

形式群の始め、相互法則を眺めるだけ

目次

§1. 準備

§2 標数0の体上の形式群

§3. 相互法則を示すのを眺めるだけ

§4. 参考文献

§1.

Def (形式群)

$$R: \text{ring}, F(x, y) \in R[[x, y]].$$

F の R 上の (1次元可換) 形式群 G があるとは、
次をみたすもの:

$$(i) F(x, 0) = x, F(0, y) = y,$$

$$(ii) F(F(x, y), z) = F(x, F(y, z)),$$

$$(iii) F(x, y) = F(y, x).$$

Def (不変微分)

$$R: \text{ring}, F(x, y) \in R[[x, y]] \text{ formal grp.}$$

F における不変微分とは

$$\omega(x) = P(x)dx \in R[[x]]dx$$

がある、次をみたすもの:

$$\omega \circ F(\alpha, \gamma) = \omega(\alpha)$$

$$\text{さらに } \omega(x) = p(x) dx \text{ のように}$$

$$p(0) = 1$$

をみたすとき, ω は正規化された不変微分形式という.

Rem. $\omega(x) = p(x) dx$ に対し $\omega \in \mathcal{F}^1$ であることは次のように:

$\omega(x)$: Invariant differential / F

$$\Leftrightarrow p(F(\alpha, \gamma)) F_\alpha(\alpha, \gamma) = p(\alpha)$$

Lem
formal grp F 上の正規化された不変微分形式 ω は 1-CA 存在せず, これをみたす.

$$\omega = F_\alpha(0, x)^{-1} dx$$

$$\text{pf. } p(F(\alpha, \gamma)) F_\alpha(\alpha, \gamma) = p(\alpha)$$

$$\leadsto p(F(0, x)) F_\alpha(0, x) = p(0) \quad (\odot x=0, y=x \text{ として})$$

$$\leadsto p(x) F_\alpha(0, x) = p(0) \quad (\odot F(0, x) = x)$$

$$\therefore p(x) = F_\alpha(0, x)^{-1} p(0)$$

$$(\odot F_\alpha(0, x) = 1 + (1\text{-次以上の項}) \in \mathbb{R}[[x]]^{\times})$$

ω は正規化されたものであるとき, $p(0) = 1$ である

$$p(x) = F_\alpha(0, x)^{-1}$$

$$\therefore \omega(x) = F_\alpha(0, x)^{-1} dx \quad \square$$

eg. $w(x) = dx$ は加法群 $\widehat{\mathbb{G}}_a(x, y) = x + y$ 上の
正規化エタラ不變微分である。

eg. $w(x) = \frac{dx}{1+x}$ は乗法群 $\widehat{\mathbb{G}}_m(x, y) = x + y - xy$ 上の
正規化エタラ不變微分である。

Def (強同型)

$F(x, y), G(x, y) \in R[x, y] : \text{formal grps.}$

$\varphi(x) \in R[x]$ $\varphi^*(F \wedge G)$ 準同型であるとは

$$\varphi(F(x, y)) = G(\varphi(x), \varphi(y))$$

をみたすこと。

さらに、可逆な準同型を弱同型と云う。

加えて、 $\varphi(x) \equiv x \pmod{\deg 2}$ をみたす弱同型を強同型と云う。

eg. $\mathbb{Q} \subset R$ とすると

$\varphi: \widehat{\mathbb{G}}_m(x, y) \rightarrow \widehat{\mathbb{G}}_a(x, y), x \mapsto -\log(1-x)$
は強同型である。

$$\textcircled{!} -\log(1-x(1-y)) = -\log(1-x) - \log(1-y)$$

$$\leadsto \varphi(\widehat{\mathbb{G}}_m(x, y)) = \widehat{\mathbb{G}}_a(\varphi(x), \varphi(y))$$

逆関数は $-e^{-x} + 1$ (2行), φ は1次で $x \neq 1$:

$$\varphi(x) = -\log(1-x) = x + \frac{1}{2}x^2 + \frac{1}{3}x^3 + \dots \equiv x \pmod{\deg 2} \quad \square$$

§2.

