

Some Remarks on Leopoldt's Conjecture

神奈川県立松陽高等学校 島田 勉 (Tsutomu Shimada)

序

p を奇素数、 k を有限次代数体とし、 K を k の有限次拡大体とする。 k に於て、 p に関する Leopoldt 予想 (以下これを $LC(k, p)$ で表す) が成立すると仮定したとき、 K に於ても予想が成立するための十分条件について報告する。このようなタイプの十分条件は既にいくつか知られているが、 K/k の拡大次数が p -巾の場合と p と素である場合とに分けられる。前者の場合としては、三木[3]、三木-佐藤[4]、山下[7]、などがあり、後者としては、Sands[6]、がある。ここでは後者の場合を扱う。

$\mathbb{Q}$ を有理数体、 E_k を k の単数群として、その部分群 $E_k(p^m)$ を、 $E_k(p^m) = \{ u \in E_k \mid u \equiv 1 \pmod{p^m} \}$, m は自然数、とする。Leopoldt 予想は次の様に表される (cf. 岩澤[2], Sands[6])。

$$LC(k, p) \text{ 成立} \iff \forall a \in \mathbb{N}. \exists m \in \mathbb{N}. \text{ s.t. } E_k(p^m) \subset E_k^{pa}.$$

但し、 $\mathbb{N}$ は自然数全体の集合を表す。

1. K/k が Galois 拡大の場合

次は良く知られている。但し、 ζ_p は 1 の原始 p 乗根。

Proposition 1.1. 次の2つのうちのひとつを仮定する；

- (1) $k \not\subset \mathbb{Q}_p$ 且、 p をわるどの prime も $k(\zeta_p)/k$ で完全分解しない、
- (2) $k \supset \mathbb{Q}_p$ 且、 p をわる k の prime はただひとつ。

このとき次がなり立つ；

$$LC(k, p) \text{ 成立} \iff \exists m \in \mathbb{N}. \text{ s.t. } E_k(p^m) \subset E_k^p.$$

証明. Sands [6] 参照.

この Prop. の仮定“(1)または(2)”を、以下 $A(k, p)$ で表す。
これを仮定すると、 $LC(k, p)$ を示すのに(前記表現で) $a=1$ の場合を示せば十分、ということである。尚、 $p-1$ が p の $k/\mathbb{Q}$ での分岐指数を割り切らなければ、 $A(k, p)$ の(1)が成り立つことは明らかだから、 $A(k, p)$ を仮定することによって除外される素数は、高々、 $k/\mathbb{Q}$ で分岐する素数たちである。

Proposition 1.2. $g \in \mathbb{N}$ は p と素、 K/k は g 次 Galois 拡大、 $K \cap k(\zeta_p) = k$ 、且、 $LC(k, p)$ と $A(K, p)$ の成立を仮定し、 $G = \text{Gal}(K/k)$ の交換子群の、 G に対する指数が $p-1$ と素である

とする. 更に, ある $m \in \mathbb{N}$ があって, すべての $\alpha \in E_K(P^m)$ に対して, $K(\zeta_P, \alpha^{\frac{1}{p}})/K(\zeta_P)$ が Galois 拡大となるとする. このとき, $LC(K, P)$ が成立する.

証明 m を上記のようなものとして, $M_K^{(m)} = E_K(P^m)K^P/K^P \subset K^X/K^P$ とする. 但し, K^P は $(K^X)^P$ を表す. $M_K^{(m)}$ は $\mathbb{F}_P$ (標数 P の素体) 上の加群である. 各 $\alpha \in E_K(P^m)$ に対して, $\bar{\alpha} = \alpha \bmod K^P$ が $\mathbb{F}_P$ 上で生成する部分加群を $\langle \bar{\alpha} \rangle \subset M_K^{(m)}$ で表す. 拡大 $K(\zeta_P, \alpha^{\frac{1}{p}})/K(\zeta_P)$ に関する仮定により, $\forall \tau \in G$ に対して自然数 $1 \leq l_\tau \leq P-1$ が存在して, $\alpha^\tau \in \alpha^{l_\tau} K(\zeta_P)^P$ となり, $K(\zeta_P)$ から K への Norm を作用させることにより, $\langle \bar{\alpha} \rangle = \langle \bar{\alpha}^\tau \rangle$ を得る. 但し, $\bar{\alpha}^\tau$ は $\overline{\alpha^\tau}$ を意味する.

