科学研究費助成事業　　研究成果報告書

平成 ２６ 年　 ５ 月 １６ 日現在

機関番号：１３３０１
研究種目：基盤研究(C)
研究期間：2011～2013
課題番号：２３５４００１０

研究課題名（和文）分岐を制限したガロアの逆問題とその類体塔問題への応用に関する研究

研究課題名（英文）Research of the inverse Galois problems with restricted ramifications and their applications to the class field tower problems

研究代表者
野村　明人（Nomura, Akito）

金沢大学・機械工学系・教授

研究者番号：００３１３７００

交付決定額（研究期間全体）：（直接経費）　　3,400,000円、（間接経費）　　1,020,000円

研究成果の概要（和文）：本研究の主目的は，p群に対するガロアの逆問題の不分岐解の存在について考察することである。p，q は異なる奇素数で，p-1またはp+1がqで割り切れるとする。さらに，Eを位数がpの３乗の非アーベル群，kを有理数体上のq次巡回拡大体とする。本研究では，k上の不分岐ガロア拡大でガロア群がEと同型なものが存在するための十分条件を証明した。また，PARIを用いた数値計算を行い，ガロア群がEと同型な不分岐拡大を持つような巡回拡大体の具体例を構成した。

研究成果の概要（英文）：The main purpose of this research is to study the inverse Galois problems with restricted ramifications for p-groups and their applications to the class field tower problems.
Let p and q be distinct odd primes such that p-1 or p+1 is divisible by q. Let E be a non-abelian group of order p cubed, and let k be a cyclic extension over rational number field Q. We obtained the sufficient conditions for the existence of the unramified extension L/k such that the Galois group is isomorphic to E. By computing with PARI, we also gave some examples of cyclic fields which has an unramified extension with the Galois group E.

研究分野：数物系科学

科研費の分科・細目：数学・代数学

キーワード：ガロアの逆問題　不分岐拡大　類体塔　類数

１．研究開始当初の背景

代数体 k と有限群 G が与えられたとき,「不分岐ガロア拡大 L/k でそのガロア群が G と同型なものが存在するか？」・・・(*) という問題を考える。G がアーベル群の場合は，類体論により，(*)が肯定的であるための必要十分条件が分かっている。

類体論の一般化の一つの方向は，代数体の類体論を Z 上有限型１次元概型のアーベル被覆の理論ととらえこれを高次元化することであり，加藤和也氏，斎藤秀司氏，S. Bloch などにより目覚ましい成果が得られている。一方，非アーベルな群 G に対して問題(*)を考察することは，類体論の一般化という枠組みでも重要であると考える。しかし，このアプローチに関しては，群の位数が小さい場合に A. Scholz－O. Taussky(J. Reine Angew. Math(1934))，C. Bachoc－S.H. Kwon(Acta Arith.(1992))，L. Bartholdi－M. R. Bush(J. Number Theory(2007)) などの個別の研究があるだけで，十分な研究が行われているとは言えない。

また，問題(*)を考察することは，代数体 k の最大不分岐 p 拡大のガロア群 Γ(k)[p]の構造を解明することにつながると考える。Γ(k)[p]は当初，有限群であると予想されていたが，無限群になるための十分条件が Golod-Schafarevich(1964) により与えられた。その後，２次体の場合には Schoof により改良され，イデアル類群の p-rank が３以上であれば Γ(k)[p]が無限群であることが証明された。また，３次体の場合は Maire により精密化されている。Γ(k)[p]に関する最も基本的な問題は，「Γ(k)[p]はいつ有限アーベル群か？」というものであるが，この問題も解決には至っていない。

２．研究の目的

本研究の目的は，<u>１．研究開始当初の背景</u>で述べた問題(*)を非アーベル p 群 G に対して考察し，その応用として「類体論の冪零拡大への一般化」「代数体 k の最大不分岐 p 拡大のガロア群 Γ(k)[p]の構造解析」について解決またはその基盤を築くことである。具体的には，関連する以下の問題を考察し結果を得ることである。

（１）k が有理数体 Q 上の巡回拡大で G が非アーベル p 群の場合に上記問題(*)を考察し，k 上の不分岐拡大でガロア群が G と同型なものが存在するための条件を考察する。先ず，k が Q 上の素数次巡回拡大で，G の位数が p^3 の場合から考察を始める。

