

群論

武井優己

2019 年 6 月 22 日

1 はじめに

本レポートでは、写像の定義や命題を多用するため、写像に関する知識に自身が無い場合は、写像のレポート: <https://github.com/noppoMan/math-report/blob/master/map/map.pdf> を読んでから、本レポートを読み進めることを推奨する。

2 群の定義と例

2.1 群の定義

G が集合であるとき、写像 $f: G \times G \rightarrow G$ のことを集合 G 上の演算という。

この写像は、集合 G のふたつの元を関数 \times に入れると、 G の元が一つ返ってくるということを言っており、この \times による演算を二項演算とも呼ぶ。この写像は二項演算に関して閉じている。

※ 二項演算が閉じているとは、集合 G の演算 \circ に関して、 $x, y \in G$ のとき、 $x \circ y \in G$ である。

定義 2.1 G を空でない集合とする。 G 上の演算が定義されていて以下の性質を満たすとき、 G を群という。

- (1) 結合法則を満たす。全ての $a, b, c \in G$ に対し、 $(ab)c = a(bc)$ が成り立つ
- (2) 単位元が存在する。単位元とは、 $e \in G$ があり、すべての $a \in G$ に対して、 $ea = ae = a$ となる。
- (3) 逆元が存在する。逆元とは、すべての $a \in G$ に対し、 $ab = ba = e$ となるような $b \in G$ のことであり、 a^{-1} と表す。言い換えると、 x に対して演算すると単位元を得ることの出来る元のこと。

群 G の任意の元 a, b が可換 ($ab = ba$) であれば、 G を可換群 (アーベル群) と言う。また、可換群でない群を非可換群と言う。

定義 2.2 G が群であるとき、その元の個数 $|G|$ を G の位数という。位数が有限な群を有限群、有限でない群を無限群という。

例 2.3 $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ は加法により群である。また可換群でもある。単位元は 0 であり、元 x の逆元は $x^{-1} = -x$ となる。

例 2.4 $\mathbb{Z}^{\times}, \mathbb{Q}^{\times}, \mathbb{R}^{\times}$ は乗法により、可換群となる。単位元は 1 、元 x の逆元は $x^{-1} = \frac{1}{x}$ である。

例 2.5 \mathbb{Z} は乗法により群にならない。単位元は 1 であるが、 $x, x^{-1} \in \mathbb{Z}$ に対して、 $xx^{-1} = 1$ となるような

x^{-1} が \mathbb{Z} に存在しない。

命題 2.6 G を群とするととき以下の性質が言える。

- (1) 群の単位元は一意に決まる
- (2) $a \in G$ に対して、その逆元は一意に決まる
- (3) $a, b' \in G$ なら、 $(ab)^{-1} = b^{-1}a^{-1}$
- (4) $a \in G$ なら、 $(a^{-1})^{-1} = a$

証明

- (1) G の単位元を e, e' とおく。任意の $a \in G$ に対して、 $ea = ae = a$ である。 $a = e'$ とおくと、 $ee' = e'e = e'$ であり、 $a = e$ とおくと、 $e'e = ee' = e$ より、 $e = e'$ となり、単位元は 1 つである。
- (2) b, c が a の逆元であれば、 $b = (ca)b = c(ab) = c$
- (3) 結合法則を使えば明らか。 $(b^{-1}a^{-1})ab = b^{-1}(a^{-1}a)b = b^{-1}b = e$ 。同様に、 $ab(b^{-1}a^{-1}) = e$ 。これより、 $b^{-1}a^{-1}$ は ab の逆元である。
- (4) $aa^{-1} = a^{-1}a = e$ より、 $a = (a^{-1})^{-1}$

2.2 部分群

G を群、 $H \subset G$ とする。 H が G の演算により群となるときの、 H を G の部分群という。

命題 2.7 $H \subset G$ が G の部分群になるための必要十分条件は、次の 3 つの条件が満たされることである。

- (1) $1_G \in H$
- (2) $x, y \in H$ ならば、 $xy \in H$
- (3) $x \in H$ ならば、 $x^{-1} \in H$

