ある種の２ベキ次巡回拡大体のイデアル類群について

（市村文男氏（茨城大学）との共同研究）

徳島大学　高橋浩樹（隅田）

§1. Introduction

今回のテーマの2つの源流

- 虚2次体のイデアル類群の2部分

  (Gauss, .. Rédei-Reichardt, ... , A. Smith)

  種の理論, Rédei行列, governing field.

  (§2で解説する.)

- 円分体の $\mathbb{Z}_p$-拡大のイデアル類群

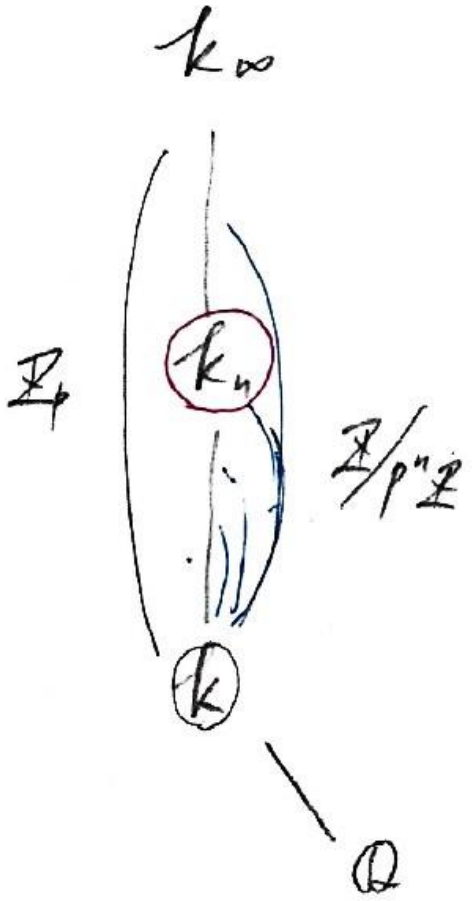
  (Iwasawa, ... , Ferrero-Washington, .. Mazur-Wiles)

  岩澤類数公式, $\mu = 0$, 岩澤主予想, p進L関数

岩澤理論との対比

p：素数，$k/\mathbb{Q}$：有限次代数体

A_n：k_nのイデアル類群のp部分



岩澤類数公式

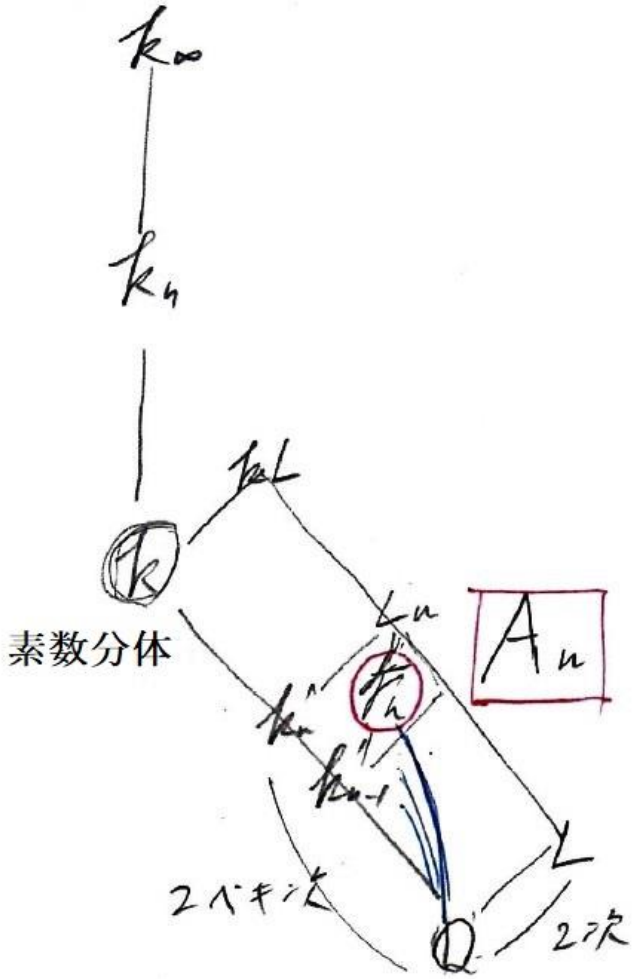
$\exists \lambda = \lambda_p(k_\infty/k)$, $\exists \mu = \mu_p(k_\infty/k) \in \mathbb{Z}_{\geq 0}$

