# Contents

# Part I
# 集合と写像

## 1 用語と記号

既に何度か使っている「:=」という記号や、その他便利でよく使う記号や用語をまとめておきましょう。念のために言っておくと、これらの熱心な暗記を勧めているわけではありません。ましてや試験に出るなんてことはないです。ただ、基本的な英単語を日常でも使うようなテイストで慣れてほしいだけです。

### 1.0.1 定義するときに使う記号 :=

数式中で「:=」と書けばこれは「左辺を右辺で定義する。」ということを意味します。

例えば「$f(x) := \cos(\sin(\tan(x)))$」という文章は「$f(x)$ を $\cos(\sin(\tan(x)))$ と定義する」を意味します。これは「$f(x) = \cos(\sin(\tan(x)))$ と定める」と書いても同じです。

### 1.0.2 s.t (such that)

「s.t」とかけば「such that」の略です。直訳は「のような」です。場合によっては「をみたす」と解釈した方がわかりやすいかもしれません。

### 1.0.3 $\exists, \exists!, \forall$

$\exists$ は「ある」とか「(少なくとも一つは) 存在する」という意味です。
$\exists!$ は「ただ一つある」とか「ただ一つだけ存在する」という意味です。
$\forall$ は「任意の」とか「すべての」とかを意味します。
例文を挙げておきます。

**例 1.1.** 写像 $f : X \to Y$ が与えられているとします。写像が全射であることの定義に現れる条件は次です。
日本語:「集合 $Y$ の任意の要素 $y$ にたいして、集合 $X$ のある要素 $x$ が存在して $y = f(x)$ を満たす。」
これを上の記号を使って書いてみましょう:
「$\forall y \in Y, \exists x \in X$ s.t. $y = f(x)$.」

# 2 集合

「集合」について補足します。日常でも「集合」という言葉を使うので紛らわしいですが、(もちろん) 数学概念としての「集合」を解説します。

## 2.1 集合

集合は簡単なものです。もしか、難しいところがあるとすれば、簡単なもの過ぎてとりとめがない、ということでしょうか。別の言い方をすれば抽象的とか言うのでしょう。
実数というのも、皆さんは馴染んでいるけれど、考えてみれば抽象的なよくわからんものです。けれども、普段の生活で散々使い倒していることもあってか当たり前に感じていますよね。
集合も実数と同じく抽象的な概念ですが、実数と同じく使うことによって慣れることができます。
このプリントでは集合の使い方を説明します。

### 2.1.1 集合のイメージ:集合は箱、要素は中身

「集合」というものをイメージするには、なにか箱をイメージしてください。おもちゃ箱とか、道具箱とか、キャラメルの箱とか、ビックリ箱とか。中に何かが入ってる箱をイメージしてください。(もしくは、なかには何も入っていない箱。つまり、空箱。) そうイメージした時に「集合の要素」といえば箱の中身のことを意味します。おもちゃ、道具、キャラメル、ビックリ人形。
箱をイメージするときには個性のない箱をイメージしてください。そうすると箱自体は中身によって中身によって規定されます。おもちゃが入ってるのがおもちゃ箱、道具が入っているのが道具箱、キャラメルが入っているのがキャラメルの箱、ビックリ人形の入っているのがビックリ箱。
集合 $X$ があったときに $x$ がその要素であること (箱 $X$ の中身が $x$ であること) を「$x \in X$」と表します。
$X$ がおもちゃ箱だったとしたら「$x \in X$」という文章は「$x$ はおもちゃである」という意味です。
$X$ が道具箱だったとしたら「$x \in X$」という文章は「$x$ は道具である」という意味です。
$X$ がキャラメル箱だったとしたら「$x \in X$」という文章は「$x$ はキャラメルである」という意味です。
$X$ がビックリ箱だったとしたら「$x \in X$」という文章は「$x$ はビックリ人形である」という意味です。

集合の取り扱いで大事なのは「$x \in X$」という文章が何を意味するかを理解する、ということです。

後にまとめますが、全員に覚えて欲しい重要な集合に「実数の集合 $\mathbb{R}$」があります。「実数の集合」って言葉の意味を規定するのは難しいかもしれません。
しかし、（なんというか、それはとりあえずどうでもいいことで、）
皆さんに理解して欲しいのは「$x \in \mathbb{R}$」という文章の意味です。
この類のことが理解できれば大丈夫です。

うえで解説してきたことからわかるとおもいますが、
「$x \in \mathbb{R}$」という文章は「$x$ は実数である」という意味です。このことが「記号 $\mathbb{R}$ は実数の集合を表す」といったことの実際的な運用方法です。

なんか、ながなが説明して来ましたが要点をいうと：
集合を学ぶ上で心がけてほしいのは、文章「$x \in X$」を読み解けるようになることです。

### 2.1.2 覚えて欲しい集合の記号

大事な集合にはそれを表す記号が設定されているので、覚えてください。

(1) $\mathbb{N}$：自然数の集合。（注意：大学からは自然数のなかに 0 を含めます。）
なので文章「$x \in \mathbb{N}$」は「$x$ は自然数である」という意味です。

(2) $\mathbb{Z}$：整数の集合。
なので文章「$x \in \mathbb{Z}$」は「$x$ は整数である」という意味です。

(3) $\mathbb{Q}$：有理数の集合。
なので文章「$x \in \mathbb{Q}$」は「$x$ は有理数である」という意味です。

(4) $\mathbb{R}$：実数の集合。
なので文章「$x \in \mathbb{R}$」は「$x$ は実数である」という意味です。

(5) $\mathbb{C}$：複素数の集合。
なので文章「$x \in \mathbb{C}$」は「$x$ は複素数である」という意味です。

(6) $\mathbb{R}^2$：2 次元実数ベクトルの集合。（つまり $xy$ 平面ですね。）
なので文章「$\vec{x} \in \mathbb{R}^2$」は「$\vec{x}$ は 2 次元実数ベクトルである」という意味です。

(7) $\mathbb{R}^3$：3 次元実数ベクトルの集合。（つまり $xyz$ 空間ですね。）
なので文章「$\vec{x} \in \mathbb{R}^3$」は「$\vec{x}$ は 3 次元実数ベクトルである」という意味です。

(8) $n$ を 1 以上の自然数とします。
$\mathbb{R}^n$：$n$ 次元実数ベクトルの集合。
なので文章「$\vec{x} \in \mathbb{R}^n$」は「$\vec{x}$ は $n$ 次元実数ベクトルである」という意味です。

### 2.1.3　名もなき集合

上の節で説明した以外の集合もありますね。いろいろ名前の付いた集合もありますが、名もなき集合、単に要素を集めただけの集合もあります。いくらでもあります。

たとえば「集合 $X = \{x, y, z\}$ を考える[1]。要素 $a \in X$、、、、」みたいな文章があったら、それは「$X$ というのは $x, y, z$ が入った箱を考える。$a$ は $x$ か $y$ か $z$ かのいずれかです、、、、、」ということを意味します。

こういう場合には $X$ は数字（自然数、整数、有理数、実数、複素数）とかベクトルとか、皆さんが数学的対象として思い浮かべるものとは何の関係もありません。ただ単に三つの名もなき物体が詰まった名もなき箱なのです。

写像の例に現れる以外では線形代数で取り上げられる集合は大抵は “有名な集合（数字やベクトルや行列の集合）” です。なので、ここで説明していることは講義自体にはあまり関わりません。しかし、いずれ後期で抽象ベクトル空間を勉強するときには大事になってきます。

## 2.2　空集合 $\emptyset$（空箱）

中身のない箱、つまり、要素をもたない集合を空集合と呼び $\emptyset$ という記号であらわします。空集合からは要素がとれません。なので「$x \in \emptyset$」という文章は（数学的な）現実のものではありえません。別の言い方をすると、集合 $X$ から要素 $x \in X$ をとってこようとおもったらば、先ず $X$ が空集合でないことが保証されていなければいけない、ということです。

**例 2.1.** （後に説明しますが）集合 $\{x \in \mathbb{R} \mid x^2 < 0\}$ と書けば、これは「$x^2 < 0$ を満たす実数 $x$ の集合」を意味します。

皆さんはご存知の通り「$x^2 < 0$ を満たす実数は存在しない」のですが、これは、つまり「$x^2 < 0$ を満たす実数 $x$ の集合は要素を持たない」ということですね。つまり「$x^2 < 0$ を満たす実数 $x$ の集合は空集合である」ということです。

空集合の記号 $\emptyset$ を使うとさらに簡略化されますね：

「$\{x \in \mathbb{R} \mid x^2 < 0\} = \emptyset$」

## 2.3　要素の個数 $|X|$ または $\#X$

集合 $X$ の要素の個数を $|X|$ または $\#X$ であらわします。

**例 2.2.** 空集合 $\emptyset$ というのは要素の個数が 0 個の集合のことなので、次の命題が成り立ちます：

「集合 $X$ が空集合であるための必要十分条件は $|X| = 0$ である。」

## 2.4　部分集合

集合 $X$ を箱とイメージするなら、部分集合 $Y \subset X$ というは箱 $X$ のなかにある箱 $Y$ とイメージできます。

おもちゃ箱の中にロボットだけを集めた小箱があったら、おもちゃ箱という集合の中のロボットが構成する部分集合、なのです。

ただし、$X$ 自身や空集合 $\emptyset$ も $X$ の部分集合とよびます。

皆さんに理解して欲しいのは次の二通りの部分集合の定め方です。

[1]注意：集合を $X = \{x, y, z\}$ と表した時にもしかすると $x = y$ だったりするかも知れません。下手すると $x = y = z$ かも知れません。こういう場合に要素の個数は 2 つだったり 1 つだったりします。

### 2.4.1　条件による部分集合の定義

集合 $X$ を考えます。$X$ の要素になにか条件を設定して、それを満たす要素全体をもってくることで、部分集合 $Y$ を定めることができます。

記法：

$$Y = \{x \in X \mid x \text{ に課される条件 }\}.$$

**例 2.3** (大事な例)**.** 2 次元数ベクトル空間 $\mathbb{R}^2$ の中で方程式 $x + y = 1$ を満たす点 $\begin{pmatrix} x \\ y \end{pmatrix}$ 全体の集合を $Y$ とする。上で説明した記法では次のように表します：

$$Y := \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \middle| x + y = 1 \right\}.$$

（しつこいようですが、）やはり大事なのは「$\vec{z} \in Y$」という文章の意味です。文章「$\vec{z} \in Y$」が表すのは「記号 $\vec{z}$ は 2 次元実数ベクトル $\vec{z} = \begin{pmatrix} x \\ y \end{pmatrix}$ で座標の値 $x, y$ が関係式 $x + y = 1$ を満たすものである」ということです。

皆さん、この部分集合 $Y \subset \mathbb{R}^2$ を図示することはできますね。

### 2.4.2　要素を記述することによる定義

集合 $X$ を考えます。別の集合 $A$ の要素 $a \in A$ で $X$ の（ある範囲の）要素を $x_a$ と記述する手段が与えられている場合に、$x_a$ と表される要素全部を集めた部分集合 $Y$ を定めることができます。

記法：

$$Y = \{x_a \in X \mid a \in A\}.$$

**例 2.4** (大事な例)**.** 実数 $a \in \mathbb{R}$ にたいして 2 次元数ベクトル空間 $\mathbb{R}^2$ の要素 $\vec{x}_s$ を $\vec{x}_s := \begin{pmatrix} s+1 \\ -s \end{pmatrix}$ と定める。部分集合 $Z \subset \mathbb{R}^2$ を $\vec{x}_s$ と表される $\mathbb{R}^2$ の要素全体の部分集合と定義する。

上で説明した記法では次のようにあらわします

$$Z := \left\{ \vec{x}_s \in \mathbb{R}^2 \middle| s \in \mathbb{R} \right\}.$$

（しつこいようですが、）やはり大事なのは「$\vec{z} \in Y$」という文章の意味です。文章「$\vec{z} \in Y$」が表すのは「記号 $\vec{z}$ はある実数 $s \in \mathbb{R}$ にたいして $\vec{z} = \begin{pmatrix} s+1 \\ -s \end{pmatrix}$ と表される 2 次元実数ベクトルである」ということです。

皆さん、この部分集合 $Z \subset \mathbb{R}^2$ を図示することはできますね。

例 *2.3* の部分集合 $Y \subset \mathbb{R}^2$ とこの $Z$ は同じ部分集合ですよね。つまり $Y = Z$ ということです。サラっとイコールの記号で書いていますが意味するところはおおきいのです。

### 2.4.3　名もなき部分集合

部分集合 $Y \subset X$ にもいろんなものがあり、やっぱり名もなき部分集合もあります。たとえば「3 つの要素からなる部分集合 $X \subset \mathbb{R}$ を考える」と言ったら「実数を三つとってくる」という意味です。方程式もなく数式による記述もない部分集合もあるのです。

## 2.5　部分集合の等号 $Y = Z$

集合 $X$ の部分集合 $Y, Z \subset X$ が一致するというのはどういうことでしょうか？イコールの記号を何の気なしに使いますが、意味するところは大きいのです。

**注意 2.5** (例えばなし)**.** 例えば、2 次元ベクトルの等号 $\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} c \\ d \end{pmatrix}$ が書かれていたとしましょう。この等式の定義は「実数の等号 $a = c$ と $b = d$ が二つとも成立する」ということですね。

例えば、上のベクトルの等号を証明せよ、と言われたら、成分の一致（後者の実数の等号）を示すのが基本手段ですよね。基本手段は、あくまで、基本で、両辺のベクトルの由来によっては別の手段が有効な場合もあります。けれども、基本手段がなんであるかを理解することは大切ですね。

今から部分集合の等号の定義を与えます。部分集合の等号を示す基本手段の解説をおもってください。

まず包含関係 $Z \subset Y$ の定義を与えます。

**定義 2.6** (部分集合の包含関係)**.** $X$ を集合とし、$Y, Z$ を $X$ の部分集合とする。
このとき「$Z \subset Y$」と書けば「$Z$ の任意の要素は $Y$ の要素である」ことを意味する。

等号の定義は次です。

**定義 2.7** (部分集合の等号)**.** $X$ を集合とし、$Y, Z$ を $X$ の部分集合とする。
このとき「$Y = Z$」と書けば「$Y \subset Z$ かつ $Z \subset Y$」を意味する。

**例 2.8.** 例 *2.3* の部分集合 $Y$ と例 *2.4* の部分集合 $Z$ とは同じ部分集合ですよね。皆さんは直感的に納得するとおもいますが、等号 $Y = Z$ を上に与えた定義に基づいて読んでいきます。

その前に言っておくことがあります。部分集合 $Y$ は方程式を満たすベクトル全体として与えられ、部分集合 $Z$ は属する要素の記述が与えられています。なんとなく感じ取れるとおもいますが、等号 $Y = Z$ を立証するというのが方程式を解くということなんですね。

このような由来をそれぞれが持っているので、単に等式 $Y = Z$ とサラっと書けますが意味するところは大きいのです。部分集合の等号 $Y = Z$ の意味するところをボチボチ読み解いていきましょう。

*(I)* 部分集合の等号 $Y = Z$ の意味は包含関係 $Y \subset Z$ と $Z \subset Y$ が二つとも成立することであった。これら二つの記号を読み解く必要が出てくる。

*(II)* 部分集合の等号 $Y = Z$ の意味は、（包含関係 $Y \subset Z$ と $Z \subset Y$ が二つとも成立するということであり、その意味というのは）以下の二つがともに成り立つということである。

*(i)* $Y$ の任意の要素は $Z$ の要素である。

*(ii)* $Z$ の任意の要素は $Y$ の要素である。

この意味を明確にするには部分集合 $Y, Z$ の定義を紐解くことになる。

*(III)* 部分集合の等号 $Y = Z$ の意味は、（包含関係 $Y \subset Z$ と $Z \subset Y$ が二つとも成立するということであり、その意味というのは）以下の二つがともに成り立つということである。

*(i)* 2 次元実数ベクトル $\vec{x} = \begin{pmatrix} x \\ y \end{pmatrix}$ で座標の値 $x, y$ が関係式 $x + y = 1$ を満たすもの（$Y$ の要素）はある実数 $s$ が存在して $\begin{pmatrix} s+1 \\ -s \end{pmatrix}$ の形に表せる（$Z$ の要素である）。

*(ii)* ある実数 $s$ が存在して $\begin{pmatrix} s+1 \\ -s \end{pmatrix}$ の形に表せる 2 次元実数ベクトル（$Z$ の要素）は座標の値 $x, y$ が関係式 $x+y=1$ を満たす 2 次元実数ベクトル $\vec{x} = \begin{pmatrix} x \\ y \end{pmatrix}$ である（$Y$ の要素である）。

（終わり）

いざ書き下してみると大変ですね。パソコン上でファイルを開いてその中のファイルを開いて、またその中のファイルを開いてやっと実態のあるテキストに辿り着く、という感じです。

強調しておくべきことは二つあります：

- 最初は面倒だけれど、すぐになれます。

  また、部分集合の等号を議論することは前期はあまりないです。なので、難しく感じても心配はまったくありません。

- こういうことが必要です。（わけもなく難しいことをやってるのではないのです。）

  上の例では方程式との関係に注意しました。「方程式を解く」というのは「条件式を満たす数を全て過不足なく見つけ出す」ということですね。「過不足ない」というのは、つまり、多すぎてもいけないし、少なすぎてもいけない、ということです。

  上の例だと *(i)* は「方程式 $x+y=1$ の解はすべて $x=s+1, y=-s$ の形に表せる」といっているので、つまり、解の表示 $\vec{x}_s$ $(s \in \mathbb{R})$ が少なすぎない、ということなのです。

  上の例の *(ii)* は「$x=s+1, y=-s$ の形のものはすべて方程式 $x+y=1$ の解である」といっているので、つまり、解の表示 $\vec{x}_s$ $(s \in \mathbb{R})$ が多すぎない、ということなのです。

## 2.6 共通部分集合、和集合、非交和

### 2.6.1 共通部分

集合 $X$ の部分集合 $X_1, X_2 \subset X$ が与えられたとき共通部分集合 $X_1 \cap X_2$ が定義されました。

「$x \in X_1 \cap X_2$」と書けば「$x \in X_1$ かつ $x \in X_2$」と同じ意味になるのでした。

共通部分をとる集合は二つ以上でもよかったですね。$n$ 個の部分集合 $X_1, \cdots, X_n \subset X$ の共通部分集合を $\bigcap_{n=1}^{n} X_i$ とあらわすこともあります：

$$\bigcap_{i=1}^{n} X_i = X_1 \cap X_2 \cap \cdots \cap X_n.$$

### 2.6.2 和集合

集合 $X$ の部分集合 $X_1, X_2 \subset X$ が与えられたとき和集合 $X_1 \cup X_2$ が定義されました。

「$x \in X_1 \cup X_2$」と書けば「$x \in X_1$ または $x \in X_2$」と同じ意味になるのでした。

和をとる集合は二つ以上でもよかったですね。$n$ 個の部分集合 $X_1, \cdots, X_n \subset X$ の和集合を $\bigcup_{n=1}^{n} X_i$ とあらわすこともあります：

$$\bigcup_{i=1}^{n} X_i = X_1 \cup X_2 \cup \cdots \cup X_n.$$

### 2.6.3 非交和 (disjoint union)

**定義 2.9.** 部分集合 $X_1, X_2$ が $X_1 \cap X_2 = \emptyset$ を満たす場合には合併集合を $X_1 \sqcup X_2$ とあらわし非交和とよぶ。

ものとしてはただの合併集合ですが、特別な条件を満たすことが記号に込められています。

**定義 2.10.** 部分集合 $X_1, X_2, \cdots, X_n$ が $X_i \cap X_j = \emptyset,\ (i \neq j)$ を満たす場合には合併集合を $\bigsqcup_{i=1}^{n} X_i$ とあらわし非交和とよぶ。

ものとしてはただの合併集合ですが、特別な条件を満たすことが記号に込められています。

さらには合併する部分集合が無限個ある場合でも同様です。

# 3 写像

写像に関する補足です。

写像も集合と同じく簡単な概念です。簡単すぎて取り止めがなくて把握したという実感を持ちにくいので、分からないと感じてしまうかもしれません。写像の方が集合よりも覚えることが多いですが、同じく、使いながらボチボチ慣れていきましょう。

関数というのは皆さんよくご存知で、写像というのはその抽象化です。関数というものの性質のある一部を取り出したのが写像というものなんですね。まず、関数を振り返りましょう。

## 3.1 「関数ってなんですか？」

「関数ってなんですか？」って尋ねられらたら、皆さんはなんと答えるでしょうか？

「三角関数とか指数関数とか対数関数とか、そういうのが関数」って返答が思い浮かぶ人が大半だとおもいます。この解答が不十分です。これらはあくまでも関数の例であって関数という概念自体の説明ではないですよね。三角関数・指数関数・対数関数以外の関数が他にもある、というのは不十分さの理由ではありません。（不可能なことですが）関数の例をすべて挙げることができても、関数というのがなんであるかを答えたことにはなりません。関数と呼ばれる資格がなんであるのかを答えないといけないのです。

資格とかって持って回った偉そうな言い方をしてしまいましたが、やりたいことは三角関数・指数関数・対数関数やその他の関数と呼ばれているものを一遍につかみ取ることです。

関数 $f$ というものの一番素朴なポイントは何かっていうことですが、それは実数 $x$ に実数 $f(x)$ を対応させている、ということです。確かに、考えてみると、実数 $x$ にたいして $e^x, \sin x, \cos x$ etc. は実数ですね。ともかく、定義を与えましょう。

**定義 3.1** (（定義域が実数全体の）関数)**.** 関数 $f$ とは各実数 $x \in \mathbb{R}$ にたいしてそれぞれ実数 $y \in \mathbb{R}$ をひとつ対応させる規則である。

関数 $f$ により $x \in \mathbb{R}$ に対応する実数 $y \in \mathbb{R}$ を $f(x)$ とあらわす。

指数関数 $e^x$, 正弦関数 $\sin x$, 余弦関数 $\cos x$, は各実数 $x \in \mathbb{R}$ にたいしてそれぞれ実数を対応させていますね。なのでこれらは定義 3.1 の意味で関数なのです。

**注意 3.2.** 上の定義では関数の定義域を実数全体の場合しか考えていません。

正接関数 $\tan x$ は部分集合 $\{\pi\left(n + \frac{1}{2}\right) \mid n \in \mathbb{Z}\}$ において定義されていないし、対数 $\log x$ は部分集合 $\{x \in \mathbb{R} \mid x \leq 0\}$ において定義されていません[2]。そういう意味で、この二つは上の定義には当てはまりません。

定義域・値域については写像を定義する段階で気にすることにします。

[2]部分集合の読み方に慣れていきましょう。

### 3.1.1 注意：関数とグラフとは別のもの !!

関数 $y = f(x)$ とそのグラフは別のものです。当たり前といえば当たり前ですが、混同してる人は多いような気がします。高校までの関数の扱いからはそれも無理もないことですが、別物であることを意識しておいてください。関数をグラフと混同していると、関数とは規則である、という定義が意味不明ですよね。

関数を調べるときにグラフは強力な武器になるし、また、関数のグラフの性質自体が求めたいものである場合もあります。なので、関数のグラフを扱うこと自体を否定してるわけではありません。

