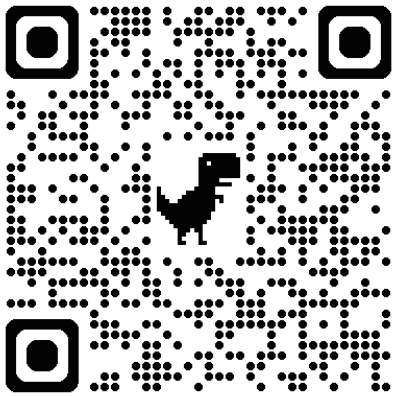
冪乗剰余の第二補充法則に関して

加塩朋和 [1]（東京理科大学）

j.w.w. 平川義之輔, 関川隆太郎, 高田直明, 山本修司

2025 年 3 月 19 日 (水) 16:00–16:50

このスライド ⇒



[1] E-mail: tomokazu_kashio@rs.tus.ac.jp

平方剰余記号

$a \in \mathbb{Z}$, 奇素数 p に対し

$$\left(\frac{a}{p}\right)_2 := \begin{cases} 1 & (a \equiv \exists b^2 \not\equiv 0 \mod p) \Leftrightarrow a \bmod p \in (\mathbb{F}_p^\times)^2, \\ -1 & (a \not\equiv \forall b^2 \mod p) \Leftrightarrow a \bmod p \in \mathbb{F}_p^\times - (\mathbb{F}_p^\times)^2, \\ 0 & (a \equiv 0 \mod p) \Leftrightarrow a \bmod p = 0, \ (\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}). \end{cases}$$

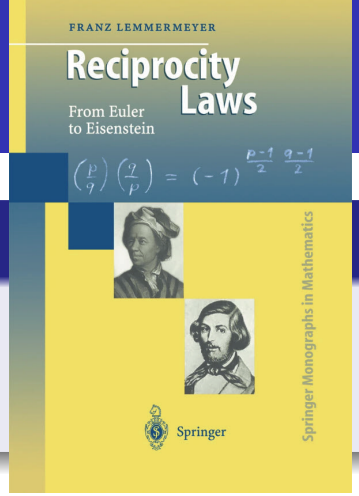
- $\mathbb{F}_p^\times \twoheadrightarrow \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2 \cong \{\pm 1\}$, $a \bmod p \mapsto (\frac{a}{p})_2$ は群準同型.
- Euler の規準: $(\frac{a}{p})_2 \equiv a^{\frac{p-1}{2}} \mod p$.

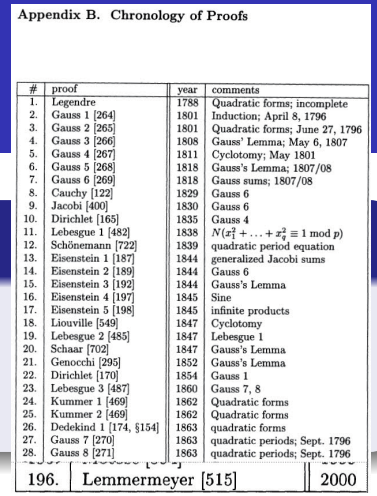
Theorem (平方剰余の相互法則)

p, q を相異なる奇素数とする.

1. 相互法則: $\left(\frac{q}{p}\right)_2 = \left(\frac{p^*}{q}\right)_2$. ただし $p^* := (-1)^{\frac{p-1}{2}} p$.
2. 第一補充法則: $\left(\frac{-1}{p}\right)_2 = (-1)^{\frac{p-1}{2}}$.
3. 第二補充法則: $\left(\frac{2}{p}\right)_2 = (-1)^{\frac{p^2-1}{8}}$.

