

# 分岐を制限した代数体の埋め込み問題 とその応用について

野村 明人（金沢大学 理工研究域）

September 9, 2008

# 予定

- §1 代数体の埋めこみ問題（用語の説明）
- §2 基本的な定理（一般論）
- §3  $\mathbb{Q}$  上の  $p$  拡大（Scholz-Reichardt の復習）
- §4 分岐する素点の最少個数
- §5 不分岐  $p$  拡大の存在について

## 参考文献

- §1, §2 J. Neukirch,  
Über das Einbettungsproblem der algebraischen Zahlen-  
theorie, Invent. Math. **21** (1973)
- §3 J-P. Serre, Topics in Galois Theory (1993)

# §1 代数体の埋めこみ問題（用語の説明）

$k$  : 代数体,  $K/k$  : 有限次ガロア拡大

## 埋め込み問題 ( $K/k, \varepsilon$ )

$$\begin{array}{c} G(\bar{k}/k) \\ \downarrow \varphi \text{ can.} \\ (\varepsilon) : 1 \longrightarrow A \longrightarrow E \xrightarrow{j} G(K/k) \longrightarrow 1 \\ (A : \text{アーベル}) \end{array}$$

**定義**  $\psi : G(\bar{k}/k) \longrightarrow E$  hom.

(1)  $\psi$  : solution  $\stackrel{\text{def}}{\iff} j \circ \psi = \varphi$

(2)  $\psi$  : proper solution  $\stackrel{\text{def}}{\iff} \psi$  : solution, onto

# §1 代数体の埋めこみ問題（用語の説明）

**注意**  $(\varepsilon) : 1 \longrightarrow A \longrightarrow E \xrightarrow{j} G(K/k) \longrightarrow 1$

(1)  $(\varepsilon) : \text{split} \Rightarrow \text{solvable}$  (i.e. solution を持つ)

(2)  $\exists$  proper solution

$\iff \exists L/K/k : \text{ガロア拡大 s.t.}$

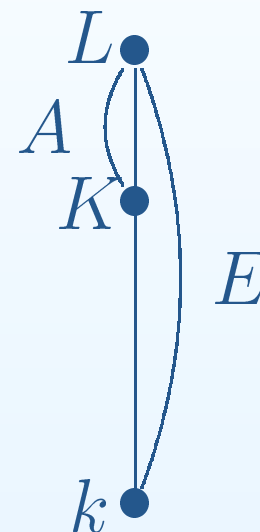
$$1 \rightarrow G(L/K) \rightarrow G(L/k) \rightarrow G(K/k) \rightarrow 1$$

は  $(\varepsilon)$  と一致

(3)  $\psi : \text{solution}$ ,  $S : k$  の素点の有限集合

・  $\text{Ker } \psi$  に対応する体も solution とよぶ

・ 対応する体が  $k$  上  $S$  の外で不分岐な時,  $\psi$  は  $S$  の外で不分岐であるという



## §2 基本的な定理

$p$  : 奇素数,  $K/k$  :  $p$  拡大

$(\varepsilon) : 1 \rightarrow \mathbf{Z}/p\mathbf{Z} \rightarrow E \rightarrow G(K/k) \rightarrow 1$  中心拡大

**定理 A** (local-global principle)

$(K_{\mathfrak{q}}/k_{\mathfrak{q}}, \varepsilon_{\mathfrak{q}}) : \text{solvable for all } \mathfrak{q} \Rightarrow (K/k, \varepsilon) : \text{solvable}$

**定理 B**  $K/k$  : 不分岐  $\Rightarrow (K/k, \varepsilon) : \text{solvable}$

## §2 基本的な定理

$p$  : 奇素数,  $K/k$  :  $p$  拡大

$(\varepsilon) : 1 \rightarrow \mathbf{Z}/p\mathbf{Z} \rightarrow E \rightarrow G(K/k) \rightarrow 1$  中心拡大

**定理 A** (local-global principle)

$(K_{\mathfrak{q}}/k_{\mathfrak{q}}, \varepsilon_{\mathfrak{q}}) : \text{solvable for all } \mathfrak{q} \Rightarrow (K/k, \varepsilon) : \text{solvable}$

**定理 B**  $K/k$  : 不分岐  $\Rightarrow (K/k, \varepsilon) : \text{solvable}$

**記号**  $S$  :  $k$  の素点の有限集合

$B_k(S) = \{\alpha \in k^\times \mid (\alpha) = \mathfrak{a}^p \ (\exists \mathfrak{a}), \alpha \in k_{\mathfrak{q}}^p \ (\forall \mathfrak{q} \in S)\}$

