Galois コホモロジーの
類体論における諸問題への応用について

半内 広貴

新潟大学大学院自然科学研究科博士前期課程
数理物質科学専攻

概要

本論文は, 著者が修士の 2 年間のセミナーを通して学んできた内容を中心に, それに関係するいくつかの問題についてまとめたものである.

代数体 k に対して, k の最大不分岐 Abel 拡大は Hilbert 類体とよばれる. k の Hilbert 類体 H に対しては, H の k 上の拡大次数 $[H : k]$ が k の類数と等しくなり, k のイデアル類群は H/k の Galois 群と同型であることが知られている. これだけでも Hilbert 類体は大変興味深い対象であるが, さらに k のイデアルを Hilbert 類体へと延長すれば, すべて単項イデアルとなるという著しい性質を持つ. ここに k のイデアルとは k の整数環のイデアルをいう. この結果は単項化定理とよばれている. D. Hilbert は, Hilbert 類体の存在や単項化定理を含むいくつかの結果を予想した. 高木貞治氏や E. Artin らの活躍により, Hilbert が予想したものよりも一般的な類体論が整備され, この類体論により単項化定理は群論的な問題へと帰着され, 1930 年に Ph. Furtwängler により証明された.

本論文では, Galois コホモロジーを用いた議論を展開し, Galois コホモロジーにおけるもっとも重要な結果の一つである Hilbert 90 を示した. それを用いて単項化定理や単項化定理の出発点となった定理の Hilbert 94 の証明をまとめた. 本論文は 4 つの章からなる:

第 1 章では, 無限次 Galois 理論と副有限群に関する諸事実を述べた. これらに関しては, 1 つにまとまって詳しく説明されているものが日本語ではあまり見つからないので, 特に詳細な証明をつけることを心がけた. また, 章の最後に特徴的な副有限群の例をいくつか挙げた.

第 2 章では, Hilbert 94 を証明するための準備として群のコホモロジーの定義を行い, Hilbert 90 とその応用として Kummer 理論を紹介した. なお副有限群のコホモロジーは有限群のコホモロジーの射影極限により表すことができ, この章で扱うコホモロジーに関する命題は副有限群のコホモロジーにおいても成立する. この観点から, ここでは議論の簡略化のため, 主に有限群のコホモロジーを扱っている.

第 3 章では, まず Hilbert 90 を用いて Hilbert 94 の証明を行う. その後 Hilbert 94 と単項化定理の関係に触れ, 単項化定理の証明を述べる. 初めは議論は長くなるが中身

がある程度見やすいように純代数的な証明を行い, その後オーギュメンテイションイデアルを用いた簡潔な証明も行っている. この比較は本論文の特色でもある. なお証明は [足立・三宅], [ノイキルヒ] を参考にしている. 章の最後には, 寺田文行氏による 1949 年の一般化と鈴木浩志氏による 2001 年のさらなる一般化についても紹介し, それらのつながりについても説明した.

第 4 章では, 単項化定理と関係する問題として類体塔問題について紹介し, それに関して既知の結果や今後の展望について述べている.

謝辞

指導教員である星明考先生には, 学部を含めて 3 年間の研究室でのセミナーにおいて本当に丁寧にご指導していただき, 研究のことだけに限らず様々な場面で貴重な助言をいただきました. また, 本論文をまとめるにあたり, 数学的な面以外にも精神的な面についても多くの励ましの言葉をいただきました. ここに心から感謝いたします.

研究室の先輩である金井和貴先輩, 池田愛輝先輩には学部の頃からセミナーを見ていただき, たくさんのアドバイスをいただきました. また数学的な議論だけでなく, コンピューターに不慣れな私に, 文書の作成の方法に至るまで様々な場面において親身に相談に乗っていただきました. 深く感謝いたします.

また, 私の拙いセミナーにも参加し議論を交わしてくださった研究室の後輩の池田瑠伽君, 髙橋和暉君, 渡邊崇弘君にも感謝いたします.

最後に, どのような状況においても常に見守り支えてくれた家族に, 心からの感謝を申し上げます.

目次

1 無限次 Galois 理論 1

1.1 位相群 1

1.2 無限次 Galois 理論 5

1.3 副有限群 8

1.4 副有限群のいくつかの例 15

2 有限群のコホモロジーと Hilbert 90 18

2.1 G 加群の概念 18

2.2 有限群のコホモロジーの定義 20

2.3 コホモロジー群における加群の変更と長完全列 23

3 Hilbert 94 と単項化定理 29

3.1 準備：類体論の復習 29

3.2 Hilbert 94 と単項化定理 34

4 類体塔問題と今後の展望 49

4.1 類体塔問題 49

1　無限次 Galois 理論

1.1　位相群

この節では, 無限次 Galois 理論を記述する上で欠かすことのできない位相群についての定義と基本的な性質を紹介する. なおこの節では主に [足立], [松坂] を参考にしている.

定義　群 G が次を満たすとき, G を**位相群** (topological group) とよぶ :

(T1) G は位相空間である. (このとき G の位相を $\mathcal{O}_G$ で表す. また, 混同の心配のない場合は G を省略する.)

(T2) 次の 2 つの写像

$$\Phi : G \times G \to G \ , \ (x, y) \mapsto xy,$$
$$\Psi : G \to G \ , \ x \mapsto x^{-1}$$

がともに連続である.

例 1.1 任意の群は離散位相, すなわち全ての部分集合を開集合とする位相に関して位相群となる. これを**離散群** (discrete group) とよぶ.

例 1.2 $\mathbb{R}$, $\mathbb{R}^\times$ は $\mathbb{R}$ における通常の位相に関して位相群となる.

注意　有限群は通常, 離散位相を入れることでコンパクトな離散群とみなす.

命題 1.3 ([足立, p. 179]) 条件 (T2) は, 次の 2 条件がなりたつことと同値である :

(a) $U \in \mathcal{O}$, $x, y \in G$ に対し, 次がなりたつ :
$xy \in U$ ならばある $V, W \in \mathcal{O}$ が存在し, $x \in V$ かつ $y \in W$ かつ $VW \subset U$ となる.

(b) $U \in \mathcal{O}$, $x \in G$ に対し, 次がなりたつ :
$x^{-1} \in U$ ならばある $V \in \mathcal{O}$ が存在し, $x \in V$ かつ $V^{-1} \subset U$ となる.

証明　(T2) において, Φ の連続性と (a) が, Ψ の連続性と (b) が同値であることを示す.

(T2) において Φ が連続であることは, $U \in \mathcal{O}_G,\ x,\ y \in G$ に対し,

$$xy \in U \text{ ならばある } U_1 \in \mathcal{O}_{G\times G} \text{が存在して}, (x,y) \in U_1, \Phi(U_1) \subset U \text{ がなりたつ.} \quad (1)$$

と言い換えられることに注意しておく.

Φ が連続であるとする. $U \in \mathcal{O}_G,\ x,\ y \in G$ に対し $xy \in U$ とすると, 上で注意したことから $(x,y) \in U_1,\ \Phi(U_1) \subset U$ を満たす $U_1 \in \mathcal{O}_{G\times G}$ がとれる. 直積位相の定義から

$$U_1 = \bigcup_{\lambda\in\Lambda} (V_\lambda \times W_\lambda)\ ,\ V_\lambda,\ W_\lambda \in \mathcal{O}_G$$

と書けるので, ある $\lambda \in \Lambda$ に対して $x \in V_\lambda,\ y \in W_\lambda$ となる. さらに

$$V_\lambda W_\lambda = \Phi(V_\lambda \times W_\lambda) \subset \Phi(U_1) \subset U$$

となり, (a) がなりたつ.

逆に (a) がなりたつとすると, $U \in \mathcal{O}_G$ に対して $U_1 = V \times W$ とすれば (1) がいえるので, Φ が連続であることと (a) は同値となる.

さらに $\Psi(x) = x^{-1},\ \psi(V) = V^{-1}$ に注意すれば, Ψ が連続であることと (b) の同値がいえる. □

命題 1.4 G を位相群とする. このとき G の任意の部分群 H は相対位相 (すなわち $\mathcal{O}_H = \{H \cap O \mid O \in \mathcal{O}_G\}$ を開集合とする位相) に関して位相群となる. つまり, 位相群の部分群は自然に位相群となる.

証明　連続写像の制限は再び連続写像となることから従う. □

定義　G を位相群とする. G の部分群 H について, H が閉集合のとき H を**閉部分群** (closed subgroup) とよぶ. 同様に, H が開集合のとき H を**開部分群** (open subgroup) とよぶ.

命題 1.5 [足立, p. 180] G を位相群とする. このとき G の任意の開部分群はまた閉部分群

となる.

証明　H を G の開部分群とし, $\overline{H} = H$ を示す. ここに $\overline{H}$ は H の位相空間における閉包である. 任意の $a \in \overline{H}$ について, 特に $a \in G$ であるので次の写像

$$f_a : G \to G \ , \ x \mapsto xa$$

は同相写像となる. よって $f_a^{-1}(Ha) = H, \ (f_a^{-1})^{-1}(H) = Ha$ から, Ha は開集合となる. Ha は a を含む開集合なので, $a \in \overline{H}$ より $Ha \cap H \neq \emptyset$ となり, $y = xa$ なる H の元 x, y がとれる. よって $a = x^{-1}y \in H$ となり, $H = \overline{H}$ となる. □

定理 1.6 (**位相の生成**) G を群とし, e を G の単位元とする. e を含む G の部分集合の族 $\mathcal{B}_0$ が以下を満たすとする :

(a) $U, \ V \in \mathcal{B}_0$ ならば $U \cap V \in \mathcal{B}_0$;
(b) $U \in \mathcal{B}_0$ ならばある $V \in \mathcal{B}_0$ が存在し, $V^{-1} \subset U$;
(c) $U \in \mathcal{B}_0$ ならばある $V, W \in \mathcal{B}_0$ が存在し, $VW \subset U$;
(d) $U \in \mathcal{B}_0$ ならば任意の $g \in G$ に対してある $V \in \mathcal{B}_0$ が存在し, $gV \subset U$;
(e) $U \in \mathcal{B}_0$ ならば任意の $g \in G$ に対してある $V \in \mathcal{B}_0$ が存在し, $gVg^{-1} \subset U$.

このとき,

$$\mathcal{B} := \{gU \mid g \in G, \ U \in \mathcal{B}_0\}$$

により G の位相が生成され, これにより G は位相群となる.

証明　まず, 位相空間論の一般論から $\mathcal{B}$ から生成される G の位相は

$$\bigcup_{\lambda \in \Lambda} (\bigcap_{i=1}^{n_\lambda} B_{\lambda_i}) \ \ (B_{\lambda_i} \in \mathcal{B}, \ n_\lambda \in \mathbb{N})$$

なる G の部分集合と $\{\phi, \ G\}$ の合併からなる. これが位相群の定義の条件 (T2) を満たすことを示す.

まず $a \in G$ に対し,

$$a \in \bigcap_{i=1}^{n} a_i U_i,\ a_i \in G,\ U_i \in \mathcal{B}_0 \text{ならば, ある } V \in \mathcal{B}_0 \text{が存在し } aV \subset \bigcap_{i=1}^{n} a_i U_i \qquad (2)$$

がなりたつ.

$a,\ b \in G,\ U \in \mathcal{B}_0$ に対し, 条件 (c) から $VW \subset U$ を満たす $V,\ W \in \mathcal{B}_0$ が存在する. 一方条件 (e) を $V \in \mathcal{B}_0,\ b^{-1} \in G$ に適用することで, $b^{-1}V_1 b \subset V$ を満たす $V_1 \in \mathcal{B}_0$ を得る. よって $b^{-1}V_1 bW \subset U$ となり,

$$aV_1 bW \subset abU \qquad (3)$$

を得る. したがって $U' = \bigcup_{\lambda\in\Lambda}(\bigcap_{i=1}^{n_\lambda} B_{\lambda_i})$ $(B_{\lambda_i} \in \mathcal{B})$ を G の開集合とすれば, (1), (2) から

$$xy \in U' \text{ならば, } xV_1 yW \subset U'$$

となり, $x \in xV_1,\ y \in yW,\ xV_1 yW \subset U'$ を満たす $V_1,\ W \in \mathcal{B}_0$ の存在, つまり命題 1.3 の (a) がいえた.

次に命題 1.3 (b) がなりたつことをを示す. 条件 (e) から, $a \in G,\ U \in \mathcal{B}_0$ に対し, $aVa^{-1} \subset U$ を満たす $V \in \mathcal{B}_0$ が存在する. 一方条件 (b) から $W^{-1} \subset V$ を満たす $W \in \mathcal{B}_0$ が存在する. $aW^{-1}a^{-1} \subset U$ なので

$$(aW)^{-1} \subset a^{-1}U \qquad (4)$$

となる. よって $U' = \bigcup_{\lambda\in\Lambda}(\bigcap_{i=1}^{n_\lambda} B_{\lambda_i})$ $(B_{\lambda_i} \in \mathcal{B})$ を G の開集合とすれば, (1), (3) から $x^{-1} \in U'$ ならば $(xW)^{-1} \subset U'$ となる. したがって $x \in xW,\ (xW)^{-1} \subset U'$ を満たす $W \in \mathcal{B}_0$ の存在, つまり命題 1.3(b) がいえた. □

最後に, 次節の準備として Krull 位相とよばれる標準的な位相の定義を与える.

定義 G を群とする. $\mathcal{N} := \{N \triangleleft G \mid (G : N) < \infty\}$ は定理 1.6 の条件を満たす.
$\mathcal{B} := \{gN \mid g \in G,\ N \in \mathcal{N}\}$ により生成される G の位相を **Krull 位相** (Krull topology)

とよぶ.

1.2 無限次 Galois 理論

Ω/k を必ずしも有限次とは限らない Galois 拡大とする.

$G := \mathrm{Gal}(\Omega/k)$ に Krull 位相を入れる:

$$\mathcal{K} := \{K \mid K \text{ は } \Omega/k \text{ の有限次 Galois 部分拡大体 }\},$$
$$\mathcal{N} := \{N \lhd G \mid (G : N) < \infty\} = \{\mathrm{Gal}(\Omega/K) \mid K \in \mathcal{K}\}.$$

Krull 位相の作り方から, $\sigma \in G$ の基本近傍系は

$$\mathcal{O} := \{\sigma \mathrm{Gal}(\Omega/K) \mid K \in \mathcal{K}\}$$

となる.

注意 $\alpha \in \Omega$ に対し, $k(\alpha)/k$ の Galois 閉包を $\overline{k(\alpha)}$ とかけば $\alpha \in \overline{k(\alpha)} \in \mathcal{K}$ より, $\Omega = \bigcup_{K \in \mathcal{K}} K$ となる.

以降, この節では G は上記の設定のものとする.

命題 1.7 ([ノイキルヒ, p. 270]) G は Krull 位相に関して Hausdorff かつコンパクトな位相群である.

証明 まず Hausdorff であることを示す. $\sigma, \tau \in G$, $\sigma \neq \tau$ とすると, 上の注意から $\sigma|_K \neq \tau|_K$ なる $K \in \mathcal{K}$ が存在する. $\sigma \in \sigma\mathrm{Gal}(\Omega/K) \in \mathcal{O}$, $\tau \in \tau\mathrm{Gal}(\Omega/K) \in \mathcal{O}$, $\sigma\mathrm{Gal}(\Omega/K) \cap \tau\mathrm{Gal}(\Omega/K) = \emptyset$ より G は Hausdorff である.

次にコンパクトであることを示す. 以下のような写像を考える:

$$h : G \to \prod_{K \in \mathcal{K}} \mathrm{Gal}(K/k)\ ,\ \sigma \mapsto \prod_{K \in \mathcal{K}} \sigma|_K\ .$$

各 $\mathrm{Gal}(K/k)$ は有限群なのでコンパクト離散群である. よって

定理 1.8 (**Tikhonov の定理**) Λ を任意の濃度の集合とし, $\{X_\lambda\}_{\lambda \in \Lambda}$ をコンパクト空間

の族とする. このとき, 直積空間 $\prod_{\lambda\in\Lambda} X_\lambda$ は直積位相に関してコンパクト空間となる.

より, $\prod_{K\in\mathcal{K}} \mathrm{Gal}(K/k)$ もコンパクトとなる. よって G と $h(G)$ が同相かつ $h(G)$ が $\prod_{K\in\mathcal{K}} \mathrm{Gal}(K/k)$ の閉部分群であることを示せばよい.

