ML3 Mathematics, of the Learner, for the Learner, by the Learner.

代数方程式について

A Note on Algebraic Equations. (Excerpt Ver. 20121021)

YAMASHITA, Koichiro (kymst)
Sun Oct 14 15:34:37 2012 JST

This document is MLˆ3docu No.20121021algEq.
Key word: Algebra, Algebraic Equations, Substitution Group,
Cubic and Quartic Equations, Lagrange.

Downloadable from FMFk page url: http://kymst.net.
mail to: kymstkymst@gmail.com
We hope your math exciting, your hack happy,
and whole lotta love. :-)

Contents

Chapter 1

Cubic Equations

§ 1-1. Excerpt from Pamphlet.

オナジミの 2 次方程式について考えてみよう．

$$x^2 - px + q = 0$$

の根を α, β とすると，基本対称式

$$\alpha + \beta = p, \quad \alpha\beta = q$$

が得られる．演算 ♡ を「ウマクハズス」ことと定義すると，根 α, β は

$$\alpha,\, \beta = \frac{1}{2}\left\{(\alpha+\beta)\heartsuit\sqrt{(\alpha-\beta)^2}\right\}$$

で与えられる．ウマクハズして得られる $\alpha - \beta$ と $-(\alpha - \beta)$ は対称性を破っている．これが，根号の前にある複号の意味である．対称性破りは，まさにべき根が現われるその時点で実行されるのである．

3 次方程式を考えよう．最初から

$$x^3 - \sigma_1 x^2 + \sigma_2 x - \sigma_3 = 0$$

として，3 個の根を α, β, γ とすれば，根の基本対称式

$$\sigma_1 = \alpha + \beta + \gamma,\ \sigma_2 = \alpha\beta + \beta\gamma + \gamma\alpha,\ \sigma_3 = \alpha\beta\gamma$$

を得る．ここで

$$\varphi = \alpha + \omega\beta + \omega^2\gamma, \quad \psi = \alpha + \omega^2\beta + \omega\gamma$$

として，♡ と ♠ で，「ソロッテウマクハズス」演算を表わすと

$$\alpha,\, \beta,\, \gamma = \frac{1}{3}\left(\sigma_1\heartsuit\sqrt[3]{\varphi^3}\spadesuit\sqrt[3]{\psi^3}\right)$$

が成り立つ．何故なら

$$\left(\sqrt[3]{\varphi^3},\ \sqrt[3]{\psi^3}\right) = (\varphi,\, \psi)\,,\ \left(\omega^2\varphi,\, \omega\psi\right)\ \left(\omega\varphi,\, \omega^2\psi\right),$$

としてウマクハズせば，順に α, β, γ が得られるからである．

ここまで読み進んでくれた貴君，貴女に感謝する．貴君と貴女は，既に 3 次方程式の代数的解法の algorithm を手にする直前にいる．と言うのも，φ^3 と ψ^3 を基本対称式 $\sigma_1, \sigma_2, \sigma_3$ で，つまりは方程式の係数で表わして，立方根をウマクハズせば. . . . . デキアガリ!

1.1.1 Guide Quiz and What To Do

φ, ψ, σ_1, σ_2, σ_3 は上で定義された通りだとします.

Quiz 1. 積 $\varphi\psi$ が $\sigma_1^2 - 3\sigma_2$ と表わされることを確かめて下さい．従って，

$$a^3 + b^3 + c^3 - 3abc = (a+b+c)(a^2+b^2+c^2-ab-bc-ca)$$

という因数分解の公式がドシガタク中途半端で，何如にフヤケタものであるか，嫌諦凶禍書への怒りを新たにして下さい．

Quiz 2. $\varphi^3 + \psi^3$ が $2\sigma_1^3 - 9\sigma_1\sigma_2 + 27\sigma_3$ と表わされることを確かめて下さい．

Quiz 3. 1. と 2. から，φ^3 と ψ^3 の値を求めて下さい．

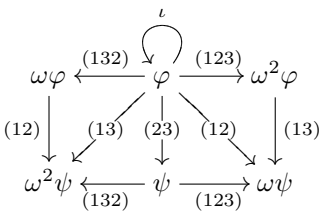
Quiz 4. ヘタナテッポウを撃たずに，方程式 $x^3 - 3x^2 + 4x - 2 = 0$ を解いて下さい．

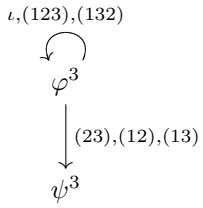
§ 1-2. 3 次方程式の還元

$\sigma_1 = \alpha+\beta+\gamma$, $\sigma_2 = \alpha\beta+\beta\gamma+\gamma\alpha$, $\sigma_3 = \alpha\beta\gamma$ とする．

