

2021年度共同利用研究報告書

2022年3月1日

所属・職名 九州大学マス・フォア・インダストリ研究所・助教

浦本 武雄

		整理番号	20210006	
1. 研究計画題目	代数的言語理論と類体論の新しい接点の追求			
2. 新規・継続	新規			
3. 種別	若手研究			
4. 種目	短期共同研究			
5. 研究代表者	氏名	浦本 武雄		
	所属 部局名	九州大学マス・フォア・インダストリ研究所	職名	助教
6. 研究実施期間	2021年08月09日(月曜日)～2021年08月13日(金曜日)			
	2022年01月27日(木曜日)～2022年01月29日(土曜日)			
7. キーワード	代数的言語理論, 類体論, semigalois圏, モジュラー関数, Witt vector, integrality, 決定可能性			
8. 参加者人数	22人			

9. 本研究で得られた成果の概要

本共同研究は、研究代表者による近年の結果が元となっている。特に代表者は、代数的言語理論と古典（明示的）類体論の関連を追求する仕事の中で、虚二次体上の代数的witt vectorが、Fricke関数族の特殊値によって得られるベクトルが生成するものと一致することを証明した。この結果は一般にはどのようなものか定義からわかりづらい代数的witt vectorの記号表現を与えるものであり、計算機での実験に適したものとなっていた。

この背景のもとで、石塚氏との本共同研究では、類数1の虚二次体上の代数的Witt vectorのintegralityの決定可能性を証明し、国際ワークショップSCSS2021のshort paperとしてまとめ提出した。また公開日の講演会で富山大学の木村巖氏に計算機数論と類体論に関するご講演をしていただき、それをきっかけとして、SCSS2021でまとめた共同研究の発展版を木村氏を迎えて準備している。また2022年1月に九州大学で研究に係る議論・ミーティングを行うことを予定している。

現時点までに、SCSS2021で仮定した類数1の条件を外す方法を見つけたため、結果として、全ての虚二次体上の代数的witt vectorのintegralityは決定可能であることを証明できている。これに伴い、関連するある決定問題・構成問題も原理的には解決できる見通しである。

ただし計算機での実装はまだ準備中であり、現在も、石塚氏、木村氏と共同で本研究を進めている。SCSS2021のshort paperの拡張版にあたる論文には、可能な範囲で、計算機実験の結果も盛り込むことを予定している。

IMI 共同利用研究 成果報告書

0. 基本情報：

整理番号：20210006

種別：若手研究-短期共同研究

研究課題名：代数的言語理論と古典類体論の新しい接点の追求

研究代表者：浦本武雄（九州大学 IMI）

研究期間：2021年8月9日～2021年8月13日，

2022年1月27日～2022年1月29日

組織委員：石塚裕大（九州大学 IMI），浦本武雄（九州大学 IMI）

招待講演者：木村巖（富山大学）

アドバイザー：阿部拓郎（九州大学 IMI）

1. 概要：

本共同研究では、代表者の近年の結果に基づき、本共同研究組織委員である石塚氏と共同で類数1の虚二次体上の代数的 Witt vector の integrality の決定可能性を証明した。本結果は国際シンポジウムである Symbolic Computation in Software Science 2021 (SCSS 2021) で発表され、short paper としてすでに出版されている。

本共同研究公開日2021年8月10日の講演会では、富山大学の木村巖氏に招待講演をしていただき、本研究の計算機実装にかかる技術的助言をいただいた。そのため、本共同研究に木村氏も参加していただくこととなり、現在、SCSS2021の結果の拡張および計算機実験に関する研究を石塚氏、木村氏、浦本で進めている。特に2022年1月に、共同研究に係る議論・ミーティングを行った。

公開日からその後、現時点までの研究ですでに、SCSS 2021のshort paperで仮定した類数1の仮定を外せること（任意の虚二次体上の代数的 Witt vector の integrality が決定可能であること）の証明ができたため、関連する決定問題・構成問題に関して計算機実験を行い、石塚氏、木村氏、浦本の共著論文としてそれらの結果をまとめてジャーナルへ提出することを予定している。2022年1月のミーティングの機会に拡張論文のプレプリントを作成した。また計算機実装についても様々な課題が見えてきた。

