Proceedings of

Algebra and Computation 2011

Tokyo Metropolitan University

November 7–9, 2011

Edited by AC2011 Proceedings Committee

Organizers

Ken Nakamula (Tokyo Metropolitan Univ.)

Katsushi Waki (Yamagata Univ.)

Hirofumi Tsumura (Tokyo Metropolitan Univ.)

Shigenori Uchiyama (Tokyo Metropolitan Univ.)

第 9 回「代数学と計算」研究集会 (AC2011)
The 9th Symposium on Algebra and Computation (AC2011)

標記の研究集会を下記の要領で開催いたしますので, ご案内申し上げます.

主催者 Organizers

中村 憲 (首都大学東京) Ken Nakamula (Tokyo Metropolitan University)
脇 克志 (山形大学) Katsushi Waki (Yamagata University)
津村 博文 (首都大学東京) Hirofumi Tsumura (Tokyo Metropolitan University)
内山 成憲 (首都大学東京) Shigenori Uchiyama (Tokyo Metropolitan University)

記

日時 (Date)：2011 年 11 月 7 日 (月) – 9 日 (水)
7(Mon.) – 9(Wed.) November 2011
場所 (Place)：首都大学東京 国際交流会館
Tokyo Metropolitan University International House

[プログラム] Program
Nov. 7（Mon.）

10:20 - 10:30: Opening

10:30 - 11:30: [特別講演 (Special lecture)] 岡本 龍明 (NTT 情報流通プラットフォーム研究所) Tatsuaki Okamoto (NTT Information Sharing Platform Laboratories)
"関数型暗号とその応用"

13:30 - 13:50: 安田 貴徳 (九州先端科学技術研究所), 櫻井 幸一 (九州先端科学技術研究所 / 九州大学), 高木 剛 (九州大学) Takanori Yasuda (Institute of Systems, Information Technologies and Nanotechnologies), Kouichi Sakurai (Institute of Systems, Information Technologies and Nanotechnologies / Kyushu University), Tsuyoshi Takagi (Kyushu University)
"Edwards 曲線を用いた効率的なペアリング暗号の構成"
"Efficient construction of pairing-based cryptography using Edwards curves"

13:50 - 14:20: 内田 幸寛 (京都大学) Yukihiro Uchida (Kyoto University)
"Hyperelliptic net による超楕円曲線上の Tate-Lichtenbaum ペアリング"
"The Tate-Lichtenbaum pairing on a hyperelliptic curve via hyperelliptic nets"

14:40 - 15:20: 原瀬 晋 (東京大学) Shin Harase (The University of Tokyo)
"F2-線形擬似乱数発生法の最適化のための高速格子簡約アルゴリズム"
"An efficient lattice reduction method for F2-linear pseudorandom number generators using Mulders and Storjohann algorithm"

15:40 - 16:10: 布田 裕一, 岡崎 裕之, 師玉 康成 (信州大学) Yuichi Futa, Hiroyuki Okazaki, Yasunari Shidama (Shinshu University)
"Mizar による素体上の楕円曲線の形式化"
"Formalization of Definitions and Theorems Related to an Elliptic Curve over a Finite Prime Field by Using Mizar"

16:10 - 16:30: 横山 俊一 (九州大学) Shun'ichi Yokoyama (Kyushu University)
"至る所良い還元を持つ楕円曲線について：計算機的手法とその最近の進展"
"On elliptic curves having everywhere good reduction: Computational approach and its recent progress"

Nov. 8（Tue.）

10:00 - 10:40: 山村健 (防衛大学校) Ken Yamamura (National Defense Academy)
"代数体の巡回拡大の不分岐 Galois 拡大の構造について"
"On the structure of unramified Galois extensions of cyclic extensions of number fields"

11:00 - 11:20: 森川 良三 (長崎大学・名誉教授) Ryozo Morikawa (Professor Emer. Nagasaki University)
"ワーリング　タイプ　の問題を探求する為の、いくつかの概念と方法　III"
"Some concepts and methods to investigate problems of Waring type III"

11:20 - 11:40: 梶谷 美帆 (東北大学) Miho Kajiya (Tohoku University)
"5 次交代群 A_5 を固定群とする 2-arc-transitive graph"
"On 2-arc transitive graphs with the alternating group of degree 5 as a one-point stabilizer"

13:30 - 14:30: [特別講演 (Special lecture)] 原田 昌晃 (山形大学 / ＪＳＴさきがけ) Masaaki Harada (Yamagata University / JST PRESTO)
"Self-dual codes -an introduction-"

14:50 - 15:30: 山田 裕理 (一橋大学) Hiromichi Yamada (Hitotsubashi University)
"パラフェルミオン頂点作用素代数の C_2 代数"
"The C_2 algebra of parafermion vertex operator algebras"

15:30 - 15:50: 入江 佑樹 (千葉大学) Yuki Irie (Chiba University)
"有向グラフの mutation が生成する群について"
"On groups generated by quiver mutations"

16:10 - 16:40: 高橋 萌子 (千葉大学) Moeko Takahashi (Chiba University)
"巡回シロー p-部分群をもつ有限群のスコット加群"
"Scott modules in finite groups with cyclic Sylow p-subgroups"

16:40 - 17:00: 脇 克志 (山形大学) Katsushi Waki (Yamagata University)
"J_4 の表現構成について"
"Construction of representation for J_4"

Nov. 9(Wed.)

10:00 - 10:20: 長谷川 武博 (工学院大学) Takehiro Hasegawa (Kogakuin University)
"関数体の塔に関する Elkies 予想の数値的証拠 II"
"Several numerical evidences of Elkies' conjecture II"

10:20 - 10:50: 橋本 竜太 (香川高等専門学校) Ryūta Hashimoto (Kagawa National College of Technology)
"基本単数の比較的大きな判別式の分類の試み"
"A certain classification of discriminants with large fundamental units"

11:10 - 11:40: 澤 正憲 (名古屋大学) Masanori Sawa (Nagoya University)
"整数の冪乗和に関する恒等式と求積公式"
"Identities involving sums of powers of intergers and cubature formulae"

13:30 - 14:30: [特別講演 (Special lecture)] 立谷 洋平 (弘前大学) Yohei Tachiya (Hirosaki University)
"パターン数列の諸性質について"
"Some properties of pattern sequence"

14:40 - 15:10: 知念 宏司 (近畿大学), 田村 知佳子 (大阪商業大学高等学校) Koji Chinen (Kinki University), Chikako Tamura (Osaka University of Commerce High School)
"平方剰余の条件を付加した $a \pmod p$ の剰余位数の分布について"
"On a distribution property of the residual order of $a \pmod p$ with a quadratic residue condition"

15:10 - 15:20: Closing

Hyperelliptic net による超楕円曲線上の Tate-Lichtenbaum ペアリング

内田 幸寛*

1 Introduction

暗号理論において，代数曲線上のペアリングは，まず離散対数問題への攻撃に用いられた．近年では，代数曲線上のペアリングは様々な暗号プロトコルの構成に応用されている．例えば，ID ベース暗号や関数型暗号，三者間鍵共有，短い署名などである．代数曲線上のペアリングは，Weil ペアリングや Tate-Lichtenbaum ペアリングなど，いくつか知られている．その中で，計算効率などの観点から，Tate-Lichtenbaum ペアリング，あるいはその変種がよく用いられている．

Tate-Lichtenbaum ペアリングの計算方法としては，通常 Miller のアルゴリズムが用いられる．2007 年，Stange [7] は，楕円曲線の場合に，elliptic net を用いた新しいアルゴリズムを与えた．Elliptic net は有限階数自由 Abel 群から整域への写像であり，ある漸化式を満たすものである．本稿では，elliptic net の超楕円曲線への拡張として hyperelliptic net を定義する．また，hyperelliptic net を用いて種数 2 の曲線上の Tate-Lichtenbaum ペアリングを計算するアルゴリズムについて述べる．

2 Stange の elliptic net

定義 2.1 (Stange [7, 8])**.** A を有限生成自由 Abel 群，R を整域とする．写像 $W\colon A \to R$ が **elliptic net** であるとは，$W(0) = 0$ であり，

$$W(p+q+s)W(p-q)W(r+s)W(r) + W(q+r+s)W(q-r)W(p+s)W(p) + W(r+p+s)W(r-p)W(q+s)W(q) = 0 \quad (1)$$

がすべての $p, q, r, s \in A$ に対して成り立つことをいう．

Elliptic net は M. Ward [9] が定義した elliptic divisibility sequence (EDS) の拡張である．整数列 $\{h_n\}$ が EDS であるとは，漸化式

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2$$

を満たし，n が m の約数ならば，h_n が h_m の約数となることをいう．$A = R = \mathbb{Z}$ として，elliptic net $W\colon \mathbb{Z} \to \mathbb{Z}$ が $W(1) = 1$ を満たし，$W(2)$ が $W(4)$ を割り切るならば，数列 $\{W(n)\}$ は EDS である．

EDS は，適当な条件のもとで，楕円曲線の等分多項式の値がなす数列と見なすことができる（cf. [9, Theorems 12.1 and 21.4]）．Stange は，これを拡張して，楕円曲線に対応する elliptic net を構成した．

* 京都大学大学院理学研究科数学教室・日本学術振興会特別研究員 PD

n を正整数，K を体，E を Weierstrass 方程式

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6,\quad a_1,a_2,a_3,a_4,a_6\in K$$

で定義される楕円曲線とする．E の無限遠点を O と書く．O は E の群演算の単位元である．

定理 2.2 (Stange [8])**.** すべての $\boldsymbol{v}=(v_1,\dots,v_n)\in\mathbb{Z}^n$ に対し，K 上定義された E^n 上の有理関数 $\Psi_{\boldsymbol{v}}$ が存在して，次を満たす：$\boldsymbol{P}=(P_1,\dots,P_n)\in E^n(K)$ とする．このとき，

(a) $\boldsymbol{v}\neq\boldsymbol{0}$ に対し，

$$\operatorname{div}(\Psi_{\boldsymbol{v}})=([v_1]\times\cdots\times[v_n])^*s^*(O)-\sum_{1\le k<l\le n}v_kv_lp_{k,l}^*(O)-\sum_{k=1}^n\left(2v_k^2-\sum_{l=1}^n v_kv_l\right)p_k^*(O).$$

ここで，$[v_i]\colon E\to E$ は v_i 倍写像，$s\colon E^n\to E$ は各成分の和，$p_{k,l}\colon E^n\to E$ は $p_{k,l}(\boldsymbol{P})=P_k+P_l$ で定まり，$p_k\colon E^n\to E$ は k 番目の射影である．

(b) $\boldsymbol{v},\boldsymbol{w}\in\mathbb{Z}^n$ が $\boldsymbol{v},\boldsymbol{w},\boldsymbol{v}+\boldsymbol{w},\boldsymbol{v}-\boldsymbol{w}\neq\boldsymbol{0}$ を満たすならば，

$$\frac{\Psi_{\boldsymbol{v}+\boldsymbol{w}}(\boldsymbol{P})\Psi_{\boldsymbol{v}-\boldsymbol{w}}(\boldsymbol{P})}{\Psi_{\boldsymbol{v}}(\boldsymbol{P})^2\Psi_{\boldsymbol{w}}(\boldsymbol{P})^2}=-x([v_1]P_1+\cdots+[v_n]P_n)+x([w_1]P_1+\cdots+[w_n]P_n).$$

(c) $P_i\neq O$ $(1\le i\le n)$ かつ $P_i+P_j\neq O$ $(1\le i<j\le n)$ であるとする．写像 $W_{\boldsymbol{P}}\colon\mathbb{Z}^n\to K$ を $W_{\boldsymbol{P}}(\boldsymbol{v})=\Psi_{\boldsymbol{v}}(\boldsymbol{P})$ で定める．このとき，$W_{\boldsymbol{P}}$ は elliptic net である．

定理の $W_{\boldsymbol{P}}$ を E **と** $\boldsymbol{P}$ **に対応する elliptic net** と呼ぶ.

注意 2.3. $\boldsymbol{P}=(P_1,\dots,P_n)\in E^n(K)$ が $P_i\neq O$ $(1\le i\le n)$ かつ $P_i+P_j\neq O$ $(1\le i<j\le n)$ を満たすとする．このとき，定理 2.2 (a) より，

$$\Psi_{\boldsymbol{v}}(\boldsymbol{P})=0\iff[v_1]P_1+\cdots+[v_n]P_n=O.$$

有理関数 $\Psi_{\boldsymbol{v}}$ は次のように構成される．まず，$K=\mathbb{C}$ の場合を考える．このとき，$E(\mathbb{C})\cong\mathbb{C}/\Lambda$ となる $\mathbb{C}$ 内の格子 Λ が存在する．格子 Λ に対応する Weierstrass の σ 関数 $\sigma\colon\mathbb{C}\to\mathbb{C}$ を

$$\sigma(u)=u\prod_{\omega\in\Lambda\setminus\{0\}}\left(1-\frac{u}{\omega}\right)\exp\left(\frac{u}{\omega}+\frac{u^2}{2\omega^2}\right)$$

で定義する．いま，$\mathbb{C}^n$ 上の有理型関数 $\Omega_{\boldsymbol{v}}$ を

$$\Omega_{\boldsymbol{v}}(u_1,\dots,u_n)=\frac{\sigma(v_1u_1+\cdots+v_nu_n)}{\prod_{i=1}^n\sigma(u_i)^{2v_i^2-\sum_{j=1}^n v_iv_j}\prod_{1\le i<j\le n}\sigma(u_i+u_j)^{v_iv_j}}$$

で定義する．有理型関数 $\Omega_{\boldsymbol{v}}$ は，各変数 u_i について Λ を周期に持つことが示せるので，$\Omega_{\boldsymbol{v}}$ を $(\mathbb{C}/\Lambda)^n$ 上の有理型関数と見なすことができる．同型 $E(\mathbb{C})\cong\mathbb{C}/\Lambda$ によって，$\Omega_{\boldsymbol{v}}$ を E^n 上の有理関数と見なして $\Psi_{\boldsymbol{v}}$ とおくと，$\Psi_{\boldsymbol{v}}$ が定理 2.2 の条件を満たすことがわかる．一般の体 K 上でも，複素数体上で定義した $\Psi_{\boldsymbol{v}}$ を用いることで，有理関数の存在を示すことができる．詳細は [8, Section 4] を参照せよ.

Stange は，楕円曲線上の Tate-Lichtenbaum ペアリングを elliptic net を用いて書き表した．$\mathbb{F}_q$ を q 個の元を持つ有限体，E を $\mathbb{F}_q$ 上定義された楕円曲線とする．m を $q-1$ の正の約数とし，

$$\tau_m\colon E(\mathbb{F}_q)[m]\times E(\mathbb{F}_q)/mE(\mathbb{F}_q)\to\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^m$$

を Tate-Lichtenbaum ペアリングとする（定義は § 4 参照）．このとき次の定理が成り立つ.

定理 2.4 (Stange [7, Corollary 1]). $P \in E(\mathbb{F}_q)[m]$, $Q \in E(\mathbb{F}_q)$ が $P, Q, P+Q \neq O$ を満たすとする．このとき,

$$\tau_m(P,Q) = \frac{W_{P,Q}(m+1,1)W_{P,Q}(1,0)}{W_{P,Q}(m+1,0)W_{P,Q}(1,1)} \bmod (\mathbb{F}_q^\times)^m.$$

Stange はこの定理を用いて，Tate-Lichtenbaum ペアリングを計算する新しいアルゴリズムを与えた．本稿の目的は，Stange の結果の超楕円曲線への拡張について述べることである．

3 Hyperelliptic net

すでに見たように，Stange は，まず elliptic net を漸化式 (1) によって定義した．そして，楕円曲線とその有理点に対応する elliptic net を構成した．しかしながら，漸化式 (1) を直接拡張して超楕円曲線に対応させるのは困難に思われる．ここでは，Tate-Lichtenbaum ペアリングへの応用を見込んで，超楕円曲線とその Jacobi 多様体の有理点から，写像 $W\colon \mathbb{Z}^n \to K$ を構成する．そして，写像 W が満たす漸化式を構成する．

K を任意の体とする．K 上定義された種数 g の超楕円曲線

$$C\colon y^2 + (b_g x^g + \cdots + b_0)y = x^{2g+1} + a_{2g}x^{2g} + \cdots + a_0$$

を考える．C はただ 1 つの無限遠点 ∞ を持つ．J を C の Jacobi 多様体とする．J は g 次元 Abel 多様体，すなわち，群構造を持つ g 次元射影多様体である．J の単位元を O と書く．埋め込み $\lambda\colon C \to J$ で，$\lambda(\infty) = O$ となるものが存在する．$\mathrm{Pic}^0(C)$ を C の次数 0 の因子類群とする．埋め込み λ を拡張して，同型 $\lambda\colon \mathrm{Pic}^0(C) \xrightarrow{\sim} J(K)$ が得られる．J 上のテータ因子 Θ を，$\Theta = \lambda(C) + \cdots + \lambda(C)$（$g-1$ 個）で定義する．

楕円曲線の場合と同様に，次の定理が成り立つ.

定理 3.1. すべての正整数 n と，すべての $\boldsymbol{v} = (v_1, \ldots, v_n) \in \mathbb{Z}^n$ に対し，K 上定義された J^n 上の有理関数 $\Phi_{\boldsymbol{v}}$ が存在して，次を満たす：$\boldsymbol{P} = (P_1, \ldots, P_n) \in J^n(K)$ とする．このとき,

(a) $\boldsymbol{v} \neq \boldsymbol{0}$ に対し,

$$\mathrm{div}(\Phi_{\boldsymbol{v}}) = ([v_1] \times \cdots \times [v_n])^* s^* \Theta - \sum_{1 \le k < l \le n} v_k v_l p_{k,l}^* \Theta - \sum_{k=1}^{n} \left(2v_k^2 - \sum_{l=1}^{n} v_k v_l \right) p_k^* \Theta.$$

ここで，$[v_i]\colon J \to J$ は v_i 倍写像，$s\colon J^n \to J$ は各成分の和，$p_{k,l}\colon J^n \to J$ は $p_{k,l}(\boldsymbol{P}) = P_k + P_l$ で定まり，$p_k\colon J^n \to J$ は k 番目の射影である.

(b) $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{Z}^n$ が $\boldsymbol{v}, \boldsymbol{w}, \boldsymbol{v}+\boldsymbol{w}, \boldsymbol{v}-\boldsymbol{w} \neq \boldsymbol{0}$ を満たすならば,

$$\frac{\Phi_{\boldsymbol{v}+\boldsymbol{w}}(\boldsymbol{P})\Phi_{\boldsymbol{v}-\boldsymbol{w}}(\boldsymbol{P})}{\Phi_{\boldsymbol{v}}(\boldsymbol{P})^2 \Phi_{\boldsymbol{w}}(\boldsymbol{P})^2} = \Phi_{(1,-1)}\big([v_1]P_1 + \cdots + [v_n]P_n, [w_1]P_1 + \cdots + [w_n]P_n\big).$$

(c) $P_i \notin \Theta$ $(1 \le i \le n)$ かつ $P_i + P_j \notin \Theta$ $(1 \le i < j \le n)$ であるとする．写像 $W_{\boldsymbol{P}}\colon \mathbb{Z}^n \to K$ を $W_{\boldsymbol{P}}(\boldsymbol{v}) = \Phi_{\boldsymbol{v}}(\boldsymbol{P})$ で定める．m を $m > 2^g$ となる整数とし，$\boldsymbol{v}^{(1)}, \ldots, \boldsymbol{v}^{(m)} \in ((1/2)\mathbb{Z})^n$ とする．すべての $1 \le i, j \le m$ に対して，$\boldsymbol{v}^{(i)} + \boldsymbol{v}^{(j)}, \boldsymbol{v}^{(i)} - \boldsymbol{v}^{(j)} \in \mathbb{Z}^n$ と仮定する．m 次正方行列 A を

$$A = \Big(W_{\boldsymbol{P}}(\boldsymbol{v}^{(i)} + \boldsymbol{v}^{(j)}) W_{\boldsymbol{P}}(\boldsymbol{v}^{(i)} - \boldsymbol{v}^{(j)}) \Big)_{1 \le i,j \le m}$$

で定義する．このとき，$\det A = 0$ である．特に，$g \equiv 1, 2 \pmod 4$ かつ m が偶数ならば，$\mathrm{Pf}\, A = 0$ である．ここで，$\mathrm{Pf}\, A$ は A の Pfaffian である.

定理の $W_{\boldsymbol{P}}$ を C と $\boldsymbol{P}$ に対応する **hyperelliptic net** と呼ぶ.

注意 3.2. $\boldsymbol{P} = (P_1, \ldots, P_n) \in J^n(K)$ が $P_i \notin \Theta$ $(1 \le i \le n)$ かつ $P_i + P_j \notin \Theta$ $(1 \le i < j \le n)$ を満たすとする．このとき，定理 3.1 (a) より，

$$\Phi_{\boldsymbol{v}}(\boldsymbol{P}) = 0 \iff [v_1]P_1 + \cdots + [v_n]P_n \in \Theta.$$

注意 3.3. 楕円曲線の場合，$\Psi_{(1,-1)}(P_1, P_2) = -x(P_1) + x(P_2)$ となる．したがって，定理 2.2 (b) は定理 3.1 (b) と同じ形に書ける．

有理関数 $\Phi_{\boldsymbol{v}}$ の構成は楕円曲線の場合と同様である．まず，$K = \mathbb{C}$ の場合を考える．このとき，$J(\mathbb{C}) \cong \mathbb{C}^g/\Lambda$ となる $\mathbb{C}^g$ 内の格子 Λ が存在する．Weierstrass の σ 関数の拡張として，超楕円 σ 関数 $\sigma\colon \mathbb{C}^g \to \mathbb{C}$ が定義されている．詳細な定義は [1, 4, 5] を参照せよ．いま，$(\mathbb{C}^g)^n$ 上の有理型関数 $\Phi_{\boldsymbol{v}}$ を

$$\Phi_{\boldsymbol{v}}(u^{(1)}, \ldots, u^{(n)}) = \frac{\sigma(v_1u^{(1)} + \cdots + v_nu^{(n)})}{\prod_{i=1}^n \sigma(u^{(i)})^{2v_i^2 - \sum_{j=1}^n v_iv_j} \prod_{1 \le i < j \le n} \sigma(u^{(i)} + u^{(j)})^{v_iv_j}}$$

で定義する．有理型関数 $\Omega_{\boldsymbol{v}}$ は，各変数 $u^{(i)}$ について Λ を周期に持つことが示せるので，$(\mathbb{C}^g/\Lambda)^n$ 上の有理型関数と見なせることがわかる．同型 $J(\mathbb{C}) \cong \mathbb{C}^g/\Lambda$ によって，$\Phi_{\boldsymbol{v}}$ を J^n 上の有理関数と見なすと，$\Phi_{\boldsymbol{v}}$ が定理 3.1 の条件を満たすことがわかる．一般の体 K 上でも，複素数体上で定義した $\Phi_{\boldsymbol{v}}$ を用いることで，有理関数の存在を示すことができる．これは楕円曲線の場合の Stange [8] の議論と同様である．

注意 3.4. 種数 $g = 1$ のとき，定理 3.1 の漸化式から，elliptic net の漸化式が導かれる．実際，$m = 4$ として，$\boldsymbol{v}^{(1)} = p + (1/2)s$, $\boldsymbol{v}^{(2)} = q + (1/2)s$, $\boldsymbol{v}^{(3)} = r + (1/2)s$, $\boldsymbol{v}^{(4)} = (1/2)s$ とおくと，$\operatorname{Pf} A = 0$ から漸化式 (1) が従う．

例 3.5. $g = 2$, $m = 6$, $n = 1$ とする．$v^{(1)} = k+1$, $v^{(2)} = k$, $v^{(3)} = 3$, $v^{(4)} = 2$, $v^{(5)} = 1$, $v^{(6)} = 0$ とすると，漸化式 $\operatorname{Pf} A = 0$ は次のようになる．

$$\begin{aligned}
&W(2k+1)\big(W(5)^3 - W(4)W(2)^3 + W(3)^3\big) \\
&\quad - W(k+4)W(k-2)\big(W(k+2)W(k-2) + W(k+1)W(k-1)W(2)^2 - W(k)^2W(3)\big) \\
&\quad + W(k+3)W(k-1)\big(W(k+3)W(k-3) - W(k+1)W(k-1)W(3)^2 + W(k)^2W(4)W(2)\big) \\
&\quad - W(k+2)W(k)\big(W(k+3)W(k-3)W(2)^2 + W(k+2)W(k-2)W(3)^2 - W(k)^2W(5)\big) \\
&\quad + W(k+1)^2\big(W(k+3)W(k-3)W(3) - W(k+2)W(k-2)W(4)W(2) + W(k+1)W(k-1)W(5)\big) \\
&\qquad = 0.
\end{aligned}$$

ここで，$W = W_P$ とおき，$W(1) = 1$ であると仮定した．

4 Tate-Lichtenbaum ペアリング

まず，一般の代数曲線上の Tate-Lichtenbaum ペアリングについて述べる．詳細は [2, 3] を参照せよ．

$\mathbb{F}_q$ を q 個の元を持つ有限体，C を $\mathbb{F}_q$ 上定義された非特異射影代数曲線とする．C が $\mathbb{F}_q$ 有理点を持つと仮定する．m を $q-1$ の正の約数とする．

Tate-Lichtenbaum ペアリング τ_m は写像

$$\tau_m\colon \mathrm{Pic}^0(C)[m] \times \mathrm{Pic}^0(C)/m\,\mathrm{Pic}^0(C) \to \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^m;$$
$$(\overline{D}, \overline{E}) \mapsto f_D(E) = \prod_{i=1}^{r} f_D(P_i)^{n_i}$$

である．ここで，f_D は $\mathrm{div}(f_D) = mD$ を満たす C 上の有理関数，$E = \sum_{i=1}^r n_i P_i$ であり，D と E は共通の点を持たないとする．Tate-Lichtenbaum ペアリング τ_m は，well-defined，双線形，非退化であることが知られている．

曲線 C を超楕円曲線として，Tate-Lichtenbaum ペアリングを hyperelliptic net を用いて書き表す．まず，同型 $\lambda\colon \mathrm{Pic}^0(C) \xrightarrow{\sim} J(\mathbb{F}_q)$ によって，τ_m をペアリング

$$J(\mathbb{F}_q)[m] \times J(\mathbb{F}_q)/mJ(\mathbb{F}_q) \to \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^m$$

と同一視する．このとき，次の定理が成り立つ．

定理 4.1. $P \in J(\mathbb{F}_q)[m]$，$Q \in J(\mathbb{F}_q)$ とする．$P, Q, P+Q \notin \Theta$ ならば，

$$\tau_m(P,Q) = \frac{W_{P,Q}(m+1,1)W_{P,Q}(1,0)}{W_{P,Q}(m+1,0)W_{P,Q}(1,1)} \bmod (\mathbb{F}_q^\times)^m.$$

5 種数 2 の曲線に対するアルゴリズム

以下，曲線 C の種数が 2 であると仮定する．前節までの記号を引き続き用いる．

C と P, Q に対応する hyperelliptic net $W_{P,Q}$ について，P, Q を省略して，$W(m,n) = W_{P,Q}(m,n)$ と書く．$W(m,0)$, $W(m,1)$ を計算するアルゴリズムを構成するために，次のようなブロックを定義する．

定義 5.1. k を整数とする．k **を中心とするブロック** V を

$$V = [[W(k-7,0), W(k-6,0), \ldots, W(k+8,0)], [W(k-3,1), W(k-2,1), \ldots, W(k+3,1)]]$$

で定義する．

k を中心とするブロック V に対し，次の関数を定義する．

(a) Double(V)：$2k$ を中心とするブロックを返す．
(b) DoubleAdd(V)：$2k+1$ を中心とするブロックを返す．

これらの関数から返されるブロックの計算には，次のような漸化式を用いる．整数 $m_1, \ldots, m_6, n_1, \ldots, n_6$ を表 1 のように与える．6 次正方行列 A を

$$A = (W(m_i + m_j, n_i + n_j)W(m_i - m_j, n_i - n_j))_{1 \le i,j \le 6}$$

で定義する．定理 3.1 (c) より，

$$\mathrm{Pf}\, A = 0.$$

例えば，表 1 の 2 行目の値からは，例 3.5 の漸化式が得られる．

計算したい項	m_1	m_2	m_3	m_4	m_5	m_6	n_1	$n_2, \ldots, n_6$
$W(2k,0)$	$k+1$	$k-1$	3	2	1	0	0	0
$W(2k+1,0)$	$k+1$	k	3	2	1	0	0	0
$W(2k+j,1)$	k	$k+j$	3	2	1	0	1	0

表 1　m_i と n_i の値

この漸化式では，$\mathbb{F}_q$ 内の四則演算のみが用いられることに注意する．また，Double(V) と DoubleAdd(V) を実行するには，次の値が 0 でないことを必要とする．

$$W(2,0),\ W(-4,1),\ W(-3,1),\ \ldots,\ W(3,1),\ \Delta = W(5,0)^3 - W(4,0)W(2,0)^3 + W(3,0)^3.$$

これらの関数を用いて，$W(m,0)$, $W(m,1)$ を計算するアルゴリズムは次のように書ける．

Algorithm 1 Hyperelliptic Net Algorithm

Input: 初期値 $W(i,0)$ $(-6 \le i \le 9)$，$W(i,1)$ $(-4 \le i \le 4)$，
　m の 2 進法での表示 $m = (d_k d_{k-1} \ldots d_1)_2$ $(d_k = 1)$.

Output: Hyperelliptic net の項 $W(m,0)$ と $W(m,1)$

1: $V \leftarrow [[W(-6,0), W(-5,0), \ldots, W(9,0)], [W(-2,1), W(-1,1), \ldots, W(4,1)]]$
2: **for** $i = k-1$ down to 1 **do**
3:　**if** $d_i = 0$ **then**
4:　　$V \leftarrow$ Double(V)
5:　**else**
6:　　$V \leftarrow$ DoubleAdd(V)
7:　**end if**
8: **end for**
9: **return** $V[0,7]$, $V[1,3]$　// それぞれ $W(m,0)$，$W(m,1)$

Algorithm 1 では，初期値として，$W(i,0)$ $(-6 \le i \le 9)$ と $W(i,1)$ $(-4 \le i \le 4)$ の値が必要である．この初期値の計算について次に述べる．

P, Q の Mumford 表現がそれぞれ，$(t^2 + u_{11}t + u_{12}, v_{11}t + v_{12})$, $(t^2 + u_{21}t + u_{22}, v_{21}t + v_{22})$ であるとする．このとき，m, n が小さいときの $W(m,n)$ の値は次の式で計算できる．

$$W(0,0) = 0, \quad W(1,0) = W(0,1) = W(1,1) = 1,$$

$$\begin{aligned} W(2,0) = {} & (-4u_{12} + 6{u_{11}}^2 + (-{b_2}^2 - 4a_4)u_{11} + b_1b_2 + 2a_3)v_{12} + 2{v_{11}}^3 + (3b_1 - 3b_2u_{11}){v_{11}}^2 \\ & + ((-8u_{11} + {b_2}^2 + 4a_4)u_{12} + 2{u_{11}}^3 + ({b_2}^2 - 2a_4){u_{11}}^2 + (2a_3 - 2b_1b_2)u_{11} - b_0b_2 + {b_1}^2 - 2a_2)v_{11} \\ & + 2b_2{u_{12}}^2 + (b_2{u_{11}}^2 - 4b_1u_{11} - a_3b_2 + 2a_4b_1 - 2b_0)u_{12} - b_2{u_{11}}^4 + (a_4b_2 + b_1){u_{11}}^3 \\ & + (-a_3b_2 - a_4b_1 + 3b_0){u_{11}}^2 + (a_2b_2 + a_3b_1 - 2a_4b_0)u_{11} - a_2b_1 + a_3b_0. \end{aligned}$$

m または n が大きいとき，$W(m,n)$ を上のように表示しようとすると，非常に多くの項が現れる．そこで，

次の式で帰納的に $W(i,0)$ $(3 \le i \le 9)$, $W(i,1)$ $(-4 \le i \le -1,\ 2 \le i \le 4)$ を計算する．

$$\frac{W(i+1,0)W(i-1,0)}{W(i,0)^2} = \Phi_{(1,-1)}([i]P, P), \tag{2}$$

$$\frac{W(i+1,1)W(i-1,1)}{W(i,1)^2} = \Phi_{(1,-1)}([i]P + Q, P). \tag{3}$$

ここで，$W(1,0) = 1$ を用いた．また，$\Phi_{(1,-1)}(P,Q)$ は次の式で表される．

$$\begin{aligned}\Phi_{(1,-1)}(P,Q) = &-(v_{11}^2 - b_2u_{11}v_{11} + b_1v_{11} - u_{11}u_{12} + u_{11}^3 - a_4u_{11}^2 + a_3u_{11}) \\ &+ (v_{21}^2 - b_2u_{21}v_{21} + b_1v_{21} - u_{21}u_{22} + u_{21}^3 - a_4u_{21}^2 + a_3u_{21}) - u_{12}u_{21} + u_{11}u_{22}.\end{aligned}$$

式 (2), (3) を使うためには，$W(i,0) \neq 0$ $(2 \le i \le 8)$, $W(i,1) \neq 0$ $(-3 \le i \le -1,\ 2 \le i \le 3)$ であることが必要であることに注意する．

また，$W(-i,0) = -W(i,0)$ となるので，$W(i,0)$ $(-6 \le i \le -2)$ が計算できる．以上によって，初期値 $W(i,0)$ $(-6 \le i \le 9)$ と $W(i,1)$ $(-4 \le i \le 4)$ を計算することができる．

以上をまとめると，Algorithm 1 による，hyperelliptic net，および Tate-Lichtenbaum ペアリングの計算量は次のように評価できる．

定理 5.2. 次の値がすべて 0 でないと仮定する．

$$W(2,0),\ W(3,0),\ \ldots,\ W(8,0),\ W(-4,1),\ W(-3,1),\ \ldots,\ W(3,1),\ \Delta. \tag{4}$$

このとき，$W(m,0)$ と $W(m,1)$ は $O(\log m)$ 回の四則演算で計算できる．特に，Tate-Lichtenbaum ペアリング $\tau_m(P,Q)$ は $O(\log m)$ 回の四則演算で計算できる．

注意 5.3. 一般の元 P, Q に対して，(4) の値はすべて 0 でない．実際，式 (4) の値を P, Q の関数とみなすと，どれも 0 でない $J \times J$ 上の有理関数となる．

注意 5.4. Miller のアルゴリズムも $\tau_m(P,Q)$ を $O(\log m)$ 回の四則演算で計算できる．

Hyperelliptic net と Tate-Lichtenbaum ペアリングの計算例を挙げる．計算には PARI/GP [6] を用いた．

例 5.5. $q = 47$, $C\colon y^2 = x^5 + x + 41/\mathbb{F}_{47}$ とする．$P, Q \in J(\mathbb{F}_{47})$ を Mumford 表現によって $P = (x^2 + 6x + 16, 31x + 3)$, $Q = (x^2 + 29 + 24, 22x + 14)$ と定める．このとき，$W(m,n)$ は表 2 のような値を取る．ここで，左下が $W(0,0)$ である．

$m = 23$ とする．このとき，m は $q - 1 = 46$ の約数である．

$$W_{P,Q}(m+1,1) = 43, \quad W_{P,Q}(m+1,0) = 8, \quad W_{P,Q}(1,0) = W_{P,Q}(1,1) = 1$$

となるから，Tate-Lichtenbaum ペアリングの値は，

$$\tau_m(P,Q) = \frac{43}{8} \bmod (\mathbb{F}_{47}^{\times})^{23} = 23 \bmod (\mathbb{F}_{47}^{\times})^{23}$$

となる．

本稿で与えたアルゴリズムは，Stange のアルゴリズムと同様の利点を持つ．例えば，Miller のアルゴリズムでは，$\tau_m(P,Q)$ の計算時間は m の Hamming 重みに依存するが，本稿で与えたアルゴリズムでは m の Hamming 重みにはよらない．

	7	12	2	36	19	33	39	18
	14	38	14	10	23	21	36	9
	13	31	32	18	8	2	2	16
	14	15	43	19	44	5	22	42
	25	6	33	11	10	36	21	16
	25	8	2	13	16	32	14	5
↑	1	1	23	4	29	40	43	7
Q	0	1	37	18	36	2	7	45

$P \rightarrow$

表 2　Hyperelliptic net $W(m, n)$

また，種数 2 以上の場合，Miller のアルゴリズムは素朴に実装すると体拡大を必要とする．これは時間を要するので，ノルムや終結式を用いて体拡大を避ける必要がある．しかし，本稿で与えたアルゴリズムは，$\mathbb{F}_q$ 内の四則演算しか用いないので，体拡大を必要としない．

種数 3 以上の超楕円曲線に対しては，定理 3.1 から得られる漸化式が非常に複雑になるので，漸化式を用いたアルゴリズムは実用的でないと考えられる．この場合に hyperelliptic net をより効率よく計算するアルゴリズムを得ることは今後の課題である．

参考文献

[1] V. M. Buchstaber, V. Z. Enolskii, D. V. Leykin, Kleinian functions, hyperelliptic Jacobians and applications, Rev. Math. Math. Phys. **10** (1997) 1–125.

[2] S. Duquesne, G. Frey, Background on pairings, in H. Cohen et al., eds., *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Math. Appl. (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2006, 115–124.

[3] G. Frey, H.-G. Rück, A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves, Math. Comp. **62** (1994) 865–874.

[4] Y. Ônishi, Determinant expressions for hyperelliptic functions (with an appendix by Shigeki Matsutani), Proc. Edinb. Math. Soc. (2) **48** (2005) 705–742.

[5] 大西良博「超楕円函数論」第 15 回整数論サマースクール報告集，2008，131–176，`http://www.ccn.yamanashi.ac.jp/~yonishi//research/pub/ss2007/06onishi.pdf` より入手可能．

[6] PARI/GP, version `2.3.4`, Bordeaux (2008), `http://pari.math.u-bordeaux.fr/`.

[7] K. E. Stange, The Tate pairing via elliptic nets, in T. Takagi, T. Okamoto, E. Okamoto, T. Okamoto, eds., *Pairing-Based Cryptography—Pairing 2007*, Lecture Notes in Comput. Sci. 4575, Springer, Berlin, 2007, 329–348.

[8] K. E. Stange, Elliptic nets and elliptic curves, Algebra Number Theory **5** (2011) 197–229.

[9] M. Ward, Memoir on elliptic divisibility sequences, Amer. J. Math. **70** (1948) 31–74.

Formalization of Definitions and Theorems Related to an Elliptic Curve over a Finite Prime Field by Using Mizar *

Yuichi Futa Hiroyuki Okazaki Yasunari Shidama
Shinshu University

Nov. 9, 2011

Abstract

In this paper, we introduce our formalization of the definitions and theorems related to an elliptic curve over a finite prime field. The elliptic curve is important in an elliptic curve cryptosystem whose security is based on the computational complexity of the elliptic curve discrete logarithm problem.

1 Introduction

Mizar[1, 2] is an advanced project of the Mizar Society, led by Andrzej Trybulec, which formalizes mathematics. The Mizar project, which was developed to describe mathematics formally, describes mathematical proofs in the Mizar language. The Mizar proof checker operates on both Windows and UNIX environments and registers proven definitions and theorems in the Mizar Mathematical Library (MML).

In this paper, we formalize the definitions and theorems related to an elliptic curve over a finite prime field[3]. An elliptic curve is a non-singular cubic curve defined by the equation $y^2 = x^3 + ax + b$. An operation on points on the elliptic curve is defined. A set of points has the structure of an Abelian group using this operation.

An elliptic curve is an important mathematical concept related to fields such as number theory, algebra, analysis, topology, and algebraic geometry. One of the most important applications of elliptic curves is in an elliptic curve cryptosystem(ECC)[4]. The ECC uses scalar multiplications of the $\mathbb{Z}$-module constructed using the Abelian group. The security of the ECC is based on the computational complexity of the elliptic curve discrete logarithm problem, in which s is computed from sP (multiplication of a scalar s and a point P).

*This work was partly supported by JSPS KAKENHI 21240001 and 22300285.

Recently, it has become necessary to prove the security of cryptosystems. A mathematical proof checker is important for this purpose. However, the formalization of mathematical definitions and theorems of the elliptic curve is not yet included in the MML. Hence, we need to enrich the MML by including the definitions and theorems.

This paper is organized as follows. In Section 2, we explain a finite prime field $\mathbb{F}_p$ and its formalization. Section 3 introduces the definitions of projective coordinates and an elliptic curve. In Section 4, we describe the relationship between the number of points on an elliptic curve over $\mathbb{F}_p$ and Legendre symbols. Section 5 explains an operation on points on an elliptic curve. We conclude our discussion in Section 6. The definitions and theorems in this paper are described as formalizations in Mizar and have been verified for correctness using the Mizar proof checker.

2 Finite Prime Field $\mathbb{F}_p$

In this section, we describe the definition of a finite prime field. A finite prime field $\mathbb{F}_p$, where p is a prime number, is used as the definition field of an elliptic curve.

First, we introduce the definition of a subfield.

Definition 2.1 (Subfield)

```
definition let K be Field;
  mode Subfield of K -> Field means
  the carrier of it c= the carrier of K
  & the addF of it = (the addF of K) || the carrier of it
  & the multF of it = (the multF of K) || the carrier of it
  & 1.it = 1.K & 0.it = 0.K;
```

Here, "`the carrier of it`" is a set constructed by the subfield of a field K, and "`(the addF of K) || the carrier of it`" and "`(the multF of K) || the carrier of it`" are limitations of the addition and multiplication of K in the set, respectively. "`0.it`" and "`1.it`" refer to the identity elements of addition and multiplication in the subfield, respectively. Definition 2.1 defines a field satisfying the following conditions as a subfield of K:

- A set constructed by the field is included in a set constructed by K.
- Addition and multiplication of the field are limited to those of K in the set constructed by the field.
- Identity elements of addition and multiplication in the field are equal to those in K.

