ガロア理論入門ノート（詳細）

Osamu MATSUDA

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．ガロア理論といって先ず思い出す有名な定理は,「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「解くことは不可能である」ということを証明したのも, ガロアが初めてであるといわれている．

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, カルダー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 次以上の方程式の中には, 代数的に解けないものがある．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．これは現代流に言えば,「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 21 歳のとき, 恋人をめぐる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 10 代の時に考えたものであるということだ．しかしこの理論は現在の私達にも, なんともいえない数学の美しさを与えてくれる．

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] の中の命題, 証明等を参考に構成した.

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

Contents

1　群について

1.1　群の定義

ガロアのとった方法は方程式の群を考えることである．群の定義から始める．

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 つの条件を充たすとき集合 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**反対元**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 に対して反対元 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, 反対元についても, y と z を x の反対元としたとき, 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．

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．

1.2 いろいろな群

キーワードは 巡回群, 対称群, 正規部分群, 商群, 可解群である. 特に対称群と可解群の関係性はとても重要である.

群 G が有限個の元でできているとき, 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. 以下内部算法の記号 $\cdot$ は省略する.

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 1 *G を群とし, $H \subset G$ とする. H が次の (0)~(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. 反対元に関しては (2) より明らかである.

（証明終）

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 $< S >$ と書く. S が有限集合 $S = \{a_1, a_2, \cdots, a_n\}$ であるとき, $< a_1, a_2, \cdots, a_n >$ 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 $< a >$ 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.

1.3 対称群

ガロア理論において方程式の可解性を決定づけるものが, 方程式の群であるということを概略編で述べた．実はこの群に相当するものが**対称群**なのである．このような理由で対称群はガロア理論において非常に重要な役割を担っている.

集合 X の元（数字）の入れ替えを行うことを**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 に入れ替えるものとの 2 種類がある．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, 下の例からわかるように 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.

さて例えば S_4 において 1 を 3 に, 3 を 4 に, 4 を 2 に, 2 を 1 に置換するものがある．これを (1342) と書こう．これを 4 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.

例 S_3 について考えよう．S_3 の元は全部で $3! = 6$ だけある．それを全部書き出してみると,

$$e=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\quad \sigma_1=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=(123),\quad \sigma_2=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=(132),$$

$$\tau_1=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=(23),\quad \tau_2=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=(13),\quad \tau_3=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=(12)$$

となる．ところで τ_1,τ_2,τ_3 は互換であり，$e=(12)(12)$，$\sigma_1=(13)(12)$，$\sigma_2=(12)(13)$ のように互換の積となる．

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 $(i_1i_2\ \cdots\ i_r)$ が $(i_1i_r)(i_1i_{r-1})\cdots(i_1i_3)(i_1i_2)$ 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 $(i_1\cdots\ \ i_r)$ 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 $(j_1j_2\cdots j_s)$ 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，恒等置換は奇数個の互換で表される．そこで，恒等置換が奇数個の互換の積で表されないことを示す．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，$e=(i_1j_1)(i_2j_2)\cdots(i_kj_k)$ 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．

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

k の最小性から $(i_1j_1)=(i_2j_2)$ とはならない．したがって，(i_1j_1) と (i_2j_2) との積は i_1 が右側の互換の互換のみに含まれる互換の積に置き換えられる．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. しかしこのような互換の積は恒等置換ではない.

（証明終）

この定理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. したがって, 偶数全体 A_n は S_n の部分群である. A_n を n 次の**交代群**という.

例 (1) S_3 の交代群は $A_3 = \{e, (123), (132)\}$ である. ところで,$(123)(123) = (132)$, $(123)(132) = e$ なので, A_3 は巡回群 $< (123) >$ である.

(2) S_4 の元は 24 個である.

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：$(123), (124), (132), (134), (142), (234), (243)$

長さ 4 の巡回置換：$(1234), (1243), (1324), (1342), (1423), (1432)$

$(i_1 i_2 \ \cdots \ i_r) = (i_1 i_r)(i_1 i_{r-1}) \cdots (i_1 i_3)(i_1 i_2)$ なので,

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

である.

命題 4 $n \geq 3$ のとき, $S_n =< (12), (13), \cdots, (1n) >$ であり, $A_n =< (123), (124), \cdots, (12n) >$ である.

証明 (1) $H =< (12), (13), \cdots, (1n) >$ 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 $S_n = H$.

(2) $K =< (123), (124), \cdots, (12n) >$ とおく. $(12k) = (12)(2k)$ より $K \subset A_n$. 任意の A_n の元は, $S_n =< (12), (13), \cdots, (1n) >$ より $(1i)(1j)$ という形の積で書ける. 一方 $(1i)(1j) = (12i)(12j)(12j)$ なので, $(1i)(1j) \in K$ である. よって $A_n \subset K$. したがって $A_n = K$. （証明終）

注意 $n = 4$ のとき A_4 は巡回群であり, $n \geq 4$ のとき A_n はアーベル群ではない.

