数理解析研究所講究録 1376 巻 2004 年 13-19

Non-abelian Iwasawa formulae for unramified p-extensions

島根大学　総合理工　尾崎 学 (Manabu Ozaki)
Department of Mathematics, Shimane Univ.

1. 序

数年前より筆者は代数体の不分岐p-拡大を$\mathbf{Z}_p$-拡大を通じて捉える「非アーベル岩澤理論」の展開を試みている(本研究集会の John Coates 氏, 加藤和也氏の講演における「non-commutative Iwasawa theory」は「$\mathbf{Z}_p$-拡大」を「p-進 Lie 拡大」へと「作用する群の非可換化」を目指しているのに対して, この稿で言うところの「非アーベル岩澤理論」は, 岩澤加群 (乃至はセルマー群) を非アーベルガロワ群へと「作用される群の非可換化」という方向を目指している).

岩澤理論に於ける最初の著しい成果は, 岩澤公式と言える. つまり, $\mathbf{Z}_p$-拡大 K/k の中間体 k_n ($n \geq 0$, $[k_n : k] = p^n$) のイデアル類群の p-part(或いは k_n 上の最大不分岐アーベル p-拡大のガロワ群) の位数の n を動かしたときの振る舞いを, K 上の最大不分岐アーベル p-拡大 L/K のガロワ群の構造不変量, すなわち岩澤不変量を用いて表す公式である. 非アーベル岩澤理論に於いてもその出発点とすべく, この公式の一般化に相当する事実の証明を最初の目標に掲げてこれまで研究を行ってきたが, 近頃 K/k の岩澤 μ-不変量が 0 である場合には満足のゆく結果を得ることに成功したのでそれについて解説する.

2. 非アーベル岩澤公式

まずオリジナルの岩澤公式の復習から始める. p を素数 (以下で固定しておく), K/k を $\mathbf{Z}_p$-拡大, $\Gamma := \mathrm{Gal}(K/k) \simeq \mathbf{Z}_p$

$$k = k_0 \subseteq k_1 \subseteq \cdots k_n \subseteq \cdots \subseteq K = \bigcup_{n=0}^{\infty} k_n, \ \ k_n/k : p^n\text{-次巡回拡大}$$

として, L_n/k_n, L/K を最大不分岐アーベル p-拡大, $X_n := \mathrm{Gal}(L_n/k_n)$($\simeq k_n$ のイデアル類群の p-part), $X := \mathrm{Gal}(L/K)$ とおく. $X \simeq \varprojlim X_n$ (射影的極限は定義域の制限写像に関する) であり, X_n は $\mathbf{Z}_p[\mathrm{Gal}(k_n/k)]$-加群なので, X は完備群環 $\Lambda := \varprojlim \mathbf{Z}_p[\mathrm{Gal}(k_n/k)]$ (射影的極限は定義域の制限写像から誘導される準同型に関する) 上の加群の構造が自然に入る. この X は $\mathbf{Z}_p$-拡大 K/k の岩澤加群と呼ばれ, 有限生成捻れ Λ-加群であることが知られている. 岩澤加群 X は全ての $n \geq 0$ に対する X_n の情報を持っている. 従って, X の Λ-加群構造より X_n ($n \geq 0$) の振る舞いを知ることができる. 特にその位数に関して次の岩澤公式が成立する：

岩澤公式 (岩澤 [1]). $\exists \nu \in \mathbf{Z}$, $\exists n_0 \geq 0$:

$$\# X_n = p^{\lambda n + \mu p^n + \nu} \ \ \text{for } \forall\, n \geq n_0.$$

ここで, $\lambda := \mathrm{rank}_{\mathbf{Z}_p} X$, μ は $\mathrm{Tor}_{\mathbf{Z}_p} X \sim \bigoplus_{i=1}^{r} \Lambda/p^{m_i}$ ($\sim$ は ker, coker が共に有限な準同型を表す) とするとき, $\mu := \sum_{i=1}^{r} m_i$ で定義される.