We now introduce the definition of a prime field.

Definition 2.2 (Prime field)

```
definition let IT be Field;
```

```
  attr IT is prime means
  K1 is strict Subfield of IT implies K1 = IT;
end;
```

Definition 2.2 indicates that a subfield of a prime field is the prime field itself.

For $\mathbb{F}_p$, where p is a prime number, the following theorem holds:

Theorem 2.3 (Prime field $\mathbb{F}_p$)

```
theorem
  for p be Prime holds GF(p) is prime;
```

Here, "`GF(p)`" denotes $\mathbb{F}_p$. Theorem 2.3 indicates that $\mathbb{F}_p$, where p is a prime number, is a prime field.

We introduce an outline of a proof of Theorem 2.3. The basic construction of the proof is as follows:

(1) proving that all elements in $K = \mathbb{F}_p$ are in a subfield K' of K, and

(2) proving that K is a subfield of K' and $K = K'$ because K' is the subfield of K.

(1) mentioned above can be proved by the inductive method. The detailed proof is as follows:

(a) 0 is included in K' because `0.it = 0.K`.

(b) When we assume that a natural number n $(0 \leq n < p-1)$ is included in K', $n+1$ is included in K'.

(c) Because of the induction of (a) and (b), all elements of K $(0, 1, \cdots p-1)$ are included in K'.

(b) is proved by using the following theorem[5]:

```
theorem :: BINOP_1:17
  for f being Function of [:X,Y:],Z st x in X & y in Y &
  Z <> {} holds f.(x,y) in Z;
```

The inductive method used in (c) is as follows[6]:

```
scheme :: INT_1:sch 7
  FinInd{M, N() -> Element of NAT, P[Nat]} : for i being
  Element of NAT st M() <= i & i <= N() holds P[i]
provided
 P[M()] and
 for j being Element of NAT st M() <= j & j < N() holds
 P[j] implies P[j+1];
```

Here, "`P[j]`" indicates that a natural number j is included in K', and "`M()`" and "`N()`" are set to 0 and $p-1$, respectively.

3 Elliptic Curve

This section defines an elliptic curve.

We define the projective coordinates on which the elliptic curve is drawn.

Definition 3.1 (Projective coordinate)

```
definition let K be Field;
  func ProjCo(K) -> non empty Subset of
  [:the carrier of K, the carrier of K, the carrier of K:] equals
  [:the carrier of K, the carrier of K, the carrier of K:]
  \ {[0.K,0.K,0.K]};
end;
```

By Definition 3.1, when P is in "`ProjCo(K)`," $P = [X_P, Y_P, Z_P] \in K^3 \backslash \{[0,0,0]\}$, where X_P, Y_P, and Z_P are the X, Y-, and Z-coordinates of P, respectively. The projective coordinates of P and Q are defined as follows such that their coordinates are equivalent:

Definition 3.2 (Equivalence of projective coordinates)

```
definition
  let p be Prime;
  let P,Q be Element of ProjCo(GF(p));
  pred P _EQ_ Q means
    ex a be Element of GF(p) st a <> 0.GF(p)
    & P‘1 = a*Q‘1 & P‘2 = a*Q‘2 & P‘3 = a*Q‘3;
  reflexivity;
  symmetry;
end;
```

Here, "`P‘1(Q‘1)`," "`P‘2(Q‘2)`," and "`P‘3(Q‘3)`" are the X, Y-, and Z-coordinates of $P(Q)$, respectively. "`_EQ_`" denotes the equivalence relation of the projective coordinates. Definition 3.2 indicates that P and Q are equivalent when $a(\neq 0)$ exists such that $X_P = a \times X_Q$, $Y_P = a \times Y_Q$, and $Z_P = a \times Z_Q$.

We describe the definition equation of an elliptic curve as follows:

Definition 3.3 (Definition equation of an elliptic curve)

```
definition
  let p be Prime;
  let a, b be Element of GF(p);
  func EC_WEqProjCo(a,b,p) -> Function of
  [:the carrier of GF(p), the carrier of GF(p),
  the carrier of GF(p):], GF(p) means
  for P be Element of [:the carrier of GF(p),
  the carrier of GF(p), the carrier of GF(p):] holds
  it. P = ((P‘2) |^2)*(P‘3)-((P‘1) |^3 +a*(P‘1)*(P‘3) |^2
  +b*(P‘3) |^3);
end;
```

Definition 3.3 indicates that an elliptic curve is defined by the equation $Y^2Z - (X^3 + aXZ^2 + bZ^3) = 0$. Note that the equation $Y^2Z - (X^3 + aXZ^2 + bZ^3) = 0$ is valid for the definition field $\mathbb{F}_p$, where "$p > 3$." In this paper, we consider $p > 3$.

Because the elliptic curve is a non-singular cubic curve, the discriminant $\delta = 4a^3 + 27b^2$ ("`Disc`") is not equal to 0. The discriminant is defined as follows:

Definition 3.4 (Discriminant of an elliptic curve)

```
definition
  let p be Prime;
  let a, b be Element of GF(p);
  func Disc(a,b,p) -> Element of GF(p) means
  for g4, g27 be Element of GF(p) st g4 = 4 mod p &
  g27 = 27 mod p
  holds it = g4*a|^3 + g27*b|^2;
end;
```

A set of $\mathbb{F}_p$-rational points on the elliptic curve is defined as follows:

Definition 3.5 (Set of $\mathbb{F}_p$-rational points)

```
definition
  let p be Prime;
  let a, b be Element of GF(p);
  func EC_SetProjCo(a,b,p) -> non empty Subset of ProjCo(GF(p))
  equals {P where P is Element of ProjCo(GF(p)) :
  EC_WEqProjCo(a,b,p).P = 0.GF(p)};
end;
```

Definition 3.5 denotes that $\mathbb{F}_p$-rational points on the elliptic curve are points satisfying the definition equation "`EC_WEqProjCo(a,b,p).P = 0`."

4 Number of $\mathbb{F}_p$-rational points on an elliptic curve

In this section, we explain the definitions and theorems related to the number of $\mathbb{F}_p$-rational points on an elliptic curve over $\mathbb{F}_p$. The number of $\mathbb{F}_p$-rational points on an elliptic curve is counted without the equivalence of the projective coordinates.

4.1 Legendre symbol

The number of $\mathbb{F}_p$-rational points on an elliptic curve can be calculated by using Legendre symbols. Legendre symbols are related to the quadratic residue defined as follows:

Definition 4.1 (Quadratic residue)

```
definition let p, a;
  attr a is quadratic_residue means
  a <> 0 & ex x being Element of GF(p) st x|^2 = a;
  attr a is not_quadratic_residue means
  a <> 0 & not ex x being Element of GF(p) st x|^2 = a;
end;
```

Definition 4.1 indicates that $a(\neq 0 \bmod p)$ is a quadratic residue when x exists such that $x^2 = a$, and is not a quadratic residue when x does not exist.

Legendre symbols $(\frac{a}{p})$ ("`Lege_p(a)`") are defined as follows:

Definition 4.2 (Legendre symbol)

```
definition let p, a;
  func Lege_p(a) -> Integer equals
  0 if a = 0,
  1 if a is quadratic_residue
  otherwise -1;
end;
```

Definition 4.2 denotes that

- $(\frac{a}{p}) = 0$ when $a = 0 \bmod p$,
- $(\frac{a}{p}) = 1$ when $a(\neq 0 \bmod p)$ is a quadratic residue, and
- $(\frac{a}{p}) = -1$ when $a(\neq 0 \bmod p)$ is not a quadratic residue.

The number of solutions of a second-degree equation $b^2 = a$ over $\mathbb{F}_p$ is related to the Legendre symbol as follows:

Theorem 4.3 (Number of solutions of the second-degree equation)

```
theorem
  2 < p implies card({b : b|^2 = a}) = 1 + Lege_p(a);
```

Theorem 4.3 indicates that the number of solutions of the equation $b^2 = a$ over $\mathbb{F}_p$ is equal to $1 + (\frac{a}{p})$.

4.2 Relationship between Legendre symbols and the number of $\mathbb{F}_p$-rational points on an elliptic curve

An $\mathbb{F}_p$-rational point is equivalent to $[0, 1, 0]$ or $[X, Y, 1]$ $(X, Y \in \mathbb{F}_p)$ as per the following theorem:

Theorem 4.4 (Equivalence of points on an elliptic curve)

```
theorem
  for p be Prime, a, b be Element of GF(p), x be set st
  p > 3 & Disc(a,b,p) <> 0.GF(p)
  & x in Class (R_EllCur(a,b,p)) holds
```

```
( ex P be Element of ProjCo(GF(p)) st P in EC_SetProjCo(a,b,p)
& P=[0,1,0]
& x = Class(R_EllCur(a,b,p),P) ) or
ex P be Element of ProjCo(GF(p)), X,Y be Element of GF(p)
st P in EC_SetProjCo(a,b,p) & P=[X,Y,1]
& x = Class(R_EllCur(a,b,p),P);
```

Here, "`Class(R_EllCur(a,b,p).P)`" is an equivalence class of P defined by the equivalence relation in Definition 3.2. "`Class(R_EllCur(a,b,p))`" denotes all the equivalence classes, that are a set of $\mathbb{F}_p$-rational points. By Theorem 4.4, the following theorem of equivalence classes holds:

Theorem 4.5 (Equivalence classes of points on an elliptic curve)

```
theorem
  for p be Prime, a, b be Element of GF(p) st
  p > 3 & Disc(a,b,p) <> 0.GF(p) holds
  Class (R_EllCur(a,b,p)) = {Class(R_EllCur(a,b,p),[0,1,0])}
  \/ {Class(R_EllCur(a,b,p),P)
  where P is Element of ProjCo(GF(p)):
  P in EC_SetProjCo(a,b,p) & ex X,Y be Element of GF(p)
  st P=[X,Y,1]};
```

Theorem 4.5 indicates that the set of all equivalence classes of $\mathbb{F}_p$-rational points consists of an equivalence class including $[0,1,0]$ and equivalence classes including $[X,Y,1]$.

We count the equivalence classes to calculate the number of $\mathbb{F}_p$-rational points on an elliptic curve (cardinality of the equivalence classes). For this purpose, we prove the following:

(1) the equivalence class of $[0,1,0]$ and the equivalence classes of $[X,Y,1]$ are disjoint, and

(2) the equivalence class of $[X_1,Y_1,1]$ and the equivalence of class $[X_2,Y_2,1]$ $(X_1 \neq X_2)$ are disjoint.

(1) is described by the following theorem:

Theorem 4.6 (Relationship of equivalence classes 1)

```
theorem
  for p be Prime, a, b be Element of GF(p),
  F1,F2 be set st p > 3 & Disc(a,b,p) <> 0.GF(p)
  & F1 = {Class(R_EllCur(a,b,p),[0,1,0])} &
  F2 = {Class(R_EllCur(a,b,p),P) where P is
  Element of ProjCo(GF(p)): P in EC_SetProjCo(a,b,p) &
  ex X,Y be Element of GF(p) st P=[X,Y,1]} holds F1 misses F2;
```

(2) is described by the following theorem:

Theorem 4.7 (Relationship of equivalence classes 2)

```
theorem
  for p be Prime, a, b, X1, Y1, X2, Y2 be Element of GF(p)
  st p > 3 & Disc(a,b,p) <> 0.GF(p)
  & [X1,Y1,1] in EC_SetProjCo(a,b,p)
  & [X2,Y2,1] in EC_SetProjCo(a,b,p) holds
  Class(R_EllCur(a,b,p),[X1,Y1,1]) =
  Class(R_EllCur(a,b,p),[X2,Y2,1]) iff X1=X2 & Y1=Y2;
```

Theorem 4.7 indicates that

$$\begin{aligned}&(\text{equivalence class of } [X_1, Y_1, 1]) = (\text{equivalence class of } [X_2, Y_2, 1])\\ &\Leftrightarrow X_1 = X_2 \,\&\, Y_1 = Y_2.\end{aligned} \tag{4.1}$$

A contraposition of Theorem 4.7 is (2).

The number of equivalence classes of $[X, Y, 1]$ is equal to that of the solutions of the second-degree equation $Y^2 = X^3 + aX + b$ by the definition equation $Y^2Z - (X^3 + aXZ^2 + bZ^3) = 0$ of the elliptic curve. Therefore, the following theorem holds by Theorem 4.3:

Theorem 4.8 (Relationship between the X-coordinate and the number of points)

```
theorem
  for p be Prime, a, b, X be Element of GF(p)
  st p > 3 & Disc(a,b,p) <> 0.GF(p) holds
  card ({Class(R_EllCur(a,b,p),[X,Y,1])
  where Y is Element of GF(p) : [X,Y,1] in EC_SetProjCo(a,b,p)})
  = 1 + Lege_p(X|^3 + a*X + b);
```

By Theorem 4.6, 4.7, and 4.8,

$$1 + \sum_{X=0}^{p-1} \left\{ 1 + \left(\frac{X^3 + aX + b}{p} \right) \right\} = 1 + p + \sum_{X=0}^{p-1} \left(\frac{X^3 + aX + b}{p} \right). \tag{4.2}$$

Hence, the following theorem holds:

Theorem 4.9 (Number of $\mathbb{F}_p$-rational points on an elliptic curve)

```
theorem
  for p be Prime, a, b be Element of GF(p)
  st p > 3 & Disc(a,b,p) <> 0.GF(p)
  ex F be FinSequence of INT st len F = p &
  (for n be Nat st n in Seg p ex d be Element of GF(p)
  st X=n-1 & F.n = Lege_p(X|^3 + a*d + b)) &
  card(Class(R_EllCur(a,b,p))) = 1 + p + Sum(F);
```

5 Operation of points on an elliptic curve

This section describes an operation on points on an elliptic curve. An addition operation of points on the elliptic curve that has an identity element $O = [0, 1, 0]$ is defined in this section.

An inversion element $-P = [X_P, -Y_P, Z_P]$ of $P = [X_P, Y_P, Z_P]$ is defined as follows:

Definition 5.1 (Inversion element of a point on an elliptic curve)

```
definition
  let p be 5_or_greater Prime;
  let z be Element of EC_WParam p;
  func compell_ProjCo(z,p) ->
  Function of EC_SetProjCo(z‘1,z‘2,p), EC_SetProjCo(z‘1,z‘2,p)
  means
  for P be Element of EC_SetProjCo(z‘1,z‘2,p)
  holds it.P = [P‘1,-P‘2,P‘3];
end;
```

Here, "`compell_ProjCo(z,p).P`" denotes $-P$, and "`z‘1`" and "`z‘2`" denote a and b, respectively. `EC_WParam p` indicates the parameters a, b satisfying that the discriminant $\delta = 4a^3 + 27b^2 \neq 0 \bmod p$.

$Y_P = -Y_P$ and $Y_P = 0$ (because $p > 3$) hold in the following theorem since $P = -P \neq O \Rightarrow [X_P, Y_P, Z_P] = [X_P, -Y_P, Z_P]$:

Theorem 5.2 (2-torsion point)

```
theorem
  for p be 5_or_greater Prime, z be Element of EC_WParam p,
  P be Element of EC_SetProjCo(z‘1,z‘2,p) st P‘3 <> 0 holds
  P _EQ_ compell_ProjCo(z,p).P iff P‘2 = 0;
```

As $P = -P \Rightarrow P + P = 2P = O$, the above P is called a 2-torsion point.

A set of $\mathbb{F}_p$-rational points on the elliptic curve has the structure of an Abelian group by the following operation:

Definition 5.3 (Addition operation on points on an elliptic curve)

```
definition
  let p be 5_or_greater Prime,
      z be Element of EC_WParam p;
  func addell_ProjCo(z,p) -> Function of
  [:EC_SetProjCo(z‘1,z‘2,p),EC_SetProjCo(z‘1,z‘2,p):],
  EC_SetProjCo(z‘1,z‘2,p) means
  for P, Q, O being Element of EC_SetProjCo(z‘1,z‘2,p)
  st O = [0,1,0]
  holds
  (P _EQ_ O implies it.(P,Q) = Q) &
  ((Q _EQ_ O & not P _EQ_ O) implies it.(P,Q) = P) &
  ((not P _EQ_ O & not Q _EQ_ O & not P _EQ_ Q) implies
```

```
  for g2, u, v, A being Element of GF(p) st g2 = 2 mod p &
  u = Q‘2*P‘3 - P‘2*Q‘3 &
  v = Q‘1*P‘3 - P‘1*Q‘3 &
  A = (u |^2)*P‘3*Q‘3 - (v |^3) - g2*(v |^2)*P‘1*Q‘3
  holds it.(P,Q) = [v*A, u*((v |^2)*P‘1*Q‘3-A) - (v |^3)*P‘2*Q‘3,
  (v |^3)*P‘3*Q‘3]) &
  ((not P _EQ_ 0 & not Q _EQ_ 0 & P _EQ_ Q) implies
  for g2, g3, g4, g8, w, s, B, h being Element of GF(p) st
  g2 = 2 mod p & g3 = 3 mod p & g4 = 4 mod p & g8 = 8 mod p &
  w = (z‘1)*(P‘3 |^2) + g3*(P‘1 |^2) &
  s = P‘2*P‘3 &
  B = P‘1*P‘2*s &
  h = (w |^2) - g8*B
  holds it.(P,Q) = [g2*h*s, w*(g4*B-h) - g8*(P‘2 |^2)*(s |^2),
  g8*(s |^3)]);
end;
```

Definition 5.3 indicates that the addition operation $(+)$ for $P = [X_P, Y_P, Z_P]$, $Q = [X_Q, Y_Q, Z_Q]$, and $R = P + Q = [X_R, Y_R, Z_R]$ is defined as follows:

(1) in the case that $P = O$, $R = Q$;

(2) in the case that $P \neq O$ and $Q = O$, $R = P$;

(3) in the case that $P \neq O,\ Q \neq O$ and $Q \neq P$,

$$X_R = vA \tag{5.1}$$
$$Y_R = u(v^2 X_P Z_Q - A) - v^3 Y_P Z_Q \tag{5.2}$$
$$Z_R = v^3 Z_P Z_Q \tag{5.3}$$

, where $u = Y_Q Z_P - Y_P Z_Q,\ v = X_Q Z_P - X_P Z_Q,\ A = u^2 Z_P Z_Q - v^3 - 2v^2 X_P Z_Q$; and

(4) in the case that $P \neq O,\ Q \neq O$ and $Q = P$,

$$X_R = 2hs \tag{5.4}$$
$$Y_R = w(4B - h) - 8Y_P^2 s^2 \tag{5.5}$$
$$Z_R = 8s^3 \tag{5.6}$$

, where $w = aZ_P^2 + 3X_P^2,\ s = Y_P Z_P,\ B = X_P Y_P s,\ h = w^2 - 8B$.

We must prove that "`addell_ProjCo(z,p).(P,Q)`" (called "`R`") is in "`EC_SetPorjCo(z‘1,z‘2,p)`" to show that the above operation "`addell_ProjCo(z,p)`" is defined in points on the elliptic curve over $\mathbb{F}_p$. This is shown by proving the following propositions:

(a) `R` is included in `ProjCo(GF(p))`, i.e., `addell_ProjCo(z,p).(P,Q)` is not equal to `[0, 0, 0]`, and

(b) `R` satisfies `EC_WEqProjCo(z‘1,z‘2,p).R = 0.GF(p)`.

(a) naturally holds in cases (1) and (2) in Definition 5.3. In case (3), (a) is satisfied as follows:

- in the case that $P = -Q$, as $v = 0$ and $u \neq 0$ by Definition 5.3, $Y_R \neq 0$, and
- in the case that $P \neq -Q$, as $v \neq 0$ by Definition 5.3, $Z_R \neq 0$.

In case (4), (a) is satisfied as follows:

- in the case that $Y_P = 0$ (that is P is a 2-torsion point), as $w \neq 0$, $Y_R \neq 0$, and
- in the case that $Y_P \neq 0$, as $s \neq 0$, $Z_R \neq 0$.

Here, $w \neq 0$ holds in the case that $Y_P = 0$ by the following theorem:

Theorem 5.4 (Discriminant of an elliptic curve and a 2-torsion point)

```
theorem
  for p be 5_or_greater Prime, z be Element of EC_WParam p,
  g3 be Element of GF(p), P be Element of EC_SetProjCo(z‘1,z‘2,p)
  st g3 = 3 mod p & P‘2 = 0 & P‘3 <> 0 holds
  (z‘1)*(P‘3 |^2) + g3*(P‘1 |^2) <> 0;
```

Theorem 5.4 indicates that for $P \neq O$ satisfying $Y_P = 0$, $w \neq 0$ holds. The theorem is proved by using the characteristic that the discriminant $\delta \neq 0$(a 2-torsion point P is non-singular).

As (b) mentioned above (`R` satisfies `EC_WEqProjCo(z‘1,z‘2,p).R = 0.GF(p)`) is proved by using complicated transformation of equations, we omit its explanation.

6 Conclusion and future work

In this paper, we introduced our formalization of the definitions and theorems related to an elliptic curve over a finite prime field $\mathbb{F}_p$. We explained in detail the definitions and theorems of a finite prime field, an elliptic curve over $\mathbb{F}_p$, and an operation of points on the elliptic curve. The correctness of our formalization of the definitions and theorems was proved using a formal verification tool in the Mizar proof-checking system. Our formalizations are very important to prove the security of the ECC.

The operation on points on the elliptic curve can construct an Abelian group from a set of $\mathbb{F}_p$-rational points on the elliptic curve. For the construction, we need to prove the commutative law ($P + Q = Q + P$) and the associative law ($P+(Q+R) = (P+Q)+R$) of the operation. However, we have not formalized these laws yet. We plan to formalize these laws and complete the formalization of the Abelian group constructed from the set of $\mathbb{F}_p$-rational points on the elliptic curve in the near future. We will also formalize other definitions and theorems related with cryptosystems, particularly those used in the ECC.

References

[1] Mizar Proof Checker, *Available at* `http://mizar.org/`

[2] E.Bonarska, An Introduction to PC Mizar, Mizar Users Group, Fondation Philippe le Hodey, Brussels (1990)

[3] Y.Futa, H.Okazaki and Y.Shidama, "Set of Points on Elliptic Curve in Projective Coordinates", Formalized Mathematics (2011, to appear)

[4] I.Blake, G.Seroussi and N.Smart, "Elliptic Curves in Cryptography", London Mathematical Society Lecture Note Series, No. 265, Cambridge University Press (1999)

[5] C.Byliński, "Binary Operations", Formalized Mathematices vol.1, no.1, 175–180 (1990)

[6] J.Trybulec, "Integers", Formalized Mathematics, vol.1, no.3, 501–505 (1990)

[7] G.Bancerek, "Cardinal Numbers", Formalized Mathematics vol.1, no.2, 377–382 (1990)

[8] K.Raczkowski and P.Sadowski, "Equivalence Relations and Classes of Abstraction", Formalized Mathematics, vol.1, no.3, 441–444 (1990)

[9] C.Schwarzweller, "The Ring of Integers, Euclidean Rings and Modulo Integers", Formalized Mathematics, vol.8, no.1, 29–34 (1999)

[10] A.Trybulec, "Tuples, Projections and Cartesian Products", Formalized Mathematics, vol.1, no.1, 97–105 (1990)

[11] W.A.Trybulec, "Vectors in Real Linear Space", Formalized Mathematics, vol.1, no.2, 291–296 (1990)

[12] E.Kusak, W.Leonczuk, and M.Muzalewski, "Abelian Groups, Fields and Vector Spaces", Formalized Mathematics, vol.1, no.2, 335–342 (1990)

至る所良い還元を持つ楕円曲線について：計算機的手法とその最近の進展

On elliptic curves having everywhere good reduction: Computational approach and its recent progress

横山 俊一（九大数理） Shun'ichi Yokoyama (Kyushu University)

概要 至る所良い還元を持つ楕円曲線については, 長年の研究によって主に実二次体上及び虚二次体上の場合について深く研究されており, 保型性予想との関連からも非常に興味深い. 本講演ではこの分野における最近の進展状況を（講演者の結果を交えて）報告する. また二次体以外の場合についても言及し, 解決に向けたアイデアを提唱したい. なお, 本研究の一部は島崎有氏（九大数理）との共同研究である.

Abstract Determination problem of elliptic curves having everywhere good reduction (especially over some real and imaginary quadratic fields) is very interesting and important problem from the viewpoint of modularity conjecture. In this talk, we report recent progress including our latest result. We also explain other cases with some ideas to solve. This work is partly joint work with Yu Shimasaki (Kyushu University).

1 問題提起

次の問題を考える：

> **問題** 代数体 K を一つとって固定する. この時 K 上至る所良い還元（everywhere good reduction: 以下 e.g.r. と略記）を持つ楕円曲線は同型を除いて幾つ存在するか？ 存在しない場合はそれを証明出来るか？

最も簡単な例として $K=\mathbb{Q}$ の場合には存在しないことが古くから知られている（Tate の結果）. また, 虚二次体 $K=\mathbb{Q}(\sqrt{-d})$（$d>0$, square-free）の場合は次の大きな規準が知られている.

定理 1.1 (Setzer '78 [16], Stroeker '83 [17])**.** K を虚二次体とする. この時 K の類数が 6 と素ならば K 上 e.g.r. な楕円曲線は存在しない.

虚二次体の場合には, 他にも石井秀則氏（'86 [5]）や木田雅成氏（'01 [14]）らによって散在的に非存在性が知られている. 一方, 存在性が示されているのは Setzer による次の規準だけである. ここでは admissible な曲線という, e.g.r. な曲線の特別なクラスが扱われている.

定義 1.2. 楕円曲線 E が K 上の **admissible curve** であるとは, K 上 e.g.r. であって位数 2 の K_d-有理点を持つことをいう.

定理 1.3 (Setzer '78 [16])**.** 虚二次体 $K=\mathbb{Q}(\sqrt{-d})$ 上 admissible な曲線が存在するための必要十分条件は, $d=65m_1$ でかつ $\underline{m_1\text{: square mod 5 and 13}}$ および $\underline{65\text{: square mod } m_1}$ を満たすことである.

これを用いると比較的容易に admissible な楕円曲線の族が求まる. 例えば

$$m=-65,-910,-1885,-3315,-3965,\cdots$$

などがある. その一方で, 基礎体が実二次体 $K_d=\mathbb{Q}(\sqrt{d})$（$d>0$, square-free）の場合は Setzer らのような統一的な基準は存在せず[1], 散在的な結果が蓄積されている. 現時点（2011 年 11 月現在）における結果は $d\leq 100$ に限定すると次の通りである.

[1] 規準にあたるものが無いわけではない（実際, これから詳しく述べる）. 例えば [5] にある「p が 8 を法として 5 と合同な素数で, $K=\mathbb{Q}(\sqrt{p})$ の類数が 3 と素な時, K 上 admissible な曲線は存在しない」などがある. 何れにしても, 虚二次体上のケースのように simple な規準は今のところ見つかっていない.

定理 1.4. 1. $d = 2, 3, 5, 10, 11, 13, 15, 17, 19, 21, 23, 30, 31, 34, 35, 39, 42, 43, 46, 47, 53, 55, 57, 58, 59, 61, 66, 69, 70, 73, 74, 78, 82, 83, 85, 89, 93, 94, 95, 97$ のとき, K_d 上 e.g.r. な楕円曲線は存在しない.

2. $d = 6, 7, 14, 22, 29, 33, 37, 38, 41, 65, 77$ のとき, K_d 上 e.g.r. な楕円曲線は全て決定されている.

3. $d = 26, 79, 86$ のとき, K_d 上 e.g.r. な楕円曲線が発見されている（これで全部か否かは証明されていない）.

4. $d = 62, 67, 71$ のとき K_d 上 e.g.r. な楕円曲線で判別式が 3 乗数となるようなものは存在しない.

この方面で大きく貢献したのは加川貴章氏（[6], [7], [8], [9], [10], [11]）である. また先ほど紹介した木田氏（[12], [13]）や, 両名の共著論文（'97 [15]）などにも詳しい. 最近著者（横山）はこの手法をベースとして計算機的限界まで改良を進め, 現存する実装で best-possible な結果を得た（'11 [22] および現在準備中の [20]）. これについては 2 章に述べる.

更に本研究を進めている最中, 日本国外においてもこの分野で大きな進展があった. University of Warwick に所属している計算機数論の大家 John Cremona 氏とその学生, OB 達のチームによるものである. ここ 10 年来は, 一般の代数体 K 上の楕円曲線の計算を可能にする descent package を独自に実装し, 種々の結果を残している. これについて 3 章で解説する.

最後に, 二次体以外への拡張例として純三次体上の同様の問題について考察する. この方面における結果は現時点では 1 つしかなく（Bertolini-Canuto '88 [1]）, ほぼ未開拓のケースである. これを 4 章で述べる.

2 最近の進展 I

まずこの章では, 加川氏の手法をベースとして得られた著者の結果を紹介する. 詳細な解説は [21] を参照願いたい. ここでは簡単にその内容を概説する. まず Setzer の定理 [16] から始めよう.

命題 2.1 (Setzer [16])**.** E を K_d 上の楕円曲線とする. K_d の類数が 6 と素であれば E は global minimal model を持つ.

以降 E は K_d 上 e.g.r. な楕円曲線とする. このとき E の global minimal model は

$$E:\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

と書ける（$a_i \in \mathcal{O}_{K_d}$ $(i = 1, 2, 3, 4, 6)$）. この判別式 $\Delta(E)$ は

$$\Delta(E) = \frac{c_4^3 - c_6^2}{1728}$$

と $c_4, c_6 \in \mathcal{O}_{K_d}$ を用いて表される. ここで次の 2 条件が同値であることを使う：

- E は K_d 上至る所 good reduction を持つ,
- $\Delta(E) \in \mathcal{O}_{K_d}^{\times}$.

二次体の一般論より, $\mathcal{O}_{K_d}^{\times}$ の元は全て K_d の基本単数 ε を用いて $\pm\varepsilon^n$ の形で表される（以降, K_d を一つとるごとに ε を固定して考える）. 従って $c_4, c_6 \in \mathcal{O}_{K_d}$ の候補は全て

$$E_n^{\pm}(\mathcal{O}_{K_d}) = \left\{(x, y) \in \mathcal{O}_{K_d} \times \mathcal{O}_{K_d} \mid\ y^2 = x^3 \pm 1728\varepsilon^n\right\},\ \ 0 \le n < 12$$

に含まれることが分かり, このような整数点の集合を決定する問題に帰着される. 更にこれらは絞り込み可能であり, 例えば次のようなものが知られている.

補題 2.2. 次の 5 つの条件を全て満たすならば, K_d 上 e.g.r. な楕円曲線の判別式は必ず K_d の 3 乗数となる：

1. K_d の類数は 6 と素.
2. 3 は K_d 上不分岐.
3. $K_d(\sqrt{-3})$ の類数は 3 で割れない.
4. $K_d(\sqrt[3]{\varepsilon})$ の類数は 2 で割れない.
5. 3 を割る K_d の素イデアル $\mathfrak{p}$ に対し, $X^3 \equiv \varepsilon \pmod{\mathfrak{p}^3}$ は解 $X \in \mathcal{O}_{K_d}$ を持たない.

補題 2.3. K_d を実二次体, E を K_d 上定義された楕円曲線とする. E が 2 の外で e.g.r. で, 更に位数 2 の K_d-有理点を持たなければ, $K_d(E[2])/K_d(\sqrt{\Delta(E)})$ は 2 の外不分岐な巡回 3 次拡大となる. 特に $K_d(\sqrt{\Delta(E)})$ の ray class number mod $\prod_{\mathfrak{p}|2}\mathfrak{p}$ は 3 で割り切れる.

候補が決まれば, 後は整数点の計算を Mordell-Weil 群 $E_n^{\pm}(K_d)$ の計算に帰着し, elliptic logarithm の手法を用いて整数点の集合を決定すれば良い. この方針で計算機的改良を進め, $d \leq 200$ に対して現時点で最良と思われる結果まで拡張を行った. admissible curve と呼ばれる曲線を決定する Comalada の規準 [2] と合わせると次の通りである.

定理 2.4 (Y.-Shimasaki '11 [22], Y. [20])**.**

1. $d = 43, 46, 59, 103, 137$ のとき, K_d 上 e.g.r. な楕円曲線は存在しない.
2. $d = 118, 134, 161, 166$ のとき, K_d 上 admissible な曲線が存在する.
3. $d = 62, 67, 71, 139, 151$ のとき K_d 上 e.g.r. な楕円曲線で判別式が 3 乗数となるようなものは存在しない.
4. $d = 107, 127, 131, 163, 179, 199$ のとき, K_d 上 admissible な曲線は存在しない.
5. $d = 158, 161$ のとき, admissible ではない e.g.r. な楕円曲線が存在する.
   (a) $d = 158$ の時, E は $y^2 + xy + \sqrt{158}y = x^3 - x^2 + Ax + B$ で与えられる. ここに
   $$\begin{aligned} A &= -361817559192191668851 - 287846594758031454 15\sqrt{158} \\ B &= 369128833319186381273841768 1108 \\ &\quad +293663132146367649175848062813\sqrt{158} \end{aligned}$$
   である.
   (b) $d = 161$ の時, E は $y^2 + xy + y = x^3 - x^2 + Cx + D$ で与えられる. ここに
   $$\begin{aligned} C &= -3680 + 290\sqrt{161} \\ D &= -148482 + 11702\sqrt{161} \end{aligned}$$
   である.

これらを纏めた存在・非存在の表を, 著者のウェブページ

`http://www2.math.kyushu-u.ac.jp/~s-yokoyama/ECtable.html`

にて公開・随時更新しているので, 興味のある方は参照頂きたい. なおデータの誤り等, 何かお気付きの点を見つけられた際には, ご連絡を頂ければ幸甚である. 現時点での $d \leq 200$ で未解決かつ類数 1 の場合に関するデータ（ウェブページ非公開, 但し [20] に同一の表を掲載）を Appendix A に示す（5 章の後）.

3 最近の進展 II

本稿の後半は, 最近の大きな進展として Cremona-Thongjunthug の結果を紹介する. 論文としては Thongjunthug 氏単著の [18] および Cremona 氏との共著 [4] が挙げられるが, これらは Thongjunthug 氏の博士論文 [19] で賄える.

最初に補足しておくが, 氏の学位論文は e.g.r. な楕円曲線を主として扱ったものではない. 主な成果は, 代数体（研究初期は総実代数体）上の楕円曲線の canonical height の bound の改善と, 楕円曲線の period lattice（と elliptic logarithm）の理論の $\mathbb{R}$ 上から $\mathbb{C}$ 上への拡張である. e.g.r. な楕円曲線の計算は, これらの定理の応用として導かれたものである. e.g.r. な楕円曲線の計算を行うには, Cremona-Lingham の手法 [3] およびこれに準じた実装を用いる. 以降は主にこの手法の解説である.

定義 3.1. K を代数体, $\mathcal{O}_K$ をその整数環とし, $\mathcal{S}$ を $\mathcal{O}_K$ の素イデアルの有限集合とする. この時 $x \in K$ が **$\mathcal{S}$-integer** であるとは, 全ての $\mathfrak{p} \notin \mathcal{S}$ に対して $\mathrm{ord}_{\mathfrak{p}}(x) \geq 0$ が成り立つことをいう.

$\mathcal{S}$-integer の集合は環をなす（これを $\mathcal{O}_{K,\mathcal{S}}$ で表す）. 続いて $m \in \mathbb{Z}_{\geq 0}$ とし, 次のような集合を定義する.

$$K(\mathcal{S}, m) = \{x \in K^*/K^{*m} \mid \mathrm{ord}_{\mathfrak{p}}(x) \equiv 0 \pmod{m} \text{ for all } \mathfrak{p} \notin \mathcal{S}\}$$

ここに $K^* = K \setminus \{0\}$ である. 以降文脈においては $x \in K^*$ が $K(\mathcal{S}, m)$ の元であることを $xK^{*m} \in K(\mathcal{S}, m)$ であることと解釈して使用する. $K(\mathcal{S}, m)$ については次の性質が成り立つ.

命題 3.2. m, n を互いに素な整数とする時,

$$K(\mathcal{S}, mn) \simeq K(\mathcal{S}, m) \times K(\mathcal{S}, n)$$

が成り立つ. ここに各元は $w \mapsto (w, w)$ で写り, 逆写像は $am + bn = 1$ として $(u, v) \mapsto v^{am}u^{bn}$ で定義される.

e.g.r. な楕円曲線を計算する上では, 特に $m = 4, 6, 12$ の場合と, natural map $K(\mathcal{S}, 12) \to K(\mathcal{S}, 6)$ の像（これを $K(\mathcal{S}, 6)_{12}$ と書く）の計算が必要になる. そのためには上の命題より, $m = 2, 3, 4$ の計算が出来れば十分である. m が素数の場合, 即ち $m = 2, 3$ の時は既に Magma の組み込み関数（例えば `pSelmerGroup` などがある）が用意されており, 残る $m = 4$ の場合は Cremona 氏によって実装が与えられている.

それでは楕円曲線を登場させよう. E を K 上の楕円曲線とし, その Weierstrass model は 2 章で与えたものと同一の表記を用いる.

定義 3.3. E が $\mathfrak{p}$ で**良い還元**（good reduction at $\mathfrak{p}$）を持つとは, $\mathfrak{p}$-integral model（i.e. 任意の j に対して $\mathrm{ord}_{\mathfrak{p}}(a_j) \geq 0$）を持ち, 更にその model の判別式が $\mathfrak{p}$-unit（i.e. $\mathrm{ord}_{\mathfrak{p}}(\Delta) = 0$）となるときを言う.

K 上 $\mathcal{S}$ の外で e.g.r. な楕円曲線は, 同型を除いて有限個しかないことが良く知られている. 次の命題はそのような楕円曲線と $K(\mathcal{S}, 6)_{12}$ との関係性を示唆している.

命題 3.4. E を K 上 $\mathcal{S}$ の外で e.g.r. な楕円曲線で, j-不変量 $j(E)$ は 0 でも 1728 でもないとする. この時 $w = j^2(j - 1728)^3$ とすると

$$\Delta \in K(\mathcal{S}, 12), \quad j \in \mathcal{O}_{K,\mathcal{S}}, \quad w \in K(\mathcal{S}, 6)_{12}$$

が成り立つ. 逆に $j \in \mathcal{O}_{K,\mathcal{S}}$ で $w = j^2(j - 1728)^3 \in K(\mathcal{S}, 6)_{12}$ とすると, 楕円曲線

$$E^{\#} : \ y^2 = x^3 - 3u^2 j(j - 1728)x - 2u^3 j(j - 1728)^2$$

は $j(E^{\#}) = j$ を満たし, 更に $\mathcal{S}^{(6)} = \mathcal{S} \cup \{\mathfrak{p} \mid \mathrm{ord}_{\mathfrak{p}}(6) > 0\}$ の外で e.g.r. である. ここに $u \in K^*$ は $(3u)^6 w \in K(\mathcal{S}, 12)$ を満たす.

上の命題の後半から $\mathcal{S}$（$\mathcal{S}^{(6)}$ ではない）の外で e.g.r. な楕円曲線の全リストを得るには $\mathfrak{p} \mid 6$ を満たす全ての素点 $\mathfrak{p}$ での reduction を見る必要がある．更に E の quadratic twist $E^{(u)}$（$u \in K(\mathcal{S}, 2)$）も調べあげて, リストが完成する．

続いてもう一つの命題を紹介する．これにより, j の候補を決定することがある種の楕円曲線の整数点を求める問題に帰着される．ここから先は 2 章のそれと殆ど同じである．まずは整数点の定義を復習しておく．

定義 3.5. 記号は前述の通りとする．$P = (x, y) \in E(K)$ が **$\mathcal{S}$-integral point** であるとは, x, y が何れも $\mathcal{O}_{K,\mathcal{S}}$ の元であることをいう．特に $\mathcal{S} = \emptyset$ である場合（つまり $\mathcal{O}_{K,\mathcal{S}} = \mathcal{O}_K$ の場合）は, 単に P を **integral point** と呼ぶ.

命題 3.6. $w \in K(\mathcal{S}, 6)$ とする．$j^2(j-1728)^3 \equiv w \pmod{K^{*6}}$ を満たす各 $j \in \mathcal{O}_{K,\mathcal{S}} \setminus \{0, 1728\}$ は

$$j = \frac{x^3}{w} = 1728 + \frac{y^2}{w}$$

で与えられる．ここに $P = (x, y)$（$xy \neq 0$）は楕円曲線

$$E_w : \ y^2 = x^3 - 1728w$$

の $\mathcal{S}$-integral point である．

以上の手法を e.g.r. な楕円曲線の探索に応用したければ, $\mathcal{S} = \emptyset$ とすれば良い．これらを纏めると, procedure は以下のように与えられる．

1. $K(\emptyset, 2)$, $K(\emptyset, 3)$ から $K(\emptyset, 6)$ を計算し, 更に $w \in K(\emptyset, 6)_{12}$ から与えられる representative set W を決定する．W は常に有限集合である．
2. 各 $w \in W$ に対し, E_w の整数点であって $j = x^3/w \in \mathcal{O}_K$ を満たすようなものを全て決定する．
3. もしも j が $j^2(j-1728)^3 \in K(\emptyset, 6)_{12}$ を満たすならば, $(3u_0)^6 j^2(j-1728)^3 \in K(\emptyset, 12)$ を満たすような $u_0 \in K^*$ を全て決定する．更に楕円曲線

   $$E^{\#} : \ y^2 = x^3 - 3u_0^2 j(j-1728)x - 2u_0^3 j(j-1728)^2$$

   が $\mathfrak{p} \mid 6$ を満たす全ての素点で良い還元を持つかどうかを調べる．そうでなければ除去する（候補から外す）．
4. quadratic twist $E^{(u)}$（$u \in K(\emptyset, 2)$）に対しても 3. を適用する．

上の procedure は $j(E) \neq 0, 1728$ を満たすものにしか適用出来ないが, $j(E) = 0$ の場合についてはそのような楕円曲線は存在しないことが知られている．また $j(E) = 1728$ の場合も考慮の必要がないことが分かっている．詳細は [3] を参照されたい.

