代数学 I 第 1,2 回講義資料

担当：大矢 浩徳 (OYA Hironori)*

本講義のテーマは

『群論』

である．今回は群論への導入となる話を述べた後に，群の定義，基本性質，簡単な例について解説を行う．

記号．本講義を通して以下の記号を用いる．これらは一般的な記号である[*1]：

- $\mathbb{N} \coloneqq \{\text{ 自然数 }\} = \{0, 1, 2, \dots\}$
- $\mathbb{Z} \coloneqq \{\text{ 整数 }\} = \{\dots, -2, -1, 0, 1, 2, \dots\}$.
- $\mathbb{Q} \coloneqq \{\text{ 有理数 }\} = \left\{ \dfrac{b}{a} \;\middle|\; a \in \mathbb{Z} \setminus \{0\}, b \in \mathbb{Z} \right\}$.
- $\mathbb{R} \coloneqq \{\text{ 実数 }\}$.
- $\mathbb{C} \coloneqq \{\text{ 複素数 }\}$.

また，$\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ の添え字に “$> 0, \geq 0, < 0, \leq 0$” を付けて，もとの集合からそれぞれ “正，0 以上，負，0 以下” の元を集めてきてできる部分集合を表す．例えば，$\mathbb{Z}_{>0}$ は正の整数全体のなす集合，$\mathbb{R}_{\leq 0}$ は 0 以下の実数全体のなす集合である．

1.1 群論はどこから来たか?：Galois 理論概観と群論の広がり

群という数学的対象は高次代数方程式の代数的解法の研究を通して 18 世紀後半から 19 世紀にかけて数学において明確に認識されるようになった[*2]．$n \in \mathbb{Z}_{>0}$ に対し，n 次代数方程式とは，

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

という形をした x に関する方程式のことである．例えば，$n = 2$ の時は，

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

という形の方程式であり，この方程式の解の公式が

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

であることは良く知っているだろう．実は同様に 3 次方程式においてもカルダノの公式[*3]として知られる加減乗除と根号を用いた解の公式が知られている．ただし，ここでの “根号” とは n 乗根を許す意味で使っており，実際この公式では 3 乗根が現れる．4 次方程式についても加減乗除と根号を用いた解の公式が存在する．それでは，5 次以上だとどうだろうかというのはごく自然な疑問であるが，N.H.Abel は**群論的な考え方を用いて** 1820 年半ばに以下の定理を証明した．

* *e-mail* : hoya@shibaura-it.ac.jp

*1 $\mathbb{N}$ は Natural number の N，$\mathbb{Z}$ は Zahl(数，ドイツ語) の Z，$\mathbb{Q}$ は Quoziente(商，イタリア語) の Q，$\mathbb{R}$ は Real number の R，$\mathbb{C}$ は Complex number の C である．

*2 こういった方向の初期の研究者の一部として，J.L.Lagrange, P.Ruffini, A.L.Cauchy 等が挙げられる．ただ，本講義で説明するような群の定義がいきなり得られたわけではなく，その定式化には長い年月を要している．一般に数学の歴史については Victor J.Katz 著『数学の歴史』が詳しい．

*3 この公式についても面白い歴史があるので，興味のある方は調べてみてほしい．

定理 1.1

5 次以上の一般代数方程式はその係数の加減乗除と根号による解の公式を持たない.[*4]

この後，E.Galois(1811–1832) は群と代数方程式との間の関係をより明確に解明し，今日では Galois 理論と呼ばれる理論につながっている．

「群」の雰囲気をつかむために，Galois 理論[*5]についてごく簡単に説明しよう．なお，以下では未定義の用語も登場し，内容も発展的なものを含むが，今後の講義の本格的な内容には影響しないので気にする必要はない．あくまで目的は雰囲気を説明することである．

まず，複素数 $\mathbb{C}$ を考えよう．$\mathbb{C}$ は，

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\} \ (i = \sqrt{-1})$$

として表される集合で，ここでは加減乗除ができる．このような加減乗除ができる数の体系を**体 (field)** という．ここで，i と $-i$ という 2 つの複素数について考えてみよう．すると，これらはいずれも $x^2 + 1 = 0$ の解であり，i と $-i$ は取り替えても本質的な差はない．特に，i を $-i$ にするという操作は $\mathbb{C}$ の “代数的な構造” を変えない．このことは以下のように述べられる．i を $-i$ に取り替える写像を

$$\mathsf{c}\colon \mathbb{C} \to \mathbb{C},\ a + bi \mapsto a - bi.$$

と書く．この変換は複素共役を取る操作と呼ばれる．このとき，任意の $z, z' \in \mathbb{C}$ に対し，

$$\mathsf{c}(z + z') = \mathsf{c}(z) + \mathsf{c}(z') \qquad \mathsf{c}(zz') = \mathsf{c}(z)\mathsf{c}(z') \tag{1.1}$$

が成立する．1 つめの式が c が “和の構造を保つ” 変換であるということを言っており，2 つめの式が c が “積の構造を保つ” 変換であるということを言っていると考え，この意味で c という変換は $\mathbb{C}$ の代数的構造を保っていると考える．専門用語を用いれば，c は体 $\mathbb{C}$ の**自己同型写像**であるということになる．これにより，$\mathbb{C}$ が i を $-i$ にすることに関する対称性を持つと考える．

対称変換 c は明らかに $\mathsf{c} \circ \mathsf{c} = \mathrm{id}_{\mathbb{C}}$(恒等写像) を満たすので，$\mathbb{C}$ から $\mathbb{C}$ への写像からなる集合 $G_1 = \{\mathrm{id}_{\mathbb{C}}, \mathsf{c}\}$ を考えると，この集合は以下のように合成という操作で閉じている．

$$\mathrm{id}_{\mathbb{C}} \circ \mathrm{id}_{\mathbb{C}} = \mathrm{id}_{\mathbb{C}} \qquad \mathrm{id}_{\mathbb{C}} \circ \mathsf{c} = \mathsf{c} \qquad \mathsf{c} \circ \mathrm{id}_{\mathbb{C}} = \mathsf{c} \qquad \mathsf{c} \circ \mathsf{c} = \mathrm{id}_{\mathbb{C}} \tag{1.2}$$