証明

- (1) H を部分群とする。 G の演算により、 $1_H 1_H = 1_H$ が成り立つ。 1_H^{-1} を両辺に対し左からかけて、 $1_H = 1_G$ となる。 $(1_H^{-1} 1_H 1_H = 1_H, 1_H 1_H^{-1} = 1_G$ より) これより、 $1_G \in H$ 。
- (2) H が G の部分群であれば、二項演算が閉じていることより明らか。 $(H$ が G の演算により閉じている)
- (3) $x \in H$ に対して、 x の逆元を $y \in H$ とする。 G の演算により、 $xy = yx = 1_H = 1_G$ となる。これより、 $y = x^{-1}$ となり、 $x^{-1} \in H$ 。

命題 2.8 G が群で、 $H_1, H_2 \subset G$ が G の部分群 $\Rightarrow H_1 \cap H_2$ も G の部分群

例 2.9 自明な部分群

G が群なら、 $\{1\}, G$ は G の部分群であるのは明らか。これらを G の自明な部分群という。

例 2.10 \mathbb{Z} を加法により群とする。 $n \in \mathbb{Z}$ のとき、 $n\mathbb{Z} := \{nx | x \in \mathbb{Z}\}$ とする。このとき、 $n\mathbb{Z}$ は \mathbb{Z} の部分群である。

証明

命題 2.7 を使い証明する。

- (1) \mathbb{Z} は加法により群だから、単位元は 0 。 $n0 = 0 \in \mathbb{Z}$ より、 $1_{\mathbb{Z}} \in n\mathbb{Z}$ が成り立つ。
- (2) $n\mathbb{Z}$ の元は、 $nx, ny (x, y \in \mathbb{Z})$ となっている。これより、 $nx + ny = n(x + y) \in \mathbb{Z}$ となる。
- (3) $nx \in n\mathbb{Z}$ の逆元を $-nx = n(-x) \in \mathbb{Z}$ である。 $nx + (-nx) = 1_{\mathbb{Z}} = 1_{n\mathbb{Z}} = 0$ より、 $-nx = nx^{-1} \in n\mathbb{Z}$ 。

問 2.11 $H = \{1, -1\} \in \mathbb{R}^x$ とする。 H が \mathbb{R}^x の部分群であることを、命題 2.7 を使って示せ。

2.3 群の生成

定義 2.12 群 G の部分集合 S に対して、 S を含む G の部分群のうち最小のものを $\langle S \rangle$ で表す。この $\langle S \rangle$ のことを、 S によって生成された部分群、 S のことを生成系、 S の元を生成元という。 ($S = \{s\}$ なら、 s が $\langle S \rangle$ の生成元である。)

$S = \{s_1, \dots, s_n\}$ なら、 $\langle \{s_1, \dots, s_n\} \rangle$ を $\langle s_1, \dots, s_n \rangle$ とも書く。

例 2.13 定義を噛み砕いた群の生成例

G を群、 $S = \{x\} \subset G$ とする。まだこの S は部分群の必要十分条件である、命題 2.7 を満たしておらず、部分群とは言えない。この S を部分群にしていく作業が生成である。

まず、逆元を加える。 x の逆元が $y \in G$ であれば、これを S に加え、 $S = \{x, y\}$ となる。これより、命題 2.7 の (3) は満たされたが、 $xy = 1_H = 1_G$ となるような 1_H が S に含まれていないため、二項演算が閉じていない。

これより、 S に 1_G を加えて、 $S = \{x, y, 1_G\}$ となり、 G の最小の部分群となる $\langle S \rangle$ を生成できた。

例 2.14 整数における群の生成

\mathbb{G} を群として、その部分集合を H とする。例 2.13 より

- (1) 逆元を加える
- (2) 各元を有限回演算して得られた元を加える

を繰り返し行うことで、群が生成できた。

これらを使い、整数全体の集合 \mathbb{Z} から最小の部分群 $\langle S \rangle$ を生成する。

\mathbb{Z} は加法に関して群、 $S = \{6, 9\} \subset \mathbb{Z}$ とする。 $6, 9$ の逆元はそれぞれ $-6, -9$ より、これらを S に加え $S_1 = \{-9, -6, 6, 9\}$ とする。

