数学の魅力をイメージする

ガロア理論のストーリー

（19 世紀のフランスの少年が作った理論）

松田 修

2024 年 2 月 21 日

本書のコンセプト

数学の問題にチャレンジし，それを一生懸命考えて，これはすばらしいと思う方法で解けたとき，あるいは，そんな方法で解けるのかと感心したとき，数学の魅力を感じた経験があるのではないだろうか．

本書は，ガロアという１９世紀のフランスの十代の少年が考えついた数学のアイディアを，高校１年生の数学の知識があれば読んでいけるように紹介したものである．

ガロアが取り組んだ問題は，

“5 次以上の方程式に解の公式はあるのか？”

という当時の未解決問題であった．

この問題を解決するために，ガロアは，“群”という道具を考えついた．そして方程式の解で構成される“体”という数の空間を，“群”で解析したのである．

そして，辿り着いたガロアの結論は以下であった．

『5 次以上の方程式の中には，$\sqrt{\ }$，$\sqrt[3]{\ }$，$\cdots$ などをどのように組み合わせても，
決して表示することができない解を持つものが存在する．』

しかしながら，一般の読者が厳密なガロア理論を学ぶためには，多くの新しい知識を獲得する必要がある．そして，結論までを正確に細かく追えば追うほど，なかなか大変な作業を行うことになり，ともすると局所的な議論に埋没してしまい，全体の流れを見失ってしまったりする．

ガロアが考えた理論の世界を，「とりあえず通読して，ある種の納得をしてみたい」

本書は，この立場から構成した．

本書によって，高校生や一般の読者が，ガロア理論という魅力を，少しでも感じていただけることを願っている．

導入：ガロア理論とは何か

ガロア理論は，１９世紀のフランスで誕生した．それは，ガロア (1811 年 10 月 25 日-1832 年 5 月 31 日) という十代の少年が作った理論で，与えられた方程式の解の形を理解するための理論である．

たとえば，2 次方程式 $x^2+3x+1=0$ の解は，2 乗根記号 $\sqrt{\ }$ を用いた解の公式があるために，それを使って

$$x=\frac{-3\pm\sqrt{5}}{2}$$

と解のかたちを見ることができる．

“3 乗根 2” と読まれる $\sqrt[3]{2}$ は，3 乗して 2 となる数のことで，3 次方程式 $x^3-2=0$ の解である．つまり，$\sqrt[3]{2}$ は $x^3-2=0$ の 1 つ目の解のかたちである．一般に，3 次方程式の 3 つの解はすべて $\sqrt{\ }, \sqrt[3]{\ }$ を組み合わせて表示されたかたちを見ることができる．さらに，4 次方程式の 4 つの解もすべて $\sqrt{\ }, \sqrt[3]{\ }, \sqrt[4]{\ }$ をいくつか組み合わせて表示されたかたちを見ることができる．

しかし，

『**定理**．5 次以上の方程式の中には，$\sqrt{\ }, \sqrt[3]{\ }, \cdots$ などをどのように組み合わせても，決して表示することができない解を持つものが存在する．』

ガロア理論とは，上の“どのようにしても求めることができないものが存在する”というフレーズが入った定理を，ガロアが発見した“群”と“体”という数学を使って，その証明の核心に迫っていくものである．

しかし，ガロア理論のストーリーを大まかに理解したいと思っても，ガロア群という少しばかり厄介な定義を理解しなければ，全容は見えてこない．そのため，それを理解するための準備に少しだけ時間がかかる．

本書では，準備段階も楽しめるように，納得いく解説に気を配り，簡単な例題でその意図を伝えるようにした．さらに，各章で扱った内容が，一目で振り返れるように，Memorize をつけた．ガロア群の定義は第 11 章で登場する．そこまでいけば，ゴールはすぐそこに見えてくる．

本書を読むための予備知識は，高校 1 年生程度の数学までで充分である．しかし，少しばかり考える持久力が必要である．陸上競技でたとえれば，中距離走程度の数学的思考の持久力が必要である．時に坂道もあるかもしれないが，ガロア理論の風景の中を，自分のペースを守りつつ，さわやかな汗をながしながら駆け抜けていけば，必ず完走できる．

目次

第 1 章

置換

ガロア理論の結論は,

『5 次以上の方程式の中には，$\sqrt{\ }$，$\sqrt[3]{\ }$，$\cdots$ などを
どのように組み合わせても,
決して表示することができない解を持つものが存在する.』

という定理である.

ガロア理論では，この定理を理解する方法として,“**置換**”によって構成される“**群**”と呼ばれる概念を用いる.“置換”とは，対象や値を「並べ替える」ことである．そして，ガロア理論で扱う置換の対象は，n 個の自然数 $1, 2, 3, \cdots, n$ である.“群”については第 2 章で述べる.

物事を並べ替えて考え方ることは，人間の自然な思考である．しかし，並べ替えるという言葉が,“置換”という数学的に意味をもつ言葉に変わり，その重要性が理解され始めたのは，18 世紀から 19 世紀に活躍したラグランジュ，ルフィニ，コーシー，アーベル，そしてガロアといった数学者たちの研究からである.

ガロア理論で扱う“置換”の扱い方に慣れるために，x^2 の係数が 1，x の係数が 2，定数項が 3 である 2 次式

$$x^2 + 2x + 3 \tag{1.1}$$

を考えよう．そして，係数である $1, 2, 3$ という数字の置換を考える．

例えば, 1 を 3 に, 3 を 2 に, 2 を 1 に入れ換える．この置換により, 方程式 (1.1) は

$$3x^2 + x + 2 \tag{1.2}$$

となる．

このとき，方程式の係数の 1 を 3 に，3 を 2 に，2 を 1 にするという置換

$$1 \to 3, \quad 3 \to 2, \quad 2 \to 1$$

という操作を，式の係数に**置換を作用させる**，という．そして，この操作を

$$(1\ 3\ 2)$$

という記号で表す．

すなわち，2 次式 $x^2 + 2x + 3$ の係数に置換 $(1\ 3\ 2)$ を作用させると，2 次式 $3x^2 + x + 2$ が得られる．このことを

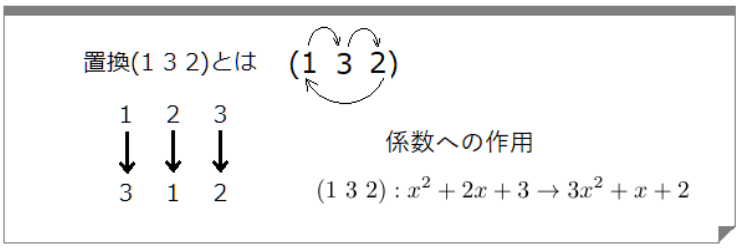
$$(1\ 3\ 2) : x^2 + 2x + 3 \to 3x^2 + x + 2 \tag{1.3}$$

と表す．

ここで，置換の記号 $(1\ 3\ 2)$ は，その意味から

$$(1\ 3\ 2) = (3\ 2\ 1) = (2\ 1\ 3)$$

であることを注意しよう．



さて，数字 $1,2,3$ の置換は全部で 6 個あり，それらは以下である．

$$(1\ 2),\ (1\ 3),\ (2\ 3),\ (1\ 2\ 3),\ (1\ 3\ 2),\ e$$

最後に書かれた記号 e は，入れ換えを行わない置換を表し，**恒等置換**とよぶ．

すなわち，

$$e : x^2+2x+3 \to x^2+2x+3$$

である．

そして，この 6 個の置換の集合を，記号で

$$S_3$$

と表す．S は対称性（Symmetry）の頭文字である．

置換の集合と対称性はどのような関係があるか？

実は，ガロア理論で扱う置換は，後で扱う対称式という式に作用するものとして考える．このため，頭文字 S が使われるのである．

4 個の数 $1,2,3,4$ から得られる置換の集合は，記号で S_4 と表す．

例えば,

$$(1\ 2)(3\ 4)$$

は S_4 の元で，これは 1 と 2 の置換，3 と 4 の置換を同時に表したものである.

例題 1. S_4 の元の個数は全部で 24 個あることを示せ.

（**解答**）これは $4 \times 3 \times 2 \times 1 = 24$ という計算から得られる．なぜならば，3 次式

$$ax^3 + bx^2 + cx + d \tag{1.4}$$

を考えて，係数 a, b, c, d に $1, 2, 3, 4$ の異なる数字を入れる方法は，a が 4 通り，b は a に入れた数字を除いて 3 通り，c が 2 通り，そして d が 1 通りだからである．□

$4 \times 3 \times 2 \times 1$ は，記号で 4! と書き，4 の**階乗** (factorial) と呼ぶ．この記号は 19 世紀にフランスのクランプという数学者が考案した.

一般に，n 個の数 $1, 2, \cdots, n$ から得られる置換の集合は，記号で S_n と表す．そして，S_n の元の個数は $n!$ であり，これを記号で

$$\sharp S_n = n!$$

と表す.

具体的には

$$\sharp S_2 = 2! = 2,\ \ \sharp S_3 = 3! = 6,\ \ \sharp S_4 = 4! = 24,\ \ \sharp S_5 = 5! = 120,\ \ \cdots$$

となる．以後，$\sharp S_n$ を S_n の**位数** (order) と呼ぶ.

Memorize：置換

・置換の集合 $S_3 = \{(1\ 2),\ (1\ 3),\ (2\ 3),\ (1\ 2\ 3),\ (1\ 3\ 2),\ e\}$
・置換の作用の例：$(1\ 3\ 2) : x^2 + 2x + 3 \to 3x^2 + x + 2$
・$\sharp S_n = n!$（S_n の位数は $n!$）

次の問題を解けますか？

問題 1. 3 次式 $3x^3 + 2x^2 + x + 4$ の係数に S_4 の次の置換を作用させると，どのような 3 次式が得られるか.

1. $(2\ 4\ 3)$　　2. $(1\ 3)(2\ 4)$

第 2 章

群

“群”(group)，この言葉はガロアが考案した．

“群”はガロア理論を理解するために不可欠な概念である．なぜならば，ある代数方程式が $\sqrt{}$，$\sqrt[3]{}$，$\cdots$ を組み合わせて解けるかどうか，それは，後に説明する“方程式のガロア群”によって判定できるからである．

“群”を理解するためには，2 つの置換の積という演算の方法を理解する必要がある．この計算法が分かれば，置換の集合である“群”のことが理解できるようになる．“群”とは単なる置換の集合ではなく，演算が定義されている集合のことなのである．

第 1 章と同様に 2 次式

$$x^2 + 2x + 3 \tag{2.1}$$

を考えよう．そして，この式に置換 (1 2 3) を作用させると，

$$(1\ 2\ 3) : x^2 + 2x + 3 \to 2x^2 + 3x + 1$$

となる．$2x^2 + 3x + 1$ に置換 (2 3) を作用させると，

$$(2\ 3) : 2x^2 + 3x + 1 \to 3x^2 + 2x + 1$$

となる．

2 次式 x^2+2x+3 に，最初に置換 (1 2 3) を作用させ，その後，得られた 2 次式 $2x^2+3x+1$ に置換 (2 3) を作用させることを

$$(2\ 3)(1\ 2\ 3) : x^2+2x+3 \to 2x^2+3x+1 \to 3x^2+2x+1$$

または簡単に

$$(2\ 3)(1\ 2\ 3) : x^2+2x+3 \to 3x^2+2x+1$$

と書く．

ここで得られた置換 (2 3)(1 2 3) から得られた係数の数字の動きを見てみる．

すると，1 は 3 に，3 は 1 に，そして 2 は 2 のままとなっていることがわかる．

すなわち，置換 (2 3)(1 2 3) は (1 3) である．

これを

$$(2\ 3)(1\ 2\ 3) = (1\ 3) \tag{2.2}$$

と表す．これは，置換の集合 S_3 に**積**という演算が定義されたことを意味する．

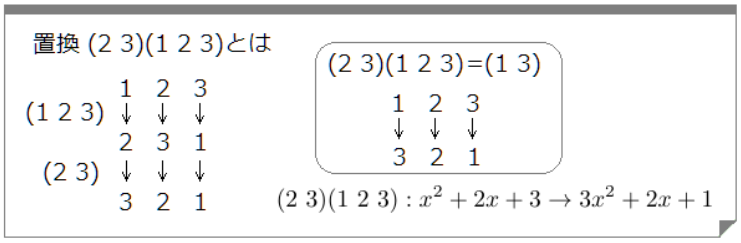
置換の積の計算は重要なので，等式 (2.2) の計算を再度確認する．

(2 3)(1 2 3) は右の置換 (1 2 3) から行うことである．これをしっかりと理解しておかないと計算を間違う．

例えば 1 は，置換 (1 2 3) により 2 に変わり，続いて 2 は置換 (2 3) により 3 に変わる．よって，1 は，(2 3)(1 2 3) により 3 に変わる．

同様に 3 は，置換 (1 2 3) により 1 に変わり，続いて 1 は，置換 (2 3) により 1 に変わる．よって 3 は，(2 3)(1 2 3) により 1 に変わる．

したがって，等式 (2.2) が得られる．



例題 2. (2 3)(1 2 3) $\neq$ (1 2 3)(2 3) であることを示せ．

（**解答**）2 次式 x^2+2x+3 に置換 (1 2 3)(2 3) を作用させると，

$$(1\ 2\ 3)(2\ 3) : x^2+2x+3 \to x^2+3x+2 \to 2x^2+x+3$$

となる．よって，

$$(1\ 2\ 3)(2\ 3) = (1\ 2) \tag{2.3}$$

である．したがって，2 つの等式 (2.2) と (2.3) から

$$(2\ 3)(1\ 2\ 3) \neq (1\ 2\ 3)(2\ 3)$$

である，□

例題 2 は，置換の集合 S_3 の 2 つの置換の積が，交換可能でないことを意味する．

交換可能であることを，**可換** (commutative)，交換可能でないことを，**非可換** (noncommutative) と呼ぶ．

したがって，S_3 は積について非可換である．

以下の表は，3 次対称群 S_3 の置換 σ（シグマ）と τ（タウ）の積 $\sigma\tau$ の計算結果をまとめたものである．たとえば，$\sigma = (1\ 3)$ と $\tau = (1\ 2\ 3)$ についての $(1\ 3)(1\ 2\ 3)$ の計算結果は，タテの $(1\ 3)$ の位置から右方向へ $(1\ 2\ 3)$ の列まで行き，$(1\ 2)$ が得られる．

σ \ τ	e	$(1\ 2)$	$(1\ 3)$	$(2\ 3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$
e	e	$(1\ 2)$	$(1\ 3)$	$(2\ 3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$
$(1\ 2)$	$(1\ 2)$	e	$(1\ 3\ 2)$	$(1\ 2\ 3)$	$(2\ 3)$	$(1\ 3)$
$(1\ 3)$	$(1\ 3)$	$(1\ 2\ 3)$	e	$(1\ 3\ 2)$	$(1\ 2)$	$(2\ 3)$
$(2\ 3)$	$(2\ 3)$	$(1\ 3\ 2)$	$(1\ 2\ 3)$	e	$(1\ 3)$	$(1\ 2)$
$(1\ 2\ 3)$	$(1\ 2\ 3)$	$(1\ 3)$	$(2\ 3)$	$(1\ 2)$	$(1\ 3\ 2)$	e
$(1\ 3\ 2)$	$(1\ 3\ 2)$	$(2\ 3)$	$(1\ 2)$	$(1\ 3)$	e	$(1\ 2\ 3)$

それでは，3 次対称群 S_3 は積に関して，非可換である性質以外に，どのような性質をもつのであろうか．それらは 3 つある．以下，それらを列挙していこう．

(性質 1) 恒等置換 e については，S_3 のどんな置換 σ に関しても

$$e\sigma = \sigma e = \sigma$$

が成り立つ．

(性質 2) S_3 のどんな置換 σ に関してもその**逆置換** σ' が存在する．すなわち，

$$\sigma\sigma' = \sigma'\sigma = e$$

となる σ' が存在する．

(性質 3) **結合法則**が成り立つ．すなわち，S_3 のどんな置換 σ, τ, η（エータ）に対しても

$$\sigma(\tau\eta) = (\sigma\tau)\eta$$

が成り立つ．

性質 1 は明らかである．性質 2 と性質 3 については，具体的な例で確認しておく．

例題 3. 置換 (1 3 2) と置換 (1 2) の逆置換をそれぞれ求めよ．

（**解答**）置換 (1 3 2) に対して，置換 (2 3 1) を考えると

$$(1\ 3\ 2)(2\ 3\ 1) = e, \quad (2\ 3\ 1)(1\ 3\ 2) = e$$

となる．よって (1 3 2) の逆置換は (2 3 1) である．

置換 (1 2) に対しては (1 2) 自身を考えればよい．つまり

$$(1\ 2)(1\ 2) = e$$

となる．よって (1 2) の逆置換は (1 2) である．□

例題 3 から，すぐに $(1\ 3)(1\ 3) = e$, $(2\ 3)(2\ 3) = e$ などが想像できる．一般に，対称群 S_n において，

$$(i\ j)(i\ j) = e$$

が成り立つ．置換 $(i\ j)$ を**互換**という．

例題 4. $(1\ 2\ 3)\{(2\ 3)(1\ 3\ 2)\} = \{(1\ 2\ 3)(2\ 3)\}(1\ 3\ 2)$ を示せ．

（**解答**）

$$(1\ 2\ 3)\{(2\ 3)(1\ 3\ 2)\} = (1\ 2\ 3)(1\ 2) = (1\ 3)$$

$$\{(1\ 2\ 3)(2\ 3)\}(1\ 3\ 2) = (1\ 2)(1\ 3\ 2) = (1\ 3)$$

よって，

$$(1\ 2\ 3)\{(2\ 3)(1\ 3\ 2)\} = \{(1\ 2\ 3)(2\ 3)\}(1\ 3\ 2)$$

が成り立つ．□

S_3 の性質
（性質 0） 非可換： $\sigma\tau \neq \tau\sigma$
（性質 1） 単位元 e： $e\sigma=\sigma e=\sigma$
（性質 2） σ の逆置換 σ' の存在： $\sigma\sigma'=\sigma'\sigma=e$
（性質 3） 結合法則： $\sigma(\tau\eta)=(\sigma\tau)\eta$