このような対称変換からなる集合 G_1 が実は**群**の例である．このとき実数 $\mathbb{R}$ という体は以下のように “G_1 によって動かない部分” として取り出すことができる．

$$\mathbb{R} = \{z \in \mathbb{C} \mid \mathsf{c}(z) = z\} = \{z \in \mathbb{C} \mid f(z) = z, \forall f \in G_1\}.$$

自明なので逆に混乱するかもしれないが，$\mathbb{C}$ もあえて以下のように記述することができる．

$$\mathbb{C} = \{z \in \mathbb{C} \mid \mathrm{id}_{\mathbb{C}}(z) = z\}.$$

この状況を以下のような対応があると考えることにしよう．$\mathbb{C}$ の中で右の群の元で動かない部分として左の体が得られているという対応である．

$$\begin{array}{ccc} \mathbb{C} & & \{\mathrm{id}_{\mathbb{C}}\} \\ \uparrow & & \downarrow \\ \mathbb{R} & & G_1 \end{array}$$

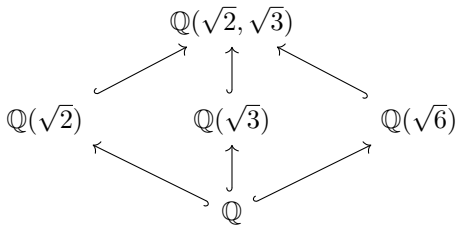
[*4] この定理において「5 次以上の一般代数方程式には解がない」とか「5 次以上の一般代数方程式は解の公式を持たない」というようにとらえるのは誤りである．一般に 5 次以上の一般代数方程式にも解は存在するが，加減乗除と根号による解の公式は作れないというのが正確な主張である．また，特殊な個別の方程式については 5 次以上でも解けるものはたくさんあるので，あくまで 5 次以上の一般的な方程式 (2 次で言うところの $x^2 + bx + c = 0$) に対しての定理であるということも認識しておく必要がある．

[*5] 本講義内では残念ながら Galois 理論までは扱わない．もし，興味のある場合は参考書などをお伝えするので個別にご連絡頂ければありがたい．

ここで見られる体 (“加減乗除ができる数の体系”) と群 (“対称性”) の対応を一般化したものが Galois 理論と呼ばれるものである[*6]．Galois 理論を標語的に言えば「体の対称性を調べればその体に含まれる体が全てわかる」というものである．もう少し非自明な例を見て雰囲気をつかもう．

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

とする．このとき，$\mathbb{Q}(\sqrt{2},\sqrt{3}), \mathbb{Q}(\sqrt{m})$ はそれぞれその中で加減乗除が完結する (加減乗除で閉じている) 数の集合となっている (本当に割り算ができるのかということについては各自チェックしてみてほしい．有理化という操作を考えれば良い．)．よってこれらは体である．ここで，明らかに次のような包含関係がある．



では，$\mathbb{Q}$ の元を動かさないような，$\mathbb{Q}(\sqrt{2},\sqrt{3})$ の自己同型 (“対称性”) はどのようなものがあるだろうか (これは $\mathbb{R}$ を動かさない $\mathbb{C}$ の対称性として c を考えたことの類似である)．基本的なものとして，$\sqrt{3}$ と $-\sqrt{3}$ を入れ替える対称性 σ と $\sqrt{2}$ と $-\sqrt{2}$ を入れ替える対称性 τ が考えられる:

$$\sigma\colon \mathbb{Q}(\sqrt{2},\sqrt{3}) \to \mathbb{Q}(\sqrt{2},\sqrt{3}),\ a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \mapsto a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6},$$
$$\tau\colon \mathbb{Q}(\sqrt{2},\sqrt{3}) \to \mathbb{Q}(\sqrt{2},\sqrt{3}),\ a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \mapsto a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6},$$

これらは (1.1) と同様の条件を満たすということは容易に確かめられる．なお，例えば σ では $\sqrt{6}$ も $-\sqrt{6}$ にしているが，これは $\sigma(\sqrt{2})=\sqrt{2}, \sigma(\sqrt{3})=-\sqrt{3}$ と定義すると，(1.1) のような条件を満たすようにするには

$$\sigma(\sqrt{6}) = \sigma(\sqrt{2}\sqrt{3}) = \sigma(\sqrt{2})\sigma(\sqrt{3}) = \sqrt{2}(-\sqrt{3}) = -\sqrt{6}$$

としないといけないということから自動的に決まっている．τ で $\sqrt{6}$ を $-\sqrt{6}$ にしているのも同じ理由である．このとき，簡単な計算で

$$\sigma\circ\sigma = \mathrm{id},\ \tau\circ\tau = \mathrm{id},\ \sigma\circ\tau = \tau\circ\sigma,\ (\sigma\circ\tau)\circ(\sigma\circ\tau) = \mathrm{id}$$

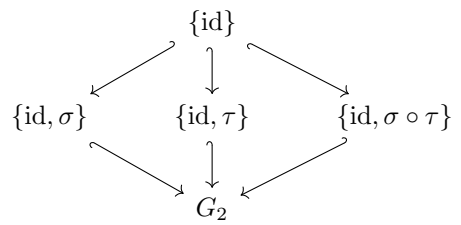
が確かめられる．$\sigma\circ\tau = \tau\circ\sigma$ は

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) \to \mathbb{Q}(\sqrt{2},\sqrt{3}),\ a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \mapsto a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6}$$