$H_\alpha = \{ \tau \in G \mid \bar{\alpha}^\tau = \bar{\alpha} \} \subset G$, ($\alpha \in E_K(P^m)$), とおく. H_α が G の正規部分群であり, G/H_α が $(\mathbb{Z}/P\mathbb{Z})^X$ ($\mathbb{Z}$ は有理整数環) の部分群に同型であることは, τ に上記 l_τ を対応させることにより, 直ちにわかる. 従って, H_α の指数は $P-1$ の約数であり, H_α は G の交換子群を含むことがわかる. よって, 仮定により, $\forall \alpha \in E_K(P^m)$ に対して, $H_\alpha = G$ となる. 今, m を十分大きくとれば, $E_K(P^m) \subset E_K^P$ であるとしてよい.

$N_{K/K} \alpha \in E_K(P^m) \subset E_K^P$ であるから, $\bar{1} = \overline{N_{K/K} \alpha} = \overline{\prod_{\tau \in G} \alpha^\tau} = \prod_{\tau \in G} \bar{\alpha}^\tau = \prod_{\tau \in G} \bar{\alpha} = \bar{\alpha}^g$. $P \nmid g$ だから, $\bar{\alpha} = \bar{1}$. 則ち,

$\alpha \in K^P$ が示された. 故に, $E_K(P^m) \subset E_K^P$ が成立し, $LC(K, P)$ の成立がわかる.

2. K/k が巡回拡大の場合

ℓ を P と異なる奇素数とする. ここでは拡大 K/k が ℓ -中次巡回拡大である場合を扱う. 始めに, 一般的な lemma をふたつ証明する.

Lemma 2.1. F を任意の有限次代数体とする. $\mathbb{Z}$ -rank $E_F \geq 1$. ならば, ある $m \in \mathbb{N}$ が存在して次がなり立つ;

$$\text{rank } M_F^{(m)} < \mathbb{Z}\text{-rank } E_F(P^m).$$

但し, $\text{rank } M_F^{(m)}$ は $\mathbb{Q}$ 上の次元を表す.

証明 $E_F(P)$ が torsion free であることは明りか. ある $m \in \mathbb{N}$ をとれば, $E_F(P^{m-1}) \supsetneq E_F(P^m)$ となる. このとき $[E_F(P^{m-1}) : E_F(P^m)] = P^e$ ($e \in \mathbb{N}$) とおく. 単因子論により $E_F(P^{m-1})$ の $\mathbb{Z}$ -basis $\{u_1, \dots, u_r\}$ ($r = \mathbb{Z}\text{-rank } E_F$) で, 次の2つをみたすものが存在する:

- (i) $\{u_1^{e_1}, \dots, u_r^{e_r}\}$ は $E_F(P^m)$ の $\mathbb{Z}$ -basis. 但し, $e_i \in \mathbb{N}$.
- (ii) $e_i | e_{i+1}$, $i=1, \dots, r-1$, 且 $e_1 \cdots e_r = P^e$.

このとき特に、 $P|e_r$ となり、 $\overline{u_r} \in K^P$ となる。よって、 $M_F^{(m)}$ の rank は r よりも小さい。

Lemma 2.2. K/k は次数が P と素な abel 拡大とする。
 $E'_{K/k} = \{u \in E_K \mid \text{任意の } K/k \text{ の中間体 } M \neq K \text{ において } N_{K/M} u = 1\}$,
 とおく。すべての K/k の中間体 $M \neq K$ に於て $LC(M, P)$ が成立
 すると仮定すると、ある $m \in \mathbb{N}$ に対して次がなり立つ；
 $M_K^{(m)} = (E_K(P^m) \cap E'_{K/k}) K^P / K^P$.