まず G と $h(G)$ が同相であることを示す. h は準同型写像であり, 先の注意から $\sigma \in G$ に対して

$$h(\sigma) = 1 \Leftrightarrow \prod_{K\in\mathcal{K}} \sigma|_K = 1 \Leftrightarrow \sigma|_K = 1 \ (\forall K \in \mathcal{K}) \Leftrightarrow \sigma = 1$$

がなりたつ. よって h は単射であり, したがって $h : G \to h(G)$ は全単射である.

$$U := \{ \prod_{K\neq K_0} \mathrm{Gal}(K/k) \times \{\overline{\sigma}\} \mid K_0 \in \mathcal{K},\ \overline{\sigma} \in \mathrm{Gal}(K_0/k)\}$$

とすれば, U は $\prod_{K\in\mathcal{K}} \mathrm{Gal}(K/k)$ の部分基となる. $h^{-1}(\overline{\sigma}) =: \sigma(\in G)$ とすると, 任意の $\tau \in \mathrm{Gal}(\Omega/K_0)$ に対して, $\sigma\tau|_{K_0} = \sigma|_{K_0} = \overline{\sigma}$ かつ $\sigma\tau \in \mathrm{Gal}(K/k)$ となる. よって

$$\sigma\mathrm{Gal}(\Omega/K_0) \subset h^{-1}(\prod_{K\neq K_0} \mathrm{Gal}(K/k) \times \{\overline{\sigma}\})$$

となる. 一方任意の $\tau \in h^{-1}(\prod_{K\neq K_0} \mathrm{Gal}(K/k) \times \{\overline{\sigma}\})$ に対して, $\tau|_{K_0} = \overline{\sigma},\ \tau|_{K\neq K_0} \in \mathrm{Gal}(K/k)$ となることから $\sigma^{-1}\tau \in \mathrm{Gal}(\Omega/K_0)$ となり, $\tau = \sigma(\sigma^{-1}\tau) \in \mathrm{Gal}(\Omega/K_0)$ となる. したがって,

$$h^{-1}(\prod_{K\neq K_0} \mathrm{Gal}(K/k) \times \{\overline{\sigma}\}) = \sigma\mathrm{Gal}(\Omega/K_0)$$

となる. $\sigma\mathrm{Gal}(\Omega/K_0)$ は G の開集合であるので, h は連続である. さらに, $\sigma\mathrm{Gal}(\Omega/K_0) \subset G$ より $h(\sigma\mathrm{Gal}(\Omega/K_0)) = h(G) \cap (\prod_{K\neq K_0} \mathrm{Gal}(K/k) \times \{\overline{\sigma}\})$ は $h(G)$ の開集合である. よって h は開写像となり, 全単射性と連続性とあわせて同相写像となる.

最後に $h(G)$ が $\prod_{K\in\mathcal{K}} \mathrm{Gal}(K/k)$ 内の閉集合であることを示す. $L,\ L' \in \mathcal{K},\ L \subset L'$ に対して,

$$M_{L'/L} := \{ \prod_{K\in\mathcal{K}} \sigma|_K \mid (\sigma|_{L'})|_L = \sigma|_L \}$$

とすれば, 任意の $L, L' \in \mathcal{K}$ と任意の $\sigma \in G$ に対し $(\sigma|_{L'})|_L = \sigma|_L$ となるので,

$$h(G) = \bigcap_{L\subset L'} M_{L'/L}$$

となる. ここで, $\mathrm{Gal}(L/K) := \{\sigma_1, \cdots, \sigma_n\}$ とし, 各 σ_i の L' への延長のなす集合を S_i とすれば, $\mathrm{Gal}(K/k)$, $\mathrm{Gal}(L/k)$, $\mathrm{Gal}(L'/k)$ において $\mathrm{Gal}(K/k)$, $\{\sigma_i\}$, S_i はそれぞれ閉集合となる. よって $\prod_{K\neq L,L'} \mathrm{Gal}(K/k) \times S_i \times \{\sigma_i\}$ は $\prod_{K\in\mathcal{K}} \mathrm{Gal}(K/k)$ 内の閉集合となり, したがって $M_{L'/L} = \bigcup_{i=1}^{n} (\prod_{K\neq L,L'} (\mathrm{Gal}(K/k) \times S_i \times \{\sigma_i\})$ も $\prod_{K\in\mathcal{K}} \mathrm{Gal}(K/k)$ 内の閉集合となる. ゆえに $h(G)$ は $\prod_{K\in\mathcal{K}} \mathrm{Gal}(K/k)$ 内の閉集合である. □

定理 1.9 (**Galois の基本定理** [ノイキルヒ, p. 271]) Ω/k を必ずしも有限次とは限らない Galois 拡大, G をその Galois 群とする.

$$\mathcal{M} := \{K \mid k \subset K \subset \Omega\},\ \mathcal{H} := \{H \mid H \text{ は } G \text{ の閉部分群 }\}$$

とするとき, $\mathcal{M}$ と $\mathcal{H}$ の間の対応

$$\Phi : K \mapsto \mathrm{Gal}(\Omega/K)$$

は 1 対 1 の対応である. さらに, G の開部分群は Ω/k の有限次部分拡大体と対応する.

証明 $K \in \mathcal{M}$ に対し K/k の Ω における Galois 閉包を $\overline{K}$ とすれば $\overline{K} \in \mathcal{K}$ であり, $\sigma \in G$ に対して $\sigma \in \sigma\mathrm{Gal}(\Omega/\overline{K}) \subset \mathrm{Gal}(\Omega/K)$ となる. よって $\mathrm{Gal}(\Omega/K)$ は G の開部分群となり, 命題 1.5 から閉部分群となる. したがって, $\mathrm{Gal}(\Omega/K) \in \mathcal{H}$ である.

K は $\mathrm{Gal}(\Omega/K)$ の不変体なので, 有限次のときと同様に Φ は単射となる.

次に Φ が全射であることを示す. これは任意の $H \in \mathcal{H}$ に対し, H の不変体 K が $\mathrm{Gal}(\Omega/K) = H$ を満たすことを示せばよい. $H \subset \mathrm{Gal}(\Omega/K)$ は明らかなので, 逆を示す.

$\sigma \in \mathrm{Gal}(\Omega/K)$ とする. L/K を Ω/K の有限次 Galois 部分拡大とすると, $\sigma \in \sigma\mathrm{Gal}(\Omega/L) \subset \mathrm{Gal}(\Omega/K)$ である. ここで次の写像

$$\chi : H \to \mathrm{Gal}(L/K),\ \rho \mapsto \rho|_L$$

を考える. $\chi(H)$ の不変体は K であるので, 有限次の場合の Galois 理論から $\chi(H) = \mathrm{Gal}(L/K)$ となる. よって χ は全射である. したがって $\tau|_L = \sigma|_L$ なる $\tau \in H$ が存在する. $\sigma^{-1}\tau \in \mathrm{Gal}(\Omega/L)$ となるので, $\tau \in H \cap \sigma\mathrm{Gal}(\Omega/L)$ となる. σ は H の $\mathrm{Gal}(\Omega/L)$ における閉包の元であり, H は G の閉部分群であることから $\sigma \in H$ となるので, $H = \mathrm{Gal}(\Omega/K)$ となる. したがって Φ は全射となる.

最後に H を G の開部分群とすれば, 命題 1.5 より H は閉部分群でもあり, H の不変体 K により $H = \mathrm{Gal}(\Omega/K)$ とかける. $\mathrm{Gal}(\Omega/k)$ の H による剰余類分解を考えれば, これはコンパクト空間 $\mathrm{Gal}(\Omega/k)$ の開被覆なのでこれらのうちの有限個で $\mathrm{Gal}(\Omega/k)$ を覆うことができる. ゆえに K/k は有限次である. □

1.3 副有限群

前節において無限次の Galois 群の特徴について触れたが, ここではその特徴を一般化し次の定義を与える. なおこの節では [足立], [松坂], [ノイキルヒ], Neukirch-Schmidt-Wingberg [NSW] を特に参考にしている.

定義 位相群 G が Hausdorff かつコンパクトであり, さらに正規開部分群からなる単位元の基本近傍系を持つとき, G を**副有限群** (pro-finite group) とよぶ.

副有限群を特徴づけるために, 射影系の概念を復習する.

定義 $(I, \leq)$ を順序集合とする. 任意の $i, j \in I$ に対して $i \leq k$ かつ $j \leq k$ を満たす $k \in I$ が存在するとき, $(I, \leq)$ を**有向集合** (directed set) という.

定義 $(I, \leq)$ を有向集合とする. 位相空間の列 $\{X_i\}$ とその間の連続写像 $f_{ij} : X_j \to X_i$ $(i \leq j)$ の組 $\{X_i,\ f_{ij} \mid i,\ j \in I,\ i \leq j\}$ について,

(1) $f_{ii} = \mathrm{id}_{X_i}$;
(2) $i \leq j \leq k$ ならば $f_{ik} = f_{ij} \circ f_{jk}$

の 2 条件がなりたつとき, この組を I についての**射影系** (projective system) とよぶ.

定義 $\{X_i,\ f_{ij}\}$ を射影系とする.

$$X := \{(x_i)_{i\in I} \mid f_{ij}(x_j) = x_i\ (i \le j)\}\ \ (\subset \prod_{i\in I} X_i)$$

を $\{X_i,\ f_{ij}\}$ の**射影極限** (projective limit) とよび,

$$X = \varprojlim_{i\in I} X_i$$

と表す.

例 1.10 $(X,\ \mathcal{O})$ を位相空間, $\{X_i\}_{i\in I}$ を X の部分集合の族とする. さらに, 次を仮定する:

$$X_i,\ X_j \in \{X_i\}_{i\in I} \text{ ならば, } X_i \cap X_j \in \{X_i\}_{i\in I}.$$

このとき, I における順序 $\le$ を $X_j \subset X_i$ ならば $i \le j$ と定めることにより, $(I,\ \le)$ は有向集合となる. $i \le j$ に対して, 包含写像 $f_{ij} : X_j \to X_i,\ f_{ij}(x_j) = x_j$ を考えれば, $\{X_i,\ f_{ij}\}$ は I についての射影系である. 仮定に注意すれば,

$$X = \varprojlim_{i\in I} X_i = \{(x_i)_{i\in I} \mid f_{ij}(x_j) = x_i\ (i \le j)\} = \{(x_i)_{\imath\in I} \mid x_i = x_j\ (i \le j)\} = \bigcap_{i\in I} X_i$$

とみなせる.

命題 1.11 ([ノイキルヒ, p. 274]) $\{X_i,\ f_{ij}\}$ を射影系とする. このとき, 各 X_i が Hausdorff 空間ならば射影極限 $X = \varprojlim_{i\in I} X_i$ も Hausdorff 空間となり, さらに $\prod_{i\in I} X_i$ の閉部分空間となる.

証明 各 X_i が Hausdorff 空間なので, $\prod_{i\in I} X_i$ は直積位相に関して Hausdorff 空間となる. よって部分空間として X も Hausdorff 空間となる.

閉部分空間であることを示す. $i \le j$ に対して

$$X_{ij} := \{(x_k)_{k\in I} \mid f_{ij}(x_j) = x_i\}$$

とおけば, $X = \bigcap_{i \leq j} X_{ij}$ となる. よって各 X_{ij} が $\prod_{i \in I} X_i$ 内の閉集合であることを示せばよい. i 番目の射影を $p_i : \prod_{k \in I} X_k \to X_i$ とかき, $f := f_{ij} \circ p_j$ とかけば, $p_i,\ f$ は連続であり,

$$X_{ij} = \{(x_k)_{k \in I} \mid p_i(x_k)) = f((x_k))\}$$

と書くことができる. 今 $\prod_{i \in I} X_i$ は Hausdorff 空間なので, このような集合は閉集合である. 以上より, $X = \bigcap_{i \leq j} X_{ij}$ は $\prod_{i \in I} X_i$ 内の閉集合となる. □

$X = \bigcap_{i \leq j} X_{ij}$ という表示から次の命題を得る.

命題 1.12 ([ノイキルヒ, p. 274]) $\{X_i,\ f_{ij}\}$ を射影系とする. このとき, 各 $i \in I$ について X_i が空でないコンパクトな Hausdorff 空間であるならば $X = \varprojlim_{i \in I} X_i$ も空でないコンパクト空間となる.

証明 Tikhonov の定理から $\prod_{i \in I} X_i$ はコンパクト空間なので, 命題 1.11 より X もコンパクトとなる.

$X \neq \emptyset$ であることを背理法を用いて示す. $X = \emptyset$ とすると, $\prod_{i \in I} X_i$ はコンパクトであり, かつ $X = \bigcap_{i \leq j} X_{ij} = \emptyset$ となる. ここで X_{ij} は命題 1.11 の証明中のものである. よって X は有限交叉性をもたない, つまり共通部分が空であるような有限個の X_{ij} を選ぶことができる. $(I,\ \leq)$ が有向集合であることに注意すれば, ここで選ばれたすべての添え字 i について, $i \leq n$ を満たす $n \in I$ がとれる. ここで $x_n \in X_n\ (\neq \emptyset)$ とし, $k \in I$ について

$$x_k = \begin{cases} f_{kn}(x_n) & (k \leq n), \\ \text{任意} & (k > n) \end{cases}$$

とすれば $(x_k)_{k \in I}$ は上で選んだ X_{ij} の共通部分に含まれ, これは矛盾である. □

ここからは, 位相群 G_i とその間の連続開準同型 $f_{ij} : G_j \to G_i\ (i \leq j)$ による射影系を考える. このとき, 射影極限 $G = \varprojlim_{i \in I} G_i$ は $\prod_{i \in I} G_i$ の部分群となる.

命題 1.13 ([足立, p. 181]) G を位相群とし, その単位元 e の連結成分を N とする. このとき, N は G の正規閉部分群である. さらに, 任意の $a \in G$ の連結成分は aN となる.

証明 まず N は e の連結成分なので閉集合である. 同相写像 $f_a : G \to G\ ,\ x \mapsto ax$ を考えれば, $aN = f_a(N)$ は a を含む連結集合であり, a の連結成分を N' とかけば, $aN \subset N'$ である. 同様に, 同相写像 $f_{a^{-1}} : G \to G\ ,\ x \mapsto a^{-1}x$ を考えれば $a^{-1}N \subset N'$ となるので, $N' = aN$ を得る.

最後に N が G の正規部分群となることを示す. $m,\ n \in N$ とすると, 2 つの同相写像 $x \mapsto x^{-1},\ x \mapsto mx$ により mN^{-1} も連結となる. よって $e \in mN^{-1}$ より N の極大性から $mN^{-1} \subset N$ となるので, $mn^{-1} \in mN^{-1} \subset N$ となる. したがって $N \leq G$ となる. さらに, 任意の $x \in G$ に対し 2 つの同相写像 $a \mapsto x^{-1}a,\ a \mapsto ax$ を考えれば xNx^{-1} は連結であり, $e \in N$ より $e \in xNx^{-1}$ である. したがって $xNx^{-1} \subset N$ となるので, N は G の正規部分群である. □

定義 G の単位元 E の連結成分を **G の連結成分** (connected component of G) という.

次の定義は位相空間論における基本的な定義であるが, 以降頻繁に登場するので改めて確認しておく.

定義 位相空間 X において, 一点集合の連結成分がつねに一点集合となるとき X は**全不連結** (totally disconnected) であるという.

命題 1.14 ([足立, p. 184]) $\{G_i,\ f_{ij}\}$ を位相群による射影系とする. このとき, 各 G_i が全不連結であるならば $\prod_{i\in I} G_i$ も全不連結となる. したがって, このとき特に $G = \varprojlim_{i\in I} G_i$ も全不連結となる.

証明 $p_i : \prod_{i\in I} G_i \to G_i$ を i 番目の射影とする. G_i の単位元を e_i, $\prod_{i\in I} G_i$ の単位元を e とかき, e の連結成分を N とする. 射影の連続性から $p_i(N)$ は連結であり, $e_i \in p_i(N)$ であるので G_i が全不連結であることにより $p_i(N) = \{e_i\}$ となる. これが任意の i についてなりたつので, $N = \{e\}$.

したがって命題 1.13 から任意の $x \in \prod_{i\in I} G_i$ の連結成分は $xN = \{x\}$ となる. □

以上の議論より次を得る.

命題 1.15 ([足立, p. 184]) 位相群の射影系 $\{G_i,\ f_{ij}\}$ について, 各 G_i が全不連結かつコンパクトな Hausdorff 空間であるならば $G = \varprojlim_{i\in I} G_i$ も全不連結かつコンパクトな Hausdorff 空間となる.

系 1.16 ([足立, p. 185]) 有限群からなる位相群の射影系 $\{G_i,\ f_{ij}\}$ において, 射影極限 $G = \varprojlim_{i\in I} G_i$ は全不連結かつコンパクトな Hausdorff 空間となる.

証明 有限群は離散位相を入れた離散群であるのでよい. □

ここで全不連結に関する特徴的な事実を確認する.

命題 1.17 T をコンパクトな Hausdorff 空間とする. このとき, 以下は同値である:

(a) T は全不連結である;

(b) 任意の $t \in T$ は開集合かつ閉集合であるような集合からなる基本近傍系を持つ.