単位元の存在，逆元の存在，結合法則という 3 つの性質は，当然，S_4 も S_5 も，一般の S_n も成り立つ．このよう性質をもつ集合が“群”というものである．以下が，群の定義である．

【群の定義】　集合 G の任意の 2 つの**元**（要素のこと）σ と τ に対して積 $\sigma\tau$ が定義されていて，G の元が以下の 3 つの性質を満たすとき，G は**群**であるという．

（性質 1）単位元 e の存在，すなわち，G の任意の元 σ に対して

$$e\sigma = \sigma e = \sigma$$

となる e が存在する．e を**単位元**という．
（性質 2）逆元の存在，すなわち，G の任意の元 σ に対して

$$\sigma\sigma' = \sigma'\sigma = e$$

となる σ' が存在する．σ' を σ の**逆元**といい，σ^{-1} と表す．
（性質 3）結合法則が成り立つ．すなわち，G の任意の置換 σ, τ, η に対して

$$\sigma(\tau\eta) = (\sigma\tau)\eta$$

が成り立つ．

以上のことから，集合 S_n は置換の積で群となる．S_n のことを n **次対称群**と呼ぶ．

Memorize：置換がつくる群

・3 次対称群 $S_3 = \{(1\ 2),\ (1\ 3),\ (2\ 3),\ (1\ 2\ 3),\ (1\ 3\ 2),\ e\}$
・非可換性：$(2\ 3)(1\ 2\ 3) \neq (1\ 2\ 3)(2\ 3)$
・単位元 e の存在：$e(1\ 3\ 2) = (1\ 3\ 2)e = (1\ 3\ 2)$
・逆元の存在：$(1\ 3\ 2)(1\ 2\ 3) = (1\ 2\ 3)(1\ 3\ 2) = e$, $(1\ 2)(1\ 2) = e$
・結合法則：$(1\ 2\ 3)\{(2\ 3)(1\ 3\ 2)\} = \{(1\ 2\ 3)(2\ 3)\}(1\ 3\ 2)$

次の問題を解けますか？

問題 2. 4 次対称群 S_4 の置換 $(2\ 4\ 3)\ (1\ 3\ 4\ 2)$ について，以下を求めよ.

1. $(2\ 4\ 3)(1\ 3\ 4\ 2)$ の計算結果
2. $(2\ 4\ 3)$ の逆置換
3. $(1\ 3\ 4\ 2)$ の逆置換

第 3 章

基本対称式

n 個の数 $1, 2, \cdots, n$ の置換の集合を S_n と表し，n 次対称群と呼んだ．S_n は“対称”という言葉と，どのように繋がっているのだろうか．実は，ガロア理論で，置換を作用させる対象は，方程式の係数ではなく，方程式の解である．

ガロア理論では，この後説明する方程式における“解と係数の関係式”，そしてそれから得られる“基本対称式”と呼ばれるものに着目する．なぜならば，“基本対称式”には，考えている方程式の解に，どのような置換を作用させても，それらの値が変化しないという“不変性”があるからである．そして，この不変性を，後で扱う“体”という世界に応用し，ガロア理論が展開されていく．

a と b を**有理数**とする．有理数とは，整数または分数のことで，記号で $\mathbb{Q}$ と表す．そして，全ての係数が有理数である方程式を，$\mathbb{Q}$ **係数の方程式**と呼ぶ．

$\mathbb{Q}$ 係数の 2 次方程式 $x^2 + ax + b = 0$ を考えよう．そして，その解を x_1, x_2 としよう．このとき，考える群は 2 次対称群

$$S_2 = \{e,\ (1\ 2)\}$$

である．そして，解の組 (x_1, x_2) に置換 $(1\ 2)$ を作用させるとは，

$$(1\ 2) : (x_1, x_2) \to (x_2, x_1)$$

とすることである．

例題 5. $\mathbb{Q}$ 係数の 2 次方程式

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

の解を x_1，x_2 とするとき，$x_1 + x_2$ と x_1x_2 は，2 次対称群 S_2 のどの置換の作用においても不変であり，これらは，どちらも有理数であることを示せ．

（**解答**）$S_2 = \{e,\ (1\ 2)\}$ であることから，$x_1 + x_2$ と x_1x_2 は，置換 e と $(1\ 2)$ のどちらの置換の作用でも不変であることは明らかである．

次に，$x_1 + x_2$ と x_1x_2 は，どちらも有理数であることを示す．

2 次方程式の解は，x_1 と x_2 であることから，

$$x^2 + ax + b = (x - x_1)(x - x_2) \tag{3.1}$$

となる．右辺を展開すると，

$$\text{右辺} = x^2 - (x_1 + x_2)x + x_1x_2 \tag{3.2}$$

なので，(3.1) と (3.2) より，解と係数の関係式

$$x_1 + x_2 = -a, \quad x_1x_2 = b \tag{3.3}$$

が得られる．したがって，$x_1 + x_2$ と x_1x_2 はどちらも有理数である．□

式 (3.3) はどちらも方程式の解による**基本対称式**と呼ばれる．方程式の解からつくられた基本対称式は群 S_2 の置換の作用によって変化しない式なのである．

このことを，方程式の解による基本対称式は，解 x_1, x_2 に対する 2 次対称群 S_2 の**作用で不変**であるという．

2次方程式 $x^2+ax+b=0$ の
解 x_1 ,x_2 による基本対称式
$x_1+x_2=-a$,　$x_1x_2=b$

例題 6. $\mathbb{Q}$ 係数の 3 次方程式

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

の解を x_1, x_2, x_3 とすると，方程式の解による基本対称式 $x_1+x_2+x_3$ と $x_1x_2+x_2x_3+x_3x_1$ と $x_1x_2x_3$ は，3 次対称群 S_3 のどの置換の作用においても不変であり，いずれも有理数であることを示せ.

（**解答**）$S_3=\{e,\ (1\ 2),\ (1\ 3),\ (2\ 3),\ (1\ 2\ 3),\ (1\ 3\ 2)\}$ であることから，方程式の解による基本対称式 $x_1+x_2+x_3$ と $x_1x_2+x_2x_3+x_3x_1$ と $x_1x_2x_3$ は，S_3 のどの置換の作用でも不変であることは明らかである.

3 次方程式の解は，x_1 と x_2 と x_3 であることから，

$$x^3+ax^2+bx+c=(x-x_1)(x-x_2)(x-x_3) \tag{3.4}$$

となる．右辺を展開すると，

$$\text{右辺}=x^3-(x_1+x_2+x_3)x^2+(x_1x_2+x_2x_3+x_3x_1)x-x_1x_2x_3 \tag{3.5}$$

なので，(3.4) と (3.5) より，基本対称式

$$x_1+x_2+x_3=-a,\quad x_1x_2+x_2x_3+x_3x_1=b,\quad x_1x_2x_3=-c \tag{3.6}$$

が得られる.

したがって，$x_1+x_2+x_3$ と $x_1x_2+x_2x_3+x_3x_1$ と $x_1x_2x_3$ はどれも有理数である．□

一般に，$\mathbb{Q}$ 係数の n 次方程式

$$x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n = 0 \tag{3.7}$$

を考える．このとき，(3.7) の解 $x_1, x_2, \cdots, x_n$ による基本対称式は以下である．

$$\begin{aligned}
&x_1 + x_2 + \cdots + x_n = -a_1 \\
&x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n = a_2 \\
&x_1x_2x_3 + x_1x_2x_4 + \cdots + x_{n-2}x_{n-1}x_n = -a_3 \\
&\cdots\cdots\cdots\cdots \\
&x_1x_2\cdots x_n = (-1)^n a_n
\end{aligned} \tag{3.8}$$

そして，方程式の解による基本対称式 (3.8) は，解 $x_1, x_2, \cdots, x_n$ に対する n 次対称群 S_n の作用で不変である．

Memorize：基本対称式

3 次方程式 $x^3 + ax^2 + bx + c = 0$ の解 x_1, x_2, x_3 と方程式の解による基本対称式

$$x_1 + x_2 + x_3 = -a, \quad x_1x_2 + x_2x_3 + x_3x_1 = b, \quad x_1x_2x_3 = -c$$

は，3 次対称群 S_3 の置換で不変である．

次の問題の証明の流れをイメージすることができますか？

問題 3. $\mathbb{Q}$ 係数の 4 次方程式 $x^4 + ax^2 + bx + c = 0$ の解を x_1, x_2, x_3, x_4 とするとき，この方程式の解による基本対称式を導き，それが，S_4 の置換で不変であること，及び，基本対称式の値が有理数であることを証明せよ．

第 4 章

整数の分割と同値関係

例えば，n を自然数として，$(-1)^n$ の値を求めてみる．このとき，n に 1 から順に自然数を当てはめて，いちいち計算結果を出す必要はない．なぜならば，n が偶数なら $(-1)^n = 1$ であり，n が奇数なら $(-1)^n = -1$ だからである．

このように扱う数の集合を，同じ性質で分割して考えた方が，目的としている答えが明確になる場合がある．そして，ガロア理論においては，群の分割が重要になる．

この章では，群を分割するための方法に繋げるために，整数全体 $\mathbb{Z}$ を割り算を使って分割し．分割されたそれぞれの集合の元たちの中にある関係性を，数式で表すことを目的とする．その数式で使う記号は $\sim$（“チルダ”と呼んだりする）であり，これは“同値関係”と呼ばれるものである．

整数全体 $\mathbb{Z}$ の数を 2 で割ると，$\mathbb{Z}$ の数は 2 で割り切れるもの（偶数）と，2 で割って 1 余るもの（奇数）に分割される．つまり，$\mathbb{Z}$ は以下のように分割される．

$$\mathbb{Z} = \{0, \pm 2, \pm 4, \pm 6, \cdots\} \oplus \{\pm 1, \pm 3, \pm 5, \pm 7, \cdots\}$$

ここで，記号 $\oplus$ は**直和**と呼ばれる記号であるが，２つの集合に共通部分がないように分割したという意味である．

$\mathbb{Z}$ の数を 3 で割ると，$\mathbb{Z}$ の数は，3 で割り切れるものと，3 で割って 1 余るものと，3 で割って 2 余るものに分割される．つまり，$\mathbb{Z}$ は以下のように分割される．

$$\mathbb{Z} = \{0, \pm 3, \pm 6, \pm 9, \cdots\} \oplus \{\cdots, -5, -2, 1, 4, \cdots\} \oplus \{\cdots, -4, -1, 2, 5, \cdots\}$$

分割された各集合は，**クラス**または**同値類**と呼ばれる．

そして，分割された同じクラスに含まれる数同士は**同値**であるという．

以下，数 a が含まれるクラスを $C(a)$ と書き，“クラス a”と呼ぶことにする．

同値ということに関しては，たとえば 0 を含むクラス $C(0) = \{0, \pm 3, \pm 6, \pm 9, \cdots\}$ では，0 と 0 は同値，0 と 3 は同値，3 と 6 は同値，3 と 9 は同値，6 と 9 も同値などなどといえる．これらをまとめて，

『$0, \pm 3, \pm 6, \pm 9, \cdots$ は，すべて 0 と同値である』

ということもできる．

ところで，整数全体 $\mathbb{Z}$ は足し算という演算により群となっている．

なぜならば，$\mathbb{Z}$ の元 m に対して $m + 0 = 0 + m = m$ なので，単位元となる 0 が存在し，$m + (-m) = (-m) + m = 0$ であることから，逆元 $-m$ も明らかに $\mathbb{Z}$ に存在するからである．

そして，$\mathbb{Z}$ の 0 を含むクラスである

$C(0) = \{0, \pm 3, \pm 6, \pm 9, \cdots\}$ も群である．

なぜならば，$C(0)$ には単位元である 0 が含まれている，すなわち $3m + 0 = 0 + 3m = 3m$ であり，$C(0)$ の元である $3m$ の逆元 $-3m$ も $C(0)$ に含まれている，すなわち $3m + (-3m) = (-3m) + 3m = 0$ だからである．

$C(0)$ は群 $\mathbb{Z}$ の部分集合であり，かつ群であることから，$\mathbb{Z}$ の**部分群**と呼ばれる．

これに対し，$C(0)$ 以外の 2 つのクラス

$$C(1) = \{\cdots, -5, -2, 1, 4, \cdots\}, \quad C(2) = \{\cdots, -4, -1, 2, 5, \cdots\}$$

は，どちらも $\mathbb{Z}$ の部分群ではない．なぜならば，どちらにも単位元 0 が含まれていないからである．

そこで，これから，$C(0)$ は群 $\mathbb{Z}$ の部分群ということを中心に，$\mathbb{Z}$ の分割を考え直すという作業を行う．具体的には，$C(1)$ と $C(2)$ をそれぞれ，部分群 $C(0)$ とどのような関係にあるのかを調べてみる．

しかし，なぜ，考え直す作業が必要なのか？

それは，次節で扱う群の分割の方法に繋がるからである．

それでは，たとえば 1 を含むクラス

$$C(1) = \{\cdots, -5, -2, 1, 4, \cdots\}$$

を眺めてみよう．すると，

$-2-(-5) = 3,\ 1-(-2) = 3,\ 4-1 = 3,\ 4-(-2) = 6,\ 1-(-5) = 6,\ 4-(-5) = 9,\ \cdots$

などの $C(1)$ の 性質が見える．

これは，$C(1)$ の 2 つの数 a と b がどのような数だろうと，必ず $a - b$ は 3 の倍数，すなわち $a - b$ は $C(0)$ の数になるということを意味する．

この観点から，2 を含むクラス

$$C(2) = \{\cdots, -4, -1, 2, 5, \cdots\}$$

を見ても，やはり $C(2)$ の 2 つの数 c と d がどのような数だろうと，$c-d$ は $C(0)$ の数となっていることがわかる．

以上のことを整理してみると，

『a と b が同じクラスに入ることは，$a-b$ が $C(0)$ の数ということである』

となる．

ところで，同じクラスに含まれる数同士は，同値であるといったが，a と b が同値であることを，記号 $\sim$（チルダ）を使って，

$$a \sim b$$

と表す．そして，$\sim$ は同値な a と b を関係付ける記号ということから**同値関係**と呼ばれる．

同値関係 $\sim$ を用いると，$C(1)$ と $C(2)$ の性質が

$$a \sim b \iff a-b \in C(0)$$

というように記述できる．ここで，記号 $\in$ はその集合の元であるという意味である．

この同値関係 $\sim$ は，以下の 3 つの性質をもつことが証明できる．実は，現代数学では，以下の 3 つの性質を同値関係の定義としている．

（性質 1）$a \sim a$

（性質 2）$a \sim b$ ならば $b \sim a$

（性質 3）$a \sim b$ かつ $b \sim c$ ならば $a \sim c$

性質 1 が成り立つことは明らかである．

性質 2 については，$a \sim b$ であるということは，$a - b \in C(0)$ ということであり，これは，$b - a \in C(0)$ と同じ意味なので，$b \sim a$ となる．

例題 7.（性質 3）$a \sim b$ かつ $b \sim c$ ならば $a \sim c$ を証明せよ．

（解答） $a - c = (a - b) + (b - c)$ とする．$a \sim b \iff a - b \in C(0)$，そして $b \sim c \iff b - c \in C(0)$ である．そして，$C(0)$ は群であることから

$$a - c = (a - b) + (b - c) \in C(0)$$

となる．したがって，$a \sim c$ である．□

$a \sim b$：aとbが同値であること
$a \sim b$とは，$a-b \in C(0)$
つまり，$a-b$が3の倍数であることをである．

数 a に対して記号 $a + C(0)$ を

$$a + C(0) = \{a + 0,\ \ a \pm 3,\ a \pm 6,\ a \pm 9,\ \cdots\}$$

という集合とする．すなわち，$a + C(0)$ は a と $C(0)$ のすべての数との足し算から得られる集合とする．

例題 8. 以下の関係式を証明せよ．

$$C(1) = 1 + C(0),\ \ C(2) = 2 + C(0)$$

（解答） まず，a を $C(1)$ の任意の数とする．このとき，$a \sim 1$ であるため，

$a-1 \in C(0)$ となる．これは，$C(1) = 1 + C(0)$ を意味する．同様に，c を $C(2)$ の任意の数とする．このとき，$c \sim 2$ であるため，$c-2 \in C(2)$ となる．これは，$C(2) = 2 + C(0)$ を意味する．□

