

相互法則の詳しい公式

九 大 理 白 谷 克 巳

§ 1. 序

1 の原始 m 乗根を含む代数体での m 中剰余の相互法則の詳しい公式を求める問題は, m が素数中 p^2 の場合に帰着し, 更に p -進体 ($f|p$) でのホルム記号を詳しく決定することになる。

体 k を標数 0 で, 離散的付値をもつ完備体, その剰余類体が標数 $p > 0$ の完成体とする。更に k が 1 の原始 p^n 乗根を含むとし, その一つ ζ_n をとって固定する。

任意の $\alpha, \beta \in k^\times$ に対し

$$u^{p^n} = \alpha, \quad v^{p^n} = \beta, \quad v u = \zeta_n u v$$

で定義される k 上の巡回多元環を $(\alpha, \beta; \zeta_n)$ とすれば,

Witt [15] により

$$(\alpha, \beta; \zeta_n) = (\pi, \omega; \zeta_n)$$

なる本質的には一意的な表示をもつ。 π は k の素元, ω は

k の p^n -primary な元で, 素元 π の選ぶ方は問題にならない。

このとき, 記号 $[\alpha, \beta]$ を $[\alpha, \beta] \equiv_{p^n} \omega$ で定義すれば, 次のことが成立する。ここで, $\equiv_{p^n}$ は両辺が k の元の p^n 乗を無視して等しいことを示す。

$$(1) \quad [\alpha_1 \alpha_2, \beta] \equiv_{p^n} [\alpha_1, \beta] \cdot [\alpha_2, \beta]$$

$$[\alpha, \beta_1 \beta_2] \equiv_{p^n} [\alpha, \beta_1] \cdot [\alpha, \beta_2]$$

$$(2) \quad [\alpha, \beta] \cdot [\beta, \alpha] \equiv_{p^n} 1$$

$$(3) \quad [\alpha, \beta] \equiv_{p^n} 1 \Leftrightarrow \alpha \text{ は } k(\sqrt[p^n]{\beta}) \text{ の元のノルムである。}$$

$$\text{特に, } [-\alpha, \alpha] \equiv_{p^n} 1, \quad [1-\alpha, \alpha] \equiv_{p^n} 1.$$

k が有限体ならば, ノルム記号 (α, β) と次の関係がある。

$$(\alpha, \beta) = (\pi, \omega) = \left(\frac{\omega}{\beta}\right), \quad [\alpha, \beta] \equiv_{p^n} \omega.$$

$\left(\frac{\omega}{\beta}\right)$ は p^n 次の中剰余記号である。

§ 2. Šafarevič の相互法則

p^n 次の中剰余記号を精密に定めることには, 先ず Šafarevič の論文 [12] 及びそれに続く Hasse, Kneser の補充, 簡易化 [8], [9] があって, 簡単にそれを説明する。

T を k の惰性体, R を T の中での, 従って k の中での, k に対する Teichmüller 代表系 (即ち, 乗法的に関して k の完全代表系, $R^p = R$ であり, このような R は一つ存在する) とする。

$K \rightarrow K^p$ なる自己同型に対応する $\mathbb{T}/\mathbb{Q}_p$ の自己同型を $\mathbb{P}$ とすれば

$$\alpha = \sum_{i \gg -\infty} \alpha_i p^i, \quad \alpha_i \in R \longrightarrow \alpha^{\mathbb{P}} = \sum_{i \gg -\infty} \alpha_i^p p^i.$$

K の代数的閉体 $\bar{K}$ に対して, $\bar{T}$ と T の不分離拡大で, 剰余類体 $\bar{K}$ をもつ体とすれば $\mathbb{P}$ は $\bar{T}$ の自己同型として定義される。

$\bar{T}$ の $\bar{K}$ に対する Teichmüller 代表系 $\bar{R}$ をとり, 上と同様である。このとき, $\wp(\bar{\alpha}) = \bar{\alpha}^{\mathbb{P}} - \bar{\alpha}$, $\bar{\alpha} \in \bar{T}$ とおけば, $\wp(\bar{\alpha} + \bar{\beta}) = \wp(\bar{\alpha}) + \wp(\bar{\beta})$ で, $\wp$ は $\bar{T}^+$ の上への自己準同型である。特に, $\alpha \in \mathcal{O}_T$ に対し $\wp(\bar{\alpha}) = \alpha$ なる $\bar{\alpha} \in \mathcal{O}_{\bar{T}}$ が存在する。