上の λ, μ は岩澤加群 X の構造不変量で, 岩澤不変量と呼ばれる.
(注 : ν も岩澤不変量と呼ばれているが, これは一般には岩澤加群の Λ-加群構造のみからは定まらない.)

古典的岩澤理論では最大不分岐アーベル p-拡大 L_n/k_n, L/K を扱ったが, 非アーベル岩澤理論の目標物は最大不分岐 p-拡大 $\tilde{L}_n/k_n$, $\tilde{L}/K$ のガロワ群 $\tilde{G}_n = \mathrm{Gal}(\tilde{L}_n/k_n)$, $\tilde{G} = \mathrm{Gal}(\tilde{L}/k)$ である. 岩澤公式のこの非アーベル的な状況での類似を考えるとき, $\tilde{G}_n$ は $X_n = \tilde{G}_n^{\mathrm{ab}}$ とは異なり必ずしも有限ではないのでこれの位数の挙動を問うことは無意味である. 従って, $\tilde{G}_n$ に適当なフィルトレーションを入れて考えるのが適切であるが, ここではは降中心列を入れて考える :

群 H に対し, H の降中心列を

$$H = C_1(H) \supseteq C_2(H) \supseteq \cdots \supseteq C_i(H) \supseteq \cdots,$$
$$C_{i+1}(H) = [C_i(H), H] \quad (i \geq 1),$$

(H が位相群のときは交換子群は位相的 (閉包をとる))
で定義し,

$$X_n^{(i)} := C_i(\tilde{G}_n)/C_{i+1}(\tilde{G}_n), \ X^{(i)} := C_i(\tilde{G})/C_{i+1}(\tilde{G})$$

とおく. 後者の加群 $X^{(i)}$ を i-次岩澤加群と呼ぶことにする. ここで, $X_n^{(1)} = X_n$, $X^{(1)} = X$ であることに注意しよう. $i \geq 0$ に対して $L_n^{(i)} := \tilde{L}_n^{C_{i+1}(\tilde{G}_n)}$ とおけばこれは有限次代数体で, $A(L_n^{(i-1)})$ で $L_n^{(i-1)}$ のイデアル類群の p-part を表すことにすれば

$$X_n^{(i)} \simeq A(L_n^{(i-1)})_{\mathrm{Gal}(L_n^{(i-1)}/k_n)} \quad (i \geq 1)$$

が分かるので, 各 $i \geq 1$, $n \geq 0$ について $X_n^{(i)}$ は有限アーベル群である. 従って $X_n^{(1)} = X_n$, $X^{(1)} = X$ を考慮すれば, $i \geq 1$ を固定して, $n \geq 0$ を動かしたときの $X_n^{(i)}$ の位数の振る舞いが岩澤公式のように高次岩澤加群 $X^{(i)}$ の何らかの構造不変量を用いて表せるか? という問題が考えられる. そのためにまず高次岩澤加群の構造についてまとめておく.

通常の岩澤理論で X に $\Gamma := \mathrm{Gal}(K/k)$ が作用するのと同様のやり方で, i-次岩澤加群 $X^{(i)} = \mathrm{Gal}(L^{(i)}/L^{(i-1)})$ ($L^{(i)} := \tilde{L}^{C_{i+1}(\tilde{G})}$) にも Γ が $\mathrm{Gal}(L^{(i)}/k)$ の内部自己同型を通じて自然に作用している. 従って $X^{(i)}$ も Λ-加群の構造を持っている. この Λ-加群構造に関して次が成立する :

命題 1. μ を K/k の岩澤 μ-不変量とする.
(i) $\mu = 0$ ならばすべての $i \geq 1$ に対して $X^{(i)}$ は有限生成捩れ Λ-加群, さらに $\mathbf{Z}_p$ 上でも有限生成 (つまり $\mu(X^{(i)}) = 0$).
(ii) $\mu > 0$ ならば, $i \geq 2$ のときは $X^{(i)}$ は捩れ Λ-加群であるが Λ 上有限生成ではない.
(iii) μ の値に拘わらず, $\lambda^{(i)} := \mathrm{rank}_{\mathbf{Z}_p} X^{(i)}$ は有限.

