

ガロア論文の古典的証明

～序文～

書名が貴方の好奇心の琴線に触れたなら幸いである。5 次方程式の解公式が書けない理由や群論に関心がある、それ以上に、現代ガロア理論に難渋したことのある方々に、本書は特別な意味をもつと信じる。気軽に読み飛ばせる内容ではないが、筆者の控えめな意図は、高等数学を巡る知的戯れとも言える。というのは必要な前提知識が高校数学（因数分解、根と係数の関係、1 の n 乗根、整数の剰余類、順列、総和 Σ 、総積 Π 、添字や集合の表記）だけなのである。

方程式の基本性質とユークリッドの互除法（1 章）は詳述し、3 次、4 次の方程式の一般解法（2 章）から群論（3 章）に導かれることを、着想の始まりから述べた。1 章 2 章は高校生読者も意識したので、夏休みの読み物にもお薦めしたい。3 章から置換の掛け算、添え字の算術へ進むと大学生の抽象思考が要るが、イメージ化に役立つよう文字計算を略さず書いた。ガロア原著のすべて（4 章）を知るという非日常的な体験を楽しまれ、現代論（5 章）にも興味が繋がることを願う。

ガロアは“方程式の解法手順、解ける必要十分条件、数値係数の素数次方程式が解けるか否かの判定法”を記した。平易な言葉で深遠な考察を述べた原著には、分かるまで考え続けずにいられない魅力がある。現代論の必須用語（体/タイや同型写像）は原著がなく、現代論を前提にして原著（古典論）を解説しようとしたら異種の考え方の混在で困難も増すと思うので、本書は今の通念と逆に、古典論を知ってから現代論を眺めることにした。原著で略された説明は、もとの言葉で補うと無理なく分かる。現代数学の進歩には畏敬の念を抱くほかないが、以下のことにも目を向けたい。

原著に次の序文がある（文献 1、訳文）。「… 方程式が根号によって解けるためには、どういう性質をもてばよいか… これほど扱い難い、またこれほど他のすべての問題から孤立したものはないであろう」。問題が孤立どころか大きく発展した今でも、高校で出会う方程式への素朴な興味は昔と変わらないであろう。多くの研究が積み重なった理論は専門教育なしには分からないが、孤立した問題を知識の少ない若者が解いたなら、自分も同じ思考径路を辿ってみたいくならないだろうか？

現代ガロア理論は神秘とも高い絶壁とも言われるが、私達は裏側の緩やかな道を選んでみる。道標は「ユークリッドの互除法」、「文字配列の置換は群/グンをなす（置換の反復も 1 つの置換、逆置換も置換）」だけである。ワンダーフォーゲルは、プロ登山家の興味を惹かないとしても、理工系読者が軽装で登り、健脚の高校ワングル部員も山頂に達したら愉快であろう。帰路で現代論の崖を降りてみる。逆ルートをとったら大変に難しい。遊歩道を歩けば神秘も薄れようが、山の魅力は変わらないと思う。

2013 年 1 月 著者 三森明夫

引用文献： 本書で言う「ガロア論文」とは、文献 1、2 に掲載された第 1 論文和訳である（解説部分は本書と共通点がない）。5 次方程式に解公式がないことの現代群論による証明は、原著の証明と異なるので、文献 3 から引用改変し 5 章末尾に配した。

1. 彌永昌吉：「ガロアの時代、ガロアの数学（第2部、数学編）」、シュプリンガー・フェアラーク東京、2003年
2. 守野美賀雄：現代数学の系譜11巻「群と代数方程式」、東京、共立出版、1975年
3. 草場公邦：「ガロワと方程式」、東京、朝倉書店、2000年

目次

第 1 章 方程式の解法の意味、多項式の性質

§ 1 解公式の歴史的な概観	6
§ 2 解法ルール、有理計算と既約式の意味	
1. 方程式を解く（ガロア論文などで用いられる）計算ルール	8
2. 既約式と可約式	9
3. 計算対象（数の範囲）に関する考察と因数定理	10
§ 3 ユークリッドの互除法と n 次方程式の性質	
1. 2 つの整数の最大公約数	12
2. 多項式どうしの互除法	13
3. 方程式の重根について	16
4. n 次方程式の性質（ガロア論文のための予備知識）のまとめ	17

第 2 章 根の配列置換、および 3 次方程式と 4 次方程式の一般解法

§ 1 根の式がもつ対称性、という概念	
1. 根と係数の関係；基本対称式	17
2. 根の関数	18
3. 根の配列置換（または単に置換）、および置換対称性の概念	
4. 解法過程に現れる、根の非対称関数	21
5. 対称性の異なる関数どうしを、どのように等式で結べるのか？	
§ 2 置換対称性を利用した、方程式の解法	
1. 3 次方程式の解法	23
2. 4 次方程式の解法	27

3. 5 次方程式の一般解が、求まらないという予想	30
---------------------------	----

第 3 章 根の配列置換の集合、および群

§ 1 置換の意味と方法

1. 根の配列置換、根の関数の変化	31
2. 置換操作の演算規則	
3. 文字配列の置換内容を、具体的に示す表記法	33

§ 2 群の概念、および方程式の解法理論に群論が使われる必然性

1. 根の或る特定の関数 θ を“変化させない置換”の、“すべて” からなる集合、これが群になる	37
2. 群の定義と性質	38
3. 群に慣れるための練習問題	41
4. ガロア論文で使うことになる、群論の諸定理	42

§ 3 n 次対称群 S_n の構造、および方程式の解公式との関係

1. S_n の元の表記法	44
2. S_3 の構造と 3 次方程式の解法の関係	45
3. S_4 の構造と 4 次方程式の解法の関係	47
4. S_5 の構造	48

§ 4 文字の添え字の算術による、置換の表記法

1. 整数の剰余類、根の添え字の表記法	48
2. 添え字の計算式で、一括表現できる置換について	49
3. $\text{mod } n$ の原始根（剰余類の原始根）	50
4. 全根を共通規則で置換するが、1 根だけ動かず、他すべてが 移り変わる巡回置換	50

第 4 章 ガロア論文

§ 1 n 次方程式の根の 1 次式 $V = A_1 \alpha_1 + A_2 \alpha_2 + \cdots + A_n \alpha_n$ を使うと、 各根が、 V の整式で $\alpha_k = \varphi_k(V)$ と表せる

1. 根の 1 次関数 $V = A_1 \alpha_1 + \cdots + A_n \alpha_n$ という概念	52
2. 各根が、 $V = A_1 \alpha_1 + \cdots + A_n \alpha_n$ の“整式”で書き表せることの証明	54
3. 根の配列変化と V の変化の関係： $\alpha_k = \varphi_k(V) \rightarrow \alpha_j = \varphi_k(V')$ の決め方	59
4. 各根 $= V$ の整式、を与える根の 1 次式 V を、 n ケよりも少数の “任意根”で書ける方程式もある	60
5. 関係式 $\alpha_j = \varphi_k(V)$ を保存する置換の集合は、群になる	61

6. V_1 を置換して作った多項式 $F(V)$ の係数に含まれる、“根の関数”の置換対称性	62
7. V を解にもつ $F(V)=0$ の因数分解が、 $f(x)=0$ の解法であるというアイデア	64
§ 2 ガロア群	
1. 方程式の群（ガロア群）の概念	65
2. 様々な方程式の、ガロア群の実例	66
3. ガロア群の定理、およびガロア群の縮小	68
4. 方程式が解ける過程の、ガロアによる説明； $F_G(V)$ の因数分解	71
5. 3 次方程式の解法における、計算対象の拡大とガロア群の縮小	
6. 4 次方程式の解法における、計算対象の拡大とガロア群の縮小	75
§ 3 方程式が解けるための、必要十分条件	
1. ガロア群 G 対称性の V 多項式 $F_G(V)$ が、1 次式の積にまで因数分解できるための必要条件	78
2. 方程式が解ける十分条件、および（現代用語による）必要十分条件	83
§ 4 任意文字係数の n 次方程式を、実際に解く計算原理	
1. 各根を、より高対称な関数（の巾根）で表す第一段階	86
2. 根の関数を、より高対称な関数で表す連立方程式における、未知関数の個数	88
3. $F_{S_n}(V)$ の分解因子の対称性が、系列 $S_n \supset A_n \supset \dots$ に従う必然性	90
§ 5 解ける素数次方程式の一般解法	
1. 5 次方程式の解法	91
2. 5 次方程式に解公式がない理由	93
3. 素数次方程式が解ける（ガロアの用語による）必要十分条件	94
4. 解ける 5 次方程式のガロア群（ガロア原著の記述法）	96
5. 係数が数値で与えられた素数次方程式が、解けるかどうかの判定法；ガロアが述べた $(n-2)!$ 次の補助方程式の意味	97
§ 6 素数次方程式が解ける条件の別な表現	
1. 解ける素数次既約方程式の各根 α_k は、任意 2 根の 1 次式を使った整式で、 $\alpha_k = \psi_k(V) = \psi_k(A \alpha_i + B \alpha_j)$ と表せる	101
2. $\alpha_k = \psi_k(A \alpha_i + B \alpha_j)$ の関係を保存する置換群は、解ける方程式のガロア群である	104
3. ガロア群の、もう一つの古典的定義	108

第 5 章 現代ガロア理論の概念

§ 1 体（タイ）と同型写像の概念	
1. 代数的な数	110
2. 体の概念（体の拡大、拡大次数、単拡大、中間体）	
3. 同型写像、同型な体、同型写像のレパートリー	114
4. 自己同型な体、自己同型群	117
5. ガロア拡大体 Γ 、および Γ の自己同型群（単拡大を用いた定義法）	118
§ 2 ガロア理論	
1. “解 V_1 を与える既約方程式” と “ Γ の自己同型群” の関係	119
2. ガロア群の定義と定理	123
3. 方程式 $f(x) = 0$ が解かれる道筋	127
4. 代数方程式が解けるための必要十分条件	128
§ 3 5 次以上の方程式に解公式がないことの、現代群論による証明	
1. 交換子という概念	133
2. $n \geq 5$ では、交代群 A_n を、正規部分群による剰余類の巡回群で書けない	

付録

3 次方程式の解公式から、2 次方程式の解公式が出る計算過程	137
--------------------------------	-----

本文に入る前に、本書の課題の本質を要約する <3 次方程式で例示する>

$x^3 + ax^2 + bx + c = 0$ の解は、 $x = \text{「}a, b, c \text{を用いた」}$ 文字式、と書かれる
根と係数の関係を使い、3 根 α, β, γ を用いて上の式を書き直せば；

$$\begin{cases} \alpha = \text{「}\alpha + \beta + \gamma, \alpha\beta + \beta\gamma + \gamma\alpha, \alpha\beta\gamma \text{を用いた」文字式} \\ \beta = \text{「}\alpha + \beta + \gamma, \alpha\beta + \beta\gamma + \gamma\alpha, \alpha\beta\gamma \text{を用いた」上記と少し違う文字式} \\ \gamma = \text{「}\alpha + \beta + \gamma, \alpha\beta + \beta\gamma + \gamma\alpha, \alpha\beta\gamma \text{を用いた」上記と少し違う文字式} \end{cases}$$

すなわち、方程式の一般解法とは、基本対称式を用いて、各根を書くことである

ガロアが見つけた、その方法の鍵は、「上の連立式が、文字を入れ替えても成り立つ
(式どうしが移り変わるが、連立式としては変わらない)」ことにある

上の連立式を（根の文字で）書けない方程式では、一般解を書けないのである

第 1 章 方程式の解法の意味、多項式の性質

x を未知数、 n を自然数とする方程式、 $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0 = 0$ を、 1 変数の **n 次代数方程式** という。以下で方程式と言えは代数方程式を指し、根が必ず存在すること（代数学の基本定理）は話の前提とする。解公式（一般解）とは、根を文字係数 $c_{n-1} \sim c_0$ で書いた式であり、以下の方法で書けるか否かが課題である。

本書の用語で「解、根」は使い分けず、慣習と文脈に応じて恣意的に記す。

§ 1 解公式の歴史的な概観

方程式の解公式には、多くの人々の興味を惹きつけた長い歴史がある。2 次方程式は、 $x^2 + ax + b = 0$ を $(x + a/2)^2 = a^2/4 - b$ と変形して解けることが（表記法は違うが）紀元前に知られていた。両辺の $\sqrt{\quad}$ つまり **2 次巾開方** をとると、 a 、 b の数値によっては無理数や虚数になる（巾開方とは巾乗の逆；巾開方値を巾根・巾乗根とも言う）。

虚数も解に含めるのは近代の考え方であり、3 次方程式の解法が考案された 16 世紀でも虚数の扱い（場合分け？除外？）に人々は悩んだそうだが、読者はむしろ虚数に抵抗がなく、**1 の n 乗根** について、下記のこともすぐ思い出せると期待する。

$x^n = 1$ の根を三角関数で書くなら、 $|x| = 1$ より、 $x = \cos \theta + i \sin \theta$ とし、加法定理 $(\cos m\theta + i \sin m\theta)(\cos \theta + i \sin \theta) = \cos(m+1)\theta + i \sin(m+1)\theta$ から帰納したド・モアブルの定理より、 $(\cos \theta + i \sin \theta)^n = \cos n\theta + i \sin n\theta = 1$ 、 $n\theta = 2\pi \times \text{整数}$ 、を得るので、 $x = \cos 2k\pi/n + i \sin 2k\pi/n$ ($k = 1, \dots, n$) となる。三角関数で書くと、複素平面の円周上に等間隔で並ぶ n 根の配置が見易いが、解法計算では下記の注釈が要る。

【以下で、**1 の n 乗根**を総称的に ω と略記する（ n が違えば ω の値も違う）】

全根を ω 、 ω^2 、 $\dots$ 、 ω^n と表せる ω が存在し、 $\omega = \cos 2\pi/n + i \sin 2\pi/n$ は、その一例である。正の実数 A の n 次巾開方で n 個の異なる値、 $\omega_n \sqrt[n]{A}$ 、 $\omega^2 \sqrt[n]{A}$ 、 $\dots$ 、 $\omega^n \sqrt[n]{A}$ が生じることも、本書で頻繁に述べる（ $\omega^k \sqrt[n]{A}$ を、 **A の巾根**とも略称する）。

ただし我々の解法では、（謂わば思考ゲームのルールとして）加減乗除と巾開方だけを使うと決め、三角関数、特殊関数などを用いない。例えば、5 次方程式を解くときに必要な **1 の 5 乗根**は、 $x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1) = 0$ を x^2 で割れば求まる。

$x^2 + x + 1 + 1/x + 1/x^2 = (x + 1/x)^2 + (x + 1/x) - 1 = 0$ に 2 次方程式の解公式を二度使い、 $x + 1/x = 1/2(-1 \pm \sqrt{5}) \rightarrow x^2 + 1/2(1 \pm \sqrt{5})x + 1 = 0$ から ω 、 ω^2 、 ω^3 、 ω^4 を得る。

2 次方程式の根は、前述の式変形で、 $x = \{\pm \sqrt{(a^2 - 4b)} - a\} / 2$ と計算できるので、解公式は、 **$x = \{\sqrt{\text{係数の有理式}}\}$ を含む有理式** であり、**1 の 2 乗根 ± 1** を含む。

3 次方程式の解公式は、 **$x = [\sqrt[3]{\sqrt{\text{係数の有理式}}}]$ を含む有理式**、となり、**1 の 3 乗根 $\omega = (-1 + \sqrt{-3})/2$ と $\omega^2 = (-1 - \sqrt{-3})/2$ を含む 2 根と、1 つの実根**から成る。係数の値によっては虚数部分が打ち消され、みな実根になる。

4次方程式では $x^4=A$ の根の1つが $\sqrt[4]{A}$ だから、公式にも $\sqrt[4]{}$ が現れるだろうか？
 解公式では、一度で4次巾開方せず、係数文字の有理計算式を Q と総称すれば、
 $x = \{\sqrt{(\sqrt{(\sqrt[3]{(\sqrt{Q} \text{を含む有理式}) \text{を含む有理式}) \text{を含む有理式}) \text{を含む有理式})}\}$ 、となる。
 すなわち算出過程に、 $\omega^2=1$ の根を伴う2次巾開方 $\sqrt{}$ 、 $-\sqrt{}$ と、 $\omega^3=1$ の根を伴う
 3次巾開方 $\sqrt[3]{}$ 、 $\omega\sqrt[3]{}$ 、 $\omega^2\sqrt[3]{}$ が現れ、 $\sqrt[4]{}$ 、 $-\sqrt[4]{}$ 、 $i\sqrt[4]{}$ 、 $-i\sqrt[4]{}$ は現れない（虚数
 単位 i は、1の3乗根にも $\sqrt{-3}=\pm i\sqrt{3}$ として含まれるが、本書は、 q が負でも $\sqrt{q}$ と書く）。
 上の式を $x^4+ax^3+bx^2+cx+d=0$ の係数 $a\sim d$ で書くのは大変な手間だが、2章を
 読んだ時点で、ガロアの一般解法が分かるので、文字式を延々と単純計算すれば公式
 を書ける。同時に、5次方程式に一般解法がないことも予測できる。

以上をみると、 n 次方程式が解けるなら、合計で $n!$ 次の巾開方を含むようであり、
 素数次の巾開方だけが現れるようにもみえる。自然科学で類推を一般化すると、しば
 しば裏切られるが、数学ではどうだろうか？

5次の既約方程式では実は、 $\{ \sqrt[5]{(\sqrt[4]{Q} \text{を含む有理式}) \text{を含む有理式}} \}$ の形の解が、
 係数数値の有理計算で、有理数値 Q がみつかる場合だけ得られ、一般解を書けない。

注) $x^5-1=(x-1)(x^4+x^3+x^2+x+1)=0$ は、課題が既約4次方程式だから上記の形でない

素数 p 次の既約方程式の解は、解ければ、 $\{ \sqrt[p]{(\sqrt[p-1]{Q} \text{を含む有理式}) \text{を含む有理式}} \}$
 の形になり（7次方程式なら 7×6 次巾開方の形）、 $p-1$ は非素数となる。

やや錯綜してきた話を整理すると； n 次方程式の一般解法には、合計 $n!$ 次の巾開方
 が必要だが、実現するのは“素数次”方程式で、 $n(n-1)$ 次巾開方までなのである。

素数次の3次、2次方程式では、 $n!=n(n-1)$ なので一般解が書けた。

$n(n-1)$ 次を越えて、合計 $n!$ 次の巾開方が、“必ず”実現するのは4次方程式だけ
 である（ただし $4\times 3\times 2\times 1$ でなく、前述の素数次ごとの巾開方、 $2\times 2\times 3\times 2\times 1$ ）。

ガロアは、“ n 次方程式の解公式が書ける必要十分条件（ $n\geq 5$ で満たされない）”、
 “素数次の既約方程式が解けるか否かを、係数の数値から判別する原理と計算法”を
 示した。非素数次の既約方程式では（ $n=4$ を除き）、解けるか否かを普遍的には言え
 ない。5次以上の方程式の解は、求まるかどうかは係数間の“数値関係”に依存する
 ので、係数文字による一般的表現はできないのである。

以上のことと、その背景にある数学的意味が、本書のテーマである。

本書では、個々の解公式における歴史的な式変形の工夫を引用せず、方程式の一般
 解法だけを論じる。その前に、以下のことは背理法ですぐ分かる。

n 次方程式の解公式が、 $n=5$ で書けないなら、 $n\geq 6$ でも書けない。

$x^6+ax^5+bx^4+cx^3+dx^2+ex+f=0$ の解公式が、 x ＝「係数 $a\sim f$ からなる式」と書け
 たら、その公式に $f=0$ を代入し、 $x(x^5+ax^4+bx^3+cx^2+dx+e)=0$ の解公式が書け

てしまう（公式が $1/f$ を含めば $f=0$ は代入できないが、係数値がみな 0 に近づけば根も 0 に近づくから、 $1/f$ などの発散形は含まれないと分かる）。実際に、3 次方程式の解公式の中に 2 次方程式の解公式が含まれる様子を、付録 137 頁に例示した。

この先の本章（§2、§3）で復習する高校数学は、すべてガロア論文（4 章）に直結する内容だが、読者ごとの興味範囲に応じ、章を略して読む選択肢も挙げておく。

I. 方程式の一般解法を知るだけなら、今すぐ 2 章へ飛んでよい。 3 次 4 次で解き、5 次での非可解性も推測できる（方法の必然性を言うには、3 章：群論を要する）。

II. 群論の意味と、方程式論に群論を使う理由は、2 章+3 章で理解される。

III. 方程式の可解条件の古典的証明を完全に知るには、1 章：多項式の性質・ユークリッドの互除法、2 章：根の置換・一般解法、3 章：群論 → 4 章：ガロア論文

IV. 現代ガロア理論による証明を、5 章に記した。 群論をすでに知っている読者は、今すぐ 5 章に行けるが、互除法は必須である。予備知識なしに高校数学から現代数学へ進むなら、1、2、3 章→5 章となるが、4 章を省いて読むと難解かもしれない。

§2 解法ルール、有理計算と既約式の意味

1. 方程式を解く（ガロア論文などで用いられる）計算ルール

1) 有理計算

有限回の（収束や無限級数を使わない）加減乗除が、有理計算である。“有理的に求める”ともいう。無限にくり返せば、有理数の加減乗除で無理数に収束することがある（面白い話だが、寄り道しない）。有理数を有理計算すれば有理数になるが、代数方程式「 x の有理式 = 有理数」を満たす x は、むしろ無理数と限らない（例； $x^2=2$ ）。

任意の無理数 x からも、有理計算で任意の有理数 n/m を作れるが（ $1=x/x$ 、 1 を n 回または m 回足す）、任意の無理数は作れない。 $\sqrt{2}$ から有理計算できる数は、すべて $P\sqrt{2}+Q$ の形になり（ P, Q は有理数 ⇨ 111 頁）、 $\sqrt[3]{2}$ 、 $\sqrt{3}$ などは算出できない。

2) 代数的な計算、および 1 の n 乗根の代数計算

ガロアが論じた「根号を使って方程式を解く」方法、つまり有理計算と巾開方だけで解くことが代数計算である。このルールで解けないなら解法はないとする。

$x^5=2$ を解くとき、 $\sqrt[5]{2}$ は求まった数とみなせるが、1 の 5 乗根は計算を要する。

2 項方程式と呼ばれる $x^n - 1 = 0$ の解（ ω と総称）が、任意自然数 n で代数計算できることは、方程式の代数的解法の必須な前提であり、ガウスが証明した。

ガロアは、 $x^n + c_{n-1}x^{n-1} + \cdots + c_0 = 0$ の根が、係数文字（値）から代数計算できる条件と方法を略述し、“あとはガウス氏の方法で（ ω を）得ればよい”と記した。本書の

目的は、ガロアが示唆した証明を実際に再現することなので、 ω の代数計算に言及（他書からの引用を）しない。

3) 1 の原始 n 乗根

$x^n - 1 = 0$ の全根を、 $\omega, \omega^2, \dots, \omega^n (=1)$ 、と表せる ω の存在を前述した。

一方、 n 乗して初めて 1 になる巾乗根（巾根）を、1 の原始 n 乗根という。

問題 1 の原始 n 乗根を巾乗すれば、1 の n 乗根すべてを表せることを示せ

答 ω が原始根なら、 $1 \leq k < n$ で $\omega^k \neq 1$ 、すると $1 \leq j < k$ で、 $\omega^{k-j} \neq 1$ だから

$\omega^k \neq \omega^j$ 、そして $(\omega^k)^n = (\omega^j)^n = 1$ だから、 ω の巾乗が、異なる n ケの根を表す

1 の 2 乗根（2 次の巾根）は、1、 -1 であり、 -1 は原始根である。

n が素数でないとき、 $n = mp$ と書けば（ p は素数）、 $(\omega^m)^p = 1$ 、そこで $\omega' = \omega^m$ と書けば $\omega'^p = 1$ 、つまり ω' は原始根の定義を満たさず、 ω' の巾乗は p 種類の値しか表さない。 n が偶数 > 2 なら、 -1 は原始根でなく、巾乗で -1 と 1 しか表せない。

n が素数なら、 $(x^n - 1)/(x - 1) = x^{n-1} + \dots + x + 1 = 0$ の根は、みな原始根である。
この注目すべき方程式では、任意 1 根の有理式（つまり巾乗）で全根を表せる。

2. 既約式と可約式

1) 因数分解

「因数分解とは」、「既約式とは」という問いは課題の本質であり、我々は解法理論に達するまで同じ問いをくり返し、答が進化する。まず有理計算の範囲で考える。

因数分解すなわち、多項式 = (左辺よりも低次の多項式) $\times$ (同左) $\times \dots$ の計算は、右辺の各因子の係数値を、左辺の係数値から有理計算できれば実現する。

既約とは、約せる（割れる）因子を既に約したこと、約された各因子が既約式である。有理計算で因数分解できれば、“可約”という。可約式 = 既約式の積

有理計算で、可約多項式 = 既約多項式の積 = 0 となれば、解くべき課題は、各々の「既約多項式 = 0」になるから、我々の興味は、主に“既約方程式”にある。

係数を任意文字（係数間の関係を指定しない）と決めた多項式は、既約式である。
可約なら、係数間に“有理計算で示せる関係”が生じ、任意でなくなる。解公式を論じるとき、係数は任意文字とするから、既約方程式を論じていることになる。

2) 2 次以上の既約方程式の根は有理計算で求まらない

$f(x) = 0$ の 1 根を α と呼べば、次節で証明する因数定理により、 $f(x) = (x - \alpha)g(x)$ になる。もし α を有理計算できるなら、 $f(x)$ は、有理計算で上のように因数分解できるから可約である。対偶を言えば、「 $f(x)$ が既約なら α は有理計算できない」。

3) 方程式の有理根は、あれば有理計算で求まり、なければないと分かる

何次方程式であっても、有理根 q があれば、 q が必ず有理計算で求まる理由を考えよう（すぐ後で説明するが、方程式の係数は有理数と仮定する）。

* まず問題を逆からみて、 $f(x)=0$ の根がすべて有理数だったとしてみる。

k と m 、 k' と m' 、 $\dots$ をそれぞれ“互いに素な整数”の組と想定し、

$f(x) = (x - k/m)(x - k'/m') \dots = 0$ が展開され、分母が払われたと想像する。

$$mm'm'' \dots x^n - (km'm'' \dots + k'mm'' \dots + \dots) x^{n-1} + \dots \pm kk'k'' \dots = 0$$

実際は、下記の方程式が与えられて、有理根を計算するのが問題である。

$$A x^n + B x^{n-1} + \dots + R = 0 \quad \cdots \star \quad A \sim R \text{ は整数、公約数は1のみとする}$$

A と R を素因数分解し、それら素数から互いに素な整数の組み合わせ（4 と 9 など非素数でもよい）、 k/m 、 k'/m' 、 $\dots$ を作り、 $\star$ に代入して 0 になるものが、有理根。

A が a ケ、 R が r ケの素数から成れば、根の候補 k/m 、 k'/m' 、 $\dots$ の作り方は「 $2^a \times 2^r$ 種類の分数から、数の重複使用を除外した選び方」（有限ケ）を越えない。

* $f(x)=0$ の根の一部が有理数なら、有理根だけが有理的に求まる。有理根は1つずつ、 $f(k/m)=0$ 、 $f(k'/m')=0$ 、 $\dots$ と確認され、もうこれだけしかないと分かれば、

$f(x) = (x - k/m)(x - k'/m') \dots \{ \text{有理的に1次式に分解できない多項式の積} \}$ 、となる。

* 係数が有理数値の方程式は、いつも整数係数に書き直せる。上記の手順で A 、 R の素因数から有理根を1つも作れなかったら“有理根をもたない”と分かる。

当然ながら、“有理根がなければ既約方程式”なのではない（下記 ii）。

<上記と似て非なる問題についての注意点>

i) 上記 $\star$ は、「 $R/A = kk' \dots / mm' \dots$ になる互いに素な数の組、 k と m 、 k' と m' 、などを求める」問題とは違う。その問題では、 $kk' \dots = p \times R$ 、 $mm' \dots = p \times A$ とすれば答は無数にある。 k/m 、 k'/m' が答なら、別の答 pk/m 、 k'/pm' も作れるからである（ p を m および k' と互いに素とする）。 $\star$ で A 、 R を pA 、 pR に替えるのは方程式全体を p 倍することであり、新たな根は生じないから、 $p=1$ とすべきである。

ii) 有理根をもたない可約方程式があることは、 $f(x) = (2 \text{ 次以上の既約式}) \times (\text{同左}) \times \dots = 0$ と因数分解される例を考えれば、当然である。

iii) 係数が数値で与えられた整式が、ii) の形で可約になるか既約かの判定法は（できる場合を述べた定理もあるが）、一般的には言えない。この問題はガロア論文の範囲で扱えないが、「 $f(x)$ が既約なら…、可約なら…である」という論証は進められる。

3. 計算対象（数の範囲）に関する考察と因数定理

1) 因数定理

α が方程式 $f(x)=0$ の根なら、 $f(x)$ が $(x-\alpha)$ で割り切れることを因数定理と言う。

証明：1 次式で割った余りは定数だから、 $f(x) = (x - \alpha) g(x) + r$ と書き、この恒等式に、 $x = \alpha$ を代入すれば $r = f(\alpha) = 0$ 、すなわち割り切れる。

因数定理を、 $f_n(x) = 0$ の根 $\alpha_1 \sim \alpha_n$ に順次適用すれば、以下のように書ける。

$$f_n(x) = (x - \alpha_1) g_{n-1}(x) = (x - \alpha_1)(x - \alpha_2) g_{n-2}(x) = \cdots = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

$$\begin{array}{r} x^2 + (a + \alpha)x + (b + a\alpha + \alpha^2) \\ x - \alpha \quad) \quad x^3 + ax^2 + bx + c \\ \underline{x^3 - \alpha x^2} \\ (a + \alpha)x^2 + bx \\ \underline{(a + \alpha)x^2 - (a + \alpha)\alpha x} \\ (b + a\alpha + \alpha^2)x + c \\ \underline{(b + a\alpha + \alpha^2)x - (b + a\alpha + \alpha^2)\alpha} \\ c + b\alpha + a\alpha^2 + \alpha^3 \quad \cdots \text{ 余り} \end{array} \quad \leftarrow \text{例：3 次方程式の場合の } g_2(x)$$

α は根だから、余り $= \alpha^3 + a\alpha^2 + b\alpha + c = 0$ となる（割り切れた）

$f(x) = x^3 + ax^2 + bx + c = (x - \alpha) \{x^2 + (a + \alpha)x + (b + a\alpha + \alpha^2)\}$ という因数分解が、

“ α を計算対象に追加したら” 有理的に得られた（係数は α の整式になる）。

$f(x)$ が可約になったわけだが、ここで「根は必ずあるから、方程式はみな可約」と言ったら適切でない。「 α が未知数のままでは、因数分解できたことにならない」と言えばよいが、もう少し発展性のある言い方がある。まず以下を考えてみよう。

$x^3 - p^2 x = x(x + p)(x - p)$ は有理計算である。この p は未知数か？既知数か？

$2x^2 - \sqrt{2}x = \sqrt{2}x(\sqrt{2}x - 1)$ という計算は、有理的か非有理的か？ 下記の定義で答は首尾一貫する。

既知数の意味：上記 a, b, c, p は（方程式を論じるとき）予め与えられた文字だから既知数と言う。数値の指定がないから未知数、とは言わない。日常の語感とやや違う。

係数値を使う有理計算で、 $x^2 - p^2$ 、 $2x^2 - \sqrt{2}x$ は因数分解でき、 $x^2 - 3$ は因数分解できない： $p^2 = p \times p$ 、および $2 = \sqrt{2} \times \sqrt{2}$ は、与えられた数を使った有理計算である。 $3 = \sqrt{3} \times \sqrt{3}$ は、予め与えられていなかった数を使った有理計算とも言えるが、 $\sqrt{3}$ を求める段階を言えば、むしろ巾開方である。

可約、既約の意味 1：多項式は、その係数（出発点の既知数）を使う有理計算で因数分解できれば“可約”、できないなら“既約”という。

可約、既約の意味 2：有理計算だけで因数分解できないとき、係数値に巾開方を含む計算を行なった数（新たに既知となった数）を使うと、因数分解できることがある（既約式が可約になる）。歴史的な解公式は、このような工夫で得られた。

2) 方程式の“係数（出発点の既知数）”を有理数と決めておくことについて

文字係数の方程式で、根が含む根号は、むしろ解法手順（の巾開方）に由来する。数値係数を扱うときも我々は、計算手順が、巾開方を要するか有理計算できるかに注目する。ガロアの一般解法（2章）は、「巾開方する（新たな既知数を得る）段階」と「それを使って有理計算する段階」を明瞭に区分し、両者の繰り返しで解法を進める。

“係数から有理計算できる値”を“有理数”と短く呼べれば、一般性を失わずに解法手順を簡潔に言えるから、本書を通じて係数（文字、数値）は有理数とする。

3) 因数分解または方程式の解法における、計算対象の拡大

例えば、 $x^4 - 2 = 0$ は、計算対象に $\sqrt{2}$ を追加すると、 $(x^2 + \sqrt{2})(x^2 - \sqrt{2}) = 0$ 、1 の 4 乗根 i と $\sqrt[4]{2}$ も追加すると、 $(x + i\sqrt[4]{2})(x - i\sqrt[4]{2})(x + \sqrt[4]{2})(x - \sqrt[4]{2}) = 0$ となる。解法ルールは、1 次式の積に因数分解できたときゴール（解けた）とする。

巾開方を繰り返し、方程式の根をすべて有理計算できる段階まで、計算対象を拡大することがテーマであり、我々は、巾根拡大が可能か？ という問いを立てる。

上の例で、2 を巾開方すべきことは自明だが、文字係数の方程式一般では、係数からなる“どんな文字式”を巾開方すべきかが問題であり、これは自明でない。

$f(x) = (x - \alpha) \{x^{n-1} + (a + \alpha)x^{n-2} + (b + a\alpha + \alpha^2)x^{n-3} + \dots\}$ のように、求めたい根を計算対象に追加した因数分解は、解法を与えない。

任意文字係数の n 次方程式で、 $f(x)$ の式変形を思案しても解法の手掛かりは得られないのである。ガロアは、 $f(x)$ と全く異なる式を創作し、段階的な因数分解の原理をみつけた。その理論（4章）を知る予備知識のうち、次項の手法は最も重要である。

§ 3 ユークリッドの互除法と n 次方程式の性質

方程式の解法の話は、しばし置いて、この古代の数学を復習しよう。

1. 2つの整数の最大公約数

まず数値の場合で考える。互除法で、整数 A と B の最大公約数（共通因子）を求めよう。 $A > B$ とする。

A を B で割る。余りが出たら C と呼ぶ $\rightarrow A = qB + C$ (q は商)

例： A が 200、 B が 75 なら、 $200 = 2 \times 75 + 50$

$C = 0$ なら、 B が最大公約数である。 $C \neq 0$ とし、 $A = qB + C$ をよく眺める。

1 でない公約数（最大公約数を r とする）があれば、 A が r で割り切れるから右辺全体も割り切れ、 B は r で割り切れるのだから、 C が r で割り切れると気づく。

つまり r は、“ B と C の公約数” でもある。 C は余りだから B より小さい。

すなわち A, B の公約数を捜す代わりに、より小さい数の組 B, C の公約数として、 r を捜せばよい。 例： $200 = 2 \times 75 + 50$ 、 $75 = 1 \times 50 + 25$

商 q には興味がなく、 r で割れても割れなくても関係ない。

日常生活で割り算したら、“商”に興味をもつだろう。自分の分け前は
いくらか？など。意義を“余り”に見出し、割り切れない割り算 $A \div B$
から出発したことにユークリッドの偉大さが感じられる。

次に B を C で割ったら、余りが $D \rightarrow B = q' C + D$ (q' は商)

r は“ C と D の公約数”でもある。次は C を D で割り… と扱う数は小さくなり、
公約数 r に近づく。 例： $200 = 2 \times 75 + 50$ 、 $75 = 1 \times 50 + 25$ 、 $50 = 2 \times 25 + 0$

$A \div B$ の余り $= C$ を、 $(A, B) = C$ と書くと算法を覚えやすい。 $(200, 75) = 50$

括弧は数学記号でなく、ここでのローカルルールである。右辺に余りだけ書き、
商は使わないから無視する。 例： $(200, 75) = 50 \rightarrow (75, 50) = 25 \rightarrow (50, 25) = 0$

$(A, B) = C \rightarrow (B, C) = D \rightarrow (C, D) = E \rightarrow$ 数の組は必ず小さくなり、どこかで
 $(E, F) = 0$ すなわち E が F で割り切れたら、 $F =$ 公約数 r 、となる。 例： $r = 25$

もし A, B に 1 以外の公約数がなければ、最後に $(Z + 1, Z) = 1$ となる。

互除法の原理（余りが 0 でないとき、なぜ必ず 1 で終わるのか）を納得するには、
証明など考えず実際に計算してみればよい。

問題：1099 と 301 の最大公約数を求めよ。 答：7

問題：871 と 92 の最大公約数を求めよ。 答：1

巨大な 2 つの数では、素因数分解を使って公約数を求めるのは大変だから、互除法
は実用的な手段になる。しかし、互除法は、多項式の割り算に応用したとき真の威力
を示す。多項式の場合、整数の割り算からは予想できない驚くべき定理が導ける。

その定理が、ガロア論文で証明法の核心になるから、注意深く分析しよう。

2. 多項式どうしの互除法

1) 2 つの多項式、 $A(x)$ と $B(x)$ の共通因数の求め方：

$A(x)$ の次数 $\geq B(x)$ の次数、とする。= であっても以下の算法は同じである。

前節と同様に、{割られるもの、割るもの} = 余り、と略記する。

商は、要らないから書かない。以下は、整数の互除法のごく自然な応用である。

計算対象は終始一貫、与えられた多項式の“係数”（数値または文字）である。

* $\{A(x), B(x)\} = C(x) \rightarrow \{B(x), C(x)\} = D(x) \rightarrow$ 各式の 次数 は必ず小さくなり、
 $\{E(x), F(x)\} = 0$ すなわち $E(x)$ が $F(x)$ で割り切れたら、 $F(x)$ が共通因子である。

* 共通因子がないとき、いずれ $\{m$ 次式, $m-1$ 次以下の式 $\} =$ 定数 $\neq 0$ となる。
定数の値に興味はなく、 $\neq 0$ が重要である（整数の互除法での $= 1 \neq 0$ と同義）。

（我々はいつも、多項式そのものよりも、多項式 $= 0$ という方程式のほうに興味をも

つので、多項式の全体に掛かった“定数”は、1 と同じことなのである)

問題： $A(x) = x^4 + 2x^3 + x^2 + 3x + 2$ と $B(x) = x^3 + 4x^2 + 7x + 6$ の共通因子を求めよ。

互除法を知らなかった人には、自分で計算することを是非奨める。

答： $\{A(x), B(x)\} = C(x) \rightarrow \text{省略} \rightarrow \{2x^2 + 11x + 14, 33/4x + 33/2\} = 0$

したがって、 $33/4 x + 33/2$ すなわち $x + 2$ が公約数 (共通因子) である。

$\{\dots, mx + n\} = 0$ と算出されたら共通因子は、 $mx + n$ と言っても、 $x + n/m$ と言っても同じである。互除法の計算途中で、 $33/4$ 、 $33/2$ のような係数も現れる (もとの多項式の係数の有理計算値が、次々に書き込まれていく) ことを体験すると、ガロア論文に使われる計算を実感するのに役立つ。

2) 方程式 $A(x) = 0$ 、 $B(x) = 0$ の共通根が、互除法で求まる特殊な場合

$A(x) = 0$ 、 $B(x) = 0$ が、“唯一”の共通根をもつとしたら、どんな計算になるか？

$\{A(x), B(x)\} = C(x) \rightarrow \dots \rightarrow \{\dots, F(x)\} = 0$ となれば、 $F(x)$ が共通因子だと知った。

$F(x) = 0$ の根はみな共通根になるから、共通根が唯一なら (重根でない限り)、 $F(x)$ は 1 次式である。1 次方程式は有理的に解ける (重根でも唯一なら有理的に求まる；後述)。

共通根が唯一なら、その根は互除法 (係数値を使う有理計算) で求まる、と分かった。ガロア論文では、このことを必須の手法として利用する。

3) 係数が文字で与えられた $A(x)$ 、 $B(x)$ の互除法

係数が任意文字なら、 m 次式で割った余りは $m - 1$ 次式、次に、この余りで割った余りは $m - 2$ 次式、…と次数が 1 ずつ下がり、どこで終了か (余りが 0 か否か) 分からないので、**{2 次式, $ax + b$ } = c** の形まで進む。 c の値は (0 か否か) 不明。

$A(x)$ 、 $B(x)$ について付加情報がなければ、この機械的な文字計算からは何の結論も得られず計算の妥当性も言えない。 $A(x) = 0$ 、 $B(x) = 0$ が唯一の共通根をもつと分かっているときのみ、文字式 $c = 0$ と結論され、 $ax + b = 0$ の解 $-b/a$ を共通根と言える。

問題： $A(x) = 0$ 、 $B(x) = 0$ が「3 つの共通根をもつ」という付加情報があったら、互除法によってどんな結論が導かれるか？

答 割る式が 3 次式、 $\{\dots, px^3 + qx^2 + rx + s\} = Px^2 + Qx + R$ となったら互除法をやめ、 $P = Q = R = 0$ と結論しなければならない。

P 、 Q 、 R は $A(x)$ 、 $B(x)$ の係数からなる文字式だから、係数間に $P = Q = R = 0$ という関係が生じる。共通根をもつ方程式の係数どうしは、任意であり得ない。

共通根はむろん、 $px^3 + qx^2 + rx + s = 0$ (これは方程式) の 3 根である。 p, q, r, s は、文字だから、根を得るには、3 次方程式の解の公式が要る。たとえ係数が数値、また根が有理数であっても、根を得る計算 (10 頁) は互除法そのものではない。

もし $px^3 + qx^2 + rx + s$ を、さらに $Px^2 + Qx + R (=0, \text{これは恒等式})$ で割ったら、矛盾を生じる。

すなわち、本項冒頭のように機械的計算を進め、 $c=0$ 、共通根の 1 つ $= -b/a$ 、とみなした後、2 つの方程式が複数の根を共有するような係数数値を代入したら、「 $c \neq 0$ 」という矛盾または「或る数 $\div 0$ 」という不可能な計算が現れる。

問題： $x^3 - Ax^2 + Bx + A$ と $x^2 + C$ の互除法を、余り = 定数となるまで続け、その後、 $A=2, B=-1, C=-1$ を代入して、矛盾の原因を考察せよ。

4) 互除法から導かれる不思議な定理

方程式 $A(x)=0$ と $B(x)=0$ が、共通根 α をもち、 **$B(x)$ が既約式の場合**

(注：前述までの $B(x)$ は、共通因子が算出できる多項式の例、つまり可約式だった)
共通根が 1 つ (α だけ) とは言っていないことに注意する。

$B(x)$ が既約式なら、 $B(x)=0$ に有理根はないから (9 頁)、 α は無理数である。

共通因子 $(x - \alpha)$ の存在は、因数定理から明らかだが、互除法とは多項式の係数の加減乗除だから、係数から有理計算できない数 α を含む $(x - \alpha)$ を算出できない。

そのため意外な結論が導かれる。

$\{A(x), B(x)\} = C(x) \rightarrow \{B(x), C(x)\} = D(x) \rightarrow \dots$ の過程を考える。

$\{A(x), B(x)\} = \text{定数} \neq 0$ なら、共通因子が存在せず $(x - \alpha)$ の存在と矛盾する。

$\{A(x), B(x)\} = C(x)$ となって互除法が次に進めば、どこかで下記いずれかになる。

* $\{\text{多項式}, F(x)\} = \text{定数} \neq 0$ になれば、やはり共通因子がないことになる。

* $\{\text{多項式}, F(x)\} = 0$ になったら、 $B(x)$ に $F(x)$ という約数があることになり、 $B(x)$ の既約性に反する。

したがって **$\{A(x), B(x)\} = 0$ 、これが今の定理の結論である。**

すなわち、 $B(x)$ 自身が $A(x)$ を割り切り、 **$A(x) = g(x) B(x)$** のように書ける。

$A(x)$ と $B(x)$ がともに既約式なら、 $g(x)$ が定数、つまり同じ次数になる他ない。

共通因子が“存在する”ことだけから上記が分かった。目にみえない (まだ算出していない) 共通因子によって、あたかも既約式 $B(x)$ が、 $A(x)$ の中に吸い込まれてしまったかのようである。

$A(x)$ 、 $B(x)$ ともに既約式で、次数が異なれば、共通根はないことも分かる。

初等数学が導いたこれらの神秘的な結論は、読者がガロア論文のすべてを理解し終えてもなお、魅力を失わないであろう。

ガロアが証明の根拠として示した手法は、ほぼ互除法に尽きる。説明が殆ど省略された論文の中で、互除法の上記諸定理は明示され、理論の前提だと述べられている。

方程式 **$A(x)=0$ と $B(x)=0$** は、一方が既約なら、“根の一部”を共有することは

できず、既約方程式の根はみな共有される（前述のことを言い直しただけである）。

$A(x) = g(x) B(x)$ なら、 $B(x) = 0$ の根はすべて $A(x) = 0$ の根になる。

例： $A(x) = x^3 + 2x^2 + 3x + 2$ と、 $B(x) = x^2 + x + 2$ の互除法を行なうと、 $(x^2 + x + 2)$ が共通因子と分かる。互除法で言えるのは、 $A(x) = (x + 1) B(x)$ と割り切れることであり、 $B(x) = 0$ の根は互除法で計算できない。

α 、 β が無理数でも、 $x^2 - (\alpha + \beta)x + \alpha\beta$ の係数は有理数でありうる。互除法で算出できるのは、そのような有理係数式であり、 $x - \alpha$ 、 $x - \beta$ それぞれは算出できない。

3. 方程式の重根について

以上のことを応用し、ガロア論文（4章）の出発点における基本事項、「既約方程式の根はみな異なる、すなわち重根をもたない」ことを証明しておこう。

$f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0 = 0$ が重根 α をもつなら（ α が何重根でも）、因数定理から $f(x) = (x - \alpha)^2 g(x)$ と書ける。3重根なら $g(x) = (x - \alpha) J(x)$ 、など

本書に上級数学は使わない方針だが、ここだけ容赦願って両辺を微分すると、

$$df(x)/dx = 2(x - \alpha)g(x) + (x - \alpha)^2 dg(x)/dx = nx^{n-1} + (n-1)c_{n-1}x^{n-2} + \cdots + c_1$$

右辺は既知（有理）係数の多項式、 α は $df(x)/dx = 0$ の根、この2点に注目する。

問題 $f(x) = 0$ が重根をもつなら、 $f(x)$ は可約式であることを証明せよ。

答：より低次の多項式と共通因子をもつ多項式は、共通根を含む既約な共通因子が互除法で算出されるから可約、これで証明されたが、もう少し詳しく考えよう。

重根の1つを α と呼ぶと、 α は $df(x)/dx = 0$ の根だから、多項式 $df(x)/dx$ の中に、 $h(\alpha) = 0$ を満たす既約因子 $h(x)$ が必ず存在する。すると $h(x)$ が、共通因子 $x - \alpha$ をもつ $f(x)$ を割り切るから、 $f(x)$ は可約である。 $df(x)/dx$ 自体が既約式 $h(x)$ だとしたら、 $df(x)/dx$ が $f(x)$ を割り切り、その商は1次式だから $(x - \alpha)$ が有理計算され、すると因子 $(x - \alpha)$ をもつ $df(x)/dx$ も可約、つまり $df(x)/dx$ が既約式なら矛盾する。

すなわち、 $f(x) = 0$ に重根があれば、 $f(x)$ 、 $df(x)/dx$ とともに可約である。

対偶を言えば、 $df(x)/dx$ または $f(x)$ が既約式なら、 $f(x) = 0$ に重根はない。

問題 $f(x) = 0$ と $df(x)/dx = 0$ の共通根 α は、 $f(x) = 0$ の重根であることを証明せよ

答 $f(x) = (x - \alpha)g(x)$ を微分すると、 $df(x)/dx \equiv f'(x) = g(x) + (x - \alpha)dg(x)/dx$ より、 $f'(\alpha) = g(\alpha)$ 、一方、 $f'(\alpha) = 0$ なのだから、 $g(\alpha) = 0$ 、すなわち α は $f(x) = 0$ の重根

$f(x) = 0$ の重根は、 $df(x)/dx = 0$ との共通根、逆に共通根は $f(x) = 0$ の重根、と分かった。すると、 α が“唯一の重根”なら、 $f(x) = 0$ と $df(x)/dx = 0$ の“唯一の共通根”だから、 α は互除法で求まる。我々は「方程式の係数から有理計算できる数は、有理

数」であるように決めるから (11 頁)、重根は、唯一なら有理数である。

α 、 β が唯二つの重根なら、有理係数の因子 $\{x^2 - (\alpha + \beta)x + \alpha\beta\}$ が互除法で求まる。

4. n 次方程式の性質 (ガロア論文のための予備知識) のまとめ

* $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 = 0$ の係数は、有理数と決めて議論できる。

この取り決めで「基本対称式は有理数」、「有理的に求まる根は有理数」、「 $\sqrt[m]{}$ 」という値は、 m 次巾開方から得られる。「重根が唯一なら、その値は有理数」になる。

方程式を解くとき、ある段階で $\sqrt{}$ 、 $-\sqrt{}$ を生じ、別の段階で $\sqrt[3]{}$ 、 $\omega\sqrt[3]{}$ 、 $\omega^2\sqrt[3]{}$ を生じる必然性がある ($\omega^3 = 1$)。方程式の係数を有理数と決めてあれば、2 次巾根、3 次巾根、…などの形は、解法過程の決まった段階でだけ登場する。

* $f(x)$ が既約なら、 $f(x) = 0$ の n 根はみな異なる。

むしろ逆はいえない：根がすべて異なっても、例えば有理根を含めば可約である。

可約なら係数間の関係が存在するから、係数が任意文字の $f(x)$ は既約式である。

* 有理根は、あれば有理計算できる。有理根がないときは、ないと分かる。

* 有理計算できる数範囲の拡張： $x^2 - 2 = 0$ の根は、「有理数と $\sqrt{2}$ 、という数範囲」で有理計算され、「有理数と $\sqrt{3}$ という数範囲」では有理計算できない。

次章への発展： $f(x) = x^2 + ax + b$ は、 $\sqrt{a^2 - 4b}$ を追加した数範囲では有理計算で、 $f(x) = [x - 1/2 \{-a + \sqrt{a^2 - 4b}\}][x - 1/2 \{-a - \sqrt{a^2 - 4b}\}]$ 、と因数分解される。

$\sqrt{a^2 - 4b}$ という式 (量、値と言ってもよい) の意味を、今から考えよう。

第 2 章 根の配列置換、および 3 次方程式と 4 次方程式の一般解法

まず 2 次方程式を考える。 $x^2 + ax + b = 0$ の解公式、

$x = 1/2 \{-a \pm \sqrt{a^2 - 4b}\}$ は、根と係数の関係より、

$= 1/2 [(\alpha + \beta) \pm \sqrt{(\alpha + \beta)^2 - 4\alpha\beta}]$ と書ける。

$= 1/2 [(\alpha + \beta) \pm (\alpha - \beta)]$ に注目する。すなわち、

根の非対称式 $\alpha - \beta$ の値が、巾開方計算で得られ、得られた値を追加した数範囲では
 α 、 $\beta = 1/2 \{(\alpha + \beta) \pm (\alpha - \beta)\}$ という有理計算で根が求まる。

“根の非対称式”を、“根の対称式の巾開方”を含む式で書き表すことが、方程式の一般解法につながる、と想像できる。

各根 $\alpha_1 \sim \alpha_n \longleftrightarrow$ 非対称な根の式 $\longleftrightarrow$ 基本対称式、で書き表す方法を考えよう。

§ 1 根の式がもつ対称性、という概念

1. 根と係数の関係；基本対称式

$f_3(x) = x^3 + ax^2 + bx + c = 0$ では、 $\alpha + \beta + \gamma = -a$ 、 $\alpha\beta + \beta\gamma + \gamma\alpha = b$ 、 $\alpha\beta\gamma = -c$

係数を根 α 、 β 、 γ で表した、これらの式を“基本対称式”と呼ぶ。

n 次方程式には、 n 個の基本対称式がある。係数は有理数とする（11 頁）から“基本対称式は有理数”である。根と係数の関係は、因数定理に由来する。

$$\begin{aligned} f_n(x) &= x^n + c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_1x + c_0 \\ &= (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) \end{aligned} \quad \cdots (1)$$

(1) の右辺を展開すると、 x^{n-k} の係数 $= c_{n-k} = (-1)^k \times \sum \alpha_i \alpha_j \cdots \alpha_l$ となる。この $\sum$ は、「 $\alpha_1 \sim \alpha_n$ から k 個選んで積をとった項」の総和の意味とする。

$$\begin{aligned} c_{n-1} &= -(\alpha_1 + \alpha_2 + \cdots + \alpha_n), \quad c_{n-2} = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots, \quad \cdots, \quad c_0 = (-1)^n \alpha_1\alpha_2 \cdots \alpha_n \end{aligned} \quad \cdots (2)$$

$\alpha_1 \sim \alpha_n$ の任意置換で、(1) は明らかに不変、したがって (2) も不変だと分かる。

2. 根の関数

根からなる式を、ガロアは“根の関数”と呼んだ。特殊な数学概念でなく、慣れれば合理的な呼び方と感ずるであろう。以下、文脈の雰囲気や恣意的に、式とも関数とも言う（根の“関数”とは何のことか思い出せるよう、ときどき“式”とも言う）。

根の関数は、文字式ないし文字である。根と係数の関係から、方程式の係数も根の式だから、我々が扱う文字はすべて、根の関数とみなせる（5 頁、カラー表参照）。この視点は現代論で（5 章）、 $\{\text{有理数すべての集合}\} = \{\text{或る方程式の基本対称式から有理計算できる値の集合}\}$ という議論になる（方程式の係数は有理数とする）。

根を含む式 $\theta = \theta(\alpha, \beta, \gamma, \cdots)$ は、みな根の関数である。基本対称式、非対称式 $\alpha^2 + \beta$ 、非有理式 $\sqrt{\alpha + \beta}$ も、1 根 α も、みな根の関数である。ただし方程式の解法に使う根の関数は限られ、対称性の理由から $\alpha^2 + \beta$ などのいびつなものは出てこない。

2 つの関数 $\theta = \alpha^2\beta - \alpha\beta^2$ と $\theta' = \alpha^2\beta + \alpha\beta^2$ 、などとも言う。 θ は非対称式、 α 、 β が 2 次方程式の根なら、 $\theta' = \alpha\beta(\alpha + \beta)$ は“基本対称式の有理式”で表せる、などと考える。

3. 根の配列置換（または単に置換）、および置換対称性の概念

1) 配列置換の意味（なぜ並べるのか、何のために置換するのか？）

方程式の解法手順は、根 $\alpha_1 \sim \alpha_n$ の名称変更に影響されない。この自明な事実が解法を制約し、制約が解法を導く。名称変更を数学的に扱う手段が、配列置換である。

根全体を $\alpha'_1 \sim \alpha'_n$ と呼び替え、「 α'_1 、 α'_2 、 α'_3 、 $\cdots$ は、この順に、 α_p 、 α_q 、 α_r 、 $\cdots$ に等しい」と“配列で指定”すれば、 $\alpha'_1 \sim \alpha'_n$ と $\alpha_1 \sim \alpha_n$ の全対応が明示される（という意味のことをガロアが述べている：現代数学では写像の概念を使うから、配列の意義が乏しい）

が、古典論/ガロア論文では重要である)。

根の名称変更は、添え字変更でもあるから、添え字 (数列の) 置換でも表わせる。

配列置換を、置換とも略記する。「根を置換する」と言った場合も、やはり n 根の配列置換であり、或る根の場所に別の根が来たことを意味する。2 根の入れ替え (互換) は、 n 根のうち “2 根を動かし他は動かさない” 配列置換である。

配列は、“置換の仕方を指定する手段” に過ぎず、頭の中で仮想するだけでもよい。我々は置換が、配列に作用する、根の関数に作用する、などと言う。

興味は、根の関数のほうにあり、我々が計算したいものである。

置換すなわち根の名称変更が、“根の関数” を変えるか変えないかが主題である。

置換とは操作である。3 つの置換、と言え、3 種類の置換の仕方、を意味する。

n 次方程式の解法では、 n 文字配列を扱う (すべての文字を 1 つの α_1 に書き換える、などの操作は配列置換ではなく、我々を行わない)。

n 文字配列の置換は、“変えない” ことも含めて $n!$ 通り、すなわち有限ヶである。

「配列 α, β, γ を 配列 β, γ, α に順送り置換」したとき、関数 α は関数 β に、 β は γ に、 γ は α に変わる。関数 $\alpha + \beta$ は、 $\beta + \gamma$ に変わる。関数 $\alpha\beta\gamma = \beta\gamma\alpha$ は変化しない。 $\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha$ は、 $\beta^2\gamma + \gamma^2\alpha + \alpha^2\beta$ という同じ関数になる。

「配列 α, β, γ を 配列 β, α, γ に置換」したら (つまり α, β を入れ替えたら)、 $\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha$ は、別の関数 $\beta^2\alpha + \alpha^2\gamma + \gamma^2\beta$ に変わる。

4 次方程式の根の関数で「 α と β を入れ替える」と言え、配列 $\alpha, \beta, \gamma, \delta$ を $\beta, \alpha, \gamma, \delta$ に変えたことを意味する。

2) 置換対称性

根の関数の対称性、とは「どんな置換で変わるか、または不変か」を意味する。

根の関数が、任意置換で不変なら、対称関数 (対称式) という (ただし重要なことに下線部の定義は、根の “有理式” に適用されるのである：次項で述べる)。

非対称関数とは、何らかの置換で値 (関数形) が変わる関数を言う (置換の仕方によっては変わらないこともある)。

ガロア論文では、根の関数形のことを、関数の値、量などとも恣意的に言う。

$\alpha + \beta$ と $\beta + \alpha$ は、同じ関数形、同じ量、同じ値である。

$\alpha - \beta$ と $\beta - \alpha$ は、異なる関数形、異なる量、($\alpha = \beta$ でない限り) 異なる値である。

非対称な根の関数には、様々な程度の対称性がある (対称性と対称は違う)。

2 次方程式の根の関数 $\alpha - \beta$ は、2 乗すれば対称式になるので対称性がかなり高い。

4 次方程式の根の関数を考えると、 $\alpha + \beta$ は、 γ, δ を含まないから非対称式であ

る。“ α 、 β の相互置換について対称”と言えるが、対称関数（対称式）ではない。

対称性の程度（高い、低い）に興味をもつ理由は、各根 α 、 β 、 $\dots$ という非対称な諸関数を、基本対称式の（巾開方値の）組み合わせで表す、という最終目標に向かって「より高対称な式」と等号で結んでいくことが、解法の唯一の道だからである。

根 $\alpha_1 \sim \alpha_n$ の関数の中で、「1 つの根 α_k 」は、最も対称性の低い関数だろうか？

対称性の“高さ”を、“何とおりの置換で不変か”で測定してみれば、関数 α_k は、 α_k 以外の任意置換、 $(n-1)!$ 通りで不変だから、むしろ対称性はかなり高い。

一方、“全根の或る配列”は、これを不変に保つ置換が、「置換しないという置換」1 つだけだから、最も対称性が低い。

既約方程式の n 根からなる 1 次関数、 $V = A_1 \alpha_1 + A_2 \alpha_2 + \dots + A_n \alpha_n$ 、を考えてみる。 $A_1 \sim A_n$ を、根の任意置換で V が必ず別の値になるように決めると、 V は、 $n!$ 個の異なる値をとる（既約方程式の根はみな異なる）。 V は、単一の関数で“最も低い対称性”を示す一例であり、全根の**配列**が目に見える関数である。

最も対称性の低い関数の組（すべての根）を、対称関数（に様々な巾開方を行なった形）で表せたとき方程式が解ける、と想像できる。

3) 根の任意置換で不変な関数は、基本対称式で表せる

短く言うと、**対称式は基本対称式で表せる**。

この定理は非常に有用であり頻繁に利用する。実例をみれば意味が明瞭なので、他書から証明（数学的帰納法）を借用するのは省略し、先に進む。

問題：下記を基本対称式で表せ

答

$$\begin{aligned}\alpha^2 + \beta^2 + \gamma^2 &= (\alpha + \beta + \gamma)^2 - 2(\alpha\beta + \beta\gamma + \gamma\alpha) \\ \alpha^3 + \beta^3 + \gamma^3 &= (\alpha + \beta + \gamma)^3 - 3(\alpha + \beta + \gamma)(\alpha\beta + \beta\gamma + \gamma\alpha) + 3\alpha\beta\gamma \\ \alpha^2\beta^2 + \beta^2\gamma^2 + \gamma^2\alpha^2 &= (\alpha\beta + \beta\gamma + \gamma\alpha)^2 - 2\alpha\beta\gamma(\alpha + \beta + \gamma) \\ \alpha^3\beta^3 + \beta^3\gamma^3 + \gamma^3\alpha^3 &= (\alpha\beta + \beta\gamma + \gamma\alpha)^3 - 3(\alpha + \beta + \gamma)(\alpha\beta + \beta\gamma + \gamma\alpha)\alpha\beta\gamma + 3\alpha^2\beta^2\gamma^2\end{aligned}$$

対称式 = 与えられた方程式の係数（有理数）から有理計算できる量 = 既知数、という関係を、ガロアは「対称式は既知数」、「対称式だから求まる」と短く述べた。

根の非対称式は、「未知量」であるが、その値が求まるとしたら、根の対称式（既知数）から計算する以外になく、我々の計算ルールでは巾開方する他ないのである。

【方程式の解き方の糸口】

「根の関数 θ が対称式なら、対称の定義（任意置換で不変）から、 $\sqrt[m]{\theta}$ も対称式」と言えるか？ 実は言えないことを、我々は 2 次方程式の例ですでに知っている。

$\sqrt[m]{\theta}$ は、置換で変化する式に等しいことがあるので、有理的な対称式 θ とは区別しなければならない。例： $\sqrt{(\alpha + \beta)^2 - 4\alpha\beta} = \alpha - \beta$ 、または $\beta - \alpha$

すなわち、 α 、 β が 2 次方程式の根なら、 $\sqrt{\text{対称式}} = \text{非対称式}$ 、となる！

注：上の $\sqrt{\quad}$ 量の意味 $= |\alpha - \beta|$ と決めれば、両辺が対称式、と言ったら適切でない。

その言い方は、 m 次巾開方 $m\sqrt{\quad}$ を含む式に使えず、等式 $\sqrt{-1} = \pm i$ も表現できない。

$m\sqrt{\quad}$ (正の実数) は、 $\sqrt[3]{8} = 2$ の如く一意的な既知数とみなすのが自然だが、 $m\sqrt{\quad}$ (文字式)

は意味の指定 (25 頁) なしに書くとき、 m 個の巾根のうちの 1 つを言う総称的

な略号であり、 $\sqrt{\{(\alpha + \beta)^2 - 4\alpha\beta\}}$ も、 $\alpha - \beta$ 、 $\beta - \alpha$ のいずれかを意味する略号である。

$\sqrt{\text{対称式}}$ を、対称式と言うと誤解 (ときには誤り) を生じると分かった。これは注目すべきことである。“対称式の巾開方 (を組み合わせで) 書ける非対称式”を見つけて出す一般的な方法があれば、方程式の一般解法が得られる可能性がある。

4. 方程式の解法過程に現れる、根の非対称関数

根の非対称関数 (非対称式) が “求まる” とは、“対称式 (方程式の係数文字から計算できる量) の巾開方” を使って表せることを意味する。

究極の非対称関数の組 $\alpha_1, \dots, \alpha_n$ は、一段階で計算できる筈がなく、途中段階で、“根の非対称関数の組み合わせ = 対称式の巾開方の組み合わせで表せる式”、という関係を扱うであろう。