平方剰余記号 (が愛される理由)




Appendix B. Chronology of Proofs

#	proof	year	comments
1.	Legendre	1788	Quadratic forms; incomplete
2.	Gauss 1 [264]	1801	Induction; April 8, 1796
3.	Gauss 2 [265]	1801	Quadratic forms; June 27, 1796
4.	Gauss 3 [266]	1808	Gauss' Lemma; May 6, 1807
5.	Gauss 4 [267]	1811	Cyclotomy; May 1801
6.	Gauss 5 [268]	1818	Gauss's Lemma; 1807/08
7.	Gauss 6 [269]	1818	Gauss sums; 1807/08
8.	Cauchy [122]	1829	Gauss 6
9.	Jacobi [400]	1830	Gauss 6
10.	Dirichlet [165]	1835	Gauss 4
11.	Lebesgue 1 [482]	1838	$N(x_1^2+\ldots+x_4^2 \equiv 1 \bmod p)$
12.	Schönemann [722]	1839	quadratic period equation
13.	Eisenstein 1 [187]	1844	generalized Jacobi sums
14.	Eisenstein 2 [189]	1844	Gauss 6
15.	Eisenstein 3 [192]	1844	Gauss's Lemma
16.	Eisenstein 4 [197]	1845	Sine
17.	Eisenstein 5 [198]	1845	infinite products
18.	Liouville [549]	1847	Cyclotomy
19.	Lebesgue 2 [485]	1847	Lebesgue 1
20.	Schaar [702]	1847	Gauss's Lemma
21.	Genocchi [295]	1852	Gauss's Lemma
22.	Dirichlet [170]	1854	Gauss 1
23.	Lebesgue 3 [487]	1860	Gauss 7, 8
24.	Kummer 1 [469]	1862	Quadratic forms
25.	Kummer 2 [469]	1862	Quadratic forms
26.	Dedekind 1 [174, §154]	1863	quadratic forms
27.	Gauss 7 [270]	1863	quadratic periods; Sept. 1796
28.	Gauss 8 [271]	1863	quadratic periods; Sept. 1796
196.	Lemmermeyer [515]	2000	

Remark

Reciprocity Laws: From Euler to Eisenstein, Springer Monogr. Math., 487 pp.

Proposition

1. $\mathfrak{f}_{\mathbb{Q}(\sqrt{p^*})} = d_{\mathbb{Q}(\sqrt{p^*})} = p$. とくに $\mathbb{Q}(\zeta_p)/\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}$ $(\zeta_n := \exp(\frac{2\pi i}{n}))$.
2. $$\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) & \xrightarrow{\sigma \mapsto \sigma|_{\mathbb{Q}(\sqrt{p^*})}} & \mathrm{Gal}(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}) \\ \downarrow \wr & & \downarrow \wr \\ (\mathbb{Z}/p\mathbb{Z})^\times & \xrightarrow{a \bmod p \mapsto \left(\frac{a}{p}\right)_2} & \{\pm 1\} \end{array}$$

c.f. 類体論 (F: 代数体, L/F: fin.ab. $\Rightarrow \mathrm{Gal}(L/F)$ が "良く分かる")

$\exists \mathfrak{f}_L$ (導手), $\exists H_{\mathfrak{f}_L}$ (max.ray class field) s.t. $H_{\mathfrak{f}_L}/L/F$: fin.ab.

$$\text{イデアル類群 } \mathrm{Cl}_{\mathfrak{f}_L} \cong \mathrm{Gal}(H_{\mathfrak{f}_L}/F) \overset{\sigma \mapsto \sigma|_K}{\twoheadrightarrow} \mathrm{Gal}(L/F).$$

q 乗剰余記号

Definition ($a \in \mathbb{Z}$, 素数 p, q s.t. $p \equiv 1 \mod q$, $p \nmid a$)

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

- $p \not\equiv 1 \mod q \Rightarrow \mathbb{F}_p^\times \overset{x \mapsto x^q}{\cong} \mathbb{F}_p^\times \Rightarrow \mathbb{F}_p^\times = (\mathbb{F}_p^\times)^q$.
- 別流儀: $\mathbb{Z}[\zeta_q] \ni \alpha$, 素元 π に対し

$$\left(\!\left(\frac{\alpha}{\pi}\right)\!\right)_q \in \{0\} \cup \langle \zeta_q \rangle, \quad \left(\!\left(\frac{\alpha}{\pi}\right)\!\right)_q :\equiv \alpha^{\frac{N(\pi)-1}{q}} \mod \pi.$$

  - c.f. Euler の規準: $(\frac{a}{p})_2 \equiv a^{\frac{p-1}{2}} \mod p$.
  - 準同型: $(\mathbb{Z}[\zeta_q]/(\pi))^\times \twoheadrightarrow (\mathbb{Z}[\zeta_q]/(\pi))^\times/((\mathbb{Z}[\zeta_q]/(\pi))^\times)^q \cong \langle \zeta_q \rangle$.
  - $p \equiv 1 \mod q \Rightarrow N_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(\exists \pi_p) = p$, $\mathbb{Z}[\zeta_q]/(\pi_p) = \mathbb{Z}/(p) = \mathbb{F}_p$.