以上の手法と Cremona による実装を用いて得られた結果は, $d \leq 100$ に限定すれば次の通りである．なお, この結果は既に定理 1.4 に組み込んでいる．

定理 3.7 (Thongjunthug '11 [19])**.** 次が成り立つ（$K = \mathbb{Q}(\sqrt{d})$）.

1. $d = 55, 78, 95$ のとき, K_d 上 e.g.r. な楕円曲線は存在しない.
2. $d = 38, 41, 65$ のとき, K_d 上 e.g.r. な楕円曲線は全て決定されている.

また, 虚二次体上の場合についても言及されている.

定理 3.8 (Thongjunthug '11 [19])**.** $d = 26, 29, 31, 59, 83, 87$（$K = \mathbb{Q}(\sqrt{-d})$）のとき, K_d 上 e.g.r. な楕円曲線は存在しない.

4 ひとつの拡張

最後に二次体からの一般化として, 純三次体の場合を考察する. この場合は基礎体が総実ではないため, 保型性予想の観点からも興味深い. このケースにおいて知られている結果は次の一つだけである.

定理 4.1 (Bertolini-Canuto '88 [1])**.** $\mathbb{Q}(\sqrt[3]{2})$ 上 e.g.r. な楕円曲線は存在しない.

当時は勿論代数体上の楕円曲線の計算はおろか, 諸構造の計算も不可能であった. 従ってここでは計算機を用いず, 幾つかの不定方程式系を解くことと $\mathbb{Q}(\sqrt[3]{2})$ の構造を活用することによって証明している. 大まかには

1. もし $\mathbb{Q}(\sqrt[3]{2})$ 上 e.g.r. な楕円曲線が存在すれば, それらは全て admissible である.
2. しかし $\mathbb{Q}(\sqrt[3]{2})$ 上 admissible な楕円曲線は存在しない.

という 2 部構成で証明が進む. 現在では計算機環境の充実により, 前半に相当する部分は瞬時に片付くようになったが, 後半は依然不定方程式の問題として残り, この手法を一般化する（他の場合に適用出来るよう書き換える）ことは得策とは思われない. また, 前半部分の証明に関しても, 他の場合への適用は煩雑さを増すだけであり, こちらも宜しくない.

そこで本稿では, 前半部分に限ってこれまでの二次体上の手法を適用して得られた結果を紹介する. これは命題 2.1 と補題 2.3 において, 基礎体を一般の代数体に取り替えても成立することが鍵となっている. 現時点で計算出来る限りの結果は次の通りである. 以降 $L_d = \mathbb{Q}(\sqrt[3]{d})$ は類数 1 とし, $1 \leq d \leq 200$ かつ d は cubic-free を仮定する. 詳細はプレプリント [20] を参照頂きたい.

定理 4.2 (Yokoyama '11 [20])**.**

1. $d = 3, 4, 5, 6, 9, 10, 12, 17, 18, 25, 29, 36, 100, 116, 137, 173, 197$ の時, もし L_d 上 e.g.r. な楕円曲線が存在すれば, それらは全て admissible である. 即ちこのケースでは e.g.r. であるならば位数 2 の L_d-有理点を必ず持つ.
2. $d = 23, 44, 45, 75, 87$ の時, e.g.r. であって位数 2 の L_d-有理点を持たない（admissible でない）もののうち, 判別式が 3 乗数となるようなものは存在しない.
3. $d = 46$ の時, L_d 上 e.g.r. な楕円曲線が存在する. これは admissible ではない.

補足 4.3. 実は純三次体上の存在例には, 類数 1 ではないが非常に安易に作ることの出来る例がある[2]. 当初の形から係数を 2 種類だけ残した楕円曲線

$$E:\ y^2 + a_1xy + a_3y = x^3$$

を考えると, この判別式は $\Delta(E) = a_3^3(a_1^3 - 27a_3)$ と書ける. この値が 1 となれば E は至る所良い還元を持つので, 方程式 $a_3^3(a_1^3 - 27a_3) = 1$ を考えると, すぐに $(a_1, a_3) = (\sqrt[3]{28}, 1)$ が求まる. 従って $L_{28} = \mathbb{Q}(\sqrt[3]{28})$ 上の楕円曲線

$$E:\ y^2 + \sqrt[3]{28}xy + y = x^3$$

は至る所良い還元を持つことが従う. 但し L_{28} の類数は 3 であるため, 極小モデルの存在は保証されない. 因みにこの曲線の Mordell-Weil 群は $\mathbb{Z}/3\mathbb{Z}$ に同型であり, admissible でもない.

この形は見ての通り, 実際にやってみると余り有用ではないと感じる. 実際, 二次体の場合は同様の手法を用いて得られた例は知られていないようである.

[2] 木田雅成氏（電気通信大）もこの例を指摘している.

5 今後の展望

本稿の最後に, これからの方針を述べて終わりとする.

1. 結局, 2 章と 3 章の手法を比較すると次のようになっている：

   2 章 計算すべき Mordell-Weil 群の候補をかなり減らせる上, 部分的に計算出来ても判別式の形が類推出来るため効率が良いが, 基礎体の性質に大きく依存するため, 取り替えに応じて新しく補題を準備しなければならない. 従って任意の代数体上という扱い方は出来ない.

   3 章 任意の代数体上に対するアルゴリズムが実現しているため, admissible かどうかの如何に関わらず全ての曲線のリストを用意することが出来る. 但し走査すべき曲線の数が多く, その（同型類の）全ての曲線の決定が成功しなければならないため, 実用的とも言い難い.

   虚二次体上 e.g.r. な楕円曲線を調べる際には, 3 章の手法しか使うことが出来ない. その意味では後者の方が汎用性は高いと言える. しかしながら今回前者を採用したのは, 代数的整数論の手法を大いに活用して計算機の負担を減らすという手法は, 今後独自に拡張を行える可能性が非常に高いと予想したからである.

2. 4 章で新しく得られた非存在性は, admissible でないものに限った結果である. 残るは admissible な曲線の判定であるが, 実二次体の場合に有用であった Comalada の規準が使えない. 更に不定方程式の非可解性に帰着する方法はかなりハードルが高いと思われるが, 現在取り組める唯一の手段だと思われる. この手法がどこまで有用なのかを今後考察して行きたい[3].

3. 2,3 章（二次体の場合）と 4 章（純三次体の場合）の決定的な違いは, 後者においては $d \neq d'$ であっても $L_d \simeq L_{d'}$ が成り立つ場合があることである（前者では square-free の仮定から生じないことが分かる）. 例えば $d \leq 200$ で類数 1 の L_d に限れば

   $$L_2 \simeq L_4,\ L_3 \simeq L_9,\ L_5 \simeq L_{25},\ L_6 \simeq L_{36},\ L_{10} \simeq L_{100},\ L_{12} \simeq L_{18},\ L_{45} \simeq L_{75}$$

   が見つかる. このような場合, 至る所良い還元を持つ楕円曲線の存在性・非存在性には何か影響があるのか？という新しい問題が生じる. これについても思案中である.

4. 他の興味深い基礎体（例えば円分体やその最大実部分体など）に対しては, 既存の実装がどこまで適用可能なのか？という問題も残っている. また potential e.g.r. を持つ場合に何か面白い問題が考えられないか？という問題も非常に興味深い.

謝辞

今回このような伝統ある研究集会にて講演の機会を下さいましたオーガナイザーの先生方に, この場を借りて厚く感謝御礼申し上げます. また, 講演後有益なコメントを下さいました松野一夫先生（津田塾大）にも重ねて御礼申し上げます.

[3]最近, 筒石奈央氏（津田塾大）によって（より一般の場合の）三次体の場合の新しい結果が得られたようである. こちらも Bertolini-Canuto の手法の拡張となっており, 幾つかの規準を満たすような基礎体上の e.g.r. な楕円曲線の非存在性, 特に admissible なものの非存在性が示されたとのことである. 帰結として, 幾つかの純三次体上での完全な非存在性が従うと見込まれる（こちらで試算しただけでも 12 個存在した）. 判明次第, データベースへ反映させる予定である.

A　未解決のケース（実二次体の場合）

Case $d = 62$　候補は E_1^-, E_3^-, E_5^-.

$E_n^{\pm}$	rank	generators (free part)
E_1^-	0	—
E_3^-	1	G_{1A}
E_5^-	1	??

基本単数: $\varepsilon = -63 + 8\sqrt{62}$

ここに $G_{1A} = \left(\frac{30492}{25} - \frac{3872}{25}\sqrt{62}, -\frac{8377936}{125} + 8512\sqrt{62}\right)$.

Case $d = 67$　候補は E_0^+, E_2^+, E_4^+.

$E_n^{\pm}$	rank	generators (free part)
E_0^+	1	G_{2A}
E_2^+	1	??
E_4^+	1	??

基本単数: $\varepsilon = -48842 + 5967\sqrt{67}$

ここに $G_{2A} = \left(-\frac{584}{49}, \frac{248}{343}\sqrt{67}\right)$.

Case $d = 71$　候補は E_1^-, E_3^-, E_5^-.

$E_n^{\pm}$	rank	generators (free part)
E_1^-	$1 \le r \le 3$	G_{3A}, ??
E_3^-	2	G_{3B}, G_{3C}
E_5^-	$1 \le r \le 3$	??

基本単数: $\varepsilon = 3480 + 413\sqrt{71}$

ここに

$$G_{3A} = \left(\frac{15025056}{49} + \frac{1782764}{49}\sqrt{71}, -\frac{82351180712}{343} - \frac{9773265400}{343}\sqrt{71}\right),$$
$$G_{3B} = \left(165300 + \frac{39235}{2}\sqrt{71}, \frac{377098253}{4} + \frac{44753329}{4}\sqrt{71}\right),$$
$$G_{3C} = \left(\frac{1560462848}{3025} + \frac{185192868}{3025}\sqrt{71}, -\frac{87152513410872}{166375} - \frac{10343100438152}{166375}\sqrt{71}\right).$$

Case $d = 107$　候補は E_0^+, E_3^+.

$E_n^{\pm}$	rank	generators (free part)
E_0^+	1	G_{4A}
E_3^+	$0 \le r \le 2$	G_{4B}, ??

基本単数: $\varepsilon = 962 + 93\sqrt{107}$

ここに

$$G_{4A} = \left(\frac{19415435}{53824}, \frac{8270595739}{12487168}\sqrt{107}\right),$$
$$G_{4B} = \left(\frac{13090698150670419032}{982587075600025} + \frac{1265524873193709948}{982587075600025}\sqrt{107},\right.$$
$$\left. -\frac{860549660043863578325024289 84}{308004152055919056561 25} - \frac{831924756766629877002052940 0}{308004152055919056561 25}\sqrt{107}\right).$$

Case $d = 109$　候補は E_0^+, E_2^+, E_4^+.

$E_n^{\pm}$	rank	generators (free part)
E_0^+	0	—
E_2^+	2	G_{5A}, ??
E_4^+	2	G_{5B}, ??

基本単数: $\varepsilon = \frac{261}{2} + \frac{25}{2}\sqrt{109}$

ここに

$$G_{5A} = \left(\frac{10154}{81} + \frac{970}{81}\sqrt{109}, -\frac{4210060}{729} - \frac{403268}{729}\sqrt{109}\right),$$
$$G_{5B} = \left(\frac{916346}{81} + \frac{87770}{81}\sqrt{109}, -\frac{1613792380}{729} - \frac{154573276}{729}\sqrt{109}\right).$$

Case $d = 127$　候補は E_3^-.

$E_n^{\pm}$	rank	generators (free part)
E_3^-	$0 \le r \le 2$	??

基本単数: $\varepsilon = -4730624 + 419775\sqrt{127}$

Case $d = 131$　候補は E_0^+, E_2^+, E_4^+, E_1^-, E_3^-, E_5^-.

$E_n^{\pm}$	rank	generators (free part)
E_0^+	1	G_{7A}
E_2^+	1	??
E_4^+	1	??
E_1^-	$0 \le r \le 2$	??
E_3^-	2	G_{7B}, ??
E_5^-	$0 \le r \le 2$	??

基本単数: $\varepsilon = -10610 + 927\sqrt{131}$

ここに

$G_{7A} = \left(-\frac{23296}{7225}, \frac{2208712}{614125}\sqrt{131}\right)$,
$G_{7B} = \left(\frac{1587256}{5} - \frac{693396}{25}\sqrt{131}, \frac{32622430104}{125} - \frac{2850234952}{125}\sqrt{131}\right)$.

Case $d = 139$　候補は E_0^+, E_2^+, E_4^+.

$E_n^{\pm}$	rank	generators (free part)
E_0^+	1	G_{8A}
E_2^+	1	??
E_4^+	1	??

基本単数: $\varepsilon = -77563250 + 6578829\sqrt{139}$

ここに $G_{8A} = \left(-\frac{21}{4}, -\frac{27}{8}\sqrt{139}\right)$.

Case $d = 151$　候補は E_1^-, E_3^-, E_5^-.

$E_n^{\pm}$	rank	generators (free part)
E_1^-	$0 \le r \le 2$	??
E_3^-	$0 \le r \le 2$	??
E_5^-	2	G_{9A}, ??

基本単数: $\varepsilon = -1728148040 + 140634693\sqrt{151}$

ここに $G_{9A} = (-3346088623246672 + 272300830362362\sqrt{151},$
$145946219003731317620795 62 - 1187693486265246101920898\sqrt{151})$.

Case $d = 163$　候補は E_0^+, E_1^+, E_2^+, E_3^+, E_4^+, E_5^+.

$E_n^{\pm}$	rank	generators (free part)
E_0^+	1	G_{10A}
E_1^+	$0 \le r \le 3$	??
E_2^+	$0 \le r \le 2$	??
E_3^+	2	G_{10B}, ??
E_4^+	$0 \le r \le 2$	??
E_5^+	$0 \le r \le 3$	??

基本単数: $\varepsilon = -64080026 + 5019135\sqrt{163}$

ここに

$G_{10A} = \left(640320, 40133016\sqrt{163}\right)$,
$G_{10B} = \left(1281600520 - 100382700\sqrt{163}, -57451588558840 + 4499955710712\sqrt{163}\right)$.

Case $d = 179$　候補は E_0^+, E_1^+, E_2^+, E_3^+, E_4^+, E_5^+.

$E_n^{\pm}$	rank	generators (free part)
E_0^+	1	G_{11A}
E_1^+	$0 \le r \le 2$	??
E_2^+	$0 \le r \le 1$	??
E_3^+	$0 \le r \le 2$	??
E_4^+	$0 \le r \le 1$	??
E_5^+	$0 \le r \le 2$	??

基本単数: $\varepsilon = 4190210 + 313191\sqrt{179}$

ここに $G_{11A} = \left(-\frac{250557131968}{113819191641}, \frac{118938892316317192}{38399294503115811}\sqrt{179}\right)$.

Case $d = 193$　候補は E_3^+.

$E_n^{\pm}$	rank	generators (free part)
E_3^+	2	G_{12A}, ??

基本単数: $\varepsilon = 1764132 + 126985\sqrt{193}$

ここに $G_{12A} = \left(\frac{74908961}{8} + \frac{5392065}{8}\sqrt{193}, -\frac{2297340821745}{16} - \frac{165366210833}{16}\sqrt{193}\right)$.

Case $d = 199$　候補は E_0^+, E_2^+, E_4^+.

$E_n^{\pm}$	rank	generators (free part)
E_0^+	1	G_{13A}
E_2^+	$0 \le r \le 1$	??
E_4^+	$0 \le r \le 1$	??

基本単数: $\varepsilon = -16266196520 + 1153080099\sqrt{199}$

ここに $G_{13A} = \left(\frac{527238916}{6477025}, \frac{859565955248}{16484028625}\sqrt{199}\right)$.

※ データは 2012 年 1 月 30 日 現在のもの

参考文献

[1] M. Bertolini and G. Canuto, *Good reduction of elliptic curves defined over* $\mathbb{Q}(\sqrt[3]{2})$, Arch. Math., vol. **50** (1988), 42-50.

[2] S. Comalada, *Elliptic curves with trivial conductor over quadratic fields*, Pacific J. Math. **144** (1990), 233-258.

[3] J. Cremona and M. Lingham, *Finding all elliptic curves with good reduction outside a given set of primes*, Exp. Math. **16** No.3 (2007), 303-312.

[4] J. Cremona and T. Thongjunthug, *The complex AGM, periods of elliptic curves over* $\mathbb{C}$ *and complex elliptic logarithms*, submitted.

[5] H. Ishii, *The non-existence of elliptic curves with everywhere good reduction over certain quadratic fields*, Japan. J. Math. **12** (1986), 45-52.

[6] T. Kagawa, *Determination of elliptic curves with everywhere good reduction over* $\mathbb{Q}(\sqrt{37})$, Acta Arith. **83** (1998), 253-269.

[7] T. Kagawa, *Determination of elliptic curves with everywhere good reduction over real quadratic fields*, Arch. Math. **73** (1999), 25-32.

[8] T. Kagawa, *Determination of elliptic curves with everywhere good reduction over real quadratic fields* $\mathbb{Q}(\sqrt{3p})$, Acta. Arith. **96** (2001), 231-245.

[9] T. Kagawa, *Elliptic curves with everywhere good reduction over real quadratic fields*, Ph. D. Thesis, Waseda University (1998).

[10] T. Kagawa, *Determination of elliptic curves with everywhere good reduction over real quadratic fields, II*, preprint.

[11] 加川貴章, 実二次体上の楕円曲線の整数点の計算, および自明な導手を持つ楕円曲線の決定, 加川氏のウェブページより入手可能.

[12] M. Kida, *Reduction of elliptic curves over certain real quadratic number fields*, Math. Comp. **68** (1999), 1679-1685.

[13] M. Kida, *Nonexistence of elliptic curves having good reduction everywhere over certain quadratic fields*, Arch. Math. **76** (2001), 436-440.

[14] M. Kida, *Good reduction of elliptic curves over imaginary quadratic fields*, Journal de Theorie de Nombres de Bordeaux **13** (2001), 201–209.

[15] M. Kida and T. Kagawa, *Nonexistence of elliptic curves with good reduction everywhere over real quadratic fields*, J. Number Theory **66** (1997), 201-210.

[16] B. Setzer, *Elliptic curves over complex quadratic fields*, Pacific J. Math. Volume 74, Number 1 (1978), 235-250.

[17] R. J. Stroeker, *Reduction of elliptic curves over imaginary quadratic number fields*, Pacific J. Math. Volume 108, Number 2 (1983), 451-463.

[18] T. Thongjunthug, *Computing a lower bound for the canonical height on elliptic curves over number fields*, Math. Comp. **79** (2010), 2431-2449.

[19] T. Thongjunthug, *Heights on elliptic curves over number fields, period lattices, and complex elliptic logarithms*, Ph. D. Thesis, The University of Warwick (2011).

[20] S. Yokoyama, *On elliptic curves with everywhere good reduction over certain number fields*, preprint (2011).

[21] 横山俊一, 二次体上至る所 good reduction を持つ楕円曲線について, 第 6 回福岡数論研究集会報告集 (2012), 1-11.

[22] S. Yokoyama and Y. Shimasaki, *Non-existence of elliptic curves with everywhere good reduction over some real quadratic fields*, J. Math-for-Industry, vol.**3** (2011B-4), 113-117.

Shun'ichi Yokoyama

Graduate School of Mathematics, Kyushu University

744 Motooka, Nishi-ku, Fukuoka, 819-0395, Japan

E-mail Address: `s-yokoyama@math.kyushu-u.ac.jp`

SOME CONCEPTS AND METHODS TO INVESTIGATE PROBLEMS OF WARING TYPE Ⅲ

R. MORIKAWA

1. Introduction

1-1. Let $B \in N$ be square free and $B \geq 11$. We put $V(1,B) = \{x^2 + y^2B | x, y \in N, (x,y) = 1\}$. Our concern is to clarify the structure of V.

We put $4B = D$, and classify the members of V as follows:

(a) $R(1,B) = \{p \in V \mid \text{prime},\ p \nmid D\}$

(b) $S(1,B) = \{n \in V \mid \text{composite}, (n,D) = 1\}$.

(c) $T(1,B) = \{n \in V \mid (n,D) > 1\}$

These sets are simply noted R, S, T.

Here if we clarify S, the other R, T are determined simply from S. Thus we concentrate the structure of S. Namely we treat the following problems.

Problem 1. To determine the prime divisors of S. We denote this set PS.

Problem 2. To obtain a criterion for a product of primes of PS whether $\in S$ or not.

Here we explain the contents of this report.

1. We classify B as follows.

$(\alpha)\ B \equiv 1 \text{ or } 2 \pmod 4$, $(\beta)\ B \equiv 3 \pmod 8$ $(\gamma)\ B \equiv 7 \pmod 8$.

We use (δ) as a general name of $(\alpha), (\beta), (\gamma)$. And we write simply $B \in (\delta)$.

2. In §2, we classify the class group of $Q(\sqrt{-B})$.

3. In §3, we separate PS into Cells, and define SC (Structure Constant) of $S(1,B)$.

4. In §4, we explain the correspondence between $H(B)$ and SC of $S(1,B)$.

5. From §5 on, we treat Problems 1,2 for $B \in (\gamma)$. For Problem 1, we introduce Γ sequences. And for Problem 2, we make ($\sharp$) cycles.

6. In §9, we give a partial answer to Problem 2.

7. §7 discusses the attainability. We say an abelian group A is (δ) attainable if there exists $B \in (\delta)$ whose $H(B)$ is A. This problem is very difficult.

(Important Remarks) 1. It is regrettable that many propositions given in this report have no proofs. But they are supported by numerous numerical researches (with no exception!). Thus we use in the report Assertion instead of Proposition to indicate the situation.

2. My old friend Professor I. Wakabayashi of Seikei Unversity has been treated this Problem from somewhat different standpoint [6]. The method is a continuation of D. Cox [3]. It allows some proofs of the Assertions of the report. I hope to amalgamate his result with those of mine, and write a joint paper in a near future.

Date: March 8, 2012.

2. Classification of class groups

2-1. [6] suggests the importance of $H(B)$ the class group of $Q(\sqrt{-B})$ for the problem. We classify $H(B)$ from our standpoint. For tables of class groups of imaginary quadratic fields, we refer [1], [2] and [5].

2-2. We decompose $H(B)$ as a direct product of cyclic subgroups. And denote

(1) $H =< (r_1)(r_2)\dots(r_k) >$ where $r_{j+1}|r_j$ for $1 \le j \le k-1$.

In (1), the latter r's are of the form $(2)\dots(2)$. We say this part Tail of H. And call the former part of (1) Head of H. (If $H =< (2)\dots(2) >$, we consider the first (2) to be Head of H.)

2-3. We treat in the following H with no Tail. We call $< (r) >$ a Single Head and $< (r)(s) >$ where $s|r$ and $s \ge 3$ a Double Head. It is known the existence of Triple Head etc. But we confine hereafter to Single and Double ones. $\boldsymbol{H}$ denotes the set of class group of those type.

2-4 We classify $\boldsymbol{H}$. Here h means the class number, and $2\|r$ means $2|r$ and $4 \nmid r$.

Take $H(B) \in \boldsymbol{H}$ with $B \in (\delta)$. They are classified as follows:

(1) Type K : The H with odd h is called Type K. They separate into $K(\beta)$ with $B \in (\beta)$ and $K(\gamma)$ with $B \in (\gamma)$.

(2) Type I : In case $2\|r$, we say H is of Type I.

(3) Type II : We say H is of Type II for Single $< (r) >$ with $4|r$. For double $< (r)(s) >$ it is of Type II if $4|r$ and $4 \nmid s$.

(4) Type III : We say H is of Type III if it is Double Head $< (r)(s) >$ with $4|s$.

3. Cells, Structure Constant

3-1. Let B be square free and ≥ 11. We put $D = 4B$. Let r be the cardinality of prime divisors of B. We put $2J = 2^{r+1}$ for $B \equiv 1 \pmod 4$, and $2J = 2^r$ for other cases. For $U \subset [1, D-1]$, we put $Q(D;U) = \{p \mid \text{prime } p \equiv u \pmod D \text{ for some } u \in U\}$. And PS is the set of prime divisors of S.

3-2. We define the following sets step by step.

Step 1. We put $F = \{n \pmod D \mid (n, D) = 1\}$. We consider $F \subset [1, D-1]$, and a multilicative group. We put $G = \{u^2 \pmod D | (u, D) = 1\}$. And consider G a subgroup of F.

Step 2. We put $M = G$ for $B \equiv 1 \pmod 4$. And $M = G \cup pG$ for $B \equiv 2, 3 \pmod 4$ where p is chosen by the following (CR1).

(CR1) Consider prime divisors p of $B + r^2$, taking $r = 1, 2, 3 \dots$. Take first p such that $p \nmid D$ and $B + r^2 = p^t u^2$ with odd t and $u \in N$.

Assertion 3.1. We take p with (CR1), and make $M = G \cup pG$. Then M is a subgroup of F. Here $[F : M] = 2J$.

Step 3. We arrange cosets of F/M as follows:

(C) $M,\ t_2M, \dots, t_{2J}M$.

For (C), we make $Q(D; t_jM)$ $(2 \le j \le 2J)$.

Assertion 3.2. We choose those $Q(D; t_jM)$ for which it contains $p \in PS$. Here exactly $J-1$ cosets of (C) are chosen. We put them x_jM $(2 \le j \le J)$.

As easily seen, $Q(D;M) \supset R$. We say $V(1,B)$ is Full-case if $R = Q(D;M)$. In the case, the structure of V is fairly simple. This case is explained in [4]. Thus we treat hereafter Non-Full case.

Step 4. We put $M(\tau) = Q(D;M) \setminus R$ and $Q(j) = Q(D;x_jM)$ $(2 \le j \le J)$.

Assertion 3.3. $PS = M(\tau) \cup Q(j)$ $(2 \le j \le J)$.

To study PS, we separate $M(\tau)$ and $Q(j)$ $(2 \le j \le J)$ into subsets which are called Cells. For $u, v \in SP$ we put $u \sim v$ if $uv \in S$. It is notable that in many cases $u \not\sim u$. And $u \sim v$, $u \sim w$ and $v \ne w$ implies $v \sim w$.
For $u \in PS$, we put $(u;\sim) = \{v \mid uv \in S,\ v \in SP\} \cup \{u\}$.

(τ-separation) We take y_1 the smallest member of $M(\tau)$. We put $(y_1;\sim) = M(\tau_1)$. Here $M(\tau_1) \subset M(\tau)$. If $M(\tau_1) = M(\tau)$, the process stops. And if $M(\tau) \setminus M(\tau_1) \ne \emptyset$, we take the smallest member y_2 from the set , and make $(y_2;\sim)$. We put $M(\tau_2) = (y_2;\sim)$. Here $M(\tau_2) \subset M(\tau)$. If $M(\tau) \setminus (M(\tau_1) \cup M(\tau_2)) \ne \emptyset$, we continue the process taking y_3. Thus finally we obtain $\sim$ classification of $M(\tau)$.

Assertion 3.4. By $\sim$ classification of $M(\tau)$, we obtain a finite classication $M(\tau) = \cup_{k=1}^{K} M(\tau_k)$, where $M(\tau_k) = (y_k;\sim)$ with $1 \le k \le K$. We call each $M(\tau_k)$ M-Cell.

Remark. We give for some cases a simple process to obtain $y_1, \dots y_K$ (cf. §5).

(j-separation) We operate $\sim$ classification for each $Q(j)$. We call this process j-separation.

Assertin 3.5. By j-separation, each $Q(j)$ separates $L(j)(< \infty)$ sets. We call them L-Cells.

Remark. For some B, there is a simple process to obtain these L-Cells.

(Structure Constant) We arrange $(K; L(2), \dots, L(J))$, and call it SC (Structure Constant) of $S(1,B)$. (In SC, $L(j)$'s are arranged as $L(2) \le \cdots \le L(J)$.)

(Complete Top System) We take the least prime from each Cell. Collecting them, we make Complete Top System of SC.

4. Correspondence between $H(B)$ and SC

Let $\boldsymbol{H}$ be as introduced in §2-4. Assume $B \in (\delta)$ have $H(B) \in \boldsymbol{H}$. Let h be the class number. In Assertion 4.1., Case 1 means $B \in (\alpha) \cup (\gamma)$, and Case 2 means $B \in (\beta)$.

Assertion 4.1. (1) If $H(B) \in \boldsymbol{H}$ be of type K, then SC of $S(1,B)$ is (K). Here $K = [h/2]$ for Case 1. And $K = 3[h/2] + 1$ for Case 2.

(2) Let $H(B)$ be of Type I. (i) Let $H(B) =< (r) >$, $2 \| r$ or $H(B) =< (r)(s) >$ with odd s. Then SC of $S(1,B)$ is $(K; K+1)$, where $K = [h/4]$ for Case 1. And $K = 3[h/4]+1$ for Case 2.
(ii) For $H(B)$ with $2 \| s$, SC of $S(1,B)$ is $(K; K+1, K+1, K+1)$. Here $K = [h/8]$ for Case 1, and $K = 3[h/8] + 1$ for Case 2.

(3) Let $H(B)$ be of Type II. (i) Take $H =< (r) >$ wih $4|r$ or $H =< (r)(s) >$ with odd s. Then SC of $S(1,B)$ is $(K;K)$ where $K = h/4$ for Case 1, and $K = 3h/4$ for Case 2.
(ii) For $H =< (r)(s) >$ with $4|r, 2\|s$, SC of $S(1,B)$ is $(K; K, K, K+1)$. Here $K = h/8$ for Case 1, and $K = 3h/8$ for Case 2.

(4) Let $H(B)$ be of Type Ⅲ. Namely $H =< (r)(s) >$ with $4|s$. Then SC of $S(1,B)$ is $(K+1;K,K,K)$. Here $K=h/8$ for Case 1, and $K=3h/8$ for Case 2.

5. Γ SEQUENCES

We treat in this §$B \in (\gamma)$ whose $H(B)$ is a cyclic group of odd order h. We put $K=[h/2]$.

(2-order) For $u \in PS$, we say u has 2-order ρ if ρ is the smallest number for which $2^\rho u \in T$. Here we denote $\varphi(u)=\rho$.

In the following we assume B satisfies the following:

(Cond B) $2^r \notin T$ for $3 \leq r \leq K$.

Remark. This condition is satisfied wth almost all B.

Assertion 5.1. Let B be as above. Then we can make Γ sequence whose length is K.

(Γ) $\quad 8u_1^2 \to 8u_1u_2 \to \cdots \to 8u_{K-1}u_K$

which satisfies the following conditions.

(1) $u_1, u_2, \ldots u_k$ are different primes contained in PS.

(2) $8u_i^2$, $8u_ju_{j+1}$ $(1 \leq j \leq K-1)$ are all in T.

(3) u_ju_{j+1} $(1 \leq j \leq K-1)$, and u_ju_{j+2} $(1 \leq j \leq K-2)$ are $\notin S$.

(4) u_j $(1 \leq j \leq K)$ are the smallest primes under (1)-(3).

We call u_j $(1 \leq j \leq K)$ the vertices of (Γ). We put $\boldsymbol{U} = \{u_j | \, (1 \leq j \leq K)\}$.

Assertion 5.2. (1) The set $\boldsymbol{U}$ is Complete Top System of $S(1,B)$.

(2) $\varphi(u_j) = K-j+3$ $(1 \leq j \leq K)$. And $(u_j;\sim) = \{u \in SP \mid \varphi(u) = K-j+3\}$.

Assertion 5.2 is a curious one. To explain this, we introduce the following concepts.

(Class representation) As well known, each ideal class of $H(B)$ corresponds to a triple (a,c,b) with $B+b^2=4ac$ where $|b| \leq a < c$. Principal ideal corresponds to $(1, B+1/8, 1)$.

For other classes , we consider $C \cup C'$ where C' is Conjugate class of C. Here $C \cup C'$ corresponds to $(a,c,\pm b)$. Thus we make K pairs of ideal classes, and denote $H/ < 2 >= \{C_j \cup C_j' \, | 1 \leq j \leq K\}$. We say $(a,c,\pm b)$ to be Class representation of $C \cup C'$.

For $u \in PS$, we put $u \rhd (C,C')$ if

(1) $(-B/u) = +1$ (Legendre Symbol).

(2) Let $p = PP'$ where P, P' are prime ideals. Then $P, P' \in C \cup C'$.

Here the following criterion is proved in [6].

(Criterion of Wakabayashi) Let $B \in (\gamma)$ and ≥ 11. Then

(1) $u \in PS$ if and only if $(-B/u) = +1$.

(2) Let $u, v \in PS$ and $u \neq v$. Then $uv \in S$ if and only if $u \rhd (C,C')$ and $v \rhd (C,C')$ with some C, C'.

Assertion 5.3. We take $A \cup A^{-1}$ whose Class-representation is $(2, B+1/4, \pm 1)$. Then $u_j \rhd (A^{K+1-j}, A^{-K-1+j})$ for $1 \leq j \leq K$.

. Table 5.1. We give numerical examples of (Γ) sequences for smaller K taking suitable B's. (We note the sequence of vertices.)

$K=1$. $B=23$. 3 is the isolated vertex.

$K=2$. $B=47$. $3 \to 7$.

$K=3$. $B=71$. $3 \to 5 \to 19$.

$K=4$. $B=199$. $5 \to 7 \to 13 \to 31$.

$K=5$. $B=167$. $7 \to 3 \to 19 \to 11 \to 31$.

$K = 6$. $B = 191$. $5 \to 23 \to 3 \to 13 \to 17 \to 79$.
$K = 7$. $B = 239$. $11 \to 3 \to 17 \to 5 \to 71 \to 29 \to 31$.
$K = 8$. $B = 383$. $7 \to 43 \to 17 \to 3 \to 23 \to 19 \to 29 \to 103$.
$K = 9$. $B = 313$. $7 \to 53 \to 3 \to 113 \to 79 \to 5 \to 73 \to 47 \to 47 \to 67$.
$K = 10$. $B = 5647$. $59 \to 101 \to 7 \to 103 \to 53 \to 127 \to 89 \to 179 \to 353 \to 709$.
$K = 19$. $B = 5119$. $61 \to 13 \to 67 \to 251 \to 43 \to 17 \to 79 \to 19 \to 47 \to 127 \to 131 \to 5 \to 137 \to 83 \to 71 \to 97 \to 167 \to 353 \to 641$

Remark. We take $B = 431$ for $K = 10$. In the case $2^7 \in T$. We have Γ sequence; $8.61^2 \to 8.61.41 \to 8.41.109$. And in the case, we have $8.11.59 \to 8.59.23 \to 8.23.3 \to 8.3.19 \to 8.19.29 \to 8.29.11 \to$ (cycle). Here $\{61, 41, 109, 11, 59, 23, 3, 19, 29\}$ makes Complete Top System. And this $\boldsymbol{U}$ makes the same ($\sharp$) cycle (cf.§6) with above $B = 5647$ for $K = 10$.

6. ($\sharp$) CYCLE

In this §, we assume Cond. B. Thus we identify $u \in \boldsymbol{U}$ and (ρ) for which $\varphi(u) = \rho$. By making Γ sequences, we get $\boldsymbol{U}$ Complete Top System of $S(1, B)$. To attack Problem 2, we separate $\boldsymbol{U}$ into ($\sharp$) cycles.

Assertion 6.1. For $u \in \boldsymbol{U}$, there exists unique $v \in \boldsymbol{U}$ for which $u^2 v \in S$. In the case we put $u \Rightarrow v$. If $u = v$, we see $v^2 u \in S$. And if $u \neq v$, we choose $w \in \boldsymbol{U}$ for which $v^2 w \in S$, and we make $u \Rightarrow v \Rightarrow w$. We continue this process till it returns to u. If it returns to u, we make a ($\sharp$) cycle. If there remains $x \in \boldsymbol{U}$ which does not appear in this ($\sharp$) cycle, we start from x and do the same process. Thus finally $\boldsymbol{U}$ decomposes into disjoint sum of ($\sharp$) cycles.

Assertion 6.2. Let B satisfy Cond B. Assume $u^2 v \in S$ for $u, v \in \boldsymbol{U}$. We put $\varphi(u) = \rho$ and $\varphi(v) = \sigma$. Then
(1) If $2\rho - 2 \leq K + 2$, then $\sigma = 2\rho - 2$.
(2) If $K + 2 < 2\rho - 2$, then $\sigma = 2(K - \rho) + 7$.

Assertion 6.2. allows us to obtain ($\sharp$) cycles for each K.

Example 6.1. We explain the process taking the case $K = 16$. We put $\boldsymbol{K} = [3, 4, \ldots 18]$. We start from (3). Applying Assertion 6.2., we obtain $(3) \Rightarrow (4) \Rightarrow (6) \Rightarrow (10) \Rightarrow (18)(\Rightarrow (3))$. We denote this cycle $\vdash (3)(4)(6)(10)(18) \dashv$. We start from (5), then we get $\vdash (5)(8)(14)(11)(17) \dashv$. Next $\vdash (7)(12)(15)(9)(16) \dashv$ appears. $\vdash (13) \dashv$ is an isolated cycle.
In the case, we put $K = 16 = 1 + 5 + 5 + 5$, and call ($\sharp$)-relation.

Table 6.1. We give exaples of ($\sharp$)-relation. (We omit the case all $\boldsymbol{U}$ makes one ($\sharp$) cycle.)
The first spritting ($\sharp$) cycle appears in case $h = 9$ $K = 4 = 1 + 3$. The next case is $h = 15$ $K = 7 = 1 + 2 + 4$. For $h = 17$, $K = 8 = 4 + 4$, For $h = 21$,$K = 10 = 1 + 3 + 6$. For $h = 25$, $K = 12 = 2 + 10$. For $h = 27$, $K = 13 = 1 + 3 + 9$. For $h = 31$, $K = 15 = 5 + 5 + 5$. For $h = 33$, $K = 16 = 1 + 5 + 5 + 5$. For $h = 35$,$K = 17 = 2 + 3 + 12$. Finally if $h = 189$, we have $K = 94 = 1 + 3 + 3 + 6 + 6 + 6 + 6 + 9 + 18 + 18 + 18$.

7. Attainability

7-1. For an abelian group A, we say A is (δ) attainable in case there exsists $B \in (\delta)$ whose class group $H(B) = A$. We use abbreviation (δ)-able, and (δ)-nable for not attainable case.

We denote in the following $K(\gamma)$ Double as $< (sf)(s) >$ where s, f odd and $s \geq 3$.

7-2. Consulting [1]and[2], we see the following $< (sf)(s) >$ are (γ)-able.

(1) For $s = 3$, $f = 5, 11, 13, 15, 17, 19, 23, 25, 27$. (2) For $s = 5$, $f = 3$. (3) For $s = 7$, $f = 11, 13$. (4) For $s = 9$, $f = 3, 9$. (5) For $s = 11$, $f = 3, 7, 9$. (6) For $s = 13$, $f = 5, 7, 11$. (7) More larger (γ)-able A's are $< (15)(15) >, < (105)(15) >, < (85)(17) >, < (57)(19) >$.

7-3. On the other hand, notable (γ)-nable A's are

(1) For $s = 3$, $f = 1, 3, 7, 9, 21$.

(2) For $s = 5$, $f = 1, 5, 7, 9$.

Remark. Also (β)-able A's are very subtle. For example $< (3)(3) >$, $< (5)(5) >$, $< (7)(7) >$, $< (13)(13) >$ are (β)-able. But $< (11)(11) >$ and $< (17)(17) >$ are (β)-nable. In short, the property of attainnable Double A is mysterious.

8. $K(\gamma)$ Double

Let $H =< (sf)(s) >$ where s, f odd. We treat here only the case $s = 3$. By studying the cases $f = 5, 11, 13, 17, 19$, we obtain the following Assertion.

Assertion 8.1. For (γ) Double with $H =< (3f)(3) >$, we obtain the following two (Γ) sequences.

(1) $\Gamma(1)$. $\quad 8u_1^2 \to 8u_1u_2 \to \cdots \to 8u_{K_1-1}u_{K_1}$.

Here $K_1 = [3f/2]$, and $\Gamma(1)$ is taken so that it satifies properties given in Assertion 5.1. for $H =< (3f) >$.

(2) We put $V(3) = \{v \in SP \mid v^3 \in S, v \notin \Gamma(1)\}$. Then $|V(3)| = 3$. We make:

$\Gamma(2)$ $\quad 8v_1v_2 \to 8v_2v_3 \to \cdots \to 8v_{K_2-1}v_{K_2} \to$. (cycle)

Here $\Gamma(2)$ satisfies the following properties.

(a) $\Gamma(2)$ is a cycle whose length $K_2 = 3f$.

(b) $v_1 \in V(3)$. We put $\boldsymbol{V} = \{v_j \mid (1 \leq j \leq K_2\}$. We denote $v_j \in \Gamma(2)$. We consider $v_{K_2+1} = v_1$ and $v_{K_2+2} = v_2$.

(c) $8v_jv_{j+1} \in T$ for $1 \leq j \leq K_2$.

(d) $v_jv_{j+1} \notin S$ for $1 \leq j \leq K_2$. And $v_jv_{j+2} \notin S$ for $1 \leq j \leq K_2$.

(e) $\boldsymbol{V}$ are the smallest primes under condition (a)-(d).

Assetion 8.2. The set $\boldsymbol{U} \cup \boldsymbol{V}$ is Complete Top System of $S(1; B)$.

Exmple 8.1. Let $B = 25447$. Then $H(B) =< (15)(3) >$. We have

$\Gamma(1)$ $\quad 59 \to 113 \to 199 \to 409 \to 809 \to 1601 \to 3181$.