証明 (a)⇒(b) を示す. $t \in T$ を固定し

$$\mathcal{P} := \{W \subset T \mid W \text{ は開集合かつ閉集合であり}, t \in W\}$$

とする. この $\mathcal{P}$ が主張の基本近傍系となることを示す.

仮定から T はコンパクト Hausdorff 空間なので, $P := \bigcap_{W\in\mathcal{P}} W = \{t\}$ である. ここで, 任意の閉集合 $F \subset T$ に対して, F がコンパクトであることから

$$F \cap P = \emptyset \text{ ならばある } W \in \mathcal{P} \text{ が存在して}, F \cap W = \emptyset$$

がなりたつ. 今 O を t の開近傍とすれば, $P = \{t\} \subset O$ より O^c $(\subset T)$ は閉集合かつ $O^c \cap P = \emptyset$ となる. よって $O^c \cap W = \emptyset$ なる $W \in \mathcal{P}$ がとれ, $t \in W \subset O$ となる.

(a)⇐(b) を示す. $t \in T$ を固定し, その連結成分を C とかく. $x \neq t$ なる $x \in C$ が存

在すると仮定すると, T が Hausdorff 空間であることから $x \notin U$ かつ $t \in U$ なる開集合 $U \subset T$ が存在する. 仮定から U は閉集合であるとしてよい. $C \cap U$ は連結集合 C 内の開集合かつ閉集合なので $C \cap U = \emptyset$ または $C \cap U = C$ となるが, $t \in C \cap U$ かつ $x \notin C \cap U$ よりどちらの場合も矛盾する. したがって $C = \{t\}$ となる. □

次の定理により, 副有限群が特徴づけられる.

定理 1.18 ([NSW, p. 3]) G を Hausdorff な位相群とする. このとき以下は同値である:

(a) G は副有限群である, つまり G はコンパクト空間かつ正規開部分群からなる単位元の基本近傍系を持つ;

(b) ある有限群からなる射影系 $\{G_i,\ f_{ij}\}_{i \in I}$ が存在し, $G \cong \varprojlim_{i \in I} G_i$ がなりたつ;

(c) G はコンパクトかつ全不連結となる.

証明 G の単位元を e とする. (b)⇒(c) は系 1.16 よりよい.

(c)⇒(a) を示す. 命題 1.17 から, 任意の $x \in G$ は開かつ閉集合のみから成る基本近傍系を持つ. よって e の開近傍 O を任意に選べば, $e \in U \subset O$ なる e の開かつ閉近傍 U が存在する.

$$V := \{v \in U \mid Uv \subset U\}$$
$$H := \{h \in V \mid h^{-1} \in V\} = V \cap V^{-1}$$

とおく. まず H が開集合であることを示す.

$v \in V$ とすると, 任意の $u \in U$ に対して $uv \in U$ となる. G が位相群なので命題 1.3 から $u \in U_u,\ v \in V_u,\ U_u V_u \subset U$ を満たす開集合 $U_u,\ V_u$ が存在する. ここで $U = \bigcup_{u \in U} U_u$ であるが, U はコンパクトであるので $U = \bigcup_{i=1}^{n} U_{u_i}$ とできる. $V_v := V_{u_1} \cap \cdots \cap V_{u_n}$ とおけば V_v は v の開近傍であり, $UV_v \in U$ となる. よって V の定義から $V_v \subset V$ となり, V は開集合となる. したがって同相写像 $x \mapsto x^{-1}$ を考えれば $H = V \cap V^{-1}$ は開集合となる.

次に H が G の部分群であることを示す. $e \in H,\ H^{-1} = H$ はよい. $x,\ y \in H\ (\subset V)$

とすると, $Uxy \subset Uy \subset U$, $Uy^{-1}x^{-1} \subset Ux^{-1} \subset U$ より xy, $y^{-1}x^{-1} \in V$ となる. よって $xy \in H$ となり, したがって H は G の部分群である.

ここで G がコンパクトであることに注意すれば $(G : H) < \infty$ なので H の共役は有限個であり, それらの共通部分を H' とすれば H' は G の正規部分群である. H が開集合であることと $H \subset U$ であることから H' は開集合であり (よってさらに閉集合でもある), さらに $H' \subset U$ となる. よってこのような H' の全体は主張の基本近傍系をなす.

(a)⇒(b) を示す. $\{N_i\}_{i\in I}$ を G の正規開部分群全体とする. 各 i に対し, $G_i := G/N_i$ とおけば G_i は標準的な準同型写像 $x \mapsto xN_i$ による商位相に関して位相群をなす. この各 G_i が有限群であることと $G \cong \varprojlim_{i\in I} G_i$ であることを示せばよい.

まず G がコンパクトであることから G_i もコンパクトであり, N_i が開集合であることから G_i は離散的となる. よって G_i はコンパクト離散群であり, ゆえに有限群である.

次に $G \cong \varprojlim_{i\in I} G_i$ となることを示す. $i,\ j \in I$ に対して $i \leq j \overset{\text{def}}{\iff} N_j \subset N_i$ で I 上の順序を定めることにより $(I,\ \leq)$ は有向集合となる. $i \leq j$ に対し, 自然な準同型 $\varphi_{ij} : G_j \to G_i\ ,\ xN_j \mapsto xN_i$ を考えれば $\{G_i,\ \varphi_{ij}\}_{i\in I}$ は射影系をなす. $\varphi : G \to \prod_{i\in I} G_i\ ,\ x \mapsto (xN_i)_{i\in I}$ とすれば商位相と積位相の定義から φ は連続準同型写像である. ここで命題 1.12 の証明中での議論から任意の $(x_iN_i)_{i\in I} \in \varprojlim_{i\in I} G_i$ に対して $\{x_iN_i\}_{i\in I}$ は有限交叉性を持つことがわかる. $f_i : G \to G_i\ ,\ x \mapsto xN_i$ を商位相を定める連続全射準同型写像とすれば $f_i^{-1}(\{x_iN_i\}) = x_iN_i \subset G$ であり, よって $\{x_iN_i\}$ が G_i の閉集合であることと合わせて x_iN_i は G 内の閉集合となる. よって有限交叉性と G のコンパクト性から $S := \bigcap_{i\in I} x_iN_i \neq \emptyset$ となる. ここで $x \in S$ とすれば $\varphi(x) = (xN_i)_{i\in I} = (x_iN_i)_{i\in I}$ となり, したがって $\varprojlim_{i\in I} G_i \subset \varphi(G)$ となる.

一方任意の $x \in G$ をとると, $i \leq j$ ならば $\varphi_{ij}(xN_j) = xN_i$ なので $\varphi(x) = (xN_i)_{i\in I} \in \varprojlim_{i\in I} G_i$ であり, よって $\varphi(G) = \varprojlim_{i\in I} G_i$ となる. さらに仮定から e は正規開部分群のみからなる基本近傍系を持つので特に命題 1.17 での議論と合わせて $\bigcap_{i\in I} N_i = \{e\}$ となることがわかる. したがって $\varphi(x) = 1$ と $x = e$ は同値となり, φ は単射となる. ゆえに $\varphi : G \to \varprojlim_{i\in I} G_i$ は同型写像となり, 特に φ はコンパクト空間 G から Hausdorff 空

間 $\varprojlim_{i\in I} G_i$ への連続な全単射となるので同相写像となる. 以上より, $G \cong \varprojlim_{i\in I} G_i$ が示された. □

注意 定理 1.18 の証明での議論から, 副有限群 G は N_i を G の正規開部分群としたとき,

$$G \cong \varprojlim_{i\in I} G/N_i$$

と表される.

1.4 副有限群のいくつかの例

以下, 重要な副有限群の例をいくつか紹介する.

例 1.19 体 k に対し k の分離閉包を k^{sep} とかく. $G_k := \mathrm{Gal}(k^{sep}/k)$ は k の**絶対 Galois 群** (absolute Galois group) とよばれる. これは前の節での議論から Krull 位相に関して副有限群となる. (k^{sep}/k は一般には無限次拡大であるのでこれは有限群とはならない)

Krull 位相の定義から K/k が k^{sep}/k の有限次 Galois 部分拡大を走るとき $\mathrm{Gal}(k^{sep}/K)$ は G の正規開部分群を走る. このとき G は有限群 $\mathrm{Gal}(K/k)$ の射影極限

$$G \cong \varprojlim \mathrm{Gal}(K/k)$$

として表される.

k^{sep}/k はその定義から k の有限次 Galois 拡大体をすべて含んでいる. 有理数体 $\mathbb{Q}$ の絶対 Galois 群の研究, つまり $\mathbb{Q}$ の絶対 Galois 群の商群としてどのような有限群が現れるか, という問題は代数的整数論における重要な問題の一つとされている. しかしこれは非常に難しい問題であり, 未解決である.

例 1.20 p を素数とする. 環 $\mathbb{Z}/p^n\mathbb{Z}$ は射影 $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ $(n \geq m)$ に関して射影系をなす. 射影極限

$$\mathbb{Z}_p := \varprojlim_{n} \mathbb{Z}/p^n\mathbb{Z}$$

は p **進整数環** (ring of p-adic integer) とよばれる. これは有理数体 $\mathbb{Q}$ の p 進付値による完備化により得られる p 進数体 $\mathbb{Q}_p$ の整数環である.

$\mathbb{Z}_p$ を Galois 群に持つ Galois 拡大は $\mathbb{Z}_p$ **拡大** ($\mathbb{Z}_p$-extension) とよばれる. K を代数体とし,

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n \subset \cdots \subset K_\infty = \bigcup_{n \geq 0} K_n \tag{5}$$

かつ $\mathrm{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$ を満たすような体の拡大の列を考えれば,

$$\mathrm{Gal}(K_\infty/K) \cong \varprojlim_n \mathrm{Gal}(K_n/K) \cong \mathbb{Z}_p$$

となり, K_∞/K は $\mathbb{Z}_p$ 拡大となる. このように $\mathbb{Z}_p$ 拡大は p^n 次の巡回拡大を積み重ねていくことで得ることができる.

$p = 2$ ならば $q = 4$ とし, $p \neq 2$ ならば $q = p$ とおく. 円分体 $\mathbb{Q}(\zeta_{qp^n})$ の $\mathbb{Q}$ 上の Galois 群 $\mathrm{Gal}(\mathbb{Q}(\zeta_{qp^n})/\mathbb{Q})$ は $(\mathbb{Z}/qp^n\mathbb{Z})^\times \cong \mathbb{Z}/p^n\mathbb{Z} \times (\mathbb{Z}/q\mathbb{Z})^\times$ と同型である. そこで $(\mathbb{Z}/q\mathbb{Z})^\times$ の固定体を $\mathbb{Q}_n$ とかけば, $\mathbb{Q}_n$ は $\mathbb{Q}$ 上の p^n 次巡回拡大体となる. よって,

$$\mathbb{Q} = \mathbb{Q}_0 \subset \mathbb{Q}_1 \subset \mathbb{Q}_2 \subset \cdots \subset \mathbb{Q}_n \subset \cdots \subset \mathbb{Q}_\infty = \bigcup_{n \geq 0} \mathbb{Q}_n$$

とすれば, 拡大 $\mathbb{Q}_\infty/\mathbb{Q}$ は $\mathbb{Z}_p$ 拡大となり, **円分的** $\mathbb{Z}_p$ **拡大** (cyclotomic $\mathbb{Z}_p$-extension) とよばれる. 一般の代数拡大 K に対しては $K_\infty = K\mathbb{Q}_\infty$ とすれば, (5) を満たし, K 上の $\mathbb{Z}_p$ 拡大が得られる. この K_∞/K をの円分的 $\mathbb{Z}_p$ 拡大とよぶ. 任意の代数体 K は, 必ず円分的 $\mathbb{Z}_p$ 拡大を持つので, 少なくとも 1 つの $\mathbb{Z}_p$ 拡大を持つことになる.

副有限群 G について, 正規開部分群 N による商群 G/N がすべて有限 p 群であるとき, G は**副** p **群** (pro-p group) とよばれる.

例 1.21 $\mathbb{N}$ における順序を約数の関係により定める. つまり $n \geq m$ であることを $m \mid n$ であることと定義する. このとき, 環 $\mathbb{Z}/n\mathbb{Z}$ は射影 $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ $(m \mid n)$ により射影系をなす. その射影極限

$$\widehat{\mathbb{Z}} := \varprojlim_n \mathbb{Z}/n\mathbb{Z}$$

は **Prüfer 環** (Prüfer ring) もしくは**ゼットハット**とよばれる.

$\widehat{\mathbb{Z}}$ は $\mathbb{Z}$ を稠密な部分環として含む. さらに $n \in \mathbb{N}$ に対して群 $n\widehat{\mathbb{Z}}$ は $\widehat{\mathbb{Z}}$ の開部分群であり, $\widehat{\mathbb{Z}}/n\widehat{\mathbb{Z}} \cong \mathbb{Z}/n\mathbb{Z}$ がなりたつ. ここで n の素因数分解 $n = \prod_p p^{\nu_p}$ を考えれば中国式剰余定理から

$$\mathbb{Z}/n\mathbb{Z} \cong \prod_p \mathbb{Z}/p^{\nu_p}\mathbb{Z}$$

となる. よって射影極限を考えることにより,

$$\widehat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$$

がなりたつ.

2　有限群のコホモロジーと Hilbert 90

この章では, 副有限群のコホモロジー群が有限群のコホモロジー群から作られ, 位相を考慮することを除いて基本的には有限群の場合と変わらないという観点から, 有限群のコホモロジーを扱うこととする. なおこの章を通して [斎藤], [河田 1], Neukirch-Schmidt-Wingberg [NSW], Harari [Har] を主に参考にしている.

2.1　G 加群の概念

以下, 断らない限り群は全て有限群であるとする.

定義　G を群とする. Abel 群 A に G が左から作用していて, 左 G 作用と A の和の間に分配法則がなりたつとき, A を**左 G 加群** (left G-module) といい, 単に G 加群と呼ぶ. すなわち, A が G 加群とは, 次の 3 条件を満たすときをいう.

(GM0) 写像 $G \times A \to A$, $(g, x) \mapsto g \cdot x$ が存在する;
(GM1) 任意の $x \in A$ に対して, $1_G \cdot x = x$ である. ここに, 1_G は G の単位元である;
(GM2) 任意の $x \in A$ と任意の $g, h \in G$ に対して, $(gh) \cdot x = g \cdot (h \cdot x)$ がなりたつ;
(GM3) 任意の $x, y \in M$ と任意の $g \in G$ に対して, $g \cdot (x + y) = g \cdot x + g \cdot y$ がなりたつ.

定義　A, B を G 加群とする. 群準同型 $f : A \to B$ が**G 準同型写像** (G-homomorphism) であるとは, 任意の $x \in A$ と $g \in G$ に対して,

$$f(g \cdot x) = g \cdot f(x)$$

がなりたつときをいう. A から B への G 準同型写像の全体を $\mathrm{Hom}_G(A, B)$ とかく.

例 2.1 2 つの G 加群 A, B に対して, これらの間の群準同型写像全体を $\mathrm{Hom}(A, B) = \mathrm{Hom}_{\mathbb{Z}}(A, B)$ とかく. これは次の作用で G 加群となる:

任意の $g \in G$ と $f \in \mathrm{Hom}(A, B)$, $x \in A$ に対して,

$$(g \cdot f)(x) = g \cdot (f(g^{-1}x))$$

(加群として $\mathrm{Hom}_G(A, B) \leq \mathrm{Hom}(A, B)$ である)

例 2.2 M を G 加群とする. $S \subset G$ に対して $M^S := \{x \in M \mid \sigma x = x \ (\forall \sigma \in S)\}$ とすれば M^S は M の部分加群となる.

例 2.3 K/k を有限次 Galois 拡大とし, G をその Galois 群とすれば $K^\times$ は G の自然な作用により G 加群となる. ($K^\times$ は乗法群であるが, このときも G 加群とよぶこととする)

G 加群 A に対して, その部分加群や商加群の概念が定まる. A の部分集合 B が G **部分加群** (G-submodule) であるとは, 任意の $g \in G$ と $x \in B$ に対して $g \cdot x \in B$ となるときをいう. また, B が A の G 部分加群であるとき, Abel 群としての商群 A/B に G 作用を, 任意の $g \in G$ と $x + B \in A/B$ に対して

$$g \cdot (x + B) = g \cdot x + B$$

と定義すれば, これは well-defined であり A/B は再び G 加群となる. これを A の B による G **商加群** (G-quotient module) という.

2 つの G-加群 A, A' に対して, **直和** (direct sum) $A \oplus A'$ を以下のように定義する. まず, 集合としては直積 $A \times A'$ をとり, G 作用を任意の $g \in G$ と $(x, y) \in A \oplus A'$ に対して

$$g \cdot (x, y) = (g \cdot x, g \cdot y)$$

と定義することで G 加群となる. A の n 個の直和を A^n と表す.

