

代数方程式の根の公式とガロア理論入門 (その3)

2026.10.7 鈴木 実

9 多項式のガロア群と対称群

前節までに、ガロア群が、可解という正規部分群の系列構造をもつときに、そのガロア群に対応する拡大体は冪根拡大体の系列を含むことを述べた。つまり、拡大体が冪根と四則演算によって得られる数によって生成されるなら、その拡大体のガロア群は可解である。逆に、ある多項式の根を含む拡大体のガロア群が可解なら、その拡大体は冪根拡大体の系列を含み、その多項式の根はそこにあることになる、根は冪根と四則演算によって得られることになる。

本節では、多項式の根を含むガロア拡大体のガロア群がどのような条件を満たすときに可解になるかということについて述べる。その結果、多項式の根が冪根と四則演算によって得られるための条件がここで明らかになる。

9.1 多項式のガロア群

重根をもたない既約な n 次多項式を考える。その根を $\alpha_1, \alpha_2, \dots, \alpha_n$ とする。基礎体 P に $\alpha_1, \dots, \alpha_n$ を追加して拡大生成した P の上の拡大体を $K = P(\alpha_1, \dots, \alpha_n)$ とする。 P を不変体とする K の自己同型群をガロア群 $G = \text{Gal}(K/P)$ とする。この群 G は多項式によって一意的に決定されるので、 G を多項式のガロア群という。

拡大体のガロア群は、その基となる拡大体が具体的に明らかでなければ、それ以上深く考えることができないように思われるが、実際には、拡大体が十分具体的ではなくてもガロア群の構造を知ることが可能である。確かに、第8節で述べたように、二項拡大体のように具体的なら、ガロア群を構成する自己同型を具体的に考えることができる。そこから、前節で述べたように、剰余群が巡回群になることを考えることができた。しかし、そこまで具体的に明らかにならなくても、群の構造など一般的な性質は明らかになるのである。すなわち、多項式の根による拡大体がどのような体であるか、ということは皆目わからないのであるが、それに対して、その拡大体に対応するガロア群の構造から実は重要な性質が明らかになるのである。そのことに気がついたこと、それを可能にした群という概念に着目したことはガロアの功績である。

9.1.1 多項式のガロア群に関する二つの前提

この節では、多項式のガロア群について、その重要な性質を述べるのであるが、その前に、二つほど注意しておきたい。一つは、多項式のガロア群を、多項式の根を生成元とする拡大体のガロア群と述べたが、その多項式の根が果たして何段階かの拡大を経た拡大体の中に含まれているか、という問題である。根が拡大体の中に含まれるか不確定であれば、この後の議論は根拠が不確定になるので、このことは重要な問題である。実は、この問題については、すべての体において、十分大きな拡大体を形成したときに、その特別な拡大体では、その体の元を係数とする多項式の根はその体の中に必ず含まれる、ということが証明されている。したがって、多項式の根を含む拡大体が必ず存在するということは十分根拠があるので以下の展開の前提としてよい。このことについては、第10節において述べる。

もう一つのことは、二項拡大のときに見られたように、根の間に特定の関係があれば、一般的な準同型規則が成り立たなくなるということである。このような関係というものは、特殊なものであるから、一般的な性質

を議論するときには例外として除く必要がある。つまり、多項式の根の間には特別な関係がないということを前提にしないといけないのである。特別な関係というのは、たとえば、係数が2項以外0であるとか、因数分解できるとか、そういう関係であるが、これは一般的に係数に関する代数的な関係に帰することができる。多項式の係数の間に代数的な関係が存在しなければ、多項式の係数は互いに独立であるといえる。多項式の係数が互いに独立であれば、根の間関係も独立であるといえることができるのである。このような多項式を一般多項式とよぶ。このことは第11節で詳しく述べる。以下で扱う多項式の係数は独立であるとする。

9.1.2 多項式の高ア群 多項式の根による拡大体の自己同型と高ア群

以上のような前提のもとで、 G の元、すなわち P の上の K の自己同型の内容は、 n 次多項式 $f(x)$ の根の集合 $\alpha_1, \dots, \alpha_n$ からそれ自身への全単射写像 (置換) を一つ決めれば、それに従い P を不変体とする K の一つの自己同型写像 σ が確定する。すなわち、 P の元を係数とする $\alpha_1, \dots, \alpha_n$ の間の四則演算結果である K の元からの自己同型による変換先は、その演算結果の中に含まれる $\alpha_1, \dots, \alpha_n$ にその置換を施した結果になるということである。このことは、根 $\alpha_1, \dots, \alpha_n$ が互いに独立であること、すなわち、そのうちの複数個の根の間に代数的な関係が存在しないことを前提にしている。たとえば、 $\alpha_1 \alpha_2 = \alpha_3$ のような関係が存在しないことである。もし、そうした代数的な関係が存在すれば、 $p(\alpha_1, \dots, \alpha_n)$ という P の元を係数とする $\alpha_1, \dots, \alpha_n$ の関数があったときに、その関数の中にある代数的な関係により、 $p(\alpha_1, \dots, \alpha_n)$ が別の関数 $q(\alpha_1, \dots, \alpha_n)$ なる場合も出てくる。その場合は、準同型規則が満たされなくなる。なぜなら、関数 p と q の間に

$$p(\alpha_1, \dots, \alpha_n) = q(\alpha_1, \dots, \alpha_n)$$

という関係が、引数が $\alpha_1, \dots, \alpha_n$ のときに限り、偶然成り立つので、

$$\sigma(p(\alpha_1, \dots, \alpha_n)) = \sigma(q(\alpha_1, \dots, \alpha_n)) = q(\sigma(\alpha_1), \dots, \sigma(\alpha_n))$$

となるが、一方、

$$p(\sigma(\alpha_1), \dots, \sigma(\alpha_n)) \neq q(\sigma(\alpha_1), \dots, \sigma(\alpha_n))$$

であるから、

$$\sigma(p(\alpha_1, \dots, \alpha_n)) \neq p(\sigma(\alpha_1), \dots, \sigma(\alpha_n))$$

となり、準同型規則が満たされなくなるからである。したがって、根が代数的に独立であれば、 $\alpha_1, \dots, \alpha_n$ の置換で決まる K の自己同型は確立する。これから、式 (14)、(15) の準同型写像の条件は自動的に満たされる。根が代数的に独立であるということは、 n 次多項式 $f(x)$ の係数が代数的に独立であることと同値である。これに関しては、第11節で詳しく述べる。

こうして定義された K の自己同型が一意的であることは次のようにしてわかる。 $p(x_1, \dots, x_n)$ を、 P の元を係数とする $x_1, \dots, x_n$ の四則演算による関数であるとする、 K のすべての元は $p(\alpha_1, \dots, \alpha_n)$ で表すことができる。 G の一つの元を σ とすると、 $\sigma(\alpha_i) = \alpha_j (1 \leq i, j \leq n)$ とすることができる。 σ によって $p(\alpha_1, \dots, \alpha_n)$ が $\sigma(p(\alpha_1, \dots, \alpha_n))$ に変換されたとする。そうすると、準同型規則によって、

$$\sigma(p(\alpha_1, \dots, \alpha_n)) = p(\sigma(\alpha_1), \dots, \sigma(\alpha_n)) \quad (144)$$

となる。2つの異なる元 $p(\alpha_1, \dots, \alpha_n)$ と $q(\alpha_1, \dots, \alpha_n)$ が自己同型 σ によって同一の元に変換されたとする。すなわち、

$$\sigma(p(\alpha_1, \dots, \alpha_n)) = \sigma(q(\alpha_1, \dots, \alpha_n))$$

であったとする。その場合、

$$\sigma(p(\alpha_1, \dots, \alpha_n)) - \sigma(q(\alpha_1, \dots, \alpha_n)) = \sigma(p(\alpha_1, \dots, \alpha_n) - q(\alpha_1, \dots, \alpha_n)) = 0$$

となるから, $p(\alpha_1, \dots, \alpha_n) = q(\alpha_1, \dots, \alpha_n)$ でなければならない. つまり, G の自己同型は 1 対 1 写像である. すなわち単射であるから, 逆写像も存在する. σ の逆写像は $\alpha_1, \dots, \alpha_n$ の逆置換で与えられるから, K のすべての元 $p(\alpha_1, \dots, \alpha_n)$ において逆置換による逆写像が可能である. つまり, 全射であることが保証される. このように, G の元による P の上の K の自己同型は, n 次多項式の根 $\alpha_1, \dots, \alpha_n$ の置換を決めることにより一意的に決定される.

このように, P の元を係数とする n 次多項式 $f(x)$ の根が拡大体 K の生成元となり, P の上の K の自己同型からガロア群 G が得られることから, つまり, この $f(x)$ によってガロア群 G が決定されることから, この群 G を特に多項式のガロア群という.

9.1.3 n 次多項式の係数と基本対称式

$f(x)$ を最高次の係数が 1 である n 次の多項式とし,

$$f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} \cdots + a_{n-1}x + a_n \quad (145)$$

とする. $a_1, a_2, \dots, a_{n-1}, a_n$ は基礎体 P の元である. $f(x)$ をその根 $\alpha_1, \dots, \alpha_n$ で表すと,

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) \quad (146)$$

である. これを展開すると,

$$f(x) = x^n + (\alpha_1 + \alpha_2 + \cdots + \alpha_n)x^{n-1} + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 + \cdots + \alpha_{n-1}\alpha_n)x^{n-2} + \cdots + \alpha_1\alpha_2 \cdots \alpha_n \quad (147)$$

となる. ここで, 式 (145) と式 (147) の x^i の係数を比較することにより, 係数の a_i は次のように表される.

$$\begin{aligned} a_1 &= \alpha_1 + \alpha_2 + \cdots + \alpha_n \\ a_2 &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 + \cdots + \alpha_{n-1}\alpha_n \\ &\vdots \\ a_i &= (-1)^i \sum_{\substack{i=1 \\ \nu_1 + \cdots + \nu_n = i \\ \nu_1, \dots, \nu_n = 0, 1}}^n \alpha_1^{\nu_1} \alpha_2^{\nu_2} \cdots \alpha_n^{\nu_n} \\ &\vdots \\ a_n &= \alpha_1\alpha_2 \cdots \alpha_n \end{aligned} \quad (148)$$

この式の右辺は, $\alpha_1, \dots, \alpha_n$ の i 次の対称式になっている. つまり, $\alpha_1, \dots, \alpha_n$ を置換しても式全体としては変わらない. 次数が決まれば, 対称式の形は一定の形に決まる. それがこの式の右辺であり, 特に, この形の対称式を基本対称式とよぶ. 一般に, すべての対称式は基本対称式の有理関数であらわすことができる (証明は後述).

