乗法的および加法的変数変換による有限体の表現構造に関する研究

1999年3月

野上保之

(1)

乗法的および加法的変数変換による
有限体の表現構造に関する研究

1999年3月

野上　保之

内　容　概　要

本論文は乗法的および加法的変数変換による有限体の表現構造に関して，筆者が信州大学工学系研究科（システム開発工学専攻）在学中に行った研究の成果をまとめたものである．本文は，4章から構成されている．

第1章では，本研究の背景およびその必要性と研究目的について述べている．

第2章では，乗法的な変数変換による既約多項式の導出およびその変遷を議論の中心として，有限体の表現構造に関して乗法的に解析する．基礎的準備に，乗法的に解析するための指標としてk乗剰余性なる概念を定義し，その性質を明確にする．これを用い，まず変数変換$x = x^k$による組織的な既約多項式の導出について考察する．次に，既約多項式の導出の際に必要となるk乗剰余性判定の一手法として，サイクル長なる概念を用いた容易な判定法を与える．次に，組織的な既約多項式の導出を可能とするための条件を満たさない元（k乗剰余元）を零点としてもつ既約多項式に対して，より実用的な既約多項式導出法という観点から，k剰剰余の除去法について検討する．さらに，これら既約多項式の導出および変遷の過程における性質を乗法的観点から明確にすることにより，与えられた既約多項式から同次の原始多項式を能動的に導出する手法を提案する．

第3章では，加法的な変数変換による既約多項式の導出およびその変遷を議論の中心として，有限体の表現構造に関して加法的に解析する．加法的に解析するための軸となる概念としてトレースなる概念を位置づけ，基礎的準備に，これを一般化したn次トレースなる概念，さらに加法的自己回帰既約多項式およびそれに付随する概念を定義する．まずトレースなる概念を用い，変数変換$x = x^P - x$による標数Pの倍数次数の既約多項式の導出法について考察する．次に，これに有限体上での形式微分および相反多項式なる概念を加え，変数変換を素体の適当な非零元sを用いた$x = x^P - x + s$とすることにより，標数倍の次数ごとの無限個の既約多項式の導出法を提案する．この導出法において，トレースの値が非零である既約多項式が重要な役割を果たすことに着目し，n次トレースなる概念を用いたトレース非零の真性元の特定について検討する．さらに，これら既約多項式の導出および変遷の過程における性質を加法的観点から明確にすることにより，加法的自己回帰既約多項式およびそれに付随する概念を用いた正規基底表現－最小多項式テーブルの一生成法について考察する．

第4章では，結論として本研究の成果を総括して述べる．

目　　次

第　1　章

序　　論

第1章 序　論

近年，情報通信・システム等の関連技術はすべてがデジタル信号による処理・制御の方向に進んでいるといえるほどデジタル信号処理の応用分野は広く発展著しい．アナログ信号に対しデジタル信号（データ）は様々な意味で処理・応用し易く，それはアナログ信号という無限の情報をもち得るデータに対してある一定の制限（限界）を定義し認めることにより，有限の情報量をもつ明確な信号（データ）となるためである．このことは言い換えれば，アナログ信号のもつ無限の情報をサンプリング等によりデジタル信号（データ）化し有限精度の情報とすることであり，情報量を減らしていることに他ならない．しかし，アナログ信号に対し無限の情報をもたせ，その情報を完全に使いきるということは不可能であり，デジタル信号化することにより有限かつ離散的なデータとして信頼性・保存性の高い情報として元のアナログ信号を十分に生かしきると言うこともできる．

デジタル信号処理がこれ程までに必要とされ，応用されてきている背景にはデータとしての扱い易さはもちろん，ここでは2つの大きな役割について見てみる．1つには，デジタル信号のもつ信頼性である．ここで述べる信頼性とは，離散的で有限の情報をもつデータであることによる，半永久的に保存可能なデータであり，またデジタル信号とすることによりシャノンの標本化・符号化定理などからくる必要十分で確実な情報通信を可能ならしめるからである．もちろん，これらのことは近年急速に発展してきたデジタル信号処理技術あるいは誤り訂正符号の採用によるところが大きい．2つめには，デジタル信号処理の応用面の広さにある．無限精度の情報を取り扱うアナログ信号処理がアナログ回路によるすなわちハード面での処理となるのに対し，デジタル信号処理はその離散信号であることによりデジタル回路による，いわば計算によるデータ処理となることから幅広い応用が容易に行えている．このことは，最近の身の回りの家電製品・電気機器からも容易にみてとれる．

本論文の研究背景として述べたいのは，これら技術のその基礎的概念が有限体理論にあるもの，または有限体理論により解析可能なものが多くあるということである．すなわち，デジタルデータが有限かつ離散的なデータ・情報であることより，有限体理論に基づいて解析・応用することがこれまでの多くのデジタル信号応用技術に対してはもちろん，今後のさらなる発展に対しても有益なこととなる．実際の応用例を挙げると，今日の迅速かつ信頼のおける情報通信を可能なものとしている背景にある誤り訂正符号の分野において，代数的誤り訂正符号等は有限体上での演算を必要とする[1]．あるいは，有限体理論における原始多項式により発生されるM系列は

理想的な雑音となり得ることから制御の分野，また相関特性の優れていることからＳＳ（Spread Spectrum）通信やＣＤＭＡ（Code Division Multiple Access）にも応用されている[2]．また，情報セキュリティーの分野においては，ＲＳＡ（Rivest Shamir Adleman）暗号やラビン暗号などの整数環上でのべき乗剰余演算を必要とする公開鍵暗合方式なども有限体理論を用いて解析することは大変意義のあることである[3]．

このように，近年の情報化社会において広く用いられている有限体理論であるが，実際用いられている有限体の性質はほんの一部であり，また有限体理論には未解決の問題も多く，明らかにされていない性質も多く残されている．代数的誤り訂正符号（線型符号）などは有限体の加法的な閉性を用い，またＲＳＡ暗号などは整数環上の乗法的な閉性（巡回性）を用いているに過ぎない．そして前者は，依然最小距離の問題等明らかにされない部分を含みながらも誤り訂正のシステムとして成り立たせているし，また後者は整数環上での元の巡回性を用いているに過ぎないにもかかわらず，第３者に対し解読困難な暗号として成り立たせている．すなわち，有限体の表現構造等をより深くまで考察・解析することによって既存のシステムをより効率良く利用・応用することはもちろん，新たなシステムの構築等が行える．

有限体とは，実数体・複素数体などに代表される無限位数の体に対し，有限位数の体であり有限の元の集合に対し乗法および加法を演算として含む代数系である．すべての有限体は，その位数が素数または素数のべき乗であり，素数位数の有限体は素体と呼ばれ，素数のべき乗位数の体はその拡大体である．拡大体とは素体上のベクトル空間であり，身近なところでは（無限体ではあるが）複素数体は実数体上の２次元ベクトル空間である．そして，拡大体を表現するために必要となるのが既約多項式であり，先の例の複素数体を実数体上の２次元ベクトル空間たらしめている既約多項式はx^2+1なる既約多項式である．また，任意の整数が素数の積の形で一意に表されるのと同様に，有限体上の任意の多項式は既約多項式の積の形に一意に因数分解され，有限体のすべての元は既約多項式の零点として特徴づけられる．このようにして有限体を捉えたとき，有限体の表現構造の解析は乗法的および加法的観点から行うべきであり，また既約多項式を議論の中心に据えることにより組織的な構造解析ができる．そして，変数変換等を用いた特定の形を有する既約多項式の導出，あるいはその過程における既約多項式の変遷について考察することは，有限体の元を乗法的・加法的に特徴づけ解析するための良い手法となる．

本論文では，以上のようなことを研究の背景として，有限体の表現構造についてより深くまで考察することを目的に２つの指標（概念）を導入する．乗法的指標として**k乗剰余性**なる概念，加法的指標として**トレース**なる概念である．そして，既約多項式を議論の中心として有限体の表現構造を乗法的・加法的に解析するという立場から，まず両概念を用い変数変換による既約多項式の導出について考察する．次に各々の既約多項式の導出過程において，導出される既約多項式の変遷をみることにより，乗法的観点から原始多項式の導出，加法的観点から元の最小多項式の特

定等について考察し，有限体の元相互間・既約多項式相互間の関係について乗法的・加法的に解析する．

本論文第2章においては，乗法的指標であるk乗剰余性なる概念及びその性質を明確にし，この観点からこれまでの有限体理論における幾つかの概念を見詰め直しその性質を明らかにする．その性質を用い，まず$x = x^k$なる形での変数変換を用いた組織的な無限個の高次既約多項式の導出法を提案する．これをより実用的なものとするために，サイクル長なる概念を用いた既約多項式の零点の容易なk乗剰余性判定法を与える．また，条件を満たさない元（k乗剰余元）を零点としてもつ既約多項式に対しては，その既約多項式から条件を満たす元（k乗非剰余元）を零点としてもつ同次既約多項式を組織的に導出するk乗剰余除去法を与える．さらに，この手法で非既約とされる場合の既約多項式の変遷の過程における性質を乗法的観点から明確にすることにより，与えられた既約多項式から同次の原始多項式を能動的に導出する手法を提案する．

第3章においては，加法的指標であるトレースなる概念を軸として，その一般拡張として与えられるn次トレースなる概念および**加法的自己回帰既約多項式**等の概念を新たに定義・導入し，その性質を明確にする．これらを用い，まず$x = x^P - x$なる変数変換による標数Pの倍数次数の既約多項式の導出法を示し，これに有限体上での形式微分および相反多項式なる概念を加え，素体のある特定の非零元sを用いることによる変数変換$x = x^P - x + s$とすることで無限個の高次既約多項式の組織的な導出法に拡張し提案する．次に，この既約多項式の導出法においてトレースの値が非零の元を零点としてもつ既約多項式が重要な役割を果たすことから，有限体の任意非零元のトレースの値を明確に与える式を示すことにより，これを用いてトレースの値の導出およびトレースの値が非零の真性元の特定を容易に行えることを示す．また，式の応用として最小多項式の新たな特定法を提案する．また，加法的観点からの既約多項式の導出の過程における既約多項式の変遷の性質を明確にすることにより，正規基底によるベクトル表現とそれに対応する最小多項式のテーブルの一生成法を提案する．

第　2　章

有限体構造の乗法的解析

第 2 章　有限体構造の乗法的解析

2.1　緒言

ＲＳＡ暗号等に代表される整数環におけるべき乗剰余演算を用いる暗号系においては，その元の位数というものが大変重要な意味をもつ．位数の大きさが，その暗号文の第３者による解読困難さを保証する大きな役割の一部分を占めているからである．また，理想的な擬似乱数系列であるM系列の長さ（周期）は，法となる原始多項式の指数，すなわちその原始多項式の零点の位数により決定される．あるいは，有限体そのものを表現する上で必要となる既約多項式の一導出法として，既約円周等分多項式による導出法があるが[4]，これは元の位数を観点とした導出法である．

このように，有限体における元の乗法的な振る舞い，巡回性について考察することは大変意義のあることである．また，これまでの有限体理論においてはその乗法的な構造解析というものは元の位数を観点として行われているものがほとんどである．しかしここで元の位数の特定・導出というものは，対象としている有限体の標数P及び拡大次数mが大きくなるほど困難なものであり，位数なる概念を用いた代表的な既約多項式の導出法である文献[5]-定理3.35などは，実用的なものとは到底ならない．例えば位数の導出が不可能であろう大きな有限体においては，文献[5]-定理3.35を用いては既約多項式$f(x)$から$f(x^2)$なる２倍の次数の既約多項式でさえ得られないのである．しかし，平方剰余性なる概念を用いることにより，標数が奇素数の有限体においては条件を満たす既約多項式$f(x)$から組織的に$f(x^{2^i})$なる既約多項式が得られるという研究結果が報告されている[6]．このように考えたとき，位数なる概念は$x = x^k$なる変数変換による既約多項式の導出に対して，必要以上の元の情報を含んでいるという考え方ができる．

本章では，位数なる概念に代わり，有限体理論における平方剰余性なる概念の一般拡張として与えられる**k乗剰余性**なる概念を用いることにより，位数なる概念よりもより細分化されかつ必要十分な乗法に関する元の情報を抽出できることを示し，この観点から変数変換による既約多項式の組織的な導出法に関する議論を軸として，有限体構造の乗法的な解析を行う．まず基礎的準備として，k乗剰余性なる概念を定義しその種々の性質を明確にする．そして，この概念を用い，$x = x^K$なる形での無限個の既約多項式の導出法を提案し，その過程において必要となるk乗剰余性判定法およびk乗剰余の除去法を与え本手法をより実用的なものとする．次に原始多項式についてk剰剰余性なる観点からその性質を明確にし，先の既約多項式導出過程におけるk乗剰余性なる観点からみた既約多項式変遷の性質と比較・考察することにより，これまで明確とされてい

なかった組織的な原始多項式の導出法を与える．

尚，本論文を通してPを素数，mを正整数とする．

2.2 基礎的準備

本節では，有限体を乗法的に解析するために必要となる基礎的な準備をする．

2.2.1 k乗剰余性

k乗剰余性なる概念を以下のように定義する．

定義（k乗剰余性）2.2.1.1：$GF(P^m)$の非零元αおよび自然数kに対して，$\alpha = \beta^k$なる元βが$GF(P^m)$に存在するとき，αを（$GF(P^m)$において）k乗剰余（k-th Power Residue）といい，そのような元βが$GF(P^m)$に存在しないときαを（$GF(P^m)$において）k乗非剰余（k-th Power Non Residue）という． ■

このように定義されたk乗剰余性に対して，以下のような性質が得られる．

性質2.2.1.2：$\gcd(P^m - 1, k) = k$であるならば，$GF(P^m)$において，原始元のkの倍数乗で表される元は$GF(P^m)$においてk乗剰余である．また，その逆も成り立つ． ■

性質2.2.1.2は，$\gcd(P^m - 1, k) = k$なる整数kに対して原始元のkの倍数乗で表わされない元は，k乗非剰余であることを示している．すなわち，$GF(P^m)$における元のk乗剰余性は，$GF(P^m)$の原始元を用いて体の元をべき表現した際の指数部を，kが割り切るか割り切らないかにより，判定できることがわかる．

性質2.2.1.3：$\gcd(P^m - 1, l) = k$が成り立つとき，$GF(P^m)$における元のl乗剰余性とk乗剰余性は等価である． ■

性質2.2.1.3より，$GF(P^m)$における元のもつ剰余性の考察は，$k \mid (P^m - 1)$となるような整数kについてのk乗剰余性のみを考えれば良いことが分かる．さらに，$\gcd(P^m - 1, k) = 1$なる整数kについては，性質2.2.1.2より$GF(P^m)$の全ての元が$GF(P^m)$においてk乗剰余となることより，考察する必要のないことを意味している．

ここで，$X \mid Y$ はXがYを割り切ること示し，$X \nmid Y$ は割り切らないことを示す．

次に，$GF(P^m)$の元の$GF(P)$に関する共役元については，次のような補題が得られる．

補題2.2.1.4：$k \mid (P^m - 1)$なる整数kに対して，$GF(P^m)$においてk乗剰余であると判定された元の$GF(P)$に関する共役元は，すべてk乗剰余である．また．k乗非剰余である元の$GF(P)$に関する共役元はすべてk乗非剰余である． ■

証明(補題2.2.1.4)：性質2.2.1.2および，$\gcd(P^m-1, P)=1$より明らかである． ■

補題2.2.1.4は共役元のもつ剰余性が等しいことを意味する．

2.2.2 サイクル長

サイクル長なる概念は次のように定義される．

定義（サイクル長）2.2.2.1[7]：$GF(P)$上の多項式$M(x)$を法とし，任意の非零剰余類$a(x)$に対してP乗演算をn回繰り返したときはじめて，

$$(a(x))^{P^n} \equiv a(x) \pmod{M(x)}$$

を満たす自然数nを“（多項式$M(x)$を法とした）剰余類$a(x)$の**サイクル長**”と呼ぶ． ■

任意の多項式を法とした剰余類(x)のサイクル長を求めることによって，その多項式の零点の存在する拡大体の拡大次数を求めることができる．これを本章では，$f(x^k)$なる形の多項式を法多項式として用いることにより，既約多項式$f(x)$の零点のk乗剰余性を判定することに用いる．

2.2.3 原始多項式

M系列の発生等に用いられる原始多項式は以下のように定義される．

定義（原始多項式）2.2.3.1：$GF(P)$上のm次既約多項式$f(x)$の指数すなわち$f(x)$の零点の位数がP^m-1のとき，$f(x)$を$GF(P)$上のm次原始多項式と呼ぶ． ■

後述するが，原始多項式の零点は零点が真性元[1]として存在する体の原始元であり，定義にあるP^m-1のすべての約数kに対してk乗非剰余である．一般に原始多項式の導出は既約多項式の原始性の判定により行われており，従来の原始性判定法は以下のようである．

原始性判定手順：$GF(P)$上のm次既約多項式$f(x)$が与えられたとき，P^m-1が次のように素因数分解されるものとする．

$$P^m-1 = P_1^{e_1} P_2^{e_2} \cdots P_r^{e_r}$$

ただし，$P_1, P_2, \cdots, P_r$は相異なる素数であり，$e_1, e_2, \cdots, e_r$は正整数であるとする．

このとき，すべての素数P_i $(i=1,2,\cdots,r)$に対して，

$$x^{(P^m-1)/P_i} \not\equiv 1 \pmod{f(x)} \tag{2.1}$$

ならば，$f(x)$は原始である． ■

[1] $f(x)$は$GF(P)$上のm次既約多項式であることより，その零点ωは$GF(P^m)$の元でありその真部分体に属することはない．このような元を，$GF(P^m)$の真性元と呼ぶ．

この判定は，仮にP^m-1が完全に素因数分解されていたとして，反復平方積による高速指数演算法を用いたとしてもかなりの時間を要する．

2.3 既約多項式の導出

任意次数の既約多項式の導出は，従来ランダムに得られた多項式の既約判定により行われている．この操作は，既約多項式の次数あるいは標数が大きくなるほど困難な操作となりあまり実用的ではない．そこで，変数変換による組織的な高次既約多項式の導出法，あるいは特定の形を有する既約多項式の導出法などの研究がこれまでいくつか行われてきた[4][6][8][9][10].