We take $A \cup A^{-1}$ which has Class-representation $(2, 3181, \pm 1)$. Then $\Gamma(1)$ satisfies properties of Assertions 5.2.-5.4. for $< 15) >$. Thus we have $(\sharp)$ relation $K_1 = 7 = 1+2+4$.

We have the following $\Gamma(2)$ sequence, whose length $= 15$.

$\Gamma(2)$ $\quad 97 \to 43 \to 157 \to 37 \to 103 \to 53 \to 139 \to 31 \to 107 \to 101 \to 191 \to 17 \to 211 \to 151 \to 47 \to$.

We obtain from $\Gamma(2)$, $(\sharp)$ cycles which have the relation $K_2 = 15 = 1+1+1+4+4+4$.

Example 8.2. We give here a very rough explanation of $B = 38047$ whose $H(B)$ $=< (15)(5) >$. In the case we have three Γ sequences.
$\Gamma(1)$ $79 \to 173 \to 397 \to 597 \to 1223 \to 2381 \to 4797$
$\Gamma(2)$ $283 \to 263 \to 163 \to 37 \to 131 \to 89 \to 179 \to 29 \to 223 \to 197 \to 41 \to 137 \to 151 \to 281 \to 17 \to$.
$\Gamma(3)$ $53 \to 103 \to 67 \to 71 \to 101 \to 191 \to 367 \to 13 \to 379 \to 211 \to 181 \to 239 \to 23 \to 227 \to 167 \to$.

Here $\Gamma(2), \Gamma(3)$ are sequences of length 15. Note that $283^5, 53^5$ are $\in S$.

We put $\boldsymbol{U}_i = \{u_i \in \Gamma(i)\ (1 \leq i \leq 3)\}$. Then $\boldsymbol{U_1} \cup \boldsymbol{U}_2 \cup \boldsymbol{U}_3$ make Complete Top System for $S(1, B)$. From $\boldsymbol{U}_1$ we have ($\sharp$) cycles with $K_1 = 7 = 1 + 2 + 4$. And from $\Gamma(2) \cup \Gamma(3)$, we have ($\sharp$) cycles with $K_2 = 30 = 2 + 2 + 2 + 2 + 2 + 4 + 4 + 4 + 4 + 4$.

9. S combination

In this section, we treat $K(\gamma)$ Single with Cond B. Thus the Top elements $u \in \boldsymbol{U}$ are identified with its 2-order $\varphi(u) = \rho$. We consider
(2) $x = u_1^{s_1} \dots u_t^{s_t}$ where $u_i \in PS$ and $s_i \in N$ $(1 \leq i \leq t)$.

If in (2), u_i's are taken from g different Cells, we say x to be g-segmental.

(Critical Order) Let $u \in PS$. If there exists the smallest τ for which $u^\tau \in S$, we call τ the citical order of u.

Assertion 9.1. (1) For any $u \in PS$, there exist the critical order τ, and $\tau | h$.

(2) Each vertex of ($\sharp$) cycle has the same critical order τ. We denote this cycle as $\sharp(m, \tau)$, where m is the length of ($\sharp$).

(S combination) If x of (2) is $\in S$, we say (2) is an S combination.

We denote $\sharp(m, \tau)\square(B)$ in case this cycle is of $S(1, B)$. For example $\sharp(1, 3)\square(23)$, $\sharp(2, 5)\square(47)$, $\sharp(3, 7)\square(71)$, $\sharp(3, 9)\square(199)$, $\sharp(5, 11)\square(167)$, and $\sharp(5, 31)\square(1719)$.

(Corecombination) We make the set of Corecombination omitting the following S combination:

If x of (2) decomposes to $x = uv$ where $u \in S$ and $v \in S$.

Assertion 9.2. For x of (2), assume u_i's are taken from Cells of one $\sharp(m, \tau)$. Then Corecombinations are determined by (m, τ).

Assertion 9.3. Let x of (2) is 1-segmental. And assume the taking Cell $(u; \sim) = U$ belong to $\sharp(m, \tau)$. Then Corecombinations are as follows.

(a) tu with $t \neq u$.

(b) Any τ-combination.

(c) $v^{2\tau}$ with $v \in U$.

To treat Corecombinations for $g \geq 2$, we introduce the following concept.

(Taking Combination) Let x of (2) be g-segmental with $g \geq 2$. Then the combination of the cardinalities of taking elements from each Cell is called Taking Combination of x.

Assertion 9.4. (Lifting Principle) Let $g \geq 2$. Then for x of (2), $x \in S$ or not is determined by its Taking Combination.

To determine Corecombination is a difficult problem. We treat here only the case that all Taking Cells belong to one $\sharp(m, \tau)$. For the case the following translation rule holds.

(Translation of Taking Cells) We explain by a numerical example. Let take $\sharp(5,11)\square(167)$. This cycle is $\vdash (3)(4)(6)(5)(7)\dashv$. And since $B = 167$, its another expression is $31 \Rightarrow 11 \Rightarrow 3 \Rightarrow 19 \Rightarrow 7 \Rightarrow$.

For g-segmental x, we arrange g Taking Cells as $[(\rho_1)\dots(\rho_g)]$, by the order of $(\sharp)$ and translate them as follows:

(a) $[(3)(4)] \to [(4)(6)] \to [(6)(5)] \to [(5)(7)] \to [(7)(3)] \to$ (cycle)
(b) $[(3)(6)] \to [(4)(5)] \to [(6)(7)] \to [(5)(3)] \to [(7)(4)] \to$ (cycle)
(c) $[(3)(4)(6)] \to [(4)(6)(5)] \to [(6)(5)(7)] \to [(5)(7)(3)] \to [(7)(3)(4)] \to$ (cycle)
(d) $[(3)(4)(5)] \to [(4)(6)(7)] \to [(6)(5)(3)] \to [(5)(7)(4)] \to [(7)(3)(6)] \to$. (cycle)

Assertion 9.5. (Translation Rule) About two g-combination which are translatable, their Corecombinations coincide. For example about (b) above, 5 numbers
$31^\alpha 3^\beta,\ 11^\alpha 19^\beta, 3^\alpha 7^\beta,\ 19^\alpha 31^\beta, 7^\alpha 11^\beta$ are $\in S$ or $\notin S$ simultaneously.

Table 9.1. (Examples of Core-combinations)

(1) $\sharp(2,5)\square(47)$. Then 2 Coreconbinations are (1,2), (1,3), (2,1), (3,1).

(2) $\sharp(3,7)\square(71)$. The $(\sharp)$ cycle is $\vdash$ (3)(4)(5) $\dashv$. For 2-combination [(3)(4)], Coreconbinatios are (1,3),(1,4) (2,1), (5,1). And 3-Core conbinations are (1,1,2), (1,1,3), (1,2,1), (1,3,1), (2,1,1), (3,1,1).

(3) $\sharp(3,9)\square(199)$. Then $(\sharp)$ cycle is $\vdash$ (3)(4)(6) $\dashv$. For 2-combination [(3)(4)], Corecombinations are (1,4), (1,5), (2,1), (3,3), (7,1). And 3 Corecombinations are (1,1,2), (1,1,3), (1,2,1), (1,3,1), (2,1,1), (3,1,1).

(4) $\sharp(5,11)\square(167)$. (a) For 2- combination [(3) (4)], Corecombinations are (1,5), (1,6), (2,1), (3,4), (5,3), (9,1).

(b) For 2-combination [(3) (6)], Corecombinations are (1,3), (1,8), (3,2), (4,1), (7,1).

(c) For 3-combination [(3),(4), (6)], Corecombinations are (1,1,2), (1,1,3), (1,2,2), (1,2,3), (2,1,1).

(d) For 3-combination [(3)(4)(5)], Corecombinations ars (1,1,1), (1,2,1), (1,2,1), (1,2,2), (1,3,2), (2,1,3), (2,3,1), (3,1,2).

(e) For 4-combination [(3),(4),(6),(5)], Corecombinations are (1,1,1,1), (1,2,1,1), (1,1,1,2), (2,1,1,1).

(f) 5-Corecombinations are (1,1,1,1,1), (1,1,1,2,1), (1,1,2,1,1), (1,2,1,1,1).

References

[1] D. Buell, Class groups of quadratic fields, Math. Comp. 30 (1976) 610-623.

[2] D. Buell, Small class numbers of extreme values of L-function of quadratic fields, Math. Comp. 31 (1977), 786-796.

[3] D. Cox, Primes of the form $x^2 + ny^2$, Fermat, Classfield theory and Complex multiplication, John Wiley and Son (1989).

[4] R. Morikawa, Some concepts and methods to investigate problems of Waring type II, Proceedings of AC 2009, http://tnt.math,metro-u.ac.jp

[5] H. Wada-M. Saito, Class groups of imginary quadratic fields, (in Japanese) Lecture Notes of Sophia Univ. 28 (1988)

[6] I. Wakabayashi, Natural numbers of the form $x^2 + my^2$, Report of Mathematical Seminar at Seikei Univ. (2010, 2012) (in Japanese,unpublished)

3-8-22-4, Nihonmatsu, Midoriku, Sagamihara 252-0137 Japan
E-mail address: rmorikawa@muj.biglobe.ne.jp

5 次交代群 A_5 を固定群とする 2-arc-transitive graph

梶谷 美帆
東北大学大学院情報科学研究科

講演日：Nov. 8, 2011
提出日：Nov. 25, 2011

概要

$G = \mathrm{PSL}(2,29)$ には 2 つの共役でない 5 次交代群 A_5 が含まれており, それらによる非同値な置換表現の $\mathbb{Z}G$ 加群は同型になるという珍しい例である (Scott, 1992). $\mathrm{PGL}(2,29)$ の中では A_5 は共役を除いて一意的で, $\mathrm{PGL}(2,29)/A_5$ は 5-regular な 2-arc-transitive graph を与える. 今回の講演では, どのような q に対して $\mathrm{PSL}(2,q)/A_5$, $\mathrm{PGL}(2,q)/A_5$ から 5-regular な 2-arc-transitive graph が得られるかについて, 計算結果を報告した. また, multiplicity-free な置換表現 $\mathrm{PGL}(2,29)/A_5$ の指標表を求めた. 利用したソフトウェアは MAGMA と GAP である.

1 Introduction

1.1 Example

初めに, 有限群の置換表現と本稿の主題である “2-arc-transitive graph” との関係をお話ししておきたい. 有限群の置換表現, 置換加群を扱う過程で現れる suborbit が, 今回の題となっている特別な graph になっている, まずその例を紹介しよう.

Example. Scott (1993) $G = \mathrm{PSL}(2,29)$ の部分群 H_1, H_2 で次を満たすものが存在する:

1. $H_i \cong A_5$,
2. H_1 と H_2 は G で共役でない,
3. $\Omega_i := G/H_i (i = 1, 2)$ とおくと, $\mathbb{Z}$ 上の置換加群は $\mathbb{Z}G$-同型: $\mathbb{Z}\Omega_1 \cong_{\mathbb{Z}G} \mathbb{Z}\Omega_2$.

これは $\mathbb{Z}$ 上の置換表現の同値問題の反例として発表された. この Ω_i に対応する置換表現を計算すると, Ω_i 上の G-suborbits には subdegree 5 及び 6 のものは現れないが, $\mathrm{PGL}(2,29)$ の中では上の例における H_1 と H_2 は共役であり, $\mathrm{PGL}(2,29)/A_5$ 上の $\mathrm{PGL}(2,29)$-suborbits には, subdegree 5, 6 のものが現れる. この subdegree 5 及び 6 の suborbit が "2-arc-transitive graph" になっているのである.

1.1.1 character table

graph の話に移る前に, $\mathrm{PSL}(2,29)/A_5$ 上の置換表現の指標表を MAGMA で計算したので記載しておく. 表の一番左の列は, 各行を特徴付ける指標の次数を表す. ただし, この指標表は $\mathrm{PSL}(2,29)$-suborbit が全て symmetric であることから置換表現は multiplicity-free であるので, 計算できるものである.

	suborbits						
principal character	1	12	20	20	30	30	30	60
30	1	α_1	α_2	α_3	α_4	α_5	α_6	α_7
30	1	${\alpha_1}^{\sigma^2}$	${\alpha_2}^{\sigma^2}$	${\alpha_3}^{\sigma^2}$	${\alpha_4}^{\sigma^2}$	${\alpha_5}^{\sigma^2}$	${\alpha_6}^{\sigma^2}$	${\alpha_7}^{\sigma^2}$
30	1	${\alpha_1}^{\sigma^4}$	${\alpha_2}^{\sigma^4}$	${\alpha_3}^{\sigma^4}$	${\alpha_4}^{\sigma^4}$	${\alpha_5}^{\sigma^4}$	${\alpha_6}^{\sigma^4}$	${\alpha_7}^{\sigma^4}$
28	1	β_1	β_2	β_3	β_4	β_5	β_6	β_7
28	1	${\beta_1}^{\tau\rho}$	${\beta_2}^{\tau\rho}$	${\beta_3}^{\tau\rho}$	${\beta_4}^{\tau\rho}$	${\beta_5}^{\tau\rho}$	${\beta_6}^{\tau\rho}$	${\beta_7}^{\tau\rho}$
28	1	${\beta_1}^{\tau\rho^2}$	${\beta_2}^{\tau\rho^2}$	${\beta_3}^{\tau\rho^2}$	${\beta_4}^{\tau\rho^2}$	${\beta_5}^{\tau\rho^2}$	${\beta_6}^{\tau\rho^2}$	${\beta_7}^{\tau\rho^2}$
28	1	${\beta_1}^{\tau\rho^3}$	${\beta_2}^{\tau\rho^3}$	${\beta_3}^{\tau\rho^3}$	${\beta_4}^{\tau\rho^3}$	${\beta_5}^{\tau\rho^3}$	${\beta_6}^{\tau\rho^3}$	${\beta_7}^{\tau\rho^3}$

ここに,

$$\begin{aligned}
\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q}) &= \langle\sigma\rangle && (\sigma(\zeta_7) = \zeta_7^5),\\
\mathrm{Gal}(\mathbb{Q}(\zeta_{15})/\mathbb{Q}) &= \langle\tau,\rho\rangle && (\tau(\zeta_{15}) = \zeta_{15}^{14},\ \rho(\zeta_{15}) = \zeta_{15}^{2}),
\end{aligned}$$

$\gamma := \zeta_7 + \zeta_7^6, \delta := \zeta_{15} + \zeta_{15}^{14}$ のもとで

$$\begin{aligned}
(\alpha_i)_{i=1}^7 =&(2\gamma^2+2\gamma, -4\gamma, 2\gamma+2,\\
&-2\gamma^2-3\gamma+2, -\gamma^2-\gamma+1, -5\gamma^2+8, 6\gamma^2+4\gamma-14),\\
(\beta_i)_{i=1}^7 =&(-2\delta^3-\delta^2+6\delta-1, \delta^3+2\delta^2-4\delta-5, 4\delta^3+2\delta^2-11\delta-4,\\
&-3\delta^3-2\delta^2+13\delta+2, 3\delta^3-3\delta^2-12\delta+9, -2\delta^3+\delta^2+5\delta-3,\\
&-\delta^3+\delta^2+3\delta+1).
\end{aligned}$$

1 行目の principal character 以下の 7 行の成分は, うち 3 行が ζ_7, 4 行が ζ_{15} を使って表せる. さらに, それぞれがガロア群 $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})$, $\mathrm{Gal}(\mathbb{Q}(\zeta_{15})/\mathbb{Q})$ の作用で移りあう.

1.2 Definition

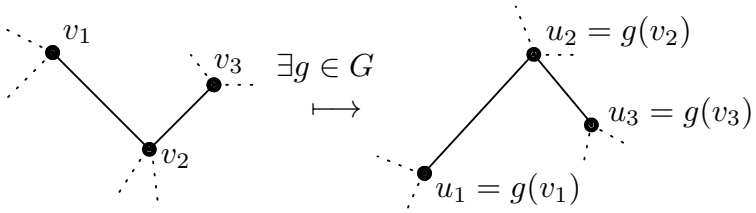
$\Gamma = (V, E)$ は (undirected simple connected regular) graph とし, G は Γ の自己同型群 $\mathrm{Aut}\Gamma$ とする.

Definition 1 (2-arc-transitive)**.** G は Γ 上 2-arc-transitive であるとは, G が Γ における 2-arc の集合

$$\{(v_1, v_2, v_3) \mid (v_i, v_{i+1}) \in E\ (i = 1, 2), v_1 \neq v_3\}$$

に transitive に作用することである.

このことを図で表すと,

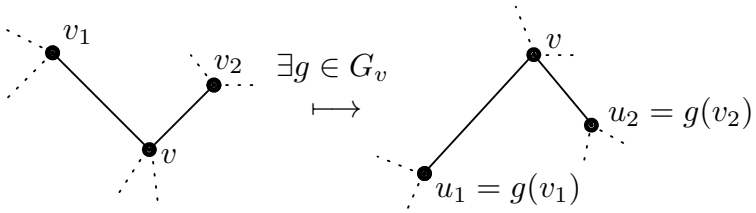


このように 2 つの 2-arc (v_1, v_2, v_3), (u_1, u_2, u_3) に対して, 2-arc をそのまま移すような $g \in G$ が存在することを意味している. この G に関する定義は, $v \in V$ の G における固定群 G_v に関する命題に言い換えることが出来る. 以下では主に G_v について述べていくので, その命題を紹介しておく.

$\Gamma = (V, E)$ は (simple connected regular undirected) graph, G は Γ の自己同型群 $\mathrm{Aut}\Gamma$ で vertex-transitive であるとする. $v \in V$ に対して v に隣接する頂点の集合 $\{u \in V \mid (u, v) \in E\}$ を $\Gamma(v)$ で表す. このとき

Remark 1. G は Γ 上 2-arc-transitive である必要十分条件は G_v が $\Gamma(v)$ に対して doubly transitive に作用することである.

このことを図で表すと,



このように頂点 v に隣接する頂点の組 (v_1, v_2), (u_1, u_2) に対して, 組をそのまま移す $g \in G_v$ が存在することを意味している.

1.3 2-arc-transitive graph

まず, 既に知られている結果を紹介する. valency d の graph Γ に対して G_v $(v \in V)$ は $\Gamma(v)$ 上 doubly transitive とする. このとき G_v はどのような群となるか, さらに Γ はどのようなグラフであるのか分類を行った (Cameron, 1983).

また Cameron はこの分類に先駆けて, 次の定理を与えている.

Theorem 2 (Cameron (1974))**.** G は primitive で, $G_v = S_n$ または A_n のとき, いずれか 1 つが成り立つ:

1. 任意の頂点 $x, z \in V$ に対して, $|\{y \in V \mid (x, y), (y, z) \in E\}| = 1$,
2. Γ は folded cube graph,
3. Γ は complete graph.

先の $\mathrm{PGL}(2, 29)/A_5$ 上の suborbit の場合, $G_v = A_5$ であり 5-regular 2-arc-transitive graph は 1 に当てはまるように思えるが, $\mathrm{PGL}(2, 29)$ は imprimitive であり, この場合は上の定理のようなパターン分類も成されていない.

2 Problem and approach

2.1 Problem

ここで, 問題とそれへの取り組みをまとめておく.

2-arc-transitive graph は, 今のところその分類が未完成である. しかし $\mathrm{PGL}(2, 29)/A_5$ の suborbits に現れることから $\mathrm{PGL}(2, q)$, $\mathrm{PSL}(2, q)$ について調査していった結果, $\mathrm{PGL}(2, q)/A_5, \mathrm{PSL}(2, q)/A_5$ 上の suborbits に時折現れる事がわかった. どの素数冪 q の場合に現れるのか, 決定するには至らなかったがそのヒントを得るべく, MAGMA,

GAP を用いていつ現れるのか確かめる計算を行った. その手法について説明する.

2.2 The Series of $\mathrm{PGL}(2,q)$, $\mathrm{PSL}(2,q)$

素数冪全てを総当りで調べる必要はなく, 次の定理から, どんな q について調べればよいか見当を付けることが出来る.

Theorem 3 (Dickson (1901))**.** $q := p^n$ は素数冪とする. このとき, $A_5 \subset \mathrm{PSL}(2,q)$ である必要十分条件は $q(q^2-1) \equiv 0 \pmod 5$.

また $\mathrm{PGL}(2,q)/A_5$ の suborbit についても調べたいが, ここで $A_5 \subset \mathrm{PGL}(2,q)$ となる必要十分条件は $A_5 \subset \mathrm{PSL}(2,q)$ である. よって, $q(q^2-1) \equiv 0 \pmod 5$ のとき, $\mathrm{PGL}(2,q)/A_5, \mathrm{PSL}(2,q)/A_5$ に subdegree 5 または 6 の suborbit が現れるか調べればよい事になる.

2.3 Approach(1) — suborbits を計算する

$q(q^2-1) \equiv 0 \pmod 5$ を満たす素数冪 q に対して, 単純に $A_5 \leq \mathrm{PSL}(2,q), \mathrm{PGL}(2,q)$ による cosets 上の suborbits を全て求めて, subdegree 5, 6 のものがあるか確かめさせる方法ではすぐにメモリ使用量の限界に達してしまう (今回の計算に使用した, メモリが 2GB 程度のコンピュータでは $q = 571$ が限界).

2.4 Approach(2) — normalizer を計算する

実は, 群の正規化群を計算することで subdegree 毎に suborbit が何個あるか知ることが出来る. その方法を紹介するため, まず記号を定義しておく.

G を集合 Ω 上の置換群とし, $K \leq G$ に対して

$$I_\Omega(K) := \{b \in \Omega \mid \forall g \in K,\ b^g = b\},$$
$$A_{L,M}(K) := \{K^g \mid g \in L,\ K^g \leq M\} \quad (L, M \leq G)$$

とする. $a \in \Omega$, $H = G_a$ とおく. ここで $H_1, \ldots, H_s$ を H の部分群の共役類の代表系とし, $\Omega_i := H/H_i$ とおくと, $\Omega \cong_H \bigcup_i y_i\Omega_i$ と分割できる. ただし y_i は H-集合 Ω_i と H-同値な H-orbit の個数を表す.

以上の記号の下で, 次の式が成り立つ.

Proposition 4 (Bannai–Iwasaki (1974))**.**

$$\sum_i y_i |I_{\Omega_i}(H_j)| = |I_\Omega(H_j)|, \qquad (*)$$
$$|I_\Omega(H_j)| = \frac{|A_{G,H}(H_j)||N_G(H_j)|}{|H|},$$
$$|I_{\Omega_i}(H_j)| = \frac{|A_{H,H_i}(H_j)||N_H(H_j)|}{|H_j|} \quad (1 \le j \le s).$$

連立方程式 $(*)$ の係数は $|A_{L,M}(K)|$ と normalizer の位数で表すことが出来, これを解けば y_i を得られる. この式を今回の計算の対象に当てはめてみよう.

$G := \mathrm{PSL}(2,q)$, $G \ge H := A_5$, $H \ge H_1, \ldots, H_9$: 部分群の共役類の代表系とすると

$$\sum_{i=1}^{9} y_i |I_{\Omega_i}(H_j)| = |I_\Omega(H_j)|, \qquad (*')$$
$$|I_\Omega(H_j)| = \frac{|A_{G,A_5}(H_j)||N_G(H_j)|}{|A_5|} = \frac{|N_G(H_j)|}{|N_{A_5}(H_j)|},$$
$$|I_{\Omega_i}(H_j)| = \frac{|A_{A_5,H_i}(H_j)||N_{A_5}(H_j)|}{|H_j|} \quad (1 \le j \le 9).$$

連立方程式 $(*')$ の係数のうち q に依存するのは $|N_G(H_j)|$ だけで, 他の値は A_5 の中だけで決まっている. この連立方程式を解くことで y_i を計算できる. 手順は以下のようになる.

前処理

$$A_5 \ge H_1 = A_5, H_2 = A_4, \cdots, H_9 = 1,$$
$$c_{ij} = |I_{\Omega_i}(H_j)| = \frac{|A_{A_5,H_i}(H_j)||N_{A_5}(H_j)|}{|H_j|} \quad (1 \ge i, j \ge 9)$$

を計算しておき,

$$C := (c_{ij})_{i,j=1}^{9}$$

と 9 次正方行列を定める.

素数冪 q : $q(q^2-1) \equiv 0 \pmod 5$ に対して

$G := \mathrm{PSL}(2,q) \geq H = A_5$, $j = 1, \ldots 9$ に対して $N_G(H_j)$ を求める. 以上の準備より, 連立方程式 (∗') を解く.

$$(y_1, \ldots, y_9)C = \left(\frac{|N_G(H_1)|}{|N_{A_5}(H_1)|}, \ldots \frac{|N_G(H_9)|}{|N_{A_5}(H_9)|} \right).$$

つまり C^{-1} を掛けて, $y_1, \ldots, y_9$ を得る.

前の方法では $q = 571$ までが限界であったが, この方法なら $q = 709$ まで調べられる.

2.5 Results

最後に, $\mathrm{PSL}(2,q)$-集合 $\mathrm{PSL}(2,q)/A_5$ 上の subdegree 毎の suborbit の個数を以下に記す. $q = 11, 19, 25, 29, 31, 41$ の場合だけは [1] に掲載されている. この計算結果を基に $\mathrm{PGL}(2,q)/A_5, \mathrm{PSL}(2,q)/A_5$ 上の suborbits に 2-arc-transitive graph が現れる条件を決定するのが, 今後の目標である.

q \ subdegrees	60	30	20	15	12	10	6	5	1
9	0	0	0	0	0	0	0	1	1
11	0	0	0	0	0	1	0	0	1
16	0	0	2	1	1	0	0	0	1
19	0	1	1	0	0	0	1	0	1
25	0	2	1	0	4	0	0	0	2
29	1	3	2	0	1	0	0	0	1
31	2	3	1	0	1	0	0	1	1
41	7	3	2	0	1	0	1	1	1
49	13	4	2	0	2	1	0	1	1
59	24	5	4	0	2	1	1	0	1
61	27	5	4	0	2	1	1	0	1
64	67	0	10	5	6	0	0	0	1
71	44	7	4	0	3	1	0	1	1
79	62	8	5	0	3	0	1	1	1
81	65	8	12	0	3	0	1	1	1
89	90	10	6	0	4	0	0	1	1
101	134	11	8	0	4	0	1	0	1
109	170	12	8	0	5	1	0	0	1

q \ subdegrees	60	30	20	15	12	10	6	5	1
121	236	12	8	0	5	1	1	1	1
125	258	15	10	0	12	0	0	0	1
131	300	15	10	0	6	1	0	0	1
139	360	16	11	0	6	0	1	0	1
149	445	18	12	0	7	0	0	0	1
151	464	18	11	0	7	0	0	1	1
169	655	19	12	0	8	1	0	1	1
179	780	20	14	0	8	1	1	0	1
181	807	20	14	0	8	1	1	0	1
191	950	22	14	0	9	1	0	1	1
199	1076	23	15	0	9	0	1	1	1
211	1284	26	17	0	10	0	0	0	1
229	1646	27	18	0	11	1	0	0	1
239	1874	27	18	0	11	1	1	1	1
241	1922	27	18	0	11	1	1	1	1
251	2172	30	20	0	12	1	0	0	1
256	4636	0	42	21	25	0	0	0	1
269	2677	33	22	0	13	0	0	0	1

q \ subdegrees	60	30	20	15	12	10	6	5	1
271	2738	33	21	0	13	0	0	1	1
281	3055	33	22	0	13	0	1	1	1
289	3325	34	22	0	14	1	0	1	1
311	4148	37	24	0	15	1	0	1	1
331	5004	41	27	0	16	0	0	0	1
349	5870	42	28	0	17	1	0	0	1
359	6392	42	28	0	17	1	1	1	1
361	6500	42	28	0	17	1	1	1	1
379	7524	46	31	0	18	0	1	0	1
389	8137	48	32	0	19	0	0	0	1
401	8917	48	32	0	19	0	1	1	1
409	9463	49	32	0	20	1	0	1	1
419	10176	50	34	0	20	1	1	0	1
421	10323	50	34	0	20	1	1	0	1
431	11078	52	34	0	21	1	0	1	1
439	11708	53	35	0	21	0	1	1	1
449	12528	55	36	0	22	0	0	1	1
461	13562	56	38	0	22	0	1	0	1
479	15218	57	38	0	23	1	1	1	1
491	16392	60	40	0	24	1	0	0	1
499	17208	61	41	0	24	0	1	0	1
509	18265	63	42	0	25	0	0	0	1
521	19591	63	42	0	25	0	1	1	1
529	20509	64	42	0	26	1	0	1	1
541	21939	65	44	0	26	1	1	0	1
569	25530	70	46	0	28	0	0	1	1
571	25800	71	47	0	28	0	0	0	1
599	29792	72	48	0	29	1	1	1	1
601	30092	72	48	0	29	1	1	1	1
619	32880	76	51	0	30	0	1	0	1
625	33828	77	51	0	124	0	0	0	2
631	34832	78	51	0	31	0	0	1	1
641	36517	78	52	0	31	0	1	1	1
659	39684	80	54	0	32	1	1	0	1
661	40047	80	54	0	32	1	1	0	1
691	45756	86	57	0	34	0	0	0	1
701	47774	86	58	0	34	0	1	0	1
709	49430	87	58	0	35	1	0	0	1

q \ subdegrees	60	30	20	15	12	10	6	5	1
719	51554	87	58	0	35	1	1	1	1
729	53716	90	120	0	36	0	0	1	1
739	55980	91	61	0	36	0	1	0	1
751	58754	93	61	0	37	0	0	1	1
761	61135	93	62	0	37	0	1	1	1
769	63085	94	62	0	38	1	0	1	1
809	73458	100	66	0	40	0	0	1	1
811	74004	101	67	0	40	0	0	0	1
821	76778	101	68	0	40	0	1	0	1
829	79046	102	68	0	41	1	0	0	1
839	81944	102	68	0	41	1	1	1	1
841	82532	102	68	0	41	1	1	1	1
859	87948	106	71	0	42	0	1	0	1
881	94885	108	72	0	43	0	1	1	1
911	104918	112	74	0	45	1	0	1	1
919	107708	113	75	0	45	0	1	1	1
929	111264	115	76	0	46	0	0	1	1
941	115634	116	78	0	46	0	1	0	1
961	123170	117	78	0	47	1	1	1	1
971	127056	120	80	0	48	1	0	0	1
991	135074	123	81	0	49	0	0	1	1
1009	142573	124	82	0	50	1	0	1	1
1019	146856	125	84	0	50	1	1	0	1
1021	147723	125	84	0	50	1	1	0	1
1024	298163	0	170	85	102	0	0	0	1
1031	152108	127	84	0	51	1	0	1	1
1039	155678	128	85	0	51	0	1	1	1
1049	160218	130	86	0	52	0	0	1	1
1051	161136	131	87	0	52	0	0	0	1
1061	165782	131	88	0	52	0	1	0	1
1069	169562	132	88	0	53	1	0	0	1
1091	180252	135	90	0	54	1	0	0	1
1109	189325	138	92	0	55	0	0	0	1
1129	199759	139	92	0	56	1	0	1	1
1151	211670	142	94	0	57	1	0	1	1
1171	222900	146	97	0	58	0	0	0	1
1181	228662	146	98	0	58	0	1	0	1
1201	240482	147	98	0	59	1	1	1	1

提出日の時点では，ここまで計算出来ている．

参考文献

[1] E. Bannai and S. Iwasaki, A note on the subdegrees of finite permutation groups, Hokkaido Math. J. 3 (1974), pp. 95-97.

[2] P. J. Cameron, Suborbits in transitive permutation groups. in Combinatorics (eds. M. Hall, Jr. and J. H. van Lint), Part 3, Math. Centre Tracts 57 (1974), pp. 98-129.

[3] P. J. Cameron and C. E. Praeger, On 2-arc transitive graphs of girth 4. J. Combin. Theory Ser. **B 35** (1983), pp. 1-11.

[4] L. E. Dickson, Linear groups : with an exposition of the Galois field theory, B. G. Teubner, 1901.

[5] L. L. Scott, Integral equivalence of permutation representations, in Group Theory, (Granville, OH, 1992), eds. S. Sehgal and R. Solomon, pp. 262-274.

パラフェルミオン頂点作用素代数の C_2 代数

山田裕理[1]
一橋大学大学院経済学研究科

1 はじめに

頂点作用素代数は、無限個の演算を持つ $\mathbb{C}$ 上の無限次元ベクトル空間であり、その構造は複雑である．Y. Zhu [7] は、頂点作用素代数 V に対して 2 つの結合的代数 $A(V)$ と $V/C_2(V)$ を導入した．これら 2 つの結合的代数は、頂点作用素代数よりはるかに簡単な構造であり、実際多くの例では有限次元になる．その一方、$A(V)$ と $V/C_2(V)$ はもとになる頂点作用素代数 V の特徴を反映しており、それらを詳しく調べることは、大切な研究課題である。

本稿では、基本的な頂点作用素代数のひとつであるパラフェルミオン頂点作用素代数の C_2 代数 $V/C_2(V)$ を考察する．パラフェルミオン頂点作用素代数 $K(\mathfrak{g},k)$ は、任意の有限次元単純 Lie 代数 $\mathfrak{g}$ と任意の正の整数 k に対して定義されるが、ここでは $\mathfrak{g}=sl_2$ の場合を扱う．$K(sl_2,k)$ について、生成元、作用素積展開、特異ベクトル、自己同型群などの基本的なことは [1, 2] で知られている[2]．それらをもとにして、$K(sl_2,k)$ の C_2 代数が有限次元であることが証明できる．ここではその証明の概略を紹介する．

一般の有限次元単純 Lie 代数 $\mathfrak{g}$ のときのパラフェルミオン頂点作用素代数 $K(\mathfrak{g},k)$ は、Dong と Wang [3, 4] により研究されているが、そこでは $\mathfrak{g}=sl_2$ の場合の重要性が指摘されている．実際、$K(\mathfrak{g},k)$ は $K(\mathfrak{g}_\alpha,k_\alpha)$ たちで頂点作用素代数として生成される．ここで、α は Lie 代数 $\mathfrak{g}$ の正ルート全体を動き、$\mathfrak{g}_\alpha$ は α に対応する sl_2 と同型な部分 Lie 代数で、k_α は α の長さに依存して定まる正の整数である．

本稿の内容は、荒川知幸氏、Ching Hung Lam 氏との共同研究で得られた結果に基づくものである．

桑原敏郎氏と鈴木武史氏には、研究の途中で貴重なアドバイスを頂いた．本研究で必要となるグレブナー基底の計算は、計算機代数システム Risa/Asir により行ったが、その際に横山和弘氏に様々な助言をいただいた．

[1]本研究の一部は日本学術振興会科学研究費補助金 基盤研究 (C) No.23540009 の助成を受けている．

[2][2] の計算の一部は AC2007 で報告した．

2 頂点作用素代数の C_2 代数

本節では、頂点作用素代数の C_2 代数に関する基本的な事項をまとめる．頂点作用素代数については、[5] および [6] を参照してください．$(V, Y, \mathbf{1}, \omega)$ あるいは簡単に V を頂点作用素代数 (vertex operator algebra, VOA) とする．V は $V = \oplus_{n\geq 0} V_{(n)}$ と直和分解される．$V_{(n)}$ はウエイト n の部分空間と呼ばれ、有限次元である．$V_{(n)}$ の元をウエイト n の元という．$v \in V$ に対して、$Y(v,z) = \sum_{n\in\mathbb{Z}} v_n z^{-n-1}$ を v に付随する頂点作用素 (vertex operator) という．ここで $v_n \in \operatorname{End} V$ で、$Y(v,z)$ は z を形式的な変数とする V の線型変換の母関数である．本稿では特に断らない限り、V の元 v に対して整数 n の下付き v_n は上記の意味で用いるものとする．$v \in V_{(m)}$ のとき、$v_n V_{(s)} \subset V_{(s+m-n-1)}$ が成り立つ．$\mathbf{1}$ および ω は、それぞれ真空ベクトルおよび Virasoro ベクトル (共形元) と呼ばれる特別な元である．

頂点作用素代数の定義では $Y(v,z)$ が満たすべき条件が規定されているが、その中でも次の 2 つの公式は特に大切である．

$$[u_m, v_n] = \sum_{i\geq 0} \binom{m}{i} (u_i v)_{m+n-i} \tag{2.1}$$

$$(u_m v)_n = \sum_{i\geq 0} (-1)^i \binom{m}{i} \bigl(u_{m-i} v_{n+i} - (-1)^m v_{m+n-i} u_i\bigr) \tag{2.2}$$

$u, v \in V$ と $n \in \mathbb{Z}$ に対して、$u_n v$ は V に含まれるが、これを u と v の V における演算と考えると、頂点作用素代数 V は無限個の演算を持つことになる．S を V の部分集合とする．S に属する元にこの演算を繰り返して得られる元 $u^1_{n_1} \cdots u^r_{n_r} v$ $(u^i \in S,\, v \in S,\, n_i \in \mathbb{Z})$ で張られる V の部分空間を $\langle S \rangle$ で表す．$\langle S \rangle = V$ が成り立つとき、頂点作用素代数 V は S で生成される、あるいは S は V の生成系であるという．このときの n_i は任意の整数であるが、n_i たちを負の整数に限って、$u^1_{-m_1} \cdots u^r_{-m_r} v$ $(u^i \in S,\, v \in S,\, m_i \geq 1)$ で V が張られるとき、S は V の強い生成系であるという．

$u_{-2}v$ $(u, v \in V)$ の形の V の元で張られる部分空間を $C_2(V)$ で表す．

$$C_2(V) = \operatorname{span}_{\mathbb{C}}\{u_{-2}v \,|\, u, v \in V\}.$$

$C_2(V)$ による剰余空間 $R_V = V/C_2(V)$ には、$\overline{u} \cdot \overline{v} = \overline{u_{-1}v}$ および $\{\overline{u}, \overline{v}\} = \overline{u_0 v}$ と定義することにより、可換な Poisson 代数の構造が入る．ただし、$\overline{v} = v + C_2(V)$ である．この Poisson 代数 R_V は Zhu [7] により導入され、C_2 代数あるいは Zhu の Poisson 代数と呼ばれる．積 $\overline{u} \cdot \overline{v} = \overline{u_{-1}v}$ に関して R_V は可換な結合代数であるが、これが有限次元になるとき頂点作用素代数 V は C_2 余有限 (C_2-cofinite) であるという．

S が V の強い生成系の場合、R_V は $\{\overline{u} \,|\, u \in S\}$ で可換結合代数として生成される．特に、強い生成系 S が有限集合 $S = \{u^1, \ldots, u^r\}$ であれば、R_V は $\overline{u^1}$, …, $\overline{u^r}$

で生成される可換結合代数なので、r 変数多項式環の準同型像になる．したがってこの場合には、R_V が有限次元であることと、$\overline{u^i}$, $i = 1, \dots, r$ がすべてベキ零であることは同値である．

実際、パラフェルミオン頂点作用素代数 $K(sl_2, k)$ の C_2 代数 $R_{K(sl_2,k)}$ が有限次元であることは、このような方針で証明する．

3 パラフェルミオン頂点作用素代数 $\mathcal{W} = K(sl_2, k)$

簡単のため、$\mathcal{W} = K(sl_2, k)$ とおく．$k = 2, 3, 4$ のときは $\mathcal{W}$ はそれぞれ $\mathcal{L}(1/2, 0)$ (Ising model), $\mathcal{L}(4/5, 0) \oplus \mathcal{L}(4/5, 3)$ (3-state Potts model), $V^+_{\mathbb{Z}\alpha}$ (ただし $\langle \alpha, \alpha \rangle = 6$) という良く知られた頂点作用素代数になる (cf. [2, Section 5])．したがって、以下では $k \geq 5$ とする．アフィン Lie 代数 $\widehat{sl}_2$ に付随する レベル k の単純アフィン頂点作用素代数を $L(k, 0) = L_{\widehat{sl}_2}(k, 0)$ で表す．パラフェルミオン頂点作用素代数 $\mathcal{W}$ は、sl_2 の Cartan 部分代数から生成される $L(k, 0)$ における Heisenberg 代数のコミュタント (commutant) として定義される．$\widehat{sl}_2$ のレベル k の Weyl 加群 $V(k, 0) = V_{\widehat{sl}_2}(k, 0)$ における Heisenberg 代数のコミュタントを $\mathcal{V}$ とおき、$\mathcal{V}$ の唯一つの極大イデアルを $\mathcal{I}$ とおくと、$\mathcal{W} = \mathcal{V}/\mathcal{I}$ である．

sl_2 の Chevalley 基底を $\{h, e, f\}$ とする．Lie 積は $[h, e] = 2e$, $[h, f] = -2f$, $[e, f] = h$ であり、正規化された Killing 形式 $\langle \, , \rangle$ について $\langle h, h \rangle = 2$, $\langle e, f \rangle = 1$, $\langle h, e \rangle = \langle h, f \rangle = \langle e, e \rangle = \langle f, f \rangle = 0$ が成り立つ．アフィン Lie 代数

$$\widehat{sl}_2 = sl_2 \otimes \mathbb{C}[t, t^{-1}] \oplus \mathbb{C}C$$

に対して、Weyl 加群 $V(k, 0)$ は、

$$V(k, 0) = \mathrm{Ind}^{\widehat{sl}_2}_{sl_2 \otimes \mathbb{C}[t] \oplus \mathbb{C}C} \mathbb{C} = U(\widehat{sl}_2) \otimes_{U(sl_2 \otimes \mathbb{C}[t] \oplus \mathbb{C}C)} \mathbb{C}$$

という誘導加群である．ここでは、$\mathbb{C}$ は $sl_2 \otimes \mathbb{C}[t]$ が 0 と作用し、C が定数 k として作用する $sl_2 \otimes \mathbb{C}[t] \oplus \mathbb{C}C$ 加群である．$a \otimes t^n$ の $V(k, 0)$ への作用を $a(n)$ で表すと、それらの作用の交換関係は

$$[a(m), b(n)] = [a, b](m + n) + m\langle a, b \rangle \delta_{m+n,0} k \tag{3.1}$$

