

令和 5 年 6 月 7 日現在

機関番号：16101

研究種目：基盤研究(C) (一般)

研究期間：2017～2022

課題番号：17K05176

研究課題名(和文) K群の特殊元を用いた多変数岩澤加群の解析

研究課題名(英文) Analysis of multivariable Iwasawa modules by using special elements of K-groups

研究代表者

高橋 浩樹 (SUMIDA-TAKAHASHI, Hiroki)

徳島大学・大学院社会産業理工学研究部(理工学域)・教授

研究者番号：90291476

交付決定額(研究期間全体)：(直接経費) 3,400,000円

研究成果の概要(和文)：岩澤加群についての各種予想(一般Greenberg予想, 総実体のGreenberg予想, Kummer-Vandiver予想)に関連して, 計算機によって円分体のK群の特殊元を計算し, それぞれの予想の成立または不成立の理由について調査した. 特に一般Greenberg予想については,  $p$ 単数群のペアリングを計算することにより, 4を法として3と合同な65536以下の素数 $p$ について3つの例外的な素数を除いて $4p$ 円分体の予想が確認できた. ペアリングの非自明な零の個数は予測した分布にほぼ近似することが確認され, これは一般Greenberg予想の成立を支持する理由のひとつとなりうる.

研究成果の学術的意義や社会的意義

円分体のイデアル類群や単数群は古典的には不定方程式の解法において有効であり, その重要性は200年ほど前から数論研究者に認識されている. 最近では耐量子計算機暗号の候補として円分イデアル格子暗号や同種写像による楕円曲線暗号などが候補に挙がっているが, その理由としては定義の簡明さと構造の複雑さという点と多数の研究者が調査対象としている点が挙げられる. 本研究は, その重要な対象の基本的な現象に関する予想が成立するか否かについて調査している.

研究成果の概要(英文)：Concerning some conjecture (generalized Greenberg's conjecture, Greenberg's conjecture for totally real fields, the Kummer-Vandiver conjecture), we computed special elements of  $K$ -groups of cyclotomic fields, and investigated reasons of validity or invalidity of these conjectures. Particularly, concerning Greenberg's generalized conjecture, we computed pairings of  $p$ -units, and check the conjecture for  $4p$ -cyclotomic fields and all  $p < 65536$  such that  $p$  is congruent to 3 modulo 4 except for 3 primes. The distributions of the number of nontrivial zeros are close to the predicted distributions, which can be one of reasons of the validity of Greenberg's generalized conjecture.

研究分野：整数論

キーワード：Greenberg予想 Kummer-Vandiver予想 一般Greenberg予想 K-群 イデアル類群 単数

## 1. 研究開始当初の背景

本研究の背景にある未解決予想の Greenberg 予想, Vandiver 予想, 一般 Greenberg 予想について説明する。 $K$  を有限次代数体,  $p$  を素数として,  $K_\infty$  を  $K$  の  $\mathbf{Z}_p$  拡大とし,  $K_n \subset K_\infty$  を  $K$  上の  $p^n$  次拡大とする。 $A_n$  を  $K_n$  のイデアル類群の  $p$  部分,  $p^{e_n}$  を  $A_n$  の位数とすると, 1950 年代に岩澤健吉氏は「 $n$  が十分大きいとき,  $e_n = \lambda n + \mu p^n + \nu$  と表される」という代数的類数公式を示した。 $L(M)$  を代数体  $M$  に対する  $M$  上の最大不分岐アーベル  $p$  拡大とし,  $X(M) = \text{Gal}(L(M)/M)$  とする。 $X(K_\infty)$  は完備群環  $\Lambda = \mathbf{Z}_p[[\text{Gal}(K_\infty/K)]]$  が連続に作用する岩澤加群となるが,  $\lambda$  はこの加群の  $\mathbf{Z}_p$  ランクであり,  $\mu$  はこの加群の無限位数の  $\mathbf{Z}_p$  ねじれ加群の大きさを表している。

