

代数学 I 第 1, 2 回講義資料

担当：大矢 浩徳 (OYA Hironori)*

1.1 導入

本講義のテーマは

『群論』

である。群とは“ある性質を満たす二項演算の定まった集合”である。正確な定義を後回しにして、大まかな説明を与えよう。“二項演算の定まった集合”というのは簡単に言えば“計算規則の定まった集合”というような意味である。良く知っている計算というと四則演算(+, -, ×, ÷)であろう。このとき、どのような数達(集合)の中でこれらの演算ができたかということを明確に意識してみる：

	集合	定義できる演算
自然数	$\mathbb{N} := \{0, 1, 2, \dots\}$ ^{*1}	+, ×
整数	$\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\}$	+, -, ×
有理数	$\mathbb{Q} := \{\frac{b}{a} \mid a \in \mathbb{Z} \setminus \{0\}, b \in \mathbb{Z}\}$	+, -, ×, (0を除くと)÷
実数	\mathbb{R}	+, -, ×, (0を除くと)÷
複素数	\mathbb{C}	+, -, ×, (0を除くと)÷

なおこの表の記号は今後も講義を通して用いられる。^{*2}“自然数 \mathbb{N} において、演算 + が定義できる”というのは、 $n_1, n_2 \in \mathbb{N}$ のとき $n_1 + n_2 \in \mathbb{N}$ なので、“+ という演算が \mathbb{N} 内で完結している (\mathbb{N} は + で閉じているという)”という意味である。一方例えば、 $2, 3 \in \mathbb{N}$ であるが、 $2 - 3 = -1 \notin \mathbb{N}$ なので、 \mathbb{N} は - で閉じていない。考える範囲を \mathbb{Z} にしておくとし、引き算 - でも閉じている。こういった調子で上の表は読めばよい。

もう少し数学的に書いてみよう。四則演算はどれも、“2つの数から新しい数を得る”という操作である。例えば、 $2 + 3 = 5$ は“2 と 3 から 5 を得ている”と考える。こう考えると、足し算は

$$\begin{array}{ccc} +: & \mathbb{N} \times \mathbb{N} & \longrightarrow & \mathbb{N} \\ & \cup & & \cup \\ & (n_1, n_2) & \longmapsto & n_1 + n_2. \end{array}$$

という写像に他ならない。

復習

集合 X, Y に対し、

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

である。(この \times は上で出てきた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。)

こうすると、四則演算 \cdot が集合 G 上で定義できるとは、 \cdot が写像

$$\therefore G \times G \rightarrow G \tag{1.1}$$

を定めるという意味である。^{*3}(1.1) の形の写像を二項演算という。

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

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

*3 上の“閉じている”という概念とも整合していることに注意すること。

なお、写像という言葉で書こうとすると、割り算 \div については少々注意が必要である。 $\div: \mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{Q}, (a, b) \mapsto a \div b$ は、 $(a, 0)$ の形の元の行き先が $a \div 0$ となって定義できないため、写像としての定義ができていない。割り算をこの形で定義するためには、

$$\mathbb{Q}^\times := \mathbb{Q} \setminus \{0\} \qquad \mathbb{R}^\times := \mathbb{R} \setminus \{0\} \qquad \mathbb{C}^\times := \mathbb{C} \setminus \{0\}. \quad (1.2)$$

としておいて、 $\div: \mathbb{X}^\times \times \mathbb{X}^\times \rightarrow \mathbb{X}^\times, (a, b) \mapsto a \div b$ ($\mathbb{X} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$) を考えるということになる。

さて、群の(ラフな)定義をもう一度思い出そう。群とはある性質を満たす二項演算 $\cdot: G \times G \rightarrow G$ が定まった集合 (G, \cdot) である。上に出てきたものの中では、実は $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{Q}^\times, \times), (\mathbb{R}^\times, \times), (\mathbb{C}^\times, \times)$ が群の例となる。(それ以外の上に出てきた集合と二項演算の組は残念ながら群の定義を満たす演算にはならない。) まずは、群とはこのような“計算ができる数”を一般化したようなものだと思えば良い。これは非常に重要な一般化で、キーワード的に書いておくと、

- 群は“対称性”を数学的に抽象化したものとなる。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。このようなことから、例えば物理においても基本的な言語として用いられるものとなる。
- “5次以上の方程式には、その係数の四則演算と冪根で表される解の公式が存在しない”という有名な事実は、方程式から定まるガロア群と呼ばれる群の性質を調べることから証明される。この講義の中では扱うことができないが、興味のある方は『ガロア理論』というキーワードで調べて勉強すると良いであろう。

ちなみに、“足し算と掛け算”の定まった $(\mathbb{Z}, +, \times)$ のような集合の抽象化の話もある。これは環論と呼ばれ、『代数学 II』で学ぶこととなる。さらに、上で四則演算が全て定義できた $(\mathbb{Q}, +, \times, \div)$ (ただし割り算においては0を除く) のような集合を扱う話は体論と呼ばれる。演算が増えるごとに難しくなっていくというわけではなく、これらは独立に、しかしあるところでは関連しながら代数学の世界をなしている。例えば、上に書いた『ガロア理論』においては、これら全ての考え方が、本質的に表れてくる。

1.2 合同算術

群の定義をするのはもう少し先にして、1.1章で見た例以外で、非自明な二項演算が定義される集合の例を学ぶ。

n を正の整数とする。各 $a \in \mathbb{Z}$ に対し、 $[a]_n$ という記号を割り当てる。ただし、 $a, b \in \mathbb{Z}$ に対し、 $[a]_n$ と $[b]_n$ は次のルールで同一視されているとする：

$$[a]_n = [b]_n \iff a - b \text{ が } n \text{ で割り切れる} (\iff a \equiv b \pmod{n}). \quad (1.3)$$

例 1. 同一視の例：

- $[2]_5 = [7]_5 = [-3]_5 = \dots$
- $[90]_{360} = [-270]_{360} = [450]_{360} = \dots$

この計算は角度計算のように考えればこれまで十分慣れ親しんだものと言えるだろう ($90^\circ = -270^\circ = 450^\circ$)。

このとき、

$$\mathbb{Z}/n\mathbb{Z} := \{[a]_n \mid a \in \mathbb{Z}\} = \{[0]_n, [1]_n, \dots, [n-1]_n\} \quad (1.4)$$

とする。ここで、(1.3)により、 $[a]_n = [b]_n$ となる必要十分条件は a と b を n で割った余りが等しいことであり、整数を n で割った余りは $0, 1, \dots, n-1$ のいずれかであることから、2つめの等号は示される。 $\mathbb{Z}/n\mathbb{Z}$

は n 元からなる有限集合であるが、ここに以下の方法で二項演算を定義する：

$$\begin{aligned} +: \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\rightarrow \mathbb{Z}/n\mathbb{Z}, ([a]_n, [b]_n) \mapsto [a + b]_n \\ -: \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\rightarrow \mathbb{Z}/n\mathbb{Z}, ([a]_n, [b]_n) \mapsto [a - b]_n \\ \times: \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\rightarrow \mathbb{Z}/n\mathbb{Z}, ([a]_n, [b]_n) \mapsto [ab]_n. \end{aligned}$$

例 2.

$$[2]_7 + [5]_7 = [7]_7 = [0]_7 \quad [2]_7 - [5]_7 = [-3]_7 = [4]_7 \quad [2]_5 \times [3]_5 = [6]_5 = [1]_5.$$

重要 (これらはちゃんと定義されている (well-defined)?)

(1.3) において a, b を有理数と考えると, $[a]_n$ の定義を $a \in \mathbb{Q}$ に拡張してみよう*4. 例えば, $[0.5]_2 = [2.5]_2 = [-1.5]_2$ 等である. 正の整数 $n \in \mathbb{Z}$ に対して, $\mathbb{Q}/n\mathbb{Z} = \{[r]_n \mid r \in \mathbb{Q}\}$ とする. このとき,

$$\times: \mathbb{Q}/n\mathbb{Z} \times \mathbb{Q}/n\mathbb{Z} \rightarrow \mathbb{Q}/n\mathbb{Z}, ([r]_n, [s]_n) \mapsto [rs]_n.$$

は定義されるだろうか? 実は以下のような困ったことが起こってしまう：

$$\begin{aligned} [1.5]_2 \times [2]_2 &= [1.5 \times 2]_2 = [3]_2 \\ &\parallel \qquad \qquad \qquad \neq \\ [1.5]_2 \times [0]_2 &= [1.5 \times 0]_2 = [0]_2. \end{aligned}$$

よって, この写像の定義として良くないことがわかる. なぜ, このようなことが起こるかということ, 『 $\mathbb{Q}/n\mathbb{Z}$ の中では, 1 つの元を表す方法が何通りもある ($[2]_2 = [0]_2$ 等) にもかかわらず, 写像の定義においてこの表示を用いてしまった』からである. この結果, 本当は同じ元なのに, 表わし方が違ったがために結果が変わるということになってしまったのである.

このように, 1 つの元の表し方が複数あるような集合からの写像を定義する際には細心の注意を払う必要がある. 定義した写像が元の表示の仕方に依らないとき, その写像は *well-defined* であるという. この注意は慣れるまで難しいと思われるが, 今後の講義でも非常に重要になる.

試しに, $\times: \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ が well-defined であることを示そう. ある元に対して, どんな表示を持ってきても結果が変わらないことを言えばよい.

証明. $a, a', b, b' \in \mathbb{Z}$ に対し, $[a]_n = [a']_n$, $[b]_n = [b']_n$ であると仮定する. このとき, (1.3) から, ある $m_1, m_2 \in \mathbb{Z}$ が存在して,

$$a' = a + m_1n \quad b' = b + m_2n$$

と書ける. これより,

$$\begin{aligned} [a']_n \times [b']_n &= [(a + m_1n)(b + m_2n)]_n \\ &= [ab + (am_2 + bm_1 + m_1m_2n)]_n \end{aligned}$$

となるが, いま $am_2 + bm_1 + m_1m_2n$ は整数なので, 結局 $[a']_n \times [b']_n = [ab]_n = [a]_n \times [b]_n$ となり, well-defined であることが示された. \square

a, b が有理数の場合には下線部分が言えないので, well-defined ではなかったのである. この調子で, $\mathbb{Z}/n\mathbb{Z}$ 上の二項演算 $+, -$ が well-defined であることを確認してもらいたい. ちなみに, $+$ や $-$ に関しては $\mathbb{Q}/n\mathbb{Z}$ においても well-defined に拡張される.

応用例：フェルマーの小定理

$\mathbb{Z}/n\mathbb{Z}$ における計算の応用例として, フェルマーの小定理を証明しよう. まず以下の命題を準備する：

*4 ちゃんと言うと, “ $a - b$ が n で割り切れる” は “ $a - b$ が n で割り切れる整数である” に修正する.

命題 1.1

p を素数とする. このとき, 各 $a, b \in \mathbb{Z}$ に対し,

$$([a]_p + [b]_p)^p = ([a]_p)^p + ([b]_p)^p$$

ここで p 乗は, $\mathbb{Z}/p\mathbb{Z}$ における \times を p 回繰り返すという意味である.

証明.

$$\begin{aligned}
([a]_p + [b]_p)^p &= ([a + b]_p)^p \\
&= [(a + b)^p]_p \\
&= [a^p + {}_p C_1 a^{p-1} b + {}_p C_2 a^{p-2} b^2 + \cdots + {}_p C_{p-1} a b^{p-1} + b^p]_p \quad (\text{二項定理}).
\end{aligned}$$

ここで, ${}_p C_k = \frac{p!}{k!(p-k)!}$ ($k = 1, \dots, p-1$) である. いま, p は素数なので, $k = 1, \dots, p-1$ のとき, $k!(p-k)!$ は p では割り切れない. 一方で, $p!$ は p で割り切れることに注意すると, ${}_p C_k$ は $k = 1, \dots, p-1$ のとき p の倍数であることがわかる. これより, 定義 (1.3) から,

$$[a^p + {}_p C_1 a^{p-1} b + {}_p C_2 a^{p-2} b^2 + \cdots + {}_p C_{p-1} a b^{p-1} + b^p]_p = [a^p + b^p]_p.$$

以上より, $([a]_p + [b]_p)^p = [a^p + b^p]_p = ([a]_p)^p + ([b]_p)^p$ となる. □

定理 1.2 (フェルマーの小定理)

p を素数とする. このとき, $a \in \mathbb{N}$ に対し, a^p を p で割った余りと, a を p で割った余りは等しい.

証明. $[a^p]_p = [a]_p$ を示せばよい. 命題 1.1 を繰り返し用いると,

$$\begin{aligned}
[a^p]_p &= ([a]_p)^p = ([1]_p + [a-1]_p)^p = ([1]_p)^p + ([a-1]_p)^p \\
&= ([1]_p)^p + ([1]_p + [a-2]_p)^p = ([1]_p)^p + ([1]_p)^p + ([a-2]_p)^p \\
&\dots \\
&= \underbrace{([1]_p)^p + ([1]_p)^p + \cdots + ([1]_p)^p}_{a \text{ 個}} = \underbrace{[1]_p + [1]_p + \cdots + [1]_p}_{a \text{ 個}} = [a]_p
\end{aligned}$$

□

1.3 次回への準備 : 拡張ユークリッド互除法

次回, $\mathbb{Z}/n\mathbb{Z}$ における “割り算” について考察する. そのために必要な拡張ユークリッド互除法について思い出す. ここでは, 具体例をもとにその方法を思い出すにとどめる. 厳密な取り扱いについては, 補足プリント “拡張ユークリッド互除法について” を参考にすること.

定義 1.3.

正の整数 a, b に対して, その最大公約数 (greatest common divisor) を $\gcd(a, b)$ と書く. さらに 0 以上の整数 a に対して, $\gcd(0, a) = \gcd(a, 0) = a$ とする.

正の整数 a, b が与えられたときに, $\gcd(a, b)$ を効率良く求める方法がユークリッド互除法である. 例として, 2394 と 714 の最大公約数 $\gcd(2394, 714)$ を求めてみよう.

ユークリッド互除法を用いて $\gcd(2394, 714)$ を求める

(Step 1) 大きい方の数を小さい方の数で割る :

$$2394 = \underset{\text{商}}{3} \times 714 + \underset{\text{余り}}{252}. \quad (1.5)$$

このとき, 以下のようにして $\gcd(2394, 714) = \gcd(714, 252)$ であることがわかる.

$m = \gcd(2394, 714)$ とすると, 714 と 2394 は共に m の倍数であるから, $[252]_m = [252 + 3 \times 714]_m = [2394]_m = [0]_m$ なので, 252 も m で割り切れる. よって, $\gcd(2394, 714) = m \leq \gcd(714, 252)$.

一方, $n = \gcd(714, 252)$ とすると, 714 と 252 は共に n の倍数であるから, $[2394]_n = [3 \times 714 + 252]_n = [0]_n$ なので, 2394 も n で割り切れる. よって, $\gcd(714, 252) = n \leq \gcd(2394, 714)$.

以上より, $\gcd(2394, 714) = \gcd(714, 252)$.

一般の状況での厳密な証明は補足プリント“拡張ユークリッド互除法について”の命題を参照のこと. (証明方法はこれと同じである.)

(Step 2) 元の問題は $\gcd(714, 252)$ を求める問題に変わったので, 714 と 252 に対して, (Step1) を繰り返す.

$$714 = \underset{\text{商}}{2} \times 252 + \underset{\text{余り}}{210}. \quad (1.6)$$

このとき, 上と同様に考えて, $\gcd(714, 252) = \gcd(252, 210)$.

(Step 3) 元の問題は $\gcd(252, 210)$ を求める問題に変わったので, 252 と 210 に対して, (Step1) を繰り返す.

$$252 = \underset{\text{商}}{1} \times 210 + \underset{\text{余り}}{42}. \quad (1.7)$$

このとき, 上と同様に考えて, $\gcd(252, 210) = \gcd(210, 42)$.

(Step 4) 元の問題は $\gcd(210, 42)$ を求める問題に変わったので, 210 と 42 に対して, (Step1) を繰り返す.

$$210 = \underset{\text{商}}{5} \times 42 + \underset{\text{余り}}{0}. \quad (1.8)$$

ここで, 割り切れたので, $\gcd(210, 42) = 42$ である. ($\gcd(210, 42) = \gcd(42, 0) = 42$ と考えても良い.) 以上より, $\gcd(2394, 714) = 42$.

この方法は, 考える整数がどんどん小さくなっていくので, どんな 2 つの数から始めても必ずいつか割り切れて終わるということが容易に想像できるだろう. (厳密な取り扱いについては, 補足プリント“拡張ユークリッド互除法について”を参考にすること.) これがユークリッド互除法である.

さて, ユークリッド互除法の各 Step を覚えておくことで, 次のような問題に答えることができる.

$2394x + 714y = 42$ を満たす整数の組 (x, y) を 1 つ求めよ.

解. ユークリッド互除法での計算を“逆にたどる”.

$$\begin{aligned} 42 &= 252 - 1 \times 210 \quad ((1.7) \text{ より}) \\ &= 252 - 1 \times (714 - 2 \times 252) \quad ((1.6) \text{ より}) \\ &= (-1) \times 714 + 3 \times 252 \\ &= (-1) \times 714 + 3 \times (2394 - 3 \times 714) \quad ((1.5) \text{ より}) \\ &= 3 \times 2394 + (-10) \times 714 \end{aligned}$$

これより, $2394x + 714y = 42$ を満たす整数の組 (x, y) の例として, $(x, y) = (3, -10)$ が取れる. \square

この解で行ったような, ユークリッド互除法を逆にたどるアルゴリズムは拡張ユークリッド互除法と呼ばれる.

ちなみに、 $2394x + 714y = 42$ を満たす整数の組 (x, y) はこれだけではない。しかし、1 つ解を見つければ、一般に次のようにして全ての整数解が見つけれられる。

$$\begin{aligned} 2394x + 714y &= 42 \\ \Leftrightarrow 2394(x - 3) + 714(y - (-10)) &= 0 \quad (\text{ここで, さっき見つけた解を用いる}) \\ \Leftrightarrow 57(x - 3) + 17(y + 10) &= 0 \quad (\text{両辺を } 42 = \gcd(2394, 714) \text{ で割る.}) \end{aligned}$$

このとき、最大公約数で割ったので、57 と 17 は互いに素であることに注意すると、最後の等式が成立するためには、

$$(x - 3, y + 10) = (17m, -57m), \quad m \in \mathbb{Z}$$

という形であることが必要十分である。よって、 $2394x + 714y = 42$ を満たす整数の組 (x, y) は

$$(x, y) = (3 + 17m, -10 - 57m), \quad m \in \mathbb{Z}$$

が全てである。以上の事実を一般的な言葉を使ってまとめておこう。

正の整数 a, b , 整数 k に対して、

$$ax + by = k \gcd(a, b)$$

を満たす整数の組 (x, y) は次のようにして求められる。

(Step 1) ユークリッド互除法で $\gcd(a, b)$ を求める。この際、途中計算を記録しておく。

(Step 2) ユークリッド互除法の計算を逆にたどる拡張ユークリッド互除法を用いて $ax + by = \gcd(a, b)$ を満たす整数の組 (x'_0, y'_0) を1つ求める。

(Step 3) $x_0 := kx'_0, y_0 := ky'_0$ とすれば、 (x_0, y_0) は $ax_0 + by_0 = k \gcd(a, b)$ を満たす整数の組である。

(Step 4) $a' := a / \gcd(a, b), b' := b / \gcd(a, b)$ とすると、 a' と b' は互いに素で、

$$ax + by = k \gcd(a, b) \Leftrightarrow a'(x - x_0) + b'(y - y_0) = 0$$

であるので、これを満たすためには、

$$(x - x_0, y - y_0) = (b'm, -a'm), \quad m \in \mathbb{Z}$$

が必要十分である。

(Step 5) $ax + by = k \gcd(a, b)$ を満たす整数の組 (x, y) は

$$(x, y) = (x_0 + b'm, y_0 - a'm), \quad m \in \mathbb{Z}$$

が全てである。

また、以下の定理の形も重要である：

定理 1.4

正の整数 a, b に対して、以下の (1) と (2) は同値である：

- (1) $ax + by = d$ を満たす整数の組 (x, y) が存在する。
- (2) $[d]_{\gcd(a, b)} = [0]_{\gcd(a, b)}$.

証明. (1) \Rightarrow (2) : a, b は $\gcd(a, b)$ の倍数なので、 $ax + by = d$ を満たす整数の組 (x_0, y_0) が存在するとき、

$$[d]_{\gcd(a, b)} = [ax_0 + by_0]_{\gcd(a, b)} = [0]_{\gcd(a, b)}.$$

(1) \Leftarrow (2) : $[d]_{\gcd(a, b)} = [0]_{\gcd(a, b)}$ のとき、ある $k \in \mathbb{Z}$ を用いて、 $d = k \gcd(a, b)$ と書ける。 $ax + by = k \gcd(a, b)$ を満たす整数の組 (x, y) が存在することは上でまとめた通りである。□

系 1.5

正の整数 a, b に対して、以下の (1) と (2) は同値である：

- (1) $ax + by = 1$ を満たす整数の組 (x, y) が存在する.
- (2) a と b は互いに素. (つまり, $\gcd(a, b) = 1$.)

代数学 I 第 3 回講義資料

担当：大矢 浩徳 (OYA Hironori)*

2.1 合同算術 (続き)

n を 2 以上の整数とする。前回, n 元からなる有限集合 $\mathbb{Z}/n\mathbb{Z}$ (\mathbb{Z} の n を法とする剰余類環と呼ばれる) に二項演算

$$\begin{aligned} \pm: \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\rightarrow \mathbb{Z}/n\mathbb{Z}, ([a]_n, [b]_n) \mapsto [a]_n \pm [b]_n := [a \pm b]_n \\ \times: \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\rightarrow \mathbb{Z}/n\mathbb{Z}, ([a]_n, [b]_n) \mapsto [a]_n [b]_n := [ab]_n. \end{aligned}$$

を定義した。では四則演算の最後の 1 つ “割り算” は $\mathbb{Z}/n\mathbb{Z}$ (\mathbb{Z} の中で考えられるだろうか? まず, “ $\div: \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}, ([a]_n, [b]_n) \mapsto [a/b]_n$ ” は明らかにダメである。(a/b は一般に有理数なので, $[a/b]_n$ という元は $\mathbb{Z}/n\mathbb{Z}$ において定義されない。)

普通の数において, “ a で割る” という事は “逆数 a^{-1} を掛ける” という事であった。これにならって, まず $\mathbb{Z}/n\mathbb{Z}$ における “逆数” を考えてみる。まず $a \neq 0$ に対し, 逆数 a^{-1} は

$$aa^{-1} = 1$$

を満たす元であった。そこで, 次のように考えてみよう。

定義 2.1

- $\mathbb{Z}/n\mathbb{Z}$ における “1” を $[1]_n$ とする。
- $[a]_n \in \mathbb{Z}/n\mathbb{Z}$ に対して, $[a]_n^{-1}$ を

$$[a]_n [a]_n^{-1} = [1]_n \tag{2.1}$$

を満たす $\mathbb{Z}/n\mathbb{Z}$ の元とする。この元を $[a]_n$ の \times に関する逆元という。

例 1 ((2.1) を満たす元の例). $\mathbb{Z}/7\mathbb{Z}$ において,

$$[4]_7 [2]_7 = [8]_7 = [1]_7$$

となるので, $[4]_7^{-1} = [2]_7$ である。 $\mathbb{Z}/12\mathbb{Z}$ において,

$$[5]_{12} [5]_{12} = [25]_{12} = [1]_{12}$$

となるので, $[5]_{12}^{-1} = [5]_{12}$ である。

“1” を $[1]_n$ とするのはいかにも自然だが, もう少しちゃんとした理由を, 次回群の定義を説明する際に説明する。実際にこれは “1” の満たして欲しい以下の性質を満たしている。

$$[1]_n [a]_n = [a]_n = [a]_n [1]_n$$

また, 条件 (2.1) によって $[a]_n^{-1}$ が確かにただ 1 つに定まることが, 以下の補題からわかる。

補題 2.2

$[a]_n \in \mathbb{Z}/n\mathbb{Z}$ に対して, 条件 (2.1) を満たす元は高々 1 つである。

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

証明. $[b]_n$ と $[b']_n$ が共に $[a]_n^{-1}$ の条件 (2.1) を満たすとす。つまり,

$$[a]_n[b]_n = [1]_n = [a]_n[b']_n$$

とする。このとき,

$$[b]_n = [1]_n[b]_n = ([a]_n[b']_n)[b]_n = [abb']_n = ([a]_n[b]_n)[b']_n = [1]_n[b']_n = [b']_n.$$

□

さて, \mathbb{C} において 0^{-1} が存在しなかったように, $\mathbb{Z}/n\mathbb{Z}$ においても \times に関する逆元がいつも存在するとは限らない。そこで, 以下のように定義する:

定義 2.3

$$(\mathbb{Z}/n\mathbb{Z})^\times := \{[a]_n \mid [a]_n^{-1} \text{ が存在} \} = \{[a]_n \mid \text{ある } b \in \mathbb{Z} \text{ が存在して, } [a]_n[b]_n = [1]_n\}.*1$$

命題 2.4

- (1) $(\mathbb{Z}/n\mathbb{Z})^\times$ は演算 \times で閉じている。
- (2) $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ に対し, $[a]_n^{-1} \in (\mathbb{Z}/n\mathbb{Z})^\times$ である。

証明. (1) $[a]_n, [b]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ に対し, $[a]_n[b]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ であること, つまり $[a]_n[b]_n$ に \times に関する逆元が存在することを示せばよい。いま, $[a]_n^{-1}, [b]_n^{-1} \in \mathbb{Z}/n\mathbb{Z}$ は存在するので,

$$([a]_n[b]_n)([b]_n^{-1}[a]_n^{-1}) = [a]_n([b]_n[b]_n^{-1})[a]_n^{-1} = [a]_n[1]_n[a]_n^{-1} = [a]_n[a]_n^{-1} = [1]_n.$$

よって, $[b]_n^{-1}[a]_n^{-1}$ が $[a]_n[b]_n$ の \times に関する逆元となる。 □

(2) $\mathbb{Z}/n\mathbb{Z}$ においては $[a]_n[b]_n = [b]_n[a]_n$ が成立するので, $[a]_n[a]_n^{-1} = [1]_n$ のとき, $[a]_n^{-1}[a]_n = [1]_n$. よって, $[a]_n^{-1}$ の \times に関する逆元は $[a]_n$ であり, 特に $[a]_n^{-1} \in (\mathbb{Z}/n\mathbb{Z})^\times$ である。 □

集合 $(\mathbb{Z}/n\mathbb{Z})^\times$ に二項演算 $\times: (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ を考えたもの $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ を $\mathbb{Z}/n\mathbb{Z}$ の乗法群という。 $(\mathbb{Z}/n\mathbb{Z})^\times$ には, “割り算”

$$\div: (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times, ([a]_n, [b]_n) \mapsto [a]_n[b]_n^{-1}$$

も定義できる。なお, $[a]_n, [b]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ に対し, $[a]_n[b]_n^{-1} \in (\mathbb{Z}/n\mathbb{Z})^\times$ となることは, 命題 2.4 (2) より $[a]_n, [b]_n^{-1} \in (\mathbb{Z}/n\mathbb{Z})^\times$ であることから, 命題 2.4 (1) よりわかる。

$(\mathbb{Z}/n\mathbb{Z})^\times$ の元の具体的表示:

さて, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ においては, 0 以外のすべての元が \times に関する逆元を持っていたが, $\mathbb{Z}/n\mathbb{Z}$ はどうだろうか。 $(\mathbb{Z}/n\mathbb{Z})^\times$ に含まれる具体的な元について考えてみよう。これは次の同値関係をたどっていくとわかる。

$$\begin{aligned} [a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times &\Leftrightarrow \text{ある } x \in \mathbb{Z} \text{ が存在して, } [ax]_n (= [a]_n[x]_n) = [1]_n \\ &\Leftrightarrow \text{ある } x, y \in \mathbb{Z} \text{ が存在して, } ax + ny = 1 \\ &\Leftrightarrow a \text{ と } n \text{ は互いに素. (第 1, 2 回講義資料, 系 1.5)} \end{aligned}$$

これより, 以下がわかる:

命題 2.5

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{[a]_n \mid \gcd(a, n) = 1\}.*2$$

上の同値関係で結んだ部分の考え方に基づけば, $(\mathbb{Z}/n\mathbb{Z})^\times$ における各元の \times に関する逆元は次のように求められることがわかる:

*1 $\mathbb{X} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ に対し, $\mathbb{X}^\times := \mathbb{X} \setminus \{0\}$ も \mathbb{X} の中で \times に関する逆元を持つものの集まりとなっていたことに注意しよう。
*2 負の数に対応する gcd については, 補足プリント “拡張ユークリッド互除法について” を参照のこと。

$[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ に対し,

$$ax + ny = 1$$

を満たす整数の組 (x, y) を見つければ, $[x]_n$ が $[a]_n$ の \times に関する逆元である. このような (x, y) は拡張ユークリッド互除法で見つけることができる. (第 1, 2 回講義資料参照)

例 2. 以下の問題を考えてみよう.

$(\mathbb{Z}/60\mathbb{Z})^\times$ において, $[17]_{60}$ の \times に関する逆元を求めよ.

なお, $\gcd(17, 60) = 1$ なので, $[17]_{60}$ は確かに $(\mathbb{Z}/n\mathbb{Z})^\times$ の元である. (命題 2.4)

解答. $17x + 60y = 1$ を満たす整数の組 (x, y) を拡張ユークリッド互除法で求める:

$$\begin{aligned} 60 &= 3 \times 17 + 9 & 17 &= 1 \times 9 + 8 \\ 9 &= 1 \times 8 + 1 & 8 &= 8 \times 1 + 0 \end{aligned}$$

であるので,

$$\begin{aligned} 1 &= 9 - 1 \times 8 \\ &= 9 + (-1) \times (17 - 1 \times 9) \\ &= (-1) \times 17 + 2 \times 9 \\ &= (-1) \times 17 + 2 \times (60 - 3 \times 17) \\ &= (-7) \times 17 + 2 \times 60 \end{aligned}$$

より, $(x, y) = (-7, 2)$ が $17x + 60y = 1$ を満たす整数の組の例である. よって, 求める逆元は $[-7]_{60} = [53]_{60}$.
□

検算してみると, 確かに $[17]_{60}[-7]_{60} = [-119]_{60} = [1]_{60}$ となっている.

定義 2.6

正の整数 n に対し, n と互いに素な 1 以上 n 以下の自然数の個数を $\varphi(n)$ と書く. つまり,

$$\varphi(n) := \#\{m \in \mathbb{N} \mid 1 \leq m \leq n, \gcd(m, n) = 1\}^{*3}$$

とする. n に対して $\varphi(n)$ を与える関数 $\varphi: \mathbb{Z}_{>0} \rightarrow \mathbb{Z}_{>0}, n \mapsto \varphi(n)$ をオイラー (Euler) の φ 関数という.

例 3.

$$\varphi(1) = 1 \quad \varphi(2) = 1 \quad \varphi(3) = 2 \quad \varphi(4) = 2 \quad \varphi(5) = 4 \quad \varphi(6) = 2$$

特に, p が素数のとき, $1, \dots, p-1$ は全て p と互いに素なので, $\varphi(p) = p-1$ である. 逆に $\varphi(n) = n-1$ となるとき, n は素数である.

命題 2.5 より, 以下のことは直ちにわかる.

命題 2.7

$$\#(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n).$$

命題 2.7 と例 3 での考察から,

$$\#(\mathbb{Z}/n\mathbb{Z})^\times = n-1 \Leftrightarrow n \text{ は素数}$$

*3 $\#(\dots)$ は “集合 (\dots) の元の個数” を表す記号である.