となる．$\mathbf{1} = 1 \otimes 1$ が真空ベクトルで、$n \geq 0$ ならば $a(n)\mathbf{1} = 0$ である．このことと (3.1) の交換関係により、$a(n)$ の $V(k, 0)$ への作用は具体的に計算できる．

$$h(-i_1) \cdots h(-i_p) e(-j_1) \cdots e(-j_q) f(-m_1) \cdots f(-m_r)\mathbf{1}, \tag{3.2}$$

($i_1 \geq \cdots \geq i_p \geq 1$, $j_1 \geq \cdots \geq j_q \geq 1$, $m_1 \geq \cdots \geq m_r \geq 1$, $p, q, r \geq 0$) は $V(k, 0)$ の基底となる．

以下、[1, 2] に沿って $\mathcal{V}$ および $\mathcal{W}$ の基本的な性質をまとめておく．記号も特に説明しない限り [1, 2] に従う．$V(k,0)$ は $e(-1)^{k+1}\mathbf{1}$ で生成される唯一つの極大イデアル (可積分条件) を持ち、その極大イデアルによる剰余代数が $L(k,0)$ である．簡単のため、$a(n)$ が引き起こす $L(k,0)$ への作用を、同じ記号 $a(n)$ で表すことにする．

$\mathcal{V}$ は、$\mathcal{V} = \{v \in V(k,0) \,|\, h(n)v = 0 \text{ for all } n \geq 0\}$ で定義される $V(k,0)$ の部分頂点作用素代数であり、また $\mathcal{W} = \{v \in L(k,0) \,|\, h(n)v = 0 \text{ for all } n \geq 0\}$ である．$e(-1)^{k+1}\mathbf{1}$ は $\mathcal{V}$ には含まれず、$\mathcal{V}$ の唯一つの極大イデアル $\mathcal{I}$ は

$$\mathbf{u}^0 = f(0)^{k+1}e(-1)^{k+1}\mathbf{1}$$

で生成される．

$\mathcal{V}$ について、次のことがで知られている (cf. [1, 2])．

(1) 4 個の元からなる $\mathcal{V}$ の強い生成系 $\{W^2, W^3, W^4, W^5\}$．ここで、W^r はウエイト r の元で、W^2 は Virasoro ベクトル ω である．

(2) W^2, W^3, W^4, W^5 の作用素積展開．

(3) $\mathcal{V}$ の自己同型群は θ で生成される位数 2 の群である．θ は生成系 W^s $(s = 2,3,4,5)$ に $\theta(W^s) = (-1)^s W^s$ と作用する．

(4) ウエイト 8 の null field と呼ばれる特異ベクトル $\mathbf{v}^0$ および上記のウエイト $k+1$ の特異ベクトル $\mathbf{u}^0$．

強い生成系 $\{W^2, W^3, W^4, W^5\}$ により、$\mathcal{V}$ は

$$W^2_{-i_1} \cdots W^2_{-i_p} W^3_{-j_1} \cdots W^3_{-j_q} W^4_{-m_1} \cdots W^4_{-m_r} W^5_{-n_1} \cdots W^5_{-n_s}\mathbf{1} \tag{3.3}$$

$(i_1 \geq \cdots \geq i_p \geq 1, j_1 \geq \cdots \geq j_q \geq 1, m_1 \geq \cdots \geq m_r \geq 1, n_1 \geq \cdots \geq n_s \geq 1)$ の形のベクトルで張られるが、これらのベクトルは線型独立ではない．実際、ウエイトが 7 以下のものは線型独立であるが、ウエイトが 8 のものは線型独立ではく 2 個の非自明な線型関係がある．そのうちのひとつが $\mathbf{v}^0 = 0$ と null field $\mathbf{v}^0$ を用いて表されるものである．もう一方のウエイト 8 の非自明な線型関係は $C_2(V(k,0))$ に含まれるため、$R_{V(k,0)}$ においては 0 になる．なお、W^s_n は頂点作用素 $Y(W^s,z) = \sum_{n\in\mathbb{Z}} W^s_n z^{-n-1}$ に現れる $\mathrm{End}\,\mathcal{V}$ の元を表す．

$W^r_i W^s$ が (3.3) の形のベクトルの線型結合で表されていれば、公式 (2.1), (2.2) により、W^s_n たちの交換関係 $[W^r_m, W^s_n]$ がわかる．上記 (2) の作用素積展開とは、(3.3) の形のベクトルの線型結合としての $W^r_i W^s$ の具体的な表示を意味する (cf. [2, Appendix B])．

4 $\mathcal{W}$ の C_2 代数 $R_{\mathcal{W}} = \mathcal{W}/C_2(\mathcal{W})$

前節で説明したように $\mathcal{W} = \mathcal{V}/\mathcal{I}$ なので、C_2 代数については $C_2(\mathcal{W}) = C_2(\mathcal{V})\mathcal{I}/\mathcal{I}$ および $\mathcal{W}/C_2(\mathcal{W}) \cong \mathcal{V}/C_2(\mathcal{V})\mathcal{I}$ が成り立つ．そのため、(i) $R_{\mathcal{V}} = \mathcal{V}/C_2(\mathcal{V})$、(ii) 極大イデアル $\mathcal{I}$ から得られる情報、の 2 段階に分けて $R_{\mathcal{W}} = \mathcal{W}/C_2(\mathcal{W})$ を調べることにする．なお、$R_{\mathcal{V}}$ は無限次元であることに注意する．

$\{W^2, W^3, W^4, W^5\}$ は $\mathcal{V}$ の強い生成系なので、$R_{\mathcal{V}}$ は $\widetilde{W^s} = W^s + C_2(\mathcal{V})$ $(s = 2, 3, 4, 5)$ で生成される可換結合代数である．よって、

$$\varphi : \mathbb{C}[x_2, x_3, x_4, x_5] \to R_{\mathcal{V}}; \quad x_s \mapsto \widetilde{W^s}$$

という 4 変数多項式環から $R_{\mathcal{V}}$ への全準同型が存在する．W^s がウエイト s なので、それに対応して変数 x_s についてもそのウエイトを s と定める．

次に、$R_{\mathcal{V}}$ を $R_{V(k,0)}$ に埋め込むことを考える．一般に、頂点作用素代数 V とその部分代数 U について、C_2 の定義から $C_2(U) \subset U \cap C_2(V)$ が成り立つ．したがって、$\mathcal{A} = \mathcal{V} + C_2(V(k,0))$ とおくと、

$$\psi : R_{\mathcal{V}} \to \mathcal{A}; \quad W^s + C_2(\mathcal{V}) \mapsto W^s + C_2(V(k,0))$$

という自然な全準同型が得られる．$u \in V(k,0)$ に対して、$\overline{u} = u + C_2(V(k,0))$ とおく．さらに、$y_0 = \overline{h(-1)\mathbf{1}}$, $y_1 = \overline{e(-1)\mathbf{1}}$, $y_2 = \overline{f(-1)\mathbf{1}}$ とおくと、(3.2) の形のベクトルが $V(k,0)$ の基底であることから、$R_{V(k,0)}$ は y_0, y_1, y_2 を変数とする多項式環 $\mathbb{C}[y_0, y_1, y_2]$ に同型である．さらに、$y = y_0$, $z = y_1 y_2$ とおくと、

$$\begin{aligned}
\overline{W^2} &= -\frac{1}{2k(k+2)}(y^2 - 2kz), \\
\overline{W^3} &= 2(y^3 - 3kyz), \\
\overline{W^4} &= -(11k+6)y^4 + 4k(11k+6)y^2 z - 2k^2(6k-5)z^2, \\
\overline{W^5} &= -2(19k+12)y^5 + 10k(19k+12)y^3 z - 10k^2(10k-7)yz^2
\end{aligned}$$

が成り立つことから、$\mathcal{A} \subset \mathbb{C}[y, z]$ がわかる．なお、頂点作用素代数 $V(k,0)$ の元として $h(-1)\mathbf{1}$, $e(-1)\mathbf{1}$, $f(-1)\mathbf{1}$ のウエイトはどれも 1 なので、それに対応して y, z のウエイトはそれぞれ 1, 2 となる．

φ と ψ の合成

$$\psi \circ \varphi : \mathbb{C}[x_2, x_3, x_4, x_5] \to R_{\mathcal{V}} \to \mathcal{A}; \quad x_s \mapsto \widetilde{W^s} \mapsto \overline{W^s}$$

は、4 変数多項式環 $\mathbb{C}[x_2, x_3, x_4, x_5]$ から 2 変数多項式環 $\mathbb{C}[y, z]$ への準同型なので、$\mathrm{Ker}\, \psi \circ \varphi$ は 0 ではない．実際、$\mathrm{Ker}\, \psi \circ \varphi$ は次の 3 つの多項式で生成されるイデアルであることが確かめられる．

$$\begin{aligned}
&-112k^4(k+2)^4(3k+4)(6k-5)(64k+107)x_2^4 + k(k+2)(16k+17)^2(26k+83)x_2 x_3^2 \\
&\quad - 4k^2(k+2)^2(36k+61)(64k+107)x_2^2 x_4 + 2(64k+107)x_4^2 + (16k+17)^2 x_3 x_5,
\end{aligned}$$

$$-16k^3(k+2)^3(674k^2+637k-1100)x_2^3x_3+(16k+17)(64k+107)x_3^3$$
$$-4k(k+2)(358k+559)x_2x_3x_4-112k^2(k+2)^2(3k+4)x_2^2x_5+4x_4x_5,$$

$$128k^5(k+2)^5(6k-5)(64k+107)(305k^2+777k+306)x_2^5$$
$$-4k^2(k+2)^2(16k+17)(17696k^3+71122k^2+91905k+29934)x_2^2x_3^2$$
$$+32k^3(k+2)^3(64k+107)(1108k^2+1853k+17)x_2^3x_4-(16k+17)(64k+107)^2x_3^2x_4$$
$$+16k(k+2)(64k+107)(83k+119)x_2x_4^2+2(16k+17)^2x_5^2.$$

変数 x_s のウエイトを s として、これらの多項式はそれぞれウエイトが 8, 9, 10 の斉次多項式である．実は、これら 3 つの多項式で生成されるイデアルのグレブナー基底は、ウエイト 12 の多項式を 1 つ加えた全部で 4 つの多項式からなるが、そのウエイト 12 の多項式は上記の 3 つの多項式を用いて容易に表すことができる．

$\mathrm{Ker}\,\psi\circ\varphi$ に関するこれらのことは、横山和弘氏により Risa/Asir を用いて計算された．横山氏に厚く御礼申し上げる．

[2, Section2] では、それぞれウエイトが 8, 9, 10 の null field、すなわち (3.3) の形のベクトルの $\mathcal{V}$ における非自明な線型関係の $R_{\mathcal{V}}$ における像と対応する x_2, x_3, x_4, x_5 の多項式 B_0, B_1, B_2 が与えられている．B_0 と $-B_1$ は上記のウエイト 8 および 9 の多項式と一致する．B_2 と上記のウエイト 10 の多項式は異なるが、B_0, B_1, B_2 で生成されるイデアルは、上記 3 つの多項式で生成されるイデアルに一致する．このことは、2 つのイデアルのグレブナー基底が同じであることから確かめられる．ところで、null field は $\mathcal{V}$ において 0 であるから、$\varphi(B_0)=\varphi(B_1)=\varphi(B_2)=0$ である．B_0, B_1, B_2 が $\mathrm{Ker}\,\psi\circ\varphi$ を生成するので、これは ψ が単射であることを意味する．以上により、次の定理が得られた．

定理 1. $C_2(\mathcal{V})=\mathcal{V}\cap C_2(V(k,0))$、特に $R_{\mathcal{V}}\cong\mathcal{A}$.

特異ベクトル $\mathbf{u}^0=f(0)^{k+1}e(-1)^{k+1}\mathbf{1}$ で生成される $\mathcal{V}$ の唯一つの極大イデアル $\mathcal{I}$ を調べる．$\overline{\mathbf{u}^0}=\mathbf{u}^0+C_2(V(k,0))\in\mathbb{C}[y,z]$ について、

$$f_0(y,z)=\frac{(-1)^{k+1}}{(k+1)!}\overline{\mathbf{u}^0}\in\mathbb{C}[y,z]$$

とおく．$f_0(y,z)$ は次のように表すことができる．

補題 2.

$$f_0(y,z)=\sum_{j=0}^{[(k+1)/2]}c_jy^{k+1-2j}z^j,\qquad c_j=(-1)^j\frac{(k+1)!}{(k+1-2j)!\,(j!)^2}.$$

特異ベクトル $\mathbf{u}^0$ だけではなく、その $W_1^3 \in \operatorname{End}\mathcal{V}$ による像も考える．$\mathbb{C}[y,z]$ に作用する微分作用素

$$D = \big((k+2)y^2 - 2kz\big)\frac{\partial}{\partial y} + (3k+4)yz\frac{\partial}{\partial z} \tag{4.1}$$

は、W_1^3 の作用と次のような関係がある．

補題 3. $v \in \mathcal{V}$ について、$\overline{v} = v + C_2(Vk,0)) \in \mathbb{C}[y,z]$ を $f(y,z)$ とおくと、$-6kD\,f(y,z) = \overline{W_1^3 v}$ が成り立つ．

$f_r(y,z) = D^r\,f_0(y,z)$ $(r = 1,2,\ldots)$ とおく．これらは $(W_1^3)^r\mathbf{u}^0 \in \mathcal{I}$ の $\mathcal{A}$ における像の定数倍に対応する．

$$\begin{vmatrix} \partial f_0/\partial y & \partial f_0/\partial z \\ \partial f_1/\partial y & \partial f_1/\partial z \end{vmatrix} \neq 0$$

が成り立つので、次のことがわかる．

補題 4. $f_0(y,z)$ と $f_1(y,z)$ は代数的に独立である．

$f_0(y,z)$ と $f_1(y,z)$ で生成される $\mathcal{A}$ のイデアルを $\langle f_0, f_1\rangle_{\mathcal{A}}$ で表すことにする．上記の補題より、次の補題が得られる．

補題 5. $\mathcal{A}/\langle f_0, f_1\rangle_{\mathcal{A}}$ は有限次元である．

$\mathcal{W}/C_2(\mathcal{W}) \cong \mathcal{V}/C_2(\mathcal{V})\mathcal{I}$ なので、$R_{\mathcal{V}} \cong \mathcal{A}$ と $(W_1^3)^r\mathbf{u}^0 \in \mathcal{I}$ に注意すると、この補題の系として目標であった次の定理が得られる．

定理 6. $R_{\mathcal{W}} = \mathcal{W}/C_2(\mathcal{W})$ は有限次元である．

$p(y,z) = -(k+1)(k+2)^2((k+1)y^2 + kz)$, $q(y) = (k+2)(2k+3)y$ とおくと、

$$f_2(y,z) = p(y,z)f_0(y,z) + q(y)f_1(y,z)$$

が成り立つので、$\mathbb{C}[y,z]$ におけるイデアルを考える際には $f_0(y,z)$ と $f_1(y,z)$ の 2 つで十分である．しかし、$p(y,z)$ も $q(y)$ も $\mathbb{C}[y,z]$ の部分環 $\mathcal{A}$ には含まれない．

より詳しく、$f_0(y,z)$ と $f_1(y,z)$ 生成される $\mathbb{C}[y,z]$ のイデアルを J とおくと、

$$\dim \mathbb{C}[y,z]/J = (k+1)(k+2)/2$$

である．一方、$f_0(y,z)$, $f_1(y,z)$, …, $f_{r-1}(y,z)$ で生成される $\mathcal{A}$ のイデアルを I_r とおくと、$I_2 \subsetneq I_3 \subsetneq I_4$ で、

$$\begin{aligned} \dim \mathcal{A}/I_2 &= (k+1)(k+2)/2, \\ \dim \mathcal{A}/I_3 &= k(k+1)/2 + 1, \\ \dim \mathcal{A}/I_4 &= k(k+1)/2 \end{aligned}$$

および、$I_4 = J \cap \mathcal{A}$ が成り立つ．特に、すべての r について $f_r(y,z) \in I_4$ である．

5 結語

パラフェルミオン頂点作用素代数 $\mathcal{W} = K(sl_2, k)$ は 4 個の元からなる強い生成系 $\{W^2, W^3, W^4, W^5\}$ を持つので、その C_2 代数 $R_{\mathcal{W}} = \mathcal{W}/C_2(\mathcal{W})$ は 4 変数多項式環の準同型像である．$R_{\mathcal{W}}$ が有限次元であることは、null field および可積分条件に関係する特異ベクトル $\mathbf{u}^0 = f(0)^{k+1}e(-1)^{k+1}\mathbf{1}$、およびそれの W_1^3 による像から従う．このような状況のため、本研究は多項式環のイデアルのグレブナー基底の計算と密接に関係する．

null field は無限個あるが、結果的には最初の 3 個、すなわちウエイトが 8, 9, 10 のもので十分であった．そのような理由のため、定理 1 の証明ではグレブナー基底の計算が本質的な役割を果たした．そこで扱う多項式は、係数にはパラメータの k を含むが、現れる項は限定されたものであり、計算機で扱えるものであった．

一方、特異ベクトル $\mathbf{u}^0$ から得られる多項式は、補題 2 からわかるように、含まれる項も次数もパラメータ k に依存するため、一般的な形では計算機で扱うことができない．もちろん k をひとつ定めた場合には、計算機で扱うことが可能であり、実際いくつかの k に対して例を計算して、一般的な場合の結果を推測することは試みている．しかし、k を定めた場合でも、最終的に必要なのは多項式環 $\mathbb{C}[y, z]$ のイデアルではなく、$\mathbb{C}[y, z]$ の部分環 $\mathcal{A}$ のイデアルである．多項式環の部分環のイデアルについて、そのグレブナー基底を計算することは、困難が伴う．

このような事情のため、null field に関係する部分は計算機で処理し、特異ベクトル $\mathbf{u}^0$ に関係する部分は計算機を用いずに数学的に手で計算した．そうではあるがしかし、計算機で得られたいくつかの例を参考にしなければ、数学的な計算も難しかったと思われる．

参考文献

[1] C. Dong, C.H. Lam, Q. Wang and H. Yamada, The structure of parafermion vertex operator algebras, *J. Algebra* **323** (2010), 371–381.

[2] C. Dong, C.H. Lam and H. Yamada, W-algebras related to parafermion algebras, *J. Algebra* **322** (2009), 2366–2403.

[3] C. Dong and Q. Wang, The structure of parafermion vertex operator algebras: general case, *Commun. Math. Phys.* **299** (2010), 783–792.

[4] C. Dong and Q. Wang, On C_2-cofiniteness of parafermion vertex operator algebras, *J. Algebra* **328** (2011), 420–431.

[5] I. B. Frenkel, J. Lepowsky and A. Meurman, *Vertex Operator Algebras and the Monster*, Pure and Applied Math., Vol. 134, Academic Press, Boston, 1988.

[6] J. Lepowsky and H.-S Li, *Introduction to Vertex Operator Algebras and Their Representations*, Progress in Math., Vol. 227, Birkhäuser, Boston, 2004.

[7] Y. Zhu, Modular invariance of characters of vertex operator algebras, *J. Amer. Math. Soc.* **9** (1996), 237–302.

有向グラフの mutation が生成する群について

入江 佑樹 Yuki Irie*

1 はじめに

変異 (mutation) は, 有向グラフに対する鏡映 (矢印の向きを逆にする操作) を変形した操作であり, Fomin と Zelevinsky がクラスター代数において導入した [3]. グラフ Γ から mutation を繰り返して得られるグラフ全体を Γ の mutation 同値類 と呼ぶ. このとき mutation は Γ の mutation 同値類上の位数 2 の置換となる.

本研究の目的は, mutation を mutation 同値類上の置換とみて, その群構造を計算・考察することである.

その結果, ほとんどの場合に交代群または対称群となるが, $\mathbb{Z}$ 上で頂点数が 4 の倍数の場合に 2 つの交代群の直積が現れる場合があることがわかった. また, $\mathbb{F}_q$ で頂点数が 3 の場合に例外的に $PSL(2,p)$ または $PGL(2,p)$ (p, q は素数) が現れる系列を発見し, 一般に証明した. その際に, 3 頂点の場合の mutation 不変量を得た.

2 mutation の定義

R を可換環とし, R から R への写像 $|\cdot|$ は

$$|a| = |-a| \in \{a, -a\} \ (\forall a \in R)$$

を満たすとする. また, $a \in R$ に対して $|a| = a$ のとき $a \geq 0$, $|a| = -a$ のとき $a \leq 0$ と表すことにする.

$\Gamma := (b_{ij})$ を成分が R の m 次交代行列とし, 隣接行列が Γ のグラフと同一視する. このとき, 頂点 $k \in \{1, 2, \ldots, m\}$ による Γ の mutation を次の m 次交代行列 $\Gamma^{\tau_k} := (b'_{ij})$ で定義する:

$$b'_{ij} := \begin{cases} -b_{ij} & (i = k \text{ or } j = k), \\ b_{ij} + |b_{ik}|b_{kj} & (b_{ik}, b_{kj} \geq 0 \text{ or } b_{ik}, b_{kj} \leq 0), \\ b_{ij} & (\text{otherwise}). \end{cases}$$

Γ に mutation を繰り返し施して得られる行列全体を Γ の mutation 同値類と呼び, O_Γ と表す. このとき, 各 mutation は, O_Γ 上の位数 2 の置換となる. そこで, $\tilde{G}_\Gamma := \langle \tau_k : O_\Gamma \to O_\Gamma \mid k \in \{1, 2, \ldots, m\} \rangle$ とおく. このとき, $\{\{\lambda, -\lambda\} \mid \lambda \in O_\Gamma\}$ は $\tilde{G}_\Gamma$ のブロック系になるので, このブロック系への作用の核 K で $\tilde{G}_\Gamma$ を割った群を G_Γ と表し, Γ の mutation が生成する群と呼ぶ.

O_Γ は一般には有限とは限らないが, ここでは有限となる場合のみを扱う.

* 千葉大学理学研究科 email: yirie@math.s.chiba-u.jp

3 $\mathbb{Z}$ 上の mutation($R = \mathbb{Z}$ の場合)

本節では, $\mathbb{Z}$ 上で mutation 同値類が有限となるグラフの分類の先行研究を紹介した後, それらの mutation が生成する群の計算結果を述べる. 以下, $m = 2$ の場合は自明なため, $m > 2$ とする.

3.1 有限となるグラフの分類

$\mathbb{Z}$ 上の mutation について, Buan と Reiten は 有限次元代数の表現論を応用し, mutation 同値類 O_Γ が有限となる tree の分類をした [1].

定理 3.1 (Buan, Reiten, 2006)**.** Γ が tree のとき O_Γ が有限となるのは, Γ から矢印を除いた無向グラフ[*1]が Coxeter-Dynkin 図形 $A_n, D_n, E_{6,7,8}$ とその拡大になる場合に限る.

さらに一般のグラフについては, Felikson らが分類した [2].

定理 3.2 (Felikson, Shapiro, Tumarkin, 2008)**.** O_Γ が有限となるのは, block decomposable なものか, Coxeter-Dynkin 図形 $E_{6,7,8}, \tilde{E}_{6,7,8}, E^{(1,1)}_{6,7,8}$ と $X_{6,7}$ になる場合に限る.

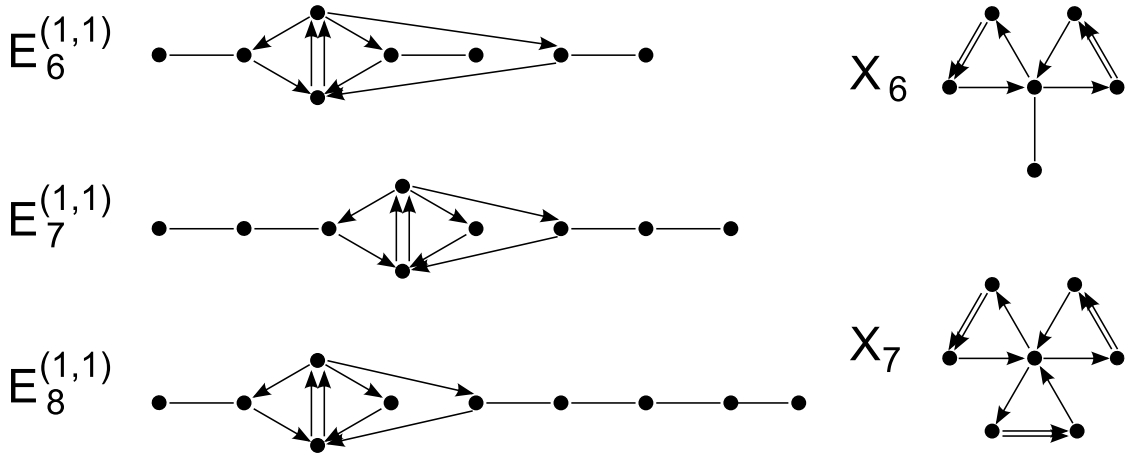


図 1 例外的に有限となるグラフ (向きの入っていない辺はどちら向きでも良いことを意味する)

なお, グラフが block decomposable とは図 2 の 6 種類のグラフの白丸同士を有限回同一視してできることを指す (黒丸は同一視できず, 一度同一視した白丸は黒丸になる). 白丸同士を同一視してできる block decomposable なグラフの例を図 3 に挙げる.

3.2 mutation が生成する群

mutation 同値類が有限となるグラフの内, 頂点数が 8 点以下の tree とその他いくつかの場合について群の構造を決定した. 表 1 と表 2 が結果である.

[*1] tree の場合, 矢印の向きを任意に変えても mutation 同値である.

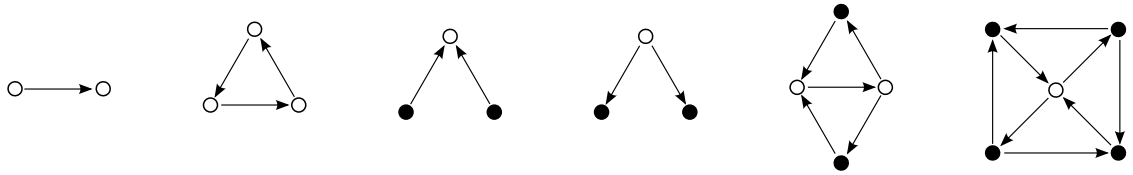


図 2　block decomposable

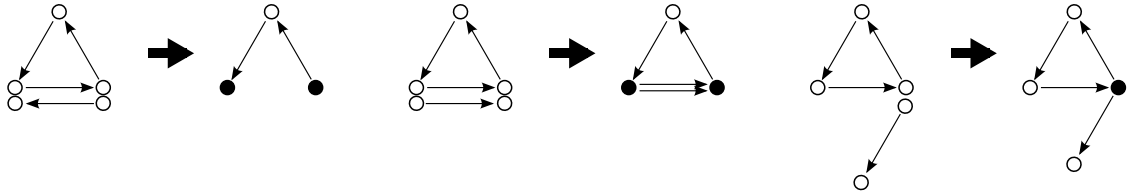


図 3　白丸を同一視してできる block decomposable なグラフ

Γ	G_Γ
A_3	S_7
A_4	$(A_{36} \times A_{36}) : 2$
A_5	S_{990}
A_6	A_{17160}
A_7	A_{360360}
A_8	$(A_{4455360} \times A_{4455360}) : 2$
D_4	A_{25}
D_5	A_{1092}
D_6	A_{20160}
D_7	A_{451440}
D_8	$A_{11891880}$

表 1　A_n, D_n

Γ	G_Γ
$\tilde{D}_4$	S_{135}
$\tilde{D}_5$	A_{8100}
$\tilde{D}_6$	S_{198450}
$\tilde{D}_7$	$A_{5715360}$
E_6	A_{21420}
$\tilde{E}_6$	A_{252000}
$E_6^{(1,1)}$	$(A_{294000} \times A_{294000}) : 2$
E_7	$A_{1048320}$
$\tilde{E}_7$	$A_{21168000}$
E_8	$(A_{15800400} \times A_{15800400}) : 2$
X_6	A_{780}
X_7	A_{840}

表 2　$\tilde{D}_n, E_n, \tilde{E}_n, E_n^{(1,1)}$

mutation 同値類や群構造は GAP を用いて計算した. ここで, 対称群や交代群は表のように次数が大きい場合でも短時間で判定できる[*2]. また, E_8 など 2 つの交代群の直積が現れる場合は, 次の方法で決定できた:

(1) Γ を m 頂点グラフとし, H を G_Γ の指数 2 の部分群 $\langle \tau_1\tau_2 K, \tau_1\tau_3 K, \ldots, \tau_1\tau_m K \rangle$ とする.
(2) H の軌道は 2 つあり, 同じ大きさ n であることがわかるので, それらを O_1, O_2 とする. そして, 各軌道に H を制限すると n 次交代群になることを確認する.
(3) O_1 の元のみ動かす H の元 h を次のようにして作る:

[*2] GAP 内部では Jordan による「次数 n の原始群がある素数 $p < n-2$ に対して p-cycle を持てば, n 次の対称群または交代群」という結果を応用している.

(a) 2 から m までをランダムに並べたものを $i_1, i_2, \ldots, i_{m-1}$ とする.

(b) $\sigma := \tau_1\tau_{i_1}\tau_1\tau_{i_2}\cdots\tau_1\tau_{i_{m-1}}K$ とおく.

(c) σ^l が O_1 の元のみ動かすような最小の正整数 l を求め, h を σ^l とする.

(4) 上の方法でいくつかの h を作り, これらが生成する群が n 次交代群となることを確認する.

4 3 頂点グラフ

本節では, 3 頂点グラフで例外的に群が射影群となる系列を紹介する. はじめにこの系列を見つけた実験を紹介する.

4.1 $\mathbb{F}_p$ における実験結果

100 以下の奇素数 p に対して, $\mathbb{F}_p$ 上で 3 頂点の全てのグラフについて mutation が生成する群を GAP を用いて計算した. その際, $|\cdot| : \mathbb{F}_p \to \mathbb{F}_p$ は次とした:

$$|a| := \begin{cases} a & (a \in \{1, 2, \cdots, \frac{p-1}{2}\}), \\ -a & (\text{otherwise}). \end{cases}$$

その結果, ほとんど全ての場合で交代群か対称群 (あるいはこれらに 2 群や 3 群がついた群) となった.
しかし, 次の 2 つの場合のみ例外的に $PGL(2,7)$ となった:

- $p = 43,\ \Gamma = (2, 19, 19)$,
- $p = 97,\ \Gamma = (2, 30, 30)$.

ここで (a, b, c) は次を表す:

$$(a, b, c) := \begin{bmatrix} 0 & a & -c \\ -a & 0 & b \\ c & -b & 0 \end{bmatrix}$$

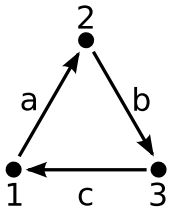


図 4 (a, b, c) の有向グラフによる表現

4.2 mutation 不変量

$\Gamma = (a, b, c)$ に対して, $a, b, c \geq 0$ または $a, b, c \leq 0$ のとき, Γ を cycle と呼び, そうでないとき acycle と呼ぶことにする. 3 頂点の場合, mutation で不変な量が存在する.

定義 4.1. $\Gamma = (a, b, c)$ に対して, $n := \#\{x \in \{a, b, c\} \mid x \leq 0\}$ とし, m_Γ を次で定義する:

$$\begin{aligned} m_\Gamma :&= \begin{cases} a^2 + b^2 + c^2 - abc & (n = 0, 1), \\ a^2 + b^2 + c^2 + abc & (n = 2, 3) \end{cases} \\ &= \begin{cases} a^2 + b^2 + c^2 - |a||b||c| & (\Gamma\text{は cycle}), \\ a^2 + b^2 + c^2 + |a||b||c| & (\Gamma\text{は acycle}). \end{cases} \end{aligned}$$

定理 4.2. m_Γ は mutation で不変.

4.3 $PGL(2,p), PSL(2,p)$

p を奇素数, 体 K は $\alpha^p = 1$ なる元 $\alpha \neq 1$ を含むとする. $a_i := \alpha^i + \alpha^{-i}$, $\Gamma := (a_0, a_1, a_1)$ とする. さらに $a_i > 0$ となるように, 写像 $|\cdot| : K \to K$ を取る.

このとき, m_Γ を考えることで次の補題を得る.

補題 4.3. (1) $(a_i, a_{i\pm j}, a_j)^{\tau_1} = -(a_i, a_{i\mp j}, a_j)$,
$(a_i, a_j, a_{i\pm j})^{\tau_2} = -(a_i, a_j, a_{i\mp j})$,
$(a_{i\pm j}, a_i, a_j)^{\tau_3} = -(a_{i\mp j}, a_i, a_j)$.

(2) $O_\Gamma = \{\pm(a_i, a_j, a_{i\pm j}) \mid i, j \in \{0, 1, \ldots, \frac{p-1}{2}\}\} \setminus \{\pm(a_0, a_0, a_0)\}$, 特に $|O_\Gamma| = p^2 - 1$.

(3) 任意の $(a_i, a_j, a_h) \in O_\Gamma$ に対して, $\{\pm(a_{ni}, a_{nj}, a_{nh}) \mid n \in \{1, 2, \ldots, \frac{p-1}{2}\}\}$ は G_Γ のサイズ $p-1$ の非原始ブロック.

補題の非原始ブロックからなるブロック系への作用の核で G_Γ を割った群を $\bar{G}_\Gamma$ と表すと, $\bar{G}_\Gamma$ は次になる.

定理 4.4.

$$\bar{G}_\Gamma \cong \begin{cases} PSL(2,p) & (p = 1 \pmod 4), \\ PGL(2,p) & (p = 3 \pmod 4). \end{cases}$$

参考文献

[1] A. B. Buan and I. Reiten. Acyclic quivers of finite mutation type. *International Mathematics Research Notices*, 2006.

[2] A. Felikson, M. Shapiro, and P. Tumarkin. Skew-symmetric cluster algebras of finite mutation type. *ArXiv e-prints*, November 2008.

[3] S. Fomin and A. Zelevinsky. Cluster algebras I: Foundations. *J. Amer. Math. Soc.*, 15:497–529, 2002.

巡回シロー p-部分群をもつ有限群のスコット加群
Scott modules in finite groups with cyclic Sylow p-subgroups

千葉大学理学研究科基盤理学専攻　高橋萌子

E-mail address: 08sm1113@graduate.chiba-u.jp

1　はじめに

これまで有限群の Scott 加群を求めるためには，p-局所部分群の Scott 加群を求め，対応する通常指標を用いて Green 対応子を計算しなければならなかった。群の位数が大きい場合には，GAP と呼ばれる計算システムが必要になることも多かった。

今回，有限群の Sylow p-部分群が巡回群である場合に，Brauer tree と通常指標の非自明な p-元上での値のみから Scott 加群を与える方法を得た。巡回 Sylow p-部分群をもつ有限群の Scott 加群は，主ブロックの Brauer tree における自明な指標に対応する頂点から例外頂点までの道の長さと密接に関係している。この道の長さの偶奇によって，Scott 加群の構造を分類し，対応する通常指標を与える。

本研究を始める動機となったのは，越谷-功刀 [7] 系 1.8 である．そこでは，trivial source module であって，vertex が属するブロックの巡回不足群 D と一致するようなものを，$N_G(D)$ のブロック B とその Brauer 対応子である $N_G(D_1)$ のブロック B_1 が Puig 同値である場合に全て与えている (ここで，D_1 は D の位数 p の部分群)．そこで，一般に，巡回不足群をもつブロックに属する trivial source module を知りたいと思い，その中でも特殊な加群である Scott 加群に限定して構造を与えたのが，本研究の結果である．

2　Scott 加群の定義

p を素数，k を標数 p の代数的閉体，G を有限群とする．加群は全て有限生成右側加群を考えるものとする．また，自明な kG-加群を k_G で表す．

定義 2.1. H を G の部分群とする．

次の 2 条件を満たす直既約 kG-加群が一意的に定まり，G の H に関する (Alperin) Scott 加群とばれる．また，この加群を $\mathrm{Scott}(G,H)$ で表す．

(1) $k_H\uparrow^G = k_H \otimes_{kH} kG$ の直既約直和因子である．[*1]
(2) socle の直和因子に自明な加群 k_G をもつ．
　(⇔ radical quotient の直和因子に k_G をもつ.)

[*1] i.e. Scott 加群は自明な source をもつ加群である．

Scott 加群は主ブロック (k_G が属するブロック) に属する．また，自己双対性をもつ．

G の全ての部分群に関する Scott 加群を考えられるが，次の命題より，G の p-部分群に関する Scott 加群のみを考えれば十分であることが分かる．

命題 2.1 (永尾-津島 [8] IV 章, 系 8.5)**.** H, H' を G の部分群，Q, Q' をそれぞれ H, H' の Sylow p-部分群とする．以下は同値である．

(1) $\mathrm{Scott}(G,H) \cong \mathrm{Scott}(G,H')$.
(2) Q と Q' は G-共役である．

特に，$\mathrm{Scott}(G,H) \cong \mathrm{Scott}(G,Q)$ である．

自明な群に関する Scott 加群 $\mathrm{Scott}(G,1)$ は k_G の projective cover である．また，G の Sylow p-部分群 P に関する Scott 加群は $\mathrm{Scott}(G,P) \cong k_G$ である．

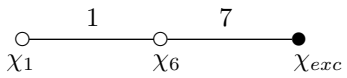
従ってこれ以降，自明な群でなく，Sylow 群でもない G の p-部分群に関する Scott 加群を考える．

3 例

$G := \mathrm{PSL}_2(8)$，$p = 3$ とする．G の Sylow 3-部分群を P とすると，$P \cong C_9$ であり，$N_G(P)$ は位数 18 の二面体群と同型である．$P_1 \cong C_3$ を P の部分群とし，$\mathrm{Scott}(G,P_1)$ を GAP を利用して計算する方法を紹介する．

kG の主ブロック A の分解行列，Brauer tree は次のように得られる．ここで 1，7 は次数を用いて既約 Brauer 指標を表している．

A	1	7
$1 = \chi_1$	1	·
$7_1 = \chi_2$	·	1
$7_2 = \chi_3$	·	1
$7_3 = \chi_4$	·	1
$7_4 = \chi_5$	·	1
$8 = \chi_6$	1	1



例外頂点の重複度 $m = 4$ である．

上の結果は GAP を用いて次のように得られる;

```
gap> G:=PSL(2,8);
Group([ (3,8,6,4,9,7,5), (1,2,3)(4,7,5)(6,9,8) ])
gap> P:=SylowSubgroup(G,3);
Group([ (1,8,6)(2,9,7)(3,5,4), (1,2,3,6,7,4,8,9,5) ])
```

```
gap>StructureDescription(P);
"C9"
gap> N:=Normalizer(G,P);
Group([ (1,8,6)(2,9,7)(3,5,4), (1,2,3,6,7,4,8,9,5), (2,5)(3,9)(4,7)(6,8) ])
gap> StructureDescription(N);
"D18"
gap> T:=CharacterTable("PSL(2,8)");;
gap> Display(T);
          2   3   3   .   .   .   .   .   .   .
          3   2   .   2   .   .   .   2   2   2
          7   1   .   .   1   1   1   .   .   .

              1a  2a  3a  7a  7b  7c  9a  9b  9c
        2P    1a  1a  3a  7b  7c  7a  9b  9c  9a
        3P    1a  2a  1a  7c  7a  7b  3a  3a  3a
        7P    1a  2a  3a  1a  1a  1a  9b  9c  9a

L2(8)
     X.1      1   1   1   1   1   1   1   1   1
     X.2      7  -1  -2   .   .   .   1   1   1
     X.3      7  -1   1   .   .   .   D   F   E
     X.4      7  -1   1   .   .   .   E   D   F
     X.5      7  -1   1   .   .   .   F   E   D
     X.6      8   .  -1   1   1   1  -1  -1  -1
     X.7      9   1   .   A   C   B   .   .   .
     X.8      9   1   .   B   A   C   .   .   .
     X.9      9   1   .   C   B   A   .   .   .
  A = E(7)+E(7)^6
  B = E(7)^3+E(7)^4
  C = E(7)^2+E(7)^5
  D = E(9)^2+E(9)^4+E(9)^5+E(9)^7
  E = -E(9)^4-E(9)^5
  F = -E(9)^2-E(9)^7
  gap> BlocksInfo(T mod 3);
  [ rec( defect := 2, ordchars := [ 1, 2, 3, 4, 5, 6 ], modchars := [ 1, 2 ],
        decinv := [ [ 1, 0 ], [ 0, 1 ] ], basicset := [ 1, 2 ],
        brauertree := [ [ 1, 6 ], [ 2, 3, 4, 5, 6 ] ] ),
    rec( defect := 0, ordchars := [ 7 ], modchars := [ 3 ], decinv := [ [ 1 ] ],
        basicset := [ 7 ] ),
    rec( defect := 0, ordchars := [ 8 ], modchars := [ 4 ], decinv := [ [ 1 ] ],      basicset := [ 8 ] ),
    rec( defect := 0, ordchars := [ 9 ], modchars := [ 5 ], decinv := [ [ 1 ] ],
        basicset := [ 9 ] ) ]
  gap> D:=DecompositionMatrix(T mod 3,1);
  [ [ 1, 0 ], [ 0, 1 ], [ 0, 1 ], [ 0, 1 ], [ 0, 1 ], [ 1, 1 ] ]
```

$\mathrm{Scott}(G, P_1)$ を求めるために，まず，$\mathrm{Scott}(N_G(P), P_1)$ と対応する通常指標[*2] を求める．$\mathrm{Scott}(N_G(P), P_1)$ は，$kN_G(P)$ の主ブロックに属する 2 つの 1 次元単純加群 1_1, 1_2 を組成因子にもつ長さ 3 の単列加群であり;

$$\mathrm{Scott}(N_G(P), P_1) \cong \begin{matrix} 1_1 \\ 1_2 \\ 1_1 \end{matrix}$$

下の $N_G(P)$ の指標表における "X.1+X.3" が対応する通常指標である．

```
gap> t:=CharacterTable(N);;
gap> Display(t);
CT1
         2    1    1    .    .    .    .
         3    2    .    2    2    2    2

              1a   2a   9a   9b   9c   3a
        2P    1a   1a   9b   9c   9a   3a
        3P    1a   2a   3a   3a   3a   1a
        5P    1a   2a   9c   9a   9b   3a
        7P    1a   2a   9b   9c   9a   3a

  X.1         1    1    1    1    1    1
  X.2         1   -1    1    1    1    1
  X.3         2    .    A    B    C   -1
  X.5         2    .    B    C    A   -1
  X.6         2    .    C    A    B   -1

A = E(9)^2+E(9)^7
B = E(9)^4+E(9)^5
C = -E(9)^2-E(9)^4-E(9)^5-E(9)^7
```

従って，"X.1+X.3" を G へ誘導すると

$$(X.1 + X.3)\uparrow^G = \chi_1 + \chi_3 + \chi_4 + \chi_5 + \chi_6 + 2(\chi_7 + \chi_8 + \chi_9)$$

となるので;

```
gap> ind:=(Irr(N)[1]+Irr(N)[3])^G;
Character( CharacterTable( Group([ (3,8,6,4,9,7,5), (1,2,3)(4,7,5)(6,9,8) ]) ), [ 84, 0, 0, 0, 4, 3,
0, 0, 0 ] )
gap> List(Irr(G),x -> ScalarProduct(x,ind));
[ 1, 0, 1, 1, 1, 1, 2, 2, 2 ]
```

[*2] trivial source module は持ち上げ可能な加群であり，対応する通常指標をもつ．

主ブロック以外に属している既約通常指標 χ_7, χ_8, χ_9 を除いて,[*3]
$\mathrm{Scott}(G, P_1)$ に対応する通常指標 $\chi_{\widehat{\mathrm{Scott}(G,P_1)}}$ は

$$\chi_{\widehat{\mathrm{Scott}(G,P_1)}} = \chi_1 + \chi_6 + \underbrace{\chi_3 + \chi_4 + \chi_5}_{exc.}$$

であることが分かる.

