$\mathbb{Q}$ 上アーベル p 拡大における岩澤不変量について

濱田 路子

平成15年1月31日

目次

1　序文

1959 年, 岩澤健吉によって証明された岩澤の定理はとても美しい定理で, そこに出てくる岩澤不変量が 0 になるかどうかということは, 今までにもよく研究されてきたことである. 特に, ある体 K に対して, K_∞/K が円分 $\mathbb{Z}_p$ 拡大のときの岩澤不変量については, $\mu = 0$ 予想と呼ばれる予想がある. $K/\mathbb{Q}$ がアーベル拡大のときは, Ferrero-Washington によって, $\mu = 0$ となることが証明されている.

本修士論文は G.Yamamoto の 2000 年の論文 [?] について細かい証明を補い, まとめたものである. 主定理 1.2.1 に関する細かい証明を補うために, [?], [?], [?], [?] 等の論文を参照した. 主定理 1.2.1 は, $\mathbb{Q}$ 上アーベル p 拡大となるような体 k の岩澤不変量がすべて 0 になるような必要十分条件を求めるものである. ここで, $\mathbb{Q}$ 上アーベル p 拡大とは, 対応する Galois 群の位数が p 巾のアーベル群になるような拡大のことである. 主定理 1.2.1 を証明する際に非常に重要な定理 3.35 については [?] に詳しいことが載っている. この章では, 本論文の主定理 1.2.1 を紹介する.

1.1　予備知識

次の二つの定義は, 主定理 1.2.1 を紹介するために必要な記号の定義であり, その性質については, 後で紹介することにする.

定義 1.1 (種の体) k の種の体 k_G とは, $\mathbb{Q}$ 上アーベル拡大になるような k の最大の不分岐アーベル拡大のことである.

つまり, 種の体 k_G は $\mathbb{Q}$ のアーベル拡大と k を合成したものとして考えることができる. 次に, p 巾剰余記号を定義するが, これは主定理 1.2.1 における岩澤不変量がすべて 0 になるような必要十分条件を書き出す時に使われる.

定義 1.2 (p 巾剰余記号) $p, b \in \mathbb{Z}^+, a \in \mathbb{Z}$, $(a, p) = 1$ のとき, $x^p \equiv a \pmod{b}$ が解を持つならば, a は modulo b の p 巾剰余であるという. このとき, a が modulo b の p 巾剰余記号であるという記号を,

$$\left(\frac{a}{b}\right)_p = 1$$

と書く. a が modulo b の p 巾剰余でないときは $\left(\frac{a}{b}\right)_p$ の値は 1 ではないとする. 実際に, ζ_p を 1 の原始 p 乗根とするとき, $\left(\frac{a}{b}\right)_p$ の値は, ある整数 r に対して, ${\zeta_p}^r$ となる. しかし, 今回は, p 巾剰余であるかそうでないかが問題になるため, 少し曖昧ではあるが, p 巾剰余記号の定義は以上のようにする.

1.2　主定理 1.2.1

この節では, 前節で定義した種の体や p 巾剰余記号を用いて本論文の主定理 1.2.1 を紹介する.

主定理 1.2.1 (G.Yamamoto(2000)) p を奇素数, k_∞/k を円分 $\mathbb{Z}_p$ 拡大とする. k を $\mathbb{Q}$ 上アーベル p 拡大とし, 互いに異なる $p_1, \cdots, p_t$ に対して, k の conductor を $m_k = p^a p_1 \cdots p_t$ とする. ここで, $p_1, \cdots, p_t$ は $k/\mathbb{Q}$ で分岐する素数である.

もし,

$$\lambda_p(k) = \mu_p(k) = \nu_p(k) = 0 \tag{1.3}$$

ならば, $t \leq 2$. 逆に, $t \leq 2$ を仮定するとき,

- $t = 0$ ならば, (1.3) を満たす.
- $t = 1$ ならば, (1.3) を満たすための必要十分条件は $k_G \subseteq k_\infty$ であり,

$$\left(\frac{p}{p_1}\right)_p \neq 1 \ \text{ または } \ p_1 \not\equiv 1 \pmod{p^2} \tag{1.4}$$

である.

- $t = 2$ ならば, (1.3) を満たすための必要十分条件は $k_G \subseteq k_\infty$ であり, $(i,j) = (1,2)$ または $(2,1)$ に対して,

$$\left(\frac{p}{p_i}\right)_p \neq 1, \ \left(\frac{p_i}{p_j}\right)_p \neq 1, \ p_j \not\equiv 1 \pmod{p^2}, \tag{1.5}$$

であり,

$$\left(\frac{p_j p^x}{p_i}\right)_p = 1, \ \left(\frac{p {p_i}^y}{p_j}\right)_p = 1, \ p_i {p_j}^z \equiv 1 \pmod{p^2}, \ xyz \neq -1 \in \mathbb{F}_p \tag{1.6}$$

なる $x, y, z \in \mathbb{F}_p$ が存在することである.

注 1.7 $k/\mathbb{Q}$ で分岐する素数 $p_1, \cdots, p_t$ に対して, k の conductor を, $m_k = p^a p_1 \cdots p_t$ としているが, これは次のことから言える.

証明　k は $\mathbb{Q}$ 上アーベル拡大なので, Kronecker-Weber の定理より, k はある円分体に含まれる. これを $k \subseteq \mathbb{Q}(\zeta_{n_k}), n_k = p^a {p_1}^{b_1} \cdots {p_t}^{b_t}$ とする.

今, $\mathbb{Q}(\zeta_{m_k}) \subseteq \mathbb{Q}(\zeta_{n_k})$ が成り立ち,

$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}(\zeta_{n_k})/\mathbb{Q}) &= \Gamma \\ \mathrm{Gal}(\mathbb{Q}(\zeta_{n_k})/\mathbb{Q}(\zeta_{m_k})) &= H \\ \mathrm{Gal}(\mathbb{Q}(\zeta_{n_k})/k) &= N \end{aligned}$$

とすると,

$$\Gamma \simeq (\mathbb{Z}/p^a\mathbb{Z})^\times \times \prod_{i=1}^{t} (\mathbb{Z}/{p_i}^{b_i}\mathbb{Z})^\times$$

$$H \simeq \{1\} \times \prod_{i=1}^{t} (\mathbb{Z}/{p_i}^{b_i - 1}\mathbb{Z})$$

となる. ここで, H から Γ への単射が存在し, Γ から $\mathrm{Gal}(k/\mathbb{Q}) = \Gamma/N$ への自然な写像が存在する. $\phi : \Gamma \to \Gamma/N$ とすると, Γ/N は位数が p 巾の群であり, 各 p_i は p とは異なる素数である. つまり, N の元は $\mathrm{Ker}\phi$ に入る. すなわち, H は N の部分群になり, H は k に自明に作用することがわかる. したがって, conductor として, 最小の値である m_k をとり, $k \subseteq \mathbb{Q}(\zeta_{m_k})$ とする.

さらに, [**?**] の命題 13.2.9 より, $\mathbb{Q}(\zeta_{m_k})$ の整数環 D に対して,

$$p_i D = (P_1 \cdots P_g)^{p_i - 1}$$

と書くことができる. ここで, P_i は次数 f の互いに異なる D の素数, $fg = \phi(m_k)$, f は ${p_i}^f \equiv 1 \pmod{m_k}$ を満たす最小の正の整数である.

今, p_i は $k/\mathbb{Q}$ で分岐するので, 分岐指数は少なくとも p では割れることになる. したがって, $p_i \equiv 1 \pmod{p}$ となることも言える. □

この主定理を使うことによって, 一般には岩澤不変量を計算することが難しかったとしても, 条件を満たすかどうかを調べることによって, 不変量が 0 になるかどうかがわかることになる.

謝辞

末筆ではありますが, 本修士論文を書き終えるまで, 2 年間セミナー等で親切に御指導下さった雪江明彦先生, 類体論に関して御指導下さった高橋豊文先生, そして, この 2 年間同じセミナーの仲間であった小林優司氏, 永田雄一氏に深く感謝の意を表します.

2 $\mathbb{Z}_p$ 拡大における岩澤理論

この節では, $\mathbb{Z}_p$ 拡大における岩澤理論を紹介する. この節の内容については [?] の 13 節に詳しいことが載っている. 主定理 1.2.1 において, $\mathbb{Q}$ 上アーベル p 拡大での岩澤不変量について考えるのだが, この岩澤不変量とは次に紹介する岩澤の定理に出てくるものである.

2.1 岩澤の定理

これから紹介する岩澤の定理 (Iwasawa(1959)) はとても有名なものである. 岩澤の定理は, ある体 K に対して, K の $\mathbb{Z}_p$ 拡大と呼ばれる拡大を考え, この拡大について考えられるものである. まずは, K の $\mathbb{Z}_p$ 拡大を定義する.

定義 2.1 ($\mathbb{Z}_p$ 拡大) K_∞/K が $\mathbb{Z}_p$ 拡大であるとは,

$$\mathrm{Gal}(K_\infty/K) \simeq \mathbb{Z}_p$$

が成り立つことである.

このとき,

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n \subseteq \cdots \subseteq K_\infty = \bigcup_{n\geq 0} K_n$$

であり, $\mathrm{Gal}(K_n/K) \simeq \mathbb{Z}/p^n\mathbb{Z}$ となる体の列を考えると,

$$\mathrm{Gal}(K_\infty/K) = \varprojlim \mathrm{Gal}(K_n/K) = \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$$

となり, K_∞ は K の $\mathbb{Z}_p$ 拡大となる. したがって, K の $\mathbb{Z}_p$ 拡大 とは以上のような体の列を考えたときにできる拡大と考えることができる.

特に, 任意の数体 K は少なくとも一つの $\mathbb{Z}_p$ 拡大を持つことがわかっていて, この拡大は K の円分 $\mathbb{Z}_p$ 拡大と呼ばれるものである. K の円分 $\mathbb{Z}_p$ 拡大とは,

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = K\cdot\mathbb{Q}_n \subseteq \cdots \subseteq K_\infty = \bigcup_{n\geq 0} K_n$$

となる体の列で, ただし, $\mathbb{Q}_n$ は $\mathbb{Q}(\zeta_{p^{n+1}})$ の $\mathbb{Q}$ 上 p^n 次の部分体である. このとき,

$$\mathrm{Gal}(K_\infty/K) = \mathrm{Gal}(K\cdot\mathbb{Q}_\infty/K) = \mathrm{Gal}(\mathbb{Q}_\infty/K\cup\mathbb{Q}_\infty) \simeq \mathbb{Z}_p$$

が成り立つことから, K_∞ は K の $\mathbb{Z}_p$ 拡大となる.

ただし, ある n に対して, $\mathbb{Q}_n \subseteq K$ となる場合も考えられる. このときは, 番号が少しずれてしまう可能性があって,

$$K = K_0 \subseteq K_1 = K\cdot\mathbb{Q}_{n+1} \subseteq \cdots \subseteq K_\infty$$

となるが, $\mathbb{Q}_{n+1} = \mathbb{Q}_1{}'$ と置き換えて考えると良い.

次に, 岩澤の定理を紹介する.

定理 2.2 (Iwasawa(1959)) K_∞/K を $\mathbb{Z}_p$ 拡大とし, p^{e_n} を $h(K_n)$ を割る最大の p 巾の数とするとき, 正の整数 λ, μ, 整数 ν が存在して, 十分大きな n に対して

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

が成り立つ. ただし, $h(K_n)$ は K_n の類数のことである.

この λ, μ, ν が岩澤不変量と呼ばれるもので, 十分大きな n に対してただ一つ決まる値である. さらに, p^{e_n} とは, K_n のイデアル類群の p シロー部分群の位数である.

本修士論文では, $\mathbb{Q}$ 上アーベル p 拡大となるような体 k に対して円分 $\mathbb{Z}_p$ 拡大を考え, そこで岩澤不変量を考えるのだが, 岩澤の定理の証明の概要は一般の $\mathbb{Z}_p$ 拡大について述べる.

2.2 $\mathbb{Z}_p[[T]]$ 加群の構造

岩澤の定理を証明する際に, 形式的巾級数環 $\mathbb{Z}_p[[T]]$ 上の加群の構造を使うため, ここでは少し説明を与えるが, $\mathbb{Z}_p[[T]]$ の性質等については [?] の 7 節と 13 節に詳しく載っている. $\Lambda = \mathbb{Z}_p[[T]]$ とおく. 特に, この Λ はネーター環である. まずは, Λ の中の多項式について次の定義をする.

定義 2.3 (distinguished 多項式) $P(T) \in \Lambda$ が distinguished であるというのは, $P(T)$ が

$$P(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0$$

と書けて, さらに, $p \mid a_i$ $(0 \leq i \leq n-1)$ が成り立つことである.

$P(T)$ は $p^2 \mid a_0$ であってもかまわないため, Eisenstein 多項式ではないが, $p^2 \nmid a_0$ ならば, Eisenstein 多項式と同じ条件を満たす.

また, この distinguished な多項式 $P(T)$ を使って, 次の補題が成り立つ.

命題 2.4 任意の $f(T) \in \Lambda$ に対して, $g(T) \in \Lambda$, distinguished な多項式 $P(T)$, $\deg(r(T)) < \deg(P(T))$ なる $r(T) \in \mathbb{Z}_p[T]$ を使って,

$$f(T) = g(T)P(T) + r(T)$$

と一意に書くことができる.

この補題を使うことによって, Λ は一意分解整域となることが言える. この補題の証明は [?] の命題 7.2 に載っている.

定理 2.5 (Weierstrass p-adic Preparation Theorem) 任意の $0 \neq f \in \Lambda$ に対して,

$$f(T) = p^{\mu}P(T)U(T) \ (0 < \mu \in \mathbb{Z}, P(T) : \text{distinguished}, U(T) \in \Lambda^{\times})$$

と書くことができる.

この定理の証明は [?] の定理 7.3 に載っている.

Λ のイデアルについて考えることにする. 次の四つの補題は, 後で紹介する擬同型に関する定理 2.13 を使って, 有限生成 Λ 加群を直和分解したときに現れる直和因子の位数を計算するときに使われる.

補題 2.6 $f, g \in \Lambda$ が互いに素なとき, イデアル (f, g) は Λ において有限指数となる. すなわち, $[\Lambda : (f, g)] < +\infty$ となる.

この補題の証明は, [?] の補題 13.7 に載っている.

補題 2.7 $f, g \in \Lambda$ が互いに素なとき, 次の二つが成り立つ.

(1) 自然な写像 $\Lambda/(fg) \to \Lambda/(f) \oplus \Lambda/(g)$ は単射で, cokernel は有限となる.

(2) $\Lambda/(f) \oplus \Lambda/(g) \to \Lambda/(fg)$ なる cokernel が有限の写像が存在する.

この補題の証明は, [?] の補題 13.8 に載っている.

補題 2.8 Λ のイデアルは

$$0, (P, T), (p), (P(T)) \text{ (ただし, } P(T) : \text{distinguished, 既約)}$$

であり, (P, T) はただ一つの極大イデアルである.

この補題の証明は, [?] の命題 13.9 に載っている.

補題 2.9 $f \in \Lambda, f \notin \Lambda^\times$ のとき, $\Lambda/(f)$ は無限になる. つまり, $[\Lambda : (f)]$ は無限である.

この補題の証明は [?] の補題 13.10 に載っている.

ここで, Λ 加群 M が M' に擬同型であるということを定義して, それに関する例を述べる.

定義 2.10 (擬同型) Λ 加群 M が M' に擬同型 $(M \sim M')$ であるとは, $M \to M'$ なる準同型が存在して, kernel, cokernel が有限になることである. したがって, 有限 Λ 加群 A, B に対して,

$$0 \to A \to M \to M' \to B \to 0$$

なる完全列が存在することである.

注 2.11 $M \sim M'$ ならば, $M' \sim M$ が成り立つということではない.

例 2.12 $(p, T) \sim \Lambda$ は明らかではあるが, $\Lambda \sim (p, T)$ は成り立たたない.

証明 $\phi : \Lambda \to (p, T)$ という準同型により, Λ が (p, T) に擬同型になるとする. このとき, $\phi(1) = f(T) \in (p, T)$ とする. Λ の image は (f) となり, $(f) \subset (p, T)$ となる. ここで, (p, T) は極大イデアルであったから, $f \notin \Lambda^\times$ となる. つまり, 補題 2.9 より, $\Lambda/(f)$ は無限指数であり, $(p, T)/(f)$ も無限指数である. すなわち, cokernel が無限になってしまうことから, $\Lambda \sim (p, T)$ は成り立たたない. □

また, 補題 2.7 を用いて次のことが言える. $f, g \in \Lambda$ が互いに素なとき,

$$\Lambda/(fg) \sim \Lambda/(f) \oplus \Lambda/(g), \Lambda/(f) \oplus \Lambda/(g) \sim \Lambda/(fg)$$

が成り立つ.

ここで, 擬同型の概念を使って, 次の定理が成り立つ. これは岩澤の定理を証明する際に非常に重要なものである.

定理 2.13 (Cohen) M を有限生成 Λ 加群とする. このとき,

$$M \sim \Lambda^r \oplus \Big(\bigoplus_{i=1}^{s} \Lambda/(p^{k_i})\Big) \oplus \Big(\bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{m_j})\Big)$$

が成り立つ. ただし, $r, s, t, k_i, m_j \in \mathbb{Z}$ であり, $f_j(T)$ は既約で distinguished な多項式である.

この定理の証明は, [?] の定理 13.12 に載っているが, 今回は簡単に説明することにする.

証明の概略　今, M は 生成元 $u_1, \cdots, u_n$ を持つと仮定する. $\lambda_i \in \Lambda$ に対して,

$$S = \Big\{(\lambda_1, \cdots, \lambda_n) \in \Lambda^n \Big| \sum_{i=1}^{n} \lambda_i u_i = 0\Big\}$$

とする. S は Λ^n の部分加群であり, Λ はネーター環なので, このような S は有限生成である. したがって,

$$\Lambda^m \xrightarrow{\phi} \Lambda^n \longrightarrow M \longrightarrow 0$$

が完全列となるような準同型 ϕ をとることができる. この ϕ を行列

$$T = \begin{pmatrix} \lambda_{11} & \cdots & \lambda_{1n} \\ \vdots & & \vdots \\ \lambda_{m1} & \cdots & \lambda_{mn} \end{pmatrix}$$

と書くことにする.

この T を基本変形して定理 2.13 が証明できるのだが, 基本変形にはいくつか種類があるため, ここでその基本変形について述べる.

定義 2.14 (行列の基本変形) 行列 T に対して, 次の六つの基本変形を定義する.

(a) 行同士, 列同士は交換することができる.

(b) ある行のスカラー倍を別の行に加える. また, ある列のスカラー倍を別の列に加える.

つまり, $\lambda' = q\lambda + r$ のとき,

$$\begin{pmatrix} \vdots & & \vdots & \\ \lambda & \cdots & \lambda' & \cdots \\ \vdots & & \vdots & \end{pmatrix} \to \begin{pmatrix} \vdots & & \vdots & \\ \lambda & \cdots & r & \cdots \\ \vdots & & \vdots & \end{pmatrix}$$

と変形する.