であることがわかる。ここで (2.1) を思い出すと、 $[0]_n$ は明らかに \times に関する逆元を持たないので、 $\#(\mathbb{Z}/n\mathbb{Z})^\times = n - 1$ は、

$$(\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/n\mathbb{Z}) \setminus \{[0]_n\}$$

と同値である。つまり、

$$(\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/n\mathbb{Z}) \setminus \{[0]_n\} \Leftrightarrow n \text{ が素数.} \quad (2.2)$$

となる。“ $[0]_n$ 以外のすべての元が \times に関する逆元を持つ” というのは、 $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ 等と似た性質である。実際にこういった代数系の抽象化は体と呼ばれるもので、本講義では体論は扱わないが、以下のように言うこともできる。

$$\mathbb{Z}/n\mathbb{Z} \text{ が体である} \Leftrightarrow n \text{ が素数.}$$

$\mathbb{Z}/p\mathbb{Z}$ (p は素数) という形の体は、有限個の元からなる体ということで、有限体と呼ばれるものの例となる。

応用例：フェルマーの小定理 (続) 前回扱ったフェルマーの小定理にもう一つ主張を付け足したものをここで述べておこう。実際にはこの追加された主張をフェルマーの小定理と呼ぶことが多い。

定理 2.8 (フェルマーの小定理, Fermat's little theorem)

p を素数する。このとき、任意の $a \in \mathbb{Z}$ に対し、

$$[a^p]_p = [a]_p.$$

となる。さらに、 a が p の倍数でないとき、

$$[a^{p-1}]_p = [1]_p. \quad (2.3)$$

証明. $[a^p]_p = [a]_p$ は第 1, 2 回講義資料の定理 1.2 の言い換えである。^{*4}よって、式 (2.3) を示す。 a が p の倍数でないとき、 $[a]_p \neq [0]_p$ である。いま p は素数なので、このとき (2.2) より $[a]_p^{-1}$ が存在する。 $[a]_p^{-1}$ を $[a^p]_p = [a]_p$ の両辺に掛けると、

$$[a^{p-1}]_p = [1]_p$$

を得る。 □

実は、(2.3) は以下のような形で p が素数でない場合についても一般化される：

定理 2.9 (オイラーの定理, Euler's theorem)

n が正の整数、 $a \in \mathbb{Z}$ 、 $\gcd(a, n) = 1$ のとき、

$$[a^{\varphi(n)}]_n = [1]_n.$$

この定理の証明は、もう少し群論の勉強を進めてから行う。群論の一般論によって実はこの定理は容易に示される (お楽しみに!)。なお、オイラーの定理で、 n を素数とすると、 a が n の倍数でさえなければ $\gcd(a, n) = 1$ となり、しかも $\varphi(n) = n - 1$ となるので、確かにこの定理はフェルマーの小定理を含んでいる。

^{*4} 正確には前回は a が負の場合は証明をしていないが、この主張は成立する。確かめてみよ。

代数学 I 第 4 回講義資料

担当：大矢 浩徳 (OYA Hironori)*

いよいよ本講義の主題である『群』が登場する。今回の講義資料では、3.1 章で群と部分群の基本性質について抽象的に解説をし、3.2 章で例について解説する。抽象的な話よりも早く例を知りたいという方は、群と部分群の定義 3.1, 3.2, 3.3 だけ読んだらすぐに 3.2 章に飛び、必要になる度に 3.1 章に戻ってくるという読み方でも良いであろう。

3.1 群と部分群

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 3.1

空でない集合 G にある写像

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

(二項演算と呼ばれる) 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。(この e を G の単位元と呼ぶ。)
- (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。(この g' を G における g の逆元と呼ぶ。以下でも用いるが、 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 (**commutative group**) 又はアーベル群 (**abelian group**) という。

定義 3.2

群 G の部分群とは、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。

定義 3.3

G を群とする。 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 (**finite group**) といい、 $|G| = \infty$ のとき、 G を無限群 (**infinite group**) という。

以下は抽象的な群と部分群の基本性質である。

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

命題 3.4

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 3.5

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

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

の定義域を $H \times H$ に制限したとき、これが

$$\cdot: H \times H \rightarrow H$$

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 $\cdot: H \times H \rightarrow H$ を定めるということより、任意の $h, k \in H$ に対し、 $h \cdot k \in H$ は成立する. 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 3.4(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 $\cdot: H \times H \rightarrow H$ 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であるため、(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. \square

3.2 群と部分群の例 (その1)

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 1 (加法群). $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ 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

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

をみますので、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。

なお、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、性質 (III)(逆元の存在) を満たさないためである。

例 2 (乗法群). $(\mathbb{Q}^\times, \times), (\mathbb{R}^\times, \times), (\mathbb{C}^\times, \times)$ 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)：

$$(I) \text{ (結合法則) 任意の } a, b, c \in \mathbb{K}^\times \text{ に対し, } (a \times b) \times c = a \times (b \times c).$$

$$(II) \text{ (単位元の存在) 単位元は } 1 \in \mathbb{K}^\times \text{ である。実際, 任意の } a \in \mathbb{K}^\times \text{ に対し, } 1 \times a = a = a \times 1 \text{ が成立する。}$$

$$(III) \text{ (逆元の存在) 任意の } a \in \mathbb{K}^\times \text{ に対し, } a^{-1} \in \mathbb{K}^\times \text{ であって, } a^{-1} \times a = 1 = a \times a^{-1} \text{ が成立する。}$$

さらに、乗法 \times は

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

をみますので、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、

$$\mathbb{K}_{>0}^\times := \{a \in \mathbb{K}^\times \mid a > 0\}$$

とすると、 $\mathbb{K}_{>0}^\times$ 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 3.5 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 a^{-1} であるが、 $a^{-1} \notin \mathbb{Z} \setminus \{0\}$ であるため、性質 (III)(逆元の存在) を満たさないためである。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、

$$1 \times 1 = 1 \quad (-1) \times 1 = -1 \quad 1 \times (-1) = -1 \quad (-1) \times (-1) = 1$$

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 3.5 より、 $\{1, -1\}$ は $(\mathbb{K}^\times, \times)$ の部分群である。さらに、 $\#\{1, -1\} = 2$ なので、これは位数 2 の有限群の例となる。

注意. 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 3.2 の、『 G の二項演算によって』という部分を満たしていないためである。

例 3 (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 $+: V \times V \rightarrow V, (u, v) \mapsto u + v,$
- \cdot は写像 $\cdot: \mathbb{K} \times V \rightarrow V, (c, v) \mapsto cv$

であって, 以下が成立する:

- (v1) 任意の $u, v \in V$ に対し, $u + v = v + u,$
- (v2) 任意の $u, v, w \in V$ に対し, $(u + v) + w = u + (v + w),$
- (v3) ある元 $0 \in V$ が存在して, 任意の $u \in V$ に対し, $u + 0 = u,$ (この 0 を零ベクトルという)
- (v4) 任意の $v \in V$ に対して, ある元 $-v \in V$ が存在して, $v + (-v) = 0,$ (この $-v$ を v の逆元という)
- (v5) 任意の $c, d \in \mathbb{K}, v \in V$ に対し, $(c + d)v = cv + dv,$
- (v6) 任意の $c \in \mathbb{K}, u, v \in V$ に対し, $c(u + v) = cu + cv,$
- (v7) 任意の $c, d \in \mathbb{K}, v \in V$ に対し, $(cd)v = c(dv),$
- (v8) 任意の $v \in V$ に対し, $1v = v.$

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 0 の存在 ((v1) より, $0 + u = u$ も成立する), (v4) が各元 $v \in V$ の逆元 $-v$ の存在 ((v1) より, $(-v) + v = 0$ 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することができる.

例 4 (整数の剰余類群). 正の整数 n に対して, $(\mathbb{Z}/n\mathbb{Z}, +)$ は群である. これは n を法とする整数の剰余類群とよばれる. 群の二項演算の 3 性質は以下のように確かめられる:

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

さらに, $+$ は

- (IV) 任意の $[a]_n, [b]_n \in \mathbb{Z}/n\mathbb{Z}$ に対し, $[a]_n + [b]_n = [b]_n + [a]_n$

をみたすので, これは可換群である. また, $|\mathbb{Z}/n\mathbb{Z}| = n$ であったので, これは位数 n の有限群である.

例 5 ($\mathbb{Z}/n\mathbb{Z}$ の乗法群). 正の整数 n に対して, $(\mathbb{Z}/n\mathbb{Z}^\times, \times)$ は群である (\times が $(\mathbb{Z}/n\mathbb{Z}^\times)$ の二項演算として定義できることについては, 第 3 回講義資料命題 2.4(1) を参照). これは $\mathbb{Z}/n\mathbb{Z}$ の乗法群とよばれる. 群の二項演算の 3 性質は以下のように確かめられる:

- (I) (結合法則) 任意の $[a]_n, [b]_n, [c]_n \in (\mathbb{Z}/n\mathbb{Z}^\times)$ に対し, $([a]_n [b]_n) [c]_n = [abc]_n = [a]_n ([b]_n [c]_n).$
- (II) (単位元の存在) 単位元は $[1]_n \in (\mathbb{Z}/n\mathbb{Z}^\times)$ である. 実際, 任意の $[a]_n \in (\mathbb{Z}/n\mathbb{Z}^\times)$ に対し, $[1]_n [a]_n = [a]_n = [a]_n [1]_n$ が成立する.
- (III) (逆元の存在) 任意の $[a]_n \in (\mathbb{Z}/n\mathbb{Z}^\times)$ に対し, 第 3 回講義資料命題 2.4(2) より $[a]_n^{-1} \in (\mathbb{Z}/n\mathbb{Z}^\times)$ であって, $[a]_n^{-1} [a]_n = [1]_n = [a]_n [a]_n^{-1}$ が成立する.

第 3 回講義資料の定義 2.1 で $[1]_n$ を “1” としたのは, $[1]_n$ が単位元の満たすべき性質を満たすためだったのである. また, (III) の逆元の存在のために, $(\mathbb{Z}/n\mathbb{Z}, \times)$ ではなく, $(\mathbb{Z}/n\mathbb{Z}^\times, \times)$ を考える必要がある.

演算 \times は,

(IV) 任意の $[a]_n, [b]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ に対し, $[a]_n[b]_n = [b]_n[a]_n$

をみたすので, これは可換群である. また, 第3回講義資料命題 2.7 より, $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$ (φ はオイラーの φ 関数) であったので, これは位数 $\varphi(n)$ の有限群である.

例 6 (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.

$$GL_n(\mathbb{K}) := \{A \mid A \text{ は } \mathbb{K} \text{ を成分とする } n \times n \text{ 行列で, } \det A \neq 0\}.$$

ただし, $\det A$ は A の行列式. 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,

$$I_n A = A = A I_n \text{ が成立する.}$$

(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,

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

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確かめられる:

$I_n \in SL_n(\mathbb{K})$ 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,

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

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 3.5 より, $SL_n(\mathbb{K})$ は $GL_n(\mathbb{K})$ の部分群である.

注意 (群の定義補足 (興味のある方向へ)). 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

$$G' := \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a \in \mathbb{C}^\times, b \in \mathbb{C} \right\}$$

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, $e := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in G'$ 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 (『 $g = g \cdot e$ 』のみにしたものの), (III) の一部 (『 $g' \cdot g = e$ 』のみにしたものを) 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

$$e'g = \begin{pmatrix} e_1 & 0 \\ e_2 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} e_1a & 0 \\ e_2a & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = g$$

なので, 特に $e_2a = b$ 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.

代数学 I 第 5 回講義資料

担当：大矢 浩徳 (OYA Hironori)*

4.1 群と部分群の例 (その 2)

前回に引き続き、群と部分群の例について解説する。ただし、今回の例はこれまでに学んだものではなく、多くの方にとって群論の講義ではじめて目にするものではないかと思われる (n 次対称群は見たことがあるかもしれない)。既習の概念を新しい視点 (『群』) からとらえることも面白いが、新しい視点をもつことで初めて数学的に扱える対象を知るといってもまた面白いものである。

例 1. X を空でない集合とする。このとき、 X から X への全単射写像全体のなす集合

$$B(X) := \{f: X \rightarrow X \mid f \text{ は全単射}\}^{*1}$$

を考える。このとき、 $B(X)$ は写像の合成 \circ を二項演算として、群をなす。

復習

写像 $f: X \rightarrow Y$ が全単射であるとは、

(全射性) 任意の $y \in Y$ に対し、ある $x \in X$ が存在して、 $f(x) = y$ となり、かつ

(単射性) 任意の $x_1 \neq x_2$ なる $x_1, x_2 \in X$ に対して、 $f(x_1) \neq f(x_2)$ となる

ということである。このとき、各 $y \in Y$ に対し、 $f(x_y) = y$ となる $x_y \in X$ が必ずただ 1 つだけ存在するので、 y に対してこの x_y を対応させることで、写像 $Y \rightarrow X, y \mapsto x_y$ が得られる。これを f の逆写像といい、 f^{-1} と書く。

写像 $f: X \rightarrow Y, g: Y \rightarrow Z$ に対し、写像の合成 $g \circ f: X \rightarrow Z$ とは、

$$(g \circ f)(x) = g(f(x)), x \in X$$

で定まる写像である。 $f: X \rightarrow Y$ が全単射のとき、

$$f^{-1} \circ f = \text{id}_X \text{ かつ } f \circ f^{-1} = \text{id}_Y$$

である。ここで、 $\text{id}_Z: Z \rightarrow Z$ は恒等写像 $z \mapsto z$ ($Z = X$ or Y)。

- (I) (結合法則) 任意の $f, g, h \in B(X)$ と任意の $x \in X$ に対し、 $((f \circ g) \circ h)(x) = f(g(h(x))) = (f \circ (g \circ h))(x)$ なので、写像として $(f \circ g) \circ h = f \circ (g \circ h)$ 。
- (II) (単位元の存在) 単位元は $\text{id}_X \in B(X)$ である。実際、任意の $f \in B(X)$ と任意の $x \in X$ に対し、 $(\text{id}_X \circ f)(x) = f(x) = (f \circ \text{id}_X)(x)$ となるので、写像として $\text{id}_X \circ f = f = f \circ \text{id}_X$ が成立する。
- (III) (逆元の存在) 任意の $f \in B(X)$ に対し、 $f^{-1} \in B(X)$ であって、上の復習で見たように $f^{-1} \circ f = \text{id}_X = f \circ f^{-1}$ が成立する。

例 2 (n 次対称群). $n \in \mathbb{Z}_{>0}$ とする。 $X = \{1, 2, \dots, n\}$ のとき、例 1 で考えた群 $B(X) = B(\{1, 2, \dots, n\})$ を n 次対称群 (symmetric group pf degree n) といい、 \mathfrak{S}_n^{*2} と書く。

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

*1 この $B(x)$ という記号は標準的な記号ではなく、この講義で用いる記号である。

*2 この文字はドイツ文字の S である。

\mathfrak{S}_n の各元 σ は全単射写像 $\sigma: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ であるが, この写像は

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

としばしば書かれる. 例えば, \mathfrak{S}_3 の元

$$\begin{array}{ccc} \sigma: & \{1, 2, 3\} & \longrightarrow & \{1, 2, 3\} \\ & \cup & & \cup \\ & 1 & \longmapsto & 2 \\ & 2 & \longmapsto & 3 \\ & 3 & \longmapsto & 1 \end{array}$$

は $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ と書かれる. また, \mathfrak{S}_n の単位元 $\text{id}_{\{1, 2, \dots, n\}}$ は, $\begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$ である. この表示を用いると二項演算, つまり写像の合成は次のように計算することができる:

\mathfrak{S}_n における二項演算

$$\begin{pmatrix} 1 & 2 & \cdots & j_k & \cdots & n \\ i_1 & i_2 & \cdots & i_{j_k} & \cdots & i_n \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & \cdots & k & \cdots & n \\ j_1 & j_2 & \cdots & j_k & \cdots & j_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & k & \cdots & n \\ i_{j_1} & i_{j_2} & \cdots & i_{j_k} & \cdots & i_n \end{pmatrix}$$

例えば, \mathfrak{S}_3 においては,

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

となる. 右の元から順にたどって計算するということに注意をする (もともと写像の合成であったということをお忘れずに!). さらに, この例から \mathfrak{S}_3 は非可換群であるということもわかる. 一般に, $n \geq 3$ のとき, \mathfrak{S}_n は非可換群である. また, 一般に $\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$ の \mathfrak{S}_n における逆元は次のように求められる.

\mathfrak{S}_n における逆元の計算

(Step 1) $\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$ の上下をひっくり返して, $\begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ 1 & 2 & \cdots & n \end{pmatrix}$ を考える.

(Step 2) $\begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ 1 & 2 & \cdots & n \end{pmatrix}$ における上下のペアを保ったまま, 上段の数字を $1, \dots, n$ に並べ替える.

こうして得られる元が $\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}^{-1}$ である.

例えば,

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \xrightarrow{\text{(Step1)}} \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} \xrightarrow{\text{(Step2)}} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

と考えると, $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ である. 確かに,

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

となる. 一般に, 最初に取った元が k の下に i_k が書かれるものであった場合 (つまり $k \mapsto i_k$ という写像であった場合), この方法で出来上がる元は i_k に下に k が書かれる (つまり $i_k \mapsto k$ という写像になる) ため, 確かにこれで逆元が得られるということがわかる.

なお, n 次対称群は集合として

$$\mathfrak{S}_n := \left\{ \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \mid i_1, \dots, i_n \text{ は } 1, \dots, n \text{ を並べ替えたもの} \right\}$$

となっているので、その位数は $|\mathfrak{S}_n| = n!$ である。

巡回置換, 互換

$\sigma \in \mathfrak{S}_n$ が, ある $\{i_1, \dots, i_k\} \subset \{1, \dots, n\}$ に対して,

$$\sigma(i_s) = \begin{cases} i_{s+1} & s = 1, \dots, k-1 \text{ のとき,} \\ i_1 & s = k \text{ のとき,} \end{cases} \quad \sigma(j) = j, \quad j \in \{1, \dots, n\} \setminus \{i_1, \dots, i_k\} \text{ のとき,}$$

を満たすとき, σ を巡回置換 (cyclic permutation) といい, $\sigma = (i_1 \dots i_k)$ と書く. 特に $k = 2$, つまり, $(i_1 i_2)$ の形の元を互換 (transposition) といい, $(i \ i+1)$ の形の互換を隣接互換 (adjacent transposition) という.

例えば, $\sigma = (132) \in \mathfrak{S}_4$ は 1 を 3 に, 3 を 2 に, 2 を 1 に移し, その他は動かさない写像, つまり,

$$\begin{array}{ccc} \sigma: & \{1, 2, 3, 4\} & \longrightarrow & \{1, 2, 3, 4\} \\ & \Downarrow & & \Downarrow \\ & 1 & \longmapsto & 3 \\ & 2 & \longmapsto & 1 \\ & 3 & \longmapsto & 2 \\ & 4 & \longmapsto & 4 \end{array}$$

という写像を表す. つまり, $(132) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$ である. 他にも, $\sigma' = (24) \in \mathfrak{S}_4$ は

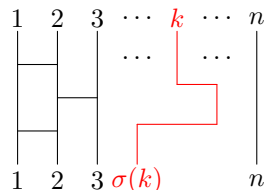
$$\begin{array}{ccc} \sigma': & \{1, 2, 3, 4\} & \longrightarrow & \{1, 2, 3, 4\} \\ & \Downarrow & & \Downarrow \\ & 1 & \longmapsto & 1 \\ & 2 & \longmapsto & 4 \\ & 3 & \longmapsto & 3 \\ & 4 & \longmapsto & 2 \end{array}$$

という写像を表す. つまり, $(24) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$ である. 一般に $(i \ j) \in \mathfrak{S}_n (i < j)$ は,

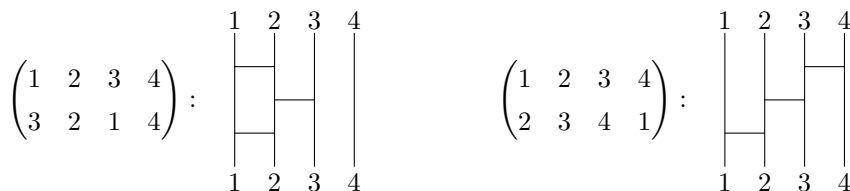
$$(i \ j) = \begin{pmatrix} 1 & \dots & i & \dots & j & \dots & n \\ 1 & \dots & j & \dots & i & \dots & n \end{pmatrix}$$

と対応する.

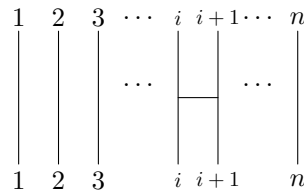
注意 (対称群とあみだくじの関係). 対称群 \mathfrak{S}_n の元は, 全単射写像 $\sigma := \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ であったが, これは k から始めると $\sigma(k)$ にたどり着くあみだくじとして表すこともできる (上から下に読む):



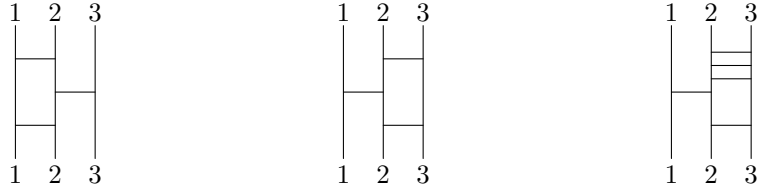
例えば, \mathfrak{S}_4 の次の元は以下のようなあみだくじと対応する:



また, \mathfrak{S}_n において, 隣接互換 $(i \ i+1)$ は以下のような横棒 1 本のあみだくじに対応する:

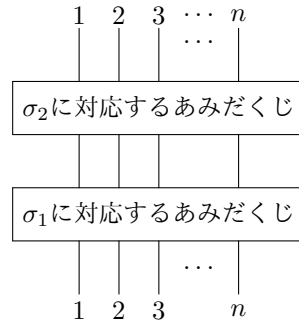


全ての \mathfrak{S}_n の元があみだくじで書けるということは非自明であるが、感覚的には OK であろう。実際にこれは正しい (厳密な証明は補足プリント“巡回置換について”を参照.)。なお、 \mathfrak{S}_n の元に対して、対応するあみだくじは 1 通りではない。例えば、



はどれも $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \in \mathfrak{S}_3$ に対応するあみだくじである。

$\sigma_1, \sigma_2 \in \mathfrak{S}_n$ に対し、 $\sigma_1 \circ \sigma_2$ に対応するあみだくじは、 σ_1, σ_2 に対応するあみだくじを次のように繋げたものとなる (順番注意!):



特に、あみだくじは n 本の縦棒に横棒をどんどん付けていって得られるので、上記の考察から、『全ての \mathfrak{S}_n の元があみだくじで書ける』ということは、『全ての \mathfrak{S}_n の元が隣接互換の合成で得られる』という主張に他ならないことに注意しよう。

$\sigma \in \mathfrak{S}_n$ に対し、 σ^{-1} に対応するあみだくじは、 σ に対応するあみだくじの上下をひっくり返したものとなる。

例 3 (n 次二面体群). 3 以上の整数 n に対し、 n 次対称群 \mathfrak{S}_n の元に以下のように名前を付ける:

$$\sigma := \begin{pmatrix} 1 & 2 & \cdots & k & \cdots & n-1 & n \\ 2 & 3 & \cdots & k+1 & \cdots & n & 1 \end{pmatrix} = (1 \ 2 \ \cdots \ n)$$

$$\tau := \begin{pmatrix} 1 & 2 & 3 & \cdots & k & \cdots & n-1 & n \\ 1 & n & n-1 & \cdots & n+2-k & \cdots & 3 & 2 \end{pmatrix}.$$

このとき、

$$D_n := \{e, \sigma, \sigma^2, \dots, \sigma^{n-1}, \tau, \sigma\tau, \sigma^2\tau, \dots, \sigma^{n-1}\tau\}$$

(e は \mathfrak{S}_n の単位元. 二項演算の記号 \circ は省略した. k 乗は k 回合成するという意味) は \mathfrak{S}_n の部分群となる。これを n 次二面体群 (**dihedral group of degree n**) という。まず、実際に部分群となることを確かめるために、 σ と τ の間の関係を記述しておこう:

命題 4.1

上記の σ と τ について以下が成立する。

- (1) $\sigma^n = e.$
- (2) $\tau^2 = e.$
- (3) $\tau\sigma = \sigma^{-1}\tau, \tau\sigma^{-1} = \sigma\tau.$

証明. 全て直接計算すれば良い. ここでは (3) の 1 つめの式だけ確かめてみよう. まず,

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & \cdots & k & \cdots & n-1 & n \\ n & 1 & \cdots & k-1 & \cdots & n-2 & n-1 \end{pmatrix}$$

である. これを踏まえると,

$$\begin{aligned} \tau\sigma &= \begin{pmatrix} 1 & 2 & 3 & \cdots & k & \cdots & n-1 & n \\ 1 & n & n-1 & \cdots & n+2-k & \cdots & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & k & \cdots & n-1 & n \\ 2 & 3 & \cdots & k+1 & \cdots & n & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & \cdots & k & \cdots & n-1 & n \\ n & n-1 & \cdots & n+1-k & \cdots & 2 & 1 \end{pmatrix} \\ \sigma^{-1}\tau &= \begin{pmatrix} 1 & 2 & \cdots & k & \cdots & n-1 & n \\ n & 1 & \cdots & k-1 & \cdots & n-2 & n-1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & \cdots & k & \cdots & n-1 & n \\ 1 & n & n-1 & \cdots & n+2-k & \cdots & 3 & 2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & \cdots & k & \cdots & n-1 & n \\ n & n-1 & \cdots & n+1-k & \cdots & 2 & 1 \end{pmatrix}. \end{aligned}$$

となるので, 確かに $\tau\sigma = \sigma^{-1}\tau$ である. □

命題 4.1 から D_n は二項演算と逆元を取る操作について閉じていることが以下のように確かめられる. これは第 4 回講義資料命題 3.5 より D_n が \mathfrak{S}_n の部分群であるということに他ならず, 特に D_n は群となる.

逆元を取る操作について閉じていること : まず命題 4.1 (1), (2) より,

- 各 $k = 0, \dots, n-1$ に対し, $(\sigma^k)^{-1} = \sigma^{n-k}$.
- $\tau^{-1} = \tau$.

である. また, 命題 4.1 (3) を繰り返し用いることで, 次がわかる.

- 任意の $k \in \mathbb{Z}$ に対し, $\tau\sigma^{-k} = \sigma^k\tau$.

さらに, 一般の群 G において以下が成立する :

命題 4.2

G を群とする. このとき, 任意の $g, h \in G$ に対し,

$$(gh)^{-1} = h^{-1}g^{-1}.$$

証明. $h^{-1}g^{-1}$ が gh の逆元の満たすべき性質を満たしていることを示せばよい.

$$\begin{aligned} (gh)(h^{-1}g^{-1}) &= g(hh^{-1})g^{-1} = geg^{-1} = gg^{-1} = e \\ (h^{-1}g^{-1})(gh) &= h^{-1}(g^{-1}g)h = h^{-1}eh = h^{-1}h = e. \end{aligned}$$

より, 確かに $h^{-1}g^{-1}$ は gh の逆元 $(gh)^{-1}$ である. □

以上より, D_n の元 $\sigma^k, \sigma^k\tau$ ($k = 0, \dots, n-1$) に対し,

$$\begin{aligned} (\sigma^k)^{-1} &= \sigma^{n-k} \in D_n \\ (\sigma^k\tau)^{-1} &= \tau^{-1}(\sigma^k)^{-1} = \tau\sigma^{-k} = \sigma^k\tau \in D_n \end{aligned}$$

となることがわかる.

二項演算で閉じていること : 一般に証明をしても良いが, 必要以上にややこしくなるので, 以下の D_7 の例で納得しよう. 逆元を取る操作について閉じていることの証明で述べた性質を用いれば良い :

$$\begin{aligned} \sigma^4\sigma^5 &= \sigma^9 = \sigma^2 \in D_7, & (\sigma^2\tau)\sigma^3 &= \sigma^2(\tau\sigma^3) = \sigma^2(\sigma^{-3}\tau) = \sigma^{-1}\tau = \sigma^6\tau \in D_7, \\ (\sigma^2\tau)(\sigma^4\tau) &= \sigma^2(\tau\sigma^4)\tau = \sigma^2(\sigma^{-4}\tau)\tau = \sigma^{-2}\tau^2 = \sigma^5 \in D_7. \end{aligned}$$

命題 4.1(3) から, D_n は非可換群であることがわかる (n は 3 以上なので, $\sigma^{-1} = \sigma^{n-1} \neq \sigma$). さらに, D_n は位数が $2n$ であることが構成からわかる. 実際には $\sigma^k, \sigma^k\tau$ ($k = 0, \dots, n-1$) が全て異なる元であることは

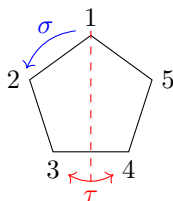
ここでは証明していないが、是非各自チェックしてみて欲しい。なお $n = 3$ のとき、 $\#D_3 = 2 \times 3 = 6$ で、 $\#S_3 = 3! = 6$ なので、 $D_3 = S_3$ である。 n が 4 以上の時は、 $D_n \subsetneq S_n$ である。

最後に、この群はいったい何なのか?ということの説明しておこう。 D_n は『正 n 角形の板』の対称性と考えることができる。『板』と言っている意味は、表と裏がある (= 二面体!) ということである。正 n 角形の板を保つ変換は

『 $\frac{2k\pi}{n}$ 回転』と、『(ある固定した対称軸に関して) 折り返してから $\frac{2k\pi}{n}$ 回転』 ($k = 0, 1, \dots, n-1$)

の $2n$ 個で全てである。このとき、 $\frac{2\pi}{n}$ 回転に対応するものが σ であり、ある固定した対称軸に関する折り返しに対応するものが τ である。こう考えると、 $\sigma^n = e$ や $\tau^2 = e$ といった性質に親しみがわくであろう。 $\tau\sigma = \sigma^{-1}\tau, \tau\sigma^{-1} = \sigma\tau$ も確かめてもらいたい。

D_5 の場合:



なぜこれが対称群 S_5 の部分群と思えるかというと、上図のように頂点の位置に反時計回りに番号をつけて、各変換によって『どの位置の頂点がどの位置の頂点に行くか』という情報を記録すれば、これは $\{1, \dots, n\} \rightarrow \{1, \dots, n\}$ という全単射を与えるからである。この対応を考えることで、 D_n は S_n の部分群として実現されていたのである。このことを念頭において σ と τ の定義を見直してみて欲しい。

代数学 I 第 6 回講義資料

担当：大矢 浩徳 (OYA Hironori)*

5.1 n 次対称群 (補足)

n を 2 以上の整数とし, \mathfrak{S}_n を n 次対称群とする. \mathfrak{S}_n の単位元を e と書く. 以下では \mathfrak{S}_n における二項演算の記号 \circ はしばしば省略する (つまり, $\sigma_1 \circ \sigma_2$ を単に $\sigma_1 \sigma_2$ と書いたりする).

復習 (第 5 回講義資料: 巡回置換, 互換)

$\sigma \in \mathfrak{S}_n$ が, ある $\{i_1, \dots, i_k\} \subset \{1, \dots, n\}$ に対して,

$$\sigma(i_s) = \begin{cases} i_{s+1} & s = 1, \dots, k-1 \text{ のとき,} \\ i_1 & s = k \text{ のとき,} \end{cases} \quad \sigma(j) = j, \quad j \in \{1, \dots, n\} \setminus \{i_1, \dots, i_k\} \text{ のとき,}$$

を満たすとき, σ を巡回置換 (cyclic permutation) といい, $\sigma = (i_1 \cdots i_k)$ と書く. 特に $k = 2$, つまり, $(i_1 i_2)$ の形の元を互換 (transposition) といい, $(i i+1)$ の形の互換を隣接互換 (adjacent transposition) という.

以下は, 定義から容易に導かれる巡回置換の基本性質である.

命題 5.1

巡回置換 $(i_1 i_2 \cdots i_k) \in \mathfrak{S}_n$ に対し, 以下が成立:

- (1) $(i_1 i_2 \cdots i_k)^{-1} = (i_k \cdots i_2 i_1)$.
- (2) $(i_1 i_2 \cdots i_k)^k = e$.

巡回置換 $\sigma = (i_1 \cdots i_k) \in \mathfrak{S}_n$ に対し,

$$S(\sigma) := \{i_1, \dots, i_k\} \subset \{1, \dots, n\}$$

とする. また単位元 e に対し, $S(e) := \emptyset$ とする. *1 例えば, $S((4 6 7)) = \{4, 6, 7\}$, $S((2 4 1)) = \{1, 2, 4\}$ である.

定義 5.2

\mathfrak{S}_n 内の巡回置換の組 $\sigma_1, \dots, \sigma_s$ が

$$\text{任意の } t \neq t' \text{ に対し, } S(\sigma_t) \cap S(\sigma_{t'}) = \emptyset$$

を満たすとする. このとき $\sigma_1, \dots, \sigma_s$ はどの 2 つも互いに素であると言われる.

例えば, $(2 4), (1 5), (3 6 8)$ はどの 2 つも互いに素な巡回置換である. 以下は巡回置換の定義から容易にわかる.

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

*1 これはこの講義だけの記号である.

命題 5.3

$\sigma_1, \dots, \sigma_s$ を \mathfrak{S}_n 内のどの 2 つも互いに素な巡回置換とする。このとき、

$$(\sigma_1 \cdots \sigma_s)(i) = \begin{cases} \sigma_t(i) & \text{ある } t \text{ について } i \in S(\sigma_t) \text{ となるとき,} \\ i & \text{全ての } t = 1, \dots, s \text{ に対して, } i \notin S(\sigma_t) \text{ のとき,} \end{cases}$$

となる。特に、 σ と σ' が互いに素な巡回置換のとき、それらは可換、つまり、

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

である。

以下の定理は重要であるが、厳密な証明は補足プリント“巡回置換について”に回す。(2) は任意の \mathfrak{S}_n の元に対して対応する『あみだくじ』があることを保証するものであり、内容としては“納得”しやすいであろう(第 5 回講義資料 p.3-4 の注意(対称群とあみだくじの関係)参照)。(1) については下の例 1 を参照のこと。

定理 5.4

n を 2 以上の整数とする。各 $i = 1, \dots, n-1$ に対し $s_i := (i \ i+1) \in \mathfrak{S}_n$ とする。このとき、以下が成立する：

- (1) 任意の \mathfrak{S}_n の単位元でない元はどの 2 つも互いに素な巡回置換の合成として書かれる。さらに、長さ 1 の巡回置換 (= 単位元) を用いないことにすると、合成の順序の違いを除いてこの表示は一意的である。
- (2) 任意の \mathfrak{S}_n の元は隣接互換 $s_i, i = 1, \dots, n-1$ らの合成として書かれる。

定理 5.4(2) においては、(1) のような表示の一意性が成り立たないことに注意する。例えば、 \mathfrak{S}_3 において、

$$s_1 s_2 s_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = s_2 s_1 s_2 = s_1 s_1 s_2 s_1 s_2 = \cdots$$

である。これは、各対称群の元に対して、対応するあみだくじは 1 通りではないという事実に対応する。

例 1. 定理 5.4(1) を証明する代わりに、以下の例でどのようにすれば任意の \mathfrak{S}_n の元をどの 2 つも互いに素な巡回置換の積として書くことができるのかを見て、定理 5.4(1) の正しさを“納得”しよう。実際に、厳密な証明も以下の方法を一般的な言葉に置き換えるだけである。

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 2 & 8 & 7 & 6 & 9 & 1 & 5 & 10 & 3 \end{pmatrix} \in \mathfrak{S}_{10}$$

とする。まず 1 をとる (これは実際には 1 でなくても何でも良い)。1 の σ による像を次々に計算する：

$$1 \xrightarrow{\sigma} 4 \xrightarrow{\sigma} 7 \xrightarrow{\sigma} 1$$

上のように初めに取った 1 に戻ってきたところでストップする (必ず初めの数字にいつか戻る)。次に、上の過程で現れていない数字を任意にとる。ここでは 2 を取る。そして、上と同様に 2 の σ による像を計算する：

$$2 \xrightarrow{\sigma} 2$$

これは、1 回で初めに取った数字に戻ってくる (つまり動かさない) のでここでストップする。さらに、上の過程でまだ今まで一度も出てきてない数字を任意にとる。ここでは 3 をとる。そして、上と同様に 3 の σ による像を次々に計算する：

$$3 \xrightarrow{\sigma} 8 \xrightarrow{\sigma} 5 \xrightarrow{\sigma} 6 \xrightarrow{\sigma} 9 \xrightarrow{\sigma} 10 \xrightarrow{\sigma} 3$$

同様に初めに取った 3 に戻ってくるのでそこでストップする。ここで、 $1, \dots, 10$ の全ての数が出そろったので、以上の反復の過程をストップする。

以上の過程で出てきた数字のサイクルをその順に並べて巡回置換を作り、その合成をとる。

$$(1 \ 4 \ 7)(2)(3 \ 8 \ 5 \ 6 \ 9 \ 10) = (1 \ 4 \ 7)(3 \ 8 \ 5 \ 6 \ 9 \ 10)$$

すると、こうして得られる巡回置換たちはその作り方から(どの2つも)互いに素であり、さらに命題 5.3 から写像として σ と一致する。よって、

$$\sigma = (1\ 4\ 7)(3\ 8\ 5\ 6\ 9\ 10)$$

であり、確かに σ を互いに素な巡回置換の合成として書くことができた。

上記の方法は任意の $\sigma \in \mathfrak{S}_n$ に対して通用する方法である。

5.2 抽象的な部分群の構成

群論の一般論に戻ろう。これまで、様々な群と部分群を見てきたが、群が与えられたときにその部分群を構成するいくつかの一般論について説明を行う。以下では、 G を群とし、その単位元を e と書く。さらに、 $g, h \in G$ に対し、それらの二項演算による像を単に gh と書き(つまり、二項演算の記号 \cdot や \circ 等は省略する)、 g と h を『掛ける』という言い方をすることにする。

5.2.1 自明な部分群

まず、面白いものではないが忘れてはいけないものとして、

- 単位元のみからなる G の部分集合 $\{e\}$
- G 自身

はどちらも G の部分群である。これらを G の自明な部分群という。

5.2.2 部分集合の生成する部分群

定義 5.5

S を群 G の任意の部分集合とする(部分群とは限らない)。このとき、

$$\langle S \rangle := \{g_1^{m_1} \cdots g_k^{m_k} \mid g_i \in S, m_i \in \mathbb{Z} (i = 1, \dots, k), k \in \mathbb{N}\} (\subset G)$$

とする。言葉で書くと、 $\langle S \rangle$ は『 S の元とその逆元たちを何度も掛けてできるもの全てを集めてきてできる集合』となる。このとき、 $\langle S \rangle$ は定義から明らかに二項演算と逆元を取る操作で閉じており、 G の部分群となる。これを、 S で生成される部分群という。

例えば、 S が $S = \{a, b, c\}$ という3つの元からなる集合であった場合、 $\langle S \rangle$ は

$$e(= a^0), a, ab^2, ac^2b^{-3}a, b^4c^{-2}a^{-1}b^2c^4b^2c^{-6}a, c^{-2}, \dots$$

などをとにかく全て集めてきてできる集合である。こう考えると、二項演算と逆元を取る操作で閉じているということは自明であろう(例えば、 ab^2 と $ac^2b^{-3}a$ を掛けてできる元は $ab^2ac^2b^{-3}a$ なのでやはり $\langle S \rangle$ の元であり、 $b^4c^{-2}a^{-1}b^2c^4b^2c^{-6}a$ の逆元 $a^{-1}c^6b^{-2}c^{-4}b^{-2}ac^2b^{-4}$ も $\langle S \rangle$ の元である)。

ここで、 S を含む部分群があるとすれば、二項演算と逆元を取る操作で閉じていないといけなことから、それは上記のような $\langle S \rangle$ という集合を必ず含んでいるはずである。よって、 $\langle S \rangle$ は S を含む部分群で最小のものである。

例 2.

