ガロア理論を理解しよう

Osamu MATSUDA

平成 30 年 11 月 16 日

ガロア理論とは，19 世紀始めのフランス人数学者エヴァリスト・ガロアの名前からきている．ガロア理論から得られる最もよく知られている定理は,「**一般の 5 次以上の方程式には解の公式が存在しない**」というものである．そして「不可能であることを証明する」ということ，これがガロア理論の醍醐味である．

2 次方程式 $ax^2 + bx + c = 0, (a \neq 0)$ の解の公式は，

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

である. これは古代バビロニアで得られたという．3 次，4 次の方程式の解の公式は，16 世紀のイタリアで, カルダノやフェラーリといった数学者達によって発見されたといわれている．そして，どんな 4 次以下の方程式も，方程式の係数どうしの四則演算と n 乗根[†] を用いて解くことができる．代数学では，方程式の係数どうしの四則演算と n 乗根を用いて解くことを**代数的に解く**という．だから 4 次以下の方程式は全て代数的に解けるのである．しかし 5 次以上の方程式となると，代数的に解けないものが存在する．これは，5 次以上の方程式には，代数的に解くための解の公式が存在しないということを意味する．この結論を証明するために，ガロアは方程式そのものを考えず，**方程式の背後に潜む群**という集合を考えていった．しかもガウスが示した「n 次の代数方程式は重複も込めてちょうど n 個の複素数解をもつ」という**代数学の基本定理を使わずに**証明にたどり着いた．この方法は，現代流に言えば,「対象となる数学の内在的性質を探る」という手法の先駆けであるように思える．ガロアは 20 歳のとき，決闘によってその人生を閉じた．これはまた驚くべきことでもある．つまりガロア理論は彼が十代の時に考えたものであるということだ.

[†] $X^n = a$ をみたす根 α のことを a の n 乗根という.

このノートではガロア理論のみを，特に最初に挙げた定理のみを扱う．そのために，必要ない代数学の知識は一切省いた．基本的に代数学の知識ゼロを出発点として，このノートだけで完全に証明を理解できるように努めた．このノート作成にあたり，特に [1],[2],[3] の中の命題，証明等を参考に構成した．

また，途中休憩として，エヴァリスト・ガロアに関する記事を，[5] を参照して入れた．[5] は詳細にガロアとその時代のことが書かれてあるもので，そちらを読まれると，ガロアの時代背景，人物とともに，より深くガロア理論を味うことができると思う．ぜひ手にとって読んで欲しい一冊である．

最後に，本研究室のホームページ上に掲載した「ガロア理論入門ノート」に対して，多くの読者から感謝された一方で，多くの間違いやご意見等も頂戴したことを付け加え，読者の方々にお礼を申し上げたい．そして，今回「ガロア理論入門ノート」を改めて見直し，不十分な点を追加し，より読みやすいものになることを心がけて，このノート「ガロア理論を理解しよう」を執筆した．まだまだ不十分な点があるかもしれないが，少しでも読者の方々の理解に貢献できればと願っている．

目 次

1　証明法，集合の写像に関する基礎知識

このノートを読み進めるために，基本的な証明法，および，集合の写像に関して，最小限の確認しておかなければならない基礎知識がある．それらを説明する．

1.1　証明法

証明法には，背理法と数学的帰納法がよく使われる．それらを以下に説明する．

(1)　背理法

命題「x が，$x \in A$ であるならば $x \in B$ である」を証明するとき,「$x \in A$ かつ $x \notin B$」と仮定して，この仮定に矛盾があることを導く証明法のことである．

（この証明法が正しい理由）　集合 A, B について，命題は $A \subset B$ を示している．これは，A の元は全て B の元であることを意味する．したがって，背理法の仮定「$x \in A$ かつ $x \notin B$」という x が存在することはない．このことから，背理法の仮定に矛盾があることを導けばよいことになる．

例　命題「自然数 a, b, c が $a^2 + b^2 = c^2$ を満たすならば，a, b, c の少なくとも 1 つは偶数である.」

(証明)　「$a^2 + b^2 = c^2$ であり，かつ a, b, c のどれも奇数である」ことを仮定する．a,b は奇数であるので，$a^2 + b^2$ は偶数である．さらに，c も奇数であるので c^2 も奇数である．これは，式 $a^2 + b^2 = c^2$ により，偶数と奇数が等しいことを意味して，偶数と奇数は一致しないという数の性質に矛盾する.（証明終）

(2)　数学的帰納法

命題「自然数 n に関して $P(n)$ が成り立つ」を証明するとき，以下の手順で示す証明法である．

ステップ 1．$n = 1$ のとき $P(1)$ が成り立つことを示す.

ステップ 2．$P(1)$ から $P(n-1)$ までは全て成り立つことを仮定して，$P(n)$ が成り立つことを示す.

（この証明法が正しい理由）　ステップ 1 と 2 がどちらも示されたとする．ステップ 1 から $P(1)$ は正しいので，ステップ 2 から $P(2)$ が正しいことがいえる．今，$P(2)$ が正しいとなったので，再び，ステップ 2 から

$P(3)$ が正しいことになる．さらに，ステップ 2 から $P(4)$ が正しいことになる．以後も同様にして，$P(5)$, $P(6)$, $\cdots$ が正しいことになる．

例 命題「自然数 n について，$P(n) = 1 + 3 + 5 + \cdots + (2n-1)$ とおくと，$P(n) = n^2$ である．」

(証明) ステップ 1．$n = 1$ のとき，$P(n) = 1$ であり $1^2 = 1$ であるので，命題は正しい．

ステップ 2．$P(n-1) = 1+3+5+\cdots+(2n-3) = (n-1)^2$ であることは正しいと仮定して，$P(n) = n^2$ となることを示す．$P(n) = P(n-1)+(2n-1)$ であり，帰納法の仮定より，$P(n) = (n-1)^2 + (2n-1)$ である．よって，

$$P(n) = n^2 - 2n + 1 + 2n - 1 = n^2$$

であり，$P(n) = n^2$ であることが示された．

ステップ 1 とステップ 2 によって，すべての自然数 n について命題は正しいことが示された．(証明終)

1.2 集合の写像

A と B を集合とし，写像 $f : A \to B$ を考える．写像には次のような種類がある．

(1) 任意の $b \in B$ に対して，$f(a) = b$ となる $a \in A$ が存在するとき，写像 f は**全射**であるという．

(2) 任意の $a_1, a_2 \in A$ について，$a_1 \neq a_2$ ならば $f(a_1) \neq f(a_2)$ であるとき，f は**単射**であるという．対偶をとれば，f が単射であることは，$f(a_1) = f(a_2)$ ならば $a_1 = a_2$ ということでもある．

(3) 写像 f が全射かつ単射であるとき，f は**全単射**，または **1 対 1 の対応**であるという．

(4) 任意の $a \in A$ に対して $f(a) = a$ となる f は，**包含写像**と呼ばれる．特に，$B = A$ のとき，f を**恒等写像**といい，特に id_A と書く．

(5) f が全単射であるとき，任意の $b \in B$ に対して $f(a) = b$ となる a を対応する写像を $f^{-1} : B \to A$ と書いて，f の**逆写像**という．

以下，写像 $f : A \to B$，$g : B \to A$ について，記号 $f \circ g$ を，$b \in B$ に対して，

$$(f \circ g)(b) = f(g(b))$$

を意味するものとする．f が全単射であることを示す必要があるときに，次の命題は有用である．

命題 1　写像 $f : A \to B$，$g : B \to A$ について，$f \circ g = id_B$ ならば f は全射で g は単射である．さらに，$f \circ g = id_B$ かつ $g \circ f = id_A$ ならば，f は全単射であり，g は f の逆写像となる．

証明　$f \circ g = id_A$ を仮定する．$b \in B$ に対して $a = g(b)$ とおくと，

$$f(a) = f(g(b)) = (f \circ g)(b) = b$$

である．よって，f は全射である．

次に，$b_1, b_2 \in B$ について，$g(b_1) = g(b_2)$ であるとすると，

$$b_1 = f(g(b_1)) = f(g(b_2)) = b_2$$

となる．よって，f は単射である．

さらに，$g \circ f = id_A$ ならば，同様にして，g は全射で f は単射であることがわかる．したがって，$f \circ g = id_B$ かつ $g \circ f = id_A$ ならば，f は全単射であり，g は f の逆写像となる．　（証明終）

⋆⋆⋆ エヴァリスト・ガロアについて 1

エヴァリスト・ガロアは，1811 年 10 月 25 日パリの郊外のブール・ラ・レーヌで生まれ，1832 年 5 月 31 日にパリで亡くなった．エヴァリストの父は，ニコラ・ガブリエル・ガロア，母はニコラより２０年下の，アデライード・マリー・ドマントである．二人は，ニコラ３０歳，アデライード１０歳のときに結婚した．エヴァリストには 2 つ上の姉と 3 つ下の弟がいて，姉はナタリー・デオール，弟はアルフレッドである．父，ニコラは寄宿学校を経営していた．当時のガロア家は,「厳粛であるとともに笑い声の耐えない」家族だった．1815 年地中海のエルバ島に流されていたナポレオンが，チュイルリー宮殿に帰還，そのときの政府によって，ニコラはブール・ラ・レーヌの町長に任命される．しかし，ヨーロッパ諸国の反仏連合軍により，１００日ほどの後，ナポレオンは英領セント・ヘレナ島に幽閉される．その後，いろいろな出来事があり，ニコラは 1829 年 7 月 2 日に自殺で亡くなる．エヴァリストが１７歳のときだった．　⋆⋆⋆

2　群に関するキーワード

ガロア理論全体が見渡せるために，以下では，群に関する基本的なキーワードを並べる．ここに並べられたキーワードが実感できれば，ガロア理論の中の群に関する理解が進んでいくはずである．

キーワード１： n 次方程式の基本対称式

（概説）2 次方程式 $x^2+ax+b=0$ の解を $\alpha_1,\ \alpha_2$ とおくと，

$$\alpha_1+\alpha_2=-a,\quad \alpha_1\alpha_2=b \tag{1}$$

という解と係数の関係式が成り立つ．注目する点は，解の表示に使われている番号 $1,2$ を入れ換えても (1) のそれぞれの右辺の値は同じである．以下，(1) を**基本対称式**呼ぶ．

3 次方程式 $x^3+ax^2+bx+c=0$ についても同様で，この解を $\alpha_1,\ \alpha_2,\ \alpha_3$ とおくと，この基本対称式は，

$$\alpha_1+\alpha_2+\alpha_3=-a,\ \ \alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_3\alpha_1=b,\ \ \alpha_1\alpha_2\alpha_3=-c \tag{2}$$

である．このとき，解の表示に使われている番号 $1,2,3$ をどのように入れ換えても，(2) のそれぞれの右辺の値は同じである．

以上のようなことは，n 次方程式 $x^n+a_1x+\cdots+a_n=0$ において，(1) や (2) を一般化した基本対称式でも成り立つ．

キーワード２： n 次対称群

（概説）n 次方程式の基本対称式は，解の表示に使われている番号 $1,2,\cdots,n$ を入れ換えても右辺の値は変化しないことであった．そこで，番号 $1,2,\cdots,n$ の集合を X とし，X の番号の入れ換える操作（**置換**という）を考える．置換の表記については，例えば，$X=\{1,2,3\}$ であるとき，1 を 3 に，2 を 1 に，3 を 2 に置換することを，

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

と表す．特に変化させない置換を**恒等置換**といい e で表す．n 個の数からなる集合 X の置換全体のことを n **次対称群**と呼び，S_n で表す．そして，n 次方程式の対称群 S_n が次数 n によってどのような違いがあるのかを研究する，これがガロア理論の群論における方針である．

ところで，S_n の元である置換 σ と τ を考え，$\tau \cdot \sigma$ という演算 $\cdot$ を，置換 σ を行った後に，置換 τ を行うものとする．S_n の中にはこのようにして演算を定義することができる．正確な定義は後で述べるが，S_n の中の演算と同様な演算が定義されている集合 G のことを**群**と呼んでいる．

キーワード３： 差積と n 次交代群

（概説）n 次対称群の中の特別な部分集合に n **次交代群** A_n と呼ばれるものがある．例えば，3 次方程式 $x^3 + ax^2 + bx + c = 0$ の解 α_1，α_2，α_3 に対して，

$$\Delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)$$

を考える．Δ は**差積**と呼ばれる．そして，Δ もまた

$$\Delta^2 = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

というタイプの解と係数の関係式を持つ．3 次対称群 S_3 の中で，Δ の値を変えない置換の集合のことを，3 次交代群 A_3 と呼んでいる．

2 次方程式 $x^2 + ax + b = 0$ の解 α_1，α_2 に対して，差積は $\Delta = \alpha_1 - \alpha_2$ であり，

$$\Delta^2 = a^2 - 4b$$

である．明らかに，$A_2 = \{e\}$ である．また，2 次方程式 $x^2 + ax + b = 0$ の解の公式

$$x = -a \pm \sqrt{a^2 - 4b} \tag{3}$$

であることから，差積 Δ は，解が重根を持つかどうかを判別するための**判別式**に対応している．実は，3 次方程式の差積 Δ も判別式に対応する．

さて，n 次交代群 A_n は，A_2 や A_3 を一般化したもので，n 次方程式の差積 Δ の値を変えない置換の集合である．そして，n 次交代群に関する重要な結果は，3 次交代群 A_3 は演算が可換であるが，4 次以上の交代群

A_n は演算が可換ではないという違いが現れることにある．演算が可換な群は**アーベル群**と呼ばれる．

キーワード４： 正規部分群と単純群

（概説）4 次以上の交代群 A_n に関して，解の公式が知られている 4 次方程式の交代群 A_4 と，$n \geq 5$ のときの n 次方程式の交代群 A_n にはどのような違いがあるのだろうか．その違いを与えるものが**正規部分群**と呼ばれる特別な群である．より正確に言えば，群 G の部分集合でかつ群である H（**部分群**と呼ばれる）が，正規部分群 H とは，任意の $x \in G$ に対して，$xH = Hx$ となるようなものである．

さて，$n \geq 4$ について A_n は S_n の正規部分群となっている．では，A_n の正規部分群についてはどうか．

G の正規部分群が $\{e\}$ と G しか存在しないような G は，**単純群**と呼ばれる．そして，A_4 については，$\{e\}$ と A_4 以外の，例えばクラインの四元数群といった正規部分群が存在する．しかし，$n \geq 5$ である A_n は単純群なのである．つまり，A_4 と $n \geq 5$ であるとき A_n の違いは，それが単純群か否かという形で現れてくる．これが最初のクライマックスである．

キーワード５： 商群と可解群

（概説）N が群 G の正規部分群のとき，任意の $x \in G$ に対して，xN というクラスを考えることができる．そして，xN と yN の間の演算を $(xN)(yN) = xyN$ と定めることで，クラスの集合 $\{xN\}$ は群となる．これを N による G の**商群**という．商群の定義によって，n 次方程式に内在していた**可解群**というものが現れてくる．そして，可解群こそが，n 次方程式に解の公式が存在するのかどうかという問題に深く関係する．一応，G が可解群であるという定義を述べておく．それは，$G \supset G_1 \supset \cdot \supset G_{r-1}, G_r = \{e\}$ というある正規部分群の列を考えたとき，$G/G_1, G_1/G_2, \cdots Gr - 1/G_r$ がすべてアーベル群となる G のことである．そして，A_n が単純群かどうかということを用いて，$n = 2, 3, 4$ のとき S_n は可解群であり，$n \geq 5$ のとき S_n は可解群ではない，ということが証明されるのである．

3　方程式と群

3.1　群の定義と対称群

ガロア理論では，n 次方程式がべき根を用いて表すことができるかどうかは，方程式の群と呼ばれるものの構造の違いにあると結論している．群の定義は以下である．

群の定義　集合 G の内部である演算 $\cdot$ が定義されいて，次の 3 つの条件を満たすとき集合 G は群であるという．

(1) G の任意の元 x, y, z に対し，$x \cdot (y \cdot z) = (x \cdot y) \cdot z$ （結合法則）が成立する．

(2) 任意の元 x に対して $x \cdot e = e \cdot x = x$ となる元 e が存在する．

(3) x に対して $x \cdot x' = x' \cdot x = e$ となる元 x' が存在する．

---

e を**単位元**，x' を元 x の**逆元**といい普通 x^{-1} と書く．ここで群 G には単位元が 1 つしかなく，G の任意の元 x に対して逆元 x^{-1} はただ 1 つしかないことを注意とする．なぜなら，仮に単位元が e と e' と 2 つあったとしよう．そうすると，定義 (2) より，$e = e \cdot e' = e'$ となるからである．また，逆元についても，y と z を x の逆元としたとき，定義 (1) と (3) より，$y = y \cdot (x \cdot y) = y \cdot e = y \cdot (x \cdot z) = (y \cdot x) \cdot z = e \cdot z = z$ となるからである．

定義　群 G の全ての元 x, y に対し，$x \cdot y = y \cdot x$ が成り立つとき，G を**アーベル群**という．G がアーベル群のとき，その演算を $+$ で表し**加法**と呼ぶことがある．この場合 G を**加法群**という．

ここで，アーベル群という呼び名は，**ニールス・アーベル**というノルウェーの数学者の名前に由来しており，5 次以上の n 次方程式には解の公式が存在しないことを証明した点においては，ガロアよりもアーベルの方が早かったとされている．しかしアーベルもまた早くこの世を去っており，その年齢は 26 歳で，病死であった．

例　(1) 整数全体の集合 $\mathbf{Z}$ は，足し算によってアーベル群となる．単位元は零である．

(2) 有理数全体の集合 $\mathbf{Q}$ から 0 を除いた集合 $\mathbf{Q}^*$ は掛け算でアーベル群となる．単位元は 1 である．

(3) 2 行 2 列の行列全体（これを $M(2)$ と書く）は足し算でアーベル群となる．単位元は零行列である．

(4) $M(2)$ の中で行列式が零にならない行列全体の集合（これを $GL(2)$ と書く）は積によって群となる．しかしアーベル群ではない．単位元は単位行列である．

キーワード 1 で与えた基本対称式 (1) においては，2 つの解 α_1 と α_2 を入れ換えても基本対称式の右辺の値は変化しないことをみた．ガロア理論では，解の置換という操作で作られる群を重要視する．

集合 X の元（数字）の入れ換えを行うことを**置換**という．X の置換全体は群になる．例えば 1 と 2 だけからなる集合 $X = \{1, 2\}$ を考える．この場合 X の置換は 2 種類ある．つまり 1 を 1 に，2 を 2 に入れ替えるものと（これを**恒等置換**といい，e で表す）もう一つは，1 を 2 に，2 を 1 に入れ替えるものである．1 を i に，2 を j に置換することを，

$$\begin{pmatrix} 1 & 2 \\ i & j \end{pmatrix}$$

と書くと，S_2 の元は,

$$e = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

となる．2 個の元からなる集合 X の置換全体を S_2 と書いて 2 次の**対称群**という．同様に 3 個の元からなる集合 $X = \{1, 2, 3\}$ の置換全体は S_3 と書いて 3 次の対称群という．3 次の対称群の位数は，3 個の文字の順列の個数であるので $3! = 6$ である．一般に n 個の元からなる集合の置換全体を S_n と書いて n 次の対称群という．n 個の文字の順列の個数は $n!$ だから S_n の位数は $n!$ である．

2 次の対称群 $S_2 = \{e,\ \sigma\}$ を考えよう．これは明らかにアーベル群であり，これが，2 次方程式の解が 2 乗根を用いて表されることに関係することが，次第に分かってくる．

3.2　3 次方程式に関する群

もう一度，3 次方程式

$$x^3 + ax^2 + bx + c = 0 \tag{4}$$

の基本対称式について考えよう．それは，(4) の解を $\alpha_1,\ \alpha_2,\ \alpha_3$ とおいたとき，

$$\alpha_1 + \alpha_2 + \alpha_3 = -a \tag{5}$$

$$\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = b \tag{6}$$

$$\alpha_1\alpha_2\alpha_3 = -c \tag{7}$$

というものであった．このとき，(4) の解 $\alpha_1,\ \alpha_2,\ \alpha_3$ の順をどのように入れ換えても基本対称式 (5) と (6) と (7) の右辺の値はどれも変化しない．したがって，対称群 S_3 について考えることは意味がある．

対称群 S_3 はどのような構造をもつのであろうか．

対称群 S_3 において 1 を 3 に，3 を 2 に，2 を 1 に置換するものがある．これを (132) と書く．このような 3 個の異なる数の置換を 3 次の**巡回置換**という．一般にある置換 σ が $\sigma = (i_1 i_2\ \cdots\ i_r)$ のように書けるとき，これを r 次の巡回置換という．特に 2 次の巡回置換を**互換**と呼ぶ．

では，S_3 の元は全部で $3! = 6$ だけしかないので，それを全部書き出してみよう．

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123),$$

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132), \quad \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (23),$$

$$\tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (13), \quad \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (12)$$

である．例えば $\sigma_1\tau_1 = (132) = \sigma_2$ で $\tau_1\sigma_1 = (13) = \tau_2$ で $\sigma_1\tau_1 \neq \tau_1\sigma_1$ なので S_3 はアーベル群ではない．ここで，内部算法の記号 $\cdot$ は省略した．以後もそのようにする．

S_3 の構造をより理解するために，互換に着目してみよう．明らかに互換は τ_1, τ_2, τ_3 だけである．しかし，これら以外は，$e = (12)(12)$, $\sigma_1 = (13)(12)$, $\sigma_2 = (12)(13)$ と書かれ，これらは互換の積となっている．

補題 2　任意の置換は互換の積に分解される．

証明　巡回置換 $(i_1 i_2 \ \cdots \ i_r)$ が $(i_1 i_r)(i_1 i_{r-1}) \cdots (i_1 i_3)(i_1 i_2)$ と等しくなることは明らかである．したがって，任意の置換 $\sigma \in S_n$ が巡回置換の積で書けることを示せばよい．適当な数字 i_1 を選び, $\sigma^r(i_1) = i_1$ となる最小の r をとり，$i_2 = \sigma(i_1), i_3 = \sigma(i_2), \cdots, i_r = \sigma(i_{r-1})$ とおく．このとき，σ は $\{i_1, \cdots, i_r\}$ 上では巡回置換 $(i_1 \cdots \quad i_r)$ に一致している．次に，$\{i_1, \cdots, i_r\}$ に含まれない数字 j_1 をとり，同様の手続きをとることにより，巡回置換 $(j_1 j_2 \cdots j_s)$ を得る．この操作を繰り返すことにより σ は巡回置換の積で表される．　（証明終）

定理 3　S_n の元 σ を互換の積で表したとき，互換の個数の偶奇は一定である．

証明　ある置換 σ が同時に偶数個の互換の積と奇数個の互換の積で表されたとすると，$\sigma e = \sigma$ より，恒等置換は奇数個の互換で表されることになる．しかし，恒等置換は奇数個の互換の積で表されないことを示そう．恒等置換の奇数個の互換の積で表す最小の奇数を k としておき，$e = (i_1 j_1)(i_2 j_2) \cdots (i_k j_k)$ とする．さて，2 個の互換 (ij)，(ab) の積は，次のように計算される．

$$(ij)(ab) = \begin{cases} (ab)(ij) & \{i,j\} \cap \{a,b\} = \emptyset \text{ の場合} \\ (jb)(ij) & \{i,j\} \cap \{a,b\} = \{i\} \text{ の場合（} a = i \text{ を仮定）} \\ (aj)(ia) & \{i,j\} \cap \{a,b\} = \{j\} \text{ の場合（} b = j \text{ を仮定）} \\ e & \{i,j\} = \{a,b\} \text{ の場合} \end{cases}$$

もし，$(i_1 j_1) = (i_2 j_2)$ なら $e = e(i_3 j_3) \cdots (i_k j_k)$ なので，$e = (i_3 j_3) \cdots (i_k j_k)$ となり，k の最小性に矛盾する．つまり，$(i_1 j_1) = (i_2 j_2)$ とはならない．したがって，$(i_1 j_1)$ と $(i_2 j_2)$ との積 $(i_1 j_1)(i_2 j_2)$ は，$(i_1 j_1)(i_2 j_2) = (**)(i_1 *)$ というように，i_1 が右側の互換のみに含まれるようにおき換えられる．同

様に考えて，$(i_1*)(i_3j_3) = (**)(i_1*)$ というように，i_1 が右側の互換のみに含まれるようにおき換えられる．この操作を繰り返すことにより，最終的には i_1 が一番右の互換にのみ現れるようにできる．これは i_1 が決して i_1 に変換されないことを意味する．つまり，$e \neq (i_1j_1)(i_2j_2)\cdots(i_kj_k)$ である．（証明終）

定理 3 により任意の置換は偶数個の互換の積か奇数個の互換の積に表されることがわかった．偶数個の互換の積で表される置換を**偶置換**，奇数個の互換の積で表される置換を**奇置換**という．S_n の偶置換全体の集合を A_n で表す．偶置換と偶置換の積は当然偶置換である．$\sigma = (ij)$ に対して $\sigma^{-1} = (ij)$ なので，偶置換の逆置換はまた偶置換である．

以下に，与えられた群の構造を理解するための，基本となるいくつかの定義と，定理に関して説明する．

定義　群 G が有限個の元をもつとき，G は**有限群**であるといい，元の個数を $|G|$ と書き G の**位数**という．

定義　群 G 部分集合 H が，G の算法によって群となるとき，H は G の**部分群**であるという．

定理 4　G を群とし，$H \subset G$ とする．H が次の (1) ∼ (2) をみたすならば H は G の部分群である．

(0) H は空集合ではない．

(1) $x, y \in H \Rightarrow xy \in H$.