本節では，前節で定義した有限体上におけるk乗剰余性なる概念を既約多項式の導出に対して用いることにより，$x=x^K$なる形での変数変換による組織的な無限個の高次既約多項式の導出法を与えることを中心に有限体，既約多項式および元相互間の関係について乗法的に考察を行う．

2.3.1 素因数kを用いた変数変換$x=x^k$による既約多項式の導出

既約多項式に変数変換$x=x^k$を施すことにより，新たにk倍の次数の既約多項式を得られる次の定理を示す．

定理2.3.1.1：$f(x)$を$GF(P)$上のm次既約多項式とし，その零点は$GF(P^m)$の真性元ωであるとする．このとき，$k\mid(P^m-1)$なる素数kで，ωが$GF(P^m)$においてk乗非剰余であると判定されたとき，このkを用いた多項式$f(x^k)$は$GF(P)$で既約である．またその逆も成り立つ． ■

証明(定理2.3.1.1)：$GF(P^m)$上の多項式$x^k-\omega$が$GF(P^m)$上で既約となり，その結果，文献[6]-定理1より$f(x^k)$が$GF(P)$において既約となることを示す．すなわち，定理2.3.1.1の証明として$x^k-\omega$の$GF(P^m)$における既約性を示す．

ωが$GF(P^m)$上で，k乗剰余であれば$GF(P^m)$にはk乗してωとなる元が存在することから，$x^k-\omega$が$GF(P^m)$では既約でないことが容易にわかる．すなわち，$x^k-\omega$の零点であり，$f(x^k)$の零点であるτは，$GF(P^m)$のk次拡大体$GF(P^{km})$に真性元として存在しない．ゆえに，$f(x^k)$は$GF(P)$において既約でない．

次に，ωが$GF(P^m)$でk乗非剰余である場合を考える．ωが，$GF(P^m)$の原始元αを用いて$GF(P^m)$で，

$$\omega=\alpha^i \tag{2.2}$$

(iは正整数) と表されるとき，ωは$GF(P^m)$でk乗非剰余であるため，性質2.2.1.2から[2] (又，kが素数であることより)，次の関係が成り立つ．

$$k \nmid i$$

すなわち，$k \nmid \gcd(i, P^m - 1)$である．また，ωは$GF(P^m)$においてk乗非剰余であることより，$x^k - \omega$は$GF(P^m)$にその零点をもたない．ここで，k乗してωとなる元が$GF(P^{km})$に真性元として存在することを示す．

ωの位数eは，$e = (P^m - 1)/\gcd(i, P^m - 1)$と表され，$\omega$は，$GF(P^m)$の$k$次拡大体$GF(P^{km})$において，$GF(P^{km})$の適当な原始元$\beta$を用いて，

$$\begin{aligned} \omega &= \beta^{\frac{P^{km}-1}{e}} \\ &= \beta^{\frac{\gcd(i,P^m-1)(P^{km}-1)}{P^m-1}} \end{aligned} \tag{2.3}$$

と表せる．

式(2.3)の指数部をAとおくと指数部Aは，

$$A = \gcd(i, P^m - 1)\left[\sum_{j=1}^{k-1}(P^{jm} - 1) + k\right] \tag{2.4}$$

と変形され，$k \mid (P^m - 1)$であることより，kは指数部Aを割り切る．したがって，性質2.2.1.2からωは$GF(P^{km})$においてk乗剰余である[3]．ゆえに，$x^k - \omega$の零点は$GF(P^{km})$に存在する．

次に，$GF(P^{km})$より小さい$1 < s < k$なる正整数sによる拡大体$GF(P^{sm})$には，k乗してωとなる元が存在しないことを示す．これまでと同様にして，ωを$GF(P^{sm})$の適当な原始元を用いてべき表現し，その指数部をBとすれば，

$$\begin{aligned} B &= \gcd(i, P^m - 1)\sum_{j=0}^{s-1} P^{jm} \\ &= \gcd(i, P^m - 1)\left[\sum_{j=1}^{s-1}(P^{jm} - 1) + s\right] \end{aligned} \tag{2.5}$$

となり，B割るkを考えたとき，式(2.5)の最終項のsのみがkで割り切れない．したがって，

$$k \nmid B$$

---

[2] $k \mid (P^m - 1)$より，$\gcd(P^m - 1, k) = k$であることから，性質2.2.1.2を用いることができる．

[3] $k \mid (P^m - 1)$より$k \mid (P^{km} - 1)$である．すなわち，$\gcd(P^{km} - 1, k) = k$であることより，性質2.2.1.2を用いることができる．

である．このことから，性質2.2.1.2よりωは$GF(P^{sm})$ではk乗非剰余となり$x^k-\omega$の零点は$GF(P^{sm})$には存在しない．すなわち，$x^k-\omega$の零点は$GF(P^{km})$の真性元であることが判明する．したがって，$x^k-\omega$は$GF(P^m)$において既約となり，その結果，文献[6]-定理1より$f(x^k)$は$GF(P)$で既約である．

また，この定理の十分性の証明は，先に述べた$x^k-\omega$が$GF(P^m)$で既約でなければ，$f(x^k)$は$GF(P)$において既約でないという証明の対偶を取ることで容易にわかる． ■

定理2.3.1.1により，1つの既約多項式から，さらに高次な既約多項式が1つ得られることがわかる．次項では，さらに無限個の高次既約多項式が得られる手法を示す．

2.3.2 素因数kを用いた変数変換$x=x^k$による無限個の既約多項式の導出

定理2.3.1.1により，1つの既約多項式から，さらに高次な既約多項式が1つ得られることがわかる．本項では，定理2.3.1.1に関連して，次の系を紹介し，無限個の高次既約多項式が得られることを示す．

系2.3.2.1：$k\neq 2$のとき，または，$k=2$かつ$P^m\equiv 1 \pmod 4$のとき，定理2.3.1.1を用いて得られる$GF(P)$上のmk次既約多項式$f(x^k)$の零点$\tau\in GF(P^{km})$は$GF(P^{km})$においてk乗非剰余となる． ■

証明(系2.3.2.1)：$f(x)$の零点$\omega\in GF(P^m)$と$f(x^k)$の零点$\tau\in GF(P^{km})$の間には，次のような関係が成り立つ．

$$\tau^k=\omega$$

ここで，τの位数をe'，ωの位数をeとすると，

$$e'=ke$$

である．上式より，τは$GF(P^{km})$の適当な原始元βおよび式(2.4)で定義したAを用いて，

$$\tau=\gamma^{\frac{A}{k}} \tag{2.6}$$

と，$GF(P^{km})$において表せる（ここで，$k\mid A$であることに注意）．ここで，$C=(P^m-1)/k$とし，式(2.2)で定義したiを用いて式(2.6)の指数部を変形する．

$$\begin{aligned}\frac{A}{k} &= \gcd(i,P^m-1)\left[C\sum_{j=1}^{k-1}\sum_{l=0}^{j-1}P^{lm}+1\right]\\ &= \gcd(i,P^m-1)\left[C\sum_{j=1}^{k-1}\left[\sum_{l=0}^{j-1}(P^{lm}-1)+j\right]+1\right]\end{aligned}$$

(2.7)

ここで，定理2.3.1.1の証明と同様にωは$GF(P^m)$においてk乗非剰余であることより，

$$k \nmid \gcd(i, P^m - 1)$$

であることに注意する．また，$f(x)$の他の零点については，$GF(P)$に関する共役元であり，補題2.2.1.4より剰余性は等しいので，零点として$\gamma^{A/k}$を代表させる．式(2.7)について考察するために，ここで以下の2つの場合分けを行う．

1. $P^m - 1$がkで2回以上割れる場合

   すなわち$k \mid C$であり，式(2.4)で定義されるAにおいて$P^m - 1$がkで2回以上割りきれることより，式(2.6)の指数部A/kは

   $$k \nmid \frac{A}{k}$$

   である．したがって，性質2.2.1.2よりτは$GF(P^{km})$でk乗非剰余となる．

2. $P^m - 1$がkで2回以上割れない場合

   すなわち$k \nmid C$であり，式(2.7)の第2式において，kで割り切れない項を集めると，

   $$\gcd(i, P^m - 1)\left[C\sum_{j=1}^{k-1} j + 1\right] = \gcd(i, P^m - 1)\left[\frac{k(k-1)C}{2} + 1\right] \tag{2.8}$$

   となる．ここで，式(2.8)を解析するために，さらに以下の場合分けを行う．

   (a) kが奇素数の場合

   kは奇素数より式(2.8)において，

   $$k \mid \frac{k(k-1)C}{2}$$

   である．したがって，式(2.8)の最終項の1がkで割り切れないことより，

   $$k \nmid \frac{A}{k}$$

   となり，性質2.2.1.2よりτは$GF(P^{km})$でk乗非剰余となる．

   (b) kが偶素数（すなわち$k = 2$）の場合

   $k = 2$であることより，式(2.8)に$k = 2$を代入して，

   $$\gcd(i, P^m - 1)\left[\frac{k(k-1)C}{2} + 1\right] = \gcd(i, P^m - 1)(C + 1) \tag{2.9}$$

となる．ここでCとは，$k=2$より，

$$C=\frac{P^m-1}{2}$$

であり，場合分け(2)の条件より$2 \nmid C$であるから，Cは奇数である．したがって，$k=2$として，

$$k \mid \gcd(i, P^m-1)(C+1)$$

である．ゆえに，

$$k \mid \frac{A}{k}$$

であるから，この場合は性質2.2.1.2よりτは$GF(P^{km})$において，k乗剰余となる．すなわち$k=2$のときは，場合分け(1)のP^m-1がkで2回以上割れる場合，すなわち$P^m \equiv 1 \pmod 4$のときに，k乗非剰余（$k=2$より平方非剰余）となる．

■

系2.3.2.1の結果を，定理2.3.1.1に用いることにより次の定理が得られる．

定理2.3.2.2：$f(x)$を$GF(P)$上のm次既約多項式とし，その零点を$GF(P^m)$の真性元ωであるとする．このとき，$k \mid (P^m-1)$なる素数kで，ωが$GF(P^m)$において，k乗非剰余であると判定されたとき，kが奇素数または偶素数2であっても$P^m \equiv 1 \pmod 4$であるならば，非負整数jを用いてmk^j次多項式$f(x^{k^j})$が$GF(P)$で既約となる．■

2.3.3　合成数Kを用いた変数変換$x=x^K$による無限個の既約多項式の導出

定理2.3.1.1で用いたk乗剰余性以外の剰余性については，次の系が得られる．

系2.3.3.1：$k \neq 2$のとき，または，$k=2$かつ$P^m \equiv 1 \pmod 4$のとき，定理2.3.1.1を用いて得られる$GF(P)$上のmk次既約多項式$f(x^k)$の零点$\tau \in GF(P^{km})$は，$f(x)$の零点$\omega \in GF(P^m)$が$GF(P^m)$においてもつ，$t \mid (P^m-1)$なるすべての素数tについての剰余性，非剰余性を$GF(P^{km})$において維持する．■

証明(系2.3.3.1)：$t \mid (P^m-1)$なるすべての素数tの集合からkのみを除いた集合を$S_{\bar{k}}$とする．系2.3.2.1及びその証明により，k乗剰余性については維持していることが容易に分かる．他の剰余性（k'乗剰余性：$k' \in S_{\bar{k}}$）については，$f(x)$の零点ωが$GF(P^m)$においてk'乗剰余である場合と，k'乗非剰余である場合について分けて考える．

k'乗剰余である場合：ωが$GF(P^m)$においてk'乗剰余であることより，式(2.2)において，性質2.2.1.2より，$k' \mid \gcd(i, P^m - 1)$であることが分かる．すなわち，式(2.7)において，

$$k' \mid \frac{A}{k}$$

となり，性質2.2.1.2よりτは$GF(P^{km})$においてk'乗剰余である．

k'乗非剰余である場合：ωが$GF(P^m)$においてk'乗非剰余であることより，式(2.2)から，性質2.2.1.2より，$k' \nmid \gcd(i, P^m - 1)$であることが分かる．また，$k' \mid (P^m - 1)$でありかつ$k' \neq k$であることより，

$$k' \mid \frac{P^m - 1}{k}$$

である．すなわち，系2.3.2.1の証明と同様に$C = (P^m - 1)/k$として，$k' \mid C$である．ゆえに，式(2.7)において，最終項の1のみがk'で割り切れないため，

$$k' \nmid \frac{A}{k}$$

となり，性質2.2.1.2よりτは$GF(P^{km})$においてk'乗非剰余である．

したがって，τは$GF(P^{km})$において，$t \mid (P^m - 1)$なる全ての素数についての，ωの$GF(P^m)$におけるt乗剰余性，非剰余性を維持している． ■

したがって，定理2.3.1.1及び系2.3.3.1より，次の定理が得られる．

定理2.3.3.2：$f(x)$を$GF(P)$上のm次既約多項式とし，その零点を$GF(P^m)$の真性元ωであるとする．このとき，$k \mid (P^m - 1)$なる全ての素数kの中から，ωが$GF(P^m)$においてk乗非剰余であると判定されるようなkによる合成数Kが，奇数または偶数であっても$P^m \equiv 1 \pmod 4$であるならば，Kを用いてmK次多項式$f(x^K)$が$GF(P)$で既約となる． ■

2.3.4 Example

Example2.3.4.1：$GF(2)$上の4次既約多項式を

$$f(x) = x^4 + x + 1$$

としたとき，$f(x)$の零点ωは$GF(2^4)$の真性元であり，その剰余性については，

$$2^4 - 1 = 3 \cdot 5$$

であることより，3乗剰余性及び，5乗剰余性について考察できる．零点ωの$GF(2^4)$においてもつ剰余性は，3乗非剰余であり5乗非剰余である．すなわち，$f(x)$は原始多項式である．

ゆえに，定理2.3.2.2および定理2.3.3.2より，次のような既約多項式が得られる．

$$f(x^{3^i}) \ , \ f(x^{5^j}) \ , \ f(x^{3^i 5^j})$$

ここで，i，jは非負整数である．

■

定理2.3.2.2および定理2.3.3.2により，条件を満たすkによって1つの既約多項式からより高次な既約多項式を無限個得られることがわかる．しかし，定理2.3.1.1，定理2.3.2.2および定理2.3.3.2を用いるには，$GF(P)$上のm次既約多項式$f(x)$の零点ωの$GF(P^m)$におけるk乗剰余性の判定が必要である．ここでkとは，$k \mid (P^m - 1)$なる素数である．次節においてその判定方法を述べる．

2.4 k乗剰余性判定法

前節に述べた$x = x^k$なる変数変換による組織的な既約多項式の導出，あるいは後述する原始多項式の判定・導出には，その既約多項式の零点のk乗剰余性判定が必要となる．本節では，標数Pおよび拡大次数mに対して$k \mid (P^m - 1)$の場合，$k \mid (P - 1)$の場合（より容易な判定が可能となる）の2つの場合に分けてk乗剰余性判定法を与える．

2.4.1 $k \mid (P^m - 1)$の場合のk乗剰余性判定

前節の既約多項式の導出に関する考察より，$GF(P)$上のm次既約多項式$f(x)$の零点ωがk乗非剰余であるならば，$f(x^k)$なる多項式はmk次既約多項式となる．逆にk乗剰余であるならば$f(x^k)$は既約多項式とはならず，以下のような特徴をもつ．

補題2.4.1.1：$GF(P)$上のm次既約多項式$f(x)$の零点$\omega \in GF(P^m)$が$GF(P^m)$において，

$$k \mid (P^m - 1)$$

なる素数kで，k乗剰余であると判定されたとき，$f(x^k)$はk個の相異なる$GF(P)$上のm次既約多項式の積で表される．■

証明(補題2.4.1.1)：$f(x)$は$GF(P)$上のm次既約多項式であり，その零点ωは$GF(P^m)$の真性元である．零点ωが$GF(P^m)$においてk乗剰余ならば，性質2.2.1.2より$GF(P^m)$の原始元αと適当な非負整数iを用いて，$\omega = \alpha^{ik}$と表せる．したがって，$f(x^k)$の零点τは，$\omega = \tau^k$を満たすことより，$\tau^k = \alpha^{ik}$であり，これを満たすτは，$GF(P^m)$のk個の元

$$\alpha^i, \alpha^{i+\frac{P^m-1}{k}}, \alpha^{i+\frac{2(P^m-1)}{k}}, \cdots, \alpha^{i+\frac{(k-1)(P^m-1)}{k}} \tag{2.10}$$