2. 背景：

本共同研究の背景は、代表者による以下の論文にある。端的に言えばこの一連の論文で代表者は、形式言語理論における一分野である代数的言語理論（或いは Eilenberg 理論）と、整数論の文脈に属すガロア理論・類体論との興味深い関連を観察した。本共同研究で得られた上述の結果（SCSS2021）は、特に論文[3]の結果に基づく（7. 参考文献も参照）：

[1] Takeo Uramoto, Semi-galois Categories I: The Classical Eilenberg Variety Theory, In Proceedings of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science (LICS'16), pp.545--554, 2016.

[2] Takeo Uramoto, Semi-galois Categories II: An arithmetic analogue of Christol's theorem, Journal of Algebra, 508(2018):539--568, 2018.

[3] Takeo Uramoto, Semi-galois Categories III: Witt vectors by deformations of modular functions, arXiv:2007.13367v7.

論文[1]の主題である代数的言語理論は形式言語理論における一分野であり、歴史的には1960年代から発展してきた。特に代数的言語理論は、正規言語 L の組合せ論的・数理論理的決定問題を、対応して得られる有限モノイド $M(L)$ (syntactic monoid) の純半群論的性質に帰着させることで解決する方法論を特色とする。この方法論はガロア理論において、代数的数の性質（四則演算と冪根で表されるか否か等）を、対応して得られる有限群（ガロア群）の純群論的性質（可解性など）に帰着させる方法論と似ている。論文[1]では、semi-galois 圏と呼ばれる圏のクラスを導入し、副有限モノイドとの双対定理を証明することで、代数的言語理論とガロア理論の類似を正当化した。これは古典的な（体や被覆空間等の）ガロア理論が galois 圏と副有限群の双対定理により公理的に統一できたこととの自然なモノイド拡張である。

代数的言語理論とガロア理論のこの統一は、それぞれが全く異なる文脈に属す理論であったため、それ自体でも興味深いとは言える。しかしより重要なことは、この両理論の統一が、それぞれ形式言語理論および整数論に対してどのような意味があるかを明らかにすることにあると代表者は考えている。この問題意識の元で論文[2]では、semigalois 圏の枠組みと類体論の関連を議論した。技術的には、特に Borger [4]によって導入された一般化 Witt vector に対する Christol 型の定理を示し、その結果を Borger と de Smit [5]による明示的類体論の新しい枠組みと関連づけている。そしてそれに続く論文[3]では、論文[2]で得られた観察を進めるため、虚二次体上の代数的 Witt vector に対する modularity theorem（虚二次体上の代数的 Witt vector は、modular 関数の変形族、特に Fricke 関数族の特殊値で作られる modular vector により生成されること）を証明した。

これらの論文[2,3]において代表者は、論文[1]で公理的に発展させた semi-galois 圏と副有限モノイドの双対定理の枠組みが、古典的（明示的）類体論の諸概念（Witt vector, modular 関数、特に Fricke 関数族の特殊値）の間の新しい秩序を開示するのに極めて自然な役割を果たすことを見出した。中でも論文[3]で与えた証明（特に modularity theorem の主張をより強くするために最後の section で新しく追加証明した結果）は、semigalois 圏と副有限モノイドの双対定理の抽象的枠組み[1]を初めて本質的に応用したものと言える（ガロア理論のモノイド版とでもいふべき議論を含む）。

3. 共同研究の目的：

上記研究は、代数的言語理論と整数論の双方にそれぞれ新しい視点をもたらすものであり、代表者は複数の理論および応用研究の展開を念頭に置いている (cf. 6. 展望). 本共同研究の目的は、その展望の下で、上記論文の観察の技術的内容をさらに発展させることである. 実際、[1,2,3]の観察は (特に理論研究の立場では)、代数的言語理論と古典類体論・ガロア理論の間に興味深い関連性 (両理論の諸概念の間にある新しい調和) があることを例示しており、証明での感触としては、この現象は表向き以上に深いルーツを持ち、計算理論・整数論双方の観点からまだ発展性があると代表者は考えている.

