Association schemes of prime order and their splitting fields

Akihide Hanaki

Shinshu University
hanaki@math.shinshu-u.ac.jp

1 はじめに

素数位数アソシエーション・スキームの構造について 2004 年秋頃に大阪教育大学の宇野勝博氏との共同研究で以下の結果を得た。

Theorem 1.1. [11] 素数位数アソシエーション・スキームは可換である。更にその最小分解体がアーベル体であるならばそれはシュアー的スキームと代数的に同型である。

この結果の後半部分において「最小分解体がアーベル体であるならば」という仮定があるが、この仮定が成り立たないような例は知られていない。より一般に坂内–伊藤 [2, p. 123] には (表現の仕方は違うが)「可換スキームの最小分解体はアーベル体か」という問題があり、これも未解決である。ここでは素数位数アソシエーション・スキームの最小分解体の構造について分かっていることを紹介する。結果としてアーベル体であることが分かれば Theorem 1.1 の精密化が得られ、そうでなければ坂内–伊藤の問題に対する反例が構成される。

講演は数論の研究者を強く意識して行った。それは数論の立場からの御意見を聞かせて頂き、そして解決への協力をお願いしたかったからである。数名の方からは既に貴重な話など聞かせて頂いたが、まだ解決には至らない。この報告についても組合せ論的な議論は詳しくは書かない。必要ならば引用文献などを見て欲しい。

2 定義と基本的な性質、問題の背景

記号などは主に Zieschang [15], [16]、または坂内–伊藤 [2] と同じものをを用いる。

2.1 アソシエーション・スキーム

X を有限集合とする。$X \times X$ の部分集合 g を X 上の**関係** (relation) という。関係 g の**隣接行列** (adjacency matrix) を σ_g で表す。すなわち σ_g は、行、列共に X で添字付けられた行列で、その (x, y)-成分は $(x, y) \in g$ のとき 1、そうでないときに 0 として定められたものである。S を空でないいくつかの X 上の関係の集合とし、次の条件を満たすものとする。

(1) S は $X \times X$ の分割である。

(2) $1 := \{(x,x) \mid x \in X\} \in S$ である。(σ_1 は単位行列になる。)

(3) $g \in S$ ならば $g^* := \{(y,x) \mid (x,y) \in g\} \in S$ である。(σ_{g^*} は σ_g の転置行列になる。)

(4) $\mathbb{Z}S := \bigoplus_{g \in S} \mathbb{Z}\sigma_g$ は環をなす。

このとき (X,S) を**アソシエーション・スキーム** (association scheme)、または**スキーム**という。$|X|$ を (X,S) の**位数** (order)、$d = |S| - 1$ を (X,S) の**クラス** (class) という。$g \in S$ に対して σ_g は各行、各列に同じ数の 1 を含む。この数を g の **valency** といい n_g と書く。

環 $\mathbb{Z}S$ が可換環であるとき (X,S) は**可換**であるという。

Example 2.1 (シュアー的スキーム). X を有限集合とし G を X 上可移な置換群とする。G をそれぞれの成分へ作用させることによって $X \times X$ 上の置換群と見る。このときの軌道の集合を S とすると (X,S) はスキームとなる。このようにして得られるスキームを**シュアー的スキーム** (Schurian scheme) という。

特に X として G 自身をとることを考えれば、アソシエーション・スキームは有限群の概念の拡張であると考えられる。

シュアー的な

Example 2.2 (サイクロトミック・スキーム $Cyc(5,2)$). 位数が素数であるアソシエーション・スキームは分類されていて、**サイクロトミック・スキーム** (cyclotomic scheme) と呼ばれるものと同型になる [4, p. 66]。サイクロトミック・スキームは位数 p とクラス d で一意に定まり、それを $Cyc(p,d)$ と書くことにする。(一般に有限体上で定義されるため、素数べき位数のものが定義されるが、ここでは素数位数のもののみ考える。)