$\exists \nu = \nu_p(k_\infty/k)$ s.t.

$$\#A_n = p^{\lambda n + \mu p^n + \nu} \qquad n \gg 0.$$

「無限次拡大で成立する式」

今回の研究対象

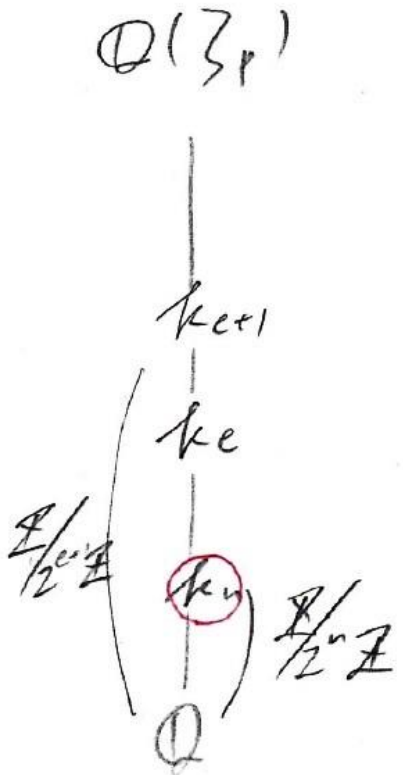


市村氏のたとえ「逆さ富士」
「k/Qを湖面と見立て，そこに無限のものを対象とする式がどう映るか？」

§2. 8p分体の部分体.

(Tokyo J. Math., 2021)

$p = 1 + 2^{e+1}f$ (f: odd, $e \geq 0$.)

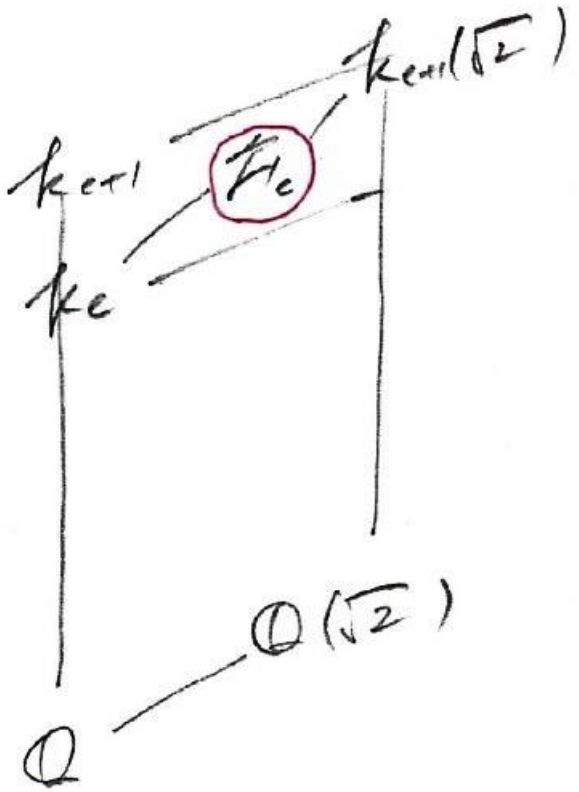


k_{e+1} : 唯一 2^{e+1}次巡回拡大

$k_e = k_{e+1}^{+}$ (最大実部分体)

$A_n := A_{k_n} = Cl(k_n)[2^n]$ は自明.

(・A_e が自明
・2べキ次巡回拡大
・1つの素点 p のみ分岐)



$\mathcal{F}_e$: 虚 2^{e+1} 次巡回拡大

$A_e := A_{\mathcal{F}_e} = \mathcal{O}(\mathcal{F}_e)[2^\infty]$ は自明ではない.