**定理 C**  $S \supset \text{Ram}(K/k)$ ,  $B_k(S) = k^{\times p}$

$(K/k, \varepsilon) : \text{solvable}$

$\Rightarrow S$  の外で不分岐な solution がある

注 :  $k = \mathbf{Q}$  のとき  $B_k(S) = k^{\times p}$  for  $\forall S$

### §3 $\mathbb{Q}$ 上の $p$ 拡大 (Scholz-Reichardt)

**定理 D** (Scholz-Reichardt)  $p$  : 奇素数

$$\forall G : p\text{-群}, \exists M/\mathbb{Q} \text{ s.t. } G(M/\mathbb{Q}) \cong G$$

#### アイデア

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_m = \{1\}$$

$$G \triangleright G_i, G_i/G_{i+1} \cong \mathbf{Z}/p\mathbf{Z}$$

#### 次を示す

$\exists K_i/\mathbb{Q}$  s.t.

- $G(K_i/\mathbb{Q}) \cong G/G_i$
- $(\varepsilon) : 1 \rightarrow \mathbf{Z}/p\mathbf{Z} \rightarrow G/G_{i+1} \rightarrow G(K_i/\mathbb{Q}) \rightarrow 1$   
に対する埋め込み問題が solvable

### §3 $\mathbb{Q}$ 上の $p$ 拡大 (Scholz-Reichardt)

**定義**  $p$  拡大  $K/\mathbb{Q}$  が  $N$ -Scholz であるとは

$\stackrel{\text{def}}{\iff}$  すべての  $q \in \text{Ram}(K/\mathbb{Q})$  に対して

(1)  $q \equiv 1 \pmod{p^N}$ , (2)  $I_q = D_q$  (惰性群 = 分解群)

### §3 $\mathbb{Q}$ 上の $p$ 拡大 ( Scholz-Reichardt )

**定義**  $p$  拡大  $K/\mathbb{Q}$  が  $N$ -Scholz であるとは

$\stackrel{\text{def}}{\iff}$  すべての  $q \in \text{Ram}(K/\mathbb{Q})$  に対して

(1)  $q \equiv 1 \pmod{p^N}$ , (2)  $I_q = D_q$  ( 惰性群 = 分解群 )

**定理 E**  $(\varepsilon) : 1 \rightarrow \mathbb{Z}/p\mathbb{Z} \rightarrow E \rightarrow G(K/\mathbb{Q}) \rightarrow 1$

$K/\mathbb{Q} : N$ -Scholz,  $\exp(E) \leq p^N$

$\Rightarrow (K/\mathbb{Q}, \varepsilon) : \text{solvable}$

### §3 $\mathbb{Q}$ 上の $p$ 拡大 (Scholz-Reichardt)

**定義**  $p$  拡大  $K/\mathbb{Q}$  が  $N$ -Scholz であるとは

$\stackrel{\text{def}}{\iff}$  すべての  $q \in \text{Ram}(K/\mathbb{Q})$  に対して

(1)  $q \equiv 1 \pmod{p^N}$ , (2)  $I_q = D_q$  (惰性群 = 分解群)

**定理 E**  $(\varepsilon) : 1 \rightarrow \mathbb{Z}/p\mathbb{Z} \rightarrow E \rightarrow G(K/\mathbb{Q}) \rightarrow 1$

$K/\mathbb{Q} : N$ -Scholz,  $\exp(E) \leq p^N$

$\Rightarrow (K/\mathbb{Q}, \varepsilon) : \text{solvable}$

$(\because) K_q/\mathbb{Q}_q : \text{cyclic for all } q$

$(\varepsilon_q) : 1 \rightarrow \mathbb{Z}/p\mathbb{Z} \rightarrow E_q \rightarrow G(K_q/\mathbb{Q}_q) \rightarrow 1$

$E_q : \text{split or cyclic} \Rightarrow (K_q/\mathbb{Q}_q, \varepsilon_q) : \text{solvable}$

$\therefore (K/\mathbb{Q}, \varepsilon) : \text{solvable}$

## §3 $\mathbf{Q}$ 上の $p$ 拡大 (Scholz-Reichardt)

### Scholz-Reichardt の手法

$K/\mathbf{Q} : N$ -Scholz,  $S = \text{Ram}(K/\mathbf{Q})$

$(\varepsilon) : 1 \rightarrow \mathbf{Z}/p\mathbf{Z} \rightarrow E \rightarrow G(K/\mathbf{Q}) \rightarrow 1 ; \exp(E) \leq p^N$