$\varphi = \alpha + \omega\beta + \omega^2\gamma$, $\psi = \alpha + \omega^2\beta + \omega\gamma$ について次が成り立つ：

$$\begin{array}{llll}
\varphi|(12) & = \beta + \omega\alpha + \omega^2\gamma & = \omega(\alpha + \omega^2\beta + \omega\gamma) & = \omega\psi, \\
\varphi|(13) & = \gamma + \omega\beta + \omega^2\alpha & = \omega^2(\alpha + \omega^2\beta + \omega\gamma) & = \omega^2\psi, \\
\varphi|(23) & = \alpha + \omega\gamma + \omega^2\beta & = \alpha + \omega^2\beta + \omega\gamma & = \psi, \\
\varphi|(123) & = \beta + \omega\gamma + \omega^2\alpha & = \omega^2(\alpha + \omega\beta + \omega^2\gamma) & = \omega^2\varphi, \\
\varphi|(132) & = \gamma + \omega\alpha + \omega^2\beta & = \omega(\alpha + \omega\beta + \omega^2\gamma) & = \omega\varphi.
\end{array}$$





Chapter 2

対称式とその基本定理

§ 2-1. 対称式

n 個の文字 (不定元)$X_1, X_2, \ldots, X_n$ についての有理式 $f(X_1, X_2, \ldots, X_n)$ が**対称式** [▷1] であるとは，任意の置換 $\mathsf{s} \in S_n$ を f に施すとき f が不変に保たれることである:

[▷1] *symmetric formula*

$$f : \text{symmetric on } X_1, X_2, \ldots, X_n \overset{\text{def}}{\iff} \forall \mathsf{s} \in S_n : f \circlearrowleft \mathsf{s} \ (\iff \forall \mathsf{s} : f \equiv f|\mathsf{s}.)$$

有理式 (rational expression) は多項式 (polynomial) の商として表されるから，ここでは多項式のみを考える．つまり，以下で対称式とは**対称な多項式**を意味する．

n 次の方程式

$$f(x) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - \ldots + (-1)^n \sigma_n = 0$$

が根として $x = X_1, X_2, \ldots, X_n$ をもつならば，$f(x)$ は

$$f(x) \equiv (x - X_1)(x - X_2) \ldots (x - X_n)$$

と分解される．これにより，係数を比較して

$$\begin{aligned}
\textstyle\sum X_1 = X_1 + X_2 + \cdots + X_n &= \sigma_1, \\
\textstyle\sum X_1 X_2 = X_1 X_2 + X_1 X_3 + \ldots + X_{n-1} X_n &= \sigma_2, \\
\ldots &\ldots \\
\textstyle\sum \prod_{j=1}^{k} X_j = \sum X_1 X_2 \ldots X_k &= \sigma_k, \qquad (2.1) \\
\ldots &\ldots \\
\textstyle\prod_{j=1}^{n} X_j = X_1 X_2 \ldots X_n &= \sigma_n
\end{aligned}$$

を得る．

これらは $X_1, X_2, \ldots, X_n$ の**基本対称式** [▷2] と呼ばれる．

[▷2] *fundamental symm. f.*

$X_1, X_2, \ldots, X_n$ の対称式について帰納法を用いるために，それらについての全順序を定義する．そのために，対称式の**型** [▷3] という概念を定義しよう．ある対称式が項 $T = X_1^{e_1} X_2^{e_2} \ldots X_n^{e_n}$ という項を含んでいるならば，列 $[12 \ldots n]$ に置換 s を施して得られる列 $[s_1 s_2 \ldots s_n]$ を subindex にもち，指数が T と同じであるような項 $T_1 = T|\mathsf{s} = X_{s_1}^{e_1} X_{s_2}^{e_2} \ldots X_{s_n}^{e_n}$ も含んでいるはずである．このようなとき，2 つの項 T と T_1 は**同型の項** [▷4] と呼ばれる．従って，同型の項すべてからなる集合に項の型 type を指定するとは，指数 $e_1, e_2, \ldots, e_n$ の並びを決めることである．これは $(n]$ から自然数 $\mathbb{N}$ の中への写像を定めることに他ならない．

[▷3] *type*

[▷4] *isotype term*

特にこの写像 τ を**単調減少** [▷5](つまり**単調非増加** [▷6]) にすることができる:

[▷5] *monotonically decrease*

$$\forall k_1, k_2 \in (n] : k_1 < k_2 \Rightarrow \tau(k_1) \geq \tau(k_2).$$

[▷6] *mon.non increase*

つまり，同型の項の集合の中から，特に $e_1 \geq e_2 \geq \ldots \geq e_n$ をみたすような項 $T = X_1^{e_1} X_2^{e_2} \ldots X_n^{e_n}$ を選んで代表させよう，という訳である．こうすることによっ

て，同型項は自然数からなる長さ n の単調減少列 $[e_1e_2\dots e_n]$ によって encode される[2.1]．以下，この表記で項の type を表わし，この type の項すべてからなる対称式を表わしたいときには $[e_1e_2\dots e_n]_X$ と表わす．

これにより，基本対称式 $\sigma_1, \sigma_2, \dots, \sigma_n$ は

$$\sigma_1 = [10\dots0]_X,\quad \sigma_2 = [110\dots0]_X,\ \dots,\ \sigma_k = [\underbrace{1\dots1}_{k\text{bits}}0\dots0]_X,\dots,\ \sigma_n = [11\dots1]_X$$

と書ける．これ以外の対称式もこの記法で特定することができる．例を挙げてみれば

$$\sum X_1^3X_2^2X_3 = [3210\dots0]_X,\quad \sum X_1^2X_2^2X_3^2 = [2220\dots0]_X$$