(c) $\lambda \in \Lambda^\times$ に対して, ある行, またはある列全体を λ 倍する.

(d) T が行 $(\lambda_1, p\lambda_2, \cdots, p\lambda_n)$ を含むとき, この $(\lambda_1, p\lambda_2, \cdots, p\lambda_n)$ を $(\lambda_1, \cdots, \lambda_n)$ と変形し, $(\lambda_1, p\lambda_2, \cdots, p\lambda_n)$ 以外の行の第一成分のみを p 倍する.

つまり,

$$T = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & & \vdots \\ \lambda_1 & p\lambda_2 & \cdots & p\lambda_n \\ \vdots & \vdots & & \vdots \\ \beta_1 & \beta_2 & \cdots & \beta_n \end{pmatrix} \to T' = \begin{pmatrix} \lambda_1 & \lambda_2 & \cdots & \lambda_n \\ p\alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & & \vdots \\ p\beta_1 & \beta_2 & \cdots & \beta_n \end{pmatrix}$$

と変形する.

(e) T が p^k で割れる行と列を持ち, その行と列の丁度重なる成分が p^{k+1} で割れないとき, p^k で割れる行 $(p^k\lambda_1, \cdots, p^k\lambda_n)$ を $(\lambda_1, \cdots, \lambda_n)$ に変形する.

つまり,

$$T = \begin{pmatrix} \alpha_1 & \cdots & p^k\alpha_j & \cdots & \alpha_n \\ \vdots & & \vdots & & \vdots \\ \lambda_1 & \cdots & p^k\lambda_j & \cdots & \lambda_n \\ \vdots & & \vdots & & \vdots \\ \beta_1 & \cdots & p^k\beta_j & \cdots & \beta_n \end{pmatrix} \to T' = \begin{pmatrix} \lambda_1 & \cdots & \lambda_j & \cdots & \lambda_n \\ p^k\alpha_1 & \cdots & \alpha_j & \cdots & \alpha_n \\ \vdots & & \vdots & & \vdots \\ p^k\beta_1 & \cdots & \beta_j & \cdots & \beta_n \end{pmatrix}$$

と変形する.

(f) T が行 $(p^k\lambda_1, \cdots, p^k\lambda_n)$ を含み, $p \nmid \lambda$ となるある λ に対して, $(\lambda\lambda_1, \cdots, \lambda\lambda_n)$ も S に含まれるとき, つまり, $\sum_{i=1}^n \lambda\lambda_i = 0$ を満たすとき, $(p^k\lambda_1, \cdots, p^k\lambda_n)$ を $(\lambda_1, \cdots, \lambda_n)$ に変形する.

つまり,

$$T = \begin{pmatrix} \vdots & & \vdots \\ p^k\lambda_1 & \cdots & p^k\lambda_n \\ \vdots & & \vdots \end{pmatrix} \to T' = \begin{pmatrix} \vdots & & \vdots \\ \lambda_1 & \cdots & \lambda_n \\ \vdots & & \vdots \end{pmatrix}$$

と変形する.

有限生成 Λ 加群 M, M' に対して,

$$\Lambda^m \xrightarrow{\phi} \Lambda^n \longrightarrow M \longrightarrow 0$$

$$\Lambda^m \xrightarrow{\phi'} \Lambda^n \longrightarrow M' \longrightarrow 0$$

が完全列になるような準同型 ϕ, ϕ' がとれて, この ϕ, ϕ' を行列 T, T' と書くことにする.

もしも, 基本変形の演算 $(\mathrm{a}), \cdots, (\mathrm{f})$ を使って, T が T' に変形できるならば, M は M' に擬同型になることがわかる.

さらに, 定理 2.13 を説明するために必要な定義を二つ述べる.

定義 2.15 (Weierstrass degree) 任意の $f \in \Lambda$ に対して,

$$\deg_w(f) = \begin{cases} \infty & if\ \mu > 0 \\ \deg(P(T)) & if\ \mu = 0 \end{cases}$$

を f の Weierstrass degree と呼ぶ.

また, M に対して決まる行列 $T = (\lambda_{ij})$ に対して,

$$\deg^{(k)}(T) = \mathrm{Min}\{\deg_w(\lambda_{ij}) | i, j \geq k\}$$

とする.

定義 2.16 ($r-1$ の normal form) 行列 T が

$$\begin{pmatrix} \lambda_{11} & \cdots & & 0 & \\ \vdots & \ddots & & \vdots & \mathbf{0} \\ 0 & \cdots & \lambda_{r-1,r-1} & & \\ & * & & * & \end{pmatrix} = \begin{pmatrix} D_{r-1} & \mathbf{0} \\ A & B \end{pmatrix}.$$

のような形をしているとき, T は $r-1$ の normal form に入ると言う. ただし, λ_{kk} は distinguished であり, $1 \leq k \leq r-1$ に対して, $\deg(\lambda_{kk}) = \deg_w(\lambda_{kk}) = \deg^{(k)}(T)$ を満たす.

補題 2.17 $B \neq 0$ ならば, T は演算 $(\mathrm{a}), \cdots, (\mathrm{f})$ を有限回用いて T' に変形でき, T' は r の normal form に入り, 初めの $r-1$ 個は R と同じ対角成分を持つ.

この補題の証明は, Claim[**?**, p.275] に載っている.

これまでの命題や補題を使って, 定理 2.13 を証明する. 補題 2.17 より, T は

$$\begin{pmatrix} D_{r-1} & \mathbf{0} \\ A & B \end{pmatrix}$$

の形をしている. このとき, 補題 2.17 と基本変形の演算 $(\mathrm{a}), \cdots, (\mathrm{f})$ を使って,

$$\begin{pmatrix} \lambda_{11} & & 0 \\ & \ddots & \vdots \\ & & \lambda_{rr} \quad \vdots \\ & A & 0 \end{pmatrix}$$

と変形できる. 任意の λ_{jj} は distinguished であり, $j \geq r$ のとき,

$$\deg(\lambda_{jj}) = \deg^{(j)}(T)$$

となるようになるまで T を変形する. ここで, λ_{jj} は $i \neq j$ のとき, $\deg(\lambda_{ij}) < \deg(\lambda_{jj})$ となるようにとっても一般性を失わないので, 今は λ_{jj} を以上の条件を満たすものとする.

ある $i \neq j$ に対して, $\lambda_{ij} \neq 0$ を仮定する.

このとき, $\deg_w(\lambda_{jj})$ は最小であるから, $p \mid \lambda_{ij}$ が成り立つ. したがって, p で割れる $(\lambda_{i1}, \cdots, \lambda_{ir}, 0, \cdots, 0)$ を持つ.

そこで, $\lambda = \lambda_{11} \cdots \lambda_{rr}$ とすると, 各 λ_{jj} は distinguished であるため, $p \nmid \lambda$ となる. したがって,

$$\left(\lambda\frac{1}{p}\lambda_{11}, \cdots, \lambda\frac{1}{p}\lambda_{rr}, 0, \cdots, 0\right)$$

は, $\lambda\dfrac{1}{p}\displaystyle\sum \lambda_{jj}u_j = 0$ を満たすので, S に含まれる.

そこで, 基本変形の演算 (f) を用いて, ある j に対して, $p \nmid \lambda_{ij}$ とできる. したがって,

$$\deg_w(\lambda_{ij}) \leq \deg(\lambda_{ij}) < \deg(\lambda_{jj}) = \deg^{(j)}(T)$$

となり, 仮定に矛盾する. よって, $A = 0$ となることがわかる. □

2.3 岩澤の定理の証明

この節では, 岩澤の定理の証明を詳しく述べることにする. まずはその道具立てとして, 記号の説明と類体論の結果を少しだけ紹介する.

$\Gamma = \mathrm{Gal}(K_\infty/K) \simeq \mathbb{Z}_p$ とする. このとき, γ_0 を Γ の位相的な生成元とする. つまり, $\Gamma = \langle \gamma_0 \rangle$ である.

L_n を K_n の最大不分岐アーベル p 拡大とする. すなわち, A_n を K_n のイデアル類群の p シロー部分群とするとき,

$$X_n = \mathrm{Gal}(L_n/K_n) \simeq A_n$$

が成り立つ. ここで, K_n のイデアル類群を $C(K_n)$ と書くことにする.

$L = \bigcup_{n\geq 0} L_n, X = \mathrm{Gal}(L/K_\infty)$ とする. このとき, L_n の最大性より, L_n/K は Galois 拡大となる. したがって, L/K も Galois 拡大となることがわかる. ここで, $G = \mathrm{Gal}(L/K)$ とする.

では次に, 証明の方針について簡単に説明することにする.

まずは, X が Γ 加群であることを示し, よって, X が Λ 加群になることを示す. その後, X は有限生成であることを示し, 前節で紹介したことから, Λ 加群の性質に則って, X は Λ^k と $\Lambda/(p^k)$ と $\Lambda/(P(T)^k)$ の形のイデアルの直和に擬同型となるが, このとき, Λ^k は現れないということを示す. この $\Lambda/(p^k)$ と $\Lambda/(P(T)^k)$ の形の直和において, n 番目の層, つまり, X_n で何が起こるかを計算し, その結果を X に持ち上げることによって証明が完成する.

では, まずは X が Γ 加群であることを示すことにする. このとき, 次の命題を使う.

命題 2.18 K_∞/K を $\mathbb{Z}_p$ 拡大とする. このとき, 少なくとも一つの素イデアルがこの拡大で分岐して, K_∞/K_e で分岐するすべての素イデアルが完全分岐になるような正の整数 e が存在する.

この命題の証明は, [?] の補題 13.3 に載っている.

X が有限生成 Λ 加群になることを証明するが, 考えやすくするため, 今は, この命題 2.18 における K_e を K と仮定して考え, 後で K を K_e に戻すことにする. つまり, 次を仮定する.

仮定 2.19 K_∞/K で分岐するすべての素イデアルは完全分岐する.

この仮定の下で, K_∞/K が不分岐拡大ならば, K の類数が無限になってしまうので, K_∞/K は不分岐拡大ではない. したがって, K_∞/K では不分岐拡大は存在しないことから, $K_{n+1} \cap L_n = K_n$ となる. つまり,

$$X_n = \mathrm{Gal}(L_n/K_n) \simeq \mathrm{Gal}(L_nK_{n+1}/K_{n+1})$$

となることがわかる. 今, $\mathrm{Gal}(L_nK_{n+1}/K_{n+1})$ は X_{n+1} の商になることから, $X_{n+1} \to X_n$ なる写像が存在し, これはイデアル類群における $A_{n+1} \to A_n$ のノルム写像に対応している.

$$X_n = \mathrm{Gal}(L_n/K_n) \simeq \mathrm{Gal}(L_nK_\infty/K_\infty)$$

より,

$$\varprojlim X_n = \mathrm{Gal}\Big(\Big(\bigcup_{n\geq 0} L_n \cdot K_\infty\Big)/K_\infty\Big) = \mathrm{Gal}(L/K_\infty) = X \tag{2.20}$$

となる.

$\gamma \in \Gamma_n = \Gamma/\Gamma^{p^n} = \mathrm{Gal}(K_n/K)$ に対して, γ を $\tilde{\gamma} \in \mathrm{Gal}(L_n/K)$ に拡張する. $x \in X_n = \mathrm{Gal}(L_n/K_n)$ に対して, γ は x に

$$x^\gamma = \tilde{\gamma} x \tilde{\gamma}^{-1}$$

と作用する.

$\tilde{\gamma_1}, \tilde{\gamma_2}$ を γ の二つの拡張とする. $\rho \in \mathrm{Gal}(L_n/K_n)$ に対して, $\tilde{\gamma_1} = \tilde{\gamma_2}\rho$ とすると,

$$x^{\gamma_1} = \tilde{\gamma_1} x {\tilde{\gamma_1}}^{-1} = \tilde{\gamma_2}\rho x(\tilde{\gamma_2}\rho)^{-1} = \tilde{\gamma_2}\rho x \rho^{-1}{\tilde{\gamma_2}}^{-1}$$

が成り立つ. $\mathrm{Gal}(L_n/K_n)$ はアーベル群より, $\rho x \rho^{-1} = x$ となり,

$$x^{\gamma_1} = \tilde{\gamma_1} x {\tilde{\gamma_1}}^{-1} = \tilde{\gamma_2} x {\tilde{\gamma_2}}^{-1} = x^{\gamma_2}$$

となる. したがって, x^γ は well defined である. よって, X_n は $\mathbb{Z}_p[\Gamma_n]$ 加群となることがわかる. また, $X \simeq \varprojlim X_n$ の元をベクトル $(x_0, x_1, \cdots)$ のように表して, $\mathbb{Z}_p[\Gamma_n]$ を n 番目の成分に作用させることで, X は $\varprojlim \mathbb{Z}_p[\Gamma_n] \simeq \Lambda$ の加群となることがわかる.

次に, $\mathcal{P}_1, \cdots, \mathcal{P}_s$ を K_∞/K で分岐する素イデアルとする. $\widetilde{\mathcal{P}_i}$ を $\mathcal{P}_i$ の上にある L の素イデアルとする. また, I_i を $\widetilde{\mathcal{P}_i}$ に対する惰性群とする. ここで, L/K_∞ は不分岐拡大より, $I_i \cap X = \{1\}$ となる.

また, 仮定 2.19 より, K_∞/K で各素イデアル $\mathcal{P}_i$ は完全分岐しているので,

$$I_i \hookrightarrow G/X = \Gamma = \mathrm{Gal}(K_\infty/K)$$

は全射となり, この写像は全単射となることがわかる. よって, $1 \leq i \leq s$ に対して, $G = XI_i = I_iX$ が成り立つ. $I_i \to \Gamma$ は全単射で, γ_0 は Γ の位相的な生成元なので, $I_i \ni \sigma_i \mapsto \gamma_0 \in \Gamma$ とすると, σ_i は I_i の位相的な生成元にならなくてはならない. そこで, $I_i \subseteq G = XI_1$ より, ある $a_i \in X$ に対して, $\sigma_i = a_i\sigma_1$ とする. ただし, $a_1 = 1$ とする. ここで, 次の補題が成り立つ.

補題 2.21 Y_0 を $\{a_i | 2 \leq i \leq s\}$ と $X^{\gamma_0 - 1} = TX$ $(T \in \mathbb{Z}_p[[T]])$ で生成される X の $\mathbb{Z}_p$ 部分加群とする.

$$\nu_n = 1 + \gamma_0 + {\gamma_0}^2 + \cdots + {\gamma_0}^{p^n - 1} = \frac{(1+T)^{p^n} - 1}{T}$$

とするとき, $Y_n = \nu_n Y_0$ とする. このとき, $n \geq 0$ に対して,

$$X_n \simeq X/Y_n$$

が成り立つ.

この補題の証明は, [?] の補題 13.15 に載っている.

次に, X が有限生成 Λ 加群であることを示す.

補題 2.22 (Nakayama) X がコンパクト Λ 加群であるとき, X が Λ 上有限生成であるための必要十分条件は $X/(p,T)X$ が有限指数になることである. ここで, コンパクトとは X の任意の開被覆が X の有限被覆を含むという意味である.

この補題の証明は, [?] の補題 13.16 に載っている. この補題を使うと次のことが言える. 次の補題は, 岩澤の定理を証明において重要なものの一つである.

補題 2.23 $X = \mathrm{Gal}(L/K_\infty)$ は有限生成 Λ 加群である.

証明

$$\nu_1 = \frac{(1+T)^p - 1}{T} \in (p, T)$$

であるから, $Y_0/(p,T)Y_0$ は $Y_0/\nu_1 Y_0$ の商であることがわかる.

$$Y_0/\nu_1 Y_0 = Y_0/Y_1 \subseteq X/Y_1 = X_1$$

となり, X_1 は有限生成であることから, Y_0 も有限生成になる. $X/Y_0 = X_0$ も有限指数になり, 補題 2.22 から X は有限生成となる. □

今までは, K_∞/K で分岐する素イデアルはすべて完全分岐するという仮定をしてきたが, ここでは, この仮定 2.19 を取り除くことにする. 命題 2.18 から, K_∞/K_e で分岐する素イデアルはすべて完全分岐となるような整数 $e \geq 0$ がとれるため, 今まで K で考えて得た結果が K_e でどうなるかを考える.

$n \geq e$ に対して,

$$1 + {\gamma_0}^{p^e} + \cdots + {\gamma_0}^{p^n - p^e} = \frac{\nu_n}{\nu_e} = \nu_{n,e}$$

とおくと, ${\gamma_0}^{p^e}$ は $\mathrm{Gal}(K_\infty/K_e)$ を生成するので, 今まで ν_n で考えていたものはすべて $\nu_{n,e}$ で考えなくてはならなくなる. したがって, K_e に対しての Y_0 を今は Y_e とすると, $n \geq e$ に対して,

$$Y_n = \nu_{n,e} Y_e \ , \ X_n \simeq X/Y_n$$

が成り立つことになる.

K_e は仮定 2.19 を満たしているので, K_e に対応する (2.20) で定義した X は X/Y_e となる. 今, X/Y_e は有限生成であり, Y_e は有限生成であるから, X は有限生成になる. 以上で, 仮定 2.19 を取り除くことができたことになる.

したがって, X は有限生成 Λ 加群であることから, 定理 2.13 を使って,

$$X \sim \Lambda^r \oplus \left(\bigoplus \Lambda/(p^{k_i})\right) \oplus \left(\bigoplus \Lambda/(f(T)^{m_j})\right)$$

が成り立つ. では, V を右辺の直和因子の一つとおいて, $V/\nu_{n,e}V$ を計算してみることにする.

(1) $V = \Lambda$ のとき

$$\nu_{n,e} = \frac{(1+T)^{p^n} - 1}{(1+T)^{p^e} - 1}$$

を計算すると, $\nu_{n,e}$ は distinguished な多項式となることから, 補題 2.9 を用いて, $V/(\nu_{n,e})$ は無限になる. ここで, $Y_e/\nu_{n,e}Y_e = Y_e/Y_n$ は有限となることから, Λ はこの直和の中には現れないことになる.

(2) $V = \Lambda/(p^k)$ のとき

$$\begin{aligned} V/\nu_{n,e}V &= (\Lambda/(p^k))/(\nu_{n,e}(\Lambda/(p^k))) \\ &\simeq \Lambda/(\nu_{n,e}, p^k) \end{aligned}$$

となる. また, $\nu_{n,e}$ は distinguished な多項式である.

$\Lambda/(\nu_{n,e}, p^k)$ の各元は, $\deg(\nu_{n,e}) = p^n - p^e$ より次数の低い多項式をさらに modulo p^k で計算した余りの多項式である. したがって, $c = -kp^e$ に対して,

$$|V/\nu_{n,e}V| = p^{k(p^n - p^e)} = p^{kp^n + c}$$

と書くことができる.

