数理解析研究所講究録
797巻 1992年 1-16

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、$E_k(p^m)=\{u\in E_k \mid u\equiv 1 \mod p^m\}$，$m$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]）.

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

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.

<u>Proposition 1.1.</u> 次の2つのうちのひとつを仮定する;

(1) $k \not\ni \zeta_p$ 且. pをわるどのprimeも$k(\zeta_p)/k$で完全分解しない,

(2) $k \ni \zeta_p$ 且. pをわるkのprimeはただひとつ.

このとき次がなり立つ;

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

<u>証明.</u> 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) $a=1$の場合に示せば十分, と言うことである. 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.

<u>Proposition 1.2.</u> $g \in \mathbb{N}$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. $G = Gal(K/k)$ 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，$M_K^{(m)} = E_K(p^m)K^p/K^p \subset K^\times/K^p$とする．但し，$K^p$は$(K^\times)^p$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$1 \leqq l_\tau \leqq p-1$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．$H_\alpha$が$G$の正規部分群であり，$G/H_\alpha$が$(\mathbb{Z}/p\mathbb{Z})^\times$（$\mathbb{Z}$は有理整数環）の部分群に同型であることは，$\tau$に上記$l_\tau$を対応させることにより，直ちにわかる．従って，$H_\alpha$の指数は$p-1$の約数であり，$H_\alpha$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-巾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．

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

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

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

<u>証明</u> $E_F(p)$ が torsion free であることは明らか．ある $m \in \mathbb{N}$ をとれば，$E_F(p^{m-1}) \supsetneqq E_F(p^m)$ 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 $\{u_1, \cdots, u_r\}$ $(r = \mathbb{Z}\text{-rank}\, E_F)$ で，次の2つをみたすものが存在する：

(i) $\{u_1^{e_1}, \cdots, u_r^{e_r}\}$ は $E_F(p^m)$ の $\mathbb{Z}$-basis．但し，$e_i \in \mathbb{N}$．

(ii) $e_i | e_{i+1}$，$i = 1, \cdots, r-1$，且 $e_1 \cdot \cdots \cdot e_r = p^e$.

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

<u>Lemma 2.2.</u> K/k は次数が p と素な abel 拡大とする。$E'_{K/k} = \{ u \in E_K \mid$ 任意の K/k の中間体 $M \neq K$ 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；

$$M_K^{(m)} = (E_K(p^m) \cap E'_{K/k}) K^p / K^p.$$

<u>証明</u>　$\Phi = \{M_i\}$ 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。$[K:M_1] = \ell_1$ とおく。$x_1 p - y_1 \ell_1 = 1$ となる整数 x_1, y_1, をとる。

$$N_{K/M_1}(\alpha_0^{1-x_1 p} v_1^{y_1 p}) = v_1^{p(1-x_1 p) + y_1 p \ell_1} = v_1^{p(1-x_1 p + y_1 \ell_1)} = 1.$$

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、$N_{K/M_1} \alpha_i = N_{K/M_2} \alpha_i = \cdots = N_{K/M_i} \alpha_i = 1$, $\overline{\alpha_0} = \overline{\alpha_i} \in M_K^{(m)}$ 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．$[K:M_{i+1}] = q_{i+1}$ は p と異なる素数だから，$xp - yq_{i+1} = 1$ となる整数 x，y がある．$\alpha_{i+1} = \alpha_i^{1-xp} v_{i+1}^{yp}$ とおけば，$\alpha_{i+1} \in E_K(p^m)$，$N_{K/M_{i+1}}\alpha_{i+1} = 1$，且 $\bar{\alpha}_0 = \bar{\alpha}_{i+1} \in M_K^{(m)}$ であることは直ちにわかる．更に，任意の j $(1 \leqq j \leqq i)$ に対して，$N_{K/M_j}\alpha_{i+1} = N_{K/M_j}(\alpha_i^{1-xp} v_{i+1}^{yp}) = N_{K/M_j} v_{i+1}^{yp} = N_{K/M_j}(N_{K/M_{i+1}}\alpha_i^{y}) = N_{K/M_{i+1}}(N_{K/M_j}\alpha_i^{y}) = 1$．帰納法により，$\bar{\alpha}_0 = \bar{\alpha}$，且，すべての i について $N_{K/M_i}\alpha = 1$，となる α の存在が示された．K/k の任意の中間体 $M \neq K$ は，ある $M_i \in \mathfrak{M}$ 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．

<u>Proposition 2.3.</u> 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．$n \geqq 2$ 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 $(\nu = 1, \cdots, n)$ 次中間体 K_ν に対して