(2) $x \in H \Rightarrow x^{-1} \in H$.

証明 (1) より結合法則に関しては良い．(2) より $x \in H$ ならば $x^{-1} \in H$. よって，$e = xx^{-1} = x^{-1}x \in H$ がいえる．逆元に関しては (2) より明らかである．（証明終）

以上の定義から，偶置換全体の集合 A_n は S_n の部分群であることがわかった．A_n を n 次の**交代群**という．

定義　S を G の部分集合とする．S を含む最小の部分群 H を，S によって**生成された**部分群といい $\langle S \rangle$ と書く．S が有限集合 $S = \{a_1, a_2, \cdots, a_n\}$ であるとき，$\langle a_1, a_2, \cdots, a_n \rangle$ と書き，群 H は**有限生成**であるという．群 G が 1 つの元から生成されているとき，すなわち

$$G = \{a^n \mid n = 0,\ \pm 1,\ \pm 2,\ \cdots\}$$

であるとき，G は a **で生成される巡回群**（簡単に**巡回群**）であるといい $\langle a \rangle$ と書く．巡回群はアーベル群である．G が有限群でかつ巡回群であるとき，**有限巡回群**という．

例　(1) 整数全体の集合 $\mathbf{Z}$ は，足し算によってアーベル群でもあり，1 で生成される巡回群でもある．単位元は 0 である．しかし掛け算では，群にならない．偶数全体の集合もアーベル群である．しかし，奇数全体の集合は群にはなり得ない．

(2) 有理数全体の集合 $\mathbf{Q}$，実数全体の集合 $\mathbf{R}$ や複素数全体の集合 $\mathbf{C}$ は，足し算でアーベル群である．$\mathbf{Q}^* = \mathbf{Q} - \{0\}$, $\mathbf{R}^* = \mathbf{R} - \{0\}$ や $\mathbf{C}^* = \mathbf{C} - \{0\}$ は掛け算においてアーベル群になる．掛け算において単位元は 1（いち）である．$\mathbf{Z}$ は $\mathbf{Q}$ の，$\mathbf{Q}$ は $\mathbf{R}$ の,$\mathbf{R}$は$\mathbf{C}$ のそれぞれ部分群になっている．

(3) p を素数とする．$\mathbf{Z}/p\mathbf{Z}$ を p で割った余りの集合とすると，$\mathbf{Z}/p\mathbf{Z}$ は有限巡回群である．$\mathbf{Z}/p\mathbf{Z}$ の全ての元が生成元となり得る．$|\mathbf{Z}/p\mathbf{Z}| = p$ である．

以上の準備のもとで，S_3 の交代群 A_3 を見てみると，$A_3 = \{e, \sigma_1, \sigma_2\}$ であることがわかる．そして，$\sigma_1\sigma_1 = \sigma_2,\ \sigma_1\sigma_2 = e$ なので, A_3 は巡回群 $\langle \sigma_1 \rangle$ であることもわかる．したがって，A_3 はアーベル群である．

以後，交代群 A_n の構造はガロア理論を理解する上で重要となる．

⋆⋆⋆ エヴァリスト・ガロアについて 2

1823 年 9 月，１１歳となったエヴァリストは，パリの名門校ルイ・ル・グランに入学し，家を離れ寄宿生となる．1824 年には第 3 級に進学し，第

3 級の終わりには，ラテン語の最優秀賞のほか 3 つの優秀賞を得る．1826 年の第 1 学期（9 月〜12 月）の学校側の記録のは,「この生徒は少し変わったところはあるが，心優しく，全く無邪気で，多くのよい性質を持っている」とある．1828 年 8 月，理科方面志望者のための数学準備級に入る．ヴェルニエという若い熱心な担任の記録には,「熱心でよくできる」しかし，性格については,「何かを隠しているようで変わり者である」「数学の狂熱に支配されている」などとある．ガロアの親友オーギュスト・シュヴァリエは，1832 年にガロアの思い出をルヴュ・アンシクロペディクに以下のように発表した.「ガロアは 1 6 歳のとき，アーベルと同じように誤って一般の 5 次方程式も代数的に解けるということの証明ができたと思った．このような生徒に対してヴェルニエ氏はどうしてよいかわからなかった．ヴェルニエ氏は何とかしてガロアの先生として振舞おうとするが，ガロアはそれからから免れようとする．彼はガロアに 7 番目の優等賞を与えるが，ガロアはもう 1 年数学準備級を修めてからでなければならないのに，もうエコールポリテクニーク（諸工芸学校）への準備を独学で始めていた.」⋆⋆⋆

3.3　4 次方程式に関する群

4 次方程式

$$x^4 + a_1x^3 + a_2x^2 + a_3x + a_4 = 0 \tag{8}$$

を考える．この場合の基本対象式は，(8) の解を $\alpha_1,\ \alpha_2,\ \alpha_3,\ \alpha_4$ とおいて得られる

$$\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = -a_1 \tag{9}$$

$$\sum_{1\le i<j\le 4} \alpha_i\alpha_j = a_2 \tag{10}$$

$$\sum_{1\le i<j<k\le 4} \alpha_i\alpha_j\alpha_k = -a_3 \tag{11}$$

$$\alpha_1\alpha_2\alpha_3\alpha_4 = a_4 \tag{12}$$

である．このとき，(8) の解 $\alpha_1,\ \alpha_2,\ \alpha_3,\ \alpha_4$ の順をどのように入れ換えても基本対称式 (9) と (10) と (11) と (12) の右辺の値はどれも変化しない．したがって，対称群 S_4 について考えることは意味がある．

対称群 S_4 の部分群である S_3 はアーベル群ではなかったので，S_4 もアーベル群ではない．そこで，交代群 A_4 を調べてみよう．

S_4 の元は 24 個である．以下，恒等置換，互換，可換な 2 個の互換の積，長さ 3 の巡回置換，長さ 4 の巡回置換を列挙する．

恒等置換：e
互換：$(12), (13), (14), (23), (24), (34)$
可換な 2 個の互換の積：$(12)(34), (13)(24), (14)(23)$
長さ 3 の巡回置換：$(123), (124), (132), (134), (142), (143), (234), (243)$
長さ 4 の巡回置換：$(1234), (1243), (1324), (1342), (1423), (1432)$

以上のことから，$(i_1 i_2 \ \cdots \ i_r) = (i_1 i_r)(i_1 i_{r-1}) \cdots (i_1 i_3)(i_1 i_2)$ なので，

$$\begin{aligned} A_4 \ = \ & \{e, (12)(34), (13)(24), (14)(23), (123), (124), (132), (134), (142), \\ & (143), \ (234), (243)\} \end{aligned}$$

であることがわかった．

命題 5　$n \geq 3$ のとき，

$$S_n = \langle (12), (13), \cdots, (1n) \rangle, \qquad A_n = \langle (123), (124), \cdots, (12n) \rangle$$

である．

証明　$S_n = \langle (12), (13), \cdots, (1n) \rangle$ を示す．

$$H = \langle (12), (13), \cdots, (1n) \rangle$$

とおく．$(1i)(1j)(1i) = (ij)$ なので，$(ij) \in H$ である．また任意の置換は互換の積なので，$S_n \subset H$．よって $S_n = H$ である．

$A_n = \langle (123), (124), \cdots, (12n) \rangle$ を示す．

$$K = \langle (123), (124), \cdots, (12n) \rangle$$

とおく．$(12k) = (12)(2k)$ より $K \subset A_n$ である．一方，任意の A_n の元は，$S_n = \langle (12), (13), \cdots, (1n) \rangle$ より $(1i)(1j)$ という形の積で書ける．さらに，

$$(1i)(1j) = \begin{pmatrix} 1 & 2 & i & j \\ j & 2 & 1 & i \end{pmatrix} = (12i)(12j)(12j)$$

なので，$(1i)(1j) \in K$ である．よって $A_n \subset K$ である．したがって $A_n = K$ である．　（証明終）

n 次方程式に関するガロア理論では，$n \leq 4$ の場合と，$n \geq 5$ の場合の対称群 S_n の構造の違いに着目しているのではあるが，命題 6 より，$n \geq 4$ のとき S_n の部分群である交代群 A_n がアーベル群ではない．現時点では，$n \leq 4$ の場合と $n \geq 5$ の違いが理解できていない．

3.4　正規部分群

$n \leq 4$ の場合と，$n \geq 5$ の場合の交代群 A_n の違いを理解するためには，正規部分群という概念が必要となる．

G を群，$a \in G$ とする．集合 $aH,\ Ha$ をそれぞれ

$$aH = \{ax \mid x \in H\}, \quad Ha = \{xa \mid x \in H\}$$

とする．

定義　G を群，$H \subset G$ を部分群とする．任意の $a \in G$ に対して，$aH = Ha$ が成り立つとき，H を G の**正規部分群**といい，$H \lhd G$ あるいは $G \rhd H$ と書く．

命題 6　G を群，$H \lhd G$ とする．このとき任意の $a \in G$ に対して

$$aH = Ha \quad \Leftrightarrow \quad aHa^{-1} = H \quad \Leftrightarrow \quad aHa^{-1} \subset H$$

が成り立つ．

証明　最初の同値性に関しては明らかなので，2 番目の同値性について証明する．$aHa^{-1} = H$ とすると $aHa^{-1} \subset H$ が成り立つことは当然である．$aHa^{-1} \subset H$ を仮定する．a の代わりに a^{-1} で考えると $a^{-1}Ha \subset H$ であって，$H = a(a^{-1}Ha)a^{-1} \subset aHa^{-1}$ が成り立つ．よって $aHa^{-1} = H$ が証明できた．　（証明終）

S_4 の部分集合 $V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$ は，**クラインの 4 元群**と呼ばれ，$V_4 = \langle (12)(34), (13)(24) \rangle$ である．明らかに V_4 は A_4 の部分群である．

命題 7　$V_4 \lhd S_4$ である．

証明　$\sigma, \tau \in S_n$ に対して，$\sigma\tau\sigma^{-1}(\sigma(i_1)) = \sigma\tau(i_1)$ である．今 $\tau = (i_1, i_2, \cdots, i_r)$ とすると，$\sigma\tau\sigma^{-1}(\sigma(i_n)) = \sigma(i_{n+1})$ となる．ただし，$r+1 = 1$ とする．よって

$$\sigma(i_1, i_2, \cdots, i_r)\sigma^{-1} = (\sigma(i_1), \sigma(i_2), \cdots, \sigma(i_r))$$

となる．さて $\eta = (ij)(kl) \in V_4$ に対して，

$$\begin{aligned} \sigma\eta\sigma^{-1} &= \sigma(ij)(kl)\sigma^{-1} = \sigma(ij)\sigma^{-1}\sigma(kl)\sigma^{-1} \\ &= (\sigma(i)\sigma(j))(\sigma(k)\sigma(l)) \in V_4 \end{aligned}$$

なので，$V_4 \lhd S_4$ がいえた．同時に $V_4 \lhd A_4$ もいえた．　（証明終）

以下の補題は，A_n の S_n に関する基本的な性質である．

補題 8　$A_n \lhd S_n$ である．

証明　$\sigma \in S_n$ が偶置換であろうと奇置換であろうと，任意の $\tau \in A_n$ に対して，$\sigma\tau\sigma^{-1}$ は偶置換である．よって $\sigma A_n \sigma^{-1} \subset A_n$，すなわち $A_n \lhd S_n$ がいえた．　（証明終）

群 G に対しその正規部分群が $\{e\}$ のみである群 G を**単純群**という．

A_4 には正規部分群 V_4 が存在したので，A_4 は単純群ではない．これに対し，$n \geq 5$ の場合の A_n にはどのような正規部分群が存在するのかという問いが立てられる．そして，その答えは，”$\{e\}$ のみである”となる．これは，$n \geq 5$ の場合の A_n が単純群であることを意味する．このことを理解するには，群論の一般的な理論を学ぶ必要があり，しばらく辛抱が必要である．

4　対称群 S_n の中の可解群

4.1　商群

以後，一般的な群の理論に入っていくが，その基礎として次の定理がある．

定理 9（ラグランジュの定理）　H を有限群 G の部分群とする．このとき $|H|$ は $|G|$ の約数である．

証明　$x_1 \in G$ に対して，$C_1 = \{x_1 h \mid h \in H\}$ とする．もし，$x_2 \in G$ が C_1 の元でなかったら，$C_2 = \{x_2 h \mid h \in H\}$ を考える．これを繰り返して，有限個の $C_1, C_2, \cdots, C_r$ が得られる．しかも作り方から $i \neq j$ のとき，$C_i \cap C_j = \emptyset$ であり，G は集合として $C_1, C_2, \cdots, C_r$ の直和となる．また，各 C_i の元の個数は $|H|$ に等しい．よって，$|H|$ は $|G|$ の約数である．

（証明終）

G を群，$N \lhd G$ とする．$a \in G$ に対して aN のことを N による**剰余類**といい，a を**代表元**という．

命題 10　G を群，$N \lhd G$ とし，G/N を N による剰余類全体とする．このとき G/N は群となる．

証明　任意の剰余類 aN, bN に対して, その演算を $aNbN = abN$ と定義すればよい．

（証明終）

定義　G/N を N による G の**商群**または**剰余群**という．

例　(1) S_n/A_n は，A_n とある奇置換 σ を代表元とする剰余類 σA_n との２つの元から出来ていて, これは明らかにアーベル群である．

(2) $A_4 = \langle (123), (124) \rangle$ なので，

$$A_4/V_4 = \{V_4,\ (123)V_4,\ (124)V_4\}$$

である．さらに,$(123)(123) = (132), (123)(132) = e$ であり，$(124) = (132)(13)(24)$ なので，$(124)V_4 = (132)V_4$ である．よって，A_4/V_4 は巡回群 $\langle (123)V_4 \rangle$ である．

命題 11　$G_1 \supset G_2 \supset N$，$G_1 \rhd N$ とする．このとき，$G_1/N \rhd G_2/N$ ならば，$G_2 \lhd G_1$ である．

証明　任意の $x \in G_1,\ y \in G_2$ を考える．$G_1/N \rhd G_2/N$ より，$(xyx^{-1})N = (xN)(yN)(x^{-1}N) \in G_2/N$ である．よって，$xyx^{-1} \in G_2$ である．したがって，$G_2 \lhd G_1$ である．　（証明終）

ガロア理論においては，商群 G/N がアーベル群になることが鍵となっている．そして，G/N がアーベル群であることを判定するために，以下で定義される G の部分群 $[G, G]$ というものが必要となる．

定義　G を群とする．$[G, G]$ を $aba^{-1}b^{-1}$ $(a, b \in G)$ 全体で生成される群，すなわち

$$[G, G] = \langle \{aba^{-1}b^{-1} \mid a, b \in G\} \rangle$$

とすると，$[G, G]$ は G の部分群となる．$[G, G]$ を G の**交換子群**という．

命題 12　G を群，H を G の部分群とする．このとき，

$$[G, G] \subset H \Leftrightarrow H \lhd G \text{ かつ } G/H \text{ がアーベル群}$$

が成り立つ．

証明　($\Rightarrow$) $[G,G] \subset H$ とする．$h \in H, a \in G$ ならば，$aha^{-1} = (aha^{-1}h^{-1})h \in H$ である．よって $H \lhd G$ がいえた．

また，$(a^{-1}b^{-1}ab)H = H$ だから，

$$(aH)(bH) = abH = ba(a^{-1}b^{-1}ab)H = baH = (bH)(aH).$$

よって，G/H はアーベル群である．

($\Leftarrow$)　$H \lhd G$ かつ G/H がアーベル群とする．任意の $a, b \in G$ に対し $(aH)(bH) = (bH)(aH)$ だから

$$aba^{-1}b^{-1}H = (aH)(bH)(aH)^{-1}(bH)^{-1} = H.$$

よって $aba^{-1}b^{-1} \in H$．　（証明終）

⋆⋆⋆ **エヴァリスト・ガロアについて３**

1828 年 9 月 ガロアは数学特別級に進学する．そして数学の教員リシャールに認められる．1829 年 4 月，ガロア 1 7 歳のとき，処女作である「循環連分数に関する一定理の証明」という論文が，リシャールの勧めと紹介によって,『数学年報（Annales de mathématiques）』という専門誌に発表された.「ルイ・ル・グラン校の生徒」という肩書きしかない無名の著者の論文が発表されたことは異例であった．その後，発表された論文のタイトルは以下である.「方程式の代数的解法についての論文の要約」（1830 年，4 月）「数字方程式の開放について」（1830 年，6 月）「群論について」（1830 年，6 月）「解析のいくつかの点について」（1830 年，12 月） ⋆⋆⋆

4.2　準同型定理と同型定理

群の理論を理解するのは，２つの群があったとき，それらの関係を知ることが重要となる．そのために２つ群の関係が定まる写像を考える必要がある．

定義　群 G から群 G' への写像 $f : G \to G'$ について，任意の $x, y \in G$ に対し

$$f(xy) = f(x)f(y)$$

が成り立つとき，f を**準同型写像**という．G' の単位元 e' の逆像を f の**核**といい $\mathrm{Ker}\ f$ で表す．G の f による像を f の**像**といい $\mathrm{Im}\ f$ で表す．

上にみたように，準同型写像を平たく言えば，群 G における演算を群 G' の演算に変換する写像のことである．このことを良く表している性質が次の命題である．

命題 13　群の準同型写像 $f : G \to G'$ に対し
(1) $f(e) = e'$，　(2) 任意の $x \in G$ に対し $f(x^{-1}) = f(x)^{-1}$.

証明　(1) $f(e) = f(ee) = f(e)f(e)$ である．両辺に $f(e)^{-1}$ をかけて $e' = f(e)$ を得る．
(2) $f(x^{-1})f(x) = f(e) = e'$ である．よって $f(x^{-1}) = f(x)^{-1}$ である．
（証明終）

これまで，S_n の部分群として，交代群 A_n と正規部分群 N を重視して述べてきたが，以下は，準同型写像から得られる正規部分群に関する一般的な命題である．

命題 14　群の準同型写像 $f : G \to G'$ に対し
(1) Im f は G' の部分群である．
(2) Ker f は G の正規部分群である．

証明　Im f は空でないことを注意しておく．
(1) $x', y' \in$ Im f とする．$x' = f(x), y' = f(y)$ となる $x, y \in G$ がある．よって，$x'y' = f(x)f(y) = f(xy) \in$ Im f である．定理 4 より，Im f は G' の部分群である．
(2) Ker f が G の部分群であることは簡単にわかる．正規であることを見よう．$n \in$ Ker f，$x \in G$ に対して

$$f(xnx^{-1}) = f(x)f(n)f(x^{-1}) = f(x)f(x)^{-1} = e'$$

である．よって，$xnx^{-1} \in$ Ker f である．したがって，命題 6 により Ker $f \lhd G$ である．
（証明終）

定義　群の準同型写像 $f : G \to G'$ が全単射であるとき，f を同型射といい，G と G' は群として**同型**であるという．G と G' が同型であることを

$$G \cong G'$$

で表す．

G と G' が同型であることを平たく言えば，G と G' は演算の仕方はそれぞれ異なっていても，群の元の動き方は類似した構造をしているということである．

命題 15　群の準同型写像 $f : G \to G'$ が単射 $\Leftrightarrow$ $\mathrm{Ker}\ f = \{e\}$ である．

証明　$(\Rightarrow)$ は明らかである．

$(\Leftarrow)$ $\mathrm{Ker}\ f = \{e\}$ とする．$x, y \in G$, $f(x) = f(y)$ と仮定する．このとき $x = y$ であることをいえばよい．

$$f(y^{-1}x) = f(y)^{-1}f(x) = f(x)^{-1}f(x) = e'$$

である．よって，$y^{-1}x \in \mathrm{Ker}\ f = \{e\}$，すなわち $y^{-1}x = e$ である．したがって，$x = y$ である．　（証明終）

以下に，準同型定理，同型定理といった重要な定理が続くが，これらは，群の構造を調べるための重要な道具である．

定理 16　(1) G を群，$N \lhd G$ とする．このとき，

$$\phi : G \to G/N, \quad x \mapsto xN$$

は全射準同型であって，$\mathrm{Ker}\phi = N$ である．これを**自然準同型**という．

(2)（**準同型定理**）　$f : G \to G'$ を群の準同型とする．このとき，$\bar{f} : G/\mathrm{Ker}f \to G', xN \mapsto f(x)$ により，

$$G/\mathrm{Ker}f \cong \mathrm{Im}\ f$$

が得られる．（準同型定理を**同型定理 1** ともいう．）

証明　(1) $x, y \in G$ とすると，$\phi(xy) = xyN = xNyN = \phi(x)\phi(y)$ より，ϕ は準同型写像である．また，任意の $xN \in G/N$ に対して $\phi(x) = xN$ だから ϕ は全射である．$\mathrm{Ker}\phi = N$ を示す．$x \in \mathrm{Ker}\phi$ であることと $\phi(x) = N$ であることは同値である．これは $xN = N$，つまり $x \in N$ を意味する．よって，$\mathrm{Ker}\phi = N$ である．

(2) まず 写像 $\bar{f}$ が代表元の選び方によらず定義されているかどうかをチェックする．$N = \mathrm{Ker}f$ とおく．$xN = yN$ ならば，$y^{-1}x \in N = \mathrm{Ker}\ f$ であり，

$$e' = f(y^{-1}x) = f(y)^{-1}f(x), \quad f(y) = f(x)$$

である．よって $\bar{f}(xN) = f(x)$ は代表元 x の取り方によらない．

次に $\bar{f}$ が準同型写像であることをみる．

$$\begin{aligned} \bar{f}(xNyN) &= \bar{f}(xyN) = f(xy) \\ &= f(x)f(y) = \bar{f}(xN)\bar{f}(yN) \end{aligned}$$

である．よって，$\bar{f}$ は準同型写像である．

最後に同型を示す．任意の $f(x) \in \mathrm{Im}\ f$ に対し，$f(x) = \bar{f}(xN) \in \mathrm{Im}\ \bar{f}$ である．よって，$\mathrm{Im}\ \bar{f} = \mathrm{Im}\ f$ なので，$\bar{f}$ は全射である．したがって，$\bar{f}$ が単射であることを示せばよい．

$$\begin{aligned} xN \in \mathrm{Ker}\ \bar{f} \quad &\Leftrightarrow \quad e' = \bar{f}(xN) = f(x) \\ &\Leftrightarrow \quad x \in \mathrm{Ker}\ f = N \ \Leftrightarrow\ xN = eN \end{aligned}$$

である．よって，$\mathrm{Ker}\ \bar{f} = \{eN\}$ である．したがって，$\bar{f}$ は単射である．

（証明終）

定理 17 G を群，$H \subset G$ を部分群，$N \lhd G$ とする．このとき，以下の (1)，(2) が成り立つ．

(1) $HN = NH$ であって，HN は G の部分群である．

(2)（**同型定理２**） $H \cap N \lhd H$ であって，以下が成り立つ．

$$H/H \cap N \cong HN/N, \quad h(H \cap N) \mapsto hN$$

証明　(1) 任意の $h \in H, n \in N$ に対し，$N \lhd G$ より $hn = hnh^{-1}h \in NH$ である．よって $HN \subset NH$ である．また，$nh = hh^{-1}nh \in HN$ でもあ