という自己同型写像である．これより，

$$G_2 \coloneqq \{\mathrm{id}, \sigma, \tau, \sigma\circ\tau\}$$

とすると，この集合は合成によって閉じている．これが群の例である．さらに，上の関係式より，G_2 の部分集合 $\{\mathrm{id}\}, \{\mathrm{id},\sigma\}, \{\mathrm{id},\tau\}, \{\mathrm{id},\sigma\circ\tau\}$ も合成によって閉じている (合成によって閉じる部分集合はこれらで全てである．例えば，$\{\sigma,\tau\}$ という部分集合を考えると，$\sigma\circ\tau \notin \{\sigma,\tau\}$ なので，これは合成では閉じていない)．このような合成によって閉じる部分集合を G_2 の**部分群**という．これらの G_2 の部分群の間には以下の包含関係がある．



[*6] なお $\mathbb{C}$ が $\mathbb{R}$ 上2次元である (複素平面) であるということは G_1 が2つの元からなる集合であるということと直接関係している．これも Galois 理論の主張の一部である．

これは上の体の包含関係と包含関係を逆にする形でピッタリ対応している．さらに，これらの対応は $\mathbb{C}$ と $\mathbb{R}$ の間の関係と同様である．つまり，例えば $H = \{\mathrm{id}, \sigma\}$ とすると，

$$\mathbb{Q}(\sqrt{2}) = \{z \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) \mid \sigma(z) = z\} = \{z \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) \mid f(z) = z, \forall f \in H\}$$

であるし，

$$\mathbb{Q} = \{z \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) \mid \sigma(z) = z, \tau(z) = z\} = \{z \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) \mid f(z) = z, \forall f \in G_2\}$$

である．この方法で，体の部分体とその対称性の群の部分群の間には包含を逆にする 1 対 1 対応が構成できる．これが Galois の基本定理の例である[*7]．

では，最後にこの話がなぜ代数方程式の可解性と関係しているのかという話を述べておこう．ここからはさらに発展的なので，雰囲気だけつかんでいただければ良い．一般代数方程式 $x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = 0$ が，加減乗除と根号で解けるということは $\mathbb{Q}(a_1, \ldots, a_{n-1}, a_n)$ という $a_1, \ldots, a_{n-1}, a_n$ の有理関数からなる体に適当な根号を追加したときに解の公式がその中に入るということを意味している．例えば，$n = 2$ のとき，$\mathbb{Q}(b, c)$ という体に $\sqrt{b^2 - 4c}$ を添加して，$\mathbb{Q}(b, c, \sqrt{b^2 - 4c})$ という体を考えると，

$$\frac{-b \pm \sqrt{b^2 - 4c}}{2} \in \mathbb{Q}(b, c, \sqrt{b^2 - 4c})$$

となる．それでは $x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = 0$ の根を $\alpha_1, \ldots, \alpha_n$ とし，$\mathbb{Q}(a_1, \ldots, a_{n-1}, a_n)$ に $\alpha_1, \ldots, \alpha_n$ を添加した体 $\mathbb{Q}(a_1, \ldots, a_{n-1}, a_n, \alpha_1, \ldots, \alpha_n)$ を考えよう．このとき，包含関係

$$\begin{array}{c} \mathbb{Q}(a_1, \ldots, a_{n-1}, a_n, \alpha_1, \ldots, \alpha_n) \\ \uparrow \\ \mathbb{Q}(a_1, \ldots, a_{n-1}, a_n) \end{array}$$

に対応する群の包含関係は n **次対称群** $\mathfrak{S}_n$ という群を用いて，

$$\begin{array}{c} \{\mathrm{id}\} \\ \downarrow \\ \mathfrak{S}_n \end{array}$$

で与えられることが知られている[*8]．一方で，$\mathbb{Q}(a_1, \ldots, a_{n-1}, a_n)$ に様々な根号を追加して得られる体を K とすると，

$$\begin{array}{c} K \\ \uparrow \\ \mathbb{Q}(a_1, \ldots, a_{n-1}, a_n) \end{array}$$

に対応する群 G，

$$\begin{array}{c} \{\mathrm{id}\} \\ \downarrow \\ G \end{array}$$

は**可解性**という群論的な性質を持つことが知られている．そこで，$\mathfrak{S}_n$ の可解性を調べてみると (これは完全に群論的な問題である)，$n \leq 4$ では可解，$n \geq 5$ では非可解であるということがわかる．これにより，n が 5 以上の場合には絶対に根号の追加では解の公式にたどりつけないということがわかるのである！

Galois 理論の古典的な応用としては例えば以下のようなものが良く知られている[*9]．

[*7] $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ は $\mathbb{Q}$ 上のベクトル空間として 4 次元であるが，これはやはり G_2 が 4 つの元からなるということに対応している．

[*8] $\mathfrak{S}$ はドイツ文字の S である．対称群は英語でSymmetric group であるということに由来している

[*9] 角の三等分問題と立方体倍積問題は円積問題と合わせてギリシャの三大作図不可能問題と呼ばれる．円積問題とは与えられた円の面積と同じ面積を持つ正方形の 1 辺を定規とコンパスだけで作図できるかという問題で，これも不可能であることが知られている．

- (角の三等分問題) 一般に与えられた角の三等分を定規とコンパスだけで作図することは不可能であることの証明.
- (立方体倍積問題) 与えられた立方体の体積の 2 倍の体積を持つ立方体の 1 辺を定規とコンパスだけで作図することは不可能であることの証明.
- (正 n 角形の作図問題) 正 n 角形が定規とコンパスだけで作図可能であるための必要十分条件は，n が $n = 2^k p_1 \cdots p_s (k \in \mathbb{Z}_{\geq 0}$, 各 p_i は $2^{m_i} + 1$ という形をした素数) と書けることであるということの証明.

