D_2$ が超楕円対合で移りあう g 個の点の対に分けることができることである. つまり $D \in \mathrm{Sym}^g(C)$ で $D'_1 + D_2 = D + D'$ と書けることである.

定理 5.27　種数 $g = 2$ のとき, $\Phi = \Phi_{2P_\infty}$ が単射とならないのは $\Phi^{-1}(0) = \{P + P' \mid P \in C\} \simeq \mathbb{P}^1$ である.

(c)　全射 $\Phi : \mathrm{Sym}^g(C) \to \mathrm{Pic}^0(C)$ を通して, $\mathrm{Pic}^0(C)$ の加法を $\mathrm{Sym}^g(C)$ の上に描く. $D_1,\ D_2 \in \mathrm{Sym}^g(C)$ とする. $D = 3\,g\,P_\infty - D'_1 - D'_2$ とおくと, D の次数は g である. $\ell(D) \geq \deg D - g + 1 = g - g + 1 = 1 > 0$ なので, 零でない $h \in L(D)$ が存在する. $D_3 = \mathrm{div}(h) + D$ とおくと, D_3 は次数 g の整因子なので $D_3 \in \mathrm{Sym}^g(C)$ である. $\ell(D) = 1$ ならば h の選び方は定数倍を除いて一意なので D_3 は一意に定まる. $\ell(D) > 1$ ならば $D_3 \in \mathrm{Sym}^g(C)$ は h の選び方で変わり, 一意に定まらない. どの h, どの D_3 を取っても,

$$\begin{aligned}\Phi(D'_1) + \Phi(D'_2) + \Phi(D_3) &= [D'_1 - g\,P_\infty] + [D'_2 - g\,P_\infty] + [D_3 - g\,P_\infty] \\ &= [D'_1 + D'_2 + D_3 - 3\,g\,P_\infty] = [\mathrm{div}(h)] = 0\end{aligned}$$

なので, $\Phi(D_3) = -\Phi(D'_1) - \Phi(D'_2) = \Phi(D_1) + \Phi(D_2)$ となる. 定理 5.15 より, D_3 に現れる $P + P'$ 型の項を $2\,P_\infty$ に置き換えたものを D_4 とおくと, $\Phi(D_4) = \Phi(D_3)$ で, $D_4 \in \mathrm{Sym}^g(C)$ は h の取り方によらない. 従って $D_1,\ D_2 \in \mathrm{Sym}^g(C)$ に対して $D_1 \oplus D_2 = D_4$ とおいて, $\mathrm{Sym}^g(C)$ の上に加法が定まる.

(d)　加法を具体的に計算するには, $L(D)$ ($D = 3\,g\,P_\infty - D'_1 - D'_2$) に属する零でない有理函数 h を具体的に与えねばならない. $L(D) \subset L(3\,g\,P_\infty)$ なので, $D'_1 + D'_2$ で零となる $h \in L(3\,g\,P_\infty)$ を作ればよい. $L(3\,g\,P_\infty)$ の任意の元は $h_1(x) + h_2(x)\,y$ ($h_1,\ h_2 \in k[x]$, $\deg h_1 \leq 3g/2$, $\deg h_2 \leq (g-1)/2$) と書ける. $D'_1 + D'_2$ で零になるように, $h_1(x) + h_2(x)\,y$ の $2g+1$ 個の係数を決めればよい. 最も単純な場合として, $D'_1 + D'_2$ が x-座標がすべて相異なる $2\,g$ 個の点の和 ($P_1 + \cdots + P_{2g}$) のときを考える. $P_1,\ \cdots,\ P_{2g}$ で $h_1(x) + h_2(x)\,y = 0$ となれば良いので, $2g$ 個の連立一次方程式を得る. その連立方程式の階数は変数の個数 $(2g+1)$ より小さいので, 自明でない解をもつ. その解を係数として $h = h_1(x) + h_2(x)\,y$ とおけば, 零でない $h \in L(D)$ を得る.

(e)　因子類群はイデアル類群の類似で, 超楕円曲線は 2 次体なので, 種の理論にあたるものを因子類群上に展開できる. 超楕円対合が 2 次体としての共役にあたるので, 特異類 (ambig class) には 2 等分点が関係する. 実際 $D \in \mathrm{Sym}^g(C)$ とし, $\Phi(D)' = [D - g\,P_\infty]' = [D' - g\,P_\infty] = \Phi(D') = -\Phi(D)$ なので, $\Phi(D)$ が特異類 ($\Phi(D)' = \Phi(D)$) なら $2\Phi(D) = 0$ となる. 特異類の全体は $\mathrm{Pic}^0(C)$ の 2 等分点の全体に等しい.

$[P' - P_\infty] = [P_\infty - P] = -[P - P_\infty]$ なので, P が Weierstrass 点なら $2\,[P - P_\infty] = 0$ となる. P_∞ 以外の Weierstrass 点を $Q_1,\ \cdots,\ Q_{2g+1}$ とおくと, $[Q_1 - P_\infty],\ \cdots,\ [Q_{2g+1} - P_\infty]$ は 2 等分点である. ところで

$\mathrm{div}(y) = Q_1 + \cdots + Q_{2g+1} - (2g+1)\,P_\infty$ なので $[Q_1 - P_\infty] + \cdots + [Q_{2g+1} - P_\infty] = 0$ が成り立つ. $[Q_1 - P_\infty]$, $\cdots$, $[Q_{2g+1} - P_\infty]$ の中から m 個 $(1 \le m \le 2g)$ を選んで和を取ると, $[Q_* - P_\infty] + \cdots + [Q_{**} - P_\infty] = [(Q_* + \cdots + Q_{**}) - m\,P_\infty]$ となる. ここで $L(m\,P_\infty) \subset L(2g\,P_\infty) = k + k\,x + \cdots + k\,x^g$ なので $L(m\,P_\infty)$ に属する函数の Q_j での位数は偶数になる. 従って $(Q_* + \cdots + Q_{**}) - m\,P_\infty$ を因子にもつ有理函数は存在しない. $\langle [Q_1 - P_\infty], \cdots, [Q_{2g} - P_\infty] \rangle$ は位数 2^{2g} の $(2, \cdots, 2)$ 型アーベル群である.

定理 5.28　種数 g (≥ 2) の超楕円曲線 C における特異類の全体は, 因子類群 $\mathrm{Pic}^0(C)$ の 2 等分点の全体に一致し, 位数 2^{2g} の基本アーベル 2-群である. また $Q_1, \cdots, Q_{2g+2}$ を C の Weierstrass 点とするとき, 特異類の全体は $[Q_i - Q_{2g+2}]$ $(1 \le i \le 2g)$ で生成される.

§5.12　種数 2 の代数曲線

(a)　C を種数 2 の非特異完備代数曲線とし, K_C をその標準整因子 (標準因子で整因子のもの) とする. $P \in C$ を任意にとる. $\ell(0) = \ell(P) = 1$ で, $m \ge 3$ に対して $\ell(m\,P) = m - 1$ である. $\ell(2\,P)$ は 1 か 2 のいずれかであるが. $\ell(2\,P) = 2$ のとき空隙値列は $\{1, 3\}$ になるので, P は Weierstrass 点である. このとき $L(2\,P)$ に属する非定数有理函数 x が取れる. x の写像度は 2 なので, C は超楕円曲線になる. $\ell(2\,P) = 1$ のとき空隙値列は $\{1, 2\}$ なので, P は Weierstrass 点ではない. しかしこのとき $\ell(P + P') = 2$ となる $P' \in C$ が存在する. $L(P + P')$ に属する 2 次の非定数有理写像がとれるので, この場合も C は超楕円曲線になる.

定理 5.29　種数が 2 の非特異完備代数曲線は, 超楕円曲線である.

(b)　上で述べたことを第一種微分を使って正当化する. C の種数は 2 なので, 第一種微分の全体は 2 次元 k 線形空間をなす. その基底 ω_1, ω_2 をとる. P が ω_1 の零点でないとする. $h = \omega_2/\omega_1$ は非定数有理函数で, $\mathrm{div}(\omega_1)$ を極因子, $\mathrm{div}(\omega_2)$ を零因子にもつ. とくに $h \in L(\mathrm{div}(\omega_1))$ である. $k = L(0) \subset L(\mathrm{div}(\omega_1))$ なので, $L(\mathrm{div}(\omega_1))$ は $k + k\,h$ を部分空間として含む. P は h の極ではないので, $a = h(P) \in k$ となる. $\omega_P = (h - a)\,\omega_1$ とおくと, ω_P は第一種微分で P を零点にもつ. $L(\mathrm{div}(\omega_1) - P) \subsetneqq L(\mathrm{div}(\omega_1))$ なので

命題 5.30　任意の $P \in C$ に対して, P を零点にもつ第一種微分 ω_P が定数倍を除いて唯一つ存在する.

命題 5.31　(1)　$\iota : C \ni P \longmapsto P' = \mathrm{div}(\omega_P) - P \in C$ は C の自己同型写像である.

(2)　$P \in C$ が Weierstrass 点であることと, ι-不変である $(P' = P)$ は同値である.

(3)　基準写像 $\Phi_{K_C} : \mathrm{Sym}^2(C) \to \mathrm{Pic}^0(C)$ は, $\mathrm{Sym}^2(C) \setminus \{\text{標準整因子}\}$ から $\mathrm{Pic}^0(C) \setminus \{0\}$ への全単射になる.

(4)　標準整因子の全体は $\{P + P' \mid P \in C\}$ に等しい.

(5)　$P + P'$ を極因子にもつ非定数有理函数 x が存在し, ι は Galois 被覆 $x : C \to \mathbb{P}^1$ の Galois 群を生成する.

(6)　C は超楕円曲線で, ι は超楕円対合である.

(7)　C の任意の自己同型写像は ι と可換である.

定理 5.32　種数 2 の非特異完備代数曲線は超楕円的で, $y^2 + a_1(x)\,y + f_2(x) = 0$ $(a_1, a_2 \in k[x], \deg a_1 \le 3, \deg a_2 \le 6)$ で定義されるアフィン平面曲線の非特異完備化に同型である.

問 58　C を種数 2 の非特異完備代数曲線とする. $P \in C$ に対して, $L(m\,(P + P'))$ $(m = 1, \cdots, 5)$ および $L(2\,(P + P') + P)$ の基底を求め, 上の定理の後半を示せ.

(c)　C を種数 2 の超楕円曲線とする. 標準整因子 K_C を基底とする基準写像 $\Phi_{K_C} : \mathrm{Sym}^2(C) \to \mathrm{Pic}^0(C)$ は全射かつ殆ど単射であった. $P + Q \in \mathrm{Sym}^2(C)$ とする. $P + Q - K_C = (P - Q') + (Q + Q' - K_C) \sim P - Q'$ なので $\Phi_{K_C}(P + Q) = [P - Q']$ と書ける. ここで因子類 $[P - Q']$ は標準整因子 K_C の選び方によらない.

定理 5.33　$\Psi : C \times C \ni (P,\, Q) \longmapsto [P-Q] \in \mathrm{Pic}^0(C)$ は全射で, $\Psi^{-1}(0) = \{(P,\, P) \in C \times C\} \simeq C$ を除いて 2 対 1 である.

問 59　種数が偶数の超楕円曲線に対して, 定理 5.33 と同様に因子類群の殆ど 2 次被覆を構成せよ.

§5.13　種数 2 の超楕円曲線の被約自己同型群

定理 5.34　C を種数 2 の超楕円曲線とする. C の被約自己同型群 $\mathrm{RAut}(C)$ は $\mathbb{P}^1$ の自己同型群 (1 次分数変換の全体) の部分群に同型で, さらに Weierstrass 点に注目することで 6 次対称群の部分群に同型である.

簡単のため k の標数は 0 とする. 種数 2 の超楕円曲線 C の被約自己同型群を, 定理 5.29 と定理 5,15 とその後の問いを使って決めることができる. 自己同型群の位数は 48 を超えないので, 被約自己同型群の位数は 24 以下である. Weierstrass 点の個数は 6 個なので, 6 次対称群 $\mathfrak{S}_6$ の部分群で位数が 24 以下のものがその候補になる. また, 2 次の有理写像 $x : C \to \mathbb{P}^1$ に適当な一次分数変換を合成して, C の Weierstrass 点 $P_1, \cdots, P_6$ のうち最初の 3 つを $x(P_1) = 0$, $x(P_2) = 1$, $x(P_3) = \infty$ にすることができる. 以下 $x(P_4) = a$, $x(P_5) = b$, $x(P_6) = c$ とおく. 被約自己同型は一次分数変換で表され, $\{0,\, 1,\, \infty,\, a,\, b,\, c\}$ の置換を引き起こす.

$$\tau : z \longmapsto \frac{1}{1-z}$$

は位数 3 の一次分数変換で, $0, 1, \infty$ をこの順に置換する. $b = \frac{1}{1-a}$, $c = \frac{a-1}{a}$ とおくと, $\tau(a) = b$, $\tau(b) = c$, $\tau(c) = a$ なので, τ は $\{0,\, 1,\, \infty,\, a,\, \frac{1}{1-a},\, \frac{a-1}{a}\}$ の位数 3 の置換を引き起こす. 超楕円曲線

$$C_a : y^2 = x\,(x-1)\,(x-a)\,(x-\frac{1}{1-a})\,(x-\frac{a-1}{a})$$

の被約自己同型群は $\langle\tau\rangle \simeq \mathbb{Z}/3\mathbb{Z}$ を部分群にもつ. また, 位数 2 の一次分数変換

$$\sigma : z \longmapsto \frac{a\,z-a+1}{z-a}$$

は $\{0,\, 1,\, \infty,\, a,\, \frac{1}{1-a},\, \frac{a-1}{a}\}$ の位数 2 の置換を引き起こす. σ もまた C_a の位数 2 の被約自己同型写像である. $\sigma\tau = \tau^2\sigma$ なので, 被約自己同型群は $\langle\sigma,\, \tau\rangle \simeq \mathfrak{S}_3$ を部分群にもつ. $a = 2$ とするとき, 位数 2 の一次分数変換

$$\sigma_2 : z \longmapsto \frac{z-2}{2z-1}$$

は $\{0,\, 1,\, \infty,\, 2,\, -1,\, 1/2\}$ の 2 次の置換を引き起こす. σ_2 と τ は可環で, $(\sigma_2\tau)^5\sigma = \sigma\,(\sigma_2\tau)$ なでの, $\langle\sigma,\, \tau,\, \sigma_2\rangle$ は位数 12 の二面体群 D_{12} に同型である.

$$C_2 : y^2 = x\,(x^2-1)\,(x-2)\,(x-1/2)$$

の被約自己同型群は D_{12} に同型である. $a = \sqrt{-1}$ とする. 位数 4 の一次分数変換

$$\sigma_4 : z \longmapsto \frac{-\sqrt{-1}}{z-1-\sqrt{-1}}$$

は $\{0,\, 1,\, \infty,\, \sqrt{-1},\, (1+\sqrt{-1})/2,\, 1+\sqrt{-1}\}$ の置換を引き起こし, $\langle\sigma,\, \tau,\, \sigma_4\rangle$ は 4 次対称群 $\mathfrak{S}_4$ に同型である.

$$C_{\sqrt{-1}} : y^2 = x\,(x-1)\,(x-\sqrt{-1})\,(x-\frac{1+\sqrt{-1}}{2})\,(x-1-\sqrt{-1})$$

の被約自己同型群は $\mathfrak{S}_4$ に同型である. $\mathfrak{S}_4$ の位数は $4! = 24$ なので, 種数 2 の場合に期待される位数最大のものが得られた. 位数 4 の一次分数変換から始めて同様に計算することで, 被約自己同型群が D_8, $\mathfrak{S}_4$ となる種数 2 の超楕円曲線が得られる.

定理 5.35　$\{1\}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, D_8, $\mathfrak{S}_3$, D_{12}, $\mathfrak{S}_4$ を被約自己同型群にもつ種数 2 の超楕円曲線が存在する. 更に k の標数が 0 のとき, 種数 2 の超楕円曲線の被約自己同型群はそれら 7 つに限る.

問 60　定理 5.35 に現れる群を被約自己同型群にもつ種数 2 の超楕円曲線をみつけよ.

§5.14 種数 2 のモジュラー曲線 $X_0(23)$

(a) 特殊線形群 $\mathrm{SL}_2(\mathbb{Z})$ は一次分数変換により複素上半平面 $\mathfrak{H}$ に作用する. その作用を $\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q})$ まで延ばすことができる. $\mathrm{SL}_2(\mathbb{Z})$ の合同部分群 $\Gamma_0(23) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \,|\, c \equiv 0 \bmod 23\}$ による商 $Y_0(23) = \Gamma_0(23)\backslash\mathfrak{H}$ は開 Riemann 面になる. また $X_0(23) = \Gamma_0(23)\backslash\mathfrak{H}^*$ は閉 Riemann 面の構造をもち, $Y_0(23)$ のコンパクト化になる. 代数的には $Y_0(23)$ は $\mathbb{C}$ 上のアフィン代数曲線で, $X_0(23)$ はその非特異完備化である. $\tau \in \mathfrak{H}^*$ で代表される $X_0(23)$ の点を (τ) で表す. $\Gamma_0(23)\backslash\mathbb{P}^1(\mathbb{Q})$ の点を $X_0(23)$ の**尖点** (cusp) という. $X_0(23)$ は $(i\infty)$ と (0) の 2 点を尖点にもつ. $\mathbb{P}^1(\mathbb{Q})$ の点としては $i\infty$ でなく単に ∞ と書くべきであろうが, 上半平面 $\mathfrak{H}$ から $\infty \in \mathbb{P}^1(\mathbb{Q})$ は虚部が無限大の方向に見えるので $i\infty$ と書いた. $X_0(23)$ を $\Gamma_0(23)$ に関する**モジュラー曲線** (modular curve) という. 幾つか計算する方法があるがともかく $X_0(23)$ の種数は 2 の超楕円曲線である. また $\Gamma_0(23)$ に関する重さ 2 の尖点形式 (cusp form) は, $X_0(23)$ の正則微分に対応する. 古典的だが Dedekind の ***η*-函数** を使って尖点形式を作る. η-函数は無限積により定義される $\mathfrak{H}$ 上の非零正則函数で, 変換公式を満たす.

$$\eta(\tau) = q^{1/24} \prod_{n=1}^{\infty} (1-q^n) \qquad (q = e^{2\pi i \tau})$$
$$\eta(\tau+1) = e^{2\pi i/24}\,\eta(\tau)\ , \quad \eta(-1/\tau) = \sqrt{-i\,\tau}\,\eta(\tau)$$

命題 5.36 (1) $f_{23}(\tau) = \eta(\tau)^2\,\eta(23\tau)^2$ は $\Gamma_0(23)$ に関する重さ 2 の尖点形式である.

(2) Hecke 作用素 T_2 で移した $f_{23}|T_2(\tau)$ も尖点形式で, $2\pi i\, f_{23}(\tau)\,d\tau$, $2\pi i\, f_{23}|T_2(\tau)\,\tau$ は, $\Gamma_0(23)$ に関する重さ 2 の尖点形式全体のなす $\mathbb{C}$ 線形空間の基底である.

(b) $X_0(23)$ の正則微分 $2\pi i\, f_{23}(\tau)\,d\tau$ は, アフィン部分曲線 $Y_0(23)$ の上では零点をもたない. $X_0(23)$ の尖点 $(i\infty)$ における局所助変数 $q = e^{2\pi i\tau}$ で $2\pi i\, f_{23}(\tau)\,d\tau$ を展開すると,

$$2\pi i\, f_{23}(\tau)\,\frac{d\tau}{dq} = q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} + 2q^{14} + 3q^{15} + \cdots$$

なので, $(i\infty)$ で 1 位の零となる. Riemann-Roch の定理より微分因子の次数は 2 なので, もう一つの尖点 (0) でも $2\pi i\, f_{23}(\tau)\,d\tau$ は 1 位の零になる. $X_0(23)$ の微分因子として $\mathrm{div}(2\pi i\, f_{23}(\tau)\,d\tau) = (i\infty) + (0)$ を得る. $(i\infty) + (0)$ は標準整因子だから, $(i\infty)$ と (0) は超楕円対合で移りあう. 一方, $2\pi i\, f_{23}|T_2(\tau)\,d\tau$ も正則微分だが,

$$2\pi i\, f_{23}|T_2(\tau)\,\frac{d\tau}{dq} = 1 - q + q^2 - 2q^4 - 3q^5 + q^7 + 2q^8 + 4q^9 - 2q^{10} + 2q^{11} + 3q^{12} + 2q^{13} + \cdots$$

なので $(i\infty)$ を零点にもたない. 従って (0) も零点にもたない. 特に $2\pi i\, f_{23}(\tau)\,d\tau$ と $2\pi i\, f_{23}|T_2(\tau)\,d\tau$ は一次独立である. $K = (i\infty) + (0)$ とおく. $x = 2\pi i\, f_{23}|T_2(\tau)\,d\tau / 2\pi i\, f_{23}(\tau)\,d\tau$ とおくと, x は $L(K)$ に属する非定数函数である. 実際, $(i\infty)$ の局所助変数 q で x を展開すると,

$$x = \frac{2\pi i\, f_{23}|T_2(\tau)\,d\tau}{2\pi i\, f_{23}(\tau)\,d\tau} = \frac{f_{23}|T_2(\tau)}{f_{23}(\tau)} = q^{-1} + 1 + 4q + 7q^2 + 13q^3 + 19q^4 + 33q^5 + 47q^6 + 74q^7 + \cdots$$

となるので, x は $(i\infty)$ で丁度 1 位の極をもつ. $X_0(23)$ の有理函数 $y \in L(3\,K)$ をうまく選んで, $X_0(23)$ を $y^2 = (x \text{ の } 6 \text{ 次多項式})$ で定義することができる. $X_0(23)$ の正則微分は $\frac{dx}{y}$, $x\,\frac{dx}{y}$ を基底にもつ. ここで $\mathrm{div}(\frac{dx}{y}) = K$ なので, y を適当に定数倍して $\frac{dx}{y} = 2\pi i\, f_{23}(\tau)\,d\tau$ とおける. x の選び方から $x\,\frac{dx}{y} = 2\pi i\, f_{23}|T_2(\tau)\,d\tau$ となる. 以上により, 有理函数 y の局所助変数 q による展開が得られる.

$$y = \frac{dx}{2\pi i\, f_{23}(\tau)\,d\tau} = \frac{q}{f_{23}(\tau)}\frac{dx}{dq} = -q^{-3} - 2q^{-2} - q^{-1} + 12 + 67q + 228q^2 + 667q^3 + 1696q^4 + \cdots$$

有理函数 x, y は $y^2 = (x \text{ の } 6 \text{ 次多項式})$ なる関係式を満たす. $y^2 - (x \text{ の } 6 \text{ 次多項式}) = 0$ なので左辺の q-展開の係数が 0 になるように x の多項式の係数を順に決めていけばよい. こうして x, y は

$$y^2 = x^6 - 2x^5 - 23x^4 - 50x^3 - 58x^2 - 32x - 11$$

を満たすことがわかる. よく知られた形に合わせるために x を $x-1$ に置き換えると,

定理 5.37 $Y_0(23)$ は $y^2 = x^6 - 8x^5 + 2x^4 + 2x^3 - 11x^2 + 10x - 7$ で定義される非特異アフィン平面曲線で, $X_0(23)$ はその非特異完備化である. また $X_0(23)$ の函数体 (**モジュラー函数体** という) $A_0(23)$ は $\mathbb{C}$ 上

x, y で生成される.

問 61　$x = f_{23}|T_2(\tau)/f_{23}(\tau)$, $y = dx/2\pi i\, f_{23}(\tau)\, d\tau$ の q-展開を使って, x の多項式 $f(x)$ で $y^2 - f(x)$ の q-展開が正のベキしか現れないものが取れることを示せ. このとき有理函数として $y^2 - f(x) = 0$ が成り立つことを示せ.

問 62　Hecke 作用素 T_2 は, 重さ 2 の尖点形式のなす 2 次元 $\mathbb{C}$ 線形空間 ($f_{23}(\tau)$, $f_{23}|T_2(\tau)$ を基底にもつ) の上に線形に作用する. $(f_{23}|T_2)|T_2(\tau) = f_{23}(\tau) - f_{23}|T_2(\tau)$ となることを使って, T_2 に関する固有形式を求めよ.

問 63　$[P_\infty - P'_\infty] \in \mathrm{Pic}^0(X_0(23))$ の 2 倍点, 3 倍点, 4 倍点, $\cdots$ を計算せよ.

§5.15　種数 2 のモジュラー曲線 $X_0(22)$

(a)　前節と同様に, 合同部分群 $\Gamma_0(22)$ に関するモジュラー曲線 $X_0(22) = \Gamma_0(22)\backslash\mathfrak{H}^*$ を考える. 閉 Riemann 面 $X_0(22)$ もまた種数が 2 の超楕円曲線である.

$$f_{11}(\tau) = \eta(\tau)^2\,\eta(11\tau)^2 = q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 + \cdots$$

は $\Gamma_0(11)$ の重さ 2 の尖点形式なので, $\Gamma_0(22)$ の重さ 2 の尖点形式でもある.

$$f_{22}(\tau) = f_{11}(2\tau) = \eta(2\tau)^2\,\eta(22\tau)^2 = q^2 - 2q^4 - q^6 + 2q^8 + q^{10} + 2q^{12} - 2q^{14} + \cdots$$

もまた $\Gamma_0(22)$ の重さ 2 の尖点形式で, $f_{11}(\tau)$ と一次独立である.

命題 5.38　(1)　$X_0(22)$ の尖点は $(i\,\infty)$, (0), $(1/2)$, $(1/11)$ の 4 点である.

(2)　$X_0(22)$ の微分 $2\pi i\, f_{11}(\tau)\, d\tau$ と $2\pi i\, f_{22}(\tau)\, d\tau$ の因子はそれぞれ $(0)+(1/11)$ と $(i\infty)+(1/2)$ である.

前節と同様に $x = f_{11}(\tau)/f_{22}(\tau)$, $y = dx/2\pi i\, f_{22}(\tau)\, d\tau$ をとおくと, $x \in L(K)$, $y \in L(3\,K)$ ($K = (i\infty) + (1/2)$) で, $y^2 =$ (x の 6 次式) なる代数関係式を満たす.

定理 5.39　$X_0(22)$ は $y^2 = x^6 + 12x^5 + 56x^4 + 148x^3 + 224x^2 + 192x + 64$ で定義される種数 2 の超楕円曲線で, モジュラー函数体 $A_0(22)$ は $\mathbb{C}$ 上 x, y で生成される. $X_0(22)$ の尖点 $(i\infty)$, $(1/2)$ は 2 つの無限遠点に対応し, 残りの尖点 (0), $(1/11)$ はそれぞれ $(0, -8)$, $(0, 8)$ で表される点に対応する. 特に $(i\infty)$ の近傍では $y = -x^3 - 6x^2 - 10x - 14 + 22x^{-1} - 88x^{-2} + 374x^{-3} + \cdots$ と $1/x$ の Laurent 級数に展開できる.

問 64　(1)　τ を $\mathfrak{H}^*$ の座標とする. 尖点 $(i\infty)$, $(1/11)$, (0), $(1/2) \in X_0(22)$ の局所助変数として, $q{=}\exp(2\pi i\,\tau)$, $q_{11}{=}\exp(2\pi i\,(\tau/(1-11\tau))\,/2)$, $q_0{=}\exp(2\pi i\,(-1/\tau)\,/22)$, $q_2{=}\exp(2\pi i\,(\tau/(1-2\tau))\,/11)$ が取れることを示せ.

(2)　有理函数 x, y を各尖点の局所助変数で展開し, どの展開を使っても同じ代数関係式を満たすことを確かめよ.

(b)　超楕円曲線 $C = X_0(22)$ の超楕円対合は, 定義方程式 $y^2 = x^6{+}12x^5{+}56x^4{+}148x^3{+}224x^2{+}192x{+}64$ のアフィン座標系 x, y で $\iota : (x, y) \longmapsto (x, -y)$ と書ける. 定義方程式を相反型

$$(y/8)^2 = (x/2)^6 + 6(x/2)^5 + 14(x/2)^4 + 37/2(x/2)^3 + 14(x/2)^2 + 6(x/2) + 1$$

にまとめることができるので, C の Weierstrass 点の x-座標を置換する一次分数変換 $x \longmapsto 4/x$ がある. この一次分数変換は C の自己同型写像 σ, σ' に延びる.

$$\sigma : (x, y) \longmapsto (4/x, -8y/x^3)\ , \quad \sigma' : (x, y) \longmapsto (4/x, 8y/x^3)$$

$\sigma^2 = \mathrm{id}$, $\sigma' = \sigma\iota = \iota\sigma$ なので σ は ι と可換な位数 2 の自己同型写像である. C の自己同型群 $\mathrm{Aut}(C)$ は $(2, 2)$-型群 $\langle\iota, \sigma\rangle$ を部分群にもつ. $\mathrm{Aut}(C)$ の部分群 $\langle\sigma\rangle$, $\langle\sigma\iota\rangle$, $\langle\iota\rangle$ に関する商代数曲線をそれぞれ C_σ, C'_σ,

C_ι とおく. 超楕円対合 ι は 2 次被覆 $x : C \to \mathbb{P}^1$ の被覆変換群の生成元なので, $C_\iota \simeq \mathbb{P}^1$ である. C_σ, C'_σ に対して自然な被覆写像 $f : C \to C_\sigma$, $g : C \to C'_\sigma$ は 2 次 Galois 被覆で, Galois 群はそれぞれ $\langle\sigma\rangle$, $\langle\sigma\iota\rangle$ である. C_σ, C'_σ の種数はともに 2 より小さいが, もし C_σ の種数が 0 (C_σ が $\mathbb{P}^1$ に同型) なら, σ もまた $X_0(22)$ の超楕円対合でなければならない. 種数が 2 以上の超楕円曲線において超楕円対合は唯一つなので, C_σ は $\mathbb{P}^1$ に同型ではない. C_σ の種数は 1 である. 同じく C'_σ の種数も 1 である. 被覆写像 $f : C \to C_\sigma$, $g : C \to C'_\sigma$ が引き起こす, 因子類群の準同型写像

$$f^* : \mathrm{Pic}^0(C_\sigma) \to \mathrm{Pic}^0(C) \qquad f_* : \mathrm{Pic}^0(C) \to \mathrm{Pic}^0(C_\sigma)$$
$$g^* : \mathrm{Pic}^0(C'_\sigma) \to \mathrm{Pic}^0(C) \qquad g_* : \mathrm{Pic}^0(C) \to \mathrm{Pic}^0(C'_\sigma)$$

をとる. f_*, g_* は明らかに全射で, 合成 $f_* \circ f^*$ は $\mathrm{Pic}^0(C_\sigma)$ の, $g_* \circ g^*$ は $\mathrm{Pic}^0(C'_\sigma)$ の 2-倍写像である. f, g は種数 2 の代数曲線から種数 1 の代数曲線への 2 次被覆なので, 丁度 2 点が分岐する. $P_1 \in C$ を f の分岐点とすると, $G_f = \langle\sigma\rangle$ なので $\sigma(P_1) = P_1$ となる. $\sigma(P'_1) = \sigma(\iota(P_1)) = \sigma\iota(P_1) = \iota\,\sigma(P_1) = \iota(\sigma(P_1)) = \iota(P_1) = P'_1$ なので, もう一つの分岐点は P'_1 である. 同様にして g の分岐点を P_2, $P'_2 \in C$ とおくことができる. 実際 P_1, $P'_1 = (-2, \pm 4\sqrt{-2})$ で, P_2, $P'_2 = (2, \pm 44\sqrt{2})$ である.

命題 5.40 (1) $P \in C$ に対して $f(\sigma\iota(P)) = f(P')$, $g(\sigma(P)) = g(P')$ が成り立つ.
(2) $\ker f^* = \langle f_*[P_2 - P'_2]\rangle$, $\ker g^* = \langle g_*[P_1 - P'_1]\rangle$ でともに位数 2 の巡回群をなす.
(3) $f_* \circ g^*$, $g_* \circ f^*$ は零写像である.

定理 5.41 $\varphi = (f_*, g_*) : \mathrm{Pic}^0(C) \ni [D] \longmapsto (f_*[D], g_*[D]) \in \mathrm{Pic}^2(C_\sigma) \times \mathrm{Pic}^0(C'_\sigma)$
$\psi = f^* + g^* : \mathrm{Pic}^0(C_\sigma) \times \mathrm{Pic}^0(C'_\sigma) \ni ([D_1], [D_2]) \longmapsto f^*[D_1] + g^*[D_2] \in \mathrm{Pic}^0(C)$
とおくと, $\psi \circ \varphi$ は $\mathrm{Pic}^0(C_\sigma) \times \mathrm{Pic}^0(C'_\sigma)$ の, $\varphi \circ \psi$ は $\mathrm{Pic}^0(C)$ の 2-倍写像である.

(c) 商代数曲線 C_σ の函数体 $\mathbb{C}(C_\sigma)$ はモジュラー函数体 $A_0(22) = \mathbb{C}(x, y)$ の $\langle\sigma\rangle$-不変体である. $\sigma(x) = 4/x$, $\sigma(y) = -8\,y/x^3$ より, $w = x + 4/x$, $z = y\,(x-2)/x^2$ は σ-不変である. $A_0(22) \supset A_0(22)^{\langle\sigma\rangle} = \mathbb{C}(C_\sigma) \supset \mathbb{C}(w, z)$ で, $[A_0(22) : \mathbb{C}(C_\sigma)] = [A_0(22) : \mathbb{C}(w, z)] = 2$ なので $\mathbb{C}(C_\sigma) = \mathbb{C}(w, z)$ を得る. 従って C_σ は

$$z^2 = (w-4)\,(w^3 + 12\,w^2 + 44\,w + 52)$$

で定義されるアフィン平面曲線と双有理同値で, その非特異完備化に一致する. §2.6 (d) の 2 つ目に従うと, C_σ は

$$v_1^2 = u_1^3 + 188\,u_1^2 + 11616\,u_1 + 234256$$

で定義される楕円曲線になる. ただし $u_1 = 484/(w-4)^2 = 484\,x/(x-2)^2$, $v_1 = 484\,z_1/(w-4)^2 = 484\,y/(x-2)^3$ とおいた. 楕円曲線において, 無限遠点を動かさない同型変換で, 少し雑な言い方だが, 係数ができるだけ小さくなるようにすることができる. こうして得られる楕円曲線の定義方程式を**極小 Weierstrass 方程式**という. 今の場合 $u = 121\,x/(x-2)^2 + 16$, $v = (121\,y/(x-2)^3 - 1)/2$ とおくと, 有理写像

$$f = (u, v) : X_0(22) \ni P \longmapsto (u(P), v(P)) \in \mathbb{P}^2$$

の像は Weierstrass 方程式 $v^2 + v = u^3 - u^2 - 10\,u - 20$ で定義される楕円曲線で, C_σ に同型である. この方程式は, モジュラー曲線 $X_0(11)$ の定義方程式と同じ物なので, C_σ は $X_0(11)$ と同型であることがわかる. u, v を尖点 $i\infty \in X_0(22)$ の局所助変数 $q = e^{2\pi i\tau}$ で展開すると,

$$u = 16 + 121\,q + 726\,q^2 + 3751\,q^3 + 18150\,q^4 + 83853\,q^5 + 375826\,q^6 + 1647294\,q^7 + \cdots$$
$$v = -61 - 726\,q - 5687\,q^2 - 37147\,q^3 - 216711\,q^4 - 1175273\,q^5 - 6050968\,q^6 - 29973878\,q^7 - \cdots$$

となる. 従って C_σ の不変微分 $\omega = du/(2v+1)$ は

$$\omega = (-q + q^3 + 2\,q^4 - q^5 + 2\,q^7 - 4\,q^8 + 2\,q^9 - q^{11} - 2\,q^{12} - 4\,q^{13} + q^{15} + 4\,q^{16} + 2\,q^{17} + \cdots)\,\frac{dq}{q}$$

と q で展開される. $\Gamma_0(11)$ に関する重さ 2 の尖点形式 $f_{11}(\tau) = \eta(\tau)^2\,\eta(11\tau)^2$ の q-展開係数と比較すると偶数次の項が食い違っている. もう少しよく観察すると,

$$\omega = -2\pi i\,(f_{11}(\tau) + 2\,f_{22}(\tau))\,d\tau$$

が成り立ちそうで, 実際容易に示せる. モジュラー曲線 $X_0(11)$ と同型と言うなら, 不変微分が尖点形式 f_{11} に対応すべきなのだが. どうしてこの様なずれが生じたのであろうか.

C_σ と $X_0(11)$ との同型は, 単に同じ Weierstrass 方程式で定義された代数曲線だったからで, モジュラー函数体として $\mathbb{C}(u, v)$ $(\subset A_0(22))$ と $A_0(11)$ が一致したわけではない. $(\Gamma_0(11):\Gamma_0(22)) = 3$ なので, $A_0(11)$ は $A_0(22)$ の 3 次部分体になり, u, v は $A_0(11)$ に含まれない. モジュラー函数 u, v の level は 22 で 11 ではない. 一方, 尖点形式 $f_{11} + 2\, f_{22}$ は, $\Gamma_0(22)$ に関する重さ 2 の Hecke 固有形式である. Atkin-Lehner 対合 W_2, W_{11} に関しても, $f_{11}|W_2 = 2\, f_{22}$, $f_{22}|W_2 = 1/2\, f_{11}$, $f_{11}|W_{11} = -f_{11}$, $f_{22}|W_{11} = -f_{22}$ なので,

$$(f_{11} + 2\, f_{22})|W_2 = f_{11} + 2\, f_{22}\ , \quad (f_{11} + 2\, f_{22})|W_{11} = -(f_{11} + 2\, f_{22})$$

となる. C_σ には, 有理写像 $f : X_0(22) \to C_\sigma \subset \mathbb{P}^2$ を通して, モジュラー媒介変数表示 (modular parametrization) が与えられる. 楕円曲線 C_σ の不変微分はこの表示の下で, $\Gamma_0(22)$ に関する重さ 2 の Hecke 固有尖点形式 $f_{11}+2\, f_{22}$ に対応する. level 22 のモジュラー函数で媒介変数表示された C_σ の不変微分には, Atkin-Lehner 対合 W_2 の固有形式ではない level 11 の f_{11} よりも, level 22 の $f_{11}+2\, f_{22}$ が対応するほうが自然であろう.

問 65　$W_2=\begin{pmatrix}12 & 1\\ 22 & 2\end{pmatrix}$, $W_{11}=\begin{pmatrix}11 & 5\\ 22 & 11\end{pmatrix}$ とおく. $f|W_2(\tau) = \dfrac{2}{(22\tau+2)^2}\, f(W_2\tau)$, $f|W_{11}(\tau) = \dfrac{11}{(22\tau+11)^2}\, f(W_{11}\tau)$ で Atkin-Lehner 対合を定義する. η-函数の変換公式を使って, $f_{11}|W_2$, $f_{11}|W_{11}$, $f_{22}|W_2$, $f_{22}|W_{11}$ を計算せよ.

問 66　(1)　$f = (u, v) : X_0(22) \to C_\sigma$ において, C_σ の無限遠点の逆像を求めよ.
(2)　尖点 $(i\infty)$, $(1/2)$, (0), $(1/11) \in X_0(22)$ の f による像を求めよ.
(3)　楕円曲線 C_σ の加法で $f((i\infty)) \in C_\sigma$ は 5 倍すると零元になることを示せ.
(4)　$\mathrm{Pic}^0(X_0(22))$ において, 因子類 $[(i\infty) - (1/2)]$ は何倍かすると 0 になることを示せ.

問 67　(1)　w, z の q-展開を計算し, z を $1/w$ の Laurent 級数に展開せよ.
(2)　$s = (z + w^2 + 4w)/2$, $t = z\,(w + 2)/2 + w^3/2 + 3w^3 - w - 16$ とおく. s, t の q-展開を計算せよ.
(3)　s, t の満たす代数関係式を求め, C_σ が $X_0(11)$ に同型であることを確かめよ.
(4)　s, t による C_σ の定義方程式に関する不変微分を, 尖点形式 f_{11}, f_{22} で表せ.

問 68　商代数曲線 $C'_\sigma = X_0(22)/\langle\sigma\iota\rangle$ について, 上と同様の計算をしてみよ.
(1)　$u = x/(x+2)^2$, $v = (y/(x+2)^3 - 1)/2 \in \mathbb{C}(X_0(22))$ は $\sigma\iota$ 不変であることを示せ.
(2)　u, v を $X_0(22)$ の尖点 $(i\infty)$ の局所助変数 q に関する Laurent 級数に展開せよ.
(3)　$\mathbb{C}(C'_\sigma) = A_0(22)^{\langle\sigma\iota\rangle} = \mathbb{C}(u, v)$ を示し, u, v の満たす代数関係式を求めよ.
(4)　上で求めた代数関係式で定義された楕円曲線としての C_σ について, 不変微分を q で展開せよ.
(5)　C'_σ の不変微分を尖点形式 f_{11}, f_{22} で表せ.

(d)　上の被覆 $f : X_0(22) \to C_\sigma$ は, 尖点 $(i\infty) \in X_0(22)$ が C_σ の無限遠点に移るように作ってはいなかった. C_σ の座標を射影平面内で取り替えて $(i\infty)$ の像を無限遠点にすることができるが, 初めから $(i\infty)$ の像が (Weierstrass 方程式に関する) 無限遠点 (加法の零元) になるように, 被覆 $X_0(22) \to C_\sigma$ を作ってみる. このことにより, $(i\infty) \in X_0(22)$ の局所助変数 q の C_σ における意味がより直接的に見えるようになるであろう. 以下 $L(*)$ が多数出てくる. どの代数曲線上の有理函数か区別するために, 単に $L(*)$ と書くと $X_0(22)$ の有理函数からなるもの, $L_\sigma(*)$ と書くことで C_σ の有理函数からなるものを表すことにする.

有理写像 $f = (u, v) : X_0(22) \to C_\sigma \in \mathbb{P}^2$ を, 尖点 $(i\infty) \in X_0(22)$ が C_σ の零元 (Weierstrass 方程式での無限遠点) に移るものとする. 有理函数 u, $v \in A_0(22)$ で $(i\infty) \in X_0(22)$ の像が無限遠点に移るものを作ればよい. f は Galois 被覆なので, u, v は Galois 不変である. 従って u_0, $v_0 \in \mathbb{C}(C_\sigma)$ で $f^*u_0 = u$, $f^*v_0 = v$ となるものが取れる. u_0, v_0 を座標函数とする C_σ の定義方程式が Weierstrass 方程式になるためには, $\infty_\sigma \in C_\sigma$ を適当に選んで $u_0 \in L_\sigma(2\,\infty_\sigma)$, $v_0 \in L_\sigma(3\,\infty_\sigma)$ となればよい. このとき ∞_σ が無限遠点に相当する. 尖点 $(i\infty) \in X_0(22)$ は ∞_σ に移されるので, $(1/11) = \sigma(i\infty)$ もまた ∞_σ に移される.

$D_\sigma = f^*\infty_\sigma = (i\infty) + (1/11) \in \mathrm{Div}(X_0(22))$ とおく．D_σ は σ 不変なので, σ^* は $L(m\,D_\sigma)$ $(m \in \mathbb{Z})$ に作用する．$L(m\,D_\sigma)^{\pm} = \{h \in L(m\,D_\sigma) \,|\, \sigma^* h = \pm h\}$ とおくと, $L(m\,D_\sigma) = L(m\,D_\sigma)^+ \oplus L(m\,D_\sigma)^-$ と直和分解する．m を自然数とする．$h_0 \in L_\sigma(m\,\infty_\sigma)$ に対して,

$$\mathrm{div}(f^*h_0) = f^*\mathrm{div}(h_0) \geq f^*(-m\,\infty_\sigma) = -m\,D_\sigma$$

となり, f^*h_0 は σ 不変なので, 線形写像 $L_\sigma(m\,\infty_\sigma) \ni h_0 \longmapsto f^*h_0 \in L(m\,D_\sigma)^+$ が定まる．そもそも $f^* : \mathbb{C}(C_\sigma) \to A_0(22)$ は単射なので, $L_\sigma(m\,\infty_\sigma)$ への制限も単射である．C_σ の種数は 1 なので $\ell_\sigma(m\,\infty) = m$ が成り立つ．以上より $\dim L(m\,D_\sigma)^+ = m$ $(m \in \mathbb{N})$ を得る．また $\ell(m\,D_\sigma) = 2\,m{-}1$ なので $\dim L(m\,D_\sigma)^- = m - 1$ となる．

$\dim L(m\,D_\sigma)^+ = m$ より, $u \in L(2\,D_\sigma)^+ \smallsetminus \mathbb{C}$, $v \in L(3\,D_\sigma)^+ \smallsetminus L(2\,D_\sigma)^+$ が存在する．このとき, 有理写像

$$f = (u,\, v) : X_0(22) \ni P \longmapsto (u(P),\, v(P)) \in C_\sigma \subset \mathbb{P}^2$$

が目的の 2 次被覆である．基礎曲線は Weierstrass 方程式で定義される非特異射影平面曲線 C_σ で, 尖点 $(i\infty) \in X_0(22)$ は零元 (無限遠点 ∞_σ) にうつる．$(i\infty)$ において f は不分岐なので, $\infty_\sigma \in C_\sigma$ の局所助変数 q_0 で $f^*q_0 = q$ となるものが存在する．つまり, f は完備離散付値体の同型 $A_0(22)_{(i\infty)} \simeq \mathbb{C}(C_\sigma)_{\infty_\sigma}$ を引き起こす．この同型により局所体を同一視すれば, q は $\infty_\sigma \in C_\sigma$ の局所助変数となる．

(e) 上の手続きを具体的に実行してみる．$K_\infty = (i\infty) + (1/2)$, $K_0 = (0) + (1/11)$, $D_\sigma = (i\infty) + (1/11) \in \mathrm{Div}(X_0(22))$ とおく．(a) で, $x = f_{11}(\tau)/f_{22}(\tau)$, $y = dx/2\pi i\, f_{22}(\tau)\, d\tau \in A_0(22)$ と取ると, $x \in L(K)$, $y \in L(3\,K)$, $A_0(22) = \mathbb{C}(x,\, y)$ を満たす．$X_0(22)$ は $y^2 = x^6 + 12\,x^5 + 56\,x^4 + 148\,x^3 + 224\,x^2 + 192\,x + 64$ で定義される種数 2 の超楕円曲線で, 尖点 $(i\infty)$, $(1/2)$ はその無限遠点にあたる．尖点 $(i\infty)$ の局所助変数 q で展開することで, y の $1/x$ に関する Laurent 級数展開 $(y = -x^3{-}6\,x^2{-}10\,x{-}14{+}22\,x^{-1}{-}88\,x^{-2}{+}374\,x^{-3}{+}\cdots)$ を得た．η-函数の変換公式などを使って, $(1/2) \in X_0(22)$ の近傍でも y を $1/x$ で展開することができるが, $(i\infty)$ と $(1/2)$ が超楕円対合で移りあう無限遠点であることと, $1/x$ が無限遠点の局所助変数であることに注意すれば, 直ちに

$$y = x^3 + 6\,x^2 + 10\,x + 14 - 22\,x^{-1} + 88\,x^{-2} - 374\,x^{-3} - \cdots$$

が言える．$v_1 = y - (x^3 + 6\,x^2 + 10\,x)$ とおく．$v_1 \in K(3\,K)$ だが $\mathrm{ord}_{(1/2)}(v_0) \geq 0$ なので, $v_1 \in L(3\,(i\infty))$ である．$\ell(3\,(i\infty)) = 3 - 2 + 1 = 2$ より, $L(3\,(i\infty)) = \mathbb{C} + \mathbb{C}\,v_1$ となる．$\sigma^*(i\infty) = (1/11)$ なので, $\sigma^*v_1 \in L(3\,(1/11))$, $L(3\,(1/11)) = \mathbb{C}{+}\mathbb{C}\,\sigma^*v_1$ となる．ここで $v = -(v_1{+}\sigma^*v_1)/2$ とおくと, $v \in L(3\,D_\sigma)^+ \smallsetminus L(2\,D_\sigma)^+$ となる．

有理函数 $x\,\sigma^*v_1$ を $(1/2)$ の近傍で展開すると

$$x\,\sigma^*v_1 = -8\,x - 88 - 176\,x^{-1} - 176\,x^{-2} + 176\,x^{-3} + 704\,x^{-4} - 2992\,x^{-5} + \cdots$$

となる．$u_1 = x\,\sigma^*v_1{+}8\,x$ とおくと, $L((i\infty){+}2\,(1/11)) = \mathbb{C}{+}\mathbb{C}\,u_1$ が従う．さらに $L(2\,(i\infty){+}(1/11)) = \mathbb{C}{+}\mathbb{C}\sigma^*u_1$ なので $L(2\,D_\sigma) = \mathbb{C}{+}\mathbb{C}\,u_1{+}\mathbb{C}\,\sigma^*u_1$ を得る．ここで $u = -(u_1{+}\sigma^*u_1)/8$ とおくと, $u \in L(2\,D_\sigma)^+ \smallsetminus \mathbb{C}$ を満たす．

以上で具体的に作った $u \in L(2\,D_\sigma)^+ \smallsetminus \mathbb{C}$, $v \in L(3\,D_\sigma)^+ \smallsetminus L(2\,D_\sigma)^+$ を使って, 有理写像

$$f = (u,\, v) : X_0(22) \ni P \longmapsto (u(P),\, v(P)) \in C_\sigma \subset \mathbb{P}^2$$

を定義する．f は尖点 $(i\infty) \in X_0(22)$ を C_σ の無限遠点にうつす 2 次被覆で, f の像としての $C_\sigma \subset \mathbb{P}^2$ は

$$C_\sigma : v^2 + 17\,v = u^3 - 19\,u^2 + 110\,u - 284$$

で定義される．$(i\infty) \in X_0(22)$ の局所助変数 q により, 座標函数 u, v と不変微分 $\omega = du/(2v + 17)$ は

$$u = 1/q^2 + 7 + q + 2\,q^2 + q^3 + 3\,q^4 - 3\,q^5 - 6\,q^7 + 2\,q^8 + 6\,q^9 + \cdots$$
$$v = 1/q^3 + 1/q - 7 - 2\,q + 2\,q^2 - 4\,q^3 + 6\,q^5 + 10\,q^6 - 7\,q^7 + 8\,q^8 + 2\,q^9 \cdots$$
$$\omega = (-q + q^3 + 2\,q^4 - q^5 + 2\,q^7 - 4\,q^8 + 2\,q^9 - q^{11} - 2\,q^{12} - 4\,q^{13} + q^{15} + 4\,q^{16} + 2\,q^{17} + \cdots)\,\frac{dq}{q}$$

と展開される．この場合もやはり $\omega = -2\pi i\,(f_{11}(\tau) + 2\,f_{22}(\tau))\,d\tau$ となる．C_σ のモジュラー媒介変数表示 u, v の与え方は少し面倒であったが, q-展開係数がちょっと驚くほど小さくなっていることを注意しておく．

問 69　上で得た $C_\sigma \subset \mathbb{P}^2$ の定義方程式から, C_σ は $X_0(11) : y^2 + y = x^3 - x^2 - 10\,x - 20$ に楕円曲線として同型であることを示せ. また C_σ の座標関数 u, v を, 尖点 $(1/11) \in X_0(22)$ の局所助変数 q_{11} で展開せよ.

問 70　(1)　尖点 $(0) \in X_0(22)$ を C_σ の無限遠点にうつす 2 次被覆 $f_0 = (u_0, v_0) : X_0(22) \to C_\sigma$ を与えよ.

(2)　座標函数 u_0, v_0 を $(0) \in X_0(22)$ の局所助変数 q_0 で展開せよ.

(3)　尖点 $(i\infty) \in X_0(22)$ を C'_σ の無限遠点にうつす 2 次被覆 $g = (u, v) : X_0(22) \to C'_\sigma$ を与えよ.

(4)　座標函数 u, v, 不変微分 ω を $(i\infty) \in X_0(22)$ の局所助変数 $q = \exp(2\pi i\,\tau)$ で展開せよ.

(5)　尖点 $(0) \in X_0(22)$ に対して, (3), (2) と同じことを試みよ.

第 15 回 整数論サマースクール 報告集, pp.61-80

Abel-Jacobi の定理 I

軍司圭一 *

1 Introduction

この稿では Riemann 面の理論において最も基本的な定理と言うべき Abel-Jacobi の定理について概説する．X を種数 g のコンパクト Riemann 面とし，X 上の正則微分形式のなすベクトル空間の基底を $\omega_1, \ldots, \omega_g$ とおく．$\Lambda = \{(\int_\gamma \omega_1, \ldots, \int_\gamma \omega_g) \in \mathbb{C}^g \mid \gamma \in H_1(X, \mathbb{Z})\}$ とおくと Λ は $\mathbb{C}^g$ の lattice であり，$\mathrm{Jac}(X) = \mathbb{C}^g/\Lambda$ はコンパクト複素 Lie 群となる．この状況の下で，Abel-Jacobi の定理 (Theorem 2.2, 4.2) は $\mathrm{Jac}(X)$ が後に述べる Picard 多様体の性質を満たすこと，すなわち 0 次の因子類群 $\mathrm{Pic}^0(X)$ と群同型であることを主張する．

この定理は古典的であり非常によく知られているが，その証明はそれほど易しくはない．本稿では証明や議論の流れは完全に，D. Mumford の教科書 ([Mum, Chapter II]) に依った．その他にも文献は非常に数多くあり，とても全部は網羅することはできない．代表的なものとしては [Shi, 第六章] や [Lan] などが挙げられるであろう．また本報告集でも紹介されるように，別な切り口からの証明として [Iwa] もあげておく．Mumford の議論の特徴的な点としては，theta 関数を前面に押し出していることがあげられる．とくにその (Riemann 面に引き戻した関数の) 零因子に関する情報を与える Riemann の定理 (定理 6.2) が，議論の一番のキーとなる．

ここではまず，Jacobi 多様体の幾何的な意味を完全に理解してもらうため，蛇足とは思ったが §2 で直線束と因子類群との関係から話を始め，その上で直線束のモジュライとしての Jacobi 多様体への意味づけを与える．§3，§4 で Jacobi 多様体及び次数 0 の因子類群からの周期写像の構成を具体的に与え，その上で Abel-Jacobi の定理の主張を述べる．定理の証明のために曲線の対称積 (§5) や theta 関数 (§6) を準備した後，いよいよ §7 が証明である．

なお代数幾何の知識を持っているものには，Abel-Jacobi の定理は非常に易しく思えるかもしれない．層の完全列 $0 \to \mathbb{Z} \to \mathcal{O}_X \to \mathcal{O}_X^\times \to 0$ から誘導される長完全列

$$\cdots \to H^1(X, \mathbb{Z}) \to H^1(X, \mathcal{O}_X) \to H^1(X, \mathcal{O}_X^\times) \xrightarrow{\varphi} H^2(X, \mathbb{Z}) \to \cdots$$

及び Poincaré 双対性 $H_1(X, \mathbb{Z}) \simeq H^1(X, \mathbb{Z})$ と Serre の双対定理 $H^1(X, \mathcal{O}_X) \simeq H^0(X, \Omega_X)^*$ より，$\mathrm{Jac}(X) = H^0(X, \Omega_X)^*/H_1(X, \mathbb{Z}) \simeq \mathrm{Ker}\,\varphi = \mathrm{Pic}^0(X)$ は容易に導

*東京大学大学院数理科学研究科 COE ポスドク， E-mail gunji@ms.u-tokyo.ac.jp

かれるからである．しかし Serre の双対定理の証明は決して易しくはない．別の言い方をすれば，Abel-Jacobi の定理の証明の難しさは，Serre 双対性の定理の証明にあるといってもよい．

最後に一言述べておきたい．Jacobi 多様体は複素多様体としてではなく，代数多様体とみなすことによって初めてその重要性が認識されると思われる．代数幾何的な Jacobi 多様体の重要な性質は，それが元の代数曲線と同じ体上定義されているという点である．すなわち Jacobi 多様体は与えられた体 k 上のアーベル多様体の実例として重要なものであり，逆に言うと，例えば有理数体上定義された Jacobi 多様体以外のアーベル多様体の例を与えることはかなり難しい．その意味では，複素数体上に話を限った本稿は，整数論的な応用という立場から見ればかなり物足りないといえるかもしれない．しかしながら実際には，$\mathrm{Jac}(X)$ の代数的な構成は簡単ではない．構成の基となるのは曲線 X の g 次の対称積 $X^{(g)}$ であるが，$X^{(g)}$ の群構造は Zariski 開集合上でしか定義されない．ここからアーベル多様体を構成する手順はかなり複雑である．代数幾何的な構成の原論文は [Weil] であり，現代的なスキーム論の立場での解説としては [Mil]，[BLR] などがあげられよう．また [Ser] では，特異点を持つようなより一般化された代数曲線に対しても Jacobi 多様体を構成している．興味のある方は是非一度目を通してみてください (筆者も読んでいませんので，是非教えてください)．

2 Jacobi 多様体，Picard 多様体

2.1 直線束

X を種数 g のコンパクトなリーマン面 (あるいは $\mathbb{C}$ 上の代数曲線) とする．X 上の点の形式的な有限和 $\sum n_P P$ を X 上の因子と呼ぶのであった．与えられた因子 D に対して，Riemann-Roch の定理は $L(D) = \{X \text{ 上の有理型関数 } f \mid (f) + D \geq 0\}$，すなわち各点 P で高々 n_P 位の極を持つような関数の成す空間の次元についての情報を与えるものであった (例えば $\deg D > 2g-2$ ならば次元そのものを与える)．この空間 $L(D)$ は，直線束の大域切断とみなすのが自然である．これを以下説明しよう．

X の直線束とは，“局所的に $X \times \mathbb{C}$ となっているような多様体” のことである．今 $X = \bigcup U_\alpha$ なる開被覆及び $U_\alpha \cap U_\beta \neq \emptyset$ なる α, β に対して $U_\alpha \cap U_\beta$ 上の零点を持たない正則関数 $g_{\alpha\beta}$ が与えられていて，次の性質を満たすとする:

(1) $g_{\alpha\alpha} = 1$.

(2) $g_{\beta\alpha} = g_{\alpha\beta}^{-1}$.

(3) $g_{\alpha\beta} g_{\beta\gamma} = g_{\alpha\gamma}$ ($U_\alpha \cap U_\beta \cap U_\gamma$ 上).

このとき $\bigcup(U_\alpha \times \mathbb{C})$ 上に同値関係を次のように入れる: $U_\alpha \times \mathbb{C} \ni (x_\alpha, u_\alpha) \sim (x_\beta, u_\beta) \in U_\beta \times \mathbb{C}$ であるとは $x_\alpha = x_\beta$ かつ $u_\alpha = g_{\alpha\beta}(x_\alpha) u_\beta$. このとき $\mathcal{L} = \bigcup(U_\alpha \times \mathbb{C})/\sim$ は複素多様体 (あるいは代数多様体) となり，$\pi\colon \mathcal{L} \to X$, $(x_\alpha, u_\alpha) \mapsto x_\alpha$ は well-defined な射影となる．

このようにして作られる $\mathcal{L}$ を X の直線束と呼ぶ．作り方より，直線束は張り合わせ関数 $\{g_{\alpha\beta}\}$ で決まる．2 つの直線束 $\mathcal{L}$ と $\mathcal{L}'$ が同型であるための条件は，その張り合わせ関数を $\{g_{\alpha\beta}\}$ 及び $\{g'_{\alpha\beta}\}$ としたとき (必要なら被覆を細分して共通のものをとっておく)，各 U_α 上に零点を持たない正則関数 h_α が存在して $g_{\alpha\beta} = h_\alpha^{-1} g'_{\alpha\beta} h_\beta$ が成り立つことである．

直線束の同型類全体を X の Picard 群と呼び，$\mathrm{Pic}(X)$ で表すことにする．名前のとおりこれには自然に群構造が入る．すなわち $\mathcal{L}$ の張り合わせ関数を $g_{\alpha\beta}$，$\mathcal{M}$ の張り合わせ関数を $h_{\alpha\beta}$ とするときに，張り合わせ関数が $g_{\alpha\beta}h_{\alpha\beta}$ で与えられるような直線束を $\mathcal{L}\otimes\mathcal{M}$ で表すことにする．この群構造の単位元はすべての g_{ij} が定数関数 1 で あるような直線束であり，これは $X\times\mathbb{C}$ に他ならない．これを自明な直線束といい $\mathcal{O}_X$ で表す．

$\Gamma(X,\mathcal{L}) = \{s\colon X \xrightarrow{\mathrm{hol}} \mathcal{L} \mid \pi\circ s = \mathrm{id}_X\}$ を $\mathcal{L}$ の大域切断と呼ぶ．自明な直線束に対しては $\Gamma(X,\mathcal{O}_X)$ は X 上定義された正則関数であり，定数関数全体 $\mathbb{C}$ と等しい．しかし一般の直線束 $\mathcal{L}$ に対しては $\Gamma(X,\mathcal{L})$ はより複雑であり，0 のみになることもありえる．

定義から $\Gamma(X,\mathcal{L}) = \{f_\alpha\colon U_\alpha \xrightarrow{\mathrm{hol}} \mathbb{C} \mid f_\alpha/f_\beta = g_{\alpha\beta}\}$ が分かる．

2.2 因子類群との関係

今 $D = \sum_{i=1}^r n_i P_i$ を X 上の因子とする．X の開被覆 $X = \bigcup_k U_k$ を，各 P_i を含む開集合 U_i が P_j $(j\neq i)$ を含まないように選んでおく．各 k に対して，U_k 上の関数 f_k を以下のように与える: $P_i\in U_i$ のとき f_i は P_i にのみ n_i 位の零点 (または $|n_i|$ 位の極) を持つ有理型関数とし，$P_i\notin U_k$ $(1\le i\le r)$ のときは $f_k = 1$ と定める．このとき $U_i\cap U_j$ 上 $g_{ij} = f_i/f_j$ とおくとこれは張り合わせ関数の性質を満たし，これにより作られる直線束を $\mathcal{O}_X(D)$ と書くことにする．$\mathcal{O}_X(D)$ の同型類は f_i のとり方によらない．実際 f_i を f_iu_i で取り替えると u_i は U_i 上極も零点も持たない関数であり，g_{ij} は $u_ig_{ij}u_j^{-1}$ で置き換えられる．

これにより X の因子全体のなす群 $\mathrm{Div}(X)$ から $\mathrm{Pic}(X)$ への写像 φ が与えられるが，作り方から φ は群準同型になる．X 上の関数 f により与えられる因子 (f) 全体のなす群を $\mathrm{Div}^\ell(X)$ と書くとき，実は $\ker\varphi = \mathrm{Div}^\ell(X)$ が成り立つ．以下それを説明しよう．$D = \sum n_iP_i = (f)$ と仮定する．このとき U_i 上 P_i にのみ極または零点を持つような関数として $f|U_i$ を選ぶことができる．よって張り合わせ関数は $g_{ij} = f/f = 1$ となり，$\varphi(D) = \mathcal{O}_X$ である．逆に $\varphi(D) = \mathcal{O}_X$ なる $D = \sum n_iP_i$ をとる．U_i 上 P_i で n_i 位の極または零点をとる関数を f_i としたとき，仮定から U_i 上零点を持たない正則関数 h_i が存在して，$f_i/f_j = h_i^{-1}1h_j$ が成り立つ．すなわち f_ih_i たちは $U_i\cap U_j$ 上等しいので，互いに張り合って X 上の有理型関数 f を定める．このとき $(f) = \sum n_iP_i$ が成り立ち，$\ker\varphi = \mathrm{Div}^\ell(X)$ が分かる．

以上の考察から，φ は単射 $\mathrm{Div}(X)/\mathrm{Div}^\ell(X)\hookrightarrow\mathrm{Pic}(X)$ を誘導する．実はこれは全射になることが知られており，これによって $\mathrm{Div}(X)/\mathrm{Div}^\ell(X)\simeq\mathrm{Pic}(X)$ が導かれる．すなわち X の因子類群 (因子全体の線形同値類) は，X 上の直線束の同値類のなす群と同型である．

注意 上で述べたことは，層の完全列 $0\to\mathcal{O}_X^\times\to\mathcal{K}_X^\times\to\mathcal{K}_X^\times/\mathcal{O}_X^\times\to 0$ より誘導される

完全列

$$H^0(X,\mathcal{K}_X^\times) \to H^0(X,\mathcal{K}_X^\times/\mathcal{O}_X^\times) \to H^1(X,\mathcal{O}_X^\times) \to H^1(X,\mathcal{K}_X^\times) = 0$$

の帰結である．ここに $\mathcal{K}_X^\times$ で X 上の 0 でない有理型関数のなす層を表す．

$D = \sum n_i P_i \in \mathrm{Div}(X)$ に対して，P_i の近傍 U_i で定義された関数 f_i で，P_i にのみ n_i 位の零点 (または $|n_i|$ 位の極) を取るものを選んでおく．このときすでに述べたように $\Gamma(X,\mathcal{O}_X(D)) = \{h_\alpha \colon U_\alpha \xrightarrow{\mathrm{hol}} \mathbb{C} \mid h_\alpha/h_\beta = f_\alpha/f_\beta\}$ である．よって $h_\alpha f_\alpha^{-1}$ たちは貼り合わさって X 上の有理型関数 ψ を定める．このとき $(\psi) + D \geq 0$ が成り立ち，これによって

$$\Gamma(X,\mathcal{O}_X(D)) \xrightarrow{\sim} L(D), \quad (h_i)_i \longmapsto \psi = (h_i f_i^{-1})_i$$

が分かる．すなわち $L(D)$ は D から定まる直線束の大域切断のなす空間と同型である．以上をまとめると次が成り立つ．

定理 2.1 (1) アーベル群の同型，$\mathrm{Div}(X)/\mathrm{Div}^\ell(X) \simeq \mathrm{Pic}(X)$, $D \mapsto \mathcal{O}_X(D)$ が成り立つ．

(2) 各 $D \in \mathrm{Div}(X)$ に対して，$\Gamma(X,\mathcal{L}) \simeq L(D)$ が成り立つ．特に $\Gamma(X,\mathcal{L})$ は有限次 $\mathbb{C}$-ベクトル空間になる．

2.3 Picard 多様体としての Jacobi 多様体

コンパクトリーマン面 X 上に直線束はどのくらいあるのか，言い換えれば $\mathrm{Pic}(X)$ の構造がどうなっているのかを調べることは興味ある問題である．重要なのは $\mathrm{Pic}(X)$ には代数多様体 (あるいは射影的な複素多様体) の構造が入るという事実である．直線束たちの群演算により $\mathrm{Pic}(X)$ にも群構造が入り，すなわち $\mathrm{Pic}(X)$ は代数群になる．

$\mathrm{Pic}(X)$ 自体はやや “大きすぎる” 代数群であるため，もう少し細かく分けて調べるほうがよい．$\mathrm{Pic}(X)$ の元はすべて $\mathcal{L} = \mathcal{O}_X(D)$ の形をしており，因子 D は線形同値をのぞいて一意的に定まる．因子の次数は線形同値で不変であるから，これによって直線束の次数 $\deg \mathcal{L}$ が定まる．$\mathrm{Pic}^n(X)$ で次数が n であるような $\mathrm{Pic}(X)$ の元からなる部分集合を表すことにする．

このとき $\mathrm{Pic}^0(X)$ は部分群であり，$\mathrm{Pic}(X) = \coprod_n \mathrm{Pic}^n(X)$ と分解される．また X 上の点 P をとったとき $\mathrm{Pic}^0(X) \to \mathrm{Pic}^n(X)$, $\mathcal{L} \mapsto \mathcal{L} \otimes \mathcal{O}(nP)$ は全単射であるから，我々の目的は $\mathrm{Pic}^0(X) \simeq \mathrm{Div}^0(X)/\mathrm{Div}^\ell(X)$ を調べることに帰着される．ただし $\mathrm{Div}^0(X)$ で次数 0 の因子からなる群を表す．

さてこの稿の一番の目的は，以下の定理について解説することである．

定理 2.2 X を種数 g のコンパクトリーマン面とする．このとき $\mathbb{C}^g$ の中にある格子 Λ が存在して，$\mathrm{Pic}^0(X)$ は g-次元複素トーラス $\mathbb{C}^g/\Lambda$ と群同型となる．

言い換えれば $\mathrm{Pic}^0(X)$ のパラメーター空間として，複素トーラス $\mathbb{C}^g/\Lambda$ が取れるということである．これを言い換えると “X 上の次数 0 の直線束のモジュライ空間は複素トーラス $\mathbb{C}^g/\Lambda$ である” ということになる．

注意 こうして作られる $\mathbb{C}^g/\Lambda$ は，単に複素トーラスというだけでなく，射影的な複素多様体である．これにより $\mathbb{C}^g/\Lambda$ には代数多様体の構造も入る．射影的な複素トーラスを ($\mathbb{C}$ 上の) アーベル多様体と呼ぶ.

例 2.1 $g=0$ の場合，$\mathrm{Pic}^0(X)=\{1\text{ 点}\}$ が定理の主張である．すなわち $\mathbb{P}^1$ の因子類は次数のみで決まってしまうということであるが，これは以下のようにして分かる．

$D=\sum_{i=1}^{r}(P_i-Q_i)$ を $\mathbb{P}^1$ 上の次数 0 の因子であるとする．例えば $P_l=P_{l+1}=\cdots=P_{i_r}=\infty$ であり，$P_i(1\le i<l)$, $Q_i(1\le i\le r)\in\mathbb{C}$ であるならば,

$$\varphi(x)=\frac{\prod_{i=1}^{l-1}(x-P_k)}{\prod_{i=1}^{r}(x-Q_i)}$$

は $\mathbb{C}$ 上において，零点集合が $\{P_1,\dots P_{l-1}\}$，極の集合が $\{Q_1,\dots,Q_r\}$ となる．また無限遠点では分母と分子の次数を比較して $r-l$ 位の零点を持つことが分かる．ゆえに $(\varphi)=D$ である．

この例は極めて簡単であるが，本稿での Abel の定理の証明の雛形ともいえるものである．なお，下記の $g=1$ の場合同様，Riemann-Roch の定理からも容易に導ける．

例 2.2 $g=1$ の場合，次数が 1 の因子 D に対して，ただ一つの点 P が存在して $D\sim P$ となる．実際次数の関係から $L(K_X-D)=0$ が成り立つことに注意すると，Riemann-Roch の定理から $\dim L(D)=\deg D-1+g=1$ であり，D と線形同値な有効因子 P が唯一つ存在することが分かる．よって X 上の一点 P_0 を固定すれば，$X\to\mathrm{Pic}^0(X)$, $P\mapsto P-P_0$ は同型射になる．すなわち $\mathrm{Pic}^0(X)\simeq X=\mathbb{C}/\Lambda$ がなりたつ.

X がコンパクトリーマン面である場合，こうしてつくられた複素トーラス $\mathbb{C}^g/\Lambda$ を **Jacobi 多様体**と呼び，$\mathrm{Jac}(X)$ で表す.

$\mathrm{Pic}^0(X)$ がモジュライ空間であるということについて補足しておく．モジュライ空間とは単にパラメーター空間であるというだけではなく，より強い条件を満たすものである．$\mathbb{C}$ 上のスキームのなす圏 $Sch/\mathbb{C}$ から集合の圏 Set への反変関手 Pic_X^0 を

$$T\longmapsto\frac{\{X\times T\text{ 上の次数 }0\text{ の直線束の同値類}\}}{\{\mathrm{pr}_T^*(\mathcal{L})\mid\mathcal{L}\text{ は }T\text{ 上の直線束}\}}$$

で定める．ただし pr_T は $X\times T$ から T への射影であるとし，$X\times T$ 上の直線束が次数 0 とは，T の各点で引き戻したときに次数が 0 であると定義する．

このとき関手 Pic_X^0 は**表現可能** (representable) である．すなわち $\mathbb{C}$ 上の群スキーム $\mathsf{Pic}^0(X)$ が存在して

$$Pic_X^0(T)=\mathrm{Hom}_{\mathbb{C}\text{-}Sch}(T,\mathsf{Pic}^0(X))$$

が成り立つ (群の同型)．このようなスキーム $\mathsf{Pic}^0(X)$ を精モジュライ (fine moduli) という．実は定理 2.2 より強い主張: 関手 Pic_X^0 は表現可能で，精モジュライ $\mathsf{Pic}^0(X)$ として $\mathbb{C}^g/\Lambda$ が取れる，が成り立っている．

特に $T=\mathrm{Spec}\,\mathbb{C}$ とすれば，X 上の直線束の同値類 $Pic_X^0(\mathbb{C})$ が $\mathbb{C}^g/\Lambda$ の各点と対応しているいう主張になる．これが定理 2.2 のいうところである．

注意　“次数 0” の条件をはずして関手 Pic_X を考えても表現可能である．この場合 $\mathrm{Pic}^0(X)$ はモジュライ群スキームの単位連結成分に相当する．

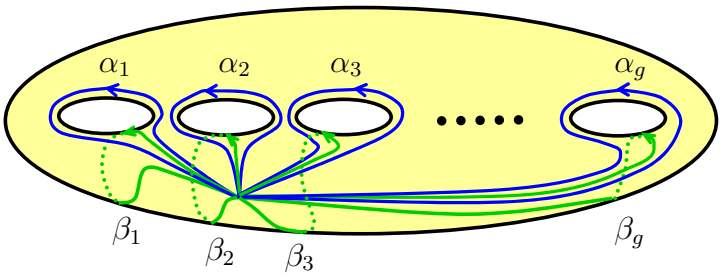
注意　X として一般の射影スキームを考えても (次数 0 の条件を適切に置き換えて) 同様の結果が成り立つ．特に X がアーベル多様体のとき，モジュライスキーム $\mathsf{Pic}^0(X)$ は双対アーベル多様体 $\widehat{X}$ になる．この場合，表現可能の定義で $T = \widehat{X}$ とおくと，$Pic^0_X(\widehat{X}) = \mathrm{Hom}(\widehat{X}, \widehat{X})$ であるから，$X \times \widehat{X}$ 上に $\mathrm{id}_{\widehat{X}}$ に対応する直線束が存在する．これが Poincaré 束に他ならない (cf [Ko])．

注意　Jacobi 多様体には，Albanese 多様体としての側面もある．一般に X を射影的な代数多様体とするとき，X に対してアーベル多様体 $\mathrm{Alb}(X)$ と写像 $\iota\colon X \to \mathrm{Alb}(X)$ が存在して以下の普遍性を満たす: 任意のアーベル多様体 A と X から A への写像 f に対して，写像 $g\colon \mathrm{Alb}(X) \to A$ が唯一つ存在して $f = g \circ \iota$ が成り立つ．

このような性質を満たす $\mathrm{Alb}(X)$ を X の Albanese 多様体と呼ぶ．X がコンパクトリーマン面である場合には $\mathrm{Alb}(X) = \mathrm{Jac}(X)$ が成り立つ．すなわち，X の Picard 多様体と Albanese 多様体は一致している (実際，コンパクト Kähler 多様体 X に対しては，$\mathrm{Pic}^0(X)$ と $\mathrm{Alb}(X)$ は互いに双対である)．

3　複素トーラスとしての Jacobi 多様体の構成

X をコンパクトなリーマン面で種数を g とする．このとき X 上の $2g$ 個の path $\alpha_1, \ldots, \alpha_g, \beta_1, \ldots, \beta_g$ を以下の図のように定める．



$H_1(X, \mathbb{Z})$ は階数が $2g$ の自由アーベル群となる．$H_1(X, Z)$ の交差積 $\langle\ ,\ \rangle$ を，X 上の 1-cycle γ と γ' に対して，γ が γ' を左から右に通過するように[1]一回交わっているとき $\langle \gamma, \gamma' \rangle = 1$, $\langle \gamma', \gamma \rangle = -1$ として定める．すなわち上の図では

$$\langle \alpha_i, \alpha_j \rangle = \langle \beta_i, \beta_j \rangle = 0, \quad \langle \alpha_i, \beta_j \rangle = -\langle \beta_i, \alpha_j \rangle = \delta_{ij}$$

となる．

注意　交差積は次のようにして定義できる: Poincaré 双対性から

$$H_1(X, \mathbb{Z}) \simeq H^1(X, \mathbb{Z})$$

[1] [Mum, P.137] では逆向きになっているが，この稿と α_i, β_i の役割が逆になっているため，辻褄は合っている．

であるが，一方普遍係数定理より自然な非退化双線形形式

$$H_1(X,\mathbb{Z}) \times H^1(X,\mathbb{Z}) \longrightarrow \mathbb{Z}$$

が存在する．これらの合成が交差積 $\langle\ ,\ \rangle$ である．

次に紹介する de Rham の定理は，$\mathbb{C}$-係数 de Rham コホモロジー $H_{\mathrm{dR}}(X,\mathbb{C})$ と，singular コホモロジー $H^1_{\mathrm{sing}}(X,\mathbb{C})$ との間の自然な同型を与える．

定理 3.1 (de Rham の定理) 自然な写像

$$H^i_{\mathrm{dR}}(X,\mathbb{C}) \to H^i_{\mathrm{sing}}(X,\mathbb{C}) = H_i(X,\mathbb{C})^*, \quad [\omega] \mapsto \left(\gamma \mapsto \int_\gamma \omega\right)$$

は同型射となる．ただし $*$ は dual を表わし，最後の積分は，i-form を i-cycle 上積分することを意味する．

$H^0(X,\Omega_X)$ の元 ω は closed 1-form，すなわち $d\omega = 0$ である．実際 $d = \delta + \overline{\delta}$ と d を正則微分と反正則微分に分けると，ω が正則であることより $\overline{\delta}\omega = 0$，また $\delta\omega$ は正則 2-form になるが，X が複素 1 次元であることより $\delta\omega = 0$ も成り立つ．

以上の考察より，$H^1(X,\mathbb{C})$ は $2g$ 次元のベクトル空間であるが，その de Rham コホモロジーとしての基底として，$\omega_1, \ldots, \omega_g, \overline{\omega}_1, \ldots, \overline{\omega}_g$ (の与える類) が選べることがわかる．以上より次が示された:

系 3.2 自然な写像

$$H_1(X,\mathbb{Z}) \longrightarrow H^0(X,\Omega_X)^*, \quad \gamma \mapsto \left(\omega \mapsto \int_\gamma \omega\right)$$

は埋め込みを与える．

よって $H_1(X,\mathbb{Z})$ は g-次元 $\mathbb{C}$-ベクトル空間 $H^0(X,\Omega_X)^*$ の中の階数 $2g$ の離散部分群を与える．

$H^0(X,\Omega_X)^*$ の基底を固定して $\mathbb{C}^g$ と同一視し，そのもとで $H_1(X,\mathbb{Z})$ の像を Λ とかくことにすると Λ は階数が $2g$ の自由アーベル群になる．まずはこの Λ について詳しく調べよう．

定理 3.3 (Riemann の関係式および不等式)

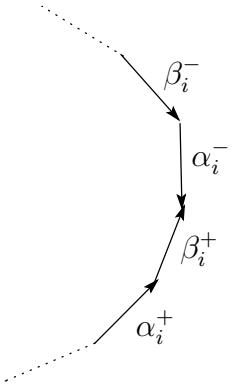
(1) ω, η を X 上の正則 1-form とするとき

$$\sum_{i=1}^{g} \left(\int_{\alpha_i} \omega \int_{\beta_i} \eta\right) - \sum_{i=1}^{g} \left(\int_{\alpha_i} \eta \int_{\beta_i} \omega\right) = 0.$$

(2) $\omega \neq 0$ を正則 1-form とするならば

$$\mathrm{Im}\left(\sum_{i=1}^{g} \overline{\int_{\alpha_i} \omega} \int_{\beta_i} \omega\right) > 0.$$

証明　X を α_i および β_i によって切り開くと $4g$ 角形ができる．1-cycle α_i, β_i の左側および右側をそれぞれ α_i^+, β_i^+ および α_i^-, β_i^- で表すことにすると以下の図のようになる．



$4g$ 角形の周囲 ∂X_0 は $\partial X_0 = \sum_{i=1}^g (\alpha_i^+ - \alpha_i^-) + \sum_{i=1}^g (\beta_i^+ - \beta_i^-)$ で与えられる[2]．

このとき X_0 は単連結であるから，ある X_0 上の正則関数 f が存在して，1-form η は $\eta = df$ の形で書くことができる．$f\omega$ は正則 1-形式より $d(f\omega) = 0$．よって Green の定理から

$$\begin{aligned} 0 &= \int_{X_0} d(f\omega) \\ &= \int_{\partial X_0} f\omega \\ &= \sum_{i=1}^{g} \left(\int_{\alpha_i^+} f\omega - \int_{\alpha_i^-} f\omega + \int_{\beta_i^+} f\omega - \int_{\beta_i^-} f\omega \right) \\ &= \sum_i \int_{\alpha_i} (f|_{\alpha_i^+} - f|_{\alpha_i^-})\,\omega + \sum_i \int_{\beta_i} (f|_{\beta_i^+} - f|_{\beta_i^-})\,\omega. \end{aligned}$$

ここで，$df = \eta$ は X 上定義されているから，当然 $\eta|_{\alpha_i^+} = \eta|_{\alpha_i^-}$ であり，よって $f|_{\alpha_i^+} - f|_{\alpha_i^-}$ は定数でなければならない．β_i は α_i^+ から α_i^- を結ぶ道であるから[3]，この値は $-\int_{\beta_i} \eta$ となる．

同様に $f|_{\beta_i^+} - f|_{\beta_i^-} = \int_\alpha \eta$ となり，結局

$$0 = -\sum_i \int_{\beta_i} \eta \int_{\alpha_i} \omega + \sum_i \int_{\alpha_i} \eta \int_{\beta_i} \omega$$

が成り立ち，(1) を得る．

(2) については $f = d\omega$ なる f をとれば上と同様の計算により，

$$\int_{X_0} d(\overline{f}\omega) = -\sum_i \overline{\int_{\beta_i} \omega} \int_{\alpha_i} \omega + \sum_i \overline{\int_{\alpha_i} \omega} \int_{\beta_i} \omega = 2i\,\mathrm{Im} \left(\sum_i \overline{\int_{\beta_i} \omega} \int_{\alpha_i} \omega \right)$$

[2][Mum] とは逆の向きになっている．
[3]β が α を右から左に通過しているから

が成り立つことが分かる．一方

$$d(\overline{f}\omega) = d\,\overline{f} \wedge df = \left|\frac{df}{dz}\right|^2 d\overline{z} \wedge dz$$

であり，$z = x + iy$ とかくと， $d\overline{z} \wedge dz = 2i\,dx \wedge dy$ が成り立つ．ゆえに $\omega \neq 0$ ならば $(1/2i)\int \overline{f}\omega > 0$ であることから主張を得る． □

この定理から次の重要な結果を得る．

定理 3.4 $\omega_1, \ldots, \omega_n$ を $H^0(X, \Omega_X)$ の基底とする．$A_{ij} = \int_{\alpha_i} \omega_j$， $B_{ij} = \int_{\beta_i} \omega_j$ とすると，$\det(A_{ij})_{i,j} \neq 0$ であり，$\tau = A^{-1}B \in \mathbb{H}_g$ が成り立つ．ここに

$$\mathbb{H}_g = \{Z \in M_g(\mathbb{C}) \mid {}^tZ = Z,\ \mathrm{Im}(Z) > 0\ (\text{正定値})\}$$

と定める．

証明 $\omega \in H^0(X, \Omega_X)$ がすべての α_i に対して $\int_{\alpha_i} \omega = 0$ を満たせば，定理 3.3 (2) から $\omega = 0$ である．よって $\det(A_{ij}) \neq 0$ が分かる．後半は，$H^0(X, \Omega_X)$ の基底を $\int_{\alpha_i} \omega_j = \delta_{ij}$ となるように正規化しておく．定理 3.3 (1) で $\omega = \omega_i$, $\eta = \omega_j$ とすれば $\tau_{ij} = \tau_{ji}$ となる．最後に (2) で $\omega = \sum a_i\omega_i$ とおけば，$a = {}^t(a_1, \ldots, a_g)$ に対して ${}^t\overline{a}\,\mathrm{Im}(\tau)a > 0$ $(a \neq 0)$ が成り立つことより主張を得る． □

これにより $H^0(X, \Omega_X)$ の基底 $\omega_1, \ldots, \omega_g$ を $\int_{\alpha_i} \omega_j = \delta_{ij}$ となるように選ぶことができる．この基底を使い $H^0(X, \Omega)^* \simeq \mathbb{C}^g$ と同一視すれば，

$$H^0(X, \Omega_X)^*/H_1(X, \mathbb{Z}) = \mathbb{C}^g/\Lambda_\tau, \quad \Lambda_\tau = \mathbb{Z}^g + \tau\mathbb{Z}^g$$

が成り立つ．以下この基底を固定して議論を進めることとする．

補題 3.5 Λ_τ は $\mathbb{C}^g$ の格子 (lattice) を与える．

証明 実際

$$\det \begin{pmatrix} 1_g & \tau \\ 1_g & \overline{\tau} \end{pmatrix} \neq 0$$

であることから $\Lambda_\tau \otimes \mathbb{R} = \mathbb{C}^g$ であることが導かれる． □

定義 3.1 $\mathrm{Jac}(X) = \mathbb{C}^g/\Lambda_\tau$ とかいて，これをコンパクトリーマン面 X の **Jacobi 多様体**と呼ぶ．

4 周期写像と Abel-Jacobi の定理

コンパクトリーマン面 X 上の基点 P_0 を固定しておく．X 上の path γ に対して，簡単のため

$$\int_\gamma \underline{\omega} := \left(\int_\gamma \omega_1, \ldots, \int_\gamma \omega_g\right) \in \mathbb{C}^g$$

と記述することにする．このとき

$$\Lambda_\tau = \{\int_\gamma \underline{\omega} \in \mathbb{C}^g \mid \gamma \in H_1(X, \mathbb{Z})\}$$

となる．

定義 4.1 $D = \sum_i (P_i - Q_i) \in \mathrm{Div}^0(X)$ を次数 0 の因子とする (P_i および Q_i には重複があってもよい)．このとき写像 $I\colon \mathrm{Div}^0(X) \to \mathrm{Jac}(X)$ を

$$I(D) = \sum_i \int_{Q_i}^{P_i} \underline{\omega} \mod \Lambda$$

で定める．

$\int_{Q_i}^{P_i} \underline{\omega} \bmod \Lambda_\tau$ は Q_i から P_i への path のとり方によらない．実際 path の取替えは 1-cycle α_i, β_i 上での積分の整係数線形結合分のずれに相当するため，同じ Λ_τ-同値類に属する．よって特に写像 I は $D = \sum_i (P_i - Q_i)$ の書き方にもよらず well-defined であることが確かめられる．

補題 4.1 $D \in \mathrm{Div}^\ell(X)$ ならば $I(D) = 0$．すなわち I は $\mathrm{Pic}^0(X) = \mathrm{Div}^0(X)/\mathrm{Div}^\ell(X)$ から $\mathrm{Jac}(X)$ への群準同型を導く．この写像も同じ I で表し，これを周期写像と呼ぶ．

証明　X 上の有理型関数 f をとる．f を X から $\mathbb{P}^1$ への写像と考え，$t \in \mathbb{P}^1$ に対して $f^{-1}(t) = D(t)$ を X の有効因子とみなすことにする．$\deg D(t)$ はすべての t に対して一定であるからこれを n とおく．今 X 上の基点 P_0 を固定しておき，

$$\phi\colon \mathbb{P}^1 \longrightarrow \mathrm{Jac}(X), \quad t \longmapsto \int_{nP_0}^{D(t)} \underline{\omega} \mod \Lambda_\tau$$

を考えるとこれは正則写像である．

ところが $\mathbb{P}^1$ は単連結ゆえ，ϕ は $\widetilde{\phi}\colon \mathbb{P}^1 \to \mathbb{C}^g$ に持ち上がる．$\mathbb{P}^1$ 上定義された正則関数は定数のみであるから $\widetilde{\phi}$，よって ϕ は定数写像になる．特に $\varphi(0) = \varphi(\infty)$ であるが，$I(D) = \phi(0) - \phi(\infty)$ であるから主張を得る．　□

定理 4.2 (Abel-Jacobi の定理) 周期写像 $I\colon \mathrm{Pic}^0(X) \to \mathrm{Jac}(X)$ は同型射である．

この定理に関しては，周期写像の単射性を Abel が，全射性を Jacobi が示したとされている．以下これを証明するのがこの稿の目的であるが，その前に曲線の対称積との関連を述べておこう．

5　曲線の対称積

まず次の補題を示す．

補題 5.1 X を種数 g のコンパクトリーマン面とする．$P_0 \in X$ を基点として固定しておくと，任意の $D \in \mathrm{Div}^0(X)$ に対してある $P_1, \ldots, P_g \in X$ が存在して，D は $P_1 + \cdots + P_g - gP_0$ と線形同値になる．

証明 $D + gP_0$ は次数が g の因子であるから，Riemann-Roch の定理より

$$l(D + gP_0) = l(K_x - D - gP_0) + \deg(D + gP_0) - g + 1 \geq g - g + 1 = 1$$

が成り立つ．よって $D + gP_0$ と線形同値な有効因子 $P_1 + \cdots + P_g$ が存在する． □

この補題から $\mathrm{Pic}^0(X)$ の代表系として $\sum_{i=1}^{g} P_i - gP_0$ の形のものが取れることがわかる．そこで

$$J\colon X^g := \underbrace{X \times \cdots \times X}_{g\text{ 個}} \to \mathrm{Jac}(X), \quad (P_1, \ldots, P_g) \mapsto \sum_i \int_{P_0}^{P_i} \underline{\omega} \mod \Lambda_\tau$$

なる写像を考えると，$\mathrm{Im}\, J = \mathrm{Im}\, I$ が成り立つ．さらに J は P_i たちの並べ替えで不変であることに注意すると，$X^{(g)} = X^g/\mathfrak{S}_g$ ($\mathfrak{S}_g$ は g 次対称群) に対して J は $X^{(g)}$ から $\mathrm{Jac}(X)$ への写像を誘導する．

補題 5.2 $X^{(g)}$ は g-次元の複素多様体になる．すなわち特異点を持たない．こうして定まる $X^{(g)}$ を X の対称積と呼ぶ．

証明 $X^{(g)}$ で特異点の出てくる可能性のあるのは，$i \neq j$ に対して i 番目と j 番目の成分が等しくなるような点の近傍のみである．ところが P_i の X での局所座標を t_i と書いたとき，例えば $P_1 = \cdots = P_g = P$ なる点の近傍に対しては，t_i たちの基本対称式 $\sigma_i(t)$ が $(P, \ldots, P)$ の局所座標を与えることが示される．よって g 個の独立な局所変数が取れるため，$X^{(g)}$ は $(P, \ldots, P)$ で特異点を持たない． □

$\mathrm{Im}\, I = \mathrm{Im}\, J$ であったから，例えば周期写像 I の全射性を言うためには J が全射であることを示せばよい．J は複素多様体の間の正則写像であるから写像の幾何的な性質を使うことができる．これが対称積を考える利点の一つである．

実は J は “ほぼ同型” である (双有理写像)．すなわち $X^{(g)}$ と $\mathrm{Jac}(X)$ は “近い” 複素多様体であることが以下示される．

例 5.1 (種数 2 のリーマン面) C を種数 2 の代数曲線とする．このとき C は超楕円曲線であり，定義方程式は $y^2 = x^5 + \cdots$ で表わされる．今 $(x, y) \mapsto (x, -y)$ で与えられる対合 (hyperelliptic involution) を ι で表わすことにしよう．$(x, y) \mapsto x$ で与えられる写像 $f\colon C \to \mathbb{P}^1$ を考えると，各 $x \in \mathbb{P}^1$ に対してある $P \in C$ が存在して，$f^{-1}(x) = \{P, \iota(P)\}$ が成り立つ．すなわち $C/\langle\iota\rangle \simeq \mathbb{P}^1$ である．

対合 ι は以下のような特徴付けも出来る．すなわち K_C を C の標準因子としたとき，各点 $P \in C$ に対して Riemann-Roch の定理より

$$l(P) - l(K_C - P) = \deg P - g + 1 = 0$$

であるが，留数定理より $l(P)=1$，よって $l(K_C-P)=1$ が成り立つ．ゆえに $K_C\sim P+Q$ が成り立つような $Q\in C$ が唯一つ定まる．この Q が $\iota(P)$ に他ならない．さて，以上の準備の下で $C^{(2)}$ と $\mathrm{Pic}^0(C)$ の関係について調べてみよう．

C の基点 P_0 として，無限遠点 ∞ をとり，

$$\Psi\colon C^{(2)}\to \mathrm{Pic}^0(C),\quad (P_1,P_2)\mapsto P_1+P_2-2\infty$$

を考える．補題 5.1 から Ψ は全射になる．Riemann-Roch の定理から

$$l(P_1+P_2)=l(K_C-P_1-P_2)+\deg(P_1+P_2)+1-g=1+l(K_C-P_1-P_2)$$

が成り立つ．$P_2\neq\iota(P_1)$ であれば $l(K_C-P_1-P_2)=0$ であり (次数が 0 であって主因子ではない)，ゆえに $l(P_1+P_2)=1$，すなわち P_1+P_2 と線形同値な有効因子は他に存在しない．これを言い換えると，

$$\mathcal{D}=\{(P,\iota(P))\in C^{(2)}\}$$

と置いたときに，$C^{(2)}\smallsetminus\mathcal{D}$ 上では Ψ は単射になる．一方任意の $P\in C$ に対して $P+\iota(P)\sim 2\infty\sim K_C$ であるから，$\Psi(\mathcal{D})=\{0\}$ が成り立つ．

$\mathcal{D}\simeq C/\langle\iota\rangle\simeq\mathbb{P}^1$ であり，実は自己交点数 $(\mathcal{D}^2)=-1$ が計算できる．ゆえに Castelnuovo の定理 ([Har, Theorem 5.7, Chapter V]) から $\mathcal{D}$ は例外因子となることが分かる．すなわちある曲面 Z と $\pi\colon C^{(2)}\to Z$ が存在して，ある $z_0\in Z$ に対して $\pi^{-1}(z_0)=\mathcal{D}$ かつ $\pi\colon C^{(2)}\smallsetminus\mathcal{D}\to Z\smallsetminus\{z_0\}$ は同型写像になる (z_0 を中心とした blow-up)．Ψ から誘導される $\widetilde{\Psi}\colon Z\to\mathrm{Pic}^0(C)$ は全単射である．よってこのようにして作られる曲面 Z こそが，我々の求めている Jacobi 多様体 $\mathrm{Jac}(C)$ に他ならない．

注意　自己交点数 $(\mathcal{D}^2)=-1$ は以下のようにして計算できる．自然な写像 $\mathrm{pr}\colon C\times C\to C^{(2)}$ と対角埋め込み $\Delta\colon C\to C\times C$, $x\mapsto(x,x)$ に対して

$$\varphi\colon C\times C\xrightarrow{1\times\iota} C\times C\xrightarrow{\mathrm{pr}} C^{(2)}$$

を考えると $\mathcal{D}=\varphi(\Delta(C))$ であり，$\deg\varphi=2$ であることから $C\times C$ において $(\Delta(C)^2)=-2$ を証明すればよい．$C\times C$ 上での層の完全列

$$0\to\mathcal{I}\to\mathcal{O}_{C\times C}\to\Delta_*\mathcal{O}_C\to 0$$

を考える．ここに $\mathcal{I}$ は閉埋め込み Δ に対応するイデアル層であり，$\mathcal{I}\simeq\mathcal{O}_{C\times C}(-\Delta(C))$ ([Har, Proposition 6.18, Chapter II])．　よって交点数の定義から　$(\Delta(C)^2)=\deg\Delta^*\mathcal{O}_{C\times C}(\Delta(C))=-\deg\Delta^*\mathcal{I}$ が成り立つ．一方上の完全系列に局所自由層 $\mathcal{I}$ をテンソルすることにより

$$0\to\mathcal{I}^2\to\mathcal{I}\to\Delta_*\mathcal{O}_C\otimes\mathcal{I}\to 0$$

を得る．すなわち $\mathcal{I}/\mathcal{I}^2\simeq\Delta_*\mathcal{O}_C\otimes\mathcal{I}$ が成り立ち，よって $\Omega^1_C=\Delta^*(\mathcal{I}/\mathcal{I}^2)\simeq\Delta^*\mathcal{I}$ である (Δ は閉埋め込みゆえ，C 上の任意の $\mathcal{O}_C$ 加群層 $\mathcal{F}$ に対して $\Delta^*\Delta_*\mathcal{F}=\mathcal{F}$ が成り立つことに注意)．以上より $(\Delta(C)^2)=-\deg\Omega^1_C=2-2g=-2$ が示された．　□

6 Riemann の theta 関数

この節ではいわゆる Riemann の theta 関数について解説する．保型形式の分野では実際の関数の構成に使うなど欠かせない道具であるが，ここで扱う Riemann の theta 関数は，$\mathbb{C}^g$-変数 z と $\mathbb{H}_g$-変数 τ に関する正則関数であり，一言で言うと “z の関数としてみれば $\mathbb{C}^g/\Lambda_\tau$ 上のある直線束の大域切断であり，($z=0$ として) τ の関数としてみると保型形式になるもの” である．

我々の目的との関連は，以下のようにして説明される．写像 I の単射性を調べるためには $\mathrm{Div}^\ell(X)$ について，すなわち X 上の有理型関数について調べることが必要である．しかし，与えられたリーマン面上の有理型関数を実際に構成するのは簡単ではない．よくある手法は X 上の直線束の大域切断の商として構成する方法である．そのためにまず $\mathrm{Jac}(X)=\mathbb{C}^g/\Lambda_\tau$ 上の直線束を構成し，それを写像

$$X \longrightarrow \mathrm{Jac}(X), \quad P \longmapsto \int_{P_0}^{P} \underline{\omega} \mod \Lambda_\tau$$

によって引き戻して X 上の直線束の切断をえることを考える．このように構成すると，零点や極の位置が分かりやすい有理型関数が得られるのである[4]．

定義 6.1 $z\in\mathbb{C}^g$ と $\tau\in\mathbb{H}_g$ に対して

$$\vartheta(z,\tau)=\sum_{l\in\mathbb{Z}^g}\exp(\pi i^t l\tau l+2\pi i^t lz)$$

と定める．

容易に分かるように右辺の無限級数は $\mathbb{C}^g\times\mathbb{H}_g$ 上広義一様絶対収束していて，特に $\mathbb{C}^g$ 上の正則関数を与える．

補題 6.1 $\vartheta(z,\tau)$ は次の性質を満たす:

(1) $\vartheta(z+m,\tau)=\vartheta(z,\tau), \quad m\in\mathbb{Z}^g$;

(2) $\vartheta(z+\tau m,\tau)=\exp(-\pi i^t m\tau m-2\pi i^t mz)\vartheta(z,\tau)$.

さらに上記 (1), (2) の性質を満たす $\mathbb{C}^g$ 上の正則関数は $\vartheta(z,\tau)$ の定数倍に限る．

証明 前半は容易．後半はそのような関数 f をとるとまず (1) の性質から

$$f(z)=\sum_{l\in\mathbb{Z}^g}c_l e^{2\pi i^t lz}$$

と Fourier 展開されるが，さらに (2) の性質から Fourier 係数 c_n の間に関係式が得られる．すなわち $\mathbb{C}^g$ の標準基底 $u_1,\ldots,u_g$ に対して

$$c_{l+u_k}=\exp(2\pi i^t l\tau u_k+\pi i^t u_k\tau u_k)\,c_l$$

が成り立つ．ゆえに (1), (2) を満たす関数のなす空間の次元は 1 であり，それは $\vartheta(z,\tau)$ の定数倍でなければならない．

[4] Riemann 自身がどのような目的意識で theta 関数を考えたのかは筆者は知らない．

注意　上記補題は，このようにして作られる $\mathrm{Jac}(X)$ 上の直線束 $\mathcal{O}_X(\Theta)$ に対して $\Gamma(X, \mathcal{O}_X(\Theta))$ が 1 次元であることを主張している．実は $\mathcal{O}_X(\Theta)$ は ample な直線束であり，これによって $\mathrm{Jac}(X)$ は主偏極をもつアーベル多様体であることが示される (cf. [Ko]).

次の Riemann 自身による定理がこの稿で最大の役割を果たす.

定理 6.2 X 上の基点 P_0 を固定しておく．$z \in \mathbb{C}^g$ に対して X 上の (多価) 関数 f_z を

$$f_z(P) = \vartheta(z + \int_{P_0}^{P} \underline{\omega}, \tau)$$

で定める．このとき Riemann 定数と呼ばれるある $\Delta \in \mathbb{C}^g$ が存在して以下の条件を満たす: $f_z \not\equiv 0$ であるような f_z の零点は重複をこめて g 個であり，それを $Q_1, \ldots, Q_g$ とかくと

$$\sum_{i=1}^{g} \int_{P_0}^{Q_i} \underline{\omega} \equiv -z + \Delta \mod \Lambda_\tau$$

が成り立つ.

注意　$f_z(P)$ の値は P_0 から P への path のとり方によるが，path の取替えは $\vartheta(z, \tau)$ の 0 でないスカラー倍の差しか引き起こさないため，$f_z(P)$ の零点の位置は定まる.

証明　定理 3.3 の証明と同じ記号を使う．f_z の零点 Q_i に対して (有限個)，その周りを回る小円盤を D_i で表わす．df_z/f_z は $X_0 \setminus \bigcup D_i$ 上の正則 1-form であり，よって closed form だから

$$\begin{aligned} 0 &= \int_{X_0 \setminus \bigcup D_i} d\left(\frac{df_z}{f_z}\right) \\ &= \int_{\partial(X_0 \setminus \bigcup D_i)} \left(\frac{df_z}{f_z}\right) \\ &= -\sum_i \int_{D_i} \frac{df_z}{f_z} + \sum_{k=1}^{g} \int_{\alpha_k^+ - \alpha_k^-} \frac{df_z}{f_z} + \sum_{k=1}^{g} \int_{\beta_k^+ - \beta_k^-} \frac{df_z}{f_z}. \end{aligned}$$

さて，f_z は α_k たちに沿った path の取替えでは不変であるから，α_k が β_k^- から β_k^+ をつなぐ path であったことに注意すると $f_z|_{\beta_k^+} = f_z|_{\beta_k^-}$ が成り立つ．すなわち第 3 項は 0 である．一方 path β_k の取替えに関しては f_z は

$$\exp(-\pi i {}^t u_k \tau u_k - 2\pi i \int_{P_0}^{P} \omega_k + {}^t u_k z)$$

倍ずれる (u_k は $\mathbb{C}^g$ の単位ベクトル)．ゆえに, β_k が α_k^+ から α_k^- をつなぐ path であることに注意すれば，第 2 項は

$$\sum_{k=1}^{g} \left\{ \int_{\alpha_k^-} d(\log f_z) - \int_{\alpha_k^+} d(\log f_z) \right\} = \sum_{k=1}^{g} \int_{\alpha_k} 2\pi i \omega_k = 2\pi i g.$$

まとめると

$$0 = -\sum_i \int_{D_i} \frac{df_z}{f_z} + 2\pi i g$$

を得る．よって f_z の零点の数が g であることが分かった．

次に X_0 上 $\omega_k = dg_k$ とおく．$g_k(P_0) = 0$ と仮定してよい．1-form $g_k\, df_z/f_z$ に対して上記の議論を適用すると

$$0 = -\sum_{i=1}^{g} \int_{D_i} g_k \frac{df_z}{f_z} + \sum_{l=1}^{g} \int_{\alpha_l^+ - \alpha_l^-} g_k \frac{df_z}{f_z} + \sum_{l=1}^{g} \int_{\beta_l^+ - \beta_l^-} g_k \frac{df_z}{f_z}$$

を得る．まず第 1 項に関しては留数定理より

$$\int_{D_i} g_k \frac{df_z}{f_z} = 2\pi i g_k(Q_i) = 2\pi i \int_{P_0}^{Q_k} \omega_k$$

となる．第 3 項に関しては $g_k|_{\beta_l^+} - g_k|_{\beta_l^-} = \int_{\alpha_l} \omega_k = \delta_{kl}$ であることに注意すれば

$$\begin{aligned}\int_{\beta_l^+ - \beta_l^-} g_k \frac{df_z}{f_z} &= \delta_{kl} \int_{\beta_l} \frac{df_z}{f_z} = \delta_{kl} \int_{\beta_l} d(\log f_z) \\ &= \delta_{kl}(-\pi i^t u_l \tau u_l - 2\pi i \int_{P_0}^{P_1} \omega_l - 2\pi i^t u_l z + 2\pi i m_l)\end{aligned}$$

が成り立つ．ここに P_1 は path α_i, β_i たちの基点であり，m_l はある整数である．

最後に第 2 項は，$g_k|_{\alpha_l^+}$ と $g_k|_{\alpha_l^-}$ の差が $-\int_{\beta_l} \omega_k = -\tau_{kl}$ であることに注意すると

$$\begin{aligned}\int_{\alpha_l^+ - \alpha_l^-} g_k \frac{df_z}{f_z} &= \int_{\alpha_l^-} \left[(g_k - \tau_{kl}) \left(\frac{df_z}{f_z} - 2\pi i \omega_l \right) - g_k \frac{df_z}{f_z} \right] \\ &= 2\pi i \tau_{kl} n_l + 2\pi i \int_{\alpha_l^+} g_k \omega_l - 2\pi i \tau_{kl}\end{aligned}$$

となる．以上をまとめると

$$\sum_{i=1}^{g} \int_{P_0}^{Q_i} \omega_k = -z_k + \left[\frac{\tau_{kk}}{2} - \int_{P_0}^{P_1} \omega_k + \sum_l \tau_{kl} - \sum_l \int_{\alpha_k^+} g_k \omega_l \right] + m_k + \sum_l \tau_{kl} n_l$$

が成り立ち，定理の主張を得る． □

7 Abel-Jacobi の定理の証明

この節では，上記の Riemann の定理を用いて Abel-Jacobi の定理を証明する．まず全射性は容易に従う．実際 $f_{\Delta - z}$ を考えると，Riemann の定理は “$f_{\Delta - z} \not\equiv 0$ でなければその零点は $Q_1, \ldots, Q_g$ の重複をこめた g 個であり，$D = \sum Q_i$ に対して

$$J(D) = \sum_{i=1}^{g} \int_{P_0}^{Q_i} \underline{\omega} \mod \Lambda_\tau = z$$

が成り立つ” ことを主張している．そこで

$$\mathcal{E}=\left\{z\in \mathrm{Jac}(X)\;\middle|\; f_{\Delta-z}(P)=\vartheta\left(\Delta-z+\int_{P_0}^{P}\underline{\omega}\right)=0,\ \forall P\in X\right\}$$

とおくと $\mathcal{E}$ は $\mathrm{Jac}(X)$ の真の解析的な閉部分集合であり，$U=\mathrm{Jac}(X)\setminus\mathcal{E}$ は空でない開集合である．上の議論から $\mathrm{Im}\,J$ は U を含むが $X^{(g)}$ はコンパクトゆえ $\mathrm{Im}\,J$ は閉集合．ゆえに J は全射となる．

さらに幾何的な議論から，より詳しく次の結果が得られる．

定理 7.1 (Jacobi の逆定理) (1) $J\colon X^{(g)}\to \mathrm{Jac}(X)=\mathbb{C}^g/\Lambda_\tau$ は全射かつ双有理写像であり，$J\colon J^{-1}(U)\to U$ は同型射である．

(2) 任意の $P_1,\dots,P_g\in X$ と $z\in\mathbb{C}^g$ に対して，$\sum_{i=1}^g\int_{P_0}^{P_i}\underline{\omega}\equiv z \bmod \Lambda_\tau$ ならば，各 i に対して $f_{\Delta-z}(P_i)=\vartheta(\Delta-z+\int_{P_0}^{P_i}\underline{\omega})=0$ である．逆に $z\in U$ に対しては $f_{\Delta-z}$ の零因子 $\sum_i P_i$ は

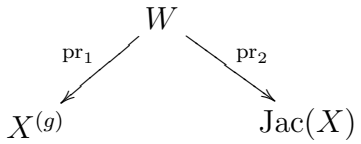
$$\sum_{i=1}^{g}\int_{P_0}^{P_i}\underline{\omega}\equiv z \bmod \Lambda_\tau$$

なる条件で一意的に定まる．

証明　$X^{(g)}\times\mathrm{Jac}(X)$ の解析的部分集合 W を

$$W=\left\{\big((P_1,\dots,P_g),z\big)\in X^{(g)}\times\mathrm{Jac}(X)\;\middle|\;\begin{array}{l}\sum\int_{P_0}^{P_i}\underline{\omega}\equiv z \bmod \Lambda_\tau,\\ f_{\Delta-z}(P_i)=0\ (1\le i\le g)\end{array}\right\}$$

と定める．W からの 2 つの射影



に関して，定理 6.2 より $\mathrm{pr}_2\colon \mathrm{pr}_2^{-1}(U)\to U$ は同型射である．実際 $z\in U$ に対して $f_{\Delta-z}$ の零点集合 $\{P_1,\dots,P_g\}$ を取れば，$z\mapsto\big((P_1,\dots,P_g),z\big)$ は pr_2 の逆写像を与える．ゆえに $\mathrm{Im}\,\mathrm{pr}_2$ は U を含む閉集合であり (W がコンパクトに注意)，よって pr_2 は全射である．これより $\dim W\ge g$ が得られる．

一方 W の定義より pr_1 は単射であり，次元の比較から全単射であることが従う．すなわち W は J のグラフ $\{(x,J(x))\mid x\in X^{(g)}\}$ に他ならない．ゆえに (2) の前半が成り立つ．(2) の後半及び (1) は今までの議論の帰結である．　□

最後に周期写像の単射性を主張する Abel の定理の証明について述べる．示すべきことを改めて定理の形で述べておこう．

定理 7.2 (Abel の定理) $P_1,\dots,P_r,Q_1,\dots,Q_r$ を X 上の任意の点とする．$I(\sum_{i=1}^r(P_i-Q_i))=0$ であれば，重複をこめて $\{P_1,\dots,P_r\}$ が零点，$\{Q_1,\dots,Q_r\}$ が極となるような X 上の有理型関数が存在する．

$f_z(P) = \vartheta(z + \int_{P_0}^{P} \underline{\omega}, \tau)$ の零点についての情報は与えられているから，これを使って関数を構成することを考えよう．$\vartheta(z_0, \tau) = 0$ となるような $z_0 \in \mathbb{C}^g$ を一つとって固定する．このような z_0 に対して X 上の (多価) 関数を $\varphi_P(x)$ を

$$\varphi_P(x) = \vartheta(z_0 + \int_P^x \underline{\omega}, \tau)$$

と定めれば，当然これは $x = P$ で零点を持つ．これから

$$f(x) = \prod_{i=1}^{r} \frac{\varphi_{P_i}(x)}{\varphi_{Q_i}(x)}$$

を考えるというのが基本的な戦略である．

そのためにはまず $\varphi_P \not\equiv 0$ でなければならない．また φ_P の他の零点についても調べる必要がある．そのために補題を 2 つ用意しておく．

補題 7.3 各 $P \in X$ に対して

$$D_P = \left\{ z \in \mathrm{Jac}(X) \;\middle|\; \vartheta(z + \int_P^y \underline{\omega}) = 0,\ \forall y \in X \right\}$$

は余次元 2 以上の解析的部分集合である．特に与えられた有限個の点 R_i $(1 \le i \le r)$ に対して φ_{R_i} が自明にならないような ϑ の零点 z_0 が存在する．

証明 D を D_P の既約成分とし，$X_P = \{\int_P^y \underline{\omega} \mid y \in X\}$ とおく．このとき $X_P + D$ は $\mathrm{Jac}(X)$ の既約閉集合であり，ϑ の零点集合に含まれるから $\dim(X_P + D) \le g - 1$ となる．もし $\dim D = g-1$ ならば $D = D + X_P$ ゆえ，$D = D + X_P = D + \underbrace{X_P + X_P + \cdots + X_p}_{g \text{ 個}} =$ $\mathrm{Jac}(X)$ となり (I の全射性) 矛盾である．ゆえに $\dim D \le g - 2$. □

補題 7.4 $z_0 \in \mathbb{C}^g$ を $\vartheta(z_0) = 0$ かつ，$X \times X$ 上の関数 $\Phi_{z_0}(P, Q) = \vartheta(z_0 + \int_P^Q \underline{\omega}) \not\equiv 0$ となるようにとっておく．このとき $2g - 2$ 個の点 $R_1, \ldots, R_{g-1}, S_1, \ldots, S_{g-1}$ が存在して次を満たす:

$$\begin{aligned} &\{(P, Q) \in X \times X \mid \Phi_{z_0}(P, Q) = 0\} \\ =&\{(P, P) \in X \times X\} \cup \bigcup_{i=1}^{g-1} (\{R_i\} \times X) \cup \bigcup_{i=1}^{g-1} (X \times \{S_i\}). \end{aligned}$$

証明 y の関数として $\Phi_{z_0}(R, y) \not\equiv 0$ となるような R をとる．定理 6.2 から $\Phi_{z_0}(R, y)$ の零点は $y_1, \ldots, y_g$ の g 個であり，さらに定理 7.1 から $(y_1, \ldots, y_g)$ は条件

$$\sum_{i=1}^{g} \int_{P_0}^{y_i} \underline{\omega} \equiv \Delta - z_0 - \int_R^{P_0} \underline{\omega} \mod \Lambda_\tau$$

の条件で唯一つ決まる $X^{(g)}$ の点であることが分かる．ところが $\Phi_{z_0}(R,R) = \vartheta(z_0 + \int_R^R \underline{\omega}) = 0$ であるから，$y_1 = R$ としてよい．よって $(y_2,\dots,y_g)$ は条件

$$\sum_{i=2}^{g}\int_{P_0}^{y_i} \equiv \Delta - z_0 \mod \Lambda_\tau$$

で唯一つ決まる $X^{(g-1)}$ の点であり，この条件は R に依らない．よって $S_i = y_{i+1}$ と置くと，$\Phi_{z_0}(*,S_i) \equiv 0$, $(1 \le i \le g-1)$ が成り立つ．言い換えると，「y の関数として $\Phi_{z_0}(R,y) \not\equiv 0$ ならば，零点集合は $\{R,S_1,\dots,S_g\}$」が示された．

逆に y の関数として $\Phi_{z_0}(R,y) \equiv 0$ となるような R は有限個であるが，それが $g-1$ 個あることを示せばよい．$S_1,\dots,S_g$ と異なるような点 S_0 をとる．このとき $\Phi(*,S_0) \not\equiv 0$ であり，$\Phi_{z_0}(x,S_0) = 0$ となるような x は,「$x = S_0$，または y の関数として $\Phi_{z_0}(x,y) \equiv 0$ が成り立つような x」でなければならない．ところが $\Phi_{z_0}(x,S_0) = \Phi_{-z_0}(S_0,x)$ は x の関数として g 個の零点を持つ．それを $S_0,R_1,\dots,R_{g-1}$ とおくと，$\Phi_{z_0}(R_i,*) \equiv 0$ である．
□

定理 7.2 の証明 補題 7.3 より与えられた P_i,Q_i に対して $\varphi_{P_i} \not\equiv 0$，$\varphi_{Q_i} \not\equiv 0$ となるような z_0 が存在するので，そのような z_0 を 1 つとって固定しておく．X 上の (多価) 関数

$$f(x) = \prod_{i=1}^{r} \frac{\varphi_{P_i}(x)}{\varphi_{Q_i}(x)}$$

を考える．$f(x)$ が一価正則関数となるように，X 上の各点 x に対して P_i 及び Q_i から x への path の取り方を指定しなければならない．仮定より $I(\sum(P_i - Q_i)) = 0$，すなわち

$$(*) \qquad \sum_{i=0}^{r}\int_{P_0}^{P_i} \underline{\omega} \equiv \sum_{i=0}^{r}\int_{P_0}^{Q_i} \underline{\omega} \mod \Lambda_\tau$$

が成り立っている．このとき P_0 から P_i 及び Q_i への path γ_i, δ_i をうまくとって，$(*)$ の両辺が ($\mathrm{mod}\,\Lambda_\tau$ のみならず) 真に等しいと仮定してよい．このようにとった γ_i,δ_i に対して，$f(x)$ の定義式の path は以下のようにとるものとする: P_0 から x への path を一つ選んでおき，それと $-\gamma_i$ や $-\delta_i$ をつなげたものとして P_i, Q_i から x への path をとる．すると P_0 から x への path の取替えは $\int_{\alpha_i}\underline{\omega}$, $\int_{\beta_i}\underline{w}$ の整数係数線型結合，すなわち Λ_τ の元による平行移動での theta 関数の変換を引き起こし，その寄与は分子と分母でキャンセルされる．ゆえに $f(x)$ は X 上の一価有理関数として well-defined となる．

このとき φ_{P_i} (φ_{Q_i}) の零点は補題 7.4 から $P_i,S_1,\dots,S_{g-1}$ $(Q_i,S_1,\dots,S_{g-1})$ の g 個である．ゆえに $f(X)$ の零点は $P_1,\dots,P_r$，極は $Q_1,\dots,Q_r$ となって $(f) = D$ が成り立つ．
□

参考文献

[BLR] S. Bosch; W. Lütkebohmert; M. Raynaud, *Néron models*. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], 21. Springer-Verlag, Berlin, 1990.