上の $\lambda^{(i)}$ $(i \geq 1)$ を i-次岩澤 λ-不変量と呼ぶことにする. $\lambda^{(1)}$ は K/k の通常の岩澤 λ-不変量に等しいことに注意しよう. 命題 1 より $\mu = 0$ の時はアーベル的な場合 $(i = 1)$ と $i \geq 2$ で $X^{(i)}$ の Λ-加群構造に大きな差はないが, $\mu > 0$ の場合には著しい違いがあることが分かる. 以下 $\underline{\mu = 0}$ の場合に限って話を進めることにする. すると, アーベル的な場合の岩澤公式を思えば自ずと次の予想へと導かれるであろう ([2]) :
予想 (非アーベル岩澤公式). $\underline{\mu = 0}$ と仮定する. このとき各 $i \geq 2$ に対して,

$$\exists \nu^{(i)} \in \mathbf{Z}\ \exists n_0^{(i)} \geq 0 : \ \# X_n^{(i)} = p^{\lambda^{(i)} n + \nu^{(i)}} \quad \text{for } \forall\, n \geq n_0^{(i)}.$$

これまで上の予想は特殊な条件を満たす $\mathbf{Z}_p$-拡大 K/k と小さい i について正しいことが知られているに過ぎなかったのであるが ([2] 参照), 遂にこれを一般に示すことに成功した：

定理 1 ([3]). 上の予想は正しい.

この定理の直接の系として k_n 上の nilpotent class i の最大不分岐 p-拡大のガロワ群 $G_n^{(i)} := \tilde{G}_n/C_{i+1}(\tilde{G}_n) = \mathrm{Gal}(L_n^{(i)}/k_n)$ の位数に関して次の公式を得る：

系． K/k の μ-不変量は 0 であると仮定する. このとき $i \geq 1$ について

$$\exists m_0^{(i)} \geq 0 : \#G_n^{(i)} = p^{(\sum_{j=1}^{i}\lambda^{(j)})n+\sum_{j=1}^{i}\nu^{(j)}} \ \text{ for } \forall\, n \geq m_0^{(i)}.$$

このように k_n 上の非アーベル不分岐 p-拡大のガロワ群 $G_n^{(i)}$ の位数に関しても岩澤公式の類似が成立するのである.

3. 非アーベル岩澤公式の証明

この節では非アーベル岩澤公式の証明を説明したいと思う. 以下では, $\mathbf{Z}_p$-拡大 K/k の μ-不変量は 0 で K/k で分岐している素点は完全分岐している と仮定する (この後半の仮定は必要であれば適当な $n \geq 0$ について k を k_n に取り替えればいつでも成立するので無害である). そして $i \geq 1$ を 1 つ固定する. このとき, $X_n^{(i)}$ は $X^{(i)}$ の商になることが分かるので, $X_n^{(i)} = X^{(i)}/Y_n^{(i)}$ となる $X_n^{(i)}$ の部分加群 $Y_n^{(i)}$ が存在する. この $Y_n^{(i)}$ の n を動かしたときの振る舞いが分かれば, $X_n^{(i)}$ の振る舞い (特にその位数) を知ることができる.
$i=1$ のときがオリジナルの岩澤公式の状況なので, まずこの場合を見てみよう. この場合は $Y_n^{(1)}$ は非常に良い振る舞いをすることが分かっている：

$$Y_n^{(1)} = \nu_n(Y_0^{(1)}),\ \nu_n := 1+\gamma+\gamma^2+\cdots+\gamma^{p^n-1} \in \Lambda,\ \Gamma = \langle\gamma\rangle. \tag{1}$$

