

与えられた構造の有限岩澤加群を持つ \mathbb{Z}_p -拡大の構成とその応用

尾崎 学 島根大学 (総合理工)

1 序

岩澤理論は代数体の \mathbb{Z}_p -拡大に付随する様々な数論的対象を扱う理論である. 特に岩澤加群はその主役と言える. 本報告では与えられた構造の岩澤加群を持つ \mathbb{Z}_p -拡大を構成することの試みについて, いくつかの結果を得たので報告する.

k を有限次代数体, p を素数, K/k を \mathbb{Z}_p -拡大 (即ち $\text{Gal}(K/k) \simeq \mathbb{Z}_p$ なる Galois 拡大) とすると, K/k の中間体の列,

$$k = k_0 \subseteq k_1 \subseteq k_2 \subseteq \cdots \subseteq k_n \subseteq \cdots \subseteq K = \bigcup_{n \geq 0} k_n$$

で, k_n/k が p^n 次巡回拡大となるものが各 n に対して唯一つ存在する (この k_n を K/k の n -th layer と呼ぶ). $A(k_n)$ を k_n のイデアル類群の Sylow p -部分群とすると, ノルム写像 $A(k_m) \rightarrow A(k_n)$ ($m \geq n$) に関する $\{A(k_n)\}$ の射影的極限 $X_K = \varprojlim A(k_n)$ を K/k の岩澤加群と呼ぶ. 各 $n \geq 0$ に対して, $A(k_n)$ には $\mathbb{Z}_p[\text{Gal}(k_n/k)]$ が作用している. この作用はノルム写像 $A(k_m) \rightarrow A(k_n)$ と自然な写像 $\mathbb{Z}_p[\text{Gal}(k_m/k)] \rightarrow \mathbb{Z}_p[\text{Gal}(k_n/k)]$ に関して可換なので, 完備群環 $\mathbb{Z}_p[[\text{Gal}(K/k)]] := \varprojlim \mathbb{Z}_p[\text{Gal}(k_n/k)]$ が岩澤加群 X_K に作用する. よって X_K は $\mathbb{Z}_p[[\text{Gal}(K/k)]]$ -加群になる. 以下 \mathbb{Z}_p -拡大 K/k に対して $\Lambda_{K/k} = \mathbb{Z}_p[[\text{Gal}(K/k)]]$ と置く.

次の定理が X_K の $\Lambda_{K/k}$ -加群構造に関する基本定理である:

定理 (岩澤) X_K は有限生成 torsion $\Lambda_{K/k}$ -加群.

上で岩澤加群はイデアル類群から定義されたが, 類体論により岩澤加群は Galois 群と見ることにもできる:

$X_K = \text{Gal}(L(K)/K)$, $L(K)/K$: 最大不分岐 pro- p abel 拡大. $\text{Gal}(K/k)$ の作用は, $\gamma \in \text{Gal}(K/k)$, $x \in \text{Gal}(L(K)/K)$ に対して, $\gamma x = \tilde{\gamma} x \tilde{\gamma}^{-1}$ ($\tilde{\gamma} \in \text{Gal}(L(K)/k)$ は γ の $L(K)$ への延長) で与えられる.

このように岩澤加群 X_K は \mathbb{Z}_p -拡大 K/k の数論において非常に重要な対象であり, その $\Lambda_{K/k}$ -加群構造を調べることは岩澤理論における主要テーマと言って良い. 例えば, 岩澤 [3] は X_K の $\Lambda_{K/k}$ -加群構造と X_K と $A(k_n)$ の関係を深く考察して次の有名な公式を示した:

岩澤の類数公式 (岩澤 [3](1959)) ある整数 $\lambda(K/k), \mu(K/k) \geq 0$ と $\nu(K/k)$ で, 十分大なるすべての n に対して

$$\#A(k_n) = p^{\lambda(K/k)n + \mu(K/k)p^n + \nu(K/k)}$$

となるものが存在する.

この公式中の $\lambda(K/k), \mu(K/k)$ と $\nu(K/k)$ を岩澤不変量と呼ぶ. 岩澤不変量 $\lambda(K/k), \mu(K/k)$ は岩澤加群 X_K の構造不変量で,

$$\lambda(K/k) = \text{rank}_{\mathbb{Z}_p} X_K$$

$$\mu(K/k) = 0 \iff X_K \text{ は } \mathbb{Z}_p \text{ 上有限生成}$$

が成立する.

