INKERI 行列と STICKELBERGER IDEAL の生成系について

東京理科大学大学院理工学研究科 谷口 哲也 (TETSUYA TANIGUCHI)

1. 概要

p^n-円分体 K の類数を h_K とし K の Galois 群 G で $\mathbb{Z}$ 上生成される群環 $\mathbb{Z}[G]$ を R, そのマイナスパートを R^-, Stickelberger ideal を I, I と R^- の共通部分を I^- としたとき, 岩澤による相対類数の公式は $h_K^- = [R^- : I^-]$ である. Skula[13] はこの公式の別の観点からの証明を次のように行った. まず, Kummer による円分体の相対類数の公式を用いて $\pmod{p^n}$ の原始根を成分にもつ行列の行列式で相対類数を表わした. 次に, Stickelberger ideal I の性質を原始根を用いて表現した後, I のマイナスパート I^- の性質を明らかにした. さらに, I^- の生成系を原始根を用いて構成して R^- の基底から I^- の生成系への変換行列が前述の行列に一致することを示した. このようにして Stickelberger ideal の生成系と円分体の相対類数との間の関連が明らかになった.

そこで, ほかの行列式による相対類数の表示から, 対応する Stickelberger ideal の生成系を構成することに注目し, これに取り組んだ. とくに Inkeri 行列は係数が原始根を用いた表示になっており, Skula[13] と同様の方法が適用できると期待して取り組んでみたところ, Inkeri 行列に関連した生成系を構成することができた.

本稿で扱う話題は, 円分体 $\mathbb{Q}(\zeta_p)$ の相対類数 h_p^- についてであり, とくに以下の二つの事柄について扱う:

- 3 節: Inkeri 行列から Stickelberger Ideal I^- の生成系を構成する ([1]),
- 4 節: h_p^- を Resultant で表し, 整除性を議論する.

それぞれの内訳は, 次のとおりである.

3 節で I^- の生成系について議論する. Inkeri 行列から決まる I^- の生成系を構成すること, $h_p^- = [R^- : I^-]$ の別証明, Inkeri 行列から決まる多項式による h_p^- の公式を紹介する.

4 節で整除性について議論する. "q, $p = 2q^n + 1$ がともに素数ならば, q が h_p^- を割り切ることと q が $h_{\mathbb{Q}(\sqrt{-p})}$ を割り切ることは同値", また "$q \equiv 3 \pmod 4$, $p = 4q + 1$ がともに素数ならば q は h_p^- を割り切らない" という事実を紹介する.

2. 記号説明

本稿で使用する記号をここにまとめる.

- p: 奇素数, $\mu := (p-1)/2$,
- r: $\mod p$ の奇の原始根, r_i: r^i の $\mod p$ での最小正剰余,
- $\zeta_m := \exp(2\pi i/m)$, $K_m := \mathbb{Q}(\zeta_m)$, h_m^-: K_m の相対類数,
- $G := \{1, s, \ldots, s^{p-2}\}$, $\gamma := (1/p)\sum_i r_{-i} s^i$,
- $R := \mathbb{Z}[G]$,
- $R^- := \{\alpha \in R \mid (1 + s^\mu)\alpha = 0\}$, ($R$ のマイナスパート)
- $I := R \cap \gamma R$, (Stickelberger ideal)
- $I^- := I \cap R^-$, (Stickelberger ideal のマイナスパート)
- $f(x) := r_0 + r_1 x + \cdots + r_{p-2} x^{p-2} \in \mathbb{Z}[x]$,
- $f_1(x) := r_{p-2} + r_{p-3} x + \cdots + r_0 x^{p-2} \in \mathbb{Z}[x]$,
- $(2p)^{\frac{p-3}{2}} h_p^- = \left| \prod_{k=0}^{\mu-1} f(\zeta_{p-1}^{2k+1}) \right|$ (Kummer による公式)

3. Inkeri 行列と I^- の生成系の関係

3.1. **結果.** Inkeri 行列とは,

$$D := \begin{pmatrix} q_\mu & q_{\mu-1} & \cdots & q_0 \\ \vdots & \vdots & & \vdots \\ q_{2\mu-2} & q_{2\mu-3} & \cdots & q_{\mu-2} \\ r_\mu & r_{\mu-1} & \cdots & r_0 \\ 1 & 1 & \cdots & 1 \end{pmatrix}, \left(q_i := \frac{rr_i - r_{i+1}}{p} \right),$$

であり, $h_p^- = \det D$ をみたす (Inkeri[5]) ことが知られている. q_i が原始根を用いて表されていることに気をつけながら計算したところ, 次の結果を得た:

Theorem 3.1. *([1])* $\varepsilon_k = s^k(1-s^\mu)$, $q_i = (rr_i - r_{i+1})/p$, $f = (r-1)/2$, $\rho_k = \sum_i (q_{-i+k} - f)s^i$, $\tau = \sum_i (2r_{-i} - p)s^i$, $g(x) = q_0 + q_1 x + \cdots + q_{p-2}x^{p-2} \in \mathbb{Z}[x]$, $\mathcal{E}^- = \{\varepsilon_k \mid k = 0, \ldots, \mu-1\}$*(* これは R^- の基底になる*)* に対して,

- $\mathcal{B}^- = \{\rho_k \mid k = 0, \ldots, \mu-2\} \cup \{\tau\}$ は I^- の生成系である.
- P を *"*$\mathcal{E}^-$ から $\mathcal{B}^-$ への変換行列*"* とすると, $h_p^- = \det P$, $h_p^- = [R^- : I^-]$ が成立する. ゆえに $\mathcal{B}^-$ は I^- の基底である.
- $\left(2^{\mu-1}(r^\mu+1)/p\right) h_p^- = \left| \prod_{k=0}^{\mu-1} g(\zeta_{p-1}^{2k+1}) \right|$ が成立する.

