代数学IIのテキスト

有限群論の基本

脇 克志
弘前大学 理工学部
waki@cc.hirosaki-u.ac.jp

平成18年1月30日

これは、平成１７年後期 「代数学 II」のためのテキストです。

Time-stamp: <05/09/30 17:14:06 waki>

目 次

第1章　群の定義と群の例

「群」とはなにか？ この章では、抽象的な「群」というものが、何なのかを具体的な例を挙げながら解説して行きます。

1.1　群の定義

群とはどんなものでしょうか?この章では群について少しづつ説明してきます。まず群を一言で表してみましょう。

$$\boxed{\text{群はある意味で動きの集合!}}$$

ところで集合といえば、どんなものを思い出しますか？次にいくつかの集合とそれが群になるかどうかを示してみます。

- 日本人の集合 $\longrightarrow$ 群でない
- 自然数の集合 $\mathbb{N} := \{1, 2, 3, \cdots\}$ $\longrightarrow$ 群でない
- 実数の集合 $\mathbb{R}$ $\longrightarrow$ 群である
- ５人でやるあみだくじ全部の集合 $\longrightarrow$ 群である
- 正方行列全体の集合 $\longrightarrow$ 群であったりなかったり？
- 逆行列を持つ $n \times n$ 行列全体の集合 $\longrightarrow$ 群である

ここから、どんな集合が群になるか想像できますか？実は集合が群になるためには重要なプラスアルファが必要なのです。それでは、これらの集合が群になるための条件を見ていきましょう。

二項演算

集合が群に変身するために必要なものが、**二項演算**です。二項演算とは、「足し算」や「引き算」のようにある集合に含まれる２つの元から新しく１つの元作るしくみのことです。例えば、「足し算」は数の集合の元 5 と 3 から新しく 8 を作り出すしくみです。このとき、私たちは、$5+3=8$ と書きます。ここで、$+$ が二項演算の「足し算」を表しています。「集合」と「二項演算」は、例えば 「食材」と「調理用具」のような関係です。「おいしい料理」を作るには、調理用具を使って食材を「変化」させる必要があります。「食材」と「調理用具」を上手に使わないと「おいしい料理」は出来ないように、「群」を作るには、集合と二項演算のうまい関係が必要になってきます。では、このうまい関係を表す言葉を定義しましょう。

定義 1.1.1 二項演算 $*$ が集合 G で定義されていて、G の任意の２つの元 x, y に対して、演算の結果 $x*y$ が常に、G の元になるとき、つまり

$$\forall x, y \in G \Longrightarrow x*y \in G$$

なら、二項演算 $*$ は集合 G で**閉じている**と呼びます。

例えば実数の集合など、１つの集合が２つ以上の二項演算を持つ場合もあります。「閉じている」という事実は対応する二項演算によって変わってきます。例えば、自然数の集合 $\mathbb{N}$ は、二項演算「足し算」で閉じていますが、二項演算「引き算」では、閉じていません。$(2-5=-3 \notin \mathbb{N})$

問 1.1.2 先ほど挙げた集合の例の中で二項演算を持ち、その二項演算で閉じているものを見つけなさい。

単位元と逆元

次に、集合 G が群になるために、G が含んでいなければいけない特別な元について説明しましょう。数字の中には、0 や 1 のように他の数よりちょっと特別な数字があります。0 や 1 は、それぞれ「足し算」や「掛け算」と組み合せて次のように「特徴付け」することができます。

$$\forall x \in \mathbb{R} \Longrightarrow x + 0 = 0 + x = x, \qquad x \times 1 = 1 \times x = x$$

つまり、0 と 1 は、それぞれの二項演算で、どんな元 x と演算しても、元 x をまったく変化させないことが見えてきます。そこで、集合と二項演算が与えられたとき、次のような特別の元を定義します。

定義 1.1.3 集合 G と G で閉じている二項演算 $*$ が与えられたとき、G の元 e で、任意の G の元 x に対して、$x * e = e * x = x$ となる元を**単位元**と呼びます。

命題 1.1.4 二項演算 $*$ で閉じている集合 G が与えられたとき、G が 2 つ以上の単位元を持つことはない。

証明 集合 G が 2 つの単位元 e_1 と e_2 を持つとすると、e_1 も e_2 も G の元なので、単位元の性質から、$e_1 = e_1 * e_2 = e_2$ となり 2 つの単位元は同一となります。∎

問 1.1.5 問 *1.1.2* の答えの中でそれぞれの単位元を見つけよ。

さて、「足し算」について考えてみましょう。0 は「足し算」における単位元となります。数直線を考えると数 0 は、ちょうど真ん中にいるイメージがあります。そして 0 以外の数には、それぞれ相方となる数がいることに気が付きます。つまり、5 に対しては -5 、12 に対しては、-12 のように 0 を中心とした対称な位置にある数です。そしてこの数のペアー同士を「足し算」すると中心に位置する単位元 0 になることも分かります。$(5 + (-5) = 0,\ 12 + (-12) = 0)$ では二項演算に関連してもう 1 つ特別な名前をつけた元を定義しましょう。

定義 1.1.6 集合 G と G で閉じている二項演算 $*$ が与えられ、さらに G の中に単位元 e があるとする。このとき、G の元 x に対して、$x * y = y * x = e$ となる G の元 y が存在するとき、この y を元 x の**逆元**と呼び、y を x^{-1} と書き表します。

命題 1.1.7 二項演算 $*$ で閉じている集合 G が与えられたとき、G の元 x が 2 つ以上の逆元を持つことはない。

証明 元 x が 2 つの逆元 x_1 と x_2 を持つとすると、$x_1 = x_1 * e = x_1 * (x * x_2) = (x_1 * x) * x_2 = e * x_2 = x_2$ より、2 つの逆元は同一となります。∎

命題 1.1.8 二項演算 $*$ で閉じている集合 G が与えられたとき、G の元 x, y が逆元 x^{-1}, y^{-1} を持つならば、その積 $x * y$ も逆元を持ち、$(x * y)^{-1} = y^{-1} * x^{-1}$ となる。

問 1.1.9 問 *1.1.5* の答えの中で逆元を持つような元を見つけよ。

群になるための条件

それでは、いよいよ集合 G が群となるための条件を示します。

定義 1.1.10 集合 G が次の *4* つの条件を満たすとき、**群**であると言います。

g1. 集合 G はある二項演算 $*$ で閉じている。

g2. 集合 G の任意の元 a, b, c に対して、等式 $(a * b) * c = a * (b * c)$ が常に成り立つ。（結合律）

g3. 集合 G は、この二項演算 $*$ に対する単位元 e を含む。

g4. 集合 G の任意の元 a に対して、その逆元 a^{-1} が G の中に常に含まれる。

では、いろいろな具体例で、上の条件が満たされているかどうか調べてみましょう。

集合	自然数	自然数	整数	整数	実数	正の実数
二項演算	足し算	掛け算	掛け算	足し算	掛け算	掛け算
条件 g1.	○	○	○	○	○	○
条件 g2.	○	○	○	○	○	○
条件 g3.	×	○	○	○	○	○
条件 g4.	×	×	×	○	×	○

定義 1.1.11 群 G に含まれる元の個数を、群 G の**位数**と呼び、$|G|$ で表します。特に位数が有限の群を**有限群**、位数が無限の群を**無限群**と呼びます。

問 1.1.12 上の表で「×」となっている部分についてその理由を述べよ。

1.2 群の例

ここでは、いろいろな有限群の例を見てみましょう。

例 1.2.1 整数全体の集合 $\mathbb{Z}$

1.1 で見たように、整数全体の集合 $\mathbb{Z}$ は、二項演算に足し算 $+$ を使うことで群となります。$\mathbb{Z}$ は、元を無限に持つ無限集合なので、無限群となります。単位元は、*0* で、ある元 x の逆元は $-x$ となります。$\mathbb{Z}$ の代りに偶数全体の集合 $2\mathbb{Z} := \{2x \,|\, x \in \mathbb{Z}\}$ にしてもやっぱり群になります。しかし奇数全体の集合は、群にはなりません。

問 1.2.2 奇数全体の集合は、なぜ群にならないのか理由を示せ。

例 1.2.3 数字の 1 だけからなる集合

つまり、$G = \{1\}$ とします。二項演算は掛け算 $\times$ にすると、G は、群になります。もちろん $1 \times 1 = 1$ より単位元は *1* でどんなに掛け算を繰り返しても *1* 以外の元は現れません。この群の位数は *1* で、もっとも小さい群です。あまりに単純な群なので、**自明な群**と呼ばれています。

例 1.2.4 数字の 1 と -1 だけからなる集合

こんどは、2 つの元で $G = \{1, -1\}$ とし二項演算は掛け算 $\times$ にすると、G は、群になります。単位元はやっぱり *1* です。$-1 \times -1 = 1$ より、-1 の逆元は、-1 自身となります。群の位数は *2* となります。**本質的**に位数が *2* の群はこの群であることが分かっています。

例 1.2.5 数字の集合 $\{1, 5, 7, 11\}$

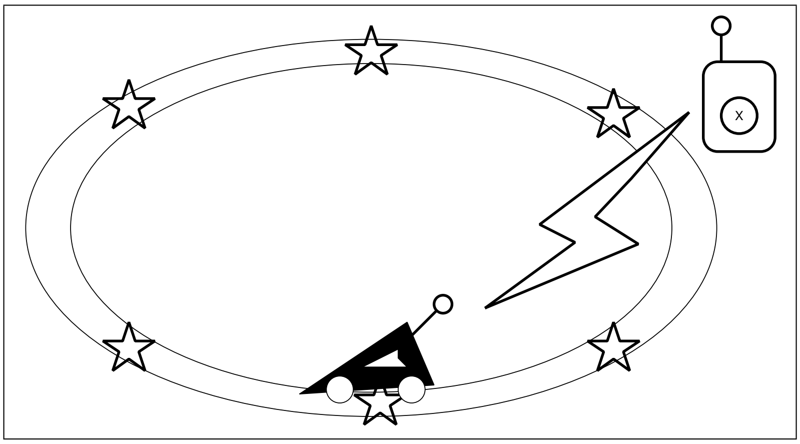
数字の集合 $G := \{1, 5, 7, 11\}$ に二項演算 を $a * b := (a \times b) \mod 12$ $(a, b \in G)$ *(*つまり、*2* つの数 a, b について $a * b$ は、a と b の積を *12* で割った余りにする*)* と決めるとこの G は、位数が *4* の群になります。

例 1.2.6 数字の 0 から $n-1$ までの集合 $\mathbb{Z}_n$

数字の集合 $\mathbb{Z}_n := \{0, 1, 2, \cdots, n-1\}$ に二項演算を $a * b := (a + b) \mod n$ $(a, b \in \mathbb{Z}_n)$ *(*つまり、*2* つの数 a, b について $a * b$ は、a と b の和を n で割った余りにする*)* と決めるとこの $\mathbb{Z}_n$ は、位数が n の群になります。特に、$n = 2$ のとき $\mathbb{Z}_2$ は、例 *1.2.4* と演算が足し算か掛け算かの違いだけで、実質同じ群になります。

例 1.2.7 おもちゃの自動車の動きからなる集合

次の絵のような、おもちゃの自動車を考えます。



このおもちゃの自動車は、右上にあるリモコンのボタン x を押すたびに次の☆マークまで移動します。ボタンを押す回数により自動車の動きが変わりますが、６回押した場合は自動車は、「動かない」のと同じ状態になります。このとき、自動車の動きは、全部で６通りあり、それぞれの動きは、１回から６回までのボタンを押す回数に対応します。ボタンを n 回押すことを x^n で表すとすると、自動車の動きの集合は、ボタンの押す回数に対応して、$G = \{x, x^2, x^3, x^4, x^5, x^6\}$ で表すことができます。ここで二項演算を「二つの動きの合成」とすると、G は群となります。単位元を e とすると、すべての動き x^i $(i = 1 \ldots 6)$ について $x^i * e = x^i$ とならなくてはいけません。このような動きは、「動かない」という動きしかありません。つまり、$e = x^6$ となります。それぞれの元の逆元を考えると、次の表になります。

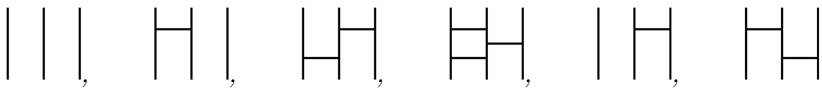
元	x	x^2	x^3	x^4	x^5
逆元	x^5	x^4	x^3	x^2	x^1

定義 1.2.8 群 G の元 x に対して、ある自然数 n が $x^n = e$ となる最小の自然数のとき、この n を x の**位数**と呼びます。ちなみに単位元の位数は *1* です。

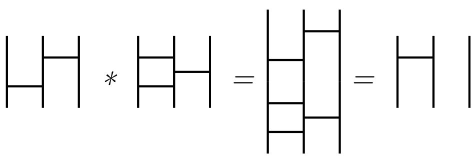
群の位数と混乱しそうですが、命題 3.2.8 で、なぜ同じ用語を使うのかが分かります。

例 1.2.9 あみだくじの集合

縦棒が３本のあみだくじの集合を考えましょう。余計な横線を省くと本質的には、縦棒が３本のあみだくじ次の *6* つになります。



このとき、*2* つのあみだくじに対する二項演算をそのあみだくじを縦に並べて、余計な横線を省いたあみだくじとします。例えば、

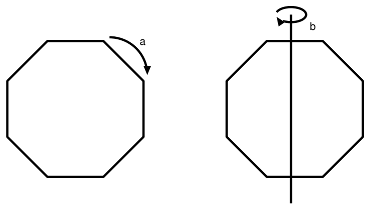


のように、二項演算を行うことができます。

問 1.2.10 あみだくじの集合が群になることを、確認し単位元とそれぞれの元の逆元を見つけよ。

例 1.2.11 正８角形に対する動きの集合

正８角形に対する時計回りの *45* 度回転の動き a と裏返す動き b の組合わせでできる動き全体の集合を考えます。



動きは全部で１６種類となります。ここでも二項演算は「動きの合成」とするとやっぱり群になります。

問 1.2.12 正８角形に対する動きの集合に含まれる動きをぜんぶ求めて a, b を使って表せ。

いままで述べてきた集合は、例 1.2.5 以外は、「ある意味で動きの集合」と見ることができます。「整数全体の集合 $\mathbb{Z}$」は、歩く動き（２歩進むとか３歩戻るとか...）の集合、「数字の１だけからなる集合」は、動かない動きの集合、「数字の１と-1 だけからなる集合」は、１枚の紙を裏返す動きの集合、また、例 1.2.6 は、「おもちゃの自動車の動きの集合」を一般化したものと捉えることが出来ます。つまり $\mathbb{Z}_6$ が「おもちゃの自動車の動きの集合」と同等であることに、気がついてください。そして残りの集合はまさに「ある意味で動きの集合」です。このように、これから学ぶ群とは、「動き」を数学的に扱っていく理論と見ることができます。

1.3　章末問題

問題 1.1 集合 $X := \{0, 1, 2, \ldots, 17\}$ に二項演算 $*$ を次のように決めた。$\forall x, y \in X,\ x * y = (x \times y)\ mod\ 18$

(a) この 2 項演算における単位元はなにか？

(b) X の元で、逆元を持つ数とその逆元をすべて求めよ。

問題 1.2 集合 $X := \{1, 2, \ldots, 12\}$ に二項演算 $*$ を次のように決めた。$\forall x, y \in X,\ x * y = (x \times y)\ mod\ 13$

(a) この 2 項演算における単位元はなにか？

(b) 逆元を持つ数とその逆元をすべて求めよ。

(c) $G = \{1, 2, \ldots, 12\}$ は、二項演算 $*$ で群になるか確認せよ。

問題 1.3 n 次元実ベクトル空間 $\mathbb{R}^n$ は、ベクトルの足し算で群となることを示せ。

問題 1.4 n 次元実ベクトル空間 $\mathbb{R}^n$ の部分空間 W がベクトルの足し算で群となることを示せ。

問題 1.5 *3* 次元実ベクトル空間 $\mathbb{R}^3$ 上で、ベクトル $v = (1, 1, 1)$ と直行するベクトル全体の集合 $G = \{w \in \mathbb{R}^3 \,|\, (v, w) = 0\}$ がベクトルの足し算で群となることを示せ。

問題 1.6 2×2 の正方行列全体の集合に対して、行列の掛け算を二項演算としたときの単位元を求めよ。

問題 1.7 *3* 次元実ベクトル空間 $\mathbb{R}^3$ に含まれる平面が、ベクトルの足し算で群となるための条件を求めよ。

問題 1.8 次にあげる集合 G の内、どれが群になり、どれが群でないかを理由をつけて説明せよ。

(a) $G = \{x | x \in \mathbb{R}\}$ 二項演算はかけ算

(b) $G = \{x^2 | x \in \mathbb{N}\}$ 二項演算はかけ算

(c) $G = \{\log x | x > 0\, x \in \mathbb{R}\}$ 二項演算は足し算

(d) $G = \{x | x \in \mathbb{R}\} \backslash \{0\}$ 二項演算は割算

(e) $G = \left\{ \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \middle| \, a, b, c, d \in \mathbb{R} \right\}$ 二項演算は行列のかけ算

1.4　章末問題の解答

解答 1.1　*(a)* *1* ですね。

(b) $1^{-1} = 1,\ 5^{-1} = 11,\ 7^{-1} = 13,\ 17^{-1} = 17$

解答 1.2　*(a)* *1* ですね。

(b) $1^{-1} = 1,\ 2^{-1} = 7,\ 3^{-1} = 9,\ 4^{-1} = 10,\ 5^{-1} = 8,\ 6^{-1} = 11,\ 12^{-1} = 12$

(c) *g1* は二項演算の定義から明らかです。*g2* は、積も mod も結合律を満たすので成り立ちます。*g3* は、*(a)* で確認していますし、*g4* は、*(b)* で確認しています。

解答 1.3 $\mathbb{R}^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in \mathbb{R}\}$ で、$\mathbb{R}^n$ の 2 つのベクトル $a := (a_1, a_2, \ldots, a_n),\ b := (b_1, b_2, \ldots, b_n)$ に対して二項演算 $a * b = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$ より、*g1,g2* は、成立します。単位元は 零ベクトル $(0, 0, \ldots, 0)$ が存在しますので、*g3* が成り立ちます。また、ベクトル $a := (a_1, a_2, \ldots, a_n)$ の逆元 a^{-1} は、明らかに $(-a_1, -a_2, \ldots, -a_n)$ でこれも $\mathbb{R}^n$ に含まれるので、*g4* も成り立ちます。

解答 1.4 部分空間の定義から部分空間 W が群の条件をすべて満たします。

解答 1.5 内積の定義から、集合 G が *3* 次元実ベクトル空間 $\mathbb{R}^3$ の部分空間になることが分かりますので、問題 *1.4* から G が群であることが分かります。

解答 1.6 単位元は、単位行列 $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ですね。

解答 1.7 平面は、原点を通るときのみ部分空間となります。よって群になるのは原点を含む平面のみとなります。

解答 1.8 *(c)* だけが、群となります。*(a)* は、*0* が逆元をもちません。*(b)* では、*4* が逆元を持ちません。*(d)* では、$(4/2)/2 \neq 4/(2/2)$ のように結合律 *g2* が成り立ちません。*(e)* では、逆行列を持たない行列が逆元を持ちません。

`Time-stamp: <05/11/22 00:20:47 waki>`

第2章　置換と置換群

この章では、群の中で特に重要な置換群を取り上げます。最初は、頭が混乱するかも知れませんが、次の言葉を心に刻んでおいてください。

置換はあみだです!