整数論の立場では、上記結果[2,3]は古典類体論に新しい視点を与えており、その自然な発展形を通して、非可換類体論の新しい定式化に繋がる可能性がある. また代数体に限らず、より一般の scheme に対しても有限 étale 被覆のなす Galois 圏があることを鑑みれば、上記観察[2,3]の自然な変種として代数幾何学由来の新しい問題群の創出を期待することは不自然ではない. (実際、現時点まで既に[2,3]の結果の少なくない部分の類似が、例えば有限体上の関数体の場合にも成立することを代表者は観察している.) 一般にガロア変形理論とも呼ぶべき理論になるかもしれない. 計算理論の立場では、まず上記結果は古典的な代数的言語理論に整数論由来の新しい問題群をもたらす. それ以上に、計算理論的な対象 (有限オートマトン) と数論幾何的な対象 (Λ 環) の間に (圏同値の意味で) 自然な対応があるという現象は、古典的な計算理論の対象に対して新しい幾何学的な意味づけを与え、古典的な計算理論に新しい視座を与える可能性がある.

本研究課題は上記の性質上、上手くいけば長期的には、個人的な研究観察である以上に自律した研究領域になることが見込まれる. 実際、一連の観察[1,2,3]の長期目標は、形式言語理論・計算理論および整数論・代数幾何学にまたがる一定の問題群の創出にある. これは代表者が数学基礎論や計算理論 (の新しい意味づけの) 研究の一環として[1,2,3]を発展させていることとも関わる. 本共同研究の目標は、この観点のもとで論文[2,3]に係る問題に取り組み、これまでの観察[1,2,3]で得た知見をさらに拡充することであった. この共同研究によってどのような展望・産業への波及効果を念頭に置いているかは、6. 展望でまとめる.

4. 研究成果：

本共同研究に際し、虚二次体上の代数的 Witt vector の integrality の決定可能性を石塚氏と共同で研究し、類数 1 の場合に解決した. その結果は、溝口佳寛氏 (九州大学) の紹介で、国際シンポジウム Symbolic Computation in Software Science 2021 (SCSS 2021) で発表することとなり、SCSS 2021 の short paper として既にオンラインで出版されている. 以下にその short paper が収録されている：

[6] Yasuhiro Ishitsuka and Takeo Uramoto, On the integrality of algebraic Witt vectors over

imaginary quadratic fields, 9th International Symposium on Symbolic Computation in Software Science (SCSS 2021), short and work-in-progress papers, pp.28--33.

https://www3.risc.jku.at/publications/download/risc_6359/21-16.pdf

上記論文では、虚二次体 K の類数が 1 である時に、与えられた代数的 Witt vector が integral であるか否かが決定可能であることを証明し、そのアルゴリズムの概略を与えている。論文 [3] で示したとおり、虚二次体上の代数的 Witt vector は、Fricke 関数族から得られる modular vector の K 係数多項式で表示できる。SCSS 2021 の上記論文では、その K 係数多項式表示が、代数的 Witt vector にかかる決定問題 (integrality) の計算機処理に利用可能である旨を強調している。

整 Witt vector はアприオリには代数的整数を成分に持つ vector であり、(数論的な意味での) 無限回の微分可能性によって定義される。そのため与えられた代数的 Witt vector が整 (integral) かどうかは、その定義通りには (modular vector による解析的表示から) 直ちには確かめられない。

この決定問題に係る技術的な障害は大きく分けて二つある。一つは Fricke 関数の特殊値が整数であるかどうかを、その近似値だけから判定しなければならないこと；もう一つは、各成分が整数であっても、それが数論的微分に関して無限回微分可能であることを有限回のステップで判定しなければならないことである。SCSS 2021 の論文ではまず Fricke 関数の特殊値の整数性を division polynomial を使って判定できることを議論し、それに基づき、整数列の (数論的) 無限回微分可能性を (簡単な単因子論を使って) 有限回微分可能性判定に帰着させることで解決した。