(1) $S = \{s_1, s_2, \dots, s_{n-1}\} \subset \mathfrak{S}_n$ としたとき、定理 5.4(2) より、

$$\langle S \rangle = \mathfrak{S}_n$$

である。

- (2) $D_n = \{e, \sigma, \sigma^2, \dots, \sigma^{n-1}, \tau, \sigma\tau, \sigma^2\tau, \dots, \sigma^{n-1}\tau\}$ を n 次二面体群とする ($n \geq 3$, 第5回講義資料例3と同じ記号を用いる). このとき, 具体的な群の元の形より明らかに,

$$\langle \{\sigma, \tau\} \rangle = D_n$$

である. また, D_n において,

$$\langle \{\sigma\} \rangle = \{\sigma^m \mid m \in \mathbb{Z}\} = \{e, \sigma, \sigma^2, \dots, \sigma^{n-1}\}$$

である.

例2の(2)の後半の例のように, G の1元からなる部分集合 $\{g\}$ で生成される部分群は,

$$\langle \{g\} \rangle = \{g^m \mid m \in \mathbb{Z}\}$$

となる. これを単に $\langle g \rangle$ と書く. $g^m g^{m'} = g^{m+m'} = g^{m'} g^m$ なので $\langle g \rangle$ は可換群である. また, 一般に $\langle g \rangle = \langle g^{-1} \rangle$.

定義 5.6

ある $g \in G$ が存在して, $G = \langle g \rangle$ となるとき, G を巡回群 (cyclic group) といい, g を G の生成元 (generator) という.

上の考察より, 巡回群は可換群である. また, 生成元の取り方は1つとは限らない ($\langle g \rangle = \langle g^{-1} \rangle$ なので, g が生成元であれば少なくとも g^{-1} は生成元である).

定義 5.7

各 $g \in G$ に対し, G の部分群 $\langle g \rangle$ の位数を g の位数 (order) といい, $\text{ord } g$ と書く.

一般に, $\langle g \rangle = \langle g^{-1} \rangle$ なので, $\text{ord } g = \text{ord } g^{-1}$ である. ここで, 『位数』という用語が群論において2通り現れたことに注意しよう. G の位数 (= G の集合としての元の個数) と, G の元 g の位数 (上で定義したもの) という概念があるのである. 以下の命題は定義からすぐわかる.

命題 5.8

群 G の元 g に対し, 以下の同値関係が成立する:

- $\text{ord } g = 1 \Leftrightarrow g = e$.
- $\text{ord } g = \#G \Leftrightarrow G$ は巡回群で, その生成元は g .

例 3.

- $\mathbb{Z}/n\mathbb{Z} = \langle [1]_n \rangle$ であるので, $\mathbb{Z}/n\mathbb{Z}$ は巡回群であり, $[1]_n$ は $\mathbb{Z}/n\mathbb{Z}$ の生成元である. ここで, $\mathbb{Z}/n\mathbb{Z}$ においては, 二項演算が $+$ であることに注意. $\text{ord}[1]_n = n$.
- $\mathbb{Z} = \langle 1 \rangle$ であるので, \mathbb{Z} は巡回群であり, 1 は \mathbb{Z} の生成元である. ここで, \mathbb{Z} においては, 二項演算が $+$ であることに注意. $\text{ord } 1 = \infty$.
- $n \in \mathbb{Z}_{>0}$ に対し, \mathbb{C}^\times の部分群 $\mu_n := \{e^{\frac{2\pi m}{n}i} \mid m \in \mathbb{Z}\}$ を考える. このとき, $\mu_n = \langle e^{\frac{2\pi}{n}i} \rangle$ であるので, μ_n は巡回群であり, $e^{\frac{2\pi}{n}i}$ は μ_n の生成元である. $\text{ord } e^{\frac{2\pi}{n}i} = n$.
- $n \geq 3$ のとき, 二面体群 D_n は非可換群なので, D_n は特に巡回群ではない. 例2(2)より, D_n において, $\text{ord } \sigma = n$ である. また,

$$\langle \tau \rangle = \{\tau^m \mid m \in \mathbb{Z}\} = \{e, \tau\}$$

より, $\text{ord } \tau = 2$ である.

群の元 g の位数 $\text{ord } g$ の計算は以下の命題を頭に置いておくとやりやすい.

命題 5.9

群 G の元 g に対し, $\text{ord } g$ は $g^m = e$ となる最小の正の整数 m である. ただし, $g^m = e$ となる正の整数が存在しないとき, $\text{ord } g = \infty$ である.

証明. $\text{ord } g = \#\langle g \rangle < \infty$ のとき, ある $m_1, m_2 \in \mathbb{Z}, m_1 < m_2$ が存在して,

$$g^{m_1} = g^{m_2}$$

となる. このとき, 両辺に g^{-m_1} を掛けると,

$$e = g^{m_2 - m_1}$$

なので, $g^m = e$ となる正の整数 m は少なくとも 1 つは存在することがわかる. このうち最小のものを ℓ とすると,

$$\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\} = \{e, g, \dots, g^{\ell-1}\}$$

である. いま示すべきことは, $\ell = \text{ord } g$ なので, あとは $e, g, \dots, g^{\ell-1}$ が全て異なる元であることを示せばよい. もし, $g^{k_1} = g^{k_2}$ ($0 \leq k_1 < k_2 \leq \ell - 1$) となったとすると, 両辺に g^{-k_1} を掛けることで, $e = g^{k_2 - k_1}$ となるが, $0 < k_2 - k_1 \leq \ell - 1$ なので, これは ℓ の最小性に矛盾する. よって, $0 \leq k_1 < k_2 \leq \ell - 1$ のとき $g^{k_1} = g^{k_2}$ とはならない. よって, $\ell = \text{ord } g$ であることが示された.

また, 上の議論により, $\text{ord } g < \infty$ のとき, $g^m = e$ となる正の整数は存在するので, $g^m = e$ となる正の整数が存在しないのであれば, $\text{ord } g = \infty$ である. \square

例 4. 巡回置換 $(i_1 i_2 \cdots i_k) \in \mathfrak{S}_n$ に対し,

$$(i_1 i_2 \cdots i_k)^m \neq e \quad (1 \leq m \leq k-1) \quad (i_1 i_2 \cdots i_k)^k = e$$

である. (前半は定義より容易にわかる. 例えば, i_1 の行き先を考えれば良い. 後半は命題 5.1 (2).) よって, $(i_1 i_2 \cdots i_k)^m = e$ となる最小の整数は k である. よって,

$$\text{ord}(i_1 i_2 \cdots i_k) = k. \quad (*)$$

一般に $\sigma_1, \dots, \sigma_s$ をどの 2 つも互いに素な巡回置換とする. このとき, 命題 5.3 の互いに素な巡回置換の可換性より, 各 $m \in \mathbb{Z}$ に対し,

$$(\sigma_1 \cdots \sigma_s)^m = \sigma_1^m \cdots \sigma_s^m$$

が成立する. このことから, $\#S(\sigma_1), \dots, \#S(\sigma_s)$ の最小公倍数を ℓ とすると, (*) より,

$$\text{ord}(\sigma_1 \cdots \sigma_s) = \ell$$

である. 例えば, 例 1 で扱った $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 2 & 8 & 7 & 6 & 9 & 1 & 5 & 10 & 3 \end{pmatrix} \in \mathfrak{S}_{10}$ を考えると,

$$\sigma = (1 \ 4 \ 7)(3 \ 8 \ 5 \ 6 \ 9 \ 10)$$

であり, $\#S((1 \ 4 \ 7)) = 3, \#S((3 \ 8 \ 5 \ 6 \ 9 \ 10)) = 6$ なので,

$$\text{ord } \sigma = 6$$

である. 実際, $\sigma^6 = (1 \ 4 \ 7)^6 (3 \ 8 \ 5 \ 6 \ 9 \ 10)^6 = e \cdot e = e$ である.

5.2.3 中心, 中心化群

定義 5.10

群 G に対し,

$$Z(G) := \{z \in G \mid zg = gz, \forall g \in G\}$$

とする. 言葉で書くと, $Z(G)$ は『 G の全ての元と可換性を持つ元全てを集めてきてできる集合』である. このとき, $Z(G)$ は G の部分群となり (証明は以下), G の中心 (**center**) と呼ばれる*2.

より一般に, S を群 G の任意の部分集合とする (部分群とは限らない). このとき,

$$Z(S) := \{z \in G \mid zs = sz, \forall s \in S\}$$

とする. 言葉で書くと, $Z(S)$ は『 S の全ての元と可換性を持つ元全てを集めてきてできる集合』となる. このとき, $Z(S)$ は G の部分群となり, G における S の中心化群 (**centralizer**) と呼ばれる.

命題 5.11

群 G とその部分集合 S に対し, S の中心加群 $Z(S)$ は G の部分群である.

証明. まず, 単位元の定義より $es = s = se, \forall s \in S$ なので, $e \in Z(S)$ であり, とくに $Z(S) \neq \emptyset$ である. さらに $z_1, z_2 \in Z(S)$ と任意の $s \in S$ に対し,

$$\begin{aligned} (z_1 z_2) s &= z_1 (z_2 s) = z_1 (s z_2) = (z_1 s) z_2 = (s z_1) z_2 = s (z_1 z_2), \\ z_1^{-1} s &= z_1^{-1} s z_1 z_1^{-1} = z_1^{-1} z_1 s z_1^{-1} = s z_1^{-1}. \end{aligned}$$

となるので, $z_1 z_2, z_1^{-1} \in Z(S)$. よって, 二項演算と逆元を取る操作について閉じているので, $Z(S)$ は G の部分群である. \square

例 5.

- 一般の群 G に対し,

$$Z(\{e\}) = \{z \in G \mid ze = ez\} = G$$

である.

- $\mathbb{K} = \mathbb{Q}, \mathbb{R}$ 又は \mathbb{C} のとき,

$$Z(GL_2(\mathbb{K})) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{K}^\times \right\}$$

である. これは以下のように確かめられる:

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{K})$ で $b \neq 0$ 又は $c \neq 0$ のとき,

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 2a & 2b \\ c & d \end{pmatrix} \neq \begin{pmatrix} 2a & b \\ 2c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}.$$

となるので, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \notin Z(GL_2(\mathbb{K}))$. よって, $Z(GL_2(\mathbb{K}))$ の元は $b = c = 0$ を満たす対角行列.

次に, $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in GL_2(\mathbb{K})$ で $a \neq d$ のとき,

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & d \\ 0 & d \end{pmatrix} \neq \begin{pmatrix} a & a \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

*2 $Z(G)$ の Z はドイツ語の Zentrum に由来.

となるので, $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \notin Z(GL_2(\mathbb{K}))$. よって, $Z(GL_2(\mathbb{K}))$ の元は $a = d$ を満たす正則な対角行列, つまり単位行列の 0 でない定数倍の形をしているもののみ. 逆に, 単位行列の 0 でない定数倍が任意の $GL_2(\mathbb{K})$ の元と可換であることは容易にわかるので, 結局 $Z(GL_2(\mathbb{K})) = \{aI_2 \mid a \in \mathbb{K}^\times\}$ である. 同様の方法で,

$$Z(GL_n(\mathbb{K})) = \{aI_n \mid a \in \mathbb{K}^\times\}$$

であることがわかる.

- $n \geq 3$ のとき,

$$Z(\mathfrak{S}_n) = \{e\}$$

である. これは以下のように確かめられる:

\mathfrak{S}_n の単位元でない元 $\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$ を取ってくる,

(i) ある $k = 1, \dots, n-1$ が存在して, $k \neq i_k$ かつ $k+1 \neq i_k$ となる,

(ii) ある $k = 1, \dots, n-1$ が存在して $\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} = \begin{pmatrix} 1 & \cdots & k-1 & k & \cdots & n-1 & n \\ 1 & \cdots & k-1 & k+1 & \cdots & n & k \end{pmatrix}$

のいずれかが成立する (理由を考えよ). (i) のとき,

$$\begin{aligned} & \left((k \ k+1) \circ \begin{pmatrix} 1 & \cdots & k & \cdots & n \\ i_1 & \cdots & i_k & \cdots & i_n \end{pmatrix} \right) (k) = i_k, \\ & \left(\begin{pmatrix} 1 & \cdots & k+1 & \cdots & n \\ i_1 & \cdots & i_{k+1} & \cdots & i_n \end{pmatrix} \circ (k \ k+1) \right) (k) = i_{k+1}, \end{aligned}$$

となるので,

$$(k \ k+1) \circ \begin{pmatrix} 1 & \cdots & n \\ i_1 & \cdots & i_n \end{pmatrix} \neq \begin{pmatrix} 1 & \cdots & n \\ i_1 & \cdots & i_n \end{pmatrix} \circ (k \ k+1).$$

これより, $\begin{pmatrix} 1 & \cdots & n \\ i_1 & \cdots & i_n \end{pmatrix} \notin Z(\mathfrak{S}_n)$. (ii) で $k = 1$ のとき,

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} = (1 \ 2 \ \cdots \ n)$$

であるが, このとき, n が 3 以上であることに注意すると,

$$((1 \ 2) \circ (1 \ 2 \ \cdots \ n))(2) = 3 \quad ((1 \ 2 \ \cdots \ n) \circ (1 \ 2))(2) = 2$$

より, $(1 \ 2) \circ (1 \ 2 \ \cdots \ n) \neq (1 \ 2 \ \cdots \ n) \circ (1 \ 2)$ なので, $(1 \ 2 \ \cdots \ n) \notin Z(\mathfrak{S}_n)$. (ii) で $k > 1$ のとき,

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} = (k \ k+1 \ \cdots \ n)$$

であるが, このとき,

$$((k-1 \ k) \circ (k \ k+1 \ \cdots \ n))(k) = k+1 \quad ((k \ k+1 \ \cdots \ n) \circ (k-1 \ k))(k) = k-1$$

より, $(k-1 \ k) \circ (k \ k+1 \ \cdots \ n) \neq (k \ k+1 \ \cdots \ n) \circ (k-1 \ k)$ なので, $(k \ k+1 \ \cdots \ n) \notin Z(\mathfrak{S}_n)$.

以上より, $Z(\mathfrak{S}_n)$ に含まれる元は単位元のみである.

ちなみに一般に中心を求める簡単な方法があるというわけではなく, その都度上のように“頑張る” 求める必要がある.

代数学 I 第 7 回講義資料

担当：大矢 浩徳 (OYA Hironori)*

今回は大学で学ぶ数学において非常に重要な『同値関係による商集合』という考え方を学ぶ。これまでは群と部分群の例を多数見てきたが、部分群を用いると、群自身に『同値関係』を入れることができる。これは、いわば群の元をいくつかの『種類』に分けるといようなものである。実はこれが群の構造を調べる際に非常に手段となる。この考え方を導入すると、例えば次のようなことがわかるようになる (これらはほんの一例である)：

- 位数が $n (< \infty)$ の群 G の部分群の位数は必ず n の約数である (Lagrange の定理)。特に、 $\text{ord } g$ は必ず n の約数であり、 G の全ての元は $g^n = e$ を満たす。
- 位数が素数 p の群は “本質的に” (数学語で言うと『同型なものを同一視すると』) $\mathbb{Z}/p\mathbb{Z}$ しかない。

また、部分群による同値関係によって群の性質がわかるというだけでなく、そこから得られる『商集合』 (これは一般には群ではない) 自体が重要な集合・空間となることもある。群から作られる集合・空間ということで、この方法で非常に良い対称性を持った集合・空間が得られるのである。例えば、円や球面といった空間は群の『商集合』として作ることができる。本講義の範囲を超えてしまうが、興味のある方は例えば “等質空間” というようなキーワードで調べてもらいたい。

6.1 同値関係

定義 6.1

S を集合とする。任意の $x, y \in S$ に対し、

$$x \sim y \quad \text{または} \quad x \not\sim y$$

のいずれかが定まっているとする。このとき \sim を S 上の関係 (relation) という*1。ここで、これが以下の 3 条件を満たすとき、 \sim を同値関係 (equivalence relation) という：

- (反射律) 任意の $x \in S$ に対して $x \sim x$ 。
- (対称律) $x \sim y$ ならば $y \sim x$ 。
- (推移律) $x \sim y$ かつ $y \sim z$ ならば $x \sim z$ 。

例 1. 集合 S において、イコール $=$ は同値関係。

- (反射律) 任意の $x \in S$ に対して $x = x$ 。
- (対称律) $x = y$ ならば $y = x$ 。

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

*1 S 上の関係はより厳密には以下のように定義される：

S 上の関係とは、 $S \times S$ の部分集合 R のことである。

$x, y \in S$ に対して、 $(x, y) \in R$ のとき $x \sim y$ 、 $(x, y) \notin R$ のとき $x \not\sim y$ と書くことにすれば、確かに任意の $x, y \in S$ に対して、 $x \sim y$ または $x \not\sim y$ のいずれかが成立すると言える。

(iii) (推移律) $x = y$ かつ $y = z$ ならば $x = z$.

例 2. n を正の整数とする. 整数のなす集合 \mathbb{Z} において,

$$a \sim_n b \Leftrightarrow a - b \text{ が } n \text{ の倍数} (\Leftrightarrow [a]_n = [b]_n)$$

とすると, \sim_n は \mathbb{Z} 上の同値関係.

(i) (反射律) 任意の $x \in \mathbb{Z}$ に対して $x \sim_n x$.

(ii) (対称律) $x - y$ が n の倍数ならば $y - x = -(x - y)$ も n の倍数.

(iii) (推移律) $x - y$ が n の倍数, $y - z$ が n の倍数ならば $x - z = (x - y) + (y - z)$ も n の倍数.

例 3. 実数のなす集合 \mathbb{R} において, 不等号 \leq は同値関係ではない. なぜなら, 『 $x \leq y$ ならば, $y \leq x$ 』は一般に成り立たないからである. なお, 反射律と推移律は満たされる.

例 4. 実数のなす集合 \mathbb{R} において,

$$x \sim y \Leftrightarrow xy > 0$$

とすると, \sim は同値関係ではない. なぜなら, $0 \times 0 = 0$ より, $0 \not\sim 0$ となって, 反射律が満たされないためである. なお, 対称律と推移律は満たされる.

例 5. $S = \{ \text{システム理工学部の学生} \}$ において,

$$a \sim b \Leftrightarrow a \text{ さんは } b \text{ さんと同じ学科である}$$

とすると, \sim は S 上の同値関係.

(i) (反射律) a さんは a さんと同じ学科である.

(ii) (対称律) a さんは b さんと同じ学科ならば, b さんは a さんと同じ学科である.

(iii) (推移律) a さんは b さんと同じ学科, b さんは c さんと同じ学科ならば, a さんは c さんと同じ学科である.

しかし,

$$a \sim' b \Leftrightarrow a \text{ さんは } b \text{ さんと一緒に遊んだことがある}$$

とすると, これは一般には同値関係ではない. なぜなら, 『 a さんは b さんと一緒に遊んだことがあって, b さんは c さんと一緒に遊んだことがあったとしても, a さんが c さんと一緒に遊んだことがない』ことがあるため*2, 推移律が成り立たないためである.

*2 私の勝手な想像ですが, 一般には良くあることだと思って書いています.

定義 6.2

集合 S 上に同値関係 \sim が定まっているとする。このとき、 $x \in S$ に対し、

$$C(x) := \{y \in S \mid y \sim x\} (\subset S)$$

とし、これを x の同値類 (equivalence class) という。 $C(x)$ の各元 $y \in C(x)$ は $C(x)$ の代表元 (representative) と呼ばれる。さらに、

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

とし、 S/\sim を S の \sim による商集合 (quotient set) という。言葉で書くと、 S/\sim は『 S における \sim に関する同値類を集めてきてできる集合』である。写像

$$p: S \rightarrow S/\sim, x \mapsto C(x)$$

を商写像 (quotient map) という。商写像は定義から明らかに全射である。さらに、 S の部分集合 R が S/\sim の各元 (同値類) の代表元をちょうど 1 つずつ含むとき、 R を \sim の完全代表系 (complete set of representatives) という。

例 6. 例 5 の同値関係 \sim の場合に、上で定義した諸概念を見てみよう。まず、 $a \in S$ に対し、

$$C(a) := \{b \in S \mid b \text{さんは} a \text{さんと同じ学科である}\}$$

となるので、 a の同値類は a さんが所属する学科の全員からなる S の部分集合となる。このため、商集合は

$$\begin{aligned} S/\sim &:= \{C(a) \mid a \in S\} \\ &= \{\text{電子情報システム学科, 機械制御システム学科, 環境システム学科, 生命科学科, 数理科学科}\} \end{aligned}$$

となる。商集合とはこのように、『 \sim によって定まるクラスの集まり』と考えれば良い。商写像 $p: S \rightarrow S/\sim$ は $a \mapsto (a \text{さんの所属する学科})$ という対応を与える写像である。完全代表系とは各学科からちょうど 1 人ずつの代表者を選んできてできる S の部分集合のことである。この例からも明らかなように完全代表系の選び方は沢山ある。

例 7. 例 2 の同値関係 \sim_n の場合に、上で定義した諸概念を見てみよう。まず、同値類は

$$C(0) = \{nk \mid k \in \mathbb{Z}\}, C(1) = \{nk + 1 \mid k \in \mathbb{Z}\}, C(2) = \{nk + 2 \mid k \in \mathbb{Z}\}, \dots$$

となる。言葉で言うと、同値類は『 n で割った余りが等しいものの集まり』である。この意味を考えれば明らかなように、任意の $k \in \mathbb{Z}$ に対し、 $C(k) = C(k+n)$ が成立する。これより、

$$\mathbb{Z}/\sim_n := \{C(a) \mid a \in \mathbb{Z}\} = \{C(0), C(1), \dots, C(n-1)\}$$

である。例えば、 $\mathbb{Z}/\sim_3 = \{C(0), C(1), C(2)\}$ などである。この例では、 0 は $C(0)$ の代表元、 5 は $C(2)$ の代表元、 -2 は $C(1)$ の代表元、... となり、例えば、 $\{0, 5, -2\}$ は \sim_3 の完全代表系である。

なお、 \sim_n に関して、 $C(k)$ を $[k]_n$ と書くことにすると、 $[k]_n = [k+n]_n$ 等も成立しており、 \mathbb{Z}/\sim_n は $\mathbb{Z}/n\mathbb{Z}$ と同一視できるものであるということに着目しておこう。実際、この見方が $\mathbb{Z}/n\mathbb{Z}$ の捉え方の 1 つであるということは今後説明をする。

以下は同値類の基本性質である。

命題 6.3

集合 S 上に同値関係 \sim が定まっているとする。このとき以下が成立する：

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

証明. (1) 定義より, $y \sim x, z \sim x$ なので, 対称律より $x \sim z$ で, 推移律より, $y \sim z$ である. \square

(2) $y \sim x$ のとき, 対称律より $x \sim y$ でもあり, このとき, 推移律から,

$$z \sim x \Leftrightarrow z \sim y$$

よって, 定義より $C(x) = \{z \in S \mid z \sim x\} = \{z \in S \mid z \sim y\} = C(y)$. \square

(3) $C(x) \cap C(y) \neq \emptyset$ のとき, $z \in C(x) \cap C(y)$ とすると, (2) より, $C(x) = C(z) = C(y)$. \square

命題 6.3 より, 同値関係 \sim の定まった集合 S は同値類によって, 『交わりのないクラス分け』がされているということがわかる. これは例 6, 例 7 から納得できるものであろう.

6.2 剰余類, Lagrange の定理 (前半)

さて, 話を群論に戻そう. 以下では G を群, $e \in G$ をその単位元とする. また, H を G の部分群とする. H を用いて, G に次のように同値関係を定めることができる:

定義 6.4

$g, g' \in G$ に対し,

$$g \stackrel{H}{\sim}_L g' \Leftrightarrow \text{ある } h \in H \text{ が存在して, } g = g'h,$$

$$g \stackrel{H}{\sim}_R g' \Leftrightarrow \text{ある } h \in H \text{ が存在して, } g = hg',$$

とする. $g \stackrel{H}{\sim}_L g'$ のとき, g は g' に (H に関して) 左合同といい, $g \stackrel{H}{\sim}_R g'$ のとき, g は g' に (H に関して) 右合同という*3.

命題 6.5

$\stackrel{H}{\sim}_L$ と $\stackrel{H}{\sim}_R$ は G 上の同値関係である.

証明. $\stackrel{H}{\sim}_L$ の場合のみ示す. $\stackrel{H}{\sim}_R$ の証明は全く同様である. $\stackrel{H}{\sim}_L$ が反射率, 対称律, 推移律を満たすことを示せばよい.

(i) (反射律) 部分群 H は G の単位元 e を必ず含むので (命題 3.4(3)), 任意の $g \in G$ に対して, $e \in H$ を取ると, $g = ge$. よって, $g \stackrel{H}{\sim}_L g$.

(ii) (対称律) $g \stackrel{H}{\sim}_L g'$ とすると, 定義より, ある $h \in H$ が存在して, $g = g'h$. この式の両辺に右から h^{-1} を掛けると, $g' = gh^{-1}$. ここで, H は部分群であることから, 逆元を取る操作について閉じているので, $h^{-1} \in H$. よって, $g' \stackrel{H}{\sim}_L g$.

(iii) (推移律) $g \stackrel{H}{\sim}_L g', g' \stackrel{H}{\sim}_L g''$ とすると, 定義より, ある $h, h' \in H$ が存在して, $g = g'h, g' = g''h'$. このとき, $g = g''h'h$ となるが, いま H は部分群であることから, 二項演算で閉じているので, $h'h \in H$. よって, $g \stackrel{H}{\sim}_L g''$.

以上より, 示すべきことは全て示された. \square

命題 6.5 の証明内では, H が部分群であること, すなわち, 空集合ではなく (=単位元を含み), 二項演算と逆元を取る操作について閉じているという事実を本質的に使っていることに注意しよう. H が部分群であることが, 定義 6.4 の方法で同値関係を入れられることを保証しているのである.

*3 h が右にあるとき左合同, h が左にあるとき右合同という名前がついていてややこしいが, これは誤植ではない.

定義 6.6

G 上の同値関係 $\overset{H}{\sim}_L, \overset{H}{\sim}_R$ による商集合はそれぞれ,

$$G/H := G/\overset{H}{\sim}_L \qquad H \backslash G := G/\overset{H}{\sim}_R$$

と書かれる. また, 各 $g \in G$ に対し, $\overset{H}{\sim}_L, \overset{H}{\sim}_R$ に関する g の同値類は, それぞれ

$$\begin{aligned} \{g' \in G \mid g' \overset{H}{\sim}_L g\} &= \{gh \mid h \in H\} =: gH \\ \{g' \in G \mid g' \overset{H}{\sim}_R g\} &= \{hg \mid h \in H\} =: Hg \end{aligned}$$

と書かれる. つまり,

$$G/H = \{gH \mid g \in G\} \qquad H \backslash G = \{Hg \mid g \in G\}$$

である. gH を g の H による左剰余類 (**left coset**) といい, Hg を g の H による右剰余類 (**right coset**) という. G/H の元の個数 $\#(G/H)$ を H の G における指数 (**index**) といい, $(G:H)$ と書く. また, $\overset{H}{\sim}_L$ の完全代表系を左完全代表系 (**complete set of left coset representatives**), $\overset{H}{\sim}_R$ の完全代表系を右完全代表系 (**complete set of right coset representatives**) という.

例 8. n を正の整数とする. 加法群 \mathbb{Z} と n の倍数全体からなる部分群 $\langle n \rangle = \{nk \mid k \in \mathbb{Z}\} (=: n\mathbb{Z})$ に関して, 定義 6.6 で定義された諸概念を見てみよう. 各 $a \in \mathbb{Z}$ に対して, a の $n\mathbb{Z}$ による左剰余類は (加法群の二項演算は $+$ であったことに注意すると),

$$a + n\mathbb{Z} = \{a + nk \mid k \in \mathbb{Z}\}$$

であり, 右剰余類は,

$$n\mathbb{Z} + a = \{nk + a \mid k \in \mathbb{Z}\} = a + n\mathbb{Z}$$

である. よって, このときには左剰余類と右剰余類の違いはない. 一般に可換群においては, 左剰余類と右剰余類の違いはないことが定義からすぐにわかるであろう. 商集合は,

$$\mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} \mid a \in \mathbb{Z}\} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}\}$$

である. よって, $n\mathbb{Z}$ の \mathbb{Z} における指数は $(\mathbb{Z} : n\mathbb{Z}) = \#(\mathbb{Z}/n\mathbb{Z}) = n$ である. 例えば, $\{0, 1, 2, \dots, n-1\}$ が (左) 完全代表系である.

また, 同値関係 $\overset{n\mathbb{Z}}{\sim}_L$ は以下のように考えると, 例 2 の同値関係と同じであることがわかる.

$$\begin{aligned} a \overset{n\mathbb{Z}}{\sim}_L a' &\Leftrightarrow \text{ある } nk \in n\mathbb{Z} \text{ が存在して, } a = a' + nk \\ &\Leftrightarrow a - a' \text{ が } n \text{ の倍数} \\ &\Leftrightarrow a \sim_n a' (\Leftrightarrow [a]_n = [a']_n). \end{aligned}$$

確かに例 7 の同値類とここでの剰余類を比べてみると, $C(a) = a + n\mathbb{Z}$ となっていることがわかる. 特に, $\mathbb{Z}/\sim_n = \mathbb{Z}/n\mathbb{Z}$ である. 剰余類 $a + n\mathbb{Z}$ を $[a]_n$ と書くと, これは今まで学んできた $\mathbb{Z}/n\mathbb{Z}$ と整合している. 実際, $a + n\mathbb{Z} = (a + kn) + n\mathbb{Z}$ ($k \in \mathbb{Z}$) も成立している (これは, 命題 6.3 (2) であると言っても良い). $\mathbb{Z}/n\mathbb{Z}$ という記号を使っていたのはこの考え方によるものだったのである.

例 9. $D_3 = \{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ を 3 次二面体群とする ($\sigma^3 = e, \tau^2 = e, \sigma^k\tau = \tau\sigma^{-k}$ ($k \in \mathbb{Z}$)). D_3 の部分群 $H = \langle \tau \rangle = \{e, \tau\}$ に関して, 定義 6.6 で定義された諸概念を見てみよう. $e \in D_3$ の H による左剰余類は,

$$eH = \{eh \mid h \in H\} = \{ee, e\tau\} = \{e, \tau\} (= H)$$

である (一般の群 G とその部分群 H に対して, 同様に $eH = H$ であることはすぐにわかるであろう). $\sigma \in D_3$ の H による左剰余類は,

$$\sigma H = \{\sigma h \mid h \in H\} = \{\sigma e, \sigma\tau\} = \{\sigma, \sigma\tau\}$$

である. $\sigma^2 \in D_3$ の H による左剰余類は,

$$\sigma^2 H = \{\sigma^2 h \mid h \in H\} = \{\sigma^2 e, \sigma^2 \tau\} = \{\sigma^2, \sigma^2 \tau\}$$

である. 以上より $D_3 = eH \cup \sigma H \cup \sigma^2 H$ であるので, 結局

$$D_3/H = \{gH \mid g \in D_3\} = \{H, \sigma H, \sigma^2 H\}$$

である (命題 6.3(2) より, $eH = \tau H, \sigma H = \sigma\tau H, \sigma^2 H = \sigma^2\tau H$ である). これより, H の D_3 における指数は, $(D_3 : H) = \#(D_3/H) = 3$ である. 例えば, $\{e, \sigma, \sigma^2\}, \{\tau, \sigma, \sigma^2\tau\}$ 等は左完全代表系である.

なお, 上の例で各剰余類に含まれる元の個数は $2 (= \#H)$ 個だったので, 指数は $(D_3 : H) = 6/2 = \#D_3/\#H$ と計算できる. 実はこのような計算は常に行うことができ, これが次回説明する Lagrange の定理である.

最後に右剰余類を見ておこう. $e \in D_3$ の H による右剰余類は,

$$He = \{he \mid h \in H\} = \{ee, \tau e\} = \{e, \tau\} (= H)$$

である (一般の群 G とその部分群 H に対して, 同様に $He = H$ であることはすぐにわかるであろう). $\sigma \in D_3$ の H による右剰余類は,

$$H\sigma = \{h\sigma \mid h \in H\} = \{e\sigma, \tau\sigma\} = \{\sigma, \sigma^{-1}\tau\} = \{\sigma, \sigma^2\tau\} \neq \sigma H$$

である. 非可換群であるので, このように同じ元の同じ部分群による左剰余類と右剰余類が異なるということがある. $\sigma^2 \in D_3$ の H による右剰余類は,

$$H\sigma^2 = \{h\sigma^2 \mid h \in H\} = \{e\sigma^2, \tau\sigma^2\} = \{\sigma^2, \sigma^{-2}\tau\} = \{\sigma^2, \sigma\tau\} \neq \sigma^2 H$$

である. 以上より $D_3 = H \cup H\sigma \cup H\sigma^2$ であるので, 結局

$$H \backslash D_3 = \{Hg \mid g \in D_3\} = \{H, H\sigma, H\sigma^2\}$$

である. 例えば, $\{e, \sigma, \sigma^2\}, \{\tau, \sigma, \sigma\tau\}$ 等は右完全代表系である.