(3) $V = \Lambda/(f(T)^m)$ のとき

$g(T) = f(T)^m$ とおく.
$g(T)$ は distinguished な多項式であり, $\deg(g(T)) = d$ とする.
このとき, ある多項式 $R(T)$ に対して, $T^d - g(T) = pR(T)$ と書くことができる.

$$T^d \equiv pR(T) \pmod{g(T)}$$

とできることから, $k \geq d$ のとき,

$$T^k \equiv p\,(\text{多項式}) \pmod{g(T)}$$

と書くことができる.

$p^n \geq d$ のとき,

$$\begin{aligned}(1+T)^{p^n} &= 1 + p \cdot (\text{多項式}) + T^{p^n} \\ &\equiv 1 + p \cdot (\text{多項式}) \pmod{g(T)}\end{aligned}$$

となることから,

$$\begin{aligned}(1+T)^{p^{n+1}} &\equiv (1 + p \cdot (\text{多項式}))^p \pmod{g(T)} \\ &\equiv 1 + p^2 \cdot (\text{多項式}) \pmod{g(T)}\end{aligned}$$

が成り立つ. $P_n(T) = (1+T)^{p^n} - 1$ とおくと,

$$\begin{aligned}P_{n+2}(T) &= (1+T)^{p^{n+2}} - 1 \\ &= ((1+T)^{p^{n+1}} - 1) \cdot ((1+T)^{(p-1)p^{n+1}} + \cdots + (1+T)^{p^{n+1}} + 1) \\ &\equiv P_{n+1}(T) \cdot (1 + \cdots + 1 + p^2 \cdot (\text{多項式}) + 1) \pmod{g(T)} \\ &\equiv P_{n+1}(T) \cdot (p + p^2 \cdot (\text{多項式})) \pmod{g(T)} \\ &\equiv P_{n+1}(T) \cdot p(1 + p \cdot (\text{多項式})) \pmod{g(T)}\end{aligned}$$

となる. 今, $1 + p \cdot (\text{多項式}) \in \Lambda^\times$ より, $\dfrac{P_{n+2}(T)}{P_{n+1}(T)}$ は $V = \Lambda/(g(T))$ において, $p \cdot (\text{単数})$ の形で書けることがわかった.

そこで, $n_0 \geq e, p^{n_0} \geq d, n \geq n_0$ と仮定する. このとき,

$$\frac{\nu_{n+2,e}}{\nu_{n+1,e}} = \frac{\nu_{n+2}}{\nu_{n+1}} = \frac{P_{n+2}(T)}{P_{n+1}(T)}$$

となり,

$$\nu_{n+2,e}V = \frac{P_{n+2}(T)}{P_{n+1}(T)}(\nu_{n+1,e}V) = p \cdot (\nu_{n+1,e}V)$$

となる. したがって, $n \geq n_0$ に対して,

$$|V/\nu_{n+2,e}V| = |V/pV| \cdot |pV/(p \cdot \nu_{n+1,e}V)|$$

が成り立つ. ここで, $(g(T), p) = 1$ より, p 倍写像は単射である. つまり,

$$|pV/(p \cdot \nu_{n+1,e}V)| = |V/\nu_{n+1,e}V|$$

となる.

$V/pV \simeq \Lambda/(p, g(T)) = \Lambda/(p, T^d)$ より, $|V/pV| = p^d$ となることがわかる.

さらに,

$$|V/\nu_{n+1,e}V| = p^d |V/\nu_{n,e}V|$$

なので, 帰納法を使って, $n \geq n_0 + 1$ に対して,

$$|V/\nu_{n,e}V| = p^{d(n-n_0-1)}|V/\nu_{n_0+1,e}V|$$

と書くことができる.

つまり, $|V/\nu_{n,e}V|$ が有限のときは, $c = -d(n_0+1)$, $n \geq n_0+1$ に対して,

$$|V/\nu_{n,e}V| = p^{dn+c}$$

となる.

$|V/\nu_{n,e}V|$ が無限のときは, V は右辺には現れない. つまり, すべてをまとめると, 次の命題を得る.

命題 2.24 r, s, t, k_i は整数, $g_j(T)$ は distinguished な多項式のとき,

$$E = \Lambda^r \oplus \Big(\bigoplus_{i=1}^{s} \Lambda/(p^{k_i})\Big) \oplus \Big(\bigoplus_{j=1}^{t} \Lambda/(g_j(T))\Big)$$

とする. $m = \sum k_i, l = \sum \deg(g_j(T))$ とおく.

$E/\nu_{n,e}E$ が任意の n に対して有限のとき, $r = 0$ であり, $n > n_0$ に対して,

$$|E/\nu_{n,e}E| = p^{mp^n+ln+c}$$

なる整数 c, n_0 が存在する.

そこで, A, B を有限な Λ 加群とするとき,

$$0 \longrightarrow A \longrightarrow Y_e \longrightarrow E \longrightarrow B \longrightarrow 0$$

なる完全列を用意して, $|E/\nu_{n,e}E|$ の値はわかっていることから, $|Y_e/\nu_{n,e}Y_e|$ の値を求めることにする. ここで, 次の補題を使う.

補題 2.25 Y, E を $Y \sim E$ を満たす Λ 加群で, $n \geq e$ のとき, $Y/\nu_{n,e}Y$ が有限になるものとする. このとき, ある整数 c, n_0, $n \geq n_0$ に対して,

$$|Y/\nu_{n,e}Y| = p^c|E/\nu_{n,e}E|$$

が成り立つ.

証明　仮定より,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \nu_{n,e}Y & \longrightarrow & Y & \longrightarrow & Y/\nu_{n,e}Y & \longrightarrow & 0 \\ & & {\scriptstyle \phi_n'}\downarrow & & {\scriptstyle \phi}\downarrow & & {\scriptstyle \phi_n''}\downarrow & & \\ 0 & \longrightarrow & \nu_{n,e}E & \longrightarrow & E & \longrightarrow & E/\nu_{n,e}E & \longrightarrow & 0 \end{array}$$

となる可換図式ができる. このとき, 次の性質が成り立つ.

(a) $|\mathrm{Ker}\phi_n{}'| \leq |\mathrm{Ker}\phi|$

(b) $|\mathrm{Coker}\phi_n{}'| \leq |\mathrm{Coker}\phi|$

(c) $|\mathrm{Coker}\phi_n{}''| \leq |\mathrm{Coker}\phi|$

(d) $|\mathrm{Ker}\phi_n{}''| \leq |\mathrm{Ker}\phi| \cdot |\mathrm{Coker}\phi|$

まず, (a) についてだが, これは, $\mathrm{Ker}\phi_n{}' \subseteq \mathrm{Ker}\phi$ より明らかである.

(b) については, $\mathrm{Coker}\phi$ の元を $\nu_{n,e}$ 倍すればよいことから明らかである.

(c) については, $Y \to Y/\nu_{n,e}Y, E \to E/\nu_{n,e}E$ は共に全射であるから, $\mathrm{Coker}\phi_n{}''$ の代表元は $\mathrm{Coker}\phi$ から来るので, これも成り立つ.

(d) については, 次のようにして考える. Snake Lemma より,

$$\begin{aligned} 0 \longrightarrow \mathrm{Ker}\phi_n{}' &\longrightarrow \mathrm{Ker}\phi \longrightarrow \mathrm{Ker}\phi_n{}'' \\ &\xrightarrow{\delta} \mathrm{Coker}\phi_n{}' \longrightarrow \mathrm{Coker}\phi \longrightarrow \mathrm{Coker}\phi_n{}'' \longrightarrow 0 \end{aligned}$$

なる長完全列ができる.

ここで, δ 以外の写像は明らかであるから, ここでは δ についてのみ考えることにする.

$x \in \mathrm{Ker}\phi_n{}''$ に対して,

$$y \mapsto x \in \mathrm{Ker}\phi_n{}''$$

なる $y \in Y$ が存在する. このとき, 可換性から, $\phi(y) = 0 \in E/\nu_{n,e}E$ が成り立つ. したがって, $\phi(y) \in \nu_{n,e}E$ となる. つまり, $\phi(y) \pmod{\phi(\nu_{n,e}Y)}$ は x にのみ依存するから, $x \mapsto \phi(y)$ となることがわかる.

この長完全列と, (b) を使って,

$$\begin{aligned} |\mathrm{Ker}\phi_n{}''| &\leq |\mathrm{Ker}\phi| \cdot |\mathrm{Coker}\phi_n{}''| \\ &\leq |\mathrm{Ker}\phi| \cdot |\mathrm{Coker}\phi_n| \end{aligned}$$

が成り立つ. したがって, (d) が成り立つ.

次に, $m \geq n \geq 0$ を仮定すると,

(e) $|\mathrm{Ker}\phi_n{}'| \geq |\mathrm{Ker}\phi_m{}'|$

(f) $|\mathrm{Coker}\phi_n{}'| \geq |\mathrm{Coker}\phi_m{}'|$

(g) $|\mathrm{Coker}\phi_n{}''| \geq |\mathrm{Coker}\phi_m{}''|$

が成り立つ.

まずは, (e) について考えることにする.

$$\nu_{m,e} = \frac{\nu_{m,e}}{\nu_{n,e}} \cdot \nu_{n,e}$$

より, $\nu_{m,e}Y \subseteq \nu_{n,e}Y$ が成り立つ. したがって, $\mathrm{Ker}{\phi_m}' \subseteq \mathrm{Ker}{\phi_n}'$.

(f) については次のようにする. $\nu_{m,e}y \in \nu_{m,e}E$ とする. $\mathrm{Coker}{\phi_n}'$ における $\nu_{n,e}y$ の代表元を $z \in \nu_{n,e}E$ とおく. このとき, ある $x \in Y$ に対して,

$$\nu_{n,e}y - z = \phi(\nu_{n,e}x)$$

が成り立つ. 両辺を $\dfrac{\nu_{m,e}}{\nu_{n,e}}$ 倍すると,

$$\begin{aligned}\frac{\nu_{m,e}}{\nu_{n,e}}\nu_{n,e}y - \frac{\nu_{m,e}}{\nu_{n,e}}z &= \frac{\nu_{m,e}}{\nu_{n,e}}\phi(\nu_{n,e}x)\\ \nu_{m,e}y - \frac{\nu_{m,e}}{\nu_{n,e}}z &= \phi(\nu_{m,e}x)\\ &= {\phi_m}'(\nu_{m,e}x)\end{aligned}$$

を得る. つまり, $\mathrm{Coker}{\phi_n}'$ の代表元を $\dfrac{\nu_{m,e}}{\nu_{n,e}}$ 倍したものは, $\mathrm{Coker}{\phi_m}'$ の代表元となる. よって, (f) は成り立つ.

(g) については, $\nu_{m,e}E \subseteq \nu_{n,e}E$ なので明らかである.

今までの (a), $\cdots$, (g) を使って, $|\mathrm{Ker}{\phi_n}'|, |\mathrm{Coker}{\phi_n}'|, |\mathrm{Coker}{\phi_n}''|$ はある整数 n_0 に対して, $n \geq n_0$ のときに定数となる. また, 再び Snake Lemma を使って,

$$|\mathrm{Ker}{\phi_n}'| \cdot |\mathrm{Ker}{\phi_n}''| \cdot |\mathrm{Coker}\phi_n| = |\mathrm{Ker}\phi_n| \cdot |\mathrm{Coker}{\phi_n}'| \cdot |\mathrm{Coker}{\phi_n}''|$$

が成り立つので, $|\mathrm{Ker}{\phi_n}''|$ も $n \geq n_0$ のときに定数となる. よって, ある整数 c, n_0 に対して, $n \geq n_0$ のとき,

$$|Y/\nu_{n,e}Y| = p^c|E/\nu_{n,e}E|$$

が成り立つ. □

この補題より, $\lambda \geq 0, \mu \geq 0, \nu \in \mathbb{Z}, n_0 \in \mathbb{Z}$ が存在して, $n \geq n_0$ のとき,

$$\begin{aligned}p^{e_n} &= |X_n|\\ &= |X/Y_e| \cdot |Y_e/\nu_{n,e}Y_e|\\ &= (\text{定数}) \cdot |E/\nu_{n,e}E|\\ &= p^{\lambda n + \mu p^n + \nu}\end{aligned}$$

が成り立つ. □

3　主定理 1.2.1 の証明の準備

この章では, 主定理 1.2.1 を証明するために必要な準備をする. 特に, 1 節においては, Tate Cohomology の定義や性質, 2 節においては, 類体論におけるイデールやイデール類群, 単数群などの定義, Tate Cohomology を使った結果などを述べる. 3 節では, 種の体, 中心 p 類体の性質, 4 節では, 主定理 1.2.1 の証明に重要な定理 3.35 について詳しく述べることにする.

3.1　Tate Cohomology

Tate Cohomology とは Galois Cohomology を $-\infty$ から $+\infty$ まで拡張したものである. Tate Cohomology については, [?] の 4 章に詳しく載っている. まずは, Tate Cohomology を定義する. これは, 補題 3.10 や定理 3.35 を証明する際に使われる.

定義 3.1 (Tate Cohomology) G を有限群, A を G 加群とする.

$$
\begin{aligned}
A^G &= H^0(G,A) = \{a \in A | \sigma a = a, \forall \sigma \in G\} \\
N &= \sum_{\sigma \in G} \sigma \in \mathbb{Z}[G] \\
I_G &= \{(\sigma - 1) | \sigma \in G\} \text{ で生成される } \mathbb{Z}[G] \text{ のイデアル} \\
A_N &= \{a \in A | Na = 0\} \\
NA &= \{Na | a \in A\}
\end{aligned}
$$

とするとき, $\widehat{H}^n(G,A) = \begin{cases} H^n(G,A) & if\ n \geq 1 \\ H_{-n-1}(G,A) & if\ n \leq -2 \\ A_N/I_G A & if\ n = -1 \\ A^G/NA & if\ n = 0 \end{cases}$ を Tate Cohomology という.

このときの, H^n, H_{-n-1} とは Galois Cohomology のことである. したがって, Galois 群 G と, G 加群 A に対して, Tate Cohomology が作れて, 定理 3.35 を証明するのにこれを多用する.

補題 3.2 $0 \to A' \to A \to A'' \to 0$ を G 加群としての完全列とするとき, 次の長完全列

$$
\begin{aligned}
\widehat{H}^{-1}(G,A') \xrightarrow{f_{-1}} \widehat{H}^{-1}(G,A) &\xrightarrow{g_{-1}} \widehat{H}^{-1}(G,A'') \\
&\xrightarrow{\delta} \widehat{H}^0(G,A') \xrightarrow{f_0} \widehat{H}^0(G,A)
\end{aligned}
$$

が誘導されて次が成り立つ.

(a) $\mathrm{Im}\delta = \mathrm{Coker}g_{-1} = \mathrm{Ker}f_0 = \dfrac{(A')^G \cap NA}{NA'}$,

(b) $\mathrm{Im}g_{-1} = \mathrm{Ker}\delta = \dfrac{A_N \cdot A'}{(I_G A) \cdot A'}$,

(c) $\mathrm{Im}f_{-1} = \mathrm{Ker}g_{-1} = \dfrac{(I_G A) \cdot A'_N}{I_G A} = \dfrac{A'_N}{(I_G A) \cap A'_N}$,

(d) $\mathrm{Im}f_0 = \mathrm{Coker}\delta = \dfrac{(A')^G \cdot NA}{NA} = \dfrac{(A')^G}{(A')^G \cap NA}$.

この補題については, [**?**] の 2 節の LEMMA に載っている.

補題 3.3 (Shapiro) G を有限群, H を G の部分群, A を H 加群とする. $\Gamma = \mathbb{Z}[G]$ を左 G 加群とみなす. $A' = \mathrm{Hom}_H(\Gamma, A)$ とするとき,

$$H^n(G, A') = H^n(H, A)$$

が成り立つ.

この補題については [**?**, p.130] に載っている.

定理 3.4 (Kunneth) 環 R を単項イデアル整域, R 加群よりなる鎖複体

$$X = \{X_n, \partial_n{}'\},\ Y = \{Y_n, \partial_n{}''\}$$

において, X_n, Y_n はすべて自由 R 加群であると仮定する. このとき,

$$H_n(X \otimes_R Y) \simeq \bigoplus_{i+j=n} (H_i(X) \otimes_R H_j(Y)) \oplus \bigoplus_{i+j=n-1} \mathrm{Tor}_1^R(H_i(X), H_j(Y))$$

が成り立つ.

ただし, 鎖複体 X とは,

$$X : \cdots \longrightarrow X_n \xrightarrow{\partial_n{}'} X_{n-1} \longrightarrow \cdots \longrightarrow X_0 \xrightarrow{\partial_0{}'} 0$$

となる列で, $\partial_{n-1}{}' \circ \partial_n{}' = 0$ を満たすものである. また, $H_i(X) = \mathrm{Ker}\partial_i{}'/\mathrm{Im}\partial_{i+1}{}'$ である.

この定理の証明は, 定理 3.22[**?**, p.128] に載っている.

3.2 類体論 1

この節では, 類体論におけるいくつかの結果を紹介することにする.

k を $\mathbb{Q}$ の有限次 Galois 拡大, $G = \mathrm{Gal}(k/\mathbb{Q})$ とする.

v, w を $\mathbb{Q}, k$ のそれぞれの付値とし, w が v に拡張できる場合は $w|v$ という記号で表すことにする.

$\mathbb{Q}_v, k_w$ をそれぞれの付値における完備化した体とする. v が有限素数の場合には U_v を $\mathbb{Q}_v$ の単数とし, v が無限素数の場合には $U_v = {\mathbb{Q}_v}^{\times}$ とする. k の場合も U_w を同様に定めることにする.

$J_{\mathbb{Q}}, C_{\mathbb{Q}}$ をそれぞれ $\mathbb{Q}$ のイデール, イデール類群とする. k のときも同様に, J_k, C_k を k のイデール, イデール類群とする.

このとき,

$$U_{\mathbb{Q}} = \prod_v U_v \subseteq J_{\mathbb{Q}}$$

とする.

V_k を

$$V_k = \prod_w V_w \subseteq C_k$$

のような J_k の G 部分加群とする. ただし, V_k は,

(i) V_w は U_w の有限指数の開部分群である.

(ii) 有限個を除いた w に対して, $V_w = U_w$.

(iii) 任意の w と $\sigma \in G$ に対して, $V_{\sigma w} = \sigma V_w$.

を満たすとする.

ここで,

$$E_k = k^{\times} \cap V_k \ , \ T_k = \frac{V_k}{E_k} = \frac{k^{\times} V_k}{k^{\times}} \subseteq C_k$$

とすると, T_k は C_k の有限指数の開部分群となることから, 類体論より, k のアーベル拡大 M をただ一つ定める. したがって,

$$\mathrm{Gal}(M/k) \simeq C_k/T_k = J_k/k^{\times} V_k$$

となる. $C_k/T_k = H_k$ とおくことにする.

注 3.5 $V_k = U_k$ ならば, M は k の Hilbert 類体となり, H_k は k のイデアル類群, E_k は k の global な単数群になる.