### 3.1.2 名もなき関数

例によって関数にも名もなき関数があります。関数 $f$ というのは単にそれぞれの実数 $x \in \mathbb{R}$ にたいしなにか実数 $f(x)$ をひとつ決めるだけのものなので、いくらでもあります。関数 $f$ といっただけでは、それが何らかの数式により与えられるとか、綺麗にまとめて書く方法があるとか、そういうことは全く要請しないのです。

## 3.2 写像

関数の定義（定義 3.1）で実数の集合 $\mathbb{R}$ が現れたところを任意の集合に置き換えることで得られます。ただ、定義域と値域とを指定しなければいけないので文言は若干長くなります。

**定義 3.3** (写像)**.** $X$ と $Y$ を集合とする。

集合 $X$ を定義域とし集合 $Y$ を値域とする写像 $f$ とは $X$ の各要素 $x \in X$ にたいして $Y$ の要素 $y \in Y$ を対応させる規則である。

記号・記法：

*(1)* 上のように写像 $f$ が与えらている状況を $f : X \to Y$ とあらわす。

すなわち、「写像 $f : X \to Y$」と書けば「$X, Y$ は集合であり、$f$ は $X$ を定義域、$Y$ を値域とする写像である」という意味です。

*(2)* 写像 $f$ により $x \in X$ に対応する $Y$ の要素を $f$ による $x$ の像と呼び $f(x)$ とあらわす。

あるいは $x \mapsto f(x)$ ともあらわす。

（矢印の根本に縦線があるのがポイントです。）

関数っていうのは写像ですね。

**例 3.4.** 定義 *3.1* で与えた関数というのは写像 $f : \mathbb{R} \to \mathbb{R}$ に他ならない。

他にも写像って沢山たくさんあります。有名な写像も名もなき写像も無数にあります。

### 3.2.1 恒等写像

**定義 3.5** (恒等写像)**.** 集合 $X$ にたいして写像 $\mathrm{id}_X : X \to X$ を

$$\mathrm{id}_X(x) := x \text{ for all } x \in X$$

で定め、これを**恒等写像**と呼ぶ。

### 3.2.2　全射、単射、全単射

**定義 3.6.** *(1)* 写像 $f : V \to U$ が**全射**とは任意の $u \in U$ に対してある $v$ が存在して $u = f(v)$ を満たすことと定める。

*(2)* 写像 $f : V \to U$ が**単射**とは $v_1, v_2 \in V$ が $f(v_1) = f(v_2)$ を満たせば $v_1 = v_2$ が成り立つことと定める。

*(3)* 写像 $f : V \to U$ が**全単射**とは全射かつ単射であることと定める。

**例 3.7.** 集合 $X$ の恒等写像 $\mathrm{id}_X$ は全単射である。

## 3.3　合成写像

二つの写像 $f : X \to Y,\ g : Y \to Z$ が与えられていて、$f$ の値域と $g$ の定義域が一致している場合、この写像をつなげて新たな写像 $g \circ f$ を作れます。定義は次です。

$$(g \circ f)(x) := g(f(x)) \text{ for all } x \in X.$$

この構成を写像の合成と呼び、得られる写像を合成写像と言い、記号では $g \circ f$ と書きます。

もう少し説明すると、この様に定義する気持ちは次です。

$$X \xrightarrow{\text{f で送ったものを}} Y \xrightarrow{\text{更に g で送る}} Z.$$

$X$ の要素 $x$ の $f$ による像 $f(x)$ を $y$ とおきましょう、（つまり、$y = f(x)$ と定義します。）これは $Y$ の要素です。更に、$y$ の $g$ による像 $g(y)$ を $z$ とおきます。つまり、$z = g(y)$ と定義します。すると、$x$ を $f$ で $Y$ に送り、更にそいつを $g$ で $Z$ に送ったものは、$z$ になります。これが合成写像 $g \circ f$ による $x$ の像です。つまり、

$$(g \circ f)(x) = g(y) = g(f(x))$$

となる訳です。

例を挙げると、写像 $f, g : \mathbb{R} \to \mathbb{R}$ を $f(x) = \cos x, g(x) = x^3$ と定義すると合成写像は

$$(f \circ g)(x) = \cos(x^3), \quad (g \circ f)(x) = \cos^3 x.$$

となります。

次のことが基本的です。

**命題 3.8** (結合法則)**.** 写像 $f : X \to Y, g : Y \to Z, h : Z \to W$ を考える。次の等式が成り立つ。

$$(h \circ g) \circ f = h \circ (g \circ f).$$

**命題 3.9** (恒等写像との合成)**.** 写像 $f : X \to Y$ を考える。次の等式が成り立つ。

$$f \circ \mathrm{id}_X = f,\ \mathrm{id}_Y \circ f = f.$$

## 3.4　写像の集合

**定義 3.10.** $X, Y$ を空集合でない集合とする。$X$ から $Y$ への写像の集合を $\mathrm{Hom}_{\mathrm{Set}}(X, Y)$ と表す。

$$\mathrm{Hom}_{\mathrm{Set}}(X, Y) := \{f : X \to Y \mid f \text{ 写像 }\}.$$

**練習問題 3.11.** $X, Y$ が有限集合の場合には次が成り立つ：

$$|\mathrm{Hom}_{\mathrm{Set}}(X, Y)| = |Y|^{|X|}.$$

### 3.4.1 空集合を定義域、値域とする写像

写像というのは要素を要素に対応させる規則でした。要素を持たない集合、つまり、空集合 $\emptyset$ だけは例外的に扱わないといけなくなります。

写像（等）の定義の読み方を工夫して通常の定義から以下で導入することを導出するという流儀もあるのですが、この講義では個別に定義することにします。

**定義 3.12.** *(1)* 空集合 $\emptyset$ から集合 $X$ への写像は一つだけ存在すると定める。

$$|\operatorname{Hom}_{\mathrm{Set}}(\emptyset, X)| = 1$$

*(2)* 唯一ある写像を $f : \emptyset \to X$ と書くことにすると、これは単射であると定める。

*(3)* 唯一ある写像を $f : \emptyset \to X$ と書くことにする。これが全射であるための必要十分条件は $X = \emptyset$ であると定める。

*(4)* $X = \emptyset$ の場合には唯一ある写像 $f : \emptyset \to \emptyset$ を $\emptyset$ の恒等写像とよび $\mathrm{id}_\emptyset$ とかく。

**定義 3.13.** 空集合でない集合 $X \neq \emptyset$ から空集合 $\emptyset$ への写像は存在しないと定める。

$$\operatorname{Hom}_{\mathrm{Set}}(X, \emptyset) = \begin{cases} \emptyset & (X \neq \emptyset) \\ \{\mathrm{id}_\emptyset\} & (X = \emptyset) \end{cases}$$

## 3.5 逆写像

**定義 3.14.** 写像 $f : X \to Y$ の**逆写像**とは $f$ の値域 $Y$ を定義域とし $f$ の定義域 $X$ を値域とする写像 $g : Y \to X$ であり次が成り立つものと定める。

$$f \circ g = \mathrm{id}_Y,\ g \circ f = \mathrm{id}_X\,. \tag{3-1}$$

つまり、逆写像 $g : Y \to X$ とは合成写像 $f \circ g : Y \to X \to Y$ と $g \circ f : X \to Y \to X$ が恒等写像であるものである。

上の写像の等式 (3-1) は要素を使うと次のように言い換えられますね：

$$(f \circ g)(y) = y \text{ for all } y \in Y, \qquad (g \circ f)(x) = x \text{ for all } x \in X$$

**命題 3.15.** *(1)* 写像 $f : X \to Y$ の逆写像は存在すれば一意的である。

*(2)* 写像 $f : X \to Y$ の逆写像が存在する為の必要十分条件は $f$ が全単射であることである。

つまり、逆写像は、若し存在すれば、ただ一つしかないので $f$ から定まると言ってよく、記号でも写像 $f$ の逆写像を $f^{-1}$ と書きます。

## 3.6 像と逆像

**定義 3.16.** 写像 $f : X \to Y$ を考える。

*(1)* $X$ の部分集合 $S \subset X$ にたいして $Y$ の部分集合 $f(S)$ を次で定め $S$ の $f$ **による像**とよぶ：

$$f(S) := \{y \in Y \mid \exists s \in S \text{ s.t } y = f(s)\} = \{f(s) \mid s \in S\}$$

*(2)* $Y$ の部分集合 $T \subset Y$ にたいして $X$ の部分集合 $f^{-1}(T)$ を次で定め $T$ の $f$ **による逆像**とよぶ：

$$f^{-1}(T) = \{x \in X \mid f(x) \in T\}.$$

**注意 3.17.** 逆像と逆写像の区別をつけよう。

**例 3.18.** 写像 $f : X \to Y$ を考える。すると次の等式がなりたつ：

$$X = \bigsqcup_{y \in Y} f^{-1}(\{y\}). \tag{3-2}$$

## 3.7 べき集合

**定義 3.19.** 集合 $X$ の部分集合のなす集合を**べき集合**と呼び $\mathcal{P}(X)$ であらわします。

$$\mathcal{P}(X) := \{S \mid S \subset X\}.$$

つまり、集合 $X$ が先に与えらえているときに、文章「$S \in \mathcal{P}(X)$」を普通の言葉になおすと「$S$ は $X$ の部分集合である。」です。
注意することは集合 $X$ の部分集合には自分自身 $X$ と空集合 $\emptyset$ もあるということです。

**例 3.20.** *(1)* 一点集合 $X = \{a\}$ のべき集合 $\mathcal{P}(X)$ は次の様に書き下すことが出来ます。

$$\mathcal{P}(X) := \{\ \emptyset,\ \{a\}\ \}$$

*(2)* 二点集合 $X = \{a, b\}$ のべき集合 $\mathcal{P}(X)$ は次の様に書き下すことが出来ます。

$$\mathcal{P}(X) := \{\ \emptyset,\ \{a\},\ \{b\},\ \{a, b\}\ \}$$

*(3)* 三点集合 $X = \{a, b, c\}$ のべき集合 $\mathcal{P}(X)$ は次の様に書き下すことが出来ます。

$$\mathcal{P}(X) := \{\ \emptyset,\ \{a\},\ \{b\},\ \{c\},\ \{a, b\}\ \{b, c\},\ \{c, a\},\ \{a, b, c\}\ \}$$

少し考えてみると次が分かります：

**命題 3.21.** 有限集合 $X$ のべき集合 $\mathcal{P}(X)$ の要素の個数は次で与えられる：

$$\#\mathcal{P}(X) = 2^{|X|}.$$

この命題は特性写像というものを導入すると見通し良く証明できます。

### 3.7.1 特性写像

**定義 3.22.** 集合 $X$ とその部分集合 $S$ にたいして特性写像 $\chi_S : X \to \{0, 1\}$ を次で定める：

$$\chi_S(x) := \begin{cases} 1 & (x \in S) \\ 0 & (x \notin S) \end{cases}$$

次の命題は集合が無限でもなりたちます：

**命題 3.23.** 集合 $X$ を考える。写像

$$\chi_{(-)} : \mathcal{P}(X) \to \mathrm{Hom}_{\mathrm{Set}}(X, \{0, 1\}),\ S \mapsto \chi_S$$

と写像

$$\iota : \mathrm{Hom}_{\mathrm{Set}}(X, \{0, 1\}) \to \mathcal{P}(X),\ f \mapsto f^{-1}(\{1\})$$

は互いにもう一方の逆写像である。特にこれらは全単射である。

# 4 同値関係

イコール $=$ の持ってる性質を抽象化して同値関係という概念を定義します。集合の要素のクラス分けを考えるさいに、同じクラスに属する要素を同じ（同値関係がある）とみなします。

### 4.0.1 前置き：集合の要素のクラス分け

集合というのは要素のあつまりでした。今回は要素のクラス分けを考えます。学校というのが学生があつまったものである、というようなイメージをとると、本当に学生を何組何組とクラス分けすることになります。やることは簡単ですね。

**定義 4.1.** 集合 $X$ の**クラス分け**とは部分集合族 $\{X_i \subset X\}_{i\in I}$ で $X = \bigsqcup_{i\in I} X_i$ を満たすもののことをいうことにします。

**例 4.2.** 写像 $f : X \to Y$ が与えられれば逆像の族 $\{f^{-1}(\{y\}) \mid y \in Y\}$ によるクラス分けができますね。

### 4.0.2 関係

**定義 4.3.** 集合 $X$ にたいして部分集合 $R \subset X \times X$ のことを**関係**とよぶ。
*[記号]* 要素 $x, y \in X$ にたいして $(x, y) \in R$ がなりたつことを $x \sim y$ とあらわすことにする。
この記号法の下で部分集合 $R \subset X \times X$ を記号 $\sim$ であらわしたりする。

**例 4.4.** *1. [等号]* 一番なじみの深い関係は等号 $=$ ですね。

集合 $X$ にたいして部分集合 $R$ を以下で定めるます。

$$R := \{(x, x) \in X \times X \mid x \in X\}.$$

すると、この $R$ にたいして $(x, y) \in R$ をみたすような $x, y \in X$ は $x = y$ をみたすものであり、それのみに限られますよね。

*2. [大小関係]* 実数の大小関係も同じく次の部分集合であらわされます：

$$R := \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}.$$

### 4.0.3 同値関係

**定義 4.5.** 集合 $X$ の**同値関係** $\sim$ とは、関係（部分集合）$R \subset X \times X$ で次を満たすものと定める：

*1.* （反射律） $x \sim x$ が任意の $x \in X$ にたいしてなりたつ。

*2.* （対称律）要素 $x, y \in X$ が $x \sim y$ を満たせば $y \sim x$ がなりたつ。

*3.* （推移律）要素 $x, y, z \in X$ が $x \sim y, y \sim z$ をみたせば $x \sim z$ がなりたつ。

**定義 4.6.** 集合 $X$ に同値関係 $\sim$ が与えられているとする。

*(1)* 要素 $x \in X$ にたいして $X$ の部分集合 $[x]$ を以下で定め、同値関係 $\sim$ に関する**$x$ の同値類**とよぶ。

$$[x] := \{y \in X \mid y \sim x\}.$$

*(2)* 集合 $X$ に同値関係 $\sim$ が与えられているとき、同値関係 $\sim$ に関する**商集合** $X/\sim$ を次で定める。

$$X/\sim := \{[x] \in \mathcal{P}(X) \mid x \in X\}.$$

（べき集合 $\mathcal{P}(X)$ の部分集合で同値類 $[x]$ 全部からなるものです。）

（つまり、「$A \in X/\sim$」というのは「$A$ は $X$ の部分集合であり、ある $x \in X$ が存在して $A = [x]$ を満たす」という意味です。）

*(3)* 写像 $\pi : X \to X/\sim,\ \pi(x) := [x]$ を同値関係 $\sim$ に関する<u>商写像</u>とよぶ。（商写像は全射である。）

*(4)* 同値関係 $\sim$ に関する<u>完全代表系</u> $S$ とは次の条件を満たす $X$ の部分集合をいう：
任意の $x \in X$ にたいしてある $s \in S$ が一意的に存在して $x \sim s$ をみたす。

**練習問題 4.7.** 集合 $X$ に同値関係 $\sim$ が与えられているとする。

*(1)* 要素 $x, y \in X$ にたいして次の 2 条件は同値であることを示せ。

*(a)* $x \sim y$.
*(b)* $[x] = [y]$.

*(2)* 部分集合 $S \subset X$ にたいして次の 2 条件は同値であることを示せ。

*(a)* $S$ は同値関係 $\sim$ に関する完全代表系である。
*(b)* 同値関係 $\sim$ に関する商写像 $\pi : X \to X/\sim$ を $S$ に制限した写像 $\pi|_S : S \to X/\sim$ は全単射である。

*(3)* 商写像 $\pi : X \to X/\sim$ による部分集合 $\{[x]\} \subset X/\sim$ の逆像 $\pi^{-1}(\{[x]\})$ は部分集合 $[x] \subset X$ であることをしめせ。

**補題 4.8.** 集合 $X$ に同値関係 $\sim$ が与えられているとする。次が成り立つ：

*(1)* 完全代表系 $S$ が存在する。

*(2)* 完全代表系 $S$ により $X$ を同値類でクラス分けすることができる。つまり、次の等式がなりたつ：

$$X = \bigsqcup_{x \in S} [x].$$

**練習問題 4.9.** 集合 $X$ にクラス分け $X = \bigsqcup_{i \in I} X_i$ が与えられているとする。次を示せ。

*(1)* $X$ に関係 $\sim$ を以下で定めると、これは同値関係であることをしめせ。
二つの要素 $x, y \in X$ にたいして、

$$x \sim y :\Longleftrightarrow \exists i \in I \text{ s.t. } x, y \in X_i.$$

*(2)* $x \in X_i$ とすれば *(1)* で定めた同値関係に関して $[x] = X_i$ がなりたつ。

商集合に関して大切なのが次の命題です。

**命題 4.10.** 集合 $X$ に同値関係 $\sim$ が与えられているとする。この時、写像 $f : X \to Y$ にたいして次の 2 条件は同値である：

1. $x_1, x_2 \in X$ が $x_1 \sim x_2$ を満たせば $f(x_1) = f(x_2)$ が成り立つ。
2. 写像 $\overline{f} : X/\sim \to Y$ が存在して $f = \overline{f} \circ \pi$ を満たす。

さらに、この条件が満たされるとき、写像 $g : X/\sim \to Y$ が存在して $f = g \circ \pi$ を満たすものは一意的である。

## 4.1　イメージ：学校 $X$ のクラス分け。

ここまででやってきたことのイメージを説明しておきます。

集合 $X$ を学校だとかなんだとかの学生の集まりとすると、そのクラス分け $X = \bigsqcup_{i\in I} X_i$ というのは本当の意味でのクラス分けにあたります。各部分集合 $X_i$ が一つのクラスで、学生みんなは必ずどれか一つのクラスに属していて、しかも、二つ以上のクラスに属していない状態にあることを非交和であらわしています。

このクラス分けにたいして Exercise 4.9 で定めた同値関係 $\sim$ を考えます。つまり「$x_1 \sim x_2$」という文章が「ある $i$ が存在して $x_1, x_2 \in X_i$ がなりたつ」を意味するものとして記号 $\sim$ を定義します。平たく言えば「$x_1$ さんと $x_2$ さんがクラスメイトである」ということを「$x_1 \sim x_2$」であらわすことに規約します。

同値関係の定義に現れた三つの条件は今の場合にはごく当たりまえのことをいっています。反射率は「$x$ さんは $x$ さん自身とクラスメイトである」、対称律は「$x_1$ さんと $x_2$ さんがクラスメイトであれば、$x_2$ さんと $x_1$ さんはクラスメイトである」推移律は「$x_1$ さんと $x_2$ さんがクラスメイトであり $x_2$ さんと $x_3$ さんはクラスメイトであれば、$x_1$ さんと $x_3$ さんはクラスメイトである。」同値関係というのはこの当たり前の性質を抽象化したものなのです。

記号 $[x]$ はある学生 $x \in X$ さんの属するクラスをあらわします。つまり $x$ さんがクラス $X_i$ に所属していることを $[x] = X_i$ であらわしています。普通の生活でもクラス名を「何年何組」と言う代わりに「$x$ さんのいるクラス」と言ったりしますが、それと同じことです。注意したいのは $x_1$ さんと $x_2$ さんが別の人でも $[x_1] = [x_2]$ となることがあるといことです。（そりゃそうですね。）

完全代表系 $S$ を決めるというのは各クラスから一人ずつ代表を選ぶことです。すると、クラス分けの等式 $X = \bigsqcup_{x\in S}[x]$ というのは各クラスの代表により学校 $X$ のクラス分けを表示する式ということがわかりますね。

商集合 $X/\sim$ というのはクラスの集合です。各クラスを一つの点とみなして、それらを集めて集合を作っています。クラスの名前の集合といったほうがわかりやすい人もいるかもしれません。

### 4.1.1　商集合の取り扱い：集団行動（Proposition 4.10）

商集合 $X/\sim$ の扱いを説明します。

学校 $X$ の学生が旅行にいく場面をイメージしてください。$Y$ を県名の集合としましょう：

$$Y = \{\text{兵庫、大阪、奈良、、、、、、}\}.$$

県単位で移動するというのは現実的でないかもしれないけれど、各学生の旅行先を対応させるという規則により写像 $f : X \to Y$ を定めます。つまり、学生 $x \in X$ にたいして $f(x) \in Y$ は $x$ さんの行き先を表します。

さて、考えたいのは、つぎのことです。

**疑問 4.11.** 旅行がクラス単位のものである、という状況をどう表現できるか？

各クラス $X_i, (i \in I)$ がまとまって移動しているということは、つまり、

「$x_1$ さんと $x_2$ さんが同じクラスならば $f(x_1) = f(x_2)$ が成り立つ。」

ということですね。

上で準備した記号では「$x_1$ さんと $x_2$ さんが同じクラス」というのは「$x_1 \sim x_2$」と簡単に表現できました。なので、上で述べた条件は次のように言い換えられますね：

$$x_1 \sim x_2 \Longrightarrow f(x_1) = f(x_2).$$

これは丁度 Proposition 4.10 で現れた条件ですね。この命題が主張しているのは、上の条件が成り立つときにはこの旅行（＝写像 $f$）がクラス単位の旅行だとみなせるということで、クラスごとの行き先を対応させる写像が $\overline{f} : X/\sim \to Y$ なのです。商集合 $X/\sim$ というのはクラス名の集合でした。写像 $\overline{f}$ は各クラス名にたいしてその行き先を対応させます。

# Part II
# 群論

## 5　群

### 5.1　演算

群というのは（実数とかの）積を抽象化して得られる概念です。実数の積というのは二つの実数$x, y$にある実数$xy$を対応させます。その部分だけを抽象化するとそれは集合$X$にたいして写像$\mu : X \times X \to X$を与えるということになります。

これはつまり$\mu$というのは$X$の二つの要素$x_1, x_2$の組$(x_1, x_2)$にたいしてある$X$の要素$\mu(x_1, x_2)$を対応させる規則です。

そのような例を見ておきましょう。

(1) $\min : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$.

二つの実数の組$(x, y)$にたいしてその小さい方$\min(x, y)$を対応さる規則。

同様に大きい方を対応させても写像ができる。

(2) $p_1 : \mathbb{R} \times \mathbb{R} \to \mathbb{R},\ p_1(x, y) := x$.