である．τは$GF(P^m)$の真性元であることより[4]，これらはそれぞれm個の$GF(P)$に関する共役元をもち，これらは互いに異なる．なぜなら，もしα^iの共役な集合の中に式(2.10)の別の元が含まれていると仮定するならば，この集合の要素をそれぞれk乗した集合，すなわち$GF(P)$に関するωと共役な元の集合の中に，α^{ik}が2つ含まれることになり，ωが$GF(P^m)$の真性元であることに矛盾する．ゆえに，式(2.10)の元は$GF(P)$に関して共役ではない．ゆえに，$f(x^k)$は，式(2.10)の各々の相異なるk個の元の最小多項式の積となる．

■

定理2.3.1.1および補題2.4.1.1より，$f(x)$の零点ωがk乗非剰余であるならば$f(x^k)$はmk次既約多項式となり，$f(x)$の零点ωがk乗剰余であるならば$f(x^k)$はk個の相異なるm次既約多項式の積となる．このような事実を踏まえ，k乗剰余性の判定法を補題として以下に与える．

補題2.4.1.2：$GF(P)$上のm次既約多項式$f(x)$に$k \mid (P^m-1)$なる素数kを用いて変数変換を施した$GF(P)$上のmk次多項式$f(x^k)$がある．このとき，剰余類(x)の法$f(x^k)$に対するサイクル長は，$f(x^k)$が$GF(P)$において既約ならばmkであり，既約でないならばmである．

■

証明(補題2.4.1.2)：サイクル長により，剰余類(x)すなわち法多項式の零点の属する体の拡大次数が得られる．すなわち，$f(x^k)$が$GF(P)$で既約ならば，剰余類(x)の$f(x^k)$を法としたサイクル長はmkである．$f(x^k)$が$GF(P)$で既約ではなく，補題2.4.1.1より$GF(P)$のk個の相異なるm次既約多項式の積で表されるならば，剰余類(x)の$f(x^k)$を法としたサイクル長はmとなる．

■

定理2.3.1.1，補題2.4.1.1および補題2.4.1.2より，$f(x)$の零点の$GF(P^m)$におけるk乗剰余性は，$f(x^k)$を法としたとき，剰余類(x)のサイクル長がmkになるかmになるかによって判定できる．この際，導出されるサイクル長はmまたはmkゆえ，m回のP乗剰余演算を施したとき，剰余類(x)にもどらなければサイクル長はmkとなる．

2.4.2 $k \mid (P-1)$の場合のk乗剰余性判定

前項のk乗剰余性判定の特別な場合として，$k \mid (P-1)$のときの判定法は次の補題で与えられより容易な判定となる．

[4] τが$GF(P^m)$の真性元でないとするならば，τ^kの形で表されるωも$GF(P^m)$の真性元となり得ないことより矛盾する．

補題2.4.2.1：$GF(P)$ 上の m 次単位既約多項式 $f(x)$ があり，その零点を $\omega \in GF(P^m)$ とする．また，$f(x)$ の零次係数を f_0 とする．このとき，$k \mid (P^m-1)$ なる素数 k が $k \mid (P-1)$ ならば，ω の $GF(P^m)$ における k 乗剰余性は，以下で示される．

$\frac{m(P-1)}{k}$ **が偶数の場合**：ω の $GF(P^m)$ における k 乗剰余性は，f_0 の $GF(P)$ における k 乗剰余性と等しい．

$\frac{m(P-1)}{k}$ **が奇数の場合**：ω の $GF(P^m)$ における k 乗剰余性は，f_0 の $GF(P)$ における k 乗剰余性の反転である．

■

証明(補題2.4.2.1)：$GF(P^m)$ のすべての非零元の k 乗剰余性の判定は，性質2.2.1.2より，判定したい非零元を $(P^m-1)/k$ 乗し，1になるか否かによって判定できることが容易に分かる．すなわち，判定したい $GF(P^m)$ の非零元を $(P^m-1)/k$ 乗して，1になれば $GF(P^m)$ において k 乗剰余であり，1にならなければ k 乗非剰余である．このような観点から，$f(x)$ の零点 ω の k 乗剰余性を判定する．

ω を $(P^m-1)/k$ 乗すると，$k \mid (P-1)$ であることより以下のような式展開が可能である．

$$\begin{aligned} \omega^{\frac{(P^m-1)}{k}} &= \omega^{\frac{(P-1)}{k}(P^{m-1}+\cdots+P+1)} \\ &= \left[\omega^{(P^{m-1}+\cdots+P+1)}\right]^{\frac{(P-1)}{k}} \end{aligned}$$

ここで，$f(x)$ の零次係数 f_0 と ω は以下の関係：

$$\begin{aligned} f_0 &= (-1)^m \omega \omega^P \omega^{P^2} \cdots \omega^{P^{m-1}} \\ &= (-1)^m \omega^{P^{m-1}+\cdots+P+1} \end{aligned} \tag{2.11}$$

を満たすことより，

$$\begin{aligned} \omega^{\frac{(P^m-1)}{k}} &= [(-1)^m f_0]^{\frac{(P-1)}{k}} \\ &= (-1)^{\frac{m(P-1)}{k}} f_0^{\frac{(P-1)}{k}} \end{aligned} \tag{2.12}$$

である．すなわち，式(2.12)において右辺の $f_0^{(P-1)/k}$ は f_0 の $GF(P)$ における k 乗剰余性の判定そのものである[5]．式(2.12)より，ω の $GF(P^m)$ における k 乗剰余性と，f_0 の $GF(P)$ における k 乗剰余性が等しいか否かは，$\frac{m(P-1)}{k}$ の偶奇による．■

[5] $k \mid (P-1)$ であり，性質2.2.1.2より $GF(P)$ において k 乗剰余性の判定は可能である．

補題2.4.2.1により素数kが$k \mid (P-1)$を満たすとき，$GF(P)$上の既約多項式の零点のk乗剰余性の判定は，$f(x)$を単位既約多項式とした際の零次係数f_0の$GF(P)$におけるk乗剰余性の判定で行えることが分かる．すなわち，前項で行える判定のうち，$k \mid (P-1)$を満たす場合には，より容易に判定が行える．

2.4.3 従来法による判定との比較

従来の原始性判定に用いられている式(2.1)をk乗剰余性判定を行えるように改良すると次のようになる．

$$x^{(P^m-1)/k} \equiv 1 \quad or \quad not \quad (\mathrm{mod}\ f(x)) \tag{2.13}$$

しかしこの方法は，プログラミング上でメモリが不足しているような状況下では逐次べき乗および多項式剰余演算を行わなければならず，たとえ高速指数演算法を用いたとしてもかなりの計算量を必要とする．また，必要となるべき乗演算および多項式による剰余演算の回数も定かではない．

他方，本章で提案するk乗剰余性判定法はサイクル長なる概念を用いていることから以下の式で計算される．

$$x^{P^m} \equiv x \quad or \quad not \quad (\mathrm{mod}\ f(x^k)) \tag{2.14}$$

式(2.14)によってk乗剰余性が判定される本提案法は，メモリが不足しているような状況においても，式(2.13)におけるべき乗演算は式(2.14)においてはP乗演算であることから単に項間をP間隔にシフトする操作だけであり，実際にはべき乗というような乗算はまったく必要とせず，さらに多項式による剰余演算も拡大次数m回で済む．以上のことからも，本提案法の方がより容易かつ明快な判定が行えていると考える．

2.5 k乗剰余の除去

$x = x^k$なる変数変換およびその組み合わせによる無限個の既約多項式の導出を行うためには，元となる既約多項式の零点がk乗非剰余でなければならずk乗剰余であるならば，変数変換を行ったとしても既約な多項式とはならない．そこで本節では，既約多項式の零点がk乗剰余であるような性質をもつ場合，変数変換および既約因数分解[11]を施すことにより，k乗剰余である性質のみ取り除かれた剰余性をもつ零点（k乗非剰余）をもつ同次の既約多項式を得る手法を，前節と同様に標数Pおよび拡大次数mに対して$k \mid (P^m-1)$の場合，$k \mid (P-1)$の場合（より容易に行える）の2つの場合に分けて与える．

2.5.1 $k \mid (P^m-1)$ の場合の k 乗剰余の除去

$f(x)$ を $GF(P)$ 上の m 次既約多項式とし，その零点を $GF(P^m)$ の真性元 ω とする．ここで，

$$P^m-1=k_1^{e_1}k_2^{e_2}\cdots k_r^{e_r}$$

$$k_j\ (j=1,2,\cdots,r)\text{：相異なる素数}$$

$$e_j\ (j=1,2,\cdots,r)\text{：正整数}$$

とし，e を元 ω の位数とする．ω の位数が e であることより，$GF(P^m)$ の適当な原始元 α を用いて，

$$\omega=\alpha^{\frac{P^m-1}{e}}$$

なる等式が成り立つ．

このとき，$(P^m-1)/e$ の素因数 k_j に対して，$f(x^{k_j})$ は補題2.4.1.1より，$GF(P)$ 上の相異なる k_j 個の m 次既約多項式の積の形に既約因数分解される．その個々の既約因数多項式の零点の剰余性を考察する．

$f(x^{k_j})$ の零点 τ は，$\omega=\tau^{k_j}$ を満たすことより，以下の $GF(P^m)$ の元である．

$$\alpha^{(P^m-1)/k_je},\alpha^{(P^m-1)/k_je+(P^m-1)/k_j},\cdots,\alpha^{(P^m-1)/k_je+(k_j-1)(P^m-1)/k_j}$$

ここで補題2.4.1.1より，これらは相異なる．各元の剰余性を判定するために，これらの指数部より，

$$\gcd(P^m-1,\frac{P^m-1}{k_je}(se+1)) \tag{2.15}$$

の取る値を調べる．ここで，$s=0,1,\cdots,k_j-1$ である．式(2.15)は，

$$\frac{P^m-1}{k_je}\gcd(k_je,se+1)$$

と変形でき，$\gcd(e,se+1)=1$ であることより，

$$\frac{P^m-1}{k_je}\gcd(k_j,se+1)$$

と変形できる．ここで，次のような場合分けを行う．

1. k_j が e を割り切る場合

$$\frac{P^m-1}{k_je}\gcd(k_j,se+1)=\frac{P^m-1}{k_je}$$

であり，性質2.2.1.2よりすべての既約因数多項式の零点のもつ最大の剰余性は $(P^m-1)/k_je$ 乗剰余（すなわち位数が k_je）である．

2. k_jがeを割り切らない場合

$$\gcd(k_j, se+1)$$

の取る値は，k_jは素数ゆえ，k_jあるいは1である．すなわち，sが0から(k_j-1)まで変化すれば，

$$k_j \mid (se+1)$$

を満たすsが必ず1つ存在する[6]．すなわち，

$$\frac{P^m-1}{k_j e}\gcd(k_j, se+1) = \frac{P^m-1}{k_j e} \ or \ \frac{P^m-1}{e}$$

である．すなわち，k_j個の既約因数多項式の内，零点のもつ最大の剰余性が$(P^m-1)/k_j e$乗剰余でない（すなわち位数がeである）既約因数多項式が，必ず1つ存在する．

以上の議論を次の定理にまとめる．

定理2.5.1.1：$f(x)$を$GF(P)$上のm次既約多項式とし，

$$P^m-1 = k_1^{e_1}k_2^{e_2}\cdots k_r^{e_r}$$

(相異なる素数のべき乗の積)

とする．

$f(x)$が原始多項式でないならば，その零点の位数eは$e < P^m-1$であり，$(P^m-1)/e$の素因数k_jに対して$f(x^{k_j})$を既約因数分解する．

このとき，$k_j \mid e$であるならば，すべての既約因数多項式の零点の位数は$k_j e$である．また，$k_j \nmid e$であるならば，必ず1つの既約因数多項式の零点の位数はeであり，他の既約因数多項式の零点の位数は$k_j e$である． ■

定理2.5.1.1をk乗剰余性という観点から考察するとき，変数変換，既約因数分解によって，零点のもつ剰余性からk_j乗剰余である性質のみ取り除くことができることを意味する．また，他の剰余性には影響を及ぼさない．すなわち，元のもつすべての剰余を取り除いたとき，既約多項式の零点は，零点が真性元として属する体において原始元となり，そのような零点をもつ最小多項式は原始多項式である．

また，取り除きたいk乗剰余の素数kが$k \mid (P-1)$を満たす場合は，より容易に除去できることを次項で示す．

[6]前提より，$\gcd(k_j, e) = 1$であることから明らかである．

2.5.2 $k \mid (P-1)$ の場合の k 乗剰余の除去

$k \mid (P-1)$ のような特別な場合における，k 乗剰余の除去に必要となる補題を与える．

補題2.5.2.1：$k \mid (P-1)$ なる素数 k がある．$GF(P)$ において k 乗剰余なる元，k 乗非剰余なる元は，$k \nmid m$ なる正整数 m に対して $GF(P^m)$ においてもそれぞれ k 乗剰余，k 乗非剰余であり，$k \mid m$ なる正整数 m に対して $GF(P^m)$ においては，ともに k 乗剰余である． ■

証明(補題2.5.2.1)：この証明は定理2.3.1.1の証明と同様に行える． ■

補題2.5.2.1により，$GF(P)$ 上の m 次既約多項式 $f(x)$ の零点が $GF(P^m)$ において k 乗剰余である場合，$k \mid (P-1)$ かつ $k \nmid m$ であるならば，$GF(P)$ の k 乗非剰余元 i を用いて，既約多項式 $f(x)$ に $f(ix)$ なる線形的変数変換を施すことにより，$GF(P^m)$ において k 乗非剰余である零点をもつ既約多項式に変換することができる．

2.5.3 Example

Example2.5.3.1：$GF(3)$ 上の4次既約多項式 $f(x) = x^4 + x^2 + 2$ の零点は，$GF(3^4)$ において5乗剰余であり補題2.4.1.1より $f(x^5)$ は既約多項式とはならない．そこで，$f(x^5)$ を既約因数分解すると以下のようになる．

$$f(x^5) = (x^4+2x^2+2)\cdot(x^4+x+2)\cdot(x^4+x^3+x^2+2x+2)\cdot(x^4+2x^3+x^2+x+2)\cdot(x^4+2x+2)$$

ここで，すべての既約因数の中の x^4+2x^2+2 のみが依然その零点が5乗剰余であり，他の既約多項式は5乗剰余が取り除かれている（この場合，原始多項式となっている）． ■

2.6 原始多項式の導出法

M系列の発生等に用いられている原始多項式は，既約多項式の中の一つの特別なクラスであり特に有用なものである．しかしこれまで原始多項式の導出は既約多項式の原始性の判定により行われており，その判定結果が非原始であるならば別の既約多項式を新たに与えなければならず組織的な導出であるとは言いがたい．また，これまで原始多項式の組織的な導出法は与えられていない．

本節では，原始多項式について k 乗剰余性なる観点から考察することによりその性質を明らかにし，1つの既約多項式から同次の原始多項式を組織的に得る手法を与える．ここでは，定義2.2.3.1で定義される原始多項式の零点は $GF(P^m)$ の原始元であるということから，原始元の性質について簡単に紹介する．

$GF(P^m)$の1つの原始元をαとする．

$$\gcd(P^m - 1, i) = 1$$

を満たす正整数iを用いて，$GF(P^m)$のすべての原始元はα^iと表現できる．すなわち原始元は，性質2.2.1.2より$k \mid (P^m - 1)$なるすべての素数kについて$GF(P^m)$においてk乗非剰余となる．

また，α^iが$GF(P^m)$の原始元でないならば，

$$\gcd(P^m - 1, i) = k \neq 1$$

であり，性質2.2.1.2よりα^iはこの整数kに対して，k乗剰余となる．

したがって，既約多項式の原始性は$k \mid (P^m - 1)$なるすべての素数kについて，その零点がk乗非剰余であることを判定すれば良い．さらに，与えられた既約多項式の零点がk乗剰余であるならば，その剰余性を前節で与えたk乗剰余除去法により除去し，これを繰り返し行うことにより最終的には原始元を零点としてもつ同次の既約多項式を導出できる．すなわち，組織的に原始多項式を導出できることになる．

次項に，原始多項式の組織的な導出アルゴリズムを与える．

2.6.1 原始多項式導出アルゴリズム

本項では，1つの既約多項式から同次の原始多項式を得るまでのアルゴリズムを提案する．尚，本アルゴリズムにおいて，行き先の表示してないステップは次のステップに順序通り進むものとする．

STEP1-1: $GF(P)$上のm次単位既約多項式$f(x)$を与え，その零次係数をf_0とする．

STEP1-2: $P^m - 1$の因数分解を行う．ここで，その因数分解を以下のようであるとする．

$$P^m - 1 = k_1^{e_1} k_2^{e_2} \cdots k_r^{e_r}$$

ただし，$k_1, k_2, \cdots, k_r$は相異なる素数であり，$e_1, e_2, \cdots, e_r$は正整数であるとする．

STEP1-3: すべてのk_i $1 \leq i \leq r$に対し，

$$\rightarrow \text{STEP2} - 1$$

を行い，すべてのk_iに対してk_i乗非剰余である判定が得られたならば，そのときの$f(x)$が$GF(P)$上のm次原始多項式でありアルゴリズム終了．

STEP2-1: $k \mid (P-1)$である．

YES $\rightarrow$ STEP2 – 3

NO $\rightarrow$ STEP2 – 2

STEP2-2: $f(x^k)$のサイクル長がmである．

YES $\rightarrow$ STEP2 – 5

NO $\rightarrow$ STEP2 – 4

STEP2-3: $m(P-1)/k$が偶かつ，f_0が$GF(P)$においてk剰非剰余である．または，$m(P-1)/k$が奇かつ，f_0が$GF(P)$においてk剰剰余である．