このように $Y_n^{(1)}$ を綺麗に記述できることが, オリジナルの岩澤公式の証明の鍵であった. さらに $\mu=0$ のときは $X^{(1)}$ は $\mathbf{Z}_p$-上有限生成で, $\nu_{m,n} := \nu_m/\nu_n \in \Lambda \ \ (m \geq n \geq 0)$ とおけば, n が十分大きいときには $\nu_{m,n}$ が $p^{m-n} \times (\Lambda^{\times}$の元) で $X^{(1)}$ に作用することも分かるので (1) より,

$$\exists n_0 \geq 0 : Y_n^{(1)} = p^{n-n_0}Y_{n_0}^{(1)} \ \ (\forall n \geq n_0) \tag{2}$$

となることも分かる. 従って,

$$\#X_n^{(1)} = \#(X^{(1)}/Y_{n_0}^{(1)})\#(Y_{n_0}^{(1)}/p^{n-n_0}Y_{n_0}^{(1)})$$

であり, n_0 を十分大きくとっておけば $Y_{n_0}^{(1)} \simeq \mathbf{Z}_p^{\oplus\lambda}$ なので, 上式より岩澤公式が導かれる.

$i \geq 2$ の場合には, $X^{(i)}$ を Λ-加群として捉えた場合に $Y_n^{(i)}$ の間に (1) のような簡明な関係は一般に存在しない. これが $i \geq 2$ の場合の $\#X_n^{(i)}$ の振る舞いの研究を困難にさせている要因であったのであるが, $X^{(i)} = C_i(G^{(i)}) \subseteq G^{(i)} := \tilde{G}/C_{i+1}(\tilde{G})$ と捉えて, $G^{(i)}$ に対して群論的手法を駆使することにより $Y_n^{(i)}$ の間に (2) のような関係が成立することを示すことができて, 公式が証明されるのである. 以下でそれを説明しよう.

$i=1$ の場合に上で見たように, $X^{(i)}$ が $\mathbf{Z}_p$-上有限生成で $\mathrm{rank}_{\mathbf{Z}_p}X^{(i)} = \mathrm{rank}_{\mathbf{Z}_p}Y_n^{(i)} = \lambda^{(i)}$ であることに注意すれば (命題 1) 非アーベル岩澤公式を示すには結局

$$\exists n_0 \geq 0 : Y_n^{(i)} = (Y_{n_0}^{(i)})^{p^{n-n_0}} \ \ (\forall n \geq n_0) \tag{3}$$

が言えればよい(以下ではアーベル群であっても群演算は乗法的に記す). そのためには次の２つ主張を示せばよい：

$$\text{(A)}\quad \exists d \geq 0 : \# X_n^{(i)} \leq p^{\lambda^{(i)}n+d} \text{ for } \forall n \geq 0.$$

$$\text{(B)}\quad \exists m_0 \geq 0 : Y_{n+1}^{(i)} \subseteq (Y_n^{(i)})^p \text{ for } \forall n \geq m_0$$

(A),(B) が示されたする. (B) より

$$\# X_{n+1}^{(i)} / \# X_n^{(i)} = \#(Y_n^{(i)}/Y_{n+1}^{(i)}) \geq \#(Y_n^{(i)}/(Y_n^{(i)})^p) \geq p^{\lambda^{(i)}} \quad \text{for } n \geq m_0.$$

なので, ある $a_n \geq 0$ $(n \geq m_0)$ について $\# X_{n+1}^{(i)} / \# X_n^{(i)} = p^{\lambda^{(i)}+a_n}$ となる. よって

$$(4)\qquad X_n^{(i)} = p^{\lambda^{(i)}(n-m_0)+\sum_{i=m_0}^{n-1} a_i + b} = p^{\lambda^{(i)}n+(\sum_{i=m_0}^{n-1} a_i + b - \lambda^{(i)} m_0)} \text{ for } n \geq m_0.$$

$(\# X_{m_0}^{(i)} = p^b)$ を得る. 従って (A) より n が十分大ならば $a_n = 0$, $Y_{n+1}^{(i)} = (Y_n^{(i)})^p$ となり, (3) が得られる.