1.4 正規部分群, 商群

正規部分群と商群は, 後に議論することになる可解群を説明するために必要不可欠である.

G を群 $a \in G$ とする. 集合 aH, Ha をそれぞれ $aH = \{ax \mid x \in H\}$, $Ha = \{xa \mid x \in H\}$ 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 5 G を群,$H \lhd G$ とする. このとき任意の $a \in G$ に対して

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

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)

例 S_4 の部分集合 $V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$ を考える. V_4 が群になることはすぐに分かる. V_4 を**クラインの 4 元群**という. さらに $V_4 =< (12)(34), (13)(24) >$ である. また V_4 は A_4 の部分群でもある. この V_4 は S_4 の正規部分群にもなっている.

$V_4 \lhd S_4$ の証明 $\sigma\tau \in S_n$ 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,

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

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

補題 6 $A_n \lhd S_n$.

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）

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．G/N を N による剰余類全体とする．

命題 7　G を群, $N \lhd G$ とする．そのとき G/N は群となる．

証明　任意の剰余類 aH, bH に対して, その演算を $aHbH = abH$ と定義すればよい．（証明終）

G/N を N による G の**商群**という．次の例は重要である．

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) $A_4 =< (123), (124) >$ なので, A_4/V_4 は V_4 と $(123)V_4$ と $(124)V_4$ からなる．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 $< (123) >$ である．

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

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

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 8　G を群, H を G の部分群とする．このとき,

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

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）

1.5　準同型定理

２つの群の関係を調べるために２つ群の間の写像を考える.

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.

命題 9　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) $f(x^{-1})f(x) = f(e) = e'$. よって $f(x^{-1}) = f(x)^{-1}$.　（証明終）

命題 10　群の準同型写像 $f : G \to G'$ に対し

(1) $\mathrm{Im}\ f$ は G' の部分群である.　*(2)* $\mathrm{Ker}\ f$ 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) $x', y' \in \mathrm{Im}\ f$ とする. $x' = f(x),\ y' = f(y)$ となる $x, y \in G$ がある. よって, $x'y' = f(x)f(y) = f(xy) \in \mathrm{Im}\ f$. 定理 1 によって Im f は G' の部分群であることがわかる.

(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. $n \in \mathrm{Ker}\ f$, $x \in G$ に対して

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

よって $xnx^{-1} \in \mathrm{Ker}\ f$. 命題 5 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.

命題 11　群の準同型写像 $f : G \to G'$ が単射 $\Leftrightarrow$ Ker $f = \{e\}$.

証明　($\Rightarrow$) は明らかである.

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

定理 12（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

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

証明　まず $\bar{f}$ が正しく定義されているかどうかをみる．$N = \mathrm{Ker} f$ とおく．$xN = yN$ ならば, $y^{-1}x \in N = \mathrm{Ker}\ f$,

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

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．

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

よって $\bar{f}$ は準同型写像である．

任意の $f(x) \in \mathrm{Im}\ f$ に対し, $f(x) = \bar{f}(xN) \in \mathrm{Im}\ \bar{f}$．よって $\mathrm{Im}\ \bar{f} = \mathrm{Im}\ f$ なので, $\bar{f}$ が単射であることを示せばよい．

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

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

定理 13 *G を群, $H \subset G$ を部分群, $N \lhd G$ とする．このとき*

(1) $HN = NH$ であって, HN は G の部分群である．

(2)（**同型定理１**） *$H \cap N \lhd H$ であって*

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

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

また

$$(HN)(HN) = H(NH)N = HHNN = HN,$$

$$(HN)^{-1} = N^{-1}H^{-1} = NH = HN$$

が成り立つ．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

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

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

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

（証明終）

定理 14 （**同型定理２**）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

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

は全射準同型であって,

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

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

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

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 $G/M \cong (G/N)/(M/N)$.　（証明終）

1.6　可解群

可解群の定義とその名前の意味は感覚的に一致しない. しかしそれはガロアの定理を理解してから初めて納得する. 変な気分でもある.