二つの実数の組$(x, y)$にたいしてその第一成分を対応させる規則。

同様に第二成分を対応させる規則もありそれを$p_2$とあらわす。

(3) $a : \mathbb{R} \times \mathbb{R} \to \mathbb{R}, a(x, y) := x + y$

(4) $\mu : \mathbb{R} \times \mathbb{R} \to \mathbb{R}, \mu(x, y) := xy$

### 5.2　群

群の定義。

**定義 5.1.** 群$G$とは 2 つ組み$G = (G, \mu)$

- $G$は集合、
- $\mu : G \times G \to G$は写像

であり、次の公理を満たすものの事である：

*(I)* *[積の結合法則]*

$$\mu(g_1, \mu(g_2, g_3)) = \mu(\mu(g_1, g_2), g_3) \text{ for } \forall g_1, g_2, g_3 \in G.$$

*(II)* *[単位元の存在]*

$$\exists e \in G \text{ s.t. } \mu(e, g) = g, \mu(g, e) = g \text{ for } \forall g \in G.$$

*(III)* *[逆元の存在]*

$$\text{For } \forall g \in G,\ \exists h \in G \text{ s. t. } \mu(g, h) = e, \mu(h, g) = e.$$

以降は、群 $(G,\mu)$ の下部集合 $G$ の要素 $g,h\in G$ にたいして

$$gh:=\mu(g,h)$$

とかくことにする。

さらに、群 $(G,\mu)$ を $G$ という記号で代表させる。

（しかし、その背後には積があることを忘れてはいけない。また、積以外はないことも忘れてはいけない。）

**練習問題 5.2.** 群の公理を $\mu$ を使わずに書いてみる。

**命題 5.3.** 群 $G$ の単位元は一意的である。

つまり、下部集合の要素 $e,e'\in G$ が

$$eg=g,ge=g,e'g=g,ge'=g\quad\forall g\in G$$

を満たせば $e=e'$ が成り立つ。

*Proof.* 以下の式変形により $e=e'$ が示される：

$$e=ee'=e'.$$

□

**命題 5.4.** 群 $G$ の下部集合の要素 $g\in G$ の逆元は一意的である。

つまり、要素 $h,k\in G$ が

$$gh=e,hg=e,gk=e,kg=e$$

を満たせば $h=k$ がなりたつ。

*Proof.* 以下の式変形により $h=k$ が示される：

$$h=he=hgk=ek=k.$$

□

注意：証明には全ての条件式を使っている訳ではない。

### 5.2.1 指数法則

**定義 5.5.**

$$g^n:=\begin{cases}gg\cdots g\quad n\text{-times} & n\geq 1,\\ e & n=0\\ g^{-1}g^{-1}\cdots g^{-1}\quad -n\text{-times} & n<0.\end{cases}$$

**練習問題 5.6.** 群 $G$ の要素 $g,h\in G$ にたいして次を示せ。

*(1)*

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

*(2) For $n,m\in\mathbb{Z}$ we have*

$$g^{n+m}=g^ng^m,(g^n)^m=g^{nm}.$$

*(3)*

$$g=e\Leftrightarrow g^2=g$$

### 5.2.2 例

**例 5.7.** *(1)* $\min : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$.

二つの実数の組 $(x, y)$ にたいしてその小さい方 $\min(x, y)$ を対応さる規則。

三つの実数 $x, y, z \in \mathbb{R}$ にたいして

$$\min(x, \min(y, z)) = \min(x, y, z) = \min(\min(x, y), z)$$

であるから、この演算は結合法則をみたす。

しかし、演算 min に関する単位元は存在しない。

$\because$ 単位元 $e \in \mathbb{R}$ が存在したとする。$e < e + 1$ より $\min(e, e + 1) = e$ である。一方、単位元の性質より $\min(e, e + 1) = e + 1$ でなくてはならない。よって実数 $e$ は $e + 1 = e$ を満たすことが導出され矛盾。

*(2)* $p_1 : \mathbb{R} \times \mathbb{R} \to \mathbb{R},\ p_1(x, y) := x$.

二つの実数の組 $(x, y)$ にたいしてその第一成分を対応させる規則。

同様に第二成分を対応させる規則もありそれを $p_2$ とあらわす。

三つの実数 $x, y, z \in \mathbb{R}$ にたいして

$$p_1(x, p_1(y, z)) = x = p_1(p_1(x, y), z)$$

であるから、この演算は結合法則をみたす。

しかし、この演算には単位元は存在しない。

*(3)* $a : \mathbb{R} \times \mathbb{R} \to \mathbb{R}, a(x, y) := x + y$

群である。

*(4)* $\mu : \mathbb{R} \times \mathbb{R} \to \mathbb{R}, \mu(x, y) := xy$

結合的で単位元を持つ。しかし、逆元をもたない元がある。

**例 5.8.** 下部集合が二点からなる場合を考える：$G = \{a, b\}$. このとき

$$G \times G = \{(a, a), (a, b), (b, a), (b, b)\}.$$

下の四つを決めることが写像 $\mu : G \times G \to G$ を決めることである：

$$\mu(a, a) =, \mu(a, b) =, \mu(b, a) =, \mu(b, b) =$$

*(1)*

$$\mu(a, a) = b, \mu(a, b) = b, \mu(b, a) = a, \mu(b, b) = a.$$

この演算は結合法則を満たさない：

$$(ab)a = ba = a,\ a(ba) = aa = b.$$

*(2)*

$$\mu(a, a) = a, \mu(a, b) = b, \mu(b, a) = b, \mu(b, b) = b.$$

結合法則がなりたつ。というのは掛け算の中に $b$ が入っていたら結果は $b$ になる。それ以外の場合というのは $a$ だけの積でそれは $a$ に一致する。

また、$a$ が単位元である。

しかし、$b$ の逆元が存在しない。

*(3)*

$$\mu(a, a) = a, \mu(a, b) = b, \mu(b, a) = b, \mu(b, b) = a.$$

これは群である。単位元は $a$. 逆元は $a^{-1} = a, b^{-1} = b$.

### 5.2.3 群の例

**例 5.9.** *(1)* $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$.

*(2)* $\mathbb{R}^n$, $\mathbb{C}^n$.

*(3)* ベクトル空間からスカラー倍を除いたもの。

*(4)* $\mathbb{R}^\times := (\mathbb{R} \setminus \{0\})$, $\mathbb{C}^\times := (\mathbb{C} \setminus \{0\}, \times)$, $\mathbb{Z}^\times := (\{\pm 1\}, \times)$.
$\mathbb{R}, \mathbb{C}, \mathbb{Z}$ の要素で掛け算に関する逆元をもつものの集合と掛け算の組。
より一般に環 $R$ の可逆元の集合と掛け算の組を環 $R$ の乗法群とよび $R^\times$ で表す。

*(5)* $\mathrm{GL}_n(\mathbb{R})$, $\mathrm{GL}_n(\mathbb{C})$

*(6)* $\mathrm{GL}_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) \mid \exists A^{-1} \in M_n(\mathbb{Z})\}$
*Exercise. For* $A \in M_n(\mathbb{Z})$,

$$A \in \mathrm{GL}_n(\mathbb{Z}) \Leftrightarrow \det A = \pm 1$$

*(7)* $\mathrm{Aff}_n(\mathbb{R})$ 下部集合は直積集合 $\mathrm{GL}_n(\mathbb{R}) \times \mathbb{R}^n$. 演算は次で定義する：

$$(A, u)(B, v) := (AB, Av + u)$$

## 5.3 部分群

**定義 5.10.** 群 $G$ の部分群とは部分集合 $H \subset G$ で次の条件を満たすものと定義する：

*(0)* $H \neq \emptyset$.

*(I)* $g, h \in H \Longrightarrow gh \in H$.

*(II)* $g \in H \Longrightarrow g^{-1} \in H$.

群 $G$ の下部集合の部分集合 $H \subset G$ が部分群 $H$ であることを $H < G$ とあらわす。

**補題 5.11.** 群 $G$ の部分群 $H$ には $G$ の単位元 $e$ が属する：

$$e \in H.$$

*Proof.* 部分集合 $H$ は空でないので要素をとってくることができる。
要素 $g \in H$ をとってくる。
公理 (II) より、$g^{-1} \in H$ である。
公理 (I) を $g, g^{-1}$ に適用して $e = gg^{-1} \in H$ を結論する。

□

**補題 5.12.** 群 $G$ の空でない部分集合 $H$ にたいして次の命題は同値：

*(1)* $H$ は $G$ の部分群。

*(2)* 任意の $g, h \in H$ にたいして $gh^{-1} \in H$ がなりたつ。

*(3)* 任意の $g, h \in H$ にたいして $g^{-1}h \in H$ がなりたつ。

*Proof.* (1) ⇒ (2).
(1) の成立を仮定する。
任意の $g, h \in H$ をとってくる。
$H$ は部分群なので、部分群の公理 (2) より $h^{-1} \in H$ である。
よって $g, h^{-1} \in H$ にたいして部分群の公理 (I) を適用して $gh^{-1} \in H$ を結論する。

(2) ⇒ (1).
(2) の成立を仮定する。
主張：$e \in H$
$\because$ $g \in H$ をとってくる。$g, g \in H$ にたいして (2) を適用すると $e = gg^{-1} \in H$ を結論する。

部分群の公理 (0) $H \neq \emptyset$ は仮定されている。

部分群の公理 (II) を確かめる。
$g \in H$ をとってくる。$e, g \in H$ にたいして (2) を適用すると $g^{-1} = eg^{-1} \in H$ を結論する。

部分群の公理 (I) を確かめる。$g, h \in H$ とする。すでに公理 (II) の成立を仮定しているので $h^{-1} \in H$ である。
$g, h^{-1} \in H$ にたいして (2) を適用して $gh = g(h^{-1})^{-1} \in H$ を結論する。

(1) ⇔ (3) も同様に確認できる。

□

部分群には $G$ の積を制限する事で群の構造が入る。部分群という時には何も言わなくても常にこの構造を入れる。

### 5.3.1 例

**例 5.13.** 群 $G$ 自身も部分群である。また、単位元のみからなる部分集合 $\{e\}$ も部分群である。

$$\{e\} < G, \quad G < G.$$

**補題 5.14.** *(1)* $H$ が $G$ の部分群であるとする。部分集合 $K \subset H$ にたいして次の命題は同値：

*(a)* $K < H$.
*(b)* $K < G$.

*(2)* 部分群 $H, K < G$ の共通部分 $H \cap K$ は $G$ の部分群である。

*Proof.* (1) 省略。

(2) 部分集合 $H \cap K \subset G$ が補題 5.12(2) をみたすことを確かめる。

空集合でないこと：$e \in H$ かつ $e \in K$ なので $e \in H \cap K$ である。よって $H \cap K \neq \emptyset$ を結論する。

$g, h \in H \cap K$ をとってくる。
$g, h \in H$ であるので補題 5.12 より、$gh^{-1} \in H$ である。
$g, h \in K$ であるので補題 5.12 より、$gh^{-1} \in K$ である。
以上より、$gh^{-1} \in H$ かつ $gh^{-1} \in K$ が示されたので $gh^{-1} \in H \cap K$ を結論する。

□

**練習問題 5.15.** $H, K$ を $G$ の部分群とする。和集合 $H \cup K$ が $G$ の部分群ならば、$H \subset K$ *or* $K \subset H$ のいずれかが成り立つ。

### 5.3.2 具体的な例

**例 5.16.**

$\mathbb{Z} < \mathbb{R} < \mathbb{C}$

$\mathbb{Z}^\times < \mathbb{R}^\times < \mathbb{C}^\times$

$S^1 = \{z \in \mathbb{C} \mid |z| = 1\} < \mathbb{C}^\times$

**例 5.17.** 体 $K$ 上で考える。体を知らない場合は $K = \mathbb{R}, \mathbb{C}$ としてください。
ベクトル空間 $V = (V.+, \cdot)$ からスカラー倍を外したもの $V = (V, +)$ は群である。
ベクトル空間 $V = (V, +, \cdot)$ の（線形代数で導入したベクトル空間としての）部分空間 $U$ は群 $V = (V, +)$ の部分群である。

群 $V = (V, +)$ の部分群がすべてこのように得られるとは限らない。

例：$K = \mathbb{R}$. 1 次元空間 $\mathbb{R} = (\mathbb{R}, +, \cdot)$ から群 $\mathbb{R} = (\mathbb{R}, +)$ を作る。
この群は環 $\mathbb{R}$ の加法群である。
この群の部分群として $\mathbb{Z}$ がある。これはベクトル空間 $\mathbb{R}$ の部分空間に由来しない。

**例 5.18** (一般線形群の部分群)**.** *(1)* 部分集合 $\mathrm{SL}(n; R) := \{A \in \mathrm{GL}(n; R) \mid \det A = 1\}$ は $\mathrm{GL}(n; R)$ の部分群である。

この群を $n$ 次特殊線形群 *(special linear group)* と呼ぶ。

*(2)* 部分集合 $O(n) := \{A \in M(n; \mathbb{R}) \mid ({}^tA)A = E_n\}$ は $\mathrm{GL}(n; \mathbb{R})$ の部分群である。

この群を $n$ 次直交群とよび、要素を直交行列とよぶ。

（${}^tA$ は転置行列。部分群であることは実数体 $\mathbb{R}$ 以外の一般の可換環 $R$ で成り立つけれど、直交群ということばは $R = \mathbb{R}$ の場合を指す。）

*(3)* 部分集合 $SO(n; R) := \{A \in M(n; R) \mid ({}^tA)A = E_n, \det A = 1\}$ は $\mathrm{GL}(n; R)$ の部分群である。

この群を $n$ 次特殊直交群とよび、要素を特殊直交行列とよぶ。

*(4)* 自然数 $n \geq 1$ にたいして $2n$ 次正方行列 $J_{2n}$ を $J_{2n} := \begin{pmatrix} 0 & E_n \\ -E_n & 0 \end{pmatrix}$ で定める。

部分集合 $\mathrm{Sp}(2n; R) := \{A \in M(2n; R) \mid {}^tAJ_{2n}A = J_{2n}\}$ は $\mathrm{GL}(n; R)$ の部分群である。

この群を $2n$ 次シンプレクティック群とよぶ。

*(5)* 次がなりたつ：

$$\mathrm{Sp}(2; R) = \mathrm{SL}(2; R).$$

## 5.4 部分集合で生成される部分群

**定義 5.19** (部分集合が生成する部分群)**.** 群 $G$ の下部集合の空でない部分集合 $S \subset G$ にたいして部分集合 $\langle S \rangle \subset G$ を以下で定義する：

$$\langle S \rangle := \{ s_1^{p_1} s_2^{p_2} \cdots s_n^{p_n} \in G \mid s_1, s_2, \cdots, s_n \in S,\ p_1, p_2, \cdots, p_n \in \mathbb{Z} \}.$$

$\langle S \rangle$ を $S$ で**生成される部分群**とよぶ。

文章「$g \in \langle S \rangle$」の意味は次ですね。
「ある $s_1, s_2, \cdots, s_n \in S,\ p_1, p_2, \cdots, p_n \in \mathbb{Z}$ が存在して

$$g = s_1^{p_1} s_2^{p_2} \cdots s_n^{p_n}$$

をみたす。」

**補題 5.20.** *(1)* $\langle S \rangle$ は部分群である。

*(2)* $S_1 \subset S_2 \ \Rightarrow\ \langle S_1 \rangle \subset \langle S_2 \rangle$.

*(3)* 部分群 $H < G$ に $S$ が含まれるならば $\langle S \rangle \subset H$ である。

*(4)* 部分集合 $S \subset G$ が部分群であるための必要十分条件は $S = \langle S \rangle$ が成り立つことである。

*(5)* $\langle S \rangle$ は $S$ を含む最小の部分群である。

**定義 5.21** (生成系)**.** 群 $G$ の**生成系**とは部分集合 $S \subset G$ であり $\langle S \rangle = G$ を満たすものをいう。

別の言い方では、部分集合 $S \subset G$ が群 $G$ の生成系であるというのはつぎが成り立つことである：
任意の $g \in G$ にたいして、ある $s_1, s_2, \cdots, s_n \in S,\ p_1, p_2, \cdots, p_n \in \mathbb{Z}$ が存在して

$$g = s_1^{p_1} s_2^{p_2} \cdots s_n^{p_n}$$

をみたす。

**補題 5.22.** 任意の群は生成系をもつ。

*Proof.* 部分集合 $G \subset G$ は群 $G$ の生成系である。 □

なので、よい（少ない or その他の良い性質をもつ）生成系をみつけるのが重要になる。

## 5.5 巡回群

**定義 5.23.** 群 $G$ は一つの要素からなる生成系 $S = \{s\}$ を持つとき $G$ は**巡回群**と呼ばれ、$s$ は**生成元**と呼ばれる。

$$G = \{ s^n \mid n \in \mathbb{Z} \}$$

**例 5.24.** $1 \in \mathbb{Z}$ は加法群 $\mathbb{Z}$ の生成元である。

$$\mathbb{Z} = \{ n \mid n \in \mathbb{Z} \} = \langle 1 \rangle.$$

**命題 5.25.** 巡回群は可換群。

*Proof.* $G$ を要素 $s \in G$ を生成元に持つ巡回群とする。
$g, h \in G$ をとってくる。ある $m, n \in \mathbb{Z}$ が存在して $g = s^m,\ h = s^n$ が成り立つ。
$gh = hg$ が以下の様にして示される：

$$gh = s^m s^n = s^{m+n} = s^{n+m} = s^n s^m = hg.$$

□

## 5.6　群の位数、要素の位数

**定義 5.26** (有限群、無限群、群の位数)**.** *(1)* 下部集合が有限集合である群を有限群と呼ぶ。

*(2)* 下部集合が無限集合である群を無限群と呼ぶ。

*(3)* 群 $G$ の下部集合の要素の個数 $\#G$ *or* $|G|$ を群 $G$ の位数と呼ぶ。

.

**定義 5.27** (群の要素の位数)**.** 群 $G$ の要素 $g \in G$ の位数 $\operatorname{ord} g$ を以下で定義する：

*(i)* あるゼロでない整数 $n$ が存在して $g^n = e$ を満たす場合：

$$\operatorname{ord} g := \min\{n > 0 \mid g^n = e\}.$$

*(ii)* どんなゼロでない整数 $n$ にたいしても $g^n \neq e$ となる場合：形式的に

$$\operatorname{ord} g := \infty.$$

**注意 5.28** (修正情報)**.** 以前の版では「ゼロでない整数」は「整数」となっていましたが、それは間違いです。

**注意 5.29.** $g^n = e$ ならば $g^{-n} = e$ であるので、定義 *(i)* により自然数が定義される。

**例 5.30.** *(1)* $\operatorname{ord} g = 1 \quad \Leftrightarrow \quad g = e.$

*(2)* $\operatorname{ord} g = 2 \quad \Leftrightarrow \quad g^2 = e, g \neq e \quad \Leftrightarrow \quad g^{-1} = g, g \neq e$

**命題 5.31.** $g \in G$ の位数と $\langle g \rangle$ の位数が等しい。

$$\operatorname{ord} g = \#\langle g \rangle.$$

とくに有限群の要素の位数は有限。

*Proof.* $n := \operatorname{ord} g$ とおく。$n < \infty$, $n = \infty$ で場合分けをする。

(I) まず $n < \infty$ と仮定する。

**主張 5.32.**

$$\langle g \rangle = \{g^a \mid 0 \leq a \leq n-1\}$$

$\because$. 包含関係 $\langle g \rangle \supset \{g^a \mid 0 \leq a \leq n-1\}$ は自明。包含関係 $\langle g \rangle \subset \{g^a \mid 0 \leq a \leq n-1\}$ を示す。
任意の整数 $b$ は $b = qn + a, (0 \leq a \leq n-1)$ と表示できる。よって、$g^b = g^a$ であり、とくに $g^b \in \{g^a \mid 0 \leq a \leq n-1\}$ である。

**主張 5.33.** $0 \leq a, b \leq n-1$ が $g^a = g^b$ を満たせば $a = b$ がなりたつ。

$\because$ $a \leq b$ と仮定して一般性を失わない。$g^a = g^b \Leftrightarrow g^{b-a} = e$ であるが、$0 \leq b-a \leq n-1$ なので位数の定義より $b-a = 0$ でなくてはならない。

主張より $\langle g \rangle = \{e, g, g^2, \cdots, g^{n-1}\}$ であり、さらに $\#\langle g \rangle = \operatorname{ord} g$ がなりたつ。

(II) 次に $n = \infty$ と仮定する。

$\#\langle g \rangle < \infty$ と仮定すると、ある整数 $a < b$ が存在して $g^a = g^b$ をみたす。このとき $g^{b-a} = e$ となり位数の仮定に矛盾。よって $\langle g \rangle = \infty$. □

同様の手法で次の命題も示せる。
整数 $a \in \mathbb{Z}$ にたいして、$a$ の倍数の集合を $a\mathbb{Z}$ とあらわす：

$$a\mathbb{Z} := \{an \mid n \in \mathbb{Z}\}.$$

**命題 5.34.** 群 $G$ の要素 $g \in G$ にたいして次がなりたつ：

*(1)* $\operatorname{ord} g < \infty$ のとき：

$$\{n \in \mathbb{Z} \mid g^n = e\} = (\operatorname{ord} g)\mathbb{Z}.$$

（集合の等号の意味は、「整数 $n \in \mathbb{Z}$ にたいして $g^n = e \quad \Leftrightarrow \quad n | \operatorname{ord} g$ が成り立つ」）

*(2)* $\operatorname{ord} g = \infty$ のとき：

$$\{n \in \mathbb{Z} \mid g^n = e\} = 0.$$

# 6 対称群

## 6.1 対称群の定義

### 6.1.1 集合の自己全単射のなす群

**定義 6.1.** 集合 $X$ の自己全単射 $f : X \to X$ が合成に関してなす群を $\mathrm{Aut}_{\mathrm{Set}}(X)$ と表す：

$$\mathrm{Aut}_{\mathrm{Set}}(X) := \{f \in \mathrm{Hom}_{\mathrm{Set}}(X, X) \mid f \text{ は全単射 }\}.$$

群 $\mathrm{Aut}_{\mathrm{Set}}(X)$ の単位元は恒等写像 $\mathrm{id}_X$ であり、要素 $f \in \mathrm{Aut}_{\mathrm{Set}}(X)$ の逆元は逆写像 $f^{-1}$ です。

### 6.1.2 対称群

**定義 6.2** (対称群)**.** $n \geq 1$ を 1 以上の自然数とする。$n$ 次対称群 $S_n$ を

$$S_n := \mathrm{Aut}_{\mathrm{Set}}(\{1, 2, \cdots, n\})$$

と定義する。

$S_n$ の要素 $\sigma \in S_n$ は $n$ 文字 $\{1, 2, \cdots, n\}$ の順列と同一視できる。
よって、位数は $n!$ です。

$$|S_n| = n!.$$

## 6.2 Coxeter 生成系

**定義 6.3** (Coxeter 生成系)**.** $n$ を 2 以上の自然数とする。$i = 1, 2, \cdots, n-1$ にたいして $s_i \in S_n$ をいかで定める：

$$s_i(j) := \begin{cases} i+1 & (j = i) \\ i & (j = i+1) \\ j & (\text{otherwise}) \end{cases}$$

**補題 6.4.** つぎが成り立つ。

*(1)* $s_i^2 = e$ *for all* $i = 1, 2, \cdots, n-1$.

*(2)* $s_i s_j = s_j s_i$ *for all pairs* $(i, j)$ *such that* $|i - j| > 1$.

*(3) (*組みひも関係式*)* $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$ *for all* $i = 1, 2, \cdots, n-1$.

**命題 6.5.** 部分集合 $\{s_1, s_2, \cdots, s_{n-1}\}$ は $S_n$ の生成系である。

証明は後回し。

## 6.3　対称群の要素の表示方法その１：対応を書き下す

要素 $\sigma \in S_n$ は定義から全単射 $\sigma : \{1, 2, \cdots, n\} \to \{1, 2, \cdots, n\}$ だった。
写像なので、これは定義域の要素 $i$ $(1 \leq i \leq n)$ の行き先（像）$\sigma(i)$ で決まってしまう。そこで要素 $\sigma \in S_n$ を表すのに、下のような表記を用いることが多い：

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

(1) 1 次対称群 $S_1 = \mathrm{Aut}_{\mathrm{Set}}\{1\}$.

$$e = \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

(2) 2 次対称群 $S_2 = \mathrm{Aut}_{\mathrm{Set}}\{1, 2\}$.

$$e = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix},\ \sigma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

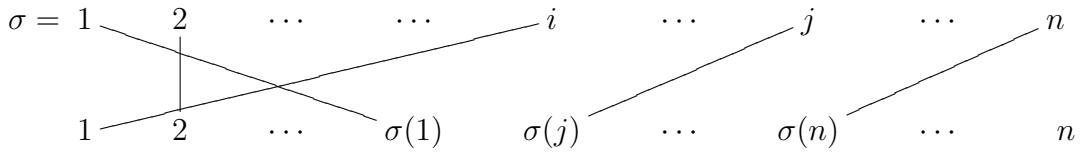
(3) 3 次対称群 $S_3 = \mathrm{Aut}_{\mathrm{Set}}\{1, 2, 3\}$.