注釈) 非対称関数 θ_k の組み合わせで、より高対称な Θ を作るとは、
 $\alpha_1, \dots, \alpha_n$ の積 $\rightarrow$ 対称関数 $\alpha_1\alpha_2\cdots\alpha_n$ 、のような作り方のことでない。
逆方向の計算手順 (各 $\theta_k \leftarrow \Theta$) が不明な作り方は、意味がない。

既約方程式の解法過程で、根の非対称関数は、どんな現れ方をするだろうか？

3 次方程式の解法途中で例えば 非対称関数 $\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha$ を扱う必要が生じるなら、 $\alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2$ も扱うことになる。 α 、 β の呼び変えて、この形に変わるからである。

同じ理屈から、既約 4 次方程式を解く過程で、もし $\alpha + \beta$ の計算が必要になるなら、“同時に” $\gamma + \delta$ についても同様の計算が必要である。4 根を求めるには、「 α 、 β 」だけでなく、「 α 、 β 」と「 γ 、 δ 」一組の対称性を考える必要がある。

既約 n 次方程式の根 α_1 が求まる計算原理とは、同時に $\alpha_2 \sim \alpha_n$ も求まる原理を意味する。解法は根の名称変更に影響されないから、常に $\alpha_1 \sim \alpha_n$ の平等性を保つ計算法を考えるしかない。既約方程式の一般解法では、 $\alpha_1 \sim \alpha_n$ のどれにも優先順位がない。

5. 対称性の異なる関数どうしを、どのように等式で結べるのか？

θ と $m\sqrt{\theta}$ の対称性が、同じでないということの意味を考えよう。

解法途中で必ず現れる筈の下記の関係式は、一見すれば不思議である。

非対称関数 = “対称式の様々な巾開方量” から構成される式

根を置換すると、左辺は別の関数になりうるのに、右辺は変化し得ない、…？

まず、2 次方程式の解法を見直そう。2 根を α 、 β とする。

$(\alpha - \beta)^2 = (\alpha + \beta)^2 - 4\alpha\beta = A$ と呼ぶと、 A は、対称式だから既知数である (20 頁)。

$\alpha - \beta = \sqrt{A}$ 、または $-\sqrt{A}$ (むろん、 $= \sqrt{A}$ と $= -\sqrt{A}$ は同時に成り立たない)

$\alpha - \beta = \sqrt{A}$ を使い、 $\alpha + \beta =$ 基本対称式 (既知数) との連立方程式より、

$\alpha = 1/2 (\alpha + \beta) + 1/2 \sqrt{A}$ 、 $\beta = 1/2 (\alpha + \beta) - 1/2 \sqrt{A}$ を得る。… ☆

根 α 、 β を置換すると、一方の等式 $\rightarrow$ 別の等式、と移り変わる。

$\alpha - \beta = -\sqrt{A}$ のほうを使ってもよく、

$\alpha = 1/2 (\alpha + \beta) - 1/2 \sqrt{A}$ 、 $\beta = 1/2 (\alpha + \beta) + 1/2 \sqrt{A}$ を得る。… ★

以上のことを一般化すると、次のように言える。

- ・ 解法で扱う非対称関数は、単独で現れない $\leftarrow$ 根を名称変更 (置換) した関数を使っても、同様に解法計算できる
- ・ 非対称関数は、求まるなら巾開方量 (無理数) を含む $\leftarrow$ 任意文字係数の方程式では、根の対称関数のみを有理計算できる
- ・ m 次巾開方は、 m ケの異なる値を生む $\leftarrow$ 「 θ の m 次巾開方値 $= \omega_m \sqrt[m]{\theta}$ 、 $\omega_m^2 \sqrt[m]{\theta}$ 、 $\dots$ 、 $\omega_m^{m-1} \sqrt[m]{\theta}$ のうちの 1 つ」という自明なことではなく、もっと重要なことがある。
2 次方程式は、「 $\alpha - \beta = \sqrt{A}$ または $-\sqrt{A}$ 」だけで解けたのではなく、連立方程式を作ったから ☆ のように解けた (☆ or ★ は、 $\sqrt{A}$ or $-\sqrt{A}$ と同等)。
一般に、 m 次巾開方から、同時に成り立つ m ケの等式 を作る方法を次節で示す。
 - * 非対称関数 $= \sqrt[m]{A}$ (より高対称な関数)、という m ケの等式 を作ると、
根の名称変更で、等式が別の等式に移り変わる。
 - * 「置換で変化する式 $=$ 変化し得ない式」という等式は、単一式なら矛盾だが、
複数の等式が同時に成り立つ “連立式” の場合は、矛盾といえない。
解法過程では、対称関数の様々な巾開方をとるたびに、より低対称な非対称関数の値を得る。究極の非対称関数は n 根、 α_1 、 $\dots$ 、 α_n である。

2 次巾開方 $\rightarrow$ 2 元連立方程式から、 m 次巾開方 $\rightarrow m$ 元連立方程式への一般化を考察するとき、もう一つ重要なことに注目する。2 次方程式では、2 次巾開方 $\sqrt{\quad}$ をとった後に、有理計算だけで根を得た。これは以下のように一般化される。

方程式を解く過程で、様々な次数の巾開方をとるが、**素数 n 次の既約方程式を解くとき、 n 次巾開方を行なうのは、根が求まる (計算が終了する) 段階である。**

α_1 、 $\dots$ 、 α_n は、平等な n ケ 1 組の非対称関数だから、より高対称な関数と $=$ で結ぶには、 n ケの式を要する。 n ケの連立式は、 n 次巾開方したときにだけ得られる。

n が素数でなければ、各根 $= \sqrt[n]{\quad}$ を含む式、となって計算が終了するとは限らず、

$\sqrt[p]{\sqrt[q]{\{\dots\}}}$ ($pq=n$) などを経由する可能性を生じ、一般的に言えない。ガロアは、議論を素数次方程式に限った(4次方程式を応用問題とみた)ことにより解法理論を得た。

ガロアの解法理論のアイデアは独特であって、
各根(答) $\longleftrightarrow$ 根の非対称関数(途中段階) $\longleftrightarrow$ 対称式(基本対称式で書ける値)
の関係を、両方向から考察する。

- 1) 各根からなる有理式 $\leftarrow$ 最後に、 n 次巾開方をとって答に達する $\leftarrow \dots \leftarrow$
- 2) 各根からなる有理式 $\rightarrow$ 最初の段階で、 n 乗して対称性を高める $\rightarrow \dots \rightarrow$
ここで、“各段階の関数”は、“隣の段階の関数”から計算できねばならない。
次節で示す 2) の方法が、根の実際の計算法になる。

§2 置換対称性を利用した、方程式の一般解法

1. 3次方程式の解法

1) 根の関数を、より高対称な根の関数から算出する方法

1) 3次方程式の「各根 α 、 β 、 γ 」という3つの非対称関数を、「より高対称な関数 θ 」で表す方法を考えたい。下記の θ を考案すると、 θ^3 が各根よりも高対称性となる。

$$\theta = \alpha + \omega \beta + \omega^2 \gamma \quad \omega^3 = 1$$

この驚くべき式は、2次方程式なら「 $\theta = \alpha + \omega \beta$ 、 $\omega^2 = 1$ 」となり、非対称式 $\alpha - \beta$ と対称式 $\alpha + \beta$ を作り出す。ラグランジュが、この θ を発明して3次方程式を解き、ガロアが一般化に成功した。以下のことは独創的だが、初等数学で説明できる。

α 、 β 、 γ の配列を下記のように、順送りする置換を考える(一斉に左へ送り、左端の文字は右にもってくる)。

$$\alpha, \beta, \gamma \rightarrow \beta, \gamma, \alpha \rightarrow \gamma, \alpha, \beta \rightarrow (3\text{ 回目の置換で}) \text{ もとの } \alpha, \beta, \gamma \text{ に戻る。}$$

これらの置換で θ は、異なる値を経て θ に戻る。 $\omega^3 = 1$ 、 $\omega^4 = \omega$ に注意する

$$\begin{aligned} \theta = \alpha + \omega \beta + \omega^2 \gamma &\rightarrow \beta + \omega \gamma + \omega^2 \alpha = \omega^2 (\alpha + \omega \beta + \omega^2 \gamma) = \omega^2 \theta \\ &\rightarrow \gamma + \omega \alpha + \omega^2 \beta = \omega (\alpha + \omega \beta + \omega^2 \gamma) = \omega \theta \\ &\rightarrow \alpha + \omega \beta + \omega^2 \gamma = \text{もとの } \theta \end{aligned}$$

上記の3乗は、右辺を見て、 $(\beta + \omega \gamma + \omega^2 \alpha)^3 = \omega^6 \theta^3 = \theta^3$ 、 $(\gamma + \omega \alpha + \omega^2 \beta)^3 = \omega^3 \theta^3 = \theta^3$ と分かる。すなわち、 **θ^3 は、順送り置換で不変に留まる!**

α 、 β 、 γ で作った θ は、より対称性の高い θ^3 という値(の巾開方)から算出できる。
各根を“根の対称式から算出する”という目標に、一歩近づく可能性がある。

一般に $\theta = \alpha_1 + \omega \alpha_2 + \cdots + \omega^{n-1} \alpha_n$ で ($\omega^n = 1$)、各根を (左へ) 1 つ順送り置換した式は、右辺を ω で割った式と同じだから、この置換で θ^n は変化しない ($1/\omega^n = 1$)。

1 の 3 乗根は 3 つあり (ω 、 ω^2 、1)、どの根でも、順送り不変量を作れるのだから、 θ だけでなく計 3 つの、同時に成り立つ独立な式、すなわち連立式を作れる。

$$\begin{aligned} \alpha + \omega \beta + \omega^2 \gamma &= \theta \\ \alpha + \omega^2 \beta + \omega \gamma &= \theta' & \omega \text{ の代わりに、別の根 } \omega^2 \text{ を使った} \\ \alpha + \beta + \gamma &= \text{既知の値 (基本対称式)} & \omega \text{ の代わりに、別の根 } 1 \text{ を使った} \\ &\cdots \cdots (1) \end{aligned}$$

すると θ 、 θ' の値を知れば (θ 、 θ' を計算対象に追加できれば)、連立 1 次方程式 (1) を解く 有理計算 で、3 根 α 、 β 、 γ が得られる。

II) θ^3 、 θ'^3 が、どんな式 (根の関数) から構成されているかをみよう。

$$\begin{aligned} \theta^3 &= (\alpha + \omega \beta + \omega^2 \gamma)^3 = \alpha^3 + \beta^3 + \gamma^3 + 6 \alpha \beta \gamma + 3 \omega (\alpha^2 \beta + \beta^2 \gamma + \gamma^2 \alpha) + 3 \omega^2 (\alpha \beta^2 + \beta \gamma^2 + \gamma \alpha^2) \\ \theta'^3 &= (\alpha + \omega^2 \beta + \omega \gamma)^3 = \alpha^3 + \beta^3 + \gamma^3 + 6 \alpha \beta \gamma + 3 \omega (\alpha \beta^2 + \beta \gamma^2 + \gamma \alpha^2) + 3 \omega^2 (\alpha^2 \beta + \beta^2 \gamma + \gamma^2 \alpha) \\ &\cdots \cdots (2) \end{aligned}$$

(2) に現れた “非対称関数” を、 $\alpha^2 \beta + \beta^2 \gamma + \gamma^2 \alpha = \varphi$ 、 $\alpha \beta^2 + \beta \gamma^2 + \gamma \alpha^2 = \varphi'$ と書く。

φ 、 φ' は根の任意置換で、 φ 、 φ' のいずれかになる (実際に確かめよう)。

すると、 φ 、 φ' の和、積は “任意置換で不変” だから、基本対称式で表せる。

$$\begin{aligned} \varphi + \varphi' &= (\alpha^2 \beta + \beta^2 \gamma + \gamma^2 \alpha) + (\alpha \beta^2 + \beta \gamma^2 + \gamma \alpha^2) = (\alpha \beta + \beta \gamma + \gamma \alpha) (\alpha + \beta + \gamma) - 3 \alpha \beta \gamma \\ \varphi \varphi' &= (\alpha^2 \beta + \beta^2 \gamma + \gamma^2 \alpha) (\alpha \beta^2 + \beta \gamma^2 + \gamma \alpha^2) = \alpha^3 \beta^3 + \beta^3 \gamma^3 + \gamma^3 \alpha^3 + \alpha \beta \gamma (\alpha^3 + \beta^3 + \gamma^3) + 3 \alpha^2 \beta^2 \gamma^2 \\ &= (\alpha \beta + \beta \gamma + \gamma \alpha)^3 - 3 \alpha \beta \gamma (\alpha \beta + \beta \gamma + \gamma \alpha) (\alpha + \beta + \gamma) + \alpha \beta \gamma \{ (\alpha + \beta + \gamma)^3 \\ &\quad - 3 (\alpha + \beta + \gamma) (\alpha \beta + \beta \gamma + \gamma \alpha) \} + 9 \alpha^2 \beta^2 \gamma^2 \quad \Rightarrow 20 \text{ 頁参照} \end{aligned}$$

$x^3 + a x^2 + b x + c = 0$ の係数を、上の式 (の基本対称式) に代入すると、

$$\begin{aligned} \underline{\varphi + \varphi'} &= -ab + 3c, \quad \underline{\varphi \varphi'} = b^3 - 6abc + a^3 c + 9c^2 & \text{係数が既知数となった 2 次方程式} \\ X^2 + (ab - 3c) X + b^3 - 6abc + a^3 c + 9c^2 &= 0 & \text{を得た。} \end{aligned}$$

この解 $= \varphi$ 、 φ' を (2) に代入し、 θ^3 、 θ'^3 から θ 、 θ' を得て (記法は次頁注釈)、3 次方程式の解公式を得る (式の全体像は、付録 137 頁参照)。

φ 、 $\varphi' = \sqrt{\text{既知数}}$ を含む有理式、となり (既知数とは係数 a 、 b 、 c の有理式)、 θ^3 、 $\theta'^3 = \sqrt[3]{\varphi}$ 、 $\sqrt[3]{\varphi'}$ と対称式」からなる既知数、その $\sqrt[3]{}$ をとり、 θ 、 θ' を得る。

α 、 β 、 γ は、「 θ 、 θ' 、と $\alpha + \beta + \gamma$ 」からなる既知数から、有理計算される。

解公式が、 $\sqrt[3]{} \sqrt{}$ の形を含むと分かった。 $x^3 + a x^2 + b x + c = 0$ を変形しようとせず、3 根からなる非対称式を対称式にまで高め、最後に a 、 b 、 c を代入して答を得た。

3 次方程式の解法に登場した根の関数、それぞれの置換対称性

α, β, γ のどれをも不変に保つ置換は、「置換しないという置換」のみ

θ^3, θ'^3 は、いずれも「根の順送り置換で不変」

$\varphi + \varphi'$ と $\varphi \varphi'$ は「根の任意置換で不変」つまり対称関数

各ステップを結ぶ計算法が存在したから、解けた

【実用的な注釈】 θ^3, θ'^3 から θ, θ' を求めるときの、巾開方の書き方

φ, φ' を 前頁 (2) に代入すると (ω と ω^2 が共役複素数、 φ と φ' が共役複素数または実数なので)、 θ^3 と θ'^3 は実数または共役複素数になる。すると θ, θ' も実数または複素共役とせねばならない (θ, θ' を非共役に書けば θ^3, θ'^3 も非共役になるので)。

前頁 (1) で両辺を足すと、 $\omega^2 + \omega + 1 = 0$ より、 $3\alpha = \theta + \theta' +$ 有理数だから、上記のことから、 α は常に実数になる (初めに $\theta = \beta + \omega\gamma + \omega^2\alpha$ と書けば、 β が実数)。

$\sqrt{\theta^3}, \sqrt{\theta'^3}$ から θ, θ' への対応には、 ω 倍、 ω^2 倍の任意性があるが、対応づけ方は揃えねばならない。 θ^3, θ'^3 が実数なら θ, θ' も実数とする対応が、簡明であろう。

< **m 次巾開方の記法** > を考えるとき、2 ケー対の共役複素数という上記の概念は、使えない。m 次の話に一般化できるよう、1 の 3 乗根を $\omega, \omega', \omega''$ と言い直せば、

$$\begin{aligned}\theta &= \alpha + \omega\beta + \omega^2\gamma & (3 \text{ 式は独立 ; それぞれの 3 乗量}) \\ \theta' &= \alpha + \omega'\beta + \omega'^2\gamma & \text{が根の順送り置換で不変)} \\ \theta'' &= \alpha + \omega''\beta + \omega''^2\gamma\end{aligned}$$

数値 R または既知の文字式 R で、 $\theta^3 = R^3$ と書けたとき、 R が含む ω を、 $\omega \rightarrow \omega', \omega \rightarrow \omega''$ と置き換え、簡単に $R \rightarrow R', R \rightarrow R''$ を得る。巾開方のとり方は ;

$$\underline{\theta = R, \omega R, \text{ or } \omega^2 R, \quad \theta' = R', \omega' R', \text{ or } \omega'^2 R', \quad \theta'' = R'', \omega'' R'', \text{ or } \omega''^2 R''}$$

$\theta, \theta', \theta''$ の書き方は、 $3 \times 3 \times 3$ 通りではなく 3 通りしかないのであり ($\theta = \omega R$ とするなら、 $\theta' = \omega' R'$ など)、 $\omega \rightarrow \omega', \omega \rightarrow \omega''$ の置き換えで揃えねばならない。

θ の値を、 $R, \omega R, \omega^2 R$ から選ぶ任意性は、根の順送り置換で、 θ の定義を変更 (根を名称変更) できる任意性に相当する。 $\theta = \omega R, \theta' = \omega' R', \theta'' = \omega'' R''$ と書けば、 $\omega, \omega', \omega''$ と $\theta, \theta', \theta''$ の対応が見易いが、(θ の定義を変更しない) 下記が簡明である。

$\theta = R, \theta' = R', \theta'' = R''$ と書こう。 この場合、 R が実数なら θ も実数になる。

記法 $\sqrt[m]{}$ を、上の意味で一意的に、 $\sqrt[3]{\theta^3} = \theta, \sqrt[3]{\theta'^3} = \theta', \sqrt[3]{\theta''^3} = \theta''$ 、と書く。

$\sqrt[m]{}$ であれば、1 の m 乗根 $\omega, \omega', \dots$ を用い、 $\sqrt[m]{\theta^m} = \theta, \sqrt[m]{\theta'^m} = \theta', \dots$ と書く。

$\zeta^2 = 1$ の根を用いた $\sqrt{(\alpha + \zeta\beta)^2}$ では、 $\sqrt{(\alpha + \beta)^2} = \alpha + \beta, \sqrt{(\alpha - \beta)^2} = \alpha - \beta$ となる。

【注】 以上は、1 の m 乗根に対応する“**m ケー組の $\sqrt[m]{}$ の記法**”を決めたのであり、巾根一般を、 $\sqrt{(\alpha + 3\beta + 2\gamma)^2} = \alpha + 3\beta + 2\gamma$ などと略記しよう、という意味でない。

2) n 根の関数、 $\theta = \alpha_1 + \omega \alpha_2 + \cdots + \omega^{n-1} \alpha_n$ は、解法の出発点である

θ は、根の関数の対称性を一段階高めるために発明された。

・3 次方程式の解法の出発点 (α, β, γ の対称性を高める) は、以下のようであった。

$\theta^3 = (\alpha + \omega \beta + \omega^2 \gamma)^3$ は、“ α, β, γ の順送り置換で不変”、 $\omega^3 = 1$

θ の3つの形のうち、 $\omega = 1$ に相当するのは、基本対称式 $\alpha + \beta + \gamma$

$\omega \neq 1$ では、非対称式 $\alpha + \omega \beta + \omega^2 \gamma, \alpha + \omega^2 \beta + \omega \gamma$

・2 次方程式の解法の出発点 (α, β の対称化) も、同じように言える。

$\theta^2 = (\alpha + \zeta \beta)^2$ は、“ α, β の順送り置換 (互換) で不変”、 $\zeta^2 = 1$ (ζ ; ゼータ)

θ の2つの形のうち、 $\zeta = 1$ に相当するのは、基本対称式 $\alpha + \beta$

$\zeta \neq 1$ では、非対称式 $\alpha + \zeta \beta = \alpha - \beta$ になる

一般に、根の関数の組が“或る置換”で互いに変換されるならば、非対称関数を、より高対称な式から算出する手順が生じる。

3) 根の非対称関数を、より高対称な関数と等号で結ぶ一般手法

～ 解法における最も重要な計算手法 ～

n 根の関数 θ に対し、根の“或る置換”をする (全根の順送り、とは限らない)。

“或る置換”を m 回くり返すと θ がもとの形に戻る、という m は、任意置換で必ず存在する (3 章で証明するが、文字配列の置換は有限種類だから直感的にも分かる)。

【手法の説明 1】

θ に、或る置換を1回行なったものを θ_1 と呼ぶ。 θ_1 をもう一度置換したもの (θ の2回置換) を、 θ_2 と呼び、…、同様に θ_{m-1} まで名付ける。すなわち、“或る1つの置換”の反復で、 $\theta \rightarrow \theta_1 \rightarrow \theta_2 \rightarrow \cdots \rightarrow \theta_{m-1} \rightarrow \theta$ 、元に戻る。

すると、 $\omega^m = 1$ の根を用いて、 $\Theta = \theta + \omega \theta_1 + \cdots + \omega^{m-1} \theta_{m-1}$ を作れば、

Θ^m は、上の“或る置換”の任意反復に対し、不変に留まる。すると以下のように、

θ よりも高対称な関数 Θ^m (および $\Theta'^m, \Theta''^m, \dots$) で、 θ を書き表せる。

$$\sqrt[m]{\Theta^m} = \theta + \omega \theta_1 + \cdots + \omega^{m-1} \theta_{m-1} \quad \leftarrow \text{前頁の巾開方のとり方}$$

$$\sqrt[m]{\Theta'^m} = \theta + \omega' \theta_1 + \cdots + \omega'^{m-1} \theta_{m-1}$$

$$\sqrt[m]{\Theta''^m} = \theta + \omega'' \theta_1 + \cdots + \omega''^{m-1} \theta_{m-1}$$

……

という、 m ヶの等式が、

1 の m 乗根「 $\omega, \omega', \omega'', \dots$ 」または原始根 ω で書いた「 $\omega, \omega^2, \dots, \omega^{m-1}, 1$ 」に
応じて生じる (m 元連立 1 次方程式が生じる)。

* 「 $\theta, \theta_1, \dots, \theta_{m-1}$ 」が、 $\alpha_1, \alpha_2, \dots, \alpha_n$ そのものである段階 ($m = n$) なら、
 $\theta \rightarrow \theta_1 \rightarrow \theta_2 \rightarrow \cdots \rightarrow \theta_{m-1} \rightarrow \theta$ という置換 (“或る置換”の反復) は、
全根の順送り置換を意味する。

* $\Theta^m, \Theta'^m, \Theta''^m, \dots$ 、が根の対称式で書かれた段階なら、「 $\theta, \theta_1, \dots, \theta_{m-1}$ 」の各値が求まる（既知数になる）。

【手法の説明 2】

我々は、次のようにも考える：目の前にある m 個の、 $\theta, \theta_1, \theta_2, \dots, \theta_{m-1}$ から、より高対称な関数を作りたい。これらが互いに移り変わる“置換の仕方”を見つければ、“手法の説明 1”の形で、より高対称な $\Theta^m, \Theta'^m, \dots$ を作れる。

3 次方程式で、 $\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha = \varphi$ の対称性を高めたのも、この手法である。

任意互換で φ は、 $\alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2 = \varphi'$ になり、2 度の互換で φ に戻るから、

$\Phi = \varphi + \zeta\varphi', (\zeta^2 = 1)$ から Φ^2 を作ると対称性が高まる。

$\zeta = 1$ を代入した $\varphi + \varphi'$ は、対称式

$\zeta = -1$ を代入した $\varphi - \varphi'$ は、対称式 $(\varphi - \varphi')^2 = (\varphi + \varphi')^2 - 4\varphi\varphi'$ の巾根

n 次方程式の解法とは、 n 文字配列の“あらゆる置換”を、“順送り置換（巡回置換が正式名）の組み合わせ”で表すことである、と 3 章で納得され、4 章で証明される。

【注】 非対称関数 = “より高対称な式の巾開方”を含む式、と書けたら、左辺と右辺を同義語とし、煩雑な右辺を書かずに「非対称関数が求まる（可能性がある）」と言う。2 次方程式なら、 $\sqrt{(\alpha + \beta)^2 - 4\alpha\beta}$ の記載を略し、「 $\alpha - \beta$ が求まる」と言う。また、 $\alpha + \beta$ は既知だから、 $\alpha - \beta$ が求まるのは「 α, β が求まる」のと同義である。

3 次方程式では、 $\sqrt[3]{\theta^3}$ の計算を書かずに、「 $\alpha + \omega\beta + \omega^2\gamma, \alpha + \omega^2\beta + \omega\gamma$ が求まる」と述べた。 $\alpha + \beta + \gamma =$ 既知だから、 α, β, γ は、連立 1 次方程式から有理計算できる。

2. 4 次方程式の解法

1) 4 が素数でないことに起因する、4 次方程式の特殊性

各根 $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ という非対称関数を、対称式に近づけたい。前節の方法に倣い、

$\theta = \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3 + \omega^3\alpha_4 \quad (\omega^4 = 1)$ を作ってみよう。

期待どおり「 θ^4 が、根の順送り置換で不変」になる。

$\omega^4 = 1$ の解 $i, -i, -1, 1$ を代入して独立な関数を 4 つ作れる …… ★

$$\theta_1 = \alpha_1 + i\alpha_2 - \alpha_3 - i\alpha_4$$

$$\theta_2 = \alpha_1 - i\alpha_2 - \alpha_3 + i\alpha_4$$

$$\theta_3 = \alpha_1 - \alpha_2 + \alpha_3 - \alpha_4$$

$$\theta_4 = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 \quad \text{既知量（基本対称式）}$$

根の添え字 1, 2, 3, 4 の順送り置換 $\rightarrow 2, 3, 4, 1 \rightarrow 3, 4, 1, 2 \rightarrow$ は、

$\theta_1, \theta_2, \theta_3$ 各々を $i, -i, -1$ で割ることの反復だから、4 乗値は不変。

$\alpha_1 \sim \alpha_4$ は、連立方程式★から有理計算して、 $\theta_1 \sim \theta_4$ で表せる。

ところが、この方法では次に、 $\theta_1 \sim \theta_3$ の対称性を高めることが不可能になる。

次の段階で、未知量 $\theta_1^4, \theta_2^4, \theta_3^4$ を組み合わせて、より高対称性の関数を作るのが、一般手法（26 頁）である。そのためには、“ $\theta_1^4, \theta_2^4, \theta_3^4$ を相互変換する或る置換”が存在せねばならないが、★をみると（ i を含む θ_1, θ_2 は、4 乗したとしても、 i を含まない θ_3^4 にはなりえないから）、 $\alpha_1 \sim \alpha_4$ のどんな配列置換を考案しても「 θ_1 と θ_3 」、
「 θ_2 と θ_3 」は相互変換されない。この難点は、素数乗根でない“1 の巾乗根 ($\omega^4 = 1$)”を使って ★ を作ったことから生じた。

n が非素数なら、 $\omega^n = 1$ の根の中には、1 以外にも非原始根がある。非原始根の巾乗で“1 の n 乗根すべて”は表せない。このため次の計算段階に進めないので、 $\sqrt[n]{}$ を、 $\sqrt[n]{}$ という素数次ごとの巾開方に分けて、下記のように試みよう。

2) 出発点を工夫した、4 次方程式の解法の実現

4 根を 2 根ずつの 2 組に分け、2 組を同時に扱う。既約方程式の根の平等性から、4 根の一斉置換、「 α_1 と α_2 を求める方法」かつ「 α_3 と α_4 を求める方法」を考える。

I) 2 次方程式に倣い、根の関数 $(\alpha_1 + \zeta \alpha_2)^2$ 、かつ $(\alpha_3 + \zeta \alpha_4)^2$ 、($\zeta^2 = 1$ 、 ζ ; ゼータ) から始めるのが、26 頁の一般手法の応用法であろう。 $\zeta = 1$ 、または -1

$\alpha_1 + \zeta \alpha_2$ 、つまり、 $\alpha_1 + \alpha_2$ と $\alpha_1 - \alpha_2$ の値が分かったときは、 α_1, α_2 が有理計算される。

$(\alpha_1 - \alpha_2)^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2$ なので、未知量は、 $\alpha_1 + \alpha_2$ と $\alpha_1\alpha_2$ に書き直され、この 2 つの関数は 2 根の相互置換、 $\alpha_1 \longleftrightarrow \alpha_2$ で不変である。対称性が少し高まった。

同様に、 α_3, α_4 のほうも、 $\alpha_3 \longleftrightarrow \alpha_4$ で不変な、 $\alpha_3 + \alpha_4$ と $\alpha_3\alpha_4$ に書き直される。

「4 根 $\alpha_1 \sim \alpha_4$ 」よりも高対称な 4 関数「 $\alpha_1 + \alpha_2, \alpha_3 + \alpha_4, \alpha_1\alpha_2, \alpha_3\alpha_4$ 」が求まれば、
 $X^2 - (\alpha_1 + \alpha_2)X + \alpha_1\alpha_2 = 0$ 、および、
 $X^2 - (\alpha_3 + \alpha_4)X + \alpha_3\alpha_4 = 0$ の解として、4 根が求まることになる。

II) 上の「 $\alpha_1 + \alpha_2$ と $\alpha_3 + \alpha_4$ 」および「 $\alpha_1\alpha_2$ と $\alpha_3\alpha_4$ 」よりも、さらに対称性の高い関数を作るには、やはり“26 頁の一般手法”を用いて、

$(\alpha_1 + \alpha_2) + \zeta(\alpha_3 + \alpha_4)$ 、および $\alpha_1\alpha_2 + \zeta\alpha_3\alpha_4$ を作ればよい ($\zeta^2 = 1$)。すなわち、置換「 $\alpha_1 + \alpha_2 \longleftrightarrow \alpha_3 + \alpha_4$ 」、「 $\alpha_1\alpha_2 \longleftrightarrow \alpha_3\alpha_4$ 」で不変な、より高対称な関数を作ろう。

・ $\zeta = -1$ を代入した関数は、2 乗すると対称性が高まる（一般手法）。

$$\begin{aligned} & \{(\alpha_1 + \alpha_2) - (\alpha_3 + \alpha_4)\}^2 \\ &= \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2 + 2(\alpha_1\alpha_2 + \alpha_3\alpha_4) - 2(\alpha_1\alpha_3 + \alpha_2\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_4) \end{aligned}$$

$$= \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2 - 2(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_4 + \alpha_4\alpha_1 + \alpha_1\alpha_3 + \alpha_2\alpha_4) + 4(\alpha_1\alpha_2 + \alpha_3\alpha_4)$$

$$= \text{対称式} + 4(\alpha_1\alpha_2 + \alpha_3\alpha_4)$$

両辺の巾開方をとるとき、25 頁の記法に従う。

$$\text{したがって、} (\alpha_1 + \alpha_2) - (\alpha_3 + \alpha_4) = \sqrt{\text{対称式} + 4(\alpha_1\alpha_2 + \alpha_3\alpha_4)} \quad \cdots (1)$$

$$\cdot \quad \zeta=1 \text{ を使うと、} (\alpha_1 + \alpha_2) + (\alpha_3 + \alpha_4) = \text{基本対称式 (既知)} \quad \cdots (2)$$

すなわち、 $\alpha_1\alpha_2 + \alpha_3\alpha_4$ が求まれば、 $\alpha_1 + \alpha_2$ と $\alpha_3 + \alpha_4$ は、(1)、(2) から求まる。

$\alpha_1\alpha_2$ と $\alpha_3\alpha_4$ も、以下のように扱える。

$\alpha_1\alpha_2 + \alpha_3\alpha_4$ が求まったときは、「基本対称式 $\alpha_1\alpha_2\alpha_3\alpha_4 = \text{既知}$ 」を使って、

$$\alpha_1\alpha_2 - \alpha_3\alpha_4 = \sqrt{(\alpha_1\alpha_2 - \alpha_3\alpha_4)^2} = \sqrt{\{(\alpha_1\alpha_2 + \alpha_3\alpha_4)^2 - 4\alpha_1\alpha_2\alpha_3\alpha_4\}} \text{ も求まる。}$$

$\alpha_1\alpha_2$ と $\alpha_3\alpha_4$ は、上 2 式から有理計算で求まる。

III) $\alpha_1\alpha_2 + \alpha_3\alpha_4$ は何から求まるか？

これよりも対称性の高い、根の関数を作るには、対称性を高める一般手法 (26 頁)、 $\Theta^m = (\Theta + \omega \Theta_1 + \cdots + \omega^{m-1} \Theta_{m-1})^m$ が、どう利用できるだろうか。

4 次方程式の解公式は、3 次方程式の解公式を包含するから (7 頁)、「3 文字の順送り置換で不変な関数を作り、3 次巾開方量を得る」計算が利用できるのではないか？

$\alpha_1\alpha_2 + \alpha_3\alpha_4$ において、例えば α_1 に対する他 3 根「 $\alpha_2, \alpha_3, \alpha_4$ 」の相対配置を置換してみよう (この方法は、どの 1 根に対する他 3 根の配列置換でも構わない、という平等性を保っている)。

$\alpha_2, \alpha_3, \alpha_4$ の添え字 2, 3, 4 の順送り置換 $\rightarrow 3, 4, 2 \rightarrow 4, 2, 3 \rightarrow$ もとに戻る。

すなわち、 $\alpha_1\alpha_2 + \alpha_3\alpha_4 \rightarrow \alpha_1\alpha_3 + \alpha_4\alpha_2 \rightarrow \alpha_1\alpha_4 + \alpha_2\alpha_3 \rightarrow$ もとに戻る。

そこで、3 次方程式でみた順送り置換での不変量 $(\alpha + \omega \beta + \omega^2 \gamma)^3$ と同様に考え、 α, β, γ の代わりに、 $\alpha_1\alpha_2 + \alpha_3\alpha_4$ 、 $\alpha_1\alpha_3 + \alpha_4\alpha_2$ 、 $\alpha_1\alpha_4 + \alpha_2\alpha_3$ を使えばよい。

上記の順送り置換で、 $\Theta \rightarrow \omega^2 \Theta \rightarrow \omega \Theta \rightarrow \Theta$ となるような ($\omega^3 = 1$)、

$$\Theta = (\alpha_1\alpha_2 + \alpha_3\alpha_4) + \omega(\alpha_1\alpha_3 + \alpha_4\alpha_2) + \omega^2(\alpha_1\alpha_4 + \alpha_2\alpha_3) \text{ が作れる。}$$

すなわち、 Θ^3 は上記の順送り置換で不変となる (対称性が高まった)。

ω 以外の 2 根、 ω^2 と 1 を使えば、 Θ と独立な下記の式も作れる。

$$\Theta' = (\alpha_1\alpha_2 + \alpha_3\alpha_4) + \omega^2(\alpha_1\alpha_3 + \alpha_4\alpha_2) + \omega(\alpha_1\alpha_4 + \alpha_2\alpha_3) \quad \omega^4 = \omega \text{ と書き直した}$$

$$\Theta'' = (\alpha_1\alpha_2 + \alpha_3\alpha_4) + (\alpha_1\alpha_3 + \alpha_4\alpha_2) + (\alpha_1\alpha_4 + \alpha_2\alpha_3) \quad \text{基本対称式になった}$$

Θ と Θ' が求まれば、(Θ'' は既知なので) 上の 3 元連立 1 次方程式を解いて、 $\alpha_1\alpha_2 + \alpha_3\alpha_4$ が求まる ($\alpha_1\alpha_3 + \alpha_4\alpha_2$ も $\alpha_1\alpha_4 + \alpha_2\alpha_3$ も求まるが、我々には必要ない)。

巾開方のとり方は、 $\Theta = \sqrt[3]{\Theta^3}$ 、 $\Theta' = \sqrt[3]{\Theta'^3}$ とする。 $\Theta'' = \text{既知の値}$

IV) Θ^3 と Θ'^3 は、どうやって求めるか？

幸いにも Θ^3 と Θ'^3 は、すでに知った方法で、より高対称な $(\Theta^3 + \zeta \Theta'^3)^2$ から、すなわち $\Theta^3 + \Theta'^3$ 、 $\Theta^3 \Theta'^3$ の値から、計算できる。なぜなら、上記、 Θ 、 Θ' の根配列をみると、「 α_1 と α_2 の互換」または「 α_3 と α_4 の互換」で、 $\Theta \longleftrightarrow \Theta'$ と変換され、「その他の互換」では、 Θ^3 、 Θ'^3 が不変と分かる。

したがって、 $\Theta^3 + \Theta'^3$ 、および $\Theta^3 \Theta'^3$ は、“任意の互換で不変”と分かった。

実は、“どんな配列置換でも、互換の組み合わせで表せる”定理（3章；36頁）があり、任意の互換で不変な関数は、任意置換で不変、つまり対称式なのである。

$\Theta^3 + \Theta'^3$ と $\Theta^3 \Theta'^3$ が、基本対称式で表せる（既知数になる）と分かったから*、 $X^2 - (\Theta^3 + \Theta'^3)X + \Theta^3 \Theta'^3 = 0$ を解いて、 Θ^3 と Θ'^3 が求まる（方程式の係数で表せる）。4次方程式が解ける原理が分かった。

IV) $\rightarrow$ III) $\rightarrow$ II) $\rightarrow$ I) に逆行する計算手順を、辿ってみるとよい。

注*) $\Theta^3 + \Theta'^3$ 、 $\Theta^3 \Theta'^3$ を展開すれば対称式になり（3次方程式より遙かに膨大な）、20頁のような計算で、4次方程式の解公式を係数文字で書ける。根の12次式 $\Theta^3 \Theta'^3$ の計算は気が重いが。

注) 到達した最高次数の式、 $\Theta^3 \Theta'^3$ が、 $4! = 24$ 次式でない理由は、次のような訳である：I) $\rightarrow$ II) で、4根からなる4次式の代わりに、「2次式 $\alpha_1 \alpha_2 + \alpha_3 \alpha_4$ を含む式の、2乗の $\sqrt{\quad}$ 」で、対称性を高めた。

巡回置換を繰り返す以上の方法の必然性は、対称性を分類する方法論すなわち群論で理解されることになる。

3. 5次方程式の一般解が、求まらないという予想

5次方程式の出発点の“根の非対称関数”は、各根“ α_1 、 α_2 、 α_3 、 α_4 、 α_5 ”である。

4次方程式で、 $\theta = \alpha_1 + \omega \alpha_2 + \omega^2 \alpha_3 + \omega^3 \alpha_4$ ($\omega^4 = 1$) から始めると、次に $\theta_1^4 \sim \theta_3^4$ を相互置換できなくなった。4根を2組に分割するとうまくいったが、素数 p 次方程式では、 $\sqrt[p]{\quad} \rightarrow \sqrt{\quad} \sqrt{\quad}$ と違い、 $\sqrt[p]{\quad}$ を低次の巾開方に分解できない。すなわち、素数 p への根を平等に扱うには、一段階で p 次巾開方 $\sqrt[p]{\quad}$ をとるしかない（23頁）ので、 $\theta = \alpha_1 + \omega \alpha_2 + \cdots + \omega^{p-1} \alpha_p$ ($\omega^p = 1$) を出発点にするしかない。

すなわち5次方程式では、 $\omega^5 = 1$ を用い、 $\theta = \alpha_1 + \omega \alpha_2 + \omega^2 \alpha_3 + \omega^3 \alpha_4 + \omega^4 \alpha_5$ から、“5根の順送り置換で不変”に留まる量、 θ^5 を作って出発する他ない。

1以外の4種の ω を代入した未知数を θ_1 、 θ_2 、 θ_3 、 θ_4 と呼ぶ（1を代入した θ は既知）

次は、 $\zeta^4 = 1$ を用い、“或る置換”で不変に留まる $(\theta_1^5 + \zeta \theta_2^5 + \zeta^2 \theta_3^5 + \zeta^3 \theta_4^5)^4 \cdots \star$ を作る選択肢しかない（5根の或る置換で、 θ_k の添え字が $1 \rightarrow 2 \rightarrow 4 \rightarrow 3 \rightarrow 1$ と巡回することと、上の計算経路を使う必然性は、4章ガロア論文で知られる）。

★に、1の4乗根、 $\zeta = 1, -1, i, -i$ を代入した4種の未知関数が、次の課題になる。

すると、未知関数どうしが移り変わる置換がない、という障害にぶつかる。

例えば、 $(\theta_1^5 + i\theta_2^5 - \theta_4^5 - i\theta_3^5)^4$ の展開式には、 $\theta_2^5 = \theta_3^5$ でない限り、文字 i が残るから、 $\alpha_1 \sim \alpha_5$ をどう置換しても、例えば $\zeta = -1$ に対応する式、 $(\theta_1^5 - \theta_2^5 + \theta_4^5 - \theta_3^5)^4$ になり得ない（4 文字 $\theta_1 \sim \theta_4$ の配列でなく、5 根 $\alpha_1 \sim \alpha_5$ の配列を置換するのだから、4 次方程式での解決策は真似できない）。5 次方程式の一般解法がないと予想できる。

第 3 章 根の配列置換の集合、および群

前章では、根の関数の対称性を利用して方程式を解いた。対称性とは、根の置換で関数形が変わるか不変かということであった。以下で置換の一般的性質を考える。

§ 1 置換の意味と方法

1. 根の配列置換、根の関数の変化

2 章の初めに述べたことを復習する。文字を $\alpha, \beta, \dots$ や、 α_k で書いてもよいが、添え字 $k = 1, 2, 3, \dots$ で示すと簡単である。

n 根のうち、“ α_1 と α_2 を入れ替える置換”とは、

添字の数列で書けば、 $1, 2, 3, \dots, n \rightarrow 2, 1, 3, \dots, n$ となり、

配列置換、 $\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n \rightarrow \alpha_2, \alpha_1, \alpha_3, \dots, \alpha_n$ を意味する。

この置換で、例えば根の関数 $2\alpha_1 + \alpha_2 + \alpha_3$ は、 $2\alpha_2 + \alpha_1 + \alpha_3$ に変化するが、関数形が $\alpha_1 + \alpha_2 + 2\alpha_3$ だったら、変化しない。

根の関数において、 $3\alpha + \beta \rightarrow \beta + 3\alpha$ は、置換でないことに注意しよう。

$3\alpha + \beta \rightarrow 3\beta + \alpha$ は、 α, β の置換である。異なる係数値が、 α, β の配置を指定するからである。 $\alpha + \beta \rightarrow \beta + \alpha$ は、 α, β の置換で不変に留まる。

置換すれば、配列は必ず変わるが、根の関数は変化しないこともある。

2. 置換操作の演算規則

1) 置換操作に、文字記号で名前をつけること

n 種の置換を例えば、 $g_1, g_2, \dots, g_n$ などと書く。 g ないし g_k と総称してもよい。

e という文字は、慣習上「置換しない」という記号にだけ使う。

置換 g は、文字の配列変化を通して、根の関数に作用する。

【例】 g が 1, 2 の互換なら、配列 $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \dots$ (数列 $1, 2, 3, 4, \dots$) は、 $\alpha_2, \alpha_1, \alpha_3, \alpha_4, \dots$ (数列 $2, 1, 3, 4, \dots$) になる。

この置換 g で、関数 $3\alpha_1 + \alpha_2$ は、 $3\alpha_2 + \alpha_1$ に変化する。

置換の作用を、掛け算のように書く。下記どちらの書き方でも構わない。

$(3\alpha_1 + \alpha_2)g = (3\alpha_2 + \alpha_1)$ g が右から作用した $\leftarrow g$ のイメージ

$g(3\alpha_1 + \alpha_2) = (3\alpha_2 + \alpha_1)$ g が左から作用した $g \rightarrow$ のイメージ

【注意】 $\theta\theta'\theta''g$ とは、根の関数の積 $\theta\theta'\theta''$ を g で置換することであり、3つの関数 θg 、 $\theta'g$ 、 $\theta''g$ の積になる。置換は式全体を貫いて作用するから、文字 g の掛け算と違う。 $g\theta\theta'\theta''$ は、3つの関数 $g\theta$ 、 $g\theta'$ 、 $g\theta''$ の積であり、 $\theta\theta'\theta''g$ と同義である。

置換記号は、どちらから掛けてもよいが、一方に統一しなければならない。
ひとつの式の中に異なる記法を混在させてはならない。

$\theta g\theta'$ のような記法は定義されていない。 $\leftarrow g \rightarrow$ とイメージしてはいけない。

$g\theta = \theta'$ だとして、 $(\theta + \theta')^2$ を計算するとき、簡略化の積もりで、 $(\theta + g\theta)^2$ と書くのはやめたほうがよい。機械的に展開したら無意味な項 $\theta g\theta$ が出る。 $g\theta g\theta$ を $g^2\theta^2$ と勘違いしても困る (g が互換なら、 g^2 は互換の互換 = e になってしまう)。

$(g\theta_1)(g\theta_2)$ なら意味は通じるが、 $g\theta_1 = \theta'_1$ 、 $g\theta_2 = \theta'_2$ として、 $\theta'_1\theta'_2$ と書くのがよい。

2) 置換の積の規則

作用の積 (掛け算) はいくらでも繰り返せる。 g_1 を作用させ (掛け)、次に g_2 を作用させ、次に g_3 を作用させるなど。

gh もまた置換だが、 $gh\theta$ と書けば、 h を先に作用させ、 θgh と書けば、 g を先に作用させる (近いほうから先に作用させる) ルールである。結果は一般に異なる。

例) 3文字について、 g が α_1, α_2 の互換 (添え字 1, 2 の互換) だとする。

h が α_2, α_3 の互換 (添え字 2, 3 の互換) だとする。

$gh\theta = gh(3\alpha_1 + \alpha_2) = g(3\alpha_1 + \alpha_3) = 3\alpha_2 + \alpha_3$ 添え字置換は $1, 2, 3 \rightarrow 2, 3, 1$

$\theta gh = (3\alpha_1 + \alpha_2)gh = (3\alpha_2 + \alpha_1)h = 3\alpha_3 + \alpha_1$ 添え字置換は $1, 2, 3 \rightarrow 3, 1, 2$

結果は異なるから、置換の積をいうときは、(根の関数に対し) 左右どちらから作用させるか明示する必要が生じる。

置換の積だけ書くとき、 gh とは、 g を先に作用させること、とした成書がある。

作用が $\leftarrow gh$ 、つまり θgh を意味する。本書もこれに従い右からの作用で書く。

可換という用語：もし、 $gh = hg$ であれば、「 g と h は可換である」という。

$\theta hg = \theta gh$ でも、 $hg = gh$ とは限らない。 θ が、 g 、 h で不変な式 (関数) なら、 g 、 h が可換でなくても、 $\theta hg = \theta gh$ になる ($\theta h = \theta g$ でも、 $h = g$ とは限らない)。

置換の積では、結合則すなわち $(g_1 g_2) g_3 = g_1 (g_2 g_3)$ が、成り立つ。

左辺と右辺は、作用する順番が同じだから同じ置換である。

すなわち、置換の掛け算に括弧は不要、単に $g_1 g_2 g_3 \cdots$ などと書けばよい。

【註】上のことを、置換の“集合”に関する下記の話と混同しないよう注意する。

$g_1, g_2, g_3, \cdots$ を含む集合において、積 $g_1 g_2, g_2 g_3$ などを、集合の要素に入れておかない場合、 $(g_1 g_2) g_3, g_1 (g_2 g_3)$ などは定義されないから、「その置換“集合”の中では、結合則が“使えない”」ことになる（結合則を満たさない置換が存在するのではない）。後述、“群の定義”で疑問を感じたなら、この頁に戻ると意味が分かる。

3) 置換の逆置換

置換しない、という置換記号を、 e と書く（前述）。

$g g' = e$ となる g' を、 g の逆置換と呼び g^{-1} と書く ($g g^{-1} = e$)。

g の次に g^{-1} を作用させればもとに戻ることを意味する。

g を g^{-1} に置き換えれば、自明な関係 $(g^{-1})^{-1} = g$ から、 $g^{-1} g = e$ も分かる。

置換の“積”についても、逆置換の定義は同様で、 $(g h)^{-1} g h = e$ である。

$h^{-1} g^{-1} g h = h^{-1} e h = h^{-1} h = e$ と計算できるので、 $(g h)^{-1} = h^{-1} g^{-1}$ が分かる。

すると帰納的に、 $(g_1 g_2 g_3 \cdots g_m)^{-1} = g_m^{-1} \cdots g_2^{-1} g_1^{-1}$

4) 1つの置換の繰り返しからなる置換集合

1つの置換 g を反復した $g, g^2, g^3, \cdots$ の全体を「 g で生成される置換」と呼ぶ。

この集合には e が含まれることが以下のように分かる。

“どんな置換でも、繰り返せばもとの置換に戻る”ことの証明

任意の置換 g から、 $g, g^2, g^3, \cdots$ を次々に作る。置換は有限種類 (n 文字の配列置換は $n!$ 種以下) なので、 $g^a = g^b$ となる自然数 a, b が必ずある ($a > b$ とする)。

$g^b \neq e$ のとき、 $a - b = m$ と書くと、 $g^m g^b = g^a = g^b$ だから、 $g^m = e$ である。

$g^b = e$ の場合は、 $b = m$ と呼ぶことにする。

つまり文字配列に、置換 g を m 回作用させたら、配列は“もとのまま”になる。

すなわち、 g を $(m+1)$ 回掛けると、置換は g に戻る。

g が順送り置換なら、繰り返せば当然もとに戻るが、順送りでなくても戻る！

3. 文字配列を置換する仕方を、具体的に示す表記法

1) ガロアによる置換の表記法

置換操作を（単なる g でなく）、配列の仕方を指定できるように表記しよう。

本書はおもに現代書の一般表記を使うが、ガロアの記法も（原著を引用する都合上）ここに書いておく。

4文字なら自然数列 1, 2, 3, 4 を基準とし、例えば、 $1, 2, 3, 4 \rightarrow 4, 3, 1, 2$ という置換を、置換された結果で示し、**4312** と書く（ガロアは、**dcab** と書いた）。

我々が使う数列は常に、根 $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \dots$ の添え字数列を意味する。

問題 $2, 1, 3 \rightarrow 3, 2, 1$ という置換を **g** とする。**g** をガロアの記法で書け。

答 置換は一対一対応を指定するので、上記は $2 \rightarrow 3, 1 \rightarrow 2, 3 \rightarrow 1$ である。

自然数列を基準にとれば、 $1, 2, 3 \rightarrow 2, 3, 1$ だから、**g = 231**

問題 3文字、4文字配列に対し、置換しない操作 **e** をガロアの記法で書け

答 3文字なら **e = 123**、4文字なら **e = 1234**

問題 3文字の配列置換のすべてを、ガロアの記法で書け

答 123 132 213 231 312 321

問題 置換 **h** ; $2, 3, 1, 4 \rightarrow 1, 2, 4, 3$ の逆置換、**h⁻¹** をガロアの記法で書け

答 矢印を逆にすればよいから、**h⁻¹** は $1, 2, 4, 3 \rightarrow 2, 3, 1, 4$ である。

基準を自然数列にすると $1, 2, 3, 4 \rightarrow 2, 3, 4, 1$ だから、**h⁻¹ = 2341**

問題 前問の **h** を数列 $1, 2, 3, 4$ に繰り返し作用させると、数列はどのように変わっていくか。

答 **h** 「 $2, 3, 1, 4 \rightarrow 1, 2, 4, 3$ 」は、 $1, 2, 3, 4 \rightarrow 4, 1, 2, 3$ と同じだから、
 $1, 2, 3, 4 \rightarrow 4, 1, 2, 3 \rightarrow 3, 4, 1, 2 \rightarrow 2, 3, 4, 1 \rightarrow 1, 2, 3, 4$ もとに戻った。
すなわち、**h = 4123 h² = 3412 h³ = 2341 h⁴ = 1234 = e h⁵ = h** である。

「どんな置換でも繰り返せばもとに戻る」ことは、すでに証明した。

2) 互換、巡回置換の一般的な表記法

以下の置換記号は重要である。（ガロア流でない）**数学書一般の表記法**を示す。

互換 : n文字配列のうちの、2文字だけ入れ替える置換を互換と呼ぶ。

1, 2 の互換は、**(1 2)** と書く。 $(2 1) = (1 2)$ である。

4文字配列の置換 $1, 2, 3, 4 \rightarrow 1, 3, 2, 4$ は、**(2 3)** と書ける。変わる部分だけ表記し、書いてない文字は固定するルールである。

以下で、異なる文字は異なる数としておく。

互換の逆置換（逆元）はそれ自身、 $(a b)^{-1} = (a b)$ である。 $(a b)^2 = e$ も分かる。

$(a b)(a c)$ の逆元は、 $(a c)(a b)$ である。 前述、 $(g h)^{-1} = h^{-1} g^{-1}$ から分かる。

共通文字がなければ可換、 $(a b)(c d) = (c d)(a b)$ だから、 $(a b)(c d)$ の逆置換は、それ自身、 $[(a b)(c d)]^{-1} = (a b)(c d)$ である。

順送り置換 = 巡回置換

巡回置換とは、 n 文字のうちの m ヶを一齐に順送りし、他の文字は変えないことを言う。むろん $m=n$ でもよい。互換は、 $m=2$ の巡回置換である。

すでに“順送り置換”という言葉（分かり易いので定義せずに）使ってきたが、正式用語では、“巡回置換”という。

巡回操作では慣習上、文字を左へ送る（右へ移動すれば逆置換になる）。

3 文字の巡回置換 $1, 2, 3 \rightarrow 2, 3, 1$ は、**(1 2 3)** と書く。ガロアの記法では 231。

5 文字列での置換 $1, 2, 3, 4, 5 \rightarrow 2, 3, 1, 4, 5$ も、3 文字の巡回置換 (1 2 3) である。これはガロアの記法で、23145 になる。

数列 $1, 2, 3, 4, \dots, n$ において、 $2, 4, 5$ を $4, 5, 2$ に変え、他の文字（数字）は固定する置換なら、(2 4 5) と書ける。

慣れれば、自然数列に書き直さなくても、置換を読み取れる。

$5, 4, 3, 2, 1 \rightarrow 5, 4, 2, 1, 3$ は、(3 2 1) である。ガロアの記法では、31245 になる。

(3 2 1) = (2 1 3) = (1 3 2) であり、どの書き方でもよい。

同様に、**(a b c) = (b c a) = (c a b)** であり、この置換は a, b, c 以外の文字を変えない。

$(a b c)^2$ は、2 度の巡回置換「 $a, b, c \rightarrow b, c, a \rightarrow c, a, b$ 」すなわち「 $a, b, c \rightarrow c, a, b$ 」を意味する。各対応 $a \rightarrow c, b \rightarrow a, c \rightarrow b$ を、 $a \rightarrow c, c \rightarrow b, b \rightarrow a$ 、と並べ直し、置き換えの系列を「 $a \rightarrow c \rightarrow b \rightarrow a$ 」と辿れば、 $(a b c)^2 = (a c b)$ と書けることも分かる。

問題 置換 $1, 2, 3, 4, 5 \rightarrow 4, 2, 3, 5, 1$ を巡回置換の記法で書け。

答 変化している文字 $1, 4, 5$ だけ眺めればよいから、(1 4 5) と分かる。

問題 置換 $5, 4, 3, 2, 1 \rightarrow 4, 2, 3, 5, 1$ を巡回置換の記法で書け。

答 (5 4 2) （ガロアの記法なら $1, 2, 3, 4, 5 \rightarrow 1, 5, 3, 2, 4$ より、15324）

5 文字巡回置換を反復したら、数列がどう変わっていくか見てみよう。

$1, 2, 3, 4, 5 \rightarrow 2, 3, 4, 5, 1 \rightarrow 3, 4, 5, 1, 2 \rightarrow 4, 5, 1, 2, 3 \rightarrow 5, 1, 2, 3, 4 \rightarrow$ 戻る
上は基準数列に置換 $(1 2 3 4 5)$ 、 $(1 2 3 4 5)^2$ 、 $(1 2 3 4 5)^3$ 、 $(1 2 3 4 5)^4$ 、 $(1 2 3 4 5)^5 = e$ を作用させた結果である。

$2, 3, 4$ だけの順送りなら； $1, 2, 3, 4, 5 \rightarrow 1, 3, 4, 2, 5 \rightarrow 1, 4, 2, 3, 5 \rightarrow$ もとに戻る。

上は初めの数列に、 $(2 3 4)$ 、 $(2 3 4)^2$ 、 $(2 3 4)^3 = e$ を作用させた結果である。

3) 置換の積の計算

置換の積を練習しよう。

自然数列を基準にして、置換した結果がどうなるかを見る（右からの作用とする）。

互換の積、 $(1\ 2)(1\ 3)$ を、3文字巡回置換に書き直してみよう。

数列を見易いよう「 $\quad$ 」で囲む（ここのローカルルールであり、数学記法でない）。

「**1, 2, 3**」 $(1\ 2) = \text{「}2, 1, 3\text{」}$ さらに $(1\ 3)$ を作用させると、

「1, 2, 3」 $(1\ 2)(1\ 3) = \text{「}2, 1, 3\text{」}(1\ 3) = \text{「}2, 3, 1\text{」}$

「1, 2, 3」が「2, 3, 1」になったから、 **$(1\ 2)(1\ 3) = (1\ 2\ 3)$** である。

問題 $(1\ 3)(1\ 2)$ 、 $(1\ 2)(2\ 3)$ 、 $(2\ 3)(1\ 2)$ を、3文字巡回置換に書き直せ

答 $(1\ 3)(1\ 2) = (1\ 3\ 2)$ 、 $(1\ 2)(2\ 3) = (2\ 1)(2\ 3) = (2\ 1\ 3) = (1\ 3\ 2)$ 、左記2つは同じ

$(2\ 3)(1\ 2) = (2\ 3)(2\ 1) = (2\ 3\ 1) = (1\ 2\ 3)$

問題 $(1\ 2\ 3\ 4\ 5)$ を互換の積に書き直せ

答 次のようにも考えられる。数列1, 2, 3, 4, 5で、数を左に順送りする巡回置換は、1を右隣の数と次々に交換していくことだから、 **$(1\ 2\ 3\ 4\ 5) = (1\ 2)(1\ 3)(1\ 4)(1\ 5)$**
右辺の互換どうしは、それぞれ可換でないことに注意する。

4) 定理： n 文字配列の置換は必ず、互換の積で書き表せる

この重要な定理を証明しよう。

上段の n 文字列を、下段の n 文字列に変える置換を考える。

すなわち $p_1, p_2, \dots, a, \dots, p_n$ を
 $q_1, q_2, \dots, b, \dots, q_n$ に変える置換を、 **g** とする。

上段の“任意文字” a に注目したとする。置換 g によって、 a は b に変わっている。
そこで上段で b を探したら、 b が下段の c に対応していたとする。

$p_1, p_2, \dots, a, \dots, b, \dots, p_n$
 $q_1, q_2, \dots, b, \dots, c, \dots, q_n$

次に、上段で c を探したら、 c が下段の d に対応していたとする。

$p_1, p_2, \dots, c, \dots, a, \dots, b, \dots, p_n$
 $q_1, q_2, \dots, d, \dots, b, \dots, c, \dots, q_n$

次に、上段で d を探したら、 d が下段の a に対応していたとする。

$p_1, p_2, \dots, c, \dots, a, \dots, d, \dots, b, \dots, p_n$
 $q_1, q_2, \dots, d, \dots, b, \dots, a, \dots, c, \dots, q_n$

つまり任意の a から始めて、 $a \rightarrow b \rightarrow c \rightarrow d \rightarrow a$ という、置換を辿る閉じた経

路、謂わば“ループ”が見つかったことになる。文字は n 個つまり有限なのだから、どんな置換の中にも、必ずループが存在すると分かるであろう。

上のループ例で、 $(a b c d) = (a b)(a c)(a d)$ 、巡回置換 = 互換の積、となっている。

注意： $(a b c d) \neq (a b)(b c)(c d)$

置換 g は、 $(a b c d)$ と「 a, b, c, d 以外の文字の置換」の積であり、 $(a b c d)$ は“ a, b, c, d 以外の文字”を変化させないから、これら 2 種の置換は可換である。

「 a, b, c, d 以外の文字置換」の中にもループが存在し、同じ議論を繰り返せるから、

$$g = (a b c d) \times \text{「} a, b, c, d \text{ を含まない文字置換」}$$

$$= (a b c d) \times \text{「} a, b, c, d \text{ を含まない様々な (巡回置換) の積」}$$

$$= (a b)(a c)(a d) \times \text{「} a, b, c, d \text{ を含まない様々な (互換) の積」}$$

したがって、 n 文字配列の置換 g を、互換の積だけで表せることが分かった。

1 つのループは、どの文字から追跡し始めても同じである。

$$(a b c d) = (b c d a) = (b c)(b d)(b a) \quad b \rightarrow c \rightarrow d \rightarrow a \rightarrow b$$

$$= (c d a b) = (c d)(c a)(c b) \quad c \rightarrow d \rightarrow a \rightarrow b \rightarrow c$$

$$= (d a b c) = (d a)(d b)(d c) \quad d \rightarrow a \rightarrow b \rightarrow c \rightarrow d$$

むしろ、4 文字の巡回置換で説明したのは例に過ぎず、何文字でも同様である。

可能な最も長いループは、 a から始まって全文字を経由して a に戻るもの、すなわち「 n 文字の巡回置換」であり、その場合 g は 1 つの n 文字巡回置換である。

最も短いループは、 $a \rightarrow a$ であり、次に短いのは、 $a \rightarrow b \rightarrow a$ すなわち互換 $(a b)$ である。共通文字をもたない互換だけからなる $g = (a b)(c d)(e f) \cdots$ もありうる。

問題 $g = (a b)(b c)(c d)(d a)$ を 1 つの巡回置換に書き直せ

答 基準列を例えば a, b, c, d と書けば、 a, d, b, c に置換されるから、ループ $b \rightarrow d \rightarrow c \rightarrow b$ になり、 $g = (b d c)$

§ 2 群の概念、および方程式の解法理論に群論が使われる必然性

1. 根の或る関数 θ を“変化させない置換”の、“すべて”からなる集合、これが群になる

2 章で、3 次、4 次の方程式を解いたとき、根の関数の“対称性を高める”ことを目標に、“或る置換で変化しない”ような関数を作った。

今は逆に、与えられた根の関数に対し、その関数を変化させない置換を考える。

上のような置換はふつう複数あるから、それらの置換“集合”の性質を考える。

θ を根 $\alpha_1 \sim \alpha_n$ の或る特定の関数とする。

θ を変えない置換が、 $g_1, \cdots, g_m$ (全部で m 個) だとして、それらの集合を $\{g_k\}$ と

書く。 $\{g_k\} = \{g_1, \dots, g_m\}$ である。 $\{ \}$ は集合を表す数学記号である。

g_k は n 文字配列の置換だから、集合 $\{g_k\}$ の要素の個数 m は、 $n!$ 以下である。

要素とは、個々の g_k のことであり、元（ゲン）ともいう。

（元は、群に特有の用語ではなく、どんな集合の要素でも、元と呼んでよい）

1) $\theta g = \theta$ となる置換 g の“すべて”からなる集合、 $\{g_k\}$ を定義する

* $\theta e = \theta$ だから、 e は $\{g_k\}$ の元である（単位元と呼ぶ）。

置換の積の意味から、 $\{g_k\}$ の任意元 g について、 $e g = g e = g$

* $\theta g = \theta$ なら、 $\theta g g^{-1} = \theta g^{-1}$ 、つまり $\theta e = \theta = \theta g^{-1}$ だから、 g^{-1} も $\{g_k\}$ の元

* $\{g_k\}$ の任意の2元を g, g' とすると、 $\theta g g' = \theta g' = \theta$ だから、 $g g'$ も元

2つの元の積が元なら、任意個数の元の積もまた元、と帰納的に分かる。

すなわち、上で定義した集合 $\{g_k\}$ は、単位元と逆元を含み、元の積も元となる。

2) 根の関数 $\theta_1, \theta_2, \dots, \theta_s$ を変化させない置換すべてからなる集合

考え方は 1) と同じである。

「 $\theta_1 g_k = \theta_1, \theta_2 g_k = \theta_2, \dots, \theta_s g_k = \theta_s$ となる置換のすべて、 $g_1, \dots, g_m$ からなる集合」を定義する。

集合 $\{g_k\}$ は、単位元 e を含み、逆元を含み、元と元の積は元になると分かる。

この規則を満たす置換元の集合 $\{g_k\}$ を、置換群と呼ぶ。

演算に関して閉じていること（元どうしの積も元）が、群の本質である。

2. 群の定義と性質

1) 群の一般的な定義

ある集合に、結合則を満たす演算が定義され（任意元を g と書いて）、

単位元 e を含み（ $e g = g e = g$ ）、逆元を含む（ $g g^{-1} = g^{-1} g = e$ ）なら、

この集合を“群”と呼ぶ。

g, g', g'' の演算が結合則を満たすとは、 $g(g' g'') = (g g') g''$ を言う。

$g'' = e$ とすれば、 $g(g') = (g g')$ 。つまり群の定義では、 g と g' の順次作用が、 $g g'$ の作用に等しい。言い換えると、 g と g' が元なら、積 $g g'$ も元である（☞ 33 頁）。

置換集合 $\{e, (12), (13)\}$ は群でない。集合が $(12)(13) = (123)$ を含まないので、 (12) と (13) を順次行なう演算が定義されない（結合則が成り立たない）から群でない。逆元は存在する。 $(12)^{-1} = (12)$ 、 $(13)^{-1} = (13)$ 、 $e^{-1} = e$

或る集合で、「任意元どうしの積もまた元」だとする。 e がこの集合の元なら、任意元 g に対し、 $gg' = e$ となる g' があるから、逆元 $g' = g^{-1}$ も、この集合の元になる。

一方、元 g の逆元 g^{-1} が、この集合の元なら、 $gg^{-1} = e$ も元になる。

すなわち群は、“結合則”の存在、“ e または逆元”の存在、の2項目で定義できる。

根の或る関数を θ とし、「 θ を変化させない置換、すべてからなる集合」は、群になるので、置換群と呼ぶ。群でない置換集合は、方程式の解法に役立たない。

問題： n 文字配列の置換の“すべて”からなる“集合”は、群であるか？

答：置換の置換が、明らかに置換（この集合の要素）だから、結合則が成り立つ。置換しない操作も置換のひとつ、という言葉の定義から、 e が含まれる。ある配列置換 g をもとに戻す配列置換が、 g の逆置換である。したがってこの集合は群である。

2) 群の基本用語：部分群、位数、巡回群、可換群

部分群：ある群の元（要素）の一部からなる集合が、群の定義を満たせば、部分群という。 H が G の部分群であることを、 $H \subset G$ 、または $G \supset H$ と書く。

群それ自身も、部分群のひとつとみなす。あらゆる群が、 $\{e\}$ を部分群として含む。

群の表記法：元をすべて書き並べ、 $G = \{g_1, g_2, g_3, \dots, g_m\}$ と書く（ G は group に因んだ文字だが、どんな文字で呼んでもよい）。 g_k のうちどれかが、 e である。

g が群 G の元であることを、 $g \in G$ と書く。

群の位数：元の個数を、群の“位数”という。上記 G の位数は m である。

元が e のみ、という群 $\{e\}$ の位数は1である。 $ee = e$ 、 $e^{-1} = e$ 。

巡回群：置換 g の積を繰り返し、 $g^m = e$ になったなら（このような m は必ずある：33 頁）、集合 $\{e, g, g^2, \dots, g^{m-1}\}$ は群であり、 g で生成される巡回群という。

注意：巡回置換とは、文字の順送りで書ける一組の文字からなる置換である。

巡回群は、巡回置換と関係なく、任意置換 g で生成されるものである。

可換群：任意2元が可換、 $gg' = g'g$ になる群を、可換群と呼ぶ。

問題 巡回群は、可換群であることを示せ。

答 巡回群は $\{e, g, g^2, g^3, \dots\}$ の形に書ける。

$g^a g^b = g^{a+b} = g^b g^a$ 、したがって任意の元どうしが可換である。

問題 巡回群 $\{e, g, g^2, \dots, g^{m-1}\}$ の元 g^k の、逆元は何か（ $e = g^m$ と書ける）

答 g^{m-k} である。 $1 \leq k \leq m$ 、 $0 \leq m-k \leq m-1$ だから、 g^{m-k} は確かに元である

問題 集合の任意の元 g, h に対し、 $g^{-1}h$ もまた元なら、この集合が群であることを証明せよ。

答 $h = g$ なら、 $g^{-1}g$ も元だから、この集合は $g^{-1}g = e$ を含む。 $h = e$ なら、 $g^{-1}e = g^{-1}$ だから、 g の逆元も含む。すると、 g, h が元なら (g^{-1}, h も元だから)、 $(g^{-1})^{-1}h = gh$ も元になる。したがって、この集合は群である。

3) 操作の内容によって命名された、重要な群

<置換群>

すでに知った、文字配列の置換からなる群であり、我々の主題である。

対称群 S_n : n 文字配列の置換のすべてからなる群を、 n 次対称群と呼び、 S_n と書く。重要な群であり、豊富な内容を含むので、後でその構造を分析する。

S_n の任意元で変化しない文字式 (根の関数) を、対称式 と言う。

n 文字置換群はすべて、 S_n の部分群である。最大の部分群が S_n 自身、最小の部分群が $\{e\}$ である。 S_n の位数は $n!$ 、例えば S_4 の位数は 24 である。

n けた数配列のうち “1, 2, ..., m を任意置換し、 $m+1, m+2, \dots, n$ を固定する置換すべての集合” を考えると、これは群であり、むしろ S_n の部分群である。

S_n はむしろ可換群でない。 S_n の部分群には、可換群が含まれる。

例えば、元が、共通文字を含まない互換どうしの積だけからなるような群は、可換群である。例 : $\{e, (12), (34), (12)(34)\} \subset S_n$ (むしろ、 $\subset S_4$ ともいえる)

S_n の元は、すべて互換の積でも表せることを、前節で証明した。

互換を偶数回かけた元を、偶置換 と呼ぶ。

交代群 : “偶置換のすべて” からなる集合は群である。交代群 (alternating group) と呼び、 A_n と書く。

A_n は、 S_n の重要な部分群である。

偶数 + 偶数 = 偶数なので、元と元の積が元、という群の定義が、集合 A_n で成り立つ。 $(ab)^2 = e$ 、互換の偶数乗 = e 、すなわち A_n は e を含むから、 A_n は群である。

問題 互換を奇数回掛けた元 (奇置換) の集合は、群になるか?

