数理解析研究所講究録
第589巻 1986年 149-160

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．

k を有限次代数体，K/k を有限次拡大，C_K, C_k をそれぞれ K, k の ideal 類群，$\tilde{N}_{K/k}: C_K \to C_k$ をノルム $N_{K/k}$ から誘導された写像とし，$C(K/k) = \operatorname{Ker} \tilde{N}_{K/k}$ 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 ([12], p.58, Theorem 2.1 又は [21], p.192, Theorem 10.11 参照).

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

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

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

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

相対類群の p-rank に関しては, 現在のところこの結果が最良の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 拡大 K/k への拡張及びその p-円分体への応用についてのスケッチを与える:

(P) $K \supset \zeta$, $k \not\supset \zeta$ 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 $k \not\supset \zeta$ 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 の単数群.

$\mathfrak{m}$ を k の整 ideal とするとき,

$(\mathrm{mod}\,\mathfrak{m})_k^\times$ k における $\mathrm{mod}\,\mathfrak{m}$ に関する既約剰余類群.

$S_k(\mathfrak{m})$ unit ray number group mod $\mathfrak{m}$ in k, すなわち

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

$k(\mathfrak{m})$ k の mod $\mathfrak{m}$ に関する ray class field.

$k^\times$ 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.

$V_k(\mathfrak{m})$ $\mathfrak{m}$ に素な k の singular numbers の群.

k' $\mathfrak{m}$ に素な k の数群.

1° 準備

Šafarevič [16], p.131 と全く同じ議論で次が示される.

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

類体論の同型定理より ([17], Lemma 39 の証明参照)

Lemma 2. $d^{(p)}(\mathrm{Gal}(k(\mathfrak{m})/k)) = e(k) + d^{(p)}((\bmod \mathfrak{m})_k^\times)$
$- d^{(p)}(V_k(\mathfrak{m})/V_k(\mathfrak{m}) \cap k'^p S_k(\mathfrak{m}))$.

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 $K(\sqrt[p]{\alpha})$ $(\alpha \in K^\times - K^{\times p})$ が K と k 上 p 次の巡回拡大との合併になるならば，$N_{K/k}\alpha \in k^{\times p}$. 加えて $[K:k]=2$ ならば，逆も成り立つ.

後半の部分は Grün [7], Hilfssatz A のチョットした拡張になっている.

$K \ni \zeta$ とし, 次の様におく.

$$W_K((1-\zeta)^p) = \{\alpha \in \nabla_K(p) \mid \exists X \in K';\ X^p \equiv \alpha \pmod{(1-\zeta)^p}\}$$

$$= \nabla_K(p) \cap K'^p S_K((1-\zeta)^p),$$

$$W(K/k) = \{\alpha \in W_K((1-\zeta)^p) \mid N_{K/k}\alpha \in k'^p\}$$

(K', k' はそれぞれ p に素な K, k の数群).

<u>Lemma 4.</u> 1) $d^{(p)}(W_K((1-\zeta)^p)/K'^p) = e(K)$.

2) もし K/k が性質 (P) を持つ Galois 拡大ならば,

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

更に $[K:k] = 2$ 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, $\tilde{N}_{K/k}(W_K((1-\zeta)^p)/K'^p)$ を把握するために, (p) の k における素 ideal 分解を

$$(p) = \prod_{\mathfrak{g}} \mathfrak{g}^{e_{\mathfrak{g}}}$$

とし

(1) $$m(p) = \prod_{\mathfrak{g}} \mathfrak{g}^{n_{\mathfrak{g}}}$$

ただし, $n_{\mathfrak{g}} = \mathrm{Min}\{\text{整数 } n \mid n \geq \frac{pe_{\mathfrak{g}}}{p-1}\}$

$$W_k(m(p)) = \nabla_k(p) \cap k'^p S_k(m(p))$$

とおく. すると $n_{\mathfrak{g}}$ の取り方, 性質 (P), Kummer 理論及び Lemma 4 によって,

$$1 \to W(K/k)/K'^p \to W_K((1-\zeta)^p)/K'^p \xrightarrow{\tilde{N}_{K/k}} W_k(\mathfrak{m}(p))/k'^p \to 1$$

が完全系列となる．従って，lemmas 1, 2, 4の1により，

$$e(K) = d^{(p)}(W(K/k)/K'^p) + d^{(p)}(\mathrm{Gal}(k(\mathfrak{m}(p))/k)) + d^{(p)}(E_k) - d^{(p)}((\mathrm{mod}\,\mathfrak{m}(p))_k^\times)$$

を得る．$p \nmid [K:k]$ なので，$e(K) = e(K/k) + e(k)$，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，

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

ここに $\mathfrak{m}(p)$ は(1)式によって定義された k 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な素因子の数とすると，

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

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

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

前半は $d^{(p)}((\mathrm{mod}\,\mathfrak{m}(p))_k^\times) \leqq [k:\mathbb{Q}]$ より出る．後半の部分は

$$d^{(p)}(\mathrm{Gal}(k(\mathfrak{m}(p))/k)) \geqq e(k)+1$$

から従うのであるが，これを示すためにはconductorに関する議論をしなければならない．要点は n_g のとり方，

$K(\sqrt[p]{\eta})/K$ が $\mathrm{mod}\,(1-\zeta)^p$ で定義されること，$\mathfrak{m}(p)$ の素因子が K に於て tamely ramified であることにある．