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

が成立する，と仮定する．このとき，$LC(K,p)$ が成立する．

<u>証明</u>　$\nu=0$に対しては$K_0=k$とし、$\nu=0,1,\cdots,n$に関する帰納法によって証明する．まず、仮定により$LC(K_0,P)$はなり立つ．次に、ν（$0\leqq\nu\leqq n-1$）において$LC(K_\nu,P)$の成立を仮定する．$Gal(K_{\nu+1}/k)=\langle\tau\rangle$とする．すべての$i\in\mathbb{N}$について、$\tau$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

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

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、$\tau$の最小多項式は定数ではなく、多項式

$$\mathbb{F}_p[X]\ni X^{\ell^\nu(\ell-1)}+X^{\ell^\nu(\ell-2)}+\cdots+X^{\ell^\nu}+1 \qquad (1)$$

の約数である．

一般に、自然数rがℓ^2を法として原始根ならば、任意の$e\geqq 3$（$e\in\mathbb{N}$）について、rはℓ^eを法として原始根である．よって、仮定により、pは$\ell^{\nu+1}$を法として原始根．また、このとき多項式(1)は($\mathbb{F}_p$上)既約である．従って、$\mathrm{rank}\,M_{K_{\nu+1}}^{(\mu)}\geqq\ell^\nu(\ell-1)=\ell^{\nu+1}(1-\ell^{-1})$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、$E_{K_{\nu+1}}(p^i)\subset K_{\nu+1}^p$となることがわかる．一方、$A(K,P)$の成立と$P$に関する仮定より、$A(K_\nu,P)$（$\nu=0,1,\cdots,n-1$）の成り立つことがわかるので，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．

<u>Corollary 2.4.</u> K/k は ℓ^n 次巡回拡大（$n \in \mathbb{N}$）とする．$n=1$ のとき p は ℓ を法として原始根、$n \geqq 2$ のときは ℓ^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．

<u>証明</u> K_ν（$\nu = 0, 1, \cdots, n$）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 $\nu = 1, \cdots, n$ に対して、$\mathrm{rank}\, M_{K_\nu}^{(m)} < \ell^\nu(1-\ell^{-1})$ 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．$\mathbb{Z}$-$\mathrm{rank}\, E_{K_1}(p^i) = \ell - 1$，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．$\mathrm{rank}\, M_{K_1}^{(\mu_1)} < \ell - 1 = \ell(1-\ell^{-1})$ となる $\mu_1 \in \mathbb{N}$ の存在がわかる．

次に、$1 \leqq \nu \leqq n-1$ に対して、$\mu_\nu \in \mathbb{N}$ があり、すべての $i = 1, \cdots, \nu$ に対して $\mathrm{rank}\, M_{K_i}^{(\mu_\nu)} < \ell^i(1-\ell^{-1})$、となったと仮定する．$\mu_\nu$ 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λ_2（$\geqq\lambda_1$）が存在して、

$$\mathrm{rank}((E_{K_{\nu+1}}(p^{\lambda_2})\cap E'_{K_{\nu+1}/k})K_{\nu+1}^{p}/K_{\nu+1}^{p})$$

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

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

$$\mathrm{rank}((E_{K_{\nu+1}}(p^{\lambda_2})\cap E'_{K_{\nu+1}/k})K_{\nu+1}^{p}/K_{\nu+1}^{p})<g^{\nu+1}(1-g^{-1}).$$

$\mu_{\nu+1}=\mathrm{Max}\{\mu_\nu,\lambda_2\}$とすれば、

$$\mathrm{rank}\,M_{K_i}^{(\mu_{\nu+1})}<g^{i}(1-g^{-1}),\quad \forall i\in\{1,\cdots,\nu+1\}$$

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

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

と定める。但し、W_FはFの中の1の巾根全体の集合である。Ωによって、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；

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

従って特に、

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

Lemma 3.1. K/kは有限次abel拡大で、$K \not\ni \zeta_p$、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、$E_M(p^m)\subset E_M^{p^{a+b}}$，$\forall M\in\Omega$，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、次がなり立つ；

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

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 $(i=0,1,\cdots)$を

$\Omega_i=\{M\in\Omega \mid [M:k]$は$i$個の素数の積$\}$，$(i\in\mathbb{N})$，$\Omega_0=\{k\}$

によって定義する．十分大きなiに対しては、$\Omega_i=\phi$（空集合）であり、$\Omega=\bigcup_{i\geq 0}\Omega_i$ (disjoint union)，となる．

$N_{K/k}\alpha^{p^b n}=N_{K/k}\xi\cdot N_{K/k}u_k\cdot\prod_{k\neq M\in\Omega}N_{K/k}u_M$． ここで、$m$のとり方より、$N_{K/k}\alpha^{p^b n}\in E_k^{p^{a+2b}}$． $K\not\ni\zeta_p$であることから$N_{K/k}\xi\in W_k=W_k^{p^{a+2b}}$． $N_{K/k}u_k=u_k^{p^b n}$，$\prod_{k\neq M\in\Omega}N_{K/k}u_M\in W_k=W_k^{p^{a+2b}}$．従って、$u_k^{p^b n}\in E_k^{p^{a+2b}}$、則ち、$u_k\in E_k^{p^{a+b}}$