[Har] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977.

[Iwa] 岩澤健吉「代数函数論」岩波書店, 1973.

[Ko] 小林真一 “Algebraic theory via schemes” 本報告集.

[Lan] S. Lang, *Introduction to algebraic and abelian functions*, Second edition. Graduate Texts in Mathematics, 89. Springer-Verlag, New York-Berlin, 1982.

[Mil] J. S. Milne, “Jacobian varieties” Chapter VII of *Arithmetic geometry*, Papers from the conference held at the University of Connecticut, Storrs, Connecticut, July 30–August 10, 1984. Edited by Gary Cornell and Joseph H. Silverman. Springer-Verlag, New York, 1986.

[Mum] D. Mumford, *Tata lectures on theta I*, Progress in Mathematics, 28. Birkhäuser Boston, Inc., Boston, MA, 1983.

[Ser] J. P. Serre, *Algebraic groups and class fields*, Graduate Texts in Mathematics, 117. Springer-Verlag, New York, 1988

[Shi] 清水秀男 「保型関数」, 岩波書店 1992.

[Weil] A. Weil, *Variétés abéliennes et courbes algébriques* Actualités Sci. Ind., no. 1064 = Publ. Inst. Math. Univ. Strasbourg 8 (1946). Hermann & Cie., Paris, 1948.

第 15 回 整数論サマースクール 報告集, pp.81-111

Abel-Jacobi の定理 II

— 岩澤健吉著「代数函数論」の手法から —

尾崎 学*, 梅垣 敦紀†

本稿では，タイトルの通り岩澤健吉著「代数函数論」([1]) に基づいて，Abel-Jacobi の定理の証明を行う．講演時の通り，前半は梅垣，後半を尾崎が担当した．

目 次

*近畿大学理工学部, ozaki@math.kindai.ac.jp
†早稲田大学高等研究所, umegaki@gm.math.waseda.ac.jp (講演時の所属は「立教大学理学部」)

0　知識の確認

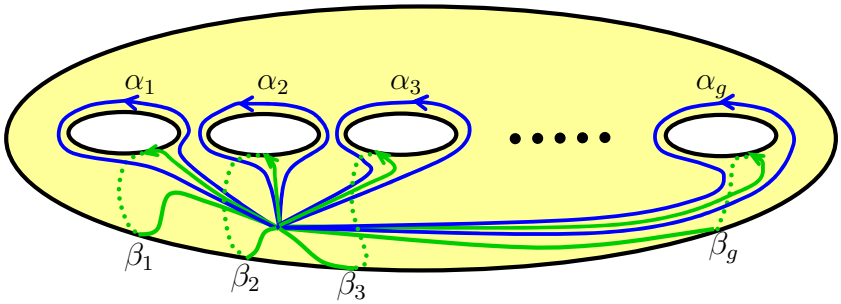
まず，吉冨氏・小川氏・軍司氏の各講でも説明されている知識について，以下を読むのに必要な分だけを [1] の書式に合わせて簡単にまとめ，記号を定義しておく．

0.1　1 次元ホモロジー群

コンパクト Riemann 面 R 上の closed path γ で生成される自由アーベル群を $Z_1(R,\mathbf{Z})$ で表し，**1 次元サイクル群**と呼ぶ．また，path のホモロジー同値を $\sim$ で表すとき，その部分群 $B_1(R,\mathbf{Z}) = \langle \gamma \mid \gamma \sim 0 \rangle_{\mathbf{Z}}$ を **1 次元バウンダリ群**と呼び，$Z_1(R,\mathbf{Z})$ を $B_1(R,\mathbf{Z})$ で割った商群 $H_1(R,\mathbf{Z})$ を **1 次元ホモロジー群**と呼ぶ．R の種数を g とするとき，

$$H_1(R,\mathbf{Z}) \cong \mathbf{Z}^{\oplus 2g}$$

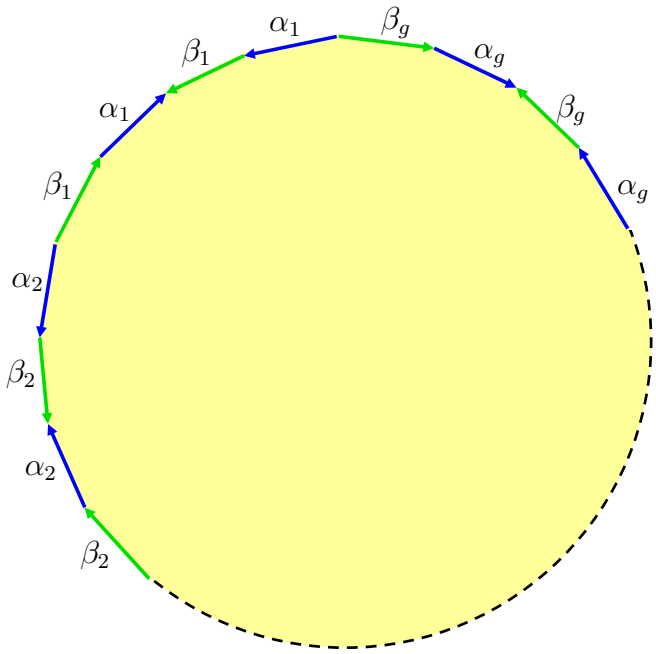
が成り立つ．



特に，具体的に α_i, β_j $(i,j = 1,\ldots,g)$ を図のようにとれば，

$$H_1(R,\mathbf{Z}) \cong \langle \alpha_1,\ldots,\alpha_g,\beta_1,\ldots,\beta_g \rangle_{\mathbf{Z}}$$

が成り立つ．この α_i, β_j $(i,j = 1,\ldots,g)$ に沿って R を切り開くと次の図で表されるような $4g$ 角形が得られる：



このように R 上の path を固定した場合、R の基本群 $\pi_1(R, \mathbf{Z})$ についても

$$\pi_1(R, \mathbf{Z}) = \langle \alpha_1, \ldots, \alpha_g, \beta_1, \ldots, \beta_g \mid [\alpha_1, \beta_1][\alpha_2, \beta_2] \cdots [\alpha_g, \beta_g] = 1 \rangle$$

となることがわかる．但し，交換子 $[\alpha_i, \beta_i]$ は $[\alpha_i, \beta_i] = \alpha_i \beta_i \alpha_i^{-1} \beta_i^{-1}$ とする．$\pi_1(R, \mathbf{Z})^{\mathrm{ab}} \cong H_1(R, \mathbf{Z})$ であることにも注意しておく．

定義 0.1. 上で決めた R 上の path $\{\alpha_i, \beta_i\}_{i=1,\ldots,g}$ に対して，

$$(\alpha_i, \alpha_j) = 0, \qquad (\beta_i, \beta_j) = 0, \qquad (\alpha_i, \beta_j) = \delta_{ij}, \qquad (\alpha_i, \beta_j) = -(\beta_j, \alpha_i)$$

で定まる**交切数**（**【英】intersection number**）を定義する．さらに，任意の $\gamma_1, \gamma_2 \in H_1(R, \mathbf{Z})$（または，$\gamma_1, \gamma_2 \in H_1(R, \mathbf{R}) = H_1(R, \mathbf{Z}) \otimes \mathbf{R}$）に対しても，

$$\gamma_1 = \sum_{i=1}^{g} (c_i \alpha_i + d_i \beta_i), \qquad \gamma_2 = \sum_{i=1}^{g} (e_i \alpha_i + f_i \beta_i) \qquad (c_i, d_i, e_i, f_i \in \mathbf{Z})$$

（または，$c_i, d_i, e_i, f_i \in \mathbf{R}$）と書くことができるから，$(\gamma_1, \gamma_2)$ を

$$(\gamma_1, \gamma_2) := \sum_{i=1}^{g} (c_i f_i - d_i e_i)$$

として

$$(\cdot, \cdot) : H_1(R, \mathbf{Z}) \times H_1(R, \mathbf{Z}) \longrightarrow \mathbf{Z}$$

（または，$(\cdot, \cdot) : H_1(R, \mathbf{R}) \times H_1(R, \mathbf{R}) \longrightarrow \mathbf{R}$）に延長する．

0.2 微分

以下で用いる微分の分類について定義しておく[1].

定義 0.2. K を函数体とするとき,

$$\Omega^1_R := \{\omega : \text{微分} \mid (\omega \neq 0 \text{ かつ } \omega \geq 0) \text{ または } \omega = 0\}$$

の元 ω を**第 1 種微分**と呼ぶ[2].

定義 0.3. K の微分 ω が唯 1 つの点でだけ極をもつとき，**第 2 種微分**という．ω が相異なる 2 点においてだけそれぞれ 1 位の極をもつとき，K の**第 3 種微分**という．

注意 1. K の任意の微分は，第 1 種・第 2 種・第 3 種微分の和で書ける．また K の微分全体の集合を $\Omega^1_{R,\mathrm{mel}}$ で表す.

[1] 第 1 種・第 2 種・第 3 種という分類は本によって異なるので，注意が必要である.
[2] [1] では $\mathfrak{L}_0$ と記されている.

1 Abel 積分

コンパクト Riemann 面上の微分に対する Abel 積分とその積分路を closed path γ としてとった周期を定義し，特別な性質をもつ第 1 種微分と第 3 種微分の定義をする．この第 1 種微分は実周期（周期の実部）に関する条件から決まる ω_γ であり，第 3 種微分は Riemann 面上の 2 点 P, Q に対して決まる $\omega_{P,Q}$ というものである．この特殊な形の 2 つ微分の間に成り立つ関係式が，Abel-Jacobi の定理を示す上で非常に重要になる．

1.1 Abel 積分と周期

$K/\mathbf{C}$ を代数函数体，R を $\mathbf{C}(R) = K$ となるコンパクト Riemann 面とする．R の微分 ω に対し，R の path γ 上で正則であるとき，

$$\int_\gamma \omega$$

が定義できる．この積分を **Abel 積分**と呼び，ω が第 1 種微分であるとき**第 1 種 Abel 積分**という．以下では，R の path γ というときは，

考えている微分の極は γ 上には存在しない

ことを常に仮定しておく[3]．

また，γ が closed path であるとき，$\displaystyle\int_\gamma \omega$ の値を γ に関する ω の**周期**という．

注意 2. $\omega \in \Omega^1_{R,\mathrm{mel}}$ が Hasse 微分 wdz として表現されたとき，

$$[0,1] \longrightarrow \gamma, \qquad s \mapsto P(s)$$

とすると，

$$\int_\gamma \omega = \int_0^1 w\frac{dz}{ds}ds \qquad (z = z(P(s)), w = w(P(s)))$$

であって，また，γ を t 平面上の曲線と見做せるとき，$dz = z'(t)dt$ とすると，

$$\int_\gamma \omega = \int_\gamma w\frac{dz}{dt}dt \qquad \left(\frac{dz}{dt} = z'(t)\right)$$

という線積分である．

定理 1.1. ω を第 1 種及び第 2 種微分の和で表される微分として，γ_1, γ_2 を R 上の closed path とする．このとき，$\gamma_1 \sim \gamma_2$ ならば，

$$\int_{\gamma_1} \omega = \int_{\gamma_2} \omega \tag{1}$$

が成り立つ．

[3] この仮定を明確にした言葉として [1] では解析曲線という用語が用いられている．

R の種数を $g \geq 1$ として，ω が第 1 種微分であるとする．

$$H_1(R, \mathbf{Z}) = \langle \gamma_1, \gamma_2, \ldots, \gamma_{2g} \rangle$$

とすれば，R の任意の path γ は

$$\gamma \sim \sum_{i=1}^{2g} c_i \gamma_i \qquad (c_i \in \mathbf{Z})$$

と書けるから，$\zeta_i = \int_{\gamma_i} \omega$ とおけば，

$$\int_\gamma \omega = \sum_{i=1}^{2g} c_i \zeta_i \tag{2}$$

が成り立つ．このことから，$(\zeta_1, \ldots, \zeta_{2g})$ を**基本周期系**と呼ぶ．

1.2 Riemann の関係式と不等式

この基本周期系に対して，以下の重要な事実が成り立つ．

定理 1.2. K を種数 $g \geq 1$ の代数函数体として，R を対応するコンパクト Riemann 面，α_i, β_i を $H_1(R, \mathbf{Z})$ の生成元，即ち，

$$H_1(R, \mathbf{Z}) = \langle \alpha_1, \ldots, \alpha_g, \beta_{g+1}, \ldots, \beta_{2g} \rangle_{\mathbf{Z}}$$

として定める．このとき，K の 2 つの第 1 種微分 ω, ω' の α_i, β_i に関する基本周期系を

$$\zeta_i = \int_{\alpha_i} \omega, \qquad \zeta_{g+i} = \int_{\beta_{g+i}} \omega,$$
$$\zeta'_i = \int_{\alpha_i} \omega', \qquad \zeta'_{g+i} = \int_{\beta_{g+i}} \omega',$$

とすると，

$$\sum_{i=1}^{g} (\zeta_i \zeta'_{g+i} - \zeta_{g+i} \zeta'_i) = 0 \tag{3}$$

が成り立つ．さらに，ζ_i を実部と虚部に分けて

$$\zeta_i = \xi_i + \eta_i \sqrt{-1} \qquad (i = 1, \ldots, 2g)$$

とおけば，$\omega \neq 0$ であれば，

$$\sum_{i=1}^{g} (\xi_i \eta_{g+i} - \xi_{g+i} \eta_i) > 0 \tag{4}$$

が成り立つ．

注意 3. (3) を **Riemann の関係式**，(4) を **Riemann の不等式**という．

Proof. α_i, β_i は 82 ページの図の通りとして，path

$$\Gamma = [\alpha_1, \beta_1][\alpha_2, \beta_2] \cdots [\alpha_g, \beta_g]$$

を考える．Γ で囲まれた領域を U として，U の内部の点 P_0 を固定する．このとき，関数 ω_0, ω_0' を

$$\omega_0 = \omega_0(P) = \int_{P_0}^{P} \omega,$$
$$\omega_0' = \omega_0'(P) = \int_{P_0}^{P} \omega'$$

で定めると，U 内で 1 価正則な関数である．ゆえに，

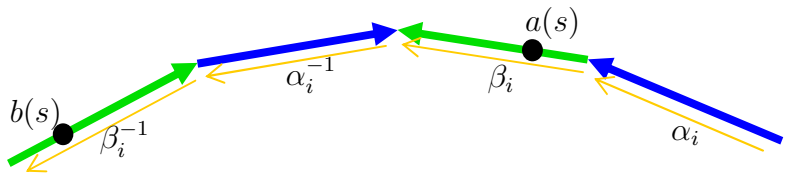
$$\int_\Gamma \omega_0 d\omega_0' = 0$$

となる．

ここで，左辺の積分を計算してみる．そのために，Γ 上の 4 辺からなる path $\alpha_i\beta_i\alpha_i^{-1}\beta_i^{-1}$ をとり，path α_i 上に

$$[0,1] \longrightarrow \alpha_i, \qquad s \mapsto a(s)$$

で対応する点



$$\begin{aligned}
&\omega_0(b(s)) - \omega_0(a(s)) \\
=&(\omega_0(b(s)) - \omega_0(P_0^{(3)})) + (\omega_0(P_0^{(3)}) - \omega_0(P_0^{(2)})) + (\omega_0(P_0^{(2)}) - \omega_0(a(s))) \\
=&\int_{P_0^{(3)}}^{b(s)} \omega + \int_{\beta_i} \omega + \int_{a(s)}^{P_0^{(2)}} \omega = \int_{\beta_i} \omega \\
=&\zeta_{g+i}
\end{aligned}$$

だから，

$$\begin{aligned}
\int_{\alpha_i} \omega_0(P) d\omega_0' &= \int_0^1 \omega_0(a(s)) \frac{d\omega_0'}{ds} ds \\
&= \int_0^1 \omega_0(b(s)) \frac{d\omega_0'}{ds} ds - \zeta_{g+i} \int_0^1 \frac{d\omega_0'}{ds} ds \\
&= -\int_{\alpha_i^{-1}} \omega_0 d\omega_0' - \zeta_{g+i} \int_{\alpha_i} \omega' \\
&= -\int_{\alpha_i^{-1}} \omega_0 d\omega_0' - \zeta_{g+i}\zeta_i'
\end{aligned}$$

となるから，

$$\int_{\alpha_i} \omega_0 d\omega_0' + \int_{\alpha_i^{-1}} \omega_0 d\omega_0' = -\zeta_{g+i}\zeta_i'$$

が成り立つ．同じ操作を β_i 上で考えれば，

$$\int_{\beta_i} \omega_0 d\omega_0' + \int_{\beta_i^{-1}} \omega_0 d\omega_0' = \zeta_i\zeta_{g+i}'$$

が成り立つ．したがって，

$$\begin{aligned}\int_\Gamma \omega_0 d\omega_0' &= \sum_{i=1}^{g} \left(\int_{\alpha_i} \omega_0 d\omega_0' + \int_{\beta_i} \omega_0 d\omega_0' + \int_{\alpha_i^{-1}} \omega_0 d\omega_0' + \int_{\beta_i^{-1}} \omega_0 d\omega_0' \right) \\ &= \sum_{i=1}^{g} (\zeta_i\zeta_{g+i}' - \zeta_{g+i}\zeta_i')\end{aligned}$$

が成り立つから，Riemann の関係式が示せた．

次に，$\xi(P), \eta(P)$ を

$$\omega_0(P) = \xi(P) + \sqrt{-1}\eta(P)$$

で定める．さきの計算と同様に，

$$\xi(b(s)) = \xi(a(s)) + \xi_i$$

であって，

$$\int_{\alpha_i} d\eta = \mathrm{Im}\left(\int_{\alpha_i} \omega \right) = \mathrm{Im}(\zeta_i) = \eta_i$$

であるから，

$$\int_\Gamma \xi d\eta = \sum_{i=1}^{g} (\xi_i\eta_{g+i} - \xi_{g+i}\eta_i) \tag{5}$$

が成り立つ．Green の定理から

$$\int_\Gamma \xi d\eta = \iint_U \left(\frac{\partial \eta}{\partial y}\frac{\partial \xi}{\partial x} - \frac{\partial \eta}{\partial x}\frac{\partial \xi}{\partial y} \right) dxdy$$

が成り立つから，$\omega_0(P)$ が正則関数なので $\dfrac{\partial \xi}{\partial x} = \dfrac{\partial \eta}{\partial y}, \dfrac{\partial \xi}{\partial y} = -\dfrac{\partial \eta}{\partial x}$ であることに注意すれば，

$$\begin{aligned}\int_\Gamma \xi d\eta &= \iint_U \left(\left(\frac{\partial \xi}{\partial x} \right)^2 + \left(\frac{\partial \eta}{\partial x} \right)^2 \right) dxdy \\ &> 0\end{aligned}$$

となって，(5) と合わせれば，Riemann の不等式が成り立つことがいえる． □

1.3 ベクトル空間 Ω^1_R

第 1 種微分に対してその周期を取るという写像が同型写像を与えることが Riemann の不等式からすぐにわかる.

Claim 1. ω を K の第 1 種微分として，$(\zeta_1, \ldots, \zeta_g)$ をその α_i $(i = 1, \ldots, g)$ に関する周期とする．このとき，

$$\omega \mapsto (\zeta_1, \ldots, \zeta_g) \tag{6}$$

によって，同型写像

$$\Omega^1_R \xrightarrow{\sim} \mathbf{C}^g \tag{7}$$

が得られる.

Proof. ω をすべての $i = 1, \ldots, g$ について $\zeta_i = 0$ を満たす第 1 種微分とすると，$i = 1, \ldots, g$ について $\xi_i = \eta_i = 0$ だから，Riemann の不等式 (4) の左辺について

$$\sum_{i=1}^{g} (\xi_i \eta_{g+i} - \xi_{g+i} \eta_i) = 0$$

となり $\omega = 0$ となるから，上の写像は単射である．したがって，$\dim_{\mathbf{C}} \Omega^1_R = g$ だから，上の写像は同型である． □

したがって，逆に，任意の $(z_1, \ldots, z_g) \in \mathbf{C}^g$ に対し，

$$\int_{\alpha_i} \omega = z_i \qquad (i = 1, \ldots, g)$$

を満たす第 1 種微分 ω が存在することがわかる.

同じことを $\mathbf{R}$ 上でも考えることができて，次の主張が成り立つ.

Claim 2. ω を K の第 1 種微分として，

$$\xi_i = \mathrm{Re}\left(\int_{\alpha_i} \omega \right), \qquad \xi_{g+i} = \mathrm{Re}\left(\int_{\beta_i} \omega \right)$$

で $(\xi_1, \ldots, \xi_{2g}) \in \mathbf{R}^{2g}$ を定める．このとき，

$$\omega \mapsto (\xi_1, \ldots, \xi_{2g}) \tag{8}$$

によって，同型写像

$$\Omega^1_R \xrightarrow{\sim} \mathbf{R}^{2g} \tag{9}$$

が得られる.

Proof. $i = 1, \ldots, 2g$ に対して $\xi_i = 0$ とすると，Riemann の不等式 (4) の左辺について

$$\sum_{i=1}^{g} (\xi_i \eta_{g+i} - \xi_{g+i} \eta_i) = 0$$

となり $\omega = 0$ となるから，上の写像は単射である．したがって，$\dim_{\mathbf{R}} \Omega^1_R = 2g$ だから，上の写像は同型である． □

上と同様に，逆に，任意の $(x_1, \ldots, x_{2g}) \in \mathbf{R}^{2g}$ に対し，

$$\mathrm{Re}\left(\int_{\alpha_i} \omega\right) = x_i, \quad \mathrm{Re}\left(\int_{\beta_i} \omega\right) = x_{g+i} \qquad (i = 1, \ldots, g)$$

を満たす第 1 種微分 ω が存在することがわかる．

1.4 第 3 種微分 $\varpi_{P,Q}$ と $\omega_{P,Q}$

Abel-Jacobi の定理には特殊な第 3 種微分が必要になる．それは 2 点 P, Q を決めると定まるものである．

Claim 3. P, Q を固定したとき，任意の $i = 1, \ldots, g$ について

$$\int_{\alpha_i} \varpi_{P,Q} = 0$$

を満たし，かつ，

$$\operatorname*{Res}_P \varpi_{P,Q} = 1, \qquad \operatorname*{Res}_Q \varpi_{P,Q} = -1$$

を満たす第 3 種微分 $\varpi_{P,Q}$ が唯 1 つ存在する．

Proof. Riemann-Roch の定理から $l(W + P + Q) = g + 1, l(W) = g$ だから，P と Q で 1 位の極をもつ微分 ω が存在する．ここで，その P における留数を α とすれば，留数定理によって Q における留数は $-\alpha$ となる．よって，$\frac{1}{\alpha}\omega$ を考えれば，P, Q における留数はそれぞれ $1, -1$ となる．さらに，条件を満たす $\varpi_{P,Q}$ が存在したとすると，$\varpi_{P,Q} - \frac{1}{\alpha}\omega$ は第 1 種微分であるから，Claim 1 よりこのような第 1 種微分が存在することがわかる．したがって，$\varpi_{P,Q}$ が存在することがいえた． □

Claim 1 の代わりに Claim 2 を使えば同様の主張が言える．

Claim 4. P, Q を固定したとき，任意の $i = 1, \ldots, g$ について

$$\mathrm{Re}\left(\int_{\alpha_i} \omega_{P,Q}\right) = 0, \qquad \mathrm{Re}\left(\int_{\beta_i} \omega_{P,Q}\right) = 0$$

を満たし，かつ，

$$\operatorname*{Res}_P \omega_{P,Q} = 1, \qquad \operatorname*{Res}_Q \omega_{P,Q} = -1$$

を満たす第 3 種微分 $\omega_{P,Q}$ が唯 1 つ存在する．

1.5 第 1 種微分 ω_γ と双対性

上述と同様に $\{\gamma_i\}_{i=1,\dots,2g}$ を

$$H_1(R,\mathbf{Z}) = \langle \gamma_1, \dots, \gamma_{2g} \rangle$$

を満たすようにとれば，任意の $\gamma \in Z_1(R,\mathbf{R}) = Z_1(R,\mathbf{Z}) \otimes \mathbf{R}$ に対し，

$$\gamma \sim \sum_{i=1}^{2g} \lambda_i \gamma_i \qquad (\lambda_i \in \mathbf{R}) \tag{10}$$

と書けるから，第 1 種微分 ω の γ に関する周期を

$$\int_\gamma \omega = \sum_{i=1}^{2g} \lambda_i \int_{\gamma_i} \omega$$

で定義する．

定理 1.3. R を種数 $g \geq 1$ のコンパクト Riemann 面として，$\gamma \in Z_1(R,\mathbf{R})$ とする．このとき，

(1) 任意の $\gamma' \in Z_1(R,\mathbf{R})$ に対し，

$$\mathrm{Re}\left(\int_{\gamma'} \omega_\gamma \right) = (\gamma, \gamma') \tag{11}$$

を満たす K の第 1 種微分 ω_γ が唯 1 つ存在する．但し，(γ,γ') は交切数である．

(2) また，$\gamma_1, \gamma_2 \in Z_1(R,\mathbf{R})$ に対し，

$$\gamma_1 \sim \gamma_2 \Longleftrightarrow \omega_{\gamma_1} = \omega_{\gamma_2}$$

が成り立つ．

(3) さらに，

$$\omega_\gamma \mapsto \gamma \bmod B_1(R,\mathbf{R}) \tag{12}$$

によって，同型写像

$$\Omega^1_R \xrightarrow{\sim} H_1(R,\mathbf{R}) = H_1(R,\mathbf{Z}) \otimes \mathbf{R} \tag{13}$$

が得られる．

Proof. (1) $\gamma' \in Z_1(R,\mathbf{R})$ について

$$\gamma' \sim \sum_{i=1}^{g} \mu_i \alpha_i + \sum_{i=1}^{g} \mu_{g+i} \beta_i \qquad (\mu_i \in \mathbf{R})$$

と書くと，

$$\mathrm{Re}\left(\int_{\gamma'}\omega\right)=\sum_{i=1}^{g}\mu_i\mathrm{Re}\left(\int_{\alpha_i}\omega\right)+\sum_{i=1}^{g}\mu_{g+i}\mathrm{Re}\left(\int_{\beta_i}\omega\right),$$
$$(\gamma,\gamma')=\sum_{i=1}^{g}\mu_i(\gamma,\alpha_i)+\sum_{i=1}^{g}\mu_{g+i}(\gamma,\beta_i)$$

である．よって，任意の γ' について (11) が成立することは，任意の $i=1,\dots,g$ に対して

$$(\gamma,\alpha_i)=\mathrm{Re}\left(\int_{\alpha_i}\omega\right),\qquad(\gamma,\beta_i)=\mathrm{Re}\left(\int_{\beta_i}\omega\right)$$

が成り立つことと同値である．ここで，Claim 2 からこのような ω が唯1つ存在することがわかるから，主張が示せる．
(2) $\omega_{\gamma_1}=\omega_{\gamma_2}$ とすれば，任意の γ' に対して

$$(\gamma_1-\gamma_2,\gamma')=(\gamma_1,\gamma')-(\gamma_2,\gamma')=0$$

となる．したがって，$\gamma_1-\gamma_2\sim 0$ だから，$\gamma_1\sim\gamma_2$ がいえた．逆に，$\gamma_1\sim\gamma_2$ ならば，任意の γ' に対して $(\gamma_1,\gamma')=(\gamma_2,\gamma')$ だから，(1) の主張の一意性から，$\omega_{\gamma_1}=\omega_{\gamma_2}$ が成り立つ．
(3) 任意の $\lambda,\mu\in\mathbf{R}$ に対して

$$\begin{aligned}\mathrm{Re}\left(\int_{\gamma'}(\lambda\omega_{\gamma_1}+\mu\omega_{\gamma_2})\right)=&\lambda\mathrm{Re}\left(\int_{\gamma'}\omega_{\gamma_1}\right)+\mu\mathrm{Re}\left(\int_{\gamma'}\omega_{\gamma_2}\right)\\=&\lambda(\gamma_1,\gamma')+\mu(\gamma_2,\gamma')=(\lambda\gamma_1+\mu\gamma_2,\gamma')\\=&\mathrm{Re}\left(\int_{\gamma'}\omega_{\lambda\gamma_1+\mu\gamma_2}\right),\\ \lambda\omega_{\gamma_1}+\mu\omega_{\gamma_2}=&\omega_{\lambda\gamma_1+\mu\gamma_2}\end{aligned}$$

が成り立つから，(12) という対応で $\mathbf{R}$ 同型写像が得られる． □

定理 1.4. pairing

$$\Omega^1_R\times H_1(R,\mathbf{R})\longrightarrow\mathbf{C}_1:=\{z\in\mathbf{C}\mid|z|=1\}$$

を

$$(\omega,\gamma)=\exp\left(2\pi\sqrt{-1}\mathrm{Re}\left(\int_{\gamma}\omega\right)\right)\tag{14}$$

で定義するとき，

$$\Omega^1_R\cong\widehat{H_1(R,\mathbf{R})}$$

が成り立つ，即ち，$\Omega^1_R, H_1(R,\mathbf{R})$ は Pontrjagin dual となる．

Proof. pairing

$$\langle\ ,\ \rangle:\Omega^1_R\times H_1(R,\mathbf{R})\longrightarrow\mathbf{R},\qquad\langle\omega,\gamma\rangle=\mathrm{Re}\left(\int_{\gamma}\omega\right)$$

を考えると，任意の $\omega, \omega' \in \Omega^1_R$, $\gamma, \gamma' \in H_1(R, \mathbf{R})$ について

$$\langle \omega + \omega', \gamma \rangle = \langle \omega, \gamma \rangle + \langle \omega', \gamma \rangle, \qquad \langle \omega, \gamma + \gamma' \rangle = \langle \omega, \gamma \rangle + \langle \omega, \gamma' \rangle$$

が成り立つから，pairing は双線形である．α_i, β_i を $H_1(R, \mathbf{Z})$ の生成元とすれば，(13) から，Ω^1_R の基底として $\{\omega_{\alpha_1}, \ldots, \omega_{\alpha_g}, \omega_{\beta_1}, \ldots, \omega_{\beta_g}\}$ が取れるから，任意の ω, γ に対して，

$$\omega = \sum_{i=1}^{g} \lambda_i \omega_{\alpha_i} + \sum_{i=1}^{g} \lambda_{g+i} \omega_{\beta_i}$$
$$\gamma \sim \sum_{i=1}^{g} \mu_i \alpha_i + \sum_{i=1}^{g} \mu_{g+i} \beta_i$$

とおけば，

$$\begin{aligned}
\langle \gamma, \omega \rangle &= \sum_{i,j=1}^{g} \left\{ \lambda_i \mu_j \mathrm{Re} \left(\int_{\alpha_j} \omega_{\alpha_i} \right) + \lambda_i \mu_{g+j} \mathrm{Re} \left(\int_{\beta_j} \omega_{\alpha_i} \right) \right. \\
&\qquad \left. + \lambda_{g+i} \mu_j \mathrm{Re} \left(\int_{\alpha_j} \omega_{\beta_i} \right) + \lambda_{g+i} \mu_{g+j} \mathrm{Re} \left(\int_{\beta_j} \omega_{\beta_i} \right) \right\} \\
&= \sum_{i,j=1}^{g} \{ \lambda_i \mu_j (\alpha_i, \alpha_j) + \lambda_i \mu_{g+j} (\alpha_i, \beta_j) + \lambda_{g+i} \mu_j (\beta_i, \alpha_j) + \lambda_{g+i} \mu_{g+j} (\beta_i, \beta_j) \} \\
&= \sum_{i,j=1}^{g} (\lambda_i \mu_{g+i} - \lambda_{g+i} \mu_i)
\end{aligned}$$

が成り立つ．ゆえに，paring $\langle \ , \ \rangle$ は非退化である．よって，

$$(\omega, \gamma) = e^{2\pi\sqrt{-1}\langle \omega, \gamma \rangle} = \exp \left(2\pi\sqrt{-1} \sum_{i=1}^{g} (\lambda_i \mu_{g+i} - \lambda_{g+i} \mu_i) \right)$$

によって Ω^1_R と $H_1(R, \mathbf{R})$ が Pontrjagin dual となることがわかる． □

1.6 Riemann の関係式の拡張

特に第 3 種微分が Abel-Jabobi の定理を証明する上で重要な役割を果たすことになるので，第 1 種でない微分に対して Riemann の関係式を考察してみると，次の定理が成り立つ．

定理 1.5. R を $g \geq 1$ のコンパクト Riemann 面として，R 上の点 P_0 を 1 つ固定する．α_i, β_{g+i} $(i = 1, \ldots, g)$ を P_0 を通る $H_1(R, \mathbf{Z})$ の生成元とする．$P_1, \ldots, P_l, Q_1, \ldots, Q_m$ をどの α_i, β_{g+i} 上にもない R の相異なる点とする．$\omega \in \Omega_{R,\mathrm{mero}}$ を高々 $P_1, \ldots, P_l$ で極をもつ微分として，$\omega' \in \Omega_{R,\mathrm{mero}}$ を高々 $Q_1, \ldots, Q_m$ で極をもつ微分とする．ζ_i, ζ_{g+i} と ζ'_i, ζ'_{g+i} をそれぞれ ω と ω' の α_i, β_{g+i} に関する期として，P_i における局所変数 t_i に関する展開を

$$\omega = \sum_s a^{(i)}_s t^s_i, \qquad \omega' = \sum_s a'^{(i)}_s t^s_i$$

とする．さらに，Q_j における局所変数 t_j に関する展開を

$$\omega = \sum_s b_s^{(j)} t_j^s, \qquad \omega' = \sum_s b_s'^{(j)} t_j^s$$

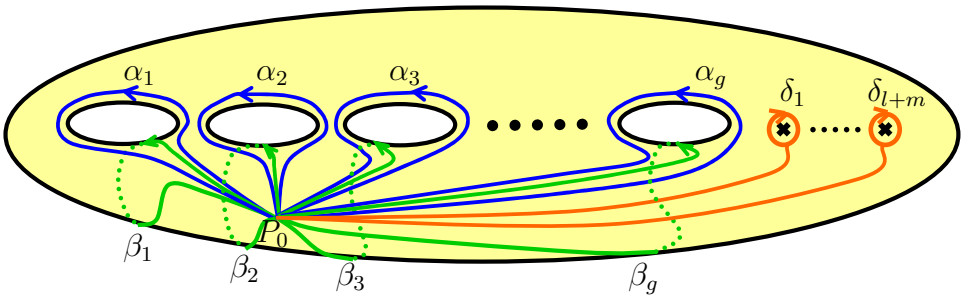
とすると，

$$(15)\quad \frac{1}{2\pi\sqrt{-1}} \sum_{i=1}^{g} (\zeta_i \zeta'_{g+i} - \zeta_{g+i}\zeta'_i) + \sum_{i=1}^{l} \left(a_{-1}^{(i)} \int_{P_0}^{P_i} \omega' + \sum_{s=0}^{\infty} \frac{a_{-s-2}^{(i)} a_s'^{(i)}}{s+1} \right) - \sum_{j=1}^{m} \left(b_{-1}^{(j)} \int_{P_0}^{Q_j} \omega + \sum_{s=0}^{\infty} \frac{b_s^{(j)} b_{-s-2}'^{(j)}}{s+1} \right) = 0$$

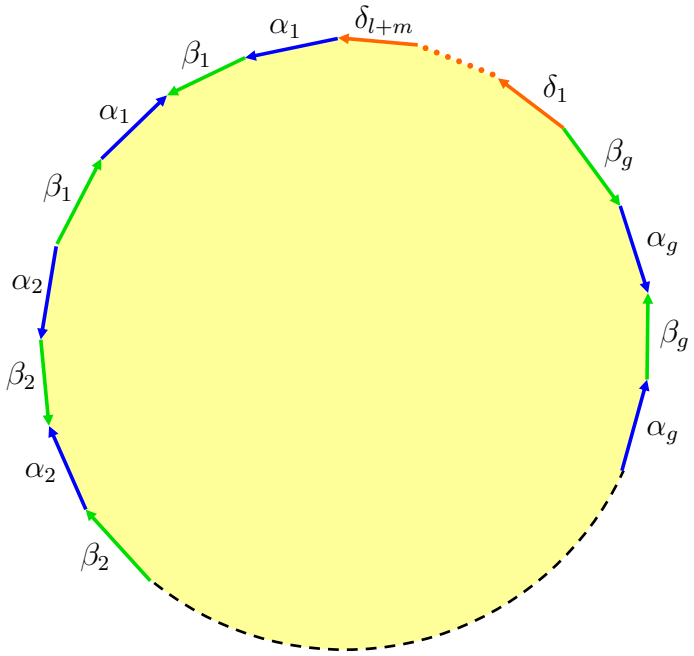
が成り立つ．但し，P_0 から P_i, Q_i への積分路は適当に取るものとする（P_0, P_i, Q_i にのみ依存して ω, ω' には依らずに定まる）．

注意 4. ω, ω' がそれぞれ正則微分である場合には，(15) 式は (3) 式と同値である．

Proof. 定理 1.2 の証明のときに使った $4g$ 角形だけでなく，さらに $l+m$ 個の極を取り除いた path で考える．即ち，α_i, β_i $(i = 1, \ldots, g)$ に加えて，極の周りをまわる path $\delta_1, \ldots, \delta_{l+m}$ をあわせて考える．



但し，$\delta_1, \ldots, \delta_l$ はそれぞれ $P_1, \ldots, P_l$ を $\delta_{l+1}, \ldots, \delta_{l+m}$ はそれぞれ $Q_1, \ldots, Q_m$ をまわる path とする．このとき，この path に沿って切り開くと，



という $(4g+l+m)$ 角形ができる．ここで，極を考えない場合と同様に，

$$\Gamma' := \Gamma\delta_1\cdots\delta_{l+m} = [\alpha_1,\beta_1][\alpha_2,\beta_2]\cdots[\alpha_g,\beta_g]\delta_1\cdots\delta_{l+m} \sim 0$$

であることに注意する．Γ' で囲まれた領域内の点 Q_0 を固定して，関数 ω_0, ω_0' を

$$\omega_0 = \omega_0(P) = \int_{Q_0}^{P} \omega,$$
$$\omega_0' = \omega_0'(P) = \int_{Q_0}^{P} \omega'$$

とする．この path Γ' に沿って積分すれば

$$\int_{\Gamma'} \omega_0 d\omega_0' = 0$$

が成り立つ．Riemann の関係式（定理 1.2）の証明のときのように左辺の積分を考えると，

$$\int_{\Gamma} \omega_0 d\omega_0' = \sum_{i=1}^{g} (\zeta_i\zeta_{g+i}' - \zeta_{g+i}\zeta_i')$$

となることはまったく同様だから，極の周りに沿った積分 $\int_{\delta_i} \omega_0 d\omega_0'$ $(i = 1,\ldots,l+m)$ を計算する．

まず，$i = 1,\ldots,l$ について P_i をまわる積分について考える．このとき，δ_i を取り換えて

$$\int_{\delta_i} \omega_0 d\omega_0' = \lim_{\varepsilon\to 0}\left(\int_{P_0}^{P_i-\varepsilon} \omega_0 d\omega_0' + \int_{C_{P_i}(\varepsilon)} \omega_0 d\omega_0' + \int_{P_i-\varepsilon}^{P_0} \omega_0 d\omega_0'\right)$$

として考えればよい．但し，$C_{P_i}(\varepsilon)$ は P_i の周りを半径 ε の円周上で負の向きにまわる積分路とする．このとき，ω_0 は P_0 で極をもつからその値は $P_0 \to P_i$ と $P_i \to P_0$ で $-2\pi\sqrt{-1}a_{-1}^{(i)}$ だけずれる．ゆえに，

$$\begin{aligned}\int_{P_0}^{P_i-\varepsilon}\omega_0 d\omega_0' + \int_{P_i-\varepsilon}^{P_0}\omega_0 d\omega_0' &= \int_{P_0}^{P_i-\varepsilon}\omega_0(P)d\omega_0' + \int_{P_i-\varepsilon}^{P_0}(\omega_0(P)-2\pi\sqrt{-1}a_{-1}^{(i)})d\omega_0' \\ &= 2\pi\sqrt{-1}a_{-1}^{(i)}\int_{P_0}^{P_i-\varepsilon}\omega'\end{aligned}$$

が成り立つ．次に，$C_{P_i}(\varepsilon)$ についての積分を P_i での局所変数 t_i を用いて

$$\int_{C_{P_i}(\varepsilon)}\omega_0 d\omega_0' = \int_{C_{P_i}(\varepsilon)}\omega_0\frac{d\omega_0'}{dt_i}dt_i = \int_{C_{P_i}(\varepsilon)}\frac{d(\omega_0\omega_0')}{dt_i}dt_i - \int_{C_{P_i}(\varepsilon)}\omega_0'\frac{d(\omega_0)}{dt_i}dt_i$$

と置き換える．ω_0' が P_i で極を持たないことに注意すれば，まったく同じ理由で，1 項目は

$$\int_{C_{P_i}(\varepsilon)}\frac{d(\omega_0\omega_0')}{dt_i}dt_i = -2\pi\sqrt{-1}a_{-1}^{(i)}\omega_0'(P_i)$$

であって，2 項目は

$$\int_{C_{P_i}(\varepsilon)}\omega_0'\frac{d(\omega_0)}{dt_i}dt_i = -2\pi\sqrt{-1}\omega_0'\frac{d\omega_0}{dt_i}\operatorname*{Res}_{t_i=0}\left(\omega_0'\frac{d(\omega_0)}{dt_i}\right)$$

と書ける．この留数を計算してみると，ω' は P_i で正則だから P_i の近傍では，

$$\omega_0'(P) = \omega_0'(P_i) + \int_{P_i}^{P}\omega'\frac{dz}{dt_i}dt_i = \omega_0'(P_i) + \sum_{s=0}^{\infty}\frac{a_s'^{(i)}}{s+1}t_i^{s+1}$$

であって，

$$\frac{d\omega_0}{dt_i} = w\frac{dz}{dt_i} = \sum_s a_s^{(i)}t_i^s$$

だから，

$$\operatorname*{Res}_{t_i=0}\left(\omega_0'\frac{d(\omega_0)}{dt_i}\right) = a_{-1}^{(i)}\omega_0'(P_i) + \sum_{s=0}^{\infty}\frac{a_{-s-2}^{(i)}a_s'^{(i)}}{s+1}$$

となる．したがって，

$$\int_{C_{P_i}(\varepsilon)}\omega_0 d\omega_0' = 2\pi\sqrt{-1}\sum_{s=0}^{\infty}\frac{a_{-s-2}^{(i)}a_s'^{(i)}}{s+1}$$

が成り立つ．したがって，

$$\begin{aligned}&\lim_{\varepsilon\to 0}\left(\int_{P_0}^{P_i-\varepsilon}\omega_0 d\omega_0' + \int_{C_{P_i}(\varepsilon)}\omega_0 d\omega_0' + \int_{P_i-\varepsilon}^{P_0}\omega_0 d\omega_0'\right) \\ =&2\pi\sqrt{-1}a_{-1}^{(i)}\int_{P_0}^{P_i}\omega' + 2\pi\sqrt{-1}\sum_{s=0}^{\infty}\frac{a_{-s-2}^{(i)}a_s'^{(i)}}{s+1}\end{aligned}$$

次に，$i = 1, \ldots, m$ について Q_i をまわる積分

$$\int_{\delta_{l+i}} \omega_0 d\omega_0' = \int_{P_0}^{Q_i-\varepsilon} \omega_0 d\omega_0' + \int_{C_{Q_i}(\varepsilon)} \omega_0 d\omega_0' + \int_{Q_i-\varepsilon}^{P_0} \omega_0 d\omega_0'$$

を考える．ω は Q_i では極を持たないから

$$\int_{P_0}^{Q_i-\varepsilon} \omega_0 d\omega_0' + \int_{Q_i-\varepsilon}^{P_0} \omega_0 d\omega_0' = 0$$

であって，

$$\lim_{\varepsilon\to 0} \int_{Q_i(\varepsilon)} \omega_0 d\omega_0' = -2\pi\sqrt{-1}\left(b_{-1}'^{(i)} \int_{Q_0}^{Q_i} \omega + \sum_{s=0}^{\infty} \frac{b_{-s-2}^{(i)} b_s'^{(i)}}{s+1} \right)$$

が成り立つ．

したがって，すべてを足して $2\pi\sqrt{-1}$ で割れば，

$$\begin{aligned} &\frac{1}{2\pi\sqrt{-1}}(\zeta_i\zeta_{g+i}' - \zeta_{g+i}\zeta_i') \\ &+ \sum_{i=1}^{l} \left(a_{-1}^{(i)} \int_{P_0}^{P_i} \omega' + \sum_{s=0}^{\infty} \frac{a_{-s-2}^{(i)} a_s'^{(i)}}{s+1} \right) \\ &- \sum_{j=1}^{m} \left(b_{-1}^{(j)} \int_{Q_0}^{Q_j} \omega + \sum_{s=0}^{\infty} \frac{b_s^{(j)} b_{-s-2}'^{(j)}}{s+1} \right) = 0 \end{aligned} \tag{16}$$

がわかる．最後に，Q_0 は Γ' で囲まれた領域内の点だったから，Q_0 を P_0 に近付ければ，定理が示せる． □

1.7 変数と係数の交換法則

次に，等式 (15) を具体的な微分に適用することによって得られる 2 つの関係式を証明する．1 つ目は，第 3 種微分 $\overline{\omega}_{P,Q}$ 同士の関係式である．

系 1.5.1 (変数と係数の交換法則). 相異なる 4 点 P, P', Q, Q' を固定し，$\overline{\omega}_{P,P'}$ と $\overline{\omega}_{Q,Q'}$ を Claim 3 で定まる第 3 種微分とすれば，

$$\int_{Q'}^{Q} \overline{\omega}_{P,P'} = \int_{P'}^{P} \overline{\omega}_{Q,Q'} \tag{17}$$

が成り立つ．

Proof. $\omega = \overline{\omega}_{P,P'}$, $\omega' = \overline{\omega}_{Q,Q'}$ とおく．第 3 種微分の定義から極は 1 位だから，(15) は

$$\frac{1}{2\pi\sqrt{-1}} \sum_{i=1}^{g} (\zeta_i\zeta_{g+i}' - \zeta_{g+i}\zeta_i') + \sum_{i=1}^{2} \left(a_{-1}^{(i)} \int_{P_0}^{P_i} \omega' \right) - \sum_{j=1}^{2} \left(b_{-1}^{(j)} \int_{P_0}^{Q_j} \omega \right) = 0$$

と書き換えられる．微分の取り方から，任意の $i = 1, \ldots, g$ について

$$\zeta_i = \zeta'_i = 0$$

であって，P, Q での留数は 1 で P', Q' での留数は -1 だったから，

$$\int_{P_0}^{P} \overline{\omega}_{Q,Q'} - \int_{P_0}^{P'} \overline{\omega}_{Q,Q'} - \left(\int_{P_0}^{Q} \overline{\omega}_{P,P'} - \int_{P_0}^{Q'} \overline{\omega}_{P,P'} \right) = 0$$

が成り立つ．したがって，

$$\int_{P'}^{P} \overline{\omega}_{Q,Q'} = \int_{Q'}^{Q} \overline{\omega}_{P,P'}$$

がいえる． □

2 つ目は，第 3 種微分 $\omega_{P,Q}$ と第 1 種微分の間の関係式であって，これがが Abel-Jacobi の定理を証明する上で鍵になる重要な結果となる．

系 1.5.2. 任意の $\gamma \in Z_1(R, \mathbf{R})$ に対して，

$$\int_{\gamma} \omega_{P,Q} = 2\pi\sqrt{-1}\mathrm{Re}\left(- \int_{Q}^{P} \omega_{\gamma} \right) \tag{18}$$

が成り立つ．

Proof. $\omega = \omega_{\alpha_i}, \omega' = \omega_{P,Q}$ に対して (15) を適用すると，2 位以上の極は無いから

$$\begin{aligned} \frac{1}{2\pi\sqrt{-1}} \sum_{i=1}^{g} (\zeta_i \zeta'_{g+i} - \zeta_{g+i}\zeta'_i) &= \left(b_{-1}^{P} \int_{P_0}^{P} \omega_{\alpha_i} \right) + \left(b_{-1}^{Q} \int_{P_0}^{Q} \omega_{\alpha_i} \right) \\ &= \left(\int_{P_0}^{P} \omega_{\alpha_i} \right) - \left(\int_{P_0}^{Q} \omega_{\alpha_i} \right) \\ &= \int_{Q}^{P} \omega_{\alpha_i} \end{aligned}$$

が成り立つ．ここで，左辺に注目すると，任意の $j = 1, \ldots, g$ について

$$\begin{aligned} \zeta_j &= \int_{\alpha_j} \omega_{\alpha_i} = (\alpha_i, \alpha_j) = 0, \\ \zeta_{g+j} &= \int_{\beta_j} \omega_{\alpha_i} = (\alpha_i, \beta_j) = \delta_{ij} \end{aligned}$$

だから，

$$\int_{Q}^{P} \omega_{\alpha_i} = \frac{1}{2\pi\sqrt{-1}} \sum_{i=1}^{g} (\zeta_i \zeta'_{g+i} - \zeta_{g+i}\zeta'_i) = -\frac{1}{2\pi\sqrt{-1}} \zeta'_i = -\frac{1}{2\pi\sqrt{-1}} \int_{\alpha_i} \omega_{P,Q}$$

両辺の実数部分を考えれば，$w_{P,Q}dz$ の周期が純虚数であることに注意すると

$$\mathrm{Re}\left(\int_{Q}^{P} \omega_{\alpha_i} \right) = -\frac{1}{2\pi\sqrt{-1}} \int_{\alpha_i} \omega_{P,Q},$$

よって，

$$\int_{\alpha_i} \omega_{P,Q} = 2\pi\sqrt{-1}\mathrm{Re}\left(-\int_Q^P \omega_{\alpha_i}\right)$$

が成り立つ．同様に，ω_{α_i} の代わりに ω_{β_i} で考えれば

$$\int_{\beta_i} \omega_{P,Q} = 2\pi\sqrt{-1}\mathrm{Re}\left(-\int_Q^P \omega_{\beta_i}\right)$$

が成り立つので，主張が言えた． □

2 Abel-Jacobiの定理の証明

この節ではこれまでの準備の下で, Abel-Jacobi の定理に軍司氏の稿と異なる方法で証明を与える．その特徴はコンパクト Riemann 面 R 上の必ずしも正則ではない有理型 1-形式を用いるところにある．大体の方針を述べれば, “狭義の乗法函数” と呼ばれる R の普遍被覆 Riemann 面上の函数を通じて, $H_1(R,\mathbb{Z})$ と $\mathrm{Pic}^0(R)$ の Pontrjagin 双対性を導き, それに基づいて Abel-Jacobi 写像が同型であることを示す．その際に鍵になるのは, 乗法函数が R 上の第 3 種微分の Abel 積分を用いて表せるという事実と, 先の節で解説された第 3 種微分の諸性質である．

以下で述べる $H_1(R,\mathbb{Z})$ と $\mathrm{Pic}^0(R)$ の Pontrjagin 双対性を導くアイディアは「代数函数論」p. 278 の脚注にもあるように井草 [2] に基づくものである．

2.1 コンパクト Riemann 面の普遍被覆

以下引き続き R を種数 $g = g(R)$ のコンパクト Riemann 面とする．位相空間としての R の普遍被覆

$$\tilde{R} \xrightarrow{\pi} R$$

に対し, π が Riemann 面間の正則写像となるような 1 次元複素構造が $\tilde{R}$ に一意的に入る．この複素構造で $\tilde{R}$ を Riemann 面と見做す．単連結 Riemann 面の分類により, $\tilde{R}$ は次のいずれかの Riemann 面と同型になる：

(i) $\mathbb{P}^1(\mathbb{C})$ $\quad (g(R) = 0$ のとき$)$

(ii) $\mathbb{C}$ $\quad (g(R) = 1$ のとき$)$

(iii) $\{z \in \mathbb{C} \mid |z| < 1\}$ $\quad (g(R) \geq 2$ のとき$)$

$\mathrm{Aut}(\tilde{R}/R)$ を被覆 $\tilde{R} \xrightarrow{\pi} R$ の被覆変換群とする（$\mathrm{Aut}(\tilde{R}/R)$ の元は自動的に $\tilde{R}$ の Riemann 面としての自己同型になることに注意）．このとき, 基点 $x_0 \in R$ と x_0 の $\tilde{R}$ への持ち上げ $\tilde{x}_0$ (即ち $\pi(\tilde{x}_0) = x_0$ を満たす点) を固定するとき, 群同型

$$\pi_1(R, x_0) \xrightarrow{\sim} \mathrm{Aut}(\tilde{R}/R), \quad \gamma \mapsto \phi_\gamma$$

が導かれる．ここで $\pi_1(R, x_0)$ は x_0 を基点とする R の基本群で, ϕ_γ は以下のように定義される：

$t \in \tilde{R}$ に対し, $\tilde{\delta}_1$ を $\tilde{R}$ 内の t を始点とし $\tilde{x}_0$ を終点とする path, $\delta_1 := \pi \circ \tilde{\delta}_1$, $\tilde{\gamma}$ を $\tilde{R}$ 内の $\tilde{x}_0$ を始点とする path で $\pi \circ \tilde{\gamma} = \gamma$ となるもの, $\tilde{\delta}_2$ を $\tilde{\gamma}$ の終点を始点とする $\tilde{R}$ 内の path で $\pi \circ \tilde{\delta}_2 = \delta_1^{-1}$ となるものとするとき, $\phi_\gamma(t)$ は $\tilde{\delta}_2 \circ \tilde{\gamma} \circ \tilde{\delta}_1$ の終点である．

上の同型は, 基点 x_0 の持ち上げ $\tilde{x}_0$ の取り方に依存することに注意しよう（$\tilde{x}_0$ の取り方を替えると, 同型写像が $\pi_1(R, x_0)$ の内部自己同型分ずれる．この点を講演後にご指摘下さった角皆氏に感謝いたします）．しかし, 上の写像の Abel 化から誘導される同型

$$H_1(R,\mathbb{Z}) \simeq \pi_1(R, x_0)^{\mathrm{ab}} \simeq \mathrm{Aut}(\tilde{R}/R)^{\mathrm{ab}}$$

は基点 x_0 や, その持ち上げ $\tilde{x}_0$ に依存しない標準的同型であるので, 以下の議論に於いて x_0 や $\tilde{x}_0$ の取り方は何ら影響を与えないことを予め注意しておく.

さらに $K := \mathbb{C}(R),\ \tilde{K} := \mathbb{C}(\tilde{R})$ をそれぞれの Riemann 面の函数体とすれば, 標準的単射群準同型

$$\Psi :\ \mathrm{Aut}(\tilde{R}/R) \longrightarrow \mathrm{Aut}(\tilde{K}/K)$$

が次で定義される :

$\phi \in \mathrm{Aut}(\tilde{R}/R),\ f(t) \in \tilde{K}$ に対して $(\Psi(\phi)f)(t) := f(\phi^{-1}(t))$.

以上より, $G := \Psi(\mathrm{Aut}(\tilde{R}/R))$ とおくと, 同型

$$\pi_1(R, x_0) \simeq \mathrm{Aut}(\tilde{R}/R) \simeq G, \quad \gamma \mapsto \phi_\gamma \mapsto \sigma_\gamma := \Psi(\phi_\gamma)$$

が得られ, この同型は標準的同型

$$H_1(R, \mathbb{Z}) \simeq \mathrm{Aut}(\tilde{R}/R)^{\mathrm{ab}} \simeq G^{\mathrm{ab}} \tag{19}$$

を誘導する. ここで $\tilde{K}^G = K$ に注意しよう.

以下, $\underline{g(R) \geq 1}$ を仮定する.

2.2 乗法函数の定義

定義 2.1. 次の条件を満たす $f \in \tilde{K}^\times$ を**乗法函数**という:
任意の $\sigma \in G$ に対して, ある $c_\sigma \in \mathbb{C}^\times$ が存在して $\sigma f = c_\sigma f$ が成立する.
乗法函数全体の集合を $\mathfrak{M}$ で表す. これは $\tilde{K}^\times$ の部分群をなす.

$f \in \mathfrak{M}$ に対し,

$$\chi_f : G \longrightarrow \mathbb{C}^\times, \quad \chi_f(\sigma) = (\sigma f)/f$$

は群準同型 (G の 1 次元指標) である. 従って, χ_f は準同型

$$\chi_f : G^{\mathrm{ab}} := G/[G, G] \longrightarrow \mathbb{C}^\times$$

を誘導する. (19) に注意すれば, χ_f は f から標準的に定まる $H_1(R, \mathbb{Z})$ の 1 次元指標と見做せる.

特に $f \in K^\times$ は乗法函数で $\chi_f = \mathbf{1}$ である. 逆に $f \in \mathfrak{M},\ \chi_f = \mathbf{1}$ ならば前節末の注意より $f \in K^\times$ である. また, $f, g \in \mathfrak{M}$ について $\chi_{fg} = \chi_f\chi_g,\ \chi_{1/f} = \chi_f^{-1}$ である. 従って群準同型

$$\mathfrak{M}/K^\times \longrightarrow \mathrm{Hom}(G^{\mathrm{ab}}, \mathbb{C}^\times), \quad f \mod K^\times \mapsto \chi_f \tag{20}$$

が得られる.

2.3 乗法函数の因子

今後の我々の目標は $H_1(R,\mathbb{Z}) \simeq G^{\mathrm{ab}}$ と $\mathrm{Pic}^0(R)$ の双対性を群準同型 (20) を土台として構成することにある．そのために乗法函数と R の因子類群の関係を見出さねばならないので, “乗法函数の因子” という概念を導入する．

$f \in \mathfrak{M}$ とする．任意の $t_0 \in \tilde{R}$, $\phi \in \mathrm{Aut}(\tilde{R}/R)$ に対し, 乗法函数の定義から $\mathrm{ord}_{t_0}(f) = \mathrm{ord}_{\phi(t_0)}(f)$ が成立する．従って, 形式和

$$\sum_{P\in R} \mathrm{ord}_{\tilde{P}}(f)P \quad (\tilde{P} \in \tilde{R} \text{ は } \pi(\tilde{P}) = P \text{ を満たす任意の点})$$

は有限和で $\mathrm{Div}(R)$ の元を与える．これを f の因子と呼び (f) で表す.

2.4 乗法函数と Abel 積分

乗法函数が R のある種の微分形式の Abel 積分を用いて表せることを説明する．
$f \in \mathfrak{M}$ に対し $\tilde{R}$ 上の有理型 1-形式 $df/f \in \Omega^1_{\tilde{R},\ \mathrm{mel}}$ を考える．t を $\tilde{R} \subseteq \mathbb{C}$ 上の変数とすれば, $df/f = \frac{1}{f(t)}\frac{df(t)}{dt}dt$ である．任意の $\phi \in \mathrm{Aut}(\tilde{R}/R)$ に対し, $\sigma = \Psi(\phi) \in G$ とすれば,

$$\begin{aligned}\phi^*(df/f) &= \frac{1}{(\sigma f)(t)}\frac{d(\sigma f)(t)}{dt}dt \\ &= \frac{1}{\chi_f(\sigma)f(t)} \cdot \chi_f(\sigma)\frac{df(t)}{dt}dt = df/f\end{aligned}$$

なので, df/f は実は R 上の有理型 1-形式であることが分かる．$a \in \tilde{R} \subseteq \mathbb{C}$ に対し, $\mathrm{ord}_a f = m \in \mathbb{Z}$, $t = a$ 近傍での展開を

$$f(t) = (t-a)^m \sum_{i=0}^{\infty} b_i(t-a)^i, \quad b_0 \neq 0$$

とすれば, $t = a$ の近傍で

$$\frac{df}{f} = \frac{1}{f}\frac{df}{dt}dt = \left(\frac{m}{t-a} + \sum_{i=0}^{\infty} c_i(t-a)^i\right)dt$$

と展開される．従って

$$\mathrm{ord}_a(df/f) \geq -1,\ \operatorname*{Res}_a(df/f) = \mathrm{ord}_a(f) \tag{21}$$

となり, df/f は R 上の第 3 種微分でその留数はすべて有理整数である．また, コンパクト Riemann 面 R における留数定理を用いれば

$$\sum_{P\in R} \mathrm{ord}_{\tilde{P}}(f) = \sum_{P\in R} \operatorname*{Res}_P\left(\frac{df}{f}\right) = 0$$

も得られる．従って, 乗法函数の因子は次数が 0 であることが分かった:

$$f \in \mathfrak{M} \Longrightarrow (f) \in \mathrm{Div}^0(R) \tag{22}$$

さて, $f \in \mathfrak{M}$ には自然に R 上の微分 df/f が対応し,

$$\mathfrak{D}_1 := \{\omega \in \Omega^1_{R,\mathrm{mel}} |\ \omega \text{ の極は高々1位で, その留数はすべて有理整数 }\}$$

（$\mathfrak{D}_1$ は $\Omega^1_{R,\mathrm{mel}}$ の $\mathbb{Z}$-部分加群）とすれば, $df/f \in \mathfrak{D}_1$ であった．この対応の逆を考える．

$\omega \in \mathfrak{D}_1$ とする．ω を $\tilde{R}$ 上の微分として定点 $a \in \tilde{R}$ から $t \in \tilde{R}$ まで積分する：

$$\int_a^t \omega$$

ω は正則とは限らないので, この積分はもちろん a から t に至る積分路の取り方に依存するが, ω の留数はすべて整数なので積分路を取り替えてもその値の差は $2\pi\sqrt{-1}$ の整数倍の違いしかない（函数論の Cauchy の積分定理）．従って,

$$f(t) := \exp\left(\int_a^t \omega\right)$$

は積分路の取り方によらず, t のみで完全に定まるので, $f \in \tilde{K}$ である．また, 任意の $\sigma \in G$ について, $\sigma = \Psi(\phi_\gamma)$ $(\gamma \in \pi_1(R, x_0))$ とすれば

$$\begin{aligned}\sigma f(t) = f(\phi_\gamma^{-1}(t)) &= \exp\left(\int_a^{\phi_\gamma^{-1}(t)} \omega\right) \\ &= \exp\left(\int_t^{\phi_\gamma^{-1}(t)} \omega\right) \exp\left(\int_a^t \omega\right) = \exp\left(\int_{-\gamma} \omega\right) f(t)\end{aligned}$$

（最後の積分は R 上で考えている）となり, f は乗法函数で

$$\chi_f(\sigma) = \exp\left(-\int_\gamma \omega\right)$$

が分かる．さらに, $f \in \mathfrak{M}$ に対して, $df/f \in \mathfrak{D}_1$ で

$$f(t) = f(a) \exp\left(\int_a^t \frac{df}{f}\right)$$

も容易に分かる．従って次を得た：

定理 2.2. $\mathbb{Z}$-加群として

$$\mathfrak{D}_1 \simeq \mathfrak{M}/\mathbb{C}^\times, \quad \omega \mapsto \exp\left(\int_a^t \omega\right) \mod \mathbb{C}^\times$$

逆写像は, $\mathfrak{M}/\mathbb{C}^\times \ni f \bmod \mathbb{C}^\times \mapsto df/f \in \mathfrak{D}_1$ で与えられる．また, $f \in \mathfrak{M}$ について

$$\chi_f(\sigma_\gamma) = \exp\left(-\int_\gamma \frac{df}{f}\right) \quad (\gamma \in \pi_1(R, x_0))$$

が成立する．

2.5 狭義の乗法函数と $\mathbf{Div}^0(R)$

ここでは, 狭義の乗法函数という概念を導入し, それと $\mathrm{Div}^0(R)$ の関係を明らかにする.

まず, § 1 で導入された第 3 種微分 $\omega_{P,Q}$ （**Claim 4** 参照）について復習しておこう : $\omega_{P,Q} \in \Omega^1_{R,\mathrm{mel}}$ は $P,\ Q \in R$ のみで極を持ち, その極は全て 1 位で

$$\operatorname*{Res}_P \omega_{P,Q} = 1,\ \operatorname*{Res}_Q \omega_{P,Q} = -1,\ \mathrm{Re}\int_\gamma \omega_{P,Q} = 0\ (\forall \gamma \in H_1(R,\mathbb{R})) \tag{23}$$

を満たす. このような性質をもつ有理型 1-形式は P, Q から一意的に定まる.

注意 2.1　一般に第 3 種微分 ω の留数は 0 とは限らないので closed path γ に関する積分 $\displaystyle\int_\gamma \omega$ は γ の homotopy 類のみでは定まらない. しかし, ω の留数がすべて実数であれば, γ と homotope な closed path γ' に対して,

$$\int_\gamma \omega - \int_{\gamma'} \omega \in \sqrt{-1}\mathbb{R}$$

が成立するので, $\mathrm{Re}\displaystyle\int_\gamma \omega$ は γ の homotopy 類のみで定まる. 従って, 留数が全て実数であるような有理型 1-形式 ω と $\gamma \in H_1(R,\mathbb{R})$ に対しては, $\mathrm{Re}\displaystyle\int_\gamma \omega$ は well-defined である.

この $\omega_{P,Q}$ を用いれば,

$$\mathfrak{D}_1 = \left(\sum_{(P,Q)\in R^2,\ P\neq Q} \mathbb{Z}\,\omega_{P,Q} \right) \oplus \Omega^1_R \tag{24}$$

となることは $\mathfrak{D}_1$ の定義と留数定理から明らかであろう（上の右辺の和が直和であることは § 1 の **Claim 2** から従う（下の議論参照））.

定義 2.3. $|\chi_f(\sigma)| = 1\ (\forall \sigma \in G)$ を満たす乗法函数 $f \in \mathfrak{M}$ を**狭義の乗法函数**と言う. $\mathfrak{M}_0$ で狭義の乗法函数全体のなす乗法群を表す.

定理 2.2 より, $f(t) \in \mathfrak{M}$ はある $\omega \in \mathfrak{D}_1$ を用いて

$$f(t) = \exp\left(\int_a^t \omega\right)$$

と書ける. このとき同定理より,

$$|\chi_f(\Psi(\phi_\gamma))| = \exp\left(-\mathrm{Re}\int_\gamma \omega\right) \quad (\gamma \in \pi_1(R,x_0))$$

なので, $f \in \mathfrak{M}_0$ となるための必要十分条件は

$$\mathrm{Re}\int_\gamma \omega = 0\ \ (\forall \gamma \in H_1(R,\mathbb{Z}))$$

である．(24) と § 1**Claim 2** で示された

$$\nu \in \Omega^1_R,\ \mathrm{Re}\int_\gamma \nu = 0\ (\forall \gamma \in H_1(R,\mathbb{Z})) \Longrightarrow \nu = 0$$

という事実より, これは結局

$$\omega \in \sum_{(P,Q)\in R^2,\ P\neq Q} \mathbb{Z}\,\omega_{P,Q}$$

と同値である．従って,

$$\mathfrak{D}_2 := \sum_{(P,Q)\in R^2,\ P\neq Q} \mathbb{Z}\,\omega_{P,Q}$$

とおけば, 次を得た：

定理 2.4. $\mathbb{Z}$-加群として

$$\mathfrak{D}_2 \simeq \mathfrak{M}_0/\mathbb{C}^\times,\quad \omega \mapsto \exp\left(\int_a^t \omega\right) \mod \mathbb{C}^\times$$

逆写像は, $\mathfrak{M}_0/\mathbb{C}^\times \ni f \bmod \mathbb{C}^\times \mapsto df/f \in \mathfrak{D}_2$ で与えられる．

この定理から次の重要な結果が得られる：

定理 2.5.

$$\mathfrak{M}_0/\mathbb{C}^\times \simeq \mathrm{Div}^0(R),\quad f \mod \mathbb{C}^\times \mapsto (f)$$
$$\mathfrak{M}_0/K^\times \simeq \mathrm{Pic}^0(R),\quad f \mod K^\times \mapsto [(f)]$$

Proof. まず (22) より,

$$f \in \mathfrak{M}_0 \Longrightarrow (f) \in \mathrm{Div}^0(R)$$

に注意しよう．任意の $\sum_{i=1}^r (P_i - Q_i) \in \mathrm{Div}^0(R)$ に対し, $\omega := \sum_{i=1}^r \omega_{P_i,Q_i} \in \mathfrak{D}_2$ とおくと, **定理 2.4** より, $f(t) := \exp\left(\int_a^t \omega\right) \in \mathfrak{M}_0$ で, (21) と (23) より

$$(f) = \sum_{i=1}^r (P_i - Q_i)$$

となる．よって,

$$\mathfrak{M}_0/\mathbb{C}^\times \longrightarrow \mathrm{Div}^0(R),\quad f \mod \mathbb{C}^\times \mapsto (f) \tag{25}$$

は全射．$f \in \mathfrak{M}_0$, $(f) = 0$ とする．このとき, (21) より $df/f \in \Omega^1_R$ となるが, 一方では**定理 2.4** より $df/f \in \mathfrak{D}_2$ なので, $\Omega^1_R \cap \mathfrak{D}_2 = 0$ より, $f \in \mathbb{C}^\times$. 従って (25) は同型写像．2 番目の同型は 1 番目の同型を $K^\times/\mathbb{C}^\times$ に制限すれば

$$K^\times/\mathbb{C}^\times \xrightarrow{\sim} \mathrm{Div}^l(R)$$

となることから得られる． □

2.6 $\mathrm{Pic}^0(R)$ と $H_1(R,\mathbb{Z})$ の Pontrjagin 双対性

定理 2.5 は, 代数体の整数論の単項化定理「有限次代数体 K の任意の因子（イデアル）は, K の最大不分岐 Abel 拡大 $\tilde{K}^{\mathrm{ab}}$ に於いては主因子（単項イデアル）になる」の類似と見做せることに注意しよう（歴史的には寧ろ単項化定理が**定理 2.5** の類似？）. 実際, 乗法函数はその定義より $G \simeq \mathrm{Aut}(\tilde{R}/R)$ の交換子群の元では不変なので R の最大 Abel 被覆 Riemann 面 $\tilde{R}^{\mathrm{ab}}$ の函数体の元である.

単項化定理の証明は, Artin 相互法則, すなわち K の因子類群と $\mathrm{Gal}(\tilde{K}^{\mathrm{ab}}/K)$ の標準的な同型の存在に基づく. 函数体の場合, ここでは逆に**定理 2.5** に基づいて $\mathrm{Pic}^0(R)$ と $G^{\mathrm{ab}} \simeq H_1(R,\mathbb{Z})$ の間に標準的な双対性が存在することを導く.

まず, 局所コンパクト Abel 群の Pontrjagin 双対定理について復習しておこう. 局所コンパクト Abel 群 A に対し, $\widehat{A} := \mathrm{Hom}_{\mathrm{cont}}(A,\mathbb{C}_1)$ ($\mathbb{C}_1 := \{z \in \mathbb{C} |\ |z| = 1\}$), 即ち A から $\mathbb{C}_1$ への連続準同型全体の成す Abel 群を A の**指標群**という. A のコンパクト部分集合 K と $\mathbb{C}_1$ の単位元の開近傍 W に対し,

$$U(K,W) := \{\chi \in \widehat{A} \mid \chi(K) \subseteq W\} \subseteq \widehat{A}$$

とおく. そして各 $\psi \in \widehat{A}$ に対し,

$$\{\psi + U(K,W) \mid K \subseteq A : \text{コンパクト},\ \ 1 \in W \subseteq \mathbb{C}_1 : \text{開集合}\}$$

を ψ の基本近傍系とする位相を入れることで $\widehat{A}$ は局所コンパクト Abel 群になる. 今後 $\widehat{A}$ は常にこの位相で位相群と考える.

定理 2.6. (i) (**Pontrjagin 双対定理**) 任意の局所コンパクト Abel 群 A について,

$$A \simeq \widehat{\widehat{A}},\ \ A \ni a \mapsto (\widehat{A} \ni \chi \mapsto \chi(a) \in \mathbb{C}_1)$$

となる.
(ii) A の 閉部分群B に対し, B の**零化部分群**$B^{\perp}$ を

$$B^{\perp} := \{\chi \in \widehat{A} |\ \chi(B) = 1\}$$

で定義するとき,

$$\widehat{A/B} \simeq B^{\perp},\ \ \widehat{B} \simeq \widehat{A}/B^{\perp},\ \ \ (B^{\perp})^{\perp} = B\ \text{((i) の同型で } A \text{ と } \widehat{\widehat{A}} \text{ を同一視)}$$

が成立する.

定理 2.5 と群準同型写像 (20) の定義域を $\mathfrak{M}_0/K^{\times}$ に制限したものより群準同型

$$\varphi : \mathrm{Pic}^0(R) \longrightarrow \widehat{G^{\mathrm{ab}}},\ \ [D] \mapsto \chi_{f_D} \tag{26}$$

が定義される. ここで, $f_D \in \mathfrak{M}_0$ は $(f_D) = D$ を満たす元である. f_D は**定理 2.5** より $D \in \mathrm{Div}^0(R)$ に対して modulo $\mathbb{C}^{\times}$ で一意に存在し, χ_{f_D} は D の因子類 $[D] \in \mathrm{Pic}^0(R)$ にのみ依存する. また, G^{ab} は離散 Abel 群と見做す.

以下, (26) の φ が同型であることを示そう．まず, χ_{f_D} の定義と**定理 2.5** より

$$\chi_{f_D} = 1 \Longleftrightarrow f_D \in K^{\times} \Longleftrightarrow D \in \mathrm{Div}^{l}(R)$$

なので, 準同型 φ は単射である.

$D = \sum_{i=1}^{r}(P_i - Q_i) \in \mathrm{Div}^0(R)$ に対し, **定理 2.5** の証明より

$$f_D(t) = \exp\left(\sum_{i=1}^{r}\int_a^t \omega_{P_i,Q_i}\right) \quad (\exists a \in \tilde{R})$$

となる．このとき, $\sigma_\gamma = \Psi(\phi_\gamma) \in G$, $\gamma \in \pi_1(R, x_0)$ に対し, **定理 2.2** より

$$\chi_{f_D}(\sigma_\gamma) = \exp\left(-\sum_{i=1}^{r}\int_\gamma \omega_{P_i,Q_i}\right)$$

となる．ここで§ 1 で示された事実（**系 1.5.2**）

$$\int_\gamma \omega_{P,Q} = -2\pi\sqrt{-1}\,\mathrm{Re}\int_Q^P \omega_\gamma \tag{27}$$

を用いると,

$$\varphi([D])(\sigma_\gamma) = \chi_{f_D}(\sigma_\gamma) = \exp\left(2\pi\sqrt{-1}\sum_{i=1}^{r}\mathrm{Re}\int_{Q_i}^{P_i}\omega_\gamma\right), \quad D = \sum_{i=1}^{r}(P_i - Q_i) \tag{28}$$

が得られる.

注意 2.2 (27) は, 右辺の積分の積分路を “然るべく” 取るとき, その積分路に関しては任意の $\gamma \in H_1(R, \mathbb{Z})$ について等式が成立するという意味であった．しかし (28) の右辺の積分については積分路を取り替えてもその値の実部の差は有理整数であるから, (28) の等式の右辺の値は積分路の取り方には依らない.

ここで $g = g(R)$ 個の点 $Q_1, Q_2, \ldots, Q_g \in R$ を固定するとき, 任意の $\mathrm{Pic}^0(R)$ の因子類は必ず $\sum_{1=1}^{g}(P_i - Q_i)$ の形の元を含むので（Riemann-Roch の定理の応用）, 写像

$$R^g \longrightarrow \mathrm{im}\,\varphi \subseteq \widehat{G^{\mathrm{ab}}},$$
$$(P_1, P_2, \ldots, P_g) \mapsto \left(\sigma_\gamma \mapsto \exp\left(2\pi\sqrt{-1}\sum_{i=1}^{g}\mathrm{Re}\int_{Q_i}^{P_i}\omega_\gamma\right)\right)$$

は (28) より全射であり, R^g に直積位相を入れるならば, この写像は指標群 $\widehat{G^{\mathrm{ab}}}$ の位相の定義より連続写像であることも分かる．よって R^g がコンパクトであることから, $\mathrm{im}\,\varphi$ は $\widehat{G^{\mathrm{ab}}}$ の閉部分群であることが分かった．そこで $A := \widehat{G^{\mathrm{ab}}}$, $B := \mathrm{im}\,\varphi \subseteq A$ とおいて, **定理 2.6** を適用してみる．このとき

$$B^{\perp} = \{\sigma \in G^{\mathrm{ab}} |\ \forall \chi \in B : \chi(\sigma) = 1\}$$

である．よって $\sigma := \sigma_\gamma \bmod [G,G] \in B^\perp$ とすると, (28) より

$$\exp\left(2\pi\sqrt{-1}\mathrm{Re}\int_Q^P \omega_\gamma\right) = 1 \tag{29}$$

が任意の $P,Q \in R$ について成り立つ．もしも G^{ab} に於いて $\sigma \neq 1$ であるならば $H_1(R,\mathbb{Z})$ において $\gamma \neq 0$ なので, $\omega_\gamma \in \Omega^1_R$ の定義と交切数ペアリングの非退化性より, $\mathrm{Re}\int_\delta \omega_\gamma \neq 0$ をみたす closed path δ が存在する．従って Q を δ の始点とすれば, δ 上のある点 P で, $\mathrm{Re}\int_Q^P \omega_\gamma \notin \mathbb{Z}$ を満たすものが存在する（積分路は δ に沿う）．これは (29) に矛盾する．よって $B^\perp = 0$ が示されたので, **定理 2.6 (ii)** より $B = (B^\perp)^\perp = A$, 即ち, $\widehat{G^{\mathrm{ab}}} = \mathrm{im}\,\varphi$ が分かった．以上で φ が同型であることが証明された.

以下同型 φ によって $\mathrm{Pic}^0(R)$ にコンパクト Abel 群 $\widehat{G^{\mathrm{ab}}}$ からの位相を入れてコンパクト Abel 群と見做す．$G^{\mathrm{ab}} \simeq H_1(R,\mathbb{Z})$ なので, 結局 φ の同型性は離散 Abel 群 $H_1(R,\mathbb{Z})$ とコンパクト Abel 群 $\mathrm{Pic}^0(R)$ の間の Pontrjagin 双対性を与える:

定理 2.7.

$$\mathrm{Pic}^0(R) \xrightarrow{\sim} H_1(R,\mathbb{Z})\widehat{\ }, \quad [D] \mapsto \chi_D$$

ここで, $D = \sum_{i=1}^r (P_i - Q_i) \in \mathrm{Div}^0(R)$ と $\gamma \in H_1(R,\mathbb{Z})$ に対し,

$$\chi_D(\gamma) = \exp\left(2\pi\sqrt{-1}\sum_{i=1}^r \mathrm{Re}\int_{Q_i}^{P_i} \omega_\gamma\right)$$

$H_1(R,\mathbb{Z}) \simeq \mathbb{Z}^{2g}$ であるから, 位相群として

$$\mathrm{Pic}^0(R) \simeq (\mathbb{R}/\mathbb{Z})^{2g}$$

が分かる．$\mathrm{Pic}^0(R)$ には位相群としての構造のみでなく, 標準的な複素 Lie 群の構造が入ることを次節で説明する.

2.7 Abel-Jacobi の定理

これまでに次の 2 つの重要な双対性が示された：

$$\begin{aligned} &\Omega^1_R \simeq H_1(R,\mathbb{R})\widehat{\ }, \\ &\omega \mapsto \left(\gamma \mapsto \exp\left(2\pi\sqrt{-1}\mathrm{Re}\int_\gamma \omega\right)\right) \end{aligned} \tag{30}$$

$$\begin{aligned} &\mathrm{Pic}^0(R) \simeq H_1(R,\mathbb{Z})\widehat{\ }, \\ &\left[\sum_{i=1}^r (P_i - Q_i)\right] \mapsto \left(\gamma \mapsto \exp\left(2\pi\sqrt{-1}\sum_{i=1}^r \mathrm{Re}\int_{Q_i}^{P_i} \omega_\gamma\right)\right) \end{aligned} \tag{31}$$

ここで, $H_1(R,\mathbb{Z})$ は $H_1(R,\mathbb{R})$ の閉部分群なので,

$$\Lambda := \left\{ \omega \in \Omega^1_R \;\middle|\; \forall \gamma \in H_1(R,\mathbb{Z}) : \mathrm{Re}\int_\gamma \omega \in \mathbb{Z} \right\}$$

とすれば, **定理 2.6** と上の 2 つの双対性 (30), (31) より,

$$\mathrm{Pic}^0(R) \simeq H_1(R,\mathbb{Z})\widehat{\ } \simeq H_1(R,\mathbb{R})\widehat{\ }/H_1(R,\mathbb{Z})^\perp \simeq \Omega^1_R/\Lambda$$

を得る. この標準的な同型を ρ で表すことにする :

$$\rho : \mathrm{Pic}^0(R) \simeq \Omega^1_R/\Lambda$$

ここで, $D = \sum_{i=1}^r (P_i - Q_i) \in \mathrm{Div}^0(R)$ に対し, $\omega \bmod \Lambda := \rho([D])$ は,

$$\mathrm{Re}\int_\gamma \omega \equiv \mathrm{Re}\sum_{i=1}^r \int_{Q_i}^{P_i} \omega_\gamma \pmod{\mathbb{Z}} \quad (\forall \gamma \in H_1(R,\mathbb{Z})) \tag{32}$$

で特徴付けられる. 同型 ρ を用いて, Abel-Jacobi の定理を証明しよう.

定理 2.8 (Abel-Jacobi の定理). $\omega_1, \ldots, \omega_g$ を Ω^1_R の $\mathbb{C}$-基底とする.

$$L := \left\{ \left(\int_\gamma \omega_1, \ldots, \int_\gamma \omega_g \right) \in \mathbb{C}^g \;\middle|\; \gamma \in H_1(R,\mathbb{Z}) \right\}$$

とおけば, Abel-Jacobi 写像 (周期写像)

$$\begin{aligned} \mathrm{Pic}^0(R) &\longrightarrow \mathbb{C}^g/L, \\ \left[\sum_{i=1}^r (P_i - Q_i) \right] &\mapsto \left(\sum_{i=1}^r \int_{Q_i}^{P_i} \omega_1, \ldots, \sum_{i=1}^r \int_{Q_i}^{P_i} \omega_g \right) \bmod L \end{aligned}$$

は群同型. ここで, $\displaystyle\int_{Q_i}^{P_i}$ の積分路は各成分共通に採る.

Proof. $H_1(R,\mathbb{Z}) = \bigoplus_{i=1}^{2g} \mathbb{Z}\gamma_i$ とすると, 写像

$$\begin{aligned} \Omega^1_R/\Lambda &\longrightarrow \mathbb{R}^{2g}/\mathbb{Z}^{2g}, \\ \omega \bmod \Lambda &\mapsto \left(\mathrm{Re}\int_{\gamma_1} \omega, \mathrm{Re}\int_{\gamma_2} \omega, \ldots, \mathrm{Re}\int_{\gamma_{2g}} \omega \right) \bmod \mathbb{Z}^{2g} \end{aligned} \tag{33}$$

は同型である. なぜなら, 単射性は Λ の定義より明らかで, 全射性は, § 1 で示された $\mathbb{R}$-ベクトル空間のペアリング

$$\Omega^1_R \times H_1(R,\mathbb{R}) \to \mathbb{R}, \quad (\omega, \gamma) \mapsto \mathrm{Re}\int_\gamma \omega$$

の非退化性と $H_1(R,\mathbb{R}) = H_1(R,\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{R}$ から従うからである.

標準的同型 $\rho : \mathrm{Pic}^0(R) \longrightarrow \Omega^1_R/\Lambda$ と同型 (33) を合成することで, (32) に注意すれば同型

$$\begin{aligned} \mathrm{Pic}^0(R) &\xrightarrow{\sim} \mathbb{R}^{2g}/\mathbb{Z}^{2g}, \\ \left[\sum_{i=1}^{r}(P_i - Q_i)\right] &\mapsto \left(\mathrm{Re}\sum_{i=1}^{r}\int_{Q_i}^{P_i}\omega_{\gamma_1}, \ldots, \mathrm{Re}\sum_{i=1}^{r}\int_{Q_i}^{P_i}\omega_{\gamma_{2g}}\right) \mod \mathbb{Z}^{2g} \end{aligned} \tag{34}$$

を得る．さて,

$$\omega_1,\ -\sqrt{-1}\,\omega_1,\ \omega_2,\ -\sqrt{-1}\,\omega_2, \ldots, \omega_g,\ -\sqrt{-1}\,\omega_g$$

と

$$\omega_{\gamma_1}, \omega_{\gamma_2} \ldots, \omega_{\gamma_{2g}}$$

は各々 Ω^1_R の $\mathbb{R}$-基底をなすので

$$(\omega_1,\ -\sqrt{-1}\,\omega_1, \ldots, \omega_g,\ -\sqrt{-1}\,\omega_g) = (\omega_{\gamma_1}, \ldots, \omega_{\gamma_{2g}})T$$

を満たす $T \in \mathrm{GL}_{2g}(\mathbb{R})$ が存在する．そこで同型 (34) に引き続きさらに同型

$$\mathbb{R}^{2g}/\mathbb{Z}^{2g} \simeq \mathbb{R}^{2g}/\mathbb{Z}^{2g}T \simeq \mathbb{C}^g/h(\mathbb{Z}^{2g}T)$$

を合成する．ここで最初の同型は右から行列 T を掛けることで得られるもので, 第 2 の同型は

$$\begin{aligned} h : \mathbb{R}^{2g} &\longrightarrow \mathbb{C}^g, \\ (x_1, x_2, \ldots, x_{2g-1}, x_{2g}) &\mapsto (x_1 + \sqrt{-1}x_2, \ldots, x_{2g-1} + \sqrt{-1}x_{2g}) \end{aligned}$$

から誘導されるものである.

$\gamma \in H_1(R, \mathbb{Z})$ について

$$\left(\int_\gamma \omega_1, \ldots, \int_\gamma \omega_g\right) = h\left(\left(\mathrm{Re}\int_\gamma \omega_{\gamma_1}, \ldots, \mathrm{Re}\int_\gamma \omega_{\gamma_{2g}}\right)T\right)$$

であり, $\left(\mathrm{Re}\displaystyle\int_{\gamma_j}\omega_{\gamma_i}\right)_{i,j} = ((\gamma_i, \gamma_j))_{i,j} \in \mathrm{GL}_{2g}(\mathbb{Z})$ なので ($H_1(R, \mathbb{Z})$ の $\mathbb{Z}$-基底として $\alpha_i,\ \beta_i\ (1 \leq i \leq g)$ を採ったときの交切数ペアリングの Gram 行列式は ± 1 だから)

$$h(\mathbb{Z}^{2g}T) = L$$

が分かる．さらに,

$$\begin{aligned} h\left(\left(\mathrm{Re}\sum_{i=1}^{r}\int_{Q_i}^{P_i}\omega_{\gamma_1}, \ldots, \mathrm{Re}\sum_{i=1}^{r}\int_{Q_i}^{P_i}\omega_{\gamma_{2g}}\right)T\right) \\ = \left(\sum_{i=1}^{r}\int_{Q_i}^{P_i}\omega_1, \ldots, \sum_{i=1}^{r}\int_{Q_i}^{P_i}\omega_g\right) \end{aligned}$$

が成り立つので, 定理の主張が証明された. □

上の定理の L は $\mathbb{C}^g$ の格子になる．なぜならば, $H_1(R,\mathbb{Z}) = \bigoplus_{i=1}^{2g} \mathbb{Z}\gamma_i$ とすれば, L は $\mathbb{Z}$ 上

$$\left(\int_{\gamma_i} \omega_1, \ldots, \int_{\gamma_i} \omega_g\right) \quad (1 \leq i \leq 2g) \tag{35}$$

で生成されるが,

$$\sum_{i=1}^{2g} c_i \left(\int_{\gamma_i} \omega_1, \ldots, \int_{\gamma_i} \omega_g\right) = 0 \ \ (c_i \in \mathbb{R})$$

ならば, $\delta = \sum_{i=1}^{2g} c_i\gamma_i \in H_1(R,\mathbb{R})$ と任意の $\omega \in \Omega^1_R$ に対して, $\int_\delta \omega = 0$ となる．従って, (30) より $\delta = 0$, つまり, $c_i = 0$ $(1 \leq i \leq 2g)$ を得る．よって (35) は $\mathbb{R}$ 上線型独立であるから, L は $\mathbb{C}^g$ の格子である．従って, Abel-Jacobi 写像は $\mathrm{Pic}^0(R)$ と g 次元複素トーラス $\mathbb{C}^g/L$ の間の群同型を与える．この $\mathbb{C}^g/L$ の複素 Lie 群としての構造は, Ω^1_R の $\mathbb{C}$-基底 $\omega_1, \ldots, \omega_g$ の採り方に依らずに R のみから一意的に定まる（$\mathbb{C}$-基底を取り替えると, 格子 L が $\mathrm{GL}_g(\mathbb{C})$ の作用で変化するから）．この $\mathbb{C}^g/L$ を R の **Jacobi 多様体**と呼び, $\mathrm{Jac}(R)$ で表す:

$$\mathrm{Jac}(R) = \mathbb{C}^g/L$$

従って, Abel-Jacobi 写像によって $\mathrm{Pic}^0(R)$ に標準的な複素 Lie 群の構造が入る．

参考文献

[1] 岩澤健吉: 代数函数論, 岩波書店

[2] J. Igusa（井草準一）: Zur klassischen Theorie der algebraischen Funktionen, *J. Math. Soc. Japan* **1** (1948), 63–72.

第 15 回 整数論サマースクール 報告集, pp.113-129

種数 1 における理論

山内 卓也*

0. 序文

これまでの話を種数 1 の代数曲線に対して具体的に展開していくことが本稿の目的である. 特に, 次の点に留意して話を進めていく.
(1) σ 関数を中心に楕円関数論をまとめること
(2) 種数 1 の (複素) 代数曲線の場合に Riemann-Roch Theorem, Abel-Jacobi Theorem を具体的に理解すること
(3) 後半の内容 (特に, [5]) の導入部分となること
尚, 楕円関数論に関する歴史に興味がある方は [6] の 7 章および [4] 等を参照して頂きたい.

1. 種数 1 の (複素) 代数曲線

吉冨氏の講演 [8] によると, 種数 1 の複素代数曲線と種数 1 のコンパクトリーマン面とは同等の概念であった. また, 種数 1 の (複素) 代数曲線は楕円曲線 (1 次元複素アーベル多様体) と呼ばれ代数的な群演算を備えている.

1 次元複素アーベル多様体 X とは 1 次元複素トーラスである. 従って, $\mathbb{C}$ の格子 Λ が存在して,

$$X = \mathbb{C}/\Lambda$$

となる.

種数 1 のコンパクトリーマン面と 1 次元の複素トーラスとの間の解析的な対応は種数 1 の場合の Abel-Jacobi の定理の自然な帰結ではある. しかし, 本稿は楕円関数論を中心に展開されているため, 出発点は 1 次元の複素トーラスである. 以下ではこの 2 つの対象を同一視して考える.

2. 擬周期関数

この節では擬周期関数の構成を問題にする. 雛型は, 周期関数 $\sin z$ の満たす等式

$$\sin z = z \prod_{n=1}^{\infty} \Big(1 - \frac{z^2}{(n\pi)^2}\Big)$$

である.

*広島大学大学院理学研究科, E-mail : yamauchi@math.sci.hiroshima-u.ac.jp

重複もこめて同じ零点をもつ二つの整関数 ($\mathbb{C}$ 上の正則関数のこと) $f_1(z), f_2(z)$ の間には

$$f_1(z) = f_2(z)\exp(g(z))$$

なる関係がある (cf. [1], p.210, 定理 7). ここで, $g(z)$ は適当な $\mathbb{C}$ 上の正則関数である. いま, 整関数 $f(z)$ の零点の成す集合 Γ が加法群となるときを考える. 上の考察から,

$$f(z+\omega) = f(z)\exp(g_\omega(z)),\ \omega \in \Gamma$$

が成り立つ. ここで, $g_\omega(z)$ は ω に依存する整関数である.

以上が擬周期関数構成のアイデアである. 本節では, 先ず, Weierstrass の因数分解定理を復習した後で, σ 関数, Weierstrass zeta 関数, $\wp$ 関数を定義し, 諸性質をまとめ, σ 関数の擬周期性について述べる.

2-1. Weierstrass の因数分解定理

k を非負整数とする. $z = 0$ で k 位の零をもち, 重複も込めて $\mathbb{C}\backslash\{0\}$ の点 $a_1, \ldots, a_n$ で零を持つ整関数は,

$$\exp(g(z))z^k \prod_{j=1}^{n}\Big(1 - \frac{z}{a_j}\Big)$$

と表せる. しかし, 指定された無限個の点で零を持つ整関数を無限積を用いて同様に与えようとすると, 無限積の収束問題を考えなければならない.

命題 2.1 $\{a_n\}_{n=1}^{\infty}$ を $\mathbb{C}\backslash\{0\}$ の元からなる点列とし, 各 a_n に対して正の整数 k_n が与えられているものとする. このとき, 任意の正の数 r に対して,

$$\sum_{n=1}^{\infty} \frac{1}{k_n+1}\Big|\frac{r}{a_n}\Big|^{k_n+1}$$

が収束するならば,

$$\prod_{n=1}^{\infty}\Big(1 - \frac{z}{a_n}\Big)\exp\Big(\frac{z}{a_n} + \frac{1}{2}\Big(\frac{z}{a_n}\Big)^2 + \cdots + \frac{1}{k_n}\Big(\frac{z}{a_n}\Big)^{k_n}\Big)$$

は $\mathbb{C}$ において広義一様絶対収束する.

この命題より次の命題が従う.

命題 2.2 (Weierstrass の因数分解定理 (cf. [1], p.210, 定理 7)) k を非負整数とする. 各 n に対して定めた点 $a_n \in \mathbb{C}\backslash\{0\}$(ただし, $|a_n| \longrightarrow \infty (n \longrightarrow \infty)$ とする) を零点として持ち, $z = 0$ で k 位の零を持つ任意の整関数 $f(z)$ は

$$z^k\exp(g(z))\prod_{n=1}^{\infty}\Big(1 - \frac{z}{a_n}\Big)\exp\Big(\frac{z}{a_n} + \frac{1}{2}\Big(\frac{z}{a_n}\Big)^2 + \cdots + \frac{1}{k_n}\Big(\frac{z}{a_n}\Big)^{k_n}\Big)$$

という形にかける. ここで, k_n, 及び, $g(z)$ はそれぞれ $f(z)$ から定まる正の整数と整関数である.

Weierstrass の因数分解定理は与えられたデータを零に持つ整関数の存在問題とその具体的構成の問題に対する解答を同時に与える強力な定理である.

ここで, Weierstrass の因数分解定理の存在問題のみを層のコホモロジーで解釈してみる.

命題 2.2 で見たように, 与えられたデータ $\{a_n\}_{n=1}^{\infty} \subset \mathbb{C}$ を零に持つ整関数の存在問題はクザンの乗法的問題と呼ばれている問題の 1 次元版である.

$M = \mathbb{C}$ を一次元複素多様体として考える. M 上の局所的に零および極のどちらも持たない正則関数の成す層を $\mathcal{O}_M^*$, M 上の有理型関数の成す層を $\mathcal{K}_M$ と表すことにすると層の完全列

$$1 \longrightarrow \mathcal{O}_M^* \longrightarrow \mathcal{K}_M^* \longrightarrow \mathcal{K}_M^*/\mathcal{O}_M^* \longrightarrow 1$$

を得る.

これより, 長完全系列

$$0 \longrightarrow H^0(M, \mathcal{O}_M^*) \longrightarrow H^0(M, \mathcal{K}_M^*) \xrightarrow{\varphi} H^0(M, \mathcal{K}_M^*/\mathcal{O}_M^*) \xrightarrow{\delta} H^1(M, \mathcal{O}_M^*) \longrightarrow \cdots$$

を得る. 今, $H^1(M, \mathcal{O}_M^*) \simeq \mathrm{Pic}^0(M) = 0$ (cf. [3]) なので, φ は全射. $H^0(M, \mathcal{K}_M^*/\mathcal{O}_M^*)$ の元は M の開被覆 $\{U_i\}_{i\in I}$ と U_i 上の 0 でない有理型関数 f_i の組, $\{(U_i, f_i)\}_{i\in I}$ で張り合わせの条件

$$f_{i,j} := \frac{f_i}{f_j} \in \mathcal{O}_M^*(U_i \cap U_j)$$

を満たすものである. 実際, そのようなデータが与えられると, $(\mathcal{K}_M^*/\mathcal{O}_M^*)(U_i \cap U_j)$ においては

$$f_i = f_j$$

なので層の公理から大域切断 $F \in \mathcal{K}_M^*(M)$ が存在して, $F|U_i = g_i f_i \equiv f_i \bmod \mathcal{O}_M^*(U_i)$ が成り立つ. ここで, g_i は零も極も持たない U_i 上の正則関数. いま, 集積点を持たない $\mathbb{C}$ の点列 $\{a_n\}_n$ と正整数 k_n を与える. $\{a_n\}_n$ に対して, $\mathbb{C}$ の開被覆 $\{U_n\}_n$ を $a_\ell \in U_\ell$ かつ a_n, $a_m \notin U_n \cap U_m$ となるようにとる. 今,

$$f_n = \begin{cases} (1 - \dfrac{z}{a_n})^{k_n} & (a_n \neq 0\ ) \\ z^{k_n} & (a_n = 0) \end{cases}$$

とすると, データ $\{(U_n, f_n)\}_n$ は $H^0(M, \mathcal{K}_M^*/\mathcal{O}_M^*)$ の元を定める. よって, 前の考察から, 大域切断 F($\mathbb{C}$ 上の有理型関数) が存在して,

$$F|U_n = g_n \cdot f_n,\ g_n \in \mathcal{O}_M^*(U_n)$$

が成り立つ. F は各開集合上で正則な関数なので整関数である. このように, 層の立場からみると, 与えられた零点に関するデータをもつ整関数の “存在” の難しさは $H^1(M, \mathcal{O}_{\mathbb{C}}^*)$ の消滅に集約されていることがわかる.

Weierstrass の因数分解定理の存在問題 (クザンの第 1 問題) は $H^1(M, \mathcal{O}_{\mathbb{C}}^*)$ の消滅と同等であり, 互いの価値を高めている.

2-2. σ 関数

本節では σ 関数の定義を与える. その精神は命題 2.1 にある.
$\mathbb{C}$ の格子 Λ は $\mathbb{R}$ 上一次独立な $\mathbb{C}$ の 2 元 ω_1, ω_2 によって,

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$$

と表せる. そこで, Weierstrass の σ 関数を

$$\sigma(z) := z \prod_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \Big(1 - \frac{z}{\omega}\Big) \exp\Big(\frac{z}{\omega} + \frac{1}{2}\Big(\frac{z}{\omega}\Big)^2\Big)$$

により定義する. 任意の正の実数 r に対して, 級数

$$\sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \frac{1}{3} \cdot \Big|\frac{r}{\omega}\Big|^3$$

が収束することから命題 2.1 より, 右辺は整関数となる[1]. さらに, σ 関数は次の性質を持つ.

命題 2.3 (1) σ 関数は Λ の各点において 1 位の零点を持ち, それ以外では零にならない.
(2) σ 関数は奇関数である. すなわち, $\sigma(-z) = -\sigma(z)$

命題 2.3 の (1) より, 任意の Λ の元 ω に対し, $\sigma(z+\omega)$ と $\sigma(z)$ との零点集合は一致するので, ある正則関数 $g_\omega(z)$ が存在して,

$$\sigma(z+\omega) = \exp(g_\omega(z))\sigma(z)$$

が成り立つ. 本節の後半でこの $g_\omega(z)$ を具体的に求める.

σ 関数が周期にも依存していることを強調するために,

$$\sigma(z; \omega_1, \omega_2)$$

とあらわことにすると次が成り立つ.

命題 2.4 σ は周期に関して, $\mathrm{GL}_2(\mathbb{Z})$ 不変である. すなわち,

$$\sigma(z; a\omega_1 + b\omega_2, c\omega_1 + d\omega_2) = \sigma(z; \omega_1, \omega_2), \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$$

(証明) $\mathrm{Aut}_{\mathbb{Z}}(\Lambda) = \mathrm{GL}_2(\mathbb{Z})$ より明らか.

---

[1] 一般に級数 $\sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \Big|\frac{1}{\omega}\Big|^k$ は $k \leq 2$ なら発散し, $k > 2$ なら収束する (cf. [7], 第二章).

この命題は本稿の内容からは独立しているが, σ 関数を特徴付けるための大事な要素である ([5] の補題 4.12).

2-3. ζ 関数

以下, 記号は 2-2 のものと同じものを使う.

Weierstrass の ζ 関数を

$$\zeta(z) := \frac{d}{dz}\log\,\sigma(z) = \frac{\sigma'(z)}{\sigma(z)}$$

により定義する. 対数微分をとっているので log の分枝のとり方によらない. $\zeta(z)$ は $\sigma(z)$ の零点 (つまり, Λ の元) 以外のところで正則な関数となる. また,

$$\zeta(z) = \frac{1}{z} + \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}}\Big(\frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2}\Big)$$

が成立する. さらに, ζ 関数は次の性質を持つ.

命題 2.5 (1) ζ 関数は Λ の各点において 1 位の極を持ち, それ以外では正則な有理型関数である.

(2) ζ 関数は奇関数である.

(3) $z=0$ の周りにおいて, $\zeta(z) = \dfrac{1}{z} - \displaystyle\sum_{n=1}^{\infty} G_{2n+2}z^{2n+1}$ が成立する. ただし, $G_n := \displaystyle\sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}}\frac{1}{\omega^n}$.

(4) $z=0$ の周りにおいて, $\sigma(z) = z - \dfrac{G_4}{4}z^5 - \dfrac{G_6}{6}z^7 + \Big(\dfrac{G_4^2}{32} - \dfrac{G_8}{8}\Big)z^9 + \Big(\dfrac{G_4G_6}{24} - \dfrac{G_{10}}{10}\Big)z^{11} + \cdots$.