これらは非常に古典的な応用であるが，Galois 理論自体は現在も数学における非常に重要な基礎理論となっている．

また，すでに見たように，群は対称性を数学的に記述する際に有効な道具となる．今では，代数方程式に関係する話ばかりでなく，ここには到底列挙できない程の応用範囲を持っている．例えば，平面図形や空間図形の回転，ルービックキューブの変形等は群を用いて表すことができる．15 パズルの可解性も群論を用いて考察することができる．他にも数学だけでなく，量子力学を含む物理においても群論は基本的な道具として用いられている．本講義を通して，このような群の基本性質を学んでいきたい．

1.2 群と部分群

それでは，群の厳密な定義について述べよう．1.1 節では，“合成で閉じている対称変換のなす集合” が群の例だと述べていた．群とは一般に良い性質を満たす何らかの二項演算 (例えば合成) が定まった集合として定義される．集合 G において，$g_1, g_2 \in G$ に対し，$g_1 \cdot g_2$ という新たな G の元を対応させる規則が定まっているとき，G に**二項演算**が定まっているという．これは，集合と写像の言葉を用いればある写像

$$\cdot \colon G \times G \to G, \quad (g_1, g_2) \mapsto g_1 \cdot g_2$$

が定まっているということと同じである[*10]．このように書いて『(g_1, g_2) を $g_1 \cdot g_2$ に対応させることで定まる写像 $\cdot \colon G \times G \to G$』と読む．写像による元の対応を表すときは『$\mapsto$』という矢印を用いるということも合わせて思い出しておこう．それでは群とそれに関連する概念の定義を始めよう．

定義 1.2

空でない集合 G にある写像

$$\cdot \colon G \times G \to G, \quad (g_1, g_2) \mapsto g_1 \cdot g_2$$

が与えられていて，以下の 3 条件を満たすとき，G を**群 (group)** であるという:

(I) 任意の $g_1, g_2, g_3 \in G$ に対して，$(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$ が成り立つ. (**結合法則**)
(II) ある $e \in G$ が存在して，任意の $g \in G$ に対し，$e \cdot g = g = g \cdot e$ が成り立つ.
(III) 任意の $g \in G$ に対して，ある $g' \in G$ が存在し，$g' \cdot g = e = g \cdot g'$ が成り立つ.

(II) の e を G の**単位元**と呼び，(III) の g' を G における g **の逆元**と呼ぶ．g の逆元は，g^{-1} と書かれることが多い．さらに，G の二項演算 $\cdot$ が

(IV) 任意の $g, h \in G$ に対し，$g \cdot h = h \cdot g$

を満たすとき，G を**可換群**又は**アーベル群 (abelian group)** という.
群 G に含まれる元の数を G の**位数 (order)** といい，$|G|$ や $\#G$ 等と書く．$|G|$ が有限のとき，G を**有限群**といい，$|G| = \infty$ のとき，G を**無限群**という.

[*10] **復習.** 集合 X, Y に対し，

$$X \times Y \coloneqq \{(x, y) \mid x \in X, y \in Y\}$$

である．この $\times$ は数の掛け算ではなくて集合の**直積**と呼ばれるものである.

定義 1.3

群 G の**部分群 (subgroup)** とは，群 G の空でない部分集合であって，G の二項演算によって群をなすものである．

例 1. 1.1 節にでてきた，$G_1 = \{\mathrm{id}_{\mathbb{C}}, \mathsf{c}\}$ や $G_2 = \{\mathrm{id}, \sigma, \tau, \sigma\circ\tau\}$ は二項演算を写像の合成として群をなす．結合法則は写像の合成で一般に成り立つ性質である．また，G_1 の単位元は $\mathrm{id}_{\mathbb{C}}$ であり，G_2 の単位元は id である．恒等写像を右や左から合成しても写像は変わらないからである．さらに，

$$\mathsf{c}\circ\mathsf{c} = \mathrm{id}_{\mathbb{C}},\ \sigma\circ\sigma = \mathrm{id},\ \tau\circ\tau = \mathrm{id},\ (\sigma\circ\tau)\circ(\sigma\circ\tau) = \mathrm{id}$$

となるので，これらは全て自分自身を逆元とする元である．つまり，

$$\mathsf{c}^{-1} = \mathsf{c},\ \sigma^{-1} = \sigma,\ \tau^{-1} = \tau,\ (\sigma\circ\tau)^{-1} = (\sigma\circ\tau)$$

である．さらに，計算法則 (1.2) より，G_1 は可換群であり，$\sigma\circ\tau = \tau\circ\sigma$ が成り立つことより，G_2 も可換群である．また，$|G_1| = 2, |G_2| = 4$ なので，G_1 は位数 2 の有限群，G_2 は位数 4 の有限群であるという．

1.1 節で考えたように，合成によって閉じる (群をなす)G_1 の部分集合は

$$\{\mathrm{id}\},\ G_1$$

で全てであり，合成によって閉じる (群をなす)G_2 の部分集合は

$$\{\mathrm{id}\},\ \{\mathrm{id}, \sigma\},\ \{\mathrm{id}, \tau\},\ \{\mathrm{id}, \sigma\circ\tau\},\ G_2$$

で全てである．これらが G_1, G_2 の部分群である．G_1 や G_2 自身も定義上は部分群であるということに注意しよう．一般に群 G において単位元のみからなる部分集合 $\{e\}$ と G 全体 G は部分群であり，これらは**自明な部分群**と呼ばれる．

なお，$\{\sigma, \tau\} \subset G_2$ という部分集合は，$\sigma\circ\tau \notin \{\sigma, \tau\}$ なので，これは合成では閉じていないため，二項演算がこの中で定義されているとは言えず，部分群ではない．