目標: 標数0の体上の形式群を分類する.

$$K: \text{field}, \text{char}(K) = 0$$

$$F(x, y) \in K[[x, y]] : \text{formal grp.}$$

F 上の正規化された不変微分 ω を

$$\omega(x) = (1 + c_1 x + c_2 x^2 + \dots) dx$$

のように明言しておく.

このとき F の形式的対数関数を次で定める.

$$\log_F(x) := \int \omega(x) = x + \frac{1}{2}c_1 x^2 + \frac{1}{3}c_2 x^3 + \dots \quad (= K[[x]])$$

また, $\log_F$ の逆関数を $\exp_F$ とおき, 形式的指数関数とよぶ:

$$\log_F \circ \exp_F(x) = \exp_F \circ \log_F(x) = x$$

e.g. 加法群 $\widehat{G}_a(x, y)$ 上の正規化された不変微分は

$$\omega(x) = dx = (1 + 0 \cdot x + 0 \cdot x^2 + \dots) dx$$

であるから

$$\log_{\widehat{G}_a}(x) = \int \omega(x) = \int dx = x, \quad \exp_{\widehat{G}_a}(x) = x.$$

e.g. 乗法群 $\widehat{G}_m(x, y)$ 上の正規化された不変微分は

$$\omega(x) = \frac{dx}{1+x}$$

であるから

$$\log_{\hat{\mathbb{A}}_m}(x) = \int \omega(x) = \int \frac{dx}{1+x} = \log(1+x),$$

$$\exp_{\hat{\mathbb{A}}_m}(x) = e^x - 1.$$

Thm

$\forall F(x,y) \in K[x,y]$ は加法群 $\hat{\mathbb{A}}_m(x,y) \simeq K$ 上強同型である。
 具体的に, $\log_F : F \xrightarrow{\sim} \hat{\mathbb{A}}_m$ である。

pf. $\omega(x) \in F$ 上の正規化された不変微分とする。

$$\omega(F(x,y)) = \omega(x)$$

$$\leadsto \log_F(F(x,y)) = \log_F(x) + C \quad \leftarrow \text{積分定数}$$

($\odot$ 両辺を $x=0$ として積分した)

$$\leadsto \log_F(y) = C$$

($\odot x=0$ に対して, $F(0,y) = y, \log_F(0) = 0$)

$$\therefore \log_F(F(x,y)) = \log_F(x) + \log_F(y) \quad \text{Fact}$$

(i.e. $\log_F : \text{dom}$)

$\therefore \log_F : \text{Iso}/K$ ($\odot \exp_F$ の存在)

Def (変換子)

$\log_F \in F$ の変換子という。

i.e. F から $\hat{\mathbb{A}}_m$ の強同型を変換子という。

一般に, $f(x) \in \mathbb{R}[x]$ かつ
 $f(x) = ax + (\text{higher order terms})$
 $(a \in \mathbb{R}^*)$

と書ける $\Rightarrow f(\exists! g(x)) = x$

§3.

Def (*)

p : prime とする.

$U = \sum_{j \geq 0} C_j T^j \in \mathbb{Z}_p[[T]]$ と $f(x_1, \dots, x_n) \in \mathbb{Q}_p[[x_1, \dots, x_n]]$ に對し

$$U * f(x_1, \dots, x_n) := \sum_{j \geq 0} C_j f(x_1^{p^j}, \dots, x_n^{p^j})$$

と定める.

このとき $\mathbb{Z}_p[[T]] \curvearrowright \mathbb{Z}_p[[x_1, \dots, x_n]]$ となる.

Def (特殊元)

• $U \in \mathbb{Z}_p[[T]]$: 特殊元 $:\Leftrightarrow U \equiv p \pmod{\deg 1}$

• $f(x) \in \mathbb{Q}_p[[x]]$ が 特殊元 $U \in \mathbb{Z}_p[[T]]$ に属する

$$:\Leftrightarrow \begin{cases} (i) f(x) \equiv x \pmod{\deg 2} \\ (ii) (U * f)(x) \equiv 0 \pmod{p} \end{cases}$$

Rem. formal grp $F(x, y) \in \mathbb{Q}_p[[x, y]]$ の変換子 $f(x)$ が 特殊元 U に属する $\Leftrightarrow$ $F(x, y)$ は U に属するといふ.

cf. $F \xrightarrow[\cong]{f} \hat{G}_a$: 同型

Fact ①

$F(x, y) \in \mathbb{Q}_p[[x, y]]$: formal grp.

