様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　(共通)

科学研究費助成事業　　研究成果報告書

平成 ２９ 年　 ５ 月　 ９ 日現在

機関番号：２２６０４
研究種目：挑戦的萌芽研究
研究期間：2013～2016
課題番号：２５６１０００７

研究課題名（和文）楕円曲面上の算術及びアーベル・ヤコビ写像とその応用

研究課題名（英文）Arithmetic and the Abel Jacobi map on elliptic surfaces and their applications

研究代表者
徳永　浩雄（TOKUNAGA, HIROO）

首都大学東京・理工学研究科・教授

研究者番号：３０２１１３９５

交付決定額（研究期間全体）：（直接経費）　　3,000,000円

研究成果の概要（和文）：本課題では楕円曲面Sの生成ファイバーとして現れる楕円曲線に対する有理点の算術およびAbel-Jacobi写像の研究を行った．具体的には有理点の倍元や和から定まるS上の曲線，S上の２重切断およびそのAbel-Jacobi写像の像から定まる曲線の性質を研究し，その成果を平面曲線のtorus分解や，Zariski N組の構成など，平面代数曲線のトポロジーの研究に応用した．具体的な成果は，conic-line arrangmentのZariski ペア，conic arrangements のZariski N組の構成，4次曲線とそのweak contact conicの幾何学の研究である．

研究成果の概要（英文）： We study arithmetic of rational points and Abel-Jacobi map for an elliptic curve appeared as the generic fiber of an elliptic surface S over a projective line. More precisely, we study curves on S given by the sum of two rational points or the duplication of a rational point. We also study bisections on S and curves determined by the bisections.
 As applications, we study quasi torus decompositions of plane curves and Zariski N plet. Precisely, we give examples of Zariski pairs for conic-line arrangements, Zariski N-plets for conic arrangements, and weak contact conics for plane quartic curves.

研究分野：代数学(代数幾何学)

キーワード：楕円曲面　Mordell Weil群　整切断　2重切断　Zariski ペア　contact conic

１．研究開始当初の背景

この研究において，代数多様体は特に断りが無い限り，複素数体 $\mathbb{C}$ 上で定義されたものを扱う．この研究においては非特異射影的代数曲面 S が非特異射影曲線 C 上の楕円曲面であるとは，C への相対極小な全射: φ： S → C で以下の条件を満たすものが存在するときをいう：（イ）φの一般のファイバーは種数 1 の非特異曲線であり，かつ，少なくともひとつのファイバーは種数 1 の非特異曲線ではない，（ロ）φは切断 O をもつ．本課題ではさらに C が射影直線 P^1であり，S が有理曲面であるとき（有理楕円曲面）が対象となっている．

有理楕円曲面φ：S → P^1の生成ファイバーは 1 変数有理函数体 K:=$\mathbb{C}$(t)上の楕円曲線 E_Sとなっている．仮定により，E_Sの K-有理点全体の集合 $E_S(K)$は，O から定まる有理点を含むので空ではなく，可換群(Mordell-Weil 群)の構造が入る．さらに $E_S(K)$はφ: S → P^1の切断全体の集合と同一視できる．本課題では塩田徹治氏による以下の定理が出発点となっている：

定理（塩田） NS(S)は S の Neron-Severi 群（S 上の既約曲線を基底として生成された自由加群の代数的同値による同値類群）とし，T は O, φのファイバーF 及びφのファイバーに含まれる既約曲線で O と交わらないもので生成される部分群とする．このとき，NS(S)/T から $E_S(K)$への自然な同型が存在する．

上記定理の証明は，E_S 上で S 上の因子 D が定義する K 上の因子に対し，アーベル・ヤコビ写像αによる像α(D)を対応させることで証明される．塩田の定理は NS(S), T という**幾何学的に定義される群**と $E_S(K)$という**整数論的な群**を結びつけるものと看做せ，これまで，「幾何から整数論へ」という形で様々な成果が得られている．そこで，本課題ではこの逆，すなわち，**「整数論から幾何へ」**という立場で研究を行うことを目指した．