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

次の例はガロア理論においてとても重要である．

例 (i) アーベル群は可解群である．

(ii) 対称群 S_3 は可解群である．なぜならば, $\{e\} \lhd A_3 \lhd S_3$ であり, $S_3/A_3, A_3$ はアーベル群だからである．

(iii) 対称群 S_4 は可解群である． なぜならば, $\{e\} \lhd V_4 \lhd A_4 \lhd S_4$ であり, $S_4/A_4, A_4/V_4, V_4$ はアーベル群だからである．

命題 15　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 $< \alpha >$ を考える．G は単純群なので, $G =< \alpha >$ である．よって G は巡回群である．$| < \alpha > | = n$ 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, $a = \alpha^p$ とする．このとき部分群 $< a >$ の位数は, $| < a > | = n/p$. しかし, G は単純群なので, $< a >= G$ これは矛盾である．よって G は位数素数の巡回群である．　（証明終）

命題 16　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．

[†] 群 G の正規部分群が G と $\{e\}$ のみであるとき, G を**単純群**という．

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. さらに同型定理１より

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

であって, 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) $f : G \to G'$ が全射であるとする. $G_j \lhd G_{j-1}$ 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

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

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

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

であって, 同型定理２より, 商群

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

がアーベル群となるものが存在する. このとき, $G_i \lhd G_{i-1}$ に注意する.

また, N が可解群だから, N の正規列

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

であって, 商群

$$G_{j-1}/G_j$$

がアーベル群となるものが存在する. このとき,

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

は G の正規列であって, その商群はアーベル群よりなる．よって G は可解群である．　（証明終）

次の定理はガロア理論の本質的な最初の定理である．後に多項式のガロア群は対称群と同型であることをみるが, 5 次以上の多項式の可解性は, その群に同型な $n \geq 5$ の対称群 S_n に大きく関係しているのである．

定理 17　$n \geq 5$ 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．$A_n =< (12k) \mid 3 \leq k \leq n >$ であるから,

$$(12k) \in N$$

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

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

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 16 (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）

2　体とガロア理論

ガロア理論のあらすじをもう一度言おう．ガロア理論は, ある代数多項式を考えたとき, その根が係数の四則演算とべき根で解けるかどうかを判定するものである．それには, まずその多項式の係数が含まれる集合を考える．その集合とは体と言われるものである．次にその体のガロア群といわれる群を考える．そのガロア群の可解性が方程式の根の公式の問題を決定するのである．

2.1 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,

(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,

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

が成り立つ.

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．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対を**有限体**という.

2.2 環について

体の説明の前に少し**環**についてふれておく．環とは整数全体の集合 $\mathbf{Z}$ を一般化した概念である．$\mathbf{Z}$ をイメージ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,

[†] 実数とは, 整数, 分数, 無理数などの数である.

[§] 実数とは, 整数, 分数, 無理数, 虚数などの数である.

(2) $a(bc) = (ab)c$ が成り立つ.

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

例　(1) 勿論, 体 K は環でもある.

(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

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

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

$$\Phi(x+y) = \Phi(x) + \Phi(y)$$

$$\Phi(xy) = \Phi(x)\Phi(y)$$

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.

2.3　体の拡大

定義　E を体, F を E の部分集合とする．もし F 自信が体であるとき, 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 K の素体が $\mathbf{Q}$ と同型なとき, 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

$$K(X_1, \cdots, X_n) = \{f(X_1, \cdots, X_n)/g(X_1, \cdots, X_n) \mid f(X_1, \cdots, X_n),\ g(X_1, \cdots, X_n) \in K[X_1, \cdots, X_n]\}$$

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.

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

$$K(\alpha_1, \cdots, \alpha_n) = \{f(\alpha_1, \cdots, \alpha_n)/g(\alpha_1, \cdots, \alpha_n) \mid f(X_1, \cdots, X_n),\ g(X_1, \cdots, X_n) \in K[X_1, \cdots, X_n], \ g(\alpha_1, \cdots, \alpha_n) \neq 0\}$$

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

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

[†] 標数が 0 でないときは拡大の状況が複雑になる. ガロアの定理を証明するだけななら, 標数は 0 としてよいが, 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.

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

定理 18　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 K 上の基底, $\{\omega_\mu\}_{\mu\in M}$ を K 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, $\zeta = \sum_i \alpha_{\lambda_i}\Omega_{\lambda_i}$, $(\alpha_{\lambda_i} \in K)$ が成り立ち, $\alpha_{\lambda_i} = \sum_j \beta^{(i)}_{\mu_j}\omega_{\mu_j}$ である. よって $\zeta = \sum_j \sum_i \beta^{(i)}_{\mu_j}\Omega_{\lambda_i}\omega_{\mu_j}$ 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, $\sum_{ij} c_{ij}\Omega_{\lambda_i}\omega_{\mu_j} = 0$, $(c_{ij} \in K)$ と置くと, $\sum_i(\sum_j c_{ij}\omega_{\mu_j})\Omega_{\lambda_i} = 0$ 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 19 次の等式が成り立つ.

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

証明　定理 18 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 や自然対数の底 e は, $\mathbf{Q}$ 上超越的であることが知られている.

2.4 最小多項式

定理 20　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 $\alpha \in L$ で 0 となる次数最小の多項式 $f(X)$ を**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 $\mathrm{Irr}(\alpha, \mathrm{K})$ と書く.