などである．

項の type に全順序を定義する．**辞書式順序** [▷1] である．n 文字の対称式 f と g について，それらが同型の項のみからなるとする (このようなとき，対称式は**単型対称式** [▷2] であると言われる)．それぞれの type が $\tau_f = [f_1f_2\dots f_n]$ と $\tau_g = [g_1g_2\dots g_n]$ であったとする．f が g よりも**高位である** [▷3]，または g が f よりも**低位である** [▷4] とは次が成り立つことである：

- $f_1 > g_1$,
- $f_1 = g_1$ ならば $f_2 > g_2$,
- $f_1 = g_1,\ f_2 = g_2$ ならば $f_3 > g_3$,

  ……
- $f_1 = g_1,\ f_2 = g_2,\ \dots,\ f_{n-1} = g_{n-1}$ ならば $f_n > g_n$.

f が g よりも高位であるとき，$f \succ g$ または $g \prec f$ と書く．

低位の順にいくつか書きだせば

- $[00\dots0]$ でこれは定数,
- 次が $[10\dots0], [110\dots0], \dots, [11\dots1]$ で，これらは基本対称式 $\sigma_1, \sigma_2, \dots, \sigma_n$,
- 次が $[20\dots0]$ で $\sum X_1^2$，$[210\dots0]$ で $\sum X_1^2X_2, \dots$

などである．

[▷1] *lexicographic order*

[▷2] *monotype symm.f.*

[▷3] *higher order*

[▷4] *lower order*

§2-2. 基本定理とその証明

対称式の基本定理 [▷5](**FTSF**) とは次の定理である：

[▷5] *Fundamental Theorem of Symm. F.*

THEOREM 2.2.1 (対称式の基本定理)

n 個の不定元についての対称式 $f(X_1, X_2, \dots, X_n)$ について次が成り立つ：

1°. f は基本対称式 $\sigma_1, \sigma_2, \dots, \sigma_n$ の整式 $g(\sigma_1, \sigma_2, \dots, \sigma_n)$ で表わすことができて，その表わし方は一意的である．

2°. g の $\sigma_1, \sigma_2, \dots, \sigma_n$ についての次数は，f における 1 つの不定元についての最大次数である．

3°. f が $X_1, X_2, \dots, X_n$ について同次式ならば，g は $\sigma_1, \sigma_2, \dots, \sigma_n$ について斉重であり，その重さは f の次数に等しい．

ここで，subindex をもつ不定元の項の**重さ** [▷6] とは，その subindex の，次数まで含めた意味での総和のことである．例えば項 $a_1^3a_2^2a_3^2$ の重さは $1\cdot3+2\cdot2+3\cdot2=13$ である．ある多項式の項の重さがすべて等しいとき，その多項式は**斉重** [▷7] である，と言

[▷6] *weight*

[▷7] *isobaric*

[2.1] コレバッカリ!! (最近，メチャハマッテイル)

われる.

Proof. 対称式はいくつかの単型対称式の線型結合として書けるから，単型の場合を証明すれば十分である．その type についての高低が定義されていて，また基本対称式については成り立っているから，帰納法が使える.

$\tau_f = [e_1e_2\dots e_n]$ として，$f = [e_1e_2\dots e_n]_X = \sum X_1^{e_1}X_2^{e_2}\dots X_n^{e_n}$ とし，f よりも低位の対称式については，定理の成立を仮定する．以下，f を表わす $\sigma_1, \sigma_2, \dots, \sigma_n$ の多項式 $g(\sigma_1, \sigma_2, \dots, \sigma_n)$ を構成する.

いま,

$$\begin{aligned}&\sigma_1^{k_1}\sigma_2^{k_2}\dots\sigma_n^{k_1}\\ &\quad= (X_1+X_2+\dots+X_n)^{k_1}(X_1X_2+\dots+X_{n-1}X_n)^{k_2}\dots(X_1X_2\dots X_n)^{k_n}\\ &\quad= [100\dots0]_X^{k_1}\cdot[110\dots0]_X^{k_2}\cdot\dots\cdot[11\dots1]_X^{k_n}\end{aligned}$$

を展開して最高位項をとれば，その type は

$$[k_1+k_2+\dots+k_n,\ k_2+k_3+\dots+k_n,\ \dots, k_n]$$

となる．これを f の type $[e_1e_2\dots e_n]$ と一致させる：

$$\begin{cases} k_1+k_2+\dots+k_n &= e_1,\\ \quad k_2+\dots+k_n &= e_2,\\ \qquad\dots & \\ \qquad k_n &= e_n \end{cases} \iff \begin{cases} k_1 &= e_1-e_2,\\ k_2 &= e_2-e_3,\\ &\dots\\ k_n &= e_n \end{cases} \tag{2.2}$$

が必要かつ十分である．列 $[e_1e_2\dots e_n]$ の単調減少性により $i\in(n]$ について $k_i\in\mathbb{N}$, つまりいずれも非負である.