$f(x)$ の根の置換が, P を不変体とする K の自己同型になることは, 式 (145) はあまり直感的ではないが, $f(x)$ がこの自己同型に対して不変になることは, 式 (147) または式 (148) において, $f(x)$ 自身または係数 a_i 自身が対象式になり, 根の置換に対し不変になっていることをみれば明解である.

9.2 多項式のガロア群と対称群

9.2.1 対称群

前節の多項式のガロア群 G を構成する P の上の K の自己同型は、 $f(x)$ の根の集合 $\alpha_1, \dots, \alpha_n$ の置換、すなわち、根をそれぞれ自分自身または他の根と置換するという同じ集合への 1 対 1 写像を決定することで確定することができた。この定義により、 K のすべての元に対して準同型条件を満たす全単射が確立することは前節で述べた。この写像を表す上で、根の集合の元を一つの定められた順に並べることが有用である。写像の 1 つを S とし、これを定められた順の根の列 $(\alpha_1, \dots, \alpha_n)$ に作用させると、

$$S(\alpha_1, \dots, \alpha_n) = (\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_n}) \quad (149)$$

と表すことができる。個別の根は写像に対して、 $S(\alpha_j) = \alpha_{i_j}$ となる。この S は、したがって、ガロア群 G の元である。

この置換を α_i の添字に着目し、添字の置換として表すことができる。 S を α_j を α_{i_j} に置換する写像とし、 α_i で決められた順の添字 n 個の列を $(1, 2, \dots, n)$ と表すと、 $(1, 2, \dots, n)$ は、 S によって変換された α_i の添字により、 $(i_1, i_2, \dots, i_n)$ に変換される。すなわち、この添字の変換を σ で表すと

$$\sigma(1, 2, \dots, n) = (i_1, i_2, \dots, i_n) \quad (150)$$

となる。 i_1 から i_n は重複しない 1 から n までの整数である。これを、個々の添字の置換が明確な表現として、慣用的に次のような表現が使われる。

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \quad (151)$$

この記法では添字の順序は必ずしも必須ではなく、上下の数の対応が置換を決定する。これは置換の積を容易に理解できるようにする。たとえば、 j_1 から j_n を重複しない 1 から n までの整数として、

$$\tau = \begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ j_1 & j_2 & \cdots & j_n \end{pmatrix} \quad (152)$$

という置換 τ があれば、その積 $\sigma\tau$ は

$$\tau\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ j_1 & j_2 & \cdots & j_n \end{pmatrix} \quad (153)$$

と表される。このことは、連鎖した置換が、 $1 \rightarrow i_1 \rightarrow j_1$, $2 \rightarrow i_2 \rightarrow j_2$ となるのを見れば明らかであろう。この積では、最初に σ の置換を施し、次に τ を施すことになる。恒等置換 e と逆置換 σ^{-1} も次のように表される。

$$e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix} \quad (154)$$

$$\sigma^{-1} = \begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ 1 & 2 & \cdots & n \end{pmatrix} \quad (155)$$

このような置換の集合は群を形成する。すべての置換の集合は 1 から n までの整数の順列の数 $n!$ に等しい。この群は n 次の対称群とよばれ、通常 S_n と表記される。 S_n の部分群は n 次の置換群とよばれる。

9.2.2 ガロア群と対称群が同型であること／対称群がなぜ重要か

ガロア群 G の元 S を式 (149) として決めれば、それに対して S_n の元は式 (151) により一意的に決まる。すなわち、 G から S_n への 1 対 1 写像が可能である。一方、 S_n の任意の元を σ のように決めれば、既約な多項式

$f(x)$ を最小分解体とするガロア群 G においては、添字が σ のように変換される α_i の置換が必ず G の中に存在する。つまり、 S_n から G への 1 対 1 写像が可能である。

ただし、既約でない多項式の最小分解体もガロア群を形成するが、その場合、根の置換は既約な多項式因子の根の中でのみ許されるので、ガロア群 G は S_n の部分群と同型になる。ここでは、 $f(x)$ は既約多項式であることを前提としているので、したがって、 G と S_n は同型である。

このことは、多項式の根の公式が存在するか否かを議論する上において、非常に重要な結論である。つまり、多項式の根を追加して拡大した拡大体が具体的にどのようなものかわからないとしても、その拡大体のガロア群がわかれば、拡大体が可解であるかどうかを判断できるのであるが、今、明らかになったことは、そのガロア群が対称群と同型であるということである。すなわち、対称群の構造を分析すれば、多項式が可解であるか否かがわかるということである。したがって、多項式の根の公式の有無を追求する立場からは、この後は対称群の中身を理解していけばそれが明らかになる、ということを示しているのである。そこで、次節からは、その対称群について、詳しく述べることにする。

9.3 対称群、置換群、巡回置換、互換、交代群

9.3.1 対称群とその部分群としての置換群

1 から n までの整数の集合からその集合自身への写像（全単射）を置換という。集合の元の個数、すなわち n は置換の次数である。したがって、上の全単射は n 次の置換である。 n 次の置換は順列の種類あるいは順列の個数で表される。このような置換を前節の式 (151) のように記述する。 n 次のすべての置換の集合の全体は群を形成し、その群が対称群 S_n である。以下では S_n の部分群について、およびそのガロア群との対応について述べる

n 次の対称群 S_n には一般に部分群が存在する。このような部分群は n 次の置換群とよばれる。多項式のガロア群 G において、 n 次の置換群は G のどの部分に対応するか考えてみよう。

ガロア拡大体 K が、2つのそれぞれ k 次と m 次の既約多項式 $g(x)$ と $h(x)$ の積 $g(x)h(x)$ の最小分解体であるとし、そのガロア群を G 、かつ、 $k+m=n$ とする。それぞれの根を α_i ($i=1, \dots, k$) と β_j ($j=k+1, \dots, n$) とする。このとき、 G のいかなる自己同型も α_i と β_j との間の置換を含まない。なぜなら、もし α_i と β_j の置換を含む自己同型があれば、 $g(\beta_j) \neq 0$ となり、準同型条件を満たさなくなるからである。したがって、ガロア群の自己同型は、全体として α_i の中だけ、および β_j の中だけの置換に閉じている。そのとき、 α_i の中だけの自己同型の写像は S_n の部分群となり、 β_j の中だけの置換も同様となる。そのような S_n の元は、

$$\begin{pmatrix} 1 & \cdots & k & k+1 & \cdots & n \\ i_1 & \cdots & i_k & j_1 & \cdots & j_m \end{pmatrix} \quad (156)$$

と表すことができる。ここで、 $i_1, \dots, i_k$ は $1, \dots, k$ の置換であり、 $j_1, \dots, j_m$ は $k+1, \dots, n$ の置換である。このような 2 つの置換の積は式 (156) と同じ型の置換になることは明らかであるから、この型の置換は 1 つの n 次部分置換群を形成することがわかる。また、この式 (156) の置換群は次の 2 つの n 次部分置換群を含む。

$$\begin{pmatrix} 1 & \cdots & k & k+1 & \cdots & n \\ i_1 & \cdots & i_k & k+1 & \cdots & n \end{pmatrix}, \quad \begin{pmatrix} 1 & \cdots & k & k+1 & \cdots & n \\ 1 & \cdots & k & j_1 & \cdots & j_m \end{pmatrix}$$

左の置換では 1 から k までは不変で、右の置換では $k+1$ から n までは不変に保たれる。3 個以上の既約多項式の積の最小分解体であれば、そのガロア群は同様な部分置換群になることは容易にわかる。以上のように、ガロア群は一般に対称群 S_n の部分群である置換群と同型である。しかし、可約な多項式のガロア群の議論は既約な多項式のガロア群に帰結できるので、以下では、既約な多項式のガロア群の場合について述べる。

9.3.2 対称群とガロア群の位数、およびガロア拡大の次数

ガロア群の位数とガロア拡大の次数については第8節で述べたように、この2つは一致する。上で述べたように、既約多項式のガロア群は対称群と同型になる。これを具体的に確かめてみよう。

ガロア群 G の位数は、対称群 S_n と同型であるから、 $n!$ である。一方、ガロア拡大の次数の計算は、ガロア拡大 K/P が、 $f(x)$ の根を $\alpha_1, \alpha_2, \dots, \alpha_n$ として、組成拡大体 $P(\alpha_1)(\alpha_2) \cdots (\alpha_n)$ と表すことができるところから始める。

組成拡大体の各段階における中間体を $K_i = K_{i-1}(\alpha_i)$, $(i = 0, 1, \dots, n)$ のように表し、 $K_0 = P$ かつ $K = K_n$ とする。すなわち、

$$\begin{aligned} K_0 &= P \\ K_1 &= K_0(\alpha_1) = P(\alpha_1) \\ K_2 &= K_1(\alpha_2) = P(\alpha_1)(\alpha_2) \\ &\vdots \\ K_i &= K_{i-1}(\alpha_i) = P(\alpha_1)(\alpha_2) \cdots (\alpha_i) \\ &\vdots \\ K_n &= K_{n-1}(\alpha_n) = P(\alpha_1)(\alpha_2) \cdots (\alpha_n) = K \end{aligned}$$

