

Galois拡大の相対類群の p -rank

富山医薬大 白井 進 (Susumu Shirai)

p を奇素数, ζ を 1 の原始 p 乗根, \mathbb{Q} を有理数体とする.

任意の有限生成 Abel 群 A に対して, その p -rank $d^{(p)}(A)$ を通常の様に, $d^{(p)}(A) = \dim A/A^p$ によって定義する.

また有限次代数体, K/k を有限次拡大, C_K, C_k をそれぞれ K, k の ideal 類群, $\tilde{N}_{K/k}: C_k \rightarrow C_K$ を $\text{ILM} N_{K/k}$ から誘導された写像とし, $C(K/k) = \text{ker } \tilde{N}_{K/k}$ とおく. $C(K/k)$ が標題にいうところの相対類群である. 更に簡単のために,

$$e(K) = d^{(p)}(C_K), \quad e(K/k) = d^{(p)}(C(K/k)), \quad e(k) = d^{(p)}(C_k)$$

とおく.

Hecke [9] は $K = \mathbb{Q}(\zeta)$, $k = \mathbb{Q}(\zeta + \zeta^{-1})$ のとき $e(K/k) \geq e(k)$ を証明し, これを用いて $e(K/k) = e(k)$ ならば, Fermat の最終定理の first case が 指数 p に対して正しいことを示した.

Leopoldt [13] は Spiegelungssatz の応用として Hecke の不等式をある種の CM-field に拡張したが, それは次の Iwasawa の

結果に含まれる ([2], p.58, Theorem 2.1 又は [21], p.192, Theorem 10.11 参照).

Theorem A. K/k を CM-field とし, $K \ni \eta$ とする. このとき

$$e(K/k) \geq e(k) - 1.$$

η を K に含まれる最高の 1 の p 中根とする. もし $K(\sqrt[p]{\eta})/K$ が分岐するならば,

$$e(K/k) \geq e(k).$$

相対類群の p -rank に関しては、現在のところこの結果が最も良きものの一つであると思われる.

本稿ではこの結果の次の性質(P)を持つ Galois 扩大 K/k への拡張及びその p -円分体への応用についてスケッチを与える:

(P) $K \ni \eta$, $\eta \neq 1$ 且 $p \nmid [K:k]$.

初めから p を奇素数に限定したのは、この中の条件 $\eta \neq 1$ のためである.

以下、次の記号を用いる.

k^\times k の乗法群.

E_k k の单数群.

m を k の整 ideal とするとき,

$(\text{mod } m)_k^*$ k における $m \bmod m$ に関する既約剩余類群.

$S_k(m)$ unit ray number group mod m in k , すなはち

$$\{ a \in k^{\times} \mid a \equiv 1 \pmod{m} \}.$$

$k(m)$ $k \pmod{m}$ は、閾値をもつ ray class field.

k' の数 a は、単項 ideal (a) が k' の ideal の p 乗となるとき、 singular と呼ばれる。

$V_{k'}(m)$ m に素な k' の singular numbers の群.

k' m に素な k' の数群.

1° 準 備

Safarevič [16], p.131 と全く同じ議論で次が示される。

Lemma 1. $d^{(p)}(V_{k'}(m)/k'^p) = e(k) + d^{(p)}(E_k).$

類体論、同型定理より ([17], Lemma 39 の証明参照.)

Lemma 2. $d^{(p)}(\text{Gal}(k(m)/k)) = e(k) + d^{(p)}((\text{mod } m)_k^{\times})$
 $- d^{(p)}(V_{k'}(m)/V_{k'}(m) \cap k'^p S_{k'}(m)).$

2° 拡張

次の Lemma は全く簡単であるが、Theorem A の拡張にとって
は重要である。

Lemma 3. K/k は性質 (P) を持つ Galois 拡大とする。

もし $K(\sqrt{d})$. ($d \in K^{\times} - K^{p^2}$) が K と k 上の巡回拡大との
合併にならなければ、 $N_{K/k} d \in k^{\times p}$. 加えて $[K:k] = 2$ ならば、
逆も成り立つ。

後半の部分は Gruij [7], Hilfsatz A のチョット (た拡張) に在
る 213.

$K \ni 3 \times l$, 次の様によく.

$$W_K((1-3)^p) = \{ d \in V_K(p) \mid \exists X \in K'; X^p \equiv d \pmod{(1-3)^p} \}$$

$$= V_K(p) \cap K'^p S_K((1-3)^p),$$

$$W(K/\mathbb{F}) = \{ d \in W_K((1-3)^p) \mid N_{K/\mathbb{F}}d \in \mathbb{F}'^p \}$$

(K' , \mathbb{F}' はそれぞれ p に素な K , \mathbb{F} の数群).