答 e は、この集合の元でない。しかも、奇数 + 奇数 = 偶数だから、どの 2 元どうしの積も元になり得ない。奇置換の集合は群でない。

S_n は、“偶置換すべての集合 A_n ” と “奇置換の集合” を合わせた集合である。群から任意の部分群を取り除いた集合は、 e を含まないから群でない。

<回転群>

図形 (または座標) の回転操作からなる群をいう。我々には必要ないのだが、群に慣れるのに役立つから考えてみる。群の定義を満たす集合は、みな群である。

元は掛け算できるから、 $g g = g^2$ 、 $g h h = g h^2$ のように書いてよいが、 g や h は数でなく“操作”であることを忘れないようにしよう。

図形 $\triangle$ を、“紙面の中で 180° 回転させる操作”を g と呼べば、 g は群の元である。

適当に記法を決め、 $\triangle g = \nabla$ と言ってもよい。 $\nabla g = \triangle$ 、 $g^2 = e$ もいえる。この群は $\{e, g\}$ と書ける。位数は 2 であり、 $g^{-1} = g$ である。

文字列を e 以外で置換すれば、必ず別の文字列になるが、文字式（根の関数）は変化するとは限らないのであった。回転の場合も、 e 以外の回転で、図形配置が変化するとは限らない。例えば 120° 回転で、正三角形 $\triangle$ は不変に留まる。回転角が 0° または 360° の倍数になる操作が e である。操作対象の図形が $\bigcirc$ だったら、どんな回転でも変化しない。回転操作される $\bigcirc$ は、文字置換される対称式と似ている。

<行列を元とする群>

本書に行列の知識は不要だが、行列（をベクトルに掛けること）は、ベクトルを 1 次変換する“操作”である。文字列を n 次元ベクトルとし、配列置換を表す正方行列（ n 行 n 列）も作れる。それら任意の正方行列どうしに積が定義され、行列の集合が群になる。対角成分が 1、他の成分が 0 である行列が、単位元 e の役をする。

3. 群に慣れるための練習問題

問題 正三角形 $\triangle$ を 120° ずつ廻す群を適当な記号で書き、元の計算規則を示せ。

答： 時計回りに 120° 廻す操作を元（ゲン） g と呼ぶ。 $g^3 = e$ 、群は $\{e, g, g^2\}$ 、位数は 3 である。 $g^{-1} = g^2$ 、 $(g^2)^{-1} = g$ も分かる。この計算は、図形で考えただけである（逆回しが逆元、 -120° は 240° と同じ、など）。

反時計回りに 120° 回転させる操作を元としても、むしろ同様に書ける。

数列の巡回置換 $(1\ 2\ 3)$ を g と呼ぶと、 $g^3 = (1\ 2\ 3)^3 = e$ 、集合 $\{e, g, g^2\}$ は巡回群であり、「図形 120° の回転群」と同じ構造である。

問題 $\triangle$ を 60° ずつ回転させる回転群と、前問の群との関係を考察せよ。

答： 60° 回転させる操作を h と呼ぶと、群は $\{e, h, h^2, h^3, h^4, h^5\}$ 、 $h^6 = e$ である。 120° ずつの回転群は、この群の部分群であり、 $\{e, h^2, h^4\} = \{e, g, g^2\}$ となる。

群論では、元どうしの計算規則と位数が同じ群は、同じとみなす。

置換群だけ考えれば、（有限位数の）群一般の知識、定理がみな得られる。

問題 「図形を任意の角度だけ回転させる」という操作すべてからなる集合は、群になるか？

答： 回転角度を x 、 y などと呼ぶと、操作の積は、 $(x \text{ 廻す操作}) \times (y \text{ 廻す操作}) = (x+y) \text{ 廻す操作}$ と定義される。 $x=0$ の回転操作が e である（一回りさせるのも e である）。 x 廻す操作と $-x$ 廻す操作は、互いに逆元である。したがって、この集合は群である。「時計回りに廻す」と決めれば、逆元は“ $360^\circ - x$ 廻す操作”となる。

この群の位数は無限（元が無数）だが、無限位数は群で禁止されていない。

ただし、本書で興味をもつのは置換群だけであり、位数は有限である。

有限個数の文字の並べ方は、明らかに有限種類である。

問題 「図形を 7° 廻す」操作を任意の回数繰り返すこと、これらの操作すべてからなる集合は、群になるか？

答：7 と 360 は互いに素だから、もとの位置に戻れないと錯覚したろうか。 7° ずつ 360 回廻すと図形はもとの位置に戻る。この操作を e と言えるから、この集合は群である。元は 360 ヶあり、「 n 回廻す操作」の逆元は「 $(360-n)$ 回廻す操作」である。

4. ガロア論文で使うことになる、群論の諸定理

置換の性質は、「置換してまた置換するのも置換」、「置換は戻せる」と要約できる。

置換を元とする集合 G において、元と元の積も G の元、元の逆元も G の元であれば、集合 G を群と言う。この規則だけで多彩な定理が生じる。ただし、我々に必要な定理は数少ない上に、証明の殆どは単純である（4 章で導く定理も少しある）。

以下、元の個数（位数）が有限なもの（有限群）だけを考える。

群が部分群をもつことは、群の性質の中で、最も基本的なことである。

* 定理 1 どんな群でも、巡回群を部分群として含む。

証明）一般的に、群 $G = \{e, g, g^2, g^3, \dots\}$ 、位数（元の個数） N 、と書いておく。

元の積も元だから、任意元 g の積、 $g^2, g^3, \dots$ 、もみな G の元だが、元の個数は有限だから、 $g^a = g^b$ ($a > b$) となる a, b がある。 $a - b = m$ と書けば、 $g^m = e$ となる（34 頁参照）。集合 $\{e, g, g^2, \dots, g^{m-1}\}$ を作れば、 g^k の逆元は g^{m-k} である。 $m - k \leq m - 1$ だから、 g^{m-k} は、この集合の元である。つまりこの集合は、巡回群であり、 G の部分群である（位数 m ）。もし $m = N$ なら、 G 自身が巡回群である。

* 定理 2 どんな群でも、位数が素数の部分群をもつ。

証明）任意の群は巡回群 $\{e, g, g^2, \dots, g^{n-1}\}$ を部分群に含む（定理 1）。左記の位数 n が素数なら、証明された。 n が非素数なら、 $n = p m$ (p は素数) とし、 $g^m = h$ と書けば、集合 $\{e, h, h^2, \dots, h^{p-1}\}$ は、上記の巡回群の部分群であり、位数は素数 p である。

* 我々が使う群論で、最も重要なこと：部分群による剰余類分割

どんな群でも、その任意部分群を使って以下のような元の集合に分割できる。

G の任意の部分群を、 H (位数 k) とする。 $G \supset H$

$$H = \{h_1, h_2, \dots, h_k\} = \{e, h_2, \dots, h_k\} \text{ と書く。 } h_1 = e$$

以下は極めて重要なので、話の煩雑さを克服する価値がある。

- H に属さない G の元を、任意に 1 つ選び、 g_1 と呼ぶ。
そして、 $Hg_1 = \{h_1g_1, h_2g_1, \dots, h_kg_1\}$ という集合を作る。
 Hg_1 は、 G の元の集合だが、 e を含まないから群でない (もし $h_jg_1 = e$ なら、 $g_1 = h_j^{-1} \in H$ となって矛盾するから、 e を含まないと分かる)。
- 次に、 H にも Hg_1 にも属さない G の元を、任意に 1 つ選び、 g_2 と呼ぶ。
そして、 $Hg_2 = \{h_1g_2, \dots, h_kg_2\}$ を作る。これも上記と同様、群でない。
- 同様にくり返し、 H にも Hg_1 にも Hg_2 にも $\dots$ Hg_{j-1} にも属さない G の元を g_j と呼び、 $Hg_j = \{h_1g_j, \dots, h_kg_j\}$ のように集合を作っていく。
- 最後に次のことがおきる。 g_{m-1} を選び、 $Hg_{m-1} = \{h_1g_{m-1}, \dots, h_kg_{m-1}\}$ と書くと、今まで作った集合のどれにも含まれない G の元は、もう残っていない。
不思議なことに G の元をぴったり使い切る！ なぜこうなるかを証明しよう。

*** 定理 3** 任意の部分群 H で、 $G = \{H, Hg_1, Hg_2, \dots, Hg_{m-1}\}$ と書けて、
 m ケに分けたどの集合 H, Hg_i, Hg_j も共通元をもたない。
すなわち G が上記の形で過不足なく書き表せる。

「 G を H の剰余類に分割した」という。 割り算の余りによる、整数の分類に似る (証明) 背理法による

H の或る元 h, h' に対し、 $h' = hg_i$ なら、両辺に h^{-1} を掛け、 $h^{-1}h' = g_i$ となる (群の定義から、 $h \in H$ なら $h^{-1} \in H$)。すると、 $g_i = h^{-1}h' \in H$ となって矛盾するから、 H のどの元 h, h' でも、 $h' \neq hg_i$ である。つまり H と Hg_i に共通元はない ($H \neq Hg_i$)。

或る $h, h' \in H$ に対し、 $hg_i = h'g_j$ なら、両辺に h^{-1} を掛けて $g_i = h^{-1}h'g_j$ だから $g_i \in Hg_j$ という矛盾がおき、両辺に h'^{-1} を掛けた、 $h'^{-1}hg_i = g_j$ からは、 $g_j \in Hg_i$ という矛盾がおきる。どんな h, h' でも、 $hg_i = h'g_j$ は矛盾を招くから、 $hg_i \neq h'g_j$ 、つまり (g_i, g_j を選んだ順序に関係なく) Hg_i と Hg_j に共通元はない ($Hg_i \neq Hg_j$)。

さて、 $H, Hg_1, Hg_2, \dots, Hg_s$ のいずれにも属さない G の元が、 k ケ以下残ったとする (H の元の個数を k ケとしている)。すると、その任意の 1 つ g で、またしても k ケの元、 $h_1g, h_2g, \dots, h_kg$ が作れるが、これら $\in Hg$ ($\subset G$) は、上で証明したように、 $H, Hg_1, Hg_2, \dots, Hg_s$ いずれの元でもない。

すると、元を剰余類に割り振るとき必然的に、残り = k ケの段階があり、 k ケのうちどれを g, g' と呼んでも、 $\{h_1g, \dots, h_kg\} = Hg$ と $\{h_1g', \dots, h_kg'\} = Hg'$ が一致し (疑問なら、次の設問を参照)、残り = 0 ケとなるほかない。定理が証明された。

群 G の位数と、その任意部分群 H の位数の間には、強い制約があると分かった。

問題 $H (\subset G)$ の 2 元 h', h に対し、 $h'g_a = hg_b$ となる $g_a, g_b (\in G)$ は必ずある (元 $h^{-1}h'g_a$ を、 g_b と呼べる)。このとき、 $Hg_a = Hg_b$ を証明せよ
答 $h'g_a = hg_b$ を、 $g_a = h'^{-1}hg_b$ と書き、両辺に、 H の任意元 h'' を掛けると、 $h''g_a = h''h'^{-1}hg_b \in Hg_b$ となる。 h'' は任意だから、 $Hg_a \subset Hg_b$ と分かる。
 $g_b = h^{-1}h'g_a$ と書けば同様に、 $Hg_b \subset Hg_a$ も言えるから、 $Hg_a = Hg_b$

剰余類分割、 $G = \{H, Hg_1, Hg_2, \dots, Hg_{m-1}\} \cdots \star$ は、 $g_1 \sim g_{m-1}$ 以外の元で
 $G = \{H, Hg'_1, Hg'_2, \dots, Hg'_{m-1}\} \cdots \star$ とも書ける ($g'_1 \sim g'_{m-1} \in G, \notin H$)。
上の設問から、 $\star$ の Hg_a に属する 1 つの元が、 $\star$ での Hg'_b の元なら、 $Hg_a = Hg'_b$ (同じ剰余類) と分かる。定理 3 (剰余類どうしの排他性) と合わせれば、 $\star, \star$ の $\{ \}$ 内は一致する $\rightarrow$ 剰余類 (分割の仕方) は H を決めれば一意的、と分かる。

算術用語で剰余類とは、整数 n を、整数 m で割った余り「 $0, 1, 2, \dots, m-1$ 」で m 種に分類したものである。群を剰余類に分割することも、これと類似性がある。

* 定理 4 G の位数が N 、部分群 H の位数が k なら、 k は N の約数である

“任意部分群の位数が、 N を割り切る”ことは、群の定義だけでは想像できないが、定理 3、 $G = \{H, Hg_1, \dots, Hg_{m-1}\}$ と書けるのを知ったから、 $N = km$ (ラグランジュの定理) は明らかである。ガロア以前のラグランジュの時代にも、群の概念はあったが、体系化されていなかった。

n 文字置換のすべてからなる群 S_n (対称群) の位数は $n!$ だから、 S_n の位数が任意部分群の位数の倍数になることは、剰余類分割のことを知らなくても分かるが、次節で S_n の構造を分析するとき、剰余類分割の考え方は必須になる。

* 定理 5 位数が素数の群は、巡回群である。

証明) この定理はコーシーが見出した、とガロアが引用している。定理 2 から、任意の群 G は、素数位数 (p としよう) の巡回群を部分群として含む。すると、 G の位数が素数 p' なら、定理 4 から、 p が p' の約数でなければならない。したがって $p' = p$ にならざるを得ない。すなわち G 自身が、位数 p の巡回群である。

§ 3 n 次対称群 S_n の構造、および方程式の解公式との関係

1. S_n の元の表記法

我々が扱う群は、 n 文字配列の置換群であり、そのすべてが S_n の部分群である。

1) ガロアの記法 (34 頁参照)

S_n の定義 (n 文字の配列置換のすべて) は、元をガロアの記法で書くと明瞭である。

2 文字の対称群 $S_2 = \{12, 21\}$ $12 = e$ が単位元

3 文字の対称群 $S_3 = \{123, 132, 213, 231, 312, 321\}$ $123 = e$

4 文字の対称群 $S_4 = \{1234, 1243, 1324, \dots\}$ $1234 = e$

2) S_n の構造を分析するときは、互換または巡回置換で書くのが適する

S_n の元すべてが、互換の積または巡回置換の積で書けることは証明した (36 頁)。そのような書き方は、 S_n に含まれる部分群の構造を調べるのに大いに役立つ。

S_2 の構造をみよう。ガロアの記法では、 $S_2 = \{12, 21\} = \{e, 21\}$ 互換の記法で書けば、 $S_2 = \{e, (1\ 2)\}$ $(1\ 2)^2 = e$ 、 $(1\ 2)^{-1} = (1\ 2)$ S_2 の構造がすべて分かった。

2. S_3 の構造と 3 次方程式の解法の関係

1) S_3 の元を、互換または順送り置換で表すこと

$S_3 = \{123, 132, 213, 231, 312, 321\}$ の構造は、一気に内容が豊富になる。

3 次方程式の解法に群論を応用するとき、 S_3 の構造分析が必要になる。

$123 = e$ 、 $132 = (2\ 3)$ 、 $213 = (1\ 2)$ 、 $321 = (1\ 3)$ 、 $231 = (1\ 2\ 3)$ 、 $312 = (1\ 2\ 3)^2$

と書き直して分析する。

$S_3 = \{e, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 2\ 3)^2\}$ と書ける

積の例 ; $(1\ 2)(1\ 3) = (1\ 2\ 3)$ 、 $(1\ 2)(2\ 3) = (1\ 2\ 3)^2$ 、など

問題 S_3 の部分群をすべて書け

答 : S_3 自身、 $\{e, (1\ 2\ 3), (1\ 2\ 3)^2\}$ 、 $\{e, (1\ 2)\}$ 、 $\{e, (1\ 3)\}$ 、 $\{e, (2\ 3)\}$ 、 $\{e\}$

問題 S_3 を、部分群 $H = \{e, (1\ 2\ 3), (1\ 2\ 3)^2\}$ で剰余類分割せよ。

答 : $S_3 = \{H, H(1\ 2)\} = \{H, H(1\ 3)\} = \{H, H(2\ 3)\}$

2) 交代群 A_3

互換を偶数回掛けた元 (偶置換) のすべてからなる交代群の概念は、すでに述べた。

復習として、 S_3 の部分群 A_3 の構造を調べよう。

$S_3 = \{e, (1\ 2), (1\ 3), (2\ 3), (1\ 2)(1\ 3), (1\ 3)(1\ 2)\}$ と書ける。

e は、(任意の互換)² だから、偶置換は e 、 $(1\ 2)(1\ 3)$ 、 $(1\ 3)(1\ 2)$ である。

すなわち、 $A_3 = \{e, (1\ 2)(1\ 3), (1\ 3)(1\ 2)\}$ 集合 A_3 は、群である。なぜなら、

$(1\ 2)(1\ 3)(1\ 2)(1\ 3) = (1\ 3)(1\ 2)$ のように、元と元の積が元になっている。

$(1\ 2)^{-1} = (1\ 2)$ 、 $[(1\ 2)(1\ 3)]^{-1} = (1\ 3)(1\ 2)$ のように、逆元が含まれている。

問題 S_3 を交代群 A_3 で、剰余類分割せよ。

答: $S_3 = \{e, (1\ 2), (1\ 3), (2\ 3), (1\ 2)(1\ 3), (1\ 3)(1\ 2)\}$
 $= \{A_3, A_3(1\ 2)\} = \{A_3, A_3(1\ 3)\} = \{A_3, A_3(2\ 3)\}$ と分かる

巡回群 $H = \{e, (1\ 2\ 3), (1\ 2\ 3)^2\} = \{e, (1\ 2)(1\ 3), (1\ 3)(1\ 2)\} = A_3$ だから、 S_3 の部分群のうち、 $A_3 = H$ 、すなわち、3 次の交代群は巡回群である。

以上で、 S_3 の構造が殆ど分かった。

一般的な、 n 次対称群 S_n と A_n の関係もみよう。

問題 S_n を交代群 A_n で、剰余類分割せよ。

答: $S_n = \{\{A_n, A_n(1\ 2)\} = \{A_n, A_n(i\ j)\} \quad (i\ j) \text{ は任意の互換}\}$
 $= \{A_n, A_n g\} \quad g \text{ は任意の奇置換、とも言える}$
剰余類分割の仕方は一意的だが、書き方は色々あることを前述した (44 頁)。

$A_n(1\ 2)$ は、奇置換すべての集合だから、偶置換の個数 = 奇置換の個数 となる。

S_2 では、偶置換の元は e だけであり $A_2 = \{e\}$ 、奇置換も $(1\ 2)$ だけである。

下記の説明でも、 S_n が含む偶置換の個数 = 奇置換の個数、と分かる。

- ・「或る 4 文字数列」を基準にとり、「2, 1, 3, 4」に変える置換を h と呼んだとする。
基準数列が「1, 2, 3, 4」だったのなら、 $h = (1\ 2)$ 、すなわち奇置換であるが、
基準数列が「1, 2, 4, 3」だったなら、 $h = (1\ 2)(3\ 4)$ 、すなわち偶置換である。

3) 3 次方程式の解法の群論的意味

2 章の解法で使った“根の関数の置換対称性”を、群論の言葉に翻訳しよう。

I) 根 α, β, γ のすべてを不変に保つ S_3 の元 (置換) は e のみ
すなわち各根は、 $\{e\}$ に関して対称

II) 根 α, β, γ を、 $\alpha_1, \alpha_2, \alpha_3$ として、群の元を添え字 1, 2, 3 で書き表す。

3 根の巡回置換、 $H = \{e, (1\ 2\ 3), (1\ 2\ 3)^2\}$ で不変な関数 θ^3 を作った (H 対称性)
 $\theta^3 = (\alpha + \omega\beta + \omega^2\gamma)^3$ が含む非対称関数は、 $\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha = \varphi$ 、 $\alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2 = \varphi'$
 $H = \{e, (1\ 2)(1\ 3), (1\ 3)(1\ 2)\} = A_3$ でもあるから、 φ, φ' は、 A_3 対称性

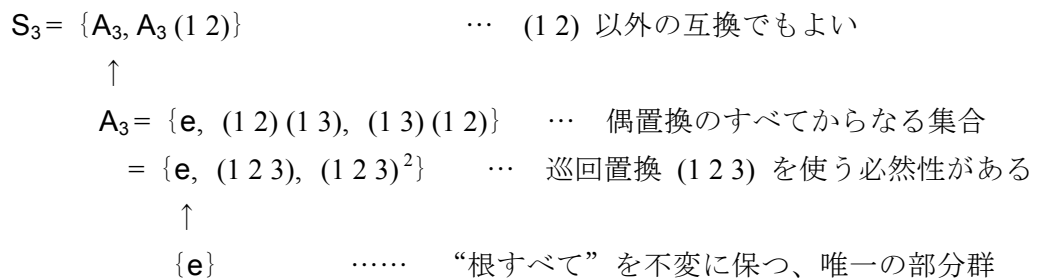
III) $S_3 = \{A_3, A_3(1\ 2)\}$

$\varphi(1\ 2) = \varphi'$ 、 $\varphi'(1\ 2) = \varphi$ 、したがって、

$\varphi + \varphi'$ 、 $\varphi\varphi'$ は、 A_3 で不変かつ、 $A_3(1\ 2)$ で不変、つまり S_3 対称性に達した

前の段階の関数を、次の段階の関数で表す計算法（26 頁の手法）が、 S_3 対称関数に至るまで存在するから、3 次方程式が解けた。

以上の解法は、下記の図を下から上へ登ることである。図は、計算法が実現した経路を示すものであり、計算法を教えるものではない。

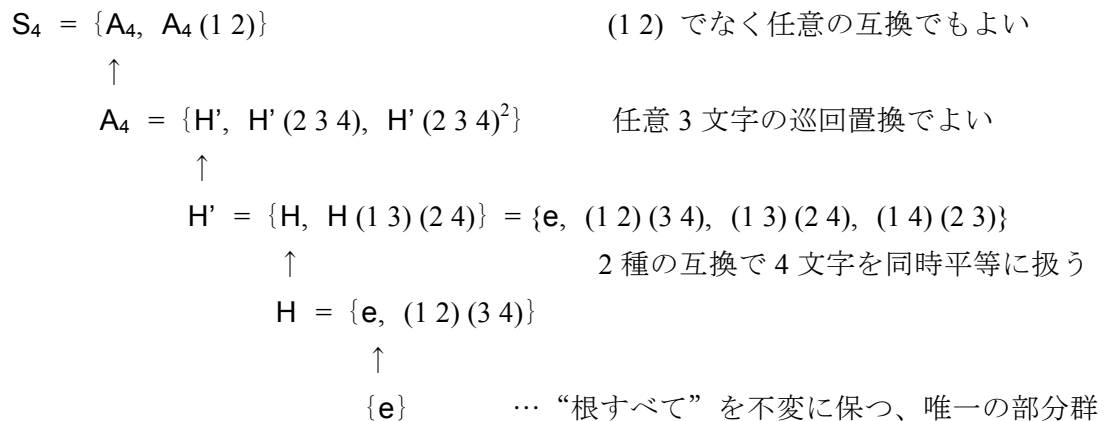


3. S_4 の構造と 4 次方程式の解法の関係

S_4 は、 S_3 よりも遙かに複雑である。

S_4 の構造のうち、4 次方程式の解法と関連する剰余類分割の仕方を記す。

下記の図を、下から上へと眺めよう（28 頁～、参照）。



H から始めて、上段に代入していけば、 S_4 が過不足なく書き尽くされる。

H' も H も、 A_4 の部分群だから、元はすべて偶置換の筈で、実際そうになっている。

$H' = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 2)(3\ 4)(1\ 3)(2\ 4)\} = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$

l) 「 $\alpha_1 + \alpha_2$ 、 $\alpha_1\alpha_2$ 」は、 H 対称性、「 $\alpha_3 + \alpha_4$ 、 $\alpha_3\alpha_4$ 」も、 H 対称性

II) $\{(\alpha_1 + \alpha_2) - (\alpha_3 + \alpha_4)\}^2, (\alpha_1\alpha_2 - \alpha_3\alpha_4)^2$ は、ともに H' 対称性 (むしろ H 対称性)
この式の中に、対称式、および H' 対称式 $\alpha_1\alpha_2 + \alpha_3\alpha_4$ が現れた。
一般に、 $H' \supset H$ のとき、 H' 対称式は、当然 H 対称式である。

III) $\alpha_1\alpha_2 + \alpha_3\alpha_4$ を 3 文字巡回置換して作る方法で、 **A_4 対称式**が 2 つ現れた

$$\Theta^3 = [(\alpha_1\alpha_2 + \alpha_3\alpha_4) + \omega(\alpha_1\alpha_3 + \alpha_4\alpha_2) + \omega^2(\alpha_1\alpha_4 + \alpha_2\alpha_3)]^3 \quad (\omega^3 = 1)$$

$$\Theta'^3 = [(\alpha_1\alpha_2 + \alpha_3\alpha_4) + \omega^2(\alpha_1\alpha_3 + \alpha_4\alpha_2) + \omega(\alpha_1\alpha_4 + \alpha_2\alpha_3)]^3$$

IV) $\Theta^3 + \Theta'^3, \Theta^3\Theta'^3$ という **S_4 対称式** (基本対称式で表せる関数) が得られた。

4. S_5 の構造

S_5 の構造は神秘である (その意味を 5 章 133 頁に記した。興味あれば見て欲しい)。
剰余類分割の仕方を、試行錯誤でみつけようとしたら、複雑すぎて途方に暮れる。

5 次方程式の一般解法も、下記の図を下から上へ登ることになる。各根の対称性を高める出発点の形は、素数次である 3 次方程式と同様に全根を含む巡回群である。

$$S_5 = \{A_5, A_5(1\ 2)\} = \{A_5, A_5(\text{任意互換})\}$$

↓

$$A_5 = \{\text{どんな部分群で剰余類分割されるか?}\}$$

径路は上から↓も

.....

下から↑も繋がらない

$$\text{どんな群} = \{H' \text{ による剰余類分割}\} ?$$

これが解公式のない

↑

理由 (4 章) となる

$$H' = \{H \text{ による剰余類分割}\}$$

↑

$$H = \{e, (12345), (12345)^2, (12345)^3, (12345)^4\}$$

この形で解くべき

↑

必然性は後述する

$$\{e\} \quad \cdots \quad \text{常に出发点となる部分群}$$

§ 4 文字の添え字の算術による、置換の表記法

以下の表記法を知することは、ガロア論文の理解に必須である。

1. 整数の剰余類、根の添え字の表記法

群を剰余類分割する、という用語は、下記のような整数の剰余類分類との見かけの類似性によるのであった。

任意の整数は、或る整数 n で割った余り (剰余) で、 n 種類「 $0, 1, 2, \dots, n-1$ 」に分類できる。この数集合を、「 n を法とする剰余類」または「**modulo n の剰余類**」

と呼び、 $\text{mod } n$ と書く。同じ剰余類に属する数どうしを合同と呼び、 $\equiv$ で結ぶ。

例) $\text{mod } 3$ で、 $3m \equiv 0$ 、 $7 \equiv 1$ 、 $8 \equiv 2$ 、 $1+2 \equiv 0$ 、 $2 \times 2 \equiv 1$ 、

$\text{mod } n$ で、 $a \equiv b$ なら $a-b \equiv 0$

文字置換を、文字を書き並べずに“添え字の算術”で表現できる場合もある。

α_1 が α_3 に置換されたら、添え字 1 が 3 になった、 $1 \rightarrow 3$ といえる。

α_k が α_{k+2} になる置換は、添え字表記で、 $k \rightarrow k+2$ と書ける。

α_k が α_{3k} になるなら、 $k \rightarrow 3k$ と書ける。

n 個の文字の添え字は n を越えないから、添え字の算術を、 $n \rightarrow n+2$ 、 $n \rightarrow 3n$ とは書けない。 $n+2 \equiv 2$ 、 $3n \equiv 0 \pmod{n}$ など、整数の剰余類で書けば首尾一貫する。

このとき n 根は、 $\alpha_1, \dots, \alpha_{n-1}, \alpha_n$ でなく、 $\alpha_1, \dots, \alpha_{n-1}, \alpha_0$ と命名する。置換は、数列に属する数の一対一対応で決まるので、基準数列の並べ方は任意である。

2. 添え字の計算式で、一括表現できる置換について

n 根の配列 $\alpha_0, \alpha_1, \dots, \alpha_{n-1}$ に対する巡回置換（順送り置換）を g とすれば、 $g = (0\ 1\ 2\ \dots\ n-1)$ と書ける。

g から生成される巡回群、 $\{e, g, g^2, \dots, g^{n-1}\}$ を考える。

g の反復で、添え字配列は、 $0, 1, 2, \dots, n-1 \rightarrow 1, 2, 3, \dots, 0 \rightarrow 2, 3, 4, \dots, 1 \rightarrow \dots$ と変化するから、 g は、 $k \rightarrow k+1$ と表現できる。 $n \equiv 0$ 、 $n+1 \equiv 1 \pmod{n}$

g^m は、 $k \rightarrow k+m$ と表現できる。添え字 $1, 2, 3, \dots$ は、 $1+m, 2+m, 3+m, \dots$ 、根配列 $\alpha_0, \alpha_1, \dots$ は、 $\alpha_m, \alpha_{1+m}, \alpha_{2+m}, \dots$ になる。

$g^n = e$ は、 $k \rightarrow k$ と書ける ($k+n \equiv k$)。

置換元を、 $k \rightarrow f_m(k) = k+m$ 、巡回群を、 $\{f_0(k), f_1(k), \dots, f_{n-1}(k)\}$ と書ける。

g は、すべての根を、 $f_m(k)$ という共通規則で置換する（置換規則は m の値に応じて n 種類ある）。置換 g をくり返すと、任意根が、他のすべての根に移り変わる。

【補足】例えば、 $\alpha_0, \alpha_1, \dots, \alpha_{n-1}$ の左右反転、 $\alpha_{n-1}, \alpha_{n-2}, \dots, \alpha_0$ の置換でも、“全根が一斉に置換”される。添え字 $k \rightarrow j$ は、 $0 \rightarrow n-1$ 、 $1 \rightarrow n-2$ 、 $2 \rightarrow n-3$ 、 $\dots$ と対応するから、 $k+j = n-1$ （定数）に従う。 j を $f(k) = -k + (n-1)$ と書けるから、全根が“同じ規則”で置換される。しかし、どの根も全根には移り変わらないから、我々には利用価値がない。この元が生成する置換群は、 $\{e, f(k)\}$ である。 $\{f(k)\}^{-1} = f(k)$

方程式論に必要な、もう 1 つの **n 根一斉置換**がある。その方法を表記するには、“剰余類の原始根”という、“方程式の原始根”とは別の概念が必要になる。

3. mod n の原始根 (剰余類の原始根)

整数 n の剰余類、 $0, 1, 2, \dots, n-1 \pmod{n}$ を考える。つまり任意整数を、 n で割った“余り”をすべて考える。 n の剰余類の 1 つを a と呼ぶとき、 a^m で、 n の剰余類の値 $1, 2, \dots, n-1$ をすべて表せるなら (0 は表せない)、 a を n の剰余類の原始根、または $\text{mod } n$ の原始根という。

$\text{mod } 5$ で、 2^m の値は、 $2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8 \equiv 3$ 、となり、 $1 \sim 4$ のすべての数が表せる (m が増せば、 $2^4 \equiv 1, 2^5 = 32 \equiv 2, \dots$ と値が繰り返される)。

したがって、**2 は mod 5 の原始根**である。(3 も、 $\text{mod } 5$ の原始根である)

$\text{mod } n$ の原始根は、 n が素数なら存在する。

n より大きい数 b を、 $b = qn + a$ (a は n の剰余類) と書くと、 $b^m = (qn + a)^m \equiv a^m \pmod{n}$ となるから、 $\text{mod } n$ の原始根は、存在するなら a のうちのどれか (つまり n の剰余類) の中にみつかることが分かる。

4. 全根を共通規則で置換するが、1 根だけ動かず、他すべてが移り変わる 巡回置換

方程式 $x^n - 1 = 0$ の n 根について、実根 1 を除く、虚根のすべて ($n-1$) ケが相互に移り変わるような、置換の表記を工夫しよう。

つまり、 $(x^n - 1)/(x - 1) = x^{n-1} + \dots + x + 1 = 0$ の根を、共通規則で巡回置換したい。 $(n-1)$ ケの根を、原始根 ω を使って $\alpha_k = \omega^k$ と書き ($k = 1 \sim n-1$)、 $\alpha_0 = 1$ とする (添え字 0 が仲間はずれになるのが、この算術の本質である)。

mod n の原始根 a を利用すれば、置換規則を下記のように表現できる。

g' を、置換 $k \rightarrow a^m k \pmod{n}$ と定義する。 **g'^m** は、 $k \rightarrow a^m k$ である。

ただし、 **n は素数に限る** (素数でないと、 a が得られない)。

g' の作用を、根の添え字数列で書けば、 $1, 2, 3, \dots \rightarrow a, 2a, 3a, \dots$ となる。

(根配列を書けば $\alpha_1, \alpha_2, \alpha_3, \dots \rightarrow \alpha_a, \alpha_{2a}, \alpha_{3a}, \alpha_{4a}, \dots$)

g^m が作用すると、添え字数列は、 $1, 2, 3, \dots \rightarrow a^m, 2a^m, 3a^m, \dots$ となる。

素数 $n = 5$ の場合を考える。 $a = 2, g'; k \rightarrow 2k \pmod{5}$ の作用をみる。

4 つの根、 $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ の添え字 1, 2, 3, 4 は、

g' で、 $a, 2a, 3a, 4a = 2, 4, 6, 8 \equiv \underline{2, 4, 1, 3} \pmod{5}$ 同様に、

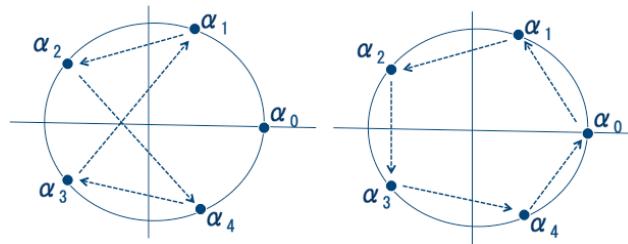
g'^2 で、 $a^2, 2a^2, 3a^2, 4a^2 = 4, 8, 12, 16 \equiv \underline{4, 3, 2, 1}$

g'^3 で、 $a^3, 2a^3, 3a^3, 4a^3 = 8, 16, 24, 32 \equiv \underline{3, 1, 4, 2}$ となり、

g'^4 で、 $a^4, 2a^4, 3a^4, 4a^4 = 16, 32, 48, 64 \equiv 1, 2, 3, 4$ もとに戻る **$g'^4 = e$**

(下線は数学記号ではなく、見易くするためにつけた)

実際は5文字列の置換を扱っているのだから、0を略さずに上の置換を書けば、
 $0, 1, 2, 3, 4 \rightarrow 0, 2, 4, 1, 3 \rightarrow 0, 4, 3, 2, 1 \rightarrow 0, 3, 1, 4, 2$ 。数の対応を保って並び順を書き直した、 $0, 1, 2, 4, 3 \rightarrow 0, 2, 4, 3, 1 \rightarrow 0, 4, 3, 1, 2 \rightarrow 0, 3, 1, 2, 4 \rightarrow$ 初めの数列を見れば、0以外の4文字(4根)が“巡回置換”されているのが分かり易い(図左)。
 “巡回置換”の添え字表記は、 $k \rightarrow k + m$ (図右) だけではなかった。



1 の n (素数) 乗根の配列は、巡回群 $\{e, g', g'^2, \dots, g'^{n-2}\}, g'^m; k \rightarrow a^m k \pmod{n}$ で置換される。 $m = 0, 1, 2, \dots, n-2$ で、 $(n-1)$ への置換元が指定される。
 どの g'^m も $k=0$ に対して、“変化させない”という作用をする。

問題 $a=3$ は、 $\text{mod } 5$ の原始根であることを示せ

答 $3^0=1, 3^1=3, 3^2=9 \equiv 4, 3^3=27 \equiv 2$ 、すなわち $1 \sim 4$ の値すべてをとれる。

$g'; k \rightarrow 3k \pmod{5}$ とすると、 g', g'^2, g'^3 の作用で、添え字数列 $1, 2, 3, 4$ は、
 g' で $3, 6, 9, 12 \equiv 3, 1, 4, 2$ g'^2 で $9, 18, 27, 36 \equiv 4, 3, 2, 1$ g'^3 で $27, 54, 81, 108 \equiv 2, 4, 1, 3$ g'^4 で $81, 162, 243, 324 \equiv 1, 2, 3, 4$ $g'^4=e$ になる

問題 $a=4$ は、 $\text{mod } 5$ の原始根か？

答 $4^0=1, 4^1=4, 4^2=16 \equiv 1, 4^3=64 \equiv 4$ 、すなわち5の剰余類のうちの、2と3を表せないから、4は原始根でない。

問題 $\text{mod } 3$ の原始根を使って、「数列 $1, 2$ 」の2文字巡回群を表せ

答: $\text{mod } 3$ の原始根2を使って、 $g'; k \rightarrow 2k$ とすればよい。

数列は、 g' で、 $1, 2 \rightarrow 2, 4 \equiv 2, 1$ g'^2 で、 $1, 2 \rightarrow 4, 8 \equiv 1, 2$ 、 $g'^2=e$ になる。

問題 $\text{mod } 4$ の原始根は存在しない ($g'; k \rightarrow ak$ から生成される巡回群は存在しない) ことを示せ。

答 e, g', g'^2 の作用で、0以外の剰余がなす数列「 $1, 2, 3$ 」の、変化の様子をみる。

$g'; a=2, k \rightarrow 2k \pmod{4}$ とすると、数列 $1, 2, 3$ は

g' で、 $2, 4, 6 \equiv 2, 0, 2$ だから、文字置換にならない

$g'; a=3, k \rightarrow 3k \pmod{4}$ とすると、数列 $1, 2, 3$ は

g' で、 $3, 6, 9 \equiv 3, 2, 1$ g'^2 で、 $9, 18, 27 \equiv 1, 2, 3$ とともに戻ってしまい、

$g^3 = e$ にならない。

$a < 4$ だから、 $\text{mod } 4$ の原始根は存在しない（原始根の定義で述べたように、 $a \geq 4$ を選んでも、上記と同じ結果が繰り返されるだけである）。

以上で、本書の群論はほぼ終了である。4 章で、正規部分群、剰余類群（商群）の概念を理解して頂上に達する（それらは現代語だが、ガロア原著と自然につながる）。

挙げた定理は最小限だが、2 章+3 章で、方程式の解法に群を使う理由を知ったから 初歩でなく本質をマスターした。群の意義は、対称性を分類できることにある。

第 4 章 ガロア論文

この章の意外で偉大な結論を導く手法は、ユークリッドの互除法である。

本章すべてで、重根がない方程式だけを扱う。我々が興味をもつのは既約方程式の解法であり、既約方程式は重根をもたないから（16 頁）、既約方程式を扱う と言ってもよいのだが、以下の手法は重根のない可約方程式にも適用できる。

§ 1 n 次方程式の根の 1 次式 $V = A_1 \alpha_1 + A_2 \alpha_2 + \cdots + A_n \alpha_n$ を使うと、
各根が、 V の整式で $\alpha_k = \varphi_k(V)$ と表せる

1. 根の 1 次関数 $V = A_1 \alpha_1 + \cdots + A_n \alpha_n$ という概念

$f_n(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0 = 0$ の n 根が、みな異なるとする（イメージを簡明にするために“既約方程式”だと思って読んでも全くかまわない）。

根 $\alpha_1 \sim \alpha_n$ のすべてからなる、ガロアの発案による 1 次式 V を考えよう。

$V_1 = A_1 \alpha_1 + A_2 \alpha_2 + \cdots + A_n \alpha_n$ と書く（添え字を自然数列で並べた V を V_1 と呼んだ）

そして、 $\alpha_1 \sim \alpha_n$ の配列を適当に置換した式を、例えば V_k と書こう（ V_k を V の総称とすれば、 V_1 は V_k の 1 つである。異なる配列の V を V_j, V' などとも書く）。

$A_1 \sim A_n$ の決め方：根 $\alpha_1 \sim \alpha_n$ の配列を置換したら、必ず V_k の値が変わるよう
に決める（根の配置は $n!$ とおりあるが、 $A_1 \sim A_n$ の決め方は無数だから、 V_k の値が必ず
変わるようにできる。 V_k を変化させない置換は e のみである）。

・ $A_1 \sim A_n$ は、有理数と決める（方程式の係数を有理数とする取り決めとまったく同じ趣旨であり、無理数を含めたら叙述が煩雑になるだけで利点がない）。

・ V_k は、各根 $\alpha_1 \sim \alpha_n$ を書き表すために発明された。

さらに、根を置換した V_k どうしを掛け合わせ、解法に必要な“非対称な根の関数”のすべてを作り出す役目を演じさせる予定である。

< V_k における根の配列置換について：本書で使用する記法の説明 >

例えば、3 次方程式の 3 根から、 $V_1 = A_1 \alpha_1 + A_2 \alpha_2 + A_3 \alpha_3$ を作る。

V_1 の根配列を置換した、 $3! = 6$ とおりをすべて書けば、 $A_1 \alpha_1 + A_2 \alpha_3 + A_3 \alpha_2$ 、 $A_1 \alpha_2 + A_2 \alpha_1 + A_3 \alpha_3$ 、 $A_1 \alpha_2 + A_2 \alpha_3 + A_3 \alpha_1$ 、 $A_1 \alpha_3 + A_2 \alpha_1 + A_3 \alpha_2$ 、 $A_1 \alpha_3 + A_2 \alpha_2 + A_3 \alpha_1$ となる。これらを総称した V_k を表す記法は、下記のように色々あるだろう。

$$V_k = A_1 \alpha_a + A_2 \alpha_b + A_3 \alpha_c \quad a, b, c \text{ は互いに異なり、} 1, 2, 3 \text{ のいずれか}$$

$$V_k = A_1 () + A_2 () + A_3 (), \quad \text{括弧に } \alpha_1, \alpha_2, \alpha_3 \text{ を配置する}$$

$$V_k = A_1 \square + A_2 \square + A_3 \square, \quad \square \text{ に } \alpha_1, \alpha_2, \alpha_3 \text{ を配置する}$$

少なくとも、 Σ を使って書こうとすると煩雑になる

本書では、 $V_k = A_1 \square + A_2 \square + A_3 \square$ と記すことにした。物理に親しい人は、 $\square$ から演算子 (ダランベリアン) を連想するなど、違和感をもつかもしいが、我々は終始一貫 “**n 根の配列置換**” だけを扱うので、 $\square$ の意味は簡明で、煩雑な添え字を減らすのに役立つと思う。

$$V - (A_1 \square + A_2 \square + A_3 \square) \text{ の可能な根配列 } 3! \text{ ケを掛けたものを}$$

$$\Pi_k (V - V_k) = \Pi_{\alpha, \beta, \gamma} \{V - (A_1 \square + A_2 \square + A_3 \square)\}$$

$$= \Pi_{S_3} \{V - (A_1 \square + A_2 \square + A_3 \square)\} \text{ のようにも書ける}$$

$V_k = A_1 \square + \cdots + A_n \square$ を解にもつ方程式、 $F(V) = 0$ を考える。

$F(V)$ の係数が、既知数になるようにしたい。

既知数とは；与えられた方程式 $f(x) = 0$ の係数と、自分で決めた $A_1 \sim A_n$ である。

未知数とは、求めたい、根の非対称関数 (究極の非対称関数は、各根) である。

未知数を、既知数から計算することが、今から考える方法論である。

$\square$ に n 根 $\alpha_1 \sim \alpha_n$ を配置し、すべての可能な配列を掛け合わせた $n!$ 次方程式

$$F(V) = \Pi_{S_n} \{V - (A_1 \square + A_2 \square + \cdots + A_n \square)\} = 0 \text{ を作れば、}$$

$F(V)$ の展開係数が既知数になる。その理由を考えよう。

$$V_1 = A_1 \alpha_1 + \cdots + A_n \alpha_n, \text{ または総称的な } V_k \text{ は、むしろ } F(V) = 0 \text{ の解である。}$$

問題 2 次方程式 $x^2 + ax + b = 0$ の根、 α, β を使って $F(V)$ を作れ。

答 $V_1 = A\alpha + B\beta$ と書き、根を配置換えしたものを $V_2 = A\beta + B\alpha$ と書けば、

$$F(V) = \Pi_{\alpha, \beta} \{V - (A\square + B\square)\} = (V - V_1)(V - V_2)$$

$$= V^2 - (A+B)(\alpha+\beta)V + (A^2+B^2)\alpha\beta + AB(\alpha^2+\beta^2) \quad \cdots \star$$

$$= V^2 + \underline{(A+B)a}V + \underline{\{(A^2+B^2)b + AB(a^2-4b)\}} \quad \cdots \star$$

たしかに、係数が既知数で、次数 $2!$ の V 多項式ができた。

★ のように、“根の対称式” と “ A, B の対称式” が分離されたから、☆ のように、

$\alpha + \beta = -a$ 、 $\alpha\beta = b$ という既知数を代入できた。

問題 $F(V) = \prod_{S_n} \{V - (A_1 \square + A_2 \square + \cdots + A_n \square)\}$ の係数が、有理数になることを示せ。 $\square$ に n 次方程式の n 根を配し、 $\prod \{ \}$ は、すべての順列の積をとる意味。

答 $F(V)$ は、 n 根の全配列置換からなる因子の積として作ったから、 $F(V)$ の中で根 $\alpha_1 \sim \alpha_n$ のどんな配列置換をしても、 $F(V)$ は変化しない。したがって $F(V)$ の係数に現れる根 $\alpha_1 \sim \alpha_n$ の式は、すべて対称式である（下線は、本書を貫く基本的考え方である）。 V の定義形（ $\alpha_1 \sim \alpha_n$ の置換は $A_1 \sim A_n$ の置換と同等であること）より、 $F(V)$ の係数に現れる $A_1 \sim A_n$ の式もまた、すべて対称式だと分かる。

或る根 α_k を含む項と、その項に掛かる“ $A_1 \sim A_n$ の式”を想像しよう。この式と、別の根 α_j を含む項に掛かる“ $A_1 \sim A_n$ の式”が異なれば、 $\alpha_1 \sim \alpha_n$ の式は対称式にならないのだから、掛かる“ $A_1 \sim A_n$ の式”は、どの根からみても共通である。すなわち、 $A_1 \sim A_n$ の対称式と $\alpha_1 \sim \alpha_n$ の対称式が、どの項でもくくり出され、分離する。

例えば 3 次方程式 $f(x) = 0$ の 3 根から、 $3!$ 次式（6 次式） $F(V)$ が作られ、

$$\begin{aligned} F(V) &= \prod_{\alpha, \beta, \gamma} \{V - (A_1 \square + A_2 \square + A_3 \square)\} = (V - V_1)(V - V_2) \cdots (V - V_6) \\ &= \{V - (A_1 \alpha + A_2 \beta + A_3 \gamma)\} \{V - (A_1 \alpha + A_2 \gamma + A_3 \beta)\} \{V - (A_1 \beta + A_2 \alpha + A_3 \gamma)\} \\ &\quad \times \{V - (A_1 \beta + A_2 \gamma + A_3 \alpha)\} \{V - (A_1 \gamma + A_2 \alpha + A_3 \beta)\} \{V - (A_1 \gamma + A_2 \beta + A_3 \alpha)\} \\ &= V^6 - 2(A_1 + A_2 + A_3)(\alpha + \beta + \gamma)V^5 + \cdots \cdots \end{aligned}$$

$$\begin{aligned} V^4 \text{ の係数は、} & (A_1^2 + A_2^2 + A_3^2)(\alpha^2 + \beta^2 + \gamma^2) + 4(A_1 A_2 + A_2 A_3 + A_3 A_1)(\alpha^2 + \beta^2 + \gamma^2) \\ & + 4(A_1^2 + A_2^2 + A_3^2)(\alpha\beta + \beta\gamma + \gamma\alpha) + 6(A_1 A_2 + A_2 A_3 + A_3 A_1)(\alpha\beta + \beta\gamma + \gamma\alpha) \end{aligned}$$

$$\begin{aligned} \text{定数項は、} & A_1^2 A_2^2 A_3^2 (\alpha^6 + \beta^6 + \gamma^6), A_1 A_2 A_3 (A_1 A_2^2 + A_2 A_3^2 + A_3 A_1^2 + A_1^2 A_2 + A_2^2 A_3 + A_3^2 A_1) \\ & \times (\alpha^5 + \beta^5 + \gamma^5)(\alpha + \beta + \gamma), \cdots, \cdots, (A_1^6 + A_2^6 + A_3^6) \alpha^2 \beta^2 \gamma^2 \text{ からなる} \end{aligned}$$

x の n 次方程式 $f(x) = 0$ を解くために、 V の $n!$ 方程式 $F(V) = 0$ を作ったら、ますます話が難しくなりそうだが、そうでないことが、今後の議論で分かる。

2. 各根が、 $V = A_1 \alpha_1 + \cdots + A_n \alpha_n$ の“整式”で書き表せることの証明

このように表せるのは驚くべきことである。各根は、 V の有理式（ V 多項式の分数式）で表され、さらに整式でも表せる。

問題 $x^2 + ax + b = 0$ の根 α 、 β を、 $V_1 = A\alpha + B\beta$ の有理式で書き表せ。

答 $\alpha + \beta = -a$ と連立させると、 $\alpha = (V_1 + Ba)/(A - B)$ 、 $\beta = (V_1 + Aa)/(B - A)$

上の問題は容易だが、3 次方程式で試みると、難しくて練習問題に向かない。

3 次どころか n 次方程式一般で、ガロアは以下の独特な方法で（原著では省略されたが）解決した。5 章の現代的証明（112 頁）は、非常に簡単なので後で見比べて欲しい。

1) “根 α_1 、および有理数” を係数にもつ $F_1(V)$ を創作する

まず前述の $F(V)$ と異なる、以下のような V 多項式を作ってみよう。

$V - (A_1\alpha_1 + A_2\alpha_2 + \cdots + A_n\alpha_n) = 0$ を、 V の 1 次方程式とみる。

上の左辺で α_1 だけ固定し、 $\alpha_2 \sim \alpha_n$ のすべての配列を $\square$ に割り振った、下記のような積を定義すると、 $(n-1)!$ 個の異なる解をもつ、 V の $(n-1)!$ 次方程式が作れる。

$$F_1(V) = \prod \{V - (A_1\alpha_1 + A_2\square + \cdots + A_n\square)\} = 0 \quad \cdots (1)$$

$$\begin{aligned} &= \prod \{(V - A_1\alpha_1) - (A_2\square + \cdots + A_n\square)\} \\ &= (V - A_1\alpha_1)^{(n-1)!} + C_1(V - A_1\alpha_1)^{(n-1)!-1} + \cdots + C_{(n-1)!} \end{aligned}$$

係数 C_k は $\alpha_2 \sim \alpha_n$ の対称式で表せる ($\alpha_1 \sim \alpha_n$ の対称式ではない) $\cdots (2)$

係数 C_k は、様々な形の $\{\alpha_2 \sim \alpha_n \text{ の対称式} \} \times \{A_2 \sim A_n \text{ の対称式} \}$ からなる。

例えば、 $C_1 = -(n-1)!(A_2 + A_3 + \cdots + A_n)(\alpha_2 + \alpha_3 + \cdots + \alpha_n)$

定数項 $C_{(n-1)!}$ は、 $\alpha_2 \sim \alpha_n$ の式と $A_2 \sim A_n$ の式が、いずれも $(n-1)!$ 次になる。

$\alpha_2 \sim \alpha_n$ の対称式は、もとの方程式を次のように変形すると得られる。

$$f_n(x)/(x - \alpha_1) = (x - \alpha_2)(x - \alpha_3) \cdots (x - \alpha_n)$$

$$\text{右辺} = x^{n-1} - (\alpha_2 + \alpha_3 + \cdots + \alpha_n)x^{n-2} + \cdots + (-1)^{n-1}\alpha_2\alpha_3\cdots\alpha_n \quad \cdots (3)$$

$$\begin{aligned} \text{左辺} &= (x^n + c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_1x + c_0)/(x - \alpha_1) \text{ を計算すれば} \\ &= x^{n-1} + (c_{n-1} + \alpha_1)x^{n-2} + (c_{n-2} + c_{n-1}\alpha_1 + \alpha_1^2)x^{n-3} + \cdots \quad \cdots (4) \end{aligned}$$

割り算の余りは (因数定理により) 0 になるから、(3)、(4) を見比べ、

$\alpha_2 \sim \alpha_n$ の基本対称式は、有理数 $c_{n-1} \sim c_0$ および α_1 で表せると分かる。

3 次方程式の例では、 $x^2 - (\alpha_2 + \alpha_3)x + \alpha_2\alpha_3 = x^2 + (a + \alpha_1)x + (b + a\alpha_1 + \alpha_1^2)$ 、

定数項 $\alpha_2\alpha_3$ は、 $\alpha_1\alpha_2\alpha_3/\alpha_1 = -c/\alpha_1$ でなく、 $b + a\alpha_1 + \alpha_1^2$ と書ける。

(4) のどの項も、 α_1 の (分数式でなく) 整式で書けることに注目しよう。

したがって、(2) と合わせると、

$F_1(V)$ の係数は、有理数「 $A_1 \sim A_n$ 、係数 $c_{n-1} \sim c_0$ 」を含む “ α_1 の整式” となる。

そこで、 $F_1(V) = F_1(V, \alpha_1) = 0$ と書くことにする。

すると $F_1(V, x) = 0$ という x の方程式が、 $x = \alpha_1$ という根をもつ、と読み替えられる。このとき V は (変数でなく)、 x の方程式の係数を構成する文字とみなせる。

2) x の方程式とみた $F_1(V, x) = 0$ と、もとの方程式 $f_n(x) = 0$ が、 唯一の根 $x = \alpha_1$ を共有することの証明

$F_1(V, x) = 0$ の定義式 (1) に、 $x = \alpha_2$ を代入して、 $F_1(V, \alpha_2) \neq 0$ を証明しよう。

$F_1(V, \alpha_1)$ の中で $\alpha_1 \rightarrow \alpha_2$ と書き換えると、(1) $\rightarrow F_1(V, \alpha_2)$ になる。

$$F_1(V, \alpha_2) = \Pi \{V - (A_1 \alpha_2 + A_2 \square + \cdots + A_n \square)\} \cdots (5)$$

□には、 α_1 以外のあらゆる配列が入っているから、

() 内に、 α_2 は二度現れ、 α_1 は無い。

一方、 V の方程式 $F_1(V, \alpha_1) = 0$ の解はすべて、 $F_1(V)$ の定義により、

$$A_1 \alpha_1 + A_2 \square + \cdots + A_n \square \text{ の形である (これらを、解 } V^* \text{ と総称しよう)} \cdots (6)$$

(6) の□には、 $\alpha_2 \sim \alpha_n$ の任意配列が入ってよい

(5) 式に、(6) の形の解 V^* を代入すると、(5) のすべての $\{ \}$ の中で、

$$\{(\text{任意の解 } V^*) - (A_1 \alpha_2 + \cdots)\} = \{(A_1 \alpha_1 + \cdots) - (A_1 \alpha_2 + \cdots)\} \neq 0 \text{ である。}$$

なぜなら； $A_1 \square + \cdots + A_n \square$ の値は、□に入る根に 1 つでも不一致があれば異なるように $A_1 \sim A_n$ を決めればよい。我々が考える V の置換は根の並べ替えのみだが、 $A_1 \sim A_n$ の決め方は無限だから、□に重複も含めた根を入れた n^n 通り（有限ヶ）の V が、すべて異なるように選べる。

したがって、 $F_1(V^*, \alpha_2) \neq 0$ である（ように $A_1 \sim A_n$ を決めておける）。

$F_1(V, x)$ は、「 $V = V^*$ 、かつ $x = \alpha_1$ 」を代入したら 0 になるよう、(1) で定義した。そして「 $V = V^*$ 、かつ $x = \alpha_2$ 」を代入したら、 $\neq 0$ と分かった。すなわち、 x の方程式 $F_1(V, x) = 0$ は、係数成分の V が値 V^* をとるとき、 $x = \alpha_1$ を解にもつが、 $x = \alpha_2$ は解にならない。

簡潔に言うと、 $F_1(V, \alpha_1) = 0$ なら、 $F_1(V, \alpha_2) \neq 0$ である。

ここで V とは、 n 根の特定の一次式 V_k の総称であり、任意の V_k で上記のことが言える。

$\alpha_2 \sim \alpha_n$ の対称性により、 $F_1(V, \alpha_3) \neq 0$ 、 $\cdots$ 、 $F_1(V, \alpha_n) \neq 0$ 、も言える。