２．研究の目的

背景で述べた演算（算術）の幾何学については以下のように述べることができる．
$E_S(K)$の元 P, Q に対しては対応する切断の像として S 上の曲線 C_P, C_Qが対応する．さらに，和 R= P+Q には第 3 の曲線 C_Rが対応している．これらの曲線は互いに和という代数的な関係に加えて幾何学的な関係も存在するはずである．この関係を調べ**(目的 1)**，幾何学への応用することを目指す **(目的 2)**．

続いて， $E_S(K)$の元 P に対し，α^{-1}(P)に含まれる元を与えるような S 上の曲線の具体的な構成およびその性質を研究する，すなわち，アーベル・ヤコビ写像の明示的な研究を目的とする．この研究は，目的 1 から派生したものでもあり，生成ファイバーの種数が 2 以上のときの研究に向けた布石でもある．また，これらの具体的計算は複雑になるけれども由緒正しい「アルゴリズム」によっているため，新しいタイプの代数曲面暗号の提案が期待される．これが究極の目標(**目的 3**)である．

３．研究の方法

研究の方法について，基本的な鍵は二つある：

（１） 考えている楕円曲面 S の生成ファイバーE_Sの Weirstrass 方程式が明示的に与えられ，さらに K-有理点 P, Q の座標が明示的に与えられているときは，よく知られた加法公式により，R = P+Q の座標を計算することができる．具体的には E_Sの方程式が

$$y^2 = F(t,x) = x^3 + a(t)x^2 + b(t)x + c(t),$$

a, b, c は t を変数とする多項式でさらに P,Q の座標も t に関する有理式となっている場合，R の座標は明示的に計算できて，(t, x, y) 空間の曲線 C_R を与える．さらに，和の定義を考えれば，P が与えられたとき，α(D) = P をみたす 2 重切断 D も明示的に記述できる．

こうして得られる C_Rや D および C_P, C_Qから定まる曲線の性質を P, Q の算術的な性質を通して調べる．

（２） 本課題で扱う楕円曲面はすべて射影平面 P^2の 2 次被覆として得られている．上記の Weierstrass 方程式に関する記号を用いるとこの被覆写像は(t, x, y) → (t,x)で与えられる．本課題では上記でのべた C_R, C_P, C_Q, D の像及び F(t, x) = 0 で定義される平面曲線 B が本課題の研究対象となる．

以上の鍵となる方法をもとに，考察を行った．具体的には，

(1) R が P の倍元で，P，R ともに座標が t の多項式なるとき，

(2) α(D) = P を与える D の P^2での像が 2 次曲線になるとき，

の具体的な研究進めた．幾何学への応用では Zariski ペアを考察した．その際，埋め込みのトポロジーを区別には Galois 分岐被覆の存在・非存在もしくはそこから生じる不変量を用いている．具体例を構成する最終的な段階では数式処理ソフト(Maple)を用いて確認した．

このようにして得られた種々の成果は論文，学会発表を通して発信した．

４．研究成果

（１）B と C_R, C_P, C_Qで与えられる平面曲線については，①研究代表者個人によるものと，②研究代表者とその大学院生 Khulan

Tumenbayar によるものがある．
①の成果では，論文⑥にある conic-line arrangement の Zariski ペアの例がある．この例は，従来にないもので専門家の注意を引いた．論文⑥では，例の構成だけでなく，以降の研究につながる基本定理も与えている．また関連する学会発表は⑮，⑰，⑱，⑲，⑳である．
②の成果では, 3 つの cusp をもつ４次曲線の quasi (2,3) torus 分解に関する論文③，3 つの node をもつ既約 4 次曲線とその contact conic のトポロジーに関する論文①，がある．この成果に関する学会発表は⑥，⑦，⑧である．

（２）α(D) = P を満たす D と B のトポロジー研究は，主として，坂内真三を共同研究者として推進した．その成果は 4 次曲線とその contact conic からなる Zarisik N 組の研究である．その成果は論文⑤および共著のプレプリント Geometry of bisections of elliptic surfaces and Zariski N-plets II，にまとめた．これらの成果に関する学会発表は①，②，⑤，⑪，⑫，⑬，⑭，⑮，⑯である．

