# 群の基本

## 1 導入

この講義の核心は、**群とは「演算の規則だけ」を抜き出した最小の代数構造であり、整数の加法・mod 演算・回転・置換がすべて同じ公理を満たす例であるという見方だ。**

「群の公理はなぜこの 4 つか」という問いに答えることが、群論の入口での最重要課題である。閉包性・結合法則・単位元・逆元の各公理は、「演算を繰り返しても世界の外へ出ず、元へ戻せる」という直感を最小限の言葉で表したものだ。

## 2 用語と定義

### 2.1 群 Group

集合 $G$ と二項演算 $*$ の組 $(G, *)$ が群 Group であるとは、以下の 4 公理が成立することである：

1. **閉包性**：$a, b \in G \Longrightarrow a * b \in G$
2. **結合法則**：$(a * b) * c = a * (b * c)$
3. **単位元の存在**：$e \in G$ が存在し $e * a = a * e = a$（すべての $a \in G$ に対して）
4. **逆元の存在**：各 $a \in G$ に対し $a * a^{-1} = a^{-1} * a = e$ となる $a^{-1} \in G$ が存在する

さらに $a * b = b * a$（可換）が成り立つとき可換群 Abelian group（またはアーベル群）という。

### 2.2 位数 Order

群 $G$ の要素の個数 $|G|$ を $G$ の位数 Order という。有限の位数を持つ群を有限群 Finite group という。元 $a \in G$ の位数とは $a^n = e$ となる最小の正整数 $n$（存在しない場合は $\infty$）をいう。

## 3 方針

1. 4 公理それぞれが「なぜ必要か」を具体例で確認する
2. 複数の群（$\mathbb{Z}$、$\mathbb{Z}/n\mathbb{Z}$、$S_n$、$GL(n, \mathbb{R})$）を比較し、共通構造を認識する
3. 部分群・準同型への橋渡しを確認する

## 4 厳密な説明

### 4.1 1. なぜこの 4 公理なのか

**閉包性が必要な理由**：演算の結果が $G$ の外へ出ると、その値に対してさらに演算することができなくなる。

$G = \{1, -1\}$ と掛け算はこれを満たすが、$G = \{1\}$ と足し算は $1 + 1 = 2 \notin G$ のため成立しない。

**結合法則が必要な理由**：$a*b*c$ の計算順序が括弧の位置に依存しないことを保証する。これがないと $n$ 個の元の積が一意に定まらない。
**単位元が必要な理由**：「何もしない操作」の代表。$a^0=e$、$a^{-n}=(a^{-1})^n$ などが意味を持つ。
**逆元が必要な理由**：方程式 $a*x=b$ が $G$ の中で解 $x=a^{-1}*b$ を持つことを保証する。逆元がなければ「取り消し」ができない。

## 4.2 2. 主要な群の一覧

| 群 | 台集合 | 演算 | 位数 | 可換 |
|---|---|---|---|---|
| $(\mathbb{Z},+)$ | 整数 | 加法 | $\infty$ | ○ |
| $(\mathbb{Z}/n\mathbb{Z},+)$ | $\{[0],\dots,[n-1]\}$ | $\bmod n$ 加法 | $n$ | ○ |
| $(\mathbb{Z}/p\mathbb{Z})^\times$ | $\{[1],\dots,[p-1]\}$ | $\bmod p$ 乗法 | $p-1$ | ○ |
| $S_n$（対称群） | $\{1,\dots,n\}$ の置換 | 写像の合成 | $n!$ | $n\geq 3$ で× |
| $GL(n,\mathbb{R})$ | $n$ 次可逆行列 | 行列積 | $\infty$ | $n\geq 2$ で× |
| $D_n$（二面体群） | 正 $n$ 角形の 対称 | 合成 | $2n$ | $n\geq 3$ で× |

**$(\mathbb{Z}/p\mathbb{Z})^\times$ の解説**：$p$ が素数のとき $\gcd(a,p)=1$ な $[a]$ はすべて逆元を持ち（フェルマーの小定理）、この集合は乗法について位数 $p-1$ の群をなす。