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

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 21　α を体 K の拡大体の元とする.

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

(2) α が代数的であって, $\deg \mathrm{Irr}(\alpha, K) = n$ であれば, $[K(\alpha) : K] = n$.

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, $f(X) \not| g(X)$. $f(X)$ は既約なので, $f(X)$ と $g(X)$ の最大公約数は 1 だから, 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. α を代入すると, $g(\alpha)b(\alpha) = 1$ となる. 一方 $K(\alpha)$ から任意の元 z をとってくると, それは $z = h(\alpha)/g(\alpha)$ $(g(X), h(X) \in K[X],\ g(\alpha) \neq 0)$ と書けている. よって, $z = h(\alpha)b(\alpha) \in K[\alpha]$ が言えた. すなわち, $K(\alpha) \subset K[\alpha]$. 逆の包含関係は明らかなので, $K(\alpha) = K[\alpha]$ が言えた.

($\Leftarrow$)　$\alpha = 0$ のときは明らか. $\alpha \neq 0$ とすると $1/\alpha \in K(\alpha) = K[\alpha]$. 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. $g(X) = a_nX^n + 1 + \cdots + a_1X^2 + a_0X - 1$ と置くと, $g(X) \in K[X],\ g(X) \neq 0,\ g(\alpha) = 0$. よって α は代数的である.

(2)　$\mathrm{Irr}(\alpha, K) = f(X) = X^n + b_1X^{n-1} + \cdots + b_n$ 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. 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 22　$\alpha_1, \cdots, \alpha_n$ を体 K の拡大体 L の元で, K 上代数的であるとすると,

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

(2)　$[K(\alpha_1, \cdots, \alpha_n) : K] < \infty$. 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 21 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, $[M : K] < \infty,\ K(\alpha_1, \cdots, \alpha_n = M(\alpha_n)$. 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 $M(\alpha_n) = M[\alpha_n]$, $[M(\alpha_n) : M] < \infty$. したがって $K(\alpha_1, \cdots, \alpha_n) = M[\alpha_n] = K[\alpha_1, \cdots, \alpha_{n-1}, \alpha_n]$, $[K(\alpha_1, \cdots, \alpha_n) : K] = [M(\alpha_n) : M][M : K] < \infty$.　（証明終）

2.5 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. このような L は存在するのだろうか. 答えは系 24 である.

定理 23 K を体とし, $f(X)$ を $K[X]$ の既約な元とする. そのとき, $L = K(\alpha)$ 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, $L = \{hI \mid h \in K[X]\}$ とおき. L の内部演算を $gI + hI = (g+h)I$, $gIhI = (gh)I$ によって定義する. 明らかに L は加法によりアーベル群である. 積でアーベル群となることを示せば, L は体である. $f|g$ ならば $I = fI = gI$ 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, $gI\varphi I = I$. よって L は体である.

次に準同型写像 $\sigma : K \to L$ を $\sigma(a) = aI$ を考える. $K \cap I = \{0\}$ なので, σ は単射である. よって a と aI を同一視することで, $K \subset L$ とみなせる. XI を α とおくと, $L = K[\alpha]$ である. $f(X) = a_0X^n + \cdots a_n$ とすると, $0 = fI = a_0IX^nI + \cdots + a_nI = a_0\alpha^n + \cdots + a_n = f(\alpha)$. 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 24 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 数学的帰納法によって証明する. さらに $f(X)$ が $K[X]$ で既約なときをいえば十分である. $n = 1$ 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 23 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 24 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.

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

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.

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.

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

補題 25　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.

証明　$f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n = a_0(X-\alpha_1)\cdots(X-\alpha_n)$, $(a_0, \cdots, a_n \in K,\ \alpha_1, \cdots, \alpha_n \in L)$ とすると, $L = K(\alpha_1, \cdots, \alpha_n)$ である．$f(\alpha_i) = 0$ $(1 \le i \le n)$ に写像 σ) を作用させて, $\sigma(f(\alpha_i)) = a_0\sigma(\alpha_i)^n + a_1\sigma(\alpha_i)^{n-1} + \cdots + a_n = 0$．したがって, 各 i に対し j $(1 \le j \le n)$ が定まって, $\sigma(\alpha_i) = \alpha_j$ となるから, $\sigma(L) \subset L$. σ は同型写像だから $[\sigma(L) : K] = [L : K]$．ゆえに $\sigma(L) = L$.　（証明終）

[†] 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.