とする。最初の拡大体 $K_1 = P(\alpha_1)$ は、 n 次多項式 $f(x)$ の根 α_1 による $P = K_0$ の上の単純拡大体であるから、拡大体 K_1 の基底は $1, \alpha_1, \dots, \alpha_1^{n-1}$ となり、基底の個数は n 個で、拡大の次数 $[K_1 : K_0]$ は n である。すなわち、

$$[K_1 : K_0] = n$$

となる。

次に、 $K_1 = P(\alpha_1)$ に α_2 を追加した単純拡大体 $K_2 = P(\alpha_1)(\alpha_2)$ を考える。 $K_1 = P(\alpha_1)$ の上の α_2 の最小多項式は $f(x)/(x - \alpha_1)$ であるから、 $n - 1$ 次多項式である。なぜなら、 α_1 はすでに K_1 に含まれているので、 $(x - \alpha_1)$ は可約式として $f(x)$ から除かれるからである。したがって、 K_1 の上の拡大体 $K_2 = P(\alpha_1)(\alpha_2)$ の基底は、 $1, \alpha_2, \dots, \alpha_2^{n-2}$ の $n - 1$ 個となり、拡大の次数は

$$[K_2 : K_1] = n - 1$$

となる。

K_2 の上の α_3 による単純拡大体 K_3 においても同様にして、 α_3 の K_2 の上の最小多項式は $f(x)/((x - \alpha_1)(x - \alpha_2))$ であるから

$$[K_3 : K_2] = n - 2$$

となる。

以下同様にして、 K_n まで進むと、

$$[K_n : K_{n-1}] = 1$$

となる。

最後の式は、 $P(\alpha_1)(\alpha_2) \cdots (\alpha_{n-1})$ に α_n を追加して体を単拡大する場合である。拡大次数が1ということ、追加しても体の次元は変化しないということである。この意味を、一つ前の拡大体 K_{n-1} から考えてみよう。 K_{n-1} に追加する α_{n-1} の最小多項式は、 $f(x)/[(x - \alpha_1) \cdots (x - \alpha_{n-2})]$ という2次式である。この2次式の係数は式(145)の $a_1, \dots, a_n$ と $\alpha_1, \dots, \alpha_{n-2}$ である。 α_{n-1} はこの2次式の根であるから、これに代入する

と α_{n-1} の 2 次方程式になる．したがって、 α_{n-1}^2 は α_{n-1} の 1 次式で表され、これにより、1 と α_{n-1} が K_{n-1} の基底になる．

この考えで次の体の拡大 K_n/K_{n-1} を考えると、 α_n の最小多項式は $f(x)/[(x - \alpha_1) \cdots (x - \alpha_{n-1})]$ という 1 次式になるが、これは $x - \alpha_n$ に他ならない．このことは、 α_n がもはや K_{n-1} の元であることを意味する．なぜなら、式 (148) を見れば明らかなように、この段階で α_n は $a_1, \dots, a_n$ と $\alpha_1, \dots, \alpha_{n-1}$ で表されるようになっているから、すでに K_{n-1} の元に含まれているのである．したがって、 K_n と K_{n-1} の次元は変わらず、 $[K_n : K_{n-1}] = 1$ となるのである．

結局、 P の上のガロア拡大体 K の拡大次数 $[K : P]$ は

$$\begin{aligned} [K : P] &= [P(\alpha_1)(\alpha_2) \cdots (\alpha_n) : P] = [K_n : K_0] \\ &= [K_n : K_{n-1}][K_{n-1} : K_{n-2}][K_{n-2} : K_{n-3}] \cdots [K_2 : K_1][K_1 : K_0] \\ &= n(n-1)(n-2) \cdots 2 \cdot 1 \\ &= n! \end{aligned}$$

となり、結局、ガロア拡大 K/P の次元は対称群 S_n の位数に等しい．さらに、ガロア群 G と対称群 S_n は同型であるから、ガロア拡大 K/P の次元はガロア群 G の位数に等しい．

9.3.3 巡回置換群

置換群の中に次のように最初の m 個の数が置換される場合を考える．

$$a = \begin{pmatrix} 1 & 2 & \cdots & m-1 & m & m+1 & \cdots & n \\ 2 & 3 & \cdots & m & 1 & m+1 & \cdots & n \end{pmatrix} \quad (157)$$

この置換では、1 から $m-1$ の数については一つ後の数で置換され、最後の m は最初の 1 で置換され、 $m+1$ から後の数はそのままになる．この置換 a をもう 1 回繰り返すと、

$$a^2 = \begin{pmatrix} 1 & 2 & \cdots & m-1 & m & m+1 & \cdots & n \\ 3 & 4 & \cdots & 1 & 2 & m+1 & \cdots & n \end{pmatrix}$$

となる． $m-1$ 回繰り返すと、

$$a^{m-1} = \begin{pmatrix} 1 & 2 & \cdots & m-1 & m & m+1 & \cdots & n \\ m & 1 & \cdots & m-2 & m-1 & m+1 & \cdots & n \end{pmatrix}$$

となる． m 回繰り返せば、明らかに、

$$a^m = \begin{pmatrix} 1 & 2 & \cdots & m-1 & m & m+1 & \cdots & n \\ 1 & 2 & \cdots & m-1 & m & m+1 & \cdots & n \end{pmatrix} = e$$

となるから、 $a, a^2, \dots, a^m$ は巡回群になることがわかる．このような置換を巡回置換という．この巡回置換で巡回する数の長さは m であるので、 m 次の巡回置換という．式 (157) の巡回置換の数の順番を変えても同じ巡回群の性質が得られるので、式 (157) は一般に次のように表すことができる．

$$a = \begin{pmatrix} i_1 & i_2 & \cdots & i_{m-1} & i_m & j_1 & \cdots & j_{n-m} \\ i_2 & i_3 & \cdots & i_m & i_1 & j_1 & \cdots & j_{n-m} \end{pmatrix} \quad (158)$$

さらに、このような巡回置換は次のように表記される．

$$a = (i_1 \ i_2 \ \cdots \ i_{m-1} \ i_m) \quad (159)$$

巡回置換であるので、次の表記は明らかに同じ巡回置換を表す。

$$(i_1 i_2 \cdots i_{m-1} i_m) = (i_2 i_3 \cdots i_m i_1) = \cdots = (i_m i_1 \cdots i_{m-2} i_{m-1}) \quad (160)$$

巡回置換の列の数の個数を巡回置換の長さという。巡回置換の長さはその巡回置換群の位数に等しい。2つの巡回置換で、移動する数が共有されないとき、この2つの巡回置換は独立であると言われる。

恒等置換を除いて、任意の置換は独立な巡回置換の積として表すことができる。この証明は少し長いので後述する。置換が独立な巡回置換に分解されるとき、その個数とそれぞれの構造は、与えられた置換によって一意的に決定される。なぜなら、それぞれの巡回置換で実際に移される数は与えられた置換の冪によって決まることから明らかである。

9.3.4 互換

巡回置換の中でもっとも短いものは長さが2の場合で、これを互換という。互換 (ij) は i と j の交換でほかのすべての数は変化しない。

巡回置換は互換の積として表すことができる。実際、

$$(i_1 i_2 i_3 \cdots i_m) = (i_1 i_2)(i_1 i_3)(i_1 i_4) \cdots (i_1 i_{m-1})(i_1 i_m) \quad (161)$$

とすることができる。この式の右辺では、最初に右端の互換をほどこし、右側から順に作用させると左辺の巡回置換に等しくなる。ここでは、右側から作用するとしたが、独立な巡回置換の間であれば作用の順序には依存しない。

巡回置換の長さが m なら、右辺は $m - 1$ 個の互換の積である。

上で述べたように、任意の置換は独立な巡回置換の積に分解することができる。一方、巡回置換は互換の積として表すことができるから、任意の置換は、互換の積として表すことができるということになる。

9.3.5 偶置換、奇置換、交代群

前節で述べたように、任意の置換は互換の積に分解できる。置換が互換に分解されたときの互換の積は一意的には定まらないが、積に組み込まれた互換の個数は、いずれの互換の積においても偶数であるか、または奇数であり、その偶奇性は互換の積の形態に依存しない。この証明も長くなるので、後述する。

以上のように、どのような置換も互換の積に分解した時に、互換の数は偶数か奇数のいずれかになり、それ以外にない。このことから、互換の積に分解した互換の個数が偶数の場合に、その置換は偶置換といい、奇数の場合には奇置換という。すなわち、すべての置換は偶置換か奇置換のいずれかになる。また偶置換と奇置換の積は奇置換になり、偶置換と偶置換の積、および奇置換と奇置換の積は偶置換になる。これは互換の個数の偶奇性に関することであるから明らかである。

恒等置換は偶置換である。長さが偶数の巡回置換は奇置換であり、長さが奇数の置換は偶置換である。これは長さが m の巡回置換が $m - 1$ 個の互換の積になるからである。置換 a が

$$a = (i_1 i_2)(i_3 i_4) \cdots (i_{r-1} i_r)$$

のように互換の積に分解されるなら、

$$a^{-1} = (i_r i_{r-1}) \cdots (i_4 i_3)(i_2 i_1)$$

となるから、偶置換の逆置換は偶置換であり、奇置換の逆置換は奇置換である。

以上のことから、 n 次の対称群 S_n において、偶置換の集合は、群を構成することがわかる。この群を n 次の交代群といい、 A_n と表す。

9.4 交代群 A_n と対称群 S_n の構造 結論

9.4.1 交代群 A_n は正規部分群

A_n の任意の置換を a とし、 S_n の任意の置換を b とする。 a は偶置換であるから、 bab^{-1} は偶置換になる。したがって、 bab^{-1} は A_n の元となるから、 A_n は S_n の正規部分群である。

