

円分体のイデアル類群の構造について

東大 館山 光一

記号

$$\mathbb{C}_m = \mathbb{Q} \left(\exp \frac{2\pi i}{m} \right)$$

$$\mathbb{C}_m^+ = \mathbb{Q} \left(\cos \frac{2\pi}{m} \right)$$

$C(m)$: \mathbb{C}_m の ideal class group.

$C^+(m)$: \mathbb{C}_m^+ の ideal class group.

j : complex conjugation

$$C^-(m) = \{ c \in C(m) \mid c^{jj} = 1 \}$$

h_m : \mathbb{C}_m の class number

h_m^+ : \mathbb{C}_m^+ の class number

$$h_m^- = h_m / h_m^+$$

E_k : k の unit group

$C_k, C_k^\pm, h_k, h_k^\pm$ も同様である。

p は素数とすると、 $C^-(p)$ については、次の結果が知られている。([1], [2])

$p < 100$, $p \neq 29, 41$ ならば cyclic

$$C^-(29) \cong (\mathbb{Z}/29\mathbb{Z})^3, \quad C^-(41) \cong (\mathbb{Z}/41\mathbb{Z})^2$$

以下は $n \in (2, 2, 2), (11, 11)$ 型と書くことはできる。

また、最近 F. Geetha III [13] は $C(68)$ が cyclic であることを判別類の計算によって示した。

ここでは、F. Geetha II, Masley [4] の方法を用いて、いくつかの円分体の ideal class group の構造を決定する。

以下体はすべて \mathbb{Q} 上有限次とする。

Lemma 1. K/k : cyclic extension, $G = \text{Gal}(K/k)$.

σ : G の generator, $a(K/k) = \#\{c \in C_K \mid c^\sigma = c\}$ とする。

$$a(K/k) = h_k \frac{e(K/k)}{[K:k](E_k: E_k \cap N_{K/k} K^*)}$$

ここで $e(K/k)$ は k の各素点の分岐指数の積を表す。

Proof) H. Y. Koi [5]

次の結果が、Geetha の用いた方法である。

Lemma 2. $[K:k] = 2$, C_K の 2-Sylow subgroup の rank

を r , $h_k \not\equiv 0 \pmod{2}$ とすると $a(K/k) = 2^r \cdot n$, $(2, n) = 1$.

Proof) F. Geetha III [13]

以下にここで用いられる class number に関する [4], [6], [7], [8] を参照。

Ex 1) $C_{120} = K$ $h_{120} = 2^2$, $h_{60} = 1$.

| 簡単計算より、分岐する素数は2個。

$C_{60} = K$ 故に $a(K/k) = 1 \times \frac{2 \times 2}{2 \times (E_k: E_k \cap N_{K/k})} \leq 2$

C_K の rank は 1以上であり $a(K/k) = 2$

よって cyclic。

$C(68)$, $C(168)$, $C(112)$ も同様にできる。

Lemma 3 (Masley's Rank Theorem)

K/k は n 次 cyclic, $p \in k \subset E \subseteq K$ なる任意の中間体に対して $n h_E \not\equiv 0 \pmod p$ なる素数 p がある。このとき C_K の p -rank は f_p の倍数である。ここで f_p は $\text{mod } n$ で p の位数である。

Proof) $c \in C_K \rightarrow \text{order } p$ であり得る。 $\sigma, \tau \in \text{Gal}(K/k)$

$c^\sigma = c^\tau$ であり、 $c = c^{\sigma\tau^{-1}}$ 。 $\sigma\tau^{-1}$ の生成する cyclic group の

不変体 $E \subset K$ であり、 $\sigma \neq \tau$ ならば、 $a(K/E) \equiv 0 \pmod p$ かつ

lemma 1 より、 $a(K/E) = h_E \frac{e(K/E)}{[K:E](E_F: E_F \cap N_{K/E})}$ 。一方仮定より

$h_E e(K/E) \not\equiv 0 \pmod p$ 。故に $c^\sigma = c^\tau$ ならば $\sigma = \tau$ 。これより