この岩澤加群と岩澤不変量に関して次のような問題が考えられる:

問題 A $\Gamma \simeq \mathbb{Z}_p$ (位相群), $\Lambda = \mathbb{Z}_p[[\Gamma]]$ とする. このとき任意の有限生成 torsion Λ -加群 X に対して, $X_K \simeq X$ となる \mathbb{Z}_p -拡大は存在するか?

ここで上の下線部は, 「適当な同型 $\text{Gal}(K/k) \simeq \Gamma$ で $\Lambda_{K/k}$ と Λ を同一視したとき, X_K と X が Λ -加群として同型」という意味である.

問題 B 任意に与えられた岩澤不変量をもつ \mathbb{Z}_p -拡大は存在するか?

ここで, ν -不変量を除けば問題 B は問題 A よりも弱いことを注意しておく.

筆者の知る限りでは, 上のような問題はこれまでに研究されたことは無い様である. ただし, 問題 B に関しては次のことが知られている.

定理 (岩澤 ([4], etc.)) 任意の素数 p と正数 N に対して, $\lambda(K/k) > N$, 或いは $\mu(K/k) > N$ となる \mathbb{Z}_p -拡大 K/k がそれぞれ存在する.

この報告ではは問題 A に関して得た部分的結果について解説し (第 2 節), その単項化問題への応用にも触れる (第 3 節).

2 主結果とその証明の概略

問題Aで、与えられた X の位数が有限の場合は、この問題は肯定的に解かれる：

定理 1 $\Gamma \simeq \mathbb{Z}_p$ (位相群), $\Lambda = \mathbb{Z}_p[[\Gamma]]$ とする. このとき任意の有限位数の Λ -加群 X に対して, $X_K \simeq X$ となる総実代数体の円分的 \mathbb{Z}_p -拡大 K/k が存在する. つまり, 問題 A は $\#X < \infty$ のときは肯定的に解決される.

注意 K/k が総実代数体の \mathbb{Z}_p -拡大のときは, 常に X_K は有限位数と予想されている (Greenberg 予想 ([2] 参照)). 従ってこの予想の下では, 総実代数体の \mathbb{Z}_p -拡大の岩澤加群として, 可能性のあるすべての Λ -加群が実際に現れる.

証明の概略

$\#X < \infty$ より, ある m, n に対して X は $\mathbb{Z}_p/p^m[\Gamma_n]$ -加群になる ($\Gamma_n = \Gamma/\Gamma^{p^n} \simeq \mathbb{Z}/p^n$).

補題 定理 1 を示すには次を示せば十分：

ある総実代数体の円分的 \mathbb{Z}_p -拡大 K/k で,

- (i) Γ_n -加群として $A(k_n) \simeq X$ (適当な同型 $\Gamma \simeq \text{Gal}(K/k)$ で $A(k_n)$ を Γ_n -加群と見た上で).
- (ii) $\#A(k_n) = \#A(k_{n+1})$
- (iii) K/k の分岐素点は完全分岐

証明 条件 (ii),(iii) より, $X_K \simeq A(k_n)$ (福田 [1]), 従って条件 (i) より, $X_K \simeq X$ □

(i) の条件に関連して, 次のような結果が知られている：

定理 (Yahagi[7](1976)) 任意の有限アーベル p -群 A に対して $A(F) \simeq A$ ($A(F)$: F のイデアル類群の Sylow p -部分群) となる有限次代数体 F が存在する.

この定理の構成手法をイデアル類群への Galois 作用もコントロールできるように発展させて, 補題の条件を満たす \mathbb{Z}_p -拡大を構成する.