YES $\rightarrow$ STEP2 – 4

NO $\rightarrow$ STEP2 – 5

STEP2-4: $f(x)$の零点はk剰非剰余である．

$\rightarrow$ STEP1 – 3

STEP2-5: $f(x)$の零点はk剰剰余である．

$\rightarrow$ STEP3 – 1

STEP3-1: $k \mid (P-1)$かつ，kがmを割り切らない．

YES $\rightarrow$ STEP3 – 2

NO $\rightarrow$ STEP3 – 3

STEP3-2: $GF(P)$のk剰非剰余元iを用い，$f(ix)$を新たな$f(x)$とする．

$\rightarrow$ STEP2 – 4

STEP3-3: $f(x^k)$を既約因数分解し，そのうちの1つを新たな$f(x)$とする．

$\rightarrow$ STEP2 – 1

2.6.2 Example

Example2.6.2.1：$GF(5)$ 上の2次既約多項式 $f(x) = x^2 + 3$ を用いて，$GF(5)$ 上の2次原始多項式を導出する．

まず，$5^2 - 1 = 2^3 \cdot 3$ であることから性質2.2.1.3より平方剰余性と3乗剰余性のみ考えればよい．ここで，$f(x)$ の零点に対して平方剰余性および3乗剰余性判定を行うと，平方非剰余であり3乗剰余であるという判定が得られる．そこで，非既約な多項式 $f(x^3)$ を既約因数分解することにより，

$$f(x^3) = (x^2 + 2) \cdot (x^2 + 4x + 2) \cdot (x^2 + x + 2)$$

となり，新たな $GF(5)$ 上の2次既約多項式 $f(x)$ として $x^2 + x + 2$ を選び再び3乗剰余性判定を行うと，3乗非剰余であると判定される．したがって，新たに得られた2次既約多項式 $f(x) = x^2 + x + 2$ は $GF(5)$ 上の2次原始多項式となる． ■

2.7 結言

本章では，これまで有限体の乗法的解析の一指標として用いられてきた位数なる概念に対し，今後暗号等の分野において用いられるであろう位数の大きな有限体におけるその非実用性を言及した．そして，位数なる概念に変わる新たな乗法的指標として，有限体理論における平方剰余性なる概念の一般拡張として捉えられる k 乗剰余性なる概念を定義し，その性質を明確にすることでその有用性を明確に示した．

本章では k 乗剰余性なる概念を用い，以下のことを示した．

1. 変数変換 $x = x^k$ およびその組み合わせによる無限個の組織的な高次既約多項式の導出法を与えた．

2. 変数変換 $x = x^k$ による既約多項式の導出の際に必要となる k 乗剰余性判定を，サイクル長なる概念を用いることにより容易に行えることを示し，従来の原始性判定法からの推測で与えられる k 乗剰余性判定法よりも，本方式の方がより有効であることを示した．

3. 与えられた既約多項式の零点に対し k 乗剰余性判定を行った結果が，k 乗剰余である場合には $x = x^k$ なる変数変換では高次の既約多項式が得られないことから，これをより実用的なものとするために変数変換および既約因数分解による k 乗剰余除去法を与えた．結果，与えられた既約多項式から必ず k 倍の次数の既約多項式を組織的に得ることができることを示した．

4. 既約多項式変遷の過程における零点のk乗剰余性に関する性質を明確にしたことにより，k乗剰余性判定およびk乗剰余除去が従来の位数なる概念に対しては位数の判定および位数の変換につながることから，これまで明確とされていなかった原始多項式の組織的な導出法をk乗剰余性なる概念を用いたことにより与えることができた．そして，これをアルゴリズムとして明確に示した．

第　3　章

有限体構造の加法的解析

第 3 章　有限体構造の加法的解析

3.1　緒言

誤り訂正符号のクラスとして代数的誤り訂正符号等があるが，その他多くの符号が有限体理論にその基礎を置く．これらは，有限体における元の加法的な閉性を用い誤り訂正のシステムを構築しているものがほとんどである．現代情報社会において，ＣＤ（Compact Disk）等の記録媒体に対する記録システムあるいは今日行われているパケット通信のような情報通信システムなど広く用いられている誤り訂正符号であるが，これらをより有効に用いることを考えたとき，有限体のその加法的な解析が必要となる．このように，有限体の加法的な性質についてみることは大変意義のあることであるが，これまでの有限体の加法的な解析は，トレース関数・随伴多項式に代表されるような体から体への写像という観点からの考察，あるいは多項式基底・正規基底に代表されるような体を表現する上で必要となる基底として特徴あるものを用いることによる考察など，ある意味でその概念のもつ性質が大いに反映された研究が多い[14][15]．

本章では，有限体を加法的に考察する上で**トレース**なる概念を加法的指標として位置づける．そして，この概念をより一般化したn**次トレース**なる概念を定義し，さらに**加法的自己回帰既約多項式**およびそれに付随する概念を新たに定義し，これらの性質を明確にする．これら概念を用い，加法的変数変換による既約多項式の導出に関する議論を中心として，その導出過程および変遷過程における性質を明確にすることにより，有限体を加法的に解析する．

はじめに，トレースなる概念を用いた$x = x^P - x$なる変数変換による標数Pの倍数次数の既約多項式の導出法を与える．そして，この手法に有限体上での形式微分および相反多項式なる概念を加えることにより，標数Pの倍数次数ごとの無限個の既約多項式を導出する手法を提案する．

トレースなる概念を用いた既約多項式の導出に際してトレースの値が非零の真性元が必要となることから，次にn次トレースなる概念を用いることにより，拡大体における任意元のトレースの値と有限体を表現するために用いる法多項式（既約多項式）の係数との関係を明確に与える式を示す．この式を用いることにより，拡大体の任意元のトレースの値の導出およびトレースの値が非零の真性元の特定ができることを示す．さらにこれを応用し，従来は多項式基底によるベクトル表現を用いての剰余類演算及び行列操作を施し連立合同式を解くなど大変煩雑な操作を必要としていた最小多項式の導出に関しても，拡大次数が標数よりも小さいような場合においては，本式を用いることにより大変容易な計算で任意元の最小多項式を特定できる手法を提案する．

最後に，トレースなる概念と加法的自己回帰既約多項式およびそれに付随する概念を組み合わ

せ，加法的変数変換$x = x^P - x$による既約多項式変遷の過程における性質を明確にする．その結果，素体の元iを用いた大変容易な加法的変数変換$x = x + i$および逆変数変換$x^P - x = x$により，1つの既約多項式からすべての同次およびその約数次数の既約多項式を零点の正規基底によるベクトル表現との対応を取りながら行えることを示し，これをアルゴリズムとして与える．

3.2 基礎的準備

本節では，有限体を加法的に解析する上で必要となる基礎的な準備を行う．

3.2.1 トレース

まずトレースなる概念の定義を明確にする．

定義（トレース）3.2.1.1：$GF(P)$上のm次拡大体$GF(P^m)$の元αに対し，αの$GF(P)$に関するトレースを$\mathrm{Tr}_{P^m|P}(\alpha)$とあらわし，

$$\mathrm{Tr}_{P^m|P}(\alpha) = \alpha + \alpha^P + \alpha^{P^2} + \cdots + \alpha^{P^{m-1}}$$

とする． ■

トレースなる概念は次のような性質をもつ．

性質3.2.1.2：$GF(P)$上のm次単位既約多項式$f(x)$の零点を$\omega \in GF(P^m)$，$m-1$次係数をf_{m-1}とするとき，

$$\mathrm{Tr}_{P^m|P}(\omega) = -f_{m-1}$$

である． ■

性質3.2.1.3：$GF(P)$上のm次単位既約多項式$f(x)$の零点を$\omega \in GF(P^m)$，$f(x+i)$の零点を$\tau \in GF(P^m)$とするとき，$f(x+i)$は$GF(P)$上のm次単位既約多項式であり，

$$\mathrm{Tr}_{P^m|P}(\omega) = \mathrm{Tr}_{P^m|P}(\tau) + m \cdot i$$

である．ここで，$0 \leq i \leq P-1$である． ■

性質3.2.1.4：$GF(P)$上のm次既約多項式$f(x)$を

$$f(x) = \sum_{i=0}^{m} f_i x^i \quad f_i \in GF(P)$$

とし，$f(x)$の零点を$\omega \in GF(P^m)$とするとき，$f(x)$の相反多項式$[f(x)]^*$の零点$\gamma = \omega^{-1}$のトレースの値は，

$$\mathrm{Tr}_{P^m|P}(\gamma) = -f_0^{-1} \cdot f'(0)$$

である．ここで，$f'(0)$とは$f(x)$を$GF(P)$上で形式微分したものに$x = 0$を代入したものであり，$f(x)$の1次係数である．

略証：$f(x)$の相反多項式を$[f(x)]^*$とすると，

$$[f(x)]^* = \sum_{i=0}^{m} f_{m-i} x^i$$

と表され，性質3.2.1.2からその零点γのトレースの値は$[f(x)]^*$を単位多項式化し，その$m-1$次係数により求まることから，

$$\mathrm{Tr}_{P^m|P}(\gamma) = -f_0^{-1} \cdot f_1$$

であり，f_1の値は$f(x)$を形式微分して$x = 0$を代入することにより求まる．

■

3.2.2 n次トレース

トレースなる概念を一般拡張した新たな概念として，**n次トレース**なる概念を以下に定義する．

定義（n次トレース）3.2.2.1：$GF(P)$上のm次拡大体$GF(P^m)$の任意元αに対し，次のようにm個の$GF(P)$に関する共役元の組を考える．

$$\{\alpha, \alpha^P, \cdots, \alpha^{P^{m-1}}\}$$

このとき，αのm個の共役元の中のn個の組すべての積を考え，その総和を元αの$GF(P^m)$における$GF(P)$に関する**n次トレース**と呼び$\mathrm{Tr}^{[n]}_{P^m|P}(\alpha)$と表す．ここで，$0 \leq n \leq m$である．尚，$\mathrm{Tr}^{[0]}_{P^m|P}(\alpha) = 1$とする．

■

このように定義されるn次トレースとは次のような特徴をもつ．

1. $GF(P)$上のm次単位既約多項式$f(x)$に対しその零点を$\omega \in GF(P^m)$とするとき，$GF(P)$に関する$GF(P^m)$の真性元ωのn次トレースの値は，$f(x)$の$m-n$次係数に$(-1)^n$を乗じたものである．すなわち，$\mathrm{Tr}^{[n]}_{P^m|P}(\omega)$は$GF(P)$の元になる．

2. 従来定義されているトレースとは本概念においては1次トレースとして定義され，また定数項である零次係数はm次トレースに$(-1)^m$を乗じたものとして定義できる．

また，有限体上でも考えられる形式微分の性質として次のような性質がある．

性質3.2.2.2：

$$[f(g(x))]' = f'(g(x)) \cdot g'(x)$$

■

3.2.3 加法的自己回帰既約多項式

加法的自己回帰既約多項式，加法的非自己回帰既約多項式および加法的自己回帰既約多項式集合を定義する．

定義（加法的自己回帰既約多項式他）3.2.3.1： $GF(P)$ 上の m 次既約多項式 $f(x)$ に対し，

$$f(x) = f(x+i), \quad 1 \leq i \leq P-1$$

となる場合，$f(x)$ を**加法的自己回帰既約多項式**と呼び，また

$$f(x) \neq f(x+i), \quad 1 \leq i \leq P-1$$

となる場合，$f(x)$ を**加法的非自己回帰既約多項式**と呼び，集合：

$$\{f(x), f(x+1), \cdots, f(x+(P-1))\}$$

を**加法的自己回帰既約多項式集合**と呼ぶ． ■

定義3.2.3.1のように，既約多項式に $x+i$ なる変数変換を施して得られる既約多項式の集合は，すべて等しい既約多項式の集合になるかあるいは，すべて相異なる既約多項式の集合になる．

証明(定義3.2.3.1)： 仮に，$GF(P)$ の非零元 s をもちいて $f(x)$ に $x = x+s$ なる変数変換を施したとき，

$$f(x) = f(x+s)$$

となったとすると，さらに変数変換を施したと考えれば，

$$f(x) = f(x+s) = f(x+2s)$$

となる．すなわち，これを繰り返し行うことにより，

$$f(x) = f(x+is), \quad 1 \leq i \leq P-1$$

である．結果，すべて等しい既約多項式もしくはすべて相異なる既約多項式となる． ■

定義3.2.3.1のようにして定義される加法的自己回帰既約多項式は次に示されるように標数倍の次数の既約多項式としてしか存在しない.

補題3.2.3.2：$GF(P)$上のm次既約多項式$f(x)$が加法的自己回帰既約多項式であるならば，$P \mid m$である. ■

証明(補題3.2.3.2)：$f(x)$が自己回帰既約多項式であるならばその零点を$\omega \in GF(P^m)$としたとき，その$GF(P)$に関する共役元の中に

$$\omega, \omega+1, \cdots, \omega+(P-1)$$

が含まれていることが分かる．したがって，$m-1$以下の適当な正整数sに対して，

$$\omega^{P^s} = \omega + 1 \tag{3.1}$$

と表せる．ゆえに，式(3.1)の両辺をP^s乗し，

$$\omega^{P^{2s}} = \omega^{P^s} + 1 = \omega + 2$$

となり，これを，P回繰り返すことにより，

$$\omega^{P^{Ps}} = \omega$$

である．したがって，ωは$GF(P^m)$の真性元であることより，

$$m \mid Ps$$

となるが，sは$m-1$以下の正整数であることより，$m \nmid s$であるから，

$$P \mid m$$

となる. ■

3.2.4 従来の最小多項式導出法

従来の最小多項式導出法を示す.

従来の最小多項式導出法：$GF(P^m)$において，$GF(P^m)$の元ωを用いた集合：

$$\{\omega^{m-1}, \omega^{m-2}, \cdots, \omega^0\}$$

が多項式基底をなすとする.

ここで，$GF(P^m)$の非零元βの最小多項式について考えてみる．仮に，β^iを多項式基底で表現したとき，

$$\beta^i = \sum_{j=0}^{m-1} S_{ij}\omega^j \quad for\ 0 \leq i \leq m$$

と表されるとする．ここで，S_{ij}は素体の元である．

このように表された$\beta^0, \beta^1, \cdots, \beta^m$を用い，次のような行列を考える．

$$B = \begin{bmatrix} S_{0\,0} & S_{0\,1} & \cdots & S_{0\,m-1} \\ S_{1\,0} & S_{1\,1} & \cdots & S_{1\,m-1} \\ \vdots & \vdots & & \vdots \\ S_{m\,0} & S_{m\,1} & \cdots & S_{m\,m-1} \end{bmatrix}$$

ここで，βの最小多項式を$g(x) = \sum_{i=0}^{m} C_i x^i$とすると，

$$g(\beta) = C_m\beta^m + \cdots + C_0\beta^0 = 0 \tag{3.2}$$

より，先に与えた行列式Bと，式(3.2)を用いて連立合同式として$C_0, \cdots, C_m$を解くことにより，βを零点とする最小多項式が求まる．ここで，最小多項式はその一意性より$C_m = 1$とする．

■

このように従来の最小多項式導出法は，$GF(P^m)$の一つの元βに対する最小多項式を一つ求めるのでさえ，β^iの基底による表現の計算（有限体上での多項式剰余演算），行列式（連立一次合同式）を解くという大変煩雑な操作を要する．

3.2.5 多項式基底・正規基底

拡大体を素体あるいは部分体上のベクトル空間として表現するためには，基底が必要となるがここでは代表的な有限体上の基底として，多項式基底および正規基底を紹介する．

まず，多項式基底は次のように定義される．

定義（多項式基底）3.2.5.1： $GF(P)$上のm次既約多項式$f(x)$の零点を$\alpha \in GF(P^m)$とするとき，その零点αを用いた集合：

$$\{\alpha^{m-1}, \alpha^{m-2}, \cdots, \alpha^0\}$$

は拡大体$GF(P^m)$において基底を成す．■

このことは，$GF(P)$上のm次既約多項式$f(x)$があるならば，必ず拡大体$GF(P^m)$を$GF(P)$上のm次元ベクトル空間として表現し得ることを別の言い方で述べているのに他ならない．

正規基底は次のように定義される．

定義（正規基底）3.2.5.2： $GF(P^m)$の真性元αに対し，αの$GF(P)$に関するm個の共役元の集合：

$$\{\alpha^{P^{m-1}}, \alpha^{P^{m-2}}, \cdots, \alpha^{P^0}\}$$

が$GF(P^m)$において基底を成すとき，これを正規基底と呼ぶ． ■

容易に分かるように，正規基底は元αの最小多項式の零点の組として特徴づけられる．しかし逆に，$GF(P)$上のm次既約多項式の零点の$GF(P)$に関するm個の共役元の組が必ずしも正規基底を成すとは限らない．

3.3 既約多項式の導出

前章の中で述べられている変数変換$x = x^k$による既約多項式の導出法では，標数倍の次数の既約多項式は導出できない．そこでこれまで，標数倍の次数の既約多項式の組織的な導出ということでいくつか研究がなされてきた[8][12][13]．