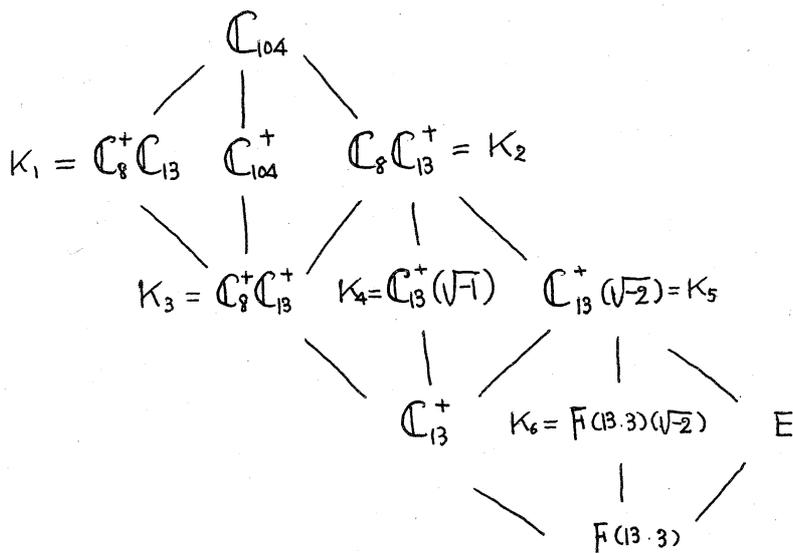
$\#\{c^\sigma \mid \sigma \in \text{Gal}(K/k)\} = n$, C_K の p -rank は r であり、order p の

元は $p^r - 1$ 個あり、 $p^r - 1 \equiv 0 \pmod n$ 。故に $f_p \mid r$ 。

Remark) K/k が Galois ならば全く同様の命題が成り立つ。証明も同じである。

は injective (ある), $c \in S_{K_0}$ と $\exists \exists \tau$. $C^{E_0} = C$ より, S_K の
 image は $S_K^{++} \times S_K^{+-}$ に $\lambda \exists$. よって $S_{K_0} \cong S_K^{++} \times S_K^{+-}$.
 同様にして $S_{K_c} \cong S_K^{++} \times S_K^+$, $S_{K_{cc}} \cong S_K^{++} \times S_K^-$.
 ここで τ $S_{K_{ccc}} = 1$ と $\exists \exists \tau$, $S_{K_0} \cong S_K^{+-}$, $S_{K_c} \cong S_K^{-+}$
 故に $S_K \cong S_{K_0} \times S_{K_c}$. //

Ex 3) C_{104} , $h_{104} = 3^3 \cdot 13$



ここで τ $F(13, 3)$ は $[C_{13}^+ : F(13, 3)] = 2$ と \exists . C_{13}^+ の部分体, τ あり。

$$h_{K_1} = 3 \cdot 13, \quad h_{K_2} = 3^2, \quad h_{K_3} = 1, \quad h_{K_4} = 3, \quad h_{K_5} = 3$$

$$h_{13}^+ = 1, \quad h_{K_6} = 3.$$

$(3, 3, 3, 13)$ 型 τ あり。

$C(144)$, $C(99)$ は τ と簡単 τ あり。

Lemma 5 p は素数, K/k は p 次 cyclic, $G = \text{Gal}(K/k)$,

S_K, S_k はそれぞれ C_K, C_k の p -Sylow group であり, τ 次の 3) の条件を満たすものとする。

1) $N_{K/k} S_K = S_k$.

2) canonical homomorphism $S_k \longrightarrow S_K$ は injective

3) $(S_K : S_k) = p^\lambda$ かつ $\lambda < p-1$

このとき $S_k = S_K^p$

Proof) 上の仮定より $S_k \subset S_K$ としてよい。このとき次の様な部分群の列がとれる。

$$S_\lambda = S_k \subset S_{\lambda-1} \subset \dots \subset S_1 \subset S_0 = S_K \quad (S_i : S_{i+1}) = p$$