ここで、まだ S_1 には $6 - 6, 9 - 9$ の演算結果である単位元 0 が入っていないため、これを加え、 $S_2 = \{-9, -6, 0, 6, 9\}$ とする。

しかし、まだこの集合は二項演算が閉じていない。なぜなら、 $9 - 6 = 3$ やその逆元 -3 が入っていないためである。

このように、有限回この演算を繰り返し行うことで、 $S_n = \{\dots, -6, 0, 6, \dots\}$ という集合が生成され、この集合は命題 2.7 の (1)-(3) を満たすことにより、 \mathbb{Z} の最小の部分群 $\langle S \rangle$ となる。

2.3.1 巡回群

定義 2.15 一つの元で生成される群を巡回群という。または、集合 S が位数 n の巡回群であるとは、任意の $s \in S$ に対して、 $s^n = 1$ が言えることである。

※ TODO その他は線形代数後にまた詳しく

2.4 元の位数

定義 2.16 G を群、 $x \in G$ とする。 $x^n = 1_G$ となる正の整数が存在すれば、その中で最小なものを x の位数という。反対に、 $x^n = 1_G$ となる正の整数が存在しなければ、 x の位数は ∞ である。

例 2.17 G が群であれば、その単位元の位数は 1 となる。あるいは、 x の位数が 1 であるということは、 $x = x^1 = 1_G$ より、単位元 1_G は G 上で位数が 1 のただ一つの元と言える。

※ TODO その他は線形代数後にまた詳しく

3 準同型

二つの群 G_1, G_2 が与えられた時、 G_1, G_2 が本質的に同じかどうかということを定式化するために用いるのが準同型・同型という概念である。群は単なる集合ではなく、群における演算がその群の構造を決定する。そのため、二つの群を比較するときに集合として対応していることを調べるだけでは不十分であり、演算自体も対応していることを考えなければならない。

3.1 準同型と同型の定義

定義 3.1 G_1, G_2 を群とし、 $\phi: G_1 \rightarrow G_2$ を写像とする。

- (1) $\phi(xy) = \phi(x)\phi(y)$ がすべての $x, y \in G_1$ に対して成り立つ時、 ϕ を準同型という
- (2) ϕ が準同型で逆写像を持ち、逆写像も準同型であるなら、 ϕ を同型という
- (3) ϕ が準同型の時、 $\text{Ker}(\phi) = \{x \in G_1 | \phi(x) = 1_{G_2}\}$ を ϕ の核 (Kernel) という (言い換えると、 $\text{Ker}(\phi)$ は ϕ に入れると、 G_2 の単位元となる G_1 の元の集合である)
- (4) ϕ が準同型の時、 $\text{Im}(\phi) = \{\phi(x) | x \in G_1\}$ を ϕ の像 (Image) という

命題 3.2 全単射写像 $\phi: G_1 \rightarrow G_2$ が群の準同型なら、同型である。

証明

ϕ の逆写像を ψ とおく。 $x, y \in G_2$ とすると、 ϕ は準同型より、

$$\phi(\psi(x)\psi(y)) = \phi(\psi(x))\phi(\psi(y)) = xy = \phi(\psi(xy))$$

となる。 ϕ は単射より、 $\phi(x)\phi(y) = \phi(xy)$ 。これより、 ψ は準同型である。

命題 3.3 $\phi: G_1 \rightarrow G_2$ を群の準同型とする時、次の命題が成り立つ。

- (1) $\phi(1_{G_1}) = 1_{G_2}$ である。
- (2) 任意の $x \in G_1$ に対し、 $\phi(x^{-1}) = \phi(x)^{-1}$
- (3) $\text{Ker}(\phi)$ は G_1 の部分群である
- (4) $\text{Im}(\phi)$ は G_2 の部分群である