証明 $\mathcal{M} = \{M_i\}$ を、 K/k の中間体で $[K:M_i]$ が素数であるよ
 うなもの全体の集合とする。仮定により、すべての i に対し
 て $E_{M_i}(P^m) \subset E_{M_i}^P$ がなり立つような $m \in \mathbb{N}$ が存在する。以下
 m をそのようなものとする。 α_0 を $E_K(P^m)$ の任意の元とする。
 $N_{K/M_1} \alpha_0 \in E_{M_1}(P^m) \subset E_{M_1}^P$ だから、ある $v_1 \in E_{M_1}$ があって
 $N_{K/M_1} \alpha_0 = v_1^P$ となる。 $[K:M_1] = f_1$ とおく。 $x_1 P - y_1 f_1 = 1$
 となる整数 x_1, y_1 をとる。

$N_{K/M_1}(\alpha_0^{1-x_1 P} v_1^{y_1 P}) = v_1^{P(1-x_1 P)+y_1 P f_1} = v_1^{P(1-x_1 P+y_1 f_1)} = 1$.
 そこで、 $\alpha_1 = \alpha_0^{1-x_1 P} v_1^{y_1 P}$ とおくと、 $\alpha_1 \in E_K(P^m)$, $N_{K/M_1} \alpha_1 = 1$
 且 $\overline{\alpha_0} = \overline{\alpha_1} \in M_K^{(m)}$ がなり立つ。

ある $i \in \mathbb{N}$ に対して、 $\alpha_i \in E_K(P^m)$ が存在して、 $N_{K/M_1} \alpha_i =$
 $N_{K/M_2} \alpha_i = \dots = N_{K/M_i} \alpha_i = 1$, $\overline{\alpha_0} = \overline{\alpha_i} \in M_K^{(m)}$ が成り立つ

とする. $N_{K/M_{i+1}} \alpha_i \in E_{M_{i+1}}(p^m) \subset E_{M_{i+1}}^p$ だから, $N_{K/M_{i+1}} \alpha_i = v_{i+1}^p$ となる $v_{i+1} \in E_{M_{i+1}}$ がとれる. $[K:M_{i+1}] = f_{i+1}$ は p と異なる素数だから, $\alpha p - \gamma f_{i+1} = 1$ となる整数 α, γ がある. $\alpha_{i+1} = \alpha_i^{1-\alpha p} v_{i+1}^{\gamma p}$ とおけば, $\alpha_{i+1} \in E_K(p^m)$, $N_{K/M_{i+1}} \alpha_{i+1} = 1$, 且 $\alpha_0 = \overline{\alpha_{i+1}} \in M_K^{(m)}$ であることは直ちにわかる. 更に, 任意の j ($1 \leq j \leq i$) に対して, $N_{K/M_j} \alpha_{i+1} = N_{K/M_j} (\alpha_i^{1-\alpha p} v_{i+1}^{\gamma p}) = N_{K/M_j} v_{i+1}^{\gamma p} = N_{K/M_j} (N_{K/M_{i+1}} \alpha_i^{\gamma}) = N_{K/M_{i+1}} (N_{K/M_j} \alpha_i^{\gamma}) = 1$. 帰納法により, $\alpha_0 = \alpha$, 且, すべての i について $N_{K/M_i} \alpha = 1$. とする α の存在が示された. K/k の任意の中間体 $M \neq K$ は, ある $M_i \in \mathcal{M}$ に含まれるので, この α についてはすべての中間体 $M \neq K$ において $N_{K/M} \alpha = 1$ となる. これで lemma が証明された.

Proposition 2.3. K/k は q^n 次巡回拡大 ($e \in \mathbb{N}$) とする. $n=1$ のとき p は q を法として原始根. $n \geq 2$ のとき p は q^2 を法として原始根であるとする. $LC(k, p)$ と $A(K, p)$ の成立を仮定し, 更に, ある $m \in \mathbb{N}$ があり, K/k の q^ν ($\nu=1, \dots, n$) 次中間体 K_ν に対して

$$\text{rank } M_{K_\nu}^{(m)} < q^\nu (1 - q^{-1}), \quad \forall \nu = 1, \dots, n$$

が成立する. と仮定する. このとき, $LC(K, p)$ が成立する.