2.1　置換の定義

最初に置換の定義をまじめに書きます。

定義 2.1.1 有限集合 $X := \{1, 2, \ldots, n\}$ が与えられたとき、集合 X から集合 X への全単射の写像 σ を、X の n 次の**置換**と呼びます。

定義 2.1.2 集合 X 上で定義された *2* つの置換 σ, ρ が与えられたとき**置換の積** $\sigma * \rho$ を次のように定義します。

$$(\sigma * \rho)(i) := \rho(\sigma(i))$$

写像 $\sigma * \rho$ も全単射となることから、$\sigma * \rho$ も置換と見ることが出来ますので、この $*$ は、置換同士の二項演算となります。

どうでしょうか? この定義だとわかりにくくて実感がわかないので例を示します。

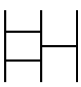
置換の例 1

集合 $X = \{1, 2, \ldots, n\}$ としましょう。写像 e を X から X への恒等写像 (つまり $\forall i \in X;\ e(i) = i$) とすると、恒等写像はは全単射になりますので、$e$ は、n 次の置換です。この恒等写像に対応する置換は、まさに単位元のような性質を持ちます。つまり、任意の置換 σ に対して $\sigma * e = e * \sigma = \sigma$ となります。

置換の例 2

集合 $X = \{1, 2, \ldots, n\}$ 上の置換 σ が与えれたとき、σ は、X から X への全単射なので、σ の逆写像 ρ が存在します。($\forall i \in X$ について $i = \rho(\sigma(i)) = \sigma(\rho(i))$) このとき、逆写像 ρ も全単射となるので、ρ も置換となります。σ の逆写像に対応する置換を σ^{-1} で表します。

置換の例 3

あみだ  を考えましょう。集合 $X := \{1, 2, 3\}$ として、X の元 i $(i \in X)$ に対して、あみだの左から i 番目の所からスタートして、下って行って左から j 番目に着いたとき、あみだに対応して写像 $\rho(i) := j$ と決めます。よって上のあみだに対応する写像は、$\rho(1) = 3,\ \rho(2) = 2,\ \rho(3) = 1$ となります。この写像 ρ も X の全単射となるので、3 次の置換と見なすことが出来ます。

命題 2.1.3 置換 σ とその逆写像に対応する置換 σ^{-1} について、$\sigma * \sigma^{-1}$ と $\sigma^{-1} * \sigma$ は、恒等写像に対応する置換 e となる。

証明この置換の積より、置換 σ とその逆写像に対応する置換 σ^{-1} が与えられると、$\forall i \in X,\ (\sigma * \sigma^{-1})(i) = \sigma^{-1}(\sigma(i)) = i = \sigma(\sigma^{-1}(i)) = (\sigma^{-1}*\sigma)(i)$ となる。よって $\sigma*\sigma^{-1}$ と $\sigma^{-1}*\sigma$ は恒等写像となり、$\sigma*\sigma^{-1} = \sigma^{-1}*\sigma = e$ となることが分かります。∎

定義 2.1.4 置換 σ を m 回掛けたものを、σ^m と表し、置換 σ^{-1} を m 回掛けたものを、σ^{-m} と表します。特に、命題 *2.1.3* より、σ^{-m} は、σ^m の逆写像に対応する置換となります。また、*2* つの自然数 n, m に対して $\sigma^m * \sigma^{\pm n} = \sigma^{m\pm n}$ となり、$\sigma^0 = e$ となります。

問 2.1.5 *2* つの全単射写像 σ, ρ が与えられたとき、$\sigma * \rho$ も全単射写像となることを示せ。

なんだか、難しく見えますが、これは前章のあみだの積をそのまま使っています！

命題 2.1.6 集合 $X := \{1, 2, \ldots, n\}$ に関する置換 σ について、X の元 i に対して、ある自然数 m が存在して、$\sigma^m(i) = i$ となる。

証明 自然数 k に対して $a_k = \sigma^k(i)$ と決めます。今数列 $a_1, a_2, a_3, \cdots$ を考えると、$1 \leqq a_k \leqq n$ より、無限に異なる a_k が現れることはなく、$a_k = a_l$ となる相異なる k と l が存在します。今 $k < l$ とすると $\sigma^k(i) = a_k = a_l = \sigma^l(i)$ より、$m = l - k$ とすると、

$$\begin{aligned}
\sigma^m(i) &= \sigma^{l-k}(i) \\
&= (\sigma^l * \sigma^{-k})(i) \\
&= \sigma^{-k}(\sigma^l(i)) \\
&= \sigma^{-k}(\sigma^k(i)) \\
&= (\sigma^{-k} * \sigma^k)(i) \\
&= e(i) \\
&= i
\end{aligned}$$

∎

置換の書き表し方

置換を表すときにいちいち写像として書き表していると大変なので、置換には独特の表し方があります。

定義 2.1.7 n 次の置換 σ に対して $\sigma(1) = i_1, \sigma(2) = i_2, \cdots, \sigma(n) = i_n$ とします。このとき、

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

と表します。もし σ が a_1 を 最小とする k 個の数 $a_1, a_2, \cdots, a_k$ $(1 \leqq k \leqq n)$ を $\sigma(a_1) = a_2,\ \sigma(a_2) = a_3,\ \cdots,$ $\sigma(a_{n-1}) = a_n,\ \sigma(a_n) = a_1$ と巡回的に移してその他の数字をまったく動かさないとき、σ を長さ k の**巡回置換**と呼び $\sigma = (a_1, a_2, \ldots, a_k)$ と表します。特に、長さ *2* の巡回置換を**互換** と呼びます。

例えば、 $\sigma = (1, 2, 3)$ なら

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

と見て、$\sigma(1) = 2,\ \sigma(2) = 3,\ \sigma(3) = 1$ を得ます。

命題 2.1.6 より、どんな置換も**共通の数字を含まない巡回置換の積**で表せることになります。例えば、

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

なら

$$\sigma = (\ 1,\quad 2,\quad 3\ )(\ 4,\quad 5\ )$$

となります。また、

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix}$$

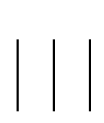
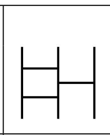
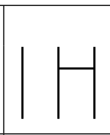
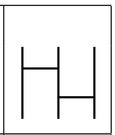
なら

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

となります。以後、置換はこの形で表現することにします。

2.2 あみだと置換

さて、あみだについてもう少し考えてみます。あみだはいくつかの横棒を、付けることで、入れ換えを作り出しています。つまりあみだで作る置換は隣り合う数字の互換の積であると言えます。 例えば、1 章に出てきたあみだの群の元は次のように置換と対応しています。

					
e	(1,2)	(1,2,3)	(1,3)	(2,3)	(1,3,2)

次の命題で、すべての置換があみだで表現できることを示します。

命題 2.2.1 n 次の置換は $n-1$ 個の互換 $(1,2),(2,3),\ldots,(n-1,n)$ の積で表すことができる。

証明 定義 2.1.7 より、すべての置換は巡回置換の積で表されていることが分かります。よって、あとは、巡回置換が互換の積で表されることを証明すれば良いことになります。そこで巡回置換 $\sigma=(a_1,a_2,\ldots,a_s)$ を考えましょう。このとき、σ は、互換を使って $\sigma=(a_1,a_s)(a_2,a_s)\cdots(a_{s-1},a_s)$ と表せます。また、どんな互換 $(i,j)=(j,i)$ も、$(i,i+1)(i+1,i+2)(\cdots)(j-1,j)(j-2,j-1)(\cdots)(i,i+1)$ $(i<j)$ と表せます。∎

これで、置換は必ずあみだの形で表現できることが分かりました。ただし、その表し方は 1 通りでは無いことに注意しましょう。例えば、置換 $(1,3)$ は、あみだの形で、$(1,2)(2,3)(1,2)$ とも $(2,3)(1,2)(2,3)$ とも表せます。

定義 2.2.2 n 次の置換全体の集合を、$\mathcal{S}_n$ で表し、n 次の**対称群**と呼びます。

問 2.2.3 $\mathcal{S}_n$ に含まれる n 次の置換の数を求めよ。また、$\mathcal{S}_n$ が群となることを確認せよ。

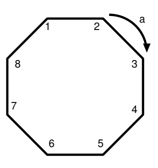
2.3 置換群の例

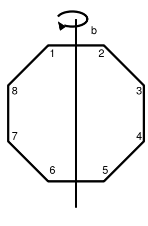
ここでは、今まで定義してきた群たちを、置換群として定義し直して見ましょう。

置換群は、有限群となるので無限群を置換群として表現することはできません。では、例 1.2.4 の数字の 1 と -1 で出来る位数 2 の群は、どうでしょうか？何も動かさない単位元を e で表すと、$\{e,(1,2)\}$ が位数 2 の群となります。これは、2 次の対称群と見ることもできます。

次に、例 1.2.7 の「おもちゃの自動車動きからなる群」はどうでしょうか？このとき、ボタン x は、自動車の移動に対応していて、自動車のいる場所に $1,2,\cdots,6$ と番号を付けると、1 にいた場合は、2 に移動し、2 にいた場合は、3 に移動しますから、ボタン x は、置換 $(1,2,3,4,5,6)$ に対応すると見ると良いでしょう。この群は、$G=\{x,x^2,x^3,x^4,x^5,x^6\}$ となりましたから $x=(1,2,3,4,5,6)$ と置けば、$G=\{(1,2,3,4,5,6),(1,3,5)(2,4,6),(1,4)(2,5)(3,6),(1,5$ $(1,6,5,4,3,2),e\}$ となります。

最後に、例 1.2.11 の「正 8 角形に対する動きの群」では、正 8 角形に次の様に番号を付けることで、





$a=(1,2,3,4,5,6,7,8)$, $b=(1,2)(3,8)(4,7)(5,6)$ と表せます。問 1.2.12 を解くと $G=\{e,a,a^2,a^3,a^4,a^5,a^6,a^7,b,a*b,a^2*b,a^3*b,a^4*b,a^5*b,a^6*b,a^7*b\}$ となりますから、置換の元としては、$\{e$, $(1,2,3,4,5,6,7,8)$, $(1,3,5,7)(2,4,6,8)$,
$(1,4,7,2,5,8,3,6)$, $(1,5)(2,6)(3,7)(4,8)$, $(1,6,3,8,5,2,7,4)$, $(1,7,5,3)(2,8,6,4)$,
$(1,8,7,6,5,4,3,2)$, $(1,2)(3,4)(5,6)(7,8)$, $(2,8)(3,7)(4,6)$, $(1,8)(2,7)(3,6)(4,5)$,
$(1,7)(2,6)(3,5)$, $(1,6)(2,5)(3,4)(7,8)$, $(1,5)(2,4)(6,8)$, $(1,4)(2,3)(5,8)(6,7)$,
$(1,3)(4,8)(5,7)\}$ となります。

2.4　章末問題

問題 2.1 次の置換の積を求め、その元の位数も答えよ。

(a) $(1,6,3,8)(2,7,5)*(1,7)(2,6,3,8)(4,5)$

(b) $(1,4,8)(2,3,7,5,6)*(1,6,3,2,8)$

(c) $(1,3)(2,6,8)(4,7,5)*(1,8,5,2,3)(4,7)$

(d) $(1,2,7)(3,6)(5,8)*(1,2,4,6,5,3,7)$

(e) $(1,8,3,5,4,7,6,2)*(1,3,8,2,6)(4,7)$

(f) $(1,8,7)(2,5,6,3,4)*(1,8)(2,4)(3,7,6,5)$

(g) $(2,7,3,8,4)*(1,6)(2,5,4,3)(7,8)$

(h) $(1,5,7,3)(2,6,8,4)*(1,2,6,3,8)$

(i) $(1,4,6,3,7,2,8)*(1,6,8,3,7,2)$

(j) $(1,5,4)(2,8)(3,6)*(1,5)(2,6,8,3)(4,7)$

問題 2.2 *6* 次の対称群 $\mathcal{S}_6$ の中に、$(1,2,3,4)(5,6)$ のように、長さ 4 の巡回置換と互換で表される元はいくつあるか求めよ。

問題 2.3 *5* 次の対称群 $\mathcal{S}_5$ の元の中で、位数が偶数となる元の個数を求めよ。

問題 2.4 *4* 次の対称群 $\mathcal{S}_4$ の元 σ の中で、$\displaystyle\sum_{i=1}^{4} i\sigma(i)$ が最大と最小になるものをそれぞれ求めて、その値も示せ。

問題 2.5 互換 $s_i := (i, i+1)$ について、次を示せ。

$$\begin{array}{rcll} s_i * s_j & = & s_j * s_i & \textit{if } |i-j| > 1 \\ s_j * s_i * s_j & = & s_i * s_j * s_i & \textit{if } |i-j| = 1 \end{array}$$

問題 2.6 *4* 次の対称群 $\mathcal{S}_4$ の元を、3 つの互換 $s_1 = (1,2),\ s_2 = (2,3),\ s_3 = (3,4)$ の積で表したとき、一番たくさん掛け算をしないと得られない元を求めよ。

問題 2.7 n 次の対称群 $\mathcal{S}_n$ は $n-1$ 個の互換 $s_1 = (1,2),\ s_1 = (2,3),\ \ldots\ ,s_{n-1} = (n-1,n)$ で生成されることを数学的帰納法を用いて証明せよ。

2.5　章末問題の解答

解答 2.1 *(a)* $(1,3,2)(4,5,6,8,7)$, *(b)* $(1,4)(3,7,5)(6,8)$, *(c)* $(2,6,5,7)(3,8)$, *(d)* $(1,4,6,7,2)(3,5,8)$, *(e)* $(1,2,3,5,7)$, *(f)* $(2,3)(6,7,8)$, *(g)* $(1,6)(2,8,3,7)(4,5)$ *(h)* $(1,5,7,8,4,6)(2,3)$, *(i)* $(1,4,6,3,7,2,8)*(1,6,8,3,7,2)$, *(j)* $(2,3,8,6)(4,5,7)$

解答 2.2 まず、互換の組み合せは全部で $(6\times5)/2 = 15$ 個、残りの *4* つの数で一番小さい数を除いた *3* つの並び方が $3! = 6$ なので、全部で $15\times6 = 90$。

解答 2.3 *5* 次の対称群 $\mathcal{S}_5$ の個数は、$5\times4\times3\times2 = 120$ です。位数が奇数となる元を考えると、単位元、 *(1,2,3)* の型、 *(1,2,3,4,5)* の型だけです。それぞれの元の数は、*1*, 5×4, $4\times3\times2$ となるので、総計 *45* となります。よって位数が偶数となるのは、 $120-45 = 75$ です。

解答 2.4 $a < b,\ i < j$ に対して $(b-a)(j-i) > 0$ より、展開すると $ai + bj > aj + bi$。よって最大は、$\sigma = e$ で、$1\times1+2\times2+3\times3+4\times4 = 30$ 最小は、$\sigma = (1,4)(2,3)$ で、$1\times4+2\times3+3\times2+4\times1 = 20$

解答 2.5 $i,\ j$ に具体的な数字を当てはめて感覚を掴んで一般の形で証明してみましょう。

解答 2.6 一番長いのは、$s_1 * s_2 * s_1 * s_3 * s_2 * s_1 = (1,4)(2,3)$ です。

解答 2.7 n に対する数学的帰納法で求めます。$n = 2$ なら、$\mathcal{S}_2$ が $s_1 = (1,2)$ で生成されることは、明らかです。$n = k$ でここでの主張が成り立つと仮定すると。$\mathcal{S}_k$ は、$s_1, s_2, \cdots, s_{k-1}$ で生成されます。$s_1, \cdots, s_{k-1}, s_k$ は、すべて $\mathcal{S}_{k+1}$ に含まれるので、$\langle s_1, \cdots, s_k \rangle$ は、$\mathcal{S}_{k+1}$ に含まれます。次に、任意の元 $\rho \in \mathcal{S}_{k+1}$ について、$\rho(k+1) = k+1$ なら、$\rho \in \mathcal{S}_k$ となり仮定より、ρ は、s_1 から s_{k-1} の積で表せます。もし、$\rho(k+1) = i < k+1$ なら、$\mathcal{S}_{k+1}$ の元 $\sigma = s_i * s_{i+1} * \cdots * s_k$ が定義できて、$\rho * \sigma(k+1) = k+1$ となり、仮定より $\rho * \sigma$ も、s_1 から s_{k-1} の積で表せます。よって、ρ は、s_1 から s_k の積で表せ $\langle s_1, \cdots, s_k \rangle$ に含まれます。

Time-stamp: <05/11/08 13:58:41 waki>

第3章　部分群とその性質

　群の性質を調べる上で、その中に含まれる部分的な構造を見ることは、とても大事です。この章で言いたいことを一言で表すと、次の様になります。

部分群は群の約数だ!

例えば、6 という数は、因数分解で 2×3 や 1×6 とできます。ちょうど、6 が群なら、2 や 3 や 1 などが部分群に当ります。

3.1　部分群の定義

　まず部分群の定義から始めましょう。

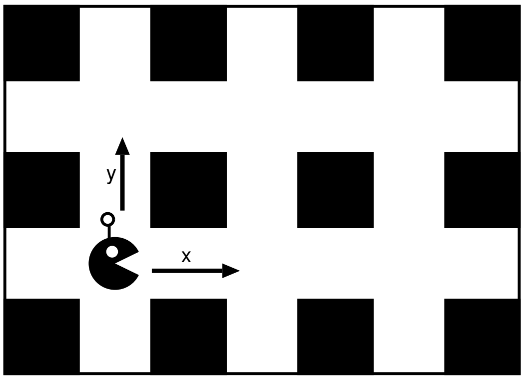
定義 3.1.1 群 G とその二項演算 $*$ が与えられているとき、G の部分集合 H が次の *2* つの条件を満たすとき H を G の**部分群**と呼びます。

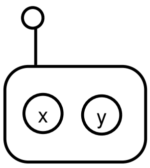
s1. $\forall a, b \in H \Longrightarrow a * b \in H$

s2. $\forall a \in H \Longrightarrow a^{-1} \in H$

　では、具体的な例を見てみましょう。

例 3.1.2 パックマンの動きの群 次の絵のように、パックマンは右のリモコンスイッチ x、y を押すことで、右または、上に 1 ブロック分移動します。ただし、右端を過ぎると左端に上辺を過ぎると底辺から、現れることとします。





　このとき、パックマンの動きは、スイッチ x、y を押すことに対応しています。とくに、x を三回押す x^3 や y を二回押す y^2 は、もとの位置に、戻ってしまうので、「動かない」動きに対応します。よって、パックマンの動きの集合 G は、単位元である「動かない」動きを e とすると $\{e, x, x^2, y, xy, x^2y\}$ と表されます。二項演算を「動きの合成」とすると、この集合 G は、群となるための条件を満たして群となります。

問 3.1.3 パックマンの動きの群が群になることを、確認せよ。

　ここでスイッチ x だけ得られる動き全体の集合を H とすると、$H = \{e, x, x^2\}$ となります。この H は、定義 3.1.1 の条件を満たすので、G の部分群となります。

3.2　部分群の性質

それでは、部分群の持つ性質を調べてみましょう。

命題 3.2.1 群 G とその部分群 H に対して、H は、G の単位元を必ず含む。

証明： H のある元 x に対して、条件 s2. より、$x^{-1} \in H$ です。よって、条件 s1. を使えば、x と x^{-1} が H の元であることより、単位元 e について、$e = x * x^{-1} \in H$ が成り立ちます。∎

命題 3.2.2 群 G とその部分群 H に対して、H は、G の二項演算で群となる。

証明： 群となるための 4 つの条件を確認しましょう。 条件 g1. は、条件 s1. そのものなので、成立します。また H の元はすべて G の元であり、G が群であるので、G のすべての元（このなかに H のすべての元も含まれますが）で条件 g2. が成り立ちます。条件 g3. は、命題 3.2.1 から成立しますし、条件 g4. は、条件 s2. なので、成立します。∎

定義 3.2.3 群 G とその部分群 H に対して、集合として、H が G より真に小さいとき、H を G の**真部分群**と呼びます。

パックマンの動きの群では、$y \notin H$ より、H は、真部分群となります。

命題 3.2.4 H_1, H_2 が群 G の部分群とすると、集合 $H_1 \cap H_2$ も G の部分群となる

問 3.2.5 命題 *3.2.4* を証明せよ。

命題 3.2.4 より、群 G の部分集合 X に対して、X の元を含む最小の G の部分群が存在することが分かります。

定義 3.2.6 群 G とその部分集合 $X \subset G$ に対して、すべての X の元を含む G の最小の部分群を、X で**生成されたと** G の部分群と呼び、$\langle X \rangle$ で表します。さらに、X を群 $\langle X \rangle$ の**生成元**の集合と呼びます。

