JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Takashi FUKUDA

Relative class numbers of subfields of the p-th cyclotomic field

Tome 34, n° 1 (2022), p. 135-140.

https://doi.org/10.5802/jtnb.1195

Journal de Théorie des Nombres de Bordeaux **34** (2022), 135–140

Relative class numbers of subfields of the p-th cyclotomic field

par Takashi FUKUDA

Résumé. Dans cet article, nous généralisons le résultat récent d'Ichimura sur les nombres de classes relatifs des sous-corps du p-ième corps cyclotomique.

Abstract. We generalize the recent result of Ichimura concerning relative class numbers of subfields of the p-th cyclotomic field.

1. Introduction

For a natural number n, we denote by ζ_n a primitive n-th root of unity contained in the complex number field $\mathbb{C}$. Let p be a prime number. It is observed that the relative class number of the p-th cyclotomic field $\mathbb{Q}(\zeta_p)$ grows rapidly as p grows. How about the relative class numbers of subfields? Let ℓ be an odd prime divisor of $p-1$ with the highest power ℓ^f dividing $p-1$ and q a divisor of $p-1$ prime to ℓ. We fix q and denote by K_t $(0 \leq t \leq f)$ the unique subfield of $\mathbb{Q}(\zeta_p)$ with degree $q\ell^t$. We are interested in the relative class number h_t^- of K_t.

Several authors observed that the ℓ-part of h_t^- $(0 \leq t \leq f)$ behaves like in Iwasawa's class number formula. Recently, Ichimura [3] gave a confirmation of this phenomenon. Namely, he proved the following which is an analogue to Corollary 3 in [1].

Let ℓ^{e_t} be ℓ-part of h_t^- and let φ denote the Euler function as usual.

Theorem 1.1 (Ichimura)**.** *Let p be a prime number with $p \equiv 3 \pmod 4$ and $q = 2$. Let ℓ^f be the highest power of an odd prime number ℓ dividing $p-1$. If $e_s - e_{s-1} < \varphi(\ell^s)$ for some s with $1 \leq s \leq f$, then $e_s - e_{s-1} = e_t - e_{t-1}$ for all t with $s \leq t \leq f$.*

Ichimura also gave examples. For example, let $(p, q, \ell) = (7860079, 2, 3)$. Then $e_0 = 3$, $e_1 = 7$, $e_2 = 17$, $e_3 = 25$ and $e_t = 8t + 1$ $(2 \leq t \leq 8)$.

In this paper, we generalize Ichimura's result and provide an another proof for Ichimura's theorem.

Manuscrit reçu le 20 août 2020, révisé le 30 octobre 2020, accepté le 13 octobre 2020.
Mathematics Subject Classification. 11R18, 11R23.
Mots-clefs. Cyclotomic field, class number.

Theorem 1.2. *Let p be a prime number, ℓ an odd prime divisor of $p-1$ with the highest power ℓ^f dividing $p-1$ and q a divisor of $p-1$ prime to ℓ.*

(1) *If $e_0 = 0$, then $e_t = 0$ for all t with $0 \le t \le f$.*
(2) *If $e_0 > 0$, then $e_{t-1} < e_t$ for all t with $1 \le t \le f$.*
(3) *If $e_s - e_{s-1} < \varphi(\ell^s)$ for some s with $1 \le s \le f$, then $e_s - e_{s-1} = e_t - e_{t-1}$ for all t with $s \le t \le f$.*

Let v_2 denote the additive 2-adic valuation normalized by $v_2(2) = 1$. If $v_2(q) < v_2(p-1)$, then K_t $(0 \le t \le f)$ is real and $h_t^- = 1$ $(0 \le t \le f)$. So the theorem has a meaning only when $v_2(q) = v_2(p-1)$. For the proof of the theorem, we recall a class number formula of an abelian number field. Let F be an imaginary abelian number field of finite degree. Then the relative class number $h^-(F)$ of F is given by

$$h^-(F) = Q(F)w(F) \prod_{K \subset F} N_{\mathbb{Q}(\zeta_d)/\mathbb{Q}}\Big(-\frac{1}{2}B_{1,\chi}\Big)\,,$$

where $Q(F)$ is the unit index of F, $w(F)$ is the number of roots of unity contained in F and K runs through all imaginary cyclic subfields of F. For each K, $d = [K : \mathbb{Q}]$ and χ is an arbitrary injective character of $G(K/\mathbb{Q})$ to $\mathbb{C}^\times$ (cf. [4, p. 294]). We also denote by χ the primitive Dirichlet character induced by χ. Then the Bernoulli number $B_{1,\chi}$ is given by

$$B_{1,\chi} = \frac{1}{m}\sum_{a=1}^{m} a\chi(a)\,,$$

where m is the conductor of K.