例 2.4 群 G に対して, G を $\mathbb{Z}$ 基底とするような形式和全体を $\mathbb{Z}[G]$ とかく. これは, 集合としては

$$\left\{ \sum_{\text{有限和}} a_g g \;\middle|\; g \in G,\ a_g \in \mathbb{Z} \right\}$$

である. $x = \sum_g a_g g$, $y = \sum_g b_g g \in \mathbb{Z}[G]$ に対して,

$$x + y = \sum_g (a_g + b_g)g, \quad xy = \sum_{g,h} (a_g b_h)gh$$

によって和と積を定義することで単位元 1 をもつ結合環となる. これを G の $\mathbb{Z}$ 上の**群環** (group algebra) という.

$\mathbb{Z}[G]$ への G 作用が $x = \sum_g a_g g \in \mathbb{Z}[G]$, $h \in G$ に対して

$$h \cdot x = \sum_g a_g (h \cdot g)$$

で定義され, この G 作用によって $\mathbb{Z}[G]$ は G 加群となる. (より一般に, G の部分群 H に対し, $\mathbb{Z}[G/H] = \oplus_{\overline{g} \in G/H} \mathbb{Z} \cdot \overline{g}$ は G 加群となる.)

A を G 加群とする. 任意の $x \in A$ と $r = \sum_g a_g g \in \mathbb{Z}[G]$ に対して,

$$rx = \sum_g a_g (g \cdot x)$$

と定めれば, A は環 $\mathbb{Z}[G]$ 上の左加群となる. 逆に, A を左 $\mathbb{Z}[G]$ 加群とすれば, 明らかに G 加群である. この見方によって G 加群を考えることと, 左 $\mathbb{Z}[G]$ 加群を考えることは同じになる.

2.2 有限群のコホモロジーの定義

以下混同の起きない場合は作用の $\cdot$ を省略する.

定義 M を G 加群とする. $n \in \mathbb{Z}_{\geq 0}$ に対し, 集合 $C^n(G, M)$ を以下により定める:

- $n = 0$ のとき $C^0(G, M) := M$;
- $n \geq 1$ のとき $C^n(G, M) := \{\varphi \mid \varphi \text{ は } G^n \text{ から } M \text{ への写像 }\}$.

各 n に対して $C^n(G, M)$ の元を n **コチェイン** (n-cochain) とよぶ.

各 $n \in \mathbb{N}$ について, $C^n(G, M)$ 上の和を φ, $\psi \in C^n(G, M)$, $\sigma \in G^n$ に対して

$$(\varphi+\psi)(\sigma) := \varphi(\sigma)+\psi(\sigma)$$

と定めることにより $C^n(G,M)$ は加法群をなす. ここで $n \in \mathbb{Z}_{\geq 0}$ に対して群準同型 $d^n : C^n(G,M) \to C^{n+1}(G,M)$ を以下で定める:

- $n=0$ のとき $(d^0(x))(\sigma) := \sigma x - x \quad (x \in M,\ \sigma \in G)$;
- $n \geq 1$ のとき $\varphi \in C^n(G,M),\ (\sigma_1, \cdots, \sigma_{n+1}) \in G^{n+1}$ に対して

$$\begin{aligned}(d^n(\varphi))(\sigma_1, \cdots, \sigma_{n+1}) := \sigma_1\varphi(\sigma_2, \cdots, \sigma_{n+1}) \\ +\sum_{i=1}^{n}(-1)^i(\sigma_1, \cdots, \sigma_{i-1}, \sigma_i\sigma_{i+1}, \sigma_{i+2}, \cdots, \sigma_{n+1}) \\ +(-1)^{n+1}\varphi(\sigma_1, \cdots, \sigma_n).\end{aligned}$$

初等的な計算を行うことにより, 任意の $n \in \mathbb{Z}_{\geq 0}$ に対して $d^{n+1} \circ d^n = 0$ となることがわかる. よって $\mathrm{Im}(d^n) \subset \mathrm{Ker}(d^{n+1})$ なので, 加群と準同型写像の列

$$M = C^0(G,M) \xrightarrow{d^0} C^1(G,M) \xrightarrow{d^1} \cdots \xrightarrow{d^{n-1}} C^n(G,M) \xrightarrow{d^n} \cdots$$

は複体をなす. これを**コチェイン複体** (cochain complex) とよぶ.

定義 上で定義した準同型写像 d^n について

$$Z^0(G,M) := \mathrm{Ker}(d^0)$$

とし, $n \in \mathbb{N}$ に対して

$$\begin{aligned}Z^n(G,M) &:= \mathrm{Ker}(d^n), \\ B^n(G,M) &:= \mathrm{Im}(d^{n-1})\end{aligned}$$

とおく. $Z^n(G,\ M), B^n(G,\ M)$ の元をそれぞれ n **コサイクル** (n-cocycle), n **コバウンダリー** (n-coboundary) とよぶ. さらに

$$H^0(G,M) := Z^0(G,M)$$

とし, $n \in \mathbb{Z}_{\geq 1}$ に対して

$$H^n(G,M) := Z^n(G,M)/B^n(G,M)$$

とおき, これを M の n **次コホモロジー群** (cohomology group) とよぶ.

定義からコホモロジー群はコチェイン複体の完全列とのずれを測る量である.

注意 M が有限生成 G 加群のとき, 各 n に対してコホモロジー群 $H^i(G,M)$ は有限群となることが知られている.

例 2.5 $n = 0,\ 1,\ 2$ の場合について n コチェインや n コバウンダリーがどのようになっているかを具体的に見ておく. 定義から実際に計算することで

$n = 0$ のとき

$$Z^0(G,M) = \{x \in M \mid \sigma x - x = 0\ (\forall \sigma \in G)\} = M^G.$$

$n = 1$ のとき

$$Z^1(G,M) = \{\varphi \in C^1(G,M) \mid \varphi(\sigma,\tau) = \sigma\varphi(\tau) + \varphi(\sigma)\ (\forall\ \sigma,\ \tau \in G)\},$$
$$B^1(G,M) = \{\varphi \in C^1(G,M) \mid \exists\ x \in M\ s.t.\ \forall\ \sigma \in G,\ \varphi(\sigma) = \sigma x - x\}.$$

特に M が自明な G 加群のとき, すなわち G の作用が自明であるとき,

$$Z^1(G,M) = \mathrm{Hom}(G,M),$$
$$B^1(G,M) = 0$$

となる. よってこのとき

$$H^1(G,M) = \mathrm{Hom}(G,M)$$

となる.

$n = 2$ のとき

$$Z^2(G,M) = \{f \in C^2(G,M) \mid \sigma f(\tau,\rho) + f(\sigma,\tau\rho) = f(\sigma\tau,\rho) + f(\sigma,\tau)\ (\forall\ \sigma,\ \tau,\ \rho \in G)\},$$
$$B^2(G,M) = \{f \in C^2(G,N) \mid \exists\ h \in C^1(G,M)\ s.t.\ \forall\ \sigma,\ \tau \in G,\ f(\sigma,\tau) = \sigma h(\tau) - h(\sigma\tau) + h(\sigma)\}$$

2.3　コホモロジー群における加群の変更と長完全列

G 加群 $M,\ N$ と $f \in \mathrm{Hom}_G(M,N)$ をとる. $n \in \mathbb{Z}_{\geq 0}$ に対し,

$$f_* : C^n(G,M) \to C^n(G,N)\ ,\ \varphi \mapsto f_*(\varphi) = f \circ \varphi$$

とおく. これは明らかに準同型写像であり, 簡単な計算から $f_*(Z^n(G,M)) \subset Z^n(G,N),\ f_*(B^n(G,M)) \subset B^n(G,M)$ となることがわかる. よって f_* はコホモロジー群の間の準同型写像 $f_* : H^n(G,M) \to H^n(G,N)$ を誘導する. これを f のコホモロジー群上の**誘導写像** (induced map) とよぶ. 特に f が同型写像であれば任意の $n \in \mathbb{Z}_{\geq 0}$ に対して誘導写像 f_* も同型写像となる.

次の定理は, コホモロジーを用いた議論の際によく用いられる非常に重要な命題である.

定理 2.6 (**コホモロジー群の長完全列** [河田 1 , p. 13]) $A,\ B,\ C$ をそれぞれ G 加群とする. これらに対して完全列

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

が得られたとする. このとき, 各 $n \in \mathbb{Z}_{\geq 0}$ に対し以下の系列を完全にするような準同型写像 $\delta : H^n(G,C) \to H^{n+1}(G,A)$ が存在する:

$$\begin{aligned}
0 \to & H^0(G,A) \xrightarrow{f_*} H^0(G,B) \xrightarrow{g_*} H^0(G,C) \\
\xrightarrow{\delta} & H^1(G,A) \xrightarrow{f_*} H^1(G,B) \xrightarrow{g_*} H^1(G,C) \\
\xrightarrow{\delta} & \cdots \\
& \vdots \\
\xrightarrow{\delta} & H^n(G,A) \xrightarrow{f_*} H^n(G,B) \xrightarrow{g_*} H^n(G,C) \\
\xrightarrow{\delta} & \cdots
\end{aligned}$$

これは次のホモロジー代数の基本的な結果による.

命題 2.7 (**蛇の補題, Snake Lemma** [河田 1 , p. 17]) 各行は完全列であるような G 加群の可換図式

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \xrightarrow{f_1} & M_2 & \xrightarrow{f_2} & M_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_3} & & \\ 0 & \longrightarrow & N_1 & \xrightarrow{g_1} & N_2 & \xrightarrow{g_2} & N_3 & \longrightarrow & 0 \end{array}$$

に対して, G 加群の完全列

$$0 \to \mathrm{Ker}(\varphi_1) \to \mathrm{Ker}(\varphi_2) \to \mathrm{Ker}(\varphi_3) \xrightarrow{\delta} \mathrm{Coker}(\varphi_1) \to \mathrm{Coker}(\varphi_2) \to \mathrm{Coker}(\varphi_3) \to 0$$

が得られる.

$$\begin{array}{ccccccccccc} & & & & 0 & & 0 & & 0 & & \\ & & & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & \longrightarrow & \mathrm{Ker}(\varphi_1) & \longrightarrow & \mathrm{Ker}(\varphi_2) & \longrightarrow & \mathrm{Ker}(\varphi_3) & & \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ \delta & & 0 & \longrightarrow & M_1 & \xrightarrow{f_1} & M_2 & \xrightarrow{f_2} & M_3 & \longrightarrow & 0 \\ & & & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_3} & & \\ & & 0 & \longrightarrow & N_1 & \xrightarrow{g_1} & N_2 & \xrightarrow{g_2} & N_3 & \longrightarrow & 0 \\ & & & & \downarrow & & \downarrow & & \downarrow & & \\ & & & & \mathrm{Coker}(\varphi_1) & \longrightarrow & \mathrm{Coker}(\varphi_2) & \longrightarrow & \mathrm{Coker}(\varphi_3) & \longrightarrow & 0 \\ & & & & \downarrow & & \downarrow & & \downarrow & & \\ & & & & 0 & & 0 & & 0 & & \end{array}$$

ここで, 完全列 $0 \to M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \to 0$ はは完全列

$$M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \to 0$$

に換えてもよい. このとき蛇の補題の結果において

$$0 \to \mathrm{Ker}(\varphi_1) \longrightarrow \mathrm{Ker}(\varphi_2) \longrightarrow \mathrm{Ker}(\varphi_3)$$

の部分は

$$\mathrm{Ker}(\varphi_1) \longrightarrow \mathrm{Ker}(\varphi_2) \longrightarrow \mathrm{Ker}(\varphi_3)$$

に換わる. また完全列 $0 \to N_1 \xrightarrow{g_1} N_2 \xrightarrow{g_2} N_3 \to 0$ は次に換えてもよい.

$$0 \to N_1 \xrightarrow{g_1} N_2 \xrightarrow{g_2} N_3$$

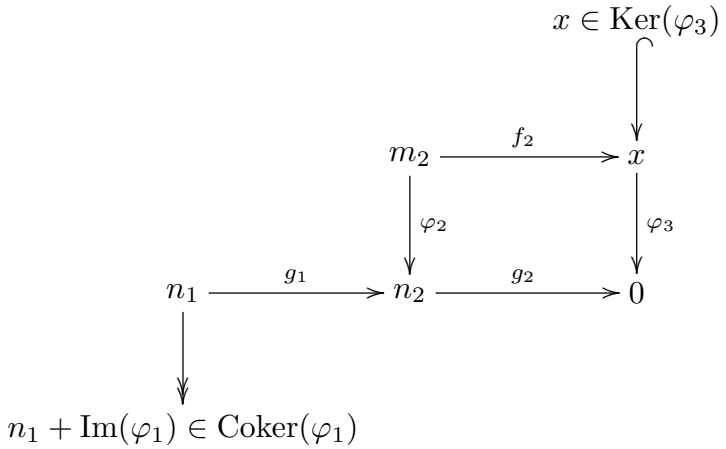
このとき蛇の補題の結果において

$$\mathrm{Coker}(\varphi_1) \longrightarrow \mathrm{Coker}(\varphi_2) \longrightarrow \mathrm{Coker}(\varphi_3) \to 0$$

は次の完全列に換わる.

$$\mathrm{Coker}(\varphi_1) \longrightarrow \mathrm{Coker}(\varphi_2) \longrightarrow \mathrm{Coker}(\varphi_3)$$

蛇の補題における δ は**連結準同型写像** (connecting homomorphism) と呼ばれる. δ の構成法だけ図式化しておこう.



定理 2.6 の証明 まず, 系列

$$0 \to A \to B \to C \to 0$$

が完全であることから, 各 n についてこれにより誘導される系列

$$0 \to C^n(G,A) \to C^n(G,B) \to C^n(G,C) \to 0$$

も完全となる. これにより次の完全可換図式

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \frac{C^n(G,A)}{B^n(G,A)} & \longrightarrow & \frac{C^n(G,B)}{B^n(G,B)} & \longrightarrow & \frac{C^n(G,C)}{B^n(G,C)} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d^n} & & \downarrow{\scriptstyle d^n} & & \downarrow{\scriptstyle d^n} & & \\ 0 & \longrightarrow & Z^n(G,A) & \longrightarrow & Z^n(G,B) & \longrightarrow & Z^n(G,C) & \longrightarrow & 0 \end{array}$$

を得る. ここでこの図式の縦の写像それぞれにおいて $\mathrm{Ker}(d^n) = H^n(G,\cdot)$, $\mathrm{Coker}(d^n) = H^{n+1}(G,\cdot)$ がわかるので, 蛇の補題から連結準同型写像 $\delta^n : H^n(G,C) \to H^{n+1}(G,A)$ を得る. □

Galois 群のコホモロジーは通常 **Galois コホモロジー** (Galois cohomology) とよばれる. 次の定理は Galois コホモロジーに関するもっとも特徴的で重要な定理の一つであるといえよう.

定理 2.8 (**Hilbert 90** [NSW, p. 344]) K/k を有限次 Galois 拡大とし, その Galois 群を G とする. このとき

$$H^1(G, K^\times) = 0$$

がなりたつ.

証明 $Z^1(G,K^\times) \subset B^1(G,K^\times)$ を示せばよい. ここで $K^\times$ が乗法群であることに注意すれば, 例 2.5 で行った計算により

$$Z^1(G,M) = \{\varphi \in C^1(G,M) \mid \varphi(\sigma,\tau) = \varphi(\sigma)\sigma\varphi(\tau)\ (\forall\ \sigma,\ \tau \in G)\},$$
$$B^1(G,M) = \{\varphi \in C^1(G,M) \mid \exists\ x \in M\ s.t.\ \forall\ \sigma \in G,\ \varphi(\sigma) = x\sigma x^{-1}\}$$

である. $f \in Z^1(G,K^\times)$ とすると, $\alpha \in K^\times$, $\sigma \in G$ に対して

$$f(\sigma)\sigma(\sum_{\tau\in G} f(\tau)\tau(\alpha)) = \sum_{\tau\in G} f(\sigma)\sigma(f(\tau))\sigma(\tau(\alpha)) = \sum_{\tau\in G} f(\sigma\tau)\sigma\tau(\alpha) = \sum_{\tau\in G} f(\tau)\tau(\alpha)$$

となる. ここで各 $\tau \in G$ について $f(\tau) \in K^\times$ なので

命題 2.9 (**Dedekind の補題** [藤井, p. 2]) k, K を体とし, $\sigma_1, \cdots, \sigma_m : k \to K$ を全て相異なる環準同型写像とする. $b_1, \cdots, b_m \in K$ とする. もし, 任意の $a \in k$ に対して $\sigma_1(a)b_1 + \cdots + \sigma_m(a)b_m = 0$ がなりたつならば $b_1 = \cdots = b_m = 0$ である.