群の定義は一見抽象的過ぎてわかりにくいが，対称変換の抽象化であるという観点で見れば，

- (I) は g_3 という変換を行ってから g_2 と g_1 という変換を続けて行うという変換は，g_3 と g_2 という変換を続けて行ってから g_1 という変換を行うという変換と同じであるということ．
- (II) は “何もしない” という変換が対称変換であるということ．
- (III) は対称変換は逆変換が行えるということ．

の一般化であるとそれぞれ考えられる．

注意 1 (結合法則 (I) に関する注釈). 結合法則 (I) は二項演算を考える順番を変えても結果が変わらないということを意味している．例えば，$g_1, g_2, g_3, g_4 \in G$ に対し，$((g_1\cdot g_2)\cdot g_3)\cdot g_4$ と $(g_1\cdot(g_2\cdot(g_3\cdot g_4))$ は一致するということが以下のようにして結合法則を繰り返し使うことによってわかる．(逆に言えばこれは結合法則を仮定しているから示されることであって，“当たり前” ではないということに注意する).

$$\begin{aligned}((g_1\cdot g_2)\cdot g_3)\cdot g_4 &= (g_1\cdot g_2)\cdot(g_3\cdot g_4) \quad (\text{(I) で } g_1\text{を } g_1\cdot g_2,\ g_2\text{を } g_3,\ g_3\text{を } g_4\text{とした})\\ &= g_1\cdot(g_2\cdot(g_3\cdot g_4)) \quad (\text{(I) で } g_1\text{を } g_1,\ g_2\text{を } g_2,\ g_3\text{を } g_3\cdot g_4\text{とした})\end{aligned}$$

一般に，結合法則を繰り返し使えば，どのように括弧を付けても全て答えが一致することが示される．この証明は講義では扱わないが，興味のある方は腕試しとして是非チャレンジしてみて欲しい[*11]． これより，群 G における演算『$\cdot$』に対しては，以下では特に 2 つずつ括弧を付けないこともある．例えば，群 G において，

$$g_1\cdot g_2\cdots g_n$$

というような書き方をすることが多くある．また，一般の群を扱う際は $g_1\cdot g_2$ を単に省略して g_1g_2 等と書くこともある．

[*11] 演算『$\cdot$』の回数に関する帰納法を用いれば良いというのがヒントである．

以下は抽象的な群と部分群の基本性質である.

命題 1.4

群 G とその部分群 H において，以下が成立する.

(1) G の単位元 e はただ 1 つに定まる.
(2) 任意の $g \in G$ に対し，G における g の逆元 g' はただ 1 つに定まる.
(3) H の単位元は G の単位元に一致する.
(4) 任意の $h \in H$ に対し，H における h の逆元は G における h の逆元に一致する.

証明. (1) $e, e' \in G$ が G の単位元であったとすると，

$$\begin{aligned} e &= e \cdot e' && (e'\text{は単位元なので}) \\ &= e'. && (e\text{ は単位元なので}) \end{aligned}$$

よって，G の単位元 e はただ 1 つに定まる. □

(2) $g', g'' \in G$ が G における g の逆元であったとすると，

$$\begin{aligned} g' &= g' \cdot e && (e\text{ は単位元なので}) \\ &= g' \cdot (g \cdot g'') && (g''\text{は } g\text{ の逆元なので}) \\ &= (g' \cdot g) \cdot g'' && (\text{結合法則}) \\ &= e \cdot g'' && (g'\text{は } g\text{ の逆元なので}) \\ &= g''. && (e\text{ は単位元なので}) \end{aligned}$$

よって，G における g の逆元 g' はただ 1 つに定まる. □

(3) H の単位元を e_H，G の単位元を e_G，G における e_H の逆元を $e_H^{-1,G}$ と書くと，

$$\begin{aligned} e_H &= e_G \cdot e_H && (e_G\text{は } G\text{ の単位元なので}) \\ &= (e_H^{-1,G} \cdot e_H) \cdot e_H && (e_H^{-1,G}\text{は } G\text{ における } e_H\text{の逆元なので}) \\ &= e_H^{-1,G} \cdot (e_H \cdot e_H) && (\text{結合法則}) \\ &= e_H^{-1,G} \cdot e_H && (e_H\text{は } H\text{ の単位元なので}) \\ &= e_G. && (e_H^{-1,G}\text{は } G\text{ における } e_H\text{の逆元なので}) \end{aligned}$$

である. 特に，これは e_G が必ず部分群 H に含まれることも意味していることに注意する. □

(4) H における h の逆元を $h^{-1,H}$，G における h の逆元を $h^{-1,G}$ と書くと，

$$\begin{aligned} h^{-1,H} &= h^{-1,H} \cdot e && (e\text{ は } G\text{ の単位元なので}) \\ &= h^{-1,H} \cdot (h \cdot h^{-1,G}) && (h^{-1,G}\text{は } G\text{ における } h\text{ の逆元なので}) \\ &= (h^{-1,H} \cdot h) \cdot h^{-1,G} && (\text{結合法則}) \\ &= e \cdot h^{-1,G} && (h^{-1,H}\text{は } H\text{ における } h\text{ の逆元であり，(3) より } H\text{ の単位元も } e\text{ なので}) \\ &= h^{-1,G}. && (e\text{ は } G\text{ の単位元なので}) \end{aligned}$$

□

また，与えられた群の部分集合が部分群であるかどうかは以下の命題を用いて判定できる.