Lemma 4. 1) $d^{(p)}(W_K((1-3)^p)/K'^p) = e(K)$.

2) もし K/\mathbb{F} が性質 (P) を持つ Galois 扩大ならば,

$$d^{(p)}(W(K/\mathbb{F})/K'^p) \geq e(\mathbb{F}).$$

更に $[K : \mathbb{F}] = 2$ ならば, 等号が成立する.

1) は Kummer 理論から, 2) は Lemma 3 から従う.

次に, $\tilde{N}_{K/\mathbb{F}}(W_K((1-3)^p)/K'^p)$ を把握するためには, (p) の \mathbb{F} に
あり 3 素 ideal 分解を

$$(p) = \prod g^{e_g}$$

とし

$$(1) \quad m(p) = \prod g^{n_g}$$

$$\text{ただし}, n_g = \min \{ \text{整数 } n \mid n \geq \frac{pe_g}{p-1} \}$$

$$W_{\mathbb{F}}(m(p)) = V_{\mathbb{F}}(p) \cap \mathbb{F}'^p S_{\mathbb{F}}(m(p))$$

とおく. すなはち n_g の取扱い, 性質 (P), Kummer 理論 及び Lemma
4 によること,

$$1 \rightarrow W(K/k)/K'^p \rightarrow W_k((1-3)^p)/K'^p \xrightarrow{\tilde{N}_{K/k}} W_k(m(p))/k'^p \rightarrow 1$$

が完全系列となる。従って 2, lemmas 1, 2, 4 の 1 による。

$$\begin{aligned} e(K) &= d^{(p)}(W(K/k)/K'^p) + d^{(p)}(\text{Gal}(k(m(p))/k)) + d^{(p)}(E_k) \\ &\quad - d^{(p)}((\text{mod } m(p))^{\times}_k) \end{aligned}$$

を得る。 $p \nmid [K:k]$ の場合、 $e(K) = e(K/k) + e(k)$ 、故に lemma 4 の 2 から次が従う。

Theorem 5. K/k を性質(P)を持つ Galois 拡大とするとき、

$$e(K/k) \geq d^{(p)}(\text{Gal}(k(m(p))/k)) + d^{(p)}(E_k) - d^{(p)}((\text{mod } m(p))^{\times}_k),$$

ここで $m(p)$ は (1) 式によって定義された長の整 ideal である。更にもし $[K:k] = 2$ ならば、等号が成り立つ。

この定理から Theorem A の拡張が得られる。

Theorem 6. K/k を性質(P)を持つ Galois 拡大、 r_2 を k の complex 方素因子の数とするとき、

$$e(K/k) \geq e(k) - (r_2 + 1).$$

η を K に含まれる最高の 1 の p 中根とする。もし $K(\sqrt[p]{\eta})/k$ が分岐するならば、

$$e(K/k) \geq e(k) - r_2.$$

前半は $d^{(p)}((\text{mod } m(p))^{\times}_k) \leq [k:\mathbb{Q}]$ より出る。後半の部分は

$$d^{(p)}(\text{Gal}(k(m(p))/k)) \geq e(k) + 1$$

から従うのであるが、これを示すためには conductor に関する議論を行ければならない。要点は n_p のとり方、

$K(\sqrt{p})/K$ が mod $(1-\zeta)^p$ で定義されることは、 $m(p)$ の素因子が K 上で tamely ramified であることにはある。

3° 応用

この節ではつねに $K = \mathbb{Q}(\zeta)$, $\mathbb{k} = \mathbb{Q}(\zeta + \zeta^{-1}) \times L$,

$$e^- = e(K/\mathbb{k}), \quad e^+ = e(L/\mathbb{k}), \quad \pi = 1 - \zeta$$

とおく。Theorems A 及び 6 から Hecke [9] の結果 $e^- \geq e^+$ が得られる。他方, deopoldt [13] の Spiegelungssatz の応用として e^- に対する upper bound が得られる (例えは, [14], p.184 参照)。ここでは e^- に対するもう一つの lower bound による精密な upper bound を与えることとする。

Theorem 5, Lemma 2 によると $\mathbb{Q}(\sqrt[3]{\zeta} + \sqrt[3]{\zeta}^{-1})/\mathbb{k}$ の conductor が $(N_{K/\mathbb{k}}\pi)^{\frac{p+1}{2}}$ に等しいことから 次を得る。

Lemma 7. $e^- = d^{(p)}(\text{Gal}(L/\mathbb{k}))$.