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$
$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

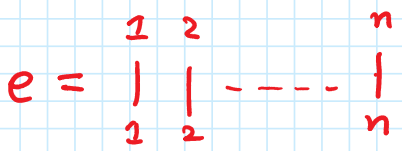
## 6.4　対称群の要素の表示方法その２：あみだくじ

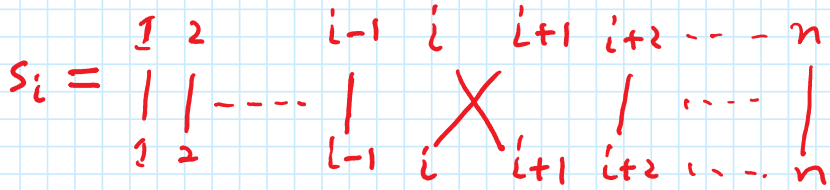
「その 2」と呼んでいますが、実際には「その 1」の表示方法の図式化です。

全単射写像 $\sigma : \{1, \cdots, n\} \to \{1, \cdots, n\}$ の値域の要素 $i$ とその像 $\sigma(i)$ を線で結んでやることで、$\sigma \in S_n$ を表示できます。

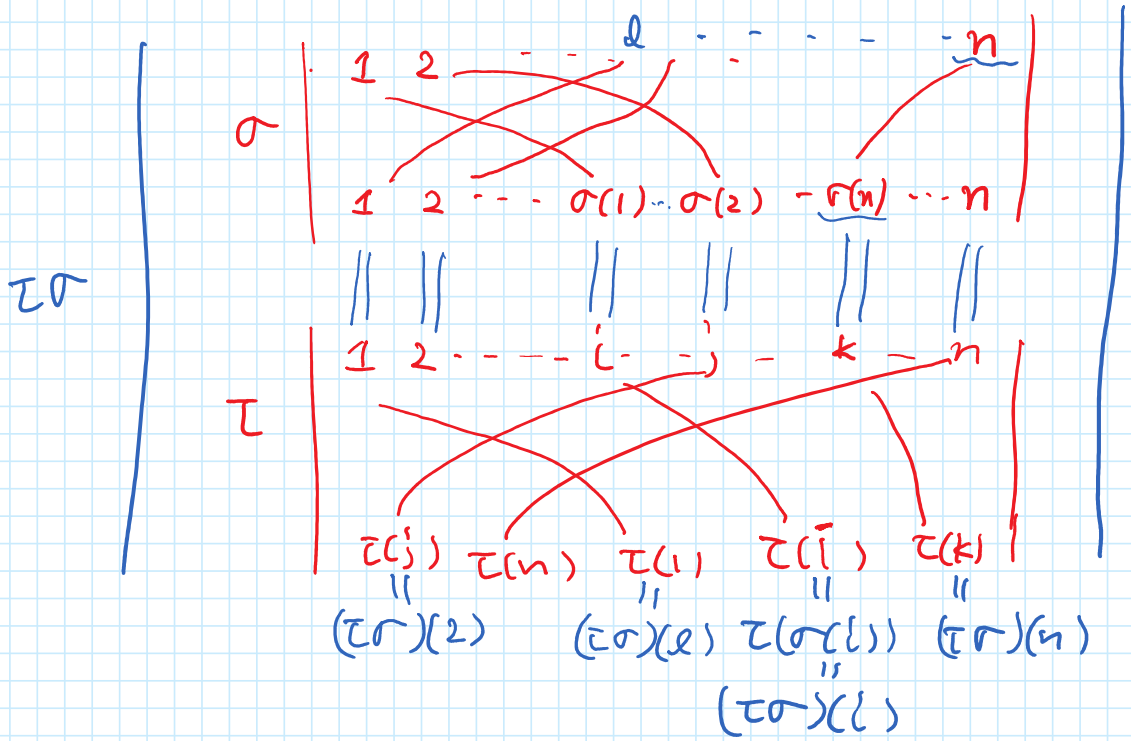



手間はかかるけれど直感的に処理しやすく、計算には向いています。

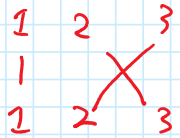


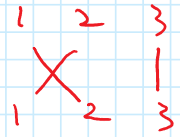



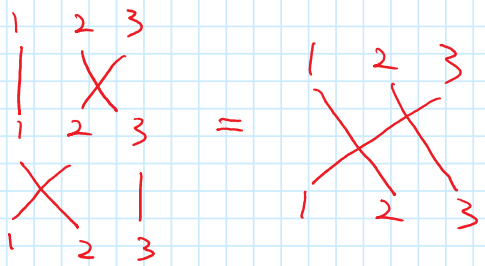

$\tau, \sigma \in S_n$

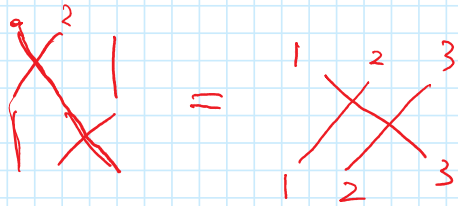


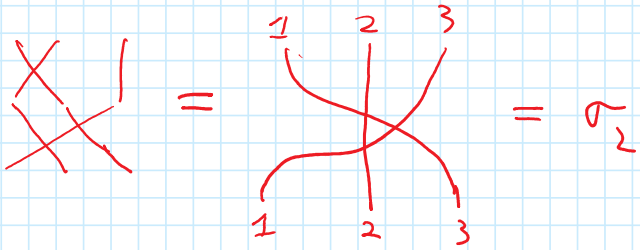
$n=3$

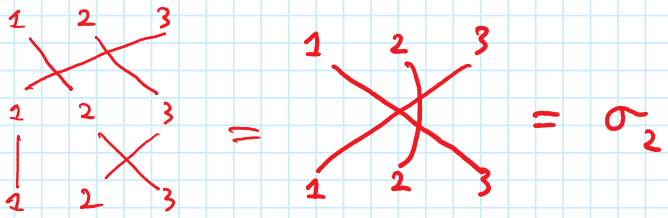
$s_2 = \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ 

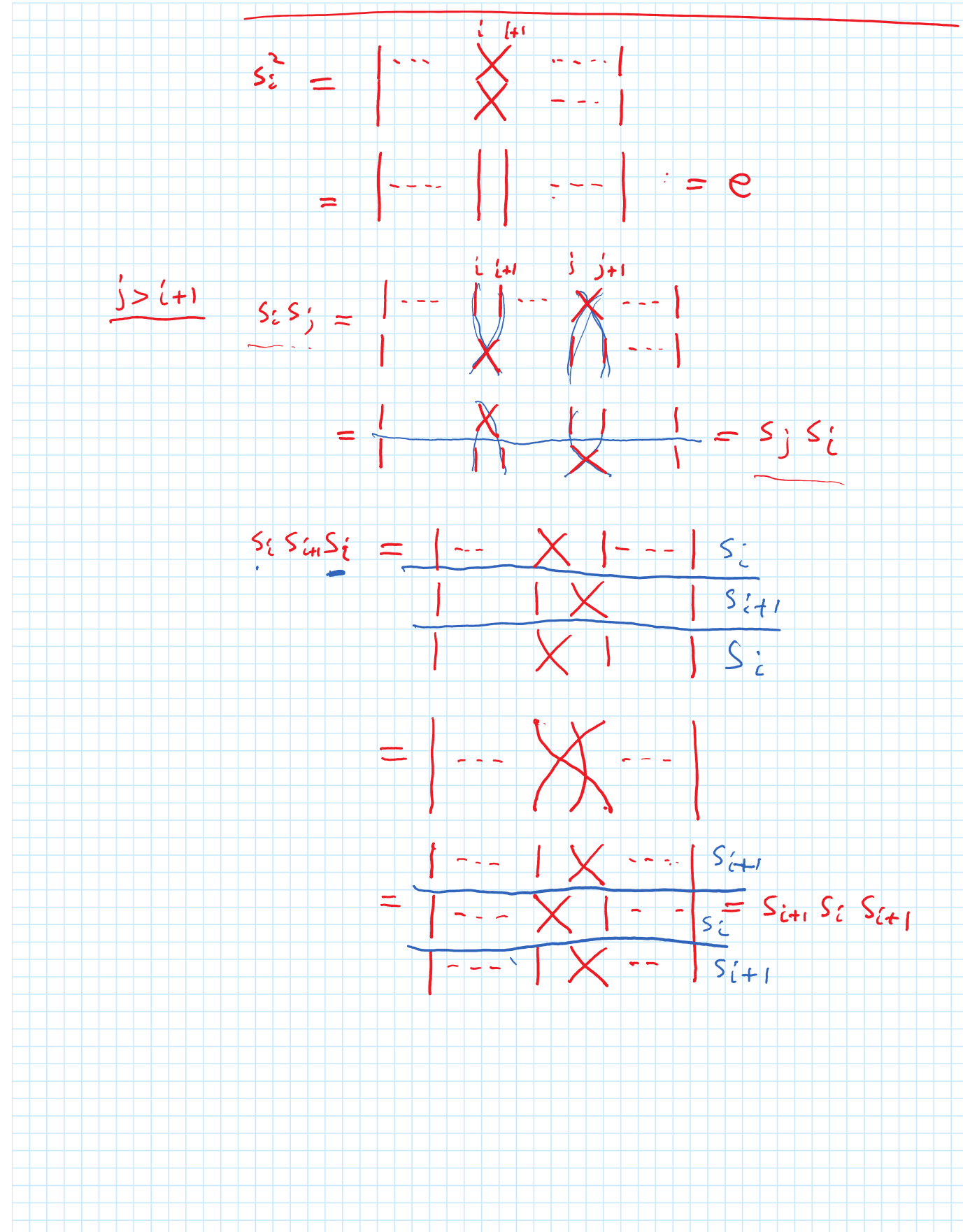
$s_1 = \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ 

$s_1 s_2 =$  $= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \tau_1$

$s_2 s_1 =$  $= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \tau_2$

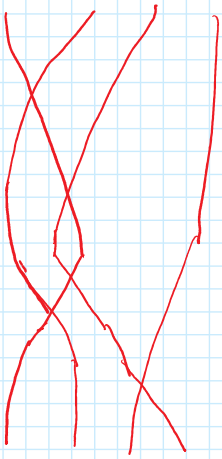
$(s_1 s_2) s_1 = \tau_1 s_1 =$  $= \sigma_2$

$s_2 s_1 s_2 = s_2 \tau_1 =$  $= \sigma_2$

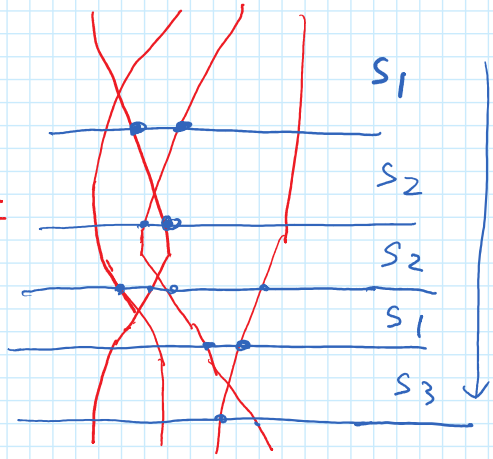

$s_i^2 = e$
$j > i+1$
$s_i s_j = s_j s_i$
$s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$

$\langle s_1, s_2, \cdots, s_{n-1} \rangle = S_n$ の証明もどき。

$\sigma =$



$=$




$= s_3 s_1 s_2 s_2 s_1 = s_3 s_1 s_1 = s_3$

## 6.5　対称群の要素の表示方法その３：巡回置換

**定義 6.6** (巡回置換)**.** $r$ を 2 以上の自然数とする。$r$ 個の要素からなる部分集合 $\{i_1, \cdots, i_r\} \subset \{1, \cdots, n\}$ にたいして要素 $(i_1 i_2 \cdots i_r) \in S_n$ をつぎの式で定義します：

記号を簡単にするために $\sigma = (i_1 i_2 \cdots i_r)$ とかくことにします：

$$\sigma(j) = \begin{cases} i_{s+1} & (j = i_s \text{ for } s = 1, 2, \cdots, r-1) \\ i_1 & (j = i_r) \\ j & (j \notin \{i_1, \cdots, i_r\}) \end{cases}$$

**例 6.7.** コクセター元 $s_i$ は

$$s_i = (i, i+1)$$

と表示できます。

**命題 6.8** (教科書 p97, 命題 4.2.1)**.** $n \geq 2$ とする。任意の $\sigma \in S_n$ にたいして互いに交わらない部分集合族

$$\{i_1^{(1)}, \cdots, i_{r_1}^{(1)}\},\ \{i_1^{(2)}, \cdots, i_{r_2}^{(2)}\}, \cdots, \{i_1^{(p)}, \cdots, i_{r_p}^{(p)}\} \subset \{1, \cdots, n\}$$

が存在して $\sigma$ はこれに付随する巡回置換の積である：

$$\sigma = (i_1^{(1)} \cdots i_{r_1}^{(1)})(i_1^{(2)} \cdots i_{r_2}^{(2)}) \cdots (i_1^{(p)}, \cdots, i_{r_p}^{(p)})$$

## 6.6　命題 6.5 の証明

### 6.6.1　転倒数、符号数

線形代数のときに導入した転倒数、符号数を復習しておきます。

**定義 6.9** (転倒数、符号数)**.** *(1)* 要素 $\sigma \in S_n$ に対して並び順 $i < j$ と並んでる数の大小関係 $\sigma(i) > \sigma(j)$ の入れ替わってる文字の組 $(i, j)$ を転倒対と呼びます。

つまり、転倒対の集合は以下で与えられます：

$$\mathcal{N}_\sigma := \{(i, j) \mid 1 \leq i < j \leq n,\ \sigma(i) > \sigma(j)\}.$$

*(2)* 要素 $\sigma \in S_n$ に対してその転倒対の個数を転倒数と呼び $N_\sigma$ と表す。

つまり、$N_\sigma$ はつぎで定義されます。

$$N_\sigma := \#\mathcal{N}_\sigma = \#\{(i, j) \mid 1 \leq i < j \leq n,\ \sigma(i) > \sigma(j)\}$$

*(3)* 順列 $\sigma$ の符号数を $\mathrm{sgn}(\sigma) := (-1)^{N_\sigma}$ と定義する。

転倒数を使うと命題 6.5 をもう少し強い形に述べることが出来ます。

**定理 6.10** (命題 6.5 の強化版)**.** $n$ を 2 以上の自然数とする。次がなりたつ。

*(1)* 要素 $\sigma \in S_n$ は $N_\sigma$ 個の *Coxeter* 元の積である。

つまり、下のような表示がある。

$$\sigma = s_{i_1} s_{i_2} \cdots s_{i_\ell}.$$

ただし $\ell := N_\sigma$ とおいた。

別の言い方をすれば、自明な順列 $e$ は $N_\sigma$ 回隣り合う二つの文字を入れ替えることで順列 $\sigma$ にすることが出来る。

*(2)* $N_\sigma$ はそのような回数の最小値である。

つまり、下のような表示があったとすれば $m \geq N_\sigma$

$$\sigma = s_{j_1} s_{j_2} \cdots s_{j_m}.$$

準備の補題が二つあります。一つ目は、単位元の特徴づけです。

**補題 6.11.** 要素 $\sigma \in \mathcal{S}_n$ について次は同値：

*(1)* $\sigma = e.$

*(2)* 任意の $i < j$ に対して $\sigma(i) < \sigma(j)$ が成り立つ。

*(3)* 任意の $i = 1, 2, \cdots, n$ に対して $\sigma(i) < \sigma(i+1)$ が成り立つ。

*(4)* 任意の $i = 1, 2, \cdots, n$ に対して $\sigma(i) \leq i$ が成り立つ。

*(5)* 任意の $i = 1, 2, \cdots, n$ に対して $\sigma(i) \geq i$ が成り立つ。

*(6)* 転倒数 $N_\sigma = 0.$

*Proof.* (4) ⇒ (1) の証明だけ与えておきます。

(4) の条件が成り立つと仮定して $\sigma(i) = i, (i = 1, 2, \cdots, n)$ が成り立つことを $i$ に関する帰納法で示します。

$i = 1$ のとき、$\sigma(1) \leq 1$ より $\sigma(1) = 1$ が従います。

$i \geq 2$ として、$\sigma(j) = j, (j = 1, \cdots, i-1)$ が成り立つと仮定します。$\sigma(i) \leq i$ ですが、$\sigma(i) < i$ ならば、ある $j = 1, \cdots, i-1$ に対して $\sigma(i) = \sigma(j)$ が成り立つことになって矛盾。よって、$\sigma(i) = i$ である。 □

二つ目の準備では、Coxeter 元 $s_i$ を左から掛けたときの転倒数の変化を調べます。

要素 $\sigma \in S_n$ を順列とみなすと、Coxeter 元 $s_i$ を掛けたもの $s_i\sigma$ は順列 $\sigma$ の第 $i$ 番目と第 $i+1$ 番目を入れ替えた順列ですね。

$$s_i\sigma(k) = \begin{cases} \sigma(k) & k \neq i, i+1 \\ \sigma(i+1) & k = i \\ \sigma(i) & k = i+1 \end{cases}$$

**補題 6.12.** $i = 1, 2, \cdots, n-1$ を考える。

この時、次が成り立つ。

$$N_{s_i\sigma} = \begin{cases} N_\sigma + 1, & (\sigma(i) < \sigma(i+1) \text{ の場合 }) \\ N_\sigma - 1. & (\sigma(i) > \sigma(i+1) \text{ の場合}) \end{cases}$$

*Proof.* 隣り合っている二文字 $\sigma(i)$ と $\sigma(i+1)$ を入れ替えるので、転倒対で変化するものは $(i, i+1)$ しかないというのがポイントです。

$\sigma(i) < \sigma(i+1)$ の場合、$(i, i+1)$ は順列 $\sigma$ の転倒対ではないですが順列 $s_i\sigma$ の転倒対にはなります。

$\sigma(i) > \sigma(i+1)$ の場合、$(i, i+1)$ は順列 $\sigma$ の転倒対ですが順列 $s_i\sigma$ の転倒対ではありません。

そして $\sigma$ と $s_i\sigma$ の転倒対にはこれ以外の違いはないので表記の結果をえます。 □

目標の定理を証明しましょう。

定理 *6.10* の証明. (1) 転倒数 $\ell = N_\sigma$ に関する帰納法を用います。$\ell = 0$ の場合は明らか。

$\ell = 1$ とする。$\sigma \neq e$ なのである $i$ が存在して $\sigma(i) > \sigma(i+1)$ を満たす。よって、$N_{s_i\sigma} = \ell - 1 = 0$ が成り立つ。よって、

$$s_i\sigma = e$$

をみたす。$s_i^2 = e$ だったので、両辺に $s_i$ を左から掛けて

$$\sigma = s_i$$

をえる。

$\ell \geq 2$ の場合。$\ell - 1$ までは命題は正しいとする。$\sigma$ を転倒数が $\ell > 0$ である順列とする。$\sigma \neq e$ なのである $i$ が存在して $\sigma(i) > \sigma(i+1)$ を満たす。よって、$N_{s_i\sigma} = \ell - 1$ が成り立つ。帰納法の仮定から $s_i\sigma$ は $\ell - 1$ 個の Coxeter 元の積である。つまり、$i_2, \cdots, i_\ell \in \{1, \cdots, \ell - 1\}$ が存在して

$$s_i\sigma = s_{i_2}s_{i_3}\cdots s_{i_{\ell-1}}$$

をみたす。$s_i^2 = e$ だったので、両辺に $s_i$ を左から掛けて

$$\sigma = s_i s_{i_2}s_{i_3}\cdots s_{i_\ell}$$

をえる。

(2)

補題 6.12 をつかうと、任意の $\tau \in S_n$ と $i = 1, 2, \ldots, n-1$ にたいして次の不等式がなりたつことに注意しましょう：

$$N_{s_i\sigma} \leq N_\sigma + 1. \tag{6-3}$$

ある $m \geq 0$ と $j_1, \ldots, j_m$ があり $\sigma = s_{j_1}s_{j_2}\cdots s_{j_m}$ がなりたつとしましょう。

不等式 (6-3) を繰り返しつかうことで次が得られます：

$$N_\sigma = N_{s_{j_1}s_{j_2}s_{j_3}\cdots s_{j_m}} \leq N_{s_{j_2}s_{j_3}\cdots s_{j_m}} + 1 \leq N_{s_{j_3}\cdots s_{j_m}} + 2 \leq N_e + m = m$$

よって $N_\sigma \leq m$ を結論します。

平たく言うと、Coxeter 元を左から掛けることで転倒数が増えるのはせいぜい 1 だけです。一方、自明な順列の転倒は $N_e = 0$ だったので、$e$ を $\sigma$ に変えるには、少なくとも $N_\sigma$ 回は Coxeter 元を掛けないといけないということです。 □

# 7　剰余類、正規部分群、商群

## 7.1　剰余類

「剰余（じょうよ）」って聞きなれない言葉ですが要するに「余り」のことです。整数の割り算をしたときの「余り」です。

### 7.1.1　部分集合を移動させる

部分集合 $S \subset G$ と要素 $g, h \in S$ から次の様に $G$ の部分集合を定める：

$$gS := \{gs \mid s \in S\}, \quad Sg := \{sg \mid s \in S\}, \quad gSh := \{gsh \mid s \in S\}.$$

**補題 7.1.** $S$ と $gS,\ Sg,\ gSh$ の間には全単射存在する。よって特に次がなりたつ：

$$\#S = \#gS = \#Sg = \#gSh.$$

### 7.1.2　剰余類

**定義 7.2.** 部分群 $H < G$ を考える。

*(1)* 要素 $g \in G$ にたいして部分集合 $gH$ を**$g$ の $H$ に関する左剰余類**とよぶ。

*(2)* 要素 $g \in G$ にたいして部分集合 $Hg$ を**$g$ の $H$ に関する右剰余類**とよぶ。

*(3)* ある要素 $g \in H$ に関する左剰余類である部分集合を左剰余類とよぶ。（「右」も同様。）

**注意 7.3.** $e \in H$ なので $g = ge$ は $gH$ に属する。

**例 7.4.** $G = \mathbb{Z},\ a > 0,\ H := a\mathbb{Z}$ の場合。
左剰余類は

$$n + a\mathbb{Z} = \{n + am \in \mathbb{Z} \mid m \in \mathbb{Z}\}$$

これは $a$ で割った余りが $n$ を $a$ で割ったときの余りと同じになる整数の集合。

**補題 7.5.** 部分群 $H < G$ と要素 $g_1, g_2 \in G$ にたいして次の条件はすべて同値：

*(1)* $g_1H = g_2H$. （$G$ の部分集合として等しい。）

*(2)* $g_1H \cap g_2H \neq \emptyset$

*(3)* *There exists* $h \in H$ *such that* $g_1h = g_2$.

