本著の概要
（代数方程式の解法とガロア群）

代数方程式の解法にガロア群が如何に関わるかを知ることは興味深い。若年で決闘により 1832 年に死亡したフランスの数学者ガロアは，ラグランジュ，オイラー，ガウスやアーベルが築いた代数方程式の解法に関する理論を基に，代数方程式の根の置換から成るガロア群を考案・創出し，「代数方程式の累乗根で解ける条件に付いて」の理論を展開した。

本著では，ガロア理論を，ガロアが辿ったと考えられる時系列順に，ガロアの，死亡後の 1846 年に発刊された論文「代数方程式の累乗根で解ける条件に付いて」の内容に先輩著者等による証明等も参考・引用しながら，著者自身の研究の結果も付けて記述した。

ガロアが「有理式」と言っている用語は，今日我々が通常言っている「有理式」よりは意味が広く（汎く），現在で言う「方程式の全ての根の，１つの有理式」の外に，この有理式の，方程式の根の置換による作用後の式も「有理式」（正確には「有理的式」）と言っている。

ラグランジュによる，n 次代数方程式の根の表式は，n 個の代数方程式の根を，$(n-1)$ 個の，その原代数方程式の全ての根の 1 次式の線形和に換えている（これを本著では未知数変換ではなく，未知数転換と言っている）。

この未知数転換後の未知数の方程式に付いて解ければ，原方程式と未知数転換後の方程式との結合関係式が定まっている場合には，原方程式が解けることになる。その手順を本著では詳細に述べた。

また，代数方程式の根が形成されていく過程を，ガロア群の元の個数の減少と，全ての根から成る１つの有理式（従って根を構成する全ての有理式）が確定する体の拡張との対応を示しながら詳細に示した。

最後に本著のまとめを述べた。

Overview of this book
(Solutions of Algebraic Equations and Galois Group)

It is interesting to know how Galois group concerns solutions of algebraic equations. Galois, mathematician of France, who died tenderly by a duel in 1832, contrived and created Galois group consisting of the substitution of roots of an algebraic equation and developed the theory of "conditions under which algebraic equations can be solved using only rational functions and their roots", based on theories about solutions of algebraic equations that Lagrange, Euler, Gauss, Abel and others built and developed

Following the time series where Galois is thought to have pursed, this book describes Galois theory in the paper published in 1846 after Galois's death, using referring and quoting proofs of contents of papers by senior authors and others, and adding expressing results in a research by the author, himself.

The term of a "rational formula" which Galois said has wider meaning than a "rational formula" which we say today generally.

Galois says that it is, also, a formula after an operation by the substitution of roots of an equation (It is a "formula like the rationality" correctly.), in addition to a "rational formula of all roots of an equation" that we say at present.

By Lagrange Expression of the whole root of an algebraic equation, the whole root of an algebraic equation of n-th degree is converted to that of an algebraic equation of $(n-1)$-th degree, consisting of a linear summation of the 1st degree formulae of all roots of the algebraic equation (In this book, it is called to be not the unknown quantity transform but unknown quantity conversion.).

If the equation with unknown quantities after this unknown quantity conversion can be solved, then the first equation will be able to be solved, in the case where the combination formula between the first equation and that after an unknown quantity conversion will be decided.

This book describes the procedure in detail. The author also shows, in detail, the process in which the roots of an algebraic equation are formed, while showing the correspondence between the decrease of an original number of Galois group and the extension of the body whose rational forms of the roots are fixed.

Finally, this book describes the summary of this work.

目　次

（良く分るガロア群―真説ガロア群）

ラグランジュによる 2～4 次方程式の解法とガロア群

Lagrange type Solutions for Algebraic Equations of the 2nd to 4th Degree and Galois Group

１．緒言

代数方程式の解法にガロア群が如何に関わるかに付いて研究することは興味深い。ガロア群は，フランスの数学者ガロア（Evariste Galois, 1811-1832）が，1846 年にフランス語で公刊された論文「代数方程式が累乗根で解ける条件に付いて」[(1), (2)] の中で述べている，代数方程式の根に関する置換群のことである。

２．群・環・体等に付いて

２．１　集合

一般に使用される「集合」は，”ものの集まり”であり，それらは，有形，無形を問わず，同類のものであるか否かを問わず，雑多なものが混在していても良い場合が多いのであるが，数学で使用される「集合」は，数や，数から派生される関数やベクトル，行列，行列式，汎関数など諸々のものの，それぞれの集まりを指す。従って，数学における「集合」は，かなり限定的であり，程度の差はあるが，かなり同類的性質のものの集まりである。これを，数学では，**「集合」は“範囲を定められた（数学的な）ものの集まり”**と定義することがある。