## §3 Q 上の p 拡大 ( Scholz-Reichardt )

### Scholz-Reichardt の手法

$K/\mathbf{Q} : N$ -Scholz,  $S = \text{Ram}(K/\mathbf{Q})$

$(\varepsilon) : 1 \rightarrow \mathbf{Z}/p\mathbf{Z} \rightarrow E \rightarrow G(K/\mathbf{Q}) \rightarrow 1 ; \exp(E) \leq p^N$

$(K/\mathbf{Q}, \varepsilon) : \text{solvable} (\because \text{定理 E})$

$\Rightarrow S$  の外で不分岐な solution  $L_0/\mathbf{Q}$  を持つ

$(\because B_{\mathbf{Q}}(S) = \mathbf{Q}^{\times p}, \text{定理 C})$

**\*\*  $L_0/\mathbf{Q}$  は Scholz 拡大とは限らない \*\***

### §3 $\mathbb{Q}$ 上の $p$ 拡大 (Scholz-Reichardt)

#### Scholz-Reichardt の手法

$K/\mathbb{Q}$  :  $N$ -Scholz,  $S = \text{Ram}(K/\mathbb{Q})$

$(\varepsilon) : 1 \rightarrow \mathbb{Z}/p\mathbb{Z} \rightarrow E \rightarrow G(K/\mathbb{Q}) \rightarrow 1 ; \exp(E) \leq p^N$

$(K/\mathbb{Q}, \varepsilon) : \text{solvable} (\because \text{定理 E})$

$\Rightarrow S$  の外で不分岐な solution  $L_0/\mathbb{Q}$  を持つ

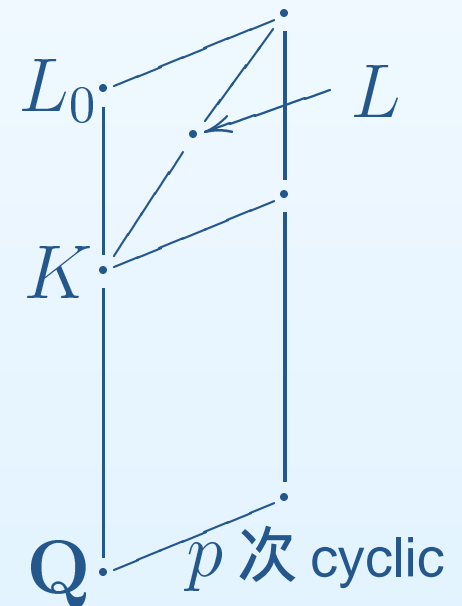
$(\because B_{\mathbb{Q}}(S) = \mathbb{Q}^{\times p}, \text{定理 C})$

**\*\*  $L_0/\mathbb{Q}$  は Scholz 拡大とは限らない \*\***

$\Rightarrow N$ -Scholz solution  $L/\mathbb{Q}$  で

$$|\text{Ram}(L/\mathbb{Q})| \leq |\text{Ram}(K/\mathbb{Q})| + 1$$

をみたすものを持つ



## §4 分岐する素点の最少個数

**記号**  $G : p$  群に対して

$$\text{ram}^t(G) = \min \left\{ |\text{Ram}(K/\mathbf{Q})| \mid \begin{array}{l} K/\mathbf{Q} \text{ tamely ramified} \\ G(K/\mathbf{Q}) \cong G \end{array} \right\}$$

$$d(G) = \text{rank} G/[G, G]$$

## §4 分岐する素点の最少個数

**記号**  $G : p$  群に対して

$$ram^t(G) = \min \left\{ |Ram(K/\mathbf{Q})| \mid \begin{array}{l} K/\mathbf{Q} \text{ tamely ramified} \\ G(K/\mathbf{Q}) \cong G \end{array} \right\}$$

$$d(G) = \text{rank} G/[G, G]$$

**知られていること**  $|G| = p^n$  とする

(1) Scholz-Reichardt :  $d(G) \leq ram^t(G) \leq n$

★ Cueto-Hernández, Villa-Salvador(2000) :

$$ram^t(G) = d(G)$$

(2) Plans(2004) : ★ のミスの指摘と (1) の改良

(3) Nomura(2007) : (2) のささやかな改良と

$$|G| \leq 3^5 \Rightarrow ram^t(G) = d(G)$$

## §5 不分岐 $p$ 拡大の存在について

**問題**  $G : p$  群

$\exists? k, \exists? K$  s.t.  $K/k$  は不分岐,  $G(K/k) \cong G$

## §5 不分岐 $p$ 拡大の存在について

**問題**  $G : p$  群

$\exists? k, \exists? K$  s.t.  $K/k$  は不分岐,  $G(K/k) \cong G$

**知られていること**

Fröhlich

$\forall n \in \mathbf{N}, \exists k, \exists K$  s.t.  $K/k$  不分岐,  $G(K/k) \cong S_n$