具体例 $Cyc(5,2)$ を以下に示す。

$$\sigma_1 = \begin{pmatrix} 1&0&0&0&0 \\ 0&1&0&0&0 \\ 0&0&1&0&0 \\ 0&0&0&1&0 \\ 0&0&0&0&1 \end{pmatrix}, \sigma_f = \begin{pmatrix} 0&1&0&0&1 \\ 1&0&1&0&0 \\ 0&1&0&1&0 \\ 0&0&1&0&1 \\ 1&0&0&1&0 \end{pmatrix}, \sigma_g = \begin{pmatrix} 0&0&1&1&0 \\ 0&0&0&1&1 \\ 1&0&0&0&1 \\ 1&1&0&0&0 \\ 0&1&1&0&0 \end{pmatrix}$$

とすれば $S = \{1, f, g\}$ はアソシエーション・スキームとなる。これは位数 5 の巡回群の正則置換表現を考え、位数 $2 = (p-1)/d$ の自己同型による軌道で和をとったものである。一般に $Cyc(p,d)$ はこのようにして得られる。

2.2 指標

定義より $\mathbb{Z}S = \bigoplus_{g \in S} \mathbb{Z}\sigma_g$ は環をなす。R を単位元を持つ可換環とするとき、係数環を取り換えて

$$RS := R \otimes_{\mathbb{Z}} \mathbb{Z}S$$

とおき、これを S の R 上の**隣接代数** (adjacency algebra) という。R として標数 0 の体をとると、隣接代数 RS は分離的であることが知られている [15, Theorem 4.1.3]。よって

半単純でもある。係数体として複素数体 $\mathbb{C}$ を考える。Wedderburn の定理 [5, Theorem 2.4.3] により $\mathbb{C}S$ は

$$\mathbb{C}S \cong M_{n_1}(\mathbb{C}) \oplus \cdots \oplus M_{n_r}(\mathbb{C})$$

と全行列環の直和に書ける。このとき各直和成分への射影が代数 $\mathbb{C}S$ の既約表現の同値類の代表系となる。表現のトレースを**指標** (character) という。表現が既約であるとき、その指標も既約であるという。$\mathbb{C}S$ の既約指標全体の集合を $\mathrm{Irr}(S)$ という記号で表す。

$\mathrm{Irr}(S)$ と S で添字付けられた表で $\chi(\sigma_g)$ ($\chi \in \mathrm{Irr}(S)$, $g \in S$) を成分とするものを (X, S) の**指標表** (character table) という。指標表を行列と見る場合もある。可換スキームの指標表は正方行列になる。

Example 2.3 (サイクロトミック・スキームの指標表). $Cyc(5, 2)$ の指標表は以下の通りである。ただし ζ は 1 の原始 5 乗根とする。

	σ_1	σ_f	σ_g
χ_1	1	2	2
χ_2	1	$\zeta + \zeta^4$	$\zeta^2 + \zeta^3$
χ_3	1	$\zeta^2 + \zeta^3$	$\zeta + \zeta^4$

一般に $Cyc(p, d)$ の指標の値は、上の例のように 1 の p 乗根 ζ の p 分体 $\mathbb{Q}(\zeta)$ のある部分体へのトレースによって得られる。

$\sigma_g \mapsto n_g$ (n_g は g の valency) は $\mathbb{C}S$ の 1 次の表現、かつ指標である。これを S の**自明な表現、指標**といい 1_S で表す。S の自明でない既約指標全体の集合を $\mathrm{Irr}^*(S)$ と書くことにする。

$\mathbb{C}S$ は行列環として定義されているので、そのままで表現を与えている。これを S の**標準表現**といい、その指標を**標準指標**という。標準指標における既約指標 χ の重複度を単に χ の**重複度** (multiplicity) といい m_χ で表す。自明な指標 1_G の重複度は 1 である。$\sum_{\chi \in \mathrm{Irr}(S)} m_\chi \chi(1) = |X|$, $\sum_{\chi \in \mathrm{Irr}(S)} \chi(1)^2 = |S|$ である。また S が可換ならば、任意の $\chi \in \mathrm{Irr}(S)$ に対して $\chi(1) = 1$ なので $\sum_{\chi \in \mathrm{Irr}(S)} m_\chi = |X|$ である。

