ガロワ理論への入門とその展望

開成学園　数学研究部

2018年9月

普段の活動

- 数学オリンピック
- レクリエーション
- 下級生ゼミ（今年から）
- 自主ゼミ（今年から）

下級生ゼミは今年から始まった新企画なので手探り状態……（一学期は群論、二学期はまだ決まっていない）

エヴァリスト・ガロワ

- フランスの数学者・革命家（1811 − 1832）
- 論文を２回も紛失される
- 決闘により死亡

方程式

「A くんが 5 個のどら焼きを食べました。B くんがいくつか食べました。二人の食べた分を合計すると 8 個でした。さあ B くんは何個食べたでしょうか？」

$$5 + x = 8$$

これを解いて $x = 3$ を得る…… といったもの[1]。

[1] 簡単のため、単に方程式といえば 1 変数の実数係数多項式 $f(x)$ による式 $f(x) = 0$ のことを指します。

対称性

小学校の算数の「線対称」「点対称」は「線について折り返すと いう操作を行っても変化しない」「点について180 度回転という操作を行っても変化しない」と言い換えられるのでは？

定義（対称性）

ある要素 a に対して操作 f を行ったときに変化が起こらない場合、a は f について対称であるとか f について対称性を持っているとかいう。

対称性を調べよう

三角形 ABC を

- 120 度回転させる操作を σ
- 裏返す操作を τ
- 「何もしない」という操作を e

とする。

120 度回転を 3 回やると元に戻り、2 回裏返すと元に戻るので、このことを次のように書く：

$$\sigma^3 = e, \quad \tau^2 = e$$

したがって、ありうる場合は

$$\{e, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$$

である。

群

こういった「対称性」を扱えるようになりたい！

→「対称性」と名乗るに値するような性質を満たすもの

を考えればよいのでは？

定義（群）

空でない集合 G に対し，G 上の演算 $\circ : G \times G \to G$ が定義されていて，次の性質を満たすとき，$(G, \circ)$ を群という．

1. 結合法則：任意の G の元 a, b, c に対して $(a \circ b) \circ c = a \circ (b \circ c)$ が成り立つ．
2. 単位元と呼ばれる元 $e \in G$ が存在し，すべての $a \in G$ に対し，$a \circ e = e \circ a = a$ が成り立つ．
3. すべての $a \in G$ に対し，$b \in G$ が存在し，$a \circ b = b \circ a = e$ となる．このとき b は a の逆元と呼ばれ，a^{-1} と書く．

実はラグランジュやガウス、ルフィニ、アーベルなどのガロワ以前の数学者がすでに

方程式と対称性は密接な関係がある

ことに気づいており、特にアーベルはうっすらとですが群のアイデアを発明していた。

$x^2 + bx + c = 0$ の解[2]を求めたい！
→少なくとも 2 個以下である[3]
→解を α, β とおいてみる

[2]別に二次の係数が 1 であるとは限らないが、簡単にするためと、筋道がわかれば非常に簡単な計算により解が従うことより省略した。

[3]証明は背理法より即座に従う。これは代数学の基本定理とは関係ない。

方程式の解：$f(x) = 0$ を満たす x のことなので

$$x^2 + bx + c = (x - \alpha)(x - \beta) = 0$$

とできる。展開して係数を比較することにより

$$b = -(\alpha + \beta), \quad c = \alpha\beta$$

を得る。したがって α と β を入れ替えても、係数 b, c は変わらない。すなわち**対称性**がある。

- 解の入れ換えについての対称性は、四則演算をおこなっても崩れない（崩せない）。
- ある対称性を持っている数の全体は四則演算について閉じている（体をなす）。

すなわち、

- 数の集まりがあれば、それらの数全てが共通に持っている対称性の集まり（群）が考えられる。
- 対称性（操作）の集まりがあれば、その全てについて対称であるような数の集まり（体）が考えられる。

解 α, β は当然入れ替えに対して対称性を持たないのに係数は対称性を持ち、そして四則演算はこの対称性を保存するということも簡単に確認できた。
→係数から解を創り出すためには

