様式 C-19

科学研究費補助金研究成果報告書

平成２１年３月３１日現在

研究種目：基盤研究（C）
研究期間：2007～2008
課題番号：19540051
研究課題名（和文）　正標数における非特異代数曲線巡回拡大の標数零への引き上げ問題について
研究課題名（英文）　On the lifting problem of cyclic coverings of non-singular curves in characteristic P to them in characteristic 0.

研究代表者
関口　力（SEKIGUCHI TSUTOMU）
中央大学・理工学部・教授
研究者番号：70055234

研究成果の概要: 正標数における代数曲線の巡回拡大の標数零へのいわゆる引き上げ問題を解決するために群スキームの変形理論を構築してきたが、この変形群スキームを用いて、新しいタイプの有限群スキームの Cartier 双対を具体的に与えることができ、また、変形群スキームの拡大群について、新しい知見を得た。また、代数曲線の Picard 群における加算アルゴリズムを Cantor アルゴリズムの拡張を行うことにより、Gröbner 基底を用いるものより高速なものを与えた。

交付額

（金額単位：円）

	直接経費	間接経費	合　計
２００７年度	700,000	210,000	910,000
２００８年度	500,000	150,000	650,000
年度			
年度			
年度			
総　計	1,200,000	360,000	1,560,000

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：　群スキーム、引き上げ問題、代数曲線被覆、巡回拡大、変形群スキーム

１．研究開始当初の背景

正標数 p における代数曲線の巡回被覆の、標数零への引き上げ問題は、次数が p のとき Oort-Sekiguchi-Suwa, “On the deformation of Artin-Schreier to Kummer”, Annales scientifiques de l'Ecole Normale Superieure, 4 serie, 22(1989), 345--375 により 1989 年に解決し、後に Green-Matignon, “Liftings of Galois covers of smooth curves” Compositio Math. 113, 239-271, 1998 により 1998 年に p^2 時の場合に肯定的に解決している。我々の手法は、Artin-Schreier 理論を Kummer 理論へ変形すること行い、Lang の類体論を変形するものであった。その後、その際に確立した Kummer-Artin-Schreier 理論を一般の Kummer-Artin=Schreier-Witt 理論として拡張する研究を行い、加法群スキームの乗法群への変形理論を構築し、そうした変形群スキームの拡大群を計算することにより、Witt ベクトルのなす群スキームのトーラスへの変形群スキームの構成について研究を行ってきている。尚、Kummer-Artin-Schreier 理論については、我々とは独立に

Waterhouse-Weisfeiler が
”One-dimensional affine group schemes”, J. of Alg., Vol.66, 1980, 550-568 によって与えている。Green-Matignon による手法は、Rigid 幾何学を用いることにより、局所的な引き上げ問題の解決に帰着し、２次元の場合の我々の研究結果である關口・諏訪“A note on extensions of algebraic and formal groups III”, Tohoku J. of Math., 49(1997), 241-257, “A note on extensions of algebraic and formal groups IV”, Tohoku Math. J. 53(2001), 203-240 により開発された群スキームの理論を用い、２次元の場合の Kummer-Artin-Schreier-Witt 理論を具体的に構築することにより解決しているものである。

一般の p^n 次巡回拡大を扱うためには、こうした理論を一般的に展開する必要がある。これについては、上記を含む關口・諏訪の一連の仕事を統括した形で、“On the unified Kummer-Artin-Schreier-Witt theory”, Mathematiques Pures de Bordeaux C.N.R.S., Prëpublication no.111(1999), 1-90 に与えている。

Kummer-Artin-Schreier-Witt 理論は不分岐巡回拡大を記述するものであり、一般の巡回拡大を記述するためには、こうした変形理論のコンパクト化を行う必要がある。こうした群スキームのコンパクト化については、正標数の場合に M. Garuti , “Linear systems attched to cyclic inertia”, Proceedings of Symposia in Pure Mathematics 70, 377-386, 2002 によって、Witt ベクトルのなす群スキームのコンパクト化を与え、その境界を用いて、幾何学的に Artin-Rees wild ramification 表現を与えている。 従って、Witt ベクトルのなる群スキームの変形を与え、Artin-Schreier-Witt 完全系列から Kummer 完全系列への変形に関する我々の理論と合わせて、Garuti によるコンパクト化の変形が議論されるべき状態にあるものと考えられる。

また、変形群スキーム理論において、様々な新しい群スキームの例が構成され、こうした群スキームを研究することは、Tate-Oort, “Group schemes of prime order”, Ann. Scient. Ec, Norm. sup., 4 serie, t.3, (1970), 1-31 において、素数位数の有限群スキームを分類しているが、更に高次の有限群スキームについて、新たな例を供給し、新しい世界を切り開くことが可能であると考えている。

Kummer-Artin-Schreier-Witt 理論の構成では、変形群スキームの拡大群を計算することにより理論構成を行ったが、こうした群スキームの拡大群については他にも様々な組み合わせによる拡大群が考えられ、こうした拡大群の計算を与えることは、理論体系を完成させる上で重要なことと考えており、我々の手法による守備範囲で解決できるものと見ている。

