q 乗剰余の第二補充法則と負 index ポリログ関数 $\mathrm{Li}_{1-q}(z)$

加塩朋和 *（東京理科大学 創域理工学部 数理科学科）

新潟代数セミナー
2025 年 11 月 28 日 (金) 16:30 – 18:00
新潟大学理学部 A 棟 312 室

概要

平方剰余記号の自然な拡張として、q 乗剰余記号 $(a/p)_q$ が $(a/p)_q = 1 \Leftrightarrow \exists b \text{ s.t. } b^q \equiv a \mod p$ で定義される。Euler は $q = 3$ の場合に様々な予想を述べ、Lemmermeyer は Kummer 理論を用いてそれらを再証明した。今回、一般の奇素数 q と、p が特殊な形の素数の場合に、第二補充法則（すなわち $(q/p)_q = 1$ の必要十分条件）を負 index ポリログ関数 $\mathrm{Li}_{1-q}(z)$ を用いて記述することができたので紹介したい。本結果は平川義之輔氏、関川隆太郎氏、高田直明氏、山本修司氏との共同研究で得られたものである。

1 平方剰余記号

定義 1. p を奇素数, $p \nmid a \in \mathbb{Z}$ とする. このとき **ルジャンドル記号 (平方剰余記号)** を

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & (\exists b \in \mathbb{Z} \text{ s.t. } a \equiv b^2 \not\equiv 0 \mod p) \\ -1 & (\forall b \in \mathbb{Z},\ a \not\equiv b^2 \mod p) \end{cases}$$

で定める.

例 2 ($p = 7$)**.** $(\pm 1)^2 \equiv 1 \mod 7$, $(\pm 2)^2 \equiv 4 \mod 7$, $(\pm 3)^2 \equiv 2 \mod 7$ より

$$\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1, \quad \left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1.$$

* E-mail: tomokazu_kashio@rs.tus.ac.jp

命題 3. p を奇素数とし, 有限体 $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z} = \{a \bmod p \mid a = 0, 1, \ldots, p-1\}$ の乗法群 $\mathbb{F}_p^\times = \{a \bmod p \mid a = 1, \ldots, p-1\}$ を考える. このとき, 自然な準同型写像

$$f\colon \mathbb{F}_p^\times \twoheadrightarrow \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2 \cong \{\pm 1\}$$

は

$$f(a \bmod p) = \left(\frac{a}{p}\right) \quad (p \nmid a \in \mathbb{Z})$$

を満たす.

系 4 (Euler の規準)**.** 奇素数 p に対し

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p \quad (a \in \mathbb{Z}).$$

証明. 完全系列 $\mathbb{F}_p^\times \xrightarrow{\cdot^2} \mathbb{F}_p^\times \xrightarrow{\cdot^{\frac{p-1}{2}}} \mathbb{F}_p^\times$ より. □

定理 5 (平方剰余の相互法則)**.** p, q を相異なる奇素数とする.

(1) 相互法則: $\left(\dfrac{q}{p}\right) = \left(\dfrac{p^*}{q}\right)$. ただし $p^* := (-1)^{\frac{p-1}{2}} p$.
(2) 第一補充法則: $\left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.
(3) 第二補充法則: $\left(\dfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

注意 6 (相互法則の証明に関して)**.** (1) Gauss は 8 種類の証明を与えている.
(2) Lemmermeyer, Reciprocity Laws: From Euler to Eisenstein によれば 2000 年時点で 196 種類の証明方法が知られている [Le, Appendix B].
(3) 第一補充法則は Euler の規準より直ちに従う. もし時間が許せば, 本講演では相互法則と第二補充法則を “類体論の初歩” から導いてみる ($\Rightarrow$ Section 3).

定義 7. 素数 p, q と $p \nmid a \in \mathbb{Z}$ に対し, q 乗剰余記号を

$$\left(\frac{a}{p}\right)_q := \begin{cases} 1 & (a \bmod p \in (\mathbb{F}_p^\times)^q) \\ -1 & (a \bmod p \in \mathbb{F}_p^\times - (\mathbb{F}_p^\times)^q) \end{cases}$$

で定める.

注意 8. $p \not\equiv 1 \mod q \Rightarrow \mathbb{F}_p^\times = (\mathbb{F}_p^\times)^q \Rightarrow (\frac{\forall a}{p})_q = 1$.