る．よって $NH \subset HN$ である．したがって，$NH = HN$ である．さらに，任意の $h_1, h_2 \in H$, $n_1, n_2 \in H$ に対して，

$$(h_1n_1)(h_2n_2) = h_1(n_2h_2)n_1 = (h_1h_2)(n_2n_1) \in HN$$

であり，$(h_1n_1)^{-1} = n_1^{-1}h_1^{-1}$ であるので，

$$(h_1n_1)^{-1} = n_1^{-1}h_1^{-1} \in NH = HN$$

である．よって HN は部分群である．

(2) 埋め込み $i : H \to G, h \mapsto h$ と自然な準同型 $\rho : G \to G/N, g \mapsto gN$ はどちらも準同型だから，合成写像

$$f : H \to G/N, h \mapsto hN$$

も準同型であって

$$\mathrm{Ker}\ f = H \cap N \subset H,\ \ \mathrm{Im}\ f = HN/N \subset G/N$$

である．よって $H \cap N \lhd H$ であり，準同型定理により

$$H/H \cap N \cong HN/N$$

である． （証明終）

定理 18 （**同型定理３**）G を群，$N \lhd G$，$M \lhd G$，$N \subset M$ とする．このとき $M/N \lhd G/N$ であり，写像

$$G/N \to G/M,\ \ xN \mapsto xM$$

は全射準同型であって，

$$G/M \cong (G/N)/(M/N)$$

が成り立つ．

証明　自然な全射 $\rho : G \to G/M, x \mapsto xM$ を考える．$N \subset M = \mathrm{Ker}\rho$ だから，ρ は全射準同型写像

$$f : G/N \to G/M,\ \ xN \mapsto \rho(x) = xM$$

を引き起こす．$\mathrm{Ker}\ f = \{xN \in G/N \mid xM = M\} = M/N$ だから，準同型定理より $G/M \cong (G/N)/(M/N)$ となる． （証明終）

4.3　対称群 S_n の中の可解群

我々は，$n \leq 4$ の場合の S_n と，$n \geq 5$ の場合の S_n の構造の違いを知ることを目標にしているわけであるが，本節で述べる可解群がその違いを明確にする．そして，このことこそが，$n \geq 5$ 以上の n 次方程式がべき根で解くことができないという定理の証明に向かっている．

定義　G を群とする．

(1) 有限個の部分群の列

$$G = G_0 \supset G_1 \supset \cdots \supset G_r = \{e\}$$

において $1 \leq i \leq r, G_{i-1} \rhd G_i$ であるとき，上の列を G の**正規列**という．また，正規列 $G = G_0 \supset G_1 \supset \cdots \supset G_r = \{e\}$ の商群

$$G_0/G_1, G_1/G_2, \cdots G_{r-1}/G_r$$

を**正規列の商群**という．

(2) ある正規列 $G = G_0 \supset G_1 \supset \cdots \supset G_r = \{e\}$ の商群

$$G_0/G_1, \cdots, G_{r-1}/G_r$$

がすべてアーベル群であるとき，G を**可解群**という．さらに，

$$G_0/G_1, \cdots, G_{r-1}/G_r$$

がすべて単純群であるとき，正規列 $G = G_0 \supset G_1 \supset \cdots \supset G_r = \{e\}$ を**組成列**という．

定理 19　$n = 2, 3, 4$ の対称群 S_n は可解群である．

証明　$n = 2$ の場合，S_2 はアーベル群であり，アーベル群は可解群なので，S_2 は可解群である．

$n = 3$ の場合，$\{e\} \lhd A_3 \lhd S_3$ であり，$S_3/A_3, A_3$ はアーベル群だから，S_3 は可解群である．

$n = 4$ の場合，$\{e\} \lhd V_4 \lhd A_4 \lhd S_4$ であり，$S_4/A_4, A_4/V_4, V_4$ はアーベル群だから，S_4 は可解群である．　（証明終）

4.4　可解群でない対称群 S_n

「可解群でない対称群 S_n は何か」という問題を解くための道具として，以下の 3 つの命題を用意し，証明する．

命題 20　群 G の正規部分群は G と $\{e\}$ のみとする．すなわち単純群とする．もし G が可解群ならば，G は位数素数の巡回群である．

証明　G は単純群で可解群なので，G はアーベル群である．よって G の部分群はすべて正規部分群である．任意の $\alpha(\neq e) \in G$ に対して，部分群 $\langle\alpha\rangle$ を考える．G は単純群なので，$G = \langle\alpha\rangle$ である．よって G は巡回群である．$|\langle\alpha\rangle| = n$ で，n は素数でないとする．そこで素数 p で $p|n^*$ となるものをとり，$\beta = \alpha^p$ とする．このとき部分群 $\langle\beta\rangle$ の位数は，$|\langle\beta\rangle| = n/p$ である．しかし，G は単純群なので，$\langle\beta\rangle = G$ であり，これは，$G = \langle\alpha\rangle$ に矛盾する．よって G は位数素数の巡回群である．　（証明終）

命題 21　G を群とする．

(1) G が可解群ならば，部分群 $H \subset G$ もすべて可解群である．G の準同型像もまたすべて可解群である．

(2) $N \lhd G$ に対し，N と G/N がともに可解群ならば，G もまた可解群である．

証明　(1) G を可解群とし，正規列

$$G = G_0 \supset G_1 \supset \cdots \supset G_r = \{e\}$$

の商群 G_{i-1}/G_i はすべてアーベル群であるとする．

(A) 部分群 $H \subset G$ に対し，$H_i = H \cap G_i$ とおく．$H_{i-1} \rhd H_i$ なので，正規列

$$H = H_0 \supset H_1 \supset \cdots \supset H_r = \{e\}$$

を得る．$H_i = H \cap G_i = H_{i-1} \cap Gi$ に注意して，さらに同型定理 2 を用いることで，

$$H_{i-1}/H_i = H_{i-1}/H_{i-1} \cap G_i \cong H_{i-1}G_i/G_i \subset G_{i-1}/G_i$$

---

* $p|n$ は，”p は n を割る” という意味の記号である．以後もよく使う．

を得る．G_{i-1}/G_i がアーベル群だから H_{i-1}/H_i もアーベル群である．よって H は可解群である．

(B) $f : G \to G'$ は全射であるとする．$G_j \lhd G_{j-1}$ より $f(G_j) \lhd f(G_{j-1})$ だから，

$$G' = f(G_0) \supset f(G_1) \supset \cdots \supset f(G_r) = \{e\}$$

は G' の正規列である．一方，f が引き起こす準同型写像

$$\bar{f} : G_{j-1}/G_j \to f(G_{j-1})/f(G_j),\ \ xG_j \mapsto f(x)f(G_j)$$

は全射であって，G_{j-1}/G_j がアーベル群だから，上の正規列の商群 $f(G_{j-1})/f(G_j)$ もアーベル群である．よって $f(G)$ は可解群である．

(2) G/N は可解群だから，G/N の正規列

$$G/N = G_0/N \supset G_1/N \supset \cdots \supset G_m/N = N/N$$

で，$(G_{i-1}/N)/(G_i/N)$ がアーベル群となるものが存在する．このとき，命題 11 より，

$$G = G_0 \supset G_1 \supset \cdots \supset G_m = N$$

は，正規列であり，さらに，同型定理 3 より，

$$(G_{i-1}/N)/(G_i/N) \cong G_{i-1}/G_i$$

が成り立つ．また，N は可解群だから，N の正規列

$$N = G_m \supset G_{m+1} \supset \cdots \supset G_r = \{e\}$$

で，G_{j-1}/G_j がアーベル群となるものが存在する．以上のことから得られた

$$G = G_0 \supset G_1 \supset \cdots \supset G_m = N \supset G_{m+1} \supset \cdots \supset G_r = \{e\}$$

は，G の正規列で，その商群 G_{j-1}/G_j はアーベル群である．よって G は可解群である．　（証明終）

命題 22　$G = G_0 \supset G_1 \supset \cdots \supset G_r = \{e\}$ を G の組成列とする．このとき，G が可解群であれば，G_{i-1}/G_i $(1 \leq i \leq r)$ は素数次の巡回群である．

証明　G_{i-1}/G_i $(1 \leq i \leq r)$ は単純群である．また，命題 21(1) より，G は可解群なので，部分群 G_{i-1} も可解群であり，自然な全射準同型 $\phi : G_{i-1} \to G_{i-1}/G_i$ よりその準同型像 G_{i-1}/G_i も可解群となる．したがって，命題 20 より G_{i-1}/G_i は素数次の巡回群である．　（証明終）

定理 19 と次の定理によって，この節の目標である $n \leq 4$ の場合の S_n と，$n \geq 5$ の場合の S_n の構造の違いが明確になる．

定理 23　$n \geq 5$ のとき，
(1) 交代群 A_n は可解群ではない．
(2) 対称群 S_n も可解群ではない．

証明　(1) A_n はアーベル群でないことに注意する．背理法で示すために A_n は可解群とする．すると $N \lhd A_n$ かつ A_n/N がアーベル群となる部分群 N がある．$A_n = N$ であることを示せば A_n が可解群であることに矛盾する．$A_n = \langle (12k) \mid 3 \leq k \leq n \rangle$ であるから，

$$(12k) \in N$$

を示せばよい．$i, j \in \{3, 4, 5\} - \{k\}$ をとる．

$$\sigma = (1ik) = (1k)(1i),\ \tau = (k2j) \in A_n$$

とおく．A_n/N は可換だから $\sigma, \tau \in A_n$ に対して，$(\sigma N)(\tau N) = (\tau N)(\sigma N)$．よって，

$$\sigma\tau\sigma^{-1}\tau^{-1}N = (\sigma N)(\tau N)(\sigma N)^{-1}(\tau N)^{-1} = N.$$

一方

$$\sigma\tau\sigma^{-1}\tau^{-1} = (1ik)(k2j)(ki1)(j2k) = (12k).$$

よって $(12k) \in N$，すなわち $A_n = N$ が証明された．

(2) 命題 21 (1) より，部分群 $A_n \subset S_n$ が可解群ではないから，S_n も可解群ではない. （証明終）

⋆⋆⋆ エヴァリスト・ガロアについて４

ガロアがアーベルについて書き残した短いノートからいくつかの文章を抜粋する.「アーベルはこの理論（すなわち代数方程式の代数的解法の理論）に最も深く関わっていた数学者であったようである.」「しかし，彼がドイツ語で発表していた論文を見ると，その不可能性の証明は補助方程式の次数についての論法によっており，それを書いたときは，アーベルは根号によって解ける方程式の特性を知っていなかったことは確かと思われる.」「アーベルは，ある種の方程式が代数的に解けることを証明したが，私たちが取り扱った一般問題についての試論は全く見られない．私たちの理論の最も注目すべき点は，すべての場合にそれが可能かどうかをはっきり答えられることである.」 ⋆⋆⋆

5　体に関するキーワード

ガロア理論の理解がスムーズに進んでいくように，体に関する基本的なキーワードを並べる．

キーワード１： 体 K に x を添加してできる体

（概説）まず，集合 K が**体**であるとは，K の２つの元に四則演算ができるものをいう．明らかに，有理数全体 $\mathbf{Q}$ は体である．そして，ガロア理論で重要な体は，体 K の**拡大体**というもので，特に，$K(x)$ と書かれる K の拡大体は，体 K に x を**添加してできる体**と呼ばれるものである．例えば，$\mathbf{Q}(\sqrt{2})$ は，$\mathbf{Q}$ に $\sqrt{2}$ を添加してできる体である．具体的には，$\mathbf{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\}$ である．$\mathbf{Q}(\sqrt{2})$ の２つの元に足し算，引き算，掛け算が定義できることは明らかであろう．割り算については，割り算を行った後，有理化をすれば，$a + b\sqrt{2}$ という形が得られることから，$\mathbf{Q}(\sqrt{2})$ が体であることがわかる．

キーワード２： 最小多項式と共役元

（概説）体 K を係数とする多項式 $f(X)$ 全体の集合は，$K[X]$ と書かれる．そして，$K[X]$ の元の中で，α を代入して 0 となる次数最小の多項式 $f(X)$ を α の K 上の**最小多項式**という．

例えば，$\sqrt{2}$ の $\mathbf{Q}$ 上の最高次数の係数が 1 である最小多項式は $X^2 - 2$ である．さらに，$-\sqrt{2}$ の $\mathbf{Q}$ 上の最高次数の係数が 1 である最小多項式も $X^2 - 2$ である．このように，最高次数の係数が 1 である最小多項式が同じである２つの数は，互いに **$\mathbf{Q}$ 上共役**であるという．

K 上の最小多項式と K 上共役というものは，次に述べる最小分解体というもので重要な役割を果たす．

キーワード３： 最小分解体

（概説）ガロア理論の中の体論において，重要な一つの定理は，$f(X) \in K[X]$ について，$f(X)$ を $L[X]$ 中で，$f(X) = c(X-\alpha_1)\cdots(X-\alpha_n)$, $(c \in K, \alpha_1, \cdots, \alpha_n \in L)$ と分解する K の拡大体 L が存在することである．このとき，$K(\alpha_1, \cdots, \alpha_n)$ を，$f(X)$ の K 上の**最小分解体**と呼んでいる．明らかに，$\alpha_1, \cdots, \alpha_n$ は，$K(\alpha_1, \cdots, \alpha_n)$ においてどれも K 上共役である．

たとえば，$f(X) = X^2 - 2 \in \mathbf{Q}[X]$ の $\mathbf{Q}$ 上の最小分解体は，$\mathbf{Q}(\sqrt{2}, -\sqrt{2}) = \mathbf{Q}(\sqrt{2})$ である．

キーワード４： ガロア拡大

（概説）K が $\mathbf{Q}$ の拡大体であるとき，L が K のガロア拡大であるとは，L の任意の元 α に対して，α の K 上の共役元がすべて L に含まれるとき，L は K の**ガロア拡大**と定義される．そして，K のガロア拡大 L は，ある $f(X) \in K[X]$ の K 上の最小分解体になっていることが重要な性質である．

明らかに，$\mathbf{Q}(\sqrt{2})$ は，$\mathbf{Q}$ 上の最小分解体であり，$\mathbf{Q}$ 上のガロア拡大である．

キーワード５： ガロア群

（概説）L が K のガロア拡大であるとき，L から L への体の同型写像で，K 上では恒等写像になっているもの全体の集合を考えると，これは群となっている．この群を L の K 上の**ガロア群**と呼び，$\mathrm{Gal}(L/K)$ と書く．特に，n 次多項式 $f(X) \in K[X]$ を考えたとき，$f(X)$ の K 上の最小分解体 L に関するガロア群を $f(X)$ のガロア群と呼ぶ．

たとえば，$f(X) = X^2 - 2 \in \mathbf{Q}[X]$ の $\mathbf{Q}$ 上の最小分解体は $L = \mathbf{Q}(\sqrt{2})$ なので，$f(X)$ の $\mathbf{Q}$ のガロア群は，$\mathrm{Gal}(L/\mathbf{Q}) = \{e, \sigma\}$ である．ここで，e は恒等写像で，σ は $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$ というもの，より簡単にい

えば，$\sigma(\sqrt{2}) = -\sqrt{2}$ となるものである．明らかに，$\mathrm{Gal}(L/\mathbf{Q}) \cong S_2$ である．

$f(X)$ のガロア群の定義は，ガロア理論の中心的な役割を果たす．なぜならば，一般的な n 次多項式 $f(X)$ のガロア群は，n 次対称群 S_n と同型である，ということが，基本対称式を用いて証明できるからである．

さらに，M が K のガロア拡大で，L が M のガロア拡大であったとき，$\mathrm{Gal}(L/M)$ が $\mathrm{Gal}(L/K)$ の正規部分群になっていることも重要な結果である．

以上のことから想像されるように，一般的な n 次多項式 $f(X)$ が代数的に解けるということは，S_n と同型である $f(X)$ のガロア群が可解群であるかどうかで判定できるのである．では，代数的に解けるとはどういうことなのだろうか．

キーワード６： べき根拡大と代数的に解ける

（概説）n 次多項式 $f(X) \in K[X]$ が代数的に解けることの定義は，現時点で理解することは難しい．しかし，とりあえず述べておこう．

ポイントになるのは，$f(X)$ の最小分解体 L と，L における $f(X)$ の根 $\alpha_1, \cdots, \alpha_n$ である．このとき，

$$K_1 = K(\alpha_1),\ K_2 = K_1(\alpha_2),\ \cdots, K_n = K_{n-1}(\alpha_n)$$

というように拡大体の列 $K_1 \subset K_2 \subset \cdots \subset K_n$ を作っていったとき，K_i の K_{i-1} 上の最小多項式が $X^{n_i} - \alpha_i$ というものになっていて（K_i を K_{i-1} の**べき根拡大**という），かつ L が K_n の部分体になっているとき，$f(X)$ は**代数的に解ける**と定義される．

この定義によって，「$f(X)$ が代数的に解けることと，GalL/K が可解群であることが同値である」というガロア理論の中の最も重要な定理が，数学的帰納法を用いて得られる．

⋆⋆⋆ エヴァリスト・ガロアについて５

ガロアはエコール・ポリテクニークの２度の受験を失敗する．その後，リシャールの勧めもあり，エコール・ノルマル（1830 年 8 月まではエコール・プレパラートという名称）に進学する．1830 年 7 月 27 日，7 月革命が起こる．これに関連して，ガロアは学校当局から過激な活動を引き起こす危険人物とされ，1831 年 1 月 4 日，エコール・ノルマルから放校される．一方，代数方程式の代数的解法に関する論文を，コーシーを通じて科学学士院に提出したが，論文はいつのまにか失われてしまう．そこで，それを書き直して 1830 年の懸賞論文に提出した．しかし，管理者として論文を持ち帰った審査員のフーリエが急死してしまい，その論文も行方不明になっている．1831 年 1 月 17 日，科学学士院会員のポアッソンから，論文をもう一度書き直して提出するようにという手紙が届く．そして再提出したが，ポアッソンは「この論文は理解できない」とした．ガロアは，それを知って,「心臓が頭脳に反逆した」と述べている． ⋆⋆⋆

6　方程式と体

n 次方程式

$$x^n + a_1 x^{n-1} + \cdots + a_1 x + a_n$$

について，もう一度考えよう．ガロア理論では，n 個の解と係数の関係から得られる対称式に対して，解の対称群 S_n に着目する．そして，可解群という概念をもとに調べると，$n \leq 4$ のときの S_n は可解群であり，$n \geq 5$ のときの S_n は可解群ではないことがわかった．S_n が可解群であることが，n 次方程式がべき根で解けることの証明に関係している．

6.1　2 次方程式の解法

2 次方程式の解法で基本的なことは平方完成させることである．すなわち，方程式

$$x^2 + ax + b = 0$$

を

$$\left(x + \frac{a}{2}\right)^2 = \frac{a^2 - 4b}{4}$$

と変形させる．$Z = x + a/2$ と置いて

$$Z^2 = \frac{a^2 - 4b}{4}$$

というタイプの 2 次方程式が得られることから，解が

$$Z = \pm\sqrt{\frac{a^2 - 4b}{4}}$$

が，求まるという仕組みになっている．ここで重要なことは $Z^2 = 1$ の解 $Z = \pm 1$ が上の解に影響を与えているということである．

さて，2 次方程式 $Z^2 = 1$ は，n 次方程式 $Z^n = 1$ に一般化される．方程式 $Z^n = 1$ は**円分方程式**と呼ばれている．そしてこの $Z = 1$ 以外の解は，複素平面上の単位円上にある偏角 $\theta = 2\pi/n$ の複素数 w となる．さらに，$w^2, w^3, \cdots, w^{n-1}$ もまた解となる．このことは**ド・モアブルの定理**を使えば簡単に証明できる．この意味で，$Z^2 = 1$ の $z = 1$ 以外の解は，$\theta = \pi$ に対応する $w = -1$ と解釈される．しかし，ガロア理論では特にド・モアブルの定理は必要としないので，これ以上詳しい説明はしない．

6.2　3 次方程式の解法

3 次方程式の解法として有名なカルダノの方法では，方程式

$$x^3 + ax^2 + bx + c = 0$$

は，$x + \dfrac{a}{3} = X$ と置いて，

$$X^3 + pX + q = 0$$

という形の方程式に書き換えて考える．以下，カルダノの方法の詳細は述べないが，$x^3 + px + q = 0$ 形の具体的な例から，この方程式の解法を扱うことにする．

それでは，方程式 $x^3 + 3x + 2 = 0$ を解いていく．

まず，因数分解

$$x^3 - 3tux + (t^3 + u^3) = (x + t + u)(x^2 + t^2 + u^2 - tx - ux - tu) \quad (13)$$

に注意して，

$$x^3+3x+2=x^3-3tux+(t^3+u^3)$$

とおく．これを x に関する恒等式と考えると，$tu=-1, t^3+u^3=2$ が得られる．$tu=-1$ より

$$t^3u^3=-1$$

を得る．これと $t^3+u^3=2$ の連立方程式から，例えば，t に関する 6 次方程式

$$t^6-2t^3-1=0 \tag{14}$$

が得られる．t^3 に関する 2 次方程式の解の公式から

$$t^3=1\pm\sqrt{2} \tag{15}$$

であり，

$$t=\sqrt[3]{1\pm\sqrt{2}} \tag{16}$$

が得られる．また，t と u は対等なので，

$$u=\sqrt[3]{1\pm\sqrt{2}}$$

でもある．$tu=-1$ かつ $t^3+u^3=2$ であったので，

$$t=\sqrt[3]{1+\sqrt{2}},\quad u=\sqrt[3]{1-\sqrt{2}}$$

としてよい．因数分解 (13) より $x=-t-u$ が $x^3+3x+2=0$ の解であるので，

$$x_1=-\sqrt[3]{1+\sqrt{2}}-\sqrt[3]{1-\sqrt{2}} \tag{17}$$

が解となることがわかった．

ところで，円分方程式 $Z^3=1$ の $Z=1$ 以外の解を考えると，複素平面上の単位円上にある偏角 $\theta=2\pi/3$ の複素数

$$w=\frac{-1+\sqrt{-3}}{2}$$

と w^2 があるので，(15) の解としては

$$u=w\sqrt[3]{1\pm\sqrt{2}},\quad u=w^2\sqrt[3]{1\pm\sqrt{2}}$$

もある．したがって，$x^3+3x+2=0$ の残りの 2 つの解として

$$x_2 = -w\sqrt[3]{1+\sqrt{2}} - w^2\sqrt[3]{1-\sqrt{2}} \tag{18}$$

$$x_3 = -w^2\sqrt[3]{1+\sqrt{2}} - w\sqrt[3]{1-\sqrt{2}} \tag{19}$$

が得られる．

実際に x_1, x_2, x_3 が方程式 $x^3+3x+2=0$ の解であることを，解と係数の関係からチェックしてみよう．まず，$w^3=1$ より $w^2+w+1=0$ であることから，

$$x_1+x_2+x_3 = -(1+w+w^2)(t+u) = 0$$

がいえる．次に，$tu=-1$ に注意すると，

$$\begin{aligned} & x_1x_2+x_2x_3+x_1x_3 \\ &= \{wt^2+w^2u^2-(w+w^2)\}+\{t^2+u^2-(w+w^2)\} \\ &\quad +\{w^2t^2+wu^2-(w+w^2)\} \\ &= -3(w+w^2) = 3 \end{aligned}$$

がいえる．最後は，$t^3+u^3=2$ より

$$\begin{aligned} x_1x_2x_3 &= -\{wt^2+w^2u^2-(w+w^2)\}(w^2t+wu) \\ &= -(t^3-w^2u-t-wt-w^2t+u^3-w^2u-u) \\ &= t^3+u^3=2 \end{aligned}$$

がいえて，確かに x_1, x_2, x_3 は解であることがわかった．

以上の解法の流れを整理すると，以下のようになる．

(**ステップ０**) 3 次方程式 $x^3+3x+2=0$ が与えられる．このとき x の係数はすべて有理数である．

(**ステップ１**) 解法の過程で，2 次方程式 $Z^2+2Z-1=0$ を解いた（ここで $Z=u^3$ とした）．このときも Z の係数はすべて有理数である．

(**ステップ２**) 解法の過程で，定数項に $\sqrt{2}$ が含まれた 3 次方程式 $t^3=1\pm\sqrt{2}$ または $u^3=1\pm\sqrt{2}$ を，円分方程式 $Z^3=1$ の解 w が含まれることを意識して解いた．