一般代数曲線の Picard 群に関する研究であるが、当初は Lang の類体論の変形を考察する上で、特異曲線の Picard 群について研究を行っていた。後に、暗号理論への応用を考え、特異代数曲線を用いることによるアルゴリズムの改良に思い至った。その目的のためには、代数曲線のコンピュータに認識させうる表現方法を確立しなければならない。幸いなことに、一般代数曲線の究極のアファイン代数曲線としての表現が、三浦晋示氏により三浦理論として “The linear code on affine algebraic curves”, in Japanese, Shingakuron(A), vol.J81-A(1998), no.10, 1396-1421 において与えられている。この表現の特にその平面表現を用いることによって、 Picard 群における加算アルゴリズムの高速化の可能性に至った。その結果の一部は Miura-Sekiguchi, “An addition algorithm on the Jacobian varieties of curves”, J. Ramanujan Math. Soc. 19, no.4(2004), 235-251 に発表している。

２．研究の目的

正標数における非特異代数曲線のガロワ巡回拡大を標数零に引き上げることが、当該研究の最終目的である。

この問題解決に当たり、Artin-Schreier-Witt 理論から Kummer 理論への変形理論を構成する必要がある。Kummer 理論は乗法群により記述され、Artin-Schreier-Witt 理論は Witt ベクトルのなす群スキームにより記述されている。従って、我々の目的のためには Witt ベクトルのなす群スキームからトーラスへの変形群スキーム理論を構成しなければならない。こうした変形群スキームについては、上記一連の研究により、一応の変形群スキーム理論を構築している。その際に、変形群スキームの拡大群の計算方法を開発に、必要最小限の拡大群についてその決定を行っている。こうした群スキーム理論を完成させるためには他の様々な拡大群の計算を行う必要があり、こうした拡大群の計算を行うことが一つの目的である。

変形群スキーム理論においては、新たな群スキームの具体例や興味深い有限群スキームの具体例を包含している。こうした変形群スキームを用いて、新しい有限群スキームについて、そのトーサーの決定、Cartier 双対の決定を行うことが目標の二つ目である。

引き上げ問題について、

Kummer-Artin=Schreier=Witt 理論は不分岐巡回拡大を記述するものであり、一般の

巡回拡大を記述するためには、分岐を取り扱える理論を作らなければならない。正標数における巡回拡大は wild ramification を持っており、従って、その wild ramification を記述する Artin-Rees 理論の票数零への変形理論とならなければならない。そうした分岐を扱うために、変形群スキームのコンパクト化を考えることは自然であり、正標数の場合に、Garuti が与えているコンパクト化を如何に変形して、変形群スキームのコンパクト化を行うかを研究することが最も重要な課題と考えている。

更に、一般代数曲線の Picard 群スキームにおける加算アルゴリズムについて、Miura-Sekiguchi. “An addition algorithm on the Jacobian varieties of curves”, J. Ramanujan Math. Soc. 19, no.4(2004), 235-251 によって、三浦理論による特異点を許して平面代数曲線表現を用いた、一般代数曲線の Picard 群加算アルゴリズムを提案している。更に、この結果を引き継ぎ、Cantor, “Computing in the Jacobian of a hyperelliptic curve”, Mathemtics of Computation, 48, 177(1987), 95-101 によるアルゴリズムを一般の代数曲線の Picard 群へ拡張すること目指し、一般代数曲線 Picard 群でのペアリングのアルゴリズムを与えることを目的としている。

また、最近暗号理論において公開鍵暗号にアーベル多様隊のペアリング利用が盛んに研究されているが、こうした研究は抽象的な数学が使われており、暗号理論の研究者にはそおうした数学の吸収に多大の努力を櫃世とする事態になってきている。こうした事態を少しでも緩和するために、代数幾何学を勉学するための指針となる書と、ペアリングに関する体系的な書が必要であろう。このような目的のために、代数幾何学の一般論の指針、代数曲線のコンピュータによる利用に耐える表現法、代数曲線の Picard 群における加算アルゴリズムとペアリング表現をまとめた書をまとめることを更なる目的の一つとしている。