この結果は論文 [3] で示した modularity theorem (代数的 Witt vector のなす K 代数の modular vector による表示) の integral 版を証明することを目指したものであり、論文 [3] に続く研究として自然なものであると考えている。ただし SCSS2021 の論文では integrality の「決定可能性」を証明したのみであり、理想としては整 Witt vector の明示的な特徴づけを与えることが望ましい。実際、論文 [3] で議論しているとおり、 K が有理数体である場合には、整 Witt vector の特徴づけが既にある (これは実質的に Borger と de Smit による結果である)。SCSS 2021 論文の上記成果は、虚二次体の場合の整 Witt vector の特徴づけのための (合理的な) ステップとなることが期待される。またそれだけでなく SCSS2021 論文の最後で言及している通り、代数的オートマトン理論と数値計算の間に関連を付けられたことは、特に計算論的な立場からも注視するに値すると考えている。

5. 研究状況:

本共同研究の公開日 (2021 年 8 月 10 日) に講演会をオンラインで開催した。特に富山大学の木村巖氏をお呼びし、計算機数論に関する講演をしていただいた。その際に上記 SCSS2021 で発表した結果に関する技術的助言をいただいたため、木村氏にも本共同研究に

加わっていただくこととなった。現在、石塚氏、木村氏、浦本の三者で上記 SCSS 2021 論文の拡張版を準備している。共同研究のために slack で情報を共有し、SCSS 2021 の論文にかかる理論的結果の拡張および計算機実験の準備を進めている。そして可能であれば、その実験結果を元に、上述した整 Witt vector の明示的な特徴づけを予想し証明することを目指している。

その後の研究で、SCSS2021 の論文で仮定していた類数 1 の条件を外す方法が分かった。従って現時点では、任意の虚二次体上の代数的 Witt vector の integrality は決定可能であることがわかっている。

類数 1 の場合には、各素 ideal が principal であるため、数論的微分を明示的に計算することができる。SCSS2021 の論文で与えたアルゴリズムは、この明示的計算に依存したものであるため、principal ではない素 ideal が存在する場合（つまり類数が 1 でない場合）には適用できない。しかし SCSS2021 論文の concluding remarks でも既に言及していたとおり、Witt vector 関手は局所化に対して良い振る舞いをする。SCSS2021 論文の後に与えた一般の類数の場合のアルゴリズムではこの事実に基づき、局所化を通して（局所的に素 ideal を principal にすることで）、SCSS2021 論文と同様のプロセスを実行する。

ただし類数 1 の場合に SCSS2021 論文で与えたアルゴリズムと、一般の場合に機能するアルゴリズムは少しだけ異なる。（簡略化できる部分と複雑になる部分が存在する。これは一般のアルゴリズムは局所化をとる操作で、類数 1 の場合にはなかった評価が必要になることと関係している。）そのため類数 1 の場合にはどちらのアルゴリズムがより効率的かという問題が生じるが、現時点では計算効率についてはまだほとんど何もわかっていない。SCSS2021 論文で与えているアルゴリズムも新しく得た一般の場合のアルゴリズムも、どちらもあくまで理論的なものであり計算量的には効率が良いようには見えない。そのため本共同研究では今後、アルゴリズムの改善も課題となってくる可能性がある。実際、既に上述した公開日で木村氏も指摘しておられた通り、Fricke 関数や j 関数の特殊値の（十分な精度の近似値の）計算は、非常に複雑になりうるようである。Fricke 関数族と同様の（虚二次体のアーベル拡大を生成する）働きをする別の関数族はその計算量の問題が緩和されるようであったが、その関数族を Fricke 関数族の代わりに用いて（代数的 Witt vector の integrality を決定する）アルゴリズムを実装するには、勿論、その関数族に対する modularity theorem の変種（代数的 Witt vector の別の計算機的表示）を証明する必要がある。現時点ではこの変種の証明が可能かは、理論的にもまだ何もわかっていない。それは今後の研究課題とする。