(**ステップ３**) $x = -t - u$ として 2 乗根と 3 乗根を用いた解が得られた．

解法の流れの中で注意すべきことは，方程式に現れる定数項も含んだ係数の形である．すなわち，ステップ 1 において，係数はすべて有理数である 2 次方程式を解いたのであるが，ステップ 2 においては $\sqrt{2}$ が含まれる 3 次方程式を解いている．詳細は後で述べるが，これは体の拡大が起こったと考える．体とは，平たく言えば四則演算が定義されている集合のことである．さらに，ステップ 2 においては，円分方程式 $Z^3 = 1$ を考えた点も注意しておく必要がある．

（**注意**）詳細は省くが，4 次方程式の解法として有名なフェラーリの方法は，解法の過程において，3 次方程式と 2 次方程式を解くことに帰着させるものである．

6.3 体の定義

体とは，大雑にいえばその集合の中で，和・差・積・商という四則演算が使える集合のことである．有理数全体 $\mathbf{Q}$ は，まさにその集合である．

体の定義　集合 F が体であるとは，F の中で加法 $+$ と乗法 $\cdot$ という 2 つの演算が定義されていて, 以下の (1),(2),(3) を満たすものをいう．

(1) 加法に関してアーベル群である．

(2) 乗法に関してもアーベル群である．

(3) 分配法則が成り立つ．即ち，任意の $a, x, y \in F$ に対して，以下が成り立つ．

$$a \cdot (x + y) = a \cdot x + a \cdot y, \quad (x + y) \cdot a = x \cdot a + y \cdot a$$

例　(1) 有理数全体の集合 $\mathbf{Q}$ は体である．これを**有理数体**という．

(2) 実数全体[†] の集合 $\mathbf{R}$ は体である．これを**実数体**という．

(3) 複素数全体[§] の集合 $\mathbf{C}$ は体である．これを**複素数体**という．

(4) 整数を素数 p で割った余りでできる集合 $\mathbf{Z}/p\mathbf{Z}$ は体である．

[†] 実数とは，整数，分数，無理数などの数である．

[§] 複素数とは，整数，分数，無理数，虚数などの数である．

例えば，$\mathbf{Z}/2\mathbf{Z}$ は $\{0,1\}$ という集合である．演算は，$0+0=0, 1+0=0+1=1, 1+1=0, 0\times 0=0\times 1=1\times 0=0, 1\times 1=1$ である．

例 (4) のように集合の元の個数が有限個である体を**有限体**という．

7　整数と環

7.1　整数に関する基礎知識

体について詳しく考えていく前に，**環**という集合についての知識も必要となる．環は整数の一般概念であるので，環の理解をスムーズにするために，この節では，整数に関する基礎知識を整理しておく．

整数の性質　整数全体の集合 $\mathbf{Z}$ には，２つの演算，加法と乗法が定義されていて，以下の性質をもつ．

(1)　$\mathbf{Z}$ は加法についてアーベル群である．

$a,b,c\in\mathbf{Z}$ について，以下の (2),(3),(4) が成り立つ．

(2)　$a(bc)=(ab)c$ が成り立つ．

(3)　$a(b+c)=ab+ac$, $(a+b)c=ac+bc$ が成り立つ．

(4)　$ab=0$ ならば，$a=0$ または $b=0$ である．

命題 24　$\mathbf{Z}$ の部分集合 I には，次の 2 つの性質を満たすものがある．

(1)　任意の $a,b\in I$ に対して，$a+b\in I, -a\in I$

(2)　任意の $x\in R, a\in I$ に対して $xa\in I$

証明　任意の $\alpha\in\mathrm{Z}$ について，$I=\{m\alpha \mid m\in\mathrm{Z}\}$ を考えればよい．
（証明終）

定義　命題 24 をみたす $\mathbf{Z}$ の部分集合 I を，$\mathbf{Z}$ の**イデアル**という．特に，イデアル $I=\{ma \mid m\in\mathrm{Z}\}$ を (a) で表し，**単項イデアル**と呼ぶ．

次は，**除法の一意性**と呼ばれる整数の基本定理である．

定理 25　a を整数，b を正の整数とすると，

$$a = qb + r, \quad 0 \leq r < n - 1$$

となる整数 q, r が 1 組だけ決まる．

証明　まず，$q, r \in \mathbf{Z}$ の存在性を示す．集合 $\{q' \in \mathbf{Z} \mid q'b \leq a\}$ の最大値を q とすると，$qb \leq a < (q+1)b$ となる．ここで，$r = a - qb \in \mathbf{Z}$ とおくと，$a = qb + r$ であって，$0 \leq r < b$ となる．したがって，$q, r \in \mathbf{Z}$ の存在性が示された．

一意性について示す．$0 \leq r, r' < b$ で，$a = qb + r = q'b + r'$ であり，$r > r'$ であるとする．このとき，$r - r' < b$ である．また，$0 < r - r' = (q' - q)b$ より $q < q'$ となる．しかし，$r - r' = (q' - q)b > b$ でもあり，これは $r - r' < b$ に矛盾する．　（証明終）

定理 26　I を $\mathbf{Z}$ の (0) でないイデアルとする．このとき，I の中の絶対値最小の数を a とすると，$I = (a)$ となる．

証明　除数の一意性より，$b \in I$ は，$b = qa + r,\ 0 \leq r < a$ と書ける．イデアルの性質から，$r = b - qa \in I$ である．よって，a の最小性から $r = 0$ であり，$b \in (a)$ となる．　（証明終）

定義　$a,\ b \in \mathbf{Z}$（ただし，$b \neq 0$）とする．

(1)　$a = bc$ となる整数 c が存在するとき，b は a の**約数**，a は b の**倍数**であるという．

(2)　a の 1 と a 以外の約数を，**真の約数**という．

(3)　$p > 1$ である $p \in \mathbf{Z}$ が，真の約数を持たないとき，p を**素数**という．

(4)　$a = da',\ b = db',\ (d, a', b' \in \mathbf{Z})$ であるとき，d を a と b の公約数という．さらに，a と b の公約数で絶対値が最大なものを，a と b の**最大公約数**という．

(5)　a と b の最大公約数が 1 であるとき，a と b は**互いに素**であるという．

系 27　自然数 a, b が互いに素である $\Leftrightarrow$ $ax + by = 1$ となる整数 x, y が存在する．

証明　($\Rightarrow$) a, b は互いに素とする．

$$a,\ 2a,\ 3a,\ \cdots,\ (b-1)a$$

をそれぞれ b で割ると，これらの余りは一意的に定まるので，それぞれの余りを，

$$r(a),\ r(2a),\ r(3a),\ \cdots,\ r((n-1)a)$$

とする．まず，$r(ja)$ は全て異なることを示す．

$0 < i < j < b$ である i, j で $r(ia) = r(ja)$ であったと仮定する．このとき，$r(j-i) \neq 0$ であり，$r(a) \neq 0$ であることも明らかである．$ia = bd_i + r(ia),\ ja = bd_j + r(ja)$ とすると，

$$(j-i)a = ja - ia = (d_j - d_i)b$$

が得られる．これは，$r(a) = 0$ または $r(j-i) = 0$ を意味する．しかし，$r(a) \neq 0$ で $r(j-i) \neq 0$ であることに矛盾する．

いま示されたことから，$r(xa) = 1$ となる x $(0 < x < b-1)$ が存在する．つまり，$xa = bd + 1$ となる x と d が存在する．よって，$y = -d$ とおくと，$ax + by = 1$ が得られる．

($\Leftarrow$) 対偶，すなわち，「自然数 a, b が互いに素でない $\Rightarrow$ $ax + by = 1$ となる整数 x, y は存在しない」ことを証明する．a と b の公約数を $d \geq 2$ とおく．このとき，$ax + by$ は d の倍数となる．したがって，$ax + by = 1$ となる整数 x, y は存在しない．　（証明終）

命題 28　$p \in \mathbf{Z}$ を素数とする．このとき，イデアル $P = (p)$ は，次の性質をもつ．

(1)　$P \neq R$

(2)　$a, b \in R$ について $ab \in P$ ならば $a \in P$ または $b \in P$ である．

証明　(1) $1 \notin P$ であるので，$P \neq R$ である．

(2) $ab \in P$ ならば，p は ab の約数である．そこで，a と p の最大公約数を d とおく．p は素数なので，$d = p, 1$ である．

(A) $d = p$ ならば，$a = a'p$ $(a' \in \mathbf{Z})$ であるので，$a \in P$ である．

(B) $d = 1$ ならば，系 27 より，$ax + py = 1$ となる $x, y \in \mathbf{Z}$ が存在する．よって，$abx + pby = b$ である．，p は ab の約数より，p は b の約数となり，$b = b'p$ $(b' \in \mathbf{Z})$ であるので，$b \in P$ である．　（証明終）

定義　イデアル $I \in \mathbf{Z}$ が，命題 28 の (1) と (2) の性質を満たすとき，I を $\mathbf{Z}$ の**素イデアル**という．

命題 28 のイデアル P は素イデアルである．さらに，P は次の性質をもつ．

命題 29　$p \in \mathbf{Z}$ を素数とする．このとき，イデアル $P = (p)$ は，次の性質をもつ．

(1) $P \neq R$

(2) I が P を含むイデアルであれば，$I = P$ または $I = \mathbf{Z}$ である．

証明　(1) は既に示してあるので，(2) において，$I \neq P$ のとき $I = \mathbf{Z}$ であることを示せばよい．$I \neq P$ より，I の中に p を約数にもたない a がある．つまり，p と a は互いに素である．よって，系 27 より $ax + py = 1$ となる $x, y \in \mathbf{Z}$ が存在する．$ax \in I$, $py \in I$ なので，イデアルの性質より $1 \in I$ となる．定理 26 より，$I = (1) = \mathbf{Z}$ となる．　（証明終）

定義　イデアル $I \in \mathbf{Z}$ が，命題 29 の (1) と (2) の性質を満たすとき，I を $\mathbf{Z}$ の**極大イデアル**という．

$\mathbf{Z}$ において，素イデアル P は極大イデアルである．

7.2　環について

環とは，前節の最初に述べた整数全体の集合 $\mathbf{Z}$ の性質を一般化した概念である．この意味で，$\mathbf{Z}$ を**有理整数環**と呼ぶ．$\mathbf{Z}$ の性質と比較しながら環の定義を理解してほしい．

定義　集合 R に 2 つの演算，加法と乗法が定義されていて，以下の 3 つの条件をみたすとき，R を**環**という．

(1) R は加法についてアーベル群である．

$a, b, c \in R$ について，

(2) $a(bc) = (ab)c$ が成り立つ．

(3) $a(b+c) = ab + ac$, $(a+b)c = ac + bc$ が成り立つ．

特に，1 をもつ環 R を**単位的環**，$ab = ba$ が成り立つ R を**可換環**という．

定義　単位的環 R において，$a \in R$ が乗法の逆元 a^{-1} をもつとき，a を**単元**という．

例　(1) 勿論，体 K は環でもある．そして K の元は全て単元である．

(2) K を体とする．K 係数の多項式全体の集合を $K[X]$ と書く．$K[X]$ は環であり，これを**多項式環**という．

(3) 一般に，体 K に対して，K を係数に持つ $X_1, \cdots, X_n$ の多項式全体の集合を $K[X_1, \cdots, X_n]$ とおく．即ち

$$K[X_1, \cdots, X_n]$$
$$= \{f(X_1, \cdots, X_n) \text{ は } n \text{ 変数の多項式で, その係数は } K \text{ の元である. }\}$$

$K[X_1, \cdots, X_n]$ を K 係数の n 変数**多項式環**という．

(4) $\mathbf{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\}$ は環である．

(5) $w^3 = 1$, $w \neq 1$ とするとき，$\mathbf{Q}[w] = \{a + bw + cw^2 \mid a, b, c \in \mathbf{Q}\}$ は環である．

定義　可換環 R の空でない部分集合 I が，次の 2 つの条件を満たすとき，I は R の**イデアル**であるという．

(1) 任意の $a, b \in I$ に対して，$a + b \in I, -a \in I$

(2) 任意の $x \in R, a \in I$ に対して $xa \in I$

注意　R を単位的可換環，I を R のイデアルとすると，I は加法群 R の正規部分群となるので，商群 R/I を考えることができる．このとき，R/I の加法は

$$(x+I)+(y+I)=(x+y)+I$$

であり，加法群としての単位元は I，$x+I$ の反対元は $-x+I$ である．さらに，R/I の乗法を

$$(x+I)(y+I):=(xy)+I$$

と定めると, R/I は単位的可換環となる．このとき，$1+I$ が R/I の乗法群としての単位元である．R/I を R の I による**商環**という．

定義　R を単位元をもつ可換環とする．

(1) 0 でない $c\in R$ で $ca=0$ となる a を**零因子**という．

(2) 0 以外に零因子をもたない R を，**整域**という．

(3) $a_1,\ \cdots,\ a_n\in R$ に対して，集合

$$\{x_1a_1+\cdots x_na_n+z_1a_1+\cdots z_na_n \mid x_1,\cdots,x_n\in R,\ z_1,\cdots,z_n\in \mathbf{Z}\}$$

を，$a_1,\ \cdots,\ a_n$ で**生成されるイデアル**といい，$(a_1,\ \cdots,\ a_n)$ で表す．

(4) R が整域で，R のすべてのイデアルがただ 1 個の元で生成されるとき，R を**単項イデアル整域**いう．単項イデアル整域を，単に **PID**（Principal Ideal Domain）とも書く．

例　(1)　$\mathbf{Q}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbf{Q}\}$ は整域であり，$\mathbf{Q}[\sqrt{2}]=(1,\sqrt{2})$ である．

(2)　$w^3=1,\ w\neq 1$ とするとき，$\mathbf{Q}[w]$ は整域であり，$\mathbf{Q}[w]=(1,w,w^2)$ である．

(3) 体 K のイデアルは (1) と (0) のみであるので，体 K は PID である．

(4) 定理 26 より，$\mathbf{Z}$ は PID である．

定義　K は体とする．

(1) $f\in K[X_1,\cdots,X_n]$ の係数が 0 でない項 ${X_1}^{i_1}{X_2}^{i_2}\cdots{X_n}^{i_n}$ の添え字の和 $i_1+i_2+\cdots+i_n$ の中の最大値 d を f の**次数**といい，$\deg\ f=d$ と表す．

(2) $\deg f > 0$ である $f \in K[X_1, \cdots, X_n]$ について，$g, h \in K[X_1, \cdots, X_n]$ が存在して，$f = gh$ $(0 < \deg g, \deg h < \deg f)$ となるとき，f は**可約**であるという．f が可約でないとき f は**既約**であるという．

定理 30　体 K 上の多項式環 $K[X]$ の元 f と g について，

$$f = Qg + R, \quad \deg R < \deg g$$

となる $Q, R \in K[X]$ がただ 1 組だけ存在する．

証明　まず，$Q, R \in K[X]$ の存在性を示す．$\deg f < \deg g$ のときは $Q = 0,\ R = f$ とすればよい．したがって，$\deg f \geq \deg g$ であるときを，$n = \deg f$ に関する数学的帰納法で証明する．$n = 0$ のときは明らかである．$n - 1$ まで $Q, R \in K[X]$ は存在性しているとする．$a_n \in K$ を X^n の係数，$m = \deg g$，$b_m \in K$ を g の最高次の係数として，$h = f - a_n b_m^{-1} X^{n-m} g$ とおくと，$\deg h < n$ であるので，帰納法の仮定から，

$$h = Q_1 g + R_1, \quad \deg R_1 < \deg g$$

となる $Q_1, R_1 \in K[X]$ が存在する．よって，$Q = Q_1 + a_n b_m^{-1} X^{n-m}, R = R_1$ とおくと，

$$f = h + a_n b_m^{-1} X^{n-m} g = Qg + R, \ \ \deg R < \deg g$$

となり，$Q, R \in K[X]$ の存在性が示された．

一意性について示す．$\deg R, \deg R' < \deg g$ で，$f = Qg + R = Q'g + R'$ であり，$Q \neq Q'$ であるとする．このとき，$\deg (Q - Q')g \geq \deg g$ である．しかし，$R - R' = (Q - Q')g$ より $\deg (Q - Q')g < \deg g$ で，これは矛盾である．　（証明終）

系 31　体 K 上の多項式環 $K[X]$ は PID である．より詳しくいえば，I を $K[X]$ の (0) でないイデアルとすると，I に含まれる 0 でない元の中で次数最小の g により，$I = (g)$ となる．

証明　I を $K[X]$ の (0) でないイデアルとすると，I に含まれる 0 でない元の中で次数最小のものを g とすると，定理 30 より，$f \in I$ は，$f = Qg + R,\ 0 \leq \deg R < \deg g$ と書け，イデアルの定義から，$R = f - Qg \in I$ がいえ，$\deg g$ の最小性から $R = 0$ であり，$f \in (g)$ となり，$I \subset (g)$ がいえる．$(g) \subset I$ は明らかでなので，$I = (g)$ である．　（証明終）

系 32　体 K とし，$f, g \in K[X]$ とする．集合 $\{q \in K[X] \mid q|f,\ q|g\}$ の中で次数最大のものを Q とすると，

$$Q = fS + gT$$

となる $S, T \in K[X]$ が存在する．特に，f が既約で $f \not| g$ であれば，$fS_1 + gT_1 = 1$ となる $S_1, T_1 \in K[X]$ が存在する．

証明　$K[X]$ のイデアル $I = (f, g)$ を考える．h を I に含まれる 0 でない次数最小の元とする．$h \in (f, g)$ より，$h = fS_0 + gT_0$ となる $S_0, T_0 \in K[X]$ が存在する．$Q|f,\ Q|g$ より，$Q|h$ である．よって，$\deg Q \leq \deg h$ である．一方，系 31 により，$I = (h)$ である．$h|f,\ h|g$ であり，仮定により，$\deg h \leq \deg Q$ である．したがって，$\deg h = \deg Q$ である．$h|Q$ より，$h = cQ\ (c \in K)$ で c は単元なので，$I = (h) = (Q)$ である．ゆえに，$Q = fS + gT$ となる $S, T \in K[X]$ が存在する．

f が既約で $f \not| g$ であれば，$Q \in K$ であり，$Q = fS + gT$ の両辺に Q^{-1} をかけて，$S_1 = Q^{-1}S,\ T_1 = Q^{-1}T$ とおくと，$S_1, T_1 \in K[X]$ であって，$1 = fS_1 + gT_1$ が成り立つ．　（証明終）

定義　R, R' を環とする．Φ を R から R' への写像とする．$x, y \in R$ に対して，条件

$$\Phi(x + y) = \Phi(x) + \Phi(y), \quad \Phi(xy) = \Phi(x)\Phi(y)$$

をみたすとき，Φ を R から R' への（環）としての準同型写像という．また Φ が全単射であるとき，R と R' は同型であるといい，$R \cong R'$ と書く．

定理 33 (**準同型定理**)　f を可換環 R から可換環 R' への準同型写像とすると，写像 $\varphi : x + \mathrm{Ker}f \mapsto f(x)$ により

$$R/\mathrm{Ker}f \cong \mathrm{Im}f$$

が成り立つ．

証明　$\mathrm{Ker}f$ は R のイデアルであるので，$R/\mathrm{Ker}f$ は商環である．φ を加法群としての写像とみると，加法群としての準同型定理より，$R/\mathrm{Ker}f \cong \mathrm{Im}f$ が得られる．また，φ を乗法群としての写像とみると，乗法群としての準同型定理より，$R/\mathrm{Ker}f \cong \mathrm{Im}f$ が得られる．したがって，$R/\mathrm{Ker}f$ と $\mathrm{Im}f$ は環として同型である．　（証明終）

定義　R を単位的可換環とする．R のイデアル M が次の 2 つの条件 (1),(2) を満たすとき，M は R の**極大イデアル**であるという．

(1) $M \neq R$

(2) イデアル I が $I \supset M$ ならば $I = M$ またが $I = R$ である．

R のイデアル P が次の 2 つの条件 (3),(4) を満たすとき，P は R の**素イデアル**であるという．

(3) $P \neq R$

(4) $a, b \in R$ について $ab \in P$ ならば $a \in P$ または $b \in P$ である．

注意　K を体とし，$f(X) \in K[X]$ を考える．このとき，以下が成り立つ．

$f(X)$ は既約である $\Leftrightarrow$ $f(X)$ を割るものは $\pm f(X)$ か $\pm c \in K$ である $\Leftrightarrow$ $(f(X))$ は極大イデアルである．

命題 34　R を単位的可換環とする．このとき以下が成り立つ．

$$M \text{ が } R \text{ の極大イデアルである} \Leftrightarrow R/M \text{ が体である．}$$

証明　M が R の極大イデアルである $\Leftrightarrow$ M を含むイデアルは M と R のみである $\Leftrightarrow$ R/M のイデアルは (0) と R/M のみである $\Leftrightarrow$ 任意の $x \in R/M$ に対し $1 \in (x)$ なので，$xy = 1$ となる $y \in R/M$ が存在する $\Leftrightarrow$ R/M は体である．　（証明終）

⋆⋆⋆ エヴァリスト・ガロアについて 6

1831 年 5 月 9 日，ガロアは共和主義者たちが集まるある祝賀会で，ナイフをかざしながら「ルイ・フィリップのために！」と叫んだ．翌日に逮捕，6 月 15 日，重罪裁判所で公判にかけられる．「今の政府のやり方をみると，ルイ・フィリップはそのうち国民を裏切るにちがいないと思います.」「王の行為は善意だけからされているかどうか疑わせるものがあると思います.」自分に不利なことを言うガロアを裁判長はたしなめたりしたが，陪審員たちの意見と協議の半時間ほどの協議の後，ガロアは無罪となり釈放される．7 月 14 日の革命記念日に，共和主義者たちはバスティーユ広場に「自由の樹」を植樹するというお祭りを計画し，一般市民にも呼びかけた．当日，ガロアは，国民軍の制服を着用し，武装していたことから，12 時半頃ポン・ヌフにて逮捕された．その後，軽罰裁判所での裁判で 9 ヶ月の禁固刑に処せられた．　⋆⋆⋆

8　ベクトル空間と次元

環をさらに一般化したものとして**ベクトル空間**という概念がある．以下では，ガロア理論において必要最小限の事柄を整理する．[3] ではベクトル空間のいろいろな世界を知ることができる．

8.1　ベクトル空間

定義　集合 V の任意の元 x, y と体 K の任意の元 a に対して，加法 $x+y \in V$ とスカラー倍 $ax \in V$ が定まっていて，以下の (1)〜(4) の条件が満たされているとき，V を K 上のベクトル空間であるという．以下，$x, y \in V$, $a, b \in K$ とする．

(1)　V は加法群である．

(2)　$(ab)x = a(bx)$

(3)　$a(x+y) = ax + by$,　$(a+b)x = ax + by$

(4)　$1x = x$

例 (1) 体 K は K 上のベクトル空間である．
(2) 複素数体 $\mathbf{C} = \{a + ib \mid a, b \in \mathbf{R}\}$ は，$\mathbf{R}$ 上のベクトル空間である．
(3) 多項式環 $K[X]$ は K 上のベクトル空間である．
(4) $\mathbf{Q}[\sqrt{2}]$ は $\mathbf{Q}$ 上のベクトル空間である．
(5) $\mathbf{Q}[w]$ は $\mathbf{Q}$ 上のベクトル空間である．

定義 V を K 上のベクトル空間する．このとき，集合 $W \subset V$ が，K 上のベクトル空間であるとき，W は V の**部分空間**であるという．

さらに，V の元 $x_1, \cdots x_n$ について，

$$W = \{a_1x_1 + \cdots + a_nx_n \mid a_i \in K\}$$

とすると，W は V の部分空間となる．W を $x_1, \cdots x_n$ で**生成される** V の**部分空間**といい，

$$W = Kx_1 + \cdots + Kx_n$$

と表す．$x_1, \cdots, x_n$ を W の**生成元**という．

例 (1) $\mathbf{Q}$ 上のベクトル空間 $V = \mathbf{Q}[\sqrt{2}]$ の生成元は $1, \sqrt{2}$ である．
(2) $\mathbf{Q}$ 上のベクトル空間 $V = \mathbf{Q}[w]$ の生成元は $1, w, w^2$ である．

8.2 ベクトル空間の基底と次元

ベクトル空間において最も大切な概念が**次元**である．次元を理解するためには，**1 次独立**と**基底**という概念の定義が必要である．

定義 V を K 上のベクトル空間とする．

(1) $x_1, \cdots, x_n \in V$ に対して，$c_1x_1 + \cdots + c_nx_n = 0$ を満たす $c_1, \cdots, c_n \in K$ は，$c_1 = \cdots = c_n = 0$ に限るとき，$x_1, \cdots, x_n$ は**1 次独立**であるという．