さて、 α_1 は、重根のない方程式 $f_n(x) = 0$ の根である。

そして、 $\alpha_2 \sim \alpha_n$ は、 x の方程式 $F_1(V, x) = 0$ の解ではないと分かったのだから、

$F_1(V, x) = 0$ と $f_n(x) = 0$ は、“唯一の” 共通解 $x = \alpha_1$ をもつ、と分かった。

すると 1 章の互除法の定理（14 頁）により、 $F_1(V, x)$ と $f_n(x)$ から、ユークリッドの互除法で α_1 が算出できる。 α_1 を、上記 2 つの x 多項式の係数値で書ける！

重要な留意点

1 章で、「 $A(x) = 0$ と $B(x) = 0$ が唯一の根を共有するなら、その根は、互除法で求まるから有理数」、「既約方程式は、他の方程式と 1 根だけを共有することはできない」ことを学んだ。今の話と矛盾するだろうか？

1 章では、多項式 $A(x)$ 、 $B(x)$ の係数を“有理数”としたから、係数から算出される根の値を有理数、と結論したのだった。

今は x の多項式 $F_1(V, x)$ の係数成分に、根 $\alpha_1 \sim \alpha_n$ の式 V がある（有理数でない）。 $\alpha_1 \sim \alpha_n$ を含む $F_1(V, x)$ の係数成分が“計算対象”だから、 $f_n(x)$ はもはや既約式でない。したがって共通因子 $(x - \alpha_1)$ が、互除法で算出できる。

$F_1(V, x)$ に $\alpha_1 \sim \alpha_n$ の姿は見え (α_1 は x に置き換え)、 V の中に隠れているから、 $\alpha_1 \sim \alpha_n$ 自体を使う計算にみえないが、 V を通じて n 個の根が使われている。すなわち互除法の最後で、 $(x - \alpha_1)$ で割った余り $= 0$ と結論できる。

3) $\alpha_1 = V$ の整式/ V の整式、という分数式 (有理式) を得る方法

$F_1(V, x)$ と $f_n(x)$ に互除法を適用するが、実際の計算はせず、想像だけを進める。

x の多項式とみた $F_1(V, x)$ において、 V は変数でなく、 V_k と総称される根の式とみなした。ここで V は、 $F_1(V) = 0$ の解を意味し、54 頁の $F(V) = 0$ の解の一部でもある。

$F_1(V, x)$ は、 x の $(n-1)!$ 次多項式、係数は「 V 、既知数 $A_1 \sim A_n$ 、既知係数 $c_{n-1} \sim c_0$ 」からなる文字式である。定数項は V の $(n-1)!$ 次多項式、ということになるが、各項の具体形は考えなくてよい。

$f_n(x)$ は、 x の n 次式。係数はむろん「 $c_{n-1} \sim c_0$ 」である。

{割られる式, 割る式} = 余り、という 1 章で使った互除法の記号で、

$\{F_1(V, x), f_n(x)\} \rightarrow \{f_n(x), \text{左記の余り}\} \rightarrow \cdots \rightarrow$ と割り算を繰り返すと、

“唯一の” 共通根 α_1 が存在するのだから、1 次式で割るところまで進み、

$\{\cdots, Px + Q\} = r$ の形に到達し、最後に割り切れる ($r = 0$) としてよい。

$Px + Q$ が共通因子だから、 $Px + Q = 0$ 、

すなわち、共通根 $\alpha_1 = -Q/P$ である。

P と Q は、 V と有理数 $c_{n-1} \sim c_0$ 、 $A_1 \sim A_n$ からなる文字の複雑な有理式である。

したがって、 $\alpha_1 = \{V \text{ の整式} \} / \{V \text{ の整式} \}$ 、という V の有理式となる。

注：3 次方程式 $f_3(x) = 0$ の場合だけは、計算が上記と少し異なる。

$F_1(V, x)$ が x の 2 次式になるので、互除法は、上記の割り算と逆に、3 次式 $f_3(x)$ を 2 次式 $F_1(V, x)$ で割ることから始まる。

4) 上の分数式を、さらに、 $\alpha_1 = \{V \text{ の整式} \}$ と書き直すことができる

任意の方程式で、解一般について思いがけない下記の定理がある。

n 次方程式、 $x^n + Ax^{n-1} + Bx^{n-2} + Cx^{n-3} + \cdots = 0$ の解の 1 つを X とすれば、

X の任意分数式 (有理式) は、必ず X の $n-1$ 次以下の整式に書き直せる。

証明しよう。ここで X は変数でなく、下記の式を満たす“或る数”を意味する。

$$X^n + AX^{n-1} + BX^{n-2} + CX^{n-3} + \cdots = 0 \quad \star$$

$\star$ を、 $X^n = -(AX^{n-1} + BX^{n-2} + CX^{n-3} + \cdots)$ と変形すれば、 X の n 次式は、 X の $(n-1)$ 次以下の式で書ける。 $X^{n+1} = -(AX^n + BX^{n-1} + \cdots)$ 、 $X^{n+2} = -(AX^{n+1} + \cdots)$ 、と帰納し、任意次数の X の整式は、 X の $(n-1)$ 次以下の整式で書けると分かる。

では、 $g(X) = X^m + P X^{m-1} + Q X^{m-2} + \dots$ ($m < n$) だとして、 $1/g(X)$ を、 X の整式に書き直すにはどうすればよいのか？

★ の両辺を $g(X)$ で割り、 $g(X) h_1(X) + r_1(X) = 0$ と書く。 $h_1(X)$ は商、 $g(X)$ が m 次だから、余り $r_1(X)$ は $m-1$ 次以下であり、 $g(X) = -r_1(X)/h_1(X)$ と書ける。

★ の両辺を今度は、 $r_1(X)$ で割れば、同様に $r_1(X) = -r_2(X)/h_2(X)$ と書けるから $g(X) = -r_1(X)/h_1(X) = r_2(X)/h_1(X) h_2(X)$ 、余り $r_2(X)$ は、 $m-2$ 次以下だから、右辺で“分子の次数”が下がった。さらに、★ の両辺を $r_2(X)$ で割る。

これをくり返せば、 $g(X) = \text{定数}/h_1(X) h_2(X) h_3(X) \dots$ に帰着する。すなわち、 $1/g(X)$ が整式になり、これをさらに $(n-1)$ 次以下の整式に書き直せる。

本論に戻る。 V は、55 頁の $(n-1)!$ 次方程式、 $F_1(V) = 0$ の解なのだから（上記 ★ に相当）、上記の定理が使えて、

$\alpha_1 = \text{「}V \text{ の分数式」}$ を、 $\alpha_1 = \text{「}V \text{ の } \{(n-1)! - 1\} \text{ 次以下の整式」}$ に書きなおせる。

この整式を、 $\phi_1(V)$ と名付ける。

$\alpha_1 = \phi_1(V)$ 右辺が V の整式と分かればよく、具体形も次数も考えなくてよい。

5) すべての根 α_k を V の整式で、 $\alpha_k = \phi_k(V)$ と書く方法

$F_1(V)$ の代わりに、 α_2 を固定し、 α_2 以外のすべての可能な配置を $\square$ に割り振った、

$$F_2(V) = \Pi \{V - (A_1 \square + A_2 \alpha_2 + A_3 \square + \dots + A_n \square)\}$$

を定義すれば、まったく同じ議論で、 $\alpha_2 = \phi_2(V)$ 、と V の整式で書ける。

ただし、この V は（前述 $\alpha_1 = \phi_1(V)$ のときと違い）、 $F_2(V) = 0$ の解である。

同様に、 A_k に α_k を固定し、 α_k 以外の可能な配列をすべて掛け合わせた $F_k(V)$ を使って、 $\alpha_k = \phi_k(V)$ が得られる。この V は、 $F_k(V) = 0$ の解を意味する。

蛇足的な注意： $F(V) = \Pi_{Sn} (V - V_k)$ は、 $F_1(V) F_2(V) \dots F_n(V)$ に等しくない。

各 $F_k(V)$ は、 $F(V)$ の因子ではあるが、 $F_1(V) \dots F_n(V)$ は、無意味な式である。

以上から、 n 次方程式の各根は、 $\alpha_1 \sim \alpha_n$ の 1 次式 V を使って、 V の整式で $\alpha_1 = \phi_1(V)$ 、 $\alpha_2 = \phi_2(V)$ 、 $\dots$ 、 $\alpha_n = \phi_n(V)$ と書けるのが分かった。ただし、これらの等式を同時に成り立たせる V は、 $F_1(V) = 0$ の解、かつ $F_2(V) = 0$ の解、 $\dots$ 、かつ $F_n(V) = 0$ の解だから、 $V_1 = \Sigma A_k \alpha_k = A_1 \alpha_1 + A_2 \alpha_2 + \dots + A_n \alpha_n$ のみである。

ところが、 $\alpha_1 = \phi_1(V_1)$ 、 $\alpha_2 = \phi_2(V_1)$ 、 $\dots$ 、 $\alpha_n = \phi_n(V_1)$ 、それぞれを得た計算法は、根の名称変更に影響されないから、この一組の等式において、左辺と右辺で一斉に根配列を置換しても等式は成り立つのである（右辺の V_1 は V_k などに変更される）。

或る根配列式の V_1 、それを配列置換した式 V_k 、などの添字表記は恣意的であり根の名称変更を言うに過ぎない。 $\alpha_k = \varphi_k(V)$ と書いた場合、 V は変数でなく 54 頁の $F(V) = 0$ の“或る解”を意味する。 $\varphi_k(V)$ を置換したら $\varphi_k(V')$ 、などを書く

V_1 と異なる V_a を n 個の等式 $\alpha_k = \varphi_k(V_1)$ に代入したら、 $\alpha_j = \varphi_k(V_a)$ 、など書ける。 $\alpha_1 \sim \alpha_n$ と $\varphi_1 \sim \varphi_n$ を結ぶ等式は、 $n!$ とおりの V に応じ、 $n!$ とおりに書けるが、 $F_k(V)$ の作り方を再度思い出すと、 α_k 以外を置換した $(n-1)!$ とおりの V すべて（それらを $V, V', V'', \dots$ と呼び）、 $\alpha_k = \varphi_k(V) = \varphi_k(V') = \varphi_k(V'') = \dots$ となる。

6) 各根 $= V$ の整式、という n 個の関係式が実在することの意味

連立した関係式、 $\alpha_1 = \varphi_1(V), \alpha_2 = \varphi_2(V), \dots, \alpha_n = \varphi_n(V) \quad \cdots \star$
が存在することには、以下の意味がある。

i) V の値を得れば、全根が求まる。 n 個の未知数 $\alpha_1 \sim \alpha_n$ が、1 個の未知数 V に減少したのではなく、 V の関数 $\varphi_1 \sim \varphi_n$ に書き換えられ、 n 根の相互関係が表現された。

ii) 根の配列を置換すると、 $\star$ の左辺の根名が変わり、右辺の V も別の V' に変わるが、関係式 $\star$ が全体として成り立つことには変わらない（我々は、根の名称変更に影響されない方法で $\star$ を導いた）。

→ 根の配列置換に対し、 n 個の関係式 $\star$ は「保存される」と言える。

保存という言葉は（物理の運動量保存のように）議論の意味を簡明に表すだろう。

3. 根の配列変化と V の変化の関係： $\alpha_k = \varphi_k(V) \rightarrow \alpha_j = \varphi_k(V')$ の決め方

V の値（ないし形）は、 $A_1 \sim A_n$ に配置した根 $\alpha_1 \sim \alpha_n$ の配列で決まる（値には数値、形には文字式のイメージをもつだろうが、同じことと考える）。

問題 V における $\alpha_1 \sim \alpha_n$ を、配列置換した形（値）を、 V' と呼ぶとする。

$\alpha_k = \varphi_k(V)$ に、 V に替えて V' を代入した $\varphi_1(V'), \varphi_2(V'), \dots, \varphi_n(V')$ は、それぞれ $\alpha_1, \alpha_2, \dots, \alpha_n$ のどれかに等しい。どれに等しいのかを示せ。

答 $\alpha_1, \dots, \alpha_n$ を配列置換した結果を、その順に $\alpha'_1, \dots, \alpha'_n$ と呼び替えれば、

$\alpha_1 = \varphi_1(V), \alpha_2 = \varphi_2(V), \dots, \alpha_n = \varphi_n(V)$ というもとの関係は、

$\alpha'_1 = \varphi_1(V'), \alpha'_2 = \varphi_2(V'), \dots, \alpha'_n = \varphi_n(V')$ となる（つまり答は簡単である）。

φ_k の添え字 k を変えてはいけない！（これも変えたら、置換にならない）

置換は、数字一般にでなく、“根の”添え字に作用する。

または下記のように言ってもよい。

g で置換したものを $Vg = V'$ 、 $\alpha_k g = \alpha_j$ と呼ぶと、 $\alpha_k = \varphi_k(V) \rightarrow \alpha_j = \varphi_k(V')$ になる。
つまり、 $\alpha_j = \alpha_k g$ 、 $\varphi_k(V) g = \varphi_k(Vg) = \varphi_k(V')$

問題 $\alpha_1 = \varphi_1(V)$ 、 $\alpha_2 = \varphi_2(V)$ 、 $\alpha_3 = \varphi_3(V)$ 、 $V = A_1 \alpha_1 + A_2 \alpha_2 + A_3 \alpha_3$ とする。

α_1 、 α_2 、 α_3 を、 $V' = A_1 \alpha_3 + A_2 \alpha_2 + A_3 \alpha_1$ の整式で書き表せ

答 $\alpha_k = \varphi_k(V)$ の左辺で、根の添え字を $1, 2, 3 \rightarrow 3, 2, 1$ と書き直し、
 $\alpha_3 = \varphi_1(V')$ 、 $\alpha_2 = \varphi_2(V')$ 、 $\alpha_1 = \varphi_3(V')$ 、が答である。
 $\varphi_k(V')$ を計算するのではなく、関係式に互換 (1 3) を作用させるだけである。

φ_k の存在のみに注目し、関数形を問わないのが、ガロアの方法論の特徴である。

根と φ の関係を一般的に言うとき、 $\alpha_k = \varphi_k(V)$ よりも、添え字を、 $\alpha_j = \varphi_k(V)$ と書くのがよい ($j, k = 1, 2, \dots, n$)。この関係は、重根のない任意方程式で成り立つが、我々が興味をもつのは (本章の冒頭で述べたように) 既約方程式である。

4. 各根 = V の整式、を与える根の 1 次式 V を、 n ケよりも少数の “任意根” で書ける既約方程式もある

ガロアは論文の初めから標記のことを述べた。 n 根で書いた前項の V と併記する意味が初読者には分かりにくい、今は「 $f(x) = 0$ の各根を、他の任意根の有理式でどう書けるかは、 $f(x)$ の係数値間の関係で決まるだろう」と想像すればよい。

“任意の方程式” で、 $\alpha_j = \varphi_k(V)$ を導くには、全根からなる $V = A_1 \alpha_1 + \dots + A_n \alpha_n$ の形を使う必要があった。

一方、少数ケの任意根からなる V で、 $\alpha_j = V$ の整式 $= \psi_k(V)$ と表せる方程式があれば、表せることを改めて示さねばならない (誤解しないよう、 φ_k と ψ_k で区別する)。

例えば 2 根で全根を表せるとき、前項の $\alpha_k = \varphi_k(A_1 \alpha_1 + \dots + A_n \alpha_n)$ に $A_3 \sim A_n = 0$ を代入して、 $\alpha_k = \varphi_k(A_1 \alpha_1 + A_2 \alpha_2) = \psi_k(A_1 \alpha_1 + A_2 \alpha_2)$ になるのではなく、 $\varphi_k \neq \psi_k$ である。

$\alpha_k = \varphi_k(V_1) = \varphi_k(A_1 \alpha_1 + \dots + A_n \alpha_n)$ を導いた前提は、任意置換で V_1 が必ず、別の値 V_j になることだから、 $A_1 \sim A_n$ の いずれも 0 であってはならない。

今は、“少数根で書ける V の実例” を見て、標記のことを納得するだけでよい。

実際、任意 1 根で、他根すべてを有理的に表せる方程式がある。

n が素数のとき、 $(x^n - 1)/(x - 1) = x^{n-1} + \dots + x + 1 = 0$ の根は、みな原始根だから、任意 1 根、例えば α_1 で、各根 $= \alpha_1^m$ ($m = 1, 2, 3, \dots, n-1$) と書ける。

この場合、単に $V_1 = \alpha_1$ とすればよいのである。

そして各根は、 $\alpha_k = \alpha_1^k = V_1^k = \psi_k(V_1)$ 、のように V_1 の整式で書ける。… (#)

59 頁の意味で、 $\alpha_k = \psi_k(V)$ を置換したら、 $\alpha_j = \psi_k(V')$ 、などと略記してもよい。

論理の重要な発展：以下を認識するのが、本項の目的である。

前頁（#）を成り立たせる（保存する）置換は、任意の置換ではあり得ない。

例えば、 $\alpha_2 = \alpha_1^2$ 、 $\alpha_3 = \alpha_1^3$ 、…の関係を、添え字互換 (2 3) で置換すると、 α_1 は変化せず（指数は、根添え字でないから変化しないので）、 $\alpha_3 = \alpha_1^2$ 、 $\alpha_2 = \alpha_1^3$ 、… となり、 $\alpha_2 = \alpha_1^2 = \alpha_3$ 、という矛盾を生じ、 $\alpha_3 = \alpha_1^3 = \alpha_2$ 、 $\alpha_1^2 = \alpha_1^3$ も矛盾である。

$V (= \alpha_1)$ が変化しない置換をしたから、矛盾がおきたのである。

m ケの根からなる V^* の整式で、 $\alpha_j = \psi_k(V^*)$ と表せるとき、この関係式を保存する置換は、 V^* を変化させる置換であることが“必要”である（十分であるかどうかは、方程式ごとに個別に考える；本章の最後に述べる）。

全根で書いた $V = A_1 \alpha_1 + \cdots + A_n \alpha_n$ は、任意置換で変化するが、一部の根で書かれた V は、或る特定置換でのみ変化する。このことは当たり前ともいえるが、ガロアの方法論は、関係式 $\alpha_j = \varphi_k(V)$ の存在と、この関係式を保存する置換が存在することだけに注目する、これは独創的で不思議な着想と思える。

以下、 ψ_k と φ_k を区別せず、 V の整式はみな $\varphi_k(V)$ と書く。とくに断らない限り、 V とは、 $\alpha_j = \varphi_k(V)$ を与える“ m 根の 1 次式 ($m = n$ も含め)”と一般的に考える。

5. 関係式 $\alpha_j = \varphi_k(V)$ を保存する置換の集合は、群になる

1) n ケの関係式 $\alpha_1 = \varphi_a(V)$ 、 $\alpha_2 = \varphi_b(V)$ 、…、 $\alpha_n = \varphi_q(V)$ … ★

を保存する（成り立たせる）置換の集合が、“群である”ことの証明

★ を配列置換すれば、左辺で $\alpha_1 \sim \alpha_n$ のどれかは、必ず変わる。

V が変化しない置換をしたら、「 $\alpha_i \rightarrow \alpha_j$ で V が不変、 $\alpha_i = \varphi_k(V) \rightarrow \alpha_j = \varphi_k(V)$ となり、 $\alpha_i = \varphi_k(V) = \alpha_j$ となる i, j 」が必ずあるから、矛盾を生じる（今、重根はない）。

V が変化して V' になったなら、関係式は $\alpha'_1 = \varphi_a(V')$ 、 $\alpha'_2 = \varphi_b(V')$ 、…、 $\alpha'_n = \varphi_q(V')$ になる。この置換で α_1 が不変なら、 $\alpha_1 = \varphi_a(V') = \varphi_a(V)$ となるが、これは矛盾でない（59 頁参照）。 V が変化することは、関係 $\alpha_j = \varphi_k(V)$ が保存される（矛盾がおきない）ための、必要条件である（前述のように、今は十分条件を考えずに先へ進む）。

“関係式 ★ を保存する置換 $g, g', g'', \dots$ のすべて” からなる集合を、 G とする。

e は、明らかに ★ を保存するから、 G の元である ($e \in G$)。

g が ★ を保存し、 g' が ★ を保存すれば、 gg' が ★ を保存し（保存するすべての置換の集合が G だから）、 gg' も G の元である ($g \in G, g' \in G$ なら $gg' \in G$)。

したがって、 G は群である。

★ を保存する「すべて」の元を含む G は ★ を保存する最大の群である。

G が上の関係式 ★ を保存すれば、 G の部分群も ★ を保存する。これは、部分群の語義そのものである。★を保存する小さな群は、大きな群の部分群である。

2) V を任意 1 根で表せるとき、 $\alpha_j = \varphi_k(V)$ を保存するのは、どんな群か？

n が素数のとき、方程式 $x^{n-1} + \cdots + x + 1 = 0$ では、任意の 1 根（原始根）で全根を有理的に表せる。 $V = \alpha_k$ として、 $\alpha_1 = \varphi_1(\alpha_k)$ 、 $\alpha_2 = \varphi_2(\alpha_k)$ 、 $\cdots$ 、 $\alpha_{n-1} = \varphi_{n-1}(\alpha_k)$

添え字 k を必ず変化させる置換を考える。 a を $\text{mod } n$ の原始根とし、 $g : k \rightarrow ak$ で生成される巡回群 $\{e, g, g^2, \cdots, g^{n-2}\}$ が、 $\alpha_j = \varphi_j(\alpha_k)$ を保存する。

$k \rightarrow k+1$ という巡回置換を使うと、 $\alpha_k^n = 1$ 、という（上の方程式の根でない）値が出てしまうから、 $k \rightarrow ak$ としなければいけないのであった（51 頁）。

問題 $x^4 + x^3 + x^2 + x + 1 = 0$ の 1 根 α_1 で、全根を $\alpha_k = \alpha_1^k$ と書き、 $\alpha_1 = V$ とするとき $k \rightarrow 2k, (\text{mod } 5)$ による置換、 $\alpha_k = \varphi_k(V) \rightarrow \alpha_{2k} = \varphi_k(V')$ を書き表せ。

答 $\varphi_k(V)$ の添え字や V の指数は、根名でないから置換対象でない（59 頁）。

根の置換 $k \rightarrow 2k$ で、 $\alpha_1 = V \rightarrow \alpha_2 = V'$ 、 $\alpha_k = \varphi_k(V) = V^k \rightarrow \alpha_{2k} = \varphi_k(V') = V'^k$
つまり、 $\alpha_1 = V$ 、 $\alpha_2 = V^2$ 、 $\alpha_3 = V^3$ 、 $\alpha_4 = V^4 \rightarrow \alpha_2 = V'$ 、 $\alpha_4 = V'^2$ 、 $\alpha_1 = V'^3$ 、 $\alpha_3 = V'^4$
と書くのが正しい。一方、「 $\alpha_1 = \omega$ で、全根を $\alpha_k = \omega^k$ と表せば、置換 $k \rightarrow 2k$ で ω 、 ω^2 、 ω^3 、 $\omega^4 \rightarrow \omega^2$ 、 ω^4 、 ω^1 、 ω^3 に変わる」と言うのは、構わないであろう。

3) 以上のまとめ

重根のない方程式の各根は必ず、 V の整式で $\alpha_j = \varphi_k(V)$ と表せる。

関係 $\alpha_j = \varphi_k(V)$ を保存する置換群が存在する。 $\alpha_j = \varphi_k(V) \rightarrow \alpha_i = \varphi_k(V')$

各根を V の整式で表すとき、方程式の構造（根どうしの間の関係）が不明なら、 $V = A_1 \alpha_1 + \cdots + A_n \alpha_n$ を使えばよく、方程式によっては少数ヶの根で V を書ける。

V の記法：或る根配列の V を V_1 とし、「 V_1 を置換したら V_k に変わる」などと言うほか、 V_1 や V_k を総称して V と略記し、「 V を置換したものを V' 」と呼んでもよい。

6. V_1 を置換して作った多項式 $F(V)$ の係数に含まれる、“根の関数” の置換対称性

$V_1 = A_1 \alpha_1 + \cdots + A_n \alpha_n$ とする。

今から、 n 次方程式の一般解法を考えるので、任意方程式に通用する「 n 根からなる V_k 」を使わねばならない（ V_k は総称、その 1 つが V_1 ）。

或る群 H (位数 m) の元、 $h_1 (= e)$ 、 h_2 、 $\dots$ 、 h_m のすべてで、 V を置換したものをそれぞれ V_1 、 V_2 、 $\dots$ 、 V_m と呼ぼう。 $V_k = V_1 h_k$ である。

群は定義上閉じている。すなわち、 $V_k = V_1 h_k$ をさらに h_j で置換した $V_k h_j = V_1 h_k h_j$ は、やはり $V_1 \sim V_m$ のどれかである。

つまり V 多項式、 $F_H(V) = (V - V_1)(V - V_2) \cdots (V - V_m)$ は、 H で変化しない。

このことを、 $F_H(V)$ は H 対称性である、と言う。

群の元すべてで置換したものの掛け合わせ $\rightarrow$ 群対称性、という手法は頻繁に使う。

注意：群でない置換集合で、 $(V - V_1) \cdots (V - V_p)$ を作ったら、 V_k を置換したとき $V_1 \sim V_p$ 以外のものになりうるから、 $(V - V_1) \cdots (V - V_p)$ は変化してしまう。

閉じた置換集合は群であり、群でない集合は閉じていない。

$$F_H(V) = \prod_H (V - V_k) = V^m - (V_1 + \cdots + V_m)V^{m-1} + \cdots \pm V_1 V_2 \cdots V_m$$

の展開係数に含まれる、様々な“根の関数”を $\theta = \theta(\alpha_1, \dots, \alpha_n)$ と総称しよう。

すると、どの θ も、 H で変化しないのは明らかである。

$V_1 \sim V_m$ を $\alpha_1 \sim \alpha_n$ で書けば、 H 対称性の θ の具体形が、この V 多項式の係数の中に現れる。より正確に言えば、 H 対称性の θ および、より高対称性の θ' が現れる。

【例】 H が、3 根の巡回置換 $(\alpha \beta \gamma)$ から生成される群なら、

$$\begin{aligned} F_H(V) &= \{V - (A\alpha + B\beta + C\gamma)\} \{V - (A\beta + B\gamma + C\alpha)\} \{V - (A\gamma + B\alpha + C\beta)\} \\ &= V^3 - (A + B + C)(\alpha + \beta + \gamma)V^2 + PV + \text{定数項 } Q \end{aligned}$$

$$P = (A^2 + B^2 + C^2)(\alpha\beta + \beta\gamma + \gamma\alpha) + (AB + BC + CA)(\alpha\beta + \beta\gamma + \gamma\alpha) + (AB + BC + CA)(\alpha^2 + \beta^2 + \gamma^2)$$

Q は、対称式 $\alpha\beta\gamma$ 、 $\alpha^3 + \beta^3 + \gamma^3$ と、 H 対称式 $\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha$ 、 $\alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2$ からなる。

H の部分群 H' (位数 m' とする) の元すべてで V を置換して作った、 m' 次の V 多項式 $F_{H'}(V) = (V - V_1) \cdots (V - V_{m'})$ は H' 対称性、すなわち展開係数に含まれる根の関数は、 H' 対称性をもつ (H' よりも高い対称性をもつ関数も含まれる)。

S_n 対称性の $F_{S_n}(V) = \prod_{S_n} (V - V_k)$ を展開すれば、 $n!$ 次の V 多項式になる。

$F_{S_n}(V)$ の係数に現れる根の関数は、明らかにすべて対称式である。

S_n より小さな部分群で作った $F_H(V)$ や $F_{H'}(V)$ の係数が、根の非対称式を含むこともまた明らかである。

$S_n \supset H \supset H'$ であれば、

$F_H(V)$ は、 $F_{S_n}(V)$ に含まれる因子であり、 $F_{H'}(V)$ は $F_H(V)$ に含まれる因子である。

$F_H(V)$ の係数が $F_{S_n}(V)$ の係数から算出されるか、 $F_{H'}(V)$ の係数が $F_H(V)$ の係数から算出されるか、すなわち分解計算が次々と実現するかどうか、課題になる。

$F_H(V)$ の因数分解で、因子 $F_{H'}(V)$ を得るとは、 H' 対称性の根の関数（係数成分）が、 H 対称性の根の関数（係数成分）から（巾開方を含む計算で）求まることである。

7. V を解にもつ $F(V)=0$ の因数分解が、 $f(x)=0$ の解法であるというアイデア

前の話と重複するが、 $F(V)$ は、その係数が、 $f(x)=0$ の係数（すなわち根の基本対称式）で書かれる既知関数であり、 $F(V)=0$ の解 V_k を得るとは、 $F(V)$ を 1 次式にまで因数分解することである。

$\alpha_j = \phi_j(V_k)$ と書けるから、 V_k を得たとき、 $f(x)=0$ の n 根 $\alpha_1 \sim \alpha_n$ は一斉に求まる。ただしガロアの議論は、 $F(V)$ の因数分解の手順だけ考え、 V_k の値は計算しないのである。 $F(V)$ の分解因子の係数の中には、分解すべき根の関数、それが分解された関数形、という計算対象がすべて入っている。

$$V_1 = A_1 \alpha_1 + \cdots + A_n \alpha_n = \sum A_j \alpha_j \text{ とする。}$$

S_n の元で V_1 を置換した、 $V_1, V_2, \dots, V_{n!}$ を解にもつ $n!$ 次方程式、

$$F_{S_n}(V) = \prod_{S_n} (V - V_k) = V^{n!} + (V_1 + \cdots + V_{n!}) V^{n!-1} + \cdots + V_1 V_2 \cdots V_{n!} = 0$$

の係数は、既知の有理数である（根 $\alpha_1 \sim \alpha_n$ の対称式、 $A_1 \sim A_n$ で書ける）。

$F_{S_n}(V)$ は既約式である。因数分解に必要な“非対称関数”が、“対称関数の巾開方量として”追加されたら、その計算範囲で $F_{S_n}(V)$ は可約になり、

$$F_{S_n}(V) = F_1(V) \times F_2(V) \times F_3(V) \times \cdots \text{ のようになる}$$

この段階で $F_1(V), F_2(V), \dots$ は既約であり、係数は非対称関数と対称関数からなる。

$$\text{下線部の比喩； } X^4 - 6X^2 + 5 = \{X^2 - (3 + \sqrt{2})\} \{X^2 - (3 - \sqrt{2})\}$$

という分解なら、右辺の因子は無理数と有理数からなる

（イメージしにくければ、76 頁～の実例を一瞥するとよい）

$S_n \supset G \supset \cdots$ だとして、 $F_{S_n}(V)$ の因数分解が実現し、因子 $F_G(V)$ が得られたら、 $F_{S_n}(V)=0$ を解く問題が、 $F_G(V)=0$ を解く問題に還元される。

このとき、 $F_G(V)$ の係数は、“ $F_{S_n}(V)$ の係数項すなわち根の対称式”を巾開方した様々な式で書かれている（と想像するだけでよい）。

因数分解の実現のたびに、解くべき V 方程式の次数は低下し、係数は“根の対称式の巾開方の、そのまた巾開方”を繰り返して書き表されていく（と思うだけでよい）。

$F_{S_n}(V)$ を、1 次式の積 $(V - V_1) \times (V - V_2) \times \cdots$ にまで因数分解する計算手順を示すことが、 n 次方程式の一般解を得る手順を示すことと同等である。

S_n より小さな群 G で作った $F_G(V)$ の係数は、むしろ非対称関数を含む。

ただし、既約方程式 $f_n(x)=0$ の係数間に特別な関係があれば、 $F_G(V)$ の係数（何

らかの非対称関数) が有理数になりうるだろう。

その場合、 $F_G(V) = 0$ の解を求めることが課題、すなわち $F_G(V)$ の因数分解を、解法の出発点にすればよい (出発点における既知数は、有理数だとしている)。

イメージ化のため、重根のない“可約方程式”で例え話をする。重根がなければ、 $\alpha_j = \varphi_k(V) = \varphi_k(A_1 \alpha_1 + \cdots + A_n \alpha_n)$ 、という整式は必ず存在する。

例えば、 $f(x) = x^4 - 2x^2 + 2 = 0$ を考えよう。この方程式は、4つの異なる無理根をもち、 $(x^2 - x + 2)(x^2 + x + 1) = \{x^2 - (\alpha_1 + \alpha_2)x + \alpha_1\alpha_2\} \{x^2 - (\alpha_3 + \alpha_4)x + \alpha_3\alpha_4\}$ と因数分解できるので、4根の基本対称式以外に、 $\alpha_1 + \alpha_2$ 、 $\alpha_1\alpha_2$ 、 $\alpha_3 + \alpha_4$ 、 $\alpha_3\alpha_4$ 、という4つの非対称関数も有理数である。

すると、 $V_1 = A_1\alpha_1 + A_2\alpha_2 + A_3\alpha_3 + A_4\alpha_4$ を、 $G = \{e, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$ で置換して G 対称性にした $F_G(V) = \Pi_G(V - V_k)$ は、有理係数 (既知数) の4次式になる。

$S_4 \supset G$ であり、 $F_G(V)$ は、4! 次である $F_{S_4}(V)$ よりも低次の、有理係数多項式である。重要なことに今の場合、 $F_{S_4}(V)$ は、有理因子 $F_G(V)$ をもつ可約式である。

因数分解が進むと、計算対象に使える既知数 = “有理数および或る巾開方量” になる。この (拡大された) 既知数を係数成分にもつ $F_G(V) = 0$ が、“次の段階の” 因数分解の出発点だと解釈できる。

$F_{S_n}(V)$ を因数分解して、因子 $F_G(V)$ が得られる場合もあり、上記の例え話のように $F_G(V)$ が因数分解の出発点のこともある。したがって解法理論では、 $F_G(V)$ の因数分解を考えることが、一般的な課題だと分かる。

§2 ガロア群

1. 方程式の群 (ガロア群) の概念

1) 方程式の群 (ガロア群) の定義

或る方程式 $f(x) = 0$ を特徴づける (根どうしの関係で決まる) 群を定義できる。 $f(x)$ の係数は、数値でも文字でもよいが、有理数と決める。

ガロアは、“方程式の群” と命名した G を次のように定義した。「根の関数が有理計算できるなら G で不変、逆に、 G で不変な根の関数は有理計算できる、という群 G が存在する」。この文は、定義自体が定理を含み、まるで謎々である。そこで、ガロア群の定義を簡明にし、その定理は後で証明するよう、原著を少し脚色しよう。

因数分解を $F_{S_n}(V)$ から始めると1次式にまで分解できないが、より低次の $F_G(V)$ か

ら始めると分解可能、という場合がある。

そこで、因数分解の開始点を決める“最小の”置換群 G 、という概念を考える。

n 次方程式 $f(x)=0$ の根の式を $V_1=\sum A_j \alpha_j = A_1 \alpha_1 + \cdots + A_n \alpha_n$ 、その根配列を置換した式を V_k と総称する

$F_G(V)=\Pi_G(V-V_k)$ の展開係数が“有理数”になる置換群 G は必ずある。なぜなら、 $G=S_n$ とすれば必ず、 $F_{S_n}(V)$ の係数成分は根の対称式になるから。上のような G が複数あれば、位数が最小の群をガロア群と呼ぶ。

S_n しかないなら、 S_n がガロア群であり、 $F_{S_n}(V)$ は $n!$ 次多項式である。最小の G で作った $F_G(V)=0$ は、 $V=V_1$ という解をもつ有理係数方程式のうちで最低次である。つまり $F_{S_n}(V)$ の因子 $F_G(V)$ は、既約式である

2. 様々な方程式の、ガロア群の実例

問題 1. 係数が任意文字の n 次方程式、 $f(x)=0$ のガロア群は何か？

答 $f(x)$ の係数が任意文字なら、 $F_G(V)=\Pi_G\{V-(A_1\alpha_1+\cdots+A_n\alpha_n)\}$ の係数を構成する根の関数で、有理数になれるのは対称式のみであり、 $G=S_n$ しかない。

したがって $f(x)=0$ のガロア群は、 S_n である。この方程式を解くために因数分解すべき V 多項式は、 $F_{S_n}(V)$ である。

問題 2. 根がみな異なる有理数のとき、この方程式のガロア群は何か？

答 $f(x)=0$ が、すべて有理根をもつ方程式なら、 V_k 自体が有理数なのだから、 $F_G(V)$ の係数を有理数にするための置換の積、 $\Pi_G(V-V_k)$ を、作る必要がない。

$G=\{e\}$ 、 $F_G(V)=V-V_k$ であり、「 $f(x)=0$ のガロア群は $\{e\}$ 」である。

問題 3. $x^4+2x^2-x-2=0$ のガロア群は何か？

答 根を求めてみよう。解法を導く筈の群を考えているのに、その群を知るために根を求めると言ったら変だが、有理根の有無を調べたいのである。

$x^4+2x^2-x-2=(x-1)(x+2)(x^2+x+1)=0$ の根を $\alpha_1=1$ 、 $\alpha_2=-2$ 、 $\alpha_3=\omega$ 、 $\alpha_4=\omega'$ と呼ぶ。 $\omega+\omega'$ 、 $\omega\omega'$ はそれぞれ、 -1 、 1 だから有理数である。

$F_G(V)$ を作るためのガロア群は、 $F_G(V)$ の係数を有理数にする置換群のうち、最小のものだから、今の場合、 S_4 でなく、 ω と ω' の互換からなる群である。

“有理係数の V 多項式を作る目的”にとって、有理根は置換する“必要がない”。

$V_1=A\alpha_1+B\alpha_2+C\alpha_3+D\alpha_4=A-2B+C\omega+D\omega'$ と書く。

4 根はみな V_1 の有理式で表せる： $\alpha_1=V_1/V_1=1$ 、 $\alpha_2=-2\times V_1/V_1=-2$

α_3 と α_4 は、 $C\omega + D\omega' = V_1 - A + 2B$ と、 $\omega + \omega' = -1$ から有理計算できる。
 $G = \{e, (3\ 4)\}$ 、 $V_1(3\ 4) = V'_1$ という置換で、
 $V'_1 = A\alpha_1 + B\alpha_2 + C\alpha_4 + D\alpha_3 = A - 2B + C\omega' + D\omega$ を作って、
 $F_G(V) = (V - V_1)(V - V'_1)$ を作ると、係数が有理数になる。
すなわちガロア群は、 $G = \{e, (3\ 4)\}$ である。

注： $\alpha_1 = \omega$ 、 $\alpha_2 = \omega'$ と名付けたら、 $G = \{e, (1\ 2)\}$ となる。今 4 根は平等でない。
 $x^4 + 2x^2 - x - 2 = 0$ と、 $x^2 + x + 1 = 0$ は、同じガロア群をもつ。
有理根を捨てて残った既約方程式のガロア群が、もとの方程式のガロア群になる。

問題 4. $f(x) = x^4 - 2x^2 + 2 = (x^2 - x + 2)(x^2 + x + 1) = 0$ のように、方程式が
 $\{x^2 - (\alpha_1 + \alpha_2)x + \alpha_1\alpha_2\} \{x^2 - (\alpha_3 + \alpha_4)x + \alpha_3\alpha_4\}$ の形で有理的に分解できるとき、
この方程式のガロア群 G は何か？

答 ガロア群は、既約方程式について定義するのが適切だが（可約方程式のガロア群は、既約方程式のガロア群の合成とみなせる）、関係式 $\alpha_j = \varphi_k(V)$ を導いた方法の前提は、「根がみな異なる」ことだけだったので、まず以下のように考えてみる。

設問の方程式では、基本対称式だけでなく、 $\alpha_1 + \alpha_2$ 、 $\alpha_1\alpha_2$ 、 $\alpha_3 + \alpha_4$ 、 $\alpha_3\alpha_4$ も有理数である。根の関数 $\theta = \theta(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ が、 α_1 、 α_2 の互換で不変なら、 θ の中で α_1 、 α_2 を含む項は α_1 、 α_2 の対称式だから、 $\alpha_1 + \alpha_2$ と $\alpha_1\alpha_2$ の有理式で書ける。 α_3 、 α_4 でも同様。

つまり θ が α_1 、 α_2 の互換 $(1\ 2)$ で不変、かつ α_3 、 α_4 の互換 $(3\ 4)$ で不変なら、 θ は有理数になる。このような θ を係数にもつ $F(V)$ の作り方は前に述べた（65 頁）。

$G = \{e, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$ を使えばよい。

$V_1 = A_1\alpha_1 + A_2\alpha_2 + A_3\alpha_3 + A_4\alpha_4$ を G の元で置換する。

$V_1(1\ 2) = V_{12}$ 、 $V_1(3\ 4) = V_{34}$ 、 $V_1(1\ 2)(3\ 4) = V_{12/34}$ と書いて、

$F_G(V) = (V - V_1)(V - V_{12})(V - V_{34})(V - V_{12/34})$ を作ると、当然 G 対称性だから、

$F_G(V)$ の係数は、 $\alpha_1 + \alpha_2$ 、 $\alpha_1\alpha_2$ 、 $\alpha_3 + \alpha_4$ 、 $\alpha_3\alpha_4$ からなる有理数である。

より小さい群 H で作った $F_H(V)$ が、有理係数でなければ、 G がガロア群である。

例えば、 $H = \{e, (1\ 2)(3\ 4)\}$ が、ガロア群でないことは以下で分かる。

$$\begin{aligned} F_H(V) &= (V - V_1)(V - V_{12/34}) = V^2 - \{(A_1 + A_2)(\alpha_1 + \alpha_2) + (A_3 + A_4)(\alpha_3 + \alpha_4)\} V \\ &\quad + (A_1^2 + A_2^2)\alpha_1\alpha_2 + A_1A_2(\alpha_1^2 + \alpha_2^2) + (A_3^2 + A_4^2)\alpha_3\alpha_4 + A_3A_4(\alpha_3^2 + \alpha_4^2) \\ &\quad + (A_1A_4 + A_2A_3)(\alpha_1\alpha_3 + \alpha_2\alpha_4) + (A_1A_3 + A_2A_4)(\alpha_1\alpha_4 + \alpha_2\alpha_3) \end{aligned}$$

定数項のうち、 $\alpha_1\alpha_3 + \alpha_2\alpha_4$ 、 $\alpha_1\alpha_4 + \alpha_2\alpha_3$ は、 $(1\ 2)$ で非対称、 $(3\ 4)$ でも非対称。

すなわち、 $F_H(V)$ は有理係数式でない。

$H' = \{e, (1\ 2\ 3\ 4), (1\ 2\ 3\ 4)^2, (1\ 2\ 3\ 4)^3\}$ で作った $F_{H'}(V)$ など、色々考えても、有理係数になるのは、 $F_G(V)$ と $F_{S_4}(V)$ しかない。

$F_G(V)$ は有理係数をもつ最低次の多項式（既約式）だから、 G がガロア群である。

本当は、解きたい $f(x)=0$ が可約なら、まず既約方程式に分解すべきである。

$f_1(x)=x^2-(\alpha_1+\alpha_2)x+\alpha_1\alpha_2=0$ のガロア群は、 $G_1=\{e, (1\ 2)\}$ 、

$f_2(x)=x^2-(\alpha_3+\alpha_4)x+\alpha_3\alpha_4=0$ のガロア群は、 $G_2=\{e, (3\ 4)\}$ であり、

$f(x)=f_1(x)f_2(x)$ のガロア群と呼んだ G は、群の直積で、 $G=G_1\times G_2$ と書ける (132 頁)。今、直積の説明を避けるため上記のように言った。

問題 5 $(x^n-1)/(x-1)=x^{n-1}+\cdots+x+1=0$ のガロア群はなにか? (n は素数)

答 この方程式では、任意 1 根で $V_1^*=\alpha_1$ と書き、各根 $=V^*$ の巾乗すなわち整式 $=\psi_j(V^*)$ 、と書ける (61-62 頁)。 $\alpha_k=\psi_j(V^*)$ を保存する群は

$G=\{e, g, \cdots, g^{n-2}\}=\{k \rightarrow a^t k\}$ 、(a は $\text{mod } n$ の原始根; $t=0, 1, \cdots, n-2$)

一方、我々が学んだ方法では、各根を $V_1=A_1\alpha_1+\cdots+A_{n-1}\alpha_{n-1}$ の整式で表して $F_G(V)$ を作り、(その係数が有理数になる場合に) G をガロア群と定義したのだから、まずは $n=5$ を例にとって次のように考えよう。

$(x^5-1)/(x-1)=x^4+x^3+x^2+x+1=0$ の根で、 $V=A\alpha_1+B\alpha_2+C\alpha_3+D\alpha_4$ と書く。

$x^5=1$ の原始根 ω で、 $\alpha_1\sim\alpha_4$ を $\omega, \omega^2, \omega^3, \omega^4$ 、と書き直し、 $G=\{k \rightarrow 2^t k\}$ を使って (2 は $\text{mod } 5$ の原始根)、 $F_G(V)=\Pi_G(V-V_k)$ を書き表すと、

$$F_G(V)=\{V-(A\omega+B\omega^2+C\omega^3+D\omega^4)\}\{V-(A\omega^2+B\omega^4+C\omega+D\omega^3)\} \\ \times \{V-(A\omega^4+B\omega^3+C\omega^2+D\omega)\}\{V-(A\omega^3+B\omega+C\omega^4+D\omega^2)\}$$

展開すれば ω が消え、 $F_G(V)$ の係数が有理数 (G がガロア群) と分かるのだが、計算ミスしそうだし、素数一般 n では計算できない。実は、次節のガロア群の定理を使えば、計算なしで有理係数と分かり、素数 n への一般化も容易である。

3. ガロア群の定理、およびガロア群の縮小

覚え書き： n 次既約方程式 $f(x)=0$ の根を α_j とする。 V_k は根の 1 次式

関係 $\alpha_j=\varphi_j(V_k)$ は置換群 G で保存され、 $\alpha_m=\varphi_j(V')$ に変わる

$F_G(V)=\Pi_G(V-V_k)$ は、 G 対称性の V 多項式

* G が $f(x)=0$ のガロア群、すなわち $F_G(V)$ の係数が既知数 (有理数)

だとする。根の有理関数一般を θ と総称する。ガロア群の定理とは;

i) θ が G で不変なら、 θ は $F_G(V)$ の係数成分から有理計算できる

ii) θ が $F_G(V)$ の係数成分から有理計算できるなら、 θ は G で不変である

$F_G(V)$ が因数分解されていない (既約式の) とき、既知数とは有理数である。

$F_G(V)$ の係数の巾開方値を使って、分解因子 $F_H(V)$ を得た段階では ($G \supset H$)、それら巾開方値も、既知数になっている。

↓

* H が $f(x)=0$ のガロア群になった、つまり $F_H(V)$ の係数が既知数になった
と言い換えると、上の定理 i) ii) は、根の有理関数一般を θ' とし

「 θ' が H で不変 $\longleftrightarrow \theta'$ が $F_H(V)$ の係数から有理計算できる」となる

ガロア群は、有理計算で求まる“根の関数”は何か、を教える役をする
(任意関数 θ が、 G で変化するか否かをみれば、 θ が、 $F_G(V)$ の係数成分の関数から
有理計算できるか否かが分かる)。

因数分解が進む過程を、「ガロア群の縮小」、「計算対象の拡大；根の関数の或る巾開
方量が既知数になる」という概念で理解しよう。

i) の証明

n 根からなる根の関数一般を、 $\theta = \theta(\alpha_1, \alpha_2, \dots, \alpha_n)$ と書く。

すでに存在を証明した関係式、 $\alpha_k = \phi_k(V_1) = \phi_k(A_1\alpha_1 + \dots + A_n\alpha_n)$ を代入すると、
 $\theta = \theta(\alpha_1, \dots, \alpha_n) = \theta[\phi_1(V_1), \phi_2(V_1), \dots, \phi_n(V_1)] = \Theta(V_1)$ 、と V_1 の整式で書ける。

V_1 は、 G の元 g_k で、 $V_1 g_k = V_k$ に変わる。

定理が言うように“ θ が G で不変”なら、 $\theta = \theta g_k = \Theta(V_1) g_k = \Theta(V_k)$

すなわち、 $\theta = \Theta(V_1) = \Theta(V_2) = \dots = \Theta(V_m)$ である (m は G の位数)。

上記は、 $\Theta(V_k)$ という関数が、 $V_1 \sim V_m$ の任意入れ替えで不変なことを意味する。

すると、 $\Theta(V_k)$ は、 $V_1 \sim V_m$ の対称式でも書ける (書き直せる) と分かる。

分かりにくければ、 $\theta = 1/m \{\Theta(V_1) + \Theta(V_2) + \dots + \Theta(V_m)\}$ と思えばよい。

したがって $V_1 \sim V_m$ の基本対称式、つまり $F_G(V)$ の係数成分で表せる。

ガロア群 G の定義により、 $F_G(V)$ の係数は“既知数”だから、証明された。

ii) の証明

θ が $F_G(V)$ の係数 (既知数) から有理計算できるなら、その値を既知数 q と呼び、
 $\theta(\alpha_1, \alpha_2, \dots, \alpha_n) = q$ と書ける。 q の値は、我々の計算対象に入っている (解法の初
段階で q は有理数だが、解法が進むと、或る巾開方値を追加した数となる)。

$\alpha_k = \phi_k(V_1)$ を代入し、 $\theta = \theta\{\phi_1(V_1), \phi_2(V_1), \dots, \phi_n(V_1)\} = \Theta(V_1) = q$ と書けば、

V の方程式 $\Theta(V) - q = 0$ が、 $V = V_1$ を解にもつ、と読み直せる。

一方、 V_1 は、 $F_G(V)$ の定義 $F_G(V) = \Pi_G(V - V_k)$ により、 $F_G(V) = 0$ の解である。

$F_G(V)$ は、ガロア群の定義 (係数が有理数になる最小の群) により、(今の計算対象
の範囲内で) 既約式である。このことが非常に重要である。

すると「 V の方程式 $\Theta(V) - q = 0$ と、既約方程式 $F_G(V) = 0$ が、解 V_1 を共有する」
のだから、 V 多項式 $\Theta(V) - q$ は、 $F_G(V)$ で割り切れる (1章；互除法の定理)。

(互除法で、共通根 V_1 が求まるのではないことに注意しよう)

すると $F_G(V)=0$ の解 $V_1 \sim V_m$ はすべて、 $\Theta(V)-q=0$ の解にもなると分かる。

したがって、 $\Theta(V_1)=\Theta(V_2)=\cdots=\Theta(V_m)=q$

つまり、 $\theta(\alpha_1, \alpha_2, \cdots, \alpha_n)=\Theta(V_1)$ は、 $V_1 \sim V_m$ どちらの任意の入れ替えで不変、すなわち G で不変 (G 対称式) である。

ガロア群の定理は、 $f(x)=0$ の根から、 $F(V)=0$ の解 V への、議論の置き換えであり、“ $\alpha_1 \sim \alpha_n$ の基本対称式”を、 $F_{S_n}(V)$ における “ $V_1 \sim V_n$ の基本対称式” に置き換え、さらに $F_G(V)$ における “ $V_1 \sim V_m$ の基本対称式” という概念に広げ、 $\alpha_1 \sim \alpha_n$ の非対称関数も扱えるようにした。

$(V-V_1)\cdots(V-V_m)=F_G(V)$ の創作が、有理計算できる非対称関数を知る方法論の要点である。本論に進む前に、前節の宿題を解こう (上記定理の理解にも役立つ)。

“ガロア群の定理”を応用すると、68 頁、問題 5 が解決する。

$(x^n-1)/(x-1)=0$ を、 $n=5$ で例示するが、素数 n 一般でも証明は同じである。

問題 $x^4+x^3+x^2+x+1=0$ の根を $\alpha_1 \sim \alpha_4$ 、 $V_1=A\alpha_1+B\alpha_2+C\alpha_3+D\alpha_4$ 、とする。

$G=\{g:k \rightarrow 2^S k\}$ で V_1 を置換し、 $V_1 g=V_2$ 、 $V_1 g^2=V_3$ 、 $V_1 g^3=V_4$ と書く。

mod 5 で計算し (51 頁参照)、 $V_2=A\alpha_2+B\alpha_4+C\alpha_1+D\alpha_3$ 、

$V_3=A\alpha_4+B\alpha_3+C\alpha_2+D\alpha_1$ 、 $V_4=A\alpha_3+B\alpha_1+C\alpha_4+D\alpha_2$

$F_G(V)=\Pi_G(V-V_i)$ を作ると、これは S_4 対称式ではないから、展開係数は A, B, C, D と $\alpha_1 \sim \alpha_4$ の非対称式を含む。にも拘わらず；

$F_G(V)$ の係数が、有理数になることを証明せよ。

すなわち、上の方程式のガロア群が G だと証明したい。

ヒント： $F_G(V)$ の係数が含む“根の諸関数”を、 $\theta=\theta(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ と総称すれば、 θ は、 $F_G(V)$ の作り方からして当然 G 対称性である。ここで、全根が任意 1 根の有理式で表せるといふ、方程式 $x^4+x^3+x^2+x+1=0$ の特徴から、 $\alpha_k=\omega^k$ と書き直し、 G の元を作用させると、 α_k は、 $\alpha_1 \sim \alpha_4$ のどれかに移り変わる。これを利用して、ガロア群の定理の証明法を真似ればよい。

答 α_k = “ α_1 の巾乗” と書けるから、 $\theta=\theta(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ は、 α_1 の多項式の形で、 $\theta=\Theta(\alpha_1)$ 、と書ける。 $\Theta(\alpha_1)$ を G の元で置換すると、 $\Theta(\alpha_2)$ 、 $\Theta(\alpha_4)$ 、 $\Theta(\alpha_3)$ 、 $\Theta(\alpha_1)$ になるが、 θ は G で不変だから、 $\theta=\Theta(\alpha_1)=\Theta(\alpha_2)=\Theta(\alpha_3)=\Theta(\alpha_4)$ である。すると θ は、 $\alpha_1 \sim \alpha_4$ 相互の入れ替えで不変だから、実は $\alpha_1 \sim \alpha_4$ の対称式にも書き直せる。したがって、 $\alpha_1 \sim \alpha_4$ の基本対称式で書ける。 $\alpha_1 \sim \alpha_4$ は、 $x^4+x^3+x^2+x+1=0$ の根なのだから、基本対称式 $=\pm 1$ 、つまり θ は有理数、したがって $F_G(V)$ の係数は有理数と証明された。

68 頁問題 5 の答のように、 ω の式を直接計算する必要はなかった。

4. 方程式が解ける過程の、ガロアによる説明； $F_G(V)$ の因数分解

$F_{Sn}(V) = 0$ を、1 次式の積にまで因数分解することが、 n 次方程式の解法に等しい。

因数分解の出発点は、一般に $F_G(V)$ 、任意文字係数方程式では、 $F_{Sn}(V)$ だった。

$F_G(V) = (V - V_1) \cdots (V - V_m) = 0$ に分解されて、 $V = V_1$ と求まれば、 $\alpha_j = \varphi_j(V_1)$ から全根が得られる（求まる原理を言っており、実際に計算するのではない）。

$F_G(V)$ の役割は、因数分解するために求めるべき“根の非対称関数”が、どんな形のものを示すことである。巾開方を含む“実際の計算手順”は、後で（ガロアの驚くべきアイデアで）明らかになるから、まず $F_G(V)$ の因数分解をイメージしよう。

2 次方程式の例を見ると、

$$F_{S2}(V) = V^2 - (A + B)(\alpha + \beta)V + (A^2 + B^2)\alpha\beta + AB(\alpha^2 + \beta^2)$$

の係数成分の対称関数「 $\alpha + \beta$ 、 $\alpha\beta$ 、 $\alpha^2 + \beta^2$ 」から、非対称関数

$\alpha - \beta = \sqrt{(\alpha + \beta)^2 - 4\alpha\beta}$ を計算すれば、 α 、 β を得たことになるので、

$F_{S2}(V) = \{V - (A\alpha + B\beta)\}\{V - (A\beta + B\alpha)\}$ のように、「次に求まる非対称関数」

が「 α 、 β 」であることが、 A 、 B の存在により分離されて目に見える。

$F_G(V)$ を因数分解するために追加される計算値つまり、非対称関数を“巾開方を用いて書いた値”を、ガロアに倣って、 $r, r', r'', \dots$ と（総称的に）書く。

$r, r', r'', \dots$ が計算可能なら、 $F_G(V) = F(V, r)F(V, r')F(V, r'') \cdots$ に分解される。

上記 2 次方程式なら、 $A\alpha + B\beta = (A + B)(\alpha + \beta)/2 + (A - B)(\alpha - \beta)/2$

の中の非対称式が、 $r = (A - B)(\alpha - \beta)/2 = (A - B)\sqrt{(\alpha + \beta)^2 - 4\alpha\beta}/2$ であり、

$A\beta + B\alpha$ の中では、 $r' = (A - B)(\beta - \alpha)/2 = (B - A)\sqrt{(\alpha + \beta)^2 - 4\alpha\beta}/2$

$F(V, r)$ は、縮小したガロア群 H で不変である。次は、 $F(V, r)$ の因数分解が課題になる（ $F(V, r')$ 、 $F(V, r'')$ 、 $\dots$ の分解は不要）。 $F(V, r) = F(V, r, r_1)F(V, r, r_2) \cdots$ と分解し、さらに $F(V, r, r_1) = F(V, r, r_1, r_a)F(V, r, r_1, r_b) \cdots$ と分解し、遂にガロア群が $\{e\}$ に縮小して、 $F(V, r, r_1, r_a, \dots) = 1$ 次式 $V - V_1$ となれば、ゴールである。その時点で、 $V_1 = A_1\alpha_1 + \cdots + A_n\alpha_n$ は、巾開方計算が積み重なった値、 $r, r_1, r_a, \dots$ で書かれている。今は計算法でなく、因数分解の各段階で求めるべき非対称関数だけを考えればよい。

5. 3 次方程式の解法における、計算対象の拡大とガロア群の縮小

1) S_3 対称性の関数から、 A_3 対称性の関数を分離すること

任意文字係数の 3 次方程式 $x^3 + ax^2 + bx + c = 0$ の根から $V_1 = A\alpha_1 + B\alpha_2 + C\alpha_3$ を作る。この方程式のガロア群は、今の時点で S_3 である。

$F_G(V) = \Pi_G(V - V_k) = V^m - (V_1 + \cdots + V_m)V^{m-1} + \cdots$ の展開係数が有理数になるに

は、 $\alpha_1 \sim \alpha_3$ の基本対称式が必要だから、 V_1 を $3!$ とおりに置換しなければならない。

S_3 の部分群を、解法段階ごとに分類する。3 章 46-47 頁の内容が、 $F(V)$ の因数分解という言葉に翻訳される。置換元は、根 $\alpha_1, \alpha_2, \alpha_3$ の添え字 1, 2, 3 で表記する。

$$S_3 = \{A_3, A_3 (1\ 2)\}$$

$$A_3 = \{e, (1\ 2)(1\ 3), (1\ 3)(1\ 2)\} \quad \cdots \text{交代群が}$$

$$= \{e, (1\ 2\ 3), (1\ 2\ 3)^2\} = H \quad \text{巡回群でもある (3 文字置換の特徴)}$$

添え字数列			添え字数列		
$\mathbf{V_1e}$	$= \mathbf{V_1 = A\alpha_1 + B\alpha_2 + C\alpha_3}$	1, 2, 3	$\mathbf{V_1(1\ 2) = V_4 = A\alpha_2 + B\alpha_1 + C\alpha_3}$		2, 1, 3
$\mathbf{V_1(1\ 2\ 3)}$	$= \mathbf{V_2 = A\alpha_2 + B\alpha_3 + C\alpha_1}$	2, 3, 1	$\mathbf{V_2(1\ 2) = V_5 = A\alpha_1 + B\alpha_3 + C\alpha_2}$		1, 3, 2
$\mathbf{V_1(1\ 2\ 3)^2}$	$= \mathbf{V_3 = A\alpha_3 + B\alpha_1 + C\alpha_2}$	3, 1, 2	$\mathbf{V_3(1\ 2) = V_6 = A\alpha_3 + B\alpha_2 + C\alpha_1}$		3, 2, 1

V_1 を $(1\ 2\ 3)$ で置換すると V_2 になり、さらに $(1\ 2\ 3)$ で置換すると V_3 になる。

V_1, V_2, V_3 を、それぞれ $(1\ 2)$ で置換すると、 V_4, V_5, V_6 になる。

$F_{S_3}(V) = \Pi_{S_3}(V - V_k)$ を展開した 6 次式の係数は、 $V_1 \sim V_6$ の対称式である。

例えば V^5 の係数は、 $V_1 + V_2 + V_3 + V_4 + V_5 + V_6 = 2(A + B + C)(\alpha_1 + \alpha_2 + \alpha_3)$ である。

一般に、因数分解に必要な“根の関数”はすべて、定数項の中に埋蔵されている。

$F_{S_3}(V)$ の因数分解が、どのように実現するかを調べる。

$$= \{V^3 - (V_1 + V_2 + V_3)V^2 + (V_1V_2 + V_2V_3 + V_3V_1)V - V_1V_2V_3\} \leftarrow A_3 \text{ 対称性の因子}$$

$$\times \{V^3 - (V_4 + V_5 + V_6)V^2 + (V_4V_5 + V_5V_6 + V_6V_4)V - V_4V_5V_6\} \leftarrow \text{第一の } \{ \} \text{ を} \\ (1\ 2) \text{ で置換したもの}$$

$$V_1V_2V_3(1\ 2) = V_4V_5V_6 \text{ など}$$

第 1 の $\{V \text{ の } 3 \text{ 次式}\}$ の係数は、

$$V_1 + V_2 + V_3 = (A + B + C)(\alpha_1 + \alpha_2 + \alpha_3)$$

$$V_1V_2 + V_2V_3 + V_3V_1 = (A^2 + B^2 + C^2)(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1)$$

$$+ (AB + BC + CA)(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1) + (AB + BC + CA)(\alpha_1^2 + \alpha_2^2 + \alpha_3^2)$$

$$V_1V_2V_3 = (A^3 + B^3 + C^3 + 3ABC)\alpha_1\alpha_2\alpha_3 + ABC(\alpha_1^3 + \alpha_2^3 + \alpha_3^3)$$

$$+ (A^2B + B^2C + C^2A)(\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1) + (AB^2 + BC^2 + CA^2)(\alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2)$$

すなわち、 $V_1V_2V_3 = \text{対称式} + \text{非対称式} = \text{有理数} + \mathbf{r}$ (巾開方を含む値)

第 2 の $\{V \text{ の } 3 \text{ 次式}\}$ では、定数項だけが第 1 式と異なる ($V_4V_5V_6$ と $V_1V_2V_3$ が、やや異なる)。 $V_4V_5V_6 = \text{対称式 (有理数)} + \mathbf{r}'$ と書いて、

$$\mathbf{r}' = (A^2B + B^2C + C^2A)(\alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2) + (AB^2 + BC^2 + CA^2)(\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1),$$

$\mathbf{r}' = \mathbf{r} (1\ 2) = \mathbf{r} (2\ 3) = \mathbf{r} (1\ 3)$ である。

$V_1 V_2 V_3 V_4 V_5 V_6$ を、 $V_1 V_2 V_3$ と $V_4 V_5 V_6$ に分解して、 $F_{S_3}(V) = F(V, \mathbf{r}) F(V, \mathbf{r}')$ を実現するには、非対称関数 $\alpha_1 \alpha_2^2 + \alpha_2 \alpha_3^2 + \alpha_3 \alpha_1^2$ と $\alpha_1^2 \alpha_2 + \alpha_2^2 \alpha_3 + \alpha_3^2 \alpha_1$ を求めればよい(対称式の巾開方形で書ければよい)、と分かった。

$F(V, \mathbf{r})$ 、 $F(V, \mathbf{r}')$ が、非対称関数を目に見えるように分離しているのも分かった(実際に計算したいのは、 $A_1 \sim A_n$ が混入した $\mathbf{r}$ 、 $\mathbf{r}'$ 、 $\dots$ でなく、 $\alpha_1 \alpha_2^2 + \alpha_2 \alpha_3^2 + \alpha_3 \alpha_1^2$ のような成分、つまり根の非対称関数である)。