Meomorize：$\mathbb{Z}$ の数を分割する方法と同値関係

整数全体 $\mathbb{Z}$ の数を 3 で割るということは，$\mathbb{Z}$ の数を 3 で割った余りが 0 である部分群 $C(0)$ を中心に，同値関係 $\sim$ で，$\mathbb{Z}$ をクラスに分割することである．

$$\mathbb{Z} = C(0) \oplus C(1) \oplus C(2)$$

$$a \sim b \iff a - b \in C(0)$$

$$C(1) = 1 + C(0), \quad C(2) = 2 + C(0)$$

次の 3 つの問題に答えることができますか？

問題 4. 整数全体 $\mathbb{Z}$ は足し算で群となるが，掛け算では群とならない理由を述べよ．

問題 5. 同値関係 $\sim$ の 3 つの性質を述べよ．

問題 6. 整数全体 $\mathbb{Z}$ を 5 つのクラスに分割する方法を述べよ．さらに，そのクラスの中で $\mathbb{Z}$ の部分群であるものはどれか説明せよ．

第 5 章

商群と well-defined

ガロア理論では，方程式の群に対して，余りの計算ような計算方法から“商群”と呼ばれる新しい群を構成し，それによって，方程式の解のあり方を調べていく．このことを理解するためには，整数の余りの計算のしくみを理解している必要がある．

整数全体 $\mathbb{Z}$ を 7 で割って，クラス分けすることは，日という時間を，曜日というラベルをつけたクラスに分割することである．

たとえば，日曜日を余り 0 のクラス，月曜日を余り 1 のクラス，以下同様に曜日と余りを対応させておく．

そして，「今日が金曜日なら 100 日後は何曜日か？」という問題を考える．

金曜日は余り 5 のクラスなので，100 日後は，$5 + 100 = 105$ を 7 で割った余りを求めればよい．

したがって，105 を 7 で割った余りは 0 より，答えは日曜日となる．

しかし，最初から 100 を 7 で割った余りを 2 とした上で，

「$5 + 2 = 7$ を 7 で割った余りは 0 なので，答えは日曜日となる」

としてもよい．

ではなぜ，余りの計算では，余り同士の足し算をすることが許されるのか？ つまり，与えられた数同士の足し算を計算してその後余りを求めても，与えられた数の余り同士を計算しても，得られる結果はなぜ同じになるのか？

ガロア理論では，このことの意味をきちんと理解することが求められる．そして，その理解に必要な獲得しなければならないキーワードが 2 つある．

それは，“商群”と“well-defined”である．

ショウグン？　この言葉だけでは，その数学はなかなかイメージできない．

整数全体 $\mathbb{Z}$ の数を素数 3 で割って，$\mathbb{Z}$ をクラスに分割することを，

$$\mathbb{Z} = C(0) \oplus C(1) \oplus C(2)$$

と表した．また，整数全体 $\mathbb{Z}$ は足し算で群であった．さらに，このクラスの中の $C(0)$ も足し算で群となっており，$C(0)$ を $\mathbb{Z}$ を部分群と呼んだ．

そこで $C(0), C(1), C(2)$ の集合を

$$\mathbb{Z}/C(0) = \{C(0), C(1), C(2)\}$$

と書くこととし，

これを $\mathbb{Z}$ の $C(0)$ による**商集合**と呼ぶ．

そして，$C(j)$ に表された数 j を $C(j)$ の**代表元**という．

代表元という言葉から，$C(j)$ の j は，何か特別な元であるかのようなイメージをもたれるかもしれない．

しかし，ここで使う代表元という言葉は，単に，そのクラスの中から適当に選んだ 1 つの元というだけの意味である．

したがって，各 $C(j)$ の代表元は，$0, 1, 2$ でなくてもよいので，$a \in C(0)$，$b \in C(1)$，$c \in C(2)$ なら，

$$\mathbb{Z}/C(0) = \{C(a), C(b), C(c)\}$$

と表してもよいのである．このとき，

$$C(a) = C(0), \quad C(b) = C(1), \quad C(c) = C(2)$$

であることを，改めて注意しておく．

さて，もし商集合 $\mathbb{Z}/C(0)$ 内の演算が，$\mathbb{Z}$ 内の足し算を利用して定義できれば，$\mathbb{Z}/C(0)$ は群となるはずである．そこで，商集合 $\mathbb{Z}/C(0)$ 内の演算を j, k を代表元とするクラス $C(j)$，$C(k)$ に対して，

$$C(j) + C(k) = C(j + k)$$

と定義してみる．

この定義を，$\mathbb{Z}$ の数を素数 3 で割った 3 つのクラスで具体的に書けば，例えば，$j = 5, k = 11$ なら $C(5) + C(11) = C(16) = C(1)$ とし，$j = 10, k = 20$ なら $C(10) + C(20) = C(30) = C(0)$ というように定義する，ということである．

《疑問》この定義をすることは本当に可能なのだろうか？ この定義による計算結果は，自分が選んだ代表元によって，結果が変わってしまうようなことが起こらないのだろうか？ もし，この 2 つの疑問が解決しないならば，上の定義は演算として機能していないことになる．つまり，商集合 $\mathbb{Z}/C(0)$ を群と考えることはできない．このようなことを正しくチェックするには，どうすればよいだろうか？

例題 9. 商集合 $\mathbb{Z}/C(0)$ 内の演算 $C(j)+C(k) = C(j+k)$ の定義は，**well-defined** であること，すなわち，これは定義可能であり，代表元を取り替えて計算しても結果は同じであることを示せ．また，$\mathbb{Z}/C(0)$ は群であることを示せ．

（**解答**）j も k も $0, 1, 2$ のいずれかの数とする．$C(j) = j+C(0)$, $C(k) = k+C(0)$ であること，$k + C(0) = C(0) + k$ であること，そして $C(0) + C(0) = C(0)$ であることに注意して，計算していくと，

$$\begin{aligned} C(j) + C(k) &= \{j + C(0)\} + \{k + C(0)\} \\ &= j + \{C(0) + k\} + C(0) \\ &= j + \{k + C(0)\} + C(0) \\ &= (j + k) + C(0) + C(0) = (j + k) + C(0) \\ &= C(j + k) \end{aligned}$$

が得られる．これは，$C(j) + C(k) = C(j + k)$ が定義可能であることを意味する．

次に，代表元を取り替えて計算しても結果は同じであることを示す．

a をクラス $C(j)$ の代表元として，b をクラス $C(k)$ の代表元として，それぞれ選びなおす．このとき，$C(a) = C(j)$, $C(b) = C(k)$ に注意する．

証明すべきことは，$C(a + b) = C(j + k)$ である．

定義の通り計算すると，

$$C(a + b) = C(a) + C(b) = C(j) + C(k) = C(j + k)$$

である．

これは，$\mathbb{Z}/C(0)$ の演算が，代表元の選び方によらず定義できていることを意味する．以上により，$C(j) + C(k) = C(j + k)$ の定義は，well-defined である．

また，単位元は $C(0)$ であり，$C(1)$ の逆元は $C(2)$ であり，結合法則は明らかなので，商集合 $\mathbb{Z}/C(0)$ は群となる．□

例題 9 から，商集合 $\mathbb{Z}/C(0)$ は群となることがいえた．

群となった $\mathbb{Z}/C(0)$ を，$\mathbb{Z}$ の $C(0)$ による**商群**または**剰余群**という．

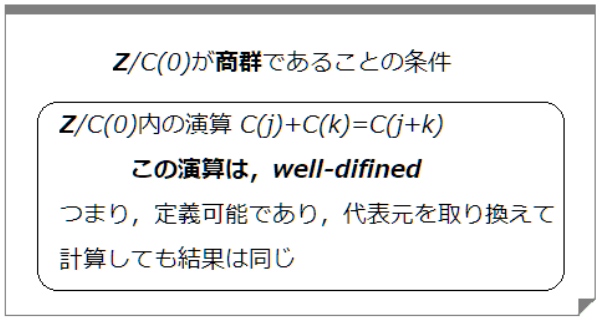
$\mathbb{Z}/C(0)$ を，$\mathbb{Z}_3$ という記号で表すこともある．

また，$\sharp\mathbb{Z}_3 = 3$，すなわち $\mathbb{Z}_3$ の位数は 3 であることも確認しておく．

ところで，例題 9 の解答の中には，次の章に繋がる注意点がある．それは，

$$C(0) + j = j + C(0)$$

という演算の交換法則が成り立っているという点である．このことは意識しておく必要がある．



例題 10. 整数全体 $\mathbb{Z}$ の数を素数 3 で割って作った集合 $\mathbb{Z}_3 = \mathbb{Z}/C(0)$ から $C(0)$ を除いた集合を $\mathbb{Z}_3^{\times} = \{C(1), C(2)\}$ とする．このとき，$\mathbb{Z}_3^{\times}$ の演算を

$$C(j) \cdot C(k) = C(j \cdot k)$$

と定義することは *well-defined* であること，そして，この定義により $\mathbb{Z}_3^{\times}$ は群となることを示せ．

（解答）　j も k も $1, 2$ のいずれかの数とする．$C(j) = j + C(0)$, $C(k) = k + C(0)$ であり，また $C(0)$ の数は $3n$（ただし $n = 0, \pm 1, \pm 2, \cdots$ ）と書けるので

$$j \cdot C(0) = C(0) \cdot j = C(0), \quad k \cdot C(0) = C(0) \cdot k = C(0)$$

であることに注意する．したがって，

$$\begin{aligned} C(j)\cdot C(k) &= \{j+C(0)\}\cdot\{k+C(0)\} \\ &= (j\cdot k)+\{j\cdot C(0)\}+\{C(0)\cdot k\}+C(0) \\ &= (j\cdot k)+\{C(0)+C(0)+C(0)\} \\ &= (j\cdot k)+C(0) \\ &= C(j\cdot k) \end{aligned}$$

となる．これは，演算 $C(j)\cdot C(k)=C(j\cdot k)$ が定義可能であることを意味する．

さらに，a を $C(j)$ の代表元，b を $C(k)$ の代表元として選び直すと，$C(a)=C(j)$，$C(b)=C(k)$ より，

$$C(a\cdot b)=C(a)\cdot C(b)=C(j)\cdot C(k)=C(j\cdot k)$$

であることから，この定義は，代表元の選び方で計算結果は変化しないことを意味する．以上により，演算 $C(j)\cdot C(k)=C(j\cdot k)$ の定義は，well-defined である．

また，単位元は $C(1)$ であり，$C(2)$ の逆元は $C(2)$ であり，結合法則は明らかなので，$\mathbb{Z}_3^{\times}$ は群である．□

例題 10 の解答の中にある次の章に繋がる注意点は，

$$C(0)\cdot a_2=a_2\cdot C(0)$$

という演算の交換法則である．このことも意識しておく必要がある．

Memorize：商群 $\mathbb{Z}/C(0)$ と well-defined

商群 $\mathbb{Z}/C(0) = \{C(0), C(1), C(2)\}$ の演算を

$$C(j) + C(k) = C(j + k)$$

$\{\mathbb{Z}/C(0)\}^{\times} = \{C(1), C(2)\}$ の演算を

$$C(j) \cdot C(k) = C(j \cdot k)$$

と定義することは well-defined である.

次の問題に答えることができますか？

問題 7. 整数全体 $\mathbb{Z}$ の数を素数 5 で割って作った商集合

$$\mathbb{Z}_5 = \mathbb{Z}/C(0) = \{C(0), C(1), C(2), C(3), C(4)\}$$

から $C(0)$ を除いた集合を $\mathbb{Z}_5^{\times} = \{C(1), C(2), C(3), C(4)\}$ とする.

このとき，$\mathbb{Z}_5^{\times}$ の演算を

$$C(j) \cdot C(k) = C(j \cdot k)$$

と定義することは，*well-defined* か．また，$\mathbb{Z}_5^{\times}$ は群となることを示せ.

第 6 章

対称群から商群をつくる

ガロア理論で使われる重要な道具，それは対称群 S_n をクラス分けして得られる商群である．そして商群をつくるための重要な部品が“正規部分群”と呼ばれるものである．この章で，私たちはこれらのアイテムを手にいれる．

商群 $\mathbb{Z}/C(0) = \{C(0), C(1), C(2)\}$ 内の演算は

$$C(j) + C(k) = C(j + k)$$

と定義できた．それはなぜか？　その理由は，第 5 章で注意した点

$$j + C(0) = C(0) + j \tag{6.1}$$

ということにある．同様に，$\mathbb{Z}_3^{\times} = \{C(1), C(2)\}$ の演算が

$$C(j) \cdot C(k) = C(j \cdot k)$$

と定義できる理由も，第 5 章の終わりで注意した点

$$a_1 \cdot C(0) = C(0) \cdot a_1 \tag{6.2}$$

ということにある．

それでは，対称群

$$S_3 = \{e,\ (1\ 2),\ (1\ 3),\ (2\ 3),\ (1\ 2\ 3),\ (1\ 3\ 2)\}$$

について考えよう．

S_3 の置換 $\sigma,\ \tau$ は特別なものを除けば $\sigma\tau \neq \tau\sigma$ であった．ところが S_3 の部分群に視点を移すと，

$$C(e) = \{e,\ (1\ 2\ 3), (1\ 3\ 2)\}$$

は，S_3 の特別な部分群となっている．

この特別という意味は，$C(e)$ がどんな $\sigma \in S_3$ に対しても

$$\sigma C(e) = C(e)\sigma \tag{6.3}$$

を満たすという意味である．

ここで，$\sigma C(e)$ は，σ と $C(e)$ の任意の元 τ との積 $\sigma\tau$ を表し，$C(e)\sigma$ は，$C(e)$ の任意の元 τ と σ の積 $\tau\sigma$ を表す．

実際，$H = \{(1\ 2),\ (1,\ 3), (2,\ 3)\}$ とすると，簡単な計算から

$$(1\ 2)C(e) = H = C(e)(1\ 2)$$
$$(1\ 3)C(e) = H = C(e)(1\ 3)$$
$$(2\ 3)C(e) = H = C(e)(2\ 3)$$

がわかる．よって，$C(e)$ は式 (6.3) を満たす．

すでに気づいていると思うが，式 (6.3) は (6.1) と (6.2) に共通する式である．

式 (6.3) で示されている性質が，ガロア理論の中で重要である商群といわれるものに繋がるのである．

そこで，以下 $\sigma C(e) = C(e)\sigma$ を

$$C(\sigma)$$

と書くことにする．

ところで，$C_1(e) = \{e,\ (1\ 2)\}$，$C_2(e) = \{e,\ (1\ 3)\}$，$C_3(e) = \{e,\ (2\ 3)\}$ は，どれも S_3 の部分群ではあるが，式 (6.3) を満たさないため，S_3 の特別な部分群とはなっていない．この点も指摘しておく．

それでは，ガロア理論で重視する商群 $S_3/C(e)$ を構成していこう．

そのためには，S_3 を $C(e)$ を用いてクラスに分解する必要がある．このことは $\sigma, \tau \in S_3$ に対して，同値関係 $\sim$ が定義できればよいことを意味する．

例題 11. 関係 $\sim$ を

$$\sigma \sim \tau \iff \sigma\tau^{-1} \in C(e)$$

とすると，$\sim$ は同値関係となることを示せ．

（解答）　(1) $\sigma\sigma^{-1} = e \in C(e)$ より $\sigma \sim \sigma$ である．(2) 次に $\sigma \sim \tau$ を仮定したとき $\tau \sim \sigma$ を，すなわち $\tau\sigma^{-1} \in C(e)$ が成り立つことを示す．$\sigma\tau^{-1} = \xi$ と置くと，仮定より $\xi \in C(e)$ であり，さらに，$\sigma = \xi\tau$, $\xi^{-1} \in C(e)$ である．よって，

$$\tau\sigma^{-1} = \tau(\xi\tau)^{-1} = \tau(\tau^{-1}\xi^{-1}) = (\tau\tau^{-1})\xi^{-1} = \xi^{-1} \in C(e)$$

となる．(3) 最後に $\sigma \sim \tau$ かつ $\tau \sim \eta$ を仮定したとき $\sigma \sim \eta$ を，すなわち $\sigma\eta^{-1} \in C(e)$ が成り立つことを示す．仮定より $\sigma\tau^{-1} \in C(e)$，$\tau\eta^{-1} \in C(e)$ である．これより

$$\sigma\eta^{-1} = \sigma(\tau^{-1}\tau)(\eta^{-1}\eta)\eta^{-1} = (\sigma\tau^{-1})(\tau\eta^{-1})(\eta\eta^{-1}) = (\sigma\tau^{-1})(\tau\eta^{-1}) \in C(e)$$