となる．

今，すべての$M\in\Omega_0\cup\Omega_1\cup\cdots\cup\Omega_{\nu-1}$（但し．$M_\nu\neq\phi$）に対して，$u_M\in E_M^{p^{a+b}}$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．$A=\{M_\nu\}\cup B$，$B\subset\Omega_0\cup\Omega_1\cup\cdots\cup\Omega_{\nu-1}$である．

(2)より次を得る；

$$N_{K/M_\nu}\alpha^{p^b n}=N_{K/M_\nu}\xi\cdot N_{K/M_\nu}u_{M_\nu}\cdot\prod_{M\in B}N_{K/M_\nu}u_M\cdot\prod_{M\in\Omega\setminus A}N_{K/M_\nu}u_M.$$

mのとり方より，$N_{K/M_\nu}\alpha^{p^b n}\in E_{M_\nu}^{p^{a+2b}}$，がなり立つ．$\nu$に関する仮定より，

$$\prod_{M\in B}N_{K/M_\nu}u_M=\prod_{M\in B}u_M^{[K:M_\nu]}\in E_{M_\nu}^{p^{a+b}[K:M_\nu]}.$$

また，$N_{K/M_\nu}u_{M_\nu}=u_{M_\nu}^{[K:M_\nu]}$．$^\forall M\in\Omega\setminus A$に於て$N_{K/M_\nu}u_M\in W_{M_\nu}=W_{M_\nu}^{p^{a+2b}}$．従って，$u_{M_\nu}^{p^c}\in E_{M_\nu}^{p^{a+b+c}}$，但し整数$c$（$\leqq b$）は$p^c\,\|\,[K:M_\nu]$なるものとする．よって，$u_{M_\nu}\in E_{M_\nu}^{p^{a+b}}$となり，帰納法により，任意の$M\in\Omega$に於て$u_M\in E_M^{p^{a+b}}$の成立が示された．故に，再び(2)より，$\alpha^{p^b n}\in E_K^{p^{a+b}}$，則ち$\alpha\in E_K^{p^a}$となり，$E_K(p^m)\subset E_K^{p^a}$となることが示された．よって$LC(K,p)$がなり立つ．

このlemmaとProp. 2.3. より次を得る；

<u>Theorem 3.2.</u>　pは奇素数，K/kはp-巾次abel拡大，$\zeta_p\notin$

K，且 $Gal(K/k)$ の exponent は ℓ^e $(e\in\mathbb{N})$ とする．$e=1$ ならば p は ℓ を法として原始根、$e\geq 2$ ならば ℓ^2 を法として原始根であり、p の上のどの prime も $K(\zeta_p)/K$ で完全分解しない、と仮定する．$LC(k,p)$ 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；

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

このとき、$LC(K,p)$ が成り立つ．

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

<u>Corollary 3.3.</u>　ℓ は奇素数、K/k は ℓ-巾次 abel 拡大、ℓ^e $(e\in\mathbb{N})$ は $Gal(K/k)$ の exponent とする．$e=1$ ならば p は ℓ を法として原始根、$e\geq 2$ ならば ℓ^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 $p\neq 3$，とする．このとき、$LC(K,p)$ が成り立つ．

<u>証明</u>　$K\not\ni\zeta_p$ 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 $LC(M,p)$ 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 ${}_pC(k)$ で表す。p-進整数環を $\mathbb{Z}_p$ とし、$\Delta = Gal(k(\zeta_p)/k)$ 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。${}_pC(k)$ は $\mathbb{Z}_p[\Delta]$-加群とみなすことができる。

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

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

<u>Lemma 4.1.</u> K/k は g 次拡大で、$(p, g) = 1$ 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、$LC(k, p)$ が成立すると仮定する。このとき、$LC(K, p)$ が成り立つ。

<u>証明</u> 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、$N_{K/k}u \in E_k(p^m) \subset E_k^p$、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できる；

<u>Theorem 4.2.</u> 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。$Gal(K(\zeta_p)/k)$ 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。

<u>証明</u> 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ー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$\varepsilon_1(_pC(K))$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$\varepsilon_1(_pC(k))$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、$xd + yp = 1$となる$x, y \in \mathbb{Z}$がある.

$$u = u^{xd} \times u^{yp} = (N_{K(\zeta_p)/k}\, u)^x \times u^{yp} = a^{di}((N_{K(\zeta_p)/k}\, \beta_0)^p)^x u^{yp}$$
$$= a^{dix}(N_{K(\zeta_p)/k}\beta_0)^{px} u^{yp} \in kK^p.$$

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.

<u>補足</u>(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.

<u>補足2</u> 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.