$D_k = J_k/V_k, P_k = k^\times/E_k$ とおくと, 次の可換図式を得る.

$$
\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E_k & \longrightarrow & V_k & \longrightarrow & T_k & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & k^\times & \longrightarrow & J_k & \longrightarrow & C_k & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P_k & \longrightarrow & D_k & \longrightarrow & H_k & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}
\tag{3.6}
$$

この可換図式は, 補題 3.10 や定理 3.35 を証明するために使われる. 次に, 類体論におけるいくつかの結果を紹介する. これもまた, 補題 3.10 や定理 3.35 を証明するために使われる.

定理 3.7 L/K を有限次アーベル拡大とするとき,

$$J_K/K^\times N_{L/K} J_L = C_K/N_{L/K} C_L \simeq \mathrm{Gal}(L/K)$$

となる準同型が存在する.

この定理については, 定理 11[**?**, p.405] に載っている.

定理 3.8 (類体論の終結定理) L/K が有限次 Galois 拡大であるとき, $L \supseteq S \supseteq K$ となるような最大アーベル拡大 S/K をとるとき,

$$[L : K] = [S : K]$$

となる. つまり, $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(S/K)$ が成り立つ.

この定理の証明は [**?**, p.245] に載っている.

定理 3.9 L/K を有限次アーベル拡大, v を K の付値, w を v の上にある一つの L の付値とする. このとき,

$$K_v{}^\times/N_{L/K} L_w{}^\times \simeq \mathrm{Gal}(L_w/K_v)$$

が成り立つ.

この定理の証明は, 定理 3[**?**, p.143] に載っている.

3.3 類体論 2

ここでは, 主定理 1.2.1 の証明の準備として, 1, 2 節で定義した Tate Cohomology や類体論の結果を用いて, 種の体, これから述べる中心 p 類体に関する性質を述べることにする.

k の種の体 k_G について次の補題が成り立つ.

補題 3.10 (Leopoldt) *p を奇素数, k を $\mathbb{Q}$ 上アーベル p 拡大, $e_1, \cdots, e_t$ を $k/\mathbb{Q}$ で分岐する素数の分岐指数とするとき,*

$$[k_G : k] = \frac{e_1 \cdots e_t}{[k : \mathbb{Q}]}$$

が成り立つ.

証明　K を k の Hilbert 類体とする. $J_K, J_{\mathbb{Q}}$ を $K, \mathbb{Q}$ のそれぞれのイデールとし, $C_K, C_{\mathbb{Q}}$ を $K, \mathbb{Q}$ のイデール類群とする. $N_{K/\mathbb{Q}}$ を K から $\mathbb{Q}$ へのノルム写像とする.

このとき, 定理 3.7 より,

$$\mathrm{Gal}(K/\mathbb{Q}) \simeq C_{\mathbb{Q}}/N_{K/\mathbb{Q}}C_K \tag{3.11}$$

が成り立つ. また, 定理 3.8 より,

$$\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathrm{Gal}(k_G/\mathbb{Q}) \tag{3.12}$$

が成り立つので, (3.11), (3.12) を使って,

$$\mathrm{Gal}(k_G/\mathbb{Q}) \simeq C_{\mathbb{Q}}/N_{K/\mathbb{Q}}C_K$$

を得る. ここで, T_k を K に対応する C_k の開部分群とすると,

$$C_k/T_k \simeq \mathrm{Gal}(K/k)$$

が成り立つ. したがって, 定理 3.7 より,

$$\mathrm{Gal}(K/k) \simeq C_k/T_k \simeq C_k/N_{K/k}C_K$$

となる.

$$N_{K/\mathbb{Q}}C_K = N_{k/\mathbb{Q}}(N_{K/k}C_K) = N_{k/\mathbb{Q}}T_k$$

が成り立つので,

$$\mathrm{Gal}(k_G/\mathbb{Q}) \simeq C_{\mathbb{Q}}/N_{k/\mathbb{Q}}T_k$$

となることがわかる.

k に対して, w を k の付値とする.

$$U_k = \prod_w U_w \subseteq J_k$$

とする. ただし, w が有限素数の場合は U_w を k_w に単数とし, w が無限素数の場合は $U_w = {k_w}^\times$ とする.

I_k, P_k, E_k を k の分数イデアルの群, 単項イデアルの群, 単数群とする. また, $C(k)$ を k のイデアル類群とする. つまり,

$$C(k) \simeq I_k/P_k$$

が成り立つ. また, K は k の Hilbert 類体なので,

$$\mathrm{Gal}(K/k) \simeq C(k) \simeq C_k/T_k$$

も成り立つ.

このとき, 次の完全列が成り立つ.

(3.13)

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E_k & \longrightarrow & U_k & \longrightarrow & T_k & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & k^\times & \longrightarrow & J_k & \longrightarrow & C_k & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P_k & \longrightarrow & I_k & \longrightarrow & C(k) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

この完全列から, Tate Cohomology を考える. $G = \mathrm{Gal}(k/\mathbb{Q})$ に対して,

(3.14)

$$\begin{aligned}
&\longrightarrow \widehat{H}^{-1}(G, T_k) \xrightarrow{f_1} \widehat{H}^0(G, E_k) \xrightarrow{f_2} \widehat{H}^0(G, U_k) \\
&\qquad\qquad \xrightarrow{f_3} \widehat{H}^0(G, T_k) \xrightarrow{f_4} \widehat{H}^1(G, E_k) \longrightarrow
\end{aligned}$$

が成り立つ. Tate Cohomology の定義から,

$$\begin{aligned}
\widehat{H}^0(G, E_k) &= E_{\mathbb{Q}}/N_{k/\mathbb{Q}}E_k \\
\widehat{H}^0(G, U_k) &= U_{\mathbb{Q}}/N_{k/\mathbb{Q}}U_k \\
\widehat{H}^0(G, T_k) &= T_{\mathbb{Q}}/N_{k/\mathbb{Q}}T_k
\end{aligned}$$

となる. したがって, (3.14) は次のように書き換えることができる.

$$\begin{aligned}(3.15)\qquad \widehat{H}^{-1}(G,T_k) &\xrightarrow{f_1} E_{\mathbb{Q}}/N_{k/\mathbb{Q}}E_k \xrightarrow{f_2} U_{\mathbb{Q}}/N_{k/\mathbb{Q}}U_k \\ &\xrightarrow{f_3} T_{\mathbb{Q}}/N_{k/\mathbb{Q}}T_k \xrightarrow{f_4} \widehat{H}^{1}(G,E_k)\end{aligned}$$

このとき, (3.13) において添字を $\mathbb{Q}$ と思うと, f_3 は全射となる. また, (3.14) を使うと, $\mathrm{Im}f_1 = \mathrm{Ker}f_2$ が成り立つ. したがって, f_2 で移して $N_{k/\mathbb{Q}}U_k$ に入るような元を考えると, $E_{\mathbb{Q}} \cap N_{k/\mathbb{Q}}U_k$ となる.

したがって,

$$(3.16)\quad 0 \longrightarrow E_{\mathbb{Q}}/(E_{\mathbb{Q}} \cap N_{k/\mathbb{Q}}U_k) \longrightarrow U_{\mathbb{Q}}/N_{k/\mathbb{Q}}U_k \longrightarrow T_{\mathbb{Q}}/N_{k/\mathbb{Q}}T_k \longrightarrow 0$$

という完全列を作ることができる.

$V_{\mathbb{Q}}$ は $\mathbb{Q}$ に対応する群であり, $h(\mathbb{Q}) = 1$ なので, (3.16) を使って,

$$(3.17)\qquad |C_{\mathbb{Q}}/N_{k/\mathbb{Q}}V_k| = |C_{\mathbb{Q}}/V_{\mathbb{Q}}| \cdot |V_{\mathbb{Q}}/N_{k/\mathbb{Q}}V_k|$$

$$(3.18)\qquad = h(\mathbb{Q}) \cdot |V_{\mathbb{Q}}/N_{k/\mathbb{Q}}V_k|$$

$$(3.19)\qquad = \frac{|U_{\mathbb{Q}}/N_{k/\mathbb{Q}}U_k|}{|E_{\mathbb{Q}}/(E_{\mathbb{Q}} \cap N_{k/\mathbb{Q}}U_k)|}$$

となる.

次に, $\mathbb{Q}$ の付値 v に対して, e_v を v の $k/\mathbb{Q}$ における分岐指数とする. v の上にある k の付値の一つを w とすると,

$$1 \longrightarrow U_w \longrightarrow {k_w}^{\times} \longrightarrow \mathbb{Z} \longrightarrow 0$$

が成り立つ. これより, Tate Cohomology を考えて,

$$\begin{aligned}\longrightarrow \widehat{H}^{-1}(G,\mathbb{Z}) \longrightarrow \widehat{H}^{0}(G,U_w) \longrightarrow \widehat{H}^{0}(G,{k_w}^{\times}) \\ \longrightarrow \widehat{H}^{0}(G,\mathbb{Z}) \longrightarrow \widehat{H}^{1}(G,U_w) \longrightarrow\end{aligned}$$

となる. 今, Tate Cohomology の定義から, G は $\mathbb{Z}$ に自明に作用するので,

$$\widehat{H}^{-1}(G,\mathbb{Z}) = (\mathbb{Z})_N/I_G(\mathbb{Z}) = 0$$

となる. よって, この Cohomology の列は,

$$(3.20)\qquad 0 \longrightarrow U_v/N_{k/\mathbb{Q}}U_w \longrightarrow {\mathbb{Q}_v}^{\times}/N_{k/\mathbb{Q}}{k_w}^{\times} \longrightarrow \mathbb{Z}/n_v\mathbb{Z} \longrightarrow$$

と書き換えることができる. ただし, $n_v = [k_w : \mathbb{Q}_v]$ である.

定理 3.9 より,

$${\mathbb{Q}_v}^{\times}/N_{k/\mathbb{Q}}{k_w}^{\times} \simeq \mathrm{Gal}(k_w/\mathbb{Q}_v)$$

となる. (3.20) を完全列にするためには, $U_v/N_{k/\mathbb{Q}}U_w$ が位数 e_v の v の惰性群になることから, $\mathbb{Z}/n_v\mathbb{Z}$ が $e_v\mathbb{Z}/n_v\mathbb{Z}$ となればよいことがわかる.

したがって,

$$0 \longrightarrow U_v/N_{k/\mathbb{Q}}U_w \longrightarrow {\mathbb{Q}_v}^{\times}/N_{k/\mathbb{Q}}{k_w}^{\times} \longrightarrow e_v\mathbb{Z}/n_v\mathbb{Z} \longrightarrow 0 \tag{3.21}$$

となる完全列を得ることができる.

つまり,

$$|U_{\mathbb{Q}}/N_{k/\mathbb{Q}}U_k| = \prod_v |U_v/N_{w/v}U_w| = \prod_v e_v$$

となることと, (3.19) を使って,

$$\begin{aligned}[k_G : \mathbb{Q}] &= \frac{\prod_v e_v}{[E_{\mathbb{Q}} : (E_{\mathbb{Q}} \cap N_{k/\mathbb{Q}}U_k)]} \\ &= \frac{\prod_v e_v}{[E_{\mathbb{Q}} : (E_{\mathbb{Q}} \cap N_{k/\mathbb{Q}}U_k)]}\end{aligned}$$

となる.

今, $k/\mathbb{Q}$ が奇数次の拡大であることから, $-1 \in N_{k/\mathbb{Q}}U_k$ なので, $E_{\mathbb{Q}} = E_{\mathbb{Q}} \cap N_{k/\mathbb{Q}}U_k$ となる. したがって, $k/\mathbb{Q}$ で分岐する素数は $p_1, \cdots, p_t$ の t 個なので,

$$\begin{aligned}[k_G : \mathbb{Q}] &= \prod_v e_v \\ [k_G : k] &= \frac{e_1 \cdots e_t}{[k : \mathbb{Q}]}.\end{aligned}$$

したがって, この補題は成り立つ. □

さらに, この補題を用いて次の補題が証明できる.

補題 3.22 k を $\mathbb{Q}$ 上アーベル p 拡大となるような $\mathbb{Q}(\zeta_{m_k})$ の最大の部分体とすると, $k = k_G$ が成り立つ.

証明　$m_k = p^a p_1 \cdots p_t$ なので,

$$\mathbb{Q}(\zeta_{m_k}) = \mathbb{Q}(\zeta_{p^a}) \cdot \mathbb{Q}(\zeta_{p_1}) \cdots \mathbb{Q}(\zeta_{p_t})$$

となる. 各 $1 \leq i \leq t$ に対して, $\mathbb{Q}$ 上アーベル p 拡大となるような $\mathbb{Q}(\zeta_{p_i})$ の最大の部分体を $k(p_i)$ と書くことにする.

また, $\mathbb{Q}$ 上アーベル p 拡大となるような $\mathbb{Q}(\zeta_{p^a})$ の最大の部分体を $k(p)$ と書くことにする.

今, k は $\mathbb{Q}$ 上アーベル p 拡大となるような $\mathbb{Q}(\zeta_{m_k})$ の最大の部分体であることから,

$$k = k(p) \cdot k(p_1) \cdots k(p_t)$$

と書くことができる.

各 $1 \leq i \leq t$ に対して, p_i は $\mathbb{Q}(\zeta_{p_i})$ でのみ分岐し, p_i 以外の素数は分岐しないことから, $k/\mathbb{Q}$ で分岐する素数は全部で $t+1$ 個あり, 各素数の分岐指数を $e_p, e_{p_1}, \cdots, e_{p_t}$ とおくと,

$$e_p = [k(p) : \mathbb{Q}], e_{p_1} = [k(p_1) : \mathbb{Q}], \cdots, e_{p_t} = [k(p_t) : \mathbb{Q}]$$

が成り立つ.

したがって, 補題 3.10 を用いると,

$$\begin{aligned}
[k_G : k] &= \frac{e_p \cdot e_{p_1} \cdots e_{p_t}}{[k : \mathbb{Q}]} \\
&= \frac{[k(p) : \mathbb{Q}] \cdot [k(p_1) : \mathbb{Q}] \cdots [k(p_t) : \mathbb{Q}]}{[k : \mathbb{Q}]} \\
&= 1
\end{aligned}$$

となることから, $k_G = k$ となる. □

補題 2.3.1 より, k が $\mathbb{Q}$ 上アーベル p 拡大であることを使うと, 各素数の分岐指数である $e_1, \cdots, e_t$ はすべて p 巾になることから, $[k_G : k]$ の値も p 巾となり, k_G は $\mathbb{Q}$ 上アーベル p 拡大となることがわかる.

注 3.23 $h(k)$ を k の類数とするとき, $p \nmid h(k)$ と仮定すると, k は不分岐なアーベル p 拡大は持たないことから, $k_G = k$ が成り立つ.

次に, k の中心 p 類体, 基本中心 p 類体を定義し, その性質を述べる.

定義 3.24 (中心 p 類体) k の中心 p 類体 k_C とは, k 上不分岐アーベル p 拡大であり, $\mathbb{Q}$ 上 Galois 拡大であり, $\mathrm{Gal}(k_C/k) \subseteq Z(\mathrm{Gal}(k_C/\mathbb{Q}))$ を満たすような k の最大 p 拡大のことである.

定義 3.25 (基本中心 p 類体) k の基本中心 p 類体 C とは, k 上不分岐 Galois 拡大であり, $\mathrm{Gal}(C/k) \subset Z(\mathrm{Gal}(C/\mathbb{Q}))$ を満たし, $\mathrm{Gal}(C/\mathbb{Q})$ を $\mathrm{Gal}(C/k)$ で割った商が基本アーベル群になるような k_C の最大の部分体である.

このとき, C は k_C において, $\mathrm{Gal}(k_C/k)^p$ の固定体となる.

ここで定義した中心 p 類体について次の補題が成り立つ.

補題 3.26 $p \nmid h(k)$ であるための必要十分条件は $k_C = k$ が成り立つことである.

証明　十分条件については, $p \nmid h(k)$ という仮定より, k は不分岐アーベル p 拡大を持たないことになり, $k_C = k$ は明らかである.

必要条件については, 対偶をとって示すことにする.

$p \mid h(k)$ を仮定すると, k は非自明な不分岐アーベル p 拡大を持つことになる. これを F とする. k の $\mathbb{Q}$ 上の Galois 閉包を $\widetilde{F}$ とおくことにする. このとき, $F \subseteq \widetilde{F}$ になる.

$\sigma \in \mathrm{Gal}(\widetilde{F}/k)$ に対して, $\sigma(F)/\sigma(k) = \sigma(F)/k$ は不分岐アーベル p 拡大 となる. $\widetilde{F}$ は $\sigma(F)$ の合成体であるから, $\widetilde{F}/k$ は不分岐アーベル p 拡大 となる.

そこで, $H = \mathrm{Gal}(\widetilde{F}/k), \Gamma = \mathrm{Gal}(\widetilde{F}/\mathbb{Q})$ とするとき,

$$\mathrm{Gal}(E/k) = H/N \subseteq Z(\Gamma/N) = Z(\mathrm{Gal}(E/\mathbb{Q}))$$

を満たす Γ の正規部分群で, H に真に含まれる N が存在することが言えれば良いことになる. ここで, E は N に対応する体である.

Γ は p 群なので,

$$\Gamma = \Gamma_0 \supseteq \Gamma_1 = [\Gamma_0, \Gamma_0] \supseteq \Gamma_2 = [\Gamma_0, \Gamma_1] \supseteq \cdots \supseteq \{e\}$$

なる中心列を持つ.

$\Gamma_1 = \{e\}$ のとき, $N = \Gamma_1$ とする. $[\Gamma_0, \Gamma_0] = \{e\}$ より, Γ はアーベル群になる. したがって,

$$H/N = H \subseteq Z(\Gamma/N) = Z(\Gamma) = \Gamma$$

となり, F は k の非自明な中心 p 類体に入る.

$\Gamma_1 \neq \{e\}$ のとき,

$$\Gamma \supsetneq H \supsetneq \Gamma_1$$

の場合と,

$$\Gamma \supsetneq H = \Gamma_1 \supsetneq \Gamma_2$$

の場合がある.

そこで, $\Gamma \supsetneq H \supsetneq \Gamma_1$ のとき, $N = \Gamma_1$ とする. Γ/H はアーベルになることから, $\Gamma_1 = [\Gamma_0, \Gamma_0] \subsetneq H$ が成り立つ. したがって, Γ/Γ_1 はアーベルになる. よって,

$$\{e\} \neq H/N \subseteq \Gamma/N = \Gamma/\Gamma_1 = Z(\Gamma/\Gamma_1) = Z(\Gamma/N)$$

より, E は k の非自明な中心 p 類体に入る.

$\Gamma \supsetneq H = \Gamma_1 \supsetneq \Gamma_2$ のとき, $N = \Gamma_2$ とする.

$$\Gamma/\Gamma_2 \supseteq \Gamma_1/\Gamma_2 \neq \{e\}$$

より,

$$\Gamma_1/N \subseteq Z(\Gamma/\Gamma_2)$$

となり, E は非自明な k の中心 p 類体に入る.

したがって, 非自明な中心 p 類体が存在することから, $k_C \neq k$ となることがわかる. □

さらに, k の中心 p 類体に対して次に示す命題 3.28 が成り立つ. まず, 命題 3.28 の証明に必要な補題を証明する.