本節では，加法的指標として位置づけたトレースなる概念を基礎におき，まず標数Pによる$x = x^P - x$なる変数変換を用いることにより標数倍の次数の既約多項式の導出法を提案する．次に，これに有限体上での形式微分および相反多項式なる概念を加え，変数変換として素体の適当な非零元sを用いた$x = x^P - x + s$を用いることにより，標数倍の次数ごとの無限個の高次既約多項式の導出法を提案する．

3.3.1 変数変換$x = x^P - x$による既約多項式の導出

既約多項式に，標数Pを用いた変数変換$x = x^P - x$なる変数変換を施すことにより，新たにP倍の次数の既約多項式が得られる次の定理を示す．

定理3.3.1.1： $GF(P)$上のm次既約多項式$f(x)$があり，その零点をωとする．このとき，

$$\mathrm{Tr}_{P^m|P}(\omega) \neq 0$$

であるならば，すなわち$f(x)$の$m-1$次係数が非零であるならば，$f(x^P - x)$は$GF(P)$上のmP次既約多項式となる．（また，逆も成り立つ） ■

証明(定理3.3.1.1)：$f(x^P-x)$が$GF(P)$上のmP次の既約多項式であるためには，$g(x)=x^P-x-\omega$が$GF(P^m)$において既約であることを示せばよい．$g(x)$の零点をτとしたとき，

$$\tau^P-\tau=\omega$$

である．両辺をP乗し，これを繰り返す事により，以下のようになる．

$$\begin{aligned}
\tau^P &- \tau &&= \omega \\
\tau^{P^2} &- \tau^P &&= \omega^P \\
&&&\vdots \\
\tau^{P^m} &- \tau^{P^{m-1}} &&= \omega^{P^{m-1}}
\end{aligned}$$

上式の両辺をそれぞれ加えることにより，

$$\tau^{P^m}-\tau=\mathrm{Tr}_{P^m|P}(\omega) \tag{3.3}$$

である．仮に，$x^P-x-\omega$が$GF(P^m)$で既約ならば，τは$GF(P^{mP})$の真性元ゆえ$\tau^{P^m}\neq\tau$となり，

$$\mathrm{Tr}_{P^m|P}(\omega)\neq 0$$

である．

また，既約でないならば，τは$1\leq r<P$なる正整数rをもちいて，$GF(P^{rm})$に存在する．したがって，

$$\begin{aligned}
\tau^P &- \tau &&= \omega \\
\tau^{P^2} &- \tau^P &&= \omega^P \\
&&&\vdots \\
\tau^{P^{rm}} &- \tau^{P^{rm-1}} &&= \omega^{P^{rm-1}}
\end{aligned}$$

であり，両辺をそれぞれ加えることにより，

$$\tau^{P^{rm}}-\tau=r\mathrm{Tr}_{P^m|P}(\omega) \tag{3.4}$$

である．したがって，τが$GF(P^{rm})$の元であり，$\tau^{P^{rm}}=\tau$であるから，

$$r\mathrm{Tr}_{P^m|P}(\omega)=0$$

となる．$1\leq r<P$でありかつ標数がPであるため，

$$\mathrm{Tr}_{P^m|P}(\omega)=0$$

となる（対偶）．■

定理3.3.1.1を用いて標数倍の次数の既約多項式を新たに得るためには，元の既約多項式の零点のトレースの値が非零でなければならないことが分かる．逆に，$f(x)$ の零点ωの$GF(P)$ に関するトレースの値が零（すなわち，$f(x)$ の$m-1$次係数が零）の場合については以下のような補題が与えられる．

補題3.3.1.2：$GF(P)$ 上のm次既約多項式$f(x)$があり，その零点をωとする．このとき，

$$\mathrm{Tr}_{P^m|P}(\omega) = 0$$

すなわち$f(x)$ の$m-1$次係数が零であるならば，$f(x^P - x)$ は$GF(P)$ のP個の相異なるm次既約多項式の積となり，以下の関係をみたす．

$$f(x^P - x) = g(x)g(x+1)\cdots g(x+(P-1))$$

ここで，$g(x)$ を$f(x^P - x)$ の1つのm次既約因数多項式とする． ■

証明(補題3.3.1.2)：$f(x)$ に対して$x = x^P - x$なる変数変換を施すということから，

$$f(x^P - x) = (x^P - x - \omega)(x^P - x - \omega^P)\cdots(x^P - x - \omega^{P^{m-1}})$$

について考えればよく，

$$x^P - x - \omega^{P^i}, \quad 1 \le i \le m-1$$

のすべての零点は$x^P - x - \omega$の零点の$GF(P)$ に関する共役元であることから，以下$x^P - x - \omega$の零点について考えることにより本補題を証明する．

$x^P - x - \omega$の零点τは，

$$\tau^P - \tau - \omega = 0$$

を満たし，これを満たす元は，

$$\tau, \tau+1, \cdots, \tau+(P-1)$$

のP個の元である．またこれら$\tau + i \quad (i = 0, 1, \cdots, P-1)$ は，すべて同じ体に真性元として存在する．したがって，$x^P - x - \omega$が$GF(P^m)$ において非既約であるならば，Pが素数であることより，$GF(P^m)$ においてP個の1次既約多項式の積の形に既約因数分解される．さらにこれら零点$\tau + i$は相異なり，それぞれ$GF(P)$ に関してm個の共役元をもつ[1]．したがって，

$$f(x^P - x) = g_0(x)g_1(x)\cdots g_{P-1}(x)$$

[1]なぜならば，仮に$\tau + i$の共役元の集合の中にτが含まれるとするならば，$\tau + i$を$x^P - x$に代入したときの値の集合すなわち，ωの共役元の集合の中にωが2つ含まれることになり矛盾する．

と表現でき，$g_i(x)$ はそれぞれ $\tau+i$ の最少多項式であり $GF(P)$ 上の m 次既約多項式となる．また，これらは以下の関係を満たす．

$$g_i(x) = g_0(x-i)$$

■

本項の結果から，$x = x^P - x$ なる変数変換により既約多項式を導出するためには，トレースの値が非零の元を零点としてもつ既約多項式が必要である．また，定理3.3.1.1および補題3.3.1.2は，後述の正規基底によるベクトル表現に対応する最小多項式テーブルの作成の際に再び用いる．

3.3.2 変数変換 $x = x^P - x + s$ および相反多項式による無限個の既約多項式の導出

前項で述べたトレースなる概念を用いた標数倍の次数の既約多項式の導出法を，無限個の組織的な導出とする次の定理を示す．

定理3.3.2.1：$GF(P)$ 上の m 次既約多項式 $f_{(0)}(x)$，$f_{(0)}(x)$ の零点 $\omega_{(0)} \in GF(P^m)$ および $GF(P)$ の適当な非零元 s が，次の2つの条件：

1. $f'_{(0)}(s) \neq 0$.
2. $\mathrm{Tr}_{P^m|P}(\omega_{(0)}) \neq m \cdot s$.

を満たすとき，

$$f_{(i)}(x) = [f_{(i-1)}(x^P - x + s)]^*, \quad i \geq 1$$

で表される $f_{(i)}(x)$ は $m \cdot P^i$ 次既約多項式である．ここで，$f'_{(0)}(s)$ は $f_{(0)}(x)$ を $GF(P)$ 上で形式微分し $x = s$ を代入したものである．また，$[f_{(i-1)}(x^P - x + s)]^*$ は $f_{(i-1)}(x^P - x + s)$ の相反多項式である．■

証明(定理3.3.2.1)：本定理条件(1)，(2)を満たす s に対して，次のような命題が成立する．ただし，命題の $k = 0$ における条件は本定理の条件(1)，(2)に等しいことに注意されたい．この命題を帰納的に用いることにより本定理が証明される．

命題：$k \geq 0$ なる整数 k に対し，$GF(P)$ 上の mP^k 次既約多項式 $f_{(k)}(x)$ およびその零点 $\omega_{(k)} \in GF(P^{mP^k})$ が，

(1') $f'_{(k)}(s) \neq 0$.

(2') $\mathrm{Tr}_{P^{mP^k}|P}(\omega_{(k)}) \neq mP^k \cdot s$.

を共に満たすとき，

$$f_{(k+1)}(x) = [f_{(k)}(x^P - x + s)]^*$$

で与えられる$f_{(k+1)}(x)$は，$GF(P)$上のmP^{k+1}次既約多項式であり，$f_{(k+1)}(x)$およびその零点$\omega_{(k+1)} \in GF(P^{mP^{k+1}})$は，

(1") $f'_{(k+1)}(s) \neq 0$.

(2") $\mathrm{Tr}_{P^{mP^{k+1}}|P}(\omega_{(k+1)}) \neq mP^{k+1} \cdot s$.

を満たす．(命題終)

命題の証明：まず，$f_{(k+1)}(x)$が$GF(P)$上のmP^{k+1}次既約多項式となることを示す．$f_{(k)}(x)$が条件(2')を満たすことから，性質3.2.1.3より$f_{(k)}(x+s)$の零点$\tau_{(k)} \in GF(P^{mP^k})$のトレースの値は非零であり，補題3.3.1.1より$f_{(k)}(x^P - x + s)$はmP^{k+1}次既約多項式となり，その相反多項式である$f_{(k+1)}(x)$も$GF(P)$上のmP^{k+1}次既約多項式となる．

次に，$f_{(k+1)}(x)$が条件(2")を満たすことを示す．$f_{(k+1)}(x)$の零点$\omega_{(k+1)}$のトレースの値をみるためには，$f_{(k+1)}(x)$が$f_{(k)}(x^P - x + s)$の相反多項式であることから，性質3.2.1.4より$f_{(k)}(x^P - x + s)$を形式微分し$x = 0$を代入する．

$$\begin{aligned}
[f_{(k)}(x^P - x + s)]' &= f'_{(k)}(x^P - x + s) \cdot \quad (x^P - x + s)' \\
&= -f'_{(k)}(x^P - x + s)
\end{aligned}$$

上式に$x = 0$を代入した値$-f'_{(k)}(s)$を求めるとこれは(1')より非零である．そしてさらに，$f_{(k)}(x^P - x + s)$の零次係数も非零であるため，$\omega_{(k+1)}$の$GF(P)$に関するトレースの値は非零となる．したがって，$\deg f_{(k+1)}(x) = mP^{k+1}$より，

$$\mathrm{Tr}_{P^{mP^{k+1}}|P}(\omega_{(k+1)}) \neq mP^{k+1} \cdot s = 0$$

となり$f_{(k+1)}(x)$の零点$\omega_{(k+1)}$は条件(2")を満たす．

次に，$f_{(k+1)}(x)$が条件(1")を満たすことを示す．$f_{(k)}(x)$を，

$$f_{(k)}(x) = \sum_{i=0}^{mP^k} f_i x^i \quad f_i \in GF(P)$$

とすると，$\deg f_{(k+1)}(x) = mP^{k+1}$より，

$$\begin{aligned}
f_{(k+1)}(x) &= [f_{(k)}(x^P - x + s)]^* \\
&= f_{(k)}(x^{-P} - x^{-1} + s) \cdot x^{mP^{k+1}}
\end{aligned}$$

$$= [\sum_{i=0}^{mP^k} f_i(x^{-P} - x^{-1} + s)^i] \cdot x^{mP^{k+1}}$$
$$= \sum_{i=0}^{mP^k} [f_i(1 - x^{P-1} + sx^P)^i \cdot x^{mP^{k+1}-iP}]$$

となり，$(x^{mP^{k+1}-iP})' = 0$であることを用い$f'_{(k+1)}(x)$を求めると，

$$f'_{(k+1)}(x) = \sum_{i=0}^{mP^k} f_i[-i(P-1) \cdot (1 - x^{P-1} + sx^P)^{i-1} \cdot x^{P-2} \cdot x^{mP^{k+1}-iP}]$$

となる．$s^{P-1} = 1$，$s^P = s^1$，$-(P-1) = 1$より，

$$f'_{(k+1)}(s) = \sum_{i=0}^{mP^k} f_i[i(1 - s^{P-1} + s \cdot s^P)^{i-1} \cdot s^{P-2} \cdot s^{mP^{k+1}-iP}]$$
$$= \sum_{i=0}^{mP^k} f_i \cdot i \cdot s^{2(i-1)-2+m-i}$$
$$= s^{m-3} \sum_{i=0}^{mP^k} f_i \cdot i \cdot s^{i-1}$$
$$= s^{m-3} \cdot f'_{(k)}(s)$$

となり，$s \neq 0$および(1')より$f'_{(k+1)}(s) \neq 0$である．ゆえに，$f_{(k+1)}(x)$は形式微分に対する条件(1")を満たす．(命題の証明終)

■

$GF(P)$上のm次既約多項式$f(x)$，その零点ωに対して，$GF(P)$の一つの非零元sが定理3.3.2.1条件(1)，(2)を満たすならば，$x = x^P - x + s$なる変数変換とその相反多項式をとるという操作を繰り返し行うことにより，標数倍の次数ごとの無限個の高次既約多項式を組織的に導出できる．しかし例えば，初期値として与えられる既約多項式$f_{(0)}(x)$の次数mが標数の倍数でかつその零点のトレースの値が零のような場合には，いかなる標数体の非零元sに対しても条件(2)は満たし得ない．そのときは，新たな$f_{(0)}(x)$を必要とする．

3.3.3 Example

Example3.3.3.1：$GF(3)$上の2次の既約多項式として$f_{(0)}(x) = x^2 + x + 2$を考える．この$f_{(0)}(x)$に対して$s = 2$とすると，定理3.3.2.1の2つの条件を満たす．したがって，

$$f_{(0)}(x) = 112$$

$$
\begin{aligned}
f_{(1)}(x) &= 1221202 \\
f_{(2)}(x) &= 1202110100222202001 \\
f_{(3)}(x) &= 1212020000220201212\cdots
\end{aligned}
$$

というように既約多項式が得られていく[2]. ■

3.4 トレース非零元の導出

前節のトレースなる概念を用いた標数倍の次数ごとの組織的な既約多項式の導出の際，トレースの値が非零の元を零点としてもつ既約多項式を定理3.3.1.1では必要であり，またそれを応用した定理3.3.2.1では必要とする場合がある．このように，トレースの値が非零であるような元の特定あるいは導出は大変重要なこととなる．

そこで本節では，トレースの値が非零の真性元の特定を目的として，新たに導入したn次トレースなる概念を用いることにより，まず有限体を表現するのに必要となる法多項式（既約多項式）の係数とn次トレースとの関係を明確に示す式を与える．そして，これを用いることにより拡大体の任意元のトレースの値の特定およびトレースの値が非零となる真性元の特定に関する考察を行う．さらに，これまで大変煩雑な操作を必要としてきた最小多項式の導出という問題に対し，拡大次数mが標数Pよりも小さいような場合においては大変簡単な計算によりその導出が行えることを示す．

尚，本節を通して従来のトレース$\mathrm{Tr}_{P^m|P}(\omega)$は$\mathrm{Tr}^{[1]}_{P^m|P}(\omega)$と統一して表記することにする．

3.4.1 トレース非零元の導出（一般論）

本章基礎的準備において定義したn次トレースなる概念を用いることにより，$GF(P^m)$の真性元ωの共役元によるn次トレースと，ωにより構成される多項式基底の各要素の1次トレースの値との相互関係を示す定理を与える．

前準備として次のような表記法を与える．

準備：$GF(P^m)$の真性元ωの$GF(P^m)$における$GF(P)$に関するn次トレースは，m個の共役元の中のn個の元の組み合わせの積で表わされる${}_mC_n$個の項の和により得られるが，その${}_mC_n$個の項の中でω^{Pj}が含まれている項の総和の部分を，

$$S_j\ of\ \mathrm{Tr}^{[n]}_{P^m|P}(\omega)$$

[2]既約多項式は右側を低次として係数のみ表示している．

含まれない項の総和の部分を，

$$S_j^*\ of\ \mathrm{Tr}^{[n]}_{P^m|P}(\omega)$$

と表記する．この表記に従えば，

性質3.4.1.1：

$$\mathrm{Tr}^{[n]}_{P^m|P}(\omega) = (S_j\ of\ \mathrm{Tr}^{[n]}_{P^m|P}(\omega)) + (S_j^*\ of\ \mathrm{Tr}^{[n]}_{P^m|P}(\omega))$$

■

性質3.4.1.2：

$$S_j\ of\ \mathrm{Tr}^{[n]}_{P^m|P}(\omega) = \omega^{Pj} \cdot (S_j^*\ of\ \mathrm{Tr}^{[n-1]}_{P^m|P}(\omega))$$

■

性質3.4.1.3：

$$S_j^*\ of\ \mathrm{Tr}^{[0]}_{P^m|P}(\omega) = 1$$

■

という性質が成り立つ．

以上のような準備を踏まえて，ωの共役元によるn次トレースとωにより構成される多項式基底の各要素の1次トレースの値との関係を与える次の定理を示す．

定理3.4.1.4： $GF(P^m)$の多項式基底を真性元ωを用いて，

$$\{\omega^{m-1}, \omega^{m-2}, \cdots, \omega^0\}$$

とするとき，$\mathrm{Tr}^{[1]}_{P^m|P}(\omega^s)$の値は次のような式で表される．ここで，$0 \leq s \leq m$とする．$s=0$および$s=1$のときは，

$$\begin{aligned} \mathrm{Tr}^{[1]}_{P^m|P}(\omega^0) &= m \\ \mathrm{Tr}^{[1]}_{P^m|P}(\omega^1) &= \mathrm{Tr}^{[1]}_{P^m|P}(\omega^1) \end{aligned}$$