$F(x, y) \in \mathbb{Z}_p[[x, y]] \Leftrightarrow F(x, y)$ はある特殊元 U に属する.

e.g. $\hat{G}_m(x, y)$ は特殊元 $p-T$ に属する.

① $-\log(1-x): \hat{G}_m \xrightarrow{\cong} \hat{G}_a$

$$(p-T) * (-\log(1-x)) = (p-T) * \sum_{n \geq 1} \frac{1}{n} x^n$$

$$= p \sum_{n \geq 1} \frac{1}{n} x^n - \sum_{n \geq 1} \frac{1}{n} x^{np}$$

$$= p \left(\sum_{\substack{n \geq 1 \\ n \nmid p}} \frac{1}{n} x^n + \sum_{n \geq 1} \frac{1}{np} x^{np} \right) - \sum_{n \geq 1} \frac{1}{n} x^{np}$$

$$= p \sum_{\substack{n \geq 1 \\ n \nmid p}} \frac{1}{n} x^n$$

$$\equiv 0 \pmod{p} \quad \square$$

Fact ②

$\{C_p^{\nu}\}_{p, \nu \geq 0}$: 整数の数列, $C_0 = 1$.

数列 $\{a_n\}_{n \geq 0} \in$

$$\sum_{n \geq 1} \frac{a_n}{n^s} = \prod_p \frac{1}{1 + \sum_{\nu \geq 1} C_p^{\nu} p^{\nu} - (1 - \nu)s} \quad (\text{Euler積表示})$$

2"定めた, 2"した

$$f(x) := \sum_{n \geq 1} \frac{a_n}{n} x^n, \quad F(x, y) := f^{-1}(f(x) + f(y))$$

と定める. (となく, Euler積表示をもつ f についてもよい)

このとき $\forall p$: prime に対し formal grp $F(x, y) \in \mathbb{Q}_p[[x, y]]$ は特殊元 $p + \sum_{\nu \geq 1} \mathbb{Z}_p T^{\nu}$ に属する.

特に, Hasseの原理とFact①より, $F(x, y)$ は $\mathbb{Z}_p$ 上 def される.

c.f. 証明は計算をガリル $\square$

ζ : odd prime に對し ζ^2 , Gauss 和 Σ

$$\tau := \sum_{n=1}^{\zeta-1} \left(\frac{n}{\zeta}\right) \zeta^n$$

ζ とする. 尤も ζ は 1 の原始 ζ 乗根である.

$K := \mathbb{Q}(\tau)$, $\mathcal{O}_K$: K の整数環とする.

(cf. $\tau^2 = \left(\frac{-1}{\zeta}\right)\zeta$)

さらに, $f(x) := \sum_{n=1}^{\infty} \left(\frac{n}{\zeta}\right) \frac{x^n}{n}$ に對し

$g(x, y) := f^{-1}(f(x) + f(y))$ ← G の変換子 h が f となる
実際

とおく.

Fact ②より, $g(x, y)$ は formal grp / $\mathbb{Z}$ である.

$$\begin{aligned} f(g(x, y)) &= f(x) + f(y) \\ &= \widehat{G}(f(x), f(y)) \end{aligned}$$

$\cong \mathbb{Z}$

$$h(x, y) := x + y + \tau xy$$

とおく. H は formal grp / $\mathcal{O}_K$ である.

H の不変微分は $\frac{dx}{1+\tau x}$ であり, 変換子は $\lambda(x) := \sum_{n \geq 1} \frac{(-\tau)^{n-1}}{n} x^n$ と与えられる.

↑ $H \times (0, 1) \rightarrow dx$
ε 計算すればよい.
cf. §10 Lem

↑ $\lambda(x) = \int \frac{dx}{1+\tau x}$
cf. 不変微分の def

Thm
[$G \simeq H$: 強同型 / $\mathcal{O}_K$

(outline of proof)

$$p(x) := \prod_{1 \leq a \leq \zeta-1} (1 - \zeta^a x), \quad Q(x) := \prod_{1 \leq b \leq \zeta-1} (1 - \zeta^b x)$$

$\left(\frac{\zeta}{\zeta}\right) = 1$ $\left(\frac{\zeta}{\zeta}\right) = -1$

とおく.