Ozaki

$k(p) : k$  の最大不分岐  $p$  拡大

$\forall G : p$  群,  $\exists k$  s.t.  $G(k(p)/k) \cong G$

## §5 不分岐 $p$ 拡大の存在について

**問題**  $G : p$  群

$\exists? k, \exists? K$  s.t.  $K/k$  は不分岐,  $G(K/k) \cong G$

**知られていること**

Fröhlich

$\forall n \in \mathbf{N}, \exists k, \exists K$  s.t.  $K/k$  不分岐,  $G(K/k) \cong S_n$

Ozaki

$k(p) : k$  の最大不分岐  $p$  拡大

$\forall G : p$  群,  $\exists k$  s.t.  $G(k(p)/k) \cong G$

注 : Ozaki 氏の手法だと  $k$  が大きくなってしまおう

やりたいこと

- $k$  を小さくしたい
- $k$  を構成したい

## §5 不分岐 $p$ 拡大の存在について

**定理 1**  $\forall G : p$  群,

$\exists^\infty k/\mathbb{Q} : \text{初等アーベル } p \text{ 拡大}, \exists K/k : \text{不分岐}$   
s.t.  $G(K/k) \cong G$

注 :  $k$  は理論的には構成できる

## §5 不分岐 $p$ 拡大の存在について

**定理 1**  $\forall G : p$  群,

$\exists^\infty k/\mathbf{Q} : \text{初等アーベル } p \text{ 拡大}, \exists K/k : \text{不分岐}$   
s.t.  $G(K/k) \cong G$

注 :  $k$  は理論的には構成できる

**補題 2**

(1)  $K/k : \text{不分岐 } p \text{ 拡大},$

(2)  $B_k(S) = k^{\times p},$

(3)  $(\varepsilon) : 1 \rightarrow \mathbf{Z}/p\mathbf{Z} \rightarrow E \rightarrow G(K/k) \rightarrow 1$

は分裂しない中心拡大

$\Rightarrow (K/k, \varepsilon)$  は  $S$  の外で不分岐な proper solution  
を持つ

## §5 不分岐 $p$ 拡大の存在について

(定理 1 の証明 : 概略)

$$G \supset G_1 = G^p[G, G] \supset G_2 \supset G_3 \supset \cdots \supset G_m = \{1\}$$

$$G \triangleright G_i, G_i/G_{i+1} \cong \mathbf{Z}/p\mathbf{Z} \quad (i \geq 1)$$

$\Rightarrow$  •  $G/G_1 \cong (\mathbf{Z}/p\mathbf{Z})^d$ ,  $d = d(G)$  :  $G$  のランク

•  $1 \rightarrow G_i/G_{i+1} \rightarrow G/G_{i+1} \rightarrow G/G_i \rightarrow 1$   
は分裂しない中心拡大

## §5 不分岐 $p$ 拡大の存在について

(定理1の証明：概略)

$$G \supset G_1 = G^p[G, G] \supset G_2 \supset G_3 \supset \cdots \supset G_m = \{1\}$$

$$G \triangleright G_i, G_i/G_{i+1} \cong \mathbf{Z}/p\mathbf{Z} \quad (i \geq 1)$$

$\Rightarrow$  •  $G/G_1 \cong (\mathbf{Z}/p\mathbf{Z})^d$ ,  $d = d(G)$  :  $G$  のランク

$$\bullet 1 \rightarrow G_i/G_{i+1} \rightarrow G/G_{i+1} \rightarrow G/G_i \rightarrow 1$$

は分裂しない中心拡大

方針 :  $G/G_1, G/G_2, G/G_3, \dots$  をガロア群に持つような不分岐拡大を順に構成する

## §5 不分岐 $p$ 拡大の存在について

(定理 1 の証明 : 概略)

$$G \supset G_1 = G^p[G, G] \supset G_2 \supset G_3 \supset \cdots \supset G_m = \{1\}$$

$$G \triangleright G_i, G_i/G_{i+1} \cong \mathbf{Z}/p\mathbf{Z} \quad (i \geq 1)$$

$\Rightarrow$  •  $G/G_1 \cong (\mathbf{Z}/p\mathbf{Z})^d$ ,  $d = d(G)$  :  $G$  のランク

$$\bullet 1 \rightarrow G_i/G_{i+1} \rightarrow G/G_{i+1} \rightarrow G/G_i \rightarrow 1$$