X は $\mathbb{Z}_p/p^m[\Gamma_n]$ -加群だから, 完全系列

$$0 \longrightarrow R_n \longrightarrow \mathbb{Z}/p^m[\Gamma_n]^{\oplus r} \longrightarrow X \longrightarrow 0$$

が存在する.

$$\tilde{R}_n = \{(x_i)_{1 \leq i \leq r+1} \in \mathbb{Z}/p^m[\Gamma_n]^{\oplus r+1} \mid (x_i)_{1 \leq i \leq r} \in R_n, x_{n+1} \equiv \sum_{j=1}^n x_j (\gamma_n - 1)\}$$

($\text{Gal}(k_n/k) = \langle \gamma_n \rangle$) とおき, \tilde{X} を完全系列

$$0 \longrightarrow \tilde{R}_n \longrightarrow \mathbb{Z}/p^m[\Gamma_n]^{\oplus r+1} \longrightarrow \tilde{X} \longrightarrow 0$$

で定義する. このとき $\tilde{X} \simeq X \oplus \mathbb{Z}/p^m$.

\mathbb{Q}_t を \mathbb{Q} 上の円分的 \mathbb{Z}_p -拡大 $\mathbb{Q}_\infty/\mathbb{Q}$ の t -th layer とする. 結論を言えば, k としては十分大きい N に対する, \mathbb{Q}_N の適当な導手 $m = \prod_{i=1}^{r+1} \mathfrak{l}_i$ の p^m 次巡回拡大体をとることができる. ここで \mathfrak{l}_i は \mathbb{Q}_N の相異なる素イデアル. この m 及び k の選び方について以下で説明していく.

今後, 同型 $\text{Gal}(\mathbb{Q}_\infty/\mathbb{Q}_N) \simeq \Gamma$ を 1 つ固定してこの 2 つの群を同一視する. L_t を \mathbb{Q}_{N+t} のアーベル p -拡大体 M で M/\mathbb{Q}_{N+t} の導手が m を割っていて, かつ $\text{Gal}(M/\mathbb{Q}_{N+t})$ の exponent が p^m 以下となる最大のものとする. このとき, 類体論により Γ -加群の完全系列

$$\mathcal{O}_{N+t}^\times/p^m \longrightarrow (\mathcal{O}_{N+t}/\mathfrak{m})^\times/p^m \longrightarrow \text{Gal}(L_t/\mathbb{Q}_{N+t}) \longrightarrow 0$$

が存在するが (\mathcal{O}_{N+t} は \mathbb{Q}_{N+t} の整数環), ここで素イデアル \mathfrak{l}_i ($1 \leq i \leq r+1$) が $\mathbb{Q}_{N+t}(\mu_{p^m})/\mathbb{Q}_N$ で完全分解しているとすれば, 上の完全系列の 2 番目の項は $\mathbb{Z}/p^m[\Gamma_t]^{\oplus r+1}$ と同型である:

$$\begin{aligned} (\mathcal{O}_{N+t}/\mathfrak{m})^\times/p^m &\simeq \bigoplus_{1 \leq i \leq r+1, \gamma \in \Gamma_t} (\tilde{\mathcal{O}}_{N+t}/\tilde{\gamma}\tilde{\mathfrak{L}}_i)^\times/p^m \\ &\simeq \bigoplus_{1 \leq i \leq r+1, \gamma \in \Gamma_t} \mu_{p^m} \bmod \tilde{\gamma}\tilde{\mathfrak{L}}_i \\ &\simeq \mathbb{Z}/p^m[\Gamma_t]^{\oplus r+1} \end{aligned}$$

ここで, $\tilde{\mathcal{O}}_{N+t}$ は $\mathbb{Q}_{N+t}(\mu_{p^m})$ の整数環, $\tilde{\gamma} \in \text{Gal}(\mathbb{Q}_{N+t}(\mu_{p^m})/\mathbb{Q}_N(\mu_{p^m}))$ は自然な同型 $\Gamma_t \simeq \text{Gal}(\mathbb{Q}_{N+t}(\mu_{p^m})/\mathbb{Q}_N(\mu_{p^m}))$ による $\gamma \in \Gamma_t$ の像 (N を $\mu_{p^m} \subseteq \mathbb{Q}_N(\mu_p)$ となるよう十分大きく選んでおく), $\tilde{\mathfrak{L}}_i$ は \mathfrak{l}_i の上にある固定された $\mathbb{Q}_{N+t}(\mu_{p^m})$ の素イデアルで, 最後の同型は

$$\begin{aligned} (\zeta_{i,\gamma} \bmod \tilde{\gamma}\tilde{\mathfrak{L}}_i)_{1 \leq i \leq r+1, \gamma \in \Gamma_t} &\mapsto \left(\sum_{\gamma \in \Gamma_t} \varphi(\zeta_{i,\gamma})\gamma \right)_{1 \leq i \leq r+1} \\ &(\varphi : \mu_{p^m} \simeq \mathbb{Z}/p^m \text{ は固定された同型}) \end{aligned}$$