9.4.2 交代群 A_n の位数

次に、任意の2つの奇置換を a および b とする。このとき、 $a^{-1}b$ は偶置換になるから、 A_n に属する。したがって、 a および b は正規部分群 A_n に関する同一の剰余類に属する (第 3.1.6 節)。これから、すべての奇置換の集合は1つの剰余類を作ることがわかる。 S_n には偶置換および奇置換の2種類からなるので、 S_n は偶置換のみからなる正規部分群 A_n と、 A_n に関する奇置換のみからなる剰余類から構成されることがわかる。剰余類の数は奇置換のみからなる集合と、偶置換のみからなる A_n であり、 A_n に関する S_n の指数 $(S_n : A_n)$ は2である。したがって、剰余群 S_n/A_n は2つの元からなり、その位数は2である。ラグランジュの定理から、 n 次の交代群 A_n の位数は対称群 S_n の位数 $n!$ の $1/2$ である。すなわち、 n 次の偶置換の個数は $n!/2$ である。

9.4.3 交代群 A_n は単純群

対称群 S_n の中の部分群には単一の巡回置換群や独立な巡回置換群などや、他にも n よりも次数の小さい対称群などが存在する。しかし、正規部分群に限ればどうだろうか。これまで述べてきたことから、正規部分群としては交代群 A_n が存在することがわかっている。単位元からなる正規部分群 $\{e\}$ や S_n 自身は自明な正規部分群とよばれているが、この自明な正規部分群をのぞけば、 A_n の他に正規部分群はあるのだろうか。結果から言えば、 $n \geq 5$ の場合に、 S_n には A_n 以外に正規部分群はない。交代群 A_n について言えば、 A_n には自明な正規部分群を除けば、正規部分群は存在しない。このような群は単純群とよばれる。すなわち、交代群 A_n は $n \geq 5$ のとき単純群である (証明は後述)。この結果は非常に重要なもので、本文章の結論を直接導く内容である。すなわち、多項式の根の公式が存在しないということがここから導かれるのである。次節でその内容を述べる。

9.4.4 結論 交代群 A_n は非可解群 多項式の根の公式は存在しない

交代群 A_n は S_n の正規部分群で、指数 $(S_n : A_n)$ が2であり、 S_n の元のうち半数の偶置換のみが属する。上で述べたように、 A_n は $n \geq 5$ のとき単純群である。このことからわかる重要なことは、 A_n は巡回群ではあり得ないということである。なぜなら、もし、 A_n が巡回群なら、 A_n の位数は素数でなければならないが、実際は上にも述べたように $n \geq 5$ では A_n の位数は $n!/2$ であり、明らかに素数ではないからである。もし、 A_n の位数が素数でなければ、その約数を位数とする巡回部分群が存在することになり、 A_n が単純群であることと矛盾するからである。 A_n の位数の約数を位数にもつ部分群があるというのはラグランジュの定理の逆であるが、巡回群の場合はこのラグランジュの定理の逆が成り立つ (第 8.1.2 節)。

結局、交代群 A_n は単純群であり、巡回群ではないことが明らかになった。このことが重要であることは、可解群と密接に関係しているからである。可解群は、ガロア群とその中に含まれる正規部分群の包含関係の列において、隣り合う正規部分群に関する剰余群が巡回群になっていることであった (第 8.4 節)。 A_n は単純群であるから、 A_n 自身が巡回群でなければ、 A_n は可解群ではないということである。つまり、このことが意味することは、 $n \geq 5$ の場合、すなわち、5 次以上の多項式は可解ではないということである。すなわち、5 次以上の多項式の根の公式は存在しないことを意味する。これが、これまで述べてきたガロア理論の一つの大きな結論である。

(つづく)

B 諸定理の証明

B.1 すべての対称式は基本対称式の有理関数であらわすことができる

$f(x)$ をモニックな n 次一般多項式とする。モニックとは最高次の係数が 1 である多項式のことである。

$$f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n \quad (\text{B } 1)$$

一般多項式については第 11 節で述べるので、ここでは重根を持たず、かつ既約な多項式であるとする。このようなことを保証するには、多項式の係数 $a_1, a_2, \dots, a_n$ が代数的に独立である必要がある。それを表すには、 $a_1, a_2, \dots, a_n$ を P の元を値にとる変数であると考え、このような変数を係数とする多項式でも必ず根を持つということは第 10 節で述べる。ここでは、 $f(x)$ の根を $\alpha_1, \alpha_2, \dots, \alpha_n$ とする。この根 α_i と係数 a_i の間の関係は式 (148) に示される。この関係は、 a_i が $\alpha_1, \alpha_2, \dots, \alpha_n$ に関して対称であり、基本対称式であることを示している。

$\alpha_1, \alpha_2, \dots, \alpha_n$ の対称式が基本対称式、すなわち $a_1, a_2, \dots, a_n$ で表されることを証明するために、次のような筋道を考える。基礎体 P に $\alpha_1, \alpha_2, \dots, \alpha_n$ を追加して拡大した代数的生成拡大体 $K = P(\alpha_1, \dots, \alpha_n)$ において、 $\alpha_1, \dots, \alpha_n$ に関して対称な元、すなわち、 $\alpha_1, \dots, \alpha_n$ の対称式のみを抽出した集合を考える。この集合は明らかに体を構成する。したがって、この体を K_0 とする。もう一つは、基礎体 P に式 (B 1) の係数 $a_1, a_2, \dots, a_n$ を変数とみなして追加した代数的生成拡大体 $K'_0 = P(a_1, \dots, a_n)$ を考える。この K'_0 と K_0 が等しいことを示す。これが等しければすべての $\alpha_1, \dots, \alpha_n$ の対称式、すなわち K_0 の元は $a_1, a_2, \dots, a_n$ の関数に等しいことを意味するからである。

まず、 K_0 から始めよう。基礎体 P に $\alpha_1, \alpha_2, \dots, \alpha_n$ を追加した拡大体 K は P の元を係数とする $\alpha_1, \dots, \alpha_n$ の有理関数の集合とみなすことができる。その関数の中には $\alpha_1, \dots, \alpha_n$ の置換に関して対称な関数も含まれる。その対称式の集合は明らかに体を構成する。この体を K_0 とする。一方、 $\alpha_1, \alpha_2, \dots, \alpha_n$ の置換は K から K への自己同型群を構成する。これを G とする。 G の任意の元 σ による置換に対して、対称式の集合である K_0 は変化しない。 K_0 の元以外はすべて σ によって変化する。したがって、 K_0 は G によって変化しない K の部分体すなわち不変体 K^G になる。これから、 $K^G = K_0$ が成り立つ。ガロア拡大の定義から (第 8.7 節の (3)), K/K_0 はガロア拡大になり、 $G = \text{Gal}(K/K_0)$ はガロア群である。

ガロア群 G の元 S の表す置換を

$$\alpha_1, \alpha_2, \dots, \alpha_n \rightarrow \alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \dots, \alpha_{\sigma(n)}$$

とする。一方、 n 次の対称群 S_n において、 S による α_i の添字の置換に対応する S_n の元を σ とすると、 σ は次の置換になる。

$$1, 2, \dots, n \rightarrow \sigma(1), \sigma(2), \dots, \sigma(n)$$

このとき、 S と σ の対応は明らかに 1 対 1 であり、 G の任意の元は必ず S_n の元に対応する。したがって、

$$|G| \leq |S_n| = n!$$

となる。一方、 G は K_0 を不変体とするガロア群であるから、ガロア群の定義から (第 8.7 節の (4)),

$$|G| = [K : K_0]$$

が成り立つ。したがって、

$$|G| = [K : K_0] \leq n! \quad (\text{B } 2)$$

となる。

次に、上の結果を K'_0 の場合と比較する。

上で述べた $P(a_1, \dots, a_n)$ は n 変数多項式環 $P[a_1, \dots, a_n]$ を、零因子を除いた $P^\times[a_1, \dots, a_n]$ で割った商体である。ただし、ここでは変数 $a_1, \dots, a_n$ は P の元を値にもつ。この体を K'_0 とすると、 $a_1, \dots, a_n$ は基本対称式であるから、 P の元を係数としたその有理式の集合である K'_0 の元も対称式である。したがって、

$$K'_0 \subset K_0 \quad (\text{B } 3)$$

が成り立つ。

一方、 K'_0 に $f(x)$ の根 $\alpha_1, \alpha_2, \dots, \alpha_n$ を追加して拡大した体は K に等しくなる。なぜなら、 $a_1, \dots, a_n$ は P の元の範囲の中で変わるものであるから、 P に $a_1, \dots, a_n$ を追加して拡大した $P(a_1, \dots, a_n)$ も、数的には、 P と同一であるので、 P に $\alpha_1, \alpha_2, \dots, \alpha_n$ を追加して拡大した K も、 $P(a_1, \dots, a_n) = K'_0$ に $\alpha_1, \alpha_2, \dots, \alpha_n$ を追加した拡大体と同じだからである。