また, $\mathrm{Scott}(G, P_1)$ は次のような加群としての構造をもつことが分かる.

$$\mathrm{Scott}(G, P_1) \simeq \begin{array}{ccccc} 1 & & & & 7 \\ & \diagdown & & \diagup & \\ & & 7 & & \\ & \diagup & & \diagdown & \\ 7 & & & & 1. \end{array}$$

4 主結果

以下, P を G の巡回 Sylow p-部分群とする.

$|P| = p^n$ $(n > 1)$ とし, P_i を P の部分群で $|P_i| = p^i$ であるものとする. また, u を P の生成元, $E(p^i) = \exp(\frac{2\pi\sqrt{-1}}{p^i})$ とする. $\mathrm{Irr}(P) \ni \lambda_j : u \mapsto E(p^n)^j$ と定める. $\{\lambda_{t_j}\}_{1 \le j \le m}$ を $N_G(P)$ の作用に関する $\mathrm{Irr}(P) - \{1\}$ の軌道の代表元の集合とし, $\chi_{\lambda_{t_j}}$ を

$$\chi_{\lambda_{t_j}}(u) = -\sum_{h \in N_G(P)} \lambda_{t_j}^h(u)$$

となる G の例外指標とする.

kG の主ブロックを A で表し, その inertial index を e とする. 巡回不足群をもつ主ブロックに対しては, $e = \mid N_G(P)/C_G(P) \mid$ である. また,

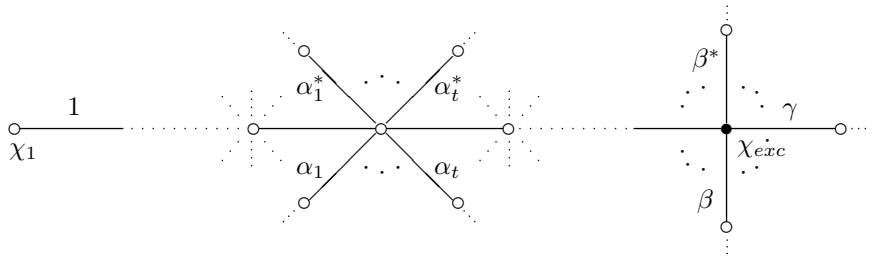
$$m = \frac{|P| - 1}{e} = \frac{p^n - 1}{e} \quad , \quad m_{n-i} = \frac{p^{n-i} - 1}{e}$$

とする (ここで, $\frac{p-1}{e}$ は自然数).

Brauer tree の各頂点には, 既約通常指標が, 各辺には既約 Brauer 指標 (単純 kG-加群) が対応する. 主ブロックの Brauer tree において, 自明な通常指標に対応する頂点は端点であり, 例外頂点 (exceptional vertex) と呼ばれる頂点が唯一つ存在する. 例外頂点には, 例外指標の和が対応し, その重複度は m である.

[*3] trivial source module に対応する通常指標の p-元上での値には制限があるため, 射影加群に対応する指標が因子に現われる場合, 指標の値による条件から取り除くこともできる.

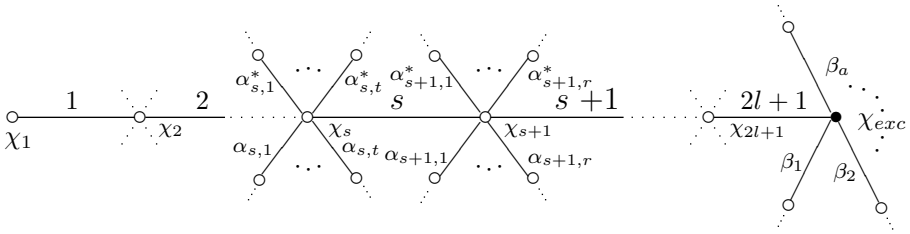
定理 4.1. (1) G の主ブロックの Brauer tree は，自明な通常指標 χ_1 に対応する頂点から例外頂点 χ_{exc} までの最短経路である直線に関して対称である．また，線対称な辺の組に対応する単純加群の組は，互いに k-双対である．



ここで，$\alpha_j{}^* := \mathrm{Hom}_k(\alpha, k)$ $(j = 1, 2, \ldots, t)$ である．

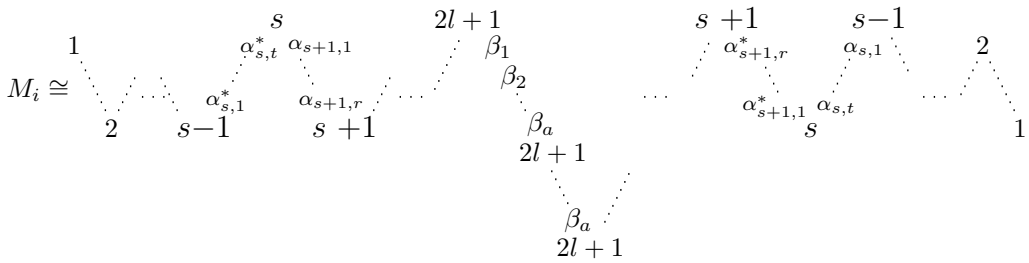
(2) $M_i = \mathrm{Scott}(G, P_i)$ $(i = 1, 2, \ldots, n-1)$ とし，$\chi_{\hat{M}_i}$ を M_i に対応する G の通常指標[*4] とする．

(a) A の Brauer tree が以下のように，自明な通常指標 χ_1 に対応する頂点から例外頂点 χ_{exc} までの最短経路の長さが奇数である場合；



ここで，$l \geq 0$，$2 \leq s \leq 2l$ である．また，例外頂点から伸びる辺に対して，反時計回りに番号付けしている．

このとき，M_i は次のような組成因子の構造をもつ直既約加群である (この図の詳細については Janusz [6]，または Feit [4] VII Section 12 を参照)．



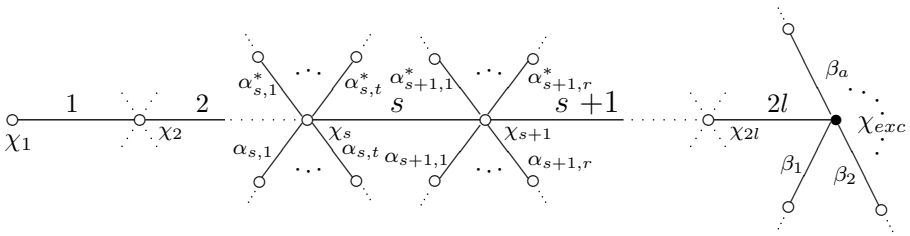
ただし，上図では s を奇数と仮定している．

[*4] $(\mathcal{K}, \mathcal{O}, k)$ を splitting p-modular system，$\hat{M}_i$ を M_i の $\mathcal{O}$ への lift とするとき，$\hat{M}_i \otimes_{\mathcal{O}} \mathcal{K}$ の通常指標を指す．

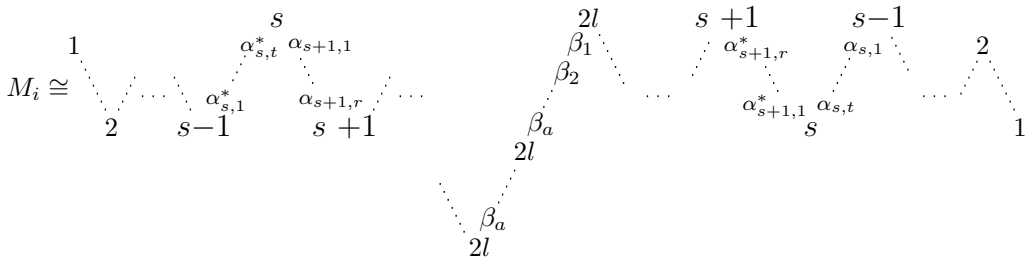
M_i の組成因子における単純加群 $2l+1$ の重複度は $m_{n-i}+1$ であり，例外頂点から伸びるその他の辺に対応する単純加群 β_j $(j=1,2,\ldots,a)$ の重複度は m_{n-i} である．また，M_i に対応する通常指標は次の通りである．

$$\chi_{\hat{M_i}} = \chi_1+\chi_2+\chi_3+\cdots+\chi_{2l+1}+\sum_{p^i \mid t_j,\ 1\le j\le m}\chi_{\lambda_{t_j}}.$$

(b) A の Brauer tree が以下のように, 自明な通常指標 χ_1 に対応する頂点から例外頂点 χ_{exc} までの最短経路の長さが偶数である場合;



ここで，$l\ge 1$，$2\le s\le 2l-1$ である．このとき，M_i は次のような構造をもつ直既約加群である．



ただし，上図では s を奇数と仮定している．

M_i の組成因子における単純加群 $2l$ の重複度は $m-m_{n-i}+1$ であり，例外頂点から伸びるその他の辺に対応する単純加群 β_j $(j=1,2,\ldots,a)$ の重複度は $m-m_{n-i}$ である．

また，M_i に対応する通常指標は次の通りである．

$$\chi_{\hat{M_i}} = \chi_1+\chi_2+\chi_3+\cdots+\chi_{2l}+\sum_{p^i \nmid t_j,\ 1\le j\le m}\chi_{\lambda_{t_j}}.$$

注意 1. $p=2$ のとき，G は 2-ベキ零群である．よって，kG の主ブロックは kP と同型である．したがって，$\mathrm{Scott}(G,P_i)$ が長さ p^{n-i} の単列加群になることは既に知られていた．

5 主結果の証明について

Janusz [6] Section 5 から，Brauer tree において Scott 加群を引き起こす道の選び方が決まる．それにより， Scott 加群に対応する通常指標における非例外指標の成分が決まる．残る例外指標成分を決定するために，指標の計算をする．具体的には，$N_G(P_1)$ の Scott 加群を求め，Green 対応や Alperin [1] Section 4, 19 の事実を用いて G の Scott 加群に対応する通常指標が p-元上でとり得る値を求める．主ブロックに属する通常指標に対しては殆ど p-元上での値を考えればよく (Feit [4] V 章 系 6.3，Brauer [2] 命題 2A 参照)，Dade [3] によって既約通常指標の p-元上での値の詳細が与えられているので，指標の計算で証明される．また，Scott 加群の構造も対応する通常指標から得られる．

6 関連する研究

関連する結果としては，S. Koshitani - N. Kunugi [7] 以外に，G. Hiss - N. Naehrig [5] が挙げられる．[5] では，巡回不足群をもつブロックに属する持ち上げ可能な直既約加群に対して，その加群を引き起こす Brauer tree 上の道を決定し，対応する通常指標を与えている．

参考文献

[1] J. L. Alperin, Local Representation Theory, Cambridge Univ. Press, Cambridge (1986).

[2] R. Brauer, On finite groups with cyclic Sylow subgroups: II, J. Algebra **58** (1979) 291-318.

[3] E. C. Dade, Blocks with cyclic defect groups, Ann. of Math. (2) **84** (1966) 20-48.

[4] W. Feit, The Representation Theory of Finite Groups, North-Holland, Amsterdam (1982).

[5] G. Hiss and N. Naehrig, The indecomposable liftable modules in cyclic blocks, Preprint.

[6] G. J. Janusz, Indecomposable modules for finite groups, Ann. of Math. (2) **89** (1969) 209-241.

[7] S. Koshitani and N. Kunugi, Trivial source modules in blocks with cyclic defect groups, Math. Z. **265** (2010) 161-172.

[8] 永尾汎 - 津島行男, 有限群の表現, 裳華房 (1987).

J_4 の表現構成について

脇 克志*

J_4 について

J_4 は、1974 年に 13 の条件で特徴付けられた 26 番目（つまり、最後の）散在型有限単純群です. 群 G から体 k 上の n 次元ベクトル空間 U への準同型写像を G の n 次表現と呼びます. J_4 では、2 元体 $GF(2)$ 上で 112 次の表現があります. 標数が 2 でない体上の表現は、最少で 1333 次であることも知られています. 今回の講演では、[1] を元にして、複素数体上の 1333 次元表現の構成方法を紹介しました. ここで、表現を作るとは J_4 の生成元による複素数体上の 1333 次ベクトル空間への線形作用を与えることを意味します.

1 $GF(2)$ 上の線形変換 $GL(U_5)$

1.1 $L^{[0]}$ とその部分群について

U_5 を $GF(2)$ 上の 5 次元ベクトル空間として、$\{u_1, u_2, u_3, u_4, u_5\}$ を U_5 の基底とします. U_5 の部分空間 U_i を $\langle u_j \mid 1 \leqq j \leqq i \rangle \qquad (i = 1, 2, 3, 4,)$ と定義します.

$$0 \subset U_1 \subset U_2 \subset U_3 \subset U_4 \subset U_5$$

線形変換全体で作られる群を $L^{[0]} := GL(U_5) = L_5(2)$ と定義すると、その部分群 $L^{[1]} := \{x \in L^{[0]} \mid {U_4}^x = U_4, {u_5}^x = u_5\} = L_4(2)$ は、8 次の交代群 Alt_8 と同型になります.

線形変換 $b_i \in L^{[0]}$ を

$$u_j^{b_i} = \begin{cases} u_j & j \neq 5 \\ u_5 + u_i & j = 5 \end{cases}$$

として、$B^{[1]} := \langle b_i \in L^{[0]} \mid 1 \leqq i \leqq 4 \rangle = 2^4$ と定義します. H を $L^{[0]}$ の部分群、V を U_5 の部分空間とした時、$H(V) := \{h \in H \mid V^h = V\}$ と定義します. 例えば、

$$L^{[0]}(U_4) = B^{[1]} : L^{[1]} = 2^4 : L_4(2)$$

また、

$$L^{[0]}(U_3) = 2^6 : (L_3(2) \times L_2(2)) = 2^6 : (L_3(2) \times Sym_3)$$

となることも分ります. ここで、$L_2(2) = Sym_3$ は、3 次の対称群を表しています. 写像 $\quad : U_4 \to L^{[0]}$ を $\quad (u_i) := b_i$ で定義すると、ベクトル空間 (加法群) から基本可換群 (乗法群) への自然な同型写像が与えられます.

本研究は日本学術振興会科学研究費補助金基盤研究 (C) No. ２２５４０００７の助成を受けています.

1.2 $\bigwedge^2 U_5$ について

$Q^{[0]}$ を位数が 2^{10} の基本可換群とします．外積 $\bigwedge^2 U_5 := \langle u_i \wedge u_j \mid 1 \leqq i < j \leqq 5 \rangle$ は、$GF(2)$ 上の 10 次元ベクトル空間となります．写像 $\tilde{} : \bigwedge^2 U_5 \to Q^{[0]}$ を $GF(2)$ 上のベクトル空間（加法群）から基本可換 2-群（乗法群）への自然な同型写像とします．また、 $: U_4 \to Q^{[0]}$ を $a_i := \ (u_i) = \tilde{}(u_i \wedge u_5), (1 \leqq i \leqq 4)$ と定義します．また $A^{[1]} := \langle a_i \mid 1 \leqq i \leqq 4 \rangle = 2^4$ と定義します．この時、$\bigwedge^2 U_4 \subset \bigwedge^2 U_5$ について $Z^{[1]} := \tilde{}(\bigwedge^2 U_4) = 2^6$ と置くと、$Q^{[0]} = \tilde{}(\bigwedge^2 U_5) = Z^{[1]}A^{[1]} = 2^{10}$ となります．以下では、$Q^{[0]}$ と $\bigwedge^2 U_5$ を同一視します．

1.3 $G^{[0]}$ と $G^{[01]}$ について

$L^{[0]}$ による $\bigwedge^2 U_5$ への自然な作用から、半直積 $G^{[0]} := Q^{[0]} : L^{[0]}$ が構成できます．$L^{[0]}$ の部分群 $B^{[1]}$ より非可換な 2-群 $Q^{[1]} := Q^{[0]} : B^{[1]} = Z^{[1]}A^{[1]} : B^{[1]} = 2^{10+4}$ も構成できます．ここで、線形写像 b_i の定義より、$Z^{[1]} = Z(Q^{[1]})$ であり、$a_j^{b_i} = \tilde{}(u_j \wedge u_i) * a_j \quad (1 \leqq i, j \leqq 4)$ より $a_j^{b_i} \in Z^{[1]} * a_j$ となります．つまり $Q^{[1]}/Z^{[1]}$ では、a_j と b_i は可換となります．よって、$Q^{[1]}/Z^{[1]} = \overline{A^{[1]}} \times \overline{B^{[1]}} = 2^8$ となり、$Q^{[1]} = 2^{6+8}$ とも表せことが分かります．

$G^{[0]}$ の部分群 $G^{[01]} := Q^{[0]} : L^{[0]}(U_4) = Z^{[1]}A^{[1]} : (B^{[1]} : L^{[1]}) = Q^{[1]} : L^{[1]}$ で、$Z^{[1]}$ は、その正規部分群となり、$Q^{[1]}/Z^{[1]} = \overline{A^{[1]}} \times \overline{B^{[1]}} = 2^4 \times 2^4$ への $L^{[1]}$ の作用が自然に導入されます．更に、$Q^{[1]}$ の部分群 $D^{[1]} := \langle \ (u) \ (u) \mid u \in U_4 \rangle$ を考えると、$(\ (u) \ (u))^2 = 1$, $(u_i) \ (u_i) \ (u_j) \ (u_j) \ (u_i + u_j) \ (u_i + u_j) = \tilde{}(u_i \wedge u_j) \in Z^{[1]}$ が得られます．ここから、$D^{[1]}$ は、$Z^{[1]}$ を含む位数 2^{10} の基本可換群であることが分かります．この $D^{[1]}$ は、$L^{[1]}$ による作用で閉じているので、$G^{[01]}$ の部分群となる半直積 $D^{[1]} : L^{[1]} = 2^{10} : L_4(2)$ が定義できます．$G^{[0]}$ は、J_4 の 2 番目に大きな極大部分群とみることが出来ます．J_4 を valency が 31 となるあるグラフの自己同型群と見ると、$G^{[0]}$ は、そのグラフの 1 点固定部分群となり、$G^{[01]}$ は、その点を含む 1 つの辺を両端の点も含めて固定する部分群となります．J_4 には、この辺を引っ繰り返す（つまり両端の点を置換する）位数 2 の元 t_1 が存在し、$G^{[1]} := \langle G^{[01]}, t_1 \rangle$ は、この辺を固定する部分群であり、$J_4 = \langle G^{[0]}, t_1 \rangle$ となります．

2 $G^{[0]}$-表現の構成

$\Pi^{[0]}$ を $\mathbb{C}$ 上の 1333 次のベクトル空間として、J_4 の表現（つまり作用）を構成するのが目的です．そこで、まず $\Pi^{[0]}$ 上の表現を $G^{[0]}$ に制限したもの (つまり $G^{[0]}$ の $\Pi^{[0]}$ への作用) を求めます．K を J_4 の部分空間として、

$$\Pi_K^{[0]} := \{v \in \Pi^{[0]} \mid \forall x \in K, \ v^x = v\}$$

と定義します．このとき、$\Pi_K^{[0]}$ は、$N_{J_4}(K)$ の作用で閉じていることになります．

2.1 Symplectic form と $L^{[0]}$ の作用

ここでは、U_5 上の双線形写像 f が次の条件を満たすとき、Symplectic form と呼ぶことにします．

(1) $\forall u \in U_5, \ f(u, u) = 0$

(2) $\forall u, v \in U_5, \ f(u, v) = f(v, u)$

また、U_5 上の Symplectic form 全体の集合を $\mathcal{S}(U_5)$ と書くことにします．特に、$1 \leqq s < t \leqq 5$ に対して、

$$f_{\{s,t\}}(u_i, u_j) := \delta_{\{s,t\}\{i,j\}} = \begin{cases} 1 & \{s,t\} = \{i,j\} \\ 0 & \{s,t\} \neq \{i,j\} \end{cases}$$

と定義すると、$f_{\{s,t\}} \in \mathcal{S}(U_5)$ となります．$\mathcal{S}(U_5)$ を $GF(2)$ 上のベクトル空間と見ると、$f_{\{s,t\}}$ は、$\mathcal{S}(U_5)$ の基底となり、$\dim \mathcal{S}(U_5) = 10$ です．Symplectic form f について、U_5 の部分空間 $\mathrm{Rad}(f) := \{u \in U_5 \mid \forall v \in U_5,\, f(u,v) = 0\}$ と定義します．特に $\mathrm{Rad}(f) = 0$ となるとき、f は、non-singular と呼びます．non-singular な Symplectic form は、偶数次元のベクトル空間でしか存在しないことが知られています．f は $U_5/\mathrm{Rad}(f)$ 上の non-singular な symplectic form と見ることが出来るので、$U_5/\mathrm{Rad}(f)$ の次元は偶数となり、$\dim \mathrm{Rad}(f)$ は、1 または 3 となることが分かります．$L^{[0]}$ の元 x による f への作用として、$f^x(u,v) := f(u^{x^{-1}}, v^{x^{-1}})$ と決めると、$\mathcal{S}(U_5)$ に $L^{[0]}$-線形作用が与えられます．$L^{[0]}$ の部分群 H について、$H(f) := \{x \in H \mid f^x = f\}$ と定義します．特に、$x \in H(f)$ なら、$\mathrm{Rad}(f)^x = \mathrm{Rad}(f)$ となります．例えば、$f_1 := f_{\{45\}}$, $f_2 := f_{\{25\}} + f_{\{34\}}$ と定めると、定義より $\mathrm{Rad}(f_1) = U_3$, $\mathrm{Rad}(f_2) = U_1$ となります．$L^{[0]}$ の f_i における安定部分群 $L^{[0]}(f_i)$ を計算すると、$L^{[0]}(f_1) = 2^6 : (L_3(2) \times Sym_3)$, $L^{[0]}(f_2) = 2^4 : S_4(2)$ となります．ここで、$S_4(2)$ は、f_2 を U_5/U_1 上の non-Singular Symplectic form $\bar{f}_2$ と見たときの固定群で、群としては、6 次の対称群 Sym_6 と同型になります．ここからそれぞれの軌道のサイズは、$|{f_1}^{L^{[0]}}| = 155$, $|{f_2}^{L^{[0]}}| = 868$ となります．155+868=1023 より、$\mathcal{S}(U_5)$ の 0 以外の Symplectic form は、f_1 か f_2 のどちらかの軌道に含まれます．定義より、$\dim \mathrm{Rad}(f)^x = \dim \mathrm{Rad}(f)$ となるので、$\mathcal{S}$ の 2 つの部分集合を $\mathcal{S}_1 := \{f \in \mathcal{S}(U_5) \mid \dim \mathrm{Rad}(f) = 3\}$, $\mathcal{S}_2 := \{f \in \mathcal{S}(U_5) \mid \dim \mathrm{Rad}(f) = 1\}$ と定義すると、$\mathcal{S}_i$ は、f_i の軌道となります．以上より、$|\mathcal{S}_1| = 155$, $|\mathcal{S}_2| = 868$, $\mathcal{S}(U_5)\backslash\{0\} = \mathcal{S}_1 \cup \mathcal{S}_2$ となります．

2.2 Symplectic form と $\bigwedge^2 U_5$ の Hyper plane

$\bigwedge^2 U_5$ の Hyper plane 全体の集合を $\mathcal{P} := \{P \subset \bigwedge^2 U_5 \mid \dim P = 9\}$ と定義します．このとき、$\mathcal{P}$ は、$L^{[0]}$ の作用で閉じている $L^{[0]}$-集合となります．また、$\bigwedge^2 U_5$ の双対空間 $\left(\bigwedge^2 U_5\right) := \left\{\Phi \mid \Phi : \bigwedge^2 U_5 \to GF(2)\right\}$ を経由する $\mathcal{S}(U_5)$ と $\mathcal{P}$ との間の 1 対 1 対応 P が次の様に定義できます．つまり $f \in \mathcal{S}(U_5)$ について、$\tilde{f}(u \wedge v) := f(u,v)$ で、$\tilde{f} \in \left(\bigwedge^2 U_5\right)$ を定め、$P(f) := \mathrm{Ker}\tilde{f} \in \mathcal{P}$ を対応させます．このとき、$x \in L^{[0]}$ について、$P(f^x) = P(f)^x$ が成り立ちます．よって、$\mathcal{P}_i := P(\mathcal{S}_i)$ と定めると、$\mathcal{P} = \mathcal{P}_1 \cup \mathcal{P}_2$ と $L^{[0]}$ の軌道で分解出来ます．$P_i := P(f_i)$ は軌道 $\mathcal{P}_i$ の代表元となります．特に、$L^{[0]}(f_i) = N_{L^{[0]}}(P(f_i))$ が成り立ちます．

2.3 $\Pi^{[0]}$ への $G^{[0]}$ の作用

まず、$\Pi^{[0]}$ への $Q^{[0]}$ の作用を考えると、$Q^{[0]}$ が基本可換群であることから、$\Pi^{[0]}$ は、$Q^{[0]}$ の 1 次表現の直和に分解されます．特に、

$$\Pi^{[0]} = \bigoplus_{P \in \mathcal{S}_1} \Pi^{[0]}_P \oplus \bigoplus_{P \in \mathcal{S}_2} \Pi^{[0]}_P$$

となりますが、$|\mathcal{S}_1| = 155$, $|\mathcal{S}_2| = 868$ より $\dim \Pi^{[0]}_{P_1} = 3$, $\dim \Pi^{[0]}_{P_2} = 1$ が得られます．

$G^{[0]}$ の $f \in \mathcal{S}(U_5)$ への作用を、$G^{[0]}/Q^{[0]} = L^{[0]}$ で与えると、固定部分群 $G^{[0]}(f_i) = Q^{[0]} : L^{[0]}(f_i)$ となるので、$G^{[0]}(f_1) = Q^{[0]} : L^{[0]}(U_3) = 2^{10} : (2^6 : (L_3(2) \times Sym_3))$, $G^{[0]}(f_2) = Q^{[0]} : L^{[0]}(U_1)(\bar{f}_2) = 10^{10} : (2^4 : S_4(2))$ となります．$\Pi_i := \Pi^{[0]}_{P_i}$ とすると、Π_i は、既約な $G^{[0]}(f_i)$-表現を持ちます．この既約な $G^{[0]}(f_i)$-表現 Π_i を $G^{[0]}$ に誘導すると、$465(= 3 \times 155)$ 次と 868 次の既約表現 $\Pi^{[0]}_i := {\Pi_i}^{\uparrow G^{[0]}}$ が得られます．そして、$\Pi^{[0]}$ の $G^{[0]}$-表現が ${\Pi^{[0]}}_{\downarrow G^{[0]}} = \Pi^{[0]}_1 \oplus \Pi^{[0]}_2$ と直和分解で得られます．

3 $G^{[01]}$-表現の構成

既約表現 $\Pi^{[0]}_i := {\Pi_i}^{\uparrow G^{[0]}}$ の $G^{[01]}$ への制限を考えるため、Mackey の分解公式を使います．そこで、最初に $G^{[01]}$ における f_1 と f_2 の軌道を調べます．

3.1 $G^{[01]}$ における軌道の長さ

まず、固定部分群 $G^{[01]}(f_1) = G^{[01]}(U_3)$ は、$Q^{[0]} : (B^{[1]} : (2^3 : L_3(2)))$ となります．次に固定部分群 $G^{[01]}(f_2) = G^{[0]}(f_2) \cap G^{[01]} = Q^{[0]} : (2^4 : (2^2 : 2 \times L_2(2)))$ となります．ここから、f_i の軌道の長さは、$|{f_1}^{G^{[01]}}| = |G^{[01]} : G^{[01]}(f_1)| = |L_4(2) : (2^3 : L_3(2))| = 15$, $|{f_2}^{G^{[01]}}| = |G^{[01]} : G^{[01]}(f_2)| = 2^6.3^2.5.7/(2^4.3)| = 420$ となります．

ここで、$x \in G^{[0]}$ を $f_1^x = f_{\{23\}}$ となるように選ぶと、$\mathrm{Rad}(f_1^x) = \langle u_1, u_2, u_5 \rangle \not\subset U_4$ より、f_1^x は f_1 と異なる $G^{[01]}$ の軌道に入ります．また、$U_1 \subset U_4$ より、$y \in G^{[0]}$ を $f_2^y = f_{\{12\}} + f_{\{34\}}$ となるように選ぶと、$\mathrm{Rad}(f_2^y) = \langle u_5 \rangle \not\subset U_4$ より、f_2^y は、f_2 と異なる軌道に入ります．f_1^x と f_2^y の固定部分群を調べると、$G^{[01]}(f_1^x) = G^{[01]}(\langle u_1, u_2, u_5 \rangle)$ より $Q^{[0]} : (2^6 : (Sym_3 \times Sym_3))$ となります．また、$G^{[01]}(f_2^y) = G^{[0]}(f_2^y) \cap G^{[01]} = G^{[01]}(u_5, f_2^y) = Q^{[0]} : S_4(2)$ となります．よって、f_1^x の軌道の長さは、$|{f_1^x}^{G^{[01]}}| = |G^{[01]} : G^{[01]}(f_1^x)| = |2^4 : L_4(2) : (2^6 : (Sym_3 \times Sym_3)| = 140$, f_2^y の軌道の長さは、$|{f_2^y}^{G^{[01]}}| = |G^{[01]} : G^{[01]}(f_2^y)| = |L_4(2) : S_4(2)| = 448$ となります．以上の計算で、15+140=155, 420+448=868 となり、$\mathcal{S}_1$, $\mathcal{S}_2$ がそれぞれ 2 つの軌道に分かれました．

3.2 $G^{[01]}$ への制限

既約加群 $\Pi^{[0]}_i := {\Pi_i}^{\uparrow G^{[0]}}$ の $G^{[01]}$ への制限を考えると、3.1 の $G^{[0]}$ の元 x,y を使った Mackey の分解公式より、

$$ {\Pi^{[0]}_1}_{\downarrow G^{[01]}} = {\Pi_1}^{\uparrow G^{[0]}}{}_{\downarrow G^{[01]}} = {\Pi_1}_{\downarrow G^{[0]}(f_1) \cap G^{[01]}}{}^{\uparrow G^{[01]}} \oplus {\Pi_1}^{x}_{\downarrow G^{[0]}(f_1)^x \cap G^{[01]}}{}^{\uparrow G^{[01]}} $$

$$ {\Pi^{[0]}_2}_{\downarrow G^{[01]}} = {\Pi_2}^{\uparrow G^{[0]}}{}_{\downarrow G^{[01]}} = {\Pi_2}_{\downarrow G^{[0]}(f_2) \cap G^{[01]}}{}^{\uparrow G^{[01]}} \oplus {\Pi_2}^{y}_{\downarrow G^{[0]}(f_2)^y \cap G^{[01]}}{}^{\uparrow G^{[01]}} $$

となります．ここから、既約表現 $\Pi^{[0]}_i := {\Pi_i}^{\uparrow G^{[0]}}$ の $G^{[01]}$ への制限は、$\Pi^{[01]}_{11} := {\Pi_1}_{\downarrow G^{[0]}(f_1) \cap G^{[01]}}{}^{\uparrow G^{[01]}}$, $\Pi^{[01]}_{12} := {\Pi_1}^{x}_{\downarrow G^{[0]}(f_1)^x \cap G^{[01]}}{}^{\uparrow G^{[01]}}$, $\Pi^{[01]}_{21} := {\Pi_2}_{\downarrow G^{[0]}(f_2) \cap G^{[01]}}{}^{\uparrow G^{[01]}}$, $\Pi^{[01]}_{22} := {\Pi_2}^{y}_{\downarrow G^{[0]}(f_2)^y \cap G^{[01]}}{}^{\uparrow G^{[01]}}$ の４つの既約表現の直和となることが分かります．特にそれぞれの既約表現の次元は、$45(= 3 \times 15)$, $420(= 3 \times 140)$, $420(= 1 \times 420)$, $448(= 1 \times 448)$ となります．

4 $G^{[1]}$-表現の構成

最後に、発表では紹介できなかった $G^{[1]}$ の表現について、その概略を紹介します. $G^{[01]} = Z^{[1]}A^{[1]}B^{[1]} : L^{[1]}$ の部分群 $Z^{[1]}L^{[1]}$ を考えます. t_1 は、共役により $A^{[1]}$ を $B^{[1]}$ に移します. また、$Z^{[1]}$ とは可換となります. ここで、$\langle Z^{[1]}, t_1 \rangle$ は、位数 2^7 の基本可換群であり、$\langle Z^{[1]}L^{[1]}, t_1 \rangle = 2^7 : L_4(2)$ の正規部分群となります. $L^{[1]} = Alt_8$ より、$Z^{[1]}$ への $L^{[1]}$ の作用は、次の様に定義できます.

4.1 $Z^{[1]}$ への $L^{[1]}$ の作用と t_1 による拡張

$GF(2)$ 上の 8 次元ベクトル空間 V_8 の部分空間として、$V_8^c := \langle (1,1,1,1,1,1,1,1) \in V_8 \rangle$ と $V_8^e := \{v \in V_8 \mid wt(v) = 0 \bmod 2\}$ を定義します. ここで、$wt(v)$ は、ベクトル v の中の 1 の個数です. それぞれのベクトル空間に、座標軸の置換により $L^{[1]} = Alt_8$ が作用しています. ここから、6 次元ベクトル空間 V_8^e/V_8^c への $L^{[1]}$ の作用が与えられますが、これが $Z^{[1]}$ への作用と同型になります. 更に、$\langle Z^{[1]}L^{[1]}, t_1 \rangle = (V_8/V_8^c) : Alt_8$ となります. この群の拡張と 1.3 の $D^{[1]}$ を使うと、$D^{[1]}$ と t_1 は、可換でであり、$G^{[01]} = Z^{[1]}A^{[1]}B^{[1]} : L^{[1]}$ の部分群 $D^{[1]}L^{[1]} = 2^{10} : L_4(2)$ も $\langle D^{[1]}L^{[1]}, t_1 \rangle = 2^{11} : L_4(2)$ に拡張できます. t_1 と $A^{[1]}$, $B^{[1]}$ の関係も細かく見ていくことにより、最終的に、$G^{[1]}$ の表現構成も可能になります.