巡回群

ある群からその部分群を作りたい場合、もっとも簡単な方法は、群から 1 つの元 x を選んでこの 1 つの元から生成される部分群を作ることです。ここでは、そんな部分群について考えてみましょう。

定義 3.2.7 群 G の中にある元 x が存在し、群 G がこの *1* つの元 x で生成されるとき、つまり、$X = \{x\}$ として、$G = \langle X \rangle$ となるとき、群 G は、**巡回群**であると呼び、$\langle x \rangle$ と表します。

「パックマンの動きの群」の例では、$H = \{e, x, x^2\}$ は、元 x で生成される巡回群となります。また、「おもちゃの自動車の動きからなる集合」が巡回群であることも納得して貰えると思います。（これこそ巡回群のイメージですよね）

命題 3.2.8 群 G が巡回群で、$G = \langle x \rangle$ と表されたとき、G の位数は、x^n が単位元となる最小の n と等しい。特に、集合として、$G = \{e, x, \ldots, x^{n-1}\}$ となる。

証明 自然数 n を x^n が単位元となる最小の自然数とします。そして集合 $X_n = \{e = x^n = x^0, x, \ldots, x^{n-1}\}$ とします。このとき、$\langle x \rangle = X_n$ となることを示します。定義 3.1.1 の条件 s1 より、集合 X_n の元がすべて集合 $\langle x \rangle$ に含まれることが分かります。よって、集合 X_n が定義 3.1.1 の条件を満たして部分群となることを示せば良ことになります。任意の自然数 k に対して、k を n で割った余りを r とすると、$0 \leqq r \leqq n-1$ となります。x^n が単位元であることから、$x^k = x^r$ となり x^k は、X_n に含まれます。よって条件 s1 が成り立ちます。また、$s = n - r$ とすると、$1 \leqq s \leqq n$ で、x^s は、X_n に含まれ、更に $x^k * x^s = x^r * x^s = x^{r+s} = x^n = e$ となり、x^s が、x^k の逆元であることも示されます。よって条件 s2. の成立します。∎

つまり、群の元 x の位数は、群 $\langle x \rangle$ の位数と同じになります。(定義 1.2.8 を参考にしてください)

次に、巡回群が持つ基本的な性質を示します。

命題 3.2.9 群 G が巡回群ならその部分群もすべて巡回群となる。

証明 群 $G=\langle x\rangle$ として、群 G の位数を n とすると上の命題より、$G=\{e,x,x^2,\dots,x^{n-1}\}$ となります。H を G の部分群とすると命題 3.2.1 より、H は単位元 e を含む G の部分集合となりす。H の位数が m であれば、集合 $H=\{e,x^{a_1},\dots,x^{a_{m-1}}\}$ と表せます。今、d を自然数 $a_1,a_2,\dots,a_{m-1}$ の最大公約数とすると、d はある整数 $k_1,k_2,\dots,k_{m-1}$ を使って、$d=k_1a_1+k_2a_2+\cdots+k_{m-1}a_{m-1}$ と表せます。 よって

$$\begin{aligned} x^d &= x^{(k_1a_1+k_2a_2+\cdots+k_{m-1}a_{m-1})} \\ &= \left(x^{a_1}\right)^{k_1}*\left(x^{a_2}\right)^{k_2}*\cdots*\left(x^{a_{m-1}}\right)^{k_{m-1}}\in H \end{aligned}$$

から、x^d は、部分群 H に含まれます。いま元 x^d で生成される部分群 $\left\langle x^d\right\rangle$ を考えると定義より、$\left\langle x^d\right\rangle\subset H$ となります。さらに、d が各 a_i の約数となることから、ある自然数 s_i が存在して、$a_i=s_id$ となり、$x^{a_i}=(x^d)^{s_i}\in\left\langle x^d\right\rangle$ が成り立ちます。よって $H=\left\langle x^d\right\rangle$ となり、H は、巡回群となります。∎

問 3.2.10 パックマンの動きの群に対して、部分群 $\langle xy\rangle$ に含まれる元をすべて求めよ。

3.3 同値と剰余類

ここでは、部分群を使って群を切り分けることを考えます。そこでまず、「**同じ**」という概念をきちんと考えることから始めましょう。

同じ＝同値

数学の中では、等式がたくさん出てきます。しかしこの「＝（イコール）」という記号が結構曖昧であることに、気付いているでしょうか？ここでは、「同じ」ということがいかに「違う」かをまず認識して貰います。

スーパーで３本１００円のキュウリが売られている状況を想像してください。山のように積まれたキュウリを前にして売り子の人が、「安いよー!どれでも３本で１００円だよー!」と叫んでいます。そこに、一人の主婦が現れて山と積まれたキュウリの中から慎重に３本のキュウリを選びだしています。さて、このとき売り子が見ているキュウリと主婦が見ているキュウリでは、まったく違う立場が発生しています。売り子の心の叫びを表すと「なにぐずぐずしてるんだー！はやく選べよ。どれでも**同じ**だよ!」となります。一方主婦の気持は、「あら、こちらのキュウリはちょっと細いわ、こんなに**違った**キュウリが混ざっていると選ぶのは大変だわ」となります。二人の間でキュウリの見方がこんなに違ってしまった理由は、二人の持つキュウリに対する「**同じ**」のレベルが違うためです。 売り子にとってはすべて**同じ**３本１００円のキュウリとなりますが、主婦にとっては夕食に使う厳選素材としてのキュウリとなるわけです。人間はその立場ごとにこの「**同じ**」のレベルを自在に調整して日々の生活を営んでいます。これは、人間が得意で機械が苦手な作業の一つと言えます。機械にとって細かい違いを無視して同一視することはかなり難しいこととなります。では、このような「**同じ**＝同値」という概念をどのようにきちんと定義したらいいでしょうか？

定義 3.3.1 集合 X に対して次の *3* つの条件を満たす関係 $\sim$ を**同値関係**と呼びます。

d1. $\forall x\in X,\ x\sim x$　　x と x は同じ

d2. $\forall x,y\in X,\ x\sim y\Longrightarrow y\sim x$　　x と y が同じなら y と x も同じ

d3. $\forall x,y,z\in X,\ x\sim y,\ y\sim z\Longrightarrow x\sim z$　　x と y が同じで y と z も同じなら x と z も同じ

例えば、X を人類全体の集合とします。二人の人 $x,y\in X$ $x\sim y$ を「x と y は、同じ星座」とします。このとき、「自分自身は同じ星座」(d1)、「x と y が同じ星座」なら「y と x も同じ星座」(d2)、「x と y が同じ星座」で「y と z が同じ星座」なら「x と z も同じ星座」(d3) なりこの関係は同値関係となります。

ある１つの同値関係を集合 X の上に決めると、この同値関係を基にして集合 X の同値な元を集めて同じもの同士のグループを作ることができます。このように、同値な物を集めていく作業を、私たちは**「分類」**と呼んでいます。

定義 3.3.2 集合 X と同値関係 $\sim$ が与えられたとき、X の元 x に対して、x と同値な元全体の集合 $\{y\in X\,|\,x\sim y\}$ を元 x の**同値類**と呼び、I_x と書き表します。

ここで同値類とは、まさに同じと思われるものの集まりであり、私達はこのように同類のものを 1 つにまとめながら全体を分類していくわけです。先程の例では、まさに天秤座の人達全体の集合や牡牛座の人達全体の集合などが同値類となります。この分類と言う作業では、どの 1 つも必ずどこかの同値類（グループ）含まれることが大事です。さらにイソップ物語に出てくる「コウモリ」の様にケモノのグループと鳥のグループのどちらにも含まれるというの事が起らないことが大事です。それでは同値類が持つ性質を見て行きましょう。

命題 3.3.3 集合 X と同値関係 $\sim$ が与えられたとき、$x, y \in X$ に対して、次の *3* つの事柄は同値である。

(i) $I_x = I_y$

(ii) $x \sim y$

(iii) $I_x \cap I_y \neq \emptyset$

証明 (i) を仮定すると定義 3.3.1 d1 より、$x \in I_x = I_y$ となり $x \sim y$ が成り立ちます。(ii) を仮定すれば、$x \in I_x \cap I_y$ となり (iii) が成り立ちます。(iii) が成り立つと仮定すると、$I_x \cap I_y$ に含まれる元 z が存在し、同値類の定義から $x \sim z$, $y \sim z$ と成り立ちます。定義 3.3.1 の d2, d3 より、 I_x に含まれる任意の元 x_0 に対して、$x_0 \sim x \sim z \sim y$ で $x_0 \in I_y$ となり、逆に I_y に含まれる任意の元 y_0 に対して、$y_0 \sim y \sim z \sim x$ より $y_0 \in I_x$ が成り立ちます。よって $I_x = I_y$ が言えます。∎

この命題から自然に次の命題も導かれます。

命題 3.3.4 集合 X は、同値関係 $\sim$ により、お互いに共通部分を持たない同値類の集合 $\{I_{x_1}, I_{x_2}, \ldots, I_{x_s}\}$ で分割される。つまり、

$$X = \bigcup_{i=1}^{s} I_{x_i}, \qquad\qquad I_{x_i} \cap I_{x_j} = \emptyset \quad (i \neq j)$$

特に、集合 X の元の個数 $|X|$ は、$\displaystyle\sum_{i=1}^{s} |I_{x_i}|$ と等しい。

問 3.3.5 整数全体の集合 $\mathbb{Z}$ に対して、同値関係 $\sim$ を「$\forall x, y \in \mathbb{Z};\ x \sim y \iff x - y$ は *3* の倍数」とする。このとき同値類の代表系を求めよ。

定義 3.3.6 集合 X は、同値関係 $\sim$ により、お互いに共通部分を持たない同値類の集合 $\{I_{x_1}, I_{x_2}, \ldots, I_{x_s}\}$ が与えられたとき、集合 $\{x_1, x_2, \ldots, x_s\}$ をこの同値類の**代表系**と呼び、そこに含まれる元 x_i を同値類 I_{x_i} の**代表元**と呼びます。

剰余類の定義

それでは、群と部分群の話に戻りましょう。群 G と部分群 H が与えられたとき、次のようなして、集合 G の中に関係を定義することができます。

$$\forall x, y \in G; \qquad x \sim y \iff xy^{-1} \in H$$

命題 3.3.7 上で定義した関係は集合 G 上の同値関係となる。

証明 定義 3.3.1 の条件を 1 つづつ見ていきましょう。まず、命題 3.2.1 より $xx^{-1} = e \in H$ となり、条件 d1 が満たされます。また、$x \sim y$ と仮定すると、$xy^{-1} \in H$ となりますが、H は、部分群であることから、xy^{-1} の逆元 $(xy^{-1})^{-1} = yx^{-1}$ も H に含まれます。よって $y \sim x$ となり、条件 d2 も満たされます。条件 d3 も、$xz^{-1} = (xy^{-1})(yz^{-1}) \in H$ より満たされることが分かります。よってこの関係は同値関係となります。∎

それでは、いよいよ剰余類を定義しましょう。

定義 3.3.8 命題 *3.3.7* で部分群 H を使って定義した同値関係に対して、群 G の元 x の同値類を、 x についての**右剰余類**）（または、**剰余類**）と呼び、Hx と表すことにします。つまり

$$Hx = I_x = \{y \in G \,|\, y \sim x\} = \{y \in G \,|\, yx^{-1} \in H\}$$

また、 群 G の部分群 H に対する右剰余類全体の集合を、G/H で 表します。更に、G/H に含まれている元の個数を、H の G に対する、**指数**と呼び、$|G : H|$ と表します。

同値関係を、

$$\forall x, y \in G; \qquad x \sim y \Longleftrightarrow x^{-1}y \in H$$

に変えると、元 x の同値類は、 x についての**左剰余類**と呼ばれ、xH と表されます。

剰余類の例

例 3.1.2 の「パックマンの動きの群」を使って剰余類を実際に求めてみましょう。$G = \{e, x, x^2, y, xy, x^2y\}$, $H = \{e, x, x^2\}$ で、同値関係の計算を表にまとめると次のようになります。

元 x	元 y	xy^{-1}	同値？	元 x	元 y	xy^{-1}	同値？
e	x	x^2	◯	x	x^2y	x^2y	×
e	x^2	x	◯	x^2	y	x^2y	×
e	y	y	×	x^2	xy	xy	×
e	xy	x^2y	×	x^2	x^2y	y	×
e	x^2y	xy	×	y	xy	x^2	◯
x	x^2	x^2	◯	y	x^2y	x	◯
x	y	xy	×	xy	x^2y	x^2	◯
x	xy	y	×				

以上から、$e \sim x \sim x^2$, $y \sim xy \sim x^2y$ となっていることが分かりました。 よって剰余類は、$He = \{e, x, x^2\}$ と $Hy = \{y, xy, x^2y\}$ の 2 つです。（つまり $G/H = \{He, Hy\}$）また、代表系として $\{e, y\}$ を選ぶことができます。(ここでは、それぞれの元に対する全部で 6 つの剰余類が作れますが、$He = Hx = Hx^2$, $Hy = Hxy = Hx^2y$ より、実質的に 2 つしか剰余類がないことが分かります)

では、剰余類が持つ性質を少し見ていきましょう。

命題 3.3.9 群 G とその部分群 H そして、任意に与えた G の元 x, y に対して、

$$Hx = Hy \Longleftrightarrow x * y^{-1} \in H$$

証明 命題 3.3.3 より $Hx = Hy$ であるための必用十分条件は $x \sim y \Longleftrightarrow x * y^{-1} \in H$ となります。∎

命題 3.3.10 群 G とその部分群 H そして、任意に与えた G の元 x, y に対して、

$$y \in Hx \Longleftrightarrow \exists h \in H; y = h * x$$

特に、集合として、$Hx = \{h * x \mid h \in H\}$ が成り立つ。

証明 まず、右側が成り立つと仮定して、$y = h * x$ と表せると $y * x^{-1} = h \in H$ となります。よって $y \sim x$ より、$y \in Hx$ が成り立ちます。逆に左側が成り立つとすると $y \sim x$ より $y * x^{-1} \in H$ となり、$h = y * x^{-1} \in H$ と定義すると、$h \in H$ で、$y = x * h$ と表せます。∎

命題 3.3.10 より、$x \in G$ に対して、剰余類 Hx は、元 x に左から H の元を順にすべて掛けて得られる元の集合であることが分かります。特に単位元 e に対する剰余類 He と部分群 H は、集合として等しくなります。また、上の例もわざわざ全ての関係を計算しなくても、$Hx = \{e*x, x*x, x^2*x\} = \{x, x^2, e\}$, $Hy = \{e*y, x*y, x^2*y\} = \{y, x*y, x^2*y\}$ と求められます。

命題 3.3.11 群 G とその部分群 H そして、任意に与えた G の元 x に対して、剰余類 Hx に含まれる元の個数は部分群 H の位数に等しい。

証明 集合 H から集合 Hx への写像 f を次のように定義する。

$$\text{任意の } H \text{ の元 } h \text{ に対して } f(h) = h * x$$

命題 3.3.10 より、$f(h)$ は Hx に含まれます。また、命題 3.3.10 は Hx の任意の元 y が、$y = h*x = f(h)$ $(h \in H)$ と表せることを示しているので、写像 f は、全射となります。さらに、もし H の元 h_1, h_2 について $f(h_1) = f(h_2)$ ならば $h_1 = h_1 * x * x^{-1} = f(h_1)x^{-1} = f(h_2)x^{-1} = h_2 * x * x^{-1} = h_2$ より、$h_1 = h_2$ が得られるので、写像 f は、単射となります。よって写像 f は、集合 H から集合 Hx への全単射となり、H と Hx に含まれる元の個数は等しくなります。∎

それでは、この章のメイン定理を示しましょう。

定理 3.3.12 (*Lagrange*)

$$|G| = |G : H| \times |H|$$

証明 命題 3.3.4 より、$|G| = \sum_{Hx \in G/H} |Hx|$ となります。よって命題 3.3.11 から定理が証明されます。∎

この定理から、**部分群 H の位数は、群 G の位数の約数である**ことが言えます。これが、この章でもっとも言いたかったことです。パックマンの群 G の位数が 6 であることから、この群の部分群の位数は、1、2、3 または 6 の 4 つの可能性しかないことが分かります。実際、この群 G の部分群として、$\{e\}$, $\{e, y\}$, $\{e, x, x^2\}$, G が見つかります。(G 自身も G の部分群なんですよ！)

もう 1 つ新しい群の例を紹介します。その前に、足し算と掛け算を持つ最も小さい集合 F_2 を定義します。F_2 は、集合としては、$\{0, 1\}$ と成ります。ただしこの集合には、次のような足し算と掛け算が定義されていて、代数構造として**体**と呼ばれるものになっています。$0+0 = 1+1 = 0, 1+0 = 0+1 = 1, 0\times 0 = 1\times 0 = 0\times 1 = 0, 1\times 1 = 1$ さて、この F_2 を成分とする 6 次元ベクトル空間を ${F_2}^6 := \{v = (v_1, v_2, \ldots, v_6) \mid v_i \in F_2\}$ を考えます。${F_2}^6$ の 2 つのベクトル $v = (v_1, v_2, \ldots, v_6)$, $w = (w_1, w_2, \ldots, w_6)$ について足し算 $v+w = (v_1+w_1, v_2+w_2, \ldots, v_6+w_6)$ と定義して、足し算についての群が定義できます。つぎに、${F_2}^6$ の 3 つのベクトルを $a = (1, 0, 0, 1, 1, 1)$, $b = (0, 1, 0, 1, 1, 0)$, $c = (0, 0, 1, 1, 0, 1)$ と決めます。そして、この 3 つのベクトルで生成される ${F_2}^6$ の部分群 $H = \langle a, b, c\rangle$ が定義できます。H の元を全て並べると、$v + v = 0$ に気がつけば、$H = \{0, a, b, c, a + b, a + c, b + c, a + b + c\}$ となり、部分群 H の位数は 8 となります。群 ${F_2}^6$ の位数は $2^6 = 64$ なので、定理 3.3.12 より、H の剰余類の個数 $|G : H|$ は、$64/8 = 8$ となります。

問 3.3.13 ${F_2}^6$ が群となることを確かめよ。

3.4　章末問題

問題 3.1 5 次元実ベクトル空間 $\mathbb{R}^5$ の部分集合 $W := \{(v_1, v_2, v_3, v_4, v_5) \mid v_1 - v_2 + v_3 - v_4 + v_5 = 0\}$ がベクトルの足し算を二項演算として $\mathbb{R}^5$ の部分群となることを示せ。

問題 3.2 「おもちゃの自動車の動きからなる群」(位数 6 の巡回群) $G = \{e, x, x^2, x^3, x^4, x^5\}$ の部分群をすべて求めよ。

問題 3.3 「3 人でやるあみだくじの群」の部分群をすべて求めよ。

問題 3.4 二項演算 $*$ を $x * y = (x \times y)\ mod\ 9$ としたとき、この二項演算を使った巡回群 $\langle 2\rangle$ の元をすべて求めよ。

問題 3.5 二項演算 $*$ を $x * y = (x \times y)\ mod\ 8$ としたとき、この二項演算を使って 3 と 5 で生成される群 $\langle 3, 5\rangle$ の元をすべて求めよ。

問題 3.6 巡回群 $G := \{e, x, x^2, x^3, \ldots, x^{11}\}$ つまり $x^{12} = e$ に対して部分群 $H_i := \langle x^i\rangle$ $(i = 1, \ldots, 12)$ として、それぞれの群の間にある包含関係を求めなさい。

問題 3.7 位数 288 の巡回群 $G := \{e, x, x^2, \ldots, x^{287}\}$ に対して、部分群 $H_1 := \langle x^{105}\rangle$, $H_2 := \langle x^{114}\rangle$, $H_3 := \langle x^{117}\rangle$, $H_4 := \langle x^{126}\rangle$ の間の包含関係を求めよ。