命題 1.5

群 G の部分集合H に対し，以下は同値である．

(1) H は G の部分群.
(2) H は空ではなく，H は二項演算と逆元をとる操作で閉じている．つまり，任意の $h, k \in H$ に対し，

$$h \cdot k \in H \quad \text{かつ} \quad h^{-1} \in H$$

となる．

証明. 群 G の部分集合 H が部分群であるとは，H が G の二項演算によって群をなすということであるが，これは以下のように書き下せる：

H は空ではなく，G の二項演算

$$\cdot : G \times G \to G, \quad (g_1, g_2) \mapsto g_1 \cdot g_2$$

の定義域を $H \times H$ に制限したとき，これが

$$\cdot : H \times H \to H$$

を与え，以下の 3 条件を満たす：

(i) 任意の $h_1, h_2, h_3 \in H$ に対して，$(h_1 \cdot h_2) \cdot h_3 = h_1 \cdot (h_2 \cdot h_3)$ が成り立つ.
(ii) ある $e_H \in H$ が存在して，任意の $h \in H$ に対し，$e_H \cdot h = h = h \cdot e_H$ が成り立つ.
(iii) 任意の $h \in H$ に対して，ある $h' \in H$ が存在し，$h' \cdot h = e_H = h \cdot h'$ が成り立つ.

この枠で囲んだ主張が (2) の主張と同値であることを示せばよい.

枠で囲んだ主張 $\Rightarrow$(2) :まず $\cdot$ が $\cdot : H \times H \to H$ を与えるということは，任意の $h, k \in H$ に対し，$h \cdot k \in H$ であるということを意味する．さらに，性質 (iii) より各 $h \in H$ に対して，H における h の逆元は H 内に存在するが，命題 1.4 (4) より，これは G における h の逆元 h^{-1} と一致するので，結局 $h^{-1} \in H$ である．よって，(2) の主張が成立する.

(2)$\Rightarrow$ 枠で囲んだ主張 :任意の $h, k \in H$ に対し，$h \cdot k \in H$ が成立することより，G の二項演算 $\cdot$ は確かに写像

$$\cdot : H \times H \to H, \ (h, k) \mapsto h \cdot k$$

を与える．さらに，この二項演算は G の二項演算を制限したものなので，(i) の性質は自明に成り立つ.

次に，$H \neq \emptyset$ より，任意に 1 つ元 $h \in H$ をとると，(2) の性質より $h^{-1} \in H$ であり，さらに，

$$H \ni h \cdot h^{-1} = e.$$

よって，H は G の単位元 e を含み，この元を e_H とすると確かに (ii) の条件を満たす.

(2) の性質より，$h \in H$ に対して，G における h の逆元 h^{-1} は H の元であるが，これは

$$hh^{-1} = e(= e_H) = h^{-1}h$$

を満たすので，H における逆元でもある．よって，(iii) の条件も満たされる． □

1.3 群と部分群の簡単な例

以下ではこれまでにすでに学習したものの中から，群と部分群の例となるものについて列挙する．なお，『$(G, \cdot)$』という書き方をした場合には，『集合 G に二項演算 $\cdot$ を考えたもの』という意味であると解釈する.

例 2 (加法群). $+$ を通常の和と考えたとき，$(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ は群である．これらは**加法群**とよばれる．群の二項演算の 3 性質は以下のように確かめられる ($\mathbb{X} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ とする)：

(I) (結合法則) 任意の $a,b,c \in \mathbb{X}$ に対し，$(a+b)+c = a+(b+c)$.
(II) (単位元の存在) 単位元は $0 \in \mathbb{X}$ である．実際，任意の $a \in \mathbb{X}$ に対し，$0+a = a = a+0$ が成立する．
(III) (逆元の存在) 任意の $a \in \mathbb{X}$ に対し，$-a \in \mathbb{X}$ であって，$(-a)+a = 0 = a+(-a)$ が成立する．

さらに，加法 $+$ は

(IV) 任意の $a,b \in \mathbb{X}$ に対し，$a+b = b+a$

をみたすので，これらは可換群である．いずれも集合に含まれる元の個数は無限なので，無限群である．また，$(\mathbb{C},+) \supset (\mathbb{R},+) \supset (\mathbb{Q},+) \supset (\mathbb{Z},+)$ であり，小さいものは大きいものの部分群である．

さらに，$n \in \mathbb{Z}_{>0}$ に対し，

$$n\mathbb{Z} \coloneqq \{nm \mid m \in \mathbb{Z}\} \ (n \text{ の倍数全体})$$

とすると，$(n\mathbb{Z},+)$ は $(\mathbb{Z},+)$ の部分群である．実際，任意の $nm_1, nm_2 \in n\mathbb{Z}$ に対し，

$$nm_1 + nm_2 = n(m_1+m_2) \in n\mathbb{Z}, \qquad -nm_1 = n(-m_1) \in n\mathbb{Z}$$

となるので，命題 1.5 より，部分群であることがわかる．

一方，二項演算として引き算 $-$ を考えると，$(\mathbb{X},-)$ は群にはならない！なぜなら，一般に $a,b,c \in \mathbb{X}$ に対して，

$$(a-b)-c = a-b-c \neq a-b+c = a-(b-c)$$

となり，結合法則が成り立たないためである．

また，$(\mathbb{N},+)$ も群にはならない！これは，$a \in \mathbb{N}$ が 0 でないとき，

$$a+a' = 0$$

を満たす a' は $-a$ であるが，$-a \notin \mathbb{N}$ であるため，逆元の存在 (III) を満たさないのである．

例 3 (乗法群).

$$\mathbb{Q}^\times \coloneqq \mathbb{Q} \setminus \{0\} \qquad \mathbb{R}^\times \coloneqq \mathbb{R} \setminus \{0\} \qquad \mathbb{C}^\times \coloneqq \mathbb{C} \setminus \{0\}.$$

とする．ここで $\times$ を通常の掛け算 (乗法) と考えたとき，$(\mathbb{Q}^\times,\times), (\mathbb{R}^\times,\times), (\mathbb{C}^\times,\times)$ は群である．これらは**乗法群**とよばれる．群の二項演算の 3 性質は以下のように確かめられる ($\mathbb{K}^\times = \mathbb{Q}^\times, \mathbb{R}^\times, \mathbb{C}^\times$ とする)：

(I) (結合法則) 任意の $a,b,c \in \mathbb{K}^\times$ に対し，$(a \times b) \times c = a \times (b \times c)$.
(II) (単位元の存在) 単位元は $1 \in \mathbb{K}^\times$ である．実際，任意の $a \in \mathbb{K}^\times$ に対し，$1 \times a = a = a \times 1$ が成立する．
(III) (逆元の存在) 任意の $a \in \mathbb{K}^\times$ に対し，$a^{-1} \in \mathbb{K}^\times$ であって，$a^{-1} \times a = 1 = a \times a^{-1}$ が成立する．

ここで，逆元の存在を保証するために，0 を除いたということに注意しよう (0^{-1} は考えられない).