で与えられる. よって完全系列

$$\mathcal{O}_{N+t}^\times/p^m \xrightarrow{\rho_t} \mathbb{Z}/p^m[\Gamma_t]^{\oplus r+1} \longrightarrow \text{Gal}(L_t/\mathbb{Q}_{N+t}) \longrightarrow 0$$

を得る. ここで ρ_t は具体的に次で与えられる:

$$\rho_t : \mathcal{O}_{N+t}^\times/p^m \longrightarrow \mathbb{Z}/p^m[\Gamma_t]^{\oplus r+1}, \quad \rho_t(\varepsilon) = \left(\sum_{\gamma \in \Gamma_t} \varphi \left(\left(\frac{\varepsilon}{\tilde{\gamma} \tilde{\mathcal{L}}_i} \right) \right) \gamma \right)_{i=1}^{r+1}.$$

ここに, $\left(\frac{\varepsilon}{\tilde{\gamma} \tilde{\mathcal{L}}_i} \right) \in \mu_{p^m}$ は $\mathbb{Q}_{N+t}(\mu_{p^m})$ における p^m 冪剰余記号.

命題 1 (1) 任意の Γ_t -準同型 $f : \mathcal{O}_{N+t}^\times/p^m \longrightarrow \mathbb{Z}/p^m[\Gamma_t]^{\oplus r+1}$ に対して, l_i ($1 \leq i \leq r+1$) (及び $\tilde{\mathcal{L}}_i$) をうまく選ぶと $\rho_t = f$ となる.

(2) $\mathcal{O}_{N+t}^\times/p^m \simeq \mathbb{Z}/p^m[\Gamma_t]^{\oplus p^N-1} \oplus \mathbb{Z}/p^m[\Gamma_t]/\sum_{\gamma \in \Gamma_t} \gamma$

$\pi : \mathbb{Z}/p^m[\Gamma_{n+1}]^{\oplus r+1} \longrightarrow \mathbb{Z}/p^m[\Gamma_n]^{\oplus r+1}$ を自然な全射とし, $\tilde{R}_{n+1} := \pi^{-1}(\tilde{R}_n)$ とおく. ここで, $\mathbb{Z}/p^m[\Gamma_{n+1}]^{\oplus r+1}/\tilde{R}_{n+1} \simeq \tilde{X}$ に注意.

命題 1 より, $p^N - 1$ が \tilde{R}_{n+1} の $\mathbb{Z}/p^m[\Gamma_n]$ 上の最小生成系の位数より大きいとき, l_i ($1 \leq i \leq r+1$) をうまく選ぶと

$$\text{Im} \rho_{n+1} = \tilde{R}_{n+1}, \quad \text{Gal}(L_{n+1}/\mathbb{Q}_{N+n+1}) \simeq \tilde{X}$$

となる. このとき $\text{Im} \rho_n = \tilde{R}_n$, $\text{Gal}(L_n/\mathbb{Q}_{N+n}) \simeq \tilde{X}$ となることを示すことができる. ここで, 埋め込み $X \hookrightarrow \tilde{X}$, $(x_1, x_2, \dots, x_r) \bmod \tilde{R}_n \mapsto (x_1, x_2, \dots, x_r, \sum_{j=1}^r x_j) \bmod \tilde{R}_n$ で $X \subseteq \tilde{X}$ と見なす. $t = n, n+1$ に対して, L_t の $X \subseteq \tilde{X} \simeq \text{Gal}(L_t/\mathbb{Q}_{N+t})$ による固定部分体を M_t とおくと次が成立する:

命題 2 (1) $t = n, n+1$ とする. M_t/\mathbb{Q}_{N+t} の導手は m の p^m 次巡回拡大で, l_i ($1 \leq i \leq r+1$) 上の \mathbb{Q}_{N+t} 上の素イデアルはすべて完全分岐.