K は $f(x)$ の K'_0 上の最小分解体である。したがって、 K/K'_0 はガロア拡大であり、 $G = \text{Gal}(K/K'_0)$ は n 次多項式 $f(x)$ のガロア群である。 G は K の自己同型群でその元は $\alpha_1, \dots, \alpha_n$ の間の置換である。このとき、拡大の次数 $[K : K'_0]$ は 9.3.2 節で述べたように、

$$[K : K'_0] = n! \quad (\text{B } 4)$$

である。また、ガロア群の定義から

$$[K : K'_0] = |G| \quad (\text{B } 5)$$

も成り立つ。以上の式 (B 2), (B 4), (B 5) から、結局、

$$n! = [K : K'_0] = |G| = [K : K_0] \leq n! \quad (\text{B } 6)$$

となる。すなわち、

$$[K : K_0] = [K : K'_0] \quad (\text{B } 7)$$

となるが、 $K'_0 \subset K_0 \subset K$ という包含関係の中で、拡大の次数が同じということは、拡大体の基底も同じであるから、拡大の基礎体も同じでなければならない。つまり、これは

$$K_0 = K'_0$$

であることを意味する。

この等式が意味することは、左辺 K_0 の任意の元が $\alpha_1, \alpha_2, \dots, \alpha_n$ の対称式であり、それに等しい元が右辺の K'_0 に存在し、その元は $a_1, \dots, a_n$ の有理関数であるということである。これはすなわち、すべての対称式は基礎対称式の有理関数で表されることを意味する (証明終)。

B.2 任意の置換は独立な巡回置換の積として一意的に表すことができる

1つの n 次の置換をみた場合、 n 個の数のうちに実際に他の数に移される数とそうでない数がある。この実際に移される数の個数を s とし、この s に関する数学的帰納法で証明する。

$s = 2$ のとき、この場合の置換は単なる互換であるから、この定理は成り立つ。

次に、 $s - 1$ 以下でこの定理が成り立つと仮定する。まず、 s 個の数が実際に移される置換をとりあげ、これを a とする。 s 個の実際に移される数のうちの1つを i_0 とする。これに a を施すと、この i_0 は i_1 に移る。 i_1 は置換 a によって移される s 個の数の中の一つである。同様にして、 i_1 に a を施すと、この i_1 は i_2 に移る。 i_2 についても同様である。これを次々に繰り返すと、必ずある回数で i_0 に移ることになる。なぜなら、数の移り先はもともとの s 個の数に限られるからである。 q 回目初めて i_0 になったとすると、 q は $a^q i_0 = i_0$ になる最小の数で、かつ、

$$i_0, i_1, \dots, i_{q-1}$$

はすべて異なる数になる。なぜなら、 $i_l = i_m$, ($0 < l < m < q$) となったとすると、 $a^l i_0 = a^m i_0$ であるから、両辺に a^{-l} を掛ければ、 $i_0 = a^{m-l} i_0$, ($0 < m-l < q$) となり、 q より小さい $m-l$ 回で i_0 に等しくなるので、 q が最小であることに反するからである。これから、 i_p ($0 < p < q$) が i_q よりも先に i_0 になるような p は存在しないということを意味する。すなわち、 i_0 から i_{q-1} はすべて異なる。したがって、次のような巡回置換が成り立つ、

$$(i_0 i_1 \dots i_{q-1})$$

この巡回置換は、置換 a による i_0 から i_{q-1} までの数の移動を表している。ここで、 $(i_0 i_1 \dots i_{q-1})^{-1} a$ という置換を考え、これを次のように、置換 b とおく。

$$(i_0 i_1 \dots i_{q-1})^{-1} a = b \quad (\text{B } 8)$$

左辺の置換は、その作りから、 $i_0, i_1, \dots, i_{q-1}$ が移されない数になっている。したがって、左辺の置換で移される数は $s - q$ 個になる。帰納法の仮定により、左辺の置換、すなわち、置換 b は独立な巡回置換に分解されることを意味する。置換 b の移される数の中には $i_0, i_1, \dots, i_{q-1}$ は含まれていない。したがって、式 (B 8) の両辺に $(i_0 i_1 \dots i_{q-1})$ を掛けて、

$$a = b (i_0 i_1 \dots i_{q-1})$$

とすると、右辺は独立な巡回置換の積である。つまり、 a は独立な巡回置換の積で表される。以上で、帰納法により任意の置換が独立な巡回置換の積に分解されることが示された。

また、こうして得られた独立な巡回置換の積の中の個々の巡回置換は、もとの置換 a の冪によりその長さと移される数が自動的に決められる。したがって、このような巡回置換の個数とそれぞれにおける構造、すなわち長さと数は一意的に決定される。このことから、置換の独立な巡回置換への分解は、因子の順序を除いて、一意的に決定される (証明終)。

B.3 任意の置換は互換の積で表され、その偶奇性は積の表現に依存しない

この定理を証明するために、次の補題を証明する必要がある。

[補題] 恒等置換に等しい互換の積があれば、その積を構成する互換の個数は偶数である。

恒等置換に等しい次のような q 個の互換の積を考える。

$$(i_1 i_2)(i_3 i_4) \dots (i_{2q-1} i_{2q}) = e \quad (\text{B } 9)$$

左辺の互換の積に含まれる異なる数の個数を s とし、 $s \geq 2$ に関する数学的帰納法を用いる。

$s = 2$ の場合, 右辺が恒等置換 e であるから, 左辺は 1 つの互換ではありえず, 必ず互換の偶数冪でなければならない. なぜなら, 互換の 2 乗は恒等置換であるから, 奇数冪なら 1 つの互換と同じになり恒等置換にはならないからである. したがって, $s = 2$ の場合に成り立つことが示された.

$s - 1$ 以下の場合, 補題は証明されていると仮定する. 式 (B 9) の互換において, 異なる s 個の数の一つを i とする. i を含む互換とその左の i を含まない互換の積に着目し, i を含む互換を, 次の関係式を用いて, 右側から左側に移すことができる.

$$(j\ k)(i\ k) = (i\ j)(j\ k) \quad (i \neq j) \quad (\text{B } 10)$$

この式が成り立つことは, $i\ j\ k$ に互換の積を右側から作用させていくと, 次の表にあるように, 左辺と右辺それぞれ

$$\begin{array}{ccc} & i & j & k \\ (i\ k) & \frac{k}{j} & \frac{j}{i} & \\ (j\ k)(i\ k) & j & k & i \end{array} \qquad \begin{array}{ccc} & i & j & k \\ (j\ k) & \frac{i}{k} & \frac{k}{j} & \\ (i\ j)(j\ k) & j & k & i \end{array}$$

となり, 両者が一致することがわかる.

2 つの互換が独立なら左右の互換は交換できるが, 上の式 (B 10) のように 2 つの互換の中に 1 つの一致する数が含まれていればそのまま交換はできないが, 式 (B 10) を用いれば i を含む互換を左に移すことができる.

このような手続きを用いて, i を含む互換をすべて左側に移すことができるので, 最終的に次のような式になる.

$$(i\ j_1)(i\ j_2)\cdots(i\ j_p)(k_1\ k_2)\cdots(k_{2r-1},\ k_{2r}) \quad (\text{B } 11)$$

左側に i を含む互換が p 個, 右側に i を含まない互換が r 個存在する. ここで, 次の 2 つの式を用いて i を含む互換の個数を 1 個または同時に 2 個減らすことができる.

$$(i\ j)(i\ k) = (i\ k)(j\ k) \quad (j \neq k) \quad (\text{B } 12)$$

$$(i\ j)(j\ i) = e \quad (\text{B } 13)$$

式 (B 12) が成り立つことは, 式 (B 10) の場合と同様にして, 次の式からわかる.

$$\begin{array}{ccc} & i & j & k \\ (i\ k) & \frac{k}{j} & \frac{j}{i} & \\ (i\ j)(i\ k) & k & i & j \end{array} \qquad \begin{array}{ccc} & i & j & k \\ (j\ k) & \frac{i}{k} & \frac{k}{j} & \\ (i\ k)(j\ k) & k & i & j \end{array}$$

この操作を続けていけば, i を含む互換の個数 p は 0 または 1 になる. $p = 1$ の場合は, i は他の数に移ったまま他に i を含む互換はないから全体の置換としては恒等置換にはならない. したがって, $p = 1$ はありえず, $p = 0$ となり, i を含む互換はなくなる. これにより, 全体の互換の積に含まれる異なる数の個数は $s - 1$ 以下になる. 帰納法の仮定により, こうして得られた互換の積は偶数の互換の積である. 一方, 以上の互換の操作で互換の個数は変わらないか, あるいは 2 個減少する場合のみである. したがって, もとの互換の積に含まれる互換の個数は偶数である. 以上により帰納法で補題は示された.

次に, 互換の積に分解する表し方が複数存在する置換 a を考える. p 個の互換の積と q 個の互換の積の場合, それぞれの表現を

$$a = (i_1\ i_2)\cdots(i_{2p-1}\ i_{2p}) \quad (\text{B } 14)$$

$$a = (i_1\ i_2)\cdots(i_{2q-1}\ i_{2q}) \quad (\text{B } 15)$$

とする. ここで, 式 (B 15) から,

$$a^{-1} = (i_{2q}\ i_{2q-1})\cdots(i_2\ i_1)$$

であるから,

$$e = a a^{-1} = (i_1 i_2) \cdots (i_{2p-1} i_{2p}) (i_{2q} i_{2q-1}) \cdots (i_2 i_1)$$

となる. 補題から, 右辺は互換の個数が偶数である. つまり, $p+q$ は偶数である. したがって, p と q は同時に偶数か, 同時に奇数のいずれかである. これから, 置換を互換に分解したときの互換の個数の偶奇性, すなわち, 置換の偶奇性は互換への分解の表し方によらず一定である (証明終).

B.4 交代群 A_n は $n \geq 5$ のとき単純群である

$n \geq 5$ のとき, N を A_n の単位元群 $\{e\}$ と異なる正規部分群とする. t を N の e とは異なる置換とする. 置換 t を N の元とする. t は A_n の元でもあるから偶置換であり, 偶数個の互換の積で表すことができるが, その表し方は必ずしも一意的でもなければすべての互換が他のどの互換とも独立とは必ずしもならない. 一方, 巡回置換の積で表せば, 必ず独立な積で表すことができる. ここでは, この後の展開で独立という条件が必要となることから, t を独立な巡回置換の積で表すことにする.