このように $k_1, k_2, \dots, k_n$ を定めて $\sigma_1^{k_1}\sigma_2^{k_2}\dots\sigma_n^{k}$ を作れば，その最高位の単型対称式が得られるから，

$$f = \sigma_1^{k_1}\sigma_2^{k_2}\dots\sigma_n^{k} + f_1$$

とすれば，f_1 は f よりも低位の対称式である．帰納法の仮定より

$$f_1 = g_1(\sigma_1, \sigma_2, \dots, \sigma_n)$$

をみたす多項式 g_1 が存在する．よって

$$g(\sigma_1, \sigma_2, \dots, \sigma_n) = \sigma_1^{k_1}\sigma_2^{k_2}\dots\sigma_n^{k_n} + g_1(\sigma_1, \sigma_2, \dots, \sigma_n) \tag{2.3}$$

とすれば

$$f \equiv g(\sigma_1, \sigma_2, \dots, \sigma_n)$$

となり，f が $\sigma_1, \sigma_2, \dots, \sigma_n$ の多項式で表わされた.

一意性について．対称式 f が $\sigma_1, \sigma_2, \dots, \sigma_n$ の多項式として 2 通りに表されたとし，それを

$$f = g(\sigma_1, \sigma_2, \dots, \sigma_n),\quad f = \overline{g}(\sigma_1, \sigma_2, \dots, \sigma_n)$$

とする．このとき，$g-\overline{g} = h$ とすると，h は $\sigma_1, \sigma_2, \dots, \sigma_n$ に関する多項式としては zero 多項式ではないが，$X_1, X_2, \dots, X_n$ で表せば 0 になることになる．これが矛盾であることを示す.

$h = h(\sigma_1, \sigma_2, \dots, \sigma_n)$ が zero 多項式ではないとすると，$\sigma_1, \sigma_2, \dots, \sigma_n$ に値を与えて, h の値が 0 でないようにすることができる．それを $\sigma_1 = S_1, \sigma_2 = S_2, \dots, \sigma_n = S_n$ とする．この $S_1, S_2, \dots, S_n$ から方程式

$$x^n - S_1x^{n-1} + S_2x^{n-2} + \dots + (-1)^nS_n = 0$$

を作り，その根を $\alpha_1, \alpha_2, \ldots, \alpha_n$ とする．h を $X_1, X_2, \ldots, X_n$ で表わしたとき $H(X_1, X_2, \ldots, X_n)$ になるとすれば，このとき，h と H の定義から

$$0 \neq h(S_1, S_2, \ldots, S_n) = H(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

となるが，H は恒等的に 0，つまり zero 多項式であるから，これは矛盾．

2° について．$f = [e_1 e_2 \ldots e_n]_X$ の最大指数は e_1 であり，また $\sigma_1^{k_1}\sigma_2^{k_2}\ldots\sigma_n^{k_n}$ の総次数は $k_1 + k_2 + \ldots + k_n$ である．等式 (2.2) の最初の条件よりこれらは一致する．式 (2.3) において，g_1 は g よりも低位の単型対称式の和であるから，e_1 よりも大きい指数を含むことはない．帰納法の仮定より g_1 の総次数は e_1 以下であり，かつ $\sigma_1^{k_1}\sigma_2^{k_2}\ldots\sigma_n^{k_n}$ は g_1 に含まれることはない．よって g の $\sigma_1, \sigma_2, \ldots, \sigma_n$ についての総次数は，ちょうど e_1 である．

3° について．$\sigma_1^{k_1}\sigma_2^{k_2}\ldots\sigma_n^{k_n}$ の重みは $\sum jk_j = k_1 + 2k_2 + \ldots + nk_n$ であるが，(2.2) によってこれは $\sum e_j = e_1 + e_2 + \ldots + e_n$ に等しい．g_1 は $X_1, X_2, \ldots, X_n$ については g と同次の同次式であり，帰納法の仮定によりその項の重みは $\sum e_j$ であるから，g は斉重で，その重みは f の次数である．

以上ですべて証明された．■

Chapter 3

群の有理式への作用

§3-1. 有理式が帰属する群

THEOREM 3.1.1 (Fundamental Theorem (D21))

対称群 S_n の要素で，有理式 $\varphi(X_1, X_2, \ldots, X_n)$ を不変に保つものの全体は S_n の部分群をなす．この群を $[\varphi]$ で表わし，φ が帰属する群と呼ぶ．

Proof. $\mathsf{s} \in S_n$ について，s を φ に作用させることを $\varphi|\mathsf{s}$ と表わす．$\mathsf{a}, \mathsf{b} \in S_n$ について，a, b が φ を不変に保つならば，$\mathsf{a}, \mathsf{b} \in [\varphi]$ であり，

$$\varphi|\mathsf{a} = \varphi, \quad \varphi|\mathsf{b} = \varphi$$

である．このとき，置換の積 ab について

$$\varphi|\mathsf{ab} = (\varphi|\mathsf{a})|\mathsf{b} = \varphi|\mathsf{b} = \varphi$$

であるから $\mathsf{ab} \in [\varphi]$ である．

$[\varphi]$ は恒等置換 $\boldsymbol{\iota}$ を含む．また，逆置換 a を含むことは

$$\varphi = \varphi|\boldsymbol{\iota} = \varphi|\mathsf{a}\mathsf{a}^{-1} = (\varphi|\mathsf{a})|\mathsf{a}^{-1} = \varphi|\mathsf{a}^{-1}$$