$$\rightsquigarrow \quad \forall \alpha \bmod \pi_p = \exists a_\alpha \bmod p, \quad \left(\!\left(\frac{\alpha}{\pi_p}\right)\!\right)_q = 1 \Leftrightarrow \left(\frac{a_\alpha}{p}\right)_q = 1.$$

※ $(\frac{a}{p})_q$, $(\!(\frac{\alpha}{\pi})\!)_q$ はここだけの記号 ($[\frac{a}{p}]_q$, $(\frac{\alpha}{\pi})_q$ が一般的).

q 乗剰余記号

$\exists$ 相互法則 $\left(\!\left(\frac{\alpha}{\beta}\right)\!\right)_q = \left(\!\left(\frac{\beta}{\alpha}\right)\!\right)_q \cdot \prod_v (\alpha,\beta)_v$. (省略)

幂乗剰余の第二補充法則: $\left(\frac{q}{p}\right)_q = \ ?$

$q = 2$ の場合

- $\mathbb{F}_3^\times = \{1,2\} > (\mathbb{F}_3^\times)^2 = \{1\} \not\ni 2 \Rightarrow \left(\frac{2}{3}\right)_2 = -1.$
- $\mathbb{F}_5^\times = \{1,2,3,4\} > (\mathbb{F}_5^\times)^2 = \{1,4\} \not\ni 2 \Rightarrow \left(\frac{2}{5}\right)_2 = -1.$
- $\mathbb{F}_7^\times = \{1,2,3,4,5,6\} > (\mathbb{F}_7^\times)^2 = \{1,2,4\} \ni 2 \Rightarrow \left(\frac{2}{7}\right)_2 = 1.$

$q = 3,\ p \equiv 1 \mod 3$ の場合

- $\mathbb{F}_7^\times = \{1,2,3,4,5,6\} > (\mathbb{F}_7^\times)^3 = \{1,6\} \not\ni 3 \Rightarrow \left(\frac{3}{7}\right)_3 = -1.$
- $\left(\frac{3}{13}\right)_3 = -1,\ \left(\frac{3}{19}\right)_3 = -1,\ \left(\frac{3}{31}\right)_3 = -1,\ \left(\frac{3}{37}\right)_3 = -1,\ \left(\frac{3}{43}\right)_3 = -1,$
- $\mathbb{F}_{61}^\times = \{1 \sim 60\} > (\mathbb{F}_{61}^\times)^3 = \left\{\begin{matrix}1,3,8,9,11,20,23,24,27,28,33,\\ 34,37,38,41,50,52,53,58,60\end{matrix}\right\} \ni 3$
  $\Rightarrow \left(\frac{3}{61}\right)_3 = 1.$

q 乗剰余記号

幂乗剰余の第二補充法則: $\left(\frac{q}{p}\right)_q = ?$

Eample ($(\frac{2}{p})_2 = 1$ となる p)

7,17,23,31,41,47,71,73,79,89,97,103,113,127,137,... $\Leftrightarrow p \equiv \pm 1 \mod 8$.

※ $(\mathbb{Z}/8\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong \{\pm 1\}$, $\overline{p} \mapsto (\frac{2}{p})_2$.

Eample ($p \equiv 1 \mod q$, $(\frac{q}{p})_q = 1$ となる p)

q = 3 61,67,73,103,151,193,271,307,367,439,499,523,547,577,613,619,643,
661,727,757,787,853,919,967,991,997,1009,1021,1093,1117,1249,...

q = 5 31,191,251,271,601,641,761,1091,1861,2381,2521,2621,2741,2851,
3061,3121,3461,3581,3631,3701,4001,4201,4261,4271,4421,4591,...

q = 7 43,281,1499,1583,2311,2423,2801,2857,2927,3067,3347,4159,4397,
5531,6217,6427,6917,7687,8443,8597,8737,8779,10501,10627,...