Let $\mathfrak{p}_t = (1 - \zeta_{\ell^t})$ be the prime ideal of $\mathbb{Q}(\zeta_{\ell^t})$ lying above ℓ. For an integer x in $\mathbb{Q}(\zeta_{\ell^t})$, let $\operatorname{ord}_{\mathfrak{p}_t} x$ denote the maximal integer n such that $\mathfrak{p}_t^n$ divides (x). The following is a key lemma for our work.

Lemma 1.1. *Let $g(X) \in \mathbb{Z}[X]$.*

(1) *If $g(1) \not\equiv 0 \pmod{\ell}$, then $\operatorname{ord}_{\mathfrak{p}_1} g(\zeta_\ell) = 0$.*
(2) *If $g(1) \equiv 0 \pmod{\ell}$, then $\operatorname{ord}_{\mathfrak{p}_1} g(\zeta_\ell) > 0$.*
(3) *If $\operatorname{ord}_{\mathfrak{p}_t} g(\zeta_{\ell^t}) > 0$ for some $t \ge 1$, then*
$$\operatorname{ord}_{\mathfrak{p}_{t+1}} g(\zeta_{\ell^{t+1}}) > 0\,.$$
(4) *If $\operatorname{ord}_{\mathfrak{p}_t} g(\zeta_{\ell^t}) < \varphi(\ell^t)$ for some $t \ge 1$, then*
$$\operatorname{ord}_{\mathfrak{p}_t} g(\zeta_{\ell^t}) = \operatorname{ord}_{\mathfrak{p}_{t+1}} g(\zeta_{\ell^{t+1}})\,.$$

Proof. We recall the well known fact $\operatorname{ord}_{\mathfrak{p}_t} \ell = \varphi(\ell^t)$ and write

$$g(X) = \sum_i a_i (X-1)^i$$

with $a_i \in \mathbb{Z}$. Then (1) is an immediate consequence of $a_0 = g(1) \not\equiv 0 \pmod{\ell}$. Also (2) and (3) are immediate consequences of $a_0 \equiv 0 \pmod{\ell}$.

In order to prove (4), we assume $r = \operatorname{ord}_{\mathfrak{p}_t} g(\zeta_{\ell^t}) < \varphi(\ell^t)$. If $a_i \equiv 0 \pmod{\ell}$ for all i with $0 \le i \le r$, then we have $\mathfrak{p}_t^{r+1} \mid g(\zeta_{\ell^t})$ which contradicts the assumption. Hence there exists some $i \le r$ such that $a_i \not\equiv 0 \pmod{\ell}$. We take i to be minimal. If $0 \le i < r$, then we have $\operatorname{ord}_{\mathfrak{p}_t} g(\zeta_{\ell^t}) = i$ which also contradicts the assumption. Hence we have $i = r$ which immediately implies the conclusion. □

2. Proof of Theorem 1.2

Let q_0 be the highest power of 2 dividing $p-1$. First we prove the theorem when $q = q_0$. Let $|\cdot|_\ell$ denote the multiplicative ℓ-adic valuation normalized by $|\ell|_\ell = 1/\ell$. We show that $e_s - e_{s-1} < \varphi(\ell^s)$ with $1 \le s < f$ implies $e_s - e_{s-1} = e_{s+1} - e_s$. Let χ be an arbitrary injective character of $G(K_{s+1}/\mathbb{Q})$. Then, the conductor of χ is p and

$$B_{1,\chi} = \frac{1}{p} \sum_{1 \le a \le p} a\chi(a)\,.$$

Since K_i $(0 \le i \le s+1)$ are all the imaginary cyclic subfields of K_{s+1}, we have

$$\ell^{e_{s+1}-e_s} = \left| N_{\mathbb{Q}(\zeta_{\ell^{s+1}})/\mathbb{Q}} \circ N_{\mathbb{Q}(\zeta_{q\ell^{s+1}})/\mathbb{Q}(\zeta_{\ell^{s+1}})}(B_{1,\chi}) \right|_\ell^{-1}$$

and

$$e_{s+1} - e_s = \operatorname{ord}_{\mathfrak{p}_{s+1}} N_{\mathbb{Q}(\zeta_{q\ell^{s+1}})/\mathbb{Q}(\zeta_{\ell^{s+1}})} \left(\sum_{1 \le a \le p} a\chi(a) \right).$$

If we fix ζ_q and $\zeta_{\ell^{s+1}}$, then there exist two functions $\rho_1,\ \rho_2 : \mathbb{N} \to \mathbb{N} \cup \{0\}$ satisfying

$$\chi(a) = \zeta_q^{\rho_1(a)} \zeta_{\ell^{s+1}}^{\rho_2(a)}\,.$$

We define $g(X) \in \mathbb{Q}(\zeta_q)[X]$ by

$$g(X) = \prod_{\sigma \in G(\mathbb{Q}(\zeta_q)/\mathbb{Q})} \left(\sum_{1 \le a \le p} a \zeta_q^{\rho_1(a)\sigma} X^{\rho_2(a)} \right).$$