であり，$2 \leq s \leq m$のときは，

$$\mathrm{Tr}^{[1]}_{P^m|P}(\omega^s) = \sum_{i=1}^{s-1}\{(-1)^{i+1} \cdot \mathrm{Tr}^{[i]}_{P^m|P}(\omega) \cdot \mathrm{Tr}^{[1]}_{P^m|P}(\omega^{s-i})\} - (-1)^s \cdot s \cdot \mathrm{Tr}^{[s]}_{P^m|P}(\omega) \quad (3.5)$$

である．■

証明(定理3.4.1.4)：$s=0$および$s=1$のときは自明であるので，$2\leq s\leq m$のときの式について証明する．

先に示した表記法を用いることにより，式(3.5)の右辺第1項は以下のように変形できる．

$$\begin{aligned}
&\sum_{i=1}^{s-1}\{(-1)^{i+1}\cdot \mathrm{Tr}^{[i]}_{P^m|P}(\omega)\cdot \mathrm{Tr}^{[1]}_{P^m|P}(\omega^{s-i})\}\\
=&\sum_{i=1}^{s-1}\{\sum_{j=0}^{m-1}(-1)^{i+1}\cdot \mathrm{Tr}^{[i]}_{P^m|P}(\omega)\cdot\omega^{(s-i)P^j}\}\\
=&\sum_{i=1}^{s-1}\{\sum_{j=0}^{m-1}(-1)^{i+1}\cdot[(S_j\ of\ \mathrm{Tr}^{[i]}_{P^m|P}(\omega))+(S_j^*\ of\ \mathrm{Tr}^{[i]}_{P^m|P}(\omega))]\cdot\omega^{(s-i)P^j}\}\\
=&\sum_{i=1}^{s-1}\{\sum_{j=0}^{m-1}(-1)^{i+1}\cdot[\omega^{P^j}(S_j^*\ of\ \mathrm{Tr}^{[i-1]}_{P^m|P}(\omega))+(S_j^*\ of\ \mathrm{Tr}^{[i]}_{P^m|P}(\omega))]\cdot\omega^{(s-i)P^j}\}\\
=&\sum_{i=1}^{s-1}\{\sum_{j=0}^{m-1}(-1)^{i+1}\cdot[\omega^{(s-(i-1))\cdot P^j}(S_j^*\ of\ \mathrm{Tr}^{[i-1]}_{P^m|P}(\omega))+\omega^{(s-i)\cdot P^j}(S_j^*\ of\ \mathrm{Tr}^{[i]}_{P^m|P}(\omega))]\}
\end{aligned}$$

$\sum_i$と$\sum_j$の順序を逆にし，iに関して分解するならば，

$$=\sum_{j=0}^{m-1}\omega^{s\cdot P^j}(S_j^*\ of\ \mathrm{Tr}^{[0]}_{P^m|P}(\omega))+(-1)^s\sum_{j=0}^{m-1}\omega^{P^j}(S_j^*\ of\ \mathrm{Tr}^{[s-1]}_{P^m|P}(\omega)) \tag{3.6}$$

となる．ここで，式(3.6)の第1項は，性質3.4.1.3より，

$$\sum_{j=0}^{m-1}\omega^{s\cdot P^j}(S_j^*\ of\ \mathrm{Tr}^{[0]}_{P^m|P}(\omega))=\mathrm{Tr}^{[1]}_{P^m|P}(\omega^s)$$

となる．また性質3.4.1.2より，式(3.6)の第2項は定数Aを用い，

$$\begin{aligned}
(-1)^s\sum_{j=0}^{m-1}\omega^{P^j}(S_j^*\ of\ \mathrm{Tr}^{[s-1]}_{P^m|P}(\omega)) &= (-1)^s\sum_{j=0}^{m-1}(S_j\ of\ \mathrm{Tr}^{[s]}_{P^m|P}(\omega)) \qquad (3.7)\\
&= (-1)^s\cdot A\cdot \mathrm{Tr}^{[s]}_{P^m|P}(\omega)
\end{aligned}$$

となることは容易にわかる．そこで，Aを特定しなければならない．

$S_j\ of\ \mathrm{Tr}^{[s]}_{P^m|P}(\omega)$の項数は，

$${}_{m-1}\mathrm{C}_{s-1}$$

である．したがって式(3.7)右辺の項数は，$0\leq j\leq m-1$まで変化させることより，

$${}_{m-1}\mathrm{C}_{s-1}\ \times m$$

となる．ここで，$\mathrm{Tr}^{[s]}_{P^m|P}(\omega)$の項数は

$${}_m\mathrm{C}_s$$

であるから，

$$\begin{aligned} A &= ({}_{m-1}\mathrm{C}_{s-1} \times m)/{}_{m}\mathrm{C}_{s} \\ &= \frac{(m-1)! \times m}{(s-1)! \cdot (m-1-(s-1))!} \times \frac{s! \times (m-s)!}{m!} \\ &= s \end{aligned}$$

となる．ゆえに，式(3.6)の第2項は

$$(-1)^s \cdot s \cdot \mathrm{Tr}^{[s]}_{P^m|P}(\omega)$$

である．したがって，式(3.5)を得る． ■

定理3.4.1.4を用いることにより，

$$\mathrm{Tr}^{[1]}_{P^m|P}(\omega^i) \quad (0 \leq i \leq m)$$

の値は次のように求められる．

$GF(P^m)$の真性元ωの最小多項式$f(x)$を

$$f(x) = x^m + f_{m-1}x^{m-1} + \cdots + f_1 x + f_0$$

$$f_i \in GF(P), \quad 0 \leq i \leq m-1$$

としたとき，

$$\mathrm{Tr}^{[n]}_{P^m|P}(\omega) = (-1)^n f_{m-n}$$

となるため，

$s = 2$

$$\mathrm{Tr}^{[1]}_{P^m|P}(\omega^2) = f^2_{m-1} - 2f_{m-2}$$

$s = 3$

$$\mathrm{Tr}^{[1]}_{P^m|P}(\omega^3) = -f_{m-1} \cdot \mathrm{Tr}^{[1]}_{P^m|P}(\omega^2) + f_{m-2} \cdot f_{m-1} - 3f_{m-3}$$

$s = 4$

$$\vdots$$

として求まる．定理3.4.1.4は，文献[16]の結果に対して係数比較を行うことにより出されると考えられるが，本定理ではn次トレースなる概念によって最小多項式の係数をその零点の組み合せの積の和の形として陽に与えたことにより，トレースの値そのものも陽に求めることができていると共に，種々の応用が考えられる．その応用を次項以降で考察する．

3.4.2 トレース非零元の導出（特定の形を有する既約多項式）

前項で与えた定理3.4.1.4により，$GF(P^m)$ の真性元ωにより構成される多項式基底の各要素ω^iの係数体に関するトレースの値はωの最小多項式 $f(x)$ の $m-1$ 次から $m-i$ 次までの係数により明確に特定されることがわかる．従って，最高次数m 未満の次数の係数で最初に非零となる次数に対応する多項式基底の要素がω^0に次ぐトレース非零の要素となる[3]．(但し，定理3.4.1.4の式(3.5) 最終項には重みsが乗じられているため，$(m-(P$の倍数$))$ 次項が最初の非零項となっていたとしても，それに対応する多項式基底の要素のトレースの値はPが乗じられ零となることに注意する．)

このようにしてトレース非零の元を特定し，その元が真性元でないならば[4]その元にそれまでのトレースの値が零の真性元を加える等の処理を行えばよい．特に以下に挙げるような既約多項式についてはより詳しく考察できる．

Example1: 前章で示した変数変換$x=x^k$による既約多項式導出の定理2.3.1.1を再掲する．

定理2.3.1.1： $f(x)$ を $GF(P)$ 上の m 次既約多項式とし，その零点は $GF(P^m)$ の真性元ωであるとする．このとき $k \mid (P^m-1)$ なる素数kで，ωが $GF(P^m)$ においてk乗非剰余であると判定されたとき，このkを用いた $f(x^k)$ は $GF(P)$ で既約である．またその逆も成り立つ． ■

定理2.3.1.1により得られる既約多項式は変数変換の形からもわかるようにkの倍数次にしか非零係数をもち得ない．従って，定理3.4.1.4より，この既約多項式 $f(x^k)$ の零点τを用いて多項式基底を構成した際，τ^{ki}というような基底の要素のみ係数体に関するトレースの値が非零となることが容易に分かる．ここで，τ^{ki}は，$\tau^k=\omega$より部分体の元である．ゆえに，τを用いて構成される多項式基底の要素の中にはトレース非零の真性元は含まれない．このようなとき，トレース非零の真性元が必要ならば，τは真性元であることからトレース非零の部分体の元τ^{ki}を用いた$\tau+\tau^{ki}$などを用いればよい．

Example2: P-polynomial なる概念を用いて既約多項式を得る次の定理を紹介する．

ここで，P-polynomial なる概念の定義をしめす．

定義3.4.2.1： 次のような多項式 $L(x)$

$$L(x)=\sum_{i=0}^{m} S_i x^{P^i} \quad S_i \in GF(P)$$

を，$GF(P)$ 上の linearized-polynomial または P-polynomial とよぶ． ■

[3] $P \mid m$ のときは，ω^0のトレースの値も零となる．

[4] サイクル長なる概念により容易に判定できる．

上記定義に示されるP-polynomialに対し次のような定理が与えられる．

定理3.4.2.2[5]：$f(x)$を$GF(P)$上の既約多項式とするとき，$f(x)$のP-polynomialを$L_f(x)$とするならば，$L_f(x)/x$のすべての既約因数多項式の次数は$f(x)$の位数に等しい．■

上記定理において$f(x)$として原始多項式を用いることにより得られる既約多項式$L_f(x)/x$は，最高次から数えてPの倍数間隔でしか非零係数が現れ得ないという特徴をもつ．すなわち，既約多項式$L_f(x)/x$の零点をτとするときτ^{Pi}なる形で表される元のみトレースの値が非零となる可能性をもつことが定理3.4.1.4より分かる．しかし，式(3.5)においてτ^{Pi}のトレースの値を求めるときには必ず最終項で重みPiが乗じられるため，τ^{Pi}なる元は係数が非零の項の次数に対応する元であるにもかかわらずそのトレースの値が零となるということがみてとれる．すなわち，このような元τにより構成される多項式基底の要素でトレースの値が非零となるのは$\tau^0=1$のみである．このようなときトレースの値が非零の真性元が必要ならば$\tau+1$などを用いればよい．

3.4.3 最小多項式の導出法

定理3.4.1.4により，次のような関係式を導くことができる．$GF(P)$のm次既約多項式$f(x)$の零点をωとして，$s=1$に対して，

$$\mathrm{Tr}^{[1]}_{P^m|P}(\omega)=\mathrm{Tr}^{[1]}_{P^m|P}(\omega) \tag{3.8}$$

であり，$s=2,\cdots m$に対して，

$$\mathrm{Tr}^{[s]}_{P^m|P}(\omega)=(-1)^s\cdot s^{-1}\cdot\{-\mathrm{Tr}^{[1]}_{P^m|P}(\omega^s)+\sum_{i=1}^{s-1}(-1)^{i+1}\cdot\mathrm{Tr}^{[i]}_{P^m|P}(\omega)\cdot\mathrm{Tr}^{[1]}_{P^m|P}(\omega^{s-i})\} \tag{3.9}$$

となる．式(3.8)，(3.9)のωの部分に任意真性元β（多項式基底$\{\omega^{m-1},\omega^{m-2},\cdots,\omega^0\}$によるベクトル表現として）を与え，$s=1,\cdots,m$まで各々の値を求めることにより，$\mathrm{Tr}^{[s]}_{P^m|P}(\beta)$が$\beta$の最小多項式の$m-s$次係数の$(-1)^s$倍を意味することから，$\beta$の最小多項式の係数を$m-1$次係数から順次計算により容易に求めることができる．

このように，定理3.4.1.4の式(3.5)を変形することにより，拡大次数が標数よりも小さいような有限体[5]における任意元の最小多項式特定にも用いることができる．以下に，真性元および部分体の元の場合の最小多項式特定の例を挙げる．

Example3.4.3.1：$GF(7)$上の4次既約多項式$f(x)=x^4+5x^2+5x+5$の零点ωに対し，ω^2の最小多項式を求める．まず，ω^2の1次トレースを求める．すなわち，定理3.4.1.4より，

$$\mathrm{Tr}^{[1]}_{7^4|7}(\omega^2)=\mathrm{Tr}^{[1]}_{7^4|7}(\omega)^2-2\times\mathrm{Tr}^{[2]}_{7^4|7}(\omega)=4$$

[5]このような条件が付加されるのは，定理3.4.1.4の式(3.5)の最終項に重みPが乗じられる場合が必ずあり，式変形の際の標数Pの乗法に関する逆元P^{-1}を考え得ないためである．

となり，ω^2の最小多項式の3次係数が$-4=3$になる．

つぎに，ω^2の2次トレースを求める．すなわち，以降は式(3.9)を用い，

$$\begin{aligned}\mathrm{Tr}^{[2]}_{7^4|7}(\omega^2) &= 2^{-1}(-\mathrm{Tr}^{[1]}_{7^4|7}(\omega^4)+\mathrm{Tr}^{[1]}_{7^4|7}(\omega^2)^2)\\ &= 0\end{aligned}$$

より，ω^2の最小多項式の2次係数が0になる．

つぎに，ω^2の3次トレースを求める．すなわち，

$$\begin{aligned}\mathrm{Tr}^{[3]}_{7^4|7}(\omega^2) &= -3^{-1}(-\mathrm{Tr}^{[1]}_{7^4|7}(\omega^6)+\mathrm{Tr}^{[1]}_{7^4|7}(\omega^2)\cdot\mathrm{Tr}^{[1]}_{7^4|7}(\omega^4)-\mathrm{Tr}^{[2]}_{7^4|7}(\omega^2)\cdot\mathrm{Tr}^{[1]}_{7^4|7}(\omega^2))\\ &= 3\end{aligned}$$

より，ω^2の最小多項式の1次係数が$-3=4$になる．

最後に，ω^2の4次トレースを求める．すなわち，

$$\begin{aligned}\mathrm{Tr}^{[4]}_{7^4|7}(\omega^2) &= 4^{-1}(-\mathrm{Tr}^{[1]}_{7^4|7}(\omega^8)+\mathrm{Tr}^{[1]}_{7^4|7}(\omega^2)\cdot\mathrm{Tr}^{[1]}_{7^4|7}(\omega^6)\\ &\quad -\mathrm{Tr}^{[2]}_{7^4|7}(\omega^2)\cdot\mathrm{Tr}^{[1]}_{7^4|7}(\omega^4)+\mathrm{Tr}^{[3]}_{7^4|7}(\omega^2)\cdot\mathrm{Tr}^{[1]}_{7^4|7}(\omega^2))\\ &= 4\end{aligned}$$

より，ω^2の最小多項式の0次係数が4になる．

したがって，ω^2の最小多項式$g(x)$は

$$g(x)=x^4+3x^3+4x+4$$

となる． ■

次に，部分体の元の最小多項式特定の例を挙げる．

Example3.4.3.2：$GF(7)$上の4次既約多項式$f(x)=x^4+x^2+3$の零点ωに対し，真部分体$GF(7^2)$の真性元ω^2の最小多項式を求める．($GF(7^2)$の元であることはサイクル長なる概念により判定できる．) ここで，ω^2の最小多項式は2次になることに注意する．

まず，ω^2の$GF(7^2)$における$GF(7)$に関する1次トレース$\mathrm{Tr}^{[1]}_{7^2|7}(\omega^2)$を求める．定理3.4.1.4より，

$$\mathrm{Tr}^{[1]}_{7^4|7}(\omega^2)=\mathrm{Tr}^{[1]}_{7^4|7}(\omega)^2-2\times\mathrm{Tr}^{[2]}_{7^4|7}(\omega)=5$$

となるが，これは$GF(7^4)$における$GF(7)$に対するトレースの値であるから，ω^2の1次トレースの値$\mathrm{Tr}^{[1]}_{7^2|7}(\omega^2)$は，

$$\mathrm{Tr}^{[1]}_{7^2|7}(\omega^2) = 5 \times 2^{-1} = 6$$

となり，ω^2の最小多項式の1次係数が$-6 = 1$になる．

つぎに，ω^2の$GF(7^2)$における$GF(7)$に関する2次トレースを求める．すなわち，以降は式(3.9)を用い，

$$\mathrm{Tr}^{[2]}_{7^2|7}(\omega^2) = 2^{-1}(\mathrm{Tr}^{[1]}_{7^2|7}(\omega^2)^2 - \mathrm{Tr}^{[1]}_{7^2|7}(\omega^4))$$

を求めることになる．(このように，真部分体$GF(7^2)$における式になることに注意する．)ここで，$\mathrm{Tr}^{[1]}_{7^2|7}(\omega^4)$を求める必要がある．このように，求める必要のある元も必ずω^4のように真部分体$GF(7^2)$の元となり，$GF(7^2)$における$GF(7)$に関するトレースの値を求めることになる．これも先と同様にして，

$$\mathrm{Tr}^{[1]}_{7^2|7}(\omega^4) = \mathrm{Tr}^{[1]}_{7^4|7}(\omega^4) \times 2^{-1}$$