主結果

Theorem

- q は奇素数, p は $p = \sum_{i=0}^{q-1} m^i n^{q-1-i}$ $(m, n \in \mathbb{Z})$ の形の素数に限定する.
- $f_q(x) := \sum_{t=1}^{q} \left(\sum_{\substack{1 \le j,k,l \le q-1 \\ k \equiv jl \mod q}} (-1)^k \binom{t}{k} jl \right) \frac{x^t}{t} \in \mathbb{Z}_{(q)}[x].$

このとき以下は同値.

1. $\left(\frac{q}{p}\right)_q = 1.$
2. $f_q(\frac{-n}{m-n}) \equiv 0 \mod q^2.$
3. $\frac{-n}{m-n} \mod q^2 \in S_q := \{a - f_q(a) \mod q^2 \mid a = 0, 1, \ldots, q-1\}.$

主結果

Theorem

- $q \geq 3$, $p = \sum_{i=0}^{q-1} m^i n^{q-1-i}$, $f_q(x) = \sum_{t=1}^{q} (\sum_{k \equiv jl} (-1)^k \binom{t}{k} jl) \frac{x^t}{t}$.

$$\left(\frac{q}{p}\right)_q = 1 \Leftrightarrow f_q(\tfrac{-n}{m-n}) \equiv 0 \mod q^2 \Leftrightarrow \tfrac{-n}{m-n} \in S_q := \{a - f_q(a) \bmod q^2\}.$$

Eample ($p = \sum_{i=0}^{q-1} m^i n^{q-1-i}$, $(\frac{q}{p})_q = 1$ となる p)

q = 3 $f_3(x) = -x^3 - 3x^2 - 5x$, $S_3 = \{0, 1, 5\}$,
$p = 61, 67, 73, 103, 151, 193, 271, 307, 367, 439, 499, 523, 547, 577, \ldots$

q = 5 $f_5(x) = 4x^5 - \frac{15}{4}x^4 - \frac{25}{3}x^3 - 15x^2 - 29x$, $S_5 = \{0, 1, 2, 13, 24\}$,
$p = 31, 19141, 30941, 48871, 114641, 125591, 141961, 170101, \ldots$

q = 7 $f_7 = 69x^7 + 28x^6 + \frac{42}{5}x^5 - \frac{21}{4}x^4 - \frac{56}{3}x^3 - \frac{77}{2}x^2 - 83x$,
$S_7 = \{0, 1, 6, 17, 25, 33, 44\}$,
$p = 43, 10501, 3692053, 109894303, 115928821, 138520537, \ldots$

主結果の条件: $p = \sum_{i=0}^{q-1} m^i n^{q-1-i}$ に関する注意

Eample ($p = \sum_{i=0}^{q-1} m^i n^{q-1-i}$, $\left(\frac{q}{p}\right)_q = 1$ となる p)

$q = 3$ $p = 61, 67, 73, 103, 151, 193, 271, 307, 367, 439, 499, 523, 547, 577, \ldots$

$q = 5$ $p = 31, 19141, 30941, 48871, 114641, 125591, 141961, 170101, \ldots$

$q = 7$ $p = 43, 10501, 3692053, 109894303, 115928821, 138520537, \ldots$

Eample ($p \equiv 1 \mod q$, $\left(\frac{q}{p}\right)_q = 1$ となる p)

$q = 3$ 61,67,73,103,151,193,271,307,367,439,499,523,547,577,613,619,643,
661,727,757,787,853,919,967,991,997,1009,1021,1093,1117,1249,...

$q = 5$ 31,191,251,271,601,641,761,1091,1861,2381,2521,2621,2741,2851,
3061,3121,3461,3581,3631,3701,4001,4201,4261,4271,4421,4591,...

$q = 7$ 43,281,1499,1583,2311,2423,2801,2857,2927,3067,3347,4159,4397,
5531,6217,6427,6917,7687,8443,8597,8737,8779,10501,10627,...