($k_{e+1}(\sqrt{2})/\mathcal{F}_e$ は不分岐
2次拡大)

$e_p = 0 \Leftrightarrow p \equiv 3 \bmod 4 \Leftrightarrow \mathcal{F}_e$: 虚二次体

- $e_p = 0$ $(p \equiv 3 \bmod 4)$ の場合

  ← $\mathbb{Q}(\sqrt{p})$ で分岐する素点の個数

  - 2-rank A_e $=$ ⓣ$-1 = 1$

    ↑ Gauss (種の理論)

  - 4-rank A_e $=$ ⓣ$-1-\mathrm{rk}\, R_{\mathbb{Q}(\sqrt{p})} = \begin{cases} 0 \cdots & \left(\frac{2}{p}\right) = -1 \\ 1 \cdots & \left(\frac{2}{p}\right) = 1 \end{cases}$

    ↑ Rédei-Reichardt (Rédei行列)

  - 8-rank 以下:

    2^k-rank $A_{\mathbb{Q}(\sqrt{dp})}$ $\longleftrightarrow$ ($M_{d,k}/\mathbb{Q}$ での p の分解)

    ↑ Governing field

    (Cohn-Lagarias 1983, Stevenhagen 1988)

  - 16-rank 以上

    - character sum (Miloric, Koyman 2017, 2021)
    - Relative governing field. (A. Smith 2017, ArXiv)

      Cohen-Lenstra heuristic (2-part) → Gold feld's conj.

      $\mathrm{rk}_{\mathbb{Z}} E^{(n)}(\mathbb{Q}) = \begin{cases} 0 \cdots 50\% \\ 1 \cdots 50\% \end{cases}$

$$2^k\text{-rank}\, A = \dim_{\mathbb{F}_2} 2^{k-1}A/2^kA$$

・$e_p \geq 1$ ($p \equiv 1 \bmod 4$) の場合

Q. A_e はどのような岩澤加群の構造を持ちうるのか？

$$\left(\begin{array}{ccc} \mathbb{Z}_2[Gal(\mathbb{Z}_e/\mathbb{Q})] \text{-加群} & & r : Gal\text{の生成元} \\ \| & & \updownarrow \\ \mathbb{Z}_2[[T]]/((1+T)^{2^{e+1}}-1) \text{-加群} & & 1+T \end{array} \right)$$

$$\Lambda := \mathbb{Z}_2[[T]]$$

$$k_p := \max\left\{ k : p \text{ は } \mathbb{Q}(2^{\frac{1}{2^{e-k+1}}}) \text{ で完全分解} \right\}$$

$$(0 \leq k \leq e+1)$$

定理A

- $k_p \geq 1$ のとき,

$$A_e \cong \Lambda/(T^{2^{e-k+1}}, 2) \cong (\mathbb{Z}/2\mathbb{Z})^{\oplus 2^{e-k+1}}$$

4-rank = 0.

ただし, $\begin{cases} e_p = 1 \text{ のとき}, & k_p \neq 1 \\ e_p \geq 2 \text{ のとき}, & k_p \neq e_p + 1. \end{cases}$

- $k_p = 0$ のとき,

$$A_e \cong \Lambda/((T+1)^{2^e}+1, 2^{s_p-1}T^{b_p}, 2^{s_p}) \cong \left(\mathbb{Z}/2^{s_p-1}\mathbb{Z}\right)^{\oplus 2^e - b_p} \oplus \left(\mathbb{Z}/2^{s_p}\mathbb{Z}\right)^{\oplus b_p}$$

ただし, $\begin{cases} e_p \neq 1, \\ e_p = 2 \text{ のとき}, \ s_p = 2, \ b_p = 1, \\ e_p \geq 3 \text{ のとき}, \ s_p = 2, \ 2 \leq b_p \leq 2^e \\ \qquad\qquad\ \ s_p \geq 3, \ 1 \leq b_p \leq 2^e \end{cases}$

(e_p, k_p) で構造が決定

(e_p, k_p) だけでは構造が決まらない!

実例

・$p < 10^6$ での (e_p, κ_p) の分布

Table 1: The number of prime numbers with $(e_p, \kappa_p) = (e, \kappa)$.

e \ κ	0	1	2	3	4	5	6	7	8	9	total
0	19669	19653	0	0	0	0	0	0	0	0	39322
1	0	0	19623	0	0	0	0	0	0	0	19623
2	2471	2426	4894	0	0	0	0	0	0	0	9791
3	600	609	1206	2434	0	0	0	0	0	0	4849
4	155	150	312	621	1218	0	0	0	0	0	2456
5	38	34	69	174	294	624	0	0	0	0	1233
6	11	12	24	29	71	149	322	0	0	0	618
7	0	1	3	11	22	41	83	146	0	0	307
8	3	1	1	0	7	18	18	33	72	0	153
9	0	0	1	2	2	2	2	10	19	34	72

e \ κ	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	total
10	1	0	1	1	1	5	7	15	0	0	0	0	0	0	0	31
11	0	0	1	2	1	1	1	4	15	0	0	0	0	0	0	25
12	0	0	0	0	1	0	0	1	2	5	0	0	0	0	0	9
13	0	0	0	0	0	0	0	0	1	1	2	0	0	0	0	4
14	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	2
15	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1