有理数体 $\mathbb{Q}$ 上の隣接代数 $\mathbb{Q}S$ の分解体を (X, S) の**分解体** (splitting field) という。可換スキーム (X, S) に対しては、体 K が分解体であることと K がすべての指標の値 $\chi(\sigma_g)$ ($\chi \in \mathrm{Irr}(S)$, $g \in S$) を含むことは同値である。特に $K = \mathbb{Q}(\chi(\sigma_g) \mid \chi \in \mathrm{Irr}(S), g \in S)$ は最小分解体となる。

$\chi \in \mathrm{Irr}(S)$ と分解体 K の自己同型 τ に対して χ^τ を $\chi^\tau(\sigma_g) = \chi(\sigma_g)^\tau$ で定めれば $\chi^\tau \in \mathrm{Irr}(S)$ である。したがって最小分解体は $\mathbb{Q}$ の正規拡大である。代数的共役な二つの既約指標の重複度は等しい。

Example 2.4 (サイクロトミック・スキームの分解体). $Cyc(p, d)$ の最小分解体は p 分体の部分体で $\mathbb{Q}$ 上の次元が d であるものとして定まる。したがってそれはアーベル体である。

1 節で述べたように「任意の可換スキームの最小分解体はアーベル体か」という問題があるが未解決である。この問題に関しては宗政 [14] が知られている。

2.3 同型と代数的同型

アソシエーション・スキーム (X, S) と (X', S') が**同型** (isomorphic) であるとは、全単射 $\varphi : X \to X'$ と $\psi : S \to S'$ が存在して、$(x, y) \in g$ と $(\varphi(x), \varphi(y)) \in \psi(g)$ が同値となることである。このとき二つのスキームは組合せ構造まで完全に一致していると言える。

一方、二つのスキームの隣接代数が基底の対応を込めて同型になっているとき、それらは**代数的に同型** (algebraically isomorphic) であるという。すなわち p^h_{fg} で構造定数を表す ($\sigma_f\sigma_g = \sum_{h\in S} p^h_{fg}\sigma_h$ とする) とき、全単射 $\psi : S \to S'$ が存在して

$$p^{\psi(h)}_{\psi(f)\psi(g)} = p^h_{fg}$$

となることである。同型ならば代数的に同型であるが、一般に逆は成り立たない。

二つの可換スキームに対しては、代数的に同型であることと、その指標表が適当な行と列の並べ替えで一致することは同値である [2, Theorem II.3.6 (ii)]。

2.4 Frame 数

アソシエーション・スキーム (X, S) に対して

$$\mathcal{F}(S) := |X|^{|S|}\frac{\prod_{g\in S} n_g}{\prod_{\chi\in \mathrm{Irr}(S)} m_\chi^{(\chi(1)^2)}}$$

とおいて、これを (X, S) の **Frame 数** (Frame number) という ([1], [6], [8], [12])。Frame 数は有理整数である。体 K 上の隣接代数 KS が半単純であることと、K の標数が $\mathcal{F}(S)$ を割り切らないことは同値である [8]。

S を可換とする。このとき $\mathcal{F}(S)$ は有理整数環 $\mathbb{Z}$ 上の隣接代数 $\mathbb{Z}S$ の判別式の絶対値に等しいことが知られている。また指標表を行列と見て P と書くと $(\det P)\overline{(\det P)} = \mathcal{F}(S)$ である [2, p. 74]。

2.5 問題の背景

Theorem 1.1 の背景には次の大きな問題がある。

Problem 2.5. すべての原始的な可換スキームを分類せよ。

九州大学の坂内英一氏はこの問題を通して有限単純群の分類を見直したいという夢 (?) を持っているそうであるが、この問題については解決の糸口さえも得られていないように思われる。

Problem 2.6. すべての素数位数スキームを分類せよ。

素数位数スキームは原始的であるので、これは Problem 2.5 の極めて特殊な場合である。また有限群に例えるならば素数位数巡回群に相当するといえる。しかしながらこの問題でさえも、完全な解決は望みがないように思われる。$p \le 29$ は計算機によって分類が済んでいる [10] が、$p = 31$ には極めて多くの同型類があることが分かっていて、