（３）上記の（１)，（２）の研究を進めていく過程において，低次曲線配置のトポロジー研究において新たな着想，**曲線の部分配置を一斉に扱う**，があった．この成果は，B. Guerville-Balle，坂内真三，白根竹人との共同研究で, プレプリント On the topology of arrangements of a cubic and its inflectional tangents にまとめた．このプレプリントで得た着想は（２）で触れたプレプリントにおいても用いられている．なお，この成果に関する学会発表は①，②，③，④である．
（４）研究分担者との取り組み当初計画していた程は進まなかった．ただ，楕円曲線に関するテーマで成果をあげている．なお，分担者の一人の内田とは，種数 2 の曲線のアーベルヤコビ写像の研究を行い，現在論文を準備中である．

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 6 件）

① Khulan Tumenbayar and <u>Hiro-o Tokunaga</u>, Elliptic surfaces and contact conics for a 3-nodal quartic，査読有，Hokkaido Math. J．に掲載予定

② Hiroshi Onuki，Tadanori，Teruya，Naoki Kanayama and <u>Shigenori Uchiyama</u>, The optimal ate pairing over the Barreto-Naehrig curve via parallelizing elliptic nets．査読有 JSIAM Lett. 8 (2016)，9-12.

③ Khulan Tumenbayar and <u>Hiro-o Tokunaga</u>, Integral section of elliptic surfaces and degenerated (2, 3) torus decompositions of a 3-cuspidal quartic,査読有，SUT J. of Math. 51 (2015)，215-226.

④ Akihiko Onishi，<u>Yukihiro Uchida</u>，and <u>Shigenori Uchiyama</u>，A small secret exponent attack on cryptosystems using Dickson polynomials，査読有 JSIAM Lett. 7 (2015).

⑤ Shinzo Bannai and <u>Hiro-o Tokunaga</u>, Geometry of bisections of elliptic surfaces and Zariski N-plets for conic arrangements， 査読有 Geom. Dedicata,178 (2015)，219-237.
DOI 10.1007/s10711-015-0054-z.

⑥ Hiro-o Tokunaga, Zariski pairs for conic-line arrangements via dihedral covers，査読有 J. Math. Soc. of Japan 66(2014)，613-640.

〔学会発表〕（計 20 件）

① <u>徳永浩雄</u>, On the topology of reducible plane curves, Topology of Singularity in Hanoi 2017, 2017 年 2 月 20 日，VIASM Hanoi(Vietnam).

② <u>徳永浩雄</u>, A remark on the topology of reducible cruves,Seminario de Geometria y Topologia, 2016年9月27日, Universidad de Zaragoza,Zaragoza (Spain).

③ <u>徳永浩雄</u>, On the topology of reducible plane curves，2016 年 8 月 1 日，Tsuda College and OIST joint workshop on Calabi-Yau varieties，津田塾大学（東京都小平市).

④ <u>徳永浩雄</u>, A remark on the topology of reducible plane curves，2016 年 7 月 2 日，第 13 回代数曲面ワークショップ at 高知，高知工科大学 永国寺キャンパス(高知県高知市).

⑤ <u>徳永浩雄</u>，Geometry of contact conics, Workshop on Hyperplane Arrangements and Singularity Theory, 2016 年 3 月 23 日,北海道大学（北海道札幌市）.

⑥ <u>徳永浩雄</u>,Integral sections of rational elliptic surfaces and contact conics to

3-nodal quartics，2015年12月12日，Various Aspects of Algebraic Geometry，国際基督教大学(東京都三鷹市).

⑦ 徳永浩雄，Elliptic curves over the rational function field and geometry of plane algebraic curves，2015年11月16日 Colloquium talk at Jacob's University, Bremen (Germany).

