数理解析研究所講究録
925巻 1995年 166-177

$\mathbf{Z}_p$拡大のKummer生成元について

東京外語大　佐藤宏孝 (Hirotaka Sato)

§1. 序

pを素数、$\mathbf{Z}_p$をp進整数環とする。また、$n\in\mathbf{Z}$に対して、

$$\xi_n = \exp(2\pi i/n)\in\mathbf{C}$$

とする。

$\xi_n\in K$なる有限次代数体 K に対して、$\mathbf{Z}_p$拡大の1-st layerのKummer生成元を求める問題は、20年程前から研究されている。

[2][3][5]は、主として、K が虚2次体で p = 2 の場合について具体的な結果を得た。また、[6][7][8][9]は、一般の K に対して、その単数群とイデアル類群から計算するアルゴリズムを示した。

一方、[1]は(K,p)に関するLeopoldt予想：

$$\mathrm{rank}_{\mathbf{Z}_p}\mathrm{Gal}(K_{\mathbf{Z}_p}/K) = r_2 + 1$$

($K_{\mathbf{Z}_p}$はKの$\mathbf{Z}_p$拡大すべての合成体、r_2はKのcomplex primesの個数とする)

を調べるために、Kの$\mathbf{Z}_p$拡大を具体的に構成する方法をとった。

我々は、[1]の方法を出発点にして、ある種の有限次abel体Kの$\mathbf{Z}_p$拡大をなるべく多く、具体的な生成元を示して構成したい。

Vandiver予想が正しいような素数pに対して、K = p分体の場合は $K_{\mathbb{Z}_p}$ の生成元を与えることができる（§2 命題2）。

しかし、一般のK（これにも条件がつくが）の場合には、(p+1)/2個の独立な$\mathbb{Z}_p$拡大を得るにとどまる（§3 定理）。

最後に、K = $\mathbb{Q}(\sqrt{-1}, \sqrt{-m})$ （mはsqure freeの正整数）、p = 2 の場合にその non-cyclotomic $\mathbb{Z}_p$拡大の 1-st layer の Kummer生成元を具体的に計算してみる（§4）。

§2. q分体の場合

$$q = \begin{cases} p & p > 2 \\ 4 & p = 2 \end{cases}$$ とし、$\mathbb{Q}[n] = \mathbb{Q}(\zeta_n)$をn分体とする($n \in \mathbb{Z}$)。

この§では、$K = \mathbb{Q}[q]$とする。

$K_n = \mathbb{Q}[qp^n]$ (n=0,1,2,･･･)、$K_\infty = \bigcup_{n=0}^{\infty} K_n$とすれば、$K_\infty$はKの cyclotomic $\mathbb{Z}_p$拡大である。

$\mathrm{Gal}(K_\infty/K)$ の位相的生成元τを

$$\zeta_{qp^n}{}^{\tau} = \zeta_{qp^n}{}^{1+q} \quad (n=0,1,2,\cdots)$$

で定義する。簡単のために、τのK_nへの制限もτで表す。

次の補題1はよく知られている。

補題1

$\alpha \in K_n^\times$に対し、

$$K_n(\sqrt[qp^n]{\alpha})/K : \text{abelian} \iff \alpha^{\tau-1-q} \in (K_n^{\times})^{qp^n}$$

多項式 $f_n(x) \in \mathbf{Z}[x]$ $(n=0,1,2,\cdots)$ を次の補題 2 で定義する。

補題 2 ([1])

$f_n(x) \in \mathbf{Z}[x]$ $(n=0,1,2,\cdots)$ と $R_n \in \mathbf{Z}$ を

$$1 + X + X^2 + \cdots\cdots + X^{p^n-1} = (X - 1 - q) \cdot f_n(x) + R_n$$

で定める。

そのとき、$p^n \mid R_n$ である。

証明

$R_n = \{(1+q)^{p^n}-1\}/q$ である。$1+q \bmod qp^n$ は、$(\mathbf{Z}/qp^n\mathbf{Z})^{\times}$ の中で、位数 p^n であるから、$R_n \equiv 0 \bmod p^n$ となる。□