代数学 I 第 8 回講義資料

担当：大矢 浩徳 (OYA Hironori)*

7.1 剰余類, Lagrange の定理 (後半)

前回の 6.2 節に引き続き, G を群, $e \in G$ をその単位元とする. 以下は, G の部分群による左・右剰余類の基本性質である.

命題 7.1

H を G の部分群とする. このとき, 以下が成立する.

- (1) $R \subset G$ が G の H に関する左完全代表系であることの必要十分条件は, $\{g^{-1} \mid g \in R\} \subset G$ が H に関する右完全代表系であることである. 特に, $|H \setminus G| = |G/H| (= (G:H))$.^{*1}
- (2) 任意の $g \in G$ に対し, $|gH| = |Hg| = |H|$.

証明.

(1) 写像 $i: G/H \rightarrow H \setminus G$ を

$$gH \mapsto Hg^{-1}$$

と定義する. これは, 実際に well-defined であることが次のようにわかる.^{*2}(well-defined については第 1, 2 回講義資料 p.3 を参照.) :

$gH = g'H \in G/H$ とする. これは $g \stackrel{H}{\sim}_L g'$ と同値なので, ある $h \in H$ が存在して, $g = g'h$. このとき,

$$Hg^{-1} = H(g'h)^{-1} = Hh^{-1}(g')^{-1} = H(g')^{-1}$$

(最後の等式は, $h^{-1}(g')^{-1} \stackrel{H}{\sim}_R (g')^{-1}$ を用いて, 右剰余類を表す代表元を取り替えた.) よって, i は well-defined.

全く同様に, $i': H \setminus G \rightarrow G/H$ を

$$Hg \mapsto g^{-1}H$$

* e-mail: hoyashibaura-it.ac.jp

*1 集合 S に対し, $|S|$ は S の元の個数を表す記号であったことを思い出すこと. $\#S$ と同じ意味である.

*2 これは well-defined 性をチェックする必要がある. なぜなら, $g' \in gH$ となる g' に対して, $gH = g'H$ が成り立つので (第 7 回講義資料命題 6.3(2)), G/H は 1 つの元の表し方が何通りもあるような集合の例であるからである. 例えば, $G = \mathbb{Z}, H = n\mathbb{Z}$ のとき, G/H が $\mathbb{Z}/n\mathbb{Z}$ に他ならなかったことを思い出すと (第 7 回講義資料例 8) わかりやすいであろう. ちなみに, 写像 $i': G/H \rightarrow H \setminus G$ を $gH \mapsto Hg$ としようとするとは well-defined ではない. 例えば, 第 7 回講義資料例 9 の $G = D_3, H = \{e, \tau\}$ の場合,

$$\begin{aligned} \sigma H &\mapsto H\sigma = \{\sigma, \sigma^2\tau\} \\ &\parallel \quad \neq \\ \sigma\tau H &\mapsto H\sigma\tau = \{\sigma\tau, \sigma^2\}. \end{aligned}$$

となる.

と定義すると、これは well-defined. このとき、 i と i' は互いに逆写像であり、特に i, i' は全単射写像である.

R は G の H に関する左完全代表系

$$\Leftrightarrow G/H = \{gH \mid g \in R\} \text{ かつ } \llbracket g, g' \in R, g \neq g' \text{ のとき } gH \neq g'H \rrbracket$$

$$\Leftrightarrow H \backslash G = \{Hg^{-1} \mid g \in R\} \text{ かつ } \llbracket g, g' \in R, g \neq g' \text{ のとき } Hg^{-1} \neq H(g')^{-1} \rrbracket \quad (i \text{ と } i' \text{ の全単射性より})$$

$$\Leftrightarrow \{g^{-1} \mid g \in R\} \text{ は } G \text{ の } H \text{ に関する右完全代表系} \quad (7.1)$$

となる. これで前半の主張は示された.

完全代表系の定義より、 G の H に関する左完全代表系の元の個数は G/H の元の個数に等しく、 G の H に関する右完全代表系の元の個数は $H \backslash G$ の元の個数に等しい. よって、 R を G の H に関する左完全代表系とすると、上で示した同値性 (7.1) から、

$$|G/H| = |R| = |\{g^{-1} \mid g \in R\}| = |H \backslash G|.$$

(2 つめの等式は逆元を取る操作が全単射であることから.) 以上より示すべきことは示された. \square

(2) 写像 $j: H \rightarrow gH$ を $h \mapsto gh$ と定義し、 $j': gH \rightarrow H$ を $h' \mapsto g^{-1}h'$ と定義する. (写像 j, j' による元への行き先は確かにそれぞれ gH, H に入っていることに注意.) このとき、 j と j' は互いに逆写像であり、特に j, j' は全単射写像である. よって、 $|gH| = |H|$. $|Hg| = |H|$ の証明もこれと全く同様である. \square

例 1. $D_3 = \{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ を 3 次二面体群とする ($\sigma^3 = e, \tau^2 = e, \sigma^k\tau = \tau\sigma^{-k}$ ($k \in \mathbb{Z}$)). $H := \langle \tau \rangle = \{e, \tau\} \subset D_3$ とし、第 7 回講義資料例 9 で行った計算を思い出すと、

$$D_3/H = \{gH \mid g \in D_3\} = \{H, \sigma H, \sigma^2 H\} = \{\{e, \tau\}, \{\sigma, \sigma\tau\}, \{\sigma^2, \sigma^2\tau\}\}$$

$$H \backslash D_3 = \{Hg \mid g \in D_3\} = \{H, H\sigma, H\sigma^2\} = \{\{e, \tau\}, \{\sigma, \sigma^2\tau\}, \{\sigma^2, \sigma\tau\}\}$$

となる. これを見ると、確かに各剰余類の元の個数は全て等しく $2 (= |H|)$ であることがわかる (命題 7.1(2)). さらに、確かに $|D_3/H| = 3 = |H \backslash D_3|$ である (命題 7.1(1)). D_3 の H に関する左完全代表系としては例えば、

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

が取れるが、このとき、

$$\{e^{-1}, \sigma^{-1}, (\sigma^2)^{-1}\} = \{e, \sigma^2, \sigma\} \text{ や } \{\tau^{-1}, \sigma^{-1}, (\sigma^2\tau)^{-1}\} = \{\tau, \sigma^2, \sigma^2\tau\}$$

は確かに、 D_3 の H に関する右完全代表系である (命題 7.1(1)).

次が群論において基本的だが非常に強力な Lagrange の定理である :

定理 7.2 (Lagrange の定理)

G を群、 H を G の部分群とすると、

$$|G| = |G/H| \cdot |H| = |H \backslash G| \cdot |H| = (G : H) \cdot |H|.^{*3}$$

証明. まず $(G : H) = |G/H|$ は定義そのものであり、 $|G/H| = |H \backslash G|$ は命題 7.1(1) からわかるので、 $|G| = |G/H| \cdot |H|$ のみ示せば十分である. R を G の H に関する左完全代表系とすると、

$$G = \bigcup_{g \in R} gH \text{ かつ } \llbracket g, g' \in R, g \neq g' \text{ のとき } gH \neq g'H \rrbracket$$

であり、さらに命題 7.1(2) より、任意の $g \in R$ に対して $|gH| = |H|$ となるので、 $|G| = |R| \cdot |H|$ となる. 完全代表系の定義より、 G の H に関する左完全代表系の元の個数は G/H の元の個数に等しいので、結局 $|G| = |G/H| \cdot |H|$ を得る. \square

*3 この等式は $|G|, |H|, (G : H)$ の中に ∞ のものがあっても成立する. 例えば、 G を無限群とし、 H をその有限部分群とすると、指数 $(G : H)$ は ∞ となる.

例 2. 例 1 の設定では $|D_3| = 6, |H| = 2, (D_3 : H) = 3$ なので, 確かに

$$|D_3| = (D_3 : H) \cdot |H|$$

が成立している.

Lagrange の定理の応用 : 以下に Lagrange の定理の応用をいくつか述べる.

系 7.3

有限群 G に対して, 以下が成立する :

- (1) H を G の部分群とすると, H の位数 $|H|$ は $|G|$ の約数である. また, H の G における指数 $(G : H)$ も $|G|$ の約数である.
- (2) 任意の $g \in G$ に対し, その位数 $\text{ord } g$ は $|G|$ の約数である.
- (3) 任意の $g \in G$ に対し, $g^{|G|} = e$.

証明.

(1) Lagrange の定理より, $|G| = (G : H) \cdot |H|$ であり, 定義より $(G : H)$ も $|H|$ も正の整数なので, (1) の主張が成立する. □

(2) $g \in G$ の位数 $\text{ord } g$ は g が生成する G の部分群 $\langle g \rangle = \{g^m \mid m \in \mathbb{Z}\}$ の位数として定義されたので, (1) よりその値は $|G|$ の約数である. □

(3) (2) より, ある $k \in \mathbb{Z}_{>0}$ が存在して, $|G| = k \cdot \text{ord } g$. ここで, 第 6 回講義資料命題 5.9 より, $\text{ord } g$ は $g^{\text{ord } g} = e$ を満たす最小の正の整数だったので,

$$g^{|G|} = g^{k \cdot \text{ord } g} = (g^{\text{ord } g})^k = e^k = e.$$

□

例 3. 第 5 回レポート課題問題 2 で 3 次二面体群 D_3 の部分群を全て列挙すると,

$$\{e\}, \{e, \sigma, \sigma^2\}, \{e, \tau\}, \{e, \sigma\tau\}, \{e, \sigma^2\tau\}, D_3$$

であることを計算してもらった (系 7.6 の後の解説も参照のこと). これを見ると, 位数は順に 1, 3, 2, 2, 2, 6 であり, どれも $|D_3| = 6$ の約数である. また, D_3 の各元の位数を計算してみると,

$$\text{ord } e = 1 \quad \text{ord } \sigma = 3 \quad \text{ord } \sigma^2 = 3 \quad \text{ord } \tau = 2 \quad \text{ord } \sigma\tau = 2 \quad \text{ord } \sigma^2\tau = 2$$

となり, 確かにどれも $|D_3| = 6$ の約数となっている.

ここで, 第 3 回講義資料で書いたオイラーの定理が (一瞬で!) 証明できる. これは n が素数 p のときフェルマーの小定理であったことを思い出そう.

系 7.4 (定理 2.9: オイラーの定理, Euler's theorem)

n が正の整数, $a \in \mathbb{Z}, \text{gcd}(a, n) = 1$ のとき, $\mathbb{Z}/n\mathbb{Z}$ において,

$$[a^{\varphi(n)}]_n = [1]_n.$$

ただし, φ はオイラーの φ 関数 (第 3 回講義資料定義 2.6).

証明. $\text{gcd}(a, n) = 1$ のとき, 第 3 回講義資料命題 2.5 より, $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ であった. $(\mathbb{Z}/n\mathbb{Z})^\times$ は乗法を二項演算 (単位元は $[1]_n$) とする位数 $\varphi(n)$ の群だったので, 系 7.3 (3) より,

$$[a^{\varphi(n)}]_n = [a]_n^{\varphi(n)} = [1]_n.$$

□

例 4. $n = 8$ のとき, $\varphi(8) = 4$. (8 と互いに素な 1 以上 8 以下の数は 1, 3, 5, 7 の 4 つ.) このとき,

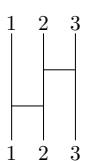
$$[1^4]_8 = [1]_8 \quad [3^4]_8 = [81]_8 = [1]_8 \quad [5^4]_8 = [625]_8 = [1]_8 \quad [7^4]_8 = [2401]_8 = [1]_8.$$

あみだくじと対称群の関係を思い出してもらおうとあみだくじに関する次のような性質もわかる:

系 7.5

n 本の縦棒があるあみだくじは $n!$ 回同じものをつなげると, どこを選んでも初めに選んだものと同じところに帰ってくるあみだくじとなる.

証明. 与えられたあみだくじは縦棒が n 本なので, n 次対称群のある元 $\sigma \in \mathfrak{S}_n$ に対応する (第 5 回講義資料 p.3 の注意参照). あみだくじの連結は \mathfrak{S}_n における二項演算に対応したので, 与えられたあみだくじを $n!$ 回つなげてできるあみだくじは $\sigma^{n!}$ に対応するあみだくじとなる. $|\mathfrak{S}_n| = n!$ であったので, 系 7.3 (3) より, $\sigma^{n!} = e$. e に対応するあみだくじとはどこを選んでも初めに選んだものと同じところに帰ってくるあみだくじに他ならないので, 系 7.5 は証明された. \square

例 5. 例えば,  というあみだくじは $3! = 6$ 回つなげると 1 は 1 に, 2 は 2 に, 3 は 3 に行くあみだく

じとなる. なお, 実際には 3 回つなげた時点でそうになっている. これは, $\text{ord} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = 3$ という事実に対応している.

系 7.6

位数が素数 p の群 G は必ず非自明な部分群を持たない巡回群となる.

証明. H を G の部分群とすると, 系 7.3 (1) より, $|H|$ は $|G| = p$ の約数であるが, p は素数なので, $|H| = 1$ または $|H| = p$. ここで, $|H| = 1$ のとき, $H = \{e\}$ であり, $|H| = p$ のとき, $H = G$ となるので, どちらも自明である. よって, G は非自明な部分群をもたない. さらに, $g \in G$ を G の単位元でない元とすると, g の生成する G の部分群 $\langle g \rangle$ は少なくとも単位元 e と g を含むことから, 位数は 1 ではないので $|\langle g \rangle| = p$ となる. これより, $G = \langle g \rangle$ で G は巡回群. \square

以上の知識を用いると例えば, 次のような問題は今までよりもかなり楽に解けるようになる.

例題: 第 5 回レポート課題問題 2

3 次二面体群 D_3 の部分群を全て列挙せよ.

解答例. まず, $|D_3| = 6$ なので, 系 7.3 (1) より, D_3 の部分群の位数は 1, 2, 3, 6 のいずれかである. さらに, 位数 1 の部分群は $\{e\}$, 位数 6 の部分群は D_3 という自明なものに限られるので, 非自明な部分群の位数は 2 か 3 である. ここで, 2 と 3 は素数なので, 系 7.6 よりこれらは巡回群である. よって, 非自明な部分群は D_3 の (単位元でない) 1 元で生成される部分群に限られる. これらを具体的に計算してみると,

$$\langle \sigma \rangle = \langle \sigma^2 \rangle = \{e, \sigma, \sigma^2\}, \quad \langle \tau \rangle = \{e, \tau\}, \quad \langle \sigma\tau \rangle = \{e, \sigma\tau\}, \quad \langle \sigma^2\tau \rangle = \{e, \sigma^2\tau\}.$$

以上より, 求める部分群は,

$$\{e\}, \{e, \sigma, \sigma^2\}, \{e, \tau\}, \{e, \sigma\tau\}, \{e, \sigma^2\tau\}, D_3$$

で全て. \square

代数学 I 第 9 回講義資料

担当：大矢 浩徳 (OYA Hironori)*

8.1 正規部分群, 剰余群

G を群, $e \in G$ をその単位元とする. H を G の部分群としたとき, $g \in G$ の H による左剰余類 gH と右剰余類 Hg は一般には異なっていた. しかし, H の取り方によってはこれらが全て一致することがある. 今回はそのような部分群に着目する.

定義 8.1

H を G の部分群とする. 任意の $g \in G$ に対して,

$$gH = Hg$$

が成立するとき, H を G の正規部分群 (normal subgroup) という.

例を見る前に定義からわかる命題を一つ述べておこう. これは与えられた群が正規部分群であるかどうかをチェックする際に便利である:

命題 8.2

H を G の部分群とする. 以下の (1), (2), (3) は同値である.

- (1) H は正規部分群である.
- (2) 任意の $g \in G$ に対して, $gHg^{-1} = H$ が成立する. ただし, $gHg^{-1} := \{ghg^{-1} \mid h \in H\}$ とする.
- (3) 任意の $g \in G$ と $h \in H$ に対して, $ghg^{-1} \in H$ である.

証明.

(1) \Rightarrow (2) 正規部分群の定義より, 任意の $g \in G$ と $h \in H$ に対して, $gh \in gH = Hg$ なので, $ghg^{-1} \in H$. よって, 任意の $g \in G$ に対して, $gHg^{-1} \subset H$. ここで $g \in G$ は任意であるので, 今の g を g^{-1} に取り替えても良く, $g^{-1}Hg \subset H$ も成立する. これより, 任意の $h \in H$ に対して, $g^{-1}hg \in H$ であるので, $h = g(g^{-1}hg)g^{-1} \in gHg^{-1}$ である. よって, $gHg^{-1} \supset H$ も言える. 以上より, 任意の $g \in G$ に対して, $gHg^{-1} = H$ である.

(2) \Rightarrow (1) 任意の $g \in G$ と $h \in H$ に対し, $ghg^{-1} \in H$ なので, $gh \in Hg$. よって, $gH \subset Hg$. ここで (2) の条件において $g \in G$ は任意であるので, 任意の $g \in G$ に対して $g^{-1}Hg = H$ も成立していることに注意すると, 任意の $g \in G$ と $h \in H$ に対し, $g^{-1}hg \in H$ も成立し, $hg \in gH$ となる. よって, $gH \supset Hg$ も成立する. 以上より, 任意の $g \in G$ に対して, $gH = Hg$ であることがわかる.

(2) \Rightarrow (3) これは意味を考えれば自明である.

(3) \Rightarrow (2) 条件 (3) は『任意の $g \in G$ に対し, $gHg^{-1} \subset H$ 』ということに他ならないので, この条件を仮定すると『任意の $g \in G$ に対し, $gHg^{-1} \supset H$ 』も成立するということを示せばよい. しかしこれは, (1) \Rightarrow (2) の証明内で証明した事実に他ならない. \square

例 1. G を可換群, H をその部分群とすると, 任意の $g \in G$ に対し, $gH = Hg$ が成立するので, H は正規部分群である. 可換群の任意の部分群は正規部分群なのである.

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

例 2. $D_3 = \{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ を 3 次二面体群とする ($\sigma^3 = e, \tau^2 = e, \sigma^k\tau = \tau\sigma^{-k}$ ($k \in \mathbb{Z}$)). $H := \langle \tau \rangle = \{e, \tau\} \subset D_3$ とすると,

$$\sigma H = \{\sigma, \sigma\tau\} \qquad H\sigma = \{\sigma, \tau\sigma\} = \{\sigma, \sigma^{-1}\tau\} = \{\sigma, \sigma^2\tau\}$$

となるので $\sigma H \neq H\sigma$. よって, H は正規部分群ではない.

一方, $N := \langle \sigma \rangle = \{e, \sigma, \sigma^2\}$ とすると,

$$\tau N = \{\tau, \tau\sigma, \tau\sigma^2\} = \{\tau, \sigma^{-1}\tau, \sigma^{-2}\tau\} = \{\tau, \sigma^2\tau, \sigma\tau\} \qquad N\tau = \{\tau, \sigma\tau, \sigma^2\tau\}$$

となるので, $\tau N = N\tau$ である. さらに, $D_3 = N \cup \tau N = N \cup N\tau$ なので, D_3 の元 g は『 $g \in N$ 又は $g \in \tau N = N\tau$ 』を満たし,

$$\begin{cases} g \in N \text{ のとき, } gN = N = Ng \\ g \in \tau N = N\tau \text{ のとき, } gN = \tau N = N\tau = Ng \end{cases}$$

となる. よって, N は D_3 の正規部分群である.

なお, N が D_3 の正規部分群であることは, 以下の一般的な命題の帰結であるとも言える. (実際にはこの命題の証明は上の証明をそのまま一般化して書いたものである.)

命題 8.3

群 G における指数が 2 であるような部分群 N は正規部分群となる.

証明. $(G : N) = 2$ のとき, G において N による左・右剰余類はそれぞれ 2 つとなる. そのうち 1 つは $eN = N = Ne$ なので, $g_0 \notin N$ なる G の元をとると, G の左・右剰余類への分割は

$$G = N \cup g_0N = N \cup Ng_0$$

となる. ここで, $N \cap g_0N = N \cap Ng_0 = \emptyset$ であることに注意すると, $g_0N = G \setminus N = Ng_0$ であることがわかる. ($G \setminus N$ は商空間ではなく G における N の補集合の意味.) このとき, G の各元 g は『 $g \in N$ 又は $g \in g_0N = Ng_0$ 』を満たし,

$$\begin{cases} g \in N \text{ のとき, } gN = N = Ng \\ g \in g_0N = Ng_0 \text{ のとき, } gN = g_0N = Ng_0 = Ng \end{cases}$$

となる. よって, N は G の正規部分群である. □

例 3. n を正の整数とし, \mathbb{K} を \mathbb{Q}, \mathbb{R} または \mathbb{C} とする. 一般線型群

$$GL_n(\mathbb{K}) := \{A \mid A \text{ は } \mathbb{K} \text{ の元を成分とする } n \times n \text{ 行列で, } \det A \neq 0\}$$

を考える (ただし, $\det A$ は A の行列式. 二項演算は行列の積であった.) このとき, $GL_n(\mathbb{K})$ の部分群

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

(特殊線型群と呼ばれるのであった) は正規部分群である. 部分群であることの確認は第 4 回講義資料で既に行っているのので, ここでは正規部分群であることをチェックしよう. 命題 8.2 の (1) と (3) の同値性より,

$$\text{任意の } A \in GL_n(\mathbb{K}) \text{ と } X \in SL_n(\mathbb{K}) \text{ に対して, } AXA^{-1} \in SL_n(\mathbb{K})$$

となることを示せばよい. 行列式が $A, B \in GL_n(\mathbb{K})$ に対して,

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

という性質を満たしたことを思い出すと,

$$\begin{aligned} \det(AXA^{-1}) &= \det(A) \det(X) \det(A^{-1}) = \det(A) \det(A^{-1}) \quad (X \in SL_n(\mathbb{K}) \text{ なので}) \\ &= \det(A) \cdot \frac{1}{\det(A)} = 1 \end{aligned}$$

となるので, 確かに $AXA^{-1} \in SL_n(\mathbb{K})$ であることがわかった.

例 4. \mathbb{K} を \mathbb{Q}, \mathbb{R} または \mathbb{C} とする. 2 次一般線型群

$$GL_2(\mathbb{K}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{C}, ad - bc \neq 0 \right\}$$

を考える. このとき,

$$B := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, d \in \mathbb{C}, ad \neq 0 \right\}$$

は部分群であるが正規部分群ではない. これは以下のように確かめられる:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in B \text{ より, } B \text{ は空ではない. 任意の } g, h \in B \text{ に対し, } g = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, h = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} \text{ とすると,}$$

$$gh = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} = \begin{pmatrix} aa' & ab' + bd' \\ 0 & dd' \end{pmatrix}$$

であり, $(aa')(dd') = (ad)(a'd') \neq 0$ なので, $gh \in B$. さらに, $g^{-1} = \frac{1}{ad} \begin{pmatrix} d & -b \\ 0 & a \end{pmatrix}$ より, $g^{-1} \in B$. 以上より, B は $GL_2(\mathbb{K})$ の部分群である.

一方, 例えば $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in GL_2(\mathbb{K}), \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in B$ に対し,

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix} \notin B$$

となる. よって, B は命題 8.2 (3) の条件を満たさず, 正規部分群とならない.

例 5. G を群としたとき, その中心 $Z(G) := \{z \in G \mid zg = gz, \forall g \in G\}$ は G の正規部分群である (中心については第 6 回講義資料を参照のこと). 中心が部分群出あることは命題 5.11 で示してあるので, ここでは正規であることを確かめる. 任意の $g \in G$ と $z \in Z(G)$ に対して,

$$gzg^{-1} = zgg^{-1} = ze = z \in Z(G)$$

である. よって, 命題 8.2 (3) が満たされるので, $Z(G)$ は G の正規部分群である.

例 6 (交換子群 (やや発展なので難しいと思う方は定理 8.8 まで飛ばしても良い)).

定義 8.4

G を群とする. 各 $g_1, g_2 \in G$ に対し, g_1 と g_2 の交換子 (commutator of g_1 and g_2) $[g_1, g_2]$ を,

$$[g_1, g_2] := g_1 g_2 g_1^{-1} g_2^{-1}$$

と定義する. さらに, G の交換子群 (commutator subgroup of G) $D(G)$ を,

$$D(G) := \langle \{[g_1, g_2] \mid g_1, g_2 \in G\} \rangle$$

と定義する. ここで, 右辺は交換子全体 $\{[g_1, g_2] \mid g_1, g_2 \in G\}$ の生成する G の部分群である.

注意. (1) 各 $g_1, g_2 \in G$ に対し, $[g_1, g_2]^{-1} = (g_1 g_2 g_1^{-1} g_2^{-1})^{-1} = g_2 g_1 g_2^{-1} g_1^{-1} = [g_2, g_1]$ である.

(2) $\{[g_1, g_2] \mid g_1, g_2 \in G\}$ は (1) より逆元をとる操作では閉じているが, 一般に二項演算では閉じておらず, これ自体は群にはならない.

命題 8.5

群 G に対し, $D(G)$ は G の正規部分群である.

命題 8.5 の証明のために, 以下の補題を用いる.

補題 8.6

群 G とその部分集合 S に対し、

$$\text{任意の } g \in G \text{ に対して, } gSg^{-1} \subset S$$

が成立するとき、 S の生成する G の部分群 $\langle S \rangle$ は G の正規部分群である。

証明. 任意の $\langle S \rangle$ の元 s は

$$s = s_1^{m_1} s_2^{m_2} \cdots s_k^{m_k} \quad (\text{ただし, } s_1, s_2, \dots, s_k \in S, m_1, m_2, \dots, m_k \in \mathbb{Z}, k \in \mathbb{N}) \quad (8.1)$$

と書けるのであった (第 6 回講義資料定義 5.5). ここで、各 $g, h \in G$ に対し、

$$\alpha_g(h) := ghg^{-1} \quad (8.2)$$

と定義すると、任意の $h_1, h_2 \in G$ に対して、

$$\begin{aligned} \alpha_g(h_1 h_2) &= gh_1 h_2 g^{-1} = gh_1 g g^{-1} h_2 g^{-1} = \alpha_g(h_1) \alpha_g(h_2), \\ \alpha_g(h_1^{-1}) &= gh_1^{-1} g^{-1} = (gh_1 g^{-1})^{-1} = \alpha_g(h_1)^{-1} \end{aligned}$$

が成立する^{*1}. よって、これを繰り返し用いると、任意の $g \in G$ と上の (8.1) の形の元 s に対して、

$$gsg^{-1} = \alpha_g(s) = \alpha_g(s_1)^{m_1} \alpha_g(s_2)^{m_2} \cdots \alpha_g(s_k)^{m_k}$$

となるが、仮定より $\alpha_g(s_1), \alpha_g(s_2), \dots, \alpha_g(s_k) \in S$ なので、上式の右辺は再び $\langle S \rangle$ の元であり、 $gsg^{-1} \in \langle S \rangle$ である。よって、命題 8.2 (3) の条件が満たされるので、 $\langle S \rangle$ は G の正規部分群である。□

命題 8.5 の証明. 補題 8.6 と交換子群の定義より、

$$\text{任意の } g, h_1, h_2 \in G \text{ に対し, } g[h_1, h_2]g^{-1} \in \{[g_1, g_2] \mid g_1, g_2 \in G\}$$

を示せばよいことがわかる (補題 8.6 における S が $\{[g_1, g_2] \mid g_1, g_2 \in G\}$ である). 補題 8.6 の証明中の (8.2) で定義した α_g という記号を用いると、補題 8.6 の証明中に示した α_g の性質より、任意の $g, h_1, h_2 \in G$ に対し、

$$g[h_1, h_2]g^{-1} = \alpha_g([h_1, h_2]) = \alpha_g(h_1 h_2 h_1^{-1} h_2^{-1}) = \alpha_g(h_1) \alpha_g(h_2) \alpha_g(h_1)^{-1} \alpha_g(h_2)^{-1} = [\alpha_g(h_1), \alpha_g(h_2)].$$

よって、 $g[h_1, h_2]g^{-1} \in \{[g_1, g_2] \mid g_1, g_2 \in G\}$ であり、示すべきことは示された。□

G に対して交換子群 $D(G)$ を取るという操作は繰り返し行うことができる。つまり、 G に対して、

$$D_0(G) := G \quad D_1(G) := D(D_0(G)) \quad D_2(G) := D(D_1(G)) \quad D_3(G) := D(D_2(G)) \quad \cdots$$

と $D_k(G) := D(D_{k-1}(G))$ ($k \in \mathbb{Z}_{>0}$) を満たすように順に定義していくことができる。このとき、命題 8.5 より、任意の $k \in \mathbb{Z}_{>0}$ に対して、 $D_k(G)$ は $D_{k-1}(G)$ の正規部分群となる。

定義 8.7

群 G がある正の整数 n において、 $D_n(G) = \{e\}$ を満たすとき、 G を可解群 (solvable group) という。

(i) G を可換群とすると、任意の $g_1, g_2 \in G$ に対し、

$$[g_1, g_2] = g_1 g_2 g_1^{-1} g_2^{-1} = g_2 g_1 g_1^{-1} g_2^{-1} = g_2 g_2^{-1} = e$$

となるので、 $D_1(G) = D(G) = \langle e \rangle = \{e\}$. よって、 G は可解群である。

^{*1} この性質は $\alpha_g: G \rightarrow G, h \mapsto ghg^{-1}$ が群準同型であるということに対応する。群準同型は次回のテーマである。

- (ii) $D_n = \{\sigma^k \tau^\ell \mid k = 0, \dots, n-1, \ell = 0, 1\}$ を n 次二面体群とする ($\sigma^n = e, \tau^2 = e, \sigma^k \tau = \tau \sigma^{-k}$ ($k \in \mathbb{Z}$)). このとき, $\sigma^{k_1} \tau^{\ell_1}, \sigma^{k_2} \tau^{\ell_2} \in D_n$ に対し,

$$\begin{aligned} [\sigma^{k_1} \tau^{\ell_1}, \sigma^{k_2} \tau^{\ell_2}] &= \sigma^{k_1} \tau^{\ell_1} \sigma^{k_2} \tau^{\ell_2} (\sigma^{k_1} \tau^{\ell_1})^{-1} (\sigma^{k_2} \tau^{\ell_2})^{-1} \\ &= \sigma^{k_1} \tau^{\ell_1} \sigma^{k_2} \tau^{\ell_2} (\sigma^{k_2} \tau^{\ell_2} \sigma^{k_1} \tau^{\ell_1})^{-1} \\ &= \sigma^{k_1 + (-1)^{\ell_1} k_2 \tau^{\ell_1 + \ell_2}} (\sigma^{k_2 + (-1)^{\ell_2} k_1 \tau^{\ell_1 + \ell_2}})^{-1} \\ &= \sigma^{k_1 + (-1)^{\ell_1} k_2 \tau^{\ell_1 + \ell_2} \tau^{-\ell_1 - \ell_2} \sigma^{-k_2 - (-1)^{\ell_2} k_1}} \\ &= \sigma^{k_1 - (-1)^{\ell_2} k_1 + (-1)^{\ell_1} k_2 - k_2} \end{aligned}$$

となるので, 特に $\{[g_1, g_2] \mid g_1, g_2 \in G\} \subset \{e, \sigma, \dots, \sigma^{n-1}\}$. これより, $D_1(D_n) = D(D_n) \subset \langle \sigma \rangle = \{e, \sigma, \dots, \sigma^{n-1}\}^{*2}$. 特に, $D_1(D_n)$ は可換群 $\langle \sigma \rangle$ の部分群なので可換群である. よって, (i) より, $D_2(D_n) = D(D_1(D_n)) = \{e\}$. よって, D_n は可解群である.

- (iii) n 次対称群 \mathfrak{S}_n は $n = 1, 2, 3, 4$ のとき可解, $n \geq 5$ のとき非可解となる. この事実の証明はここでは行わないが (興味のある方は調べてみて欲しい), 実はこのことは “5 次以上の方程式には, その係数の四則演算と冪根で表される解の公式が存在しない” という有名な事実に対応している. 興味のある方は『ガロア理論』というキーワードで調べて勉強してみて欲しい. 「可解」という言葉もこの理論を由来とする言葉のようである.

さて, G の部分群 N が正規部分群だと何が良いのだろうか? 実はこのとき, 商集合 G/N に再び群構造が入るのである! 定理の形で述べておこう.

定理 8.8

G を群, N を G の正規部分群とすると, 二項演算

$$\cdot : G/N \times G/N \rightarrow G/N, (gN, hN) \mapsto gN \cdot hN := ghN$$

が well-defined であり, これによって G/N が再び群となる.

定義 8.9

定理 8.8 の方法で作られる群 G/N を G の N による剰余群という.

定理 8.8 の証明. まず, 二項演算の well-defined 性をチェックする. このためには,

$$gN = g'N, hN = h'N \text{ としたとき, } ghN = g'h'N$$

となることを示せばよい. $gN = g'N, hN = h'N$ のとき, $g \stackrel{N}{\sim}_L g', h \stackrel{N}{\sim}_L h'$ なので (この記号については第 7 回講義資料定義 6.4 を参照のこと), ある $n_1, n_2 \in N$ が存在して, $g = g'n_1, h = h'n_2$ となる. このとき,

$$gh = g'n_1 h'n_2 = g'h'(h')^{-1} n_1 h'n_2$$

となるが, いま N は正規部分群なので, 命題 8.2 (3) の同値条件から $(h')^{-1} n_1 h' \in N$ であることがわかる. よって, $(h')^{-1} n_1 h'n_2 \in N$ (N は二項演算で閉じている). これより, 上の等式は $gh \stackrel{N}{\sim}_L g'h'$ であることを示している. よって, $ghN = g'h'N$.

次に, この二項演算が群の二項演算の 3 性質を満たしていることを確かめる:

- (I) (結合法則) 任意の $gN, hN, kN \in G/N$ に対し,

$$(gN \cdot hN) \cdot kN = ghN \cdot kN = (gh)kN = g(hk)N = gN \cdot hkN = gN \cdot (hN \cdot kN)$$

*2 もう少し真面目に考えると, $D_1(D_n) = \langle \sigma^2 \rangle$ であることがわかる. 考えてみよ.

*2 この等式は $|G|, |H|, (G:H)$ の中に ∞ のものがあっても成立する. 例えば, G を無限群とし, H をその有限部分群とすると, 指数 $(G:H)$ は ∞ となる.

(群 G の二項演算が結合法則を満たしていることを用いた.)

(II) (単位元の存在) 単位元は $eN = N \in G/N$ である. 実際, 任意の $gN \in G/N$ に対し,

$$eN \cdot gN = egN = gN = geN = gN \cdot eN$$

が成立する.