任意の置換は独立な巡回置換の積で表したときに次の 4 つの型に分類される. したがって, t は必ず次の 4 つの形式のいずれか 1 つに該当する.

- (1) 長さ 4 以上の巡回置換を含む

$$t = (i_0 i_1 i_2 i_3 \cdots)(\cdots) \cdots$$

- (2) 長さ 3 の巡回置換を含む

$$t = (i_0 i_1 i_2)(i_3 i_4 \cdots)(\cdots) \cdots$$

- (3) 長さ 3 の巡回置換である

$$t = (i_0 i_1 i_2)$$

- (4) 独立な互換の積である

$$t = (i_0 i_1)(i_2 i_3)(\cdots) \cdots$$

この t に次に示す任意の偶置換 r を用いて $s = rtr^{-1}t^{-1}$ のような変形操作を施す.

$$r = (i_1 i_2 i_3)$$

実際, r は, $r = (i_1 i_2 i_3) = (i_1 i_2)(i_1 i_3)$ のように偶数個の互換の積に分解できるから, 偶置換であり, A_n の元である. N は A_n の正規部分群であるから, rtr^{-1} も N の元である. t^{-1} も N の元であるから, $s = rtr^{-1}t^{-1}$ は N の元である.

以下の表は s の計算の過程を表したものである. $s = rtr^{-1}t^{-1}$ の計算では, 右端の t^{-1} から順に $i_0, i_1, i_2, \dots$ に作用させる. 最初の結果は第 1 段に示され, それに対して, 次は r^{-1} を作用させる. 次の演算以下も同様に表した. t の巡回置換の積の中で, r と独立な巡回置換は s の中の t^{-1} で相殺されるから s の中には現れない. そのため, 以下の計算では陽に示していない.

- (1) の形式の場合

t は i_0 から始まる長さ 4 以上の巡回置換である. 最後の i_α, i_5, i_6 は途中の計算の便宜上使用したが, 計算が終われば, 結果に変化がないので消える.

		i_0	i_1	i_2	i_3	i_4	$\cdots$	i_5	i_6
t^{-1}	$=$	$(i_6 i_5 i_\alpha \cdots i_4 i_3 i_2 i_1 i_0)$							
r^{-1}	$=$	$(i_3 i_2 i_1)$							
t	$=$	$(i_0 i_1 i_2 i_3 i_4 \cdots i_\alpha i_5 i_6)$							
r	$=$	$(i_1 i_2 i_3)$							

		i_0	i_1	i_2	i_3	i_4	$\cdots$	i_5	i_6
t^{-1}	$=$	i_6	i_0	i_1	i_2	i_3	$\cdots$	i_α	i_5
$r^{-1} t^{-1}$	$=$			i_3	i_1	i_2	$\cdots$		
$t r^{-1} t^{-1}$	$=$	i_0	i_1	i_4	i_2	i_3	$\cdots$	i_5	i_6
$r t r^{-1} t^{-1}$	$=$		i_2		i_3	i_1	$\cdots$		

結局、変化する数は i_1, i_2, i_4 の 3 個であり、巡回置換で表すと

$$s = (i_1 i_2 i_4)$$

となる.

(2) の形式の場合

(1) の場合と同じく、 t の最後の i_α, i_6, i_7 は途中計算の便宜上用いただけで、結果には現れない.

			i_0	i_1	i_2	i_3	i_4	i_5	$\cdots$	i_6	i_7
t^{-1}	$(i_7 i_6 i_\alpha \cdots i_5 i_4 i_3)(i_2 i_1 i_0)$	t^{-1}	i_2	i_0	i_1	i_7	i_3	i_4	$\cdots$	i_α	i_6
r^{-1}	$(i_3 i_2 i_1)$	$r^{-1} t^{-1}$	i_1		i_3		i_2		$\cdots$		
t	$(i_0 i_1 i_2)(i_3 i_4 i_5 \cdots i_\alpha i_6 i_7)$	$t r^{-1} t^{-1}$	i_2	i_1	i_4	i_3	i_0	i_5	$\cdots$	i_6	i_7
r	$(i_1 i_2 i_3)$	$r t r^{-1} t^{-1}$	i_3	i_2		i_1			$\cdots$		

変化する数は i_0 から i_4 のまで 5 個であり、巡回置換で表すと

$$s = (i_0 i_3 i_1 i_2 i_4)$$

となる.

(3) の形式の場合

この場合は単一の長さが 3 の巡回置換である.

			i_0	i_1	i_2	i_3
t^{-1}	$(i_2 i_1 i_0)$	t^{-1}	i_2	i_0	i_1	
r^{-1}	$(i_3 i_2 i_1)$	$r^{-1} t^{-1}$	i_1		i_3	i_2
t	$(i_0 i_1 i_2)$	$t r^{-1} t^{-1}$	i_2	i_1		i_0
r	$(i_1 i_2 i_3)$	$r t r^{-1} t^{-1}$	i_3	i_2	i_1	

i_0 から i_3 まですべてが変化する. 巡回置換で表すと

$$s = (i_0 i_3)(i_1 i_2)$$

となる.

(4) の形式の場合

2 個の互換の積が複数組合まれる巡回置換の積である. r と独立でない互換の積は最初の 2 組であるが、それ以外の場合を $(i_l i_m)$ で明示的に表し、最後の結果には現れないことを示した.

			i_0	i_1	i_2	i_3	$\cdots$	i_l	i_m	$\cdots$
t^{-1}	$\cdots (i_m i_l) \cdots (i_3 i_2)(i_1 i_0)$	t^{-1}	i_1	i_0	i_3	i_2	$\cdots$	i_m	i_l	$\cdots$
r^{-1}	$(i_3 i_2 i_1)$	$r^{-1} t^{-1}$	i_3		i_2	i_1	$\cdots$			$\cdots$
t	$(i_0 i_1)(i_2 i_3) \cdots (i_l i_m) \cdots$	$t r^{-1} t^{-1}$	i_2	i_1	i_3	i_0	$\cdots$	i_l	i_m	$\cdots$
r	$(i_1 i_2 i_3)$	$r t r^{-1} t^{-1}$	i_3	i_2	i_1		$\cdots$			$\cdots$

i_0 から i_3 までが変化する. 巡回置換で表すと

$$s = (i_0 i_3)(i_1 i_2)$$

となる.

以上, A_n の正規部分群 N の元 t が, 必ずそのうちの 1 つは属する 4 つの形式の場合について, 巡回置換の演算により置換 t を, t が N の中に留まる範囲において, 置換 s に変形した. その結果,

(1) の形式の場合, t が $(i_0 i_1 i_3)$ に変わった. これは (3) の形式と同じである.

(2) の形式の場合, t は $(i_0 i_3 i_1 i_2 i_4)$ に変化した. これは長さが 5 の (1) の形式に相当する. したがって, これに同じ巡回置換の演算操作を施すと, $(i_0 i_3 i_2)$ という長さ 3 の巡回置換になり, (3) の形式と同じである.

(3) の形式の場合, 独立な 1 対の 2 つの互換の積 $(i_0 i_3)(i_1 i_2)$ になった.

(4) の形式の場合, この場合も, 独立な 1 対の 2 つの互換の積 $(i_0 i_3)(i_1 i_2)$ になった.

上の計算において, (1) の形式および (2) の形式の場合には, 巡回置換の積という変形によって t は (3) の形式に変換できることが示されたが, (3) の形式は独立な 1 対の 2 つの互換の積 $(i_0 i_3)(i_1 i_2)$ になることが示されているので, 結局, (1) から (4) のすべての場合において,

$$s = (i_0 i_3)(i_1 i_2)$$

の形の独立な互換対の積に変換されることがわかった. 以上長々と説明したが, 結局示されたのは次のことである. N の中には必ず $(i_0 i_3)(i_1 i_2)$ という形の独立な 1 対の 2 つの互換の積が含まれる.

次は, 1 対の任意の独立な 2 つの互換の積が N に含まれることを示す. そのため, この 2 つの互換の積を, 一般的に $(j_1 j_2)(j_3 j_4)$ と表す. j_1, j_2, j_3, j_4 はすべて互いに異なる. ここで, 次のような一つの S_n の一般的な置換を考える.

$$a = \begin{pmatrix} j_1 & j_2 & j_3 & j_4 & \cdots \\ k_1 & k_2 & k_3 & k_4 & \cdots \end{pmatrix}$$

a は置換であるから, 上段の数の組は下段の数の組と同じで, それぞれの組の数に重複はない. a の偶奇性はこの段階では決まっていない. また, 逆元 a^{-1} は,

$$a^{-1} = \begin{pmatrix} k_1 & k_2 & k_3 & k_4 & \cdots \\ j_1 & j_2 & j_3 & j_4 & \cdots \end{pmatrix}$$

となる.

以上の a と a^{-1} を用いると,

$$a(j_1 j_2)(j_3 j_4)a^{-1}s = (k_1 k_2)(k_3 k_4) \quad (\text{B } 16)$$

という関係式が成り立つ. 実際, これを示すために, 数の列 $j_1 j_2 j_3 j_4 \cdots k_1 k_2 k_3 k_4 \cdots l_1 l_2 l_3 l_4$ を考えて左辺の演算を右側から一つずつ施そう. 数の列 $l_1 l_2 l_3 l_4$ は計算の便宜上示しただけであって, 結果には現れない. そうすると,

$$\begin{array}{cccccccccccccccccccc} & & & & & & j_1 & j_2 & j_3 & j_4 & \cdots & k_1 & k_2 & k_3 & k_4 & \cdots & l_1 & l_2 & l_3 & l_4 & \cdots \\ a^{-1} & & & & & & l_1 & l_2 & l_3 & l_4 & \cdots & j_1 & j_2 & j_3 & j_4 & \cdots & k_1 & k_2 & k_3 & k_4 & \cdots \\ (j_1 j_2)(j_3 j_4) & a^{-1} & & & & & \cdots & j_2 & j_1 & j_4 & j_3 & \cdots & & & & & & & & & & \cdots \\ a & (j_1 j_2)(j_3 j_4)a^{-1} & & & & & j_1 & j_2 & j_3 & j_4 & \cdots & k_2 & k_1 & k_4 & k_3 & \cdots & l_1 & l_2 & l_3 & l_4 & \cdots \end{array}$$

となり, 上の関係式になることがわかる.