その分類は終わっていない。これは $p = 31$ が特別であるということではなく、これより大きなすべての素数について、その分類は困難であると思われている。しかしながらこれまでに知られている素数位数スキームのすべての例はサイクロトミック・スキームと代数的に同型である。これによって次の弱い問題が得られる。

Problem 2.7. 素数位数スキームの代数的な同型類を分類せよ。特にそれはサイクロトミック・スキームと代数的に同型なものに限るかを考察せよ。

これが今回の話の動機であり Theorem 1.1 はこれに対する部分的な解を与えるものである。分解体の構造を考えることはこの問題の完全解決への有効な手段であると考えている。

3 素数位数アソシエーション・スキームの分解体の構造

3.1 一般的な考察

この節を通して (X, S) を素数位数アソシエーション・スキームとし $|X| = p$, $|S| = d+1$ とする。Theorem 1.1 は証明せずに仮定する。したがって (X, S) は可換である。また $p = 2$ のときは自明なので p は奇素数と仮定する。Theorem 1.1 の証明の重要な部分は [9] の結果を用いて [3] のある部分とほぼ同様に得られ、以下の様に一般化される。

Proposition 3.1. K を (X, S) の分解体で $\mathbb{Q}$ 上正規拡大であるものとする。また K' を K の部分体で、$p\mathbb{Z}$ 上のある素イデアルが $K'/\mathbb{Q}$ で分岐しないものとする *(p は $K'/\mathbb{Q}$ で分岐してもよい)*。このとき $Gal(K/K')$ は $\mathrm{Irr}^*(S)$ に可移に作用する。したがって d は $p-1$ を割り切り、自明でない既約指標の重複度はすべて等しく $(p-1)/d$ である。

これによって任意の $1 \neq g \in S$ に対して、その valency も $(p-1)/d$ であることが分かる。以下 $k = (p-1)/d$ とおく。自明でない重複度と valency がすべて k であり、かつ S が可換であることにより Frame 数は

$$\mathcal{F}(S) = p^{d+1}$$

となる。

以下 K を (X, S) の最小分解体とする。すなわち $K = \mathbb{Q}(\chi(\sigma_g) \mid \chi \in \mathrm{Irr}(S), g \in S)$ である。またガロア群 $Gal(K/\mathbb{Q})$ を G と書く。$K' = \mathbb{Q}$ として Porposition 3.1 を適用すれば G は $\mathrm{Irr}^*(S)$ に可移に作用する。また $\rho \in G$ がすべての既約指標を固定すれば K のすべての元を固定するので G は対称群 $\mathrm{Sym}(\mathrm{Irr}^*(S)) \cong \mathrm{Sym}(d)$ の部分群に同型であり、したがって p'-群である。$\mathfrak{P}$ を $p\mathbb{Z}$ 上にある K の素イデアルとし、その惰性群を T とする。Hilbert の分岐群に関する理論により T は巡回群となる [17, 定理 3.2.14]。$\mathfrak{P}$ の下にある K_T の素イデアルは分岐しないから Proposition 3.1 によって T は $\mathrm{Irr}^*(S)$ に可移に作用する。

$\chi \in \mathrm{Irr}^*(S)$ を一つ固定し G における χ の固定部分群を H とする。T が可移で H が一点の固定部分群だから $G = HT$ である。$\rho \in H \cap T$ とする。任意の $\varphi \in \mathrm{Irr}\ *(S)$ に対して、ある $\tau \in T$ があって $\varphi = \chi^\tau$ である。T が巡回群であるから

$$\varphi^\rho = \chi^{\tau\rho} = \chi^{\rho\tau} = \chi^\tau = \varphi$$

となり、したがって $\rho = 1$ である。

T は一つの素イデアルの惰性群だから、その共役をとっても上と同様の議論が成り立つ。以上より次を得る。

Proposition 3.2. 任意の $\rho \in G$ について次が成り立つ。

(1) $G = HT^\rho$

(2) $H \cap T^\rho = 1$

(3) $d = |G : H| = |T|$

(4) T^ρ は $\mathrm{Sym}(d)$ の部分群として、長さ d の巡回置換で生成される巡回群である。

Z を $\mathfrak{P}$ の分解群とする。$p\mathbb{Z}$ の上にある K_H の素イデアルと G の (H, Z) による両側剰余類のと間には一対一の対応がある [17, 定理 3.2.10]。$Z \supset T$ なので $G = HT = HZ$ となり、よって $p\mathbb{Z}$ の上にある K_H の素イデアルは唯一つである。それを $\mathfrak{p}$ とおく。