さらに，乗法 $\times$ は

(IV) 任意の $a,b \in \mathbb{K}^\times$ に対し，$a \times b = b \times a$

をみたすので，これらは可換群である．いずれも集合に含まれる元の個数は無限なので，無限群である．また，$(\mathbb{C}^\times,\times) \supset (\mathbb{R}^\times,\times) \supset (\mathbb{Q}^\times,\times)$ であり，小さいものは大きいものの部分群である．

さらに，

$$\mathbb{K}^\times_{>0} \coloneqq \{a \in \mathbb{K}^\times \mid a > 0\}$$

とすると，$\mathbb{K}^\times_{>0}$ は $\mathbb{K}^\times$ の部分群である。これは，正の数の積は再び正の数であり，正の数の逆数は再び正の数であることから，命題 1.5 よりわかる．

なお，二項演算として割り算 $\div$ を考えると，$(\mathbb{K}^\times,\div)$ は群にはならない！なぜなら，一般に $a,b,c \in \mathbb{K}^\times$ に対して，

$$(a \div b) \div c = \frac{\frac{a}{b}}{c} = \frac{a}{bc} \neq \frac{ac}{b} = \frac{a}{\frac{b}{c}} = a \div (b \div c)$$

となり，結合法則が成り立たないためである．

また，$(\mathbb{Z}\setminus\{0\},\times)$ も群にはならない！これは，$a\in\mathbb{Z}\setminus\{0\}$ が ±1 でないとき，

$$a\times a'=1$$

を満たす a' は $\frac{1}{a}$ であるが，$\frac{1}{a}\notin\mathbb{Z}\setminus\{0\}$ であるため，逆元の存在 (III) を満たさないのである．一方，$\{1,-1\}$ という 2 つだけの元からなる集合を考えると，$(\{1,-1\},\times)$ は群をなす．実際積を全通り考えると，

$$1\times1=1\qquad(-1)\times1=-1\qquad1\times(-1)=-1\qquad(-1)\times(-1)=1$$

となり，確かに $\{1,-1\}$ は積で閉じていて，しかも 1 の逆元は 1，-1 の逆元は -1 となるため，逆元をとる操作でも閉じている．よって，命題 1.5 より，$\{1,-1\}$ は $(\mathbb{K}^\times,\times)$ の部分群である．

注意 2. 集合としては $\mathbb{K}^\times\subset\mathbb{K}$ であるが，$(\mathbb{K}^\times,\times)$ は $(\mathbb{K},+)$ の部分群ではない！$(\mathbb{K}=\mathbb{Q},\mathbb{R},\mathbb{C})$ これは，$(\mathbb{K}^\times,\times)$ と $(\mathbb{K},+)$ で考えている二項演算が異なるため，部分群の定義 1.3 の，『G の二項演算によって』という部分を満たしていないのである．

例 4 (ベクトル空間)**.** ベクトル空間も加法 $+$ に関して群をなす．念のためベクトル空間の定義を復習しておこう．

復習

$\mathbb{K}$ を $\mathbb{Q},\mathbb{R}$ または $\mathbb{C}$ とする．$(V,+,\cdot\,)$ が $\mathbb{K}$ **上のベクトル空間**であるとは，これが以下のような 3 つ組であることである：

- V は空でない集合，
- $+$ は写像 $+\colon V\times V\to V,\ (\boldsymbol{u},\boldsymbol{v})\mapsto\boldsymbol{u}+\boldsymbol{v}$,
- $\cdot$ は写像 $\cdot\colon\mathbb{K}\times V\to V,\ (c,\boldsymbol{v})\mapsto c\boldsymbol{v}$

であって，以下が成立する：

(v1) 任意の $\boldsymbol{u},\boldsymbol{v}\in V$ に対し，$\boldsymbol{u}+\boldsymbol{v}=\boldsymbol{v}+\boldsymbol{u}$,
(v2) 任意の $\boldsymbol{u},\boldsymbol{v},\boldsymbol{w}\in V$ に対し，$(\boldsymbol{u}+\boldsymbol{v})+\boldsymbol{w}=\boldsymbol{u}+(\boldsymbol{v}+\boldsymbol{w})$,
(v3) ある元 $\boldsymbol{0}\in V$ が存在して，任意の $\boldsymbol{u}\in V$ に対し，$\boldsymbol{u}+\boldsymbol{0}=\boldsymbol{u}$，(この $\boldsymbol{0}$ を**零ベクトル**という)
(v4) 任意の $\boldsymbol{v}\in V$ に対して，ある元 $-\boldsymbol{v}\in V$ が存在して，$\boldsymbol{v}+(-\boldsymbol{v})=\boldsymbol{0}$，(この $-\boldsymbol{v}$ を $\boldsymbol{v}$ **の逆元**という)
(v5) 任意の $c,d\in\mathbb{K},\boldsymbol{v}\in V$ に対し，$(c+d)\boldsymbol{v}=c\boldsymbol{v}+d\boldsymbol{v}$,
(v6) 任意の $c\in\mathbb{K},\boldsymbol{u},\boldsymbol{v}\in V$ に対し，$c(\boldsymbol{u}+\boldsymbol{v})=c\boldsymbol{u}+c\boldsymbol{v}$,
(v7) 任意の $c,d\in\mathbb{K},\boldsymbol{v}\in V$ に対し，$(cd)\boldsymbol{v}=c(d\boldsymbol{v})$,
(v8) 任意の $\boldsymbol{v}\in V$ に対し，$1\boldsymbol{v}=\boldsymbol{v}$.