(III) (逆元の存在) 各 $gN \in G/N$ に対し, $g^{-1}N$ を考えると, これは

$$gN \cdot g^{-1}N = gg^{-1}N = eN = g^{-1}gN = g^{-1}N \cdot gN$$

を満たしている. よって, $(gN)^{-1} = g^{-1}N$ である.

以上より, 示すべきことは示された. □

例 7. n を正の整数とする. 加法群 \mathbb{Z} と n の倍数全体からなる部分群 $\langle n \rangle = \{nk \mid k \in \mathbb{Z}\} (= n\mathbb{Z})$ を考える. \mathbb{Z} は可換群なので, その部分群 $n\mathbb{Z}$ は正規部分群である. これにより, 定理 8.8 から剰余群 $\mathbb{Z}/n\mathbb{Z}$ が構成できる. これは集合としては,

$$\mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} \mid a \in \mathbb{Z}\} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}\}$$

であったことを思い出そう (第 7 回講義資料例 7). このとき, $\mathbb{Z}/n\mathbb{Z}$ の二項演算は定理 8.8 から,

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = a + b + n\mathbb{Z}$$

で定義される. 剰余類 $a + n\mathbb{Z}$ を $[a]_n$ と書くと, これは今まで学んできた群 $(\mathbb{Z}/n\mathbb{Z}, +)$ に他ならない. $\mathbb{Z}/n\mathbb{Z}$ という記号を使っていたのはこの考え方によるものだったのである.

なお, $n\mathbb{Z}$ は加法群 $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ らの部分群でもあるので, 剰余群 $(\mathbb{Q}/n\mathbb{Z}, +), (\mathbb{R}/n\mathbb{Z}, +), (\mathbb{C}/n\mathbb{Z}, +)$ も同様に定義することができる.

例 8. 例 2 の状況を考えよう. $D_3 = \{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ を 3 次二面体群とする ($\sigma^3 = e, \tau^2 = e, \sigma^k\tau = \tau\sigma^{-k}$ ($k \in \mathbb{Z}$)). このとき, $N := \langle \sigma \rangle = \{e, \sigma, \sigma^2\}$ は正規部分群であり,

$$D_3/N = \{gN \mid g \in G_3\} = \{N, \tau N\}$$

となるのであった. このとき, D_3/N の二項演算は定理 8.8 から,

$$N \cdot N = N, \quad N \cdot \tau N = \tau N \quad \tau N \cdot N = \tau N \quad \tau N \cdot \tau N = \tau^2 N = N$$

となる.

例 9. n を正の整数とし, \mathbb{K} を \mathbb{Q}, \mathbb{R} または \mathbb{C} とする. 一般線型群 $GL_n(\mathbb{K})$ を考える. このとき, $GL_n(\mathbb{K})$ の中心は

$$Z(GL_n(\mathbb{K})) = \{aI_n \mid a \in \mathbb{K}^\times\}^{*3}$$

となるのであった (第 6 回講義資料例 5. I_n は単位行列). 例 5 より, $Z(GL_n(\mathbb{K}))$ は $GL_n(\mathbb{K})$ の正規部分群である. $GL_n(\mathbb{K})$ の $Z(GL_n(\mathbb{K}))$ による剰余群

$$PGL_n(\mathbb{K}) := GL_n(\mathbb{K})/Z(GL_n(\mathbb{K}))$$

は射影一般線型群 (**projective general linear group**) と呼ばれる.

例 10. G を群とする. このとき, 命題 8.5 より, $D(G)$ は G の正規部分群となるのであった. このとき, 剰余群 $G/D(G)$ は可換群となる. なぜなら, 各 $gD(G), hD(G) \in G/D(G)$ に対し, $h^{-1}g^{-1}hg = [h^{-1}, g^{-1}] \in D(G)$ となるので,

$$gD(G) \cdot hD(G) = ghD(G) = gh(h^{-1}g^{-1}hg)D(G) = hgD(G) = hD(G) \cdot gD(G)$$

*3 第 6 回講義資料ではこの \mathbb{K}^\times を \mathbb{K} としてしまっていたので修正しておきました.

となるためである. 実は $G/D(G)$ は G を割って可換にするような “最小の割り方” であるということがわかる (証明は今後). 厳密に言うと, N を G の正規部分群とし, 剰余群 G/N が可換群となるとき, $D(G) \subset N$ となるのである.

代数学 I 第 10 回講義資料

担当：大矢 浩徳 (OYA Hironori)*

9.1 群準同型

2つの群 G_1, G_2 が与えられたとき、それらは一見見た目が違っても群としては“本質的に同じ”であるということがある。簡単な例として、加法群 $(\mathbb{Z}/2\mathbb{Z}, +)$ と乗法群 $(\{1, -1\}, \times)$ を考えてみよう。これらは次のような演算規則を持つ：

$$[0]_2 + [0]_2 = [0]_2 \quad [0]_2 + [1]_2 = [1]_2 \quad [1]_2 + [0]_2 = [1]_2 \quad [1]_2 + [1]_2 = [0]_2 \quad (9.1)$$

$$1 \times 1 = 1 \quad 1 \times (-1) = -1 \quad (-1) \times 1 = -1 \quad (-1) \times (-1) = 1 \quad (9.2)$$

これを見ると、 $[0]_2$ を 1 に (=単位元を単位元に)、 $[1]_2$ を -1 に対応させ、 $+$ を \times で読み替えると、上の群の演算規則がしたの群の演算規則となることがわかる。このようなときに、 $(\mathbb{Z}/2\mathbb{Z}, +)$ と $(\{1, -1\}, \times)$ は見かけは違うが、群としての構造は全く同じであると考えられる。

さらに、 n 次二面体群 $D_n = \{\sigma^k \tau^\ell \mid k = 0, \dots, n-1, \ell = 0, 1\}$ ($\sigma^n = e, \tau^2 = e, \sigma^k \tau = \tau \sigma^{-k}$ ($k \in \mathbb{Z}$)) において、

$$e \circ e = e \quad e \circ \tau = \tau \quad \tau \circ e = \tau \quad \tau \circ \tau = e \quad (9.3)$$

が成り立っていた。これを見ると、 $[0]_2$ を e に (=単位元を単位元に)、 $[1]_2$ を τ に対応させ、 $+$ を \circ で読み替えると、やはり $\mathbb{Z}/2\mathbb{Z}$ での演算規則が、 D_n の部分群 $\langle \tau \rangle = \{e, \tau\}$ の演算規則と対応することがわかる。これにより、先ほどの“群としての同一視”を考えると、 D_n は群として $\mathbb{Z}/2\mathbb{Z}$ を含んでいるということが出来る。

一般に、群は“対称性”の抽象化であったという気持ちを思い出すと、2つの対称性 (=群) が与えられた時に、それらが本質的に同じものかどうか、あるいは一方が他方を含むようなものであるかどうかを知ることは重要なことと言えるだろう (対称性の比較)。今回はそういった“群間の関係”ことを定式化する概念として、準同型と呼ばれるものを学ぶ。

定義 9.1

G, G' を群とする。写像 $\phi: G \rightarrow G'$ が

$$\text{任意の } g_1, g_2 \in G \text{ に対して, } \phi(g_1 g_2) = \phi(g_1) \phi(g_2)$$

を満たすとき、 ϕ を準同型 (homomorphism) あるいは群準同型 (group homomorphism) という。さらに写像として ϕ が全射であるとき ϕ を全射準同型、単射であるとき単射準同型、全単射であるとき全単射準同型という、

準同型 $\phi: G \rightarrow G'$ に対し、

$$\text{Ker } \phi := \{g \in G \mid \phi(g) = e'\} \text{ (ただし, } e' \text{ は } G' \text{ の単位元)}$$

$$\text{Im } \phi := \{g' \in G' \mid \text{ある } g \in G \text{ が存在して, } \phi(g) = g'\}$$

とし、 $\text{Ker } \phi$ を ϕ の核 (kernel)、 $\text{Im } \phi$ を ϕ の像 (image) という。ここで $\text{Ker } \phi$ は G の部分集合であり、 $\text{Im } \phi$ は G' の部分集合であることに注意すること。

例を見る前に定義からわかる準同型の基本的な命題を3つ述べよう。まず例を見たいという方はこれらを一旦

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

飛ばして例を見てもらっても良い (ただしこれらは全て基本的な命題なので, 例を見た後はこちらに戻ってくること).

命題 9.2

$\phi: G \rightarrow G'$ を準同型とし, e を G の単位元, e' を G' の単位元とする. このとき, 以下が成立する:

- (1) $\phi(e) = e'$. (“単位元は必ず単位元に送られる”)
- (2) 任意の $g \in G$ に対して, $\phi(g^{-1}) = \phi(g)^{-1}$.

証明.

(1) 単位元と準同型の性質より,

$$\phi(e) = \phi(ee) = \phi(e)\phi(e)$$

が成立する. これより, $\phi(e)^{-1}$ を両辺に掛けると, $e' = \phi(e)$ がわかる. □

(2) $\phi(g^{-1})$ が $\phi(g)$ の逆元の定義の性質を満たしていることを確かめる.

$$\begin{aligned}\phi(g^{-1})\phi(g) &= \phi(g^{-1}g) \quad (\text{準同型の性質より}) \\ &= \phi(e) = e' \quad ((1) \text{より}) \\ \phi(g)\phi(g^{-1}) &= \phi(gg^{-1}) \quad (\text{準同型の性質より}) \\ &= \phi(e) = e' \quad ((1) \text{より})\end{aligned}$$

となるので, 確かに $\phi(g^{-1}) = \phi(g)^{-1}$ である. □

命題 9.3

$\phi: G \rightarrow G'$ を準同型とする. このとき, 以下が成立する:

- (1) $\text{Im } \phi$ は G' の部分群.
- (2) $\text{Ker } \phi$ は G の正規部分群.

証明.

(1) 定義より $\text{Im } \phi$ の元は $\phi(g)$ ($g \in G$) の形で書けるものであったので, $\text{Im } \phi$ は明らかに空ではない. 次に, 任意の $\phi(g_1), \phi(g_2) \in \text{Im } \phi$ に対し, 準同型の性質から,

$$\phi(g_1)\phi(g_2) = \phi(g_1g_2) \in \text{Im } \phi.$$

また, 任意の $\phi(g) \in \text{Im } \phi$ に対し, 命題 9.2 (2) から,

$$\phi(g)^{-1} = \phi(g^{-1}) \in \text{Im } \phi.$$

よって, $\text{Im } \phi$ は二項演算と逆元を取る操作について閉じているので, $\text{Im } \phi$ は G' の部分群である. □

(2) G の単位元を e , G' の単位元を e' とする. 命題 9.2 (1) より, $\phi(e) = e'$ なので, $e \in \text{Ker } \phi$ となり, 特に $\text{Ker } \phi$ は空ではない. 次に, 任意の $g_1, g_2 \in \text{Ker } \phi$ に対し, 準同型の性質から,

$$\phi(g_1g_2) = \phi(g_1)\phi(g_2) = e'e' = e'$$

より, $g_1g_2 \in \text{Ker } \phi$. また, 任意の $g \in \text{Ker } \phi$ に対し, 命題 9.2 (2) から,

$$\phi(g^{-1}) = \phi(g)^{-1} = (e')^{-1} = e'$$

より, $g^{-1} \in \text{Ker } \phi$. よって, $\text{Ker } \phi$ は二項演算と逆元を取る操作について閉じているので, $\text{Ker } \phi$ は G の部分群である.

次に正規性を確かめる. 任意の $g \in G, k \in \text{Ker } \phi$ に対し,

$$\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)e'\phi(g^{-1}) = \phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = \phi(e) = e' \quad (\text{命題 9.2(1)})$$

となるので, $gkg^{-1} \in \text{Ker } \phi$. よって, 第 9 回講義資料命題 8.2 より, $\text{Ker } \phi$ は正規部分群. □

命題 9.4

$\phi: G \rightarrow G'$ を準同型とする. e を G の単位元とする. このとき, 以下が成立する:

- (1) $\text{Im } \phi = G' \Leftrightarrow \phi$ は全射.
- (2) $\text{Ker } \phi = \{e\} \Leftrightarrow \phi$ は単射.
- (3) ϕ が全単射のとき, 逆写像 $\phi^{-1}: G' \rightarrow G$ も準同型.

証明.

(1) これは全射の定義そのものである. □

(2) の \Rightarrow 方向 この証明中では G' の単位元を e' と書くことにする. $g_1, g_2 \in G$ で $g_1 \neq g_2$ のとき, $g_1 g_2^{-1} \neq e$ である. いま, $\text{Ker } \phi = \{e\}$ なので, ϕ で e' に送られる元は e だけであることから,

$$e' \neq \phi(g_1 g_2^{-1}) = \phi(g_1) \phi(g_2)^{-1}$$

(最後の等式では命題 9.2 (2) も用いた). これより, $\phi(g_1) \neq \phi(g_2)$ であることがわかる.

(2) の \Leftarrow 方向 ϕ が単射であることより, 任意の $e \neq g \in G$ に対して, $e' = \phi(e) \neq \phi(g)$ (最初の等式では命題 9.2 (1) を用いた) となる. よって, $g \notin \text{Ker } \phi$ であるから, 結局 $\text{Ker } \phi$ の元は e のみ, つまり $\text{Ker } \phi = \{e\}$ であることがわかる. □

(3) 任意の $g'_1, g'_2 \in G'$ に対して,

$$\phi(\phi^{-1}(g'_1 g'_2)) = g'_1 g'_2 = \phi(\phi^{-1}(g'_1)) \phi(\phi^{-1}(g'_2)) = \phi(\phi^{-1}(g'_1) \phi^{-1}(g'_2)).$$

(最後の等式は ϕ の準同型としての性質を用いた.) ここで, ϕ は単射であることより, 結局

$$\text{任意の } g'_1, g'_2 \in G' \text{ に対して, } \phi^{-1}(g'_1 g'_2) = \phi^{-1}(g'_1) \phi^{-1}(g'_2)$$

が言える. これは ϕ^{-1} が準同型であるということに他ならない. □

定義 9.5

$\phi: G \rightarrow G'$ が全単射準同型であるとき, ϕ を同型 (isomorphism) あるいは群同型 (group isomorphism) という. 命題 9.4 (3) より, 準同型 $\phi: G \rightarrow G'$ が同型であるとは, ある準同型 $\phi': G' \rightarrow G$ が存在して, $\phi' \circ \phi = \text{id}_G, \phi \circ \phi' = \text{id}_{G'}$ となることとも言える (id_X で X 上の恒等写像を表す.)

同型 $\phi: G \rightarrow G'$ が存在するとき, G と G' は同型である (isomorphic) であるといい, $G \simeq G'$ と書く.

例 1. ここまで準備した言葉で 9.1 章の冒頭の例を定式化してみよう. 初めの例は, 写像

$$\phi: \mathbb{Z}/2\mathbb{Z} \rightarrow \{1, -1\}, [0]_2 \mapsto 1, [1]_2 \mapsto -1$$

が同型であるということをチェックしたことに他ならない. 実際このように対応させると, これは全単射で, 任意の $[a]_2, [b]_2 \in \mathbb{Z}/2\mathbb{Z}$ に対して,

$$\phi([a]_2 + [b]_2) = \phi([a]_2) \times \phi([b]_2)$$

が成り立つことが (9.1), (9.2) からわかる ($\phi([1]_2 + [0]_2) = \phi([1]_2) = -1 = (-1) \times 1 = \phi([1]_2) \times \phi([0]_2)$ 等). このように, 群 G と G' が同型であるというのは, 群としては実質的に全く同じである (この例のように “見かけ” が違うだけ) ということを主張することに他ならない.

また, $n \geq 3$ に対して,

$$\phi': \mathbb{Z}/2\mathbb{Z} \rightarrow D_n, [0]_2 \mapsto e, [1]_2 \mapsto \tau$$

とすると, これは準同型であることがわかる. 実際, 任意の $[a]_2, [b]_2 \in \mathbb{Z}/2\mathbb{Z}$ に対して,

$$\phi'([a]_2 + [b]_2) = \phi'([a]_2) \circ \phi'([b]_2)$$

が成り立つことが (9.1), (9.3) からわかる ($\phi'([1]_2 + [1]_2) = \phi'([0]_2) = e = \tau \circ \tau = \phi'([1]_2) \circ \phi'([1]_2)$ 等). ϕ' は構成から明らかに単射準同型である.

例 2. 乗法群 \mathbb{C}^\times から \mathbb{R}^\times への絶対値を取る写像

$$|\cdot|: \mathbb{C}^\times \rightarrow \mathbb{R}^\times, z = x + iy \mapsto |z| := \sqrt{x^2 + y^2} \quad (x, y \in \mathbb{R})$$

は準同型である。実際、絶対値の性質として、任意の $z_1, z_2 \in \mathbb{C}^\times$ に対し、

$$|z_1 z_2| = |z_1| |z_2|$$

が成り立つのであった。これは準同型の定義条件に他ならない。このとき

$$\text{Ker } |\cdot| := \{z \in \mathbb{C}^\times \mid |z| = 1\} = \{e^{i\theta} \mid \theta \in \mathbb{R}\} (=: \mathbb{T})$$

$$\text{Im } |\cdot| := \{r \in \mathbb{R}^\times \mid \text{ある } z \in \mathbb{C}^\times \text{ が存在して, } |z| = r\} = \mathbb{R}_{>0}$$

であり、 $|\cdot|$ は全射でも単射でもない。

例 3. 加法群 \mathbb{C} から \mathbb{R} への絶対値を取る写像

$$|\cdot|: \mathbb{C} \rightarrow \mathbb{R}, z \mapsto |z|$$

は準同型ではない。実際、いま加法群を考えているので考える演算は和 $+$ であるが、

$$|z_1 + z_2| = |z_1| + |z_2|$$

は一般には成立しない (例えば、 $|1 + (-1)| = 0 \neq |1| + |-1|$)。

例 4. 指数・対数写像

$$\exp: \mathbb{R} \rightarrow \mathbb{R}_{>0}, x \mapsto e^x$$

$$\log: \mathbb{R}_{>0} \rightarrow \mathbb{R}, x \mapsto \log(x)$$

はどちらも準同型である。実際、任意の $x, y \in \mathbb{R}$ に対し、

$$\exp(x + y) = e^{x+y} = e^x e^y = \exp(x) \exp(y) \quad (\text{指数法則})$$

が成り立ち、任意の $x, y \in \mathbb{R}_{>0}$ に対し、

$$\log(xy) = \log(x) + \log(y)$$

が成り立つことは良く知っていると思われるが、これらは準同型の定義条件に他ならない。また、このとき

$$\log \circ \exp = \text{id}_{\mathbb{R}} \quad \exp \circ \log = \text{id}_{\mathbb{R}_{>0}}$$

が成立するので、定義 9.5 より、 \exp, \log はいずれも同型である (特に $\mathbb{R} \simeq \mathbb{R}_{>0}$)。加法群 \mathbb{R} と乗法群 $\mathbb{R}_{>0}$ は見かけは違うが、実は群としては同じものだったのである！*1

例 5. n を正の整数とし、 \mathbb{K} を \mathbb{Q}, \mathbb{R} または \mathbb{C} とする。一般線型群

$$GL_n(\mathbb{K}) := \{A \mid A \text{ は } \mathbb{K} \text{ の元を成分とする } n \times n \text{ 行列で, } \det A \neq 0\}$$

を考える。このとき、行列式を取る写像

$$\det: GL_n(\mathbb{K}) \rightarrow \mathbb{K}^\times, A \mapsto \det(A)$$

は準同型である。実際、任意の $A, B \in GL_n(\mathbb{K})$ に対して、

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

*1 舞台を有理数にうつすと、加法群 \mathbb{Q} と乗法群 $\mathbb{Q}_{>0}$ は実は同型ではない！今回の本レポート課題にしたので、証明を考えてみよ。

という性質が成り立つのであったが、これは準同型の定義条件に他ならない。このとき

$$\begin{aligned} \text{Ker det} &:= \{A \in GL_n(\mathbb{K}) \mid \det(A) = 1\} = SL_n(\mathbb{K}) \\ \text{Im det} &:= \{r \in \mathbb{K}^\times \mid \text{ある } A \in GL_n(\mathbb{K}) \text{ が存在して, } \det(A) = r\} = \mathbb{K}^\times \end{aligned}$$

である。ここで、像 Im det が \mathbb{K}^\times であることは、任意の $a \in \mathbb{K}^\times$ に対し、

$$\det \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} = a$$

であることからわかる。よって、これは全射準同型である。命題 9.3(2) から、 Ker det は $GL_n(\mathbb{K})$ の正規部分群だったので、特殊線型群 $SL_n(\mathbb{K})$ が一般線型群 $GL_n(\mathbb{K})$ の正規部分群であることはこの事実からもわかる*2。

例 6. n を 2 以上の整数とし、 n 次対称群 \mathfrak{S}_n を考える。 \mathfrak{S}_n の各元 σ に対し、その符号 $\text{sgn } \sigma$ を

$$\text{sgn } \sigma := \det E_\sigma \quad \text{ただし, } E_\sigma \text{ は } \begin{cases} (\sigma(i), i) \text{ 成分が } 1 \\ \text{それ以外の成分が } 0 \end{cases} \text{ として定義される } n \times n \text{ 行列}$$

と定義する*3。例えば、 $n = 3$ のとき、

$$\begin{aligned} E_{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}} &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & E_{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}} &= \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} & E_{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}} &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \\ E_{\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}} &= \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} & E_{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}} &= \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} & E_{\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}} &= \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \end{aligned}$$

であり、

$$\begin{aligned} \text{sgn} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} &= 1 & \text{sgn} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} &= -1 & \text{sgn} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} &= -1 \\ \text{sgn} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} &= 1 & \text{sgn} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} &= 1 & \text{sgn} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} &= -1 \end{aligned}$$

である。符号は、 $n \times n$ 行列

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

の行列式 $\det(A)$ の一般形を表す際に、

$$\det(A) = \sum_{\sigma \in \mathfrak{S}_n} (\text{sgn } \sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)} \quad (9.4)$$

として出てきていたものであったことを思い出そう。さらに、符号 sgn は以下の性質を満たすのであった。

(S1) $\text{sgn}(\sigma) = (-1)^k$ 。ただし、 k は σ を隣接互換 $(i \ i+1)$ の何回かの合成で書いた際に現れる隣接互換の個数である (第 6 回講義資料定理 5.4 (2) 参照)。これは、対称群とあみだくじの関係を思い出すと σ に対応するあみだくじを書いたときの横棒の本数の数と言っても良い (σ に対応するあみだくじは無数にあるが、横棒の本数の偶奇は表し方にはよらない)*4。

*2 命題 9.3(2) における正規性の証明は $SL_n(\mathbb{K})$ の正規性の証明とほぼ同じなので「命題 9.3(2) を使うことが $SL_n(\mathbb{K})$ の正規性の別証明である」ということには少し抵抗がある。

*3 [細かい注意。余りにしなくても良い。] 行列式の定義として (9.4) を用いることもあり、その流儀の方にとっては符号 $\text{sgn } \sigma$ を \det で定義するということは「 \det の定義に sgn が必要で、 sgn の定義に \det が必要」というよう循環してしまうので良くない。私が 2019 年度の後期に担当した線形代数 II では第 1 行目に関する余因子展開で行列式の定義を行ったので、昨年私の講義を受けた方はこの点の問題は生じないことになっている。

*4 先学期の私が担当した線形代数 II を受けていた方にはこちらのあみだくじの方で説明した。

(S2) 任意の $\sigma_1, \sigma_2 \in \mathfrak{S}_n$ に対して, $\text{sgn}(\sigma_1\sigma_2) = \text{sgn}(\sigma_1)\text{sgn}(\sigma_2)$.

(S1) は特に $\text{sgn } \sigma$ の値は 1 か -1 であるということを主張しており, (S2) と合わせると, これは

$$\text{sgn}: \mathfrak{S}_n \rightarrow \{1, -1\}, \sigma \mapsto \text{sgn } \sigma$$

が全射準同型であるということに他ならない. さらにこのとき,

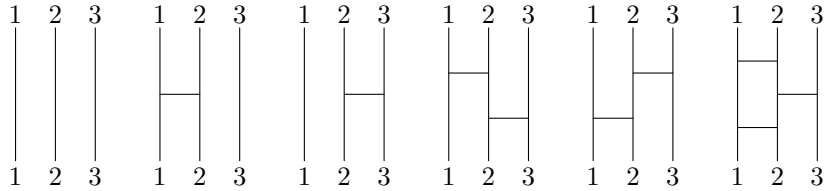
$$\text{Ker sgn} := \{\sigma \in \mathfrak{S}_n \mid \text{sgn } \sigma = 1\}$$

であるが, この群は n 次交代群 (**alternating group**) と呼ばれ, \mathfrak{A}_n *5 と書かれる. \mathfrak{A}_n の元, すなわち $\text{sgn } \sigma = 1$ となる \mathfrak{S}_n の元を偶置換とよび, $\text{sgn } \sigma = -1$ となる \mathfrak{S}_n の元を奇置換と呼んだこともついでに思い出しておこう.

なお, 性質 (S1) は実際の符号の計算において便利である. 例えば $n = 3$ のとき,

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

に対応するあみだくじはこの順に以下のようにとれる:



横棒の本数は順に 0 本, 1 本, 1 本, 2 本, 2 本, 3 本なので,

$$\begin{aligned} \text{sgn} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} &= (-1)^0 = 1 & \text{sgn} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} &= (-1)^1 = -1 & \text{sgn} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} &= (-1)^1 = -1 \\ \text{sgn} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} &= (-1)^2 = 1 & \text{sgn} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} &= (-1)^2 = 1 & \text{sgn} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} &= (-1)^3 = -1 \end{aligned}$$

となっている.

例 7. \mathbb{K} を \mathbb{Q}, \mathbb{R} または \mathbb{C} とする. \mathbb{K} 上のベクトル空間は加法 $+$ に関して群をなすのであった (第 4 回講義資料例 3 参照). V, W を \mathbb{K} 上のベクトル空間としたとき, 線形写像 $f: V \rightarrow W$ は準同型でもある. 実際, 線形写像の性質

$$f(\mathbf{v}_1 + \mathbf{v}_2) = f(\mathbf{v}_1) + f(\mathbf{v}_2), \forall \mathbf{v}_1, \mathbf{v}_2 \in V$$

は準同型の定義条件に他ならない. このとき, 準同型としての核 $\text{Ker } f$ や像 $\text{Im } f$ は線形写像としての核や像と一致していることが定義からすぐにわかる.

例 8. 任意の巡回群 $G = \langle g \rangle = \{g^m \mid m \in \mathbb{Z}\}$ に対し,

$$p: \mathbb{Z} \rightarrow G, m \mapsto g^m$$

は全射準同型である. 実際, 任意の $m_1, m_2 \in \mathbb{Z}$ に対して,

$$p(m_1 + m_2) = g^{m_1+m_2} = g^{m_1}g^{m_2} = p(m_1)p(m_2)$$

という性質が成り立つ. このとき,

$$\text{Ker } p := \{m \in \mathbb{Z} \mid g^m = e\}$$

である. ここで, 第 6 回講義資料命題 5.9 より, $g^m = e$ を満たす最小の正の整数が $\text{ord } g$ であった. これより,

$$\begin{cases} \text{ord } g = \infty \text{ のとき, } \text{Ker } p = \{0\}. \\ \text{ord } g < \infty \text{ のとき, } \text{Ker } p = \langle \text{ord } g \rangle = \{k \text{ ord } g \mid k \in \mathbb{Z}\} = (\text{ord } g)\mathbb{Z}. \end{cases}$$

*5 \mathfrak{A} はドイツ文字の A である.

となる。実際には $\text{ord } g < \infty$ のときの等号についてはもう少しきちんと示す必要があるが、 $\text{ord } g$ の最小性を用いれば難しくないのでこれは練習問題としよう。この結果より、 $\text{ord } g = \infty$ の場合には、 p は単射であることもわかり (命題 9.4 (2)), p は同型であることがわかる。 $\text{ord } g = \infty$ である巡回群 $\langle g \rangle$ は全て加法群 \mathbb{Z} と同型となるのである。

例 9. G を群, N をその正規部分群とする。このとき, 剰余群 G/N を考えることができた (第 9 回講義資料 定理 8.8, 定義 8.9). 商写像

$$p: G \rightarrow G/N, g \mapsto gN$$

は全射準同型である。実際, 任意の $g_1, g_2 \in G$ に対して, 剰余群の二項演算の定義から,

$$p(g_1g_2) = g_1g_2N = g_1N \cdot g_2N = p(g_1) \cdot p(g_2)$$

という性質が成り立つ。このとき,

$$\text{Ker } p := \{g \in G \mid gN = eN\} = \{g \in G \mid g \in eN\} = N$$

である。例えば, $G = \mathbb{Z}, N = n\mathbb{Z} (n \in \mathbb{Z}_{>0})$ のとき,

$$p: \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}, a \mapsto [a]_n$$

は全射準同型であり, $\text{Ker } p = n\mathbb{Z}$ である。

例 10. G を群とし, $a \in G$ とする。このとき, 写像 $\alpha_a: G \rightarrow G$ を

$$\alpha_a: G \rightarrow G, g \mapsto aga^{-1}$$

と定めると, これは準同型である。実際, 任意の $g_1, g_2 \in G$ に対して,

$$\alpha_a(g_1g_2) = ag_1g_2a^{-1} = ag_1aa^{-1}g_2a^{-1} = \alpha_a(g_1)\alpha_a(g_2)$$

が成立する。さらに, 上の a を a^{-1} として, $\alpha_{a^{-1}}: G \rightarrow G, g \mapsto a^{-1}ga$ を考えると, 任意の $g \in G$ に対し,

$$(\alpha_{a^{-1}} \circ \alpha_a)(g) = a^{-1}(aga^{-1})a = g \quad (\alpha_a \circ \alpha_{a^{-1}})(g) = a(a^{-1}ga)a^{-1} = g$$

となるので, $\alpha_{a^{-1}} \circ \alpha_a = \alpha_a \circ \alpha_{a^{-1}} = \text{id}_G$ である。よって定義 9.5 より, α_a は同型である。このような $\alpha_a (a \in G)$ を G の内部自己同型 (**inner automorphism**) という。

例 11 (やや発展.). G を群とする。このとき, G から G への同型を全て集めてきてできる集合

$$\text{Aut}(G) := \{\phi: G \rightarrow G \mid \phi \text{ は同型}\}$$

を考える。同型は全単射写像なので, これは第 5 回講義資料の例 1 で考えた G 上の全単射写像 (準同型とは限らない) のなす群 $B(G)$ (二項演算は写像の合成) の部分集合となるが, 実は $\text{Aut}(G)$ は $B(G)$ の部分群となる。この群 $\text{Aut}(G)$ を G の自己同型群 (**automorphism group**) という。このことは以下のように確かめられる:

任意の $\phi_1, \phi_2 \in \text{Aut}(G)$ と $g_1, g_2 \in G$ に対し,

$$(\phi_1 \circ \phi_2)(g_1g_2) = \phi_1(\phi_2(g_1g_2)) = \phi_1(\phi_2(g_1)\phi_2(g_2)) = \phi_1(\phi_2(g_1)) \cdot \phi_1(\phi_2(g_2)) = (\phi_1 \circ \phi_2)(g_1) \cdot (\phi_1 \circ \phi_2)(g_2)$$

となるので, $\phi_1 \circ \phi_2$ も準同型である*6。さらに全単射性は合成で保たれるので, 結局 $\phi_1 \circ \phi_2$ も G から G への同型となり, $\phi_1 \circ \phi_2 \in \text{Aut}(G)$ である。また, 任意の $\phi \in \text{Aut}(G)$ に対し, 命題 9.4 (3) より ϕ^{-1} も G から G への同型となるので, $\phi^{-1} \in \text{Aut}(G)$ 。以上より, $\text{Aut}(G)$ は二項演算 (=写像の合成) と逆元を取る操作で閉じているので, $B(G)$ の部分群となる。

*6 全く同じ証明で任意の 2 つの準同型 $\psi: G \rightarrow G', \psi': G' \rightarrow G''$ に対し, $\psi' \circ \psi$ が再び準同型となることがわかる。

さらに、例 10 で考えた内部自己同型全体のなす集合

$$\text{Inn}(G) := \{\alpha_a : G \rightarrow G \mid a \in G\}$$

を考えると、 α_a は同型だったので、これは $\text{Aut}(G)$ の部分集合である。このとき、実は $\text{Inn}(G)$ は $\text{Aut}(G)$ の正規部分群となる。この群 $\text{Inn}(G)$ を内部自己同型群 (inner automorphism group) という。このことは、次のように確かめられる：

任意の $\alpha_{a_1}, \alpha_{a_2} \in \text{Inn}(G)$ と $g \in G$ に対し、

$$(\alpha_{a_1} \circ \alpha_{a_2})(g) = \alpha_{a_1}(\alpha_{a_2}(g)) = a_1(a_2ga_2^{-1})a_1^{-1} = (a_1a_2)g(a_1a_2)^{-1} = \alpha_{a_1a_2}(g)$$

となるので、

$$\alpha_{a_1} \circ \alpha_{a_2} = \alpha_{a_1a_2} \in \text{Inn}(G) \tag{9.5}$$

である。また、例 10 で見たように、任意の $\alpha_a \in \text{Inn}(G)$ に対して、 $\alpha_a^{-1} = \alpha_{a^{-1}} \in \text{Inn}(G)$ であった。以上より、 $\text{Inn}(G)$ は二項演算と逆元を取る操作で閉じているので、 $\text{Aut}(G)$ の部分群となる。次に正規性を確かめる。任意の $\phi \in \text{Aut}(G), \alpha_a \in \text{Inn}(G)$ と $g \in G$ に対し、

$$(\phi \circ \alpha_a \circ \phi^{-1})(g) = \phi(a\phi^{-1}(g)a^{-1}) = \phi(a)\phi(\phi^{-1}(g))\phi(a^{-1}) = \phi(a)g\phi(a)^{-1} = \alpha_{\phi(a)}(g)$$

となるので、 $\phi \circ \alpha_a \circ \phi^{-1} = \alpha_{\phi(a)} \in \text{Inn}(G)$ 。よって、 $\text{Inn}(G)$ は $\text{Aut}(G)$ の正規部分群である。

ここで、(9.5) より少し面白いことがわかる。(9.5) は写像

$$\alpha : G \rightarrow \text{Inn}(G), g \mapsto \alpha_g$$

が全射群準同型であるという式に他ならない。ではこの核を考えてみると、

$$\begin{aligned} \text{Ker } \alpha &:= \{z \in G \mid \alpha_z = \text{id}_G\} \\ &= \{z \in G \mid zgz^{-1} = g, \forall g \in G\} \\ &= \{z \in G \mid zg = gz, \forall g \in G\} = Z(G) \end{aligned}$$

となる。自己同型群への写像を考えると核が中心となるような準同型が得られるのである。特に、 $Z(G) = \{e\}$ のとき ($G = \mathfrak{S}_n, n \geq 3$ など。第 6 回講義資料例 5 参照)、 α は同型となり、 $G \simeq \text{Inn}(G)$ となる。

代数学 I 第 11 回講義資料

担当：大矢 浩徳 (OYA Hironori)*

10.1 準同型定理

準同型 $\phi: G \rightarrow G'$ があると、その核 $\text{Ker } \phi$ は G の正規部分群となるのであった (第 10 回講義資料命題 9.3(2)). これより、剰余群 $G/\text{Ker } \phi$ を考えることができる。準同型に関する基本的な重要定理である以下の準同型定理は、この剰余群が実は ϕ の像 $\text{Im } \phi$ と群として同等なものになることを主張する：

定理 10.1 (準同型定理 (第 1 同型定理))

$\phi: G \rightarrow G'$ が準同型であるとき、写像

$$\bar{\phi}: G/\text{Ker } \phi \rightarrow \text{Im } \phi, g \text{Ker } \phi \mapsto \phi(g)$$

は well-defined であり、群同型になる。特に、 $G/\text{Ker } \phi \simeq \text{Im } \phi$ である。

証明. まず、写像 $\bar{\phi}$ の well-defined 性をチェックする。このためには、

$$g_1 \text{Ker } \phi = g_2 \text{Ker } \phi \text{ であるとき, } \phi(g_1) = \phi(g_2)$$

となることを示せばよい。 $g_1 \text{Ker } \phi = g_2 \text{Ker } \phi$ のとき、 $g_1 \stackrel{\text{Ker } \phi}{\sim}_L g_2$ なので (この記号については第 7 回講義資料定義 6.4 を参照)、ある $k \in \text{Ker } \phi$ が存在して、 $g_1 = g_2 k$ 。これより、

$$\phi(g_1) = \phi(g_2 k) = \phi(g_2)\phi(k) = \phi(g_2)$$

となる (最後の等式は $k \in \text{Ker } \phi$ より $\phi(k)$ が G' の単位元となることからわかる)。よって、 $\bar{\phi}$ の well-defined 性は示された。

次に、 $\bar{\phi}$ が準同型となることを示す。任意の $g_1 \text{Ker } \phi, g_2 \text{Ker } \phi \in G/\text{Ker } \phi$ に対し、

$$\bar{\phi}(g_1 \text{Ker } \phi \cdot g_2 \text{Ker } \phi) = \bar{\phi}(g_1 g_2 \text{Ker } \phi) = \phi(g_1 g_2) = \phi(g_1)\phi(g_2) = \bar{\phi}(g_1 \text{Ker } \phi)\bar{\phi}(g_2 \text{Ker } \phi)$$

となるので、 $\bar{\phi}$ は確かに準同型である。

後は $\bar{\phi}$ が全単射写像であることを見ればよい。まず、任意の $\phi(g) \in \text{Im } \phi$ に対し、 $\bar{\phi}(g \text{Ker } \phi) = \phi(g)$ であるから、 $\bar{\phi}$ は全射である。単射性を示す。 G の単位元を e 、 G' の単位元 (= $\text{Im } \phi$ の単位元) を e' と書く。 $\bar{\phi}(g \text{Ker } \phi) = e'$ となるとき、 $\bar{\phi}$ の定義より、 $\phi(g) = e'$ 。よって、 $g \in \text{Ker } \phi$ 。これは、 $g \stackrel{\text{Ker } \phi}{\sim}_L e$ に他ならないので、 $g \text{Ker } \phi = e \text{Ker } \phi$ である。これより、

$$\text{Ker } \bar{\phi} := \{g \text{Ker } \phi \in G/\text{Ker } \phi \mid \bar{\phi}(g \text{Ker } \phi) = e'\} = \{e \text{Ker } \phi\}$$

がわかるが、剰余群の定義から $e \text{Ker } \phi$ は $G/\text{Ker } \phi$ の単位元なので第 10 回講義資料命題 9.4 (2) より、 $\bar{\phi}$ が単射であることがわかる。 \square

例 1. 乗法群 \mathbb{C}^\times から \mathbb{R}^\times への絶対値を取る写像

$$|\cdot|: \mathbb{C}^\times \rightarrow \mathbb{R}^\times, z = x + iy \mapsto |z| := \sqrt{x^2 + y^2} \quad (x, y \in \mathbb{R})$$

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

は準同型であり,

$$\begin{aligned}\text{Ker } |\cdot| &:= \{z \in \mathbb{C}^\times \mid |z| = 1\} = \{e^{i\theta} \mid \theta \in \mathbb{R}\} (=:\mathbb{T}) \\ \text{Im } |\cdot| &:= \{r \in \mathbb{R}^\times \mid \text{ある } z \in \mathbb{C}^\times \text{ が存在して, } r = |z|\} = \mathbb{R}_{>0}\end{aligned}$$

となるのであった (第 10 回講義資料例 2). よって, 準同型定理より,

$$\mathbb{C}^\times / \mathbb{T} \xrightarrow{\sim} \mathbb{R}_{>0}, z\mathbb{T} \mapsto |z|$$

は同型である. これは“複素数平面において偏角の違い (\mathbb{T} の元倍の差) を同一視すると結局原点からの距離 ($\mathbb{R}_{>0}$) だけを見ていることになる”という事実に対応している.