$V_1 = A_1 \alpha_1 + \dots + A_n \alpha_n$ の置換を掛け合わせると、様々な根の関数が、 $A_1 \sim A_n$ の式に付き添われて出現する、その様子は美しい(欧州で社交界デビューする令嬢を、然るべきグループに案内する人々はシャペロンと呼ばれ、自分達はグループに立ち入らないそうである。 $A_1 \sim A_n$ は、群がる $\alpha_1 \sim \alpha_n$ を様々な小グループに導き、最後に独り立ちさせる。方程式のことを一日中考えていると舞踏会の夢を見るかもしれない)。

上記の計算は、次のような指針に立っている。

$F_{S_3}(V) = \{V \text{ の } 3 \text{ 次式}\} \{V \text{ の } 3 \text{ 次式}\}$ という因数分解に、 $S_3 = \{A_3, A_3 (1\ 2)\}$ という剰余類分割が対応する。この因数分解は、 A_3 対称な根の関数を、 $(1\ 2)$ で置換した関数と組み合わせて S_3 対称にすれば、実現する。

2) 補足：n 根の差積という用語

S_n は互換だけの積で書けるので、 A_n 対称関数(任意の偶置換で不変な関数)は任意置換で「不変、または符号だけ変化」のいずれかになる。

A_n 対称の最も簡単な式は“差積”と呼ばれ、任意の互換(奇置換)で符号が変わる。 V が満たす方程式を分解するときに、第一段階で求まる“根の非対称関数”である。

2 次方程式の根の差積は、 $\alpha - \beta$

3 次方程式では、 $(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$

4 次方程式では $(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)(\alpha_2 - \alpha_4)(\alpha_3 - \alpha_4)$

n 次方程式では $\prod_{i < j} (\alpha_i - \alpha_j)$

差積はすべて、2 乗すれば対称式になるから、 $\sqrt{\text{(対称式)}}$ の形で求まる。

$S_n = \{A_n, A_n (1\ 2)\}$ あるいは $\{A_n, A_n (\text{任意奇置換})\}$ に対応して、常に因数分解 $F_{S_n}(V) = \{V \text{ の } n!/2 \text{ 次多項式}\} \times \{V \text{ の } n!/2 \text{ 次多項式}\}$ が実現する。

任意文字係数の n 次方程式のガロア群は、 S_n である。差積を追加した計算対象の中では、 S_n 対称関数が、有理的に A_n 対称関数に因数分解できる。

すなわち、 S_n から A_n への「ガロア群の縮小」は必ず実現する。

3 次方程式の話に戻る（以下の式を是非、筆算するとよい。理解に役立つ）。

前述の非対称関数を、 $\alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2 = \varphi$ 、 $\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1 = \varphi'$ と書く。

$\varphi - \varphi'$ を計算して整理すると、 $=(\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)$ 、差積になる！

$\varphi + \varphi' = (\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1)(\alpha_1 + \alpha_2 + \alpha_3) - 3\alpha_1\alpha_2\alpha_3$ 、（計算なしでも対称式と分かる）

$\varphi + \varphi'$ が既知数だから、 $\varphi - \varphi' = \text{差積}$ が求まれば、 φ 、 φ' が求まる。

$$\begin{aligned} & \text{差積の 2 乗 } \{(\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)\}^2 = (\varphi - \varphi')^2 \\ & = (\alpha_1^2\alpha_2^2 + \alpha_2^2\alpha_3^2 + \alpha_3^2\alpha_1^2)(\alpha_1^2 + \alpha_2^2 + \alpha_3^2) - 3\alpha_1^2\alpha_2^2\alpha_3^2 \\ & \quad - 2\alpha_1\alpha_2\alpha_3(\alpha_1^3 + \alpha_2^3 + \alpha_3^3) - 2(\alpha_1^3\alpha_2^3 + \alpha_2^3\alpha_3^3 + \alpha_3^3\alpha_1^3) \\ & = \text{対称式 (既知数)} \quad (\varphi - \varphi')^2 \text{ が求まった} \end{aligned}$$

【2 章の計算と本章の、方法論の比較】

2 章の計算法では、以下のような根の関数を求める必要が生じた。

$$\begin{aligned} \theta^3 &= (\alpha + \omega\beta + \omega^2\gamma)^3 \\ &= \alpha^3 + \beta^3 + \gamma^3 + 6\alpha\beta\gamma + 3\omega(\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha) + 3\omega^2(\alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2) \\ \theta^3 &= (\alpha + \omega^2\beta + \omega\gamma)^3 \\ &= \alpha^3 + \beta^3 + \gamma^3 + 6\alpha\beta\gamma + 3\omega(\alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2) + 3\omega^2(\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha) \end{aligned}$$

本章 F (V) では、上の下線部が、 $\sqrt{(\alpha, \beta, \gamma \text{ の 6 次対称式})}$ で表せると分かったので、因数分解が一段実現すると理解し、下記の関数から構成される分解因子になる、と解釈する（巾開方形は書かずに済みます）。定数項には $(AB^2 + BC^2 + CA^2)(\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha)$ と $(A^2B + B^2C + C^2A)(\alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2)$ 、他の項には、 $(A, B, C \text{ の 1} \sim 3 \text{ 次対称式}) \times (\alpha, \beta, \gamma \text{ の 1} \sim 3 \text{ 次対称式})$ が現れる。

3) 3 次方程式を解く次の段階

$$V^3 - (V_1 + V_2 + V_3)V^2 + (V_1V_2 + V_2V_3 + V_3V_1)V - V_1V_2V_3 \quad \cdots \star$$

を因数分解することになる。この係数は、 φ 、 φ' 、および有理数からなる（計算対象に、 φ 、 φ' を追加したから、因子 $\star$ が分離抽出された）。

$\star$ は、 $H = \{e, (1\ 2\ 3), (1\ 2\ 3)^2\}$ で対称な多項式である。

$\star$ を因数分解するために、 $V_1V_2V_3$ から V_1 、 V_2 、 V_3 を分離したい。

$$\begin{aligned} V_1(1\ 2\ 3) &= V_2, \quad V_1(1\ 2\ 3)^2 = V_3 \text{ を利用して } H \text{ 対称性の } (V_1 + \omega V_2 + \omega^2 V_3)^3 \\ &\text{を作り } (\omega^3 = 1)、3 \text{ 次巾開方をとれば、} V_1, V_2, V_3 \text{ が得られるが、実際は、} \\ &\text{下記のように考えるのが合理的である。} \end{aligned}$$

$\star$ の因数分解は、 $V - V_1$ 、 $V - V_2$ 、 $V - V_3$ それぞれを求めることだから、 $V - V_1$ を求めればよく、すなわち V_1 の構成要素である α 、 α_2 、 α_3 自体を求めればよい。

$(V_1V_2V_3V_4V_5V_6)$ から、 $V_1V_2V_3$ と $V_4V_5V_6$ を得るときも同様に、構成要素の

$\alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2$ と $\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1$ を求めればよかった)

α_1 、 α_2 、 α_3 の 1 次式が、求めるべき関数形だから、 $\alpha_1 + \omega \alpha_2 + \omega^2 \alpha_3$ を扱う計算が現れる（この形は、 $F(V)$ が教えてくれるわけではなく、後述する“分解因子の計算法”から知られる。 $F(V)$ の分解過程で、3 次式を、1 次式 3 つの積に分解するとき、1 の 3 乗根 ω 、 ω^2 の出現を伴うのである）。

【2 章と本章の、方法論の比較】

2 章では、以下 3 種類の根の関数を求める必要が（出発点で）生じた。

$$\theta = \alpha + \omega \beta + \omega^2 \gamma, \theta' = \alpha + \omega' \beta + \omega'^2 \gamma, \theta'' = \alpha + \omega'' \beta + \omega''^2 \gamma$$

（ただし θ 、 θ' 、 θ'' のうち 1 つは、 $\alpha + \beta + \gamma =$ 既知数であった）

$F(V)$ の因数分解では、最後の段階で上式に相当する因子が（見かけは違うが）、 $A\alpha + B\beta + C\gamma$ 、 $A\beta + B\gamma + C\alpha$ 、 $A\gamma + B\alpha + C\beta$ になる。 $F(V)$ がこれら 1 次式まで分解されるのは、根の対称式の巾開方形で“ θ 、 θ' 、 θ'' ”を表せたとき”、すなわち“ α 、 β 、 γ が有理計算できるとき”である。

V の 1 次式にまで分解できたときがゴール、すなわち、 V_1 、 V_2 、 V_3 を基本対称式で表せたときである。ガロア群は、 $S_3 \rightarrow A_3 = H \rightarrow \{e\}$ と縮小した。

6. 4 次方程式の解法における、計算対象の拡大とガロア群の縮小

1) 4 次方程式のガロア群が、剰余類分割されていく過程

2 章で 4 次方程式を解くとき、根の関数の対称性を試行錯誤で高めた。現れた根の諸関数は、下記それぞれの群で対称なものだった（48 頁）。前節と同様、2 章で実行した解法を逆向きに辿り、 $F_{S_4}(V)$ の因数分解を考える。

4 次方程式は素数次でない。その特殊性は、下記 H 、 H' が巡回群でないことに現れている。ガロア群は、 $S_4 \rightarrow A_4 \rightarrow H' \rightarrow H \rightarrow \{e\}$ と縮小する。

$$S_4 = \{A_4, A_4(1\ 2)\}$$

$$A_4 = \{H', H'(2\ 3\ 4), H(2\ 3\ 4)^2\}$$

$$H' = \{H, H(1\ 3)(2\ 4)\} = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

$$H = \{e, (1\ 2)(3\ 4)\}$$

2) $F_{S_4}(V)$ の因数分解過程

$V_1 \sim V_{24}$ は、 $V_1 = A_1\alpha_1 + A_2\alpha_2 + A_3\alpha_3 + A_4\alpha_4$ に対し、下記のような群対称性をもつように、4 根 $\alpha_1 \sim \alpha_4$ の配列を置換したものとする。

V_1 を偶置換したものを $V_1 \sim V_{12}$ 、

V_1 を奇置換したものを $V_{13} \sim V_{24}$ 、と命名しよう。

$$(1) \quad F_{S_4}(V) = \{V^{12} - (V_1 + V_2 + \dots + V_{12})V^{11} + \dots\} \leftarrow A_4 \text{ 対称性の因子} \\ \times \{V^{12} - (V_{13} + V_{14} + \dots)V^{11} + \dots\} \leftarrow \text{上の } \{ \} \text{ を任意互換したもの}$$

差積 $(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)(\alpha_2 - \alpha_4)(\alpha_3 - \alpha_4) = \psi - \psi'$ と書くと、 $\{ \}$ 内に ψ, ψ' がみつかり、 $\psi + \psi' =$ 対称式、 $\psi - \psi' = \sqrt{\text{対称式}}$ から、 ψ, ψ' が求まって $F_{S4}(V) = F(V, r_1) F(V, r_2)$ と分解できる、と想像すればよい。

r_1, r_2 は、非対称関数であり、 $\sqrt{\text{対称式}}$ を含む有理式でも表せる (2 次方程式とのアナロジーでいえば、 $A\alpha + B\beta, B\alpha + A\beta$ は、 $\sqrt{(\alpha + \beta)^2 - 4\alpha\beta}$ を使って表せる)。

4 次方程式の (差積)² を計算する気になれないのは、30 頁で述べたことと同様だが、 $F_{S4}(V) = \{V \text{ の 12 次式} \} \{V \text{ の 12 次式} \}$ は必ず実現し、5 次方程式なら、 $F_{S5}(V) = \{V \text{ の 60 次式} \} \{V \text{ の 60 次式} \}$ が実現する。

次は、 A_4 対称式 $F(V, r_1)$ だけを分解すればよい。最後に V の値を 1 つ得れば、全根 $\alpha_1 \sim \alpha_4$ を得るから、どの分解段階でも分解因子のうち 1 つだけをみればよい。

A_4 対称関数の中に含まれる、 H' 対称関数に注目する (前頁)。

$$H' = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

$$\begin{aligned} (2) \quad F(V, r_1) &= \{V^{12} - (V_1 + V_2 + \cdots + V_{12}) V^{11} + \cdots\} \leftarrow A_4 \text{ 対称性} \\ &= \{V^4 - (V_1 + V_2 + V_3 + V_4) V^3 + \cdots\} \leftarrow H' \text{ 対称性の因子} \\ &\quad \times \{V^4 - (V_5 + \cdots) V^3 + \cdots\} \leftarrow \text{第一の } \{ \} \text{ を } (2\ 3\ 4) \text{ で置換したもの} \\ &\quad \times \{V^4 - (V_9 + \cdots) V^3 + \cdots\} \leftarrow \text{第一の } \{ \} \text{ を } (2\ 3\ 4)^2 \text{ で置換したもの} \\ &= F'(V, r_3) F'(V, r_4) F'(V, r_5) \quad <\text{注: } F' \text{ は微分の意味ではない}> \end{aligned}$$

r_3, r_4, r_5 は、この段階で求めた非対称関数を含む式である。それらを構成する成分 $\alpha_1\alpha_2 + \alpha_3\alpha_4, \alpha_1\alpha_3 + \alpha_4\alpha_2, \alpha_1\alpha_4 + \alpha_2\alpha_3$ は、30 頁では下記 Θ, Θ' から得ようとした。

$$\Theta = (\alpha_1\alpha_2 + \alpha_3\alpha_4) + \omega(\alpha_1\alpha_3 + \alpha_4\alpha_2) + \omega^2(\alpha_1\alpha_4 + \alpha_2\alpha_3) \quad \omega^3 = 1$$

$$\Theta' = (\alpha_1\alpha_2 + \alpha_3\alpha_4) + \omega^2(\alpha_1\alpha_3 + \alpha_4\alpha_2) + \omega(\alpha_1\alpha_4 + \alpha_2\alpha_3)$$

および、 $\alpha_1\alpha_2 + \alpha_3\alpha_4 + \alpha_1\alpha_3 + \alpha_4\alpha_2 + \alpha_1\alpha_4 + \alpha_2\alpha_3 =$ 基本対称式

今、 Θ^3, Θ'^3 は (1) で得た $\sqrt{\text{対称式}}$ を含む既知数であり、 Θ, Θ' ないし r_3, r_4, r_5 は $\sqrt[3]{\sqrt{\text{対称式}}}$ (有理数) を含む形の既知数になっている (と思うだけでよい)。

$$\begin{aligned} (3) \quad F'(V, r_3) &= \{V^4 - (V_1 + V_2 + V_3 + V_4) V^3 + \cdots\} \leftarrow H' \text{ 対称性} \\ H' &= \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \end{aligned}$$

文字数も減ったので、ここで V 多項式の具体形を見てみる。

$$V_1 = A_1\alpha_1 + A_2\alpha_2 + A_3\alpha_3 + A_4\alpha_4$$

$$V_2 = V_1(1\ 2)(3\ 4), V_3 = V_1(1\ 3)(2\ 4), V_4 = V_1(1\ 4)(2\ 3) \quad \text{と書く。}$$

前記 (2) では、 $\alpha_1\alpha_2 + \alpha_3\alpha_4, \alpha_1\alpha_3 + \alpha_4\alpha_2, \alpha_1\alpha_4 + \alpha_2\alpha_3$ が求まった (計算対象に追加された) から、12 次式が因数分解され、 $V^4 - (V_1 + V_2 + V_3 + V_4) V^3 + \cdots + V_1V_2V_3V_4$ が抽出されたのである。

今の課題は、 $\{V^2 - (V_1 + V_2) V + V_1V_2\} \{V^2 - (V_3 + V_4) V + V_3V_4\}$ への因数分解である。

つまり、 H' の正規部分群 $H = \{e, (1\ 2)(3\ 4)\}$ で不変な関数を使って、係数を書く。
 $\sqrt{\{\text{対称式} + 4(\alpha_1\alpha_2 + \alpha_3\alpha_4)\}}$ 、 $\sqrt{\{\text{対称式} + 4(\alpha_1\alpha_3 + \alpha_4\alpha_2)\}}$ 、 $\sqrt{\{\text{対称式} + 4(\alpha_1\alpha_4 + \alpha_2\alpha_3)\}}$
 を使って「 $\alpha_1 + \alpha_2, \alpha_3 + \alpha_4, \alpha_1\alpha_2, \alpha_3\alpha_4$ 」、 $\alpha_1 + \alpha_3, \alpha_2 + \alpha_4, \alpha_1\alpha_3, \alpha_2\alpha_4$ 、 $\alpha_1 + \alpha_4, \alpha_2 + \alpha_3,$
 $\alpha_1\alpha_4, \alpha_2\alpha_3$ 」 $\cdots (A)$
 が書き表され (29 頁参照)、計算対象に追加されたことになる。

$$\begin{aligned} & V^2 - (V_1 + V_2)V + V_1V_2 \quad \cdots (B) \quad \text{の係数の全体像は} \\ & = V^2 - \{(A_1 + A_2)(\alpha_1 + \alpha_2) + (A_3 + A_4)(\alpha_3 + \alpha_4)\}V \\ & \quad + A_1A_2(\alpha_1^2 + \alpha_2^2) + A_3A_4(\alpha_3^2 + \alpha_4^2) + (A_1^2 + A_2^2)\alpha_1\alpha_2 + (A_1A_4 + A_2A_3)\alpha_1\alpha_3 \\ & \quad + (A_1A_3 + A_2A_4)\alpha_1\alpha_4 + (A_2A_4 + A_1A_3)\alpha_2\alpha_3 + (A_2A_3 + A_1A_4)\alpha_2\alpha_4 + (A_3^2 + A_4^2)\alpha_3\alpha_4 \end{aligned}$$

(A) の様々な非対称関数が計算対象に含まれるから (今その値を巾根形で書くのは略しているのだが)、(B) の係数が書けた、すなわち因子 (B) が抽出されたことになる。
 $V^2 - (V_3 + V_4)V + V_3V_4$ も同様に得られる。

$$\begin{aligned} & \text{まとめると、}\{V^2 - (V_1 + V_2)V + V_1V_2\} \leftarrow H \text{ 対称性の因子} \\ & \quad \times \{V^2 - (V_3 + V_4)V + V_3V_4\} \leftarrow \text{上記を } (1\ 3)(2\ 4) \text{ で置換したもの} \\ & = F''(V, r_6)F''(V, r_7) \end{aligned}$$

r_6, r_7 は、 $\sqrt{(\alpha_1\alpha_2 + \alpha_3\alpha_4 + \text{有理数})}$ 、 $\sqrt{(\alpha_1\alpha_3 + \alpha_4\alpha_2 + \text{有理数})}$ 、 $\sqrt{(\alpha_1\alpha_4 + \alpha_2\alpha_3 + \text{有理数})}$
 を含む形で書かれる値を意味するから $\sqrt[3]{\sqrt{\sqrt{\text{有理数}}}}$ の形を含んだ数である。

$$\begin{aligned} (4) \quad & F''(V, r_6) = \{V^2 - (V_1 + V_2)V + V_1V_2\} \\ & = (V - V_1)(V - V_2) \text{ の分解が実現する } \leftarrow \{e\} \text{ 対称性} \\ & = \{V - (A_1\alpha_1 + A_2\alpha_2 + A_3\alpha_3 + A_4\alpha_4)\}\{V - (A_1\alpha_2 + A_2\alpha_1 + A_3\alpha_4 + A_4\alpha_3)\} \end{aligned}$$

$\sqrt[3]{\sqrt{\sqrt{\text{有理数}}}}$ を含む “ $\alpha_1 + \alpha_2, \alpha_3 + \alpha_4, \alpha_1\alpha_2, \alpha_3\alpha_4$ ” が (3) で得られたので、これら
 4 つに対し $\sqrt{}$ をとる計算を行なえば、 $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ が得られ、 V 多項式の因数分解
 が 1 次式に達する。各根は、 $\sqrt{\sqrt[3]{\sqrt{\sqrt{\text{有理数}}}}}$ の形を含む。

V_1 を得たから $\varphi_k(V_1)$ を計算して $\alpha_k = \varphi_k(V_1)$ を得る、のではなく、 $(V - V_1)$
 にまで分離したことが、各根を得たことである (φ_k の関数形は詮索しない)。

繰り返し述べたように $F(V)$ は、「因数分解を実現するために必要な非対称関数は
 何か」を教える役をするだけである。一般的な計算法は次の §3 で知られる。

以上のように、 $F_G(V) = \prod_G (V - V_k)$ のアイデアは、右辺の展開式を因数分解す
 るために、 G をどんな部分群に分けていけばよいか分かることにある。

群を部分群で、 $G = \{H, Hg, Hg', \cdots\}$ のように剰余類分割することは、形式的には
 必ずできるが、これに対応する因数分解が、本当に実現するか否かが問題である。

$$F_G(V) = \prod_H (V - V_k) \times \prod_{Hg} (V - V_i) \times \prod_{Hg'} (V - V_j) \times \cdots \quad \text{と因数分解されたなら、}$$

$\Pi_H(V-V_k)=F_H(V)$ を作り出す H が、縮小した“ガロア群”である。
 H で不変な根の関数は、 $F_H(V)$ の展開式の係数の中で目に見える。

以上のように、3 次、4 次方程式では幸いにも計算が実現したが、 n 次方程式ではどうなのか？ $F_G(V)$ の因数分解が進むための条件を考えよう。

§ 3 方程式が解けるための、必要十分条件

1. ガロア群 G 対称性の V 多項式 $F_G(V)$ が、1 次式の積にまで因数分解できるための必要条件

3 次、4 次方程式の一般解法では、ガロア群 S_n から出発したから、 $F_{S_n}(V)$ がまず、 $\sqrt{(A_n \text{ 対称関数})}$ を使って分解された。ここでは、一般的な“出発点のガロア群 G ”から考え始める。

“出発点のガロア群”から“縮小したガロア群”に進むときは、計算対象に“特定の巾開方値（新たな既知数）”が追加されている。特定のとは“因数分解を一段階進めるために必要な巾開方値（根の非対称関数）”である。

そして、全段階で因数分解が実現すれば、 $F_G(V)$ は 1 次式にまで分解される。

1) V 多項式 = (より低次の既約 V 多項式) $\times$ (同左) $\times \cdots = 0$ と分解されるなら、右辺の各因子につき、既約 V 多項式 $= 0$ となる：解どうしは共役解（すなわち 1 つの既約方程式の解どうし）として拘束され、勝手な値はとれない。

基本対称式 = 有理数、という条件は、根が有理数なら何の制約にもならないが、根が無理数なら（既約方程式の根どうしなら）強い制約になる。例えば、有理数係数の 2 次方程式の 1 根が $\sqrt{2}$ なら、他根は必ず $-\sqrt{2}$ 、1 根が $1+i$ なら他根は $1-i$ になる。有理数係数の 3 次方程式は、3 つの虚根を持ち得ない。

共役解の意味を考察することによって、ガロア論文の結論の 1 つ、 $F_G(V)$ の因数分解が実現する“必要条件”が導かれる。

出発点になるガロア群対称性の $F_G(V)=0$ は、有理係数値の既約方程式である。

根の非対称関数（巾開方を含む値）を計算対象に追加できたら $F_G(V)$ は可約となり、 $F_G(V) = (\text{より低次の } V \text{ 多項式}) \text{ の積} = 0$ に分解されるが、“より低次の V 多項式”それぞれは、再び既約式である。したがって解どうしが拘束される。これが群の言葉でどう表現されるかを考えよう。

G 対称性の根の関数 θ から、 m 次巾開方で下記の値を求める方法があったとする。

つまり、根の非対称関数 (= 対称関数の m 次巾開方を含む値) を $r, r', \dots$ と書き ;
 $r = \sqrt[m]{\dots}$ を含む式、 $r' = \text{「}r\text{」における根名を置換した式}$ 、 $r'' = \text{「}r'\text{」における根名を置換した式}$ 、 $\dots$ という m ケの式が得られたとする。

r の構成成分である「非対称関数」を、不変に保つ群を H と呼ぶことにする。

どんな根の関数に対しても、それを不変に保つ群は必ず存在する (3 章)

「 θ が G 対称、 $\sqrt[m]{\theta}$ が H 対称」を、2 次方程式の根の関数のアナロジーで言えば、

$\theta = (\alpha + \beta)^2 - 4\alpha\beta$ が S_2 対称、 $\sqrt{\theta} = \alpha - \beta$ が A_2 対称である。

H は G の部分群だから、剰余類分割 $G = \{H, Hg, Hg', \dots\}$ が必ずできる。

ここで、 $F_H(V) = \prod_H (V - V_k) = V^{N/m} - (V_1 + V_2 + \dots) V^{N/m-1} + \dots \pm V_1 V_2 \dots V_{N/m}$
 と定義すれば、 $V_2, V_3 \dots$ は、 V_1 を H の元で置換したものの“すべて”だから、
 $F_H(V)$ は H 対称性である。

$F_H(V) = F_H(V, r)$ と書き、これを g で置換すれば、 $F_{Hg}(V) = F_{Hg}(V, r')$ と書ける。

$rg = r'$ であり、同様に $rg' = r'', rg'' = r''' \dots$ (76-77 頁の実例、参照)。

m 次巾解法を含む $r, r', r'', \dots$ を、計算対象に追加できたなら、有理計算で $F_G(V)$ が
 m ケの因子に因数分解できて (G の位数が N なら、各因子は、 N/m 次多項式)、

$F_G(V) = F_H(V) F_{Hg}(V) F_{Hg'}(V) \dots$

$= F_H(V, r) \times F_{Hg}(V, r') \times F_{Hg'}(V, r'') \times \dots = 0$ となる。なぜなら、

H 対称性の根の関数を係数にもつ $F_H(V)$ を分離する計算手順が、本当にあれば、
 (既約方程式の解法は根の名称変更に影響されないから) 根を名称変更した $F_{Hg}(V)$
も分離でき、 $F_{Hg'}(V), \dots$ も分離できる筈だからである。

$Hg, Hg', \dots$ は群でない。根の名称変更で Hg が群になれば、 H が群でなくなる。

(例えば g^{-1} を掛けるという名称変更で、 Hg は、 $Hgg^{-1} = H$ という群になり、 H は Hg^{-1} という群でない置換集合になる)

上記の因数分解が本当に実現したなら、 $F_H(V, r) = 0, F_{Hg}(V, r') = 0, \dots$ となる。

ここから結論される各方程式の共役解 (V の値) どうしの拘束を、群論で表現したアイデアは、ガロア論文の中で最も神秘的に思えるが、以下の説明は (煩雑であっても飛躍はないので) 理解しうる。

$F_H(V, r) = \prod_H (V - V_k) = 0$ の解のひとつを、 V_a と呼び、別の解を V_b と呼ぶ。

根の 1 次式 V_b に含まれる各根 α_j のそれぞれに、 $\alpha_j = \varphi_k(V_a)$ を代入すれば、

V_b は V_a の整式で、 $V_b = \Phi(V_a)$ と書ける。つまり $F_H(V_b, r) = F_H[\Phi(V_a), r] = 0$

これは、 V の方程式 $F_H[\Phi(V), r] = 0$ が、 V_a を解にもつことを意味する。

すると、 $F_H[\Phi(V), r] = 0$ と $F_H(V, r) = 0$ が、解 V_a を共有することになるが、 $F_H(V, r)$ は既約式だから、 $F_H[\Phi(V), r]$ が、 $F_H(V, r)$ で割り切れることになる (15 頁；互除法の定理による)。

有理数に $r, r', \dots$ を追加した計算範囲で、 $F_G(V)$ を分解して $F_H(V, r)$ をくくり出すことができたとするが、 $F_H(V, r)$ の分解は、まだ出来ていない段階の話だから、 $F_H(V, r)$ は既約式なのである。

したがって、 $F_H[\Phi(V), r] = q(V) F_H(V, r) = 0$ と書ける。商 $q(V)$ には関心がない。

上の両辺を、 g で置換する。すなわち、 $Vg = V', rg = r'$ と書く。

g は、関係 $\alpha_j = \phi_k(V)$ を保存する群 G の元だから、この置換ができる！

すると、 $F_{Hg}[\Phi(V'), r'] = q(V') F_{Hg}(V', r') = 0$ となる。… (#)

<ここで、 $F_H(V, r) = 0$ の解の議論から、 $F_{Hg}(V', r') = 0$ の解の話に移った>

(#) が意味すること： $X = V'$ が $F_{Hg}(X, r') = 0$ の解なら、 $X = \Phi(V')$ も解である。

すなわち、 $F_H(V, r) = 0$ の解どうしが H で相互変換されるのと同様に、 $F_{Hg}(V, r') = 0$ の解どうしも H で相互変換されることが分かった。同様の議論で、 $F_{Hg}(V, r') = 0$ 、 $F_{Hg'}(V, r'') = 0$ 、…の解どうしがみな、 H で相互変換される … ☆
解どうしが H で相互変換されるということは、 $F_{Hg}(V, r')$ 、 $F_{Hg'}(V, r'')$ 、…がみな、 H 対称性であることを意味する！ (Hg 、 Hg' 、…が群でないにも関わらず！)

< $F_G(V)$ が因数分解される必要条件が、群の言葉で表現できた>

念のため再確認する： H で置換して作った $F_H(V, r) = \Pi_H(V - V_k)$ は、 H が群だから (V_k を置換した V_j もまた右辺の中にあるから)、 H 対称性なのである。

一方、 H がどんな部分群であっても、 $G = \{H, Hg, Hg', \dots\}$ という剰余類分割はできるが、 $F_{Hg}(V, r')$ 、 $F_{Hg'}(V, r'')$ 、… はどれも、「 $F_H(V, r)$ を g 、 g' 、… で置換した」という意味だから、 H 対称性になる必然性は全くない (Hg の元と H の元が、すべて異なることは群の基本知識である。 Hg の元には e もない)。

しかし、 H 対称性の $F_H(V, r)$ を本当に分離できる計算手順がある場合は、 $F_G(V) = F_H(V, r) \times F_{Hg}(V, r') \times \dots = 0 \dots \star$ と因数分解されるのだから、 $F_H(V, r) = 0$ 、 $F_{Hg}(V, r') = 0$ 、…が成り立ち、すると前記 $\star$ が言えるのである。

では、因数分解の実現が本当かどうかは、どのように確かめられるだろうか？

$F_{Hg}(V, r')$ 、 $F_{Hg'}(V, r'')$ 、…を H の元で置換してみて、不変と判明すれば本当であり、 $F_{Hg}(V, r')$ 、 $F_{Hg'}(V, r'')$ 、…が変化してしまう (H 対称性でない) なら、 $\star$ は架空の式、その形の因数分解は実現しない、と分かる (変化しない場合、変化する場合、それぞれの実例を後で示す)。

問題 3 次方程式の解法 72 頁をみて、「 V_4, V_5, V_6 」が、「 V_1, V_2, V_3 」と同じ置換群 H で相互変換されることを確かめよ。

答 H の元 $(1\ 2\ 3)$ 、 $(1\ 2\ 3)^2$ を V_4, V_5, V_6 に作用させてみればよい。

$$V_4(1\ 2\ 3) = (A\alpha_2 + B\alpha_1 + C\alpha_3)(1\ 2\ 3) = A\alpha_3 + B\alpha_2 + C\alpha_1 = V_6 \text{ のように書けば、}$$

$$V_4(1\ 2\ 3)^2 = V_5, V_5(1\ 2\ 3) = V_4, V_5(1\ 2\ 3)^2 = V_6, V_6(1\ 2\ 3) = V_5, V_6(1\ 2\ 3)^2 = V_4$$

すなわち、 G 対称性の $F_G(V)$ から H 対称性の $F_H(V)$ が分離されて、因数分解 $F_G(V) = F_H(V, r) \times F_{Hg}(V, r') \times F_{Hgr'}(V, r'') \times \dots$ が実現する必要条件は、分解された因子がみな H 対称性になることである。

この条件は、 $F_G(V)$ が最後に V の 1 次式にまで分解されるときまでの、どの段階でも要求される（前記、3 次方程式、4 次方程式の例を参照）。

以上が、後に述べる十分条件とともにガロア論文の頂上の 1 つである。

以下で、現代論に繋がるように説明するが、原著では、いきなり 86 頁 §4 の議論に進む

<上記 ★ は、下記の言い方で、より簡明に言える>

・ $F_H(V) = \Pi_H(V - V_k) = V^m - (V_1 + V_2 + \dots) V^{m-1} + \dots \pm V_1 V_2 \dots V_m = 0$ の解は、 $H = \{h_i\}$ で変換されるのだから、任意の 2 つの解 V_a, V_b に対し、なんらかの元 h_i が存在して、 $V_a h_i = V_b$ が成り立つ。… (1)

・ $F_H(V)g = F_{Hg}(V) = V^m - (V'_1 + V'_2 + \dots) V^{m-1} + \dots = 0$ の解が H で変換される条件は、任意の V'_a, V'_b に対し、 $V'_a h_j = V'_b$ となる h_j があることである。… (2)

・ $F_{Hg}(V)$ は、 $F_H(V)$ を g で置換したものだから、 $V_a g = V'_a$ … (3)

および、 $V_b g = V'_b$ … (4)

そこで、(1) に g を掛けたものと (4) を比べて、 $V_a h_i g = V_b g = V'_b$

(2) を満たす h_j を (3) に掛けると、 $V_a g h_j = V'_a h_j = V'_b$

したがって、 $V_a h_i g = V_a g h_j$ が分かる。… (5)

解 V_a は G の元 (e 以外の h_k, g など) で置換すると必ず別の V になるから、(5) より、 $h_i g = g h_j$ と分かる。この関係を、 $Hg = gH$ または $g^{-1}Hg = H$ と書ける。

注： g が H の元と可換 ($h_j g = g h_j$) であることは、意味しない。

ガロアは、以上の表記を第一論文で明示していないが、友人への手紙（高瀬正仁訳：アーベル/ガロア楕円関数論. 東京、朝倉書店、1998、p288）の中で述べている。

2) 正規部分群の概念（現代用語）

H を G の部分群とする。

G の任意元 g に対し、 $gH = Hg$ なら、 H を G の正規部分群と呼ぶ。

この言葉を使うと、ガロア群 G が縮小して H になる必要条件、すなわち $F_G(V)$ が因数分解される条件は、「 G に正規部分群 H が存在すること」と言える。

また、方程式が解ける必要条件是、 $F_G(V)$ の各分解因子の対称性を表す群の系列 $G \supset H \supset \cdots \supset \{e\}$ において、隣接する部分群がみな正規部分群であること、となる。

<例：正規部分群であるものとなないもの>

* 4 次方程式の解法 (77 頁) でみた、 H' と H の関係を調べよう。

$$H' = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \supset H = \{e, (1\ 2)(3\ 4)\}$$

H' の元、例えば $(1\ 3)(2\ 4)$ を H に作用させると、

$$H(1\ 3)(2\ 4) = \{(1\ 3)(2\ 4), (1\ 2)(3\ 4)(1\ 3)(2\ 4)\} = \cdots = (1\ 3)(2\ 4)H$$

同様に、 $H(1\ 4)(2\ 3) = (1\ 4)(2\ 3)H$ 、すなわち、 H は H' の正規部分群である。

3 次、4 次方程式の解法で使った様々な部分群は、すべて正規部分群の系列になっていることを容易に確かめられる。

* 正規部分群でない部分群の例を、1 つ作ってみよう。

S_n の元を (ガロア流の記法 ; 40 頁) で書くと、 $\{123\cdots, 213\cdots, \cdots\}$ などである。

このうち “1 を固定して他を任意置換” する部分群を H^* とする。

□ に、数字を配置すると考えて、

$$H^* = \{1234\cdots n, 1\square\square\square\cdots, 1\square\square\square\cdots, \cdots\} \text{ の形である。 } 1234\cdots n = e$$

問題 S_n を H^* で剰余類分割せよ

答 $S_n = \{H^*, H^*(1\ 2), H(1\ 3), H^*(1\ 4), \cdots, H^*(1\ n)\}$ n ケの集合になる。

$H^*(1\ 2)$ の元は、 $2\square\square\square\cdots, 2\square\square\square\cdots, 2\square\square\square\cdots$ 、の形だとすぐ分かる。

$(1\ 2)H^*$ の元は、 $\square 1\square\square\cdots, \square 1\square\square\cdots, \square 1\square\square\cdots$ 、これは数列 $1, 2, 3, \cdots$ に左記の元を作用させて、少し考えると分かる。

$2\ 1\square\square\cdots$ の形の元の個数は $(n-2)!$ ケだが、 $H^*(1\ 2)$ の元は $(n-1)!$ ケだから、すべての元が、 $2\ 1\square\square\cdots$ になることはない。すなわち、 $H^*(1\ 2) \neq (1\ 2)H^*$ である。

一般的に書けば $gH^* \neq H^*g$ 、すなわち、 H^* は S_n の正規部分群でない。

上の H^* で、 $F_{S_n}(V) = F_{H^*}(V) F_{H^*g}(V) F_{H^*g'}(V) \cdots = F_{H^*}(V) F_{H^*(1\ 2)}(V) F_{H^*(1\ 3)}(V) \cdots$ という因数分解が (形式的には書けても) 実現しないことを、確かめよう。

$$F_{H^*}(V) = \Pi_{H^*} (V - V_k) = \Pi_{H^*} \{V - (A_1\alpha_1 + A_2\square + A_3\square + \cdots)\} \quad \square \text{ には } \alpha_1 \text{ 以外が入る。}$$

$g = (1\ 2)$ を掛けて $F_{H^*g}(V)$ を作ると、

$$F_{H^*g}(V) = \Pi \{V - (A_1\alpha_2 + A_2\square + A_3\square + \cdots)\} \quad \square \text{ には } \alpha_2 \text{ 以外が入る。}$$

$F_{H^*g}(V) = F_{H^*(1\ 2)}(V)$ に H^* の元 (添え字 1 を変えない置換)、例えば $(2\ 3)$ を作用させたら、 $\Pi \{V - (A_1\alpha_3 + A_2\square + A_3\square + \cdots)\}$ 、すなわち $F_{H^*g}(V)$ と別のものになる。

$F_{H^*g}(V)$ は H^* 対称性でない。同様に $F_{H^*g'}(V)$ などみな H^* 対称性でない。

* n の値によらず、交代群 A_n は S_n の正規部分群である。

剰余類分割の定理から、 $S_n = \{A_n, g A_n\} = \{A_n, A_n g'\}$ と書ける。

g, g' は A_n に属さない S_n の任意元（奇置換）である。 $g = g'$ でもよいから、 $g A_n = A_n g$ 、すなわち A_n は S_n の正規部分群である。

例えば $g = (1\ 2)$ として、剰余類分割 $S_n = \{A_n, A_n (1\ 2)\}$ に対応する因数分解、 $F_{S_n}(V) = F_{A_n}(V) F_{A_n g}(V)$ は常に実現する。

74 頁（根の差積は、常に 2 次巾開方で求まるという議論）で説明した。

3) 剰余類群（商群）の概念

正規部分群では、 $g H = H g$ より、 $g H g' H = g g' H H = g g' H$ または $H g H g' = H g g'$ となる。

すなわち、集合 $g H$ または $H g$ は、積に関して群の元と同様に扱える。

また、 $H g^{-1} H g = H g^{-1} g H = H$ なので、 $H = H e$ を単位元とみなし、 $H g^{-1}$ を $H g$ の逆元と同様に扱える。

したがって、 H が正規部分群のとき、 G の剰余類分割 $= \{H, H g, H g', \dots\}$ では、それぞれの要素集合（剰余類）を元と同様にみて、群の定理が成り立つ。

この形に書いた G すなわち $\{H, H g, H g', \dots\}$ を 剰余類群（または商群）と呼ぶ。

この概念を使うと、次節のように十分条件を述べることができる（ガロア原著にならない現代用語だが、自然な言い換えであり、原著を簡潔に解説できる）

2. 方程式が解ける十分条件、および（現代用語による）必要十分条件

H を正規部分群として含む群 H' があるとき、 $F_{H'}(V)$ を因数分解して、因子 $F_H(V)$ を得る計算手順を示せる。

V 多項式の因数分解法とは、係数に含まれる“根の非対称関数”の計算法である。「各根という根の関数が、より対称性の高い根の関数の巾開方で書かれ、最終的に対称式の巾開方で書かれるか」を、一般的に考察する（3 次と 4 次の方程式では、これが実現することを 2 章でみた）。

1) 根の関数が、より高対称な根の関数で表せるための十分条件

$H_2 \supset \dots \supset H_1 \supset H$ という関係を考える。

H が、 H_2 の正規部分群なら、 H_2 の剰余類分割 $\{H, H h_2, H h'_2, H h''_2, \dots\}$ は、剰余類群をなす（前述）。

「素数位数の部分群は必ずある（定理 2、42 頁）」を、剰余類群の言葉で言えば；

H_2 の部分群には、位数が H の素数 p 倍になる群 H_1 が必ずある。

「素数位数の群は巡回群である（定理 5、44 頁）」を、剰余類群の言葉で言えば；
 H_1 が巡回群（巡回剰余類群）になる。 $H_1 = \{H, Hh', \dots, Hh'^{p-1}\}$ 、 $h' \in H_2$
 すると H 対称関数は、すでに知った下記の方法で、 H_1 対称関数から算出できる。

θ を H 対称関数とする、 $\theta H = \theta$

$\theta h' = \theta_1$ 、 $\theta h'^2 = \theta_2$ 、 $\dots$ 、 $\theta h'^{p-1} = \theta_{p-1}$ と書いて（2 章、26 頁と同様）、

$\varphi_\omega = \theta + \omega \theta_1 + \omega^2 \theta_2 + \dots + \omega^{p-1} \theta_{p-1}$ を作る（ $\omega^p = 1$ ） $\dots$ (1)

$\varphi_\omega^p = (\theta + \omega \theta_1 + \dots + \omega^{p-1} \theta_{p-1})^p$ は、 Hh'^k で不変だから、 H_1 対称関数である。

1 の p 乗根、 ω 、 ω' 、 ω'' 、 $\dots$ 、1 に応じた、 φ_ω 、 $\varphi_{\omega'}$ 、 $\varphi_{\omega''}$ 、 $\dots$ から、 p 元連立 1 次方程式が作れる（25 頁、巾開法の取り方、参照）。

$$\begin{aligned} \sqrt[p]{\varphi_\omega^p} &= \theta + \omega \theta_1 + \omega^2 \theta_2 + \dots + \omega^{p-1} \theta_{p-1} & \dots (2) \\ \sqrt[p]{\varphi_{\omega'}^p} &= \theta + \omega' \theta_1 + \omega'^2 \theta_2 + \dots + \omega'^{p-1} \theta_{p-1} \\ \sqrt[p]{\varphi_{\omega''}^p} &= \theta + \omega'' \theta_1 + \omega''^2 \theta_2 + \dots + \omega''^{p-1} \theta_{p-1} \\ &\dots\dots = \dots \end{aligned}$$

$F_H(V)$ の係数成分である H 対称関数 θ 、 θ_1 、 $\dots$ 、 θ_{p-1} を、
 $F_{H_1}(V)$ の係数成分である H_1 対称関数の巾根、 $\sqrt[p]{\varphi_\omega^p}$ 、 $\sqrt[p]{\varphi_{\omega'}^p}$ 、 $\dots$ で表せるから、
 $F_{H_1}(V)$ の因数分解が実現する。

* H を正規部分群として含む群 H_2 が存在すれば、以上のように、 H 対称性の関数を、 H よりも大きな群 $H_1 = \{H, Hh', \dots, Hh'^{p-1}\}$ 対称性の関数から必ず求められる。

$h' \in H_2$ だから、 $Hh' = h'H$ 、 $Hh'^k = h'^k H$ であり（ H_1 の作り方からして当然だが）
 H は H_1 の正規部分群になる。

* ただし、 H_1 が H_2 の正規部分群（ $h'' \in H_2$ 、 $h'' H_1 = H_1 h''$ ）になるとは限らない。

$h'' H_1 = h'' H h'^k = H h'' h'^k$ 、一方、 $H_1 h'' = H h'^m h''$ だから、正規性の定義
 $h'' H_1 = H_1 h''$ は、 $H h'' h'^k = H h'^m h''$ となる。 $H = H h'^m h'' (h'^k)^{-1} (h'')^{-1}$ と
 書けば、 $h'^m h'' (h'^k)^{-1} (h'')^{-1} \in H$ を意味する。

つまり任意の h' 、 $h'' \in H_2$ 、任意 m に対し、 k を適当に選び、 $h'^m h'' (h'^k)^{-1} (h'')^{-1}$ が
 H の元になれば、 H_1 が H_2 の正規部分群になる。

* H_1 を正規部分群として含む群がみつき、さらに拡大された部分群のどれかが、
 H_2 の正規部分群になったら、 H 対称関数が、 H_2 対称関数で書き表せたことになる。

$H_2 = G$ なら、 H 対称関数が、 G （ガロア群）対称関数で書き表せたことになる。

以上のような、正規部分群による剰余類分割の連鎖が、 $\{e\}$ からガロア群 G にまで

つながれば、その逆過程として、 $F_G(V)$ が 1 次式にまで因数分解されることになる。
そして $G = S_n$ のときは、 n 次方程式の一般解が得られることになる。

2) 必要十分条件のまとめ

使用した群論の定理の復習：1) どんな群でも、任意の部分群で剰余類分割できる、
2) 正規部分群で剰余類分割すると剰余類群となる、3) その剰余類群に、素数 k の剰余類からなる部分（剰余類）群は必ず存在し、巡回（剰余類）群をなす。

以上より、方程式が解ける条件を（ガロア原著と異なる）現代用語でまとめると

(1) 係数が任意文字の方程式が解ける必要十分条件は；

ガロア群の部分群系列 $S_n \supset \cdots \supset H \supset \cdots \supset \{e\}$ を、隣接する群が
正規部分群、かつ位数比が素数になるように作れること。

$S_n \supset A_n \supset \cdots \supset \{e\}$ の系列が上記を満たすことともいえる。ただし系列が
 A_n を経由できることは示したが（73 頁）、経由が必須なことは後で証明する

(2) 方程式のガロア群が G であるとき、解ける必要十分条件は；

$G \supset H \supset \cdots \supset \{e\}$ が、正規部分群の系列になり、隣接する群の位数比が、
 H 以降で素数になること。

（87 頁で示すが、 G 、 H の位数比は素数でなくても、 H 対称関数の値が求まる。

$G = S_n$ なら、 S_n 、 A_n の位数比が素数 2 なので全系列で素数比になる）

上記 (1) が満たされ、 S_n が $\{e\}$ にまでつながるのは、実はあっけなくも $n \leq 4$ のときだけである（だから解公式は、4 次方程式までしか得られない）。

$F_{S_n}(V)$ または $F_G(V)$ が、1 次式にまで因数分解される必要十分条件が分かったが、
下記のような色々な課題が残っている。

- ・ 正規部分群によって剰余類に分割する方向から考えると、 **$n \geq 5$ では、 S_n の次の A_n が分割できない。**その証明はガロア原著にないので、5 章（現代論）§3 に記した。興味あれば今すぐ 133 頁に飛び、すでに知った群論の言葉で、理解できる。

では、 A_n を経由しない分割経路はあるだろうか？ 後で考えよう（90 頁）。

- ・ 実際に方程式を解いて根を計算するとき、 S_n の分割法を捜すのは適切でない。
（ただし S_3 では簡単である。 S_4 も、元をすべて書き出せば出来るから、興味あれば試みるとよい：どの元を集めれば群になるか掛け算で試行錯誤する、できた群が正規部分群であるかどうか調べるなど。しかし、 S_5 で試行錯誤したら徒労に終わる）

- ・ 一般解が書けない方程式でも、“解ける場合”は見分けられるのだろうか？

§ 4 任意文字係数の n 次方程式を、実際に解く計算原理

G の剰余類分割 $\{H, Hg, Hg^2, \dots\}$ を用いて $F_G(V)$ が因数分解される“原理”が、以上で分かったが、以下では、根を“実際に計算する”ガロアの方法を示す。

すなわち、 S_n または G の分割でなく、各根から始めて根の関数の対称性を高め、 S_n または G へ到達する。これは 2 章で 3 次、4 次方程式を解いた方法である。2 章では、根配列の巡回置換を、天下りの使っただけだったが、今は、巡回置換を使う理由が、剰余類群に由来する必然性を知った。

1. 各根を、より高対称な関数（の巾根）で表す第一段階

求めたい未知関数は、各根である。既約方程式の n 根は、平等に扱わねばならない。

n ケ 1 組の非対称関数（各根）を、より高対称の関数と等号で結ぶのは、“合計で n 次”の巾開方を使ってのみ可能である（23 頁）。

1) n が素数でないとき：4 次方程式、6 次方程式の例

n が素数でないとき、 n 根の対称性を高める手順は、一段階にならない。その理由を考えよう。4 次方程式の解き方（28 頁）を復習し、問題点をもっと明確にする（ここでは、根の添え字を $\alpha_1, \alpha_2, \alpha_3, \dots$ でなく、 $\alpha_0, \alpha_1, \alpha_2, \dots$ と書く）。

4 次方程式で（26 頁の一般手順に従い）、 $\theta = \alpha_0 + \omega \alpha_1 + \omega^2 \alpha_2 + \omega^3 \alpha_3$ ($\omega^4 = 1$) を作ると、 θ^4 が根の巡回置換で不変（より高対称の関数）になった。

$\omega^4 = 1$ の解、 $\omega, \omega', \omega'', 1$ を代入して、 θ^4 の関数形をみると、

1 を代入した、 $\theta_4 = \alpha_0 + \alpha_1 + \alpha_2 + \alpha_3$ （既知数）を除く、3 つの“未知関数”を得る。

下記が、さらに対称性を高めるべき（対称式への接近を目指す）関数である。

$$\begin{aligned}\theta_1^4 &= (\alpha_0 + \omega \alpha_1 + \omega^2 \alpha_2 + \omega^3 \alpha_3)^4 \\ \theta_2^4 &= (\alpha_0 + \omega' \alpha_1 + \omega'^2 \alpha_2 + \omega'^3 \alpha_3)^4 && \dots \star \\ \theta_3^4 &= (\alpha_0 + \omega'' \alpha_1 + \omega''^2 \alpha_2 + \omega''^3 \alpha_3)^4\end{aligned}$$

$\omega, \omega', \omega''$ に、 $i, -i, -1$ を代入した、 $\theta_1^4, \theta_2^4, \theta_3^4$ の $()^4$ の中身を見ると、

$$\alpha_0 + i \alpha_1 - \alpha_2 - i \alpha_3, \quad \alpha_0 - i \alpha_1 - \alpha_2 + i \alpha_3, \quad \alpha_0 - \alpha_1 + \alpha_2 - \alpha_3,$$

すると、根のどんな配列置換をしても、 $\theta_1^4 \longleftrightarrow \theta_3^4, \theta_2^4 \longleftrightarrow \theta_3^4$ とは移り変わらない（ $\theta_1^4 \longleftrightarrow \theta_2^4$ なら、 α_1, α_3 の互換で実現するが）。移り変わらない原因は、 $\omega^4 = 1$ の解に、1 以外の非原始根（ θ_3 に含まれる -1 ）があるからである。

★をみると、根 $\alpha_1 \sim \alpha_4$ の置換（名称変更）で、 $\theta_1^4 \longleftrightarrow \theta_2^4 \longleftrightarrow \theta_3^4$ と変換可能か

どうかは、 $()^4$ の形の式どうしの間で、 $\omega \longleftrightarrow \omega' \longleftrightarrow \omega''$ と呼び変え可能かどうか、と同じだと分かる。

ω 、 ω' 、 ω'' が、みな原始根なら、 $()^4$ の式の中で、 $(\omega$ の巾乗を掛ければ相互に移り変わるから) 呼び変え可能だが、非原始根が混入していれば、不可能である。

非原始根の混入は、非素数 m に対する 1 の m 乗根を使って、★ に類する連立式を作ると必ず生じるから、解法が先へ進むには、“素数次の巾開方”が必要になる。一方、解が求まる「最後の巾開方」段階なら、素数次巾開方である必要はないのである。

相互変換されない（本節の冒頭、剰余類分割の用語で言えば、 g 、 g^2 、…で変換されない）関数の組、 θ_1^4 、 θ_2^4 、 θ_3^4 は、それ以上に対称性を高める方法がないのだった。

すなわち、非素数の n 次方程式で、 $\theta = \alpha_0 + \omega \alpha_1 + \cdots + \omega^{n-1} \alpha_{n-1}$ ($\omega^n = 1$) から出発したら、一般解が得られない。

4 次方程式では（28 頁～参照）；

$\{e, (0\ 1)(2\ 3)\}$ から出発し、4 根を 4 つの関数 $\alpha_0 + \alpha_1$ 、 $\alpha_2 + \alpha_3$ 、 $\alpha_0 \alpha_1$ 、 $\alpha_2 \alpha_3$ に置き換えた。次の段階の群 $\{e, (0\ 1)(2\ 3), (0\ 2)(1\ 3), (0\ 3)(1\ 2)\}$ で“4 根を平等に”扱った。2 組の 2 元連立方程式を 2 回使い、2 回の 2 次巾開方 $\sqrt{}\sqrt{}$ を行なった。

6 次方程式なら； $H_1 = \{e, (0\ 1)(2\ 3)(4\ 5)\} = \{e, h\}$ から出発し、次に $g = (0\ 2\ 4)(1\ 3\ 5)$ を使って、 $H' = \{H_1, H_1 g, H_1 g^2\}$ を利用しうる。

$hg = gh$ 、 $hg^2 = g^2h$ と分かるので、 H_1 は H' の正規部分群である。

6 根は 6 つの関数 $\alpha_0 + \alpha_1$ 、 $\alpha_2 + \alpha_3$ 、 $\alpha_4 + \alpha_5$ 、 $\alpha_0 \alpha_1$ 、 $\alpha_2 \alpha_3$ 、 $\alpha_4 \alpha_5$ （を含む巾開方形）と 3 組の 2 元連立方程式で結ばれ、次に 1 組の 3 元連立方程式を介して、 H' 対称関数の $\sqrt[3]{}\sqrt{}$ の形で書かれる。

一方、 $H_2 = \{e, g, g^2\}$ から出発しても、 $\{H_2, H_2 h\} = H'$ となり、 H_2 も H' の正規部分群である。6 つの関数 $\alpha_0 + \omega \alpha_2 + \omega^2 \alpha_4$ 、 $\alpha_0 + \omega^2 \alpha_2 + \omega \alpha_4$ 、 $\alpha_0 + \alpha_2 + \alpha_4$ 、 $\alpha_1 + \omega \alpha_3 + \omega^2 \alpha_5$ 、 $\alpha_1 + \omega^2 \alpha_3 + \omega \alpha_5$ 、 $\alpha_1 + \alpha_3 + \alpha_5$ が使われ、各根は H' 対称関数の $\sqrt[3]{}\sqrt{}$ の形で書かれる。

$\sqrt[3]{}\sqrt{}$ 、 $\sqrt[3]{}\sqrt{}$ とともに行き止まる道なので、式形の違いは矛盾を意味しない。 H_1 対称関数、 H_2 対称関数いずれから出発しても、 S_6 対称性に達しない（証明 91 頁）。

3) 素数 n 次方程式

n が素数なら ($n\sqrt{}$ を、 $6\sqrt{} \rightarrow 3\sqrt{}\sqrt{}$ のようには分解できないから) 下記 (1) を選ぶ必然性がある（前述）。根の添え字の巡回置換で、 n 根を平等に一斉に置換できる。

$$\alpha_0 + \omega \alpha_1 + \cdots + \omega^{n-1} \alpha_{n-1} = \theta_\omega \quad \omega^n = 1 \quad \cdots (1)$$

h を、 $k \rightarrow k+1 \pmod{n}$ 、 $H = \{e, h, h^2, h^3, \cdots, h^{n-1}\}$ とする。

θ_ω は ($\omega = 1$ でない限り) H で変化するが、 θ_ω^n は、 H で不変である。

1 の n 乗根 $\omega, \omega', \omega'', \dots, 1$ を代入して n ケの式を生じる。

$$\begin{aligned} \alpha_0 + \omega \alpha_1 + \dots + \omega^{n-1} \alpha_{n-1} &= \sqrt[n]{\theta_\omega^n} \\ \alpha_0 + \omega' \alpha_1 + \dots + \omega'^{n-1} \alpha_{n-1} &= \sqrt[n]{\theta_{\omega'}^n} \quad \dots (2) \\ \alpha_0 + \omega'' \alpha_1 + \dots + \omega''^{n-1} \alpha_{n-1} &= \sqrt[n]{\theta_{\omega''}^n} \\ \dots\dots\dots &\dots\dots \\ \alpha_0 + \alpha_1 + \dots + \alpha_{n-1} &= \text{既知数} = \sqrt[n]{\theta_1^n} = \theta_1 \quad (25 \text{ 頁の記法}) \end{aligned}$$

$\alpha_0 \sim \alpha_{n-1}$ は、(3) から有理計算して、 $n-1$ ケの未知関数で表せる。

<重要な概念の暗示> (2) をみると(次に求めるべき右辺の)未知関数の個数が、 n ケから $n-1$ ケに減っている。基本対称式を 1 つ利用できたからである。

(2) に H の元 を作用させると、左辺は (ω^k と根の配置関係が変わるから) むろん変化する。右辺の関数形は H で変化しないが、左辺は H で変化するので等式が別の等式に移り変わる、という意味で“変化する”。ただし下記の例外に注目しよう。

$\omega = 1$ を代入した、 $\alpha_0 + \dots + \alpha_{n-1} = \theta_1$ の等式関係だけが、 H で不変である。

第 2 段階は、 θ_1 以外の、 $\theta_\omega^n, \theta_{\omega'}^n, \theta_{\omega''}^n, \dots$ 、をより高対称な関数で表すのが課題となる。 $\theta_\omega^n \rightarrow \theta_{\omega'}^n \rightarrow \theta_{\omega''}^n \rightarrow \dots$ 、の変換を起こす巡回置換の存在が必要である。

第 2 段階に限らない一般的な段階で、“より高対称な関数で表す”ときにおきることを、次節で考えてみる。

2. 根の関数を、より高対称な関数で表す連立方程式における、未知関数の個数

一般的に下記の群、 H, H^* を考える (前項の群名 H とは関係ない)。

n 次方程式の根からなる 1 組の関数、 $\varphi_1 \sim \varphi_m$ が与えられており、 $\varphi_1 \sim \varphi_m$ それぞれが H 対称性だとする。

【復習】 相互変換 $\varphi_1 \rightarrow \varphi_2 \rightarrow \dots \rightarrow \varphi_m \rightarrow \varphi_1$ を引き起こす置換 h' が存在し、 $h' H = H h'$ なら、 $H^* = \{e, H h', \dots, H h'^{m-1}\}$ で対称な関数 (Φ と総称する) を使い、 $\varphi_1 \sim \varphi_m$ を、 Φ で表せた (対称式に一段階近づく)。

$\varphi_1 h' = \varphi_2, \varphi_1 h'^2 = \varphi_3, \dots, \varphi_1 h'^{m-1} = \varphi_m$ なら、既述のように下記の Φ_ω を作れる。

$$\varphi_1 + \omega \varphi_2 + \dots + \omega^{m-1} \varphi_m = \Phi_\omega \quad \dots (3) \quad \omega^m = 1$$

1 の m 乗根、 $\omega, \omega', \omega'', \dots, 1$ を代入した、 $\Phi_\omega, \Phi_{\omega'}, \dots$ から m ケの式を作れる

$$\begin{aligned} \varphi_1 + \omega \varphi_2 + \dots + \omega^{m-1} \varphi_m &= \sqrt[m]{\Phi_\omega^m} \\ \varphi_1 + \omega' \varphi_2 + \dots + \omega'^{m-1} \varphi_m &= \sqrt[m]{\Phi_{\omega'}^m} \\ \varphi_1 + \omega'' \varphi_2 + \dots + \omega''^{m-1} \varphi_m &= \sqrt[m]{\Phi_{\omega''}^m} \quad \dots (4) \end{aligned}$$

.....

$$\varphi_1 + \varphi_2 + \varphi_3 + \cdots + \varphi_m = {}_m\sqrt{\Phi_1^m} = \Phi_1 \quad \leftarrow \quad \omega=1 \text{ を代入した式}$$

(4) から、 H 対称関数 $\varphi_1 \sim \varphi_m$ が、 H^* 対称関数 Φ_ω^m 、 $\Phi_{\omega'}^m$ 、 $\cdots$ の巾開方で表せる。
この手順を逆に見ると、因数分解の実現 $F_{H^*}(V) = F_H(V) F_{Hh'}(V) F_{Hh''}(V) \cdots$ を意味した。

以上は、84 頁の説明の繰り返しだが、以下の視点で問題を見直そう。

Φ_ω^m は H^* 対称だが、 $\Phi_\omega = {}_m\sqrt{\Phi_\omega^m}$ は H^* 対称ではなく、 H^* で変化する。

すなわち、 ${}_m\sqrt{\Phi_\omega^m}$ は、 H^* で変化する (4) の左辺の関数に等しいのである。

H^* の元で置換したとき、 ${}_m\sqrt{\Phi_\omega^m}$ は (4) の中で、別の式に移らねばならない (解法が先へ進むために、これが必要である：86-87 頁説明)。

ガロア群の定理 (69 頁) の言葉で言うと；(4) 左辺の各式は H^* で変化する。

右辺は H^* 対称関数から有理計算できない (H^* 対称関数の巾開方量である)。

しかし、 $\omega=1$ を代入した、 $\varphi_1 + \cdots + \varphi_m = \Phi_1$ だけは、 H^* で不変である。

Φ_1 が H^* で不変とは、 H^* 対称関数の巾開方量でなく、 H^* 対称関数 (と有理数) の範囲で有理計算できることを意味する。このような計算可能性を A と呼ぼう。

(4) の段階で求めたい未知量は、“ H^* 対称関数から有理計算できない関数” なのである (B と総称しよう)。すなわち、 A は求めなくてよい。

なぜなら、 B が、(H^* よりも高対称な関数の巾開方形を使って) 有理計算できたときは、 A もその範囲で有理計算できるからである。

比喩：「 $\sqrt{2}$ と $\sqrt{3}$ 」を使う有理計算で、 $\sqrt{6}$ は得られ、 ${}_4\sqrt{6}$ は得られない。

「 ${}_4\sqrt{2}$ と ${}_4\sqrt{3}$ を含む数範囲」では、 $\sqrt{6}$ も、 ${}_4\sqrt{6}$ も有理計算できる。

すなわち、各根から始め、(より高対称な関数と結ぶ) 連立方程式を作るたびに、
(次の段階の連立方程式へ持ち越される) 未知関数の個数が、
($\omega^m=1$ の根、 $\omega=1$ の代入に起因して) 減る。そして、1つだけしか減らない。

$H \rightarrow H^* \rightarrow \cdots$ は、ガロア群の縮小の逆過程、つまり出発点のガロア群に戻る過程である。出発点のガロア群とは、有理数値の“根の関数”だけを不変に保ち、巾開方値の“根の関数”のどれをも、変化させる群だった。

3. $F_{S_n}(V)$ の分解因子の対称性が、系列 $S_n \supset A_n \supset \cdots$ に従う必然性

1) n 次方程式の根の関数を、より高対称な関数で表す手順

m 個の未知数からなる前頁、(4) 式から得た一般論 ($H \subset H^*$) :

H 対称関数を未知数とする連立方程式は、 H^* 対称関数の m 次巾開方形と等式で結ばれたが、1 つ例外があった。 $\omega = 1$ を代入した式は、 H^* 対称関数の有理式であり、次の段階へ持ち越される未知関数にならない。

$\{e\} \rightarrow H \rightarrow H_1 \rightarrow \cdots$ (左隣りが正規部分群) の系列で計算が実現すれば、求めるべき未知関数は n 個 $\rightarrow (n-1)$ 個 $\rightarrow (n-2)$ 個 $\cdots$ と減っていく。

4 次方程式の出発点では、2 段階の系列で未知関数が 1 個減った (29 頁)。その特殊事情を分析してみよう (29 頁の添え字表記は、ここと少し違う) :