がなりたつ. すなわち, *"Inkeri* 行列の係数に関係した係数をもつ I^- の基底 $\mathcal{B}^-$ を構成でき, その基底に関する変換行列の行列式は *Inkeri* 行列の行列式に一致する.*"*

最後の $\left(2^{\mu-1}(r^\mu+1)/p\right) h_p^- = \left| \prod_{k=0}^{\mu-1} g(\zeta_{p-1}^{2k+1}) \right|$ は, 左辺の h_p^- の前にかかっている係数が p で割り切れないようにできるため, 右辺を調べることによって正則性のチェックが行いやすくなる可能性はある.

4. h_p^- と Resultant の関係

4.1. **復習.** Lehmer[8] は, 次のようにして Kummer の h_p^- の公式から h_p^- の分解を得た:

$$\begin{aligned} (2p)^{\mu-1} h_p^- &= \left| \prod_{k=0}^{\mu-1} f_1(\zeta_{p-1}^{2k+1}) \right| \\ &= \left| \mathrm{Res}(f_1(x), x^{\frac{p-1}{2}} + 1) \right| \\ &= \left| \prod_{\beta_i} (\beta_i^{\frac{p-1}{2}} + 1) \right| \\ &= \left| \prod_{d \mid \frac{p-1}{2^\lambda}} \left(\prod_{\beta_i} \Phi_{2^\lambda d}(\beta_i) \right) \right|. \end{aligned}$$

ただし, λ は $2^\lambda || (p-1)$ をみたすものであり, $\Phi_d(x)$ は円分多項式である. また, β_i は $f_1(x) = 0$ の根であり, $\prod_{\beta_i} \Phi_{2^\lambda d}(\beta_i) \in \mathbb{Z}$ であるから, 右辺は左辺を整数の範囲で分解している. Lehmer[8] ではさらに両辺から $(2p)^{\mu-1}$ を取り除いて純粋な h_p^- の分解を与えている.

以下, 上記の変形の途中に Resultant が表れていることに注目し, これを用いて整除性を議論する.

4.2. **方針.** h_p^- の整除性を $\mod q$ の多項式の最大公約数の有無にいいかえる. $q \neq 2$, p なる素数に対して,

$$\begin{aligned} & h_p^- \equiv 0 \pmod{q} \\ & \Leftrightarrow \mathrm{Res}(f_1(x), x^{\frac{p-2}{2}} + 1) \equiv 0 \pmod{q} \\ & \Leftrightarrow \deg(\gcd(f_1(x), x^{\frac{p-2}{2}} + 1)) > 0 \ (\mathbb{F}_q[x] \text{ 内で}) \end{aligned}$$

がなりたつ. 以下, この帰着を用いて計算する.

4.3. **結果.** 次の結果を得た:

Theorem 4.1. $p = 2q^n + 1$, q がともに素数ならば, $q \mid h_p^- \Leftrightarrow q \mid h_{\mathbb{Q}(\sqrt{-p})}$ がなりたつ.

※ Metsänkylä[10] の結果は上の $n = 1$ の場合であり, これはその拡張にあたる. また, $p \equiv 3 \mod 4$ のとき $h_{\mathbb{Q}(\sqrt{-p})} | h_p^-$ がなりたつことは, Lehmer[8] の相対類数の次数別分解からわかる.

Theorem 4.2. $p = 4q + 1$, $q \equiv 3 \pmod 4$ がともに素数ならば, $q \nmid h_p^-$ がなりたつ.

※この整除性自体は既に T.Agoh が別方針で示している.

4.4. **数値実験.** Theorem 4.1 の条件 ($p = 2q^n + 1$, q がともに素数) をみたす (q, n) の一覧表を作成した (Table 1). まずは Web を参考にしたが, この形の素数は網羅されていない. そこで見つけられなかったものはこちらで計算した. 計算プログラムは newpgen と prp, proth である.

- Web で見つけたもの
  - $q = 3$ の全範囲 (On-Line Encyclopedia of Integer Sequences から).
  - $(q, n) = (5, 121995), (23, 47589), (23, 93337), (71, 36977), (107, 26303), (107, 48043), (251, 51905)$(The Prime Pages から).
- こちらで計算したもの
  - $3 < q \leq 101$ の $1 \leq n \leq 10^4$ は計算済みで,
  - $101 < q \leq 257$ の $1 \leq n \leq 10^5$ の範囲は計算中である.
- 表中の $\cdots$ 部は, その範囲の素数の有無は不明 (私が把握していない) という意味である.