(証明) (1), (2) は明らか. (3) は次の等式

$$\begin{aligned}\frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2} &= \frac{-1}{\omega}\Big(1 + \Big(\frac{z}{\omega}\Big) + \Big(\frac{z}{\omega}\Big)^2 + \cdots\Big) + \frac{1}{\omega} + \frac{z}{\omega^2}\\ &= -\Big(\frac{z^2}{\omega^3}\Big) - \Big(\frac{z^3}{\omega^4}\Big) - \cdots\end{aligned}$$

及び, $G_{2n+1}=0$, $n\geq 1$ となることを使えばよい.

(4) は (3) の式を積分して exp をとればよい.

2-4. $\wp$ 関数

Weierstrass の $\wp$ 関数を

$$\wp(z) := -\frac{d}{dz}\zeta(z)$$

により定義する. $\wp(z)$ も $\sigma(z)$ の零点 (つまり, Λ の元) 以外のところで正則な関数となる. また,

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}}\Big(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\Big)$$

が成立する. さらに, $\wp(z)$, 及び, その 1 階微分 $\wp'(z) = \sum_{\omega\in\Lambda} \frac{-2}{(z-\omega)^3}$ は次の性質を持つ.

命題 2.6 (1) $\wp$ 関数は Λ の各点において 2 位の極を持ち, それ以外では正則な有理型関数である.
(2) $\wp$ 関数は偶関数, $\wp'(z)$ は奇関数である.
(3) $z = 0$ の周りにおいて, $\wp(z), \wp'(z)$ はそれぞれ次の様に展開される.

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)G_{2n+2}z^{2n},\ \wp'(z) = \frac{-2}{z^3} + \sum_{n=1}^{\infty} 2n(2n+1)G_{2n+2}z^{2n-1}$$

が成立する.

定義 2.7 $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ に周期をもつ有理型関数 $f(z)$ のことを**楕円関数**という. すなわち,

$$f(z+\omega) = f(z),\ \omega \in \Lambda.$$

命題 2.8 $\frac{d^n}{dz^n}\wp(z),\ n \geq 0$ は楕円関数である.

(証明) $\wp'(z) = \sum_{\omega\in\Lambda} \frac{-2}{(z-\omega)^3}$ より, $\wp'(z)$ は楕円関数, とくに, その高階微分も楕円関数.
各 Λ の $\mathbb{Z}$ 基底 $\omega_i, i = 1, 2$ に対して, 等式 $\wp'(z+\omega_i) = \wp'(z)$ の両辺を積分するとで

$$\wp(z+\omega_i) = \wp(z) + c_{\omega_i},\ c_{\omega_i} \in \mathbb{C}$$

をえる. ここで $z = -\frac{\omega_i}{2} \notin \Lambda$ は $\wp(z)$ の極ではないので, これを上の式に代入すると,

$$c_{\omega_i} = \wp(\frac{\omega_i}{2}) - \wp(-\frac{\omega_i}{2}).$$

$\wp(z)$ は偶関数より, $c_{\omega_i} = 0$. Λ は $\omega_i, (i = 1, 2)$ で $\mathbb{Z}$ 上生成されるので $\wp(z)$ は Λ を周期に持つ楕円関数である.

$\wp(z)$ とその微分の間には様々な関係式が成り立つ. 先ず, 最初に登場するのが次の関係式である.

命題 2.9 (1) $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$. ここで,

$$g_2 := 60G_4 = 60\sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \frac{1}{\omega^4},\quad g_3 := 140G_6 = 140\sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \frac{1}{\omega^6}.$$

(2) $\wp''(z) = 6\wp(z)^2 - \frac{1}{2}g_2$.

(証明) (1) の両辺の $z = 0$ でのローラン展開の主要部が命題 2.6 から具体的な計算で一致することがわかる. 周期関数であることから他の極における主要部も等しい. よって,

$\wp'(z)^2-(4\wp(z)^3-g_2\wp(z)-g_3)$ は極を持たない有界な楕円関数となるが, このような関数は Liouville の定理より, 定数関数 c になる. しかし、c は楕円関数より $c=0$. (2) は (1) の両辺を微分すればよい.

2-5. $\sigma(z)$ の擬周期性

Λ の元 ω を任意に固定する. $\wp(z)$ は楕円関数だから,

$$\wp(z+\omega)=\wp(z)$$

が成り立つ. これを積分すると, z によらない定数 η_ω が存在して,

$$\zeta(z+\omega)=\zeta(z)+\eta_\omega$$

が成り立つ.

$$\zeta(z+\omega+\omega')=\zeta(z+\omega)+\eta_{\omega'}=\zeta(z)+\eta_\omega+\eta_{\omega'}$$

が成り立つので, $\Lambda\longrightarrow\mathbb{C}:\omega\mapsto\eta_\omega$ は加法群としての準同型写像となる. また, 自然な同一視 $\Lambda\otimes_{\mathbb{Z}}\mathbb{R}\simeq\mathbb{C}$ より, 上の準同型は $\mathbb{C}$ から $\mathbb{C}$ への $\mathbb{R}$ 線型写像に拡張される.

命題 2.10 (Legendre の関係式) $\mathrm{Im}(\frac{\omega_2}{\omega_1})>0$ と仮定する. このとき, 次の関係式が成り立つ. $\omega_2\eta_{\omega_1}-\omega_1\eta_{\omega_2}=2\pi\sqrt{-1}$.

(証明) $\mathbb{C}/\Lambda$ の基本領域 D を境界が Λ と交わらないようにとる. D の内部には $\zeta(z)$ の極が丁度 1 つあり, その留数は 1 である. D の頂点はある $t\in\mathbb{C}\backslash\Lambda$ によって, $t, t+\omega_1, t+\omega_1+\omega_2, t+\omega_2$ となる. この順番に沿って $\zeta(z)$ を積分すると, 留数定理より,

$$\int_t^{t+\omega_1}\zeta(z)dz+\int_{t+\omega_1}^{t+\omega_1+\omega_2}\zeta(z)dz+\int_{t+\omega_1+\omega_2}^{t+\omega_2}\zeta(z)dz+\int_{t+\omega_2}^{t}\zeta(z)dz=2\pi\sqrt{-1}.$$

左辺の 2,3 番目の積分において, $z\longrightarrow z+w_i,(i=1,2)$ と変数変換することで

$$\int_t^{t+\omega_1}(\zeta(z)-\zeta(z+\omega_2))dz+\int_t^{t+\omega_2}(\zeta(z+\omega_2)-\zeta(z))dz=-\eta_{\omega_2}\omega_1+\eta_{\omega_1}\omega_2$$

となる.

例 2.11 (1) $\Lambda=\mathbb{Z}+\mathbb{Z}\sqrt{-1}$ のとき, $\zeta(\sqrt{-1}z)=\dfrac{\zeta(z)}{\sqrt{-1}}$ より, $\eta_{\sqrt{-1}}=\dfrac{\eta_1}{\sqrt{-1}}$. 従って, 命題 2.10 より, $\eta_1=\pi$ を得る.
(2) $\Lambda=\mathbb{Z}+\mathbb{Z}\zeta_3$, $\zeta_3=\frac{-1+\sqrt{-3}}{2}$ のとき, $\zeta(\zeta_3 z)=\dfrac{\zeta(z)}{\zeta_3}$ より, $\eta_{\zeta_3}=\dfrac{\eta_1}{\zeta_3}$. 従って, 命題 2.10 より, $\eta_1=\frac{2\pi}{\sqrt{3}}$ を得る.
(3) $\Lambda=\mathbb{Z}+\mathbb{Z}\alpha$ が虚 2 次体の整数環のとき, η_1,η_α はどんな値になるか?

定義 2.12 (theta 関数[2]) 整関数 $f(z)$ が Λ に関する **theta 関数**であるとは

$$f(z+\omega) = \exp(2\pi\sqrt{-1}(L(\omega, z) + c_\omega))f(z)$$

を満たすことをいう. ここで, $L(\omega, z)$ は z に関して $\mathbb{C}$-線型, ω に関して $\mathbb{R}$-線型な関数, c_ω は ω にのみよる定数.

命題 2.13. $\sigma(z)$ は theta 関数である. とくに,

$$\sigma(z+\omega) = \psi(\omega)\exp(\eta_\omega(z+\frac{\omega}{2}))\sigma(z)$$

が成り立つ. ただし,

$$\psi(\omega) = \begin{cases} 1 & (\frac{\omega}{2} \in \Lambda\ ) \\ -1 & (\frac{\omega}{2} \notin \Lambda) \end{cases}$$

とおく.

(証明) 定義より, $\zeta(z) = \dfrac{d}{dz}\log\ \sigma(z)$ だから, 等式

$$\zeta(z+\omega) = \zeta(z) + \eta_\omega$$

を積分して,

$$\log\ \sigma(z+\omega) - \log\ \sigma(z) = \eta_\omega z + c_\omega$$

が $2\pi\sqrt{-1}$ の整数倍の差を除いて成り立つ. この曖昧さは両辺の exp をとることで解消される. つまり,

$$\frac{\sigma(z+\omega)}{\sigma(z)} = \exp(\eta_\omega z + c_\omega)$$

をえる. 便宜上,

$$\frac{\sigma(z+\omega)}{\sigma(z)} = \psi(\omega)\exp(\eta_\omega(z+\frac{\omega}{2}))$$

とあらわし, $\psi(\omega)$ を求める.

$\dfrac{\omega}{2} \notin \Lambda$ のとき, $z = -\dfrac{\omega}{2}$ を代入すると $\sigma(z)$ は奇関数より,

$$\psi(\omega) = -1.$$

一方で,

$$\frac{\sigma(z+2\omega)}{\sigma(z)} = \frac{\sigma(z+2\omega)}{\sigma(z+\omega)}\frac{\sigma(z+\omega)}{\sigma(z)}$$

より,

$$\psi(2\omega) = \psi(\omega)^2.$$

特に, $\dfrac{\omega}{2^n} \in \Lambda$, $\dfrac{\omega}{2^{n+1}} \notin \Lambda$ のとき,

$$\psi(\omega) = \psi(\frac{\omega}{2})^2 = \cdots = \psi(\frac{\omega}{2^{n+1}})^{2^{n+1}} = (-1)^{2^{n+1}} = 1$$

[2] [2] の第 5 章, 参照

をえる.

明らかに, $L(\omega,z):=\dfrac{1}{2\pi\sqrt{-1}}\eta_\omega z$ は z に関して $\mathbb{C}$-線型, ω に関して $\mathbb{R}$-線型 (に拡張可能) である. また, $c_\omega:=\dfrac{1}{2\pi\sqrt{-1}}\eta_\omega\dfrac{\omega}{2}$ は ω にしかよらない定数である.

命題 2.14 $L(\omega,z)$ は上記のように $\mathbb{C}\times\mathbb{C}$ 上に拡張しておく. $E(x,y)=L(x,y)-L(y,x)$ とおく. このとき, E は $\mathbb{C}\times\mathbb{C}$ 上の $\mathbb{R}$-双線型交代形式であり, $E(\omega_1,\omega_2)=1$ が成り立つ. 特に, $E(\Lambda,\Lambda)\subset\mathbb{Z}$ である.

(証明) $x=a_1\omega_1+a_2\omega_2,\ y=b_1\omega_1+b_2\omega_2, a_i,b_i\in\mathbb{R}\ (i=1,2)$ とおく.

$$E(x,y)=\frac{1}{2\pi\sqrt{-1}}(a_1b_2-a_2b_1)(\omega_2\eta_{\omega_1}-\omega_1\eta_{\omega_2})=(a_1b_2-a_2b_1)=(a_1,a_2)\begin{pmatrix}0&1\\-1&0\end{pmatrix}{}^t(b_1,b_2)$$

より主張は明らか. ただし, 途中の計算で命題 2.10 を用いた.

命題 2.15 $E(x,y)$ は Riemann 形式である. すなわち, $E(x,iy)$ は半正値対称形式である.

(証明) $L(x,y)$ は y に関して $\mathbb{C}$-線形だったので, $L(x,\sqrt{-1}y)=\sqrt{-1}L(x,y)$. また, 命題 2.14 より $E(x,y)$ は常に実数値をとるので,

$$E(x,\sqrt{-1}y)=\mathrm{Re}(L(x,\sqrt{-1}y))-\mathrm{Re}(L(\sqrt{-1}y,x))=-\mathrm{Im}(L(x,y))-\mathrm{Im}(L(\sqrt{-1}x,\sqrt{-1}y))$$

また, $0=\mathrm{Im}(E(x,y))=\mathrm{Im}(L(x,y))-\mathrm{Im}(L(y,x))$ であることから, $(x,y)\mapsto E(x,\sqrt{-1}y)$ は対称であることがわかる.

次に半正値であることを示す ($E(z,\sqrt{-1}z)\geq 0$ を示す).

$$h(z):=\sigma(z)\exp(-\frac{\pi}{2}E(z,\sqrt{-1}z))$$

とおくと,

$$L(\omega,z)=\frac{1}{2}(E(\omega,z)-\sqrt{-1}E(\omega,\sqrt{-1}z)),\ L(\omega,\omega)=\frac{-\sqrt{-1}}{2}E(\omega,\sqrt{-1}\omega),$$

および, E の対称性より,

$$h(z+\omega)=h(z)\psi(\omega)\exp(\sqrt{-1}\pi E(\omega,z))$$

を得る. $E(\omega,z)$ は実数なので,

$$|h(z)|=|h(z+\omega)|$$

したがって, $h(z)$ は有界である. その上界を M とすると,

$$|\sigma(z)|\leq M\exp(\frac{\pi}{2}E(z,\sqrt{-1}z))$$

を得る. いま, $E(z_0,\sqrt{-1}z_0)<0$ なる $z_0\in\mathbb{C}\backslash\{0\}$ が存在したと仮定する. 上の不等式に $z=x+yz_0,\ x,y\in\mathbb{C}$ を代入すると,

$$|\sigma(z)|\leq M\exp(\frac{\pi}{2}(E(x,\sqrt{-1}x)+2\mathrm{Re}\,y(E(z_0,\sqrt{-1}x)+\sqrt{-1}E(z_0,x))+|y|^2E(z_0,\sqrt{-1}z_0)))$$

$|y| \longrightarrow \infty$ とすると, 左辺は 0 に近づくから, $\sigma(z)$ が有界関数となり矛盾.

よって,

$$E(z, \sqrt{-1}z) \geq 0.$$

3. Abel-Jacobi Theorem

本節では, いくつかの準備のあとに種数 1 のコンパクト リーマン面 (複素代数曲線) に対する Abel-Jacobi Theorem を証明する.

先ず, 与えられた零点と極をもつ周期関数の構成を問題とする. アイデアは σ 関数の平行移動 $\sigma(z-a)$ の積や商を用いることである. まず, これがいつ楕円関数になるのか調べる. $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m \in \mathbb{C}$ を互いに異なるようにとる. また, 各 α_i, および, 各 β_j に対して, 正の整数 k_i, ℓ_j をそれぞれ適当に定める. このとき,

$$f(z) := \prod_{i=1}^{n} \sigma(z-\alpha_i)^{k_i} \prod_{j=1}^{m} \sigma(z-\beta_j)^{-\ell_j}$$

は $\alpha_i + \Lambda$ $(i = 1, \ldots, n)$ の各元で k_i 位の零点を持ち, $\beta_j + \Lambda$ $(j = 1, \ldots, m)$ の各元で ℓ_j 位の極を持つ. 命題 2.13 の σ 関数の変換公式より, $\omega \in \Lambda$

$$f(z+\omega) = \frac{\prod_{i=1}^{n} \psi(\omega)^{k_i} \exp(\eta_\omega(z-\alpha_i+\frac{\omega}{2}))^{k_i} \sigma(z-\alpha_i)^{k_i}}{\prod_{j=1}^{m} \psi(\omega)^{\ell_j} \exp(\eta_\omega(z-\beta_j+\frac{\omega}{2}))^{\ell_j} \sigma(z-\beta_j)^{\ell_j}}$$

$$= (\psi(\omega)\exp(\eta_\omega(z+\frac{\omega}{2})))^{\sum_{i=1}^{n} k_i - \sum_{j=1}^{m} \ell_j} \exp(\eta_\omega(\sum_{i=1}^{n} k_i\alpha_i - \sum_{j=1}^{m} \ell_j\beta_j)) f(z)$$

したがって, $f(z)$ が楕円関数になるためには,

$$\textstyle\sum_{i=1}^{n} k_i = \sum_{j=1}^{m} \ell_j \text{ かつ } \eta_\omega(\sum_{i=1}^{n} k_i\alpha_i - \sum_{j=1}^{m} \ell_j\beta_j) \in 2\pi\sqrt{-1}\mathbb{Z}$$

が必要条件である. 後者の条件と, 命題 2.10 より,

$$\sum_{i=1}^{n} k_i\alpha_i - \sum_{j=1}^{m} \ell_j\beta_j \in \Lambda$$

が従う. 以下では, 逆に与えられた楕円関数はこのような形に書けることをみていく.

3-1. Liouville の定理

$\mathbb{C}/\Lambda$ の基本領域を D とし, $f(z)$ を Λ を周期にもつ楕円関数とする. $f(z)$ は D の境界で極は持たないと仮定する[3].

[3] $f(z)$ は有理型関数なので D 内に高々有限個の極しか持たない. 従って, 適当に D を取り替えればこの仮定はいつでも満たされる.

命題 3.1 次が成り立つ.

(1) $\displaystyle\int_{\partial D} f(z)dz = 0$, とくに, 1 位の楕円関数は存在しない.

(2) $\displaystyle\sum_{P\in D} \mathrm{ord}_P(f) = \frac{1}{2\pi\sqrt{-1}}\int_{\partial D}\frac{f'(z)}{f(z)}dz = 0.$

(3) $\displaystyle\sum_{P\in D} \mathrm{ord}_P(f)P = \frac{1}{2\pi\sqrt{-1}}\int_{\partial D}\frac{zf'(z)}{f(z)}dz \in \Lambda.$

(証明) (1) 前半は命題 2.10 を参照. 1 位の楕円関数が存在すると, その極における留数は 0 でない. しかし, これは楕円関数の留数の和が 0 であるという前半の事実に反する. (2) は偏角の原理. $\mathrm{Im}(\frac{\omega_2}{\omega_1})>0$ と仮定すると, (3) は $f(z)$ は楕円関数であることから,

$$\begin{aligned}\frac{1}{2\pi\sqrt{-1}}\int_{\partial D}\frac{zf'(z)}{f(z)}dz &= \frac{1}{2\pi\sqrt{-1}}\Big(\int_t^{t+\omega_1} + \int_{t+\omega_1}^{t+\omega_1+\omega_2} + \int_{t+\omega_1+\omega_2}^{t+\omega_2} + \int_{t+\omega_2}^{t}\Big)\frac{zf'(z)}{f(z)}dz\\ &= \frac{1}{2\pi\sqrt{-1}}\int_t^{t+\omega_1}\frac{(-\omega_2)f'(z)}{f(z)}dz + \frac{1}{2\pi\sqrt{-1}}\int_t^{t+\omega_2}\frac{\omega_1 f'(z)}{f(z)}dz\\ &= -\omega_2 m_1 + \omega_1 m_2 \in \Lambda.\end{aligned}$$

ここで, $m_i := \dfrac{1}{2\pi\sqrt{-1}}\displaystyle\int_t^{t+\omega_i}\frac{f'(z)}{f(z)}dz = \frac{1}{2\pi\sqrt{-1}}\int_t^{t+\omega_i} d\log f(z)$ は t から $t+\omega_i$ にいたる線分の $f(z)$ の像 ($f(t) = f(t+\omega_i)$ より閉曲線となる) が原点の周りを回転した数となる.

注意 3.2 命題「極を持たない楕円関数は定数である」と命題 3.1-(1),(2),(3) をあわせて, Liouville の基本定理という.

3-2. 楕円関数の σ 関数による表示

$\mathbb{C}(\Lambda)$ を周期 Λ をもつ楕円関数のなす集合する. 関数の通常の演算に関して, $\mathbb{C}(\Lambda)$ は体になるのでこれを**楕円関数体**と呼ぶ.

前節で σ 関数の積の適当な比は楕円関数となることをみたが, この逆が成立する. つまり,

命題 3.3. $\mathbb{C}(\Lambda) = \Big\{C\dfrac{\prod_{i=1}^n\sigma(z-\alpha_i)^{k_i}}{\prod_{j=1}^m\sigma(z-\beta_j)^{\ell_j}}\Big|\ C\in\mathbb{C},\ \displaystyle\sum_{i=1}^n k_i\alpha_i - \sum_{j=1}^m \ell_j\beta_j \in \Lambda,\ \sum_{i=1}^n k_i = \sum_{j=1}^m \ell_j\Big\}.$

(証明) 右辺が左辺に含まれることは明らか. $f(z)$ を楕円関数とし, $\mathbb{C}/\Lambda$ の基本領域 D の境界には $f(z)$ の零点も極も含まれないと仮定する. このとき, 命題 3.1-(2), (3) より, $f(z)$ の D の内部における重複度 k_i の零点 a_i と重複度 ℓ_j の極 b_j の間には

$$\sum_{i=1}^n k_i\alpha_i - \sum_{j=1}^m \ell_j\beta_j \in \Lambda,\ \sum_{i=1}^n k_i = \sum_{j=1}^m \ell_j$$

が成り立つ.

このとき,

$$f(z)\Big/\Big(\frac{\prod_{i=1}^n\sigma(z-\alpha_i)^{k_i}}{\prod_{j=1}^m\sigma(z-\beta_j)^{\ell_j}}\Big)$$

は極を持たない楕円関数となり, Liouville の定理より, 定数. 従って, $f(z)$ は右辺の元である.

軍司氏の講演によると, 種数 g のコンパクトリーマン面 X に対して,

$$0 \longrightarrow \mathrm{Div}^{\ell}(X) \longrightarrow \mathrm{Div}^{0}(X) \longrightarrow \mathrm{Jac}(X) \longrightarrow 0 \text{ (exact)}$$

を主張するのが, Abel-Jacobi Theorem であった. ただし, $\mathrm{Jac}(X) = \mathbb{C}^g/\Lambda$,

$$\Lambda := \left\{ \left(\int_\gamma \omega_1, \ldots, \int_\gamma \omega_g \right) \;\middle|\; \gamma \in H_1(X, \mathbb{Z}) \right\}$$

である. (ω_j) は正則 1 形式の成す空間 $H^0(X, \Omega_X)$ の基底である.

$g = 1$ のとき, つまり, 種数 1 のコンパクトリーマン面は $X = \mathbb{C}/\Lambda_X$ と表せるのであった (本稿第 1 章).

このとき, $H^0(X, \Omega_X) = \mathbb{C}dz$, $\left\{ \int_\gamma dz \middle|\ \gamma \in H_1(X, \mathbb{Z}) \right\} = \Lambda_X$ が成り立つ.

命題 3.4 ($g = 1$ の Abel-Jacobi Theorem). $X = \mathbb{C}/\Lambda_X$ の原点 O とする. このとき,

$$0 \longrightarrow \mathbb{C}(\Lambda)^* \longrightarrow \mathrm{Div}^{0}(X) \xrightarrow{\phi} \mathbb{C}/\Lambda_X \longrightarrow 0 \text{ (exact)}$$

が成り立つ. ただし, $\phi(P - O) = \displaystyle\int_O^P dz = P \bmod \Lambda_X$.

(証明) ϕ の全射性は明らか. X 上の有理型関数とは楕円関数 $f(z)$ のことである. 命題 3.1 および命題 3.3 より, $\mathrm{Div}^{\ell}(X) = \mathrm{Ker}(\phi)$ がわかる.

4. Riemann-Roch Theorem

$X = \mathbb{C}/\Lambda$ を種数 1 のコンパクトリーマン面とし, 原点を O とする. 本節では, $n \in \mathbb{Z}$ に対して, $\mathbb{C}$ ベクトル空間

$$\Gamma(X, \mathcal{O}(nO)) := \{ f(z) \in \mathbb{C}(\Lambda)^* \mid f(z) \text{ は } O \text{ においてのみ高々 } n \text{ 位の極をもつ}^4 \} \cup \{0\}$$

の次元を問題にする[5]. 3-2 より $\Gamma(X, \mathcal{O}(nO))$ の元は $\sigma(z)^n$ と同じ変換公式を満たす整関数の積を $\sigma(z)^n$ で割ったものとなる. 従って, $\sigma(z)^n$ と同じ変換公式を満たす整関数の張る空間の次元を調べればよいことになる.

$\sigma(z)^n$ の変換公式は, 変数変換 $z \mapsto z + 1$ で不変になるように $\sigma(z)$ を正規化し, $q = \exp(2\pi\sqrt{-1}z)$ とおいて, q-展開の係数の漸化式と捉えられる. この漸化式を用いると

$$\Gamma(X, \mathcal{O}(nO)) = n \ (n \geq 1)$$

が導かれる.

---

[4] $n<0$ のときは「少なくとも $-n$ 位の零点をもつ」となる.

[5] $\Gamma(X, \mathcal{O}(nO))$ は X 上の直線束 $\mathcal{O}(nO)$ の大域切断に他ならない (cf. [2]).

4-1. σ 関数の q-展開

この節を通じて, $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ $(\mathrm{Im}\tau > 0)$ と仮定する. 前の記号にあわせると, $\omega_1 = 1$, $\omega_2 = \tau$ である. $\sigma(z)$ の変数を正規化するために

$$\varphi(z) := \exp(-\eta_1 \frac{z^2}{2} + \pi\sqrt{-1}z)\sigma(z)$$

とおく.

命題 4.1 上記の $\varphi(z)$ に対して,

$$\varphi(z+1) = \varphi(z),\ \varphi(z+\tau) = -\frac{1}{q}\varphi(z)$$

が成り立つ. ただし, $q := \exp(2\pi\sqrt{-1}\tau)$ とおく.
(証明) (1) は命題 2.13 より明らか. (2) はさらに命題 2.10 を使えばよい.

命題 4.1 より, $r \geq 1$ に対して, $\varphi(z)^r$ は変数変換 $z \mapsto z+1$ で不変だから q-展開可能である. つまり,

$$\varphi(z)^r = \sum_{n\in\mathbb{Z}} A_n h^n,\ h = \exp(2\pi\sqrt{-1}z)$$

とあらわせる. これがさらに, $\varphi(z+\tau)^r = (-\frac{1}{q})^r\varphi(z)^r$ を満たすための必要十分条件は,

$$\sum_{n\in\mathbb{Z}} A_n q^n h^n = \sum_{n\in\mathbb{Z}} (-1)^r A_n h^{n-r}$$

次数が同じところで係数を比較して

$$A_n q^n = (-1)^r A_{n+r}$$

をえる. つまり, r 個の係数 $A_1, \ldots, A_r$ を決めれば, 残りの係数は自動的に定まるので, $\mathbb{C}$-線型空間

$$\left\langle \varphi(z) : \text{整関数} \,\middle|\, \varphi(z+1) = \varphi(z),\ \varphi(z+\tau) = (-\frac{1}{q})^r\varphi(z) \right\rangle$$

の次元は r となる[6].

命題 4.2

$$\dim_{\mathbb{C}}\Gamma(X, \mathcal{O}(rO)) = \begin{cases} r & (r \geq 1\ ) \\ 1 & (r = 0) \\ 0 & (r < 0) \end{cases}$$

[6]逆に, そのような係数 $\{A_n\}_n$ から構成された級数 $\sum_n A_n h^n$ は全平面で収束し, 上記線型空間の元となる.

(証明) r <0 のときは正則かつ O で少なくとも $-r$ 位の零点を持つもつ楕円関数は存在しないので次元は 0. $r=0$ のときは正則な楕円関数は定数のみなので次元は 1.

$r \geq 1$ のとき, 次の $\mathbb{C}$-線型写像

$$\Gamma(X, \mathcal{O}(rO)) \longrightarrow \left\langle \varphi(z) : \text{整関数} \;\middle|\; \varphi(z+1)=\varphi(z),\ \varphi(z+\tau)=(-\frac{1}{q})^r\varphi(z) \right\rangle$$

$$f(z) \mapsto \exp(-\eta_1\frac{z^2}{2}+\pi\sqrt{-1}z)^r\sigma(z)^r f(z)$$

を考えると, 明らかに, この写像は同型となるので次元は r.

命題 4.3 任意の X の点 $P_1, \ldots, P_n$ と正整数 $r_1, \ldots, r_n$ に対して, $D=\sum_{i=1}^{n} r_iP_i \in \mathrm{Div}(X)$ とおく. D に対して,

$$\Gamma(X, \mathcal{O}(D)) = \{f(z) \in \mathbb{C}(\Lambda) \mid f(z) \text{ は各 } P_i\ (i=1,\ldots,n) \text{ において高々} r_i \text{ 位の極をもつ}\}$$

とおく. このとき,

$$\dim_{\mathbb{C}}\Gamma(X, \mathcal{O}(rO)) = \deg(D) = \sum_{i=1}^{n} r_i$$

(証明) 次の $\mathbb{C}$-線型写像の同型

$$\Gamma(X, \mathcal{O}(D)) \longrightarrow \left\langle \varphi(z) : \text{整関数} \;\middle|\; \varphi(z+1)=\varphi(z),\ \varphi(z+\tau)=(-\frac{1}{q})^{\sum_{i=1}^{n} r_i}\varphi(z) \right\rangle$$

$$f(z) \mapsto \prod_{i=1}^{n} \sigma(z-P_i)^{r_i} f(z)$$

を考えればよい.

周期 Λ を持つ楕円関数は $X=\mathbb{C}/\Lambda$ 上の有理型関数とみなすことができる.

命題 4.4 (1) $\Gamma(X, \mathcal{O}(nO)) = \langle \wp(z)^m |\ 0 \leq m \leq \frac{n}{2} \rangle \oplus \langle \wp(z)^m\wp'(z) |\ 0 \leq m \leq \frac{n-3}{2} \rangle$
(2) $\bigoplus_{n\geq 0} \Gamma(X, \mathcal{O}(nO)) = \mathbb{C}[\wp(z), \wp'(z)]$
(3) $\mathbb{C}(\Lambda) = \mathbb{C}(\wp(z), \wp'(z))$
(証明) (1) は命題 2.6, 命題 4.2 より従う. (2) は左辺が右辺に含まれることを示す際に命題 2.9-(1) を使えばよい. (3) $\mathbb{C}(\Lambda)$ は $\mathbb{C}[\wp(z), \wp'(z)]$ の商体である.

5. 楕円曲線の定義方程式

この節では種数 1 のコンパクトリーマン面 $\mathbb{C}/\Lambda$ の代数曲線として定義方程式および, 1 次元アーベル多様体としての群演算を求める.

4-1. 定義方程式

$E = \{(X : Y : Z) \in \mathbb{P}^2(\mathbb{C}) |\ Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3\}$ とおく. ただし, g_2, g_3 は命題 2.9-(1) において定義された定数である.

命題 5.1 E は非特異である. すなわち, $g_2^3 - 27g_3^2 \neq 0$.

(証明) $\wp'(z)$ は奇関数だから, $\frac{\omega_1}{2},\ \frac{\omega_2}{2},\ \frac{\omega_1+\omega_2}{2}$ は $\wp'(z)$ の零点となる. $\wp'(z)$ は 3 位の楕円関数なので, この 3 点を含む $\mathbb{C}/\Lambda$ の基本領域において, これらが丁度 $\wp'(z)$ の零点となる.

一方, 命題 2.9 より $\alpha = \frac{\omega_1}{2},\ \frac{\omega_2}{2},\ \frac{\omega_1+\omega_2}{2}$ に対して,

$$4\wp(\alpha)^3 - g_2\wp(\alpha) - g_3 = 0$$

また, $\wp(z)$ が 2 位の偶関数であることに注意すれば,

$$\wp(\frac{\omega_1}{2}),\ \wp(\frac{\omega_2}{2}),\ \wp(\frac{\omega_1+\omega_2}{2})$$

は互いに異なる. よって, 多項式 $4x^3 - g_2x - g_3$ の判別式は消えないので主張をえる.

命題 5.2 写像

$$\Phi : \mathbb{C}/\Lambda \longrightarrow E : z \mapsto (\wp(z) : \wp'(z) : 1)$$

は正則 (解析的) かつ全単射.

(証明) 先ず, 写像

$$\mathbb{C} \longrightarrow E : z \mapsto (\wp(z) : \wp'(z) : 1)$$

は $z \notin \Lambda$ において正則. $z = \omega \in \Lambda$ のとき, ω の除いた $z = \omega$ の近傍では

$$(\wp(z) : \wp'(z) : 1) = (\frac{\wp(z)}{\wp'(z)} : 1 : \frac{1}{\wp'(z)}) = (\frac{-1}{2}(z-\omega)g_1(z) : 1 : \frac{-1}{2}(z-\omega)^3g_2(z))$$

となるので $z = w$ に正則に拡張できる. ここで, $g_i(z), (i = 1, 2)$ は $z = \omega$ の近傍で正則な関数.

(全射性) $(a : b : c) \in E(\mathbb{C})$ をとる. $c = 0$ に対しては $z = 0$ が対応しているので, $c \neq 0$ の時を考える. $c = 1$ とする. $\wp(z) - a$ は 2 位の楕円関数より, 二つの零点 $\pm\alpha(\notin \Lambda)$ は零点の代表系である. 命題 2.9-(1) より, α に対して, $\wp'(\alpha)^2 = b^2$ である, もし, $\wp'(\alpha) = b$ なら $\Phi(\alpha) = (a : b : 1)$ であり, そうでなければ $\Phi(-\alpha) = (a : b : 1)$ である.

(単射性) 2 点 $z_1, z_2 \notin \Lambda$ に対して, $\wp(z_1) = \wp(z_2)$ ならば $z_1 = \pm z_2 + \omega,\ \omega \in \Lambda$ が成り立つことと, $\wp'(z)$ が奇関数であることを使えばよい.

各 $p \in \mathbb{C}/\Lambda$ に対して, 接空間の間の射 $d_p\Phi$ が消えないことが簡単に示せるので Φ は双正則である.

注意 5.3 命題 5.2 の逆写像は $E \longrightarrow \mathbb{C}/\Lambda : P \mapsto \displaystyle\int_{O_E}^{P} \frac{dx}{y}$ で与えられる. ただし, $O_E = (0:1:0)$.

5-2. 加法公式

定理 5.4 $\alpha, \beta, \alpha \pm \beta \notin \Lambda$ とする. このとき,

$$\wp(\alpha)+\wp(\beta)+\wp(\alpha+\beta) = \frac{1}{4}\Big(\frac{\wp'(\alpha)-\wp'(\beta)}{\wp(\alpha)-\wp(\beta)}\Big)^2,\ 2\wp(\alpha)+\wp(2\alpha) = \frac{1}{4}\Big(\frac{12\wp(\alpha)^2-g_2}{\wp'(\alpha)}\Big)^2$$

(証明) $f(z) = \wp'(z) - a\wp(z) - b$ が α, β を零点を持つように定める. すなわち,

$$a = \frac{\wp'(\alpha)-\wp'(\beta)}{\wp(\alpha)-\wp(\beta)},\ b = \frac{\wp'(\beta)\wp(\alpha)-\wp'(\alpha)\wp(\beta)}{\wp(\alpha)-\wp(\beta)}.$$

$f(z) = \dfrac{-2}{z^3} + \cdots$ は 3 位の楕円関数だから, α, β 以外にもう一つ零点 γ をもつ[7]. 命題 3.1-(3) より, $\alpha+\beta+\gamma \in \Lambda$. よって, 連立方程式

$$\begin{cases} \wp'(z) - a\wp(z) - b = 0 \\ \wp'(z)^2 - (4\wp(z)^3 - g_2\wp(z) - g_3) = 0 \end{cases}$$

において, $\wp'(z)$ を消去し, 解と係数の関係から

$$\wp(\alpha)+\wp(\beta)+\wp(\gamma) = \frac{1}{4}a^2$$

を得る. $\wp(\gamma) = \wp(-\alpha-\beta) = \wp(\alpha+\beta)$ より, 求める式を得る.

二つ目の公式は前の式の極限 $\beta \longrightarrow \alpha$ をとり, 命題 2.9-(2) を代入すればよい.

命題 5.5 命題 5.2 の双正則写像 Φ は群演算を保つ. すなわち,

$$\Phi(\alpha+\beta) = \Phi(\alpha) \oplus_E \Phi(\beta)$$

が成り立つ. ここで, $\oplus_E$ はアーベル多様体としての E の群演算.
(証明) 代数曲線として楕円曲線の代数的な演算, および, 定理 5.4 から従う.

注意 5.6 楕円曲線 E の群演算を完備化することで自然に形式群が定義される. $P = (X, X'), Q = (Y, Y')$ とし, $P \oplus_E Q$ の x-座標を $G(X,Y)$ とする. $G(X,Y)$ を $(X,Y) = (0,0)$ の周りで形式的に展開したものを $\widehat{G}(X,Y)$ とかく. $\widehat{G}(X,Y)$ は $\mathbb{Z}[g_2, g_3, \frac{1}{2}][[X,Y]]$ の元となる. このとき,

$$F(X,Y) = -\widehat{G}(X,Y) = X + Y + \cdots$$

は E の形式群となる (cf. 西来路氏の講演).

[7] α, β, γ は同一の基本領域に入っていると仮定してよい.

参考文献

[1] L.V. Ahlfors, 複素解析 (笠原乾吉 訳), 現代数学社

[2] 軍司 圭一, Abel-Jacobi の定理 I, 本報告集

[3] R. Hartshone, Algebraic Geometry, GTM.

[4] F. Klein, クライン 19 世紀の数学, 彌永昌吉 監修, 共立出版株式会社

[5] 大西 良博, 超楕円函数論, 本報告集

[6] 上野健爾 他, 数学史 II, 岩波書店

[7] 梅村 浩, 楕円関数論, 楕円曲線の解析学, 東京大学出版会

[8] 吉富賢太郎, Riemann 面, 代数曲線, 函数体の対応, 本報告集

第 15 回 整数論サマースクール 報告集, pp.131-176

超 楕 円 函 数 論

大西 良博*

序 文

今日では楕円曲線を扱つた書物が数多く出版されてゐて, そのほとんどが楕円函数にも触れてゐるので, 楕円函数を学ぶのに不自由はないと思はれる.

一方, 種数の高い代数曲線に付随する Abel 函数については, 抽象論 (Abel 函数といふ言葉さへ登場しない) を展開した書物や論文はあるものの, この方面の具体的な記述に触れるのは困難に感じられる. 筆者は, 永らく, 例へば 竹内端三著, 「楕圓函數論」 (岩波全書) の様に, 実際の計算に耐へる様な記述をしたものが見当たらないことに不満を抱いてゐた. その希望に最も近いものは D.Mumford: Tata lectures on theta II, Birkhäuser ([Mu2]) であつた. しかしその後, Cambridge 大学の H.F.Baker がおよそ 1 世紀前にこの方面に多大な貢献をしてゐること, 中でも, 一般の Abel 函数を極めて具体的に扱つた大著 Abelian Functions (1897, Cambridge Univ. Press) と種数 2 の場合を詳述した Introduction to Multiply Periodic Functions (1907, Cambridge Univ. Press) が書かれてゐたことを知つてからは, この方面の研究に没頭してきた.

本稿は超楕円函数の基礎理論を H.F.Baker らによる優れた定式化にしたがつて解説したものである.

この記事では, 主として超楕円函数の一般論を展開する. 必要な基礎事項については, 随時, 本報告集収録の解説 [Y], [Og], [Gu], [OU] を引用することが望ましいが, その様に稿をまとめるため (記号等の整理) の時間的な制約から, 必要な事項はすべてこの記事の内部でも述べることとにした. 時間の許す範囲で, 本報告集の解説の参照すべき箇所を記したが, 完全さからは程遠い. しかし, ほとんどのことがらに実際にこの報告集に述べられてゐるはずであるので, 証明については必要に応じてこれらの解説をご参照いただきたい.

本稿で述べる Abel 函数論は, 超楕円曲線以外の代数曲線に対しても, 無限遠点が 1 点だけ ((n,s)-curves) であれば, 同様に一般化される. その基本的な定式化は本稿に述べたものと同様であるが, それは現在, 進展中のことがらでもあり, ここに取り入れない. 文献をいくつかあげておくので, それを辿つて最新の成果に踏み込んでいただけたることを望む.

*岩手大学 人文社会科学部

1 Riemann 面の一般論から

1.1 Riemann 面と Abel 微分

以下では Riemann 面について必要な事柄を整理することから始める.

第 1 種微分形式, 周期行列

種数 g の境界のない Riemann 面 X を考える. 1 点 I を固定し, 図 1.2 の様に交点数が $\alpha_i \cdot \alpha_j = \delta_{ij}$, $\alpha_i \cdot \beta_j = 0$, $\beta_i \cdot \beta_j = \delta_{ij}$ で, そのどれもが I を始点にして再び I に戻る様な路

$$\alpha_1, \cdots, \alpha_g, \beta_1, \cdots, \beta_g \tag{1.1}$$

をとり, これらに沿って X を切り開いてできる "多角形" $X_\circ$ をとする.

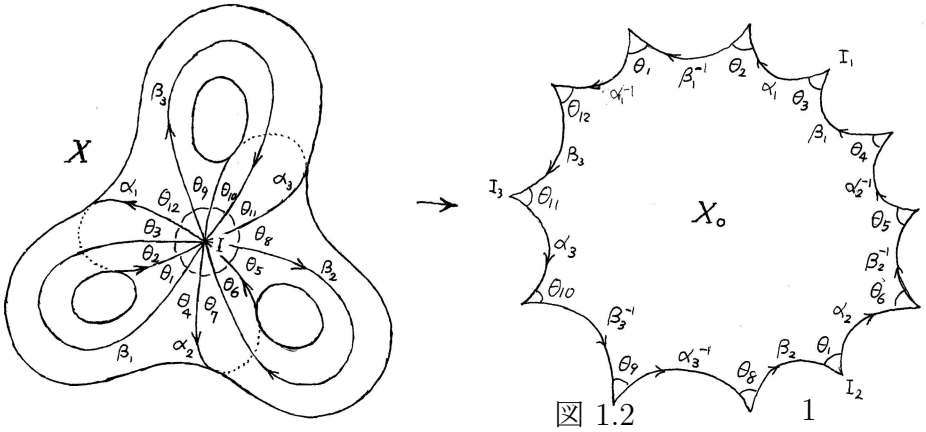


図 1.2 1

このとき $X_\circ$ の各辺を各 α_j と β_j に因み,

$$\alpha_1,\ \beta_1,\ {\alpha_1}^{-1},\ {\beta_1}^{-1},\ \cdots,\ \alpha_g,\ \beta_g,\ {\alpha_g}^{-1},\ {\beta_g}^{-1} \tag{1.3}$$

と記す. X 上の任意の閉曲線はいくつかの α_j, ${\alpha_j}^{-1}$, β_j, ${\beta_j}^{-1}$ をつないたものと homotope である.

Riemann 面上の有理型微分形式のことを単に **微分** または **微分形式** または **Abel 微分** と呼ぶ. Abel 微分の X 上での線積分を **Abel 積分** とよぶ.

命題 1.4 Riemann 面 X 上の微分の留数の和は 0 である.

証明 任意の微分 ω について

$$\begin{aligned} \text{"留数の和"} &= \frac{1}{2\pi i}\int_{\partial X_\circ} \omega \\ &= \frac{1}{2\pi i}\sum_{j=1}^{g}\left(\int_{\alpha_j}\omega + \int_{\beta_j}\omega + \int_{\alpha_j^{-1}}\omega + \int_{\beta_j^{-1}}\omega\right) \\ &= \frac{1}{2\pi i}\sum_{j=1}^{g}\left(\int_{\alpha_j}\omega + \int_{\beta_j}\omega - \int_{\alpha_j}\omega - \int_{\beta_j}\omega\right) \\ &= 0 \end{aligned} \tag{1.5}$$

が成り立つ. □

もしこの逆が成立すれば, 事は単純なのであるが, 全くその様にはなつてゐない. 例へば, Weierstrass の空隙定理と呼ばれる定理がある ([Ku]). そこで, どの様な微分が存在するのかを調べたい.

定義 1.6 ([Ku], pp.116-117) $D_1, \cdots, D_m$ は X 上の互ひに共通部分を持たない有限個の局所円板とし, 各閉包 $\overline{D_j}$ の近傍の上に, 次の様な (多価) 実数値函数 s_j が定義されてゐるとする.

(i) s_j は D_j の有限個の点を除いて $\overline{D_j}$ の近傍で調和であり,

(ii) s_j は境界 ∂D_j の近傍で一価である.

このとき X 上の函数 U で

(a) u は $X - \bigcup_{j=1}^m U_j$ で一価調和であり,

(b) 各 $\overline{D_j}$ で一価調和

である様なものが存在するとき, U を, 与へられた**特異性 $\{D_j, s_j\}_{j=0}^m$ を持つ調和函数** (あるいは potential) といふ.

次の定理が基本的である.

補題 1.7 (存在定理) ([Ku], p.117) X 上に与へれた特異性 $\{D_j, s_j\}_{j=0}^m$ を持つ調和函数が存在するための必要十分条件は

$$\sum_{j=1}^{m} \int_{\partial D_j} {}^* ds_j = 0 \tag{1.8}$$

が成立することである. そして, もし存在すれば定数の差を除いて一意的である. ここに * は共役微分を取ることを示す.

証明 証明は [Ku] を参照されたい. Riemann はこれの証明を Dirichlet の原理により証明したが, その証明に関する経緯について [Kl], p.266 付近を読まれることをお勧めする. □

これの証明は解析的であるが, Weil ([Wei], p.43) がいふ様に, ここを認めれば, 以下はほぼ代数的な議論で進むことができる.

命題 1.9 Δ を X 上の局所開円板とする. P, Q を Δ 内の 2 点とするとき, X 上の微分形式 τ_{PQ} が存在し, P, Q 以外の点では正則で, P において留数 1 の 1 位の極, Q において留数 -1 の 1 位の極を持ち, さらに $\Re \int_{\partial\Delta} \tau_{\mathrm{PQ}} = 0$ となる. いま Δ 内で P と Q を結ぶ単連結な曲線を選び, それを γ と記すとき, X 上の任意の閉曲線 α に対して

$$\frac{1}{2\pi} \int_{\alpha} \Re\, \tau_{\mathrm{PQ}} = \gamma \cdot \alpha. \tag{1.10}$$

証明 Δ の局所変数 z を, Δ が $\{z \,\big|\, |z| < 1\}$ に対応する様に取り,

$$s(z) = \frac{1}{2\pi} \arg \frac{z - z(\mathrm{P})}{z - z(\mathrm{Q})} \tag{1.11}$$

とおくとき,

$$\int_{\partial\Delta} {}^*ds = -\frac{1}{2\pi}\int_{|z|=1} d\log\left|\frac{z-z(\mathrm{P})}{z-z(\mathrm{Q})}\right| = 0 \tag{1.12}$$

なので, 1.7 により, 特異性 $\{\Delta, s\}$ を持つ調和函数 $U_{\mathrm{P,Q}}$ が存在する. このとき, $\tau_{\mathrm{P,Q}} = i\,dU_{\mathrm{P,Q}} - {}^*dU_{\mathrm{P,Q}}$ とおくと, 可微分多様体における微分形式の性質から主張が導かれる. Weyl ([Wey], p.114) を参照されたい. □

命題 1.13 Riemann 面 X 上の正則な微分形式 (**第 1 種微分形式**ともよばれる) の空間の次元は g である.

証明 その様な空間の基底は次の様に作ればよい. X 上の閉曲線 α に対して, P_1, P_2, $\cdots$, P_n をその上に順に十分近接して取つた点列とし,

$$\omega_\alpha = \frac{1}{2\pi}\big(\tau_{\mathrm{P}_1\mathrm{P}_2} + \tau_{\mathrm{P}_2\mathrm{P}_3} + \cdots + \tau_{\mathrm{P}_n\mathrm{P}_1}\big) \tag{1.14}$$

とおく. ここで十分近接してゐるといふのは, すべての隣合つた 2 点の組が, それぞれ適当な局所円板に含まれることをいふ. このとき α は X の至るところ正則な微分形式である[1]. しかも (1.10) の後半の主張により, β が X 上の任意の閉曲線であれば

$$\int_\beta \Re\,\omega_\alpha = \beta\cdot\alpha \tag{1.15}$$

が成り立つ. そこで, 標準切断を与へる様な閉曲線の組を

$$\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_g,\ \beta_1,\ \beta_2,\ \cdots,\beta_g \tag{1.16}$$

として, これらに応じて $\omega_{\alpha_j}, \omega_{\beta_j}$ を作る. (これは $\mathrm{P}_1, \cdots, \mathrm{P}_n$ の取り方に依存する.) それらを単に

$$\omega_1,\ \omega_2,\ \cdots,\ \omega_{2g} \tag{1.17}$$

と書けば, これらが X 上の任意の第 1 種微分形式の空間を $\mathbb{R}$ 上張る. 実際 ω を X 上の任意の第 1 種微分形式として,

$$c_j = \int_{\alpha_j}\omega,\quad c_{g+j} = \int_{\beta_j}\omega \tag{1.18}$$

とすれば, 任意の閉曲線 β について

$$\Re\int_\beta\big(\omega - c_1\,\omega_1 - \cdots - c_{2g}\,\omega_{2g}\big) = 0 \tag{1.19}$$

となるから, 始点 I を固定して X 上の函数

$$\varphi(\mathrm{P}) = \Re\int_{\mathrm{I}}^{\mathrm{P}}\big(\omega - c_1\,\omega_1 - \cdots - c_{2g}\,\omega_{2g}\big) = 0 \tag{1.20}$$

[1] ここに de Rham の定理 (1-forms と 1-cocyles の対応) の原型が見られる.

が得られる. しかし, これは極を持たない調和函数なので定数である. よつて

$$\omega = c_1\,\omega_1 + \cdots + c_{2g}\,\omega_{2g} \tag{1.21}$$

である. さらに (1.15) から $\omega_1, \cdots, \omega_{2g}$ が $\mathbb{R}$ 上 1 次独立であることもわかる. 次に, いま, 第 1 種微分形式の空間の $\mathbb{C}$ 上の次元が q であつたとして, その基底を (上の記号を忘れて) $\omega_1, \cdots, \omega_q$ とすれば

$$\omega_1,\ \cdots,\ \omega_q,\ \sqrt{-1}\,\omega_1,\ \cdots,\ \sqrt{-1}\,\omega_q \tag{1.22}$$

は $\mathbb{R}$ 上 1 次独立なので $2q \leqq 2g$. しかるに, 任意の第 1 種微分形式は $\omega_1, \cdots, \omega_q$ の $\mathbb{C}$ 上の 1 次結合で書けるから $2q \geqq 2g$. よつて $q = g$. 以上に関しては ([Ku], p.128, 定理 5.8; [Wey], pp.114-115 を参照されたい. ([I], p.90, 定理 2.15 も参照).

□

つぎの補題から Riemann-Roch の定理をはじめ, 以下のほとんどの定理が導かれる.

補題 1.23 $X_\circ$ において $\mathrm{P}_1, \cdots, \mathrm{P}_m$ および $\mathrm{Q}_1, \cdots, \mathrm{Q}_n$ を $\partial X_\circ$ 上にない点とせよ. η を高々 $\mathrm{P}_1, \cdots, \mathrm{P}_m$ において極をもつ微分, η' を同じく高々 $\mathrm{Q}_1, \cdots, \mathrm{Q}_n$ において極をもつ微分とし, 各点 P_i における局所径数 t_i に関する展開を

$$\eta = \sum_\nu a_\nu^{(i)} t_i^\nu dt_i, \quad \eta' = \sum_\nu {a'}_\nu^{(i)} t_i^\nu dt_i \tag{1.24}$$

とせよ. 同様に Q_j における局所径数 t'_j に関する展開を

$$\eta = \sum_\nu b_\nu^{(i)} {t'_i}^\nu dt_i, \quad \eta' = \sum_\nu {b'}_\nu^{(i)} {t'_i}^\nu dt_i \tag{1.25}$$

とすれば

$$\begin{aligned} &\frac{1}{2\pi i}\sum_{i=1}^{g}\left(\int_{\alpha_i}\eta\int_{\beta_i}\eta' - \int_{\beta_i}\eta\int_{\alpha_i}\eta'\right) \\ &\quad + \sum_{i=1}^{m}\left(a_{-1}^{(i)}\int_{\mathrm{I}_1}^{\mathrm{P}_i}\eta' + \sum_{\nu=0}^{\infty}\frac{a_{-\nu-2}^{(i)}{a'}_\nu^{(i)}}{\nu+1}\right) \\ &\quad + \sum_{j=1}^{n}\left(b_{-1}^{(j)}\int_{\mathrm{I}_1}^{\mathrm{Q}_i}\eta' + \sum_{\nu=0}^{\infty}\frac{a_{-\nu-2}^{(j)}{a'}_\nu^{(j)}}{\nu+1}\right) = 0 \end{aligned} \tag{1.26}$$

である.

証明[2] $X_\circ$ のなかで P_i と I_1 および Q_j と I_1 をどの 2 本も互いに交わらないような連続曲線 γ_i および ${\gamma'}_j$ で結び, P_i, Q_j を中心とした十分小さい円 ε_i, ${\varepsilon'}_j$ を描く. これらはすべて有向曲線と考えて逆の向きは γ^{-1} などと表すことにする. 証明は図のような積分路 $\gamma_i\varepsilon\gamma_i{}^{-1}$

[2][I], 第 5 章, p.252, 定理 5.5 による.

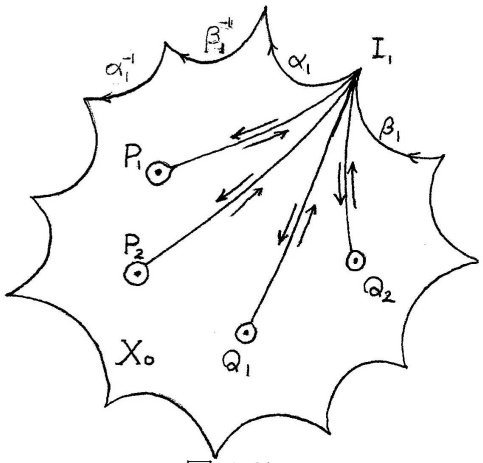


図 1.27

や ${\gamma'}_j\varepsilon{\gamma'}_j^{-1}$ と $\partial X_\circ$ を結んだ路に沿った $\eta d\eta'$ の積分を計算することで得られる: 命題 1.4 より

$$\begin{aligned}\int_{\partial X_\circ} &+\sum_{i=1}^{m}\left(\int_{\gamma_i}+\int_{{\gamma_i}^{-1}}+\lim\int_{\varepsilon_i}\right)\\ &+\sum_{j=1}^{n}\left(\int_{{\gamma'}_j}+\int_{{\gamma'}_j{}^{-1}}+\lim\int_{{\varepsilon'}_j}\right)=0.\end{aligned}\tag{1.28}$$

この左辺の各項が順に, 示すべき式の左辺の各項に対応する. □

補題 1.29 ω', ω を第 1 種微分とし, $w(\mathrm{P})=\int_{\mathrm{P}_0}^{\mathrm{P}}\omega$ とおくと,

$$\begin{aligned}&\sum_{j=1}^{g}\left(\int_{\alpha_j}\omega\int_{\beta_j}\omega'-\int_{\alpha_j}\omega'\int_{\beta_j}\omega\right)\left(=\int_{\partial X_\circ}w\omega'\right)=0,\\ &\sum_{j=1}^{g}\left(\int_{\alpha_j}\overline{\omega}\int_{\beta_j}\omega-\int_{\alpha_j}\omega\int_{\beta_j}\overline{\omega}\right)\geqq 0.\end{aligned}\tag{1.30}$$

ここで, 不等号の等号は $\omega=0$ のときのみ成り立つ.

証明 第 1 式. 補題 1.23 で $\eta=\omega_i$, $\eta'={\omega'}_j$ とおけば良い. 第 2 式は 1.23 と Stokes の定理:

$$\int_{\partial X_\circ}w\overline{\omega}=\int_{X_\circ}d(w\overline{\omega})=\int_{X_\circ}\omega\overline{\omega},\quad\left(w=w(P)=\int_{\infty}^{P}\omega\right)\tag{1.31}$$

から出る. 実際 $X_\circ$ を複素平面 (座標 $z=x+iy$) に埋め込んで $\omega=fdx+gdy$ とおけば, Cauchy-Riemann の関係式より $g=if$ なので, $\omega\overline{\omega}=-2i|f|dxdy$, したがって, $\int_{X_\circ}\omega\overline{\omega}\geq 0$ となるからである. □

X 上の正則な微分形式の空間の基底を $\omega_1, \cdots, \omega_g$ として, これらについて

$$\Omega' = \left[\int_{\alpha_j} \omega_i\right], \quad \Omega'' = \left[\int_{\beta_j} \omega_i\right], \quad \Omega = \begin{bmatrix}\Omega' & \Omega''\end{bmatrix} \tag{1.32}$$

とおき α_j, β_j での**周期行列**とよぶ. また X 上の閉曲線に関する Abel 積分を Abel 微分 ω の**周期**とよぶ. 補題 1.29 から次の補題が導かれる.

補題 1.33 第 1 種微分 ω について
(i) すべての $j = 1, \cdots, g$ について $\displaystyle\int_{\alpha_j} \omega = 0$,
(ii) すべての $j = 1, \cdots, g$ について $\displaystyle\int_{\beta_j} \omega = 0$,
(iii) すべての $j = 1, \cdots, g$ について $\displaystyle\int_{\alpha_j} \omega \in \mathbb{R}$ かつ $\displaystyle\int_{\beta_j} \omega \in \mathbb{R}$,
のうちいづれか一つでも成り立てば $\omega = 0$ である

証明 いづれも (1.30) の第 2 式からわかる. (主張 (i) は [OU], 1.3, Claim 1 の単射性に他ならない. そちらも参照されたい.) 同様の方法で, (ii), (iii) がわかる. □

系 1.34 Ω', Ω'' は正則行列である.

証明 いま $(c_1, \cdots, c_g)\Omega' = (0, \cdots, 0)$ とする. これは $\omega = \sum_i c_i\omega_i$ のすべての α_j に関する周期が 0 であることを意味するが, このとき 1.33 (i) により, $(c_1, \cdots, c_g) = (0, \cdots, 0)$ を得る. Ω'' についても 1.33 (ii) から同様に導ける. □

補題 1.35 任意に g 個の複素数 $z_1, \cdots, z_g$ が与へられたとき,

$$\int_{\alpha_j} \omega = z_j \quad (\text{for all } j = 1, \cdots, g) \tag{1.36}$$

となる第 1 種微分形式 ω が存在する.

証明 系 1.34 により, 写像 $\omega \longmapsto \int_{\alpha_j} \omega$ は 2 つの $\mathbb{C}$ 上の g 次元線形空間の同型であるからである. (この主張は [OU], 1.3, Claim 1 の全射性に他ならない. そこの証明も参照されたい.) □

補題 1.29 は次の様にも記述できる:

定理 1.37 (Riemann の関係式)
(1) $\Omega \begin{bmatrix} & 1_g \\ -1_g & \end{bmatrix} {}^t\Omega = O$
(2) $i\Omega \begin{bmatrix} & 1_g \\ -1_g & \end{bmatrix} {}^t\overline{\Omega}$ は正定値 Hermite 行列である.

$T = \Omega'^{-1}\Omega''$ とおくとき 1.37 の主張は ${}^tT = T$ かつ $\Im T$ は正定値行列であることに他ならない. いま, すぐ上でとった第 1 種微分形式の基底をとりかえて

$$ {}^t\begin{bmatrix}\hat{\omega}_1 & \cdots & \hat{\omega}_g\end{bmatrix} := \Omega'^{-1}{}^t\begin{bmatrix}\omega_1 & \cdots & \omega_g\end{bmatrix} \tag{1.38} $$

とおけば, $T = \Omega'^{-1}\Omega''$ であるから

$$ \left[\int_{\alpha_j}\hat{\omega}_i\right] = 1_g, \quad \left[\int_{\beta_j}\hat{\omega}_i\right] = T \tag{1.39} $$

となる. このような基底を本稿では

$$ \hat{\omega} = {}^t\begin{bmatrix}\hat{\omega}_1 & \cdots & \hat{\omega}_g\end{bmatrix} \tag{1.40} $$

の様に書く. これらを**正規化された**第 1 種微分形式の基底といふ. $\Omega = \begin{bmatrix}\Omega_1 & \Omega_2 & \cdots & \Omega_{2g}\end{bmatrix}$ と書くとき, $\Omega_1, \cdots, \Omega_{2g}$ は $\mathbb{R}$ 上 1 次独立であることが, 1.33 より容易にわかる. それゆゑ, $\Lambda = \mathbb{Z}\Omega_1 + \cdots + \mathbb{Z}\Omega_{2g}$ あるいは $\omega\hat{\Lambda} = \Omega'^{-1}\Lambda$ とおくとき, Λ, $\hat{\Lambda}$ はそれぞれ $\mathbb{C}^g$, $\Omega'^{-1}\mathbb{C}^g$ の 格子になつてゐる.

定義 1.41 上記の $\mathbb{C}^g/\Lambda$ や $\Omega'^{-1}\mathbb{C}^g/\hat{\Lambda}$ は X の **Jacobi 多様体** と呼ばれ, Abel 多様体といふ代数多様体の一種である. この note では第 1 種微分形式の基底を定めるごとに, それから得られる $\mathbb{C}^g/\Lambda$ の方を J と記して,

$$ J = \mathbb{C}^g/\Lambda \tag{1.42} $$

とし, 正規化された微分形式 $\hat{\omega}$ から得られる $\Omega'^{-1}\mathbb{C}^g/\hat{\Lambda}$ とは同一視しない.

1.1.1 第２種・第３種微分形式

ここで, 1.9 で述べた τ_{PQ} の再定義を込めて正規化された微分形式の定義をまとめておく.

定義 1.43 (1) 2 点 $\mathrm{Q}_1, \mathrm{Q}_2 \in X$ に対し $\tau_{\mathrm{Q}_1,\mathrm{Q}_2}$ を Q_1, Q_2 以外のすべての点において正則で, $\mathrm{ord}_{\mathrm{Q}_1}\tau_{\mathrm{Q}_1,\mathrm{Q}_2} = \mathrm{ord}_{\mathrm{Q}_2}\tau_{\mathrm{Q}_1,\mathrm{Q}_2} = -1$ かつ $\mathrm{Res}_{\mathrm{Q}_1}\tau_{\mathrm{Q}_1,\mathrm{Q}_2} = 1$, $\mathrm{Res}_{\mathrm{Q}_2}\tau_{\mathrm{Q}_1,\mathrm{Q}_2} = -1$ であり, すべての j について

$$ \int_{\alpha_j}\tau_{\mathrm{Q}_1,\mathrm{Q}_2} = 0 \tag{1.44} $$

となるような微分形式とする. ここで ord, Res はそれぞれ位数, 留数 ([I], p.139) をあらわす. このような微分形式を **正規化された第 3 種微分形式** とよぶ. このような微分形式は 1.7 と 1.35 より存在する ([I], p.110, 定理 2.26 を参照されたい → [Ku], pp.133–134). また, このような微分形式が 2 つあればその差は第 1 種微分形式であるから, 1.33(i) よりそれらは等しい. したがって上記条件のもとで一意的に定まる.

(2) $k \geq 2$ を与えられた自然数とする. 局所径数 t の与えられた点 $\mathrm{P} \in X$ に対して $\eta_{\mathrm{P},t,k}$ を P 以外のすべての点において正則で, $\mathrm{ord}_{\mathrm{P}}\eta_{\mathrm{P},t,k} = -k$ で P における Laurent 展開が

$$\eta_{\mathrm{P},t,k} = \left(-\frac{k-1}{t^k} + O(1)\right) dt \tag{1.45}$$

の形であり, $j = 1, \cdots, g$ に対して

$$\int_{\alpha_j} \eta_{\mathrm{P},t,k} = 0 \tag{1.46}$$

となるような微分形式とする[3]. ただし $O(1)$ は t に関して 0 次以上の項を表す. このような微分形式を**正規化された第２種微分形式** とよぶ. このような微分形式も, やはり 1.9, 1.34 より存在する ([I], p.109, 定理 2.25, → [Ku], pp.133–134). また, 上と同様に 1.33(i) より一意的に定まる.

今後は, 函数, 微分形式などは X 上のものとも $X_\circ$ 上のものとも考える. それをいちいち断らないが混乱はないと信ずる.

定理 1.47 X 上の, 局所径数の与えられた点 P および 2 点 Q_1, Q_2 とに対して, 先にとってあった道 α_i, β_j をこの 3 点を通過しないようにすこしずらす. いま, P の近傍の動点 P_t を局所径数 t の値が定める点, つまり, $t(\mathrm{P}_t) = t$, $\mathrm{P}_0 = \mathrm{P}$ なる $X_\circ$ の点とする. このとき $X_\circ$ 上の積分に関して次が成り立つ.

$$\begin{aligned} \frac{d}{dt}\int_{\mathrm{P}}^{\mathrm{P}_t} \tau_{\mathrm{Q}_1,\mathrm{Q}_2}\Big|_{t=0} &= \int_{\mathrm{Q}_1}^{\mathrm{Q}_2} \eta_{\mathrm{P},t,2}, \\ -2\pi\sqrt{-1}\frac{d^{k-1}}{dt^{k-1}}\int_{\mathrm{P}}^{\mathrm{P}_t} \hat{\omega}_j\Big|_{t=0} &= \int_{\beta_j} \eta_{\mathrm{P},t,k}. \end{aligned} \tag{1.48}$$

証明 補題 1.23 において $m = 1$, $n = 2$, $\mathrm{P}_1 = \mathrm{P}$, $t_1 = t$, ${a_\nu}^{(i)} = a_\nu$, ${a'}_\nu^{(i)} = {a'}_\nu$ とし, $\eta = \eta_{\mathrm{P},t,2}$, $\eta' = \tau_{\mathrm{Q}_i,\mathrm{Q}_j}$ とおけば η が正規化されているので最初の和は消える. また η の P における展開の係数 $a_{-1} = 0$ であるから, 第 2 項の最初の項は消える. $a_\nu = 0$ $(\nu \leq -3)$, $b_\nu^{(i)} = 0$ $(\nu \leq -2)$ なので, 第 2 項の和の部分は $\nu = 0$ の項を除いて消え, 第 3 項も消える. $a_{-2} = 1$, ${a'}_\nu = \frac{\eta}{dt}\big|_{t=0} = \frac{d}{dt}\int_{\mathrm{P}}^{\mathrm{P}_t}\eta$, $b'_{-1} = 1$ なので, 最初の式がでる. ([I], 第 5 章, p.259, (1.27)). $\eta = \hat{\omega}_j$, $\eta' = \eta_{\mathrm{P},t,k+1}$ とおけば, 第 2 の式を得る. □

定理 1.49 4 点 P_1, P_2, Q_1, Q_2 について, すべての道 β_j をこれらの点を通らないようにずらしておく. このとき $X_\circ$ 上の積分に関して次が成り立つ.

$$\int_{\mathrm{P}_1}^{\mathrm{P}_2} \tau_{\mathrm{Q}_1,\mathrm{Q}_2} = \int_{\mathrm{Q}_1}^{\mathrm{Q}_2} \tau_{\mathrm{P}_1,\mathrm{P}_2}, \quad 2\pi\sqrt{-1}\int_{\mathrm{P}_1}^{\mathrm{P}_2} \hat{\omega}_j = \int_{\beta_j} \tau_{\mathrm{P}_1,\mathrm{P}_2}. \tag{1.50}$$

[3]いつもこの様な微分が存在するわけではないことに注意せよ.

最初の式は**変数と径数の交換法則**と呼ばれてゐる. 後者は (2.16), 3.48, (5.23) などの証明などに使ふ.

証明 前者は [I], 第 5 章, p.259, (1.28) そのもので, 1.23 で $m = n = 2$, $\eta = \tau_{\mathrm{P}_1,\mathrm{P}_2}$, $\eta' = \tau_{\mathrm{Q}_1,\mathrm{Q}_2}$ とすれば得られる. 後者を得るには, やはり, 1.23 で $m = 2$, $n = 0$, $\eta = \tau_{\mathrm{P}_1,\mathrm{P}_2}$, $\eta' = \hat{\omega}_j$ とすればよい. □

これらの証明について一言. 定理 1.23 は [I], p.243, 定理 5.2 そのものであり, 1.47 と 1.49 は同書, p.252. 定理 5.5 に含まれている[4].

X 上の点の形式的な有限和

$$D = \sum_{\mathrm{P}\in X} n_{\mathrm{P}}\mathrm{P} \quad (n_{\mathrm{P}} \in \mathbb{Z}) \tag{1.51}$$

を X の**因子** (divisor) といひ, これらのなす Abel 群を**因子群**といふ. この因子 D についての n_{P} の和を D の**次数**といふ:

$$\deg D = \sum_{\mathrm{P}\in X} n_{\mathrm{P}}. \tag{1.52}$$

また, 全ての n_{P} が正または 0 で, 少なくともひとつの n_{P} が 0 でないとき, ある様な因子を**整因子** (integral divisor) といふ. いま X 上の函数 f と各点 P について f が P で n_{P} 位の零, または $-n_{\mathrm{P}}$ の極であるとする. このとき

$$(f) = \sum_{\mathrm{P}\in X} n_{\mathrm{P}}\mathrm{P} \tag{1.53}$$

と書いて (f) を f の因子と呼ぶ. さらに ω が X 上の微分形式であるとき, 各点 P における局所径数を t をとれば, $\omega = g(t)dt$ (g は函数) と書けるが, $g(t)$ の P における (零または極) の位数を n_{P} として, ω の因子を

$$(\omega) = \sum_{\mathrm{P}\in X} n_{\mathrm{P}}\mathrm{P} \tag{1.54}$$

と定義する. これは局所径数 t_{P} の取り方に依らない.

2 つの因子 D_1 と D_2 に対してその差 $D_1 - D_2$ がある函数の因子 (f) に一致するとき, D_1 と D_2 は**有理同値**であるといふ. これは明らかに同値関係である.

どんな 2 つの微分形式の因子も有理同値であるから, 微分形式の因子全体のなす類あるいはその 1 つの代表を K_X で表はすことにする.

函数の因子に有理同値な因子の全体は Abel 群をなすので, 全因子 (または次数 0 の因子全体) の有理同値に関する剰余群を考へることができる. それを**因子類群**または **Picard 群**と呼び

$$\mathrm{Pic}X \quad (\text{または } \mathrm{Pic}^{\circ}X) \tag{1.55}$$

と書く.

[4] これらは [HL] ではどの様に書かれてゐるのであらうか.

定義 1.56 因子 D に対し, $(f)+D$ が正因子になるような有理関数 f の全体のなす $\mathbb{C}$ 上の線形空間を $L(D)$ であらわす.

これにより, $(\eta)+D$ が整因子になるような有理型微分 η 全体のなす $\mathbb{C}$ 上の線形空間は, 明らかに, $L(K_X-D)$ と表はされる.

命題 1.57 D_1 と D_2 が有理同値であるとき $L(D_1)=L(D_2)$ である.

定理 1.58 (Riemann-Roch の定理)
$\dim L(D)=\deg D-g+1+\dim L(K_X-D)$.

証明[5] Step 1. D が整因子のときは 1.47 の第 2 の式と 1.49 の第 2 の式から線形代数学の簡単な事実から示される. [TD], p.85 をみよ. この証明は直観に訴える, わかりやすい証明であると思う.
Step 2. 次に D または K_X-D が整因子と有理同値であれば, 成り立つことはすぐにわかる.
Step 3. $\dim L(D)>0$ ならば $0\neq f\in L(D)$ について $(f)+D$ は整因子なので, その様な因子 D は整因子と有理同値となり, 与式は成り立つ.
Step 4. 同様に $\dim L(K_X-D)>0$ のときも成り立つ.
Step 5. 以上により, もし D も K_X-D も整因子とは有理同値でないとすれば, $\dim L(D)=\dim L(K_X-D)=0$ となることがわかつたから, このとき示すべき等式は

$$\deg D=g-1 \tag{1.59}$$

となる. つまり $D=D_1-D_2$ （D_i は 0 でない互ひに素な整因子）と書けてゐるとき, (1.59) を示せば良い. それは [FK], p.77 Theorem の様にすればできる. まづ

$$\dim L(D_1)\geqq\deg D_1-g+1=\deg D_2+\deg D-g+1. \tag{1.60}$$

ここで

$$\deg D\geqq g \tag{1.61}$$

だとすると

$$\dim L(D_1)\geqq\deg D_2+1. \tag{1.62}$$

となるので, $0\neq f\in L(D_1)$ で丁度 D_2 に極を持つものが取れる. これは線形代数である. かくして $f\in L(D_1-D_2)=L(D)$ となり, $\dim L(D)>0$ となるが, これは仮定に矛盾する. よつて

$$\deg D\leqq g-1. \tag{1.63}$$

[5] [I] は先にこの定理を証明しているので, 我々とは議論の進め方が全く異なる.

しかるに $\dim L(D) = \dim L(K_X - D) = 0$ なので

$$\deg(K_X - D) \leqq g - 1, \tag{1.64}$$

つまり

$$\deg D \geqq g - 1 \tag{1.65}$$

がわかり, 結局

$$\deg D = g - 1 \tag{1.66}$$

でなければならない. □

1.2 Theorem of Abel-Jacobi

定義 1.67 整因子 D に対して $\dim L(-D) = 1$ が成り立つとき, すなはち高々 D なる極をもつような X 上の有理型関数が定数以外に存在しないとき D を**一般因子**とよぶ.

D が一般因子であることは定理 1.13 から

$$\dim L(K_X - D) = g - \deg D \tag{1.68}$$

と同値である. とくに一般因子の次数は g を越えない. また次数 g の因子が一般であるための必要十分条件は

$$\dim L(K_X - D) = 0 \tag{1.69}$$

となることである. 次数が g 以下で一般因子でないものを**特殊因子**とよぶ. X 上には必ず一般因子が存在する: すなわち

定理 1.70 $\dim L(K_X - P) = g - 1$. すなわち, すべての第 1 種微分の共通零点は存在しない.

証明 [TD], p.86. □

定理 1.71 X 上に相異なる点 $\mathrm{P}_1, \cdots, \mathrm{P}_g$ を因子 $\mathrm{P}_1 + \cdots + \mathrm{P}_g$ が一般であるようにとれる.

証明 [TD], p.87, 定理 11 □

定義 1.72 基点 P_0 を固定する. 次数 0 の因子 $D = c_1\mathrm{P}_1 + \cdots + c_n\mathrm{P}_n$ $(c_i \in \mathbb{Z})$ と第 1 種微分の基底 ω に対し, 適当な積分路を用意して写像

$$D \longmapsto \sum_i c_i \int_{\mathrm{P}_0}^{\mathrm{P}_i} \omega \tag{1.73}$$

を考へる. これは　mod Λ で積分路の選び方に依らず定まる. これを

$$D \longmapsto a(D,\omega) \tag{1.74}$$

と略記して **Abel 写像**といふ. X の n 個の順序を無視した直積

$$\mathrm{Sym}^n X \tag{1.75}$$

を考へて, その元を $\mathrm{P}_1+\cdots+\mathrm{P}_n-n\mathrm{P}_0$ の形の因子の全体と同一視する. 従つて Abel 写像を写像

$$\begin{aligned} \mathrm{Sym}^n X &\longrightarrow J \\ (\mathrm{P}_1,\cdots,\mathrm{P}_n) &\longmapsto a(\mathrm{P}_1+\cdots+\mathrm{P}_n-n\mathrm{P}_0,\omega) \end{aligned} \tag{1.76}$$

のことであると思ふこともある. このとき, これの像を

$$W^{[n]} = a(\mathrm{Sym}^n X,\omega) = \{a(\mathrm{P}_1+\cdots+\mathrm{P}_n-n\mathrm{P}_0,\omega)\,|\,\mathrm{P}_j \in X\} \tag{1.77}$$

と記すことが多い.

定理 1.78 (Abel's theorem)　ω を第 1 種微分形式の基底からなる vector とし, Λ を ω の周期格子とする. P_0 を X の基点とする. 因子 D について, D が主因子, つまりある函数の因子になっているためには

$$\deg D = 0 \quad \text{且つ} \quad a(D,\omega) \in \Lambda \tag{1.79}$$

となることが必要十分条件である. それゆゑ

$$\begin{aligned} \mathrm{Pic}^\circ X &\longrightarrow J \\ D &\longmapsto a(D,\omega) \mod \Lambda \end{aligned} \tag{1.80}$$

は群の同型である.

証明　[TD], p.89　□

定理 1.81　特殊因子の全体の Abel 写像による像は $W^{[g-2]}$ に一致する.

証明　[Ku], p.159　□

補題 1.82　D_0 を g 次の任意の因子とせよ. D を 0 次の任意の因子とせよ. このときある g 次の正因子 D_1 が存在して, 適当な積分路により

$$a(D_1-D_0,\omega) = a(D,\omega) \tag{1.83}$$

となる.

証明 [TD], pp.89-90. □

Abel 写像が全射であることをつぎの強い形で述べられる. 本稿では, この定理を使ふといふよりは, 具体的な函数を構成することで, この定理を計算可能なものに具体化することを主眼としてゐる. それにより, 所謂 Jacobi の Umkehrproblem を具体的に解くのである.

定理 1.84 (Jacobi's theorem) D_0 を g 次の任意の因子とせよ. u を $\mathbb{C}^g$ の任意の元とせよ. このとき g 次の正因子 D が存在して, 適当な積分路により

$$a(D-D_0,\omega)=u \tag{1.85}$$

となる. しかも $u\notin W^{[g-2]}$ であれば, D は一意的に定まる. それゆゑ, $n=g$ の場合の (1.76)

$$\mathrm{Sym}^g X\to J \tag{1.86}$$

は双有理写像である.

証明 [TD], p.90 □

2 Theta 函数

2.1 Theta 函数の定義

ここでは, 第 1 節の記号を使ふ. さらに $\hat\Theta$ や $\hat\Theta+\hat\Lambda$ も ω を $\hat\omega$ に変えるなどして定義しておく. Riemann の **theta 函数**を

$$\vartheta(z)=\sum_{n\in\mathbb{Z}^{2g}}\exp\left[2\pi\sqrt{-1}\left\{\frac{1}{2}\,{}^tnTn+\,{}^tnz\right\}\right]. \tag{2.1}$$

で定義する. ここに T は 1.39 で定義した $\hat\omega$ の周期のなす行列である.

補題 2.2 $a,b\in\mathbb{Z}^g$ のとき, theta 函数は**平行移動公式**

$$\vartheta(z+Ta+b)=\vartheta(z)\exp 2\pi\sqrt{-1}\left\{\tfrac{1}{2}\,{}^taTa+\,{}^ta(z+b)\right\} \tag{2.3}$$

をもつ. 証明は容易である.

まづ, 函数 $\vartheta(z)$ の零点を調べる. その為に以下の 2 つを用意しなくてはならない.

定義 2.4

$$\left\{\sum_{j=1}^{g-1}\int_{\mathrm{P}_0}^{\mathrm{P}_j}\omega\in\mathbb{C}^g\mod\Lambda\,\middle|\,\mathrm{P}_1,\cdots,\mathrm{P}_{g-1}\right\}\subset J \tag{2.5}$$

なる集合, つまり $\mathrm{P}_1+\cdots+\mathrm{P}_{g-1}-(g-1)\cdot\mathrm{P}_0$ なる形の因子全体の Abel 写像による像を **theta 因子**とよび, Θ と記す. これは (1.77) の $W^{[g-1]}$ に他ならない. Θ は, J 上の重要な有理型函数の極となる点からなる因子に現れることがあとでわかる. また

$$\Theta+\Lambda:=\left\{\sum_{j=1}^{g-1}\int_{\mathrm{P}_0}^{\mathrm{P}_j}\omega\in\mathbb{C}^g\Big|\mathrm{P}_1,\cdots,\mathrm{P}_{g-1}\right\}\subset\mathbb{C}^g \tag{2.6}$$

と記すことにする.

定義 2.7 これまでの記号で ($T=[T_{ij}]$)

$$K_j=-\frac{1}{2}T_{jj}-\int_{\mathrm{P}_0}^{\mathrm{I}_j}\hat{\omega}_j+\sum_{i=1}^{g}\int_{\alpha_i}\Big(\int_{\mathrm{P}_0}^{\mathrm{P}}\hat{\omega}_j\Big)\hat{\omega}_i(\mathrm{P}) \tag{2.8}$$

とおいて, これを **Riemann の定数** とよぶ. ただし積分は $X_\circ$ の上でのものである. ここに I_j は $X_\circ$ の頂点であつて (1.1) の所で述べた点 I に対応する α_j と β_j の共通の始点である (図 1.27). もちろんこれは積分路の取り方によるが $\mod\hat{\Lambda}$ では一意的に定まる. また, 点 I や $\{\alpha_j\}$, $\{\beta_j\}$ をずらしても K_j の値は変はらない (要説明).

定理 2.9 (Riemann の定理) 点 $\mathrm{P}_1,\cdots,\mathrm{P}_g\in X$ をとり, 固定する. $\mathrm{P}\in X$ の函数

$$G(\mathrm{P})=\vartheta\Big(\int_{\mathrm{P}_0}^{\mathrm{P}}\hat{\omega}-\sum_{j=1}^{g}\int_{\mathrm{P}_0}^{\mathrm{P}_j}\hat{\omega}+K\Big) \tag{2.10}$$

について
(1) $G(\mathrm{P})$ が恒等的に 0 でないためには, 因子 $\mathrm{P}_1+\cdots+\mathrm{P}_g$ が一般因子であることが必要十分である.
(2) $G(\mathrm{P})$ が恒等的に 0 でないとき, $G(\mathrm{P})$ は $\mathrm{P}=\mathrm{P}_1,\cdots,\mathrm{P}_g$ においてのみ 1 位の零点をもつ. (いくつかの P_j が一致すればもちろん重根となる.)

証明 [TD], p.98, 定理 1 と p.100, 定理 3 から出る. □

定理 2.11 函数 $\vartheta(z)$ ($z\in{\Omega'}^{-1}\mathbb{C}^g$) について, $\vartheta(z)=0$ となるための必要十分条件は $z+K\in\hat{\Theta}+\hat{\Lambda}$ となることである.

証明 [TD], p.99, 定理 2 そのもの. □

2.2 第 3 種微分形式と Theta 函数の関係

ここでは第 3 種微分形式と theta 函数を結びつける重要な公式を証明しよう.

定理 2.12 基点 $\mathrm{P}_0\in X$ に対して, g 個の点 $\mathrm{A}_1,\cdots,\mathrm{A}_g$ が存在して, 任意に与へられた g 個の固定された点 $\mathrm{P}_1,\cdots,\mathrm{P}_g$ についての P の函数

$$\mathrm{P}\longmapsto\vartheta\Big(\int_{\mathrm{P}_0}^{\mathrm{P}}\hat{\omega}-\sum_{j=1}^{g}\int_{\mathrm{A}_j}^{\mathrm{P}_j}\hat{\omega}\Big) \tag{2.13}$$

の零点がいつも丁度 $\mathrm{P}_1,\cdots,\mathrm{P}_g$ だけになる.

証明 [Ba1]. p.255 にある. □

定理 2.14 点 P_j, Q_j $(j = 1, \cdots, g)$ を

$$\sum_{j=1}^{g} \int_{\mathrm{P}_0}^{\mathrm{P}_j} \hat{\omega} \notin \hat{\Theta} + \hat{\Lambda}, \quad \sum_{j=1}^{g} \int_{\mathrm{P}_0}^{\mathrm{Q}_j} \hat{\omega} \notin \hat{\Theta} + \hat{\Lambda} \tag{2.15}$$

なる X の点とするとき, $\mathrm{P}, \mathrm{Q} \in X$ に対して次が成り立つ.

$$\exp\left(\sum_{j=1}^{g} \int_{Q}^{\mathrm{P}} \tau_{\mathrm{P}_j,\mathrm{Q}_j}\right) = \frac{\vartheta\left(\int_{\mathrm{P}_0}^{\mathrm{P}} \hat{\omega} - \sum_{j=1}^{g} \int_{\mathrm{A}_j}^{\mathrm{P}_j} \hat{\omega}\right)\vartheta\left(\int_{\mathrm{P}_0}^{\mathrm{Q}} \hat{\omega} - \sum_{j=1}^{g} \int_{\mathrm{A}_j}^{\mathrm{Q}_j} \hat{\omega}\right)}{\vartheta\left(\int_{\mathrm{P}_0}^{\mathrm{P}} \hat{\omega} - \sum_{j=1}^{g} \int_{\mathrm{A}_j}^{\mathrm{Q}_j} \hat{\omega}\right)\vartheta\left(\int_{\mathrm{P}_0}^{\mathrm{Q}} \hat{\omega} - \sum_{j=1}^{g} \int_{\mathrm{A}_j}^{\mathrm{P}_j} \hat{\omega}\right)}. \tag{2.16}$$

ここで, A_j は 2.12 のそれである. 積分路は, $\int_{\mathrm{Q}}^{\mathrm{P}}$ の積分路が $\int_{\mathrm{P}_0}^{\mathrm{P}}$ のそれと $\int_{\mathrm{P}_0}^{\mathrm{Q}}$ のそれの差に homotope になる様に取るものとする. (ただし, 多変数函数に関する適当な解析接続の可能性定理を使えば, P_j や Q_j に関する条件は無用である.)

証明 両辺を P の函数として見て, それぞれの因子を調べる. 右辺の因子は 2.9 より $\sum_{j=1}^{g} \mathrm{P}_j - \sum_{j=1}^{g} \mathrm{Q}_j$ であり, 左辺も $\tau_{\mathrm{P}_j,\mathrm{Q}_j}$ の定義, つまり 1.43 よりこれと同じ因子を持つ. しかも, 道 α_j を点 P を通るようにとっておくとき, $\tau_{\mathrm{P}_j,\mathrm{Q}_j}$ の定義と theta 函数の平行移動公式により, その α_j に沿って P を一周させてみても両辺は変わらない. また, 道 β_j を点 P を通るようにとっておき, β_i に沿って P を一周させてみると, 左辺には 1.49 の第 2 式により,

$$\exp\left[2\pi\sqrt{-1}\left(\sum_{j=1}^{g} \int_{\mathrm{Q}_j}^{\mathrm{P}_j} \hat{\omega}_i\right)\right] \tag{2.17}$$

が倍され, 一方, 右辺は (2.3) により,

$$\begin{aligned} \exp\Bigg[2\pi\sqrt{-1}\Bigg[&\left\{\left(\int_{\infty}^{\mathrm{P}} \hat{\omega}_i - \sum_{j=1}^{g} \int_{\mathrm{A}_j}^{\mathrm{P}_j} \hat{\omega}_i\right) + \frac{1}{2}\tau_{ii}\right\} \\ &- \left\{\left(\int_{\infty}^{\mathrm{P}} \hat{\omega}_i - \sum_{j=1}^{g} \int_{\mathrm{A}_j}^{\mathrm{Q}_j} \hat{\omega}_i\right) + \frac{1}{2}\tau_{ii}\right\}\Bigg]\Bigg] \end{aligned} \tag{2.18}$$

だけ倍される. したがってもともと $X_\circ$ 上の函数と考えていた両辺の商は実際は X 上の函数とみなせる. しかるにはじめに述べたことから, 極を持たないのであるから定数でなければならない. ところが $\mathrm{P} = \mathrm{Q}$ としてみると両辺ともに 1 となるので実際に両辺が等しいことがわかる. □

3 超楕円的 Theta 関数・$\wp$ 関数

3.1 超楕円的 Riemann 面とその Abel 微分

無限遠点が 1 点のみの代数曲線 (d,s)-curve

いま $d<s$ を互ひに素な 2 つの自然数とし,

$$f(x,y)=y^d+p_1(x)y^{d-1}+\cdots+p_{d-1}(x)y-p_d(x) \tag{3.1}$$

とおく. 但し $p_j(x)$ は x の $\lfloor\frac{js}{d}\rfloor$ 次の多項式で, その係数を

$$\begin{aligned} p_j(x)&=\sum_k \mu_{ds-dk}x^k,\quad (1\leqq j\leqq d-1)\\ p_d(x)&=x^s+\mu_{ds-d}x^{s-1}+\mu_{ds-2d}x^{s-2}+\cdots+\mu_{ds} \end{aligned} \tag{3.2}$$

と書くことにする. ここで

$$f(x,y)=0 \tag{3.3}$$

で定義される曲線を考へる. これは無限遠点に唯 1 つの点をもつ代数曲線 C の affine 部分である. この様な曲線を (d,s) **曲線** と呼ぶ. この場合, 次の **weight** を導入することができる. 即ち

$$\mathrm{wt}(x)=-d,\quad \mathrm{wt}(y)=-s,\quad \mathrm{wt}(\mu_j)=-j. \tag{3.4}$$

さすれば, $f(x,y)$ のみならず, この曲線に関するあらゆる等式はこの weight について斉次になる.

この note のほとんどの内容は上のより一般な曲線についても定式化されてつつある. 一方例へば d と s が互ひに素でない様な曲線については, それが上の形の曲線と同型でないならば, それの扱ひは今後の課題である様に思はれる.

超楕円曲線

以下では $d=2$, $s=2g+1$ (奇数), $p_1(x)=0$ の場合のみ, 即ち,

$$y^2=x^{2g+1}+\mu_2x^{2g}+\cdots+\mu_{4g+2} \tag{3.5}$$

により得られる射影曲線[6](超楕円曲線) C についてのみ Abel 函数について述べる. ここで μ_j はすべて定数 $(\in\mathbb{C})$ であり, 右辺を $f(x)$ と書くとき $f(x)=0$ は重根を持たないものと仮定する. この場合, **weight** は

$$\mathrm{wt}(x)=-2,\quad \mathrm{wt}(y)=-(2g+1),\quad \mathrm{wt}(\mu_j)=-j \tag{3.6}$$

となつてゐる.

[6]実際にこれを射影空間内の代数曲線として実現することに関しては, [Mu2], p.3.12-3.16 に記されている.

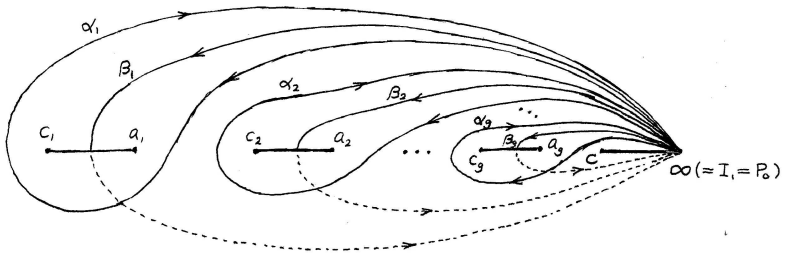


図 3.11

第 1 種微分形式, 周期行列

第 1 節と第 2 節の Riemann 面 X として上の超楕円曲線 C を取る. したがって, X の種数は g である. 次に, $f(x)=0$ の $2g+1$ 個の根に順序を適当に入れて

$$c_1,\, a_1,\, c_2,\, a_2,\, \cdots,\, c_g,\, a_g,\, c \tag{3.7}$$

とする. 従つてもちろん

$$f(x) = (x-a_1)\cdots(x-a_g)(x-c_1)\cdots(x-c_g)(x-c). \tag{3.8}$$

また, 記号 ∞ で X の無限遠点を記す. また $A_j(a_j, 0)$ と書く. 1.13 にある様に X には g 個の $\mathbb{C}$ 上 1 次独立な第 1 種微分形式が存在するが, いまの場合は

$$\omega_j = \frac{x^{j-1}dx}{2y} \quad (j=1,\cdots,g) \tag{3.9}$$

をそれらに取ることができる.

さて, 前章と同様に X 上に $2g$ 個の路

$$\alpha_j,\ \beta_j\ (j{=}1,\cdots,g) \tag{3.10}$$

を の様に定めると, その交点数は

$$\alpha_i \cdot \alpha_j = \beta_i \cdot \beta_j = 0, \quad \alpha_i \cdot \beta_j = \delta_{ij} \tag{3.12}$$

となつてをり, これらは, X の homology 群 $H_1(X,\mathbb{Z})$ の基底をなす. 以下では, 簡単のために,

$$\omega = {}^t\begin{bmatrix}\omega_1 & \cdots & \omega_g\end{bmatrix} \tag{3.13}$$

とかく. 上の ω_j に対する α_j, β_j の周期のなす行列をやはり

$$\Omega' = \begin{bmatrix}\displaystyle\int_{\alpha_j}\omega_i\end{bmatrix}, \quad \Omega'' = \begin{bmatrix}\displaystyle\int_{\beta_j}\omega_i\end{bmatrix}, \quad \Omega = \begin{bmatrix}\Omega' \\ \Omega''\end{bmatrix} \tag{3.14}$$

と書く. 系 1.34 により Ω' は正則であるが, いま

$$\begin{gathered} {}^t\begin{bmatrix}\hat{\omega}_1 & \cdots & \hat{\omega}_g\end{bmatrix} := \Omega'^{-1}\ {}^t\begin{bmatrix}\omega_1 & \cdots & \omega_g\end{bmatrix} \\ T := \Omega'^{-1}\Omega'' \end{gathered} \tag{3.15}$$

とおけば,

$$\left[\int_{\alpha_j}\hat{\omega}_i\right]=1_g,\quad \left[\int_{\beta_j}\hat{\omega}_i\right]=T \tag{3.16}$$

となる. これも本書では

$$\hat{\omega}={}^t\begin{bmatrix}\hat{\omega}_1 & \cdots & \hat{\omega}_g\end{bmatrix} \tag{3.17}$$

のように書く. 上記の微分形式 $\hat{\omega}_1,\cdots,\hat{\omega}_g$ を**正規化された**第 1 種微分形式と呼ぶのであつた.

3.1.1 標準的な第 1, 第 2 種・第 3 種微分形式とそれらの関係

以下, X 上の各点 P における局所径数 t を考へるが, 具体的には

$$t=\begin{cases}x-x(\mathrm{P}) & y(\mathrm{P})\neq 0,\infty \text{ のとき},\\ y & y(\mathrm{P})=0 \text{ のとき}\\ \dfrac{y}{x^{g+1}} & y(\mathrm{P})=\infty \text{ のとき}\end{cases} \tag{3.18}$$

とすればよい.

定義 3.19 定義 1.43 の記号をここでも用いる : 即ち
(1) 2 点 $\mathrm{Q}_1,\mathrm{Q}_2\in X$ に対し微分形式 $\tau_{\mathrm{Q}_1,\mathrm{Q}_2}$ で次の条件を満すものが唯 1 つ存在する: $\mathrm{Q}_1,\mathrm{Q}_2$ 以外のすべての点において正則で, $\mathrm{ord}_{\mathrm{Q}_1}\tau_{\mathrm{Q}_1,\mathrm{Q}_2}=\mathrm{ord}_{\mathrm{Q}_2}\tau_{\mathrm{Q}_1,\mathrm{Q}_2}=-1$ かつ $\mathrm{Res}_{\mathrm{Q}_1}\tau_{\mathrm{Q}_1,\mathrm{Q}_2}=1$, $\mathrm{Res}_{\mathrm{Q}_2}\tau_{\mathrm{Q}_1,\mathrm{Q}_2}=-1$ であり, すべての j について

$$\int_{\alpha_j}\tau_{\mathrm{Q}_1,\mathrm{Q}_2}=0 \tag{3.20}$$

となる.
(2) 局所径数 t を与えられた点 $\mathrm{P}\in X$ に対して $\eta_{\mathrm{P},t}$ を P 以外のすべての点において正則で, $\mathrm{ord}_{\mathrm{P}}\eta_{\mathrm{P},t}=-2$ で P における Laurent 展開が

$$\eta_{\mathrm{P},t}=\left(-\frac{1}{t^2}+\cdots\right)dt \tag{3.21}$$

の形であり,

$$\int_{\alpha_j}\eta_{\mathrm{P},t}=0 \tag{3.22}$$

となるような微分形式とする.

次に $H_1(C,\mathbb{Z})$ の生成元

$$\alpha_i, \beta_j \quad (1 \leqq i, j \leqq g) \tag{3.23}$$

を (1.16) の様に, それらの交点数が $\alpha_i \cdot \alpha_j = \beta_i \cdot \beta_j = \delta_{ij}$, $\alpha_i \cdot \beta_j = 0$ となるやうに選ぶ. 次に, 先の (3.9) の ω_j から定まる周期

$$[\,\Omega' \;\; \Omega''] = \left[\int_{\alpha_i} \omega_j \quad \int_{\beta_i} \omega_j \right]_{i,j=1,2,\cdots,g} \tag{3.24}$$

を考へる. さらに文字 Z, W を使つて C 上の 2 点 $\mathrm{P}(x,y)$, $\mathrm{Q}(z,w)$ について

$$[(x,y),\,(z,w)] = \frac{1}{(x-z)\frac{\partial}{\partial y}f(x,y)} \sum_{k=1}^{g} y^{g-k} \left[\frac{f(Z,W)}{W^{g+1-k}} \right]_W^+ \Bigg|_{(Z,W)=(z,w)} \tag{3.25}$$

とおく. これは weight が $-d=-2$ で斉次である. ただし, $[\;\;]_W^+$ は W について負冪の項を取り除くことを意味する.

補題 3.26 (fundamental 2-forms of second kind) $C \times C$ の上の 2-form

$$\big((x,y),(z,w)\big) \longmapsto R\big((x,y),(z,w)\big)dzdx \tag{3.27}$$

であつて

$$\lim_{(x,y)\longrightarrow(z,w)} R\big((x,y),(z,w)\big)(x-z)^2 = 1 \tag{3.28}$$

が成り立ち, $(x,y)=(z,w)$ なる点でのみ極を持ち, その他の点では正則である様なものを考へる. 第 1 種微分形式 (3.9) と (3.14) の微分形式, および C 上の 2 点 (x,y), (z,w) に対して, 無限遠点 ∞ のみに極を持つ第 2 種微分形式 $\eta_j = \eta_j(x,y)$ $(j = 1, 2, \cdots, 3)$ が存在して, 上の様な 2-form は

$$R\big((x,y),(z,w)\big) := \frac{d}{dx}[(z,w),(x,y)] + \sum_{j=1}^{g} \frac{\omega_j(z,w)}{dz}\frac{\eta_j(x,y)}{dx} \tag{3.29}$$

と書かれる. ただし, 先頭の微分は動点 $(x,y) \in C$ に関する微分である[7]. ここでさらに $R\big((x,y),(z,w)\big)$ が Sato weight に関して斉重 (重さ 6), かつ 2 点の座標に関して対称, つまり

$$R\big((z,w),(x,y)\big) = R\big((x,y),(z,w)\big) \tag{3.30}$$

が成り立つことを要請する. その様な $\{\eta_j\}$ の組は, 以下に説明する様に $\mathrm{Sp}(2g,\mathbb{Z})$ の作用と $\{\omega_j\}$ の張る空間とを modulo として唯 1 組だけに定まる. これらを満足する 2-form $R\big((x,y),(z,w)\big)dxdz$ を (Klein の) **fundamental 2-form of second kind** と呼ぶ.

証明. 所望の fundamental 2-form of second kind を与へる様な微分形式 η_j ($j = 1, 2, \cdots, g$) の存在は η_j を未定係数法で求められることからわかる. また $\mathrm{Sp}_{2g}(\mathbb{Z})$ の作用と $\{\omega_j\}$ の張る空間とを modulo しての一意性については [BG], pp.3617–3618 と同様なので省略する ([Ba1], p.194 の周辺も参照されたい). □

上の様な η_j が

$$\eta_j(x,y) = \frac{h_j(x,y)}{\frac{\partial}{\partial y}f(x,y)}, \qquad \text{但し}\ \ h_j(x,y) \in \mathbb{Q}[\mu_1, \cdots, \mu_{ds}][x,y] \quad \text{で斉重}, \tag{3.31}$$

の形に書かれることは容易にわかる. ここで

$$h_j(x,y)\ \text{の項数が最も少くなること} \tag{3.32}$$

を要請すれば, η_j は一意的に定まる ([BG], p.3618) から, 以後はその様なものを η_j と記すことにする.

3.2

3.2.1 In the Case of Hyperelliptic Curves

C が 超楕円曲線のとき $h_j(x,y)$ を具体的に書き下すこと以下の様になる:

$$[(x,y),(z,w)] = \frac{y+w}{x-z}\frac{1}{2y} \tag{3.33}$$

および

$$R\big((x,y),(z,w)\big) = \frac{F(x,z)+2yw}{(x-z)^2}\frac{1}{2y}\frac{1}{2w} \tag{3.34}$$

ここで

$$F(x,z) = \sum_{j=0}^{g-1} x^j z^j (\mu_{2j+1}(x+z) + 2\mu_{2j}) \tag{3.35}$$

である.

定義 3.36 Riemann 面 X 上の動点 $\mathrm{P}(x,y)$, $\mathrm{Q}(z,w)$ と定点 $\mathrm{A}(a,b)$, $\mathrm{B}(c,d)$ について (1) 以下では (3.29) の $R(\ \ ,\ \ )$ に対して,

$$\begin{aligned} \mathsf{R}^{\mathrm{P,A}}_{\mathrm{Q,B}} &= \int_{\mathrm{A}}^{\mathrm{P}}\int_{\mathrm{B}}^{\mathrm{Q}} R\big((x,y),(z,w)\big)dxdz \\ &= \int_{\mathrm{A}}^{\mathrm{P}}\int_{\mathrm{B}}^{\mathrm{Q}} \frac{F(x,z)+2yw}{(x-z)^2}\frac{dx}{2y}\frac{dz}{2w} \end{aligned} \tag{3.37}$$

[7] x と y に依存関係があるので ∂ を使はないで表した.

とおく.

(2) (3.25) の $[\mathrm{P},\mathrm{A}]=\dfrac{y+b}{x-a}\dfrac{1}{2y}$ について

$$\mathsf{P}^{\mathrm{P},\mathrm{A}}_{\mathrm{Q},\mathrm{B}}:=\int_{\mathrm{A}}^{\mathrm{P}}\left([\mathrm{P},\mathrm{Q}]-[\mathrm{P},\mathrm{B}]\right)dx \tag{3.38}$$

とおく. $\mathsf{R}^{\mathrm{P},\mathrm{A}}_{\mathrm{Q},\mathrm{B}}$ も $\mathsf{P}^{\mathrm{P},\mathrm{A}}_{\mathrm{Q},\mathrm{B}}$ も P の関数としては, $\mathrm{P}=\mathrm{Q}$, B でそれぞれ留数 1, -1 なる 1 位の極をもち, その他の点では正則な微分形式の積分になっている.

定義 3.39 以下では (3.29) を満たす η_j として

$$\eta_j=\frac{1}{2y}\sum_{k=j}^{2g-j}(k+1-j)\mu_{k+1+j}x^k dx\quad(j=1,\cdots,g) \tag{3.40}$$

が取れる. これらは点 ∞ においてのみ留数 0 の極を持ち, 他の点では正則な第 2 種微分形式である.

定理 3.41 定義 3.37, 3.38 の記号のもとで

$$\mathsf{R}^{\mathrm{P},\mathrm{A}}_{\mathrm{Q},\mathrm{B}}=\int_{\mathrm{A}}^{\mathrm{P}}\omega_1\int_{\mathrm{B}}^{\mathrm{Q}}\eta_1+\cdots+\int_{\mathrm{A}}^{\mathrm{P}}\omega_g\int_{\mathrm{B}}^{\mathrm{Q}}\eta_g+\mathsf{P}^{\mathrm{P},\mathrm{A}}_{\mathrm{Q},\mathrm{B}} \tag{3.42}$$

が成り立つ.

証明 両辺に $\dfrac{\partial^2}{\partial z\partial x}$ を施したものを比較すると (いくらかの計算の後) 両者が等しいことがわかる. しかるに $\mathrm{P}=\mathrm{A}$ または $\mathrm{Q}=\mathrm{B}$ のとき元の両辺はともに 0 であるから, 実際に両辺は等しい. □

命題 3.43 ある定数成分の行列 $\Gamma=[c_{ij}]$ が存在して, 任意の P, Q, A, B $\in X_\circ$ に対して

$$\mathsf{R}^{\mathrm{P},\mathrm{A}}_{\mathrm{Q},\mathrm{B}}=\int_{\mathrm{A}}^{\mathrm{P}}\tau_{\mathrm{Q},\mathrm{B}}-2\sum_{i=1}^{g}\sum_{j=1}^{g}c_{ij}\int_{\mathrm{A}}^{\mathrm{P}}\omega_i\int_{\mathrm{B}}^{\mathrm{Q}}\omega_j \tag{3.44}$$

が成り立つ.

証明 $\mathsf{R}^{\mathrm{P},\mathrm{A}}_{\mathrm{Q},\mathrm{B}}-\int_{\mathrm{A}}^{\mathrm{P}}\tau_{\mathrm{Q},\mathrm{B}}$ は P の関数として正則であるから第 1 種微分形式の 1 次結合と定数の和で書き表せる. これは Q の関数と見ても同様である. また両辺ともに $\mathrm{P}=\mathrm{A}$ のとき 0 となり, $\mathrm{Q}=\mathrm{B}$ のときも 1.49 の第 2 式を使えば両辺が 0 となることがわかり, 与式が成り立たねばならない. □

以上の状況で,

$$R\big((x,y),(z,w)\big)\,dxdz=\frac{\mathscr{F}\big((x,y),(z,w)\big)}{(x-z)^2\frac{\partial}{\partial y}f(x,y)\frac{\partial}{\partial w}f(z,w)}dxdz \tag{3.45}$$

と書いたとき, $F\big((x,y),(z,w)\big)$ が x, y, z, w の Sato weight について斉重 (重さ $4g+2$) な多項式であることも容易にわかる. 上で得られた第 2 種微分形式 η_j の周期のなす行列を

$$[\,H'\ \ H''\,]=\left[\int_{\alpha_i}\eta_j\quad\int_{\beta_i}\eta_j\right]_{i,j=1,2,\cdots,g} \tag{3.46}$$

と記す. これと (3.13) の行列を結合して

$$M = \begin{bmatrix} \Omega' & \omega'' \\ H' & H'' \end{bmatrix} \tag{3.47}$$

と書く.

既に 1.37 において $\Omega(=[\Omega', \Omega''])$ について Riemann の関係式, 不等式を述べたが, ここでそれ少し別の形で再確認しておきたい. 上の M (3.26) の $R(\ ,\ )$ と ω_j と η_j と $[\ ,\ ]$ の関係から Ω', Ω'', H', H'' に間に symplectic な関係があることは予測される. いづれにしても, 実際には次が成り立つ.

補題 3.48　一般 Legendre 関係式 (Weierstrass relations)

$$M \begin{bmatrix} & -1_g \\ 1_g & \end{bmatrix} {}^tM = 2\pi\sqrt{-1} \begin{bmatrix} & -1_g \\ 1_g & \end{bmatrix} \tag{3.49}$$

を満たす. 特に 3.43 の記号で

$$\Gamma = -\frac{1}{2} H' \Omega'^{-1}, \tag{3.50}$$

かつ Γ は対称行列であり, ${\Omega'}^{-1}\Omega''$ は対称行列である. さらに, 良く知られてゐる様に

$$\mathrm{Im}\,({\Omega'}^{-1}\Omega'') \quad \text{は正定値行列} \tag{3.51}$$

となつてゐる (1.37 (2), または [FK], Chap.III など).