補題 3.27 *G を有限群, $Z(G)$ を G の中心, $[G,G]$ を G の交換子部分群とする. このとき, ある $m \in \mathbb{Z}$ に対して*

$$[G,G] \subseteq Z(G)\ ,\ [G,G]^m = e \ \text{ ならば } \ G^m \subseteq Z(G)$$

が成り立つ.

証明　$a, b \in G$ に対して, $[a,b] = a^{-1}b^{-1}ab$ とする. このとき, $a, b, c \in G$ に対して,

$$\begin{aligned}
[ab,c] &= (ab)^{-1}c^{-1}abc \\
&= b^{-1}a^{-1}c^{-1}abc \\
&= b^{-1}a^{-1}c^{-1}acc^{-1}bc \\
&= b^{-1}[a,c]bb^{-1}c^{-1}bc \\
&= b^{-1}[a,c]b[b,c]
\end{aligned}$$

が成り立つ. そこで, $[G,G] \subseteq Z(G)$ なので, $g \in G$ に対して,

$$G \ni x \mapsto [x,g] \in [G,G]$$

という対応をつけることで,

$$\begin{aligned}
G \ni xy \mapsto [xy,g] &= y^{-1}[x,g]y[y,g] \\
&= [x,g][y,g] \in [G,G]
\end{aligned}$$

となり, 準同型が成り立つ. ここで, $[G,G]^m = e$ なので,

$$[x,g]^m = [x^m,g] = e$$

となり, $G^m \subseteq Z(G)$ である. □

このとき, この補題を用いて次の命題を示す.

命題 3.28 *k を $k_G = k$ なる $\mathbb{Q}$ 上アーベル p 拡大, k' を $\mathrm{Gal}(k'/\mathbb{Q})$ が基本アーベル群になるような $k/\mathbb{Q}$ の最大の中間拡大とするとき,*

$$\mathrm{rank}_p[\mathrm{Gal}(k_C/k)] = \mathrm{rank}_p[\mathrm{Gal}({k'}_C/k')]$$

が成り立つ. ただし, $\mathrm{rank}_p[\mathrm{Gal}(k_C/k)]$ とは $\mathrm{Gal}(k_C/k)$ を p 巾位数の巡回群の直積で書いたときの巡回群の個数のことである.

証明　この命題の証明は $\mathrm{Gal}(k/\mathbb{Q})$ が $k/\mathbb{Q}$ で分岐する素数の惰性群の直積で書けることがポイントである.

C を k の基本中心 p 類体とする. (定義 3.25 を参照.)

C は k_C において, $\mathrm{Gal}(k_C/k)^p$ の固定体になることから,

$$\mathrm{Gal}(k_C/k)/\mathrm{Gal}(k_C/k)^p = \mathrm{Gal}(C/k)$$

が成り立つので,

$$\mathrm{rank}_p[\mathrm{Gal}(k_C/k)] = \mathrm{rank}_p[\mathrm{Gal}(C/k)]$$

が成り立つ. したがって, C' を k' の基本中心 p 拡大として,

$$\mathrm{rank}_p[\mathrm{Gal}(C/k)] = \mathrm{rank}_p[\mathrm{Gal}(C'/k')]$$

を示すことにする.

つまり, (a) $k \cap C' = k'$ と (b) $kC' = C$ を示すことができれば, $\mathrm{Gal}(C/k) \simeq \mathrm{Gal}(C'/k')$ となり, 命題が証明できたことになる.

(a) $k \cap C' = k'$ について

q を $k/\mathbb{Q}$ で分岐する素数とする. $k/\mathbb{Q}$ はアーベル拡大なので, q を分解したときに現れる素イデアルのそれぞれの惰性群はすべて同じになる. したがって, q の $\mathrm{Gal}(k/\mathbb{Q})$ での共通の惰性群を $T_{k/\mathbb{Q}}(q)$ と書くことにする.

仮定より, 補題 3.10 から, $k_G = k$ なので,

$$\mathrm{Gal}(k/\mathbb{Q}) = \prod T_{k/\mathbb{Q}}(q)$$

と書くことができる. $\mathrm{Gal}(k'/\mathbb{Q})$ は $\mathrm{Gal}(k/\mathbb{Q})$ の商が基本アーベル群になるような最大の部分群なので,

$$\mathrm{Gal}(k/k') = \mathrm{Gal}(k/\mathbb{Q})^p = \prod T_{k/\mathbb{Q}}(q)^p \tag{3.29}$$

となる.

ここで, q' を q 上にある k' の素イデアルとし, $T_{k/k'}(q')$ を k/k' で分岐する素イデアルの共通の惰性群とすると,

$$\begin{aligned} T_{k/k'}(q') &= T_{k/\mathbb{Q}}(q) \cap \mathrm{Gal}(k/\mathbb{Q})^p \\ &= T_{k/\mathbb{Q}}(q) \cap \prod T_{k/\mathbb{Q}}(q)^p \\ &= T_{k/\mathbb{Q}}(q)^p. \end{aligned}$$

が成り立つ. したがって,

$$T_{k/k'}(q') = T_{k/\mathbb{Q}}(q)^p \tag{3.30}$$

となる.

(3.29), (3.30) を使って,

$$\mathrm{Gal}(k/k') = \prod T_{k/\mathbb{Q}}(q)^p = \prod T_{k/k'}(q')$$

より, k' は k に含まれる不分岐拡大を持たないことがわかる. よって, $k \cap C' = k'$ となる.

(b) $kC' = C$ について

今までと同様に, q を $k/\mathbb{Q}$ で分岐する素数とする. このとき, $\mathcal{P}_1$ を q 上にある C の素イデアルとする. $T(\mathcal{P}_1)$ を $\mathcal{P}_1$ の惰性群とすると, $T(\mathcal{P}_1)$ は $\mathrm{Gal}(C/\mathbb{Q})$ の部分群になる.

今, C/k は不分岐拡大なので, q_k を q 上の k の素イデアルとするとき, $\prod T_{C/k}(q_k) = \mathrm{Gal}(C/k)$ であることから,

$$T(\mathcal{P}_1) \simeq T_{k/\mathbb{Q}}(q)\ ,\ T(\mathcal{P}_1)^p \simeq T_{k/k'}(q')$$

が成り立つ.

また, $\mathcal{P}_2$ を p 上にある C の別な素イデアルとすると, 素イデアルは Galois 群の元で移り合うので,

$$\mathcal{P}_1 = g(\mathcal{P}_2)$$

なる $g \in \mathrm{Gal}(C/\mathbb{Q})$ が存在する. この g に対して,

$$g^{-1}T(\mathcal{P}_1)g = T(\mathcal{P}_2)$$

が成り立つ.

今, 定義から, $\mathrm{Gal}(C/k) \subseteq Z(\mathrm{Gal}(C/\mathbb{Q}))$ であり, $\mathrm{Gal}(k/\mathbb{Q}) = \mathrm{Gal}(C/\mathbb{Q})/\mathrm{Gal}(C/k)$ はアーベル群である.

$a \cdot \mathrm{Gal}(C/k), b \cdot \mathrm{Gal}(C/k) \in \mathrm{Gal}(C/\mathbb{Q})/\mathrm{Gal}(C/k)$ に対して,

$$(a \cdot \mathrm{Gal}(C/k))(b \cdot \mathrm{Gal}(C/k)) = (b \cdot \mathrm{Gal}(C/k))(a \cdot \mathrm{Gal}(C/k))$$

であることと, $\mathrm{Gal}(C/k) \subseteq Z(\mathrm{Gal}(C/\mathbb{Q}))$ を使って,

$$ab \cdot \mathrm{Gal}(C/k) = ba \cdot \mathrm{Gal}(C/k)$$

が成り立つ. したがって, $aba^{-1}b^{-1} \in \mathrm{Gal}(C/k) \subseteq Z(\mathrm{Gal}(C/\mathbb{Q}))$ となり,

$$[\mathrm{Gal}(C/\mathbb{Q}), \mathrm{Gal}(C/\mathbb{Q})] \subseteq \mathrm{Gal}(C/k)$$

が成り立つ. また, C の定義から, $\mathrm{Gal}(C/k)^p = \{e\}$ となる. したがって, 補題 3.27 より,

$$\mathrm{Gal}(C/\mathbb{Q})^p \subseteq Z(\mathrm{Gal}(C/\mathbb{Q}))$$

となり, $T(\mathcal{P}_1)^p \subset Z(\mathrm{Gal}(C/\mathbb{Q}))$ なので,

$$\begin{aligned}(g^{-1}T(\mathcal{P}_1)g)^p &= T(\mathcal{P}_2)^p \\ g^{-1}T(\mathcal{P}_1)^p g &= T(\mathcal{P}_2)^p \\ T(\mathcal{P}_1)^p &= T(\mathcal{P}_2)^p\end{aligned}$$

である. したがって, $T(\mathcal{P}_1)^p = T_{C/k'}(q')$ として共通の惰性群を定義することができる.

C'' を $\prod T_{C/k'}(q')$ の固定体とすると, C''/k' は不分岐拡大であり, $C'' \cap k = k'$ となる.

今, $\mathrm{Gal}(C/k) \to \mathrm{Gal}(C/k')$ なる単射が存在し,

$$\mathrm{Gal}(C/k') \to \mathrm{Gal}(C/k')/\mathrm{Gal}(C/C'') \simeq \mathrm{Gal}(C''/k')$$

なる自然な写像が存在する. $\mathrm{Gal}(C/k)$ は基本アーベル群なので, $\mathrm{Gal}(C''/k')$ は基本アーベル群となる. また,

$$\mathrm{Gal}(C/k) \subseteq Z(\mathrm{Gal}(C/\mathbb{Q}))$$

なので,

$$\mathrm{Gal}(C''/k') \subseteq Z(\mathrm{Gal}(C''/\mathbb{Q}))$$

が成り立つ. C' の最大性から, $C'' \subseteq C'$ となる.

最後に,

$$[C : k'] = [C : k][k : k'] \tag{3.31}$$

$$= [C : C'][C' : k'] \leq [C : C''][C' : k'] \tag{3.32}$$

なので, (3.31) を使って,

$$[C : k][k : k'] = [C : k]\left|\prod T_{k/k'}(q')\right| \tag{3.33}$$

となり, (3.32) を使って,

$$[C : C''][C' : k'] = \left|\prod T_{C/k'}(q')\right|[C' : k'] \tag{3.34}$$

となる.

(3.32), (3.33), (3.34) を使って,

$$[C : k]\left|\prod T_{k/k'}(q')\right| \leq \left|\prod T_{C/k'}(q')\right|[C' : k']$$

が成り立つ. C/k は不分岐拡大なので, $T_{k/k'}(q') \simeq T_{C/k'}(q')$ となり,

$$\left|\prod T_{k/k'}(q')\right| = \left|\prod T_{C/k'}(q')\right|$$

となる. したがって, $[C : k] \leq [C' : k']$ となる.

一方, $kC' \subseteq C$ なので, (a) を使って,

$$[C : k] \geq [kC' : k] = [C' : C' \cap k] = [C' : k']$$

となり, この二つを合わせると, $[C : k] = [C' : k']$ である. したがって, $kC' = C$ が成り立つ. □

この命題と補題 3.26 を合わせると, 次のことがわかる.

$$\begin{aligned} p \nmid h(k) &\iff k_C = k \\ &\iff k'_C = k' \end{aligned}$$

3.4 定理 3.35 について

この章では, 次に紹介する定理 3.35 の証明をする. この定理 3.35 は, 主定理 1.2.1 証明するために非常に重要なもので, [?] に詳細が載っている. まずは, この定理を紹介する.

定理 3.35 k を $k_G = k$ であり, $\mathrm{Gal}(k/\mathbb{Q})$ が基本アーベル群になるようなアーベル p 拡大とするとき,

$$\mathrm{Gal}(k_C/k) \simeq \mathrm{Coker}(\bigoplus_{i=1}^{n} \wedge^2(G_{p_i}) \to \wedge^2(G))$$

が成り立つ. ただし, $G = \mathrm{Gal}(k/\mathbb{Q})$ であり, G_{p_i} は $k/\mathbb{Q}$ で分岐する素数に対する分解群である.

この定理 3.35 は主定理を証明する際に非常に重要なものである. 証明は次のように類体論を使う.

類体論 1 において定義した記号を使って, k の種の体や, 後で定義する k の中心類体 k_Z が k のイデール類群 C_k のどんな開部分群と対応しているかについて述べる. その後, k の中心類体 k_Z が $k/\mathbb{Q}$ がアーベル p 拡大であることから, k の中心 p 類体 k_C になるということを示す.

証明　$k/\mathbb{Q}$ はアーベル p 拡大, $G = \mathrm{Gal}(k/\mathbb{Q})$ とする. これから出てくる記号 C_k, J_k, V_k などは, 類体論 1 で定義したものと同じである.

$$E_k = k^\times \cap V_k \ , \ T_k = \frac{V_k}{E_k} = \frac{k^\times V_k}{k^\times} \subseteq C_k$$

とすると, T_k は C_k の有限指数の開部分群となることから, 類体論 1 より, k のアーベル拡大 M をただ一つ定める. 今回は, この M を k の Hilbert 類体とする. したがって,

$$\mathrm{Gal}(M/k) \simeq C_k/T_k = J_k/k^\times U_k \tag{3.36}$$

となる. このとき, $C_k/T_k \simeq C(k)$ であり, E_k は k の global な単数群となる.

$D_k = J_k/U_k, P_k = k^\times/E_k$ とおくと,

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E_k & \longrightarrow & U_k & \longrightarrow & T_k & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & k^\times & \longrightarrow & J_k & \longrightarrow & C_k & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P_k & \longrightarrow & D_k & \longrightarrow & C(k) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

となる可換図式を得る.

この可換図式より, Tate Cohomology を考えると,

$$\begin{array}{ccccc}
\widehat{H}^{-1}(G,U_k) & \xrightarrow{\lambda} & \widehat{H}^{-1}(G,T_k) & \xrightarrow{\rho} & \widehat{H}^{0}(G,E_k) \\
\downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \tau} \\
\widehat{H}^{-1}(G,J_k) & \xrightarrow{\theta} & \widehat{H}^{-1}(G,C_k) & \xrightarrow{\delta} & \widehat{H}^{0}(G,k^\times) \\
\downarrow{\scriptstyle \nu} & & \downarrow{\scriptstyle \sigma} & & \\
\widehat{H}^{-1}(G,D_k) & \xrightarrow{\mu} & \widehat{H}^{-1}(G,C(k)) & &
\end{array} \tag{3.37}$$

となる. ここで,

$$U_{\mathbb{Q}} = {U_k}^G, E_{\mathbb{Q}} = {E_k}^G = \mathbb{Q}^\times \cap U_{\mathbb{Q}}, T_{\mathbb{Q}} = U_{\mathbb{Q}}/E_{\mathbb{Q}}$$

とおくと, 補題 3.2 より次の補題を得る.

補題 3.38 (a) $\mathrm{Im}\delta = \mathrm{Coker}\theta = \dfrac{\mathbb{Q}^\times \cap N_{k/\mathbb{Q}}J_k}{N_{k/\mathbb{Q}}k^\times}$,

(b) $\mathrm{Im}\sigma = \mathrm{Coker}\beta = \dfrac{(C_k)_{N_{k/\mathbb{Q}}} \cdot T_k}{(I_G C_k)\cdot T_k}$,

(c) $\mathrm{Im}\rho = \dfrac{E_{\mathbb{Q}} \cap N_{k/\mathbb{Q}}U_k}{N_{k/\mathbb{Q}}E_k}$,

(d) $\mathrm{Im}\tau = \dfrac{E_{\mathbb{Q}}}{E_{\mathbb{Q}} \cap N_{k/\mathbb{Q}}k^\times}$,

(e) $\mathrm{Ker}\tau = \dfrac{E_{\mathbb{Q}} \cap N_{k/\mathbb{Q}}k^\times}{N_{k/\mathbb{Q}}E_k}$.

が成り立つ. ただし, $N_{k/\mathbb{Q}}$ とは k から $\mathbb{Q}$ へのノルム写像である.

次に, k の種の体 k_G , k の中心類体 k_Z とイデール類群 C_k の開部分群との関係について考える. まずは, k の中心類体 k_Z を定義する.

定義 3.39 k の中心類体 k_Z とは, k 上不分岐アーベル拡大であり, $\mathbb{Q}$ 上 Galois 拡大であり, $\mathrm{Gal}(k_Z/k) \subseteq Z(\mathrm{Gal}(k_Z/\mathbb{Q}))$ を満たすような k の最大のアーベル拡大である.

このとき, k の種の体 k_G と k の中心類体 k_Z とが, イデール類群 C_k の開部分群とどのような関係になっているかについて, 次の命題が成り立つ.

命題 3.40 T_k を C_k の有限指数の開部分群とし, M/k を T_k に対応する類体とする. このとき, k_Z/k は $I_G C_k \cdot T_k$ に対応する類体で, k_G/k は $(C_k)_{N_{k/\mathbb{Q}}} \cdot T_k$ に対応する類体である.

証明　今, M は k の Hilbert 類体であり, M/k に対応する類体は T_k である. H/k を $\mathbb{Q}$ 上 Galois となる M/k の部分体とする. また, H/k を $S_k \supseteq T_k$ に対応する類体とする.

$$\mathrm{Gal}(H/k) \simeq C_k/S_k$$

が成り立つ.

(a) k_Z/k が $I_G C_k \cdot T_k$ に対応する類体であることを示す.

$g \in G = \mathrm{Gal}(k/\mathbb{Q})$ に対して, g を $\tilde{g} \in \mathrm{Gal}(H/\mathbb{Q})$ に拡張する. このとき, $n \in \mathrm{Gal}(H/k)$ に対して, g は,

$$n^g = \tilde{g} n \tilde{g}^{-1}$$

と作用する.

したがって, $\mathrm{Gal}(H/k) \subseteq Z(\mathrm{Gal}(H/\mathbb{Q}))$ であるためには, $G = \mathrm{Gal}(k/\mathbb{Q})$ が共役の作用で $\mathrm{Gal}(H/k)$ を不変にすればよいことになる.

このとき, G が共役の作用で $\mathrm{Gal}(H/k) \simeq C_k/S_k$ を不変にするとは, $I_G C_k \subset S_k$ が成り立つこと必要十分である.

なぜならば, $I_G C_k \subset S_k$ を仮定すると, $x \in C_k$ と, $g \in G$ に対して,

$$(x^g)(x^{-1}) \in I_G C_k \subset S_k$$

より, G は C_k/S_k に自明に作用することがわかる.

逆に, G が C_k/S_k に自明に作用するならば, 任意の $x \in C_k$ と, $g \in G$ に対して,

$$(x^g)(x^{-1}) \in S_k$$

が成り立つことから, $(gx)(x^{-1}) \in I_G C_k$ より, $I_G C_k \subset S_k$.

$H = k_Z$ とすると, S_k は T_k と $I_G C_k$ を含んだ最小の有限指数となる開部分群でなくてはならない.