関連する研究 (Euler 予想, Feit-Thompson 予想)

Theorem (Euler 予想, Lehmer の定理)

$p \equiv 1 \mod 3 \Rightarrow 4p = L^2 + 27M^2$ と表せて

$\vdots$

② $\left(\frac{3}{p}\right)_3 = 1 \Leftrightarrow M \equiv 0 \mod 3.$

$\vdots$

Conjecture (Feit-Thompson 予想)

相異なる素数 p, q に対し $\Phi_q(p) \nmid \Phi_p(q)$. ($\Phi_q(x) = \sum_{i=0}^{q-1} x^i$ は円分多項式)

Remark

1. 主結果 with $q = 3 \Leftrightarrow$ Euler 予想 ②.
2. Euler 予想 ② $\Rightarrow$ Feit-Thompson 予想 with $q = 3$ and $p \not\equiv 8 \mod 9$. (c.f. M. Le.)
3. 高田氏の修士論文中で $q = 5$ の場合 + α. (c.f. E. Lehmer, L. E. Dickson, J. B. Muskat.)

関連する研究 (Euler 予想とその拡張)

Theorem (Euler 予想, Lehmer の定理)

$p \equiv 1 \mod 3 \Rightarrow 4p = L^2 + 27M^2$ と表せて

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. $(\frac{6}{p})_3 = 1 \overset{?}{\Leftrightarrow} LM \equiv 0, \pm 1 \mod 12$.
5. $(\frac{7}{p})_3 = 1 \Leftrightarrow LM \equiv 0 \mod 7$.

Theorem (E. Lehmer, L. E. Dickson, J. B. Muskat)

$$p \equiv 1 \bmod 5 \Rightarrow \begin{cases} 16p = x^2 + 50u^2 + 50v^2 + 125w^2 \\ xw = v^2 - 4uv - u^2 \\ x \equiv 1 \mod 5 \end{cases}$$ と表せて

- $(\frac{5}{p})_5 = 1 \Leftrightarrow u \equiv 2v \mod 5$.

証明の準備: Kummer 理論, Lemmermeyer の手法

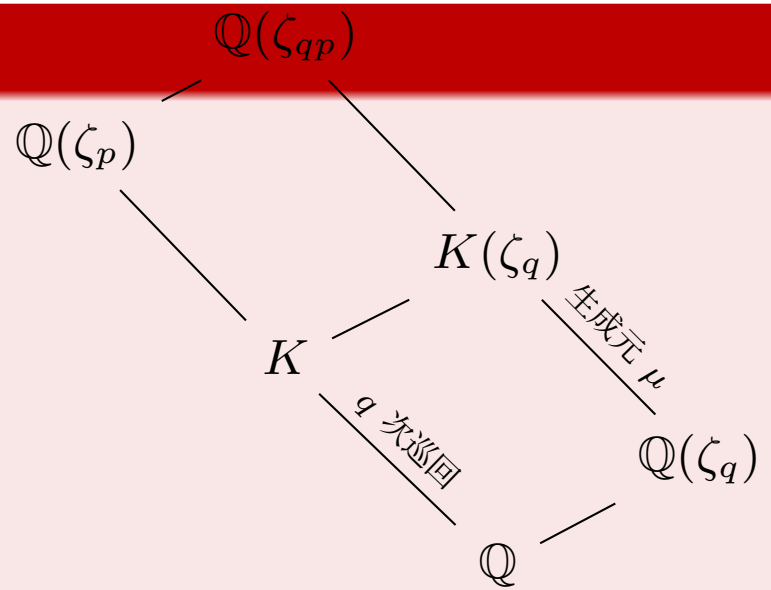
Theorem (Kummer 理論)

q 次巡回拡大 L/F $(\ni \zeta_q)$ $\overset{L=F(\sqrt[q]{\mu})}{\Longleftrightarrow}$ 生成元 $\mu \in F^\times/(F^\times)^q$.

1. $\mathfrak{p} \nmid q$ が L/F で不分岐 $\Leftrightarrow v_{\mathfrak{p}}(\mu) \equiv 0 \mod q$.
2. $\mathfrak{p} \nmid q$ が L/F で (完全) 分解 $\Leftrightarrow \mu \in (L_{\mathfrak{P}}^\times)^q$.
3. $\mathfrak{q} \mid q$ が L/F で不分岐 $\Leftrightarrow \mu \equiv \exists \xi^q \mod \mathfrak{q}^{qe_{\mathfrak{q}|(1-\zeta_q)}}$.
4. $\mathfrak{q} \mid q$ が L/F で (完全) 分解 $\Leftrightarrow \mu \equiv \exists \xi^q \mod \mathfrak{q}^{qe_{\mathfrak{q}|(1-\zeta_q)}+1}$.