となる．(1),(2),(3) により $\sim$ は同値関係である．□

$C(e)=\{e, (1\ 2\ 3), (1\ 3\ 2)\}$は，$S_3$の特別な部分群

つまり，　$\sigma\in S_3$，　$\sigma C(e)=C(e)\sigma$

そして，$\sigma\sim\tau$　$\Leftrightarrow$　$\sigma\tau^{-1}\in C(e)$

S_3 には $C(e)$ を用いて同値関係 $\sim$ が定義された．そして，

$$(1\ 2)(1\ 3)^{-1} = (1\ 2)(1\ 3) = (1\ 3\ 2) \in C(e)$$
$$(1\ 2)(2\ 3)^{-1} = (1\ 2)(2\ 3) = (1\ 2\ 3) \in C(e)$$

なので，

$$(1\ 2) \sim (1\ 3),\quad (1\ 2) \sim (2\ 3)$$

となり，S_3 は以下のようなクラスに分解される．

$$S_3 = C(e) \oplus C((1\ 2))$$

ここで，

$$C(e) = \{e,\ (1\ 2\ 3),\ (1\ 3\ 2)\},\quad C((1\ 2)) = \{(1\ 2),\ (1\ 3),\ (2\ 3)\}$$

である．

それぞれのクラスの元の個数が同じであることは明らかであるが，一応注意しておく．

以上により，商集合

$$S_3/C(e) = \{C(e),\ C((1\ 2))\}$$

が構成できたのである．

$\sharp S_3/C(e) = 2$ であることは明らかであるが，これについても一応注意しておく．

さて，S_3 内の演算を利用して，商集合 $S_3/C(e)$ 内の演算の定義を

$$C(\sigma)C(\tau) = C(\sigma\tau)$$

として，$S_3/C(e)$ を群にしたい．

問題は，この定義が well-defined であるか，つまり，これを定義をすることは可能で，しかも，代表元の選び方で演算結果が変わらないように定義されているかである．

例題 12. 商集合 $S_3/C(e)$ 内の演算 $C(\sigma)C(\tau) = C(\sigma\tau)$ の定義は，*well-defined* であることを示せ．

（**解答**）まず, $C(\sigma)C(\tau) = C(\sigma\tau)$ が定義可能であることを示す．$C(\sigma) = \sigma C(e) = C(e)\sigma$, $C(\tau) = \tau C(e) = C(e)\tau$, そして $C(e)C(e) = C(e)$ であることに注意すると，

$$\begin{aligned} C(\sigma)C(\tau) &= \{\sigma C(e)\}\{\tau C(e)\} = \sigma\{C(e)\tau\}C(e) \\ &= \sigma\{\tau C(e)\}C(e) = (\sigma\tau)C(e) \\ &= C(\sigma\tau) \end{aligned}$$

となり，$C(\sigma)C(\tau) = C(\sigma\tau)$ は定義可能である．

次に，代表元の選び方で計算結果は変化しないかをチェックする．そのために，σ', τ' を $C(\sigma), C(\tau)$ の別の代表元として，それぞれ選び直す．すなわち，$C(\sigma') = C(\sigma)$，$C(\tau') = C(\tau)$ とする．これより

$$C(\sigma'\tau') = C(\sigma')C(\tau') = C(\sigma)C(\tau) = C(\sigma\tau)$$

である．これは代表元の選び方で計算結果が変化しないことを示している．

以上により，商集合 $S_3/C(e)$ 内の演算 $C(\sigma)C(\tau) = C(\sigma\tau)$ は，well-defined である．□

以上のことを，n 次対称群 S_n について，一般的にまとめる．

まず，S_n の任意の置換 σ に対して

$$\sigma C(e) = C(e)\sigma \tag{6.4}$$

を満たす S_n の部分群 $C(e)$ を考える．

この特別な部分群 $C(e)$ は，**正規部分群**と呼ばれる．

正規部分群 $C(e)$ が見つかれば，S_n は $C(e)$ を用いて，

$$\sigma \sim \tau \iff \sigma\tau^{-1} \in C(e)$$

という同値関係 $\sim$ を定義することができ，これによって S_n は

$$S_n = C(e) \oplus \sigma_1 C(e) \oplus \sigma_2 C(e) \oplus \cdots \oplus \sigma_r C(e)$$

とクラス分けされる．

さらに，

$$C(\sigma_1) = \sigma_1 C(e),\ C(\sigma_2) = \sigma_2 C(e),\ \cdots,\ C(\sigma_r) = \sigma_r C(e)$$

とそれぞれ置くことで，商集合

$$S_n/C(e) = \{C(e),\ C(\sigma_1),\ C(\sigma_2),\ \cdots, C(\sigma_r)\}$$

が構成できる．

そして，商集合 $S_n/C(e)$ 内の演算の定義を，

$$C(\sigma)C(\tau) = C(\sigma\tau)$$

とすることができる．

商群 $S_n/C(e)$ こそが，ガロア理論で重要となる群である．

商群 $S_n/C(e)$ の在り方が，S_n に関係する n 次方程式の特徴を表す．

この意味が徐々に鮮明になっていく．

Momorize：正規部分群 $C(e)$，商群 $S_n/C(e)$

・n 次対称群 S_n の正規部分群 $C(e)$ は，$\sigma C(e) = C(e)\sigma$ を満たす部分群
・S_n と正規部分群 $C(e)$ によって，商群 $S_n/C(e)$ が構成できる．
・$S_n/C(e)$ 内の演算は，$C(\sigma)C(\tau) = C(\sigma\tau)$：well defined

次の問題に答えることができますか？

問題 8. 4 次対称群 S_4 の位数 4 の正規部分群を H_4 とする．以下の問いに答えよ．

（1）S_4 の H_4 によるクラス分けの方法を説明し，クラスの個数を求めよ．

（2）商集合 S_4/H_4 が商群となるための演算を定義し，*well-defined* であることを証明せよ．

第 7 章

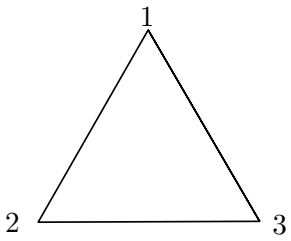
正三角形と商群 $S_3/C(e)$

ガロア理論では，なぜ商群 $S_n/C(e)$ を重視するのか？　現段階で説明できる回答を，

$$S_3/C(e) = \{C(e),\ C((1\ 2))\}$$

を用いて説明しよう．ここで, $S_3 = \{e,\ (1\,2),\ (1\,3),\ (2\,3),\ (1\,2\,3),\ (1\,3\,2)\}$ で，$C(e) = \{e,\ (1\ 2\ 3),\ (1\ 3\ 2)\}$，$C((1\ 2)) = \{(1\ 2),\ (1\ 3),\ (2\ 3)\}$ である．

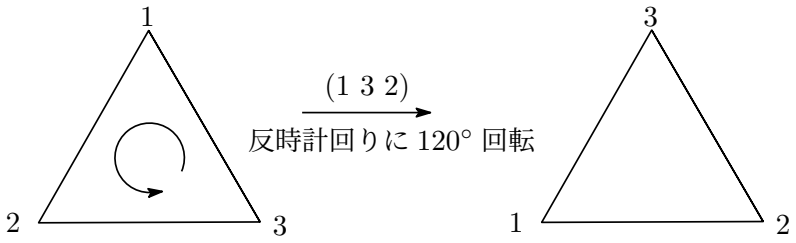
頂点を $1, 2, 3$ とする正三角形 123 を考える．



正三角形 123 に 3 次対称群 S_3 を**作用させる**とは，正三角形 123 の頂点の番号を S_3 の置換によって入れ換えることとである．

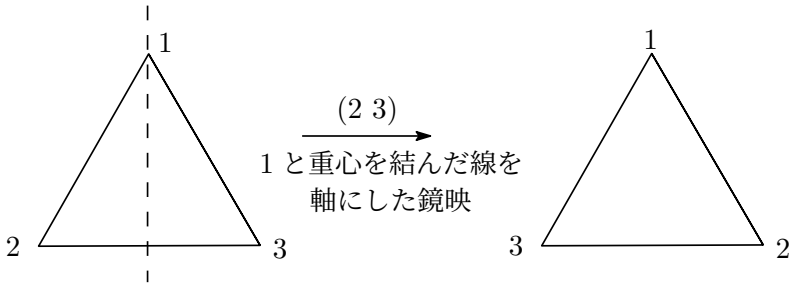
例題 13. 正三角形 123 に作用する置換 (1 2 3), (1 3 2) は，回転という作用の集合であり，置換 (1 2), (1 3), (2 3) は，鏡映という作用の集合であることを示せ.

（**解答**） たとえば，置換 (1 3 2) は，以下のように正三角形 123 の重心を中心として，反時計回りに 120° 回転することを意味する.



同様して (1 3 2) は正三角形 123 の重心を中心として，時計回りに 120° 回転することを意味する.

たとえば，置換 (2 3) は，以下のように正三角形 123 の頂点 1 と重心を結んだ線を軸にした鏡映を意味する.



同様にして，置換 (1 2) は，正三角形 123 の頂点 3 と重心を結んだ線を軸にした鏡映を意味し，置換 (1 3) は，正三角形 123 の頂点 2 と重心を結んだ線を軸にした鏡映を意味する．□

では，改めて S_3 と $C(e)$ と $C((1\ 2))$ を整理すると，

$$S_3 = \{C(e),\ ((1\ 2),\ (1\ 3),\ (2\ 3),\ (1\ 2\ 3),\ (1\ 3\ 2)\}$$

$$C(e) = \{e,\ (1\ 2\ 3),\ (1\ 3\ 2)\ \}$$

$$C((1\ 2)) = \{\ ((1\ 2),\ (1\ 3),\ (2\ 3)\}$$

となる．

例題 13 から，

$C(e)$ は回転に関する置換の集合，

$C((1\ 2))$ は鏡映に関する置換の集合

であることがわかる．

そして，この観点から商群 $S_3/C(e)$，すなわち

$$S_3/C(e) = \{C(e),\ C((1\ 2))\}$$

をみると，これは回転と鏡映という集合を要素にもつ群であるということがいえる．

すなわち，商群 $S_3/C(e)$ は，正三角形 123 に作用する S_3 の中の本質的な要素だけを取り出した群であるといえる．

Memorize：商群 $S_3/C(e)$ の幾何学的な意味

商群 $S_3/C(e) = \{C(e),\ C((1\ 2))\}$ は，正三角形 123 に作用する回転 $C(e)$ と鏡映 $C((1\ 2))$ という集合を要素にもつ群である．

次の問題に答えることができますか？

問題 9. $1, 2, 3, 4$ を頂点とする正方形 1234 に作用する置換からなる群 D_4 を考える．

1. D_4 の中の回転を表す置換を全て求めよ．

2. D_4 の中の鏡映を表す置換を全て求めよ．

3. D_4 の中の回転を表す置換と恒等置換 e からなる集合 $C(e)$ は D_4 の正規部分群，すなわち，任意の $\sigma \in D_4$ に対して $\sigma C(e) = C(e)\sigma$ を満たすことを示せ．

4. 商群 $D_4/C(e)$ はどのような要素をもつ群か述べよ．

第 8 章

四則演算が可能な集合“体”

体とは，四則演算が可能な集合のことである．

このため，整数全体の集合 $\mathbb{Z}$ は体ではない．なぜなら，$\mathbb{Z}$ の数 2 に対して，割り算 $1 \div 2 =$ から得られる分数 $\frac{1}{2}$ は $\mathbb{Z}$ の数ではないからである．すなわち，$\mathbb{Z}$ には割り算が定義されていないのである．

$\mathbb{Z}$ にすべての分数を含めた集合は体となる．この集合に含まれる整数と分数のことをまとめて**有理数**と呼び，有理数全体を $\mathbb{Q}$ で表す．$\mathbb{Q}$ は**有理数体**と呼ばれる．有理数とは 2 つの整数の比で表される数という意味である．

ガロア理論で重視する体は，$\mathbb{Q}$ に含まれないある数を $\mathbb{Q}$ **に添加した体**である．そして，この種の体が理解できた後，目的とする方程式の群にたどりつく．

それでは，$\mathbb{Q}$ に添加した体の説明に入ろう．

たとえば方程式 $x^2 = 2$ の解である $\sqrt{2}$ は，2 つの整数の比で表すことができないため $\mathbb{Q}$ には含まれない．$\sqrt{2}$ は**無理数**と呼ばれる数である．

$\mathbb{Q}$ に $\sqrt{2}$ を添加した体を $\mathbb{Q}(\sqrt{2})$ と書く．その定義は

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

である．

ここで，

$$a + b\sqrt{2} = a \cdot \mathbf{1} + b \cdot \sqrt{\mathbf{2}}$$

と考えると，1 と $\sqrt{2}$ は $\mathbb{Q}(\sqrt{2})$ の任意の数を作るための必要最低な元であることがわかる．

そこで，数 1 と $\sqrt{2}$ を，$\mathbb{Q}(\sqrt{2})$ の $\mathbb{Q}$ 上の**生成元**，あるいは，$\mathbb{Q}(\sqrt{2})$ は $\mathbb{Q}$ 上 1 と $\sqrt{2}$ から**生成されている**という．

以下，生成元が明確に分かるようにするために，

$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}\langle 1,\ \sqrt{2}\rangle$$

と書くことにする．

生成元をもう少し詳しく説明しよう．

$\mathbb{Q}\langle 1,\ \sqrt{2}\rangle$ の生成元である $\sqrt{2}$ は，その 2 乗を考えると $(\sqrt{2})^2 = 4$ となり，これは $\mathbb{Q}$ の数なので，1 の有理数倍の数である．

さらに，$(\sqrt{2})^3 = 2\sqrt{2}$ は $\sqrt{2}$ の有理数倍の数である．

これを繰り返しても，$(\sqrt{2})^n$ は 1 か $\sqrt{2}$ の有理数倍のどちらかの数である．

したがって，1 と $\sqrt{2}$ は $\mathbb{Q}(\sqrt{2})$ の任意の数を作るための必要最低な元である．

さて，$\mathbb{Q}(\sqrt{2})$ の 2 つの数 $a+b\sqrt{2}$ と $c+d\sqrt{2}$ に対して，足し算，引き算，掛け算は

$$(a+b\sqrt{2})+(c+d\sqrt{2})=(a+c)+(b+d)\sqrt{2}$$
$$(a+b\sqrt{2})-(c+d\sqrt{2})=(a-c)+(b-d)\sqrt{2}$$
$$(a+b\sqrt{2})(c+d\sqrt{2})=(ac+2bd)+(ad+bc)\sqrt{2}$$

となるため，$\mathbb{Q}(\sqrt{2})$ には，足し算，引き算，掛け算が定義されていることが確かめられる．

問題は割り算である．

例題 14. $\mathbb{Q}(\sqrt{2})$ には割り算が定義されていることを確かめよ．

（**解答**）　$1/(a+b\sqrt{2})$ が $\mathbb{Q}(\sqrt{2})$ の数であることを確かめればよい．

$$\frac{1}{a+b\sqrt{2}}=\frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})}=\frac{a-b\sqrt{2}}{a^2-2b^2}$$
$$=\left(\frac{a}{a^2-2b^2}\right)+\left(\frac{-b}{a^2-2b^2}\right)\sqrt{2}$$

であるので，$1/(a+b\sqrt{2})$ は $\mathbb{Q}(\sqrt{2})$ の数である．□

$\sqrt[3]{2}$ は $x^3=2$ 満たす数のことであった．これを使った $\mathbb{Q}$ に $\sqrt[3]{2}$ を添加した体は $\mathbb{Q}(\sqrt[3]{2})$ と書かれる．

ここでは証明はしないが，この体は，1 と $\sqrt[3]{2}$ に加えて，$\left(\sqrt[3]{2}\right)^2=\sqrt[3]{4}$ を含めた 3 つの数が $\mathbb{Q}(\sqrt[3]{2})$ の $\mathbb{Q}$ 上の生成元である．

つまり

$$\mathbb{Q}(\sqrt[3]{2})=\mathbb{Q}\langle 1,\ \sqrt[3]{2},\ \sqrt[3]{4}\rangle$$

である．

実は，次の定理が知られている．

定理（$\mathbb{Q}(\sqrt[n]{u})$ の生成元）　$u \in \mathbb{Q}$ とすると，$\mathbb{Q}(\sqrt[n]{u})$ は体であり，$x = \sqrt[n]{u}$ とすると，

$$\mathbb{Q}(\sqrt[n]{u}) = \mathbb{Q}\langle 1,\ x,\ \cdots, x^{n-1}\rangle$$

である．さらに，$K = \mathbb{Q}(\sqrt[n]{u})$，$v \in \mathbb{Q}$ とすると $K(\sqrt[r]{v})$ は体であり，そして $y = \sqrt[r]{v}$ とすると，

$$K(\sqrt[r]{v}) = K\langle 1,\ y,\ \cdots, y^{r-1}\rangle$$

である．

さて，$\mathbb{Q}$ にすべての無理数を含めた集合も体である．

この集合に含まれる有理数と無理数のことをまとめて**実数**と呼び，実数全体を $\mathbb{R}$ で表し，$\mathbb{R}$ は**実数体**と呼ばれる．