(A),(B) を示すためにまず $Y_n^{(i)}$ が $X^{(i)}$ の如何なる部分群であるかを記述する. $\mathcal{G}^{(i)} := \mathrm{Gal}(L^{(i)}/k)$ とおき, $\mathfrak{p}_j$ を K/k で分岐する k の素点 $(1 \leq j \leq s)$ とし, $I_j \subseteq \mathcal{G}^{(i)}$ を $\mathfrak{p}_j$ 上の $L^{(i)}$ の素点に対する惰性群 $(j = 1, 2, \ldots, s)$ とする. このとき, $\mathfrak{p}_j$ は K/k で完全分岐して, $L^{(i)}/K$ で不分岐であるから, 自然な全射 $\mathcal{G}^{(i)} \longrightarrow \Gamma$ が同型 $I_j \simeq \Gamma \simeq \mathbf{Z}_p$ を誘導する. そこで, $I_1 = \langle \gamma \rangle \simeq \Gamma$, $I_j = \langle \gamma g_j \rangle$ $(g_j \in G^{(i)},\ 2 \leq j \leq s)$ としよう. このとき次が成立する:

命題 2. (i) $G_n^{(i)} \simeq G^{(i)}/R_n^{(i)}$, $R_n^{(i)} = (\nu_n([\gamma, x]),\ \nu_n(g_j) | x \in G^{(i)},\ 2 \leq j \leq s)_{G^{(i)}}$
ここで, 交換子は $[x,y] := x^{-1}y^{-1}xy$ で,

$$\nu_n(g) := (\gamma^{-(p^n-1)} g \gamma^{p^n-1})(\gamma^{-(p^n-2)} g \gamma^{p^n-2}) \cdots (\gamma^{-1} g \gamma) g \quad (g \in G^{(i)})$$

であり, $(*)_{G^{(i)}}$ は, 括弧内の元で生成される $G^{(i)}$ の正規 (閉) 部分群を表す.
(ii) $Y_n^{(i)} = C_i(G^{(i)}) \cap R_n^{(i)} \subseteq X^{(i)} = C_i(G^{(i)})$.

この命題は, 岩澤類数公式の証明の過程で示された $i = 1$ の場合の主張と全く同じ考察で示すことができる (例えば [4, Lemma 13.15] 参照).

まず (A) であるが, これは以下のように容易に示される：

補題 1. $\exists c \geq 0 : (X^{(i)})^{p^{n+c}} \subseteq Y_n^{(i)}$ for $\forall n \geq 0$.

(証明) i に関する帰納法で示す. $i = 1$ のときは (2) より OK!
$i = l-1$ に対して補題が成立と仮定. $[\ ,\ ] : X^{(l-1)} \times X^{(1)} \longrightarrow X^{(l)}$ を交換子積が誘導する pairing, $A \subseteq X^{(l-1)}$, $B \subseteq X^{(1)}$ に対して $[A, B]$ を $\{[a,b] | a \in A, b \in B\}$ で生成される $X^{(l)}$ の部分群とする. 命題 2 より $R_n^{(l-1)} = R_n^{(l)} C_l(G^{(l)})/C_l(G^{(l)}) \subseteq G^{(l-1)} = G^{(l)}/C_l(G^{(l)})$ であるから $[Y_n^{(l-1)}, X^{(1)}] \subseteq Y_n^{(l)}$ となることに注意すれば, 帰納法の仮定より,

$$Y_n^{(l)} \supseteq [Y_n^{(l-1)}, X^{(1)}] \supseteq [(X^{(l-1)})^{p^{n+c}}, X^{(1)}] = [X^{(l-1)}, X^{(1)}]^{p^{n+c}} = (X^{(l)})^{p^{n+c}}$$

となり, $i = l$ のときも補題は成立. よって補題は示された. □

(A) は上の補題より直ちに従う.