は分裂しない中心拡大

方針 :  $G/G_1, G/G_2, G/G_3, \dots$  をガロア群に持つような不分岐拡大を順に構成する

Step 1 : genus theory より

$\exists k_1/\mathbf{Q}$  :  $p$  次巡回拡大,  $\exists K_1/k_1$  : 不分岐

$$\text{s.t. } G(K_1/k_1) \cong G/G_1$$

## §5 不分岐 $p$ 拡大の存在について

Step 2 :  $(\varepsilon) : 1 \rightarrow \mathbf{Z}/p\mathbf{Z} \rightarrow G/G_2 \rightarrow G(K_1/k_1) \rightarrow 1$   
 $\exists S : k_1$  の素点の有限集合 s.t.

$$(1) B_{k_1}(S) = k_1^{\times p} \quad (2) N(\mathfrak{q}) \equiv 1 \pmod{p} \text{ for } \forall \mathfrak{q} \in S$$

$$(3) S \cap \text{Ram}_{k_1}(k_1/\mathbf{Q}) = \emptyset$$

## §5 不分岐 $p$ 拡大の存在について

Step 2 :  $(\varepsilon) : 1 \rightarrow \mathbf{Z}/p\mathbf{Z} \rightarrow G/G_2 \rightarrow G(K_1/k_1) \rightarrow 1$

$\exists S : k_1$  の素点の有限集合 s.t.

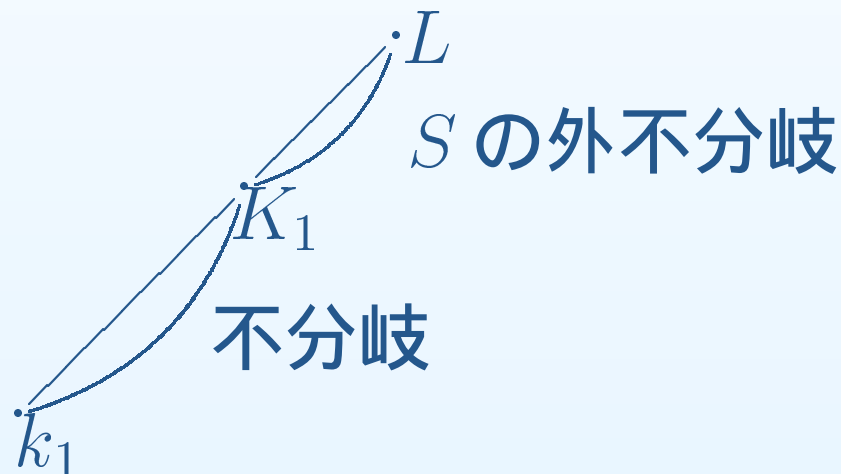
(1)  $B_{k_1}(S) = k_1^{\times p}$     (2)  $N(\mathfrak{q}) \equiv 1 \pmod{p}$  for  $\forall \mathfrak{q} \in S$

(3)  $S \cap \text{Ram}_{k_1}(k_1/\mathbf{Q}) = \emptyset$

補題 2 より

$\exists L/K_1/k_1$  ガロア拡大 s.t.

- $G(L/k_1) \cong G/G_2$
- $L/k_1$  は  $S$  の外で不分岐



## §5 不分岐 $p$ 拡大の存在について

Step 2 :  $(\varepsilon) : 1 \rightarrow \mathbf{Z}/p\mathbf{Z} \rightarrow G/G_2 \rightarrow G(K_1/k_1) \rightarrow 1$

$\exists S : k_1$  の素点の有限集合 s.t.

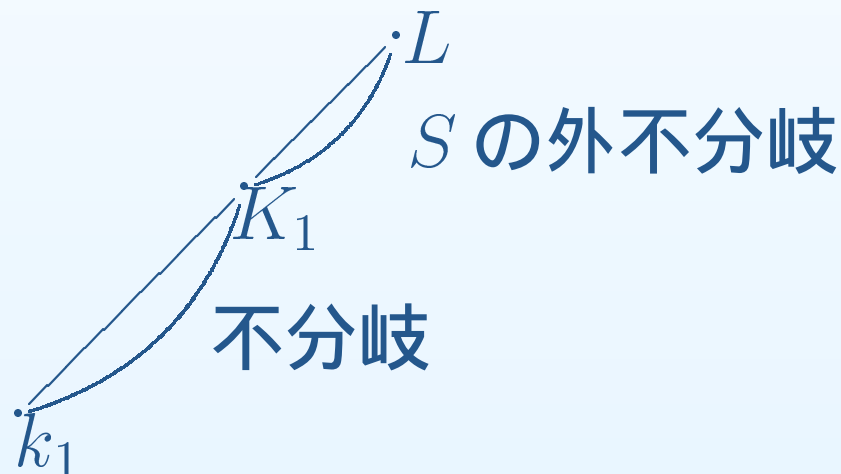
(1)  $B_{k_1}(S) = k_1^{\times p}$     (2)  $N(\mathfrak{q}) \equiv 1 \pmod{p}$  for  $\forall \mathfrak{q} \in S$