定義 9. (負 index の) ポリログ関数を以下で定義する:

$$\mathrm{Li}_{-n}(x) := \left(x\frac{d}{dx}\right)^n \frac{x}{1-x} \in \mathbb{Q}(x)\ (n \in \mathbb{N}).$$

定理 10 (平川-関川-高田-山本-加塩, arXiv:2504.11666)**.** 以下を仮定する:

- q は奇素数.
- p は $p = \sum_{i=0}^{q-1} m^i n^{q-1-i}$ $(m, n \in \mathbb{Z})$ の形に表せる q 以外の素数.

このとき以下は同値.

(1) $\left(\frac{q}{p}\right)_q = 1$.
(2) $\mathrm{Li}_{1-q}(\frac{n}{m}) \equiv 0 \mod q^2$.

ただし, 有理数 $\frac{a}{b}$ $(a, b \in \mathbb{Z},\ b \neq 0,\ \gcd(a, b) = 1)$ に対し, $\frac{a}{b} \equiv 0 \mod q^2 \Leftrightarrow a \equiv 0 \mod q^2$ と定める.

注意 11 (二平方和定理)**.** 奇素数 p に対して以下は同値.

(1) $\mathbb{Z}[\sqrt{-1}]$ において p は可約元.
(2) $\exists x, y \in \mathbb{N}$ s.t. $p = x^2 + y^2$.
(3) $\left(\frac{-1}{p}\right) = 1$.
(4) $p \equiv 1 \mod 4$.

この例に限らず, 平方剰余や q 乗剰余は, 代数体における素数 (より一般に素イデアル) の分解と関係する.

二平方和定理の証明の概略. (1)⇒(2) $p = (a+b\sqrt{-1})(c+d\sqrt{-1}) \Rightarrow p = (a+b\sqrt{-1})(a-b\sqrt{-1}) \Rightarrow p = a^2 + b^2$.

(2)⇒(3) $p = x^2 + y^2 \Rightarrow p = x^2 + y^2,\ p \nmid y \Rightarrow (x/y \bmod p)^2 = -1 \bmod p$.

(3)⇔(4) 第一補充法則 (または Euler の規準).

(3)⇒(1) $-1 \equiv a^2 \mod p \Rightarrow$ (UFD $\mathbb{Z}[\sqrt{-1}]$ の世界で) $p \mid (a + \sqrt{-1})(a - \sqrt{-1})$, $p \nmid (a \pm \sqrt{-1}) \Rightarrow \gcd(a + \sqrt{-1}, p)\gcd(a - \sqrt{-1}, p) \fallingdotseq p$. □

2　代数体での素イデアルの分解

定義-命題 12.　(1) $\mathbb{C}/\mathbb{Q}$ の中間体 K s.t. $[K:\mathbb{Q}]<\infty$ を代数体と呼ぶ. とくに

(a) $d\in\mathbb{Z}-\mathbb{Z}^2$ に対し $\mathbb{Q}(\sqrt{d})=\{x+y\sqrt{d}\mid x,y\in\mathbb{Q}\}$ を二次体と呼ぶ.

(b) $n\in\mathbb{N}$ に対し $\mathbb{Q}(\zeta_n)$ ($\zeta_n:=e^{\frac{2\pi i}{n}}$) を円分体と呼ぶ.

(2) 代数体 K に対し, その整数環を

$$\mathcal{O}_K:=\{\alpha\in K\mid \alpha \text{ は } \mathbb{Z} \text{ 上整}\}$$

で定義する. ただし α が $\mathbb{Z}$ 上整であるとは

$$\text{monic (すなわち最高次係数が 1) な } \exists f(x)\in\mathbb{Z}[x] \text{ s.t. } f(\alpha)=0$$

を満たすことである.

(3) 整数環の非零イデアル $(0)\neq\mathfrak{A}\subset\mathcal{O}_K$ は素イデアルの積に一意的に分解される:

$$\mathfrak{A}=\mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\dots\mathfrak{P}_r^{e_r}\quad(\mathfrak{p}_i \text{ は相異なる素イデアル}, e_i>0).$$

とくに代数体の拡大 K/k に対し, $\mathcal{O}_k$ の素イデアル $\mathfrak{p}$ の $\mathcal{O}_K$ での素イデアル分解:

$$\begin{array}{ccccc} K & \supset & \mathcal{O}_K & \supset & \mathfrak{p}\mathcal{O}_K=\mathfrak{P}_1^{e_1}\dots\mathfrak{P}_g^{e_g} \\ \cup & & \cup & & \wr \\ k & \supset & \mathcal{O}_k & \supset & \mathfrak{p} \end{array}$$

を考えたとき,

(a) ($e_i>0$ となる) $\mathfrak{P}_i$ を $\mathfrak{p}$ の上にある素イデアルと呼ぶ.