問題 3.8 「正 8 角形に対する動きの群」$G = \{e, x, x^2, x^3, x^4, x^5, x^6, x^7, y, x*y, x^2*y, x^3*y, x^4*y, x^5*y, x^6*y, x^7*y\}$ で、2 つ以下の生成元で作られる部分群をすべて求めよ。

問題 3.9 集合 $X := \{1, 2, 3, 4, 5, 6\}$ 上ので定義された次の関係 $\sim$ が、同値関係となるか関係を表にまとめて調べよ。また、同値関係と成るものについては、同値類となる集合を求めよ。

(a) $x \sim y \Leftrightarrow (x + y)\ mod\ 3 = 0$

(b) $x \sim y \Leftrightarrow (x - y)\ mod\ 3 = 0$

(c) $x \sim y \Leftrightarrow (x + y)\ mod\ 3 = 0$ 又は $(x - y)\ mod\ 3 = 0$

問題 3.10 「パックマンの動きの群」G に対して、部分群 $H := \{e, y\}$ とする。このとき、H のすべての右剰余類を元のリストとして書け。

問題 3.11 集合 $\mathbb{Z}_{27}^{\times} = \{1,2,4,5,7,8,10,11,13,14,16,17,19,20,22,23,25,26\}$ に二項演算を $x * y = (x \times y) \mod 27$ で定義すると、$\mathbb{Z}_{27}^{\times}$ は群になる。部分群 $H := \langle 10 \rangle$ とするとき、H のすべての右剰余類を元のリストとして書け。

問題 3.12 「正 *8* 角形の動きの群」$G := \langle x, y \rangle$ に対して、部分群 $H := \left\langle x^2 \right\rangle$ とするとき、H のすべての右剰余類を元のリストとして書け。

問題 3.13 集合 $\mathbb{Z}_{72}^{\times} = \{1,5,7,11,13,17,19,23,25,29,31,35,37,41,43,47,49,53,55,59,61,65,67,71\}$ に二項演算を $x * y = (x \times y) \mod 72$ で定義すると、$\mathbb{Z}_{72}^{\times}$ は、群になる。H を $\mathbb{Z}_{72}^{\times}$ の部分群 $H = \{1, 17, 55, 71\}$ で生成される部分群とするとき、H の右剰余類のなかで、*19* を含むものを求めよ。

問題 3.14 群 G とその部分群 H, K が与えられたとき、G 上の関係 $\sim$ を $x \sim y \Leftrightarrow \exists h \in H,\ \exists k \in K;\ x = h * y * k$ によって定義するとき、$\sim$ は、同値関係であることを示せ。

問題 3.15 問題 *3.14* で定義された関係 $\sim$ に対して、$x \in G$ が属する同値類 $I_x = \{y \in G | y \sim x\}$ が $HxK := \{h * x * k \mid h \in H,\ k \in K\}$ であることを示せ。

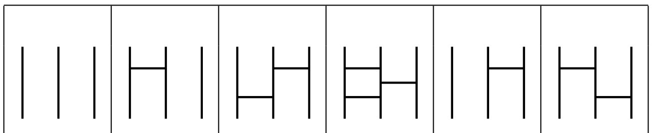
問題 3.16 群 G の *2* つの部分群 H_1, H_2 に対して、H_1 と H_2 の位数が互いに素なら、部分群 $H_1 \cap H_2 = \{e\}$ となることを証明せよ。

3.5 章末問題の解答

解答 3.1 ベクトル $w := (w_1, w_2, w_3, w_4, w_5),\ u := (u_1, u_2, u_3, u_4, u_5)$ が W の元であるとすると、等式 $w_1 - w_2 + w_3 - w_4 + w_5 = 0,\ u_1 - u_2 + u_3 - u_4 + u_5 = 0$ が成り立ちます。よって ベクトル $v = (v_1, v_2, v_3, v_4, v_5) = w + u$ について、$v_i = w_i + u_i$ なので、$v_1 - v_2 + v_3 - v_4 + v_5 = (w_1 + u_1) - (w_2 + u_2) + (w_3 + u_3) - (w_4 + u_4) + (w_5 + u_5) = 0$ となり、部分群となるための条件 *s1* が成り立ちます。また、W の元 v に対してその逆元 $-v$ が W に含まれることが $(-v_1) - (-v_2) + (-v_3) - (-v_4) + (-v_5) = 0$ から分かりますので、条件 *s2* も成り立ち、W は部分群となります。

解答 3.2 $G = \langle x \rangle$ で、巡回群の部分群がすべて巡回群であることより、G の部分群は、$\left\langle x^i \right\rangle$ の形になります。ここで、$\left\langle x^1 \right\rangle = \left\langle x^5 \right\rangle = G,\ \left\langle x^2 \right\rangle = \left\langle x^4 \right\rangle = \{e, x^2, x^4\},\ \left\langle x^3 \right\rangle = \{e, x^3\}$ からこの 3 つですべての部分群となります。

解答 3.3 「3 人でやるあみだくじの群」G に次の様に名前をつけます。



e	a	b*a	a*b*a	b	a*b

名前のつけ方から $a * a = e,\ b * b = e,\ a * b * a * b * a * b = e$ などが、分かります。命題 *3.3.12* より、部分群の元の数は、*6* の約数となります。よって、真部分群の位数は *1,2,3* のいずれかとなります。*1* は自明な群 $\{e\}$ ですね。*2* となるのは、単位元 e ともう *1* つ別の元 x があるということになります。このとき、$x * x$ は e または、x となるはずですが、$x * x = x$ だと $x = e$ となり最初の x の設定と矛盾します。よって $x * x = e$ となり x は、a, b, $a * b * a$ のどれかということになります。つまり位数が *2* の部分群は、$\{e, a\},\ \{e, b\},\ \{e, a * b * a\}$ です。最後に位数が *3* の部分群ですが、3 つの元を $\{e, x, y\}$ としましょう。このとき、$x * y$ は、$e,\ x,\ y$ のいずれかとなりますが、$x * y = x$ や $x * y = y$ だと、$y = e$ や $x = e$ が出て最初の設定と矛盾します。よって $x * y = e$ となり x の逆元が y となります。次に、$x * x$ がどうなるか考えましょう。もし、$x * x = e$ だと x の逆元が x となってしまいますが、最初の設定から $x \neq y$ で、y が x の逆元であることから、$x * x \neq e$ となります。もし、$x * x = x$ だと $x = e$ となり、やっぱり最初の設定と矛盾しますので、$x * x = y$ が得られます。よって、$G = \{e, x, x^2\}$ と言うことになり、この場合の x は、$a * b$ または、$b * a$ となりますが、$\langle a * b \rangle = \langle b * a \rangle = \{e, a * b, b * a\}$ よりこの群が唯一の位数 3 の部分群となります。これですべての部分群が求まりました。

解答 3.4 巡回群 $\langle x\rangle$ は、命題 *3.2.8* より、集合として、$\{e, x, x^2, \cdots, x^{n-1}\}$ と表せるので、$\langle 2\rangle$ は、$\{1, 2, 2^2, \cdots\}$ となっていくはずです。$2*2=4,\ 2^3=8,\ 2^4=7,\ 2^5=5,\ 2^6=1$ より、$\langle 2\rangle=\{1,2,4,8,7,5\}$ となります。

解答 3.5 $3*3=1,\ 5*5=1,\ 3*5=7,\ 3*7=5,\ 5*7=3,\ 7*7=1$ から、集合 $G:=\{1,3,5,7\}$ は問題の二項演算で閉じています。また、それぞれの元は自分自身を逆元として持ちます。もちろん単位元 *1* が存在し、結合律も満たしているので、G は、*3,5* を含む最小の群となります。つまり $\langle 3,5\rangle=\{1,3,5,7\}$

解答 3.6 $H_1=H_5=H_7=H_{11}=G,\ H_2=H_{10}=\{e,x^2,x^4,x^6,x^8,x^{10}\},\ H_3=H_9=\{e,x^3,x^6,x^9\},\ H_4=H_8=\{e,x^4,x^8\},\ H_6=\{e,x^6\}$ 包含関係は、ここから明らかですね。

解答 3.7 問題 *3.6* をじっくり見ると、巡回群 $G=\langle x\rangle$ の位数が n のとき、n 以下の自然数 m に対して、d を n と m の最大公約数 $Gcd(n,m)$ とすると、部分群 $\langle x^m\rangle=\langle x^d\rangle$ で、さらに $\langle x^m\rangle$ の位数が n/d になっていることが分かります。このことを利用すると、$Gcd(288,105)=3,\ Gcd(288,144)=6,\ Gcd(288,117)=9,\ Gcd(288,126)=18$ から、$H_1=\langle x^3\rangle,\ H_2=\langle x^6\rangle,\ H_3=\langle x^9\rangle,\ H_4=\langle x^{18}\rangle$ となります。よってこれらの部分群の間の包含関係は、$H_4\subset H_2\subset H_1,\ H_4\subset H_3\subset H_1$ となります。

解答 3.8 生成元をとしてある元 a を選ぶと、そこから生成された群は、a^i を必ず含みますから、a と a^i を同時に生成元にする必要はありません。群 G の位数が *16* なので、真部分群の位数は、*1,2,4,8* となります。いろいろ試せば次の様な群が出てきます。位数が 4 以上の群については、生成元に下線を引きます。位数 *2* の群は、$\{e,x^4\},\ \{e,y\},\ \{e,x*y\},\ \{e,x^2*y\},\ \{e,x^3*y\},\ \{e,x^4*y\},\ \{e,x^5*y\},\ \{e,x^6*y\},\ \{e,x^7*y\}$。位数 *4* の群は、$\{e,\underline{x^2},x^4,x^6\},\ \{e,\underline{x^4},\underline{y},x^4*y\},\ \{e,\underline{x^4},\underline{x*y},x^5*y\},\ \{e,\underline{x^4},\underline{x^2*y},x^6*y\},\ \{e,\underline{x^4},\underline{x^3*y},x^7*y\}$。位数 *8* の群は、$\{e,\underline{x},x^2,x^3,x^4,x^5,x^6,x^7\},\ \{e,\underline{x^2},x^4,x^6,\underline{y},x^2*y,x^4*y,x^6*y\},\ \{e,\underline{x^2},x^4,x^6,\underline{x*y},x^3*y,x^5*y,x^7*y\}$

解答 3.9 *(a)* は、 $1\not\sim 1$ *(*つまり $1+1\ mod\ 3\neq 0$ より同値関係となるための条件 *d1* が成り立たないので、同値関係になりません。*(b), (c)* は、同値関係です。同値類は、*(b)* では、$\{1,4\},\ \{2,5\},\ \{3,6\}$、*(c)* では、$\{1,2,4,5\}$, $\{3,6\}$ となります。

解答 3.10 $He=H=\{e,y\},\ Hx=\{x,x*y\},\ Hx^2=\{x^2,x^2*y\}$

解答 3.11 $H=\langle 10\rangle=\{1,10,19\}$ より、$H*1=H*10=H*19=H,\ H*2=H*11=H*20=\{2,11,20\}$, $H*4=H*13=H*22=\{4,13,22\},\ H*5=H*14=H*23=\{5,14,23\},\ H*7=H*16=H*25=\{7,16,25\}$, $H*8=H*17=H*26=\{8,17,26\}$

解答 3.12 $H=\{e,x^2,x^4,x^6\}$ なので、$Hx=\{x,x^3,x^5,x^7\},\ Hy=\{y,x^2y,x^4y,x^6y\},\ Hxy=\{xy,x^3y,x^5y,x^7y\}$ となります。

解答 3.13 $H*19=\{19,35,37,53\}$

解答 3.14 同値関係となるための *3* つの条件を確認します。まず、部分群 H, K 共に命題 *3.2.1* より、G の単位元 e を含んでいます。よって、$\forall x\in G;\ x=e*x*e$ より $x\sim x$ となり条件 *d1* が成り立ちます。次に $x\sim y$ と仮定すると、$\exists h\in H,\ \exists k\in K$ で $x=h*y*k$ よって、等式の両辺に右から k^{-1}, 左から h^{-1} を掛けると、$h^{-1}*x*k^{-1}$ となります。ここで、部分群の条件 *s2* より、$h^{-1}\in H$ と $k^{-1}\in K$ が成り立つので、$y\sim x$ が言えます。最後に $x\sim y,\ y\sim z$ と仮定すると、$x=h_1*y*k_1,\ y=h_2*z*k_2$ となる $h_1,h_2\in H,\ k_1,k_2\in K$ が存在します。よって $x=h_1*y*k_2=h_1*(h_2*z*k_2)*k_2=(h_1*h_2)*z*(k_2*k_1)$ で、部分群の条件 *s1* より $h_1*h_2\in H,\ k_2*k_1\in K$ が成り立つので、$x\sim z$ となり、これで、*3* つの条件をすべて確認できました。

解答 3.15 同値関係の定義から $\{y\in G|y\sim x\}=\{y\in G\,|\,\exists h\in H,\exists k\in K, y=h{*}x{*}k\}=\{h{*}x{*}k\,|\,h\in H,k\in K\}$

解答 3.16 命題 *3.3.12* より、$H_1\cap H_2$ の位数は、H_1 と H_2 のそれぞれの位数の約数となります。ところが H_1 と H_2 の位数が互いに素となるため、$H_1\cap H_2$ の位数は、*1* 以外にありません。命題 *3.2.1* より、単位元は、必ず含まれるので、$H_1\cap H_2=\{e\}$ となります。

Time-stamp: <05/12/06 14:08:40 waki>

第4章　作用と固定化

あるものを調べるときにそのもの自身を調べる以外に、そのものが他に与えている影響から、そのものを調べることがあります。例えば、私たちは体内の風邪のウィルスを見ることはできませんが、ウィルスによる「**作用**」で体内に起こされている発熱、頭痛、咳きなどの反応から、体内に風邪のウイルスが存在することを知ります。この章では、群の元が別の集合に起こす「作用」を見つめることにより、群自身の性質を見つけ出す。つまり

$$\boxed{\text{作用を通して群を見つめる}}$$

ことを学びます。

4.1　作用

この章では、作用される集合 X と作用する群 G の間の関係を調べるため、「作用」というものをもっときちんと考えてみます。では、作用をきちんと定義してみましょう。

定義 4.1.1 集合 X と集合 G が与えられたとします。G の元 a を集合 X から X への全単射写像と見ることができるとき、a は、集合 X に**作用している**と呼びます。また、集合 X の元 i についてこの全単射写像による i の像を i^a と表すことにします。

さらに、集合 G が群となるときには、さらに次の様な条件を付けます。

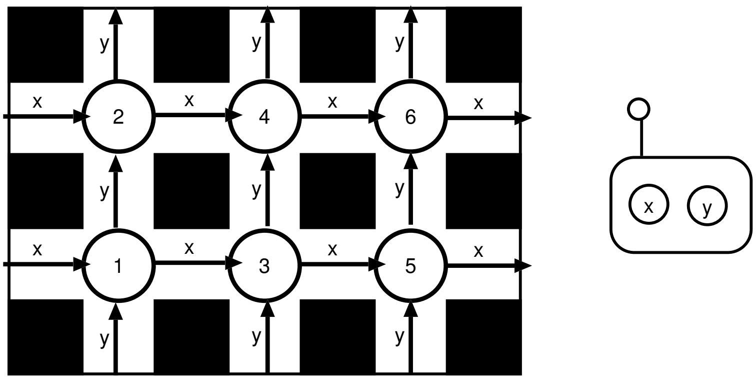
定義 4.1.2 集合 X と群 G が与えられて、次の条件が成り立つとき、群 G は集合 X に **作用している** と呼びます。このとき集合 X を**作用域**と呼びます。

a1. G の任意の元 a は、集合 X に作用している。

a2. $\forall a, b \in G; \forall i \in X; i^{(a*b)} = (i^a)^b$

a3. G の単位元 e について、$\forall i \in X; i^e = i$

例えば、パックマンの動きの群に対して、次の様にパックマンのいる位置に番号を付けます。



このとき、集合 X をパックマンのいる位置全体の集合つまり $\{1, 2, \ldots, 6\}$ として、ボタン x による X の作用を見ると、$1^x = 3, 3^x = 5, 5^x = 1, 2^x = 4, 4^x = 6, 6^x = 2$ となります。置換として x を表現すると $x = (1, 3, 5)(2, 4, 6)$ と表すこともできます。

定義 4.1.3 集合 X を作用域として持つ群 G が与えられたとき、X の元 i について、$\mathcal{O}_G(i) := \{i^a \mid a \in G\}$ を群 G による i の**軌跡**と呼びます。特に、集合 $\{\mathcal{O}_G(i)_\sigma \mid i \in X\}$ を群 G の**軌跡の集合**と呼び、$\mathcal{O}_G(X)$ と表すことにます。

パックマンの群では、G による 1 の軌跡は、$\mathcal{O}_G(1) = \{1, 2, 3, 4, 5, 6\}$ と全部になってしまいます。またパックマンの群の部分群 $H := \{e, x, x^2\}$ について軌跡を求めれば、 $\mathcal{O}_H(1) = \{1, 3, 5\}, \mathcal{O}_H(2) = \{2, 4, 6\}$ と 2 つの軌跡があることが分かります。

定義 4.1.4 集合 X を作用域として持つ群 G が与えられたとき、群 G がただ *1* つの軌跡を持つとき、つまり $\mathcal{O}_G = \{X\}$ のとき群 G は集合 X に**可移**に作用していると呼びます。

命題 4.1.5 集合 X を作用域として持つ群 G が与えられたとき、集合 X の元 i, j に対して次の様に関係 $\sim$ を定義すると $\sim$ は、X 上の同値関係となる。

$$i \sim j \Leftrightarrow \exists a \in G;\ j^a = i$$

証明 定義 3.3.1 の 3 つの条件を順に確認していく。定義 4.1.2 より、任意の X の元 x に対して群 G の単位元 e は、$i^e = i$ となるので、$i \sim i$ が成り立ちます。また、$i \sim j$ であると仮定すると $\exists a \in G;\ i^a = j$ ですが、群の定義から、G は、$a * a^{-1} = e$ となる逆元 a^{-1} を含みます。このとき、$j^{a^{-1}} = (i^a)^{a^{-1}} = i^{(a*a^{-1})} = i^e = i$ となり、$j \sim i$ であることも言えます。最後に $i \sim j,\ j \sim k$ と仮定して $\exists a, b \in G;\ i^a = j,\ j^b = k$ ならば、またまた群の定義より、$a * b \in G$ となり $i^{(a*b)} = k$ より $i \sim k$ が成り立ちます。∎

4.2　置換の多項式への作用

n 個の変数 $x_1, \ldots, x_n$ を持つ、整数を係数とする多項式の集合を、$\mathcal{F}(x_1, \ldots, x_n)$ で表すことにします。$\mathcal{F}(x_1, \ldots, x_n)$ に含まれる多項式 $f(x_1, \ldots, x_n)$ に対する n 次の置換 σ の作用 (つまり多項式を別の多項式に変える動き) を次のように、定義します。

$$f(x_1, \ldots, x_n)^\sigma = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$$

例えば、 $n = 3$ で、$f(x_1, x_2, x_3) = x_1x_2 + x_3^2$ とします。$\sigma = (1, 2, 3)$ なら、$f(x_1, x_2, x_3)^\sigma = x_{\sigma(1)}x_{\sigma(2)} + x_{\sigma(3)}^2 = x_2x_3 + x_1^2$ となります。ここで $\mathcal{F}(x_1, \ldots, x_n)$ に含まれる特別な多項式 Δ_n を定義します。

定義 4.2.1 自然数 n に対して $\mathcal{F}(x_1, \ldots, x_n)$ に含まれる多項式 Δ_n を次のように決める。

$$\Delta_n = \prod_{1 \leqq i < j \leqq n} (x_i - x_j)$$

この多項式 Δ_n を n 次の**差積**と呼びます。

例えば、 $\Delta_3 = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$ となります。
この差積 Δ_n は、次の命題で示す特徴を持っています。

