代数方程式におけるガロア理論
—環・体およびガロア群とべき根による可解性について—

2004MM005 戎祐輔
指導教員: 宮元忠敏

1 はじめに

本研究では，[1]と[2]を用いて，**ガロアの定理**の理解を目的としている．ガロアの定理とは,『多項式がべき根によって可解であるための必要十分条件は，その多項式のガロア群が可解となる』という定理であるが，本研究では，この定理の十分条件を示すまで至り，さらに，**アーベル=ルフィニの定理**にアプローチし，証明することができた．そこで，以降では，アーベル=ルフィニの定理の証明に必要な定義・定理を中心に説明し，実際に証明を行う．

2 アーベル=ルフィニの定理

アーベル=ルフィニの定理とは,『一般の5次方程式は，べき根によって可解にならない』という，N.H.AbelとPaolo Ruffiniが証明した定理であり，これは，言い換えれば,『5次方程式の解の公式は存在しない』となる．この定理に対して，E.Galoisは，方程式に群と体を関連させることで新しい理論を作りだし，これをより詳しく証明した．これがガロアの定理であり，**ガロア理論**である．

3 諸定義・諸定理

この章では，以降で取り挙げる**ガロア群**や**べき根による可解性**，そして，ガロアの定理やアーベル=ルフィニの定理の証明に必要な定義や定理を挙げる．

定義

拡大体 $\cdots$ 体Fを含む体Eのことで，E/Fと表記．
分解体 $\cdots$ $f(x)\in F[x]$が1次式の積に分解し，しかしながら，その任意の真の部分体では分解しない拡大体E/Fのこと．
拡大次数 $\cdots$ F上のベクトル空間としてのEの次元のことで，$[E:F]$と表記．
巡回群 $\cdots$ 生成元と呼ばれる元gがあって，すべての元がgのべきとして表せる群Gのこと．
正規部分群 $\cdots$ 任意の$g\in G$に対して，$gHg^{-1}=\{ghg^{-1}\mid h\in H\}=H$が成り立つ群$G$の部分群$H$のこと．
モニック多項式 $\cdots$ 最高次係数が1の多項式．

定理0

拡大体E/Fに対して，$\alpha\in E$がF上代数的であるとき，αを根にもつ既約なモニック多項式$p(x)\in F[x]$に対して，$[F(\alpha):F]=\partial(p)$が成り立つ．
※ $\partial(p)$とは，多項式$p(x)$の次数のことである．

アイゼンシュタインの既約判定法

$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in Z[x]$としたとき，素数$p$がすべての$i<n$に対して$a_i$を割り切るが，$a_n$を割り切らず，しかも$p^2$は$a_0$を割り切らないならば，$f(x)$は$\mathbb{Q}$ 上既約である．

次元公式

$F\subset B\subset E$が体で，$[E:B]$と$[B:F]$が有限であるとき，$[E:F]$も有限で，$[E:F]=[E:B]\cdot[B:F]$が成り立つ．

4 ガロア群

この章では，ガロア群とそれに関する定理を取り挙げる．まずは，定義を以下に示す．

定義 (ガロア群)

E/Fを拡大体とする．このとき，E/Fの**ガロア群**とは，$\mathrm{Gal}(E/F)$で表し，

$\mathrm{Gal}(E/F)=\{F$を点ごとに固定するEの自己同型写像$\}$

のことである．

※ E**の自己同型写像**とは，Eからそれ自身への同型写像のことである．また，F**を点ごとに固定する**とは，Eの自己同型写像σが，すべての$c\in F$に対して，$\sigma(c)=c$が成り立つことである．

拡大次数とガロア群には，以下のようなとても重要な関係が成り立つ．

定理1

$f(x)\in F[x]$が重根をもたない多項式で，E/Fが$f(x)$の分解体であるならば，

$$|\mathrm{Gal}(E/F)|=[E:F]$$

が成り立つ．

【例1】

$f(x)=x^3-1\in\mathbb{Q}[x]$とする．このとき，$f(x)$のガロア群とは，$\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$のことである．ここで，$f(x)$は$\mathbb{Q}$上で，$f(x)=(x-1)(x^2+x+1)$と変形できることから，**定理1**より，$2=[\mathbb{Q}(\omega):\mathbb{Q}]=|\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})|$ となるので，ガロア群は，位数2の巡回群となる．□

以下の定理は，ガロア群において，のちに挙げる**定理3**との関係において，非常に重要な定理である．

定理2

$F\subset B\subset E$を体の塔とし，B/Fはある多項式$f(x)\in F[x]$の分解体，E/Fはある多項式$g(x)\in F[x]$の分解体とする．このとき，

1. $\mathrm{Gal}(E/B)$は$\mathrm{Gal}(E/F)$の正規部分群
2. $\mathrm{Gal}(E/F)/\mathrm{Gal}(E/B)\simeq\mathrm{Gal}(B/F)$

が成り立つ．

5　べき根による可解性

べき根による可解性は，本論文の最重要テーマであり，アーベル=ルフィニの定理の証明には，ガロア群における計算が大いに関係する．以降では，べき根に関連する定義や定理，またその例について紹介する．

定義 (べき根による可解性)

$f(x) \in F[x]$とする．F上の$f(x)$の分解体Eを含むべき根拡大B/Fが存在するとき，$f(x)$はF上で**べき根によって可解である**という．

※ べき根拡大については，以下を参照.