(b) e_i を分岐指数と呼ぶ.

(c) $f_i:=[\mathcal{O}_K/\mathfrak{P}_i:\mathcal{O}_k/\mathfrak{p}]$ を剰余次数と呼ぶ:

$$\left.\begin{array}{rcccc} \mathfrak{P}_i & \subset & \mathcal{O}_K & \twoheadrightarrow & \mathcal{O}_K/\mathfrak{P}_i \\ \cup & & \cup & & \cup \\ \mathfrak{P}_i\cap\mathcal{O}_k=\mathfrak{p} & \subset & \mathcal{O}_k & \twoheadrightarrow & \mathcal{O}_k/\mathfrak{p} \end{array}\right\} f_i \text{ 次拡大}$$

(d) $\exists e_i>1$ のとき分岐, $\forall e_i=1$ のとき不分岐と呼ぶ.

(e) 基本等式

$$[K:k]=\sum_{i=1}^{g}e_if_i$$

が成り立つ. $g=[K:k]$ (すなわち $\forall e_i=\forall f_i=1$) のとき完全分解と呼ぶ.

(4) さらに K/k がガロア拡大のとき $e = e_i$, $f = f_i$ は i によらず一定で, 基本等式は

$$[K : k] = efg$$

となる.

例 13. $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$ を考える. このとき

$$\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}, \quad \mathcal{O}_{\mathbb{Q}(\sqrt{-1})} = \mathbb{Z}[\sqrt{-1}]$$

である. 有理素数 $p \in \mathbb{Z}$ で生成される素イデアル $p\mathbb{Z}$ の $\mathcal{O}_{\mathbb{Q}(\sqrt{-1})}$ での分解の様子

$$\begin{array}{ccccccc} \mathbb{Q}(\sqrt{-1}) & \supset & \mathbb{Z}[\sqrt{-1}] & \supset & p\mathbb{Z}[\sqrt{-1}] & = & \boxed{\text{？？？}} \\ \cup & & \cup & & \wr & & \\ \mathbb{Q} & \supset & \mathbb{Z} & \supset & p\mathbb{Z} & & \end{array}$$

は以下の 3 通りに判別できる:

(1) $(e, f, g) = (1, 1, 2)$, すなわち $p\mathbb{Z}[\sqrt{-1}] = \mathfrak{p} \cdot \overline{\mathfrak{p}}$: 分解 $\Leftrightarrow$ $p \equiv 1 \mod 4$.
(2) $(e, f, g) = (1, 2, 1)$, すなわち $p\mathbb{Z}[\sqrt{-1}] = \mathfrak{p}$: 惰性 $\Leftrightarrow$ $p \equiv 3 \mod 4$.
(3) $(e, f, g) = (2, 1, 1)$, すなわち $p\mathbb{Z}[\sqrt{-1}] = \mathfrak{p}^2$: 分岐 $\Leftrightarrow$ $p = 2$.

例えば

(1) $5 = (2 + \sqrt{-1}) \cdot (2 - \sqrt{-1})$.
(2) $3\mathbb{Z}[\sqrt{-1}]$ は素イデアル.
(3) $2 = (1 + \sqrt{-1})^2 \cdot (-\sqrt{-1})$, $-\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]^\times$.

3 素数次 Kummer 拡大の場合

定理 14. k は代数体で $k \in \zeta_n$ とする. このとき k の任意の n 次巡回拡大 K は

$$K = k(\sqrt[n]{\alpha}) \quad (\alpha \in k^\times)$$

の形に書ける. このような K/k は Kummer 拡大と呼ばれる.

定理 15. q を素数とし, 代数体 k, K が

$$\zeta_q \in k, \quad K = k(\sqrt[q]{\mu}) \quad (\mu \in k^\times - (k^\times)^q)$$

を満たしているとする. このとき以下が成り立つ.