Lemmermeyer の手法 for Euler 予想

$$
\begin{aligned}
&\left(\frac{q}{p}\right)_q = 1 \\
&\Leftrightarrow q^{\frac{p-1}{q}} \equiv 1 \mod p \\
&\Leftrightarrow q \text{ が } K/\mathbb{Q} \text{ で分解} \\
&\Leftrightarrow (1-\zeta_q) \text{ が } K(\zeta_q)/\mathbb{Q}(\zeta_q) \text{ で分解} \\
&\Leftrightarrow \mu \equiv \exists \xi^q \mod (1-\zeta_q)^{q+1}.
\end{aligned}
$$



証明の概略

Step1. Kummer 理論 ⇒ 生成元の決定

$$\mu =: \zeta_q^{-n(m-n)^*} \prod_{j=1}^{q-1} (m - n\zeta_q^j)^{j^*} \in \mathbb{Z}[\zeta_q] \quad (a^* :\equiv a^{-1} \bmod q).$$

Step2. Lemmermeyer の手法 ⇒ 合同条件

$$\left(\tfrac{q}{p}\right)_q = 1 \Leftrightarrow \mu \equiv \exists \xi^q \mod (1-\zeta_q)^{q+1} \Leftrightarrow \log_q \mu \equiv 0 \mod (1-\zeta_q)^{q+1}.$$

Step3. q 進計算 ⇒ $f_q(x) = \sum_{t=1}^{q} \left(\sum_{k \equiv jl} (-1)^k \binom{t}{k} jl\right) \frac{x^t}{t}$

$$\log_q \mu = \log_q \left(\zeta_q^{-n(m-n)^*} \cdot \left(\tfrac{-n}{m-n}\right)^{\frac{(q-1)q}{2}} \cdot \prod_{j=1}^{q-1} \left(1 + \tfrac{n}{m-n}(1-\zeta_q^j)\right)^{j^*} \right)$$

$$\equiv \sum_{1 \le j \le q-1} \sum_{1 \le t \le q} \frac{-j^* \left(\frac{-n}{m-n}(1-\zeta_q^j)\right)^t}{t} \mod (1-\zeta_q)^{q+1}$$

$$\equiv \sum_{t,j,k} \frac{-(-1)^k j^* \binom{t}{k} \left(\frac{-n}{m-n}\right)^t \zeta_q^{jk}}{t} \equiv \cdots \equiv (1-\zeta_q) f_q\left(\tfrac{-n}{m-n}\right) \mod (1-\zeta_q)^{q+1}.$$

※ プロ研 2022 水戸さん (Lemmermeyer の手法 (?)) ⇒ プロ研 2022(?) 関川さん (Kummer 理論)
⇒ 2023 年後期 高田さん-平川さん (問題提起) ⇒ プロ研 2023 山本さんと相部屋 (計算方法の確立)

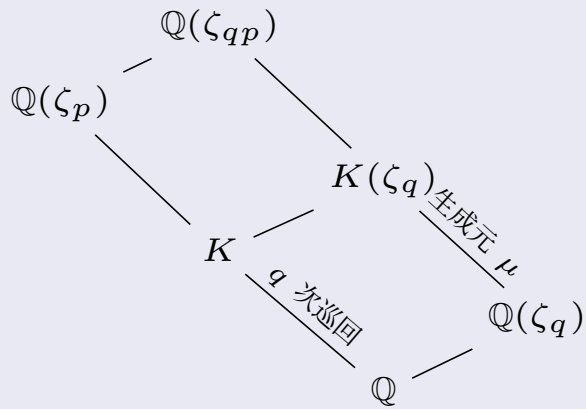
証明の難所 1

Step1. Kummer 理論 ⇒ 生成元の決定

$$\mu =: \zeta_q^{-n(m-n)^*} \prod_{j=1}^{q-1} (m - n\zeta_q^j)^{j^*} \in \mathbb{Z}[\zeta_q] \quad (a^* :\equiv a^{-1} \bmod q).$$

Kummer 理論

1. $\mathfrak{p} \nmid q$ が $K(\zeta_q)/\mathbb{Q}(\zeta_q)$ で不分岐
   $\Leftrightarrow v_{\mathfrak{p}}(\mu) \equiv 0 \mod q.$
3. $\mathfrak{q} = (1 - \zeta_q) \mid q$ が $K(\zeta_q)/\mathbb{Q}(\zeta_q)$ で不分岐
   $\Leftrightarrow \mu \equiv \exists \xi^q \mod \mathfrak{q}^q.$