であり，本提案法により$\mathrm{Tr}^{[1]}_{7^4|7}(\omega^4) = 4$と求まることから，

$$\mathrm{Tr}^{[1]}_{7^2|7}(\omega^4) = 4 \times 2^{-1} = 2$$

となる．よって

$$\mathrm{Tr}^{[2]}_{7^2|7}(\omega^2) = 3$$

となる．

したがって，ω^2の最小多項式$g(x)$は

$$g(x) = x^2 + x + 3$$

となる． ■

3.5 最小多項式ー正規基底表現対応表の生成

従来，多項式基底等によるベクトル表現に対応する最小多項式の特定は，本章基礎的準備でも述べたように大変煩雑な操作が必要となる．すべてのベクトル表現に対するすべての最小多項式の特定となると，その計算量は最小多項式の個数倍となり現実的には無理であるといってもよいであろう．

本節では，$x = x^P - x$なる変数変換後の多項式が既約・非既約となる際の性質を加法的自己回帰既約多項式とそれに付随する概念およびその性質を用いることにより明確にする．そして，既

約多項式変遷の過程における特徴をこれら加法的観点から明確に捉えることにより，正規基底による元のベクトル表現とそれに対応する最小多項式テーブルの一生成法を提案する．本手法により，すべてのベクトル表現と最小多項式の対応がとれることはもとより，拡大次数のすべての約数次数のすべての既約多項式が組織的に得られることに注意されたい．

3.5.1 基本的概念

従来の最小多項式導出法は，ある既約多項式の零点を用いた多項式基底によるベクトル表現に対して有限体上での剰余類演算を施し行列を作成し，その行列に対して行操作等を施し，連立合同式を解いて最小多項式との対応づけを行うという大変煩雑であり，計算量を必要とする方法である．

しかし本節で提案する最小多項式導出法は，元の正規基底によるベクトル表現に対して，容易な加法的変数変換および逆変数変換を用いて最小多項式を導出するという大変計算量の少ない手法であり，次項においてアルゴリズムとして提案するにあたって本項ではその基本概念を示す．

最小多項式導出： $GF(P)$ 上の加法的非自己回帰既約多項式 $f(x)$ に対して，その加法的自己回帰既約多項式集合：

$$\{f(x), f(x+1), \cdots, f(x+(P-1))\}$$

を考えその総積を考えてみる．すなわち，

$$F(x) = \prod_{i=0}^{P-1} f(x+i)$$

である．ここで，$f(x)$ の零点を $\omega \in GF(P^m)$ とすると，

$$\begin{aligned} F(x) &= \prod_{i=0}^{P-1}[\prod_{j=0}^{m-1}(x+i-\omega^{P^j})] \\ &= \prod_{j=0}^{m-1}[\prod_{i=0}^{P-1}(x-\omega^{P^j}+i)] \\ &= \prod_{j=0}^{m-1}((x-\omega^{P^j})^P-(x-\omega^{P^j})) \\ &= \prod_{j=0}^{m-1}(x^P-x-(\omega^{P^{j+1}}-\omega^{P^j})) \end{aligned}$$

である[6]．ここで，

$$\omega^P - \omega = \tau \tag{3.10}$$

[6] $f(x)$ は単位多項式であるものとする．

とすると，

$$F(x) = \prod_{j=0}^{m-1} (x^P - x - \tau^{P^j})$$

となるから，$F(x)$ は $x^P - x = x$ で変数変換が可能となる（今後，逆変数変換と呼ぶ）．したがって，$F(x) = g(x^P - x)$ とかんがえると，

$$g(x) = \prod_{j=0}^{m-1} (x - \tau^{P^j})$$

となり，τ は $g(x)$ の零点である．では，この $g(x)$ はどのような多項式になるかを次に考えてみると，式(3.10)より τ が $GF(P^m)$ の元であることは容易に分かる．ここで仮に，$m' \mid m$ なる正整数 $m' < m$ に対して $\tau \in GF(P^{m'})$ であるとするならば，

$$\begin{aligned} \tau^{P^{m'}} - \tau &= (\omega^P - \omega)^{P^{m'}} - (\omega^P - \omega) \\ &= (\omega^{P^{m'}} - \omega)^P - (\omega^{P^{m'}} - \omega) \\ &= 0 \end{aligned}$$

である．ここで，$\omega^{P^{m'}} - \omega = \gamma$ とすると，

$$\gamma^P - \gamma = 0$$

となり，$\gamma \in GF(P)$ ということになる．したがって，

$$\omega^{P^{m'}} - \omega = \gamma \in GF(P)$$

であるから，$m' < m$ よりこれは ω を零点としてもつ既約多項式 $f(x)$ が加法的非自己回帰既約多項式であることに矛盾する．したがって，$m' = m$ となり τ は $GF(P^m)$ の真性元となることから，$g(x)$ は m 次既約多項式である．また，$\tau = \omega^P - \omega$ であることより，$\mathrm{Tr}_{P^m|P}(\tau) = 0$ であることも容易に分かる．以上の議論を次の補題にまとめる．

補題3.5.1.1：$f(x)$ を $GF(P)$ 上の m 次の加法的非自己回帰既約多項式とするとき，その加法的自己回帰既約多項式集合の総積 $F(x)$ は

$$F(x) = g(x^P - x)$$

となり，$F(x)$ を $x^P - x = x$ で逆変数変換して得られる多項式 $g(x)$ は $GF(P)$ 上の m 次既約多項式である．また，$g(x)$ の零点 τ は $f(x)$ の零点 ω により $\tau = \omega^P - \omega$ で表され，

$$\mathrm{Tr}_{P^m|P}(\tau) = 0$$

である． ■

補題3.5.1.1により，$GF(P)$ 上の m 次加法的非自己回帰既約多項式 $f(x)$ から同次の既約多項式 $g(x)$ を容易に得ることができ，またその零点 τ は $\omega^P - \omega$ で表される．この操作は得られていく同次の既約多項式 $g(x)$ が加法的非自己回帰既約多項式である限り繰り返し行うことができる．また，補題3.3.1.2と本補題3.5.1.1により1組の加法的自己回帰既約多項式集合に対し1つの同次のトレース零の既約多項式が対応していることに注意する．

正規基底によるベクトル表現： 補題3.5.1.1において，$f(x)$ の加法的自己回帰既約多項式集合の総積に対して逆変数変換を施して得られる $g(x)$ の零点 τ は $\omega^P - \omega$ で表され，さらに $g(x)$ が加法的非自己回帰既約多項式の場合には再び同様の操作を施すことにより得られる m 次既約多項式 $h(x)$ の零点 γ は，

$$\begin{aligned} \gamma &= \tau^P - \tau \\ &= \omega^{P^2} - 2\omega^P + \omega \end{aligned}$$

になる．このことから，ω がある正規基底によりベクトル表現されているならば，P 乗という演算は正規基底によるベクトル表現に対して1回の巡回シフトという単純な操作により行えることから，このような操作により得られる既約多項式すべての零点が正規基底を用いたベクトル表現との対応を容易に取りながらその最小多項式を特定付けるという操作を並行して行えることになる．

すなわち，例えば $f(x)$ の零点 ω の $GF(P)$ に関する共役元の組：

$$\{\omega^{P^{m-1}}, \cdots, \omega^{P^1}, \omega^{P^0}\}$$

を正規基底とするならば，$f(x)$，$g(x)$ および $h(x)$ の零点 ω，τ および γ をベクトル表現すると，

$$\begin{aligned} f(x) &\rightarrow (0, \cdots, 0, 0, 1) \\ g(x) &\rightarrow (0, \cdots, 0, 1, -1) \\ h(x) &\rightarrow (0, \cdots, 1, -2, 1) \end{aligned}$$

のようになる[7]．一般式として与えれば，もとの既約多項式の零点のベクトル表現を $\mathbf{v}_\omega$，加法的自己回帰集合の総積をとって逆変数変換を施すことにより得られる既約多項式の零点のベクトル表現を $\mathbf{v}_\tau$ とすると，

$$\mathbf{v}_\tau = \mathbf{v}_\omega{}^P - \mathbf{v}_\omega$$

[7] $+$，$-$ が交番する二項分布のようになる特徴がある．

で与えられる．ここで，$\mathbf{v}_\omega{}^P$は正規基底によるベクトル表現より1回の巡回シフトである．また，これら元（零点）の$GF(P)$に関する共役元に対するベクトル表現はその1回ずつの巡回シフトにより各々与えられることが分かる．

次に，加法的自己回帰既約多項式集合各々の零点の正規基底によるベクトル表現の対応づけは，$f(x)$の零点ωの正規基底によるベクトル表現を$\mathbf{v}_\omega$とすれば，$f(x+i)$の零点$\omega-i$のベクトル表現$\mathbf{v}_{\omega-i}$は，正規基底として用いられている元の素体に対するトレースの値をAとしたとき[8]，

$$\mathbf{v}_{\omega-i} = \mathbf{v}_\omega - A^{-1}\cdot(i,i,\cdots,i)$$

となる．ここで，$i=0,1,\cdots,P-1$である．さらに，先と同様に$\omega-i$の素体に関する共役元のベクトル表現は$\mathbf{v}_{\omega-i}$の1回ずつの巡回シフトで各々与えられる．

同様にして，$f(x)$の加法的自己回帰既約多項式集合の総積に対して逆変数変換を施して得られる$g(x)$が加法的非自己回帰既約多項式であるならば，その加法的自己回帰既約多項式集合の各々の既約多項式の零点に対しても同じように正規基底によるベクトル表現を対応づけることができる．

ここまで，加法的非自己回帰既約多項式およびその回帰集合に対して議論してきたが，次に加法的自己回帰既約多項式の逆変数変換に対する補題を与えておく．

補題3.5.1.2：$GF(P)$上のm次加法的自己回帰既約多項式$f(x)$に対し$x^P-x=x$なる逆変数変換を施して得られる$g(x)$なる多項式は$GF(P)$上のm/P次既約多項式である．また，$f(x)$の零点を$\omega\in GF(P^m)$，$g(x)$の零点を$\tau\in GF(P^{m/P})$とするとき，$\tau=\omega^P-\omega$でありかつ$\mathrm{Tr}_{P^{m/P}|P}(\tau)\neq 0$である． ■

証明(補題3.5.1.2)：$GF(P)$上のm次加法的自己回帰既約多項式$f(x)$に対し，その零点を$\omega\in GF(P^m)$とする．$f(x)$が加法的自己回帰既約多項式であることより，ωの$GF(P)$に関する適当な共役元ω^{P^s}に対し，

$$\omega^{P^s} = \omega+1 \tag{3.11}$$

が成り立つ．上式を両辺P回繰り返しP^s乗することにより，

$$\begin{aligned}\omega^{P^s} &= \omega+1\\ \omega^{P^{2s}} &= \omega+2\\ &\vdots\end{aligned}$$

[8]正規基底をなすことから$A\neq 0$である．

$$\omega^{P^{Ps}} = \omega + P = \omega$$

となり，$\omega \in GF(P^m)$ より $m \mid Ps$ となる．したがって，

$$Ps = mA, \quad 1 \leq A \leq P-1$$

とおくことができ，$f(x)$ は加法的自己回帰既約多項式でありその存在条件から $P \mid m$ である．ゆえに，

$$s = \frac{m}{P}A$$

となりこれを式(3.11)に代入して，

$$\omega^{P^{\frac{m}{P}A}} = \omega + 1$$

上式を $i(1 \leq i \leq P-1)$ 回繰り返し $P^{\frac{m}{P}A}$ 乗すると，

$$\begin{aligned} \omega^{P^{\frac{m}{P}Ai}} &= \omega + i \\ (\omega^{P^{\frac{m}{P}(Ai-1)}})^{P^{\frac{m}{P}}} &= \omega + i \end{aligned}$$

であり，$1 \leq A \leq P-1$ であることから $1 \leq i \leq P-1$ の中に必ず1つ

$$iA \equiv 1 \pmod{P}$$

を満たす i が存在する．上式を満たす i をここで仮に $b \neq 0$ とすると，

$$(\omega^{P^{m \cdot \frac{(Ab-1)}{P}}})^{P^{\frac{m}{P}}} = \omega^{P^{\frac{m}{P}}} = \omega + b \tag{3.12}$$

となり，これを $P-1$ 回繰り返し $P^{\frac{m}{P}}$ 乗すると以下のようになる．

$$\begin{aligned} \omega^{P^{\frac{m}{P}}} &= \omega + b \\ \omega^{P^{\frac{m}{P}2}} &= \omega + 2b \\ &\vdots \\ \omega^{P^{\frac{m}{P}(P-1)}} &= \omega + (P-1)b \end{aligned}$$

また，式(3.12)を $m/P-1$ 回繰り返し P 乗を施すと，

$$\omega^{P^{\frac{m}{P}+1}} = \omega^P + b$$

$$
\begin{aligned}
\omega^{P^{\frac{m}{P}+2}} &= \omega^{P^2} + b \\
&\vdots \\
\omega^{P^{\frac{m}{P}+(\frac{m}{P}-1)}} &= \omega^{P^{\frac{m}{P}-1}} + b
\end{aligned}
$$

となる．以上のことを踏まえると，次のような式変形が可能となる．

$$
\begin{aligned}
f(x) &= \prod_{i=0}^{m-1}(x-\omega^{P^i}) \\
&= \prod_{j=0}^{P-1}\prod_{i=0}^{m/P-1}(x-\omega^{Pjm/P+i}) \\
&= \prod_{i=0}^{m/P-1}\prod_{j=0}^{P-1}(x-\omega^{Pjm/P+i}) \\
&= \prod_{i=0}^{m/P-1}[(x-\omega^{P^i})(x-\omega^{P^i}+b)\cdots(x-\omega^{P^i}+(P-1)b)] \\
&= \prod_{i=0}^{m/P-1}(x^P-x-(\omega^{P^{i+1}}-\omega^{P^i})) \\
&= \prod_{i=0}^{m/P-1}(x^P-x-(\omega^P-\omega)^{P^i})
\end{aligned}
$$

したがって，$\omega^P-\omega=\tau$とすると，

$$
\begin{aligned}
\tau^{P^{\frac{m}{P}}} &= (\omega^{P^{\frac{m}{P}}})^P-(\omega^{P^{\frac{m}{P}}}) \\
&= (\omega+b)^P-(\omega+b) \\
&= \omega^P-\omega \\
&= \tau
\end{aligned}
$$

となり，$\tau\in GF(P^{m/P})$である．

ここで仮に，$m'\mid m/P$なる正整数$m'<m/P$に対して$\tau\in GF(P^{m'})$であるとするならば，

$$
\begin{aligned}
\tau^{P^{m'}}-\tau &= (\omega^P-\omega)^{P^{m'}}-(\omega^P-\omega) \\
&= (\omega^{P^{m'}}-\omega)^P-(\omega^{P^{m'}}-\omega) \\
&= 0
\end{aligned}
$$

である．ここで，$\omega^{P^{m'}}-\omega=\gamma$とすると，

$$\gamma^P-\gamma=0$$

となり，$\gamma\in GF(P)$ということになる．したがって，

$$\omega^{P^{m'}}-\omega=\gamma\in GF(P)$$

であるから，両辺をP回それぞれ$P^{m'}$乗し得られる式を辺々加えることにより，

$$\omega^{P^{m'P}}-\omega=0$$

となる．これは，$m'<m/P$よりωが$GF(P^m)$の真性元であることに矛盾する．したがって，$m'=m/P$となりτは$GF(P^{m/P})$の真性元となることから，$g(x)$はm/P次既約多項式である．また，

$$\begin{aligned}
\mathrm{Tr}_{P^{m/P}|P}(\tau) &= \tau+\tau^P+\cdots+\tau^{P^{m/P-1}} \\
&= (\omega^P-\omega)+(\omega^P-\omega)^P+\cdots+(\omega^P-\omega)^{P^{m/P-1}} \\
&= (\omega^P-\omega)+(\omega^{P^2}-\omega^P)+\cdots+(\omega^{P^{m/P}}-\omega^{P^{m/P-1}}) \\
&= \omega^{P^{m/P}}-\omega \\
&= b
\end{aligned}$$

となり，$\mathrm{Tr}_{P^{m/P}|P}(\tau)=b\neq 0$である．

■

定理3.3.1.1および本補題3.5.1.2により，m/P次のトレースの値が非零の零点をもつ既約多項式とその既約多項式に$x=x^P-x$なる変数変換を施すことにより得られる加法的自己回帰既約多項式が1対1に対応することが示された．また，加法的自己回帰既約多項式はその加法的自己回帰既約多項式集合がすべて等しくなるという性質があるため，その総積をとって逆変数変換を施すことで同次の既約多項式を得るという操作は本節の目的に対して意味を成さず，補題3.5.1.2のように加法的自己回帰既約多項式そのものに逆変数変換を施すという操作を用いる．