さて, Artin - Hasse - Serre の函数 $E(\alpha, x)$ と数 $E(\alpha)$ を次のように定義する。

$$\alpha \in \mathcal{O}_T \text{ に対し, } \alpha = \sum_{i=0}^{\infty} \alpha_i p^i, \quad \alpha_i \in R \text{ とし}$$

$$E(\alpha, x) = \prod_{i=0}^{\infty} E(\alpha_i, x)^{p^i} = \prod_{i=0}^{\infty} \prod_{\substack{m \geq 1 \\ (m, p) = 1}} (1 - \alpha_i^m x^m)^{\frac{\mu(m) p^i}{m}}.$$

容易にわかるように, $E(\alpha, x) \in \mathcal{O}_{\bar{T}}\{x\}$ で, $E(\alpha, x) = e^{-L(\alpha, x)}$ が $\alpha \in R$ に対して成り立つ。ここに, $L(\alpha, x) = \sum_{i=0}^{\infty} \frac{\alpha p^i}{p^i} x^{p^i}$, $\alpha \in \mathcal{O}_T$ である。更に, $E(\alpha + \beta, x) = E(\alpha, x) E(\beta, x)$, $\alpha, \beta \in \mathcal{O}_T$ が成立する。

S_n を 1 の原始 p^n 乗根とし, $S_n = E(1, \bar{\pi}_n)$ により, 素元 $\bar{\pi}$, $\alpha \in \mathcal{O}_T$ に対し $\wp(\bar{\alpha}) = \alpha$ なる $\bar{\alpha}$ を $K\bar{T} = \bar{K}$ の中に

とり $E(\alpha) = E(p^n \bar{\alpha}, \tilde{\pi}_n) = E(\bar{\alpha}, \tilde{\pi}_n)^{p^n}$ で $E(\alpha)$ を定義

する。これは $\bar{\alpha}$ の選ぶ方に依存せず、 α のみで定まる。

そして、 $E(\alpha)$ は k の p^n -primary な単数である。逆に、 k の p^n -primary な元は p^n 乗中を無視して $E(\alpha)$ と書ける。し

かも、 $E(\alpha+\beta) = E(\alpha) \cdot E(\beta)$ であり、この準同型の核は $\mathcal{V} \in \mathcal{O}_T$, $\mathcal{V} \equiv \mathcal{P}(\eta) \pmod{p^n}$, $\eta \in \mathcal{O}_T$ である $\mathcal{V}$ である。

このような $\mathcal{V}$ を $\mathcal{V} \equiv 0 \pmod{p^n}$, $\mathcal{P}$ と書く。

さて、 e を k の分岐指数、 $e_0 = \frac{e}{p-1}$, π を k の任意の素元としたとき、Šafarevič の底表示が次のように成立する。

任意の $\gamma \in k^\times$ に対して

$$\gamma \equiv_{p^n} \pi^{\gamma^*} E(\gamma') \prod_{\substack{1 \leq j \leq e_0 p \\ (j, p) = 1}} E(\gamma_j, \pi^j),$$

γ^* は $\pmod{p^n}$ で定まる有理整数、 γ', γ_j は $\pmod{p^n}$, $\mathcal{P}$ 及び $\pmod{p^n}$ で定まる $\mathcal{O}_T$ の元である。

このとき、Šafarevič の相互法則

$$[\alpha, \beta] \equiv_{p^n} E(\alpha^* \beta' - \alpha' \beta^* + \gamma')$$

即ち

$$(\alpha, \beta) = \sum_n S(\alpha^* \beta' - \alpha' \beta^* + \gamma')$$

が成り立つ。ここで、 S は情性体 T の絶対的スフールを示し、 γ' は次のようにして定まる $\mathcal{O}_T$ の元である。

$p \neq 2$ ならば

$$\prod_{\substack{1 \leq i, j \leq e_0 p \\ (i, p) = (j, p) = 1}} E(j\alpha_i \beta_j, \pi^{ij}) \stackrel{p^n}{=} E(\gamma') \prod_{\substack{1 \leq j \leq e_0 p \\ (j, p) = 1}} E(\gamma_j, \pi^j),$$