さらに，$x^2 = -1$ の解として $\sqrt{-1}$ という空想的な数を考える．

$\sqrt{-1}$ は i で表し，**虚数単位**と呼ばれる．

そして，a を 0 でない実数とした数 ai は**虚数**と呼ばれる．

さらに，$\mathbb{R}$ に i を添加した体

$$\mathbb{C} = \mathbb{R}(i) = \mathbb{R}\langle 1,\ i\rangle$$

は，**複素数体**と呼ばれ，$\mathbb{C}$ の数を**複素数**と呼ぶ．

どうして，虚数や複素数のような空想的な数を考える必要があるのか？

実は，方程式に関して次の重要な定理がある．これをはじめて証明した人は，１９世紀のドイツの数学者ガウス (1777 年-1885 年) である．

代数学の基本定理　$a_1, a_2, \cdots a_n$ を複素数とする．このとき n 次方程式

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1} x + a_n = 0$$

の解は重複も込めて丁度 n 個あり，それらはすべて複素数である．

代数学の基本定理より，有理数を係数とする n 次方程式の解も n 個あり，それらはすべて複素数であることは明らかであろう．

しかし，それらの解が，$\sqrt{\ }$，$\sqrt[3]{\ }$，$\cdots$ を組み合わせて表現できるかどうかまではわからない．

方程式の解の細かな構造を知るためには，複素数体 $\mathbb{C}$ は解たちをすくうための網の目が大きすぎるのである．

ガロア理論では，有理数を係数とした n 次方程式を考えるときは，有理数体 $\mathbb{Q}$ に有理数以外の数を添加した体を考えるのである．

その体は，解たちをすくうための最適な目の網を提供するのである．

Memorize：$\mathbb{Q}$ に α を添加した体 $\mathbb{Q}(\alpha)$

$\mathbb{Q}$：有理数体，$\mathbb{R}$：実数体
$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}\langle 1,\ \sqrt{2}\rangle = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ ：$\mathbb{Q}$ に $\sqrt{2}$ を添加した体
$\mathbb{C} = \mathbb{R}(i) = \mathbb{R}\langle 1,\ i\rangle = \{\alpha + \beta i \mid \alpha, \beta \in \mathbb{R}\}$ ：複素数体（$\mathbb{R}$ に i を添加した体）

次の問題に答えることができますか？

問題 10. $\mathbb{R}$ に $i = \sqrt{-1}$ を添加した体，すなわち複素数体

$$\mathbb{C} = \mathbb{R}(i) = \{\alpha + \beta i \mid \alpha, \beta \in \mathbb{R}\}$$

の 2 つの数 $a + bi$ と $c + di$ に対して，足し算，引き算，掛け算，割り算の各計算結果が $\mathbb{R}(i)$ の元となることを確かめよ．ただし，割り算に関しては，$1/(a + bi)$ が $\mathbb{R}(i)$ の元であることを確かめるだけでよい．（ヒント：$(a + bi)(a - bi) = a^2 + b^2$ であることを使う．）

第 9 章

体の拡大と拡大率

ガロア理論は，群と体の理論と呼ばれる．
その理由は，体の生成元をもとに群をつくって，その群が方程式の解の判定に使われるからである．したがって，考えている体の生成元の個数を理解することは重要となる．そして，その個数は体の拡大次数というものに関係する．以下で，このことを理解していく．

$\mathbb{Q}$ に $\sqrt{2}$ を添加した体 $\mathbb{Q}(\sqrt{2})$ は

$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}\langle 1,\ \sqrt{2}\rangle$$

であり，$\mathbb{Q}$ 上の生成元は 1 と $\sqrt{2}$ である．

そして，$\mathbb{Q}$ は $\mathbb{Q}(\sqrt{2})$ の部分集合であることから，$\mathbb{Q}(\sqrt{2})$ は $\mathbb{Q}$ の**拡大体**という．

さらに，$\mathbb{Q}$ 上の生成元が 1 と $\sqrt{2}$ の 2 個であることから，$\mathbb{Q}(\sqrt{2})$ の $\mathbb{Q}$ 上の**拡大次数**は 2 であるとし，

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$$

と書く．このことから，$\mathbb{Q}(\sqrt{2})$ は $\mathbb{Q}$ の 2 **次拡大体**であるということもある．

$\mathbb{Q}$ に $\sqrt[3]{2}$ を添加した体 $\mathbb{Q}(\sqrt[3]{2})$ は

$$\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}\langle 1,\ \sqrt[3]{2},\ \sqrt[3]{4}\rangle$$

であり，$\mathbb{Q}$ 上の生成元は $1,\ \sqrt[3]{2}, \sqrt[3]{4}$ である．このことから，$\mathbb{Q}(\sqrt[3]{2})$ の $\mathbb{Q}$ 上の拡大次数は 3 となる．よって，$\mathbb{Q}(\sqrt[3]{2})$ は $\mathbb{Q}$ の 3 次拡大体となる．

ところで，α が $\mathbb{Q}$ の数でないとき，$\mathbb{Q}(\alpha)$ を $\mathbb{Q}$ の**単拡大**という．

また，α がある $\mathbb{Q}$ 係数の方程式 $x^n + c_1x^{n-1} + \cdots c_{n-1}x + c_n = 0$ の解であるとき，
α を $\mathbb{Q}$ **上代数的数である**という．

以下のことが知られている．

定理（代数的数の単拡大）　K を体，α を K 上代数的数であるとする．このとき

$$K(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_0, \cdots, a_{n-1} \in K\}$$

は体である．

定理（代数的数の単拡大）において $K(\alpha)$ は体であるので，$x \in K(\alpha)$ は，$x \neq 0$ ならば $\dfrac{1}{x} \in K(\alpha)$ となることが言えることに注意しよう．

さて，体 $\mathbb{Q}(\sqrt{2})$ を K と表して，K に $\sqrt{3}$ を添加した体 $K(\sqrt{3})$（K の単拡大）を考えよう．

明らかに生成元が 1 と $\sqrt{3}$ であることから

$$K(\sqrt{3}) = K\langle 1,\ \sqrt{3}\rangle = \{\alpha + \beta\sqrt{3} \mid \alpha, \beta \in K\}$$

である．そこで，$K(\sqrt{3})$ を $\mathbb{Q}$ の拡大体として考えよう．これを，

$$\mathbb{Q}(\sqrt{2},\sqrt{3})$$

と書ことにする．

α,β は $K=\mathbb{Q}(\sqrt{2})$ の数なので，a,b,c,d を $\mathbb{Q}$ の数，すなわち有理数として

$$\alpha=a+b\sqrt{2},\quad \beta=c+d\sqrt{2}$$

と書くと，

$$\beta\sqrt{3}=(c+d\sqrt{2})\sqrt{3}=c\sqrt{3}+d\sqrt{6}$$

であることから

$$\begin{aligned}\mathbb{Q}(\sqrt{2},\sqrt{3}) &= \mathbb{Q}\langle 1,\ \sqrt{2},\ \sqrt{3},\ \sqrt{6}\rangle \\ &= \{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\mid a,b,c,d\in\mathbb{Q}\}\end{aligned}$$

となる．

同様にして，$\mathbb{Q}(\sqrt{3})$ を F として，F に $\sqrt{2}$ を添加した体 $F(\sqrt{2})$（F の単拡大）は，生成元が 1 と $\sqrt{2}$ であることから

$$F(\sqrt{2})=\{\alpha+\beta\sqrt{2}\mid \alpha,\beta\in F\}$$

となる．

そして $F(\sqrt{2})$ を $\mathbb{Q}$ の拡大体とみて $\mathbb{Q}(\sqrt{3},\sqrt{2})$ と書くと，

$$\mathbb{Q}(\sqrt{3},\sqrt{2})=\mathbb{Q}(\sqrt{2},\sqrt{3})$$

であることがわかる．

$\mathbb{Q}(\sqrt{2},\sqrt{3})$ を $\mathbb{Q}$ に $\sqrt{2}$ と $\sqrt{3}$ を添加した体という．

例題 15. $\mathbb{Q}$ に $\sqrt{2}$ と $\sqrt{3}$ を添加した体

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$$

は $\mathbb{Q}$ の単拡大であることを示せ．さらに，$\mathbb{Q}(\sqrt{2},\sqrt{3})$ の $\mathbf{Q}(\sqrt{2})$ 上の拡大次数と，$\mathbb{Q}(\sqrt{2},\sqrt{3})$ の $\mathbf{Q}(\sqrt{3})$ 上の拡大次数と，$\mathbb{Q}(\sqrt{2},\sqrt{3})$ の $\mathbf{Q}$ 上の拡大次数をそれぞれ求めよ．

（**解答**）　まず，$\mathbb{Q}(\sqrt{2}+\sqrt{3})$ の生成元について考える．$\alpha = \sqrt{2}+\sqrt{3}$ と置くと，$\alpha^2 = 5 + 2\sqrt{6}$ であり，これより $(\alpha^2-5)^2 = 24$，すなわち，$\alpha^4 - 10\alpha^2 + 1 = 0$ を得る．これは $\alpha^4 = 10\alpha^2 - 1$ であることを意味する．さらに，$\alpha^5 = 10\alpha^3 - \alpha$，$\alpha^6 = 10\alpha^4 - \alpha^2 = 99\alpha^2 - 10$, $\alpha^7 = 99\alpha^3 - 10\alpha$, $\cdots$ となるので，$\mathbb{Q}(\sqrt{2}+\sqrt{3})$ の生成元は $1,\ \alpha,\ \alpha^2,\ \alpha^3$ である．よって，

$$\mathbb{Q}(\alpha) = \{a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 \mid a_0, a_1, a_2, a_3 \in \mathbb{Q}\}$$

となる．

$\mathbb{Q}(\sqrt{2},\sqrt{3})$ が $\mathbb{Q}$ の単拡大であること，すなわち $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ であることを示す．

$\mathbb{Q}(\sqrt{2},\sqrt{3}) \supset \mathbb{Q}(\sqrt{2}+\sqrt{3})$ を示すには，生成元である $\sqrt{2}+\sqrt{3}$，$(\sqrt{2}+\sqrt{3})^2 = 5+2\sqrt{6}$ と $(\sqrt{2}+\sqrt{3})^3 = 11\sqrt{2}+9\sqrt{3}$ がそれぞれ $\mathbb{Q}(\sqrt{2},\sqrt{3})$ の元であることをいえばよいが，これは明らかである．

$\mathbb{Q}(\sqrt{2},\sqrt{3}) \subset \mathbb{Q}(\sqrt{2}+\sqrt{3})$ を示す．そのためにには，生成元である $\sqrt{2}$ と $\sqrt{3}$ と $\sqrt{6}$ がそれぞれ $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ の元であることを示せばよい．$\alpha = \sqrt{2}+\sqrt{3}$ と置く．$\alpha^2 = 5+2\sqrt{6}$ より，

$$\sqrt{6} = \frac{\alpha^2 - 5}{2} \in \mathbb{Q}(\alpha)$$

である．また，$(\alpha - \sqrt{2})^2 = 3$ より $\alpha^2 - 1 = 2\sqrt{2}\alpha$ であり，$\mathbb{Q}(\alpha)$ は体なので，

$$\sqrt{2} = \frac{\alpha^2 - 1}{2\alpha} \in \mathbb{Q}(\alpha)$$

である．$\sqrt{6}, \sqrt{2} \in \mathbb{Q}(\alpha)$ より，

$$\sqrt{3} = \frac{\sqrt{6}}{\sqrt{2}} \in \mathbb{Q}(\alpha)$$

となる．ゆえに，$\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subset \mathbb{Q}(\sqrt{2} + \sqrt{3})$ である．したがって，$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ より $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ は $\mathbb{Q}$ の単拡大である．

次に，$\mathbb{Q}(\sqrt{2}, \sqrt{3})$ の $\mathbf{Q}$ 上の拡大次数を求める．拡大次数については，$\mathbb{Q}(\sqrt{2}, \sqrt{3})$ の $\mathbf{Q}(\sqrt{2})$ 上の拡大次数は生成元が 1 と $\sqrt{3}$ であることから 2 であり，同様に，$\mathbb{Q}(\sqrt{2}, \sqrt{3})$ の $\mathbf{Q}(\sqrt{3})$ 上の拡大次数は生成元が 1 と $\sqrt{2}$ であることから 2 である．そして，$\mathbb{Q}(\sqrt{2}, \sqrt{3})$ の $\mathbf{Q}$ 上の拡大次数は，生成元が $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ であることから 4 である．□

$\mathbb{Q}(\alpha, \beta)$ の拡大次数に関しては，以下の定理が知られている．

定理（$\mathbb{Q}(\alpha, \beta)$ の拡大次数）　α と β が $\mathbb{Q}$ の数でなく $\alpha \neq \beta$ のとき，拡大次数 $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$ に関して，次の掛け算

$$\begin{aligned}[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] &= [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] \\ &= [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}]\end{aligned}$$

が成り立つ．

Memorize：$\mathbb{Q}(\alpha)$ 上の $\mathbb{Q}$ 上の拡大次数

・$[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2,\quad [\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3,\quad [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=4$
・$\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}\langle 1,\ \sqrt{2},\ \sqrt{3},\ \sqrt{6}\rangle$

次の問題に答えることができますか？

問題 11. 体 $\mathbb{Q}(\sqrt[3]{2},\sqrt{3})$ について以下を求めよ.

(1) $\mathbb{Q}(\sqrt[3]{2},\sqrt{3})=\mathbb{Q}(\sqrt[3]{2}+\sqrt{3})$ を示せ.

(2) $[\mathbb{Q}(\sqrt[3]{2},\sqrt{3}):\mathbb{Q}(\sqrt[3]{2})]$ を求めよ.

(3) $[\mathbb{Q}(\sqrt[3]{2},\sqrt{3}):\mathbb{Q}(\sqrt{3})]$ を求めよ.

(4) $[\mathbb{Q}(\sqrt[3]{2},\sqrt{3}):\mathbb{Q})]$ を求めよ.

第 10 章

拡大体の最小多項式

体の拡大次数を決めるものは生成元の個数であったが，実は，$\mathbb{Q}$ の単拡大 $\mathbb{Q}(\alpha)$ において，$x = \alpha$ として 0 となる次数が最小な多項式が，拡大次数に関係する．したがって，次数が最小な多項式は，方程式の解がどういった拡大体の中に存在するのかを理解する手掛かりとなる．

たとえば，$\mathbb{Q}$ に $\sqrt{2}$ を添加した体 $\mathbb{Q}(\sqrt{2})$ の生成元である $\sqrt{2}$ を代入して 0 となる $\mathbb{Q}$ 係数の多項式の中で，

次数が最小でかつ最高次数の係数が 1 である**既約多項式**を考えよう．

ここで，既約多項式とは $\mathbb{Q}$ 係数の多項式を使って $\mathbb{Q}$ 上で因数分解できない多項式のことである．

答えは簡単で

$$x^2 - 2$$

である．この多項式を $\sqrt{2}$ の $\mathbb{Q}$ 上の**最小多項式**という．

すでに気づいていると思うが,

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$$

であったので，生成元である $\sqrt{2}$ の $\mathbb{Q}$ 上の最小多項式の次数は，$\mathbb{Q}(\sqrt{2})$ の $\mathbb{Q}$ 上の拡大次数に一致する.

次に，$\mathbb{Q}$ に $\sqrt[3]{2}$ を添加した体 $\mathbb{Q}(\sqrt[3]{2})$ について考えよう.

$\mathbb{Q}(\sqrt[3]{2})$ の生成元である $\sqrt[3]{2}$ の $\mathbb{Q}$ 上の最小多項式は，明らかに

$$x^3 - 2$$

である.

さらに，もう一つの生成元である $\sqrt[3]{4}$ の $\mathbb{Q}$ 上の最小多項式について考えると，明らかに

$$x^3 - 4$$

であることがわかる.

すなわち，$\sqrt[3]{2}$ の $\mathbb{Q}$ 上の最小多項式も $\sqrt[3]{4}$ の $\mathbb{Q}$ 上の最小多項式もどちらも次数は 3 である.

そしてこれは，生成元が $1, \sqrt[3]{2}, \sqrt[3]{4}$ である $\mathbb{Q}(\sqrt[3]{2})$ の $\mathbb{Q}$ 上の拡大次数 3 に一致する.

例題 16. $\mathbb{Q}$ の単拡大 $\mathbb{Q}(\sqrt[4]{3})$ について，以下を求めよ.

(1) $\mathbb{Q}(\sqrt[4]{3})$ の生成元を求め，集合 $\mathbb{Q}(\sqrt[4]{3})$ を生成元を用いて表せ.

(2) $\mathbb{Q}(\sqrt[4]{3})$ の $\mathbb{Q}$ 上の拡大次数を求めよ.

(3) $\mathbb{Q}(\sqrt[4]{3})$ の 1 以外の各生成元の $\mathbb{Q}$ 上の最小多項式を求めよ.