このとき実は

$$\varphi(x) := \frac{Q(x) - P(x)}{\tau P(x)}$$

A: $G \cong H$: 同型 / $\sigma_k \in S$ とする.

• $\langle \sigma \rangle = \text{Gal}(K/\mathbb{Q})$ に属して

$$\sigma(Q(x) - P(x)) = -(P(x) - Q(x))$$

A: 成り立つことより, $\tau^2 = (-\frac{1}{\delta})\delta$ に注意すると

$$\varphi(x) \in \sigma_k \mathbb{Z}[x]$$

A: 示す.

• φ を計算することより, φ は homomorphism であること A: 示す.

• φ の可逆性は形式的逆関数定理より示す.

• $\varphi(x) \equiv x \pmod{\deg 2}$ は可逆的. $\square$

Fact

$\varphi: \text{hom}$

$\Leftrightarrow \exists c \in R$ s.t.

$$\varphi^*(df) = cdf$$

Main Thm (平方剰余の相互法則)

$$\left(\frac{p}{\delta} \right) \left(\frac{\delta}{p} \right) = (-1)^{\frac{1}{2}(p-1) \cdot \frac{1}{2}(\delta-1)} \quad (p, \delta: \text{odd prime})$$

pf. 前Thmより $g(x) = (\tau \circ \varphi)(x)$ とあるから

$$\sum_{n \geq 1} \frac{\left(\frac{n}{\delta} \right)}{n} x^n = \sum_{n \geq 1} \frac{(-\tau)^{n-1}}{n} (\varphi(x))^n$$

A: 成り立つ.

$$\therefore p \sum_{n=1}^p \frac{\left(\frac{n}{\delta} \right)}{n} x^n \equiv p \sum_{n=1}^p \frac{(-\tau)^{n-1}}{n} (\varphi(x))^n \pmod{\deg(p+1)}$$

$1 \leq n < p$ なる n に対して, $n \perp p$ より

$$\left(\frac{p}{\delta} \right) x^p \equiv \frac{(-\tau)^{p-1}}{p} (\varphi(x))^p$$

$$\equiv \left\{ \left(\frac{-1}{\delta} \right) \delta \right\}^{\frac{1}{2}(p-1)} x^p \pmod{\deg p+1, \text{ mod } p}$$

$$\leftarrow \odot (-\tau)^{p-1} = \tau^{p-1} = (\tau^2)^{\frac{1}{2}(p-1)} = \left\{ \left(\frac{-1}{\delta} \right) \delta \right\}^{\frac{1}{2}(p-1)}$$

$$\varphi(x) \equiv x \pmod{\deg 2} \text{ より, } x^p \equiv (\varphi(x))^p \pmod{\deg p+1}$$

$$= \left(\frac{-1}{\delta} \right)^{\frac{1}{2}(p-1)} \delta^{\frac{1}{2}(p-1)} x^p \pmod{\deg p+1, \text{ mod } p}$$

$$\equiv \left\{ (-1)^{\frac{1}{2}(\delta-1)} \right\}^{\frac{1}{2}(p-1)} \left(\frac{\delta}{p} \right) x^p \pmod{\deg p+1, \text{ mod } p}$$

となり、次に得らる:

$$\left(\frac{p}{q}\right) = (-1)^{\frac{1}{2}(p-1) \cdot \frac{1}{2}(q-1)} \left(\frac{q}{p}\right)$$

$$\therefore \left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{1}{2}(p-1) \cdot \frac{1}{2}(q-1)} \quad \square$$

§4.

[1] 形式群の本田理言命, 中央大学集中講義・講義録.

(西栗路文朗)

[2] 超楕円曲線のヤコビ多様体の形式群

(西栗路文朗, 第15回整数論サマースクール報告集 p265~p290)

[3] 形式群の入門的な授業のレジュメ, 代数学特論3.

(加塩月和)

[4] The Arithmetic of Elliptic Curves.

(Silverman, Springer)