証明　等式 (3.42) と (3.44) より $\mathrm{P}(x, y)$ について,

$$\begin{aligned} &\int_{\mathrm{A}}^{\mathrm{P}} \{[\mathrm{P},\mathrm{Q}] - [\mathrm{P},\mathrm{B}]\} dx + \sum_{j=1}^{g} \int_{\mathrm{A}}^{\mathrm{P}} \omega_j \int_{\mathrm{B}}^{\mathrm{Q}} \eta_j \\ &\qquad = \int_{\mathrm{A}}^{\mathrm{P}} \tau_{\mathrm{Q},\mathrm{B}} - 2 \sum_{i=1}^{g} \sum_{j=1}^{g} c_{ij} \int_{\mathrm{A}}^{\mathrm{P}} \omega_i \int_{\mathrm{B}}^{\mathrm{Q}} \omega_j \end{aligned} \tag{3.52}$$

である. これを P における局所径数 t で微分すると, 1.47 から

$$\begin{aligned} &\{[\mathrm{P},\mathrm{Q}] - [\mathrm{P},\mathrm{B}]\} \frac{dx}{dt}\Big|_{t=0} + \sum_{j=1}^{g} \frac{x^{j-1}}{2y} \frac{dx}{dt}\Big|_{t=0} \int_{\mathrm{B}}^{\mathrm{Q}} \eta_j \\ &\qquad = \int_{\mathrm{B}}^{\mathrm{Q}} \eta_{\mathrm{P},t} - 2 \sum_{j=1}^{g} \sum_{j=1}^{g} c_{ij} \frac{x^{j-1}}{2y} \frac{dx}{dt}\Big|_{t=0} \int_{\mathrm{B}}^{\mathrm{Q}} \omega_j. \end{aligned} \tag{3.53}$$

次に各 $1 \le k \le g$ ごとに α_k の上に一点 B をとり, Q を B から α_k に沿って一周させると

$$\begin{aligned} &0 + H'\ {}^t \left[\frac{1}{2y} \frac{dx}{dt}\Big|_{t=0} \ \cdots\ \frac{x^{g-1}}{2y} \frac{dx}{dt}\Big|_{t=0} \right] \\ &\qquad = 0 - 2[c_{ij}]\Omega' \left[\frac{1}{2y} \frac{dx}{dt}\Big|_{t=0} \ \cdots\ \frac{x^{g-1}}{2y} \frac{dx}{dt}\Big|_{t=0} \right] \end{aligned} \tag{3.54}$$

を得る. P は任意であるから, これは

$$H'\,{}^t\left[\frac{1}{2y}dx \quad \cdots \quad \frac{x^{g-1}}{2y}dx\right] = -2[c_{ij}]\Omega'\,{}^t\left[\frac{1}{2y}dx \quad \cdots \quad \frac{x^{g-1}}{2y}dx\right] \tag{3.55}$$

を意味する. $\dfrac{1}{2y}dx, \cdots, \dfrac{x^{g-1}}{2y}dx$ は 1 次独立なので

$$H' = -2\Gamma\Omega' \tag{3.56}$$

でなければならず, 与式を得る. Γ の対称性は 1.49 と 3.43 の c_{ij} の定義からわかる. 次に

$$\mathsf{R}^{\mathrm{Q,B}}_{\mathrm{P,A}} = \mathsf{R}^{\mathrm{P,A}}_{\mathrm{Q,B}}$$

に注意すれば, (3.41) と (3.43) と 1.49 の第 1 式から

$$\mathsf{P}^{\mathrm{P,A}}_{\mathrm{Q,B}} + \sum_{j=1}^{g}\int_{\mathrm{A}}^{\mathrm{P}}\omega_j\int_{\mathrm{B}}^{\mathrm{Q}}\eta_j = \int_{\mathrm{B}}^{\mathrm{Q}}\tau_{\mathrm{A,P}} - 2\sum_{i=1}^{g}\sum_{j=1}^{g}c_{ij}\int_{\mathrm{A}}^{\mathrm{P}}\omega_j\int_{\mathrm{B}}^{\mathrm{Q}}\omega_j \tag{3.57}$$

が得られる. ここで, B から Q への積分路を β_k へと変形すれば

$$\int_{\mathrm{A}}^{\mathrm{P}} 0\,dx + \sum_{j=1}^{g}\int\omega_j\cdot H''_{jk} = \int_{\beta_k}\tau_{\mathrm{P,A}} - 2\sum_{i=1}^{g}\sum_{j=1}^{g}c_{ij}\int_{\mathrm{A}}^{\mathrm{P}}\omega_j\cdot\Omega''_{kj}, \tag{3.58}$$

従つて 1.49 の第 2 式より

$$+\sum_{j=1}^{g}\int\omega_j\cdot H''_{jk} = 2\pi\sqrt{-1}\int_{\mathrm{A}}^{\mathrm{P}}\hat{\omega}_j - 2\sum_{i=1}^{g}\sum_{j=1}^{g}c_{ij}\int_{\mathrm{A}}^{\mathrm{P}}\omega_j\cdot\Omega''_{kj}, \tag{3.59}$$

を得る. ここでさらに A から P へ至る積分路を α_i に近づけることで

$$\Omega' H'' = 2\pi\sqrt{-1}\,1_g - 2\Gamma\Omega'\Omega'' \tag{3.60}$$

となる. これに上の (3.56) を代入すれば

$$\Omega' H'' = 2\pi\sqrt{-1}\,1_g - 2(-\tfrac{1}{2}H')\Omega'^{-1}\Omega'\Omega'' \tag{3.61}$$

つまり

$$\Omega' H'' - \Omega'' H' = 2\pi\sqrt{-1}\,1_g \tag{3.62}$$

がわかる. □

4 Sigma 函数 (General case)

4.1 σ function for an (n,s)-curve

この節では, 一般の (d,s) 曲線 $C: f(x,y)=0$ について, σ 函数の定義を述べる. 曲線 C に付随する **sigma 函数**とは種数（$g=(d-1)(s-2)/2$）個の変数 $u_1, \cdots, u_g$ の整型函数であり, ここからほとんど全ての理論が構築される. いま

$$\delta = \begin{bmatrix} \delta' \\ \delta'' \end{bmatrix} \in \left(\tfrac{1}{2}\mathbb{Z}\right)^{2g} \tag{4.1}$$

を, C の基点を ∞ としたときの $[\Omega'\ \Omega'']$ に関して Riemann 定数を与へる theta characteristic ([Mu1], pp.163–166, または [BEL1], p.15, (1.19)) とする. 微分形式 (3.9) を見れば C の標準因子類 (canonical divisor class) は $2(g-1)\infty$ になつてゐることがわかるので, 任意の theta characteristic は $\left(\frac{1}{2}\mathbb{Z}\right)^{2g}$ に属する ([Mu1], p.166, Coroll. 3.11).

定義 4.2 曲線 C の discriminant D を以下の様に定める:

$$\begin{aligned} R_1 &= \mathrm{rslt}_x\big(\mathrm{rslt}_y\big(f(x,y), f_x(x,y)\big), \mathrm{rslt}_y\big(f(x,y), f_y(x,y)\big)\big), \\ R_2 &= \mathrm{rslt}_y\big(\mathrm{rslt}_x\big(f(x,y), f_x(x,y)\big), \mathrm{rslt}_x\big(f(x,y), f_y(x,y)\big)\big), \\ R_3 &= \gcd(R_1, R_2) \end{aligned} \tag{4.3}$$

とすると R_3 は

$$\mathbb{Z}[\lambda_{s-\lfloor s/d\rfloor d}, \cdots, \lambda_{ds}] \tag{4.4}$$

の中で平方元になる. そこで C discriminant を

$$D = \sqrt{R_3} \tag{4.5}$$

と定義する

定義 4.6 $a, b \in \mathbb{R}^g$ (縦ベクトル) と周期のなす行列 T に対して **指標付き theta 函数** を

$$\begin{aligned} \vartheta\begin{bmatrix} a \\ b \end{bmatrix}(z) &= \vartheta\begin{bmatrix} a \\ b \end{bmatrix}(z;T) \\ &= \sum_{n\in\mathbb{Z}^g} \exp\left[2\pi i\left\{\tfrac{1}{2}\ {}^t(n+a)T(n+a) + {}^t(n+a)(z+b)\right\}\right]. \end{aligned} \tag{4.7}$$

で定義する.

以上の準備の下で,

$$\begin{aligned} \sigma(u) &= \sigma(u;M) = \sigma(u_1, u_2, \cdots, u_g; M) \\ &= c\exp(-\tfrac{1}{2}uH'\Omega'^{-1}\ {}^tu)\vartheta[\delta]\left(\Omega'^{-1}\ {}^tu;\ \Omega'^{-1}\Omega''\right) \\ &= c\exp(-\tfrac{1}{2}uH'\Omega'^{-1}\ {}^tu) \\ &\qquad \times \sum_{n\in\mathbb{Z}^g} \exp\left[2\pi\sqrt{-1}\left\{\tfrac{1}{2}\ {}^t(n+\delta')\Omega'^{-1}\Omega''(n+\delta')\right.\right. \\ &\qquad\qquad \left.\left. +\ {}^t(n+\delta')(\Omega'^{-1}u+\delta'')\right\}\right] \end{aligned} \tag{4.8}$$

と定義する[8].

これは (3.51) により収束する. ここに

$$c = \frac{1}{\sqrt[8]{D}} \left(\frac{\pi^g}{|\Omega'|} \right)^{\frac{1}{2}} \tag{4.9}$$

である. 但し D は (4.2) で定義した判別式, π は円周率, $|\Omega'|$ は (3.14) の周期行列の行列式である. また 8 乗根の取り方は後の 6.19 で定める. この定数 c は一般化された Thomae の公式を利用して [Mu2], p.3.120, §8 の方法で決定されるのであるが, 以下ではあまり重要ではないので, ここでは省略する.

以下では, 与へられた $u \in \mathbb{C}^g$ に対して u' および u'' で

$$u = u'\Omega' + u''\Omega'' \tag{4.10}$$

となる $\mathbb{R}^g$ の元を示す. このとき $u, v \in \mathbb{C}^g$ と ℓ $(= \ell'\Omega' + \ell''\Omega'') \in \Lambda$ について

$$\begin{aligned} L(u,v) &:= {}^t u(H'v' + H''v''), \\ \chi(\ell) &:= \exp\left\{2\pi\sqrt{-1}\left({}^t\ell'\delta'' - {}^t\ell''\delta' + \tfrac{1}{2}{}^t\ell'\ell''\right)\right\} \ (\in \{1,-1\}) \end{aligned} \tag{4.11}$$

とおく. 以上の準備の下で $\sigma(u;M)$ の一般的な重要性質は次の様に述べられる ;

補題 4.12 あらゆる $u \in \mathbb{C}^g$ と $\ell \in \Lambda$, および $\gamma \in \mathrm{Sp}(2g,\mathbb{Z})$ について
(1) $\sigma(u+\ell;M) = \chi(\ell)\sigma(u;M)\exp L(u+\frac{1}{2}\ell,\ell)$,
(2) $\sigma(u;\gamma M) = \sigma(u;M)$, ($\gamma$ は定数 c に含まれる Ω' にも作用),
(3) $u \longmapsto \sigma(u;M)$ は $\kappa^{-1}(\Theta)$ に 1 位の零を持つ,
(4) また $\sigma(u;M) = 0 \iff u \in \kappa^{-1}(\Theta)$ が成り立つ.

証明 主張 (1) は [Ba1], p.286, ℓ.22 の特殊な場合に他ならない. 主張 (2) は γ による M の変換が (3.10) の積分路 α_j, β_j の取り換へに対応してゐることから (?) 示される. 詳しくは [BEL1], pp.10–15 を参照されたい. 主張 (3) と (4) は [Ba1], p.252 に解説されてゐる. また一部の主張は [BEL1] の p.12, Theorem 1.1 と p.15 にも解説されてゐる. □

注意 4.13 いま (3.49) と (3.51) を満たす行列 M が与へられたとき, $L(\ ,\ )$ の定める Riemann 形式 $E(u,v) = L(u,v) - L(v,u)$ の Pfaffian が 1 であることがわかるので (たとへば) [L], p.93, Th.4.1 により, 4.12(1) を満たすものは $\mathbb{C}$ 上 1 次元しかなく, それゆゑ, その自明でない解は (2), (3), (4) を自動的に満たす. つまり 4.12 は sigma 函数を定数倍を除いて, 特徴付けるものなのである. $g = 1$ のときの $\sigma(u)$ については Weierstraß によるの無限積表示

$$\sigma(u) = \prod_{\substack{\ell \in \Lambda \\ \ell \neq 0}} \left(1 - \frac{u}{\ell}\right) \exp\left(\frac{u}{\ell} + \frac{u^2}{2\ell^2}\right) \tag{4.14}$$

[8]函数 $\sigma(u)$ の定義 (4.8) において 3.26 の fundamental 2-forms of second kind を (3.30) で指定したものから別のものに取り換へ, それに応じて (3.46) の周期行列を再定義したならば, 対応する $\sigma(u)$ は指数函数の部分のみが変ることに注意されたい. ただし, その際に H' と H'' が変化するので, 2 次形式 $L(\ ,\ )$ も変更を受けることに注意.

があり, この $\sigma(u)$ は H' と H'' に依存しない形に書けてゐる. 一方, $g>1$ の場合は, H', H'' を元の H', H'' に Ω' や Ω'' の張る空間の元（weight homogeneousness を考慮した）を加へたものと置き代へると trivial theta が倍されるだけである.

次の事実の一般的な証明は正に中屋敷氏の報告 [N] の主結果であるので証明は省略する. $(3,4)$-curve の別証明が [EEMOP] にあるが, それは, このノートの最後 8.34 で述べる $\sigma(u)$ の満たす微分方程式に相当する物を先に導出する方法によつてゐるのでやや複雑である.

命題 4.15 函数 $\sigma(u)$ を $u_1,\cdots,u_g$ の冪級数に展開するとき,

$$\sigma(u)\in\mathbb{Q}[\mu_{ds-\lfloor s/d\rfloor d},\cdots,\mu_{ds}][[u_1,u_2,\cdots,u_g]] \tag{4.16}$$

であつて, その weight は $(s^2-1)(d^2-1)/24$ 次で斉重である

補題 4.17 $\sigma(u)$ は奇函数または偶函数である. つまり

$$\sigma([-1]u)=-(-1)^{(d^2-1)(s^2-1)/24}\sigma(u) \tag{4.18}$$

が成り立つ.

証明 周期格子について $[-1]\Lambda=\Lambda$ が成り立つ. これは各周期 $\ell\in\Lambda$ を与へる積分の積分路を逆にした積分を考へればよい. このことと 4.13 とを合はせれば, 定数 K が存在して

$$\sigma([-1]u)=K\sigma(u) \tag{4.19}$$

となることがわかる. あとは後述の 6.19 を考慮することで $K=-1$ であることがわかる. □

以後では,

$$\sigma_j(u)=\frac{\partial}{\partial u_j}\sigma(u),\quad \sigma_{ij}(u)=\frac{\partial^2}{\partial u_i\partial u_j}\sigma(u) \tag{4.20}$$

などと略記する.

5 超楕円曲線に付随する σ 函数と $\wp$ 函数

5.1 超楕円函数についての Riemann 定数と判別式

ここでは 2.14 の式を後に述べる後述の 5.24 に変形する.

Riemann 定数

超楕円的 Riemann 面の場合は Riemann の定数はつぎのようになる.

定理 5.1 X を前節 3 で定義された超楕円的 Riemann 面とせよ. このとき Riemann の定数 K (2.8) は

$$K = \sum_{j=1}^{g} \int_{\infty}^{\mathrm{A}_j} \hat{\omega} \tag{5.2}$$

で与えられる.

証明 以下

$$\hat{w}_j(\mathrm{P}) = \int_{\infty}^{\mathrm{P}} \omega_j \tag{5.3}$$

と書く. (2.7) から

$$\begin{aligned} K_i &= -\frac{1}{2}T_{ii} - \hat{w}_i(\alpha_j \text{ の始点}) + \sum_{j=1}^{g} \int_{\alpha_j} \hat{w}_i(\mathrm{P})\hat{\omega}_j(\mathrm{P}) \\ &\equiv -\frac{1}{2}\tau_{ii} - \frac{1}{2}\int_{\alpha_i} \hat{\omega}_i + \sum_{j=1}^{g} \int_{\alpha_j} \hat{w}_i(\mathrm{P})\hat{\omega}_j(\mathrm{P}) \mod \hat{\Lambda}. \end{aligned} \tag{5.4}$$

まず $j = i$ については

$$\begin{aligned} \int_{\alpha_j} \hat{w}_j(\mathrm{P}) d\hat{w}_j =& \frac{1}{2}\int_{\alpha_j} d(\hat{w}_j(\mathrm{P}))^2 \\ =& \frac{1}{2}\{\hat{w}_j(\alpha_j \text{ の始点})^2 - \hat{w}_j(\alpha_j \text{ の終点})^2\}. \end{aligned} \tag{5.5}$$

ここで X 上では α_j の終点は α_j の始点であり, $\int_{\alpha_j} \hat{\omega}_j = 1$ であるから,

$$\begin{aligned} =& \frac{1}{2}\{\hat{w}_j(\alpha_j \text{ の始点})^2 - (\hat{w}_j(\alpha_j \text{ の始点}) - 1)^2\} \\ =& \hat{w}_j(\alpha_j \text{ の始点}) - \frac{1}{2}. \end{aligned} \tag{5.6}$$

$j \neq i$ のときは,

$$\int_{\alpha_j} \hat{w}_i(\mathrm{P})\hat{\omega}_j(\mathrm{P}) = \int_{\mathrm{C}_j}^{\mathrm{A}_j} \left(\hat{w}_i(\mathrm{P}) + \hat{w}_i(\overline{\mathrm{P}})\right) \hat{\omega}_j(\mathrm{P}). \tag{5.7}$$

ここで $d(\hat{w}_i(\mathrm{P}) + \hat{w}_i(\overline{\mathrm{P}})) = \hat{\omega}_i(\mathrm{P}) + \hat{\omega}_i(\overline{\mathrm{P}}) = 0$ なので $\hat{w}(\mathrm{P}) + \hat{w}(\overline{\mathrm{P}})$ は定数 $(= 2\hat{w}_i(\mathrm{A}_j))$ である. また $\int_{\mathrm{C}_j}^{\mathrm{A}_j} \hat{\omega}_j = \frac{1}{2}\int_{\alpha_j} \hat{\omega}_j = \frac{1}{2}$ なので

$$= \hat{w}_i(\mathrm{A}_j) = \int_{\infty}^{\mathrm{A}_j} \hat{\omega}_i \tag{5.8}$$

となって目的の結果が得られた. □

補題 5.9 2.12 に言ふ A_j は (3.5) の超楕円曲線 X については $\mathrm{A}_j(a_j, 0)$ である.

補題 5.10 いま

$$\delta'' = {}^t\left[\tfrac{1}{2} \quad \cdots \quad \tfrac{1}{2}\right], \quad \delta' = {}^t\left[\tfrac{g}{2} \quad \tfrac{g-1}{2} \quad \cdots \quad \tfrac{1}{2}\right] \tag{5.11}$$

とするとき, $\mathrm{A}_j(a_j, 0)$ に対して

$$\sum_{j=1}^{g} \int_{\infty}^{\mathrm{A}_j} \hat{\omega} = \delta' + T\delta'' \quad \left(\text{あるいは} \ \sum_{j=1}^{g} \int_{\infty}^{\mathrm{A}_j} \omega = \Omega'\delta' + \Omega''\delta''\right) \tag{5.12}$$

が成り立つ.

証明 $\mathrm{C}(c, 0)$ とする. 下の図を参考にして まづ

$$\int_{\mathrm{C}}^{\mathrm{A}_g} \hat{\omega} = -\frac{1}{2}\int_{\beta_g} \hat{\omega} = T\,{}^t\left[0 \quad 0 \quad \cdots \quad \frac{1}{2}\right]. \tag{5.13}$$

$j \neq g$ のとき

$$\begin{aligned} \int_{\mathrm{C}}^{\mathrm{A}_j} \hat{\omega} &= -\frac{1}{2}\int_{\beta_j} \hat{\omega} - \frac{1}{2}\sum_{i=j+1}^{g} \int_{\alpha_i} \hat{\omega} \\ &= {}^t\Big[0 \quad 0 \quad \cdots \quad 0 \quad \underset{j}{\tfrac{1}{2}} \quad \cdots \quad -\tfrac{1}{2}\Big] + T\,{}^t\Big[0 \quad \cdots \quad \underset{j}{\tfrac{1}{2}} \quad \cdots \quad 0\Big]. \end{aligned} \tag{5.14}$$

また

$$\int_{\infty}^{\mathrm{C}} \hat{\omega} = \tfrac{1}{2}\sum_{j=1}^{g} \int_{\alpha_j} \hat{\omega} = {}^t\left[\tfrac{1}{2} \quad \cdots \quad \tfrac{1}{2}\right]. \tag{5.15}$$

以上より

$$\int_{\infty}^{\mathrm{A}_j} \hat{\omega} = {}^t\Big[\tfrac{1}{2} \quad \cdots \quad \underset{j}{\tfrac{1}{2}} \quad 0 \quad \cdots \quad 0\Big] + T\,{}^t\Big[0 \quad \cdots \quad \underset{j}{\tfrac{1}{2}} \quad \cdots 0\Big]. \tag{5.16}$$

したがって与式が得られる. □

判別式

超楕円曲線の場合の discriminant は以下の様になる.

補題 5.17 超楕円曲線 $y^2 = f(x)$ について, 4.2 で定義した discriminant R_3 は $f(x) = 0$ の g 個の根の差積の平方に一致する.

5.2 Sigma function for a hyperelliptic curve

定義 5.18 我々の超楕円的 Riemann 面 X に対し, σ **函数** を

$$\sigma(u) = \sigma(u; X) = \ c\exp(-\tfrac{1}{2}\,{}^t\!uH'\Omega'^{-1}u)\vartheta\begin{bmatrix}\delta''\\ \delta'\end{bmatrix}(\Omega'^{-1}u;\ T) \tag{5.19}$$

で定義する. 定数 c は 4.9 で定義したものである.

命題 5.20 $\sigma(u)$ は $\lfloor (g+1)/2 \rfloor$ の偶奇に応じて偶函数か奇函数である.

定理 2.9 を σ 函数に訳せば $\sigma(u)$ の零点集合は丁度 $\Theta + \Lambda$ になっていることがわかる.

定理 5.21 P_j, $\mathrm{Q}_j \in X$, $(j = 1, \cdots, g)$, に対して

$$u = \sum_{j=1}^{g} \int_{\infty}^{\mathrm{P}_j} \omega, \quad u' = \sum_{j=1}^{g} \int_{\infty}^{\mathrm{Q}_j} \omega \tag{5.22}$$

とおくとき

$$\exp\left(\sum_{j=1}^{g} \mathsf{R}^{\mathrm{P,Q}}_{\mathrm{P}_j,\mathrm{Q}_j}\right) = \frac{\sigma\Big(\displaystyle\int_{\infty}^{\mathrm{P}} \omega - u\Big)\sigma\Big(\displaystyle\int_{\infty}^{\mathrm{Q}} \omega - u'\Big)}{\sigma\Big(\displaystyle\int_{\infty}^{\mathrm{P}} \omega - u'\Big)\sigma\Big(\displaystyle\int_{\infty}^{\mathrm{Q}} \omega - u\Big)} \tag{5.23}$$

が成り立つ.

$g = 1$ のときは [Ta], p.187, ℓ.5-6 がほぼこの式にあたる.

証明 点 $\mathrm{A}_j(a_j, 0)$ に対し

$$\begin{aligned}
&\sum_{r,s} c_{rs}\left(\int_{\mathrm{A}}^{\mathrm{P}} \omega_r - \sum_{j=1}^{g}\int_{\mathrm{A}_j}^{\mathrm{P}_j} \omega_r\right)\left(\int_{\mathrm{A}}^{\mathrm{P}} \omega_s - \sum_{j=1}^{g}\int_{\mathrm{A}_j}^{\mathrm{P}_j} \omega_s\right)\\
&-\sum_{r,s} c_{rs}\left(\int_{\mathrm{A}}^{\mathrm{Q}} \omega_r - \sum_{j=1}^{g}\int_{\mathrm{A}_j}^{\mathrm{P}_j} \omega_r\right)\left(\int_{\mathrm{A}}^{\mathrm{Q}} \omega_s - \sum_{j=1}^{g}\int_{\mathrm{A}_j}^{\mathrm{P}_j} \omega_s\right)\\
&+\sum_{r,s} c_{rs}\left(\int_{\mathrm{A}}^{\mathrm{P}} \omega_r - \sum_{j=1}^{g}\int_{\mathrm{A}_j}^{\mathrm{Q}_j} \omega_r\right)\left(\int_{\mathrm{A}}^{\mathrm{P}} \omega_s - \sum_{j=1}^{g}\int_{\mathrm{A}_j}^{\mathrm{Q}_j} \omega_s\right)\\
&-\sum_{r,s} c_{rs}\left(\int_{\mathrm{A}}^{\mathrm{Q}} \omega_r - \sum_{j=1}^{g}\int_{\mathrm{A}_j}^{\mathrm{Q}_j} \omega_r\right)\left(\int_{\mathrm{A}}^{\mathrm{Q}} \omega_s - \sum_{j=1}^{g}\int_{\mathrm{A}_j}^{\mathrm{Q}_j} \omega_s\right)\\
&= 2\sum_{j=1}^{g}\sum_{r,s} c_{rs}\int_{\mathrm{Q}}^{\mathrm{P}} \omega_r \int_{\mathrm{Q}_j}^{\mathrm{P}_j} \omega_s\\
&= \sum_{j=1}^{g}\Big(\mathsf{R}^{\mathrm{P,Q}}_{\mathrm{P}_j,\mathrm{Q}_j} - \int_{\mathrm{Q}}^{\mathrm{P}} \tau_{\mathrm{P}_j,\mathrm{Q}_j}\Big)
\end{aligned} \tag{5.24}$$

最後の等号は 3.43 による. これの指数函数を取り, それを (2.16) の式の両辺に掛ける. このとき 3.50, 5.10 および σ 函数の定義 5.18 から与式が導かれる. □

注意 5.25 もし P_j, Q_j を $\overline{\mathrm{P}_j}$, $\overline{\mathrm{Q}_j}$ と入れ替えるならば, 対応する積分の符号が逆転する.

5.3 σ 函数の変換公式

$u \in \mathbb{C}^g$ に対し, 記号 u', u'' でもって

$$u = \Omega' u' + \Omega'' u'', \tag{5.26}$$

となるような $\mathbb{R}^g$ の元を表すことにする. さらに $\mathbb{C}$ に値を持つ $\mathbb{R}$-双線型形式 $L(\quad,\quad)$ を

$$L(u,v) = {}^t u(H'v' + H''v''), \quad (u, v \in \mathbb{C}^g) \tag{5.27}$$

で定める. 格子点 $\ell = \Omega'\ell' + \Omega''\ell'' \in \Lambda$ に対し

$$\chi(\ell) = \exp[2\pi i({}^t\ell'\delta'' - {}^t\ell''\delta') - \pi i {}^t\ell'\ell''], \tag{5.28}$$

ここに δ' および δ'' は 5.10 で定義したものである.

補題 5.29 (変換公式) σ 函数 $\sigma(u)$ は任意の $u \in \mathbb{C}^g$ と $\ell \in \Lambda$ について

$$\sigma(u+\ell) = \chi(\ell)\sigma(u)\exp L(u + \tfrac{1}{2}\ell, \ell) \tag{5.30}$$

を満たす.

証明 もちろん平行移動公式 (2.3) を変形するのであるが, ここでは [Ba1], p.286, ℓ.21 を参照されたい. □

以下のことはあとでする $\wp$ 函数の定義には必要でないが参考までに述べておく. まづ

$$E(u,v) = L(u,v) - L(v,u), \quad (u, v \in \mathbb{C}^g) \tag{5.31}$$

とおくと明らかに $E(\quad,\quad)$ は $\mathbb{C}$ に値をとる $\mathbb{R}$ 上の双線型形式で $E(u,v) = -E(v,u)$ をみたす. この $E(\quad,\quad)$ を $\sigma(u)$ の **Riemann 形式** とよぶ.

補題 5.32 次が成り立つ:
(1) $E(iu, v) = E(iv, u)$.
(2) $E(u,v) = 2\pi i({}^t u'v'' - {}^t u''v')$.
特に $E(\quad,\quad)$ は一般に $i\mathbb{R}$ に値をとり $\Lambda \times \Lambda$ 上では $2\pi i\mathbb{Z}$ 値をとる.

証明 (1) は [L], p.85, Theorem 1.2 に示されている.
(2) を示そう.

$$\begin{aligned} E(u,v) =& L(u,v) - L(v,u) \\ =& {}^t u(H'v' + H''v'') - {}^t v(H'u' + H''u'') \\ =& {}^t uH'v' + {}^t uH''v'' - {}^t vH'u' - {}^t vH''u'' \\ =& {}^t u {}^t\Omega'^{-1t}\Omega' H'v' + {}^t u {}^t\Omega''^{-1t}\Omega'' H''v'' \\ & - {}^t v {}^t\Omega'^{-1t}\Omega' H'u' - {}^t v {}^t\Omega''^{-1t}\Omega'' H''u''. \end{aligned} \tag{5.33}$$

ここで, (3.49) より ${}^t\Omega' H'$ と ${}^t\Omega'' H''$ は対称行列である. ゆゑに

$$
\begin{aligned}
&= {}^t v'^t\Omega' H' \Omega'^{-1} u + {}^t v'^t\Omega'' H'' \Omega''^{-1} u - {}^t u'^t\Omega' H' \Omega'^{-1} v - {}^t u''^t\Omega'' H'' \Omega''^{-1} v \\
&= {}^t v'^t\Omega' H' (u' + Tu'') + {}^t v'^t\Omega'' H'' (T^{-1}u' + u'') \\
&\quad - {}^t u'^t\Omega' H' (v' + Tv'') - {}^t u''^t\Omega'' H'' (T^{-1}v' + v'').
\end{aligned} \tag{5.34}
$$

また ${}^t\Omega' H'$ と T も対称行列だから

$$
\begin{aligned}
{}^t\Omega' H' T &= {}^t T {}^t\Omega' H' = {}^t\Omega''^t\Omega'^{-1t}\Omega' H' = {}^t\Omega'' H', \\
{}^t\Omega'' H'' T &= {}^t T {}^t\Omega'' H'' = {}^t\Omega'^t\Omega''^{-1t}\Omega'' H'' = {}^t\Omega' H''
\end{aligned} \tag{5.35}
$$

であり, ${}^t\Omega'' H'$ と ${}^t\Omega' H''$ も対称行列である. したがって, 再び ${}^t\Omega' H'$ と ${}^t\Omega'' H''$ が対称行列であることと一般の Legendre 関係式 (3.49) ${}^t\Omega' H'' - {}^t\Omega'' H' = 2\pi i 1_g$ を用いて

$$
\begin{aligned}
&= {}^t u'^t\Omega' H' v' + {}^t u''^t\Omega'' H' v' + {}^t u'^t\Omega' H'' v'' + {}^t u''^t\Omega'' H'' v'' \\
&\quad - {}^t v'^t\Omega' H' u' - {}^t v''^t\Omega'' H' u' - {}^t v'^t\Omega' H'' u'' - {}^t v''^t\Omega'' H'' u'' \\
&= 2\pi i ({}^t u' v'' - {}^t u'' v').
\end{aligned} \tag{5.36}
$$

□

5.4 $\wp$ 函数の定義

いよいよ $\wp$ 函数の定義である.

定義 5.37 我々は

$$
\wp_{ij}(u) = -\frac{\partial^2}{\partial u_i \partial u_j} \log \sigma(u) = \frac{\sigma_i(u)\sigma_j(u) - \sigma_{ij}(u)\sigma(u)}{\sigma(u)^2} \tag{5.38}
$$

と定め, これを $\wp$ **函数** とよぶ. ここで $\sigma_i(u) = \dfrac{\partial}{\partial u_i}\sigma(u)$, $\sigma_{ij}(u) = \dfrac{\partial}{\partial u_i}\sigma_j(u)$ である. 変換公式から σ 函数は u を $u + \ell$ ($\ell \in \Lambda$) に変えても u_i の 1 次式の指数函数がかかるだけであるが, $\wp$ 函数は σ 函数の対数をとって 2 回微分しているのでそのような指数函数の部分は消えてしまう. したがって $\wp_{ij}(u)$ は Λ を周期とする周期函数であることがわかる. また 4.12 から $\wp_{ij}(u)$ は Θ で 2 位の極を持ち, それ以外では正則であることがわかる. このことは普通 $\wp_{ij}(u) \in \Gamma(J, \mathscr{O}(2\Theta))$ とかかれる.

命題 5.39 $\wp_{ij}(u)$ は偶函数である.

補題 5.40 $\mathrm{P}_j(x_j, y_j)$ $(j = 1, \cdots, g)$ と $\mathrm{P}(x, y)$ に対して

$$
v = {}^t[v_1, \cdots, v_g] = \int_\infty^{\mathrm{P}} \omega + \sum_{j=1}^{g} \int_\infty^{\mathrm{P}_j} \omega \tag{5.41}
$$

とおくとき

$$
4y_r y \frac{\partial^2}{\partial x_r \partial x} = \sum_{i=1}^{g}\sum_{j=1}^{g} x_r^{i-1} x^{j-1} \frac{\partial^2}{\partial v_i \partial v_j}. \tag{5.42}
$$

証明 Jacobi の定理 1.84 により, P, P_1, $\cdots$, P_g が動くとき v_1, $\cdots$, v_g は $\mathbb{C}^g$ 全体を動くことに注意する. このとき

$$\begin{aligned}\frac{\partial^2}{\partial x_r \partial x} =& \frac{\partial}{\partial x_r}\left(\sum_{i=1}^{g}\frac{\partial v_i}{\partial x}\frac{\partial}{\partial v_i}\right)\\ =& \sum_{i=1}^{g}\left[\frac{\partial^2 v_i}{\partial x_r \partial x}\frac{\partial}{\partial v_i}+\frac{\partial v_i}{\partial x_r}\left(\sum_{j=1}^{g}\frac{\partial v_j}{\partial x}\frac{\partial^2}{\partial v_i \partial v_j}\right)\right]\\ =& \sum_{i=1}^{g}\sum_{j=1}^{g}\frac{x_r^{i-1}}{2y_r}\frac{x^{j-1}}{2y}\frac{\partial^2}{\partial v_i \partial v_j}.\end{aligned} \tag{5.43}$$

この両辺に $4y_r y$ を掛ければよい. □

次の関係式は, 第 8 節でも Jacobi 多様体の定義方程式系を美しく構成するのに使はれる非常に重要なものである. $g=1$ の場合は $\wp(u)$ の代数的加法公式であつて, 竹内 [Ta] の p.142, $\ell.-2$ の式に他ならない.

定理 5.44 $F(x,z)$ は (3.35) で定義したものとする.

$$\frac{F(x_r,x)+2y_r y}{(x_r-x)^2}=\sum_{i=1}^{g}\sum_{j=1}^{g}\wp_{ij}\left(\int_{\infty}^{\mathrm{P}}\omega-u\right)x_r^{i-1}x^{j-1} \tag{5.45}$$

証明 まづ, $\mathrm{P}(x,y)$, $\mathrm{P}_j(x_j,y_j)$, $\mathrm{Q}_j\in X$ について

$$\begin{aligned}2y_j\frac{\partial}{\partial x_j}\mathsf{R}^{\mathrm{P},\mathrm{Q}}_{\mathrm{P}_j,\mathrm{Q}_j}&=\int_{\mathrm{Q}}^{\mathrm{P}}\frac{F(x,x_j)-2yy_j}{4(x-x_j)^2}\frac{dx}{2y},\\ 4yy_j\frac{\partial^2}{\partial x\partial x_j}\mathsf{R}^{\mathrm{P},\mathrm{Q}}_{\mathrm{P}_j,\mathrm{Q}_j}&=\frac{F(x,x_j)-2yy_j}{4(x-x_j)^2}\end{aligned} \tag{5.46}$$

であることに注意する (右辺の分子が差になっている！). (5.43) の作用素を (5.23) の両辺の対数にそれぞれ施せば, 所望の式を得る. □

定理 5.47 いま X 上の g 個の点 (x_1,y_1), $\cdots$, (x_g,y_g) について

$$u=\sum_{j=1}^{g}\int_{\infty}^{(x_j,y_j)}\omega \tag{5.48}$$

とおく. このとき

$$\sum_{i=1}^{g}\sum_{j=1}^{g}\wp_{ij}(u)x_r^{i-1}x_s^{j-1}=\frac{F(x_r,x_s)-2y_r y_s}{(x_r-x_s)^2},\qquad x_r^g-\sum_{j=1}^{g}\wp_{jg}(u)x_r^{j-1}=0 \tag{5.49}$$

が任意の (x_r,y_r) と (x_s,y_s) $(r,s=1,\cdots,g)$ について成り立つ. 特に, 第 2 式より

$$(-1)^{g-j}\wp_{jg}(u)=\text{“}x_1,\cdots,x_g\text{ の }g-j+1\text{ 次基本対称式”} \tag{5.50}$$

である.

証明 基本関係式 (5.45) において, $g \geq 2$ のときは $\mathrm{P} \to \overline{\mathrm{P}_r}$ としたあとで $\mathrm{P}_s \to \infty$ とすれば求める最初の式が得られる. また両辺を x^{g-1} で割ったあとで $\mathrm{P} \to \infty$ とするとき, $F(x_r, x)$ の x についての最高次の項は $x_r^g x^{g+1}$ であり $\dfrac{y}{x^{g-1+2}} \to 0$ であるから求める第 2 の式が得られる. □

定理 5.51 函数 $\sigma(u)$ を $u_1, \cdots, u_g$ の冪級数に展開するとき,

$$\sigma(u) \in \mathbb{Q}[\lambda_2, \cdots, \lambda_{4g+2}][[u_1, u_2, \cdots, u_g]] \tag{5.52}$$

であつて, その weight は $g(g+1)/2$ 次で斉重である

証明 まづ (5.49) を $\wp_{ij}(u)$ の方程式と見れば, それを解くことにより, $\wp_{ij}(u)$ の (x_1, y_1), $\cdots$, (x_g, y_g) による表示が得られるわけだが, 方程式が斉重なので, $\wp_{ij}(u)$ も斉重でなければならない. それゆゑ $\sigma(u)$ も斉重である. その weight については方程式 (5.49) の weight および $\wp_{ij}(u)$ と $\sigma(u)$ の関係から $g(g+1)/2$ 次であるとわかる. 前半は (5.49) と後の 8.34 を併用して, 帰納的に証明される. □

6 退化 σ 函数

6.1 The Schur-Weierstrass Polynomial

ここでは Schur-Weierstraß多項式についての基礎事項をまとめる. 主な文献は [Ma] and [BEL2].

しばらくは g は単なる正整数であると考へる. $u_g^{(1)}, \cdots, u_g^{(g)}$ は不定元とする. 整数 n $(0 \leqq n \leqq g)$ を固定する. 以下では単に $\boldsymbol{u}_g$ と書いて, 変数 $u_g^{(1)}, \cdots, u_g^{(n)}$ の集合, あるいはこれらを成分とする vector を表はすことにする.

各 $k \geqq 0$ に対して $(-1)^k U_k^{[n]}(\boldsymbol{u}_g)$ は k **次の完全対称式** (complete symmetric polynomial) を表すものとする. 即ち, それは変数 $u_g^{(1)}, \cdots, u_g^{(n)}$ の, 全次数が k なる全ての単項式の単純和である. 我々は, それが n 変数であることを添字 $[n]$ を付けて表すのである. もし $k < 0$ であれば, $U_k^{[n]}(\boldsymbol{u}_g)$ は 0 であると見做すことにする.

さて, 行列式

$$|U^{[g]}_{g-2i+j+1}(\boldsymbol{u}_g)|_{1 \leqq i,j \leqq g}. \tag{6.1}$$

を考へる. いま単に $U_k = U_k^{[g]}(\boldsymbol{u}_g)$ と書けば $k < 0$ なら $U_k = 0$ なので, この行列式は具体的には

$$\begin{vmatrix} U_g & U_{g+1} & U_{g+2} & \cdots & U_{2g-2} & U_{2g-1} \\ U_{g-2} & U_{g-1} & U_g & \cdots & U_{2g-4} & U_{2g-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ U_1 & U_2 & U_3 & \cdots & * & * \\ & U_0 & U_1 & \cdots & * & * \\ & & & \ddots & \vdots & \vdots \\ & & & & U_0 & U_1 \end{vmatrix} \qquad (g \text{ が奇数のとき}) \tag{6.2}$$

$$
(6.3)\qquad
\begin{vmatrix}
U_g & U_{g+1} & U_{g+2} & U_{g+3} & \cdots & U_{2g-2} & U_{2g-1} \\
U_{g-2} & U_{g-1} & U_g & U_{g+1} & \cdots & U_{2g-4} & U_{2g-3} \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
U_0 & U_1 & U_2 & U_3 & \cdots & * & * \\
 & & U_0 & U_1 & \cdots & * & * \\
 & & & & \ddots & \vdots & \vdots \\
 & & & & & U_0 & U_1
\end{vmatrix}
\qquad (g \text{ が偶数のとき})
$$

と書かれる. 以下においては

$$
(6.4)\qquad
\begin{aligned}
p_j &:= (u_g^{(1)})^j + \cdots + (u_g^{(g)})^j, \\
u_j^{(i)} &:= \tfrac{1}{2(g-j)+1}(u_g^{(i)})^{2(g-j)+1}, \\
u^{(i)} &:= (u_1^{(i)}, \cdots, u_g^{(i)}), \\
u_j &:= u_j^{(1)} + u_j^{(2)} + \cdots + u_j^{(g)} = \tfrac{1}{2(g-j)+1} p_{2(g-j)+1}, \\
u &:= u^{(1)} + u^{(2)} + \cdots + u^{(g)} = (u_1, u_2, \cdots, u_g)
\end{aligned}
$$

と記す. ここで, $|U^{[g]}_{g-2i+j+1}(\boldsymbol{u}_g)|_{1\leqq i,j\leqq g}$ が [BEL2] の $S_{2,2g+1}$ に他ならないことを説明しておく. その為に, 新たな変数 s_1, s_2, $\cdots$, s_{2g-1} を用意し, これらは

$$
(6.5)\qquad p_j = -{s_1}^j - {s_2}^j - \cdots - {s_{2g-1}}^j, \quad (1 \leqq j \leqq 2g-1)
$$

を満すものとする. 実際, この様な s_j は以下の理由から存在する. まづ, $\varepsilon_k(\boldsymbol{s})$ ($\boldsymbol{s} = (s_1, s_2, \cdots, s_{2g-1})$) で s_j 達の k 次の基本対称式とするとき (6.5) を満たす s_1, s_2, $\cdots$, s_{2g-1} は

$$
(6.6)\qquad
\varepsilon_k(\boldsymbol{s}) = \frac{1}{k!}
\begin{vmatrix}
-p_1 & 1 & & & \\
-p_2 & -p_1 & 2 & & \\
\vdots & \vdots & \vdots & \ddots & \\
-p_{k-1} & -p_{k-2} & -p_{k-3} & \cdots & k-1 \\
-p_k & -p_{k-1} & -p_{k-2} & \cdots & -p_1
\end{vmatrix}
= (-1)^k U_k^{[g]}(\boldsymbol{u}_g)
$$

の解に他ならない. このことは [Ma], p.29, $\ell.-4$ と p.28, ℓ.13 に書かれてゐる. 代数方程式の基本的な定理からこの方程式系はいつも解を持つ. よつて, $|U_k^{[g]}(\boldsymbol{u}_g)|$ が [BEL2] の Theorem 4.3 の Schur-Weierstrass 多項式 $S_{2,2g+1}(-p_1, -p_3, \cdots, -p_{2g-1})$ に他ならないことがわかつた.

注意 6.7 ここで, 我々の記号 u_j は [BEL2] の記号 z_j と少し異なり, $z_j = -(2j-1)u_{g-j+1}$ であることを注意しておく. さらに積分 (5.47) と [BEL2] の definition (5.3) とは積分の方向と乗定数が異なるこにも注意して欲しい.

多項式 $|U^{[g]}_{g-2i+j+1}(\boldsymbol{u}_g)|$ の値はもちろん $u_g^{(1)}$, $\cdots$, $u_g^{(g)}$ によつて定まるが, 実は次のことが成り立つ.

命題 6.8 上の多項式 $|U^{[g]}_{g-2i+j+1}(\boldsymbol{u}_g)|_{1\leqq i,j\leqq g}$ は上に定義した g 個の値 $-p_1, -p_3, \cdots, -p_{2g-1}$ だけで定まる. つまり $u_1, u_2, \cdots, u_g$ の値だけにより定まる.

証明 [BEL2] の p.86 の Theorem 4.1 を参照されたい. □

ここでは

$$S(u) := |U^{[g]}_{g-2i+j+1}(\boldsymbol{u}_g)|_{1\leqq i,j\leqq g}. \tag{6.9}$$

と書いて, これを **Schur-Weierstrass 多項式**と呼ぶ.

ここで, 上の変数について u_j の重さを $2(g-j)+1$ とする**重さ**を定義することができる. これを **Sato weight** と呼ぶことがある. このとき $S(u)$ はこの重さに関して $\frac{1}{2}g(g+1)$ 次の斉重となる.

いま m を正の整数として固定し, $\xi_1, \cdots, \xi_m$ を不定元とする. 不定元 $\xi_1, \cdots, \xi_m$ についての全次数 k の単項式の単純和の $(-1)^k$ 倍を $U^{[m]}_k(\xi)$ と記す. ここで ξ は $\xi_1, \cdots, \xi_m$ の全体を略記したものである.

定義 6.10 上の様に m, ξ_i および $U^{[m]}_k(\xi)$ を定める. どの行も両方向数列

$$\cdots, 0, 0, 1, U^{[m]}_1(\xi), U^{[m]}_2(\xi), \cdots \tag{6.11}$$

の連続した $(m+1)$ 項である様な行列 M について, それが

$$0, \cdots, 0, 0, 1 \tag{6.12}$$

なる行を含まないとき, M を $\xi_1, \cdots, \xi_m$ に関する**単純な行を持たない基本行列**（fundamental matrix without a simple row）であるといふ.

補題 6.13 正整数 m について, $\xi_1, \cdots, \xi_m$ と $U^{[m]}_k(\xi)$ は上の通りであるとする. いま M は $\xi_1, \cdots, \xi_m$ に関する単純な行を持たない基本行列であるとする. さらに $\varepsilon_j(\xi)$ で $\xi_1, \cdots, \xi_m$ の j 次基本対称式を表す. このとき

$$M \begin{bmatrix} \varepsilon_m(\xi) \\ \varepsilon_{m-1}(\xi) \\ \vdots \\ \varepsilon_1(\xi) \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{bmatrix} \tag{6.14}$$

となる.

証明 [Ma], p.21, (2.6′) を参照. □

次の事実はこの本では使はれないが, Riemann singularity theorem に深く関係するものであるからここに述べておく.

補題 6.15 $S(u)$ は変数 $u^{(1)}_g, \cdots, u^{(g-1)}_g, u^{(g)}_g$ についての多項式として $u^{(g)}_g = 0$ のとき恒等的に消える:

$$S(u^{(1)} + \cdots + u^{(g-1)}) = 0. \tag{6.16}$$

証明 これは 6.13 で $m = g-1$ とし M として, (6.9) の右辺の中の行列を取れば良い. □

注意 6.17 いくつかの例を挙げておく.
(1) $g = 1$ のとき $S(u) = u$.
(2) $g = 2$ のとき $S(u_1, u_2) = u_1 - \frac{1}{3}{u_2}^3$.
(3) $g = 3$ のとき $S(u_1, u_2, u_3) = {u_2}^2 - u_1 u_3$.
(4) $g = 4$ のとき

$$S(u_1,u_2,u_3,u_4) = \tfrac{1}{4725}{u_4}^{10} - \tfrac{1}{105}u_3{u_4}^7 + \tfrac{1}{15}u_2{u_4}^5 - \tfrac{1}{3}u_1{u_4}^3 + u_2u_3{u_4}^2 - {u_1}^3u_4 + (u_1u_3 - {u_2}^2). \tag{6.18}$$

定理 6.19 $\sigma(u)$ の u_j 達に関する冪級数展開は

$$\mathbf{Q}[\mu_2, \mu_4, \cdots, \mu_{4g+2}][[u_1, u_2, \cdots, u_g]] \tag{6.20}$$

に属し, 1 の 8 乗根 ε が存在して

$$\sigma(u) = \varepsilon\, S(u) + \text{“higher terms of } \mu_j\text{s”} \tag{6.21}$$

となつてゐる.

以下では (4.9) の根号を $\varepsilon = 1$ となる様に取るものとする.
証明 中屋敷氏の報告 [N] を参照いただきたい. □

7 $\wp$ 函数に関する代数的加法公式

7.1 一般論

この章では 次の方針で $\wp_{k\cdots\ell}(u+v)$ を $\wp_{ij}(u)$, $\wp_{ij}(v)$, $\wp_{hij}(u)$ および $\wp_{hij}(v)$ 等の有理函数として表すことを目標とする. まづ, これまでのことから

$$\frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2}$$

は $\wp_{ij}(u)$ と $\wp_{ij}(v)$ 達の $\mathbb{Q}$ 係数の多項式で書かれるはづである. それができれば, 両辺に

$$\frac{\partial}{\partial u_i}\Big(\frac{\partial}{\partial u_j} + \frac{\partial}{\partial v_j}\Big)\log$$

を作用させることで所望の式を得ることができる.

7.2 基底

命題 7.1 (3.5) の超楕円曲線において $g=2$ のとき

$$\Gamma(J,\mathscr{O}(2\Theta))=\mathbb{C}1\oplus\mathbb{C}\wp_{11}\oplus\mathbb{C}\wp_{12}\oplus\mathbb{C}\wp_{22}$$

証明 次元の公式 ([Mu3], 小林氏の報告 [Ko]) より

$$\dim\Gamma(J,\mathscr{O}(2\Theta))=2^2=4. \tag{7.2}$$

一方 4.12 から $\wp_{ij}\in\Gamma(J,\mathscr{O}(2\Theta))$ である. ところが, 6.19 と 6.17(2) から容易に $\wp_{11}$, $\wp_{12}$, $\wp_{22}$ が 1 次独立であることがわかるので, 主張が示された. □

これにより,

$$\frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2}=a[\wp_{11}(u)-\wp_{11}(v)]+b[\wp_{12}(u)\wp_{22}(v)-\wp_{12}(v)\wp_{22}(u)]$$

であるが, 6.17(2) から

$$\sigma(u)=u_1-\tfrac{1}{3}{u_2}^3+\cdots$$

なので, これを代入することで, 容易に a, b を求めることができる. 結果は $a=b=1$ であり,

定理 7.3 (3.5) の超楕円曲線において $g=2$ のとき

$$\frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2}=\wp_{11}(u)-\wp_{11}(v)+\wp_{12}(u)\wp_{22}(v)-\wp_{12}(v)\wp_{22}(u)$$

7.3 $\wp$ 函数に関する代数的加法公式

命題 7.4 $\dfrac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2}$ は $g(g+1)$ 個の函数 $\wp_{ij}(u)$, $\wp_{ij}(v)$ の $\mathbb{Q}$ 上の多項式として表される. たとえば

(1) $g=1$ のときは

$$\frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2}=\wp_{11}(u)-\wp_{11}(v),$$

(2) $g=2$ のときは

$$\frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2}=\wp_{11}(u)-\wp_{11}(v)+\wp_{12}(u)\wp_{22}(v)-\wp_{12}(v)\wp_{22}(u),$$

(3) $g=3$ のときは

$$\begin{aligned}&\frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2}\\ =&\left(\wp_{31}(u)-\wp_{31}(v)\right)^2-\left(\wp_{33}(u)-\wp_{33}(v)\right)\left(\wp_{11}(u)-\wp_{11}(v)\right)\\ &+\left(\wp_{21}(u)-\wp_{21}(v)\right)\left(\wp_{23}(u)-\wp_{23}(v)\right)\\ &-\left(\wp_{22}(u)-\wp_{22}(v)\right)\left(\wp_{31}(u)-\wp_{31}(v)\right).\end{aligned} \tag{7.5}$$

証明 (1) については [Ta], p.141 を, その他については [Ba2] を参照されたい. □

系 7.6 各 $\wp_{ij\cdots r}(u+v)$ は $\wp_{ij}(u)$, $\wp_{ij}(v)$, $\wp_{hij}(u)$ および $\wp_{hij}(v)$ 達の $\mathbb{Q}(\lambda_0, \cdots, \lambda_{2g+1})$ 上の有理式として表される.

証明 7.4 の式を u と v のそれぞれに関して対数微分したあと, その両者を辺々加えると $2(\log\sigma(u+v)-2\log\sigma(u)-2\log\sigma(v))$ の $\wp_{ij}(u)$, $\wp_{ij}(v)$, $\wp_{hij}(u)$. および $\wp_{hij}(v)$ 達による式が得られる. それに $\dfrac{\partial^2}{\partial u_i \partial u_j}$ を施せば $\wp_{ij}(u+v)$ が $\wp_{ij}(u)$, $\wp_{ij}(v)$, $\wp_{hij}(u)$, $\wp_{hij}(v)$, $\wp_{ijk\ell}(u)$, $\wp_{ijk\ell}(v)$, $\wp_{ijk\ell m}(u)$ および $\wp_{ijk\ell m}(v)$ 達の有理式として表される. あとは後述の 8.34 の等式達を用いて結論を得る. □

$g=2$ の時の詳しい議論が [Gr] にある.

8 Set of Defining Equations of the Jacobian Variety

8.1 Matrix whose entries are $\wp$-functions

Fundamental formula to a matrix

いま u は C 上の g 個の点 (x_1, y_1), $\cdots$, (x_g, y_g) と

$$u = \Big(\int_\infty^{(x_1,y_1)} + \int_\infty^{(x_2,y_2)} + \cdots + \int_\infty^{(x_g,y_g)} \Big)\omega \tag{8.1}$$

なる関係があるとせよ. このとき fundamental relation

$$\sum_{i=1}^{g}\sum_{j=1}^{g} \wp_{ij}\Big(u - \int_\infty^{(x,y)}\Big) {x_r}^{i-1} x^{j-1} = \frac{F(x_r,x)-2y_r y}{(x_r-x)^2} \tag{8.2}$$

が成り立つ. これから Jacobi 多様体の自然な方程式系を導くのが本節の目標である. まづ (8.2) から, いくつかの必要な式を導いておく. (8.2) の分母を払つて,

$$(x_r-x)^2 \sum_{i=1}^{g}\sum_{j=1}^{g} \wp_{ij}\Big(u - \int_\infty^{(x,y)}\Big) {x_r}^{i-1} x^{j-1} - \big(F(x_r,x)-2y_r y\big) = 0 \tag{8.3}$$

を得る. ここで $x = 1/t^2$, $y = 1/t^{2g+1} + \cdots$ として, (8.3) の左辺を t で展開すれば, その t に関する各係数が消える. 特に最低次とその次の項が消えることから, 各 r について

$$\begin{aligned} 2y_r &= \wp_{ggg} {x_r}^{g-1} + \wp_{gg,g-1} {x_r}^{g-2} + \cdots + \wp_{gg2} x_r + \wp_{gg1}, \\ x_r^g &= \wp_{gg} {x_r}^{g-1} + \wp_{g,g-1} {x_r}^{g-2} + \cdots + \wp_{g2} x_r + \wp_{g1} \end{aligned} \tag{8.4}$$

が成り立つ.

$$\sum_{i=1}^{g}\sum_{j=1}^{g} \wp_{ij}(u) {x_r}^{i-1} {x_s}^{j-1} = \frac{F(x_r,x_s)-2y_r y_s}{(x_r-x_s)^2} \tag{8.5}$$

つぎに $r \neq 1$ についての (8.3) において $(x_1, y_1) \to \infty$ としてから, $(x, y) \to (x_1, -y_1)$ とすれば

$$(x_r - x_1)^2 \sum_{i=1}^{g} \sum_{j=1}^{g} \wp_{ij}(u) {x_r}^{i-1} {x_1}^{j-1} - \big(F(x_r, x_1) - 2y_r y_1\big) = 0 \tag{8.6}$$

となる. (x_1, y_1) 以外についても同様な操作が可能であるから, すべての r, s について

$$(x_r - x_s)^2 \sum_{i=1}^{g} \sum_{j=1}^{g} \wp_{ij}(u) {x_r}^{i-1} {x_s}^{j-1} - \big(F(x_r, x_s) - 2y_r y_s\big) = 0 \tag{8.7}$$

が成り立つ. これを

$$2\, y_r y_s = {}^t W(x_r) H W(x_s) \tag{8.8}$$

の形に変形する. 但し,

$$W(x) = {}^t[1,\ x,\ \cdots,\ x^{g-1},\ x^g,\ x^{g+1}] \tag{8.9}$$

である. このときの $H = [h_{ij}]$ の成分は

$$\begin{aligned} h_{ij} = {} & 2\wp_{i-1,j-1} - \wp_{i-2,j} - \wp_{i,j-2} + \delta_{ij}(\mu_{2g+6-4i} + \mu_{2g+6-4j}) \\ & + (\delta_{i,j+1}\mu_{4g+8-4i} + \delta_{i+1,j}\mu_{4g+8-4j}) \end{aligned} \tag{8.10}$$

となる. 例へば $g = 4$, つまり

$$y^2 = x^9 + \mu_2 x^8 + \mu_4 x^7 + \cdots + \mu_{18} \tag{8.11}$$

のときは

$$H = \begin{bmatrix} 2\mu_{18} & \mu_{16} & -\wp_{11} & -\wp_{12} & -\wp_{13} & -\wp_{14} \\ \mu_{16} & 2\wp_{11} + 2\mu_{14} & \wp_{12} + \mu_{12} & 2\wp_{13} - \wp_{22} & 2\wp_{14} - \wp_{23} & -\wp_{24} \\ -\wp_{11} & \wp_{12} + \mu_{12} & 2\wp_{22} - 2\wp_{13} + 2\mu_{10} & \wp_{23} - \wp_{14} + \mu_8 & 2\wp_{24} - \wp_{33} & -\wp_{34} \\ -\wp_{12} & 2\wp_{13} - \wp_{22} & \wp_{23} - \wp_{14} + \mu_8 & 2\wp_{33} - 2\wp_{24} + 2\mu_6 & 2\wp_{34} - \wp_{34} + \mu_4 & -\wp_{44} \\ -\wp_{13} & 2\wp_{14} - \wp_{23} & 2\wp_{24} - \wp_{33} & 2\wp_{34} - \wp_{34} + \mu_4 & 2\wp_{44} + 2\mu_2 & 1 \\ -\wp_{14} & -\wp_{24} & -\wp_{34} & -\wp_{44} & 1 & 0 \end{bmatrix}. \tag{8.12}$$

このとき, もちろん

$$-2f(x_r) = {}^t W(x_r) H W(x_r). \tag{8.13}$$

いま

$$U(x) = {}^t[1,\ x,\ \cdots,\ x^{g-1},\ x^g] \tag{8.14}$$

とおき, (8.8) を

$${x_r}^g = \wp_{gg} {x_r}^{g-1} + \wp_{g2} {x_r}^{g-2} + \cdots + \wp_{g,g-1} x_r + \wp_{gg} \tag{8.15}$$

を利用して ${}^tU(x_r)KU(x_s)$ の形に変形すれば, この K は

$$K = \left[\det H\begin{bmatrix} i & g+1 & g+2 \\ j & g+1 & g+2 \end{bmatrix}\right]_{1\leqq i\leqq g, 1\leqq j\leqq g} \tag{8.16}$$

となる. 実際,

(8.17)

$$W'(x) = \begin{bmatrix} 1 \\ x \\ \vdots \\ x^{g-1} \\ x^g \end{bmatrix}, \quad U(x) = \begin{bmatrix} 1 \\ x \\ \vdots \\ x^{g-1} \end{bmatrix}, \quad H = \begin{bmatrix} H_{11} & H_{12} \\ {}^tH_{12} & 0 \end{bmatrix}, \quad H_{11} = \begin{bmatrix} H'_{11} & H'_{12} \\ {}^tH'_{12} & h_{g+1,g+1} \end{bmatrix},$$

とするとき

$$\begin{aligned}
&{}^tW(x_r)HW(x_r) \\
&\quad = [{}^tW'(x_r) \;\; {x_r}^{g+1}] \begin{bmatrix} H_{11} & H_{12} \\ {}^tH_{12} & 0 \end{bmatrix} \begin{bmatrix} {}^tW'(x_s) \\ {x_s}^{g+1} \end{bmatrix} \\
&\quad = [{}^tW'(x_r)H_{11} + {x_r}^{g+1t}H_{12} \;\; 0] \begin{bmatrix} {}^tW'(x_s) \\ {x_s}^{g+1} \end{bmatrix}, \quad ((8.16)) \\
&\quad = {}^tW'(x_r)H_{11}W'(x_s) + {x_r}^{g+1t}H_{12}\,{}^tW'(x_s) \\
&\quad = {}^tW'(x_r)H_{11}W'(x_s) + {x_r}^{g+1} \cdot 0 \\
&\quad = {}^tU(x_r)H'_{11}U(x_s) + {x_r}^{g\,t}H'_{12}U(x_s) + {}^tU(x_r)H'_{12}{x_s}^g + {x_r}^g h_{g+1,g+1}{x_s}^g \\
&\quad = {}^tU(x_r)H'_{11}U(x_s) \\
&\qquad + {}^tU(x_r)\begin{bmatrix} \wp_{1g} \\ \vdots \\ \wp_{gg} \end{bmatrix} {}^tH'_{12}U(x_s) \\
&\qquad + {}^tU(x_r)H'_{12}[\wp_{1g} \quad \cdots \quad \wp_{gg}]U(x_s) \\
&\qquad + {}^tU(x_r)\begin{bmatrix} \wp_{1g} \\ \vdots \\ \wp_{gg} \end{bmatrix} h_{g+1,g+1}[\wp_{1g} \quad \cdots \quad \wp_{gg}]U(x_s) \\
&\quad = {}^tU(x_r)\left[\det\, H\begin{bmatrix} i & g+1 & g+2 \\ j & g+1 & g+2 \end{bmatrix}\right]U(x_s).
\end{aligned}$$

(ここの計算は全く形式的なもの). また,

$$2\,y_r = \wp_{ggg}{x_r}^{g-1} + \wp_{gg,g-1}{x_r}^{g-2} + \cdots + \wp_{gg2}x_r + \wp_{gg1}$$

なので,

$$4\,y_r y_s = \sum_{i=1}^{g}\sum_{j=1}^{g} \wp_{ggi}\wp_{ggj}\, {x_r}^{i-1}{x_s}^{j-1}$$

$$= {}^tU(x_r) \begin{bmatrix} \wp_{gg1}\wp_{gg1} & \wp_{gg1}\wp_{gg2} & \cdots & \wp_{gg1}\wp_{ggg} \\ \wp_{gg2}\wp_{gg1} & \wp_{gg2}\wp_{gg2} & \cdots & \wp_{gg2}\wp_{ggg} \\ \vdots & \vdots & \ddots & \vdots \\ \wp_{ggg}\wp_{gg1} & \wp_{ggg}\wp_{gg2} & \cdots & \wp_{ggg}\wp_{ggg} \end{bmatrix} U(x_s)$$

である. ここで $[{}^tU(x_1)\ {}^tU(x_2)\ \cdots\ {}^tU(x_g)]$ は generic には正則行列なので,

$$\tfrac{1}{2}\wp_{ggi}\wp_{ggj} + \det H\begin{bmatrix} i & g+1 & g+2 \\ j & g+1 & g+2 \end{bmatrix} = 0 \qquad (i,\, j = 1,\, \cdots,\, g) \tag{8.18}$$

である. これが Jacobi 多様体を定義する十分な量の方程式を含んでゐることを示さう. いま

$$\{P_{11}, \cdots, P_{gg}\},\ \{P_{gg1}, \cdots, P_{ggg}\} \tag{8.19}$$

をその 1 つの解とせよ. （どれがどの変数に対応してゐるかは言ふまでもないと思ふが）. このとき

$$\begin{aligned} y &= P_{ggg}x^{g-1} + P_{gg,g-1}x^{g-2} + \cdots + P_{gg2}x + P_{gg1}, \\ x^g &= P_{gg}x^{g-1} + P_{g,g-1}x^{g-2} + \cdots + P_{g2}x + P_{g1} \end{aligned} \tag{8.20}$$

が与へる g 個の根を

$$(x_1, y_1),\ \cdots,\ (x_g, y_g) \tag{8.21}$$

とし, これから

$$u = \left(\int_\infty^{(x_1,y_1)} + \int_\infty^{(x_2,y_2)} + \cdots + \int_\infty^{(x_g,y_g)} \right)\omega \tag{8.22}$$

を定めると, 先の等式 $y_r = \wp_{gg1}{x_r}^{g-1} + \cdots$, $x^g = \wp_{g1}{x_r}^{g-1} + \cdots$ により,

$$P_{g1} = \wp_{g1}(u), \cdots, P_{gg} = \wp_{gg}(u),\ P_{gg1} = \wp_{gg1}(u), \cdots, P_{ggg} = \wp_{ggg}(u) \tag{8.23}$$

となる. 後は方程式を i, j の大きい方から順に辿つて, 順に, その他の組 (i, j) について $P_{ij} = \wp_{ij}(u)$ が了解される. 実際, 例へば $g = 4$ なら, まづ

$$\frac{1}{2}\,{\wp_{444}}^2 = -\begin{vmatrix} 2\wp_{33} - 2\wp_{24} + 2\mu_6 & \wp_{34} + \mu_4 & -\wp_{44} \\ \wp_{34} + \mu_4 & 2\wp_{44} + 2\mu_2 & 1 \\ -\wp_{44} & 1 & 0 \end{vmatrix} \tag{8.24}$$

と

$$\frac{1}{2}\,{P_{444}}^2 = -\begin{vmatrix} 2P_{33} - 2P_{24} + 2\mu_6 & P_{34} + \mu_4 & -P_{44} \\ P_{34} + \mu_4 & 2P_{44} + 2\mu_2 & 1 \\ -P_{44} & 1 & 0 \end{vmatrix} \tag{8.25}$$

より $P_{33}=\wp_{33}(u)$ でなければならない. さらに

$$\frac{1}{2}\,\wp_{443}\wp_{444}=-\begin{vmatrix}\wp_{23}-\wp_{14}+2\mu_8 & 2\wp_{24}-\wp_{33} & -\wp_{34}\\ \wp_{34}+\mu_4 & 2\wp_{44}+2\mu_2 & 1\\ -\wp_{44} & 1 & 0\end{vmatrix} \tag{8.26}$$

と

$$\frac{1}{2}\,P_{443}P_{444}=-\begin{vmatrix}P_{23}-P_{14}+2\mu_8 & 2P_{24}-P_{33} & -P_{34}\\ P_{34}+\mu_4 & 2P_{44}+2\mu_2 & 1\\ -P_{44} & 1 & 0\end{vmatrix} \tag{8.27}$$

により, $P_{23}=\wp_{23}(u)$ でなければならない. 以下順に進めると $P_{gg,i+1}P_{gg,j+1}$ についての方程式から $P_{ij}=\wp_{ij}(u)$ が得られて, 結局, すべての i,j について $P_{ij}=\wp_{ij}(u)$, $P_{ggj}=\wp_{ggj}(u)$ となるで, 上の解 $\{P_{ij},P_{ggj}\}$ は Jacobi 多様体の上の座標を与へる.

従つてこれらの解は, 確かに Jacobi 多様体の 1 つの点の座標を与へる. 以上から上の方程式系は Jacobi 多様体の定義方程式系である. ちなみに Jacobi 多様体の次元 g は変数

$$\{\wp_{11},\ \wp_{12},\ \cdots,\wp_{gg}\},\ \{\wp_{gg1},\cdots,\wp_{ggg}\} \tag{8.28}$$

の個数 $\frac{1}{2}g(g+1)+g$ から, 方程式の個数 $\frac{1}{2}g(g+1)$ を差し引いたものと一致してゐて, 辻褄が合つてゐる.

以上を定理としてまとめておく.

定理 8.29 超楕円曲線 C の Jacobi 多様体の 1 つの model の定義方程式は

$$\tfrac{1}{2}\wp_{ggi}\wp_{ggj}+\det H\begin{bmatrix}i & g+1 & g+2\\ j & g+1 & g+2\end{bmatrix}=0\qquad(i,\,j=1,\,\cdots,\,g) \tag{8.30}$$

で与へられる. これは特異点を含み得る.

注意 8.31 これは特異点を含み得るが, それはこの方程式系を偏微分して得られる方程式により（座標を $\wp_{ijk\ell}$ などで増やせば）解消されていく.

8.2 $\wp$ 函数のみたすその他の微分方程式

Weierstraßの $\wp$ 函数は $\wp'(u)^2=4\wp(u)^3-g_2\wp(u)-g_3$ なる微分方程式を満たす. 超楕円函数の場合も $\wp_{ij}(u)$ はいくつかの微分方程式を満たす. 本章では [Ba3] に従つてこのことについて説明する.

8.2.1 種数 3 以下の場合

任意の $j,k,\cdots,r\in\{1,\cdots,g\}$ に対して

$$\wp_{jk\cdots r}(u)=\frac{\partial}{\partial u_j}\wp_{k\cdots r}(u) \tag{8.32}$$

と定めると $\wp_{jk\cdots r}(u)$ はすべて Λ を周期とする周期函数つまり **Jacobi 多様体** $J=\mathbf{C}^g/\Lambda$ 上の有理型函数になっている. 種数 $g=1$ のときは $\wp_{11}(u)$ は (定数の差を除いて) いわゆる Weierstraßの $\wp$ 函数である.

σ 函数は $\Theta+\Lambda$ を 1 位の零の因子としているので, 定義 5.37 にも述べたように,

$$\wp_{ij}(u)\in\Gamma(J,\mathscr{O}(2\Theta)),\quad \wp_{ijk}(u)\in\Gamma(J,\mathscr{O}(3\Theta)) \tag{8.33}$$

となることがわかる. ここで $\Gamma(J,\mathcal{O}(n\Theta))$ は Θ に n 位の極をもち, 他の点では正則であるような J 上の函数全体のなす空間をあらわす.

命題 8.34 X はいままで通り, (3.5) の方程式 $y^2=\mu_0+\mu_1x+\cdots+\mu_{2g+1}x^{2g+1}$ で定義されているものとする. 簡単のために $\wp_{ijk\ell}=\wp_{ijk\ell}(u)$, $\wp_{ij}=\wp_{ij}(u)$ とかくと以下の方程式が $g=1,2$ または 3 のとき成り立つ:

(1) $\wp_{3333}-6\wp_{33}^2=2\mu_5\mu_7+4\mu_6\wp_{33}+4\mu_7\wp_{32}$,

(2) $\wp_{3332}-6\wp_{33}\wp_{32}=4\mu_6\wp_{32}+2\mu_7(3\wp_{31}-\wp_{22})$,

(3) $\wp_{3331}-6\wp_{31}\wp_{33}=4\mu_6\wp_{31}-2\mu_7\wp_{21}$,

(4) $\wp_{3322}-4\wp_{32}^2-2\wp_{33}\wp_{22}=2\mu_5\wp_{32}+4\mu_6\wp_{31}-2\mu_7\wp_{21}$,

(5) $\wp_{3321}-2\wp_{33}\wp_{21}-4\wp_{32}\wp_{31}=2\mu_5\wp_{31}$,

(6) $\wp_{3311}-4\wp_{31}^2-2\wp_{33}\wp_{11}=2\Delta$,

(7) $\wp_{3222}-6\wp_{32}\wp_{22}=-4\mu_2\mu_7-2\mu_3\wp_{33}+4\mu_4\wp_{32}+4\mu_5\wp_{31}-6\mu_7\wp_{11}$,

(8) $\wp_{3221}-4\wp_{32}\wp_{21}-2\wp_{31}\wp_{22}=-2\mu_1\mu_7+4\mu_4\wp_{31}-2\Delta$,

(9) $\wp_{3211}-4\wp_{31}\wp_{21}-2\wp_{32}\wp_{11}=-4\mu_0\mu_7+2\mu_3\wp_{31}$,

(10) $\wp_{3111}-6\wp_{31}\wp_{11}=4\mu_0\wp_{33}-2\mu_1\wp_{32}+4\mu_2\wp_{31}$,

(11) $\wp_{2222}-6\wp_{22}^2=-8\mu_2\mu_6+2\mu_3\mu_5-6\mu_1\mu_7$
$-12\mu_2\wp_{33}+4\mu_3\wp_{32}+4\mu_4\wp_{22}+4\mu_5\wp_{21}-12\mu_6\wp_{11}+12\Delta$,

(12) $\wp_{2221}-6\wp_{22}\wp_{21}=-4\mu_1\mu_6-8\mu_0\mu_7-6\mu_1\wp_{33}+4\mu_3\wp_{31}+4\mu_4\wp_{21}$
$-2\mu_5\wp_{11}$,

(13) $\wp_{2211}-4\wp_{21}^2-2\wp_{22}\wp_{11}=-8\mu_0\mu_6-8\mu_0\wp_{33}-2\mu_1\wp_{32}+4\mu_2\wp_{31}$
$+2\mu_3\wp_{21}$,

(14) $\wp_{2111}-6\wp_{21}\wp_{11}=-2\mu_0\mu_5-8\mu_0\wp_{32}+2\mu_1(3\wp_{31}-\wp_{22})+4\mu_2\wp_{21}$,

(15) $\wp_{1111}-6\wp_{11}^2=-4\mu_0\mu_4+2\mu_1\mu_3+4\mu_0(4\wp_{31}-3\wp_{22})$
$+4\mu_1\wp_{21}+4\mu_2\wp_{11}$.

ここに

$$\Delta=\wp_{32}\wp_{21}-\wp_{31}\wp_{22}+\wp_{31}^2-\wp_{33}\wp_{11}. \tag{8.35}$$

ただし, $g=1$ または 2 のときは $j>g$ なる添字を含むような $\wp$ 函数や $i>2g+1$ なる添字を含む μ_i はすべて 0 とする.

とくに $g=1$ のときは方程式 (15) のみ意味があるが, それは $\wp'(u)^2=4f(\wp(u))$ から導かれる.

証明 [Ba3] を参照されたい. そこでは, 一般の種数に対して一般的な見地から議論がなされている. □

参考文献

[Ba1] Baker, H.F. : *Abelian functions – Abel's theorem and the allied theory including the theory of the theta functions* – Cambridge Univ. Press, 1897

[Ba2] Baker, H.F. : On the hyperelliptic sigma functions Amer. J. of Math., XX(1898)301-384

[Ba3] Baker, H.F. : On a system of differential equations leading to periodic functions, Acta math., 27(1903)135-156

[Ba4] Baker, H.F. : *An introduction to the theory of multiply periodic functions* Cambridge Univ. Press, (1907)

[BEL1] Buchstaber, V.M., Enolskii, V.Z. and Leykin, D.V. : Kleinian functions, hyperelliptic Jacobians and applications, Reviews in Math. and Math. Physics, 10(1997)1–125

[BEL2] Buchstaber, V.M., Enolskii, V.Z. and Leykin, D.V. : Rational analogs of Abelian functions, Functional Anal. Appl., **33**(1999)83–94

[BEL3] Buchstaber, V.M., Enolskii, V.Z. and Leykin, D.V. : Uiformaization of Jacobi varaieties of trigonal curves, Functional Anal. Appl., **34**(2000)159-171

[BG] Bauldwin, S., and Gibbons, J. : Genus 4 trigonal reduction of the Benney equations, J.Phy. A, **39**(2006)3607-3639

[EEMOP] Eilbeck, J.C., Enolskii, V.Z., Matsutani, S., Ônishi, Y. and Previato, E. : Abelian functions of trigonal curves of genus three, to appear in "Int. Math. Res. Notices",

[FK] Farkas, H.M. and Kra, I. : *Riemann Surfaces* (2nd ed.), Grad. Text in Math.,71

[Gr] Grant, D. : Formal groups in genus two, J. reine angew. Math., 411(1990)96–121

[Gu] 軍司圭一 : Abel-Jacobi の定理 I, 本報告集

[HL] Hensel, K. and Landsberg, G. : *Theorie der algebraischen Funktionen einer Variabeln und ihre Anwendung auf algebraische Kurven und Abelsche Integrale*, Teubner, 1902

[I] 岩澤健吉： 代数函数論, 1952, 岩波書店

[Kl] Klein, F.: 19 世紀の数学, 1995, 共立出版

[Ko] 小林 真一： Algebraic theory of Abelian varieties via schemes 本報告集

[Ku] 楠 幸男： 函数論, 1973, 朝倉書店

[L] Lang, S.： *An introduction to Algebraic and Abelian Functions* (2nd ed.), Springer-Verlag, 1982

[Ma] Macdonald, I.G.： *Symmetric functions and Hall polynomials*, 1995, Clarendon Press, Oxford

[Mu1] Mumford, D.： *Tata lectures on theta I* (Prog. in Math. 28), 1983, Birkhäuser

[Mu2] Mumford, D.： *Tata lectures on theta II* (Prog. in Math. 43), 1984, Birkhäuser

[Mu3] Mumford, D.： Abelian varieties, 1985, Oxford Univ. Press

[N] 中屋敷 厚： シグマ函数の代数的表示本報告集

[Og] 小川裕之： 代数曲線の Riemann-Roch の定理, 本報告集

[OU] 尾崎 学, 梅垣敦紀： Abel-Jacobi の定理 II, 本報告集

[Ta] 竹内端三： 楕圓函數論, 1936, 岩波全書

[TD] 田中俊一·伊達悦朗： KdV 方程式 （第５・６章）, 1979, 紀伊國屋数学叢書 16

[Wei] Weil, A.： 数学の創造, 1983, 日本評論社

[Wey] Weyl, H.： *Die Idee der Riemanschen Fläche,* Tuebner, 1913, 「リーマン面」, 田村二郎訳, 岩波書店, 1974

[Y] 吉富賢太郎： リーマン面と代数曲線, 本報告集

第 15 回 整数論サマースクール 報告集, pp.177-189

シグマ関数の代数的表示

中屋敷 厚*

1 はじめに

Weierstrass の楕円関数論の大きな特徴は, 楕円曲線の定義方程式に直接結びついた代数的性格にある. Eisenstein 級数の間の関係式の導出などはその帰結の一つである. 楕円関数 $\wp(u)$, 加法的関数 $\zeta(u)$ はシグマ関数の対数微分として記述されるという意味で, シグマ関数が最も基本的である. シグマ関数の代数的性質は, その原点におけるべき級数展開の係数が, 楕円曲線の定義方程式

$$y^2 = 4x^3 - g_2x - g_3 \tag{1}$$

の係数 g_2, g_3 の同次多項式 ($\deg g_i = 2i$) となるという事実の中に基本的には表現しつくされていると思われる. 現今の関数論では, $\wp(u)$ の満たす非線形微分方程式を導いてそれからシグマ関数のべき級数展開を決定するが, これを多変数で一般に実行しようとすると困難が多い. Weierstrass 自身は楕円関数論をシグマ関数を定義することから始めそれを用いて $\wp(u)$, $\zeta(u)$ を定義した. さらにシグマ関数の満たす線形の微分方程式を導出し, べき級数展開を決定している.

さて Klein はシグマ関数を代数的積分を用いて表示する公式を見出した. その直接の帰結としてシグマ関数のべき級数展開の係数は g_2, g_3 の同次多項式になることが分かる. さらに Klein はその公式を拡張することにより種数 2 以上の超楕円曲線に対してシグマ関数の拡張を定義した. それは g 変数の擬周期的正則関数であるが, その定義の仕方から原点におけるべき級数展開の係数は, 超楕円曲線の定義方程式の係数の適当な同次多項式になることが分かる. Klein の公式はシグマ関数の代数的性格を見事に表現したものと言える.

本稿ではまず Weierstrass のシグマ関数に対する Klein の公式について説明し, その後より一般の平面代数曲線のシグマ関数に対する同様の公式について簡単に説明する. 本稿の詳細については [7] を, シグマ関数についての基本的な事柄や本稿で触れていない重要な性質については本報告集中の大西さんによる原稿をご参照ください.

2 Weierstrass のシグマ関数

拡張された場合の記述に都合のよいように, Weierstrass のシグマ関数を 3 次曲線 (1) から出発して定義する. Weierstrass の楕円関数論についての参考文献として [9, 10] をあげて

*九州大学大学院数理学研究院　e-mail: 6vertex@math.kyushu-u.ac.jp

おく. 3 次曲線 (1) の判別式 $\Delta = g_2^3 - 27g_3^2 \neq 0$ とし, それから定義されるコンパクトリーマン面を X とする.

有理型微分

$$du = \frac{dx}{y} \qquad dr = \frac{xdx}{y}$$

はそれぞれ X 上の第一種, 第二種微分を定義する. X 上に標準ホモロジー基底 $\{\alpha, \beta\}$ をとり,

$$2\omega_1 = \int_\alpha du, \quad 2\omega_2 = \int_\beta du, \quad -2\eta_1 = \int_\alpha dr, \quad -2\eta_2 = \int_\beta dr,$$

により 4 つの周期を定義する (大西さんの原稿では, 左辺の 2 はなく, η_i の符号は逆である). du, dr は 1 次元コホモロジー $H^1(X, \mathbb{C})$ の交叉型式 $\circ$:

$$du \circ dr := \sum \mathrm{Res}\left(\int^p du\right) dr$$

について

$$du \circ dr = 1$$

を満たすので, リーマンの周期関係式から

$$\omega_2\eta_1 - \omega_1\eta_2 = \frac{\pi i}{2}$$

が成り立つ. これはルジャンドルの関係式とよばれているものである. またリーマンの不等式から $\omega_1 \neq 0$ であること, $\mathrm{Im}\,\tau > 0$, $\tau = \omega_1^{-1}\omega_2$ であることがわかる. 従って特に ω_1, ω_2 は $\mathbb{R}$ 上 1 次独立であることが分かる. この ω_1, ω_2, η_1, η_2 を用いて, シグマ関数を次のように定義する.

定義 次の条件を満たす関数 $\sigma(u)$ をシグマ関数という.

(i) $\mathbb{C}$ 上正則である.

(ii) 次の擬周期性を満たす:

$$\frac{\sigma(u+\ell)}{\sigma(u)} = \chi(\ell) \exp\, L(u + \frac{1}{2}\ell, \ell).$$

ただし

$$\begin{aligned}
&\ell = 2\omega_1\ell' + 2\omega_2\ell'', \quad \ell', \ell'' \in \mathbb{Z}, \\
&L(u, v) = (2\eta_1 v' + 2\eta_2 v'')u, \quad v = 2\omega_1 v' + 2\omega_2 v'', v', v'' \in \mathbb{R}. \\
&\chi(\ell) = (-1)^{\ell'+\ell''+\ell'\ell''}.
\end{aligned}$$

(iii) 原点におけるべき級数展開は次の形をしている:

$$\sigma(u) = u + O(u^2).$$

条件 (i), (ii) を満たす関数は, ヤコビ-リーマンのテータ関数

$$\theta \left[\begin{array}{c} a \\ b \end{array} \right] (z,\tau) = \sum_{n\in\mathbb{Z}} \exp\left(\pi i\tau(n+a)^2 + 2\pi i(n+a)(n+b)\right), \quad a,b \in \mathbb{R}, \quad \operatorname{Im}\tau > 0,$$

を用いて

$$\exp\left(\frac{\eta_1}{2\omega_1}u^2\right) \theta \left[\begin{array}{c} 1/2 \\ 1/2 \end{array} \right] (\frac{u}{2\omega_1},\tau), \quad \tau = \frac{\omega_2}{\omega_1} \tag{2}$$

のように具体的に作ることが出来る. これは奇関数で原点に 1 位の零点を持つこともテータ関数の性質からわかるので, 定数倍して条件 (iii) を満たすようにすればシグマ関数になる. また $\theta(z) = \theta \left[\begin{array}{c} 0 \\ 0 \end{array} \right] (z)$ と同じ擬周期性を満たす正則関数は $\theta(z)$ の定数倍に限ることから, 条件 (i)-(iii) を満たす関数は唯一つであることも分かる.Weierstrass のシグマ関数は (i)-(iii) を満たすので, 上で定義したシグマ関数は Weierstrass のシグマ関数に一致する. 従って

$$\wp(u) = -\frac{d^2}{du^2}\log\,\sigma(u) \tag{3}$$

と定めると, $(x,y) = (\wp(u), \wp'(u))$ は X 上の点となる. 今

$$p_i = (x_i, y_i) = (\wp(u_i), \wp'(u_i)), \quad i = 1,2$$

として $X \times X$ 上の 2-型式

$$\widehat{\omega}(p_1,p_2) = \wp(u_2 - u_1)du_1du_2 \tag{4}$$

を考えると, $\wp(u)$ の加法定理により, $\widehat{\omega}$ は

$$\widehat{\omega}(p_1,p_2) = \frac{2y_1y_2 + 4x_1x_2(x_1+x_2) - g_2(x_1+x_2) - 2g_3}{4y_1y_2(x_1-x_2)^2}dx_1dx_2$$

と代数関数 x_i, y_i を用いて表示できることが分かる.

Weierstrass のシグマ関数に対する Klein の公式 [4] とは次のようなものである:

$$\sigma\left(u_2 - u_1\right) = \frac{x_1 - x_2}{\sqrt{y_1y_2}} \exp\left(\frac{1}{2}\int_{\bar{p}_1}^{\bar{p}_2}\int_{p_1}^{p_2}\widehat{\omega}\right). \tag{5}$$

ただし $\bar{p}_i = (x_i, -y_i) = (\wp(-u_i), \wp'(-u_i))$. 右辺の積分路の不定性による多価性をきちんと記述するには普遍被覆上で定式化する必要があるがその辺を詳しく知りたい方は論文 [7] を参照してください. 以下で述べる一般の場合の公式についても同様である.

この公式は, 解析的表示を用いて次のように簡単にチェックすることが出来る. $\widehat{\omega}$ の解析的表示 (4) と (3) を用いて積分を計算すると

$$\begin{aligned}\exp\left(\int_{\bar{p}_1}^{\bar{p}_1}\int_{p_1}^{p_2}\widehat{\omega}\right) &= \frac{\sigma(2u_1)\sigma(2u_2)}{\sigma(u_1+u_2)^2} \\ &= \frac{\sigma(2u_1)\sigma(2u_2)}{\sigma(u_1+u_2)^2\sigma(u_1-u_2)^2}\sigma(u_1-u_2)^2.\end{aligned}$$

最後の式の $\sigma(u_1-u_2)^2$ 以外の部分は各 u_j について $2\omega_i$ 周期的 $(i=1,2)$ であることが分かるので x_k, y_l の有理関数として記述できるはずである. 実際シグマ関数の加法定理

$$\frac{\sigma(v_1-v_2)\sigma(v_1+v_2)}{\sigma(v_1)^2\sigma(v_2)^2} = \wp(v_2)-\wp(v_1) \tag{6}$$

で, $v_1 = u_1+u_2$, $v_2 = u_1-u_2$ とすると

$$\frac{\sigma(2u_1)\sigma(2u_2)}{\sigma(u_1+u_2)^2\sigma(u_1-u_2)^2} = \wp(u_1-u_2)-\wp(u_1+u_2).$$

(6) の両辺の $\dfrac{\partial^2}{\partial v_1\partial v_2}\log\cdot$ をとると

$$\wp(v_1-v_2)-\wp(v_1+v_2) = \frac{\wp'(v_1)\wp'(v_2)}{\left(\wp(v_1)-\wp(v_2)\right)^2}.$$

従って

$$\frac{\sigma(2u_1)\sigma(2u_2)}{\sigma(u_1+u_2)^2\sigma(u_1-u_2)^2} = \frac{y_1y_2}{(x_1-x_2)^2}$$

となる. これを先の式に代入して $\sigma(u_1-u_2)$ について解くと (5) が得られる. ただし平方根をとるとき符号は次のように決めた. $g_2, g_3 \in \mathbb{R}$, $u_2 > u_1 > 0$ とし u_2 は十分 0 に近いとする. このとき x_i, y_i はともに実数で $0 < x_2 < x_1$, $y_1, y_2 < 0$, $\widehat{\omega}$ の積分の exp は正, $\sigma(u_2-u_1) > 0$ となる. 変数がこのような条件を満たすとき両辺の符号が一致するようにした. ただしそのような範囲で $\sqrt{y_1y_2}$ は正数の平方根を意味するものとする.

Klein の公式を用いると次のようにしてシグマ関数のべき級数展開を調べることが出来る. ∞ における局所座標 t を

$$x = \frac{1}{t^2}, \qquad y = -\frac{2}{t^2}(1-g_2t^4-g_3t^6)^{1/2}$$

を満たすようにとる. この t を用いて変数 u を表すと

$$u = \int_\infty^p \frac{dx}{y} = t + \frac{g_2}{40}t^5 + \frac{g_3}{56}t^7 + \frac{g_2^2}{384}t^9 + \frac{3g_2g_3}{704}t^{11} + \cdots .$$

これを逆に解いて

$$t = u - \frac{g_2}{40}u^5 - \frac{g_3}{56}u^7 + \cdots .$$

$\widehat{\omega}$ の展開は

$$\widehat{\omega}(p_1, p_2) = \left(\frac{1}{(t_1-t_2)^2} + \frac{g_2}{8}(t_1^2+t_2^2) + \frac{g_3}{8}(t_1^4+t_2^4+3t_1^2t_2^2) + \cdots\right) dt_1dt_2,$$

となりそれを用いて計算すると

$$\exp\left(\frac{1}{2}\int_{\bar{p}_1}^{\bar{p}_2}\int_{p_1}^{p_2}\widehat{\omega}\right)$$

$$= \frac{2\sqrt{t_1t_2}}{t_1+t_2}\left(1 - \frac{g_2}{24}(t_1^4+t_2^4-t_1^3t_2-t_1t_2^3) - \frac{g_3}{240}(11t_1^6+11t_2^6-6t_1t_2^5-6t_1^5t_2-10t_1^3t_2^3) + \cdots\right).$$

また

$$\frac{x_1-x_2}{\sqrt{y_1y_2}} = \frac{t_2^2-t_1^2}{2\sqrt{t_1t_2}}\left(1 + \frac{g_2}{16}(t_1^4+t_2^4) + \frac{g_3}{16}(t_1^6+t_2^6) + \cdots\right)$$

である. これらを用いて計算すると

$$\begin{aligned}&\sigma(u_2-u_1)\\ &= (t_2-t_1)\left(1 + \frac{g_2}{48}(t_1^4+t_2^4-2t_1^3t_2-2t_1t_2^3) + \frac{g_3}{120}(2t_1^6+2t_2^6+3t_1t_2^5+3t_1^5t_2+5t_1^3t_2^3) + \cdots\right)\end{aligned}$$

となる. 最後の式で $t_1=0$, $t=t_2$, $u=u_2$ とすると

$$\begin{aligned}\sigma(u) &= t + \frac{g_2}{48}t^5 + \frac{g_3}{60}t^7 + \cdots\\ &= u - \frac{g_2}{240}u^5 - \frac{g_3}{840}u^7 + \cdots\end{aligned}$$

となる. 展開係数が $\mathbb{Q}[g_2, g_3]$ の元であること, $\deg u = -1$, $\deg g_i = 2i$ により $\sigma(u|g_2, g_3)$ は -1 次同次式であることなどもこのような計算で分かる.

さて, 種数 g のリーマン面に対するシグマ関数の表示を作ろうと思うと $\sigma(\sum_{i=1}^g u_i)$ のようなものを記述することになる. Weierstrass のシグマ関数に対してはそのような関数を 2

変数の関数 $\sigma(u-v)$ を用いて記述する公式がある. Frobenius-Stickelberger の公式というのがそれで, 少し書き換えると次のようになる:

$$\sigma\left(\sum_{i=1}^{N}(u_i-v_i)\right) = \frac{\prod_{i,j=1}^{N}\sigma(u_i-v_j)}{\prod_{i<j}\sigma(u_i-u_j)\sigma(v_j-v_i)\prod_{i,j=1}^{N}(\wp(v_j)-\wp(u_i))}D_N$$

$$D_N = \det\left(\wp^{(i-1)}(u_j)\right)_{1\le i,j\le 2N}, \tag{7}$$

ただし D_N において $u_{N+j}=-v_j$, $1\le j\le N$ とおいた. Klein はシグマ関数の高種数への拡張を, (5), (7) を手掛かりに同様の公式を作ることで与えたのである.

3 (n,s)-曲線のシグマ関数

n,s を互いに素な自然数で $s>n\ge 2$ をみたすものとする. このとき

$$f(x,y)=y^n-x^s-\sum_{ni+sj<ns}\lambda_{ij}x^iy^j$$

の形の多項式を考える. $f(x,y)=0$ で定義される代数曲線は非特異であると仮定し, 対応するコンパクトリーマン面を X とする. X を (n,s) 曲線とよぶ. 種数は $g=1/2(n-1)(s-1)$ である.

さてシグマ関数を変換性を用いて楕円曲線の場合のように定義しようとするとき必要になるデータは周期である. その周期は勝手ではなく, 変換性が矛盾なく定義出来るようなものでなくてはならない. Weierstrass のシグマ関数の場合, 4 つの周期はルジャンドルの関係式をみたしていた. そのような関係式が必要である. 以下で与えるデータの満たす条件は, そのような要請から出てくるものである.

シグマ関数を定義するために以下のようなデータを用意する.

(i) 標準ホモロジー基底 $\{\alpha_i,\beta_j\}$. i.e. 交点数が次を満たす:

$$\alpha_i\cdot\beta_j=\delta_{ij},\quad \alpha_i\cdot\alpha_j=\beta_i\cdot\beta_j=0.$$

(ii) 標準コホモロジー基底 $\{du_i,dr_j\}$. ただし $\{du_i\}$ は第一種微分の基底, dr_j は第二種微分. 条件はコホモロジー $H^1(X,\mathbb{C})$ の交叉型式 $\circ$ について

$$du_i\circ dr_j=\delta_{ij},\quad du_i\circ du_j=dr_i\cdot dr_j=0.$$

このデータを用いて 4 つの周期行列を

$$2\omega_1=\left(\int_{\alpha_j}du_i\right),\quad 2\omega_2=\left(\int_{\beta_j}du_i\right),\quad -2\eta_1=\left(\int_{\alpha_j}dr_i\right),\quad -2\eta_2=\left(\int_{\beta_j}dr_i\right),$$

で定義する. $\{du_i, dr_j\}$ の交叉条件からリーマンの関係式は次の形になる:

$$MJ^tM = -\frac{\pi i}{2}J, \quad M = \begin{pmatrix} \omega_1 & \omega_2 \\ \eta_1 & \eta_2 \end{pmatrix}, \quad J = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}.$$

これは

$$ {}^tMJM = -\frac{\pi i}{2}J \tag{8}$$

と同値である. 実際変換性を示すときに使うのはこちらの形である. またリーマンの不等式から

$$\det \omega_1 \neq 0, \quad \mathrm{Im}\tau > 0, \quad \tau = \omega_1^{-1}\omega_2, \tag{9}$$

が成り立つ. ただし > 0 は正定値であることを意味する.

次の du_i は第一種微分の基底となる:

$$du_i = -\frac{x^{a_i-1}y^{n-1-b_i}dx}{f_y}, \tag{10}$$

ここで $\{(a_i, b_i)\}$ は

$$1 \leq b \leq n-1, 1 \leq a \leq [\frac{sb-1}{n}],$$

を満たす非負整数の組 (a, b) を $-na_1 + sb_1 < \cdots < -na_g + sb_g$ を満たすように並べたものである. 以下この du_i をデータ (ii) の du_i とする.

X はアフィン代数曲線 $f(x, y) = 0$ に 1 点を付け加えて出来るが, その 1 点を ∞ であらわす. ∞ における gap sequence を $w_1 < \cdots < w_g$ とする.

例

$(n, s) = (2, 2g+1)$: $(w_1, ..., w_g) = (1, 3, ..., 2g-1)$,

$(n, s) = (3, 4)$, $g = 3$: $(w_1, w_2, w_3) = (1, 2, 5)$,

$(n, s) = (4, 5)$, $g = 6$: $(w_1, ...w_6) = (1, 2, 3, 6, 7, 11)$,

変数 u_i の次数を

$$\deg u_i = -w_i$$

で定義する. 基点を ∞ としたときのリーマン定数の指標を

$$\delta = \begin{bmatrix} \delta' \\ \delta'' \end{bmatrix} \in \frac{1}{2}\mathbb{Z}^{2g}$$

とする. du_i を上のように指定したとき, (i), (ii) のデータに対しシグマ関数を次のように定義する [2].

定義 次の条件を満たす関数 $\sigma(u)$ をシグマ関数という.

(i) $\mathbb{C}^g$ 上正則である.

(ii) 次の擬周期性を満たす:

$$\frac{\sigma(u+\ell)}{\sigma(u)} = \chi(\ell)\exp\, L(u+\frac{1}{2}\ell,\ell).$$

ただし

$$\begin{aligned}
&\ell = 2\omega_1\ell' + 2\omega_2\ell'', \quad \ell',\ell'' \in \mathbb{Z}^g,\\
&L(u,v) = (2\eta_1 v' + 2\eta_2 v'')u, \quad v = 2\omega_1 v' + 2\omega_2 v'', v', v'' \in \mathbb{R}^g.\\
&\chi(\ell) = (-1)^{2({}^t\delta'\ell' + {}^t\delta''\ell'') + {}^t\ell'\ell''}.
\end{aligned}$$

(iii) 原点におけるべき級数展開は次の形をしている:

$$\sigma(u) = S_{\lambda(n,s)}(T)|_{T_{w_i}=u_i} + \cdots .$$

ただし $S_{\lambda(n,s)}(T)$ はシューア関数とよばれる $\{T_i\}$ の多項式で, $S_{\lambda(n,s)}(T)|_{T_{w_i}=u_i}$ は $\{u_i\}$ の同次多項式となる. $\cdots$ 部分は $\deg S_{\lambda(n,s)}(T)|_{T_{w_i}=u_i}$ より次数の小さい同次多項式の（無限）和である.

楕円曲線の場合と同様に条件 (i), (ii) を満たす関数はリーマンのテータ関数を用いて簡単に作ることが出来るがそれについては大西さんの原稿を見てください. 条件 (iii) は自明ではなく, Klein の公式の拡張を作ることでシグマ関数の存在が証明される.

先に進む前にここでシューア関数 $S_{\lambda(n,s)}(u)$ についてごく簡単に説明する. 詳しくは [6, 7, 8, 3] などをご覧ください.

T_1, T_2,... の多項式 $p_n(T)$ を

$$\exp(\sum_{n=1}^{\infty} T_n k^n) = \sum_{n=0}^{\infty} p_n(T)k^n,$$

で定める.

$$p_0 = 1, \quad p_1 = T_1, \quad p_2 = T_2 + T_1^2/2, \quad p_3 = T_3 + T_1T_2 + T_1^3/6$$

等である. 整数の組 $(\lambda_1,...,\lambda_l)$ が $\lambda_1 \geq \cdots \geq \lambda_l \geq 0$ をみたすとき分割という. 分割 λ とその後に 0 を任意個付け加えた分割 $(\lambda_1,...,\lambda_l,0,...,0)$ を同一視し, $\lambda_k = 0$, $k \geq l+1$ と置く. 分割 $\lambda = (\lambda_1,...,\lambda_l)$ に対して T_1, T_2,... の多項式 $S_\lambda(T)$ と t_1, t_2,... の対称多項式 $s_\lambda(t)$ を

$$S_\lambda(T) = \det\left(p_{\lambda_i - i + j}(T)\right)_{1\leq i,j\leq l}, \tag{11}$$

$$s_\lambda(t_1,...,t_n) = \frac{\det(t_j^{\lambda_i+l-i})_{1\leq i,j\leq l}}{\prod_{1\leq i<j\leq l}(t_i - t_j)}, \quad n \geq l \tag{12}$$

により定める. どちらもシューア関数という. 2 つのシューア関数は次の関係で結ばれている:

$$S_\lambda(T) = s_\lambda(t_1, ..., t_n), \qquad T_i = \frac{\sum_{j=1}^n t_j^i}{i}. \tag{13}$$

例 $S_{(1)}(T) = T_1, \quad S_{(2,1)}(T) = \dfrac{T_1^3}{3} - T_3, \quad S_{(3,2,1)}(T) = \dfrac{1}{45}T_1^6 - \dfrac{1}{3}T_1^3T_3 - T_3^2 + T_1T_5,$

$$s_{(g,g-1,...,1)}(t_1, ..., t_g) = \prod_{i=1}^g t_i \prod_{1\le i<j\le g}(t_i + t_j),$$
$$s_{(g,g-1,...,1)}(t_1, ..., t_{g+1}) = \prod_{1\le i<j\le g+1}(t_i + t_j).$$

これらの例からも見て取れるように, 一般に

$$\deg T_i = -i, \qquad \deg t_i = -1$$

と定めると, $S_\lambda(T)$, $s_\lambda(t)$ はそれぞれの変数に関して $-|\lambda|$ 次の同次多項式になる. ただし $\lambda = (\lambda_1, ..., \lambda_l)$ に対し $|\lambda| = \lambda_1 + \cdots + \lambda_l$ とする. ここで次数を負にしたのはシグマ関数との関係でそうしたので, シューア関数のみ論じる分には正にしてもよい（むしろそれが普通である）.

分割 $\lambda(n, s)$ を

$$\lambda(n, s) = (w_g, ..., w_1) - (g - 1, ..., 1, 0).$$

で定める. このとき次が知られている [3]:

命題

(i) $S_{\lambda(n,s)}(T)$ は T_{w_1}, ..., T_{w_g} にしかよらない.

(ii) $\deg S_{\lambda(n,s)}(T) = |\lambda(n, s)| = -\dfrac{1}{24}(n^2 - 1)(s^2 - 1).$

さて標準コホモロジー基底 $\{du_i, dr_j\}$ の dr_j をどうやって具体的に作るかという問題が残っているが, それは Weierstrass の場合の $\widehat{\omega}$ に対応する 2 型式を構成することにより構成される.

$p_i = (x_i, y_i) \in X$, $i = 1, 2$ とし

$$\Omega(p_1, p_2) = \frac{\sum_{i=0}^{n-1} y_1^i \left[\frac{f(z,w)}{w^{i+1}}\right]_+\Big|_{(z,w)=(x_2,y_2)}}{(x_1 - x_2)f_y(p_1)}dx_1,$$

とする. ここで

$$[\sum_{n\in\mathbb{Z}} a_n w^n]_+ = \sum_{n\geq 0} a_n w^n.$$

である. これを用いて次のような形の $\widehat{\omega}$ を考える.

$$\widehat{\omega}(p_1,p_2) = d_{p_2}\Omega(p_1,p_2) + \sum_{i=1}^{g} du_i(p_1)dr_i(p_2), \tag{14}$$

ただし dr_i は次の形をしているとする:

$$dr_i = \sum c_{i;jk}\frac{x^j y^k}{f_y}dx.$$

このとき, $\widehat{\omega}(p_1,p_2) = \widehat{\omega}(p_2,p_1)$ が成り立てば, dr_j は ∞ のみに極を持つ第二種微分で, $\{du_i, dr_j\}$ は標準コホモロジー基底となる. このような $\widehat{\omega}$ は $X\times X$ 上の有理型 2 型式で次の性質をみたすものである.

(i) 対角線 $\{(p,p)|p\in X\}$ にのみ 2 位の極をもつ.

(ii) $p\in X$ のまわりの局所座標を t とするとき, (p,p) のまわりでの展開が次の形になる:

$$dt_1 dt_2/(t_1-t_2)^2 + \cdots$$

ただし $\cdots$ 部分は t_1, t_2 の正べきの級数である.

このような $\widehat{\omega}$ は唯一つではないが, その不定性は完全に記述することが出来る.
λ_{ij}, x, y, dx の次数を

$$\deg\lambda_{ij} = ns - ni - sj, \quad \deg x = \deg dx = n, \quad \deg y = s,$$

により定める.

命題 次の条件を満たす $\{dr_j\}$ が存在する.

(i) $\widehat{\omega}(p_1,p_2) = \widehat{\omega}(p_2,p_1)$.

(ii) $c_{i;jk}$ はすべて $\{\lambda_{lm}\}$ の同次多項式である.

(iii) $\deg dr_i = -\deg du_i = w_i$.

この命題を満たす $\{dr_i\}$ は一般には唯一つではないが, 以下この命題の条件を満たす $\{dr_i\}$ を一つ固定し対応する $\widehat{\omega}$ を考える. ほかの $\{dr_i\}$ をとった場合のことはこの場合から分かる. また dr_i や $\widehat{\omega}$ の具体形も, 超楕円曲線の場合や種数の小さいいくつかの場合には知られている.

さてこれから $\widehat{\omega}$ を用いてシグマ関数の代数的表示を作ってゆく. いくつか記号の準備が必要である.

$\pi : X \longrightarrow \mathbb{P}^1$ を $\pi(x,y) = x$ で定義する. $p = (x,y) \in X$ に対して

$$\pi^{-1}(x) = \{p^{(0)}, p^{(1)}, ..., p^{(n-1)}\}, \qquad p^{(0)} = p$$

とする. $p^{(0)}$ 以外の番号のつけ方は以下で問題にならないので勝手につけてよい.

$x^i y^j$, $i \geq 0$, $0 \leq j \leq n-1$ を次数の小さい順に並べて f_1, f_2,... とする. 最初の 2 つは $f_1 = 1$, $f_2 = x$ である.

まず Weierstrass のシグマ関数の表示 (5) と同様の表示を持つ関数を導入する:

$$\tilde{E}(p_1,p_2) = \frac{x(p_2)-x(p_1)}{\sqrt{f_y(p_1)f_y(p_2)}} \exp\left(\frac{1}{2}\sum_{i=1}^{n-1}\int_{p_1^{(i)}}^{p_2^{(i)}}\int_{p_1}^{p_2}\widehat{\omega}\right),$$

この $\tilde{E}(p_1,p_2)$ は p_i が X のサイクルを回るとき, シグマ関数と同じ変換性に従う. 公式 (7) で与えられた処方箋に従って, $N \geq g$ に対してつぎのような関数を考える:

$$M_N = \frac{\prod_{i,j=1}^N \tilde{E}(p_i,q_j)}{\prod_{i<j}\left(\tilde{E}(p_i,p_j)\tilde{E}(q_i,q_j)\right)\prod_{i,j=1}^N (x(p_i)-x(q_j))}.$$

この関数は, シグマ関数と同じ変換性を持つ. あとは X^N 上の適当な有理型関数を掛けて正則になるように出来ればよい. 最終的に次の公式が得られる. $N \geq g$ に対して

$$\sigma\left(\sum_{i=1}^N \int_{p_i}^{q_i} du\right) = C_N \; M_N \; F_N,$$

ただし $du = {}^t(du_1, ..., du_g)$ で,

$$\begin{aligned}
F_N &= \frac{D_N}{\prod_{i<j}(x(q_i)-x(q_j))^{n-2}\prod_{k=1}^N\prod_{1\leq j\leq n-1}\left(y(q_k^{(i)})-y(q_k^{(j)})\right)}, \\
D_N &= \det\left(f_i(p_j)\right)_{1\leq i,j\leq nN}, \\
C_N &= (-1)^{\frac{1}{24}(n^2-1)(s^2-1)+\frac{1}{2}nN(N-1)}\left(\frac{\epsilon(s)}{\epsilon(1)}\right)^N \\
&\quad \times \epsilon_n^{\frac{1}{2}N(N-1)-\frac{1}{4}N(N-1)(n-1)(n-2)+\frac{1}{2}Nn(n-1)-\frac{1}{2}gNn(n-3)}, \\
&\quad \epsilon_n = \exp(2\pi i/n), \qquad \epsilon(r) = \prod_{1\leq i<j\leq n-1}(\epsilon_n^{ri}-\epsilon_n^{rj}).
\end{aligned} \tag{15}$$

である. D_N の定義式の中で

$$p_{N+(n-1)(k-1)+j} = q_k^{(j)}, \qquad 1 \leq k \leq N, \quad 1 \leq j \leq n-1$$

と置いた.

$(n,s)=(2,2g+1)$ の場合, つまり超楕円曲線の場合は, $F_N=D_N$ となり上の公式は定数倍を除いて Klein の公式 [5, 1] に一致する. この場合 $(x_i,y_i)=(x(p_i),y(p_i))$, $(X_i,Y_i)=(x(q_i),y(q_i))$ と書くと D_N, C_N は

$$D_N=\begin{vmatrix} 1 & \cdots & 1 & 1 & \cdots & 1 \\ x_1 & & x_N & X_1 & & X_N \\ x_1^2 & & x_N^2 & X_1^2 & & X_N^2 \\ \vdots & & \vdots & \vdots & & \vdots \\ x_1^g & & x_N^g & X_1^g & & X_N^g \\ y_1 & & y_N & -Y_1 & & -Y_N \\ x_1^{g+1} & & x_N^{g+1} & X_1^{g+1} & & X_N^{g+1} \\ x_1y_1 & \cdots & x_Ny_N & -X_1Y_1 & \cdots & -X_NY_N \\ \vdots & & \vdots & \vdots & & \vdots \end{vmatrix}.$$

$$C_N=(-1)^{\frac{1}{2}g(g+1)+\frac{1}{2}N(N+1)+gN}$$

となる.

すべての $q_i\longrightarrow\infty$ とすることにより $\sigma(\sum_{i=1}^{N}\int_{\infty}^{p_i}du)$ の表示を得ることが出来る. $\tilde{E}(p_1,p_2)$ は p_1,p_2 に関して反対称で, $p_1=\infty$ に $g-1$ 位の零点を持つ. そこで ∞ のまわりの局所座標 t を

$$x=\frac{1}{t^n},\qquad y=\frac{1}{t^s}(1+O(t))$$

を満たすようにとり $t_i=t(p_i)$ としたとき

$$\tilde{E}(p_1,p_2)=\tilde{E}(\infty,p_2)t_1^{g-1}+O(t_1^g)$$

により $\tilde{E}(\infty,p)$ を定義する. $\tilde{E}(\infty,p)$ は $\tilde{E}(p_1,p_2)$ のようなきれいな表示を持たないのが難点である. しかし, ともかくこれを用いると次の公式が $N\geq g$ に対して成り立つ.

$$\sigma(\sum_{i=1}^{N}\int_{\infty}^{p_i}du\ )\ =\ \frac{\prod_{i=1}^{N}\tilde{E}(\infty,p_i)^N}{\prod_{i<j}\tilde{E}(p_i,p_j)}\ \det(f_i(p_j))_{1\leq i,j\leq N}. \tag{16}$$

右辺を $t_i=t(p_i)$ で展開すると

$$s_{\lambda(n,s)}(t_1,...,t_N)+\cdots$$

の形になる. これを

$$(u_1,...,u_g):=\sum_{k=1}^{N}\int_{\infty}^{p_k}du=(\frac{\sum_{j=1}^{N}t_j^{w_1}}{w_1},...,\frac{\sum_{j=1}^{N}t_j^{w_N}}{w_N})+\cdots$$

により $u_1, ..., u_g$ で書き換えることにより, シグマ関数の定義の中の条件 (iii) がみたされることが示される. また $\sigma(u)$ の展開係数が, $\{\lambda_{ij}\}$ の同次多項式になることもこの公式を用いて $g = 1$ の場合と同様にして示される.

参考文献

[1] H. F. Baker, *Abelian functions*, 1897, Cambridge University Press.

[2] Buchstaber, V.M., Enolskii, V.Z. and Leykin, D.V., Kleinian functions, hyperelliptic Jacobians and applications, in *Reviews in Math. and Math. Phys.* **Vol.10**, No.2, Gordon and Breach, London, 1997, 1-125.

[3] Buchstaber, V.M., Enolskii, V.Z. and Leykin, D.V., Rational analogue of Abelian functions, *Funct. Annal. Appl.* **33-2** (1999), 83-94.

[4] F. Klein, Ueber hyperelliptische Sigmafunctionen, *Math. Ann.* **27** (1886),341-464 .