$p = 2$ ならば

$$\begin{aligned} & (-1)^{\alpha^* \beta^*} \prod_{\substack{1 \leq i, j \leq 2e_0 \\ (i, 2) = (j, 2) = 1}} \left[E(j\alpha_i \beta_j, \pi^{ij}) \prod_{\mu, \nu=1}^{\infty} E((i2^{\mu-1} + j2^{\nu-1})\alpha_i^{p^\mu} \beta_j^{p^\nu}, \pi^{2^{\mu+\nu}ij}) \right] \\ & \stackrel{p^n}{=} E(\gamma') \prod_{\substack{1 \leq j \leq 2e_0 \\ (j, 2) = 1}} E(\gamma_j, \pi^j). \end{aligned}$$

この Šafarevič の公式では, α, β から定まる元 γ' を求めることが実際の計算において困難である。記号 (α, β) を, α と β それ自身で出来るだけ簡明に求めることが望まれる。
 k の分岐の状態と, α, β をパラメータにして, (α, β) を計算しやすい形に求めることである。

実際, $k = \mathbb{Q}_p(\zeta_p)$ の場合には, Kummer, Takagi, Hasse, Yamamoto, Artin-Tate 等の簡単な公式がある [1], [2], [6], [16]。 p を奇素数, $S = \zeta_p$ とし

$$\begin{aligned} (\alpha, \beta) &= S^{\frac{1}{p}} S_k(S \log \alpha D \log \beta), \\ (\beta, S) &= S^{\frac{1}{p}} S_k(-\log \beta), \\ (\beta, \lambda) &= S^{\frac{1}{p}} S_k\left(\frac{S}{\lambda} \log \beta\right). \end{aligned}$$

ここで, $\alpha \equiv 1 \pmod{p^2}$, $\beta \equiv 1 \pmod{p}$, $\lambda = 1-S$ であり, S_k は k での絶対的スプールを示す。 $\beta = \sum_{i=0}^{\infty} \beta_i \lambda^i$, $\beta_i \in \mathcal{O}_{2p}$ と β の λ -展開としたとき, $D \log \beta = \frac{1}{\beta} \sum_{i=1}^{\infty} i \beta_i \lambda^{i-1}$ と定義す

る。

$p=2$ の場合には, Shiratani [14] が (α, β) を詳しく決定することを試みたが, 最近 Brückner [3] が, 奇素数の場合も含めて, 一つの公式を求めたので, 以下その紹介をする。

§ 3. Brückner の公式

π は k の素元, $\lambda = 1 - \pi$, $\pi = \pi_p$ とする。 $\gamma \in k^{\times}$ に対し, その π -展開を

$$\gamma = \sum_{i \geq -\infty}^{\infty} \gamma_i \pi^i, \quad \gamma_i \in R$$

としたとき, γ に $\gamma(x) = \sum_{i \geq -\infty}^{\infty} \gamma_i x^i \in \mathcal{O}_T\{x\}$ なる級数を対応させる。そして

$$\gamma(x)^p = \sum_{i \geq -\infty}^{\infty} \gamma_i^p x^{pi}$$

と置く。まず, $p \neq 2$ に対して, 記号 $\langle \alpha, \beta \rangle$ を次のように定義する。

$$\langle \alpha, \beta \rangle = \text{Res} \frac{1}{\lambda(x)^p} \left(\frac{1}{p} \log \frac{\alpha(x)^p}{\alpha(x)^p} D \log \beta(x) - \frac{1}{p} \log \frac{\beta(x)^p}{\beta(x)^p} \frac{1}{p} D \log \alpha(x)^p \right).$$

ここで, $\frac{\alpha(x)^p}{\alpha(x)^p} \equiv 1 \pmod{x}$ から $\log \frac{\alpha(x)^p}{\alpha(x)^p}$ 等は意味をもつ。

$D \log \alpha(x)$ は形式的な計数微分即ち $D \log \alpha(x) = \frac{\alpha(x)'}{\alpha(x)}$ を意味し, Res は留数を示す。

定義から計算して

$$\langle \alpha, \beta \rangle \in \mathcal{O}_T,$$

$$\langle \alpha, \beta \rangle + \langle \beta, \alpha \rangle \equiv 0 \pmod{p},$$

$$\langle \alpha_1 \alpha_2, \beta \rangle \equiv \langle \alpha_1, \beta \rangle + \langle \alpha_2, \beta \rangle \pmod{p, \delta},$$

$$\langle \alpha, \beta_1 \beta_2 \rangle \equiv \langle \alpha, \beta_1 \rangle + \langle \alpha, \beta_2 \rangle \pmod{p, \delta},$$