の対偶を考えることで $\sum_{\tau \in G} f(\tau)\tau(\alpha) \neq 0$ を満たすような $\alpha \in K^\times$ をとることができる. この α に対し $x := \sum_{\tau \in G} f(\tau)\tau(\alpha)$ $(\in K^\times)$ とおけば, 任意の $\sigma \in G$ に対して $f(\sigma)\sigma(x) = x$ となる. ゆえに $f(\sigma) = x\sigma x^{-1}$ となり $f \in B^1(G, K^\times)$ を得る. □

注意 特に Galois 群が巡回群の場合, Hilbert 90 は次のように表現される:

定理 2.10 K/k を n 次巡回拡大とし, その Galois 群を $G = \langle \sigma \rangle = \{1, \sigma, \cdots, \sigma^{n-1}\}$ とする. このとき $\alpha \in K$ について, ノルム $N_{K/k}(\alpha) = 1$ であることと, ある $\beta \in K^\times$ が存在して $\alpha = \beta^{-1}\sigma\beta$ となることは同値である.

Hilbert 90 の応用例として Kummer 理論を紹介する. $n \in \mathbb{Z}_{\geq 1}$ に対して, μ_n を 1 の n 乗根のなす群とする. 体 k は標数が n と素であるとし, さらに $\mu_n \subset k$ とする.

定理 2.11 (**Kummer 理論** [藤井, p. 18]) K/k を有限次 Abel 拡大とし, その Galois 群を G とする. さらに G の指数が n であると仮定する. このとき, 標準的な同型

$$G \cong \mathrm{Hom}\left(\frac{(K^\times)^n \cap k^\times}{(k^\times)^n}, \mu_n\right)$$

が存在する.

証明 G 加群の完全列

$$0 \to \mu_n \to K^\times \xrightarrow{a \mapsto a^n} (K^\times)^n \to 0$$

に対して定理 2.6 からコホモロジー群の完全列

$$0 \to H^0(G, \mu_n) \to H^0(G, K^\times) \to H^0(G, (K^\times)^n) \xrightarrow{\delta} H^1(G, \mu_n) \to H^1(G, K^\times) \to H^1(G, (K^\times)^n) \to \cdots$$

を得る. ここでそれぞれのコホモロジー群を調べる.

まず $\mu_n \subset k$ から G の μ_n への作用は自明であり, よって

$$H^0(G, \mu_n) = \mu_n^G = \mu_n,\ H^1(G, \mu_n) = \mathrm{Hom}(G, \mu_n)$$

となる. さらに, Galois 理論と Hilbert 90 から

$$H^0(G, K^\times) = (K^\times)^G = k^\times,\ H^1(G, K^\times) = 0,$$
$$H^0(G, (K^\times)^n) = ((K^\times)^n)^G = (K^\times)^n \cap k^\times$$

となる. よって上の長完全列から以下の完全列

$$0 \to \mu_n \to k^\times \xrightarrow{a \mapsto a^n} (K^\times)^n \cap k^\times \xrightarrow{\delta} \mathrm{Hom}(G, \mu_n) \to 0$$

を得る. したがって準同型定理から

$$\frac{(K^\times)^n \cap k^\times}{(k^\times)^n} \cong \mathrm{Hom}(G, \mu_n)$$

を得る. この同型は $\dfrac{(K^\times)^n \cap k^\times}{(k^\times)^n}$ と G が互いに双対であることに他ならない. □

3　Hilbert 94 と単項化定理

3.1　準備：類体論の復習

ここでは Hilbert 類体について説明するべく, 類体論について復習を行う. 主に [河田 2] に沿って進めるが, 基本的に証明等の詳しい議論は省略するので, 必要があれば類体論を完成させた高木貞治氏の著書である [高木] や, [足立・三宅] 等を参照してほしい.

k を代数体とする. $\mathcal{O}_k$ で k の整数環を, I_k, P_k でそれぞれ k の分数イデアル全体のなす乗法群, k の単項分数イデアルのなす乗法群を表す. r_1 で k の実埋め込みの数を, r_2 で k の虚埋め込みのペアの数を表す. $\alpha \in k$ の各共役に対して無限素点 $\mathfrak{p}_\infty^{(1)}, \cdots \mathfrak{p}_\infty^{(r_1+r_2)}$ を対応させ, $\alpha \equiv 1 \pmod{\mathfrak{p}_\infty^{(i)}}$ であることを

$$\begin{cases} \alpha^{(i)} > 0 & (1 \leq i \leq r_1), \\ \alpha^{(i)} \neq 0 & (r_1 + 1 \leq i \leq r_1 + r_2) \end{cases}$$

により定義する. さらに, α, $\beta \in k^\times$ に対し, $\alpha \equiv \beta \pmod{\mathfrak{p}_\infty^{(i)}}$ であることを

$$\begin{cases} \alpha^{(i)}\beta^{(1)} > 0 & (1 \leq i \leq r_1), \\ \alpha^{(i)}\beta^{(i)} \neq 0 & (r_1 + 1 \leq i \leq r_1 + r_2) \end{cases}$$

により定める.

有限素点と無限素点の有限個の形式的な冪積を**整因子** (integral factor) という. 整因子 $\mathfrak{m}$ を有限部分と無限部分にわけて $\mathfrak{m} = \mathfrak{m}_0 \prod_i \mathfrak{p}_\infty^{(i)}$ と書いたとき, $\alpha \equiv \beta \pmod{\mathfrak{m}}$ を

$$\alpha \equiv \beta \pmod{\mathfrak{m}_0} \text{ かつ } \alpha \equiv \beta \pmod{\mathfrak{p}_\infty^{(i)}} \ (i = 1, \cdots r_1 + r_2)$$

であることにより定義する.

注意　上の定義において $\alpha \equiv 1 \pmod{\mathfrak{m}_0}$ とは, $\alpha \in \mathcal{O}_k$ のときは $\alpha - 1 \in \mathfrak{m}_0$ を意味するが, $\alpha \notin \mathcal{O}_k$ の場合は $\beta \equiv \gamma \pmod{\mathfrak{m}_0}$ を満たすような β, $\gamma \in \mathcal{O}_k$ が存在して, $\alpha = \beta/\gamma$ と表されることをいう.

定義　$\mathfrak{m}$ を k の整因子とする このとき,

$$\alpha \equiv 1 \pmod{\mathfrak{m}}$$

を満たすような $\alpha \in k^\times$ から生成される単項イデアル (α) の全体のつくる (乗法) 群を, $\mathfrak{m}$ を法とする**シュトラール** (Strahl) とよび, $S_\mathfrak{m}$ で表す.

注意　Strahl はドイツ語で, 英語では ray (**射線**) とよばれる.

$$A_\mathfrak{m} := \{\mathfrak{a} = \mathfrak{b}/\mathfrak{c} \mid \mathfrak{b},\ \mathfrak{c} \subset \mathcal{O}_k,\ (\mathfrak{m}, \mathfrak{b}) = (\mathfrak{m}, \mathfrak{c}) = 1\}$$

とする. このとき明らかに $S_\mathfrak{m} \subset A_\mathfrak{m}$ である.

定義　$S_\mathfrak{m}$ を含む $A_\mathfrak{m}$ の部分群を $H_\mathfrak{m}$ と書き, $\mathfrak{m}$ を法とする**イデアル群** (ideal group) とよぶ. $A_\mathfrak{m}/H_\mathfrak{m}$ を $H_\mathfrak{m}$ に対する**イデアル類群** (ideal class group) とよび, 各剰余類を $H_\mathfrak{m}$ に対する**イデアル類** (ideal class) とよぶ. また, $A_\mathfrak{m}/H_\mathfrak{m}$ の位数を**類数** (class number) とよぶ.

注意　$\mathfrak{m} = \mathcal{O}_k$ のとき, $A_\mathfrak{m}$, $S_\mathfrak{m}$ はそれぞれ I_k, P_k となる. また, このときの類数は特に**絶対類数** (absolute class number) とよばれる.

次の定義は高木貞治氏ではなく H. Weber による類体の定義であるが, 類体がどのような体であるのかがわかりやすいためこちらを採用することとする.

定義　k の n 次 Galois 拡大 K/k が k の $\mathfrak{m}$ に対する**類体** (class field) であるとは, $\mathfrak{m}$ を割らない k の 1 次の素イデアル $\mathfrak{p}$ (すなわち $N_k\mathfrak{p} = p$ (素数)) が K/k において

$$\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_n$$

と完全分解するのは, $\mathfrak{p}$ が $H_\mathfrak{m}$ に属する場合でありかつその場合に限ることをいう.

定義　$\mathfrak{m} = \mathcal{O}_k$, $H_\mathfrak{m} = P_k$ に対する k の類体を k の **Hilbert 類体** (Hilbert class field) とよぶ. これは k の最大不分岐 Abel 拡大としても特徴づけられる.

以下の定理は, 高木貞治氏により証明された. 類体論はこれらの一連の定理からなる.

定理 3.1 (**類体の存在定理** [高木, p. 194]) k の任意のイデアル群 $H_{\mathfrak{m}}$ を与えるとき, $H_{\mathfrak{m}}$ に対する類体が一意的に存在する.

定理 3.2 (**同型定理** [高木, p. 196]) $H_{\mathfrak{m}}$ に対する類体 K/k は Galois 拡大であり,

$$\mathrm{Gal}(K/k) \cong A_{\mathfrak{m}}/H_{\mathfrak{m}}$$

がなりたつ.

定理 3.3 (**分解定理** [高木, p. 196]) $H_{\mathfrak{m}}$ の導手を $\mathfrak{f}$ とする. (すなわち $\mathfrak{f}$ は $H_{\mathfrak{m}} \cap A_{\mathfrak{m}\mathfrak{n}} = H_{\mathfrak{n}} \cap A_{\mathfrak{m}\mathfrak{n}}$ を満たす $\mathfrak{n}$ の中で包含関係で最小のものである) このとき, $\mathfrak{f}$ と素なイ素デアル $\mathfrak{p}$ は $H_{\mathfrak{m}}$ に対する類体 K/k において, $\mathfrak{p}^f \in H_{\mathfrak{m}}$ を満たす最小の f に対して

$$\mathfrak{p} = \mathfrak{P}\cdots\mathfrak{P}_g \ , \ N_{K/k}\mathfrak{P}_i = \mathfrak{p}^f \quad (i = 1, \cdots, g)$$

と分解される.

以下では k のイデアル群 $H_{\mathfrak{m}_1}$, $H_{\mathfrak{m}_2}$ に対する類体をそれぞれ K_1, K_2 とする.

定理 3.4 (**順序定理** [高木, 193]) イデアル群と類体の間には逆の包含がなりたつ. すなわち

$$K_1 \supset K_2 \Leftrightarrow H_{\mathfrak{m}_1} \subset H_{\mathfrak{m}_2}$$

となる.

定理 3.5 (**結合定理** [高木, p. 192]) 合成体 K_1K_2 は $H_{\mathfrak{m}_1} \cap H_{\mathfrak{m}_2}$ に対応する類体である.

定理 3.6 (**推進定理** [高木, p. 199]) k のイデアル群 H に対する類体を K とし, Ω を k を含む任意の代数体とする. このとき, $K\Omega/\Omega$ は Ω のイデアル群 $\tilde{H} := \{\tilde{\mathfrak{a}} \mid N_{\Omega/k}\tilde{\mathfrak{a}} \in H\}$ に対する類体である.

定理 3.7 (**類体論の基本定理** [高木, p. 174]) 代数体 k 上の任意の Abel 拡大 K/k は, あ

るイデアル $\mathfrak{m}$ を法とするイデアル群 $H_{\mathfrak{m}}$ に対する類体である．ここに $\mathfrak{m}$ は K/k で分岐するイデアルのみを含む．

$k=\mathbb{Q}, H_{\mathfrak{m}}=H_m:=H_{(m)}$ として直ちに次の定理を得る．

定理 3.8 (**Kronecker-Weber の定理** [高木, p. 110]) $\mathbb{Q}$ の任意の Abel 拡大はあるイデアル群 H_m に対する類体であり，したがってシュトラール S_m に対する類体 $\mathbb{Q}(\zeta_m)$ に含まれる．

最後に E. Artin による著しい結果である Artin の相互律を紹介しよう．

まず一般の Galois 拡大 K/k において，その Galois 群を $G=\mathrm{Gal}(K/k)$ とする．K の素イデアル $\mathfrak{P}$ が K/k で分岐していないとき，すなわち $\mathfrak{P}$ の惰性群が自明であるとき，$\mathfrak{P}$ に対して **Frobenius 自己同型** (Frobenius automorphism) とよばれる G の元

$$\left[\frac{K/k}{\mathfrak{P}}\right]=:\sigma\in G$$

が定まる．これは任意の $\alpha\in\mathcal{O}_K$ に対して

$$\alpha^{\sigma}\equiv\alpha^{N_k\mathfrak{p}}\pmod{\mathfrak{P}}$$

によって一意に定まる．

注意　Frobenius 自己同型は $\mathfrak{P}$ の分解群の生成元である．

命題 3.9 $\tau\in G$ に対して

$$\left[\frac{K/k}{\mathfrak{P}^{\tau}}\right]=\tau\left[\frac{K/k}{\mathfrak{P}}\right]\tau^{-1}$$

がなりたつ．

この命題により，K/k が Abel 拡大のとき Frobenius 自己同型は $\mathfrak{P}$ の共役によらず $\mathfrak{p}=\mathfrak{P}\cap k$ のみに依存する．このとき $\left[\frac{K/k}{\mathfrak{P}}\right]$ を $\left(\frac{K/k}{\mathfrak{p}}\right)$ とかき，これを **Artin 記号** (Artin symbol）とよぶ．$\mathfrak{a}=\prod_i\mathfrak{p}_i^{e_i}\in A_{\mathfrak{m}}$ に対しては，

$$\left(\frac{K/k}{\mathfrak{a}}\right) := \prod_i \left(\frac{K/k}{\mathfrak{p}_i}\right)^{e_i}$$

と定義する,

定理 3.10 (**Artin の相互律** [高木, p. 198]) Abel 拡大 K/k がイデアル群 $H_\mathfrak{m}$ に対する類体であるとする. このとき

$$\Phi : A_\mathfrak{m} \to \mathrm{Gal}(K/k)\ ,\ \mathfrak{a} \mapsto \left(\frac{K/k}{\mathfrak{p}}\right)$$

とすると, 次がなりたつ:

(a) $\mathrm{Ker}(\Phi) = H_\mathfrak{m}$,

(b) $A_\mathfrak{m}/H_\mathfrak{m} \cong \mathrm{Gal}(K/k)$.

注意 Artin の相互律について, 写像 Φ は **Artin 写像** (Artin map) とよばれる. (a) は素イデアルが完全分解することと $\mathrm{Ker}(\Phi)$ に属することが同値であることを示している. さらに Artin 写像 Φ は全射であり, 準同型定理により (b) が得られる.

注意 2 次体における Artin の相互律は平方剰余の相互律の一般化としてとらえることができ, Artin の相互律は一般相互法則ともよばれる.

例 3.11 簡単な例として奇素数 l の l 分体における Artin 写像を紹介する.
$\zeta = e^{\frac{2\pi i}{l}}$ とし, $k = \mathbb{Q}(\zeta)$ とする. このとき, $k/\mathbb{Q}$ は Galois 拡大でありその Galois 群は $\mathbb{F}_l^\times$ である. これは $l-1$ 次の巡回群であるから, $l-1$ の約数と Galois 群の部分群が 1 対 1 に対応する. したがって Galois 理論から $k/\mathbb{Q}$ の中間体も $l-1$ の約数と 1 対 1 に対応する. 具体的には, $k/\mathbb{Q}$ の n 次の中間体を k_n とかけば, $\mathrm{Gal}(k_n/\mathbb{Q}) \cong \mathbb{F}_l^\times/(\mathbb{F}_i^\times)^n$ である.

k の判別式 $\Delta_k = (-1)^{\frac{l-1}{2}} l^{l-2}$ を考えれば, 素数 $p \neq l$ は $k/\mathbb{Q}$ で不分岐であり, したがって任意の中間体においても不分岐となる.