[5] F. Klein, Ueber hyperelliptische Sigmafunctionen (Zweiter Aufsatz), *Math. Ann.* **32** (1888), 351-380.

[6] I.G. Macdonald, *Symmetric Functions and Hall Polynomials, second edition*, Oxford University Press, 1995.

[7] A. Nakayashiki, On algebraic expressions of sigma functions for (n, s) curves, preprint.

[8] 野海　正俊, パンルヴェ方程式, , 朝倉書店, 2000.

[9] 梅村　浩, 楕円関数論, , 東京出版会, 2000.

[10] E.T. Whittaker and G.N. Watson, *A course of modern analysis*, Cambridge University Press, 1902.

第 15 回 整数論サマースクール 報告集, pp.191-198

Inversions of Abelian Integrals

難波 誠*

1 Weierstrass の楕円関数論の一解釈

Weierstrass の楕円関数論を幾何学的に解釈すると, 次のようになる:

$$W = \{ \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \in \mathbb{C}^2 \Big| \omega_2 \neq 0, \mathrm{Im}(\omega_1/\omega_2) > 0 \},$$

$$G = \left\{ \begin{pmatrix} 1 & n_1 & n_2 \\ 0 & a & b \\ 0 & c & d \end{pmatrix} \in \mathrm{SL}(3,\mathbb{Z}) \right\}$$

とおくと, G は $\mathbb{C} \times W$ に行列群として, 真性不連続, かつ固定点なしに作用[1]する. したがって商空間 $(\mathbb{C} \times W)/G$ は複素多様体になる.

$$V = \left\{ \big((x,y),(g_2,g_3)\big) \in \mathbb{P}^2 \times \mathbb{C}^2 \,|\, y^2 = 4x^3 - g_2 x - g_3,\ {g_2}^3 \neq 27{g_3}^2 \right\}$$

($(x,y) = (1:x:y)$ は $\mathbb{P}^2 = \mathbb{P}^2(\mathbb{C})$ の非斉次座標) とおくと, 正則写像

$$\widetilde{\wp} : (z,\omega_1,\omega_2) \in \mathbb{C} \times W \mapsto \big((\wp(z),\wp'(z)),(E_2,E_3)\big) \in V$$

($\wp$ は Weierstrass の $\wp$-関数, E_2, E_3 は Eisenstein 級数 $E_2 = E_2(\omega_1,\omega_2)$, $E_3 = E_3(\omega_1,\omega_2)$) は双正則写像

$$(\mathbb{C} \times W)/G \underset{\cong}{\longrightarrow} V$$

を導く. $\widetilde{\wp}$ の逆写像 $\widetilde{\wp}^{-1}$ (多価写像) は次であたえられる:

$$\big((x,y),(g_2,g_3)\big) \in V \mapsto \left(\int_\infty^{(x,y)} \frac{dx}{y},\ \left(\int_\beta \frac{dx}{y}, \int_\alpha \frac{dx}{y} \right) \right) \in \mathbb{C} \times W.$$

ここに α, β はトーラス $y^2 = 4x^3 - g_2 x - g_3$ の homology basis で $\alpha \cdot \beta = 1$ (交点数) となるもの.

*追手門学院大学経済学部, 〒 567-8502 茨木市西安威 2–1–15, Email : namba@res.otemon.ac.jp

[1] $\gamma = \begin{pmatrix} 1 & n_1 & n_2 \\ 0 & a & b \\ 0 & c & d \end{pmatrix}$ は $(z,(\omega_1,\omega_2))$ に対して $\gamma(z,(\omega_1,\omega_2)) = (z + n_1\omega_1 + n_2\omega_2, (a\omega_1 + b\omega_2, c\omega_1 + d\omega_2))$ と作用する.

注意 1.1. 楕円曲線のモジュライ理論, テータ関数論は, この理論の「射影化」と解釈できる.

2 周期積分

上の理論の analogy を genus が高い場合に作りたいが, いくつか困難がある. 以下に述べるのは, 困難でない部分だけを取り上げたものである.

$$\mathbb{H}_g = \{A \in \mathrm{GL}(g,\mathbb{C}) |^t A = A, \mathrm{Im}(A) > 0\}$$

($\mathrm{Im}(A) > 0$ は A の虚部が正定値を意味する) を Siegel の上半空間, ($g \geqq 2$).

$\mathbb{A}_g = \mathbb{H}_g/\mathrm{PSp}(2g,\mathbb{Z})$: 主偏極 g 次元アーベル多様体のモジュライ空間,

$\dim \mathbb{H}_g = \dim \mathbb{A}_g = \dfrac{g(g+1)}{2}$,

$\mathbb{M}_g =$ genus g の compact Riemannn 面 の moduli space,

$\dim \mathbb{M}_g = 3g-3$.

X を genus g の compact Riemann 面, $J(X)$ をその Jacobi 多様体とする.

Torelli の定理

$$\iota : [X] \in \mathbb{M}_g \mapsto [J(X)] \in \mathbb{A}_g$$

は holomorphic injection である.

注意 2.1. (1) 元の Torelli の定理は「injection である」だが holomorphic injection ($d\iota$ も injective) がわかったのは, そんな昔ではない.
(2) 像 $\iota(\mathbb{M}_g)$ の特長付けは, Schottky の問題とよばれ, 難問だったが, 近年かなりわかってきた.

さて, $g=2$, $g=3$ のときは

$$\dim \mathbb{M}_2 = \dim \mathbb{A}_2 = 3,$$
$$\dim \mathbb{M}_3 = \dim \mathbb{A}_3 = 6$$

と一致している.

$\iota(\mathbb{M}_2)$ は $\mathbb{A}_2$ の中の Zariski open set で $\mathbb{A}_2 - \iota(\mathbb{M}_2)$ は elliptic curves の積であるアーベル曲面の locus である. $\iota(\mathbb{M}_3)$ も同様である. この辺りの詳細は, 上野-清水 [2] を参照されたい.

さて

$$\kappa : \mathbb{H}_2 \to \mathbb{A}_2 = \mathbb{H}_2/\mathrm{PSp}(4,\mathbb{Z})$$

を自然な射影とするとき, $\kappa^{-1}(\iota(\mathbb{M}_2))$ は $\mathbb{H}_2$ の Zariski open set である.

$$W = \left\{ \begin{pmatrix} \Omega_1 \\ \Omega_2 \end{pmatrix} = \Omega \in \mathrm{GL}(2,\mathbb{C})^2 \middle| \Omega_1 {\Omega_2}^{-1} \in \kappa^{-1}(\iota(\mathbb{M}_2)) \right\}$$

とおく. W は次の写像で $\kappa^{-1}(\iota(\mathbb{M}_2)) \times \mathrm{GL}(2,\mathbb{C})$ と双正則で, $\dim W = 7$ である:

$$\begin{pmatrix} \Omega_1 \\ \Omega_2 \end{pmatrix} \in W \mapsto \begin{pmatrix} \Omega_1 {\Omega_2}^{-1} \\ \Omega_2 \end{pmatrix} \in \kappa^{-1}(\iota(\mathbb{M}_2)) \times \mathrm{GL}(2,\mathbb{C}).$$

今

$$G = \left\{ \begin{pmatrix} 1 & m & n \\ 0 & A & B \\ 0 & C & D \end{pmatrix} \in \mathrm{SL}(5,\mathbb{Z}) \;\middle|\; m = (m_1, m_2),\ n = (n_1, n_2),\ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Sp}(4,\mathbb{Z}) \right\}$$

とおく. G は $\mathbb{C}^2 \times W$ に行列群として, 真正不連続, かつ固有点なしに作用する. したがって $(\mathbb{C}^2 \times W)/G$ は複素多様体である.

$$\begin{aligned} U = \{ a = (a_0, a_1, \cdots, a_6) \in \mathbb{C}^7 \mid \\ X_a : y^2 = a_0 x^6 + a_1 x^5 + \cdots + a_6 \text{ が genus 2 の compact Riemann 面} \} \end{aligned}$$

とおく. この条件は, $a_0 \neq 0$ のときは右辺の多項式の判別式がゼロでないことであり, $a_0 = 0$ のときは右辺の 5 次の多項式の判別式がゼロでないことである. $\{\alpha_1, \alpha_2, \beta_1, \beta_2\}$ を $H_1(X_a, \mathbb{Z})$ の symplectic basis $(\alpha_i \cdot \beta_j = \delta_{ij})$ とし, 多価正則写像 (周期積分を用いた周期写像)

$$\Omega : a \in U \mapsto \Omega(a) \in W$$

を考える. ここに

$$\Omega(a) = \begin{pmatrix} \Omega_1(a) \\ \Omega_2(a) \end{pmatrix}, \quad \Omega_1(a) = \begin{pmatrix} \int_{\beta_1} \frac{xdx}{y} & \int_{\beta_1} \frac{dx}{y} \\ \int_{\beta_2} \frac{xdx}{y} & \int_{\beta_2} \frac{dx}{y} \end{pmatrix}, \ \Omega_2(a) = \begin{pmatrix} \int_{\alpha_1} \frac{xdx}{y} & \int_{\alpha_1} \frac{dx}{y} \\ \int_{\alpha_2} \frac{xdx}{y} & \int_{\alpha_2} \frac{dx}{y} \end{pmatrix}.$$

定理 2.2. Ω は次の双正則写像を導く:

$$U \to W/\mathrm{Sp}(4,\mathbb{Z}).$$

系 2.3. $\Lambda = \Omega^{-1} : W \to U$ は, 上への well-defined 正則写像で, $\mathrm{Sp}(4,\mathbb{Z})$-不変かつ双正則写像 $W/\mathrm{Sp}(4,\mathbb{Z}) \cong U$ を導く. さらに Λ は次式を満たす:

$$\Lambda\left(\begin{pmatrix} \Omega_1 \\ \Omega_2 \end{pmatrix} {}^t A \right) = \frac{1}{(\det A)^2} R_6(A) \left(\Lambda \begin{pmatrix} \Omega_1 \\ \Omega_2 \end{pmatrix} \right).$$

ここに $A \in \mathrm{GL}(2,\mathbb{C})$ で, $R_6(A)$ は A の 6 次既約表現である.

注意 2.4. これと類似の定理が $g = 3$ の場合, すなわち非特異平面 4 次曲線の場合もなりたつと考えている.

定理の証明は, 二段に分かれていて, 次の順で行なう.

(1) 各点 $a \in U$ で $(d\Omega)_a$ の rank は 7 である. したがって局所的に双正則である.
(2) 大域的に injective である.

このうち (1) を示すには, $\partial(\frac{xdx}{y})/\partial a_j$, $\partial(\frac{dx}{y})/\partial a_j$ が第二種アーベル微分 (すなわり留数が各極でゼロになる有理型微分) であることを用いて, de Rham-Hodge の定理を使う. (2) を示すには, (1) と Torelli の定理と, 次の知られていることを用いる:

$$X_a : y^2 = a_0x^6 + a_1x^5 + \cdots + a_6,$$
$$X_b : y^2 = b_0x^6 + b_1x^5 + \cdots + b_6$$

が双正則 $\iff \exists \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, \mathbb{C})$ such that

$$x = \frac{az + b}{cz + d},$$
$$y = \frac{w}{(cz + d)^3},$$
$$a_0 = b_0p^6 + b_1p^5r + \cdots + b_6r^6,$$
$$\cdots$$
$$a_6 = b_0q^6 + b_1q^5s + \cdots + b_6s^6.$$

ここに

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}.$$

そしてこのとき

$$(\frac{xdx}{y}, \frac{dx}{y}) = (\frac{zdx}{w}, \frac{dz}{w}) \begin{pmatrix} a & b \\ c & d \end{pmatrix} (\det A)$$

という変換則がある.

3 基本アーベル関数

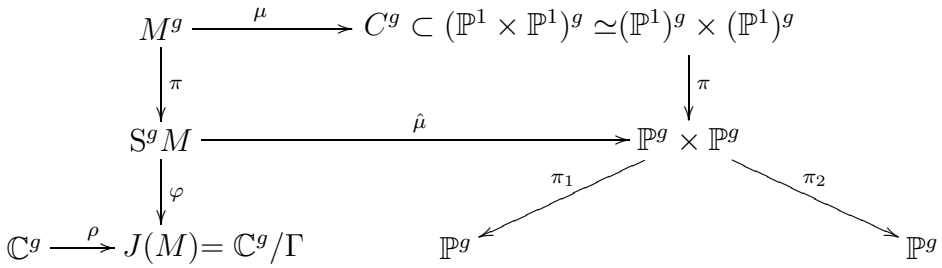
$\mathbb{C}$ 上で考える. $\mathbb{P}^n = \mathbb{P}^n(\mathbb{C})$ を対称積 $\mathrm{S}^n\mathbb{P}^1$ と同一視する. この同一視は, 非斉次座標を用いて,

$$\begin{aligned}
&\pi : (x_1, \cdots, x_n) \in (\mathbb{P}^1)^n \longmapsto (a_0 : a_1 : \cdots : a_n) \in \mathbb{P}^n, \\
&\frac{a_1}{a_0} = -(x_1 + \cdots + x_n), \\
&\frac{a_2}{a_0} = (x_1x_2 + \cdots + x_{n-1}x_n), \\
&\qquad \cdots\cdots\cdots \\
&\frac{a_n}{a_0} = (-1)^n x_1 \cdots x_n
\end{aligned}$$

で与えられる. (x_1, $\cdots$, x_n のうちの k 個が $\infty \iff a_0 = \cdots = a_{k-1} = 0$.) さて, $f(x, y)$ を規約多項式,

$$\begin{aligned}
&C = \{f(x, y) = 0\} \text{ の } \mathbb{P}^1 \times \mathbb{P}^1 \text{ での閉包}, \\
&\mu : M = \widetilde{C} \longrightarrow C \quad \text{正規化}
\end{aligned}$$

とおく. $\dim C = 1$ なので, 正規化 = 非特異化で, M は compact Riemann 面である. この genus を g とする. M 上の有理型関数の作る体 $\mathbb{C}(M)$ は, 代数関数体 $\mathbb{C}(x, y)$ と一致する. さて, 次の可換 diagram を考える:



ここで, $\mathrm{S}^g M$ は M の g 次対称積, $\hat{\mu}$ は μ より induce された正則写像, π, ρ, π_1, π_2 は自然な射影である. $\hat{\mu}$ は, $\mathrm{S}^g M$ から $\mathbb{P}^g \times \mathbb{P}^g$ への有限正則写像で, しかも generically injective になっている. したがって像 $\hat{\mu}(\mathrm{S}^g M)$ は projective variety で

$$\hat{\mu} : \mathrm{S}^g M \to \hat{\mu}(\mathrm{S}^g M)$$

は双有理な正則写像である. φ は Abel-Jacobi map で, 次で定義される:

$$P_1 + \cdots + P_g \in \mathrm{S}^g M \to \Big(\sum_{i=1}^{g} \int_{P_i^0}^{P_i} \omega_1, \cdots, \sum_{i=1}^{g} \int_{P_i^0}^{P_i} \omega_g \Big) \ (\bmod \Gamma) \in J(M)$$

(Γ : 周期の加群, $P_i^0 + \cdots + P_g^0 = D^0$: 固定因子.) φ は上への双有理正則写像 (Jacobi inversion) で, $J(M)$ の各元の逆像は, 完備な一次系になっている (Abel の定理). さて, 上への有理型写像

$$\wp^x : \mathbb{C}^g \dashrightarrow \mathbb{P}^g, \quad \wp^y : \mathbb{C}^g \dashrightarrow \mathbb{P}^g$$

を

$$\wp^x = \pi_1 \circ \hat{\mu} \circ \varphi^{-1} \circ \rho, \quad \wp^y = \pi_2 \circ \hat{\mu} \circ \varphi^{-1} \circ \rho$$

で定義する. $\mathbb{P}^g$ の斉次座標を用いて

$$\wp^x(z) = (1 : \xi_1(z) : \cdots : \xi_g(z)), \quad \wp^y(z) = (1 : \eta_1(z) : \cdots : \eta_g(z))$$

とおくと, $\xi_1(z), \cdots, \xi_g(z), \eta_1(z), \cdots, \eta_g(z)$ はアーベル関数で, これらが Riemann の基本アーベル関数である岩澤 ([1]). 上に述べた事から, ただちに

$$\mathbb{C}(J(M)) = \mathbb{C}\big(\xi_1(z), \cdots, \xi_g(z), \eta_1(z), \cdots, \eta_g(z)\big)$$

がわかる. これら $\xi_1(z), \cdots, \xi_g(z), \eta_1(z), \cdots, \eta_g(z)$ の間の基本関係式は

$$\begin{aligned} f(x_1, y_1) = 0, \ \cdots, \ f(x_g, y_g) = 0, \\ \xi_1 = -(x_1 + \cdots + x_g), \\ \cdots\cdots \\ \xi_g = (-1)^g x_1 \cdots x_g, \\ \eta_1 = -(y_1 + \cdots + y_g), \\ \cdots\cdots \\ \eta_g = (-1)^g y_1 \cdots y_g \end{aligned}$$

より $x_1, \cdots, x_g, y_1, \cdots, y_g$ を消去して得られる. (一般に, この計算はめんどうである.)

4 $g = 2$ の場合の基本アーベル関数

$g = 2$ の場合は, 計算が実行できる: $a = (a_0, a_1, a_2, a_3, a_4, a_5, a_6)$ を固定し, 二つの方程式

$$\begin{aligned} {y_1}^2 &= a_0 {x_1}^6 + a_1 {x_1}^5 + \cdots + a_5 x_1 + a_6 \\ {y_2}^2 &= a_0 {x_2}^6 + a_1 {x_2}^5 + \cdots + a_5 x_2 + a_6 \end{aligned}$$

を辺々加え, または掛ける. それらを

$$\begin{aligned} \xi_1 = -(x_1 + x_2), \quad \xi_2 = x_1 x_2 \\ \eta_1 = -(y_1 + y_2), \quad \eta_2 = y_1 y_2 \end{aligned}$$

であらわす:

$$\begin{aligned} {\eta_1}^2 - 2\eta_2 = {} & a_0({\xi_1}^6 - 6{\xi_1}^4 \xi_2 + 9{\xi_1}^2 {\xi_2}^2 - 2{\xi_2}^3) \\ & + a_1(-{\xi_1}^5 + 5{\xi_1}^3 \xi_2 - 5\xi_1 {\xi_2}^2) \\ & + a_2({\xi_1}^4 - 4{\xi_1}^2 \xi_2 + 2{\xi_2}^2) \\ & + a_3(-{\xi_1}^3 + 3\xi_1 \xi_2) \\ & + a_4({\xi_1}^2 - 2\xi_2) + a_5(-\xi_1) \\ & + 2a_6, \end{aligned} \tag{1}$$

$$\eta_2{}^2 = a_6{}^2\xi_2{}^6 + a_0a_6\xi_2{}^5(-\xi_1) + \cdots + a_5a_6(-\xi_1) + a_6{}^2. \tag{2}$$

これら (1), (2) が $\xi_1(z)$, $\xi_2(z)$, $\eta_1(z)$, $\eta_2(z)$ の間の基本関係式である. なお, (1), (2) は (上の記号で) $\hat{\mu}(\mathrm{S}^2M)$ の $\mathbb{P}^2 \times \mathbb{P}^2$ における定義方程式でもある.

$\wp^x$, $\wp^y$ を有理 (型) 写像

$$\wp^x : J(M) \dashrightarrow \mathbb{P}^2$$
$$\wp^y : J(M) \dashrightarrow \mathbb{P}^2$$

を見ると, これらは surjective で, (1), (2) によりその mapping degree は, それぞれ 4, 12 になっている.

また (1) より η_2 は ξ_1, ξ_2, η_1 の多項式であらわされるので

$$\mathbb{C}(J(M)) = \mathbb{C}\big(\xi_1(z), \xi_2(z), \eta_1(z)\big)$$

であり, $\xi_1(z)$, $\xi_2(z)$, $\eta_1(z)$ の間の基本関係式はその多項式を (2) に代入することにより得られる.

偏導関数 $\dfrac{\partial\xi_1}{\partial z_1}$ 等も $J(M)$ 上の有理型関数 (アーベル関数) なので, $\xi_1(z)$, $\xi_2(z)$, $\eta_1(z)$, $\eta_2(z)$ の有理式で書けるはずである. 実際, 上記の可換 diagram を用いて

$$d\wp^x = \begin{pmatrix} \dfrac{\partial\xi_1}{\partial z_1} & \dfrac{\partial\xi_1}{\partial z_2} \\ \dfrac{\partial\xi_2}{\partial z_1} & \dfrac{\partial\xi_2}{\partial z_2} \end{pmatrix}$$

を計算すると

$$d\wp^x = \begin{pmatrix} \dfrac{x_1y_2 - x_2y_1}{x_2 - x_1} & \dfrac{y_1 - y_2}{x_2 - x_1} \\ \dfrac{x_2{}^2y_1 - x_1{}^2y_2}{x_2 - x_1} & \dfrac{x_1y_2 - x_2y_1}{x_2 - x_1} \end{pmatrix}$$

となる. 各成分の分母, 分子に $y_1 + y_2 = -\eta_1$ をかけると, それらは ξ_1, ξ_2, η_1, η_2 であらわされ, 結局

$$\begin{aligned} \frac{\partial\xi_1}{\partial z_1} = \frac{\partial\xi_2}{\partial z_2} = \frac{1}{\eta_1}\big\{&\eta_2 - a_0(\xi_1{}^4\xi_2 - 3\xi_1{}^2\xi_2{}^2 + \xi_2{}^3) \\ &+ a_1(\xi_1{}^3\xi_2 - 2\xi_1\xi_2{}^2) - a_2(\xi_1{}^2\xi_2 - \xi_2{}^2) + a_3\xi_1\xi_2 - a_4\xi_2 + a_6\big\} \end{aligned} \tag{3}$$

$$\begin{aligned} \frac{\partial\xi_1}{\partial z_2} = \frac{1}{\eta_1}\big\{&a_0(-\xi_1{}^5 + 4\xi_1{}^3\xi_2 - 3\xi_1\xi_2{}^2) \\ &+ a_1(\xi_1{}^4 - 3\xi_1{}^2\xi_2 + \xi_2{}^2) + a_2(-\xi_1{}^3 + 2\xi_1\xi_2) \\ &+ a_3(\xi_1{}^2 - \xi_2) - a_4\xi_1 + a_5\big\} \end{aligned} \tag{4}$$

$$\begin{aligned} \frac{\partial\xi_2}{\partial z_1} = \frac{1}{\eta_1}\big\{&\xi_1\eta_2 - a_0(\xi_1{}^3\xi_2{}^2 - 2\xi_1\xi_2{}^3) + a_1(\xi_1{}^2\xi_2{}^2 - \xi_2{}^3) \\ &- a_2\xi_1\xi_2{}^2 + a_3\xi_2{}^2 - a_5\xi_2 + a_6\xi\big\} \end{aligned} \tag{5}$$

がえられる. $\dfrac{\partial \eta_1}{\partial z_1}$ 等の方は, より複雑であるが, 同様に得られる.

(4) より η_1 が $\xi_1, \xi_2, \dfrac{\partial \xi_1}{\partial z_2}$ で逆に解け, 従って

$$\mathbb{C}(J(M)) = \mathbb{C}\big(\xi_1(z), \xi_2(z), \frac{\partial \xi_1}{\partial z_2}(z)\big)$$

となっている.

加法定理も, 複雑な式になるが計算できる.

以上の議論において, 我々は $a = (a_0, \cdots, a_6)$ を固定し, 固定された

$$X_a = M : y^2 = a_0 x^6 + a_1 x^5 + \cdots + a_6$$

についての $J(M)$ 上のアーベル関数を議論してきた. 次に a を動かすことを考える. その場合は積分の始点となる因子 $D^0 = P_1^0 + P_2^0$ は $\infty_1 + \infty_2$ と取る. (∞_1, ∞_2 は無限遠点 $(\infty, \infty) \in \mathbb{P}^1 \times \mathbb{P}^1$ に対応する M の点.) そして, アーベル積分とその逆写像を考えるのである.

5 まとめ

以上から $g = 2$ の場合は, 有理型写像

$$(\wp^x, \wp^y, \Lambda) : \mathbb{C}^2 \times W \dashrightarrow \mathbb{P}^2 \times \mathbb{P}^2 \times U$$

とその像が, §2 の群 G による商多様体 $(\mathbb{C}^2 \times W)/G$ を「おおよそ」実現していると考えられる.

文 献

[1] 岩澤健吉： 代数函数論, 岩波書店, 1952

[2] 上野健爾・清水勇二： モジュライ理論 3, 岩波書店, 1999

第 15 回 整数論サマースクール 報告集, pp.199-210

CM 型の Abel 曲面について

梅垣 敦紀*

1 導入

1.1 1 次元（楕円曲線）の場合

一般に $\mathbf{C}$ 上の楕円曲線 E の自己準同型環 $\mathrm{End}(E)$ について，$\mathbf{Z}$ または 虚 2 次体の整環 $\mathcal{O}$ のどちらかに同型であることが知られている．言い換えれば，

$$\mathrm{End}(E)\otimes\mathbf{Q}=\begin{cases}\mathbf{Q}\\ K \quad (K:\text{虚 2 次体})\end{cases}$$

が成り立つ．

定義 1.1. 楕円曲線 E に対して，$\mathrm{End}(E)\otimes\mathbf{Q}=K$ となるとき，K に**虚数乗法** (**CM**) をもつという．

以下では，常に $\mathcal{O}_K$ を K の整数環として，

$$\mathrm{End}(E)\cong\mathcal{O}_K \tag{1}$$

となることを仮定する．

$\mathcal{A}_1$ を $\mathbf{C}$ 上の楕円曲線の moduli 空間とする．良く知られているように，上半平面 $\mathfrak{H}_1:=\{\tau\in\mathbf{C}\mid \mathrm{Im}(\tau)>0\}$ を用いれば，$\mathcal{A}_1$ は $\mathrm{SL}_2(\mathbf{Z})\backslash\mathfrak{H}_1$ と同一視できる．ここで，CM をもつ楕円曲線の同型類のなす $\mathcal{A}_1$ の部分集合

$$\mathcal{A}_1^{\mathrm{CM}}:=\{[E]\in\mathcal{A}_1\mid \mathrm{End}(E)\cong\mathcal{O}_K\ (\exists K:\text{虚 2 次体})\}$$

を考える．虚数乗法論によって，次がわかる．

Fact 1. $[E]\in\mathcal{A}_1^{\mathrm{CM}}$ に対して，以下の条件は同値である：

1. $j(E)\in\mathbf{Q}$,
2. E が $\mathbf{Q}$ 上定義される,

*早稲田大学高等研究所 (講演時の所属は「立教大学理学部」でした.)

3. 虚 2 次体 K の類数が 1 である.

また，条件 (3) について，1960 年代半ばに Baker, Stark によって示された次の事実は良く知られている.

Fact 2. 類数 1 の虚 2 次体は

$$\mathbf{Q}(\sqrt{d}) \quad (d = -1, -2, -3, -7, -11, -19, -43, -67, -163) \tag{2}$$

の 9 個に限られる.

今の 2 つの事実を併せると, 以下のことがわかる.

定理 1.2. $\mathcal{A}_1^{\mathrm{CM}}$ には丁度 9 個の $\mathbf{Q}$ 有理点が存在する.

これらの 9 個の有理点に対応する楕円曲線 $[E] \in \mathcal{A}_1^{\mathrm{CM}}$ の定義方程式は，類数 1 の虚 2 次体 $K = \mathbf{Q}(\sqrt{-d})$ $(d \in \mathbf{N})$ から以下のように簡単に求めることができる：

K の $\mathbf{C}$ への埋め込みを 1 つ決める．例えば,

$$K \hookrightarrow \mathbf{C}, \quad \sqrt{-d} \mapsto \sqrt{d}i \quad (i:\ \text{虚数単位})$$

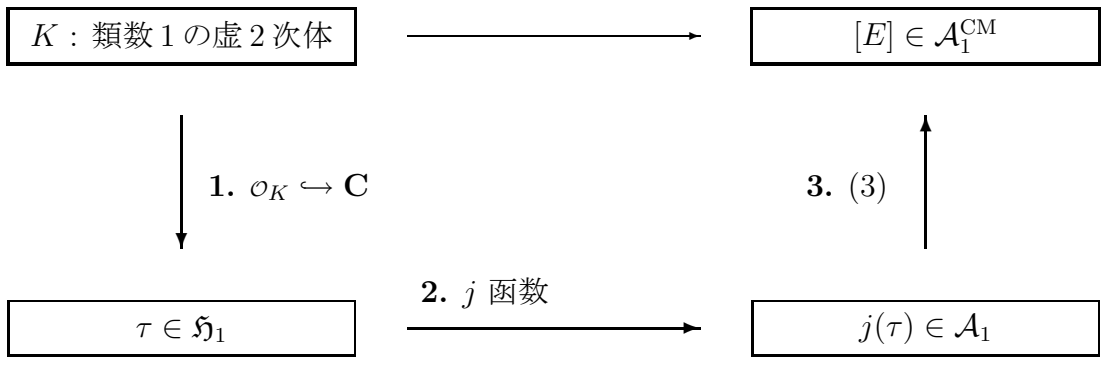
としておく．この埋め込みで $\tau \in \mathfrak{H}_1$ となる $\mathcal{O}_K$ の整基底 $\{1, \tau\}$ を選んで，整数環 $\mathcal{O}_K = \mathbf{Z} + \mathbf{Z}\tau \hookrightarrow \mathbf{C}$ を格子と見做せば，楕円曲線 $\mathbf{C}/\mathcal{O}_K$ を考えることができる．この楕円曲線の j 不変量は，j 函数の Fourier 展開

$$j(\tau) = \frac{1}{q} + 744 + 196884\ q + 21493760\ q^2 + 864299970\ q^3 + \cdots \quad (q = e^{2\pi i\tau})$$

を利用して近似計算することができる.（虚数乗法論から，$j(\tau) \in \mathbf{Z}$ が保証されていることにも注意する.）よって，定義方程式は

$$y^2 + xy = x^3 - \frac{36}{j(\tau) - 1728}x - \frac{1}{j(\tau) - 1728} \qquad (j(\tau) \neq 0, 1728) \tag{3}$$

で与えられる．以上のことをまとめると，計算の流れは以下のようになる：



例 1.3. 例えば，体 $K=\mathbf{Q}(\sqrt{-3})$ を考える．整数環を

$$\mathcal{O}_K=\mathbf{Z}+\mathbf{Z}\tau,\quad \tau=\frac{1+\sqrt{3}\,i}{2}\quad (i:\text{虚数単位})$$

として $\mathbf{C}$ 内の格子と見做すとき，j 函数を近似計算すると，$j(\tau)\fallingdotseq 0$ という値が求まる．$j=0$ となる楕円曲線 E は

$$E: y^2=x^3-1$$

であって，実際 $\mathrm{End}(E)$ には

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

という元が含まれる．

1.2 2 次元（Abel 曲面）の場合

総実代数体の総虚 2 次拡大を **CM 体**という．$K/\mathbf{Q}$ を 4 次 CM 体として，F を K に含まれる実 2 次体，$\mathcal{O}_K$ を K の整数環とする．$\mathcal{O}_K$ に CM をもつ Abel 曲面，即ち，Abel 曲面 $A/\mathbf{C}$, A の偏極 $\mathcal{C}$ と単射 $\theta\colon K\hookrightarrow \mathrm{End}(A)\otimes\mathbf{Q}$ で条件

$$\theta^{-1}(\mathrm{End}(A))=\mathcal{O}_K \tag{4}$$

を満たすものからなる 3 つ組 $(A,\mathcal{C},\theta)$ を考える．以下に於いては，CM をもつ Abel 曲面を考えるときは，常に (4) を仮定する．

定義 1.4. K の部分体 k に対して，$\mathbf{C}$ の部分体 M_k が以下の性質を満たすとき，$(A,\mathcal{C},\theta|_k)$ の **moduli の体**という：

任意の $\tau\in\mathrm{Aut}(\mathbf{C})$ に対して，$\tau\in\mathrm{Aut}(\mathbf{C}/M_k)$ となるための必要十分条件は

$$\begin{cases}\lambda(\mathcal{C})=\mathcal{C}^\tau,\\ \lambda\circ\theta(a)=\theta^\tau(a)\circ\lambda\quad(\forall a\in k)\end{cases}$$

を満たすような同型写像

$$\lambda\colon A\xrightarrow{\sim}A^\tau$$

が存在することである．

注意 1.4.1. 楕円曲線 E に対しては，moduli の体 $\mathbf{Q}(j(E))$ と定義体は一致したが，一般の Abel 多様体に対しては，moduli の体と定義体は必ずしも一致しない．

$\mathcal{A}_2$ を主偏極 Abel 曲面の moduli 空間とする．2 次元の Siegel 上半空間

$$\mathfrak{H}_2:=\{\tau\in\mathrm{M}_2(\mathbf{C})\mid \tau=\tau^t\ \text{かつ}\ \tau>0\}$$

を考えれば，$\mathcal{A}_2$ は $\mathrm{Sp}_2(\mathbf{Z})\backslash\mathfrak{H}_2$ と同一視できる．ここで，CM をもつ主偏極 Abel 曲面の同型類のなす部分集合

$$\mathcal{A}_2^{\mathrm{CM}}:=\{[(A,\mathcal{C})]\in\mathcal{A}_2\mid \mathrm{End}(A)\cong\mathcal{O}_K\ (\exists K:4\text{ 次 CM 体})\}$$

を考える．$\mathcal{A}_2^{\mathrm{CM}}$ の $\mathbf{Q}$ 有理点とはmoduliの体 $M_{\mathbf{Q}}$ が $\mathbf{Q}$ と一致するような点である．Fact 1.1, Fact 1.2 に対応する結果として，次の結果がある．

定理 1.5 (Murabayashi [4]). $K/\mathbf{Q}$ を4次CM体として，$[(A,\mathcal{C})] \in \mathcal{A}_2$ が $\mathrm{End}(A) \supseteq o_K$ を満たすとする．このとき，$[(A,\mathcal{C})] \in \mathcal{A}_2^{\mathrm{CM}}$ かつ $M_{\mathbf{Q}} = \mathbf{Q}$ となる必要十分条件は K が以下の条件 (a), (b) を満たすことである：

(a) K が

$$K = \mathbf{Q}(\sqrt{-q_1 \cdots q_t \varepsilon_F \sqrt{p}}) \quad (t \geq 0),$$

という形の表示をもつ．但し，ε_F は $\varepsilon_F > 0$ を満たす $F = \mathbf{Q}(\sqrt{p})$ の基本単数であって，$p, q_1, \ldots, q_t$ は以下の3条件 (a_1), (a_2), (a_3) のうちの1つを満たす相異なる素数である：

(a_1) $p \equiv 5 \pmod 8$ であって，さらに $t \geq 1$ ならば，

$$q_i \equiv 1 \pmod 4 \quad \text{かつ} \quad \left(\frac{p}{q_i}\right) = -1 \quad (i = 1, \ldots, t)$$

を満たす．

(a_2) $p \equiv 5 \pmod 8$, $t \geq 1$, $q_1 = 2$ であって，さらに $t \geq 2$ ならば，

$$q_i \equiv 1 \pmod 4 \quad \text{かつ} \quad \left(\frac{p}{q_i}\right) = -1 \quad (i = 2, \ldots, t)$$

を満たす．

(a_3) $p = 2$ であって，さらに $t \geqq 1$ ならば，

$$q_i \equiv 5 \pmod 8 \quad (i = 1, \ldots, t)$$

を満たす．

(b) K の相対類数 h_K^- が 2^t となる．

定理 1.6 (Murabayashi-U [6]). $K/\mathbf{Q}$ を (a) かつ (b) を満たす4次CM体として，$r = q_1 \cdots q_t$ とする．このとき，K は次の13個の体のいずれかであって，表中の線より上は類数が1であり，下は類数が2である：

K	p	ε_F	r
$\mathbf{Q}\left(\sqrt{-(2+\sqrt{2})}\right)$	2	$1+\sqrt{2}$	1
$\mathbf{Q}\left(\sqrt{-(5+2\sqrt{5})}\right)$	5	$\frac{1+\sqrt{5}}{2}$	1
$\mathbf{Q}\left(\sqrt{-(13+2\sqrt{13})}\right)$	13	$\frac{3+\sqrt{13}}{2}$	1
$\mathbf{Q}\left(\sqrt{-(29+2\sqrt{29})}\right)$	29	$\frac{5+\sqrt{29}}{2}$	1
$\mathbf{Q}\left(\sqrt{-(37+6\sqrt{37})}\right)$	37	$6+\sqrt{37}$	1
$\mathbf{Q}\left(\sqrt{-(53+2\sqrt{53})}\right)$	53	$\frac{7+\sqrt{53}}{2}$	1
$\mathbf{Q}\left(\sqrt{-(61+6\sqrt{61})}\right)$	61	$\frac{39+5\sqrt{61}}{2}$	1
$\mathbf{Q}\left(\sqrt{-5(2+\sqrt{2})}\right)$	2	$1+\sqrt{2}$	5
$\mathbf{Q}\left(\sqrt{-(5+\sqrt{5})}\right)$	5	$\frac{1+\sqrt{5}}{2}$	2
$\mathbf{Q}\left(\sqrt{-13(5+2\sqrt{5})}\right)$	5	$\frac{1+\sqrt{5}}{2}$	13
$\mathbf{Q}\left(\sqrt{-17(5+2\sqrt{5})}\right)$	5	$\frac{1+\sqrt{5}}{2}$	17
$\mathbf{Q}\left(\sqrt{-(13+3\sqrt{13})}\right)$	13	$\frac{3+\sqrt{13}}{2}$	2
$\mathbf{Q}\left(\sqrt{-5(13+2\sqrt{13})}\right)$	13	$\frac{3+\sqrt{13}}{2}$	5

次節で解説する計算によって，上の定理の 13 個の体の各イデアル類のそれぞれに対して，1 つずつの主偏極 Abel 曲面の同型類 $[(A,\mathcal{C})] \in \mathcal{A}_2^{\mathrm{CM}}$ が定まることがわかるから，次の結論を得る．

定理 1.7 (Murabayashi-U [6]). $\mathcal{A}_2^{\mathrm{CM}}$ には丁度 19 個の $\mathbf{Q}$ 有理点が含まれる．

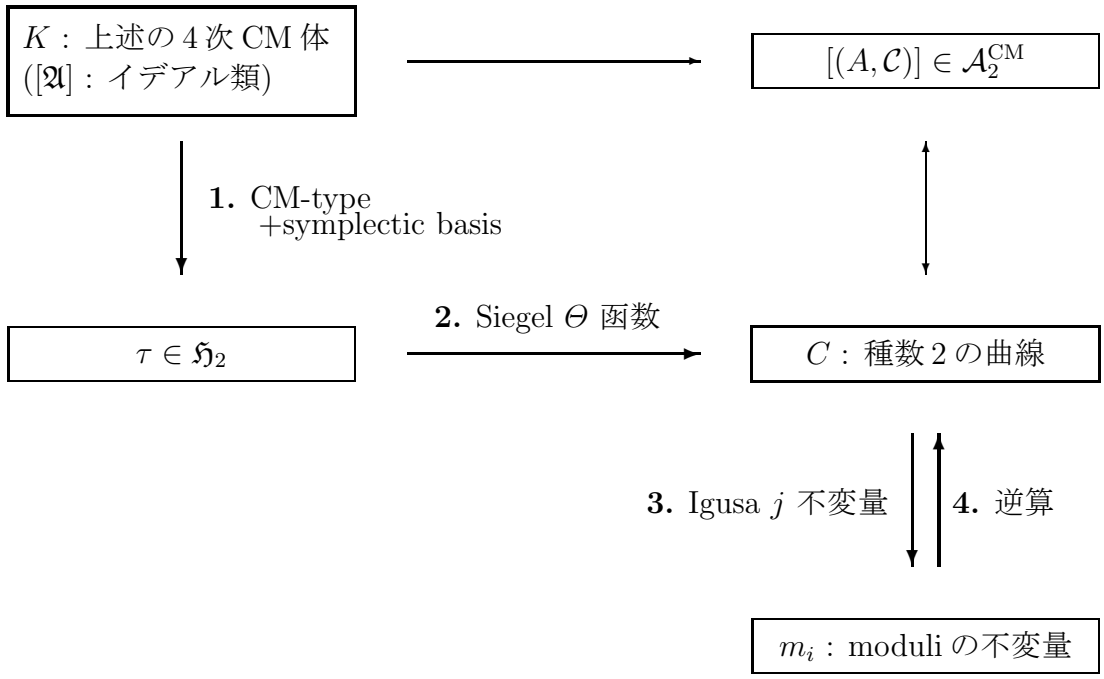
注意 1.7.1. 主偏極でない偏極をもつ Abel 曲面の moduli 空間に対しても，$\mathbf{Q}$ 有理 CM 点の個数は決定されている (cf. [8])．

注意 1.7.2. 村林氏によって，次節で行うような計算を行わなくても，具体的な Hecke 指標を構成することにより，理論的に各イデアル類に対応するアーベル曲面の存在がわかる (cf. [5])．

ここで，1 次元の場合には，例 1.3 で見たように，$\mathcal{A}_1^{\mathrm{CM}}$ の $\mathbf{Q}$ 有理点に対応する楕円曲線を復元することができたことを思い出してみる．これと同様に 2 次元の場合にも,「19 個の主偏極 Abel 曲面を 4 次 CM 体の情報から復元することは可能であるか?」という疑問が生じる．定理 1.5 の条件を満たす 13 個の体 K は巡回拡大である．ゆえに，虚数乗法論から，19 個の点に対応する主偏極 Abel 曲面 $(A,\mathcal{C})$ は単純となることがわかる．よって，これらは種数 2 の代数曲線の Jacobi 多様体として得られるから，この曲線の定義方程式を求めることを目標とする．

2　計算に必要な知識

まず始めに，上述の 13 個の 4 次 CM 体 K の（イデアル類 $\mathfrak{A}$）から対応する種数 2 の代数曲線 C の定義方程式を計算するための流れを図示しておいて，その後で各 step に必要な言葉の定義と意味を説明する：



2.1　CM-type

1 次元の場合は，虚 2 次体の $\mathbf{C}$ への埋め込みを指定することで整数環（とイデアル）を $\mathbf{C}$ の格子と見做すことができた．2 次元の場合にも，4 次 CM 体の整数環（とイデアル）を $\mathbf{C}^2$ 内の格子と見做すことができる．そのために，次の CM-type を定義する．

定義 2.1. 4 次 CM 体 K の $\mathbf{C}$ への埋め込み $\iota : K \hookrightarrow \mathbf{C}$ 全体のなす集合を I とする．I の部分集合

$$\Phi = \{\sigma_1, \sigma_2\}$$

に対して，$\Phi \cup \overline{\Phi} = I$ となるとき，Φ を **CM-type** という．但し，$\bar{\cdot}$ を複素共役とするとき，$\overline{\Phi} = \{\overline{\sigma}_1, \overline{\sigma}_2\}$ を意味する．

CM-type $\Phi = \{\sigma_1, \sigma_2\}$ に対して，同型

$$\Phi\colon K \otimes_{\mathbf{Q}} \mathbf{R} \longrightarrow \mathbf{C}^2, \qquad \alpha \otimes a \mapsto (a\alpha^{\sigma_1}, a\alpha^{\sigma_2})$$

が誘導される．K の分数イデアル $\mathfrak{A}$ に対して，$\Lambda_{\mathfrak{A}} := \Phi(\mathfrak{A})$ は $\mathbf{C}^2$ 内の格子となるから，複素トーラス $\mathbf{C}^2/\Lambda_{\mathfrak{A}}$ を考えることができる．このとき，$\eta \in K$ を

$$\overline{\eta} = -\eta, \quad \mathrm{Im}(\eta^{\tau}) > 0 \quad (\tau = \sigma_1, \sigma_2)$$

を満たすようにとると，

$$e(\Phi(x),\Phi(y)) = \mathrm{Tr}_{K/\mathbf{Q}}(\eta x\overline{y}) \qquad (\forall x,y\in K)$$

が $\mathbf{C}^2/\Lambda_{\mathfrak{A}}$ に付随する Riemann form となるから，複素トーラス $\mathbf{C}^2/\Lambda_{\mathfrak{A}}$ は Abel 曲面となる．

定義 2.2. 上述の様にして得られる $(\mathbf{C}^2/\Lambda_{\mathfrak{A}},\eta)$ を **type (K,Φ)** の Abel 曲面という．

逆に，K に CM をもつ Abel 多様体 $(A,\mathcal{C},\theta)$ に対して，CM-type Φ と K のイデアル $\mathfrak{A}$, さらに $\eta\in K$ が存在する．したがって，以下では $(A,\mathcal{C},\theta)$ と $(K,\Phi;\mathfrak{A},\eta)$ の組を同一視する．

注意 2.2.1. CM-type の取り方は本来は複数ある．しかしながら，我々が考えている 4 次 CM 体は巡回拡大だから，$\mathrm{Gal}(K/\mathbf{Q})$ の生成元を σ とする．ここで，埋め込み $\iota : K\hookrightarrow\mathbf{C}$ を 1 つ指定したとき，$\Phi=\{\iota\circ\mathrm{id.},\iota\circ\sigma\}$ という 1 つの CM-type を考えれば十分であることがわかる．以下では，この CM-type を単に $\Phi=\{1,\sigma\}$ とかく．

2.2 symplectic basis

次に，今得られた主偏極 Abel 曲面の複素トーラスとしての表示から，対応する Siegel 上半空間 $\mathfrak{H}_2$ の点を求める．

定義 2.3. $(A,\mathcal{C},\theta)$ を K に CM をもつ主偏極 Abel 曲面として，対応する組を $(K,\Phi;\mathfrak{A},\eta)$ とする．$\mathfrak{A}$ の $\mathbf{Z}$ 基底 (v_1,v_2,v_3,v_4) (即ち，$\mathfrak{A}=\mathbf{Z}v_1+\mathbf{Z}v_2+\mathbf{Z}v_3+\mathbf{Z}v_4$) について，行列 $(a_{ij})=(e(\Phi(v_i),\Phi(v_j)))$ が

$$(a_{ij}) = \begin{pmatrix} & I_2 \\ -I_2 & \end{pmatrix}$$

をみたすとき，**symplectic basis** という．

注意 2.3.1. A が主偏極をもつとき，symplectic basis が存在する．

我々が考えている主偏極 Abel 曲面に対応する組を $(K,\{1,\sigma\};\mathfrak{A},\eta)$ とする．$\mathfrak{A}$ の symplectic basis (v_1,v_2,v_3,v_4) をとって，行列 A, B を

$$A=\begin{pmatrix} v_1 & v_2 \\ v_1^\sigma & v_2^\sigma \end{pmatrix},\ B=\begin{pmatrix} v_3 & v_4 \\ v_3^\sigma & v_4^\sigma \end{pmatrix}$$

で定義する．このとき，

$$\tau = -B^{-1}A$$

が対応する Siegel 上半空間 $\mathfrak{H}_2$ の点である．

2.3 Siegel Θ-函数

楕円曲線の場合は，保型函数 j の近似計算が必要であった．これに対応するものとして $\mathfrak{H}_2 \times \mathbf{C}^2$ 上の **Siegel Θ 函数**を以下で定義する：

$$\Theta\left(\tau, z\,;\begin{bmatrix} a_1 & b_1 \\ a_2 & b_2 \end{bmatrix}\right)$$
$$:= \sum_{n\in\mathbf{Z}^2} \exp\left(\frac{1}{2}\left(n+\frac{1}{2}\begin{bmatrix} a_1 \\ a_2 \end{bmatrix}\right)^t \tau \left(n+\frac{1}{2}\begin{bmatrix} a_1 \\ a_2 \end{bmatrix}\right) + \left(n+\frac{1}{2}\begin{bmatrix} a_1 \\ a_2 \end{bmatrix}\right)^t \left(z+\frac{1}{2}\begin{bmatrix} b_1 \\ b_2 \end{bmatrix}\right)\right).$$

但し，$a_i, b_i \in \{0,1\}$ とする．ここで，

$$\Theta_{a_1a_2b_1b_2} := \Theta\left(\tau, 0\,;\begin{bmatrix} a_1 & b_1 \\ a_2 & b_2 \end{bmatrix}\right)$$

とおいて，さらに，

$$\lambda_1 := \left(\frac{\Theta_{1100}\Theta_{1000}}{\Theta_{0100}\Theta_{0000}}\right)^2,\ \lambda_2 := \left(\frac{\Theta_{1001}\Theta_{1100}}{\Theta_{0001}\Theta_{0100}}\right)^2,\ \lambda_3 := \left(\frac{\Theta_{1001}\Theta_{1000}}{\Theta_{0001}\Theta_{0000}}\right)^2$$

を定義する．

命題 2.4 ([2]). $\tau \in \mathfrak{H}_2$ は種数 2 の曲線

$$y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$$

に対応する．

2.4 Igusa j 不変量

上の Propositionで得られた曲線の定義方程式は，係数がいずれの体に含まれているかわからない．我々が扱っている主偏極 Abel 曲面の moduli の体 $M_{\mathbf{Q}}$ が $\mathbf{Q}$ であるので，この性質を利用して，より定義体の小さい定義方程式を求めることを考える．

$\mathbf{C}$ 上の種数 2 の曲線 C は

$$f(x) = a_0x^6 + a_1x^5 + a_2x^4 + a_3x^3 + a_4x^2 + a_5x + a_6$$

に対して．

$$C : y^2 = f(x) \quad (a_0 \neq 0 \text{ または } a_1 \neq 0) \tag{5}$$

とかける．楕円曲線の j 不変量と同様に同型類を表現するための不変量として **Igusa J 不変量**が知られている．これは $\mathbf{Q}[a_0, \ldots, a_6]$ の元であって，以下の式で定義される：

$$J_2 = 2^{-2}(-120a_0a_6 + 20a_1a_5 - 8a_2a_4 + 3a_3^2),$$
$$J_4 = 2^{-7}(240(a_0a_3a_4a_5 + a_1a_2a_3a_6) - 400(a_0a_2a_5^2 + a_1^2a_4a_6) - 64(a_0a_4^3 + a_2^3a_6)$$

$$
\begin{aligned}
&+16(a_1a_3a_4^2+a_2^2a_3a_5)-672a_0a_3^2a_6+240a_1^2a_5^2-112a_1a_2a_4a_5-8a_1a_3^2a_5\\
&+16a_2^2a_4^2-16a_2a_3^2a_4+3a_3^4+2640a_0^2a_6^2-880a_0a_1a_5a_6+1312a_0a_2a_4a_6),\\
J_6 =&2^{-10}(1600(a_0^2a_4^2a_5^2+a_1^2a_2^2a_6^2)+1600(a_0a_1a_2a_5^3+a_1^3a_4a_5a_6)\\
&+640(a_0a_1a_3a_4a_5^2+a_1^2a_2a_3a_5a_6)-4000(a_0^2a_3a_5^3+a_1^3a_3a_6^2)\\
&-384(a_0a_1a_4^3a_5+a_1a_2^3a_5a_6)-640(a_0a_2^2a_4a_5^2+a_1^2a_2a_4^2a_6)\\
&+80(a_0a_2a_3^2a_5^2+a_1^2a_3^2a_4a_6)+192(a_0a_2a_3a_4^2a_5+a_1a_2^2a_3a_4a_6)\\
&-48(a_0a_3^3a_4a_5+a_1a_2a_3^3a_6)-224(a_1^2a_3a_4^2a_5+a_1a_2^2a_3a_5^2)\\
&+64(a_1^2a_4^4+a_2^4a_5^2)-64(a_1a_2a_3a_4^3+a_2^3a_3a_4a_5)+16(a_1a_3^3a_4^2+a_2^2a_3^3a_5)\\
&-4096(a_0^2a_4^3a_6+a_0a_2^3a_6^2)+6400(a_0^2a_2a_5^2a_6+a_0a_1^2a_4a_6^2)\\
&+10560(a_0^2a_3a_4a_5a_6+a_0a_1a_2a_3a_6^2)+2624(a_0a_1a_3a_4^2a_6+a_0a_2^2a_3a_5a_6)\\
&-4432a_0a_1a_3^2a_5a_6-8a_2a_3^4a_4+a_3^6-320a_1^3a_5^3+64a_1^2a_2a_4a_5^2+176a_1^2a_3^2a_5^2\\
&+128a_1a_2^2a_4^2a_5+112a_1a_2a_3^2a_4a_5-28a_1a_3^4a_5+16a_2^2a_3^2a_4^2+5120a_0^3a_6^3\\
&-2544a_0^2a_3^2a_6^2+312a_0a_3^4a_6-14336a_0^2a_2a_4a_6^2+1024a_0a_2^2a_4^2a_6-2560a_0^2a_1a_5a_6^2\\
&-2240a_0a_1^2a_5^2a_6-6528a_0a_1a_2a_4a_5a_6-1568a_0a_2a_3^2a_4a_6),\\
J_{10} =&2^{-12}\mathrm{disc}_6(f).
\end{aligned}
$$

但し，disc_6 は f を 6 次の多項式と見たときの判別式である．さらに，$J_{10}\neq 0$ のとき，**moduli の不変量**

$$m_1=\frac{J_2^5}{J_{10}},\ m_2=\frac{J_2^3J_4}{J_{10}},\ m_3=\frac{J_2^2J_6}{J_{10}}$$

を定義する．このとき，以下の定理がある：

定理 2.5 (Igusa [1]). C と C' を $J_{10}\neq 0$ を満たす種数 2 の曲線として，m_i と m_i' を対応する moduli の不変量とする．このとき，C と C' が $\mathbf{C}$ 上同型であるための必要十分条件はすべての $i=1,2,3$ に対して

$$m_i=m_i'$$

が成り立つことである．

注意 2.5.1. 我々が扱っている主偏極 Abel 曲面は，moduli の体 $M_{\mathbf{Q}}$ が $\mathbf{Q}$ であったから，$m_i\in\mathbf{Q}$ となる．

注意 2.5.2. 種数 2 の曲線についても moduli の体と定義体は必ずしも一致しない，即ち，$m_i\in\mathbf{Q}$ であっても，$\mathbf{Q}$ 上の model をもつとは限らない (cf. Remark 1.4.1).

3 計算例

実際に，計算をするためには，以下の 5 つの step を踏めば良い：

1. o_K の整基底（対応するイデアル類 $\mathfrak{A}$ の $\mathbf{Z}$ 上の基底）を求めて，適当な η を選び，symplectic basis を用いて，対応する点 $\tau\in\mathfrak{H}_2$ を求める．
2. Θ 函数の値を計算して，$\lambda_1,\lambda_2,\lambda_3$ を求める．

3. 対応する moduli の不変量 m_1, m_2, m_3 を求めて，$\mathbf{Q}$ の元で近似する．

4. moduli の不変量 m_1, m_2, m_3 から，C を復元する．

5. 求めた C が条件を満たす曲線かどうかを確認する．

この計算を実際に行なえば，$\mathcal{A}_2^{\mathrm{CM}}$ の 19 個の $\mathbf{Q}$ 有理点に対応する種数 2 の曲線の定義方程式 C を求めることができる．

例 3.1. 7 個の類数 1 の 4 次 CM 体 $K = \mathbf{Q}(\sqrt{-r\varepsilon_F\sqrt{p}})$ に対して，moduli の不変量 m_i を求めると，以下のようになる：

p	r	m_1	m_2	m_3
2	1	$2^4 \cdot 3^{15}$	$2 \cdot 3^{10} \cdot 61$	$3^7 \cdot 47$
5	1	0	0	0
13	1	2^{25}	$2^{18} \cdot 7$	$2^{14} \cdot 11$
29	1	$\frac{2^{35} \cdot 3^{10} \cdot 11^5}{5^{12}}$	$\frac{2^{24} \cdot 3^7 \cdot 11^3 \cdot 37 \cdot 73 \cdot 109}{5^{12}}$	$\frac{2^{18} \cdot 3^6 \cdot 11^2 \cdot 17 \cdot 31 \cdot 89 \cdot 827}{5^{12}}$
37	1	$-\frac{2^{30} \cdot 1319^5}{3^7 \cdot 11^{12}}$	$-\frac{2^{21} \cdot 1319^3 \cdot 5647 \cdot 8167}{3^8 \cdot 11^{12}}$	$\frac{2^{16} \cdot 13 \cdot 1297 \cdot 1319^2 \cdot 6976381}{3^{10} \cdot 11^{12}}$
53	1	$\frac{2^{25} \cdot 3^{15} \cdot 5805193^5}{17^{12} \cdot 29^{12}}$	$\frac{2^{21} \cdot 3^{10} \cdot 11 \cdot 571 \cdot 5805193^3 \cdot 884388736313}{17^{12} \cdot 29^{12}}$	$\frac{2^{15} \cdot 3^7 \cdot 31 \cdot 37 \cdot 47 \cdot 5805193^2 \cdot 1952727367 \cdot p_1}{17^{12} \cdot 29^{12}}$
61	1	$-\frac{2^{25} \cdot 7^{15} \cdot 39079^5}{3^{19} \cdot 5^{12} \cdot 41^{12}}$	$\frac{2^{25} \cdot 7^9 \cdot 13 \cdot 239 \cdot 39079^3 \cdot 63649 \cdot 69539}{3^{20} \cdot 5^{12} \cdot 41^{12}}$	$\frac{2^{15} \cdot 7^7 \cdot 487 \cdot 3449 \cdot 3467 \cdot 39079^2 \cdot p_2}{3^{22} \cdot 5^{12} \cdot 41^{12}}$

(但し，$p_1 = 30482871647$, $p_2 = 42488533591199$ である.)

これらの moduli の不変量 m_i をもつ曲線を以下に挙げておく：

p	r	C
2	1	$y^2 = x^5 + 3x^4 - 2x^3 - 6x^2 + 3x + 1$
5	1	$y^2 = x^5 - 1$
13	1	$y^2 = x^5 - 156x^4 + 10816x^3 - 421824x^2 + 8998912x - 80427776$
29	1	$y^2 = 116x^5 - 928x^4 + 2552x^3 - 2900x^2 + 1492x - 289$
37	1	$y^2 = 131769x^5 - 951786x^4 - 497048x^3 - 113232x^2 - 12336x - 544$
53	1	$y^2 = 70241161x^5 + 54250213x^4 + 21706954x^3 + 4502426x^2 + 446045x + 16697$
61	1	$y^2 = 5191138125x^5 + 859281075x^4 - 70429502x^3 + 2736582x^2 - 214719x + 6095$

注意 3.1.1. これらの曲線がすべて $\mathbf{Q}$ 上定義されていることに注意されたい (cf. Remark 2.5.2)．同様の計算により，19 個の Abel 曲面のすべてに対しても，定義体が $\mathbf{Q}$ であることが確認できる．$\mathbf{Q}$ 上定義される 4 次 CM 体の整数環に CM をもつ種数 2 の曲線は，こうして得られた 19 個に限られる．

注意 3.1.2. Spallek や van Wamelen も沢山の CM 体を走らせて同様の計算を実行し $\mathbf{Q}$ 上定義される種数 2 の曲線を探索している (cf. [7], [9])．さらに，これらの曲線の Jacobi 多様体が実際に CM をもつことも確認している (cf. [10])．

注意 3.1.3. 今まで述べた計算法は $\mathcal{A}_2^{\mathrm{CM}}$ の $\mathbf{Q}$ -有理点で無くても有効である．例えば，$K = \mathbf{Q}(-3(1+\sqrt{2})\sqrt{2})$ は，Theorem 1.5 の条件 (a) を満たさない．しかしながら，

$$m_1 = \frac{2^4 \cdot 3 \cdot 26221231 \cdot 1656350182261 + 2^7 \cdot 7 \cdot 73 \cdot 97 \cdot 421 \cdot 32117 \cdot 16918079\sqrt{2}}{3 \cdot 7^{12}}$$
$$= \frac{1}{3 \cdot 7^{12}}(1+\sqrt{2})^2\sqrt{2}^8(5-\sqrt{2})^5(1+4\sqrt{2})^5(9-\sqrt{2})^5(13+24\sqrt{2})^5$$

$$m_2 = \frac{2\cdot 3\cdot 31\cdot 109\cdot 151\cdot 28005785343139 + 2^4\cdot 7\cdot 13\cdot 31\cdot 1301546813215981\sqrt{2}}{3^2\cdot 7^{12}},$$
$$= \frac{1}{3^2\cdot 7^{12}}(1+\sqrt{2})^2\sqrt{2}^2(5-\sqrt{2})^3(-1+4\sqrt{2})(1+4\sqrt{2})^3(9-\sqrt{2})^3$$
$$(13+24\sqrt{2})^3(305+12\sqrt{2})(563+10724\sqrt{2})$$
$$m_3 = \frac{3\cdot 1963819166621235607 + 2^3\cdot 5^2\cdot 7\cdot 20231\cdot 139343759033\sqrt{2}}{3^4\cdot 7^{12}}$$
$$= \frac{1}{3^4\cdot 7^{12}}(1+\sqrt{2})(5-\sqrt{2})^2(1+4\sqrt{2})^2(9-\sqrt{2})^2(13+24\sqrt{2})^2(13+27\sqrt{2})$$
$$(41+8\sqrt{2})(45-11\sqrt{2})(89+14\sqrt{2})(6649+721\sqrt{2})$$

という値を求めることができて，この値に対応する曲線の方程式は

$$y^2 = 3x^5 + (96+24\sqrt{2})x^4 + (836+280\sqrt{2})x^3 + (2256+696\sqrt{2})x^2 + (678-432\sqrt{2})x$$

であることがわかる.

参考文献

[1] J. Igusa, Arithmetic variery of moduli for genus two, *Ann. of Math. (2)* **72**, no. 3, 612–649, 1960.

[2] J. Igusa, On siegel modular formas of genus two, *Amer. J. Math.* **84**, 175–200, 1960.

[3] G. Shimura, Abelian varieties with complex multiplication and modular funcions, Princeton Mathematical Series **46**, Princeton Univ. Press, 1998.

[4] N. Murabayashi, The field of moduli of abelian surfaces with complex multiplication, *J. reine angew. Math.* **470**, 1–26, 1996.

[5] N. Murabayashi, Determination of simple CM abelian surfaces defined over $\mathbf{Q}$, *submitted*, 2007.

[6] N. Murabayashi-A. Umegaki, Determination of all $\mathbf{Q}$-rational CM-points in the moduli space of principally polarized abelian surfaces, *Journal of Algebra* **235**, 267–274, 2001.

[7] A. M. Spallek, *Kurven von Geshlecht* 2 *und ihre Anwendung in Public-Key-Kryptosystemen*, Preprint 18, Universität GH. Essen, Ellernstraße 29, 45326 Essen, Germany, 1994.

[8] A. Umegaki, Determination of all $\mathbf{Q}$-rational CM-points in the moduli spaces of polarized abelian surfaces, *Analytic Number Theory (Beijing/Tokyo 1999)*, 347–357, Dev. Math., 6, Kluwer, 2002.

[9] P. van Wamelen, Examples of genus two CM curves defined over the rationals, *Math. Comp.* **68**, no. 225, 307–320, 1999.

[10] P. van Wamelen, Proving that a genus 2 curve has complex multiplication, *Math. Comp.* **68**, no. 228, 1663–1677, 1999

第 15 回 整数論サマースクール 報告集, pp.211-222

暗号理論に向けての因子の加法の計算法

志村 真帆呂*

1 公開鍵暗号の基礎知識

有限アーベル群があると (解読されやすさは別にして) 公開鍵暗号が作れます.

そこで有限アーベル群として超楕円曲線の因子類群を選び, 公開鍵暗号を作ろうというのが本稿の背景の一つです.

定義 1 (離散対数問題) G を有限アーベル群, $a, b \in G$ を与えたとき, 次の方程式の整数解 x を求める問題を**離散対数問題**といいます.

$$a^x = b.$$

G の積を加法で書けば次のようになります.

$$ax = b.$$

解説 a^x の計算量と x を求めるための計算量に大きな差があるとき, その離散対数問題を用いて公開鍵暗号が作れます.

例 1 (離散対数問題を用いた公開鍵暗号の例)
暗号化に必要なデータと手順:

$$\text{受信者}\begin{cases} G: \text{有限アーベル群} \\ P \in G: \text{位数の大きな元} \\ e \in \mathbf{Z}: \text{秘密鍵} \\ Q := eP \\ (G, P, Q): \text{公開鍵} \end{cases} \qquad \text{送信者}\begin{cases} M \in G: \text{平文 (のコード化)} \\ r \in \mathbf{Z}: \text{秘密鍵} \\ C_1 := rP \\ C_2 := M + rQ \\ (C_1, C_2): \text{暗号文} \end{cases}$$

復号化の手順:

$$C_2 - eC_1 = M + rQ - erP = M + rQ - r(eP) = M + rQ - rQ = M$$

解説 秘密鍵 e を知っていると上記のように簡単に復号化 (暗号を正規の手続きで解読すること) できます.

公開鍵 (G, P, Q) だけから e を求めるためには, $eP = Q$ という離散対数問題を解く必要がありますが, その計算量が膨大だとすれば現実的に安全な暗号と言えます.

もちろん, e を直接求める以外の方法で暗号が破られないかを検証する必要はあります.

*東海大学 理学部

1.1 目標

有効な公開鍵暗号を作るためには超楕円曲線の因子類群に関する離散対数問題の計算量が大きくなることの保証と, 因子類群の加算を高速に行うアルゴリズムが必要です.

本稿では, 後者の因子類群の加算の高速化について論じます.

加算を高速化するには因子の表示にも工夫が必要ですが, 都合のよいことに超楕円曲線の因子には多項式表現 (Mumford 表現) という非常に使い勝手のよいものがあります.

2 準備

2.1 定義と記法

- k : 体.
- $\overline{k}$: k の代数閉包.
- C : k 上定義された超楕円曲線.
- $k[C]$: C の k 上の座標環.
- $k(C) := \left\{ \dfrac{g}{f} \middle| f, g \in k[C], f \neq 0 \right\}$: C の k 上の関数体.
- $k[C]_P := \left\{ \dfrac{g}{f} \middle| f, g \in k[C], f(P) \neq 0 \right\}$: $k[C]$ の 点 $P(\in C)$ での局所化.

2.2 超楕円曲線 (Hyperelliptic curves)

この講演では超楕円曲線暗号への応用を念頭におき, 次の形の定義方程式で与えられる k 上定義された種数 g の 超楕円曲線 C を扱います.

$$C: \ Y^2 + h(X)Y = f(X).$$

ここで $h(X), f(X) \in k[X]$, $\deg h(X) \leq g$, $\deg f(X) = 2g+1$, $f(X)$ はモニックで C は非特異代数曲線とします.

解説 $h(X)Y$ の項は, k の標数が 2 の場合も扱うためにあります.

k の標数が 2 でないときは, C の定義方程式として $Y^2 = F(X)$ という形のものが取れます.

逆に k の標数が 2 かつ $h(X) = 0$ とすると, C は非特異になりません.

また, $\deg f(X) = 2g+2$ とすることもできますが, 取り扱いが難しいので本稿では扱いません.

- ∞ : C の 無限遠点.

- $\iota : C \longrightarrow C$: C の超楕円対合 (hyperelliptic involution).
  $\iota(P)$: 点 $P = (x, y) \in C$ の opposite, $\iota(P) := (x, -y - h(x))$ と定義する. $P = \infty$ の場合は, $\iota(P) = \infty$ と定義する.
- $P \in C$ が *special* : $P = \iota(P)$, (つまり, Weierstrass 点).
- $P \in C$ が *ordinary* : $P \neq \iota(P)$.

2.3 超楕円曲線 C 上の多項式と有理関数

$\overline{k}$ 上の C の座標環は, 次で定義されます.

$$\overline{k}[C] = \overline{k}[X, Y]/(Y^2 + h(X)Y - f(X)).$$

任意の $G(X, Y) \in \overline{k}[C]$ は, $G(X, Y)$ を $Y^2 + h(X)Y - f(X)$ で割った余り $a(X) - b(X)Y$ を用いて以下の形の多項式で表せます.

$$G(X, Y) = a(X) - b(X)Y, \quad a(X),\ b(X) \in \overline{k}[X].$$

定義 2 (共役) $G(X, Y) = a(X) - b(X)Y \in \overline{k}[C]$ の**共役** $\overline{G}(X, Y)$ を $a(X) + b(X)(h(X) + Y)$ で定義する.

定義 3 (台) 因子 $D = \sum_{P \in C} m_P P$ に対し, D の**台** $\mathrm{supp}(D)$ を次で定義する. $\mathrm{supp}(D) := \{P \in C | m_P \neq 0\}$.

定義 4 (ノルム) $G(X, Y) = a(X) - b(X)Y \in \overline{k}[C]$ の**ノルム** $\mathrm{N}(G)$ を $G\overline{G}$ で定義する.

定義 5 (次数) $G = G(X, Y) = a(X) - b(X)Y \in \overline{k}[C]$ $(G \neq 0)$ の**次数**を次で定義する.

$$\deg(G) = \max(2\deg_X(a), 2g + 1 + 2\deg_X(b)).$$

解説 ∞ での X の位数は 2, Y の位数は $2g + 1$. つまり, $\deg(G)$ は G の ∞ での位数を表しています.

2.4 超楕円曲線の因子

$P = (x, y) \in C$ に対し,

$$P \text{ が ordinary のとき, } \mathrm{div}(X - x) = P + \iota(P) - 2\infty.$$
$$P \text{ が special のとき, } \mathrm{div}(X - x) = 2P - 2\infty.$$

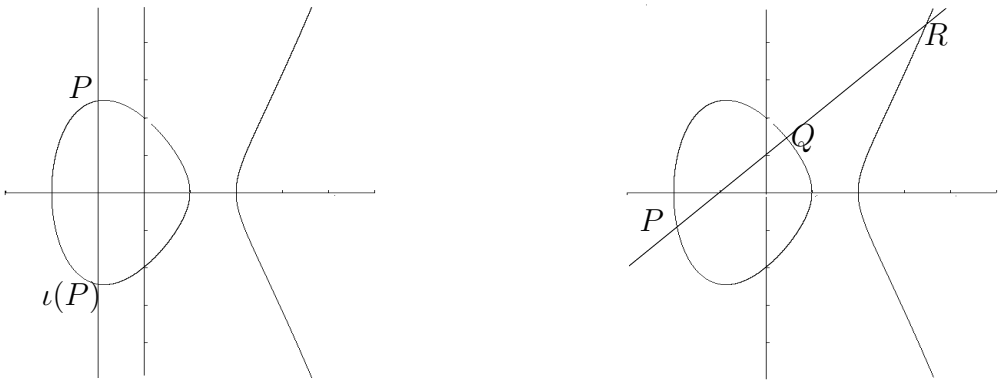
定義 6 (最大公約因子) 二つの因子 $D_1 = \sum_{P \in C} m_P P$ と $D_2 = \sum_{P \in C} n_P P$ に対し, D_1 と D_2 の最大公約因子 $\gcd(D_1, D_2)$ を次で定義する.

$$\gcd(D_1, D_2) := \sum_{P \in C - \{\infty\}} \min(m_P, n_P)P - \left(\sum_{P \in C - \{\infty\}} \min(m_P, n_P) \right) \infty.$$

3　因子の加法

3.1　楕円曲線の因子の加法

楕円曲線 $E : Y^2 = f(X)$ の加法は, $P, Q \in E$ を結ぶ直線 $Y = aX + b$ と E との第 3 の交点 R を取り, R の X 軸に関する対称点 $\iota(R)$ を $P + Q$ とするのでした. このことは次のように考えると容易にわかります.



$P = (x, y) \in E$ に対し, E 上の関数 $(X - x)$ を考えて $\mathrm{div}(X - x)$ を計算すると

$$0 \sim \mathrm{div}(X - x) = (x, y) + (x, -y) - 2\infty = P + \iota(P) - 2\infty = (P - \infty) + (\iota(P) - \infty).$$

よって, $P - \infty \in \mathrm{Div}^0(E)$ の逆元は $\iota(P) - \infty$ となります. これを略記して $-P = \iota(P)$ と書きます.

同様にして, $P, Q, R \in E$ を通る直線 $Y - aX - b = 0$ を考えると,

$$0 \sim \mathrm{div}(Y - aX - b) = P + Q + R - 2\infty.$$

よって, 加法は次のようになります.

$$P + Q = -R = \iota(R)$$

解説　任意の 2 点 $P, Q \in E$ を通る直線が E と 3 点で交わるのでこの操作で E の加法がうまく計算できました.

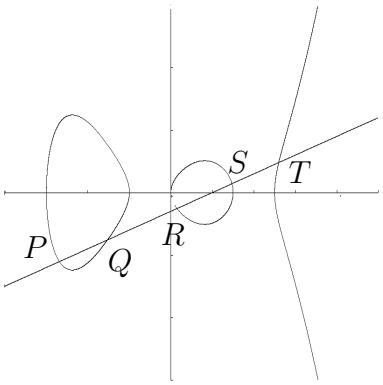
3.2　超楕円曲線の因子の加法

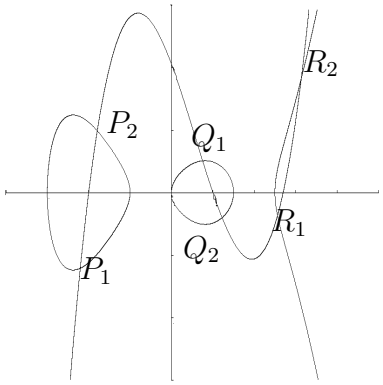
簡単のため $C : Y^2 = f(X)$, $\deg f(X) = 5$ で定義される $g = 2$ の超楕円曲線 C を用いて説明します.

超楕円曲線の場合には, 楕円曲線のように $P, Q \in C$ を通る直線を考えてもうまくいきません. 図からわかるように

$$P + Q = -R - S - T$$

という関係式が得られるだけです.





しかし, 右図のように P_1,P_2,Q_1,$Q_2 \in C$ に対し, この 4 点を通る 3 次式を考えると, R_1, R_2 という 2 点を交点に持ちます.

$$(P_1 + P_2) + (Q_1 + Q_2) = -(R_1 + R_2)$$

このように $g = 2$ の場合, 2 点の和を因子の代表として和を表すことができます.

一般に $n(> 2)$ 点の和からなる因子があると, その全てを通る $(n-1)$ 次の曲線 $Y = g(X)$ が取れ, C と $\max(2(n-1), 5)(= \max(g(X)^2$の次数, $f(X)$ の次数)) 個の点で交わります. 元は n 個の点なので, それ以外の交点は

$$\max(2(n-1), 5) - n = \begin{cases} n-2 & (n > 3), \\ 2 & (n = 3). \end{cases}$$

つまり, n 個の点の和が $(n-1)$ 個以下の点の和になります. これを繰り返すと $n = 3$ のとき 2 になるので, 全ての因子は 2 個以下の点の和で代表されます.

解説 C を超楕円曲線とすると, $P = (x, y) \in C$ が ordinary のときは $\mathrm{div}(X - x) = P + \iota(P) - 2\infty$ より

$$m_P P = (-m_P)\iota(P)$$

となるので, 係数は正として構いません.

また, $P = (x, y) \in C$ が special のときは $\mathrm{div}(X - x) = 2P - 2\infty$ より

$$2P = 0$$

となるので, 係数は 0 か 1 とできます.

これまで見てきたように, 種数 2 だと全ての因子は 2 個以下の点の和で代表されますが, 種数 g の超楕円曲線でも任意の因子は高々 g 個の点の和と線形同値という性質が, Riemann-Roch の定理から示せます.

この性質により, 6 節で定義される被約因子が意味を持ちます.

被約因子を扱う前に, 計算に便利な半被約因子を以下のように定義します.

4　半被約因子 (Semi-reduced divisors)

定義 7 (半被約因子 (semi-reduced divisor)) $D \in \mathrm{Div}^0(C)$ が**半被約因子** (semi-reduced divisor) であるとは, D が次の形をしていることをいう.

$$D = \sum_{P \in C} m_P P - \left(\sum_{P \in C} m_P \right) \infty.$$

ただし,

- $m_P \geq 0$.
- $P \in \mathrm{Supp} D$ が ordinary ならば $\iota(P) \notin \mathrm{Supp} D$.
- $P(\neq \infty) \in \mathrm{Supp} D$ が special ならば $m_P = 1$.

定義 8 (Weight) 半被約因子 $D = \sum_{P \in C} m_P P - \left(\sum_{P \in C} m_P \right) \infty$ に対し, D の *weight* $\mathrm{wt}(D)$ を次で定義する.

$$\mathrm{wt}(D) := \sum_{P \in C} m_P.$$

補題 1 任意の $D \in \mathrm{Div}^0(C)$ に対し, D と線型同値な半被約因子 $D_1 \in \mathrm{Div}^0(C)$ が存在する.

(証明)

$$D = \sum_{P \in C} m_p P.$$

と置きます.

C 上の点の集合 C_0, C_1, C_2 を以下のように定義します.

1. $P = \iota(P) \iff P \in C_0$.
2. $P \in C_1$, $P \neq \iota(P) \iff \iota(P) \in C_2$.
3. $P \in C_1 \implies m_p \geq m_{\iota(P)}$.

すると, D は以下のように表示できます.

$$D = \sum_{P \in C_1} m_P P + \sum_{P \in C_2} m_P P + \sum_{P \in C_0} m_P P - m\infty.$$

ここで次の因子を考えると,

$$D_1 = D - \sum_{P=(x,y) \in C_2} m_P \mathrm{div}(X - x) - \sum_{P=(x,y) \in C_0} \left[\frac{m_P}{2} \right] \mathrm{div}(X - x).$$

$D \sim D_1$ となり, 次の等式より ∞ 以外の係数が負にならないことから半被約因子であることもわかります.

$$D_1 = \sum_{P=(x,y) \in C_1} (m_P - m_{\iota(P)}) P + \sum_{P \in C_0} \left(m_P - 2 \left[\frac{m_P}{2} \right] \right) P - m_1 \infty.$$

□

5 半被約因子の多項式表現 (Mumford 表現)

2 次体のイデアルが高々 2 元生成であることの類似を, 超楕円曲線の因子類群でも考えることができます. それが半被約因子の多項式表現 (Mumford 表現) です.

これにより, 因子の計算を多項式の計算に持ち込むことができます.

Mumford 表現が有効な理由

- 任意の因子と線形同値な半被約因子が存在する.
- 半被約因子は Mumford 表現によって表せる.
- Mumford 表現を用いると半被約因子の加法が高速に計算できる.
- 被約因子全体と $\mathrm{Pic}^0(C)$ は同型.
- 半被約因子と線形同値な被約因子が一意に存在する.

Mumford 表現による計算手順

1. 任意の因子と線形同値な半被約因子の Mumford 表現を求める.
2. Mumford 表現によって加法を計算する. 結果は半被約因子になる.
3. 計算結果を被約因子で表す.

補題 2 *$P=(x,y)\in C$ を ordinary, $R\in\overline{k}[C]_P$ (つまり,R は P で極を持たない) とする.*

任意の $n\geq 0$ に対し, 以下の条件を満たす $c_0, c_1, \cdots, c_n\in\overline{k}$ と $R_n\in\overline{k}[C]_P$ が一意に存在する.

$$R=\sum_{i=0}^{n} c_i(X-x)^i+(X-x)^{n+1}R_n,$$

(証明) P が ordinary ならば $(X-x)$ を P での局所助変数 (local parameter) に取れるので, 補題の結果が得られます. □

補題 3 *$P=(x,y)\in C$ を ordinary, $n\in\mathrm{N}$ とすると, 以下の条件を満たす $b_n\in\overline{k}[X]$ が一意に存在する.*

1. $\deg_X b_n(X)<n$.
2. $b_n(x)=y$.
3. $b_n^2(X)+h(X)b_n(X)\equiv f(X) \pmod{(X-x)^n}$.

(証明) 補題 2 を $R=R(X,Y)=Y$ に適用すると,

$$Y=\sum_{i=0}^{n-1} c_i(X-x)^i+(X-x)^n R_{n-1},\quad R_{n-1}\in\overline{k}[C]_P.$$

さらに,

$$b_n(X) := \sum_{i=0}^{n-1} c_i (X-x)^i$$

と置くと, 以下が容易に確かめられます.

1. $\deg_X b_n(X) = n-1 < n$,
2. $b_n(x) = c_0 = y$,
3. $Y^2 + h(X)Y = f(X)$ より,
   $b_n^2(X) + h(X)b_n(X) \equiv f(X) \pmod{(X-x)^n}$.

$b_n(X)$ の一意性は, n に関する数学的帰納法で示せます. □

定理 1 半被約因子

$$D = \sum_{P_i \in C} m_i P_i - \left(\sum_{P_i \in C} m_i \right) \infty, \quad (P_i = (x_i, y_i) \in C)$$

と, 多項式

$$a(X) = \prod (X - x_i)^{m_i}$$

を与えると, 以下の条件を満たす 多項式 $b(X) \in \overline{k}[C]$ が一意に定まります.

1. $\deg_X b(X) < \deg_X a(X)$.
2. $m_i > 0$ を満たす任意の m_i に対し, $b(x_i) = y_i$.
3. $a(X)$ は $(b^2(X) + h(X)b(X) - f(X))$ を割り切る.

このとき D は次のように表せます.

$$D = \gcd(\mathrm{div}(a(X)),\ \mathrm{div}(b(X) - Y)).$$

(証明) 次のような $\mathrm{supp}(D)$ の部分集合を定義します.

- $C_0 := \{P \in \mathrm{supp}(D) \mid P : \mathrm{special}\}$.
- $C_1 := \{P \in \mathrm{supp}(D) \mid P : \mathrm{ordinary}\}$.
- $C_2 := \{\iota(P) \mid P \in C_1\}$.

半被約因子の定義より, ある $m \in \mathrm{N}$ を用いて D は次のように表せます.

$$D = \sum_{P \in C_0} P_i + \sum_{P \in C_1} m_i P_i - m\infty.$$

任意の $P_i = (x_i, y_i) \in C_1$ に対し, 以下の条件を満たす $b_i(X) \in \overline{k}[X]$ が一意に存在します.

1. $\deg_X b_i(X) < m_i$.
2. $b_i(x_i) = y_i$.
3. $(X - x_i)^{m_i}$ は $(b_i^2(X) + h(X)b_i(X) - f(X))$ を割り切る.

任意の $P_i = (x_i, y_i) \in C_0$ に対し, 定数関数 $b_i(X) = y_i$ は以下の条件を満たす唯一の多項式となります.

1. $\deg_X b_i(X) < 1$.
2. $b_i(x_i) = y_i$.
3. $(X - x_i)$ は $(b_i^2(X) + h(X)b_i(X) - f(X))$ を割り切る.

多項式に関する Chinese Remainder Theorem を用いると, 以下の条件を満たす多項式 $b(X) \in \overline{k}[X]$ が一意に存在します.

$$b(X) \equiv b_i(X) \pmod{(X - x_i)^{m_i}}, \quad \text{for } \forall i, \quad \deg_X b(X) < \sum m_i.$$

よって,

$$\mathrm{div}(a(X)) = \sum_{P \in C_0} 2P_i + \sum_{P \in C_1} m_i P_i + \sum_{P \in C_1} m_i \iota P_i - m'\infty.$$

$$\mathrm{div}(b(X) - Y) = \sum_{P \in C_0} t_i P_i + \sum_{P \in C_1} s_i P_i + \sum_{P \in C,\ P \notin \mathrm{supp}(D)} m_i \iota P_i - m''\infty.$$

$(X - x_i)^{m_i}$ が $N(b - Y) = b^2 + hb - f$ を割り切るので, $s_i \geq m_i$.

もし $P = (x, y) \in C_0$ ならば, $(X - x)$ は $b^2 + hb - f$ を割り切る.

$$\begin{aligned}
&(b^2 + hb - f)' \mid_{X=x} \\
&= 2b(x)b'(x) + h'(x)b(x) + h(x)b'(x) - f'(x) \\
&= b'(x)(2y + h(x)) + (h'(x)y - f'(x)) \quad (b(X) \text{は定数なので,} b'(x) = 0) \\
&= h'(x)y - f'(x) \\
&\neq 0. \quad (C \text{が非特異曲線であることと,} P \text{が special から 0 にならない})
\end{aligned}$$

よって $t_i = 1$ となるので,

$$\gcd(a(X), b(X) - Y) = \sum_{P \in C_0} P_i + \sum_{P \in C_1} m_i P_i - m\infty.$$

□

補題 4 $a = a(X)$, $b = b(X) \in \overline{k}[C]$ が, $\deg_X b < \deg_X a$ かつ $a | b^2 + bh - f$ ならば,(a, b) は半被約因子となる.

(証明) 定理 1 の証明より明らか. □

定義 9 (多項式表現 (Mumford 表現)) C の半被約因子 D は, 定理 1 の対応により $(a(X), b(X))$ で表現される. この表現を 多項式表現 あるいは Mumford 表現という.

つまり, $(a(X), b(X))$ と書いたら以下の因子を表すと定めます.

$$D = \gcd(a(X), b(X) - Y).$$

6　被約因子

定義 10 (被約因子) 半被約因子 $D = \sum_{P \in C} m_P P - \left(\sum_{P \in C} m_P \right) \infty \in \mathrm{Div}^0(C)$ が 被約因子であるとは, $\mathrm{wt}(D) = \left(\sum_{P \in C} m_P \right) \leq g$ となることをいう.

定理 2 任意の因子 $D \in \mathrm{Div}^0(C)$ に対し, D と線型同値な被約因子 $D_1 \in \mathrm{Div}^0(C)$ が一意に存在 する.

(証明) (存在) 半被約因子 D' が $D \sim D'$ かつ $\mathrm{wt}(D') \leq \mathrm{wt}(D)$ と仮定します.

もし $\mathrm{wt}(D') \leq g$ ならば, D' は被約因子.

$\mathrm{wt}(D') > g$ ならば, 重複度を込めて少なくとも $g+1$ 個の点 $P_1, P_2, \cdots, P_{g+1} \in \mathrm{supp}(D)$ が存在します. ただし, $P_i \neq \infty$. $(a(X), b(X))$ を次の因子の多項式表現とします.

$$P_1 + P_2 + \cdots + P_{g+1} - (g+1)\infty.$$

$\deg_X b(X) \leq g$ かつ $\deg_X (b - Y) = 2g + 1$ なので,

$$\mathrm{div}(b(X) - Y) = P_1 + P_2 + \cdots + P_{g+1} + Q_1 + Q_2 + \cdots + Q_g - (2g+1)\infty.$$

$D'' = D' - \mathrm{div}(b(X) - Y)$ と置くと $D'' \sim D$ と $\mathrm{wt}(D'') \leq \mathrm{wt}(D')$ がわかります. この操作を繰り返すことにより, 被約因子が得られます.

(一意性) 二つの被約因子 D_1, D_2 が $D_1 \sim D_2$ かつ $D_1 \neq D_2$ と仮定します. $D_3 \sim D_1 - D_2$ を満たす半被約因子 D_3 を考えます. $D_1 \neq D_2$ なので, $\mathrm{ord}_P D_1 \neq \mathrm{ord}_P D_2$ となる点 P が存在します. よって, $D_3 \neq 0$. 仮定より $D_1 \sim D_2$ なので, $\mathrm{div}(G) = D_3$ を満たす $G \in \overline{k}(C)$ が取れる. ここで, $\mathrm{wt}(D_3) \leq \mathrm{wt}(D_1 - D_2) \leq \mathrm{wt}(D_1) + \mathrm{wt}(D_2) \leq 2g$ となっています. D_3 は半被約因子なので, G は $a(X) - b(X)Y$ という形の多項式で表せます. $\deg Y = 2g + 1$ であることと $\deg(G) = \mathrm{wt}(D_3) \leq 2g$ より, $b(X) = 0$. よって $a(x) = 0$ を満たす $x \in \overline{k}$ に対し, $P = (x, y) \in \mathrm{supp}(D_3)$ かつ $\iota(P) \in \mathrm{supp}(D_3)$ が成り立ちます. しかしこれは D_3 が半被約因子であることに矛盾します. よって, 二つの被約因子 D_1, D_2 が $D_1 \sim D_2$ ならば $D_1 = D_2$ となります. □

7　Mumford 表現に関する加算アルゴリズム

解説　実は, ここで紹介するアルゴリズムよりも高速なアルゴリズムもあります. たとえば奇標数で種数が 2 の場合は, [6] などをご参照ください.

以下のアルゴリズムは, わかりやすさを重視したものです.

入力	2 つの半被約因子 $D_1 = (a_1, b_1),\ D_2 = (a_2, b_2)$.	
出力	半被約因子 $D = (a, b) \sim D_1 + D_2$.	
Step		
1	$d_1 = \gcd(a_1, a_2),\ d_1 = e_1 a_1 + e_2 a_2$.	
2	$d = \gcd(d_1, b_1 + b_2 + h),\ d = c_1 d_1 + c_2(b_1 + b_2 + h)$.	
3	$s_1 = c_1 e_1,\ s_2 = c_1 e_2,\ s_3 = c_2$.	
4	$d = s_1 a_1 + s_2 a_2 + s_3(b_1 + b_2 + h)$.	
5	$a = \dfrac{a_1 a_2}{d^2}$.	
6	$b = \dfrac{s_1 a_1 b_2 + s_2 a_2 b_1 + s_3(b_1 b_2 + f)}{d} \pmod{a}$.	

定理 3 $D_1 = (a_1, b_1),\ D_2 = (a_2, b_2)$ を半被約因子とすると, $D = (a, b)$ も半被約因子となる.

入力	半被約因子 $D = (a, b)$.	
出力	被約因子 $D' = (a', b') \sim D$.	
Step		
1	$a' = \dfrac{f - bh - b^2}{a}$.	
2	$b' = (-h - a) \pmod{a'}$.	
3	もし $\deg_X a' > g$ ならば, $a \leftarrow a'$, $b \leftarrow b'$ step 1 に戻る.	
4	c を a' の先頭係数とする. $a' \leftarrow c^{-1} a'$.	
5	$D = (a', b')$.	

定理 4 任意の半被約因子 $D = (a, b)$ に対し, $D' = (a', b')$ は 被約因子となる.

参考文献

[1] N. Kobilitz, Algebraic Aspects of Cryptography, Springer, 1998.

[2] N. Kobilitz (林彬 訳), 暗号の代数理論 ([1] の翻訳), シュプリンガー・フェアラーク東京, 1999.

[3] J.W.S Cassels, E.V. Flynn, Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2, Cambridge 1996.

[4] D. Mumford, Tata Lecture on Theta II, Birkhauser 1984.

[5] H. Cohen and G. Frey, Handbook of Ellptic and Hyperelliptic Curve Cryptography, Chapman & Hall/CRC, 2006.

[6] 「暗号理論とそれを支える代数曲線理論」第 1 回ワークショップ報告集, 中央大学理工学研究所プロジェクト研究, 2000.

[7] 「暗号理論とそれを支える代数曲線理論」第 2 回ワークショップ報告集, 中央大学理工学研究所プロジェクト研究, 2001.

第 15 回 整数論サマースクール 報告集, pp.223-238

代数曲線暗号とその安全性

松尾 和人*

1 はじめに

本稿では「代数曲線暗号」とその安全性に関する議論を紹介する。代数曲線暗号の研究者には整数論出身者が多く、また多くの整数論研究者がその中に問題を見出し研究に取り組んでいる。整数論を学んだ方が新たに代数曲線暗号の研究を始めるときや整数論を専門とする研究者の方々が関連研究を新たに始めるときに、その研究の暗号学的な背景や意義を知る手掛かりとなることを意図して書いた。この主旨の下、研究の流れに沿って一本の筋を通した記述を行った。その結果いくつかの重要な結果について触れることができなかったことに御留意頂きたい。

2 公開鍵暗号と離散対数問題

（代数曲線暗号が含まれる）公開鍵暗号は 1976 年に Diffie と Hellman によって提案された [12]。この Diffie と Hellman のプロトコルは事前に秘密情報のやりとりをせずに共通鍵暗号に利用する共通鍵を二者間で共有しようというものである。表 1 に Diffie-Hellman プロトコルを示す。

	システム設定	
	p: 素数, $b \in \mathbb{F}_p^*$ (s.t. $\langle b \rangle = \mathbb{F}_p^*$)	
	太郎	花子
	鍵ペア生成	
秘密鍵設定	$K_a \in \mathbb{Z}/(p-1)\mathbb{Z}$	$K_b \in \mathbb{Z}/(p-1)\mathbb{Z}$
公開鍵計算	$K_a' = b^{K_a}$	$K_b' = b^{K_b}$
鍵公開	公開鍵 K_a' を公開	K_b' を公開
	共通鍵計算	
	$K = K_b'^{K_a}$	$K = K_a'^{K_b}$
	同一の鍵 K を共有できた	

表 1: Diffie-Hellman 鍵共有プロトコル

*情報セキュリティ大学院大学

Diffie と Hellman の提案の後、Rivest, Shamir, Adleman [35] によって RSA 暗号・署名が ElGamal [13] によって ElGamal 暗号・署名が提案された。この中で RSA 暗号・署名は素因数分解の困難性に基づいた暗号プロトコロルであり、Diffie-Hellman, ElGamal は離散対数問題の困難性に基づいたアルゴリズムである。

「共通鍵計算」の速度が Diffie-Hellman プロトコルの暗号化速度であるが、これは明らかに p に依存する。この計算は $K_a \in \mathbb{Z}/(p-1)\mathbb{Z}$ を整数と看做し $K_a = (x_{k-1}x_{k-2}\dots x_1x_0)_2$ と 2 進展開すれば $K = \prod_{0\le i<k} K_b'^{2^{x_i}}$ と計算され、$k = O(\log p)$ より $O(\log p)$ 回の $\mathbb{F}_p$-乗算によって実現される。また、$\mathbb{F}_p$-乗算は（暗号アルゴリズムに利用される）標準的な方法では $O((\log p)^2)$ のビット演算量を必要とする。従って p が大きくなるに連れて暗号化速度が遅くなりプロトコルの実用性は低くなる。一方、p を小さくとると $K_a' = b^{K_a}$ に対する全数探索により K_a を知ることが可能となり、$K = K_b'^{K_a}$ から誰でも秘密 K を知ることが可能な（「暗号」としての機能を持たない）プロトコルとなる。従って、p は K が求められない程度に大きくとる必要がある。この K_a を求める問題を一般に離散対数問題という。

定義 2.1 (離散対数問題) 与えられた $b \in \mathbb{F}_p^*$, $a \in \langle b\rangle$ に対し $a = b^x$ を満足する $x \in \mathbb{Z}/(p-1)\mathbb{Z}$ を求める問題を $\mathbb{F}_p$ 上の離散対数問題という。また、この x を $\mathrm{Ind}_b a$ と書く。

離散対数問題は全数探索により $O(p)$ の $\mathbb{F}_p$-演算で解くことが可能である。現在のところ 2^{80} 程度の手間の掛かる計算は不可能であると考えられているので、もし離散対数問題の解法として全数探索が最良であるならば、80 ビット程度の p を利用すれば安全な暗号が得られる。しかし、全数探索より効率的な離散対数問題の解法アルゴリズムが存在するならば、安全性を確保するためにはより大きな p を選択する必要があり、それを利用した Diffie-Hellman 等の暗号プロトコルの効率が悪くなる。また、もし $\log p$ の低次多項式時間のアルゴリズムが存在した場合には、もはや Diffie-Hellman プロトコル等を暗号アルゴリズムと呼ぶことは出来ない。

注意 2.1 離散対数問題が解ければ *Diffie-Hellman* プロトコルを破れるが、離散対数問題を解かずに *Diffie-Hellman* プロトコルを破る方法がないことは示されていない。

3 離散対数問題の解法

前節を受け本節では定義 2.1 で与えられた離散対数問題の解法について紹介する。離散対数問題の解法として全数探索より効率的な方法が 2 種類知られている。その一つは square-root 法と呼ばれる方法であり、もう一つは（一般に）より効率的な指数計算法である。ここでは、まず square-root 法を紹介し、次に指数計算法を紹介する。

3.1 Square-root 法

良く知られた square-root 法に、Shanks [36] の baby-step giant-step アルゴリズムと Pollard [34] の rho 法がある。これらのアルゴリズムは同一の漸近計算量を持つがその性質は大きく異なる。現実的な離散対数問題に対してはメモリー効率の優位性から rho 法を用い

ることが通常である。そこでここではrho法を紹介する。また、中国の剰余定理を利用したこれらのアルゴリズムの効率向上策[33]が知られているので、これについても紹介する。

3.1.1 Pollardのrho法

Rho法は「誕生日のパラドクス」を利用したアルゴリズムである。誕生日のパラドクスについては例えば[9, Section 5.4.1]を参照されたい。Algorithm 1にrho法の原型を示す。

Algorithm 1 Rho法の原型

Input: p: prime, $b \in \mathbb{F}_p^*$, $a \in \langle b \rangle$
Output: $x \in [0, p-2]$ s.t. $a = b^x$

1: $i := 0$
2: **repeat**
3: $\quad i := i + 1$
4: $\quad$ Choose $\alpha_i, \beta_i \in [0, p-2]$ randomly
5: $\quad c_i := a^{\alpha_i} b^{\beta_i}$
6: **until** $^{\exists} j$ s.t. $1 \leq j < i, c_j = c_i$
7: $x := (\beta_j - \beta_i)(\alpha_i - \alpha_j)^{-1} \bmod p-1$ /*$\alpha_i x + \beta_i \equiv \alpha_j x + \beta_j \bmod p-1$*/
8: Output x and terminate

Algorithm 1のループ回数の期待値は誕生日のパラドクスより$O(\sqrt{p})$となる。従ってこれの計算量は$O(\sqrt{p})$ $\mathbb{F}_p$-演算であり全数探索と比較し大幅に効率的である。実際、これにより例えばpが160ビット程度のとき離散対数問題の解読は2^{80}倍程度高速化することが見込まれる。

例 3.1 *Rho*法の原型による離散対数計算の具体例として与えられた$p = 47$, $a = 40$, $b = 11$に対し$a \equiv b^x \bmod p$を満足するxを求める。

下表のように$i = 1, 2, \ldots$に対しα_i $\beta_i \in [0, 45]$をランダムに選択し$c_i \equiv a^{\alpha_i} b^{\beta_i} \bmod p$を計算していく。

i	1	2	3	4	5	6	7	8	9	10
α_i	35	36	17	9	3	17	16	37	38	39
β_i	3	41	15	0	28	14	7	17	25	8
c_i	27	43	24	29	<u>30</u>	15	40	6	13	<u>30</u>

表から*10*ステップの計算の後$i = 10$において計算した結果が*5*ステップ目の計算結果と一致することが判る。従って

$$a^{\alpha_5} b^{\beta_5} \equiv a^{\alpha_{10}} b^{\beta_{10}} \bmod p$$

であり、

$$x \equiv \frac{\beta_{10} - \beta_5}{\alpha_5 - \alpha_{10}} \equiv 21 \bmod p - 1$$

を得る。

注意 3.1 ここで示したアルゴリズムは、テーブルサイズの多項式時間で探索可能なデータベースに全ての (c_i, α_i, β_i) を記録する必要があり、空間計算量 $O(\sqrt{p})$ を必要とする。そこで通常は「ランダムウォーク関数」を利用して空間計算量を $O(1)$ とした変形が利用される。このランダムウォーク関数の選択などについても多くの研究がなされている。これらについては *[39]* 等を参照されたい。

3.1.2 中国の剰余定理の利用

Square-root 法は中国の剰余定理によって効率化されることが知られている[1][33]。

いま $d \mid p-1$ に対し $a_d = a^{(p-1)/d}$, $b_d = a^{(p-1)/d}$ とすると、

$$a_d \equiv b_d^{x_d} \bmod p$$

を満足する x_d に対し

$$x \equiv x_d \bmod \frac{p-1}{d}$$

が成立する。適切に選択した十分な数の d に対し square-root 法によって x_d を求めれば、中国人の剰余定理（と、場合によっては Newton 反復）によって x を求めることが可能である。この方法の詳細については、例えば [37, Section 11.2], [25, Section 3.6.4] を参照されたい。

この方法により離散対数問題に対する square-root 法の計算量は $O(\sqrt{l})$ となる。ここで l は $p-1$ を割る最大素因数を表す。

3.2 指数計算法

離散対数問題に対して一般に square-root 法より効率的な「指数計算法」と呼ばれるアルゴリズムが知られている [1]。Algorithm 2 にこの指数計算法を示す。

[1] この手法を全数探索とともに用いることも可能であるが、通常は square-root 法とともに用いる。

Algorithm 2 指数計算法

Input: p: 素数, $a, b \in \mathbb{F}_p^*$ s.t. $\langle b \rangle = \mathbb{F}_p^*$, $s \in \mathbb{N}$ s.t. $s < p$
Output: $x \in \mathbb{Z}/(p-1)\mathbb{Z}$ s.t. $a = b^x$

1: $B := \{l_j \in \mathbb{Z} \mid l_j : \text{prime number} \leq s\}, n := \#B$
`/*`因子基底 `(factor base)*/`
2: $i := 1$
3: **repeat** `/*STAGE 1:` 対数表の作成`*/`
4: Choose $r_i \in \mathbb{Z}/(p-1)\mathbb{Z}$ randomly
5: **if** $(b^{r_i} \bmod p) = \prod_{j=1}^{n} l_j^{e_j} \in \mathbb{Z}$ **then** `/*via trial division*/`
6: $e_{ij} := e_j$ for $j = 1 \ldots n$
7: $i = i + 1$
8: **until** $\mathrm{rank}(e_{ij}) = n$ (over $\mathbb{Z}/(p-1)\mathbb{Z}$)
9: Compute $\mathrm{Ind}_b l_i$ for $i = 1 \ldots n$
10: **repeat** `/*STAGE 2:` $\mathrm{Ind}_b a$ の求解`*/`
11: Choose $r \in \mathbb{Z}/(p-1)\mathbb{Z}$ randomly
12: **until** $(ab^r \bmod p) = \prod_{j=1}^{n} l_j^{f_j} \in \mathbb{Z}$ `/*via trial division*/`
13: Output $\sum_{j=1}^{n} f_j \mathrm{Ind}_b l_j - r \bmod p - 1$ as x and terminate

指数計算法は、まず小さな素数からなる因子基底と呼ばれる集合を決め、次にこの因子基底の要素に対する対数表を作成する。そして、この対数表を用いて与えられた離散対数問題を解くものである。以下にこのアルゴリズムの実例を示す。

例 3.2 例 *3.1* と同様に、与えられた $p = 47$, $a = 40$, $b = 11$ に対し $a \equiv b^x \bmod p$ を満足する x を求める。まず、因子基底として $B = \{2, 3, 5, 7, 11, 13\}$ を選ぶ。そして、*Algorithm 2* のステップ *4* に従い $r_1 \in \mathbb{Z}/(p-1)\mathbb{Z}$ をランダムに選択する。例えば $r_1 = 9$ を選択すると $b^{r_1} \equiv 38 = 2 \cdot 19 \bmod p$ が得られる。しかし、この場合はステップ *5* に示された因子基底の要素による関係が（簡単には）得られないのでこれを破棄し、新たに r_1 を選択し直す。幾度かの試行の後に $r_1 = 42$ を選択すると $b^{r_1} \equiv 2 = \bmod p$ が得られ、因子基底の要素による関係式が得られたこととなる。同様の試行を n 個の関係式が得られる間で繰り返すと、例えば

$$\begin{pmatrix} 11^{42} \\ 11^{3} \\ 11^{29} \\ 11^{11} \\ 11^{31} \\ 11^{1} \end{pmatrix} = \begin{pmatrix} 2 \\ 15 \\ 10 \\ 39 \\ 35 \\ 11 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \cdot 5 \\ 2 \cdot 5 \\ 3 \cdot 13 \\ 5 \cdot 7 \\ 11 \end{pmatrix} = \begin{pmatrix} 11^{\mathrm{Ind}_{11} 2} \\ 11^{\mathrm{Ind}_{11} 3} \cdot 11^{\mathrm{Ind}_{11} 5} \\ 11^{\mathrm{Ind}_{11} 2} \cdot 11^{\mathrm{Ind}_{11} 5} \\ 11^{\mathrm{Ind}_{11} 3} \cdot 11^{\mathrm{Ind}_{11} 13} \\ 11^{\mathrm{Ind}_{11} 5} \cdot 11^{\mathrm{Ind}_{11} 7} \\ 11^{\mathrm{Ind}_{11} 11} \end{pmatrix}$$

が得られる。この式は指数に関し線形方程式系

$$\begin{pmatrix} 42 \\ 3 \\ 29 \\ 11 \\ 31 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \mathrm{Ind}_{11}2 \\ \mathrm{Ind}_{11}3 \\ \mathrm{Ind}_{11}5 \\ \mathrm{Ind}_{11}7 \\ \mathrm{Ind}_{11}11 \\ \mathrm{Ind}_{11}13 \end{pmatrix}$$

を満足するので、これを解き小さな素数に対する「対数表」

$$\begin{pmatrix} \mathrm{Ind}_{11}2 & \mathrm{Ind}_{11}3 & \mathrm{Ind}_{11}5 & \mathrm{Ind}_{11}7 & \mathrm{Ind}_{11}11 & \mathrm{Ind}_{11}13 \end{pmatrix} \equiv \begin{pmatrix} 42 & 16 & 33 & 44 & 1 & 41 \end{pmatrix} \bmod p-1$$

が得られる。次に *Algorithm 2* のステップ *10* 以降を実行し、対数表を用いて与えられた問題を解く。まず、*Algorithm 2* のステップ *4* に従い $r \in \mathbb{Z}/(p-1)\mathbb{Z}$ をランダムに選択する。そして、選択した r に対し ab^r を計算し、対数表の作成と同様にこれが因子基底の要素に分解されるまで繰り返す。例えば、$r = 33$ を選択すると $ab^5 \equiv 40 \cdot 11^{33} \equiv 12 \equiv 2^2 \cdot 3 \bmod p$ が得られ、これと対数表から

$$\mathrm{Ind}_{11}40 \equiv 2\mathrm{Ind}_{11}2 + \mathrm{Ind}_{11}3 - 33 \equiv 21 \bmod p-1$$

を得る。

注意 3.2 *Algorithm 2* は標準的なものだが、実際には対数表を作成しない変形を用いることも多い。この方法ついては例えば *[37, Chapter 16]* を参照されたい。

3.3 指数計算法の計算量

Algorithm 2 の計算量は明らかに s の選択に依存する。すなわち、s を小さくとると「関係式」を得られる確率が低くなり、逆に s を大きくとると、より多くの「関係式」集める必要が生じ、さらに行列の次数が高くなるので線形代数計算のコストもより大きくなる。s の最良の設定は素数分布等の知見から得られ、Algorithm 2 の漸近計算量は $O(L_p(1/2, 2+o(1)))$ となる。ここで

$$L_n(\alpha, \beta) := \exp\left(\beta(\log n)^{\alpha}(\log\log n)^{1-\alpha}\right)$$

である。この記法を用いると rho 法の計算量は $O(L_p(1, 1/2))$ となり、指数計算法は rho 法と比較し著しく高速であることが判る。さらに指数計算法に対し多くの改良が行われており、上式において $\alpha = 1/3$ のアルゴリズムが知られている。このような $0 < \alpha < 1$ のアルゴリズムは準指数時間アルゴリズムと呼ばれる[2]。Algorithm 2 の計算量評価については [37, Chapter 16] を、指数計算法とその改良についてはこれの他に [10, Section 6.4], [25, Section 3.6.5] とこれらに挙げられている文献を参照されたい。

以上のように離散対数問題に対しては全数探索や square-root 法と比較し著しく効率的なアルゴリズムが知られているため、解読に 2^{80} 程度の手間を必要とする暗号を離散対数を利用して構成する場合には 1024 ビット程度の p を選択する必要があると考えられている。（より大きな p が必要であるとの推測もある。）

[2] $\alpha = 1$ が指数時間アルゴリズム、$\alpha = 0$ が多項式時間アルゴリズムである。

4 離散対数問題の一般化と楕円曲線暗号

以上で見たように、定義 2.1 で与えた離散対数問題には準指数時間計算量アルゴリズムが知られており、近年のコンピュータ能力の指数関数的な進歩が、これを利用した暗号にとって両刃の剣となった。すなわち、計算速度の急激な向上によって暗号解読時間もまた急激に短くなり、安全性確保のために問題のサイズを準指数関数的に増加させる必要が生じ、結果として暗号化速度の面でコンピュータ性能の進歩を完全には享受できないこととなった。そこで、このようなコンピュータ性能の進歩による性能の劣化が生じない暗号が要求されることとなった。

定義 2.1 で与えた離散対数問題は以下に示すように一般の有限可換群 G 上の問題として一般化可能である。

定義 4.1 (離散対数問題) 与えられた有限可換群 G, $b \in G$, $a \in \langle b \rangle$ に対し $a = [x]b$ を満足する $x \in \mathbb{Z}/\#G\mathbb{Z}$ を求める問題を G 上の離散対数問題という。また、この x を $\mathrm{Ind}_b a$ と書く。

3.1 節で示した square-root 法は一般の G 上の離散対数問題に適用可能であるが、一方 Algorithm 2 に示した指数計算法は一般の G 上の離散対数問題に適用可能なアルゴリズムではない。従って、square-root 法以上に効率的なアルゴリズムが存在しない問題を設定できれば、それを用いた暗号は上述の課題を解決できることとなる。このような G として有限体上の楕円曲線の有理点群が知られている。これを用いた楕円曲線暗号は、Miller [27] と Koblitz [20] によって独立に提案された。特に [27] は指数計算法が楕円曲線上の離散対数問題 (ECDLP) に対して有効に働かないことを主張している。実際にその後も ECDLP に対する指数計算法的なアルゴリズムの研究が盛んに行われているが、現在まで一般的且つ効率的なアルゴリズムは得られていない。一方 [20] は中国の剰余定理を利用した square-root 法に対する耐性が高い曲線の構成法を主旨とした論文となっている。即ち、楕円曲線暗号では固定された定義体の上においても曲線を選択により $\#G$ が変化するので、適切な選択により（中国の剰余定理が無意味となる）素数若しくは素数に近い $\#G$ に設定可能である。与えられた曲線の群位数が計算が可能であればそのような位数を持つ曲線を選択可能であり、長い間、曲線の位数計算アルゴリズムは楕円曲線暗号研究の主要課題の一つであった。多くの研究の結果として現状では暗号に利用するサイズの位数を実用的な時間で計算することが可能となっている。