特に 2022 年 1 月 27 日から 29 日の日程で、石塚氏・木村氏・代表者で研究に係る議論・ミーティングを行い、計算機実装の準備を進めた。またこの機会にジャーナル版の論文のプレプリントを準備することができたが、共同研究として一定の期限を設けたことが、本研究を加速させるのに役立った。

6. 展望

現時点で応用への波及効果・実効性を見通すことは難しいが、本研究で代表者は複数の応用研究の方向性を念頭においている。

その中でも産業的に重要なものは、計算複雑性理論への基礎的貢献である。上述したとおり本研究の大元にある代数的言語理論は、正規言語と呼ばれる階層の計算論的・論理的複雑性階層の体系的分類を与える理論として歴史的にも顕著なものであり、代表者の研究を含めて近年、この理論を正規言語以上の階層に展開しようとする潮流がある。計算複雑性階層の分類は P 対 NP 問題が未解決であることから見て取れる通り、一般には難しい問題であり、また ad hoc な手法に依存することが多い。一方、計算複雑性階層の分類は、暗号の安全性保証など実学的応用の理論的基盤になる課題であるため、より高階の計算・言語複雑性階層に対しても上述した代数的言語理論の体系的な方法論の拡張を試みることに産業的な意義がある。

本研究は正規言語階層に対応する分類理論と整数論との融合研究であり、高階の言語階層への展開そのものを課題としてはいないが、本研究で正規言語階層に対応する分類理論の基礎がさらに固められれば、より高階の言語階層の分類理論を展開する際にも重要な参考材料になるだろうと考えている。特に本研究では、数論（幾何学）のアイデアと有限オートマトン理論のアイデアとの融合を通して、古典的な計算モデルに対しより幾何学的な意味づけを与えることを意識している。

7. 参考文献：

[1] Takeo Uramoto, Semi-galois Categories I: The Classical Eilenberg Variety Theory, In Proceedings of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science (LICS'16), pp.545--554, 2016.

[2] Takeo Uramoto, Semi-galois Categories II: An arithmetic analogue of Christol's theorem, Journal of Algebra, 508(2018):539--568, 2018.

[3] Takeo Uramoto, Semi-galois Categories III: Witt vectors by deformations of modular functions, arXiv:2007.13367v7.

[4] James Borger, The basic geometry of Witt vectors I, the affine case. Algebra and Number Theory, 5(2):231--285, 2011.

[5] James Borger and Bart de Smit, Lambda actions of rings of integers, arXiv:1105.4662.

[6] Yasuhiro Ishitsuka and Takeo Uramoto, On the integrality of algebraic Witt vectors over

imaginary quadratic fields, 9th International Symposium on Symbolic Computation in Software Science (SCSS 2021), short and work-in-progress papers, pp.28--33, 2021.

九州大学 IMI 共同利用・短期共同研究 公開講演会

代数的言語理論と古典類体論の新しい接点の追求

New interplays between algebraic language theory and classical class field theory

日時：2021年8月10日（火）13：30～17：40

場所：Zoom ミーティングによるオンライン開催

代表者：浦本 武雄（九州大学マス・フォア・インダストリ研究所）



8月10日（火）

13：30-13：40 本共同研究について

13：45-14：40

講演者：浦本 武雄（九州大学 IMI 助教）

講演タイトル：代数的言語理論の背景

14：45-15：40

講演者：石塚 裕大（九州大学 IMI 助教）

講演タイトル：楕円曲線と代数的整数論の基礎事項

15：45-16：40

講演者：浦本 武雄（九州大学 IMI 助教）

講演タイトル：代数的 witt vector とその関連問題

16：45-17：40

招待講演者：木村 巖（富山大学学術研究部理学系 准教授）

講演タイトル：類体の構成問題と計算機数論

※研究実施期間：2021年8月9日（月）～8月13日（金）

※公開日：2021年8月10日（火）のみ