(2) $t = n, n+1$ とする. L_t/M_t は不分岐拡大で $\text{Gal}(L_t/M_t) \simeq X$. さらに L_t は M_t/\mathbb{Q}_{N+t} の genus p -class field, 即ち M_t の不分岐アーベル p -拡大体で \mathbb{Q}_{N+t} 上アーベル拡大体となる最大のもの. したがって, $\text{Gal}(L_t/M_t) \simeq A(M_t)/(\sigma - 1)$ ($\langle \sigma \rangle = \text{Gal}(M_t/\mathbb{Q}_{N+t})$).

(3) ある導手 m の p^m 次巡回拡大 k/\mathbb{Q}_N で $M_n = k_n$, $M_{n+1} = k_{n+1}$ ($k_m:k$ の円分的 \mathbb{Z}_p -拡大の m -th layer) となるものが (一意に) 存在する (k は総実であることに注意).

この命題と補題により, もしも $t = n, n+1$ に対して L_t が $M_t = k_t$ の Hilbert p -類体であれば, k 上の円分的 \mathbb{Z}_p -拡大が求める \mathbb{Z}_p -拡大にな

る. そのためには, $\text{Gal}(L_t/k_t) \simeq A(k_t)/(\sigma - 1)$ より, $A(k_t)/(\sigma - 1)$ が $\text{Gal}(k_t/\mathbb{Q}_{N+t})$ -不変なイデアル類で生成されていれば, $A(k_t)/(\sigma - 1) = A(k_t)$ となるのでよい. もし,

$$\text{Gal}(L_{n+1}/k_{n+1}) = \left\langle \left(\frac{L_{n+1}/k_{n+1}}{\mathfrak{L}} \right) \middle| \overline{\mathfrak{L}}|_{\mathfrak{m}} : k_{n+1} \text{ の素イデアル} \right\rangle$$

であれば, この条件は満たされている ($\overline{\mathfrak{L}}$ は $k_{n+1}/\mathbb{Q}_{N+n+1}$ で完全分岐しているから). 実際に, $i = 1$ から順に k_i ($1 \leq i \leq r + 1$) をうまく帰納的に選ぶことによって上の条件 (及び前提の条件 $\text{Im} \rho_{n+1} = \tilde{R}_{n+1}$) が満たされるようにできる. このようにして, 定理 1 が示される.

3 単項化問題への応用

F を有限次代数体, H を F の Hilbert 類体とすると, 単項化定理により F のすべてのイデアルは H で単項化する. 言い換えれば, イデアルの持ち上げから生ずる自然な写像 $\text{Cl}(F) \rightarrow \text{Cl}(H)$ は零写像である ($\text{Cl}(\ast)$ はイデアル類群). ところが, 必ずしも Hilbert 類体まで持ち上げなくとも, H/F のある真の中間体 M で既に自然な写像 $\text{Cl}(F) \rightarrow \text{Cl}(M)$ が零写像になることもある. 岩澤 [5] では, \mathbb{Z}_p -拡大の理論を用いて, そのような代数体 F の無限族を構成している.

定理 (岩澤 [5](1989))

任意の素数 p に対し, 次をみたく代数体 F が無数に存在する:

- (i) $\text{Cl}(F)[p^\infty] \simeq (\mathbb{Z}/p\mathbb{Z})^{\oplus r}$, $r \geq 2$,
- (ii) F のある p 次不分岐巡回拡大 F'/F に於いて, $\text{Cl}(F)[p^\infty]$ が単項化する.

上の定理の F に対し, M を F' とすべての素数 $l \neq p$ についての F の Hilbert l -類体との合成体とすれば, $F \subseteq M \subsetneq H$ で, $\text{Cl}(F)$ は M で単項化する.