注意 $f_0(x) = 0$ である。

次の条件を満たす数列 $\{\pi_n\}$ を考える：

$$\pi_n \in K_n \quad , \quad N_{K_{n+1}/K_n}(\pi_{n+1}) = \pi_n \qquad (n = 0,1,2,\cdots\cdot)$$

[1] に従って、数列 $\{\pi_n\}$ から、数列 $\{\alpha_n\}$ を次のように作る：

$$\alpha_n = \pi_0 \, \pi_n^{q f_n(\tau)} \in K_n \qquad (n = 0,1,2,\cdots\cdot)$$

$\alpha_0 = \pi_0$ である。

$$L_n = K_n(\sqrt[qp^n]{\alpha_n}) \qquad (n = 0,1,2,\cdots\cdot)$$

とすれば、次の命題が成り立つ。

命題 1 ([1])

上の記号のもとで、

(1) L_n / Kは abelian である。

(2) $L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_n \subset \cdots$

証明

(1) : $f_n(x)$ の定義から $\alpha_n^{\tau-1-q}$ を計算することによって、$\alpha_n^{\tau-1-q} \in K_n^{\times qp^n}$ を示すことができる。補題 1 よりL_n / Kは abelian である。

(2) : 同様の計算から、$\alpha_{n+1}/\alpha_n \in K_{n+1}^{\times qp^n}$ がわかり、

$$K_{n+1}(\sqrt[qp^n]{\alpha_n}) = K_{n+1}(\sqrt[qp^n]{\alpha_{n+1}})$$

よって、 $$L_n \subset K_{n+1}(\sqrt[qp^n]{\alpha_n}) = K_{n+1}(\sqrt[qp^n]{\alpha_{n+1}}) \subset L_{n+1} \quad \square$$

次の補題は難しいものではない。証明は、たとえば [10] にある。

補題 3

n と m は 1 より大きい整数で、$n \mid m$ かつ $n, m \not\equiv 2 \bmod 4$ とする。

素数 q に対して、$\sigma_q \in \mathrm{Gal}(\mathbb{Q}[n]/\mathbb{Q})$ を $\zeta_n \longmapsto \zeta_n^q$ で定義する (Frobenius automorphism)。

そのとき、$N_{\mathbb{Q}[m]/\mathbb{Q}[n]}(1-\zeta_m) = (1-\zeta_n)^{y(m,n)}$, $y(m,n) = \prod(1-\sigma_q^{-1})$ となる。ただし、$\prod$ は $q \mid m$ かつ $q \nmid n$ なる素数 q にわたる積とする。$q \mid m$ かつ$q \nmid n$ なる素数 q がない場合は、 $y(m,n) = 1$ とする。

さて、

$$\pi_n = 1 - \zeta_{qp^n} \in K_n^\times \qquad (n = 0,1,2,\cdots)$$

とおくと、補題３より

$$N_{K_{n+1}/K_n}(\pi_{n+1}) = \pi_n \qquad (n = 0,1,2,\cdots)$$

が満たされるから、

$$\alpha_n = \pi_0 \cdot \pi_n^{qf_n(\tau)} \in K_n, \quad L_n = K_n(\sqrt[qp^n]{\alpha_n}) \qquad (n = 0,1,2,\cdots)$$

とすれば、命題１より

L_n/K は abelian かつ $L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_n \subset \cdots$

となる。

$L_\infty = \bigcup_{n=0}^{\infty} L_n$ とする。

命題２

p は、素数で、 $p \nmid h(\mathbb{Q}[p]^+)$ ($h(\mathbb{Q}[p]^+)$は $\mathbb{Q}[p]$ の最大実部分体の類数 ）を満たすとする（つまり、p は Vandiver 予想が成り立つような素数）。

そのとき、

（１） L_∞/K は、$\mathbb{Z}_p^2$ 拡大である。

（２） Δを $Gal(K_\infty/\mathbb{Q})$ の torsion 部分群とする。Δは $p>2$ のとき（resp.p=2 のとき）、位数 p-1 の（resp.位数 2 の）巡回群である。$\sigma \in \Delta$に対して、 $L_n^\sigma = K_n(\sqrt[qp^n]{\alpha_n^\sigma})$, $L_\infty^\sigma = \bigcup_{n=0}^{\infty} L_n^\sigma$, $\widetilde{L_\infty} = \prod_{\sigma\in\Delta} L_\infty^\sigma$ とおく。そのとき、$\widetilde{L_\infty} = K_{\mathbb{Z}_p}$ である。