このとき，確かに $+$ は V における二項演算となっており，(v2) が結合法則，(v3) が単位元 $\boldsymbol{0}$ の存在 ((v1) より，$\boldsymbol{0}+\boldsymbol{u}=\boldsymbol{u}$ も成立する)，(v4) が各元 $\boldsymbol{v}\in V$ の逆元 $-\boldsymbol{v}$ の存在 ((v1) より，$(-\boldsymbol{v})+\boldsymbol{v}=\boldsymbol{0}$ も成立する) に対応する．(v1) より，これは可換群である．ベクトル空間は可換群 $(V,+)$ にスカラー倍 $\cdot$ の構造を加えたものであると言うことができる．

例 5 (一般線型群，特殊線型群)**.** n を正の整数とし，$\mathbb{K}$ を $\mathbb{Q},\mathbb{R}$ または $\mathbb{C}$ とする．

$$GL_n(\mathbb{K}):=\{A\mid A\text{ は }\mathbb{K}\text{ の元を成分とする }n\times n\text{ 行列で, }\det A\neq0\}.$$

ただし，$\det A$ は A の行列式である．このとき，$GL_n(\mathbb{K})$ は行列の積に関して群をなす．これを**一般線型群 (general linear group)** という．ここで，$n\times n$ 行列 A,B に対し，

$$\det(AB)=\det A\cdot\det B$$

であったので，$GL_n(\mathbb{K})$ は行列の積に関して閉じているということに注意しよう．群の二項演算の 3 性質は以下のように確かめられる：

(I) (結合法則) 任意の $A, B, C \in GL_n(\mathbb{K})$ に対し，$(AB)C = A(BC)$．(行列の積の性質)

(II) (単位元の存在) 単位元は単位行列 $I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$ である．実際，任意の $A \in GL_n(\mathbb{K})$ に対し，$I_n A = A = A I_n$ が成立する．

(III) (逆元の存在) 任意の $A \in GL_n(\mathbb{K})$ に対し，$\det A \neq 0$ より，逆行列 $A^{-1} \in GL_n(\mathbb{K})$ が存在する．逆行列は $A^{-1}A = I_n = AA^{-1}$ を満たすので，群論の意味での逆元となっている．

逆元の存在を保証するために，$\det A \neq 0$ を満たす行列のなす集合を考えている．また，$n \geq 2$ のとき，行列の積は一般に $AB = BA$ とはならないので，$GL_n(\mathbb{K})$ は非可換群である．さらに，

$$SL_n(\mathbb{K}) \coloneqq \{A \in GL_n(\mathbb{K}) | \det A = 1\}$$

とすると，$SL_n(\mathbb{K})$ は $GL_n(\mathbb{K})$ の部分群であり，**特殊線型群 (special linear group)** と呼ばれる．これは以下のように証明される．

証明. $I_n \in SL_n(\mathbb{K})$ より，$SL_n(\mathbb{K})$ は空ではない．任意の $A, B \in SL_n(\mathbb{K})$ に対し，

$$\det(AB) = \det(A) \cdot \det(B) = 1 \cdot 1 = 1 \qquad \det(A^{-1}) = \det(A)^{-1} = 1^{-1} = 1$$

より，$AB \in SL_n(\mathbb{K})$ かつ $A^{-1} \in SL_n(\mathbb{K})$ である．よって，命題 1.5 より，$SL_n(\mathbb{K})$ は $GL_n(\mathbb{K})$ の部分群である． □

注意 3 (**群の定義補足 (興味のある方向け)**)．群の定義で (II) や (III) にある等式を『$g = g \cdot e$』のみ，『$g' \cdot g = e$』のみというようにさぼってはいけない．例えば，2×2 行列のなす集合

$$G' \coloneqq \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \middle| a \in \mathbb{C}^\times, b \in \mathbb{C} \right\}$$

を考える．すると，

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \begin{pmatrix} a' & 0 \\ b' & 0 \end{pmatrix} = \begin{pmatrix} aa' & 0 \\ ba' & 0 \end{pmatrix}$$

より，G' には行列の積から定まる二項演算が定まっている (結合法則 (I) を満たす)．

さらに，$e \coloneqq \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in G'$ と定めると，任意の $g = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \in G'$ に対し，

$$ge = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = g$$

が成立する．さらに，任意の $g = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \in G'$ に対し，$g' = \begin{pmatrix} a^{-1} & 0 \\ 0 & 0 \end{pmatrix} \in G'$ とすると，

$$g'g = \begin{pmatrix} a^{-1} & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = e$$

となる．これより，G' は群の性質のうち二項演算の存在，(I)，(II) の一部 (『$g = g \cdot e$』のみにしたもの)，(III) の一部 (『$g' \cdot g = e$』のみにしたもの) を満たすが，G' は群ではない．実際，G' が群であるなら単位元の存在から，任意の $g = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \in G'$ に対し，$e'g = g$ を満たす $e' = \begin{pmatrix} e_1 & 0 \\ e_2 & 0 \end{pmatrix} \in G'$ が存在するはずである．しかし，このとき

$$e'g = \begin{pmatrix} e_1 & 0 \\ e_2 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} e_1 a & 0 \\ e_2 a & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = g$$

なので，特に $e_2 a = b$ が任意の $a \in \mathbb{C}^\times$、$b \in \mathbb{C}$ に対して成り立つことになるが，そのような定数 e_2 は存在せず，矛盾する．