Then $g(X) \in \mathbb{Z}[X]$ because $g(X)$ is invariant under the action of $G(\mathbb{Q}(\zeta_q)/\mathbb{Q})$. Now we have

$$N_{\mathbb{Q}(\zeta_{q\ell^{s+1}})/\mathbb{Q}(\zeta_{\ell^{s+1}})} \left(\sum_{1 \le a \le p} a\chi(a) \right) = g(\zeta_{\ell^{s+1}})$$

and hence

$$e_{s+1} - e_s = \operatorname{ord}_{\mathfrak{p}_{s+1}} g(\zeta_{\ell^{s+1}})\,.$$

Let n be an integer satisfying $n \equiv 1 \pmod{q}$ and $n \equiv \ell \pmod{\ell^{s+1}}$. Then $\psi = \chi^n$ is an injective character of $G(K_s/\mathbb{Q})$ and

$$\begin{aligned} e_s - e_{s-1} &= \operatorname{ord}_{\mathfrak{p}_s} N_{\mathbb{Q}(\zeta_{q\ell^s})/\mathbb{Q}(\zeta_{\ell^s})} \left(\sum_{1 \le a \le p} a\psi(a) \right) \\ &= \operatorname{ord}_{\mathfrak{p}_s} g(\zeta_{\ell^s}) \,. \end{aligned}$$

Then Lemma 1.1 (4) yields $e_s - e_{s-1} = e_{s+1} - e_s$. Hence we can prove (3) inductively. Next we consider (1) and (2). Let χ be an arbitrary injective character of $G(K_1/\mathbb{Q})$ and $\psi = \chi^n$ with n satisfying $n \equiv 1 \pmod{q}$ and $n \equiv 0 \pmod{\ell}$. Then,

$$\begin{aligned} e_1 - e_0 &= \operatorname{ord}_{\mathfrak{p}_1} N_{\mathbb{Q}(\zeta_{q\ell})/\mathbb{Q}(\zeta_\ell)} \left(\sum_{1 \le a \le p} a\chi(a) \right) \\ &= \operatorname{ord}_{\mathfrak{p}_1} g(\zeta_\ell) \end{aligned}$$

with $g(X) \in \mathbb{Z}[X]$ defined similarly as above and

$$\begin{aligned} |g(1)|_\ell^{-1} &= \left| N_{\mathbb{Q}(\zeta_{q\ell})/\mathbb{Q}(\zeta_\ell)} \left(\sum_{1 \le a \le p} a\psi(a) \right) \right|_\ell^{-1} \\ &= \left| N_{\mathbb{Q}(\zeta_q)/\mathbb{Q}} \left(\sum_{1 \le a \le p} a\psi(a) \right) \right|_\ell^{-1} \\ &= \left| N_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(B_{1,\psi}) \right|_\ell^{-1} = \ell^{e_0} \end{aligned}$$

because K_0 is the only imaginary cyclic subfield of K_0. Assume $e_0 = 0$. Then we have $e_1 - e_0 = 0$ by Lemma 1.1 (1) and $e_t - e_{t-1} = 0$ $(1 \le t \le f)$ by Theorem 1.2 (3). We note that this is also an immediate consequence of [6, Theorem 10.4 (a)]. Assume $e_0 > 0$. Then we have $e_1 - e_0 > 0$ by Lemma 1.1 (2) and $e_t - e_{t-1} > 0$ $(1 \le t \le f)$ by Lemma 1.1 (3).

Now we return to a general q with $q_0 \mid q$. In this case, q is a product of q_0 and q_1, where q_1 is an odd divisor of $p-1$ prime to ℓ. If $\sigma(n)$ denotes the number of divisors of an integer n, then K_t has $\sigma(q_1)(t+1)$ number of imaginary cyclic subfields. These subfields are determined by the degree. Namely, if we denote by $\mathbb{Q}(p,m)$, for a divisor m of $p-1$, a unique subfield of $\mathbb{Q}(\zeta_p)$ with degree m, then all the imaginary cyclic subfields of K_t are $\mathbb{Q}(p, q_0 d\ell^i)$ $(d \mid q_1, 0 \le i \le t)$. For each d and i, there exists an injective character $\chi_{d,i}$ of $G(\mathbb{Q}(p, q_0 d\ell^i)/\mathbb{Q})$. Then we have