次に (B) であるが, これは命題 2 からも分かるように $R_n^{(i)}$ の n を動かしたときの挙動をまず見極めることが必要となる. その前に新たに記号を少し導入する. 群 H と素数 p に対し,

$$H^{p^n} := \langle h^{p^n} | h \in H \rangle,\ H^{[p^n]} := \{h^{p^n} | h \in H\} \quad (n \geq 0)$$

とおく (H が位相群の場合は $\langle * \rangle$ は常に括弧の中の元で生成される閉部分群を表す).

さて, $g \in G^{(i)}$ と $m \geq n \geq 0$ に対して

$$\nu_{m,n}(g) = (\gamma^{-p^n(p^{m-n}-1)} g \gamma^{p^n(p^{m-n}-1)})(\gamma^{-p^n(p^{m-n}-2)} g \gamma^{p^n(p^{m-n}-2)}) \cdots (\gamma^{-p^n} g \gamma^{p^n}) g$$

とおく ($i = 1$ のときはこの作用素は (1) の後で定義したものに他ならないことに注意). このとき $\nu_m(g) = \nu_{m,n}(\nu_n(g))$ となることが容易に分かるので命題 2 より

$$(5) \qquad R^{(i)}_{n+1} = \langle \nu_{n+1,n}(\nu_n([\gamma, x])),\ \nu_{n+1,n}(\nu_n(g_j)) | x \in G^{(i)},\ 2 \leq j \leq s \rangle_{G^{(i)}}$$

となる. ここで群論的な考察により次を示すことができる：

補題 2. 任意の $d \geq 0$ に対し, 次をみたす $n_1 \geq 0$ が存在する：
γ の作用で閉じている任意の部分群 $R \subseteq G^{(i)}$ に対して, $n \geq n_1$ ならば

$$\nu_{n+d,n}(R) \subseteq R^{p^d}$$

となる.
特に n が十分大ならば

$$\nu_{n+1,n}(R^{(i)}_n) \subseteq (R^{(i)}_n)^p$$

となる.

これは $G^{(1)} = X$ に注意すれば, $i = 1$ の場合と同じ状況が成立しているとみることができる (式 (1) の後の記述参照). よって補題 2 と (5) より次を得る：

補題 3. n が十分大きいとき, $R^{(i)}_{n+1} \subseteq (R^{(i)}_n)^p$.

この補題から

$$Y^{(i)}_{n+1} = C_i(G^{(i)}) \cap R^{(i)}_{n+1} \subseteq C_i(G^{(i)}) \cap (R^{(i)}_n)^p$$

が出るが, (B) を示すにはさらに

$$(6) \qquad C_i(G^{(i)}) \cap (R^{(i)}_n)^p \subseteq (Y^{(i)}_n)^p = (C_i(G^{(i)}) \cap R^{(i)}_n)^p$$

を示さなければならない. $Y^{(i)}_n$ はアーベル群であるから $(Y^{(i)}_n)^p = (Y^{(i)}_n)^{[p]}$ である. また大雑把に言って $C_i(G^{(i)}) \cap (R^{(i)}_n)^p$ の元は $R^{(i)}_n$ のいくつかの p-乗元たちの積からなっている. したがって (6) を示すには, 「適当な条件をみたすいくつかの p-乗元たちの積が 1 つの p-乗元で表される」という類のことを示す必要がある. それに応えてくれるのが次の組み合わせ群論的な結果である：

命題 3. 次の条件を満たす $i \geq 1$ にのみ依存する定数 $e = e(i)$ が存在する:
任意の $C_{i+1}(H) = 1$ となる抽象群 H と素数 p に対して,

$$x, y \in H,\ n \geq 0 \Longrightarrow x^{p^n} y^{p^{n+e}} \in H^{[p^n]}$$

が成立する.

特に, 次の系を得る.

系 . $e = e(i)$ を命題 3 の定数, H を $C_{i+1}(H) = 1$ となるコンパクト (もしくは離散) 位相群, p を素数とすれば任意の $n \geq 0$ に対して

$$H^{p^{n+e}} \subseteq H^{[p^n]}$$

が成立する.