$\mathbb{Q}$ において, 分数イデアルは $\mathbb{Q}$ の正元と同一視される. したがって

$$I_k = \{a \in \mathbb{Q} \mid a > 0,\ (a, l) = 1\}$$
$$P_k = \{a \in I_k \mid a \equiv 1 \pmod{l}\}$$

となる. $n \in \mathbb{N}$ に対して

$$H_n := \{a \in I_k \mid \exists x \in \mathbb{N}\ s.t.\ a \equiv x^n \pmod{l}\}$$

とおく. 定義から $H_{l-1} = P_k,\ H_1 = I_k$ である. さらに $n,\ m \in \mathbb{N}$ に対して $m \mid n$ ならば $H_n \subset H_m$ となる. $\mathrm{Gal}(k_n/\mathbb{Q}) \cong \mathbb{F}_l^\times/(\mathbb{F}_i^\times)^n$ であるから, 各 n に対して Artin 写像は

$$\Phi_n : I_k \to \mathbb{F}_l^\times/(\mathbb{F}_i^\times)^n\ ,\ a \mapsto \overline{a} \bmod (\mathbb{F}_i^\times)^n$$

と同一視される. $\mathrm{Ker}(\Phi_n) = H_n$ であるので, Artin の相互律から

$$\mathrm{Gal}(k_n/\mathbb{Q}) \cong I_k/H_n$$

となる. 類体の一意性から k は $H_{l-1} = P_k$ に対する類体であり, 各 k_n は H_n に対する類体である.

3.2 Hilbert 94 と単項化定理

この節では, 単項化定理の証明を目標とする. なお証明に関しては主に [足立・三宅], [ノイキルヒ] を参考にしている.

まず Hilbert が単項化定理を予想するに至ったであろう定理を紹介しよう.

定理 3.12 (**Hilbert 94** [足立・三宅, p. 162]) k を代数体とする. K/k を n 次巡回不分岐拡大とすると, k の n 個以上のイデアル類に属する任意のイデアルが K において単項化する.

証明 $G = \mathrm{Gal}(K/k)$ とする. k の素イデアル $\mathfrak{p}$ の K における素イデアル分解:

$$\mathfrak{p}\mathcal{O}_K = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$$

を考える. 両辺に $\sigma \in G$ を作用させることで $\mathfrak{p}\mathcal{O}_K = (\mathfrak{p}\mathcal{O}_K)^\sigma = (\mathfrak{P}_1^\sigma \cdots \mathfrak{P}_g^\sigma)^e$ となる. $\mathfrak{P}_1 = \mathfrak{P}$ とおくと, $\mathfrak{P}_1 \cdots \mathfrak{P}_g = \mathfrak{P}_1^\sigma \cdots \mathfrak{P}_g^\sigma$ であり G の $\{\mathfrak{P}_1 \cdots \mathfrak{P}_g\}$ への作用が推移的であることから

$$g = 1 \Leftrightarrow \mathfrak{P}^\sigma = \mathfrak{P}\ (\forall \sigma \in G) \Leftrightarrow \mathfrak{P} \in I_K^G$$

となる. このとき $e = 1$ ならば $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}$ となることから $\mathfrak{P} \in I_K^G$ は $\mathfrak{p}$ の K への延長であり, $e > 1$ ならば $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}^e$ となることから $\mathfrak{P} \in I_K^G$ は $\mathfrak{p}$ の K への延長でない. 今 K/k は不分岐拡大なので $e = 1$ であり, よって L_K^G は k のイデアルを K に延長したもの全体, P_K^G は I_K^G のうち K で単項イデアルになるもの全体となる. したがって P_K^G/P_k^G のイデアル類の個数が n 以上であることを示せばよい.

G 加群の完全列

$$1 \to \mathcal{O}_K^\times \to K^\times \xrightarrow{a \mapsto (a)} P_K \to 1$$

からコホモロジー群の長完全列

$$0 \to H^0(G, \mathcal{O}_K^\times) \to H^0(G, K^\times) \to H^0(G, P_K) \xrightarrow{\delta} H^1(G, \mathcal{O}_K^\times) \to H^1(G, K^\times) \to H^1(G, P_K) \to \cdots$$

を得る. 定義と Galois 理論から

$$H^0(G, \mathcal{O}_K^\times) = (\mathcal{O}_K^\times)^G,\ H^0(G, K^\times) = (K^\times)^G = k^\times,\ H^0(G, P_K) = P_K^G$$

となり, Hilbert 90 から

$$H^1(G, K^\times) = 0$$

となる. よって

$$1 \to (\mathcal{O}_K^\times)^G \to (K^\times)^G \to P_K^G \to H^1(G, \mathcal{O}_K^\times) \to 0$$

は完全列であり, これにより完全列

$$k^\times \xrightarrow{f} P_K^G \xrightarrow{g} H^1(G, \mathcal{O}_K^\times) \to 0$$

を得る. ここで $\mathrm{Ker}(g) = \mathrm{Im}(f) = P_k$ なので準同型定理から

$$P_K^G/P_k^G \cong \mathrm{Im}(g) = H^1(G, \mathcal{O}_K^\times)$$

を得る．Herbrand 商 $h(G,\mathcal{O}_K^\times) = |H^0(G,\mathcal{O}_K^\times)|/|H^1(G,\mathcal{O}_K^\times)|$ を考える．ここで巡回拡大 K/k とその Galois 群 G に対し．K/k で分岐する k の無限素点の数を ρ とすれば,

$$h(G,\mathcal{O}_K^\times) = 2^\rho/[K:k]$$

がなりたつことがわかるが, K/k は不分岐拡大なので $\rho = 0$ であることに注意して

$$|H^1(G,\mathcal{O}_K^\times)| = |H^0(G,\mathcal{O}_K^\times)|/h(G,\mathcal{O}_K^\times) = [K:k]|H^0(G,\mathcal{O}_K^\times)| \geq [K:k] = n$$

を得る．ゆえに

$$|P_K^G/P_K^G| = |H^1(G,\mathcal{O}_K^\times)| \geq n$$

である． □

Hilbert 94 において, 巡回拡大の条件を Abel 拡大に拡張して考えてみよう．すると Hilbert 94 は次のように拡張される:

k を代数体とし, K/k を n 次不分岐 Abel 拡大とする．このとき k の n 個以上のイデアル類に属する任意のイデアルが K において単項化する．

上記の主張が正しいとすると, K/k が最大不分岐 Abel 拡大, すなわち K を k の Hilbert 類体とすれば Hilbert 類体の性質から $\mathrm{Gal}(K/k) \cong \mathrm{Cl}(k)$ なので, k のすべてのイデアルが K において単項化することになる．実際 Hilbert によってこの結果が予想され, 1930 年に P. Furtwängler により証明がなされた.

定理 3.13 (**単項化定理** Furtwängler [Fur]) k を代数体とする．k の任意のイデアルは k の Hilbert 類体 K において単項化する．すなわち, k の整数環 $\mathcal{O}_k$ の任意のイデアル $\mathfrak{a}$ の K への延長 $\mathfrak{a}\mathcal{O}_K$ は単項イデアルとなる.

証明 ([足立・三宅, p. 162] を参照) K の Hilbert 類体を K_1 とする．K/k は無限素点が完全分解するような k の最大不分岐 Abel 拡大であり, よって K_1/k の最大の Abel 部分拡大となるので $\Gamma := \mathrm{Gal}(K_1/k)$ の交換子群を Γ' とすれば $\Gamma' = \mathrm{Gal}(K_1/K)$ となる.

$\mathfrak{P}$ を K_1 の素イデアルとし, その K, k への射影を $\mathfrak{q}$, $\mathfrak{p}$ とする:

$$\mathfrak{q} = K \cap \mathfrak{P},\ \mathfrak{p} = K \cap \mathfrak{q} = K \cap \mathfrak{P}.$$

k の素イデアル $\mathfrak{p}$ が K で単項化することは, Artin の相互律によって

$$\left(\frac{K_1/K}{\mathfrak{p}}\right) = 1$$

といい換えることができる. $\mathfrak{p}$ の K における素イデアル分解を $\mathfrak{p} = \mathfrak{q}^{\tau_1} \cdots \mathfrak{q}^{\tau_g}$ とすれば $\tau_1, \cdots \tau_g$ は $\mathfrak{q}$ の K/k における分解群による Γ/Γ' の剰余類の代表系である. $\tau_1, \cdots \tau_g$ を Γ まで延長してそれをまた $\tau_1, \cdots \tau_g$ とかけば,

$$\left(\frac{K_1/K}{\mathfrak{p}}\right) = \prod_{i=1}^{g} \left(\frac{K_1/K}{\mathfrak{q}^{\tau_i}}\right) = \prod_{i=1}^{g} \left(\frac{K_1/K}{\mathfrak{q}}\right) \tau_i^{-1}$$

がなりたつ.

$\mathfrak{P}$ の K_1/k における Frobenius 自己同型を σ とする. つまり

$$\sigma := \left[\frac{K_1/k}{\mathfrak{P}}\right]$$

とする. このとき Frobenius 自己同型の定義から

$$\left(\frac{K_1/K}{\mathfrak{q}}\right) = \sigma^f,\ N_K\mathfrak{q} = N_k\mathfrak{p}^f$$

がわかる. よって単項化定理を示すには

$$\prod_{i=1}^{g} \tau_i \sigma^f \tau_i^{-1} = 1$$

がなりたつことを示せばよい.

σ で生成される巡回群を H とすれば, これは定義から $\mathfrak{P}$ の K_1/k における分解群であり, よって $\mathfrak{q}$ の K/k における分解群は $H\Gamma'/\Gamma'$ である. したがって $\tau_1\Gamma', \cdots, \tau_g\Gamma'$ は Γ/Γ' の $H\Gamma'/\Gamma'$ による剰余類の代表系をなす. したがって Γ/Γ' の代表系として

$$\tau_i \sigma^j \quad (i = 1, \cdots, g,\ j = 0,\ 1, \cdots, f-1)$$

をとることができる. 今 $\rho \in \Gamma$ の属する類の代表を $\overline{\rho}$ とかけば,

$$\tau_i \sigma^f \tau_i^{-1} = (\tau_i \cdot \sigma \cdot \overline{\tau_1 \sigma}^{-1})(\overline{\tau_i \sigma} \cdot \sigma \cdot \overline{\tau_i \sigma \cdot \sigma}^{-1}) \cdots (\overline{\tau_i \sigma^{f-1}} \cdot \sigma \cdot \overline{\tau_i \sigma^{f-1} \cdot \sigma}^{-1})$$

と変形される. よって単項化定理は次の群論的な問題に帰着される:

定理 3.14 S_σ, $\sigma \in \Gamma/\Gamma'$ を Γ' による剰余類の代表系とする. このとき

$$V(\sigma) := \prod_{\tau \in G} S_\tau S_\sigma S_{\tau\sigma}^{-1} \in \Gamma'$$

により定まる準同型写像 $V : \Gamma/\Gamma' \to \Gamma'$ は零写像である. つまり,

$$\Gamma/\Gamma' = \mathrm{Ker}(V)$$

がなりたつ.

証明 群拡大

$$1 \to \Gamma' \to \Gamma \to \Gamma/\Gamma' \to 1$$

を考え, $a_{\sigma,\tau} := S_\sigma S_\tau S_{\sigma\tau}^{-1}$ $(\in \Gamma')$ とおく. このとき

$$\prod_{\sigma \in \Gamma/\Gamma'} a_{\sigma,\tau} = 1$$

が任意の $\tau \in \Gamma/\Gamma'$ に対してなりたつことを示せばよい.

簡単のため, 必要があれば代表 S_σ を取り換えることにより $a_{\sigma,1} = a_{1,\tau} = 1$ となるように選ぶ. このとき $S_\sigma = 1$ である.

各 $\tau \neq 1$ に対して記号 x_τ を作り

$$B := \Gamma' \times \prod_{\tau \neq 1} \langle x_\tau \rangle$$

とおく. $x_1 := 1$ を B の単位元と定める. さらに σ, $\tau \in \Gamma/\Gamma'$ に対して

$$x_\tau^\sigma := a_{\sigma,\tau} x_{\sigma\tau} x_\sigma^{-1}$$

と定義し, さらに $a \in \Gamma'$ に対して

$$a^\sigma := S_\sigma a S_\sigma^{-1}$$

とおく. すると形式的な計算により B は G 加群となることがわかる.

$T := \sum_{\sigma\in\Gamma/\Gamma'} \sigma$ とかけば

$$V(\tau) = \prod_{\sigma\in\Gamma/\Gamma'} a_{\sigma,\tau} = \prod_{\sigma\in\Gamma/\Gamma'} x_\tau^\sigma x_{\sigma\tau}^{-1} x_\sigma = x_\tau^T \tag{6}$$

と表すことができる. ここで $\gamma \in \mathbb{Z}[\Gamma/\Gamma']$ とすると,

$$x_\tau^{\sum_{\sigma\in\Gamma/\Gamma'} m_\sigma \sigma} \equiv \prod_{\sigma\in\Gamma/\Gamma'} (x_{\sigma\tau}x_\sigma^{-1})^{m_\sigma} \equiv \prod_{\sigma\in\Gamma/\Gamma'} x_\sigma^{m_{\sigma\tau^{-1}}-m_\sigma} \pmod{\Gamma'}$$

がなりたつ. よって $B^\gamma \subset \Gamma'$ がなりたつ条件は, 任意の $\sigma,\ \tau \in \Gamma/\Gamma'$ に対して $m_{\sigma\tau-1} - m_\sigma = 0$ がなりたつことである. 特に $\sigma = \tau$ として $m_\sigma = m_\tau$ を得る. したがって $B^\gamma \subset \Gamma'$ ならば $\Gamma = mT$ を満たす $m \in \mathbb{Z}$ が存在する.

Γ' の元は $g_1,\ g_2 \in \Gamma$ の交換子 $[g_1, g_2] = g_1 g_2 g_1^{-1} g_2^{-1}$ から生成されるが, Γ の任意の元は aS_σ $(a \in \Gamma',\ \sigma \in \Gamma/\Gamma')$ という形に表せ,

$$\begin{aligned}
[a_1 S_\sigma, a_2 S_\tau] &= a_1 S_\sigma a_2 S_\tau (a_1 S_\sigma)^{-1} (a_2 S_\tau)^{-1} \\
&= a_1 a_2^\sigma S_\sigma S_\tau S_\sigma^{-1} S_\tau^{-1} a_1^{-\tau} a_2^{-1} \\
&= a_1^{1-\tau} a_2^{\sigma-1} a_{\sigma,\tau} a_{\tau,\sigma}^{-1} \\
&= a_1^{1-\tau} a_2^{\sigma-1} x_\tau^\sigma x_{\sigma\tau}^{-1} x_\sigma (x_\sigma^\tau x_{\tau\sigma}^{-1} x_\tau)^{-1} \\
&= a_1^{1-\tau} a_2^{\sigma-1} x_\sigma^{1-\tau} x_\tau^{\sigma-1}
\end{aligned}$$

となる. ここで 2 行目には $S_\sigma a = a^\sigma S_\sigma$ となることを, 3 行目には $S_\sigma S_\tau S_\sigma^{-1} S_\tau^{-1} = a_{\sigma,\tau} a_{\tau,\sigma}^{-1}$ となることをそれぞれ用いた.

ところで, Γ/Γ' は有限 Abel 群であるので基底 $\sigma_1, \cdots, \sigma_r$ を持つ.

$$x_{\sigma\tau} \equiv x_\sigma x_\tau^\sigma \pmod{\Gamma'} \tag{7}$$

であるから, $i = 1, \cdots, r$ に対して $x_i := x_{\sigma_i}$ とおけば $\mathbb{Z}[\Gamma/\Gamma']$ 加群として B は $x_1, \cdots, x_r$ で生成されることがわかる. 以上から $\Gamma' = \{a_1, \cdots, a_l\}$ とかいたとき,

$$a_j \prod_{i=1}^{r} x_i^{f_{ji}} \prod_{s=1}^{l} a_s^{g_{js}} = 1 \quad (j = 1, \cdots, l) \tag{8}$$

を満たすような $\sum_{\sigma,\tau} c_{\sigma,\tau}(\sigma-\tau)$ $(c_{\sigma,\tau}\in\mathbb{Z})$ の形をした $f_{ji},\ g_{js}\in\mathbb{Z}[\Gamma/\Gamma']$ が存在する.