(1) k の素イデアル $\mathfrak{p} \nmid q$ に対し
  (a) $\mathfrak{p}$ が K/k で不分岐 $\Leftrightarrow v_{\mathfrak{p}}(\mu) \equiv 0 \mod q$.
  (b) $\mathfrak{p}$ が K/k で完全分解 $\Leftrightarrow \exists \alpha \in k$ s.t. $\frac{\mu}{\alpha^q} \equiv 1 \mod \mathfrak{p}$.
  ここで $v_{\mathfrak{p}}(\mu)$ は (μ) が $\mathfrak{p}$ で割れる回数とする.
(2) k の素イデアル $\mathfrak{q} \mid q$ に対し
  (a) $\mathfrak{q}$ が K/k で不分岐 $\Leftrightarrow \exists \alpha \in k$ s.t. $\frac{\mu}{\alpha^q} \equiv 1 \mod q(1-\zeta_q)$.
  (b) $\mathfrak{q}$ が K/k で完全分解
    $\Leftrightarrow$ (a) を満たす $\alpha \in k$ が更に $\mathrm{tr}_{(\mathcal{O}_k/\mathfrak{q})/\mathbb{F}_q}(\frac{\frac{\mu}{\alpha^q}-1}{q(1-\zeta_q)} \bmod \mathfrak{q}) = 0$.

証明の概略. 体 K を変えずに $\mu \in \mathcal{O}_K$ とできる. 基本的には, $\sqrt[q]{\mu}$ の最小多項式 $x^q - \mu$ の mod$\mathfrak{p}$ での分解の様子が, $\mathfrak{p}$ の分解の様子を知っている (Dedekind-Kummer の定理):

$\mathfrak{p}$ が完全分解 $\overset{\text{おおよそ}}{\Leftrightarrow}$ $x^q - \mu \bmod \mathfrak{p}$ が 1 次式の積に分解 $\overset{\text{おおよそ}}{\Leftrightarrow}$ $\mu \bmod \mathfrak{p}$ が q 乗元.

完全な証明は少し準備が必要. 詳細は [Gr, Chap.I, §6, Theorem 6.3] などを参照. □

例 16. 定理 15 を $q = 2$, $K/k = \mathbb{Q}(\sqrt{-1})/\mathbb{Q}$, $\mu = -1$ に適用して例 13 を導いてみる. $\mathbb{Q} \ni \zeta_2 = -1$ に注意.

(1) $p \neq 2$ に対し,
  (a) $v_p(-1) = 0$ なので不分岐.
  (b) p が分解 $\Leftrightarrow -1 \equiv \exists a^2 \mod p \Leftrightarrow \left(\frac{-1}{p}\right) = 1 \Leftrightarrow p \equiv 1 \mod 4$.
(2) $q = 2$ に対し,
  (a) $-1 \not\equiv \forall a^2 \mod 2^2$ なので 2 は分岐.

なお (1)-(b) の最後の同値には第一補充法則を使った.

例 13 の一般化として以下が成り立つ.

定理 17. $K = \mathbb{Q}(\sqrt{d})$ (d は平方因子を持たない整数) において素数 p は以下の分解法則を満たす. $d_K := \begin{cases} d & (d \equiv 1 \mod 4) \\ 4d & (d \equiv 2, 3 \mod 4) \end{cases}$ とおき, 平方剰余記号を

$$\left(\frac{a}{2}\right) := \begin{cases} 1 & (a \equiv \pm 1 \mod 8) \\ -1 & (a \equiv \pm 3 \mod 8) \end{cases}$$

で拡張しておく.

(1) $\left(\frac{d_K}{p}\right) = 1$ のとき $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, $\mathfrak{p}_1, \mathfrak{p}_2$ は相異なる素イデアル.
(2) $\left(\frac{d_K}{p}\right) = -1$ のとき $p\mathcal{O}_K$ は素イデアル.
(3) $p \mid d_K$ のとき $p\mathcal{O}_K = \mathfrak{p}^2$, $\mathfrak{p}$ は素イデアル.