拡大 K/K_H における $\mathfrak{P}$ の惰性群は $T \cap H = 1$ である [17, 定理 3.2.6]。よって $\mathfrak{p}$ は K/K_H で分岐せず、$\mathfrak{P}$ の $K/\mathbb{Q}$ における分岐指数が d であることにより $p\mathcal{O}_{K_H} = \mathfrak{p}^d$ である。ここで $\mathcal{O}_{K_H}$ は K_H の整数環とする。よって Dedekind の判別定理 [17, 定理 3.5.4] より K_H の判別式 $d(K_H)$ の p-部分は p^{d-1} である。

判別式 $d(K_H)$ を決定しよう。まず $\{\chi(\sigma_g) \mid g \in S \setminus \{1\}\}$ は $\mathbb{Q}$ 上一次独立であることが指標表を考えることによって分かる。次に隣接代数 $\mathbb{Q}S$ の分解を考えれば、S の可換性よりそれは体の直和に同型で、直和因子は $\mathrm{Irr}(S)$ の代数的共役類に対応する。ガロア群が $\mathrm{Irr}^*(S)$ に可移に作用していることから $\mathbb{Q}S \cong \mathbb{Q} \oplus F$ と書けて $\dim_{\mathbb{Q}} F = d$ である。ここで F の $\mathbb{C}$ への埋め込みを適当に固定して射影 $\mathbb{Q}S \to F$ から $\mathbb{Q}S \to \mathbb{C}$ を作れば、これは自明でない既約表現を与える。したがってこれを χ であると仮定しても構わない。これにより

$$F \cong \mathbb{Q}(\chi(\sigma_g) \mid g \in S) = K_H$$

であることが分かる。直和分解

$$\mathbb{Q}S \cong \mathbb{Q} \oplus K_H$$

において $\mathbb{Z}S$ を考えれば、それは $\mathbb{Z} \oplus \mathcal{O}_{K_H}$ に埋め込まれる。$|d(\mathbb{Z}S)| = \mathcal{F}(S) = p^{d+1}$ であるから $|d(K_H)|$ はその約数で p べきとなる。これまでの議論から $|d(K_H)| = p^{d-1}$ であり、p は奇素数と仮定しているので Stickelberger の定理 [17, 定理 2.2.1] により、その符号も $d(K_H) \equiv 1 \pmod 4$ で定まる。

以上をまとめて次を得る。

Proposition 3.3. (1) $p\mathcal{O}_{K_H} = \mathfrak{p}^d$ である。

(2) $|d(K_H)| = p^{d-1}$ であり、符号は $d(K_H) \equiv 1 \pmod 4$ で定まる。

(3) K/K_H は不分岐拡大である。

最も示したいことは G がアーベル群になることである。そこで、このための同値な条件をまとめておく。

Proposition 3.4. 上記の記号の下で以下は同値である。

(1) G はアーベル群。

(2) $H = 1$

(3) $H \lhd G$

(4) $T = G$

(5) $T \lhd G$

Proof. K は K_H を含む最小の正規拡大であることに注意する。(1) を仮定すると (2), (3), (4), (5) が成り立つことは明らかである。また (2), (3), (4) の一つが成り立てば (1) が成り立つこともこれまでの議論から明らかである。(5) を仮定する。このとき $p\mathbb{Z}$ の上にある K の任意の素イデアルの惰性群は T となり、よって $K_T/\mathbb{Q}$ ではすべての素数が分岐しない。Minkowski の定理 [17, 定理 2.8.8] により $T = G$ である。 □

更にいくつかの分かることをまとめておく。次の結果は、これまでの議論と指標表の行列式の $\mathfrak{P}$-進付値を注意深く計算することによって得られる。

Proposition 3.5. ある $g \in S$ が存在して $\chi(\sigma_g) - k$ は次数 d の *p-Eisenstein* 多項式の根になる。