また，この場合も先の証明過程からも分かるように加法的自己回帰既約多項式の零点に対応する正規基底によるベクトル表現を$\mathbf{v}_\omega$，自己回帰既約多項式そのものに逆変数変換を施すことにより得られる$1/P$の次数の既約多項式の零点に対する正規基底によるベクトル表現を$\mathbf{v}_\tau$とすると，

$$\mathbf{v}_\tau=\mathbf{v}_\omega{}^P-\mathbf{v}_\omega$$

で与えられる．これら零点の共役元に対するベクトル表現も先と同様その1回ずつの巡回シフトにより各々与えられる．

次項において本手法をアルゴリズム化するにあたり，注意点を$P \nmid m$および$P \mid m$の2つの場合に分けて述べておく．

$P \nmid m$の場合： 補題3.3.1.2と補題3.5.1.1により逆変数変換前のトレースの値が零の零点をもつ加法的自己回帰既約多項式集合中の既約多項式と，逆変数変換後のトレースの値が零の零点をもつ既約多項式は1対1に対応する．すなわち，正規基底によるあるベクトル表現に対応する元の最小多項式を起点として，加法的自己回帰既約多項式集合の総積および逆変数変換という操作を繰り返し行って最小多項式と正規基底によるベクトル表現の対応をとっていくとき，いくつもの既約多項式を渡り最終的には必ず起点として用いた既約多項式の加法的自己回帰既約多項式集合中のトレースの値が零の既約多項式に戻ることとなり，その後は再び同じ最小多項式の軌跡を辿ることとなる．アルゴリズム上では，これが繰り返し操作部分の終了条件となる．(もちろん，同じ最小多項式が現れることを終了条件としてもよい.) この時点で，すべてのベクトル表現とその最小多項式との対応がとれていればテーブルの作成終了である．そうでない場合には，現れていないベクトル表現に対応する最小多項式を従来法により導出し[9]，その最小多項式を新たな起点として用ることにより，すべての対応がとれるまで繰り返すこととなる．

$P \mid m$の場合： 正規基底によるベクトル表現に対応する元の最小多項式を起点として考えた場合，その最小多項式が加法的自己回帰既約多項式か否かを常に監視しなければならない．というのは，自己回帰か否かによって逆変数変換を施す前の処理が変わるからである（回帰集合の総積をとるか否か）．また，加法的非自己回帰既約多項式に対してもその加法的自己回帰既約多項式集合中のトレースの値はすべて等しいため，$P \nmid m$の場合のように逆変数変換前の集合中の既約多項式のいずれかと，逆変数変換後に得られる既約多項式との1対1対応をみることができない．したがって，正規基底によるベクトル表現およびその最小多項式を起点としてその加法的自己回帰既約多項式集合の総積および逆変数変換という操作を（加法的自己回帰既約多項式であるか否かの判定を行いながら）繰り返し行っていったとき，繰り返し操作部分の終了条件は再び同じ最小多項式が現れることでのみなされる．

3.5.2 正規基底表現-最小多項式テーブル生成アルゴリズム

本項では，正規基底によるベクトル表現とそれに対応する最小多項式テーブルの生成アルゴリズムを示す．本アルゴリズムを実行することにより，拡大次数のすべての約数次数のすべての既

[9]正規基底によるベクトル表現を有限体上の剰余類演算によって多項式表現に変換することで行える．

約多項式が得られることにも注意されたい．尚，本アルゴリズムにおいて，行き先の表示してないステップは次のステップに順序通り進むものとする．

STEP 1-1: 標数Pおよび零点$\alpha \in GF(P^m)$の$GF(P)$に関する共役元の集合：

$$\{\alpha^{P^{m-1}}, \cdots, \alpha^{P^1}\alpha^{P^0}\}$$

が$GF(P^m)$において正規基底を成すm次既約多項式$p(x)$を入力する．そして，元ω，m字組のベクトル$\mathbf{v}_\omega$，次数M，トレースの値Tおよび最小多項式$f(x)$をそれぞれ以下のように初期化する．

$$\begin{aligned} \omega &= \alpha \\ \mathbf{v}_\omega &= (0, 0, \cdots, 1) \\ M &= m \\ T &= \mathrm{Tr}_{P^m|P}(\alpha) \\ f(x) &= p(x) \end{aligned}$$

STEP 1-2: $P \mid M$である．

$$\mathrm{YES} \rightarrow \mathrm{STEP1-3}$$

$$\mathrm{NO} \rightarrow \mathrm{STEP2-1}$$

STEP 1-3: $f(x)$は自己回帰既約多項式である．

$$\mathrm{YES} \rightarrow \mathrm{STEP3-1}$$

$$\mathrm{NO} \rightarrow \mathrm{STEP2-1}$$

STEP 2-1: ωの$GF(P)$に関する共役元すべてに対しそのベクトル表現を，$\mathbf{v}_\omega$の左へのサイクリックシフトにより求める．

STEP 2-2: 既約多項式$f(x+i)$に対し，その零点$\omega - i$に対するベクトル表現$\mathbf{v}_{\omega-i}$を以下の式で求める．

$$\mathbf{v}_{\omega-i} = \mathbf{v}_\omega - T^{-1} \cdot (i, i, \cdots, i)$$

そして，$f(x+i)$の他の零点（$GF(P)$に関する$\omega - i$の共役元）に対するベクトル表現$\mathbf{v}_{\omega-i}$を$\mathbf{v}_{\omega-i}$の左へのサイクリックシフトにより求める．ここで，$1 \leq i \leq P-1$である．

STEP 2-3: $f(x)$の自己回帰既約多項式集合の総積$F(x)$を求め，$x^P - x = x$なる逆変数変換を$F(x)$に施すことによりM次既約多項式$g(x)$を求める．

STEP 2-4: $g(x)$の零点τに対し，そのベクトル表現$\mathbf{v}_\tau$を以下のように求める．

$$\mathbf{v}_\tau = \mathbf{v}_\omega{}^P - \mathbf{v}_\omega$$

ここで，$\mathbf{v}_\omega^P$は$\mathbf{v}_\omega$の1回の左サイクリックシフトである．

STEP 2-5: $g(x)$は既に得られている最小多項式である．

YES $\rightarrow$ STEP4 – 1

NO $\rightarrow$ Set $\omega = \tau$, $f(x) = g(x)$ and $\mathbf{v}_\omega = \mathbf{v}_\tau$. And go to STEP1 – 2

STEP 3-1: ωの$GF(P)$に関するすべての共役元に対するベクトル表現を$\mathbf{v}_\omega$の左へのサイクリックシフトにより求め，$f(x)$に対して$x^P - x = x$なる逆変数変換を施すことによりM/P次の既約多項式$g(x)$を求める．

STEP 3-2: $g(x)$の零点τに対し，そのベクトル表現$\mathbf{v}_\tau$を以下の式で求める．

$$\mathbf{v}_\tau = \mathbf{v}_\omega{}^P - \mathbf{v}_\omega$$

ここで，$\mathbf{v}_\omega^P$は$\mathbf{v}_\omega$の1回の左サイクリックシフトである．

STEP 3-3: 各々$M = M/P$, $f(x) = g(x)$, $\omega = \tau$, $\mathbf{v}_\omega = \mathbf{v}_\tau$というようにセットしSTEP 1-2へ．

STEP 4-1: $GF(P^m)$のすべての元に対しその$GF(P)$に関する最小多項式との対応がとれているならばアルゴリズム終了．対応がとれていなければ，現れていない任意のベクトル表現$\mathbf{v}$に対し従来の最小多項式特定法を適用し，$\mathbf{v}$の最小多項式$h(x)$を求める．$h(x)$の零点をτとして，各々$\mathbf{v}_\omega = \mathbf{v}$, $f(x) = h(x)$, $\omega = \tau$, $M = \deg h(x)$としてSTEP 1-2へ．

3.5.3 Example

Example3.5.3.1： 簡単な例として，$GF(3^5)$，正規基底として$p(x) = x^5 + 2x^4 + x^3 + x^2 + x + 1$ (121111)の零点を用いる．ただし，既約多項式は係数のみ表記するものとする．また，紙面の関係上トレース1のものの対応のみ記載する．また，共役元に対する最小多項式との対応は省略してある．

最小多項式 $\rightarrow$ ベクトル表現

$$
\begin{aligned}
121111(=p(x)) &\rightarrow (00001)\\
122021 &\rightarrow (22201)\\
120221 &\rightarrow (22000)\\
120212 &\rightarrow (20221)\\
121012 &\rightarrow (01210)\\
120202 &\rightarrow (00112)\\
122002 &\rightarrow (20200)\\
122102 &\rightarrow (01021)\\
121112 &\rightarrow (01111)\\
122201 &\rightarrow (02221)\\
120011 &\rightarrow (12211)\\
120001 &\rightarrow (02122)\\
121222 &\rightarrow (11020)\\
120022 &\rightarrow (21100)\\
122212 &\rightarrow (12121)\\
122101 &\rightarrow (01012)
\end{aligned}
$$

この場合，STEP4-1の従来法を用いた最小多項式の特定を行うことなく（従来の最小多項式導出法を用いることなく）すべての5次既約多項式とその正規基底による零点のベクトル表現との対応をとることができた． ■

Example3.5.3.2：簡単な例として，$GF(3^3)$，正規基底として$p(x)=x^3+x^2+2$ (1102)の零点を用いる．ただし，既約多項式は係数のみ表記するものとする．また，共役元に対する最小多項式との対応は省略してある．

$$
\begin{aligned}
\text{最小多項式} &\rightarrow \text{ベクトル表現}\\
0010 &\rightarrow (000)\\
1102 &\rightarrow (001)\\
1201 &\rightarrow (002)\\
1211 &\rightarrow (011)\\
1021 &\rightarrow (012)
\end{aligned}
$$

$$1022 \rightarrow (021)$$

$$1112 \rightarrow (022)$$

$$0011 \rightarrow (111)$$

$$1121 \rightarrow (112)$$

$$1222 \rightarrow (122)$$

$$0012 \rightarrow (222)$$

■

3.6 結言

本章では，有限体の加法的解析の一指標としてトレースなる概念を位置づけ，この概念を一般化したn次トレースなる概念および加法的自己回帰既約多項式とそれに付随する概念を新たに定義・導入し，有限体の加法的な表現構造をより詳しく解析しようと試みた．

これら概念を用い，以下のことを本章では示した．

1. 変数変換$x = x^P - x$による標数Pの倍数次数の既約多項式の導出法を与えた．

2. 標数Pの倍数次数の既約多項式の導出をより組織的に行えるように，有限体上の形式微分および相反多項式なる概念を用い，変数変換を素体の適当な非零元sを用いた$x = x^P - x + s$とすることによって無限個の標数倍の次数ごとの組織的な高次既約多項式導出法として提案した．

3. トレースの値が非零である真性元の特定が重要であることに着目し，n次トレースなる概念を用いることにより，有限体を表現する法多項式（既約多項式）の係数とその零点のn次トレースとの関係を明確に示す式を与え，これによりトレースの値の導出およびトレースの値が非零である真性元の特定が行えることを示した．またこれを，これまで大変煩雑な操作を必要としてきた従来の最小多項式の特定法に対して，拡大次数が標数よりも小さいような有限体の場合には大変容易な最小多項式導出法としても用い得ることを述べた．

4. 加法的自己回帰既約多項式およびそれに付随する概念・性質を用いることにより，正規基底によるベクトル表現とそれに対応する最小多項式テーブルの一生成法を与えアルゴリズム化した．そして，本アルゴリズムを実行することにより拡大次数のすべての約数次数のすべての既約多項式の導出が行えることを述べた．

第　4　章

結　　論

第 4 章　結　　論

本研究は，”乗法的および加法的変数変換による有限体の表現構造に関する研究”として筆者が行った研究の成果をまとめたものである．以下に，これを総括する．

1. 有限体の表現構造に対して，乗法的に解析するためにk乗剰余性なる概念を定義・導入し，その性質を明確にしたことにより以下の成果を得た．
    i. 変数変換$x = x^k$による無限個の組織的な高次既約多項式の導出法を提案した．
    ii. k乗剰余性の判定法として，サイクル長なる概念を用いた判定法を与えその有用性を示した．
    iii. 変数変換および既約因数分解によるk乗剰余除去法を与え，本稿提案の変数変換$x = x^k$による既約多項式の導出法をより実用的なものとした．
    iv. k乗剰余性なる概念から，これまで明確とされていなかった原始多項式の組織的な導出法を提案した．そして，これをアルゴリズムとして明確に与えた．

2. 有限体の表現構造に対して，加法的に解析するためにトレースなる概念を軸として，n次トレース，加法的自己回帰既約多項式およびそれに付随する概念を定義し，その性質を明確にしたことにより以下の成果を得た．
    i. トレースなる概念から，変数変換$x = x^P - x$による標数Pの倍数次数の既約多項式の導出法を与えた．
    ii. 上述の導出法に有限体上の形式微分および相反多項式なる概念を加え，変数変換$x = x^P - x + s$による無限個の標数倍の次数ごとの高次既約多項式導出法を与えた．
    iii. n次トレースなる概念と有限体を表現する法多項式の係数との関係を明確に示す式を与え，これによりトレースの値の導出，トレースの値が非零である真性元の特定，拡大次数が標数よりも小さいような場合における最小多項式導出法を与えた．
    iv. 加法的自己回帰既約多項式およびそれに付随する概念・性質を用いることにより，正規基底によるベクトル表現とそれに対応する最小多項式テーブルの一生成法を与えアルゴリズムとして明確に示した．

本論文では，乗法に関する指標としてk乗剰余性なる概念，加法に関する指標としてトレースなる概念を位置づけ，既約多項式の導出およびその変遷過程における既約多項式（零点）の特徴

抽出というものを議論の中心に，有限体の表現構造に対して乗法・加法の両面からの解析を試み，これら一応の成果をみた．有限体の表現構造に関する乗法的解析および加法的解析は，本論文においては独立して考察されているが，変数変換による既約多項式（零点）の特徴・性質の変遷という共通する観点からすると，一つの既約多項式に対してこれら両面からの解析を平行して行うべきであり，乗法・加法の２つの観点における各々の性質を統合して解析できるような概念あるいは指標というものを提唱することが今後の課題となる．

本研究の成果は，序論で述べたような様々な分野において適用可能であり，今後のデジタルシステムの発展に寄与するものとなれば筆者の最も幸いとするところである．

謝　辞

本研究は，信州大学教授大下眞二郎博士の御指導のもとに，大学院における研究テーマとして，乗法的および加法的変数変換による有限体の表現構造に関して遂行され，ここに一応の成果をみるに至った．この間，先生から賜った懇篤なる御教示，御鞭撻に対して，ここに深甚なる感謝の意を表する次第である．

本論文をまとめるにあたり，暖かい励ましと有益な御助言を頂いた信州大学教授中村八束博士，同教授野村彰夫博士および同助教授田中清博士に厚く感謝する．

筆者は信州大学助教授杉村立夫博士より博士後期課程入学および研究の機会を与えて頂き，昼夜を分かたぬ御指導ならびに並々ならぬ御厚情を賜った．本稿を終わるにあたり衷心より謝意を表する次第である．

本研究の遂行にあたり，有益な御助言と御便宜を計って頂いた瀧澤君明技官に深く感謝の意を表する．また，本研究について御討論，御協議頂いた情報通信講座の諸氏，杉村研究室卒業生，在学生に厚く御礼申し上げる．

最後に，本研究の途上終始暖かく見守り，励ましを与えてくれた家族に深く感謝する．

文　献

[1] 嵩，都倉，岩垂，稲垣，“符号理論”，CORONA PUBLISHING CO.,LTD(1975).

[2] 柏木，“M系列とその応用”，センシング/認識シリーズ第8巻，株式会社　昭晃堂(1996).

[3] D.R.Stinson，“暗号理論の基礎”，共立出版　株式会社(1996).

[4] 杉村，末次，　“既約円周等分多項式に関する考察”，電子情報通信学会論文誌A，Vol.j73-A No.12 pp.1929-1935(1990-12).

[5] Lidl R. and Niederreiter H. , “Finite Field”, Encyclopedia of Mathematics and Its Applications 20, Cambridge University Press(1984).

[6] 杉村，末次，“多元既約多項式の導出に関する一考察”，電子情報通信学会論文誌(A)，Vol.j76-A，No.10，pp.1474-1481(1993-10).

[7] 杉村，末次，“多項式の既約判定アルゴリズム”，電子情報通信学会論文誌A，Vol.j72-A No.8 pp.1345-1352(1989-8).

[8] 杉村，末次，“既約多項式の導出に関する一考察”，信学技報，IT89-61 (1989-11).

[9] 野上，杉村，“変数変換による既約多項式の導出の一般化”，第17回情報理論とその応用シンポジウム予稿集（第2分冊），pp.559-562(1994-12).

[10] 野上，杉村，“トレースによる既約多項式の導出”，第18回情報理論とその応用シンポジウム予稿集（第2分冊），pp.659-662(1995-10).

[11] Berlekamp.E.R，“Algebraic Coding Theory”，McGraw-Hill(1968).

[12] Ian F . Blake , Shuhoug Gao and Robert Lambert,　“Constructive Problems for Irreducible Polynomials over Finite Fields”, in “Information Theory and Application” , Springer-Verlag(1994).

[13] Muzhong WANG,　“Irreducibility of $f(x^2+x+1)$ and $f(x^2+x)$ and Normal Basis in Finite Field $GF(2^{2^n})$”, pp.2040-2042, IEICE Trans, Vol.E80-A, No.10, OCT.1997.

[14] 野上，田中，杉村，大下，“P-polynomialを用いた素数次拡大体における正規基底に関する一考察”，電子情報通信学会技術研究報告，IT97-5，pp25-30，1997年5月.

[15] 野上，田中，杉村，大下，“素体の拡大体における正規基底に関する一考察”，第20回情報理論とその応用シンポジウム予稿集，第2分冊，pp875-878，1997年12月．

[16] 上原, 今村, “有限体のトレースの計算法”, 信学技法, vol.90, No.264, IT90-75, pp.1-4 (1990).