証明 $\nu=0$ に対しては $K_0=k$ とし、 $\nu=0,1,\dots,n$ に関する帰納法により証明する。まず、仮定により $LC(K_0, P)$ は成り立つ。次に、 ν ($0 \leq \nu \leq n-1$) において $LC(K_\nu, P)$ の成立を仮定する。 $\text{Gal}(K_{\nu+1}/k) = \langle \tau \rangle$ とする。すべての $i \in \mathbb{N}$ について、 τ は $\mathbb{F}_p$ -vector space $M_{K_{\nu+1}}^{(i)}$ の一次変換である。帰納法の仮定と Lemma 2.2. により、 μ が十分大のとき $M_{K_{\nu+1}}^{(\mu)}$ の上の一次変換として

$$N_{K_{\nu+1}/K_\nu} = \tau^{f^\nu(f-1)} + \tau^{f^\nu(f-2)} + \dots + \tau^{f^\nu} + 1 = 0.$$

このような μ をひとつ固定する。今、 $M_{K_{\nu+1}}^{(\mu)} \neq 1$ であるとする。このとき、 τ の最小多項式は定数ではなく、多項式

$$\mathbb{F}_p[X] \ni X^{f^\nu(f-1)} + X^{f^\nu(f-2)} + \dots + X^{f^\nu} + 1 \quad (1)$$

の約数である。

一般に、自然数 r が f^2 を法として原始根ならば、任意の $e \geq 3$ ($e \in \mathbb{N}$) について、 r は f^e を法として原始根である。よって、仮定により、 P は $f^{\nu+1}$ を法として原始根。また、このとき多項式 (1) は $(\mathbb{F}_p)$ 既約である。従って、 $\text{rank } M_{K_{\nu+1}}^{(\mu)} \geq f^\nu(f-1) = f^{\nu+1}(1-f^{-1})$ となり、仮定に反する。よって十分大きな $i \in \mathbb{N}$ に対して $M_{K_{\nu+1}}^{(i)} = 1$ となり、 $E_{K_{\nu+1}}(P^i) \subset K_{\nu+1}^P$ となることかわかる。一方、 $A(K, P)$ の成立と P に関する仮定より、 $A(K_\nu, P)$ ($\nu=0,1,\dots,n-1$) の成り立つことかわかるので、Prop. 1.1. により $LC(K_{\nu+1}, P)$ の成立が示され

る。これで prop. が証明された。

Corollary 2.4. K/k は f^n 次巡回拡大 ($n \in \mathbb{N}$) とする。

$n=1$ のとき P は f を法として原始根、 $n \geq 2$ のときは f^2 を法として原始根であるとする。 k は $\mathbb{Q}$ 、または、虚 2 次体であり $P \neq 3$ 、と仮定する。このとき $LC(K, P)$ が成り立つ。

証明 K_ν ($\nu=0, 1, \dots, n$) を prop. と同様とする。今の場合、 $LC(K, P)$ と $A(K_\nu, P)$ の成立は明らか。よって、すべての $\nu=1, \dots, n$ に対して、 $\text{rank } M_{K_\nu}^{(m)} < f^\nu(1-f^{-1})$ となる $m \in \mathbb{N}$ の存在を示せば十分である。以下、帰納法で示す。
 $\nu=1$ のとき、 $\mathbb{Z}\text{-rank } E_{K_1}(P^i) = f-1$ 、がすべての $i \in \mathbb{N}$ について成立するので、Lemma 2.1. により、 $\text{rank } M_{K_1}^{(\mu_1)} < f-1 = f(1-f^{-1})$ となる $\mu_1 \in \mathbb{N}$ の存在がわかる。

次に、 $1 \leq \nu \leq n-1$ に対して、 $\mu_\nu \in \mathbb{N}$ があり、すべての $i=1, \dots, \nu$ に対して $\text{rank } M_{K_i}^{(\mu_\nu)} < f^i(1-f^{-1})$ 、となつたと仮定する。 μ_ν を m と見ることにより、 $LC(K_\nu, P)$ の成立が prop. によってわかる。この事と Lemma 2.2. により、ある $\lambda_1 \in \mathbb{N}$ が存在して

$$M_{K_{\nu+1}}^{(\lambda_1)} = (E_{K_{\nu+1}}(P^{\lambda_1}) \cap E'_{K_{\nu+1}/K}) K_{\nu+1}^P / K_{\nu+1}^P$$