*(4)* *There exists* $h \in H$ *such that* $g_2h = g_1$.

*(5)* $g_1^{-1}g_2 \in H$

*(6)* $g_2^{-1}g_1 \in H$

*Proof.* (1) ⇒ (2) は明らか。（注意 $gH \neq \emptyset$.）

(2) ⇒ (3). 条件より要素 $x \in g_1H \cap g_2H$ がとれる。$x \in g_1H$ なので、ある $h_1 \in H$ が存在して $x = g_1h_1$ をみたす。$x \in g_2H$ なので、ある $h_2 \in H$ が存在して $x = g_2h_2$ をみたす。ゆえに $g_1h_1 = x = g_2h_2$ が成り立つ。

要素 $h := h_1h_2^{-1}$ が目標としている性質をもつものである。

$H$ は部分群であるから $h \in H$ である。うえの等式の両辺に $h_2^{-1}$ を右から掛けて等式 $g_1h = g_2$ をえる。

(3) ⇒ (4). $h^{-1}$ をもってくればいい。

(4) ⇒ (5) ⇔ (6). あきらか。

(5) ⇒ (1) $g_2H \subset g_1H$ を示す。

$x \in g_2H$ とする。ある $h \in H$ が存在して $x = g_2h$ をみたす。

$x = g_2h = g_1(g_1^{-1}g_2)h$ である。条件より $g_1^{-1}g_2 \in H$ であり、$H$ は部分群なので $g_1^{-1}g_2h \in H$. ゆえに $x \in g_1H$ である。

逆向きの包含関係も同様に示される。 □

特に (1) と (2) の同値性より次が成り立つ：

**系 7.6.** 要素 $g_1, g_2 \in G$ に対してどちらか一方のみが必ず成り立つ：

1. *(*完全に一致）$g_1H = g_2H$.
2. （交わらない）$g_1H \cap g_2H = \emptyset$.

このことから $H$ による左剰余類 $gH$ $(g \in G)$ により $G$ は敷き詰められる（非交和分解される）ように思えてくる。
しかし、重複 $g_1H = g_2H$ を除かないといけない。

**練習問題 7.7.** 補題の条件が掴みづらい場合は、各条件が例 *7.4* の場合にどういうことを意味してるかを考えよう。

### 7.1.3 完全代表系

**定義 7.8** (完全代表系)**.** 部分群 $H < G$ を考える。

部分集合 $R \subset G$ が $H$ **の左剰余に関する完全代表系**とは次が成り立つことをいう：

任意の $g \in G$ にたいしてある $r \in R$ が一意的に存在して $gH = rH$ を満たす。

**注意 7.9.** 完全代表系の要素 $r, s \in R$ にたいして次の同値が成り立つ：

$$r \neq s \quad \Leftrightarrow \quad rH \neq sH.$$

**例 7.10** (例 7.4 の続き)**.** $G = \mathbb{Z},\ a > 0,\ H := a\mathbb{Z}$ の場合。

左剰余類は

$$n + a\mathbb{Z} = \{n + am \in \mathbb{Z} \mid m \in \mathbb{Z}\}$$

これは $a$ で割った余りが $n$ を $a$ で割ったときの余りと同じになる整数の集合。

$a\mathbb{Z}$ に関する左剰余の完全代表系 $R$ の条件を今の場合に書いてみると

「任意の $n \in \mathbb{Z}$ にたいしてある $r \in R$ が一意的に存在して $a$ で $n$ を割った余りと $r$ を割った余りが等しい。」

なので、完全代表系の一つの例としては $a$ で割ったときの余りの集合がとれます：

$$R = \{r \mid 0 \leq r < a\}$$

これはあくまでも一例で、完全代表系の選び方はいくらでもありますね。

**補題 7.11.** 任意の群 $G$ の任意の部分群 $H < G$ にたいして左剰余に関する完全代表系は存在する。

## 7.2 ラグランジュの定理

**定理 7.12.** $G$ を群、$H$ を $G$ の部分群、$R \subset G$ を $H$ の左剰余に関する完全代表系とする。そうすると、次の非交和分解がえられる：

$$G = \bigsqcup_{r \in R} rH.$$

つまり、以下の二つがなりたつ：

*(1)* $G = \bigcup_{r \in R} rH.$

*(2)* $rH \cap sH = \emptyset$ $(\forall r, s \in R)$

定理の主張してることは、

「任意の $g \in G$ は必ず $rH$ $(r \in R)$ のどれか一つに属し、他の奴には属さない」

ということです。

*Proof.* (1) $g \in G$ をとってくる。$g = ge \in gH$ に注意しておく。
完全代表系の定義よりある $r \in R$ が存在して $gH = rH$ をみたす。よって $g \in rH$ である。

(2) は上で注意した。 □

**例 7.13** (例 7.4 の続き)**.** $G = \mathbb{Z},\ a > 0,\ H := a\mathbb{Z}$ の場合。
左剰余類は

$$n + a\mathbb{Z} = \{n + am \in \mathbb{Z} \mid m \in \mathbb{Z}\}$$

これは $a$ で割った余りが $n$ を $a$ で割ったときの余りと同じになる整数の集合。
完全代表系の一つの例としては $a$ で割ったときの余りの集合がとれました：

$$R = \{r \mid 0 \leq r < a\}$$

上の定理の主張することは

$$\mathbb{Z} = \bigsqcup_{0 \leq r < a} (r + a\mathbb{Z})$$

これを翻訳すると、

「任意の整数 $n$ にたいして $r$ $(0 \leq r < a)$ が一意的に存在して $x \in r + a\mathbb{Z}$ である。」

もう少し頑張ると

「任意の整数 $n$ にたいして $r$ $(0 \leq r < a)$ が $a$ を $n$ で割ったときの余りとして一意的に定まる。」

と良く知っていることを言ってるのだと判明しますね。

**例 7.14.** 次の場合を考える：

$$G = S_3, \quad H = \langle s_1 \rangle = \{e, s_1\}$$

ただし $s_1$ は *Coxeter* 元。

計算すると次が分かります：

$$\begin{aligned} G &= \{e, s_1, s_2, s_1s_2, s_2s_1, s_1s_2s_1\} \\ H &= \{e, s_1\} \\ s_2H &= \{s_2, s_2s_1\} = s_2s_1H \\ s_1s_2H &= \{s_1s_2, s_1s_2s_1\} = s_1s_2s_1H. \end{aligned}$$

なので $H$ の左剰余に関する完全代表系 $R$ としては次が選んでこれます：

$$R = \{s_1, s_2, s_1s_2\}$$

（選び方は $8 = 2^3$ 通りありますね。）

上の定理が主張するのは

$$S_3 = s_1H \sqcup s_2H \sqcup s_1s_2H$$

ということです。

言っていることは、

「任意の $\sigma \in S_3$ は必ず $s_1H, s_2H, s_1s_2H$ のどれか一つに属し、他の奴には属さない」

ということです。

**系 7.15** (ラグランジュの定理)**.** $G$ を有限群、$H$ を $G$ の部分群、$R$ を $H$ に関する左剰余の完全代表系とする。次がなりたつ：

$$|G| = |R||H|$$

特に $H$ の位数は $G$ の位数の約数である。

*Proof.*

$$|G| = \sum_{g \in R} |gH| = \sum_{g \in R} |H| = |R||H|.$$

□

**系 7.16.** 有限群 $G$ の要素 $g \in G$ の位数 $\operatorname{ord} g$ は $G$ の位数の約数である：

$$\operatorname{ord} g | \#G.$$

*Proof.* $\operatorname{ord} g = \#\langle g \rangle$ より従う。 □

## 7.3 素数位数の群の構造

**定理 7.17.** 素数位数の群は巡回群である。とくに可換群である。

*Proof.* $G$ を位数が素数 $p$ である群とする。
$p > 1$ なので $G$ には単位元でない要素 $g \in G$ が存在する。
$|\langle g \rangle| = \operatorname{ord} g > 1$ である。
一方、系 7.16 より、$\operatorname{ord} g \mid |G|$ なので、$|G| = |\langle g \rangle|$ でなくてはならず、
よって、$\langle g \rangle = G$ を結論する。

□

## 7.4 商集合

**定義 7.18.** 部分群 $H < G$ を考える。

*(1)* $G/H$ により左剰余類のなすべき集合 $\mathcal{P}(G)$ の部分集合をあらわし
$G$ の $H$ による（左）商集合とよぶ。

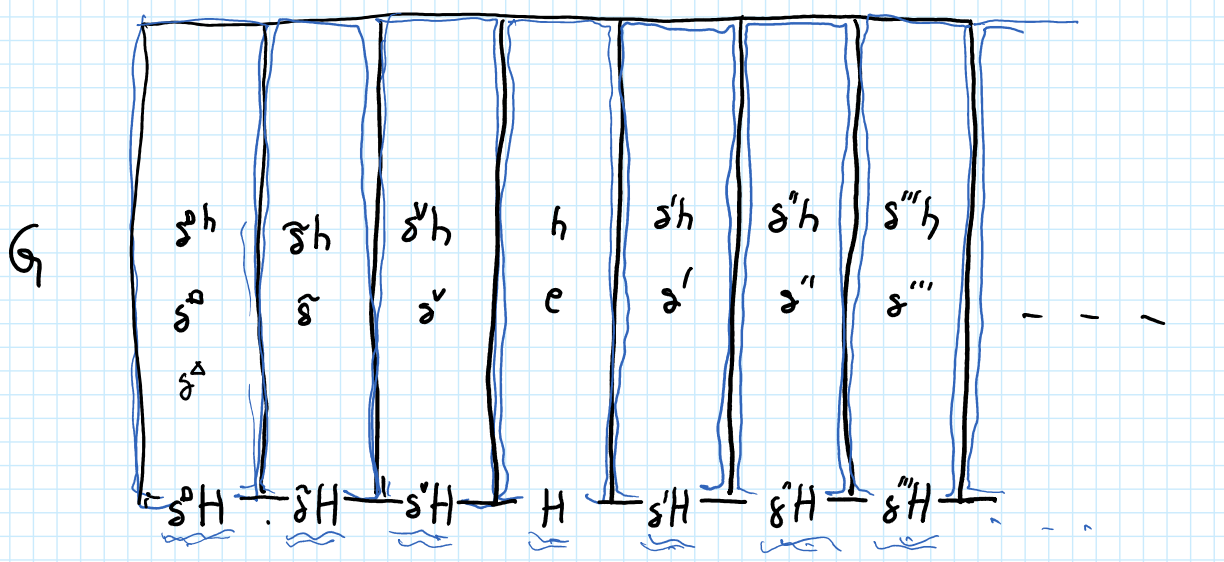
$$G/H := \{gH \in \mathcal{P}(G) \mid g \in G\}$$

*(2)* $gH$ に対応する $G/H$ の要素を $[g]$ または $\overline{g}$ であらわす。

*(3)* 写像 $\pi : G \to G/H$ を

$$\pi(g) := [g] = \overline{g}$$

により定める。商写像と呼ばれる。




$[s^{\triangle}]$
$=$
$s$さんのいるクラス

$$G/H = \{[s^{\square}], [\tilde{s}], [s'], [e], [s'], [s''], [s'''], \cdots\}$$

$s^{\square}$さんのいるクラス
$=$
$s^{\triangle}$さんのいるクラス

**補題 7.19.** 上の状況で部分集合 $R \subset G$ が $H$ による左剰余に関する完全代表系であるための必要十分条件は商写像 $\pi$ を $R$ に制限したもの $\pi|_R : R \to G/H$ が全単射になることである。

**定義 7.20** (部分群の指数)**.** $G$ を群とする。部分群 $H < G$ の指数 $[G : H]$ を以下で定める：

$$[G : H] = \#G/H.$$

**補題 7.21.** 群 $G$ と部分群 $H < G$ にたいして次が成り立つ：

$$|G| = [G : H]|H|.$$

*Proof.* $G$ の $H$ の左剰余に関する完全代表系 $R$ をとる。$|R| = |G/H| = [G : H]$ なので、主張はラグランジュの定理の言い換えである。 □

## 7.5 例

例を挙げます。念のために言っておくと完全代表系 $R$ の取り方は例で挙げているもの以外にもあります。

**例 7.22.** $G = \mathbb{Z} > H = 5\mathbb{Z}$ の場合。剰余類は次の五つ：

$$5\mathbb{Z}, 1 + 5\mathbb{Z}, 2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}.$$

ただし、剰余類の表し方はいろいろある。例えば、次も同じものを表してる：

$$10 + 5\mathbb{Z}, -9 + 5\mathbb{Z}, 102 + 5\mathbb{Z}, 78 + 5\mathbb{Z}, -196 + 5\mathbb{Z}.$$

完全代表系の取り方としては、次のものが標準的ですね：

$$R = \{0,\ 1,\ 2,\ 3,\ 4\} \subset \mathbb{Z}.$$

商集合は

$$\mathbb{Z}/5\mathbb{Z} = \{[n] \in \mathcal{P}(\mathbb{Z}) \mid n \in \mathbb{Z}\} = \{[0],\ [1],\ [2],\ [3],\ [4]\}.$$

**例 7.23.** $\mathbb{Z} \subset \mathbb{R}$ の場合。

剰余類は

$$x + \mathbb{Z}\ (x \in \mathbb{R}).$$

二つの実数 $x, y \in \mathbb{R}$ が等しい剰余類を持つための必要十分条件は

$$x + \mathbb{Z} = y + \mathbb{Z} \ \Leftrightarrow x - y \in \mathbb{Z} \ \Leftrightarrow \ x, y \text{の小数部分が一致.}$$

完全代表系としては次がとれる：

$$R = [0, 1) \subset \mathbb{R}.$$

よって商集合は

$$\mathbb{R}/\mathbb{Z} = \{[x] \in \mathcal{P}(\mathbb{R}) \mid x \in \mathbb{R}\} = \{[x] \in \mathcal{P}(\mathbb{R}) \mid x \in [0, 1)\}.$$

商集合 $\mathbb{R}/\mathbb{Z}$ は円周と自然に同一視できる。

**例 7.24** (例 7.14 の続き)**.** 次の場合を考える：

$$G = S_3, \quad H = \langle s_1 \rangle = \{e, s_1\}$$

ただし $s_1$ は *Coxeter* 元。

計算すると次が分かります：

$$\begin{aligned} G &= \{e, s_1, s_2, s_1s_2, s_2s_1, s_1s_2s_1\} \\ H &= \{e, s_1\} \\ s_2H &= \{s_2, s_2s_1\} = s_2s_1H \\ s_1s_2H &= \{s_1s_2, s_1s_2s_1\} = s_1s_2s_1H. \end{aligned}$$

よって、

$$[e] = [s_1],\ [s_2] = [s_2s_1],\ [s_1s_2] = [s_1s_2s_1].$$

完全代表系の例としては

$$R = \{e,\ s_1,\ s_1s_2\} \subset S_3$$

よって商集合は

$$G/H = \{[e],\ [s_2],\ [s_1s_2]\}.$$

## 7.6　正規部分群、商群

注意すべき点は集合 $G/H$ の要素の表示には群 $G$ の要素を用いますが、

　異なる要素 $x, y \in G,\ x \neq y$ が同じ $G/H$ の点を表すことがあるということです。
　大事なことなのでもう一回書いておきます。

**注意 7.25.** 要素 $x, y \in G$ は $x \neq y$ であっても $G/H$ の中では $[x] = [y]$ かもしれない。

　こういう時に大切になるのは $[x] = [y]$ となる必要十分条件をもとめることですね。ところが、それは補題 7.5 で既に済んでいます。
　内容をおさらいしましょう。

**補題 7.26.** $G$ を群、$H$ を部分群とする。

　要素 $x, y \in G$ にたいして次の同値がある：

$$[x] = [y] \ \Leftrightarrow\ xH = yH \ \Leftrightarrow\ y^{-1}x \in H \ \Leftrightarrow\ \exists h \in H \text{ s.t. } xh = y.$$

**疑問 7.27.** 部分群 $H < G$ を考える。
　もし $x, x', y, y' \in G$ が $[x] = [x'], [y] = [y']$ をみたしたとすれば、
等式 $[xy] = [x'y']$ が成り立つか？

$$\begin{array}{ccc} G \times G & \xrightarrow{\quad\mu\quad} & G \\ {\scriptstyle \pi\times\pi}\downarrow & & \downarrow{\scriptstyle \pi} \\ G/H \times G/H & \dashrightarrow & G/H \end{array}$$

　いつでも成り立つわけではない。

**例 7.28** (例 7.14 の続き)**.** 次の場合を考える：

$$G = S_3, \quad H = \langle s_1 \rangle = \{e, s_1\}$$

ただし $s_1$ は *Coxeter* 元。
　計算すると次が分かります：

$$\begin{aligned} G &= \{e, s_1, s_2, s_1s_2, s_2s_1, s_1s_2s_1\} \\ H &= \{e, s_1\} \\ s_2H &= \{s_2, s_2s_1\} = s_2s_1H \\ s_1s_2H &= \{s_1s_2, s_1s_2s_1\} = s_1s_2s_1H. \end{aligned}$$

　そこで次のように元を設定する：

$$x = s_2,\ x' = s_2s_1,\ y = y' = s_1s_2$$

すると

$$[x] = [x'], [y] = [y'].$$

であるが、

$$xy = s_2s_1s_2 = s_1s_2s_1 \in s_1s_2H, \quad x'y' = s_2s_1s_1s_2 = e \in H.$$

よって

$$[xy] = [s_1s_2], \quad [x'y'].\ = [e]$$

$G$ の部分集合 $S,T \subset G$ にたいして次のように部分集合 $ST \subset G$ を定義する：

$$ST := \{st \in G \mid s \in S,\ t \in T\}.$$

**定理 7.29.** 群 $G$ の部分群 $H < G$ ににたいして次の条件は同値。

*(1)* もし要素 $x, x', y, y' \in G$ が等式 $[x] = [x'], [y] = [y']$ をみたせば等式 $[xy] = [x'y']$ が成り立つ。

*(2)* 任意の要素 $x, y \in G$ にたいして $xHyH = xyH$ がなりたつ。

*(3)* $xHx^{-1} = H$ *for all* $x \in G$.

*(4)* $xHx^{-1} \subset H$ *for all* $x \in G$.
つまり、任意の $x \in G$ と任意の $h \in H,\ x \in G$ にたいして $xhx^{-1} \in H$ がなりたつ。

*(5)* $x^{-1}Hx \subset H$ *for all* $x \in G$.
つまり、任意の $x \in G$ と任意の $h \in H,\ x \in G$ にたいして $x^{-1}hx \in H$ がなりたつ。

*Proof.* (1) ⇒ (5). 任意に $z \in G$ を持ってくる。($z^{-1}Hz \subset H$ を示したい。そこで、)
任意に $h \in H$ を持ってくる。($z^{-1}hz \in H$ を示したい。)
(1) を $x = h, x' = e, y = z, y' = z$ に適用する。すると等号 $[hz] = [z]$ を得る。これは所属関係 $z^{-1}hz \in H$ と同値だったので、$z^{-1}hz \in H$ を結論する。

(5) ⇒ (4).
任意に $z \in G$ を持ってくる。($zHz^{-1} \subset H$ を示したい。)
(5) を $x = z^{-1}$ に適用することで以下のように包含関係 $zHz^{-1} \subset H$ を得る：

$$zHz^{-1} = (z^{-1})^{-1}Hz^{-1} \subset H.$$

(4) ⇒ (5). 上と同様に示せる。

(4) ⇒ (3).
任意に $z \in G$ を持ってくる。($zHz^{-1} = H$ を示したい。そこで、)
(i) $zHz^{-1} \subset H$, (ii) $zHz^{-1} \supset H$ を示す。

(i) は (4) そのもの。(ii) を示す。$h \in H$ をとってくる。($h \in zHz^{-1}$ が示したい。)
(4) から (5) が従うことをすでに示しているので (5) を使うことが出来る。
(5) より $z^{-1}hz \in H$ である。よって、以下の様に所属関係 $h \in zHz^{-1}$ を得る：

$$h = z(z^{-1}hz)z^{-1} \in zHz^{-1}.$$

(3) ⇒ (4). 明らか。

(5) ⇒ (2).
$x, y \in G$ をとってくる。($xHyH = xyH$ を示したい。そこで、)
(i) $xHyH \subset xyH$, (ii) $xHyH \supset xyH$ を示す。

(ii) $h \in H$ をとってくる。($xyh \in xHyH$ を示したい。)
$e \in H$ なので $xyh = xeyh$ は $xHyH$ に属する。

(i) $h, k \in H$ をとってくる。($xhyk \in xyH$ を示したい。)
(5) より $y^{-1}hy \in H$ なので、以下の様に $xhyk \in xyH$ を得る：

$$xhyk = xy\left((yhy^{-1})k\right) \in xyH.$$

(2) $\Rightarrow$ (1).
$x, x'y, y' \in G$ が

$$[x] = [x'],\ [y] = [y']$$

を満たすとする。これは $G$ の部分集合としての等号

$$xH = x'H,\ yH = y'H$$

を意味する。よって、次の $G$ の部分集合の等号をえる：

$$xyH = xHyH = x'Hy'H = x'y'H$$

ただし、一つ目と三つ目の等号は (2) を用いている。ゆえに $[xy] = [x'y']$ を結論する。

□

**定義 7.30** (正規部分群)**.** 部分群 $H < G$ は次を満たすとき**正規部分群**と呼ばれる：
任意の $h \in H,\ x \in G$ にたいして $xhx^{-1}$ は $H$ に属する。

正規部分群であることを次の記号であらわす：

$$H \lhd G$$

**定義 7.31** (商群)**.** $G$ を群、$H$ を正規部分群とする。

対応 $\overline{\mu} : G/H \times G/H \to G/H,\ ([x], [y]) \to [xy]$ は
定義域の各要素 $(\xi, \eta)$ にたいし、要素の表示方法 $\xi = [x],\ \eta = [y]$ に依存しない像 $\overline{\mu}(\xi, \eta)$ を与える。
よって、この対応は写像 $\overline{\mu} : G/H \times G/H \to G/H,\ ([x], [y]) \to [xy]$ である。

$$\begin{array}{ccc} G \times G & \xrightarrow{\mu} & G \\ {\scriptstyle \pi\times\pi}\downarrow & & \downarrow{\scriptstyle \pi} \\ G/H \times G/H & \xrightarrow[\overline{\mu}]{} & G/H \end{array}$$

商集合 $G/H$ と写像 $\overline{\mu}$ の組 $(G/H, \overline{\mu})$ は群である。
これを $G$ の $H$ による**商群**と呼ぶ。
積の定め方を簡単に書く：

$$[x][y] := [xy].$$

$\because$

$$([x][y])[z] = [xy][z] = [(xy)z] = [x(yz)] = [x][yz] = [x]([y][z]).$$

単位元は $e_{G/H} = [e_G]$ である。逆元は $[x]^{-1} = [x^{-1}]$ である。

### 7.6.1 例

**命題 7.32.** 可換群の任意の部分群は正規。

**例 7.33.** $G = \mathbb{Z},\ n > 0,\ H = n\mathbb{Z}$ の場合。上の命題から $n\mathbb{Z}$ は $\mathbb{Z}$ の正規部分群。

商群 $\mathbb{Z}/n\mathbb{Z}$ の要素の個数は $n$:

$$|\mathbb{Z}/n\mathbb{Z}| = n.$$

要素の表し方としては

$$[0],\ [1],\ [2],\ \cdots, [n-1]$$

が互いに相異なる要素を表している。

積を書いてみると

$$[a] + [b] := [a + b].$$

なので例えば

$$[n-1] + [3] = [n+2] = [2].$$

**注意 7.34.** 二つ目の等号はあくまでも説明のために書いています。

$\mathbb{Z}/n\mathbb{Z}$ の要素をいつでも $[r]$ $(0 \leq r < n)$ の形に表すことを推奨・指導するものではありません。

**例 7.35.** $G = S_3,\ H = A_3 := \{e,\ s_1s_2,\ s_2s_1\}$ の場合。

$H$ は 3 次交代群と呼ばれ $A_3$ と書かれる。これは $S_3$ の正規部分群である。

計算すると

$$H = s_1s_2H = s_2s_1H,$$
$$s_1H = s_2H = s_1s_2s_1H.$$

よって、

$$S_3/A_3 = \{[e], [s_1]\}$$

唯一、非自明な積 $[s_1][s_1]$ を計算すると

$$[s_1][s_1] = [s_1s_1] = [e]$$

念のために別の表記でも計算してみる

$$[s_2][s_1s_2s_1] = [s_2][s_2s_1s_2] = [s_2s_2s_1s_2] = [s_1s_2] = [e].$$

**例 7.36.** 特殊線形群 $\mathrm{SL}_n(R)$ は一般線形群 $\mathrm{GL}_n(R)$ の正規部分群

$$\mathrm{SL}_n(R) \lhd \mathrm{GL}_n(R).$$

**例 7.37.** *(1)* 群 $G$ の部分群 $\{e\}, G$ は正規。

*(2)* $H, K \lhd G \quad \Rightarrow \quad H \cap K \lhd G.$

*(3)* $H < G, K \lhd G \quad \Rightarrow \quad H \cap K \lhd H.$

**7.6.2**

**命題 7.38.** 任意の部分群が正規だからといって可換とは限らない。

*Proof.* 次の反例により示される。

群 $G = \{\pm 1, \pm i, \pm j, \pm k\} \subset \mathrm{GL}_4(\mathbb{R})$ を次で定める。

$$i = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix},\ j = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix},\ k = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

次の関係式がある：

$$i^2 = j^2 = k^2 = -1, ijk = -1.$$

この群は非可換であるが、任意の部分群は正規である。次のように示される：

(1) 等式 $ij = -ji$ が成り立つ。とくに $G$ は非可換。

(2) 部分群は以下のものに限られる：

$$\{1\},\ \langle i\rangle,\ \langle j\rangle,\ \langle k\rangle,\ G.$$

(3) これらが正規であることは個別に確認できる。

□

**命題 7.39.** *(1)* $K < H,\ H < G \quad \Rightarrow \quad K < G.$

*(2)* $K \lhd H,\ H \lhd G$ だからといって $K \lhd G$ とは限らない。

.