（２）p が小さい素数で G が非アーベル p 群の場合に，k 上の不分岐拡大でガロア群が G と同型なものが存在するような巡回拡大体 k を数値計算により具体的に構成する。

（３）代数体 k と奇素数 p に対して，Γ(k)[p]が有限アーベル群になるための k，p の条件を考察する。k が２次体の場合には，代表者野村(Osaka J.(1991))により解決されており，吉田英司氏がある種の(2,2)拡大について解決した。本研究では，一般の(2,2)拡大についてこの問題を考察する。

（４）k が２次体でイデアル類群の p-rank が２の場合について Γ(k)[p]が無限群になるための条件を調べる。また，Pari-gp と GAP を利用し，無限群になるような具体例を構成する。

３．研究の方法

代数体の埋め込み問題と群論的な考察を組み合わせて不分岐拡大を構成する。先ず，代数体の埋め込み問題について説明する。ガロア拡大 K/k と群拡大(ε):1→A→E→G(K/k)→1 が与えられたときに，ガロア拡大 L/K/k で自然な完全列 1→G(L/K) →G(L/k) →G(K/k)→1 が(ε)と一致するものが存在するかどうかを考察するのが埋め込み問題であり，これを(K/k, ε)で表す。

本研究では，不分岐拡大を構成する必要があるので，埋め込み問題の解 L は「L/K は不分岐」という条件を満たす必要がある。研究代表者の野村は，群拡大(ε)が中心拡大の場合に埋め込み問題の解の分岐をコントロールする手法を提案し，Osaka J. Math. 28(1991),55－62 で発表した。この手法を適用する場合の問題は，群拡大の構造が複雑になることである。

本研究の方法は，群拡大の構造を詳細に考察し，野村の手法を適用することにより不分岐非アーベル拡大の存在を示すことである。数論的な考察は，代表者野村と分担者平林が主に担当した。また群論的な考察は分担者の伊藤が，組合せ論的なアプローチは連携研究者の山田が担当した。さらに本研究では，位数が小さい非アーベル p 群に対して具体的な数値計算を行うことも重要である。Pari-gp による数値計算は，代表者野村と連携研究者の木村が行った。また GAP による群の数値計算については，専門家である脇克志氏（山形大学）の助言を仰いだ。

４．研究成果

p 群に対するガロアの逆問題を考察し，以下の結果を得た。

（１）<u>位数が p^3 の群に対するガロアの逆問題</u>：p，q を異なる奇素数とし，k を有理数体 Q 上の q 次巡回拡大体とする。また，E1 と E2 は位数が p^3 の非アーベル群で，E1 の群指数が p で E2 の群指数が p^2 であるとする。本研究では，K 上の不分岐ガロア拡大でガロア群が E1 や E2 と同型なものが存在するための条件を考察した。

① q が p+1 の約数の場合

このケースの主結果は「k の類数が p で割り切れるならば，k 上の不分岐拡大 L/k でそのガロア群が E1 と同型なものが存在する」である。さらに，その応用または付随する結果として以下を示した。

(a) ガロア拡大 L/k/Q で，L/k が不分岐 E2 拡

大となるものは存在しない。
(b) L/k が不分岐 E2 拡大ならば，L の類数は p で割り切れる。
(c) k のイデアル類群は p-rank が２で位数 p^2 の元を持つとする。このとき，不分岐ガロア拡大 L/k でそのガロア群が E2 と同型なものが存在する。

② q が p-1 の約数の場合

このケースは，ガロア群 G(k/Q)のイデアル類群 Cl(k)への作用のパターンがたくさんあり①の場合より複雑である。K/k/Q はガロア拡大で，K/k は不分岐(p,p)拡大であるとする。このとき，ガロア群 G(k/Q)は G(K/k)に作用する。この作用は 2 種類あり，それを以下のように定義する。K/F/k，[F:Q]=p を満たす任意の F が有理数体 Q 上のガロア拡大である時に Type[α,α]，そうでない時 Type[α,β]と呼ぶことにする。このとき，以下を示した。
(a) K/k/Q はガロア拡大で，K/k は不分岐(p,p)拡大であるとし，G(k/Q)の G(K/k)への作用が Type[α,β]であり，かつある種の付帯条件を満たすとする。このとき，不分岐ガロア拡大 L/k でそのガロア群が E1 と同型なものが存在する。
(b) k/Q は 3 次巡回拡大とし，p は 3n+1(n は自然数)の形の素数であるとする。不分岐 p 次巡回拡大 F/k で F/Q がガロア拡大でないものが存在するならば，不分岐ガロア拡大 L/k でそのガロア群が E1 と同型なものが存在する。