より従う．■

THEOREM 3.1.2 (群に帰属する有理式の存在 (D25))

n 次の置換群 G が任意に与えられたとき，G に帰属する有理式が存在する．

Proof. 実際にこの有理式を構成する．与えられた群を $G = \{\boldsymbol{\iota}(= \mathsf{s}_1), \mathsf{s}_2, \ldots, \mathsf{s}_k\}$ とする．$m_1, m_2, \ldots, m_n$ をすべて異なるとして

$$V = m_1X_1 + m_2X_2 + \ldots + m_nX_n$$

を作れば，V は $n!$ 価である．

この V に G の置換を作用させて，次の list (L),

$$(\mathrm{L}): \quad V = V|\boldsymbol{\iota},\ V|\mathsf{s}_2,\ V|\mathsf{s}_3,\ \ldots,\ V|\mathsf{s}_k$$

を考える．

- まず (L) の要素はすべて異なる．なぜなら

  $$V|\mathsf{a} = V|\mathsf{b} \Rightarrow V = V|\mathsf{b}\mathsf{a}^{-1} \Rightarrow \mathsf{b}\mathsf{a}^{-1} = \boldsymbol{\iota} \Rightarrow \mathsf{b} = \mathsf{a}$$

  が成り立つから．

- 任意の $\mathsf{s} \in G$ を (L) のそれぞれに作用させて，次の (L_1) を作る：

$$(\mathrm{L}_1): \quad V|\mathsf{s},\ V|\mathsf{s}_2\mathsf{s},\ V|\mathsf{s}_3\mathsf{s},\ \ldots,\ V|\mathsf{s}_k\mathsf{s}.$$

この (L_1) は (L) の並べ替えである．

そこで，適当な不定元 Y をとり

$$\varphi = (Y - V)(Y - V|\mathsf{s}_2)(Y - V|\mathsf{s}_3)\ldots(Y - V|\mathsf{s}_k)$$

を作れば，φ は G の任意の置換によって不変に保たれる．しかし，G に含まれない任意の置換 $\mathsf{t} \in S_n$ を作用させるとき，

$$\varphi|\mathsf{t} = (Y - V|\mathsf{t})(Y - V|\mathsf{s}_2\mathsf{t})(Y - V|\mathsf{s}_3\mathsf{t})\ldots(Y - V|\mathsf{s}_k\mathsf{t})$$

を得るが，$V|\mathsf{t}$ は list (L) のいずれとも異なるから，V は変異する．■

§ 3-2. 部分群と指数

THEOREM 3.2.1 (部分群の位数 (D26))

部分群の位数はもとの群の位数の約数である．

Proof. G を群，H をその部分群とする (これを今後 $H \triangleleft G$，または $G \triangleright H$ と書く)．また G の位数を N，H の位数を p とする (これもそれぞれ $\mathrm{Ord}(G) = N$，$\mathrm{Ord}(H) = p$ と書く)．示すべきことは $p \,\big|\, N$ である．

H が次の list (H) であるとする：

$$(\mathrm{H}): \quad \boldsymbol{\iota}(=\mathsf{h}_1),\ \mathsf{h}_2,\ \mathsf{h}_3,\ \ldots,\ \mathsf{h}_p.$$

もし $H = G$ であれば証明すべきことはない．H に含まれない G の置換 g_2 があるとする．H の要素との積からなる list (H_2) を作る：

$$(\mathrm{H}_2): \quad \mathsf{g}_2,\ \mathsf{h}_2\mathsf{g}_2,\ \mathsf{h}_3\mathsf{g}_2,\ \ldots,\ \mathsf{h}_p\mathsf{g}_2.$$

$H \triangleleft G$ であるから，(H_2) は G に含まれる．まず，$\mathsf{h}_i\mathsf{g}_2 = \mathsf{h}_j\mathsf{g}_2 \Rightarrow \mathsf{h}_i = \mathsf{h}_j$ であるから，(H_2) は同じ置換を含まない．また，(H_2) の置換は (H) の置換とはすべて異なる．なぜならば，もしある j について $\mathsf{h}_i\mathsf{g}_2 = \mathsf{h}_j$ であるとすれば，$\mathsf{g}_2 = {\mathsf{h}_i}^{-1}\mathsf{h}_j \in H$ となり，仮定に反する．よって G は (H) と (H_2) とを合わせて $2p$ 個の置換を含む．これで群 G が尽されていれば，(H_2) の置換の集合を $H\mathsf{g}_2$ として $G = H \uplus H\mathsf{g}_2$ であり，H と $H\mathsf{g}_2$ は対等であるから，$N = 2p$ となり，示すべき命題が成り立つ．

もし G が $H \uplus H\mathsf{h}_2$ 以外の置換 g_3 を含んでいるとする．このとき，H の置換との積からなる list (H_3) を作る：

$$(\mathrm{H}_3): \quad \mathsf{g}_3,\ \mathsf{h}_2\mathsf{g}_3,\ \mathsf{h}_3\mathsf{g}_3,\ \ldots,\ \mathsf{h}_p\mathsf{g}_3.$$