となることがわかる。Lemma 2.1. の証明と同様の議論により

ある自然数 $\lambda_2 (\geq \lambda_1)$ が存在して.

$$\text{rank}((E_{K_{\nu+1}}(p^{\lambda_2}) \cap E'_{K_{\nu+1}}/K) K_{\nu+1}^P / K_{\nu+1}^P) \\ < \mathbb{Z}\text{-rank}(E_{K_{\nu+1}}(p^{\lambda_2}) \cap E'_{K_{\nu+1}}/K), \text{ となる.}$$

一方, $\mathbb{Z}\text{-rank}(E_{K_{\nu+1}}(p^{\lambda_2}) \cap E'_{K_{\nu+1}}/K) = q^{\nu+1}(1-q^{-1})$ であるから,

$$\text{rank}((E_{K_{\nu+1}}(p^{\lambda_2}) \cap E'_{K_{\nu+1}}/K) K_{\nu+1}^P / K_{\nu+1}^P) < q^{\nu+1}(1-q^{-1}).$$

$\mu_{\nu+1} = \max\{\mu_{\nu}, \lambda_2\}$ とすれば,

$$\text{rank } M_{K_i}^{(\mu_{\nu+1})} < q^i(1-q^{-1}), \quad \forall i \in \{1, \dots, \nu+1\}$$

となる. 帰納法により, 上記の m の存在が示され, corollary が証明された.

3. K/k が abel 拡大の場合

K/k を n 次 ($n \in \mathbb{N}$) abel 拡大であるとする. K/k の中間体 M に対して, 相対単数群を, 通常のように

$$E_{M/K} = \{u \in E_M \mid M/k \text{ の任意の中間体 } F \neq M \text{ に於て } N_{M/F} u \in W_F\}$$

と定める. 但し, W_F は F の中の 1 の n 根全体の集合である. Ω によつて, K/k の巡回中間体全ての集合を表せば, 尾台 [5] により次がなり立つ;

$$(E_K/W_K)^n \subset \prod_{M \in \Omega} (E_{M/K} W_K / W_K).$$

従つて特に,

$$E_K^n \subset \left(\prod_{M \in \Omega} E_{M/K} \right) W_K, \text{ となる.}$$

Lemma 3.1. K/k は有限次 abel 拡大で、 $K \not\subset \mathbb{Q}_p$ とする。すべての $M \in \Omega$ に於て $LC(M, p)$ が成り立てば、 $LC(K, p)$ が成立する。

証明 $[K:k] = p^b n$, b は負でない整数、 $n \in \mathbb{N}$ は p と素とする。 $\forall a \in \mathbb{N}$ に対して、仮定により、ある $m \in \mathbb{N}$ が存在して、 $E_M(p^m) \subset E_M^{pa+b}$, $\forall M \in \Omega$, となる。 $E_K(p^m) \ni \forall \alpha$ に対して、上に述べたことから、各 $M \in \Omega$ に対する $u_M \in E_{M/K}$ と $\xi \in W_K$ が存在して、次が成り立つ；

$$\alpha^{p^b n} = \xi \cdot \prod_{M \in \Omega} u_M \quad (2)$$

K/k が巡回拡大ならば lemma の成立は明らかだから、巡回拡大ではないと仮定する。 Ω の部分集合 Ω_i ($i=0, 1, \dots$) を

$\Omega_i = \{M \in \Omega \mid [M:k] \text{ は } i \text{ 個の素数の積} \}$, ($i \in \mathbb{N}$), $\Omega_0 = \{k\}$ により、定義する。十分大きな i に対しては、 $\Omega_i = \emptyset$ (空集合) であり、 $\Omega = \bigcup_{i \geq 0} \Omega_i$ (disjoint union), となる。