3° 応用

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

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

とおく．Theorems A又は6から Hecke [9] の結果 $e^- \geqq e^+$ 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（例えば，[14], p. 184 参照）．ここでは e^- に対するもう一つの lower bound とより精密な upper bound を与えることにする．

Theorem 5, Lemma 2 及び $\mathbb{Q}(\sqrt[p]{\zeta}+\sqrt[p]{\zeta}^{-1})/k$ の conductor が $(N_{K/k}\pi)^{\frac{p+1}{2}}$ に等いことから次を得る．

<u>Lemma 7.</u> $\quad e^- = d^{(p)}(\mathrm{Gal}(k(p)/k))$.

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

この式に lemmas 1, 2 を適用すると

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

となる．$V_k(p)\cap k'^p S_k(p)\ni a$ をとり，$(a)=\mathfrak{a}^p$ として写像 $a \to$ class of $\mathfrak{a}$ in C_k を考えると，

$$1 \to E_k\cap k'^p S_k(p)/E_k^p \to V_k(p)\cap k'^p S_k(p)/k'^p \to C_k$$

は完全系列となる．従って

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

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

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

$$\begin{cases} B_{ip^j} \equiv 0 \pmod{p^{2j+1}} \text{ for } 0 \leqq j < u_i, \\ B_{ip^{u_i}} \not\equiv 0 \pmod{p^{2u_i+1}} \end{cases}$$

によって Bernoulli 数の p-character $u_2, u_4, \cdots, u_{p-3}$ を定義し，[3] において 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 k の基本単数系 $\{\delta_2, \delta_4, \cdots, \delta_{p-3}\}$ が存在する：

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

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

a_i, b_i は p に素な有理整数．

この様な u_i' は [3], Satz 3 の意味において一意的に決定される．([20], Theorem 2 も参照のこと．)

仮定された p-character の有限性は Washington [20], Theorem 1 において，p-adic regulator $\neq 0$ の一結果として証明された．

さて，

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

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

とおく. $i(p)$ は p の irregularity index として知られているものである. Theorem B を用いると,

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

と計算される. 従って,

Theorem 8. $\mathrm{Max}\{e^+, i(p)-d(p)\} \leqq e^- \leqq e^+ + i(p) - d(p)$.

これと Ribet [15] の有名な結果 (Herbrand の定理の逆) を結び付けると,

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

が従う. しかし, 種々の状況から

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

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 に対して成り立つ.

を証明した.

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

とおくと,

$$1 \to T(K/k)/K'^p \to T_K(p)/K'^p \to T_k(p)/k'^p \to 1$$

は完全系列となる. よって Lemma 1 より

$$d^{(p)}(T(K/k)/K'^p) = e^- + 1.$$

Lemmas 3 と 7 によって 次の様な $\alpha_i \in K^\times$ が存在する:

$$(2)\quad \begin{cases} K \cdot k(p) = K(\sqrt[p]{\alpha_1}, \cdots, \sqrt[p]{\alpha_{e^-}}) \\ N_{K/k}\alpha_i \in k^{\times p} \quad \text{for } i = 1, \cdots, e^- \\ K(\sqrt[p]{\alpha_i})/K \text{ unramified for } i = 1, \cdots, e^+. \end{cases}$$

ここで conductor に関する議論を用いると, 各 α_i を p と素になる様に選ぶことが出来, そのとき $\{\zeta, \alpha_1, \cdots, \alpha_{e^-}\}$ が $T(K/k)/K'^p$ の basis となることが示される. そこで $T(K/k)/K'^p$ から $(\mathrm{mod}\ p)_K^\times$ の中への homomorphism g を $g(\alpha \bmod K'^p) = \alpha^{p-1} \bmod p$ $(\alpha \in T(K/k))$ によって定義すると, (2) の 3 番目の条件から,

Lemma 10. $d^{(p)}(\mathrm{Im}\, g) \leqq e^- - e^+ + 1.$

となることが分る. この事実と Eichler [5] の手法を組み合せると,

Theorem 11. x, y を

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

となる有理整数とする. このときもし $e^- - e^+ < \sqrt{p} - 2$ ならば,

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

Corollary 12. もし $e^- - e^+ < \sqrt{p} - 2$ ならば，FLTのCase Iは指数 p に対して正しい．

Theorem 8より，$e^- - e^+ \leqq i(p) - d(p) \leqq i(p)$ なので，このCor.はTheorems C, Dを含んでいる．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. Dénes, Über irreguläre Kreiskörper, Publ. Math. Debrecen, 3 (1953), 17-23.

[3] P. Dénes, Über Grundeinheitssysteme der irregulären Kreiskörper von besonderen Kongruenzeigenschaften, Publ. Math. Debrecen, 3 (1954), 195-204.

[4] P. Dénes, 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 $\mathbb{Q}(\mu_p)$, Invent. Math., 34 (1976), 151-162.

[16] I. R. Šafarevič, Extensions with given ramification points (in Russian), Publ. Math. IHES, 18 (1964),

71-95 = 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. Skula, 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.