が成立することになる。

さて, $a_1) \alpha = -\pi, \beta = \pi, a_2) \alpha = 1 - p\pi^i, \beta = \pi,$
 $(i, p) = 1, p \in R^\times = R - \{0\}, a_3) \alpha = 1 - p\pi^{e_0 p}, \beta = \pi,$
 $p \in R^\times$ について $[\alpha, \beta] = E(\langle \alpha, \beta \rangle)$ を確かめて, 第2
 補充法則

$$[\alpha, \pi] = E(\langle \alpha, \pi \rangle) = E\left(\text{Res}_{\lambda(\omega)^p} \frac{x^{-1}}{\lambda(\omega)^p} \frac{1}{p} \log \frac{\alpha(\omega)^p}{\alpha(\omega)^p}\right)$$

を得る。b) $\alpha = 1 - p\pi^i, \beta = 1 - \alpha\pi^j, p, \alpha \in R^\times$ に
 ついては, Eisensteinの方法により計算する。即ち

$$[\alpha, \beta] = [\alpha, \delta][\delta, \beta] [-1, \delta] \text{ より}$$

$$[1 - p\pi^i, 1 - \alpha\pi^j] = \prod_{\substack{(m,n)=1 \\ m,n \geq 1}} [1 - (p\pi^i)^m (\alpha\pi^j)^n, \pi]^{-(m_0 i + n_0 j)} [-1, 1 - (p\pi^i)^m (\alpha\pi^j)^n].$$

ここで, m_0, n_0 は $mn_0 - m_0n = 1$ なる有理整数である。

この式を利用して, 少し計算すれば

$$[1 - p\pi^i, 1 - \alpha\pi^j] = E(\langle 1 - p\pi^i, 1 - \alpha\pi^j \rangle)$$

が得られる。従って, すべての場合に, $p \neq 2$ ならば

$[\alpha, \beta] = E(\langle \alpha, \beta \rangle)$ が成立する。これから, 先に述べた

Artin-Tate の式も得られる。

次に, $p = 2$ の場合には, 記号 $\langle \alpha, \beta \rangle$ を次式で定義する

$$\langle \alpha, \beta \rangle = \text{Res} \left[\frac{1}{2\alpha^p} \left(\frac{1}{2} \frac{\alpha\alpha^p - d\alpha^p}{\alpha\alpha^p} D \log \beta(\alpha) - \frac{1}{2} \frac{\beta\alpha^p - \beta\alpha^p}{\beta\alpha^p} \frac{1}{2} D \log \alpha(\alpha)^p \right) \right. \\ \left. + \left(\frac{x}{2\alpha} + x^2 D \log x 2\alpha \right) D \log \alpha(\alpha) \cdot D \log \beta(\alpha) \right].$$

以前と全く同様にして,

$$\langle \alpha, \beta \rangle \in \mathcal{O}_T, \quad ,$$

$$\langle \alpha, \beta \rangle + \langle \beta, \alpha \rangle \equiv 0 \pmod{2},$$

$$\langle \alpha_1 \alpha_2, \beta \rangle \equiv \langle \alpha_1, \beta \rangle + \langle \alpha_2, \beta \rangle \pmod{2, \mathfrak{p}},$$

$$\langle \alpha, \beta_1 \beta_2 \rangle \equiv \langle \alpha, \beta_1 \rangle + \langle \alpha, \beta_2 \rangle \pmod{2, \mathfrak{p}},$$

が確かめられて,

$$[\alpha, \beta] = E(\langle \alpha, \beta \rangle)$$

が成立する。

a), a₂), a₃) の場合にこれを検証し,

$$[\alpha, \pi] = E(\langle \alpha, \beta \rangle)$$

$$= E(\text{Res} \left[\frac{x^{-1}}{2\alpha^p} \frac{\alpha(\alpha)^2 - d\alpha^p}{2 \cdot \alpha(\alpha)^p} + \left(\frac{1}{2\alpha} + x \log x 2\alpha \right) D \log \alpha(\alpha) \right]),$$

$$[-1, \beta] = E(\text{Res} \frac{1}{2\alpha} D \log \beta(\alpha)),$$

がわかる。後, Eisenstein の手続きで, $[1 - p\pi^i, 1 - \alpha\pi^j]$ と $\langle 1 - p\pi^i, 1 - \alpha\pi^j \rangle$ を計算して b) の場合を証明するのであるが, $[-1, (p\pi^i)^m (\alpha\pi^j)^n]$ が寄与して, 以前より複雑な変形を必要とする。