命題 4.2.2 任意の互換 (i, j) $(1 \leqq i < j \leqq n)$ に対して、$\Delta_n^{(i,j)} = -\Delta_n$

証明 Δ_n の中で、互換 (i, j) によって変わる変数は x_i と x_j だけです。特にそこで、x_i, x_j が関わっている因子を選び出すと、$\mathcal{I}_1(k) = (x_k - x_i)(x_k - x_j)$ $(1 \leqq k < i)$, $\mathcal{I}_2(l) = (x_i - x_l)(x_l - x_j)$ $(i < l < j)$, $\mathcal{I}_3(k) = (x_i - x_m)(x_j - x_m)$ $(j < m \leqq n)$, そして $(x_i - x_j)$ となります。$\mathcal{I}_1(k)^{(i,j)} = \mathcal{I}_1(k)$, $\mathcal{I}_2(l)^{(i,j)} = \mathcal{I}_2(l)$, $\mathcal{I}_3(m)^{(i,j)} = \mathcal{I}_3(m)$ となるのがすぐにわかります。よってただ 1 つの因子 $(x_i - x_j)$ 以外のすべての因子を掛けたものは、互換 (i, j) の作用で変化しないことが分かります。そして、因子 $(x_i - x_j)^{(i,j)}$ は $(x_j - x_i) = -(x_i - x_j)$ となり、全体で考えると Δ_n に互換 (i, j) を作用させると、$-\Delta_n$ に変わることが分かります。∎

定義 4.2.3 n 次の置換 σ を差積 Δ_n に作用させる。このとき、$\Delta_n^\sigma = \Delta_n$ となる σ を**偶置換**と呼び、$\Delta_n^\sigma = -\Delta_n$ となる σ を**奇置換**と呼びます。

命題 4.2.4 偶置換は、偶数個の互換の積で表せ、奇置換は、奇数個の互換の積で表せる。

証明命題 2.2.1 から置換は必ず互換の積で表されます。よってこの命題は、命題 4.2.2 より証明できます。∎

偶置換と奇置換の例

$n=3$ とすると、$\Delta_3=(x_1-x_2)(x_1-x_3)(x_2-x_3)$ となります。$\Delta_3^e=\Delta_3^{(1,2,3)}=\Delta_3^{(1,3,2)}=\Delta_3$ より、e, $(1,2,3)$, $(1,3,2)$ は、偶置換となります。$\Delta_3^{(1,2)}=\Delta_3^{(1,3)}=\Delta_3^{(2,3)}=-\Delta_3$ より、$(1,2)$, $(1,3)$, $(2,3)$ は、奇置換となります。あみだとの対応をみるとあみだの横棒の数が偶数のとき偶置換、奇数のとき奇置換になっていることが分かります。もちろんこれは、偶然ではありません。

問 4.2.5 次の置換が偶置換か奇置換か調べよ。$(1,2,3,4)$, $(1,2,3,4,5)$, $(1,2,3,4,5,6)$, $\sigma_1*\sigma_2$, $\sigma_1*\rho_1$, $\rho_1*\sigma_1$, $\rho_1*\rho_2$ ただし σ_1, σ_2 は偶置換、ρ_1, ρ_2 は奇置換とする。

4.3 固定化

群 G が集合 X に作用させているとき、その作用を調べる上でもっとも大事な作用は、実は「まったく動かない」作用となります。武道の世界では、「静」と「動」を表裏一体のものと捕らえますが、動きを捕らえるときにもっとも注目しなければならないものが、動かない所というのは、何だか武道の奥義のような気がしませんか？ここでは、まず固定化という言葉を持ち込みます。

命題 4.3.1 群 G が集合 X に作用させているとき、集合 X の部分集合 Y に対して、

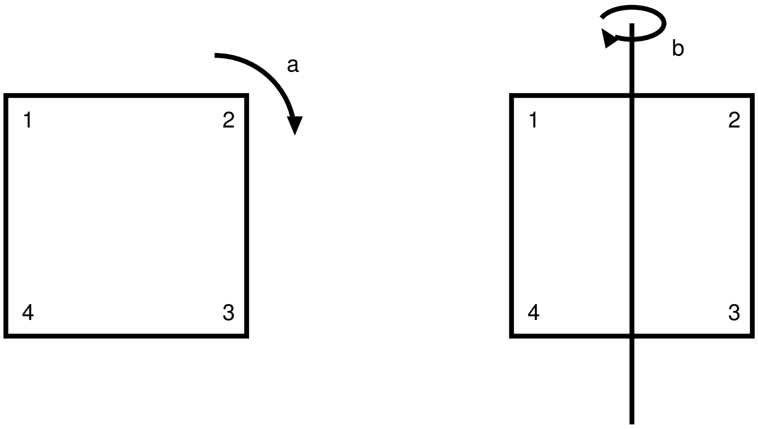
$$S_G(Y):=\{x\in G\,|\,\forall i\in Y,\, i^x=i\}$$

とすると、集合 $S_G(Y)$ は、G の部分群となる。

証明 定義 3.1.1 の 2 つの条件を $S_G(Y)$ が満たすことを示します。$x,y\in S_G(Y)$ とすると、$S_G(Y)$ の定義から $\forall i\in Y; i^x=i^y=i$ よって $i^{(x*y)}=(i^x)^y=i^y=i$ よって、$x*y\in S_G(Y)$ が成り立ちます。また、x の逆元 x^{-1} に対して、$i^{x^{-1}}=(i^x)^{x^{-1}}=i^{(x*x^{-1})}=i^e=i$ となり、$x^{-1}\in G$ を成り立つ。∎

定義 4.3.2 上の命題で定義された部分群 $S_G(Y)$ を G の Y に対する**固定部分群**と呼びます。特に、集合 Y に１つの元 i しか含まれていないとき、つまり $Y=\{i\}$ ならこの群を $S_G(i)$ と表し、**一点固定部分群**と呼びます。

それでは、次に示す群を使って固定部分群を求めてみましょう。



この群は、正方形を動かしている群です。基本的な動きは、正方形に対する時計回りの 90 度回転の動き a と裏返す動き b の 2 つで、この 2 つの動きのの組合わせでできる動き全体の集合を G としますと、$G=\{e,a,a^2,a^3,b,a*b,a^2*b,a^3*b\}$ の 8 つの動きからなる位数 8 の群が出来上がります。正方形の 4 つの頂点に番号を付けて、頂点の集合 $X=\{1,2,3,4\}$ とします。すると動きによる頂点の移動から頂点の集合 X に対する群 G の作用が生まれます。具体的に置換で表すと $a=(1,2,3,4)$ で $b=(1,2)(3,4)$ となります。では、集合 Y をいろいろ選んだときの固定化部分群 $S_Y(G)$ を求めてみましょう。

$$\begin{aligned}
Y=\{1,3\} &\implies S_G(Y)=\{e,a*b\}\\
Y=\{2,4\} &\implies S_G(Y)=\{e,a^3*b\}\\
Y=\{1,2\} &\implies S_G(Y)=\{e\}\\
Y=\{1\} &\implies S_G(Y)=\{e,a^3*b\}
\end{aligned}$$

次の命題で、固定部分群 $S_G(Y)$ の剰余類が持つ性質を紹介します。

命題 4.3.3 群 G が集合 X に作用させているとき、集合 X の部分集合 Y に対して、部分群 $H := S_G(Y)$ とします。このとき H の右剰余類 $Ha,\ Hb$ について

$$Ha = Hb \Longleftrightarrow \forall i \in Y;\ i^a = i^b$$

が成り立ちます。

証明命題 3.3.9 より、$Ha = Hb$ となるための必用十分条件は $a * b^{-1} \in H = S_G(Y)$ です。よって任意の Y の元 i に対して $i^{(a*b^{-1})} = i$ となります。この両辺に b を作用させると、$i^b = \left(i^{(a*b^{-1})}\right)^b = i^{(a*b^{-1}*b)} = i^a$ となります。逆に、$i^a = i^b$ なら同様に $i^{a*b^{-1}} = i$ となることが分かりますから、$a * b^{-1} \in H$ が言えます。∎

命題 4.3.4 群 G が集合 X に作用させているとき、$i \in X$ に対して $H = S_G(i)$ とする。このとき、$\mathcal{O}_G(i)$ の元の個数は、H における G の右剰余類の個数に等しい。

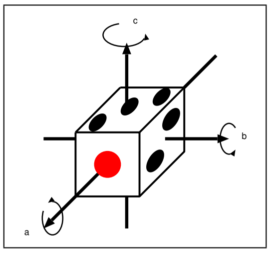
証明 $\mathcal{O}_G(i)$ の元の個数を n として、$\mathcal{O}_G(i) = \{i_1, i_2, \cdots, i_n\}$ $(i_1 = i)$ と決めておきます。このとき各 i_k に対して $\exists a_k \in G\ i^{a_k} = i_k$ となります。命題 4.3.3 より、右剰余類 $Ha_1, Ha_2, \cdots, Ha_n$ は、すべて相異なります。もし、この n 個の右剰余類以外に別の剰余類 Hb が存在すると、その代表元 b による i への作用 i^b は、命題 4.3.3 より $\{i_1, i_2, \cdots, i_n\}$ のどれとも異なることになります。これは、$\mathcal{O}_G(i) = \{i_1, i_2, \cdots, i_n\}$ としたことに矛盾しますので、$Ha_1, Ha_2, \cdots, Ha_n$ は、すべての右剰余類の集合となります。∎

命題 4.3.5 n 次の偶置換全体は、n 次の対称群 $\mathcal{S}_n$ の指数 *2* の部分群となる。この部分群を、**交代群**と呼び、$\mathcal{A}_n$ と書き表します。

証明 G を n 次の対称群 $\mathcal{S}_n$ として、$X = \{\Delta_n, -\Delta_n\},\ i = \Delta_n \in X$ とすれば、一点固定部分群 $S_G(i) = \mathcal{A}_n$ となり、命題 4.3.1、 命題 4.3.4 より、$\mathcal{A}_n$ は、指数 $2 = |X| = |\mathcal{O}_G(i)|$ の $\mathcal{S}_n$ の部分群となる。∎

4.4　章末問題

問題 4.1 サイコロを３次元座標の中心に置き、「6」から「1」に向かう方向を x 軸、「5」から「2」に行く方向を y 軸、そして「4」から「3」に行く方向を z 軸とする。 x 軸に対する 90 度回転を a, y 軸に対する 90 度回転を b、z 軸に対する 90 度回転を c とするとき、



$a,\ b,\ c$ の作用をサイコロの数字への置換として表せ。

問題 4.2 問題 4.1 の元 $a,\ b,\ c$ で生成される 群 $\langle a,b,c\rangle$ の元の内サイコロの数字「2」と「5」を入れ換える動きを、すべて求め、$a,\ b,\ c$ の積で表せ。

問題 4.3 問題 4.1 のサイコロの 1 辺の長さを 2 とすると、さいころの各頂点の座標は、$p_1 = (1,1,1)$, $p_2 = (1,1,-1)$, $p_3 = (1,-1,-1)$, $p_4 = (1,-1,1)$, $p_5 = (-1,1,1)$, $p_6 = (-1,1,-1)$, $p_7 = (-1,-1,-1)$, $p_8 = (-1,-1,1)$ この８つの点に対する $a,\ b,\ c$ の作用を置換の形で表せ。

問題 4.4 群 $\langle a,b,c\rangle$ の元で、頂点 p_1 を動かさない動きをすべて求め、この集合が群となることを示せ。

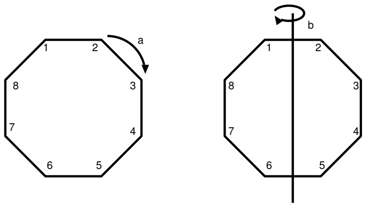
問題 4.5 問題 4.4 の群を H としたとき、H による 1 の軌跡と H による 4 の軌跡を求めよ。

問題 4.6 $f(x_1,x_2,x_3,x_4) = (x_1 - x_2)(x_3 - x_4)$ としたとき、4 次の対称群の元 σ で、$f^{\sigma}(x_1,x_2,x_3,x_4) = f(x_1,x_2,x_3,x_4)$ となるものをすべて求めよ。

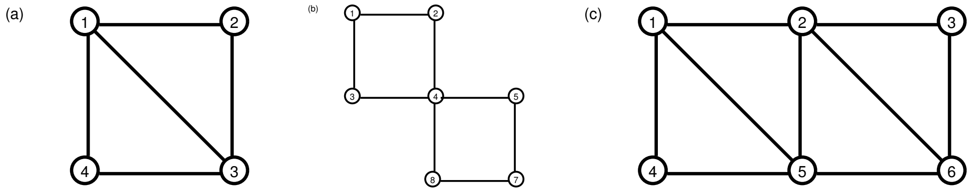
問題 4.7 $f(x_1,x_2,x_3,x_4) = x_1x_2 + x_2x_3 + x_3x_4 + x_4x_1$ としたとき、4 次の対称群の元 σ で、$f^{\sigma}(x_1,x_2,x_3,x_4) = f(x_1,x_2,x_3,x_4)$ となるものをすべて求めよ。

問題 4.8 $G := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, a,b,c,d \in \mathbb{R},\ ad - bc \neq 0 \right\}$、二項演算は行列のかけ算、集合 X は、$\mathbb{R}$ 上の 2 次元縦ベクトル全体とする。行列 $M \in G$ とベクトル $v \in X$ に対して作用 $M(x) := M * x$ (行列とベクトルの積) で決める。このとき、集合 G と集合 X の組合わせで、G が X を作用域として持つ群になっているか？

問題 4.9 正８角形に下の図のように番号をふり、正８角形に対する作用を考える。作用 $a,\ b$ で生成される群 G に対して点１を固定する 1 点固定部分群 $S_G(1)$ の元をすべて求めよ。



問題 4.10 次の番号のついたグラフを X として、このグラフに作用する群 G (回転させたり、裏返したりして頂点の位置は変わるがグラフ全体では同じに見える変換) を求めよ。



問題 4.11 ４次の対称群 $\mathcal{S}_4$ は、４変数多項式全体の集合に作用していると考えることができる。$f_1(x_1,x_2,x_3,x_4) = x_1x_2 + x_2x_3 + x_3x_4 + x_4x_1$ の軌跡を求めよ。

問題 4.12 $f_2(x_1,x_2,x_3,x_4) = (x_1 + x_2)(x_3 + x_4)$ として問題 4.11 の f_1 と合わせて、$Y := \{f_1, f_2\}$ とする。このとき $S_{\mathcal{S}_4}(Y)$ を求めよ。

4.5　章末問題の解答

解答 4.1 $a = (2,3,5,4)$, $b = (1,4,6,3)$, $c = (1,2,6,5)$

解答 4.2 $\{a^2, a^2 * b, a^2 * b^2, a^2 * b^3\}$

解答 4.3 $a = (1,4,3,2)(5,8,7,6)$, $b = (1,2,6,5)(3,7,8,4)$, $c = (1,5,8,4)(2,6,7,3)$

解答 4.4 $ac = (2,5,4)(3,6,8)$ が p_1 を固定する、サイコロの動きより、p_1 を固定する集合のは、$\{e, ac, (ac)^2\}$ となる ac は、位数 *3* の元なので、この集合は群となるための *4* つの条件を満たし、位数 *3* の巡回群になっている。

解答 4.5 $\mathcal{O}_H(1) = \{1,2,3\}$, $\mathcal{O}_H(4) = \{4,5,6\}$

解答 4.6 $\{e,\ (1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3)\}$

解答 4.7 $f(x_1,x_2,x_3,x_4) = x_1x_2 + x_2x_3 + x_3x_4 + x_4x_1 = (x_1+x_3)(x_2+x_4)$ より、$\langle(1,3),\ (1,2,3,4)\rangle = \{e, (1,2,3,4), (1,3)(2,4), (1,4,3,2), (1,3), (1,4)(2,3), (2,4), (1,2)(3,4)\}$

解答 4.8 G の元 M は、行列式の値 $(ad - bc)$ が *0* でないため逆行列を持ちます。よって、M による X から X への写像は全単射になります。（自分で確認しま しょう）よって、M は X に作用することになります。しかし、一般に $M, N \in G$ について、$M * N \neq N * M$ なので、X が G の作用域となるための定義 *4.1.2* の二つ目の条件を満たしません。（なぜでしょうか？）よって、G は、X を作用域として持つ群になりません。

解答 4.9 $\{e, ab\}$

解答 4.10 *(a)* $\{e,\ (1,3),\ (2,4),\ (1,3)(2,4)\}$ *(b)* $\{e,\ (1,7)(2,8)(3,5),\ (2,3)(5,8),\ (1,7)(2,5)(3,8)\}$ *(c)* $\{e,\ (1,6)(2,5)(3,4)\}$

解答 4.11 問題 *4.7* から $S_{\mathcal{S}_4}(f_1)$ の元の数が *8* であることより、軌跡の個数は *3(=24/8)* となります。具体的には、$(x_1+x_3)(x_2+x_4)$, $(x_1+x_2)(x_3+x_4)$, $(x_1+x_4)(x_2+x_3)$

解答 4.12 $S_{\mathcal{S}_4}(f_1) \supset S_{\mathcal{S}_4}(Y)$ で、$(1,2,3,4) \notin S_{\mathcal{S}_4}(Y)$ なので、$S_{\mathcal{S}_4}(Y)$ は、ほんとに $S_{\mathcal{S}_4}(f_1)$ より小さくなります。今、$S_{\mathcal{S}_4}(f_1)$ の元の個数が *8* なので、その真部分群 $S_{\mathcal{S}_4}(Y)$ の位数は、４以下になります。ここで、e, $(1,2)(3,4)$, $(1,3)(2,4)$, $(1,4)(2,3)$ は、$S_{\mathcal{S}_4}(Y)$ に含まれるので、これで全部になります。

`Time-stamp: <06/01/30 10:27:46 waki>`

第5章　共役と共役類

「群」の中の元を分類するとき、「共役」という考え方がとても有用です。これは、動きの本質を見極める意味でもとても重要な概念となるでしょう。

共役同士は似た者同士！

5.1　共役な元

まず、群 G の元の共役を定義してみましょう。

定義 5.1.1 群 G の元 $x, g \in G$ に対して、$g^{-1} * x * g$ を x の g による**共役**と呼び、x^g と書きます。また、群 G の *2* つの元 $x, y \in G$ に対して、$y = x^g$ となる元 $g \in G$ が存在するとき、x と y は、お互いに**共役である**と呼び、$x \overset{G}{\sim} y$ と表します。

例えば、3 次の対称群 $\mathcal{S}_3$ に対して、$(1,2)^{(1,2,3)} = (1,3,2) * (1,2) * (1,2,3) = (2,3)$ から、$(1,2)$ の $(1,2,3)$ による共役は $(2,3)$ であり、$(1,2)$ と $(2,3)$ は、$\mathcal{S}_3$ の中で共役なり、$(1,2) \overset{\mathcal{S}_3}{\sim} (2,3)$ と表せます。

命題 5.1.2 元 $g \in G$ による共役で群 G に対する作用を考えると、群 G は、作用域 G を持つ。

証明 定義 4.1.2 の条件を見ていきましょう。群 G から G への写像 f_g を $x \mapsto x^g$ で定めると、この写像は全単射になります。(問題 5.4) よって 群 G の任意の元 g は、群 G に作用していることになりますので、条件 a1 が確認できました。共役の定義 5.1.1 から条件 a2, a3 が成り立つこともすぐに確認できます。∎

命題 5.1.3 定義 *5.1.1* の関係 $\overset{G}{\sim}$ は、同値関係になる。

証明命題 5.1.2 と命題 4.1.5 より、$\overset{G}{\sim}$ は、同値関係になる。∎

定義 5.1.4 $x \in G$ に対して、同値関係 $\overset{G}{\sim}$ に関する x の同値類 I_x を x の G での**共役類**と呼び、x^G と表すことにします。

具体的には次の様な集合となります。

$$\begin{aligned} x^G = I_x &= \{y \in G \mid x \overset{G}{\sim} y\} \\ &= \{y \in G \mid \exists g \in G,\, y = x^g = g^{-1} * x * g\} \\ &= \{g^{-1} * x * g \mid g \in G\} \end{aligned}$$