実例

・$p < 10^6$ での (e_p, κ_p, i_p) の分布，$i_p = \mathrm{ord}_2(\#A_e)$

Table 2: The exponent of 2-class number and the minimum primes.

e	i	$n_{e,i}$	$p_{e,i}$	e	i	$n_{e,i}$	$p_{e,i}$	e	i	$n_{e,i}$	$p_{e,i}$
3	10	309	337	4	18	85	2593	5	34	18	15809
	11	112	43441		19	31	26849		35	8	131009
	12	80	39761		20	21	10657		36	1	868801
	13	49	28657		21	13	68449		37	6	83777
	14	25	12049		22	8	138977		38	4	92737
	15	5	79889		23	2	598817		39	1	470081
	16	11	34961		24	6	31649				
	17	7	44497		25	1	476513				
	18	2	57457		26	2	572321				

e	i	$n_{e,i}$	$p_{e,i}$	e	i	$n_{e,i}$	$p_{e,i}$
6	66	6	266369	8	258	3	115201
	67	2	195457				
	68	2	299393				
	70	1	710273				

• $p < 5 \times 10^7$ で $(3, 0, i_p)$ の個数

Table 3: The exponent of 2-class number ($p < 5 \times 10^7$).

i	$n'_{3,i}$	$p_{3,i}$	$A_{\mathcal{F}}$
10	11718	337	$(\mathbb{Z}/2)^{\oplus 6} \oplus (\mathbb{Z}/4)^{\oplus 2}$
11	5481	43441	$(\mathbb{Z}/2)^{\oplus 5} \oplus (\mathbb{Z}/4)^{\oplus 3}$
12	3170	39761	$(\mathbb{Z}/2)^{\oplus 4} \oplus (\mathbb{Z}/4)^{\oplus 4}$
13	1394	28657	$(\mathbb{Z}/2)^{\oplus 3} \oplus (\mathbb{Z}/4)^{\oplus 5}$
14	740	12049	$(\mathbb{Z}/2)^{\oplus 2} \oplus (\mathbb{Z}/4)^{\oplus 6}$
15	367	79889	$(\mathbb{Z}/2) \oplus (\mathbb{Z}/4)^{\oplus 7}$
16	269	34961	$(\mathbb{Z}/4)^{\oplus 8}$
17	133	44497	$(\mathbb{Z}/4)^{\oplus 7} \oplus (\mathbb{Z}/8)$
18	46	57457	$(\mathbb{Z}/4)^{\oplus 6} \oplus (\mathbb{Z}/8)^{\oplus 2}$
19	34	2347409	$(\mathbb{Z}/4)^{\oplus 5} \oplus (\mathbb{Z}/8)^{\oplus 3}$
20	15	3295249	$(\mathbb{Z}/4)^{\oplus 4} \oplus (\mathbb{Z}/8)^{\oplus 4}$
21	11	3238801	$(\mathbb{Z}/4)^{\oplus 3} \oplus (\mathbb{Z}/8)^{\oplus 5}$
22	3	5897329	$(\mathbb{Z}/4)^{\oplus 2} \oplus (\mathbb{Z}/8)^{\oplus 6}$
23	3	21061361	$(\mathbb{Z}/4) \oplus (\mathbb{Z}/8)^{\oplus 7}$
24	2	20264401	$(\mathbb{Z}/8)^{\oplus 8}$
26	1	6765169	$(\mathbb{Z}/8)^{\oplus 6} \oplus (\mathbb{Z}/16)^{\oplus 2}$