ここで, T_k は M に対応していることから, $I_G C_k \cdot T_k$ が有限指数の最小な開部分群となっていて, k_Z/k は $I_G C_k \cdot T_k$ に対応している類体となる.

(b) k_G/k が $(C_k)_{N_{k/\mathbb{Q}}} \cdot T_k$ に対応する類体であることを示す.

定理 3.7 より,

$$\mathrm{Gal}(k/\mathbb{Q}) \simeq C_{\mathbb{Q}}/N_{k/\mathbb{Q}}C_k \tag{3.41}$$

が成り立つ. また, 定理 3.8 より,

$$\mathrm{Gal}(k_G/\mathbb{Q}) \simeq \mathrm{Gal}(M/\mathbb{Q}) \tag{3.42}$$

$$\simeq C_{\mathbb{Q}}/N_{M/\mathbb{Q}}C_M \tag{3.43}$$

が成り立つ. M/k は T_k に対応する類体なので,

$$C_k/T_k \simeq \mathrm{Gal}(M/k) \simeq C_k/N_{M/k}C_M \tag{3.44}$$

となるので,

$$N_{M/\mathbb{Q}}C_M = N_{k/\mathbb{Q}}(N_{M/k}C_M) = N_{k/\mathbb{Q}}T_k \tag{3.45}$$

が成り立つ. したがって, (3.43), (3.45) を使って,

$$\mathrm{Gal}(k_G/\mathbb{Q}) \simeq C_{\mathbb{Q}}/N_{M/\mathbb{Q}}C_M \tag{3.46}$$

$$\simeq C_{\mathbb{Q}}/N_{k/\mathbb{Q}}T_k \tag{3.47}$$

となる. (3.47), (3.41) を使って,

$$\begin{aligned}\mathrm{Gal}(k_G/k) &\simeq \mathrm{Gal}(k_G/\mathbb{Q})/\mathrm{Gal}(k/\mathbb{Q}) \\ &\simeq (C_{\mathbb{Q}}/N_{k/\mathbb{Q}}T_k)/(C_{\mathbb{Q}}/N_{k/\mathbb{Q}}C_k) \\ &\simeq C_k/{N_{k/\mathbb{Q}}}^{-1}(N_{k/\mathbb{Q}}T_k) \\ &\simeq C_k/(C_k)_{N_{k/\mathbb{Q}}} \cdot T_k\end{aligned}$$

が成り立つ. ここで,

$$(C_k)_{N_{k/\mathbb{Q}}} = \{x \in C_k | N_{k/\mathbb{Q}}(x) = 1\}$$

である.

したがって, k_G/k は $(C_k)_{N_{k/\mathbb{Q}}} \cdot T_k$ に対応する類体である. □

ここで, 補題 3.38 と命題 3.40 より, 次の系が成り立つ.

系 3.48

$$\mathrm{Im}\sigma \simeq \mathrm{Gal}(k_Z/k_G)$$

が成り立つ.

証明　次のような完全列

$$0 \longrightarrow \frac{(C_k)_{N_{k/\mathbb{Q}}} \cdot T_k}{I_G C_k \cdot T_k} \longrightarrow \frac{C_k}{I_G C_k \cdot T_k} \longrightarrow \frac{C_k}{(C_k)_{N_{k/\mathbb{Q}}} \cdot T_k} \longrightarrow 0$$

を考えると,

$$\begin{aligned} \mathrm{Im}\sigma &= \frac{(C_k)_{N_{k/\mathbb{Q}}} \cdot T_k}{I_G C_k \cdot T_k} \\ \mathrm{Gal}(k_Z/k) &= \frac{C_k}{I_G C_k \cdot T_k} \\ \mathrm{Gal}(k_G/k) &= \frac{C_k}{(C_k)_{N_{k/\mathbb{Q}}} \cdot T_k} \end{aligned}$$

となることから, Galois 群の性質を使うと明らかである. □

ここで, $\mathrm{Im}\sigma$ について考える.

今,

$$\mathrm{Im}\delta\beta = \frac{\mathrm{Im}\beta}{\mathrm{Im}\beta \cap \mathrm{Ker}\delta}$$

となる. (3.37) を使って,

$$\mathrm{Im}\delta = \widehat{H}^{-1}(G, C_k)/\mathrm{Im}\theta, \mathrm{Im}\beta = \mathrm{Ker}\sigma, \mathrm{Ker}\delta = \mathrm{Im}\theta$$

が成り立つので,

$$\frac{\mathrm{Im}\delta}{\mathrm{Im}\delta\beta} = \mathrm{Im}\delta \cdot \frac{\mathrm{Im}\beta \cap \mathrm{Ker}\delta}{\mathrm{Im}\beta} \tag{3.49}$$

$$= \frac{\widehat{H}^{-1}(G, C_k)}{\mathrm{Im}\theta} \cdot \frac{\mathrm{Ker}\sigma \cap \mathrm{Im}\theta}{\mathrm{Ker}\sigma} \tag{3.50}$$

$$= \frac{\widehat{H}^{-1}(G, C_k)}{\mathrm{Ker}\sigma} \cdot \frac{\mathrm{Ker}\sigma \cap \mathrm{Im}\theta}{\mathrm{Im}\theta} \tag{3.51}$$

$$= \frac{\mathrm{Im}\sigma}{\mathrm{Im}\sigma\theta} \tag{3.52}$$

が得られる. このとき, 次の補題が成り立つ.

補題 3.53 $k/\mathbb{Q}$ がアーベル p 拡大のとき, $|\mathrm{Im}\delta\beta| = 1$ が成り立つ.

証明　$\mathrm{Im}\delta\beta = \mathrm{Im}\tau\rho$ となることから, $|\mathrm{Im}\tau\rho| = 1$ となることを示す.

補題 3.38 の (c) より,

$$\mathrm{Im}\rho = \frac{E_{\mathbb{Q}} \cap N_{k/\mathbb{Q}} U_k}{N_{k/\mathbb{Q}} E_k}$$

となる.

$k/\mathbb{Q}$ はアーベル p 拡大なので, $-1 \in N_{k/\mathbb{Q}}U_k$ となり, $E_{\mathbb{Q}} \cap N_{k/\mathbb{Q}}U_k = E_{\mathbb{Q}}$ が成り立つ.

また, $N_{k/\mathbb{Q}}E_k = E_{\mathbb{Q}}$ なので, $|\mathrm{Im}\rho| = 1$ が成り立つ. □

したがって, この補題を使って, (3.52) は次のように書くことができる.

$$\frac{|\mathrm{Im}\delta|}{|\mathrm{Im}\delta\beta|} = \frac{|\mathrm{Im}\sigma|}{|\mathrm{Im}\sigma\theta|} \tag{3.54}$$

$$|\mathrm{Im}\delta| = \frac{|\mathrm{Im}\sigma|}{|\mathrm{Im}\sigma\theta|} \tag{3.55}$$

次に, $\mathrm{Im}\sigma\theta$ について考えることにする.

補題 3.3 より, Cohomology 群 $\widehat{H}^q(G, J_k), \widehat{H}^q(G, U_k)$ は local に計算することができて,

$$\widehat{H}^q(G, J_k) = \bigoplus_v \widehat{H}^q(G, \prod_{w|v} {k_w}^\times) = \bigoplus_v \widehat{H}^q(G_w, {k_w}^\times) \tag{3.56}$$

と,

$$\widehat{H}^q(G, V_k) = \bigoplus_v \widehat{H}^q(G, \prod_{w|v} U_w) = \bigoplus_v \widehat{H}^q(G_w, U_w) \tag{3.57}$$

が成り立つことがわかる.

このとき, (3.56), (3.57) における最後の項の w は v の上にあるいくつかの素数のうちの一つとする.

ここで, 写像 $\gamma : \widehat{H}^{-1}(G, U_k) \to \widehat{H}^{-1}(G, J_k)$ を, $\gamma = \oplus_v \gamma_w$ のとき,

$$\gamma_w : \widehat{H}^{-1}(G_w, U_w) \to \widehat{H}^{-1}(G_w, {k_w}^\times)$$

なる写像と決めて, γ を以上のような写像からできるものとする.

ここで,

$$0 \longrightarrow U_w \longrightarrow {k_w}^\times \xrightarrow{w} \mathbb{Z} \longrightarrow 0$$

という完全列が成り立つことから,

$$\longrightarrow \widehat{H}^{-1}(G_w, U_w) \xrightarrow{\gamma_w} \widehat{H}^{-1}(G_w, {k_w}^\times) \longrightarrow \widehat{H}^{-1}(G_w, \mathbb{Z}) \longrightarrow \tag{3.58}$$

という Tate Cohomology の完全列ができる. このとき, 定義から, G は $\mathbb{Z}$ に自明に作用するので,

$$\widehat{H}^{-1}(G_w, \mathbb{Z}) = \mathbb{Z}_{N_{k/\mathbb{Q}}}/(I_{G_w}\mathbb{Z}) = 0$$

となる. よって, (3.58) は,

$$\longrightarrow \widehat{H}^{-1}(G_w, U_w) \xrightarrow{\gamma_w} \widehat{H}^{-1}(G_w, {k_w}^\times) \longrightarrow 0$$

となる. したがって, γ_w は全射となるので, $\mathrm{Coker}\gamma_w = 0$ が成り立つ. つまり, $\mathrm{Coker}\gamma = 0$ となり, (3.37) を使って, $\mathrm{Im}\nu = \mathrm{Coker}\gamma = 0$ となる. よって, $|\mathrm{Im}\mu\nu| = |\mathrm{Im}\sigma\theta| = 1$ が成り立つ. □

したがって, (3.55) は次にように書くことができる.

$$|\mathrm{Im}\delta| = \frac{|\mathrm{Im}\sigma|}{|\mathrm{Im}\sigma\theta|} \tag{3.59}$$

$$|\mathrm{Im}\delta| = |\mathrm{Im}\sigma| \tag{3.60}$$

今, 系 3.48 より, $k/\mathbb{Q}$ がアーベル p 拡大のとき,

$$\mathrm{Im}\sigma \simeq \mathrm{Gal}(k_Z/k_G)$$

であるが, (3.60) より, $\mathrm{Im}\sigma$ を考えることは, $\mathrm{Im}\delta$ を考えることと同じである. また, $\mathrm{Im}\delta$ を考えることは, $\mathrm{Coker}\theta$ を考えることと同じである. したがって, $\mathrm{Coker}\theta$ がどうなるかを考えることにする.

(3.37) より,

$$\widehat{H}^{-1}(G, J_k) \xrightarrow{\theta} \widehat{H}^{-1}(G, C_k)$$

であるが, ここで, $\widehat{H}^2(G, C_k)$ と $\widehat{H}^{-3}(G, \mathbb{Z})$ との積を考えると, $\widehat{H}^{-3}(G, \mathbb{Z})$ から, $\widehat{H}^{-1}(G, C_k)$ に同型ができる. したがって,

$$\begin{array}{ccc} \bigoplus_v \widehat{H}^{-3}(G_w, \mathbb{Z}) & \xrightarrow{\varphi} & \widehat{H}^{-3}(G, \mathbb{Z}) \\ \downarrow & & \downarrow \\ \bigoplus_v \widehat{H}^{-1}(G_w, {k_w}^{\times}) & \xrightarrow{\theta} & \widehat{H}^{-1}(G, C_k) \end{array}$$

のような可換図式を得る. つまり, $\mathrm{Coker}\theta$ を考えることは, $\mathrm{Coker}\varphi$ を考えることと同じである. そこで, Tate Cohomology の定義から,

$$\bigoplus_v \widehat{H}^{-3}(G_w, \mathbb{Z}) = \bigoplus_v H^2(G_w, \mathbb{Z})$$

$$\widehat{H}^{-3}(G, \mathbb{Z}) = H^2(G, \mathbb{Z})$$

となる. このとき, 次の命題が成り立つ.

命題 3.61 *G が有限アーベル群のとき, $\wedge^2(G)$ から $H^2(G, \mathbb{Z})$ に自然な同型が存在する.*

証明　$H_2(G, \mathbb{Z}) \times H^2(G, \mathbb{Q}/\mathbb{Z}) \to \mathbb{Q}/\mathbb{Z}$ という対応は非退化であり, したがって, $H^2(G, \mathbb{Q}/\mathbb{Z})$ から $\mathrm{Hom}(\wedge^2(G), \mathbb{Q}/\mathbb{Z})$ への写像が同型になることが示せれば, $\wedge^2(G)$ から $H_2(G, \mathbb{Z})$ に自然な同型が存在することが言える.

$f(\sigma,\tau)$ を $\mathbb{Q}/\mathbb{Z}$ に値を取るような G 上の 2-cocycle とする．このとき, G は $\mathbb{Q}/\mathbb{Z}$ に自明に作用するので, f は

$$f(\sigma\tau,\mu)+f(\sigma,\tau)=f(\sigma,\tau\mu)+f(\tau,\mu)$$

を満たすので,

$$f(\sigma\tau,\mu)-f(\sigma,\mu)-f(\tau,\mu)=f(\sigma,\tau\mu)-f(\sigma,\tau)-f(\sigma,\mu)$$

と書くことができる.

G はアーベル群であるから, 左辺は σ,τ で対称, 右辺は τ,μ で対称になる．したがって, この式全体は σ,τ,μ の置換では不変になる. つまり,

$$f(\sigma\mu,\tau)-f(\sigma,\tau)-f(\mu,\tau)=f(\tau,\sigma\mu)-f(\tau,\sigma)-f(\tau,\mu)$$

を得る.

$\mathbb{Q}/\mathbb{Z}$ に値を取るような G 上の任意の 2-cocycle f を, 任意の $\sigma,\tau\in G$ に対して,

$$f^*(\sigma,\tau)=f(\sigma,\tau)-f(\tau,\sigma)$$

と定義することにする.

このとき, f^* は $G\times G$ から $\mathbb{Q}/\mathbb{Z}$ への双対写像になる． $\psi_0 : Z^2(G,\mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(\wedge^2(G),\mathbb{Q}/\mathbb{Z})$ なる準同型を, $\psi_0(f)=f^*$ として定義する.

ψ_0 の kernel はすべての対称な 2-cocycle であるため, すべての 2-coboundary を含む. したがって, ψ_0 は

$$\psi : H^2(G,\mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(\wedge^2(G),\mathbb{Q}/\mathbb{Z})$$

なる準同型を誘導する.

$\mathrm{Ker}\psi$ は対称な cocycle の類から成っていることから, $\mathrm{Ker}\psi=\mathrm{Ext}(G,\mathbb{Q}/\mathbb{Z})=0$ より, ψ は単射となる.

G は有限アーベル群であるから, 位数が素数巾の巡回群の直和で書くことができる.

$$G\simeq C_1\oplus\cdots\oplus C_t$$

と書くことにする.

定理 3.4 を用いて,

$$H^2(G,\mathbb{Q}/\mathbb{Z})\simeq\bigoplus_{i=1}^{t}H^2(C_i,\mathbb{Q}/\mathbb{Z})\oplus\bigoplus_{i<j}\mathrm{Hom}(C_i\otimes C_j,\mathbb{Q}/\mathbb{Z})$$

となる. C_i は巡回群なので, $H^2(C_i,\mathbb{Q}/\mathbb{Z})=0$ であるから,

$$\mathrm{rank}_p[H^2(G,\mathbb{Q}/\mathbb{Z})]=\frac{t(t-1)}{2}$$

が成り立つ. また,

$$\mathrm{rank}_p[\mathrm{Hom}(\wedge^2(G), \mathbb{Q}/\mathbb{Z})] = \frac{t(t-1)}{2}$$

となるので, $H^2(G, \mathbb{Q}/\mathbb{Z})$ と $\mathrm{Hom}(\wedge^2(G), \mathbb{Q}/\mathbb{Z})$ の位数は同じになることがわかる. つまり, ψ は同型となることがわかる. □

したがって, この命題 3.61 より,

$$H^2(G, \mathbb{Z}) \simeq \wedge^2(G)$$
$$\bigoplus_v H^2(G_w, \mathbb{Z}) \simeq \bigoplus_v \wedge^2(G_w)$$

が成り立つ. 系 3.48 を使って, $k/\mathbb{Q}$ がアーベル p 拡大のとき,

$$\mathrm{Coker}\varphi = \mathrm{Im}\sigma \simeq \mathrm{Gal}(k_Z/k_G)$$

が成り立つので,

$$\mathrm{Gal}(k_Z/k_G) \simeq \mathrm{Coker}(\bigoplus_v \wedge^2(G_w) \to \wedge^2(G)) \tag{3.62}$$

が成り立つ.

ここで, v 上の k の付値 w は, $G = \mathrm{Gal}(k/\mathbb{Q})$ の作用で移り合い, G はアーベル群なので, v の分解群はすべて等しくなる したがって, $G_w = G_v$ と書くことにする.

また, G は p 群になることから, $\mathrm{Gal}(k_Z/k_G)$ も p 群になる. 定理 3.35 の仮定から, $k = k_G$ を使うと,

$$\mathrm{Gal}(k_Z/k_G) = \mathrm{Gal}(k_Z/k)$$

となり, $\mathrm{Gal}(k_Z/k)$ は p 群になる. したがって, k_Z は, k 上不分岐アーベル p 拡大であり, $\mathbb{Q}$ 上 Galois 拡大であり, $\mathrm{Gal}(k_Z/k) \subseteq Z(\mathrm{Gal}(k_Z/\mathbb{Q}))$ を満たすような k の最大の p 拡大ということになる. これは, 定義 3.24 と一致する. したがって, $k/\mathbb{Q}$ がアーベル p 拡大のときは, $k_Z = k_C$ が成り立つ.

したがって, (3.62) は

$$\mathrm{Gal}(k_C/k) \simeq \mathrm{Coker}(\bigoplus_v \wedge^2(G_v) \to \wedge^2(G))$$

と書き換えることができる. よって, 定理 3.35 が証明できた. □

4　主定理 1.2.1 の証明

4.1　1st Step

まず, 第一段階として, 岩澤不変量がすべて 0 になるとしたとき, $k/\mathbb{Q}$ で分岐する素数が二つ以下, すなわち, $t \leq 2$ となることを示す.

$$\lambda_p(k) = \mu_p(k) = \nu_p(k) = 0$$

ならば, 十分大きな n に対して, $A(k_n) = 0$ が成り立つ.

$A(k_n) = 0$ は $p \nmid h(k_n)$ を意味するから, 補題 3.10 より, $k_{n,G} = k_n$ が成り立つ. したがって,

$$k_G \subseteq k_{n,G} = k_n \subseteq k_\infty$$

となり, $t = 1, 2$ のときにおける一つ目の条件 $k_G \subseteq k_\infty$ は満たされたことになる.

ここで, $\mathrm{Gal}(L/\mathbb{Q})$ が基本アーベル群になるような $k_n/\mathbb{Q}$ の最大の部分体を L とする. このとき, L は G^p で固定される体である.