例：3 次の対称群 $\mathcal{S}_3$ で共役類を考えると、

$$\begin{aligned} e^{\mathcal{S}_3} &= \{e\} \\ (1,2)^{\mathcal{S}_3} &= \{(1,2),\, (1,3),\, (2,3)\} \\ (1,2,3)^{\mathcal{S}_3} &= \{(1,2,3),\, (1,3,2)\} \end{aligned}$$

の 3 つの共役類があることが分かります。

命題 5.1.5 $x^G = \mathcal{O}_G(x)$

証明 $x^G = \{x^g \mid g \in G\} = \mathcal{O}_G(x)$ ∎

定義 5.1.6 群 G の元 x について、部分集合 $\{g \in G \mid x^g = x\}$ を x の**中心化部分群**と呼び、$C_G(x)$ と書き表します。

中心化群 $C_G(x)$ は、G による x の作用で x を動かさない元の集まりとなるので、一点固定部分群 $S_G(x)$ と一致します。命題 4.3.4 と命題 5.1.5 より、共役類 x^G に含まれる元の個数は、$|G|/|C_G(x)|$ に等しくなります。

例：$G = \mathcal{S}_3$ とすると、$C_G(e) = G$, $C_G(1,2) = \{e,(1,2)\}$, $C_G(1,2,3) = \{e,(1,2,3),(1,3,2)\}$ よって、$|e^G| = 1$, $|(1,2)^G| = 3$, $|(1,2,3)^G| = 2$ です。具体的な元は１つ前の例で出していますね。

共役類は似た者同士と言いましたが、例えば、$x \overset{G}{\sim} y$ なら、x の位数と y の位数は等しくなります。また共役な置換はその「形」が同じになることも分かります。例えば、置換 $(1,2,3)$ と置換 $(4,5,6)$ は、$g = (1,4)(2,5)(3,6)$ で、$(1,2,3)^g = (4,5,6)$ となり、お互いが共役になります。

問 5.1.7 *3* 次の対称群 $\mathcal{S}_3$ の中で、$(1,2,3)$ と $(1,3,2)$ が共役であることを $(1,2,3)^g = (1,3,2)$ となる g を見付けて示せ。

5.2　共役な部分群

元についての共役以外に部分群の共役も考えることが出来ます。

定義 5.2.1 群 G とその部分群 H があるとき、G の元 g による H の共役を集合 $\{h^g \mid h \in H\}$ として、H^g と書き表すことにする。

命題 5.2.2 群 G とその部分群 H があるとき、G の元 g による H の共役 H^g は、G の部分群となる。

証明 部分群の条件を示す。H^g の元を２つ ${h_1}^g, {h_2}^g$ を選ぶと、${h_1}^g * {h_2}^g = g^{-1} * h_1 * g * g^{-1} * h_2 * g = (h_1 * h_2)^g$ なり、$h_1 * h_2 \in H$ より ${h_1}^g * {h_2}^g \in H^g$ が言える。また、$(h^g)^{-1} = (g^{-1} * h * g)^{-1} = g^{-1} * h^{-1} * g$ で、$h^{-1} \in H$ より、$(h^g)^{-1} \in H^g$ も言えるので、H^g は、G の部分群になります。∎

例：3 次の対称群 $\mathcal{S}_3$ の部分群 $H_1 = \{e,(1,2)\}$ について、$g = (1,2,3)$ による共役を考えると $H_2 = H^g = \{e,(1,2)^g\} = \{e,(1,3,2)*(1,2)*(1,2,3)\} = \{e,(2,3)\}$, $H_3 = H^g = \{e,(2,3)^g\} = \{e,(1,3,2)*(2,3)*(1,2,3)\} = \{e,(1,3)\}$ となります。また、$K = \{e,(1,2,3),(1,3,2)\}$ については、$g = (1,2)$ としても、$K^g = \{e,(1,2,3)^{(1,2)},(1,3,2)^{(1,2)}\} = \{e,(1,3,2),(1,2,3)\} = K$ と変わらない場合もあります。

命題 5.2.3 置換群 G が作用域 $X := \{1,2,\cdots,n\}$ を持つとき、$i \in X$ に対する一点固定部分群 $S_G(i)$ と $\sigma \in G$ おいて、

$$(S_G(i))^\sigma = S_G(i^\sigma)$$

が成り立つ。

証明 $j := i^\sigma$ とすると、$i = j^{\sigma^{-1}}$ となるので、$(S_G(i))^\sigma$ の任意の元 $g^\sigma = \sigma^{-1} * g * \sigma$ $(g \in S_G(i))$ について、$j^{g^\sigma} = j^{\sigma^{-1}*g*\sigma} = i^{g*\sigma} = i^\sigma = j$ よって、$g^\sigma \in S_G(j) = S_G(i^\sigma)$ が成り立ち、$(S_G(i))^\sigma \subset S_G(i^\sigma)$ が示せました。逆に $g' \in S_G(j)$ なら、$j^{g'} = j$ で、$g = \sigma * g' * \sigma^{-1}$ と置くと、$i^g = i^{\sigma*g'*\sigma^{-1}} = i$ が確かめられて、$g \in S_G(i)$ で $g' = \sigma^{-1} * g * \sigma$ となり、$g' \in (S_G(i))^\sigma$ が成り立ち、$(S_G(i))^\sigma \supset S_G(i^\sigma)$ が示せました。∎

5.3　章末問題

問題 5.1 *7* 次の対称群 $\mathcal{S}_7$ で、元 $(1,2)$ と $(5,7)$ が共役であることを、$(1,2)^g = (5,7)$ となる元 $g \in \mathcal{S}_7$ を見つけて示せ。

問題 5.2 *7* 次の対称群 $\mathcal{S}_7$ で、元 $(1,2,3,4)$ と $(1,3,5,7)$ が共役であることを、$(1,2,3,4)^g = (1,3,5,7)$ となる元 $g \in \mathcal{S}_7$ を見つけて示せ。

問題 5.3 $\forall g \in \mathcal{S}_n$ について、$(1,2)^g$ が互換になることを証明せよ。

問題 5.4 群 G の元 g に対して、G から G への写像 $f_g\colon x \mapsto g^{-1} * x * g$ が全単射となることを示せ。

問題 5.5 *4* 次の対称群 $\mathcal{S}_4$ の元 $(1,2)(3,4)$ を含む共役類 $(1,2)(3,4)^{\mathcal{S}_4}$ を求めよ。また、$(1,2)(3,4)^{\mathcal{S}_4}$ に含まれるそれぞれの元 x について、$x = (1,2)(3,4)^g$ となる元 $g \in \mathcal{S}_4$ を求めよ。

問題 5.6 問題 *5.5* を参考にして、S_4 の $(1,2)(3,4)$ に対する中心化部分群 $C_{\mathcal{S}_4}((1,2)(3,4))$ の元をすべて求めよ。

問題 5.7 群 G の元 x について、部分集合 $\{g \in G \mid x^g = x\}$ が G の部分群になることを示しなさい。

問題 5.8 $\mathcal{S}_4$ の部分群 $H = \{e, (1,2), (1,4), (2,4), (1,2,4), (1,4,2)\}$ について、共役な部分群 $H^{(1,2,3,4)}$ の元をすべて求めよ。

5.4 章末問題の解答

解答 5.1 例えば、$g = (1,5)(2,7)$ など

解答 5.2 例えば、$g = (2,3,5)(4,7)$ など

解答 5.3 $i := 1^g,\ j := 2^g$ とすると $\forall k \notin \{i,j\},\ k^{g^{-1}(1,2)g} = k$ また、$i^{g^{-1}(1,2)g} = j,\ j^{g^{-1}(1,2)g} = i$ となる。以上より、$(1,2)^g = g^{-1}(1,2)g = (i,j)$

解答 5.4 $\forall y \in G,\ x := g * y * g^{-1} \in G,$ とすれば、$f_g(x) = g^{-1} * (g * y * g^{-1}) * g = y$ より、全射が成り立ちます。$x, y \in G$ について $f_g(x) = f_g(y)$ なら $g^{-1} * x * g = g^{-1} * y * g$ となり、$x = y$ が言えて単射も成り立ちます。

解答 5.5 $(1,2)(3,4)^{\mathcal{S}_4} = \{(1,2)(3,4) = (1,2)(3,4)^e,\ (1,3)(2,4) = (1,2)(3,4)^{(2,3,4)},\ (1,4)(2,3) = (1,2)(3,4)^{(2,4,3)}\}$

解答 5.6 問題 *5.5* より、$|C_{\mathcal{S}_4}((1,2)(3,4))| = |\mathcal{S}_4|/|(1,2)(3,4)^{\mathcal{S}_4}| = 24/3 = 8,\ (1,3,2,4) \in C_{\mathcal{S}_4}((1,2)(3,4))$ であることに気がつけば、$C_{\mathcal{S}_4}((1,2)(3,4)) = \{e, (1,3,2,4), (1,2)(3,4), (1,4,2,3), (1,2), (1,3)(2,4), (3,4), (1,4)(2,3)\}$

解答 5.7 $H = \{g \in G \mid x^g = x\},$ と置きましょう。$h, g \in H$ について $x^h = x,\ x^g = x$ より、$x^{(h*g)} = \left(x^h\right)^g = x^g = x,$ よって、 $h * g \in H$ また、$x = x^e = x^{h*h^{-1}} = \left(x^h\right)^{h^{-1}} = x^{h^{-1}}$ より、$h^{-1} \in H$ も成り立ちます。

解答 5.8 $H = S_{\mathcal{S}_4}(3)$ であることに気がつけば $H^{(1,2,3,4)} = S_{\mathcal{S}_4}(3)^{(1,2,3,4)},$ 命題 *5.2.3* より、$S_{\mathcal{S}_4}(3)^{(1,2,3,4)} = S_{\mathcal{S}_4}(3^{(1,2,3,4)}) = S_{\mathcal{S}_4}(4) = \{e, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$

`Time-stamp: <06/01/27 14:27:09 waki>`

第6章　正規部分群とその性質

前節では、「共役な」部分群を定義しましたが、部分群の中にはこの「共役」に動じない部分群が存在します。この節では、そんな部分群の性質を紹介します。

$\boxed{\text{共役に負けない正規部分群}}$

6.1　正規部分群の定義

定義 6.1.1 群 G の部分群 H について、任意の G の元 g について、$H^g = H$ が成り立つとき、H は、G の**正規部分群**と呼び、$H \triangleleft G$ と表します。

例：3 次の対称群 $\mathcal{S}_3 = \{e, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$ について、$K = \{e, (1,2,3), (1,3,2)\}$ とすると、$\forall x \in G, H^g = H$ がなりたちますので、K は、G の正規部分群です。しかし $H = \{e, (1,2)\}$ は、$H^{(1,2,3)} = \{e, (2,3)\}$, $H^{(1,3,2)} = \{e, (1,3)\}$ となり、H は、正規部分群ではありません。

命題 6.1.2 群 G の部分群 H について、

$$\forall g \in G;\ H^g \subset H \Leftrightarrow H \triangleleft G$$

証明 定義 6.1.1 より、右を仮定して左が成り立つことは分かります。(注：$X = Y \Rightarrow X \subset Y$) よって、左を仮定して右を示します。仮定から G の任意の元 g について、$H^g \supset H$ を示せば良いので、h を H から勝手に選んだ元とします。G が群であることから $g^{-1} \in G$ が言えますので、仮定より $(g^{-1})^{-1} * h * g^{-1} \in H$ が成り立ちます。そこで、H の元 $h' = (g^{-1})^{-1} * h * g^{-1}$ について左から g^{-1} 右から g をかけると等式 $g^{-1} * h' * g = h$ が表れ、$h = h'^g \in H^g$ が分かります。よって $H \subset H^g$ が成り立ち $H = H^g$ となり H は、G の正規部分群になります。∎

例：n 次の対称群とその部分群である交代群 $\mathcal{S}_n$, $\mathcal{A}_n$ を見てみましょう。$x \in \mathcal{A}_n$ は、n 次の偶置換です。任意の置換 $g \in \mathcal{S}_n$ について、命題 2.2.1 から互換 σ_i を使って $g = \sigma_1 * \sigma_2 * \cdots * \sigma_s$ と表すことが出来ます。このとき、$(\sigma_i)^2 = e$ から $g^{-1} = \sigma_n * \sigma_{n-1} * \cdots * \sigma_1$ が成り立ちますので、$\mathcal{A}_n$ の任意の元である偶置換 x について、$x^g = g^{-1} * x * g = \sigma_n * \sigma_{n-1} * \cdots * \sigma_1 * x * \sigma_1 * \sigma_2 * \cdots * \sigma_s$ が分かります。x が $2m$ 個の互換の積で表されていれば、x^g は、$2(m+s)$ 個の互換の積で表せることになり、x^g も偶置換であることが分かります。よって $x^g \in \mathcal{A}_n$ が分かり、${\mathcal{A}_n}^g \subset \mathcal{A}_n$ が示されましたので、命題 6.1.2 より、$\mathcal{A}_n$ は、$\mathcal{S}_n$ の正規部分群となります。

6.2　正規部分群の性質

それでは、正規部分群の性質を見て生きましょう。ここで示す性質は正規部分群を見付けるときにとても役に立ちます。

命題 6.2.1 群 G の部分群 H について、

$$\exists Y \subset G;\ H = \bigcup_{y \in Y} y^G \Leftrightarrow H \triangleleft G$$

証明 まず右を仮定して左を示しましょう。ここでは、$Y = H$ と置きます。すると $y \in y^G$ (命題 5.1.3 参照) より、$H \subset \cup y^G$ は、成り立ちます。また、$\forall y \in Y = H$ で $H \triangleleft G$ より、y^G の任意の元 y^g について $y^g \in H^g = H$ が成り立つので、$H \supset \cup y^G$ も分かり、$H = \cup y^G$ が示せました。
逆に左を仮定して右を示しましょう。H の任意の元 h について、仮定からある $\exists y \in Y$ が存在して h は、共役類 y^G に含まれて $y \overset{G}{\sim} h$ となります。このとき、任意の $g \in G$ について $h \overset{G}{\sim} h^g$ より命題 5.1.3 から $y \overset{G}{\sim} h^g$ となり

h^g も同じ共役類 y^G に含まれます。よって、$h^g \in y^G \subset \cup y^G = H$ となり、命題 6.1.2 から、H は、G の正規部分群となります。∎

例:27 ページで示した通り、$\mathcal{S}_3$ の共役類は、$e^{\mathcal{S}_3} = \{e\}, (1,2)^{\mathcal{S}_3} = \{(1,2),(1,3),(2,3)\}, (1,2,3)^{\mathcal{S}_3} = \{(1,2,3),(1,3,2)\}$ の 3 つです。$\mathcal{S}_3$ の真部分群は、位数が 1,2,3 のいずれかで、必ず単位元を含んでいる必要があるので、正規部分群となるのは、自明な群 $H_1 = e^G$ または位数 3 の部分群 $H_2 = e^G \cup (1,2,3)^G$ の 2 つだけとなります。

命題 6.2.2 群 G の部分群 H について、

$$\forall g \in G;\ Hg = gH \Leftrightarrow H \triangleleft G$$

証明この命題もまず右を仮定して左を示しましょう。G の任意の元 g について Hg の任意の元 $h * g$ $(h \in H)$ を考えると、$H \triangleleft G$ より、$h^g \in H$ となり、$h * g = g * (g^{-1} * h * g) = g * h^g \in gH$ が分かり、$Hg \subset gH$ が示せます。逆に gH から任意の元 $g * h$ を取っても、$h \in H = H^g$ より、$h' \in H$ で $h = h'^g$ となる h' が存在するので、$g * h = g * h'^g = g * (g^{-1} * h' * g) = h' * g \in Hg$ となり、$Hg \supset gH$ も成り立ち、$Hg = gH$ が示せました。
次に左を仮定して右を示しましょう。元 $h^g \in H^g$ について、$h * g \in Hg = gH$ より、$h' \in H$ で $h * g = g * h'$ となる元が存在します。この等式に左から g^{-1} を加えると $g^{-1} * h * g = h' \in H$ となり、$h^g \in H$ が示されました。
よって命題 6.1.2 から、H は、G の正規部分群となります。∎

定義 6.2.3 群 G の任意の元 $x, y \in G$ について、$x * y = y * x$ が成り立つとき、G は、**可換群**であると呼びます。

例：可換群 G とその部分群 H に対して、$\forall g \in G, Hg = \{h * g \,|\, h \in H\} = \{g * h \,|\, h \in H\} = gH$ が成り立ちます。よって命題 6.2.2 より、可換群 G の任意の部分群は G の正規部分群になります。

6.3　章末問題

問題 6.1 H は G の部分群で、K は H の部分群であり、$K \triangleleft G$ ならば、$K \triangleleft H$ であることを証明せよ。

問題 6.2 $H \triangleleft G$、$K \triangleleft G$ ならば、$H \cap K \triangleleft G$ であることを証明せよ。

問題 6.3 H は G の正規部分群で、K は G の部分群ならば、$H \cap K$ は、K の正規部分群であることを証明せよ。

問題 6.4 K は G の正規部分群で、H は G の部分群ならば、$HK := \{h * k \mid h \in H,\ k \in K\}$ は、G の部分群であることを証明せよ。

問題 6.5 K と H がともに G の正規部分群ならば、HK も正規部分群であることを証明せよ。

問題 6.6 群 G と部分群 H が与えられて、$|G : H| = 2$ ならば、H は G の正規部分群であることを証明せよ。

問題 6.7 問題 *4.9* の群 G に含まれる正規部分群を求めよ。

6.4　章末問題の解答

解答 6.1 H の任意の元で $g \in H \subset G$ で、$K \triangleleft G$ より、$K^g = K$ が成り立ちます。。

解答 6.2 $\forall g \in G$ に対して $x \in H \cap K$ について $x \in H \triangleleft G$ より $x^g \in H$, $x \in K \triangleleft G$ より $x^g \in K$ となり $x^g \in H \cap K$ が分かります。よって $(H \cap K)^g \subset H \cap K$ が成り立ち、命題 *6.1.2* から、$H \cap K \triangleleft G$。

解答 6.3 $\forall g \in K$ に対して $x \in H \cap K$ について $x \in H \triangleleft G$ より $x^g \in H$ が分かります。また K が群であることから $g^{-1} \in K$ で $x \in K$ より $x^g \in K$ となり $x^g \in H \cap K$ が分かります。よって $(H \cap K)^g \subset H \cap K$ が成り立ち、命題 *6.1.2* から、$H \cap K \triangleleft K$。

解答 6.4 HK が部分群となるための条件を見ましょう。HK の任意の元 $h_1k_1,\ h_2k_2$ に対して、$K \triangleleft G$ より、${h_2}^{-1} * k_1 * h_2 \in K$ です。よって、$h_1k_1 * h_2k_2 = (h_1h_2) * \left(({h_2}^{-1} * k_1 * h_2) * k_2\right) \in HK$ が成り立ちます。また、$hk \in HK$ について、$K \triangleleft G$ より、$h * k^{-1} * h^{-1} \in K$ となるので、$(hk)^{-1} = k^{-1}h^{-1} = h^{-1} * (h * k^{-1} * h^{-1}) \in HK$ が成り立ちます。

解答 6.5 問題 *6.4* より、HK は部分群となるが、任意の元 $g \in G$ について、$H^g = H,\ K^g = K$ より、$(HK)^g = \{(hk)^g \mid h \in H,\ k \in K\} = \{h^g k^g \mid h \in H,\ k \in K\} \subset HK$ が成り立ち命題 *6.1.2* から、$HK \lhd G$。

解答 6.6 $|G:H| = 2$ より、剰余類の個数は *2* 個です。よって、H に含まれない G の元 g を使って $G = H \cup gH$ つまり H 以外の左剰余類はただ *1* つでそれは、$G \backslash H$ となります。また、右剰余類の個数も *2* 個になりますので、H 以外の右剰余類はただ *1* つで同じく $G \backslash H$ になり、$\forall g \in G$ に対して $g \in H$ なら、$Hg = H = gH$ で、$g \notin H$ なら、$Hg = G \backslash H = gH$ が成り立ち、命題 *6.2.2* より、$H \cap K \lhd G$。