(2) V の生成元 $x_1, \cdots, x_n$ が 1 次独立であるとき，$x_1, \cdots, x_n$ を V の**基底**という．このとき V を $V = \langle x_1, \cdots x_n \rangle$ で表す．

命題 35 V を K 上のベクトル空間で，$x_1, \cdots, x_n \in V$ とする．このとき，以下が成り立つ．

$x_1, \cdots, x_n \in V$ が 1 次独立である $\Leftrightarrow$ $x_1, \cdots, x_{n-1} \in V$ が 1 次独立で，$x_n \notin Kx_1 + \cdots + Kx_{n-1}$ である．

証明 ($\Rightarrow$) $x_1, \cdots, x_n \in V$ が 1 次独立であるならば，$x_1, \cdots, x_{n-1}$ は明らかに 1 次独立である．$x_n \in Kx_1 + \cdots + Kx_{n-1}$ と仮定する．このとき，ある $c_i \neq 0$ である K の元が存在して，

$$x_n = c_1x_1 + \cdots + c_{n-1}x_{n-1} \quad (c_i \in K)$$

と書けるが，

$$c_1x_1 + \cdots + c_{n-1}x_{n-1} - x_n = 0$$

であるため，$x_1, \cdots, x_n \in V$ が 1 次独立であることに矛盾する．

($\Leftarrow$) $c_1x_1 + \cdots + c_nx_n = 0$ とする．このとき $c_n = 0$ である．なぜならば，$c_n \neq 0$ とすると，

$$x_n = -c_1c_n^{-1}x_1 - \cdots - c_{n-1}c_n^{-1}x_{n-1} \in Kx_1 + \cdots + Kx_{n-1}$$

となり，仮定に矛盾するからである．よって，$c_n = 0$ である．したがって，$c_1x_1 + \cdots + c_{n-1}x_{n-1} = 0$ となり，$x_1, \cdots, x_{n-1}$ は 1 次独立だったので，$c_1 = \cdots = c_{n-1} = 0$ しかありえない．したがって，$x_1, \cdots, x_n$ は 1 次独立である． （証明終）

定理 36　V を K 上のベクトル空間で，$V \neq \{0\}$ とする．このとき，V には基底が存在する．すなわち，$V = Kx_1 + \cdots Kx_m$ とすると，順番を適当に並べ替えた $x_1, \cdots, x_m$ の中に，1 次独立な $x_1, \cdots, x_n$ で，$V = Kx_1 + \cdots Kx_n$ となるものが存在する．

証明　$x_1, \cdots, x_m$ の中には必ず 0 でないものがあるから，それを改めて x_1 とする．明らかに x_1 は 1 次独立である．$V = Kx_1$ であれば証明は終わる．$V \neq Kx_1$ であるとき，$j = 2, 3, \cdots, m$ の中から $x_j \notin Kx_1$ となるものを一つ選んで x_2 とすると，命題 35 より，x_1, x_2 は 1 次独立である．このとき，$V = Kx_1 + Kx_2$ であれば証明は終わる．$V \neq Kx_1 + Kx_2$ であるとき，$j = 3, 4, \cdots, m$ の中から $x_j \notin Kx_1 + Kx_2$ となるものを一つ選んで x_3 とすると，やはり命題 35 より，x_1, x_2, x_3 は 1 次独立である．このとき，$V = Kx_1 + Kx_2 + x_3$ であれば証明は終わる．この操作を n 回繰り返すことで，定理は証明される． （証明終）

命題 37　V を K 上のベクトル空間で，$V = \langle x_1, \cdots, x_n \rangle$ とする．このとき，$y_1, \cdots, y_r \in V$ かつ $y_1, \cdots, y_r$ が 1 次独立ならば，$x_1, \cdots, x_n$ から r 個を $y_1, \cdots, y_r$ で置き換えて，例えば $x_1, \cdots, x_r$ を $y_1, \cdots, y_r$ で置き換えて，$V = \langle y_1, \cdots, y_r, x_{r+1}, \cdots, x_n \rangle$ とすることができる．

証明　$y_1 \in V$ より，

$$y_1 = c_1 x_1 + \cdots + c_n x_n \quad (c_i \in K)$$

と表され，ある $c_i \neq 0$ である．たとえば，$c_1 \neq 0$ とすると

$$x_1 = c_1^{-1} y_1 - c_2 c_1^{-1} x_2 - \cdots - c_n c_1^{-1} x_n$$

となる．よって，$V = Ky_1 + Kx_2 + \cdots + Kx_n$ である．$y_1 \notin Kx_2 + \cdots + Kx_n$ と命題 35 より，$y_1, x_2, \cdots, x_n$ は 1 次独立である．したがって，$V = \langle y_1, x_2, \cdots, x_n \rangle$ である．同様に $y_2 \in V$ について

$$y_2 = c_1 y_1 + c_2 x_2 \cdots + c_n x_n \quad (c_i \in K)$$

と表され，y_1, y_2 が 1 次独立なので，$2 \leq i \leq n$ で $c_i \neq 0$ となるものがある．たとえば，$c_2 \neq 0$ とすると

$$x_2 = -c_1 c_2^{-1} y_1 + c_2^{-1} y_2 - \cdots - c_n c_2^{-1} x_n$$

となる．よって，$V = \langle y_1, y_2, y_3 \cdots, x_n \rangle$ となる．この操作を繰り返して，$V = \langle y_1, \cdots, y_r, x_{r+1}, \cdots, x_n \rangle$ とすることができる．　（証明終）

定義　V を K 上のベクトル空間とする．

V の 1 次独立な元の最大個数 n を V の次元といい，$\dim_K V = n$ と表す．このとき，V は**有限次元**であるという．V が有限次元でないとき，V は**無限次元**であるといい，$\dim_K V = \infty$ と表す．

定理 38　V を K 上のベクトル空間とする．$x_1, \cdots, x_n$ が V の基底，すなわち，$V = \langle x_1, \cdots, x_n \rangle$ ならば，$\dim_K V = n$ である．

証明　$V = Kx_1 + \cdots + Kx_n$ かつ $n < \dim V$ を仮定する．$m = \dim_K V$ とおくと，1 次独立な $y_1, \cdots, y_m \in V$ がとれる．一方，各 y_i は $x_1, \cdots, x_n$ で生成されているので，$V = Ky_1 + \cdots + Ky_m$ である．よって，$V = \langle y_1, \cdots, y_m \rangle$ である．命題 37 より，

$$V = \langle x_1, \cdots x_n, y_{n+1}, \cdots, y_m \rangle$$

とすることができる．これは，$x_1, \cdots x_n, y_{n+1}, \cdots, y_m$ が 1 次独立であることを意味する．しかし，これは各 y_i が $x_1, \cdots, x_n$ で生成されていることに矛盾する．　（証明終）

例　(1)　$\mathbf{Q}$ 上のベクトル空間 $V = \mathbf{Q}[\sqrt{2}]$ において，$1, \sqrt{2}$ は V の 1 次独立な生成元であるので，V の基底である．したがって，$\dim_{\mathbf{Q}} V = 2$ である．

(2)　$\mathbf{Q}$ 上のベクトル空間 $V = \mathbf{Q}[w]$ において，$1, w, w^2$ は V の 1 次独立な生成元であるので，V の基底である．したがって，$\dim_{\mathbf{Q}} V = 3$ である．

(3)　体 K 上のベクトル空間 $V = K[X]$ は無限次元，すなわち $\dim_K V = \infty$ である．

9　最小分解体とガロア拡大

ガロア理論とは群と体の理論である．その方法は，考えている体とそれを拡大して得られる体の関係性から，適切な群を見つけるものである．特に，最小分解体やガロア拡大といった拡大体は重要となる．そして，拡大体から見つけられた適切な群は，対称群 S_n と関係する．

9.1　体の拡大

§ 3.2 において，有理数体 $\mathbf{Q}$ を係数とする方程式 $x^3 + 3x + 2 = 0$ の解法の流れを説明した．ステップ 0 で，因数分解

$$x^3 - 3tux + (t^3 + u^3) = (x + t + u)(x^2 + t^2 + u^2 - tx - ux - tu)$$

を注意して，x に関する恒等式

$$x^3 + 3x + 2 = x^3 - 3tux + (t^3 + u^3)$$

から，$tu=-1, t^3+u^3=2$ とした．ステップ 1 においては，6 次方程式

$$(t^3)^2-2(t^3)-1=0$$

というタイプの方程式を解いたのだが，このとき，解は有理数体 $\mathbf{Q}$ にはなく，体 $\mathbf{Q}$ に $\sqrt{2}$ を**添加してできる体** M の中にあると考えることができる．より具体的には，

$$\mathbf{Q}(\sqrt{2})=\{a+b\sqrt{2}\mid a,b\in\mathbf{Q}\} \tag{20}$$

は，体の公理を満たすので体であり，この体 $\mathbf{Q}(\sqrt{2})$ が $\mathbf{Q}$ に $\sqrt{2}$ を添加してできる体 M である．

ステップ 2 においては，体 $\mathbf{Q}(\sqrt{2})$ を係数とする方程式

$$t^3=1\pm\sqrt{2}$$

を解いた．そして，この方程式の解は，w を $w^3=1, w\neq 1$ なる複素数として，

$$t=\sqrt[3]{1\pm\sqrt{2}},\quad w\sqrt[3]{1\pm\sqrt{2}},\quad w^2\sqrt[3]{1\pm\sqrt{2}}$$

であることがわかった．そして，

$$t=\sqrt[3]{1+\sqrt{2}}$$

と置いたとき，

$$u=\sqrt[3]{1-\sqrt{2}}=-\frac{1}{t}$$

であることに注意すると，これらの 6 つの解は，体 $M=\mathbf{Q}(\sqrt{2})$ に t と w を添加してできる体

$$\begin{aligned} L &= M(t,w) \\ &= \left\{a_1+a_2w+a_3t+a_4t^2+a_5wt+a_6wt^2\mid a_j\in M\right\} \end{aligned} \tag{21}$$

の元であると考えることができる．

そして，ステップ 3 で，最初に述べた因数分解から得られる式 $x=-t-u$ を用いて，求めるべき方程式 $x^3+3x+2=0$ の解である

$$x_1=-t-u,\quad x_2=-wt-w^2u,\quad x_3=-w^2t-wu$$

を得ることができた．

今，みてきたように 3 次方程式の解法は，先ず，体 $\mathbf{Q}$ から $M = \mathbf{Q}(\sqrt{2})$ へ，次に，$L = M\left(\sqrt[3]{1+\sqrt{2}}, w\right)$ へ，というように，少しずつ体を拡大させて，適当な拡大体の中で解を見つける方法である．そして，一般に，n 次方程式に関しても，体を拡大させていって，適当な拡大体の中で解の構造を調べる方法が，ガロア理論なのである．

以下，体の拡大についてもう少し詳しく見ていく．

定義　E を体，F を E の部分集合とする．もし F 自身が体であるとき，F を E の**部分体**であるといい，逆に E は F の**拡大体**であるという．さらに E の部分体であり，F の拡大体であるような体 K を E と F の**中間体**という．

例　$\mathbf{C}$ は $\mathbf{R}$ の拡大体であり，$\mathbf{R}$ は $\mathbf{Q}$ の拡大体である．よって，$\mathbf{R}$ は $\mathbf{C}$ と $\mathbf{Q}$ の中間体である．

定義　体 K の部分体が K だけであるとき，K を**素体**という．素体は $\mathbf{Q}$ と $\mathbf{Z}/p\mathbf{Z}$（p は素数）だけしかないことが知られている．K が，素体 $\mathbf{Z}/p\mathbf{Z}$ の拡大体となっているとき，K の**標数**は p であるといい，素体 $\mathbf{Q}$ の拡大体となっているとき，K の標数は 0 であるという．

以下考える体の標数は 0 とする．[†]

定義　$K(X_1, \cdots, X_n)$ を K 係数の n 変数の有理式全体とする．即ち

$$K(X_1, \cdots, X_n) = \left\{ \frac{f(X_1, \cdots, X_n)}{g(X_1, \cdots, X_n)} \;\middle|\; f(X_1, \cdots, X_n), g(X_1, \cdots, X_n) \in K[X_1, \cdots, X_n] \right\}$$

である．$K(X_1, \cdots, X_n)$ は体であり，これを n 変数**有理関数体**という．

[†] 標数が 0 でないときは拡大の状況が複雑になる．代数方程式の可解性に関する定理を証明するだけなら，標数は 0 としてよい．しかし，今後述べる定理や命題には標数が 0 でなくとも成立するものもある．

K を体，L を K の拡大体，$\alpha_1, \cdots, \alpha_n \in L$ とする．$K(\alpha_1, \cdots, \alpha_n)$ を

$$K(\alpha_1, \cdots, \alpha_n) = \left\{ \frac{f(\alpha_1, \cdots, \alpha_n)}{g(\alpha_1, \cdots, \alpha_n)} \;\middle|\; f(X_1, \cdots, X_n), g(X_1, \cdots, X_n) \in K[X_1, \cdots, X_n], \; g(\alpha_1, \cdots, \alpha_n) \neq 0 \right\}$$

とおく．$K(\alpha_1, \cdots, \alpha_n)$ も体であり，K の拡大体である．

例　(1) $\mathbf{Q}(\sqrt{2}) = \mathbf{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\}$ である．このことから，$\mathbf{Q}(\sqrt{2})$ は $\mathbf{Q}$ 上のベクトル空間で，基底は $1, \sqrt{2}$ である．

(2) $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbf{Q}\}$ である．このことから，$\mathbf{Q}(\sqrt{2}, \sqrt{3})$ は $\mathbf{Q}$ 上のベクトル空間で，基底は $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ である．

(3) $\mathbf{Q} = (\sqrt[3]{2})\{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbf{Q}\}$ である．このことから，$\mathbf{Q}(\sqrt[3]{2})$ は $\mathbf{Q}$ 上のベクトル空間とみなすことができ，基底は $1, \sqrt[3]{2}, \sqrt[3]{4}$ である．

定義　L が K の拡大体であるとき，L は K のベクトル空間とみなすことができ，K 上のベクトル空間としての L の次元を，L の K 上の**次数**といい，$[L : K]$ で表す．$[L : K] < \infty$ のとき，L は K の**有限次拡大体**であるといい，$[L : K] = \infty$ のとき，L は K の**無限次拡大体**であるという．

例　$[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2$ である．

定理 39　L を体 K の拡大体，M を中間体とする．このとき，$\{\Omega_\lambda\}_{\lambda \in \Lambda}$ を L の M 上の基底，$\{\omega_\mu\}_{\mu \in M}$ を M の K 上の基底とすると，$\{\Omega_\lambda \omega_\mu\}_{\lambda \in \Lambda, \mu \in M}$ は L の K 上の基底となる．

証明　仮定より，任意の $\zeta \in L$ に対し，$\zeta = \sum_i \alpha_{\lambda_i} \Omega_{\lambda_i}, (\alpha_{\lambda_i} \in M)$ であり，$\alpha_{\lambda_i} = \sum_j \beta_{\mu_j}^{(i)} \omega_{\mu_j}, (\beta_{\mu_j}^{(i)} \in K)$ である．よって，$\zeta = \sum_j \sum_i \beta_{\mu_j}^{(i)} \Omega_{\lambda_i} \omega_{\mu_j}$ と書ける．すなわち，$\{\Omega_\lambda \omega_\mu\}$ は，L の K 上の生成元である．

また，$\sum_{ij} c_{ij}\Omega_{\lambda_i}\omega_{\mu_j} = 0, (c_{ij} \in K)$ とおくと，$\sum_i (\sum_j c_{ij}\omega_{\mu_j})\Omega_{\lambda_i} = 0$ より，$\sum_j c_{ij}\omega_{\mu_j} = 0$ であり，したがって $c_{ij} = 0$ を得る．よって $\{\Omega_\lambda \omega_\mu\}$ は K 上 1 次独立である． （証明終）

系 40 次の等式が成り立つ．

$$[L : K] = [L : M][M : K].$$

証明　定理 39 より，すぐわかる． （証明終）

定義　L を体 K の拡大体とする．0 でない $\alpha \in L$ に対して，$f(\alpha) = 0$ となるような多項式 $f(X) \in K[X]$ が存在するとき，α は K 上**代数的**であるという．そうでないとき，α は K 上**超越的**であるという．

L の全ての元が代数的であるとき，L は K の**代数拡大**（**代数拡大体**）であるという．そうでないとき，L は K の**超越拡大**（**超越拡大体**）であるという．

例　(1) $\sqrt{2}$ は $\mathbf{Q}$ 上代数的である．$\mathbf{Q}(\sqrt{2})$ は $\mathbf{Q}$ の代数拡大である．
(2) 円周率 π やネイピア数 e は，$\mathbf{Q}$ 上超越的であることが知られている．

さて，これから次第に明らかになってくるガロア理論の重要な点は，体 K 係数の n 次方程式 $x^n + a_1x^{n-1} + \cdots a_{n-1} + a_n$ の解 $x_1, x_2, \cdots, x_n$ を全て含む体 $\mathbf{Q}(x_1, x_2, \cdots, x_n)$ の構造を問題にするところにある．以下に，§ 4.3 の有理数体 $K = \mathbf{Q}$ を係数とする方程式 $x^3+3x+2 = 0$ の解 $x_1,\ x_2,\ x_3$ 全てを含む体 $F = \mathbf{Q}(x_1, x_2, x_3)$ の構造をこの観点から考えていく．

§ 4.3 のステップ 1 で述べた 2 次方程式 $Z^2 - 2Z - 1 = 0$ の解は，体 $M = \mathbf{Q}(\sqrt{2})$ の中にあり，このとき $[M : K] = 2$ である．ステップ 2 においては，体 M を係数とする方程式 $t^3 = 1 \pm \sqrt{2}$ を解いて，その解は，体 $L = M\left(\sqrt[3]{1+\sqrt{2}}, w\right)$ にあるといえる．そして，(21) からもわかるように，$[L : M] = 6$ である．

すなわち，3 次方程式の解は，2 乗根や 3 乗根といったべき根を添加してできる拡大体を用いて，$[M : K] = 2$，$[L : M] = 6$ といった次数で拡大

している．よって，L は K 上の次数が $[L:K]=[L:M][M:K]=12$ である体である．

しかし，我々が問題にしている体 F は，$F=\mathbf{Q}(x_1,x_2,x_3)$ という L の部分体である．なぜならば，ガロア理論においては，n 次方程式がべき根で解けるかどうかは，対称群 S_n に関係すると主張してきたからである．この主張からいえば，もし $[F:K]=3!=6$ が成り立てば，対称群 S_3 との関係性が少し想像できるようになるだろう．以下に，$[F:K]=3!=6$ を証明していこう．

$x^3+3x+2=0$ の解 x_1, x_2, x_3 をもう一度書くと，

$$x_1=-t-u,\quad x_2=-wt+w^2u,\quad x_3=-w^2t+wu$$

ここで，$t=\sqrt[3]{1+\sqrt{2}}$，$u=-1/t$ である．解と係数の関係より

$$x_1+x_2+x_3=0,\ x_1x_2+x_2x_3+x_3x_1=3,\ x_1x_2x_3=2$$

が成り立つ．したがって，$F=\mathbf{Q}(x_1,x_2)$ とできる．

さて，一般的な 3 次方程式 $x^3+ax^2+bx+c=0$ の解 x_1, x_2, x_3 に対して，

$$\Delta=(x_1-x_2)(x_1-x_3)(x_2-x_3)$$

とおくと，

$$\Delta^2=-4a^3c+a^2b^2+18abc-4b^3-27c^2$$

となる．Δ は**差積**と呼ばれる．いま，$x^3+3x+2=0$ を考えているので，

$$\Delta^2=-2^3\cdot 3^3$$

より，$\Delta=6\sqrt{-6}$ を得る．よって，$F_0=\mathbf{Q}(\Delta)$ とおくと，$[F_0:\mathbf{Q}]=2$ である．さらに，$w=(-1+\sqrt{-3})/2$ に注意すると，$L=M(t,w)\supset \mathbf{Q}(\sqrt{2},w)=\mathbf{Q}(\sqrt{2},\sqrt{-3})$ より，$F_0\subset L$ であることがわかる．

そこで，次に $F_0(x_1)=F$ であることを示す．

$$g(x)=(x-x_1)(x-x_2)(x-x_3)$$

とおく．そして $g(x)$ を x で微分する．

$$g'(x)=(x-x_2)(x-x_3)+(x-x_1)(x-x_3)+(x-x_1)(x-x_2)$$

より，$g'(x_1) = (x_1 - x_2)(x_1 - x_3) \in F_0(x_1)$ である．したがって，

$$x_2 - x_3 = \frac{\Delta}{(x_1 - x_2)(x_1 - x_3)} \in F_0(x_1)$$

となる．よって，$F_0(x_1) = F_0(x_1, x_2) = F$ である．$x = -t + 1/t$（ただし $t = \sqrt[3]{1+\sqrt{2}}$ ）であったので $[F : F_0] = 3$ となる．したがって，

$$[F : \mathbf{Q}] = [F : F_0][F_0 : \mathbf{Q}] = 3 \cdot 2 = 6$$

であることが示された．

9.2 最小多項式

定理 41　L を体 K の代数拡大体，α を K 上の代数的な L の元とする．α を代入して 0 となる $K[X]$ の 0 でない多項式のうちで次数が最小のものの 1 つを $f(X)$ とすると，$f(X)$ は，$K[X]$ において定数倍を除いて因数分解されない．つまり，もし $f(X) = g(X)h(X)$ と分解されたなら $g(X), h(X)$ のどちらかは K の元である．

証明　$g(X), h(X) \in K[X], f(X) = g(X)h(X)$ と分解されたとする．$g(\alpha)h(\alpha) = f(\alpha) = 0$ より，$g(\alpha) = 0$ か $h(\alpha) = 0$ である．$f(X)$ は α で 0 になる次数最小の多項式であるから，$g(\alpha) = 0$ なら $f(X)$ の次数と $g(X)$ の次数は等しい．よって，$h(X)$ の次数は 0，すなわち $h(X)$ は K の元である．　（証明終）

定義　$K[X]$ の元の中で，α を代入して 0 となる次数最小の多項式 $f(X)$ を α の K 上の**最小多項式**という．特に最高次の係数が 1 の (α の K 上の) 最小多項式を $\mathrm{Irr}(\alpha, K)$ と書く．

例　$\mathrm{Irr}(\sqrt{2}, \mathbf{Q}) = X^2 - 2$ である．

命題 42　L を K の拡大体，α を K 上代数的な L の元，$f(X) = \mathrm{Irr}(\alpha, K)$ とすると，以下が成り立つ．

(1)　$f(X)$ は $K[X]$ において既約である．

(2)　$g(X) \in K[X], g(\alpha) = 0$ とすると，$f(X)|g(X)$ である．

証明　(1) $g_1(X) \in K[X], g_1(X)|f(X)$ とすると，$f(X) = g_1(X)g_2(X)$, $g_2(X) \in K[X]$ と表される．$g_1(\alpha)g_2(\alpha) = f(\alpha) = 0$, $g_1(\alpha), g_2(\alpha) \in L$ より $g_1(\alpha) = 0$ か $g_2(\alpha) = 0$ である．$f(X)$ は最小多項式なので，$g_1(\alpha) = 0$ なら $\deg f = \deg g_1$ であり，これより g_2 は定数 C となる．したがって，$f(X) = Cg_1(X)$ と書け，$f(X)$ は既約となる．$g_2(\alpha) = 0$ の場合も同様にして $f(X)$ は既約となる．

(2) $g(X) \in K[X], g(\alpha) = 0$ より，

$$g(X) = f(X)q(X) + r(X),\ q(X), r(X) \in K[X],\ \deg r < \deg f$$

または $r(X) = 0$ と表される．$g(\alpha) = f(\alpha) = 0$ より $r(\alpha) = 0$ であるが，$f(X)$ は最小多項式であるので $r(X) = 0$ となる．したがって，$f(X)|g(X)$ である．　（証明終）

定義　K を体，α, β を K の代数的な元とする．$\mathrm{Irr}(\alpha, K) = \mathrm{Irr}(\beta, K)$ であるとき，α と β は K 上**共役**である, または K 上の**共役元**である，という．また β は α の K 上の**共役元**である，という．