S_i は G -invariant であり、また G は S_i/S_{i+1} に trivial に作用する。

σ は G の generator, $c \in S_K$ とすると $c^{\sigma^{-1}} \in S_1$ 。帰納的に

$S_i \ni c_i, c = c_0, c_i^{\sigma^{-1}} = c_{i+1}$ とおくと、簡単な計算により

$$c^{\sigma^k} = \prod_{i=0}^{k-1} c_i^{\binom{k}{i}}, \quad c_{p-1} = 1, \quad \text{ここで } \binom{k}{i} \text{ は二項係数を表す。}$$

$$\text{よって } N_{K/k} c = \prod_{i=0}^{p-1} c_i^{\alpha_i} \quad \alpha_i = \sum_{k=i}^{p-1} \binom{k}{i} \quad \alpha_0 = p.$$

$\binom{k}{i}$ は $(1+t)^k$ にあける t^i の係数であるから、 α_i は

$$\sum_{k=0}^{p-1} (1+t)^k \text{ にあける } t^i \text{ の係数となる。}$$

$$\sum_{k=0}^{p-1} (1+t)^k = \frac{(1+t)^p - 1}{t} \equiv t^{p-1} \pmod{p} \quad \text{よって } i \neq p-1 \text{ ならば}$$

$$\alpha_i \equiv 0 \pmod{p}.$$

また $c_{p-2} = c_{p-3}^{\sigma^{-1}}$ より $N_{K/k} c_{p-2} = c_{p-2}^p = 1$ 、さきにより帰納法

$\therefore C_i^p = 1$ ($i \neq 0$) を得る。故に $N_{\mathbb{K}/\mathbb{C}} = \mathbb{C}^p$ より lemma 5 は証明された。

Ex 4) C_{31} (Kummer)

$$\begin{array}{l} C_{31} \\ | \\ \mathbb{F}(31, 6) = \mathbb{K} \\ | \\ \mathbb{Q}(\sqrt{31}) = \mathbb{K} \end{array} \quad \begin{array}{l} h_{31} = 3^2, \quad h_{\mathbb{K}} = 3^2, \quad h_{\mathbb{R}} = 3 \\ \lambda = 1 < 3 - 1 \\ \text{lemma 5 の条件 1) は, } \mathbb{K}/\mathbb{R} \text{ が totally ramified} \\ \text{であるから, 類体論より成り立つ。} \\ \text{2) は, Kida [10] 参照。} (h_{31}^+ = 1 \text{ である}) \end{array}$$

以上の結果と lemma 5 より $S_{\mathbb{R}} = S_{\mathbb{K}}^3$, 故に $S_{\mathbb{K}}$ は cyclic.

$C(31) \simeq S_{\mathbb{K}}$ より $C(31)$ も cyclic となる。

$C(57)$ も同様に cyclic となる。

Remark) \circ $h_m < 10^4$ の場合を考察の対象としたが, 次の
よ, \circ 場合は決定できなかった。 $C(65)$, $C(156)$,
 $C(177)$, $C(87)$, $C(240)$ 。

\circ $h_m < 10^4$ の場合 $h_m^+ = 1$ が証明されている

(Masley [8])。 $h_m > 10^4$ の場合 h_m^+ の値がほとんどわかっていない。(しかし $C(m)$ ならば, ある程度構造を決定することができた。 \mathbb{K} が imaginary abelian とすると, lemma 1 と同じ記号の下で次の命題が成り立つ。

Lemma 1' $a^-(K/R) = \#\{c \in C_{\bar{K}} \mid c^0 = c\}$ とする。

$$a^-(K/R) = h_{\bar{K}}^{-1} \frac{e^-(K/R)}{(\mu_{\bar{K}} : \mu_{\bar{K}} \cap N_{\bar{K}} K^s)} \cdot 2^s \quad s \in \mathbb{Z}$$

ここで $e^-(K/R) = e^{(K/R)} / e^{(K/R^+)}$, $\mu_{\bar{K}}$ は $E_{\bar{K}}$ に含まれる
1 の中根全体のつくる群を表す。

これより, lemma 3 と同様に, 次の結果を示すことができる。

Lemma 3' $p \neq 2$, $m \bar{h} \not\equiv 0 \pmod{p}$ ならば $C_{\bar{K}}$ の p -rank
は f_p の倍数となる。

lemma 5 は, 更に単純に, $p \neq 2$, $S_K \rightarrow S_{\bar{K}}$, $S_R \rightarrow S_{\bar{R}}$
とすればよい。