（解答）　(1)　$\mathbb{Q}(\sqrt[4]{3})$ の生成元は $1,\ \sqrt[4]{3},\ \sqrt[4]{9},\ \sqrt[4]{27}$ であるので，

$$\mathbb{Q}(\sqrt[4]{3}) = \mathbb{Q}\langle 1,\ \sqrt[4]{3},\ \sqrt[4]{9},\ \sqrt[4]{27}\rangle$$

である．

(2)　(1) より $\mathbb{Q}(\sqrt[4]{3})$ の $\mathbb{Q}$ 上の拡大次数は 4 である．

(3)　$\sqrt[4]{3}$ の $\mathbb{Q}$ 上の最小多項式は x^4-3，$\sqrt[4]{9}$ の $\mathbb{Q}$ 上の最小多項式は x^4-9，$\sqrt[4]{27}$ の $\mathbb{Q}$ 上の最小多項式は x^4-27 である．□

以下の定理が証明されている．

定理（単拡大の拡大次数）　K を $\mathbb{Q}$ の拡大体とする．このとき，$K(\alpha)$ の K 上の拡大次数は，α の K 上の最小多項式の次数に一致する．したがって，$K=\mathbb{Q}(\alpha)$，$L=K(\beta)$ とし，さらに，α の $\mathbb{Q}$ 上の最小多項式の次数を m，β の K 上の最小多項式の次数を n とすると，$[L:\mathbb{Q}]=mn$ が成り立つ．

例題 17. $\mathbb{Q}$ の単拡大 $\mathbb{Q}(\sqrt{3}+\sqrt{5})$ について，以下を求めよ．

(1)　$\sqrt{3}$ の $\mathbb{Q}$ 上の最小多項式の次数を求めよ．

(2)　$K=\mathbb{Q}(\sqrt{3})$ と置く．$\sqrt{5}$ の K 上の最小多項式の次数を求めよ．

(3)　$\sqrt{3}+\sqrt{5}$ の $\mathbb{Q}$ 上の最小多項式の次数を求めよ．

（解答）　(1)　$\sqrt{3}$ の $\mathbb{Q}$ 上の最小多項式は x^2-3 より，次数は 2 である．

(2)　$\sqrt{5}$ の K 上の最小多項式は x^2-5 より，次数は 2 である．

(3)　$K=\mathbb{Q}(\sqrt{3})$ と置くと，$\sqrt{3}+\sqrt{5}\in K(\sqrt{5})=\{a+b\sqrt{5}\mid a,b\in K\}$ であるので，$\sqrt{3}+\sqrt{5}$ の $\mathbb{Q}$ 上の最小多項式の次数は，(1) と (2) と定理（単拡大の拡大次数）より $2\times 2=4$ である．□

Memorize：α の $\mathbb{Q}$ 上の最小多項式

・$\sqrt{2}$ の $\mathbb{Q}$ 上の最小多項式は x^2-2 で，$[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$
・$\sqrt[3]{2}$ の $\mathbb{Q}$ 上の最小多項式は x^3-2 で，$[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$
・$\sqrt[4]{2}$ の $\mathbb{Q}$ 上の最小多項式は x^4-2 で，$[\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}]=4$
・$\sqrt{3}+\sqrt{5}$ の $\mathbb{Q}$ 上の最小多項式の次数は $2\times 2=4$ で，$[\mathbb{Q}(\sqrt{3}+\sqrt{5}):\mathbb{Q}]=4$

次の問題に答えることができますか？

問題 12. $\sqrt[3]{2}+\sqrt{3}$ の $\mathbb{Q}$ 上の最小多項式の次数を求め，$[\mathbb{Q}(\sqrt[3]{2}+\sqrt{3}):\mathbb{Q}]$ を求めよ．

第 11 章

最小分解体とガロア群

$\mathbb{Q}$ 係数の n 次方程式

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots a_{n-1} x + a_n = 0$$

を考える．このとき，解 $x_1,\ x_2, \cdots, x_n$ を含んだ $\mathbb{Q}$ の拡大体の中で，拡大次数が最小であるものを n 次式方程式の**最小分解体**という．

それでは，“n 次方程式のガロア群”（あるいは“n 次方程式の群”ともいう）について説明しよう．頂上までもう少しである．

“n 次方程式のガロア群”は，その方程式の解による基本対称式の考え方がもとになっている．

$\mathbb{Q}$ 係数の 2 次方程式

$$x^2 - 2 = 0$$

を考える．この解を x_1, x_2 とすると，これらは

$$x_1 = \sqrt{2}, \quad x_2 = -\sqrt{2}$$

である．

そして，この方程式の最小分解体は $\mathbb{Q}(\sqrt{2}, -\sqrt{2})$，つまり $\mathbb{Q}(\sqrt{2})$ である．

一方，解 x_1, x_2 による基本対称式は

$$x_1 + x_2 = 0, \quad x_1 x_2 = -2 \tag{11.1}$$

である．

そこで，2 次対称群 $S_2 = \{e,\ (1\ 2)\}$ を，基本対称式 (11.1) にそれぞれ作用させる．

明らかに，

$$e : (x_1, x_2) \to (x_1, x_2), \quad (1\ 2) : (x_1, x_2) \to (x_2, x_1)$$

であり，(11.1) の 2 つの基本対象式は，どちらも変化しない．

しかし，この考え方から，方程式 $x - 2 = 0$ の“ガロア群”を S_2 と定義することはしない．

なぜなら，この考え方によれば，n 次方程式の“ガロア群”はすべて S_n となってしまうからである．

“ガロア群”は，考えている n 次方程式の解のかたちの違いが表れるように定義されなければならない．

そこで，2 次式 $x^2 - 2 = 0$ の最小分解体，つまり $\mathbb{Q}$ に $\sqrt{2}$ を添加した体 $\mathbb{Q}(\sqrt{2})$ の世界で，基本対称式のもつ意味は残しながら，方程式の解のかたちの違いが表れるように，“ガロア群”というものの定義を考えていく．

以下は，方程式の最小分解体であるの世界で，方程式の“ガロア群”といえるものを，どのような考え方から定義していくのかについて説明する．

そのために扱う方程式は,

$$x^3 - 3x^2 - 2x + 6 = 0 \tag{11.2}$$

である.

$$x^3 - 3x^2 - 2x + 6 = (x - \sqrt{2})(x + \sqrt{2})(x - 3)$$

と因数分解できることから，方程式の解は

$$x_1 = \sqrt{2},\ x_2 = -\sqrt{2},\ x_3 = 3$$

となる．したがって，この方程式の最小分解体は，$\mathbb{Q}(\sqrt{2})$ である．

ガロア理論で，群が作用する対象は方程式の解であると述べてきた.

したがって，今，考えている方程式は 3 次方程式なので，この 3 つの解たちに作用する群は 3 次対称群 S_3 である.

そして，S_3 のどんな置換をこの 3 つの解たちによる基本対称式に作用させても，基本対称式の値は変化しない.

しかし，この考え方で，方程式の“ガロア群”を S_3 とすることはできない.

なぜならば．この方程式には解 $x_3 = 3$ という $\mathbb{Q}$ の数が含まれているからである.

ガロア理論で問題にしているのは，方程式の $\mathbb{Q}$ でない解のかたちである.

したがって，ガロア理論で問題にすべきこの方程式の解は，$x_1 = \sqrt{2}$ と $x_2 = -\sqrt{2}$ だけであり，そしてこれが関係する方程式は，$x - 3$ を除外した 2 次方程式

$$x^2 - 2 = 0$$

でなければならない.

したがって，方程式 $x^3 - 3x^2 - 2x + 6 = 0$ の“ガロア群”は S_2 となるように定義したい.

このようなことから, 考え出された数学的な道具が, 次に説明する最小分解体 $\mathbb{Q}(\alpha)$ の“$\mathbb{Q}$ 自己同型写像”というものである.

“写像”，“同型写像”，“$\mathbb{Q}$ 自己同型写像”を，順に簡単に説明しよう.

写像：集合 A の元 a に対して，集合 B の元 b を対応づけるもの

$$a \longrightarrow b$$

同型写像：集合 A の元 a に対して，A と同じ元の個数の集合 B の元 b を
1 体 1 に対応づけるもの

$$a \longleftrightarrow b$$

“$\mathbb{Q}$ 自己同型写像”については，方程式 $x^3 - 3x^2 - 2x + 6 = 0$ の最小分解体 $\mathbb{Q}(\sqrt{2})$ で説明する.

$\mathbb{Q}(\sqrt{2})$ の $\mathbb{Q}$ **自己同型写像**：$\mathbb{Q}(\sqrt{2})$ から自分自身 $\mathbb{Q}(\sqrt{2})$ への同型写像で,

$\mathbb{Q}$ の元は動かさないようなもの

$$a + b\sqrt{2} \longleftrightarrow a + c\sqrt{2}$$

ここで，$a, b, c \in \mathbb{Q}$

$\mathbb{Q}(\sqrt{2})$ の $\mathbb{Q}$ 自己同型写像という道具を使うと，方程式 $x^3 - 3x^2 - 2x + 6 = 0$ の解から $x = 3$ という $\mathbb{Q}$ の数を除外することもできるし，方程式によっては，$\mathbb{Q}$ でない解に関しても，より細かく解のかたちの違いを解析することもできるのである．

以下が，$\mathbb{Q}(\alpha)$ の“$\mathbb{Q}$ 自己同型写像”の正確な定義である．

$\mathbb{Q}(\alpha)$ の $\mathbb{Q}$ 自己同型写像の定義

α は有理数ではない数とする．φ（ファイと読む）が $\mathbb{Q}(\alpha)$ の $\mathbb{Q}$ **自己同型写像**とは，変換する前の $\mathbb{Q}(\alpha)$ の数と変換した後の $\mathbb{Q}(\alpha)$ の数が 1 対 1 に対応付けるものであって，さらに以下の 2 つの条件を満たすものである．

（条件 1）$\mathbb{Q}(\alpha)$ のどんな数 x, y に対しても

(1)　$\varphi(x + y) = \varphi(x) + \varphi(y)$　　(2)　$\varphi(xy) = \varphi(x)\varphi(y)$

（条件 2）$\mathbb{Q}$ の数 u に対しては

(3)　$\varphi(u) = u$

条件 1 は，変換する前の $\mathbb{Q}(\alpha)$ 内の演算が，変換後の $\mathbb{Q}(\alpha)$ 内の演算に影響を与えないように定義されている．

つまり，変換前の x と y の足し算 $x + y$ は，変換後に $\varphi(x + y)$ となるが，これは $\varphi(x)$ と $\varphi(y)$ の足し算に一致するように定義されている．

掛け算 xy は変換後に $\varphi(xy)$ となるが，これは $\varphi(x)$ と $\varphi(y)$ の掛け算に一致するように定義されている．

条件 2 は，有理数は変換によって動かさないということを定義している．

”$\mathbb{Q}$ 自己同型写像”を理解することが，”ガロア群”を理解することに繋がるのである．

しかし，“$\mathbb{Q}$ 自己同型写像”をどのように作ればよいのか？

これに対応する回答として，ガロア理論では，以下の重要な定理が証明されている．

定理（$\mathbb{Q}$ 自己同型写像と置換の関係） n 次方程式の最小分解体を M とする．このとき，M の $\mathbb{Q}$ 自己同型写像について，以下が成り立つ．

(1) M の $\mathbb{Q}$ 自己同型写像の個数は，$[M:\mathbb{Q}]$ に一致する．

(2) M の $\mathbb{Q}$ 同型写像は，n 次方程式の n 個の解の内，$\mathbb{Q}$ の解以外の解同士を変換するものとして定義できる．

(3) M の $\mathbb{Q}$ 自己同型写像は，n 次方程式の解に作用する n 次対称群 S_n のある置換に対応し，それらの置換全体は S_n の部分群である．

例題 18. $\mathbb{Q}$ 係数の方程式 $x^3-3x^2-2x+6=0$ を考える．このとき，この方程式の最小分解体 $\mathbb{Q}(\sqrt{2})$ の $\mathbb{Q}$ 自己同型写像全体は，S_2 に対応することを示せ．

（解答）　定理（$\mathbb{Q}$ 自己同型写像と置換の関係）を用いる．

最小分解体は $\mathbb{Q}(\sqrt{2})$ なので，$[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$ である．よって，$\mathbb{Q}(\sqrt{2})$ の $\mathbb{Q}$ 自己同型写像の個数は 2 個である．

$\mathbb{Q}(\sqrt{2})$ の $\mathbb{Q}$ 自己同型写像は，$x^3-3x^2-2x+6=0$ の解 $x_1=\sqrt{2},\ x_2=-\sqrt{2},\ x_3=3$ の内，$\mathbb{Q}$ の解 $x_3=3$ 以外の $\sqrt{2}$ と $-\sqrt{2}$ 同士を変換するものとして定義できるので，以下に，それを作る．

(1) $\mathbb{Q}(\sqrt{2})$ の数を $a+b\sqrt{2}$ に対して，

$$\varphi_1 : a+b\sqrt{2} \longrightarrow a+b\sqrt{2}$$

とすると，これは明らかに，同型写像 $a+b\sqrt{2} \leftrightarrow a+b\sqrt{2}$ であり，$\varphi_1(\sqrt{2}) = \sqrt{2}$, $\varphi_1(-\sqrt{2}) = -\sqrt{2}$ である．

(2) $\mathbb{Q}(\sqrt{2})$ の数 $a+b\sqrt{2}$ に対して，

$$\varphi_2 : a+b\sqrt{2} \longrightarrow a-b\sqrt{2}$$

とすると，これも明らかに，同型写像 $a+b\sqrt{2} \leftrightarrow a-b\sqrt{2}$ であり，$\varphi_2(\sqrt{2}) = -\sqrt{2}$, $\varphi_2(-\sqrt{2}) = \sqrt{2}$ である．

解 x_1, x_2 に作用する置換は，e と $(1\ 2)$ である．そして，φ_1 は恒等置換 e に対応し，φ_2 は置換 $(1\ 2)$ に対応する．したがって，$\mathbb{Q}(\sqrt{2})$ の $\mathbb{Q}$ 自己同型写像全体は，$S_2 = \{e,\ (1\ 2)\}$ に対応する．□

準備は整った．以下が，n 次方程式のガロア群の定義である．

【n 次方程式の群の定義】　定理（$\mathbb{Q}$ 自己同型写像）で述べられた M の $\mathbb{Q}$ 自己同型写像全体に対応する S_n の部分群のことを，n **次方程式のガロア群**，または単に**方程式の群**といい，以下のように表す．

$$Gal(M/\mathbb{Q})$$

「ガロア群の定義の意味を振り返る．」

なぜ，方程式のガロア群をつくるための $\mathbb{Q}$ 自己同型写像には，「$\mathbb{Q}$ の元は動かさない」という条件が付くのだろうか？

この疑問に対する回答をもう一度振り返る．

例題 18 で扱った方程式は，見かけ上は 3 次方程式 $x^3-3x^2-2x+6=0$ であった．

この 3 つの解 $x_1 = \sqrt{2},\ x_2 = -\sqrt{2},\ x_3 = 3$ に対して，基本対称式を考えると，

$$x_1 + x_2 + x_3 = -3,\quad x_1x_2 + x_2x_3 + x_3x_1 = -2,\quad x_1x_2x_3 = -6$$

となる．

そしてこれらの解に作用する置換は，形式的には S_3 の元であり，S_3 の中のどの置換を作用させても，基本対称式の値は動かない．

しかし，この 3 次方程式は $\mathbb{Q}$ 上で $(x-3)(x^2-2) = 0$ と因数分解される．

ガロア理論は，解が $\mathbb{Q}$ 以外の数となるもの，すなわち解が有理数以外の数となる方程式の構造を扱うことを目的としている．

したがって，2 次方程式 $x^2 - 2 = 0$ がガロア理論で扱う対象となる．

この 2 次方程式から得られる基本対称式 $x_1 + x_2 = 0,\ x_1x_2 = -2$ に作用する置換の集合は S_2 となる．

つまり，$\mathbb{Q}$ 自己同型写像に付けられた条件「$\mathbb{Q}$ の元は動かさない」は，最初から，置換を作用する解に $\mathbb{Q}$ の解は考えないことにしたかったために，付けられた条件となっている．

このような理由から，$\mathbb{Q}$ 係数の n 次方程式方程式のガロア群は，必然的に有理数以外の解だけに作用する置換の集合となる．

しかし，S_n の元の中のある置換 σ が，最小分解体 M から M への 1 対 1 対応を与えるものであるにもかかわらず，有理数を動かすものである場合も当然起こりうるはずである．

このような置換 σ は，定義より，この方程式のガロア群の元から除外される．

そして，これこそがガロア群の定義が主張していることである．

すなわち，ガロア理論では，S_n からこのような置換を除外していくことで，その方程式がどのような種類の解を持っているのかを調べようとしているのである．

Memorize：方程式のガロア群

$\mathbb{Q}$ 係数の n 次方程式に使われる n 次式の最小分解体を M とする．このとき n 次対称群 S_n の置換から得られる M の $\mathbb{Q}$ 自己同型写像全体が，n 次方程式のガロア群である．

次の問題に答えることができますか？

問題 13. $\mathbb{Q}$ 係数の方程式 $x^3 + x^2 - 3x - 3 = 0$ のガロア群を求めよ．

第 12 章

方程式 $x^n - a = 0$ のガロア群

方程式 $x^n - \alpha = 0$ のガロア群を調べて，それと一般の n 次方程式との違いをみること，これがガロア理論のアイディアである．

なぜならば，一般に $x^n - \alpha = 0$ というタイプの方程式の解は，$\sqrt{}$，$\sqrt[3]{}$，$\sqrt[4]{}\cdots$ を組み合わせて表すことができるからである．