例　$\mathrm{Irr}(\sqrt{2}, \mathbf{Q}) = \mathrm{Irr}(-\sqrt{2}, \mathbf{Q}) = X^2 - 2$ なので，$\sqrt{2}$ と $-\sqrt{2}$ は $\mathbf{Q}$ 上共役である．

定理 43　α を体 K の拡大体の元とする．

(1)　α が K 上代数的である $\Leftrightarrow$　$K[\alpha] = K(\alpha)$ である．

(2)　α が代数的で，$\deg \mathrm{Irr}(\alpha, K) = n$ ならば，$[K(\alpha) : K] = n$ である．

証明　(1) ($\Rightarrow$) $\mathrm{Irr}(\alpha, K) = f(X)$ とおく．$g(X) \in K[X], g(\alpha) \neq 0$ とすると，$f(X) \not| g(X)$ である．$f(X)$ は既約で $f(X) \not| g(X)$ なので，系 32 より，ある多項式 $a(X), b(X) \in K[X]$ があって，$f(X)a(X) + g(X)b(X) = 1$ とすることができる．よって，$g(\alpha)b(\alpha) = 1$ となる．

$K(\alpha) \subset K[\alpha]$ を示す．$K(\alpha)$ から任意の元 z をとってくると，それは

$$z = h(\alpha)/g(\alpha) \quad (g(X), h(X) \in K[X], g(\alpha) \neq 0)$$

と書けている．よって，$z = h(\alpha)b(\alpha) \in K[\alpha]$ である．すなわち，$K(\alpha) \subset K[\alpha]$ である．逆の包含関係は明らかなので，$K(\alpha) = K[\alpha]$ が示された．

($\Leftarrow$) $\alpha = 0$ のときは明らかである．$\alpha \neq 0$ とすると $1/\alpha \in K(\alpha) = K[\alpha]$ である．したがって，$1/\alpha = a_0 + a_1\alpha + \cdots + a_n\alpha^n, a_i \in K$ と書ける．

$$g(X) = a_nX^{n+1} + \cdots + a_1X^2 + a_0X - 1$$

とおくと，$g(X) \in K[X], g(X) \neq 0, g(\alpha) = 0$．よって α は代数的である．

(2) $\mathrm{Irr}(\alpha, K) = f(X) = X^n + a_1X^{n-1} + \cdots + a_n$ とする．$1, \alpha, \cdots, \alpha^{n-1}$ は K 上 1 次独立である．なぜならば，

$$b_1 + b_2\alpha + \cdots + b_n\alpha^{n-1} = 0, b_i \in K$$

とすると，$f|(b_1 + b_2X + \cdots + b_nX^{n-1})$ であるが，しかし次数の関係から，$b_1 = \cdots = b_n = 0$ となるからである．したがって，$1, \alpha, \cdots, \alpha^{n-1}$ は拡大 $K(\alpha) \supset K$ の基底であり，$[K(\alpha) : K] = n$ である．　（証明終）

系 44　$\alpha_1, \cdots, \alpha_n$ を体 K の拡大体 L の元で，K 上代数的であるとすると，以下の (1)，(2) が成り立つ．

(1) $K(\alpha_1, \cdots, \alpha_n) = K[\alpha, \cdots, \alpha_n]$ である．

(2) $[K(\alpha_1, \cdots, \alpha_n) : K] < \infty$ である．つまり $K(\alpha_1, \cdots, \alpha_n)$ は K の代数拡大である．

証明　n に関する数学的帰納法で証明する．$n = 1$ のときは，定理 43 により正しい．$n \geq 2$ とし $n - 1$ まで成立しているとする．

$$K(\alpha_1, \cdots, \alpha_{n-1}) = K[\alpha_1, \cdots, \alpha_{n-1}] = M$$

とおくと，$[M : K] < \infty, K(\alpha_1, \cdots, \alpha_n) = M(\alpha_n)$ である．α_n は K 上代数的で $M \supset K$ なので，M 上代数的である．ゆえに，命題 43(1) より，$M(\alpha_n) = M[\alpha_n]$，$[M(\alpha_n) : M] < \infty$ である．したがって

$$K(\alpha_1, \cdots, \alpha_n) = M[\alpha_n] = K[\alpha_1, \cdots, \alpha_{n-1}, \alpha_n],$$

$$[K(\alpha_1, \cdots, \alpha_n) : K] = [M(\alpha_n) : M][M : K] < \infty$$

である．　（証明終）

命題 45　α を K 上代数的で，$f(X) = \mathrm{Irr}(\alpha, K)$ とする．このとき，$K[X]/(f(X))$ は体であり，K 同型写像 $\bar{\varphi} : K[X]/(f(X)) \to K(\alpha)$ が存在する．このとき，$\bar{\varphi}(X + f(X)) = \alpha$ である．

証明　$f(X)$ は $K[X]$ において既約なので，$f(X)$ を割るものは K の元だけである．よって，$(f(X))$ は極大イデアルである．したがって，命題 34 より，$K[X]/(f(X))$ は体である．

さて，環 $K[X]$ と環 $K(\alpha)$ の間の写像 $\varphi : K[X] \to K(\alpha)$ を，$g(X) \in K[X]$ に対して，$\varphi(g(X)) = g(\alpha)$ とする．このとき，φ は全射な準同型写像で，$\varphi|_K$ は恒等写像である．明らかに，$((f(X)) = \mathrm{Ker}\varphi$ である．よって，命題 33 より $\bar{\varphi} : K[X]/(f(X)) \to K(\alpha)$ は K 同型写像である．$\bar{\varphi}(X + f(X)) = \alpha$ であることは明らかである．　（証明終）

以下において，K, K' を体，$\sigma : K \to K'$ を同型写像とし，$K[X]$ の元 $f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n$ に対し，$f^\sigma(X) \in K'[X]$ を，

$$f^\sigma(X) = \sigma(a_0)X^n + \sigma(a_1)X^{n-1} + \cdots + \sigma(a_n)$$

と表すことにする．

命題 46　α, β を K 上代数的であるとする．このとき，以下が成り立つ．α, β が K 上共役である $\Leftrightarrow$ K 同型写像 $\sigma : K(\alpha) \to K(\beta)$, $\sigma(\alpha) = \beta$ が存在する．

証明　（$\Rightarrow$）α, β が K 上共役ならば，$f(X) = \mathrm{Irr}(\alpha, K) = \mathrm{Irr}(\beta, K)$ である．命題 45 より K 同型写像 $\tau : K[X]/(f(X)) \to K(\alpha)$ と，K 同型写像 $\eta : K[X]/(f(X)) \to K(\beta)$ が存在する．よって，$\sigma = \eta\tau^{-1}$ が求めるものとなる．$\sigma(\alpha) = \beta$ であることは明らかである．

（$\Leftarrow$）$f(X) = \mathrm{Irr}(\alpha, K)$ とすると，

$$0 = f(\alpha) = f^\sigma(\sigma(\alpha)) = f(\beta)$$

より $f(X) = \mathrm{Irr}(\beta, K)$ である．よって，α, β は K 上共役である．

（証明終）

⋆⋆⋆ エヴァリスト・ガロアについて 7

1831 年 7 月 11 日『科学学士院報告』に，ラクロアとポアッソンにより，懸賞論文に投稿されたガロアの代数方程式の代数的解法に関する論文は，理解困難なために，この論文を発表することはできないという記事が載った．ガロアは獄中において，このことを，7 月革命のときエコールポリテクニークの校長であった物理学者で，科学学士院書記であったフランソワ・アラゴの署名のある手紙から知った． ⋆⋆⋆

9.3 最小分解体とガロア拡大

ある多項式 $f(X)$ が与えられたとき，$f(X)$ をある体 L で 1 次の積に分解したい．そうすると，L には $f(x)$ の共役な元が全て含まれる．このような L は存在するのだろうか．答えは系 48 である．

定理 47 K を体とし，$f(X)$ を $K[X]$ の既約な元とする．このとき，$L = K(\alpha)$ で，α の最小多項式が $f(X)$ となるような 体 L が存在する．

証明 $I = \{fg \mid g \in K[X]\}$ とする．さらに，$L = \{h + I \mid h \in K[X]\}$ とおき. L の内部演算を

$$(g + I) + (h + I) = (g + h) + I, \quad (g + I)(h + I) = (gh) + I$$

によって定義する．明らかに L は加法でアーベル群であり，乗法においても可換である．よって，任意の $g \in K[X]$ に対し，乗法で逆元が存在すれば，L は体である．$f|g$ ならば $I = f + I = g + I$ である．$f \not| g$ ならば $f\psi + g\varphi = 1$ となる $\psi, \varphi \in K[X]$ が存在する． $(f\psi + I) + (g\varphi + I) = I$ より，$g\varphi + I = I$，すなわち，$(g + I)(\varphi + I) = I$．よって L は体である．

次に準同型写像 $\sigma : K \to L$ を $\sigma(a) = a + I$ を考える．$K \cap I = \{0\}$ なので，σ は単射である．よって a と $a+I$ を同一視することで，$K \subset L$ とみ

なせる．$X+I$ を α とおくと，$L=K[\alpha]$ である．$f(X)=a_0X^n+\cdots+a_n$ とすると，

$$\begin{aligned} 0 &= f+I=(a_0+I)(X+I)^n+\cdots+(a_n+I) \\ &= a_0\alpha^n+\cdots+a_n=f(\alpha) \end{aligned}$$

である．よって $f(X)$ は α の K 上の最小多項式である．$L=K[\alpha]$ は体なので $L=K(\alpha)$ である． （証明終）

系 48　K を体，$f(X)\in K[X]$ で $n=\deg f$ $(n\geq 1)$ とする．このとき，$f(X)$ を $L[X]$ 中で，1 次の積に分解するような K の拡大体 L が存在する．

証明　$f(X)$ は $K[X]$ で既約であるとしてよく，数学的帰納法によって証明する．$n=1$ のときは $K=L$ でよい．$n-1$ まで成り立っているとする．定理 47 より，K 上の最小多項式が $f(X)$ となるような元 α が存在する．$K(\alpha)=K_1$ とおくと，$f(X)=(X-\alpha)f_1(X)$ $(f_1(X)\in K_1[X])$ と表される．$\deg f_1=n-1$ だから，帰納法の仮定から，$L[X]$ において $f_1(X)$ は 1 次の積に分解されるような K_1 の拡大体 L が存在する．したがって $f(X)$ も 1 次の積に分解する． （証明終）

定義　K を体，L を K の代数拡大体とする．$L[X]$ において，$K[X]$ の元 $f(X)$ が，$f(X)=c(X-\alpha_1)\cdots(X-\alpha_n)$, $(c\in K,\alpha_1,\cdots,\alpha_n\in L)$ と分解されたとする (このような体 L があることは系 48 で保障されている)．$K(\alpha_1,\cdots,\alpha_n)$ を $f(X)$ の K 上の**最小分解体**という．

注意　最小分解体は K 同型の差を除いて一意的に定まることが証明されている．

例　$\mathbf{Q}(\sqrt{2})$ は, X^2-2 の $\mathbf{Q}$ 上の最小分解体である．

補題 49　K を体，$f(X) \in K[X]$, L を $f(X)$ の K 上の最小分解体とする．このとき，$[L : K] \leq n!$ である．

証明　数学的帰納法で証明する．$n = 1$ のときは，$L = K$ より明らかである．$n \geq 2$ で $n-1$ まで $[L : K]$ に関する不等式が成り立っていることを仮定する．$L = K(x_1, \cdots, x_n)$，$f(X) = c(X - x_1) \cdots (X - x_n)$ とする．$K_1 = K(x_1)$ とおくと $\mathrm{Irr}(x_1, K) | f(X)$ なので，$[K_1, K] = \deg(\mathrm{Irr}(x_1, K)) \leq n$ である．$L = K_1(x_2, \cdots, x_n)$ は $f(X)/(X - x_1)$ の K_1 上の最小分解体なので，帰納法の仮定から $[L : K_1] \leq (n-1)!$ である．よって，$[L : K] \leq n!$ である．（証明終）

命題 50　K, K' を体，$\sigma : K \to K'$ を同型写像とする．さらに，$f(X) \in K[X]$ の K 上の最小分解体を L，$f^\sigma(X) \in K'[X]$ の K' 上の最小分解体を L' とすると，σ は同型写像 $\tau : L \to L'$ に拡張される．

証明　系 44 より，$[L : K] < \infty$ である．以下，$[L : K] = m$ に関する数学的帰納法で証明する．$\sigma' : K[X] \to K'[X]$ を $\sigma'(g(X)) = g^\sigma(X)$ と定義すると，σ' は環の同型写像である．$m = 1$ のとき，$L = K$ で $L' = K'$ より，$\tau = \sigma$ であるので，命題は成り立つ．$m \geq 2$ のとき $m - 1$ まで命題は成り立っていると仮定する．$m \geq 2$ より，$f(X)$ は $K[X]$ では一次の積には分解されない．したがって，$f_1(X), f_2(X) \in K[X]$ で $\mathrm{def} f_1 \geq 2$ かつ $f_1(X)$ は $K[X]$ で既約であるものを考え，$f(X) = f_1(X) f_2(X)$ と仮定できる．このとき，

$$f^\sigma(X) = \sigma'(f_1(X) f_2(X)) = \sigma'(f_1(X)) \sigma'(f_2(X)) = f_1^\sigma(X) f_2^\sigma(X)$$

であり，$\deg f_1 = \deg f_1^\sigma$ かつ $f_1^\sigma(X)$ は $K'[X]$ は既約である．L は $f(X)$ の最小分解体であるので，$f_1(\alpha_1) = 0$ となる $\alpha \in L$ が存在する．命題 45 より K 同型写像

$$\varphi : K[X]/(f_1(X)) \to K(\alpha_1)$$

が存在する．同様に，L' は $f^\sigma(X)$ の最小分解体であるので，$f_1^\sigma(\alpha_1') = 0$ となる $\alpha' \in L'$ が存在し，命題 45 より K' 同型写像

$$\varphi' : K'[X]/(f_1^\sigma(X)) \to K'(\alpha_1')$$

が存在する．また，イデアル $(f_1(X))$ は σ' によって $(f_1^\sigma(X))$ に写像されるので，同型写像

$$\bar{\sigma}' : K[X]/(f_1(X)) \to K'[X]/(f_1^\sigma(X))$$

も定まる．したがって，

$$\sigma_1 = \varphi' \bar{\sigma}' \varphi^{-1} : K(\alpha_1) \to K'(\alpha_1')$$

は同型写像であって，$\sigma_1|_K = \sigma$ かつ $\sigma_1(\alpha_1) = \alpha_1'$ を満たす．

そこで，$K_1 = K(\alpha_1)$，$K_1' = K'(\alpha_1')$，さらに，$f_1(X) = (X - \alpha_1) f_3(X)$，$f_3(X) \in K_1[X]$ とおくと，

$$f_1^\sigma(X) = (X - \sigma_1(\alpha_1)) f_3^{\sigma_1}(X) = (X - \alpha_1') f_3^{\sigma_1}(X), \quad f_3^{\sigma_1}(X) \in K_1'[X]$$

となる．定理 43 より $[K_1 : K] = \deg\ f_1 \geq 2$ なので，$[L : K_1] < m$ である．

さて，$h(X) = f_2(X) f_3(X) \in K_1[X]$ を考えると，

$$h^{\sigma_1}(X) = f_2^\sigma(X) f_3^{\sigma_1}(X) \in K_1'[X]$$

である．そして，L は $h(X)$ の K_1 上の最小分解体であり，L' は $h^{\sigma_1}(X)$ の K_1' 上の最小分解体となる．したがって，帰納法の仮定より，$\sigma_1 : K_1 \to K_1'$ は同型写像 $\tau : L \to L'$ に拡張される．$\sigma|_K = \sigma$ より，τ は σ の拡張となる． （証明終）

定義　K を体，L を K の代数拡大体とする．L の任意の元 α に対して，α の K 上の共役元がすべて L に含まれるとき，L は K の**ガロア拡大**[†]（**ガロア拡大体**）であるという．

例　$\mathbf{Q}(\sqrt{2})$ は, $\mathbf{Q}$ のガロア拡大である．

補題 51　K を体，$f(X) \in K[X]$, L を $f(X)$ の K 上の最小分解体，L' を L の拡大体とする．σ が L から L' の中への K 上の単射準同型写像であれば，$\sigma(L) = L$ である．

[†] 一般にはこれを**正規拡大**というが，今標数 0 の体を考えているのでこれでよい．

証明　$a_0, \cdots, a_n \in K$,$\alpha_1, \cdots, \alpha_n \in L$ に対し，

$$f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n = a_0(X - \alpha_1)\cdots(X - \alpha_n)$$

とおくと，$L = K(\alpha_1, \cdots, \alpha_n)$ である．$f(\alpha_i) = 0$ $(1 \leq i \leq n)$ に写像 σ を作用させて，

$$\sigma(f(\alpha_i)) = a_0\sigma(\alpha_i)^n + a_1\sigma(\alpha_i)^{n-1} + \cdots + a_n = 0$$

を得る．したがって，各 i に対し j $(1 \leq j \leq n)$ が定まって，$\sigma(\alpha_i) = \alpha_j$ となるから，$\sigma(L) \subset L$ である．σ は K 同型写像だから K からの拡大次数は一致するので，$[\sigma(L) : K] = [L : K]$ である．$\sigma(L) \subset L$ より，$\sigma(L) = L$ である．　（証明終）

定理 52　L は K の有限次ガロア拡大である $\Leftrightarrow$ L はある $f(X)(\in K[X])$ の K 上の最小分解体である．

証明　$(\Rightarrow)$　仮定より $L = K(\alpha_1, \cdots, \alpha_n)$ と書ける．

$$\mathrm{Irr}(\alpha_i, K) = f_i(X), \quad \prod_{i=1}^{n} f_i(X) = f(X)$$

とおく．L は K のガロア拡大だから，α_i の K 上の共役元はすべて L に属する．したがって，$L[X]$ において $f_i(X) = \prod_{j=1}^{m_i}(x - \alpha_{ij})$ と分解し，$f(X) = \prod_{i,j}(x - \alpha_{ij})$ となる．ゆえに，$L = K(\alpha_{11}, \alpha_{12}, \cdots, \alpha_{nm_n})$ となり，L は $f(X)$ の K 上の最小分解体である．

$(\Leftarrow)$　L の任意の元 α に対し，α の K 上の任意の共役元 β を，L の $f(X) = \mathrm{Irr}(\alpha, K)$ の L 上の最小分解体からとる．K 上共役という仮定と命題 46 から K 同型写像 $\sigma : K(\alpha) \to K(\beta)$ $(\sigma(\alpha) = \beta)$ が存在する．L は $f(X)$ の $K(\alpha)$ 上の最小分解体であり，$L(\beta)$ は $f(X)$ の $K(\beta)$ 上の最小分解体であるから，命題 50 により，σ を同型写像 $\tau : L \to L(\beta)$ に拡張できる．τ を K 上の単射準同型写像とみると，補題 51 より $L(\beta) = \tau(L) = L$ となる．よって，$\beta \in L$ である．したがって L は K のガロア拡大である．有限次拡大であることは明らかである．　（証明終）

系 53　L を体 K の有限次ガロア拡大体，M を L と K の中間体とする．このとき，L は M の有限次ガロア拡大である．

証明　定理 52 より L は K のある $f(x)(\in K[x])$ の K 上の最小分解体なので，$L = K(\alpha_1, \cdots, \alpha_n)$ と書ける．ただし，$f(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$, $c \in K, \alpha_1, \cdots, \alpha_n \in L$ である．$K \subset M \subset L$ であり，$\alpha_1, \cdots, \alpha_n \in L$ なので，$L = K(\alpha_1, \cdots, \alpha_n) \subset M(\alpha_1, \cdots, \alpha_n) \subset L$ である．したがって，$L = M(\alpha_1, \cdots, \alpha_n)$ である．よって L は $f(x)$ の M 上の最小分解体となるので，M のガロア拡大である．　（証明終）

補題 54　K を体とするとき，既約多項式 $f(X) \in K[X]$ は K のどんな拡大体 L においても重根を持たない．

証明　$f(x)$ が重根 $\alpha \in L$ を持つと仮定する．このとき，$f'(\alpha) = 0$ である．根 α の K 上の最小多項式を $g(x)$ とすると, g は K 上既約であり，$g|f, g|f'$ である．また f も K 上既約なので，f は g の定数倍である．これより，$f|f'$ である．一方 K の標数は 0 なので，$\deg f' = \deg f - 1$ である．これは矛盾である．　（証明終）

定理 55　K を体とする．このとき，任意の有限次拡大 $K \subset L$ は，単純拡大である．

証明　L は K 上有限次拡大体なので，$L = K(\alpha_1, \cdots, \alpha_n)$ で，各 α_i は K 上代数的と仮定してよい．$n = 2$ の場合を証明すれば，結論は帰納的に導かれる．したがって，$K(\eta, \zeta)$ が単純拡大になることを示す．

$g(X)$ を η の，$h(X)$ を ζ の K 上の最小多項式とする．gh の $K(\eta, \zeta)$ 上の最小分解体を M とすれば，$M[X]$ において，g, h は共に 1 次式に分解する．すなわち，

$$g(X) = \prod_{i=1}^{k}(X - \eta_i),\ \eta_1 = \eta,\quad h(X) = \prod_{i=1}^{l}(X - \zeta_i),\ \zeta_1 = \zeta$$

となる．補題 54 より g, h は重根をもたない．ここで K の元の中から $(\eta-\eta_i)/(\zeta_j-\zeta), i=2,\cdots,k, j=2\cdots,l$ とは異なるものを選び，それを c とする．$\alpha=\eta+c\zeta$ とおくと，$h(X)$ と $\tilde{g}(X)=g(\alpha-cX)\in K(\alpha)[X]$ とは，共通根 ζ をもつ．ζ の $K(\alpha)$ 上の最小多項式を $f(X)$ とすると，$f|h, f|\tilde{g}$ となる．しかし c の選び方から $\tilde{g}$ と h の共通根は ζ のみなので，$f(x)=X-\zeta$ である．これより $\zeta\in K(\alpha)$ がいえる．また $\eta=\alpha-c\zeta\in K(\alpha)$ でもある．よって $K(\eta,\zeta)=K(\alpha)$ である．　（証明終）

命題 56　L を体 K のガロア拡大とし，α,$\beta\in L$ とする．このとき，α,β を K 上共役である $\Leftrightarrow$ $\sigma(\alpha)=\beta$ となる L の K 自己同型写像 σ が存在する．

証明　（$\Rightarrow$）命題 46 より，α と β に対して K 自己同型写像 $\tau: K(\alpha)\to K(\beta)$ が存在する．仮定より L は $f(X)\in K[X]$ の K 上の最小分解体なので，L は $f(X)$ の $K(\alpha)$ 上の最小分解体であり，$K(\beta)$ 上の最小分解体でもある．したがって，命題 50 より τ は σ に拡張される．

（$\Leftarrow$）σ を $K(\alpha)$ に制限すると，K 同型写像 $K(\alpha)\to K(\beta)$ $(\sigma(\alpha)=\beta)$ となるから，命題 46 より，α と β は共役である．　（証明終）

⋆⋆⋆ エヴァリスト・ガロアについて８

1832 年 5 月 30 日午前，ガロアは，グラシエールの池の端に倒れていた．そこを通りかかった農民（一説によれば退役軍人）によって，コシャン病院に運ばれ，銃創の治療を受ける．自宅から，弟のアルフレッドが駆けつけ，ベッドの側で泣いてしまう．ガロアは弟に向かって，「泣くんじゃないよ．２０歳で死ぬのは大変な勇気がいるんだから」と言ったと伝えられる．ガロアは死に際してのキリスト教の儀式を全て自ら断った．そして，翌朝１０時に息を引き取った．　⋆⋆⋆

10　ガロアの定理

いよいよ，ガロア理論の主たる定理へと向かっていこう．

10.1　ガロアの定理 1

定義　L を体 K のガロア拡大とする．L から L への同型写像で，その写像は K 上では恒等写像になっているものを L の K **自己同型写像**という．この L の K 自己同型写像全体は，合成を積として群をなす．この群のことを，L の K 上の**ガロア群** といい, $\mathrm{Gal}(L/K)$ と書く．

さらに，L が K のガロア拡大であって，ガロア群 $\mathrm{Gal}(L/K)$ がアーベル群であるとき，L を K の**アーベル拡大** であるという．またガロア群 $\mathrm{Gal}(L/K)$ が巡回群であるとき，L を K の**巡回拡大** であるという．