§3. 8pℓ分体の部分体

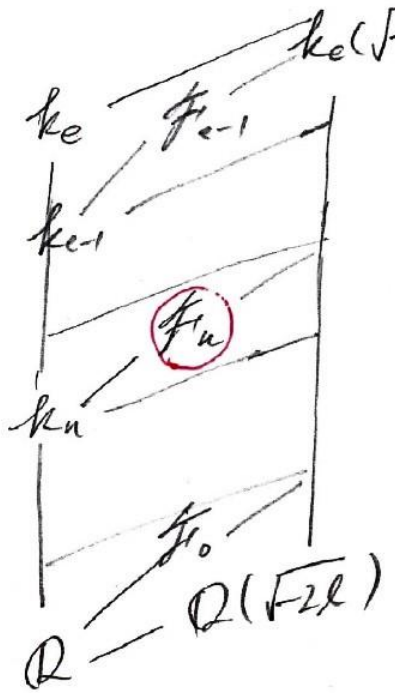
$L = \mathbb{Q}(\sqrt{2})$ $(\S 2) \longrightarrow L = \mathbb{Q}(\sqrt{-2\ell})$

とすると、どうなるか？

$\mathbb{P} = \{\ell : \text{prime} \mid (\frac{p}{\ell}) = -1,\ \ell \equiv \pm 1 \bmod 8\} \cup \{1\}$

↓ $k_{e+1}/\mathbb{Q}$で不分解、 ↓ 4-rank >0 となりうる。

$= \mathbb{P}^+ \sqcup \mathbb{P}^-$ （$\ell \bmod 8$ で分ける。）



F_n：底 2^{n+1}次巡回拡大

$(0 \le n \le e-1)$

$(F_n \neq F_{n-1})$

$\boxed{A_n} := A_{F_n} = Cl(F_n)[2^\infty]$

e_p, k_p : $\S 2$ と同じ

$f_p := \min\{e_p - k_p + 1,\ e_p\}$

$n_p^{\pm} := \min\left\{ n \;\middle|\; 4\text{-rank } A_n < 2^n \right\}$ or ∞

$\left.\begin{array}{l} {}^2\ell \in \mathbb{P}^{\pm} \\ (1 \le n \le f_p - 1) \end{array}\right\}$

$\Updownarrow$

${}^4\ell$

$$A_n \cong \begin{cases} \Lambda / \Theta_n(1) & \cdots\cdots\cdots\ \ell = 1 \\ \Lambda/(T,2) \oplus \Lambda/\Theta_n(\ell) & \cdots\ \ell \neq 1 \end{cases}$$

$\cup$

A_n'

定理B　$0 \le n \le e_p - 1$, $\ell \in \mathbb{P}^{\pm}$ に対し,

- $f_p \le n \le e_p - 1$ のとき,

$$A_n' \cong \Lambda/(T^{2^{f_p}}, 2) \cong \left(\mathbb{Z}/2\mathbb{Z}\right)^{\oplus 2^{f_p}}$$

2-rank 一定,　4-rank = 0.

- $n_p^{\pm} \le n \le f_p - 1$ のとき,

$$A_n' \cong \Lambda/((T+1)^{2^n}+1, 2T^{b_p^{\pm}}, 4) \cong \left(\mathbb{Z}/2\mathbb{Z}\right)^{\oplus 2^n - b_p^{\pm}} \oplus \left(\mathbb{Z}/4\mathbb{Z}\right)^{\oplus b_p^{\pm}}$$

$(2^{n_p^{\pm}-1} \le b_p^{\pm} < 2^{n_p^{\pm}})$

2-rank $= 2^n$, 4-rank $= b_p^{\pm}$, 8-rank $= 0$

(ℓ によらない!!)　((e_p, k_p) だけで $\pm$ は決まらない.)

(n によらない!)

- $0 \le n \le n_p^{\pm} - 1$ のとき,

$$A_n' \cong \Lambda/((T+1)^{2^n}+1, 2^{s_n(\ell)-1}T^{b_n(\ell)}, 2^{s_n(\ell)}) \cong \left(\mathbb{Z}/2^{s_n(\ell)-1}\mathbb{Z}\right)^{\oplus 2^n - b_n(\ell)} \oplus \left(\mathbb{Z}/2^{s_n(\ell)}\mathbb{Z}\right)^{\oplus b_n(\ell)}$$

$(s_n(\ell) \ge 2)$

2-rank $=$ 4-rank $= 2^n$, 8-rank ≥ 0　($\ell = 5, 13$ / $n = 5$)