証明. 定理 15 を $n = 2$, $K/k = \mathbb{Q}(\sqrt{d})/\mathbb{Q}$, $\mu = d$ に適用しても得られる. 標準的な証明は [小野, §25], [足立, 第 11 章, §6] などを参照. □

命題 18 (円分体論 + 類体論の初歩)**.** p を素数とし, 円分体 $\mathbb{Q}(\zeta_p)$ ($\zeta_p := e^{\frac{2\pi i}{p}}$) を考える.

(1) $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong \mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$ である. とくに $0 < d \mid (p-1)$ に対し, $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ の中間体 K_d で $[K_d : \mathbb{Q}] = d$ を満たすものがガロア対応により定まる:

$$\begin{array}{ccccc}
\mathbb{Q}(\zeta_p) & \leftrightarrow & \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}(\zeta_p)) & \cong & \{1\} \\
\cup & & \cap & & \cap \\
K_d & \leftrightarrow & \mathrm{Gal}(\mathbb{Q}(\zeta_p)/K_d) & \cong & (\mathbb{F}_p^\times)^d \\
\cup & & \cap & & \cap \\
\mathbb{Q} & \leftrightarrow & \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) & \cong & \mathbb{F}_p^\times \\
 & & \cup & & \cup \\
 & & [\zeta_p \mapsto \zeta_p^a] & \leftarrow\!\shortmid & a \bmod p.
\end{array}$$

(2) $K_2 = \mathbb{Q}(\sqrt{p^*})$, $p^* := (-1)^{\frac{p-1}{2}}p$.
(3) q を p と異なる素数とし, q 上の K_d の素イデアルの一つを $\mathfrak{Q}$ とおく. このとき q 乗写像 (Frobenius 写像) $\in \mathrm{Gal}((\mathcal{O}_{K_d}/\mathfrak{Q})/\mathbb{F}_q)$ の $\mathrm{Gal}(K_d/\mathbb{Q})$ への持ち上げ (Frobenius 元) は

$$\mathrm{Frob}_q := [\zeta_p \mapsto \zeta_p^q]|_{K_d}$$

である. とくに

$q \bmod p \in (\mathbb{F}_p^\times)^d \Leftrightarrow \mathrm{Frob}_q = \mathrm{id}_{K_d} \Leftrightarrow f = [\mathcal{O}_{K_d}/\mathfrak{Q} : \mathbb{F}_q] = 1 \Leftrightarrow q$ は $K_d/\mathbb{Q}$ で完全分解.

例 19 (平方剰余の相互法則と第二補充法則の証明)**.** [命題 18-(3) の $d = 2$ の場合] + [定理 17 の $d = p^*$ の場合]:

$$q \bmod p \in (\mathbb{F}_p^\times)^2 \Leftrightarrow q \text{ は } \mathbb{Q}(\sqrt{p^*})/\mathbb{Q} \text{ で分解} \Leftrightarrow \left(\frac{p^*}{q}\right) = 1 \tag{3.1}$$

より以下を得る:

(1) $(\frac{q}{p}) = 1 \overset{\text{定義}}{\Leftrightarrow} q \bmod p \in (\mathbb{F}_p^\times)^2 \overset{\text{Eq.(3.1)}}{\Leftrightarrow} (\frac{p^*}{q}) = 1.$

(2) $(\frac{2}{p}) = 1 \overset{\text{定義}}{\Leftrightarrow} q \bmod 2 \in (\mathbb{F}_p^\times)^2 \overset{\text{Eq.}(3.1)}{\Leftrightarrow} (\frac{p^*}{2}) = 1 \Leftrightarrow p \equiv \pm 1 \mod 8 \Leftrightarrow (-1)^{\frac{p^2-1}{8}} = 1$.

詳細は [小野, §29] などを参照.

4 主結果

4.1 考察

定義 20 (定義 7 の再掲)**.** 素数 p, q と $p \nmid a \in \mathbb{Z}$ に対し, q 乗剰余記号を

$$\left(\frac{a}{p}\right)_q := \begin{cases} 1 & (a \bmod p \in (\mathbb{F}_p^\times)^q) \\ -1 & (a \bmod p \in \mathbb{F}_p^\times - (\mathbb{F}_p^\times)^q) \end{cases}$$

で定める.