定理 26　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. $\mathrm{Irr}(\alpha_i, K) = f_i(X)$, $\prod_{i=1}^{n} f_i(X) = f(X)$ 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 $f(X)$ 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 の拡大体 ($f(X) = \mathrm{Irr}(\alpha, K)$ の L の最小分解体) からとる. K 上共役という仮定から 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, σ を単射準同型写像 $\tau : L \to L(\beta)$ まで拡張することができる. τ は K 上の単射準同型写像なので, 補題 25 より $L(\beta) = \tau(L) = L$. すなわち $\beta \in L$ である. したがって L は K の正規拡大である. 有限次拡大であることは明らかである.　(証明終)

系 27　L を体 K の有限次ガロア拡大体, M を L と K 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 26 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. $K \subset M \subset L$, $\alpha_1, \cdots, \alpha_n \in L$ なので, $L = K(\alpha_1, \cdots, \alpha_n) \subset M(\alpha_1, \cdots, \alpha_n) \subset L$. したがって, $L = M(\alpha_1, \cdots, \alpha_n)$. よって L は $f(x)$ の M 上の最小分解体となるので, K のガロア拡大である.　(証明終)

補題 28　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 29　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 共に 1 次式に分解する．すなわち,

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

補題28 より g, h は重根をもたない．ここで K の元の中から $(\eta - \eta_i)/(\zeta_j - \zeta)$, $i = 2, \cdots, n$, $j = 2 \cdots, n$ 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, $f|h$, $f|\tilde{g}$ である．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）

2.6　ガロアの定理１

定義　L を体 K のガロア拡大とする．L の K 自己同型群全体のなす群とは, 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いう．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.

注意　L を体 K のガロア拡大とする．このとき, $|\mathrm{Gal}(L/K)| = [L : K]$ である.

L を体 K の拡大体, M を L と K の中間体とする．このとき, L の M 自己同型写像は自動的に, K 自己同型写像になるので, $\mathrm{Gal}(L/M) \subset \mathrm{Gal}(L/K)$ となる.

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 30 （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, $\mathrm{Gal}(L/M) = L^{\mathrm{Gal(L/M)}}$ 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, $\varphi(M_1) \subset \varphi(M_2)$, $G_1 \supset G_2$ なら $\psi(G_1) \subset \psi(G_2)$.

証明　$M \subset \mathcal{I}$ に対し $\mathrm{Gal}(L/M) = G$ とおく．$L^G = M$ であることは明らかなので, $\psi\varphi$ は $\mathcal{I}$ の恒等写像である．

$G \subset \mathcal{F}$ 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 29 より $L = M(\alpha)$ 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, $\{\sigma\sigma_1, \cdots, \sigma\sigma_n\} = \{\sigma_1, \cdots, \sigma_n\}$ なので, $f^\sigma(X) = \prod_{i=1}^{n}(X - \sigma\sigma_i(\alpha)) = f(X)$．すなわち, $f(X) \in L^G[X] = M[X]$．σ_1 を G の単位元とすると $\sigma_1(\alpha) = \alpha$．ゆえに $f(\alpha) = 0$．したがって, $\mathrm{Irr}(\alpha, M) | f(X)$．よって, $[L : M] = \deg \mathrm{Irr}(\alpha, M) \leq \deg f(X) = n$．つまり $\varphi\psi$ は $\mathcal{F}$ の恒等写像である．

$M_1 \supset M_2$ 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, $\mathrm{Gal}(L/M_1) \subset \mathrm{Gal}(L, M_2)$．$L$ の元が H_1 の元によって不変であれば, 当然 H_2 の元によっても不変であるから, $L^{H_1} \subset L^{H_2}$.　（証明終）

系 31　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, $\tau\mathrm{Gal}(L/M)\tau^{-1} = \mathrm{Gal}(L/\tau(M))$.

(2) M が K のガロア拡大である．$\Leftrightarrow$ $\mathrm{Gal}(L/M)$ は $\mathrm{Gal}(L/K)$ の正規部分群である．このとき, $\mathrm{Gal}(M/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)$.

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．任意の $\sigma \in \mathrm{Gal}(L/M)$ に対し, $(\tau\sigma\tau^{-1})(\tau(\alpha)) = \tau\sigma(\alpha) = \tau(\alpha)$ だから, $\tau\mathrm{Gal}(L/M)\tau^{-1} \subset \mathrm{Gal}(L/\tau(M))$. 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, $\tau^{-1}\rho\tau \in \mathrm{Gal}(L/M)$．したがって $\rho \in \tau\mathrm{Gal}(L/M)\tau^{-1}$ がわかり, 逆の包含関係がいえた.

(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 26 と補題 25 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, $\mathrm{Gal}(L/M)$ は $\mathrm{Gal}(L/M)$ の正規部分群である.