「四則演算以外の、対称性を壊す武器」

が必要。

$$(\alpha - \beta)^2 = b^2 - 4c$$

なので[4]、両辺のルートをとって

$$\alpha - \beta = \pm\sqrt{b^2 - 4c}$$

[4]ちょっとした計算（暗算）によりわかる。

ここで

$$\alpha = \frac{\alpha + \beta}{2} + \frac{\alpha - \beta}{2}$$

より

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

を得る。β はこの符号を反転させたものになる。よって、二次方程式が解けたことになった。おめでとう。

入れ換え

今までは単純に $(\alpha\,\beta) \to (\alpha\,\beta)$ と $(\alpha\,\beta) \to (\beta\,\alpha)$ という入れ換えだけだったが、3つとなると事情が変わってくる。
結果から言えば

$$(\alpha\,\beta\,\gamma),\ (\alpha\,\gamma\,\beta),\ (\beta\,\alpha\,\gamma),$$

$$(\beta\,\gamma\,\alpha),\ (\gamma\,\alpha\,\beta),\ (\gamma\,\beta\,\alpha)$$

である。

ここで

$$
\begin{aligned}
e(\alpha\,\beta\,\gamma) &= (\alpha\,\beta\,\gamma) \\
\tau(\alpha\,\beta\,\gamma) &= (\alpha\,\gamma\,\beta) \\
\sigma(\alpha\,\beta\,\gamma) &= (\beta\,\gamma\,\alpha)
\end{aligned}
$$

とする。

$$
\begin{aligned}
e(\alpha\,\beta\,\gamma) &= (\alpha\,\beta\,\gamma) \\
\tau(\alpha\,\beta\,\gamma) &= (\alpha\,\gamma\,\beta) \\
\sigma(\alpha\,\beta\,\gamma) &= (\beta\,\gamma\,\alpha) \\
\tau\sigma(\alpha\,\beta\,\gamma) &= (\beta\,\alpha\,\gamma) \\
\sigma^2(\alpha\,\beta\,\gamma) &= (\gamma\,\alpha\,\beta) \\
\tau\sigma^2(\alpha\,\beta\,\gamma) &= (\gamma\,\beta\,\alpha)
\end{aligned}
$$

となる…… あれ？ 正三角形と同じじゃん！

対称群

こういったタイプの構造は**対称群**と呼ばれ、次のように定義される：

定義（対称群）

集合 X の置換とは全単射写像 $\sigma : X \to X$ である。置換全体は群の構造が自然に入り、これを置換群という。特に $X = \{1, 2, \ldots, n\}$ であればその置換群を n 次対称群 $\mathfrak{S}_n$ という。

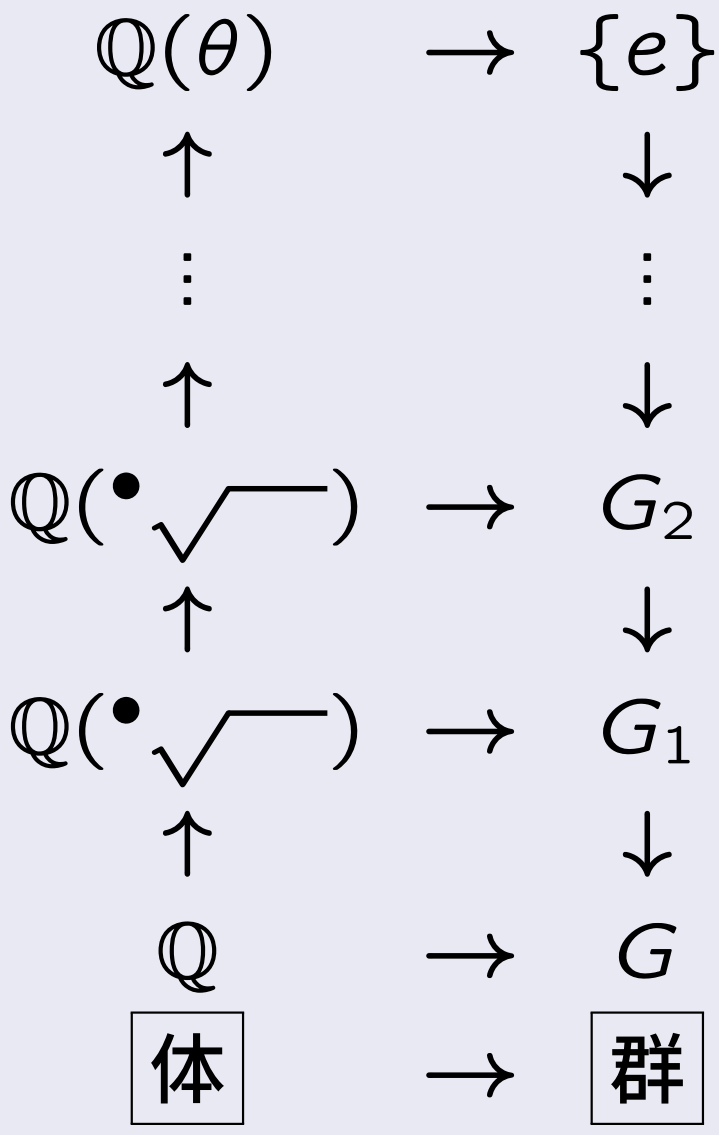
ここまで言っておいて、３次方程式の解き方は省略[5]。だが、ある数θが$+, -, \times, \div$に加えて、対称性を崩す武器：$\sqrt{}$で書けるかということが問題だということを考えればよい。