証明

（１）： $(1-\zeta_q)$ は K の素イデアルだから、$\alpha_0 = 1-\zeta_q \notin K^{\times p}$ よって

$[L_0 : K] = q$

また、$L_0 \cap K_\infty = K$ である。実際、$L_0 \cap K_\infty \neq K$ とすれば、

$$K(\sqrt[p]{1-\xi_q}) = K_1$$

であり、従って、$1-\xi_q = \xi_q^i \cdot x^p$ ($^\exists x \in K$, $^\exists i \in \mathbb{Z}$)と書ける。よって、$(1-\xi_q) = (x)^p$ だが、これは、$(1-\xi_q)$ が素イデアルであることに反する。

特に、$\alpha_0 \notin K_n^{\times p}$ であるから、$\alpha_n = \alpha_0 \cdot \pi_n^{q f_n(\tau)} \notin K_n^{\times p}$ であり、従って、

$[\ L_n : K_n\ ] = qp^n$

ゆえに、$\mathrm{Gal}(L_\infty/K_\infty) \simeq \mathbb{Z}_p$

L_∞/K は abelian だから、L_∞ は K の $\mathbb{Z}_p^2$ 拡大となる。

(2) : p = 2 のときは、$L_\infty = K_{\mathbb{Z}_p}$ となり明らか。 p >2 とする。C を、K の cyclotomic p-unit 群 (i.e. ξ_p と $\{1-\xi_p^\sigma : \sigma \in \Delta\}$ で生成される $K^\times$ の部分群) とする。また、E と H は、それぞれ K の単数群、円単数群とする。

M を $\widetilde{L_\infty}$ に含まれる K の最大 elementary abel p-拡大とする。$M = \prod_{\sigma \in \Delta} L_0^\sigma$ であるから、$\mathrm{Gal}(M/K) \simeq CK^p/K^p \simeq C/C \cap K^p$

ところで、仮定 $p \nmid h(\mathbb{Q}[p]^+)$ より $p \nmid (\ E : H\ )$ であるが、このことから、$C \cap K^p = C^p$ がわかる。実際、$\varepsilon^p \in C \cap K^p$ $(\varepsilon \in K)$とすると、ε は p-unit だから、$\varepsilon = (1-\xi_p)^a \eta$ $(a \in \mathbb{Z}$, $\eta \in E)$ と書ける。$\varepsilon^p = (1-\xi_p)^{ap} \eta^p \in C$ より、$\eta^p \in C \cap E = H$ であり、p 乗は E/H の automorphism だから、$\eta \in H$ となる。従って、$\varepsilon \in C$ となり、$C \cap K^p \subset C^p$ よって、$C \cap K^p = C^p$

ゆえに、$\mathrm{Gal}(M/K) \simeq C/C^p$

$\dim_{\mathbb{F}_p} C/C^p = (p+1)/2$ だから、$\mathrm{Gal}(\widetilde{L_\infty}/K) \simeq \mathbb{Z}_p^{\frac{p+1}{2}}$

(K,p) に関する Leopoldt 予想は正しいから、$\widetilde{L_\infty} = K_{\mathbb{Z}_p}$ □

§3．一般の場合

$m = \prod_{i=1}^{r} q_i^{e_i}$ ，各 q_i は素数で $\equiv 1 \bmod p$ ，e_i は正の整数

とする。

この§では、K は

$$Q[q] \subset K \subset Q[qm]$$

を満たす体とする。

§2と同様に、 $K_n = K(\zeta_{qp^n})$ $(n = 0,1,2,\cdots)$, $K_\infty = \bigcup_{n=0}^{\infty} K_n$ とし、

$Gal(K_\infty/K)$ の位相的生成元 τ を

$$\zeta_n{}^\tau = \zeta_n{}^{1+q} \qquad (n=0,1,2,\cdots)$$

で定める。

$$\pi_n = N_{Q[qp^n m]/K_n}(1-\zeta_{qp^n m}) \qquad (n = 0,1,2,\cdots)$$

とおくと、$\{\pi_n\}$ は $N_{K_{n+1}/K_n}(\pi_{n+1}) = \pi_n$ $(n = 0,1,2,\cdots)$ を満たすので、

$$\alpha_n = \pi_0 \cdot \pi_n{}^{qf_n(\tau)} \in K_n, \quad L_n = K_n(\sqrt[qp^n]{\alpha_n}) \qquad (n = 0,1,2,\cdots)$$