スキーム (X, S) が**対称スキーム**であるとは、任意の $g \in S$ が $g^* = g$ を満たすことをいう。一般に可換スキーム (X, S) に対して、$g \cup g^*$ を関係とする対称スキームが定義される [2, p. 57]。これを (X, S) の **symmetrization** という。

Proposition 3.6. K_H は総実、または総虚である。

Proof. (X, S) が非対称な関係をもつとする。このとき、その symmetrization も素数位数スキームであるから、1 でないすべての関係が非対称である。$g \in S$ が対称ならば、任意の $\varphi \in \mathrm{Irr}(S)$ について $\varphi(\sigma_g) \in \mathbb{R}$ であり、$g \in S$ が非対称ならば、ある $\varphi \in \mathrm{Irr}(S)$ について $\varphi(\sigma_g) \notin \mathbb{R}$ である。

すべての関係が対称であるならば、すべての指標の値が実数なので K_H は総実である。

1 でないすべての関係が非対称であるとする。もし $\varphi \in \mathrm{Irr}^*(S)$, $g \neq 1$ について $\varphi(\sigma_g) \in \mathbb{R}$ ならば、ガロア群の可移性から任意の $\varphi' \in \mathrm{Irr}^*(S)$ に対して $\varphi'(\sigma_g) = \varphi'(\sigma_{g^*})$ となる。これは可換スキームの指標表が正則行列であることに反する。よって K_H は総虚である。 □

ここで考えたい問題を代数体の問題としてまとめておく。

Problem 3.7. p を有理素数、d は $p-1$ の約数とする。代数体 F は d 次の p-Eisenstein 多項式で定義されるもので、総実、または総虚であり、判別式の絶対値 $|d(F)|$ は p^{d-1} であるものとする。このとき F は $\mathbb{Q}$ のアーベル拡大に限るかを考察し、成り立たないのであれば反例を構成せよ。

このような非アーベル体が存在したとしても、それに伴う組合せ構造が存在するかどうかは別の問題である。しかしこのような体がアーベル体に限るのであれば素数位数スキームはすべてサイクロトミック・スキームと代数的に同型であるといえる。以下の節で特別な場合についての考察を行うが、そこで述べる結果は組合せ構造まで考慮したものであり、Problem 3.7 についての結果ではない。

3.2 特別な場合

ここでも (X, S) はスキームで $|X| = p$ は素数、$d = |S| - 1$、$k = (p-1)/d$ とする。p, d, k が特別な値の場合に分かることを記す。記号はこれまでと同じものを使う。

Proposition 3.8. $d \leq 3$ ならば (X, S) はサイクロトミック・スキームと代数的に同型である。

Proof. $d \leq 2$ ならば対称群がアーベル群なのでガロア群もそうである。$d = 3$ とする。p は奇素数であるので $d(K_H) = p^2$ である。よって $\sqrt{d(K_H)} \in \mathbb{Q}$ であり、$G = Gal(K/\mathbb{Q})$ は交代群 Alt(3) に含まれ [17, 補題 1.7.1]、したがってアーベル群である。 □

Theorem 1.1 と平坂 [13] を併せて次が成り立つ。

Proposition 3.9. $k \leq 3$ ならば (X, S) はサイクロトミック・スキームと同型である。また $k = 4$ で S が $g^* \neq g$ なる関係を含めば (X, S) はサイクロトミック・スキームと同型である。

次は計算機による位数の小さいスキームの分類結果 [10] などから分かる。

Proposition 3.10. $p \leq 37$ ならば (X, S) はサイクロトミック・スキームと代数的に同型である。$p \leq 37$ かつ $d \neq 2$ ならば (X, S) はサイクロトミック・スキームと同型である。

これまでに知られているサイクロトミック・スキームと同型でない素数位数スキームはすべて $d = 2$ のものであり、その最小位数は $p = 19$ である。$d \geq 3$ でサイクロトミック・スキームと同型でない素数位数スキームが存在するかどうかは分かっていない。