[5]時間と労力の都合。

ここで$\mathbb{Q}$は有理数体で、それに「ルート」という対称性を崩す道具を持ってくるとき$\mathbb{Q}(\bullet\sqrt{})$と書く。

このとき、対称性を崩していくとどのような挙動をするかということを逐一見ていき、最終的なところの性質を調べることにより、ある数が$+, -, \times, \div, \sqrt{}$で書けるかどうかがわかる！

ガロア理論の基本定理


$\mathbb{Q}(\theta)$ → $\{e\}$
↑ ↓
⋮ ⋮
↑ ↓
$\mathbb{Q}(\sqrt{\bullet})$ → G_2
↑ ↓
$\mathbb{Q}(\sqrt{\bullet})$ → G_1
↑ ↓
$\mathbb{Q}$ → G
体 → 群

という塔を作ったとき G が可解群と呼ばれるものなら、$\mathbb{Q}$ にベキ根を装備させつづけることで $\mathbb{Q}(\theta)$ に到達することができることがわかる。

そして $\mathfrak{S}_n$ は $n \geqq 5$ のときに可解群ではないことが示される[6]ので、示された。

[6] これは群論サイドの地道な結果。

ベキ根という道具をつけていく様子がそれに対応する群によって統制される

↓

体 K を有限次元ガロワ拡大して L になった際、そこまでの中間にある体を、そのガロア群と呼ばれる群 $\mathrm{Gal}(L/K)$ の部分群によって統制する分類理論

↓

1960 年代のアレキサンダー・グロタンディークが体上の有限エタール代数をその絶対ガロワ群により統制（絶対ガロワ理論）。

↓

最終目標：体上有限な代数の分類理論

絶対ガロワ群

それ自体、非常に重要な意義を持っている：

定理（ノイキルヒ-内田の定理（1976））

有限次拡大 $K/\mathbb{Q}$ と $K'/\mathbb{Q}$ に対し、絶対ガロワ群が位相群として同型であることと、体として同型であることが同値。

これは遠アーベル幾何の現象だと考えられる。また、絶対ガロワ群の情報を一般線型群に埋め込むことで得られるガロワ表現も重要な分野である。

微分ガロワ理論

今までは代数方程式だったが、微分方程式についても応用することができるのではないか？
→微分ガロワ理論
→$\int e^{-x^2}$が初等関数で表せないことや、三体問題が（ある程度の条件を課した上で）解けないことなどが証明できる！

ガロワの手紙

親愛なるオギュスト君。僕の研究したものがこのメモだけに留まらないことを君ならばよく知ってくれているだろう。……だが僕にはもう時間がない。それに僕の発想はまだこの限りなき（数学という）領域で通用するほど実り多きものにはなっていない。

……の部分は？

このごろは、主に**曖昧の理論** « la théorie de l'ambiguité » を超越解析学へ応用することばかりを考えていたのだ。超越量または函数のある関係において、どのような変換を行ったときに、つまり与えられた量をどのような量で置き換えたらならば、この関係が無意味になることがなくてすむか、を前もって知ることが望ましいのだ。このことで、探してきた多くの表示式は成り立たないことを認識することができる。

クライン：リーマン面や多重被覆のことではないか？
高木貞治：『はっきりとは解しかねるが、モノドロミー群などに関するものでもあろうか。』

実際、モノドロミー群に「被覆空間にまで拡張されたガロワ理論」を適用させることで、リーマンの存在定理というものを証明することができる。

ご清聴ありがとうございました。