命題 3 の証明の詳細はここでは省略するが，基本的には Hall の公式とよばれる，アルファベット X, Y に関する語 $(XY)^m$ $(m \geq 0)$ のある種の展開式 (例えば $(XY)^2 = X^2Y^2[Y,X][[Y,X],Y]$) を使って証明される．

以下，この命題を $G^{(i)} = \tilde{G}/C_{i+1}(\tilde{G})$ やその部分群に適用してゆくのであるがその前に 1 つ補題を述べておく：

補題 4. 任意の $d \geq 0$ に対し，次をみたす $n_2 \geq 0$ が存在する：
任意の正規部分群 $N \subseteq G^{(i)}$ に対して，$(G^{(i)})^{[p^{n_2}]}$ の元は N/N^{p^d} に共役で自明に作用する．

この補題も補題 2 と同様の群論的議論で容易に示される．

以上の準備の下で (B) を示そう．補題 2 と命題 3 系より，与えられた $a \geq 0$ に対して n が十分大きいときには $R_n^{(i)} \subseteq (G^{(i)})^{[p^a]}$ となることが分かる．このとき，a を十分大きく取っておけば $x, y \in R_n^{(i)}$ に対し，

$$[x,y] = x^{-1}(y^{-1}xy) \in x^{-1}(x(R_n^{(i)})^{p^{1+3e}}) \subseteq (R_n^{(i)})^{[p^{1+2e}]}$$

$(e = e(i)$ は命題 3 の定数) が補題 4 と命題 3 系より示される．よって

$$[R_n^{(i)}, R_n^{(i)}] \subseteq (R_n^{(i)})^{p^{1+2e}} \subseteq (R_n^{(i)})^{[p^{1+e}]}$$

が再び命題 3 系より分かる．従って，任意の $r, s \in R_n^{(i)}$ に対して

$$r^p s^p \in (rs)^p[R_n^{(i)}, R_n^{(i)}] \subseteq (rs)^p (R_n^{(i)})^{[p^{1+e}]} \subseteq (R_n^{(i)})^{[p]}$$

が命題 3 より出るで，結局

$$(R_n^{(i)})^p = (R_n^{(i)})^{[p]} \tag{7}$$

が n が十分大きいときには成立する．さて，補題 3 と (7) より

$$Y_{n+1}^{(i)} \subseteq C_i(G^{(i)}) \cap (R_n^{(i)})^{[p]}$$

であるから，任意の $y \in Y_{n+1}^{(i)}$ は $y = r^p$, $r \in R_n^{(i)}$ と書ける．ここで $G^{(i)}/C_i(G^{(i)})$ に非自明な捩れ元が存在しない と仮定すれば $y = r^p \in C_i(G^{(i)})$ より，$r \in C_i(G^{(i)})$ が出るので $y = r^p \in (C_i(G^{(i)}) \cap R_n^{(i)})^p = (Y_n^{(i)})^p$ となり，(B) が証明される．一般の場合についても，もう少し議論をすれば同様に (B) が示されて，非アーベル岩澤公式の証明が完結する．

さて，上の証明により $Y_n^{(i)}$ の挙動が (3) のようになることが明らかになり，$X_n^{(i)}$ の挙動も

$$X_n^{(i)} \simeq X^{(i)}/(Y_{n_0}^{(i)})^{p^{n-n_0}} \quad (n \geq n_0)$$

となることが分かった．それでは，$R_n^{(i)}$ や $G_n^{(i)}$ の挙動はどうであろうか？ $R_n^{(i)}$ に関しては，非アーベル岩澤公式の証明では補題 3 で十分であったがもう少し議論するとより強く次のことが分かる：

命題 4. $i \geq 1$ に対し，

$$\exists l_0 = l_0^{(i)} \geq 0 : R_m^{(i)} = (R_n^{(i)})^{p^{m-n}} = (R_n^{(i)})^{[p^{m-n}]} \text{ for } m \geq n \geq l_0$$