注意 21. $a \in \mathbb{Z}$ を固定したとき, $q = 2$ の場合, $\left(\frac{a}{p}\right)_2$ の値は p に関する合同条件で表せる ($\because$ 相互法則, 補充法則). 例えば

$$\begin{aligned}
&\left(\tfrac{-1}{p}\right)_2 = 1 && && \Leftrightarrow p \equiv 1 \mod 4, \\
&\left(\tfrac{2}{p}\right)_2 = 1 && && \Leftrightarrow p \equiv 1, 7 \mod 8, \\
&\left(\tfrac{3}{p}\right)_2 = 1 && \Leftrightarrow \left(\tfrac{p^*}{3}\right)_2 = 1 && \Leftrightarrow p \equiv 1, 11 \mod 12, \\
&\left(\tfrac{5}{p}\right)_2 = 1 && \Leftrightarrow \left(\tfrac{p}{5}\right)_2 = 1 && \Leftrightarrow p \equiv 1, 4 \mod 5.
\end{aligned}$$

一方で $q \geq 3$ の場合はそう単純ではない. とくに以下の "Euler 予想" で見られるように, p 自身の合同条件では書き表せない.

定理 22 (Euler–Jacobi–Lehmer)**.** $p \equiv 1 \mod 3$ のとき $4p = L^2 + 27M^2$ $(L, M \in \mathbb{Z})$ と表せる. また, 以下の各同値が成り立つ.

(1) $(\frac{2}{p})_3 = 1 \Leftrightarrow LM \equiv 0 \mod 4$ $(\Leftrightarrow M \equiv 0 \mod 2)$.
(2) $(\frac{3}{p})_3 = 1 \Leftrightarrow LM \equiv 0 \mod 3$ $(\Leftrightarrow M \equiv 0 \mod 3)$.
(3) $(\frac{5}{p})_3 = 1 \Leftrightarrow LM \equiv 0 \mod 5$.
(4) $(\frac{6}{p})_3 = 1 \Leftrightarrow LM \equiv 0, \pm 1 \mod 12$.
(5) $(\frac{7}{p})_3 = 1 \Leftrightarrow LM \equiv 0 \mod 7$.

4.2 q 乗剰余の第二補充法則

(負 index の) ポリログ関数を以下で定義する:

$$\mathrm{Li}_{-n}(x) := \left(x\frac{d}{dx}\right)^n \frac{x}{1-x} \in \mathbb{Q}(x)\ (n \in \mathbb{N}).$$

注意 23. 正 index の方が有名 (?):

$$\begin{aligned}
\mathrm{Li}_0(x) &:= \frac{x}{1-x} = \sum_{k=1}^{\infty} x^k, \\
\mathrm{Li}_1(x) &:= \int \frac{\mathrm{Li}_0(x)}{x}\,dx = \sum_{k=1}^{\infty} \frac{x^k}{k}, \\
&\vdots \\
\mathrm{Li}_n(x) &:= \int \frac{\mathrm{Li}_{n-1}(x)}{x}\,dx = \sum_{k=1}^{\infty} \frac{x^k}{k^n}\ (n \in \mathbb{N}).
\end{aligned}$$

とくに $\mathrm{Li}_1(x) = -\log(1-x)$, $\mathrm{Li}_n(1) = \zeta(n)$, etc.

定理 24 (定理 10 の再掲)**.** 以下を仮定する:

- q は奇素数.
- p は $p = \sum_{i=0}^{q-1} m^i n^{q-1-i}$ $(m, n \in \mathbb{Z})$ の形に表せる q 以外の素数.

このとき以下は同値.

(1) $\left(\frac{q}{p}\right)_q = 1$.
(2) $\mathrm{Li}_{1-q}(\frac{n}{m}) \equiv 0 \mod q^2$.

例 25. $q = 3, 5, 7$ に対し

- $\mathrm{Li}_{1-q}(x)$
- $T_q := \{\frac{n}{m} \bmod q^2 \mid \mathrm{Li}_{1-q}(\frac{n}{m}) \equiv 0 \mod q^2\}$ (∞ は $\frac{m}{n} \equiv 0 \mod q^2$ を意味する).
- 素数 $p = \sum_{i=0}^{q-1} m^i n^{q-1-i}$ で $(\frac{q}{p})_q = 1$ を満たすもの (の一部)

を計算してみる.

(1) $q = 3$.

- $\mathrm{Li}_{1-3}(x) = x(x+1)/(1-x)^3$
- $T_3 = \{0, 8, \infty\}$
- $p = 61, 67, 73, 103, 151, 193, 271, 307, 367, 439, 499, 523, 547, 577, 613, \ldots$

(2) $q = 5$.