$N_{K/K} \alpha^{p^b n} = N_{K/K} \xi \cdot N_{K/K} u_k \cdot \prod_{M \in \Omega} N_{K/K} u_M$. ここで、 m のとり方より、 $N_{K/K} \alpha^{p^b n} \in E_K^{pa+2b}$, $K \not\subset \mathbb{Q}_p$ であることから $N_{K/K} \xi \in W_K = W_K^{pa+2b}$. $N_{K/K} u_k = u_k^{p^b n}$, $\prod_{M \in \Omega} N_{K/K} u_M \in W_K = W_K^{pa+2b}$. 従って、 $u_k^{p^b n} \in E_K^{pa+2b}$. 則ち、 $u_k \in E_K^{pa+b}$

となる。

今、すべての $M \in \Omega_0 \cup \Omega_1 \cup \dots \cup \Omega_{\nu-1}$ (但し $M_\nu \neq \emptyset$) に対して、 $\mathcal{U}_M \in E_M^{pa+b}$ であると仮定する。任意の $M_\nu \in \Omega_\nu$ に対して、 $A = \{M \in \Omega \mid M_\nu \supset M \supset k\}$, $B = \{M \in A \mid M \neq M_\nu\}$ とする。 $A = \{M_\nu\} \cup B$, $B \subset \Omega_0 \cup \Omega_1 \cup \dots \cup \Omega_{\nu-1}$ である。

(2) より次を得る；

$N_{K_{M_\nu}} \alpha^{pbn} = N_{K_{M_\nu}} \xi \cdot N_{K_{M_\nu}} \mathcal{U}_{M_\nu} \cdot \prod_{M \in B} N_{K_{M_\nu}} \mathcal{U}_M \cdot \prod_{M \in \Omega \setminus A} N_{K_{M_\nu}} \mathcal{U}_M$.
 m のとり方より、 $N_{K_{M_\nu}} \alpha^{pbn} \in E_{M_\nu}^{pa+2b}$, が成り立つ。 ν に関する仮定より、

$$\prod_{M \in B} N_{K_{M_\nu}} \mathcal{U}_M = \prod_{M \in B} \mathcal{U}_M^{[k: M_\nu]} \in E_{M_\nu}^{pa+b[k: M_\nu]}.$$

また、 $N_{K_{M_\nu}} \mathcal{U}_{M_\nu} = \mathcal{U}_{M_\nu}^{[k: M_\nu]}$. $\forall M \in \Omega \setminus A$ に於て $N_{K_{M_\nu}} \mathcal{U}_M \in W_{M_\nu} = W_{M_\nu}^{pa+2b}$. 従って、 $\mathcal{U}_{M_\nu}^{p^c} \in E_{M_\nu}^{pa+b+c}$, 但し整数 c ($\leq b$) は $p^c \parallel [k: M_\nu]$ なるものとする。よって、 $\mathcal{U}_{M_\nu} \in E_{M_\nu}^{pa+b}$ となり、帰納法により、任意の $M \in \Omega$ に於て $\mathcal{U}_M \in E_M^{pa+b}$ の成立が示された。故に、再び(2)より、 $\alpha^{pbn} \in E_K^{pa+b}$. 則ち $\alpha \in E_K^{pa}$ となり、 $E_K(p^m) \subset E_K^{pa}$ となることが示された。よって $LC(K, p)$ が成り立つ。

この lemma と Prop. 2.3. より次を得る；

Theorem 3.2. ℓ は奇素数、 K_ℓ は ℓ -中次 abel 拡大、 $\zeta_p \notin$

K , 且 $\text{Gal}(K/k)$ の exponent は f^e ($e \in \mathbb{N}$) とする. $e=1$ ならば P は f を法として原始根, $e \geq 2$ ならば f^2 を法として原始根であり, P の上でのどの prime も $K(\zeta_P)/K$ で完全分解しない, と仮定する. $\text{LC}(K, P)$ の成立を仮定し, 更に, ある $m \in \mathbb{N}$ があって, すべての $M \in \Omega$ に対して次がなり立つとする;

$$\text{rank } M_M^{(m)} < [M:k](1-f^{-1}).$$

このとき, $\text{LC}(K, P)$ が成り立つ.