ちなみに,

$$\phi: \mathbb{C}^\times \rightarrow \mathbb{T}, z \mapsto \frac{z}{|z|}$$

という写像を考えるとこれも準同型となっており (チェックせよ. また, 任意の $z \in \mathbb{C}^\times$ に対し, $\frac{z}{|z|} \in \mathbb{T}$ であることもあわせて確認せよ.),

$$\begin{aligned}\text{Ker } \phi &:= \{z \in \mathbb{C}^\times \mid \frac{z}{|z|} = 1\} = \{z \in \mathbb{C}^\times \mid z = |z|\} = \mathbb{R}_{>0} \\ \text{Im } \phi &:= \{t \in \mathbb{T} \mid \text{ある } z \in \mathbb{C}^\times \text{ が存在して, } t = \frac{z}{|z|}\} = \mathbb{T}\end{aligned}$$

である. なお, 最後の等式については任意の $\theta \in \mathbb{R}$ に対し, $\frac{e^{i\theta}}{|e^{i\theta}|} = e^{i\theta}$ であることよりわかる. こちらに対して準同型定理を用いると,

$$\mathbb{C}^\times / \mathbb{R}_{>0} \xrightarrow{\sim} \mathbb{T}, z\mathbb{R}_{>0} \mapsto \frac{z}{|z|}$$

が同型であることがわかる. こちらは“複素数平面において原点からの距離のみが違う元 ($\mathbb{R}_{>0}$ の元倍の差) を同一視すると結局偏角 (\mathbb{T}) だけを見ていることになる”という事実に対応している.

例 2. 加法群 \mathbb{R} から乗法群 \mathbb{C}^\times への写像

$$\phi: \mathbb{R} \rightarrow \mathbb{C}^\times, \theta \mapsto e^{2\pi i\theta}$$

は準同型である. 実際, 任意の $\theta_1, \theta_2 \in \mathbb{R}$ に対し,

$$\phi(\theta_1 + \theta_2) = e^{2\pi i(\theta_1 + \theta_2)} = e^{2\pi i\theta_1} e^{2\pi i\theta_2} = \phi(\theta_1)\phi(\theta_2)$$

が成立する. このとき,

$$\begin{aligned}\text{Ker } \phi &:= \{\theta \in \mathbb{R} \mid e^{2\pi i\theta} = 1\} = \mathbb{Z}, \\ \text{Im } \phi &:= \{z \in \mathbb{C}^\times \mid \text{ある } \theta \in \mathbb{R} \text{ が存在して, } z = e^{2\pi i\theta}\} = \mathbb{T}.\end{aligned}$$

よって, 準同型定理より,

$$\mathbb{R}/\mathbb{Z} \xrightarrow{\sim} \mathbb{T}, \theta + \mathbb{Z} \mapsto e^{2\pi i\theta}$$

は同型である.

例 3. n を正の整数とし, \mathbb{K} を \mathbb{Q}, \mathbb{R} または \mathbb{C} とする. n 次一般線型群 $GL_n(\mathbb{K})$ の各元に対し, その行列式を与える写像

$$\det: GL_n(\mathbb{K}) \rightarrow \mathbb{K}^\times, A \mapsto \det(A)$$

は全射準同型であり,

$$\text{Ker } \det := \{A \in GL_n(\mathbb{K}) \mid \det(A) = 1\} = SL_n(\mathbb{K})$$

となるのであった (第 10 回講義資料例 5). よって, 準同型定理より,

$$GL_n(\mathbb{K})/SL_n(\mathbb{K}) \xrightarrow{\sim} \mathbb{K}^\times, A \cdot SL_n(\mathbb{K}) \mapsto \det(A)$$

が同型であることがわかる.

例 4. n を 2 以上の整数とする. n 次対称群 \mathfrak{S}_n の各元に対し, その符号を与える写像

$$\text{sgn}: \mathfrak{S}_n \rightarrow \{1, -1\}, \sigma \mapsto \text{sgn } \sigma$$

は全射準同型であり,

$$\text{Ker sgn} := \{\sigma \in \mathfrak{S}_n \mid \text{sgn } \sigma = 1\} =: \mathfrak{A}_n \text{ (} n \text{ 次交代群)}$$

となるのであった (第 10 回講義資料例 6). よって, 準同型定理より,

$$\mathfrak{S}_n / \mathfrak{A}_n \xrightarrow{\sim} \{1, -1\}, \sigma \mathfrak{A}_n \mapsto \text{sgn } \sigma$$

が同型であることがわかる.

例 5. 任意の有限巡回群 $G = \langle g \rangle = \{g^m \mid m \in \mathbb{Z}\}$, $\text{ord } g < \infty$ に対し,

$$p: \mathbb{Z} \rightarrow G, m \mapsto g^m$$

は全射準同型であり,

$$\text{Ker } p = \langle \text{ord } g \rangle = \{k \text{ ord } g \mid k \in \mathbb{Z}\} = (\text{ord } g)\mathbb{Z}.$$

となるのであった (第 10 回講義資料例 8). よって, 準同型定理より,

$$\mathbb{Z}/(\text{ord } g)\mathbb{Z} \xrightarrow{\sim} G, [m]_{\text{ord } g} \mapsto g^m$$

が同型であることがわかる. よって, 第 10 回講義資料例 8 の $\text{ord } g = \infty$ の場合の考察と合わせて以下の命題が言える:

命題 10.2

n を正の整数とすると, 位数が n の巡回群は必ず $\mathbb{Z}/n\mathbb{Z}$ と同型である. また, 位数が無限の巡回群は必ず \mathbb{Z} と同型となる.

さらに, 第 8 回講義資料系 7.6 と合わせると次が言える.

命題 10.3

位数が素数 p の群は必ず $\mathbb{Z}/p\mathbb{Z}$ と同型である.

※以下のこの章の内容はおそらく講義内では時間的に扱えないものである. 難しさを感じる方はここから 10.2 節に飛んでもらって構わない. 一方で以下は興味のある方には是非勉強してほしい事項である. もしもこの範囲について質問がある場合には, 講義前後の時間には是非質問をしてもらいたい.

コラム: 有限群の分類

命題 10.3 では群の位数を素数とすると, そのような群は同型なものを同一視すると 1 通りしかないということを見た. 群の定義は非常に抽象的なものであったのに, 位数によってはこれほどまでに構造がきっちり決まってしまうというのは大変面白い話である. このように, 「正の整数 n を与えたときに, 同型なものを同一視したうえで位数 n の群は何通りあるか?」という問題を位数 n の群の分類問題という. その中でも特に大事なのは, 以下で定義される単純群の分類である.

定義 10.4

群 G が自明な正規部分群 $G, \{e\}$ 以外に正規部分群を持たないとき, G を単純群 (simple group) という.

もし群 G が単純群でない場合, G は非自明な正規部分群 N を含む. このとき, G の構造は, 正規部分群 N とそれによる剰余群 G/N という G よりも小さな群を調べることから調べ始めることができる (もちろん N と G/N の構造が分かれば G の構造が全てわかるわけではないのだが, 大きな助けにはなる). この意味で, これ以上分割できない “群論の世界の原子” に当たるものが単純群なのである. これは自然数の世界で素数が重要

であったことも似ていると考えればその重要性がわかるであろう。そして、なんと驚くべきことに有限単純群の分類はわかっているのである！分類は以下の通りである。

- (1) 巡回群 $\mathbb{Z}/p\mathbb{Z}$, p は素数.
- (2) 交代群 \mathfrak{A}_n , $n \geq 5$. (第 10 回講義資料例 6 参照)
- (3) Lie 型の単純群 (Tits 群を含む).
- (4) 26 個の散在型単純群.

(1)–(3) の型については、それぞれ無限個存在しており、それ以外だと (4) の 26 個だけになるという状況である。(4) の 26 個の例外の中で最も大きい群の位数は

$$808017424794512875886459904961710757005754368000000000$$

であり、モンスター群と呼ばれる。この分類定理は (主に)20 世紀の多くの数学者による膨大な研究の賜物であり、証明を説明することは到底できないが、結果としては知っていても良いであろう。歴史的な部分やより詳細について知りたい方は、『鈴木 通夫, “有限単純群の分類”, 数学, 1982 年 34 卷 3 号, 193–210 <https://doi.org/10.11429/sugaku1947.34.193>』などが参考になる。他にも「有限単純群の分類」で検索すると様々な面白い記事に当たることができる。

例 6 (やや発展). G を群とする. G から自己同型群 $\text{Aut}(G) := \{\phi: G \rightarrow G \mid \phi \text{ は同型}\}$ への写像

$$\alpha: G \rightarrow \text{Aut}(G), a \mapsto \alpha_a$$

(ただし, α_a は $\alpha_a: G \rightarrow G, g \mapsto aga^{-1}$ で定まる写像.) は準同型であり,

$$\begin{aligned} \text{Ker } \alpha &= Z(G) \quad (G \text{ の中心}) \\ \text{Im } \alpha &:= \{\alpha_a \mid a \in G\} (= \text{Inn}(G)) \end{aligned}$$

となるのであった (第 10 回講義資料例 11). よって, 準同型定理より,

$$G/Z(G) \xrightarrow{\sim} \text{Inn}(G), gZ(G) \mapsto \alpha_g$$

が同型であることがわかる。一見とらえどころのない内部自己同型群 $\text{Inn}(G)$ は $G/Z(G)$ に同型だったのである。例えば, n を正の整数とし, \mathbb{K} を \mathbb{Q}, \mathbb{R} または \mathbb{C} とするとき,

$$\text{Inn}(GL_n(\mathbb{K})) \simeq GL_n(\mathbb{K})/Z(GL_n(\mathbb{K})) =: PGL_n(\mathbb{K}) \quad (\text{射影一般線型群})$$

となる。射影一般線型群は一般線型群の内部自己同型群に同型な群だったのである。

定理 10.5 (第 2 同型定理)

G を群, H を G の部分群, N を G の正規部分群とする。このとき,

$$HN := \{hn \mid h \in H, n \in N\}$$

は G の部分群, $H \cap N$ は H の正規部分群であり,

$$H/(H \cap N) \rightarrow HN/N, h(H \cap N) \mapsto hN \tag{10.1}$$

は well-defined な群同型になる。特に, $H/(H \cap N) \simeq HN/N$ である。

証明.

HN が G の部分群であること : 任意の $h_1n_1, h_2n_2 \in HN$ ($h_1, h_2 \in H, n_1, n_2 \in N$) に対し,

$$h_1n_1h_2n_2 = h_1h_2(h_2^{-1}n_1h_2)n_2.$$

いま N は正規部分群なので $h_2^{-1}n_1h_2 \in N$ であるから, $(h_2^{-1}n_1h_2)n_2 \in N$ であるので, 上式の右辺は HN の元である. よって, $h_1n_1h_2n_2 \in HN$.

任意の $hn \in HN$ ($h \in H, n \in N$) に対して,

$$(hn)^{-1} = n^{-1}h^{-1} = h^{-1}(hn^{-1}h^{-1}).$$

いま N は正規部分群なので $hn^{-1}h^{-1} \in N$ であるから, 上式の右辺は HN の元である. よって, $(hn)^{-1} \in HN$. 以上より, HN は二項演算と逆元を取る操作で閉じているので, G の部分群である.

$H \cap N$ が H の正規部分群であること, (10.1) が well-defined な群同型であること : 写像

$$\phi: H \rightarrow HN/N, h \mapsto hN$$

を考える. 任意の $h_1, h_2 \in H$ に対し, $\phi(h_1h_2) = h_1h_2N = h_1N \cdot h_2N = \phi(h_1) \cdot \phi(h_2)$ となるので, ϕ は準同型である. また, 任意の $h \in H, n \in N$ に対して, $hnN = hN \in HN/N$ なので,

$$HN/N = \{hnN \mid h \in H, n \in N\} = \{hN \mid h \in H\} = \text{Im } \phi.$$

さらに,

$$\text{Ker } \phi = \{h \in H \mid hN = N\} = \{h \in H \mid h \in N\} = H \cap N.$$

これより, 第 10 回講義資料命題 9.3 (2) から $H \cap N$ は H の正規部分群であり, 準同型定理から,

$$H/(H \cap N) \xrightarrow{\sim} HN/N, h(H \cap N) \mapsto hN$$

は well-defined な群同型になる. □

例 7. n を 3 以上の整数とし, $D_n = \{\sigma^k\tau^\ell \mid k = 0, \dots, n-1, \ell = 0, 1\}$ を n 次二面体群とする ($\sigma^n = e, \tau^2 = e, \sigma^k\tau = \tau\sigma^{-k}$ ($k \in \mathbb{Z}$)). $H = \langle \tau \rangle = \{e, \tau\}, N = \langle \sigma \rangle = \{e, \sigma, \dots, \sigma^{n-1}\}$ とする. H は D_n の正規でない部分群であり, N は D_n の正規部分群であったことを思い出そう (第 9 回講義資料例 2, 命題 8.3 参照). このとき,

$$HN := \{\tau^\ell\sigma^k \mid \ell = 0, 1, k = 0, \dots, n-1\} = D_n \quad H \cap N = \{e\}$$

であるので, 第 2 同型定理より,

$$H/\{e\} = H \xrightarrow{\sim} D_n/N, \tau^\ell \mapsto \tau^\ell N \quad (\ell = 0, 1)$$

は well-defined な群同型になる.

定理 10.6 (第 3 同型定理)

G を群, M, N を $M \subset N$ を満たす G の正規部分群とする. このとき, 剰余群 N/M は剰余群 G/M の正規部分群であり,

$$(G/M)/(N/M) \rightarrow G/N, (gM) \cdot N/M \mapsto gN$$

は well-defined な群同型になる. 特に, $(G/M)/(N/M) \simeq G/N$ である. (M を “約分” できる.)

証明. 写像

$$\phi: G/M \rightarrow G/N, gM \mapsto gN$$

を考える. これが well-defined であることは以下のように確かめられる:

$$g_1M = g_2M \text{ であるとき, } g_1N = g_2N$$

となることを示せばよい. $g_1M = g_2M$ のとき, $g_1 \stackrel{M}{\sim} g_2$ なので, ある $m \in M$ が存在して, $g_1 = g_2m$ となる. いま $M \subset N$ であるので, m は N の元でもあるから, このとき $g_1 \stackrel{N}{\sim} g_2$ でもある. よって, $g_1N = g_2N$.

いま, 任意の $g_1, g_2 \in G$ に対し, $\phi(g_1M \cdot g_2M) = \phi(g_1g_2M) = g_1g_2N = g_1N \cdot g_2N = \phi(g_1M) \cdot \phi(g_2M)$ となるので, ϕ は準同型である. また,

$$\begin{aligned}\text{Im } \phi &= \{\phi(gM) \mid g \in G\} = \{gN \mid g \in G\} = G/N, \\ \text{Ker } \phi &= \{gM \in G/M \mid gN = N\} = \{gM \in G/M \mid g \in N\} = N/M.\end{aligned}$$

よって, 第 10 回講義資料命題 9.3 (2) から N/M は G/M の正規部分群であり, 準同型定理から,

$$(G/M)/(N/M) \xrightarrow{\sim} G/N, (gM) \cdot N/M \mapsto gN$$

は well-defined な群同型になる. □

例 8. \mathbb{R} 上の 2 次一般線型群 $GL_2(\mathbb{R})$ からの写像

$$\phi: GL_2(\mathbb{R}) \rightarrow \{1, -1\}, A \mapsto \frac{\det(A)}{|\det(A)|}$$

を考えるとこれは全射準同型である (チェックせよ). このとき,

$$\begin{aligned}\text{Ker } \phi &:= \{A \in GL_2(\mathbb{R}) \mid \frac{\det(A)}{|\det(A)|} = 1\} \\ &= \{A \in GL_2(\mathbb{R}) \mid \det(A) = |\det(A)|\} \\ &= \{A \in GL_2(\mathbb{R}) \mid \det(A) > 0\} =: GL_2^+(\mathbb{R})\end{aligned}$$

となる (この正規部分群は第 9 回レポート課題で扱った). よって, 準同型定理より,

$$GL_2(\mathbb{R})/GL_2^+(\mathbb{R}) \xrightarrow{\sim} \{1, -1\}, A \cdot GL_2^+(\mathbb{R}) \mapsto \frac{\det(A)}{|\det(A)|}$$

が同型であることがわかる. ここで, $GL_2(\mathbb{R})$ の中心は

$$Z(GL_2(\mathbb{R})) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{R}^\times \right\}$$

であり (第 6 回講義資料例 5), 任意の $a \in \mathbb{R}^\times$ に対し, $\det \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = a^2 > 0$ なので, $Z(GL_2(\mathbb{R}))$ は $GL_2^+(\mathbb{R})$ の部分群である. これより, G を $GL_2(\mathbb{R})$, M を $Z(GL_2(\mathbb{R}))$, N を $GL_2^+(\mathbb{R})$ とすると, これは第 3 同型定理が適用できる状況になっている. よって, 第 3 同型定理より,

$$\begin{aligned} & \underbrace{(GL_2(\mathbb{R})/Z(GL_2(\mathbb{R})))}_{\cup} / \underbrace{(GL_2^+(\mathbb{R})/Z(GL_2(\mathbb{R})))}_{\cup} \xrightarrow{\sim} GL_2(\mathbb{R})/GL_2^+(\mathbb{R}) (\simeq \{1, -1\}), \\ & (A \cdot Z(GL_2(\mathbb{R}))) \cdot GL_2^+(\mathbb{R}) / Z(GL_2(\mathbb{R})) \mapsto A \cdot GL_2^+(\mathbb{R}) \end{aligned}$$

は well-defined な群同型になる. ちなみに, $GL_2(\mathbb{R})/Z(GL_2(\mathbb{R}))$ は $PGL_2(\mathbb{R})$ と書かれたことも合わせて思い出しておこう.

10.2 中国式剰余定理

準同型定理の応用として, 中国式剰余定理を述べよう. このために 1 つ用語を準備する.

定義 10.7

G_1, G_2 を群とし、それぞれの単位元を e_1, e_2 とする。 G_1 と G_2 直積集合

$$G_1 \times G_2 := \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}$$

に二項演算 $\cdot: (G_1 \times G_2) \times (G_1 \times G_2) \rightarrow G_1 \times G_2$ を

$$(g_1, g_2) \cdot (h_1, h_2) := (g_1 h_1, g_2 h_2), \forall g_1, h_1 \in G_1, g_2, h_2 \in G_2$$

と定義する。この二項演算によって、 $G_1 \times G_2$ は再び群となる (チェックは容易なのでここでは省略する。試してみよ。)。ここで、 $G_1 \times G_2$ の単位元は (e_1, e_2) であり、 (g_1, g_2) の逆元は (g_1^{-1}, g_2^{-1}) である。この群を G_1 と G_2 の直積 (**direct product**) という。

以下は直積の基本性質である。この命題も証明は容易なので省略する。

命題 10.9

G_1, G_2 を群とし、それぞれの単位元を e_1, e_2 とする。このとき、以下が成立する。

- (1) $G_1 \times G_2$ の位数は $|G_1| \cdot |G_2|$ である。
- (2) $\text{pr}_1: G_1 \times G_2 \rightarrow G_1, (g_1, g_2) \mapsto g_1, \text{pr}_2: G_1 \times G_2 \rightarrow G_2, (g_1, g_2) \mapsto g_2$ は全射準同型である。(自然な射影 (**canonical projection**) と呼ばれる。)
- (3) $\iota_1: G_1 \rightarrow G_1 \times G_2, g_1 \mapsto (g_1, e_2), \iota_2: G_2 \rightarrow G_1 \times G_2, g_2 \mapsto (e_1, g_2)$ は単射準同型である。(自然な入射 (**canonical injection**) と呼ばれる。)
- (4) $\text{Ker pr}_2 = \text{Im } \iota_1 = G_1 \times \{e_2\} \simeq G_1, \text{Ker pr}_1 = \text{Im } \iota_2 = \{e_1\} \times G_2 \simeq G_2$ 。とくに、 $G_1 \simeq G_1 \times \{e_2\}, G_2 \simeq \{e_1\} \times G_2$ は $G_1 \times G_2$ の正規部分群である。

例 9. $\mathbb{Z}/2\mathbb{Z}$ と $\mathbb{Z}/3\mathbb{Z}$ の直積 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ を考えてみよう。まず集合としては、

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = \{([0]_2, [0]_3), ([0]_2, [1]_3), ([0]_2, [2]_3), ([1]_2, [0]_3), ([1]_2, [1]_3), ([1]_2, [2]_3)\}$$

であり、位数は $2 \cdot 3 = 6$ である (命題 10.9 (1))。二項演算は例えば、

$$([1]_2, [1]_3) + ([0]_2, [2]_3) = ([1]_2 + [0]_2, [1]_3 + [2]_3) = ([1]_2, [0]_3)$$

というようにそれぞれの成分ごとに計算される (ここでは直積を考えている群が共に加法群なので直積の二項演算も $+$ で書いた)。ちなみに、

$$\begin{aligned} ([1]_2, [1]_3) + ([1]_2, [1]_3) &= ([0]_2, [2]_3) & ([0]_2, [2]_3) + ([1]_2, [1]_3) &= ([1]_2, [0]_3) & ([1]_2, [0]_3) + ([1]_2, [1]_3) &= ([0]_2, [1]_3) \\ ([0]_2, [1]_3) + ([1]_2, [1]_3) &= ([1]_2, [2]_3) & ([1]_2, [2]_3) + ([1]_2, [1]_3) &= ([0]_2, [0]_3) \end{aligned}$$

となるので、 $\text{ord}([1]_2, [1]_3) = 6$ であり、 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ は $([1]_2, [1]_3)$ によって生成される巡回群 $\langle ([1]_2, [1]_3) \rangle$ であることがわかる。よって、命題 10.2 より、これは $\mathbb{Z}/6\mathbb{Z}$ と同型であり、具体的な同型写像は

$$\mathbb{Z}/6\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, [a]_6 \mapsto ([a]_2, [a]_3)$$

で与えられることがわかる (生成元 $[1]_6$ を生成元 $([1]_2, [1]_3)$ にうつした)。次の中国剰余定理はこの同型の一般化である。

定理 10.10 (中国剰余定理)

n_1, n_2 を互いに素な 2 以上の自然数とする。このとき、

$$\mathbb{Z}/n_1 n_2 \mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/n_1 \mathbb{Z} \times \mathbb{Z}/n_2 \mathbb{Z}, [a]_{n_1 n_2} \mapsto ([a]_{n_1}, [a]_{n_2})$$

は well-defined な群同型となる。特に、 $\mathbb{Z}/n_1 n_2 \mathbb{Z} \simeq \mathbb{Z}/n_1 \mathbb{Z} \times \mathbb{Z}/n_2 \mathbb{Z}$ である。

証明. 写像

$$\phi: \mathbb{Z} \rightarrow \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}, a \mapsto ([a]_{n_1}, [a]_{n_2})$$

を考える. 任意の $a, b \in \mathbb{Z}$ に対し, $\phi(a+b) = ([a+b]_{n_1}, [a+b]_{n_2}) = ([a]_{n_1}, [a]_{n_2}) + ([b]_{n_1}, [b]_{n_2}) = \phi(a) + \phi(b)$ となるので, ϕ は準同型である. また,

$$\begin{aligned} \text{Ker } \phi &= \{a \in \mathbb{Z} \mid ([a]_{n_1}, [a]_{n_2}) = ([0]_{n_1}, [0]_{n_2})\} \\ &= \{a \in \mathbb{Z} \mid a \text{ は } n_1 \text{ と } n_2 \text{ で割り切れる}\} \\ &= \{a \in \mathbb{Z} \mid a \text{ は } n_1 n_2 \text{ で割り切れる}\} \quad (\text{ここで, } n_1 \text{ と } n_2 \text{ が互いに素であることを用いた.}) \\ &= \{n_1 n_2 k \in \mathbb{Z} \mid k \in \mathbb{Z}\} = n_1 n_2 \mathbb{Z} \end{aligned}$$

これより, 準同型定理から,

$$\mathbb{Z}/n_1 n_2 \mathbb{Z} \xrightarrow{\sim} \text{Im } \phi, [a]_{n_1 n_2} \mapsto ([a]_{n_1}, [a]_{n_2})$$

は well-defined な群同型になる. ここで, $\text{Im } \phi$ は $\mathbb{Z}/n_1 n_2 \mathbb{Z}$ と同型であることから位数 $n_1 n_2$ の群となるが, 一方 $\text{Im } \phi$ は位数 $n_1 n_2$ の群である $\mathbb{Z}/n_1 \mathbb{Z} \times \mathbb{Z}/n_2 \mathbb{Z}$ の部分群であったことに注意すると, 結局 $\text{Im } \phi = \mathbb{Z}/n_1 \mathbb{Z} \times \mathbb{Z}/n_2 \mathbb{Z}$ となることがわかる. よって,

$$\mathbb{Z}/n_1 n_2 \mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/n_1 \mathbb{Z} \times \mathbb{Z}/n_2 \mathbb{Z}, [a]_{n_1 n_2} \mapsto ([a]_{n_1}, [a]_{n_2})$$

が同型となることがわかる. □

ちなみに, 中国剰余定理の仮定である「 n_1, n_2 は互いに素」は重要であり, 実際 n_1, n_2 が互いに素でないとき必ず

$$\mathbb{Z}/n_1 n_2 \mathbb{Z} \not\cong \mathbb{Z}/n_1 \mathbb{Z} \times \mathbb{Z}/n_2 \mathbb{Z}$$

となる. 例えば, $\mathbb{Z}/60\mathbb{Z} \not\cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ などとなる. 今回の本レポート課題となっているので, 理由を考えてみて欲しい (ヒント: 各元の位数に着目せよ).

最後にこの定理の“意味”を考えてみよう. $\mathbb{Z}/n\mathbb{Z}$ において $[a]_n$ は“ a を n で割った余りを見る”というように考えられるのであった. このため, n_1 と n_2 が互いに素のとき,

$$\phi_{n_1, n_2}: \mathbb{Z}/n_1 n_2 \mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/n_1 \mathbb{Z} \times \mathbb{Z}/n_2 \mathbb{Z}, [a]_{n_1 n_2} \mapsto ([a]_{n_1}, [a]_{n_2})$$

という同型が存在するという事実は,

n_1 と n_2 が互いに素のとき, 任意の $0 \leq r_1 < n_1, 0 \leq r_2 < n_2$ に対して, 『 n_1 で割った余りが r_1 , n_2 で割った余りが r_2 となるような整数 a 』^{*1} が $\text{mod } n_1 n_2$ でただ一つ存在する.

ということに他ならない. ϕ_{n_1, n_2} が全単射なので, 任意の $0 \leq r_1 < n_1, 0 \leq r_2 < n_2$ に対して, $\phi_{n_1, n_2}^{-1}([r_1]_{n_1}, [r_2]_{n_2}) \in \mathbb{Z}/n_1 n_2 \mathbb{Z}$ が定まり, これを $[a]_{n_1 n_2}$ とすると, a は n_1 で割った余りが r_1 , n_2 で割った余りが r_2 となるような整数なのである.

具体的には次のように計算すればよい.

^{*1} このような数を求める問題が古代中国の文献『孫子算経』に登場しており, そのことが中国剰余定理という名前の由来となっている.

n_1 と n_2 を互いに素な整数としたとき, n_1 で割った余りが r_1 , n_2 で割った余りが r_2 となるような整数 a を求める ($0 \leq r_1 < n_1, 0 \leq r_2 < n_2$).

(Step 1) 拡張ユークリッド互除法を用いて $n_1x + n_2y = 1$ を満たす整数の組 (x, y) を 1 つ求める (第 1, 2 回講義資料参照). 見つけた解を (x_0, y_0) とする.

(Step 2) いま,

$$\begin{aligned}\phi_{n_1, n_2}([n_1x_0]_{n_1n_2}) &= ([n_1x_0]_{n_1}, [n_1x_0]_{n_2}) = ([n_1x_0]_{n_1}, [n_1x_0 + n_2y_0]_{n_2}) = ([0]_{n_1}, [1]_{n_2}) \\ \phi_{n_1, n_2}([n_2y_0]_{n_1n_2}) &= ([n_2y_0]_{n_1}, [n_2y_0]_{n_2}) = ([n_1x_0 + n_2y_0]_{n_1}, [n_2y_0]_{n_2}) = ([1]_{n_1}, [0]_{n_2})\end{aligned}$$

であることに注意すると,

$$\begin{aligned}\phi_{n_1, n_2}([r_2n_1x_0 + r_1n_2y_0]_{n_1n_2}) &= \phi_{n_1, n_2}([r_2n_1x_0]_{n_1n_2}) + \phi_{n_1, n_2}([r_1n_2y_0]_{n_1n_2}) \\ &= ([0]_{n_1}, [r_2]_{n_2}) + ([r_1]_{n_1}, [0]_{n_2}) = ([r_1]_{n_1}, [r_2]_{n_2}).\end{aligned}$$

となることがわかるので,

$$\phi_{n_1, n_2}^{-1}([r_1]_{n_1}, [r_2]_{n_2}) = [r_2n_1x_0 + r_1n_2y_0]_{n_1n_2}.$$

よって, 求める a は $r_2n_1x_0 + r_1n_2y_0 + n_1n_2k$ (k は任意の整数).

この解法を用いて 1 つ問題を解いてみよう.

例題

39 で割ると 2 余り, 119 で割ると 3 余る整数を 1 つ求めよ.

解答例. 【まず拡張ユークリッド互除法で $39x + 119y = 1$ を満たす整数の組 (x, y) を見つける.】

$$119 = 3 \times 39 + 2$$

$$39 = 19 \times 2 + 1$$

より, $1 = 39 - 19 \times 2 = 39 - 19 \times (119 - 3 \times 39) = 58 \times 39 + (-19) \times 119$.