とおけば、命題1と同じ方法で

L_n/K は abelian かつ $L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_n \subset \cdots$

が証明できる。

また、

$$\pi^\circ_n = N_{K_n/Q[qp^n]}(\pi_n) = N_{Q[qp^n m]/Q[qp^n]}(1-\zeta_{qp^n m}) \in Q[qp^n] \quad (n = 0,1,2,\cdots)$$

とおく。

$\{\pi^\circ_n\}$ も $N_{Q[qp^{n+1}]/Q[qp^n]}(\pi^\circ_{n+1}) = \pi^\circ_n$ $(n = 0,1,2,\cdots)$ を満たすので、

$$\alpha^\circ_n = \pi^\circ_0 \cdot \pi^\circ_n{}^{qf_n(\tau)}, \quad L^\circ_n = Q[qp^n](\sqrt[qp^n]{\alpha^\circ_n}) \qquad (n = 0,1,2,\cdots)$$

とおくと、

L°_{n} /$\mathbb{Q}$[q] は abelian かつ $L^{\circ}_{0} \subset L^{\circ}_{1} \subset L^{\circ}_{2} \subset \cdots \subset L^{\circ}_{n} \subset \cdots$

である。$L^{\circ}_{\infty} = \bigcup_{n=0}^{\infty} L^{\circ}_{n}$ とおく。

$f_n(x)$ を具体的に表し、補題3を使ってα°_{n} を計算することによって次の補題4が得られる。

補題4

m のみによって定まる次のような自然数 N が存在する：

任意の $n \geqq N$ に対して

$\alpha^{\circ}_{n} = (1-\xi_q)^{p^N t} \cdot x^{qp^N}$ ただし、$t \in \mathbb{Z}$ は p と素 ，$x \in \mathbb{Q}[qp^n]$

定理

m ，K は上の条件を満たすものとし、また p は $p \nmid h(\mathbb{Q}[p]^+)$満たす素数とする。

そのとき、

（１）L_{∞}/K は $\mathbb{Z}_p^2$ 拡大である。

（２）p＞2 とする。$\mathrm{Gal}(\mathbb{Q}[p^{\infty}m]/\mathbb{Q})$ の torsion 部分群を $\mathrm{Gal}(\mathbb{Q}[qm]/\mathbb{Q})$と同一視し、$\mathrm{Gal}(\mathbb{Q}[qm]/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}[qm]/\mathbb{Q}[m]) \times \mathrm{Gal}(\mathbb{Q}[qm]/\mathbb{Q}[q])$ なる分解の第１成分 $\mathrm{Gal}(\mathbb{Q}[qm]/\mathbb{Q}[m]) = \Delta$ とおく（$\Delta \simeq \mathrm{Gal}(\mathbb{Q}[q]/\mathbb{Q})$ である）。Δを$\mathrm{Gal}(\mathbb{Q}[p^{\infty}m]/\mathbb{Q})$の部分群とみなし、また、$\sigma \in \Delta$ の K_nへの制限もσで表す。$\sigma \in \Delta$に対して、$L^{\sigma}_{n} = K_n(\sqrt[qp^n]{\alpha^{\sigma}_{n}})$，$L^{\sigma}_{\infty} = \bigcup_{n=0}^{\infty} L^{\sigma}_{n}$ ，$\widetilde{L_{\infty}} = \prod_{\sigma \in \Delta} L^{\sigma}_{\infty}$ とおく。そのとき、$\widetilde{L_{\infty}}$ は $\mathbb{Z}_p^{\frac{p+1}{2}}$ 拡大である。

証明

（１）∴ N を補題4で定義した整数とする。補題4より、

$$L_N^{\circ} = \mathbf{Q}[qp^N](\sqrt[q]{1-\xi_q})$$

である。命題２の証明から $[\ L_N^{\circ} : \mathbf{Q}[qp^N]\ ] = q$ かつ $L_N^{\circ} \cap \mathbf{Q}[qp^{\infty}] = \mathbf{Q}[qp^N]$