「集合」を構成している要素（構成員）のそれぞれを，その集合の「**元**」と言う。集合の全体は英字の大文字で，集合の元は英字の小文字で表すのが普通である。

集合 A の元のいくつかを取り出した集合を B とするとき，集合 B を集合 A の**部分集合**と言う。

集合の元の個数が有限であるとき，その集合は**有限集合**と呼ばれ，元の個数が無限であるとき，その集合は**無限集合**と呼ばれる場合がある。部分集合についても同様である。

代数方程式とガロア群

２．２　群，環，体

「群」とは，「集合」の任意の２元に演算が，かつ任意の 3 元に結合演算が定義され，それらの演算の結果もその集合に属する（演算の結果である数や式も，その集合の元である）ような集合を指し，その集合は，その演算に対して「群」を成す，または，「群」であると言う。

具体的には，以下に示す内容になる。(3)

１）空でない集合 G に属する任意の２元 a, b に対し，a, b の積（product）と呼ばれる G の元 c が一意に定まり，この元 c を $c=ab$ と書くとき，この対応 $(a, b)\to ab$ を **G における乗法（multiplication）**と言う。

２）G が**群または乗法群**（multiplicative group）であるとは，次の２条件：

ｉ）乗法が G の任意の３元 a, b, c に対し，
結合法則（associative law） $a(bc)=(ab)c$ が成立する；

ii）G の任意の２元 a, b に対し，
$ax=b$ および，$ya=b$ となる G の元が一意に存在する；

を満足する「集合」を言う。上の条件 ii）は，

iii）単位元（unit element, neutral elemennt）の存在，すなわち，G の中に特別な元 e が存在して，G の任意の元 a に対して $ae=ea=a$ が成立する；

iv）逆元（inverse element）の存在，すなわち，G の元 a に対し，$ax=xa=e$ なる x（これを a^{-1} と書き，a の逆元と言う）が G の元の中に存在する；

と言う２条件 iii），iv）と同等である。このとき，$c=ab$ の逆元は $c^{-1}=b^{-1}a^{-1}$ である。

乗法に関する群の単位元は，通常，e または 1 で表す。$ab=ba$ であるとき，a と b は可換（commutative）であると言う。

G の任意の２元　a, b に対し，乗法の可換法則（commutative law） $ab=ba$ が成立することは一般には仮定しないが，$ab=ba$ が成立する群は，**可換群（commutative group）**または **アーベル（Niels Henrik Abel，1802~1829，ノルウェーの数学者）群**と言う。

（註１）群と言う概念は，アーベルが５次方程式の一般解法存在の有無を研究するために考案したものと言われている。アーベルは可換群のみを想定していたと考えられる。

（3）「岩波数学辞典　第２版」，岩波書店，1968，p.181 を参照のこと。

群・環・体

可換群の元の積は，しばしば，$a+b$ の形で書かれる。このときには，対応 $(a,\ b)\to a+b$ は加法（addition）と言い，$a+b$ を a と b との和（sum）と呼び，G を**加法群**または**加群（additive group, module）**と言う。

加法群の単位元を普通 0 で表し，a の逆元を $-a$ と書く(Abel 群，加群)。乗法，加法以外の記号が用いられることもある。それらを一般に**算法（law of composition）**または**演算**と言う。

通常の加法，乗法とは異なる算法のときには，加法または乗法の記号を用いる場合があり，加法の記号を用いるときには加群と言い，乗法の記号を用いるときには乗法群と言う場合がある。従って，乗法群，加法群と言うのは，形式上，便宜上の算法による呼び名であることもある。

「環」とは，次の条件：

ⅰ）「集合」の任意の２元 $a,\ b$ に集合の元 $a+b$ が定義され，**任意の２元 $a,\ b$ と任意の３元 $a,\ b,\ c$ に対して加法に関し可換群（これを単に加群と言う）であり，**

ⅰ） $a+b=b+a$ （交換則），

ⅱ） $(a+b)+c=a+(b+c)$ （結合則）

が成立し，　ⅲ） $a+x=b$ は，唯１つの（x の）解を「集合」の中に有する；

ⅱ）「集合」の任意の２元 $a,\ b$ に対し，集合の元 ab が定義され，**任意の３元 $a,\ b,\ c$ に対して乗法に関し，**

ⅳ） $(ab)c=a(bc)$ （結合則），

ⅴ） $a(b+c)=ab+ac,\quad (a+b)c=ab+ac$ （分配則）

が成立する；**演算に関し閉じている**（演算結果を示す数・式もその元である）**「集合」を言う。**

「体」とは，２つ以上の元を含む集合 A において，２種の算法（演算）〔加法および乗法〕が定義され，次の３つの公理 1），2），3）が成立するとき，集合 A を「体」と言う。すなわち，