証明 各 $M \in \Omega$ に於て, $d \in \mathbb{N}$ ($d \leq e$) があって, M/k は f^d 次巡回拡大となり, P は f^d を法として原始根である. よって, Prop. 2.3. により, $\text{LC}(M, P)$ の成立がわかり, Lemma 3.1. により定理の成立がわかる.

Corollary 3.3. f は奇素数, K/k は f -巾次 abel 拡大, f^e ($e \in \mathbb{N}$) は $\text{Gal}(K/k)$ の exponent とする. $e=1$ ならば P は f を法として原始根, $e \geq 2$ ならば f^2 を法として原始根であるとし, k は $\mathbb{Q}$, または, 虚 2 次体であって $P \nmid 3$, とする. このとき, $\text{LC}(K, P)$ が成り立つ.

証明 $K \nmid \zeta_P$ であることは P に関する仮定よりわかる.

Cor. 2.4. より, 任意の $M \in \Omega$ について $\text{LC}(M, P)$ の成立がわ

かるので、Lemma 3.1. により主張がみちびかれる。

4. ひとつの lemma とその応用

$k(\zeta_p)$ の prime で、 p をわるもの全体の集合を S とし、 $k(\zeta_p)$ の S -ideal 類群 (S の要素を含む類が生成する部分群で "ideal 類群をわったもの") を $C(k)$, $C(k)/C(k)^p$ を ${}_p C(k)$ で表す。 p -進整数環を $\mathbb{Z}_p$ とし、 $\Delta = \text{Gal}(k(\zeta_p)/k)$ から $\mathbb{Z}_p^\times$ への指標 ω を、 $\zeta_p^\sigma = \zeta_p^{\omega(\sigma)}$, $\forall \sigma \in \Delta$, によって定義する。

${}_p C(k)$ は $\mathbb{Z}_p[\Delta]$ -加群とみなすことができる。

$$\varepsilon_i = \frac{1}{|\Delta|} \sum_{\sigma \in \Delta} \omega^i(\sigma) \sigma^{-1} \in \mathbb{Z}_p[\Delta], \quad i = 1, \dots, |\Delta|,$$

とおくと、 $\sigma \varepsilon_i = \omega^i(\sigma) \varepsilon_i$, $\forall \sigma \in \Delta$, が成り立つ。

Lemma 4.1. K/k は q 次拡大で、 $(p, q) = 1$ であり、 $A(K, p)$ が成り立つとする。ある $m \in \mathbb{N}$ が存在して、 $E_k(p^m) \subset kK^p$ となり、更に、 $LC(k, p)$ が成り立つと仮定する。このとき、 $LC(K, p)$ が成り立つ。

証明 仮定により、 $m \in \mathbb{N}$ に於て、 $E_k(p^m) \subset kK^p$ 、且、 $E_k(p^m) \subset E_k^p$ となる、としてよい。各 $u \in E_k(p^m)$ に対して、 $a \in k$ と $\beta \in K$ があって、 $u = a \beta^p$ となる。

$N_{K/k} u = a^g (N_{K/k} \beta)^p \in a^g k^p$. ここで、 $N_{K/k} u \in E_K(p^\infty) \subset E_k^p$. だから $a^g \in k^p$. 則ち、 $a \in k^p$ となる. 従って、 $u \in K^p$ となり、 $LC(K, p)$ が成り立つ.

この lemma を用いて、Sands [6] の Theorem 4.8. のひとつの一般化を得ることが出来る;

Theorem 4.2. K/k は g 次拡大で、 $(p, g) = 1$ であり、 $A(K, p)$ が成り立ち、 $K \cap k(\zeta_p) = k$ となるものとする. $\text{Gal}(K(\zeta_p)/k)$ と Δ を同一視したとき、 $\varepsilon_1(pC(k)) \cong \varepsilon_1(pC(K))$ が成り立つと仮定する. このとき、更に、 $LC(k, p)$ が成り立てば、 $LC(K, p)$ が成り立つ.