実例

- $p = 65537 = 2^{16} + 1$, $e_p = 15$, $k_p = 5$, $f_p = 11$

Table 4: $\mathrm{ord}_2(\bar{h}_n)$ for $p = 65537$ ($f_p = 11$).

l \ n	0	1	2	3	4	5	6	7	8	9	10	11∼14
∗1	5	6	8	12	20	36	68	132	260	516	1028	2048
41	2	4	10	12	20	36	68	132	260	516	1028	2048
73	3	5	8	12	20	36	68	132	260	516	1028	2048
89	5	5	8	12	20	36	68	132	260	516	1028	2048
113	3	7	8	12	20	36	68	132	260	516	1028	2048
137	2	4	10	12	20	36	68	132	260	516	1028	2048
313	2	4	13	12	20	36	68	132	260	516	1028	2048
337	8	5	8	12	20	36	68	132	260	516	1028	2048
401	2	4	10	12	20	36	68	132	260	516	1028	2048
409	2	4	9	12	20	36	68	132	260	516	1028	2048
433	2	4	10	12	20	36	68	132	260	516	1028	2048
449	2	4	9	12	20	36	68	132	260	516	1028	2048
457	2	4	10	12	20	36	68	132	260	516	1028	2048
521	2	4	10	12	20	36	68	132	260	516	1028	2048
569	2	4	10	12	20	36	68	132	260	516	1028	2048
577	4	5	8	12	20	36	68	132	260	516	1028	2048
601	4	5	8	12	20	36	68	132	260	516	1028	2048
641	2	4	9	12	20	36	68	132	260	516	1028	2048
857	2	4	9	12	20	36	68	132	260	516	1028	2048
881	3	6	8	12	20	36	68	132	260	516	1028	2048
929	2	4	11	12	20	36	68	132	260	516	1028	2048

7	2	4	10	12	20	36	68	132	260	516	1028	2048
23	2	4	10	12	20	36	68	132	260	516	1028	2048
31	3	6	8	12	20	36	68	132	260	516	1028	2048
47	3	6	8	12	20	36	68	132	260	516	1028	2048
127	4	6	8	12	20	36	68	132	260	516	1028	2048
151	2	4	11	12	20	36	68	132	260	516	1028	2048
167	2	4	10	12	20	36	68	132	260	516	1028	2048
223	7	6	8	12	20	36	68	132	260	516	1028	2048
271	3	7	8	12	20	36	68	132	260	516	1028	2048
311	2	4	10	12	20	36	68	132	260	516	1028	2048
359	2	4	11	12	20	36	68	132	260	516	1028	2048
383	3	6	8	12	20	36	68	132	260	516	1028	2048
463	3	10	8	12	20	36	68	132	260	516	1028	2048
607	3	6	8	12	20	36	68	132	260	516	1028	2048
727	2	4	10	12	20	36	68	132	260	516	1028	2048
743	2	4	10	12	20	36	68	132	260	516	1028	2048
823	2	4	10	12	20	36	68	132	260	516	1028	2048
863	3	6	8	12	20	36	68	132	260	516	1028	2048
887	2	4	11	12	20	36	68	132	260	516	1028	2048
983	2	4	11	12	20	36	68	132	260	516	1028	2048
991	3	6	8	12	20	36	68	132	260	516	1028	2048

実例

- $p = 65537 = 2^{16}+1$, $e_p = 15$, $k_p = 5$, $f_p = 11$

$$A_n' \cong \begin{cases} (\mathbb{Z}/2\mathbb{Z})^{\oplus 2^n} & \cdots\cdots\ 11 \le n \le 14 \\ (\mathbb{Z}/2\mathbb{Z})^{\oplus 2^n - 4} \oplus (\mathbb{Z}/4\mathbb{Z})^{\oplus 4} & \cdots\ 3 \le n \le 10 \\ \qquad (n_p^{\pm}, b_p^{\pm}) = (3, 4) & \\ (\mathbb{Z}/4\mathbb{Z})^{\oplus 4} \sim (\mathbb{Z}/8\mathbb{Z})^{\oplus 3} \oplus (\mathbb{Z}/16\mathbb{Z}) \sim & \cdots\ n = 2 \\ (\mathbb{Z}/4\mathbb{Z})^{\oplus 2} \sim (\mathbb{Z}/32\mathbb{Z})^{\oplus 2} \sim & \cdots\ n = 1 \\ (\mathbb{Z}/4\mathbb{Z}) \sim (\mathbb{Z}/256\mathbb{Z}) \sim & \cdots\cdots\ n = 0 \end{cases}$$