- $\mathrm{Li}_{1-5}(x) = x(x+1)(x^2+10x+1)/(1-x)^5$
- $T_5 = \{0, 2, 13, 24, \infty\}$
- $p = 31, 19141, 30941, 48871, 114641, 125591, 141961, 170101, 225241, \ldots$

(3) $q = 7$.

- $\mathrm{Li}_{1-7}(x) = x(x+1)(x^4+56x^3+246x^2+56x+1)/(1-x)^7$
- $T_7 = \{0, 9, 11, 24, 47, 48, \infty\}$
- $p = 43, 10501, 3692053, 109894303, 115928821, 138520537, 141903217, \ldots$

4.3 証明の概略

■Step0. Lemmermeyer **の手法**. 素数 p, q が $p \equiv 1 \mod q$ を満たすとする. このとき, 命題 18-(3) より

$$(\tfrac{q}{p})_q = 1 \Leftrightarrow q \text{ が } K_q/\mathbb{Q} \text{ で完全分解}$$

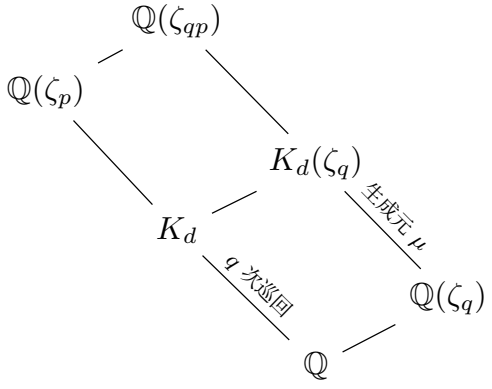
が成り立つ. さらに “分岐指数や剰余次数の基本的な性質” により

$$\Leftrightarrow (1-\zeta_q) \text{ が } K_q(\zeta_q)/\mathbb{Q}(\zeta_q) \text{ で完全分解}$$

と言い換えられる. よって定理 15-(2)-(b) より

$$\Leftrightarrow \exists \xi \in \mathbb{Z}[\zeta_q] \text{ s.t. } \mu \equiv \xi^q \mod (1-\zeta_q)^{q+1} \tag{4.1}$$

と言い換えられる.



■Step1. Kummer **理論による生成元の決定**. $[K_q(\zeta_q)/\mathbb{Q}(\zeta_q)$ が q の外不分岐] と $[K_q(\zeta_q)/\mathbb{Q}$ が Abel 拡大] から, 生成元 μ s.t. $K_q(\zeta_q) = \mathbb{Q}(\zeta_q)(\sqrt[q]{\mu})$ が

$$\mu := \zeta_q^{-n(m-n)^*} \prod_{j=1}^{q-1} (m - n\zeta_q^j)^{j^*} \in \mathbb{Z}[\zeta_q] \tag{4.2}$$

と具体的に書ける. ただし a^* は $aa^* \equiv 1 \mod q$, $1 \leq a \leq q-1$ を満たす整数.

■Step2. **合同条件**. Eq. (4.2) の μ は

$$\mu \equiv \pm 1 \mod (1-\zeta_q)^2 \tag{4.3}$$

を満たしてることが計算で分かる. これが効いて, Eq. (4.1) の条件から更に

$$\Leftrightarrow \log_q \mu \equiv 0 \mod (1-\zeta_q)^{q+1} \tag{4.4}$$

と言い換えられる. ただし

$$\begin{aligned} \log_q \colon \pm 1 + (1-\zeta_q)\mathbb{Z}[\zeta_q] &\to \mathbb{Z}[\zeta_q]/(1-\zeta_q)^{q+1}\mathbb{Z}[\zeta_q], \\ \pm(1+x) &\mapsto \sum_{t=1}^{q} \frac{-(-x)^t}{t} \mod (1-\zeta_q)^{q+1} \quad (x \in (1-\zeta_q)\mathbb{Z}[\zeta_q]) \end{aligned}$$

と定める.