**命題 7.40.** 指数 2 の部分群は正規である。

# 8　群準同型写像、群同型写像

## 8.1　群準同型写像、群同型写像

**定義 8.1.** $G, H$ を群とする。

*(1)* 写像 $f : G \to H$ が**群準同型**とは次が成り立つことをいう：

$$f(gg') = f(g)f(g') \text{ for all } g, g' \in G$$

*(2)* 全単射な群準同型写像を**群同型写像**という。

**補題 8.2.** 群準同型写像 $f : G \to H$ に対して次が成り立つ：

*(1)* $f(e_G) = e_H$.

*(2)* $f(g^{-1}) = f(g)^{-1}$ *for all* $g \in G$.

*Proof.* (1) 等式 $f(e_G)^2 = f(e_G)$ が以下で示される：

$$f(e_G)^2 = f(e_G)f(e_G) = f(e_G e_G) = f(e_G).$$

両辺に $f(e_G)^{-1}$ を掛けて $f(e_G) = e_H$ を結論する。

(2) 等式 $f(g)f(g^{-1}) = e_H$ が以下で示される：

$$f(g)f(g^{-1}) = f(gg^{-1}) = f(e_G) = e_H.$$

両辺に $f(g)^{-1}$ を左から掛けて $f(g^{-1}) = f(g)^{-1}$ を結論する。

□

**補題 8.3.** *(1)* 群準同型写像の合成写像は群準同型写像である。

*(2)* 群同型写像の合成写像は群同型写像である。

*(3)* 群同型写像の逆写像は群同型写像である。

### 8.1.1　群（準）同型の集合

**定義 8.4.** $G,\ H$ を群とする。

*(1)* $\mathrm{Hom}_{\mathrm{Gp}}(G, H)$ により群準同型写像 $f : G \to H$ の集合を表す：

$$\mathrm{Hom}_{\mathrm{Gp}}(G, H) := \{f \in \mathrm{Hom}_{\mathrm{Set}}(G, H) \mid f \text{ は群準同型写像 }\}$$

*(2)* $\mathrm{End}_{\mathrm{Gp}}(G)$ により自己群準同型写像 $f : G \to G$ の集合を表す。
別の言い方では $\mathrm{End}_{\mathrm{Gp}}(G) := \mathrm{Hom}_{\mathrm{Gp}}(G, G)$.

*(3)* $\mathrm{Aut}_{\mathrm{Gp}}(G)$ により自己群同型写像 $f : G \to G$ の集合を表す。
自己群同型写像 $f : G \to G$ というのは自己群準同型写像（$\mathrm{End}_{\mathrm{Gp}}(G)$ の要素）かつ自己全単射（$\mathrm{Aut}_{\mathrm{Set}}(G)$ の要素）ということなので、$\mathrm{Hom}_{\mathrm{Set}}(G, G)$ の部分集合の等号がなりたつ：

$$\mathrm{Aut}_{\mathrm{Gp}}(G) = \mathrm{Aut}_{\mathrm{Set}}(G) \cap \mathrm{End}_{\mathrm{Gp}}(G).$$

$\mathrm{Aut}_{\mathrm{Gp}}(G)$ は自己全単射群 $\mathrm{Aut}_{\mathrm{Set}}(G)$ の部分群である。この群を自己同型群とよぶ。

## 8.2 核と像

**定義 8.5** (像と核)**.** 群準同型写像 $f : G \to H$ にたいして次のように $G$ の部分集合 $\ker f$ と $H$ の部分集合 $\mathrm{Im}\, f$ を定める：

$$\ker f := \{g \in G \mid f(g) = e_H\},$$
$$\mathrm{Im}\, f := \{h \in H \mid h = f(g) \text{ for some } g \in G\}$$

**命題 8.6.** 群準同型写像 $f : G \to H$ にたいして次が成り立つ：

*(1)* 像 $\mathrm{Im}\, f$ は $H$ の部分群である。

*(2)* 核 $\ker f$ は $G$ の正規部分群である。

*Proof.* (1) $e_H = f(e_G)$ なので $e_H \in \mathrm{Im}\, f$ である。ゆえに $\mathrm{Im}\, f \neq \emptyset$.
$u, v \in \mathrm{Im}\, f$ をとってくる。ある $x, y \in G$ が存在して $u = f(x),\ v = f(y)$ をみたす。
等式

$$uv^{-1} = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1})$$

より、$uv^{-1}$ は $\mathrm{Im}\, f$ に属すると結論できる。

(2) $f(e_G) = e_H$ なので $e_G \in \mathrm{Ker}\, f$ である。ゆえに $\mathrm{Ker}\, f \neq \emptyset$.
$x, y \in \ker f$ をとってくる。等式

$$f(xy^{-1}) = f(x)f(y)^{-1} = ee = e$$

より $xy^{-1} \in \ker f$ である。よって、$\ker f$ は $G$ の部分群である。
$x \in \ker f,\ g \in G$ をとってくる。等式 $f(gxg^{-1}) = e$ が以下で確認できる：

$$f(gxg^{-1}) = f(g)f(x)f(g)^{-1} = f(g)ef(g)^{-1} = f(g)f(g)^{-1} = e$$

よって、$gxg^{-1} \in \ker f$ である。ゆえに、$\ker f$ は正規部分群である。 □

**命題 8.7.** 群準同型写像 $f : G \to H$ にたいして次が成り立つ。

*(1)* $f$ が全射 $\Leftrightarrow \mathrm{Im}\, f = H$.

*(2)* $f$ が単射 $\Leftrightarrow \ker f = \{e\}$.

*Proof.* (1) は自明。

(2) （簡単な証明は教科書に載ってる。線形代数でやったのと実質同じ。少し、違った証明を与える。）

準備を二つします。

**補題 8.8.** $h \in H$ にたいして次が成り立つ：

$$f^{-1}(\{h\}) = \begin{cases} g \ker f & \text{if there exists } g \in G \text{ such that } f(g) = h \\ \emptyset & h \notin \mathrm{Im}\, f \end{cases}$$

*Proof.* 証明の要点は次です：
群 $G$ の要素 $g_1, g_2 \in G$ にたいして次の命題は同値：

$$f(g_1) = f(g_2) \ \Leftrightarrow \ f(g_1^{-1}g_2) = e_H \ \Leftrightarrow \ g_1^{-1}g_2 \in \ker f \ \Leftrightarrow \ g_2 \in g_1 \ker f$$

□

系として次が成り立ちますね：

**系 8.9.** $g \in G$ にたいして次がなりたつ：

$$f^{-1}(\{f(g)\}) = g \ker f.$$

もうひとつの準備は単射性の判定法です。

**補題 8.10.** 写像 $f : X \to Y$ が単射であるための必要十分条件は $f^{-1}(\{f(x)\}) = \{x\}$ $(\forall x \in X)$ である。

[命題の証明] $(\Rightarrow)$. $\ker f = f^{-1}(\{e\}) = f^{-1}(\{f(e_G)\})$ である。いま $f$ は単射と仮定しているので、補題 8.10 より $\ker f = \{e\}$ が従う。

$(\Leftarrow)$. $\ker f = \{e\}$ ならば系 8.9 より $f^{-1}(\{f(g)\}) = g$ $(\forall g \in G)$ が成り立つので補題 8.10 より単射性がしたがう。 □

## 8.3 例

**例 8.11.** *(1)* 指数関数写像 $\exp : \mathbb{R} \to \mathbb{R}^\times$ は群同型写像。

$$\ker \exp = \{0\}, \ \mathrm{Im} \exp = \mathbb{R}_{>0}.$$

*(2)* 対数関数写像 $\log : \mathbb{R}_{>0} \to \mathbb{R}$ は群同型写像。うえの指数関数写像の逆写像。

$$\ker \log = \{1\}, \ \mathrm{Im} \log = \mathbb{R}.$$

*(3)* 符号数写像 $\mathrm{sgn} : S_n \to \{\pm 1\}$ は群準同型写像。

**定義 8.12** (交代群)**.** 符号数写像 sgn の核を $n$ 次交代群とよび $A_n$ で表す：

$$A_n := \{\sigma \in S_n \mid \mathrm{sgn}(\sigma) = 1\}$$

*(4)* 可換環 $R$ にたいして行列式写像 $\det : \mathrm{GL}_n(R) \to R^\times$ は群準同型写像。
特殊線型群の定義を復習すると

$$\mathrm{SL}_n(R) = \{A \in \mathrm{GL}_n(R) \mid \det A = 1\}.$$

行列式写像の核として定義されている。

$$\ker \det = \mathrm{SL}_n(R), \ \mathrm{Im} \det = R^\times.$$

像については議論が必要ですが、お任せします。

**8.3.1**

• 符号数写像 $\mathrm{sgn} : S_n \to \{\pm 1\}$ が群準同型写像であることの証明. 示すべきことは
「任意の $\sigma, \tau \in S_n$ にたいして

$$\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau) \tag{8-4}$$

がなりたつ。」

この主張を $\sigma$ の転倒数 $n := N_\sigma$ に関する帰納法で示す。

$n = 0$ の場合。このとき $\sigma = e$ であり $\mathrm{sgn}(e) = 1$ なので等式 (8-4) がなりたつことが確認できる。

$n = 1$ の場合。$\sigma$ は Coxeter 元である。補題 6.12 により、$N_{\sigma\tau} = N_\tau \pm 1$ なので、等式 (8-4) がなりたつ。

$n > 1$ の場合。$n - 1$ までは主張が示されていると仮定する。

定理 6.10 により、$\sigma$ は $n = N_\sigma$ 個の Coxeter 元の積であらわせる。つまり、Coxeter 元 $s_{i_1}, \cdots, s_{i_n}$ が存在して

$$\sigma = s_{i_1} s_{i_2} \cdots s_{i_n}$$

を満たす。$\sigma' := s_{i_2} \cdots s_{i_n}$ とおく。すると、$\sigma = s_{i_1}\sigma'$ であり、定理 6.10 より、$N_{\sigma'} \leq n - 1$ がなりたつ。(注意：補題 6.12 とあわせると $N_{\sigma'} = n - 1$ が分かる。しかし、帰納法を使うためには上の不等式で十分。)

以下の様にして等式 8-4 が確認できる：

$$\begin{aligned}
\mathrm{sgn}(\sigma\tau) &= \mathrm{sgn}(s_{i_1}(\sigma'\tau)) \\
&= \mathrm{sgn}(s_{i_1})\mathrm{sgn}(\sigma'\tau) \\
&= \mathrm{sgn}(s_{i_1})\mathrm{sgn}(\sigma')\mathrm{sgn}(\tau) \\
&= \mathrm{sgn}(s_{i_1}\sigma')\mathrm{sgn}(\tau) \\
&= \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau)
\end{aligned}$$

ただし、二つ目と四つ目の等号には $n = 1$ の場合を用いている。三つ目の等号には帰納法の仮定を用いている。 □

**例 8.13.** 群 $G$ を考える。

*(1)* 恒等写像 $\mathrm{id}_G : G \to G$ は群同型写像。

*(2)* $G'$ を群とする。$G$ のすべての要素を $G'$ の単位元 $e_{G'}$ に送る写像

$$\epsilon : G \to G',\ \epsilon(g) := e_{G'}\ (\forall g \in G)$$

は群準同型写像。

$$\mathrm{Ker}\,\epsilon = G,\ \mathrm{Im}\,\epsilon = \{e_{G'}\}.$$

*(3)* 正規部分群 $H$ に関する商写像 $\pi : G \to G/H$ は群準同型写像。

$$\ker \pi = H,\ \mathrm{Im}\,\pi = G/H.$$

*(4)* 要素 $g \in G$ から随伴写像 $\mathrm{ad}_g : G \to G$ を以下で定めると、これは群同型写像である：

$$\mathrm{ad}_g(x) := gxg^{-1}\quad (\forall x \in G).$$

写像 $\mathrm{ad}_g$ を内部自己群同型写像とよぶこともある。

*(5)* 各要素 $g \in G$ にたいして自己群同型写像 $\mathrm{ad}_g \in \mathrm{Aut}_{\mathrm{Gp}}(G)$ が定義された。これは、つまり、写像

$$\mathrm{ad} : G \to \mathrm{Aut}_{\mathrm{gp}}(G), \quad g \mapsto \mathrm{ad}_g$$

が定義されるということである。

**定義 8.14** (群の中心)**.** 群 $G$ にたいしてその**中心** $Z(G)$ をいかで定義する：

$$Z(G) = \{g \in G \mid gh = hg \ (\forall h \in G)\}$$

**補題 8.15.**

$$Z(G) = \ker \mathrm{ad}\,.$$

像 $\mathrm{Im}\,\mathrm{ad} < \mathrm{Aut}_{\mathrm{Gp}}(G)$ を内部自己同型群とよぶ。これは正規部分群である。

## 8.4 群準同型写像定理

**補題 8.16.** 群準同型写像 $f : G \to H$ と部分群 $K < G$ を考える。次は同値：

*(1)* $K < \ker f$

*(2)* 要素 $g_1, g_2 \in G$ が $[g_1] = [g_2]$ をみたすならば $f(g_1) = f(g_2)$ が成り立つ。

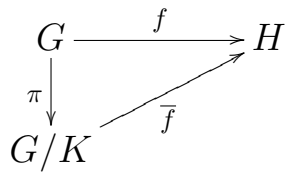
略証. (1) $\Rightarrow$ (2).

$$[g_1] = [g_2] \ \Rightarrow\ g_2^{-1}g_1 \in K \ \Rightarrow\ g_2^{-1}g_1 \in \ker f \ \Rightarrow\ f(g_2^{-1}g_1) = e \ \Rightarrow\ f(g_1) = f(g_2).$$

(2) $\Rightarrow$ (1) は略。 □

**系 8.17.** 群準同型写像 $f : G \to H$ と部分群 $K < G$ を考える。$K < \ker f$ と仮定する。

すると、対応 $\overline{f} : [g] \in G/K \mapsto f(g) \in H$ は写像を定める。




さらに $\overline{f}$ の像は $f$ のそれと一致する：

$$\operatorname{Im}\overline{f} = \operatorname{Im} f.$$

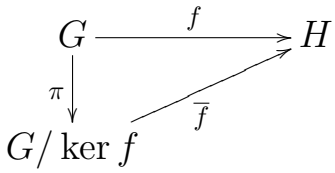
**補題 8.18.** 上の系で $K$ が正規部分群のときは $\overline{f} : G/K \to H$ は群準同型写像である。さらに次が成り立つ：

$$\ker\overline{f} = \{[g]_K \mid g \in \ker f\}$$

注意：$[g]_K$ は $K$ に関する左剰余類であることを表している。

**定理 8.19** (群準同型定理)**.** 群準同型 $f : G \to H$ を考える。次が成り立つ：

*(1)* 単射群準同型写像 $\overline{f} : G/\ker f \to H$ で $\overline{f} \circ \pi = f$ を満たすものが一意的に存在する：




*(2)* さらに $\overline{f}$ の像は $f$ のそれと一致する：

$$\operatorname{Im}\overline{f} = \operatorname{Im} f.$$

*(3)* $\overline{f}$ の像を $\operatorname{Im}\overline{f}$ に制限したものを改めて $\overline{f}$ と書くと、

群同型写像

$$\overline{f} : G/\ker f \cong \operatorname{Im} f.$$

をえる。

*Proof.* (1) 存在は既に示している。一意性を示そう。(これは $\pi$ の全射性の帰結である。)
ある写像 $g : G/\ker f \to H$ が存在して $g \circ \pi = f$ をみたしたと仮定する。
$\xi \in G/\ker f$ をとってくる。ある $x \in G$ が存在して $\xi = [x] = \pi(x)$ を満たす。よって、次の計算で $g(\xi) = \overline{f}(\xi)$ がわかる：

$$g(\xi) = g(\pi(x)) = (g \circ \pi)(x) = f(x) = (\overline{f} \circ \pi)(x) = \overline{f}(\pi(x)) = \overline{f}(\xi)$$

よって、$g = \overline{f}$ が示された。

単射性：上の補題より

$$\ker \overline{f} = \{[g]_{\ker f} \mid \ker f\} = \{[e]_{\ker f}\}$$

よって、群準同型写像 $\overline{f} : G/\ker f \to H$ は単射である。
(2) は既に示している。

(3) は (1)(2) の帰結である。 □

## 8.5 同型の構成

群準同型定理をもちいて同型な群を見つけることができます。

**例 8.20.** 符号数写像 $\mathrm{sgn} : S_n \to \{\pm 1\}$ は次の同型を誘導します：

$$\overline{\mathrm{sgn}} : S_n/A_n \xrightarrow{\cong} \{\pm 1\}.$$

**例 8.21.** 行列式写像 $\det : \mathrm{GL}_n(R) \to R^\times$ は次の同型を誘導します：

$$\overline{\det} : \mathrm{GL}_n(R)/\mathrm{SL}_n(R) \xrightarrow{\cong} R^\times$$

**例 8.22.** 群準同型写像

$$f : \mathbb{R} \to S^1, \quad f(x) := e^{2\pi x i}.$$

は $\mathrm{Ker}\, f = \mathbb{Z},\ \mathrm{Im}\, f = S^1$ なので群同型写像

$$\overline{f} : \mathbb{R}/\mathbb{Z} \xrightarrow{\cong} S^1, \quad \overline{f}([x]) := e^{2\pi x i}.$$

を誘導する。

### 8.5.1 一つの要素の生成する部分群

**例 8.23.** $G$ を群、$g \in G$ を要素とする。指数法則から次の写像は群準同型写像であるとわかる：

$$f : \mathbb{Z} \to G, \quad f(n) := g^n.$$

像と核は

$$\ker f = \{n \in \mathbb{Z} \mid g^n = e\} = \begin{cases} (\mathrm{ord}\, g)\mathbb{Z}, & (\mathrm{ord}\, g < \infty) \\ 0, & (\mathrm{ord}\, g = \infty) \end{cases}$$

$$\mathrm{Im}\, f = \{g^n \mid n \in \mathbb{Z}\} = \langle g \rangle.$$

なので、次の同型写像を得る：

$$\overline{f} : \mathbb{Z}/(\mathrm{ord}\, g)\mathbb{Z} \xrightarrow{\cong} \langle g \rangle, \quad (\mathrm{ord}\, g < \infty)$$

$$\overline{f} : \mathbb{Z} \xrightarrow{\cong} \langle g \rangle, \qquad (\mathrm{ord}\, g = \infty)$$

**系 8.24.** 巡回群 $G$ は $\mathbb{Z}$ または $\mathbb{Z}/n\mathbb{Z}$ に同型である。

## 8.6 全射群準同型

群準同型定理は全射群準同型 $f : G \to H$ があれば値域 $H$ は商群 $G/\operatorname{Ker} f$ と同一視できますね：

$$\overline{f} : G/\operatorname{Ker} f \xrightarrow{\cong} H$$

### 8.6.1 部分群の対応

**命題 8.25.** 全射群準同型 $f : G \to H$ があったとする。すると $f$ は、$\operatorname{Ker} f$ と $G$ の間の部分群と $H$ の部分群との間に全単射対応を引き起こす。さらに、それにより正規性は対応する。

きちんとした主張は以下です。

核 $\ker f$ と $G$ の間の部分群の集合を $X$, $H$ の部分群の集合を $Y$ とおく。

$$X := \{K \mid \operatorname{Ker} f < K < G\}$$
$$y := \{L \mid L < H\}$$

次の写像 $\alpha, \beta$ が定まり、互いに他の逆写像である。特にこれらは全単射である。

$$\alpha : X \to Y,\ \alpha(K) := f(K),$$
$$\beta : Y \to X,\ \beta(L) := f^{-1}(L)$$

さらに $K \in X$ が $G$ の正規部分群であるための必要十分条件は $f(K)$ が $H$ の正規部分群であることである。

証明方針. まずは、写像 $\alpha, \beta$ がキチンと定義されていることを確かめないといけない。つまり、$K \in X$ ならば $f(K)$ は $H$ の部分群であること、また、$L \in Y$ ならば $f^{-1}(L)$ は $G$ の部分群でありかつ $\operatorname{Ker} f$ を含むということ。

つぎに、互いに逆写像であることを確認する。

$\beta \circ \alpha(K) = K$ は $f^{-1}(f(K)) = K$ を意味する。包含関係 $\supset$ は集合と写像の簡単な問題。逆の包含関係 $\subset$ は補題 8.8 を使う。（あるいは直接示す。ここに $\operatorname{Ker} f < K$ を使う。）

$\alpha \circ \beta(L) = L$ は $f(f^{-1}(L)) = L$ を意味する。これも集合と写像の簡単な問題。

正規性の対応。$K$ が $G$ の正規部分群なら $f(K)$ が $H$ の正規部分群であることは簡単に確認できる。$f(K)$ が $H$ の正規部分群とする。直接、$K$ が $G$ の正規部分群であることを示してもいい。別の方法：商写像 $\pi : H \to H/f(K)$ を考えると、合成写像 $\pi \circ f : G \to H/f(K)$ は群準同型であり核が $K$ であることを示す。 □

**練習問題 8.26.** 群準同型写像 $f : G \to H$ と部分群 $K < G,\ H' < H$ にたいして $f(K)$ は $H$ の部分群であり、$f^{-1}(H')$ は $G$ の部分である。さらに $f^{-1}(f(K)) = \langle K, \operatorname{Ker} f \rangle$ が成り立つ。

### 8.6.2 像の位数

**命題 8.27.** $G$ を有限群とする。全射群準同型写像 $f : G \to H$ が存在すれば $H$ も有限群であり、$H$ の位数は $G$ の位数の約数である：

$$\#H | \#G$$

*Proof.* $f$ の誘導する同型写像 $\overline{f} : G/\operatorname{Ker} f \xrightarrow{\cong} H$ が存在するので

$$\#H = \#(G/\operatorname{Ker} f) \mid \#G$$

が成り立つ。 □

**系 8.28.** 群準同型写像 $f : G \to H$ と要素 $g \in G$ を考える。次が成り立つ：

*(1)* $\langle g \rangle$ の $f$ による像は $\langle f(g) \rangle$ である。

*(2)* $\operatorname{ord} f(g) | \operatorname{ord} g$.