($\Leftarrow$) $\mathrm{Gal}(L/M)$ が $\mathrm{Gal}(L/K)$ の正規部分群であるとすると, 任意の $\tau \in \mathrm{Gal}(L/K)$ に対し,

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

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

このとき, $\mathrm{Gal}(L/K)$ 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 $\varphi : \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K),\ \varphi(\tau) = \tau'$ は準同型写像である．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.

$$\mathrm{Ker}\varphi = \{\tau \in \mathrm{Gal}(L/K) \mid \tau' = 1_M\} = \{\tau \in \mathrm{Gal}(L/K) \mid \text{任意の}\alpha \in M \text{に対し}\tau(\alpha) = \alpha\} = \mathrm{Gal}(L/M).$$

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

2.7　べき根拡大.

定義　L を体 K の有限次拡大体とする.

(i) 次の 2 つの条件を充たすような 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) $K_i = K_{i-1}(\alpha_i),\ \mathrm{Irr}(\alpha_i, K_{i-1}) = X^n - a_i\ \ (1 \leq i \leq r)$.

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

補題 32　L を体 K のガロア拡大とし, $|\mathrm{Gal}(L/K)| = n$ とする. このとき, $\alpha_1, \cdots, \alpha_n \in L$ について, L の任意の元 θ に対し

$$\sum_{i=1}^{n} \alpha_i \sigma_i(\theta) = 0 \Rightarrow \alpha_1 = \cdots = \alpha_n = 0$$

が成り立つ. ここで, $\sigma_1 = e, \sigma_2, \cdots, \sigma_n$ は $\mathrm{Gal}(L/K)$ の元である.

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,

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

と仮定する. 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, $0 = \sigma_i^{-1}(\sum_{i=1}^{n} \alpha_i \sigma_i(\theta)) = \sum_{i=1}^{n} \sigma_j^{-1}(\alpha_i)(\sigma_j^{-1}\sigma_i(\theta))$ となるから, はじめから $\sigma_1 \neq 0$ 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

$$\alpha_1 \eta\theta + \alpha_2 \sigma_2(\eta\theta) + \cdots + \alpha_n \sigma_n(\eta\theta) = 0,$$

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

が得られる. この二つの式の差より,

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

となるが, $\alpha_k(\sigma_k(\eta) - \eta) \neq 0$ であり, L の組 $(0, \alpha_2(\sigma_2(\eta) - \eta), \cdots, \alpha_n(\sigma_n(\eta) - \eta))$ は, $(\alpha_1, \cdots, \alpha_n)$ より多くの 0 を含む. これは α_i のとり方に矛盾する.　（証明終）

定理 33　体 K が 1 の原始 n 乗根 ζ を含むとする. すなわち, $\zeta \in K$ は $\zeta^r \neq 1$ $(1 \leq r \leq n-1)$, $\zeta^n = 1$ をみたす.

(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) $\mathrm{Gal}(L/K) =< \sigma >$ とする．補題 32 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

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

となるから, $\sigma^i(\alpha) = \alpha\zeta^i$ 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, $\mathrm{deg}q(X) = [L(\alpha) : K] \leq [L : K] = n$ 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, $\mathrm{deg}q(X) = n$ 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, α は $X^n - a \in K[X]$ 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から, L は K のガロア拡大である．α の K 上の共役元は, $\{\alpha, \alpha\zeta, \cdots, \alpha\zeta^{n-1}\}$ に含まれる．$\mathrm{Gal}(L/K) \ni \sigma_i$ を $\sigma_i(\alpha) = \alpha\zeta^i$ と定義すると, $\mathrm{Gal}(L/K) \to \{1, \zeta, \cdots, \zeta^{n-1}\}$, $\sigma_i \mapsto \zeta^i$ 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, $\mathrm{Gal}(L/K)$ は巡回群である．よって L は K の巡回拡大である．　（証明終）

定理 34　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, 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 $\{\zeta^{i_1}, \cdots, \zeta^{i_n}\}$ に含まれる．また $K(\zeta)$ は K 上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 $\mathbf{Gal}(K(\zeta)/K) \to G$, $\sigma_r \mapsto i_r$ 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）

2.8 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, $\mathbf{Q}(a_1/a_0, \cdots, a_n/a_0)$ 上の $f(X)$ 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　$f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n$ を $K = \mathbf{Q}(a_1, \cdots, a_n)$ 係数の多項式とし, 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.

補題 35　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 の K 上の最小分解体とする. L の分解を $f(X) = a(X - \alpha_1)\cdots(X - \alpha_n)$ とすると, $L = K(\alpha_1, \cdots, \alpha_n)$ である. したがって $LM = M(\alpha_1, \cdots, \alpha_n)$ である. これは LM が $f(X)$ の M 上の最小分解体であることを示す. すなわち LM は M のガロア拡大である. よって, $\mathrm{Gal}(LM/M) = \mathrm{Gal}_M(f)$.