筆者はこの岩澤先生の手法を用いて, 上の定理の条件 (i) の「 $r \geq 2$ 」を, 任意の N について「 $r \geq N$ 」で置き換えても, 定理が成立することを示していた ([6]). 今回の定理 1 の構成手法を応用することによって, さらに一般に次を示すことができる:

定理 2 p を素数とする. 任意の有限アーベル p -群 A に対して次の性質 (i), (ii) を持つ代数体 F が存在する:

- (i) $\text{Cl}(F)[p^\infty] \simeq A$,
(ii) ある不分岐 p^e 次巡回拡大 F'/F ($p^e: A$ の exponent) が存在して, $\text{Cl}(F)[p^\infty]$ は F' で単項化する.

証明 $A = A' \oplus \mathbb{Z}/p^e$ とする. 定理 1 で $X = A'$, $n = 0$ (つまり Γ -作用は自明), $m = e$ として k を構成する. このとき F を k_e/\mathbb{Q}_N (N は定理 1 の証明中と同じ) の中間体で $\text{Gal}(F/\mathbb{Q}_N) \simeq \mathbb{Z}/p^e$, $F \neq k$, \mathbb{Q}_{N+e} なるものとする. このとき k_e/F は不分岐 p^e 次巡回拡大になる. $L_e := L_0 k_e = L_0 \mathbb{Q}_{N+e}$ は k_e のヒルベルト p -類体で L_0/\mathbb{Q}_N はアーベル拡大 (命題 2 (2)) だから, L_e/\mathbb{Q}_N はアーベル拡大. 従って L_e/F は不分岐アーベル拡大になるから, L_e は F の Hilbert p -類体でもある. $L_e = L_0 F$, $L_0 \cap F = \mathbb{Q}_N$ なので (F/\mathbb{Q}_N では p 上の素点が完全分岐するが L_0/F では不分岐だから), $\text{Gal}(L_e/F) = \text{Gal}(L_0 F/F) \simeq \text{Gal}(L_0/\mathbb{Q}_N) \simeq A' \oplus \mathbb{Z}/p^e = A$. 故にこの F は (i) を持たしている. 次に $\text{Cl}(F)[p^\infty]$ は不分岐 p^e 次巡回拡大 k_e/F で単項化することを示す. 類体論から生ずる可換図式

$$\begin{array}{ccc} \text{Cl}(k_e)[p^\infty] & \xrightarrow{\sim} & \text{Gal}(L_e/k_e) \\ \uparrow & & \uparrow \text{Ver} \\ \text{Cl}(F)[p^\infty] & \xrightarrow{\sim} & \text{Gal}(L_e/F) \simeq A \end{array}$$

(横写像は Artin 写像, 左縦写像はイデアルの持ち上げから生ずる自然な準同型, 右縦写像は $\text{Gal}(L_e/F)^{\text{ab}} = \text{Gal}(L_e/F)$ から $\text{Gal}(L_e/k_e)^{\text{ab}} = \text{Gal}(L_e/k_e)$ への移送写像.) において, 右縦写像はこの場合 p^e 倍写像と一致しているから零写像, 従って左縦写像も零写像となり, (ii) も満たされている. \square

参考文献

- [1] T. Fukuda, Remarks on \mathbb{Z}_p -extensions of number fields, *Proc. Japan Acad.* **70A** (1994), 264–266.
- [2] R. Greenberg, On the Iwasawa invariants of totally real number fields, *Amer. J. of Math.* **98** (1976), 263–284.
- [3] K. Iwasawa, On Γ -extensions of algebraic number fields., *Bull. Amer. Math. Soc.* **65** (1959), 183–226.

- [4] K. Iwasawa, On the μ -invariants of \mathbb{Z}_ℓ -extensions, *Number Theory, Algebraic Geometry and Commutative Algebra, in honor of Y. Akizuki, Kinokuniya, Tokyo*, (1973), 1–11.
- [5] K. Iwasawa, A note on capitulation problem for number fields II, *Proc. Japan Acad.* **65** (1989), 183–186.
- [6] M. Ozaki, Iwasawa invariants of p -extensions of totally real number fields, preprint
- [7] O. Yahagi, Construction of Number fields with prescribed l -class groups, *Tokyo J. of Math.* **1** (1978), 275–283.

尾崎 学 (Manabu Ozaki)
島根大学 総合理工学部 数理・情報システム学科
〒 690-8504 島根県松江市西川津町 1060
e-mail: ozaki@math.shimane-u.ac.jp