位数計算を含め楕円曲線暗号全般については近年多数の良書が出版されているのでそれらを参照されたい [24, 22, 23, 5, 41, 6, 8]。また、特殊な楕円曲線上の離散対数問題に対する効率的なアルゴリズムがいくつか知られているので、これらについてもここに挙げた文献を参照されたい。

現在では多くの製品に楕円曲線暗号が利用されている。これは同一の安全性を仮定した場合、有限体上の離散対数問題に基づく暗号や事実上の標準暗号である RSA 暗号と比較してより高速な暗号を実現可能となったためである[3]。また、これには楕円曲線の持つ豊富な性質を利用した高速化手法に関する研究の寄与も大きい。現在に至るまで高速化に関する研究は盛んに行われ続けている。高速化の実際に関しては例えば [42] 等を参照されたい。

[3]講演ではこれについても触れたが、本稿ではこれ以上触れない。講演資料 [43] を参照されたい。

5 超楕円曲線暗号

楕円曲線暗号は強力だが暗号アルゴリズムは突然その価値を失うことが少なくない。そこで、新たな暗号アルゴリズムの探求が常に行われている。この観点から Koblitz [21] によって楕円曲線暗号の自然な一般化として超楕円曲線暗号が提案された。

以下では種数 g の超楕円曲線 C が

$$\begin{aligned} C: \quad & Y^2 = F(X), \\ & F(X) = X^{2g+1} + f_{2g}X^{2g} + \cdots + f_0 \in \mathbb{F}_p[X] \end{aligned} \tag{1}$$

と定義されているとする。また、C の Jacobian を $\mathcal{J}_C$ と書く。超楕円曲線暗号は定義 4.1 において $G = \mathcal{J}_C(\mathbb{F}_p)$ としたものである。効率的な暗号を構成するためには G 上の効率的な加算アルゴリズムが必要であるが、Koblitz はこれに Cantor [7] が陽に示したアルゴリズムを用いた。この加算アルゴリズムを暗号界では「Cantor アルゴリズム」と呼ぶ。Cantor アルゴリズムは $\mathcal{J}_C(\mathbb{F}_p)$ の要素表現に [29] に記述のある多項式の組による表現を用いている。この表現を最近の暗号界では「Mumford 表現」と呼ぶ。

定義 5.1 (Mumford 表現) 式 (1) で与えられた C に対し、*1.* $\mathrm{lc}(U) = 1$, *2.* $\deg V < \deg U$, *3.* $U \mid F - V^2$ を満足する多項式の組 $(U, V) \in (\overline{\mathbb{F}}_p[X])^2$ を $\mathcal{J}_C(\overline{\mathbb{F}}_p)$ の元の *Mumford* 表現と呼ぶ。

与えられた $\mathcal{D} = \sum_{1 \le i \le n} P_i - nP_\infty \in \mathcal{J}_C(\overline{\mathbb{F}}_p)$ $(P_i \in C(\overline{\mathbb{F}}_p))$ の Mumford 表現 (U, V) は

$$U = \prod_{1 \le i \le n} (X - X(P_i)),\ Y(P_i) = V(X(P_i))$$

と上記 3 条件から得られる。$\mathcal{J}_C(\overline{\mathbb{F}}_p)$ の任意の元は $\deg U \le g$ を満足する Mumford 表現で一意表現されることが知られている。さらに、

$$\mathcal{J}_C(\mathbb{F}_p) = \{(U, V) \in (\mathbb{F}_p[X])^2 \mid \mathrm{lc}(U) = 1, \deg V < \deg U \le g, U \mid F - V^2\}$$

と看做すことが可能である。この性質によって（手間のかかる）拡大体上の演算が不要となるため Mumford 表現は暗号実装に向いた表現であるといえる。Cantor アルゴリズムと Mumford 表現の詳細については本報告集の志村氏の報告や [26] を参照されたい。また、偶数次の超楕円曲線に対する Mumford 表現と Cantor アルゴリズムが [32] に示されていることを付記する[4]。

$\#\mathcal{J}_C(\mathbb{F}_p) \approx p^g$ より、(square-root 法より効率的な解読アルゴリズムが存在しないとの仮定の下で) 同一の安全性を持つ楕円曲線暗号と比較し、より小さい定義体上で超楕円曲線暗号を構成可能であり、プラットフォームによってはより効率的な実装が可能となる。このような利点を有するので、例えば [44] 等 $\mathcal{J}_C$ 上の加算アルゴリズムの研究が現在に至るまで盛んに行われている。実際、Cantor アルゴリズムを用いた超楕円曲線暗号は同一の安全性を有する楕円曲線暗号と比較し数倍低速であることが知られていたが、多くの研究の

[4] これまでの処偶数次の超楕円曲線を（攻撃以外に）暗号利用する利点は見出されていない

結果、楕円曲線暗号とほぼ同一の速度を達成可能なアルゴリズムが知られるようになった。この種のアルゴリズムは「Harley アルゴリズム」と呼ばれる。Harley アルゴリズムについては [8, Chapter 14] とそこに挙げられている文献等を参照されたい。また、[3], [8, Section 14.7] 等、より一般の曲線の Jacobian 上の加算アルゴリズムの研究も盛んに行われていることを付記する。

6 超楕円曲線上の離散対数問題に対する指数計算法

超楕円曲線暗号が提案されて暫くの後、[2] が超楕円曲線上の離散対数問題に対する準指数時間アルゴリズムを示した。このアルゴリズムは、s より小さい素数に代えて次数が s より小さい多項式を因子基底とし、Mumford 表現に現れる多項式 U が因子基底の要素に分解される場合に対して関係式を得るものである。このアルゴリズムの計算量は $\log p < (2g+1)^{0.98}$, $g \to \infty$ に対し $O(L_{p^{2g+1}}(1/2, c < 2.181))$ である。またこのアルゴリズムの改良が研究され、計算量が $p^g \to \infty$ に対し $O(L_{p^g}(1/2, \cdot)$ のアルゴリズムが得られている [14]。これらのアルゴリズムの出現により種数が 2 桁以上の曲線を暗号に利用することは難しくなった。しかし、これらは超楕円曲線暗号にとっての脅威とは考えられてこなかった。何故ならば、(暗号応用に対して適切な設定である) g を固定した場合には、これらはいずれも指数時間計算量のアルゴリズムであり、実際に効果が現れる種数が暗号に利用される曲線の種数より大きいと考えられたからである。しかし、Gaudry [16] によって上記アルゴリズム低種数曲線に対する変形が示された。この Gaudry アルゴリズムは、指数時間計算量アルゴリズムであるものの、ある範囲の種数の超楕円曲線上の離散対数問題に対する計算量が square-root 法より小さいアルゴリズムであり、超楕円曲線の暗号応用に対し現実的な脅威となりうるものである。

Algorithm 3 に Gaudry アルゴリズムを示す。Algorithm 3 に示したアルゴリズムは、Algorithm 2 との対応を見やすくするために、[16] に示されたアルゴリズムに修正を施したものであることに注意されたい。Algorithm 3 を Algorithm 2 と比較すると Gaudry アルゴリズムが因子基底の選択を除き有限体上の離散対数問題に対する指数計算法とほぼ同一のアルゴリズムであることが理解される。以下に Algorithm 3 による離散対数問題解法の具体例を示す。

例 6.1 与えられた $p = 47$, $a = 40$, $b = 11$ に対し $a \equiv b^x \bmod p$ を満足する x を求める。

$p = 7$ とし、$\mathbb{F}_p$ 上の種数 *6* の超楕円曲線

$$(2)\quad C/\mathbb{F}_p : Y^2 = X^{13} + 5X^{12} + 4X^{11} + 6X^9 + 2X^8 + 6X^7 + 5X^4 + 5X^3 + X^2 + 2X + 6$$

を選ぶ。ここで $N := \#\mathcal{J}_C(\mathbb{F}_p) = 208697$ であり、これは素数である。以下では

$$\begin{aligned} \mathcal{D}_a &= (X^6 + 2X^5 + 4X^4 + X^3 + 5X^2 + 3, 4X^5 + 5X^3 + 2X^2 + 5X + 4), \\ \mathcal{D}_b &= (X^5 + 6X^3 + 3X^2 + 1, 3X^4 + X^3 + 4X^2 + X + 3) \in \mathcal{J}_C(\mathbb{F}_p) \end{aligned}$$

に対し、$\mathcal{D}_a = [\mathrm{Ind}_{\mathcal{D}_b}\mathcal{D}_a]\mathcal{D}_b$ を満足する $\mathrm{Ind}_{\mathcal{D}_b}\mathcal{D}_a$ を求める。

Algorithm 3 Gaudry アルゴリズム

Input: $C/\mathbb{F}_p$: 超楕円曲線, $\mathcal{D}_a, \mathcal{D}_b \in \mathcal{J}_C(\mathbb{F}_p)$ s.t. $\mathcal{D}_a \in \langle \mathcal{D}_b \rangle$, $N := \#Jc(\mathbb{F}_p)$
Output: $x \in \mathbb{Z}/N\mathbb{Z}$ s.t. $\mathcal{D}_a = [x]\mathcal{D}_b$

1: $B := \{P_j \in C(\mathbb{F}_p) \setminus P_\infty \mid X(P_j) \neq X(P_i) \text{ for } i \neq j\}, n := \#B$ /*因子基底*/
2: $i := 1$
3: **repeat** /*STAGE 1: 対数表の作成*/
4: Choose $r_i \in \mathbb{Z}/N\mathbb{Z}$ randomly
5: **if** $[r_i]\mathcal{D}_b = \sum_{j=1}^{n} e_j P_j^{e_j} - mP_\infty$ **then** /*via factorization of U*/
6: $e_{ij} := e_j$ for $j = 1 \ldots n$
7: $i = i + 1$
8: **until** $\mathrm{rank}(e_{ij}) = n$ (over $\mathbb{Z}/N\mathbb{Z}$)
9: Compute $\mathrm{Ind}_{\mathcal{D}_b} P_i$ for $i = 1 \ldots n$
10: **repeat** /*STAGE 2: $\mathrm{Ind}_{\mathcal{D}_b}\mathcal{D}_a$ の求解*/
11: Choose $r \in \mathbb{Z}/N\mathbb{Z}$ randomly
12: **until** $\mathcal{D}_a + [r]\mathcal{D}_b = \prod_{j=1}^{n} [s_j]P_j - mP_\infty \in \mathbb{Z}$ /*via factorization of U*/
13: Output $\sum_{j=1}^{n} s_j \mathrm{Ind}_{\mathcal{D}_b} P_j - r \bmod N$ as x and terminate

まず、$C(\mathbb{F}_p) = \{P_\infty, (1,1), (1,6), (2,1), (2,6), (4,1), (4,6)(5,3), (5,4), (6,3), (6,4)\}$ から因子基底

$$B = \{(1,1), (2,1), (4,1), (5,3), (6,3)\}$$

を選択する。そして、*Algorithm 3* のステップ *4* に従い $r_1 \in \mathbb{Z}/N\mathbb{Z}$ をランダムに選択する。例えば $r_1 = 9343$ を選択すると、ステップ *5* に現れる $[r_1]\mathcal{D}_b$ は

$$[9343]\mathcal{D}_b = (X^5 + 6X^4 + 6X^3 + 5X^2 + 6X + 4, X^4 + X^3 + X^2 + 4X + 6)$$

となる。これの第一多項式は $\mathbb{F}_p$ 上で $X^5+6X^4+6X^3+5X^2+6X+4 = (X-1)^2(X-4)^2(X-5)$ と *1* 次式に素因子分解される。従ってこの r_1 からは関係式が得られる。実際、$X^4 + X^3 + X^2 + 4X + 6 \mid_{X=1} = 6$, $X^4 + X^3 + X^2 + 4X + 6 \mid_{X=4} = 1$, $X^4 + X^3 + X^2 + 4X + 6 \mid_{X=5} = 3$ より、

$$[9343]\mathcal{D}_b = -[2](1,1) + [2](4,1) + (5,3)$$

が得られる。これを繰り返すことで、線形方程式系

$$\begin{pmatrix} [9343]\mathcal{D}_b \\ [120243]\mathcal{D}_b \\ [121571]\mathcal{D}_b \\ [120688]\mathcal{D}_b \\ [151649]\mathcal{D}_b \end{pmatrix} = \begin{pmatrix} -2 & 0 & 2 & 1 & 0 \\ 0 & -2 & 1 & 1 & -2 \\ -1 & 0 & 2 & -1 & -1 \\ 2 & 1 & 0 & 2 & 0 \\ 1 & 0 & 1 & -2 & 1 \end{pmatrix} \begin{pmatrix} (1,1) \\ (2,1) \\ (4,1) \\ (5,3) \\ (6,3) \end{pmatrix}$$

が得られる。この方程式系を解き対数表

$$\begin{pmatrix} \mathrm{Ind}_{\mathcal{D}_b}(1,1) & \mathrm{Ind}_{\mathcal{D}_b}(2,1) & \mathrm{Ind}_{\mathcal{D}_b}(4,1) & \mathrm{Ind}_{\mathcal{D}_b}(5,3) & \mathrm{Ind}_{\mathcal{D}_b}(6,3) \end{pmatrix}$$
$$\equiv \begin{pmatrix} 85159 & 114347 & 182999 & 22360 & 136908 \end{pmatrix} \bmod N$$

を得る。

従って、

$$\mathcal{D}_a + [105454]\mathcal{D}_b = (1,1) + [2](2,1) + (4,1) - (6,3)$$

であり、

$$\mathrm{Ind}_{\mathcal{D}_b}\mathcal{D}_a \equiv \mathrm{Ind}_{\mathcal{D}_b}(1,1) + 2\mathrm{Ind}_{\mathcal{D}_b}(2,1) + \mathrm{Ind}_{\mathcal{D}_b}(4,1) - \mathrm{Ind}_{\mathcal{D}_b}(6,3) - 105454 \equiv 45793 \bmod N$$

を得る。

以下では Algorithm 3 の計算量を評価する。評価を必要とするのは $\#B + 1 = O(p)$ 個の関係式を得るために必要な計算量と線形方程式系を解くために必要な計算量である。

Algorithm 3 のステップ 5, 12 は因子類の整数倍算と g 次多項式の素因子分解を必要する。因子類の加算は $O(g^2(\log p)^2)$ ビット演算を必要とするので整数倍算に必要な計算量は $O(g^2(\log p)^3)$ である。また、g 次多項式の素因子分解に必要な計算量は $O(g^3(\log p)^3)$ ビット演算である[1]。従って、これらのステップの実行には $O(g^3(\log p)^3)$ ビット演算を必要とする[1]。$\mathbb{F}_p$ 上のモニック g 次多項式の数は p^g であり、1 次式の積に分解するモニック g 次多項式の数は $p^g/g!$ であるので、$O(p)$ 個の関係式を得るために必要な計算量は $O(g!g^3p(\log p)^3)$ となる。一方、対数表の作成過程で得られる行列は各行に高々 g 個の要素を持つ疎行列である。疎行列に対しては効率的なアルゴリズムが知られており [37, Section 19.4]、これを用いることでステップ 9 に必要な計算量は $O(gp^2(\log N)^2) = O(g^3p^2(\log p)^2)$ となる。以上より、Algorithm 3 の計算量は

$$O\left(g!g^3p(\log p)^3 + g^3p^2(\log p)^2\right) \tag{3}$$

ビット演算であり、種数 g が十分に小さい範囲で $g \geq 5$ に対し rho 法より漸近的に計算量が小さい。これはあくまでも「漸近的」な振舞について述べたものであり、暗号に利用される範囲のサイズの p に対して実際に効果があるとはいえないことに注意されたい。

7 Gaudry アルゴリズムの改良

[16] は Algorithm 3 の計算量削減手法についても言及している。この手法は (3) の 2 項を（p に関して）バランスをとり全体の計算量を削減するものである。実際、因子基底を B の代わりに $\#B_0 = O(p^r)$, $0 < r < 1$ を満足する $B_0 \subset B$ とすれば、Algorithm 3 の計算量は、（g や $\log p$ を無視して）

$$\tilde{O}\left(\frac{p^g}{p^{rg}}p + p^{2r}\right) = \tilde{O}\left(p^{g+(1-g)r} + p^{2r}\right)$$

となる。従って、$r = g/(g+1)$ とすれば、その計算量が $\tilde{O}(p^{2g/(g+1)})$ となり、種数 $g \geq 4$ に対し rho 法より漸近的に計算量が小さいアルゴリズムが得られる。

また、Thériault[40] によってこのアルゴリズムのさらなる改良が行われた。この改良は素因数分解の標準的な高速化手法として知られる larg prime 手法を Gaudry アルゴリズム

[1]暗号応用考慮し、標準的な乗算アルゴリズムを利用することを仮定している。

に応用したものである。これは、B_0 の要素による関係式が得られる確率が $O(p^{g(r-1)})$ であるのに対して、1 個だけ $B \setminus B_0$ の要素[5]を含み他は B_0 の要素による関係式が得られる確率が $O(p^{(g-1)(r-1)})$ と高確率であることを利用している。実際、Algorithm 3 のステップ 3 のループを p^s 回繰り返した後には B_0 の要素による関係式が $O(p^{sg(r-1)})$ 個得られるが、さらに 1 個だけ $B \setminus B_0$ の要素を含み他は B_0 の要素による関係式が $O(p^{s(g-1)(r-1)})$ 個得られると期待される。これらの関係式の中には $B \setminus B_0$ の同一要素を含む組が $O(p^{2s(g-1)(r-1)-1})$ 組あると期待されるので、それぞれの組から $B \setminus B_0$ の要素を消去することで B_0 の要素のみによる新たな関係式が得られる。そしてその数は元々得られていた関係式の数より多い。そこで、r と s を最適に選択することで Gaudry アルゴリズムの計算量が削減される。

さらに、Nagao [30] と Gaudry, Thomḿe, Thériault, Diem [19] によって独立に 2 個の large prime を利用する改良が示された。このアルゴリズムの計算量は

$$\tilde{O}\left(q^{2-\frac{2}{g}}\right)$$

であり、これが低種数の超楕円曲線上の離散対数問題に対する現在までの最良計算量アルゴリズムである。この計算量から種数 g が十分に小さい範囲で $g \geq 3$ に対し rho 法より漸近的に計算量が小さいアルゴリズムであることがわかる。

このように種数が 3 以上の代数曲線上の離散対数問題に対しては漸近計算量が rho 法より小さいアルゴリズムが存在するため、これらを暗号利用する際にはその安全性に際し詳細な議論を必要とするようになった。特に種数が大きい代数曲線については暗号速度を維持しつつ安全性を確保することが困難であり、事実上暗号利用は不可能である。

注意 7.1 上記のような改良は素因数分解では漸近計算量削減手法ではなく高速化手法であるのに対し、超楕円曲線上の離散対数問題に対しては漸近計算量削減手法として働く。更に *large prime* を *3* 個以上含む関係式を利用しても漸近計算量は削減されない。

注意 7.2 ここで紹介したアルゴリズムは超楕円曲線以外の代数曲線上の離散対数問題に対しても適用可能である。更に、最近になって *Diem [11]* によって同一種数の超楕円曲線と比較して次数が小さい平面代数曲線に対するより効率的なアルゴリズムが示された。このアルゴリズムの計算量は次数 $d \geq 4$ の平面代数曲線に対して

$$\tilde{O}\left(p^{2-\frac{2}{d-2}}\right)$$

である。このアルゴリズムの出現により、超楕円曲線以外の高種数代数曲線を暗号に利用することは困難になった。

8 楕円曲線上の離散対数問題への応用

前節で紹介した攻撃法を拡大体上定義された楕円曲線（や超楕円曲線等）の上の離散対数問題に適用可能な場合があることが Frey, Gangle [15] によって指摘された。これは、楕

[5] このような要素を large prime という。

円曲線の $\mathbb{F}_{p^k}$ 有理点群 $E(\mathbb{F}_{p^k})$ を種数 $g \geq k$ の代数数曲線 C の Jacobian の有理点群 $\mathcal{J}_C(\mathbb{F}_p)$ に埋め込み、$\mathcal{J}_C(\mathbb{F}_p)$ 上で前節のアルゴリズムによって離散対数問題を解くものである。この攻撃は「Weil descent 攻撃」と呼ばれる。その後、Gaudry, Hess, Smart [18] によって、この攻撃の陽な（GHS-Weil descent と呼ばれる）アルゴリズムが示され、これについて多くの研究がなされてきた。これらについては [6, Chapter VIII], [8, Section 22.3] 等を参照されたい。この攻撃が効率的であるためには C の種数 g が（$g = k$ を満足する等）k に十分に近い必要があり、どの程度の数の曲線に対し効果があるか等研究課題が多い。このような状況において、例えば、$\mathbb{F}_{p^4}$ 上の（暗号に適した）楕円曲線の全てに対し Weil descent 攻撃の計算量が漸近的に rho 法より小さいこと等が示され始めている [4]。さらに、高種数代数曲線 C を介さない方法が最近提案された [17], [31]。これは、因子基底に $\mathcal{J}_C(\mathbb{F}_p)$ を用いる代わりに

$$B = \left\{ P \in E(\overline{\mathbb{F}}_p) | X(P) \in \mathbb{F}_p \right\}$$

を用いて（従って、一般には $B \not\subset E(\mathbb{F}_{p^k})$）、「関係式」を得るために 1 変数多項式の素因子分解を行う代わりに多変数代数方程式系の求解を行うものである。

暗号に利用されるサイズの離散対数問題に対してこれらのアルゴリズムがどの程度の効果を持つのかについては、現在迄殆ど知見がない状態である。

9 おわりに

本稿では触れることができなかったが、（楕円曲線暗号を含む）代数曲線暗号に関する最近の研究成果の多くが「ペアリング暗号」に関するものであることを付記する。この分野は、[45] や [28] 等、日本人の研究結果を端緒としている。また、多くの（計算）数論的な問題を残している分野である。この分野の研究状況については [6, Part 4] や [41, 8] の他に本スクールの直前に東京で開催された国際会議の proceedings [38] 等を参照されるとよいだろう。

参考文献

[1] L. Adleman. A subexponential algorithm for the discrete logarithm problem with applications. In *Proc. 20th Ann. IEEE Symp. on Foundations of Computer Science*, pp. 55–60, 1979.

[2] L. Adleman, J. DeMarrais, and M. Huang. A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobian of large genus hyperelliptic curves over finite fields. In *ANTS-I*, LNCS 877, pp. 28–40. Springer, 1994.

[3] S. Arita. An addition algorithm in Jacobian of C_{34} curve. In *Information Security and Privacy, ACISP 2003*, LNCS 2727, pp. 248–258. Springer, 2003.

[4] S. Arita, K. Matsuo, K. Nagao, and M. Shimura. A Weil descent attack against elliptic curve cryptosystems over quartic extension fields. *IEICE Trans.*, Vol. E89-A, No. 5, May 2006. 1246-1254.

[5] I. Blake, G. Seroussi, and N. Smart. *Elliptic Curves in Cryptography.* LMS 265. Cambridge U. P., 1999.

[6] I. Blake, G. Seroussi, and N. Smart, editors. *Advances in Elliptic Curves Cryptography.* LMS 317. Cambridge U. P., 2005.

[7] D. G. Cantor. Computing in the Jacobian of hyperelliptic curve. *Math. Comp.*, Vol. 48, No. 177, pp. 95–101, 1987.

[8] H. Cohen, G. Frey, C. Doche, editors. *Handbook of elliptic and hyperelliptic curve cryptography.* Chapman & Hall/CRC, 2005.

[9] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein. *Introduction to Algorithms.* MIT Press, 2nd edition, 2001.

[10] R. Crandall and C. Pomerance. *Prime Numbers.* Springer, 2nd edition, 2005.

[11] C. Diem. An index calculus algorithm for plane curves of small degree. In *ANTS-VII*, LNCS 4076, pp. 543–557. Springer, 2006.

[12] W. Diffie and M. Hellman. New direction in cryptography. *IEEE Trans.*, Vol. IT-23, No. 6, pp. 644–654, 1976.

[13] T. ElGamal. A public key cryptosystem and sigunature scheme based on discrete logarithms. *IEEE Trans.*, Vol. IT-31, No. 4, pp. 469–472, 1985.

[14] A. Enge and P. Gaudry. A general framework for subexponential discrete logarithm algorithms. *Acta Arith.*, Vol. 102, pp. 83–103, 2002.

[15] G. Frey and H. Gangl. How to disguise an elliptic curve (Weil descent). Talk at ECC '98, The 2nd Workshop on Elliptic Curve Cryptography, U. Waterloo, `http://www.cacr.math.uwaterloo.ca/conferences/1998/ecc98/frey.ps`, 1998.

[16] P. Gaudry. An algorithm for solving the discrete log problem on hyperelliptic curves. In *Advances in Cryptology - EUROCRYPT 2000*, LNCS 1807, pp. 19–34. Springer, 2000.

[17] P. Gaudry. Index calculus for abelian varieties and the elliptic curve discrete logarithm problem. Cryptology ePrint Archive, Report 2004/073, 2004. `http://eprint.iacr.org/`.

[18] P. Gaudry, F. Hess, and N. P. Smart. Constructive and destructive facets of Weil descent on elliptic curves. *Journal of Cryptology*, Vol. 15, No. 1, pp. 19–46, 2002.

[19] P. Gaudry, E. Thomé, N. Thériault, and C. Diem. A double large prime variation for small genus hyperelliptic index calculus. *Math. Comp.*, Vol. 76, No. 257, pp. 475–492, 2007.

[20] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, Vol. 48, pp. 203–209, 1987.

[21] N. Koblitz. Hyperelliptic curve cryptosystems. *J. Cryptology*, Vol. 1, No. 3, pp. 139–150, 1989.

[22] N. Koblitz. *A course in number theory and cryptography.* GTM 114. Springer, 2nd edition, 1994.

[23] N. Koblitz. *Algebraic Aspects of Cryptography*, Vol. 3 of *Algorithms and Computation in Mathematics.* Springer, 1998.

[24] A. Menezes. *Elliptic Curve Public Key Cryptosystems.* Kluwer Academic Pub., 1993.

[25] A. Menezes, P. van Oorschot, and S. Vanstone. *Handbook of applied cryptography.* CRC Press, 1997.

[26] A. Menezes, Y. Wu, and J. Zuccherato. An elementary introduction to hyperelliptic curves. Appendix to [23], 1998.

[27] V. S. Miller. Use of elliptic curves in cryptography. In *Advances in Cryptology - CRYPTO '85*, LNCS 218, pp. 417–426. Springer, 1986.

[28] A. Miyaji, M. Nakabayashi, and S. Takano. New explicit conditions of elliptic curve traces for FR-reduction. *IEICE Trans.*, Vol. E84-A, No. 5, pp. 1234–1243, 2001.

[29] D. Mumford. *Tata Lectures on Theta II.* PM 43. Birkhäuser, 1984.

[30] K. Nagao. Index calculus attack for Jacobian of hyperelliptic curves of small genus using two large primes. *Japan J. of Industrial and Applied Math.*, Vol. 24, No. 3, 2007.

[31] K. Nagao. On the decomposition of an element of jacobian of a hyperelliptic curve. Cryptology ePrint Archive, Report 2007/112, 2007. `http://eprint.iacr.org/`.

[32] S. Paulus and A. Stein. Comparing real and imaginary arithmetics for divisor class groups of hyperelliptic curves. In *ANTS-III*, LNCS 1423, pp. 576–591. Springer, 1998.

[33] G. C. Pohlig and M. E. Hellman. An improved algorithm for comuting logarithms over GF(p) and its cryptographic significance. *IEEE Trans. on Info. Theory*, Vol. IT-24, pp. 106–110, 1978.

[34] J. M. Pollard. Monte Carlo methods for index computation (mod p). *Math. Comp.*, Vol. 32, pp. 918–924, 1978.

[35] R. L. Rivest, A. Shamir, and L. M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Com. of the ACM*, Vol. 21, No. 2, pp. 120–126, 1978.

[36] D. Shanks. Class number, a theory of factorization, and genera. In *Proc. of Symp. Math. Soc. 20*, pp. 415–440, 1971.

[37] V. Shoup. *A computational introduction to number theory and algebra*. Cambridge U. P., 2005.

[38] T. Takagi, T. Okamoto, E. Okamoto, and T. Okamoto, editors. *Pairing-based cryptography - Pairing 2007*. LNCS 4575. Springer, 2007.

[39] E. Teske. Square-root algorithms for the discrete logarithm problem (A survey). In *Public-Key Cryptography and Computational Number Theory*, pp. 283–301. Walter de Gruyter, 2001.

[40] N. Thériault. Index calculus attack for hyperelliptic curves of small genus. In *Advances in Cryptology - ASIACRYPT 2003*, LNCS 2894, pp. 75–92. Springer, 2003.

[41] L. Washington. *Elliptic curves: number theory and cryptography*. Chapman & Hall/CRC, 2003.

[42] 青木. 楕円曲線暗号はどこまで速くなるか? — ソフトウェア実装の到達点. 仙台数論小研究集会 2000, 東北大, 2000. `http://staff.miyakyo-u.ac.jp/~taya/sendaiNT/2000/aoki_m.pdf`.

[43] 松尾. 代数曲線暗号とその安全性. 2007 年度 整数論サマースクール講演資料, `http://http://lab.iisec.ac.jp/~matsuo_lab/pub/pdf/sss_mats.pdf`, 2007.

[44] 入海, 松尾, 趙, 辻井. 超楕円曲線上の Harley アルゴリズムにおける resultant 計算について. Technical Report ISEC2006-5, 電子情報通信学会, 2006.

[45] 大岸, 境, 笠原. 楕円曲線上の ID 鍵共有方式の基礎的考察. Technical Report ISEC99-57, 電子情報通信学会, 1999.

第 15 回 整数論サマースクール 報告集, pp.239-246

アーベル多様体の有理等分点について

小川 裕之*

§1 序文

(a) いきなりですが, 定理をひとつ.

定理 1.1 (Mordell-Weil) k を有限次代数体とし, A を k 上定義されたアーベル多様体とする. このとき, A の k-有理点の全体 $A(k)$ (Mordell-Weil 群) は有限生成アーベル群である.

アーベル多様体について学び始めてすぐに習う定理のひとつと思います. 多様体の有理点は適当な連立方程式系の解で, 有限個の生成元を求めればすべての解がわかるわけです. 例えとして適切ではないかもしれませんが, Pell 方程式の解の全体が二次体の単数群に関係し, 基本解 (基本単数) から簡単な手続きですべての解が得られることに似ています. Mordell-Weil 群の生成元を具体的に求めることができるでしょうか. "アーベル多様体とその点の記述方法" を考え, "有理点をすべて見つけるアルゴリズム" を作る. 有理数体上の楕円曲線 (1 次元アーベル多様体) の場合でもまだ完全ではありません. 問いを少し易しくして, "自由部分の階数がどの程度であるか" とか, "ねじれ部分群としてどの様な群が現れるか" とか, "等分点の位数としてどの様な数が現れるか" とか. 自由部分の階数については, "幾らでも階数の大きな, 有理数体上定義された楕円曲線が存在するだろう" と思われていますが, "有理数体上定義された楕円曲線の階数は上に有界であろう" と相反する予想もあります. どちらもそれなりに言い分があります. 階数にはあまり深入りせず, Mordell-Weil 群のねじれ部分群について話します.

(b) アーベル多様体の等分点は, 類体の構成など重要な対象ですが, 図形的にも面白い. 有理数体上定義された楕円曲線の場合, 例外点 (exceptional point) というものがありました. 楕円曲線上のある点 P_0 から始めて, その点での接線が元の楕円曲線と交わる点 P_1 とおく. P_1 での接線が再び楕円曲線と交わる点を P_2 とおきます. 以下これを繰り返して, 楕円曲線上の点を取り続けます. 点の列が周期的になるとき P_0 を例外点と言いました. 例外点でなければ, 楕円曲線上の有理点がどんどん見つかります. 周期の長い例外点を探す過程で, 加法群としての楕円曲線が詳しく調べられました. 各回の操作は楕円曲線の -2 倍写像で, 例外点は等分点に当たります. 例外点の周期の長さの探求は, "有理数体上定義されたすべての楕円曲線について, 等分の位数は有界か?" (Kubert) という上限予想につながりました. 結局,

*大阪大学大学院 理学研究科

定理 1.2 (Mazur) (Springer LNM 601 (1977), 107–148) 楕円曲線 $E/\mathbb{Q}$ に対して, $\mathbb{Q}$-有理等分点全体 $E(\mathbb{Q})_{\mathrm{tors}}$ は次の群のいずれかに同型である： $\mathbb{Z}/n\mathbb{Z}$ $(n = 1, 2, 3, \cdots, 9, 10, 12)$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ $(m = 1, 2, 3, 4)$

これら 15 個の群が実際に現れることは具体的に計算すればできますが, これら以外の群が現れないことを証明するのは非常に大変なことです. Billing-Mahler (J. London Math. Soc. 15 (1940), 32–43), Ogg (Invent. Math. 12 (1971), 105–111), Mazur-Tate (Invent. Math. 22 (1973/74), 41–49) らによって, 与えられた自然数が有理等分点の位数として現れないことを証明する方法が確立されました. Ogg (Bull. Amer. Math. Soc. 81, 1975) が上の 15 個に限ると予想し, Mazur が証明しました.

(c) 次に向かうべき方向は, 定義体をより大きな次数の代数体に取ることと, 次元の高いアーベル多様体を扱うことの 2 つ考えられます. 定義体の次数を上げる方向でも, 次の様に予想されました.

予想 1.3 (楕円曲線の上限予想) 自然数 d にのみ依存する定数 $B(d)$ が存在し, 次が成り立つ： d 次代数体 k 上定義された楕円曲線 E に対して, E の k-有理等分点の位数は $B(d)$ を越えない.

Kenku-Momose (Nagoya Math. J. 109 (1988), 125–149) によって, 二次体上定義された楕円曲線の有理等分点群の取り得る形 (25 個) が得られ, 更に 17 以上の素数位数等分点が存在しないなら, その 25 個に限ることが示されました. また, 幾つかの素数について, その位数の等分点が存在しないことも示されました. Kamienny (Bull. Amer. Math. Soc. 23 (1990), no. 2, 371–373 / Invent. Math. 109 (1992), no. 2, 221–229) により, "二次体上定義された楕円曲線において, 有理等分点の位数の素因子は 13 以下である" ことが示され,

定理 1.4 (Kamienny-Kenku-Momose) 2 次体 k 上定義された楕円曲線の有理等分点のなす群は, 次のいずれかに同型である： $\mathbb{Z}/n\mathbb{Z}$ $(n = 1, 2, \cdots, 14, 16, 18)$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ $(m = 1, 2, \cdots, 6)$,

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3m\mathbb{Z} \ \ (m = 1, 2 \ \ k = \mathbb{Q}(\sqrt{-3})), \ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \ \ (k = \mathbb{Q}(\sqrt{-1}))$$

Kamienny は, 二次体のときの流れを踏まえて, "楕円曲線の有理等分点の素因子は, 定義体の次数にのみ依存する定数を上限にもつだろう" と, 上限予想より少し弱い予想を考えました. Kamienny-Mazur (Astérisque No. 228 (1995), 3, 81–100) は, Kamienny の予想から上限予想が従うことを示し, $d \leq 8$ について Kamienny の予想が成り立つことを示しました. Abramovich (Astérisque No. 228 (1995), 3, 5–17) は, Kamienny-Mazur の方法を精密化して $d \leq 12$ について上限予想が正しいことを示しました. 結局, Merel (Invent. Math. 124 (1996), no. 1–3, 437–449) により, d 次代数体について, 楕円曲線の有理等分点の位数の素因子は $(1 + 3^{d/2})^2$ 以下であることが示されました.

定理 1.5 (Merel) すべての自然数 d に対して, 上限 $B(d)$ が存在する. つまり, 楕円曲線の上限予想は正しい.

Parent (J. Reine Angew. Math. 506 (1999), 85–116) は, Merel 結果から $B(d)$ の効率的な上界を与るために, 素数べキ位数の等分点に関する評価を与えました. 煩雑になりますが, Merel の結果と合わせると, $B(d)$ の具体的な評価式が得られます.

定理 1.6 (Parent) d 次代数体上定義された楕円曲線について, 有理等分点の位数が p^n ($p \geq 5$ は素数) であるなら, $p^n \leq 65\,(3^d-1)\,(2d)^6$ が成り立つ.

(d) アーベル多様体の次元を上げる方向には, 余り多くの結果は得られていません. ともかく想定されるのは, 次の一般上限予想でしょう.

予想 1.7 (一般上限予想) 自然数 d, g にのみ依存する定数 $B(d, g)$ が存在し, 次が成り立つ: d 次代数体 k 上定義された絶対既約な g 次元アーベル多様体 A に対して, A の k-有理等分点の位数は $B(d, g)$ を越えない.

虚数乗法をもつアーベル多様体に限るなら, Silverberg (Contemp. Math. 133 (1992), 175–193) により,

定理 1.8 (Silverberg) アーベル多様体として虚数乗法をもつもののみを考えるとき, 上限予想は正しい. 特に, 虚数乗法をもつ有理数体上定義された 2 次元アーベル多様体について, 有理等分点の位数は 185640 を越えない.

一般的には殆ど何も得られておらず, 良し悪しは別にして, 楕円曲線で例外点と言って楽しんでいたころの様なのんびりした雰囲気にあるようです. 以下, §2 で代数曲線の因子類群について話します. Torelli の定理により, 3 次元以下の (絶対既約な) アーベル多様体は非特異完備代数曲線のヤコビ多様体に同型であるので, 代数曲線の因子類群に限定してもそれほど不都合はないでしょう. 一般のアーベル多様体で加法を扱うのはとても大変なのですが, 因子類群の加法なら Riemann-Roch の定理を使って, 楕円曲線と同じ感覚で計算できるでしょう. §3 で位数の高い有理等分点探索の記録について話し, それらのもとになった Leprévost による位数の高い有理因子類を見つける方法を §4 で解説します.

§2 有理因子類

(a) k を有限次代数体とし, $\overline{k}$ をその代数閉包とする. ガロア群を $G_k = \mathrm{Gal}(\overline{k}/k)$ とおく. C を k 上定義された非特異完備代数曲線とし, その種数を $g = g(C)$ とする. C の点で生成された自由アーベル群を C の因子類群 $\mathrm{Div}(C)$ という. 任意の因子 $D \in \mathrm{Div}(C)$ は, C の各点ごとにまとめた和 $D = \sum e_P P \quad (e_P \in \mathbb{Z})$ に表すことができる. すべての係数 e_P が非負の因子 D を整因子といい, $D \geq 0$ と書く. 因子 D の係数の和 $\deg D = \sum e_P$ を D の次数といい, 次数が 0 の因子の全体を $\mathrm{Div}^0(C)$ と書く. $\overline{k}(C)$ を C の函数体とする. 有理函数 $\varphi \in \overline{k}(C)^\times$ の因子を $\mathrm{div}(\varphi)$ と書く. 函数の因子を主因子といい, 主因子全体のなす群 $\mathrm{Div}^\ell(C)$ を主因子群という. 主因子の次数は 0 なので, 主因子群は $\mathrm{Div}^0(C)$ の部分群である. $\mathrm{Pic}^0(C) = \mathrm{Div}^0(C)/\mathrm{Div}^\ell(C)$ を因子類群 (Picard 群) という. 因子 D の属する因子類を $[D]$ と書く.

(b) 代数曲線 C として k 上定義された物を取ったので, ガロア群 G_k の作用を考えることができる. これまで単に C の点というときには, 座標が $\overline{k}$ に含まれるものを考えていた. 点の各座標に G_k を作用させることで, C の点の全体に G_k が働く. この作用で不変な点

$P \in C$ を k-有理点と呼び, k-有理点の全体を $C(k)$ と書く. C への G_k の作用が因子群に自然に延びる. G_k-不変な因子を k-有理因子といい, k-有理因子の全体を $\mathrm{Div}(C)(k)$ と書く. $\mathrm{Div}(C)(k) \subset \mathrm{Div}(C)$ は G_k-不変な部分群である. 因子の次数はガロア群の作用で変わらないので, $\mathrm{Div}^0(C) \subset \mathrm{Div}(C)$ も G_k-不変な部分群である. 有理函数の係数への作用により, G_k は函数体にも働く. G_k-不変な有理函数を k 上定義された有理函数といい. k 上定義された有理函数の全体を $k(C)$ と書く. 任意の $\sigma \in G_k$ に対して $\mathrm{div}(\varphi)^\sigma = \mathrm{div}(\varphi^\sigma)$ が成り立つので, 主因子群 $\mathrm{Div}^\ell(C) \subset \mathrm{Div}(C)$ も G_k-不変な部分群である. $\mathrm{Div}^0(C)$ も $\mathrm{Div}^\ell(C)$ も G_k-不変だったので, 因子類群 $\mathrm{Pic}^0(C) = \mathrm{Div}^0(C)/\mathrm{Div}^\ell(C)$ に自然にガロア群 G_k が作用する. 実際 $\sigma \in G_k$, $[D] \in \mathrm{Pic}^0(C)$ に対して, $[D]^\sigma = [D^\sigma]$ で σ の作用が定まる. G_k-不変な因子類を k-有理因子類といい, k-有理因子類の全体を $\mathrm{Pic}^0_k(C)$ とおき, k-有理因子類群という.

(c) Riemann-Roch の定理より, 種数 $g = g(C)$ が 0 のとき 0 次の因子は主因子になり ($\mathrm{Div}^0(C) = \mathrm{Div}^\ell(C)$), 因子類群 $\mathrm{Pic}^0(C)$ は消える. 以下, 種数は 1 以上とする. 因子類群 $\mathrm{Pic}^0(C)$ は C のヤコビ多様体 $J(C)$ (の $\overline{k}$-有理点全体のなす群) に同型で, $\mathrm{Pic}^0_k(C)$ はその k-有理点群 $J(C)(k)$ である. ヤコビ多様体は $g = g(C)$ 次元の k 上定義されたアーベル多様体なので, Mordell-Weil の定理により k-有理因子類群 $\mathrm{Pic}^0_k(C)$ は有限生成アーベル群になる. 位数が有限の因子類を等分点 (あるいは, ねじれ因子類) といい, 位数が有限の k-有理因子を k-有理等分点という. $\mathrm{Pic}^0_k(C)$ のねじれ部分群を $\mathrm{Pic}^0_k(C)_{\mathrm{tors}}$ と書き, k-有理等分点群という.

(d) 点 $P_0 \in C$ を任意にとる. C から $\mathrm{Pic}^0(C)$ への写像 $\Phi_{P_0} : C \ni P \longmapsto [P - P_0] \in \mathrm{Pic}^0(C)$ を (P_0 を基点とする) 基準写像という.

Riemann-Roch の定理より, 種数が 1 なら Φ_{P_0} は単射になる. Φ_{P_0} により C は $\mathrm{Pic}^0(C)$ に (部分多様体として) 埋め込まれる. 曲線 C の n 個の対称積を $\mathrm{Sym}^n(C)$ とおく. $\mathrm{Sym}^n(C)$ は n 次の整因子の全体に等しい. n 次の因子 D_0 に対して, 写像 $\Phi_{D_0} : \mathrm{Sym}^n(C) \ni D \longmapsto [D - D_0] \in \mathrm{Pic}^0(C)$ が定義できる. Φ_{D_0} を D_0 を基点とする (一般) 基準写像という. Riemann-Roch の定理より, $n \geq g$ のとき Φ_{D_0} は全射になる. 特に $g = 1$ のとき, 基準写像 $\Phi_{P_0} : C \to \mathrm{Pic}^0(C)$ は C からヤコビ多様体 $J(C)$ への代数多様体の同型写像を引き起こす. ヤコビ多様体 (因子類群) の加法演算が, 基準写像を通して, 種数 1 の代数曲線 C の上に定義される. C の加法演算における零元は P_0 なので, 結局のところ, 種数 1 の代数曲線 C に零元 P_0 を指定することでアーベル多様体 (C, P_0) $(= J(C) = \mathrm{Pic}^0(C))$ が定まる. 同じ様に, 種数 g の非特異完備代数曲線 C に対して, g 次の (整) 因子 D_0 を指定することで, 因子類群 $\mathrm{Pic}^0(C)$ の加法演算を $\mathrm{Sym}^g(C)$ の上に描くことができる. ただし, 種数が 2 以上の場合 Φ_{D_0} は単射でないので因子類の代表としての $\mathrm{Sym}^g(C)$ の元の選び方を指定する必要がある. 殆どの点で (余次元 1 以下の部分多様体の和を除いて) 単射なので, 計算機に載せるのでなければ, あまり神経質にならなくてもちょっと手を動かしてみればすぐに見分けがつくようになるでしょう. 最も簡単な場合だが, 種数が 2 のものをまとめておく.

命題 2.1 C を種数が 2 の超楕円曲線とし, 無限遠点 ∞ は超楕円対合に関して不変とする. 2 次の因子として 2∞ をとると, $\Phi_{2\infty}$ は $\Phi_{2\infty}^{-1}(0)$ を除いて 1 対 1 に対応する. 更に $\Phi_{2\infty}^{-1}(0) = \{P + P' \in \mathrm{Sym}^2(C)\} \simeq \mathbb{P}^1$ である.

基準写像を使って, 因子類の代表として次数 g の整因子を取った. 2 点 $P, Q \in C$ に対して, 因子類 $[P-Q]$ をパケットという. 種数が 2 のとき, 因子類の代表としてパケットを取ることができる. 基準写像は基点の選び方に依存する. パケットで代表を取ると, 基点の様なものに依存せず, 因子類の点を表せる. 一般の種数 (偶数の方が易しい) に対しても, パケットの和, あるいは $g/2$ 次の整因子のパケットを考えれば, 基点によらない因子類の記述ができる.

命題 2.2 C を種数が 2 の非特異完備曲線とし, 写像 $\Psi : C \times C \ni (P, Q) \longmapsto [P-Q] \in \mathrm{Pic}^0(C)$ を考える. このとき Ψ は全射で, $\Psi^{-1}(0) = \{(P, P) \in C \times C\} \simeq C$ を除いて 2 対 1 に対応する.

(e) n 次整因子の全体 $\mathrm{Sym}^n(C)$ に自然に G_k が作用する. G_k-不変な n 次整因子の全体を $\mathrm{Sym}^n_k(C)$ とおく. $D_0 \in \mathrm{Sym}^n_k(C)$ をとる. 基準写像 $\Phi_{D_0} : \mathrm{Sym}^n(C) \to \mathrm{Pic}^0(C)$ について, $\mathrm{Sym}^n_k(C)$ の像は k-有理因子類群 $\mathrm{Pic}^0_k(C)$ に含まれる.

§3 位数の高い有理等分点探索の記録

ここでは, 定義体は有理数体 $\mathbb{Q}$ か 1 変数有理函数体 $\mathbb{Q}(t)$ 上定義された非特異完備代数曲線で, 位数の高い有理等分点をもつものの構成についてまとめます. 一般上限予想 (予想 1.7) で言うなら $B(1, g)$ の下界を与えることになります. 上限 $B(1, g)$ が種数 g に関してどの様な変動をするか眺めることができるかもしれない. 1 変数つき ($\mathbb{Q}(t)$ 上) で考えるのは, 等分点のモジュライ空間に射影直線などの多様体が ($\mathbb{Q}$ 上で) 埋め込まれているかどうかなど, モジュライ空間の様子を垣間見たい. あるいは, ともかく $\mathbb{Q}$ 上定義されるものをたくさん作って楽しみたい.

一般上限予想では絶対既約なアーベル多様体に限定していますが, 楕円曲線の直積など絶対既約でないものも許せば $B(d, g) \geq B(d, 1)^g + O(1)$ となります. $B(d, g)$ は有理等分点群に含まれる最大位数の上限なので, 互いに素な有理点を選ぶ必要があるので誤差項 $O(1)$ を含んでいます. 誤差項の評価を良くすることもできますが, 余り意味がないので書きません. また, 代数体上の楕円曲線の線形制限 (scalar restriction) を考えれば $B(d, g) \geq B(dg, 1)$ などの評価も得られます.

E. V. Flynn (J. Number Theory 36 (1990), no. 3, 257–265) は, $\mathbb{Q}(t)$ 上定義された種数が g の超楕円曲線で位数が $2g^2 + g + 1$ の有理等分点をもつものを作りました. 特に $g = 2$ のとき $2 \times 2^2 + 2 + 1 = 11$ なので, 有理数体上定義された楕円曲線の有理等分点として現れない, 位数 11 の有理等分点を得ました.

F. Leprévost (C. R. Acad. Sci. Paris Ser. I Math. 313 (1991), no. 7, 451–454 / no. 11, 771–774) は, 有理等分点を作り出すうまい手続きを与え, それを使って種数が 2 のときに位数 13, 15, 17, 19, 21 の有理等分点をもつ超楕円曲線の 1 パラメータ族を作りました. その手続きを一般種数に拡げ, Leprvost (Manuscripta Math. 75 (1992), no. 3, 303–326) は, 種数が g の超楕円曲線で位数が $2g^2 + 2g + 1$ のものと $2g^2 + 3g + 1$ のものの 1 パラメータ族を作りました. 次節 (§4) でその方法を説明します. 更に Leprévost (C. R. Acad. Sci. Paris Sér. I Math. 316 (1993), no. 8, 819–821) は, 一つか二つずつですが, 22 ～ 29 の等

分点をもつ, 種数 2 の $\mathbb{Q}$ 上の超楕円曲線を作りました. これらの幾つかはそのヤコビ多様体が絶対既約ではないのですが, 29 等分点をもつものは絶対既約になっています. ここで得られた下限 $B(1,2) \geq 29$ は, $B(1,2)$ について現在最良のものです.

Ogawa (Proc. Japan Acad. Ser. A Math. Sci. 70 (1994), no. 9, 295–298) は, Leprévost の方法を真似て, 23 等分点をもつ超楕円曲線の 1 パラメータ族を作りました. 単に作るだけでなく問題意識として 2 のことを指摘しました. ひとつはこの節の始めにある絶対既約の必要性で, もうひとつは, パラメータ族が等分点のモジュライ空間で退化していないことを井草不変量を使って確かめることです.

Leprévost (Manuscripta Math. 92 (1997), no. 1, 47–63) は, $\mathbb{Q}$ 上で位数が $2g(2g+1)$ の有理等分点をもつ超楕円曲線と, $2g^2+5g+5$ の有理等分点をもつ超楕円曲線を作りました. $g \geq 3$ では $B(1,g) \geq 2g(2g+1)$ が下限として現在知られている最良のものです.

Leprévost (Forum Math. 12 (2000), no. 3, 315–364) は, 絶対既約でないものについても, 曲線のヤコビ多様体という条件下でなら自明とは言い切れないことから, 絶対既約のものとは区別して有理等分点の位数の評価を問うた. 種数 2 で 63 等分点, 種数 3 で 60 等分点をもつものを作っています. 絶対既約でない場合は有理等分点群が幾つもの巡回群の直積に分かれるので, 有理等分点群の位数としては, 種数 2 のとき位数 128, 種数 3 のとき位数 864 のものが得られています. 2 個の楕円曲線の直積で, 位数が $12 \times 7 = 84$ の有理等分点や $10 \times 9 = 90$ の有理等分点をもつものが作れ, 3 個の楕円曲線の直積では, 位数が $12 \times 7 \times 5 = 420$ や $10 \times 9 \times 7 = 630$ のものが作れます. 有理等分点群の位数としては g 個の直積で $(2 \times 8)^g = 16^g$ のものが作れます. それらが曲線のヤコビ多様体 (に同種) なものとして作れるかどうかはわかっていません. 絶対既約などの条件をつけても, 有理等分点の位数の上限は殆ど同じではないかと思われていますので, これらの数が $B(d,g)$ の値の目標値になるかもしれません.

§4 Leprèvost の方法

(a) Leprévost は, 位数の高い有理等分点をもつ超楕円曲線を見つける方法を考えました. 楕円曲線のときは因子類群と曲線自身が同型だったので, 各因子類は楕円曲線のある 1 点に対応していました. 種数が 2 以上のときは因子類の代表として, 曲線上の幾つかの点の組で表されます. 曲線上の有理点を幾つかとって, うまく組み合わせて適当な位数の有理因子類を作り出すのが彼のアイディアです.

$g \geq 1$ とする. 代数曲線

$$C : y^2 = f(x) = A^2(x) - \lambda\, x^{g+1}(x-a)^g$$

をとる. ここで $A(x) \in \mathbb{Q}[t]$ $(\deg A \leq g)$, $\lambda \in \mathbb{Q}$ とし, $f(x) = 0$ が重根を持たないようにとる. このとき C は種数 g の超楕円曲線で, $\mathbb{Q}$-有理点 $P_0 = (0,\, A(0))$, $P_1 = (1,\, A(1))$ をもつ. また $f(x)$ は奇数次なので C は唯一つの無限遠点 ∞ をもつ. このとき ∞ もまた $\mathbb{Q}$-有理的なので, $\{P_0,\, P_0',\, P_1,\, P_1',\, \infty\} \subset C(\mathbb{Q})$ となる. 因子 $D_0 = P_0 - \infty$, $D_1 = P_1 - \infty$ はともに $\mathbb{Q}$-有理因子なので, 因子類 $[D_0]$, $[D_1]$ は $\mathbb{Q}$-有理因子類になる.

命題 4.1 $a\,[D_0] + b\,[D_1] = 0$ をみたす $a,\, b \in \mathbb{Z}$ をとり, $\ell = (g+1)\,b - g\,a$ とおく. このとき $\ell[D_0] = 0$ が成り立つ.

この命題を示す. $\varphi(x,\,y)=y-A(x)\in\mathbb{Q}(C)$ とおくと,

$$\varphi\,\varphi'=(y-A(x))(-y-A(x))=-y^2+A^2(x)=\lambda\,x^{g+1}(x-1)^g$$

ここで $\varphi(P_0)=\varphi(P_1)=0$, $\varphi(P_0')\neq 0$, $\varphi(P_1')\neq 0$ なので,

$$\mathrm{div}(\varphi)=(g+1)\,P_0+g\,P_1-(2g+1)\,\infty=(g+1)\,D_0+g\,D_1$$

となる. 因子類で書くと $(g+1)\,[D_0]+g\,[D_1]=0$ となる. よって

$$\ell\,[D_0]=((g+1)b-g\,a)\,[D_0]=b(g+1)\,[D_0]-g\,a\,[D_0]=-b\,g\,[D_1]-g\,(-b)\,[D_1]=0$$

が従う.

(b) Leprévost が最初に与えた 13 等分点をもつ種数 2 の超楕円曲線は, Flynn の方法を真似て作ったものであった. 有理的な Weierstrass 点で高々 22 位の極をもつ有理函数の全体の中で, 特定の零点をもつ有理函数を見つける必要があり, 煩雑な計算の後に得られている. 1992 年の位数 $2g^2+2g+1$ の有理等分点をもつ超楕円曲線は, $\ell=2g^2+2g+1=(g+1)^2+g^2$ $(a=-g,\,b=g+1)$ に対して上の命題を満たす $A(x)\in\mathbb{Q}[x]$, $\lambda\in\mathbb{Q}$ を与えたものである. 一般の g でも全く同じ計算で, ここでは $g=2$ で述べる. $2\times 2^2+2\times 2+1=13$ なので, 13 等分点をもつ種数 2 の超楕円曲線が得られる. 計算に必要な有理函数は, 有理的な Weierstrass 点で高々 5 位の極をもつもので, Flynn の方法の大幅な改良になっているだけでなく, 驚くほど簡単に定義方程式が得られる.

$a=-2$, $b=3$, $\ell=(2+1)\,b-2\,a=3^2+2^2=13$ とおく. $A(x)\in\mathbb{Q}[x]$ $(\deg A\le 2)$, $\lambda\in\mathbb{Q}$ で, 超楕円曲線 $C:y^2=f(x)=A^2(x)-\lambda\,x^3(x-1)^2$ の有理因子 $D_0=P_0-\infty$, $D_1=P_1-\infty$ が $-2[D_0]+3[D_1]=0$ となるものを与えたい. 超楕円対合で $D_0'=P_0'-\infty$ とおくと, $\mathrm{div}(x)=P_0+P_0'-2\infty$ なので, $[D_0']=-[D_0]$ となる. 満たすべき条件式は

$$0=-2[D_0]+3[D_1]=2[D_0']+3[D_1]=[2\,P_0'+3\,P_1-5\infty]$$

と書ける. 有理函数 h で $\mathrm{div}(h)=2\,P_0'+3\,P_1-5\infty$ となるものを作ればよい. ∞ でのみ 5 位の極をもつ有理函数の全体 $L(5\infty)$ を考える. Riemann-Roch の定理より $\dim L(5\infty)=\ell(5\infty)=5-2+1=4$ となる. 座標関数 x は ∞ でのみ 2 位の極をもち, y は ∞ でのみ 5 位の極をもつ. $L(5\infty)$ は 1, x, x^2, y を基底にもつ. $h\in L(5\infty)$ なので $h=u(x)-y$ $(\deg u\le 2)$ とおける.

$$\mathrm{div}(h\,h')=\mathrm{div}(h)+\mathrm{div}(h)'=2\,(P_0+P_0'-2\infty)+3\,(P_1+P_1'-2\infty)=\mathrm{div}(x^2(x-1)^3)$$

なので,

$$h\,h'=\mu\,x^2(x-1)^3\quad(\mu\in\overline{\mathbb{Q}})$$

と書ける.

$$h\,h'=(u(x)-y)(u(x)+y)=u^2(x)-y^2=u^2(x)-A^2(x)+\lambda\,x^3(x-1)^2$$

だから,

$$(u(x)-A(x))(u(x)+A(x))=u^2(x)-A^2(x)=x^2(x-1)^2((\mu-\lambda)x-\mu)$$

を得る. $A(x)$ も $u(x)$ も次数は 2 以下なので, $\mu=\lambda$ である. $h=u(x)-y$ は $P_0'=(0,\,-A(0))$ と $P_1=(1,\,A(1))$ を零点にもつので, $u(0)+A(0)=0$, $u(1)-A(1)=0$ を満たす. 従って

$$u(x)-A(x)=r\,(x-1)^2\ ,\quad u(x)+A(x)=s\,x^2\ ,\quad r\,s=-\lambda\quad(r,\,s\in\overline{\mathbb{Q}})$$

となる.

すべてを 1 パラメータつきで取り直して,

$\lambda = 4\,t \in \mathbb{Q}(t)$, $A(t) = t\,x^2 - (x-1)^2$, $u(x) = t\,x^2 + (x-1)^2 \in \mathbb{Q}(t)[x]$ $(r = -2$, $s = 2t)$

とおく. $\mathbb{Q}(t)$ 上定義された超楕円曲線

$$C : y^2 = (t\,x^2 - (x-1)^2)^2 - 4\,t\,x^3(x-1)^2$$

において, 有理函数 $y - u(x)$ の因子は $\mathrm{div}(y - u(x)) = 2\,P_0' + 3\,P_1 - 5\infty$ である. $-2\,[D_0] + 3\,[D_1] = 0$ なので, 有理因子類 $[D_0]$ は $13\,[D_0] = 0$ を満たす.

第 15 回 整数論サマースクール 報告集, pp.247-264

Algebraic Theory of Abelian Varieties via Schemes

小林真一*

1 前書き

この講演では Mumford の Abelian varieties [Mum] の２章 Algebraic theory via varieties と３章 Algebraic theory via schemes について解説する. 内容はアーベル多様体の純代数的な取り扱いについてである. これにより基礎体の標数が正の場合にもアーベル多様体が扱える.

さてこの講演のタイトルは Mumford の本の３章の名前だったのだが, ２章の内容に重点をおき紹介する. そういう意味ではタイトルに偽りありである. しかし内容やアイデアを理解するには２章で十分で, via varieties といっておきながらも, ２章でも scheme 論の強力な定理や道具たちをフル活用するので, 抽象代数幾何的方法を味わうには十分である.

この講演では line bundle が頻出し, 内容は line bundle の研究といってもよいので, これらに馴染みがないとつらいのだが, よく知られているように複素トーラスの line bundle の section は, 複素一意化により theta 関数と思える. したがって line bundle やその section が出てきたら theta 関数が代数的に登場していると思うと理解の助けになるかもしれない. またこの講演では invertible sheaf と line bundle を同一視する. 実際ほとんどの場合 sheaf と思っている.

前書きの最後にアーベル多様体の基本文献について述べておく. Mumford [Mum] の他には, 古典として Lang [L] がよく知られているが, スキームではなく Weil の Foundation の言葉で書かれている. 現代的な解説としては Arithmetic Geometory という本の中で, Milne が書いたもの [Mil1] もよく知られている. また彼の Web page に Lecture Note [Mil2] もおいてある ([Mil1] とは異なる.) 最近の本としては Polishchuk [Pol] がある. また Van der Geer と Moonen が最近アーベル多様体の本を書いており, Geer の Web page に書きかけの draft [GM] (かなりの章が完成しているようにみえる) があり, おもしろい. Mumford [Mum] の他にこれらも参考にしていただけたらと思う.

前書きの最後に, 講演機会をくださった岩手大学の大西良博さんに感謝致します.

*名古屋大学大学院多元数理科学研究科

2　アーベル多様体の基本的な性質と Cube の定理

2.1　アーベル多様体の定義

k を代数閉体とする. k 上の完備 (complete, つまり k 上 proper) な代数多様体 X(integral, separated, finite type over k) と, 群の公理の条件をみたす“２項演算 morphism” , “単位元”, “逆元をとる morphism”

$$m : X \times X \to X, \quad e \in X, \quad i : X \to X$$

が与えられているとき, X とその演算の組をアーベル多様体という. ここでは２項演算の可換性は仮定してないが, 下ですぐに見るように, 自動的に可換になるので, m を $+$, e を 0, i を $(-1)_X$ または単に $-$ と書くことにする.

X には群演算があるので X はもしある一点で non-singular だったら平行移動により他の任意の点でも non-singular. X は variety なので必ず non-singular な点はあるから X は non-singular であることがわかる.

次の基本的な補題を使うと演算も自動的にアーベルになることがわかる. ここでは完備であることが非常に効いている. これ以外にも完備性 (compact 性と思ってよい) は群演算をもつ多様体に非常に強い制約を与える. たとえばあとでみるように X は射影多様体になる.

Lemma 2.1 (Rigidity の補題) X を完備代数多様体, Y, Z を任意の代数多様体とする. ここで *morphism* $f : X \times Y \to Z$ があり $y \in Y$ に対し, $X \times \{y\}$ を一点 z_0 につぶすと仮定する. このとき f はある写像 $g : Y \to Z$ と *projection* $p_2 : X \times Y \to Y$ の合成である.

証明　任意の $x_0 \in X$ をとって $g(y) = f(x_0, y)$ とおく. $X \times Y$ の既約性より, これが求める性質をもつことは f と $g \circ p_2$ が空でない開集合上一致することを示せばよい. U を z_0 を含むアフィン開集合とし, このとき X の完備性より p_2 が閉写像であることを使うと, ちょっとした集合論的な議論により Y の空でない開集合 V をとって f が写像 $X \times V \to U$ を引き起こすようにできる. ここで任意の $y \in V$ に対し, 完備な代数多様体は $X \times \{y\}$ はアフィン多様体 U におくられることになるので $f|_{X \times \{y\}}$ は定数写像. これより $(x, y) \in X \times V$ に対し $f(x, y) = f(x_0, y) = g \circ p_2(x, y)$. □

この補題より, 原点を固定する morphism は必ず群の homomorphism になることがわかる. 実際 $f(x + y) - f(y) - f(x)$ (正確には $f(x \cdot y) \cdot f(y)^{-1} \cdot f(x)^{-1}$ と書いた方がよいかもしれない) に Rigidity の補題を適用すればよい. 演算がアーベルであることは逆元をとるという写像は原点を固定するので homomorphism になることからわかる.

これらの性質は簡単に導けたが, たとえば等分点の構造などアーベル多様体の基本的な性質を導くためには, 次の節でみるシーソーの定理や Cube の定理などのツールが必要になる.

2.2　Cube の定理とその応用

アーベル多様体を研究する上での基本的なツールは次のものがある.

Theorem 2.2 (シーソーの定理) X を完備代数多様体. T を任意の代数多様体. $\mathscr{L}$ を $X \times T$ 上の *line bundle* とする. このとき集合

$$T_1 = \{t \in T \mid \mathscr{L}\,|_{X\times\{t\}} \text{は } \textit{trivial line bundle} \text{ と同型 }\}$$

は T の閉集合. そしてある T_1 上の *line bundle* $\mathscr{M}$ があって

$$p_2^*\mathscr{M} = \mathscr{L}\,|_{X\times T_1}.$$

ここで p_2 は *second projection* $X \times T_1 \to T_1$.

Theorem 2.3 (Cube の定理) X, Y を完備代数多様体. Z を任意の代数多様体. x_0, y_0, z_0 をそれぞれ X, Y, Z の点とする. このとき $X \times Y \times Z$ 上の *line bundle* $\mathscr{L}$ が *trivial* になるための必要充分条件は次の 3 つの *line bundle* がすべて *trivial* になることである.

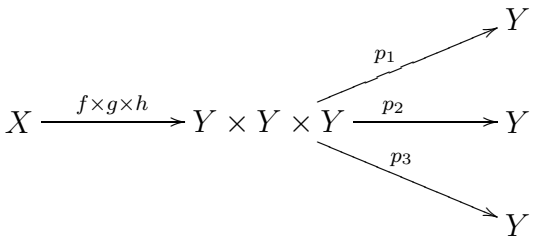
$$\mathscr{L}\,|_{\{x_0\}\times Y\times Z}, \quad \mathscr{L}\,|_{X\times\{y_0\}\times Z}, \quad \mathscr{L}\,|_{X\times Y\times\{z_0\}}$$

これらの定理の応用としてただちに次のことがわかる.

Corollary 2.4 X を代数多様体, Y をアーベル多様体とし, *3* つの *morphism* $f, g, h : X \to Y$ を考える. このとき $\mathscr{L} \in \mathrm{Pic}(Y)$ に対し,

$$(f+g+h)^*\mathscr{L} \cong (f+g)^*\mathscr{L} \otimes (g+h)^*\mathscr{L} \otimes (h+f)^*\mathscr{L} \otimes f^*\mathscr{L}^{-1} \otimes g^*\mathscr{L}^{-1} \otimes h^*\mathscr{L}^{-1}.$$

証明　下のダイヤグラムより $X = Y \times Y \times Y$ で f, g, h は projection である場合に示せば十分.



この場合は左辺と右辺の line bundle の商は $x_0 = y_0 = z_0$ を Y のゼロ元として Cube の定理の仮定を満たすことがただちにわかる. したがって trivial. □

Remark 2.5 Y が楕円曲線 *E*, $X = E \times E \times E$, f, g, h が *projection* とし, $\mathscr{L}$ が原点がつくる *divisor*$[0]$ に対応する *line bundle* $\mathcal{O}_E([0])$ とする. このとき上の系は E の *Weierstrass* σ-関数に対し, 関数

$$\frac{\sigma(z+y+w)\,\sigma(z)\,\sigma(y)\,\sigma(w)}{\sigma(z+w)\,\sigma(y+w)\,\sigma(w+z)}$$

が $E \times E \times E$ 上 *rational,* つまりそれぞれの変数に対し 2 重周期関数であるというよく知られた事実に他ならない. *(*σ は $\mathscr{L}$ の *(*定数倍をのぞいて*)* 唯一の *global section* に対応しており*, line bundle* が *trivialize* されると普通の *rational function* になる. *)*

Remark 2.6 この系はいわゆる *theta* 関数の *cubical structure* というものを与える *(Breen [Br]).* また *Barsotti, Cristante* の代数的 *(*ベキ級数*)theta* 関数の理論で本質的な役割を果たす *([Bar], [Cri1], [Cri2], [CC]).* つまり Y 上の *line bunde* の *section* から上のようにして *projection* により $Y \times Y \times Y$ 上に引き戻すことで*, line bundle* を *trivialize* し*, rational function* を取り出す. この $3dimY$*-*変数関数を適当な条件下 *(ordinary* など*)* で代数的に *split* させて Y 上の *theta* 関数を取り出す. *(Mazur-Tate* の *p-adic theta* 関数 *[MT]* もこのようにして作ることができる.*)*

Corollary 2.7 X をアーベル多様体*,* n を整数. このとき $\mathscr{L} \in \mathrm{Pic}(X)$ に対し*,*

$$n_X^*\mathscr{L} \cong \mathscr{L}^{\otimes \frac{n(n+1)}{2}} \otimes (-1)_X^*\mathscr{L}^{\otimes \frac{n(n-1)}{2}}.$$

証明　上の系において, $X = Y$, $f = (n+1)_X$, $g = 1_X$, $h = (-1)_X$ として $(n+2)_X^*\mathscr{L}$, $(n+1)_X^*\mathscr{L}$, $n_X^*\mathscr{L}$ に関する 3 項間の関係式を得る. $n = 0, 1$ のときは自明だから, 帰納法が成立. □

Intersection theory や line bundle の degree の理論と後で示す ample line bundle の存在を認めると, 上の系からアーベル多様体の n 倍写像の degree が $n^{2\dim X}$ であることがわかる. (degree はその morphism から生じる関数体の拡大の拡大次数.) 実際, D を ample で symmetric ($(-1)^*D = D$) な divisor とする. (たとえば D が ample なら $(-1)^*D + D$ は ample symmetric.) D は symmetric だから上の系より $n_X^*\mathscr{L} \cong \mathscr{L}^{n^2}$ がわかる. このとき Intersection theory から $g = \dim X$ 個の D の self-intersection に関して

$$(\deg n_X)(D, \ldots, D)_X = (n_X^*D, \ldots, n_X^*D)_X = n^{2g}(D, \ldots, D)_X.$$

または line bundle の degree の理論を使うと,

$$n^{2g}\deg \mathscr{L} = \deg \mathscr{L}^{n^2} = \deg (n_X^*\mathscr{L}) = \deg n_X \cdot \deg \mathscr{L}.$$

ample 性は $(D, \ldots, D)_X$, $\deg \mathscr{L}$ が zero でないことを保証する.

n 倍写像の degree が n^{2g} であることがわかると, 楕円曲線のときと同じような簡単な議論で X の n 等分点がなす群の構造がわかる. (n のすべての約数 d に関しても degree が d^{2g} であることが効く.)

Theorem 2.8 k の標数を p*,* $\dim X = g$ とおく.
i) $\deg n_X = n^{2g}$.
ii) n が p と素ならば*,* $X_n = \mathrm{Ker}\ n_X = (\mathbb{Z}/n\mathbb{Z})^{2g}$.
iii) ある自然数 $0 \leq i \leq g$ があって $X_{p^n} = (\mathbb{Z}/p^n\mathbb{Z})^i$.

次の定理は様々な応用上 (双対アーベル多様体の構成, Weil pairing の構成など) 非常に重要である.

Theorem 2.9 (正方形定理) X をアーベル多様体, x, y を X の点とする. このとき $\mathscr{L} \in \mathrm{Pic}(X)$ に対し,

$$T_{x+y}^*\mathscr{L} \otimes \mathscr{L} \cong T_x^*\mathscr{L} \otimes T_y^*\mathscr{L},$$

あるいは

$$T_{x+y}^*\mathscr{L} \otimes \mathscr{L}^{-1} \cong (T_x^*\mathscr{L} \otimes \mathscr{L}^{-1}) \otimes (T_y^*\mathscr{L} \otimes \mathscr{L}^{-1}).$$

ここで T_x は x をたすという平行移動 $X \to X, y \mapsto y + x$.

証明 系 2.4 において, $X = Y$, f をすべての点を x におくるという定数写像, g をすべての点を y におくるという定数写像, h を identity として適用すればよい. $T_x = \mathrm{id} + f$ に注意. □

ここで次の重要な (抽象群としての) 写像を定義する.

Definition 2.10 アーベル多様体 X 上の *line bundle* $\mathscr{L}$ に対し, 写像 $\phi_{\mathscr{L}}$ を次で定義する.

$$\phi_{\mathscr{L}} : \quad X \longrightarrow \mathrm{Pic}(X), \qquad x \longmapsto T_x^*\mathscr{L} \otimes \mathscr{L}^{-1}.$$

正方形定理より $\phi_{\mathscr{L}}$ は群の *homomorphism* になる. $\phi_{\mathscr{L}}$ が自明な写像になるような $\mathscr{L}$ の集合を $\mathrm{Pic}^0(X)$ とおく. このときやはり正方形定理より $\phi_{\mathscr{L}}$ の像は $\mathrm{Pic}^0(X)$ に含まれる.

Remark 2.11 楕円曲線 E の場合, $\mathscr{L} = \mathcal{O}_E([0])$ として, *linear equivalence* $\sim$ に対し

$$\phi_{\mathscr{L}} : \ E \to \mathrm{Pic}^0(E) = \mathrm{Div}^0(E)/\sim, \quad P \mapsto [P] - [0] \text{ の } \textit{class}.$$

双対アーベル多様体の節で, 実は $\phi_{\mathscr{L}} : X \to \mathrm{Pic}^0(X)$ は全射になることをみる. ここではまず $\phi_{\mathscr{L}}$ の核の性質を調べる.

Definition 2.12 $K(L) = \mathrm{Ker}\ \phi_{\mathscr{L}} = \{x \in X \mid T_x^*\mathscr{L} \cong \mathscr{L}\}$

$\phi_{\mathscr{L}}$ は単なる抽象群の写像として定義したので, 次は非自明である.

Proposition 2.13 $K(L)$ は X の *Zariski* 閉部分集合.

証明 閉集合であること以外は自明. 閉集合であることは $X = T$ として $X \times T$ 上の line bundle $m^*\mathscr{L} \otimes p_1^*\mathscr{L}^{-1}$ に対しシーソーの定理を使えばよい. □

次の命題はアーベル多様体の射影埋め込みを与える.

Proposition 2.14 D をアーベル多様体の *effective divisor*. $\mathscr{L} = \mathcal{O}_X(D)$ とおく. このとき次は同値.

i). X の部分群 $H = \{x \in X \mid T_x^*D = D\}$ は有限. *(divisor class* ではなく *divisor* としての等号.*)*

ii). $K(\mathscr{L})$ は有限.

iii). linear system

$$|2D| = \{D_0 \mid D_0 \text{ は } \textit{effective} \text{ で } D_0 \sim 2D\}$$

は *base point* をもたなく, それから誘導される $X \to \mathbb{P}^N$ *(*$N = \dim\Gamma(X, \mathscr{L}) - 1$*)* は *finite morphism.*

iv). $\mathscr{L}$ は *ample.*

Remark 2.15 おおざっぱなイメージとしては, *linear system* $|D|$ は $\mathcal{O}_X(D)$ に付随する正則 *theta* 関数の *divisor* になるものたち. *base point* がないとは $\mathcal{O}_X(D)$ に付随する正則 *theta* 関数たちは共通零点をもたないということ. したがって $\Gamma(X, \mathscr{L})$ の基底をつくる *theta* 関数 *(section)* たちを射影座標にならべて *morphism* $X \to \mathbb{P}^N$ を作ることができる. *(*古典的な *theta* 関数による射影埋め込み*.)* これらの正確な *scheme theoretic* な扱いや任意のスキーム X に一般化したものは *Hartshorne §7, Chapter II* にある.

$\mathscr{L}$ が *ample* とは非常に大雑把にいうと *global section* が十分にあるということ. $\mathscr{L}$ が *ample* になるための必要十分条件はある自然数 n があって $\mathscr{L}^n$ は *base point* がなくそこから誘導される $X \to \mathbb{P}^N$ が *closed immersion* になることである *(Hartshorne §7, Chapter II.)*

証明 iii) ⇒ iv) は一般論. Serre の ample 性に関するコホモロジカルな判定法により, finite morphism による pull back で ample 性は保たれるから (Hartshorne, ex 5.7, Chapter III.)

iv) ⇒ ii) を示す. 完備代数多様体 X の Zariski 閉集合 $K(\mathscr{L})$ が有限でないとすると, 0 を含む連結成分 Y は positive な次元をもつアーベル多様体になる. このとき $\mathscr{L}$ の Y への制限 $\mathscr{L}_Y$ も ample. $Y \subset K(\mathscr{L})$ よりシーソーの定理から $m^*\mathscr{L}_Y \otimes p_1^*\mathscr{L}_Y^{-1} \otimes p_2^*\mathscr{L}_Y^{-1}$ は trivial であることがわかる. これから $\mathscr{L}_Y \otimes (-1)_Y * \mathscr{L}_Y$ も trivial であることがわかる. しかし $\mathscr{L}_Y$ が ample だからこの Y の trivial bundle も ample. これは次元が 0 でないと起こりえない.

ii) ⇒ i) は自明.

i) ⇒ iii) を示す. base point がないことは $T_x^*D + T_{-x}^*D \in |2D|$ をみることでわかる. なぜなら任意の $u \in X$ に対し, $\mathrm{Supp}D \pm u$ は codimension 1 なので $u \pm x \notin \mathrm{Supp}D$ となる x がとれる. したがって $u \notin T_x^*D + T_{-x}^*D$. これより basis $s_1, \ldots, s_{N+1} \in \Gamma(X, \mathscr{L})$ を $\mathbb{P}^N$ の座標にならべて $f : X \to \mathbb{P}^N$ を作れる. つまり $f^*\mathcal{O}_{\mathbb{P}^N}(1) = \mathscr{L}$ で $f^*z_i = s_i$ となるように作れる. ここで z_i は $\mathbb{P}^N$ の i-座標関数が定める section. f が finite でなかったとしよう. このとき X に含まれる曲線 C で f で一点 $z \in \mathbb{P}^N$ につぶれるものがある. ここで任意の $D' \in |2D|$ に対して, D' は $f(D')$ が z を含むかどうかに応じて $C \subset D'$ または $C \cap D' = \emptyset$ である. 実際, $\Gamma(X, \mathscr{L})$ の basis の取り方で $f : X \to \mathbb{P}^N$ は単に $\mathbb{P}^N$ の自己同型だけ違うだけだから, 最初から D' は section s_1 の zero-divisor としてよい. このとき $x \in D'$ であるための必要十分条件は $f(x)$ の第一成分が 0 である. これから z の第一成分が 0 かどうかに応じて $C \subset D'$ または $C \cap D' = \emptyset$ である. したがってある $x \in X$ に対し, C と $T_x^*D + T_{-x}^*D$ は disjoint である. (上でみたようにこの形の divisor たちは base point をもたないから.) E をこのような $T_x^*D + T_{-x}^*D$ の既約成分とする. i) の条件より $T_xE = E$ となる無限個の x を構成すればよい. X の元で C の 2 つの元の差として表されるものに対してはこれが成り立つことを示す.

任意の x に対し, T_x^*E と E は同じ degree で C に制限しても同じ degree だが, E と C は交わらないので degree 0. ところが $T_x^*E|_C$ は non-negative divisor なので全体か空集合でなけ

ればならない. これから任意の x に対し $T_x^*(C) \subset E$ または $T_x^*C \cap E = \emptyset$ がわかる. ここで $c_1, c_2 \in C, u \in E$ に対し, $u \in T^*_{u-c_2}(C) \cap E$ なので $T^*_{u-c_2}(C) \cap E$ は空ではなく, したがって $T^*_{u-c_2}(C) \subset E$. とくに $u - c_2 + c_1 \in E$. ここで $u \in E$ は任意なので $T^*_{c_1-c_2}E \subset E$. 次元と既約性より $T^*_{c_1-c_2}E = E$. □

Corollary 2.16 アーベル多様体は射影的.

証明 U を X のアフィン開集合とする. X は完備代数多様体なのでよく知られているように補集合 $D = X - U$ は divisor になる. (任意の点 $P \in X - U$ に対し, U で正則で P では定義されないような有理関数 (関数体の元) がとれる. したがってこの関数体の元の極 divisor D は 作り方から $P \in D \subset X - U$. したがって $X - U$ は divisor の合併.) D は ample になることを示す. 平行移動で $0 \in U$ としてよい. もし $T_x^*D = D$ とすると $T_x^*U = U$ で $0 \in U$ だから $x \in U$. したがって完備な $K(\mathscr{L})$ がアフィン開集合 U に含まれることになるので, $K(\mathscr{L})$ は有限集合でなければならない. ゆえに上の命題から ample であることがわかる. □

2.3 Cube の定理の証明

シーソーの定理, Cube の定理の証明に使われるのは, 次の Grothendieck による上半連続定理である.

Theorem 2.17 $f : X \to Y$ を *Noether* スキームの *proper morphism* とする. また $\mathscr{F}$ を X 上の *coherent sheaf* で Y 上 *flat* なものとする. このとき次が成り立つ.
a) 任意の整数 $p \geq 0$ に対し, 次の関数

$$Y \to \mathbb{Z}, \qquad y \mapsto \dim_{k(y)} H^p(X_y, \mathscr{F}_y)$$

は *upper-semicontinuous (*任意の自然数 n に対し $[n, \infty) \cap \mathbb{Z}$ の逆像が閉集合.*)*
b) 関数

$$Y \to \mathbb{Z}, \qquad y \mapsto \chi(\mathscr{F}_y) := \sum_{p=0}^{\infty} (-1)^p \dim_{k(y)} H^p(X_y, \mathscr{F}_y)$$

は Y 上局所定数.
c) もし Y が *reduced* かつ *connected* ならば次の *i), ii)* は同値.
i) $Y \to \mathbb{Z},\ y \mapsto \dim_{k(y)} H^p(X_y, \mathscr{F}_y)$ は定数関数.
ii) $R^p f_* \mathscr{F}$ は Y 上の *locally free sheaf* で, 任意の $y \in Y$ に対し, 自然な写像

$$R^p f_* \mathscr{F} \otimes_{\mathcal{O}_Y} k(y) \longrightarrow H^p(X_y, \mathscr{F}_y)$$

は同型. またもしこの同値な条件がみたされるならば任意の $y \in Y$ に対し, 次も同型

$$R^{p-1} f_* \mathscr{F} \otimes_{\mathcal{O}_Y} k(y) \longrightarrow H^{p-1}(X_y, \mathscr{F}_y).$$

シーソーの定理の証明：一般に完備代数多様体 X とそれ上の line bundle $\mathscr{L}$ が trivial になるための必要十分条件は

$$\dim_k \Gamma(X, \mathscr{L}) \geq 1 \quad \text{かつ} \quad \dim_k \Gamma(X, \mathscr{L}^{-1}) \geq 1.$$

なぜならば上の条件が満たされると, non-zero な $\mathcal{O}_X$-module の homomorphism

$$\rho : \quad \mathcal{O}_X \longrightarrow \mathscr{L} \longrightarrow \mathcal{O}_X$$

がある. ρ による 1 の行き先は $\mathcal{O}_X$ の non-zero section だから X が proper なことより定数 ($\neq 0$). これよりこの写像は (non-zero な) 定数倍. 従って上の 2 つの射は全部同型.

この判定法と上半連続定理より T_1 が閉集合であることがわかる. 最後のパートは T と T_1 を入れ替えて $T = T_1$ とすると (ただし T はもはや代数多様体ではなく単なる k 上 finite な reduced scheme), 任意の $t \in T$ に対し $\mathscr{L}\,|_{X\times\{t\}}$ は trivial で

$$\dim_{k(t)} H^0(X \times \{t\}, \mathscr{L}\,|_{X\times\{t\}}) = 1.$$

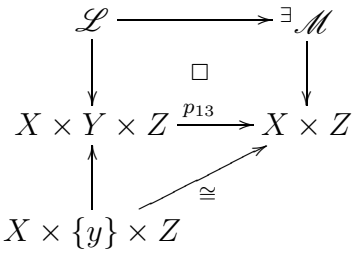
よってやはり上半連続定理より $\mathscr{M} = p_{2*}\mathscr{L}$ は invertible sheaf で

$$\mathscr{M} \otimes_{\mathcal{O}_T} k(t) \to H^0(X \times \{t\}, \mathscr{L}\,|_{X\times\{t\}})$$

は同型. $\mathscr{L}\,|_{X\times\{t\}}$ が trivial であることを使うと自然な射 $\varphi : p_2^*\mathscr{M} \to \mathscr{L}$ は $X \times \{t\}$ 上では trivial sheaf の射 $\mathcal{O}_X \to \mathcal{O}_X$. この射は global section では上の同型を引き起こすので zero ではない. これより任意の $t \in T$ に対し φ は $X \times \{t\}$ 上では同型. これより中山の補題から φ は全射, 従って (invertible sheaf 間の射なので) 同型であることがわかる. □

Cube の定理の証明 :

Lemma 1. シーソーの定理より任意の $x \in X$, $z \in Z$ に対し, $\mathscr{L}$ が $\{x\} \times Y \times \{z\}$ 上で trivial をいえばよい. (シーソーより下図の line bundle $\mathscr{M}$ が存在し, $\mathscr{L}|_{X\times\{y\}\times Z}$ が trivial だから $\mathscr{M}$ も trivial.)



Lemma 2. X は non-singular curve としてよい.
なぜならば x と x_0 を結ぶ X の curve C' をとる. (例えば Chow の補題を使って X が projective な場合に帰着し, Bertini の定理などを使って x, x_0 を通る超平面で X を切断して C' を得る.) $C \to C'$ を normalization とすれば写像

$$\{x\} \times Y \times \{z\} \to C \times Y \times Z \to X \times Y \times Z$$

を得る. Step 1 より $\mathscr{L}|_{C\times Y\times Z}$ が trivial を言えばよいから. ($C\times Y\times Z$ 上で Cube の定理の仮定も満たされている.)

Lemma 3. Z を z_0 を含む空でない開集合 Z' に取り替えてもよい.
シーソーより $\mathscr{L}|_{X\times Y\times\{z\}}$ が trivial なるような z 達は閉集合だから, Z の既約性より開集合 Z' を含めば全体 Z に一致するから.

Key idea. 簡単のため $(y,z)\in Y\times Z$ に対し $\mathscr{L}|_{X\times\{y\}\times\{z\}}$ を $\mathscr{L}_{(y,z)}$ と書く. Cube の定理を証明するためには, $\mathscr{L}_{(y,z_0)}$ の自明性から $\mathscr{L}_{(y,z)}$ の自明性を導けばよい. (このとき Lemma 1 と同じで $\mathscr{L}$ 自身が trivial になる.) 方法は上半連続定理で, とくに c) の ii) の部分から $p=0$ に対し $\mathscr{L}_{(y,z_0)}$ と $\mathscr{L}_{(y,z)}$ を fibre として結びつける $p_{23*}\mathscr{L}$ を使って自明性を導きたい. そのためには $p=0$ に対し c) の i) が成り立つことを示さないといけないが, これを直接示すのは難しい. しかし上半連続定理の b) で Euler 指標の定数性はわかっているので, もし $\mathscr{L}_{(y,z)}$ の 0 次以外のコホモロージが全部消えていれば c) の i) が $p=0$ で成り立つ. $\mathscr{L}_{(y,z)}$ 自身は trivial になると予想されているのでこのような都合のよいことになっていないが, 証明のアイデアは $\mathscr{L}$ の無害な twist を考えることでこの状況にもっていくことである.

Step 1. $\mathscr{L}$ の twist $\mathscr{L}'$.
非特異カーブ X の種数を g とする. つまり $g=\dim H^0(X,\Omega^1)$. このとき X の点 $P_1,\dots,P_g$ で divisor $D=\sum_{i=1}^g P_i$ に対し, $\dim H^0(X,\Omega^1\otimes\mathcal{O}_X(-D))=0$ となるものが取れる. ($H^0(X,\Omega^1)$ の basis $\omega_1,\dots,\omega_g$ に対し, $X^g=X\times\cdots\times X$ で projection p_i に対し, $\begin{vmatrix} p_1^*\omega_1 & \cdots & p_1^*\omega_g \\ \vdots & \vdots & \vdots \\ p_g^*\omega_1 & \cdots & p_g^*\omega_g \end{vmatrix}$ の support として定義される X^g の閉集合の外から $(P_i)\in X^g$ を取ればよい.) $p_1: X\times Y\times Z\to X$ に対し $\mathscr{L}'=\mathscr{L}\otimes p_1^*\mathcal{O}_X(D)$ とおく. このとき $\mathscr{L}'$ は次の性質 **1**, **2** をもつ.
1. z_0 を含むある開集合 Z' で, 任意の $z\in Z'$ に対し $H^i(X,\mathscr{L}'_{(y,z)})=0$ $(i\neq 0)$.
X は非特異曲線なので $i=1$ としてよい. $\mathscr{L}'_{(y,z_0)}=\mathcal{O}_X(D)$ なので $z=z_0$ に対しては,

$$\dim H^1(X,\mathscr{L}'_{(y,z_0)})=\dim H^0(X,\Omega^1\otimes\mathcal{O}_X(-D))=0.$$

したがって集合 $F=\{(y,z)\in Y\times Z\mid \dim H^1(X,\mathscr{L}'_{(y,z)})\geq 1\}$ は z_0 を含まない. 上半連続定理より F は閉集合だから, Y の proper 性とこの F を使って Z の中で $\dim H^i(X,\mathscr{L}'_{(y,z)})\geq 1$ となる z を削って, 求めたい開集合 Z' を見つけることができる.
とくに Lemma 3 から $Z=Z'$ としてよい. このとき
2. 任意の $(y,z)\in Y\times Z$ に対し $\dim H^0(X,\mathscr{L}'_{(y,z)})=1$.
なぜならば性質 **1**, 上半連続定理の b) の Euler 指標の定数性と Riemann-Roch から

$$\dim H^0(X,\mathscr{L}'_{(y,z)})=\chi(\mathscr{L}'_{(y,z)})=\chi(\mathscr{L}'_{(y_0,z_0)})=\chi(\mathcal{O}_X(D))=1-g+\deg D=1.$$

性質 **2** より $p_{23}: X\times Y\times Z\to Y\times Z$ に対し, $\mathscr{L}'$ には上半連続定理の c) の ii) が $p_{23*}\mathscr{L}'$ は invertible sheaf で次は同型.

$$p_{23*}\mathscr{L}'\otimes k(y,z)\ \longrightarrow\ H^0(X,\mathscr{L}'_{(y,z)}).$$

$\mathscr{L}_{(y,z)}$ の自明性を示すということは $\mathscr{L}'_{(y,z)}$ が $\mathcal{O}_X(D)$ と同型であることを示すことである. つまり 1 次元ベクトル空間 $H^0(X, \mathscr{L}'_{(y,z)})$ の非自明 section の zero-divisor が D を示すことである.

Step 2. $X \times Y \times Z$ 上の divisor $\widetilde{D}$ で $\widetilde{D}|_{X\times\{y\}\times\{z\}}$ が $H^0(X, \mathscr{L}'_{(y,z)})$ の非自明 section の zero-divisor になるものの構成.

$Y \times Z$ の open cover (U_i) で U_i 上 invertible sheaf $p_{23*}\mathscr{L}'$ を trivial にするようなものをとる. 生成元

$$\sigma_{U_i} \in \Gamma(U_i, p_{23*}\mathscr{L}') = \Gamma(p_{23}^{-1}U_i, \mathscr{L}')$$

の $p_{23}^{-1}U_i$ 上の zero-divisor を $\widetilde{D}_{U_i}$ とする. σ_{U_i} と σ_{U_j} は $U_i \cap U_j$ 上どこでも消えない正則関数倍しか違わないから, $\widetilde{D}_{U_i}$ は U_i ごと張り合って $X \times Y \times Z$ 上の divisor $\widetilde{D}$ を作る. 作り方から $\widetilde{D}$ の $X \times \{y\} \times \{z\}$ への制限は $H^0(X, \mathscr{L}'_{(y,z)})$ の非自明 section の zero-divisor に等しい. とくに $\widetilde{D}$ の $X \times \{y_0\} \times \{z\}$, $X \times \{y\} \times \{z_0\}$ への制限は D.

Step 2 より次を示せば Cube の定理の証明は完成する.

Final Step. $\widetilde{D} = \sum_{i=1}^{g} \{P_i\} \times Y \times Z$.

ある自然数に対し $\widetilde{D} = \sum_{i=1}^{g} n_i\{P_i\} \times Y \times Z$ を示せば, $X \times \{y_0\} \times \{z_0\}$ への制限より $n_i = 1$ がわかるので, $\operatorname{Supp} \widetilde{D} = \cup_i \{P_i\} \times Y \times Z$ を示せば十分. そのためには任意の $P \neq P_i$ $(i = 1, \ldots, g)$ に対し

$$S = \operatorname{Supp} \widetilde{D} \cap (\{P\} \times Y \times Z) = \emptyset$$

を示せば, $\operatorname{Supp} \widetilde{D} \subset \cup_i \{P_i\} \times Y \times Z$ で両方とも pure codimiension 1 で $X \times \{y_0\} \times \{z_0\}$ への制限を考えれば一致することがわかる. S が空集合であることは次のようにしてわかる. S の projection $\{P\} \times Y \times Z \to Z$ による像は Z 全体にならない (z_0 は像に入らない.)

したがってある Z の codimension 1 の閉集合 $T_i (i = 1, \ldots, m)$ で $S \subset \cup_{i=1}^{m} \{P_i\} \times Y \times T_i$ となるものがある. S が空集合でないとすると両方とも pure codimiension 1 であるから $S = \cup_{i=1}^{n} \{P_i\} \times Y \times T_i$ の形. しかし $S \cap (\{P\} \times \{y_0\} \times Z) = \emptyset$ だから矛盾する. □

Remark 2.18 実は非特異曲線の *Jacobi* 多様体の存在を認めると *Cube* の定理は簡単に示せる. X が非特異曲線の場合に帰着させるまでは同じで, このとき X の *Jacobi* 多様体を J とおく. 示したいのは $\mathscr{L}_{(y,z)}$ の自明性だが, $(y, z) \in Y \times Z$ に対し, $\mathscr{L}_{(y,z)}$ を対応させて, *morphism* $f : Y \times Z \to J$ を得る. ($y = y_0$ または $z = z_0$ のとき $\mathscr{L}_{(y,z)}$ は自明で, 特に *degree* は 0. したがって一般の (y, z) に対しても $\mathscr{L}_{(y,z)}$ の *degree* は 0 で, 集合論的に射 f が定まる. この集合論的射が代数多様体の *morphism* になるのは *Jacobi* 多様体の重要な性質で自明ではない. *Cube* の定理より難しい?) $f(\{y_0\} \times Z) = 0$ なので *Rigidity* の補題と z_0 での自明性より, f は 0 写像であることがわかる. したがって $\mathscr{L}_{(y,z)}$ は *trivial.*

3 双対アーベル多様体

アーベル多様体 X の双対アーベル多様体とは大雑把にいうと (閉点の集合が) 抽象群として $\mathrm{Pic}^0(X)$ に同型なアーベル多様体である. “大雑把に”というのは, これだけでは特徴づけにならないからである. $\mathrm{Pic}^0(X)$ に代数多様体としての構造が複数入るかもしれないし, 我々は同型を除いて unique に定めたい. とくに標数が正のときは purely inseparable な isogeny があるので閉点の構造だけでは同型を除いて unique に定めることができない. ここで登場するのが Poincaré bundle で, この bundle と組にすることで, 双対アーベル多様体は同型を除いて unique に定まる.

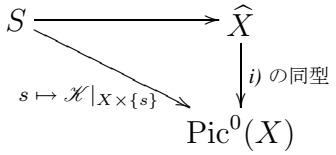
3.1 双対アーベル多様体の定義と性質

Definition 3.1 X をアーベル多様体とする. 次の性質をもつアーベル多様体 $\widehat{X}$ と $X \times \widehat{X}$ 上の *line bundle* $\mathscr{P}$ の組 $(\widehat{X}, \mathscr{P})$ を考える.

i). 任意の $\alpha \in \widehat{X}$ に対し, $\mathscr{P}$ の埋め込み $X \times \{\alpha\} \to X \times \widehat{X}$ による *pull-back* は $\mathrm{Pic}^0(X)$ の元で, 抽象群としての同型 $\widehat{X} \cong \mathrm{Pic}^0(X)$ を引き起こす.

ii). (Rigidity) $\mathscr{P}|_{\{0\}\times\widehat{X}}$ は *trivial.*

iii). (Universality) 任意の *normal* な代数多様体 S, と $X \times S$ 上の *line bundle* $\mathscr{K}$ で次の性質 *1. 2.* をもつものを考える.
1. ある閉点 $s \in S$ に対し *(*従って結果として任意の閉点 $s \in S$ に対し*)*, $\mathscr{K}|_{X\times\{s\}} \in \mathrm{Pic}^0(X)$.
2. $\mathscr{K}|_{\{0\}\times S}$ は *trivial.*
このとき代数多様体の *morphism* $f : S \to \widehat{X}$ で集合の圏での図式



を可換にし, $\mathscr{K} \cong (1_X \times f)^*\mathscr{P}$ となるものがただ一つ存在する.

i), ii) の性質とシーソの定理からこのような組 $(\widehat{X}, \mathscr{P})$ は存在すれば同型を除いてただひとつであることがわかる. $\widehat{X}$ を X の双対アーベル多様体, $\mathscr{P}$ を *Poincaré bundle* という.

Remark 3.2 X が楕円曲線 E のときは, E 自身が双対アーベル多様体で *Poincaré bundle* は $E \times E$ の *divisor* $\Delta - (E \times \{0\}) - (\{0\} \times E)$ に対応する *line bundle* である. ここで Δ は足し算 $m : X \times X \to X, (x, y) \mapsto x + y$ の核. とくに *Weierstrass* σ-関数に対し,

$$\frac{\sigma(z+w)}{\sigma(z)\sigma(w)}$$

は E の *Poincaré bundle* の *section.* この関数は本質的に *CM* 楕円曲線の 2 変数 p- 進 L 関数の母関数になることが知られている *(cf. [BK]).*

3.2 双対アーベル多様体の構成のアイデア

$\mathscr{L}$ を ample line bundle とする. このとき今まで見てきたように,

$$\phi_{\mathscr{L}} : X \to \mathrm{Pic}^0(X)$$

の核は有限群 $K(\mathscr{L})$ であった. もし $\mathrm{Pic}^0(X)$ にアーベル多様体の構造が入り, $\phi_{\mathscr{L}}$ が scheme の射になるなら, 核の有限性より $\phi_{\mathscr{L}}$ は isogeny であり, 全射であることがわかる. したがって $\phi_{\mathscr{L}}$ の "**スキームとしての核**"を $\widetilde{K}(\mathscr{L})$ とすると $\mathrm{Pic}^0(X)$ は抽象群として X の有限群スキーム $\widetilde{K}(\mathscr{L})$ による商と同型でなければならない. ここで $\widetilde{K}(\mathscr{L})$ と $K(\mathscr{L})$ には $\widetilde{K}(\mathscr{L})$ を被約化したものが $K(\mathscr{L})$ という関係があるはずである. (位相空間としては同型だが, のっている関数環が無限小レベルで違う.) 双対アーベル多様体はこれを逆手にとって次のように構成する.

i). $\phi_{\mathscr{L}} : X \to \mathrm{Pic}^0(X)$ の全射性を証明する.

ii). 有限群 $K(\mathscr{L})$ に適切な有限群スキームとしての構造を入れ, 商多様体 $X/K(\mathscr{L})$ を構成する.

iii). これが Poincaré bundle による双対アーベル多様体の特徴付けをみたすことを示す.

ii) についてだが, もし基礎体 k の標数が 0 ならば, すべての isogeny は separable で, 核はétale な有限群スキームになる. つまりスキームの構造は忘れて単なる有限群と思ってよい (trivial なスキーム構造). とくに $\widetilde{K}(\mathscr{L}) = K(\mathscr{L})$ であり, 欲しい商多様体は X を普通の有限群 $K(\mathscr{L})$ で割ればよいので, ii) の部分は簡単になる.

Mumford の 2 章では "有限群"による商多様体の一般論を展開し, 双対アーベル多様体を標数 0 の場合に構成している. 3 章では, シーソーの定理をスキーム論的に一般化し (無限小の厚みをつける), 単なる集合ではなく $K(\mathscr{L})$ を scheme として構成する. そして今度は" 有限群スキーム"による商多様体の一般論を展開し, 双対アーベル多様体を任意の標数で構成する. 2 章も 3 章も方法論的にまったく同じで, 2 章の内容は 3 章の内容に完全に含まれてしまうが, アイデアを理解するためには 2 章だけで十分で, 証明も簡略化される (それが Mumford が 2 章を挿入した理由であろう.) この講演でも 2 章の内容のみを紹介してきた. 3 章を説明するためには, シーソーの定理, Cube の定理を代数多様体だけでなく, さらにスキーム論的に無限小の厚みをつける必要がある.

3.3 $\phi_{\mathscr{L}}$ の全射性

アーベル多様体 X に対し, 次が命題が成り立つことはシーソーの定理や Cube の定理からただちにわかる.

Proposition 3.3 *i).* $\mathscr{L} \in \mathrm{Pic}^0(X) \iff m^*\mathscr{L} \cong p_1^*\mathscr{L} \otimes p_2^*\mathscr{L}$ *on* $X \times X$.

ii). 任意のスキーム S と $f, g : S \to X$ と $\mathscr{L} \in \mathrm{Pic}^0(X)$ に対し, $(f+g)^*\mathscr{L} \cong f^*\mathscr{L} \otimes g^*\mathscr{L}$. とくに $n_X^*\mathscr{L} \cong \mathscr{L}^n$.

iii). S を任意の代数多様体. $s_1, s_2 \in S$ とする. このとき $X \times S$ 上の任意の *line bundle* $\mathscr{L}$ に対し,

$$\mathscr{L}_{s_1} \otimes \mathscr{L}_{s_2}^{-1} \in \mathrm{Pic}^0(X).$$

ここで $\mathscr{L}_s = \mathscr{L}|_{X\times\{s\}}$. つまり一つの *fibre* で $\mathrm{Pic}^0(X)$ の元ならほかの *fibre* でもそうである.

Proposition 3.4 $\mathscr{L} \in \mathrm{Pic}^0(X)$ に対し, もし $\mathscr{L}$ が *non-trivial* ならば, 任意の i に対し $H^i(X, \mathscr{L}) = 0$.

証明 $H^0(X, \mathscr{L})$ がゼロでなかったとすると non-trivial な global section の divisor D を考えると D は non-negative で $\mathscr{L} = \mathcal{O}_X(D)$. ここで

$$\mathcal{O}_X \cong \mathscr{L} \otimes \mathscr{L}^{-1} \cong \mathscr{L} \otimes (-1)^*\mathscr{L}$$

だから non-negative divisor $D + (-1)_X^* D$ が 0 に linealy equivalent になるので $D = 0$. $\mathscr{L}$ が non-trivial に矛盾. 写像 $s_1 : X \to X \times X, x \mapsto (x, 0)$ を考えると $m \circ s_1$ は恒等写像で,

$$H^i(X, \mathscr{L}) \xleftarrow{s_1^*} H^i(X \times X, m^*\mathscr{L}) \xleftarrow{m^*} H^i(X, \mathscr{L})$$

も恒等写像. ところが $m^*\mathscr{L} \cong p_1^*\mathscr{L} \otimes p_2^*\mathscr{L}$(前命題) より Künneth formula を使うと

$$H^i(X \times X, m^*\mathscr{L}) \cong H^i(X \times X, p_1^*\mathscr{L} \otimes p_2^*\mathscr{L}) \cong \sum_{k+l=i} H^k(X, \mathscr{L}) \otimes H^l(X, \mathscr{L}).$$

帰納法を使えばこの群は 0 としてよい. よって恒等写像がゼロ写像を引き起こすことになり $H^i(X, \mathscr{L}) = 0$. □

Theorem 3.5 $\mathscr{L}$ をアーベル多様体 X の *ample* な *line bundle* とする. このとき任意の $\mathscr{M} \in \mathrm{Pic}^0(X)$ に対して, ある $x \in X$ があって

$$\mathscr{M} \cong T_x^*\mathscr{L} \otimes \mathscr{L}^{-1}$$

とかける. つまり $\phi_{\mathscr{L}}$ は全射.

証明 アイデアは $X \times X$ 上の line bundle

$$\mathscr{K} = m^*\mathscr{L} \otimes p_1^*\mathscr{L}^{-1} \otimes p_2^*\mathscr{L}^{-1} \otimes p_2^*\mathscr{M}^{-1}$$

のコホモロジーをみることである. 定義から任意の $x \in X$ に対し,

$$\mathscr{K}|_{\{x\}\times X} \cong T_x^*\mathscr{L} \otimes \mathscr{L}^{-1} \otimes \mathscr{M}^{-1}, \quad \mathscr{K}|_{X\times\{x\}} \cong T_x^*\mathscr{L} \otimes \mathscr{L}^{-1}.$$

このとき 2 つの projection $X \times X \to X$ に関する Leray スペクトル系列

$$H^l(X, R^k p_{1*}\mathscr{K}) \;\Rightarrow\; H^{k+l}(X \times X, \mathscr{K}),$$

$$H^l(X, R^k p_{2*}\mathscr{K}) \;\Rightarrow\; H^{k+l}(X \times X, \mathscr{K})$$

を考える. もしこの定理の主張が正しくないとすると $\mathscr{K}|_{\{x\}\times X}$ は常に non-trivial になる. したがって前命題より $\mathscr{K}|_{\{x\}\times X}$ のすべてのコホモロジーは消える. よって上半連続定理より $R^k p_{1*}\mathscr{K}$ の fibre はすべて trivial で, $R^k p_{1*}\mathscr{K}$ 自身が trivial になる. これより最初のスペクトル系列からすべての k に対し $H^k(X \times X, \mathscr{K}) = 0$. つぎに同様の議論で

$$\mathrm{Supp}(R^k p_{2*}(\mathscr{K})) \subset K(\mathscr{L})$$

がわかる. $K(\mathscr{L})$ は有限集合だから 2 番目のスペクトル系列から

$$\oplus_{x\in K(\mathscr{L})}\, R^k p_{2*}(\mathscr{K})_x \subset H^k(X \times X, \mathscr{K}) = 0.$$

これから全て x に対し, $H^k(X, \mathscr{K}|_{X\times\{x\}}) = 0$. しかし $\mathscr{K}|_{X\times\{0\}}$ は trivial だから non-trivial な global section をもつので矛盾. □

3.4 双対アーベル多様体の構成

$\phi_{\mathscr{L}}$ は全射であることがわかったので, ample line bundle $\mathscr{L}$ に対し, X の有限群による $K(\mathscr{L})$, $X/K(\mathscr{L})$ は抽象群として $\mathrm{Pic}^0(X)$ と同型になることがわかった. したがって $\mathrm{Pic}^0(X)$ にアーベル多様体としての構造をいれることができた. しかし双対アーベル多様体の構成のアイデアでのべたように, 一般にはこれが双対アーベル多様体 $\widehat{X}$ であるとは期待できない. もし基礎体の標数が 0 ならばそうであると期待できるのであった. 以下では基礎体の標数は 0 として, Poincaré bundle の構成と $X/K(\mathscr{L})$ が双対アーベル多様体になることをみる.

3.4.1 Poincaré bundle の構成

$\widehat{X} = X/K(\mathscr{L})$ とおき, 自然な projection $X \to \widehat{X}$ を π とおく. このとき容易にわかるように Poincaré bundle $\mathscr{P}$ が存在するならば, $\mathscr{P}$ の

$$X \times X \xrightarrow{1\times\pi} X \times \widehat{X}$$

による pull-back は

$$\mathscr{M} := m^*\mathscr{L} \otimes p_1^*\mathscr{L}^{-1} \otimes p_2^*\mathscr{L}^{-1}$$

でなければならない. これより $X \times X$ への有限群 $\{0\} \times K(\mathscr{L})$ の作用を $\mathscr{M}$ に自然にのばして商 $\mathscr{M}/\{0\} \times K(\mathscr{L})$ を $\mathscr{P}$ とおけばよいことがわかる.

一般に有限群 G の X への作用を X 上の line bundle に自然にのばすことはできないが (たとえば G がいわゆる Mumford の theta 群だったら ample symmetric line bundle に作用をのばすことができるというのが Mumford の theta 理論の核心で, まったく自明でない), しかしながら この $\mathscr{M}$ には次のようにして $\{0\} \times K(\mathscr{L})$ の作用をのばせる. 作用をのばすためには任意の $a \in K(\mathscr{L})$ に対し, canonical に同型 $T^*_{(0,a)}\mathscr{M} \cong \mathscr{M}$ を与えてあげればよい. (いい加減にあたえると作用の結合性などが成り立たなくなる.) $a \in K(\mathscr{L})$ より同型 $T_a^*\mathscr{L} \cong \mathscr{L}$

が存在するので, このような同型 f_a をひとつとって固定する. f_a の取り方には定数倍の曖昧さがあることに注意しておく. そして同型

$$T^*_{(0,a)}\mathscr{M} \cong m^*T^*_a\mathscr{L} \otimes p_1^*\mathscr{L}^{-1} \otimes p_2^*T^*_a\mathscr{L}^{-1} \cong m^*\mathscr{L} \otimes p_1^*\mathscr{L}^{-1} \otimes p_2^*\mathscr{L}^{-1} = \mathscr{M}$$

を考える. ここで最初の同型は canonical で 2 番目は $f_a \otimes \mathrm{id} \otimes f_a^{\otimes -1}$ である. f_a は constant 倍の自由度があるが, この同型は f_a と $f_a^{\otimes -1}$ が constant 倍の曖昧さを打ち消し合って f_a の取り方に依存しなく canonical である. この canonical 同型 $T^*_{(0,a)}\mathscr{M} \cong \mathscr{M}$ を使って $\{0\} \times K(\mathscr{L})$ の $\mathscr{M}$ への作用が定まる.