上の定義で補正項をつけるのは, -1 が R に属さず, $\langle \pi, \pi \rangle \equiv 0$ かつ $\langle 1 - p\pi^i, \pi \rangle \equiv 0$ がもしも成立しなからである。

$\langle \alpha, \beta \rangle$ の定義は素元 π に依存するが, ノルム記号と一致し

たのだから， π の取り方に依存しないこともわかる。

この公式を使用して，Hilbert のノルム剰余記号の公式は容易に計算出来る。この節では，等号 $\equiv$ には特に注意せずすべて省略した。

§ 4. Lubin-Tate の式

k の素元 π に対応する $\mathcal{O}_k[[X]]$ の級数 $f(X) : f(X) \equiv \pi X \pmod{\deg 2}$ ， $f(X) \equiv X^q \pmod{\pi}$ ， $q = N_k \pi$ ，から生ずる $\mathcal{O}_k$ で定義される形式的 Lie 群 $F(X, Y)$ の形式的虚数乗法から，Lubin-Tate [10] は次のような公式を導いた。

k の代数的閉体 $\bar{k}$ の中で， π^m -等分点の全体を $\Lambda_{f,m}$ とし，その体を $L_{f,m} = k(\Lambda_{f,m})$ とする。 k の任意の単数 u に対して

$$(u, L_{f,m}/k) \lambda = [u^{-1}]_f(\lambda), \quad \lambda \in \Lambda_{f,m}$$

が成立する。 $(u, L_{f,m}/k)$ は， $L_{f,m}/k$ の相互法則で u に対応する $L_{f,m}/k$ の自己同型を， $[u^{-1}]_f$ は $F(X, Y)$ の u^{-1} に対応する自己準同型を示す。特に， $k = \mathbb{Q}_p$ で， $\pi = p$ ， $f(X) = (1+X)^p - 1$ のときには，これは円体の相互法則 [5] になる。

特別な体 $L_{f,m}$ だけでなく，一般的に k 上のアーベル体に対して，このような詳しい公式が得られることが望ましい。

文 献

- [1] E. Artin - H. Hasse , Die beiden Ergänzungssätze zum Reziprozitätsgesetz der l^n -ten Potenzreste im Körper der l^n -ten Einheitswurzeln , Abh. Math. Semi. Hamburg , 6 , 1928 .
- [2] E. Artin - J. Tate , Class field theory , Princeton Univ., 1951 / 1952 .
- [3] H. Brückner , Eine explizite Formel für das p -te Normsymbol in diskret bewerteten vollständigen Körpern der Charakteristik 0 mit vollkommenem Restklassenkörper der Charakteristik p , Diss. Hamburg Univ., 1965 .
- [4] M. Deuring , Algebren , Berlin , 1935 .
- [5] B. Durck , Norm residue symbol in local number fields , Abh. Math. Semi. Hamburg , 22 , 1958 .
- [6] H. Hasse , Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper , II , J.B.D.M.V. , 1930 ,
- [7] H. Hasse , Die Gruppe der p^n -primären Zahlen für einen Primteiler $\mathfrak{f}$ von p , Jour. reine angew. Math. , 176 , 1937 .

- [8] H. Hasse , Zur Arbeit von I.R. Šafarevič über das allgemeine Reziprozitätsgesetz , Math. Nachr. , 5 , 1951 .
- [9] M. Kneser , Zum expliziten Reziprozitätsgesetz von I.R. Šafarevič , Math. Nachr. , 6 , 1951/52 .
- [10] J. Lubin - J. Tate , Formal complex multiplication in local fields , Ann. Math. , 81 , 1965 .
- [11] H. Rothgiesser , Zum Reziprozitätsgesetz für ℓ^n , Abh. Math. Semi. Hamburg , 11 , 1934 .
- [12] I.R. Šafarevič , A general reciprocity law , Amer. Math. Soc. Transl. , 4 , 1956 .
- [13] K. Shiratani , Note on the Kummer-Hilbert reciprocity law , Jour. Math. Soc. Japan , 12 , 1960 .
- [14] K. Shiratani , On the quadratic norm symbol in local number fields , Journ. Math. Soc. Japan , 13 , 1961 .
- [15] E. Witt , Zyklische Körper und Algebren der Charakteristik p vom Grad p^n , Jour. reine angew. Math. , 196, 1937 .
- [16] K. Yamamoto , On the Kummer-Hilbert reciprocity law , Mem. Fac. Scie. Kyushu Univ. , Ser. A , 3 , 1959 .