*Proof.* (1) は考えてみましょう。

(2) は (1) と $\operatorname{ord} g = \#\langle g \rangle$ と先の命題の帰結です。 □

**系 8.29.** 有限群 $G, H$ の位数は互いに素とする。このとき、群準同型写像 $f : G \to H$ は自明なものしかない。

# 9 巡回群

例 8.23 より、巡回群 $G$ は $\mathbb{Z}$ またはその商群と同型であり、同型類は位数のみで決定される。

**命題 9.1.** 巡回群 $G,\ H$ が同型であるための必要十分条件は位数が等しいことである。

$$G \cong H \quad \Leftrightarrow \quad \#G = \#H.$$

**定義 9.2.** 位数 $n \in \mathbb{Z}_{>0} \cup \{\infty\}$ の巡回群を $C_n$ とあらわす。（生成元を指定することもおおい。）

もちろん、$n \in \mathbb{N}$ ならば $C_n \cong \mathbb{Z}/n\mathbb{Z}$ であり、$C_\infty \cong \mathbb{Z}$ です。

## 9.1 無限巡回群

**命題 9.3.** $g$ を生成元とする無限巡回群 $C_\infty$ を考える。
整数 $a \geq 0$ にたいして $g^a$ の生成する部分群を $H_a$ とあらわす：

$$H_a = \langle g^a \rangle = \{g^{an} \mid n \in \mathbb{Z}\}.$$

*(1)* 任意の部分群 $H$ にたいしてある非負整数 $a \geq 0$ が一意的に存在して $H = H_a$ を満たす。
特に、$a, b \geq 0$ にたいして $a = b \quad \Leftrightarrow \quad H_a = H_b$ である。

*(2)* $C_\infty$ の任意の非自明な部分群は無限巡回群である。

*Proof.* (1) $H = \{e\}$ の場合は $H = H_0$ である。$a > 0$ にたいして $H_a \neq \{e\}$ なので、一意性も示された。

$H \neq \{e\}$ とする。
主張：ある $b > 0$ が存在して $g^b \in H$ を満たす。
$\because$ 仮定より $h \in H,\ h \neq e$ がとれる。よって、ある $c \in \mathbb{Z} \setminus \{0\}$ が存在して $h = g^c$ を満たす。$c > 0$ であればこれでよい。$c < 0$ のばあいは $g^{-c} = h^{-1} \in H$ なので、これで主張が示された。

$a := \min\{b > 0 \mid g^b \in H\}$ とおく。包含関係 $H_a \subset H$ は明らか、
逆向きの包含関係を示す。
$h \in H$ をとってくる、ある $q \in \mathbb{Z}$ と $r$ $(0 \leq r < a)$ が存在して

$$h = g^{aq+r} = (g^a)^q g^r$$

が成り立つ。これは

$$g^r = (g^a)^{-q} h \in H$$

を意味するが、$a$ の選びからから $r = 0$ をえる。よって、$h \in H_a$ が示された。
ゆえに $H = H_a$ を結論する。

一意性は

$$\min\{c > 0 \mid g^c \in H_a\} = a$$

なので $H_a = H_b$ ならば

$$a = \min\{c > 0 \mid g^c \in H_a\} = \min\{c > 0 \mid g^c \in H_b\} = b$$

により導ける。 □

**練習問題 9.4.** *(1)* 正整数 $a, b \geq 1$ にたいして次がなりたつ：

$$a|b \iff b\mathbb{Z} < a\mathbb{Z} \iff H_b < H_a.$$

*(2)* 正整数 $N$ にたいして次の写像は全単射である：

$$\{a \geq 1 \mid a|N\} \to \{H \mid N\mathbb{Z} < H < \mathbb{Z}\}, \quad a \mapsto a\mathbb{Z}.$$

*(3)* 正整数 $a, b \geq 1$ を考える。
次を示せ：

*(i)* 正整数 $d > 0$ が $a, b$ の最大公約数であるための必要十分条件は $\langle a, b\rangle = d\mathbb{Z}$ である。
ただし $\langle a, b\rangle$ は整数 $a, b \in \mathbb{Z}$ が加法群 $\mathbb{Z}$ のなかで生成する部分群を表す。

*(ii)* 正整数 $d > 0$ が $a, b$ の最大公約数とする。ある整数 $p, q$ が存在して

$$pa + qb = d$$

を満たすことを示せ。

*(4)* 正整数 $a, b \geq 1$ が互いに素であるための必要十分条件はある整数 $p, q$ が存在して

$$pa + qb = 1$$

を満たすことであることを示せ。

## 9.2 有限巡回群

**命題 9.5.** 自然数 $N$ にたいして $g$ を生成元とする位数 $N$ の巡回群 $C_N$ を考える。

*(1)* 整数 $a > 0$ にたいして $a$ と $N$ の最大公約数を $d = \gcd(a, N)$ とし、$m = N/d$ とおく。
すると、$g^a$ の位数は $\mathrm{ord}_{C_N} g^a = m$ である。

*(2)* $g^a$ の生成する部分群を $H_a$ とあらわす：

$$H_a := \langle g^a \rangle = \{g^{an} \mid n \in \mathbb{Z}\}$$

すると $H_a$ は $m$ 次の巡回群である。

*(3)* 任意の部分群 $H$ にたいしてある正の $N$ の約数 $a$ が一意的に存在して $H = H_a$ を満たす。
（例：$a = N$ の場合は $H_N = \{e\}$，$a = 1$ の場合が $H_1 = C_N$ である。）

*(4)* $C_N$ の任意の部分群は巡回群である。

*Proof.* (1)(2) は省略。

(3) 例 8.23 の全射群準同型 $f : \mathbb{Z} \to C_N,\ n \mapsto g^n$ を考える。（$\mathbb{Z}$ は 1 を生成元とする無限巡回群であることを思い出す。なので、前節の結果が使える。）
命題 8.25 より、部分群 $H < C_N$ にたいして $f^{-1}(H)$ は $\mathrm{Ker}\, f = N\mathbb{Z}$ を含む $\mathbb{Z}$ の部分群である。
よって、命題 9.3 と練習問題 9.4 から、ある $N$ の正の約数 $a$ が一意的に存在して $f^{-1}(H) = a\mathbb{Z}$ を満たす。よって、$H = f(f^{-1}(H)) = f(a\mathbb{Z}) = \langle g^a \rangle$ である。
ここまでで用いた二つの対応は全単射対応なので $a$ は一意的である。

$$\{H \mid H < C_N\} \leftrightarrows \{K \mid N\mathbb{Z} < K < \mathbb{Z}\} \leftrightarrows \{a \geq 1 \mid a|N\}$$

□

**練習問題 9.6.** 上の命題の *(1)(2)* を示せ。

# 10　非同型の判定

群 $G, H$ が同型ならばそれらは群論的には同じとみなしてよい。同型であることを確認するのは同型を構成しなければいけないが、非同型であることは確認しやすかったりする。

### 10.0.1　位数の不一致

同型な群は位数が一致する。

**例 10.1.** 群 $\mathbb{Z}/2\mathbb{Z}$ と群 $\mathbb{Z}/3\mathbb{Z}$ は位数がそれぞれ $2, 3$ であり、異なっているので非同型。

**例 10.2.** 群 $\mathbb{Z}$ と群 $\mathbb{R}$ は位数がそれぞれ可算無限、非可算無限であり、異なっているので非同型。

### 10.0.2　要素の位数分布の不一致

同型な群は要素の位数分布が一致する。

**例 10.3.** 群 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ と群 $\mathbb{Z}/4\mathbb{Z}$ を考える。
　$\mathbb{Z}/4\mathbb{Z}$ には位数 $4$ の要素が存在するが、$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ には存在しないことを確認して、非同型であることが示せる。

### 10.0.3　可換性

可換群に同型な群は可換

**例 10.4.** 群 $\mathbb{Z}/6\mathbb{Z}$ と群 $S_3$ を考える。
　$\mathbb{Z}/6\mathbb{Z}$ は可換群であるが、$S_3$ は非可換群なので、非同型であることが示せる。

# 11　群の直積

**定義 11.1.** 群 $G = (G, \mu_G),\ H = (H, \mu_H)$ の直積群 $G \times H$ とは下部集合が $G$ と $H$ の下部集合の直積集合 $G \times H$ に積を

$$(g_1, h_1)(g_2, h_2) := (g_1 g_2, h_1 h_2)$$

で定めたものと定義する。
　単位元は

$$e_{G\times H} = (e_G, e_H).$$

要素 $x = (g, h)$ の逆元は

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

　同様に複数個の群の直積 $G_1 \times G_2 \times \cdots \times G_n$ や、無限個の群の直積 $\prod_{i=1}^{\infty} G_i$ を定義する。

　少しだけ注意したいのは次の可換性です：

$$(g, e_H)(e_G, h) = (g, h) = (e_G, h)(g, e_H).$$

**例 11.2.** 可換群の直積群は可換群である。

**例 11.3.** *(1)* $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$.

*(2)* $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} = \mathbb{Z}^3$.

**例 11.4.** *(1)* 位数 4 の群は次のいずれかの群と同型である。特に可換群である。

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z}$$

*(2)* しかし、これら二つの群は非同型：

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \ncong \mathbb{Z}/4\mathbb{Z}.$$

（これにて位数 4 の群の同型類の分類が完了した。）

*(3)* 一方、次の同型がある：

$$\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

**命題 11.5.** $G$ を群、$H, K$ を $G$ の部分群とする。任意の $h \in H,\ k \in K$ にたいして $hk = kh$ が成り立つと仮定する。

このとき、次が成り立つ：

*(1)* 写像

$$\phi : H \times K \to G, \quad \phi(h,k) := hk \quad (\forall h \in H,\ k \in K)$$

は群準同型写像である。

*(2)* 写像

$$\psi : H \cap K \to H \times K, \quad \phi(l) := (l, l^{-1})$$

は単射群準同型写像であり、等式

$$\operatorname{Im}\psi = \operatorname{Ker}\phi$$

がなりたつ。

**注意 11.6.** 上の命題で $hk = kh \ \ (\forall h \in H,\ k \in K)$ という仮定がなければ $\phi, \psi$ は群準同型写像にはならない。

**系 11.7.** $G$ を群、$H, K$ を $G$ の部分群とする。次が成り立つと仮定する：

*(i)* $\langle H, K\rangle = G$. つまり、$H$ と $K$ は $G$ を生成している。

*(ii)* $H \cap K = \{e\}$.

*(iii)* 任意の $h \in H,\ k \in K$ にたいして $hk = kh$ が成り立つ

このとき、写像

$$f : H \times K \xrightarrow{\cong} G, \quad f(h,k) := hk \quad (\forall h \in H,\ k \in K)$$

は群同型写像である。

**練習問題 11.8.** *(1)*

$$\operatorname{ord}_{G\times H}(g,h) = \begin{cases} \operatorname{lcm}(\operatorname{ord}_G g, \operatorname{ord}_H h) & \operatorname{ord}_G(g) < \infty \text{ かつ } \operatorname{ord}_H(h) < \infty \\ \infty & \operatorname{ord}_G(g) = \infty \text{ または } \operatorname{ord}_H(h) = \infty \end{cases}$$

ただし lcm は最小公倍数を意味する。

*(2)* $G' < G,\ H' < H \ \Rightarrow\ G' \times H' < G \times H$.

*(3)* $G' \lhd G,\ H' \lhd H \ \Rightarrow\ G' \times H' \lhd G \times H.$

さらに、この状況で、以下の写像は群同型写像である：

$$(G \times H)(G' \times H) \overset{\cong}{\to} (G/G') \times (H/H'),\ [(g,h)] \mapsto ([g],[h]).$$

*(4)* 次の写像は群準同型である。

*(i)* $p_1 : G \times H \to G,\ (g,h) \mapsto g.$

*(ii)* $p_2 : G \times H \to G,\ (g,h) \mapsto h.$

*(iii)* $\Delta : G \to G \times G,\ g \mapsto (g,g)$

*(5)* うえの写像 $p_1, p_2$ の誘導する写像

$$\mathrm{Hom}_{\mathrm{Gp}}(G, H \times K) \to \mathrm{Hom}_{\mathrm{Gp}}(G,H) \times \mathrm{Hom}_{gp}(G,K), \quad f \mapsto (p_1 \circ f, p_2 \circ f).$$

は全単射である。

*(6)* 次の写像は全単射である：

$$\mathrm{Hom}(\mathbb{Z} \times \mathbb{Z}, G) \to \{(g,h) \in G \times G \mid gh = hg\}, \quad f \mapsto (f(1,0), f(0,1)).$$

# 12　有限生成アーベル群の構造定理

可換群のことをアーベル群とも呼びます。

**定義 12.1.** 群が有限生成とは有限個の要素から構成される生成系をもつことをいう。

有限群は有限生成である。有限生成だが有限群でない群もある。たとえば加法群 $\mathbb{Z}$ は $\{1\}$ を生成系としてもつので有限生成。

**定理 12.2** (有限生成アーベル群の構造定理)**.** 有限生成アーベル群 $G$ は次の形の群と同型である：

$$\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}.$$

ここで $m_i \geq 2$ は自然数であり、つぎの関係を満たす：

$$m_1 | m_2 | \cdots | m_r$$

系として有限アーベル群の構造定理が導出できますね。

**定理 12.3** (有限アーベル群の構造定理)**.** 有限群 $G$ は次の形の群と同型である：

$$\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}$$

ここで $m_i \geq 2$ は自然数であり、つぎの関係を満たす：

$$m_1 | m_2 | \cdots | m_r$$

**注意 12.4.** 無限生成アーベル群はもっと複雑である。巡回群 $\mathbb{Z},\ \mathbb{Z}/m\mathbb{Z}$ の無限直積と同型でないものも存在する。例えば有理数のなす加法群 $\mathbb{Q}$ はそういう例である。

### 12.0.1 準備

**補題 12.5.** $G$ をアーベル群、$g_1, \cdots, g_N$ を $G$ の要素とする。次がなりたつ：

*(1)* 写像

$$f : \mathbb{Z}^N \to G, (k_1, \cdots, k_N) \mapsto k_1 g_1 + \cdots + k_N g_N$$

は群準同型写像である。

*(2)* 部分集合 $\{g_1, \cdots, g_N\}$ が生成系であるための必要十分条件は写像 $f$ が全射なことである。

**補題 12.6.** $G$ をアーベル群とする。ある $m_1, m_2, \cdots, m_r \in \mathbb{N}$ にたいして同型

$$G \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}$$

が存在するための必要十分条件は以下の条件を満たす生成系 $\{g_1, g_2, \cdots, g_r\}$ が存在することである：
$r$ 次の整数ベクトル $\vec{k} = (k_i) \in \mathbb{Z}^r$ が

$$k_1 g_1 + k_2 g_2 + \cdots + k_r g_r = 0$$

を満たすための必要十分条件は

$$k_1 \in m_1\mathbb{Z},\ k_2 \in m_2\mathbb{Z},\ \cdots\ k_r \in m_r\mathbb{Z}$$

である。

*Proof.* 条件は上の補題 12.5 で作った全射準同型写像 $f$ の核 $\mathrm{Ker}\, f$ が

$$\mathrm{Ker}\, f = m_1\mathbb{Z} \times m_2\mathbb{Z} \times \cdots \times m_r\mathbb{Z} \subset \mathbb{Z}^r$$

ということに他ならない。 □

この補題の $m_1, \cdots, m_r$ は 0 かも知れないことを注意しておく。定理の証明の為には次の形に主張を言い換えておくと便利である。

**定理 12.7** (有限生成アーベル群の構造定理の言い換え)**.** 有限群 $G$ は次の形の群と同型である：

$$\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_N\mathbb{Z}$$

ここで $m_i$ は 2 以上の自然数または 0 であり、つぎの関係を満たす：

$$m_1\mathbb{Z} \supset m_2\mathbb{Z} \supset \cdots \supset m_N\mathbb{Z}$$

### 12.0.2 証明

*Proof.* $G$ の生成系 $\{g_1, \cdots, g_N\}$ で構成要素の個数が最小なものの個数 $N$ に関する帰納法を用いる。

$N = 1$ のとき。これは $G$ が巡回群ということ。この場合はすでに示している。

$N - 1$ までは命題が示されたと仮定する。（つまり、$N - 1$ 個以下の要素から生成されるアーベル群は定理で与えらえた形のものと同型である、と仮定する。）
ある $G$ の生成系 $\underline{g} := \{g_1, \cdots, g_N\}$ をとってきて、補題 12.5 の全射群準同型写像 $f_{\underline{g}} : \mathbb{Z}^N \to G$ を作る。
もし、$\mathrm{Ker}\, f_{\underline{g}} = 0$ ならである生成系 $\underline{g}$ が存在すれば、$f_{\underline{g}}$ は同型写像となり、証明は終わる。
なので、以下ではどんな生成系 $\underline{g}$ にたいしても $\mathrm{Ker}\, f_{\underline{g}} \neq 0$ と仮定する。

正の整数 $n_{\underline{g}}$ を $\mathrm{Ker}\, f_{\underline{g}}$ の要素の成分として現れる最小の正整数として定義する。

$$n_{\underline{g}} = \min\{m > 0 \mid \exists i = 1, \cdots, N \text{ s.t. } (n_1, \cdots, n_{i-1}, n, n_{i+1}, \cdots, n_N)^t \in \mathrm{Ker}\, f \text{ for some } n_1, \cdots, n_N \in \mathbb{Z}\}$$

$\mathcal{G}$ を $N$ 個の要素から構成される $G$ の生成系（に順序を与えたもの）の集合とする。そして

$$n_{\min} := \min\{n_{\underline{g}} \mid \underline{g} \in \mathcal{G}\}$$

と定める。以下、$g := \{g_1, \cdots, g_N\}$ を $n = n_{\underline{g}}$ を満たす $G$ の生成系とする。さらに $n_{\underline{g}}$ の定義に現れた $i$ が 1 と異なる場合は、生成系の順序を入れ替えることで $i = 1$ としてよい。

以下、$n_1 := n_{\min}$ とあらわす。なので整数の組 $n_2, \cdots, n_N \in \mathbb{Z}$ が存在して、

$$n_1 g_1 + n_2 g_2 + \cdots + n_N g_N = 0 \tag{12-5}$$

がなりたつ。

**主張 12.8.** *(1)* $n_2, \cdots, n_N$ は $n_1$ の倍数である。

*(2)* 任意の要素 $\vec{m} = (m_1, \cdots, m_N)^t \in \mathrm{Ker}\, f_{\underline{g}}$ の第 1 成分 $m_1$ は $n_1$ の倍数である。

*Proof.* (1) $n_1 = 1$ の場合は明らか。$n_1 \geq 2$ とする。

ある $i = 2, \cdots, N$ で $n_i$ が $n_1$ の倍数ではないものが存在したとする。$n_i = qn_1 + r$ を満たす整数 $q$ と $r = \{1, \cdots, n_1 - 1\}$ が存在する。すると部分集合 $\{g_1 + qg_i, g_2, \cdots, g_N\} \subset G$ は $G$ の生成系であり、等式

$$n_1(g_1 + qg_1) + n_2 g_2 + \cdots + n_{i-1} g_{i-1} + r g_i + n_{i+1} g_{i+1} + \cdots n_N g_N = 0$$

を満たす。これは $n_{\min}$ の定義に反する。

(2) $n_1 \geq 2$ としてよい。$m_1$ が $n_1$ の倍数でないとする。$m_1 = qn_1 + r$ を満たす $q \in \mathbb{Z}$ と $r \in \{1, \cdots, n_1 - 1\}$ が存在する。$\vec{m}$ は $f_{\underline{g}}$ の核に属するので等式

$$m_1 g_1 + m_2 g_2 + \cdots + m_N g_N = 0 \tag{12-6}$$

を満たす。等式 (12-5) を用いて、$g_1, \cdots, g_N$ の関係式で $g_1$ の係数が $r$ のものを作ることが出来るので $n_1 = n_{\min}$ の定義に矛盾する。

□

$i = 2, \cdots, N$ にたいして $q_i := n_i / n_1$ とおく。さらに

$$g_1' := g_1 + q_2 g_2 + \cdots + q_N g_N, \quad \underline{g'} := \{g_1', g_2, \cdots, g_N\}, \quad \underline{g''} := \{g_2, \cdots, g_N\}$$

とおく。等式 (12-5) は

$$n_1 g_1' = 0$$

とあらわされる。

**主張 12.9.** *(1)* $\vec{k} \in \mathbb{Z}^N$ が

$$k_1 g_1' + k_2 g_2 + \cdots + k_N g_N = 0 \tag{12-7}$$

を満たしたと仮定する（つまり、$\vec{k} \in \mathrm{Ker}\, f_{\underline{g'}}$）。すると、$k_1$ は $n_1$ の倍数であり、さらに、

$$k_1 g_1 = 0, \ k_2 g_2 + \cdots + k_N g_N = 0$$

がなりたつ。

とくに $n_1 g_1 = 0$ がなりたつ。

*(2)* $n_1 \geq 2$.