$K$  が円分体であるとき, 円分  $\mathbf{Z}_p$  拡大の  $\mu$  不変量は 0 であることが示されている。また, 円分  $\mathbf{Z}_p$  拡大の  $\lambda$  不変量は, 実円分体からの寄与のプラス部分と残りのマイナス部分に分けて考察され, マイナス部分については  $p$  進  $L$  関数の零点から計算できて様々な値をとることが知られている。その一方で, プラス部分については 0 以外の値は知られておらず, Greenberg 予想「総実代数体の  $\lambda$  不変量と  $\mu$  不変量は 0 であろう」と予想されている。この予想は岩澤氏が理論の創始期にこの問題を提起してから 60 年近く経過しており, 個々の代数体に対するいくつかの判定法が知られているものの, 円分体に限っても未解決である。

さらに  $p$  円分体に限ると, Greenberg 予想よりも強い Vandiver 予想「 $p$  円分体の実部分体の 3 つの岩澤不変量は全て 0 であろう」という予想があるが, 1 億 6,000 万以下の素数について計算機により成立が確認されていたものの, 証明の糸口は不明である。

Greenberg 予想の一般化である一般 Greenberg 予想は, 「代数体  $K$  に対して最大  $\Gamma = \mathbf{Z}_p^d$  拡大  $\tilde{K}$  を考えたとき, 岩澤加群  $X(\tilde{K}) = \text{Gal}(L(\tilde{K})/\tilde{K})$  は  $\mathbf{Z}_p[[\Gamma]]$  加群として擬有限であろう」という予想である。 $d = 1$  が従来の総実代数体の Greenberg 予想である。多変数版である  $d \geq 2$  についても虚二次体や  $p$  円分体などに対し複数の判定条件により計算機を用いて個々の代数体について成立が確認されているが, 一般的解決には遠い状況にある。

## 2. 研究の目的

本研究の目的は, 代数体上のガロア表現から構成される多変数岩澤加群の構造を  $K$  群の特殊元を効果的に利用することによって具体的に調査し, 総実代数体に対する Greenberg 予想の一般化である代数体の一般 Greenberg 予想という岩澤加群の擬有限性に関する未解決予想の成立理由を明らかにし, その精密な予想を定式化して解決への道筋を探ることである。

## 3. 研究の方法

本研究の特色は, 特殊元を系統的に利用することによってイデアル類群および Selmer 群の性質を効率良く明らかにすることにある。その際に, 古典的理論において重要であった岩澤加群の分類やガロア群の作用による分解を有効に利用していることを強調したい。なお, 円単数とガウス和と二種類の補助素数による実円分体のイデアル類群の計算から, Voevodsky によって証明された Quillen-Lichtenbaum 予想から二次体の整数環に対する高次  $K$  群の各素数部分が求められる。一般 Greenberg 予想に関わる現象を特徴的なケースで調べる際には, これらは貴重なデータになると期待される。また, 正規整数基底の存在問題および  $\mathbf{Z}_l$  拡大における  $\lambda_p$  不変量の決定問題において, 円単数,  $p$  進  $L$  関数, Gauss 和, 一般 Bernoulli 数などの特殊元が総合的に有効に利用されており, この種の類似の現象を一般化された岩澤理論の対象に対して考察することは, 興味深い研究になると期待される。

## 4. 研究成果

Kummer-Vandiver 予想, 総実代数体の Greenberg 予想に関連して, 二次体に 1 の原始  $p$  乗根を添加した体の円分  $\mathbf{Z}_p$  拡大に対する岩澤加群の構造について, 二次体の判別式の絶対値が 200 未満に対して 100 万までの素数の範囲について 2 回の調査, 絶対値が 10 未満に対しては 2000 万までの素

数の範囲での1回の調査を完了した。本研究成果は、[1]で公表しており、Kummer-Vandiver 予想に関連する一般化された例外素数の個数(図1参照)の漸近的な関数を求める問題およびその関数の候補を提出している。特に、 $p$  円分体に対して例外素数が見つげにくい理由(図2参照)について、2つの部分的な理由を挙げている。なお、この調査は継続しており、実二次体に対しては前者は140万まで、後者は3000万までの素数に対し調査が進行している。

図1:例外素数の個数 ( $p < 10^6$ )