（２）数値計算による具体的構成

計算ソフト Pari を用いて，ガロア群が E1 や E2 と同型な不分岐拡大が存在するような有理数体上の巡回拡大 k を構成した。

① k が Q 上の 3 次巡回拡大の場合(q=3)

方程式 $x^3-nx^2-(n+3)x-1=0$(n:整数)の分解体を k とし，p=7 とする。
(a) n=193，295，508，523，525，532，548，762，852，983 のとき，k 上の不分岐ガロア拡大でそのガロア群が E1 と同型なものが存在する。
(b) n=-269 のとき，k 上の不分岐ガロア拡大でそのガロア群が E2 と同型なものが存在する。

② k が Q 上の 5 次巡回拡大の場合(q=5)

方程式

$$x^5+324x^4+9890x^3+79115x^2-4706x+1=0$$

の分解体を k とし，p=11 とする。このとき，k 上の不分岐ガロア拡大でそのガロア群が E1 と同型なものが存在する。

以下で本研究の今後の展望と課題について述べる。

２．研究の目的で述べた（３）（４）の研究ついては、まだ十分な成果が得られていないがアプローチの方向性はわかってきた。

（３）Γ(k)[p]が有限アーベル群になるための条件であるが、吉田英司氏の結果を拡張するためには、単項化の問題を詳しく調べる必要があることがわかった。単項化との関係は古くは Scholz-Taussky により指摘されているが、その後の進展を踏まえ代数体の埋め込み問題との関係を考察することで進展が得られると考えている。

（４）2 次体の場合のΓ(k)[p]の構造解析であるが、中心拡大に対する野村の手法だけでは，代数体 k の最大不分岐 p 拡大に到達することはできないことが分かっている。よって，中心拡大でない場合の埋め込み問題で分岐をコントロールする理論の構築が必要であると考える。また具体的に数値例を計算することも重要であるが，そのためには計算代数ソフト GAP の専門家との共同研究が必要不可欠である。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計７件）

① Nomura Akito、Some remarks on the existence of certain unramified p-extensions、Tokyo J. of Math.、査読有、印刷中
② Momihara Koji、Yamada Mieko、Divisible difference families from Galois rings GR(4,s) and Hadamard matrices、Designs, Codes and Cryptography、査読有、印刷中
③ Hirabayashi Mikihito、A generalization of Jakubec's formula、Mathematica Slovaca、査読有、印刷中
④ Nomura Akito、Notes on the existence of unramified non-abelian p-extensions over cyclic fields、Proc. Japan Acad.、査読有、vol. 90、2014、pp. 67－70、DOI:10.3792/pjaa.90.67
⑤ 伊藤達郎、TD 対と q-Onsager 代数、数学、査読有、65 巻、2013、pp. 69－92
⑥ Ito Tatsuro、Terwilliger Paul、Mock tridiagonal systems、Linear Algebra Appl.、査読有、vol. 435、No. 8、2011、pp. 1997－2006 DOI:10.1016/j.laa.2011.03.025
⑦ Ito Tatsuro、Nomura Kazumasa、Terwilliger Paul、A classification of sharp tridiagonal pairs、Linear Algebra Appl.、査読有、vol. 435、No. 8、2011、pp. 1857－1884 DOI:10.1016/j/laa.2011.03.032

〔学会発表〕（計２０件）

① 野村明人、位数が p^3 の群に対するガロアの逆問題の不分岐解について、香川セミナー、2014 年 5 月 24 日（講演決定）、香川大学、高松市
② 平林幹人、Hasse の方法による虚アーベル体の相対類数公式についてのいくつかの注意、北陸数論セミナー、2014 年 5 月

1 日、金沢大学サテライトプラザ、金沢市

③ Yamada Mieko、A decoding algorithm of BCH codes over Galois rings、The 3rd Taiwan-Japan Conference on Combinatorics and its Applications、2014.3.21、National Chiayi Univ.、Taiwan