このとき，先ほどと同様にして，(H_3) の置換はすべて異なり，かつ (H) と (H_3) には共通な置換は存在しない．更に，(H_3) の置換は (H_2) のいずれとも異なる．なぜならば，もしある $j \in (p]$ について $\mathsf{h}_i\mathsf{g}_3 = \mathsf{h}_j\mathsf{g}_2$ が成り立つとすれば，$\mathsf{g}_3 = {\mathsf{h}_i}^{-1}\mathsf{h}_j\mathsf{g}_2 = \mathsf{h}_k\mathsf{g}_2\ (\exists k)$ となり，$\mathsf{g}_3 \in H\mathsf{g}_2$ となるが，これは g_3 のとり方に矛盾する．従って，G は $3p$ 個の置換を含む．list (H_3) の置換の集合を $H\mathsf{g}_3$ で表わす．もし G が $H \uplus H\mathsf{g}_2 \uplus H\mathsf{g}_3$ で尽されていれば，$N = 3p$ となり，定理が成り立つ．

G がこれら以外の置換を含んでいるとしよう．G の位数 N は有限であるから，この操作は有限回で終了する．つまり $\nu \in \mathbb{Z}^+$ として，次の list (H_ν) を作るとする：

$$(\mathrm{H}_\nu): \quad \mathsf{g}_\nu,\ \mathsf{h}_2\mathsf{g}_\nu,\ \mathsf{h}_3\mathsf{g}_\nu,\ \ldots,\ \mathsf{h}_p\mathsf{g}_\nu.$$

これらの置換がそれぞれ互いに異なり，また H, $H\mathsf{g}_2$, …, $H\mathsf{g}_{\nu-1}$ に含まれる置換のいずれとも異なることの証明は先ほどと同じである．list (H_ν) の置換の集合を $H\mathsf{g}_\nu$ と表わそう．(H_ν) で G が尽されたとすれば

$$G = H \uplus H\mathsf{g}_2 \uplus \ldots \uplus H\mathsf{g}_\nu = \biguplus_{k\in(\nu]} H\mathsf{g}_k$$

であり，かつ

$$H \simeq H\mathsf{g}_2 \simeq \ldots \simeq H\mathsf{g}_\nu$$

であるから，$N = \nu p$ が成り立つ．

この $\nu = \dfrac{N}{p} = \dfrac{\mathrm{Ord}(G)}{\mathrm{Ord}(H)}$ を群 G における部分群 H の**指数** [▷1] と言い，これを $[G:H] = \nu$ で表わす．

[▷1] *index*

Corollary 3.2.2

n 次の置換群の位数は $n!$ の約数である．

THEOREM 3.2.3 (位数と置換の周期 (D27))

置換群 G について，その位数が N のとき，G に含まれる置換の周期は N の約数である．

Corollary 3.2.4

$\mathrm{Ord}(G) = p$ (p: prime) ならば，G は周期 p をもつ置換 s の巡回群である．

3.2.1 Anachronical Notes No.1

今日では，この Theorem 3.2.4 (p.11) を Lagrange's Theorem と呼ぶことが多いようである．というか，ほとんどの代数学の教科書でそうなっている．

重要な定理であることに疑いはない．少しだけ「現代からの時代錯誤」を犯しておこう．オイシイオマケもついてくる．

まず一般の群について．方程式論では，置換群が中心に据えられて考察が進むが，群そのものは何も置換からなるものだけではない．整数の全体 $\mathbb{Z}$ は加法について群をなすし，正の実数全体 $\mathbb{R}^+$ は乗法について群をなす (これらはいずれも「可換」な群である．置換群は可換群ではなかったことに注意せよ)．

従って，群そのものの定義は極めて「殺伐」としたものになる：

Definition 3.2.5 ((一般の群))

群 [▷2] とは次の公理をみたすような 2 項演算 $(a,b) \to ab$ が定義された集合 G である：

閉包性 [▷3] a と b が G に含まれるならば，ab も G に含まれる．

結合性 [▷4] 任意の a, b, $c \in G$ について $a(bc) = (ab)c$.

単位元 [▷5] ある要素 $1 \in G$ が存在して，G の任意の元 a について $a1 = 1a = a$ が成り立つ．

逆元 [▷6] a が G の要素ならば，G には $aa^{-1} = a^{-1}a = 1$ が成り立つような要素 a^{-1} が存在する．

[▷2] *group*

[▷3] closure

[▷4] associativity

[▷5] identity

[▷6] inverse

Definition 3.2.6 (部分群)

群 G の**部分群** [▷7] とは G の空でない部分集合で，G の 2 項演算の下で群をなすものである．

[▷7] *subgroup*

Definition 3.2.7 (巡回群，位数)

A が群 G の任意の部分集合であるとき，A によって**生成される部分群** [▷1] とは，A を含むような最小の部分群であり，$\langle A\rangle$ と書かれることが多い．形式的には，$\langle A\rangle$ は，A を含むような部分群すべてに渡る共通部分である．