以下では, 方程式 $x^4-3=0$ を例に, 4 つの解のかたちや方程式 $x^4-3=0$ のガロア群の求め方を説明する．

$\sqrt[4]{3}$ は 4 乗して 3 となる数を意味するものであった．

したがって，$\sqrt[4]{3}$ は 4 次方程式 $x^4 - 3 = 0$ の 1 つの解である．

そして，$-\sqrt[4]{3}$ も $x^4 - 3 = 0$ の解であることはすぐわかる．

残りの 2 つの解はなんだろう．

ここで虚数単位 $i = \sqrt{-1}$ を思い出すと，$i^2 = -1$ であったので $i^4 = 1$ である．

したがって，残りの 2 つの解は $i\sqrt[4]{3}$ と $-i\sqrt[4]{3}$ であることがわかる．

すなわち，方程式 $x^4 - 3 = 0$ は $\sqrt[4]{3}$ と $i = \sqrt{-1}$ を用いて表現できたことを意味する．

以下，方程式 $x^4 - 3 = 0$ のガロア群を求めていく．

そのためには $x^4 - 3$ の最小分解体を求めなくてはならない．

方程式 $x^4 - 3 = 0$ の 4 つの解を

$$x_1 = \sqrt[4]{3},\quad x_2 = -\sqrt[4]{3},\quad x_3 = i\sqrt[4]{3},\quad x_4 = -i\sqrt[4]{3}$$

と置く．

この数から $\mathbb{Q}$ の数でないものは，$\sqrt[4]{3}$ と i であるので，$x^4 - 3$ の最小分解体は $\mathbb{Q}(\sqrt[4]{3}, i)$ である．

$\mathbb{Q}(\sqrt[4]{3}, i)$ を $K = \mathbb{Q}(\sqrt[4]{3})$ として $K(i)$ と考えると，体 $K(i)$ は K の 2 次拡大，すなわち $[K(i) : K] = 2$ である．

体 K は $\mathbb{Q}$ の 4 次拡大，すなわち $[K : \mathbb{Q}] = 4$ であるので，

$$[\mathbb{Q}(\sqrt[4]{3}, i) : \mathbb{Q}] = [K(i) : K][K : \mathbb{Q}] = 8$$

すなわち，最小分解体 $\mathbb{Q}(\sqrt[4]{3}, i)$ は $\mathbb{Q}$ の 8 次拡大であることがわかる．

$\mathbb{Q}(\sqrt[4]{3}, i)$ を，生成元を用いて表すと，

$$\mathbb{Q}(\sqrt[4]{3}, i) = \mathbb{Q}\langle 1,\ \sqrt[4]{3},\ \sqrt[4]{9},\ \sqrt[4]{27},\ i,\ i\sqrt[4]{3},\ i\sqrt[4]{9},\ i\sqrt[4]{27}\rangle$$

となる．

$x^4 - 3 = 0$ のガロア群を求めることは，24 個の元をもつ 4 次対称群 S_4 を用いて，これを一つずつチェックして，$\mathbb{Q}(\sqrt[4]{3}, i)$ の $\mathbb{Q}$ 自己同型写像を決めていくことである．

ところが，$\mathbb{Q}(\sqrt[4]{3}, i)$ の生成元は，

$$1,\ \sqrt[4]{3},\ \sqrt[4]{9},\ \sqrt[4]{27},\ i,\ i\sqrt[4]{3},\ i\sqrt[4]{9},\ i\sqrt[4]{27}$$

の 8 個もあり，これらの組み合わせを考慮した置換から，$\mathbb{Q}$ 自己同型写像を考えていくことは大変な作業に思える．

しかし，第１１章の中の定理（$\mathbb{Q}$ 自己同型写像と置換の関係）を思い出そう．もう一度，この定理の使い方を，次の例題で確認しよう．

例題 19. 方程式 $x^4 - 3 = 0$ のガロア群 $Gal(\mathbb{Q}(\sqrt[4]{3}, i)/\mathbb{Q})$ を求めよ．

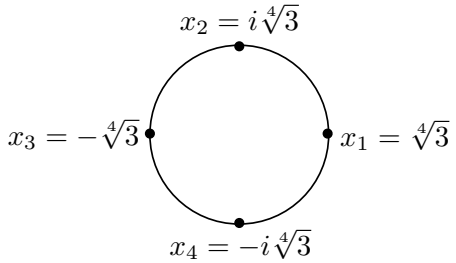
（解答）　最小分解体 $\mathbb{Q}(\sqrt[4]{3}, i)$ から $\mathbb{Q}(\sqrt[4]{3}, i)$ への置換から作られる $\mathbb{Q}$ 自己同型写像をすべて求めればよい．$\mathbb{Q}(\sqrt[4]{3}, i)$ の生成元は，

$$1,\ \sqrt[4]{3},\ \sqrt[4]{9},\ \sqrt[4]{27},\ i,\ i\sqrt[4]{3},\ i\sqrt[4]{9},\ i\sqrt[4]{27}$$

の 8 個あるので，定理（$\mathbb{Q}$ 自己同型写像と置換の関係）の (1) より，$\mathbb{Q}$ 自己同型写像は 8 個ある．$x^4 - 3 = 0$ の 4 つの解を

$$x_1 = \sqrt[4]{3},\ \ x_2 = i\sqrt[4]{3},\ \ x_3 = -\sqrt[4]{3},\ \ x_4 = -i\sqrt[3]{3}$$

とする．この 4 つの解を形式的に下図のように配置して考える．



まず，恒等置換 e に対応する $\varphi_1(x_j) = x_j$ は，明らかに $\mathbb{Q}$ 自己同型写像である．ここで，$j = 1, 2, 3, 4$ を意味する．

次に，図の 4 つの解を回転させるイメージから 3 つの $\mathbb{Q}$ 自己同型写像が作れることがわかる．1 つ目は，90° 回転とする置換 $\sigma = (1\ 2\ 3\ 4)$ に対応する $\mathbb{Q}$ 自己同型写像

$$\varphi_2(x_j) = ix_j$$

である．2 つ目は，180° 回転とする置換 $\sigma^2 = (1\ 2\ 3\ 4)(1\ 2\ 3\ 4) = (1\ 3)(2\ 4)$ に対応する $\mathbb{Q}$ 自己同型写像

$$\varphi_3(x_j) = i^2x_i = -x_j$$

であり，3 つ目は，270° 回転とする置換 $\sigma^3 = (1\ 3)(2\ 4)(1\ 2\ 3\ 4) = (1\ 4\ 3\ 2)$ に対応する $\mathbb{Q}$ 自己同型写像

$$\varphi_4(x_j) = i^3x_i = -ix_j$$

である．そして，鏡映に関する置換 $\tau = (1\ 3)$ に対応する $\mathbb{Q}$ 自己同型写像は

$$\varphi_5(x_j) = (-1)^j x_j$$

であり，鏡映に関する置換 $\sigma\tau = (1\ 4)(2\ 3)$ に対応する $\mathbb{Q}$ 自己同型写像は

$$\varphi_6(x_j) = (-1)^j ix_j$$

で，さらに鏡映に関する置換 $\sigma^2\tau = (2\ 4)$ に対応する $\mathbb{Q}$ 自己同型写像は

$$\varphi_7(x_j) = (-1)^{j+1}x_i$$

となる．最後に，鏡映に関する置換 $\sigma^3\tau = (1\ 2)(3\ 4)$ に対応する $\mathbb{Q}$ 自己同型写像

$$\varphi_8(x_j) = (-1)^{j+1}ix_j$$

がある．

以上のことから，$\sigma = (1\ 2\ 3\ 4)$，$\tau = (1\ 3)$ と置くと，

$$Gal(\mathbb{Q}(\sqrt[4]{3}, i)/\mathbb{Q}) = \{e,\ \sigma,\ \sigma^2,\ \sigma^3,\ \tau,\ \sigma\tau,\ \sigma^2\tau,\ \sigma^3\tau\} \tag{12.1}$$

であることがわかった．□

例題 19 から得られた $x^4 - 3 = 0$ のガロア群 $Gal(\mathbb{Q}(\sqrt[4]{3}, i)/\mathbb{Q})$ の表示 (12.1) をみると，90° 回転とする $\sigma = (1\ 2\ 3\ 4)$ と，鏡映とする $\tau = (1\ 3)$ で生成されていることがわかる．

これを，簡単に

$$Gal(\mathbb{Q}(\sqrt[4]{3}, i)/\mathbb{Q}) = \langle \sigma, \tau \rangle, \quad \sigma^4 = \tau^2 = e$$

と表し，群 $\langle \sigma, \tau \rangle$ を 4 **次二面体群** D_4 ともいう．

一般に，$\sigma^n = \tau^2 = e$ となる置換 σ と τ で生成される

群 $D_n = \langle \sigma, \tau \rangle$ を n **次二面体群**という．

これは正 n 角形の頂点に作用する群である．そしてガロア理論では，以下の定理が証明されている．

定理（$x^n - a = 0$ のガロア群）　$\mathbb{Q}$ 係数の n 次方程式 $x^n - a = 0$ のガロア群は，ほとんどの場合，n 次二面体群 D_n となる．

くり返しになるが，$x^4 - 3 = 0$ のガロア群は S_4 ではなく，回転 $\sigma = (1\ 2\ 3\ 4)$と鏡映 $\tau = (1\ 3)$ といった巡回的な元から生成される S_4 の部分群である D_4 である．

しかし，振り返ってみると，$x^4 - 3 = 0$ の解が円上に巡回的に配置しているというイメージからガロア群 D_4 を推測することは難しくない．

このような解の配置の考え方は，どのような 3 次方程式や 4 次方程式もその解がすべて $\sqrt{\ }$, $\sqrt[3]{\ }$, $\cdots$ を組み合わせて表現できるということに繋がっている．

つまり，3 次方程式や 4 次方程式は，なんらかの方法で，それらの解の配置を，円上に巡回的に並べて考えられることができることを意味し，その結果，方程式のガロア群がいくつかの巡回的な元から構成されているのである．

一般に，考えている n 次方程式の解が，円上に規則的に配置しているように考えられるとき，または，何らかの方法で，そのような配置にすることができるなら，そのガロア群は n 次対称群 S_n ではなく，巡回的な特徴をもつ S_n の部分群であると考えられる．

このような特徴が，この種の方程式のガロア群の中に隠されている．

Memorize：$x^4 - 3 = 0$ の最小分解体とガロア群

・$x^4 - 3 = 0$ の最小分解体は
　$\mathbb{Q}(\sqrt[4]{3}, i) = \mathbb{Q}\langle 1,\ \sqrt[4]{3},\ \sqrt[4]{9},\ \sqrt[4]{27},\ i,\ i\sqrt[4]{3},\ i\sqrt[4]{9},\ i\sqrt[4]{27}\rangle$ である．
・$x^4 - 3 = 0$ のガロア群 $Gal(\mathbb{Q}(\sqrt[4]{3}, i)/\mathbb{Q})$ は，4 次四面体群 D_4 である．

次の問題に答えることができますか？

問題 14. $\mathbb{Q}$ 係数の方程式 $x^6 - 2 = 0$ の解は，$\eta = \dfrac{1 + \sqrt{3}i}{2}$ とすると，

$$x_1 = \sqrt[6]{2},\quad x_2 = \eta\sqrt[6]{2},\quad x_3 = \eta^2\sqrt[6]{2},\quad x_4 = -\sqrt[6]{2},\quad x_5 = \eta^4\sqrt[6]{2},\quad x_6 = \eta^5\sqrt[6]{2}$$

である．これを円上に等間隔に配置し，それを用いて，$x^6 - 2 = 0$ のガロア群を求めよ．

第 13 章

ガロア理論の結論

ガロア理論で扱う中心的な問題は

『どのような方程式の解が，$\sqrt{\ }$，$\sqrt[3]{\ }$，$\sqrt[4]{\ }$，$\cdots$ という記号を用いて表すことができるか，それを判定する方法は何か？』

というものである．

この問題に対する解答のイメージを，すなわち，ガロア理論の結論を，これまで準備してきた基本的な道具や考え方をもとに説明する．

まず，方程式 $x^4 - 3 = 0$ のガロア群 $D_4 = \langle \sigma, \tau \rangle$ について，その正規部分群 $C(e)$ ついて考えよう．

正規部分群 $C(e)$ とは，D_4 の特別な部分群，つまり，任意の $\eta \in D_4$ に対して

$$\eta C(e) = C(e)\eta$$

を満たすものであった．

そこで，回転に関する巡回群 $C(e) = \langle \sigma \rangle = \{e,\ \sigma,\ \sigma^2,\ \sigma^3\}$ を考えると，これは，D_4 の正規部分群である．

なぜならば，$\sigma C(e) = C(e)\sigma \in C(e)$ が成り立つことは明らかで，

$C(\tau) = \{\tau,\ \sigma\tau, \sigma^2\tau,\ \sigma^3\tau\}$ と置くと，

$$\tau\sigma = (1\ 3)(1\ 2\ 3\ 4) = (1\ 2)(3\ 4) = (1\ 4\ 3\ 2)(1\ 3) = \sigma^3\tau \in C(\tau)$$

となり，

これを参考に実際に計算すると，$\tau C(e) = C(e)\tau \in C(\tau)$ が成り立つことも確かめられ，同様にして，$j = 1, 2, 3$ として

$$(\sigma^j\tau)C(e) = C(e)(\sigma^j\tau) \in C(\tau)$$

も，実際の計算から成り立つことがわかるからである．

したがって，D_4 は

$$D_4 = C(e) \oplus C(\tau)$$

と，回転部 $C(e)$ と鏡映部 $C(\tau)$ にクラス分けされる．

これより，位数 2 の巡回群である商群

$$D_4/C(e) = \{C(e),\ C(\tau)\} = \langle C(\tau)\rangle$$

が得られる．

以上をまとめると，

多項式 $x^4 - 3$ の最小分解体は，$\mathbb{Q}(\sqrt[4]{3}, i)$ である．

これを使って方程式 $x^4 - 3 = 0$ のガロア群 $Gal(\mathbb{Q}(\sqrt[4]{3}, i)/\mathbb{Q})$ を求めると，

$Gal(\mathbb{Q}(\sqrt[4]{3}, i)/\mathbb{Q})$ は 4 次二面体群 D_4 であることが分かる．

さらに，D_4 の正規部分群 $C(e)$ を用いると，

商群 $D_4/C(e)$ は，位数 2 の巡回群 S_2 と**群として同じ**である，

ということがいえたのである．

以下，ある群 G が S_n の部分群 H と群として同じ（**同型**という）であるとき，必要に応じて G を H として扱う．

ところで，明らかに巡回群 $S_2 = \{e, (1\ 2)\}$ の正規部分群は $\{e\}$ のみである．

そして，一般に群 G の正規部分群が $\{e\}$ のみであるとき，

G は**単純群**と呼ばれる．

したがって，S_2 と同型である $D_4/C(e)$ は単純群である．

例題 20. 4 次四面体群 D_4 の置換 $\sigma = (1\ 2\ 3\ 4)$ の 2 乗 $\sigma^2 = (1\ 3)(2\ 4)$ から生成される部分群 $C(e) = \langle \sigma^2 \rangle = \{e,\ \sigma^2\}$ を考える．このとき，$C(e)$ は D_4 の正規部分群で，商群 $D_4/C(e)$ は単純群ではないことを示せ．

（**解答**）　$D_4 = \langle \sigma,\ \tau \rangle$ であった．ここで，$\tau = (1\ 3)$ である．そして，D_4 の置換は $\sigma^j\tau$ と書けた．ただし $j = 1, 2, 3, 4$ である．D_4 の置換は 8 個あり，e と σ^2 以外の 6 個は

$$\sigma = (1\ 2\ 3\ 4),\ \ \sigma^3 = (1\ 4\ 2\ 3),\ \ \tau(1\ 3),$$

$$\sigma\tau = (1\ 4)(2\ 3),\ \ \sigma^2\tau = (2\ 4),\ \ \sigma^3\tau = (1\ 2)(3\ 4)$$

である．そこで，

$$C(\sigma) = \{\sigma,\ \sigma^3\},\ \ C(\sigma\tau) = \{\sigma\tau,\ \sigma^3\tau\},\ \ C(\tau) = \{\tau,\ \sigma^2\tau\}$$

と置くと，

$$\sigma C(e) = C(e)\sigma \in C(\sigma),\ \ \sigma^3 C(e) = C(e)\sigma^3 \in C(\sigma),$$

$$(\sigma\tau)C(e) = C(e)(\sigma\tau) \in C(\sigma\tau),\ \ (\sigma^3\tau)C(e) = C(e)(\sigma^3\tau) \in C(\sigma\tau)$$

$$\tau C(e) = C(e)\tau \in C(\tau),\ \ (\sigma^2\tau)C(e) = C(e)(\sigma^2\tau) \in C(\tau)$$