「 $\alpha_0, \alpha_1, \alpha_2, \alpha_3$ 」を、2 組の 2 元連立方程式で「 $\alpha_0 + \alpha_1, \alpha_0 \alpha_1, \alpha_2 + \alpha_3, \alpha_2 \alpha_3$ 」に替えたとき、(4 根の扱いが不平等だから対称式が現れず) 未知数の個数は減少しない。

次に 2 組の 2 元連立方程式 (実質 4 元) で 4 根を平等に扱うと、2 つの基本対称式 $\alpha_0 + \alpha_1 + \alpha_2 + \alpha_3, \alpha_0 \alpha_1 \alpha_2 \alpha_3$ が現れ、未知数が 2 つ減った (連立方程式 1 組で 1 つ減る)。

一方、残る 2 つの未知数 $(\alpha_0 + \alpha_1) - (\alpha_2 + \alpha_3)$ と、 $\alpha_0 \alpha_1 - \alpha_2 \alpha_3$ から、3 つの未知数、 $\alpha_0 \alpha_1 + \alpha_2 \alpha_3, \alpha_0 \alpha_2 + \alpha_3 \alpha_1, \alpha_0 \alpha_3 + \alpha_1 \alpha_2$ を生じ、未知関数は 1 つ増えたから、差し引きで $4 \rightarrow 3$ 個に減り、2 組の 2 元連立方程式が、1 つの 3 元連立方程式になった。

2) 解公式の求め方が、 A_n (交代群) 対称関数を経由する必然性

n 次方程式の未知関数を、連立方程式によって、より高対称性の関数に書き換える手順が実現するなら、「 n 根すなわち n 個の未知関数 $\rightarrow n-1$ 個の未知関数 $\rightarrow 1$ 個ずつ減り $\cdots \rightarrow$ 遂に 2 個の非対称関数」になると分かった。

すなわち一般解が得られるなら、最後は、剰余類分割 $S_n = \{A_n, A_n(\text{互換})\}$ で求まる。

未知数の個数 = 連立方程式の元の数 = 巾開方次数 = “ $F(V)$ の因数分解で生じる因子の個数” だから、 $F_{S_n}(V)$ を分解する方向で言えば、2 分割 $\rightarrow$ 3 分割 $\rightarrow \cdots$ とならざるを得ない。 $F_{S_4}(V)$ では、2 分割 $\rightarrow$ 3 分割 $\rightarrow 2 \times 2$ 分割となる (4 次方程式の一般解法は、 $\sqrt{\quad}$ をとり $\rightarrow \sqrt[3]{\quad}$ をとり $\rightarrow \sqrt{\quad}$ を二度とり、 $\sqrt{\quad} \rightarrow \sqrt[3]{\sqrt{\quad}} \rightarrow \sqrt{\sqrt[3]{\sqrt{\quad}}}$)。

すなわち、ガロア群を分割する方向から解法を眺めると、 $S_n \supset A_n \supset \cdots \supset \{e\}$ であり、最初の分割は必然的に $F_{S_n}(V) = F_{A_n}(V) \times F_{\text{奇置換}}(V)$ 、と分かった。

3) 各根の対称性を高める、出発点で使う群

以上の理由で、 S_n に達しうる系列の群は、みな A_n の部分群になる (S_n に達するのを諦めるなら、つまり S_n よりも小さなガロア群をもつ方程式を解くときは、 A_n の部分群でない群を使うことができる)。

素数 n 次方程式を解く出発点「 n 文字巡回置換 $h; k \rightarrow k+1$ で生成される巡回群」の構造を見よう。 $h = (0\ 1\ \cdots\ n-1)$ と書けば、 $h = (0\ 1)(0\ 2)\ \cdots\ (0\ n-1)$ は、 $n-1$ 個の互換の積である。

n が素数なら $n-1$ は偶数だから、この群は確かに、 A_n の部分群である。

問題 n が偶数のとき、 $h; k \rightarrow k+1$ から生成される群 $\{k \rightarrow k+s\} = \{e, h, h^2, \dots, h^{n-1}\}$ が、 A_n の部分群にならない理由を述べよ。

答 $n-1$ が奇数だから、 $h = (0\ 1) \cdots (0\ n-1)$ は奇数ヶの積になり、この群の元 $h, h^2, h^3, \dots$ は奇置換と偶置換からなる (A_n の部分群でない)

4次方程式の解法を、4文字巡回群 $\{k \rightarrow k+s\}$ から出発したら、 A_4 に達しない。

6次方程式が非可解な理由：6根の対称性を高めるには、奇置換 $h = (0\ 1)(2\ 3)(4\ 5)$ を含めざるを得なかったから (87頁)、その先で A_6 に達しない (一般解法がない)。

§5 解ける素数次方程式の一般解法

p を素数とし、任意文字係数の $f_p(x) = x^p + c_{p-1}x^{p-1} + \dots + c_1x + c_0 = 0$ を解こう。

5次方程式で説明するが、 p 次でも同じである。

1. 5次方程式の解法

5根を“対称化”する出発点は、 $\theta_\omega = \alpha_0 + \omega\alpha_1 + \omega^2\alpha_2 + \omega^3\alpha_3 + \omega^4\alpha_4$ を使うことである。対称化の過程が、 A_5 対称関数に達しないことは知ったが、どこまで進めるかを考えよう (2章では類推だけだったが、ここでは必然性のある言葉で言い直す)。

θ_ω^5 を不変に保つ群は、 $h; k \rightarrow k+1$ が生成する、 $H = \{e, h, h^2, h^3, h^4\}$ である。

<記法1> 1の5乗根を $\omega, \omega', \omega'', \omega''', 1$ と書けば、各根の対称性を高める、5つの独立な式を得る (例えば原始根 $\omega, \omega' = \omega^2, \omega'' = \omega^3, \omega''' = \omega^4$ など)。

文字の簡単化のため、 θ_ω^5 を (ガロアに倣って) X_k と書こう。

$$X_1 = (\alpha_0 + \omega\alpha_1 + \omega^2\alpha_2 + \omega^3\alpha_3 + \omega^4\alpha_4)^5$$

$$X_2 = (\alpha_0 + \omega'\alpha_1 + \omega'^2\alpha_2 + \omega'^3\alpha_3 + \omega'^4\alpha_4)^5$$

$$X_3 = (\alpha_0 + \omega''\alpha_1 + \omega''^2\alpha_2 + \omega''^3\alpha_3 + \omega''^4\alpha_4)^5$$

$$X_4 = (\alpha_0 + \omega'''\alpha_1 + \omega'''^2\alpha_2 + \omega'''^3\alpha_3 + \omega'''^4\alpha_4)^5$$

$$X_5 = \alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = \text{既知の数値}$$

上記の関数はみな、 $H = \{e, h, h^2, h^3, h^4\}$ 対称性である。

$\alpha_0 \sim \alpha_4$ は、上の連立方程式を解き、次の未知量 $X_1 \sim X_4$ の巾解法を含む有理式で書かれるのだった。巾開方の取り方は、

$$\alpha_0 + \omega\alpha_1 + \dots + \omega^4\alpha_4 = {}_5\sqrt{X_1},$$

$$\alpha_0 + \omega'\alpha_1 + \dots + \omega'^4\alpha_4 = {}_5\sqrt{X_2},$$

$$\alpha_0 + \omega''\alpha_1 + \dots + \omega''^4\alpha_4 = {}_5\sqrt{X_3},$$

$$\alpha_0 + \omega'''\alpha_1 + \dots + \omega'''^4\alpha_4 = {}_5\sqrt{X_4}, \quad \text{のように対応づけてよい (25頁)}.$$

$$\alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = \text{既知数}$$

次に、4つの未知関数 $X_1 \sim X_4$ を、より対称性の高い関数の4次巾開方で表すのが課題になる。 $X_1 \sim X_4$ を相互変換させる巡回置換を見つけねばならない。その置換は、実は $X_1 \sim X_4$ の形そのものに内在していることが、以下の記法に書き直すと分かる。

<記法2> 剰余類の原始根 (51 頁) を使えば、記法 1 を、下記の形に書き直せる。この記法は、**根が素数 ω (素数次方程式) の場合にのみ可能**である。

ω を 1 の原始 5 乗根、**a** を **mod 5** の原始根 (例えば $a=2$) とすれば、添え字 1, 2, 3, 4 は、**a** の巾乗で、 $a^4=1$ 、 $a=2$ 、 $a^3=3$ 、 $a^2=4 \pmod{5}$ と書ける。

$$X_1 = (\alpha_0 + \omega \alpha_1 + \omega^2 \alpha_2 + \omega^3 \alpha_3 + \omega^4 \alpha_4)^5 \quad \text{下記で、} a^2, a^3 \text{ を } b, c \text{ と略記する}$$

$$X_a = (\alpha_0 + \omega \alpha_a + \omega^2 \alpha_{2a} + \omega^3 \alpha_{3a} + \omega^4 \alpha_{4a})^5 = X_2 = (\alpha_0 + \omega \alpha_2 + \omega^2 \alpha_4 + \omega^3 \alpha_1 + \omega^4 \alpha_3)^5$$

$$X_b = (\alpha_0 + \omega \alpha_b + \omega^2 \alpha_{2b} + \omega^3 \alpha_{3b} + \omega^4 \alpha_{4b})^5 = X_4 = (\alpha_0 + \omega \alpha_4 + \omega^2 \alpha_3 + \omega^3 \alpha_2 + \omega^4 \alpha_1)^5$$

$$X_c = (\alpha_0 + \omega \alpha_c + \omega^2 \alpha_{2c} + \omega^3 \alpha_{3c} + \omega^4 \alpha_{4c})^5 = X_3 = (\alpha_0 + \omega \alpha_3 + \omega^2 \alpha_1 + \omega^3 \alpha_4 + \omega^4 \alpha_2)^5$$

【根添え字の表 (mod 5)】

$$a, 2a, 3a, 4a = 2, 2 \times 2, 3 \times 2, 4 \times 2 \equiv 2, 4, 1, 3$$

$$b, 2b, 3b, 4b = 2^2, 2 \times 2^2, 3 \times 2^2, 4 \times 2^2 \equiv 4, 3, 2, 1$$

$$c, 2c, 3c, 4c = 2^3, 2 \times 2^3, 3 \times 2^3, 4 \times 2^3 \equiv 3, 1, 4, 2$$

X_1, X_2, X_4, X_3 を一括して、 $X_{(k)} = (\alpha_0 + \omega \alpha_{(k)} + \omega^2 \alpha_{2(k)} + \omega^3 \alpha_{3(k)} + \omega^4 \alpha_{4(k)})^5$ と書いてもよい。(k) は、 $(k) = 2^{k-1}$ の意味とする

記法 1 は、方程式の各根 α_k を固定して、 ω^k を配列替えしたことに相当し、

記法 2 は、1 の 5 乗根 ω^k を固定して、 α_k を配列替えした書き方である。

記法 1 の $\omega, \omega', \omega'', \omega'''$ はみな原始根だから、記法 2 の $\omega, \omega^2, \omega^3, \omega^4$ と同じである。

$\alpha_0 \sim \alpha_4$ は、全体として $\alpha_0, \alpha_a, \alpha_{2a}, \alpha_{3a}, \alpha_{4a}$ と同じ (a を、b, c と書いても同様) である。

つまり記法 1 の $X_1 \sim X_4$ と、記法 2 の X_1, X_a, X_b, X_c は、全体として同じである。

今から、根の置換による X_k の変換を調べたいので、 **X_k は、記法 2 で書いていることにする。**

< $X_1 \sim X_4$ の相互変換の仕方 >

問題# 配列「 X_1, X_2, X_4, X_3 」は、 $h'(k \rightarrow 2k)$ 、 $h'^2(k \rightarrow 2^2k)$ 、 $h'^3(k \rightarrow 2^3k)$ の作用で、どう変わるか

答 上記【添え字の表】から、0, 1, 2, 3, 4 が、 h' で 0, 2, 4, 1, 3 になる、などが分かる。

X_1, X_2, X_4, X_3 それぞれに、 h' を掛けると X_2, X_4, X_3, X_1

h'^2 を掛けると X_4, X_3, X_1, X_2

h'^3 を掛けると X_3, X_1, X_2, X_4

つまり X_1, X_2, X_4, X_3 の順送りになる（注： X_k の添え字は置換対象でない）

巡回置換、 $h'; k \rightarrow 2k$ で、 $H_1 = \{H, Hh', Hh'^2, Hh'^3\}$ を作ると、 H_1 は群であり、 H は H_1 の正規部分群である（証明は下記）。

問題 上のことを証明せよ。

答 $h'H = Hh'$ であることを確かめよう。mod 5 で計算する。

下記の「 」は、数列を見やすくしただけであり数学記号でない。

数列「0, 1, 2, 3, 4」に、 $h'; k \rightarrow 2k$ を作用させると「0, 2, 4, 1, 3」になり、さらに H の元 $h; k \rightarrow k+1$ を作用させると「1, 3, 0, 2, 4」になる。

右からの作用で、「0, 1, 2, 3, 4」 $h'h =$ 「1, 3, 0, 2, 4」と書こう。同様に、

$$\text{「0, 1, 2, 3, 4」 } h'h^2 = \text{「2, 4, 1, 3, 0」}$$

$$\text{「0, 1, 2, 3, 4」 } h'h^3 = \text{「3, 0, 2, 4, 1」}$$

$$\text{「0, 1, 2, 3, 4」 } h'h^4 = \text{「4, 1, 3, 0, 2」}$$

一方、「0, 1, 2, 3, 4」 $hh' =$ 「1, 2, 3, 4, 0」 $h' =$ 「2, 4, 1, 3, 0」である。

上と見比べて、 $hh' = h'h^2$ が分かる。

同様な計算を試みて、 $h'H = Hh'$ が分かる。この両辺に左から h' を掛け、 $h'^2H = h'Hh' = Hh'^2$ 、同様に、 $h'^3H = Hh'^3$ も分かる。したがって、 H は H' の正規部分群である。 $(Hh'^2)(Hh'^3) = Hh'$ など、剰余類群の掛け算規則も成り立つ。

$H_1 = \{H, Hh', Hh'^2, Hh'^3\}$ で不変になる関数を、 $X_1 \sim X_4$ から作れる。

すなわち、 H 対称関数 $X_1 \sim X_4$ が、 H_1 対称関数から計算できる。

（4 次方程式の解法を真似て、 X_1+X_2, X_1X_2 、と X_3+X_4, X_3X_4 から $X_1 \sim X_4$ を得ることはできない。 $X_1 \sim X_4$ は、5 文字置換群で変換され、4 文字置換群で変換される 4 次方程式の根の関数 $\alpha_1 + \alpha_2, \alpha_1\alpha_2, \alpha_3 + \alpha_4, \alpha_3\alpha_4$ の対称性とまったく違う）

2. 5 次方程式に解公式がない理由

方程式の一般解法では、下記の系列を“←方向”へ拡大しなければならない。

対称性をどこまで高められるかが、問題である。

$$\begin{array}{ccccc} ? \supset & H_1 = \{H, Hh', Hh'^2, Hh'^3\} & \supset & H = \{e, h, h^2, h^3, h^4\} & \supset & \{e\} \\ & h'; k \rightarrow 2k & & h; k \rightarrow k+1 & & e; k \rightarrow k \\ & Y_j (X_1 \sim X_4 \text{ の式}) & & X_1 \sim X_4 (\alpha_0 \sim \alpha_4 \text{ の式}) & & \alpha_0 \sim \alpha_4 \\ ? \leftarrow & \underline{H_1 \text{ 対称式にする}} & \leftarrow & \underline{H \text{ 対称性}} & \leftarrow & \underline{\{e\} \text{ 対称性}} \end{array}$$

$S_5 \supset A_5 \supset \cdots \supset H_1 \supset H \supset \{e\}$ の系列を左に辿り、 S_5 に達すれば根が求まる。

$X_1 \sim X_4$ から、 H_1 対称性の Y_j を作るのが、今の目標である。

H の元、 $h; k \rightarrow k+1$ は、巡回置換の記法で、 $(0\ 1\ 2\ 3\ 4)$ と書ける。

$h = (0\ 1\ 2\ 3\ 4) = (0\ 1)(0\ 2)(0\ 3)(0\ 4)$ は偶置換だから、 $H = \{e, h, h^2, h^3, h^4\}$ は、元がすべて偶置換、すなわち A_5 の部分群である。

一方、 $H_1 = \{H, Hh', Hh'^2, Hh'^3\}$ の元の中身をみてみよう。

問題 h', h'^2, h'^3 を、それぞれ互換の積に書き直せ

答 $h'; k \rightarrow 2k$ は、数列置換 $0, 1, 2, 3, 4 \rightarrow 0, 2, 4, 1, 3$ だから、 $(1\ 2)(1\ 3)(3\ 4)$ という奇置換である。 $h'^2 = (1\ 4)(2\ 3)$ は偶置換、 $h'^3 = (1\ 3)(1\ 2)(2\ 4)$ は奇置換。
すなわち、 H の元と Hh'^2 の元は、偶置換、 Hh' の元と Hh'^3 の元は、奇置換。

H_1 が A_5 の部分群でないから、5 次方程式の解法手順は A_5 に達しない。すなわち一般解が得られないと証明できた。

もっと直接的な証明、 H_1 が対称化手順の終点であることを次項で示す（4 次方程式について、87 頁で説明したのと同様のことを考える）。

3. 素数次方程式が解ける（ガロアの言葉による）必要十分条件

前節の “ Y_j ” の形を求めよう。すなわち $X_1 \sim X_4$ から H' 対称式を作る。

$y = X_1 + \zeta X_2 + \zeta^2 X_4 + \zeta^3 X_3$ とする（関数添え字の並び順は **1, 2, 4, 3**）。 $\zeta^4 = 1$

問題 $y = X_1 + \zeta X_2 + \zeta^2 X_4 + \zeta^3 X_3$ に、 α_k の添え字に関する巡回置換 ($k \rightarrow 2^t k$)、
 h', h'^2, h'^3 を作用させると、どのように変化するか。

答 $yh' = X_2 + \zeta X_4 + \zeta^2 X_3 + \zeta^3 X_1 = \zeta^3 (X_1 + \zeta X_2 + \zeta^2 X_4 + \zeta^3 X_3) = \zeta^3 y$

同様にして、 $yh'^2 = \zeta^2 y$ 、 $yh'^3 = \zeta y$

y^4 は、 H 対称関数 $X_1 \sim X_4$ から、 h', h'^2, h'^3 で不変になる形に作ったから、 H_1 対称性である。 y^4 に $\zeta^4 = 1$ の根 $1, -1, i, -i$ を代入した、 H_1 対称関数を $Y_1 \sim Y_4$ と命名し

$$Y_1 = (X_1 + X_2 + X_4 + X_3)^4$$

$$Y_2 = (X_1 - X_2 + X_4 - X_3)^4$$

$$Y_3 = (X_1 + iX_2 - X_4 - iX_3)^4$$

$$Y_4 = (X_1 - iX_2 - X_4 + iX_3)^4 \quad \text{が得られる。}$$

各 Y_j の中に、 $X_a = (\alpha_0 + \omega \alpha_a + \omega^2 \alpha_{2a} + \omega^3 \alpha_{3a} + \omega^4 \alpha_{4a})^5$ の形が入っている ($\omega^5 = 1$)。
 $\{(\omega^k \text{ を含む、根の 1 次式})^5 \pm (\text{同左})^5 \pm \dots\}^4$ に、根のどんな配列置換をしても、
 $\{(\omega^k \text{ を含む、根の 1 次式})^5 \pm i(\text{同左})^5 \pm \dots\}^4$ の形にならないのは明らかである。

± 1 と $\pm i$ の違いが、障害になっている。

$X_1 \sim X_4$ は、より高対称な $Y_1 \sim Y_4$ で表せたが、 $Y_1 \sim Y_4$ どうしを相互変換する置換は無いから、 $Y_1 \sim Y_4$ を、さらに高対称な関数で表すことはできない。

同じ障害が、素数 p 次方程式すべてに共通する。

p 々の関係式、 $\{\text{根の式}\}^p = \theta_k$ を作って対称性を高め、次に $p-1$ 々の関係式、 $\{\theta_k \text{ の式}\}^{p-1} = \theta_j$ を作る。これ以外に解きようがない。

すなわち、素数次方程式では、根の対称性を高める方法が、2段階で終わってしまう（3次方程式は2段階で解け、2次方程式は1段階で解けた）。

4次方程式では、根の関数の対称化が、4根の式でなく、2組の“2根の式”から出発できた（素数 p 通りの巾開方で扱えた）ので、上記の障害が回避された。

$Y_1 \sim Y_4$ は求まらないが、 $Y_1 \sim Y_4$ が既知量になっている5次方程式は解ける。

巾開方のとり方は、 $\sqrt[4]{Y_1} = X_1 + X_2 + X_4 + X_3$

$$\sqrt[4]{Y_2} = X_1 - X_2 + X_4 - X_3$$

$$\sqrt[4]{Y_3} = X_1 + iX_2 - X_4 - iX_3$$

$$\sqrt[4]{Y_4} = X_1 - iX_2 - X_4 + iX_3 \quad \text{と決められるから (25 頁)、}$$

$X_1 = 1/4 (\sqrt[4]{Y_1} + \sqrt[4]{Y_2} + \sqrt[4]{Y_3} + \sqrt[4]{Y_4})$ 、 $X_2 = 1/4 (\sqrt[4]{Y_1} - \sqrt[4]{Y_2} - i\sqrt[4]{Y_3} + i\sqrt[4]{Y_4})$ 、…などと簡単に解かれ、各根が、 $\sqrt[5]{X_1} \sim \sqrt[5]{X_4}$ から得られる。

5次方程式が解けるのは、 H_1 対称式 $Y_1 \sim Y_4$ に含まれる根の関数すべての値が既知（より高対称性の関数の巾開方から得られる数でなく、もとの方程式の係数から有理計算できる数、すなわち有理数）のときだけである。

つまり上の H_1 が、解ける5次方程式のガロア群である。

以後、 H_1 と書くと群一般の名と紛らわしいので、“解ける5次方程式のガロア群”を明示するため、Galois に因んで、 H_1 を Gal5 と呼ぶことにしよう。

5次の既約方程式では、 $F_{\text{Gal5}}(V)$ が有理係数になる場合にだけ、解が求まる。ガロアはこのことを、5次（ないし素数次）方程式が解ける必要十分条件と述べた。

注釈：ガロアは、「 $g(X) = (X - X_1)(X - X_2)(X - X_3)(X - X_4)$ の展開係数が有理数なら解ける」という言い方をした。「 Gal5 対称関数が有理数なら解ける」とことと同義である。 $X_1 \sim X_4$ は、 H 対称性、かつ h', h'^2, h'^3 で相互変換されるから、 $g(X) = \prod (X - X_k)$ は、 H_1 対称性（ Gal5 対称性）なのである。

5次方程式の“根の関数”のうち「 Gal5 対称関数」を、例えば上記の式の展開計算により、係数に現れる文字式として書き出したとする。それらが有理数かどうかを、

方程式の与えられた数値係数から、どうやって判定すればよいのだろうか？

4. 解ける 5 次方程式のガロア群（ガロア原著の記述法）

再掲 $\text{Gal}5 = H_1 = \{H, H h', H h'^2, H h'^3\}$ $h' = h'(k); k \rightarrow 2k$ ($k \rightarrow 3k$ でもよい)

$$H = \{e, h, h^2, h^3, h^4\} \quad h = h(k); k \rightarrow k+1 \pmod{5} \quad k=0,1,2,3,4$$

$\text{Gal}5 (= H_1)$ の元、 $h^s h'^t$ は、根の添え字を $k \rightarrow 2^t(k+s)$ に変換する。下記の表が見易い。数列 0, 1, 2, 3, 4 を、例えば 1, 2, 3, 4, 0 に変える元を、ガロア流に（原著は bcdea だが）12340 と書き、解ける 5 次方程式の $\text{Gal}5$ の元を書き並べよう。

元は、 $5 \times 4 = 20$ ケある（自分で書いてみると、理解に役立つ）

$\text{Gal}5 (= H_1)$ の元	$\times h'$	$\times h'^2$	$\times h'^3$
$e =$ 01234	02413	04321	03142
$\times h$ 12340	24130	43210	31420
$\times h^2$ 23401	41302	32104	14203
$\times h^3$ 34012	13024	21043	42031
$\times h^4$ 40123	30241	10432	20314

↑

この列をまず作り、それに h', h'^2, h'^3 を掛けて、右隣の各列を作った。

(H が、 $H_1 = \text{Gal}5$ の正規部分群だから、 h', h'^2, h'^3 を先に掛けてから、 h, h^2, h^3, h^4 を掛けても、元の全体は同じだが、表中の配置は変わる)

前節での記法を用い、 $F_{\text{Gal}5}(V)$ の因数分解が実現する過程を書けば、

$$F_{\text{Gal}5}(V) = F_H(V) = V^{20} - (V_1 + \cdots + V_{20}) V^{19} + \cdots + V_1 V_2 \cdots V_{20}$$

$$= F_H(V, r_1) F_{Hh'}(V, r_2) F_{Hh''}(V, r_3) F_{Hh'''}(V, r_4) \quad \text{計算対称に追加された } r_1 \sim r_4 \text{ は}$$

$$1 \text{ の } 4 \text{ 乗根と } X_1 \sim X_4 \text{ (すなわち } \sqrt[4]{Y_1} \sim \sqrt[4]{Y_4}) \text{ からなる}$$

$Y_1 \sim Y_4$ は有理数

次に、上記の因子のうち H 対称式、 $F_H(V, r_1)$ を因数分解する

$$F_H(V, r_1) = (V - V_1)(V - V_2)(V - V_3)(V - V_4)(V - V_5) \quad \text{計算対象に追加された関数は}$$

$$\sqrt[5]{X_1} \sim \sqrt[5]{X_4} \text{ と } 1 \text{ の } 5 \text{ 乗根からなる}$$

根 $\alpha_0 \sim \alpha_4$ は、 $\sqrt[5]{X_1} \sim \sqrt[5]{X_4}$ で書かれ、 $X_1 \sim X_4$ は、 $\sqrt[4]{Y_1} \sim \sqrt[4]{Y_4}$ で書かれる。

$Y_1 \sim Y_4$ に含まれる根の関数を $\theta = \theta(\alpha_0, \alpha_1, \alpha_2, \alpha_3, \alpha_4)$ と総称すれば、

θ が、みな有理数になる方程式は解ける、と言える。或る 5 次方程式の係数が数値で与えられたとき、 θ が有理数になるかどうかの判定法を考えよう。

5. 係数が数値で与えられた素数次方程式が、解けるかどうかの判定法；

ガロアが述べた、 $(n-2)!$ 次の補助方程式の意味

1) $F_{\text{Gal5}}(V)$ の係数が有理数になるかどうかの判定法

5 次方程式 $f(x)=0$ が、数値係数で与えられたとき、それらの数値を頼りに、
 $F_{\text{Gal5}}(V) = V^{20} - (V_1 + \cdots + V_{20}) V^{19} + \cdots + V_1 V_2 \cdots V_{20}$
の係数（に含まれる根の関数）が有理数かどうか判定したい。まず次の問題を解く。

問題 5 文字対称群 S_5 を、ガロア群 Gal5 で剰余類分割せよ

Gal5 の元が、96 頁表の 20 ケであることを利用する： S_5 の元は $5! = 120$ ケ、 Gal5 の元は 20 ケだから、 $120 \div 20 = 6$ ケの剰余類に分かれる（ラグランジュの定理）。

答 Gal5 の元でない S_5 の元を、まず 1 つ選び（ $120 - 20 = 100$ 種類のうちのどれでもよい）、他の 5 ケを 44 頁の方法で次々に選べばよい。

Gal5 の元は、5 根または 4 根の添え字を一斉に変えるのだから、例えば 2 根だけの入れ替え（互換）という置換は、明らかに Gal5 の元でない。

互換 (01) を選ぼう（ガロアの記法では 10234 と書かれ、当然、表中にない）。

表の 20 ケの元に (01) を掛けると、どれも表にない元になる（群 H の元に、 H 以外の元を掛けたら H の元にならない。これは群の基本性質だった；43 頁）。

次に、 Gal5 の元でなく、 $\text{Gal5}(01)$ の元でもないもの、として類推すれば、例えば (02) を選べる。同様に (03)、(04) を選び、残りは (12)(34) としよう。

したがって剰余類分割は（分割法は一意的だが、書き表し方は色々あり）例えば、

$$S_5 = \{\text{Gal5}, \text{Gal5}(01), \text{Gal5}(02), \text{Gal5}(03), \text{Gal5}(04), \text{Gal5}(12)(34)\}$$

注) Gal5 は A_5 の部分群でないから（前述）、上記の剰余類分割は、一般解法につながらない。置換集合、 $\{e, (01), (02), (03), (04), (12)(34)\}$ は群でない。

$F_{\text{Gal5}}(V)$ の係数が含む“根の非対称関数”の、任意の 1 つを $\theta = \theta(\alpha_0, \alpha_1, \alpha_2, \alpha_3, \alpha_4)$ と呼ぶ。 θ を、(01)、(02)、(03)、(04)、(12)(34) のそれぞれで置換した 5 ケの関数を作り、 θ_{01} 、 θ_{02} 、 θ_{03} 、 θ_{04} 、 θ_{1234} と呼ぼう（ $\alpha_0 \sim \alpha_4$ で実際に書けるが、20 次式だから想像するだけで十分であろう）。

θ の定義から、「 θ を Gal5 の元で置換した根の関数」= θ である。

S_5 の元は、上記の剰余類分割の形で書き尽くされている。

すると、 θ を S_5 の任意元で置換したら、 θ 、または θ_{01} 、 θ_{02} 、 θ_{03} 、 θ_{04} 、 θ_{1234} 、

計 6 ケのうちのどれかに必ずなり、他の関数形にはならないと分かる。

問題 $\theta_{01} \sim \theta_{1234}$ は互いに異なることを示せ。

答 もし $\theta_{01} = \theta_{02}$ 、すなわち $\theta(0\ 1) = \theta(0\ 2)$ なら、 $\theta = \theta(0\ 2)(0\ 1)$ 、すると $(0\ 2)(0\ 1) = (0\ 2\ 1) \in \text{Gal}_5$ 、となるが、3 文字巡回置換は Gal_5 の元でない。したがって $\theta_{01} \neq \theta_{02}$ 、他も同様にして、互いに異なることがいえる。

問題 $\theta_{01}, \theta_{02}, \theta_{03}, \theta_{04}, \theta_{1234}$ を S_5 の元で置換すると、どんな関数になるか。

答 $g \in S_5$ とする。例えば、 $\theta_{01} g = \theta(0\ 1) g = \theta g'$ ($g' \in S_5$) だから、 $\theta, \theta_{01} \sim \theta_{1234}$ のどれかになり、他も同様。もし、 $\theta_{01} g = \theta_{02} g$ つまり $\theta(0\ 1) g = \theta(0\ 2) g$ なら、 $\theta = \theta(0\ 2) g \{(0\ 1) g\}^{-1} = \theta(0\ 2) g g^{-1}(0\ 1) = \theta(0\ 2)(0\ 1)$ となり、これは前問と同様成り立たないから、 $\theta_{01} g \neq \theta_{02} g$ なども分かる。

$\theta, \theta_{01}, \theta_{02}, \theta_{03}, \theta_{04}, \theta_{1234}$ を、 S_5 の任意元で置換すると、相互に移り変わり、6 ケ 1 組は全体として変わらないことが分かった。したがって以下が分かる。

2) 或る 5 次方程式が解けるかどうかの判定式 (ガロアは補助方程式と呼んだ)

$F_\theta(X) = (X - \theta)(X - \theta_{01})(X - \theta_{02})(X - \theta_{03})(X - \theta_{04})(X - \theta_{1234})$ を作ると、

$$= X^6 - (\theta + \theta_{01} + \theta_{02} + \theta_{03} + \theta_{04} + \theta_{1234}) X^5 + \cdots + \theta \theta_{01} \theta_{02} \theta_{03} \theta_{04} \theta_{1234} = 0$$

S_5 のどの元を作用させても $F_\theta(X)$ は不変、つまり S_5 対称性である。すると $F_\theta(X)$ の係数は、根 $\alpha_0 \sim \alpha_4$ の対称式で表せる。したがって、方程式 $f_5(x) = 0$ の係数が数値で与えられたとき、その数値を代入すれば、 $F_\theta(X)$ は具体的な既知数値の 6 次多項式となる (実際に書ける)。(S_5 の位数 5!) $\div$ (ガロア群の位数 5×4) = 6

θ は $F_\theta(X) = 0$ の解だから、 θ が有理数なら下記の有理的な因数分解で求まる。

$$F_\theta(X) = (X - \theta) \{X^5 - (\theta_{01} + \theta_{02} + \theta_{03} + \theta_{04} + \theta_{1234}) X^4 + \cdots - \theta_{01} \theta_{02} \theta_{03} \theta_{04} \theta_{1234}\} = 0$$

6 次方程式の解法は必要なく、有理数解は、あれば求まる (10 頁参照)。

ところで、 θ が有理根のとき、上記の因子 $\{X^5 - \cdots\}$ も可約になるだろうか？

注：“根の或る関数が求まるなら、既約方程式の根の平等性から、根を名称変更した関数も求まる”と言えるが、これは文字計算できる原理がある場合の話である。今の場合、 θ の有理数値は文字計算で得るのではないから、 $\theta_{01} \sim \theta_{1234}$ も求まる (有理数になる) とはいえない。

問題： $\theta_{01} \sim \theta_{1234}$ はどれも、ガロア群 Gal_5 対称性でないことを示せ

答 定義 $\theta_{01} = \theta(0\ 1)$ より、 $\theta_{01} \text{Gal}_5 = \theta(0\ 1) \text{Gal}_5$ 、一方、 θ は Gal_5 対称式だから、 $\theta = \theta \text{Gal}_5$ 、すると $\theta_{01} = \theta(0\ 1) = \theta \text{Gal}_5(0\ 1)$ 。ところが、 $(0\ 1) \text{Gal}_5 \neq \text{Gal}_5(0\ 1)$ なのだから、 $\theta_{01} \text{Gal}_5 \neq \theta_{01}$ と分かる。同様に $\theta_{02} \text{Gal}_5 \neq \theta_{02}$ 、 $\cdots$ 、 $\theta_{1234} \text{Gal}_5 \neq \theta_{1234}$

$\theta_{01} \sim \theta_{1234}$ は、Gal5 対称性でないと分かったから、ガロア群の定理（69 頁）によれば、Gal5 対称関数から有理計算できない（ $\theta_{01} \sim \theta_{1234}$ は有理数でない）ことが分かる。Gal5 対称関数とは、 $F_{\text{Gal5}}(V)$ の係数成分すなわち既知数（有理数）である。

$F_{\theta}(X)=0$ に有理根 θ が見つからなければ、その 5 次方程式 $f_5(x)=0$ は解けないと分かる。 $f_5(x)=0$ が文字係数で与えられたら、以上の判定法は実行できない。

3) 5 次方程式の解き方のまとめ；再掲

5 次方程式 $f_5(x)=0$ の係数が、数値で与えられた場合、解けるかどうかの判定法と、解けるときに根の数値を求める方法は、以下のようである。

以下は、文字式のコンピュータプログラムで実行できるであろう。

- 1) $f_5(x)=0$ の根 $\alpha_0 \sim \alpha_4$ の文字式で、 $X_1 \sim X_4$ を書く。 ω は 1 の原始 5 乗根
92 頁の表記、 $X_{(k)} = (\alpha_0 + \omega \alpha_{(k)} + \omega^2 \alpha_{2(k)} + \omega^3 \alpha_{3(k)} + \omega^4 \alpha_{4(k)})^5$ は未知数； $(k) = 2^{k-1}$
 $X_5 = \alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4$ は、既知数
 - 2) $Y_1 \sim Y_4$ を作る。 $Y_j = (X_1 + \zeta X_2 + \zeta^2 X_4 + \zeta^3 X_3)^4$ 、 $\zeta^4 = 1$ の 4 根を ζ に代入する。
右辺に現れる“ $\alpha_0 \sim \alpha_4$ の非対称関数”をすべてリストアップする（ θ と総称する）。
 - 3) それらの θ から前記のように文字式で、それぞれの $F_{\theta}(X)$ を作る。
 $F_{\theta}(X)$ の係数は必ず根 $\alpha_0 \sim \alpha_4$ の対称式になるから、基本対称式に書き直し、
もとの方程式 $f_5(x)=0$ の係数値（与えられた数値）を代入する。
 - 4) 数値係数で書けた $F_{\theta}(X)=0$ が、有理根をもつかどうか数値計算する（10 頁）。
その有理根が、 θ である。
 - 5) 総称した θ のすべてについて有理数値が得られた場合、 $f_5(x)=0$ は解ける。
それらすべての θ の数値を $Y_1 \sim Y_4$ に代入する（戻す）。
 - 6) 各 $X_1 \sim X_4 = \sqrt[4]{Y_1} \sim \sqrt[4]{Y_4}$ の連立 1 次方程式の解」の形で数値を得る
各 $\alpha_0 \sim \alpha_4 = \sqrt[5]{X_1} \sim \sqrt[5]{X_4}$ 、および X_5 を含む連立 1 次方程式の解」を得る
 $\sqrt[5]{\{ \sqrt[4]{(\text{有理数値})} \text{を含む有理式} \}}$ を含む有理式が、1 の 5 乗根 ω と 1 の 4 乗根 i を
使って書かれる。
-

すなわち 5 次方程式では、係数の数値の与えられ方により、根を数値で答えられるが、係数の文字式では表せない（解公式が書けない）。

4) 素数 n 次への一般化：解ける方程式の群

5 次方程式とまったく同様に、解ける素数 n 次方程式のガロア群は（前述の命名に倣って Gal と書こう）、 $n(n-1)$ ケの元をもつ下記のものである。

$\text{Gal} = (H, H h', \dots, H h'^{n-2}) \quad h' = h'(k); \quad k \rightarrow a k \quad a \text{ は、mod } n \text{ の原始根}$

$H = \{e, h, h^2, \dots, h^{n-1}\} \quad h = h(k); \quad k \rightarrow k+1 \quad k=0, 1, 2, \dots, n-1$

Gal の元は、 $k \rightarrow a^t(k+s)$ と書ける ($s=0, 1, \dots, n-1; \quad t=0, 1, \dots, n-2$)。

s と t の値が決まれば置換元が決まる、または $k \rightarrow q k+r$ と書けば q と r という 2 つの値で、置換 $\alpha_k \rightarrow \alpha_{qk+r}$ が決まる。添え字 k が、1 次式で変換されるので、 Gal を線形群ともいう。すなわち、

解ける素数次方程式のガロア群 (Gal) は、線形群である。

問題 任意文字係数の 3 次方程式のガロア群は、線形群であることを示せ。

答 このガロア群は、すでに知ったように S_3 である。

$S_3 = \{H, H(1\ 2)\}, \quad H = \{e, (1\ 2\ 3), (1\ 2\ 3)^2\} = \{e, h, h^2\}$ と書くと、

$h; k \rightarrow k+1, \quad (1\ 2) = h'; k \rightarrow 2k, \quad (\text{mod } 3) \quad k=0, 1, 2$ である。

したがって S_3 の元は、 $k \rightarrow 2^s(k+t) = qk+r$ の形になる。

すなわち、 **S_3 は線形群なので、3 次方程式は常に解ける。**

S_4 は線形群でないのに、4 次方程式は常に解ける。一般理論の応用問題と言える。

5) 数値係数の、素数 n 次方程式が解けるかどうかの判定式 $F_\theta(X)$

* 99 頁に表記したことを n 次に一般化し、 $X_1 \sim X_{n-1}$ 、次いで $Y_1 \sim Y_{n-1}$ を作り、展開式の中の根の関数をすべて書き出す (θ と総称)。

* $S_n = \{\text{Gal}, \text{Gal } g_1, \text{Gal } g_2, \dots, \text{Gal } g_{m-1}\}$ となる元 $g_1 \sim g_{m-1}$ を選び (部分群による剰余類分割は、常に可能である)、 $\theta g_k = \theta_k$ を作る。

* $F_\theta(X) = (X - \theta)(X - \theta_1) \cdots (X - \theta_{m-1})$ を作る。 $m = n! / n(n-1) = (n-2)!$ 次式になる。 $n!$ は S_n の位数、 $n(n-1)$ は Gal の位数である。

* すべての $F_\theta(X) = 0$ が有理数解をもつかどうかは、前項と同様の計算 (10 頁) で確認できる。

ガロアは、「 **$(n-2)!$ 次の補助方程式が有理解をもつかどうか**で、もとの方程式が解けるかどうか分かる。それは、やればできる」とだけ記したので、理解困難だった。補助方程式とは、我々が判定式と名付けた $F_\theta(X)$ を指す筈である。

3 次方程式で、 $F_\theta(X)$ は 1 次式になるから、 $F_\theta(X) = 0$ は必ず有理解をもつ。

§ 6 素数次方程式が解ける条件の別な表現

1. 解ける素数次既約方程式の各根 α_k は、任意 2 根の 1 次式を使った整式で、 $\alpha_k = \psi_k(V) = \psi_k(A \alpha_i + B \alpha_j)$ と表せる

偶数次の既約方程式 $f(x) = 0$ が実根をもつとき、実根は偶数ヶになることが、

x - y 平面で $y=f(x)$ のグラフを思い浮かべると分かる。2 つの実根で虚根を“有
理的”には表せないから、上記の定理は、偶数次方程式に当てはまらない。

1) 各根が任意 2 根の有理式（整式）で書けることの意味

ガロアが論文の最後に記したのは、「各根を、任意 2 根の 1 次式で有理的に表せる
ことが、素数次方程式が解けることと同等」、という定理であった。

すなわち、 $V=A\alpha_i+B\alpha_j$ で、 n 根を $\alpha_0=\psi_0(V)$ 、 $\alpha_1=\psi_1(V)$ 、 $\cdots$ 、 $\alpha_{n-1}=\psi_{n-1}(V)$
と整式で書けることと、 n （素数）次方程式が解けることが同等、となる。

$\alpha_k=\psi_k(V)=\psi_k(A\alpha_i+B\alpha_j)$ と書ければ、この関係を保存する置換で V は変化する。

54-58 頁で関係式、 $\alpha_k=\varphi_k(V)=\varphi_k(A_0\alpha_0+\cdots+A_{n-1}\alpha_{n-1})$ を証明した。この式で、 A_i
と A_j 以外の A_k に 0 を代入したら φ_k が ψ_k になる、ということではない。 $A_k=0$ と
したら、 $\varphi_k(V)$ の導き方の前提に反する。新たな等式、 $\alpha_k=\psi_k(A\alpha_i+B\alpha_j)$ を示そう。

2) 解ける素数次方程式のガロア群（前記の Gal）では、2 根の配置を指定する と、置換元が 1 つに決まること

ガロアは、「解ける方程式では、根の配列が、2 根を決めるだけで決まってしまう」
から「各根が 2 根で表せる」と言った。この後半は謎々のようなものである。

根の配列とは、 $V=A_0\alpha_0+A_1\alpha_1+\cdots+A_{n-1}\alpha_{n-1}$ の中の配置と思えばよい。

2 根の指定で配列が決まるとは、下記の意味である：

線形群の元は、根の添え字を $k \rightarrow qk+r$ に変えるので、 k の値（根の名）を 2 つ
指定すれば q 、 r の値が（置換元が）決まり、ほかの添え字置換もすべて決まる。

96 頁の表（解ける 5 次方程式のガロア群 Gal5 の元一覧）を見直してみよう。

例えば初めの 2 文字が、1, 2 である元 12□□□ を搜すと 12340 のみ、21□□□ なら
21043 のみ、一方、2□□□1 なら 23401 のみ、なども分かる。任意に選んだ 2 数
（例えば 1 と 2）が、どの 2 箇所にも見つかる。この意味は後で考察する。

3) 解ける 5 次方程式では、2 根を計算対象に追加すると、全根を有理計算で きてしまうことの証明

例えば「 α_0 と α_1 」で、5 根 $\alpha_0 \sim \alpha_4$ を表す方法を考えよう

* 96 頁の表を見る。20 枚のカードから好きな 1 枚を選ぶように、例えば右下隅の
ものを選んでみると、20314 である。根添え字の自然数列 0, 1, 2, 3, 4 が、この 20314
で置換された V を V_a と名付けよう。

$V_a=A_0\alpha_2+A_1\alpha_0+A_2\alpha_3+A_3\alpha_1+A_4\alpha_4$ α_0 は A_1 に、 α_1 は A_3 に配置されている。

* V_a は定義から、 $F_{\text{Gal5}}(V) = 0$ の解である。 $F_{\text{Gal5}}(V)$ は、 $5 \times 4 = 20$ 次式である。

$$F_{\text{Gal5}}(V) = \Pi_{\text{Gal5}}(V - V_k) = V^{20} + C_{19}V^{19} + \cdots + C_1V + C_0 = 0 \quad n = 5$$

Gal5 がガロア群だから、係数は有理数である。 $\alpha_0 \sim \alpha_4$ は解ける方程式の根であり、99頁の方法で値が得られるのだから、 $C_{19} \sim C_0$ は既知数である（と言えるだけでよく、今の証明のために計算する必要はない）。

* 一方、 V_a を解にもつ、もう一つの関数を創作する。

$V - V_a = V - (A_0\alpha_2 + A_1\alpha_0 + A_2\alpha_3 + A_3\alpha_1 + A_4\alpha_4)$ に対し、 α_0 と α_1 を固定して、他の 3 根のすべての置換 ($3! = 6$ とおり) を行なって掛け合わせたものを作る。

根の添え字 0 と 1 を固定したことに因んで、 $F^{01}(V)$ と書こう。

$$\begin{aligned} F^{01}(V) &= \Pi \{V - (A_0\Box + A_1\alpha_0 + A_2\Box + A_3\alpha_1 + A_4\Box)\} \quad \Box \text{ への } \alpha_2, \alpha_3, \alpha_4 \text{ の} \\ &= \Pi [\{V - (A_1\alpha_0 + A_3\alpha_1)\} - (A_0\Box + A_2\Box + A_4\Box)] \quad \text{入れ方は } 3! \text{ 通り} \\ &= \{V - (A_1\alpha_0 + A_3\alpha_1)\}^6 + D_5\{V - (A_1\alpha_0 + A_3\alpha_1)\}^5 + \cdots + D_1\{V - (A_1\alpha_0 + A_3\alpha_1)\} + D_0 \end{aligned}$$

係数 $D_5 \sim D_0$ は、 $\alpha_2, \alpha_3, \alpha_4$ の基本対称式からなる。… (1)

$$\text{例えば、} D_5 = 2(A_0 + A_2 + A_4)(\alpha_2 + \alpha_3 + \alpha_4)$$

$$\begin{aligned} f_5(x) / (x - \alpha_0)(x - \alpha_1) &= \{(x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0) \div (x - \alpha_0)\} \div (x - \alpha_1) \text{ を計算し、} \\ &= (x - \alpha_2)(x - \alpha_3)(x - \alpha_4) \text{ と比べると、} \end{aligned}$$

$\alpha_2, \alpha_3, \alpha_4$ の基本対称式が、根 α_0 と α_1 、有理数 $c_4 \sim c_0$ で書ける。… (2)

(1)、(2) から、 $F^{01}(V)$ の係数 $D_5 \sim D_0$ は、2 根 α_0, α_1 、方程式 $f_5(x) = 0$ の係数、および適当に決めた $A_0 \sim A_4$ の文字式で書かれることが分かった。

一方、 $F_{\text{Gal5}}(V)$ の係数 $C_{19} \sim C_0$ は、前述のように値が分かった有理数である。

* $F_{\text{Gal5}}(V) = 0$ の解で、 $V = A_0\Box + A_1\alpha_0 + A_2\Box + A_3\alpha_1 + A_4\Box$ の形になるのは唯一、 $V_a = A_0\alpha_2 + A_1\alpha_0 + A_2\alpha_3 + A_3\alpha_1 + A_4\alpha_4$ のみ。

一方、 $V = A_0\Box + A_1\alpha_0 + A_2\Box + A_3\alpha_1 + A_4\Box$ の形のものが、すべて解になるように作った方程式が、 $F^{01}(V) = 0$ である。

したがって、 V_a が、 $F^{01}(V) = 0$ と $F_{\text{Gal5}}(V) = 0$ の、唯一の共通解になる。

するとユークリッドの互除法で、共通因子 $(V - V_a)$ が算出できる。

補足) $5!$ 次式 $F(V) = \Pi \{V - (A_0\Box + A_1\Box + A_2\Box + A_3\Box + A_4\Box)\} = 0$ もまた、 V_a を解にもつ既知係数の方程式だが、これは、 $F_{\text{Gal5}}(V) = 0$ の解すべてを含んでいる。つまり $F_{\text{Gal5}}(V)$ が $F(V)$ を割り切り、 V_a は求まらない。

$F_{\text{Gal5}}(V) = 0$ と“唯一の”共通解をもつ V 方程式は、2 根を計算対象に含めたときにのみ作れる、と分かる。

前述のガロアの言葉、「解ける方程式では、根の配列が、2根を決めるだけで決まってしまうから、各根が2根で表せる」という意味が分かり始めた。

* 係数が既知の数値である2つの多項式、6次式 $F^{01}(V)$ と、20次式 $F_{\text{Gal5}}(V)$ の互除法を、 V の1次式の割り算になるまで続けて最後に、余り=0と結論する。

互除法の計算結果は(14頁の書き方で)、

$\{V \text{ の 2 次式, } V - \theta_a(\alpha_0, \alpha_1)\} = 0$ となり、共通因子は $V - \theta_a(\alpha_0, \alpha_1)$ である。

$V - \theta_a(\alpha_0, \alpha_1) = 0$ の解が V_a だから、 $V_a = \theta_a(\alpha_0, \alpha_1)$ となる。

(この式は、 α_0 、 α_1 、および既知の有理数 $c_4 \sim c_0$ 、 $A_0 \sim A_4$ からなる)

$V_a = A_0 \alpha_2 + A_1 \alpha_0 + A_2 \alpha_3 + A_3 \alpha_1 + A_4 \alpha_4 = \theta_a(\alpha_0, \alpha_1)$ と書ける計算原理が分かった。

* 次に、また96頁表で、20枚のカードから好きな2枚を選ぶように、他の2つを選ぶ。例えば最後の行の 30241、10432 を使ってみよう。同様の計算原理で

$$V_b = A_0 \alpha_3 + A_1 \alpha_0 + A_2 \alpha_2 + A_3 \alpha_4 + A_4 \alpha_1 = \theta_b(\alpha_0, \alpha_1)$$

$$V_c = A_0 \alpha_1 + A_1 \alpha_0 + A_2 \alpha_4 + A_3 \alpha_3 + A_4 \alpha_2 = \theta_c(\alpha_0, \alpha_1) \quad \text{のように書ける。}$$

$$\text{すなわち、} \quad A_0 \alpha_2 + A_2 \alpha_3 + A_4 \alpha_4 = \theta_a(\alpha_0, \alpha_1) - A_1 \alpha_0 - A_3 \alpha_1$$

$$A_0 \alpha_3 + A_2 \alpha_2 + A_3 \alpha_4 = \theta_b(\alpha_0, \alpha_1) - A_1 \alpha_0 - A_4 \alpha_1 \quad \dots \star$$

$$A_2 \alpha_4 + A_3 \alpha_3 + A_4 \alpha_2 = \theta_c(\alpha_0, \alpha_1) - A_1 \alpha_0 - A_0 \alpha_1$$

この連立方程式を解いて、 α_2 、 α_3 、 α_4 を、 α_0 、 α_1 の有理式で表せることが分かった(各根を表す式の中で、 $A_0 \sim A_4$ の値は相互の比としてのみ寄与する)。

4) 2根、 α_0 、 α_1 を、 $V = A \alpha_0 + B \alpha_1$ の有理式で表す方法

α_2 、 α_3 、 α_4 は連立1次方程式 $\star$ を解いて得られるから、 α_0 、 α_1 を1つの V で表せたら、全根が $V = A \alpha_0 + B \alpha_1$ で表せることになる。下記のアイデアが湧く。

重根のない任意の n 次方程式 $f_n(x) = x^n + c_{n-1}x^{n-1} + \dots + c_1x + c_0 = 0$ 、の任意根は、その任意根自身と、他の任意1根の2つで、有理的に表せる(定理が言う、任意に指定した“共通の”2根で全根を表わすのとは全く違う話である)。

例えば、 $\alpha_0 = Q_0(A \alpha_0 + B \alpha_m)$ と書けることを示そう。

Q_0 は整式を意味し、 α_m は α_0 以外の任意根である。

証明)

$V - (A \alpha_0 + B \alpha_m) = 0$ の左辺で α_0 を固定し、他の根すべてを変えた掛け算を作る。

$$F_0(V) = \prod_j \{V - (A \alpha_0 + B \alpha_j)\} = \prod_j \{(V - A \alpha_0) - B \alpha_j\}$$

$$= (V - A \alpha_0)^{n-1} - B(\alpha_1 + \dots + \alpha_{n-1})(V - A \alpha_0)^{n-2} + \dots \pm B^{n-1} \alpha_1 \dots \alpha_{n-1} = 0$$

$(V - A \alpha_0)$ の $n-1$ 次式である $F_0(V)$ の係数は、 $\alpha_1 \sim \alpha_{n-1}$ の基本対称式で表せる。

そして、 $\alpha_1 \sim \alpha_{n-1}$ の基本対称式は、 $f_n(x)/(x - \alpha_0) = (x - \alpha_1) \dots (x - \alpha_{n-1})$ の両辺を見比

べれば、 $f_n(x)$ の係数 $c_{n-1} \sim c_0$ 、および根 α_0 で表せる。

したがって $F_0(V) = F_0(V, \alpha_0)$ と書いて、

x の方程式 $F_0(V, x) = 0$ と $f_n(x) = 0$ が、根 $x = \alpha_0$ を共有することが分かる。

$F_0(V, \alpha_0)$ で、 α_0 を α_k ($k \neq 0$) に置き換えたら、 $F_0(V, \alpha_k) = \prod_j \{V - (A \alpha_k + B \alpha_j)\}$ となるが、 $A \alpha_k + B \alpha_j$ は、 $F_{01}(V) = 0$ の解 $A \alpha_0 + B \alpha_j$ と異なるから、 $F_0(V, \alpha_k) \neq 0$ である。

したがって、 $x = \alpha_0$ は、 $F_0(V, x) = 0$ と $f_n(x) = 0$ の唯一の共通根である。

x の多項式 $F_0(V, x)$ の係数は、 V 、根 α_0 、および有理数 ($c_{n-1} \sim c_0$ 、 A 、 B) で書き表されているので、 $F_0(V, x)$ と $f_n(x)$ の互除法により、共通根 $x = \alpha_0$ が「 V の有理式」の形で求まる (この有理式は、整式に書き直せるのであった ; 58 頁)。

すなわち、 $\alpha_0 = Q_0(V) = Q_0(A \alpha_0 + B \alpha_m)$ という整式が書ける。

まったく同じ議論で、 A 、 B の役目を交換し、今度は α_1 を固定して他の根すべてを変えた掛け算で、 $F_1(V) = \prod_j \{(V - B \alpha_1) - A \alpha_j\}$ を作れば、

$\alpha_1 = Q_1(A \alpha_k + B \alpha_1)$ が示せる。 α_k は、 α_1 以外の任意根

前述と合わせ、 $\alpha_0 = Q_0(A \alpha_0 + B \alpha_m)$ 、 $\alpha_1 = Q_1(A \alpha_k + B \alpha_1)$ 、 $m=1$ 、 $k=0$ とすれば
 $\alpha_0 = Q_0(A \alpha_0 + B \alpha_1)$ 、 $\alpha_1 = Q_1(A \alpha_0 + B \alpha_1)$ になる。1 組の恒等式が得られた。

* 前記☆ に、 $\alpha_0 = Q_0(A \alpha_0 + B \alpha_1) = Q_0(V)$ 、 $\alpha_1 = Q_1(A \alpha_0 + B \alpha_1) = Q_1(V)$ を代入し、 α_2 、 α_3 、 α_4 も、 $V = A \alpha_0 + B \alpha_1$ の整式で表されることが分かる。

したがって、定理の前半が証明された。

5 次方程式で証明したが、素数次方程式一般でも方法は同様と分かるであろう。

2. $\alpha_k = \psi_k(A \alpha_i + B \alpha_j)$ の関係を保存する置換群は、解ける方程式のガロア群である

今までの話の逆 (定理の後半) を証明しよう。関係式 $\alpha_k = \psi_k(V) = \psi_k(A \alpha_i + B \alpha_j)$ を、保存する置換群が、線形群 ($k \rightarrow qk + r$, Gal5 : 96 頁) になることを示したい (置換は根の添え字に作用する。 ψ_k の添え字を置換してはいけない注意点は前述した)。

1) 任意 2 根の 1 次式、 $V = A \alpha_i + B \alpha_j$ を必ず変化させる置換 “群”

関係式 $\alpha_k = \psi_k(V)$ を保存する置換は、(e 以外は) V を必ず変化させ、その置換集合は群を成す (62 頁)。

$\alpha_k = \psi_k(A \alpha_i + B \alpha_j)$ を保存する置換がなす群を G と呼び、元 g の形を考えよう。

g で変化しない文字が 2 ケ以上あると、「或る α_i 、 α_j が不変、 $V = A \alpha_i + B \alpha_j$ が不変」ということがおきるから、 g は $(n-1)$ ケ以上の根を変化させねばならない。

問題 根配列 $\alpha_0, \alpha_1, \alpha_2, \alpha_3, \dots$ を、添え字数列 $0, 1, 2, 3, \dots$ または文字で書く

$g_1, g_2 \in G$ だとして、 $0, 1, 2, 3, 4, \dots$ が、

g_1 で $a, b, c, d, e, \dots$ に置換され、一方、

g_2 で $a, b, p, q, r, \dots$ に置換されたとする

すると $g_1 = g_2$ であること、すなわち 2 文字の対応「 $0, 1, \dots \rightarrow a, b, \dots$ 」を決めると、文字列（置換結果）は 1 通りに決まってしまうことを示せ。

ヒント $V = A\alpha_0 + B\alpha_1$ で書いた関係式、 $\alpha_0 = \psi_0(V)$ 、 $\alpha_1 = \psi_1(V)$ 、 $\alpha_2 = \psi_2(V)$ 、 $\dots$ を、 g_1, g_2 それぞれで置換した結果を比べ、関係が保存されるか否かを見る。

答 g_1 で置換すると、 $\alpha_a = \psi_0(V')$ 、 $\alpha_b = \psi_1(V')$ 、 $\alpha_c = \psi_2(V')$ 、 $\dots$; $V' = A\alpha_a + B\alpha_b$

g_2 で置換すると、 $\alpha_a = \psi_0(V')$ 、 $\alpha_b = \psi_1(V')$ 、 $\alpha_p = \psi_2(V')$ 、 $\dots$; $V' = A\alpha_a + B\alpha_b$

配列「 $c, d, e, \dots$ 」と「 $p, q, r, \dots$ 」に 1 文字でも不一致があれば、例えば $c \neq p$

なら、 $\alpha_c = \psi_2(A\alpha_a + B\alpha_b) = \alpha_p$ 、が矛盾だから（重根は無いのが前提）、 $g_1 = g_2$

上記を一般的に言えば、「 $\dots, i, \dots, j, \dots \rightarrow \dots, a, \dots, b, \dots$ 」のように、 $\dots$ 以外の 2 文字で指定しただけで、配列置換は一意的に決まる。

「 $\dots, i, \dots, j, \dots \rightarrow \dots, i, \dots, j, \dots$ 」となる G の元は、 e のみである。

任意に i, j を特定して、置換「 $\dots, i, \dots, j, \dots \rightarrow \dots, a, \dots, b, \dots$ 」を g と呼び、

「 $\dots, i, \dots, j, \dots \rightarrow \dots, a', \dots, b', \dots$ 」を g' 、

「 $\dots, i, \dots, j, \dots \rightarrow \dots, a'', \dots, b'', \dots$ 」を g'' 、

などと呼ぼう。置換結果の選び方は、 $a, a', \dots$ が「 $0 \sim (n-1)$ 、つまり n 通り」、

$b, b', \dots$ は「それぞれ $a, a', \dots$ 以外、つまり $(n-1)$ 通り」だから、

$g, g', g'', \dots$ の種類は、最大 $n(n-1)$ ケまで可能である。その中で「元どうしの積が元、すなわち $g g' = g''$ など」が成り立つ元からなる集合が、群 G になる。

問題 G の元の個数（位数）は、 $n(n-1)$ であることを示せ。

答 任意 2 根で、各根 $= \psi_i(V)$ と書けるなら、 $n(n-1)$ 種類の α_a, α_b の選び方で作った、 $V = A\alpha_a + B\alpha_b$ のどれでも、各根 $= \psi_i(A\alpha_a + B\alpha_b)$ と書ける。この関係を保存する置換「 $a \rightarrow i, b \rightarrow j$ 」は群を成す。左記の置換はどれも、上述の「 $i \rightarrow a, j \rightarrow b$ の指定で決まる置換」それぞれの、逆置換だと分かる。すなわち、前述 $n(n-1)$ ケの可能な置換はみな G の元でなければならない。

巡回置換 $(0, 1, \dots, n-1)$ の反復は、明らかに G の元であり、「 $k \rightarrow k+m$ 」と書ける（ $m=0, 1, \dots, n-1$ ）。 $k \rightarrow f(k) = k+m$ と書けば、 m に応じて $f_m(k)$ 、または $f_0(k)$ 、 $f_1(k)$ 、 $\dots$ 、 $f_{n-1}(k)$ と表せる。

g が（全文字に作用する）1 つの巡回置換なら（上記 $f_m(k)$ も含めた）一般形は、 $(a b c d \dots) = (b c d \dots a) = \dots$ 、または $(a b)(a c)(a d)\dots = (b c)(b d)\dots(b a) = \dots$ 、

と書ける。或る文字と、他の任意文字の置換のされ方が同じだから、これらの置換はみな、 $k \rightarrow f(k)$ の形に書ける可能性がある。

1 つの巡回置換でない（共通文字をもたない巡回置換の積に分解される）元が、 G の元になりうるかどうかの考察も要するが、もし $k \rightarrow f(k)$ の形で $n(n-1)$ 個の置換を表せたなら、 G の元をすべて得たのだから、その考察は不要になる（もし、より少数の元しか表せなかったら、 $f(k)$ の形に書けない G の元を捜さねばならない）。

今の場合、添え字の値は、 $\text{mod } n$ で書かねばならない： $f(k)=n$ なら $\equiv 0$ 、など。

数列 $0 \quad 1 \quad 2 \quad \cdots \quad k \quad \cdots \quad k+s \quad \cdots \quad n-1$ を g で置換すると、

数列 $f(0) \quad f(1) \quad f(2) \quad \cdots \quad f(k) \quad \cdots \quad f(k+s) \quad \cdots \quad f(n-1)$ になるとしよう。

下段も添え字だから、全体として $0 \sim (n-1)$ に等しい。

下段 $\rightarrow$ 上段への置換は、 g の逆元である。

置換 g を $f(k)$ と書けるなら、群は、 $\{e, g, g', \cdots\} = \{k, f(k), f'(k), \cdots\}$ と書ける。

$g'g = g''$ 、 $gg' = g'''$ は、 $f(f'(k)) = f''(k)$ 、 $f'(f(k)) = f'''(k)$ となる（' は微分でない）。

置換を $k \rightarrow f(k)$ と書ける、というだけでは、 f の関数形が一意的に決まらないが、1 つの巡回置換だと仮定すれば、以下のように考えられる。

添え字 $f(k)$ を、別の添え字 $f(k+s)$ に変える“添え字の算術”は、 k を $(k+s)$ に変える算術と同形式とみなせるから、 $f(k+s) = f(k) + S$ と書いてみる $\cdots \star$