補題４より容易にわかるように、$n \geqq N$ に対し

$$[\ L_n^{\circ} : \mathbf{Q}[qp^n]\ ] = qp^{n-N}$$

である。よって、$\mathrm{Gal}(L_{\infty}^{\circ} / \mathbf{Q}[qp^{\infty}]) \simeq \mathbf{Z}_p$

従って、L_{∞}° は $\mathbf{Q}[q]$ の $\mathbf{Z}_p^2$ 拡大である。

$$\alpha^{\circ}_n = N_{K_n/\mathbf{Q}[qp^n]}(\alpha_n) \qquad (n = 0,1,2,\cdots\cdot)$$

であるから、L_{∞}/K も $\mathbf{Z}_p^2$ 拡大である。

（２）： $\sigma \in \Delta$ に対して、$L_N^{\circ\sigma} = \mathbf{Q}[qp^N](\sqrt[q]{1-\xi_q^{\sigma}})$ とおくと、命題１－（２）の証明により、

$$\mathrm{rank}\ \mathrm{Gal}(\prod_{\sigma\in\Delta} L_N^{\circ\sigma}\cdot\mathbf{Q}[qp^{n+1}]/\mathbf{Q}[qp^N]) = (p+1)/2$$

よって、

$$\mathrm{rank}\ \mathrm{Gal}(\prod_{\sigma\in\Delta} L_N^{\sigma}\cdot K_{N+1}/K_N) = (p+1)/2$$

従って、$\widetilde{L_{\infty}}/K$ は $\mathbf{Z}_p^{\frac{p+1}{2}}$ 拡大である。□

§４．例

$p = 2$, m = square free かつ正の奇数 , また、$K = \mathbf{Q}(\sqrt{-1},\sqrt{-m})$ とする。$\mathbf{Q}[4] \subset K \subset \mathbf{Q}[4m]$ である。 K の $\mathbf{Z}_2$ 拡大（独立なものが３つある）の 1-st layer を実際に計算してみる。

この場合、[4]の方法を使うと、π_0 と π_1 は、２次体の類数と基本単数を使って、次のように表される。

命題３

m を割る（奇）素数の個数を r とし、ρ, ρ' を次のように定める。

$\rho = 0 \qquad \exists p \mid m : p \equiv 1 \bmod 4$

$\quad\ \ 1 \qquad \forall p \mid m : p \equiv 3 \bmod 4$

$\rho' = 0 \qquad \exists p \mid m : p \equiv 1$ または $3 \bmod 8$

$\quad\ \ 1 \qquad \forall p \mid m : p \equiv 5$ または $7 \bmod 8$

また、square free の整数 d に対して、h_d は $\mathbb{Q}(\sqrt{d})$ の類数、ε_d は $\mathbb{Q}(\sqrt{d})$ の基本単数（ >1 ）とする。

そのとき、π_0 と π_1 の絶対値と argument は次のように表される。

	m ≡ 1 mod 4 のとき	m ≡ 3 mod 4 のとき
$\lvert\pi_0\rvert$	$\varepsilon_m^{-\frac{1}{2}(1-(\frac{2}{m}))h_m}$	$\varepsilon_m^{-\frac{1}{2}h_m}$
$\arg \pi_0$	$-\frac{\pi}{4}\left(h_{-m} + 2^{r-1}\rho\right)$	$-\frac{\pi}{4}\left\{\left(1-\left(\frac{2}{m}\right)\right)h_{-m} + 2^{r-1}\rho\right\}$
$\lvert\pi_1\rvert$	$\varepsilon_m^{-\frac{1}{4}(1-(\frac{2}{m}))h_m} \cdot \varepsilon_2^{-2^{r-2}\cdot\rho} \cdot \varepsilon_{2m}^{-\frac{1}{4}h_{2m}}$	$\varepsilon_m^{-\frac{1}{4}h_m}\ \varepsilon_2^{-2^{r-2}\rho}\ \varepsilon_{2m}^{-\frac{1}{4}h_{2m}}$
$\arg \pi_1$	$-\frac{\pi}{8}\left(h_{-m}+2^{r-1}\rho+2^{r}\rho'+h_{-2m}\right)$	$-\frac{\pi}{8}\left(\left(1-\left(\frac{2}{m}\right)\right)h_{-m}+2^{r-1}\rho+2^{r}\rho'+h_{-2m}\right)$