(3)  $S \cap \text{Ram}_{k_1}(k_1/\mathbf{Q}) = \emptyset$

補題 2 より

$\exists L/K_1/k_1$  ガロア拡大 s.t.

- $G(L/k_1) \cong G/G_2$
- $L/k_1$  は  $S$  の外で不分岐



$\mathfrak{q} \in S$  とする

$k_1/\mathbf{Q} : p$  拡大だから  $N(\mathfrak{q}) = q^{p^t} \equiv 1 \pmod{p} \therefore q \equiv 1 \pmod{p}$

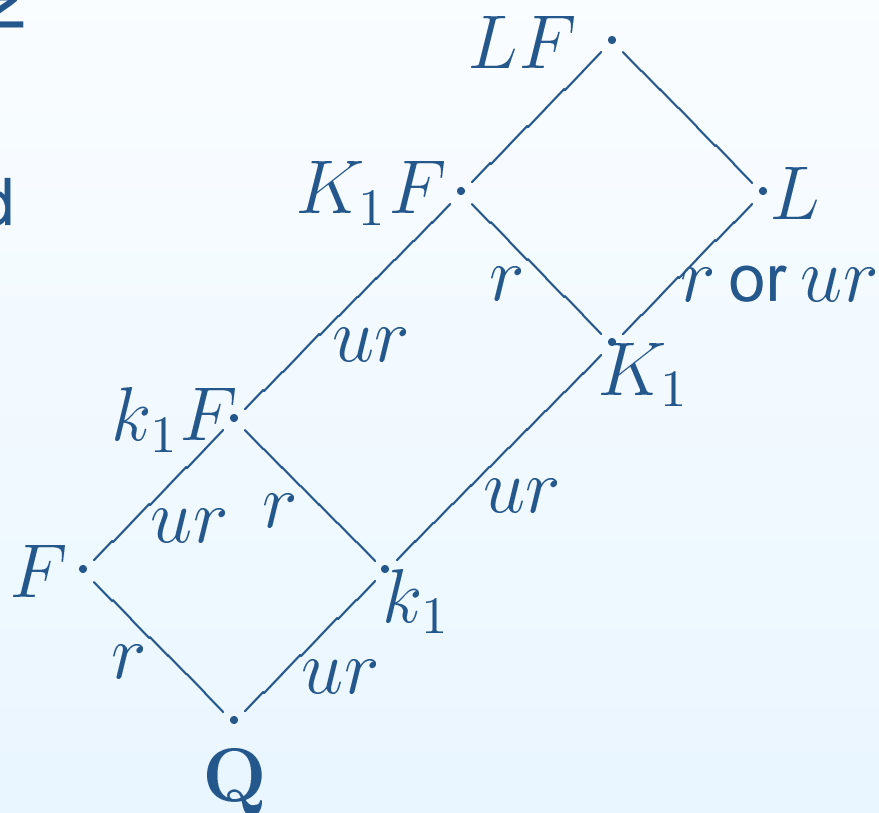
$\exists^\infty F/\mathbf{Q} : p$  次巡回拡大 s.t.  $\forall \mathfrak{q} \in S |_{\mathbf{Q}}$  は分岐