今, $k_n = k_{n,G}$ より, 補題 3.10 を用いて, $k_n/\mathbb{Q}$ で分岐する素数 q の共通の惰性群を $T_{k_n/\mathbb{Q}}(q)$ とすると,

$$\mathrm{Gal}(k_n/\mathbb{Q}) = \prod T_{k_n/\mathbb{Q}}(q)$$

と書くことができる.

今, L がどんな体で書けているかを考えることにする.

$\mathrm{Gal}(L/\mathbb{Q})$ が基本アーベル群になることから, $G = \mathrm{Gal}(k_n/\mathbb{Q}) = \prod T_{k_n/\mathbb{Q}}(q)$ とおくと, L の固定群は

$$\mathrm{Gal}(k_n/L) = G^p = \prod T_{k_n/\mathbb{Q}}(q)^p$$

となる.

このとき, q_L を q 上にある L の素イデアルとすると,

$$T_{k_n/L}(q_L) = T_{k_n/\mathbb{Q}}(q) \cap G^p = T_{k_n/\mathbb{Q}}(q)^p$$

となることから,

$$G^p = \prod T_{k_n/\mathbb{Q}}(q)^p = \prod T_{k_n/L}(q_L)$$

である. 惰性群に対しては,

$$\prod T_{k_n/\mathbb{Q}}(q) = \prod \Big(T_{k_n/L}(q_L) \times T_{L/\mathbb{Q}}(q) \Big)$$

が成り立つ. よって,

$$\mathrm{Gal}(k_n/\mathbb{Q}) = \mathrm{Gal}(k_n/L) \times \mathrm{Gal}(L/\mathbb{Q})$$
$$\prod T_{k_n/\mathbb{Q}}(q) = \left(\prod T_{k_n/L}(q_L)\right) \times \mathrm{Gal}(L/\mathbb{Q})$$

が成り立つことから,

$$\mathrm{Gal}(L/\mathbb{Q}) = \prod T_{L/\mathbb{Q}}(q)$$

となる. つまり, $\mathrm{Gal}(L/\mathbb{Q})$ は $L/\mathbb{Q}$ で分岐する素数の惰性群の直積で書ける.

仮定から, $\mathrm{Gal}(L/\mathbb{Q})$ は基本アーベル群であるから,

$$L = k(p_1)\cdots k(p_t)\mathbb{Q}_1$$

である. ただし, $k(p_1),\cdots,k(p_t)$ は $\mathbb{Q}(\zeta_{p_1}),\cdots,\mathbb{Q}(\zeta_{p_t})$ の $\mathbb{Q}$ 上 p 次の部分体であり, $\mathbb{Q}_1$ は $\mathbb{Q}$ の円分 $\mathbb{Z}_p$ 拡大の一つ目の層である.

そこで, 補題 3.28 を用いると,

$$\mathrm{rank}_p[\mathrm{Gal}(k_{n,C}/k_n)] = \mathrm{rank}_p[\mathrm{Gal}(L_C/L)]$$

が成り立つことから, 補題 3.26 を使って,

$$\begin{aligned} A(k_n) = 0 &\Longleftrightarrow k_{n,C} = k_n \\ &\Longleftrightarrow L_C = L \\ &\Longleftrightarrow p \nmid h(L). \end{aligned}$$

したがって, 今後は L で $p \nmid h(L)$ かどうかを考えるだけで良いことがわかる.

さらに, 定理 3.35 より,

$$\mathrm{Gal}(L_C/L) \simeq \mathrm{Coker}(\bigoplus_{i=1}^{t+1} \wedge^2(G_{p_i}) \to \wedge^2(G))$$

が成り立ち, 右辺における $\wedge^2(G)$ の次元を $\mathbb{Z}/p\mathbb{Z}$ 上で考えると,

$$\dim_p[\wedge^2(G)] = \frac{t(t+1)}{2}$$

となる. $\wedge^2(G_i)$ の次元を計算するためには, G_{p_i} がどんな群であるかを調べれば良いことになるが, これは, L の整数環を D_L とし, p_i 上にある L の素イデアル P に対して, T_{p_i} を p_i の惰性群とすると,

$$\mathrm{Gal}((D_L/P)/(\mathbb{Z}/p_i)) = G_{p_i}/T_{p_i}$$

が成り立つ. $\mathrm{Gal}((D_L/P)/(\mathbb{Z}/p_i))$ は巡回群になることから, $T_{p_i} = \mathbb{Z}/p\mathbb{Z}$ で割って巡回群になるような G_{p_i} は $\mathrm{Gal}(L/\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^{t+1}$ から,

$$G_{p_i} = \mathbb{Z}/p\mathbb{Z} \text{ または } (\mathbb{Z}/p\mathbb{Z})^2$$

となる. このとき, 求める次元は,

$$\dim_p[\wedge^2(G_{p_i})] = 0 \text{ または } 1$$

となる. $L_C = L$ となる必要十分条件は $p \nmid h(L)$ が成り立つことなので,

$$0 = \dim_p[\mathrm{Gal}(L_C/L)] \geq \frac{t(t+1)}{2} - (t+1) = \frac{(t+1)(t-2)}{2}$$

となる. したがって, $t \leq 2$ である.

4.2 2nd Step

では, 第二段階として, $t = 0, 1, 2$ のそれぞれの場合について主定理 1.2.1 が成り立つがどうか証明する.

(a) $t = 0$ のとき, 次の命題を使って証明する.

命題 4.1 *k を数体, K を k 上の Galois 拡大とする. $h(k), h(K)$ をそれぞれ k, K の類数とする. このとき, K/k が p 巾次数の巡回拡大で, p 以外に K/k で分岐する素イデアルがなく, p は K/k で完全分岐するとき,*

$$p \mid h(K) \text{ ならば } p \mid h(k) \text{ が成り立つ.}$$

証明　k', K' を k, K の Hilbert 類体, $C(k), C(K)$ を k, K のイデアル類群とするとき, 類体論より,

$$\begin{aligned} \mathrm{Gal}(k'/k) &\simeq C(k)\ ,\ [k' : k] = h(k) \\ \mathrm{Gal}(K'/K) &\simeq C(K)\ ,\ [K' : K] = h(K) \end{aligned}$$

が成り立つ.

A を $[A : K]$ が p 巾で, $[K' : A]$ が p とは素になるような K'/K の中間体とする. このとき, A/k は Galois 拡大であり, $\mathrm{Gal}(A/k) = G$ は p 群となる.

そこで, $p \mid h(K)$ を仮定すると, $A \neq K$ であり,

$$N = \mathrm{Gal}(A/K) \neq \{e\}$$

となる. 今, G は p 群であるから, 巾零群である. すなわち, 中心列が存在するから,

$$M \subseteq N\ ,\ [N : M] = p$$

を満たす G の正規部分群 M が存在して, $N/M \subseteq Z(G/M)$ が成り立つ. ただし, $Z(G/M)$ とは G/M の中心のことである.

また, 仮定より, $G/N = (G/M)/(N/M)$ は巡回群で, $N/M \subseteq Z(G/M)$ である. $a^i(N/M), a^j(N/M) \in (G/M)/(N/M)$ に対して, $N/M \subseteq Z(G/M)$ なので,

$$\begin{aligned} a^i(N/M)a^j(N/M) &= a^i a^j(N/M) \\ &= a^{i+j}(N/M) \\ &= a^j a^i(N/M) \\ &= a^j(N/M)a^i(N/M) \end{aligned}$$

が成り立つので, G/M はアーベル群である. そこで, M に対応する A/K の中間体を E とおくことにする. このとき, E/k はアーベル拡大である.

p を E 上で分解したときに現れる E の素イデアルは, E/k がアーベル拡大であることから, 同じ惰性体を持つ. これを F とおくことにする.

今, p は K/k で完全分岐し, E/K では不分岐になる. したがって,

$$[F : k] = p$$

となる. また, F/k で分岐する素数は p 以外には存在しないが, p は F では不分岐である. よって, $F \subseteq k'$ が成り立つ.

したがって, $p \mid h(k)$ となることがわかる. □

この命題の証明は, [?] にも詳しいことが載っている.

この命題を用いて, $t = 0$ の場合を考えることにする. このとき, $L = \mathbb{Q}_1$ となる.

特に, $\mathbb{Q}$ の整数環 $\mathbb{Z}$ は単項イデアル整域であることから, $\mathbb{Q}$ の類数は 1 となる. 今, $\mathbb{Q}_1$ は $\mathbb{Q}$ 上 p 次の巡回拡大であり, $\mathbb{Q}_1/\mathbb{Q}$ 上で分岐する素数は p のみであり, しかも p は完全分岐する. したがって, 命題 4.1 の条件をすべて満たす. したがって, $p \nmid h(\mathbb{Q})$ なので, $p \nmid h(\mathbb{Q}_1)$ となり, 不変量はすべて 0 になる.

(b) $t = 1$ のとき, $L = k(p_1)\mathbb{Q}_1$ である.

岩澤不変量がすべて 0 になるということは, $p \nmid h(L)$ が成り立つことと同値である. このとき, 次の命題が成り立つ.

命題 4.2 p, p_1 のみが $L/\mathbb{Q}$ で分岐するとき, $p \mid h(L)$ であるための必要十分条件は

$$\left(\frac{p}{p_1}\right)_p = 1 \ , \ p_1 \equiv 1 \pmod{p^2}$$

が成り立つことである.

証明　今, $p \mid h(L)$ であるための必要十分条件は $L_C \neq L$ であることなので, $L_C \neq L$ であることと,

$$\left(\frac{p}{p_1}\right)_p = 1 \ , \ p_1 \equiv 1 \pmod{p^2}$$

であることの二つが同値であることを示す.

$G = \mathrm{Gal}(L/\mathbb{Q})$, G_p, G_{p_1} を p, p_1 の分解群とすると, 定理 3.35 より,

$$\mathrm{Gal}(L_C/L) \simeq \mathrm{Coker}(\wedge^2(G_p) \oplus \wedge^2(G_{p_1}) \to \wedge^2(G))$$

が成り立つ.

ここで, $\mathrm{Gal}(L/\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^2$ より,

$$\dim_p[\wedge^2(G)] = 1$$

となる. したがって, $L_C \neq L$ であるための必要十分条件は

$$G_p, G_{p_1} \neq (\mathbb{Z}/p\mathbb{Z})^2$$

となることである. 今, p, p_1 は $L/\mathbb{Q}$ で分岐することから, T_p, T_{p_1} を p, p_1 の惰性群とすると,

$$G_p = T_p = \mathbb{Z}/p\mathbb{Z}\ ,\ G_{p_1} = T_{p_1} = \mathbb{Z}/p\mathbb{Z}$$

でなくてはならない.

惰性群 T_p, T_{p_1} で固定されるそれぞれの惰性体は p, p_1 が分解されるような L の最大の部分体である. p, p_1 は $\mathbb{Q}_1, k(p_1)$ で完全分岐することから, $k(p_1), \mathbb{Q}_1$ で完全分解することになる.

そこで, p が $k(p_1)/\mathbb{Q}$ で完全分解するための必要十分条件は p が modulo p_1 の p 巾剰余であるということを示す. まずは, p が $k(p_1)/\mathbb{Q}$ で完全分解するならば, p は modulo p_1 の p 巾剰余であることを示す.

p が $k(p_1)/\mathbb{Q}$ で

$$(p) = {q_1}' \cdots {q_p}'\ ,\ N({q_i}') = p$$

のように分解したとする. $\mathbb{Q}(\zeta_{p_1})/\mathbb{Q}$ では,

$$(p) = q_1 \cdots q_g\ ,\ N(q_i) = p^f\ ,\ fg = p_1 - 1$$

と分解したとする. ここで, f は $p^f \equiv 1 \pmod{p_1}$ を満たす最小の正の整数である.

今, 分解の仕方から見て, $p \mid g$ が成り立ち, $fg = p_1 - 1$ なので,

$$f \,\Big|\, \frac{p_1 - 1}{p}$$

となる. さらに, f は $p^f \equiv 1 \pmod{p_1}$ を満たす最小の正の整数であるから,

$$p^{\frac{p_1-1}{p}} \equiv 1 \pmod{p_1}$$

が成り立つ. これは, p が modulo p_1 の p 巾剰余になることを意味している.

逆に, p が modulo p_1 の p 巾剰余であるとすると,

$$p^{\frac{p_1-1}{p}} \equiv 1 \pmod{p_1}$$

が成り立つが, 今, p が $\mathbb{Q}(\zeta_{p_1})/\mathbb{Q}$ で先程定義したように分解すると仮定すると, f の最小性から,

$$f \Big| \frac{p_1-1}{p}$$

が成り立つ. したがって, $p \mid g$ となる. $\mathrm{Gal}(\mathbb{Q}(\zeta_{p_1})/D_{p_1}) \subset \mathrm{Gal}(\mathbb{Q}(\zeta_{p_1})/k(p_1))$ となるので, p は $k(p_1)$ では完全分解する.

次に, p_1 が $\mathbb{Q}_1/\mathbb{Q}$ で完全分解するための必要十分条件は $p_1 \equiv 1 \pmod{p^2}$ であることを示す.

まずは, p_1 が $\mathbb{Q}_1/\mathbb{Q}$ で完全分解するならば, $p_1 \equiv 1 \pmod{p^2}$ が成り立つことを示す.

p_1 が $\mathbb{Q}_1/\mathbb{Q}$ で

$$(p_1) = {q_1}' \cdots {q_p}', N({q_i}') = p_1$$

のように分解したとする. $\mathbb{Q}(\zeta_{p^2})/\mathbb{Q}$ では,

$$(p_1) = q_1 \cdots q_g, N(q_i) = {p_1}^f, fg = p(p-1)$$

と分解したとする. ここで, f は ${p_1}^f \equiv 1 \pmod{p^2}$ を満たす最小の正の整数である.

今, 分解の仕方から見て, $p \mid g$ が成り立ち, $fg = p(p-1)$ なので,

$$f \mid (p-1)$$

となる. さらに, f は, ${p_1}^f \equiv 1 \pmod{p^2}$ を満たす最小の正の整数であるから,

$${p_1}^{p-1} \equiv 1 \pmod{p^2}$$

が成り立つ. ここで,

$$\begin{aligned} {p_1}^{p-1} - 1 &= (p_1 - 1)({p_1}^{p-2} + {p_1}^{p-3} + \cdots + 1) \\ &\equiv 0 \pmod{p^2} \end{aligned}$$

なので, ここで,

$${p_1}^{p-2} + {p_1}^{p-3} + \cdots + 1 \equiv 0 \pmod{p^2}$$

が成り立つと仮定する. 注意 1.7 より, $p_1 \equiv 1 \pmod{p}$ が成り立っているので,

$$\begin{aligned} {p_1}^{p-2} + {p_1}^{p-3} + \cdots + 1 &\equiv 0 \pmod{p} \\ 1 + 1 + \cdots + 1 &\equiv 0 \pmod{p} \\ p - 1 &\equiv 0 \pmod{p} \end{aligned}$$

となるが, $p-1 \not\equiv 0 \pmod{p}$ なので, これは矛盾.

したがって, $p_1 \equiv 1 \pmod{p^2}$ が成り立つ.

逆に, $p_1 \equiv 1 \pmod{p^2}$ が成り立つとする. p_1 が $\mathbb{Q}(\zeta_{p^2})/\mathbb{Q}$ で,

$$(p_1) = q_1 \cdots q_g, N(q_i) = {p_1}^f, fg = p(p-1)$$

のように分解しているとする. ただし, f は ${p_1}^f \equiv 1 \pmod{p^2}$ を満たす最小の正の整数である.

今, $p_1 \equiv 1 \pmod{p^2}$ が成り立ち, f の最小性を考えると, $f = 1, g = p(p-1)$ となる. したがって, p_1 は $\mathbb{Q}(\zeta_{p^2})/\mathbb{Q}$ で完全分解していることになる. つまり, p_1 は $\mathbb{Q}_1/\mathbb{Q}$ でも完全分解することは明らかである.

したがって, この命題は成り立つ. □

つまり, この命題を使うことによって, $t = 1$ のときに定理が成り立つことがわかる.

(c) $t = 2$ のとき, $L = k(p_1)k(p_2)\mathbb{Q}_1$ ででである.

まずは, $t = 2$ のときの証明をする際に必要な定義を一つ述べる.

定義 4.3 (Artin 記号) $k/\mathbb{Q}$ で不分岐な素数 p に対して, $(p) = \mathcal{P}_1 \cdots \mathcal{P}_g$ のような形で k 上素イデアル分解されているとする. このとき, $\mathcal{P}_1, \cdots, \mathcal{P}_g$ の一つを $\mathcal{P}$ と書くことにする. このとき, $\mathcal{P}$ の Frobenius 写像 $\sigma_{\mathcal{P}}$ が一意に決まり, これを,

$$\sigma_{\mathcal{P}} = \left(\frac{k/\mathbb{Q}}{\mathcal{P}}\right)$$

と書くことにする. 特に, $k/\mathbb{Q}$ がアーベル拡大のときには, $\sigma_{\mathcal{P}} = \sigma_p$ とし,

$$\left(\frac{k/\mathbb{Q}}{\mathcal{P}}\right) = \left(\frac{k/\mathbb{Q}}{p}\right)$$

と書く. この $\left(\frac{k/\mathbb{Q}}{p}\right)$ という記号のことを Artin 記号と呼ぶ.

また, $k/\mathbb{Q}$ がアーベル拡大のとき, a が $a = {p_1}^{b_1} \cdots {p_n}^{b_n}$ と素因数分解されるとき, Artin 記号を

$$\left(\frac{k/\mathbb{Q}}{a}\right) = \prod_{i=1}^{n} \left(\frac{k/\mathbb{Q}}{p_i}\right)^{b_i}$$

と定義する.

注 4.4 $\left(\frac{k/\mathbb{Q}}{p}\right) = 1$ であるための必要十分条件は p が $k/\mathbb{Q}$ で完全分解することである.

では $t = 2$ のときの証明を始める.

G_p, G_{p_i} を p, p_i の分解群, D_p, D_{p_i} をそれぞれ分解体とする. このとき,

$$D_p \subseteq k(p_1)k(p_2)\ ,\ D_{p_1} \subseteq k(p_2)\mathbb{Q}_1\ ,\ D_{p_2} \subseteq k(p_1)\mathbb{Q}_1$$

が成り立つ.

岩澤不変量がすべて 0 になるというのは $p \nmid h(L)$ と同値になる. 次の命題 4.6 は重要だが, その命題の証明に必要な補題を示す.

補題 4.5 F をベクトル空間, V を F 上の次元が 3 となるようなベクトル空間とする. V_i を V の真部分空間とするとき, 自然な写像 $\oplus_{i=1}^{3}\wedge^2(V_i) \to \wedge^2(V)$ が全射になる必要十分条件は, 次の二つが成り立つことである.

(a) $\dim(V_i) = 2$ であり, $i \neq j$ に対して, $V_i \neq V_j$.

(b) $i \neq j$ に対して, $V_i \cap V_j = \langle x_{ij} \rangle$ ならば, x_{12}, x_{13}, x_{23} は V の基底になる.