解答 6.7 正８角形の作用で出来る群は、$a = (1,2,3,4,5,6,7,8),\ b = (1,2)(3,8)(4,7)(5,6)$ について $G = \langle a, b \rangle$ となります。$b{*}a{*}b = a^7$ より、$a^{-1}{*}b{*}a = a^6{*}b$ 共役類は、$e^G = \{e\},\ (a^4)^G = \{a^4\},\ a^G = \{a, a^7\},\ (a^2)^G = \{a^2, a^6\},\ (a^3)^G = \{a^3, a^5\},\ b^G = \{b, a^2b, a^4b, a^6b\},\ ab^G = \{ab, a^3b, a^5b, a^7b\}$ となります。G の真部分群の位数は、*1,2,4,8* なので、正規部分群は、$H_1 = e^G,\ H_2 = e^G \cup (a^4)^G,\ H_3 = e^G \cup (a^4)^G \cup (a^2)^G,\ H_4 = e^G \cup (a^4)^G \cup (a^2)^G \cup a^G \cup (a^3)^G,\ H_5 = e^G \cup (a^4)^G \cup (a^2)^G \cup b^G,\ H_6 = e^G \cup (a^4)^G \cup (a^2)^G \cup ab^G$ となります。

`Time-stamp: <06/01/27 14:29:39 waki>`

第7章　準同形写像

この節では、２つの動きの集合を上手に結びつける手段として準同形写像を紹介します。

$\boxed{\text{準同形写像は動きの連係}}$

7.1　準同形写像の定義

定義 7.1.1 *2*つの群 G, G' のそれぞれ二項演算 $*$, $\circ$ が与えられているとします。このとき、写像 $f: G \longrightarrow G'$ が**準同形写像**であるとは、$\forall x, y \in G$; $f(a * b) = f(x) \circ f(y)$ が成り立つことです。

例：G を n 次の対称群 $\mathcal{S}_n$、$G' = \{1, -1\}$ として、置換の積を $*$ 普通のかけ算を $\circ$ とすると、$*$ と $\circ$ は、それぞれ G と G' の二項演算になります。G から G' への写像 f を $x \in G$ に対して、x が偶置換なら $f(x) = 1$、x が奇置換なら $f(x) = -1$ で決めます。すると、写像 f は、準同形写像となります。

問 7.1.2 上の例での f が準同形写像であることを確かめなさい。

命題 7.1.3 *2*つの群 G, G' そして G から G' への準同形写像 f が与えられたとき、次のことが成り立ちます。

(i) G の単位元 e に対して $e' = f(e)$ は、G' の単位元となります。

(ii) G の任意の元 x に対して、$f(x^{-1}) = f(x)^{-1}$

(iii) G の任意の元 x と整数 n に対して $f(x^n) = f(x)^n$

証明 (i) $e * e = e$ より、$e' = f(e) = f(e * e) = f(e) * f(e) = e' \circ e'$ ここで、e' の逆元を両辺にかけると、左辺は G' の単位元であり右辺は e' となります。よって、e' は、G' の単位元です。(以後 e' で G' の単位元を表すことにします。(ii) 逆元の性質から $e' = f(e) = f(a * a^{-1}) = f(a) \circ f(a^{-1})$ となります。ここで、左から $f(a)$ の逆元 $f(a)^{-1}$ をかけると、e' は単位元なので、$f(a)^{-1} = f(a^{-1})$ が得られます。(iii) $n \geqq 0$ のときは、n についての数学的帰納法で分かります。n が負の数の場合は、$n = -m$ $(m \in \mathbb{N})$ として、$f(x^n) = f(x^{-m}) = f((x^{-1})^m) = f(x^{-1})^m = (f(x)^{-1})^m = f(x)^{-m} = f(x)^n$ と出来ます。∎

定義 7.1.4 *2*つの群 G, G' そして G から G' への準同形写像 f が与えられたとき、f が全単射写像であれば、f を**同形写像**と呼びます。*2*つの群 G,G' の間に、同形写像が存在するとき、G と G' は、**同型**であると呼び、$G \cong G'$ で表します。

例：$G := \{e, x, x^2, y, xy, x^2y\}$ をパックマンの動きの群、$G' := \{e', a, a^2, a^3, a^4, a^5\}$ をおもちゃの自動車の動きの群とします。準同形写像 f が、$f(x) = a^2$, $f(y) = e'$ と元を移すとすると、その他の元は、$f(x^2) = f(x^2y) = a^4$, $f(xy) = a^4$ となります。この対応から f は、単射ではありませんし、a に対応する G の元が存在しないことから、全射にもなりません。では、別の準同形写像 h として $h(x) = a^4$, $h(y) = a^3$ を対応させたらどうでしょうか？こんどは、$h(x^2) = a^2$, $h(x^2y) = x^5$, $h(xy) = a$ と h は、全単射写像となり、h は、同形写像となります。よって、G と G' は同型です。(このように同型な群の間に同形写像でない準同形写像がある場合もあります)

7.2　準同形写像から生まれる部分群

命題 7.2.1 *2*つの群 G, G' そして G から G' への準同形写像 f が与えられたとき、G の部分群 H に対して、$H' := \{f(h) \,|\, h \in H\}$ は、G' の部分群となる。

証明 $x' \in H' \Leftrightarrow \exists x \in H \;\; x' = f(x)$ であることを、十分に理解して証明しましょう。$\forall x', y' \in H', \exists x, y \in H;\; x' = f(x),\, y' = f(y)$ より、$x' \circ y' = f(x) \circ f(y) = f(x * y)$, もちろん $x * y \in H$ より、$x' \circ y' \in H'$ が示されました。また、$\forall x' \in H',\, (x')^{-1} = f(x)^{-1} = f(x^{-1}),\, x^{-1} \in H$ より、$(x')^{-1} \in H'$ も言えます。∎

命題 7.2.1 の H' を f による H の**像**と呼び、$f(H)$ と書き表します。また、$f(G)$ を $\mathrm{Im}\ f$ と書き表すときもあります。特に、

$$\text{準同形写像 } f \text{ が全射} \Longleftrightarrow \mathrm{Im}\ f = G'$$

命題 7.2.2 *2* つの群 $G,\, G'$ そして G から G' への準同形写像 f が与えられたとき、G' の単位元 e' に対して、$H := \{x \in G \,|\, f(x) = e'\}$ は、G の正規部分群となる。

証明 まず H が部分群になることを示しましょう。$\forall x, y \in H$ に対して、$f(x * y) = f(x) \circ f(y) = e' \circ e' = e'$ より、$x * y \in H$ です。さらに $e' = f(x) \circ f(x)^{-1} = f(x) \circ f(x^{-1}) = e' \circ f(x^{-1}) = f(x^{-1})$ より、$x^{-1} \in H$ となり、H は、G の部分群です。次に正規部分群であることを見ましょう。任意の元 $g \in G$ について、$x^g \in H^g$ $(x \in H)$ を任意に取ると、$f(x^g) = f(g^{-1} * x * g) = f(g)^{-1} \circ f(x) \circ f(g) = f(g)^{-1} \circ f(g) = e'$ から、$x^g \in H$ が示せます。よって $H^g \subset H$ となり、命題 6.1.2 より H は G の正規部分群です。∎

命題 7.2.2 の H を f による G の**核**とよび、$\mathrm{Ker}\ f$ で表します。

例 定義 7.1.1 のすぐ後に出ている例で、G' の単位元は 1 です。よってこの準同形写像の核は、$\mathrm{Ker}\ f = \{x \in G \,|\, f(x) = 1\} = \mathcal{A}_n$ となります。よって、命題 7.2.2 からも $\mathcal{A}_n$ が $\mathcal{S}_n$ の正規部分群であることが証明されます。

命題 7.2.3 *2* つの群 $G,\, G'$ そして G から G' への準同形写像 f が与えられたとき、

$$\text{写像 } f \text{ は、単射である} \Longleftrightarrow Ker\ f = \{e\}$$

証明 まず、左を仮定して右を示します。核の定義から $e \in \mathrm{Ker}\ f$ ですが、もし e 以外の元 x が $\mathrm{Ker}\ f$ に含まれていると、$f(x) = e'$ となり $f(e) = e'$ と合わせて考えると f が単射であることに矛盾します。よって、$\mathrm{Ker}\ f = \{e\}$ となります。逆に、右を仮定すると、$\forall x, y \in G$ に対して、$f(x) = f(y)$ なら、$f(x^{-1} * y) = f(x)^{-1} \circ f(y) = e'$ となり、$x^{-1} * y \in \mathrm{Ker}\ f = \{e\}$ となり、$x^{-1} * y = e$ が成り立ち、$x = y$ が導かれます。よって、f は、単射となります。∎

7.3　章末問題

問題 7.1 $G := \left\{ \begin{pmatrix} a & b \\ 0 & a' \end{pmatrix} \middle|\, a,\, a',\, b \in \mathbb{C},\, aa' \neq 0 \right\}$ としたとき、次の写像が準同型写像となるか調べよ。

(a) $f : G \to \mathbb{C}^{\times}$; ただし $f\left(\begin{pmatrix} a & b \\ 0 & a' \end{pmatrix}\right) = a.$

(b) $f : G \to \mathbb{C}^{\times}$; ただし $f\left(\begin{pmatrix} a & b \\ 0 & a' \end{pmatrix}\right) = a'.$

(c) $f : G \to \mathbb{C}$; ただし $f\left(\begin{pmatrix} a & b \\ 0 & a' \end{pmatrix}\right) = b.$

ただし、G の二項演算は行列の積、$\mathbb{C}^{\times}$ は、$\mathbb{C}$ から *0* を除きいた集合に二項演算をかけ算で群にしたもので、$\mathbb{C}$ は、2 項演算を足し算で群にしたもの。

問題 7.2 群 G とその元 x が与えられたとき、写像 $f_x : G \to G;\; f_x(g) := x^{-1} * g * x$ は、同型写像であることを示せ。

問題 7.3 問題 *6.7* で得られた *6* つの正規部分群それぞれを「核」にする群 G から G への準同型写像を求めよ。

問題 7.4 2 つの準同型写像 $f : G \to H,\, g : H \to K$ があるとき、その写像の合成 $f \circ g : G \to K$ も準同型写像となることを示せ。

問題 7.5 ある群 G の G から G への同型写像全体が、問題 *7.4* の写像の合成を 2 項演算にして群となることを示せ。

問題 7.6 $f : G \to G'$ が準同型写像のとき、G の部分群 H に対して、$f^{-1}(f(H)) \supset H$ となることを示せ。ただし $X \subset G'$ に対して、$f^{-1}(X) := \{g \in G \mid f(g) \in X\}$ とする。

問題 7.7 もし写像 $f : G \to G;\ f(a) := a^{-1}$ が準同型写像ならば群 G は、可換群であることを示せ。

7.4 章末問題の解答

解答 7.1 $m_1 = \begin{pmatrix} a_1 & b_1 \\ 0 & a_1' \end{pmatrix}$, $m_2 = \begin{pmatrix} a_2 & b_2 \\ 0 & a_2' \end{pmatrix}$ と置けば、$m_1 \times m_2 = \begin{pmatrix} a_1a_2 & a_1b_2 + b_1a_2' \\ 0 & a_1'a_2' \end{pmatrix}$ よって、

(a) $f(m_1 \times m_2) = a_1a_2 = f(m_1)f(m_2)$

(b) $f(m_1 \times m_2) = a_1'a_2' = f(m_1)f(m_2)$

(c) $f(m_1 \times m_2) = a_1b_2 + b_1a_2' \neq b_1 + b_2 = f(m_1)f(m_2)$

から、(a), (b) は、準同形写像であります。

解答 7.2 $\forall g_1, g_2 \in G$ について、$f_x(g_1) * f_x(g_2) = (x^{-1} * g_1 * x) * (x^{-1} * g_2 * x) = x^{-1} * g_1 * g_2 * x = f_x(g_1 * g_2)$ となり f_x が準同形写像であることが分かります。また、問題 5.4 より、f_x は、全単射となります。

解答 7.3 $H_1 = \{e\}$ 恒等写像 $f : G \to G,\ \forall x \in G;\ f(x) = x$

$H_2 = \{e, x^4\}$ $f(x) = x^2,\ f(y) = y$

$H_3 = \{e, x^2\, x^4\, x^6\}$ $f(x) = x^4,\ f(y) = y$

$H_4 = \langle x \rangle$ $f(x) = e,\ f(y) = y$

$H_5 = \left\langle x^2, y \right\rangle$ $f(x) = x^4,\ f(y) = e$

$H_6 = \left\langle x^2, xy \right\rangle$ $f(x) = x^4,\ f(y) = x^4$

解答 7.4 $x,\ y$ を G の任意の元とする。$f,\ g$ が準同形写像であることを使えば、$f \circ g(x * y) = g\left(f(x * y)\right) = g(f(x) * f(y)) = g(f(x)) * g(f(y)) = f \circ g(x) * f \circ g(y)$

解答 7.5 問題 7.4 から、この二項演算で閉じていることは示されている。結合律は、$x \in G$ に対して、f, g, k が G から G への同型写像なら $f \circ (g \circ k)(x) = (g \circ k)\left(f(x)\right) = k\left(g\left(f(x)\right)\right) = k\left(f \circ g(x)\right) = \left((f \circ g) \circ k\right)(x)$ より、示されます。単位元にあたる写像は、恒等写像 (つまり $x \in G$ に対して x 自身を対応させる写像)。最後に、同型写像 f の逆元は逆写像 f^{-1} となります。

解答 7.6 集合の包含関係を示せば良いので、$h \in H$ について、$h' = f(h)$ と置くと、$f(H)$ の定義から $h' \in f(H)$ よって、$h' = f(h)$ より、$h \in f^{-1}\left(f(H)\right)$

解答 7.7 G の任意の元 a, b に対して f が準同形写像なので、$f(a * b) = f(a) * f(b)$ が成り立ちます。f の定義より、これは、$(a * b)^{-1} = a^{-1} * b^{-1}$ を表していることになります。ここで、$(a * b)^{-1} = b^{-1} * a^{-1}$ が常に成り立つので、$b^{-1} * a^{-1} = a^{-1} * b^{-1}$ が得られます。これは、a, b が G の任意の元であることを考えると G が可換群であることを意味しています。

`Time-stamp: <06/01/30 18:11:07 waki>`

第 8 章　剰余群とその性質

このテキストの後半では、正規部分群や準同型写像を学びましたが、これらは、この章で紹介する剰余群の準備と見ることも出来ます。剰余群には、必ず正規部分群が必要ですし、群とその剰余群は準同形写像で結ばれています。剰余群はなかなか理解するのが難しい群ですが、一言で言うと

$$\boxed{\text{剰余群は群を遠くから見たもの!?}}$$

て感じでしょうか？つまり群と言う動きの集合を遠くから見ると細かい動きがはっきりしないで似たような動きは同じに見えます。

8.1　集合に対する二項演算

今までに、集合とその元 a, b が与えられたときにこの元 a, b に対するの二項演算 $a * b$ を考えて来ました。ここでは、群 G とその部分集合 S, T が与えられたときにこの**集合** S, T に対する二項演算を定義してみましょう。

定義 8.1.1 群 G とその部分集合 S, T が与えられたとき、群 G の元に対する二項演算 $*$ を使って、集合 S, T に対するの**部分集合の積** $S * T := \{s * t \mid s \in S, t \in T\}$ と決めます。もちろん $S * T$ も G の部分集合となります。

例：G を 3 次対称群 S_3 としたとき、$S := \{(1,2), (2,3)\}$, $T := \{(2,3), (1,3)\}$ とすると、$S * T := \{(1,2) * (2,3), (1,2) * (1,3), (2,3) * (2,3), (2,3) * (1,3)\} = \{(1,3,2), (1,2,3), e\} \subset G$ となります。

問 8.1.2 群 G の部分集合全体の集合を $2^G := \{S \mid S \subset G\}$ とすると、部分集合の積で、2^G は、閉じていることを示し、集合の二項演算に置ける単位元を求めなさい。

命題 8.1.3 群 G の部分群 H について、$H * H = H$ となる。

証明 H が部分群より、$H * H \subset H$ になります。逆に、$e \in H$ より、任意の $h \in H$ に対して $h = h * e \in H * H$ となり、$H \subset H * H$ となります。∎

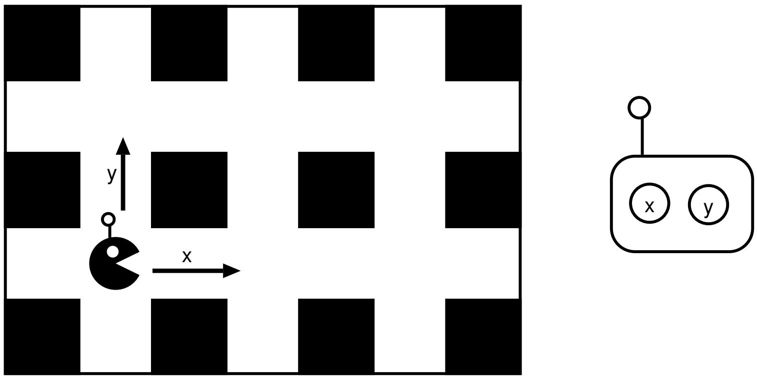
それでは、正規部分群が持つ部分集合の積に対する特徴を紹介しましょう。

命題 8.1.4 群 G とその部分群 H が与えられたとき、H の G に対する任意の剰余類 Ha, Hb に対して、$Ha * Hb = H(a * b)$ であることと H が G の正規部分群であること $(H \triangleleft G)$ は同値である。

証明 まずは、左を仮定して H が正規部分群を示します。任意に $g \in G$ を選んで、$a = g^{-1}$, $b = g$ と置きます。仮定より $Hg^{-1} * Hg = H(g^{-1} * g) = He = H$ となります。$H^g = g^{-1}Hg$ の任意の元 h^g に対して、$e \in H$ より、$h^g = e * g^{-1} * h * g = (e * g^{-1}) * (h * g) \in Hg^{-1} * Hg = H$ よって命題 6.1.2 より、H は正規部分群となります。逆に H が正規部分群だと仮定します。$x \in Ha * Hb$ とすると、$\exists h_1, h_2 \in H;\ x = h_1 * a * h_2 * b,$ このとき、H は正規部分群なので、$g = a^{-1}$ と置くと、$a * h_2 * a^{-1} = h_2^{a^{-1}} = h_2^g \in H$ から、$x = h_1 * a * h_2 * b = h_1 * a * h_2 * a^{-1} * a * b \in H(a * b)$ となり、$Ha * Hb \subset H(a * b)$ が言えます。また、$e \in H$ より、任意の $H(a * b)$ の元 $h * a * b$ について、$h * a * b = h * a * e * b \in Ha * Hb$ なので、$H(a * b) \subset Ha * Hb$ も言えて左が成り立つことが示されました。∎

上の命題より、H が正規部分群ならば、2 つの剰余類 Ha, Hb が与えられたときその 2 つの剰余類の積 $Ha * Hb$ も剰余類 $H(a * b)$ になります。つまり、剰余類の集合は、部分集合の積で閉じていることが分かります。

例：群 G を「パックマンの動きの群」としましょう。$G = \{e, x, x^2, y, xy, x^2y\}$ で、$x^3 = y^2 = e$, $x * y = y * x$ が成り立っています。



G の部分群 $H = \{e, y\}$ とおくと、剰余類の集合は、$G/H = \{H, Hx, Hx^2\}$ となります。「部分集合の積」を使って、剰余類同士の積を計算すると、次の表のようにまとめることが出来ます。

	H	Hx	Hx^2
H	H	Hx	Hx^2
Hx	Hx	Hx^2	H
Hx^2	Hx^2	H	Hx

命題 8.1.5 群 G とその正規部分群 H が与えられたとき、H の G に対する剰余類の集合に二項演算として部分集合の積を入れたとき、この演算に対する単位元が H であることを証明しなさい。