さて基礎体の標数が 0 のときはこのようにしてできた組 $(\widehat{X}, \mathscr{P})$ が実際に双対アーベル多様体を特徴づける性質をもつことを示そう. 特徴付けの性質のうち, iii) の Universality のみが非自明である. 実際正標数のときはこれが成り立つとは限らず, この組は双対アーベル多様体を定めない. しかし標数 0 という仮定をつけるとこれが成り立つ. 特徴付けの ii) と同じ記号を使う.

アイデアは欲しい $f : S \to \widehat{X}$ のグラフ $\Gamma = \{(x, f(x) | x \in S\} \subset S \times \widehat{X}$ に注目することである.

$$\begin{array}{ccc} & \Gamma \subset S \times \widehat{X} & \\ {\scriptstyle p_1}\swarrow & & \searrow{\scriptstyle p_2} \\ S & & \widehat{X} \end{array}$$

もし欲しい f があったとすると (集合論の圏ではあるので), Γ の見当はつき, 幾何的に構成できる. つまり $X \times S \times \widehat{X}$ 上の line bundle $\mathscr{E} = p_{12}^*(\mathscr{K}) \otimes p_{13}^*(\mathscr{P}^{-1})$ に対して

$$\Gamma := \{(s, \alpha) \in S \times X \mid \mathscr{E}\,|_{X \times \{(s,\alpha)\}} \text{は trivial } \}$$

とおけばシーソの定理よりこれは Zariski 閉集合で, 集合論的には存在する f のグラフになっていることがわかる. よってスキームの間の射である p_1 は集合論的に Γ と S に bijection を引き起こす. ここで標数が 0 を使うと, これは Γ と S の (代数多様体の射としての) birational equivalence であることがわかる. (標数が 0 を使うのはここのみ!) ここで S は normal だから Zariski の主定理より, p_1 は Γ と S の代数多様体としての同型を引き起こすことがわかる. よってこの逆写像を p_1^{-1} とすれば欲しい f を $p_2 \circ p_1^{-1}$ として得る. ほかの主張はシーソの定理をつかって容易に証明できる.

標数が p のときは, $K(\mathscr{L})$ に適切なスキーム構造を入れた後, 同様に双対多様体を定義し, Universality も上と同様にグラフ Γ を考えてまったく同様な方針で証明される. しかし p_1 が Γ 上で同型であることを示すのはテクニカルにずっと困難になる. Mumford の本ではその過程で次の重要な事実も証明される.

Proposition 3.6

$$H^i(X \times \widehat{X}, \mathscr{P}) = \begin{cases} 0 & (i \neq g), \\ 1 \text{ 次元ベクトル空間 } k & (i = g). \end{cases}$$

4 Riemann-Rochの定理と直線束のコホモロジー

Theorem 4.1 (Riemann-Roch) $\mathscr{L}$ をアーベル多様体 X の *line bundle* $\mathcal{O}_X(D)$ とする. このとき

$$\chi(\mathscr{L}) = \frac{(D^g)}{g!}, \quad \chi(\mathscr{L})^2 = \deg \phi_{\mathscr{L}}.$$

ここで (D^g) は g 個の D の *self-intersection number.*

証明 まず $\mathscr{L}_1 \otimes \mathscr{L}_2^{-1} \in \mathrm{Pic}^0(X)$ ならば, $\chi(\mathscr{L}_1) = \chi(\mathscr{L}_2)$ である. これは $\mathrm{Pic}^0(X)$ は $\mathscr{P}$ によりパラメータづけられ, 上半連続定理よりオイラー指標は fibre で constant であることからわかる. したがってオイラー指標の計算は modulo $\mathrm{Pic}^0(X)$ ですればよい. 任意の line bundle は symmetric な bundle と $\mathrm{Pic}^0(X)$ の元の積としてかけるので, $\mathscr{L}$ は symmetric としてよい. このとき Corollary 2.7 より任意の整数 n に対し, $n_X^*\mathscr{L} = \mathscr{L}^{n^2}$ で,

$$\chi(\mathscr{L}^{n^2k}) = \chi(n_X^*\mathscr{L}^k) = \deg n_X \cdot \chi(\mathscr{L}^k) = n^{2g}\chi(\mathscr{L}^k).$$

いま $\chi(\mathscr{L}^k)$ は k に関する多項式 (Hilbert polynomial) なので,

$$\chi(\mathscr{L}^k) = \text{constant} \times k^g$$

の形でなければならない. よって $\chi(\mathscr{L}^k) = a(\mathscr{L}) \cdot k^g/g!$ とおいて, $a(\mathscr{L}) = (D^g)$ を示せばよい. 任意の line bundle は適当な very ample line bundle (section たちをならべてできる射影空間への写像が閉埋め込みを定義するような bundle) $\mathscr{L}_1, \mathscr{L}_2$ を使って $\mathscr{L} = \mathscr{L}_1 \otimes \mathscr{L}_2^{-1}$ と書ける. ここである多項式 $P(x, y)$ があって $P(n_1, n_2) = \chi(\mathscr{L}_1^{n_1} \otimes \mathscr{L}_2^{n_2})$ とかけることと, intersection number の線形性を使うと, ちょっとした議論により, 結局 very ample な $\mathscr{L}$ について証明すればよいことがわかる. このときは $\mathscr{L}$ の global section $\sigma_0, \ldots, \sigma_g$ を使って morphism $\phi : X \to \mathbb{P}^g$ を作ることができる. その際, $\sigma_1, \ldots, \sigma_g$ を適当に取り替えてそれらの zero-divisor が transversal に交わるようにできる. したがってこれらの divisor の交わりは異なる (D^g) 個の点である. とくに点 $(1 : 0 : \cdots : 0) \in \mathbb{P}^g$ の ϕ による逆像は (D^g) 個の点であり, $\deg \phi = (D^g)$ である. 一方

$$a(\mathscr{L}) \cdot \frac{k^g}{g!} = \chi(\mathscr{L}^k) = \chi(\phi^*\mathcal{O}_{\mathbb{P}^g}(k)) = \deg \phi \cdot \chi(\mathcal{O}_{\mathbb{P}^g}(k)) = \deg \phi \cdot \frac{k^g}{g!}.$$

□

Proposition 4.2 $\mathscr{L}$ をアーベル多様体 X の *ample line bundle* とする. このときある非負整数 i_0 があって, $i \neq i_0$ ならば $H^i(X, \mathscr{L}) = 0$. また $H^{i_0}(X, \mathscr{L}) \neq 0$.

証明 Proposition 3.6 では $\mathscr{P}$ のコホモロジーを計算したが, そこから標準的な議論で $m^*\mathscr{L} \otimes p_1^*\mathscr{L}^{-1} \otimes p_2^*\mathscr{L}^{-1}$ のコホモロジー (second projection による higher direct image) を計算できる. これから

$$\dim H^i(X \times \widehat{X}, m^*\mathscr{L} \otimes p_1^*\mathscr{L}^{-1}) = \begin{cases} 0 & (i \neq g), \\ \deg \phi_{\mathscr{L}} & (i = g). \end{cases}$$

$h^i(\mathscr{L}) = H^i(X, \mathscr{L})$ とおくと, Künneth formula より

$$\sum_{i=0}^{q} h^i(\mathscr{L}) h^{q-i}(\mathscr{L}^{-1}) = \begin{cases} 0 & (q \neq g), \\ \deg \phi_{\mathscr{L}} & (q = g). \end{cases}$$

主張はこのことから従う. □

Corollary 4.3 *J を non-singular curve C の Jacobian. Θ を C の theta divisor とする. このとき*

$$\dim \Gamma(J, \mathcal{O}_J(n\Theta)) = n^g.$$

証明 divisor $n\Theta$ は effective なので global section をもつ. よって前定理よりコホモロジーは H^0 のみ zero でない. したがって Riemann-Roch より H^0 の次元は (Θ^g) を計算すればわかる. しかし $(\Theta^g) = g!$ であることが知られている. □

参考文献

[BK] K. Bannai and S. Kobayashi, p-adic interpretation of Eisenstein-Kronecker numbers and algebraic theta functions, preprint.

[Bar] I. Barsotti, Considerazioni sulle funzioni theta, In: *Symposia Mathematica*, Vol. III (INDAM, Rome, 1968/69), pp. 247–277, Academic Press, London, 1970.

[Br] L. Breen, Fonctions thêta et théorème du cube. Lecture Notes in Mathematics, 980. Springer-Verlag, Berlin, 1983. xiii+115 pp.

[CC] M. Candilera, V. Cristante, Bi-extensions associated to divisors on abelian varieties and theta functions. Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **10** (1983), no. 3, 437–491.

[Cri1] V. Cristante, Theta functions and Barsotti-Tate groups. Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **7** (1980), no. 2, 181–215.

[Cri2] V. Cristante, p-adic theta series with integral coefficients. p-adic cohomology, Astérisque No. **119-120** (1984), 6, 169–182.

[GM] G. van der Geer, B. Moonen, Lecture note, Abelian varieties. http://staff.science.uva.nl/ bmoonen/boek/BookAV.html

[L] S. Lang, Abelian varieties. Interscience Tracts in Pure and Applied Mathematics. No. 7 Interscience Publishers, Inc., New York; Interscience Publishers Ltd., London 1959 xii+256 pp.

[MT] B. Mazur and J. Tate, The p-adic sigma function, Duke. Math. **62**, No. 3, (1991), 663-688.

[Mil1] J. Milne, Abelian varieties. In Arithmetic geometry (Storrs, Conn., 1984), 103–150, Springer, New York, 1986.

[Mil2] J. Milne, Lecture note, Abelian varieties.
http://www.jmilne.org/math/CourseNotes/math731.html

[Mum] D. Mumford, Abelian varieties. Tata Institute of Fundamental Research Studies in Mathematics, No. 5 Published for the Tata Institute of Fundamental Research, Bombay; Oxford University Press, London 1970 viii+242 pp.

[Pol] A. Polishchuk, *Abelian varieties, theta functions and the Fourier transform*, Cambridge Tracts in Mathematics **153**, Cambridge University Press, Cambridge, 2003.

第 15 回 整数論サマースクール 報告集, pp.265-290

超楕円曲線のヤコビ多様体の形式群

西来路文朗*

0 序文

本稿では第 1 節において, 形式群の本田理論と $\mathbb{Q}$ 上の楕円曲線の形式群への応用について述べる. また, 第 2 節においては, Freije の結果と筆者の結果を中心に, ヤコビ多様体の形式群に関する結果について述べる.

1 形式群の本田理論とその応用

形式的べき級数の諸性質や形式群の定義を振り返った後, 標数 0 の体上の形式群が加法群に同型であることを示す. そして, $\mathfrak{p}$ 進整数環上の形式群の本田 [8] による分類理論についてまとめる. 具体例を与えた後, 楕円曲線の形式群に関する本田の定理を紹介する.

1.1 形式的べき級数

R を可換環とする. n を自然数, $x_1, \ldots, x_n$ を変数とし, $\boldsymbol{x}$ を列ベクトル ${}^t(x_1, \ldots, x_n)$ とおく. 自然数 m に対し, $\boldsymbol{x}^m := {}^t(x_1^m, \ldots, x_n^m)$ とおく. n 変数形式的べき級数環を $R[[\boldsymbol{x}]]$ とあらわす. また, $R[[\boldsymbol{x}]]$ の元を成分とする m 次列ベクトル ${}^t(\varphi_1(\boldsymbol{x}), \ldots, \varphi_m(\boldsymbol{x}))$ 全体を $R[[\boldsymbol{x}]]^m$ とあらわす.

$R[[\boldsymbol{x}]]^m$ の 2 元 $\varphi(\boldsymbol{x})$, $\psi(\boldsymbol{x})$ が**次数 d で合同**とは, $\varphi(\boldsymbol{x}) - \psi(\boldsymbol{x})$ の各成分 $\varphi_j(\boldsymbol{x}) - \psi_j(\boldsymbol{x})$ が全次数 $d-1$ 以下の項を含まないことをいい,

$$\varphi(\boldsymbol{x}) \equiv \psi(\boldsymbol{x}) \mod \deg d$$

とあらわす. 関係 mod deg d は同値関係である.

$R[[\boldsymbol{x}]]$ において, mod deg 1 で 0 に合同な元全体を $R[[\boldsymbol{x}]]_0$ とあらわす.

$$R[[\boldsymbol{x}]]_0 = \{\varphi(\boldsymbol{x}) \in R[[\boldsymbol{x}]] \mid \varphi(0) = 0\}$$

が成り立つ. $\boldsymbol{y} = {}^t(y_1, \ldots, y_n)$ とする. $R[[\boldsymbol{y}]]^n$ の元 $\psi(\boldsymbol{y})$ と $R[[\boldsymbol{x}]]_0^n$ の元 $\varphi(\boldsymbol{x})$ に対し, y_i に $\varphi_i(\boldsymbol{x})$ を代入することができ, **合成** $(\psi \circ \varphi)(\boldsymbol{x})$ が定義できる.

*広島国際大学, Email : sairaiji@it.hirokoku-u.ac.jp

$R[[\boldsymbol{x}]]_0^n$ の元 $\varphi(\boldsymbol{x})$ に対し,

$$(\varphi \circ \psi)(\boldsymbol{x}) = (\psi \circ \varphi)(\boldsymbol{x}) = \boldsymbol{x}$$

を満たす $R[[\boldsymbol{x}]]_0^n$ の元 $\psi(\boldsymbol{x})$ が存在するとき, $\varphi(\boldsymbol{x})$ は**可逆**であるという. このとき, $\psi(\boldsymbol{x})$ は一意的に定まる. $\psi(\boldsymbol{x})$ を $\varphi^{-1}(\boldsymbol{x})$ とあらわす.

命題 1.1 (形式的陰関数定理 cf.eg. [1] IV35). $\boldsymbol{x} = {}^t(x_1, \ldots, x_m)$, $\boldsymbol{y} = {}^t(y_1, \ldots, y_n)$ とし, $F(\boldsymbol{x}, \boldsymbol{y}) = {}^t(F_1(\boldsymbol{x}, \boldsymbol{y}), \ldots, F_n(\boldsymbol{x}, \boldsymbol{y}))$ を $R[[\boldsymbol{x}, \boldsymbol{y}]]_0^n$ の元とする.

$$\left[\frac{\partial F_i}{\partial y_j}(0,0)\right]_{\substack{1 \le i \le n \\ 1 \le j \le n}} \in \mathrm{GL}_n(R)$$

ならば, $R[[\boldsymbol{x}]]_0^n$ の元 $\varphi(\boldsymbol{x})$ がただひとつ存在し,

$$F(\boldsymbol{x}, \varphi(\boldsymbol{x})) = 0$$

を満たす.

命題 1.2 (形式的逆関数定理). $\boldsymbol{x} = {}^t(x_1, \ldots, x_n)$ とする. $R[[\boldsymbol{x}]]_0^n$ の元 $\varphi(\boldsymbol{x})$ が可逆であるための必要十分条件は,

$$\varphi(\boldsymbol{x}) \equiv P\boldsymbol{x} \bmod \deg 2$$

を満たす $\mathrm{GL}_n(R)$ の行列 P が存在することである.

証明 必要条件であることは明らか. 十分条件であることを示す. $\boldsymbol{y} = {}^t(y_1, \ldots, y_n)$ とし, $F(\boldsymbol{x}, \boldsymbol{y}) := \boldsymbol{x} - \varphi(\boldsymbol{y})$ とおく. $F(0,0) = 0$ だから, $F(\boldsymbol{x}, \boldsymbol{y}) \in R[[\boldsymbol{x}, \boldsymbol{y}]]_0^n$ であり, また,

$$\left[\frac{\partial F_i}{\partial y_j}(0,0)\right]_{\substack{1 \le i \le n \\ 1 \le j \le n}} = -P \in \mathrm{GL}_n(R)$$

が成り立つので, 形式的陰関数定理より, $R[[\boldsymbol{x}]]_0^n$ の元 $\psi(\boldsymbol{x})$ が存在し,

$$F(\boldsymbol{x}, \psi(\boldsymbol{x})) = \boldsymbol{x} - \varphi(\psi(\boldsymbol{x})) = 0$$

が従う. したがって, $\varphi(\boldsymbol{x})$ は可逆である. □

1.2 形式群

定義 1.3 (形式群). $\boldsymbol{x} := {}^t(x_1, \ldots, x_g)$, $\boldsymbol{y} := {}^t(y_1, \ldots, y_g)$ とする. $R[[\boldsymbol{x}, \boldsymbol{y}]]_0^g$ の元 $F(\boldsymbol{x}, \boldsymbol{y})$ が R 上定義された (g 次元可換) **形式群**とは, 以下の 3 条件を満たすことをいう.

(1) $F(\boldsymbol{x}, \boldsymbol{y}) \equiv \boldsymbol{x} + \boldsymbol{y} \bmod \deg 2$,

(2) $F(F(\boldsymbol{x}, \boldsymbol{y}), \boldsymbol{z}) = F(\boldsymbol{x}, F(\boldsymbol{y}, \boldsymbol{z}))$,

(3) $F(\boldsymbol{x},\boldsymbol{y}) = F(\boldsymbol{y},\boldsymbol{x})$.

命題 1.4. $F(\boldsymbol{x},\boldsymbol{y})$ を $R[[\boldsymbol{x},\boldsymbol{y}]]_0^g$ の元とする. 定義 1.3 の条件 (2) の仮定のもと, 定義 1.3 の条件 (1) は,

(1)′ $F(\boldsymbol{x},0) = \boldsymbol{x}, \qquad F(0,\boldsymbol{y}) = \boldsymbol{y}$

と同値である.

証明 (1)′ ⇒ (1) は明らか. (1) ⇒ (1)′ を示す. 条件 (2) において, $\boldsymbol{y} = \boldsymbol{z} = 0$ として,

$$F(F(\boldsymbol{x},0),0) = F(\boldsymbol{x},F(0,0)) = F(\boldsymbol{x},0) \tag{1.1}$$

が成り立つ. $\varphi(\boldsymbol{x}) := F(\boldsymbol{x},0)$ とおくと, $\varphi(\boldsymbol{x}) \in R[[\boldsymbol{x}]]_0^g$ であり, 条件 (1) より,

$$\left[\frac{\partial\varphi_i}{\partial x_j}(0)\right]_{\substack{1\le i\le n\\ 1\le j\le n}} = I_g \in \mathrm{GL}_g(R)$$

が成り立つ. ただし, I_g は g 次単位行列とする. したがって, $F(\boldsymbol{x},0)$ は可逆であり, (1.1) 式より,

$$F(\boldsymbol{x},0) = \boldsymbol{x}$$

を得る. $F(0,\boldsymbol{y}) = \boldsymbol{y}$ についても同様である. □

定義 1.3 の条件 (1)-(3) はそれぞれ, 群の公理における, 零元の存在, 結合則, 可換則に対応する. また, 形式的陰関数定理により, 次の命題 1.5 が成立する. 命題 1.5 は群の公理の逆元の存在に対応する.

命題 1.5. $F(\boldsymbol{x},\boldsymbol{y})$ を R 上の g 次元形式群とする. このとき, $R[[\boldsymbol{x}]]_0^g$ の元 $[-1]_F(\boldsymbol{x})$ がただひとつ存在し,

$$F(\boldsymbol{x},[-1]_F(\boldsymbol{x})) = 0, \qquad [-1]_F(\boldsymbol{x}) \equiv -\boldsymbol{x} \bmod \deg 2$$

を満たす.

例 1.6 (形式群). R 上の 1 次元形式群の例をあげる.

(1) $\hat{\mathbb{G}}_a(x,y) := x + y$ は R 上の形式群である. **加法群**と呼ばれる.

(2) $\hat{\mathbb{G}}_m(x,y) := x + y - xy$ は R 上の形式群である. 実際,

$$1 - \hat{\mathbb{G}}_m(x,y) = (1-x)(1-y)$$

より,

$$1 - \hat{\mathbb{G}}_m(\hat{\mathbb{G}}_m(x,y),z) = (1-x)(1-y)(1-z) = 1 - \hat{\mathbb{G}}_m(x,\hat{\mathbb{G}}_m(y,z))$$

が成り立つ. $\hat{\mathbb{G}}_m(x,y)$ は**乗法群**と呼ばれる.

(3) $F_t(x,y) := (x+y)/(1-xy)$ は R 上の形式群である. 形式群 $F_t(x,y)$ は

$$\tan(x+y) = F_t(\tan x, \tan y)$$

を満たす.

(4) $2 \in R^*$ と仮定する. $F_s(x,y) := x\sqrt{1-y^2} + y\sqrt{1-x^2}$ は R 上の形式群である. 形式群 $F_s(x,y)$ は

$$\sin(x+y) = F_s(\sin x, \sin y)$$

を満たす.

注意 1.7. $\mathbb{T}: x^2+y^2=1$ とおく. 乗法 $(x_1,y_1)\otimes_{\mathbb{T}}(x_2,y_2) := (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)$ により, $\mathbb{T}$ は R 上のアフィン代数群になる. y/x, y は $\mathbb{T}$ の単位元 $(1,0)$ における局所変数であり, これらの局所変数により $\mathbb{T}$ の乗法を展開すると, 例 1.6 (3), (4) の形式群が得られる.

問題 1.8. $s(u)$ をレムニスケートサインとする. このとき, レムニスケートコサインは,

$$c(u) = \sqrt{\frac{1-s^2(u)}{1+s^2(u)}}$$

と表され, レムニスケートサインの加法公式は

$$s(u+v) = \frac{s(u)c(v) + s(v)c(u)}{1 - s(u)s(v)c(u)c(v)}$$

となる. この加法公式から, $\mathbb{Z}[2^{-1}]$ 上の形式群 $F_l(x,y)$ が得られる. (問題 1.28 に続く.)

$F(\boldsymbol{x},\boldsymbol{y})$, $G(\boldsymbol{x},\boldsymbol{y})$ を R 上の g 次元形式群とする. $\varphi(\boldsymbol{x})$ を $R[[\boldsymbol{x}]]_0^g$ の元とする.

定義 1.9. $\varphi(\boldsymbol{x})$ が $F(\boldsymbol{x},\boldsymbol{y})$ から $G(\boldsymbol{x},\boldsymbol{y})$ への R 上の**準同型**であるとは,

$$\varphi(F(\boldsymbol{x},\boldsymbol{y})) = G(\varphi(\boldsymbol{x}), \varphi(\boldsymbol{y}))$$

を満たすことをいう. さらに, 可逆な準同型を**弱同型**といい, $\varphi(\boldsymbol{x}) \equiv \boldsymbol{x} \bmod \deg 2$ を満たす弱同型 $\varphi(\boldsymbol{x})$ を**強同型**という.

R 上の形式群において, R 上の弱同型の存在, R 上の強同型の存在は, 同値関係となる. それぞれ,

$$F(\boldsymbol{x},\boldsymbol{y}) \sim_R G(\boldsymbol{x},\boldsymbol{y}), \qquad F(\boldsymbol{x},\boldsymbol{y}) \approx_R G(\boldsymbol{x},\boldsymbol{y})$$

とあらわす.

例 1.10 (形式群の自己準同型). $F(\boldsymbol{x},\boldsymbol{y})$ を R 上の g 次元形式群とする.

(1) 非負整数 n に対し, $[n]_F(x) \in R[[\boldsymbol{x}]]_0^g$ を,

$$[0]_F(\boldsymbol{x}) = 0, \qquad [n]_F(\boldsymbol{x}) = F(\boldsymbol{x}, [n-1]_F(\boldsymbol{x})) \quad (n > 0)$$

により帰納的に定義し, 負の整数 n に対しては, 命題 1.5 の $[-1]_F(\boldsymbol{x})$ を利用して,

$$[n]_F(\boldsymbol{x}) = [-1]_F \circ [-n]_F(\boldsymbol{x}) \quad (n < 0)$$

と定義する. $[n]_F(x)$ は $F(x, y)$ の自己準同型になる. n **倍自己準同型**という.

特に,

$$[n]_{\hat{\mathbb{G}}_a}(x) = nx, \qquad [n]_{\hat{\mathbb{G}}_m}(x) = 1 - (1-x)^n$$

が成り立つ.

(2) $R = \mathbb{F}_q$ と仮定する.

$$F(\boldsymbol{x}, \boldsymbol{y})^q = F(\boldsymbol{x}^q, \boldsymbol{y}^q)$$

となるので, $\boldsymbol{x}^q$ は $F(\boldsymbol{x}, \boldsymbol{y})$ の自己準同型になる. Frobenis q **乗自己準同型**と呼ばれる.

例 1.11 (形式群の準同型). (1) $\mathbb{Q} \subset R$ と仮定する. $f(x) := -\log(1-x)$ は, 乗法群 $\hat{\mathbb{G}}_m(x, y)$ から加法群 $\hat{\mathbb{G}}_a(x, y)$ への R 上の強同型である. 実際,

$$-\log(1-x)(1-y) = -\log(1-x) - \log(1-y)$$

より,

$$f(\hat{\mathbb{G}}_m(x, y)) = \hat{\mathbb{G}}_a(f(x), f(y))$$

が成り立つ.

(2) $\mathbb{Q} \subset R$ と仮定する. 例 1.6 (2)(3) より, $\tan x$, $\sin x$ はそれぞれ, 加法群 $\hat{\mathbb{G}}_a(x, y)$ から, $F_t(x, y)$, $F_s(x, y)$ への R 上の強同型である.

(3) $2 \in R^*$ と仮定する. $\tan(\arcsin x) = x/\sqrt{1-x^2}$ だから, $x/\sqrt{1-x^2}$ は $F_s(x, y)$ から $F_t(x, y)$ への R 上の強同型である.

(4) $2 \in R^*$, $i \in R$ と仮定する. $1 - \sqrt{1-x^2} - ix$ は $F_s(x, y)$ から $\hat{\mathbb{G}}_m(x, y)$ への弱同型である.

注意 1.12. 例 1.11 (3) は代数群 $\mathbb{T}$: $x^2 + y^2 = 1$ の単位元 $(1, 0)$ における 2 つの局所変数 y と y/x の変数変換を表している. また, 例 1.11 (4) は $\mathbb{T}$ から乗法群 $\mathbb{G}_m$ への準同型 $(x, y) \mapsto x + yi$ に対応している.

次の命題により, 標数 0 の体上の任意の形式群は, 加法群 $\hat{\mathbb{G}}_a^g(\boldsymbol{x}, \boldsymbol{y}) = \boldsymbol{x} + \boldsymbol{y}$ と強同型となる.

命題 1.13 (cf. e.g. [8], Thm. 1). $\mathbb{Q} \subset R$ と仮定する. このとき, R 上の任意の g 次元形式群 $F(\boldsymbol{x}, \boldsymbol{y})$ に対し, $F(\boldsymbol{x}, \boldsymbol{y})$ から $\hat{\mathbb{G}}_a^g(\boldsymbol{x}, \boldsymbol{y})$ への強同型 $f(\boldsymbol{x})$ が一意的に存在する.

定義 1.14. 命題 1.13 において, 強同型 $f(\boldsymbol{x})$ を $F(\boldsymbol{x},\boldsymbol{y})$ の**変換子**という.

注意 1.15. $f(\boldsymbol{x})$ を形式群 $F(\boldsymbol{x},\boldsymbol{y})$ の変換子とするとき,

$$f(F(\boldsymbol{x},\boldsymbol{y})) = \hat{\mathbb{G}}_a^g(f(\boldsymbol{x},\boldsymbol{y})) = f(\boldsymbol{x}) + f(\boldsymbol{y}) \tag{1.2}$$

が成り立つ. $f(\boldsymbol{x})$ は可逆だから,

$$F(\boldsymbol{x},\boldsymbol{y}) = f^{-1}(f(\boldsymbol{x}) + f(\boldsymbol{y}))$$

が成り立つ. 形式群 $F(\boldsymbol{x},\boldsymbol{y})$ は $2g$ 変数であるが, g 変数の変換子 $f(\boldsymbol{x})$ を用いて表される.

注意 1.16. $f(\boldsymbol{x})$ を形式群 $F(\boldsymbol{x},\boldsymbol{y})$ の変換子とする. (1.2) 式の両辺を $\boldsymbol{x}$ で全微分すると,

$$\sum_{j=1}^{g}\sum_{k=1}^{g}\frac{\partial f_i}{\partial x_k}(F(\boldsymbol{x},\boldsymbol{y}))\frac{\partial F_k}{\partial x_j}(\boldsymbol{x},\boldsymbol{y})dx_j = \sum_{j=1}^{g}\frac{\partial f_i}{\partial x_j}(\boldsymbol{x})dx_j$$

が成り立つ. すなわち,

$$\sum_{j=1}^{g}\frac{\partial f_i}{\partial x_j}(\boldsymbol{x})dx_j$$

は, 右移動 $\boldsymbol{x} \mapsto F(\boldsymbol{x},\boldsymbol{y})$ に対する不変微分である.

k を代数体とし, $\mathcal{O}_k$ を k の整数環とする. $\mathfrak{p}$ を $\mathcal{O}_k$ の素イデアルとし, $\mathcal{O}_\mathfrak{p}$ で $\mathfrak{p}$ 進完備化をあらわす. 命題 1.13 により, 次の Hasse の原理が成り立つ.

系 1.17. (1) $F(\boldsymbol{x},\boldsymbol{y})$ を k 上の形式群とする. $F(\boldsymbol{x},\boldsymbol{y})$ が $\mathcal{O}_k$ 上定義されるための必要十分条件は, すべての $\mathfrak{p}$ に対し $F(\boldsymbol{x},\boldsymbol{y})$ が $\mathcal{O}_\mathfrak{p}$ 上定義されることである.

(2) $F(\boldsymbol{x},\boldsymbol{y})$, $G(\boldsymbol{x},\boldsymbol{y})$ を $\mathcal{O}_k$ 上の形式群とする. $F(\boldsymbol{x},\boldsymbol{y})$ と $G(\boldsymbol{x},\boldsymbol{y})$ が, $\mathcal{O}_k$ 上で強同型となるための必要十分条件は, すべての $\mathfrak{p}$ に対し $F(\boldsymbol{x},\boldsymbol{y})$ と $G(\boldsymbol{x},\boldsymbol{y})$ が, $\mathcal{O}_\mathfrak{p}$ 上で強同型となることである.

したがって, $\mathcal{O}_k$ 上の形式群を分類するには, $\mathcal{O}_\mathfrak{p}$ 上の形式群を分類すればよい.

1.3 $\mathfrak{p}$ 進整数環上の形式群の本田理論

$k_\mathfrak{p}$ を $\mathbb{Q}_p$ の有限次不分岐 Galois 拡大とする. $\mathcal{O}_\mathfrak{p}$ を k の整数環とする. $\sigma \in \mathrm{Gal}(k_\mathfrak{p}/\mathbb{Q}_p)$ を $\mathfrak{p}$ の Frobenius 準同型とする. $M_g(\mathcal{O}_\mathfrak{p})[[T]]$ を行列環係数の 1 変数形式的べき級数環とする. ただし, 係数 A と T の交換関係を

$$TA = {}^{\sigma}AT \quad ({}^{\forall}A \in M_g(\mathcal{O}_\mathfrak{p}))$$

と定める. 写像

$$*:\ M_g(\mathcal{O}_\mathfrak{p})[[T]] \times k_\mathfrak{p}[[\boldsymbol{x}]]_0^g \to k_\mathfrak{p}[[\boldsymbol{x}]]_0^g$$

を

$$\left(\sum_{\nu\geq 0} c_\nu T^\nu\right) * f(\boldsymbol{x}) := \sum_{\nu\geq 0} c_\nu{}^{\sigma^\nu} f(\boldsymbol{x}^{p^\nu})$$

により定義する. 写像 $*$ は左作用になる.

定義 1.18. $M_g(\mathcal{O}_\mathfrak{p})[[T]]$ の元 v が**特殊元**であるとは,

$$v \equiv pI_g \bmod \deg 1$$

をみたすことをいう. また, $k_\mathfrak{p}[[\boldsymbol{x}]]_0^g$ の元 $f(\boldsymbol{x})$ が**特殊元 v に属する**とは,

$$\begin{aligned} &(1) \quad f(\boldsymbol{x}) \equiv \boldsymbol{x} \bmod \deg 2, \\ &(2) \quad (v * f)(\boldsymbol{x}) \equiv 0 \bmod \mathfrak{p} \end{aligned}$$

を満たすことをいう. ただし, $f(\boldsymbol{x}) \equiv 0 \bmod \mathfrak{p}$ は, $f_i(\boldsymbol{x})$ の各係数がイデアル $\mathfrak{p}$ に属することを意味する.

また本稿では, 形式群 $F(\boldsymbol{x}, \boldsymbol{y})$ の変換子 $f(\boldsymbol{x})$ が特殊元 v に属することを, 単に, $F(\boldsymbol{x}, \boldsymbol{y})$ が特殊元 v に属するという.

定理 1.19 ([8], Thm. 2-4). (1) $F(\boldsymbol{x}, \boldsymbol{y})$ を $k_\mathfrak{p}$ 上の形式群とする. $F(\boldsymbol{x}, \boldsymbol{y})$ が $\mathcal{O}_\mathfrak{p}$ 上定義されるための必要十分条件は, $F(\boldsymbol{x}, \boldsymbol{y})$ がある特殊元 v に属することである.

(2) $\mathcal{O}_\mathfrak{p}$ 上の g 次元形式群 $F(\boldsymbol{x}, \boldsymbol{y})$, $G(\boldsymbol{x}, \boldsymbol{y})$ が, それぞれ, 特殊元 v, u に属すると仮定する. $F(\boldsymbol{x}, \boldsymbol{y})$ と $G(\boldsymbol{x}, \boldsymbol{y})$ が, $\mathcal{O}_\mathfrak{p}$ 上で強同型となるための必要十分条件は, $M_g(\mathcal{O}_\mathfrak{p})[[T]]$ の単元 t が存在して,

$$u = tv$$

を満たすことである.

命題 1.20. $\{A_p,\ C_p\}_{p:prime}$ を互いに可換な $M_g(\mathbb{Z})$ に属する行列の集合とする. 形式的 L 級数を

$$\sum_{n \geq 1} A_n n^{-s} := \prod_p (I_n - A_p p^{-s} + C_p p^{1-2s})^{-1}$$

により定義する. このとき,

$$\sum_{n \geq 1} \frac{A_n}{n} \boldsymbol{x}^n$$

は特殊元 $pI_n - A_p T + C_p T^2$ に属する.

証明 $\sum_{n \geq 1} A_n n^{-s}$ が形式的 Euler 積を持つことは,

$$\begin{aligned} A_{mn} &= A_m A_n \quad ((m, n) = 1) \\ A_{np^2} &= A_p A_{np} - p C_p A_n \quad (n \geq 1) \end{aligned}$$

と同値である. この関係式を用いると次が従う.

$$
\begin{aligned}
&(pI_n - A_pT + C_pT^2) * \sum_{n\geq 1} \frac{A_n}{n}\boldsymbol{x}^n \\
&= p\sum_{n\geq 1} \frac{A_n}{n}\boldsymbol{x}^n - A_p\sum_{n\geq 1} \frac{A_n}{n}\boldsymbol{x}^{np} + C_p\sum_{n\geq 1} \frac{A_n}{n}\boldsymbol{x}^{np^2} \\
&= p\Big(\sum_{\substack{n\geq 1\\(n,p)=1}} \frac{A_n}{n}\boldsymbol{x}^n\Big) + \sum_{\substack{n\geq 1\\(n,p)=1}} \frac{A_{np}}{np}\boldsymbol{x}^{np} + \sum_{n\geq 1} \frac{A_{np^2}}{np^2}\boldsymbol{x}^{np^2}\Big) \\
&- A_p\Big(\sum_{\substack{n\geq 1\\(n,p)=1}} \frac{A_n}{n}\boldsymbol{x}^{np} + \sum_{n\geq 1} \frac{A_{np}}{np}\boldsymbol{x}^{np^2}\Big) + C_p\sum_{n\geq 1} \frac{A_n}{n}\boldsymbol{x}^{np^2} \\
&= p\sum_{\substack{n\geq 1\\(n,p)=1}} \frac{A_n}{n}\boldsymbol{x}^n + \sum_{\substack{n\geq 1\\(n,p)=1}} \frac{A_{np} - A_pA_n}{n}\boldsymbol{x}^{np} + \sum_{n\geq 1} \frac{A_{np^2} - A_pA_{np} + pC_pA_n}{np}\boldsymbol{x}^{np^2} \\
&\equiv 0 \bmod p
\end{aligned}
\tag{1.3}
$$

□

例 1.21. 命題 1.20 により, 次が従う.

(1) $\hat{\mathbb{G}}_m(x,y)$ は特殊元 $p-T$ に属する. なぜならば, 変換子 $-\log(1-x) = \sum_{n\geq 1} x^n/n$ に対応する形式的 L 級数は Riemann ゼータ関数

$$\sum_{n\geq 0} \frac{1}{n^s} = \prod_p \frac{1}{1-p^{-s}}$$

である.

(2) $F_t(x,y)$ は特殊元 $p-(-4/p)T$ に属する. なぜならば, 変換子は

$$\arctan x = \int \frac{dx}{1+x^2} = \sum_{n\geq 1}(-1)^n \frac{x^{2n+1}}{2n+1} = \sum_{n\geq 1} \big(\frac{-4}{n}\big)\frac{x^n}{n}$$

であり, 対応する形式的 L 級数は指標 $(-4/n)$ に付随する Dirichlet 級数

$$\sum_{n\geq 1} \big(\frac{-4}{n}\big)\frac{1}{n^s} = \prod_p \frac{1}{1-(-4/p)p^{-s}}$$

である.

楕円曲線の形式群の本田の定理の理解のため, 形式群 $\hat{\mathbb{G}}_m(x,y)/\mathbb{Z}_p$ が特殊元 $p-T$ に属することを, 幾何的に説明する.

代数群 $\mathbb{G}_m$ において, p を法とする簡約を考えると, p 乗 Frobenius 自己準同型と p 倍写像が等しくなる. したがって, $\hat{\mathbb{G}}_m(x,y)/\mathbb{F}_p$ においても, p 乗 Frobenius 自己準同型と p 倍写像が等しくなる. 実際, 例 1.10 により,

$$[p]_{\hat{\mathbb{G}}_m}(x) = 1-(1-x)^p \equiv x^p \bmod p \tag{1.4}$$

が成り立つ. $\hat{\mathbb{G}}_m(x,y)$ の変換子を $f(x)$ とおくと, (1.4) 式より,

$$f^{-1}(pf(x)) \equiv x^p \bmod p$$

が成り立ち, 次の命題 1.22 により,

$$pf(x) - f(x^p) \equiv 0 \bmod p$$

が成り立つ. すなわち, $\hat{\mathbb{G}}_m(x,y)/\mathbb{Z}_p$ は特殊元 $p-T$ に属する.

命題 1.22 ([8], Lem. 4.2). $f(x)$ をある特殊元 v に属するとする. このとき, $k_{\mathfrak{p}}[[\boldsymbol{x}]]_0^n$ の元 $\psi_1(\boldsymbol{x})$ と $\mathcal{O}_{\mathfrak{p}}[[\boldsymbol{x}]]_0^n$ の元 $\psi_2(\boldsymbol{x})$ 対し, 次は同値である.

(1) $f \circ \psi_1 \equiv f \circ \psi_2 \mod \mathfrak{p}$,

(2) $\psi_1 \equiv \psi_2 \mod \mathfrak{p}$.

1.4 計算例：$F_s(x,y)$ の属する特殊元

$p \neq 2$ と仮定し, $R := \mathbb{Z}_p$ とおく. $\mathbb{Z}_p$ 上定義された形式群 $F_s(x,y)$ の属する特殊元を 3 通りに求める.

命題 1.23. $F_s(x,y)$ は特殊元 $p-(-1/p)T$ に属する.

証明 1 $F_s(x,y)$ が $F_t(x,y)$ と $\mathbb{Z}_p$ 上強同型であることを利用する.

例 1.11(3) により, $F_t(x,y)$ と $F_s(x,y)$ は $\mathbb{Z}_p$ 上強同型である. また, 例 1.21(2) により, $F_t(x,y)$ は特殊元 $p-(-1/p)T$ に属する. したがって, 命題 1.19(2) より, $F_s(x,y)$ は特殊元 $p-(-1/p)T$ に属する. □

証明 2 [1] $F_s(x,y)$ の変換子 $\sum_{n\geq 1} a_n x^n/n = \arcsin x$ の係数 a_n の関係式を, p 進ガンマ関数 $\Gamma_p(x)$ を用いて書き下す.

(1.3) 式と同様に計算して, $\sum_{n\geq 1} a_n x^n/n$ が特殊元 $p-(-1/p)T$ に属することは, 合同式

$$a_{np} - (-1/p)a_n \equiv 0 \bmod p^{\nu+1}$$

と同値である. ただし, $p^\nu \parallel n$ とおいた. $\arcsin x$ は奇関数であるから, n が偶数のとき, $a_n = 0$ である. 任意の奇数 n に対して,

$$a_{np} - (-1/p)a_n \equiv 0 \mod p^{\nu+1}$$

を示せばよい.

$$\arcsin x = \int \frac{1}{\sqrt{1-x^2}}\,dx = \sum_{j\geqq 0} \begin{bmatrix} -1/2 \\ j \end{bmatrix} \frac{(-1)^j x^{2j+1}}{2j+1} = \sum_{j\geqq 0} \frac{1}{2^{2j}} \begin{bmatrix} 2j \\ j \end{bmatrix} \frac{x^{2j+1}}{2j+1} \tag{1.5}$$

[1] この方法は大西-安田 [10] による.

が成立つことに注意する. (1.5) 式より,

$$a_{np} = \frac{(np-1)!}{2^{np-1}((np-1)/2)!((np-1)/2)!}$$

が成り立つ. ここで, p 進ガンマ関数 $\Gamma_p(x)$ に関する等式 (cf. e.g. [11], p.369)

$$\begin{aligned}(np-1)! &= \Gamma_p(np)(-1)^{np}(n-1)!p^{n-1}\\ ((np-1)/2)! &= \Gamma_p((np+1)/2)(-1)^{(np+1)/2}((n-1)/2)!p^{(n-1)/2}\end{aligned}$$

を用いると,

$$a_{np} = \frac{-\Gamma_p(np)}{2^{np-1}\Gamma_p^2((np+1)/2)}\begin{bmatrix} n-1 \\ (n-1)/2 \end{bmatrix} = \frac{-\Gamma_p(np)}{2^{np-n}\Gamma_p^2((np+1)/2)}a_n$$

ところが, 次の合同式 (cf. e.g. [11], p.369)

$$\begin{aligned}2^{n(p-1)} &\equiv 1 \mod p^{\nu+1}\\ \Gamma_p(np) &\equiv \Gamma_p(0) = 1 \mod p^{\nu+1}\\ \Gamma_p^2((np+1)/2) &\equiv \Gamma_p^2(1/2) = (-1)^{(p+1)/2} \mod p^{\nu+1}\end{aligned}$$

が成り立つので, 第 1 補充法則 $(-1/p) = (-1)^{(p-1)/2}$ を用いて,

$$a_{np} \equiv (-1/p)a_n \bmod p^{\nu+1}$$

を得る. □

証明 3　形式群 $F_s(x,y)$ の p 倍べき級数 $[p]_{F_s}(x)$ に着目する. $f(x) = \arcsin x$ とおく.

$$\cos px + i\sin px = (\cos x + i\sin x)^p \equiv \cos^p x + i\sin^p x \mod p$$

より,

$$\sin px \equiv i^{p-1}\sin^p x \mod p$$

を得る. さらに,

$$[p]_{F_s}(x) = f^{-1}(pf(x)) = \sin(p\arcsin x)$$

より,

$$[p]_{F_s}(x) = f^{-1}(pf(x)) \equiv i^{p-1}x^p \mod p$$

が成り立つ. 命題 1.22, 第 1 補充法則 $(-1/p) = (-1)^{(p-1)/2}$ と $f(x) = \arcsin x$ が奇関数であることから,

$$pf(x) \equiv f(i^{p-1}x^p) \equiv (-1/p)f(x^p) \mod p$$

が成り立つ. したがって, $F_s(x,y)$ は特殊元 $p-(-1/p)T$ に属する. □

1.5 楕円曲線の形式群

1.5.1 加法公式を用いた形式群の構成

c_i を不定元とし, $k := \mathbb{Q}(c_1, \ldots, c_6)$, $R := \mathbb{Z}[c_1, \ldots, c_6]$ とおく. E を Weierstrass モデル

$$y^2 + c_1xy + c_3y = x^3 + c_2x^2 + c_4x + c_6$$

で定義された k 上の楕円曲線とする. E には無限遠点 O を零元とするアーベル群構造が入る. O における局所変数 $t := -x/y$ をとり, 加法公式を用いて形式群 $\hat{E}(x, y)$ を構成する.

$w := -1/y$ とおく. このとき,

$$w - c_1tw - c_3w^2 = t^3 + c_2t^2w + c_4w^2 + c_6w^3 \tag{1.6}$$

が成立する. 陰関数定理により, (1.6) を満たす

$$w = w(t) \in R[[t]]_0$$

がただひとつ存在する.

E の加法を $\oplus_E$ で表す. t_1, t_2 を不定元とし,

$$(t_1, w(t_1)) \oplus_E (t_2, w(t_2)) = (\hat{E}(t_1, t_2), w(\hat{E}(t_1, t_2)))$$

により, $\hat{E}(t_1, t_2)$ を定義する. E の加法の性質（零元の存在, 結合則, 可換則）より, $\hat{E}(x, y)$ は k 上の形式群になる.

命題 1.24 (cf. e.g. [14], p.115). $\hat{E}(x, y)$ は R 上の形式群である.

証明

$$(t_1, w(t_1)) \oplus_E (t_2, w(t_2)) \oplus_E (t_3, w(t_3)) = O$$

とおく.

$$\begin{aligned} [-1]_{\hat{E}}(t) &= \frac{-t}{1 - c_1t - c_3w(t)} \in R[[t]], \\ \hat{E}(t_1, t_2) &= [-1]_{\hat{E}}(t_3(t_1, t_2)) \end{aligned}$$

が成り立つので, $t_3(t_1, t_2) \in R[[t_1, t_2]]$ を示せば十分である.

$$\lambda := \frac{w(t_1) - w_2(t_2)}{t_1 - t_2} \in R[[t_1, t_2]],$$

$$\nu := w(t_1) - \lambda t_1 \in R[[t_1, t_2]]$$

とおく. t_1, t_2, t_3 は (1.6) と直線 $w = \lambda t + \nu$ との交点だから,

$$t_3 = t_3(t_1, t_2) = -t_1 - t_2 + \frac{c_1\lambda + c_3\lambda^2 - c_2\nu - 2c_4\lambda\nu - 3c_6\lambda^2\nu}{1 + c_2\lambda + c_4\lambda^2 + c_6\lambda^3} \in R[[t_1, t_2]]$$

が成り立つ. □

1.5.2 不変微分を用いた形式群の構成

不変微分 $\omega_E := dx/(2y + c_1x + c_3)$ を

$$\frac{dx}{2y + c_1x + c_3} = \sum_{n\geq 0} b_n t^n \frac{dt}{t}$$

と展開する. このとき, $b_n \in \mathbb{Z}$, $b_1 = 1$ が成立する. このとき, 右辺が形式群 $\hat{E}(x, y)$ の不変微分になることから,

$$\hat{E}(x, y) = f^{-1}(f(x) + f(y)), \qquad f(x) := \sum_{n\geq 1} \frac{b_n}{n} x^n \tag{1.7}$$

が成立する. したがって, 式 (1.7) により $\hat{E}(x, y)$ を定義することも可能である.

1.5.3 本田の定理

$G_{\mathbb{Q}}$ の E 上の l 進表現に関する L 級数を

$$L(E/\mathbb{Q}, s) = \prod_p \frac{1}{1 - a_p p^s + \varepsilon_p p^{1-2s}} = \sum_{n\geq 1} \frac{a_n}{n^s}$$

とおく. このとき, a_n は l によらず $\mathbb{Z}$ の元となり, $a_1 = 1$ が成立する. E の L 級数 $L(E/\mathbb{Q}, s)$ の形式群 $\hat{L}(x, y)$ を

$$\hat{L}(x, y) := g^{-1}(g(x) + g(y)), \qquad g(x) := \sum_{n\geq 1} \frac{a_n}{n} x^n$$

により定義する.

定理 1.25 ([8], Thm. 9). $\hat{L}(x, y)$ は $\mathbb{Z}$ 上の形式群である. また, $\hat{L}(x, y)$ と $\hat{E}(x, y)$ は $\mathbb{Z}$ 上で強同型である.

証明 証明の概略を述べる. 命題 1.20 により, $\hat{L}(x, y)/\mathbb{Q}_p$ は特殊元 $p - a_pT + \varepsilon_pT$ に属する. したがって, 命題 1.19 により, $\hat{L}(x, y)$ は $\mathbb{Z}_p$ 上の形式群となる. Hasse の原理により, $\hat{L}(x, y)$ は $\mathbb{Z}$ 上の形式群である.

p を E のよい素点とする. E の p を法とする簡約の Frobenius p 乗自己準同型に着目して,

$$f^{-1}(pf(x) - a_p f(x^p) + f(x^{p^2})) \equiv 0 \bmod p$$

を得る. $\hat{E}(x, y)$ は $\mathbb{Z}$ 上の形式群だから, 命題 1.22 により,

$$pf(x) - a_p f(x^p) + f(x^{p^2}) \equiv 0 \bmod p$$

が成り立つ. したがって, $\hat{E}(x, y)/\mathbb{Z}_p$ は特殊元 $p - a_pT + \varepsilon_pT$ に属する.

悪い素点 p に対しては, $\hat{E}(x, y)$ の p を法とする簡約が $\hat{\mathbb{G}}_a(x, y)$, または $\hat{\mathbb{G}}_a(x, y)$ に強同型になることを用いて, $\hat{E}(x, y)/\mathbb{Z}_p$ は特殊元 $p - a_pT + \varepsilon_pT$ に属することが示される.

したがって, 再び命題 1.19 を用いて, 任意の p に対して, $\hat{L}(x, y)$ と $\hat{E}(x, y)$ は $\mathbb{Z}_p$ 上で強同型である. Hasse の原理により, $\hat{L}(x, y)$ と $\hat{E}(x, y)$ は $\mathbb{Z}$ 上で強同型となる. □

系 1.26. 任意の素数 p に対し, $a_p \equiv b_p \bmod p$ が成り立つ.

証明 (1.3) 式と同様に計算する. $\hat{E}(x,y)/\mathbb{Z}_p$ が特殊元 $p - a_pT + \varepsilon_pT^2$ に属することは,

$$\begin{aligned} b_{np} &\equiv a_pb_n \bmod p \quad ((n,p)=1), \\ b_{np^2} &\equiv a_pb_{np} - p\varepsilon_pb_n \bmod p^{\nu+1} \quad (n \geq 1) \end{aligned}$$

と同値である. □

注意 1.27. Hasse-Weil の不等式 $|a_p| \leq 2\sqrt{p}$ を利用すると, $p \geq 17$ においては,

$$a_p = (b_p \text{ の } p \text{ を法とする絶対値最小の剰余})$$

が成り立つ.

問題 1.28. 以下の形式群は, $\mathbb{Z}[2^{-1}]$ 上定義され互いに強同型である.

(1) レムニスケートサインの加法公式から定義した形式群 $F_l(x,y)$ (問題 1.8),

(2) 楕円積分 $\displaystyle\int \frac{dx}{\sqrt{1-x^4}}$ を変換子にもつ形式群,

(3) $y^2 = x^3 - x$ の形式群, また, $y^2 = x^3 - x$ の L 級数の形式群.

2 ヤコビ多様体の形式群

本節ではヤコビ多様体の形式群について述べる.

標数 0 の体上定義された楕円曲線の場合, 形式群の構成には, 加法公式を用いた構成と正則微分形式を用いた構成がある (1.5 節).

加法公式を用いた構成は, Grant [6], Flynn [4] により, 種数 2 の超楕円曲線のヤコビ多様体に一般化されている. Grant [6] は, 超楕円曲線が定義体上有理的な Weierstrass 点を持つと仮定した場合に, Flynn [4] はこの仮定なしに, それぞれ, $\mathbb{P}^8$, $\mathbb{P}^{15}$ へのヤコビ多様体の埋め込みを与え, 定義方程式や加法公式を明示的に与え, ヤコビ多様体の形式群を構成している.

正則微分形式を用いた構成は, Freije [5] により, 代数曲線が定義体上有理的な Weierstrass 点を持つという仮定の下で, 種数が 1 以上の場合に一般化されている.

本節では, Freije の議論を一般化し, 代数曲線の正則微分の局所変数による展開とヤコビ多様体の形式群の強同型類の特殊元との関係を明らかにする. また, 代数曲線が超楕円曲線の場合に, Riemann-Roch の定理を用いて, ヤコビ多様体の加法公式を明示的に与え, ヤコビ多様体の形式群を構成する.

2.1 $\Omega^1(C)$ を用いた $\hat{J}(\boldsymbol{x},\boldsymbol{y})$ の構成

2.1.1 Freije の結果

k を標数 0 の体とし, C を体 k 上定義された種数 g の完備非特異代数曲線とする. 代数曲線 C は Weierstrass 点ではない k 有理点 P を持つと仮定する. J を C のヤコビ多様体とし, C から J への k 上の基準写像 Λ を $\Lambda(P)$ が J の零元に一致するようにとる.

まず, 本節で扱うヤコビ多様体の形式群 $\hat{J}(\boldsymbol{x},\boldsymbol{y})$ を定義する. アーベル多様体の形式群は, 零元における局所変数を用いて加法を展開することにより得られる. したがって, 局所変数の選び方が問題である.

C の点 P における局所変数 t をとし, C^g の点 $(P,\dots,P)$ における局所変数

$$\boldsymbol{t} = {}^t(t_1,\dots,t_g)$$

を, 各 t_j が t に等しくなるようにとる. $t_1,\dots,t_g$ の j 次基本対称式を $s_j(\boldsymbol{t})$ であらわし,

$$\boldsymbol{s}(\boldsymbol{t}) := {}^t(s_1(\boldsymbol{t}),\dots,s_g(\boldsymbol{t}))$$

とおくと, $\boldsymbol{s}(\boldsymbol{t})$ は対称空間 $\mathrm{Sym}^g C$ の点 $(P,\dots,P)$ における局所変数となる. Λ は対称空間 $\mathrm{Sym}^g C$ から J への双有理写像 Λ^g を引き起こす. Λ^g は $(P,\dots,P)$ において双正則であるから, Λ^g を通じ, $\boldsymbol{s}(\boldsymbol{t})$ を J の零元における局所変数と同一視できる. $\hat{J}(\boldsymbol{x},\boldsymbol{y})$ を局所変数 $\boldsymbol{s}(\boldsymbol{t})$ に付随する形式群とする.

次に, Freije による $\hat{J}(\boldsymbol{x},\boldsymbol{y})$ の変換子の明示的な構成について説明する.

有理点 P は Weierstrass 点ではないと仮定したので, C の正則微分形式の基底 $\{\omega_j\}_{j=1}^g$ を,

$$\omega_j \equiv (-t)^{j-1}dt \mod t^g dt \quad (1 \le j \le g)$$

を満たすようにとれる. 便宜上, 列ベクトルを用いて,

$$\omega := {}^t(\omega_1,\dots,\omega_g)$$

とおく. $k[[t]]_0^g$ の元 $l(t) = {}^t(l_1(t),\dots,l_g(t))$ を

$$l(t) = \int \omega$$

により定義する. $\boldsymbol{x} = {}^t(x_1,\dots,x_g)$ とおき, $k[[\boldsymbol{x}]]_0^g$ の元 $L(\boldsymbol{x}) = {}^t(L_1(\boldsymbol{x}),\dots,L_g(\boldsymbol{x}))$ を

$$L(\boldsymbol{s}(\boldsymbol{t})) = l(t_1) + \cdots + l(t_g) \tag{2.8}$$

により定義する.

定理 2.1 ([5], Thm. 2). $L(\boldsymbol{x})$ は $\hat{J}(\boldsymbol{x},\boldsymbol{y})$ の変換子である.

定理 2.1 により,

$$\hat{J}(\boldsymbol{x},\boldsymbol{y}) = L^{-1}(L(\boldsymbol{x}) + L(\boldsymbol{y})) \tag{2.9}$$

が成立する. したがって, $\hat{J}(\boldsymbol{x},\boldsymbol{y})$ は $L(\boldsymbol{x})$ を用いて明示的に構成できる.

2.1.2 形式群 $\hat{J}(\boldsymbol{x},\boldsymbol{y})$ の本田理論

k を $\mathbb{Q}_p$ の有限次不分岐拡大, $\mathcal{O}_\mathfrak{p}$ をその整数環とする. $\sigma \in \mathrm{Gal}(k/\mathbb{Q}_p)$ を $\mathfrak{p}$ の Frobenius 準同型とする.

正則微分形式の展開係数を用いて, 形式群 $\hat{J}(\boldsymbol{x},\boldsymbol{y})$ を定義する場合, $\hat{J}(\boldsymbol{x},\boldsymbol{y})$ がいつ整数環 $\mathcal{O}_\mathfrak{p}$ 上定義されるかを調べることが問題となる. この問いに対する答えのひとつが形式群の本田理論を用いて得られる. Freije [5] の議論を一般化し, $\hat{J}(\boldsymbol{x},\boldsymbol{y})$ が $\mathcal{O}_\mathfrak{p}$ 上定義される為の必要十分条件を求める.

定義 2.2. $\mathcal{O}_\mathfrak{p}[[t]]_0^g$ の元 $l(t) = {}^t(l_1(t),\dots,l_g(t))$ が**特殊元 v に属する**とは, $l(t)$ が次の 2 条件を満たすことをいう.

(1) $l_j(t) \equiv (-1)^{j-1}t^j/j \mod \deg g+1 \quad (1 \le j \le g)$,

(2) $(v * l)(t) \equiv 0 \mod \mathfrak{p}$.

$l(t)$, $L(\boldsymbol{x})$, $\hat{J}(\boldsymbol{x},\boldsymbol{y})$ は 2.1.1 節の通りとする. このとき, 次の定理が成立する.

定理 2.3. $\hat{J}(\boldsymbol{x},\boldsymbol{y})$ が $\mathbb{Z}_p$ 上定義される為の必要十分条件は, $l(t)$ がある特殊元 v に属することである.

注意 2.4. 十分条件であることは, 本田 [9, Thm. 1] において本質的に示されている. 定理 2.3 は, $C = X_0(N)$, $P = i\infty$ の場合には, Freije [5] により証明されている. この場合, 特殊元は $I_g - A_pT + \varepsilon_pT^2 \quad (A_p \in M_g(\mathbb{Z}_p),\ \varepsilon_p = 0,1)$ という形になる.

k 係数の列ベクトル $c(n) = {}^t(c_1(n),\dots,c_g(n))$ を,

$$l(t) = \sum_n c(n)\frac{t^n}{n}$$

により定義する.

定義 2.5. 行列 $\Big[c(p), -c(2p), \dots, (-1)^g c(gp)\Big]$ を, **Cartier-Manin 行列**, または, Hasse-Witt 行列と呼ぶ.

定理 2.6. $l(t)$ が $v = pI_g + b_1T + \cdots$ に属すると仮定する. このとき, $p > g$ ならば, 合同式

$$\Big[c(p), -c(2p), \dots, (-1)^g c(gp)\Big] \equiv -b_1 \mod \mathfrak{p}$$

が成り立つ.

$k = \mathbb{Q}$ とする. Hasse の原理と定理 2.3 により, 次の系が得られる.

系 2.7. $\hat{J}(\boldsymbol{x},\boldsymbol{y})$ が $\mathbb{Z}$ 上定義されるための必要十分条件は, 任意の素数 p に対し, $l(x)$ がある特殊元に属することである.

2.1.3 定理 2.3 の証明

$I=(i_1,\dots,i_g)$ を非負整数の添え字の集合とし, $I!=i_1!\dots i_g!$, $N_I=i_1+2i_2+\cdots+gi_g$, そして,

$$B(I):=\frac{(-1)^{i_2+i_4+\cdots}(i_1+i_2+\cdots+i_g-1)!}{I!}$$

とおく. 任意の $n=1$,...,g に対し, $i_nB(I)$ は多項係数となり, 整数となる. $i_nB(I)$ が整数なので, $N_IB(I)=\sum_n ni_nB(I)$ も整数である.

また, $\boldsymbol{x}^I:=x_1^{i_1}x_2^{i_2}\cdots x_g^{i_g}$ とおく.

補題 2.8 ([5], Lem. 1).

$$x_1^n+\cdots+x_g^n=n\sum_{I,N_I=n}B(I)\boldsymbol{s}(\boldsymbol{x})^I$$

が成り立つ.

補題 2.9 ([5], Lem. 4). 合同式 $B(I/p^\nu)\equiv p^\nu B(I) \bmod p$ が成立する. ただし, $p^\nu\nmid I$ のとき, $B(I/p^\nu)=0$ と定める.

定理 2.3 は, 以下の 2 つの補題から従う.

補題 2.10. 次は同値である.

(1) $l_j(t)\equiv(-1)^{j-1}t^j/j \mod \deg g+1 \quad (1\le j\le g)$,

(2) $L(\boldsymbol{x})\equiv\boldsymbol{x} \mod \deg 2$.

証明

$$\begin{aligned}L(\boldsymbol{s}(\boldsymbol{x})) &= \sum_n c(n)\frac{x_1^n+\cdots+x_g^n}{n}\\ &= \sum_n c(n)\sum_{I,N_I=n}B(I)\boldsymbol{s}(\boldsymbol{x})^I\\ &= \sum_I c(N_I)B(I)\boldsymbol{s}(\boldsymbol{x})^I\end{aligned}$$

が成り立つ. それゆえ,

$$L(\boldsymbol{x})=\sum_I c(N_I)B(I)\boldsymbol{x}^I \tag{2.10}$$

が成り立つ. (2.10) により,

$$\begin{aligned}L(\boldsymbol{x}) &\equiv \sum_{i_1+\cdots+i_g=1}c(N_I)B(I)\boldsymbol{x}^I \mod \deg 2\\ &\equiv \sum_{n=1}^{g}c(n)(-1)^{n-1}x_n \mod \deg 2\end{aligned}$$

が成立する. それゆえ条件 (2) は, 条件 (1)

$$\Big[c(1), -c(2), \ldots, (-1)^g c(g)\Big] = [(-1)^{i-1}\delta_{ij}]$$

と同値である. □

補題 2.11. 次は同値である.

(1) $(v * l)(t) \equiv 0 \mod \mathfrak{p}$,

(2) $(v * L)(\boldsymbol{x}) \equiv 0 \mod \mathfrak{p}$.

証明 特殊元 v を $v = pI_g + \sum_\nu b_\nu T^\nu$ とおく. b_ν が $M_g(\mathbb{Z}_p)$ の行列であることに注意する.

$$\begin{aligned}(v * l)(t) &= (pI_g + \sum_\nu b_\nu T^\nu) * \sum_n c(n)\frac{t^n}{n} \\ &= p\sum_n c(n)\frac{t^n}{n} + \sum_k \sum_\nu {b_\nu}^{\sigma^\nu} c(n)\frac{t^{np^\nu}}{n} \\ &= p\sum_k c(n)\frac{t^n}{n} + \sum_k \sum_\nu {b_\nu}^{\sigma^\nu} c(n/p^\nu)\frac{p^\nu t^n}{n}\end{aligned}$$

が成り立つ. ただし, $p^\nu \nmid n$ のとき, $c(n/p^\nu) = 0$ と定める. t^n の係数 a_n は,

$$a_n = \frac{1}{n}\left(pc(n) + \sum_\nu p^\nu {b_\nu}^{\sigma^\nu} c(n/p^\nu)\right) \tag{2.11}$$

を満たす.

一方で, 次が成り立つ.

$$\begin{aligned}(v * L)(\boldsymbol{x}) &= (pI_g + \sum_\nu b_\nu T^\nu) * \sum_I c(N_I)B(I)\boldsymbol{x}^I \\ &= p\sum_I c(N_I)B(I)\boldsymbol{x}^I + \sum_I \sum_\nu {b_\nu}^{\sigma^\nu} c(N_I)B(I)\boldsymbol{x}^{Ip^\nu} \\ &= p\sum_I c(N_I)B(I)\boldsymbol{x}^I + \sum_I \sum_\nu {b_\nu}^{\sigma^\nu} c(N_I/p^\nu)B(I/p^\nu)\boldsymbol{x}^I.\end{aligned}$$

ただし, $p^\nu \nmid I$ のとき, $B(I/p^\nu) = 0$ と定める. $N_{I/p^\nu} = N_I/p^\nu$ if $p^\nu | I$ であることを注意する. $\boldsymbol{x}^I$ の係数 A_I は

$$A_I = pc(N_I)B(I) + \sum_\nu {b_\nu}^{\sigma^\nu} c(N_I/p^\nu)B(I/p^\nu)$$

となる. 補題 2.9 と $N_I B(I)$ が整数であることより,

$$\begin{aligned}A_I &= pc(N_I)B(I) + \sum_\nu {b_\nu}^{\sigma^\nu} c(N_I/p^\nu)B(I/p^\nu) \\ &\equiv pc(N_I)B(I) + \sum_\nu {b_\nu}^{\sigma^\nu} c(N_I/p^\nu)p^\nu B(I) \mod \mathfrak{p} \\ &\equiv \frac{1}{N_I}\left(pc(N_I) + \sum_\nu p^\nu {b_\nu}^{\sigma^\nu} c(N_I/p^\nu)\right)N_I B(I) \mod \mathfrak{p} \\ &\equiv a_{N_I} N_I B(I) \bmod \mathfrak{p}\end{aligned}$$

が従う.

また, $I=(n,0,\dots,0)$ のとき, $N_I=n$ かつ $N_IB(I)=1$ が成り立つ. したがって,

$$A_{(n,0,\dots,0)} \equiv a_n \mod \mathfrak{p}$$

が成り立つ.

それゆえ, すべての n について $a_n \equiv 0 \bmod \mathfrak{p}$ であることと, すべての I について $A_I \equiv 0 \bmod \mathfrak{p}$ であることとは同値である. 以上により補題の主張が示された. □

2.2 $\mathbf{Pic}^0(C)$ の加法公式を用いた $\hat{J}(\boldsymbol{x},\boldsymbol{y})$ の構成

2.2.1 超楕円曲線の場合

$f_0,\dots,f_{2g+2}$ を不定元とし, $k:=\mathbb{Q}(f_0,\dots,f_{2g+2})$, $R:=\mathbb{Z}[f_0,\dots,f_{2g+2},f_{2g+2}^{-1/2},2^{-1}]$ とおく. 関数体 k 上の種数 g の超楕円曲線 C を

$$y^2 = f_{2g+2}x^{2g+2} + f_{2g+1}x^{2g+1} + \cdots + f_1x + f_0,$$

$$u^2 = 1 + f_{2g+1}t + \cdots + f_1t^{2g+1} + f_0t^{2g+2}$$

を双有理変換

$$x=\frac{1}{t}, \qquad y=\frac{u}{t^{g+1}}$$

で張り合わせた抽象多様体として定義する. (x,y) 座標を用いて,

$$P_0 := (0,\sqrt{f_0}), \qquad P_0' := (0,-\sqrt{f_0})$$

とおく. (t,u) 座標を用いて,

$$P_\infty := (0,1), \qquad P_\infty' := (0,-\sqrt{f_{2g+2}})$$

とおく. P は Wierstrass 点ではなく, t は P における局所変数となる. 実際,

$$x=\frac{1}{t}, \qquad y=\frac{\sqrt{f_{2g+2}}}{t^{g+1}} + \frac{f_{2g+1}}{2\sqrt{f_{2g+2}}}\frac{1}{t^g} + \cdots$$

が成り立つ. d_n を

$$\sum_{n\geq 0} d_nt^n = u = \sqrt{f_{2g+2}} + \frac{f_{2g+1}}{2\sqrt{f_{2g+2}}}t + \cdots \in R[[t]] \tag{2.12}$$

により定義する. 2.1.1 節における固定点 P として P_∞ をとり, ヤコビ多様体 J の局所変数系 $\boldsymbol{s}(\boldsymbol{t})$ に対する形式群を $\hat{J}(\boldsymbol{x},\boldsymbol{y})$ とおく. このとき, 次が成り立つ.

定理 2.12. 形式群 $\hat{J}(\boldsymbol{x},\boldsymbol{y})$ は R 上定義される.

注意 2.13. Flynn [4] は, $g=2$ の場合にヤコビ多様体 J の, $\boldsymbol{s}(\boldsymbol{t})$ とは異なる, ある局所変数系に付随する形式群が R 上定義されることを示している.

2.2.2 定理 2.12 の証明

この節ではヤコビ多様体 J の加法を因子類群 $\mathrm{Pic}^0(C)$ の加法としてとらえる. $\Lambda^{(g)}$: $\mathrm{Sym}^g(C) \to \mathrm{Pic}^0(C)$: $Q \mapsto Q - P_\infty$ が全射, かつ, 一般点上で単射であることに注意する.

(t_i, u_i) $(i = 1, \ldots, 2g)$ を C の一般点とする. 加法

$$\sum_{n=2g+1}^{3g} (t_n, u_n) := \sum_{n=1}^{g} (t_n, u_n) \oplus_J \sum_{n=g+1}^{2g} (t_n, u_n)$$

を

$$\sum_{n=1}^{g} (t_n, u_n) - gP_\infty + \sum_{n=g+1}^{2g} (t_n, u_n) - gP_\infty \sim \sum_{n=2g+1}^{3g} (t_n, u_n) - gP_\infty$$

により定義する. つまり,

$$\sum_{n=1}^{2g} (t_n, u_n) + \sum_{n=2g+1}^{3g} (t_n, -u_n) - 2gP_\infty - gP'_\infty \sim 0$$

が成立する. C 上の関数 h を

$$\mathrm{div}(h) = \sum_{n=1}^{2g} (t_n, u_n) + \sum_{n=2g+1}^{3g} (t_n, -u_n) - 2gP_\infty - gP'_\infty$$

により定義する.

$y + \sum_{n=0}^{g+1} d_n x^{g+1-n} \in L((g+1)P_\infty - P'_\infty)$ に注意する. Riemann-Roch の定理を用いて,

$$L(2gP_\infty + gP'_\infty) = \langle x^n \mid 0 \le n \le g \rangle \oplus \langle x^n (y + \sum_{m=0}^{g+1} d_m x^{g+1-m}) \mid 0 \le n \le g-1 \rangle$$

が成り立つ.

$$h = \sum_{n=0}^{g} A_{2g-n} x^n + \sum_{n=0}^{g-1} A_{g-1-n} \left(x^n (y + \sum_{m=0}^{g+1} d_m x^{g+1-m}) \right)$$

とおく. ここで, $A_0 \neq 0$ である. なぜならば, もし $A_0 = 0$ ならば,

$$\mathrm{div}(h) + (2g-1)P_\infty + gP'_\infty > 0$$

が成り立ち, それゆえ,

$$\sum_{n=1}^{2g} (t_n, u_n) + \sum_{n=2g+1}^{3g} (t_n, -u_n) - P_\infty > 0$$

が成り立つ. ある i に対し, $(t_i, u_i) = P_\infty$ または P'_∞ が成り立ち, (t_i, u_i) が一般点であることに矛盾する.

以下, $A_0 = 1$ と仮定して一般性を失わない. h を変型して,

$$\begin{aligned} h &= \sum_{n=0}^{g} A_{2g-n}t^{-n} + \sum_{n=0}^{g-1} A_{g-1-n}\left(t^{-n}\left(ut^{-(g+1)} + \sum_{m=0}^{g+1} d_m t^{-(g+1)+m}\right)\right) \\ &= t^{-2g}\left(\sum_{n=0}^{g} A_{2g-n}t^{2g-n} + \sum_{n=0}^{g-1} A_{g-1-n}t^{g-1-n}(u + \sum_{m=0}^{g+1} d_m t^m)\right) \\ &= t^{-2g}\left(\sum_{n=0}^{g-1} A_n t^n(u + \sum_{m=0}^{g+1} d_m t^m) + \sum_{n=g}^{2g} A_n t^n\right) \end{aligned}$$

を得る. $\mathrm{div}(t) = P_\infty + P'_\infty - P_0 - P'_0$ なので,

$$\begin{aligned} &\mathrm{div}\left(\sum_{n=0}^{g-1} A_n t^n(u + \sum_{m=0}^{g+1} d_m t^m) + \sum_{n=g}^{2g} A_n t^n\right) \\ &= \sum_{n=1}^{2g}(t_n, u_n) + \sum_{n=2g+1}^{3g}(t_n, -u_n) + gP'_\infty - 2gP_0 - 2gP'_0 \end{aligned} \tag{2.13}$$

である. h は (t_i, u_i) $(1 \le i \le 2g)$ を零点として持ち,

$$\sum_{n=1}^{g-1} A_n t_i^n(u_i + \sum_{m=0}^{g+1} d_m t_i^m) + \sum_{n=g}^{2g} A_n t_i^n = -\left(u_i + \sum_{m=0}^{g+1} d_m t_i^m\right) \quad (1 \le i \le 2g)$$

が成り立つ. 行列を用いて表示すると,

$$\left[\left[t_i^j(u_i + \textstyle\sum_{n=0}^{g+1} d_n t_i^n)\right]_{\substack{1\le i\le 2g \\ 1\le j\le g-1}} \quad \left[t_i^j\right]_{\substack{1\le i\le 2g \\ g\le j\le 2g}}\right]\left[A_i\right]_{\substack{1\le i\le 2g \\ j=1}} = \left[-u_i - \sum_{n=0}^{g+1} d_n t_i^n\right]_{\substack{1\le i\le 2g \\ j=1}}$$

を得る. Cramer の公式を用いて,

$$A_n = A'_n/M \quad (1 \le i \le 2g)$$

を得る. ただし,

$$M := \det\left[\left[t_i^j(u_i + \textstyle\sum_{n=0}^{g+1} d_n t_i^n)\right]_{\substack{1\le i\le 2g \\ 1\le j\le g-1}} \quad \left[t_i^j\right]_{\substack{1\le i\le 2g \\ g\le j\le 2g}}\right],$$

$$A'_1 := \det\left[\left[-u_i - \textstyle\sum_{n=0}^{g+1} d_n t_i^n\right]_{\substack{1\le i\le 2g \\ j=1}} \quad \left[t_i^j(u_i + \textstyle\sum_{n=0}^{g+1} d_n t_i^n)\right]_{\substack{1\le i\le 2g \\ 2\le j\le g-1}} \quad \left[t_i^j\right]_{\substack{1\le i\le 2g \\ g\le j\le 2g}}\right], \ldots$$

とおく. 記法を簡潔にするため,

$$A'_0 := M$$

とおく.

$$\Delta := \prod_{1\le i<j\le 2g}(t_i - t_j)$$

とおく. A'_n $(0 \leq n \leq 2g)$ は $t_1, \ldots, t_{2g}$ の交代的形式的べき級数だから, A'_n は Δ で割り切れる.

$$B_n := A'_n/\Delta \quad (0 \leq n \leq 2g)$$

とおく.

補題 2.14. B_n $(0 \leq i \leq 2g)$ は $R[[t_1, \ldots, t_{2g}]]$ に属する.

$B_n = A_n M/\Delta$ $(0 \leq i \leq 2g)$ より, 等式

$$\sum_{n=0}^{g-1} A_n t^n (u + \sum_{m=0}^{g+1} d_m t^m) + \sum_{n=g}^{2g} A_n t^n = 0$$

は等式

$$\sum_{n=0}^{g-1} B_n t^n (u + \sum_{m=0}^{g+1} d_m t^m) + \sum_{n=g}^{2g} B_n t^n = 0$$

と同値である. $t_{2g+1}, \ldots, t_{3g}$ を得るために連立方程式

$$\begin{cases} \displaystyle\sum_{n=0}^{g-1} B_n t^n (u + \sum_{m=0}^{g+1} d_m t^m) + \sum_{n=g}^{2g} B_n t^n = 0 \\ u^2 = f_{2g+2} + f_{2g+1} t + f_{2g} t^2 + \cdots + f_0 t^{2g+2} \end{cases}$$

を解く. u を消去して,

$$\left(\frac{\sum_{n=0}^{g-1} B_n t^n \sum_{m=0}^{g+1} d_m t^m + \sum_{n=g}^{2g} B_n t^n}{-\sum_{n=0}^{g-1} B_n t^n} \right)^2 = \sum_{n=0}^{2g-2} f_{2g-2-n} t^n$$

$$\left(\sum_{n=0}^{g-1} B_n t^n \sum_{m=0}^{g+1} d_m t^m + \sum_{n=g}^{2g} B_n t^n \right)^2 - \left(\sum_{n=0}^{g-1} B_n t^n \right)^2 \left(\sum_{n=0}^{2g-2} f_{2g-2-n} t^n \right) = 0 \tag{2.14}$$

を得る. (2.14) の右辺を $\Phi(t)$ とおく. $\Phi(t)$ の次数は $4g$ 以下である. (2.13) により

$$\sum_{n=0}^{g-1} B_n t^n (u + \sum_{m=0}^{g+1} d_m t^m) + \sum_{n=g}^{2g} B_n t^n \in L(2gP_0 + 2gP'_0 - gP'_\infty)$$

が成り立つので, $\Phi(t)$ は t^g で割り切れる. $4g$, $4g-1$, $4g-2$ 次の係数は, それぞれ,

$$B_{2g}^2 - B_{g-1}^2 f_0,$$

$$2B_{2g}B_{2g-1} - 2B_{g-1}B_{g-2}f_0 - B_{g-1}^2 f_1,$$

$$B_{2g-1}^2 + 2B_{2g}(B_{2g-2} + d_{g-1}B_{g-1}) - (B_{g-2}^2 + 2B_{g-1}B_{g-3})f_0 - 2B_{g-1}B_{g-2}f_1 - B_{g-1}^2 f_2$$

である. $\Phi(t)$ の係数は $B_i B_j$ の R 線型結合である.

命題 2.15.

$$B_{2g}^2 - B_{g-1}^2 f_0 \equiv 2^{2g} \mod \deg 1$$

が成り立つ. 特に,

$$B_{2g}^2 - B_{g-1}^2 f_0 \in R[[t_1, \ldots, t_{2g}]]^*$$

が成立する.

証明 Vandermonde の公式を用いることにより,

$$\begin{aligned} A'_{2g} &= \det \left[\left[t_i^j (u_i + \textstyle\sum_{n=0}^{g+1} d_n t_i^n) \right]_{\substack{1 \le i \le 2g \\ 1 \le j \le g-1}} \left[t_i^j \right]_{\substack{1 \le i \le 2g \\ g \le j \le 2g-1}} \left[-u_i - \textstyle\sum_{n=0}^{g+1} d_n t_i^n \right]_{\substack{1 \le i \le 2g \\ j = 2g}} \right] \\ &\equiv \det \left[\left[2t_i^j \right]_{\substack{1 \le i \le 2g \\ 1 \le j \le g-1}} \left[t_i^j \right]_{\substack{1 \le i \le 2g \\ g \le j \le 2g-1}} \left[-2 \right]_{\substack{1 \le i \le 2g \\ j = 2g}} \right] \mod \deg g(2g-1)+1 \\ &\equiv 2^g \Delta \mod \deg g(2g-1)+1 \end{aligned}$$

が成り立つ. ただし,

$$\Delta = \det \left[t_i^{j-1} \right]_{\substack{1 \le i \le 2g \\ 1 \le j \le 2g}}$$

とおく. $B_{2g} = A_{2g}/\Delta$ かつ Δ は $g(2g-1)$ 次だから,

$$B_{2g} \equiv -2^g \mod \deg 1 \tag{2.15}$$

を得る. さらに,

$$A'_{g-1} = \det \left[\left[t_i^j (u_i + \textstyle\sum_{n=0}^{g+1} d_n t_i^n) \right]_{\substack{1 \le i \le 2g \\ 1 \le j \le g-2}} \left[-u_i - \textstyle\sum_{n=0}^{g+1} d_n t_i^n \right]_{\substack{1 \le i \le 2g \\ j = g-1}} \left[t_i^j \right]_{\substack{1 \le i \le 2g \\ g \le j \le 2g}} \right]$$

より, A'_{g-1} の最も次数の低い項の全次数は

$$1 + 2 + \cdots + (g-2) + 0 + g + (g+1) + \cdots + 2g = 2g^2 - 1$$

以上となる. したがって,

$$A'_{g-1} \equiv 0 \mod \deg g(2g-1)+1$$

が成り立つ. それゆえ,

$$B_{g-1} \equiv 0 \mod \deg 1 \tag{2.16}$$

が成り立つ. (2.15) と (2.16) により 1 番目の主張が従う. また, 2 が R の単元だから, 2 番目の主張も成り立つ. □

$s_d(z_1, \ldots, z_n)$ を $z_1, \ldots, z_n$ の d 次基本対称式とする. また, $s_0(z_1, \ldots, z_n) := 1$ とおく. $\{t_i\}_{i=1}^{3g}$ は $\Phi(t) = 0$ の根だから,

$$s_1(t_1, \ldots, t_{3g}) = -\frac{2B_{2g}B_{2g-1} - 2B_{g-1}B_{g-2}f_0 - B_{g-1}^2 f_1}{B_{2g}^2 - B_{g-1}^2 f_0}, \ldots$$

が成り立つ.

補題 2.16. 基本対称式 $s_d(t_{2g+1},\dots,t_{3g})$ は $t_1,\dots,t_{2g}$ の R 係数の形式的べき級数となる.

証明 $(-1)^d s_d(t_1,\dots,t_{3g})$ は, $\Phi(t)$ の $4g-d$ 次の係数の最高次の係数による商で表されるので, $s_d(t_1,\dots,t_{3g})$ は, B_iB_j の R 線型結合の $B_{2g}^2 - B_{g-1}^2 f_0$ による商である. 補題 2.15 により, $s_d(t_1,\dots,t_{3g})$ は $t_1,\dots,t_{2g}$ の R 係数の対称式で表される. 公式

$$s_d(t_1,\dots,t_{3g}) = s_d(t_{2g+1},\dots,t_{3g}) + \sum_{i=1}^{d} s_{d-i}(t_1,\dots,t_{2g}) s_i(t_{2g+1},\dots,t_{3g}),$$

により, 帰納的に $s_d(t_{2g+1},\dots,t_{3g}) \in R[[t_1,\dots,t_{2g}]]$ $(1 \le d \le g)$ が得られる. □

$$\xi_1 := \boldsymbol{s}(t_1,\dots,t_g), \quad \xi_2 := \boldsymbol{s}(t_{g+1},\dots,t_{2g})$$

とおく. 形式群 $F(\boldsymbol{x},\boldsymbol{y}) \in R[[\boldsymbol{x},\boldsymbol{y}]]_0^g$ を

$$F(\xi_1,\xi_2) = \boldsymbol{s}(t_{2g+1},\dots,t_{3g})$$

により定義する. このとき, $\hat{J}(\boldsymbol{x},\boldsymbol{y}) = F(\boldsymbol{x},\boldsymbol{y})$ が成り立つ. 補題 2.16 により, 定理 2.12 が成り立つ.

2.3 $\hat{J}(\boldsymbol{x},\boldsymbol{y})$ が $\mathbb{Z}$ 上定義されるための必要十分条件

この節では, $k=\mathbb{Q}$, $R=\mathbb{Z}$ とおく. また, $f_n \in \mathbb{Z}$ $(0 \le n \le 2g+2)$, $f_{2g+2}=1$ を仮定する. さらに, $x^{2g+2} + f_{2g+1}x^{2g+1} + \cdots + f_1 x + f_0$ は重解をもたない, すなわち C は完備非特異代数曲線である, と仮定する.

定理 2.17. 次は同値である.

(1) $\hat{J}(\boldsymbol{x},\boldsymbol{y})$ が $\mathbb{Z}$ 上定義される.

(2) u が $\mathbb{Z}[[t]]$ に属する.

(3) [2] $g+1$ 次以下の $\mathbb{Z}[t]$ の多項式 h が存在し,

$$1 + f_{2g+1}t + \cdots + f_{2g+2}t^{2g+2} \equiv h^2 \bmod 4$$

を満たす.

系 2.18. $g=2$ を仮定する. このとき, $\hat{J}$ が $\mathbb{Z}$ 上定義されるための必要十分条件は, $(f_5,\dots,f_0)$ が 4 を法として次のいずれかに合同になることである.

$$(0,0,0,0,0,0),\ (0,0,2,0,0,1),\ (0,2,0,1,0,0),\ (0,2,2,1,2,1),$$
$$(2,1,0,0,0,0),\ (2,1,2,2,0,1),\ (2,3,2,1,0,0),\ (2,3,0,3,2,1)$$

[2](3) は山内卓也氏（広島大）による.

2.4 計算例：$H(a,b,c)$ のヤコビ多様体上の λ 進表現

超楕円曲線 C として, 橋本-Brumer の曲線族 $H(a,b,c)$ から,

$$H(0,0,0):\ u^2 = 1 - 4t + 2t^2 - 6t^3 + t^4 + 2t^5 + t^6$$

をとる (cf. 橋本 [7]). このとき, $\mathrm{End}_{\mathbb{Q}}(J) \cong \mathbb{Z}[(-1+\sqrt{5})/2]$ が成立し, J は GL_2-type のアーベル多様体になる. さらに, 橋本 [7] により, 次のような可換図式が得られる.

$$\begin{array}{ccccc}
(-1+\sqrt{5})/2 \in \mathbb{Z}[(-1+\sqrt{5})/2] & & \longrightarrow & & \mathrm{End}_{\mathbb{Q}}(J) \\
\Big\downarrow & \Big\downarrow \rho & & & \Big\downarrow \text{pull-back} \\
 & & & & \mathrm{End}_{\mathbb{Q}}(\Omega^1(J)) \\
 & & & & \Big\downarrow \Lambda^* \\
 & & & & \mathrm{End}_{\mathbb{Q}}(\Omega^1(C)) \\
 & & & & \Big\downarrow \omega\text{:fix} \\
\begin{bmatrix} 2 & -5 \\ 1 & -3 \end{bmatrix} & \in & M_2(\mathbb{Z}) & \longrightarrow & M_2(\mathbb{Q})
\end{array}$$

$\sum a_n n^{-s}$ を J の λ 進表現の L 級数とする. このとき, λ のとりかたによらず, a_n は $\mathbb{Z}[(-1+\sqrt{5})/2]$ の元である. 系 2.18 より $\hat{J}(\boldsymbol{x},\boldsymbol{y})$ は $\mathbb{Z}$ 上の形式群である. また, Deninger-Nart [3] により, p が J のよい素点ならば, $\hat{J}(\boldsymbol{x},\boldsymbol{y})/\mathbb{Z}_p$ は特殊元 $pI_2 - \rho(a_p)T + T^2$ に属する. したがって, 定理 2.6 により, $p > 2$ において, 合同式

$$[c(p), -c(2p)] \equiv \rho(a_p) \mod p \tag{2.17}$$

が成り立つ.

合同式 (2.17) の左辺の計算は容易であるが, 右辺の計算は難しい. この合同式は, 正則微分形式の展開係数 $c(n)$ から, λ 進表現の L 級数の係数 a_p を求める合同式と見ることができる.

例えば, $p = 3$ のとき, C の合同ゼータ関数の主要部は,

$$1 + 3z + 7z^2 + 9z^3 + 9z^4 = (1 - \frac{-3+\sqrt{5}}{2}z + 3z^2)(1 - \frac{-3-\sqrt{5}}{2}z + 3z^2)$$

である. したがって,

$$a_3 = \frac{-3+\sqrt{5}}{2} \quad \text{または,} \quad a_3 = \frac{-3-\sqrt{5}}{2}$$

が成り立つ. ρ により行列で表現すると,

$$\rho(a_3) = \begin{bmatrix} 1 & -5 \\ 1 & -4 \end{bmatrix} \quad \text{または,} \quad \rho(a_3) = \begin{bmatrix} -4 & 5 \\ -1 & 1 \end{bmatrix}$$

が成り立つ. しかしながら,

$$[c(3), -c(6)] = \begin{bmatrix} 1 & -86 \\ -2 & 59 \end{bmatrix} \equiv \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \mod 3$$

だから,

$$a_3 = \frac{-3+\sqrt{5}}{2}$$

であることがわかる.

同様に $p = 5$ のとき, C の合同ゼータ関数の主要部は

$$1 + 5z^2 + 25z^4 = (1 - \sqrt{5}z + 5z^2)(1 + \sqrt{5}z + 5z^2)$$

となり, Cartier-Manin 行列は

$$[c(5), -c(10)] = \begin{bmatrix} 25 & -15375 \\ -17 & 9350 \end{bmatrix} \equiv \begin{bmatrix} 0 & 0 \\ -2 & 0 \end{bmatrix} \mod 5$$

で与えられる. したがって,

$$a_5 = -\sqrt{5}$$

が成り立つ.

p を J のよい素点とし, a'_p を a_p の $\mathbb{Q}$ 上の共役とする. $\rho(a_p) \not\equiv \rho(a'_p) \bmod p$ であれば, 上述の方法で a_p を決定することができる.

参考文献

[1] N. Bourbaki, *Éléments de Mathématique, Algébre*, Springer-Verlag Berlin Heidelberg 2007.

[2] J.W.S. Cassels-E.V. Flynn, *Prolegomena to a Middlebrow arithmetic of Curves of Genus 2*, London Math. Soc. Lect. Note **230** (1996), Cambridge University Press.

[3] C. Deninger-E. Nart, *Formal groups and L-series*, Comment Math. Helvetici **65** (1990), 318-333.

[4] E.V. Flynn, *The Jacobian and formal group of a curve of genus two over an arbitary ground field*, Math. Proc. Camb. Phil. Soc. **107** (1990), 425-441.

[5] M.N. Freije, *The formal group of the Jacobian of an algebraic curve*, Pacific J. Math. **157** (1993), 241-255.

[6] D. Grant, *Formal groups in genus two*, J. reine. angew. Math. **411** (1990), 96-121.

[7] K. Hashimoto, $\mathbb{Q}$-*curves of degree 5 and jacobian surfaces of* GL_2-*type*, Manuscripta Math. **98** (1999) 165-182.

[8] T. Honda, *On the theory of commutative formal groups*, J. Math. Soc. Japan **22** (1970) 213-246.

[9] T. Honda, *On the formal structure of the jacobian variety of the Fermat curve over a p-adic integer ring,* Symposia Math. XI (1973) 271-284.

[10] Y. Onishi and S. Yasuda, *Theory of generalized Bernoulli-Hurwitz numbers for algebraic functions of cyclotomic type and universal Bernoulli numbers*, preprint.

[11] A. M. Robert, *A course in p-adic analysis*, Springer GTM 198.

[12] F. Sairaiji, *Formal groups of certain* $\mathbb{Q}$-*curves over quadratic fields*, Osaka J. Math. **39** (2002), 223-243.

[13] F. Sairaiji, *Formal groups of building blocks completely defined over finite abelian extensions of* $\mathbb{Q}$, Bull. London Math. Soc. **38** (2006), 81-92.

[14] J.H. Shilverman, *The arithmetic of elliptic curves*, Springer GTM 106.

[15] Y. Yamamoto, *Suron Nyumon* (in Japanese), Ch. 10, Iwanami Shoten 2003.

Fumio SAIRAIJI
Hiroshima International University,
Hiro, Hiroshima
737-0112, Japan.
e-mail: sairaiji@it.hirokoku-u.ac.jp

第 15 回 整数論サマースクール 報告集, pp.291-328

アーベル多様体の Birch-Swinnerton-Dyer 予想についての話題

安田 正大*

1 ごあいさつ

皆さんお早うございます. 本年度のサマースクールもようやく最終日を迎えました. 本日の私の講演では Birch-Swinnerton-Dyer 予想についてお話しいたします.

Birch-Swinnerton-Dyer 予想とは, 大域体上のアーベル多様体の L 関数の特殊値に関する予想です. この講演ではまず Birch-Swinnerton-Dyer 予想について述べたあと, その予想中に現れる高さ対 (height pairing) や Shafarevich-Tate 群といった概念について説明をします. 特に主偏極アーベル多様体の Shafarevich-Tate 群の位数が平方数になるかどうかの判定条件を与える Poonen-Stoll [44] の結果を紹介します. そのあと強い Birch-Swinnerton-Dyer 予想を玉河数に関する公式として解釈できるという Bloch [5] の結果と, 正標数の大域体の場合の強い Birch-Swinnerton-Dyer 予想に関する加藤-Trihan [26] の結果について解説します.

モジュラ楕円曲線や GL_2 型のアーベル多様体など, 楕円モジュラ曲線と関係するアーベル多様体に関しては, Gross-Zagier [23], Kolyvagin [28], [29], 加藤 [25] などの Birch-Swinnerton-Dyer 予想を支持する重要な結果がいろいろとあります. ひょっとすると皆さんの中には, こういった結果に関する解説を期待しておられた方もいらっしゃるかもしれません. そういった方には大変申し訳ないのですが, これらの結果について本日はほとんど触れません. 触れない理由はふたつあります. 今回のサマースクールのテーマが種数の高い曲線ということですので, 楕円曲線と関連して出てくるような話題をなるべく避けようというのがひとつの理由です. 楕円モジュラ曲線に関する話題はあちこちで耳にする機会があり, 退屈に感じられるかたもいらっしゃるでしょうから, ここでは多くの皆さんにとってあまり聞く機会がないような話をしたいというのがもうひとつの理由です.

この原稿は 2007 年 8 月 24 日に, 第 15 回整数論サマースクールにおいて筆者が行った講演のスライドに加筆・修正を加えたものです. 講演の機会を与えてくださいました大西良博氏にこの場を借りて感謝いたします. 岡崎武生氏と山内卓也氏には, 合宿中の体調の整え方について有益な助言を賜りました. 大坪紀之氏は講演終了後に, スライドにあった誤りをいろいろとご指摘くださいました. 山下剛氏は完成前の原稿を通読し, 沢山あった書き誤りおよび内容に関していくつもの改善すべき点をご指摘くださいました. 小林真一氏は完成直前の原稿にあったいくつもの書き誤りをご指摘くださいました. 五人に対しここに感謝の意を表します.

*京都大学 数理解析研究所

2　記号の準備

本稿を通じて以下の記号・用語を用います.

2.1　集合に関する記号

有限集合 S に対し, S の濃度を $\sharp S$ で表わします.

2.2　記号 $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

記号 $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ で, それぞれ有理整数のなす環, 有理数体, 実数体, 複素数体を表わします. 素数 p に対し, $\mathbb{Z}_p$, $\mathbb{Q}_p$ でそれぞれ p 進整数のなす環, p 進数のなす体を表わします.

2.3　アーベル群に関する記号

アーベル群 M に対し, 以下の記号を用います.

- 記号 M_{tors} で位数が有限の元全体のなす M の部分群を表わします. $M = M_{\mathrm{tors}}$ のとき, M を捻れアーベル群とよびます.
- 整数 m に対し, 記号 $M[m]$ で位数が m の元全体のなす M_{tors} の部分群を表わします.
- 素数 p に対し, 記号 $M\{p\}$ で位数が p 巾の元全体のなす M_{tors} の部分群を表わします. $M_{\mathrm{tors}} = \bigoplus_p M\{p\}$ となることに注意しておきます.
- 記号 $M_{\mathbb{Q}}$ で $\mathbb{Q}$ ベクトル空間 $M \otimes_{\mathbb{Z}} \mathbb{Q}$ を表わします.
- 記号 M_{red} で M を M の最大可除部分群で割った剰余群を表わします.

2.4　関数体

有限体上の一変数代数関数体のことをこの稿では関数体とよびます. 大域体とは代数体または関数体のことです.

2.5　大域体の素点に関する記号

F を大域体, v を F の素点とするとき, F_v で F の v による完備化を表わします. また v における正規化された乗法的付値を $|\ |_v : F_v \to \mathbb{R}$ で表わします. (v が複素素点のときは, $|\ |_v$ を通常の複素数の絶対値の 2 乗となるように正規化します). さらに v が F の有限素点のとき, $\mathcal{O}_v$, k_v, q_v でそれぞれ F_v の整数環, $\mathcal{O}_v$ の剰余体, k_v の位数を表わします.

2.6 大域体の整イデアル

F を代数体とするとき, $\mathcal{O}_F$ で F の整数環を表わします. $\mathcal{O}_F$ のイデアルのことを F の整イデアルとよびます. 0 でない F の整イデアル $\mathfrak{A} \subset \mathcal{O}_F$ に対し, $N(\mathfrak{A}) = \sharp(\mathcal{O}_F/\mathfrak{A})$ とおきます. F を関数体とするとき, F に対応する有限体上の代数曲線 X 上の構造層を $\mathcal{O}_F$ で表わします. $\mathcal{O}_F$ のイデアル層のことを F の整イデアルとよびます. 0 でない F の整イデアル $\mathfrak{A} \subset \mathcal{O}_F$ に対し, $N(\mathfrak{A}) = \sharp(\Gamma(X, \mathcal{O}_F/\mathfrak{A}))$ とおきます.

2.7 スキームに関する記号

スキーム X に対し, X の構造層を $\mathcal{O}_X$ で表わします. X を体 F 上のスキーム, F' を F の拡大体とするとき, $X \times_{\operatorname{Spec} F} \operatorname{Spec} F'$ のことを $X_{F'}$ で表わします.

3 Birch-Swinnerton-Dyer 予想の主張

F を大域体, A を F 上のアーベル多様体とします. A の次元を g とします.

3.1 アーベル多様体の L 関数

Birch-Swinnerton-Dyer 予想とは, A の L 関数 $L(A,s)$ の $s=1$ におけるふるまいに関する予想です. ここで A の L 関数 $L(A,s)$ は Euler 積

$$L(A,s) := \prod_v P_v(A, q_v^{-s})^{-1} \tag{3.1}$$

で与えられる複素数 s についての関数です. 上式 (3.1) の右辺の積において v は F の有限素点を動きます. また §3.2, 3.3 で詳しく述べますが, $P_v(A,T)$ は定数項が 1 の T についてのとある $\mathbb{Z}$ 係数多項式です. Euler 積 (3.1) は $\mathrm{Re}(s) > 3/2$ の範囲で絶対収束します. したがって $L(A,s)$ は同じ範囲で s についての正則関数となります.

予想 3.1. 関数 $L(A,s)$ は全複素平面に正則に解析接続される.

すべての無限素点を含む素点の有限集合 S に対し,

$$L^S(A,s) := \prod_{v \notin S} P_v(A, q_v^{-s})^{-1}.$$

とおきます. また

$$\Lambda(A,s) := \begin{cases} L(A,s)\Gamma_{\mathbb{C}}(s)^{g[F:\mathbb{Q}]}, & F \text{ が代数体のとき} \\ L(A,s), & F \text{ が関数体のとき} \end{cases} \tag{3.2}$$

とおきます. ここで $\Gamma_{\mathbb{C}}(s) = 2\cdot(2\pi)^{-s}\Gamma(s)$ です. このとき 予想 3.1 よりも強く次のことが予想されています.

予想 3.2. 関数 $\Lambda(A,s)$ は全平面に正則に解析接続され, さらに関数等式とよばれる等式

$$\Lambda(A, 2-s) = \pm N(\mathfrak{N}_A)^{s-1}\Lambda(A,s)$$

が成り立つ. ここで $\mathfrak{N}_A$ は A の導手である.

上の予想に現れる A の導手 $\mathfrak{N}_A$ とは A から定まる F の 0 でない整イデアルです. $\mathfrak{N}_A$ の定義は §3.3 で与えます. また予想 3.2 の式に現れる符号を A から具体的に定めることによって予想 3.2 を精密化することもできますが, 本稿ではそれについての詳細も省略します (詳しくは [34], [14], [56] をご参照ください). 予想 3.1, 3.2 は, F が関数体の時には証明されています. F が代数体の場合にはこれらの予想が解かれている場合は今のところあまり多くはなく, 虚数乗法論やモジュラ曲線等を通じて $L(A,s)$ が保型 L 関数と結びつくような場合くらいしかありません.

3.2 多項式 $P_v(A,T)$ の定義 (その 1)

F の各有限素点 v に対し, 多項式 $P_v(A,T)$ は以下のようにして定義されます.

A が v でよい還元 A_v を持つとき. このとき $\mathbb{C}$ 係数の可逆行列 φ_v であって, 任意の有限次拡大 k/k_v に対し $\det(1-\varphi_v^{-[k:k_v]}) = \sharp A_v(k)$ を満たすものが存在します. この φ_v を用いて $P_v(A,T) := \det(1-\varphi_v q_v T)$ と定義します.

v が一般の有限素点のときも, A の Néron モデルの還元の単位元成分を A_v とおくことにより, A が v でよい還元 A_v を持つときと同様の方法で $P_v(A,T)$ を定義します (A の Néron モデルについては §3.4 で説明します).

3.3 多項式 $P_v(A,T)$ の定義 (その 2)

ここ §3.3 では, §3.2 で定義した多項式 $P_v(A,T)$ の別の記述のしかたを紹介します. $\overline{F}$ を F の分離閉包, $G_F = \mathrm{Gal}(\overline{F}/F)$ を F の絶対 Galois 群とします. F の有限素点 v に対し, G_v, I_v, $\mathrm{Frob}_v \in G_v/I_v$ をそれぞれ v における分解群, 惰性群, (幾何的) Frobenius とします. 素数 ℓ であって $v \nmid \ell$ となるものをひとつ固定し, $T_\ell A := \mathrm{Hom}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, A(\overline{F}))$, $V_\ell A := (T_\ell A)_{\mathbb{Q}}$ とおきます. この $T_\ell A$ のことを A の ℓ 進 Tate 加群とよびます. $T_\ell A$, $V_\ell A$ には G_F が連続に作用します. このとき $P_v(A,T)$ は

$$P_v(A,T) := \det(1-\mathrm{Frob}_v q_v T; (V_\ell A)^{I_v}).$$

で与えられます.

この $V_\ell(A)$ を用いると, 予想 3.2 の主張に現れた F の整イデアル $\mathfrak{N}_A$ の定義ができます. $\mathfrak{N}_A$ は F の整イデアルであって, F の各有限素点 v に対し次の条件を満たす唯一のものです.

> k_v の標数と異なる素数 ℓ をとり, G_F の表現 $V_\ell A$ の v における分解群 $G_v \subset G_F$ への制限を $V_{\ell,v} = \mathrm{Res}^{G_F}_{G_v} V_\ell A$ とおくと, 等式
>
> $$\mathrm{ord}_v(\mathfrak{N}_A) = \mathrm{sw}(V_{\ell,v}) + 2g - \dim_{\mathbb{Q}_\ell}(V_{\ell,v})^{I_v} \tag{3.3}$$
>
> が成り立つ.

ここで $\mathrm{sw}(V_{\ell,v})$ は $V_{\ell,v}$ の Swan 導手を表わします. Swan 導手については例えば Serre [50, §19] をご参照ください. [50, §19] では G_v が有限商を経由して作用するような G_v の線型表現のみを取り扱っていますが, v での暴惰性群が $V_{\ell,v}$ に有限商を通じて作用する (Grothendieck [51, APPENDIX]) ことから, [50, §19] の方法で V に対しても Swan 導手を定義できます. 式 (3.3) の右辺を $\mathrm{art}(V_{\ell,v})$ と書くこともあります (群 I_v は $V_{\ell,v}$ に有限商を通じて作用するとは限らないので, [50, §19] にある Artin 導手の定義は $V_{\ell,v}$ に適用できるとは限りません). 整数 $\mathrm{sw}(V_{\ell,v})$ および $\dim_{\mathbb{Q}_\ell}(V_{\ell,v})^{I_v}$ は素数 ℓ のとり方に依存しないことが知られているので, 式 (3.3) の右辺は ℓ に依存しないことに注意しておきます. また, 剰余体 k_v の標数が A の次元 g に比べて十分大きいときは $\mathrm{sw}(V_{\ell,v}) = 0$ となります. した

がってこのとき k_v 上の可換群スキーム A_v^a, A_v^t を後述の式 (3.4) に現れるものとすると, 等式

$$\mathrm{ord}_v(\mathfrak{N}_A) = 2\dim\ A_v^a - \dim\ A_v^t$$

が成り立ちます.

3.4 Néron モデル

本節ではアーベル多様体の Néron モデルについて簡単に説明します.

F が代数体のとき, $X = \mathrm{Spec}\,\mathcal{O}_F$ とおきます. F が関数体のとき, X を F を関数体に持つ有限体上滑らかかつ射影的な代数曲線とします. 以下では X の閉点と F の有限素点とをしばしば同一視します.

$U \subset X$ を空でない開部分スキームとします. このとき U 上のスキーム $\mathcal{A}_U$ であって, 性質

(N) $\mathcal{A}_U$ は U 上滑らか, かつ U 上滑らかな任意のスキーム Y に対し, $\mathcal{A}_U(Y) := \mathrm{Hom}_U(Y, \mathcal{A}_U) \cong A(Y \times_U \mathrm{Spec}\,F)$ が成り立つ.

によって特徴づけられるものが存在します ([40], [9]). この $\mathcal{A}_U$ を A の U 上の Néron モデルとよびます. $U = X$ のとき, 以下では $\mathcal{A}_X$ のことを $\mathcal{A}$ で表わします. $\mathcal{A}_U$ は U 上の可換群スキームの構造を持ちます. U' を連結かつ U 上エタールなスキーム, F' を $\mathcal{O}'_U$ の全商環の大域切断とすると, $\mathcal{A}_U \times_U U'$ は $A \times_{\mathrm{Spec}\,F} \mathrm{Spec}\,F'$ の U' 上の Néron モデルとなります.

3.5 Néron モデルの閉ファイバー

閉点 $v \in X$ に対し $\mathcal{A}$ の v でのファイバーを A_v とおきます. 体 k_v 上の可換群スキームとして A_v は次の標準的なフィルトレーションを持ちます:

$$A_v \supset A_v^o \supset A_v^a \supset A_v^t. \tag{3.4}$$

ここで A_v^o は連結群スキーム, A_v/A_v^o は有限エタール群スキーム, A_v^a は連結アフィン群スキーム, A_v^o/A_v^a はアーベル多様体, A_v^t はトーラス, A_v^a/A_v^t は巾単群スキームです. 素数 ℓ が体 k_v の標数と異なるとき, $T_\ell A_v^o := \mathrm{Hom}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, A_v^o(\overline{k}_v)) \cong T_\ell A^{I_v}$ が成り立ちます. A^* を A の双対アーベル多様体とすると, 完全対 $T_\ell A \times T_\ell A^* \to \mathbb{Z}_\ell(1)$ が存在します. 偏極 $A \to A^*$ によって交代的かつ非退化な双一次形式 $T_\ell A \times T_\ell A \to \mathbb{Z}_\ell(1)$ が得られます. この対に関して, $T_\ell(A_v^t) = T_\ell(A_v^o) \cap T_\ell(A_v^o)^\perp$ が成り立ちます (Grothendieck [59, Exposé IX, Théorème 2.4]).

定義 3.3. v を F の有限素点とする. A が v で良い還元を持つとは, 次の同値な条件を満たすことをいう.

1. A_v はアーベル多様体である.

2. A_v は $\kappa(v)$ 上固有である.

3. $A_v^a = 1$ である.

4. 群 I_v は $T_\ell A$ に自明に作用する.

この 4 条件の同値性については [59, Exposé IX, Corollaire 2.2.9] をご参照ください.

定義 3.4. v を F の有限素点とする. A が v で半安定還元を持つとは, 次の同値な条件を満たすことをいう.

1. $A_v^a = A_v^t$ である.

2. 群 I_v は $T_\ell A/(T_\ell A)^{I_v}$ に自明に作用する.

3. 群 I_v は $T_\ell A$ に巾単に作用する.

この 3 条件の同値性については [59, Exposé IX, Proposition 3.5] をご参照ください.

定義 3.5. $U \subset X$ を空でない開部分集合とする. A が U 上で良い (ないし半安定) 還元を持つとは, A が U のすべての閉点で良い (ないし半安定) 還元を持つことをいう.

定理 3.6 ([59, Exposé IX, Théorème 3.6], [59, Exposé I, Théorème 6.1]). *F を大域体, A を F 上のアーベル多様体とすると, ある有限次分離拡大 F'/F が存在して $A \times_{\operatorname{Spec} F} \operatorname{Spec} F'$ は半安定還元を持つ.*

例 3.7. $A = E$ が楕円曲線の場合, $\mathcal{C}$ を E の X 上の極小正則モデルとすると, E の X 上の Néron モデル $\mathcal{E}$ は $\mathcal{C}$ から, $\mathcal{C}$ の特異ファイバーの滑らかでない部分をすべて取り除いたスキームと同型です. X の閉点における $\mathcal{C}$ のファイバーの形は小平 [27], Néron [40] によって分類されています. また E が具体的に Weierstrass 方程式で与えられているとき, Tate のアルゴリズム [55] により, 方程式の係数から $\mathcal{C}$ の各閉ファイバーの形を容易に決定することができます. 例えば $F = \mathbb{Q}(\sqrt{-1})$, v を 2 の上にある F の唯一の素点, $a \in F$ を $0 \leq \operatorname{ord}_v(a) \leq 3$ を満たす元とし, E を Weierstrass 方程式 $y^2 = x^3 + ax$ で与えられる楕円曲線とすると, $\mathcal{C}$ の v での閉ファイバーの分類は次のようになります.