S の値は、 f の関数形と s で決まり、 k に依存しないと考えよう。

S は負でもよいが、 $\text{mod } n$ で書けば正に直せる（例； $-2 \equiv +3, \text{mod } 5$ ）

$\star$ で、 $k=0$ とすれば、 $f(s) = f(0) + S$ （数列先頭の置換結果を $f(0)$ と指定）

$k=1$ とすれば、 $f(s+1) = f(1) + S$ （第2文字の置換結果を $f(1)$ と指定）

未知数 S を消去すると、

$f(s+1) = f(s) + f(1) - f(0)$ 簡単のため、 $f(1) - f(0) = q$ と書くと、

$f(s+2) = f(s+1) + q = f(s) + 2q$ 、 $f(s+3) = f(s+2) + q = f(s) + 3q$ 、 $\cdots$ 、

帰納的に、 $f(s+m) = f(s) + mq$

m を、使い慣れた添え字 k に書き換え、 $s=0$ とおくと

$f(k) = qk + f(0) = \{f(1) - f(0)\}k + f(0)$ が得られる。（ $S = qs$ も分かる）

すなわち、 $f(k)$ は線形置換（ k の1次式）であり、 $f(0)$ と $f(1)$ が決まれば決まる（むろん、数列のどの2箇所でも指定してもよい）。

数列 $0 \quad 1 \quad 2 \quad 3 \quad \cdots$ を g で置換した配列が、

$r \quad q+r \quad \cdots \quad \cdots \quad \cdots$ であれば、全配列が決まり、

置換 g が、 $k \rightarrow f(k)$ と書けるなら、 $f(k) = qk + r$ だと分かった。

(i) $q=1, r=1$ になる置換、 $k \rightarrow f(k)=k+1$ を g' と呼ぶと、 g'^s は、 $k \rightarrow k+s$ である。 $\{e, g', g'^2, \dots, g'^{n-1}\}$ は、線形置換群の部分群であり、位数 n の巡回群である。

$q=1, r=0$ となる置換は、 $k \rightarrow k$ 、すなわち e である。

(ii) $r=0$ になる置換を g'' と呼ぶと、 g'' は、 $k \rightarrow f(k)=qk$ 、 $g''^t = q^t k$ である。

q を $\text{mod } n$ の原始根とすれば、 $\{e, g'', g''^2, \dots, g''^{n-1}\}$ は、位数 $n-1$ の、すでに知った巡回群である。

以上で、元の個数が $n(n-1)$ ヶ得られたから、 $G = \{qk+r\}$ 、すなわち G の元はみな、 $qk+r$ の形に書けると分かった。

注意点： n が素数でないなら、 $\text{mod } n$ の原始根は一般に存在しないので、今考えている置換を、 $k \rightarrow f(k)$ と書けない。

或る 4 次方程式の 4 根が“任意”2 根で、 $\alpha_i = \psi_i(A\alpha_k + B\alpha_j)$ と書けたら
(実際は不可能；101 頁 §6 冒頭)、 $\{e, (0\ 1)(2\ 3), (0\ 2)(1\ 3), (0\ 3)(1\ 2)\}$
が上の関係を保存する群の“部分群”、と言っても矛盾を指摘できない。

2) $V^* = A\alpha_i + B\alpha_j$ を Gal (線形群； $k \rightarrow qk+r$) で置換して作った、

$$F^*_{\text{Gal}}(V) = \Pi_{\text{Gal}} \{V - (A\alpha_i + B\alpha_j)\} \quad \dots \star$$

の展開係数が有理数になる (すなわち Gal がガロア群である) ことの証明

$V^* = A\alpha_i + B\alpha_j$ を必ず変化させる置換が、 $k \rightarrow qk+r$ だから、 $\star$ の右辺では、 A, B に α_i, α_j を配する仕方の全てが掛け合わされる (n 文字から 2 ヶ選んで並べる順列)。

したがって、根の任意の互換、すなわち $\{ \quad \}$ 内での互換でも、異なる $\{ \quad \}$ にまたがる互換でも、 $\star$ は変化しない。任意互換で不変なら、任意置換で不変である。

$\star$ は、 Gal 対称性であるだけでなく **S_n 対称性**、有理係数多項式だと分かった。

ガロアの第一論文は、ここまですべて終わっている (論文末尾に 96 頁の表がある)。

【まとめ】

$V = A_1\alpha_1 + \dots + A_n\alpha_n$ 、 $\text{Gal} = \{k \rightarrow qk+r\}$ で作った $F_{\text{Gal}}(V)$ の係数が有理数なら、任意 2 根で全根が有理的に表せた。

逆に、任意 2 根で全根が有理的に表せるなら、 $V^* = A\alpha_i + B\alpha_j$ から作った $F^*_{\text{Gal}}(V)$ の係数が有理数となった。

$\{k \rightarrow qk+r\}$ の部分群、 $\{k \rightarrow qk\}$ または $\{k \rightarrow k+r\}$ で、 $V = A\alpha_i + B\alpha_j$ を置換して $F(V)$ を作ったら、係数は有理数にならない。つまり、 $\{k \rightarrow qk+r\}$ は、有理係数の $F(V)$ を与える最小の群 = ガロア群、という定義に合う。

$\{k \rightarrow qk+r\}$ より大きな群は、 V を変えない元を含むから、 $\alpha_k = \psi_k(A\alpha_i + B\alpha_j)$ を保存しない。すると、 $\{k \rightarrow qk+r\}$ は、有理係数の V 多項式を与える唯一の群である。

3. ガロア群の、もう一つの古典的定義

今までの話を、少し違う言い方で整理してみよう。69 頁“ガロア群の定理”に戻り、証明をみると、 $\alpha_k = \varphi_k(V)$ を与える根の 1 次式は、 $V = A_1\alpha_1 + \cdots + A_n\alpha_n$ でなくてもよいと分かる。 m 本の任意根で書いた V^* を使って、 $\alpha_k = \psi_k(V^*)$ 、と整式で書ければ、ガロア群の定理は成り立つ。

覚え書き： n 次方程式 $f(x)=0$ の根 $\alpha_1 \sim \alpha_n$ が、すべて異なるとする。

以下は、与えられた $f(x)$ の、係数間に存在する関係で決まることである。

定義 1. (66 頁の再掲) n 本の 1 次式を、 $V = A_1\alpha_1 + \cdots + A_n\alpha_n$ とする。

$F_G(V) = \Pi_G(V - V_k)$ の展開係数が、有理数になる置換群 G は必ずある。

複数があれば、位数が最小の G をガロア群と呼ぶ。

S_n しかないなら、 S_n がガロア群であり、 $F_{S_n}(V)$ は $n!$ 次多項式になる。

最小の G で作った $F_G(V)$ が、最低次の有理係数多項式（既約式）になる。

定義 2. 最小 m 本の任意根を使った V^* で、 $\alpha_j = \psi_j(V^*)$ と書けるなら、… ★
この関係式を保存する置換群 G^* をガロア群と定義できる。なぜなら
 G^* 対称性の、 $F_{G^*}(V) = \Pi_{G^*}(V - V_k^*)$ が有理係数になるからである（下記）。
保存とは、根配列の置換 $V^* \rightarrow V^{*'}$ で、 $\alpha_j = \psi_j(V^*) \rightarrow \alpha_k = \psi_j(V^{*'})$ が
成り立つこと。 $m = n$ なら、 $G^* = S_n$ である。

些末な例： $m = n$ の場合の関係式、 $\alpha_j = \{V \text{ の整式} \}$ は、以下に書き換えられる。

基本対称式 $\alpha_1 + \cdots + \alpha_n =$ 既知数だから、1 根を消去し、任意 $(n-1)$ 根を使った V^* で、 n 根を常に $\alpha_j = \{V^* \text{ の整式} \}$ と表せる。したがって、任意文字係数の方程式で、 $m = n-1$ は常に可能であり、ガロア群は、 $m = n$ の場合と同じ S_n である。

仮定★が本当なら、定義 2 の G^* で作った、 $F_{G^*}(V) = \Pi_{G^*}(V - V_k^*)$ の係数は、以下で分かるように有理数になる。

任意 m 根で書いた $V^* = A_1\alpha_1 + \cdots + A_m\alpha_m$ で、各根 $= \psi_j(V^*)$ と書ける方程式では、 $\alpha_1 \sim \alpha_m$ の並べ替えでも他の根でも、 $\alpha'_1 \sim \alpha'_m$ と呼べば、 $V^{*'} = A_1\alpha'_1 + \cdots + A_m\alpha'_m$ で、各根 $= \psi_j(V^{*'})$ と書ける。

m 本の根の対応「 $\alpha_1 \rightarrow \alpha'_1, \cdots, \alpha_m \rightarrow \alpha'_m$ 」を指定すれば、関係（#）を保存する置換が 1 つに決まることは、105 頁（ $m=2$ の場合）とまったく同様である。

ありうる V_j の形すべてで作った、 $\Pi(V - V_j^*) = \Pi\{V - (A_1\alpha_1 + \cdots + A_m\alpha_m)\}$ の（ ）には、“ n 根から m 本を選んで並べた順列”がすべて入る。

各根 $= \psi_j(V^{*'})$ が実在する式なら、この関係式を保存する群 G^* が、上記 V_j^* のす

べてを実現し、 $\Pi(V - V^*_j) = F_{G^*}(V) = \Pi_{G^*}(V - V^*_k)$ である (106 頁と同様)。

$\Pi_{G^*}(V - V^*_k)$ で、例えば α_1 と α_2 に注目する。() 内に α_1, α_2 両者を含むものでは、 $(\cdots + A_k \alpha_1 + \cdots + A_j \alpha_2 + \cdots)$ と $(\cdots + A_k \alpha_2 + \cdots + A_j \alpha_1 + \cdots)$ があり、 α_1, α_2 の一方のみ含む () では、 $(\cdots + A_p \alpha_1 + \cdots)$ と $(\cdots + A_p \alpha_2 + \cdots)$ など、「 α_1, α_2 以外の根配列がみな等しいペア」が必ず存在する。そして上記以外の括弧は α_1, α_2 を含まない。

したがって、 $F_{G^*}(V)$ は互換 (1 2) で不変、同様に任意互換で不変すなわち任意置換で不変 (S_n 対称性) である。したがって、 $G^* \neq S_n$ なのに、 $F_{G^*}(V)$ の係数成分は n 根の対称式 (有理数) になる。すなわち G^* はガロア群である。

本章で実際に、 $\alpha_j = \psi_j(V_k)$ と書ける方程式を明示したのは、 $m = n, m = n - 1, m = 1, m = 2$ の場合だった。

m が最小であることは、上の証明に使わず、ガロア群の命名のために使った。

最低次数の有理係数 V 多項式、 $F_{G^*}(V)$ を作れる群が、ガロア群である。

ただし、数値係数で与えられた特定の方程式 $f(x) = 0$ の根が、 $m (< n)$ ケの任意根で表せるかどうかは、 n 根の式 $V_k = A_1 \alpha_1 + \cdots + A_n \alpha_n$ で作った、 $F_G(V) = \Pi_G(V - V_k)$ が有理係数になるかどうかで判定することになる。

ガロア原著 (第一論文) の記述がすべて証明された。ガロアの考察はさらに先に進み、友人への手紙の中に以上の内容を「すでに明らかなこと」と述べている (高瀬正仁訳: アーベル/ガロア楕円関数論. 東京、朝倉書店、1998、p288)。その先を我々は想像するしかないが、少なくとも第一論文から、“現代ガロア理論”が生じたのだから、以上の内容と現代論の関係を述べなければ片手落ちのように思われる。そこで次章を追加してみた。それは現代書からの引き写しでなく、本 4 章の古典論を現代論の言葉に直したものである。非常に分かり易いと感じていただければ幸いである。

5 章 現代ガロア理論の概念

n 次代数方程式が解ける必要十分条件を、現代用語で述べる。ただし成書と異なり、ガロア原著を現代化するのに必要な言葉だけで証明し、一般的な代数学の概念はあまり使わない（分離的、固定体、最小分解体などの語は使わずに文脈で意味を示した。現代書との対応はすぐ分かると思う）。他書ですでに群論を知っていれば、本章だけ読んでも話が完結するが、多項式の基本性質とユークリッドの互除法は必須である（本章では既知とした 1 章）。

§ 1. 体（タイ）と同型写像の概念

1. 代数的な数

代数方程式 $x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0 = 0$ を満たす数（すなわち根）を、代数的な数という。係数 $c_{n-1} \sim c_0$ は有理数と定義する。

円周率 π や自然対数の底 e は、代数的な数でないことが知られている。

現代ガロア理論では、“代数的な数”の集合の構造と、集合どうしの関係を考察する。

代数的数を論じることは、方程式の解法理論を含む。とみなせば、現代数学の文脈から方程式という言葉が消えたときも、意味を見失わずに済む。

$x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0 = 0$ の根 α は、 $\alpha^n = -(c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0)$ を満たす。

このことから帰納して、下記の定理が証明できる（57 頁）。

α の有理式のすべて（任意次数の整式と分数式）は、 $(n-1)$ 次以下の α の整式、 $C_{n-1}\alpha^{n-1} + C_{n-2}\alpha^{n-2} + \cdots + C_1\alpha + C_0$ 、の形に書き直せる（ $C_{n-1} \sim C_0$ は有理数）。

共役根：1 つの既約方程式の根どうしを、共役根と言う。共役の概念が重要な理由は、共役根の形が、相互に制約し合い（例えば、有理係数の既約 2 次方程式は無数にあるが、1 根が $1 + \sqrt{2}$ なら、その共役根は $1 - \sqrt{2}$ のみ）、これが解法理論を導くからである。

2. 体の概念（体の拡大、拡大次数、単拡大、中間体）

2-1. 体（タイ、Körper、field）

数集合が、加減乗除で閉じている（任意要素の計算結果 = 要素）なら、数体と言う（生体のように結びつく要素集合のイメージらしい）。一般に体とは、加法と乗法の“操作”に関して群をなす集合をいう（引き算と割り算は、操作の逆元として含まれる）。

整数すべての集合は、割り算で閉じないから（例、 $1/2 \neq$ 整数）、体でない

実数、複素数、有理数、それぞれのすべてを含む集合は、それぞれ体である

体は、ドイツ語で Körper というので、よく K と記される（常にイタリックで書く。英語では、body でなく field なので F とも書くが、文字 F は関数だけに使いたないので本書では恣意的に K, L, M などと書き、或る特定の体を Q, Γ (ガンマ) と呼ぶ。

有理数だけを要素とする体を、 Q と呼ぶことにする。 Q の要素は無限ヶある。

Q 上の方程式とは； Q の要素を係数にもつ方程式、つまり我々がふつうに考えてきた有理係数方程式である。 Q 上の（2 次以上の）既約方程式の根は、 Q の要素でない；それらの根は、どんな（計算法で作れる）体の要素なのかが、本章の主題である。

2-2. 体の拡大；拡大体の構造と次元

要素の巾開方値を添加して要素を拡大した体を、**拡大体**という。 Q に $\sqrt{2}$ を添加した体を、 $Q(\sqrt{2})$ と書く [$Q(x)$ は x の関数を意味せず、類似性もない]

・ Q 上の方程式 $x^2 + ax + b = 0$ の根は、 $\alpha, \beta = 1/2 \{-a \pm \sqrt{a^2 - 4b}\}$ 、すると根は $Q(\sqrt{a^2 - 4b})$ の中で有理計算できると分かるから、 $\alpha, \beta \in Q(\sqrt{a^2 - 4b})$

・ もう 1 つの重要な書き方：根の非対称式を添加した拡大体、 $Q(\alpha - \beta)$ の中で $\alpha, \beta = 1/2 \{(\alpha + \beta) \pm (\alpha - \beta)\}$ と有理計算できる。すなわち $\alpha, \beta \in Q(\alpha - \beta)$

我々は、或る代数方程式の“根の、非対称な有理式”を添加した拡大体を作りたいのである。 $Q(\alpha, \beta) = Q(\alpha - \beta)$ は、 Q に $\sqrt{(\alpha + \beta)^2 - 4\alpha\beta}$ を添加すれば作れる、など

$Q(\sqrt{2})$ の要素はみな、 $A\sqrt{2} + B$ と書ける（文字は有理数）。 $1/(\sqrt{2} + 1) = \sqrt{2} - 1$ 、 $1/\sqrt{2} = (\sqrt{2})/2$ 、などと確認されるが、前記の定理を利用すれば、計算せずに分かる（下記）。

$Q(\sqrt[3]{2})$ の要素はみな、 $A(\sqrt[3]{2})^2 + B\sqrt[3]{2} + C$ 、と書ける。なぜなら、 n 次方程式の根 α を添加した $Q(\alpha)$ の任意要素は、有理係数式で $C_{n-1}\alpha^{n-1} + \cdots + C_1\alpha + C_0$ と書けるから、今は $\alpha = \sqrt[3]{2}$ を、3 次方程式 $x^3 - 2 = 0$ の根とみて、 $n = 3$ とすればよい。

注：円周率 π を添加して $Q(\pi)$ を作ったら、上の議論は意味をなさない。

π は代数的数でないから、例えば $1/\pi$ は、 π の整式に書き直せない。

以下の殆どで、 n 次既約方程式を考える。既約方程式には、重根も有理根もない（1 章）。その 1 根 α を添加した体 $Q(\alpha)$ の要素は、 $C_{n-1}\alpha^{n-1} + C_{n-2}\alpha^{n-2} + \cdots + C_1\alpha + C_0$ と書けるから、 $(n-1)$ 次までの α の項で書かれた、 **n ヶまでの項**からなる。

上の数表記を、 **n 次元空間のベクトル**とみると、代数的数をイメージし易い（ α の 0 次項が第 1 次元）： $\alpha^{n-1}, \cdots, \alpha, \alpha^0$ を、ベクトル空間の座標軸、 $C_{n-1}, C_{n-2}, \cdots, C_0$ を座標成分とみる。 Q の要素（有理数）は、正負の方向をもつ 1 次元ベクトルといえる。

$Q(\alpha)$ は、 Q の **n 次拡大体**と呼ばれる。 n 次元の数を含むイメージに適う。

2-3. 拡大次数の概念と算定

n 次既約方程式 $f(x) = 0$ の根 α を Q に添加すると、 n 次拡大体になると分かった。

$[Q(\alpha) : Q]$ という記号を“**拡大次数**”と称する。今、 $[Q(\alpha) : Q] = n$ である。

次に、 $f(x) = 0$ の、 α 以外のもう 1 根、 β も添加した拡大体、 $Q(\alpha, \beta)$ の構造を考えよう。 $Q(\alpha)$ には、 α の有理式で書かれる代数的数がみな含まれる。そこに β も添加す

ると、 Q の何次拡大体になる（何次元空間の数ができる）か？

因数定理から、 $f(x) = (x - \alpha) g(x)$ と書ける。 $Q(\alpha)$ の中で、 $f(x) \div (x - \alpha)$ を計算し、 $g(x) = x^{n-1} + (c_{n-1} + \alpha) x^{n-2} + (c_{n-2} + \alpha c_{n-1} + \alpha^2) x^{n-3} + \dots$ を得る。係数は n 次元数 $\in Q(\alpha)$

β は、 $Q(\alpha)$ 上の $(n-1)$ 次方程式 $g(x) = 0$ の根だから、 β の任意有理式は、 $(n-1)$ までの項で、 $B_{n-2} \beta^{n-2} + \dots + B_1 \beta + B_0$ と書いて、この係数は n 次元数である。

$Q(\alpha, \beta)$ は、 $Q(\alpha)$ の $(n-1)$ 次拡大体、 Q の $n(n-1)$ 次拡大体、と言える。

さらに根を添加してみよう。 n 次既約方程式の n 根を、 $\alpha_1, \alpha_2, \dots, \alpha_n$ と書く。

$[Q(\alpha_1) : Q] = n$ 、 $[Q(\alpha_1, \alpha_2) : Q(\alpha_1)] = n-1$ 、 $[Q(\alpha_1, \alpha_2, \alpha_3) : Q(\alpha_1, \alpha_2)] = n-2$ 、 $\dots$ の積をとれば、 $[Q(\alpha_1, \alpha_2, \dots, \alpha_n) : Q] = n!$ 、**拡大次数 $n!$** の拡大体に達する。

注：基本対称式、 $\alpha_1 + \dots + \alpha_n =$ 有理数だから、 $(n-1)$ 根、 $\alpha_1 \sim \alpha_{n-1}$ を含む拡大体

は α_n も含み、 $Q(\alpha_1, \dots, \alpha_{n-1}) = Q(\alpha_1, \dots, \alpha_{n-1}, \alpha_n)$ となる。 $n \times (n-1) \times \dots \times 2 = n!$

$x^2 - 2 = 0$ の 2 根は、 $Q(\sqrt{2})$ の中で有理計算され、 $Q(\sqrt{2}) = Q(\sqrt{2}, -\sqrt{2})$ など

以上は、拡大次数を数え、数構造を考えただけであり、1 根ずつ添加するのが解法手順になるのではない（因数定理が、方程式の解法でないのと同様である）。

2-4. 代数方程式の根の添加における、単拡大の概念（解法理論の出発点）

既約方程式の根を添加していく、 $Q \rightarrow Q(\alpha_1) \rightarrow Q(\alpha_1, \alpha_2) \rightarrow \dots \rightarrow Q(\alpha_1, \dots, \alpha_n)$ の過程は、以下のような根の 1 次式（単一の代数的数）を添加していくことと同等である：**単拡大**という、この意外なことを帰納法で証明しよう。

$f(x) = 0$ を n 次既約方程式とする（既約なら重根をもたない ⇨ 16 頁）。

証明手法として、2 つの方程式が“唯一の”共通解をもつ状況を設定する（重根があると、我々にとって無用な煩雑さを招く）。

1) $v = \alpha_1 + c \alpha_2$ とし（ c は有理数）、 **x の方程式 $f(v - c x) = 0$ を作ると、係数 $\in Q(v)$** となる。 $f(v - c \alpha_2) = f(\alpha_1) = 0$ だから、「 $x = \alpha_2$ は、 $f(v - c x) = 0$ の根」である。

$x = \alpha_k$ ($\neq \alpha_2$) を代入し、 $f(v - c \alpha_k) = f(\alpha_1 + c \alpha_2 - c \alpha_k) = 0$ となるのは (α_j を $f(x) = 0$ の根とし)、 $\alpha_1 + c(\alpha_2 - \alpha_k) = \alpha_j$ 、つまり $c = (\alpha_j - \alpha_1)/(\alpha_2 - \alpha_k)$ のときである（右辺は一般に無理数）。 c を、上記以外の適当な値（有理数）に決めよう。必ず可能である。

すると $f(v - c \alpha_k) \neq 0$ 、つまり「 α_2 以外の $\alpha_1 \sim \alpha_n$ は、 $f(v - c x) = 0$ の根でない」。

したがって、 α_2 は、 $f(v - c x) = 0$ と $f(x) = 0$ の唯一の共通解である。

するとユークリッドの互除法で、 $f(v - c x)$ の係数 $\in Q(v)$ と、 $f(x)$ の係数 $\in Q$ から、 α_2 が算出できる。

したがって、 **$\alpha_2 \in Q(v)$** 、そして $\alpha_1 = v - c \alpha_2$ より、 **$\alpha_1 \in Q(v)$** 、すなわち ψ_1, ψ_2 を有理係数の整式だとして、 **$\alpha_1 = \psi_1(v)$ 、 $\alpha_2 = \psi_2(v)$** 、などと書ける（111 頁）。

2) 上記の 1 つ、 $\alpha_1 = \psi_1(v)$ を使い、 $f(\psi_1(v)) \equiv F(v)$ と名付ける。 $F(X)$ の係数は (c に依存する) 有理数、 $F(v) = f(\alpha_1) = 0$ より、 $X = v$ は、 $F(X) = 0$ の解の 1 つである。

$v' = v + c' \alpha_3$ と書き (c' は有理数)、 x の方程式 $F(v' - c'x) = 0$ を作ると、係数 $\in Q(v')$ になり、 $F(v' - c' \alpha_3) = F(v) = 0$ だから、 $x = \alpha_3$ は $F(v' - c'x) = 0$ の解である。

$x = \alpha_k$ ($\neq \alpha_3$) を代入して $F(v' - c' \alpha_k) = 0$ になるのは、 $F(X) = 0$ の解を X_j と呼ぶとして、 $v' - c' \alpha_k = \alpha_1 + c \alpha_2 + c' (\alpha_3 - \alpha_k) = X_j$ となるような、特定の c' の値を選んだときだけである。 c' を他の適当な有理数に選べば (常に可能)、 $F(v' - c' \alpha_k) \neq 0$ 。

すると、 α_3 は、 $F(v' - c'x) = 0$ と $f(x) = 0$ の、唯一の共通解となる。したがって α_3 が $F(v' - c'x)$ の係数 $\in Q(v')$ と、 $f(x)$ の係数 $\in Q$ から、互除法で算出されるから、 $\alpha_3 \in Q(v')$ 。前述 $\alpha_1, \alpha_2 \in Q(v)$ 、 $v = v' - c' \alpha_3 \in Q(v')$ より、 $\alpha_1, \alpha_2, \alpha_3 \in Q(v')$ 、すなわち、有理係数の v' の整式で、 $\alpha_1 = \xi_1(v')$ 、 $\alpha_2 = \xi_2(v')$ 、 $\alpha_3 = \xi_3(v')$ 、と書ける。

3) $\alpha_1 = \xi_1(v')$ を使い、 $f(\xi_1(v')) \equiv F^\#(v')$ と名付けると、 $F^\#(X)$ の係数は (c, c' に依存する) 有理数であり、 $F^\#(v') = f(\alpha_1) = 0$ だから、 $X = v'$ は $F^\#(X) = 0$ の解。そこで、 $v'' = v' + c'' \alpha_4$ ($= \alpha_1 + c \alpha_2 + c' \alpha_3 + c'' \alpha_4$) と書き、 $F^\#(v'' - c''x) = 0$ を作ると、係数 $\in Q(v'')$ 、 $x = \alpha_4$ は解、そこで c'' を適切に選び…… と繰り返せば、帰納的に、 $\alpha_1, \dots, \alpha_n \in Q(\alpha_1 \sim \alpha_n \text{ の } 1 \text{ 次式})$ になる。 n 根を平等な形に、 $V_1 = A_1 \alpha_1 + \dots + A_n \alpha_n$ と書けば、 $\alpha_1, \dots, \alpha_n \in Q(V_1)$ だから、 $Q(\alpha_1, \dots, \alpha_n) \subset Q(V_1)$ 。一方、 V_1 は $\alpha_1 \sim \alpha_n$ の有理式なのだから $Q(\alpha_1, \dots, \alpha_n) \supset Q(V_1)$ 、したがって $Q(\alpha_1, \dots, \alpha_n) = Q(V_1)$ 。

V_1 と異なる $\alpha_1 \sim \alpha_n$ 配置の式を V_j と呼べば、 $Q(V_1) = Q(V_j)$ も、同様に分かる。

上記を満たす $c, c', \dots$ には無数の任意性があるから、重根のない任意方程式 で必ず、上のような有理数 $A_1 \sim A_n$ を選べる。或る仕掛けをした $A_1 \sim A_n$ で $\alpha_1 \sim \alpha_n$ を結んで体に放り込むとヒモが複雑に絡み合った後ほどけ、各根それぞれになる手品のようなのである (手品の種はユークリッドの互除法だった)。

4) m ($< n$) ケの任意根の 1 次式で、全根を有理的に表せる (下記実例のような) 方程式なら、 $\alpha_1 + c \alpha_2 + c' \alpha_3 + \dots$ の作成を m ケでやめ、 $V_1 = A_1 \alpha_1 + \dots + A_m \alpha_m$ として、 $Q(V_1) = Q(\alpha_1, \dots, \alpha_m) = Q(\alpha_1, \dots, \alpha_m, \dots, \alpha_n)$ 、と書けることになる。

実例： n が素数の、 $(x^n - 1)/(x - 1) = x^{n-1} + \dots + x + 1 = 0$ では、任意 1 根 (原始根) の巾乗が全根を表すから、 $Q(\alpha_1, \dots, \alpha_n) = Q(V_k) = Q(\alpha_k)$ と書ける。任意 2 根で全根を表せる方程式なら、 $Q(\alpha_1, \dots, \alpha_n) = Q(V_i) = Q(A\alpha_j + B\alpha_k)$ となる (4 章で論じた)。

今後の議論では、 $A_1 \sim A_m$ への根の配し方が異なる任意 V_k, V_j で、必ず $V_k \neq V_j$ となるよう、 $A_1 \sim A_m$ を選ぶ ($V_k = V_j$ となったら、 $A_1 \sim A_m$ の値を変更すればよい)。

重根のない任意方程式の根が、「 $A_1 \alpha_1 + \dots + A_n \alpha_n = V_1$ の整式で、 $\alpha_k = \varphi_k(V_1)$ と書ける」ことを、55 頁で体を使わずに証明した。関係式 $\alpha_k = \varphi_k(V_1)$ の存在だけを論じ、 φ_k

の関数形を問わないガロアの方法は、現代論で、 $Q(\alpha_1, \dots, \alpha_n) = Q(V_1)$ と表現される。

体を用いた上記の証明では、 m 根で書いた V_1 で全根を表せる方程式の意味が、原著よりも分かり易い。 $Q(\alpha_1, \dots, \alpha_n) = Q(V_1)$ から、 $\alpha_j = \text{「}V_1\text{の有理係数整式」} = \varphi_j(V_1)$ が導かれることは、体の意味から分かる。根を名称変更すれば、 $\alpha_i = \varphi_j(V_k)$ と書ける。

(注： φ_j の添え字は、根の添え字でなく関数名だから、変更してはならない；59 頁)

2-5. 中間体の概念

有理数体 Q を、全根が有理計算できる体 $Q(\alpha_1, \dots, \alpha_n)$ にまで拡大する方法論が、我々の課題である。途中段階にある体は、**中間体**と呼ばれ、解法の焦点になる。

前述、 $Q(\alpha_1)$ 、 $Q(\alpha_1, \alpha_2)$ 、 $Q(\alpha_1, \alpha_2, \alpha_3)$ 、 $\dots$ は架空の拡大体であり、 $Q(\alpha_1, \dots, \alpha_n)$ に至る解法過程に登場しない。我々は実際の中間体を、根の平等性を保ちながら作る。

< 中間体の実例 >

3 次方程式を、2 章 24 頁で初等的に解いた。その方法に沿って、中間体を例示する (本章だけ読む人も 24 頁は見ていただきたい)。対称性を利用して根を求める過程で、

非対称式、 $\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha = \varphi$ 、 $\alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2 = \varphi'$ を扱った。この 2 つの式は、

$$\theta^3 = (\alpha + \omega\beta + \omega^2\gamma)^3 = \alpha^3 + \beta^3 + \gamma^3 + 6\alpha\beta\gamma + 3\omega\varphi + 3\omega^2\varphi' \quad (\text{ただし、}\omega^3 = 1)$$

$$\theta'^3 = (\alpha + \omega^2\beta + \omega\gamma)^3 = \alpha^3 + \beta^3 + \gamma^3 + 6\alpha\beta\gamma + 3\omega\varphi' + 3\omega^2\varphi \quad \text{の中に現れた。}$$

$\varphi - \varphi' = (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)$ と計算される。 $\{\text{右辺}\}^2$ は、根の任意置換で不変だから対称式 (有理数) つまり、 $\varphi - \varphi' = \pm\sqrt{\text{(有理数)}}$ 。 $\varphi + \varphi' =$ 対称式 $\in Q$ だから、 $\varphi - \varphi'$ を添加した $Q(\varphi - \varphi')$ の中で φ 、 φ' は、 $1/2 \{(\varphi + \varphi') \pm (\varphi - \varphi')\}$ 、と有理計算される。

θ^3 と θ'^3 は、「 φ 、 φ' 、 ω 、および対称式」から有理計算されるので (ω を含める考え方は 130 頁以後で述べる)、 θ^3 、 $\theta'^3 \in Q(\varphi, \varphi', \omega) = Q(\varphi - \varphi', \omega)$ 、である。

そして、 $\sqrt[3]{\theta^3} = \alpha + \omega\beta + \omega^2\gamma$ 、 $\sqrt[3]{\theta'^3} = \alpha + \omega^2\beta + \omega\gamma$ 、 $\alpha + \beta + \gamma =$ 有理数、から根が求まる。3 次方程式の根は、 $Q(\sqrt[3]{\theta^3}, \sqrt[3]{\theta'^3}, \omega) = Q(\alpha, \beta, \gamma)$ の中で、有理計算できる。 $Q(\varphi, \varphi', \omega) \subset Q(\sqrt[3]{\theta^3}, \sqrt[3]{\theta'^3}, \omega)$ 。 ω は、2 次方程式 $\omega^2 + \omega + 1 = 0$ の根である。

$Q(\varphi, \varphi', \omega) = Q((\alpha - \beta)(\beta - \gamma)(\gamma - \alpha), \omega) = Q(\sqrt{\text{(対称式)}}, \omega)$ が、**中間体**と分かった。

体に添加すべき“**巾開方量**”は (実は常に)、“**根の非対称式**”でもある。

解法に必要な“ $\alpha_1 \sim \alpha_n$ の式”は、“対称式の巾開方量”、“非対称な有理式”の 2 種の形で書ける (この意味は 2 章、4 章で詳述した)。

	2 次拡大、 $\sqrt{\quad}$ 量を添加	3 次拡大、 $\sqrt[3]{\quad}$ 量を添加
Q	$\rightarrow Q((\alpha - \beta)(\beta - \gamma)(\gamma - \alpha), \omega)$	$\rightarrow Q(\alpha, \beta, \gamma)$
有理数体	中間体	根が求まる体 ($2 \times 3 = 6$ 次拡大体)

3. 同型写像、同型な体、同型写像のレパートリー

既約方程式の解法は、根の名称変更に影響されない。ガロア原著は、その数学的扱い方を開発し、“根の式”を“置換対称性”で分類して計算可能性を解明した。現代論では根を“代数的な数”とみて、根の配列置換よりも広い概念“写像”を考える。

3-1. 同型写像 (isomorphic mapping または isomorphism)

写像とは、或る体の各要素を別の要素またはそれ自身に置き換える（写すと称する）操作である。要素が別の要素に写ると、他の体の要素になるか、もとの体に留まる。

我々は写像を、体全体に作用させることを考える（体の一部に作用させる概念は、本書で略す）。写像によって体は、他の体に写る、またはそれ自身に写る。

同型写像は、有理計算の規則を保つよう定義した操作であり、代数的数どうしの関係を分析する“道具”として役立つ。写像は、要素の写し方の指定で定義される。

今、体を L と呼び、 L を写す写像を、 σ (シグマ) と総称しよう (トリックカメラ σ で、 L を撮影すると、変身する要素・しない要素が見え、別の σ' で撮影すると違う像が見え、様々なカメラで撮った写真を比べて体 L の構造を調べる、と思ってもよく、思わなくてもよい)。

σ が、任意の $a, b \in L$ について下記を満たすとき、 σ を同型写像と呼ぶ。

1) $a = 0$ なら $\sigma(a) = 0$ 、 $\sigma(a) = 0$ なら $a = 0$

2) $\sigma(a + b) = \sigma(a) + \sigma(b)$ 、 $\sigma(a - b) = \sigma(a) - \sigma(b)$

3) $\sigma(ab) = \sigma(a)\sigma(b)$

4) $\sigma(a/b) = \sigma(a)/\sigma(b)$ ただし $b \neq 0$ 、その場合 1) より $\sigma(b) \neq 0$

$a = b$ なら、2) と 1) より $\sigma(a) - \sigma(b) = \sigma(0) = 0$ だから、 $\sigma(a) = \sigma(b)$

同様に、 $\sigma(a) = \sigma(b)$ なら $a = b$ 、すなわち、 $a \rightarrow \sigma(a)$ は一対一対応である。

(一対一対応の写像を、単射という：同型写像は単射である)

<有理数の同型写像>

代数的数 ($\in L$) のうち、有理数 ($\in \mathbb{Q} \subset L$) は、どんな数 ($\in L'$) に写るか？

3) より、 $\sigma(1) = \sigma(1)\sigma(1)$ 、一方 1) より $\sigma(1) \neq 0$ だから、 $\sigma(1) = 1$

2) より、 $\sigma(m+1) = \sigma(m) + \sigma(1) = \sigma(m) + 1$

$\sigma(-m) = \sigma(0-m) = \sigma(0) - \sigma(m) = -\sigma(m)$

したがって、文字が整数であれば帰納的に、 $\sigma(m) = m$

4) より、 $\sigma(m/n) = \sigma(m)/\sigma(n) = m/n$ (ただし $n \neq 0$)

したがって、任意の有理数 $q (= m/n)$ について、 $\sigma(q) = q$

これが任意 σ で成り立つ。つまり有理数は、任意の同型写像で変化しない。

逆に、「任意の σ で、 $\sigma(x) = x$ なら、 x は有理数」といえるだろうか？

この問いに答えるには、もう少し説明が要る (⇨ 124 頁の定理 I の 1)

<代数方程式の根の同型写像>

有理係数の既約方程式、 $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0 = 0$ 、の1根を α と呼ぶ。

α と $\sigma(\alpha)$ の関係は？ α が K の要素 ($\alpha \in K$) なら、 $\alpha \rightarrow \sigma(\alpha) = ? \in K$?

既約方程式の根 α は有理数でないから、(σ の定義に用いた有理計算規則で)、 $\sigma(\alpha)$ の“値”が計算できる筈はないが、興味深いことに“値の候補”は特定される。

3) より、 $\sigma(\alpha^m) = \sigma(\alpha \times \cdots \times \alpha) = \sigma(\alpha) \times \cdots \times \sigma(\alpha) = \{\sigma(\alpha)\}^m$ 、

q を有理数とすると、 $\sigma(q\alpha^m) = \sigma(q)\sigma(\alpha^m) = q\{\sigma(\alpha)\}^m$ 、

すると2) より、 $0 = \sigma(0) = \sigma(\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0)$

$$= \{\sigma(\alpha)\}^n + c_{n-1}\{\sigma(\alpha)\}^{n-1} + \cdots + c_1\{\sigma(\alpha)\} + c_0 = f(\sigma(\alpha))$$

すなわち、 $\sigma(\alpha)$ もまた $f(x) = 0$ の根だと分かる。

$\sigma(\alpha)$ は、 α の共役根のどれにでも(α 自身にも)なりうる。

同型写像は、既約方程式の根を、共役根に写すと分かった。

同型写像は、既約方程式に適用したとき、論理が次のように首尾一貫する：

有理根は、それ自身だけに写る。これを一般化し、可約方程式は因数分解してから扱えば、因数分解後の既約方程式の中で、共役根どうしが写り合う(#、後述125頁)。既約方程式は重根をもたない(16頁)。重根があれば写像は一対一対応にならない。

3-2. 同型写像 σ で同型な体、という概念

体 K' の“任意要素”が、 K の要素の“写像”であって(これを全射という)、写像 σ が同型写像なら、 **K' と K は σ で同型な体である**、と言う。

<共役体>

有理数体 $\mathbb{Q}$ 上の既約 n 次方程式 $f(x) = 0$ の共役根を、 $\alpha_1 \sim \alpha_n$ とする。共役根を添加した拡大体、 $\mathbb{Q}(\alpha_1)$ 、 $\cdots$ 、 $\mathbb{Q}(\alpha_n)$ どうしを**共役体**、または **$\mathbb{Q}$ 上の共役体**と言う。

$\mathbb{Q}$ を、拡大体 L に言い換えて、 L 上の既約方程式(意義は後述)の共役解を V_k 、 V_j 、 $\cdots$ と呼べば、 $L(V_k)$ 、 $L(V_j)$ どうしは、 **L 上の共役体**である(V_k は、 $\alpha_1 \sim \alpha_n$ の式)。 K 、 L の書き分けに意味はなく、有理数体 $\mathbb{Q}$ でないというにすぎない。

< σ で同型な共役体>

拡大体 $\mathbb{Q}(\sigma(\alpha_k))$ を、 σ で $\mathbb{Q}(\alpha_k)$ と同型な、 **$\mathbb{Q}$ 上の共役体**と呼ぶ。

$f(x) = 0$ の1根を α とし、 $\sigma_1(\alpha) = \alpha_1$ 、 $\sigma_2(\alpha) = \alpha_2$ 、 $\cdots$ 、 $\sigma_k(\alpha) = \alpha_k$ 、 $\cdots$ 、 $\sigma_n(\alpha) = \alpha_n$ のように、同型写像を添え字で区別できる。このとき、次の言い方をする。

$\mathbb{Q}(\alpha_1)$ は σ_1 で $\mathbb{Q}(\alpha)$ と同型、 $\cdots$ 、 $\mathbb{Q}(\alpha_k)$ は σ_k で $\mathbb{Q}(\alpha)$ と同型、 $\cdots$

ただし上記では、別の根 α' の写像が不明、 $\sigma_1(\alpha') = ?$ 、 $\sigma_2(\alpha') = ?$ 、 $\cdots$ 、すなわち写像の指定法が不完全である。一意的な決め方を次に考えよう。

3-3. 同型写像 σ のレパートリー

<根の配列置換とのアナロジー>

n 次の既約方程式 $f(x)=0$ の、様々な根（非有理数）を添加した、様々な拡大体どうしを考えると、同型写像（総称 σ ）のレパートリーは、最大で何個あるだろうか？

同型写像は一対一対応だから、「 $\sigma(\alpha_1)=\alpha_2=\sigma(\alpha_3)$ 」や「 $\alpha_1=\sigma'(\alpha_2)=\alpha_3$ 」はありえない（既約方程式を考えるから重根はない）。「 $\sigma(\alpha_1)=\alpha_2=\sigma'(\alpha_3)$ 、 $\sigma \neq \sigma'$ 」はありうる。

すると、「 n 根すべての配列 $\rightarrow$ 並べ替え」の対応づけの 1 つが、1 つの σ を決め、 $n!$ 種類までの σ が可能と分かる（説明されるより自分で納得するほうが容易であろう）。

{様々な σ の集合} は、{ n 根の配列置換の集合} に対応し、{可能なすべての σ からなる、最大の集合} は、 n 文字置換の対称群 S_n (45 頁) に対応する、と分かる。

我々は、写像一般でなく、115 頁で定義した“同型写像”という操作（道具）だけを利用する。同型写像は、共役根どうしを一対一に写すから、根の配列置換と同等だと分かった。

{ σ の集合} は、写される根が、“どんな方程式”の根であるかによって決まる。

例： $(x^5-1)/(x-1)=x^4+x^3+x^2+x+1=0$ 、の 4 根を写し合う $\sigma(\alpha_k)=\alpha_j$ は、添え字関係が $k \rightarrow j=2^m k$ (2 は mod 5 の原始根：51 頁) と書いて、4 々の σ で完全に決まる。 $\{\sigma_m\} = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$ 、 $\sigma_0(\alpha_k)=\alpha_k$ は恒等写像、 $\sigma_1(\alpha_k)=\alpha_{2k}$ 、 $\sigma_2(\alpha_k)=\alpha_{4k}$ 、 $\sigma_3(\alpha_k)=\alpha_{3k}$

同型写像は、根の関数 $\varphi, \varphi', \dots$ などを、何らかの根の関数に写す。 σ_k が恒等写像なら $\sigma_k(\varphi)=\varphi$ だが、 $\sigma_k(\varphi)=\varphi$ だからといって σ_k が恒等写像とは、むろん言えない。

4. 自己同型な体、自己同型群

4-1. 自己同型な体

前項の要約：有理数体 Q に、代数的数 α を添加した拡大体 $K=Q(\alpha)$ は、同型写像 σ で、同型な共役体 $K'=Q(\sigma(\alpha))$ に写る (3-2 の用語)。 $\sigma(\alpha)$ は α の共役根である。

一般には $K' \neq K$ 、すなわち $\sigma(\alpha) \in K'$ は、 K の要素とは限らない。

$K'=K$ となる、すなわち 同型写像 σ で“自分自身に写る体” を考案しよう。

或る σ について「 $\alpha \in K$ なら、 $\sigma(\alpha) \in K$ 」となる体を、 σ で自己同型な体 と言う ($\sigma(\alpha)=\alpha$ である必要はなく、 $\sigma(\alpha)$ が K の中に留まればよい)。

$K=Q(\alpha, \sigma(\alpha))$ を作れば、 $\sigma(\alpha) \in K$ だが、 $\sigma(\sigma(\alpha))$ は、 K の要素とは限らず、 α でも $\sigma(\alpha)$ でもない共役根でありうる、 $\dots$ と考えると以下のことが分かる。

有理数体 Q 上の n 次既約方程式 $f(x)=0$ の、共役根を $\alpha_1 \sim \alpha_n$ とする。

同型写像を σ と総称し、 $\alpha_1, \dots, \alpha_n$ それぞれを、 $\sigma(\alpha_1), \dots, \sigma(\alpha_n)$ に写したのも“共役根のすべて”だから、全体として同じである。したがって、

$Q(\alpha_1, \dots, \alpha_n)=Q(\sigma(\alpha_1), \dots, \sigma(\alpha_n))$ であり、両者は、 σ で自己同型な共役体 どうしである。根 $\rightarrow$ 共役根という写り方は、どんな σ についても言えるから、我々の到達目標

である全根を含む体 $Q(\alpha_1, \dots, \alpha_n)$ は、任意の σ で自己同型な体だと分かった。

4-2. 自己同型群

同型写像が、自己同型な体（の要素）に作用する場合を考える（このとき自己同型写像と呼ぶ）と、明らかに、 $Q(\sigma'(\alpha_1), \dots, \sigma'(\alpha_n)) = Q(\alpha_1, \dots, \alpha_n) = Q(\sigma(\alpha_1), \dots, \sigma(\alpha_n))$

$\sigma(\alpha)$ を、さらに σ' で写像したものを、 $\sigma'(\sigma(\alpha)) = \sigma'\sigma(\alpha)$ と表記する。

今考えようとする自己同型写像の“すべて”を含む集合 $\{\sigma, \sigma', \sigma'', \dots\}$ を、 $\{\sigma\}$ と略記する。すると明らかに、 $\sigma'\sigma \in \{\sigma\}$ 、となる。

$\alpha \rightarrow \sigma(\alpha)$ の逆写像を σ^{-1} と書けば、 σ^{-1} も $\{\sigma\}$ の要素（ $\sigma^{-1}\sigma =$ 恒等写像も、 $\{\sigma\}$ の要素）である。したがって、 $\{\sigma\}$ は群であり、自己同型群と言う。

或る作用で“不変なもの”が見つかりと常に、（ σ で不変、 σ' で不変なら $\sigma'\sigma$ で不変、恒等写像で不変だから）その作用すべての集合を群として扱える。

以後は、“自己同型な体に作用する同型写像”のみを考える。その集合は群をなす。

さて、既約方程式 $f(x) = 0$ の全根を含む $Q(\alpha_1, \dots, \alpha_n)$ は、 $\{\sigma\}$ の任意元でそれ自身に写ると分かったが、問題は、 $Q(\alpha_1, \dots, \alpha_n)$ の作り方である。これは、 $f(x) = 0$ の解法そのものであり、 $Q(\alpha_1, \dots, \alpha_n)$ の自己同型群、 $\{\sigma\}$ を使って分析できる。

5. ガロア拡大体 Γ (ガンマ)、および Γ の自己同型群（単拡大を用いた定義法）

まず例を見る： n が素数、 $x^{n-1} + \dots + x + 1 = 0$ では、任意 1 根（原始 n 乗根）の有理式で全根を書けるから、 $Q(\alpha_1, \dots, \alpha_n) = Q(\alpha_j)$ 、すると $\{\sigma\}$ の元は n ケとなる（117 頁）。

任意文字係数の n 次方程式 $f(x) = 0$ では、 $\{\sigma\}$ の元が $n!$ ケである（116 頁）。

$f(x) = 0$ の根構造の違いを反映した、 $Q(\alpha_1, \dots, \alpha_n)$ の適切な表記法を、考えよう。

単拡大（113 頁）： m ケの任意根で全根を有理的に表せる方程式では、 $m = n$ の場合も含め、 $V_1 = A_1 \alpha_1 + \dots + A_m \alpha_m$ と書けば、 $Q(V_1) = Q(V_j) = Q(\alpha_1, \dots, \alpha_n)$ 、となる。

任意文字係数の $f(x) = 0$ なら、 $m = n$ （または $m = n-1$ 、112 頁注釈）。

n が素数、 $x^{n-1} + \dots + x + 1 = 0$ なら $m = 1$ 。4 章では $m = 2$ の例を見た。

$\{\sigma\} = \{\text{根配置が異なる } V_k, V_j \text{ を写し合う自己同型写像の全て}\}$ は、群であった。

すなわち、 $\sigma(V_k), \sigma'(V_k) \in Q(V_1), \sigma\sigma'(V_k) \in Q(V_1), \sigma^{-1}(V_k) \in Q(V_1)$

$\{\sigma\}$ の位数を N と呼ぼう。すると今の場合、

$N = n!/(n-m)! =$ 「 n 根から m 根を選び、 V_1 の $A_1 \sim A_m$ に配する仕方の数」である。

（ $m = n, m = n-1, m = 1$ を代入すれば、3-3 の説明と附合する；117 頁）

V_1 は、 $\{\sigma\}$ で $V_1 \sim V_N$ のどれかに写る。すなわち、

全根を含む体の、適切な表記法は、 $Q(\alpha_1, \dots, \alpha_n) = Q(V_1) = \dots = Q(V_N)$ となる。

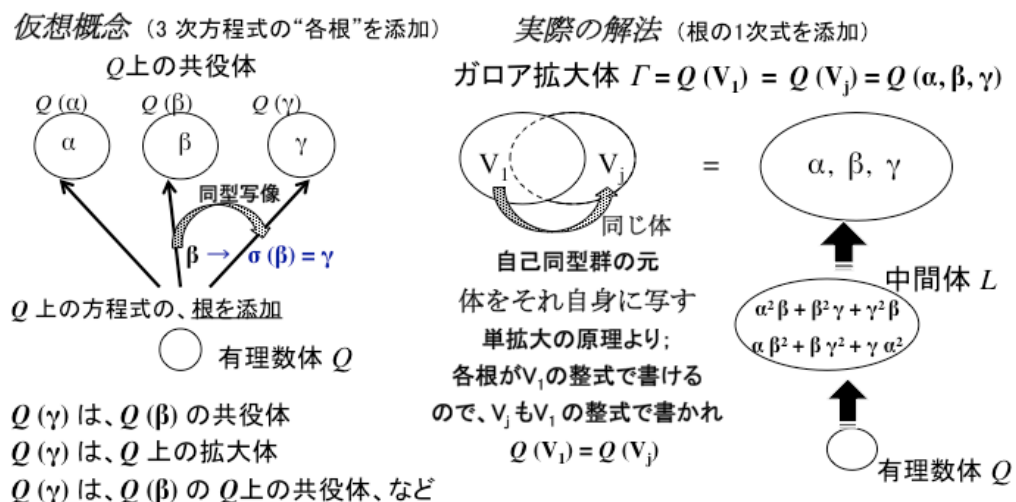
ガロア拡大体の定義： Γ の、 $\mathbb{Q}$ 上の共役体（それは $\{\sigma\}$ の元の数だけ生じる）が全て Γ 自身なら、 Γ を、 $\mathbb{Q}$ のガロア拡大体と呼ぶ（ Γ は、 σ で Γ に写る）。

Γ の自己同型群 $\{\sigma\}$ ： Γ は、 $\Gamma = \mathbb{Q}(V_1) = \cdots = \mathbb{Q}(V_N)$ を満たす体として、 $\{\sigma\}$ を用いて定義できた。 $V_1 \sim V_N$ を写し合う同型写像の群 $\{\sigma\}$ を、 Γ の自己同型群と呼び、後述の文脈の中で、ガロア群と呼ぶ。

拡大体が Γ に達すると、解くべき方程式は、 Γ 上でなく Γ の中にある $X - V_1 = 0$ となり、共役解は 1 つだから、 $\{\sigma\} = \{\text{恒等写像}\}$ となる。

特殊例： $\mathbb{Q}$ 上の或る方程式の根がみな有理根なら、方程式のガロア拡大体 Γ は、 $\mathbb{Q}$ 自体である。方程式は、有理計算で 1 次式にまで因数分解され、共役根が 1 つだから、 $\{\sigma\} = \{\text{恒等写像}\}$ 、元は 1 個である。

図 体上の共役体 (σ で同型な共役体)、およびガロア拡大体の概念



§ 2. ガロア理論

1. “解 V_1 を与える既約方程式” と “ Γ の自己同型群” の関係

以下、 n 次既約方程式の根の 1 次式を、 $V_1 = A_1\alpha_1 + \cdots + A_m\alpha_m$ 、と一般的に ($m = n$ も含めて) 書く。 V_1 を用いた単拡大で、 $\mathbb{Q}$ から $\mathbb{Q}(V_1) = \Gamma$ に至る方法を考える。

1-1. 解法の出発点となる、 $\mathbb{Q}$ 上の方程式

$\Gamma = \mathbb{Q}(V_1) = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$ の関係から、 $\alpha_1 \sim \alpha_n$ は、 V_1 の有理係数整式で書かれ、根を名称変更した V_j の式でも書ける。そこで $f(x) = 0$ を解くのではなく、 $X = V_1 \sim V_N$ を解にもつ $\mathbb{Q}$ 上の方程式を解くアイデアが生じる。その方程式を、 $F_{\mathbb{Q}}(X) = 0$ と書こう。

$V_1 \sim V_N$ の求まり方は、 $\alpha_1 \sim \alpha_n$ の名称変更に影響されず平等性を保つから、互いに共役、すなわち $F_Q(X) = 0$ は既約方程式である。 V_j を、 $f(x)$ の係数 (有理数) から代数計算したいのだから、 $F_Q(X)$ の係数は有理数でなければならない、すなわち、

$F_Q(X) = 0$ は、「 $V_1 \sim V_N$ を共役解にもつ、 Q 上の既約方程式」となる筈である。

$\sigma(V_1) = V_j$ を用いて、 $\Pi_\sigma(X - V_j) = (X - V_1) \cdots (X - V_N) = F_Q(X)$ を作れば、この係数が、実際に有理数になることを示そう。

1) n 次既約方程式 $f(x) = 0$ の係数が任意文字で与えられた場合

この場合の $F_Q(X) = 0$ が解ければ、 $f(x) = 0$ の一般解法が得られる。

単拡大には、 $m = n$ とした、 $V_1 = A_1 \alpha_1 + \cdots + A_n \alpha_n$ を使わねばならない。

なぜなら、少数根を使った V_1 で全根が書けたら、根どうしに「基本対称式 $= \pm$ 係数」の関係以外の関係も生じ、 $f(x)$ の係数が任意と言えなくなるからである。

$\{\sigma\}$ は、 V_j を異なる根配置の $V_1 \sim V_n$ すべてに写すから、元は $n!$ ケである。

$n!$ 次式、 $\Pi_\sigma(X - V_j)$ は、 $\alpha_1 \sim \alpha_n$ の任意入れ替えで不変だから、展開係数は $\alpha_1 \sim \alpha_n$ の対称式、すると $\alpha_1 \sim \alpha_n$ の基本対称式で表せる (証明は略す; 20 頁)。

すなわち、 $\Pi_\sigma(X - V_j)$ の展開係数は有理数 ($\in Q$) である。

$F_Q(X) = \Pi_\sigma(X - V_j) = (X - V_1) \cdots (X - V_n) = 0$ は、 Q 上の既約方程式と分かった。

2) 任意 m 根で書いた V_1 で、全根を有理的に表せる既約方程式 $f(x) = 0$ の場合

$f(x)$ の係数間に、何らかの関係があれば (例えば、 $x^4 + x^3 + x^2 + x + 1 = 0$)、 $m < n - 1$ になりうる (112 頁注釈; $m = n$ と $m = n - 1$ は同等)。その場合;

$V^*_1 = A_1 \alpha_1 + \cdots + A_m \alpha_m$ を用いて、 $\Gamma = Q(V^*_1)$ と書ける。

n 根で書いた V_1 と比較検討したいので、本節でだけ *印で区別する同型写像、 $V^*_1 \rightarrow V^*_k$ などを、 σ^* と総称する。

自己同型群 $\{\sigma^*\}$ の位数 $N = n!/(n - m)!$ ($\Rightarrow$ 118 頁)

$\{\sigma^*\}$ は、前記 1) の $\{\sigma\}$ の部分群である。 $\{\sigma^*\} \subset \{\sigma\}$

$V^*_1 \sim V^*_N$ それぞれは、 $\alpha_1 \sim \alpha_n$ の非対称式だが、 $V^*_1 \sim V^*_N$ の基本対称式は、 $\alpha_1 \sim \alpha_n$ を平等に含むから (109 頁)、 $\Pi_{\sigma^*}(X - V^*_k) = (X - V^*_1) \cdots (X - V^*_N)$ の展開係数は、 $\alpha_1 \sim \alpha_n$ の対称式、すなわち有理数である。したがって

$F_Q^*(X) = \Pi_{\sigma^*}(X - V^*_k) = 0$ が、解くべき Q 上の方程式、これは N 次式となる。

1) の $n!$ 次方程式、 $F_Q(X) = \Pi_\sigma(X - V_j) = 0$ を、解く必要はないのである。

2) の場合、1) の形の $F_Q(X)$ が可約式になることを示そう。まず下記を準備する。

$F_Q^*(X) =$ 「 m 根の式 V^*_1 を、 $\{\sigma^*\}$ で写した $V^*_1 \sim V^*_N$ で作った N 次式」と別に

$F^*(X) =$ 「 n 根の式 V_1 を、 $\{\sigma^*\}$ で写した $V_1 \sim V_N$ からなる N 次式」を作る。

$F^*(X) = \Pi_{\sigma^*}(X - V_j) = (X - V_1) \cdots (X - V_N)$ である; $\{\sigma^*\}$ に因んで、*印をつけた

$\{\sigma\} \supset \{\sigma^*\}$ だから、 $F^*(X)$ は明らかに、 $F_Q(X)$ に含まれる因子である
 $\{\sigma^*\}$ は群だから、 $\{\sigma^*\}$ で作った $F^*(X)$ の係数は、 $\{\sigma^*\}$ で変化しない (★)
(群でなければ、 $\sigma_j^*(V_k)$ が $V_1 \sim V_N$ の中にある可能性を生じ、 $F^*(X)$ が σ_j^* で変化しうる)

$F^*(X)$ の展開係数 ($V_1 \sim V_N$ の基本対称式) は、 $V_1 \sim V_{n!}$ のすべてでなく一部を使って書かれるのだから、 $\alpha_1 \sim \alpha_n$ の非対称式を含む。したがって一般には有理数でないが、2) の場合は有理数になる ($V_1 \sim V_N$ が、 $\{\sigma^*\}$ で写り合うからなのである；下記)。

証明：2) では、 $V^*_1 = A_1 \alpha_1 + \cdots + A_m \alpha_m$ で単拡大され、 $\Gamma = Q(V^*_1) = Q(\alpha_1, \cdots, \alpha_n)$ となるから、 $\alpha_1, \cdots, \alpha_n$ はそれぞれ、 V^*_1 の有理係数整式で書ける。したがって、 V_j で作った N 次式、 $F^*(X) = \prod_{\sigma^*} (X - V_j)$ の展開係数の成分を $\theta = \theta(\alpha_1, \cdots, \alpha_n)$ と総称すれば (θ は $\alpha_1 \sim \alpha_n$ の非対称式を含む)、 $\theta = \Theta(V^*_1)$ 、と V^*_1 の整式で書ける。

上記 (★) より、 θ は、 $\{\sigma^*\}$ で不変だから、 $\theta = \Theta(V^*_1) = \cdots = \Theta(V^*_N)$ である。

すると θ は、 $V^*_1 \sim V^*_N$ の対称式でも書ける (例えば $V^*_1 = \{\Theta(V^*_1) + \cdots + \Theta(V^*_N)\}/N$)、すなわち $V^*_1 \sim V^*_N$ の基本対称式 ($F_Q^*(X)$ の係数) で書ける。2) の場合、 $F_Q^*(X)$ の係数が有理数だから、 θ は有理数、すなわち $F^*(X)$ の係数は有理数と証明された。

前記 1) の $n!$ 次式 $F_Q(X)$ は、2) の場合、有理係数の $F^*(X)$ を因子に含むから、可約式だと分かった。注： $F^*(X)$ は、 $\{\sigma^*\}$ を使い、 $V^*_1 \sim V^*_N$ でなく $V_1 \sim V_N$ で作った。

$f(x) = 0$ を解くために解くべき、 Q 上の既約方程式は、 $N = n!/(n-m)!$ 次式であり、 $F^*(X) = \prod_{\sigma^*} (X - V_j) = \prod_{\sigma^*} \{X - (A_1 \alpha_1 + \cdots + A_m \alpha_m + \cdots + A_n \alpha_n)\} = 0$ 、または $F_Q^*(X) = \prod_{\sigma^*} (X - V^*_k) = \prod_{\sigma^*} \{X - (A_1 \alpha_1 + \cdots + A_m \alpha_m)\} = 0$ のいずれでもよい。

ただし、 m 根で書いた V^*_k で全根を表せるか、すなわち $F_Q^*(X)$ が作れるか否かは、 $F^*(X)$ が有理係数になるか否かで判定される (4 章； $m=2$ の場合で証明した)。

$Q(V_1) = Q(\alpha_1, \cdots, \alpha_n)$ だから、 $Q(V_1) = \cdots = Q(V_{n!})$ は常に成り立つ ($V_1 \sim V_{n!}$ は可約方程式 $F_Q(X) = 0$ の解)。一方、ガロア拡大体 Γ とは、既約方程式の解を添加した体と考え、 $Q(V_1) = \cdots = Q(V_N) = \Gamma$ 、または $Q(V^*_1) = \cdots = Q(V^*_N) = \Gamma$ 、と書くのが適切である (同型写像は、既約方程式に適用される：116 頁)。

V_1, V^*_1 いずれを使ってもよく、共通点は、位数 N の自己同型群 $\{\sigma^*\}$ である。

$f(x) = 0$ の根構造を反映する概念は、“ガロア拡大体 Γ の自己同型群”と分かった。

まとめ： Γ の自己同型群は、任意文字係数の方程式で位数 $n!$ の $\{\sigma\}$ であり、任意 m 根の V^*_k で単拡大できる既約方程式では $\{\sigma^*\}$ となる。 $\{\sigma^*\} \subset \{\sigma\}$

以後は、 V^*_1 を * なしで、 $m=n$ の場合も含め、 $V_1 = A_1 \alpha_1 + \cdots + A_m \alpha_m$ と書くことにする。 Q 上の自己同型群も、位数 $N = n!$ の場合を含め、 $\{\sigma^*\}$ でなく $\{\sigma\}$ と書く。

1-2. V_1 を解にもつ“中間体 L ”上の既約方程式、および L 上の自己同型群

再掲： Q 上の既約方程式、 $F_Q(X) = X^N - (V_1 + \cdots + V_N)X^{N-1} + \cdots \pm V_1 \cdots V_N = 0$ を解いて V_1 を得れば、ガロア拡大体 $\Gamma = Q(V_1) = \cdots = Q(V_N)$ を得る。

$F_Q(X) = 0$ を解くとは、因数分解を進め、 $(X - V_1) = 0$ に達することである。分解の途中段階を考えよう（どの段階でも、目指す解は $V_1 = A_1 \alpha_1 + \cdots + A_m \alpha_m$ である）。

1) L 上の既約方程式、 $F_L(X) = 0$

因数分解の過程で、 N 次式 $F_Q(X)$ の中の或る既約因子を得たとして、次数を L と呼び、その既約因子の構成成分を $V_1 \sim V_L$ と名付ければ（命名しただけで選び方は未知）、 $F_L(X) = X^L - (V_1 + \cdots + V_L)X^{L-1} + \cdots \pm V_1 \cdots V_L$ 、 $L < N$ 、と書ける。

$F_L(X)$ の係数値（ $V_1 \sim V_L$ の基本対称式の値）が算出されたら、 $F_Q(X)$ が因数分解され、解 V_1 を与える方程式が、 $F_Q(X) = 0$ から、 $F_L(X) = 0$ に還元される。