参考文献

[1] A.A. Ivanov, The fourth Janko group J_4, Oxford mathematical monographs, Oxford : Clarendon, 2004

GAP による計算

講演では、紹介できませんでしたが J_4 の極大部分群の解析に当たっては、[1] を参考にしながら GAP によるプログラムを構成しました。以下にその一部を紹介します。例えば、固定部分群 $G^{[01]}(f_1)$, $G^{[01]}(f_2)$, $G^{[01]}(f_1^x)$, $G^{[01]}(f_2^y)$ は、I11, I21, I12, I22 として、計算されています.

```
############################################################
#
# Basic objects, groups and homomorphisms
#
############################################################

N:=5;

IdxSq:=[];
for j in [2..N] do
  for i in [1..j-1] do
    Add(IdxSq,[i,j]);
  od;
od;

############################################################
#
# Define elementary abelian permutation group 2^10 named Q0
# and subgroup A1, Z1 such that Q0=Z1A1
#
q12:=( 1, 2);;q13:=( 3, 4);;q23:=( 5, 6);;q14:=( 7, 8);;q24:=( 9,10);;
q34:=(11,12);;q15:=(13,14);;q25:=(15,16);;q35:=(17,18);;q45:=(19,20);;
```

```
genQ0:=[q12,q13,q23,q14,q24,q34,q15,q25,q35,q45];
Q0:=Group(genQ0);;
genA1:=[q15,q25,q35,q45];
A1:=Group(genA1);
Z1:=Group([q12,q13,q23,q14,q24,q34]);

############################################################
#
# Define vectors space U5 of dimension 5
#
u1:=[1,0,0,0,0]*Z(2);
u2:=[0,1,0,0,0]*Z(2);
u3:=[0,0,1,0,0]*Z(2);
u4:=[0,0,0,1,0]*Z(2);
u5:=[0,0,0,0,1]*Z(2);
genU5:=[u1,u2,u3,u4,u5];
U5:=VectorSpace(GF(2),genU5);
U4:=VectorSpace(GF(2),genU5{[1..4]});
U3:=VectorSpace(GF(2),genU5{[1..3]});
U1:=VectorSpace(GF(2),[genU5[1]]);
U3x:=VectorSpace(GF(2),genU5{[1,2,5]});
U1y:=VectorSpace(GF(2),[genU5[5]]);
############################################################
#
# Define vectors space A2U5 of dimension 10
# and Multiplicative Group M2U5 of order 2^10
#
u12:=[1,0,0,0,0,0,0,0,0,0]*Z(2);
u13:=[0,1,0,0,0,0,0,0,0,0]*Z(2);
u23:=[0,0,1,0,0,0,0,0,0,0]*Z(2);
u14:=[0,0,0,1,0,0,0,0,0,0]*Z(2);
u24:=[0,0,0,0,1,0,0,0,0,0]*Z(2);
u34:=[0,0,0,0,0,1,0,0,0,0]*Z(2);
u15:=[0,0,0,0,0,0,1,0,0,0]*Z(2);
u25:=[0,0,0,0,0,0,0,1,0,0]*Z(2);
u35:=[0,0,0,0,0,0,0,0,1,0]*Z(2);
u45:=[0,0,0,0,0,0,0,0,0,1]*Z(2);

genA2U5:=[u12,u13,u23,u14,u24,u34,u15,u25,u35,u45];
genM2U5:=List(genA2U5,u->AdditiveElementAsMultiplicativeElement(u));
A2U5:=VectorSpace(GF(2),genA2U5);
M2U5:=Group(genM2U5);

############################################################
#
# Define homomorphism between M2U5 to Q0
M2U5toQ0:=GroupHomomorphismByImages(M2U5,Q0,genM2U5,genQ0);

############################################################
#
# Define L_5(2) as permutation and matrix group named L0, mL0.
#

genL0:=[
  (16,24)(17,25)(18,26)(19,27)(20,28)(21,29)(22,30)(23,31),
  (1,2,4,8,16)(3,6,12,24,17)(5,10,20,9,18)(7,14,28,25,19)(11,22,13,26,21)(15,30,29,27,23) ];
L0:=Group(genL0);

mb51:=[[1,0,0,0,0],[0,1,0,0,0],[0,0,1,0,0],[0,0,0,1,0],[1,0,0,0,1]]*Z(2);
mb52:=[[1,0,0,0,0],[0,1,0,0,0],[0,0,1,0,0],[0,0,0,1,0],[0,1,0,0,1]]*Z(2);
mb53:=[[1,0,0,0,0],[0,1,0,0,0],[0,0,1,0,0],[0,0,0,1,0],[0,0,1,0,1]]*Z(2);
mb54:=[[1,0,0,0,0],[0,1,0,0,0],[0,0,1,0,0],[0,0,0,1,0],[0,0,0,1,1]]*Z(2);
mc4:=[[0,1,0,0,0],[0,0,1,0,0],[0,0,0,1,0],[1,0,0,0,0],[0,0,0,0,1]]*Z(2);
mc5:=[[0,1,0,0,0],[0,0,1,0,0],[0,0,0,1,0],[0,0,0,0,1],[1,0,0,0,0]]*Z(2);

mL0:=Group([mb51,mc5]);
```

```
mb12:=mb51^(mc5^1);
mb23:=mb51^(mc5^2);
mb34:=mb51^(mc5^3);
mb45:=mb51^(mc5^4);
mb13:=mb52^(mc5^1);
mb24:=mb52^(mc5^2);
mb35:=mb52^(mc5^3);
mb41:=mb52^(mc5^4);
mb14:=mb53^(mc5^1);
mb25:=mb53^(mc5^2);
mb31:=mb53^(mc5^3);
mb42:=mb53^(mc5^4);
mb15:=mb54^(mc5^1);
mb21:=mb54^(mc5^2);
mb32:=mb54^(mc5^3);
mb43:=mb54^(mc5^4);

mx:=[[1,0,0,0,0],[0,1,0,0,0],[0,0,0,0,1],[0,0,1,0,0],[0,0,0,1,0]]*Z(2); # (3,5,4)
my:=[[0,0,0,0,1],[0,1,0,0,0],[0,0,1,0,0],[0,0,0,1,0],[1,0,0,0,0]]*Z(2); # (1,5)


############################################################
#
# Isomorphism between L0 and mL0
#
PermToMatInL0:=GroupHomomorphismByImages(L0,mL0,[L0.1,L0.2],[mL0.1,mL0.2]);
MatToPermInL0:=GroupHomomorphismByImages(mL0,L0,[mL0.1,mL0.2],[L0.1,L0.2]);

############################################################
#
# Programs
#
############################################################
#
# [i,j] -> k in [1..10]
#
IndexToNumber:=function(idx)
  return idx[1]+(idx[2]-1)*(idx[2]-2)/2;
end;

############################################################
#
# Define 5x5-matrices which are basis of
# Symplectic Form Space SU5
#
BasisOfSymplecticFormSpace:=function(IdxSq,N)
  local Bs,m,idx;
  Bs:=[];
  for idx in IdxSq do
    m:=NullMat(N,N,GF(2));
    m[idx[1]][idx[2]]:=Z(2);
    m[idx[2]][idx[1]]:=Z(2);
    Add(Bs,m);
  od;
  return Bs;
end;

############################################################
#
# Radical of Symplectic Form
RadicalOfSymplecticForm:=function(B)
  return VectorSpace(GF(2),NullspaceMat(B));
end;

############################################################
#
# Transrate Symplectic Form to Dual of A2U5.
```

```
#
SymplecticFormToDual:=function(B,IdxSq)
  local V,idx;
  V:=[];
  for idx in IdxSq do
    Add(V,[B[idx[1]][idx[2]]]);
  od;
  return V;
end;

############################################################
#
# Kernel space in GF(2)^10 of dual a
#
KernelOfDual:=function(a)
  return VectorSpace(GF(2),NullspaceMat(a));
end;

############################################################
#
# Define wedge matrix from 5x5-matrix A
#
WedgeMatrix:=function(A)
  local v,a,i,j,k,l,N;
  N:=Size(A);
  a:=[];
  if N<2 then return fail; fi;
  for i in [2..N] do
    for j in [1..i-1] do
      v:=[];
      for l in [2..N] do
        for k in [1..l-1] do
          Add(v,A[i][k]*A[j][l]+A[i][l]*A[j][k]);
        od;
      od;
      Add(a,v);
    od;
  od;
  return a;
end;

############################################################
# q is permutation in 2^10 on [1..20]
# return vector in GF(2)^10 corresponding to q
#
ElementsQ0ToVec:=function(q)
  local idx,v,i;
  idx:=[2,4..20];
  v:=[0,0,0,0,0,0,0,0,0,0];
  for i in [1..10] do
    if IsOddInt(idx[i]^q) then
      v[i]:=1;
    fi;
  od;
  return v*Z(2);
end;
############################################################
#
# Define action of 5x5-matrix A in mL0 to q in Q0.
#
OnActionForQ0:=function(q,A)
  local v,a;
  v:=ElementsQ0ToVec(q)*WedgeMatrix(A);
  a:=AdditiveElementAsMultiplicativeElement(v);
  return Image(M2U5toQ0,a);
end;
############################################################
```

```
#
# Define action of 5x5-matrix A in mL0  to B in SU5.
#
OnActionForSU5:=function(B,A)
  return A^-1*B*TransposedMat(A)^-1;
end;

############################################################
#
# Define action of permutation x in L0  to B in SU5.
#
OnActionForSU5ByPerm:=function(B,x)
  return OnActionForSU5(B,Image(PermToMatInL0,x));
end;

############################################################
#
# Define action of permutation x in L0  to subspace U.
#
OnActionForU5ByPerm:=function(U,x)
  return U^Image(PermToMatInL0,x);
end;

############################################################
#
# Define automorphism of Q0 from 5x5-matrix A
#
AutomorphismForQ0:=function(Q0,A)
   local gen, gen_images;
   gen:=GeneratorsOfGroup(Q0);
   gen_images:=List(gen,q->OnActionForQ0(q,A));
  return GroupHomomorphismByImages(Q0,Q0,gen,gen_images);
end;
############################################################
#
# Define Symplectic Form Space S(U5)
#
BS:=BasisOfSymplecticFormSpace(IdxSq,N);
SU5:=VectorSpace(GF(2),BS);
f12:=BS[IndexToNumber([1,2])];
f34:=BS[IndexToNumber([3,4])];
f45:=BS[IndexToNumber([4,5])];
f1234:=BS[IndexToNumber([1,2])]+BS[IndexToNumber([3,4])];
f2345:=BS[IndexToNumber([2,3])]+BS[IndexToNumber([4,5])];
f2534:=BS[IndexToNumber([2,5])]+BS[IndexToNumber([3,4])];
############################################################
#
# Define G0:=2^10:L5(2)
#
genAutoQ0:=List(genL0,x->AutomorphismForQ0(Q0,Image(PermToMatInL0,x)));
AutoQ0:=Group(genAutoQ0);
HomForSemidirect:=GroupHomomorphismByImages(L0,AutoQ0,genL0,genAutoQ0);
G0:=SemidirectProduct(L0,HomForSemidirect,Q0);
#
# From L0 to G0
L0ToG0:=Embedding(G0,1);
#
# From Q0 to G0
Q0ToG0:=Embedding(G0,2);
#
# From G0 to L0
G0ToL0:=Projection(G0);
#
# Define B1 in L0 of order 2^4
genB1:=List([mb51,mb52,mb53,mb54],m->Image(MatToPermInL0,m));
B1:=Group(genB1);
#
```

```
# Define L1:=L4(2) in L0
genL1:=List([mb12,mc4],m->Image(MatToPermInL0,m));
L1:=Group(genL1);
#
# Define D1 in G0
eltA1:=[q15,q25,q35,q45,q15*q25,q15*q35,q15*q45,q25*q35,q25*q45,q35*q45];
eltB1:=List(
  [mb51,mb52,mb53,mb54,mb51*mb52,mb51*mb53,mb51*mb54,mb52*mb53,mb52*mb54,mb53*mb54],
  m->Image(MatToPermInL0,m));

genD1:=List([1..10],i->Image(Q0ToG0,eltA1[i])*Image(L0ToG0,eltB1[i]));;
D1:=Group(genD1);
#
# Define G01/Q0 and G01:=2^10:(2^4:L4(2)) in L0
genG01q:=List([mb51,mb12,mc4],m->Image(MatToPermInL0,m));
mG01q:=Group([mb51,mb12,mc4]);
G01q:=Group(genG01q);
G01:=PreImages(G0ToL0,G01q);
############################################################
#
# Define Subgruoups H11,H12,H21,H22 in G0
#
# Define G02/Q0 in L0
G02q:=Stabilizer(L0,U3,OnActionForU5ByPerm);
H11:=PreImages(G0ToL0,G02q);
#
# Define G02x/Q0 in L0
G02xq:=Stabilizer(L0,f34,OnActionForSU5ByPerm);
H12:=PreImages(G0ToL0,G02xq);
#
# Define G04(f)/Q0 in L0
G04fq:=Stabilizer(L0,f2534,OnActionForSU5ByPerm);
H21:=PreImages(G0ToL0,G04fq);
#
# Define G04(f)y/Q0 in L0
G04fyq:=Stabilizer(L0,f1234,OnActionForSU5ByPerm);
H22:=PreImages(G0ToL0,G04fyq);
############################################################
#
# Define Subgruoups I11,I12,I21,I22 in G01
#
#
# Define G012/Q0 in L0
G012q:=Stabilizer(G01q,U3,OnActionForU5ByPerm);
I11:=PreImages(G0ToL0,G012q);
#
# Define G012x/Q0 in L0
G012xq:=Stabilizer(G01q,f34,OnActionForSU5ByPerm);
I12:=PreImages(G0ToL0,G012xq);
#
# Define G014(f)/Q0 in L0
G014fq:=Stabilizer(G01q,f2534,OnActionForSU5ByPerm);
I21:=PreImages(G0ToL0,G014fq);
#
# Define G014(f)y/Q0 in L0
G014fyq:=Stabilizer(G01q,f1234,OnActionForSU5ByPerm);
I22:=PreImages(G0ToL0,G014fyq);
############################################################
```

関数体の塔に関する Elkies 予想の数値的証拠 II

長谷川武博 (thasegawa@suou.waseda.jp)

25/Feb/2012

Contents

1 関数体の塔と Elkies 予想

q を素数の冪とし $\mathbb{F}_{q^2}$ を q^2 個の元からなる有限体とする．定数体が $\mathbb{F}_{q^2}$ である関数体 F を $\mathbb{F}_{q^2}$ 上の関数体 $F/\mathbb{F}_{q^2}$ という．その種数を $g(F)$ と，その有理点の個数を $N(F)$ と書くことにする．

$\mathcal{F} = (F_0, F_1, F_2, \ldots)$ が $\mathbb{F}_{q^2}$ 上の **関数体の塔** とは，次の 2 条件をみたすときをいう．(1) すべての i に対し F_{i+1}/F_i は次数 2 以上の分離拡大である．(2) ある s に対し $g(F_s) > 1$ である．

$\lambda(\mathcal{F}) = \lim_{i\to\infty} N(F_i)/g(F_i)$ を $\mathcal{F}/\mathbb{F}_{q^2}$ の **極限** という．$0 \le \lambda(\mathcal{F}) \le q-1$ はいつでも成り立つ (Drinfeld-Vladut (1983))．$\mathcal{F}/\mathbb{F}_{q^2}$ が **最良** とは $\lambda(\mathcal{F}) = q-1$ となるときをいう．

$f(x, y)$ を $\mathbb{F}_{q^2}$ 上の 2 変数多項式とする．関数体の塔 $\mathcal{F}/\mathbb{F}_{q^2}$ が **方程式 $f(x, y) = 0$ によって再帰的に定義される** とは，次の条件をみたすときをいう．(0) $F_0 = \mathbb{F}_{q^2}(x_0)$ は有理関数体である．(1) $F_1 = \mathbb{F}_{q^2}(x_0, x_1)$ は 1 つの方程式 $f(x_0, x_1) = 0$ が定義する関数体である．(2) $F_2 = \mathbb{F}_{q^2}(x_0, x_1, x_2)$ は 2 つの方程式 $f(x_0, x_1) = f(x_1, x_2) = 0$ が定義する関数体である．(3) $\cdots$

関数体の塔の例を 2 つ紹介する．

例 1 (Garcia-Stichtenoth (1996))：方程式 $y^2 + (1-x)^2 - 1 = 0$ によって再帰的に定義される $\mathbb{F}_9$ 上の関数体の塔は 最良 である． □

例 2 (Garcia-Stichtenoth (1996))：方程式 $y^3 + (1-x)^3 - 1 = 0$ によって再帰的に定義される $\mathbb{F}_4$ 上の関数体の塔は 最良 である． □

関数体 $F/\mathbb{F}_{q^2}$ が **モジュラー** であるとは，$F/\mathbb{F}_{q^2}$ の非特異モデルが保型関数によってパラメトライズされるときをいう．関数体の塔 $\mathcal{F}/\mathbb{F}_{q^2}$ が **モジュラー** であるとは，各関数体 $F_i/\mathbb{F}_{q^2}$ がモジュラーのときをいう．

この研究の目標の一つは，次の予想を解決することにある．

Elkies 予想 (1997)：方程式 $f(x,y)=0$ によって再帰的に定義される $\mathbb{F}_{q^2}$ 上の最良塔はモジュラー (楕円モジュラー塔，志村曲線の塔，ドリンフェルトモジュラー塔) である．□

注意 (Elkies (1997))：例 1 と例 2 は楕円モジュラー塔に対応する．

AC2009 では楕円モジュラー塔の構成方法を紹介した．このノート (AC2011) では志村塔の構成方法を紹介する．これらの塔はいずれも Elkies 予想の数値的証拠になっている．

2 楕円モジュラー曲線と志村曲線

ここでは楕円モジュラー曲線と，その一般化である志村曲線とを比較する．

はじめに，楕円モジュラー曲線を紹介する．$\Gamma\subseteq \mathrm{PSL}_2(\mathbb{Z})$ を合同部分群とし $\mathfrak{H}$ を上半平面とする．このとき，$\Gamma\backslash\mathfrak{H}$ をコンパクト化したものを **楕円モジュラー曲線** という．

例 3：N を自然数とし

$$\Gamma_0(N)=\left\{\left(\begin{array}{cc}a&b\\c&d\end{array}\right)\in \mathrm{PSL}_2(\mathbb{Z})\;\middle|\; c\equiv 0 \pmod N\right\}$$

と定義する．このとき，$\Gamma_0(N)\backslash\mathfrak{H}$ をコンパクト化したものは $X_0(N)$ と書かれ，$\mathrm{PSL}_2(\mathbb{Z})\backslash\mathfrak{H}$ をコンパクト化したものは $X(1)$ と書かれる．これらは楕円モジュラー曲線である．□

ここからは $X_0(N^2)$ の種数を零と仮定する．この研究では，被覆写像

$$X_0(N^2)\to X_0(N)\to X(1)$$

を具体的に決定しなければならない．このような写像は，分岐の様子がわからなければ計算できない．ところが，楕円モジュラー曲線はカスプをもつから，もっと単純に決定することができる．それぞれのハウプトモジュールのカスプにおける q-展開を比較すればよい．

例 4：$X(1)$ と $X_0(3)$ のハウプトモジュールはそれぞれ

$$j(q)=\frac{1}{q}+744+196884q+21493760q^2+864299970q^3+\cdots,$$

$$j_3(q)=\frac{1}{q}+15+54q-76q^2-243q^3+1188q^4$$

であることが知られている．このとき，q-展開を比較すれば

$$j(q)=j_3(q)(j_3(q)+216)^3/(j_3(q)-27)^3$$

を得る．□

志村曲線を紹介する．K を総実数体とし A を K 上の四元数環とする．$\Gamma\subseteq A$ を数論的フックス群とする．このとき，$\Gamma\backslash\mathfrak{H}$ を **志村曲線** という．$\Gamma\backslash\mathfrak{H}$ はコンパクトだからコンパクト化は必要ない．志村曲線はカスプをもたない．ここが楕円モジュラー曲線との大きな違いである．

例 5：(1) O を A の最大整環とし N を A/K の被約ノルムとし

$$\Gamma^{(1)}=\{x\in O\mid N(x)=1\},\qquad \Gamma^{(+)}=\{x\in O\mid N(x)\text{ は }K\text{ の単元かつ総正}\}$$

と定義する．このとき，$\Gamma^{(1)}\backslash\mathfrak{H}$ や $\Gamma^{(+)}\backslash\mathfrak{H}$ は $X(1)$ と書かれる．これらは志村曲線である．

(2) 竹内喜佐雄や John Voight のリストにある (e_1,e_2,e_3) 三角群や，四元数環 A の判別式と互いに素な K のイデアルからも志村曲線が定義できる．これらは次の節において紹介する．□

志村曲線はカスプをもたないから，被覆写像を具体的に決定するのに q-展開が使えない．ところが，次のような場合は計算できる．$X(1)$ を (e_1,e_2,e_3) 三角群に付随する志村曲線とし $X_0(I)$ を A の判別式と互いに素な K のイデアル I に付随する志村曲線とする．このとき，$X(1)$ は位数がそれぞれ e_1,e_2,e_3 の 3 つの楕円点をもち，被覆写像 $X_0(I)\to X(1)$ における分岐点はこれら 3 点だけであり，さらに，それぞれの分岐指数も具体的に決定することができる．

3 $(2,4,12)$ 三角群 (Elkies)

ここでは，Elkies による $(2,4,12)$ 三角群に付随する志村曲線の塔の構成方法を紹介する．

K を数体 $\mathbb{Q}(\sqrt{3})$ とし O_K をその数環 $\mathbb{Z}[\sqrt{3}]$ とする．このとき，$\mathfrak{p}_2$ を有理素数 $p=2$ の上にある K の素点とすれば，$p=2$ が K において完全分岐することから $\mathfrak{p}_2=(5-3\sqrt{3})$ である．なぜならば：ϵ を K の単数 $26+15\sqrt{3}$ とすれば，$2=\epsilon(5-3\sqrt{3})^2$ と素因数分解できる．

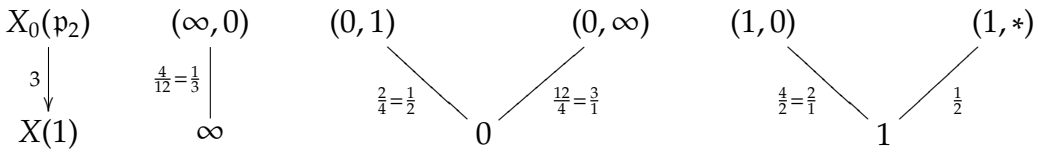
その剰余体は $O_K/\mathfrak{p}_2\simeq\mathbb{F}_2$ となる．A を $\mathfrak{p}_3=(\sqrt{3})$ と 1 つの無限素点において分岐する K 上の四元数環とすれば，A の判別式は $\mathfrak{p}_3$ である．このとき，$\Gamma^{(+)}$ は $(2,4,12)$ 三角群である．志村曲線 $X(1)=\Gamma^{(+)}\backslash\mathfrak{H}$ の種数は零だから，ハウプトモジュール J を次のように選ぶ：

楕円点の位数	楕円点における値
2	1
4	0
12	∞

A の判別式と互いに素な K のイデアル I に対し，志村曲線 $X_0(I)$ は

$$X_0(I)=\left\{\left(J(P),J(P')\right)\in X(1)\times X(1)\;\middle|\;\left(J(P),J(P')\right)\text{は}I\text{-同種によって関係する順序対}\right\}$$

と定義され，対合 $(J(P),J(P'))\leftrightarrow(J(P'),J(P))$ をもつ．$I=\mathfrak{p}_2$ のとき，種数は零である．被覆写像 $\pi_0\colon X_0(\mathfrak{p}_2)\to X(1)$ は $\pi_0(J(P),J(P'))=J(P)$ によって定義され，次数は 3 である．なぜならば：$N(\mathfrak{p}_2)\prod_{\mathfrak{p}|\mathfrak{p}_2}(1+1/N(\mathfrak{p}))=3$ である．ただし $\mathfrak{p}$ の下にある有理素数を p としその剰余次数を f とすれば $N(\mathfrak{p})=p^f$ となる．π_0 は $\{1,0,\infty\}$ においてだけ分岐し，その分岐指数は，既約分数 (P' の位数)/(P の位数) の分母である．ただし非楕円点の位数は 1 とする．このとき，



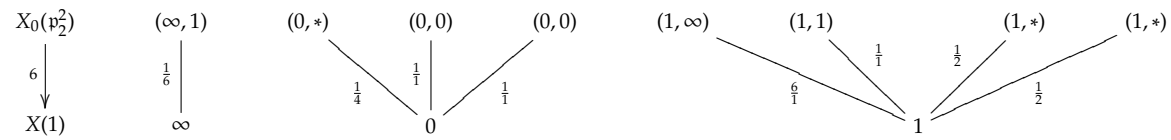
となる．ただし $*$ は非楕円点とする．$X_0(\mathfrak{p}_2)$ のハウプトモジュール t を

$$J=t(4t-3)^2,\qquad J-1=(t-1)(4t-1)^2$$

となるように選ぶ．このとき，対合は

$$\omega^{(1)}(t)=\frac{3}{4t}\tag{1}$$

となる．同様に，志村曲線 $X_0(\mathfrak{p}_2^2)$ の種数は零，被覆写像 $X_0(\mathfrak{p}_2^2)\to X(1)$ の次数は 6 だから



となる．$X_0(\mathfrak{p}_2^2)$ のハウプトモジュール x を

$$t=\frac{x^2+3}{4},\qquad t-1=\frac{x^2-1}{4}\tag{2}$$

となるように選ぶ．このとき，対合は $\omega^{(2)}(x)=(x+3)/(x-1)$ となる．

(1) に (2) を代入すると

$$\frac{x^2+3}{4}\cdot\omega^{(1)}\left(\frac{x^2+3}{4}\right)=\frac{3}{4}$$

を得る．

$$\omega^{(1)}\left(\frac{x^2+3}{4}\right)=\frac{\omega^{(2)}(y)^2+3}{4}$$

だから

$$\left(x^2+3\right)\left(\left(\frac{y+3}{y-1}\right)^2+3\right)=12$$

を得る．志村曲線の塔 $\{X_0(\mathfrak{p}_2^n)\}$ はこの方程式によって構成される．

4 $(2,3,9)$ 三角群 (Elkies)

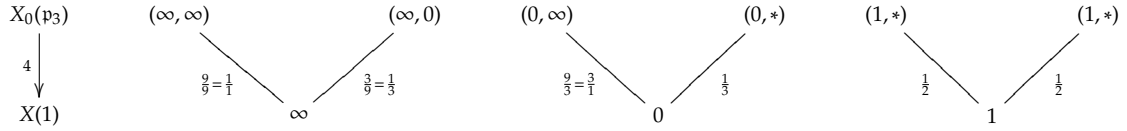
ここでは，Elkies による $(2,3,9)$ 三角群に付随する志村曲線の塔の構成方法を復習する．

K を数体 $\mathbb{Q}(\cos\pi/9)$ とする．$\cos\pi/9$ の $\mathbb{Q}$ 上の最小多項式は $8X^3-6X-1$ である．有理素数 $p=3$ は K において完全分岐する．$\mathfrak{p}_3$ を $p=3$ の上にある K の素点とする．その剰余体は $O_K/\mathfrak{p}_3\simeq\mathbb{F}_3$ となる．ただし O_K は K の数環である．A を 2 つの無限素点において分岐する K 上の四元数環とする．A の判別式は (1) である．このとき，$\Gamma^{(1)}$ は $(2,3,9)$ 三角群である．志村曲線 $X(1)=\Gamma^{(1)}\backslash\mathfrak{H}$ の種数は零だから，ハウプトモジュール J を次のように選べる：

楕円点の位数	楕円点における値
2	1
3	0
9	∞

志村曲線 $X_0(\mathfrak{p}_3)$ の種数もまた零である．被覆写像 $\pi_0\colon X_0(\mathfrak{p}_3)\to X(1)$ の次数は 4 である．なぜならば：$N(\mathfrak{p}_3)\prod_{\mathfrak{p}|\mathfrak{p}_3}(1+1/N(\mathfrak{p}))=4$ である．

π_0 は $\{1,0,\infty\}$ においてだけ分岐し，その他の点では惰性するが不分岐である．このとき，



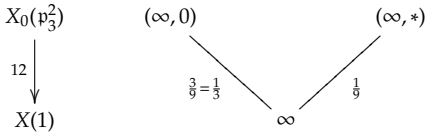
となる．$X_0(\mathfrak{p}_3)$ のハウプトモジュール t を

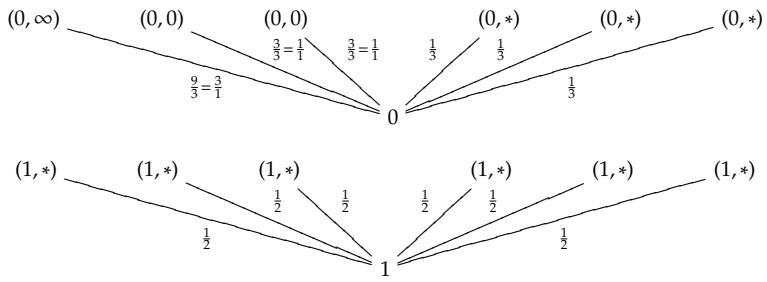
$$J=-\frac{(t-1)^3(9t-1)}{64t^3},\qquad J-1=-\frac{(3t^2+6t-1)^2}{64t^3}$$

となるように選ぶ．このとき，対合は

$$\omega^{(1)}(t)=1-t \tag{3}$$

となる．志村曲線 $X_0(\mathfrak{p}_3^2)$ の種数も零である．被覆写像 $X_0(\mathfrak{p}_2^2)\to X(1)$ の次数は 12 だから





となる．$X_0(\mathfrak{p}_3^2)$ のハウプトモジュール x を

$$t = x^3 \tag{4}$$

となるように選ぶ．このとき，対合は $\omega^{(2)}(x) = (x+2)/(x-1)$ となる．

(3) に (4) を代入すると $x^3 + \omega^{(1)}(x^3) = 1$ を得る．$\omega^{(1)}(x^3) = \omega^{(2)}(y)^3$ だから

$$x^3 + \left(\frac{y+2}{y-1}\right)^3 = 1$$

を得る．志村曲線の塔 $\{X_0(\mathfrak{p}_3^n)\}$ はこの方程式によって構成される． □

注意：志村曲線 $X_0(\mathfrak{p}_3)$ は $(3,3,9)$ 三角群に付随するから楕円点を 3 つもつ．それらは

$$(\infty,\infty), \quad (\infty,0), \quad (0,\infty)$$

である．$X_0(\mathfrak{p}_3^2)$ は $(3,3,3,3)$ 群に付随するから楕円点を 4 つもつ．それらは

$$(\infty,0), \quad (0,\infty), \quad (0,0), \quad (0,0)$$

である．$X_0(\mathfrak{p}_3^3)$ は $(3,3,3)$ 群に付随する楕円曲線である．

5 $(3,3,6)$ 三角群 (オリジナル)

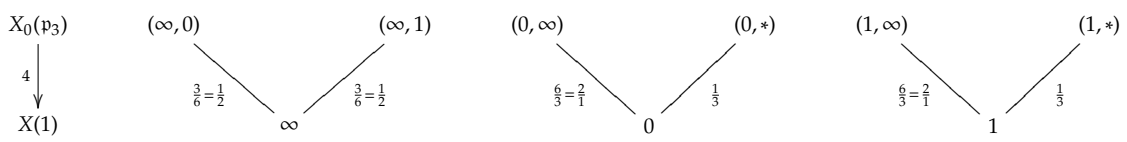
ここでは，$(3,3,6)$ 三角群に付随する志村曲線の塔の構成方法を紹介する．

K を数体 $\mathbb{Q}(\sqrt{3})$ とする．$p = 3$ は K において完全分岐する．$p = 3$ の上にある K の素点 $\mathfrak{p}_3$ に対し $O_K/\mathfrak{p}_3 \simeq \mathbb{F}_3$ となる．ただし O_K は K の数環である．A を 1 つの無限素点において分岐する K 上の四元数環とする．A の判別式は $\mathfrak{p}_2$ である．$\Gamma^{(1)}$ は $(3,3,6)$ 三角群である．志村曲線 $X(1) = \Gamma^{(1)}\backslash\mathfrak{H}$ の種数は零だから，ハウプトモジュール J を次のように選べる：

楕円点の位数	楕円点における値
3	1
3	0
6	∞

志村曲線 $X_0(\mathfrak{p}_3)$ の種数もまた零である．被覆写像 $\pi_0 \colon X_0(\mathfrak{p}_3) \to X(1)$ の次数は 4 である．なぜならば：$N(\mathfrak{p}_3)\prod_{\mathfrak{p}|\mathfrak{p}_3}(1+1/N(\mathfrak{p})) = 4$ である．

π_0 は $\{1,0,\infty\}$ においてだけ分岐し，その他の点では惰性するが不分岐である．このとき，



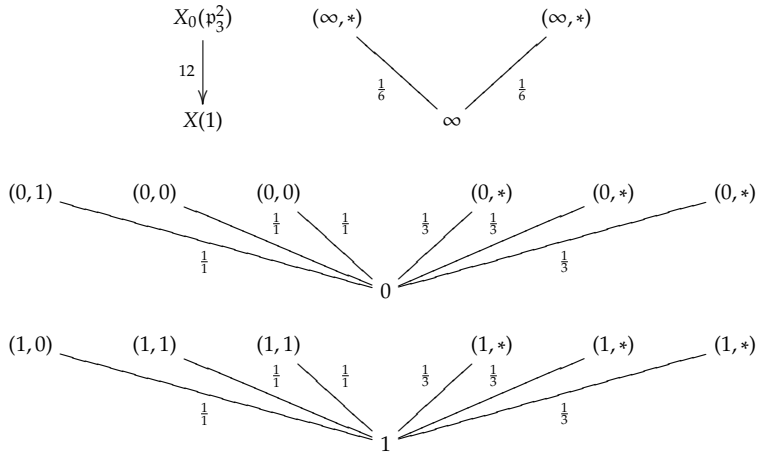
となる．$X_0(\mathfrak{p}_3)$ のハウプトモジュール t を

$$J = \frac{4(2t+1)^3}{(t^2+10t-2)^2}, \qquad J-1 = -\frac{t(t-4)^3}{(t^2+10t-2)^2}$$

となるように選ぶ．このとき，対合は

$$\omega^{(1)}(t) = -\frac{(5-3\sqrt{3})t-2}{t+(5-3\sqrt{3})} \tag{5}$$

となる．$X_0(\mathfrak{p}_3^2)$ の種数も零である．被覆写像 $X_0(\mathfrak{p}_2^2) \to X(1)$ の次数は 12 だから



となる．$X_0(\mathfrak{p}_3^2)$ のハウプトモジュール x を

$$t = -\frac{(5+3\sqrt{3})x^3+4}{x^3-2(5+3\sqrt{3})}, \qquad \xi^3 = 2\frac{(5-3\sqrt{3})t-2}{t+(5+3\sqrt{3})} \tag{6}$$

となるように選ぶ．このとき，対合は $\omega^{(2)}(x) = -2(x-1)/(x+2)$ となる．

(5) と (6) から

$$\left(-2\frac{y-1}{y+2}\right)^3 = 2\frac{(5-3\sqrt{3})x^3+4}{x^3-2(5-3\sqrt{3})}$$

を得る．志村曲線の塔 $\{X_0(\mathfrak{p}_3^n)\}$ はこの方程式によって構成される． □

注意：志村曲線 $X_0(\mathfrak{p}_3)$ は $(3,3,3,3)$ 群に付随するから楕円点を 4 つもち，それらは

$$(\infty,0), \quad (\infty,1), \quad (0,\infty), \quad (1,\infty)$$

である．$X_0(\mathfrak{p}_3^2)$ は $(3,3,3,3,3,3)$ 群に付随するから楕円点を 6 つもち，それらは

$$(0,1), \quad (0,0), \quad (0,0), \quad (1,0), \quad (1,1), \quad (1,1)$$

である．

整数の冪乗和に関する恒等式と求積公式

澤　正憲

1. Hilbert 恒等式

正整数 r が与えられたとき，任意の自然数 n を幾つかの自然数の r 乗の和で表わすことができるか，という類の問題を Waring の問題といいます [2]．古典的な結果としてお馴染み Lagrange の四平方定理があります．Waring の問題そのものは 1909 年に Hilbert によって完全解決されましたが，Hilbert の仕事から派生した数々の興味深い問題が現在でも考えられています [6].

Hilbert は Waring 問題を解決させるうえで次の鍵となる定理を示しました.

定理 1.1. (Hilbert [4]). n, r を正の整数とし，$N = \binom{n+2r-1}{n-1}$ とおく．このとき正の有理数 λ_k および整数 α_{kj} で次を満たすものが存在する：

$$(x_1^2 + \cdots + x_n^2)^r = \sum_{k=1}^{N} \lambda_k (\alpha_{k1}x_1 + \cdots + \alpha_{kn}x_n)^{2r} \tag{1.1}$$

Reznick は，1992 年の有名な論文 [9] で,（1.1）のような式を Hilbert 恒等式と名付け[1]，必ずしもワーリング問題と結びつけることなく，恒等式そのものの “美しさ” を評価する様々な尺度について論じました．こうした尺度として，例えば，恒等式の $2r$ 乗項の和に現れる異なる項の個数 N の大小を比較することなどが挙げられます．Reznick の Hilbert 恒等式の定義では，係数 λ_k は正の実数，また α 達は実数全体を動きます．式（1.1）のように，λ_k が有理数，α が整数を動く Hilbert 恒等式は有理的であるといいます．有理的恒等式は，Hilbert の Waring 問題の解に用いられたのみならず，Schülting が 1987 年に Obserwolfach の会議で提案した，holomorphy 環の単元に関わる一問題との関連性 [11] 等においても重要な役割を果たしました.

2. 立体求積法

定理 1.1 の Hilbert による証明は，Bolzano-Weierstrass の定理や Carathéodori の定理など純解析的な議論に基づいており，それゆえに非構成的でした．これを受け，Hilbert の仕事以降，多くの研究者が Hilbert 恒等式の具体的な構成法を模索してきました．一連の研究の流れにおける重要な進展として，Reznick の等価性定理 [9] が挙げられます．そこには球面上の立体求積公式という（数値）解析的な概念が深く関与しています.

S^{n-1} を $(n-1)$-次元単位球面とします．すなわち,

$$S^{n-1} = \{(u_1, \ldots, u_n) \in \mathbb{R}^n \mid u_1^2 + \cdots + u_n^2 = 1\}.$$

球面 S^{n-1} 上の Haar 測度を μ と表します．V を S^{n-1} の有限部分集合とし，その上で正値実数値関数（重み関数）$\lambda : V \to \mathbb{R}_{>0}$ が定義されているとします.

1991 *Mathematics Subject Classification.* Primary 65D32, Secondary 46B04, 05B05, 05B15.

本報告書は Yuan Xu 教授（University of Oregon）および野崎寛氏（Tohoku University）との最新の共同研究における成果をまとめることにより作成されています．また一連の研究は学術研究助成基金助成金 (若手研究 (B)) により支えられています.

[1]ほぼ同時期に Schmid[11] も同じネーミングを使っています.

定義 2.1.

$$\int_{u\in S^{n-1}} f(u)d\mu = \sum_{v\in V}\lambda(v)f(v) \tag{2.1}$$

が次数 $2r$ のすべての斉次多項式 f に対して成り立つとき[2]，(V,λ) を指数 $2r$ の立体求積公式という．

注 2.2. 数値解析およびその周辺分野で通常考察されるのは “次数型”の立体求積公式です．すなわち，式 (2.1) が次数 $2r$“以下”のすべての斉次多項式に対して成り立つとき，(V,λ) を次数 $2r$ の立体求積公式といいます．なお代数的組合せ論の分野で頻繁に取り上げられる球デザインは，次数型で，かつ重み関数に制約が課せられた[3]特殊な求積公式です．

次は Hilbert 恒等式と球面上の立体求積公式の等価性に言及する基本的な定理です．

定理 2.3. (Reznick [9]). 次は同値である．

(1)

$$\int_{u\in S^{n-1}} f(u)d\mu = \sum_{k=1}^{N}\lambda(v_k)f(v_k)$$

は指数 $2r$ の立体求積公式をなす．

(2)

$$(x_1^2+\cdots+x_n^2)^r = \sum_{k=1}^{N}\frac{\lambda(v_k)}{c_{n,2r}}(v_{k1}x_1+\cdots+v_{kn}x_n)^{2r}$$

が成り立つ．ただし，

$$c_{n,2r} = \frac{B(\frac{1}{2},\frac{n-1}{2})}{B(\frac{2r+1}{2},\frac{n-1}{2})} = \prod_{j=1}^{r}\frac{n+2j}{1+2j},\quad v_k=(v_{k1},\cdots,v_{kn})$$

球面上の立体求積公式の存在性は，古典的な有限次元のバナッハ空間上のある種の等長埋め込みの存在性と等価であることが知られていて，その文脈においても，Reznick と同様の主張が示されています．詳しくは [7] を参照してください．

3. 求積公式論への群論的アプローチ

ここでは，球面上の立体求積公式の理論への一群論的アプローチと，関連する新しい結果を幾つか紹介します．講演ではブロックデザインの構造に基づいた組合せ論的アプローチにも触れましたが，ここでは省略させていただきます．

3.1. Sobolev の定理.

$\mathcal{P}_t(\mathbb{R}^n)$ を次数 t 以下の多項式全体からなる空間とします．すなわち，$\mathcal{P}_t(\mathbb{R}^n)=\sum_{i=1}^{t}\mathrm{Hom}_i(\mathbb{R}^n)$．次数 t の斉次調和多項式からなる $\mathcal{P}_t(\mathbb{R}^n)$ の部分空間を $\mathrm{Harm}_t(\mathbb{R}^n)$ と表すことにします．

n 次直交群 $O(n)$ の有限部分群を G とします．$f\in\mathcal{P}_t(\mathbb{R}^n)$ に対して，$\sigma\in G$ の f 上への作用を

$$(\sigma f)(u) = f(u^{\sigma^{-1}}),\qquad u\in\mathbb{R}^n$$

と定めます．任意の $\sigma\in G$ に対して $\sigma f=f$ を満たす多項式 f は G-不変であるといいます．空間 $\mathcal{P}_t(\mathbb{R}^n),\mathrm{Harm}_t(\mathbb{R}^n)$ の G-不変多項式からなる部分空間をそれぞれ $\mathcal{P}_t(\mathbb{R}^n)^G,\mathrm{Harm}_t(\mathbb{R}^n)^G$ と表します．

---

[2]次数 $2r$ の斉次多項式からなる空間を $\mathrm{Hom}_q(\mathbb{R}^n)$ で表わします．

[3]具体的には重み関数 λ が V 上の定数関数です．

立体求積公式 (V,λ) は，次の条件を満たすとき，G-不変であるといいます．

(1) V は G-軌道 $z_1^G,\dots,z_M^G$ の和集合で表わされる．
(2) 各軌道 z_i^G および $v,v'\in z_i^G$ に対して，$\lambda(v)=\lambda(v')=\lambda_i$.

次は Sobolev の定理と呼ばれています.

定理 3.1. (Sobolev [12]). G を $O(n)$ の有限部分群とする．$V=\cup_{k=1}^M z_k^G$ とする．ただし，$z_k\in S^{m-1}, r_k>0$. このとき次は同値である．

(1) (V,λ) は次数 t の G-不変求積公式である．
(2) 任意の $1\le l\le t$，$\varphi\in \mathrm{Harm}_l(\mathbb{R}^m)^G$ に対して，$\sum_{v\in V}\lambda(v)\varphi(v)=0$.

以下 G を $\mathbb{R}^n$ における既約鏡映群としましょう．そのような鏡映群は完全に分類されることが知られています．整数 $1=d_1\le d_2\le\cdots\le d_m$ を G の exponent とします.

定理 3.2. (Molien-Poincaré 級数). $q_i=\dim(\mathrm{Harm}_i(\mathbb{R}^n)^G)$ とする．このとき

$$\sum_{i=0}^{\infty} q_i\lambda^i=\prod_{i=2}^{n}\frac{1}{1-\lambda^{1+d_i}}$$

G の基本ルート $\alpha_1,\alpha_2,\dots,\alpha_n$ に対して，ベクトル $z_1,z_2,\dots,z_n$ を

$$z_i\perp\alpha_j\Longleftrightarrow i\neq j$$

によって定めます．z_i 達は *corner vector* と呼ばれています．一般性を失わないので，各 z_k は正規化されているとしましょう．$J\subset\{1,2,\dots,n\}$ および $r_k>0$ に対して，次の集合を考えます.

$$\mathcal{Z}(G,J)=\bigcup_{k\in J} z_k^G$$

Bajnok は，定理 3.1 および定理 3.2 を用いて次の定理を示しました.

定理 3.3. (Bajnok [1]). 自然数 $n\ge 2$ に対して，$(\mathcal{Z}(B_n,J),\lambda)$ が指数 8 の B_n-不変求積公式をなすような J，λ は存在しない.

この定理は最近次のように一般化されました.

定理 3.4. (野崎-澤 [8]，野崎-澤 (2012)). n を 2 以上の整数，G を $\mathbb{R}^n$ における有限既約鏡映群とする．このとき，次の各場合に対して，$(\mathcal{Z}(G,J),\lambda)$ が指数 t の G-不変求積公式をなすような J，λ は存在しない.

(1) $t\ge 6$ $\quad G=A_{n-1}$ のとき;
(2) $t\ge 8$ $\quad G=B_n,D_n$ のとき;
(3) $t\ge 10$ $\quad G=E_6$ のとき;
(4) $t\ge 12$ $\quad G=F_4,H_3,E_7$ のとき;
(5) $t\ge 16$ $\quad G=E_8$ のとき;
(6) $t\ge 24$ $\quad G=H_4$ のとき.

定理 3.4 の t の評価は最良です．例えば，$G=F_4$ の場合，指数 11 の求積公式が存在し，その完全な分類も行うことができます.

定理 3.3 の Bajnok の証明は理論的にはとても興味深いものですが，不変調和多項式に関わる厄介な計算を多数必要とし，このため比較的証明が長く，また解析などの分野の研究者に理解されにくいという難点があります．そこで講演では，Bajnok の定理の Hilbert 恒等式を用いた初等的な別証明にも触れましたが，ここでは詳細を省略いたします.

4. Hilbert 恒等式の例

1900 年初頭，Hurwitz は次の恒等式を導き，Waring 問題を 8 乗数の場合に進展させました．

定理 4.1. (Hurwitz [5]).

$$\begin{aligned}5040\Big(\sum_{i=1}^{4}x_i^2\Big)^4 &= 6\sum_{4}(2x_i)^8+60\sum_{12}(x_i\pm x_j)^8\\ &\quad+\sum_{48}(2x_i\pm x_j\pm x_k)^8+6\sum_{8}(x_1\pm x_2\pm x_3\pm x_4)^8\end{aligned}\tag{4.1}$$

次の恒等式は多次元正則単体上の立体求積公式から導出することができます[4].