ガロア群 $G = \mathrm{Gal}(LM/K) = \mathrm{Gal}_M(f)$ の元の L への制限を考えることにより, これはもちろん K の元を固定するので, 準同型写像 $\varphi : G \to \mathrm{Gal}(LM/M) \ni \sigma \mapsto \sigma|_L \in \mathrm{Gal}(L/K)$ が得られる. $\mathrm{Im}\varphi = H$ とおくと, $L^H = L \cap M$ である. 実際, 任意の $\tau \in H$ は, $\tau = \sigma|_L$ $(\sigma \in \mathrm{Gal}(LM/K))$ と表されるから, $L \cap M \subset L^H$ であり, L に属し M に属さない元 β は, 適当な $\sigma \in \mathrm{Gal}(LM/K)$ によって, $\sigma(\beta) \neq \beta$ となるから, $\sigma|_L = \tau$ とおけば, $\tau(\beta) \neq \beta$ である. よって $L \cap M = L^H$. φ は単射だから, $\mathrm{Gal}_M(f) = \mathrm{Gal}(LM/K) \cong H = \mathrm{Gal}(L/L \cap M) \subset \mathrm{Gal}_K(f)$ となる.　（証明終）

補題 36 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_1L_2 が K のガロア拡大であることは, 補題 35 の証明の中で述べた. ガロア群 $\mathrm{Gal}(L_1L_2/K) = G$ とおくと, L_1 は K のガロア拡大だから, $G \rhd G(L_1L_2/L_1)$ であって, 系 31 より $\mathrm{Gal}(L_1/K) \cong G/\mathrm{Gal}(L_1L_2/L_1)$ である. $\mathrm{Gal}(L_1/K)$ はアーベル群だから, 命題 8 より交換子群 $[G,G] \subset G/\mathrm{Gal}(L_1L_2/L_1)$ である. 同様に, $[G,G] \subset \mathrm{Gal}(L_1L_2/L_2)$. 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, 上の包含関係から, $M \supset L_1L_2$. したがって $M = L_1L_2$. すなわち, $[G,G] = \{e\}$ となり, 全ての $a, b \in G$ に対して $aba^{-1}b^{-1} = e$. つまり $ab = ba$. よって G はアーベル群である. （証明終）

定理 37 （ガロアの定理２） K を体とし, $f(X) \in K[X]$ とする.

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, $L = K(\alpha_1, \cdots, \alpha_n)$ とおくと, $f(X) = 0$ 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で, このとき方程式 $f(X)$ 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.'
を証明すればよい.

($\Rightarrow$) 仮定により, $K = K_0 \subset K_1 \subset \cdots \subset K_r = L'$, $L \subset L'$, $K_i = K_{i-1}(\alpha_i)$, $\mathrm{Irr}(\alpha_i, K_{i-1}) = X^{n_i} - a_i$, $1 \leq i \leq r$ と書ける. L'' を L' を含む K の有限次ガロア拡大とすると, 系 31 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. $\mathrm{Gal}(L''/K)$ が可解であれば, $\mathrm{Gal}(L/K)$ も可解群であるから, $\mathrm{Gal}(L''/K)$ が可解群となるように L'' が選べることを示せばよい.

r に関する数学的帰納法によって示す.

$r = 1$ の場合. $a_1 = a$, $\alpha_1 = \alpha$ とおくと, $L' = K(\alpha)$, $\mathrm{Irr}(\alpha, K) = X^n - a$. $\zeta \in \mathbf{C}$ を 1 の原始 n 乗根の 1 つとすると, $L'' = L'(\zeta)$ は $X^n - a$ の K 上の最小分解体であるから, K の有限次ガロア拡大である. 定理 33 より, $L'' = K(\zeta, \alpha)$ は $K(\zeta)$ の巡回拡大であり, 定理 34 より, $K(\zeta)$ は K のアーベル拡大である. すなわち, $\mathrm{Gal}(L''/K) \rhd \mathrm{Gal}(L''/K(\zeta)) \rhd \{1\}$ で, $\mathrm{Gal}(L''/K)/\mathrm{Gal}(L''/K(\zeta)) \cong \mathrm{Gal}(K(\zeta)/K)$, $\mathrm{Gal}(L''/K(\zeta))$ はともにアーベル拡大である. したがって, $\mathrm{Gal}(L''/K)$ 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. 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$\alpha$を$\sqrt[n]{a}$と書く. すなわち, $L' = K_r = K'(\sqrt[n]{a})$. ζを1の原始n乗根の1つとすると, $M(\zeta)$はMのアーベル拡大で, Kのガロア拡大である. 系31により$\mathrm{Gal}(M(\zeta)/K) \triangleright \mathrm{Gal}(M(\zeta)/M))$で$\mathrm{Gal}(M(\zeta)/K)/\mathrm{Gal}(M(\zeta)/M) \cong \mathrm{Gal}(M/K)$であり, またこれは可解群で, $\mathrm{Gal}(M(\zeta)/M)$はアーベル群だから可解群である. よって$\mathrm{Gal}(M(\zeta)/K)$は可解群である.