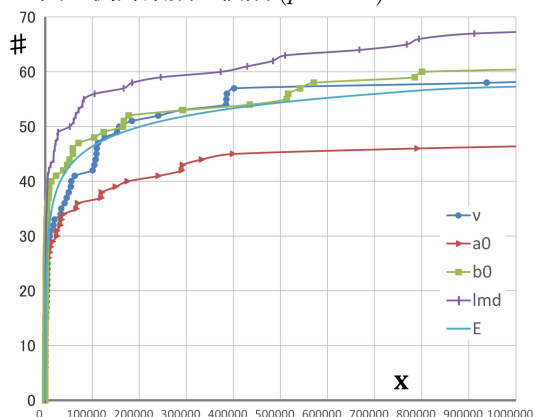
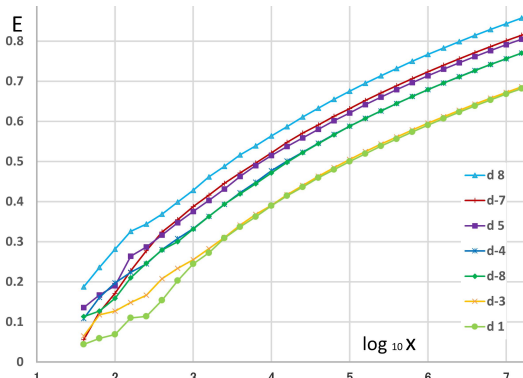


図2:例外素数の個数の期待値 ( $p < 2 \times 10^7$ )



岩澤加群の構造に深く関係する有限次代数体のイデアル類群の構造について、 $8p$  円分体に含まれる有理数体上2べき次の虚アーベル体に対する計算機による調査を行った。Redei-Reichardの二次体のイデアル類群の2部分の構造に関する定理がアーベル体に拡張されており、大半の場合にはアーベル体の二つの基本的な量からイデアル類群の2部分の構造が決定されることが市村文男氏により示されていた。一方、残りの場合にも前半の調査から具体的な構造が決定されることが期待されたが、市村氏との共同研究によりこの場合にはさらに類数の2部分という数論的な量からイデアル類群の2部分の構造が決定されることが理論的に示された。後半の調査では、5000万以下の素数 $p$ に対して有理数体上4次以上となる虚アーベル体の類数の2部分を求め、イデアル類群の2部分の構造ごとの分布表を作成した。特にこの範囲では、16ランクが正となる素数は唯一であることが分かった。この結果は、[2]において公表している。

また、上記の調査に引き続き $l$ を素数として $8pl$ 円分体に含まれる有理数体上2べき次の虚アーベル体に対する計算機による調査を行った。大半の場合にはアーベル体の二つの基本的な量からイデアル類群の2部分の構造が決定されるが、 $l$ と $p$ によって変化する構造と $p$ によって変化する構造が数値計算から予測されたが、理論的にこの現象について説明することができた。さらにこの現象に関連して、10億以下の素数 $p$ に対し条件を満たす $8p$ 円分体に含まれた32次の虚アーベル体の類数の2部分を求め、4ランクが16となる素数は6個、8ランクが正となる素数は4個あることが分かった。これらの結果は、[3]において公表している。

さらに、上記の調査に関連して、 $p$ 円分体に含まれる二次体上の素数 $l$ べき次の虚アーベル体のイデアル類群の $l$ 部分についての計算機による調査を100万以下の素数 $p$ に対して行い、3以上101以下の素数 $l$ に関する実例を表にまとめた。ここでは、 $l=3$ の場合に市村文男氏によって定義された岩澤不変量に類似した不変量についても与えており、 $\mu$ 不変量に対応する量は0、 $\lambda$ 不変量に対応する量については1~6の範囲、 $\nu$ 不変量に対応する量には-2~5の範囲であり、特に負となる $\nu$ 不変量の実例が興味深いと考えられる。これらの結果は、[4]において公表している。