この置換 a は偶置換か奇置換かは明らかではないので, もう一つの置換 b を次のようにおく.

$$b = a(j_1 j_2)$$

これにより, b の互換の個数は a より 1 個多くなるので, a と b の偶奇性は反対になる. このとき, 式 (B 16)

を用いて,

$$\begin{aligned} b(j_1 j_2)(j_3 j_4)b^{-1} &= a(j_1 j_2)(j_1 j_2)(j_3 j_4)(j_1 j_2)a^{-1} \\ &= a(j_3 j_4)(j_1 j_2)a^{-1} = a(j_1 j_2)(j_3 j_4)a^{-1} \\ &= (k_1 k_2)(k_3 k_4) \end{aligned}$$

となる. すなわち,

$$b(j_1 j_2)(j_3 j_4)b^{-1} = (k_1 k_2)(k_3 k_4) \quad (\text{B } 17)$$

である. これから, もし a が奇置換なら b が偶置換になるので, a または b は必ずどちらかが偶置換になり, 同じ結果を得ることができる. そこで, この a と b どちらかの偶置換を c とおくと, c は A_n の元であり, 式 (B 16), (B 17) より,

$$c(j_1 j_2)(j_3 j_4)c^{-1} = (k_1 k_2)(k_3 k_4) \quad (\text{B } 18)$$

となる. すなわち, 独立な 2 個の互換の積の乗算は適当な偶置換の置換を用いればもう一つの独立な 2 個の互換の積となり, 両方とも正規部分群 N に含まれるということである. より具体的に言えば, 任意の $(k_1 k_2)(k_3 k_4)$ という独立な 2 個の互換の積は a または b という S_n の置換を用いれば N の中に含まれることを示すことができるのである. このことは, N には独立な 2 個の互換の積で表される置換はすべて含まれることを意味する. さらに, このような複数の独立な 2 個の互換の積からなる積はすべて N に含まれるから, すべての独立な偶数個の互換の積は N に含まれる.

次に, 独立でない 2 個の互換の積である置換について考えてみよう. このような互換の積は $(j_1 j_2)(j_1 j_3)$ と表される. $n \geq 5$ であるから, $j_1, j_2, j_1 j_3$ と異なる n 以下の数は少なくとも 2 個存在する. これを l_1 および l_2 とする. そうすると, 2 つの置換 $(j_1 j_2)(l_1 l_2)$ と $(l_1 l_2)(j_1 j_3)$ は 2 つの互換の積であるから, 上で証明したように, それぞれ N に属し, したがって, その積も N に属する. 一方,

$$(j_1 j_2)(l_1 l_2)c(l_1 l_2)(j_1 j_3) = (j_1 j_2)(j_1 j_3)$$

となる. 左辺は N に属するから, 右辺の $(j_1 j_2)(j_1 j_3)$ も N に属する. このことは, 独立でない 2 個の互換の積も N に属する. したがって, 任意の偶数個の互換の積は N に属する. すなわち, すべての偶置換は N に属する. ゆえに, N は A_n に等しい (証明終).

C 交代群 A_2, A_3, A_4 の構造

本節では, $n \leq 4$ の対称群 A_n は可解群であることを述べる.

C.1 S_2 の部分群構造

対称群 S_2 の交代群 A_2 は恒等置換 e である. 剰余群 S_2/e は C_2 と同型の巡回群である. したがって, S_2 は可解群である.

C.2 交代群 A_3 の部分群構造

対称群 S_3 は 1, 2, 3 の順列の間の置換であり, 位数は $3!$ である. その元は, 巡回置換で表すと, $e, (1\ 2), (2\ 3), (3\ 1), (1\ 2\ 3), (1\ 3\ 2)$ である. 交代群は, 偶置換であるから, $e, (1\ 2\ 3), (1\ 3\ 2)$ の 3 個の置換からなる. 位数が素数の乗法群は巡回群であるから, この交代群は巡回群である. 実際, $(1\ 2\ 3)(1\ 2\ 3) = (1\ 3\ 2), (1\ 3\ 2)(1\ 2\ 3) = e$ が成り立ち, $(1\ 2\ 3)$ は生成元である. $(1\ 3\ 2)$ も同様に生成元になる.

A_3 は S_3 の正規部分群であるから、正規部分群列

$$S_3 \supset A_3 \supset e$$

が存在し、その隣り合う部分群間の剰余群は巡回群である。したがって、 S_3 は可解群である。

C.3 交代群 A_4 の部分群構造

対称群 S_4 は $1, 2, 3, 4$ の順列の間の置換であり、位数は $4!$ である。交代群 A_4 の位数は $4!/2 = 12$ である。その元は、独立な 2 つの互換の積と長さ 3 の巡回置換である。なお、独立でない 2 つの互換の積は長さ 3 の巡回置換になる。 A_4 の e 以外の元を以下に示す。

$$t_1 = (1\ 2)(3\ 4), \quad t_2 = (1\ 3)(2\ 4), \quad t_3 = (1\ 4)(2\ 3) \quad (\text{C } 1)$$

$$s_1 = (1\ 2\ 3), \quad s_2 = (1\ 2\ 4), \quad s_3 = (1\ 3\ 2), \quad s_4 = (1\ 3\ 4), \quad (\text{C } 2)$$

$$s_5 = (1\ 4\ 2), \quad s_6 = (1\ 4\ 3), \quad s_7 = (2\ 3\ 4), \quad s_8 = (2\ 4\ 3), \quad (\text{C } 3)$$

以上の 12 個の元の中で e, t_1, t_2, t_3 は群を形成する。実際、まず、

$$t_1^2 = t_2^2 = t_3^2 = e$$

が成り立つ。

t_1, t_2, t_3 の間の積も以下のようにしてわかる。実際に、数の列 $1, \dots, 4$ に対し、以下の表のように、積 $t_i t_j$ を右側の t_j を数に作用させ、その結果を第 1 段に、さらに t_i を作用させた結果を第 2 段に示した。これを最初の数と比較すると、その下に示すような置換に対応するので、その結果、積 $t_i t_j$ の演算結果がわかる。

$\begin{array}{c} \begin{array}{cccc} & 1 & 2 & 3 & 4 \\ \hline t_1 & 2 & 1 & 4 & 3 \end{array} \\ t_2 t_1 \quad \begin{array}{cccc} & 4 & 3 & 2 & 1 \end{array} \\ t_2 t_1 = (1\ 4)(2\ 3) = t_3 \end{array}$	$\begin{array}{c} \begin{array}{cccc} & 1 & 2 & 3 & 4 \\ \hline t_1 & 2 & 1 & 4 & 3 \end{array} \\ t_3 t_1 \quad \begin{array}{cccc} & 3 & 4 & 1 & 2 \end{array} \\ t_3 t_1 = (1\ 3)(2\ 4) = t_2 \end{array}$	$\begin{array}{c} \begin{array}{cccc} & 1 & 2 & 3 & 4 \\ \hline t_2 & 3 & 4 & 1 & 2 \end{array} \\ t_3 t_2 \quad \begin{array}{cccc} & 2 & 1 & 4 & 3 \end{array} \\ t_3 t_2 = (1\ 2)(3\ 4) = t_1 \end{array}$
$\begin{array}{c} \begin{array}{cccc} & 1 & 2 & 3 & 4 \\ \hline t_2 & 3 & 4 & 1 & 2 \end{array} \\ t_1 t_2 \quad \begin{array}{cccc} & 4 & 3 & 2 & 1 \end{array} \\ t_1 t_2 = (1\ 4)(2\ 3) = t_3 \end{array}$	$\begin{array}{c} \begin{array}{cccc} & 1 & 2 & 3 & 4 \\ \hline t_3 & 4 & 3 & 2 & 1 \end{array} \\ t_1 t_3 \quad \begin{array}{cccc} & 3 & 4 & 1 & 2 \end{array} \\ t_1 t_3 = (1\ 3)(2\ 4) = t_2 \end{array}$	$\begin{array}{c} \begin{array}{cccc} & 1 & 2 & 3 & 4 \\ \hline t_3 & 4 & 3 & 2 & 1 \end{array} \\ t_2 t_3 \quad \begin{array}{cccc} & 2 & 1 & 4 & 3 \end{array} \\ t_2 t_3 = (1\ 2)(3\ 4) = t_1 \end{array}$

以上の結果をまとめると、

$$t_2 t_1 = t_1 t_2 = t_3, \quad t_3 t_1 = t_1 t_3 = t_2, \quad t_3 t_2 = t_2 t_3 = t_1 \quad (\text{C } 4)$$

となる。この結果から、 t_1, t_2, t_3 の間の演算は可換であることがわかる。以上のようにして、 e, t_1, t_2, t_3 は群を構成する。この群は一般にクラインの 4 元群とよばれる。ここでは B_4 と表す。元の間の演算上の結果からわかるように可換である。したがって、 B_4 はアーベル群である。

さらに、この群は正規部分群である。実際、次のような計算から明らかになる。これを示すためには、 $s_i t_j s^{-1}$ を計算してそれが e, t_1, t_2, t_3 のいずれかであることを示せばよい。その準備として、式 (C 2), (C 3) から得られるところの次の逆元の関係式が必要である。

$$s_1 = s_3^{-1} \quad s_2 = s_5^{-1}, \quad s_4 = s_6^{-1} \quad s_7 = s_8^{-1} \quad (\text{C } 5)$$