３．研究の方法

1998 年、Oort-Sekiguchi-Suwa, “On the deformation of Artin-Schreier to Kummer”, Annales scientifiques de l’Ecole Normale Superieure, 4 serie, 22(1989), 345-375 によって、正標数 p における代数曲線の p 次巡回拡大の標数零への引き上げ問題を解決し、その際、用いた手法を本質部分は、Artin-Schreier-Witt 理論の Kummer 理論への変形理論として研究を継続している。すなわち、上部で述べたように、加法群からなる Artin-Schreier 完全系列から乗法群からなる Kummer 完全系列への変形完全系列理論への変形理論を構築し、それを一般化し，高次元化した Kummer-Artin-Schreier-Witt 完全系列を構築するものである。一方、Green-Matignon, “Liftings of Galois covers of smooth curves”, Compositio Math。, 113, 239-271、 1998 により p^2 次の引き上げ問題が、rigid 幾何学による局所化と、我々關口・諏訪が構築してきた理論の２次元の場合の結果を用いて解決している。従って、一般の引き上げ問題の解決のためには、統一 Kummer-Artin-Schreier-Witt 理論を完全に把握する必要があるが、これについては、關口・諏訪 “On the unified Kummer-Artin-Schreier-Witt theory”, Mathematiques Pure de Bordeaux C.N.R.S., Prepublication no. 111(1999) によって一応の完成をみている。また、Artin-Schreier-Witt 理論のコンパクト化は、Garuti, “Linear systems attched to cyclic inertia”, Proceedings of Symposia in Pure Mathematics 70, 377-386, 2002 によって与えられている。従って、關口・諏訪理論の充実を図り、Garuti のコンパクト化の変形理論を構成することを考え、Green-Matignon の p^2 次の結果を参考に分岐拡大へのこうしたコンパクト化の幾何学的な表現を考察するものである。

変形群スキームの様々な拡大群を計算することは、上記關口・諏訪により、Gronthendieck 位相に基ずく群層の完全列を用いることによる計算方法を与えている。また、大切な手法として、Artin-Hasse べき級数の変形べき級数を与えており、こうした手法道具を旨く組み合わせることにより、更に様々な拡大群を計算するものである。

有限群スキームについては、素数位数群スキームの分類は上記 Oort-Tate により与えているが、合成数位数の有限群スキームについては、その詳しい全容が見えていない。ここでは、我々の開発した変形群スキーム理論を用いて、様々な有限群スキームの具体例を与え、そうした有限群スキームの Cartier 双対を計算するものである。Cartier 双対については、変形群スキーム理論において、上記変形 Artin=Hasse べき級数を用いて、変形群スキームから乗法群への準同型射のなす群の決定を与えており、こうした手法を使うものである。

公開鍵暗号への応用を目指して、一般代数曲線の Picard 群を具体的に記述し、高速な加算アルゴリズムの開発、及びそこにおけるペアリングのアルゴリズム構成を行うことであるが、そのために三浦理論による Cab 曲線表現を用いるものであり、特に、平面表現を用いることによって、高速アルゴリズムを実現するものである。平面表現を用いる場

合、一般には特異点が現れる。我々の提案は、こうした特異点を許容するアルゴリズムを採用し、Cantor の超楕円曲線上の Picard 群加算アルゴリズムを一般化するものである。こうした研究は、代数幾何学の指針と代数曲線の具体的取り扱い方、ペアリング理論をまとめることを考えている。

４．研究成果

關口・諏訪理論において、n 次元変形群スキーム E_n に対し拡大群 $Ext^1(E_n, E_1)$ を決定したが、ここでは更に拡大群 $Ext^1(E_1, E_n)$ の計算を与えた。こうした結果は大学院博士課程の学生に纏めさせている。

n 次元変形群スキーム E_n 間の isogeny を考えることにより、その核として様々な新しい有限群スキームの具体例を与えることが分かってきている。こうした変形群スキームの部分有限群スキームについて、準同型射のなす群及び拡大群の計算結果を組み合わせることにより、具体的な Cartier 双対について、新しい知見を得ている。これはやはり大学院博士課程の学生に成果の取り纏めを行わせている。

Bordeaux プレプリントの正式な論文化は、２００９年度に行う予定である。

変形群スキームのコンパクト化については、Garuti の結果と Neron blow-up の組み合わせを考えており、Green-Matignon の２次元における結果と合わせて、検討している段階であり、現実的な成果は、これからの仕事である。

一般代数曲線の Picard 群における加算アルゴリズムへの Cantor アルゴリズムの一般化については、平面 Cab 曲線を用いて、その座標環のイデアル類群として Picard 群を表し、２次元座標の記述を用いてアルゴリズムの構成に至っており、その成果は現在プレプリント　關口・三浦“Geometric Aspects of the addition algorithm on the Picard group of a C_{ab} curve”としてまとめており、雑誌への投稿を準備している。

暗号および数学両分野の研究者の便宜を図り、代数幾何学の概念指針と代数曲線のコンピュータに認識しうる具体的表現法、ペアリングの一般論を本として著述中である。２００９年度中に出版を考えている。

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０件）

〔学会発表〕（計２件）

(1)三浦晋示、<u>關口　力</u>、｛¥sl C_{ab} 曲線の Picard 群への Cantor アルゴリズムの拡張について｝、「２００７代数曲線暗号を巡って」ワークショップ、中央大学理工学研究所、２００７年１１月３０日、東京

(2)<u>SEKIGUCHI TSUTOMU</u>, “On the deformations of group schemes of Witt vectors to tori}, Workshop on Arithmetic Geometry and Related Area, Toronto University, Canada, 14--23 March 2007(Gave a lecture on 20 Mar.)

６．研究組織

(1)研究代表者

関口　力（SEKIGUCHI TSUTOMU）

中央大学・理工学部・教授

研究者番号：70055234

(2)研究分担者

なし

(3)連携研究者

なし