命題 57　　$|\mathrm{Gal}(L/K)| = [L : K]$

証明　L を体 K のガロア拡大とする．定理 55 より，ある $\alpha \in L$ により，$L = K(\alpha)$ と書ける．$f(X) = \mathrm{Irr}(\alpha, K)$ とおくと，定理 43 より $[L : K] = \deg f$ である．S を L における $f(X)$ の根の集合とし，$\sigma \in \mathrm{Gal}(L/K)$ に対して $\sigma(\alpha) \in S$ を対応させる写像 φ を考えると，補題 54 より $f(X)$ は重根を持たないので，φ は全単射となる．したがって，

$$|\mathrm{Gal}(L/K)| = |S| = \deg f = [L : K]$$

となる．　（証明終）

定義　体 L の自己同型部分群 G について，

$$L^G = \{\, \alpha \in L \mid \sigma(\alpha) = \alpha,\ \forall \sigma \in G \,\}$$

は，L の部分体になる．L^G を L の G による**固定体**という．

定理 58 （ガロアの定理１） 体 L を体 K の有限次ガロア拡大とする．このとき，L と K の中間体 M に対し, $M = L^{\mathrm{Gal}(L/M)}$ である．

さらに，L と K の中間体全体の集合 $\mathcal{I}$ と，$\mathrm{Gal}(L/K)$ の部分群全体の集合 $\mathcal{F}$ は，

$$\varphi : \mathcal{I} \to \mathcal{F}, M \mapsto \mathrm{Gal}(L/M), \quad \psi : \mathcal{F} \to \mathcal{I}, G \mapsto L^G$$

によって 1 対 1 に対応し，包含関係を逆にする．すなわち，$M_1 \supset M_2$ なら $\varphi(M_1) \subset \varphi(M_2)$ であり，$G_1 \supset G_2$ なら $\psi(G_1) \subset \psi(G_2)$ となる．

証明 $M \in \mathcal{I}$ に対し $\mathrm{Gal}(L/M) = G$ とおく．$L^G \supset M$ であることは明らかである， そこで，$\alpha \notin M$ かつ $\alpha \in L^G$ なる α が存在したと仮定する．しかし，命題 56 と L^G の定義より，L^G の中には α の M 上共役な元は α 以外にない．つまり $\alpha \in M$ となり仮定に矛盾する．したがって，$L^G = M$ であり，前半部分は証明された．また，同時に $\psi\varphi$ は $\mathcal{I}$ の恒等写像であることもいえた．

次に，$\varphi\psi$ は $\mathcal{F}$ の恒等写像であることを示す．$G \in \mathcal{F}$ に対し $L^G = M$ とおく．$G \subset \mathrm{Gal}(L/M)$ は明らかなので，$|G| \geq [L : M] = |\mathrm{Gal}(L/M)|$ を示せばよい．$G = \{\sigma_1, \cdots, \sigma_n\}$ とする．L は M の有限次拡大だから，定理 55 より $L = M(\alpha),\ \alpha \in L$ と書ける．

$$f(X) = \prod_{i=1}^{n} (X - \sigma_i(\alpha))$$

とおく．任意の $\sigma \in G$ に対して $\sigma G = G$，すなわち，$\{\sigma\sigma_1, \cdots, \sigma\sigma_n\} = \{\sigma_1, \cdots, \sigma_n\}$ なので，

$$f^\sigma(X) = \prod_{i=1}^{n} (X - \sigma\sigma_i(\alpha)) = f(X)$$

である．よって，$f(X)$ の解 $\sigma_1(\alpha), \cdots, \sigma_n(\alpha)$ と係数の関係式である基本対称式より，$f(X) \in L^G[X] = M[X]$ である．σ_1 を G の単位元とすると $\sigma_1(\alpha) = \alpha$ であるので，$f(\alpha) = 0$ である．したがって，$\mathrm{Irr}(\alpha, M) | f(X)$ である．よって，

$$[L : M] = \deg \mathrm{Irr}(\alpha, M) \leq \deg f(X) = n$$

であり， $G = \mathrm{Gal}(L/M)$ つまり $\varphi\psi$ は $\mathcal{F}$ の恒等写像である．よって，$\mathcal{I}$ と $\mathcal{F}$ は 1 対 1 に対応することが示された．

$M_1 \supset M_2$ なら $\varphi(M_1) \subset \varphi(M_2)$ であることを示す．$M_1 \supset M_2$ のとき，$\mathrm{Gal}(L/K)$ の元が M_1 の元を動かさなければ，当然 M_2 の元も動かさないから，$\mathrm{Gal}(L/M_1) \subset \mathrm{Gal}(L, M_2)$，すなわち，$\varphi(M_1) \subset \varphi(M_2)$ である．

最後に，$G_1 \supset G_2$ なら $\psi(G_1) \subset \psi(G_2)$ であることを示す．L の元が G_1 の元によって不変であれば，当然 G_2 の元によっても不変であるから，$L^{G_1} \subset L^{G_2}$ である．よって，$\psi(G_1) \subset \psi(G_2)$ である．　（証明終）

例　$\mathbf{Q}$ のガロア拡大 $L = \mathbf{Q}(\sqrt{2}, \sqrt{3})$ を考える．そして

$$\sigma(\sqrt{2}) = -\sqrt{2},\ \sigma(\sqrt{3}) = \sqrt{3},\ \tau(\sqrt{2}) = \sqrt{2},\ \ \tau(\sqrt{3}) = -\sqrt{3}$$

とする．このとき，$\mathrm{Gal}(L/\mathbf{Q})$ の部分群は，

$$\{e\},\ \{e, \sigma\},\ \{e, \tau\},\ \{e, \sigma\tau\}$$

であり，これらに対応する L と $\mathbf{Q}$ の中間体は，

$$L,\ \mathbf{Q}(\sqrt{3}),\ \mathbf{Q}(\sqrt{2}),\ \mathbf{Q}(\sqrt{6}),\ \mathbf{Q}$$

である．

系 59　L を K の有限次ガロア拡大とし，M を L と K との中間体とする．

(1)　$\tau \in \mathrm{Gal}(L/K)$ に対し，$\tau\mathrm{Gal}(L/M)\tau^{-1} = \mathrm{Gal}(L/\tau(M))$ となる．

(2)　M が K のガロア拡大である $\Leftrightarrow$ $\mathrm{Gal}(L/M) \lhd \mathrm{Gal}(L/K)$ である．このとき，$\mathrm{Gal}(M/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)$ である．

証明　(1) $\tau(M)$ が L と K との中間体であることは明らかである．$\tau(M)$ の元は $\tau(\alpha)(\alpha \in M)$ と表されるので，任意の $\sigma \in \mathrm{Gal}(L/M)$ に対し，

$$(\tau\sigma\tau^{-1})(\tau(\alpha)) = \tau\sigma(\alpha) = \tau(\alpha)$$

となる．よって，

$$\tau\mathrm{Gal}(L/M)\tau^{-1} \subset \mathrm{Gal}(L/\tau(M))$$

である．逆に，任意 $\rho \in \mathrm{Gal}(L/\tau(M))$ と任意の $\alpha \in M$ について

$$\rho\tau(\alpha) = \tau(\alpha)$$

だから，$\tau^{-1}\rho\tau \in \mathrm{Gal}(L/M)$ である．したがって，$\rho \in \tau\mathrm{Gal}(L/M)\tau^{-1}$ であるので，

$$\mathrm{Gal}(L/\tau(M)) \subset \tau\mathrm{Gal}(L/M)\tau^{-1}$$

がいえた．よって，$\mathrm{Gal}(L/\tau(M)) = \tau\mathrm{Gal}(L/M)\tau^{-1}$ である．

(2) ($\Rightarrow$) M が K のガロア拡大であれば，任意の $\tau \in \mathrm{Gal}(L/K)$ に対し，定理 52 と補題 51 より $\tau(M) = M$ である．(1) により

$$\tau\mathrm{Gal}(L/M)\tau^{-1} = \mathrm{Gal}(L/M)$$

だから，$\mathrm{Gal}(L/M) \lhd \mathrm{Gal}(L/K)$ である．

($\Leftarrow$) $\mathrm{Gal}(L/M) \lhd \mathrm{Gal}(L/K)$ とすると，任意の $\tau \in \mathrm{Gal}(L/K)$ に対し，

$$\mathrm{Gal}(L/\tau(M)) = \tau\mathrm{Gal}(L/M)\tau^{-1} = \mathrm{Gal}(L/M)$$

である．よって，ガロアの定理 1 より $\tau(M) = M$ である．したがって M は K のガロア拡大である．

最後に，$\mathrm{Gal}(M/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)$ を示す．$\mathrm{Gal}(L/K)$ の元 τ を M に制限したものを τ' と書くと，$\tau' \in \mathrm{Gal}(M/K)$ であって，写像

$$\varphi : \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K), \quad \varphi(\tau) = \tau'$$

は準同型写像である．命題 50 より，M の自己同型写像は L まで拡張できるから，φ は全射である．一方，

$$\begin{aligned} \mathrm{Ker}\varphi &= \{\tau \in \mathrm{Gal}(L/K) \mid \tau' \text{は } M \text{ 上では恒等写像 }\} \\ &= \{\tau \in \mathrm{Gal}(L/K) \mid \text{任意の} \alpha \in M \text{ に対し} \tau(\alpha) = \alpha\} \\ &= \mathrm{Gal}(L/M) \end{aligned}$$

となる．したがって準同型定理より $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/M) \cong \mathrm{Gal}(M/K)$ である． （証明終）

10.2　べき根拡大.

§ 4.3 において考えた有理数体 $\mathbf{Q}$ を係数とする方程式

$$x^3 + 3x + 2 = 0$$

の解法を再度検討してみる.

この方程式の解は，ステップ 1 で 2 次方程式 $Z^2 - 2Z - 1 = 0$ の解を $\sqrt{2}$ を添加して得られる $\mathbf{Q}$ の拡大体 $M = \mathbf{Q}[\sqrt{2}]$ で考え，さらにステップ 2 で，$t^3 = 1 \pm \sqrt{2}$ の解を $\sqrt[3]{1+\sqrt{2}}$ と w を添加して得られる M の拡大体 $L = M\left(\sqrt[3]{1+\sqrt{2}}, w\right)$ で考えることで，L の中に含まれることがわかった．つまり，べき根を添加して得られる拡大体の列

$$\mathbf{Q} \subset M \subset L$$

を考えることができ，そして，$f(x) = x^3 + 3x + 2$ の最小分解体 F は，$F \subset L$ となっていたのである.

定義　L を体 K の有限次拡大体とする.

(I) 次の 2 つの条件を満たすような K の拡大列がとれるとき，L は K の**広義べき根拡大（広義べき根拡大体）**である，という．特に $r = 1$ のときは単に，**べき根拡大**という.

(1)　$K = K_0 \subset K_1 \subset \cdots \subset K_r = L$

(2)　$K_i = K_{i-1}(\alpha_i), \quad \mathrm{Irr}(\alpha_i, K_{i-1}) = X^{n_i} - a_i \ \ (1 \leq i \leq r)$

(II) K の広義べき根拡大体 L を適当に選び，$F \subset L$ とできるとき，F は K 上**べき根によって構成される**，という.

上の定義によって，$f(x) = x^3 + 3x + 2$ の最小分解体 F は，$\mathbf{Q}$ 上べき根によって構成されることがいえた.

補題 60　L を体 K のガロア拡大で，$\mathrm{Gal}(L/K) = \{\, \sigma_1 = e, \sigma_2, \cdots, \sigma_n \,\}$ とする．このとき，$\alpha_1, \cdots, \alpha_n \in L$ が，任意の元 $\theta \in L$ に対して

$$\sum_{i=1}^{n} \alpha_i \sigma_i(\theta) = 0$$

を満たすならば，$\alpha_1 = \cdots = \alpha_n = 0$ である.

証明　ある α_i は 0 でないような L の元の組 $(\alpha_1, \cdots, \alpha_n)$ で，任意の $\theta \in L$ に対して，

$$\sum_{i=1}^{n} \alpha_i \sigma_i(\theta) = 0 \tag{22}$$

を仮定する．このような性質をもつ L の元の組 $(\alpha_1, \cdots, \alpha_n)$ のうち，0 の個数が最も多いものをあらためて $(\alpha_1, \cdots, \alpha_n)$ とする．$\alpha_j \neq 0$ のとき，

$$0 = \sigma_j^{-1}\left(\sum_{i=1}^{n} \alpha_i \sigma_i(\theta)\right) = \sum_{i=1}^{n} \sigma_j^{-1}(\alpha_i)\left(\sigma_j^{-1}\sigma_i(\theta)\right) \tag{23}$$

となり，$\sigma_j^{-1}\mathrm{Gal}(L/K) = \mathrm{Gal}(L/K)$ であるので，(23) は仮定 (22) と同等である．したがって，はじめから $\alpha_1 \neq 0$ としてよい．また α_1 以外にも少なくとも 1 つは 0 でない元 α_k があることに注意しよう．$\sigma_k \neq e$ なので，L の元 η で $\sigma_k(\eta) \neq \eta$ となるものがとれる．したがって，L のすべての元 θ に対し，二つの関係

$$\alpha_1\eta\theta + \alpha_2\sigma_2(\eta\theta) + \cdots + \alpha_n\sigma_n(\eta\theta) = 0 \tag{24}$$

$$\eta\left(\sum_{i=1}^{n} \alpha_i \sigma_i(\theta)\right) = \alpha_1\eta\theta + \alpha_2\eta\sigma_2(\theta) + \cdots + a_n\eta\sigma_i(\theta) = 0 \tag{25}$$

が得られる．この二つの式の差 (24)−(25) より，

$$0 \cdot \theta + \alpha_2(\sigma_2(\eta) - \eta)\sigma_2(\theta) + \cdots + \alpha_n(\sigma_n(\eta) - \eta)\sigma_n(\theta) = 0 \tag{26}$$

となる．このとき，$\alpha_k(\sigma_k(\eta) - \eta) \neq 0$ であるため，(26) は仮定 (22) と同等である．しかし，ここで得られた L の元の組

$$(0, \alpha_2(\sigma_2(\eta) - \eta), \cdots, \alpha_n(\sigma_n(\eta) - \eta))$$

は，0 の個数が最も多いと仮定していた $(\alpha_1, \cdots, \alpha_n)$ に，矛盾している．したがって，$\alpha_1 = \cdots = \alpha_n = 0$ でなければならない．　（証明終）

定理 61　体 K が 1 の原始 n 乗根 ζ （$\zeta^r \neq 1$ $(1 \leq r \leq n-1)$，$\zeta^n = 1$）を含むとする．

(1) L が K の n 次巡回拡大であれば，$L = K(\alpha)$，$\mathrm{Irr}(\alpha, K) = X^n - a$ となる α が存在する．

(2) もし $L = K(\alpha)$，$\alpha^n = a \in K$ であれば，L は K の巡回拡大である．

証明　(1) $\mathrm{Gal}(L/K) = \langle\sigma\rangle$ とする．補題 60 により，L の元で

$$\alpha = \theta + \zeta^{n-1}\sigma(\theta) + \cdots + \zeta^{n-i}\sigma^i(\theta) + \cdots + \zeta\sigma^{n-1}(\theta) \neq 0$$

となるものがとれる．したがって

$$\begin{aligned}\sigma(\alpha) &= \sigma(\theta) + \zeta^{n-1}\sigma^2(\theta) + \cdots + \zeta\theta \\ &= \{\theta + \zeta^{n-1}\sigma(\theta) + \cdots + \zeta\sigma^{n-1}(\theta)\}\zeta \\ &= \alpha\zeta\end{aligned}$$

である．よって，$\sigma^i(\alpha) = \alpha\zeta^i$ であり，とくに $i = 0, 1, \cdots, n-1$ に対し，$\sigma^i(\alpha)$ は相異なるものである．ところで，α の K 上の最小多項式を $q(X)$ とすると，$\deg q(X) = [K(\alpha) : K] \leq [L : K] = n$ である．一方 $q(\alpha) = 0$ より $q(\sigma^i(\alpha)) = 0$ であり，$q(X) = 0$ は相異なる根を n 個もつ．すなわち，$\deg q(X) = n$ で $L = K(\alpha)$ となる．また

$$\sigma^i(\alpha^n) = (\sigma^i(\alpha))^n = (\alpha\zeta^i)^n = \alpha^n$$

だから，$\alpha^n = a$ は K の元であり，この α が $X^n - a \in K[X]$ の根である．

(2) $X^n - a = (X-\alpha)(X-\alpha\zeta)\cdots(X-\alpha\zeta^{n-1})$ であって，$\alpha, \alpha\zeta, \cdots, \alpha\zeta^{n-1}$ は相異なるから，$L = K(\alpha)$ は $X^n - a$ の最小分解体である．よって，L は K のガロア拡大である．したがって，命題 57 より $\mathrm{Gal}(L/K) = n$ である．さらに，α の K 上の共役元は，$\{\alpha, \alpha\zeta, \cdots, \alpha\zeta^{n-1}\}$ に含まれる．$\sigma_i \in \mathrm{Gal}(L/K)$ を $\sigma_i(\alpha) = \alpha\zeta^i$ で定義すると，写像

$$\varphi : \mathrm{Gal}(L/K) \to \{1, \zeta, \cdots, \zeta^{n-1}\}, \quad \varphi(\sigma_i) = \zeta^i$$

が得られる．明らかに，φ は群の準同型写像で単射である．$\{1, \zeta, \cdots, \zeta^{n-1}\}$ は巡回群なので，$\mathrm{Gal}(L/K)$ も巡回群となる．よって L は K の巡回拡大である．　（証明終）

補題 62　ζ を 1 の原始 n 乗根とする．$1 \leq a \leq n-1$ なる自然数 a について，a が n と互いに素ならば，ζ^a は 1 の原始 n 乗根であり，そうでなければ，ζ^a は 1 の原始 n 乗根ではない．

証明　a が n と互いに素でないとき，a は n と公約数をもつので，それを $d > 1$ とすると，$(\zeta^a)^{n/d} = (\zeta^n)^{a/d} = 1$ となり，ζ^a は 1 の原始 n 乗根ではない．a が n と互いに素であるとき，$(\zeta^a)^m = 1$ であれば，$n|am$ より，$n|m$ である．したがって，この場合，ζ^a は 1 の原始 n 乗根である．
（証明終）

定理 63　K を体とし，ζ を K の拡大体に含まれている 1 の原始 n 乗根とする．このとき，$K(\zeta)$ は K のアーベル拡大である．

証明　$\mathbf{Z}/n\mathbf{Z}$ の単元全体を $G = \{\bar{i}_1, \bar{i}_2, \cdots, \bar{i}_h\}$ とすると，補題 62 より，1 の原始 n 乗根は，$\zeta^{i_1}, \cdots, \zeta^{i_h}$ の h 個である．

$1 \leq n' < n$ について，1 の原始 n' 乗根は $X^{n'} - 1 = 0$ の根であり，ζ はそうではないから，ζ は原始 n' 乗根と共役では有り得ない．すなわち，ζ の K 上の共役元は $\{\zeta^{i_1}, \cdots, \zeta^{i_h}\}$ に含まれる．また $K(\zeta)$ は K 上 $X^n - 1$ の最小分解体だから，ガロア拡大である．ζ^{i_r} が ζ の K 上の共役元であるとき，$\mathrm{Gal}(K(\zeta)/K) \ni \sigma_r$ を $\sigma_r(\zeta) = \zeta^{i_r}$ と定義する $(1 \leq r \leq h)$．$\sigma_r\sigma_s(\zeta) = \sigma_r(\zeta^{i_s}) = \zeta^{i_r i_s}$ であるから，写像

$$\mathrm{Gal}(K(\zeta)/K) \to G, \quad \sigma_r \mapsto \bar{i}_r$$

は群の単射準同型である．G は可換群だから，$\mathrm{Gal}(K(\zeta)/K)$ も可換であり，したがって，$K(\zeta)$ は K のアーベル拡大である．
（証明終）

10.3　ガロアの定理２（方程式の可解性）

定義　K を体，$f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n$ $(a_0 \neq 0)$ を K 係数の多項式とし，$f(X)$ の $\mathbf{Q}(a_1/a_0, \cdots, a_n/a_0)$ 上の最小分解体を L とする．

L が $\mathbf{Q}(a_1/a_0, \cdots, a_n/a_0)$ 上べき根によって構成されるとき，

「方程式 $f(X) = 0$ は**べき根によって解ける**，または**代数的に解ける**」

という．

定義　$f(X)=X^n+a_1X^{n-1}+\cdots+a_n$，$K=\mathbf{Q}(a_1,\cdots,a_n)$ とし，L を K 上の $f(X)$ の最小分解体とする．このとき，$\mathrm{Gal}(L/K)$ を**方程式 $f(X)=0$ のガロア群**，または，**多項式 $f(X)$ のガロア群**という．多項式 $f(X)$ のガロア群を $\mathrm{Gal}_K(f)$ と表す．

命題 64　K を体，体 L を K のガロア拡大，M を K の拡大体とする．このとき，L の元と M の元の有限和（n 個の和）全体の集合

$$LM=\left\{\sum_i^n \alpha_i\beta_i \mid \alpha_i\in L,\ \beta_i\in M\right\}$$

は体であり，M のガロア拡大である．

証明　まず，LM が体であることを示す．そのためには，$x\in LM$, $z\neq 0$ が単元であればよい．$x=\sum_{i=1}^{n}\alpha_i\beta_i$ とする．α_i は M 上代数的だから，体 $M_1=M(\alpha_1,\cdots,\alpha_n)$ を考えると，$x\in M_1$ である．よって，$x^{-1}\in M$ である．系 44 より，$M_1=M[\alpha_1,\cdots,\alpha_n]$ であったので，x^{-1} は $\alpha_1,\cdots,\alpha_n$ の M を係数とする多項式で表される．したがって，$x^{-1}\in LM$ である．

次に，LM が K のガロア拡大であることを示す．L は K のガロア拡大なので，ある $f(X)\in K[X]$ の最小分解体である．よって，$f(X)=(X-\alpha_1)\cdots(X-\alpha_n)$ としたとき，$L=K(\alpha_1,\cdots,\alpha_n)$ となる．したがって，

$$LM=M(\alpha_1,\cdots,\alpha_n)$$

となる．これは LM が $f(X)$ の M 上の最小分解体であることを意味する．よって，LM は M のガロア拡大である．　（証明終）

命題 65　K を体，$f(X)\in K[X]$ とする．M を K の拡大体とするとき，$\mathrm{Gal}_M(f)$ は $\mathrm{Gal}_K(f)$ の部分群に同型である．

証明　L を $f(X)$ の K 上の最小分解体とすると，命題 64 より LM は M のガロア拡大となる．したがって，$\mathrm{Gal}(LM/M) = \mathrm{Gal}_M(f)$ である．

さて，ガロア群 $G = \mathrm{Gal}(LM/M) = \mathrm{Gal}_M(f)$ の元 σ の L への制限 $\sigma|_L$ を考える．$\sigma|_L$ はもちろん K の元を固定するので，単射準同型写像

$$\varphi : G = \mathrm{Gal}(LM/M) \to \mathrm{Gal}(L/K), \quad \varphi(\sigma) = \sigma|_L$$

が得られる．よって，$H = \mathrm{Im}\varphi$ として，$L^H = L \cap M$ が示されれば，φ が単射であることから，

$$\mathrm{Gal}_M(f) = \mathrm{Gal}(LM/M) \cong H = \mathrm{Gal}(L/L \cap M) \subset \mathrm{Gal}_K(f)$$

が得られ，命題は示される．

$L^H = L \cap M$ を示す．任意の $\tau \in H$ は，$\tau = \sigma|_L$ $(\sigma \in \mathrm{Gal}(LM/M))$ と表される．よって，$x \in L \cap M$ は $\tau(x) = \sigma|_L(x) = x$ であるので $x \in L^H$，すなわち，$L \cap M \subset L^H$ がいえる．$L \cap \bar{M} \not\subset L^H$ を示す．$\beta \in L$, $\beta \notin M$ とする．このとき，適当な $\sigma \in \mathrm{Gal}(LM/M)$ によって，$\sigma(\beta) \neq \beta$ となる．$\sigma|_L = \tau$ とおけば，$\tau(\beta) \neq \beta$ である．よって，$L \cap \bar{M} \not\subset L^H$ である．したがって，$L \cap M = L^H$ が示された．　（証明終）

命題 66　K を体，L を K の拡大体，L_1, L_2 を L と K の中間体とする．L_1, L_2 が K の有限次アーベル拡大であれば，L_1L_2 も K の有限次アーベル拡大である．