## §5 不分岐 $p$ 拡大の存在について

$q \in S$  の分岐の様子

$r$  : ramified

$ur$  : unramified



$p \nmid q$  だから  $q$  : 不分岐 in  $LF/K_1F$

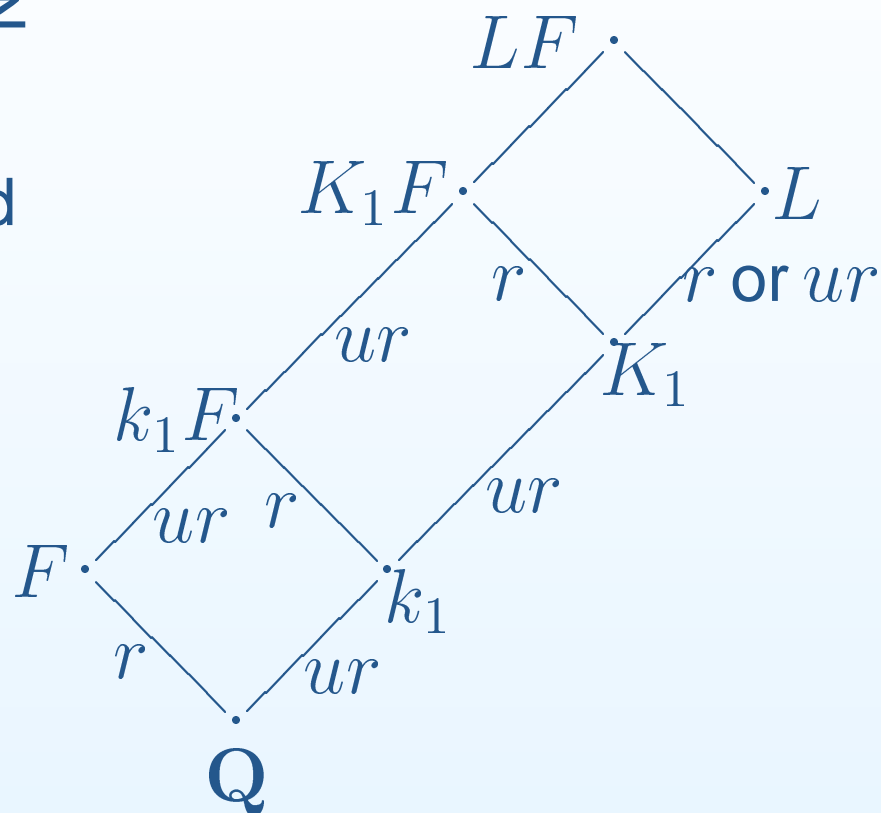
$\therefore LF/k_1F$  : 不分岐,  $G(LF/k_1F) \cong G/G_2$

## §5 不分岐 $p$ 拡大の存在について

$q \in S$  の分岐の様子

$r$  : ramified

$ur$  : unramified



$p \nmid q$  だから  $q$  : 不分岐 in  $LF/K_1F$

$\therefore LF/k_1F$  : 不分岐,  $G(LF/k_1F) \cong G/G_2$

同様の操作を繰り返せば良い

(証明終)

## §5 不分岐 $p$ 拡大の存在について

$G = \mathbf{Z}/p^n\mathbf{Z}$  に対して, 定理 1 を適用し証明に注意すれば次を得る

系 3

$\forall n, \exists^\infty k/\mathbf{Q}$  ガロア拡大

$$\text{s.t. } G(k/\mathbf{Q}) \cong (\mathbf{Z}/p\mathbf{Z})^n, \mathbf{Z}/p^n\mathbf{Z} \subset Cl_k$$

## §5 不分岐 $p$ 拡大の存在について

$G = \mathbf{Z}/p^n\mathbf{Z}$  に対して, 定理 1 を適用し証明に注意すれば次を得る

系 3

$\forall n, \exists^\infty k/\mathbf{Q}$  ガロア拡大

s.t.  $G(k/\mathbf{Q}) \cong (\mathbf{Z}/p\mathbf{Z})^n, \mathbf{Z}/p^n\mathbf{Z} \subset Cl_k$

質問

$\exists? k/\mathbf{Q} : p$  次巡回拡大 s.t.  $\mathbf{Z}/p^n\mathbf{Z} \subset Cl_k$

御清聴ありがとうございました

# 質問についての補足

**質問**  $\exists? k/\mathbf{Q} : p$  次巡回拡大 s.t.  $\mathbf{Z}/p^n\mathbf{Z} \subset Cl_k$

すぐわかること  $n \geq 2$

$\nexists k/\mathbf{Q} : p$  次巡回拡大 s.t.  $Cl_k(p) \cong \mathbf{Z}/p^n\mathbf{Z}$

# 質問についての補足

**質問**  $\exists? k/\mathbb{Q} : p$  次巡回拡大 s.t.  $\mathbb{Z}/p^n\mathbb{Z} \subset Cl_k$

すぐわかること  $n \geq 2$

$\nexists k/\mathbb{Q} : p$  次巡回拡大 s.t.  $Cl_k(p) \cong \mathbb{Z}/p^n\mathbb{Z}$