これは [21], p.193, Prop. 10.13 の simple version である。

この式は Lemmas 1, 2 を適用することで

$$e^- = d^{(p)}(\mathcal{V}_{\mathbb{k}}(p) \cap \mathbb{k}'^p S_{\mathbb{k}}(p)/\mathbb{k}'^p)$$

となる。 $\mathcal{V}_{\mathbb{k}}(p) \cap \mathbb{k}'^p S_{\mathbb{k}}(p) \ni a$ をとく, $(a) = \pi \mathbb{k}'^p$ とし 写像 $a \rightarrow \text{class of } \pi a$ in $C_{\mathbb{k}}$ を考へよ。

$$1 \rightarrow E_{\mathbb{k}} \cap \mathbb{k}'^p S_{\mathbb{k}}(p)/E_{\mathbb{k}}^p \rightarrow \mathcal{V}_{\mathbb{k}}(p) \cap \mathbb{k}'^p S_{\mathbb{k}}(p)/\mathbb{k}'^p \rightarrow C_{\mathbb{k}}$$

は完全系である。従って

$$d^{(p)}(E_k \cap k'^p S_k(p)/E_k^p) \leq e^- \leq d^{(p)}(E_k \cap k'^p S_k(p)/E_k^p) + e^+.$$

$d^{(p)}(E_k \cap k'^p S_k(p)/E_k^p)$ を計算するためには, Dénes [2], [3] や Washington [20] を用いよ.

B_i (i は偶数) を Bernoulli 数とする. Dénes [2] は 合同式

$$\begin{cases} B_{ipj} \equiv 0 \pmod{p^{2j+1}} & \text{for } 0 \leq j < u_i, \\ B_{ipu_i} \not\equiv 0 \pmod{p^{2u_i+1}} \end{cases}$$

によると Bernoulli 数, p -character u_2, u_4, \dots, u_{p-3} を定義し, [3] における p -character の有限性の仮定の下で, 次の定理を証明した.

Theorem B ([3], Sätze 1 u. 2). 次の様な π の基本单数系 $\{\delta_2, \delta_4, \dots, \delta_{p-3}\}$ が存在する:

$$\delta_i \equiv a_i + b_i \pi^{c_i} \pmod{\pi^{c_i+1}},$$

$$c_i = i + (p-1)u'_i, \quad 0 \leq u'_i \leq u_i,$$

$$a_i, b_i (i \neq p-1) \text{ は素有理整数}.$$

この様な u'_i は [3], Satz 3 の意味に於て一意的に決定され
る. ([20], Theorem 2 を参考のこと.)

假定された p -character の有限性は Washington [20], Theorem 1 によって, p -adic regulator $\neq 0$ の結果として証明される.

さて,

$$I(p) = \{i=2, 4, \dots, p-3 \mid p \mid B_i\}, \quad D(p) = \{i \in I(p) \mid u'_i = 0\},$$

$$i(p) = \# I(p), \quad d(p) = \# D(p)$$

とおく。 $i(p)$ は p の irregularity index として知られてゐるもので、
ある。 Theorem B を用ひて、

$$d^{(p)}(E_k \cap k'^p S_k(p)/E_k^p) = i(p) - d(p)$$

と計算される。従って、

Theorem 8. $\max\{e^+, i(p) - d(p)\} \leq e^- \leq e^+ + i(p) - d(p)$.

これと Ribet [15] の有名な結果 (Herbrand の定理の逆) を
組み付けて、

Corollary 9. $e^+ \geq \frac{d(p)}{2}$.

が従う。しかし、種々の状況から

$$e^+ \geq d(p)$$

が予想される。

最後に Fermat の最終定理 (FLT) の first case に関する
一注意を述べる。Eichler [6] は

Theorem C. もし $e^- < \sqrt{p} - 2$ ならば、Case I は 指数 p に
対して正しい。

を、Brückner [1] と Skula [19] は

Theorem D. もし $i(p) < \sqrt{p} - 2$ ならば、Case I は 指数 p に
対して成立する。

を証明した。

$$\nabla(K/k) = \{\alpha \in \nabla_k(p) \mid N_{K/k} \alpha \in k'^p\}$$

とよくと、

$$1 \rightarrow V(K/k)/K'^P \rightarrow V_K(p)/K'^P \rightarrow V_k(p)/k'^P \rightarrow 1$$

は完全系列となる。よって Lemma 1 より

$$d^{(p)}(V(K/k)/K'^P) = e^- + 1.$$

lemmas 3 と 7 によると 次の様な $d_i \in K^\times$ が存在する：

$$(2) \quad \begin{cases} K \cdot k(p) = K(\sqrt[p]{d_1}, \dots, \sqrt[p]{d_{e^-}}) \\ N_{K/k} d_i \in k^{\times P} \text{ for } i = 1, \dots, e^- \\ K(\sqrt[p]{d_i})/K \text{ unramified for } i = 1, \dots, e^+. \end{cases}$$