証明

- (1) $\phi(1G_1) = \phi(1G_1 1G_1) = \phi(1G_1)\phi(1G_1)$ なので、両辺に左から $\phi(1G_1)^{-1}$ をかけて、 $\phi(1G_1) = 1G_2$ ($\phi(1G_1)\phi(1G_1)\phi(1G_1)^{-1} = \phi(1G_1), \phi(1G_1)\phi(1G_1)^{-1} = 1G_2$ より)
- (2) $x \in G_1$ なら $1G_2 = \phi(1G_1) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1})$ より、 $\phi(x)(\phi(x))^{-1} = \phi(1G_1) = 1G_2$ となる。したがって、 $\phi(x^{-1}) = \phi(x)^{-1}$
- (3) $1G_1 \in \text{Ker}(\phi)$ と $1G \ni x^{-1} \in \text{Ker}(\phi)$ を示す。 $\text{Ker}(\phi)$ は行き先が $1G_2$ となる G_1 の元から構成されているため、 (1) より、 $1G_1 \in \text{Ker}(\phi)$ である。 $x, y \in \text{Ker}(\phi)$ なら $\phi(xy) = \phi(x)\phi(y) = 1G_2 1G_2 = 1G_2$ なので、 $xy \in \text{Ker}(\phi)$ である。 ϕ は準同型なので、 $\phi(x^{-1}) = \phi(x)^{-1} = 1G_2^{-1} = 1G_2$ より、 $x^{-1} \in \text{Ker}(\phi)$ である。したがって、 $\text{Ker}(\phi)$ は G_1 の部分群である。
- (4) $1G_1 \in \text{Im}(\phi)$ と $\phi(x)^{-1} \in \text{Im}(\phi)$ ($x \in \text{Im}(\phi)$) を示す。 $1G_2 = \phi(1G_1)$ なので、像の定義より、 $1G_2 \in \text{Im}(\phi)$ である。任意の $x, y \in G_1$ を取り、 $\phi(x)\phi(y) = \phi(xy)$ が準同型より言え、像の定義より、 $\phi(x), \phi(y), \phi(xy) \in G_2$ である。また、 $x^{-1} \in G_1$ より、 $\phi(x^{-1}) = \phi(x)^{-1}$ も同様に $\text{Im}(\phi)$ の元となる。したがって、 $\text{Im}(\phi)$ は G_2 の部分群である。

例 3.4 G を群、 $x \in G$ とする。 \mathbb{Z} を加法により群とし、写像 $\phi: \mathbb{Z} \rightarrow G$ を $\phi(n) = x^n$ と定義する。任意の $m, n \in \mathbb{Z}$ に対し、 $\phi(n+m) = x^{n+m} = x^n x^m = \phi(n)\phi(m)$ なので、 ϕ は準同型である。

例 3.5 $\mathbb{R}_{>0} = \{r \in \mathbb{R} | r > 0\}$ とおく。 $\mathbb{R}_{>0}$ を乗法により群、 \mathbb{R} を加法により群とする。写像 $\phi: \mathbb{R} \rightarrow \mathbb{R}_{>0}$ を $\phi(x) = e^x$ と定義する。 $x, y \in \mathbb{R}$ なら $\phi(x+y) = e^{x+y} = e^x \cdot e^y = \phi(x)\phi(y)$ なので、 ϕ は準同型である。指数関数は \mathbb{R} から $\mathbb{R}_{>0}$ への全単射より、 ϕ は同型である。(命題 3.2 より)

4 剰余類

4.1 同値関係の復習

まずは、剰余類の定義や証明に必要な同値関係や合同関係、同値類などに関して簡単に復習する。

4.1.1 同値関係

集合 S 上の関係 \sim が次の条件を満たすとき、同値関係と呼ぶ。

定義 4.1 同値関係

- (1) 反射律: $a \sim a$
- (2) 対称律: $a \sim b$ ならば $b \sim a$
- (3) 推移律: $a \sim b, b \sim c$ なら $a \sim c$

例 4.2 集合 S があり、 $x, y \in S$ のとき、 $x = y$ (等号) は同値関係である。

例 4.3 $x, y \in \mathbb{Z}$ における通常の不等号、 $x \leq y$ は、 $0 \leq 1$ ではあるが、 $1 \leq 0$ とはならず、対称律を満たさないため、同値関係ではない。

4.1.2 合同関係

合同とは、ある正の整数 p を法として、 $x, y \in \mathbb{Z}$ を p で割ったときの剰余 (余り) が等しいときの x と y の関係を言い、 $x \equiv y \pmod{p}$ と書く。