## 4.3 3. 部分群

$H\subseteq G$ が部分群（Subgroup）であるとは：

$$H\neq\emptyset,\quad a,b\in H\Longrightarrow ab\in H,\quad a\in H\Longrightarrow a^{-1}\in H$$

**判定条件**（一行判定）：$H\neq\emptyset$ かつ $a,b\in H\Longrightarrow ab^{-1}\in H$ ならば $H$ は部分群。
**例**：$2\mathbb{Z}=\{2k\mid k\in\mathbb{Z}\}$（偶数全体）は $(\mathbb{Z},+)$ の部分群。
**ラグランジュの定理**：$G$ が有限群で $H$ が部分群のとき $|H|$ は $|G|$ を割り切る。

## 4.4 4. 巡回群と位数

$G$ の元 $a$ が生成する部分群 $\langle a\rangle=\{a^n\mid n\in\mathbb{Z}\}$ を巡回群（Cyclic group）という。元 $a$ の位数が $m$ のとき $|\langle a\rangle|=m$。
**例**：$\mathbb{Z}/6\mathbb{Z}$ では $[1]$ の位数は 6、$[2]$ の位数は 3（$[2]+[2]+[2]=[6]=[0]$）、$[3]$ の位数は 2。

## 4.5 5. 群準同型

写像 $\varphi:G\to H$ が

$$\varphi(a*b)=\varphi(a)\cdot\varphi(b)$$

を満たすとき群準同型（Group homomorphism）という。準同型は単位元を単位元へ、逆元を逆元へ送る。全単射準同型を群同型（Isomorphism）といい、$G\cong H$ と書く。
**ケイリーの定理**：任意の群 $G$ はある対称群 $S_{|G|}$ の部分群と同型である—群は常に「置換の群」として実現できる。

### 4.6 6. 群の現れる場面

- **整数論**：$(\mathbb{Z}/p\mathbb{Z})^\times$ はフェルマーの小定理・RSA暗号の基盤
- **幾何**：回転の群 $SO(n)$、対称の群（結晶群）
- **物理**：リー群（$SU(2), U(1)$）による素粒子の分類
- **方程式論**：ガロア群が方程式の根号による解の存在を決める

## 5 見分け方

- 演算を何度でも繰り返せ、元へ戻す操作が存在する → 群を疑う
- 集合が有限で演算が閉じている → 位数を計算し、部分群の候補をラグランジュの定理で絞る
- 構造が等しいか調べたい → 準同型の核と像を調べる

## 6 どこまで成り立つか

ここでの群は最小の構造で、演算が 1 種類しかない。足し算と掛け算の両方を持ち、それらが分配法則で結びついた構造が環・体である。連続な群（微分可能な多様体の構造を持つ群）はリー群と呼ばれ、現代物理の基盤をなす。

## 7 最終形

$$\boxed{(G,*)\text{ が[群/ぐん]} \iff \text{[閉包/へいほう]・[結合/けつごう]・[単位元/たんいげん]・[逆元/ぎゃくげん]}}$$

$$\boxed{|\,H\,|\,|\,G\,| \quad (\text{ラグランジュ}, H \le G, |\,G\,| < \infty)}$$

$$\boxed{\varphi(ab)=\varphi(a)\varphi(b) \Longrightarrow \varphi(e_G)=e_H,\ \varphi(a^{-1})=\varphi(a)^{-1}}$$

## 8 一言でいうと

群とは「演算の規則だけ」を抜き出した最小の代数構造であり、整数・置換・行列・回転のすべてを統一する枠組みだ—ラグランジュの定理が有限群の構造を 強力 に制約し、ケイリーの定理がすべての群を「置換の群」として見る視点を与える。

## 9 関連リンク

→ 講義 **合同式と mod 演算の基本** lecture math abstract-algebra
https://study.bem130.com/lecture/math/abstract-algebra/合同式と mod 演算の基本-講義/

→ 講義 **環の基本** lecture math abstract-algebra
https://study.bem130.com/lecture/math/abstract-algebra/環の基本-講義/

→ 講義 **準同型の基本** lecture math abstract-algebra
https://study.bem130.com/lecture/math/abstract-algebra/準同型の基本-講義/