一方 (7) より $x_{\sigma^j}\equiv x_\sigma^{1+\sigma+\cdots+\sigma^{j-1}}\pmod{\Gamma'}$ であるから, n_i を σ_i の位数として

$$T_i := 1+\sigma_i+\cdots+\sigma_i^{n_1-1}$$

とすれば $x_{\sigma^{n_i}}=1$ によって

$$x_i^{T_i}\equiv 1\pmod{\Gamma'}$$

を得る. これを

$$x_i^{T_i}a_i'=1\ (i=1,\cdots,r) \tag{9}$$

と書くことにする. ここに a_i' は Γ' の適当な元とする. (8), (9) を加法の形で書き直し, $r+l$ 個の変数 $x_1,\cdots,x_r,\ a_1,\cdots,a_l$ に関する連立 1 次方程式とみる:

$$\begin{cases} T_1x_1 & & & & & +a_1'=0 \\ \vdots & & & & & \\ & & T_rx_r & & & +a_r'=0 \\ f_{11}x_1+\cdots+f_{1r}x_r & & & +(1+g_{11})a_1+\cdots+g_{1l}a_l=0 \\ \vdots & & & & & \\ f_{l1}x_1+\cdots+f_{lr}x_r & & & +g_{l1}a_1+\cdots+(1+g_{ll})a_l=0 \end{cases} \tag{10}$$

$\mathbb{Z}[\Gamma/\Gamma']$ は可換環なので $\mathbb{Z}[\Gamma/\Gamma']$ の元を成分とする正方行列の行列式を考えることができる. (10) は, 係数行列を (γ_{ij}) と略記すれば a_i を x_{r+i} と置き換えることにより

$$\sum_{j=1}^{r+l}\gamma_{ij}x_j=0\ \ (i=1,\cdots,r+l) \tag{11}$$

と書き直せる. (i,j) 成分の余因子を $\tilde{\gamma}_{ij}$ と書き, $\gamma:=\det(\gamma_{ij})$ とおく. すると行列論から

$$\sum_{i=1}^{r+l}\tilde{\gamma}_{ik}\gamma_{ij}=\gamma\cdot\delta_{jk}$$

がわかる. ここに δ_{jk} は Kronecker のデルタである. したがって (11) に $\tilde{\gamma}_{ik}$ をかけて i についての和をとることにより

$$\gamma x_j = 0 \ \ (j = 1, \cdots, r+l)$$

を得る. 今, B が $x_i,\ a_j$ によって生成されていることを振り返れば,

$$B^\gamma = \{1\} \subset \Gamma'$$

がなりたち, よって $\gamma = mT$ を満たす $m \in \mathbb{Z}$ が存在する.

$\sum_\sigma a_\sigma \sigma \in \mathbb{Z}[\Gamma/\Gamma']$ に $\sum_\sigma a_\sigma \in \mathbb{Z}$ を対応させる環準同型写像 $\Phi : \mathbb{Z}[\Gamma/\Gamma'] \to \mathbb{Z}$ を考えれば $\Phi(mT) = m|G|$ であるが, (10) の形から $\Phi(f_{ji}) = \Phi(g_{js}) = 0$ であることに注意して,

$$\Phi(\gamma) = \Phi(T_1) \cdots \Phi(T_r) = n_1 \cdots n_r = |G|$$

を得る. したがって $m = 1$ となり, (6) から

$$V(\tau) = x_\tau^T = x_\tau^\gamma = 1$$

を得る. これが示すべきことであった. □

単項化定理の証明中に登場した写像 $V : \Gamma/\Gamma' \to \Gamma'$ は群論において**移送** (transfer, Verlagerung) とよばれる準同型写像である. この写像をより一般的な形で述べる.

群 G の交換子群を $G' = [G, G]$ とかく. また, G の最大 Abel 商を $G^{ab} := G/G'$ とかく. G の指数有限な部分群 H に対して, 準同型写像 $V : G^{ab} \to H^{ab}$ を次のように定義する.

R を G の H による左剰余類分解の代表系で $G = RH$ を満たすものとする. $\sigma \in G$ とすると, 任意の $\theta \in R$ に対して $\sigma\theta = \theta^\sigma \sigma_\theta$ を満たす $\sigma_\theta \in H, \theta^\sigma \in R$ が一意的に定まる. このとき定義から

$$\theta^{\sigma\tau} = (\theta^\sigma)^\tau,\ (\sigma\tau)_\theta = \sigma_\theta \tau_{\theta^\sigma}$$

となることがわかる. これにより

$$V(\sigma \bmod G') := \prod_{\theta \in R} \sigma_\theta \bmod H'$$

が定義される. これにより $V : G^{ab} \to H^{ab}$ を定義する.

G の部分群 $\langle\sigma\rangle$ と H による両側剰余類分解 $G = \bigcup_{\tau}\langle\sigma\rangle\tau H$ に対して, m を $\sigma_\tau = \tau^{-1}\sigma^m\tau \in H$ なる最小の自然数とすれば $H \cap \langle\tau^{-1}\sigma\tau\rangle = \langle\sigma_\tau\rangle$ である. ここで $R = \{\sigma^i\tau \mid i = 1, \cdots, m\}$ とおくことにより

$$V(\sigma \bmod G') = \prod_{\tau}\sigma_\tau \bmod H'$$

と表すこともできる.

代数体 k の Hilbert 類体を K とし, さらに K の Hilbert 類体を K_1 とする. また, $\mathrm{Gal}(K/k) = G$ とおく. このとき

$$\begin{array}{ccc} I_K/P_K & \xrightarrow[\cong]{\Phi} & \mathrm{Gal}(K_1/K) = [G,G] \\ {\scriptstyle i}\uparrow & & \uparrow{\scriptstyle V} \\ I_k/P_k & \xrightarrow[\Phi]{\cong} & \mathrm{Gal}(K/k) = G^{ab} \end{array}$$

は可換図式となることが Artin によって示された. ここで Φ は Artin 写像から誘導される同型写像, i はイデアルの持ち上げから誘導される写像である. 単項化定理は i が自明であることに他ならないが, この図式によりこれは v が自明であることと同値である. このことからも V を考えることが本質的であることがわかるでろう.

さて, ここからは [ノイキルヒ, p. 420] を参考に V が自明であることの別証明を与えるとしよう.

G を有限生成な群とし, G の交換子群を G', G' の交換子群を G'' とする. このとき $(G : G') < \infty$ ならば

$$V : G/G' \to G'/G'' \tag{12}$$

が自明な準同型写像であることを示す.

$$f : \mathbb{Z}[G] = \{\sum_{\sigma\in G} n_\sigma\sigma \mid n_\sigma \in \mathbb{Z}\} \to \mathbb{Z},\ \sum_{\sigma\in G} n_\sigma\sigma \mapsto \sum_{\sigma\in G} n_\sigma$$

とおく. f は**オーギュメンテイション写像** (augmentation map) とよばれる環準同型写像であり, その核 $I_G := \mathrm{Ker}(f)$ は**オーギュメンテイションイデアル** (augmentation ideal)

とよばれる. G の部分群 H に対して $I_H \subset I_G$ であり, Span 性と独立性をみることで $\{\tau - 1 \mid \tau \in H, \tau \neq 1\}$ は I_H の $\mathbb{Z}$ 基底をなすことがわかる.

注意

(12) を示すために次の補題を用意する.

補題 3.15 H を指数有限な G の部分群とする. このとき次の図式

$$\begin{array}{ccc} G/G' & \xrightarrow{\quad V \quad} & H/H' \\ {\scriptstyle\delta}\downarrow{\scriptstyle\cong} & & {\scriptstyle\cong}\downarrow{\scriptstyle\delta} \\ I_G/I_G^2 & \xrightarrow[S]{} & (I_H + I_G I_H)/I_G I_H \end{array} \tag{13}$$

は可換となる. ただし δ は $\sigma \mapsto \delta\sigma = \sigma - 1$ により引き起こされる準同型写像とし, S は G/H の左剰余類の代表系で 1 を含むような R によって

$$S(x \bmod I_G^2) = x\sum_{\rho \in R}\rho \bmod I_G I_H$$

によって定義される準同型写像である.

証明 まず

$$\delta : H/H' \to (I_H + I_G I_H)/I_G I_H \tag{14}$$

が同型写像であることを示す. δ は準同型写像であるので逆写像の存在を示せばよい.

$\tau \in H\backslash\{1\},\ \rho \in R$ に対して,

$$\rho\delta\tau = \rho(\tau - 1) = \tau - 1 + (\rho - 1)(\tau - 1) = \delta\rho + \delta\tau$$

となる. よって $\{\rho\delta\tau \mid \tau \in H\backslash\{1\},\ \rho \in R\}$ は $\mathbb{Z}$ 上 $I_H + I_G I_H$ を生成する. さらに

$$0 = \sum_{\rho,\tau} n_{\rho,\tau}\rho\delta\tau = \sum_{\rho,\tau} n_{\rho,\tau}(\rho\tau - \rho) = \sum_{\rho,\tau} n_{\rho,\tau}\rho\tau - \sum_{\rho}(\sum_{\tau} n_{\rho,\tau})\rho$$

とすれば, $\rho\tau, \rho$ は互いに異なるため $n_{\rho,\tau} = 0$ となることから独立性もわかる. したがって $\{\rho\delta\tau \mid \tau \in H\backslash\{1\},\ \rho \in R\}$ は $I_H + I_G I_H$ の $\mathbb{Z}$ 基底となる. ここで $\rho\delta\tau \mapsto \tau \bmod H'$

により定まる準同型写像

$$I_H + I_G I_H \to H/H' \tag{15}$$

を考えればこれは明らかに全射である. また,

$$\begin{aligned}\delta(\rho\tau')\delta\tau &= (\rho\tau' - 1)(\tau - 1)\\ &= \rho\tau'\tau - \rho\tau' - \tau + 1\\ &= \rho(\tau'\tau - 1) - \rho(\tau' - 1) - (\tau - 1)\\ &= \rho(\tau'\tau) - \rho\delta\tau' - \delta\tau\end{aligned}$$

であるから, $I_G I_H \ni \delta(\rho\tau')\delta\tau \mapsto \tau'\tau\tau'^{-1}\tau^{-1} \equiv 1 \bmod H' \in H/H'$ となり, よって (15) は (14) の逆写像となる準同型写像を誘導する. 特に $H = G$ とすれば $\delta : G/G' \to I_G/I_G^2$ は同型写像となる.

ここで V の定義を思い出せば, V は

$$V(\sigma \bmod G') = \prod_{\rho\in R} \sigma_\rho \bmod H'$$

によって定義されるのであった. よって V は $S(\delta\sigma \bmod I_G^2) = \sum_{\rho\in R} \delta\sigma_\rho \bmod I_G I_H$ により定義される準同型写像

$$S : I_G/I_G^2 \to (I_H + I_G I_H)/I_G I_H$$

を引き起こす. $\sigma\rho = \rho'\sigma_\rho$ に注意して

$$\begin{aligned}\delta\rho + (\delta\sigma)\rho &= \delta\rho + (\sigma - 1)\rho\\ &= (\rho - 1) + \rho'\sigma_\rho - \rho\\ &= (\sigma_\rho - 1) + (\rho' - 1) + (\rho' - 1)(\sigma_\rho - 1)\\ &= \delta\sigma_\rho + \delta\rho' + \delta\rho'\delta\sigma_\rho\end{aligned}$$

を得る. ρ が R を走るとき ρ' も R を走るので

$$S(\delta\sigma \bmod I_G^2) \equiv \sum_{\rho\in R} \delta\sigma_\rho \equiv (\delta\sigma)\rho \equiv \delta\sigma \sum_{\rho\in R} \rho \bmod I_G I_H$$

となる. □

(12) を示そう. G を G/G' で置き換えることにより G' が Abel 群であるとしてよい. このとき $G''=\{1\}$ である.

R を G/G' の左剰余類分解の代表系で 1 を含むものとする. さらに $\{\sigma_1,\cdots,\sigma_n\}$ を G の生成元とする. (G は有限生成であったことに注意する.) $e_i=(0,\cdots,0,1,0,\cdots,0)\in\mathbb{Z}^n$ を σ_i に移す写像 g により次の完全列

$$0\to\mathbb{Z}^n\xrightarrow{f}\mathbb{Z}^n\xrightarrow{g}G/G'\to 1$$

を得る. ただし f は $\det(m_{ik})=(G:G')$ なる $n\times n$ 行列 (m_{ik}) により与えられる. これにより

$$\prod_{i=1}^{n}\sigma_i^{m_{ik}}\tau_k=1\ \ (\tau_k\in G')$$

となる. つまり

$$\delta(\prod_{i=1}^{n}\sigma_i^{m_{ik}}\tau_k)=0$$

がなりたつ. ここで $\delta(xy)=\delta x+\delta y+\delta x\delta y,\ \delta(x^{-1})=-(\delta x)x^{-1}$ を繰り返し用いることにより, τ_k は σ_i 達の交換子の積で表されることがわかるので,

$$0=\delta(\prod_{i=1}^{n}\sigma_i^{m_{ik}}\tau_k)=\sum_{i=1}^{n}(\delta\sigma_i)\mu_{ik}\ \ (\mu_{ik}\equiv m_{ik}\bmod I_G)$$

となる. I'_G の定義から $\mathbb{Z}[G/G']\cong\mathbb{Z}[G]/\mathbb{Z}[G]I_{G'}$ となることに注意して (μ_{ik}) を $\mathbb{Z}[G/G']$ 上の行列とみなすと, $\mu:=\det(\mu_{ik})\in\mathbb{Z}[G/G']$ とみなせる. (μ_{ik}) の余因子行列を (λ_{kj}) とし μ を余因子展開することで,

$$(\delta\sigma_j)\mu=\sum_{i,k}(\delta\sigma_i)\mu_{ik}\lambda_{kj}\equiv 0\bmod I_G\mathbb{Z}[G]I_{G'}$$

となる. したがってすべての $\sigma\in G$ について

$$(\delta\sigma)\mu\equiv 0\bmod I_G\mathbb{Z}[G]I_{G'}=I_GI_{G'}$$

となる．よって $\mu \in \mathbb{Z}[G/G']$ を $\mu = \sum_{\rho \in R} n_\rho \bar{\rho}$ $(\bar{\rho} = \rho \bmod G')$ とかけば, すべての $\bar{\sigma} \in G/G'$ に対して

$$\overline{\sigma}\mu = \sum_{\rho} n_\rho \bar{\sigma}\bar{\rho} = \sum_{\rho} n_\rho \bar{\rho}$$

となるので, すべての n_ρ は等しくなる．よって $\mu \equiv m \sum_{\rho \in R} \rho \bmod \mathbb{Z}[G]I_{G'}$ とかけるが, $\mu_{ik} \equiv m_{ik} \bmod I_G$ に注意して

$$\mu \equiv \det(m_{ik}) \equiv (G : G') \equiv m(G : G') \bmod I_G$$

となる．したがって $m = 1$ となるので,

$$\mu \equiv \sum_{\rho \in R} \rho \bmod \mathbb{Z}[G]I_{G'}$$

となる．ここで補題 3.15 の可換図式を用いることで

$$\delta(V(\sigma)) = S(\delta\sigma \bmod I_G^2) \equiv \delta\sigma \sum_{\rho \in R} \rho \equiv (\delta\sigma)\mu \equiv 0 \bmod I_G I_{G'}$$

がなりたつ．したがって V は自明な準同型写像である． □

例 3.16 $k = \mathbb{Q}(\sqrt{-15})$, $K = \mathbb{Q}(\sqrt{-3}, \sqrt{5})$ とする．それぞれの判別式を計算すれば $\Delta_k = -15$, $\Delta_K = -15^2$ であり, よって K/k は不分岐拡大である．K/k は 2 次 Abel 拡大であり, その類数が 2 であることが Minkowski bound により示される．したがって K は k の Hilbert 類体であり, 単項化定理によって k のイデアルは K で単項化する．例えば $(2, (1 + \sqrt{-15})/2)$ は k において単項でないが, K に延長すれば $((1 + \sqrt{5})/2)$ となり単項化する．

単項化定理の一般化として, 次の結果が知られている．

定理 3.17 (**寺田の単項化定理** [Ter]) K/k を不分岐巡回拡大とし, その Galois 群を $\mathrm{Gal}(K/k) = \langle \sigma \rangle$ とする．このとき $\mathfrak{a}^{\sigma-1} \in P_K$ を満たす K のイデアル $\mathfrak{a}$ は k の Hilbert 類体 K_1 で単項化する．

この定理は淡中忠郎氏によって予想され, 寺田文行氏によって証明された (そのため淡

中-寺田の単項化定理ともよばれる). $K = k$ の場合が特に通常の単項化定理なので, 確かに一般化になっているといえる. さらにこれは次のように一般化される.

まず K を代数体 k の Hilbert 類体とし, K_1 を K の Hilbert 類体とする. $H = \mathrm{Gal}(K_1/k)$, $H^{ab} = H/[H,H] = \mathrm{Gal}(K/k)$ とおく. このとき Artin の相互律から $H^{ab} \cong \mathrm{Cl}_k$ である.

H の自己同型写像 α が与えられたとする. これは自然に H^{ab} の自己同型写像を定め, したがって Cl_k の自己同型写像を定める. これらも同様に α で表すことにする. さらに

$$\mathrm{Cl}_k^{[\alpha]} := \langle c^\alpha \cdot c^{-1} \mid c \in \mathrm{Cl}_k \rangle,\ \mathrm{Cl}_k^{\langle\alpha\rangle} := \langle c \in \mathrm{Cl}_k \mid c^\alpha = c \rangle$$

とおく. 鈴木浩志氏は, 以下を示した.