あるいは、正の整数 p を固定する。 $x, y \in \mathbb{Z}$ に対し、 $x - y$ が p で割り切れる時も x と y は同値関係にあり、 $x \equiv y \pmod{p}$ と書く。

例 4.4 7 と 1 は 3 を法として、合同である。 $7 \equiv 1 \pmod{3}$

$7 - 1$ が 3 で割り切れることも確認できる。

例 4.5 29 と 15 は 7 を法として、合同である。 $29 \equiv 15 \pmod{7}$

$29 - 15$ が 7 で割り切れることも確認できる。

命題 4.6 合同関係は同値関係である。

証明

正の整数 p を固定し、 $x, y \in \mathbb{Z}$ とする。 $x - y$ が p で割り切れれば、 $y - x$ も p で割り切れることより、 $x \equiv y \pmod{p}$ なら、 $y \equiv x \pmod{p}$ である。これより、対称律を満たす。また、 $x \equiv x \pmod{p}$ は明らかなので、反射律を満たす。 $x, y, z \in \mathbb{Z}$ で、 $x \equiv y \pmod{p}$, $y \equiv z \pmod{p}$ であるなら、 $x - y = ap$, $y - z = bp$ となるような $a, b \in \mathbb{Z}$ があるので、 $x - z = (x - y) + (y - z) = (a + b)p$ も p で割り切れる。よって、 $x \equiv z \pmod{p}$ より、推移律を満たす。これらより、合同関係は同値関係である。

4.1.3 同値類

定義 4.7 \sim を集合 S 上の同値関係とする。 $x \in S$ に対し、 $C(x) = \{y \in S \mid y \sim x\}$ を x の同値類という。

命題 4.8 集合 S 上の同値関係、 $C(X)$ を $x \in S$ の同値類とすると、以下の命題が成り立つ。

- (1) 任意の $y, z \in C(X)$ に対し、 $y \sim z$
- (2) もし $y \in C(x)$ なら $C(x) = C(y)$ である。
- (3) もし $x, y \in S$ で $C(x) \cap C(y) \neq \emptyset$ なら $C(x) = C(y)$ である。

証明

- (1) 同値類は同値関係を満たしているので明らか。 $z \sim x$ なので、 $x \sim z$ である。 $y \sim x$ でもあるので、推移律より $y \sim z$ となる。
- (2) $y \in C(x)$ とする。(1) より、 $x \sim z$ なら、 $y \sim x$ であり、 $y \sim z$ となるので、 $C(x) \subset C(y)$ である。ここで、 $x \in C(y)$ なので、 y と x を入れ替えて、 $C(y) \subset C(x)$ も言える。こより、 $C(x) = C(y)$ である。
- (3) $x, y \in S, z \in C(x) \cap C(y)$ なら、(2) より、 $C(x) = C(z), C(y) = C(z)$ となり、 $C(x) = C(y)$ である。

例 4.9 n を正の整数とする。 $x, y \in \mathbb{Z}$ であり、 $x \in \mathbb{Z}$ の同値類は $y - x$ が n で割り切れるような y 全体となる。これは、 $y - x \in n\mathbb{Z}$ と同値であるので、

$$C(x) = \{x + z \mid z \in n\mathbb{Z}\} = x + n\mathbb{Z}$$

となる。命題 4.8 より、任意の $y \in n\mathbb{Z}$ に対し、 $x + n\mathbb{Z} = y + n\mathbb{Z}$ である。

4.1.4 同値類の類別

集合 S に同値関係 \sim が与えられると、同値類によって S が互いに素な空でない部分集合に分割されることになる。これを S の同値関係 \sim による同値類別という。

定義 4.10 商集合

同値類別された同値類の集合を商集合といい、

$$S/\sim = \{C(x) | x \in S\}$$

と表す。

このとき、同値類 (各元) を \bar{x} と書く。

例 4.11 正の整数 n を法として合同な整数全体の商集合を $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \dots, \overline{n-1}\}$ と書く。2 を法として合同な整数の商集合は $\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$ であり、3 を法として合同な整数の商集合は $\mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\}$ となる。

