# ガロア理論を知る

芝浦工業大学 数理科学研究会
bv18025 加藤諒

令和元年 5 月 19 日

## 研究背景

ガロアのあまりに有名な生涯とそのうちに果たした偉大な業績に以前から興味があった．ガロア理論に関する本を何度も読んでは挫折してきたが大学新 2 年になり授業で群論にも少し触れるようになったし心機一転, 今度こそその概形を捉えたいと思った．

## 1　$n$ 次方程式を解くとは

"$n$ 次方程式を代数的に解く"とは，その方程式の係数の和，差，積，商とべき乗の組み合わせのみで解を得ることをいう．また，代数学の基本定理から $n$ 次方程式には重解を含めれば $\mathbb{C}$ の範囲では $n$ 個の解が存在する．

## 2　ガロア理論

### 2.1　準備

有理数体 $\mathbb{Q}$ に代数的数 $\alpha$ を添加した拡大体を $\mathbb{Q}(\alpha)$ と書く．

組 $(G, \cdot)$ が群をなすとは，以下の 3 条件が成立することをいう．

群の定義

i (結合法則) $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$　　$(g_i \in G)$
ii (単位元の存在) $\exists e \in G, \ \forall g \in G, \ g \cdot e = g = e \cdot g$
iii (逆元の存在) $\forall g \in G, \exists g' \in G \ s.t. \ g \cdot g' = e = g' \cdot g$

例えば，$n$ 次の置換全体は群をなし，それを $n$ 次対称群という．

**定義** (ガロア群)**.** $\mathbb{Q}(\alpha)$ 上の写像で $\mathbb{Q}$ を動かさないものの集合をガロア群という．

**定義** (可解群)**.** 以下のようにアーベル群の"積み上げ"で作ることができる群を可解群という．

可解群の定義

G が可解群とは，次が成り立つことをいう．

$$G : \text{可解} \Leftrightarrow G \rhd G_1 \rhd G_2 \rhd \cdots$$
$$\text{s.t. } G_i/G_{i+1} \text{ はアーベル群}$$

また，次が成り立つ．

ガロア群と対称群は同型である．　…(A)

### 2.2　ガロアの発想

$n$ 次方程式の解が作る対称性から群を考え，その群について考えることで $n$ 次方程式の可解性を考える．

### 2.3　$n$ 次方程式の可解性

ガロアの定理

$n$ 次方程式が代数的に解ける $\Longleftrightarrow$ ガロア群が可解群　…(B)

以上，(B)，(A) から次のことがわかる．

方程式の可解性

$n$ 次方程式が代数的に解ける $\Longleftrightarrow$ $n$ 次対称群が可解である

### 2.4　$n$ 次対称群の可解性

ガロアによって，$n$ 次対称群の有限個の元のみに着目することで $n$ 次方程式の可解性が判断できることになった．ここで，$n = 5$ とするとその 5 次対称群の元は 120 個あり，そこから元が 60 個の正規部分群を作ることができる．しかしそこから新たに正規部分群を作り出すことができないため，5 次方程式は代数的には解くことができない．これが有名な"5 次方程式には解の公式が存在しない"ことの所以である．また，一般の $n \in \mathbb{N}$ に対して $\mathfrak{S}_{n+1} \supset \mathfrak{S}_n$ が成り立つため，$n$ 次方程式 $(n \geqq 5)$ についても同様であることがわかる．（厳密には証明が必要）

## 今後の課題

今回ガロア理論についていくつかの数学書を読むなどして多方面から知識を得て学んだがそれでもなお厳密な議論を理解するには至らなかった．ただ，ガロアの着想やあらゆる群のことを理解できたという点で確かな進歩もあったので今後も継続して丁寧に数学を学んでいき完全な理解に努めたい．

## 参考文献

[1]　鈴木智秀, 図解と実例と論理で、今度こそわかるガロア理論,SB クリエイティブ株式会社,2017.
[2]　石井俊全, ガロア理論の頂を踏む, ベレ出版,2013.
[3]　小林吹代, ガロア理論超入門, 株式会社技術評論社,2016.