加法に関し，

1）集合 A の任意の２元 $a,\ b$ に集合の元 $a+b$ が定義され，更に任意の３元 $a,\ b,\ c$ に，

ⅰ） $a+b=b+a$ （可換則），

ⅱ） $(a+b)+c=a+(b+c)$ （結合則）

が成立し，

ⅲ） $a+x=b$ を満足させる x が集合 A 内に一意的に存在する（すなわち，集合 A

が加法についてアーベル群を作る。その加群の単位元を 0 で表し，集合 A の零元（zero element, neutral element）と言う）；

乗法に関し，

2）集合 A の任意の2元 a, b に A の元 ab が定義され，更に任意の3元 a, b, c に，

iv） $ab = ba$ （可換則）

v） $(ab)c = a(bc)$ （結合則），

が成立し，

vi） $ax = b \ (a \neq 0)$ を満足する x が集合 A 内に存在し，従って，集合 A から 0 を除いた集合 B は，乗法についてアーベル群を作る（このとき，集合 B は集合 A の乗法群と言う。集合 B の単位元を 1 で表し，**集合 A の単位元**と言う）；

加法と乗法に関し，

3）集合 A の3元 a, b, c の間に，加法と乗法が定義され，

vii） $a(b+c) = ab + ac$ （分配則）

が成立する；**演算に関し閉じている「集合」**を言う。

言い換えると，“**「体」は「可換環」である**”と言える。上の「体」では，加法の iii）により**減法**が，また，乗法の vi）により**除法**が定義されて来るのである。

2．3　群・環・体等の細分

（I）群等の細分

i）集合 G の任意の3元 a, b, c に対し，

結合法則（associative law） $a(bc) = (ab)c$

を満足するとき，この集合を乗法に関する**半群**と言う。

ii）集合 G の任意の3元 a, b, c に対し，

結合法則（associative law） $a + (b + c) = (a + b) + c$

を満足するとき，この集合を加法に関する**半群**と言う。

iii）集合 G の任意の3元 a, b, c に対し，

イ）結合法則（associative law） $a(bc) = (ab)c$ を満足する，

ロ）単位元（unit element, neutral elemennt）の存在，すなわち，G の中に特別な元 e が存在して，G の任意の元 a に対して $ae = ea = a$ が成立する，

とき，この集合を乗法に関する**モノイド**と言う。

群・環・体

iv）集合 G の任意の３元 a, b, c に対し，

イ）結合法則（associative law） $a+(b+c)=(a+b)+c$ を満足する，

ロ）単位元（unit element, neutral elemennt）の存在，すなわち， G の中に特別な元 e が存在して，G の任意の元 a に対して $a+e=e+a=a$ が成立する，

とき，この集合を加法に関する**モノイド**と言う。

v）集合 G の任意の３元 a, b, c に対し，

イ）結合法則（associative law） $a(bc)=(ab)c$ を満足する，

ロ）単位元（unit element, neutral elemennt）の存在，すなわち， G の中に特別な元 e が存在して，G の任意の元 a に対して $ae=ea=a$ が成立する，

ハ） 逆元（inverse element）の存在，すなわち，G の元 a に対し，$ax=xa=e\ (=1)$ なる x（これを a^{-1} と書き，a の逆元と言う）が存在する，

とき，この集合を乗法に関する**群**と言う。

vi）集合 G の任意の３元 a, b, c に対し，

イ）結合法則（associative law） $a+(b+c)=(a+b)+c$ を満足する，

ロ）単位元（unit element, neutral elemennt）の存在，すなわち， G の中に特別な e が存在して，G の任意の元 a に対して $a+e=e+a=a$ が成立する，

ハ）逆元（inverse element）の存在，すなわち，G の元 a に対し，$a+x=x+a=e\ (=0)$ なる x（これを $-a$ と書き，a の逆元と言う）が存在する，

とき，この集合を加法に関する**群**と言う。

vii）半群である集合 G の任意の２元 a, b に対し，交換則 $ab=ba$ が成立する場合のものを乗法に関する**可換半群**と言い，交換則が成立しないものを乗法に関する**非可換半群**と言う。

viii）半群である集合 G の任意の２元 a, b に対し，交換則 $a+b=b+a$ が成立する場合のものを加法に関する**可換半群**と言い，交換則が成立しないものを加法に関する**非可換半群**と言う。

ix）モノイドである集合 G の任意の２元 a, b に対し，交換則 $ab=ba$ が成立する場合のものを乗法に関する**可換モノイド**と言い，交換則が成立しないものを乗法に関する**非可換モノイド**と言う。

x）半群である集合 G の任意の２元 a, b に対し，交換則 $a+b=b+a$ が成立する場合の