【 $(x_0, y_0) = (58, -19)$, $r_1 = 2$, $r_2 = 3$ として, $r_2(39x_0) + r_1(119y_0)$ を計算】

これより求める値の 1 つは,

$$3 \times (39 \times 58) + 2 \times (119 \times (-19)) = 2264.$$

□

※この解法において, r_1 を n_2y_0 の方に掛けて, r_2 を n_1x_0 の方に掛けないといけないという点は間違えがちである。「この方法でなぜ求まるか」という原理も含めて解法を覚えておくことが望ましい. また, この問題は検算ができるので検算を行うこと.

代数学 I 第 12 回講義資料

担当：大矢 浩徳 (OYA Hironori)*

11.1 群の作用

群とは“対称性”の抽象化であるということを第 1, 2 回講義資料内で述べた。今回は“ある集合 X が群 G の対称性を持っている”という状況を数学的に定式化する。これが群 G の集合 X への作用である。

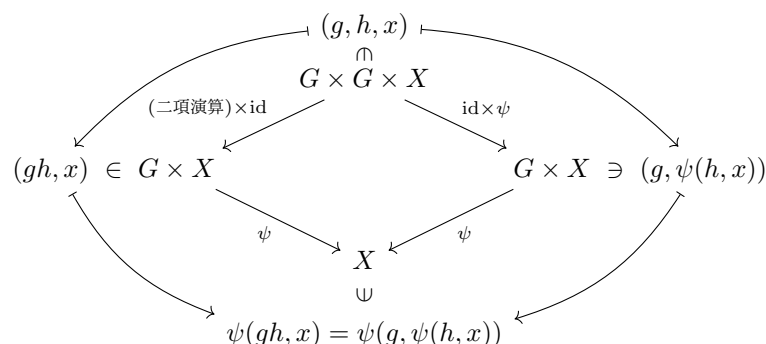
定義 11.1

群 G と集合 X に対し、 X 上の G の作用 (action of G on X)*¹とは、写像

$$\psi: G \times X \rightarrow X, (g, x) \mapsto \psi(g, x)$$

であって、次の 2 条件を満たすものを言う。

- (1) 任意の $x \in X$ に対し、 $\psi(e, x) = x$ 。ただし、 e は G の単位元。
- (2) 任意の $g, h \in G, x \in X$ に対し、 $\psi(gh, x) = \psi(g, \psi(h, x))$ 。この条件は以下の図式で表される。



作用の定義条件は $\psi(g, x)$ を単に $g \cdot x$ と書くことにすると以下のように見やすくなる。以下ではこの記号をしばしば用いる。(群の二項演算と混乱しないように。)

- (1)' 任意の $x \in X$ に対し、 $e \cdot x = x$ 。
- (2)' 任意の $g, h \in G, x \in X$ に対し、 $gh \cdot x = g \cdot (h \cdot x)$ 。

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

*¹ ここで定義した作用は左作用と呼ばれるものである。講義内では左作用のみを扱うのでこれを単に作用と呼ぶことにする。集合 X 上の群 G の右作用 (right action of G on X) とは、写像

$$\psi: G \times X \rightarrow X, (g, x) \mapsto \psi(g, x)$$

であって、次の 2 条件を満たすものを言う。

- (i) 任意の $x \in X$ に対し、 $\psi(e, x) = x$ 。ただし、 e は G の単位元。(左作用の定義条件の (1) と同じ)
- (ii) 任意の $g, h \in G, x \in X$ に対し、 $\psi(gh, x) = \psi(h, \psi(g, x))$ 。

右作用の定義条件は $\psi(g, x)$ を単に $x \cdot g$ と書くことにすると以下のように見やすくなる。

- (i)' 任意の $x \in X$ に対し、 $x \cdot e = x$ 。
- (ii)' 任意の $g, h \in G, x \in X$ に対し、 $x \cdot gh = (x \cdot g) \cdot h$ 。

例 1. n を正の整数とし, $X := \{1, 2, \dots, n\}$ としたとき, 写像

$$\psi: \mathfrak{S}_n \times X \rightarrow X, (\sigma, i) \mapsto \sigma \cdot i := \sigma(i)$$

は X 上の \mathfrak{S}_n の作用を定める. 例えば, $n = 5$ の場合,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix} \cdot 1 = 3, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix} \cdot 2 = 1, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix} \cdot 5 = 5$$

などとなる. これが作用であることは次のように確かめられる.

$$(1) \text{ 任意の } i \in X \text{ に対し, } \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix} \cdot i = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix} (i) = i.$$

$$(2) \text{ 任意の } \sigma_1, \sigma_2 \in \mathfrak{S}_n, i \in X \text{ に対し, } (\sigma_1 \circ \sigma_2) \cdot i = (\sigma_1 \circ \sigma_2)(i) = \sigma_1(\sigma_2(i)) = \sigma_1 \cdot (\sigma_2 \cdot i).$$

例 2. 例 1 は次のように一般化できる. X を任意の空でない集合とする. 第 5 回講義資料例 1 で考えた, X から X への全単射写像全体のなす群

$$B(X) := \{f: X \rightarrow X \mid f \text{ は全単射}\}$$

を考える. ここで, 二項演算は写像の合成 \circ , 単位元は X 上の恒等写像 id_X であった. さらに, n 次対称群 \mathfrak{S}_n の定義は X を $\{1, 2, \dots, n\}$ としたときの $B(X) = B(\{1, 2, \dots, n\})$ であったということを思い出しておこう (第 5 回講義資料例 2)*2. このため, 上の $B(X)$ という群は対称群の一般化とすることができる.

さて, 写像 ψ を

$$\psi: B(X) \times X \rightarrow X, (f, x) \mapsto f \cdot x := f(x)$$

とすると, これは X 上の $B(X)$ の作用を定める. これは例 1 の一般化であり, 作用であることのチェックは例 1 と全く同様である.

例 3. 写像

$$\psi: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, (a, n) \mapsto n - a$$

は集合 \mathbb{Z} 上の加法群 \mathbb{Z} の作用を定める ($\mathbb{Z} \times \mathbb{Z}$ の左側の \mathbb{Z} が加法群と思う方). これが作用であることは次のように確かめられる.

$$(1) \text{ 任意の } n \in \mathbb{Z} \text{ に対し, } \psi(0, n) = n - 0 = n.$$

$$(2) \text{ 任意の } a_1, a_2, n \in \mathbb{Z} \text{ に対し, } \psi(a_1 + a_2, n) = n - (a_1 + a_2) = (n - a_2) - a_1 = \psi(a_1, \psi(a_2, n)).$$

ちなみに引き算 $-$ は結合法則を満たさないため, 集合 \mathbb{Z} は $-$ を二項演算として群にはならなかったことを合わせて思い出そう (第 4 回講義資料例 1). 引き算は加法群 \mathbb{Z} の作用なのである.

写像

$$\psi': \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, (a, n) \mapsto a^2 + n$$

は集合 \mathbb{Z} 上の加法群 \mathbb{Z} の作用ではない. なぜなら, このとき

$$\psi'(a_1 + a_2, n) = (a_1 + a_2)^2 + n \neq a_1^2 + a_2^2 + n = \psi'(a_1, \psi'(a_2, n)) \quad (a_1 a_2 \neq 0 \text{ のとき})$$

となり, 作用の定義条件の (2) が満たされないためである (なお, 定義条件 (1) は満たされる).

写像

$$\psi'': \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, (a, n) \mapsto 0 \quad (\text{全てを } 0 \text{ に送る})$$

は集合 \mathbb{Z} 上の加法群 \mathbb{Z} の作用ではない. なぜなら, このとき

$$\psi''(0, n) = 0 \neq n \quad (n \neq 0 \text{ のとき})$$

となり, 作用の定義条件の (1) が満たされないためである (なお, 定義条件 (2) は満たされる).

*2 対称群の定義は計算にある程度慣れてくると忘れがちである. ここでもう一度復習しておこう.

例 4. n を正の整数とし, \mathbb{K} を \mathbb{Q}, \mathbb{R} または \mathbb{C} とする. このとき, 写像

$$\psi: GL_n(\mathbb{K}) \times \mathbb{K}^n \rightarrow \mathbb{K}^n, (A, \mathbf{v}) \mapsto A\mathbf{v} \text{ (行列の積)}$$

は \mathbb{K}^n 上の一般線型群 $GL_n(\mathbb{K})$ の作用を定める (\mathbb{K}^n の元は n 次列ベクトルと考える). 例えば, $n = 2$ のときこの写像は具体的には以下である:

$$\psi: GL_2(\mathbb{K}) \times \mathbb{K}^2 \rightarrow \mathbb{K}^2, \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} x \\ y \end{pmatrix} \right) \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$$

これが作用であることは次のように確かめられる.

- (1) 任意の $\mathbf{v} \in \mathbb{K}^n$ に対し, $\psi(I_n, \mathbf{v}) = I_n \mathbf{v} = \mathbf{v}$. ただし, I_n は n 次単位行列 ($GL_n(\mathbb{K})$ の単位元).
- (2) 任意の $A_1, A_2 \in GL_n(\mathbb{K}), \mathbf{v} \in \mathbb{K}^n$ に対し, $\psi(A_1 A_2, \mathbf{v}) = (A_1 A_2) \mathbf{v} = A_1 (A_2 \mathbf{v}) = \psi(A_1, \psi(A_2, \mathbf{v}))$ (行列の積の結合法則).

また,

$$\text{Mat}_n(\mathbb{K}) := \{A \mid A \text{ は } \mathbb{K} \text{ の元を成分とする } n \times n \text{ 行列} \}$$

とすると, 写像

$$\psi': GL_n(\mathbb{K}) \times \text{Mat}_n(\mathbb{K}) \rightarrow \text{Mat}_n(\mathbb{K}), (P, A) \mapsto PAP^{-1}$$

は $\text{Mat}_n(\mathbb{K})$ 上の $GL_n(\mathbb{K})$ の作用を定める. これが作用であることは次のように確かめられる.

- (1) 任意の $A \in \text{Mat}_n(\mathbb{K})$ に対し, $\psi'(I_n, A) = I_n A I_n^{-1} = A$.
- (2) 任意の $P_1, P_2 \in GL_n(\mathbb{K}), A \in \text{Mat}_n(\mathbb{K})$ に対し,

$$\psi'(P_1 P_2, A) = P_1 P_2 A (P_1 P_2)^{-1} = P_1 (P_2 A P_2^{-1}) P_1^{-1} = \psi'(P_1, \psi'(P_2, A)).$$

例 5. \mathbb{R} 上の実数値連続関数全体のなす集合を $C^0(\mathbb{R})$ と書く. このとき,

$$\psi: \mathbb{R} \times C^0(\mathbb{R}) \rightarrow C^0(\mathbb{R}), (r, f(x)) \mapsto f(x+r) \text{ (関数の平行移動)}$$

は $C^0(\mathbb{R})$ 上の加法群 \mathbb{R} の作用を定める. これが作用であることは次のように確かめられる.

- (1) 任意の $f(x) \in C^0(\mathbb{R})$ に対し, $\psi(0, f(x)) = f(x+0) = f(x)$.
- (2) 任意の $r_1, r_2 \in \mathbb{R}, f(x) \in C^0(\mathbb{R})$ に対し,

$$\psi(r_1 + r_2, f(x)) = f(x + (r_1 + r_2)) = f((x + r_1) + r_2) = \psi(r_1, f(x + r_2)) = \psi(r_1, \psi(r_2, f(x))).$$

例 6. G を群とし, e をその単位元とする. このとき, 二項演算の写像

$$\psi_\ell: G \times G \rightarrow G, (g, h) \mapsto gh$$

は集合 G 上の群 G の作用を定めているとも考えられる ($G \times G$ の左側の G が群と思う方). 実際, 以下のよう
に作用であることが確かめられる.

- (1) 任意の $g \in G$ に対し, $\psi_\ell(e, g) = eg = g$.
- (2) 任意の $g_1, g_2, h \in G$ に対し, $\psi_\ell(g_1 g_2, h) = (g_1 g_2) h = g_1 (g_2 h) = \psi_\ell(g_1, \psi_\ell(g_2, h))$ (群の二項演算の結合法則).

また, H を G の部分群とし, 写像

$$\psi_{\ell, H}: G \times (G/H) \rightarrow G/H, (g, g'H) \mapsto gg'H$$

を考えると, これは商集合 G/H 上の群 G の作用を定める. 作用であることのチェックは上の ψ_ℓ の場合と全く同様である.

写像

$$\psi_{\text{ad}}: G \times G \rightarrow G, (g, h) \mapsto ghg^{-1}$$

は集合 G 上の群 G の作用を定める ($G \times G$ の左側の G が群と思う方). これが作用であることは次のように確かめられる.

- (1) 任意の $g \in G$ に対し, $\psi_{\text{ad}}(e, g) = ege^{-1} = g$.
- (2) 任意の $g_1, g_2, h \in G$ に対し,

$$\psi_{\text{ad}}(g_1g_2, h) = (g_1g_2)h(g_1g_2)^{-1} = g_1(g_2hg_2^{-1})g_1^{-1} = \psi_{\text{ad}}(g_1, \psi_{\text{ad}}(g_2, h)).$$

作用 ψ_{ad} は随伴作用 (**adjoint action**) と呼ばれる.

命題 11.2

G を群, X を集合とする.

- (1) $G \times X \rightarrow X, (g, x) \mapsto g \cdot x$ を集合 X 上の群 G の作用とすると, 各 $g \in G$ に対し, 写像

$$\phi_g: X \rightarrow X, x \mapsto g \cdot x$$

は全単射である. つまり, $\phi_g \in B(X)$ である (例 2 の記号を思い出すこと). さらに, 写像

$$\phi: G \rightarrow B(X), g \mapsto \phi_g$$

は準同型である.

- (2) 逆に, 準同型 $\phi: G \rightarrow B(X)$ が存在するとき, 写像

$$G \times X \rightarrow X, (g, x) \mapsto g \cdot x := \phi(g)(x) \quad (\phi(g) \text{ が全単射写像 } X \rightarrow X \text{ であることに注意})$$

は X 上の G の作用を定める.

Point

G を群, X を集合としたとき, 命題 11.2 は,

- X 上の G の作用 $G \times X \rightarrow X$
- 準同型 $G \rightarrow B(X)$

の間に一対一の対応が作れるということを述べている. X 上の G の作用を定めるということは, 準同型 $G \rightarrow B(X)$ を与えることと等価なのである.

命題 11.2 の証明.

- (1) ϕ_g の全単射性: 各 $g \in G$ に対し, ϕ_g の逆写像が構成できることを示せばよい. 各 $x \in X$ に対し,

$$\begin{aligned} (\phi_{g^{-1}} \circ \phi_g)(x) &= \phi_{g^{-1}}(\phi_g(x)) \\ &= g^{-1} \cdot (g \cdot x) \\ &= (g^{-1} \cdot g) \cdot x \quad (\text{作用の定義 (2) より}) \\ &= e \cdot x = x \quad (\text{作用の定義 (2) より}) \end{aligned}$$

となる. 全く同様に $(\phi_g \circ \phi_{g^{-1}})(x) = x$. よって, $\phi_{g^{-1}} \circ \phi_g = \phi_g \circ \phi_{g^{-1}} = \text{id}_X$ となる. よって, $\phi_{g^{-1}}$ が ϕ_g の逆写像であり, 特に ϕ_g は全単射である.

ϕ が準同型であること: 任意の $g_1, g_2 \in G, x \in X$ に対し,

$$\phi(g_1g_2)(x) = \phi_{g_1g_2}(x) = (g_1g_2) \cdot x = g_1 \cdot (g_2 \cdot x) = \phi_{g_1}(\phi_{g_2}(x)) = (\phi(g_1) \circ \phi(g_2))(x)$$

となるので, $\phi(g_1g_2) = \phi(g_1) \circ \phi(g_2)$. □

- (2) 作用の定義条件 (1) を満たすこと: e を G の単位元とすると, 任意の $x \in X$ に対し,

$$e \cdot x = \phi(e)(x) = \text{id}_X(x) = x.$$

ここで、 $\phi(e) = \text{id}_X$ は第 10 回講義資料命題 9.2 と群 $B(X)$ の単位元が id_X であることからわかる。
作用の定義条件 (2) を満たすこと：任意の $g, h \in G, x \in X$ に対し、

$$\begin{aligned} gh \cdot x &= \phi(gh)(x) = (\phi(g) \circ \phi(h))(x) \quad (\phi \text{ が準同型であることより}) \\ &= \phi(g)(\phi(h)(x)) = g \cdot (h \cdot x). \end{aligned}$$

□

定理 11.3

G が位数 n の有限群であるとき、単射準同型 $\phi: G \rightarrow \mathfrak{S}_n$ が存在する。つまり、任意の位数 n の有限群は n 次対称群のある部分群と同型になる。

証明. 例 6 で考えた G 上の G の作用 $\psi_\ell: G \times G \rightarrow G, (g, h) \mapsto gh$ を考える。ここで、 G の元に適当に 1 から順に番号をつけ、集合として G と $\{1, 2, \dots, n\}$ を同一視すると、この作用は $\psi_\ell: G \times \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ と見ることができる。命題 11.2 (1) より、これに対して準同型

$$\phi: G \rightarrow B(\{1, 2, \dots, n\}) = \mathfrak{S}_n$$

が構成できる。これが、単射であることを示せばよい。 $g \in \text{Ker } \phi$ とする。このとき、 $\phi(g) = \text{id}_{\{1, 2, \dots, n\}} = \text{id}_G$ だが (G と $\{1, 2, \dots, n\}$ を同一視していたことを忘れないように)、命題 11.2 (1) における ϕ の構成から、これは任意の $h \in G$ に対し、 $h = \phi(g)(h) = \psi_\ell(g, h) = gh$ となることを主張している。ここで、 $h = e$ とすると (e は G の単位元)、 $e = ge = g$ となるので、結局 $g = e$ である。よって、 $\text{Ker } \phi = \{e\}$ となり、 ϕ は単射である。 □

注意 (興味のある方向へ)。 \mathbb{K} を \mathbb{Q}, \mathbb{R} または \mathbb{C} とする。 V を \mathbb{K} 上のベクトル空間とし、

$$GL(V) := \{f: V \rightarrow V \mid f \text{ は全単射線形写像}\}$$

とする (V 上の一般線型群と呼ばれる)。このとき、 $GL(V)$ は $B(V)$ の部分群である (チェックせよ)。また、 V が n 次元ベクトル空間のとき、 V の基底を 1 つ固定すると、 $GL(V)$ は $GL_n(\mathbb{K})$ と同一視できるのであった (線形代数 II の内容。線形写像とその表現行列を同一視する)。

このとき、群 G に対し、準同型

$$\rho: G \rightarrow GL(V)$$

を群 G の V における線形表現 (linear representation) という。これは命題 11.2 の後の Point の見方で言うと、 G の V 上の“線形な”作用 $G \times V \rightarrow V$ を考えているとも言える。群 G を 1 つ与えたときに、『どのような線形表現が存在するか・どうすれば線形表現を構成できるか』ということ調べる数学の分野を (群の) 表現論 (representation theory) という。表現論は様々な数学的手法 (代数・幾何・解析全て!) を用いて研究されており、数学の枠を超えて物理・化学への応用も持つ非常に大きな分野である。興味を持った方は是非進んで勉強してもらいたい*3。

1 つ例を挙げておこう。 $D_n = \{\sigma^k \tau^\ell \mid k = 0, \dots, n-1, \ell = 0, 1\}$ ($\sigma^n = e, \tau^2 = e, \sigma^k \tau = \tau \sigma^{-k}$ ($k \in \mathbb{Z}$)) を n 次二面体群とする。このとき、準同型

$$\rho: D_n \rightarrow GL_2(\mathbb{R})$$

であって、

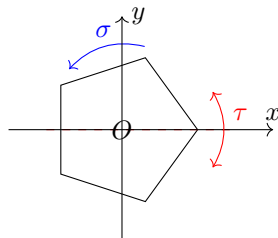
$$\rho(\sigma) = \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix} \quad \rho(\tau) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

*3 私 (大矢) は代数的な方向から表現論の研究を行っている。もしもこの分野に興味を持った方は、3 年生の研究室配属時に私の研究室を候補に入れていただくと良いだろう。

を満たすものが存在する。これが定める \mathbb{R}^2 上の D_n の作用は

$$D_n \times \mathbb{R}^2 \rightarrow \mathbb{R}^2, \left(\sigma^k \tau^\ell, \begin{pmatrix} x \\ y \end{pmatrix} \right) \mapsto \rho(\sigma^k \tau^\ell) \begin{pmatrix} x \\ y \end{pmatrix}$$

となる。このとき、 σ は \mathbb{R}^2 の原点を中心とする $2\pi/n$ 回転に対応し、 τ は x 軸に関する線対称変換に対応する。 n 次二面体群が正 n 角形の対称性であったことを思い出すと、これは自然な作用である。



定義 11.4

$G \times X \rightarrow X, (g, x) \mapsto g \cdot x$ を集合 X 上の群 G の作用とする。 G の作用による $x \in X$ の G -軌道 (G -orbit) を

$$G \cdot x := \{g \cdot x \mid g \in G\} (\subset X)$$

と定める。また、 $x \in X$ における G の固定部分群 (stabilizer) を

$$G_x := \{g \in G \mid g \cdot x = x\} (\subset G)$$

と定める。記号は似ているが $G \cdot x$ は X の部分集合であり、 G_x は G の部分集合であることを注意しておく。

例を見る前に、軌道と固定部分群に関する以下の基本命題を述べよう。先に例を見たい方は例 7 に先に飛んでもらっても良い。

命題 11.5

$G \times X \rightarrow X, (g, x) \mapsto g \cdot x$ を集合 X 上の群 G の作用とする。このとき、以下が成立する。

(1) 集合 X において、

$$x \sim y \iff \text{ある } g \in G \text{ が存在して, } x = g \cdot y$$

とすると、 \sim は X 上の同値関係を定める。このとき、 $x \in X$ の G -軌道 $G \cdot x$ は同値関係 \sim に関する x の同値類である。

(2) 各 $x \in X$ に対し、固定部分群 G_x は G の部分群である。

証明.

(1) 関係 \sim が同値関係であれば、 G 軌道 $G \cdot x$ が \sim に関する x の同値類であることは定義から明らかである。よって、 \sim が同値関係であること、つまり、反射律、対称律、推移律を満たすことをチェックすればよい。

(反射律) 任意の $x \in X$ に対して、 $x = e \cdot x$ なので (e は G の単位元)、 $x \sim x$ である。

(対称律) $x \sim y$ であるとき、ある $g \in G$ が存在して、 $x = g \cdot y$ 。このとき

$$g^{-1} \cdot x = g^{-1} \cdot (g \cdot y) = (g^{-1}g) \cdot y = e \cdot y = y$$

となるので、 $y \sim x$ 。

(推移律) $x \sim y$ かつ $y \sim z$ であるとき、ある $g_1, g_2 \in G$ が存在して、 $x = g_1 \cdot y, y = g_2 \cdot z$ 。このとき、

$$x = g_1 \cdot y = g_1 \cdot (g_2 \cdot z) = (g_1 g_2) \cdot z$$

となるので、 $x \sim z$ 。

□

(2) まず, $e \cdot x = x$ なので, $e \in G_x$ であるから G_x は空ではない. 任意の $g_1, g_2 \in G_x$ に対し,

$$(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x) = g_1 \cdot x = x$$

となるので, $g_1, g_2 \in G_x$. また, 任意の $g \in G_x$ に対し,

$$g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1} g) \cdot x = e \cdot x = x.$$

となるので, $g^{-1} \in G_x$. 以上より, G_x は二項演算と逆元を取る操作について閉じている空でない集合なので, G の部分群である. \square

命題 11.5 (1) と同値関係の一般論 (第 7 回講義資料命題 6.3) より, X は互いに交わりのない G -軌道に分割されることがわかる. これを, X の軌道分解という. 軌道と固定部分群の関係については次の定理が重要である.

定理 11.6 (軌道・固定群定理 Orbit-stabilizer theorem)

$G \times X \rightarrow X, (g, x) \mapsto g \cdot x$ を集合 X 上の群 G の作用とする. このとき, 任意の $x \in X$ に対し,

$$f_x: G/G_x \rightarrow G \cdot x, gG_x \mapsto g \cdot x$$

は well-defined な全単射写像となる. (ここで, $G \cdot x$ は X の部分集合で群ではなく, G_x は一般には正規部分群では無いので G/G_x も一般には群構造を持たない単なる商集合であることに注意! このため, これは群同型ではなく, 単なる全単射写像である.) これより, 特に

$$(G : G_x) = |G \cdot x|$$

である. ただし, 左辺は G_x の G における指数である (第 6 回講義資料定義 6.6).

証明. f_x の well-defined 性:

$$g_1 G_x = g_2 G_x \text{ であるとき, } g_1 \cdot x = g_2 \cdot x$$

となることを示せばよい. $g_1 G_x = g_2 G_x$ のとき, $g_1 \overset{G_x}{\sim}_L g_2$ なので (この記号については第 7 回講義資料定義 6.4 を参照), ある $h \in G_x$ が存在して, $g_1 = g_2 h$. これより,

$$g_1 \cdot x = (g_2 h) \cdot x = g_2 \cdot (h \cdot x) = g_2 \cdot x$$

となる.

f_x の全単射性: 全射性は写像の定義から明らかなので, 単射性を示す. $g_1 G_x \neq g_2 G_x$ とする. このとき, $g_1^{-1} g_2 \notin G_x$ なので, $x \neq (g_1^{-1} g_2) \cdot x$. このとき, 命題 11.2 (1) で考えた ϕ_g の全単射性より,

$$f_x(g_1 G_x) = g_1 \cdot x = \phi_{g_1}(x) \neq \phi_{g_1}((g_1^{-1} g_2) \cdot x) = g_1 \cdot ((g_1^{-1} g_2) \cdot x) = (g_1 g_1^{-1} g_2) \cdot x = g_2 \cdot x = f_x(g_2 G_x).$$

よって, f_x は単射である.

このとき, $(G : G_x) = |G \cdot x|$ であることは, 指数の定義を思い出せば直ちにわかる. \square

以下は軌道・固定群定理と Lagrange の定理 (第 8 回講義資料定理 7.2) から直ちにわかる.

系 11.7

G を有限群とし, $G \times X \rightarrow X, (g, x) \mapsto g \cdot x$ を集合 X 上の G の作用とする. このとき, 任意の $x \in X$ に対し,

$$|G \cdot x| = (G : G_x) = \frac{|G|}{|G_x|}$$

であり, 特に各 G -軌道に含まれる元の個数は G の位数の約数である.

例 7. 例 1 の作用を考える。このとき、任意の $k \in X = \{1, 2, \dots, n\}$ に対し、 $(1 k) \cdot 1 = k$ となるので、1 の \mathfrak{S}_n -軌道は

$$\mathfrak{S}_n \cdot 1 = \{\sigma \cdot 1 \mid \sigma \in \mathfrak{S}_n\} = \{1, 2, \dots, n\} = X$$

となる。つまり、このとき X は 1 つの \mathfrak{S}_n -軌道からなっている*4。また、固定部分群 $(\mathfrak{S}_n)_1$ は

$$(\mathfrak{S}_n)_1 = \{\sigma \in \mathfrak{S}_n \mid \sigma \cdot 1 = 1\} = \left\{ \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & i_2 & \cdots & i_n \end{pmatrix} \mid i_2, \dots, i_n \text{ は } 2, \dots, n \text{ の並べ替え} \right\}$$

となる。とくに、 $|(\mathfrak{S}_n)_1| = (n-1)!$ であり、確かに、

$$(\mathfrak{S}_n : (\mathfrak{S}_n)_1) = \frac{|\mathfrak{S}_n|}{|(\mathfrak{S}_n)_1|} = \frac{n!}{(n-1)!} = n = |X| = |\mathfrak{S}_n \cdot 1|$$

となっている (系 11.7)。

例 8. 例 4 で考えた作用

$$\psi: GL_2(\mathbb{R}) \times \mathbb{R}^2 \rightarrow \mathbb{R}^2, \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} x \\ y \end{pmatrix} \right) \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$$

を考える ($\mathbb{K} = \mathbb{R}$ とした)。このとき、

$$\begin{aligned} GL_2(\mathbb{R}) \cdot \begin{pmatrix} 0 \\ 0 \end{pmatrix} &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 \\ 0 \end{pmatrix} \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R}) \right\} = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\}, \\ GL_2(\mathbb{R}) \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R}) \right\} = \mathbb{R}^2 \setminus \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\} \end{aligned}$$

となるので、 \mathbb{R}^2 の軌道分解は

$$\mathbb{R}^2 = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\} \cup \left(\mathbb{R}^2 \setminus \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\} \right) = GL_2(\mathbb{R}) \cdot \begin{pmatrix} 0 \\ 0 \end{pmatrix} \cup GL_2(\mathbb{R}) \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

となり、 \mathbb{R}^2 は 2 つの $GL_2(\mathbb{R})$ -軌道からなっていることがわかる。また、

$$\begin{aligned} GL_2(\mathbb{R})_{\begin{pmatrix} 0 \\ 0 \end{pmatrix}} &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\} = GL_2(\mathbb{R}), \\ GL_2(\mathbb{R})_{\begin{pmatrix} 1 \\ 0 \end{pmatrix}} &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\} = \left\{ \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \mid b, d \in \mathbb{R}, d \neq 0 \right\} \end{aligned}$$

となる。この例からもわかるようにある元の固定部分群が群全体になるということは、その元が群作用で一切動かないということに対応する。軌道・固定群定理より、

$$\begin{aligned} GL_2(\mathbb{R})/GL_2(\mathbb{R})_{\begin{pmatrix} 0 \\ 0 \end{pmatrix}} &= GL_2(\mathbb{R})/GL_2(\mathbb{R}) = \{GL_2(\mathbb{R})\} \rightarrow \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\}, \quad GL_2(\mathbb{R}) \mapsto \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \\ GL_2(\mathbb{R})/GL_2(\mathbb{R})_{\begin{pmatrix} 1 \\ 0 \end{pmatrix}} &\rightarrow \mathbb{R}^2 \setminus \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\}, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot GL_2(\mathbb{R})_{\begin{pmatrix} 1 \\ 0 \end{pmatrix}} \mapsto \begin{pmatrix} a \\ c \end{pmatrix}, \end{aligned}$$

はともに全単射写像である。

例 9. 例 4 で考えた作用

$$\psi': GL_n(\mathbb{C}) \times \text{Mat}_n(\mathbb{C}) \rightarrow \text{Mat}_n(\mathbb{C}), (P, A) \mapsto PAP^{-1}$$

を考える ($\mathbb{K} = \mathbb{C}$ とした)。各 $A \in \text{Mat}_n(\mathbb{C})$ のこの作用に関する軌道

$$\{PAP^{-1} \mid P \in GL_n(\mathbb{C})\}$$

の中に対角行列が含まれるとき、 A を対角化可能というのであった (線形代数 II の内容の言い換え)。対角化可能性は固有多項式 $\Phi_A(\lambda) = \det(\lambda I_n - A)$ の各根の重複度とそれに対応する固有空間の次元が等しいかどうかで判定できた (全て等しいとき対角化可能) という話を思い出しておこう。

*4 このように、群 G が作用している集合 X が 1 つの軌道からなっている (=“群作用によって、集合内の任意の 2 元間を移動できる”) とき、この作用は推移的 (transitive) であり、 X は G の等質空間 (homogeneous space) であるという。

例 10. G を群とする. 例 6 で考えた随伴作用 $\psi_{\text{ad}}: G \times G \rightarrow G, (g, h) \mapsto ghg^{-1}$ を考える. このとき, 各元 $h \in G$ の随伴作用に関する軌道

$$K(h) := \{ghg^{-1} \mid g \in G\}$$

を h の共役類 (conjugacy class) という*5. 軌道分解可能性から, G は互いに交わりのない共役類に分割されることがわかる. またこのとき, 各 $h \in G$ における固定部分群 G_h は

$$G_h = \{g \in G \mid ghg^{-1} = h\} = \{g \in G \mid gh = hg\} = Z(\{h\})$$

となる (最後は $\{h\}$ の中心化群. 第 6 回講義資料定義 5.10 参照). よって, 系 11.7 より,

$$|K(h)| = (G : Z(\{h\}))$$

となる.

例として, 3 次二面体群 D_3 の共役類を全て求めてみよう. 最初に単位元 e の共役類を考えると,

$$K(e) = \{geg^{-1} \mid g \in D_3\} = \{e\}$$

(同じ理由で任意の群 G において $K(e) = \{e\}$ となる.) 次に $K(e)$ に含まれない元であれば何でも良いが, $\sigma \in D_3$ の共役類を考えると,

$$\begin{aligned} K(\sigma) &= \{\sigma^k \sigma (\sigma^k)^{-1}, (\sigma^k \tau) \sigma (\sigma^k \tau)^{-1} \mid k = 0, 1, 2\} \\ &= \{\sigma, \sigma^{-1}\} = \{\sigma, \sigma^2\}. \end{aligned}$$

ちなみに, 共役類は随伴作用の定める同値関係に関する同値類なので, $\sigma^2 \in K(\sigma)$ であることから, $K(\sigma) = K(\sigma^2)$ であることにも注意する. 次に $K(e), K(\sigma)$ のいずれにも含まれない元であれば何でも良いが, $\tau \in D_3$ の共役類を考えると,

$$\begin{aligned} K(\tau) &= \{\sigma^k \tau (\sigma^k)^{-1}, (\sigma^k \tau) \tau (\sigma^k \tau)^{-1} \mid k = 0, 1, 2\} \\ &= \{\tau, \sigma^2 \tau, \sigma^4 \tau\} = \{\tau, \sigma \tau, \sigma^2 \tau\}. \end{aligned}$$

ここで, $\sigma^3 = e$ を用いた. 以上で D_3 の全ての元がいずれかの共役類の中に現れたので, D_3 の共役類への分割が $D_3 = K(e) \cup K(\sigma) \cup K(\tau)$ となることがわかる. よって, D_3 の共役類は $K(e), K(\sigma), K(\tau)$ で全てである.

11.2 群の作用の応用 (やや発展)

最後に群作用の応用としてわかる定理を 2 つ紹介して講義資料を締めくくろう. (ただし, 以下の内容は時間的に講義内では扱えない可能性が高い. 質問のある方は講義前後の時間に是非質問をしてもらいたい.)

定理 11.8

p を素数とする. このとき, 位数 p^k (k は 1 以上の整数) の群*6 G の中心 $Z(G)$ は $Z(G) \neq \{e\}$ となる. つまり, このような群においては必ず単位元以外に全ての元と可換性を持つ元が存在する.

証明. G の共役類への分割を,

$$K(e) \cup K(g_1) \cup K(g_2) \cup \cdots \cup K(g_m)$$

とする. (ただし, $i \neq j$ のとき, $K(g_i) \neq K(g_j) (\neq K(e))$ となるとする.)

*5 共役類のありがたみは P.5 の注意で述べた表現論を学ぶと非常に良く分かる. 興味のある方は是非勉強してみたい.

*6 位数が素数 p の自然数べきであるような群を p 群 (p -group) という. 例えば, 4 次 2 面体群 D_4 は位数 $8 = 2^3$ なので, 2-群である. 実際 D_4 においては $Z(D_4) = \{e, \sigma^2\}$ である.