証明　L_1, L_2 は K の有限次アーベル拡大なので，命題 64 より，L_1L_2 は L_2 のガロア拡大なので，K のガロア拡大でもある．$G = \mathrm{Gal}(L_1L_2/K)$，$H_1 = \mathrm{Gal}(L_1L_2/L_1)$ とおく．L_1 は K のガロア拡大だから，系 59 より，$H_1 \lhd G$ であり，$\mathrm{Gal}(L_1/K) \cong G/H_1$ となる．$\mathrm{Gal}(L_1/K)$ はアーベル群より，G/H_1 もアーベル群である．

さて，命題 12 より，$H_1 \lhd G$ かつ G/H_1 がアーベル群だから，$[G, G] \subset H_1$ である．$H_2 = \mathrm{Gal}(L_1L_2/L_2)$ とおくと，同様にして，$[G, G] \subset H_2$ もわかる．

L_1L_2 と K の中間体で $[G, G]$ に対応するものを M とすれば，上の包含関係と定理 58（ガロアの定理 1 ）から，$M \supset L_1$ であり，$M \supset L_2$ でもある．よって，$M \supset L_1L_2$ でとなり，$M = L_1L_2$ がいえる．したがって，

$[G,G]=\{e\}$ である．これは，全ての $a,b\in G$ に対して $aba^{-1}b^{-1}=e$ ということ，つまり $ab=ba$ である．よって G はアーベル群である．したがって，L_1L_2 は K の有限次アーベル拡大である．　　（証明終）

定理 67 体 L' を K の広義べき根拡大とし，L は L' の部分体とする．このとき，L'' を L' を含む K の有限次ガロア拡大で，$\mathrm{Gal}(L''/K)$ が可解群となるような L'' が存在する．

証明　L' は K の広義べき根拡大より，

$$K=K_0\subset K_1\subset\cdots\subset K_r=L'$$

$$K_i=K_{i-1}(\alpha_i),\ \ \mathrm{Irr}(\alpha_i,K_{i-1})=X^{n_i}-a_i\ \ (1\leq i\leq r)$$

となっている．定理を満たす体 L'' の存在を，r に関する数学的帰納法によって示す．

$r=1$ の場合．$n_1=n,\ a_1=a,\ \alpha_1=\alpha$ とおくと，

$$L'=K(\alpha),\ \ \mathrm{Irr}(\alpha,K)=X^n-a$$

である．$\zeta\in\mathbf{C}$ を 1 の原始 n 乗根の 1 つとし，$L''=L'(\zeta)$ とおく．このとき，L'' は X^n-a の K 上の最小分解体，すなわち，L'' は K のガロア拡大である．定理 61 より $L''=K(\zeta,\alpha)$ は $K(\zeta)$ の巡回拡大であり，また，定理 63 より $K(\zeta)$ は K のアーベル拡大である．

L'' は K のガロア拡大であること，$K(\zeta)$ が L'' と K との中間体であることと，系 59 から，$\mathrm{Gal}(L''/K)\rhd\mathrm{Gal}(L''/K(\zeta))\rhd\{e\}$ で，

$$\mathrm{Gal}(L''/K)/\mathrm{Gal}(L''/K(\zeta))\cong\mathrm{Gal}(K(\zeta)/K),\ \ \mathrm{Gal}(L''/K(\zeta))$$

はともにアーベル群である．したがって，命題 21 より $\mathrm{Gal}(L''/K)$ は可解群である．

$r\geq 2$ の場合．$r-1$ まで成り立っているとする．したがって，K_{r-1} を含む K の有限次ガロア拡大 M を，ガロア群 $\mathrm{Gal}(M/K)$ が可解となるように選ぶことができることを仮定する．簡単のために，$n_r=n,\ a_r=a,\ \alpha_r=\alpha$，$K_{r-1}=K'$ とおき，$\mathrm{Irr}(\alpha,K')=X^n-a$ となる α を $\sqrt[n]{a}$ と書く．すなわち，$L'=K_r=K'(\sqrt[n]{a})$ とする．ζ を 1 の原始 n 乗根の 1 つとすると，

定理 63 より $M(\zeta)$ は M のアーベル拡大で，K のガロア拡大である．系 59 により $\mathrm{Gal}(M(\zeta)/K) \rhd \mathrm{Gal}(M(\zeta)/M))$ で

$$\mathrm{Gal}(M(\zeta)/K)/\mathrm{Gal}(M(\zeta)/M) \cong \mathrm{Gal}(M/K)$$

であり，仮定によりこれは可解群である．さらに，$\mathrm{Gal}(M(\zeta)/M)$ はアーベル群より可解群である．よって，命題 21 より $\underline{\mathrm{Gal}(M(\zeta)/K) \text{ は可解群}}$ である．

さて，$\mathrm{Gal}(M/K) = \{\sigma_1, \cdots, \sigma_m\}$ の任意の元 σ_j について，$X^n - \sigma_j(a)$ は $\sigma_j(K')[X]$ において既約である $(\sigma_j(a) \in M)$．その M 上の分解体における零点の一つを $\sqrt[n]{\sigma_j(a)}$ と書くことにすると，

$$X^n - \sigma_j(a) = \prod_{i=0}^{n-1} \left(X - \sqrt[n]{\sigma_j(a)}\zeta^i \right)$$

と表され，定理 61 により $M\left(\zeta, \sqrt[n]{\sigma_j(a)}\right)$ は $M(\zeta)$ の巡回拡大であるので，アーベル拡大である．一方，

$$g(X) = \prod_{j=1}^{m} \left(X^n - \sigma_j(a) \right)$$

の M 上の最小分解体は，

$$M\left(\zeta, \sqrt[n]{\sigma_1(a)}, \cdots, \sqrt[n]{\sigma_m(a)}\right)$$

であるので，これを L'' とおく．命題 66 より $\underline{L'' \text{ は } M(\zeta) \text{ のアーベル拡大}}$ である．

$\mathrm{Gal}(M/K)$ の任意の元 σ に対し $\{\sigma\sigma_1, \cdots, \sigma\sigma_m\} = \mathrm{Gal}(M/K)$ であり，$g(X)$ の係数は $\sigma_1(a), \cdots, \sigma_m(a)$ と基本対称式を作るので，$g(X) \in K[X]$ となる．よって，L'' は K の最小分解体，つまり，$\underline{L'' \text{ は } K \text{ のガロア拡大}}$ である．$L'' \supset L'$ であることは明らかである．

L'' は K のガロア拡大であること，$M(\zeta)$ は L'' と K との中間体であることと，系 59 から，$\mathrm{Gal}(L''/K) \rhd \mathrm{Gal}(L''/M(\zeta)) \rhd \{e\}$ で，

$$\mathrm{Gal}(L''/K)/\mathrm{Gal}(L''/M(\zeta)) \cong \mathrm{Gal}(M(\zeta)/K)$$

がいえる．$\mathrm{Gal}(M(\zeta)/K)$ が可解群より，$\mathrm{Gal}(L''/K)/\mathrm{Gal}(L''/M(\zeta))$ である．そして，$\mathrm{Gal}(L''/M(\zeta))$ はアーベル群であるから可解群である．したがって $\mathrm{Gal}(L''/K)$ も可解群である．すなわち r のときも成り立つ．

（証明終）

定理 68 （ガロアの定理２）　K を体とし，$f(X) \in K[X]$ とする．このとき，方程式 $f(X) = 0$ が代数的に解ける $\Leftrightarrow$　$f(X)$ のガロア群が可解群である．

証明　$f(X) = X^n + c_1X^{n-1} + \cdots + c_n = (X - \alpha_1)\cdots(X - \alpha_n)$ とし，$\mathbf{Q}(c_1, \cdots, c_n)$ を改めて K とおき，$L = K(\alpha_1, \cdots, \alpha_n)$ とおく．このとき，$f(X) = 0$ が代数的に解けるとは, L が K 上べき根によって構成されることなので，方程式 $f(X)$ のガロア群 $\mathrm{Gal}(L/K)$ について，

"L が K 上べき根によって構成される．$\Leftrightarrow$ $\mathrm{Gal}(L/K)$ が可解群である."

ことを証明すればよい．

($\Rightarrow$)　仮定により，$L \subset L'$ である体 L' が存在し，

$$K = K_0 \subset K_1 \subset \cdots \subset K_r = L',$$

$$K_i = K_{i-1}(\alpha_i), \quad \mathrm{Irr}(\alpha_i, K_{i-1}) = X^{n_i} - a_i \ (1 \leq i \leq r)$$

となっている．このとき，定理 67 により，L'' を L' を含む K の有限次ガロア拡大で，$\mathrm{Gal}(L''/K)$ が可解群となるような L'' が存在する．系 59 より，$\mathrm{Gal}(L''/K) \rhd \mathrm{Gal}(L''/L)$ で，

$$\mathrm{Gal}(L''/K)/\mathrm{Gal}(L''/L) \cong \mathrm{Gal}(L/K)$$

である．命題 21 より，$\mathrm{Gal}(L''/K)$ が可解なので，$\mathrm{Gal}(L''/L)$ も可解群であり，$\mathrm{Gal}(L''/K)/\mathrm{Gal}(L''/L)$ も可解群である．よって，$\mathrm{Gal}(L/K)$ は可解群である．

($\Leftarrow$)　$n = |\mathrm{Gal}(L/K)|$ に関する帰納法で証明する．$n = 1$ のときは, 明らかに正しい．n 未満の位数の可解群をガロア群としてもつ多項式は，べき根によって解けるとする．M を $X^n - 1$ の K 上の最小分解体とする．定理 63 より，M は K のアーベル拡大である．よって $\mathrm{Gal}(M/K)$ はアーベル群である．$X^n - 1 = (X - 1)(X^{n-1} + \cdots + X + 1)$ であるので，$|\mathrm{Gal}(M/K)| < n$ となる．よって，帰納法の仮定より広義べき根拡大 $\tilde{M} \supset K$ が存在し，$M \subset \tilde{M}$ である．$\tilde{L}$ を $f(X)$ の $\tilde{M}$ 上の最小分解体とすると，$L \subset \tilde{L}$ である．命題 65 より $\mathrm{Gal}(\tilde{L}/\tilde{M})$ は $\mathrm{Gal}(L/K)$ の部分群と同型だから，$\mathrm{Gal}(\tilde{L}/\tilde{M})$ も可解群である．そこで，$G = \mathrm{Gal}(\tilde{L}/\tilde{M})$ とおき，組成列 $G = G_0 \supset G_1 \supset \cdots \supset G_r = \{e\}$ を考える．$\mathrm{Gal}(\tilde{L}/\tilde{M})$ は可解群

だから，命題 22 より G_{i-1}/G_i は素数 p_i 次の巡回群である．各 G_i に対応する $\tilde{L}$ と $\tilde{M}$ の中間体を L_i とすると，$\tilde{M} = L_0 \subset L_1 \subset \cdots \subset L_r = \tilde{L}$ であって，L_i は L_{i-1} の p_i 次の巡回拡大である $(1 \leq i \leq r)$．よって定理 61 より，L_i は L_{i-1} のべき根拡大である $(1 \leq i \leq r)$．したがって，

$$K \subset \tilde{M} \subset L_1 \subset \cdots \subset L_r = \tilde{L}$$

は広義べき根拡大である．$L \subset \tilde{L}$ より，L は K 上べき根によって構成された． （証明終）

10.4 最終セクション

いよいよ方程式に関するガロア理論の最終段階に入る．結論は,「5 次以上の方程式は，一般に代数的に解くことは出来ない」ということである．その証明のポイントになる定理は「n 次多項式のガロア群は，n 次対称群と同型である」というものである．したがって，今上で証明したガロアの定理 2 により，5 次以上のガロア群は可解群でないことがわかり，ゆえに，5 次以上の方程式は，一般に代数的に解くことは出来ないという結論に至る．改めて，基本対称式の定義を述べよう．

定義 K を体，$f(X_1, \cdots, X_n) \in K[X_1, \cdots, X_n]$ とする．このとき，$\sigma \in S_n$ の $K[X_1, \cdots, X_n]$ への作用を

$$(\sigma f)(X_1, \cdots, X_n) = f(X_{\sigma(1)}, \cdots, X_{\sigma(n)})$$

で定義する．さらに，すべての置換 $\sigma \in S_n$ について，$\sigma f = f$ が成立しているとき，f は**対称式**であるという．特に，次の式 $s_1, \cdots, s_n$ を**基本対称式**という．

$$\begin{aligned}
s_1 &= X_1 + \cdots + X_n \\
s_2 &= X_1X_2 + \cdots + X_{n-1}X_n \\
&\cdots \\
s_k &= \sum_{i_1 < \cdots < i_k} X_{i_1} \cdots X_{i_k} \\
&\cdots \\
s_n &= X_1 \cdots X_n
\end{aligned}$$

注意　2 次方程式 $X^2+aX+b=0$ の解を α,β とすると，$\alpha+\beta=-a$ $\alpha\beta=b$ であった．任意の i に対して，$s_i=s_i(\alpha_1,\cdots,\alpha_n)$ とすると，基本対称式は n 次方程式の解と係数の関係を表し，

$$(X-\alpha_1)\cdots(X-\alpha_n)=X^n-s_1X^{n-1}+\cdots+(-1)^ns_n$$

が成り立つ．

命題 69　n 変数の対称式は $f(X_1,\cdots,X_n)$ は，次の性質をもつ．

(1) f が $\alpha X_1^{i_1}\cdots X_n^{i_n}$ という項を含んでいるならば，$1,\cdots,n$ を任意に並べ替えた $j_1,\cdots,j_n$ について，f は $\alpha X_{j_1}^{i_1}\cdots X_{j_n}^{i_n}$ という項を含む．

(2) X_n が f の因数ならば，s_n は f の因数である．

証明　(1) f が $\alpha X_1^{i_1}\cdots X_n^{i_n}$ という項を含んでいるとする．このとき，各 k について，$\sigma(k)=j_k$ となる $\sigma\in S_n$ を考えると，

$$\sigma f=\alpha X_{j_1}^{i_1}\cdots X_{j_n}^{i_n}+\cdots$$

であり，$\sigma f=f$ より，f にも $\alpha X_{j_1}^{i_1}\cdots X_{j_n}^{i_n}$ が含まれる．

(2) $f=gX_n$ とする．各 i について $\sigma=(in)$ とおくと，$f=\sigma f=(\sigma g)X_i$ となるので，X_i は f の因子である．よって，s_n は f の因子である．

（証明終）

定理 70　対称式について，以下が成り立つ．

(1) $K[X_1,\cdots,X_n]$ の任意の対称式は，基本対称式の多項式で表される．

(2) $f(X_1,\cdots,X_n)=P(s_1,\cdots,s_n)=Q(s_1,\cdots,s_n)$ ならば $P=Q$ である．

証明　(1) f の次数を d とし，n と f の d に関する二重帰納法で示す．すべての d について，$n=1$ の場合は明らかに成り立つ．また，すべての n について，$d=0$ の場合も明らかに成り立つ．そこで,「すべての d について，変数の個数が $n-1$ まで成り立っている」，および,「すべての n について，f の次数が $d-1$ まで成り立っている」ことを仮定する．

$1\le i\le n-1$ について，$\bar{s}_i=s_i(X_1,\cdots,X_{n-1},0)$ とすると，$\bar{s}_i$ は $K[X_1,\cdots,X_{n-1}]$ の基本対称式である．$f(X_1,\cdots,X_{n-1},0)$ は $n-1$ 変数

の対称式であるので,「すべての d について，変数の個数が $n-1$ まで成り立っている」という帰納法の仮定から，

$$f(X_1, \cdots, X_{n-1}, 0) = P(\bar{s}_1, \cdots, \bar{s}_{n-1})$$

となる多項式 P が存在する．ここで，$\deg P \leq d$ に注意する．そして，

$$g(X_1, \cdots, X_n) = f(X_1, \cdots, X_n) - P(\bar{s}_1, \cdots, \bar{s}_{n-1})$$

を考える．明らかに g は対称式であり，$g(X_1, \cdots, X_{n-1}, 0) = 0$ でもある．よって，g は X_n を因子にもつ．したがって，命題 69(2) より，s_n は g の因子となる．よって，$g = s_n h$ と表され，h は対称式である．さらに，$\deg P \leq d$ より $\deg h < d$ である.「すべての n について，次数が $d-1$ まで成り立っている」という帰納法の仮定から，$h = Q(s_1, \cdots, s_n)$ となる多項式 Q が存在する．したがって，$R(s_1, \cdots, s_n) = P(\bar{s}_1, \cdots, \bar{s}_{n-1}) + s_n Q(s_1, \cdots, s_n)$ とおくと，f は多項式 $R(s_1, \cdots, s_n)$ より $f = R(s_1, \cdots, s_n)$ と表される．

(2) $H = P - Q$ と置いて，$H(s_1, \cdots, s_n) = 0$ ならば $H = 0$ であることを，変数の個数 n に関する帰納法で示す．勿論，H は対称式である．$n = 1$ のときは $f(X_1) = P(X_1) = Q(X_1)$ より，$H = 0$ であることは明らかである．変数の個数が $n-1$ まで成り立っていると仮定する．そして，$H(X_1, \cdots, X_n)$ を $H(s_1, \cdots, s_n) = 0$ を満たす $H \neq 0$ である次数最小の多項式として，矛盾を導く．$H(s_1, \cdots, s_n) = 0$ において，$X_n = 0$ とすると，$H(\bar{s}_1, \cdots, \bar{s}_{n-1}, 0) = 0$ である．よって，帰納法の仮定から $H = 0$ である．これは，X_n が H の因子であることを意味し，命題 69(2) より，s_n も H の因子となり，$H = s_n G$ と表すことができる．よって，$H(s_1, \cdots, s_n) = 0$ は，$s_n G(s_1, \cdots, s_n) = 0$ を意味する．$s_n \neq 0$ であるため，$G(s_1, \cdots, s_n) = 0$ である．しかし，$G \neq 0$ で $\deg G < \deg H$ であることは，H の次数最小性に矛盾する．（証明終）

命題 71　体 K 上の有理関数体 $K(x_1,\cdots,x_n)$ について，$K(s_1,\cdots,s_n)$ の拡大体 $K(x_1,\cdots,x_n)$ は，多項式 $f(X)=X^n-s_1X^{n-1}+\cdots+(-1)^ns_n$ の体 $K(s_1,\cdots,s_n)$ 上の最小分解体であり，

$$\mathrm{Gal}_{K(s_1,\cdots,s_n)}(f)\cong S_n$$

である．ここで，$\{s_1,\cdots,s_n\}$ は $\{x_1\cdots,x_n\}$ の基本対称式である．

証明　多項式 $f(X)=\prod_{i=1}^{n}(X-x_i)$ の根の集合は $\{x_1,\cdots,x_n\}$ である．したがって，$L=K(x_i,\cdots,x_n)$ は $f(X)$ の $K_s=K(s_1,\cdots,s_n)$ 上の最小分解体である．$\sigma\in S_n$ に対して，根の置換 $\sigma(X_i)$ を $X_{\sigma(i)}$ と定義し，写像

$$\Psi:K(x_1\cdots,x_n)\to K(x_1,\cdots,x_n)$$
$$\Psi\left(\varphi(x_1,\cdots,x_n)\right)=\varphi(x_{\sigma(1)},\cdots,x_{\sigma(n)})$$

を考えると，Ψ は，K_s 自己同型写像である．よって $[L:K_s]\geq|S_n|=n!$ である．一方，L は K_s の最小分解体なので，補題 49 より，$[L:K_s]\leq n!$ である．したがって，$\mathrm{Gal}(L/K_s)\cong S_n$，すなわち

$$\mathrm{Gal}_{K(s_1,\cdots,s_n)}(f)\cong S_n$$

である．　（証明終）

元 $\alpha_1,\cdots,\alpha_n$ が K 上**代数的に独立**であるとは，すべての零でない n 変数多項式 $f(X_1,\cdots,X_n)\in K[X_1,\cdots,X_n]$ について，$f(\alpha_1,\cdots,\alpha_n)\neq 0$ であることをいう．簡単にいえば，$\alpha_1,\cdots,\alpha_n$ は不定元ということである．

準備は全て整った．最後の定理を述べよう．

定理 72　$t_1, \cdots, t_n$ を $\mathbf{Q}$ 上代数的独立な元とする．$n \geq 5$ のとき，n 変数有理関数体 $\mathbf{Q}(t_1, \cdots, t_n)$ 上の多項式 $f(X) = X^n + t_1 X^{n-1} + \cdots + t_n$ はべき根によって解くことはできない．つまり 5 次以上の方程式の解の公式は存在しない．

証明　$f(X) = X^n + t_1 X^{n-1} + \cdots + t_n = (X - \alpha_1) \cdots (X - \alpha_n)$ とし，$K = \mathbf{Q}(t_1, \cdots, t_n)$, $L = \mathbf{Q}(\alpha_1, \cdots, \alpha_n)$ とおく．n 変数有理関数体 $\mathbf{Q}(X_1, \cdots, X_n)$ を L' とし，$g(X) = X^n + s_1 X^{n-1} + \cdots + s_n$ とする．ここで, $s_1, \cdots, s_n$ は $X_1, \cdots, X_n$ の基本対称式とする．$K' = \mathbf{Q}(s_1, \cdots, s_n)$ とおく．L, L' は それぞれ $f(X), g(X)$ の K, K' 上の最小分解体だから K, K' 上のガロア拡大である．

$\mathbf{Q}[X_1, \cdots, X_n]$ から $\mathbf{Q}[\alpha_1, \cdots, \alpha_n]$ への写像 Φ を $\Phi(f) = f(\alpha_1, \cdots, \alpha_n)$ で定義すれば，Φ は環の準同型写像である．$\mathrm{Ker}(\Phi) = \{0\}$ ということと，$\alpha_1, \cdots, \alpha_n$ が $\mathbf{Q}$ 上代数的に独立であることは同値であるので Φ は単射である．勿論全射でもあるので，環の同型 $\mathbf{Q}[X_1, \cdots, X_n] \cong \mathbf{Q}[\alpha_1, \cdots, \alpha_n]$ が成立する．そして $\mathbf{Q}(X_1, \cdots, X_n)$ から $\mathbf{Q}(\alpha_1, \cdots, \alpha_n)$ の写像 Ψ を $\Psi(g/f) = \Phi(g)\Phi(f)^{-1}$ とおくことで，体の同型 $\mathbf{Q}(X_1, \cdots, X_n) \cong \mathbf{Q}(\alpha_1, \cdots, \alpha_n)$ も成立する．したがって，$\mathrm{Gal}(L/K) \cong \mathrm{Gal}(L'/K')$ が成り立つ．さらに命題 71 により，$\mathrm{Gal}(L'/K') \cong S_n$ なので，$\mathrm{Gal}(L/K) \cong S_n$ である．$n \geq 5$ のとき，S_n は可解群ではないので，ガロアの定理 2 より，$X^n + t_1 X^{n-1} + \cdots t_n = 0$ は代数的に解けないことが証明された．　（証明終）

⋆⋆⋆ エヴァリスト・ガロアについて 9

最後に，ガロアが書いたオーギュスト・シュヴァリエへの遺書の最初の部分を紹介する．

親しい友よ．

僕は解析でいくつか新しいことをしました．そのうちのいくつかは方程式論に関するもので，他は積分関数に関するものです．

方程式論では，方程式がどういう場合に根号で解けるかを調べましたが，その機会にこの理論をもっと深く掘り下げ，根号で解けない場合でも，方程式のすべての可能な変形が記述できるようになりました．

これらの研究全体から三つの論文を書くことができるでしょう．

その第 1 の論文はもうできています．ポアッソンはそれについて何か（説明が不十分であるなどと）言っていますが，僕はそれを訂正しましたので，それさへつけ加えればそれでよいと思います．

第 2 の論文は，方程式論のかなりおもしろい応用を含むものです．· · ·

⋆⋆⋆

参考文献

[1] 彌永昌吉, 有馬哲，浅枝陽, 代数入門, 東京図書.

[2] 酒井文雄, 環と体の理論, 共立出版.

[3] 石田信, 代数入門, 実況出版株式会社.

[4] 松田修, ベクトル空間からはじめる抽象代数入門, 森北出版.

[5] 彌永昌吉, ガロアの時代　ガロアの数学　第一部時代編, シュプリンガー・フェアラーク東京.

Present Address:
Osamu Matsuda
National Institute of Technology, Tsuyama College
624-1, Numa, Tsuyama-City, Okayama, Japan, 708-8509
e-mail : matsud @ tsuyama-ct.ac.jp