注意 26. 実際は $\log_q$ は乗法群から加法群への連続かつ準同型写像 $\log_q \colon \mathbb{Q}_q(\zeta_q)^\times \to \mathbb{Q}_q(\zeta_q)$. とくに Eq. (4.4) より弱い条件

$$\mu \equiv \xi^q \mod (1-\zeta_q)^{q+1} \Rightarrow \log_q(\xi) \equiv q \log_q(\xi) \equiv 0 \mod (1-\zeta_q)^q$$

は Eq. (4.3) なしでも成り立つ.

■Step3. q **進計算**. $\log_q$ と二項係数の性質を使って計算を頑張ると

$$\begin{aligned}
\log_q \mu &= \log_q \left(\zeta_q^{-n(m-n)^*} \cdot \left(\frac{-n}{m-n}\right)^{\frac{(q-1)q}{2}} \cdot \prod_{j=1}^{q-1} \left(1 + \frac{n}{m-n}(1-\zeta_q^j)\right)^{j^*} \right) \\
&\equiv \sum_{1\le j\le q-1} \sum_{1\le t\le q} \frac{-j^*(\frac{-n}{m-n}(1-\zeta_q^j))^t}{t} \mod (1-\zeta_q)^{q+1} \\
&\equiv \sum_{1\le t\le q,\ 1\le j\le q-1,\ 0\le k\le t} \frac{-(-1)^k j^* \binom{t}{k} (\frac{-n}{m-n})^t \zeta_q^{jk}}{t} \\
&\equiv \cdots \quad (\text{二項係数の性質}) \quad \cdots \\
&\equiv (1-\zeta_q) f(\tfrac{-n}{m-n}) \mod (1-\zeta_q)^{q+1},\ f(x) := \sum_{t=1}^{q} \left(\sum_{\substack{1\le j,k,l\le q-1 \\ k\equiv jl \mod q}} (-1)^k \binom{t}{k} jl \right) \frac{x^t}{t} \\
&\equiv \cdots \quad (1 \text{ 次分数変換: } f(\tfrac{-n}{m-n}) = f(\tfrac{x}{x-1})|_{x=\frac{n}{m}}) \quad \cdots \\
&\equiv (1-\zeta_q) \left(\sum_{j=1}^{q-1} j j^* \right) \mathrm{Li}_{1-q}(\tfrac{n}{m}) \mod (1-\zeta_q)^{q+1}.
\end{aligned}$$

が分かる. $(1-\zeta_q)^{q+1} = q(1-\zeta_q)^2$ に注意すると, Eq. (4.4) は

$$\mathrm{Li}_{1-q}(\tfrac{n}{m}) \equiv 0 \mod q^2$$

と同値になり, 定理 10 の主張を得る.

注意 27. 上記の計算で, 有理式 $f(\frac{x}{x-1})$ と負 index ポリログ関数 $\mathrm{Li}_{1-q}(x)$ が結びつくポイントは, $0 < s \in \mathbb{Z}$ に対して

$$\begin{aligned}
\mathcal{F}_s(x) &:= \sum_{t=0}^{s} \sum_{\substack{s_1,\dots,s_t\ge 1 \\ s_1+\cdots+s_t=s}} \binom{s}{s_1,\dots,s_t} x^t \in \mathbb{Z}[x] \quad \left(\binom{s}{s_1,\dots,s_t} := \frac{s!}{s_1!\cdots s_t!} \right) \\
&= \frac{\mathrm{Li}_{-s}(\frac{x}{1+x})}{x+1}
\end{aligned}$$

が成り立つことであった. この関係式は母関数表示

$$\sum_{s=0}^{\infty} \mathrm{Li}_{-s}(x) \frac{y^s}{s!} = \frac{xe^y}{1-xe^y}, \quad \sum_{s=0}^{\infty} \mathcal{F}_s(x) \frac{y^s}{s!} = \frac{1}{1-x(e^y-1)}$$

から従う.

参考文献

[主結果] Y. Hirakawa, T. Kashio, R. Sekigawa, N. Takada, S. Yamamoto, A note on the second supplementary law of rational power residue symbols, preprint (arXiv:2504.11666).

[Gr] G. Gras, Class field theory: From theory to practice, Springer Monogr. Math. (2003).

[Le] F. Lemmermeyer, Reciprocity Laws: From Euler to Eisenstein, Springer Monogr. Math. (2000).

[足立] 足立 恒雄, 類体論へ至る道 改訂新版: 初等数論からの代数入門, 日本評論社 (2010).

[小野] 小野 孝, 数論序説, 裳華房 (2001).