証明

$$\phi : \wedge^2(V_i) \times V \ni (x \wedge y, z) \mapsto x \wedge y \wedge z \in \wedge^3(V) \simeq F$$

という pairing は非退化である.

まずは, $\oplus_{i=1}^{3}\wedge^2(V_i) \to \wedge^2(V)$ が全射であると仮定する. このとき, (a) は明らかである.

$$V_1 = \langle x_{12}, u \rangle, V_2 = \langle x_{12}, v \rangle, V_3 = \langle x_{13}, w \rangle$$

とおく. 仮定より,

$$x_{12} \wedge u, x_{12} \wedge v, x_{13} \wedge w$$

は, $\wedge^2(V)$ の基底になる. ϕ の非退化性より, $x_{12} \wedge x_{13} \wedge w \neq 0$ が成り立つ. したがって, x_{12}, x_{13} は線形独立であり, $V_1 = \langle x_{12}, x_{13} \rangle$ となる. 同様にして, $V_2 = \langle x_{12}, x_{23} \rangle, V_3 = \langle x_{13}, x_{23} \rangle$ となる. $w = x_{23}$ とすると, $x_{12} \wedge x_{13} \wedge x_{23} \neq 0$ が成り立つ. したがって, (b) が成り立つ.

逆に, (a), (b) が成り立つと仮定すると,

$$V_1 = \langle x_{12}, x_{13} \rangle, V_2 = \langle x_{12}, x_{23} \rangle, V_3 = \langle x_{13}, x_{23} \rangle$$

となるから, $\oplus_{i=1}^{3}\wedge^2(V_i)$ の像は $x_{12} \wedge x_{13}, x_{12} \wedge x_{23}, x_{13} \wedge x_{23}$ で生成され, (b) から, この三つは $\wedge^2(V)$ の基底をなす. したがって, 全射が成り立つ. □

この補題を使うことによって, 次の命題が成り立つ.

命題 4.6 p, p_1, p_2 のみが $L/\mathbb{Q}$ で分岐し, D_p, D_{p_1}, D_{p_2} をそれぞれの素数の分解体とするとき, $p \nmid h(L)$ であるための必要十分条件は

$$[D_p : \mathbb{Q}] = [D_{p_1} : \mathbb{Q}] = [D_{p_2} : \mathbb{Q}] = p \ , \ L = D_p D_{p_1} D_{p_2}$$

である.

証明　　L の中心 p 類体 L_C に対して, $p \nmid h(L)$ であることと $L_C = L$ が成り立つことは同値なので, $L_C = L$ が成り立つことと,

$$[D_p : \mathbb{Q}] = [D_{p_1} : \mathbb{Q}] = [D_{p_2} : \mathbb{Q}] = p \ , \ L = D_p D_{p_1} D_{p_2}$$

が成り立つことが同値であることを示す.

ここで, $G = \mathrm{Gal}(L/\mathbb{Q})$ に対して,

$$\mathrm{Gal}(L_C/L) \simeq \mathrm{Coker}(\oplus_{i=1}^{3} \wedge^2(G_{p_i}) \to \wedge^2(G))$$

が成り立つ. $L_C = L$ を仮定すると, $\oplus_{i=1}^{3} \wedge^2(G_{p_i}) \to \wedge^2(G))$ が全射になることから, 補題 4.5 を使って,

(a) $\dim(G_{p_i}) = 2$ であり, $i \neq j$ に対して, $G_{p_i} \neq G_{p_j}$.

(b) $G_{p_1} \cap G_{p_2}, G_{p_1} \cap G_{p_3}, G_{p_2} \cap G_{p_3}$ は G を生成する.

となることがわかる. これを体で考え直すと,

(a') $[D_{p_i} : \mathbb{Q}] = p$ であり, $i \neq j$ に対して, $D_{p_i} \neq D_{p_j}$.

(b') $D_{p_1} D_{p_2} \cap D_{p_1} D_{p_3} \cap D_{p_2} D_{p_3} = \mathbb{Q}$

となる.

この二つが成り立つと仮定すると, $D_{p_1} = D_{p_1} D_{p_2} \cap D_{p_1} D_{p_3}$ となり, $D_{p_1} \cap D_{p_2} D_{p_3} = \mathbb{Q}$ より, $D_{p_1} D_{p_2} D_{p_3} = L$ となる.

逆も明らかである. □

では, 証明の続きを考えることにする. この命題 4.6 において,

$$[D_p : \mathbb{Q}] = [D_{p_1} : \mathbb{Q}] = [D_{p_2} : \mathbb{Q}] = p, L = D_p D_{p_1} D_{p_2}$$

が成り立つと仮定して,

$$\left(\frac{p}{p_1}\right)_p = 1 \text{ または } \left(\frac{p_1}{p_2}\right)_p = 1 \text{ または } p_2 \equiv 1 \pmod{p^2} \tag{4.7}$$

と,

$$\left(\frac{p}{p_2}\right)_p = 1 \text{ または } \left(\frac{p_2}{p_1}\right)_p = 1 \text{ または } p_1 \equiv 1 \pmod{p^2} \tag{4.8}$$

の (4.7), (4.8) が同時に成り立つと仮定する. 命題 4.2 の証明でも出てくるように, $\left(\frac{p}{p_i}\right)_p = 1$ であるための必要十分条件は p が $k(p_1)$ で完全分解することなので, この仮定は $(i,j) = (1,2)$ または $(2,1)$ のとき,

$$D_p = k(p_i) \text{ または } D_{p_i} = k(p_j) \text{ または } D_{p_j} = \mathbb{Q}_1$$

が成り立つことと同値になる.

そこで, 最初の場合を考えて, $D_p = k(p_1)$ とする. このとき, $D_p = k(p_1)$ と $L = D_p D_{p_1} D_{p_2} = k(p_1)k(p_2)\mathbb{Q}_1$ を使って, D_{p_1} も D_{p_2} も $k(p_1)$ にはならないことがわかる.

$(i,j) = (1,2)$ の場合を考えて,

$$D_p = k(p_2) \text{ または } D_{p_2} = k(p_1) \text{ または } D_{p_1} = \mathbb{Q}_1$$

のうちどれがが成り立つので, $D_p = k(p_1)$ と $D_{p_2} \neq k(p_1)$ を使って, $D_{p_1} = \mathbb{Q}_1$ が成り立つことになる. したがって, $D_p = k(p_1), D_{p_1} = \mathbb{Q}_1$ となる.

ところが,

$$D_{p_2} \subseteq k(p_1)\mathbb{Q}_1 = D_p D_{p_1}$$

となり, これは $L = D_p D_{p_1} D_{p_2}$ に矛盾する.

同様にしてその他の場合も矛盾する.

したがって, $(i,j) = (1,2)$ または $(2,1)$ のとき,

$$\left(\frac{p}{p_i}\right)_p \neq 1\ ,\ \left(\frac{p_i}{p_j}\right)_p \neq 1\ ,\ p_j \not\equiv 1 \pmod{p^2}$$

が成り立つ.

次に (1.6) について考える. 今は $(i,j) = (1,2)$ としても一般性を失わない.

そこで,

$$\left(\frac{p}{p_1}\right)_p \neq 1\ ,\ \left(\frac{p_1}{p_2}\right)_p \neq 1\ ,\ p_2 \not\equiv 1 \pmod{p^2}$$

とおく.

まず, $\left(\frac{p}{p_1}\right)_p \neq 1$ より, p は $k(p_1)$ では分岐せず, 分解しない. したがって,

$$\sigma = \left(\frac{k(p_1)/\mathbb{Q}}{p}\right)$$

とするとき, $\sigma \neq 1$ である. ただし, $\left(\frac{k(p_1)/\mathbb{Q}}{p}\right)$ は Artin 記号である.

このとき, σ は位数が p となる $\mathrm{Gal}(k(p_1)/\mathbb{Q})$ を生成する.

同様にして,

$$\tau = \left(\frac{k(p_2)/\mathbb{Q}}{p_1}\right), \eta = \left(\frac{\mathbb{Q}_1/\mathbb{Q}}{p_2}\right)$$

とおくと,

$$\langle\tau\rangle = \mathrm{Gal}(k(p_2)/\mathbb{Q}), \langle\eta\rangle = \mathrm{Gal}(\mathbb{Q}_1/\mathbb{Q})$$

となる.

ここで, $\left(\frac{p}{p_1}\right)_p \neq 1$ より, $\left(\frac{p_2p^x}{p_1}\right)_p = 1$ なる $x \in \mathbb{F}_p$ が存在する. したがって,

$$\left(\frac{p_2p^x}{p_1}\right)_p = 1 \Longleftrightarrow \left(\frac{k(p_1)/\mathbb{Q}}{p_2p^x}\right) = \left(\frac{k(p_1)/\mathbb{Q}}{p_2}\right)\left(\frac{k(p_1)/\mathbb{Q}}{p^x}\right) = 1$$

となり,

$$\left(\frac{k(p_1)/\mathbb{Q}}{p_2}\right) = \sigma^{-x}$$

が成り立つ.

その他も同様にして,

$$\left(\frac{k(p_2)/\mathbb{Q}}{p}\right) = \tau^{-y}\ ,\ \left(\frac{\mathbb{Q}_1/\mathbb{Q}}{p_1}\right) = \eta^{-z}$$

とできる.

そこで,

$$\left(\frac{k(p_1)k(p_2)/\mathbb{Q}}{p}\right) = \left(\frac{k(p_1)/\mathbb{Q}}{p}\right)\left(\frac{k(p_2)/\mathbb{Q}}{p}\right) = \sigma\tau^{-y}$$

となる. D_p は $k(p_1)k(p_2)$ で $\langle\sigma\tau^{-y}\rangle$ の固定体になる. したがって, $\mathrm{Gal}(L/\mathbb{Q})$ では, G_p は

$$\mathrm{Gal}(k(p_1)k(p_2)\mathbb{Q}_1/k(p_1)k(p_2)) \simeq \mathrm{Gal}(\mathbb{Q}_1/\mathbb{Q})$$

を部分群に持つので,

$$G_p = \langle\sigma\tau^{-y}, \eta\rangle$$

が成り立つ. その他同様に,

$$G_{p_1} = \langle\sigma, \tau\eta^{-z}\rangle\ ,\ G_{p_2} = \langle\tau, \eta\sigma^{-x}\rangle$$

となる.

ここで,

$$\begin{aligned} G_p \cap G_{p_1} &= \langle\eta, \sigma\tau^{-y}\rangle \cap \langle\sigma, \tau\eta^{-z}\rangle \\ &= \langle\eta, \sigma\tau^{-y}\rangle \cap \langle\sigma, \tau^{-y}\eta^{-yz}\rangle \\ &= \langle\eta^{-yz}, \sigma\tau^{-y}\rangle \cap \langle\sigma, \tau^{-y}\eta^{-yz}\rangle \\ &= \langle\sigma\tau^{-y}\eta^{-yz}\rangle \end{aligned}$$

となるので,

$$\begin{aligned} G_p \cap G_{p_1} \cap G_{p_2} &= \langle \sigma\tau^{-y}\eta^{-yz} \rangle \cap \langle \tau, \eta\sigma^{-x} \rangle \\ &= \langle \sigma\tau^{-y}\eta^{-yz} \rangle \cap \langle \tau^{-y}, \eta^{-yz}\sigma^{-xyz} \rangle \end{aligned}$$

となる. もし, $xyz \neq -1 \in \mathbb{F}_p$ ならば, $\sigma^{-xyz} \neq \sigma$ なので,

$$G_p \cap G_{p_1} \cap G_{p_2} = \{1\}$$

となり, もし, $xyz = -1 \in \mathbb{F}_p$ ならば, $\sigma^{-xyz} = \sigma$ なので,

$$\begin{aligned} G_p \cap G_{p_1} \cap G_{p_2} &= \langle \sigma\tau^{-y}\eta^{-yz} \rangle \cap \langle \tau^{-y}, \eta^{-yz}\sigma^{-xyz} \rangle \\ &= \langle \sigma\tau^{-y}\eta^{-yz} \rangle \end{aligned}$$

となる.

今は, $D_p D_{p_1} D_{p_2} = L$ という仮定から, $G_p \cap G_{p_1} \cap G_{p_2} = \{1\}$ とならなくてはならない. したがって, $xyz \neq -1 \in \mathbb{F}_p$ が成り立つ.

逆に, $t = 2$ のときの条件をすべて満たすとすると, $(i, j) = (1, 2)$ のとき,

$$\mathrm{Gal}(k(p_1)k(p_2)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^2$$

となることから, p は $k(p_1)k(p_2)/\mathbb{Q}$ で分解することがわかる. しかし,

$$\left(\frac{p}{p_1}\right)_p \neq 1$$

より, p は $k(p_1)/\mathbb{Q}$ では分解しない. したがって, $[D_p : \mathbb{Q}] = p$.

同様にして, $[D_{p_1} : \mathbb{Q}] = [D_{p_2} : \mathbb{Q}] = p$ となる. また, $L = D_p D_{p_1} D_{p_2}$ となることから, $xyz \neq -1 \in \mathbb{F}_p$ が成り立つ. □

4.3 主定理 1.2.1 の例

ここでは, 主定理を満たすような例を与えることにする.

例 4.9 $t=0$ の場合, $k \subseteq \mathbb{Q}(\zeta_{p^a})$ として考える.

不変量がすべて 0 になるようにするには, 十分大きな n に対して $p \nmid h(k_n)$ であれば良い. 今, $k \subseteq \mathbb{Q}(\zeta_{p^a})$ より, $k \subseteq \mathbb{Q}_a$ であるから,

$$k_n = k \cdot \mathbb{Q}_n \subseteq \mathbb{Q}_a \cdot \mathbb{Q}_n = \mathbb{Q}_n$$

が成り立ち, $k_n = \mathbb{Q}_n$ となる.

$\mathbb{Q}_n$ は $\mathbb{Q}$ 上 p 巾次の巡回拡大で, p 以外に分岐する素数は存在しない. また, p は完全分岐する. そこで, 命題 4.1 を使って, $p \nmid h(\mathbb{Q})$ なので, $p \nmid h(k_n)$ が言える.

したがって, 主定理 1.2.1 より, 不変量はすべて 0 となる. □

例 4.10 $t=1$ の場合, $p=3, p_1=19$ を考える.

k を $\mathbb{Q}(\zeta_{3^2 \cdot 19})$ の $\mathbb{Q}$ 上 27 次の部分体とする. このとき, k は $\mathbb{Q}(\zeta_{3^2 \cdot 19})$ の 最大の $\mathbb{Q}$ 上 3 巾次の部分体なので, 補題 3.22 を使って, $k_G = k \subseteq k_\infty$ となることがわかる.

また,

$$\left(\frac{3}{19}\right)_3 \neq 1$$

が成り立つことから, 主定理 1.2.1 より, 不変量はすべて 0 になる. □

例 4.11 $t=2$ の場合, $p=3, p_1=7, p_2=19$ を考える.

まず, $k(7)$ を $\mathbb{Q}(\zeta_7)$ の $\mathbb{Q}$ 上 3 次の部分体, $k(19)$ を $\mathbb{Q}(\zeta_{19})$ の $\mathbb{Q}$ 上 3 次の部分体, $\mathbb{Q}_1$ を $\mathbb{Q}(\zeta_9)$ の $\mathbb{Q}$ 上 3 次の部分体とする. このとき, $k = k(7)k(19)$ とし, $k_1 = k \cdot \mathbb{Q}_1$ として, 円分 $\mathbb{Z}_3$ 拡大を作ることにする.

まず, $k_G \subseteq k_\infty$ が成り立つことを示す. 補題 3.10 より, k_G は k 上 3 拡大となる. そこで, $3 \nmid h(k)$ ならば $k_G = k$ となり, $k_G \subseteq k_\infty$ が言える.

まず, $k(7)$ において $3, 19$ が分解しないことを示す. $k(7) \subseteq \mathbb{Q}(\zeta_7)$ より, 19 が $\mathbb{Q}(\zeta_7)$ で,

$$(19) = P_1 \cdots P_g$$

のように分解したとする. このとき, $N(P_i) = 19^f \equiv 1 \pmod 7$ なる最小の整数 f が存在し, $fg = 6$ となる. ただし, 19 は $\mathbb{Q}(\zeta_7)$ では分岐しない.

このような f は,

$$\begin{aligned} 19 &\equiv 5 \not\equiv 1 \pmod 7 \\ 19^2 &\equiv 4 \not\equiv 1 \pmod 7 \\ 19^3 &\equiv 6 \not\equiv 1 \pmod 7 \\ 19^4 &\equiv 2 \not\equiv 1 \pmod 7 \\ 19^5 &\equiv 3 \not\equiv 1 \pmod 7 \\ 19^6 &\equiv 1 \pmod 7 \end{aligned}$$

なので, $f = 6$ である. したがって, $g = 1$ となる. つまり, 19 は, $\mathbb{Q}(\zeta_7)$ では分解しない.

同様にして, 3 も $\mathbb{Q}(\zeta_7)$ では分解しないことがいえる.

3 が $\mathbb{Q}(\zeta_7)$ で

$$(3) = R_1 \cdots R_g$$

のように分解したとする。このとき, $N(R_i) = 3^f \equiv 1 \pmod{()7}$ を満たす最小の正の整数 f が存在し, $fg = 6$ となる. ただし, 3 は $\mathbb{Q}(\zeta_7)$ では分岐しない.

このような f は,

$$\begin{aligned} 3 &\not\equiv 1 \pmod 7 \\ 3^2 &\equiv 2 \not\equiv 1 \pmod 7 \\ 3^3 &\equiv 6 \not\equiv 1 \pmod 7 \\ 3^4 &\equiv 4 \not\equiv 1 \pmod 7 \\ 3^5 &\equiv 5 \not\equiv 1 \pmod 7 \\ 3^6 &\equiv 1 \pmod 7 \end{aligned}$$

なので, $f = 6$ である. したがって, $g = 1$ となる. つまり, 3 は $\mathbb{Q}(\zeta_7)$ では分解しない.

つまり, 今までの結果から, 3, 19 は共に $k(7)$ では分解しないことがわかる.

そこで, 命題 4.1 より, $3 \nmid h(\mathbb{Q})$ なので, $3 \nmid h(k)$ となり, $k_G \subseteq k_\infty$.

$(i, j) = (2, 1)$ のとき,

$$\left(\frac{3}{19}\right)_3 \neq 1,\ \left(\frac{19}{7}\right)_3 \neq 1,\ 7 \not\equiv 1 \pmod 9$$

が成り立つ.

$x = 0, y = 1, z = 0$ のとき,

$$\begin{aligned} \left(\frac{7 \cdot 3^x}{19}\right)_3 = \left(\frac{7}{19}\right)_3 = \left(\frac{4^3}{19}\right)_3 = 1 \\ \left(\frac{3 \cdot 19^y}{7}\right)_3 = \left(\frac{3 \cdot 19}{7}\right)_3 = \left(\frac{1}{7}\right)_3 = 1 \\ 19 \cdot 7^z \equiv 19 \equiv 1 \pmod 9 \end{aligned}$$

なので, 主定理 1.2.1 を使って, 不変量は 0 になることがわかる. □

参考文献