背理法で証明する. もし, $Z(G) = \{e\}$ となるとすると, 全ての $\ell = 1, \dots, m$ に対し, $K(g_\ell) \neq \{g_\ell\}$ となる. なぜなら, $K(g_\ell) = \{g_\ell\}$ は, 共役類の定義から任意の $g \in G$ に対して, $gg_\ell g^{-1} = g_\ell$ となることを意味するので, このとき, 任意の $g \in G$ に対して $gg_\ell = g_\ell g$ で, $g_\ell \in Z(G)$ となるからである. よって, 全ての $\ell = 1, \dots, m$ に対し, $|K(g_\ell)| > 1$ である. 一方, 共役類は随伴作用に関する G -軌道なので, 系 11.7 から, $|K(g_\ell)|$ は $|G| = p^k$ の約数である. よって, 各 $\ell = 1, \dots, m$ に対し, $|K(g_\ell)|$ は p の倍数となる. よって,

$$p^k = |G| = |K(e)| + |K(g_1)| + \dots + |K(g_m)| \equiv |K(e)| = |\{e\}| = 1 \pmod{p}$$

となり, これは矛盾である. 以上より, $Z(G) \neq \{e\}$. □

次に紹介する応用は Sylow の定理と呼ばれ, 群の分類問題を扱う際に非常に便利になる定理である*7:

定理 11.9 (Sylow の定理)

p を素数, G を有限群とし, G の位数が p^ℓ では割り切れるが, $p^{\ell+1}$ では割り切れなかったとする. (ただし ℓ は正の整数.) このとき, 任意の $1 \leq k \leq \ell$ に対し, G は位数 p^k の部分群を持つ.

Sylow の定理より, 特に G は位数 p^ℓ の部分群をもつ. これを p -Sylow 部分群 (p -Sylow subgroup) という.

証明. 仮定より, G の位数は $p^\ell n$ (ただし, p と n は互いに素) という形で書かれる.

$$X := \{\{g_1, \dots, g_{p^k}\} \subset G \mid g_1, \dots, g_{p^k} \text{ は相異なる } G \text{ の } p^k \text{ 個の元}\}$$

としたとき,

$$G \times X \rightarrow X, (g, \{g_1, \dots, g_{p^k}\}) \mapsto \{gg_1, \dots, gg_{p^k}\}$$

は X 上の G の作用を定める (チェックせよ). このとき, 各 $\{g_1, \dots, g_{p^k}\} \in X$ の固定部分群は定義より,

$$G_{\{g_1, \dots, g_{p^k}\}} = \{g \in G \mid \{gg_1, \dots, gg_{p^k}\} = \{g_1, \dots, g_{p^k}\}\}$$

であるので, 各 $g \in G_{\{g_1, \dots, g_{p^k}\}}$ に対してある $i \in \{1, \dots, p^k\}$ が定まり, $gg_1 = g_i$ となる. このとき, $g = g_i g_1^{-1}$ となるので,

$$G_{\{g_1, \dots, g_{p^k}\}} \subset \{g_i g_1^{-1} \mid i = 1, \dots, p^k\}.$$

特に, $|G_{\{g_1, \dots, g_{p^k}\}}| \leq p^k$ である. ここで, $|G_{\{g_1, \dots, g_{p^k}\}}| = p^k$ となるものが存在することを示せば, 固定部分群 $G_{\{g_1, \dots, g_{p^k}\}}$ が G の位数 p^k の部分群となり, 示すべきことが示される.

Lagrange の定理より $|G_{\{g_1, \dots, g_{p^k}\}}|$ の値は $|G| = p^\ell n$ の約数なので, $|G_{\{g_1, \dots, g_{p^k}\}}| < p^k$ とすると特にこれは $p^{k-1}n$ の約数である. いま各 $\{g_1, \dots, g_{p^k}\} \in X$ に対し, 系 11.7 から,

$$|G \cdot \{g_1, \dots, g_{p^k}\}| = \frac{|G|}{|G_{\{g_1, \dots, g_{p^k}\}}|} = \frac{p^\ell n}{|G_{\{g_1, \dots, g_{p^k}\}}|}$$

が成立するので, 以上の考察から, $|G \cdot \{g_1, \dots, g_{p^k}\}|$ は $p^{\ell-k+1}$ の倍数 ($|G_{\{g_1, \dots, g_{p^k}\}}| < p^k$ のとき), または $p^{\ell-k}n$ ($|G_{\{g_1, \dots, g_{p^k}\}}| = p^k$ のとき) となる. これより, もし $|G_{\{g_1, \dots, g_{p^k}\}}| = p^k$ となる $\{g_1, \dots, g_{p^k}\} \in X$ が存在しないと仮定すると, X を軌道分解したときに元の個数が $p^{\ell-k+1}$ の倍数の軌道で軌道分解されるので, 特に $|X|$ は $p^{\ell-k+1}$ の倍数となる. 今示したかったことは, $|G_{\{g_1, \dots, g_{p^k}\}}| = p^k$ となるものの存在なので, あとは $|X|$ が $p^{\ell-k+1}$ の倍数でないことを示せば良い.

いま,

$$|X| = p^{\ell n} C_{p^k} = \frac{p^\ell n (p^\ell n - 1) \cdots (p^\ell n - p^k + 1)}{p^k (p^k - 1) \cdots 1} = p^{\ell-k} n \cdot \frac{(p^\ell n - 1) \cdots (p^\ell n - p^k + 1)}{(p^k - 1) \cdots 1}$$

である. ここで, $m \in \mathbb{Z}_{>0}$ に対し, $\ell(m)$ を

*7 実はこの定理には続きがあり, 群の分類問題を扱う上ではそこまで知っているより良い. 興味のある方は是非調べてほしい. (例えば, 雪江明彦 著「代数学 1 群論入門」(日本評論社)の定理 4.5.7 参照.)

m は $p^{\ell(m)}$ で割り切れるが $p^{\ell(m)+1}$ では割り切れない

という条件で定まる 0 以上の整数とすると、定義より $p^{-\ell(m)}m$ は p で割り切れない整数であり、 $m = 1, 2, \dots, p^k - 1$ のとき $\ell(m) < k$ である。よって、

$$\begin{aligned} & \frac{(p^\ell n - 1) \cdots (p^\ell n - p^k + 1)}{(p^k - 1) \cdots 1} \\ &= \frac{(p^{\ell-\ell(1)}n - p^{-\ell(1)}1) \cdots (p^{\ell-\ell(m)}n - p^{-\ell(m)}m) \cdots (p^{\ell-\ell(p^k-1)}n - p^{-\ell(p^k-1)}(p^k - 1))}{(p^{k-\ell(1)} - p^{-\ell(1)}1) \cdots (p^{k-\ell(m)} - p^{-\ell(m)}m) \cdots (p^{k-\ell(p^k-1)} - p^{-\ell(p^k-1)}(p^k - 1))}. \end{aligned}$$

ここで、右辺の分子分母の積の各項は整数であることに注意する。このとき、右辺の分子に現れる $(p^{\ell-\ell(m)}n - p^{-\ell(m)}m)$, $m = 1, \dots, p^k - 1$ という形の整数は $p^{\ell-\ell(m)}n$ が p の倍数、 $-p^{-\ell(m)}m$ が p で割り切れない整数であることより、 p で割り切れない整数である。よって、それらの積である右辺の分子は p で割り切れず、それをさらに整数で割って得られる数である右辺の値は p の倍数ではない。

以上より、 $\frac{(p^\ell n - 1) \cdots (p^\ell n - p^k + 1)}{(p^k - 1) \cdots 1}$ は p の倍数ではないことが示され、さらに p と n は互いに素であることより、結局 $|X|$ は $p^{\ell-k+1}$ の倍数ではないことがわかった。よって、示すべきことは全て示された。 \square

拡張ユークリッド互除法について

担当：大矢 浩徳 (OYA Hironori)

本資料では、拡張ユークリッド互除法の厳密な取扱いを示しておく。

定義.

正の整数 $a, b \in \mathbb{Z}_{>0}$ に対して、その最大公約数を $\gcd(a, b)$ と書く。さらに $a, b \in \mathbb{Z}$ に対する $\gcd(a, b)$ を以下のように定義する：

- 任意の 0 以上の整数 $a \in \mathbb{Z}_{\geq 0}$ に対して $\gcd(0, a) = \gcd(a, 0) = a$ とする。
- 各 $a, b \in \mathbb{Z}$ に対し、 $\gcd(a, b) := \gcd(|a|, |b|)$ とする。

例 1.

$$\gcd(20, 8) = 4 \quad \gcd(0, 7) = 7 \quad \gcd(42, -54) = 6 \quad \gcd(-5, 0) = 5.$$

注意 1. • この定義は要するに「マイナスは無視して最大公約数を考えよ。」ということである。

- 定義より、 $\gcd(a, b) = 0$ となるのは、 $(a, b) = (0, 0)$ のときのみであり、それ以外の場合は $\gcd(a, b)$ は正の整数である。
- 各 $a, b \in \mathbb{Z}$ に対し、 $\gcd(a, b) = \gcd(b, a)$ である。

補題.

$a, b \in \mathbb{Z}$ が、ある $c \in \mathbb{Z}_{\geq 0}, d, d' \in \mathbb{Z}$ によって $a = cd, b = cd'$ と書けるとき、 c を a と b の公約数ということにする。 $(a, b) \neq (0, 0)$ のとき、 $\gcd(a, b)$ は a と b の公約数の中で最大のものである。

補題の証明は容易なので省略する。ただし、この補題は $a \in \mathbb{Z}_{>0}$ に対し、 $\gcd(0, a) = \gcd(a, 0) = a$ と定義しておかないと成立しないことに注意する。以下は \gcd の重要な性質である。

命題.

任意の $a, b, r \in \mathbb{Z}$ に対し、

$$\gcd(a, b) = \gcd(a + rb, b).$$

証明. $(a, b) = (0, 0)$ のとき主張は自明なので、 $(a, b) \neq (0, 0)$ と仮定する。 $\gcd(a, b) = c, \gcd(a + rb, b) = c'$ とし、 $c = c'$ を証明すればよい。 $a = cd_1, b = cd'_1, a + rb = c'd_2, b = c'd'_2$ とする ($d_1, d'_1, d_2, d'_2 \in \mathbb{Z}$)。このとき、

$$a + rb = cd_1 + rcd'_1 = c(d_1 + rd'_1)$$

なので、 $a + rb$ も b も c で割り切れることから、補題より、 $c' = \gcd(a + rb, b) \geq c$ である。一方、

$$a = a + rb - rb = c'd_2 - rc'd'_2 = c'(d_2 - rd'_2)$$

なので、 a も b も c' で割り切れることから、補題より、 $c = \gcd(a, b) \geq c'$ である。以上より、 $c = c'$ である。□

$a, b \in \mathbb{Z}$ に対して $\gcd(a, b)$ を求めたいときは、定義より $\gcd(|a|, |b|)$ を求めればよい。これより、 $a \in \mathbb{Z}_{>0}, b \in \mathbb{Z}_{>0}$ の場合に $\gcd(a, b)$ を求める方法を知っていれば十分である (どちらかが 0 の場合は容易なので、それ以外の場合を考える)。この方法の一つにユークリッド互除法がある。

ユークリッド互除法.

$a, b \in \mathbb{Z}_{>0}, a \geq b$ とする. このとき, 以下の操作を行う:

- (0) $a_1 := a, b_1 := b$ において, ステップ (1) へ進む.
- (1) $a_1 = q_1 b_1 + r_1$ なる $q_1 \in \mathbb{Z}_{>0}, 0 \leq r_1 < b_1$ を取る (q_1, r_1 はそれぞれ a_1 を b_1 で割った時の商と余り). $r_1 = 0$ のときここで終了し, $r_1 \neq 0$ のとき, $a_2 := b_1, b_2 := r_1$ において, ステップ (2) へ進む.
- (2) $a_2 = q_2 b_2 + r_2$ なる $q_2 \in \mathbb{Z}_{>0}, 0 \leq r_2 < b_2$ を取る (q_2, r_2 はそれぞれ a_2 を b_2 で割った時の商と余り). $r_2 = 0$ のときここで終了し, $r_2 \neq 0$ のとき, $a_3 := b_2, b_3 := r_2$ において, ステップ (3) へ進む.
- ...
- (k) $a_k = q_k b_k + r_k$ なる $q_k \in \mathbb{Z}_{>0}, 0 \leq r_k < b_k$ を取る (q_k, r_k はそれぞれ a_k を b_k で割った時の商と余り). $r_k = 0$ のときここで終了し, $r_k \neq 0$ のとき, $a_{k+1} := b_k, b_{k+1} := r_k$ において, ステップ (k+1) へ進む.
- ...

このとき, この操作は必ずあるステップで終了し, ステップ (n) で終了したとき, $b_n = \gcd(a, b)$ である.

操作が有限回のステップで終了することの証明.

定義より, $b_1 > r_1 = b_2 > r_2 = b_3 > r_3 = b_4 > \dots$ となるが, 任意の ℓ に対し $r_\ell \geq 0$ となることから, この操作は有限回で止まる. □

ステップ (n) で終了したとき, $b_n = \gcd(a, b)$ であることの証明.

命題より,

$$\begin{aligned} \gcd(a, b) &= \gcd(a_1, b_1) = \gcd(a_1 - q_1 b_1, b_1) = \gcd(r_1, b_1) \\ &= \gcd(a_2, b_2) = \gcd(a_2 - q_2 b_2, b_2) = \gcd(r_2, b_2) \\ &= \gcd(a_3, b_3) = \dots \\ &= \gcd(a_n, b_n) = \gcd(a_n - q_n b_n, b_n) = \gcd(r_n, b_n) = \gcd(0, b_n) = b_n. \end{aligned}$$

である. □

このユークリッド互除法の途中経過を用いて, $ax + by = \gcd(a, b)$ を満たす整数の組 (x, y) を見つけることができる. これを拡張ユークリッド互除法という. ユークリッド互除法の途中経過は以下のように行列を用いて表すことができる:

$$\begin{aligned} \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} &= \begin{pmatrix} b_1 \\ a_1 - q_1 b_1 \end{pmatrix} = \begin{pmatrix} b_1 \\ r_1 \end{pmatrix} = \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} \\ \begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix} \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} &= \begin{pmatrix} b_2 \\ a_2 - q_2 b_2 \end{pmatrix} = \begin{pmatrix} b_2 \\ r_2 \end{pmatrix} = \begin{pmatrix} a_3 \\ b_3 \end{pmatrix} \\ &\dots \\ \begin{pmatrix} 0 & 1 \\ 1 & -q_k \end{pmatrix} \begin{pmatrix} a_k \\ b_k \end{pmatrix} &= \begin{pmatrix} b_k \\ a_k - q_k b_k \end{pmatrix} = \begin{pmatrix} b_k \\ r_k \end{pmatrix} = \begin{pmatrix} a_{k+1} \\ b_{k+1} \end{pmatrix} \\ &\dots \end{aligned}$$

これより, ステップ (n) でユークリッド互除法が終了するとき,

$$\begin{aligned} \begin{pmatrix} \gcd(a, b) \\ 0 \end{pmatrix} &= \begin{pmatrix} b_n \\ r_n \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} \begin{pmatrix} a_n \\ b_n \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{n-1} \end{pmatrix} \begin{pmatrix} a_{n-1} \\ b_{n-1} \end{pmatrix} = \dots \\ &= \begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{n-1} \end{pmatrix} \dots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} \end{aligned}$$

ここで,

$$\begin{pmatrix} x_0 & y_0 \\ z_0 & w_0 \end{pmatrix} := \begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{n-1} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix}$$

とすると,

$$\begin{pmatrix} \gcd(a, b) \\ 0 \end{pmatrix} = \begin{pmatrix} x_0 & y_0 \\ z_0 & w_0 \end{pmatrix} \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} = \begin{pmatrix} x_0 & y_0 \\ z_0 & w_0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} ax_0 + by_0 \\ az_0 + bw_0 \end{pmatrix}.$$

なので, (x_0, y_0) が $ax + by = \gcd(a, b)$ を満たす整数の組 (x, y) の 1 つである.

例 2. $2394x + 714y = \gcd(2394, 714)$ を満たす整数の組 (x, y) を 1 つ求めてみる. ここでは, 講義資料で扱った方法とこの資料で説明した方法を比較しておく. まず, $\gcd(2394, 714)$ を求める:

$$\begin{aligned} 2394 &= 3 \times 714 + 252 & 714 &= 2 \times 252 + 210 \\ 252 &= 1 \times 210 + 42 & 210 &= 5 \times 42 + 0 \end{aligned}$$

であるので, $\gcd(2394, 714) = \gcd(714, 252) = \gcd(252, 210) = \gcd(210, 42) = \gcd(42, 0) = 42$.

【講義で行った方法】

$$\begin{aligned} 42 &= 1 \times 252 + (-1) \times 210 \\ &= 1 \times 252 + (-1) \times (714 - 2 \times 252) = (-1) \times 714 + 3 \times 252 \\ &= (-1) \times 714 + 3 \times (2394 - 3 \times 714) = 3 \times 2394 + (-10) \times 714. \end{aligned}$$

より, $(x, y) = (3, -10)$ が $2394x + 714y = \gcd(2394, 714)$ を満たす整数の組 (x, y) の例である.

【この資料で行った方法】

$$\begin{aligned} \begin{pmatrix} x_0 & y_0 \\ z_0 & w_0 \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 1 & -5 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \\ &= \begin{pmatrix} 1 & -1 \\ -5 & 6 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \\ &= \begin{pmatrix} -1 & 3 \\ 6 & -17 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \\ &= \begin{pmatrix} 3 & -10 \\ -17 & 57 \end{pmatrix} \end{aligned}$$

となるので, $(x_0, y_0) = (3, -10)$ が $2394x + 714y = \gcd(2394, 714)$ を満たす整数の組 (x, y) の例である. ここで, 行列の積は左のものから順に計算している.

これらを見比べると, 色を付けた部分の数がそれぞれ対応していることがわかる. 実際にこれらは一般的に一致することがわかり (確かめてみよ), この資料での計算と講義で紹介した計算は同じ計算手続きとなる.

コラム : 連分数との関係

次のような分母にさらに分数が含まれているような数の表記を (単純) 連分数という:

$$q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{1}{\ddots + \frac{1}{q_n}}}}$$

ただし, $q_1 \in \mathbb{Z}, q_2, \dots, q_n \in \mathbb{Z}_{>0}$. 有理数が与えられたとき, その連分数展開はユークリッド互除法を用いて次のように求めることができる:

2 ページ目上部のユークリッド互除法の説明中に用いられた記号を用いて $a, b \in \mathbb{Z}, a \geq b$ に対して, a/b の連分数展開を求める. ここでユークリッド互除法はステップ n で終わるとする (つまり $r_n = 0$). いま

$a = a_1, b = b_1, a_1 = q_1 b_1 + r_1$ より,

$$\begin{aligned} \frac{a}{b} &= \frac{a_1}{b_1} = q_1 + \frac{r_1}{b_1} = q_1 + \frac{1}{\frac{b_1}{r_1}} = q_1 + \frac{1}{\frac{a_2}{b_2}} \\ &= q_1 + \frac{1}{q_2 + \frac{r_2}{b_2}} = q_1 + \frac{1}{q_2 + \frac{1}{\frac{b_2}{r_2}}} = q_1 + \frac{1}{q_2 + \frac{1}{\frac{a_3}{b_3}}} \\ &= \dots \\ &= q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{1}{\ddots + \frac{1}{q_{n-1} + \frac{r_{n-1}}{b_{n-1}}}}}} = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{1}{\ddots + \frac{1}{q_{n-1} + \frac{1}{\frac{b_{n-1}}{r_{n-1}}}}}}} \\ &= q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{1}{\ddots + \frac{1}{q_{n-1} + \frac{1}{b_n}}}}} = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{1}{\ddots + \frac{1}{q_{n-1} + \frac{1}{q_n}}}}} \end{aligned}$$

ちなみに、 $a \leq b$ の場合には、 $\frac{a}{b} = \frac{1}{\frac{b}{a}}$ より、 $q_1 = 0$ であると考えて先に進めば、以降は同じである。また、 $a < 0, b > 0$ のときも、

$$a = q_1 b + r_1, q_1 \in \mathbb{Z}_{<0}, 0 \leq r_1 < b$$

を満たす q_1, r_1 をとることができ、このとき $\frac{a}{b} = q_1 + \frac{r_1}{b}$ となるので、 q_1 が負の値をとるだけで以降は同じである。

上でユークリッド互除法のアルゴリズムは必ず終了することを見たので、以下がわかる：

定理.

任意の有理数は (有限の長さで) 連分数展開できる。

例 3. $\frac{2394}{714}$ の連分数展開を求めてみる：

$$\begin{aligned} 2394 &= 3 \times 714 + 252 \\ 252 &= 1 \times 210 + 42 \end{aligned}$$

$$\begin{aligned} 714 &= 2 \times 252 + 210 \\ 210 &= 5 \times 42 + 0 \end{aligned}$$

であったので、

$$\begin{aligned} \frac{2394}{714} &= 3 + \frac{252}{714} = 3 + \frac{1}{\frac{714}{252}} \\ &= 3 + \frac{1}{2 + \frac{210}{252}} = 3 + \frac{1}{2 + \frac{1}{\frac{252}{210}}} \\ &= 3 + \frac{1}{2 + \frac{1}{1 + \frac{42}{210}}} = 3 + \frac{1}{2 + \frac{1}{1 + \frac{1}{\frac{210}{42}}}} = 3 + \frac{1}{2 + \frac{1}{1 + \frac{1}{5}}} \end{aligned}$$

巡回置換について

大矢 浩徳 (OYA Hironori)

本資料では、第6回講義資料の定理5.4の厳密な証明を与える。まず、定理5.4を思い出そう。

定理 5.4

n を2以上の整数とする。各 $i = 1, \dots, n-1$ に対し $s_i := (i \ i+1) \in \mathfrak{S}_n$ とする。このとき、以下が成立する：

- (1) 任意の \mathfrak{S}_n の単位元でない元はどの2つも互いに素な巡回置換の合成として書かれる。さらに、長さ1の巡回置換 (=単位元) を用いないことにすると、合成の順序の違いを除いてこの表示は一意的である。
- (2) 任意の \mathfrak{S}_n の元は隣接互換 $s_i, i = 1, \dots, n-1$ らの合成として書かれる。

巡回置換について2つの補題を準備する。証明はいずれも各用語の定義より容易である。

補題 1.

$\sigma \in \mathfrak{S}_n$ を巡回置換とし、 $i \in S(\sigma)$ とする。このとき、 m を $\sigma^m(i) = i$ を満たす最小の m とすると*1、

$$\sigma = (i \ \sigma(i) \cdots \sigma^{m-1}(i))$$

である。特に、 $S(\sigma) = \{i, \sigma(i), \dots, \sigma^{m-1}(i)\}$ である。

補題 2 (命題 5.3)

$\sigma_1, \dots, \sigma_s$ を \mathfrak{S}_n 内のどの2つも互いに素な巡回置換とする。このとき、

$$(\sigma_1 \cdots \sigma_s)(i) = \begin{cases} \sigma_t(i) & \text{ある } t \text{ について } i \in S(\sigma_t) \text{ となるとき,} \\ i & \text{全ての } t = 1, \dots, s \text{ に対して, } i \notin S(\sigma_t) \text{ のとき,} \end{cases}$$

となる。特に、 σ と σ' が互いに素な巡回置換のとき、それらは可換、つまり、

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

である。

以下の定理5.4 (1)の証明は少し込み入っているように見えるので、証明の前に実際にどのようにすれば任意の \mathfrak{S}_n の元をどの2つも互いに素な巡回置換の合成として書くことができるのかということ为例で見ておくが良い。実際に、定理5.4 (1)の証明は以下の方法を一般的な言葉に置き換えただけのものである。

$$\sigma = \left(\begin{array}{cccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 4 & 2 & 8 & 7 & 10 & 9 & 1 & 5 & 6 \end{array} \right) \in \mathfrak{S}_{10}$$

とする。まず1をとる (これは実際には1出なくても何でも良い)。この1の σ による像を次々に計算する：

$$1 \xrightarrow{\sigma} 3 \xrightarrow{\sigma} 2 \xrightarrow{\sigma} 4 \xrightarrow{\sigma} 8 \xrightarrow{\sigma} 1$$

上のように初めに取った1に戻ってきたところでストップする (必ず初めの数字にいつか戻る)。次に、上の過程で現れていない数字を任意にとる。ここでは5を取る。そして、上と同様に5の σ による像を次々に計算

*1 このような m の存在は巡回置換の定義よりわかる。

する :

$$5 \xrightarrow{\sigma} 7 \xrightarrow{\sigma} 9 \xrightarrow{\sigma} 5$$

同様に初めに取った 5 に戻ってくるのでそこでストップする. さらに, 上の過程で今まで一度も出てきてない数字を任意にとる. ここでは, 6 をとる. そして, 上と同様に 6 の σ による像を次々に計算する :

$$6 \xrightarrow{\sigma} 10 \xrightarrow{\sigma} 6$$

同様に初めに取った 6 に戻ってくるのでそこでストップする. ここで, $1, \dots, 10$ の全ての数が出そろったので, 以上の反復の過程をストップする.

以上の過程で出てきた数字のサイクルをその順に並べて巡回置換を作り, その合成をとる.

$$(1\ 3\ 2\ 4\ 8)(5\ 7\ 9)(6\ 10)$$

すると, こうして得られる巡回置換たちはその作り方からどの 2 つも互いに素であり, さらに補題 2 から写像として σ と一致する. よって,

$$\sigma = (1\ 3\ 2\ 4\ 8)(5\ 7\ 9)(6\ 10)$$

であり, 確かに σ を互いに素な巡回置換の合成として書くことができた.

以下の定理 5.4 (1) の証明はこの方法がいつでも可能であるということを抽象的に書いたものである.

定理 5.4 の証明. (1) 任意の元 $\sigma \in \mathfrak{S}_n$ をとる. このとき σ がどの 2 つも互いに素な巡回置換の合成として書かれることを示す. 各 $i \in \{1, \dots, n\}$ に対して,

$$\Sigma_i := \{\sigma^m(i) \mid m \in \mathbb{Z}\} \subset \{1, \dots, n\}$$

とおく. このとき,

主張 1. 各 $i, i' \in \{1, \dots, n\}$ に対し,

$$\Sigma_i \cap \Sigma_{i'} \neq \emptyset \Leftrightarrow \Sigma_i = \Sigma_{i'}.$$

主張 1 の証明. $i = \sigma^0(i) \in \Sigma_i$ なので Σ_i は空集合ではないため, \Leftarrow 方向は明らか. \Rightarrow 方向を示す. $\Sigma_i \cap \Sigma_{i'}$ は空集合でないので, その元 i'' を取ると定義よりある $l, l' \in \mathbb{Z}$ が存在して, $i'' = \sigma^l(i) = \sigma^{l'}(i')$ と書ける. このとき,

$$\Sigma_i = \{\sigma^{m+l}(i) \mid m \in \mathbb{Z}\} = \{\sigma^m(i'') \mid m \in \mathbb{Z}\} = \{\sigma^{m+l'}(i') \mid m \in \mathbb{Z}\} = \Sigma_{i'}.$$

□

主張 1 より, $\{i_1, \dots, i_s\} \subset \{1, \dots, n\}$ であって,

- (a) $\Sigma_{i_1} \cup \dots \cup \Sigma_{i_s} = \{1, \dots, n\}$
- (b) 任意の $t \neq t'$ に対し, $\Sigma_{i_t} \cap \Sigma_{i_{t'}} = \emptyset$

を満たすものが次の手続きで取れる :

(Step 0) $i_1 = 1$ とする. $\Sigma_{i_1} = \{1, \dots, n\}$ ならばここで終了する ($s = 1$). $\Sigma_{i_1} \neq \{1, \dots, n\}$ のとき Step1 に進む.

(Step s') $i_1, \dots, i_{s'} \in \{1, \dots, n\}$ が, (b) を満たすとする.

Case 1 : $\Sigma_{i_1} \cup \dots \cup \Sigma_{i_{s'}} = \{1, \dots, n\}$ ならば, ここで終了する ($s = s'$).

Case 2 : $\Sigma_{i_1} \cup \dots \cup \Sigma_{i_{s'}} \neq \{1, \dots, n\}$ のとき, $i_{s'+1} \in \{1, \dots, n\} \setminus \Sigma_{i_1} \cup \dots \cup \Sigma_{i_{s'}}$ を任意にとる. このとき $k = 1, \dots, s'$ に対し, $\Sigma_{i_{s'+1}} \ni i_{s'+1} \notin \Sigma_{i_k}$ なので, 主張 1 より $\Sigma_{i_{s'+1}} \cap \Sigma_{i_k} = \emptyset$ である. よって, $i_1, \dots, i_{s'}, i_{s'+1} \in \{1, \dots, n\}$ は再び (b) を満たし, Step ($s' + 1$) に進む.

$\Sigma_{i_1} \cup \dots \cup \Sigma_{i_s''}$ よりも $\Sigma_{i_1} \cup \dots \cup \Sigma_{i_s''} \cup \Sigma_{i_s''+1}$ は真に大きいため、これらの Step を繰り返せばいずれ (a) が成立し、手続きが終了する。

さてこのとき $t = 1, \dots, s$ に対し、 $\sigma^m(i_t) = i_t$ を満たす最小の正の整数を m_t とする*1。このとき、

- 任意の $0 \leq k < k' < m_t$ に対し、 $\sigma^k(i_t) \neq \sigma^{k'}(i_t)$

となる。なぜなら、もし $\sigma^k(i_t) = \sigma^{k'}(i_t)$ なる $0 \leq k < k' < m_t$ が存在したとすると両辺に σ^{-k} を適用して、 $i_t = \sigma^{k'-k}(i_t)$ となり、 $0 < k' - k < m_t$ より、これは m_t の最小性に反するからである。よって、

$$\sigma_t := (i_t \sigma(i_t) \dots \sigma^{m_t-1}(i_t))$$

とすると、これは意味を持つ巡回置換である。定義から $S(\sigma_t) = \Sigma_{i_t}$ であることに注意すると、 Σ_{i_t} らの性質 (b) より、 $\sigma_1, \dots, \sigma_s$ はどの2つも互いに素な巡回置換の組である。よって、

$$\sigma = \sigma_1 \cdots \sigma_s$$

を言えばよい。各 $i \in \{1, \dots, n\}$ の両辺の写像による像を比較する。 Σ_{i_t} らの性質 (a), (b) より、 i に対してただ一つ t が定まり、 $i \in \Sigma_{i_t}$ となる。このとき、ある m が存在して、 $i = \sigma^m(i_t)$ と書けるが、補題2と σ_t の定義より、

$$(\sigma_1 \cdots \sigma_s)(i) = \sigma_t(i) = \sigma_t(\sigma^m(i_t)) = \sigma^{m+1}(i_t) = \sigma(i).$$

今 i は任意だったので、写像 $\{1, \dots, n\} \rightarrow \{1, \dots, n\}$ として、 $\sigma = \sigma_1 \cdots \sigma_s$ 、つまり、対称群 \mathfrak{S}_n の元として $\sigma = \sigma_1 \cdots \sigma_s$ である。

次に、 σ を単位元でないとして、 σ を

$$\sigma = \sigma_1^{(1)} \cdots \sigma_{s_1}^{(1)} = \sigma_2^{(2)} \cdots \sigma_{s_2}^{(2)}$$

と、長さ1の巡回置換 (= 単位元) を含まない互いに素な巡回置換の合成として2通りの方法で表示したとする。このとき、 $\{\sigma_1^{(1)}, \dots, \sigma_{s_1}^{(1)}\} = \{\sigma_1^{(2)}, \dots, \sigma_{s_2}^{(2)}\}$ であることを言えばよい。背理法で示す。補題2より、互いに素な巡回置換どうしは可換なので $\sigma_1^{(1)}$ が $\{\sigma_1^{(2)}, \dots, \sigma_{s_2}^{(2)}\}$ に含まれないとして一般性を失わない (必要があれば2つの表示を入れ替える)。ここで、 $\sigma_1^{(1)} \neq e$ なので $i \in S(\sigma_1^{(1)})$ をとり、 $i \in S(\sigma_t^{(2)})$ なる $t = 1, \dots, s_2$ をとる (存在しないとき $\sigma_t^{(2)} = e$ とする)。このとき、仮定から $\sigma_1^{(1)} \neq \sigma_t^{(2)}$ なので補題1より、ある整数 m が存在して、 $(\sigma_1^{(1)})^m(i) \neq (\sigma_t^{(2)})^m(i)$ となる。しかしこのとき、補題2より、

$$\sigma^m(i) = (\sigma_1^{(1)})^m(i) \neq (\sigma_t^{(2)})^m(i) = \sigma^m(i)$$

なので矛盾。よって、表示の一意性が示された。

(2)*2 (1) より、任意の \mathfrak{S}_n の元は巡回置換の合成として書けるので、巡回置換が s_i らの合成で表されることを示せばよい。今 $(i_1 \cdots i_k)$ を巡回置換とすると、

$$(i_1 \cdots i_k) = (i_1 i_2)(i_2 i_3) \cdots (i_{k-1} i_k) \quad (1)$$

となることが直接各 $i \in \{1, \dots, n\}$ の両辺の写像による像を比較することで、容易に確かめられる。これより、互換が s_i らの合成で表されることを示せば十分である。この事実を各互換 $(i j)$, $i < j$ に対して、 $j - i$ の値に関する帰納法で示す。 $j - i = 1$ のとき、 $(i j) = (i i + 1) = s_i$ なので良い。 $j - i > 1$ のとき、

$$s_{j-1}(i j - 1)s_{j-1} = (j - 1 j)(i j - 1)(j - 1 j) = (i j) \quad (2)$$

となることが直接各 $i \in \{1, \dots, n\}$ の両辺の写像による像を比較することで、容易に確かめられる。今、帰納法の仮定より $(i j - 1)$ は s_i らの合成で表されることがわかっているので、(2) より $(i j)$ も s_i らの合成で表される。帰納法により、証明すべきことは全て示された。□

*1 さらに詳しく説明すると、 Σ_{i_t} は有限集合なので、ある $m_1, m_2 (m_1 < m_2)$ が存在して、 $\sigma^{m_1}(i_t) = \sigma^{m_2}(i_t)$ となる。両辺に σ^{-m_1} を適用すると $i_t = \sigma^{m_2-m_1}(i_t)$ となるので、 $\sigma^m(i_t) = i_t$ を満たす正の整数 m は必ず存在する。

*2 ここでは (1) を用いた証明を行うが、(1) を用いなくても直接証明できる。例えば、 $\mathfrak{S}_{n-1} \hookrightarrow \mathfrak{S}_n$ という自然な埋め込みを用いて、 n に関する数学的帰納法を用いる証明もある。考えてみよう。