- 条件: $p = \sum_{i=0}^{q-1} m^i n^{q-1-i} = N_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(m - n\zeta_q)$
  $\Rightarrow (m - n\zeta_q^j) \mid p \Rightarrow pq$ の外で不分岐.
- p で不分岐 $\Leftarrow$ 条件 3 $\Leftarrow$ Step2, 3.
- $K(\zeta_q)/\mathbb{Q}$: アーベル拡大 $\Rightarrow$ 指数の決定.

証明の難所 2

Step2. Lemmermeyer の手法 ⇒ 合同条件

$$\left(\frac{q}{p}\right)_q = 1 \Leftrightarrow \mu \equiv \exists \xi^q \mod (1-\zeta_q)^{q+1} \Leftrightarrow \log_q \mu \equiv 0 \mod (1-\zeta_q)^{q+1}.$$

- 自明な議論だと $\log_q \xi^q = q \log_q \xi \in q(1-\zeta_q) = (1-\zeta_q)^q$ 止まり.
- 特殊事情： $\mu \equiv \pm 1 = (\pm 1)^q \mod (1-\zeta_q)^2$.
- $A \equiv \zeta \mod (1-\zeta_q)^e \overset{A \equiv \zeta \mod (1-\zeta_q)^2}{\Leftrightarrow} \log_q A \equiv 0 \mod (1-\zeta_q)^e$
  $\rightsquigarrow$ ($\Leftarrow$).
- ($\Rightarrow$) では任意の ξ が対象
  $\rightsquigarrow \mathbb{Z}[\zeta_q]/(1-\zeta_q)^{q+1} \supset \{\text{“}q \text{ 乗元”}\} = \cdots$.

証明の難所 3

Step3. q 進計算 $\Rightarrow f_q(x) = \sum_{t=1}^{q}(\sum_{k\equiv jl}(-1)^k\binom{t}{k}jl)\frac{x^t}{t}$

$$\log_q \mu \equiv \sum_{t,j,k} \frac{-(-1)^k j^* \binom{t}{k}(\frac{-n}{m-n})^t \zeta_q^{jk}}{t} \equiv \cdots \equiv (1-\zeta_q) f_q(\tfrac{-n}{m-n}).$$

- 計算めっちゃ頑張る.

まとめ

- $q \geq 3$, $p = \sum_{i=0}^{q-1} m^i n^{q-1-i}$, $f_q(x) = \sum_{t=1}^{q} (\sum_{k \equiv jl} (-1)^k \binom{t}{k} jl) \frac{x^t}{t}$.

$\left(\frac{q}{p}\right)_q = 1 \Leftrightarrow f_q(\frac{-n}{m-n}) \equiv 0 \mod q^2 \Leftrightarrow \frac{-n}{m-n} \in S_q := \{a - f_q(a) \bmod q^2\}$.

- 条件: $p = \sum_{i=0}^{q-1} m^i n^{q-1-i} = N_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(m - n\zeta_q)$.
- Kummer-Lemmermeyer: $(\frac{q}{p})_q = 1 \Leftrightarrow \mu \equiv \exists \xi^q \mod (1-\zeta_q)^{q+1}$
  $\Leftrightarrow \log_q \mu \equiv 0 \mod (1-\zeta_q)^{q+1}$.
- 計算: $\log_q \mu \equiv (1-\zeta_q) f_q(\frac{-n}{m-n}) \mod (1-\zeta_q)^{q+1}$.

- p の条件を弱められるか？
- $\left(\frac{l}{p}\right)_q$ (素数 $l \neq q$), $\left(\frac{n}{p}\right)_q$ (合成数 n), $\left(\left(\frac{\lambda}{\pi}\right)\right)_q$ ($\lambda, \pi \in \mathbb{Z}[\zeta_q]$) では？
- $f_q(x) = \sum_{t=1}^{q} \left(\sum_{\substack{1 \leq j,k,l \leq q-1 \\ k \equiv jl \mod q}} (-1)^k \binom{t}{k} jl \right) \frac{x^t}{t}$ v.s. ポリログ.