3.3 計算機による実験

前節の内容により、サイクロトミック・スキームと代数的に同型であることが分かっていない最小の場合は $(p, d) = (41, 4)$ の場合である。これについて計算機を用いた実験を行った。[17, 補題 2.7.1] の考え方を用いる。

まず Proposition 3.5 により $\chi(\sigma_g) - k$ がある d 次の Eisenstein 多項式の根になる。また一般に $|\varphi(\sigma_g)| \leq k$ である [16, Corollary 9.3.2]。よって $|\varphi(\sigma_g) - k| \leq 2k$ が任意の $\varphi \in \mathrm{Irr}^*(S)$ について成り立つ。したがって、その Eisenstein 多項式を

$$f(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$

とおけば $-80 \leq a_3 \leq 80$, $-2400 \leq a_2 \leq 2400$, $-32000 \leq a_1 \leq 32000$, $-160000 \leq a_0 \leq 160000$, $41^2 \nmid a_0$, $41 \mid a_0, a_1, a_2, a_3$, である。この条件を満たすすべての多項式を生成し、その判別式、ガロア群を計算することによって求める条件を満たす体は存在しないことが分かる。計算には GAP [7] を用いた。この計算にはそれなりの時間がかかっているので、このような方法でこれよりも大きい例を計算するのは現実的ではないように思われる。

4　おわりに

ここで述べた内容は、そのほとんどが素数 p に関するものである。最小分解体がアーベル体であるということを結論付けるには p 以外の素数を考える必要があると思われる。例えば q を p と異なる素数とするとき、位数 p のスキームの q 元体上での既約表現の様子は分からない。これが完全に分かれば解決への大きな手がかりになると思われる。

References

[1] Z. Arad, E. Fisman, and M. Muzychuk, *Generalized table algebras*, Israel J. Math. **114** (1999), 29–60.

[2] E. Bannai and T. Ito, *Algebraic combinatorics. I*, The Benjamin/Cummings Publishing Co. Inc., Menlo Park, CA, 1984.

[3] R. Brauer, *Investigations on group characters*, Ann. of Math. (2) **42** (1941), 936–958.

[4] A. E. Brouwer, A. M. Cohen, and A. Neumaier, *Distance-regular graphs*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 18, Springer-Verlag, Berlin, 1989.

[5] Yu. A. Drozd and V. V. Kirichenko, *Finite-dimensional algebras*, Springer-Verlag, Berlin, 1994.

[6] J. S. Frame, *The double cosets of a finite group*, Bull. Amer. Math. Soc. **47** (1941), 458–467.

[7] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4*, 2005, (`http://www.gap-system.org`).

[8] A. Hanaki, *Semisimplicity of adjacency algebras of association schemes*, J. Algebra **225** (2000), no. 1, 124–129.

[9] ———, *Locality of a modular adjacency algebra of an association scheme of prime power order*, Arch. Math. (Basel) **79** (2002), no. 3, 167–170.

[10] A. Hanaki and I. Miyamoto, *Classification of association schemes with small vertices*, published on web (`http://kissme.shinshu-u.ac.jp/as/`).

[11] A. Hanaki and K. Uno, *Algebraic structure of association schemes of prime order*, to appear in J. Algebraic Combin.

[12] D. G. Higman, *Schur relations for weighted adjacency algebras*, Symposia Mathematica, Vol. XIII (Convegno di Gruppi e loro Rappresentazioni, INDAM, Rome, 1972), Academic Press, London, 1974, pp. 467–477.

[13] M. Hirasaka, *The enumeration of primitive commutative association schemes with a non-symmetric relation of valency of at most 4*, Standard integral table algebras generated by a non-real element of small degree, Lecture Notes in Math., vol. 1773, Springer, Berlin, 2002, pp. 105–119.

[14] A. Munemasa, *Splitting fields of association schemes*, J. Combin. Theory Ser. A **57** (1991), no. 1, 157–161.

[15] P.-H. Zieschang, *An algebraic approach to association schemes*, Lecture Notes in Mathematics, vol. 1628, Springer-Verlag, Berlin, 1996.

[16] ———, *Theory of association schemes*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2005.

[17] 藤崎源ニ郎, **代数的整数論入門**, 裳華房, 1975.