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