ここで conductor 1= 開きの議論を用ひよると、各 d_i を p の素に
たる様に選ぶことが出来、そのとき $\{1, d_1, \dots, d_{e^-}\}$ が
 $V(K/k)/K'^P$ の basis となることが示される。 $\exists \tau \in V(K/k)/K'^P$
が $\bar{x} \pmod{p}^x$ 中への homomorphism g を $g(x \pmod{K'^P}) =$
 $x^{p-1} \pmod{p}$ ($x \in V(K/k)$) によると定義する。 (2) の 3 番目の
条件から、

Lemma 10. $d^{(p)}(\operatorname{Im} g) \leq e^- - e^+ + 1.$

となることが分る。この事実と Eichler [5] の手法を組み合せ、

Theorem 11. $x, y \in$

$$x + y \bar{x} \in V_K(p) \text{ 且 } (p, xy) = 1$$

とある有理整数である。このときもし $e^- - e^+ < \sqrt{p} - 2$ ならば、

$$x \equiv y \pmod{p}.$$

Corollary 12. $\#L(e^- - e^+) < \sqrt{p} - 2$ ならば, FLT, Case I
は指數 p に対して正(1).

Theorem 8 より, $e^- - e^+ \leq i(p) - d(p) \leq i(p)$ なので, \Rightarrow Cor.
1は Theorems C, D を含んでいき. そして同時に最初に述べた
Hecke の結果 ($e^- = e^+$ の場合, $p > 3$) も含まれる.

参考文献

- [1] H. Brückner, Explizites Reziprozitätsgesetz und Anwendungen, Vorlesungen aus dem Fachbereich Math. der Univ. Essen, Heft 2, 1979.
- [2] P. Dénés, Über irreguläre Kreiskörper, Publ. Math. Debrecen, 3 (1953), 17-23.
- [3] P. Dénés, Über Grundeinheitssysteme der irregulären Kreiskörper von besonderen Kongruenzeigenschaften, Publ. Math. Debrecen, 3 (1954), 195-204.
- [4] P. Dénés, Über den zweiten Faktor der Klassenzahl und den Irregularitätsgrad der irregulären Kreiskörper, Publ. Math. Debrecen, 4 (1956), 163-170.
- [5] M. Eichler, Eine Bemerkung zur Fermatschen Vermutung, Acta Arith., 11 (1965), 129-131, (Errata) 261.

- [6] M. Eichler, Zum 1. Fall der Fermatschen Vermutung, J. reine angew. Math., 260 (1975), 214.
- [7] O. Grün, Zur Fermatschen Vermutung, J. reine angew. Math., 170 (1934), 231 - 234.
- [8] H. Hasse, Zahlentheorie, Akademie-Verlag, Berlin, 1949.
- [10] F.-P. Heider, Kapitulationsproblem und Knotentheorie, Manuscripta Math., 46 (1984), 229 - 272.
- [11] J. Herbrand, Sur les classes des corps circulaires, J. Math. Pures Appl. (9), 11 (1932), 417 - 441.
- [12] S. Lang, Cyclotomic Fields II, Springer-Verlag, New York - Heidelberg - Berlin, 1980.
- [13] H. W. Leopoldt, Zur Struktur der ℓ -Klassengruppe galoisscher Zahlkörper, J. reine angew. Math., 199 (1958), 165 - 174.
- [14] P. Ribenboim, 13 lectures on Fermat's Last Theorem, Springer-Verlag, New York - Heidelberg - Berlin, 1979.
- [15] K. Ribet, A modular construction of unramified p -extensions of $\mathbb{Q}(u_p)$, Invent. Math., 34 (1976), 151 - 162.
- [16] I. R. Šafarevič, Extensions with given ramification points (in Russian), Publ. Math. IHES, 18 (1964),

$71 - 95 = \text{Amer. Math. Soc. Transl. Ser 2, 59 (1966),}$
 $128 - 149.$

- [17] S. Shirai, On the central class field mod m of Galois extensions of an algebraic number field, Nagoya Math. J., 71 (1978), 61-85.
- [18] S. Shirai, The main theorems of Furtwängler on Fermat's last theorem.
- [19] L. Škula, Non-possibility to prove infinity of regular primes from some theorems, J. reine angew. Math., 291 (1977), 162-181.
- [20] L. C. Washington, Units of irregular cyclotomic fields, Illinois J. Math., 23 (1979), 635-647.
- [21] L. C. Washington, Introduction to Cyclotomic Fields, Springer-Verlag, New York-Heidelberg-Berlin, 1982.
- [9] E. Hecke, Über nicht-reguläre Primzahlen und den Fermatschen Satz, Nachr. Akad. d. Wiss. Göttingen, 1910, 420-424.