④ 伊藤達郎、The classification of TD-pairs、RIMS 研究集会「有限群とその表現，頂点作用素代数，代数的組合せ論の研究」、2014 年 3 月 6 日、京都大学数理解析研究所

⑤ Ito Tatsuro、The classification of TD-pairs of Type II、12th Korea-Japan Workshop on Algebra and Combinatorics、2014 年 1 月 23 日、KAIST、Daejeon、Korea

⑥ 山田美枝子、局所体の部分集合から得られるガロア環の差集合、応用数学合同研究集会、2013 年 12 月 19 日、龍谷大学、大津市

⑦ 木村巌、モジュラー形式の計算、「代数学と計算」研究集会、2013 年 12 月 19 日、首都大学東京、八王子市

⑧ 野村明人、位数が p^3 の群に対するガロアの逆問題の不分岐解について、北陸数論セミナー、2013 年 7 月 4 日、金沢大学サテライトプラザ、金沢市

⑨ 木村巌、冪剰余記号のガウス和と相互法則について、北陸数論セミナー、2013 年 5 月 9 日、金沢大学サテライトプラザ、金沢市

⑩ 平林幹人、Jakubec による p 分体の相対類数公式の一般化、北陸数論セミナー、2012 年 11 月 8 日、金沢大学サテライトプラザ、金沢市

⑪ Ito Tatsuro、The Pfaff-Saalschutz summation formula revisited、Workshop on Algebraic Combinatorics、2012.8.21、Jiao Tong University、Shanghai、China

⑫ 伊藤達郎、置換群，アソシエーションスキーム，ターウィリガー代数、第 24 回有限群論草津セミナー、2012 年 7 月 28 日、草津セミナーハウス、群馬県吾妻郡

⑬ 木村巌、Boston-Ellenberg heuristic の紹介、北陸数論セミナー、2012 年 5 月 10 日、金沢大学サテライトプラザ、金沢市

⑭ 平林幹人、Hasse の第二変形法による虚アーベル体の相対類数公式と Jakubec の論文の紹介、北陸数論セミナー、2012 年 4 月 26 日、金沢大学サテライトプラザ、金沢市

⑮ 木村巌、Redei の公式の結び目と素数の視点からの紹介、北陸数論セミナー、2011 年 12 月 15 日、金沢大学サテライトプラザ、金沢市

⑯ 野村明人、巡回体上の不分岐非アーベル p^3 次拡大の存在について、北陸数論セミナー、2011 年 11 月 25 日、金沢大学サテライトプラザ、金沢市

⑰ 山田美枝子、円分体の数論の組合せ数学への応用、北陸数論セミナー、2011 年 10 月 13 日、金沢大学サテライトプラザ、金沢市

⑱ Ito Tatsuro、Finite dimensional irreducible representation of certain subalgebras of the quantum affine algebra U_q(sl_2)、Workshop on Algebraic Combinatorics、2011.9.16、Jiao Tong Univ.、Shanghai, China

⑲ 伊藤達郎、アファイン量子群のある種の部分代数の有限次元規約表現について、第 23 回有限群論草津セミナー、2011 年 7 月 31 日、草津セミナーハウス、群馬県吾妻郡

⑳ 野村明人、最少分岐問題（minimal ramification problem）について、北陸数論セミナー、2011 年 7 月 21 日、金沢大学サテライトプラザ、金沢市

〔その他〕
ホームページ等
研究代表者の論文リストは
http://www.ms.t.kanazawa-u.ac.jp/~maths/nomura/nompaper.htm
で確認できる。また，本研究課題に関する発表が多数されている北陸数論セミナーでの講演概要等は
http://www.ms.t.kanazawa-u.ac.jp/~maths/Seminar/hokuriku.htm
で公開されている。

６．研究組織

(1)研究代表者
野村　明人（Nomura Akito）
金沢大学・機械工学系・教授
研究者番号：00313700

(2)研究分担者
伊藤　達郎（Ito Tatsuro）
金沢大学・数物科学系・教授
研究者番号： 90015909

(3)研究分担者
平林　幹人（Hirabayashi Mikihito）
金沢工業大学・基礎教育部・教授
研究者番号： 20167612

(4)連携研究者
山田美枝子（Yamada Mieko）
金沢大学・数物科学系・教授
研究者番号： 70130226

(5)連携研究者
木村巌（Kimura Iwao）
富山大学・理工学研究部・准教授
研究者番号： 10313587