⑧ 徳永浩雄，Integral sections of rational elliptic surfaces and contact conics to an irreducible 3-nodal quartic，2015年9月18日，Geometry，Topology and Combinatorics of Hyperplane Arrangements and Related Problems，Universidad de Zaragoza，Zaragaoza(Spain).

⑨ 小貫啓史，照屋唯紀，金山直樹，内山成憲，Elliptic net の並列化による optimal ate paringの計算，2015年9月11日，日本応用数理学会2015年度年会，金沢大学(石川県金沢市).

⑩ 池田崇，内田幸寛，内山成憲，楕円曲線を用いた Multi-Secret Sharing について，2015年9月11日,日本応用数理学会2015年度年会，金沢大学（石川県金沢市).

⑪ 徳永浩雄，Topology of plane curves of low degree via Galois covers and rational elliptic surfaces，2015年3月16日，Arrangements of plane curves and related problems，首都大学東京（東京都八王子市）.

⑫ 徳永浩雄，楕円曲面の bisection について，2015年1月25日，第2回 代数幾何学研究集会-宇部-，宇部工業高等専門学校（山口県宇部市）.

⑬ 徳永浩雄，Conic-line，conic arrangements and rational elliptic surfaces，2014年9月19日,Seminar Komplexe Geometrie,Ruhr Universitaet Bochum，Bochum(Germany).

⑭ 徳永浩雄，Zariski N-plets for arrangements of plane curves of low degree and rational elliptic surfaces，2014年9月1日，The 1st Workshop of JSPS-MAE Sakura Program，北海道大学（北海道札幌市）.

⑮ 徳永浩雄，有理楕円曲面上の section 及び bisection の幾何，2014年5月27日，函館数論幾何ワークショップ，函館中央図書館（北海道函館市).

⑯ 徳永浩雄，Galois covers，bisections of elliptic surfaces and Zariski N-plets for arrangement of curves of low degree,2014年 3月4日， Seminar on topology and singularities，首都大学東京/東京理科大学（東京都八王子市).

⑰ 徳永浩雄，有理楕円曲面とある line -conic arrangements，2013年11月26日，トポロジーセミナー，東京大学(東京都目黒区).

⑱ 徳永浩雄，Geometry of (mulit-) sections of elliptic surfaces and its applications，2013年11月2日，射影多様体の幾何とその周辺，高知大学（高知県高知市).

⑲ 徳永浩雄，Geometry of sections of elliptic surfaces and its application，2013年9月20日，1st Franco-Japanese-Vietnamese Symposium on Singularities，Nice (France).

⑳ 徳永浩雄，Elliptic surfaces and Zariski pairs for conic-line arrangements，2013 年 6 月 29 日，Joint international meeting of American Math. Soc. and Romania Math. Soc，Alba-Iulia (Romania)

〔図書〕（計０件）

〔産業財産権〕

○出願状況（計０件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計０件）

名称：
発明者：

権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等
本課題の関連した研究集会の URL
① http://www.math.sci.hiroshima-u.ac.jp/branched/index2016.html
② http://www.math.sci.hokudai.ac.jp/~yoshinaga/research/conference/201503TMU.html
③ http://www.math.sci.hiroshima-u.ac.jp/branched/index2014.html

6．研究組織
(1)研究代表者
徳永浩雄（TOKUNAGA HIROO）
首都大学東京・理工学研究科・教授
研究者番号：30211395

(2)研究分担者
内山成憲（UCHIYAMA SHIGENORI）
首都大学東京・理工学研究科・教授
研究者番号：40433172

内田幸寛（UCHIDA YUKIHIRO）
首都大学東京・理工学研究科・准教授
研究者番号：90533258

(3)連携研究者
なし
(4)研究協力者
坂内真三（BANNAI SHINZO）
茨城工業高等専門学校・講師
研究者番号：20732556

白根竹人（SHIRANE TAKETO）
宇部工業高等専門学校・准教授
研究者番号：70615161

Benoit Guerville-Balle
東京学芸大学/JSPS PD

Kuhlan Tumenbayar
National University of Mongolia
(研究協力時は首都大学東京大学院生)