(ここで、 $\mathbb{Z}/2\mathbb{Z}$ のとき、 $\bar{0} = \{x \in \mathbb{Z} | x = 2n + 0\}$, $\bar{1} = \{x \in \mathbb{Z} | x = 2n + 1\}$ 。 $\mathbb{Z}/3\mathbb{Z}$ のとき、 $\bar{0} = \{x \in \mathbb{Z} | x = 3n + 0\}$, $\bar{1} = \{x \in \mathbb{Z} | x = 3n + 1\}$, $\bar{2} = \{x \in \mathbb{Z} | x = 3n + 2\}$)

定義 4.12 自然な写像

S を商集合とする。以下のような写像を、自然な写像と呼ぶ。

$$\begin{array}{ccc} S & \xrightarrow{\pi} & S/\sim \\ \psi & & \psi \\ x & \mapsto & C(x) \end{array}$$

定義 4.13 代表元

S を商集合とする。 S の元 C に対して、 $x \in C$ となる S の元を代表元という

例 4.14 $\mathbb{Z}/2\mathbb{Z}$ の代表元は、 $\bar{0} = \{x \in \mathbb{Z} | x = 2n + 0\}$, $\bar{1} = \{x \in \mathbb{Z} | x = 2n + 1\}$ の中からそれぞれ自由に選んでよい。

定義 4.15 完全代表系

商集合 S の部分集合 R が S/\sim の各代表元をちょうど一つずつ含む時、 R を同値関係 \sim の完全代表系という。

例 4.16 $\mathbb{Z}/2\mathbb{Z}$ の完全代表系は、 $R = \{0, 1\}$ である。

4.2 剰余類

定義 4.17 H を G の部分群、 $x, y \in G$ とする。

- (1) $x^{-1}y \in H$ であるとき $x \sim y$ と定義する。このとき、 $x \in G$ の同値類を xH と書き、 x の H による左剰余類という。この集合を G/H と書く。
- (2) $y^{-1}x \in H$ であるとき $y \sim x$ と定義する。このとき、 $x \in G$ の同値類を Hx と書き、 x の H による右剰余類という。この集合を H/G と書く。

$xH = Hx$ のとき、これらを単に剰余類と呼ぶ。

5 正規部分群

定義 5.1 H を群 G の部分群とする。 H が G の正規部分群であるとは

- (1) すべての $g \in G$ に対し $gHg^{-1} = H$
 (2) すべての $g \in G, h \in H$ に対し $ghg^{-1} \in H$

が成り立つことであり、(1) と (2) は同値である。これを、 $H \triangleleft G$ 、あるいは $G \triangleright H$ と書く。

例 5.2 G が可換群で、 H が任意の部分群なら、 $gHg^{-1} = gg^{-1}H = g^{-1}gH = H$ となり、 H は正規部分群である。

命題 5.3 G_1, G_2 を群とし、 $\phi: G_1 \rightarrow G_2$ が準同型の時、 $\text{Ker}(\phi)$ は G_1 の正規部分群である。

証明

命題 3.3(3) より、 $\text{Ker}(\phi)$ は G_1 の部分群である。 $\text{Ker}(\phi)$ は G_1 の正規部分群であることを示す。
 $g \in G_1, h \in \text{Ker}(\phi)$ なら、

$$\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = 1_{G_2}$$

(※ $\text{Ker}(\phi)$ の定義より、 $\phi(h) = 1_{G_2}$ なので、 $\phi(g)\phi(h)\phi(g)^{-1} = \phi(g)\phi(g)^{-1}$ となる)

これより、 $ghg^{-1} \in \text{Ker}(\phi)$ となり、 $\text{Ker}(\phi)$ は G_1 の正規部分群である。

6 群の直積

定理 6.1 中国剰余定理

7 準同型定理

定理 7.1 準同型定理 (第一同型定理)

$\phi: G \rightarrow H$ を群の準同型とする。 $\pi: G \rightarrow G/\text{Ker}(\phi)$ を自然な準同型写像とすると、下図が可換図式となるような準同型写像 $\psi: G/\text{Ker}(\phi) \rightarrow H$ がただ一つ存在し、 ψ は $G/\text{Ker}(\phi)$ から $\text{Im}(\phi)$ への同型となる。

参考文献

- [1] 雪江明彦 [代数学 1 群論入門] 日本評論社