証明 一般に、 $(p, g) = 1$ のとき、 $\varepsilon_1(pC(k))$ は $\varepsilon_1(pC(K))$ の部分群に同型である. 類体論により、 $C(k)$ (及び $C(K)$) は、 $k(\zeta_p)$ (及び $K(\zeta_p)$) の、 p の上のすべての prime が完全分解するような最大不分岐 abel 拡大に対応し、 $pC(k)$ (及び $pC(K)$) は、そのような拡大の中の最大基本 p -拡大に対応している. ideal 類群についての仮定により、すべての、 $K(\zeta_p)$ の不分岐 p 次巡回拡大で、 p の上のすべての prime が完全分解し、(その $K(\zeta_p)$ 上の Galois 群への) $\sigma \in \Delta$ の作用

が ω によるものと一致するようなものは、 $k(\zeta_p)$ 上のそのような拡大と $K(\zeta_p)$ との合成によって得られる。

Kummer理論により、ある $m \in \mathbb{N}$ をとれば、任意の $u \in E_k(p^m)$ に対して、 $K(\zeta_p, u^{\frac{1}{p}})$ は $\mathcal{E}_1(pC(k))$ のある剰余群に対応する。よって、仮定により、任意の $u \in E_k(p^m)$ に対して、 $k(\zeta_p)$ のある p 次巡回拡大 M が存在して、 $K(\zeta_p, u^{\frac{1}{p}}) = k(\zeta_p)M$ となる。 M は $\mathcal{E}_1(pC(k))$ に対応するから、 $M = k(\zeta_p, a^{\frac{1}{p}})$ となる $a \in k$ がとれる。このとき、 $K(\zeta_p, u^{\frac{1}{p}}) = K(\zeta_p, a^{\frac{1}{p}})$ だから、 $u = a^i \beta_0^p$ となる自然数 i ($1 \leq i \leq p-1$)と、 $\beta_0 \in K(\zeta_p)$ がとれる。 $d = |\Delta|$ は p と素だから、 $\alpha d + \gamma p = 1$ となる $\alpha, \gamma \in \mathbb{Z}$ がある。

$$\begin{aligned} u &= u^{\alpha d} \times u^{\gamma p} = (N_{K(\zeta_p)/k} u)^{\alpha} \times u^{\gamma p} = a^{di} ((N_{K(\zeta_p)/k} \beta_0)^p)^{\alpha} u^{\gamma p} \\ &= a^{di\alpha} (N_{K(\zeta_p)/k} \beta_0)^{p\alpha} u^{\gamma p} \in kK^p. \end{aligned}$$

従って、 $E_k(p^m) \subset kK^p$ となり、Lemma 4.1. により $LC(k, p)$ の成立がわかる。

補足(蛇足) Cor. 3.3. はもちろん、Brumer[1]の定理の特殊な場合の“純代数的”な別証明である。

補足2 三木博雄教授より、Lemma 3.1. と Cor. 3.3 は、1982年12月の東大代数コロキウム及び1983年10月のシンポジウムでの御自身のお話(unpublished)の中に含まれている、との連絡を頂きました(92.3.3)。

References

- [1] A. Brumer, On the units of algebraic number fields, *MATHEMATIKA*, 14 (1967), 121—124.
- [2] K. Iwasawa, On Leopoldt's conjecture (in Japanese), *Seminar Note on Algebraic Number Theory*, 数理解研 (1984), 45—53.
- [3] H. Miki, On the Leopoldt conjecture on the p -adic regulators, *J. Number Theory*, 26 (1987), 117—128.
- [4] H. Miki and H. Sato, Leopoldt's conjecture and Reiner's theorem, *J. Math. Soc. Japan*, 36 (1984), 47—51.
- [5] Y. Odai, On the group of units of an abelian extension of an algebraic number field, *Proc. Japan Acad. Ser. A* 64 (1988), 304—306.
- [6] J. W. Sands, Kummer's and Iwasawa's version of Leopoldt's conjecture, *Canad. Math. Bull.* 31 (1988), 338—346.
- [7] H. Yamashita, Remarks on connections between the Leopoldt conjecture, p -class groups and unit groups of algebraic number fields, *J. Math. Soc. Japan*, 42 (1990), 221—237.