例1　$m = 3\cdot 73 = 219$, $K = \mathbf{Q}(\sqrt{-1}, \sqrt{-219})$ のとき、

$\varepsilon_{219} = 74 + 5\sqrt{219}$, $h_{219} = 4$, $h_{-219} = 4$, $\rho = 0$ より、

$$|\pi_0| = (74 + 5\sqrt{219})^{-2} , \arg\pi_0 = -2\pi$$

よって、$\alpha_0 = \pi_0 = (74 - 5\sqrt{219})^2$

$74 - 5\sqrt{219} \notin K^{\times 2}$であることがわかり、$L_0 = K(\sqrt{74 - 5\sqrt{219}})$ は K の2次拡大である。

定理より、これは K の $\mathbf{Z}_2$ 拡大に含まれる。

また、簡単な計算から、$K(\sqrt{74 - 5\sqrt{219}}) = K(\sqrt{-146})$ がわかる。

よって、K の $\mathbf{Z}_2$拡大の 1-st layer は $K(\sqrt{2})$ (cyclotomic) , $K(\sqrt{1-i})$, $K(\sqrt{-146})$ (これら3つは独立) である。

例2　$m = 3\cdot 5\cdot 7\cdot 11 = 1155$, $K = \mathbf{Q}(\sqrt{-1}, \sqrt{-1155})$ のとき、

上と同様に計算すると、$\alpha_0 = \pi_0 = \varepsilon_{1155}^{-4}$ となり、$L_0 = K$ となってしまう。

π_1 を計算すると、$\pi_1 = \varepsilon_{1155}^{-2}\ \varepsilon_{2310}^{-2}$ より、

$$\alpha_1 = \pi_0\cdot\pi_1^4 = \varepsilon_{1155}^{-4}\cdot(\cdots)^8$$

よって、$L_1 = K_1(\sqrt[8]{\alpha_1}) = K_1(\sqrt{\varepsilon_{1155}})$

$\sqrt{\varepsilon_{1155}} = (35 + \sqrt{1155})/\sqrt{70}$ となり、$L_1 = K_1(\sqrt{35})$ がわかる。

K の $\mathbf{Z}_2$拡大の 1-st layer は $K(\sqrt{2})$ (cyclotomic) , $K(\sqrt{1-i})$, $K(\sqrt{35})$ (これら3つは独立) である。

REFERENCES

[1] F.Bertrandias and J.-J.Payan, Γ-extensions et invariants cyclotomiques,Ann.Sci.Ecole Norm.Sup.(4),5(1972),517-543

[2] J.E.Carroll, On determining the quadratic subfields of $\mathbb{Z}_2$-extensions of complex quadratic fields,Compositio Math.,30(1975),259-271

[3] J.E.Carroll and H.Kisilevsky, Initial layers of $\mathbb{Z}_\ell$-extensions of complex quadratic fields,Compositio Math.,32(1976),157-168

[4] K.H.Dovermann and L.C.Washington, Relations between cyclotomic units and Smith equivalence of representations,Topology,28(1989),81-89

[5] A.Endo, On the quadratic subfield of a $\mathbb{Z}_2$-extension of an imaginary quadratic number field,Proc.Amer.Math.Soc.,101(1987),417-423

[6] G.Gras, Logarithme p-adique et groupes de Galois,J.Reine Angew.Math., 343(1983),64-80

[7] G.Gras, Sur les $\mathbb{Z}_2$-extensions d'un corps quadratique imaginaire,Ann. Inst.Fourier,33(1983),1-18

[8] G.Gras, Plongements kummeriens dans les $\mathbb{Z}_p$-extensions,Compositio Math.,55(1985),383-396

[9] D.Hemard, Modules galoisiens de torsion et plongement dans les $\mathbb{Z}_p$-extensions,J.Number theory,30(1988),357-374

[10] D.Solomon, On a construction of p-units in abelian fields,Invent. Math.,109(1992),329-350