定理 4.2. (澤-Xu, [10]).

$$\begin{aligned}80640\Big(\sum_{i=1}^{4}x_i^2\Big)^4 &= 60\sum_{8}(x_1\pm x_2\pm x_3\pm x_4)^8+60\sum_{4}(2x_i)^8+6\sum_{12}(2x_i\pm 2x_j)^8\\ &\quad+\sum_{16}(2x_i\pm 2x_j\pm 2x_k)^8+\sum_{32}(3x_i\pm x_j\pm x_k\pm x_l)^8\end{aligned}\tag{4.2}$$

(4.1)，(4.2) はともに $(\sum_{i=1}^4 x_i^2)^4$ に関する有理的な Hilbert 恒等式です．これらを何かしらの尺度で比較して，一方は他方よりも優れているということはできないでしょうか．例えば，２つの恒等式の右辺はともに 72 個の 8 乗項の和であるのに対して，左辺については (4.1) の方が小さくなっています．このことは Waring 問題への応用的側面からは (4.1) の方が優れていることを示しています[5]．(4.1) よりも (4.2) の方が良いというような尺度を新しく提示することはできるでしょうか．

続いて，$(\sum_{i=1}^4 x_i^2)^5$ に関する恒等式を紹介します．

定理 4.3. (野崎-澤，2012)．$\frac{1}{192}\le a\le\frac{1}{120}$ とする．このとき，

$$\begin{aligned}(\sum_{i=1}^{4}x_i^2)^5 &= \tfrac{1}{2520}\sum_{4}(2x_i)^{10}+\tfrac{1}{2520}\sum_{8}(x_1\pm x_2\pm x_3\pm x_4)^{10}\\ &\quad+\tfrac{1-120a}{272160}\sum_{32}(3x_i\pm x_j\pm x_k\pm x_l)^{10}+\tfrac{1-120a}{272160}\sum_{16}(2x_i\pm 2x_j\pm 2x_k)^{10}\\ &\quad+\tfrac{192a-1}{68040}\sum_{48}(2x_i\pm x_j\pm x_k)^{10}+\tfrac{12-960a}{630}\sum_{12}(x_i\pm x_j)^{10}\end{aligned}\tag{4.3}$$

特に a が有理数のとき，対応する恒等式も有理的である．

Reznick 氏によると，上のように係数達に自由度がある Hilbert 恒等式を構成するテクニックは，高次形式の研究者の間ではあまり知られていないよそうです．このことは Hilbert 恒等式の理論を立体求積公式論に帰着させることの利点を示唆するものと見なすことができ，興味深いのではないでしょうか．

(4.3) は有名な Schur の恒等式を含みます．

---

[4]詳細は [10] を参照してください．

[5]これについて，岩手大学の川田浩一先生，首都大学東京の津村博文先生から様々なご指摘・示唆をいただきました．

系 4.4. (Schur [2, p. 721]).

$$22680(\sum_{i=1}^{4} x_i^2)^5 = 9\sum_{4}(2x_i)^{10} + 9\sum_{8}(x_1 \pm x_2 \pm x_3 \pm x_4)^{10} + \sum_{48}(2x_i \pm x_j \pm x_k)^{10} + 180\sum_{12}(x_i \pm x_j)^{10} \tag{4.4}$$

Schur の恒等式は 10 乗項に関する式であるのに対して，前述の Hurwitz の恒等式は 8 乗項に関する式ですから，それらはもちろん “恒等式としては” 異なります．しかしながら，立体求積公式としてはそれらは完全に等価であることが確かめられます．同様に，4 乗項に関する Lucas の恒等式，Liouville の恒等式 [2] が変数間の適当な可逆変換により移りあうこともよく知られています．これらのことは Hilbert 恒等式を立体求積公式の言葉で捉え直すことの意義を示唆するものと捉えることができます．

最後に，ブロックデザインの一つ，t-wise balanced design の構造をもつ Hilbert 恒等式を紹介します[6].

定理 4.5. (澤，2011).

$$120(\sum_{i=1}^{7} x_i^2)^3 = \sum_{56}(x_i \pm x_{i+2} \pm x_{i+3} \pm x_{i+4})^6 + 2\sum_{28}(x_i \pm x_{i+2} \pm x_{i+3})^6 + \sum_{7}(2x_i)^6 \tag{4.5}$$

ただし，右辺の x 達の添え字は 7 を法として巡回的に計算します．

Reznick [9, p. 112] は，2-$(7, 3, 1)$ の構造を利用して次の美しい恒等式を導きました:

$$960(\sum_{7} x_i^2)^3 = 2\sum_{i=1}^{7}(2x_i)^6 + \sum_{42}(2x_i \pm 2x_j)^6 + \sum_{64}(x_1 \pm \cdots \pm x_7)^6 \tag{4.6}$$

(4.5) 右辺には異なる 6 乗項が 91 個現れるのに対して，Reznick の恒等式では 113 個の異なる 6 乗項が現れます．このことから (4.5) は Reznick の恒等式を改良していると見ることができます．91 から項数をさらに落とすことができるかどうかについては今後検討の余地の残るところです．ちなみに，$(\sum_{i=1}^{7} x_i^2)^3$ を表現するために 6 乗項は少なくとも 84 個必要であることが知られています．

謝辞 本研究集会において成果発表の機会をくださいました主催者ならびに実行委員の皆様に深く感謝致します．特に首都大学東京の津村博文先生におかれましては，講演内容について貴重なコメントをくださいましたこと，また岩手大学の川田浩一先生をご紹介くださいましたことを厚く御礼申し上げます．

[6] t-wise balanced design の定義等については [3] をご参照ください.

References

[1] B. Bajnok. *Orbits of the hyperoctahedral group as Euclidean designs*. J. Algebraic Combin. **25** (2007), 375–397.
[2] L. E. Dickson. *History of the Theory of Numbers, II*. Carnegie Institution of Washington, 1923.
[3] R. Fuji-Hara, S. Kuriki, M. Jimbo. *On balanced complementation for regular tt-wise balanced designs*. Discrete Math. **76** (1989), 29–35.
[4] D. Hilbert. *Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n-ter Potenzen (Waringsches Problem)*. Math. Ann. **67** (1909), 281–300.
[5] A. Hurwitz. *Über die Darstellung der ganzen Zahlen als Summen von n^{ten} Potenzen ganzer Zahlen*. Math. Ann. **65** (1908), 424–427.
[6] K. Kawada, T. Wooley. *Sums of fourth powers and related topics*. J. reine angew. Math. **512** (1999), 173–223.
[7] Y. I. Lyubich, L. N. Vaserstein. *Isometric embeddings between classical Banach spaces, cubature formulas, and spherical designs*. Geom. Dedicata **47** (1993), 327–362.
[8] H. Nozaki, M. Sawa. *Note on cubature formulae and designs obtained from group orbits*. Canad. J. Math. (doi.org/10.4153/CJM-2011-069-5).
[9] B. Reznick. *Sums of even powers of real linear forms*. Mem. Amer. Math. Soc. **96** (1992), No. 463.
[10] M. Sawa, Y. Xu. *On positive cubature rules on the simplex and isometric embeddings*. Submitted (arXiv:1108.3385v1).
[11] J. Schmid. *On totally positive units of real holomorphy rings*. Israel J. Math. **85** (1994), 339–350.
[12] S. L. Sobolev. *Cubature formulas on the sphere which are invariant under transformations of finite rotation groups* (in Russian). Dokl. Akad. Nauk SSSR **146** (1962), 310–313.

名古屋大学大学院情報科学研究科, 464-8601 名古屋市不老町千種区
E-mail address: sawa@is.nagoya-u.ac.jp

平方剰余の条件を付加した $a \pmod p$ の剰余位数の分布について

知念 宏司 (近畿大学 理工学部)
田村 知佳子 (大阪商業大学高等学校)

2011.11.9
第 9 回「代数学と計算」研究集会 (AC2011)
(首都大学東京)

概 要

平方因子を持たない 2 以上の自然数 a を固定し, p を $(a,p)=1$ となる奇素数, $D_a(p)$ を $\mathbf{Z}/p\mathbf{Z}^\times$ での a の位数 (剰余位数) とする. $D_a(p)$ が素数 q で割り切れるような p の自然密度 $\Delta Q_a(q,0)$ は Hasse (1965,66), Odoni (1981) らによってすでに求められている. 本稿では, 別に整数 b をとり, $D_a(p)$ が素数 q で割り切れ, かつ $(b/p)=1$ となる素数 p の自然密度を, a,b への軽い制限のもとで求める ((b/p) は Legendre 記号). それは $\Delta Q_a(q,0)$ の半分になると考えるのが自然だが, a,b が影響し合ってそうならない場合もある. その状況を調べるのが目的である. また計算機実験の結果, 手法についても述べる.

1 導 入

a を平方因子を持たない 2 以上の自然数, p を $(a,p)=1$ となる奇素数とする. また $D_a(p)$ を a の $\bmod p$ での剰余位数, つまり $\mathbf{Z}/p\mathbf{Z}^\times$ において a が生成する部分群 $\langle a\rangle$ の位数とする. 本稿では a を固定して p を動かす状況を考える. まず, 集合

$$Q_a(k,l)=\{p\in\mathbf{P}\ ;\ D_a(p)\equiv l \pmod k\}$$

を考える ($\mathbf{P}$ は奇素数全体の集合). この集合 $Q_a(k,l)$ の自然密度は比較的古くから考察されている. ここで一般に, 素数からなる集合 S の自然密度とは

$$\Delta S=\lim_{x\to\infty}\frac{\#\{p\in S\ ;\ p\le x\}}{\#\{p\in\mathbf{P}\ ;\ p\le x\}}$$

で定義される (正確にはこの極限値が存在するとき ΔS を S の自然密度と呼ぶ). したがって, $Q_a(k,l)$ の場合, 集合

$$Q_a(x;k,l)=\{p\in\mathbf{P}\ ;\ p\le x,\ D_a(p)\equiv l \pmod k\}$$

を定義しておいて

$$\Delta Q_a(k,l)=\lim_{x\to\infty}\frac{\#Q_a(x;k,l)}{\pi(x)}$$

を考える, とも言いかえられる ($\pi(x)$ は x 以下の素数の個数).

注 意. 集合 $\mathbf{P}$ をわれわれの問題に合わせて「奇素数全体の集合」としてしまうと, 一般的定義における S が素数 2 を含むかどうか, $\pi(x)$ が 2 を数えるかどうか, また a を割る

素数を数えるかどうか, といった点が気になるかも知れないが, 状況によって臨機応変に解釈頂ければ幸いである. 尤も, $x \to \infty$ とする極限においては有限個の差は問題にならない.

さて, 密度 $\Delta Q_a(k,l)$ であるが, $k=q$ が素数かつ $l=0$ の場合は比較的簡単で, 次の結果が知られている:

定 理 1.1 (Hasse [5], [6], Odoni [11]) q が素数のとき,

$$\Delta Q_a(q,0) = \begin{cases} \dfrac{q}{q^2-1}, & a>2 \text{ のとき}, \\ \dfrac{17}{24}, & a=2 \text{ のとき}. \end{cases} \tag{1.1}$$

この場合は Sierpinski [12] によって問題提起され, Hasse [5], [6] により解析的密度が求められた. さらに Odoni [11] によって, a と k がやや一般的な形に広げられて自然密度が求められた.

$l \neq 0$ の場合は複雑かつ困難であるが, k が素数べきの場合, ある種の無限個の Kummer 拡大体の Dedekind zeta 関数についての Riemann 予想 (**一般 Riemann 予想**) を仮定すると自然密度を決定することができる ([1], [10], [2]). また k が一般の合成数のときは, やはり一般 Riemann 予想の仮定のもと, 自然密度を求めるアルゴリズムが存在し, したがって手間さえ厭わなければ自然密度を決定することができる ([3]).

本稿では, a とは別に整数 b $(\neq 0)$ をとって固定し, 素数集合

$$S_{a,b}(k,l) = \left\{ p \in \mathbf{P} \ ; \ p \nmid a,b, \ D_a(p) \equiv l \pmod{k}, \ \left(\frac{b}{p}\right) = 1 \right\}$$

を考える. ただし $(\frac{b}{p})$ は Legendre 記号である. ところで, 次のことはよく知られている:

$$\Delta \left\{ p \in \mathbf{P} \ ; \ p \nmid b, \ \left(\frac{b}{p}\right) = 1 \right\} = \frac{1}{2}. \tag{1.2}$$

集合 $S_{a,b}(k,l)$ は $Q_a(k,l)$ に条件 $(\frac{b}{p})=1$ を付け加えたものだから,

$$\Delta S_{a,b}(k,l) = \frac{1}{2} \Delta Q_a(k,l) \tag{1.3}$$

と予想するのが確率的には自然である. しかし, a, b の選び方によっては, 確率通りにならないこともあると考えられる. それは a と b が何らかの形で代数的に影響を与えあう場合に起こることである. 本稿の目的は, $(k,l)=(q,0)$ (q: 素数) の場合に $S_{a,b}(k,l)$ の自然密度を決定し, どのような場合にこの密度が確率的推論通りになるか, あるいはならないかを観察することである.

以下, 主結果を述べる. $Q_a(k,l)$ のときと同様に, 集合

$$S_{a,b}(x;k,l) = \left\{ p \in \mathbf{P} \ ; \ p \leq x, \ p \nmid a,b, \ D_a(p) \equiv l \pmod{k}, \ \left(\frac{b}{p}\right) = 1 \right\}$$

を定義しておく. まず q が奇素数の場合である:

定 理 1.2 a, b は平方因子をもたず, $a, b \geq 2$, q は奇素数とする. このとき,

$$\#S_{a,b}(x;q,0) = \Delta S_{a,b}(q,0)\mathrm{li}\, x + O\left(\frac{x}{\log x \log\log x}\right) \quad (x \to \infty).$$

ここで, $\mathrm{li}\, x = \int_2^x (\log t)^{-1} dt$ であり,

$$\Delta S_{a,b}(q,0) = \begin{cases} \dfrac{q}{q^2-1}, & b = q,\ q \equiv 1 \pmod 4 \text{ のとき,} \\ \dfrac{q}{2(q^2-1)}, & \text{その他の場合.} \end{cases}$$

関数 $\mathrm{li}\, x$ は x 以下の素数の個数 $\pi(x)$ を近似する関数で $\mathrm{li}\, x \sim x/\log x$ $(x \to \infty)$, したがって, 定理において主要項 $\mathrm{li}\, x$ の係数が求める自然密度である. また, 第 1 の場合に $\Delta S_{a,b}(q,0) = \Delta Q_a(q,0)$ (より詳しく, 集合として $S_{a,b}(q,0) = Q_a(q,0)$) であることは, 相互法則などにより初等的に示すことができる. $q = 2$ の場合は少々複雑である:

定 理 1.3 a, b は平方因子をもたず, $a, b \geq 2$ とする. このとき,

$$\#S_{a,b}(x;2,0) = \Delta S_{a,b}(2,0)\mathrm{li}\, x + O\left(\frac{x}{\log x \log\log x}\right) \quad (x \to \infty).$$

ただし, 自然密度 $\Delta S_{a,b}(2,0)$ は次で与えられる:

$$\Delta S_{2,2}(2,0) = \frac{5}{24};\ \Delta S_{a,a}(2,0) = \frac{1}{6}\ (a \neq 2 \text{ のとき});$$
$$\Delta S_{a,b}(2,0) = \frac{1}{3}\ (a, b \neq 2,\ a \neq b,\ a \neq 2b \ \text{ かつ } \ b \neq 2a \text{ のとき});$$

それ以外の場合, すなわち下の (i) から (iii) のうちどれかが成り立つときには

$$\Delta S_{a,b}(2,0) = \frac{17}{48}$$

となる:

(i) $a, b \neq 2$, で $a = 2b$ または $b = 2a$,
(ii) $a \neq 2$, $b = 2$,
(iii) $a = 2$, $b \neq 2$.

定理 1.2 からわかることは, q が奇素数のときは, $Q_a(q,0)$ に平方剰余の条件 $(\frac{b}{p}) = 1$ を付加した場合, 初等的に $S_{a,b}(q,0) = Q_a(q,0)$ が示せる場合を除いて確率的推論 (1.3) の通りになっているということであり, ほとんどの場合に標準的な分布になっていると言える. 定理 1.3, すなわち $q = 2$ の場合に標準的といえるのは $\Delta S_{a,b}(2,0) = 1/3$ となる場合である ($\Delta Q_a(2,0) = 2/3$ $(a \neq 2)$ であった). この場合の a, b の条件を見ると, a と b の間に特別な関係は見られず, さらに 2 という数も a, b には含まれないことが観察される. 一方, $\Delta S_{a,b}(2,0) = 17/48$ となる場合は非常に特殊なように見えるが, $\Delta Q_2(2,0) = 17/24$

であったことを考えると, これは a, b が何らかの形で 2 と関係する場合の標準的分布と見ることもできる.

さて, 本稿における問題を考察した動機についてもう少し詳しく述べよう. そもそも条件 $D_a(p) \equiv 0 \pmod q$ に $(\frac{b}{p}) = 1$ を付け加えることにどのような意味があるか, という点である. 確かに, $(\frac{b}{p}) = 1$ は素数の集合を二分するのには最も安直な条件であるが, それだけではなく, 次のような考えがあった: それは原始根の動きをある程度追えるのではないか, ということである. まず a が $\bmod p$ で原始根であるとは, a が群 $\mathbf{Z}/p\mathbf{Z}^\times$ の生成元となることである. 一方, $(\frac{b}{p}) = 1$ であることは, b が $\mathbf{Z}/p\mathbf{Z}^\times$ において平方元となることと同値である. 容易にわかるように, 平方元は $\mathbf{Z}/p\mathbf{Z}^\times$ の生成元とはなり得ない (平方元全体の集合は $\mathbf{Z}/p\mathbf{Z}^\times$ の指数 2 の部分群である). さらに, $\mathbf{Z}/p\mathbf{Z}^\times$ の位数 $p-1$ は偶数であるから, a が $\bmod p$ で原始根であるならば, $D_a(p) \equiv 0 \pmod 2$ が成り立つことになる.

これらのことを考え合わせると, まず集合 $Q_a(2,0)$ には a が $\bmod p$ で原始根であるような素数 p がすべて含まれている. しかし, $b = a$ として $Q_a(2,0)$ に条件 $(\frac{a}{p}) = 1$ を付け加えると, それらの p はすべて $Q_a(2,0)$ から追い出されることになる. したがって, もし a が $\bmod p$ で原始根となる p がたくさんあるならば, 集合 $S_{a,a}(2,0)$ は確率的推論から想定されるよりも小さな密度となるはずである. というのも, 確率的推論通りならば密度は $2/3$ から $1/3$ にならなければならないが, 一方 Hooley [7] によれば, 一般 Riemann 予想のもと, a が $\bmod p$ で原始根である p の密度は, (a の値によって異なるが, 標準的な場合は) およそ 0.37395 程度であり, これは $2/3 - 1/3 = 1/3$ より大きいからである. そして実際, 定理 1.3 によれば, $S_{a,a}(2,0) = 1/6$ $(a \neq 2)$ であり, 確率的推論よりも確かに少なくなっている.

こうした観点から再度主結果を見たとき, 興味深いのは

- $\Delta Q_a(2,0)$ と $\Delta S_{a,a}(2,0)$ の比較
- $\Delta Q_a(q,0)$ と $\Delta S_{a,a}(q,0)$ $(q \geq 3)$ の比較

ということになる. まず, $a \neq 2$ のとき,

$$\Delta Q_a(2,0) = \frac{2}{3}, \quad \Delta S_{a,a}(2,0) = \frac{1}{6}$$

であり, 上述の通り, $Q_a(2,0)$ に条件を付け加えると, 大量の p が取り除かれていることがわかる. 一方で $q \geq 3$ のとき, $b = q$, $q \equiv 1 \pmod 4$ が成り立たない標準的な場合は

$$\Delta Q_a(q,0) = \frac{q}{q^2-1}, \quad \Delta S_{a,a}(q,0) = \frac{q}{2(q^2-1)}$$

であり, たとえ $a = b$ であっても密度は代数的な影響を受けず, 確率的推論通りであると見られるのである. もちろん, $(\frac{a}{p}) = 1$ を付け加えることで原始根以外の p で取り除かれるものもあるため, 原始根の動きを直接捉えられているとは言えないが, 間接的にせよこの現象の観察はなかなか興味深い. また, われわれの結果に一般 Riemann 予想の仮定は不要であることも付け加えておく.

注 意. 定義から明らかに, $\Delta S_{a,b}(2,1)$ も $\Delta S_{a,b}(2,1) = 1/2 - \Delta S_{a,b}(2,0)$ として求めることができる. また, $\Delta S_{a,b}(4,0)$ も主結果と同様の方法で求めることができ, したがって $\Delta S_{a,b}(4,2)$ も $\Delta S_{a,b}(4,2) = \Delta S_{a,b}(2,0) - \Delta S_{a,b}(4,0)$ から求まる ([4]).

以下, 第 2 節では証明の概略を述べ, 第 3 節では数値実験の方法, 結果を紹介する. なお, 本稿の結果についてより詳しくは [4] を参照されたい.

2 証明の概略

本節では定理 1.2 の証明の概略を述べる (定理 1.3 も概ね同様に示される). まず, $b = q$, $q \equiv 1 \pmod 4$ の場合には次のようにして $S_{a,b}(q,0) = Q_a(q,0)$ が示される: $D_a(p)$ は $p-1$ を割り切るから, $D_a(p) \equiv 0 \pmod q$ から $p \equiv 1 \pmod q$ が得られる. これと $q \equiv 1 \pmod 4$ を合わせると平方剰余の相互法則から

$$\left(\frac{b}{p}\right) = \left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = \left(\frac{1}{q}\right) = 1.$$

こうして $D_a(p) \equiv 0 \pmod q$ からつねに $(\frac{b}{p}) = 1$ が従うのである.

次に $b = q$, $q \equiv 1 \pmod 4$ が成り立たない場合を考える. 位数 $D_a(p)$ は直接扱いにくいため, 指数, すなわち

$$D_a(p) I_a(p) = p - 1$$

で定義される量 $I_a(p)$ の条件に置き換える. これはこの種の問題を扱う場合によく行なわれることである. すると

$$\begin{aligned} \#S_{a,b}(x;q,0) = {} & \#\left\{p \le x\ ;\ p \equiv 1 \pmod q, \left(\frac{b}{p}\right) = 1\right\} \\ & - \sum_{j\ge 1} \#\left\{p \le x\ ;\ p \equiv 1 \pmod{q^j},\ q^j \mid I_a(p),\ \left(\frac{b}{p}\right) = 1\right\} \\ & + \sum_{j\ge 1} \#\left\{p \le x\ ;\ p \equiv 1 \pmod{q^{j+1}},\ q^j \mid I_a(p),\ \left(\frac{b}{p}\right) = 1\right\} \end{aligned} \tag{2.1}$$

と分解される. 各集合の元の個数の漸近的評価を, いわゆる素イデアル定理と代数体の知識を用いて求めることになる. まず, $j \ge l$ のとき,

$$p \equiv 1 \pmod{q^j},\ q^l \mid I_a(p) \Leftrightarrow p \text{ は } \mathbf{Q}(\zeta_{q^j}, a^{1/q^l}) \text{ で完全分解}$$

が知られている (例えば [7] 参照). さらに, $(\frac{b}{p}) = 1$ と p が $\mathbf{Q}(\sqrt{b})$ で完全分解することが同値だから, 結局

$$p \equiv 1 \pmod{q^j},\ q^l \mid I_a(p),\ (\tfrac{b}{p}) = 1 \Leftrightarrow p \text{ は } K_{j,l} := \mathbf{Q}(\zeta_{q^j}, a^{1/q^l}, \sqrt{b}) \text{ で完全分解}$$

となる. さらに素イデアル定理は次のように述べられる (この形のものは [9] にある):

定 理 2.1 (素イデアル定理) K を $\mathbf{Q}$ の有限次 Galois 拡大体, $n=[K:\mathbf{Q}]$, Δ を K の判別式とする. 条件 $\exp(10n(\log|\Delta|)^2)\le x$ のもとで次が成り立つ:

$$\begin{aligned}\pi_K(x)&=\#\{\mathfrak{p}:\ K\text{ の素イデアル};\ N\mathfrak{p}\le x\}\\&=\operatorname{li}x+O\left(\operatorname{li}(x^{\beta_0})+x\exp\left(-c_1\sqrt{\frac{\log x}{n}}\right)\right),\end{aligned}$$

ただし $\beta_0\in\mathbf{R}$,

$$\left(\frac{1}{2}<\right)\beta_0<\max\left\{1-\frac{1}{4\log|\Delta|},\ 1-\frac{1}{c_2|\Delta|^{1/n}}\right\},$$

$c_1,\ c_2>0$ で, O の含む定数は $n,\ \Delta$ によらない.

素数 p が $\mathbf{Q}$ の Galois 拡大体 K で完全分解するということは, p の上に K の素イデアルがちょうど $[K:\mathbf{Q}]$ 個あるということだから, 素イデアルの個数の評価から逆にそのような素数 p の個数が評価できるわけである (x 以下のところには $\pi_K(x)/[K:\mathbf{Q}]$ 個ということになる).

これらを用いて (2.1) 右辺各項を評価し, 少々複雑な剰余項の処理を経ると, 次の式が得られる:

$$\begin{aligned}\#S_{a,b}(x;q,0)=&\left(\frac{1}{[\mathbf{Q}(\zeta_q,\sqrt{b}):\mathbf{Q}]}-\sum_{j\ge1}\frac{1}{[K_{j,j}:\mathbf{Q}]}+\sum_{j\ge1}\frac{1}{[K_{j+1,j}:\mathbf{Q}]}\right)\operatorname{li}x\\&+O\left(\frac{x}{\log x\log\log x}\right).\end{aligned}\tag{2.2}$$

拡大次数については

$$[K_{j,l}:\mathbf{Q}]=\begin{cases}q^l\varphi(q^j)=(q-1)q^{j+l-1}, & b=q,\ q\equiv1\pmod4\text{ のとき},\\ 2q^l\varphi(q^j)=2(q-1)q^{j+l-1}, & \text{その他のとき}.\end{cases}\tag{2.3}$$

これを用いて (2.2) 式 $\operatorname{li}x$ の係数を計算すると目的の密度が得られ, 定理 1.2 の証明が終わる.

注 意. (2.2) 式における密度計算には (2.3) 式第 1 の場合は不要だが, これを用いて計算しても $b=q,\ q\equiv1\pmod4$ の場合の密度 0 が出ることはもちろんである.

3 数値実験について

本節では数値実験の結果, その意義などについて述べる. ここで

$$S_{a,b}(x;q,0)=\left\{p\le x\ ;\ q|D_a(p),\ \left(\frac{b}{p}\right)=1\right\}$$

を思い出そう. 以下の表は $\#S_{a,b}(x;q)/\pi(x)$, すなわち x 以下の素数の中で $S_{a,b}(x;q)$ が占める密度を $x=10^4$ から $x=10^9$ までの範囲で計算機実験により求めたものである. なお, $x=10^9$ までのところには素数が 50847534 個存在する.

まず表 1 は定理 1.2 に対応する場合である. 理論値は, $q=3$ の場合が $3/16=0.1875$, $q=5$ の場合が $5/48\approx 0.104167$ である.

続いて表 2 には定理 1.3, すなわち $q=2$ に対応する数値例を示す. $(a,b)=(2,2)$ は 2 が関係する特殊な場合で, この場合の理論値は $5/24\approx 0.208333$, $(a,b)=(10,3)$ は確率的推論通りになる標準的な場合で理論値は $1/3$, $(a,b)=(3,3),(6,6)$ は大量の移動がある場合で理論値は $1/6$ である. いずれも比較的よく一致していることがわかる.

x	$(a,b,q)=(3,2,3)$	$(a,b,q)=(3,3,3)$	$(a,b)=(3,2,5)$	$(a,b)=(5,3,5)$
10^4	0.190709	0.191524	0.101874	0.106036
10^5	0.188843	0.186340	0.104484	0.105016
10^6	0.187653	0.186914	0.104859	0.103306
10^7	0.187309	0.187179	0.104102	0.104101
10^8	0.187495	0.187469	0.104165	0.104099
10^9	0.187474	0.187481	0.104168	0.104185

表 1

x	$(a,b)=(2,2)$	$(a,b)=(10,3)$	$(a,b)=(3,3)$	$(a,b)=(6,6)$
10^4	0.206026	0.331158	0.164629	0.162999
10^5	0.207069	0.332256	0.164234	0.165693
10^6	0.207320	0.332798	0.165856	0.166187
10^7	0.208054	0.333408	0.166599	0.166288
10^8	0.208284	0.333218	0.166595	0.166656
10^9	0.208309	0.333338	0.166652	0.166658

表 2

さて, 本稿で考察している問題は, 広い意味での素数分布論の問題と言える. つまり, 素数自体の分布を調べているわけではないが, ある性質をみたす素数がどの程度分布しているか, という問題である. こうした問題においては, 数値実験によって傾向をつかみ, 結果を予想して理論的計算の指針とする, ということがよく行なわれる. 証明自体に計算機を用いるのとは雰囲気が違うが, これも整数論研究への計算機活用の一つである (実際, 理論的結果と数値実験の結果を照合することは最良の検算方法である !).

こうした問題における数値実験の大きな特徴は, まず主に扱うべき対象が有理整数, しかも自然数である, ということ, そして, 扱うべき整数の桁数はそれほど大きくないが, 扱うべきデータ量が多いことである. 実際, 2, 3, 5, 7, 11, 13, $\cdots$ といった具合に, 最初から順次もれなく素数を調べていく必要があるのである.

このような目的のためには, C 言語は比較的適しているように思われる. それは, 自前で書かなければならない関数がそれほど多くなく, 一般的に計算速度が稼げる, というのが理由である.

表 1, 2 の数値例も C 言語によるものである. 以下, アルゴリズムの概略を述べる. まず 10^9 までの素数表のファイルを準備する. これはエラトステネスの篩によれば非常に速い. 次に中心となる部分は剰余位数 $D_a(p)$ の計算であるが, $D_a(p)$ は $p-1$ の約数であるということ以外, 有効な判定法 (特徴づけ) はないと思われる. そこで $p-1$ を素因数分解し, $p-1$ の約数を小さい順に調べて行って $D_a(p)$ になるかどうか判定する, という方法を採った. この部分の計算に最初に作っておいた素数表のファイルを利用する. 結果は 1 つのファイルにまとめておき, 条件 $q|D_a(p)$, $(\frac{b}{p})=1$ の検証に使用する. 高速化の工夫として, $p-1$ の最大の素因数と 2 番目に大きい素因数を記録したファイルを別に作っておき, 素因数分解に利用している (このアイデアは C. Pomerance に教わった). a を取り替えるごとにあらためてプログラムを動かさなければならないから, この部分の高速化は効果的である. また, Legendre 記号のアルゴリズムは種々の書物に紹介されているが, ここでは木田 · 牧野 [8, p. 97] のものを参考にし, C 言語で実装した.

計算機環境は, OS が Windows7 (64bit), RAM は 4.0GB, CPU は Intel Core i5-2520M (2.5GHz), コンパイラー は GCC 4.5.2 (MinGW) である. また使用している機械はノート型である. 要した時間は, 10^9 までの素数 50847534 個に対し, $D_a(p)$ の計算に約 3 時間 10 分 (これは a によって異なるが, a が大きいほど実行時間が短くなる傾向が観察される), Legendre 記号の計算に約 20 秒程度, 条件 $q|D_a(p)$, $(\frac{b}{p})=1$ の検証も約 20 秒程度であった. なお, 異なる a に対する $D_a(p)$ 計算のプログラムを 2 個同時に実行しても計算時間はあまり変わらず 3 時間程度で終わったので, 複数のコアによる並列計算がうまく行なわれているようである. その意味では 1 つの a につき 1 時間半程度で計算できていることになる.

Submitted on February 19, 2012.

参考文献

[1] K. Chinen, L. Murata: On a distribution property of the residual order of a (mod p), J. Number Theory **105** (2004), 60-81.

[2] _____ : On a distribution property of the residual order of a (mod p) — III, J. Math. Soc. Japan **58-3** (2006), 693-720.

[3] _____ : On a distribution property of the residual order of a (mod p) — IV, in *Number Theory: Tradition and Modernization*, W. Zhang and Y. Tanigawa, eds., Developments in Math. **15**, 11-22, Springer Verlag, 2006.

[4] K. Chinen, C. Tamura: On a distribution property of the residual order of a (mod p) with a quadratic residue condition, to appear in Tokyo J. Math.

[5] H. Hasse: Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von durch eine vorgegebene Primzahl $l \neq 2$ teilbarer bzw. unteibarer Ordnung mod p ist, Math. Ann. **162** (1965), 74-76.

[6] H. Hasse: Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von gerader bzw. ungerader Ordnung mod p ist, Math. Ann. **166** (1966), 19-23.

[7] C. Hooley: On Artin's conjecture, J. Reine Angew. Math. **225** (1967), 209-220.

[8] 木田 祐司, 牧野 潔夫: UBASIC によるコンピュータ整数論, 日本評論社, 1994.

[9] J. C. Lagarias, A. M. Odlyzko: Effective versions of the Chebotarev density theorem, in: Algebraic Number Fields (Durham, 1975), Academic Press, London, 1977, pp.409-464.

[10] L. Murata, K. Chinen: On a distribution property of the residual order of $a \pmod p$, II, J. Number Theory **105** (2004), 82-100.

[11] R. W. K. Odoni: A conjecture of Krishnamurthy on decimal periods and some allied problems, J. Number Theory **13** (1981), 303-319.

[12] W. Sierpinski: Sur une décomposition des nombre premiers en deux classes, Collect. Math. **10** (1958), 81-83.

On the Structure of Unramified Galois Extensions of Cyclic Extensions of Number Fields

Ken Yamamura

National Defense Academy

Main Th. K/F : **a cyclic ext. of num. fds of deg.** n

P : **a fin. simple gp. with** $(n, |P|) = 1$

and moreover with $(n, |\mathrm{Out}\, P|) = 1$ **if** P **is nonabel.**

Assume $\forall\ E$ **with** $F \subsetneqq E \subsetneqq K$ **has no unram.** P**-ext.**

If K **has an unram.** P**-ext.** L**, then** $\mathrm{Gal}(\widetilde{L}/K) \cong P^m$ **with**

$$m = \begin{cases} \mathrm{ord}(p \bmod n)(:= f) & \text{if } P \cong C_p \\ n & \text{otherwise,} \end{cases}$$

where $\widetilde{L}$ **is the normal cl. of** L **over** F**.**

Hence if K **has an unram.** P^r**-ext. normal over** F**, then the above** $m \mid r$**.**

Implication.

The abel. cases ($P \cong C_p$).

(By slight modif., we can replace $P = C_p$ by C_{p^a}.)

$n = 2$**:** $m = f = 1$**; the normality of unram. abel. exts.** M **of quad. exts.** K **of** F **of degs. prime to** $h(F)$**.**

(odd deg. cases. valid for even deg. if $2 \nmid h(F)$**.)**

$$\mathrm{Gal}(M/F) \cong \mathrm{Gal}(M/K) \rtimes \mathrm{Gal}(K/F) \quad \textbf{(gen. dihedral)}$$

Rem. If $2 \mid h(F)$**, then** F **has a quad. ext. that has an unram. quad. ext. nonnormal over** F**. (Madden-Vélez)**

$n \geqq 3$: str. thm. (rank thm.) on p-class groups (Masley)

$$f := \mathrm{ord}(p \bmod n) \mid (p^a\text{-rank of } \mathrm{Cl}^{(p)}(K))$$

From this we have

$$p \mid h(K) \Longrightarrow p^f \mid h(K)$$

$$h(K) \leqq [K_{\mathrm{ur}} : K] < p^f \Longrightarrow p \nmid h(K)$$

These were used to determine class numbers or class groups of real or cyclotomic fields of small conductors.

The nonabel. cases ($(n, |\mathrm{Out}\, P|) = 1$).

$$K \textbf{ has an unram. } P\textbf{-ext.} \Longrightarrow |P|^n \mid [K_{\mathrm{ur}} : K]$$

$$[K_{\mathrm{ur}} : K] < |P|^n \Longrightarrow K \textbf{ has no unram. } P\textbf{-ext.}$$

We apply this to some layers of (cyclo.) $\mathbb{Z}_l$-exts. of $\mathbb{Q}$.

Rem. For almost all fin. nonabel. simple gps P, $|\mathrm{Out}\, P|$ are very small. In fact, $\mathrm{Out}\, A_n \cong C_2$ if $n \geqq 5$ and $n \neq 6$ and $\mathrm{Out}\, A_6 \cong V_4$; $|\mathrm{Out}\, P| \leqq 2$ for all sporadic groups P; $\mathrm{Out}\,(\mathrm{L}_2(p)) \cong C_2$ if $p \geqq 5$. (For these groups, $(n, |P|) = 1$ implies $(n, |\mathrm{Out}\, P|) = 1$ since $2 \mid |P|$ (Feit-Thompson).)

$K_n^{(l)}$ **: the** n **th layer of (cyclo.)** $\mathbb{Z}_l$**-ext. of** $\mathbb{Q}$**.**

Under GRH, $K_1^{(13)}$ **has no unram. nonsolv. Gal. ext.**

Combined with other results, we have the following.

Th. Under GRH, $(K_n^{(l)})_{\mathrm{ur}} = K_n^{(l)}$ **for the following** (l, n)**:**

$l = 2$, $1 \leqq n \leqq 6$; $l = 3$, $1 \leqq n \leqq 4$; $l = 5$, $n = 1, 2$;

$7 \leqq l \leqq 13$, $n = 1$.

Coates' conj. $h(K_n^{(l)}) = 1$ **for any** l **and** n**.** ($n = 2$**: Weber's)**

Conj. For all but fin. many pairs (l, n)**,** $h(\mathbb{Q}(\zeta_{l^{n+1}})_+) = h(\mathbb{Q}(\zeta_{l^n})_+)$.

Th. Under GRH, for any fin. nonabel. simple gp. P with $|P| > 3.53 \quad 10^{13}$ or $17 \nmid |P|$, $K_1^{(17)}$ does not have an unram. P-ext.

$[(K_1^{(17)})_{\mathrm{ur}} : K_1^{(17)}] \leqq 3.52\cdots \quad 10^{13} \longleftarrow$ **Odlyzko's disc. bd.**

For any P with $|P| \leqq 3.53 \quad 10^{13}$, we have $17 \nmid |\mathrm{Out}\, P|$.

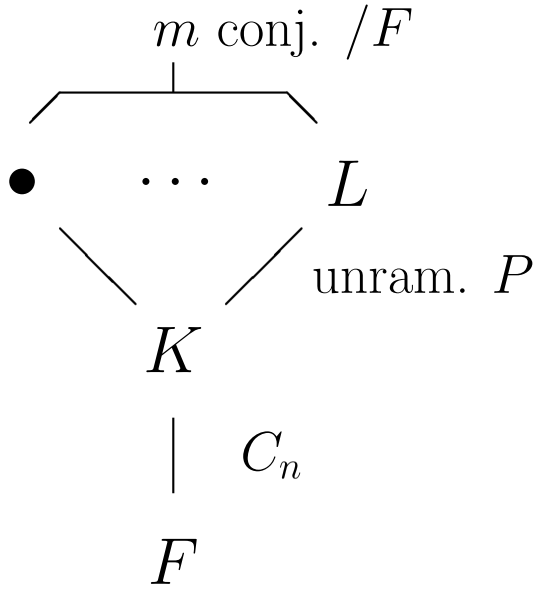
# of such P is 4526, and 565 satisfy $|P| \equiv 0 \bmod 17$.

$\dfrac{565}{4526} = 0.12453 \doteqdot \dfrac{1}{8} = \dfrac{2}{\varphi(17)}$**, the probab. for** $17 \mid \mathrm{L}_2(p)$

The p-class group of the $\mathbb{Z}_{17}$-ext. of $\mathbb{Q}$ is trivial if p is a prim. root modulo 17 (K. Horie and M. Horie).

AC2011

108



Assumption: $\forall\ E$ **with** $F \subsetneqq E \subsetneqq K$ **has no unram.** P**-ext.**

$$\Longrightarrow m = \begin{cases} \mathrm{ord}(p \bmod n) & \textbf{if } P \cong C_p \\ n & \textbf{otherwise} \end{cases}$$

Sketch of proof of Main Th.

$\mathrm{Gal}(K/F)(\cong C_n) \curvearrowright \mathrm{Gal}(\widetilde{L}/K)(\cong P^m)$

$$\rightsquigarrow \rho\colon C_n \to \mathrm{Out}\, P^m \cong \begin{cases} \mathrm{GL}(m,p) & \textbf{if } P \cong C_p \\ (\mathrm{Out}\, P) \wr S_m & \textbf{otherwise} \end{cases}$$

Assump. $\Longrightarrow$ ρ **inj.,** $\rho(C_n)$ **irred. (or** $\rho(C_n) \hookrightarrow S_m$ **prim.)**

$(P \cong C_p) \quad \Longrightarrow \rho(C_n) \leqslant$ (**Singer subgp. of** $\mathrm{GL}(m,p)) \cong \mathbb{F}_{p^m}$

$$\Longrightarrow p^m \equiv 1 \bmod n \Longrightarrow m = \mathrm{ord}(p \bmod n).$$

$\rho(C_2) = \langle -I \rangle \Longrightarrow m = 1$, $\mathrm{Gal}(\widetilde{L}/K)$ **gen. dihed.**

$(P$ **nonabel.)** $\Longrightarrow \rho(C_n) \to \langle n$**-cycle**$\rangle \Longrightarrow m = n$ □

Also for gen. G-exts. K/F, by considering gp. hohmom.

$$\rho\colon G \to \begin{cases} \mathrm{GL}(m,p) \\ (\mathrm{Out}\, P) \wr S_m \end{cases}$$

we obtain useful information on unram. Galois exts. of K. For example, if G is nonabel. simple and $P \cong C_p$, then ρ induces an inj. hom. $G \to \mathrm{PSL}(m,p)$ when $p \mid h(K)$, which implies (an improvement of) Ohta's result: $m > 1$ and $(p^m - 1)(p^{m-1} - 1) \cdots (p-1) \equiv 0 \bmod |G|$.