さらに、以下の計算から得られる $s_i s_j = s_k$ の形の関係式が必要である.

$$\begin{array}{ccc}
& \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\
s_1 & \begin{array}{ccc} 2 & 3 & 1 \end{array} \\
s_4 & \begin{array}{ccc} & 4 & 3 & 1 \end{array} \\
s_4 s_1 & = (1\ 2\ 4) = s_2
\end{array}
\qquad
\begin{array}{ccc}
& \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\
s_2 & \begin{array}{ccc} 2 & 4 & & 1 \end{array} \\
s_7 & \begin{array}{ccc} 3 & 2 & 4 \end{array} \\
s_7 s_2 & = (1\ 3\ 4) = s_4
\end{array}$$

すなわち、次の関係式が得られる.

$$s_4 s_1 = s_2 \qquad s_7 s_2 = s_4 \qquad (C\ 6)$$

最初に、 $s_1 t_i s_1^{-1} (i = 1, 2, 3)$, および $s_2 t_i s_2^{-1} (i = 1, 2, 3)$ を計算する. 計算の表の見方は上で述べたのと同じである.

$$\begin{array}{ccc}
\begin{array}{ccc} & \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ s_1^{-1} & \begin{array}{ccc} 3 & 1 & 2 \end{array} \\ t_1 s_1^{-1} & \begin{array}{ccc} 4 & 2 & 1 & 3 \end{array} \\ s_1 t_1 s_1^{-1} & \begin{array}{ccc} & 3 & 2 & 1 \end{array} \\ s_1 t_1 s_1^{-1} & = (1\ 4)(2\ 3) = t_3 \end{array}
&
\begin{array}{ccc} & \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ s_1^{-1} & \begin{array}{ccc} 3 & 1 & 2 \end{array} \\ t_2 s_1^{-1} & \begin{array}{ccc} 1 & 3 & 4 & 2 \end{array} \\ s_1 t_2 s_1^{-1} & \begin{array}{ccc} 2 & 1 & & 3 \end{array} \\ s_1 t_2 s_1^{-1} & = (1\ 2)(3\ 4) = t_1 \end{array}
&
\begin{array}{ccc} & \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ s_1^{-1} & \begin{array}{ccc} 3 & 1 & 2 \end{array} \\ t_3 s_1^{-1} & \begin{array}{ccc} 2 & 4 & 3 & 1 \end{array} \\ s_1 t_3 s_1^{-1} & \begin{array}{ccc} 3 & & 1 & 2 \end{array} \\ s_1 t_3 s_1^{-1} & = (1\ 3)(2\ 4) = t_2 \end{array} \\
\\
\begin{array}{ccc} & \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ s_2^{-1} & \begin{array}{ccc} 4 & 1 & & 2 \end{array} \\ t_1 s_2^{-1} & \begin{array}{ccc} 3 & 2 & 4 & 1 \end{array} \\ s_2 t_1 s_2^{-1} & \begin{array}{ccc} & 4 & 1 & 2 \end{array} \\ s_2 t_1 s_2^{-1} & = (1\ 3)(2\ 4) = t_2 \end{array}
&
\begin{array}{ccc} & \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ s_2^{-1} & \begin{array}{ccc} 4 & 1 & & 2 \end{array} \\ t_2 s_2^{-1} & \begin{array}{ccc} 2 & 3 & 1 & 4 \end{array} \\ s_2 t_2 s_2^{-1} & \begin{array}{ccc} 4 & & 2 & 1 \end{array} \\ s_2 t_2 s_2^{-1} & = (1\ 4)(2\ 4) = t_3 \end{array}
&
\begin{array}{ccc} & \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ s_2^{-1} & \begin{array}{ccc} 4 & 1 & & 2 \end{array} \\ t_3 s_2^{-1} & \begin{array}{ccc} 1 & 4 & 2 & 3 \end{array} \\ s_2 t_3 s_2^{-1} & \begin{array}{ccc} 2 & 1 & 4 \end{array} \\ s_2 t_3 s_2^{-1} & = (1\ 2)(3\ 4) = t_1 \end{array}
\end{array}$$

これをまとめると,

$$s_1 t_1 s_1^{-1} = t_3 \qquad s_1 t_2 s_1^{-1} = t_1 \qquad s_1 t_3 s_1^{-1} = t_2 \qquad (C\ 7)$$

$$s_2 t_1 s_2^{-1} = t_2 \qquad s_2 t_2 s_2^{-1} = t_3 \qquad s_2 t_3 s_2^{-1} = t_1 \qquad (C\ 8)$$

となる.

以上の結果をもとに、式 (C 7) の s_1 に式 (C 5) の $s_1 = s_3^{-1}$ を代入すると、 $s_3^{-1} t_1 s_3 = t_3$ となるが、この式に左から s_3 を掛け、右から s_3^{-1} を掛けると $t_1 = s_3 t_3 s_3^{-1}$ となる. これを、その他の関係式についても同様にすると、以下の関係式が得られる.

$$s_3 t_1 s_3^{-1} = t_2 \qquad s_3 t_2 s_3^{-1} = t_3 \qquad s_3 t_3 s_3^{-1} = t_1 \qquad (C\ 9)$$

式 (C 8) の s_2 についても、式 (C 5) の $s_2 = s_5^{-1}$ を代入すると同様の計算の後で次の関係式が得られる.

$$s_5 t_1 s_5^{-1} = t_3 \qquad s_5 t_2 s_5^{-1} = t_1 \qquad s_5 t_3 s_5^{-1} = t_2 \qquad (C\ 10)$$

次に、式 (C 7) の式に左から s_4 を掛け右から s_4^{-1} を掛けると、 $(s_4 s_1) t_1 (s_4 s_1)^{-1} = s_4 t_1 s_4^{-1}$ となる. これに式 (C 6) の $s_4 s_1 = s_2$ を代入すると、 $s_2 t_1 s_2^{-1} = s_4 t_1 (s_4 s_1)^{-1}$ となるが、左辺は式 (C 8) で t_2 と与えられているから、 $t_2 = s_4 t_1 (s_4 s_1)^{-1}$ という関係式が得られる. 他の関係式についても同様に展開することができて、以下の関係式が得られる.

$$s_4 t_1 s_4^{-1} = t_3 \qquad s_4 t_2 s_4^{-1} = t_1 \qquad s_4 t_3 s_4^{-1} = t_2 \qquad (C\ 11)$$

次は、式 (C 5) の $s_4 = s_6^{-1}$ を用いて、式 (C 9) を得たときと同じ方法で、次の関係式を得ることができる.

$$s_6 t_1 s_6^{-1} = t_2 \qquad s_6 t_2 s_6^{-1} = t_3 \qquad s_6 t_3 s_6^{-1} = t_1 \qquad (C\ 12)$$

次に、式 (C 6) の $s_7 s_2 = s_4$ を用いて、式 (C 11) を得たときの方法を用いる． $s_4 t_1 s_4^{-1} = s_7 t_1 s_7^{-1}$ という式が得られるが、この式の左辺に式 (C 11) の結果を代入すれば $t_3 = s_7 t_1 s_7^{-1}$ の関係式が得られる．まとめると、以下の式になる．

$$s_7 t_1 s_7^{-1} = t_2 \quad s_7 t_2 s_7^{-1} = t_3 \quad s_7 t_3 s_7^{-1} = t_1 \quad (\text{C } 13)$$

最後に、式 (C 5) の $s_7 = s_8^{-1}$ と式 (C 13) を用いて、式 (C 9) を得たときの方法を用いる．結果は以下の式である．

$$s_8 t_1 s_8^{-1} = t_3 \quad s_8 t_2 s_8^{-1} = t_1 \quad s_8 t_3 s_8^{-1} = t_2 \quad (\text{C } 14)$$

式 (C 7) から式 (C 14) はすべての $s_i t_j s_i^{-1}$ が t_k になること、つまり、群 B_4 の元になる．すなわち、群 B_4 は交代群 A_4 の正規部分群である． A_4 の正規部分群 B_4 に関する指数は $12/4 = 3$ であるから、剰余群 A_4/B_4 は位数 3 の巡回群である．

最後に、 $\{e, t_1\}$ も群を形成する．実際、明らかに 2 つの元は乗法に関して閉じており、逆元 $t_1^{-1} = t_1$ および単位元 e が存在する．この群を C_4 とする． C_4 には、互いに同型な群 $\{e, t_2\}$ および $\{e, t_3\}$ も存在するが、互いに包含関係がないので、ここでは C_4 のみを取り上げる． C_4 はアーベル群 B_4 の部分群であるから、可換であり、したがって、正規部分群である．その結果、次の正規部分群列が形成される．

$$S_4 \supset B_4 \supset C_4 \supset \{e\} \quad (\text{C } 15)$$

B_4 の位数は 4 で、 C_4 の位数は 2 であるから、剰余群 B_4/C_4 は巡回群である．これで、正規部分群列のすべての隣り合う部分群に関する剰余群は巡回群である．これにより、 S_4 は可解群であることがわかる．

したがって、 $n \leq 4$ の交代群 A_n は可解群である．

参考文献

- [1] エム・ポストニコフ 「ガロアの理論」 日野寛三訳 (東京図書, 1964).
- [2] エミール・アルティン 「ガロア理論入門」 寺田文行訳 (ちくま学芸文庫) (筑摩書房, 2010).
- [3] 彌永 昌吉 「ガロアの時代 ガロアの数学 第二部 数学篇」 (シュプリンガー数学クラブ) (シュプリンガー・フェアラーク, 2002).
- [4] 中島 匠一 「代数方程式とガロア理論」 (共立叢書現代数学の潮流,) (共立出版, 2006).
- [5] 雪江 明彦 「代数学 2 環と体とガロア理論 第 2 版」 (日本評論社, 2023).