$4p$ 円分体の一般Greenberg予想について、プログラムを改良した上で $p$ 単数群のペアリングを計算することにより、4を法として3と合同となる65536以下の素数について3つの例外的な素数を除いて確認することができた。特に $p$ 単数群のペアリングにおける非自明な零の個数は均等性を基にする予測された分布にほぼ近似していることを引き続き確認しており、これは一般Greenberg予想の成立を支持する理由のひとつとなる。

## 参考文献

- [1] H. Sumida-Takahashi. A Generalized Problem Associated to the Kummer-Vandiver Conjecture (online). *Arnold Math. J.*, 2022.
- [2] H. Ichimura and H. Sumida. On the Class Group of an Imaginary Cyclic Field of Conductor  $8p$  and 2-power Degree. *Tokyo J. Math.*, Vol. 44, pp. 157–173, 2021.
- [3] H. Ichimura and H. Sumida. On the class groups of certain imaginary cyclic fields of 2-power degree. *J. Math. Soc. Japan*, Vol. 74, pp. 945–972, 2022.
- [4] H. Sumida-Takahashi, N. Furuya, and K. Kitano. On the  $l$ -part of the Class Groups of Imaginary Cyclic Fields of Conductor  $p$  and Degree  $2l^n$ . *J. Math., Tokushima Univ.*, Vol. 56, pp. 1–10, 2022.

## 5. 主な発表論文等

〔雑誌論文〕 計4件（うち査読付論文 3件/うち国際共著 0件/うちオープンアクセス 2件）

1. 著者名 ICHIMURA Humio, SUMIDA-TAKAHASHI Hiroki	4. 巻 44
2. 論文標題 On the Class Group of an Imaginary Cyclic Field of Conductor $8p$ and $2$ -power Degree	5. 発行年 2021年
3. 雑誌名 Tokyo Journal of Mathematics	6. 最初と最後の頁 157-173
掲載論文のDOI（デジタルオブジェクト識別子） 10.3836/tjm/1502179326	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

1. 著者名 ICHIMURA Humio, SUMIDA-TAKAHASHI Hiroki	4. 巻 74
2. 論文標題 On the class groups of certain imaginary cyclic fields of $2$ -power degree	5. 発行年 2022年
3. 雑誌名 Journal of the Mathematical Society of Japan	6. 最初と最後の頁 945-972
掲載論文のDOI（デジタルオブジェクト識別子） 10.2969/jmsj/86438643	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 -

1. 著者名 SUMIDA-TAKAHASHI Hiroki	4. 巻 -
2. 論文標題 A Generalized Problem Associated to the Kummer-Vandiver Conjecture	5. 発行年 2022年
3. 雑誌名 Arnold Mathematical Journal	6. 最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s40598-022-00220-3	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

1. 著者名 SUMIDA-TAKAHASHI Hiroki, FURUYA Naoki, KITANO Kodai	4. 巻 56
2. 論文標題 On the $l$ -part of the Class Groups of Imaginary Cyclic Fields of Conductor $p$ and Degree $2l^n$	5. 発行年 2022年
3. 雑誌名 Journal of Mathematics, Tokushima University	6. 最初と最後の頁 1-10
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 -

〔学会発表〕 計2件（うち招待講演 0件 / うち国際学会 0件）

1. 発表者名 高橋浩樹
2. 発表標題 ある種の 2 ベキ巡回拡大体のイデアル類群について
3. 学会等名 早稲田整数論セミナー
4. 発表年 2021年

1. 発表者名 高橋浩樹
2. 発表標題 ゼータ値と円分体
3. 学会等名 岐阜数理科学セミナー
4. 発表年 2018年

〔図書〕 計0件

〔産業財産権〕

〔その他〕

Exploring the Galois Universe <a href="https://math0.pm.tokushima-u.ac.jp/~hiroki/major/galois1-e.html">https://math0.pm.tokushima-u.ac.jp/~hiroki/major/galois1-e.html</a>
--

6. 研究組織	氏名 (ローマ字氏名) (研究者番号)	所属研究機関・部局・職 (機関番号)	備考
---------	---------------------------	-----------------------	----

7. 科研費を使用して開催した国際研究集会

〔国際研究集会〕 計0件

8 . 本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関
---------	---------