$\ell \le 1000$

• $p < 10^5$, $f_p = 5$ の $(n_p^{\pm}, b_p^{\pm})$ $(n_p^{\pm} \leq 4)$

Table 5: $(n_p^{\pm}, b_p^{\pm})$ with $f_p \geq 5$.

f_p	p	e_p	κ_p	(n_p^+, b_p^+)	(n_p^-, b_p^-)
11	65537	15	5	(3,4)	(3,4)
8	59393	10	3	(2,2)	(2,3)
6	6529	6	1	(3,5)	(3,4)
6	25601	9	4	(4,10)	(3,4)
6	50177	9	4	(2,2)	(2,2)
6	96001	7	2	(2,2)	(2,3)
5	15809	5	0	(2,3)	(2,2)
5	21569	5	1	(2,3)	(2,2)
5	35201	6	2	(3,5)	(2,2)
5	45697	6	2	(3,6)	(2,2)
5	50753	5	1	(3,6)	(4,10)
5	53633	6	2	(2,2)	(2,2)
5	83777	5	0	(2,3)	(3,5)
5	92737	5	0	(3,4)	(3,6)
5	93377	5	0	(2,2)	(2,2)

• $p < 10^9$, $|A_4| \geq 2^{32}$ ⟶ $n_p^+ = 5 \times 7 \times 3 \times 3 \times 9$ P.

Table 6: The number of primes with the $\mathrm{ord}_2(\bar{h}_4) = i$ ($p < 10^9$, $f_p \geq 5$).

i	17	18	19	20	21	22	23	24	25	26
	0	48078	25053	12771	6409	3281	1576	822	384	212
i	27	28	29	30	31	32	33	34	≥ 35	
	120	56	24	13	8	2	2	2	0	

Table 7: $\mathrm{ord}_2(\bar{h}_n)$ for the six primes with $\mathrm{ord}_2(\bar{h}_4) \geq 32$.

p	e_p	κ_p	(n_p^+, b_p^+)			
l \ n	0	1	2	3	4	5
156731329	5	0	–			
∗1	7	8	12	20	34	
41	2	4	8	16	32	
89	4	5	9	17	33	
97	2	4	8	16	32	
574717313	6	1	(5,17)			
∗1	4	6	10	18	33	49
73	8	7	12	20	33	49
193	2	4	8	16	32	49
233	4	5	9	17	37	49
579604033	5	0	–			
∗1	4	6	10	18	34	
41	2	4	8	16	32	
73	4	8	14	22	35	
89	3	9	10	18	34	

640935553	6	0	(5,17)			
∗1	5	10	12	20	33	49
17	2	4	8	16	32	49
41	2	4	8	16	32	49
89	3	6	18	20	33	49
676199297	6	1	(5,16)			
∗1	4	6	10	18	32	48
73	4	6	10	18	32	48
113	4	5	9	17	32	48
137	2	4	8	16	33	48
816873089	6	2	–			
∗1	4	6	10	18	32	32
17	2	4	8	16	35	32
89	8	5	9	17	32	32
97	2	4	8	16	33	32

§4. 証明の概略＋α

- A_n' の ガロア加群と17の構造.

  (1-cyclic
  (Annihilator) $\Rightarrow J+1=(T+1)^{2^n}+1$
  Eisenstein多項式 $\longrightarrow$ $\mathcal{O}(\ell)$の構造)

- 2次不分岐拡大のKummer生成元
  (2の分解)

- 4次不分岐拡大にのびる2次拡大
  ($A_n'[2]$を生成するイデアル
  特異類(ambig類)とKummer生成元)

岩澤加群, 種の理論, Kummer理論, 類体論

☆実2ベキ次巡回拡大の狭義・広義イデアル類群の2部分についても，結果を得ている．

最後に宣伝：
　ゼータ値の分子と分母（クンマーの合同式，素数分体の類数）

https://math0.pm.tokushima-u.ac.jp/~hiroki/major/galois2.html

ガロアーゼータ1

緑：素数
赤：ζ(1-2k)に現れる素数

分子

分母

ご清聴ありがとうございました！