従って，

$$G_n^{(i)} \simeq G^{(i)}/R_{l_0}^{p^{n-l_0}} \text{ for } n \geq l_0$$

となる．

$i=1$ の場合では (2) より,

$$G_n^{(1)} = X_n \simeq X/p^{n-n_0}Y_{n_0} \quad (n \geq n_0)$$

であったから, 上の命題よりこれの類似が非アーベルガロワ群 $G_n^{(i)}$ についても成立しているとみることができる. このように非アーベル岩澤公式の証明は非アーベル不分岐 p-拡大のガロワ群 $G_n^{(i)}$ の位数のみならず, その構造の n を動かしたときの挙動もある程度教えてくれる.

4. 今後の課題

非アーベル岩澤公式の証明を読んでみると, $\mathbf{Z}_p$-拡大 K/k の数論を全くと言ってよいほど使っていないことが分かる (強いて使っている箇所を言えば, 命題 2(i) を導く所と, 有限次代数体上の最大不分岐アーベル p-拡大の有限次性ぐらいであろう). これはオリジナルの岩澤公式の証明についても言えることであり, 一度命題 2 を導いてしまった後は, 純群論的に事が運ぶのである. 振り返ってみれば, これが非アーベル岩澤公式を証明できたことの主要因と考えられる. 更に言えば, Λ-加群の構造定理も使われておらず「Γ が作用する pro-p-群」を扱うという立場で証明が与えられている.

しかし, $\mu > 0$ の場合も含む一般の場合に $X_n^{(i)}$ 乃至は $G_n^{(i)}$ の挙動を調べることは, 先の証明の手法では未だ困難である. より数論的な異なる手法で, 特殊な $\mu > 0$ なる $\mathbf{Z}_p$-拡大については次のような $\#X_n^{(2)}$ の公式が得られているが, これはオリジナルの岩澤公式とは随分と形が異なっている ([2], [3] 参照):

定理 2. K/k を次を満たす $\mathbf{Z}_p$-拡大 $(p \neq 2)$ とする:
(i) K/k の岩澤加群 X が $(\Lambda/p)^{\oplus\mu}$ と同型, (このとき $\mu(K/k) = \mu$),
(ii) K の p 上の素点は唯 1 つ.
このとき, ある非負整数 $\kappa(K/k)$ と整数 $\nu^{(2)}(K/k)$ が存在して, 十分大なるすべての n について

$$\#X_n^{(2)} = p^{(\frac{\mu p^n - 1}{2}\mu)p^n - \kappa(K/k)p^n + \nu^{(2)}(K/k)}$$

が成立する.

もしも $\Gamma \simeq \mathbf{Z}_p$ が作用している pro-p 群 G で降中心列が有限で切れるものに対して, 何らかの一般的な構造定理が得られるならば, 先の $\mu = 0$ の場合の証明も見通しの良いものが与えられて, さらには一般の場合の公式も得られるかもしれない (その場合には定理 2 が示唆するように, $\kappa(K/k)$ に相当する新しい構造不変量も登場するに違いない). 実際に G がアーベル群の場合には, 岩澤 [1] においてこれが実行されて岩澤公式が証明されたのである (それが後の Λ-加群の構造定理). 今後はそのようなことも視野に入れた研究が進められてゆくと良いと考える.

References

[1] K.Iwasawa, On Γ-extensions of algebraic number fields, *Bull. Amer. Math. Soc.* **65** (1959), 183-226.
[2] 尾崎 学, $\mathbf{Z}_p$-拡大の非アーベル岩澤理論, 数理解析研究所講究録 **1256** (2002), 25–37.
[3] M.Ozaki, Non-abelian Iwasawa theory for $\mathbf{Z}_p$-extensions, submitted
[4] L.C. Washington, Introduction to Cyclotomic Fields (2nd. edition) (GTM 83), Springer-Verlag, New York, 1997