すると中間体の語義そのものから、 $F_L(X)$ の係数値は“ Γ に至る中間体の要素”である。この中間体を L と呼べば、 $F_L(X)$ の係数 $\in L$ である。

$F_Q(X) = 0$ の解 V_1 が得られるなら、前述のとおり $Q(V_1) = Q(\alpha_1, \cdots, \alpha_n)$ となる（が、一気には実現しない）。 $F_L(X) = 0$ の解として V_1 が得られるなら（これも一気には実現しないが）、 $L(V_1) = Q(\alpha_1, \cdots, \alpha_n)$ であり、 L 上の共役体 $L(V_1) = \cdots = L(V_L) = \Gamma$ は、言葉の定義から、 L のガロア拡大体である。「 Q のガロア拡大体」を求める課題が、「中間体 L のガロア拡大体」を求める課題に更新されて、解法が進む。

2) ガロア拡大体 $\Gamma = L(V_j)$ の、 L 上の自己同型群

L 上の方程式 $F_L(X) = 0$ の共役解 $V_1 \sim V_L$ を写し合う同型写像を、 τ （タウ）と呼び、すべての $\tau, \tau', \cdots$ を含む集合を $\{\tau\}$ とする（恒等写像；任意 j で $V_j \rightarrow V_j$ 、も含む）。

ガロア拡大体の定義により Γ は、すべての τ で Γ 自身に写る。

すべての τ の集合を $\{\tau\}$ と定義したから、 Γ が、 τ で Γ に写り、 τ' で Γ に写れば、 $\tau\tau'$ でも Γ に写り、恒等写像でも Γ に写る。したがって、 $\{\tau\}$ は群である（これは自明とはいえ、概念の定義が導いた発展性といえる）。

$\{\tau\}$ は、 L 上の共役体を写すのだから、 L 上の自己同型群と呼べる。

根 $\alpha_1 \sim \alpha_n$ を写すことにより、「 $\{\sigma\}$ は $V_1 \sim V_N$ を写し」、「 $\{\tau\}$ は（ $V_1 \sim V_N$ の一部をなす） $V_1 \sim V_L$ を写す」から、 $\{\sigma\} \supset \{\tau\}$ である。

中間体の上に乗ると、自己同型群が、部分群に縮小する（123頁図）。

3) 本節のまとめ

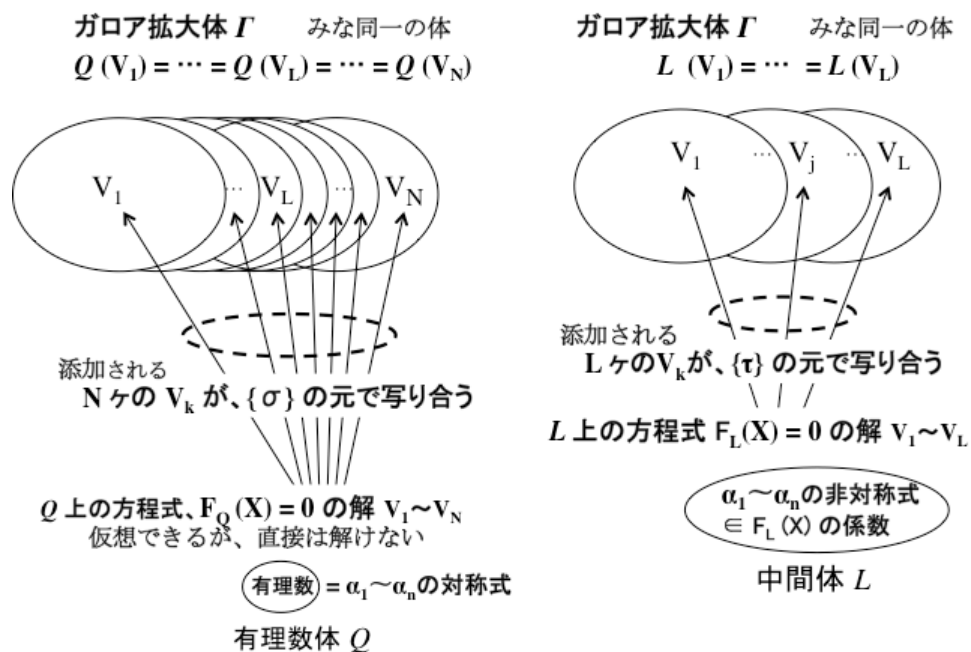
$F_Q(X)$ を因数分解して因子 $F_L(X)$ を得るとは、 $F_L(X)$ の係数値（ $V_1 \sim V_L$ の基本対

称式) が、 $F_Q(X)$ の係数値 ($V_1 \sim V_N$ の基本対称式) から代数計算できることである。

今までの予備説明で、親しみにくいのは、“… 上の …” という言葉であろう (… 上の方程式、… 上の共役体、… 上の同型写像、という非日常語は記憶に定着しにくい)。この言葉に注意を集中し、以下を復習してみよう。

- ・ 或る体を L と呼ぶ。 L 上の既約方程式の解は、 L の要素ではない。この既約方程式の共役解を L に添加した拡大体が、“ L 上の共役体” である。 $L \subset L$ 上の共役体
体上の方程式を、 Q 上で $F_Q(X)=0$ 、拡大体 L 上では $F_L(X)=0$ と呼んだ。
- ・ L 上の同型写像は、 L 上の既約方程式の解を写し、 L 上の共役体を写し合う。

図 ガロア拡大体の、「 Q 上の自己同型群 $\{\sigma\}$ 」、「 L 上の自己同型群 $\{\tau\}$ 」



2. ガロア群の定義と定理

2-1. ガロア群の定義

再掲 ; $\Gamma = Q(V_1) = \cdots = Q(V_N) : Q$ 上の共役体がみな一致すれば、ガロア拡大体 Γ と呼ぶ
 $V_1 \sim V_N$ を写し合う、 Q 上の自己同型写像の集合 $\{\sigma\}$ は、群をなす

(121 頁で、 $\{\sigma\}$ 、 $\{\sigma^*\}$ を区別して説明し、以後一括して $\{\sigma\}$ と書いている)

- ・ 上記の $\{\sigma\}$ を、 $f(x)=0$ の“ガロア群”と呼び、 $\text{Gal}(\Gamma/Q)$ と表記する。
- ・ 中間体 L 上では、 Γ の、 L 上の自己同型群 $\{\tau\}$ を、ガロア群 $\text{Gal}(\Gamma/L)$ と呼ぶ。
 $\{\sigma\} \supset \{\tau\}$ 、すなわち $\text{Gal}(\Gamma/L)$ は、 $\text{Gal}(\Gamma/Q)$ の部分群である (上図)。

2-2. ガロア群が満たす定理

解法の出発点になる体は、 n 次既約方程式 $f(x)=0$ の係数が属する、有理数体 Q である。 $f(x)=0$ の共役根すべてを $\alpha_1 \sim \alpha_n$ と書く。

下記 I、II はふつう一括され、“ガロアの基本定理”とも呼ばれる（原著では 69 頁）

I. 解法の出発点における、ガロア群が満たす定理

- 1) 或る代数的数が、 $\text{Gal}(\Gamma/Q)$ で不変なら、その数は有理数 ($\in Q$) である
- 2) 或る代数的数が、 Q の要素なら、その数は、 $\text{Gal}(\Gamma/Q)$ で不変である

$\text{Gal}(\Gamma/Q)$ は、前節で $\{\sigma\}$ と略記したものである

1) の証明：我々が扱う代数的数は、 $f(x)=0$ の根の有理式である（巾開方は非対称な有理式になりうる；114 頁）。或る代数的数を θ と呼ぶと、 $\theta = \theta(\alpha_1, \dots, \alpha_n)$ と書ける。単拡大の原理で、 $\alpha_1 \sim \alpha_n$ は V_1 の整式 ($\in Q(V_1)$) で表せるから、 $\theta = \Theta(V_1)$ と書ける。

$\text{Gal}(\Gamma/Q)$ の元で写り合う全ての $V_1 \sim V_N$ で作った、 $F_Q(X) = (X - V_1) \cdots (X - V_N)$ は、有理係数をもつと証明した（120 頁では $F_Q(X)$ 、 $F_Q^*(X)$ に書き分けたが、今は一括する）。

定理が言うように、 θ が $\text{Gal}(\Gamma/Q)$ で不変なら、 $\theta = \Theta(V_1) = \cdots = \Theta(V_N)$ だから、 θ は $V_1 \sim V_N$ の対称式でも書ける（121 頁）、すると $V_1 \sim V_N$ の基本対称式すなわち $F_Q(X)$ の係数（有理数）で表せる。 θ が有理数だと証明された。

今、体の要素として終始一貫、1 つの方程式 $f(x)=0$ の根からなる代数的数だけを扱うと考えている（1 の巾乗根も同時に扱う課題は、後で考える # ♪ 132 頁）。有理数は、任意の有理数から有理計算できるから、 Q の任意要素は、 $\alpha_1 \sim \alpha_n$ の対称式で表せる。

2) は自明である：有理数は任意の同型写像で不変（115 頁）であり、 $\text{Gal}(\Gamma/Q)$ の元は自己同型写像だから、 Q の要素は、 $\text{Gal}(\Gamma/Q)$ で不変である。

II. 縮小したガロア群が満たす定理

ガロア拡大体 Γ に至る、中間体の 1 つを、 L と呼ぶ ($Q \subset L \subset \Gamma$)

ガロア群 $\text{Gal}(\Gamma/L)$ とは、 Γ の、 L 上の自己同型群、つまり 123 頁の $\{\tau\}$

- 1) 或る代数的数が、群 $\text{Gal}(\Gamma/L)$ で不変なら、その数は、体 L の要素である
- 2) 或る代数的数が、 L の要素なら、その数は、 $\text{Gal}(\Gamma/L)$ で不変である

122 頁 1-2 で、 $F_L(X)$ が、 $F_Q(X)$ の因数分解で算出できる式なら、 $F_L(X)$ の係数を含む体が、すなわち中間体であると述べ、 L と呼んだ。以下では、中間体が得られるなら L と呼び、 L 上の自己同型群で不変な方程式を作って、 $F_L(X)=0$ と名付ける（本章の中で最も抽象的な部分である）。本定理から、中間体を得る後述の方法に進める。

【準備】まず、 L 上の自己同型群 $\text{Gal}(\Gamma/L)$ で不変な、代数的数の“実例”を作る。

$\text{Gal}(\Gamma/L)$ の位数を L と呼び、元を τ_k と総称すれば、 V_1 の写像 L_k が（すべての元

を使って)、 $\tau_0(V_1) = V_1$ 、 $\tau_1(V_1) = V_2$ 、 $\dots$ 、 $\tau_{L-1}(V_1) = V_L$ 、と書ける。

X の方程式、 $\Pi(X - V_k) = X^L - (V_1 + \dots + V_L)X^{L-1} + \dots \pm V_1 V_2 \dots V_L = 0$ を作り、 $F_L(X) = 0$ と名付ける。 $\text{Gal}(\Gamma/L)$ が群だから ($V_1 \sim V_L$ の 1 つは $V_1 \sim V_L$ の 1 つに写るから)、 $F_L(X)$ の係数は、 $\text{Gal}(\Gamma/L)$ で不変である。

知ったとおり、 $F_Q(X) = 0$ の解 $V_1 \sim V_N$ で、 $Q(V_1) = \dots = Q(V_N) = \Gamma$ だから、その一部をなす $F_L(X) = 0$ の解 $V_1 \sim V_L$ でも当然、 $Q(V_1) = \dots = Q(V_L) = \Gamma$ となる。

すると、「 Γ の、 L 上の自己同型群」という $\text{Gal}(\Gamma/L)$ の語義により、 $F_L(X)$ を L 上の方程式と呼べるから (係数が属する体の名が L)、その係数 $\in L$ である (123 頁図)。

また、ガロア群の位数に等しい L ケの共役解 ($V_1 \sim V_L$) が、相互に写り合うのだから、 $F_L(X)$ は既約式である (可約なら L ケのうちの一部分だけが写り合う ; 116 頁#)。

$\text{Gal}(\Gamma/L)$ 不変量かつ体 L の要素、という実例が、 $F_L(X)$ の“係数”として作れた。

1) の証明 (前記 I の証明の反復である。ここでは代数的数を θ' と総称する)

$\text{Gal}(\Gamma/L)$ で不変な代数的数すべてが、上記のように作った「 $F_L(X)$ の係数 $\in L$ 」から有理計算できると言えれば、1) が証明される。

単拡大の原理から、 $\alpha_1, \dots, \alpha_n$ は V_1 の整式で表せるので ($\in Q(V_1)$)、 $\alpha_1 \sim \alpha_n$ からなる代数的数を θ' と呼ぶと、 $\theta' = \theta'(\alpha_1, \dots, \alpha_n) = \theta'(V_1)$ と書ける。

定理が言うように、 θ' が $\text{Gal}(K/L)$ の元で不変なら、 $\theta'(V_1) = \dots = \theta'(V_L)$ 、すると $\theta' = \theta'(V_1)$ が、 $V_1 \sim V_L$ の対称式でも (すなわち $V_1 \sim V_L$ の基本対称式で) 書ける、と分かった。 θ' が、「 $F_L(X)$ の係数 $\in L$ 」から有理計算できると証明された。

2) の証明

1) の説明と同様、扱う代数的数は、 $\varphi = \varphi(\alpha_1, \dots, \alpha_n) = \Phi(V_1)$ と書ける。 $\varphi \in L$ だとして、 $\varphi = \Phi(V_1) = \Lambda$ (ラムダ) $\in L$ と書く。左記を「 X の方程式 $\Phi(X) - \Lambda = 0$ が、 $X = V_1$ を解にもつ」と読み直す。この方程式は、1) の $F_L(X) = 0$ と、解 V_1 を共有する。 $F_L(X)$ は既約式だから (前述【準備】)、互除法の定理 (15 頁) より、 $\{\Phi(X) - \Lambda\}$ が、 $F_L(X)$ で割り切れる。すると、 $F_L(X) = 0$ の解 $V_1 \sim V_L$ はみな、 $\Phi(X) - \Lambda = 0$ の解になるから、 $\Phi(V_1) = \dots = \Phi(V_L) = \Lambda$ 。すなわち、 φ の値は、 $V_1 \sim V_L$ の任意入れ替えで不変と分かり、 $\text{Gal}(\Gamma/L)$ の任意元で不変と証明された。

【注釈】定理の目的と、或る代数的数とは何か？について： $F_Q(X) = 0$ の解 V_1 を得るために因数分解する、その途中で得る因子を $F_L(X)$ と呼んだ。因数分解を実現させるには、 $F_L(X)$ だけでなく、 $F_Q(X) = F_L(X) \times A(X) \times B(X) \times \dots$ の、全因子を考察せねばならない。各因子どうし、および $F_Q(X)$ との間の写像関係の分析が“目的”、“或る代数的数”とは右辺各因子の係数の構成成分である。

2-3. $\text{Gal}(\Gamma/L)$ の位数、拡大次数 $[\Gamma:L]$ 、 L 上の方程式の次数、の関係

1) L 上の方程式の具体形

有理数体 Q から始めて、段階的に拡大体 (L と総称) を作り、 Γ に至る方法論が準備できた。今までのことを整理する。解 V_1 を与える、 L 上の既約方程式を、改めて

$$F_L(X) = X^L + \lambda_{L-1}X^{L-1} + \cdots + \lambda_1X + \lambda_0 = 0 \quad \cdots \star \quad \text{と書こう。}$$

$\lambda_{L-1}, \cdots, \lambda_0$ は、 $f(x)$ の係数を代数計算した (巾開方量を含む) 値だとする。一方、 $F_L(X) = X^L - (V_1 + \cdots + V_L)X^{L-1} + \cdots \pm V_1V_2\cdots V_L = 0 \quad \cdots \star$ とも書けるから、 $V_1 \sim V_L$ の基本対称式 ($\alpha_1 \sim \alpha_n$ の非対称式を含んだ有理式) の値でもある。すなわち 根の非対称式が、根の対称式の巾開方量 で書かれることになる (114 頁)。

☆、★の係数 ($\in$ 中間体 L) の一部を、 $f(x) = x^3 + ax^2 + bx + c = 0$ の根で例示すると $V_1V_2V_3 = (A^3 + B^3 + C^3 + 3ABC) \alpha\beta\gamma + ABC(\alpha^3 + \beta^3 + \gamma^3) + (A^2B + B^2C + C^2A)(\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha) + (AB^2 + BC^2 + CA^2)(\alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2)$ 、である (73 頁)。

$\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha$ 、 $\alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2 = 1/2 [ab - 3c \pm \sqrt{\{(-ab + 3c)^2 - 4(b^3 - 6abc + 9c^2 + a^3c)\}}]$ なので (24 頁)、 $\lambda_0 = -V_1V_2V_3$ は、有理数と $\sqrt{\text{(有理数)}}$ からなる代数的数である。

$\text{Gal}(\Gamma/L) = \{\tau_0, \tau_1, \cdots, \tau_{L-1}\}$ の位数を L と呼んだから、 $F_L(X) = 0$ は、 L 次方程式 である。共役解 $V_1 \sim V_L$ を体 L に添加すれば、ガロア拡大体 Γ になる。すでに知った単拡大の原理により、 $L(V_1, \cdots, V_L) = L(V_1) = \Gamma$ 、すなわち、 L 次方程式の解 1 つを L に添加すれば Γ になるから (拡大次数は 112 頁の話と違って $L!$ でなく)、 $[\Gamma:L] = L$ である。

群 $\text{Gal}(\Gamma/L)$ の位数 = 体の拡大次数 $[\Gamma:L] = L$ 上の既約方程式の次数、となる。

2) 有理数体 Q から、ガロア拡大体 Γ に至るまでのイメージ

拡大次数とは (112 頁で、代数的数が属するベクトル空間の次元に喩えたが、ここでは)、 Q から Γ へ至る距離、 L から Γ へ至る距離、 $\cdots$ 、のようにイメージできる。代数的数を添加して $Q \rightarrow L \rightarrow M$ と登る、と考えるよりも、解 V_1 を与える方程式の次数が、「 $Q \rightarrow \Gamma$ 」 $\rightarrow$ 「 $L \rightarrow \Gamma$ 」 $\rightarrow$ 「 $M \rightarrow \Gamma$ 」と“更新”され下がっていくとみるのが適切である。

$\text{Gal}(\Gamma/Q)$ の位数 $= [\Gamma:Q]$ $[\Gamma:Q] = N$ とする。 $Q \rightarrow \cdots \rightarrow \Gamma$
体の拡大 (群の縮小) 過程は下記のように進む

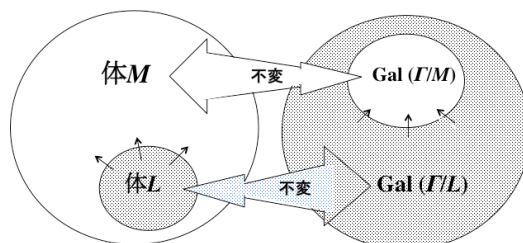
$\text{Gal}(\Gamma/L)$ の位数 $= [\Gamma:L]$ この値を前項で L と呼んだ。 $L \rightarrow \cdots \rightarrow \Gamma$

$\text{Gal}(\Gamma/M)$ の位数 $= [\Gamma:M]$ この値を以下で M とする。 $M \rightarrow \cdots \rightarrow \Gamma$
方程式が解けるときのガロア群を、 $\{e\}$ と書く。

ガロア群は縮小、 $\text{Gal}(\Gamma/Q) \supset \text{Gal}(\Gamma/L) \supset \text{Gal}(\Gamma/M) \supset \{e\}$ 、位数 $N > L > M > 1$ 、体は拡大する、 $Q \subset L \subset M \subset \Gamma$

ガロアの基本定理（124 頁）は、下図のような関係を述べている。

図 <群と体の、このような表裏一体の関係を双対/ツイ性という>



3. 方程式 $f(x) = 0$ が解かれる道筋

方程式を解く過程を、体の拡大と説明すれば、拡大が解法にみえるが、計算は（基本的には）逆である。「 Q から始め、既知となった代数的数を添加し、より大きな拡大体を得て I に達する」概念を語るが、実際は「 I の未知要素を、より小さな体の未知要素で表す」計算をして、拡大の由来を遡り「 Q の要素で表せた」とき、根の値を得る。拡大する概念は順行、拡大を実現させた計算は逆行のイメージで理解しよう。

今から、 n 次方程式の一般解法を考えるので、 $f(x) = 0$ の係数は任意文字とする。

$\text{Gal}(I/Q)$ の元による、 V_1 の自己同型写像のすべて、 $V_1, \dots, V_k, \dots, V_{n!}$ で作った、 $F_Q(X) = \Pi(X - V_k)$ の展開式 $= 0$ は、 $X = V_1$ を解にもち、 $\text{Gal}(I/Q)$ で不変、すなわち有理係数方程式だから、これを解けばよいのであった（120 頁）。

I) 任意文字係数の $f(x) = 0$ の根からは、 $n!$ 個の異なる V_k が生じるから、

Q が含む“根の式” は、“ $V_1 \sim V_{n!}$ の（基本）対称式”である。

解きたい Q 上の方程式、 $F_Q(X) = X^{n!} - (V_1 + \dots + V_{n!})X^{n!-1} + \dots \pm V_1 V_2 \dots V_{n!} = 0$

の係数は、 $f(x)$ の係数（ $\alpha_1 \sim \alpha_n$ の基本対称式）と同様に対称式ではあるが、

求めたい“ $\alpha_1 \sim \alpha_n$ の非対称式すべて”を含む和積から成り立っている。

$F_Q(X) = 0$ が解かれる途中段階を考えよう（前述の順行 $\downarrow$ ・逆行 $\uparrow$ を意識する）。

$\downarrow \uparrow$

II) L が含む“根の式” は、 L 個の V_k からなる“ $V_1 \sim V_L$ の基本対称式”である。

L 上の方程式、 $F_L(X) = X^L - (V_1 + \dots + V_L)X^{L-1} + \dots \pm V_1 V_2 \dots V_L = 0$ を解きたい。

$V_1 \sim V_{n!}$ の一部をなす $V_1 \sim V_L$ が、どう選ばれたかは、次の段階の一组（ $V_1 \sim V_L$ の一部をなす） $V_1 \sim V_M$ が、どう選ばれるかを考える連鎖で、いずれ分かる。

$\downarrow \uparrow$

III) M が含む“根の式” は、 M 個の V_k からなる“ $V_1 \sim V_M$ の基本対称式”である。

段階的に進む過程を考えているから、 $V_1 \sim V_M$ は当然、 $V_1 \sim V_L$ の一部である。

M 上の方程式、 $F_M(X) = X^M - (V_1 + \dots + V_M)X^{M-1} + \dots \pm V_1 V_2 \dots V_M = 0$ を解きたい。

↓ ↑

↓ ↑ 上記と同様の過程を経て、

IV) Γ が含む“根の式”は、 V_1 に到達し（どの V_k でもよい）、解くべき方程式は、
 $X - V_1 = 0$ となる。これは Γ 上でなく Γ の中にあり、有理的に $X = V_1$ と解ける。

注釈： $f(x)=0$ が、任意文字係数でなく、“位数 N のガロア群 $\text{Gal}(\Gamma/Q)$ で表現される係数関係”をもつ方程式だったら、上記の $n!$ を N に置き換えればよい。

4. 代数方程式が解けるための必要十分条件

4-1. 必要条件：“拡大体 L の要素”と“より大きい拡大体 M の要素”を結ぶ 計算法が存在するための前提

L とその拡大体 M の関係を調べれば、すべての拡大体が結べる条件が分かる。

$F_L(X)=0$ の共役解 $V_1 \sim V_L$ のうちの一部が、 $F_M(X)=0$ の共役解 $V_1 \sim V_M$ だから、
 $V_1 \sim V_M$ を写す $\text{Gal}(\Gamma/M)$ は明らかに、 $V_1 \sim V_L$ を写す $\text{Gal}(\Gamma/L)$ の部分群である。

$L \ni F_L(X)$ の係数成分、 $M \ni F_M(X)$ の係数成分である。

簡素化のために群の名を、 $\text{Gal}(\Gamma/L) = L$ 、 $\text{Gal}(\Gamma/M) = M$ 、と書く。 $L \supset M$

体の拡大、 $L \rightarrow M$ が実現する、という意味は（群は縮小、体は拡大：127 頁図）、
「 L の要素の巾開方値を、 L に添加すると、 M になる」こと、すなわち
「 M の要素（根の式）が、 L の要素（根の式）の巾開方値を使って有理的に書ける」
ことである。“ガロアの基本定理（124 頁）”を使って、言い換えると、下記 A になる。
「群 M で不変な量が、群 L 不変量の巾開方値を使って有理的に書ける」… A
重要な注意点： L 不変量の巾開方値は、 L 不変量と言えない（この意味は 22
頁参照）。例えば、 $\sqrt{\{(\alpha + \beta)^2 - 4\alpha\beta\}} = \sqrt{(\text{対称式})} = \pm(\alpha - \beta) = \text{非対称式}$
すなわち、「 L で移り変わる量を使って、 M 不変量を有理的に書ける」… A'
以上から、下記のことが導かれる。

体 L の要素を、 $\lambda, \lambda', \dots$ 、体 M の要素を、 $\mu, \mu', \dots$ 、などと書こう。

群 L の或る元（写像）を τ と呼び、 $\tau(\mu) = \mu'$ と書く。 μ が、“ $\lambda, \lambda', \dots$ の巾開方量
（ L で変化する値）”を含む有理式で書かれていれば、一般に $\mu' \neq \mu$ である。

一方、ガロアの定理（体 M の要素は群 M で不変）より、 M の任意元 η_j, η_k で、
 $\eta_j(\mu) = \mu, \eta_k(\mu) = \mu$ だから、 $\tau \eta_j(\mu) = \tau(\mu) = \mu'$ 、同様に、 $\eta_k \tau(\mu) = \eta_k(\mu') = \mu'$ となる。

写像集合 $\{\tau \eta_j\}, \{\eta_k \tau\}$ はともに、 M の任意要素 μ を、対応する μ' に写す写像「す
べて」からなるので、 $\{\tau \eta_j\} = \{\eta_k \tau\}$ 、つまり「任意 $\tau \in L$ で、 $\tau M = M \tau$ 」と書ける。

このとき、 M は、 L の正規部分群と呼ばれる（81 頁）… B

A (ないし A') が成り立てば B となるから、B は A (A') の必要条件である。

4-2. 十分条件：M の要素が、実際に L の要素から計算できる条件

1) 群による記述

3 章 4 章の群論の定理をフル活用する (疑問なら 42-44 頁、83-84 頁参照)。

群一般は、部分群で必ず剰余類分割できるから、 $L = \{M, \tau_1 M, \tau_2 M, \dots, \tau_q M\}$ 、
となる元 $\tau_1, \tau_2, \dots, \tau_q \in L$ 、が存在する。 $q = (L \text{ の位数}) / (M \text{ の位数}) = L/M$

群 M が、L の正規部分群 ($\tau_k M = M \tau_k$) なら、上記の剰余類は、“剰余類群” をなす。
すなわち $\tau_k M$ が、一塊となって群の元と同じ振る舞いをする。

すると「群の部分群には、素数 q の元からなる巡回群が必ず存在する」定理より、
 $L \supset M' = \{M, \tau M, \dots, \tau^{p-1} M\}$ 、という巡回 (剰余類) 群 M' が存在する (p は素数)。

この τ は (前頁、L の任意元の総称でなく)、 $\tau_1, \dots, \tau_q$ のどれかを意味する。

$\tau^k M = M \tau^k$ だから (上記 B)、L の正規部分群 M は、 M' の正規部分群でもある。

- $L = M'$ なら、 $L = \{M, \tau M, \dots, \tau^{p-1} M\}$ 、と M の巡回 (剰余類) 群で書ける。
- $L \neq M'$ なら、 $M' = \{M, \tau M, \dots, \tau^{p-1} M\}$ と書き、次に L を M' の巡回 (剰余類) 群で書く試みに進むが、試みを実現するには、 M' が L の正規部分群になる必要がある。
これは必ずしも成り立たない。以下をみよう。

$M' \tau' = M \tau^k \tau'$ 、一方、 $\tau' M' = \tau' \tau^k M = M \tau' \tau^k$ (正規部分群の性質) だから、任意 $\tau' \in L$ で、 $M \tau' \tau^k = M \tau^k \tau'$ が成り立つときのみ、 $M' \tau' = \tau' M'$ (M' が L の正規部分群) となる。

成り立たなければ (前記、必要条件が満たされないから) 方程式は解けない。

成り立てば、L を、 M' の巡回群 (巡回剰余類群) で書ける、または M' よりも大きな正規部分群 M'' の巡回群 (巡回剰余類群) で書ける可能性に繋がる。

正規部分群を (意味する記号) $\triangleright$ で書けば、隣の群による剰余類の巡回群で書く系列が、繋がるイメージは、 $L \cdots \triangleright M$ 、 $L \cdots \triangleright M' \triangleright M$ 、 $L \triangleright M'' \triangleright M' \triangleright M$
(隣の群との位数比 p が非素数でも、巡回群は実現しうるが、その次で実現しなくなる : 87 頁)

2) 体による記述

体の言葉で言えば、「体 L を (M' に拡大し、必要なら M'' も経て) M へ拡大する」方法を知りたい。各段階の拡大法の説明は共通だから、使う記号を簡素化するため、体 L が、(M' 、 M'' を経ずに) 一段階で体 M に拡大される、として記述しよう。

L の要素と M の要素を結ぶ計算原理は、剰余類がなす巡回群を利用した、天才的なガロアの手法で得られる。すなわち、

$$L = \{M, \tau M, \tau^2 M, \dots, \tau^{p-1} M\} \quad \cdots \star$$

体 M の或る要素 (群 M 不変量) を、 θ_1 とする (前述 μ の構成成分を意味する)。

$\tau(\theta_1) = \theta_2$ 、 $\tau^2(\theta_1) = \theta_3$ 、 $\dots$ 、 $\tau^{p-1}(\theta_1) = \theta_p$ と書き、**1 の原始 p 乗根** を ω と書けば、

$$\Theta = (\theta_1 + \omega \theta_2 + \omega^2 \theta_3 + \dots + \omega^{p-1} \theta_p)^p \quad \dots \star$$

は、群 L 不変量だと分かる。

なぜなら、 $\tau^k(\Theta) = (1/\omega^k)^p \times \Theta = \Theta$ 、 θ_j は M で不変だから、 Θ は、 M 、 τ^k で不変。

Θ は、正確には L の要素でなく、 $L(\omega)$ の要素である (下記、*注)。

体の要素どうし、 $\Theta \in L(\omega)$ と、 $\theta_j \in M$ が、等式 $\star$ で結ばれた。

【*注 ; ω の代数計算】 体拡大では、 $\text{Gal}(F/L)$ と $\text{Gal}(F/M)$ の位数比 $= p$ に応じ、**1 の p 乗根** を添加する必要がある。つまり解きたい方程式 $f(x) = 0$ と別に、二項方程式、 $x^n - 1 = 0$ の一般解法を要する。この解が代数的に求まることは、ガロア拡大の (ここに引用しない) 定理と数学的帰納法で証明されるが、本書では、ガロアが論じた範囲で理解する趣旨 (8 頁) から、1 の n 乗根は代数計算可能と認めて先に進む。

3) M の要素 $\theta_1 \sim \theta_p$ を、 $L(\omega)$ の要素の巾開方値を使って表す計算法

p は素数とし、 $x^p - 1 = 0$ の根を、 $\omega_0, \omega_1, \dots, \omega_{p-1}$ と書き、 $\omega_0 = 1$ とする。

$(x^p - 1)/(x - 1) = x^{p-1} + \dots + x + 1 = 0$ の任意根は原始根、その 1 つを ω として、

$\omega_1 = \omega$ 、 $\omega_2 = \omega^2$ 、 $\dots$ 、 $\omega_{p-1} = \omega^{p-1}$ 、とも書ける。 $\omega_0 = \omega^p = 1$ である。

$\omega_0 \sim \omega_{p-1}$ を写す同型写像の群を、 $P_\omega = \{\rho^0, \rho, \rho^2, \dots, \rho^{p-1}\}$ とする (ρ^0 は恒等写像)。

まず、上記 $\star$ のように書かれた $L(\omega)$ の要素に、 P_ω を作用させると、

$\rho(\omega_k) = \omega_{k+1}$ 、 $\rho^m(\omega_k) = \omega_{k+m}$ 、 $\rho(\Theta_k) = \Theta_{k+1}$ 、 $\rho^m(\Theta_k) = \Theta_{k+m}$ 、と写る (添え字は、mod p で書く)。

$$\Theta_0 = (\theta_1 + \omega_0 \theta_2 + \omega_0^2 \theta_3 + \dots + \omega_0^{p-1} \theta_p)^p$$

$$\Theta_1 = (\theta_1 + \omega_1 \theta_2 + \omega_1^2 \theta_3 + \dots + \omega_1^{p-1} \theta_p)^p$$

$$\Theta_2 = (\theta_1 + \omega_2 \theta_2 + \omega_2^2 \theta_3 + \dots + \omega_2^{p-1} \theta_p)^p$$

.....

上記から、(または $\star$ の巾開方を、 $\omega_p \sqrt{\Theta} = \theta_1 + \omega \theta_2 + \omega^2 \theta_3 + \dots + \omega^{p-1} \theta_p$ 、と書き、 P_ω の元を作用させると) 下記の連立 1 次方程式が得られ (表記法の説明 25 頁)、**「 $M(\omega) \ni \theta_1, \dots, \theta_p$ 」が、「 $L \ni \Theta_j$ 」の巾開方量と ω から有理計算できる。**

$$\omega_p \sqrt{\Theta_0} = \theta_1 + \theta_2 + \dots + \theta_p \quad (\omega_0 = \omega^p = 1)$$

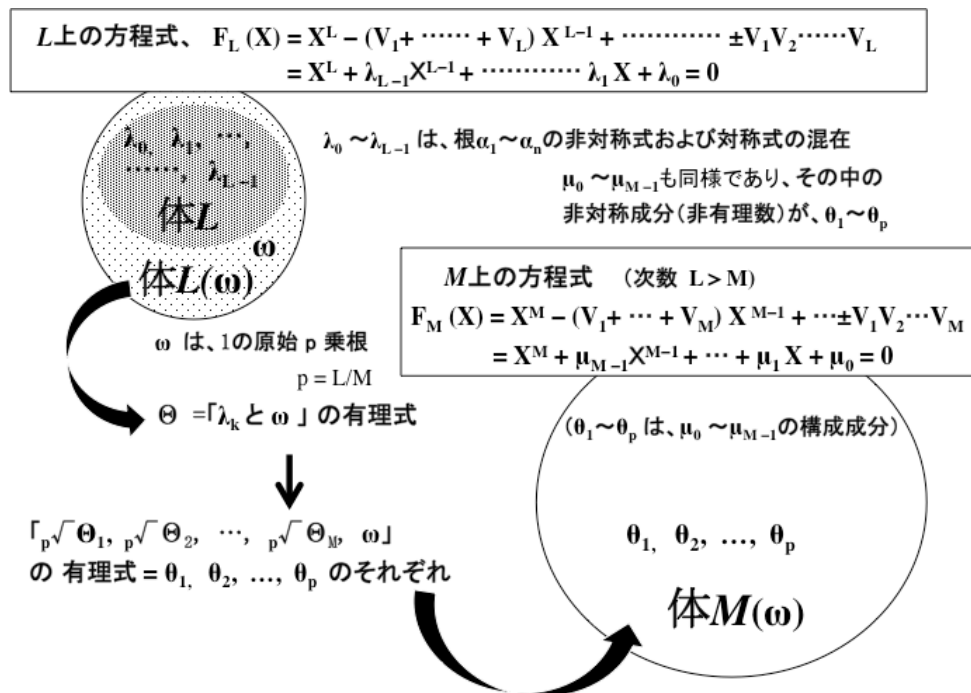
$$\omega_p \sqrt{\Theta_1} = \theta_1 + \omega_1 \theta_2 + \omega_1^2 \theta_3 + \dots + \omega_1^{p-1} \theta_p$$

$$\omega_p \sqrt{\Theta_2} = \theta_1 + \omega_2 \theta_2 + \omega_2^2 \theta_3 + \dots + \omega_2^{p-1} \theta_p$$

.....

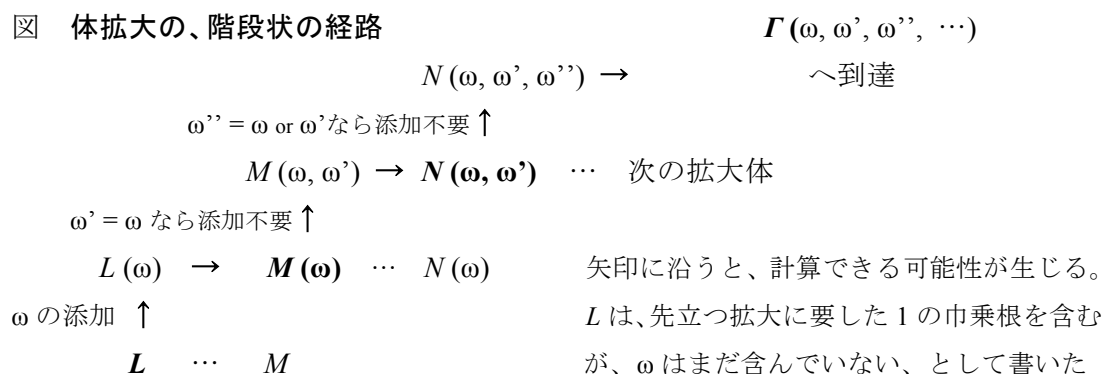
$$\omega_p \sqrt{\Theta_{p-1}} = \theta_1 + \omega_{p-1} \theta_2 + \omega_{p-1}^2 \theta_3 + \dots + \omega_{p-1}^{p-1} \theta_p$$

図 方程式の解法過程で、計算対象となる代数的数の一覧



ガロアは、図の $F_L(X)$ 、 $F_M(X)$ の係数値を終始一貫、計算対象として論じた。これらが、現代論で体の要素とされる。体は、有理計算を何でもこなすから、ユークリッドの互除法も自動計算し、驚くべき単拡大、 $Q(A_1 \alpha_1 + \dots + A_n \alpha_n) = Q(\alpha_1, \dots, \alpha_n)$ も表示する電算機のようなが(デデキントの発明と言われる)、巾開方は、体の外で我々が手計算し、結果を添加して拡大体を作るのも、我々の手作業である。

図 体拡大の、階段状の経路



以上の計算手順(図)、 L から $M(\omega)$ への拡大は、“巾根拡大”と呼ばれる。

M が、 L の正規部分群で、位数比が素数なら、巾根拡大が実現する。これが全段階で成り立てば、 Q から $\Gamma = Q(\alpha_1, \dots, \alpha_n)$ まで巾根拡大できる筈だが、1の巾乗根(総称 ω)の扱い方が、まだ不明確である。以下で考えよう。

体 L の要素を不変に保つガロア群 $\text{Gal}(L/L)$ を、128 頁で L と略記した。

$L(\omega)$ の要素を不変に保つ群の構造は、 ω を写す群 P_ω (130 頁) も含めて考えねばならない。

群の直積という概念で、複数の群による写像を同時に扱える：例えば 2 つの群の直積を、 $G \times H = \{(g_1, h_1), (g_2, h_2), \dots\}$ と書き、元の積を $(g_k, h_k)(g_j, h_j) = (g_k g_j, h_k h_j)$ と定義すれば、 $G \times H$ は群になる。

$L = \{M, \tau M, \tau^2 M, \dots, \tau^{p-1} M\}$ と、 $P_\omega = \{\rho^0, \rho, \rho^2, \dots, \rho^{p-1}\}$ の直積、またはその部分群を考える (p は素数。 ρ^0 は e を意味する)。

ω は原始根だから、 $L(\omega)$ は、 $x^p - 1 = 0$ の全根を含む。 $L(\omega)$ は L 上のガロア拡大体 ($(p-1)$ 次拡大)、ガロア群 P_ω は、正規部分群 $\{\rho^0\}$ による剰余類の巡回群である。

体 $L(\omega)$ の全要素を変化させないガロア群を、(直積の意味で) L_ω と書く。重要なことに、 ω ないし ω^k を変化させない P_ω の元は、恒等写像 ρ^0 しかない。

すなわち、 $L_\omega = L \times \{\rho^0\}$ であり、 L_ω と L は、位数と計算規則が同じ群である。群として**同型**と言う (例えば、3 文字巡回置換が生成する群は、図形を平面内で 120° ずつ廻す回転群と、同型である)。

同様に、 $M(\omega)$ の要素を不変に保つガロア群を M_ω と呼べば、 M_ω と M は、群として同型である (以上のことを厳密に論じると難解なので、本書では概略に留めている)。

したがって、 M が、 L の正規部分群なら、 M_ω は、 L_ω の正規部分群である。

L を、 M による巡回剰余類群で書ければ、 L_ω も、 M_ω による巡回剰余類群で書ける。

【注】 L から $L(\omega)$ へ、そして $M(\omega)$ へ拡大する拡大次数が、2 段階 $(p-1) \times p$ 次でなく、1 段階 p 次になるのは、「 $f(x) = 0$ の根の式」の添加についてだけ算定すればよいからであり、その意味は上記 (L_ω と L 、 M_ω と M が群として同型) から理解される。

n 次方程式 $f(x) = 0$ のガロア群の位数が N なら、ガロア拡大体 $Q(\alpha_1, \dots, \alpha_n) = Q(V_1) = \dots = Q(V_N)$ は、 Q の N 次拡大体であるが、この拡大体は、 $f(x) = 0$ とは別に、2 項方程式、 $x^2 - 1 = 0$ 、 $x^3 - 1 = 0$ 、 $\dots$ 、などの解も、必要に応じ添加するという作成過程を経た、謂わば“複合的な”拡大体である (124 頁# 参照)。

4.3. 方程式が解けるための必要十分条件のまとめ

1 の巾乗根 ω を添加した場合の叙述法が、一応解決したので、 ω に触れずに以下のように言える。

方程式 $f(x) = 0$ の“根 $\alpha_1 \sim \alpha_n$ の式”を、有理数体から始めて段階的に添加し、 $Q \subset \dots \subset L \subset M \subset \dots \subset \Gamma = Q(\alpha_1, \dots, \alpha_n)$ と拡大する計算が実現するためには、ガロア群の系列、 $\text{Gal}(\Gamma/Q) \supset \dots \supset \text{Gal}(\Gamma/L) \supset \text{Gal}(\Gamma/M) \supset \dots \supset \{e\}$ において、各群が、隣接する正規部分群による剰余類の巡回群で書けることが、必要十分である。

上記の系列条件を満たすガロア群 $\text{Gal}(\Gamma/Q)$ は、“可解群”と呼ばれる。

ガロア群が可解群なら、 Q から $\Gamma = Q(\alpha_1, \dots, \alpha_n)$ への“巾根拡大”が実現する。

(隣接する正規部分群との位数比が“すべて”、素数になることが、可解群である
必須条件どうかは、4章 87 頁などに詳述した。すべてで必須ではない)

同型写像がなす群は、置換群と同等 (群として同型) だと前述した (117 頁)。

任意文字係数の n 次方程式 $f(x) = 0$ のガロア群は、対称群 S_n と同型であり、
 $S_1 = \{e\}$ 、 S_2 、 S_3 、 S_4 は可解群である (3 章 47 頁)。

$n \geq 5$ の S_n は可解群でない。次節で証明するが、5 次以上の方程式一般の解公式が
書けないと分かるだけである。解ける方程式の形は古典論で明示された (4 章 §5)。

§3 5 次以上の方程式に解公式がないことの、現代群論による証明

S_n を剰余類分割する一般解法で、初めに使う部分群は、交代群 A_n である (4 章 90
頁で証明した : 5 章だけ読む人には、これを以下の議論の前提とみなしていただく)。

$n \geq 5$ では、次に A_n を、正規部分群による剰余類の巡回群で書くのが不可能なので
ある。その証明を「草場公邦、ガロワと方程式、東京、朝倉書店、2000 年 : 158 頁」
から引用改変して以下に記す。 【群と元は Arial 文字、太字は単なる強調】

1. 交換子という概念

N が G の正規部分群なら、下記 (1) 左辺の形の群 (N による剰余類がなす巡回群)
が必ず存在する (83-84 頁)。左辺の群 $\subset G$ である。今、左辺の群 $= G$ だとする。

$$\{N, Ng, Ng^2, \dots, Ng^{p-1}\} = G \quad (g \notin N, g \in G) \quad \dots (1)$$

正規部分群の定義より、任意の $n_i \in N$ に対し、 $n_i g = g n_j$ となる元 $n_j \in N$ がある。
この関係を $Ng = gN$ と書く。

上の両辺に、 g を掛ければ、 $Ng^2 = gNg = g^2N$ 、帰納的に $Ng^k = g^kN$

$$\text{このとき、}(Ng^k)(Ng^j) = Ng^{k+j}N = Ng^{j+k}N = (Ng^j)(Ng^k) \quad \dots (2)$$

すなわち剰余類 Ng^k と Ng^j が、あたかも可換のように略記できる。実際は、
 $n_a g^k n_b g^j = n_c g^j n_d g^k$ となる $n_a, n_b, n_c, n_d (\in N)$ の存在を意味する $\dots (3)$

議論の準備ができたので、(1) を満たす N の元はすべて、 G の元 x, y を使っ
て $xyx^{-1}y^{-1}$ の形で書ける、という興味深い定理を証明しよう。

群の規則「 $g_i, g_j \in G$ なら $g_i g_j \in G$ 」を、 $G^2 = G$ と略記する

$xyx^{-1}y^{-1}$ という元は、 x, y の交換子と呼ばれる

・ $x \in N, y \in N$ なら、群の定義から当然、 $xyx^{-1}y^{-1} \in N$

- $x \in Ng^i, y \in Ng^j$ のとき ($i=j$ でもよく、 $i=0$ つまり $x \in N$ でもよい)、
 $Nxy = N^2xy = \underline{NxNy} = NyNx = N^2yx = Nyx$ 下線部は、(2) から導かれる
 上の両辺に $x^{-1}y^{-1}$ を掛ければ、 $Nxyx^{-1}y^{-1} = Ne = N$
 すると群の定義から、 $xyx^{-1}y^{-1} \in N$ と分かる。
- すなわち (1) の関係があれば、**G** の任意 2 元で作った交換子 $xyx^{-1}y^{-1}$ は、
 (x, y が N の元でないときにも) **N** の元になると分かった。

- 逆に、**N** の任意元が、**G** の或る元 x, y で、 $xyx^{-1}y^{-1}$ と書けることを示そう。

問題 (3) を参照 : $n_a g^k n_b g^j = n_c g^j n_d g^k$ を満たす N の元は、必ずある。

n_a を、 N の任意元とする。 G の適当な 2 元を $x = n_c g^j, y = n_d g^k$
 と名付ければ、 $n_a = xyx^{-1}y^{-1}$ と書けることを示せ。

答 (3) を変形すると、 $n_a = xy(g^k n_b g^j)^{-1}$ だから、 $(g^k n_b g^j)^{-1} = x^{-1}y^{-1}$ を示
 そう。逆元をとると、 $g^k n_b g^j = yx = n_d g^k n_c g^j$ だから、 $g^k n_b = n_d g^k n_c$ を言
 えばよい。 $g^k n_b n_c^{-1} = n_d g^k$ と書き直せば、「或る n_1 に対し、 $g^k n_1 = n_2 g^k$
 を満たす $n_2 \in N, g^k \in G$ が、存在するか？」という問題になる。

N は G の正規部分群だから、必ず存在すると分かる。

- 以上から、 $N = \{xyx^{-1}y^{-1}\}$ が分かった。($x=y$ なら、 $xyx^{-1}y^{-1} = e$ となる)

2. $n \geq 5$ では、交代群 A_n を、正規部分群による剰余類の巡回群で書けない

(1) を書き直し、 $A_n = \{N, Ng, \dots, Ng^{p-1}\}, g \notin N, g \in A_n$ だと仮定する。… (1')
 A_n の任意 2 元から作った $xyx^{-1}y^{-1}$ は、前述のとおり (正規部分群) N の元になる
 が、その場合 (1') が矛盾した式になることを示す。

S_n の任意元は、互換の積で表せる (36 頁)。交代群 A_n の任意元は (定義により)、
 偶数ヶの互換の積 = 「互換 2 ヶの積、またはそれらの積」である。

互換 2 ヶの積は ($n \geq 4$ なら)、共通文字のある互換の積、 $(12)(13)$ など、または
共通文字のない互換の積、 $(12)(34)$ など、の 2 種に分類される。前者は $(\text{互換})^2 = e$ 、
 および $(12)(23) = (21)(23)$ など含む。

上記はすべて、 $(12)(13) = (123), (12)(34) = (123)(314), e = (3 \text{ 文字巡回置換})^3$ 、
 のように、3 文字巡回置換で書ける。したがって、

($n \geq 3$ なら) 任意の偶置換は、**3 文字巡回置換**の単独または積で表せる。… (4)

さて、 A_n の或る 2 つの元 x, y が、3 文字巡回置換の単独の形だとしてみよう。

$n=5$ とする。1, 2, 3, 4, 5 を適宜、文字で呼び、異なる文字は異なる数とする。

配列置換の記法上、() 内に同じ数字・文字の重複はないことにも留意する

5 文字で 3 文字巡回置換を 2 つ作ると、共通文字が最低 1 つある。それを 1 とする。

$\mathbf{x} = (1 \ a \ b)$ 、 $\mathbf{y} = (1 \ c \ d)$ $\mathbf{x} = (1 \ a \ b) = (a \ b \ 1) = (b \ 1 \ a)$ だから、1 の配置は任意

$\mathbf{xyx}^{-1}\mathbf{y}^{-1}$ を計算して簡単化しよう。

$\mathbf{xyx}^{-1}\mathbf{y}^{-1} = (1 \ a) (1 \ b) \times (1 \ c) (1 \ d) \times (1 \ b) (1 \ a) \times (1 \ d) (1 \ c)$ と書くと逆置換も見易い。

任意の 5 文字列 1, a, b, c, d に、右から $\mathbf{xyx}^{-1}\mathbf{y}^{-1}$ を掛ける。つまり (1 a) から始めて (1 c) まで 8 つの互換を順に掛けると、d, a, 1, c, b になる。

変化部分だけ書くと、 $1, b, d \rightarrow d, 1, b$ 、対応を保って、 $1, d, b \rightarrow d, b, 1$ と書き直せば、 $\mathbf{xyx}^{-1}\mathbf{y}^{-1} = (1 \ d \ b)$ と分かる。d, b は「1~5 のうち、1 でない異なる 2 数」なら何でもよいのである。1 の代わりに 2 を使えば、 $\mathbf{xyx}^{-1}\mathbf{y}^{-1} = (2 \ p \ q)$ 、「p, q は、1~5 のうち、2 でない異なる 2 数」、同様の任意性をもつ (3 e f)、(4 g h)、(5 i j) も作れる。

すなわち、 $\mathbf{xyx}^{-1}\mathbf{y}^{-1}$ で、任意の 3 文字巡回置換が作れる。前節より $\{\mathbf{xyx}^{-1}\mathbf{y}^{-1}\} = N$ だから、(4) より、N の元の単独または積で、すべての偶置換が表せることになる。したがって、 $N \supset A_5$ だが、むしろ $N \subset A_5$ なのだから、驚いたことに $N = A_5$ となる。(1') を満たす N が A_5 自身だから、 A_5 は (1') のように書けないと分かった。

任意文字係数の 5 次方程式では、ガロア群が S_5 であり、可解条件が、 A_5 の段階で破綻する。根を文字係数で書けない（解公式が書けない）ことが証明された。

$n \geq 6$ なら、 $\mathbf{x} = (a \ b \ c)$ 、 $\mathbf{y} = (d \ e \ f)$ も選べるが、共通文字のない置換は可換だから、 $\mathbf{xyx}^{-1}\mathbf{y}^{-1} = \mathbf{xx}^{-1}\mathbf{yy}^{-1} = \mathbf{e}$ となる。

$\mathbf{x}$ 、 $\mathbf{y}$ に共通文字が 1 つ入っていると、任意の $n \geq 5$ でも、 $\{\mathbf{xyx}^{-1}\mathbf{y}^{-1}\} = A_n$ になると分かるから、 A_n を (1') のように書けない、つまり S_n の可解条件は満たされない。

共通文字が 2 つ入ったら、どんな $\mathbf{xyx}^{-1}\mathbf{y}^{-1}$ になるか、 $n = 4$ の場合をみよう。

<4 次方程式では、上記の結論にならない>

4 文字で、3 文字巡回置換 $\mathbf{x}$ 、 $\mathbf{y}$ を作ったら、必ず共通文字が（最低 2 つ）含まれる。1 が $\mathbf{x}$ 、 $\mathbf{y}$ に共通だとしよう。 $\mathbf{x} = (1 \ a \ b)$ と書き、 $\mathbf{x}$ と異なる置換 $\mathbf{y}$ を列挙すれば、(1 b a)、(1 a c)、(1 c a)、(1 b c)、(1 c b) がすべてだが、 $\mathbf{x}$ と本質的に異なる形は、 $\mathbf{y} = (1 \ b \ a)$ 、(1 a c)、(1 c b) の 3 つと言える。

問題 $\mathbf{x} = (1 \ a \ b)$ と、 $\mathbf{y} = (1 \ b \ a)$ 、(1 a c)、(1 c b) から、 $\mathbf{xyx}^{-1}\mathbf{y}^{-1}$ を計算せよ

答 4 文字列を任意に 1, a, b, c と書き、これに上記 3 種の $\mathbf{xyx}^{-1}\mathbf{y}^{-1}$ を作用させた文字列と見比べると、 $\mathbf{xyx}^{-1}\mathbf{y}^{-1}$ は順に e、(1 a) (b c)、e と分かる。すなわち（任意の偶置換でなく）共通文字のない互換の積、または e しか作れない。

問題 4 文字から作った、 $\mathbf{xyx}^{-1}\mathbf{y}^{-1}$ のすべての形を列挙せよ

答 前問の 1 を他の数に替えれば、e、(1 a) (b c)、(2 a') (b' c')、(3 a'') (b'' c'')、可換性を考慮して整理すると、e、(1 2) (3 4)、(1 3) (2 4)、(1 4) (2 3)、となる。

すなわち、 A_4 の正規部分群、 $N = \{xyx^{-1}y^{-1}\}$ は、

$N = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ 、47 頁で群 H' と書いたものである。

元どうしの積、 $(1\ 2)(3\ 4)(1\ 3)(2\ 4) = (1\ 4)(2\ 3)$ なども分かる。

実際、 $A_4 = \{N, N(2\ 3\ 4), N(2\ 3\ 4)^2\}$ は剰余類の巡回群になるのだった (47 頁)。

～結び～

「ガロア群が可解群であることが、代数方程式が解ける必要十分条件」と言えば、木で鼻をくくったような言い方だが、根の式の対称性を表現する群を分割していく理論が納得できたと思う。解法理論の別の一面として (群の分割と逆方向に)、根を実際に計算する方法を考えるのが“原著の論旨”だった。

根を計算するには、1 の p 乗根が計算できる (ガウスが証明した) ことが前提となる。現代ガロア理論では、この前提も含めて証明されるが、ガロア第一論文の範囲外であり (8 頁)、現代理論書の難解な部分でもあるので (記述は短いのだが)、本書で省いた。一方、原著の内容は (現代書が殆ど触れない下記のこと) 本書に網羅した。

5 章だけ読んだ人へ：4 章では、ガロアの解法計算、素数 n 次方程式が解けるかどうかを係数値から知る $(n-2)!$ 次の判定式 (97 頁)、および 1 の p 乗根の、解法計算における重要な役割を示した。「130 頁の連立方程式を解けば、 θ_k を、より高対称な関数 Θ_j の巾開方で書ける」のだが、 p が非素数だと「次に Θ_j を、より高対称な関数の巾開方で書くのが不可能」になる (82 頁、95 頁)。これは、2 章 30 頁の初等数学でも予想できた。5 次以上の方程式で解公式が書けない理由は、様々に説明できる。

古典論 4 章も読んだ人へ：解ける素数次方程式 (4 章 §5) では、全根が $V_i = A\alpha_j + B\alpha_k$ の有理式で表せることを長々と証明したが (§6)、現代論では、「ガロア拡大体が Q の $n(n-1)$ 次拡大なら、 $Q(V_i) = Q(A\alpha_j + B\alpha_k)$ 」 (112 頁)、と遙かに簡潔に分かる。

高校数学のみの予備知識で、 n 根の対称性と群論を飛躍なしに了解し、解法理論に達するには、1～3 章→5 章 (現代論) よりも、1～3 章→4 章 (古典論) が分かり易く、思考の歴史にも沿うと思うが、初等用語で延々と文字計算するのと、沢山の新概念を用意してから簡潔に言うのと、どちらが理解し易いかは人によって違うかもしれない。

モーツァルトの音楽は、いつの時代に聴いても新鮮だが、現代の作曲家が同じ古典スタイルで創作したら意味がない…、ユークリッドの古典も同じだ、と或る数学者が書いている。本書の内容は、創作でなく鑑賞だから、無意味と言われたい願う。読者に美しい旋律がきこえたなら、幸いである。

<付録> 3次方程式の解公式から、2次方程式の解公式が出る計算過程

24頁の計算の続き；

$x^3 + ax^2 + bx + c = 0$ の3根 α, β, γ を、係数 a, b, c の式（解公式）で書く。

我々は、下記の θ, θ' を定義した (ω は1 の原始3乗根)

$$\alpha + \beta + \gamma = -a, \quad \alpha + \omega\beta + \omega^2\gamma = \theta, \quad \alpha + \omega^2\beta + \omega\gamma = \theta'$$

適宜 1、 ω, ω^2 を掛けて、3 式の両辺の和をとると ($\omega^2 + \omega + 1 = 0$ より)、

$$3\alpha = -a + \theta + \theta', \quad 3\beta = -a + \omega^2\theta + \omega\theta', \quad 3\gamma = -a + \omega\theta + \omega^2\theta' \quad \cdots \star$$

すなわち、 θ, θ' を得れば根の値を得る。

$$\theta^3 = (\alpha + \omega\beta + \omega^2\gamma)^3 = \alpha^3 + \beta^3 + \gamma^3 + 6\alpha\beta\gamma + 3\omega(\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha) + 3\omega^2(\alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2)$$

$$\theta'^3 = (\alpha + \omega^2\beta + \omega\gamma)^3 = \alpha^3 + \beta^3 + \gamma^3 + 6\alpha\beta\gamma + 3\omega(\alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2) + 3\omega^2(\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha)$$

上の非対称関数を ϕ, ϕ' と書き、 $\phi + \phi' = -ab + 3c$ 、 $\phi\phi' = b^3 - 6abc + a^3c + 9c^2$

より、 $X^2 + (ab - 3c)X + b^3 - 6abc + a^3c + 9c^2 = 0$ を解いて、

$$\phi, \phi' = \{(-ab + 3c) \pm \sqrt{(a^2b^2 + 18abc - 27c^2 - 4b^3 - 4a^3c)}\}/2 \quad \text{を得る。}$$

$$\alpha^3 + \beta^3 + \gamma^3 + 6\alpha\beta\gamma = (\alpha + \beta + \gamma)^3 - 3(\alpha + \beta + \gamma)(\alpha\beta + \beta\gamma + \gamma\alpha) + 9\alpha\beta\gamma = -a^3 + 3ab - 9c$$

以上の値、および $\omega, \omega^2 = (-1 \pm \sqrt{3}i)/2$ を、 θ^3, θ'^3 に代入し

$$\theta^3 = -a^3 + 9ab/2 - 27c/2 + \{3\sqrt{3}i \times \sqrt{(a^2b^2 + 18abc - 27c^2 - 4b^3 - 4a^3c)}\}/2 \quad \cdots \star$$

$$\theta'^3 = -a^3 + 9ab/2 - 27c/2 - \{3\sqrt{3}i \times \sqrt{(a^2b^2 + 18abc - 27c^2 - 4b^3 - 4a^3c)}\}/2 \quad \cdots \star$$

★ で、 $\theta = \sqrt[3]{\theta^3}$ 、 $\theta' = \sqrt[3]{\theta'^3}$ と書けば (25 頁)、3 次方程式の解公式になる。

($\sqrt{3}i = 2\omega + 1$ 、 $-\sqrt{3}i = 2\omega^2 + 1$ と書いておいてもよい)

☆ は、 a, b, c に付加情報（数値か特定の関係式）があるときのみ、簡単化しうる。

例えば ☆ で $c = 0$ とすれば、 $\theta^3, \theta'^3 = -a^3 + 9ab/2 \pm \{3\sqrt{3}ib\sqrt{(a^2 - 4b)}\}/2 \quad \cdots *$

$\sqrt{(a^2 - 4b)} = P$ とおき、これを変形した $b = (a^2 - P^2)/4$ も使い、* を書き直すと

$$\theta^3 = -a^3 + 9a(a^2 - P^2)/8 + 3\sqrt{3}i(a^2 - P^2)P/8$$

$$= a^3/8 - 9aP^2/8 + 3\sqrt{3}ia^2P/8 - 3\sqrt{3}iP^3/8$$

$$= (a/2 + \sqrt{3}iP/2)^3 = \{a/2 + \sqrt{3}i\sqrt{(a^2 - 4b)}/2\}^3 \quad \cdots \#$$

そこで、 $\theta, \theta' = \{a \pm \sqrt{3}i\sqrt{(a^2 - 4b)}\}/2$ と書ける (25 頁の記法)。★ に代入し、

$$\alpha = 0, \quad \beta = -a/2 + \sqrt{(a^2 - 4b)}/2, \quad \gamma = -a/2 - \sqrt{(a^2 - 4b)}/2$$

すなわち、 $x(x^2 + ax + b) = 0$ の解公式になった。

例として、 $x(x^2 + 3x + 2) = 0$ の係数、 $a = 3$ 、 $b = 2$ を

$$\# \text{ に代入すれば、} \theta, \theta' = (3 \pm \sqrt{3}i)/2 \text{ より、} \alpha = 0, \beta = -1, \gamma = -2$$

$$* \text{ に代入すれば、} \theta^3 = 3\sqrt{3}i, \theta'^3 = -3\sqrt{3}i, \theta = -\sqrt{3}i, \theta' = \sqrt{3}i \text{ より、}$$

$$\alpha = -1, \beta = -2, \gamma = 0 \text{ だが、} \theta = -\sqrt{3}i \text{ を、} \theta^3 = \theta^3\omega^3 = \{-\sqrt{3}i \times (-1 + \sqrt{3}i)/2\}^3$$

$$= \{(3 + \sqrt{3}i)/2\}^3 \text{ と書いてみれば、} \# \text{ を用いて計算したのと同じになる。}$$

$\sqrt[3]{\theta^3}$ を θ で書くときの ω 倍、 ω^2 倍の任意性は、根の巡回置換に相当する (25 頁)。

～あとがき、家族（しげり、隆広、雅広）への謝辞～

通勤電車の中で数年、ときどき考えては中断し、ある時期続けて模索し、4年程前、ガロアが省略した証明を19世紀初頭の言葉だけで自然に言えると分かったので、子供達（大学院、高3当時）に説明したくて鉛筆書き原稿を作った。夕食後の食卓を紙束と消しゴム屑で一杯にしていた頃、何に夢中なのか家内に訊かれて示唆を得た（そういう本、色々あるでしょ、うちにも）。これは違う、と答えたとき数学専攻でない人達のための数学に意義を感じた。長男と次男からは本質的な助言を得た。証明の不備、証明前の予告説明は不要、章立て無しに話が連続した初稿の欠点、など様々な指摘で（自分で言うのも何だが）見違える改訂稿になり、他人に読解可能になったと思う。理工系の方々、受験数学に飽き足らない高校生、その生徒達の指導教官に関心をもっていただけのことを切に願っている。