$\operatorname{ord}_v(a)$	a の合同条件			型	m	f	c
0	$1(v^3)$	$1(v^4)$		I_0^*	5	8	k_v
		$3+2\sqrt{-1}(v^4)$	$3 \pm 2\sqrt{-1}(v^6)$	II^*	9	4	0
			$7 \pm 2\sqrt{-1}(v^6)$	I_0	1	0	0
	$-1(v^3)$	$-1(v^4)$	$-1, 3(v^6)$	I_2^*	7	6	$\mathcal{O}_F/v^2$
			$-1+4\sqrt{-1}, 3+4\sqrt{-1}(v^6)$	I_2^*	7	6	k_v
		$1+2\sqrt{-1}(v^4)$		I_0^*	5	8	0
	$\pm\sqrt{-1}(v^3)$			II	1	12	0
1				III	2	14	k_v
2	$2\sqrt{-1}(v^4)$	$6\sqrt{-1}(v^5)$	$8+6\sqrt{-1}, 4+2\sqrt{-1}(v^7)$	I_4^*	9	10	$\mathcal{O}_F/v^2$
			$6\sqrt{-1}, 12+2\sqrt{-1}(v^7)$	I_4^*	9	10	k_v
		$2\sqrt{-1}(v^5)$	$12+6\sqrt{-1}, 2\sqrt{-1}(v^7)$	I_4^*	9	10	$\mathcal{O}_F/v^2$
			$4+6\sqrt{-1}, 8+2\sqrt{-1}(v^7)$	I_4^*	9	10	k_v
	$2(v^4)$	$2(v^5)$		I_2^*	7	12	k_v
		$6(v^5)$		I_2^*	7	12	$\mathcal{O}_F/v^2$
3				III^*	8	14	k_v

上の表で m は E の極小モデルの特殊ファイバーの幾何的既約成分の個数, $f = \mathrm{ord}_v(\mathfrak{N}_E)$ は E の導手 $\mathfrak{N}_E$ の v での指数, c は $A = E$ に関する群 $A_v/A_v^o(k_v) \subset A_v/A_v^o(\overline{k_v})$ の $\mathcal{O}_F$ 加群としての構造を表わします.

例 3.8. 同じく $A = E$ が楕円曲線の場合, v を F の素点, $\mathcal{C}'$ を E の $\mathcal{O}_v$ 上の極小 Weierstrass 方程式

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

で定義されるモデルとすると, E_v^0 は $\mathcal{C}'$ の閉ファイバーの滑らかな部分と標準的に同型となります. さらに $dx/(2y + a_1x + a_3)$ は $H^0(\mathcal{E} \times_X \mathrm{Spec}\,\mathcal{O}_v, \Omega^1_{\mathcal{E}\times_X \mathrm{Spec}\,\mathcal{O}_v/\mathcal{O}_v})$ の生成元となります ([22]). E が v で極小とは限らない Weierstrass 方程式で与えられているとき, 例 3.7 でふれた Tate のアルゴリズム [55] を使うと v で極小となる E の Weierstrass 方程式を見つけることができます. 例えば例 3.7 持ち出した $F = \mathbb{Q}(\sqrt{-1})$, $v|2$, $E : y^2 = x^3 + ax$, $0 \le \mathrm{ord}_v(a) \le 3$ の場合には, $v \not\equiv 7 \pm 2\sqrt{-1} (\mathrm{mod}\, v^6)$ であれば方程式 $y^2 = x^3 + ax$ は v で極小となり, 残る $v \equiv 7 \pm 2\sqrt{-1} (\mathrm{mod}\, v^6)$ の場合には E は v でよい還元を持ちます.

3.6 Birch-Swinnerton-Dyer 予想の主張

A についての Birch-Swinnerton-Dyer 予想は A の L 関数 $L(A, s)$ の $s = 1$ のふるまいに関する予想です. ところが $L(A, s)$ の定義に現れる Euler 積 (3.1) は $s = 1$ では絶対収束しません. そこでここ §3.6 では, Birch-Swinnerton-Dyer 予想を述べるために $L(A, s)$ について次の仮定をおきます.

(A) $L(A, s)$ は $s = 1$ を含む領域にまで解析接続される.

A の F 有理点の全体 $A(F)$ を A の Mordell-Weil 群とよびます. $A(F)$ は有限生成アーベル群となります ([57]). アーベル群 $A(F)$ の階数を r とおきます. Birch-Swinnerton-Dyer 予想には弱い形のものと強い形のものがありますが, 弱い形の Birch-Swinnerton-Dyer 予想とは次の予想のことです.

予想 3.9 (弱い形の Birch-Swinnerton-Dyer 予想 [4, §1 (A)], [54, §1 (A)]). $\mathrm{ord}_{s=1}L(A, s) = r$.

強い形の Birch-Swinnerton-Dyer 予想は弱い形の予想 3.9 を仮定した上で値

$$L^*(A, 1) := \lim_{s\to 1}(s - 1)^{-r}L(A, s)$$

の精密な記述を与える予想です. この予想を述べるために少し準備をします. まず A の Shafarevich-Tate 群もしくは Tate-Shafarevich 群とよばれるアーベル群 Ш(A) を次で定義します. [1]

$$Ш(A) = \mathrm{Ker}\left[H^1(F, A(\overline{F})) \to \prod_v H^1(F_v, A(\overline{F}_v))\right]. \tag{3.5}$$

ここで F の分離閉包 $\overline{F}$, および F の各素点 v に対する F_v の分離閉包 $\overline{F}_v$ を $\overline{F} \subset \overline{F}_v$ を満たすように固定しました. 群 Ш(A) に関して次の予想がなされています.

[1] 記号 Ш を出力するために東北大学の佐藤篤氏作成の `easywncy.sty` を使用しました.

予想 3.10. $Ш(A)$ は有限群である.

この予想 3.10 のことを Tate-Shafarevich 予想とよぶこともあります.

Birch-Swinnerton-Dyer 予想の主張を述べるためには必要ないのですが, あとで必要となるので A の Selmer 群をここで導入しておきます. 素数 p に対し, Selmer 群 $\mathrm{Sel}_{\mathbb{Q}_p/\mathbb{Z}_p}(A) \subset H^1(F, A(\overline{F})\{p\})$ を準同型

$$H^1(F, A(\overline{F})\{p\}) \to H^1(F, A(\overline{F}))$$

による $Ш(A)$ の逆像として定義します. 整数 $m \geq 1$ に対し, $A(\overline{F})$ の部分群 $A(\overline{F})[m]$ のことを $A[m]$ と書くことにします. 整数 $n \geq 0$ に対し, 短完全系列

$$0 \to A[p^n] \to A(\overline{F}) \xrightarrow{p^n} A(\overline{F}) \to 0$$

より, Galois コホモロジーの長完全系列

$$\cdots \to A(F) \xrightarrow{p^n} A(F) \to H^1(F, A[p^n]) \to H^1(F, A(\overline{F})) \xrightarrow{p^n} H^1(F, A(\overline{F})) \to \cdots$$

が得られます. この完全系列の n についての帰納的極限をとることにより, 短完全系列

$$0 \to A(F) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \to H^1(F, A(\overline{F})\{p\}) \to H^1(F, A(\overline{F}))\{p\} \to 0$$

が得られます. これにより単完全系列

$$0 \to A(F) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_{\mathbb{Q}_p/\mathbb{Z}_p}(A) \to Ш(A)\{p\} \to 0 \tag{3.6}$$

を得ます.

F の各素点 v に対し F_v の Haar 測度 μ_v をほとんど全ての有限素点 v に対し $\mu_v(\mathcal{O}_v) = 1$ を満たすように選びます. このとき $\mu := \prod_v \mu_v$ は $\mathbb{A}_F$ の Haar 測度を定めます. 0 でない $\omega \in H^0(A, \Omega^g_{A/F})$ をひとつとります. $\mathcal{A}$ を A の X 上の Néron モデルとします. F の各有限素点 v に対し, ω が $H^0(\mathcal{A} \times_X \operatorname{Spec} \mathcal{O}_v, \Omega^g_{\mathcal{A}\times_X \operatorname{Spec}\mathcal{O}_v/\mathcal{O}_v})$ の生成元の a_v 倍になるような a_v を選び, $c_v := n_v|a_v|_v \cdot \mu_v(\mathcal{O}_v)^d$ とおきます. ここで $n_v = \sharp(A_v/A_v^o)(k_v)$ です. 各無限素点 v に対し, 実数 c_v を $c_v := \int_{A(F_v)} |\omega|_v \mu_v^d$ によって定めます. 個々の c_v の値は ω のとり方に依存しますが, F の全ての素点 v をわたる積 $\prod_v c_v$ は ω のとり方に依存しないことに注意しておきます.

例 3.11. 例 3.7, 3.8 で説明したことを合わせると, Weierstrass 方程式で与えられている大域体 F 上の楕円曲線 E に対して 値 $\prod_{v\nmid\infty} c_v$ を計算することはさほど困難なくできます.

予想 3.12 (強い形の Birch-Swinnerton-Dyer 予想 [4, §1 (B)], [54, §1 (B)]). 大域体 F 上のアーベル多様体 A に対し予想 *3.9, 3.10* が成り立ち, さらに上の記号の下, 等式

$$L^*(A, 1) = \frac{\prod_v c_v}{\mu(F\backslash\mathbb{A}_F)^g} \cdot \frac{|\mathrm{disc}(h)| \cdot \sharp Ш(A)}{\sharp A(F)_{\mathrm{tors}} \cdot \sharp A^*(F)_{\mathrm{tors}}}$$

が成り立つ. ここで A^* は A の双対アーベル多様体であり, $\mathrm{disc}(h)$ は高さ対 $h(\ ,\ ) : A(F) \times A^*(F) \to \mathbb{R}$ の判別式である.

上の定理に出てきた高さ対 $h(\ ,\ )$ については §4.3 で定義を与えます. また $h(\ ,\ )$ の判別式 $\mathrm{disc}(h)$ とは, 指数有限の部分アーベル群 $B \subset A(F)$, $B' \subset A'(F)$ を B, B' が自由アーベル群になるようにとり, B の基底 $P_1, \ldots, P_r$, B' の基底 $P'_1, \ldots, P'_r$ を選んだとき, 式

$$\frac{\mathrm{disc}(h)}{\sharp(A(F)_{\mathrm{tors}}) \cdot \sharp(A^*(F)_{\mathrm{tors}})} = \frac{|\det(h(P_i, P'_j))|}{\sharp(A(F)/B) \cdot \sharp(A^*(F)/B')}$$

で定まる値のことです.

3.7 より弱い予想

強い形の Birch-Swinnerton-Dyer 予想は特に次の主張を導きます.

1. $L(A,1) \in \prod_{v|\infty} c_v \cdot \mathbb{Q}$.
2. $L^*(A,1) \in \prod_{v|\infty} c_v \cdot \mathrm{disc}(h) \cdot \mathbb{Q}^\times$.

(1), (2) はそれぞれ Deligne の予想 [15, Conjecture 1.8], Beilinson の予想 [2, Conjecture 3.8] の特別な場合です. A が楕円モジュラ曲線のヤコビ多様体の中に現れるアーベル多様体の場合には主張 (1) を確かめることができます.

4 高さ対 (height pairing)

4.1 射影空間の高さ関数

F を大域体とします. $n \geq 1$ を整数, $\mathbb{P}^n$ を F 上の n 次元射影空間とします. $\mathbb{P}^n(F)$ 上の高さ関数 $h : \mathbb{P}^n(F) \to \mathbb{R}$ を, $x = [x_0 : \cdots : x_n] \in \mathbb{P}^n(F)$ に対し

$$h(x) := \frac{1}{[F : \mathbb{Q}]} \sum_v \max_{0 \leq i \leq n} (\log |x_i|_v)$$

とおくことによって定めます. ここで v は F のすべての素点を動きます.

4.2 アーベル多様体上の高さ関数

A を F 上のアーベル多様体とします. $\mathcal{L}$ を A 上の非常に豊富な直線束とし, $n+1 = \dim_F H^0(A, \mathcal{L})$ とおきます. $H^0(A, \mathcal{L})$ の基底を選ぶことにより, 標準的な埋め込み $|\mathcal{L}| : A \to \mathbb{P}^n$ が得られます. $h_{\mathcal{L}} := h \circ |\mathcal{L}| : A(\overline{F}) \to \mathbb{R}$ とおきます. $h_{\mathcal{L}}$ は有界関数の差を除いて $H^0(A, \mathcal{L})$ の基底の選び方に依存しません.

A 上の (非常に豊富とは限らない) 直線束 $\mathcal{L}$ に対しては, A 上の非常に豊富な直線束 $\mathcal{L}_1$, $\mathcal{L}_2$ を用いて, $\mathcal{L}$ を $\mathcal{L} = \mathcal{L}_1 \otimes \mathcal{L}_2^{\otimes -1}$ の形に書きます. $h_{\mathcal{L}} = h_{\mathcal{L}_1} - h_{\mathcal{L}_2}$ とおくと, $h_{\mathcal{L}}$ は有界関数の差を除いて表示 $\mathcal{L} = \mathcal{L}_1 \otimes \mathcal{L}_2^{\otimes -1}$ の取り方に依存しません.

4.3 Néron-Tate の標準的高さ関数

A を F 上のアーベル多様体, $\mathcal{L}$ を A 上の直線束とすると, 関数 $q_{\mathcal{L}} : A(F) \to \mathbb{R}$ であって, 条件

- $q_{\mathcal{L}} - h_{\mathcal{L}}$ は有界.
- $\langle\ ,\ \rangle_{\mathcal{L}} : (x, y) \mapsto \frac{1}{2}(q_{\mathcal{L}}(x+y) - q_{\mathcal{L}}(x) - q_{\mathcal{L}}(y))$ は双加法的.

を満たすものが唯一つ存在します. この関数 $q_{\mathcal{L}}$ を Néron-Tate の標準的高さ関数といいます. さらに $\mathcal{L}$ が対称的, すなわち $(-1)^*\mathcal{L} \cong \mathcal{L}$ であれば $(A(F), q_{\mathcal{L}})$ は $\mathbb{Z}$ 上の 2 次形式となります.

4.4 Néron-Tate の高さ対

$\mathcal{P}$ を $A \times A^*$ 上の Poincaré 直線束とします. $(x, y) \in A(F) \times A^*(F)$ に対し $h(x, y) := q_{\mathcal{P}}(x, y)$ とおきます. $h(\ ,\ ) : A(F) \times A^*(F) \to \mathbb{R}$ は双加法的となります. これを Néron-Tate の高さ対とよびます.

4.5 Néron シンボル

A 上の因子であって, 代数的に 0 と同値であるものの全体を $\mathrm{Div}^0(A)$ とおきます. A の閉点を基底とする自由アーベル群を $Z_0(A)$ で表わし, $Z_0(A)$ の元 $Z = \sum_i n_i P_i$ であって, $\sum_i n_i[\kappa(P_i) : F] = 0$ をみたすもの全体のなす $Z_0(A)$ の部分群を $Z_0(A)^0 \subset Z_0(A)$ で表わします.

$D \in \mathrm{Div}^0(A)$, $Z \in Z_0(A)^0$ が $\mathrm{Supp}(D) \cap \mathrm{Supp}(Z) = \emptyset$ を満たすとします. このとき $h(Z, D)$ は和 $h(Z, D) = \sum_v h(Z, D)_v$ の形に分解されます ([41, §14], [32, THÉORÈME 5]). ここで $h(\ ,\ )_v$ は以下で特徴づけられる関数であり, Néron シンボルとよばれます (以下の特徴づけは Lang [32, THÉORÈME 4] によります).

1. $h(\ ,\ )_v$ は, $D \in \mathrm{Div}^0(A_{F_v})$, $Z \in Z_0(A_{F_v})^0$ であって $\mathrm{Supp}(D) \cap \mathrm{Supp}(Z) = \emptyset$ を満たすものに対し実数 $h(Z, D)_v \in \mathbb{R}$ を対応させる関数である (ここで $\mathrm{Div}^0(A_{F_v})$, $Z_0(A_{F_v})^0$ は $\mathrm{Div}^0(A)$, $Z_0(A)^0$ と同様の方法で定義されるアーベル群である).

2. $h(\ ,\ )_v$ は定義されている範囲で双加法的である.

3. $D = \mathrm{div}(f)$ のとき $h(Z, D)_v = -\log |f(Z)|_v$ が成り立つ. ここで $f(Z)$ は以下で与えられる: $Z = \sum_i n_i P_i \in Z_0(A_{F_v})^0$ とおき, f の $\kappa(P_i)$ における像を $f(P_i)$ で表わすとき, $f(Z) := \prod_i \mathrm{N}_{\kappa(P_i)/F_v}(f(P_i))$.

4. $a \in A(F_v)$ に対し, $t_a : A_{F_v} \xrightarrow{\cong} A_{F_v}$ で a による平行移動を表わすことにすると, $h(Z, D)_v = h(t_a^* Z, t_a^* D)_v$ が成り立つ.

5. 各 $D \in \mathrm{Div}^0(A_{F_v})$, $x_0 \in A(F_v) \setminus \mathrm{Supp}(D)$ に対し, $A(F_v) \setminus \mathrm{Supp}(D)$ 上の関数 $x \mapsto h(x - x_0, D)_v$ は $A(F_v) \setminus \mathrm{Supp}(D)$ の v 進位相に関して局所有界である.

4.6 アーベル多様体でない場合への予想の一般化 (Bloch-Beilinson)

4.6.1 Hasse-Weil L 関数

X を大域体 F 上の滑らかかつ射影的な代数多様体とします. 適当な予想を仮定すると, 整数 $i \geq 0$ に対し, X の Hasse-Weil L 関数とよばれる複素数 s についての関数 $L(h^i(X), s)$ が, 式 (3.1) と同様の Euler 積

$$L(h^i(X), s) := \prod_v P_v(h^i(X), q_v^{-s})^{-1} \tag{4.1}$$

によって定まります. ここで $P_v(h^i(X), T)$ は定数項が 1 の T についてのとある整数係数多項式です. Euler 積 (4.1) は $\mathrm{Re}(s) > 1 + \frac{i}{2}$ で絶対収束します. また (3.2) と類似の補正をすることにより関数 $\Lambda(h^i(X), s)$ を定めることができ (詳細は [49] をご参照ください), 関数 $\Lambda(h^i(X), s)$ について予想 3.2 と同様の予想がなされています.

多項式 $P_v(h^i(X), T)$ は, §3.3 で多項式 $P_v(A, T)$ を定めたときと同様に, k_v の標数と異なる素数 ℓ をとって

$$P_v(h^i(X), T) := \det(1 - \mathrm{Frob}_v T; H^i_{\mathrm{et}}(X_{\overline{F}}, \mathbb{Q}_\ell)^{I_v}) \tag{4.2}$$

とすることによって定めます. 前の段落で適当な予想と述べたものは, 正確には式 (4.2) の右辺が ℓ のとり方に依存しない整数係数の多項式となるという予想です. この予想は X が v でよい還元を持つ場合には証明されています.

4.6.2 Chow 群上の高さ対

X を $\mathbb{Q}$ 上の滑らかかつ射影的な d 次元代数多様体とします. 整数 $n \geq 0$ に対し, X の余次元 n の整型 (integral) 閉部分スキームの集合を基底とする自由アーベル群を $Z^n(X)$ と書きます. $Z^n(X)$ の元を X 上の余次元 n のサイクルとよびます. $Z^n(X)$ を 0 に有理同値なサイクルのなす部分群で割って得られるアーベル群を X の n 次 Chow 群とよび, 記号 $\mathrm{CH}^n(X)$ で表わします. $n = 1$ のとき $\mathrm{CH}^n(X) = \mathrm{Pic}(X)$ となります.

整数 i およびアーベル群 M に対して, $H^i(X(\mathbb{C}), M)$ で複素多様体 $X(\mathbb{C})$ の M 係数 i 次 Betti コホモロジー (特異コホモロジー) を表わします. また整数 i および部分アーベル群 $M \subset \mathbb{C}$ に対し, $M(i) := (2\pi\sqrt{-1})^i M \subset \mathbb{C}$ とおきます. このとき, サイクル写像とよばれる標準的な準同型

$$Z^n(X) \twoheadrightarrow \mathrm{CH}^n(X) \xrightarrow{\mathrm{cl}} H^{2n}(X(\mathbb{C}), \mathbb{Z}(n))$$

が存在します. $Z^n(X)$ の元 Z がホモロジー論的に 0 と同値であるとは, この準同型による Z の $H^{2n}(X(\mathbb{C}), \mathbb{Z}(n))$ における像が 0 になることをいいます. また準同型 cl の核を $\mathrm{CH}^n(X)^0$ とおきます.

X の $\mathbb{Z}$ 上のモデル $\mathfrak{X}$ であって, 正則かつ $\mathbb{Z}$ 上平坦射影的となるものが存在すると仮定します. $1 \leq n \leq d$ とします. Beilinson [3, §4], Bloch [6], Gillet-Soulé [19, THÉORÈME 3 のあとの Remarques] は独立に, とある予想 ([6, Assumption 2], [3, conjecture 2.2.1, conjecture 2.2.3]) を仮定した下で, 高さ対とよばれる双線型写像

$$h(\ ,\ ) : \mathrm{CH}^n(X)^0_{\mathbb{Q}} \times \mathrm{CH}^{d+1-n}(X)^0_{\mathbb{Q}} \to \mathbb{R} \tag{4.3}$$

を構成しました. [3], [6], [19] の構成法はそれぞれ, コホモロジー論的手法, ホモトピー論的手法, Arakelov 幾何的手法に基づくものです. [3] の構成したものと [19] の構成したものは一致することが知られていますが, [6] の定義と [3] の定義とが一致するかどうか筆者は知りません. [19] の方法は後の論文 [20] で数論的 Chow 群の交叉理論という形に結実しました.

本稿では §4.6.4 で [19] の方法に基づいた写像 (4.3) の構成について説明します. 次の §4.6.3 ではその説明に必要な概念をいくつか導入します.

4.6.3 Green カレント

X を $\mathbb{Q}$ 上または $\mathbb{R}$ 上の滑らかかつ射影的な d 次元スキームとします. 整数 $p, q \geq 0$ に対し, $X(\mathbb{C})$ 上の $\mathbb{C}$ 値 (p,q) 形式のなす $\mathbb{C}$ ベクトル空間を $A^{p,q}(X(\mathbb{C}))$ とおきます. $A^{p,q}(X(\mathbb{C}))$ から $\mathbb{C}$ への連続準同型全体のなす $\mathbb{C}$ ベクトル空間を $D_{p,q}(X(\mathbb{C}))$ とおきます. ここでいう連続は Schwartz 超関数を定義する際の連続と同様の意味で用いています. $D^{p,q}(X(\mathbb{C})) := D_{d-p,d-q}(X(\mathbb{C}))$ とおくと, 自然な埋め込み $A^{p,q}(X(\mathbb{C})) \hookrightarrow D^{p,q}(X(\mathbb{C}))$ が

存在します. この埋め込みによって $A^{p,q}(X(\mathbb{C}))$ を $D^{p,q}(X(\mathbb{C}))$ の部分空間とみなします. $D^{p,q}(X(\mathbb{C}))$ の元のことを $X(\mathbb{C})$ 上の (p,q) カレントとよびます.

$$(-1)^{p+q+1}\partial : A^{d-p-1,d-q}(X(\mathbb{C})) \to A^{d-p,d-q}$$

および

$$(-1)^{p+q+1}\overline{\partial} : A^{d-p,d-q-1}(X(\mathbb{C})) \to A^{d-p,d-q}$$

の引き起こす準同型 $D^{p,q}(X(\mathbb{C})) \to D^{p+1,q}(X(\mathbb{C}))$, $D^{p,q}(X(\mathbb{C})) \to D^{p,q+1}(X(\mathbb{C}))$ をそれぞれ $\partial, \overline{\partial}$ で表わします. 複素共役 $F_\infty : X(\mathbb{C}) \xrightarrow{\cong} X(\mathbb{C})$ による微分形式の引き戻しは $\mathbb{C}$ 線型な同型

$$F_\infty^* : A^{p,q}(X(\mathbb{C})) \xrightarrow{\cong} A^{q,p}(X(\mathbb{C})),\ F_\infty^* : D^{p,q}(X(\mathbb{C})) \xrightarrow{\cong} D^{q,p}(X(\mathbb{C}))$$

を引き起こします. 整数 $p \geq 0$ に対し

$$A^{p,p}(X) = \{\omega \in A^{p,p}(X(\mathbb{C})) \mid F_\infty^*\omega = (-1)^p\omega\},$$

$$D^{p,p}(X) = \{T \in D^{p,p}(X(\mathbb{C})) \mid F_\infty^*T = (-1)^pT\}$$

とおきます. 定義により $A^{p,p}(X)$ は $D^{p,p}(X)$ の部分空間とみなせます.

$Y \subset X$ を整型な余次元 p の閉部分スキームとします. $Y(\mathbb{C})$ (の非特異部分) 上で積分するという操作は $D^{p,p}(X)$ の元 δ_Y を定めます. Y の Green カレントとは, $g_Y \in D^{p-1,p-1}(X)$ であって等式

$$\frac{1}{2\pi\sqrt{-1}}\partial\overline{\partial}g_Y - \delta_Y \in A^{p,p}(X)$$

を満たすもののことをいいます. 任意の整型な余次元 p の閉部分スキーム $Y \subset X$ に対して Y の Green カレントが存在することが知られています.

4.6.4 Chow 群上の高さ対の構成

X, d を §4.6.2 の通りとします ($\mathfrak{X}$ の存在も仮定します). $1 \leq n \leq d$ とします. $Z = \sum_i n_iZ_i \in Z^n(X)$, $W = \sum_j m_jW_j \in Z^{d+1-n}(X)$ をホモロジー的に 0 と同値なサイクルとします. $\mathrm{Supp}(Z) \cap \mathrm{Supp}(W) = \emptyset$ と仮定します. $\mathfrak{Z}_i$, $\mathfrak{W}_j$ をそれぞれ Z_i, W_j の $\mathfrak{X}$ における閉包とし,

$$h_f(Z_i, W_j) := \sum_{i',j'}(-1)^{i'+j'}\log(\sharp H^{i'}(\mathfrak{X}, \underline{\mathrm{Tor}}_{j'}^{\mathcal{O}_\mathfrak{X}}(\mathcal{O}_{Z_i}, \mathcal{O}_{W_j}))$$

とおきます. W がホモロジー論的に 0 と同値であることから, 各 j に対し W_j の Green カレント g_{W_j} を, 等式

$$\sum_j m_j\left(\frac{1}{2\pi\sqrt{-1}}\partial\overline{\partial}g_Y - \delta_Y\right) = 0$$

を満たすようにとることができます. そこで各 i, j に対し

$$h_\infty(Z_i, W_j) := -\int_{Z_i(\mathbb{C})} g_{W_j}$$

とおきます. Z, W がホモロジー論的に 0 と同値であることから,

$$\sum_{i,j} n_i m_j h_\infty(Z_i, W_j)$$

が Green カレント g_{W_j} のとり方に依存しないことがわかります. この h_f, h_∞ を用いて $h(Z,W) \in \mathbb{R}$ を

$$h(Z,W) = \sum_{i,j} n_i m_j (h_f(Z_i, W_j) + h_\infty(Z_i, W_j))$$

によって定めます. 適当な予想 ([3, conjecture 2.2.1, conjecture 2.2.3]) を仮定すると, $h(Z,W)$ が Z, W の $\mathrm{CH}^n(X)^0$, $\mathrm{CH}^{d+1-n}(X)^0$ における類にしか依存しないことがわかります.

4.6.5 予想

X, d, $\mathfrak{X}$ を §4.6.2 の通り, $1 \leq n \leq d$ とします.

予想 4.1. n を $0 \leq n \leq d+1$ を満たす整数とすると, $\mathrm{CH}^n(X)^0_{\mathbb{Q}}$, $\mathrm{CH}^{d+1-n}(X)^0_{\mathbb{Q}}$ は有限次元で, $h(\ ,\ ) : \mathrm{CH}^n(X)^0_{\mathbb{Q}} \times \mathrm{CH}^{d+1-n}(X)^0_{\mathbb{Q}} \to \mathbb{R}$ は非退化となる.

予想 4.2 (Swinnerton-Dyer). $\mathrm{ord}_{s=n} L(h^{2n-1}(X), s) = \dim_{\mathbb{Q}} \mathrm{CH}^n(X)^0_{\mathbb{Q}}$ が成り立つ.

複素共役 $F_\infty : X(\mathbb{C}) \xrightarrow{\cong} X(\mathbb{C})$ は自己同型 $F_\infty^* : H^i(X(\mathbb{C}), M) \to H^i(X(\mathbb{C}), M)$ の引き起こします. $\epsilon \in \{\pm 1\}$ に対し, F^* が ϵ 倍で作用する部分を $H^i(X(\mathbb{C}), M)^\epsilon \subset H^i(X(\mathbb{C}), M)$ で表わします.

n を $0 \leq n \leq d+1$ を満たす整数とします. このとき合成

$$I^+ : H^{2n-1}(X(\mathbb{C}), \mathbb{C})^{(-1)^n} \hookrightarrow H^{2n-1}(X(\mathbb{C}), \mathbb{C}) \cong H^{2n-1}_{\mathrm{dR}}(X_{\mathbb{C}}/\mathbb{C}) \twoheadrightarrow H^{2n-1}_{\mathrm{dR}}(X_{\mathbb{C}}/\mathbb{C})/\mathrm{Fil}^n$$

は $\mathbb{C}$ ベクトル空間の同型となります. 同型 I^+ の定義域 $H^{2n-1}(X(\mathbb{C}), \mathbb{C})^{(-1)^n}$ および値域 $H^{2n-1}_{\mathrm{dR}}(X_{\mathbb{C}}/\mathbb{C})/\mathrm{Fil}^n$ は, それぞれ標準的な $\mathbb{Q}$ 構造 $H^{2n-1}(X(\mathbb{C}), (2\pi\sqrt{-1})^n\mathbb{Q})^{(-1)^n}$, $H^{2n-1}_{\mathrm{dR}}(X/\mathbb{Q})/\mathrm{Fil}^n$ を持ちます. そこで $\det I^+ \in \mathbb{C}^\times/\mathbb{Q}^\times$ を以下のようにして定義します: まず $\mathbb{Q}$ ベクトル空間 $H^{2n-1}(X(\mathbb{C}), (2\pi\sqrt{-1})^n\mathbb{Q})^{(-1)^n}$, $H^{2n-1}_{\mathrm{dR}}(X/\mathbb{Q})/\mathrm{Fil}^n$ の基底をとります. この基底を用いて同型 I^+ を $\mathbb{C}$ 係数の正則行列として表示します. この行列の行列式の $\mathbb{C}^\times/\mathbb{Q}^\times$ における類を $\det I^+$ とおきます. $\det I^+$ は $H^{2n-1}(X(\mathbb{C}), (2\pi\sqrt{-1})^n\mathbb{Q})^{(-1)^n}$, $H^{2n-1}_{\mathrm{dR}}(X/\mathbb{Q})/\mathrm{Fil}^n$ の基底の取り方に依存しません. また同型 I^+ が $H^{2n-1}(X(\mathbb{C}), \mathbb{C})^{(-1)^n}$ の $\mathbb{R}$ 部分空間 $H^{2n-1}(X(\mathbb{C}), (2\pi\sqrt{-1})^n\mathbb{R})^{(-1)^n}$ を $H^{2n-1}_{\mathrm{dR}}(X_{\mathbb{R}}/\mathbb{R})/\mathrm{Fil}^n$ に送ることから, $\det I^+$ は $\mathbb{R}^\times/\mathbb{Q}^\times \subset \mathbb{C}^\times/\mathbb{Q}^\times$ に属することがわかります. 次の 2 つの予想はそれぞれ Deligne の予想 [15, Conjecture 1.8], Beilinson の予想 [2, Section 3] の特別な場合です.

予想 4.3 (Deligne の予想 [15, Conjecture 1.8] の特別な場合). $L(h^{2n-1}(X), n) \in \det I^+ \cdot \mathbb{Q}$.

予想 4.4 (Beilinson の予想 [2, Section 3] の特別な場合). $r = \dim_{\mathbb{Q}} \mathrm{CH}^n(X)^0_{\mathbb{Q}}$ とおくと,
$\lim_{s \to n} \frac{L(h^{2n-1}(X), s)}{(s-1)^r} \in \det I^+ \cdot \mathrm{disc}(h) \cdot \mathbb{Q}^\times$.

注 4.5. Beilinson の予想 [2, Section 3] は, 任意の $n \geq 0$, 任意の $m \in \mathbb{Z}$ に対する $L(h^n(X), s)$ の $s = m$ でのふるまいに関する予想です.

注 4.6. Beilinson の予想 [2, Section 3] を Deligne の予想 [15, Conjecture 1.8] の混合モチーフに対するある種の拡張と解釈することもできます ([47]).

5 Shafarevich-Tate 群 $Ш(A)$

F を大域体, A を F 上のアーベル多様体とします. $Ш(A)$ の定義は式 (3.5) に与えたように

$$Ш(A) = \mathrm{Ker}[H^1(F, A(\overline{F})) \to \prod_v H^1(F_v, A(\overline{F}_v))]$$

です. $Ш(A)$ は次のように書くこともできます.

$$\begin{aligned} Ш(A) &= \mathrm{Ker}[H^1(F, A(\overline{F})) \to \textstyle\bigoplus_v H^1(F_v, A(\overline{F}_v))] \\ &= \mathrm{Ker}[H^1(F, A(\overline{F})) \to H^1(F_v, A(\mathbb{A} \otimes \mathbb{Q}\overline{F}))] \\ &= \mathrm{Ker}[H^1(F, A(\overline{F})) \to \textstyle\prod_v H^1(G_v, A(\overline{F}))] \\ &= \mathrm{Ker}[H^1(G_{F,S}, A(F_S)) \to \textstyle\bigoplus_{v\in S} H^1(G_v, A(\overline{F}))] \end{aligned}$$

ここで $\mathbb{A}$ は ($\mathbb{Q}$ の) adele 環, S は F の素点の集合で, 無限素点と悪い素点をすべて含むもの, F_S は S の外不分岐な $\overline{F}/F$ の最大部分拡大体, $G_{F,S} = \mathrm{Gal}(F_S/F)$ です.

定義から $Ш(A)$ は捻れアーベル群です. 上記最後の記述により, $Ш(A)$ の Pontryagin 双対 $Ш(A)^\vee = \mathrm{Hom}(Ш(A), \mathbb{Q}/\mathbb{Z})$ は位相的に有限生成な副有限アーベル群となります. 特に任意の整数 m に対し, $Ш(A)[m]$ は有限群です.

予想 3.10 に述べたように $Ш(A)$ は有限群であると予想されています. $L(A, s)$ が GL_2 の保型 L 関数と結びつくときには, Euler 系の理論を用いると $Ш(A)$ の有限性を証明できる場合があります ([28], [29], [25], [30], [10]).

Cassels-Tate 対 ([11], [53], [39]) $Ш(A) \times Ш(A^*) \to \mathbb{Q}/\mathbb{Z}$ の構成を復習します. 構成には主に以下の 2 通りの方法があります.

5.1 Cassels-Tate 対の構成 (その 1)

$a \in Ш(A)$ とします. P_a を a に対応する A 捻子 (torsor) とし, $Q_a := \overline{F}(P_{a,\overline{F}})^\times/\overline{F}^\times$ とおきます (ここで $P_{a,\overline{F}} = (P_a)_{\overline{F}}$ です). つまり Q_a は $P_{a,\overline{F}}$ の主因子のなすアーベル群です. 短完全系列

$$0 \to Q_a \to \mathrm{Div}^0(P_{a,\overline{F}}) \to \mathrm{Pic}^0(P_{a,\overline{F}}) \to 0$$

および標準的な同型 $\mathrm{Pic}^0(P_{a,\overline{F}}) \cong \mathrm{Pic}^0(A_{\overline{F}}) \cong A^*(\overline{F})$ により, Galois コホモロジーの連結準同型 $H^1(F, A^*(\overline{F})) \to H^2(F, Q_a)$ が得られます. F の各素点 v に対し, $Q_{a,v} = \overline{F}_v(P_{a,\overline{F}_v})^\times/\overline{F}_v^\times$ とおきます. 可換図式

$$\begin{array}{ccc} H^1(F, A^*(\overline{F})) & \longrightarrow & H^2(F, Q_a) \\ \downarrow & & \downarrow \\ \prod_v H^1(F_v, A^*(\overline{F}_v)) & \longrightarrow & \prod_v H^2(F_v, Q_{a,v}) \end{array}$$

により, 準同型

$$Ш(A^*) \to Ш^2(Q_a) := \mathrm{Ker}[H^2(F, Q_a) \to \bigoplus_v H^2(F_v, Q_{a,v})] \tag{5.1}$$

が得られます. 一方, 短完全系列 $0 \to \overline{F}^{\times} \to \overline{F}(P_{a,\overline{F}})^{\times} \to Q_a \to 0$ より図式

$$\begin{array}{ccccccc} & & \mathrm{Br}(F) & \longrightarrow & H^2(F, \overline{F}(P_{a,\overline{F}})^{\times}) & \longrightarrow & H^2(F, Q_a) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \bigoplus_v \mathrm{Br}(F_v) & \longrightarrow & \bigoplus_v H^2(F_v, \overline{F}_v(P_{a,\overline{F}_v})^{\times}) & \longrightarrow & \bigoplus_v H^2(F_v, Q_{a,v}) & & \end{array}$$

が得られます. したがって蛇の補題により準同型

$$Ш^2(Q_a) \to \mathrm{Coker}[\mathrm{Br}(F) \to \bigoplus_v \mathrm{Br}(F_v)] \cong \mathbb{Q}/\mathbb{Z} \tag{5.2}$$

を得ます. 準同型 (5.1) と (5.2) との合成 $Ш(A^*) \to \mathbb{Q}/\mathbb{Z}$ による $a' \in Ш(A^*)$ の行き先を $\langle a, a' \rangle$ とおくことによって $\langle\ ,\ \rangle$ が構成されます.

5.2 Cassels-Tate 対の構成 (その 2)

まず各整数 $m \geq 1$ に対し, 対

$$Ш(A)[m] \times Ш(A^*)[m] \to \mathbb{Q}/\mathbb{Z}$$

を構成します.

$a \in Ш(A)[m]$, $a' \in Ш(A^*)[m]$ とします. $b \in H^1(F, A[m])$, $b' \in H^1(F, A^*[m])$ をそれぞれ a, a' の持ち上げとします. F の素点 v に対し, $b_v \in H^1(F_v, A[m])$ を b の v における分解群 G_v への制限とします. 各 b_v はある $\widetilde{b_v} \in H^1(F_v, A[m^2])$ に持ち上がります. $\beta \in Z^1(F, A[m])$, $\beta' \in Z^1(F, A^*[m])$, $\widetilde{\beta}_v \in Z^1(F_v, A[m^2])$ をそれぞれ b, b', $\widetilde{b_v}$ を代表する 1 コサイクルとします. $\widetilde{\beta} \in C^1(F, A[m^2])$ を β の 1 コチェインとしての持ち上げとすると, $d\widetilde{\beta} \in Z^2(F, A[m])$ となります. ($d\widetilde{\beta}$ の定義から, $d\widetilde{\beta}$ の $H^2(F, A[m])$ における類は Bockstein 準同型 $H^1(F, A[m]) \to H^2(F, A[m^2])$, すなわち短完全系列

$$0 \to A[m] \to A[m^2] \to A[m] \to 0$$

が誘導する Galois コホモロジーの境界準同型 $H^1(F, A[m]) \to H^2(F, A[m^2])$, による b の像に一致します.) $d\widetilde{\beta} \cup \beta' \in Z^3(F, \mathbb{G}_m)$ を考えます. $H^3(F, \mathbb{G}_m) = 0$ よりある $\epsilon \in C^2(F, \mathbb{G}_m)$ が存在して $d\widetilde{\beta} \cup \beta' = d\epsilon$ の形に書けます. $(\widetilde{\beta})_v \in C^1(F_v, A[m^2])$, $\beta'_v \in Z^1(F_v, A^*[m])$, $\epsilon_v \in C^2(F_v, \mathbb{G}_m)$ をそれぞれ $\widetilde{\beta}$, β', ϵ の G_v への制限とします. $\widetilde{\beta}_v - (\widetilde{\beta})_v \in C^1(F_v, A[m])$ となることに注意すると,

$$\gamma_v := (\widetilde{\beta}_v - (\widetilde{\beta})_v) \cup \beta'_v \in C^2(F_v, \mathbb{G}_m)$$

が考えられます. 定義から直ちに $d\gamma_v = d\epsilon_v$ となることがわかるため, $\gamma_v - \epsilon_v$ は $Z^2(F_v, \mathbb{G}_m)$ の元を定めます. そこで

$$\langle a, a' \rangle := \sum_v \mathrm{inv}_v(\gamma_v - \epsilon_v) \in \mathbb{Q}/\mathbb{Z}$$

とおきます. m' が m の倍数のとき, 図式

$$\begin{array}{ccccc} Ш(A)[m] & \times & Ш(A^*)[m] & \xrightarrow{\langle\ ,\ \rangle} & \mathbb{Q}/\mathbb{Z} \\ \downarrow & & \downarrow & & \| \\ Ш(A)[m'] & \times & Ш(A^*)[m'] & \xrightarrow{\langle\ ,\ \rangle} & \mathbb{Q}/\mathbb{Z} \end{array}$$

は可換となります. $Ш(A)$, $Ш(A^*)$ は捻れアーベル群なので, 帰納的極限をとることによって対 $Ш(A)[m] \times Ш(A^*)[m] \to \mathbb{Q}/\mathbb{Z}$ が得られます. この対は §5.1 で構成した対 $\langle\ ,\ \rangle$ と一致します (証明は [44, Section 12] をご参照ください).

定理 5.1 (Cassels [11, Theorem 1.1], Tate [53, THEOREM 3.2]). *Cassels-Tate* 対は完全対

$$Ш(A)_{\mathrm{red}} \times Ш(A^*)_{\mathrm{red}} \to \mathbb{Q}/\mathbb{Z}$$

を誘導する.

5.3 元 $c_\lambda \in Ш(A^*)$

$\lambda : A \to A^*$ を A の偏極とします. λ に対応する $\mathrm{NS}(A_{\overline{F}})^{G_F}$ の元を同じ記号 λ で表わします. λ は準同型 $\lambda_* : Ш(A) \to Ш(A^*)$ を誘導します. この λ_* を用いて双加法的写像

$$\langle\ ,\ \rangle_\lambda : Ш(A) \times Ш(A) \to \mathbb{Q}/\mathbb{Z}$$

を $\langle a, b\rangle_\lambda := \langle a, \lambda_*(b)\rangle$ によって定義します.

短完全系列

$$0 \to A^*(\overline{F}) \to \mathrm{Pic}(A_{\overline{F}}) \to \mathrm{NS}(A_{\overline{F}}) \to 0$$

が誘導する Galois コホモロジーの連結準同型 $\mathrm{NS}(A_{\overline{F}})^{G_F} \to H^1(F, A^*(\overline{F}))$ を考えます. この連結準同型による $\lambda \in \mathrm{NS}(A_{\overline{F}})^{G_F}$ の行き先を $c_\lambda \in H^1(F, A^*(\overline{F}))$ とおきます.

注 5.2. $\mathcal{L}$ を $A \times A^*$ 上の Poincaré 直線束の $(\mathrm{id}, \lambda) : A \to A \times A^*$ による引き戻しとすると, $\mathcal{L}$ の定める射 $A \to A^*$ は 2λ に一致します. このことより $2c_\lambda = 0$ であることがわかります.

命題 5.3 (Poonen-Stoll [44, Corollary 2]). 上で定めた $c_\lambda \in H^1(F, A^*(\overline{F}))$ は $Ш(A^*) \subset H^1(F, A^*(\overline{F}))$ に属する.

(証明) v を F の素点とします. 短完全系列

$$0 \to A^*(\overline{F}_v) \to \mathrm{Pic}(A_{\overline{F}_v}) \to \mathrm{NS}(A_{\overline{F}_v}) \to 0 \tag{5.3}$$

が誘導する Galois コホモロジーの連結準同型 $\mathrm{NS}(A_{\overline{F}_v})^{G_v} \to H^1(F_v, A^*(\overline{F}_v))$ が 0 準同型であることをいえば十分です. 簡単のため v を有限素点とします. Tate [53] の双対性が引き起こす同型 $H^1(F_v, A^*(\overline{F}_v)) \xrightarrow{\cong} \mathrm{Hom}_{\mathrm{cont}}(A(F_v), \mathbb{Q}/\mathbb{Z})$ は $H^1(F_v, A^*(\overline{F}_v)) \to H^1(F_v, \mathrm{Pic}(A_{\overline{F}_v}))$ の像を経由するので, $H^1(F_v, A^*(\overline{F}_v)) \to H^1(F_v, \mathrm{Pic}(A_{\overline{F}_v}))$ は単射です. したがって, 短完全系列 (5.3) が誘導する Galois コホモロジーの長完全系列から求める主張が得られます. □

定理 5.4 (Poonen-Stoll [44, Theorem 5]). A を大域体 F 上の偏極アーベル多様体, $\lambda : A \to A^*$ を A の偏極とする. $c_\lambda \in Ш(A^*)$ を上で定めた元とする. このとき任意の $a \in Ш(A)$ に対し, $\langle a, a\rangle_\lambda = \langle a, c_\lambda\rangle$ が成り立つ.

(証明) $a \in Ш(A)$ とします. P を a に対応する A 捻子とします. $D \in \mathrm{Div}(A_{\overline{F}})$ を, λ を与える因子とします. $x \in P(\overline{F})$ を取ります. 原点を x に送ることにより同型 $A_{\overline{F}} \cong P_{\overline{F}}$ を得ます. $D' \in \mathrm{Div}(P_{\overline{F}})$ を, この同型のもと D に対応する因子とします. このとき $\lambda(a) - c_\lambda$ は 1 コサイクル

$$G_F \ni \sigma \mapsto \sigma(D') - D' \in \mathrm{Pic}^0(P_{\overline{F}}) \cong \mathrm{Pic}^0(A_{\overline{F}})$$

の類に一致します. したがって $\langle\ ,\ \rangle$ の定義により, $\langle a, \lambda(a) - c_\lambda\rangle = 0$ が成り立ちます. □

系 5.5 (Poonen-Stoll [44, Corollary 6]). $\langle\ ,\ \rangle_\lambda$ は反対称である, すなわち $\langle a, b\rangle = -\langle b, a\rangle$ が成り立つ.

A が主偏極 $\lambda : A \xrightarrow{\cong} A^*$ をもつとき, λ は完全対 $\langle\ ,\ \rangle_\lambda : Ш(A)_{\mathrm{red}} \times Ш(A)_{\mathrm{red}} \to \mathbb{Q}/\mathbb{Z}$ を誘導します. したがって各素数 $p \geq 3$ に対し $\sharp Ш(A)_{\mathrm{red}}\{p\}$ は平方数となります. 特に $Ш(A)_{\mathrm{red}}$ が有限群であれば, $\sharp Ш(A)_{\mathrm{red}}$ は平方数または平方数の 2 倍です.

系 5.6 (Poonen-Stoll [44, Theorem 8] の一部分). A が主偏極 $\lambda : A \xrightarrow{\cong} A^*$ を持つとし, $c := \lambda^{-1}(c_\lambda)$ とおく. このとき, $\sharp Ш(A)_{\mathrm{red}}\{2\}$ が平方数であることと $\langle c, c\rangle_\lambda = 0$ となることとは同値である.

5.4 曲線のヤコビ多様体の場合

C を F 上滑らか射影的かつ幾何学的に連結な代数曲線とします. g を C の種数, $J = \mathrm{Jac}(C)$ を C のヤコビ多様体とします.

J は標準的な主偏極 $\lambda : J \to J^*$ をもちます. この λ はテータ因子 $\Theta \subset \mathrm{Pic}^{g-1}_{C/F}$ を同型 $J_{\overline{F}} \cong (\mathrm{Pic}^{g-1}_{C/F})_{\overline{F}}$ で引き戻した $J_{\overline{F}}$ 上の因子によって与えられます. このことより $c = [\mathrm{Pic}^{g-1}_{C/F}]$ であることがわかります.

$\langle c, c\rangle_\lambda$ の計算を行います. F の各素点 v に対し, 図式

$$1 \to \overline{F}_v^\times \to \overline{F}_v(C_{\overline{F}_v})^\times \to \mathrm{Div}(C_{\overline{F}_v}) \to \mathrm{Pic}(C_{\overline{F}_v}) \to 0 \tag{5.4}$$

を考えます $c = [\mathrm{Pic}^{g-1}_{C/F}] \in Ш(J)$ であることから, F_v 有理点 $x_v \in \mathrm{Pic}^{g-1}_{C/F}(F_v)$ が存在します. 1 を x_v に送る準同型 $\mathbb{Z} \to \mathrm{Pic}(C_{\overline{F}_v})$ によって図式 (5.4) を引き戻すことにより, $H^2(F_v, \overline{F}_v^\times)$ の元が得られます. したがって標準的な同型 $H^2(F_v, \overline{F}_v^\times) \cong \mathbb{Q}/\mathbb{Z}$ により元 $\phi_v(x_v) \in \mathbb{Q}/\mathbb{Z}$ が得られます.

命題 5.7. このとき $\langle c, c\rangle_\lambda = (1-g)\sum_v \phi_v(x_v)$ が成り立つ. □

命題 5.8. $(2g-2)\phi_v(x_v) = 0$ が成り立つ. さらに $(g-1)\phi_v(x_v) = 0$ であるための必要十分条件は $\mathrm{Pic}^{g-1}(C_{F_v})$ が空集合でないことである. □

$\mathrm{Pic}^{g-1}(C_{F_v})$ は $\mathrm{Pic}^{g-1}_{C/F}(F_v)$ の部分集合とみなせますが, 両者は必ずしも一致しないことに注意しておきます.

系 5.9 (Poonen-Stoll [44, Theorem 11]). $Ш(J)_{\mathrm{red}}\{2\}$ が平方数となるための必要十分条件は $\mathrm{Pic}^{g-1}(C_{F_v}) = \emptyset$ となる F の素点 v がちょうど偶数個存在することである.

系 5.9 より特に C が F 有理点をもてば, $Ш(J)_{\mathrm{red}}\{2\}$ は平方数となります.

注 5.10. v を F の有限素点, $\mathcal{C}$ を C_{F_v} の極小正則固有モデル, Y を $\mathcal{C}$ の閉ファイバーとすると,

$$\{n \in \mathbb{Z} \mid \mathrm{Pic}^n(C_{F_v}) \neq \emptyset\} = \sum_{E \in \mathrm{Irr}(Y_{\mathrm{red}})} m_E f_E \mathbb{Z}$$

が成り立ちます. ここで m_E は Y における E の重複度であり, f_E は E の関数体の定数体の k_v 上の次数です.

系 5.9 を用いると $Ш(J)_{\mathrm{red}}\{2\}$ が平方数にならないような C の例を構成することができます. 以下にそのような C の例をいくつか挙げます. 論文 [44, Section 10] では, 下に挙げるもの外にもいくつか例が与えられています.

例 5.11 (Poonen-Stoll [44, Proposition 26]). g を 2 以上の整数, t を正の整数とすします. 式 $y^2 = -(x^{2g+2} + x + t)$ で与えられる $\mathbb{Q}$ 上の種数 g の超楕円曲線を C とすると, $Ш(J)_{\mathrm{red}}\{2\}$ は平方数になりません.

例 5.12 (Jordan-Livné [24, Theorem 1]). p, q を $p \equiv 5 (\mathrm{mod}\, 24)$, $q \equiv 5 (\mathrm{mod}\, 12)$, $\left(\frac{p}{q}\right) = -1$ を満たす異なる 2 つの素数とします. 判別式 pq の $\mathbb{Q}$ 上の 4 元数環に付随する志村曲線を Atkin-Lehner 対合 w_p の作用で割った曲線を C とすると, $Ш(J)_{\mathrm{red}}\{2\}$ は平方数になりません.

5.5 Bloch-加藤 [7, Section 5] による $Ш(A)$ の記述

$Ш(A)$ は捻れアーベル群なので, 標準的な直和分解

$$Ш(A) = \bigoplus_{\ell:\text{素数}} Ш(A)\{\ell\}$$

を持ちます. 以下 §5.5 では $\ell \neq \mathrm{char}(F)$ と仮定します. F の各有限素点 v に対し, $p := \mathrm{char}(k_v)$ とおき, 部分空間 $H^1_f(F_v, V_\ell A) \subset H^1(F_v, V_\ell A)$ を以下で定めます:

$$H^1_f(F_v, V_\ell A) = \begin{cases} \mathrm{Ker}[H^1(F_v, V_\ell A) \to H^1(I_v, V_\ell A)], & p \neq \ell \text{ のとき}, \\ \mathrm{Ker}[H^1(F_v, V_\ell A) \to H^1(F_v, V_\ell A \otimes_{\mathbb{Q}_\ell} B_{\mathrm{crys}})], & p = \ell \text{ のとき}. \end{cases}$$

ここで B_{crys} とは Fontaine [16, p. 554] が導入した $G_{\mathbb{Q}_p} = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ が連続に作用する $\mathbb{Q}_p$ 代数 B のことです (ここでは Fontaine [16] の記号で $K = \mathbb{Q}_p$ の場合を考えています). さらに部分空間 $H^1_f(F, V_\ell A) \subset H^1(F, V_\ell A)$ を以下のように定めます:

$$H^1_f(F, V_\ell A) = \mathrm{Ker}\left[H^1(F, V_\ell A) \to \prod_{v \nmid \infty} \frac{H^1(F_v, V_\ell A)}{H^1_f(F_v, V_\ell A)} \right].$$

$A\{\ell\} := A(\overline{F})\{\ell\} \cong V_\ell A/T_\ell A$ とおきます. F の各有限素点 v に対し, 部分アーベル群 $H^1_f(F_v, A\{\ell\}) \subset H^1(F_v, A\{\ell\})$ を以下のように定めます:

$$H^1_f(F_v, A\{\ell\}) := \mathrm{Im}[H^1_f(F_v, V_\ell A) \hookrightarrow H^1(F_v, V_\ell A) \to H^1(F_v, A\{\ell\})].$$

さらに部分アーベル群 $H^1_f(F, A\{\ell\}) \subset H^1(F, A\{\ell\})$ を以下のように定めます:

$$H^1_f(F, A\{\ell\}) := \mathrm{Im}[H^1_f(F, V_\ell A) \hookrightarrow H^1(F, V_\ell A) \to H^1(F, A\{\ell\})].$$

このとき $H^1(F, A\{\ell\})$ の部分群として等式

$$\mathrm{Sel}_{\mathbb{Q}_\ell/\mathbb{Z}_\ell}(A) = \mathrm{Ker}\left[H^1(F, A\{\ell\}) \to \prod_v \frac{H^1(F_v, A\{\ell\})}{H^1_f(F_v, A\{\ell\})}\right]$$

が成り立ちます. この等式と短完全系列 (3.6) から同型

$$Ш(A)\{\ell\}_{\mathrm{red}} \cong \mathrm{Ker}\left[\frac{H^1(F, A\{\ell\})}{H^1_f(F, A\{\ell\})} \to \prod_v \frac{H^1(F_v, A\{\ell\})}{H^1_f(F_v, A\{\ell\})}\right] \tag{5.5}$$

が得られます. 式 (5.5) を用いれば, G_F の表現 $T_\ell A$ だけを用いて ($A(\overline{F})$ などを用いずに) $Ш(A)_{\mathrm{red}}$ を定義できます. これによって, より一般の (例えば 重さ -1 のモチーフに付随する) Galois 表現に対して, 強い形の Birch-Swinnerton-Dyer 予想を一般化した予想を定式化できます (詳細は [7], [17] をご参照ください). 特に予想 4.4 を強い形の Birch-Swinnerton-Dyer 予想 3.12 と類似の形に精密化できます.

6 Birch-Swinnerton-Dyer 予想と玉河数の公式

6.1 アフィン代数群 G の玉河数

大域体 F 上のアフィン代数群 G に対し, G の玉河数と呼ばれる実数 $\tau(G)$ が以下の方法で定義されます.

$$G(\mathbb{A}_F)^1 := \{g \in G(\mathbb{A}_F) \mid \text{任意の } \chi : G \to \mathbb{G}_m \text{ に対し } |\chi(g)| = 1\}$$

とおきます. $G(\mathbb{A}_F)^1$ はユニモジュラーな局所コンパクト位相群であり, $G(F)$ は $G(\mathbb{A}_F)^1$ の離散部分群となります. $\mathbb{A}_F$ の Haar 測度 μ であって, $\mu(F\backslash\mathbb{A}_F) = 1$ を満たすものをとります. μ を用いて $\mathrm{Lie}\, G(\mathbb{A}_F)$ の Haar 測度 $\mu_{\mathrm{Lie}\, G}$ を標準的に定めます. この測度を用いて $G(\mathbb{A}_F)$ の Haar 測度 μ_G が標準的に定まります. 以下に μ_G を定める手続きの概略を書きます (詳細は [58] をご参照ください). まず測度 $\mu_{\mathrm{Lie}\, G}$ の, F の各素点 v に対する $\mathrm{Lie}\, G(F_v)$ の Haar 測度 $\mu_{\mathrm{Lie}\, G,v}$ の積 $\mu_{\mathrm{Lie}\, G} = \prod_v \mu_{\mathrm{Lie}\, G,v}$ への分解をひとつとります. 次に F の各素点 v に対し, $G(\mathbb{F}_v)$ の左不変 Haar 測度 $\mu_{G,v}$ を, この $\mu_{\mathrm{Lie},\, G,v}$ を用いて標準的に定めます. F が代数体の場合は, 単位元の近傍で定義される局所同型写像 $\exp : \mathrm{Lie}\, G(F_v) \dashrightarrow G(F_v)$ を通じて, $\mu_{\mathrm{Lie}\, G}$ と $\mu_{G,v}$ とが対応します. このとき $G(\mathbb{A}_F)$ 上の測度 μ_G は, いわば $\mu_{G,v}$ たちの「直積」とでもいうべきものになります. 但し $\mu_{G,v}$ の直積を素直に定義しようとすると収束しない無限積が現れるため, 実際の $\mu_{G,v}$ の構成は以下のように行います: $X(G) = \underline{\mathrm{Hom}}_F(G, \mathbb{G}_m)$ とおきます. ここで $\underline{\mathrm{Hom}}_F$ は $\mathrm{Spec}\, F$ 上の適当な位相に関する群の層のなす圏における $\underline{\mathrm{Hom}}$ です. $X(G)$ は群 G_F が有限商を経由して作用する有限生成自由アーベル群とみなせます. そこで $X(G)$ の Artin L 関数

$$L(X(G), s) = \prod_v L_v(X(G), s)$$

を考えます. F の各素点 v に対し正の実数 $\lambda_v > 0$ を, ほとんど全ての v に対し $\lambda_v = L_v(X(G), 1)^{-1}$ となるようにとります. λ_v を v での収束因子とよびます. F の各素点 v に対し $G(F_v)$ の測度 $\mu'_{G,v}$ を $\mu'_{G,v} = \lambda_v \mu_{G,v}$ で定めると, 直積測度 $\mu'_G = \prod_v \mu'_{G,v}$ を定めることができます. この μ'_G と $G(\mathbb{A}_F)/G(\mathbb{A}_F)^1$ 上の標準的な測度を用いて, $G(\mathbb{A}_F)^1$ に Haar 測度 $\mu'_{G,1}$ が定まります. 最後に, $\prod_v \lambda_v$ の代わりとなる実数 λ を $L(X(G), s)$ の $s = 1$ での先頭項を用いて定義することにより, $G(\mathbb{A}_F)^1$ に標準的な Haar 測度 $\mu_{G,1} = \lambda^{-1}\mu'_{G,1}$ が定まりますこの測度 $\mu_{G,1}$ による $G(F)\backslash G(\mathbb{A}_F)^1$ の体積

$$\tau(G) = \mu_{G,1}(G(F)\backslash G(\mathbb{A}_F)^1)$$

のことを G の玉河数とよびます (Borel [8, THEOREM 1] により $\tau(G) < \infty$ となることに注意しておきます). アーベル多様体に対する Shafarevich-Tate 群の定義 (3.5) と同様に

$$Ш(G) = \mathrm{Ker}[H^1(F, G) \to \prod_v H^1(F_v, G)]$$

によって G の Shafarevich-Tate 群 $Ш(G)$ を定義します. このとき次の定理が成り立ちます.

定理 6.1 ([42], [45], [31], [13], [43]). G を代数体 F 上の連結アフィン代数群, $G_u \subset G$ を G の巾単根基とする. このとき $Ш(G)$ は有限群であり, 公式

$$\tau(G/G_u) = \frac{\sharp \mathrm{Pic}(G)}{\sharp Ш(G)}$$

が成り立つ.

6.2 強い形の Birch-Swinnerton-Dyer 予想の玉河数を用いた定式化 (Bloch [5])

F を代数体, A を F 上のアーベル多様体とします. $\tau(G)$ の定義の際にとある L 関数の特殊値が現れること, および $\mathrm{Pic}(A)_{\mathrm{tors}}$ が $A^*(F)$ と同型であることに注意すると, A についての強い形の Birch-Swinnerton-Dyer 予想 3.12 の主張と上の定理 6.1 の主張の間に類似性が見てとれますそもそも強い形の Birch-Swinnerton-Dyer 予想が定式化された背景のひとつに, トーラスの玉河数に関する公式の影響があります ([4], [12]). このことをふまえて, 強い形の Birch-Swinnerton-Dyer 予想を定理 6.1 とそっくりな形に再定式化したのが Bloch [5] です. 以下この節ではこの Bloch の結果を概説します.

$A(\mathbb{A}_F)$ はコンパクトなので, $A(F)$ が無限群のときは $A(F)$ は $A(\mathbb{A}_F)$ の離散部分群になりません. そのため $A(F)$ が無限群のときは, 定理 6.1 の主張中の G を単純に A で置き換えただけでは, $\tau(A)$ の定義の際に困難が生じてうまくいきません. そこで次のようにします.

$B \subset A^*(F)$ を指数有限かつ捻れを持たない部分群とします. $T = \underline{\mathrm{Hom}}_F(B, \mathbb{G}_m)$ とおきます. ここで式 (6.1) の右辺は $\mathrm{Spec}\, F$ 上の適当な Grothendieck 位相におけるアーベル群の層のなす圏における $\underline{\mathrm{Hom}}$ を表わすものとします. T は F 上の分裂トーラスとなります.

よく知られているように標準的な同型

$$A^* \cong \underline{\mathrm{Ext}}^1_F(A, \mathbb{G}_m) \tag{6.1}$$

が存在します. ここで式 (6.1) の右辺は F 上の適当な Grothendieck 位相におけるアーベル群の層のなすアーベル圏における $\underline{\mathrm{Ext}}^1$ を表わすものとします. 式 (6.1) により, F 上の群スキームの拡大

$$1 \to T \to G \to A \to 1$$

が得られます. イデールノルム $|\ |: F^\times \backslash \mathbb{A}_F^\times \to \mathbb{R}$ の引き起こす準同型 $T(F)\backslash T(\mathbb{A}_F) \cong \mathrm{Hom}(B, F^\times \backslash \mathbb{A}_F^\times) \to \mathrm{Hom}(B, \mathbb{R})$ は一意的に連続準同型 $T(F)\backslash G(\mathbb{A}_F) \to \mathrm{Hom}(B, \mathbb{R})$ に延ばせます (このことは後の §6.3 に書くことを用いると示せます詳細は [5, p. 68] はご参照ください). $A(F) \cong T(F)\backslash G(F) \hookrightarrow T(F)\backslash G(\mathbb{A}_F) \to \mathrm{Hom}(B, \mathbb{R}) \cong \mathrm{Hom}(A^*(F), \mathbb{R})$ により, $\langle\ ,\ \rangle : A(F) \times A^*(F) \to \mathbb{R}$ が得られます. この節の話題で鍵となるのが次の定理です.

定理 6.2 ([5, (1.9) Theorem]). $\langle\ ,\ \rangle$ は高さ対 $h(\ ,\ )$ と一致する.

系 6.3 (Bloch [5, (1.10) Theorem]). $G(F) \subset G(\mathbb{A}_F)$ は離散的かつ余コンパクトな部分群となる.

ここで §3.6 の (A) を仮定します. G はアフィンではありませんが, 上の系を用いると G の玉河数 $\tau(G)$ が, アフィン代数群の場合と同様に定義できます.

定理 6.4 (Bloch [5, (1.17) Theorem]). *A を大域体 F 上のアーベル多様体とし, G を上の通りとする. A について §3.6 の (A), および予想 3.9, 3.10 を仮定する. このとき, A についての強い形の Birch-Swinnerton-Dyer 予想 3.12 は等式*

$$\tau(G) = \frac{\sharp \mathrm{Pic}(G)_{\mathrm{tors}}}{\sharp Ш(G)}$$

と同値である.

6.3 定理 6.4 の証明の準備

$X = \operatorname{Spec} \mathcal{O}_F$ とおきます. $\mathcal{A}$, $\mathcal{A}^*$ をそれぞれ A, A^* の X 上の Néron モデルとします. $\mathcal{A}^o \subset \mathcal{A}$ を開部分群で各ファイバーが連結なものとします. このとき (6.1) の拡張となる標準的な同型

$$\mathcal{A}^* \cong \underline{\mathrm{Ext}}^1_X(\mathcal{A}^o, \mathbb{G}_m) \tag{6.2}$$

が存在します ([35, §5]). ここで (6.2) の右辺は X 上の適当な Grothendieck 位相に関するアーベル群の層の圏における $\underline{\mathrm{Ext}}^1$ です.

$B \subset A^*(F) \cong \mathcal{A}^*(X)$ より $\mathcal{T} = \underline{\mathrm{Hom}}_X(B, \mathbb{G}_m)$ は X 上の分裂トーラスとなります. 式 (6.2) を用いると, X 上の群スキームの拡大

$$1 \to \mathcal{T} \to \mathcal{G} \to \mathcal{A}^o \to 1 \tag{6.3}$$

が得られます.

6.4 定理 6.2 を認めた定理 6.4 の証明

(証明) $T(F)\backslash T^1$ を $T(F)\backslash T(\mathbb{A}_F)$ の極大コンパクト部分群, $T(F)\backslash G^1$ を $T(F)\backslash G(\mathbb{A}_F)$ の極大コンパクト部分群とします. A, T, G に対する収束因子 $(\lambda_{A,v})$, $(\lambda_{T,v})$, $(\lambda_{G,v})$ を

- v が有限素点のとき

$$\lambda_{A,v} = P_v(A, q_v^{-1}),\ \lambda_{T,v} = (1 - q_v^{-1})^r,\ \lambda_{G,v} = (1 - q_v^{-1})^r P_v(A, q_v^{-1}).$$

- v が無限素点のとき $\lambda_{T,v} = \lambda_{A,v} = \lambda_{G,v} = 1$.

と選びます. ここで $A(F)$ の階数を r とおきました. これらの収束因子から定まる $A(\mathbb{A}_F)$, T^1, $G(\mathbb{A}_F)$, G^1 の Haar 測度をそれぞれ μ'_A, $\mu'_{T,1}$, μ'_G, $\mu'_{G,1}$ とおきます. 完全系列

$$1 \to T(F)\backslash T^1 \to T(F)\backslash G^1 \to A(\mathbb{A}_F) \to 0$$

および $T^1\backslash T(\mathbb{A}_F) \cong G^1\backslash G(\mathbb{A}_F)$ に注意し, 式 (6.3) より F の各素点 v に対して

$$0 \to \mathcal{T}(\mathcal{O}_{F_v}) \to \mathcal{G}(\mathcal{O}_{F_v}) \to \mathcal{A}^o(\mathcal{O}_{F_v}) \to 0$$

が完全になることを用いると, $\mu'_{G,1}(T(F)\backslash G^1) = \mu'_A(A(\mathbb{A}_F))\mu'_{T,1}(T(F)\backslash T^1)$ となります. さらに完全系列

$$0 \to A(F)_{\mathrm{tors}} \to T(F)\backslash G^1 \to G(F)\backslash G(\mathbb{A}_F) \to \frac{\mathrm{Hom}(B,\mathbb{R})}{A(F)/A(F)_{\mathrm{tors}}} \to 0$$

と定理 6.2 とを用いると

$$\mu'_G(G(F)\backslash G(\mathbb{A}_F)) = \frac{\mu'_A(A(\mathbb{A}_F))\mu'_{T,1}(T(F)\backslash T^1)\cdot \mathrm{disc}(h)\cdot \sharp(A^*(F)/(B+A^*(F)_{\mathrm{tors}}))}{\mu(F\backslash \mathbb{A}_F)^g \sharp A(F)_{\mathrm{tors}}}$$

がわかります. ここで

$$\mu'_A(A(\mathbb{A}_F)) = \prod_v c_v,\ \mu'_{T,1}(T(F)\backslash T^1) = (\lim_{s\to 1}(s-1)\zeta_F(s))^r$$

(但し上式の $\prod_v c_v$ は強い Birch-Swinnerton-Dyer 予想 3.12 の主張中に表れる値, $\zeta_F(s)$ は F の Dedekind ζ 関数です) に注意すると,

$$\mu'_G(G(F)\backslash G(\mathbb{A}_F)) = \frac{\prod_v c_v\cdot(\lim_{s\to 1}(s-1)\zeta_F(s))^r\cdot \mathrm{disc}(h)\cdot \sharp(A^*(F)/(B+A^*(F)_{\mathrm{tors}}))}{\mu(F\backslash \mathbb{A}_F)^g \sharp A(F)_{\mathrm{tors}}}$$

となります. したがって

$$\tau(G) = \frac{\prod_v c_v\cdot \mathrm{disc}(h)\cdot \sharp(A^*(F)/(B+A^*(F)_{\mathrm{tors}}))}{\mu(F\backslash \mathbb{A}_F)^g \sharp A(F)_{\mathrm{tors}}}\cdot \lim_{s\to 1}\frac{(s-1)^r}{L(A,s)}$$

が成り立ちます. 以上により定理 6.4 は次の (1), (2) に帰着されます.

1. $Ш(G) \cong Ш(A)$.
2. $\mathrm{Pic}(G)_{\mathrm{tors}} \cong A^*(F)/B$.

(1) は $1 \to T \to G \to A \to 0$ から得られる可換図式

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^1(F,G) & \longrightarrow & H^1(F,A) & \longrightarrow & \mathrm{Hom}(B,\mathrm{Br}(F)) \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \prod_v H^1(F_v,G) & \longrightarrow & \prod_v H^1(F_v,A) & \longrightarrow & \prod_v \mathrm{Hom}(B,\mathrm{Br}(F_v)) \end{array}$$

より従います. (2) は $G \to A \to \mathrm{Spec}\, F$ に関する Leray スペクトル系列を用いて $\mathrm{Pic}(G)$ を計算することによって得られます. □

6.5 定理 6.2 の証明のスケッチ

(証明のスケッチ) 証明は $\langle\ ,\ \rangle$ を各素点 v に関する項の和の形に分解することから始まります.

v を F の素点とします. $D \in \mathrm{Div}^0(A_{F_v})$, $Z \in Z_0(A_{F_v})^0$ であって $\mathrm{Supp}(D) \cap \mathrm{Supp}(Z) = \emptyset$ を満たすものに対し, 次の段落に書く方法で実数 $\langle Z, D\rangle_v \in \mathbb{R}$ を定めます.

D は $A^*(F_v)$ の元 $\mathcal{L}(D)$ を与えます. 式 (6.1) により $\mathcal{L}(D)$ はとある拡大 $1 \to \mathbb{G}_m \to G_D \to A_{F_v} \to 0$ に対応します. 可逆層 $\mathcal{L}(D)$ に対応する A 上の直線束を $V(\mathcal{L}(D))$ とおくと, A_{F_v} 上の $\mathbb{G}_m$ 捻子として G_D は $V(\mathcal{L}(D)) \setminus (0$ 切断$)$ と同型です. したがって切断 $\sigma_D : A_{F_v} \setminus \mathrm{Supp}(D) \hookrightarrow G_D \times_{A_{F_v}} (A_{F_v} \setminus \mathrm{Supp}(D))$ を取ると, $\sigma_D(Z) \in G_D(F_v)$ です. $F_v^\times \subset G_D(F_v)$ ですが, 準同型 $F_v^\times \xrightarrow{-\log|\ |_v} \mathbb{R}$ は連続準同型 $\psi_D : G_D(F_v) \to \mathbb{R}$ に一意的に延ばせます. この ψ_D を用いて

$$\langle Z, D\rangle_v := \psi_D(\sigma_D(Z))$$

と定めます. このとき次のことが確かめられます.

> $D \in \mathrm{Div}^0(A)$, $Z \in Z_0(A)^0$ が $\mathrm{Supp}(D) \cap \mathrm{Supp}(Z) = \emptyset$ を満たすとする. $a \in A(F)$, $a' \in A^*(F)$ をそれぞれ Z, D の定める類とする. このとき $\langle a, a'\rangle = \sum_v \langle Z, D\rangle_v$ が成り立つ.

さらに $\langle Z, D\rangle_v \in \mathbb{R}$ は §4.5 の条件 (1), (2), (3), (5), および $a \in \mathcal{A}^o(X)$ に対する条件 (4) を満たします. このことから $\langle\ ,\ \rangle_v = h(\ ,\ )_v$ であることを確かめられます. □

7　関数体の場合

p を素数, F を標数 p の関数体, A を F 上のアーベル多様体とします. ここ §7 では, 次の定理とその証明を [26] の記述に沿った形で紹介します.

定理 7.1 (Artin-Tate [54], Milne [38], Schneider [46], Bauer [1], 加藤-Trihan [26]). *A を関数体 F 上のアーベル多様体とし, ある素数 ℓ に対し $Ш(A)\{\ell\}$ が有限と仮定する. このとき $Ш(A)$ は有限となり, かつ A について強い形の Birch-Swinnerton-Dyer 予想が成り立つ.*

7.1　問題の素数成分への分解

$\mathbb{F}$ を F の定数体とし, $q = \sharp\mathbb{F}$ とすると, $L(A,s)$ は q^{-s} についての整数係数の多項式となることが知られています. これは代数体上のアーベル多様体が持たない強い性質で, 特にこのことから $L(A,s)$ は全複素平面に正則に解析接続されます. さらに高さ対 $h(\ ,\ ) : A(F) \times A^*(F) \to \mathbb{R}$ は $\log(q)\mathbb{Q} \subset \mathbb{R}$ に値を持つこともわかります. これらのことから予想 3.10 の下, A に対する弱い形の Birch-Swinnerton-Dyer 予想 3.9 から強い形の Birch-Swinnerton-Dyer 予想 3.12 の式が $\bmod \mathbb{Q}^\times$ で従います. このような事情から, 関数体上のアーベル多様体に対する強い形の Birch-Swinnerton-Dyer 予想は, 関数体上のアーベル多様体に対する強い形の Birch-Swinnerton-Dyer 予想と比べてかなり易しい予想となっています.

ℓ を素数とします. A について弱い形の Birch-Swinnerton-Dyer 予想 3.9 および予想 3.10 が成り立っていて, さらに強い形の Birch-Swinnerton-Dyer 予想 3.12 に現れる式の両辺の比が ℓ 進絶対値 1 の有理数となるとき, A について強い形の Birch-Swinnerton-Dyer 予想の ℓ 成分が成り立つといいます. 定理 7.1 は次の 2 つの定理から従います:

定理 7.2. *A を関数体 F 上のアーベル多様体, ℓ を素数とする. このとき $Ш(A)\{\ell\}$ が有限であることと, A について弱い形の Birch-Swinnerton-Dyer 予想が成り立つことは同値である.*

定理 7.3. *A を関数体 F 上のアーベル多様体, ℓ を素数とする. このとき $Ш(A)\{\ell\}$ が有限であれば, A について強い形の Birch-Swinnerton-Dyer 予想の ℓ 成分が成り立つ.*

7.2　定理 7.1 の証明の流れ

定理 7.1 の証明は, 各素数 ℓ について定理 7.2, 定理 7.3 をこの順番で示すことによってなされます.

以下この稿では

- $\ell \neq p$ のときの定理 7.2.
- $\ell \neq p$ のときの定理 7.3.

- $\ell = p$ のときの定理 7.2,7.3.

の順番に概要を述べます. $\ell = p$ の場合は非常に大まかな証明の概略しか述べません. 興味のある方は原論文 [26] をご参照くださると幸いです.

7.3 $\ell \neq p$ のときの定理 7.2, 7.3 の証明のための準備

F の素点の有限集合 S を十分大きく固定します. $U = X \setminus S$ とおきます.

$T_\ell A$, $V_\ell A$, $A\{\ell\} = V_\ell A/T_\ell A$ は G_F の表現です. $\mathcal{T}_\ell\mathcal{A}$, $\mathcal{V}_\ell\mathcal{A}$, $\mathcal{A}\{\ell\}$ をそれぞれに対応する U 上の滑らかな層とします.

7.3.1 幾何的コホモロジーと数論的コホモロジー

幾何的コホモロジー $H^i_{\mathrm{g},\mathbb{Q}_\ell}$, $H^i_{\mathrm{g},\mathbb{Q}_\ell/\mathbb{Z}_\ell}$ を

- $H^i_{\mathrm{g},\mathbb{Q}_\ell} := H^i_{\mathrm{et},c}(\overline{U}, \mathcal{V}_\ell\mathcal{A})$,
- $H^i_{\mathrm{g},\mathbb{Q}_\ell/\mathbb{Z}_\ell} := H^i_{\mathrm{et},c}(\overline{U}, \mathcal{A}\{\ell\})$.

によって定めます. ここで $\overline{U} = U \times_{\operatorname{Spec}\mathbb{F}} \operatorname{Spec}\overline{\mathbb{F}}$ です. $\varphi = \mathrm{Frob}_q$ が $H^i_{\mathrm{g},\mathbb{Q}_\ell}$, $H^i_{\mathrm{g},\mathbb{Q}_\ell/\mathbb{Z}_\ell}$ に作用します.

数論的コホモロジー $H^i_{\mathrm{a},\mathbb{Q}_\ell}$, $H^i_{\mathrm{a},\mathbb{Q}_\ell/\mathbb{Z}_\ell}$ を

- $H^i_{\mathrm{a},\mathbb{Q}_\ell} := H^i_{\mathrm{et},c}(U, \mathcal{V}_\ell\mathcal{A})$,
- $H^i_{\mathrm{a},\mathbb{Q}_\ell/\mathbb{Z}_\ell} := H^i_{\mathrm{et},c}(U, \mathcal{A}\{\ell\})$

によって定めます.

7.3.2 5 つのベクトル空間

$\mathbb{Q}_\ell$ ベクトル空間 $I_{i,\ell}$ $(i = 1, 2, 3, 4, 5)$ および図式

$$I_{1,\ell} \hookrightarrow I_{2,\ell} \hookrightarrow I_{3,\ell} \to I_{4,\ell} \twoheadrightarrow I_{5,\ell} \tag{7.1}$$

を以下で定義します.

- $I_{1,\ell} = A(F) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$.
- $I_{2,\ell} = (H^1_{\mathrm{g},\mathbb{Q}_\ell})^{\varphi}$: $H^1_{\mathrm{g},\mathbb{Q}_\ell}$ の φ 不変部分.
- $I_{3,\ell} = (H^1_{\mathrm{g},\mathbb{Q}_\ell})^{\varphi-\mathrm{unip}}$: $H^1_{\mathrm{g},\mathbb{Q}_\ell}$ の中で φ が巾単に作用する部分.
- $I_{4,\ell} = (H^1_{\mathrm{g},\mathbb{Q}_\ell})_{\varphi}$: $H^1_{\mathrm{g},\mathbb{Q}_\ell}$ の φ 余不変商.
- $I_{5,\ell} = \mathrm{Hom}(A^*(F), \mathbb{Q}_\ell)$.

定義から $I_{2,\ell} \hookrightarrow I_{3,\ell} \hookrightarrow H^1_{\mathrm{g},\mathbb{Q}_\ell} \twoheadrightarrow I_{4,\ell}$ が成り立ちます. これを用いて図式 (7.1) の真ん中の 2 つの準同型を定めます.

スペクトル系列

$$E_2^{p,q} = H^p(\mathbb{F}, H^q_{\mathrm{et},c}(\overline{U}, \mathcal{V}_\ell\mathcal{A})) \Rightarrow H^{p+q}_{\mathrm{et},c}(U, \mathcal{V}_\ell\mathcal{A})$$

と重さの議論により, $I_{2,\ell} \cong H^1_{\mathrm{a},\mathbb{Q}_\ell}$ および $I_{4,\ell} \cong H^2_{\mathrm{a},\mathbb{Q}_\ell}$ が成り立ちます.

Kummer 系列により完全系列

$$0 \to A(F) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \to H^1_{\mathrm{a},\mathbb{Q}_\ell} \to \mathrm{Hom}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, Ш(A)) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \to 0$$

を得ます. また Kummer 系列および (数論的) 双対性により, 完全系列

$$0 \to \mathrm{Hom}(Ш(A^*), \mathbb{Q}_\ell/\mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \to H^2_{\mathrm{a},\mathbb{Q}_\ell} \to \mathrm{Hom}(A^*(F), \mathbb{Q}_\ell) \to 0$$

を得ます. したがって (7.1) の図式

$$I_{1,\ell} \hookrightarrow I_{2,\ell} \hookrightarrow I_{3,\ell} \to I_{4,\ell} \twoheadrightarrow I_{5,\ell}$$

が得られます.

定義により,

$$I_{1,\ell} \xrightarrow{\cong} I_{2,\ell} \iff Ш(A)\{\ell\}\text{: 有限} \iff Ш(A^*)\{\ell\}\text{: 有限} \iff I_{4,\ell} \xrightarrow{\cong} I_{5,\ell}$$

が成り立ちます. また, 等式

$$L^S(A,s) = \prod_{i=0}^{2} \det(1 - \varphi q^{1-s}; H^i_{\mathrm{g},\mathbb{Q}_\ell})^{(-1)^{i+1}}$$

により $\dim_{\mathbb{Q}_\ell} I_{3,\ell} = \mathrm{ord}_{s=1} L(A,s)$ が成り立ちます. さらに合成 $I_{1,\ell} \to \cdots \to I_{5,\ell}$ は同型となります. 実際, この合成は

$$h(\ ,\ ) : A(F) \times A^*(F) \to \log q \cdot \mathbb{Q} \xrightarrow{1/\log(q)} \mathbb{Q}$$

の誘導する準同型 $A(F) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \to \mathrm{Hom}(A^*(F), \mathbb{Q}_\ell)$ と一致することが, 定理 6.2 の証明と同様の方法でわかります ([46, §3]).

7.4 $\ell \neq p$ のときの定理 7.2 の証明

(証明) $Ш(A)\{\ell\}$ が有限と仮定します. 上で述べたことから $I_{1,\ell} \xrightarrow{\cong} I_{2,\ell}$, $I_{4,\ell} \xrightarrow{\cong} I_{5,\ell}$ となりますが, 合成 $I_{1,\ell} \to \ldots \to I_{5,\ell}$ が同型であることから $I_{2,\ell} \xrightarrow{\cong} I_{4,\ell}$ です. $I_{2,\ell}$, $I_{3,\ell}$, $I_{4,\ell}$ の定義により $I_{2,\ell} = I_{3,\ell}$ が成り立ちます. 特に $\dim I_{1,\ell} = \dim I_{3,\ell}$ となることから弱い形の Birch-Swinnerton-Dyer 予想が成り立ちます.

逆に弱い形の Birch-Swinnerton-Dyer 予想が成り立つとすると, $I_{1,\ell} \xrightarrow{\cong} I_{3,\ell}$ となるから, $I_{1,\ell} \xrightarrow{\cong} I_{2,\ell}$ であり, したがって $Ш(A)\{\ell\}$ は有限です. □

7.5 $\ell \neq p$ のときの定理 7.3 の証明

(証明) スペクトル系列

$$E_2^{p,q} = H^p(\mathbb{F}, H^q_{\mathrm{et},c}(\overline{U}, \mathcal{A}\{\ell\})) \Rightarrow H^{p+q}_{\mathrm{et},c}(U, \mathcal{A}\{\ell\})$$

により, 数論的-幾何的完全系列

$$\begin{aligned} 0 \to H^0_{\mathrm{a},\mathbb{Q}_\ell/\mathbb{Z}_\ell} \to H^0_{\mathrm{g},\mathbb{Q}_\ell/\mathbb{Z}_\ell} &\xrightarrow{1-\varphi} H^0_{\mathrm{g},\mathbb{Q}_\ell/\mathbb{Z}_\ell} \\ \to H^1_{\mathrm{a},\mathbb{Q}_\ell/\mathbb{Z}_\ell} \to H^1_{\mathrm{g},\mathbb{Q}_\ell/\mathbb{Z}_\ell} &\xrightarrow{1-\varphi} H^1_{\mathrm{g},\mathbb{Q}_\ell/\mathbb{Z}_\ell} \\ \to H^2_{\mathrm{a},\mathbb{Q}_\ell/\mathbb{Z}_\ell} \to H^2_{\mathrm{g},\mathbb{Q}_\ell/\mathbb{Z}_\ell} &\xrightarrow{1-\varphi} H^2_{\mathrm{g},\mathbb{Q}_\ell/\mathbb{Z}_\ell} \to 0 \end{aligned}$$

を得ます. ここで以下の補題を用います.

補題 7.4. J を有限次元 $\mathbb{Q}_\ell$ ベクトル空間, $\varphi : J \to J$ を $\mathbb{Q}_\ell$ 線形な自己同型写像, J' を捻れ $\mathbb{Z}_\ell$ 加群, $\varphi : J' \to J'$ を自己同型写像, $J \to J'$ を φ と可換な $\mathbb{Z}_\ell$ 準同型写像であって核が J の $\mathbb{Z}_\ell$ 格子, 余核が有限群となるものとする. このとき合成 $J^\varphi \hookrightarrow J \twoheadrightarrow J_\varphi$ が同型ならば, $r = \dim J^\varphi$, $f : (J')^\varphi \to (J')_\varphi$ とおくと,

$$\lim_{t\to 1} \frac{\det(1-\varphi t; J)}{(1-t)^r} \equiv \frac{\sharp \mathrm{Ker}\, f}{\sharp \mathrm{Coker}\, f} (\mathrm{mod}\, \mathbb{Z}_\ell^\times)$$

が成り立つ. □

$Ш(A)\{\ell\}$ が有限と仮定し, $J = H^i_{\mathrm{g},\mathbb{Q}_\ell}$, $J' = H^i_{\mathrm{a},\mathbb{Q}_\ell/\mathbb{Z}_\ell}$ に補題 7.4 を適用します. 合成

$$H^1_{\mathrm{a},\mathbb{Q}_\ell/\mathbb{Z}_\ell} \to (H^1_{\mathrm{g},\mathbb{Q}_\ell/\mathbb{Z}_\ell})^\varphi \to (H^1_{\mathrm{g},\mathbb{Q}_\ell/\mathbb{Z}_\ell})_\varphi \to H^2_{\mathrm{a},\mathbb{Q}_\ell/\mathbb{Z}_\ell}$$

を f とおくと,

$$\lim_{s\to 1} \frac{L_S(A,s)}{(\log q)^r (s-1)^r} \equiv \frac{\sharp \mathrm{Ker} f}{\sharp H^0_{\mathrm{a},\mathbb{Q}_\ell/\mathbb{Z}_\ell} \sharp \mathrm{Coker} f} (\mathrm{mod}\, \mathbb{Z}_\ell^\times)$$

が成り立ちます. 図式

$$0 \to H^0_{\mathrm{a},\mathbb{Q}_\ell/\mathbb{Z}_\ell} \to A(F)\{\ell\} \to \bigoplus\nolimits_{v\in S} A(F_v)\{\ell\} \to H^1_{\mathrm{a},\mathbb{Q}_\ell/\mathbb{Z}_\ell} \to \begin{array}{c} 0 \\ \downarrow \\ A(F)\otimes_Z \mathbb{Q}_\ell/\mathbb{Z}_\ell \\ \downarrow \\ \mathrm{Sel}_{\mathbb{Q}_\ell/\mathbb{Z}_\ell}(A) \\ \downarrow \\ Ш(A)\{\ell\} \\ \downarrow \\ 0 \end{array} \to 0$$

と $Ш(A)\{\ell\}$ の有限性より同型 $H^2_{\mathrm{a},\mathbb{Q}_\ell/\mathbb{Z}_\ell} \cong \mathrm{Hom}(A^*(F), \mathbb{Q}_\ell/\mathbb{Z}_\ell)$ を得ます. すでに述べたように, 合成 $I_{1,\ell} \to \ldots \to I_{5,\ell}$, すなわち

$$A(F)\otimes_{\mathbb{Z}} \mathbb{Q}_\ell \cong H^1_{\mathrm{a},\mathbb{Q}_\ell} \to (H^1_{\mathrm{g},\mathbb{Q}_\ell})^\varphi \to (H^1_{\mathrm{g},\mathbb{Q}_\ell})_\varphi \to H^2_{\mathrm{a},\mathbb{Q}_\ell} \to \mathrm{Hom}(A^*(F), \mathbb{Q}_\ell)$$

は $h(\ ,\ ) : A(F) \times A^*(F) \to \log q \cdot \mathbb{Q}$ から誘導される準同型と一致します. したがって定理 7.3 が成り立ちます. □

7.6 $\ell = p$ の場合の定理 7.2, 7.3 の証明の方針

$\ell = p$ の場合の定理 7.2, 7.3 の証明も, 上に述べた $\ell \neq p$ の場合の定理 7.2, 7.3 の証明と方針は同様です. F の素点の有限集合 S を十分大きくとり (どのくらい大きく取るかは §7.6.2 で述べます), $U = X \setminus S$ とおきます.

7.6.1

$\ell = p$ の場合も $\ell \neq p$ の場合と同様 $\mathbb{Q}_p$ 係数幾何的コホモロジー, $\mathbb{Q}_p/\mathbb{Z}_p$ 係数幾何的コホモロジー, $\mathbb{Q}_p$ 係数数論的コホモロジー, $\mathbb{Q}_p/\mathbb{Z}_p$ 係数数論的コホモロジーの 4 種類のコホモロジー群について考察します. このうち, $\mathbb{Q}_p$ 係数幾何的コホモロジー, $\mathbb{Q}_p$ 係数数論的コホモロジー, $\mathbb{Q}_p/\mathbb{Z}_p$ 係数数論的コホモロジーの 3 種類は, それぞれ以下ようにして構成されます:

- $\mathbb{Q}_p$ 係数幾何的コホモロジー $H^i_{\mathrm{g},\mathbb{Q}_p}$ を $\mathcal{A}: A$ の Néron モデルに付随する U 上の過収束アイソクリスタルの剛 (rigid) コホモロジーとして構成する.
- $\mathbb{Q}_p$ 係数数論的コホモロジー $H^i_{\mathrm{a},\mathbb{Q}_p}$ をコンパクト台をもつ平坦コホモロジーとして構成する.
- $\mathbb{Q}_p/\mathbb{Z}_p$ 係数数論的コホモロジー $H^i_{\mathrm{a},\mathbb{Q}_p/\mathbb{Z}_p,V}$ を適当な境界条件 V つきの平坦コホモロジーとして構成する.

残る $\mathbb{Q}_p/\mathbb{Z}_p$ 係数幾何的コホモロジーは $\ell \neq p$ の場合と異なり $H^i_{1,\mathrm{g},\mathbb{Q}_p/\mathbb{Z}_p}$ と $H^i_{2,\mathrm{g},\mathbb{Q}_p/\mathbb{Z}_p}$ との 2 種類を構成します.

$\mathbb{Q}_p/\mathbb{Z}_p$ 係数幾何的コホモロジーを 2 種類用意することが必要となるのは, $\ell = p$ のときには ($H^i_{\mathrm{g},\mathbb{Q}_p}$ やそれを構成する際に用いるものへの) φ の作用の分母に p が現れるためです. この分母のせいで自己準同型 φ をもつ $H^i_{\mathrm{g},\mathbb{Q}_p/\mathbb{Z}_p}$ を構成できず, 自己準同型の代わりに $\iota: H^i_{1,\mathrm{g},\mathbb{Q}_p/\mathbb{Z}_p} \to H^i_{2,\mathrm{g},\mathbb{Q}_p/\mathbb{Z}_p}$, $\varphi: H^i_{1,\mathrm{g},\mathbb{Q}_p/\mathbb{Z}_p} \to H^i_{2,\mathrm{g},\mathbb{Q}_p/\mathbb{Z}_p}$ を考えるため, 2 種類の $\mathbb{Q}_p/\mathbb{Z}_p$ 係数幾何的コホモロジーが必要になるのです.

7.6.2 対数的 Dieudonné クリスタルの理論と $\mathbb{Q}_p/\mathbb{Z}_p$ 係数幾何的コホモロジーの構成

$H^i_{1,\mathrm{g},\mathbb{Q}_p/\mathbb{Z}_p}$ と $H^i_{2,\mathrm{g},\mathbb{Q}_p/\mathbb{Z}_p}$ は, いずれも構成は対数的 Dieudonné クリスタルの理論を用いてなされます. もう少し説明するために, 次の段落で記号を準備します.

F の有限次 Galois 拡大 F' であって $A' := A \times_{\operatorname{Spec} F} \operatorname{Spec} F'$ が半安定還元を持つものを選びます. $G = \operatorname{Gal}(F'/F)$ とおきます. F の素点の有限集合 S を, A は S の外でよい還元をもち, F'/F は S の外で不分岐となるように選びます. $S' = \bigcup_{v \in S} \{w : F' \text{ の素点} \mid w|v\}$ とおきます. X' を F' に対応する代数曲線とします.

$X'^{\sharp}$ を (X', S') に付随する対数的スキーム, $\mathcal{A}'$ を A' の X' 上の Néron モデルとします. このとき X' 上の対数的 1 モチーフの概念を用いることにより, $X'^{\sharp}/\mathbb{Z}_p$ 上の (対数的) Dieudonné クリスタル D' が構成されます.

$D'_1 \subset D'_2 \subset D'$ を適当に選び, $H^i_{1,\mathrm{g},\mathbb{Q}_p/\mathbb{Z}_p} := H^i(R\Gamma(G, R\Gamma_{\mathrm{crys}}(X'^{\sharp}/\mathbb{Z}_p, D'_1)) \otimes^{\mathbb{L}}_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)$. $H^i_{2,\mathrm{g},\mathbb{Q}_p/\mathbb{Z}_p} := H^i(R\Gamma(G, R\Gamma_{\mathrm{crys}}(X'^{\sharp}/\mathbb{Z}_p, D'_2)) \otimes^{\mathbb{L}}_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)$ とおくことによって, $H^i_{1,\mathrm{g},\mathbb{Q}_p/\mathbb{Z}_p}$, $H^i_{2,\mathrm{g},\mathbb{Q}_p/\mathbb{Z}_p}$ が構成されます.

7.6.3 証明の完結

($\ell = p$ の場合の定理 7.2, 7.3 の証明) 共分 (syntomic) 複体の理論を用いると, 数論的-幾何的完全系列

$$\begin{aligned} 0 \to H^0_{\mathrm{a},\mathbb{Q}_p/\mathbb{Z}_p,V} \to H^0_{1,\mathrm{g},\mathbb{Q}_p/\mathbb{Z}_p} &\xrightarrow{\iota-\varphi} H^0_{2,\mathrm{g},\mathbb{Q}_p/\mathbb{Z}_p} \\ \to H^1_{\mathrm{a},\mathbb{Q}_p/\mathbb{Z}_p,V} \to H^1_{1,\mathrm{g},\mathbb{Q}_p/\mathbb{Z}_p} &\xrightarrow{\iota-\varphi} H^1_{2,\mathrm{g},\mathbb{Q}_p/\mathbb{Z}_p} \\ \to H^2_{\mathrm{a},\mathbb{Q}_p/\mathbb{Z}_p,V} \to H^2_{1,\mathrm{g},\mathbb{Q}_p/\mathbb{Z}_p} &\xrightarrow{\iota-\varphi} H^2_{2,\mathrm{g},\mathbb{Q}_p/\mathbb{Z}_p} \to 0 \end{aligned}$$

が得られ, $\mathbb{Q}_p/\mathbb{Z}_p$ 係数数論的コホモロジーと $\mathbb{Q}_p/\mathbb{Z}_p$ 係数幾何的コホモロジーとが結びつきます. $\ell \neq p$ の場合と同様, 次が成立します:

- 合成

$$A(F) \otimes_{\mathbb{Z}} \mathbb{Q}_p \to H^1_{\mathrm{a},\mathbb{Q}_p} \to (H^1_{\mathrm{g},\mathbb{Q}_p})^{\varphi} \to (H^1_{\mathrm{g},\mathbb{Q}_p})_{\varphi} \to H^2_{\mathrm{a},\mathbb{Q}_p} \to \mathrm{Hom}(A^*(F), \mathbb{Q}_p)$$

  が, $h(\ ,\ ) : A(F) \times A^*(F) \to \log q \cdot \mathbb{Q}$ から誘導される準同型と一致する.

- $H^i_{\mathrm{a},\mathbb{Q}_p/\mathbb{Z}_p,V}$ は $A(F) \otimes \mathbb{Q}_p/\mathbb{Z}_p$, $\mathrm{Hom}(A^*(F), \mathbb{Q}_p/\mathbb{Z}_p)$, $\mathrm{Sel}_{\mathbb{Q}_p/\mathbb{Z}_p}(A)$, $Ш(A)\{p\}$, $\mathrm{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, Ш(A^*))$ と結びつく.

これらのことから定理 7.2, 定理 7.3 が得られます. □

8　本稿で触れなかった話題と参考文献

本稿でふれなかった Birch-Swinnerton-Dyer 予想に関する重要な話題として, §1 に挙げたものの他に, Birch-Swinnerton-Dyer 予想の同変版への拡張 ([18]) があります. これによって例えば

- 大域体の有限次 Galois 拡大 F'/F および, F 上のアーベル多様体 A が与えられている状況下でのモチーフ $h_1(A) \otimes_{\mathbb{Z}} \mathbb{Z}[\mathrm{Gal}(F'/F)]$ の L 関数の特殊値.
- 大域体 F 上のアーベル多様体 A と環準同型 $i : R \to \mathrm{End}(A)$ の組 (A, i) であって $H_1(A(\mathbb{C}), \mathbb{Z})$ が R 加群として射影次元有限となるようなものが与えられているときの $L(A, s)$ の特殊値.

について, 通常の Birch-Swinnerton-Dyer 予想よりも詳しい内容を予想することができます. 例えば上に 2 つ挙げたうちの後者に対する予想は Gross の予想 [21] を含みます.

また, A の p 進 L 関数が定義されている場合には, Birch-Swinnerton-Dyer 予想の p 進類似という重要な話題があります (例えば [37]) が, これについても同変版の Birch-Swinnerton-Dyer 予想と解釈することができます.

参考文献

[1] Bauer, W.: *On the conjecture of Birch and Swinnerton-Dyer for abelian varieties over function fields in characteristic $p > 0$.* Invent. Math. **108**, no. 2, 263–287 (1992)

[2] Beilinson, A. A.: *Higher regulators and values of L-functions.* (ロシア語) Itogi Nauki i Tekhniki, Akad. Nauk SSSR **24**, 181–238 (1984); 英訳: J. Soviet Math. **30**, no. 2, 2036-2070 (1985)

[3] Beilinson, A. A.: *Height pairing between algebraic cycles.* K-theory, arithmetic and geometry (Moscow, 1984–1986), 1–25, Lect. Notes Math. **1289**, Springer-Verlag, Berlin (1987)

[4] Birch, B. J., Swinnerton-Dyer, H. P. F.: *Notes on elliptic curves. II.* J. Reine Angew. Math. **218** 79–108 (1965)

[5] Bloch, S.: *A note on height pairings, Tamagawa numbers, and the Birch and Swinnerton-Dyer conjecture.* Invent. Math. **58**, no. 1, 65–76 (1980)

[6] Bloch, S.: *Height pairings for algebraic cycles.* Proceedings of the Luminy conference on algebraic K-theory (Luminy, 1983). J. Pure Appl. Algebra **34**, no. 2-3, 119–145 (1984)

[7] Bloch, S., Kato, K.: *L-functions and Tamagawa numbers of motives.* The Grothendieck Festschrift I, 333–400. Prog. Math. **86**, Birkhäuser Boston, MA (1990)

[8] Borel, A.: *Some properties of adele groups attached to algebraic groups*. Bull. Amer. Math. Soc. **67**, 583–585 (1961)

[9] Bosch, S., Lütkebohmert, W., Raynaud, M.: *Néron models*. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) **21**. Springer-Verlag, Berlin (1990)

[10] Brown, M. L.: *Heegner modules and elliptic curves*. Lect. Notes Math. **1849**, Springer-Verlag, Berlin (2004)

[11] Cassels, J. W. S.: *Arithmetic on curves of genus* 1. *IV. Proof of the Hauptvermutung*. J. Reine Angew. Math. **211**, 95–112 (1962)

[12] Cassels, J. W. S.: *Arithmetic on an elliptic curve*. Proc. Internat. Congr. Mathematicians (Stockholm, 1962), 234–246. Inst. Mittag-Leffler, Djursholm (1963)

[13] Chernousov, V. I.: *The Hasse principle for groups of type* E_8. (ロシア語) Dokl. Akad. Nauk SSSR **306**, no. 5, 1059–1063 (1989); 英訳: Soviet Math. Dokl. **39**, no. 3, 592–596 (1989)

[14] Deligne, P.: *Les constantes des équations fonctionnelles des fonctions L*. In: Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), 501–597. Lect. Notes Math. **349**, Springer-Verlag, Berlin (1973)

[15] Deligne, P.: *Valeurs de fonctions L et périodes d'intégrales*. With an appendix by N. Koblitz and A. Ogus. In Automorphic forms, representations and *L*-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Proc. Sympos. Pure Math. **33**, Part 2, 313–346. American Mathematical Society, Providence, RI (1979)

[16] Fontaine, J.-M.: *Sur certains types de représentations p-adiques du groupe de Galois d'un corps local; construction d'un anneau de Barsotti-Tate*. Ann. of Math. (2) **115**, no. 3, 529–577 (1982)

[17] Fontaine, J.-M., Perrin-Riou, B.; *Autour des conjectures de Bloch et Kato: cohomologie galoisienne et valeurs de fonctions L* In: Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math. **55**, Part 1, 599–706. American Mathematical Society, Providence, RI (1994)

[18] Fukaya, T., Kato, K.: *A formulation of conjectures on p-adic zeta functions in noncommutative Iwasawa theory*. Proceedings of the St. Petersburg Mathematical Society **12**, 1–85. Amer. Math. Soc. Transl. Ser. 2, **219**, American Mathematical Society, Providence, RI (2006)

[19] Gillet, H., Soulé, C.: *Intersection sur les variétés d'Arakelov*. C. R. Acad. Sci. Paris Sér. I Math. **299**, no. 12, 563–566 (1984)

[20] Gillet, H., Soulé, C.: *Arithmetic intersection theory.* Publ. Math., Inst. Hautes Étud. Sci. **72**, 93–174 (1991)

[21] Gross, B. H.: *On the conjecture of Birch and Swinnerton-Dyer for elliptic curves with complex multiplication.* Number theory related to Fermat's last theorem (Cambridge, MA, 1981), 219–236. Prog. Math. **26**, Birkhäuser, Boston, MA (1982)

[22] Gross, B. H.: *Minimal models for elliptic curves with complex multiplication.* Compositio Math. **45**, no. 2, 155–164 (1982)

[23] Gross, B. H., Zagier, D. B.: *Heegner points and derivatives of L-series.* Invent. Math. **84**, no. 2, 225–320 (1986)

[24] Jordan, B. W., Livné, R.: *On Atkin-Lehner quotients of Shimura curves.* Bull. London Math. Soc. **31**, no. 6, 681–685 (1999)

[25] Kato, K.: *p-adic Hodge theory and values of zeta functions of modular forms.* Cohomologies p-adiques et applications arithmétiques. III. Astérisque **295**, 117–290 (2004)

[26] Kato, K., Trihan, F.: *On the conjectures of Birch and Swinnerton-Dyer in characteristic $p > 0$.* Invent. Math. **153**, no. 3, 537–592 (2003)

[27] Kodaira, K.: *On compact analytic surfaces, II.* Ann. of Math. (2) **77**, 563–626 (1963)

[28] Kolyvagin, V. A.: *Finiteness of $E(Q)$ and Ш(E, Q) for a subclass of Weil curves.* (ロシア語) Izv. Akad. Nauk SSSR Ser. Mat. **52**, no. 3, 522–540, 670–671 (1988); 英訳: Math. USSR-Izv. **32**, no. 3, 523–541 (1989)

[29] Kolyvagin, V. A.: *The Mordell-Weil and Shafarevich-Tate groups for Weil elliptic curves.* (ロシア語) Izv. Akad. Nauk SSSR Ser. Mat. **52**, no. 6, 1154–1180, 1327 (1988); 英訳: Math. USSR-Izv. **33**, no. 3, 473–499 (1989)

[30] Kolyvagin, V. A., Logachëv, D. Yu.: *Finiteness of* Ш *over totally real fields.* (ロシア語) Izv. Akad. Nauk SSSR Ser. Mat. **55**, no. 4, 851–876 (1991); 英訳: Math. USSR-Izv. **39**, no. 1, 829–853 (1992)

[31] Kottwitz, R. E.: *Tamagawa numbers.* Ann. of Math. (2) **127**, no. 3, 629–646 (1988)

[32] Lang, S.: *Les formes bilinéaires de Néron et Tate.* Séminaire Bourbaki, Exp. 274 (1963/64)

[33] Lang, S., Tate, J.: *Principal homogeneous spaces over abelian varieties.* Amer. J. Math. **80**, 659–684 (1958)

[34] Langlands, R. P.: *On the functional equation of the Artin L-functions*. Unpublished notes, available from `http://www.sunsite.ubc.ca/DigitalMathArchive/Langlands/`.

[35] Mazur, B.; Messing, W.: *Universal extensions and one dimensional crystalline cohomology*. Lect. Notes Math. **370**, Springer-Verlag, Berlin-New York (1974)

[36] Mazur, B., Tate, J.: *Canonical height pairings via biextensions*. In: Arithmetic and geometry, Vol. I, Prog. Math. **35**, 195–237. Birkhäuser Boston, Boston, MA (1983)

[37] Mazur, B., Tate, J., Teitelbaum, J.: *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*. Invent. Math. **84**, no. 1, 1–48 (1986)

[38] Milne, J. S.: *On a conjecture of Artin and Tate*. Ann. of Math. (2) **102**, no. 3, 517–533 (1975)

[39] Milne, J. S.: *Arithmetic duality theorems*. Perspect. Math. **1**, Academic Press, Boston, MA (1986)

[40] Néron, A.: *Modèles minimaux des variétés abéliennes sur les corps locaux et globaux*. Inst. Hautes Études Sci. Publ. Math. **21**, 361–482 (1964)

[41] Néron, A.: *Quasi-fonctions et hauteurs sur les variétés abéliennes*. Ann. of Math. (2) **82** 249–331 (1965)

[42] Ono, T.: *On the Tamagawa number of algebraic tori*. Ann. of Math. (2) **78**, 47–73 (1963)

[43] Platonov, V., Rapinchuk, A.: *Algebraic groups and number theory*. Translated from the 1991 Russian original by Rachel Rowen. Pure and Applied Mathematics **139**, Academic Press, Boston, MA (1994)

[44] Poonen, B., Stoll, M.: *The Cassels-Tate pairing on polarized abelian varieties*. Ann. of Math. (2) **150**, no. 3, 1109–1149 (1999)

[45] Sansuc, J.-J.: *Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres*. J. Reine Angew. Math. **327**, 12–80 (1981)

[46] Schneider, P.: *Zur Vermutung von Birch und Swinnerton-Dyer über globalen Funktionenkörpern*. (ドイツ語) Math. Ann. **260**, no. 4, 495–510 (1982)

[47] Scholl, A. J.: *Remarks on special values of L-functions*. *L*-functions and arithmetic (Durham, 1989), 373–392, London Math. Soc. Lecture Note Ser., 153, Cambridge Univ. Press, Cambridge, 1991

[48] Scholl, A. J.: *Height pairings and special values of L-functions*. In: Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math., 55, Part 1, 571–598. American Mathematical Society, Providence, RI (1994)

[49] Serre, J.-P.: *Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures)*. Séminaire Delange-Pisot-Poitou, exposé **19** (1969/70)

[50] Serre, J.-P.: *Représentations linéaires des groupes finis*. Third revised edition. Hermann, Paris (1978)

[51] Serre, J.-P., Tate, J.: *Good reduction of abelian varieties*. Ann. of Math. (2) **88**, 492–517 (1968)

[52] Tate, J.: *Duality theorems in Galois cohomology over number fields*. In: Proc. Internat. Congr. Mathematicians (Stockholm, 1962), 288–295. Inst. Mittag-Leffler, Djursholm (1963)

[53] Tate, J.: *WC-groups over* $\mathfrak{p}$*-adic fields*. Séminaire Bourbaki Exp. 156 (1957/1958)

[54] Tate, J.: *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*. Séminaire Bourbaki Exp. 306 (1965/1966)

[55] Tate, J.: *Algorithm for determining the type of a singular fiber in an elliptic pencil*. In: Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Lect. Notes Math. **476**, 33–52. Springer-Verlag, Berlin, 1975.

[56] Tate, J.: *Number theoretic background*. In: Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Proc. Sympos. Pure Math. **33**, Part 2, 3–26. American Mathematical Society, Providence, RI (1979)

[57] Weil, A.: *Sur un théorème de Mordell*, Bull. Sci. Math. **54**, 182–191 (1930)

[58] Weil, A.: *Adeles and algebraic groups*. With appendices by M. Demazure and Takashi Ono. Prog. Math. **23**, Birkhäuser, Boston, MA (1982)

[59] *Groupes de monodromie en géométrie algébrique. I.* Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I). Lect. Notes Math. **288**, Springer-Verlag, Berlin-New York (1972)