定理 3.18 (Suzuki [Suz]) 不分岐 Abel 拡大 K/k に対し, K のイデアル類群 Cl_K が $N_{K/k}(\mathrm{Cl}_K) \supset \mathrm{Cl}_k^{[\alpha]}$ を満たすとする. このとき, $\mathrm{Cl}_k^{\langle\alpha\rangle} \cap \mathrm{Ker}(j_{K/k} : \mathrm{Cl}_k \to \mathrm{Cl}_K)$ の位数は拡大次数 $[K:k]$ で割り切れる. ただし $j_{K/k}$ はイデアルの持ち上げによる写像である.

定理 3.18 において, 最初の自己同型写像を恒等写像ととれば定義から $\mathrm{Cl}_k^{[\alpha]} = \{1\}$, $\mathrm{Cl}_k^{\langle\alpha\rangle} = \mathrm{Cl}_k$ であり, さらに K を k の Hilbert 類体とれば単項化定理を与える.

不分岐巡回拡大 K/k をとり, $\mathrm{Gal}(K/k) = \langle\sigma\rangle$ とする. K に定理 3.18 を適用する. K の Hilbert 類体を K_1 とし, K_1 の Hilbert 類体を K_2 とする. このとき $\mathrm{Gal}(K_2/K)$ は $\mathrm{Gal}(K_2/k)$ の正規部分群である. 自己同型写像 $a \in \mathrm{Gal}(K_2/k)$ を, $a|_K = \sigma$ を与えるようにとるならば, これによる $\mathrm{Gal}(K_2/k)$ の内部自己同型写像は $H = \mathrm{Gal}(K_2/K)$ の自己同型写像 α を与える. このとき Cl_K の部分群 $\mathrm{Cl}_K^{\langle\alpha\rangle}$ は $c^{\alpha-1} \in P_K$ を満たすイデアルからなる. また不分岐拡大 L/K に対して, $N_{L/K}(\mathrm{Cl}_K) \supset \mathrm{Cl}_K^{[\alpha]}$ は L が k 上 Abel 拡大であることと同値であることに注意すると, 特に K_1/K は最大不分岐 Abel 拡大であるから $N_{K_1/K}(\mathrm{Cl}_K) = \mathrm{Cl}_K^{[\alpha]}$ となる. Cl_K の準同型写像 $\alpha - 1$ によって完全列

$$0 \to \mathrm{Cl}_K^{\langle\alpha\rangle} \to \mathrm{Cl}_K \to \mathrm{Cl}_K^{[\alpha]} \to 0$$

が得られ, よって拡大次数 $[K_1/K]$ は $\mathrm{Cl}_K^{\langle\alpha\rangle}$ の位数と一致する. よって定理 3.18 から

$$\mathrm{Cl}_K^{\langle\alpha\rangle} \subset \mathrm{Ker}(j_{K_1/K} : \mathrm{Cl}_K \to \mathrm{Cl}_{K_1})$$

となることがわかるが. これは $\mathfrak{a}^{\alpha-1} \in P_K$ を満たす K のイデアル $\mathfrak{a}$ は K_1 で単項化することを示しており, 定理 3.18 が寺田の単項化定理の一般化になっていることがわかる.

4　類体塔問題と今後の展望

4.1　類体塔問題

単項化定理に密接に関係して, 次のような問題が考えられる.

問題 1 (**類体塔問題**) $K = K_0$ を代数体とし, K_0 の Hilbert 類体を K_1 とする. さらに K_1 の Hilbert 類体を K_2 とする. このように K_i の Hilbert 類体を K_{i+1} としたとき, 次のような類体の昇鎖

$$K = K_0 \subset K_1 \subset K_2 \subset K_3 \subset K_4 \subset \cdots$$

は常に停留するか.

この昇鎖は, 類体が塔のように積み重なっていることから**類体塔** (class field tower) とよばれる. 類体塔問題は, Ph. Furtwängler により提唱された. この問題が正しいとすると, 単項化定理により一番上の体は単項イデアル整域となり K_0 のイデアルだけでなく全てのイデアルが単項イデアルとなる. このことからも大変興味深い対象であるといえるであろうが, この問題は 1964 年に Golod-Šafarevič [GS] により否定的に解決された.

実際にその反例は

$$K = \mathbb{Q}(\sqrt{-2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17})$$

となっている.

p を素数とする. k を代数体とし, その Hilbert 類体を K とする. このとき, 類体論と Galois 理論から $\mathrm{Gal}(K/k)$ の $q \neq p$ なる全ての q-Sylow 部分群の直積に対応する K/k の部分体 $K_{(p)}$ が存在する. この $K_{(p)}$ を k の **Hilbert** p **類体** (Hilbert p-class field) とよぶ. 定義から $\mathrm{Gal}(K_{(p)}/k)$ は $\mathrm{Gal}(K/k)$ の p-Sylow 群と同型である.

素数 p を固定する. k を代数体とし, その最大不分岐副 p 拡大を $\tilde{L}(k)/k$ とかく. さらにその Galois 群を $\tilde{G}(k) := \mathrm{Gal}(\tilde{L}(k)/k)$ とする. $\tilde{L}(k)$ は ,k の Hilbert p 類体を積み重ねて得られることから p **類体塔** (p-class field tower) ともよばれる.

類体論により $\tilde{G}(k)$ の最大 Abel 商は k のイデアル類群の p-Sylow 部分群と同型となることから, 数論的情報を多く含むことが予想され, p 類体塔は古くから研究されている.

E. S. Golod と I. R. Šhafarevič によって上述のように $\tilde{G}(k)$ は無限群となりうることが示されたが, 一般に $\tilde{G}(k)$ の構造を調べることは難しくほとんど知られていない.

これに関連した問題として,

問題 2 代数体 k の円分的 $\mathbb{Z}_p$ 拡大 k_∞ の p 類体塔 $\tilde{L}(k_\infty)/k_\infty$ は, どのような条件のもと Abel 拡大となるか

という問題を考える. $p = 2$ の場合の虚 2 次体については 2010 年に水澤靖氏と尾崎学氏により決定されている:

定理 4.1 (Mizusawa-Ozaki [MO]) 虚 2 次体 k に対して, その円分的 $\mathbb{Z}_2$ 拡大体 k_∞ の最大不分岐副 2 拡大の Galois 群 $\tilde{G}$ が Abel 群となるための必要十分条件は, k の判別式の最大奇数因子 m が以下のいずれかのように素因数分解されることである:

$$m = \begin{cases} 1 & \\ q & (q \equiv 3 \pmod 8) \\ p & (p \equiv 5 \pmod 8) \\ q & (q \equiv 7 \pmod{16}) \\ pq & (p \equiv 5,\ q \equiv 3 \pmod 8) \\ q_1 q_2 & (q_1 \equiv q_2 \equiv 3 \pmod 8) \\ p & (p \equiv 9 \pmod{16},\ 2^{\frac{p-1}{4}} \equiv 1 \pmod p) \\ q_1 q_2 q_3 & (q_1 \equiv q_2 \equiv q_3 \equiv 3 \pmod 8) \\ pq & (q \equiv 3 \pmod 8,\ p \equiv 9 \pmod{16},\ 2^{\frac{p-1}{4}} \equiv 1 \pmod p) \\ q & (q \equiv 15 \pmod{32},\ P(-1) \equiv 1 \pmod 4) \end{cases} .$$

ここに $p,\ q,\ q_i$ は奇素数を表し, $P(T) \in \mathbb{Z}_2[T]$ は岩澤加群 $X \cong \tilde{G}/[\tilde{G}, \tilde{G}]$ に付随する岩澤多項式である.

さらに岡野恵司氏によってこの主張が p が奇素数の場合に拡張された:

定理 4.2 (Okano [Oka]) p を奇素数 , k を虚二次体, k_∞ を k の円分的 $\mathbb{Z}_p$ 拡大, λ_k を K_∞/k の岩澤 λ 不変量とする. k_∞ の p 類体塔が Abel となる必要十分条件は, 次のいずれかがなりたつことである:

(a) $\lambda_k \leq 1$;
(b) $\lambda_k = 2$ かつ k のイデアル類群の p-Sylow 部分群が p の上の素イデアルの冪の類で生成される.

ここからは虚二次体の場合の岩澤 λ 不変量の計算について, [田谷・福田] を参考に知られている計算法を紹介する.

k を代数体とし, p を素数とする. 例 1.20 でみたように, k の $\mathbb{Z}_p$ 拡大は k 上の p 次巡回拡大 k_n の列

$$k = k_0 \subset k_1 \subset k_2 \cdots \subset k_n \subset \cdots \subset k_\infty = \bigcup_{n \geq 0} k_n$$

と同一視することができる. k_n のイデアル類群の p-Sylow 部分群を A_n とかくと, これは $\mathrm{Gal}(k_n/k)$ が作用する有限 p 群なので $\mathbb{Z}_p[\mathrm{Gal}(k_n/k)]$ 加群となる. このとき岩澤健吉氏により

定理 4.3 (**岩澤の類数公式** [Iwa]) $|A_n| = p^{e_n}$ とする. このとき n に無関係な 3 つの整数 $\lambda \geq 0,\ \mu \geq 0,\ \nu$ が存在して,

$$e_n = \lambda n + \mu p^n + \nu$$

がなりたつ.

が証明された. これらの整数 $\lambda,\ \mu,\ \nu$ は p と k_∞/k だけで定まる定数であり, それぞれ k_∞/k の岩澤 λ 不変量, 岩澤 μ 不変量, 岩澤 ν 不変量とよばれる.

以下, 円分的 $\mathbb{Z}_p$ 拡大 k_∞/k の岩澤 λ 不変量を $\lambda_p(k)$, 岩澤 μ 不変量を $\mu_p(k)$ と表す. k が $\mathbb{Q}$ 上の Abel 拡大の場合, Ferrero-Washington [FW] によって $\mu_p(k) = 0$ となることが知られており, $\lambda_p(k)$ の値が問題となる. 特に, k が虚二次体で p が奇素数の場合, $\lambda_p(k)$

の計算方法として R. Gold による以下の方法が知られている.

定理 4.4 (Gold [Gol2]) $|A_n| = p^{e_n}$ とし, φ を Euler 関数とする. このとき,

(1) p が k で分解しない場合: ある $n \in \mathbb{N}$ に対し, $e_n - e_{n-1} < \varphi(p^n)$ ならばそのような最小の n に対し, $\lambda_p(k) = e_n - e_{n-1}$ となる.

(2) p が k で分解する場合: ある $n \in \mathbb{N}$ に対し, $e_n - e_{n-1} \leq \varphi(p^n)$ ならばそのような最小の n に対し, $\lambda_p(k) = e_n - e_{n-1}$ となる.

つまり $e_n - e_{n-1}$ を計算することができれば, $\lambda_p(k)$ を求めることができる. さらに, この $e_n - e_{n-1}$ については, Bernoulli 数を用いて計算することもできるが, $k = \mathbb{Q}(\sqrt{-m})$ において, $m \not\equiv 0 \bmod p$ の場合以下の方法で比較的初等的に計算できることも知られている.

g を $\bmod p^{n+1}$ の原始根とし, $g(s) \in \mathbb{Z}$ $(s \in \mathbb{Z}_{\geq 0})$ を

$$g(s) \equiv g^s \pmod{p^{n+1}},\ 0 < g(s) < p^{n+1}$$

により定義する. さらに $s \in \mathbb{Z}$ および $r \in \mathbb{Z}_{\geq 0}$ に対し,

$$s_r \equiv s \pmod{p^r},\ \leq s_r \leq p^r$$

により $s_r \in \mathbb{Z}$ を定義する. $yp^{n+1} \equiv 1 \pmod{d}$ なる $y \in \mathbb{Z}$ をとり

$$c_s = \sum_{i=0}^{p-2} \{\alpha(y \cdot g(s + ip^n)) - \alpha(y \cdot g(s_{n-1} + ip^n + \varphi(p^n)))\} \quad (s \in \mathbb{Z}_{\geq 0})$$

とおく. ここで k に付随する非自明な指標 χ に対して $\alpha(r) = \sum_{i=1}^{r-1} \chi(i)$ である. このとき,

定理 4.5 (Gold [Gol1]) $m \not\equiv 0 \pmod{p}$ のとき, 任意の $n \in \mathbb{N}$ に対し,

$$e_n - e_{n-1} = \mathrm{ord}_{\mathfrak{p}} \left(\sum_{s=0}^{\varphi(p^n)-1} c_s \zeta_{p^n}^s \right)$$

である. ここに ζ_{p^n} は 1 の原始 p^n 乗根であり, $\mathrm{ord}_{\mathfrak{p}}$ は p の上にある $\mathbb{Q}(\zeta_{p^n})$ の素イデアル $\mathfrak{p} = (1 - \zeta_{p^n})$ に関する指数である.

福田隆氏は本論文の草稿を読み, 著者へ有益な助言を与えて下さった. 特にその後, [福田] には岩澤理論の詳細や, その Pari/GP を用いた計算方法が記載されていることを知り, 大いなる興味を掻き立てられた. ここに福田隆氏へのお礼を追記しておきたい.

今後の課題としては, まず岩澤理論についての学習を進め, [福田] の内容をより深く理解するとともに, 水澤氏と尾崎氏の結果や岡野氏の結果の一般化を模索していきたい.

参考文献

[足立] 足立 恒雄, ガロア理論講義 [増補版], 日本評論社, 2014.

[足立・三宅] 足立 恒雄, 三宅 克哉, 類体論講義, 日本評論社, 2015.

[河田 1] 河田 敬義, ホモロジー代数, 岩波書店, 1991.

[河田 2] 河田 敬義, 数論, 岩波書店, 1992.

[斎藤] 斎藤 秀司, 整数論, 共立出版, 2006.

[高木] 高木 貞治, 代数的整数論 第 2 版, 岩波書店, 1974.

[田谷・福田] 田谷 久雄, 福田 隆, 岩澤不変量の計算, 日本応用数理学会論文誌 Vol. 12, No. 4 (2002) 293–306.

[ノイキルヒ] J. ノイキルヒ (足立 恒雄 監修, 梅垣 敦紀 訳), 代数的整数論, 丸善出版, 2018.

[福田] 福田 隆, 重点解説 岩澤理論 : 理論から計算まで, サイエンス社, 2019.

[藤井] 藤井 俊, ガロア理論続論, 第 27 回整数論サマースクール報告集 構成的ガロア逆問題と不変体の有理性問題, 2019, 1–26.

[松坂] 松坂 和夫, 集合・位相入門, 岩波書店, 2018.

[三宅] 三宅 克哉, 類数とイデアル類群–古くて新しい問題–, 京都大学数理解析研究所講究録 1026 代数的整数論とその周辺, 1998, 1–11.

[Art] E. Artin, *Idealklassen in Oberkörpern und allgemeines Reziporzitätsgesetz*, Abh. Math. Sem. Univ. Humburg **7** (1930), 46–51.

[FW] B. Ferrero, L. C. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. (2) **109** (1979), 377–395.

[Fur] Ph. Furtwängler, *Beweis des Hauptidealsatzes für die Klassenkörper algebraischer Zahlkörper*, Abh. Math. Sem. Univ. Hamburg **7** (1930), 14–36.

[Gol1] R. Gold. Γ-*extensions of imaginary quadratic fields*, Pacific J. Math. **40** (1972), 83–88.

[Gol2] R. Gold, *Examples of Iwasawa invariants, I, II*, Acta Arith. **26**

(1974/75), 21–32, 233–240.

[GS] E. S. Golod, I. R. Šhafarevič, *On class field towers*, Izv. Akad. Nauk SSSR Ser. Mat. **28** (1964), 261–272, English translation in Amer. Math. Soc. Transl. (2) **48** (1965), 91–102.

[Har] D. Harari, *Galois cohomology and class field theory*, translated from the 2017 French original by Andrei Yafaev, Universitext, Springer, Cham, 2020, xiv+338 pp.

[Iwa] K. Iwasawa, *On* Γ*-extensions of algebraic number fields*, Bull. Amer. Math. Soc. **65** (1959), 183–226.

[MO] Y. Mizusawa, M. Ozaki, *Abelian* 2*-class field towers over the cyclotomic* $\mathbb{Z}_2$*-extensions of imaginary quadratic fields*, Math. Ann. **347** (2010), 437–453.

[NSW] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of number fields*, Second edition, Grundlehren der Mathematischen Wissenschaften, 323, Springer-Verlag, Berlin, 2008.

[Oka] K. Okano, *Abelian* p*-class field towers over the cyclotomic* $\mathbb{Z}_p$*-extensions of imaginary quadratic fields*, Acta Arith. **125** (2006), 363–381.

[Suz] H. Suzuki, *On the Capitulation Problem*, Class field theory—its centenary and prospect (Tokyo, 1998), 483–507, Adv. Stud. Pure Math. 30, Math. Soc. Japan, Tokyo, 2001.

[Ter] F. Terada, *On a generalization of the principal ideal theorem*, Tohoku Math. J. (2) **1** (1950), 229–269.