定義 (純拡大・べき根塔・べき根拡大)

適当な正整数mに対して，$\alpha^m \in F$となるαを用いて，$B = F(\alpha)$ と表せるとき，拡大体B/Fを**m型純拡大**という．また，体の塔

$$F = B_0 \subset B_1 \subset \cdots \subset B_t$$

に対して，各々のB_{i+1}/B_iが純拡大のとき，この塔を**べき根塔**といい，B_t/Fを**べき根拡大**という．

※ 標数0の体上の2次・3次・4次方程式には，べき根拡大が存在するので，べき根によって可解である．

6　証明に必要な定理

本節では，アーベル=ルフィニの定理を証明するために必要な可解群・巡回群に関連する定理を挙げる．

定理集

1. pが$|G|$を割り切る素数であれば，Gは位数pの元を含む．(**コーシーの定理**)
2. αがS_5の5巡回元で，τがS_5の互換であれば，$\langle \alpha, \tau \rangle = S_5$になる．
   ※ S_5とは，$\{1,2,3,4,5\}$のすべての置換の合成の群のことであり，**対称群**と呼ばれる．
3. nが5より小さければ，S_nは可解であるが，nが5以上であれば，S_nは可解ではない．

次の定理は，ガロアの定理の十分条件を与えており，これを示すためには，**定理2**が必要となる．また，この定理が証明されることで，アーベル=ルフィニの定理が考えられるので，本研究でも特に重要な定理である．

定理3

$f(x) \in F[x]$が，標数0の体F上べき根によって可解であるとし，またE/Fを分解体とする．このとき，$\mathrm{Gal}(E/F)$は可解群になる．

7　アーベル=ルフィニの定理の証明

それでは，以上のことを踏まえてアーベル=ルフィニの定理を証明するが，ここで示す定理は，アーベル=ルフィニの定理よりも強い主張である．

アーベル=ルフィニの定理 (改)

5次多項式$f(x) \in \mathbb{Q}[x]$で，べき根によって可解にならないものが存在する．

[証明] 定理0，1，3，定理集を用いて示す.

$f(x) = x^5 - 4x + 2$とする．このとき，**アイゼンシュタインの既約判定法**により，$f(x)$は$\mathbb{Q}$上既約となる．ここで，$E/\mathbb{Q}$を$\mathbb{C}$に含まれる$f(x)$の分解体とし，$G = \mathrm{Gal}(E/\mathbb{Q})$とする．このとき，$\alpha$が$f(x)$の根であったとすると，**定理0**から，

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$$

が成り立ち，さらに**次元公式**を用いると，

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 5[E : \mathbb{Q}(\alpha)]$$

となり，**定理1**を適用すると，

$$|G| = [E : \mathbb{Q}] = 5[E : \mathbb{Q}(\alpha)]$$

となるので，$|G|$は5の倍数となる．ここで，$f(x)$は異なる3つの実数解と2つの複素数解をもつ．よって，この5つの解に対して，Gを5つの根の置換群(G からそれ自身への全単射全体)の部分群とみなすと，Gは5巡回元を含む.

なぜなら，$|G|$は5の倍数であることから，**定理集1**より，Gは位数5の元を含み，さらにS_5の個別の性質から，S_5における位数5の元は，巡回元のみであるからである．

さて，ここで，複素共役のEへの制限をσとすると，$\sigma \in G$となる．よって，$\sigma \in S_5$とすると，σは複素共役のみを入れ換える互換となる．また，**定理集2**より，S_5は任意の互換と任意の5巡回元から生成されるので，

$$G \simeq S_5$$

が成り立つ．ここで，**定理集3**より，S_5は可解群ではないので，同型なGも可解群ではない．ここで，$f(x)$がべき根によって可解であったとすると，**定理3**からGは可解群となるが，これは矛盾である．したがって，$f(x)$は$\mathbb{Q}$上でべき根によって可解ではない．■

8　おわりに

本研究では，群や環，体など，ガロア理論にアプローチするための準備段階を経ることによって，実際にガロアの定理の十分条件である**定理3**を証明し，さらに，アーベル=ルフィニの定理の証明までカバーすることができた.

今後の課題としては，**指標の独立性**と**ガロア拡大**という概念を研究することで，**ガロア理論の基本定理とその応用**にアプローチし，その内容を理解することである．こうすることにより，**定理3**の逆，すなわち，ガロアの定理の必要条件を証明することができる.

参考文献

[1] J．ロットマン 著：関口 次郎 訳：「改訂新版 ガロア理論」，シュプリンガー・フェアラーク東京(2000).

[2] 中島 匠一 著：「代数方程式とガロア理論」，共立出版株式会社(2006).

[3] 桂 利行 著:「体とガロア理論」，東京大学出版会(2005).