[▷1] *subgroup generated by A*

群 G が**巡回群** [▷2] であるとは，G がただ 1 つの要素から生成されることである：$G = \langle a\rangle$．a によって生成される有限な巡回群は必然的に可換群となり，$a^n = 1$ として $G = \{1, a, a^2, \ldots, a^{n-1}\}$ である．または，加法的記法では $na = 0$ として $\{0, a, 2a, \ldots, (n-1)a\}$ となる．

[▷2] *cyclic group*

群 G において，要素 a の**位数** [▷3] とは，$a^n = 1$ となるような最小の正整数 n のことであり，それは $\left|a\right|$ と表される．そのような正整数が存在しない場合には，a の位数は無限大であるとする． 従って，$\left|a\right| = n$ である場合には，a によって生成される巡回部分群 $\langle a\rangle$ はちょうど n 個の要素からなり，k が n の倍数であるとき，かつそのときに限り，$a^k = 1$ である．

[▷3] *order*

群 G の位数 [▷4] とは G の要素の個数のことである．それは $\left|G\right|$ と書かれる．

[▷4] *order of group*

Lagrange's Theorem は次のように導かれる：

H を G の部分群とする．$g \in G$ について，g によって生成される H の**右剰余類** [▷5] を

[▷5] *right coset*

$$Hg = \left\{hg \,\middle|\, h \in H\right\}$$

によって定義する．同様に，g によって生成される H の**左剰余類** [▷6] とは

[▷6] *left coset*

$$gH = \left\{gh \,\middle|\, h \in H\right\}$$

である．もし $a, b \in G$ ならば，

$$Ha = Hb \iff ab^{-1} \in H,$$

および

$$aH = bH \iff a^{-1}b \in H$$

が成り立つ[3.1]．従って，a, b についてそれらが同値であることを $ab^{-1} \in H$ によって定義すれば，同値関係を得る[3.2]．またこのとき，a の同値類は

$$\left\{b \,\middle|\, ab^{-1} \in H\right\} = Ha$$

となる[3.3]．以上より，**右剰余類は G の類別を与える．左剰余類についても同様**．$h \in H$ について $h \to ha$ は単射であるから，それぞれの剰余類の要素の個数は $\sharp H$ である．右剰余類の個数と左剰余類の個数は等しい．なぜならば，写像 $aH \to Ha^{-1}$ は単射だからである[3.4]．$[G : H]$ で右 (ないしは左) 剰余類の個数を表せば (これは H の G における**指数** [▷7] と呼ばれる)，次の基本的な結果を得る．

[▷7] *index*

以下，G を群として，$\left|G\right|$ は G の位数を表す．

THEOREM 3.2.8 (Lagrange's Theorem)

H を G の部分群とするとき，$\left|G\right| = \left|H\right|[G : H]$ が成り立つ．特に，G が有限群であれば $\left|H\right|$ は $\left|G\right|$ を割り切り，次が成り立つ：

$$\frac{\left|G\right|}{\left|H\right|} = [G : H].$$

[3.1] $Ha = Hb$ とすれば，ある $h \in H$ について $a = 1a = hb$ であるから $ab^{-1} = h \in H$ となる．逆に，$ab^{-1} = h \in H$ とすれば，$Ha = Hhb = Hb$ となる．

[3.2] 反射性は $aa^{-1} = 1 \in H$ により，対称性は ab^{-1} ならば $(ab^{-1})^{-1} = ba^{-1} \in H$ により，また推移性は $ab^{-1} \in H$, $bc^{-1} \in H$ とすれば $(ab^{-1})(bc^{-1}) = ac^{-1} \in H$ により，成り立つ．

[3.3] $ab^{-1} \in H \iff (ab^{-1})^{-1} = ba^{-1} \in H \iff b \in Ha$.

[3.4] $Ha^{-1} = Hb^{-1} \iff a^{-1}(b^{-1})^{-1} = a^{-1}b \in H \iff aH = bH$.

Proof. 剰余類の個数は $[G:H]$ であり，それぞれの要素の個数は $\left|H\right|$ である．■

G を有限群とする．

Corollary 3.2.9

(i) $a \in G$ について，$\left|a\right|$ は $\left|G\right|$ を割り切る．特に $a^{|G|} = 1$ である．従って，$\left|G\right|$ は G の要素それぞれの位数の倍数であるから，G の**指数** [▷1] を $\{\left|a\right| : a \in G\}$ の最小公倍数と定めれば，$\left|G\right|$ はその指数の倍数になる．

(ii) G の位数が素数ならば，G は巡回群である．

[▷1] *exponent*

Proof. $a \in G$ が位数 n をもつならば，$H = \left\{1, a, a^2, \ldots, a^{n-1}\right\}$ $\left|H\right| = n$ をみたす G の巡回部分群である．Lagrange' Theorem によって，n は $\left|G\right|$ を割り切るから，(i) が成り立つ．もし $\left|G\right|$ が素数ならば，$a \neq 1$ として $n = \left|G\right|$ となる．従って，H は G と同数の要素からなる部分群となり，H と G は一致する．これで (ii) が示された．■