証明任意の剰余類 Ha について、$H * Ha = \{h * h' * a \mid h, h' \in H\} \subset Ha$ また、$h * a \in Ha$ について、$h * a = e * h * a \in H * Ha$ より、$H * Ha = Ha$ また、H は正規部分群で命題 6.2.2 より、$aH = Ha$ が成り立つので、$Ha * H = \{h * a * h' \mid h, h' \in H\} = H * aH = H * Ha = Ha$ となり、H は、単位元の条件を満たす。∎

8.2　剰余群の定義

命題 8.2.1 群 G とその正規部分群 H が与えられたとき、H の G に対する剰余類全体の集合は、部分集合の積を二項演算とする群となる。

証明：命題 8.1.4 より、二項演算が閉じていることが示されています。また、もともと群の二項演算が結合律を満たすことから集合の積も結合律を満たします。命題 8.1.5 より、H は、剰余類の中で単位元となり、任意の剰余類 Ha に対する逆元が Ha^{-1} であることも自明です。∎

定義 8.2.2 群 G とその正規部分群 H が与えられたとき、命題 *8.2.1* で定義された剰余類から構成される群を**剰余群**と呼び、G/H で表すことにします。

例：

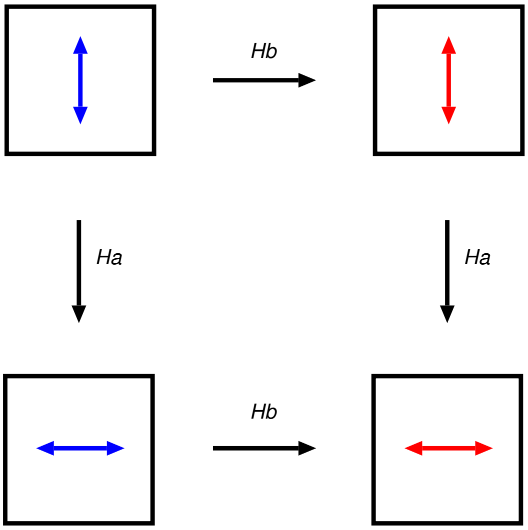
正方形に対する動きの集合 $\{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, その部分群 $H = \{e, a^2\}$ と置きます。このとき、$H \triangleleft G$ となります。剰余類は、全部で 4 つあります。具体的には、$\{H, Ha, Hb, Hab\}$ であり、$Ha = \{a, a^3\}$, $Hb = \{b, a^2b\}$, $Hab = \{ab, a^3b\}$ です。部分集合の積を計算してみると、

- $Ha * Ha = \{a * a, a * a^3, a^3 * a, a^3 * a^3\} = Ha^2 = H$
- $Ha * Hb = \{a * b, a * a^2b, a^3 * b, a^3 * a^2b\} = Hab$
- $Ha * Hab = \{a * ab, a * a^3b, a^3 * ab, a^3 * a^3b\} = Hb$
- $Hb * Ha = \{b * a, b * a^3, a^2b * a, a^2b * a^3\} = Hab$
- $Hb * Hb = \{b * b, b * a^2b, a^2b * b, a^2b * a^2b\} = H$
- $Hb * Hab = \{b * ab, b * a^3b, a^2b * ab, a^2b * a^3b\} = Ha \ldots$

で、$H = \{e, a^2\}$ は、G の正規部分群なので、以下の様な積表を持つ、剰余群となります。

	H	Ha	Hb	Hab
H	H	Ha	Hb	Hab
Ha	Ha	H	Hab	Hb
Hb	Hb	Hab	H	Ha
Hab	Hab	Hb	Ha	H

正方形の表と裏にに次のように模様をつけてその動きを、観察してみましょう。



ここで、正方形に付けた模様は、H の元が行う上下のヒックリ返しによって、変化しないものを選んでいます。つまり動き a^2 を無視する群 G の動きは、8 種類から 4 種類に減少していることが見えて来ます。

剰余群と正規部分群

命題 8.2.3 群 G とその正規部分群 H が与えられたとき、群 G から剰余群 G/H への写像 f を $\forall a \in G;\ f(x) = Ha \in G/H$ と決めると f は、G から G/H の準同形写像となります。この写像 f を正規部分群 H による G から G/H への**自然な準同形写像**と呼びます。

例：40 ページの例では、G から G/H への自然な準同形写像 f は、$f(e) = f(a^2) = H$, $f(a) = f(a^3) = Ha$, $f(b) = f(a^2b) = Hb$, $f(ab) = f(a^3b) = Hab$ と対応させます。それでは最後に、この講義の締めくくりとして、「準同型定理」を紹介します。

定理 8.2.4 群 G と全射な準同形写像 $f : G \longrightarrow G'$ があるとき、$H = Ker\ f$ と置くと、$G' \cong G/H$ となる。

証明

- 写像 $\overline{f} : G' \longrightarrow G/H$ を次のように決めます。仮定より、f が全射なので、任意の G' の元 a' に対して、$f(a) = a'$ となる G の元 a が存在します。よって、この a を使って $\overline{f}(a') = Ha \in G/H$ と決めます。**大事なことは、**このように写像を決めて a' に対して $\overline{f}(a')$ がちゃんと決まっているかを確認することです。f は、全射ですが単射でない場合もありますので、$a' \in G'$ に対して、$f(a) = a'$, $f(b) = a'$ と 2 つの G の元が a' になった場合、$\overline{f}(a')$ は、Ha でも Hb でもどちらでもいいことになります。きちんと $\overline{f}(a')$ が決まるためには、$Ha = Hb$ となることを確認する必要があります。しかし f が準同形写像であることから、$f(a) = f(b) = a'$ なら、$e' = f(b)^{-1} * f(a) = f(b^{-1} * a)$ (ただし e' は、G' の単位元) より、$b^{-1} * a \in \mathrm{Ker}\ f = H$ となり、命題 3.3.9 より $Ha = Hb$が示されました。これで、$\overline{f}$ がきちんと定義できました。(これを写像 $\overline{f}$ は、**well-defined** となっと呼びます。)

- 次に写像 $\overline{f}$ が準同形写像であることを示します。G' の元 a', b' に対して、a, b が $a' = f(a)$, $b' = f(b)$ となる G の元としましょう。よって、$a' * b' = f(a) * f(b) = f(a * b)$ となります。ここから $\overline{f}(a') * \overline{f}(b') = Ha * Hb = H(a * b) = \overline{f}(a' * b')$

- 次に写像 $\overline{f}$ が全射になることを見ましょう。剰余群 G/H の元 (つまり剰余類) Ha を任意に取った時、G' の元 $a' := f(a)$ を選べば $\overline{f}$ の定義から $\overline{f}(a') = Ha$ となることが、分かります。
- 最後に写像 $\overline{f}$ が単射になることを見てみます。G/H の単位元は $H = eH$ ですから、$\mathrm{Ker}\ \overline{f} = \{a' \in G' \mid \overline{f}(a') = H\}$ となります。ここで、$\overline{f}$ の定義から、$\overline{f}(a') = H \Leftrightarrow \exists a \in H;\ f(a) = a'$ となります。$H = \mathrm{Ker}\ f$ であることを思い出すと、$a \in H \Leftrightarrow f(a) = e'$ であり、1 つ上の事実を合わせると $a' = f(a) = e'$ が得られます。つまり $\mathrm{Ker}\ \overline{f} = \{e'\}$ が得られて、命題 7.2.3 から、写像 $\overline{f}$ が単射になります。

これで、$\overline{f}$ は、同形写像となり、定理が証明されました。∎

8.3　章末問題

問題 8.1 *3* 次の対称群 $\mathcal{S}_3$ が与えられたとき、S_3 のすべての部分群同士の部分集合の積を表にまとめよ。

問題 8.2 可換群 G とその部分群 $H,\ K$ が与えられたとき、集合の積 $H * K$ も G の部分群となることを示せ。

問題 8.3 群 G とその部分群 H と空でない部分集合 K が与えられたとき、$H * K = H$ と $H \supset K$ が同値であることを示せ。

問題 8.4 *3* 次の対称群 $\mathcal{S}_3$ とその部分群 $H = \{e,\ (1,2)\}$ の剰余類の集合 $\{Ha \mid a \in G\}$ の元 *(*つまり剰余類*)* 同士の部分集合の積が閉じているか*?* 積を表にまとめて調べよ。

問題 8.5 *3* 次の対称群 $\mathcal{S}_3$ とその部分群 $H = \{e,\ (1,2,3),\ (1,3,2)\}$ の剰余類の集合 $\{Ha \mid a \in G\}$ の元 *(*つまり剰余類*)* 同士の部分集合の積が閉じているか*?* 積を表にまとめて調べよ。

問題 8.6 可換群 G とその部分群 H が与えられたとき、H は正規部分群となることを示し、更に剰余群 G/H も可換群となることを証明しなさい。

問題 8.7 G を n 次の逆行列を持つ実正方行列全体の集合、H をその部分集合で、行列式の値が *1* となるもの全体の集合とするとき、H が G の正規部分群となることを示せ。

問題 8.8 問題 *8.7* で定義した群 G と正規部分群 H について、その剰余群 G/H が可換群となることを示せ。

問題 8.9 準同型定理と使って、問題 *8.8* の剰余群 G/H が $\mathbb{R}^\times$ *(*実数から *0* を除いた集合にかけ算を二項演算にして群にしたもの*)* と同型であることを示しなさい。

問題 8.10 $\mathcal{S}_n$ を n 次の対称群、$\mathcal{A}_n$ を n 次の交代群としたとき、準同型定理を使って、$\mathcal{S}_n/\mathcal{A}_n$ が群 $G = \{1, -1\}$ *(*二項演算はかけ算）と同型であることを証明しなさい。

問題 8.11 パックマンの群 $G = \{e, x, x^2, y, xy, x^2y\}$ とその部分群 $H = \{e, x, x^2\}$ と $K = \{e, y\}$ が与えられたとき、$G/H \cong K,\ G/K \cong H$ となることを、準同型定理を使って証明しなさい。

問題 8.12 正 8 角形に対する動きの群 $D_{16} = \{e, x, x^2, \cdots, x^7, y, xy, x^2y, \cdots, x^7y\}$ とその正規部分群 $K = \{e, x^4\}$ が与えられたとき、D_{16}/K が正方形に対する動きの群 $D_8 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$ と同型になることを準同型定理を使って証明しなさい。

問題 8.13 群 G とその正規部分群 H が与えられたとき、

$$\forall x, y \in G;\ x * y * x^{-1} * y^{-1} \in H \Leftrightarrow G/H \text{ は可換群}$$

を証明せよ。

問題 8.14 群 G とその正規部分群 N が与えられたとき、N の位数 $|N|$ と G に対する指数 $|G : N|$ が互いに素で、G の部分群 H の位数 $|H|$ が $|N|$ の約数となるとき、$H \subset N$ を証明しなさい。

8.4 章末問題の解答

解答 8.1 $H_1 := \{e\},\ H_2 := \{e,\ (1,2)\},\ H_3 := \{e,\ (2,3)\},\ H_4 := \{e,\ (1,3)\},\ H_5 := \{e,\ (1,2,3),\ (1,3,2)\},$ $H_6 := \mathcal{S}_3$ として、「部分集合の積」を表にまとめると、

	H_1	H_2	H_3	H_4	H_5	H_6
H_1	H_1	H_2	H_3	H_4	H_5	H_6
H_2	H_2	H_2	B_1	A_2	H_6	H_6
H_3	H_3	A_1	H_3	B_3	H_6	H_6
H_4	H_4	B_2	A_3	H_4	H_6	H_6
H_5	H_5	H_6	H_6	H_6	H_6	H_6
H_6	H_6	H_6	H_6	H_6	H_6	H_6

となります。ただし、$A_1 = \{e,\ (2,3),\ (1,2),\ (1,2,3)\},\ A_2 = \{e,\ (1,2),\ (1,3),\ (1,2,3)\},\ A_3 = \{e,\ (1,3),\ (2,3),\ (1,2,3)\}$ $B_1 = \{e,\ (1,2),\ (2,3),\ (1,3,2)\},\ B_2 = \{e,\ (1,3),\ (1,2),\ (1,3,2)\},\ B_3 = \{e,\ (2,3),\ (1,3),\ (1,3,2)\}$。

解答 8.2 $H * K = \{h * k \,|\, h \in H,\ k \in K\}$ について、G が可換群であることから、$\forall h_1 * k_1,\ h_2 * k_2 \in H * K;$ $(h_1 * k_1) * (h_2 * k_2) = (h_1 * h_2) * (k_1 * k_2) \in H * K$ となります。更に、$\forall h * k \in H * K;\ (h * k)^{-1} = k^{-1} * h^{-1} = h^{-1} * k^{-1} \in H * K$ となり、部分群の条件 (定義 *3.1.1*) を満たします。

解答 8.3
- まず $H * K = H$ を仮定すると、$\forall k \in K$ に対し H は、部分群なので G の単位元 $e \in H$ よって、$k = e * k \in H * K = H$ より、$K \subset H$。
- 逆に $H \supset K$ とすると、$\forall h * k \in H * K;\ k \in K \subset H$ より $h * k \in H$ となり $H * K \subset H$ が言えます。更に、$\forall h \in H$ で、$k \in K$ を一つ選ぶと、$h * k^{-1} \in H$ より、$h = h * k^{-1} * k \in H * K$ で、$H \subset H * K$ も成り立ちます。よって、$H = H * K$ となります。

解答 8.4 例えば、剰余類 $H(1,3),\ H(2,3)$ を選ぶと、$H(1,3) * H(2,3) = \{(1,3),\ (1,2,3)\} * \{(2,3),\ (1,3,2)\} = \{(1,2,3),\ (1,2),\ (1,3),\ e\}$ となり、これは、剰余類にならない (剰余類の中の元の個数はどれも同じになるから)。

解答 8.5 剰余類は、H と $H(1,2) = \{(1,2),\ (2,3),\ (1,3)\}$ だけで、下の表の通り閉じている。

	H	$H(1,2)$
H	H	$H(1,2)$
$H(1,2)$	$H(1,2)$	H

解答 8.6 部分群 H に対して $\forall g \in G;\ H^g = \{h^g \mid h \in H\}$ で、$\forall h^g \in H^g;\ h^g = g^{-1} * h * g = g^{-1} * g * h = h \in H$ よって、$H^g \subset H$ となり、H は、G の正規部分群となる。更に、剰余群 G/H の *2* つの元 $Ha,\ Hb$ について、$a, b \in G$ より、$a * b = b * a$ が成り立ち、$Ha * Hb = H(a * b) = H(b * a) = Hb * Ha$ となり、G/H も可換群となります。

解答 8.7 線形代数の基本事項から a を n 次の実正方行列とすると、a が逆行列を持つことと行列式 $|a|$ が *0* にならないことは、同値です。G の部分集合 $H = \{h \in G \,|\, |h| = 1\}$ と決めます。まず、H の任意の元 $h_1,\ h_2$ について、仮定より $|h_1| = 1,\ |h_2| = 1$ となります。よって、$|h_1 \times h_2| = |h_1| \times |h_2| = 1 \times 1 = 1$ となり、ここから $h_1 \times h_2 \in H$ が言えます。更に任意の $h \in H$ の逆行列 h^{-1} についても、$|h^{-1}| = 1/|h| = 1$ が言えるので、$h^{-1} \in H$ も成り立ち、H **は、部分群**となります。また、任意の $a \in G$ について、$h^a = a^{-1} \times h \times a$ より、$|h^a| = |a^{-1}| \times |h| \times |a| = 1$ となることより、$h^a \in H$ となり、H **は、**G **で正規部分群**となります。

解答 8.8 H の定義より、剰余群 $Ha = \{h \times a \,|\, h \in H\}$ で、$|h \times a| = |h| \times |a| = |a|$ から、Ha に含まれる元の行列式の値は、全て a の行列式と一致します。また、b が $|a| = |b|$ となる n 次の正方行列なら、$|a \times b^{-1}| = |a||b^{-1}| = |a| \times (1/|a|) = 1$ から、$a \times b^{-1} \in H$ が示され、$Ha = Hb$ が分かりました。つまり、剰余類 Ha は、行列式の値が $|a|$ となる、G の行列全体となります。$Ha,\ Hb$ が、G/H の元とすると、$|a \times b| = |b \times a|$ から、$Ha * Hb = H(a \times b)$ も $Hb * Ha = H(b \times a)$ も行列式が $|a \times b|$ と等しくなる行列全体の集合となり、等式 $Ha * Hb = Hb * Ha$ が成り立ちます。

解答 8.9 G から $\mathbb{R}^\times$ への写像 f を任意の M について、$f(M)=|M|$ と決めると、行列式の性質から f は、準同形写像となる。更に $\mathbb{R}^\times$ の任意の数 α について、例えば、

$$M=\begin{pmatrix} \alpha & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & & \vdots \\ \vdots & \vdots & & \ddots & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

から、$f(M)=\alpha$ も得られて、f は、全射な準同型となります。$H=Ker\ f$ も簡単に分かるので、準同型定理より $G/H\cong\mathbb{R}^\times$

解答 8.10 例 *7.2* にあるように、写像 $f:\mathcal{S}_n\longrightarrow G$ を σ が偶置換なら $f(\sigma)=1$、σ が奇置換なら $f(\sigma)=-1$ と決めると、これが準同形写像となり、$Ker\ f=\mathcal{A}_n$ となることも分かります。

解答 8.11 写像 $f:G\longrightarrow K$ を $f(x)=e,\ f(y)=y$ と決めて、写像 $g:G\longrightarrow H$ を $f(x)=x,\ f(y)=e$ と決める。このとき、$f,\ g$ のどちらも準同形写像となり、$Ker\ f=H,\ Ker\ g=K$ が示されます。

解答 8.12 準同形写像 $f:D_{16}\longrightarrow D_8$ を $f(x)=a,\ f(y)=b$ と決めると、f は準同形写像となります。また、$Ker\ f=K$ より準同型定理を使って、$D_{16}/K\cong D_8$ が示されました。

解答 8.13 まず、$\forall x,y\in G;\ x*y*x^{-1}*y^{-1}\in H$ を仮定して、G/H が可換であることを示す。G/H の任意の元 $Hx,\ Hy$ について、$(x*y)*(y*x)^{-1}=(x*y)*(x^{-1}*y^{-1})\in H,$ 命題 *3.3.9* より、$H(x*y)=H(y*x)$ が成り立つ。逆に、G/H が可換なら、$\forall x,y\in G;\ H(x*y)=H(y*x)$ が成り立つので、いままでと、逆に理論を進めると $\forall x,y\in G;\ x*y*x^{-1}*y^{-1}\in H$ が示されます。

解答 8.14 自然な全射準同形写像 $f:G\longrightarrow G/N\ \ (x\mapsto Nx)$ を考えと、$Ker\ f=N$ となります。部分群 H について、$f(H)$ は、G/N の部分群 *(*命題 *7.2.1* 参照*)* なので、$f(H)$ の位数 $|f(H)|$ は、指数 $|G:N|$ の約数となります。また、写像 $g:H\longrightarrow f(H)$ を $\forall h\in H;\ g(h)=f(h)$ ときめると、g は、全射な準同形写像となり、準同型定理から $H/Ker\ g\cong f(H)$ となり、特に $|f(H)|$ が H の位数 $|H|$ の約数となります。問題の仮定から $|H|$ が $|N|$ の約数なので、$|f(H)|$ も $|N|$ の約数となり、結局 $|f(H)|$ は、$|N|$ と $|G:N|$ の公約数となります。ところが、問題の仮定から $|N|$ と $|G:N|$ が互いに素であることから最大公約数が *1* となり、$|f(H)|=1$ が分かります。今、G の単位元 e は、部分群 H にも含まれますので、G/N の単位元 $N=f(e)$ は、$f(H)$ の唯一の元となります。このことは、$\forall h\in H;\ f(h)=N$ を意味しますので、$H\subset Ker\ f=N$ が示されます。

`Time-stamp: <06/01/30 17:58:01 waki>`

索 引