TABLE 1. $2q^n + 1$ が素数になる q, n の組

q	n	q	n	q	n	q	n	q	n	q	n	q	n	q	n
3	1	3	57	3	1252	3	64822	5	105	11	9	23	47589	29	26605
3	2	3	60	3	1454	3	82780	5	159	11	43	23	$\cdots$	41	1
3	4	3	65	3	4217	3	105106	5	297	11	79	23	93337	41	819
3	5	3	132	3	5480	3	152529	5	1443	11	175	29	1	41	1449
3	6	3	180	3	6225	3	165896	5	2977	17	47	29	7	41	1677
3	9	3	320	3	7842	3	191814	5	3699	17	5991	29	23	47	175
3	16	3	696	3	12096	5	1	5	$\cdots$	23	1	29	177	53	1
3	17	3	782	3	13782	5	3	5	121995	23	21	29	327	53	5
3	30	3	822	3	17720	5	13	11	1	23	261	29	875	59	3
3	54	3	897	3	43956	5	45	11	3	23	$\cdots$	29	6645	71	3

q	n	q	n	q	n	q	n	q	n	q	n	q	n
71	29	83	65	113	77	149	2075	173	21	191	66971	239	25
71	83	89	1	131	1	149	7941	179	1	227	347	239	9157
71	153	89	93	131	3139	149	8959	179	7	227	2159	251	1
71	327	89	931	131	8485	149	19395	179	4239	227	3395	251	5
71	753	107	551	137	327	149	43911	191	1	233	1	251	23
71	879	107	1775	137	3443	149	52135	191	61	233	9	251	251
71	3333	107	26303	137	31947	149	64107	191	2211	233	277	251	$\cdots$
71	$\cdots$	107	$\cdots$	149	5	167	6547	191	4005	233	1389	251	51905
71	36977	107	48043	149	15	167	12447	191	14993	233	4225	257	12183
83	1	113	1	149	75	173	1	191	61303	239	1	257	16863

q	n
239	25
239	9157
251	1
251	5
251	23
251	251
251	$\cdots$
251	51905
257	12183
257	16863

5. 参考文献

1 T. Agoh and T. Taniguchi, A study of Inkeri's class number formula, *Expo. Math.* **24** (2006), 53 - 79.

2 L. Carlitz and F.R. Olson, Maillet's determinant, *Proc. Amer. Math. Soc.* **6** (1955), 265 - 269.

3 P. Fuchs, Maillet's determinant and a certain basis of the Stickelberger ideal, *Tatra Mount. Math. Publ.* **11** (1997), 121 - 128.

4 M. Hirabayashi, Inkeri's determinant for an imaginary abelian number field, *Arch. Math.* **79** (2002), 175 - 181.

5 K. Inkeri, Über die Klassenzahl des Kreiskörpers der l^{ten} Einheitswurzeln, *Ann. Acad. Sci. Fenn.* Ser. A.I. **199** (1955), 1 - 12.

6 K. Iwasawa, A class number formula for cyclotomic fields, *Ann. Math.* **76** (1962), 171 - 179.

7 R. Kučera, Formulae for the relative class number of an imaginary abelian field in the form of a determinant, *Nagoya Math. J.* **163** (2001), 167 - 191.

8 D.H. Lehmer, Prime factors of cyclotomic class numbers, *Math. Comp.* **31** (1977), 599 - 607.

9 T. Lepistö, On the first factor of the class number of the cyclotomic field and Dirichlet's L-function, *Ann. Acad. Sci. Fenn.* Ser. A.I. **387** (1966), 1 - 52.

10 T. Metsänkylä, On prime factors of the relative class numbers of cyclotomic fields, *Ann. Univ. Turku.* Ser. A.I. **149** (1971), 8pp.

11 P. Ribenboim, "Classical theory of algebraic numbers", Springer-Verlag, New York, 2001.

12 W. Sinnott, On the Stickelberger ideal and the circular units of a cyclotomic field, *Ann. Math.* **108** (1978), 107 - 134.

13 L. Skula, Another proof of Iwasawa's class number formula, *Acta Arith.* **39** (1981), 1 - 6.

14 L. Skula, Some bases of the Stickelberger ideal, *Math. Slovaca* **43** (1993), 541 - 571.

15 L.C. Washington, "Introduction to cyclotomic fields", 2nd ed., Springer-Verlag, New York, 1996.

[参考 URI]

- On-Line Encyclopedia of Integer Sequences
  - `http://www.reserch.att.com/~njas/sequences/A003306`
- The Prime Pages
  - `http://primes.utm.edu/`

谷口 哲也
東京理科大学大学院理工学研究科

〒 278-8510 千葉県野田市山崎 2641
email: `taniguti_tetuya@ma.noda.tus.ac.jp`

Tetsuya Taniguchi
Graduate School of Science and Engineering,
Tokyo University of Science
2641, Yamazaki, Noda, Chiba, 278-8510, Japan
`http://www.ed.noda.tus.ac.jp/~j6101703/`