$\mathrm{Gal}(M/K) = \{\sigma_1, \cdots, \sigma_m\}$の任意の元$\sigma$について, $X^n - \sigma(a)$は$\sigma(K')[X]$において既約である$(\sigma(a) \in M)$. そのM上の分解体における零点の一つを$\sqrt[n]{\sigma(a)}$と書くことにすると, $X^n - \sigma(a) = \prod_{i=0}^{n-1}(X - \sqrt[n]{\sigma(a)}\zeta^i)$と表され, 定理33により, $M(\zeta, \sqrt[n]{\sigma(a)})$は$M(\zeta)$の巡回拡大である. $g(X) = \prod_{i=1}^{m}(X^n - \sigma_i(a))$の$M$上の最小分解体は, $L'' = M(\zeta, \sqrt[n]{\sigma_1(a)}, \cdots, \sqrt[n]{\sigma_m(a)})$であって, 補題36より$L''$は$M(\zeta)$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, また$g(X)$の係数は対称的だから$g(X) \in K[X]$である. よって$L''$は$K$のガロア拡大であり, $L'' \supset L'$でもある.

$\mathrm{Gal}(L/K) \triangleright \mathrm{Gal}(L''/M(\zeta)) \triangleright \{1\}$で, 系31により$\mathrm{Gal}(L''/K)/\mathrm{Gal}(L''/M(\zeta) \cong \mathrm{Gal}(M(\zeta)/K)$であって, またこれは可解群で, $\mathrm{Gal}(L''/M(\zeta))$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.

$(\Leftarrow)$ n=|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34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. $|\mathrm{Gal}(M/K)| < n$なので, 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. 補題35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$G = G_0 \supset G_1 \supset \cdots \subset G_r = \{e\}$を考える. $\mathrm{Gal}(\tilde{L}/\tilde{M})$は可解群だから, 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, $\tilde{M} = L_0 \subset L_1 \subset \cdots L_r = \tilde{L}$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33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,

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

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る. (証明終)

2.9 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．

定義　$f(X) = 0$ の複素数体 $\mathbf{C}$ における根を $\alpha_1, \cdots, \alpha_n$ とする．このとき, 次の式 $s_1, \cdots, s_n$ を**基本対称式**という．

$$\begin{aligned} s_1 &= \alpha_1 + \cdots + \alpha_n, \quad s_2 = \alpha_1\alpha_2 + \cdots + \alpha_{n-1}\alpha_n, \cdots, \\ s_k &= \sum_{i_1 < \cdots < i_k} \alpha_{i_1} \cdots \alpha_{i_k}, \ \cdots, \ s_n = \alpha_1 \cdots \alpha_n. \end{aligned}$$

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．基本対称式は n 次方程式の解と係数の関係を表す．

命題 38　体 K 上の有理関数体 $K(X_1, \cdots, X_n)$ について, 拡大 $K(X_1, \cdots, X_n) \supset K(s_1, \cdots, s_n)$ は多項式 $f(X) = X^n - s_1X^{n-1} + \cdots + (-1)^n s_n$ 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, $K(X_i, \cdots, X_n)$ は $f(X)$ の $K(s_1, \cdots, s_n)$ 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

$$K(X_1 \cdots, X_n) \ni \varphi(X_1, \cdots, X_n) \mapsto \varphi(X_{\sigma(1)}, \cdots, X_{\sigma(n)}) \in K(X_1, \cdots, X_n)$$

を考えれば, これは, $K(s_1, \cdots, s_n)$ 自己同型写像である．よって $\mathrm{Gal}_{K(s_1, \cdots, s_n)}(f) \cong S_n$ 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 39　$t_1, \cdots, t_n$ 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．$K' = \mathbf{Q}(s_1, \cdots, s_n)$ と置く．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 K 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 $K[X_1, \cdots, X_n] \cong K[\alpha_1, \cdots, \alpha_n]$ が成立する．そして $K(X_1, \cdots, X_n)$ から $K(\alpha_1, \cdots, \alpha_n)$ の写像 Ψ を $\Psi(g/f) = \Phi(g)\Phi(f)^{-1}$ と置くことで, 体の同型 $K(X_1, \cdots, X_n) \cong K(\alpha_1, \cdots, \alpha_n)$ 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 38 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）

References

[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.

Present Address:
Osamu Matsuda
Tsuyama National College of Technology
624-1, Numa, Tsuyama-City, Okayama, Japan, 708-8509
e-mail : matsuda@tsuyama-ct.ac.jp