$$e_{s+1} - e_s = \sum_{d \mid q_1} \operatorname{ord}_{\mathfrak{p}_{s+1}} N_{\mathbb{Q}(\zeta_{q_0 d\ell^{s+1}})/\mathbb{Q}(\zeta_{\ell^{s+1}})} \left(\sum_{1 \le a \le p} a\chi_{d,s+1}(a) \right)$$

and

$$e_s - e_{s-1} = \sum_{d|q_1} \mathrm{ord}_{\mathfrak{p}_s} N_{\mathbb{Q}(\zeta_{q_0 d\ell^s})/\mathbb{Q}(\zeta_{\ell^s})} \left(\sum_{1\le a\le p} a\chi_{d,s}(a) \right)$$

because we may assume $\chi_{d,s} = \chi_{d,s+1}^n$ with $n \in \mathbb{N}$ satisfying $n \equiv 1 \pmod{q_0 d}$ and $n \equiv \ell \pmod{\ell^{s+1}}$. Now, $e_s - e_{s-1} < \varphi(\ell^s)$ implies

$$\mathrm{ord}_{\mathfrak{p}_s} N_{\mathbb{Q}(\zeta_{q_0 d\ell^s})/\mathbb{Q}(\zeta_{\ell^s})} \left(\sum_{1\le a\le p} a\chi_{d,s}(a) \right) < \varphi(\ell^s)$$

for each d. Hence we can follow the argument for $q = q_0$. □

3. Examples

We show some examples having large f. These were calculated by PARI/GP [5]. All the examples behave like Theorem 1.2.

(p, q, ℓ, f)	e_0	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8	e_9
$(1194103, 26, 3, 8)$	3	6	9	12	15	18	21	24	27	
$(1268623, 2, 3, 4)$	1	3	9	16	23					
$(1924561, 80, 3, 7)$	4	8	12	16	20	24	28	32		
$(3123037, 4, 3, 8)$	2	6	14	22	30	38	46	54	62	
$(5826169, 8, 3, 9)$	2	4	6	8	10	12	14	16	18	20
$(7295833, 8, 3, 8)$	4	8	12	16	20	24	28	32	36	
$(7715737, 8, 3, 9)$	4	10	16	22	28	34	40	46	52	58
$(9723403, 2, 3, 9)$	1	3	5	7	9	11	13	15	17	19
$(9723403, 26, 3, 9)$	4	9	14	19	24	29	34	39	44	49
$(1637501, 4, 5, 5)$	2	5	8	11	14	17				
$(3797501, 4, 5, 4)$	5	10	15	20	25					
$(8365001, 8, 5, 4)$	6	10	14	18	22					
$(1190897, 16, 7, 4)$	8	12	16	20	24					
$(1336337, 16, 17, 4)$	1	3	5	7	9					

Finally, in connection with the Corollary in [2, p. 237], we would like to make some comments about further investigations on h_t^-. The condition $e_s - e_{s-1} < \varphi(\ell^s)$ in Theorem 1.2 (3) can not be replaced by $e_s - e_{s-1} \le \varphi(\ell^s)$ because the case $p = 1268623$ gives a counterexample. On the other hand, there are many examples satisfying $e_s - e_{s-1} = \varphi(\ell^s)$ and $e_s - e_{s-1} = e_{s+1} - e_s$, for example $(p, \ell, s) = (5826169, 3, 1)$, $(7715737, 3, 2)$, $(9723403, 3, 1)$, $(8365001, 5, 1)$. It may be interesting to consider under which conditions, $e_s - e_{s-1} = \varphi(\ell^s)$ implies $e_s - e_{s-1} = e_{s+1} - e_s$.

Acknowledgments. The author would like to express his gratitude for the anonymous referee who read the manuscript very carefully and gave advice how to clarify some ambiguous expressions.

References

[1] R. GOLD, "Examples of Iwasawa invariants", *Acta Arith.* **26** (1974), p. 21-32.
[2] ———, "Examples of Iwasawa invariants. II", *Acta Arith.* **26** (1975), p. 233-240.
[3] H. ICHIMURA, "Relative class numbers inside the pth cyclotomic field", *Osaka J. Math.* **57** (2020), no. 4, p. 949-959.
[4] S. LOUBOUTIN, "Computation of relative class numbers of imaginary abelian number fields", *Exp. Math.* **7** (1998), no. 4, p. 293-303.
[5] THE PARI GROUP, "PARI/GP version `2.12.1`", 2019, available from `http://pari.math.u-bordeaux.fr/`.
[6] L. C. WASHINGTON, *Introduction to Cyclotomic Fields*, 2nd ed., Graduate Texts in Mathematics, vol. 83, Springer, 1997.

Takashi FUKUDA
Department of Mathematics
College of Industrial Technology
Nihon University
2-11-1 Shin-ei, Narashino, Chiba, Japan
E-mail: `fukuda.takashi@nihon-u.ac.jp`