であることが簡単な計算で確かめられる．よって，$C(e)$ は D_4 の正規部分群である．

そして，商群 $D_4/C(e) = \{C(e),\ C(\sigma),\ C(\sigma\tau),\ C(\tau)\}$ が得られる．

ここで，$D_4/C(e)$ の部分集合

$$N(e) = \{C(e),\ C(\sigma)\}$$

を取り出すと，これは $D_4/C(e)$ の正規部分群である．

なぜならば，$N(\tau) = \{C(\tau),\ C(\sigma\tau)\}$ と置くと，

$$C(\tau)N(e) = N(e)C(\tau) \in N(\tau),\ \ C(\sigma\tau)N(e) = N(e)C(\sigma\tau) \in N(\tau)$$

が，得られるからである．

以上により，$D_4/C(e)$ は単純群でないことが示された．□

ガロア理論では，例題 20 は，以下のように一般化された定理にまとめられる．

定理（単純群となる商群）　N を群 G の正規部分群として，さらに，$N \subset N'$ となる G の正規部分群 N' は存在しないとする．このとき，商群 G/N は単純群である．

さて，群 G の正規部分群 N_1，N_1 の正規部分群 N_2，N_2 の正規部分群 N_3 などを考える．

このような正規部分群たちを使って得られる包含関係の列

$$G \supset N_1 \supset N_2 \cdots \supset N_r \supset \{e\}$$

を，G の**正規部分群の列**という．

もし，G の正規部分群の列の途中に，

これ以上正規部分群を含めることができないとき，

その列を G の**組成列**という．

定理（単純群となる商群）から，直ちに次の定理が得られる．

定理（組成列から得られる単純群）　群 G の組成列を

$$G \supset N_1 \supset N_2 \cdots \supset N_r \supset \{e\}$$

とする．このとき，これらから得られる商群たち

$$G/N_1,\quad N_1/N_2,\quad \cdots\quad N_{r-1}/N_r,\quad N_r/\{e\}$$

は，すべて単純群である．

群 G の組成列から得られる単純群である商群を，

群 G の**組成列から得られる単純群**，または，群 G の**組成因子**と呼ぶ．

そして，次の定理は，ガロア理論の理解に繋がる重要なものである．

定理（$x^n - a = 0$ の群の組成因子による分解）　a を有理数とした n 次方程式 $x^n - a = 0$ を考えると，この解は $\sqrt{\ }$, $\sqrt[3]{\ }$, $\cdots$ を組み合わせて表現できる．さらに，$x^n - a = 0$ のガロア群を G とすると，G のある組成列から得られる単純群（組成因子）の位数は，すべて素数となる．

上の定理を理解するために，例題 19 で扱った方程式 $x^4 - 3 = 0$ の解とガロア群を復習する．

まず，この方程式の 4 つの解は，$i = \sqrt{-1}$ とすると

$$\sqrt[4]{3},\quad -\sqrt[4]{3},\quad i\sqrt[4]{3},\quad -i\sqrt[4]{3}$$

であり，$\sqrt[4]{\ }$ と $\sqrt{\ }$ で書けている．

次に，この方程式 $x^4 - 3 = 0$ のガロア群 $Gal(\mathbb{Q}(\sqrt[4]{3}, i)/\mathbb{Q})$ は，S_4 の部分群 $D_4 = \langle \sigma, \tau \rangle$ であった．

ここで，σ は $\sigma = (1\ 2\ 3\ 4)$ であり $\sigma^4 = e$ という回転を，τ は $\tau = (1\ 3)$ であり $\tau^2 = e$ となる鏡映を表す．

そして，$N_1 = \langle \sigma \rangle$ は，ガロア群 D_4 の正規部分群であり，さらに $N_2 = \langle \sigma^2 \rangle$ は N_1 の正規部分群であり，そして N_2 の正規部分群は $\{e\}$ である．

これより，D_4 の組成列

$$D_4 \supset N_1 \supset N_2 \supset \{e\}$$

が得られる．

したがって，D_4/N_1 と N_1/N_2 はどちらも単純群で，しかも，それらの位数はどちらも素数 2 である．

それでは，ガロア理論の結論を述べよう．

それは，定理（$x^n - a = 0$ の群の組成因子による分解）に対比する形で述べられ，以下のようになる．

ガロア理論の結論

『与えられた方程式のガロア群 G のどのような組成列を考えても
それから得られる単純群（組成因子）の列の中に，
必ず位数が素数でないものが含まれるなら，
その方程式は，$\sqrt{\ }$，$\sqrt[3]{\ }$，$\cdots$ をどのように組み合わせても
表現できない解をもつ.』

Memorize：ガロア理論の結論

・$x^n - a = 0$ の解は $\sqrt{\ }$，$\sqrt[3]{\ }$，$\cdots$ を組み合わせて表現できる.
・$x^n - a = 0$ のガロア群のある組成列から得られる単純群（組成因子）はすべて位数が素数である.
・与えられた方程式のガロア群 G の組成列から得られる単純群（組成因子）の中に，位数が素数でないものが存在したら，その方程式は $\sqrt{\ }$，$\sqrt[3]{\ }$，$\cdots$ を組み合わせても表現できない解をもつ.

次の問題に答えることができますか？

問題 15. $\mathbb{Q}$ 係数の方程式 $x^3 - 2 = 0$ は，定理（$x^n - a = 0$ のガロア群）によって，$D_3 = S_3 = \{e,\ (1\ 2),\ (1\ 3),\ (2\ 3),\ (1\ 2\ 3),\ (1\ 3\ 2)\}$ である．それでは，群 S_3 のある組成列から得られる単純群は，すべて位数が素数となっていることを示せ.

ガロア理論の結論までの流れ

１．ガロア理論で扱うテーマは，$\sqrt{\ }$，$\sqrt[3]{\ }$，$\cdots$ をどのように組み合わせても表現することができない解をもつ $\mathbb{Q}$ 係数の n 次方程式

$$x^n + a_1 x^{n-1} + \cdots + a_{n+1} x + a_n = 0$$

は，どのような特徴をもつのか？　である．

$\Downarrow$

２．そのために，まず $\mathbb{Q}$ 係数の n 次方程式の解 $x_1, x_2 \cdots, x_n$ をすべて含む最小分解体 $\mathbb{Q}(x_1, x_2, \cdots, x_n)$ を考える．

$\Downarrow$

３．次に，n 次方程式のガロア群 G を求める．そのために，n 次対称群 S_n の置換を，n 次方程式の解 $x_1, x_2 \cdots, x_n$ に作用させたものから，$\mathbb{Q}(x_1, x_2, \cdots, x_n)$ の $\mathbb{Q}$ 自己同型写像が得られるかどうかを確かめる．このとき，$\mathbb{Q}$ 自己同型写像となった置換をすべて集めた集合が，方程式のガロア群 G である．

$\Downarrow$

４．その後，n 次方程式のガロア群 G の正規部分群からなる組成列

$$G \supset N_1 \supset N_2 \cdots \supset N_r \supset \{e\}$$

を考え，そしてそれらの商群

$$G/N_1,\quad N_1/N_2,\quad \cdots\quad N_{r-1}/N_r,\quad N_r/\{e\}$$

すなわち，上の組成列から得られる単純群（組成因子）の列をつくる．

⇓

５．n 次方程式のガロア群 G のある組成列から得られる単純群のすべての位数が，素数となっていれば，いま考えている n 次方程式の解 $x_1, x_2 \cdots, x_n$ は，すべて $\sqrt{\ }$，$\sqrt[3]{\ }$，$\cdots$ を組み合わせて表現できる．
　そうでなければ，G の別の組成列を考え，それから得られる単純群（組成因子）の列をつくり直す．

⇓

６．しかし，n 次方程式のガロア群 G のどのような組成列を考えても，それから得られる単純群（組成因子）の列の中に，必ず位数が素数でないものが含まれるならば，いま考えている n 次方程式のある解は，$\sqrt{\ }$，$\sqrt[3]{\ }$，$\cdots$ をどのように組み合わせても表現することができない．

５の条件を満たす群 G のことを，**可解群**と呼ぶ．

そして，ガロア理論では，$n \geq 5$ のとき，n 次対称群 S_n は可解群ではないことが示される．

このことから，5 次以上の一般的な方程式は，$\sqrt{\ }$，$\sqrt[3]{\ }$，$\cdots$ をどのように組み合わせても表現できない解が存在するという結論が得られるのである．

ガロア理論の風景を楽しむことができただろうか．

ガロア理論のストーリー【終】

問題の解答

問題 1. 1. $2x^3+4x^2+x+3$, 2. x^3+4x^2+3x+2

問題 2. 1. (1 2), 2. (2 3 4), 3. (1 2 4 3)

問題 3. 基本対称式は, $x_1+x_2+x_3+x_4$, $x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_3+x_4$, $x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4$, $x_1x_2x_3x_4$ である．また，解と係数の関係より $x_1+x_2+x_3+x_4=0$, $x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_3+x_4=a$, $x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4=-b$, $x_1x_2x_3x_4=c$ なので，基本対称式の値はすべて有理数である．

問題 4. $m\in\mathbb{Z}$ で $m\neq 1$ のとき，$m\times n=n\times m=1$ となる n は $\mathbb{Z}$ に存在しない．したがって，$\mathbb{Z}$ は掛け算で群とはならない．

問題 5.（性質 1）$a\sim a$,（性質 2）$a\sim b$ ならば $b\sim a$（性質 3）$a\sim b$ かつ $b\sim c$ ならば $a\sim c$

問題 6. $C(k)$ を 5 で割った余りが k であるものの集合とすると，$\mathbb{Z}=C(0)\oplus C(1)\oplus C(2)\oplus C(3)\oplus C(4)$ と，5 つのクラスに分割できる．このとき，$\mathbb{Z}$ の部分群は加法における単位元 0 が含まれる $C(0)$ だけである．

問題 7. $a\in C(j)$, $b\in C(k)$ とすると，$C(a)=C(j)$, $C(b)=C(k)$ であり，$C(a\cdot b)=C(a)\cdot C(b)=C(j)\cdot C(k)=C(j\cdot k)$ である．したがって，代表元の選び方に関係なく演算が定義されている，すなわち well-defined である．また，単位元は $C(1)$ であり，$C(2)$ の逆元は $C(3)$，$C(4)$ の逆元は $C(4)$ である．結合法則は明らか．よって，$\mathbb{Z}_5^{\times}$ は群である．

問題 8. $H_4=\{e,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)$ とする．まず，確認のため H_4 が正規部分群であることを示す．$\sigma\in S_4$ に対して，$\sigma(i\ j)\sigma^{-1}(\sigma(i))=\sigma(i\ j)(i)=\sigma(j)$, $\sigma(i\ j)\sigma^{-1}(\sigma(j))=\sigma(i\ j)(j)=\sigma(i)$ である．これは，$\sigma(i\ j)\sigma^{-1}=(\sigma(i)\ \sigma(j))$ を意味する．これより，$\sigma(i\ j)(k\ l)\sigma^{-1}=(\sigma(i\ j)\sigma^{-1})(\sigma(k\ l)\sigma^{-1})=(\sigma(i)\ \sigma(j))(\sigma(k)\ \sigma(l))$．したがって，$\sigma(i\ j)(k\ l)\sigma^{-1}\in H_4$ であり，$\sigma H_4=H_4\sigma$ が成り立つ．したがって，H_4 は S_4 の正規部分群である．

（1）S_4 は H_4 により，以下のように 6 個のクラスに分割される．

$$S_4=C(e)\oplus C(\sigma_1)\oplus C(\sigma_2)\oplus C(\sigma_3)\oplus C(\sigma_4)\oplus C(\sigma_5)$$

ここで，$C(e) = H_4$, $\sigma_1 = (1\ 2)$, $\sigma_2 = (1\ 3)$, $\sigma_3 = (1\ 4)$, $\sigma_4 = (1\ 2\ 3)$, $\sigma_5 = (1\ 3,\ 3)$ である．

（2）$\sigma,\tau \in S_4$ に対して，$C(\sigma)C(\tau) = C(\sigma\tau)$ と定義する．$\sigma' \in C(\sigma)$, $\tau' \in C(\tau)$ とすると，$C(\sigma') = C(\sigma)$, $C(\tau') = C(\tau)$ より，$C(\sigma'\tau') = C(\sigma')C(\tau') = C(\sigma)C(\tau) = C(\sigma\tau)$ である．よって，well-defined である．

問題 9. 1. (1 2 3 4), (1 4 3 2), (1 3)(2 4)

2. (1 3), (2, 4)

3. $\sigma = (1\ 3)$, $(2\ 4)$ のどちらにおいても，$\sigma(1\ 2\ 3\ 4) = (1\ 4\ 3\ 2)\sigma$, $\sigma(1\ 3)(2\ 4) = (1\ 3)(2\ 4)\sigma$ である．よって，$\sigma C(e) = C(e)\sigma$ が成り立つ．

4. 回転 $C(e)$ と鏡映 $C((1\ 3))$ を要素にもつ群．

問題 10. 足し算，引き算，掛け算が $\mathbb{R}(i)$ の元であることは明らか．割り算については，$\dfrac{1}{a+bi} = \dfrac{a-bi}{(a+bi)(a-bi)} = \dfrac{a}{a^2+b^2} - \dfrac{b}{a^2+b^2}i \in \mathbb{R}(i)$

問題 11. (1) まず，$\mathbb{Q}(\sqrt[3]{2},\sqrt{3}) = \{a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4} + a_3\sqrt{3} + a_4\sqrt[3]{2}\sqrt{3} + a_5\sqrt[3]{4}\sqrt{3} \mid a_j \in \mathbb{Q}\}$ である．$\mathbb{Q}(\sqrt[3]{2},\sqrt{3}) \supset \mathbb{Q}(\sqrt[3]{2}+\sqrt{3})$ は，$\sqrt[3]{2}+\sqrt{3} \in \mathbb{Q}(\sqrt[3]{2},\sqrt{3})$ より明らかである．

次に，$\mathbb{Q}(\sqrt[3]{2},\sqrt{3}) \subset \mathbb{Q}(\sqrt[3]{2}+\sqrt{3})$ を示すために，$\mathbb{Q}(\sqrt[3]{2}+\sqrt{3})$ の生成元を求める．$\alpha = \sqrt[3]{2}+\sqrt{3}$ と置くと，$(\alpha-\sqrt{3})^3 = 2$ であり，これより $\alpha^3+9\alpha-2 = (3\alpha^2+3)\sqrt{3}$ を得る．さらに両辺を 2 乗することで，$\alpha^6 + 18\alpha^4 - 4\alpha^3 + 81\alpha^2 - 36\alpha + 4 = 27\alpha^4 + 54\alpha^2 + 27$，すなわち，$\alpha^6 - 9\alpha^4 - 4\alpha^3 + 27\alpha^2 - 36\alpha - 23 = 0$ を得る．したがって，$\mathbb{Q}(\sqrt[3]{2}+\sqrt{3})$ の生成元は，1, α, α^2, α^3, α^4, α^5 である．よって，$\mathbb{Q}(\alpha) = \{a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4\alpha^4 + a_5\alpha^5 \mid a_j \in \mathbb{Q}\}$ である．したがって，$\sqrt{3} = (\alpha^3+9\alpha-2)/(3\alpha^2+3) \in \mathbb{Q}(\alpha)$, $\sqrt[3]{2} = \alpha - \sqrt{3} \in \mathbb{Q}(\alpha)$ であるので，$\mathbb{Q}(\sqrt[3]{2},\sqrt{3}) \subset \mathbb{Q}(\sqrt[3]{2}+\sqrt{3})$ である．

(2) $[\mathbb{Q}(\sqrt[3]{2},\sqrt{3}) : \mathbb{Q}(\sqrt[3]{2})] = 2$

(3) $[\mathbb{Q}(\sqrt[3]{2},\sqrt{3}) : \mathbb{Q}(\sqrt{3})] = 3$

(4) $[\mathbb{Q}(\sqrt[3]{2},\sqrt{3}) : \mathbb{Q}] = 6$

問題 12. 6

問題 13. $Gal(\mathbb{Q}(\sqrt{3}/\mathbb{Q})$

問題 14. $Gal(\mathbb{Q}(\sqrt[6]{2}, \sqrt{3})/\mathbb{Q})$

問題 15. $x^3 - 2 = 0$ の解は，$\sqrt[3]{2},\ \mu\sqrt[3]{2},\ \mu^2\sqrt[3]{2}$，ただし $\dfrac{-1+\sqrt{3}i}{2}$ である．したがって，この方程式のガロア群は $Gal(\mathbb{Q}(\sqrt[3]{2},\ \sqrt{3}i)/\mathbb{Q}$ であり，これは 3 次対称群 $S_3 = \langle \sigma,\ \tau \rangle$ と同型である．ここで $\sigma = (1\ 2\ 3),\ \tau = (1\ 2)$ である．このとき，S_3 の正規部分群は $N_1 = \langle \sigma \rangle$ のみであり，N_1 の正規部分群は $\{e\}$ のみである．したがって，$S_3 \supset N_1 \supset \{e\}$ は組成列であり，商群 S_3/N_1 と $N_1/\{e\}$ はどちらも単純群であり，それらの位数は，それぞれ 2 と 3 の素数である．