( $\therefore$ ) 存在したとすると

$\exists L/k/\mathbb{Q}$  s.t.  $L/k$  : 不分岐  $p^2$  次巡回拡大

このとき,  $G(L/\mathbb{Q})$  は

- 位数  $p^3$  の非アーベル群
- $\mathbb{Z}/p^2\mathbb{Z}$  を部分群に持つ
- 位数  $p$  の元で生成される

しかし, このような群は存在しない

## 参考文献

1. A. Cueto-Hernández and G.D. Villa-Salvador, *Nilpotent extensions of number fields with bounded ramification*, Pacific J. Math. **196** (2000)
2. Fröhlich, *On non-ramified extensions with prescribed Galois group*, Mathematika **9** (1962)
3. J. Neukirch, *Über das Einbettungsproblem der algebraischen Zahlentheorie*, Invent. Math. **21** (1973)
4. A. Nomura, *Notes on the minimal number of ramified primes in some  $l$ -extensions of  $\mathbb{Q}$* , Arch. Math. **90**(2008)
5. M. Ozaki, 準備中
6. B. Plans, *On the minimal number of ramified primes in some solvable extensions of  $\mathbb{Q}$* , Pacific J. Math. **215**(2004)
7. J.-P. Serre, *Topics in Galois Theory*, 1992.
8. A. Scholz, *Konstruktion algebraischer Zahlkörper mit beliebiger Gruppe von Primzahlpotenzordnung I*, Math. Z. **42**(1936)
9. H. Reichardt, *Konstruktion vom Zahlkörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung*, J. Reine Angew. Math. **177**(1937)

# 系3の補足

$k/\mathbf{Q} : p$  次巡回拡大 s.t.  $|Ram(k/\mathbf{Q})| \geq 2$

$S : k$  の素点の有限集合 s.t.

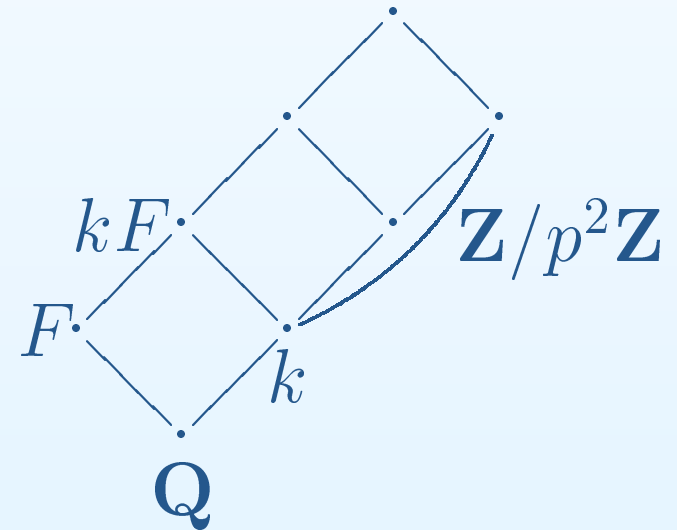
(1)  $B_k(S) = k^{x^p}$  (2)  $N(\mathfrak{q}) \equiv 1 \pmod{p}$  for  $\forall \mathfrak{q} \in S$

(3)  $S \cap Ram_k(k/\mathbf{Q}) = \emptyset$

$F/\mathbf{Q} : p$  次巡回拡大 s.t.  $\forall q \in S |_{\mathbf{Q}}$  は分岐

このとき

- $G(kF/\mathbf{Q}) \cong (\mathbf{Z}/p\mathbf{Z})^2$
- $\mathbf{Z}/p^2\mathbf{Z} \subset Cl_{kF}$



# $B_k(S) = k^{x^p}$ の判定

$$B_k(S) = \{ \alpha \in k^\times \mid (\alpha) = \mathfrak{a}^p \ (\exists \mathfrak{a}), \ \alpha \in k_{\mathfrak{q}}^p \ (\forall \mathfrak{q} \in S) \}$$

$$B := B_k(\emptyset) = \{ \alpha \in k^\times \mid (\alpha) = \mathfrak{a}^p \ (\exists \mathfrak{a}) \}$$

$$K := k(\zeta_p), \quad L := k(\sqrt[p]{\alpha}; \alpha \in B)$$

$\mathfrak{q} : k$  の素点,  $\tilde{\mathfrak{q}} : L$  への延長

$$\left\langle \left[ \frac{L/K}{\tilde{\mathfrak{q}}} \right]; \mathfrak{q} \in S \right\rangle = G(L/K) \Rightarrow B_k(S) = k^{x^p}$$

( $\because$ )  $\beta \in B_k(S)$   $\beta \notin k^{x^p}$  とする.

$\forall \mathfrak{q} \in S$  は  $K(\sqrt[p]{\beta})/K$  で完全分解する.