以上の結果と次の結果を用いることにより, $p \leq 211$,
 $p \neq 139, 157$ なる素数 p に対して, $C^-(p)$ の構造を決定すること
ができる。

Lemma 6. $C_K \supset A$ を次の条件を満たす $\text{Gal}(K/R)$ -invariant
subgroup とする。 $(\#A, [K:R]) = 1$. このとき

$$1 \longrightarrow \text{Ker } N_{K/R} \cap A \longrightarrow A \longrightarrow N_{K/R} A \longrightarrow 1 \quad (\text{exact})$$

は split する。

証明は容易である。

Table I ($h_m < 10^4$)

m	h_m	Type	
120	2^2	(2^2)	
29	2^3	$(2 \cdot 2 \cdot 2)$	(Kummer)
68	2^3	(2^3)	(Gearth)
31	3^2	(3^2)	(Kummer)
57	3^2	(3^2)	
96	3^2	$(3 \cdot 3)$	
65	2^6	?	
180	$3 \cdot 5^2$	$(3, 5, 5)$	
168	$2^2 \cdot 3 \cdot 7$	$(2^2, 3, 7)$	
41	11^2	$(11, 11)$	(Kummer)
156	$2^2 \cdot 3 \cdot 13$?	
104	$3^3 \cdot 13$	$(3, 3, 3, 13)$	
112	$2^2 \cdot 3^2 \cdot 13$	$(2^2, 3, 3, 13)$	
144	$3 \cdot 13^2$	$(3, 13, 13)$	
77	$2^8 \cdot 5$?	
87	$2^9 \cdot 3$?	
99	$3 \cdot 31^2$	$(3, 31, 31)$	
240	$2^8 \cdot 5^2$	$(?, 5, 5)$	
93	$3^2 \cdot 5 \cdot 151$	$(3^2, 5, 151)$	

Table II ($71 \leq p \leq 211$)

p	h_p (平方因子(…は…因子は省略) · type		
71	7^2	(7^2)	(Kummer)
101	5^5	$(5^2, 5^3)$	
113	2^3	$(2, 2, 2)$	
131	$3^3 \cdot 5^2$	$(3, 3, 3, 5^2)$	
137	17^2	(17^2)	
139	$3^2 \cdot 47^2 \cdot 277^2$	$(3^2, ?, 277, 277)$	
149	3^2	$(3, 3)$	
151	11^2	$(11, 11)$	
157	$13^2 \cdot 157^2$	$(13^2, 157, 157)$	
163	2^2	$(2, 2)$	
197	2^3	$(2, 2, 2)$	
199	3^4	(3^4)	
211	$3^2 \cdot 7^2 \cdot 281^2$	$(3^2, 7^2, 281, 281)$	

Remark) $C(157)$ の 157-Sylow group の構造は,

Iwasawa and Sims, *Computation of invariants
in the theory of cyclotomic fields,*

J. Math. Soc. Japan Vol. 18, No. 1, 1966

で決定されている。

References

- 1 E. Kummer, Über die Irregularität der Determinanten
Monatsber, Akad. d. Wissensch. Berlin, (1853), 194-200
- 2 K. Iwasawa, A note on ideal class groups.
Nagoya Math. J. 27 (1966)
- 3 F. Gearth, The ideal class groups of two cyclotomic
fields. Pro. A.M.S. Vol 78 (1980)
- 4 J. Masley, Class numbers of real cyclotomic number
fields with small conductor. Comp. Math. Vol. 37 (1978)
- 5 H. Yokoi, On the class number of a relatively cyclic
number fields. Nagoya Math. J. 29 (1967) 31-44
- 6 J. Masley, Solution of small class number problems
for cyclotomic fields. Comp. Math. 33 (1976) 179-186
- 7 G. Schrutka v. Rechtenstamm, Tabelle der (relative-)
Klassenzahlen von Kreiskörpern. Abh. Deutsche Akad.
Wiss. Berlin 1964 Math. Nat. Kl. Nr. 2.
- 8 J. Masley, Class groups of abelian number fields
Preprint
- 9 S. Lang, Cyclotomic fields
- 10 Y. Kida, l -extension of CM-fields and cyclotomic
invariant J. Number Theory 12 (1980)