では，オマチカネのオマケを召し上がれ．$n \in \mathbb{Z}^+$ として，mod n での乗法を考えるとき，逆元をもつような元を**単数** [▷2] と言う．n が素数 p ならば，mod p での単数は $\{1, 2, \ldots, p-1\}$ であるが，n が合成数の場合には，$\varphi(n)$ 個ある．ここで φ は **Euler の φ 関数** [▷3] である．n を固定するとき，mod n の単数全体は乗法に関して群をなす．この群を mod n における**単数群** [▷4] と言う．

[▷2] *unit*

[▷3] *Euler's φ-Function*

[▷4] *group of units*

THEOREM 3.2.10 (Euler's Theorem)

a と n を互いに素である正整数として，$n \geq 2$ とするとき，$a^{\varphi(n)} \equiv 1 \pmod{n}$ が成り立つ．この特別な場合として，**フェルマーの小定理** [▷5] がある：p を素数，a を p で割り切られない正整数とすれば，$a^{p-1} \equiv 1 \pmod{p}$ が成り立つ．

[▷5] *Fermat's Minor Theorem*

Proof. (mod n) における単数群は位数 $\varphi(n)$ をもつから，Corollary 3.2.9 から主張が成り立つ．■

§ 3-3. 群の有理式への作用

G を N 次の置換群とし，$H \triangleleft G$ を

$$H = \{\mathsf{h}_1(=\boldsymbol{\iota}), \mathsf{h}_2, \mathsf{h}_3, \ldots, \mathsf{h}_p\}$$

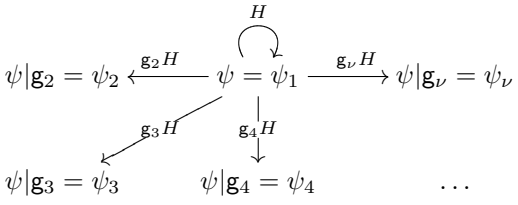
とする．G は次の矩形配列によって表わされる：

H	$\mathsf{h}_1 = \boldsymbol{\iota}$	h_2	h_3	$\ldots$	h_p
$H\mathsf{g}_2$	g_2	$\mathsf{h}_2\mathsf{g}_2$	$\mathsf{h}_3\mathsf{g}_2$	$\ldots$	$\mathsf{h}_p\mathsf{g}_2$
$H\mathsf{g}_3$	g_3	$\mathsf{h}_2\mathsf{g}_3$	$\mathsf{h}_3\mathsf{g}_3$	$\ldots$	$\mathsf{h}_p\mathsf{g}_3$
	$\ldots$		$\ldots$		
$H\mathsf{g}_\nu$	g_ν	$\mathsf{h}_2\mathsf{g}_\nu$	$\mathsf{h}_3\mathsf{g}_\nu$	$\ldots$	$\mathsf{h}_p\mathsf{g}_\nu$.

THEOREM 3.3.1 (有理式と部分群 (D29))

G を n 次の置換群とし，$H \triangleleft G$, $[G:H] = \nu$ とする．

$\psi = \psi(X_1, X_2, \ldots, X_n)$ を H に帰属する有理式とすれば，ψ は G において ν 価である．



このようにして得られる $\psi_2, \ldots, \psi_\nu$ を，$\psi(=\psi_1)$ の**共役** [▷6] と呼ぶ.

[▷6] *conjugate*

THEOREM 3.3.2 (Lagrange (D29))

有理式 $\psi = \psi(X_1, X_2, \ldots, X_n)$ に S_n を作用させて ν 個の式が得られるならば，ν は $n!$ の約数である：$\nu \,\big|\, n!$.

THEOREM 3.3.3 (共役を根にもつ方程式 (D30))

有理式 $\varphi = \varphi(X_1, X_2, \ldots, X_n)$ に S_n を作用させて得られる共役が ρ 個あるとき，これらの共役は ρ 次の方程式の根であり，この方程式の係数は $X_1, X_2, \ldots, X_n$ の基本対称式 $\sigma_1, \sigma_2, \ldots, \sigma_n$ の有理式である.

これらの共役を根にもつ方程式を**還元方程式** [▷1] と呼ぶ.

[▷1] *resolvent equation*

THEOREM 3.3.4 (Lagrange's Theorem (D31))

$\psi = \psi(X_1, X_2, \ldots, X_n)$ を不変に保つすべての置換によって $\varphi = \varphi(X_1, X_2, \ldots, X_n)$ が不変に保たれるならば，φ は ψ と $\sigma_1, \sigma_2, \ldots, \sigma_n$ によって有理的に表わされる.

$[\psi] = \{\mathsf{g} \in S_n \,|\, \psi \circlearrowleft \mathsf{g}\}$, $[\varphi] = \{\mathsf{g} \in S_n \,|\, \varphi \circlearrowleft \mathsf{g}\}$ とすると

$$[\psi] \subseteq [\varphi] \Rightarrow \psi \vdash_R \varphi.$$

ここで，$g \vdash_R f$ は有理式 f が有理式 g と $\sigma_1, \sigma_2, \ldots, \sigma_n$ によって**有理式として表わされる** [▷2] ことを意味する.

[▷2] *rationally expressible*

THEOREM 3.3.5 ((D32))

$[[\varphi] : [\psi]] = \nu$ ならば，ψ は φ と $\sigma_1, \sigma_2, \ldots, \sigma_n$ の有理式を係数とする ν 次方程式の根である.

Index