*Proof.* (1) 等式 (12-7) を $g_1$ を使って表し、補題 12.8(2) を適用することで $k_1$ は $n_1$ の倍数であることが分かる。$n_1 g_1' = 0$ であったから、$k_1 g_1' = 0$ を得る。

(2) $n_1 = 0$ ならば $0 = n_1 g_1 = g_1$ となり生成系の構成要素の仮定に矛盾する。 □

$G' := \langle g_2, \cdots, g_N \rangle$ とおく。これは $N-1$ 個の要素で生成される（有限生成）アーベル群である。

群 $G'$ の生成系と $\{g_1'\}$ の合併集合は $G$ の生成系である。もしも $G'$ が $N-2$ 個以下の要素で構成される生成系をもてば、$N$ の定義に矛盾するので、$G'$ の極小な生成系の構成要素は $N-1$ 個である。

帰納法の仮定から $G'$ は生成系 $\{g_2', \cdots, g_N'\}$ で次の性質を持つものが存在する。

ある $m_2, \cdots, m_N \in \mathbb{Z}_{\geq 2} \sqcup \{0\}$ が存在して次が成り立つ：

(i)
$$m_2\mathbb{Z} \supset \cdots \supset m_N\mathbb{Z}$$

(ii) $N-1$ 次の整数ベクトル $\vec{k} = (k_i) \in \mathbb{Z}^{N-1}$ が
$$k_2 g_2' + \cdots + k_{N-1} g_{N-1}' = 0$$
を満たすための必要十分条件は
$$k_2 \in m_2\mathbb{Z}, \ \cdots \ k_{N-1} \in m_{N-1}\mathbb{Z}$$
である。

主張 12.9 より、部分集合 $\{g_1', g_2', \cdots, g_N'\}$ は上と同様な性質をもつ $G$ の生成系なので、これで $G$ は同型
$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_N\mathbb{Z}$$
を持つことが示された。さらに主張 12.8 をこの生成系に適用すれば
$$m_1\mathbb{Z} \supset m_2\mathbb{Z} \supset \cdots \supset m_N\mathbb{Z}$$
をえる。 □

**注意 12.10.** この証明をそのまま一般化して *"*単項イデアル整域上 $R$ の有限生成加群の構造定理*"* が得られる。整数環 $\mathbb{Z}$ 上の加群はアーベル群に他ならず、$R = \mathbb{Z}$ の場合が上で与えた定理である。それを体上の一変数多項式環 $R = K[X]$ に適用すると *Jordan* 標準形の存在証明が得られる。

# 13　作用（群の集合への左作用）

## 13.1　作用

**定義 13.1.** 群 $G$ の集合 $X$ への（左）作用 $\lambda : G \curvearrowright X$ とは、群準同型

$$\lambda : G \to \mathrm{Aut}_{\mathrm{set}}(X).$$

の別名である。

作用（= 群準同型）$\lambda$ による $g \in G$ の像を

$$\lambda_g := \lambda(g) \in \mathrm{Aut}_{\mathrm{Set}}(X)$$

とあらわす。

さらに、場合によっては全単射 $\lambda_g : X \to X$ による $x \in X$ の像を

$$gx := g \cdot x := g \cdot_\lambda x := \lambda_g(x) \in X$$

とあらわす。

次がなりたつ：

$$(gh) \cdot x = g \cdot (h \cdot x) \ \ (\forall g, h \in G,\ x \in X)$$
$$e \cdot x = x \ \ (\forall x \in X)$$

自然にあらわれる作用はいろいろあります。

**例 13.2.** *(1)* $\mathrm{GL}(n;\mathbb{R}) \curvearrowright \mathbb{R}^n$

*(2)* $S_n \curvearrowright \{1, 2, \cdots, n\}$.

**補題 13.3.** $G$ を群、$X$ を集合とする。

作用 $\lambda : G \curvearrowright X$ を与えることは、写像

$$\lambda : G \to \mathrm{Hom}_{\mathrm{Set}}(X, X),\ g \mapsto \lambda_g$$

で次を満たすものを与えることと同値：

*(1)* $\lambda_{gh} = \lambda_g \lambda_h$.

*(2)* $\lambda_e = \mathrm{id}_X$

**定義 13.4.** 作用 $\lambda : G \curvearrowright X$ を考える。

*(1)* 要素 $x \in X$ の安定化部分群 $\mathrm{stab}\, x < G$ をいかで定める：

$$\mathrm{stab}\, x := \{g \in G \mid gx = x\}.$$

*(2)* 要素 $x \in X$ の $G$ 軌道 $Gx$ を次で定める：

$$Gx := \{gx \mid g \in G\}$$

*(3)* 集合 $X$ の作用 $\lambda : G \curvearrowright X$ による商集合 $G\backslash X$ を次で定める：

$$G\backslash X := \{Gx \mid x \in X\} \subset \mathcal{P}(X)$$

*(4)* $Gx$ に対応する $G\backslash X$ の要素を $[x]$ または $\bar{x}$ であらわす。

*(5)* 以下で定義される写像 $\pi : X \to G\backslash X$ を商写像とよぶ：

$$\pi : X \to G\backslash X, \quad x \mapsto [x]$$

*(6)* 部分集合 $R \subset X$ は次をみたすとき作用 $\lambda : G \curvearrowright X$ に関する完全代表系と呼ばれる：

任意の $x \in X$ にたいしてある $r \in R$ が一意的に存在して $Gx = Gr$ を満たす。

### 13.1.1 軌道分解

左剰余のところで見たような性質がなりたちます。

**補題 13.5.** 作用 $\lambda : G \curvearrowright X$ を考える。

要素 $x, y \in G$ にたいして次の命題は同値：

*(1)* $Gx = Gy$

*(2)* $Gx \cap Gy \neq \phi$

*(3)* $x \in Gy$

*(4)* $y \in Gx$

**定理 13.6** (軌道分解)**.** 作用 $\lambda : G \curvearrowright X$ を考える。この作用の完全代表系 $R \subset X$ をとってくる。

すると、次の非交和分解がなりたつ：

$$X = \bigsqcup_{x \in R} Gx$$

**系 13.7.** 上の定理の状況で次がなりたつ：

$$\#X = \sum_{x \in R} \#Gx$$

**注意 13.8.** 左剰余類の場合とは異なり、$x \in R$ ごとに $Gx$ の要素の個数は異なるかも知れない。

なので、上の系の式はこれ以上はまとめられない。

### 13.1.2 軌道を商集合として表示する。

**定理 13.9.** 作用 $\lambda : G \curvearrowright X$ を考える。

要素 $x \in X$ から定まる写像

$$\lambda^x : G \to Gx, \quad g \mapsto gx$$

は全単射

$$G/\operatorname{stab} x \cong Gx, \quad [g]_{\operatorname{stab} x} \mapsto gx$$

を誘導する。

**系 13.10.** 作用 $\lambda : G \curvearrowright X$ と要素 $x \in X$ にたいして、次がなりたつ：

$$(\#Gx)(\#\operatorname{stab} x) = \#G.$$

## 13.2 例

**例 13.11.** 次の作用を考える：

$$\lambda : \mathbb{R}^{>0} \curvearrowright \mathbb{R}^{n+1},\quad r \cdot x \ \text{（スカラー倍）}.$$

*(1)* $x \neq 0$ の場合。軌道 $\mathbb{R}^{>0}x$ は $x$ を通り原点に伸びる半直線。安定化部分群は $\operatorname{stab} x = \{1\}$.

*(2)* 軌道 $\mathbb{R}^{>0}0$ は原点のみからなる集合。安定化部分群は $\operatorname{stab} 0 = \mathbb{R}^{>0}$.

*(3)* $n$ 次元球面 $S^n := \{x \in \mathbb{R}^{n+1} \mid |x| = 1\}$ と原点の合併集合 $R = S^{n+1} \sqcup \{0\}$ が完全代表系の一例。

**例 13.12.** 次の作用を考える：

$$\lambda : \mathbb{R}^{>0} \curvearrowright \mathbb{R}^{n+1} \setminus \{0\},\quad r \cdot x \ \text{（スカラー倍）}.$$

*(1)* $x \neq 0$ の場合。軌道 $\mathbb{R}^{>0}x$ は $x$ を通り原点に伸びる半直線。安定化部分群は $\operatorname{stab} x = \{1\}$.

*(2)* $n$ 次元球面 $S^n := \{x \in \mathbb{R}^{n+1} \mid |x| = 1\}$ が完全代表系の一例。

*(3)* 商集合 $\mathbb{R}^{>0}\backslash(\mathbb{R}^{n+1} \setminus \{0\})$ は商写像を通じて $n$ 次元球面 $S^n$ と同一視できる。

**例 13.13.** 次の作用を考える：

$$\lambda : \mathbb{R}^{\times} \curvearrowright \mathbb{R}^{n+1} \setminus \{0\},\quad r \cdot x \ \text{（スカラー倍）}.$$

*(1)* 軌道 $\mathbb{R}^{\times}x$ は $x$ と原点を通る直線から原点を抜いたもの。安定化部分群は $\operatorname{stab} x = \{1\}$.

*(2)* 商集合 $\mathbb{R}^{\times}\backslash(\mathbb{R}^{n+1} \setminus \{0\})$ は $\mathbb{R}^{n+1}$ の 1 次元部分空間を集めたものと見做せ $n$ 次元射影空間と呼ばれ $\mathbb{P}^n(\mathbb{R})$ と書かれる。

*(3)* 完全代表系の一例は次のようなもの：

$$R = \bigsqcup_{i=1}^{n} R_i$$

ただし $R_1 := \{x \in S^n \mid x_1 > 0\}$, $R_i := \{x \in S^n \mid x_1 = \cdots = x_{i-1} = 0,\ x_i > 0\}$ $(i = 2, \cdots, n)$

### 13.2.1

**例 13.14.** $n \geq 1$ を自然数、$X$ を集合とする。$n$ 個の $X$ の直積

$$X^n = X \times X \times \cdots \times X$$

に $n$ 次対称群 $S_n$ を次のように作用させる：

(13-8) $$\sigma(x_1, x_2, \cdots, x_n) := (x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, \cdots, x_{\sigma^{-1}(n)}).$$

*(1)* 商集合 $S_n \backslash X^n$ は $X$ の対称積と呼ばれる。

*(2)* $x = (x_1, x_2, \cdots, x_n) \in X^n$ の安定化部分群 $\operatorname{stab} x$ は

- *(i)* すべての成分が等しい場合、つまり $x_1 = x_2 = \cdots = x_n$ の場合は、$\operatorname{stab} x = S_n$ である。
- *(ii)* すべての成分が互いに相異なる場合、つまり $x_i \neq x_j \quad (i \neq j)$ の場合は、$\operatorname{stab} x = \{e\}$ である。
- *(iii)* 一般的な場合は考えてみよう。

**練習問題 13.15.** 定義 (13-8) が作用を定めることを示せ。

### 13.2.2 （左）正則作用

**例 13.16.** $G$ を群とする。群 $G$ の集合 $G$ への作用 $\lambda : G \curvearrowright G$ を以下で定義する：

$$g \cdot x := gx \quad (\forall g \in G, x \in G).$$

これを（左）正則作用とよぶ。

*(1)* 任意の $x \in G$ にたいして

$$\operatorname{stab} x = \{e\}, \quad Gx = G$$

*(2)* $G \backslash G = \{[e]\}$.

## 13.3 作用の性質

**定義 13.17.** *(1)* 作用 $\lambda : G \curvearrowright X$ が推移的とは、任意の $(x, y) \in X$ にたいしてある $g \in G$ が存在して $gx = y$ が成り立つことと定める。

*(2)* 作用 $\lambda : G \curvearrowright X$ が自由とは $g \in G$ がある $x \in X$ にたいして $gx = x$ をみたせば $g = e$ が成り立つことと定める。

*(3)* 作用 $\lambda : G \curvearrowright X$ が効果的とは $g \in G$ が任意の $x \in X$ にたいして $gx = x$ をみたせば $g = e$ が成り立つことと定める。

**補題 13.18.** 作用 $\lambda : G \curvearrowright X$ が効果的であるための必要十分条件は対応する群準同型写像 $\lambda : G \to \mathrm{Aut}_{\mathrm{Set}}(X)$ が単射であることである。

*Proof.* 必要性：作用 $\lambda : G \curvearrowright X$ が効果的であると仮定する。

要素 $g \in \mathrm{Ker}\,\lambda$ をとってくる。つまり、これは $\lambda_g = \mathrm{id}_X$ を満たす $G$ の要素をとってくるということ。すると、$g \cdot x = x \ \ (\forall x \in X)$ が次のように導出できる：

$$g \cdot x = \lambda_g(x) = \mathrm{id}_X(x) = x.$$

いま、作用が効果的と仮定しているので $g = e$ を結論する。

ゆえに、群準同型写像 $\lambda$ は単射である。 □

**補題 13.19.** 作用 $\lambda : G \curvearrowright X$ が自由であるための必要十分条件は任意の要素 $x \in X$ にたいして

$$\#\,\mathrm{stab}\,x = 1$$

がなりたつことである。

作用の基本的な性質を思い出しましょう：

$$X = \bigsqcup Gx, \quad Gx \cong G/\,\mathrm{stab}\,x.$$

上の補題から次が従います。

**系 13.20.** 有限集合 $X$ に群 $G$ が作用しているとする：$\lambda : G \curvearrowright X$. 作用が自由であれば $G$ は有限群であり、この作用の完全代表系を $R$ とすると

$$\#X = \#R \times \#G$$

がなりたつ。

### 13.3.1

**補題 13.21.** $G$ を群とする。左正則作用 $\lambda : G \curvearrowright G$ は自由である、とくに効果的である。

この補題から、任意の有限群は対称群の部分群として実現されることがわかる。

**定理 13.22** (Cayley の定理)**.** 有限群 $G$ にたいして、単射準同型写像 $f : G \to S_{|G|}$ が存在する。

*Proof.* 同型 $\mathrm{Aut}_{\mathrm{Set}}(G) \cong \mathrm{Aut}_{\mathrm{Set}}(\{1, 2, \cdots, |G|\})$ と左正則作用に対応する単射群準同型写像 $\lambda : G \to \mathrm{Aut}_{\mathrm{Set}}(G)$ を合成すればいい。 □

## 13.4 右作用

### 13.4.1 群の集合への右作用

右作用という概念もあり、左作用と同様に軌道、安定化部分群等が定義でき、同様の命題が成り立ちます。

**定義 13.23.** $G$ を群、$X$ を集合とする。

右作用 $\rho : X \curvearrowleft G$ とは部分集合

$$\{\rho_g \mid g \in G\} \subset \mathrm{Hom}_{\mathrm{Set}}(X, X)$$

で次を満たすものをいう

*(1)* $\rho_{gh} = \rho_h \circ \rho_g$.

*(2)* $\rho_e = \mathrm{id}_X$

右作用 $\rho : X \curvearrowleft G$ が与えられたときに

$$xg = x \cdot g := \rho_g(x)$$

とかあらわすことにすると、上の条件 (1)(2) はそれぞれ次の様になる：

$$x \cdot (gh) = (x \cdot g) \cdot h, \quad x \cdot e = x \quad (\forall x \in X)$$

軌道は $xG$, 安定化部分群は $\mathrm{stab}\, x$ とあらわし、商集合は $X/G$ とあらわします。

**注意 13.24.** これらに関して左作用の場合と同様の命題が成り立ちます。
証明は直接行ってもいいし、または、反群を用いることで左作用に帰着することでも行えます。

**例 13.25.** 群 $G$ とその部分群 $H < G$ を考える。
群 $H$ の集合 $G$ への右作用を次で定義する：

$$\rho : G \curvearrowleft H, \quad \rho_h(g) := gh.$$

*(1)* $g \in G$ の軌道は左剰余類 $gH$ に他ならない。

*(2)* 商集合 $G/H$ は $H$ の左剰余類による商集合と一致する。

## 13.5 練習問題

**練習問題 13.26.** 作用 $\lambda : G \curvearrowright X$ を考える。

*(1)* $\mathrm{stab}(gx) = g(\mathrm{stab}\, x)g^{-1}$.

*(2)* 要素 $x \in X$ にたいして

$$\lambda^x : G \to X, \quad \lambda^x(g) := gx \quad (\forall g \in G,\ x \in X)$$

と定める。次がなりたつ：

$$\mathrm{stab}\, x = (\lambda^x)^{-1}(x), \quad Gx = \mathrm{Im}\, \lambda^x.$$

*(3)* 部分集合 $R \subset X$ が $\lambda : G \curvearrowright X$ に関する完全代表系であるための必要十分条件は制限写像 $\pi|_R : R \to G\backslash X$ が全単射であることである。

*(4)* 二点 $x, y \in X$ は軌道が一致する（つまり、$Gx = Gy$ をみたす）ならば安定化部分群 $\mathrm{stab}\, x,\ \mathrm{stab}\, y$ の間には全単射が存在する。

*(5)* $\ker[\lambda : G \to \mathrm{Aut}_{\mathrm{set}}(X)] = \bigcap_{x \in X} \mathrm{stab}\, x$

**練習問題 13.27.** *(1)* 自由な作用は効果的である。

*(2)* 作用 $\lambda : G \curvearrowright X$ にたいして次は同値：

*(i)* $\lambda$ は推移的。

*(ii)* ある $x \in X$ が存在して $Gx = X$ がなりたつ。

*(iii)* 任意の $x \in X$ にたいして $Gx = X$ が成り立つ。

*(3)* 作用が自由であるための必要十分条件は次が成り立つことである：

$$\mathrm{stab}\, x = \{e\} \quad (\forall x \in X)$$

*(4)* 作用が効果的であるための必要十分条件は次が成り立つことである：

$$\ker \lambda = e.$$

# 14　随伴作用、共役な元、類等式

**定義 14.1.** 群 $G$ を考える。

*(1)* 要素 $g \in G$ から随伴写像 $\mathrm{ad}_g : G \to G$ を以下で定めると、これは群同型写像である：

$$\mathrm{ad}_g(x) := gxg^{-1} \quad (\forall x \in G).$$

写像 $\mathrm{ad}_g$ を内部自己群同型写像とよぶこともある。

*(2)* 各要素 $g \in G$ にたいして自己群同型写像 $\mathrm{ad}_g \in \mathrm{Aut}_{\mathrm{Gp}}(G)$ が定義された。これは、つまり、写像

$$\mathrm{ad} : G \to \mathrm{Aut}_{\mathrm{gp}}(G), \quad g \mapsto \mathrm{ad}_g$$

が定義されるということである。

*(3)* これによって定まる作用 $\mathrm{ad} : G \curvearrowright G$ を随伴作用とよぶ。

*(4)* 要素 $x \in G$ の随伴作用による軌道を $C(x)$ とあらわし、共役類とよぶ：

$$C(x) := \{gxg^{-1} \mid g \in G\}.$$

*(5)* 二つの要素 $x, y \in G$ が共役とは、ある $g \in G$ が存在して

$$gxg^{-1} = y$$

を満たすことをいう。

もちろん、これは随伴作用による軌道が一致する、つまり、等式 $C(x) = C(y)$ が成り立つ、ということと同値。

*(6)* 要素 $x \in G$ と可換な要素 $g \in G$ の集合を $Z_G(x)$ とあらわす：

$$Z_G(x) := \{g \in G \mid gx = xg\}$$

**補題 14.2.** 随伴作用 $\mathrm{ad} : G \curvearrowright G$ を考える。

*(1)* $\ker \mathrm{ad} = Z(G)$

*(2)* $x \in X$ にたいして次がなりたつ：

$$\mathrm{stab}\, x = Z_G(x).$$

*(3)* $x \in X$ にたいして定まる次の写像は *well-defined* であり全単射である：

$$G/Z_G(x) \xrightarrow{1:1} C(x), \quad [g] \mapsto gxg^{-1}$$

*(4)* 要素 $x \in G$ にたいして次は同値：

*(a)* $x$ は中心 $Z(G)$ に属する。

*(b)* $\#C(x) = 1$.

*(c)* $Z_G(x) = G$.

**定理 14.3.** 有限群 $G$ にたいして次が成り立つ：

*(1)* 任意の要素 $x \in G$ にたいして次がなりたつ：

$$\#C(x) \times \#Z_G(x) = \#G$$

*(2)* $R$ を共役類の完全代表系とする。

$$\#G = \sum_{x \in R} \#C(x)$$

この等式を類等式とよぶ。

**補題 14.4.** 類等式にたいして次がなりたつ：

*(1)* 右辺の和の各項は $G$ の位数 $\#G$ の約数である。

*(2)* 右辺の和の項には少なくとも一つは 1 が現れる。

*(3)* 右辺の和に現れる 1 の個数は群 $G$ の位数 $\#G$ の約数である。

*Proof.* (1) 上の定理 14.3(1) より従う。

(2) $\#C(e) = 1$.

(3) $\#C(x) = 1 \Leftrightarrow x \in Z(G)$ だったので、右辺の和に現れる 1 の個数は中心 $Z(G)$ の位数である。 □

## 14.1 応用

**定義 14.5.** $p$ を素数とする。位数が $p$ のべきである非自明な有限群を $p$ 群とよぶ。

**補題 14.6.** $p$ 群 $G$ は非自明な中心をもつ。
つまり、$\#Z(G) \geq 1$.

*Proof.* 群 $G$ の位数を $p^n$ とする。
類等式の性質

$$\#G = \sum \#C(x),\ \#C(e) = 1,\ \#C(x) | p^n$$

から、要素 $x \in G \setminus \{e\}$ で $\#C(x) = 1$ を満たすものが存在しなければいけないことがわかる。

□

位数が素数 $p$ の有限群は巡回群で、特に可換群でした。位数が $p^2$ の群も可換と示すことができます。

**命題 14.7.** $p$ を素数とする。位数が $p^2$ の群 $G$ は可換である。

*Proof.* 背理法を用いる。
中心が全体に一致しない、つまり、$Z(G) \neq G$ と仮定する。すると、補題より $\#Z(G) = p$ である。

要素 $x \in G \setminus Z(G)$ をとってくる。
すると、$Z(G) \subset Z_G(x)$ であり $x \in Z_G(x)$ である。
よって、$Z_G(x) \supsetneq Z(G)$ である。とくに、不等式 $\#Z_G(x) > p$ が成り立つ。一方、次が成り立つ：

$$\#Z_G(x) | \#G = p^2$$

ゆえに $Z_G(x) = G$ でなければならない。
しかし、この等号は $x \in Z(G)$ を意味するので矛盾。 □

# 15　共役な部分群と正規化部分群

部分群 $H$ と要素 $g \in G$ にたいして定まる部分集合 $gHg^{-1}$ は $G$ の部分群です。

**定義 15.1.** 群 $G$ の部分群 $H, K$ が共役とは、ある要素 $g \in G$ が存在して

$$K = gHg^{-1}$$

がなりたつことをいう。

**定義 15.2.** 群 $G$ を考える。部分群 $H$ の正規化部分群 $N_G(H)$ を以下で定める：

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}.$$

**命題 15.3.** 群 $G$ を考える。部分群 $H$ と共役な部分群のなすべき集合 $\mathcal{P}(G)$ の部分集合を $\mathcal{C}$ とおく。すると、対応

$$\phi : G/N_G(H) \to \mathcal{C}, \quad [g] \mapsto gHg^{-1}$$

は写像であり、全単射である。

**系 15.4.** 有限群 $G$ を考える。部分群 $H$ と共役な部分群の個数は以下で与えられる：

$$\#G/\#N_G(H).$$

## 15.1　命題 15.3 の証明

### 15.1.1　予備的な考察

群 $G$ の集合 $X$ への作用 $\lambda : G \curvearrowright X$ を考えましょう。この作用からべき集合 $\mathcal{P}(X)$ への作用が誘導されます：

それは作用 $\lambda^{\mathcal{P}} : G \curvearrowright \mathcal{P}(X)$ を

$$g \cdot U := \lambda_g(U) = \{g \cdot_\lambda u \mid u \in U\} \quad (\forall U \in \mathcal{P}(X))$$

と定めればいいのです。

作用 $U \mapsto g \cdot_{\lambda^{\mathcal{P}}} U$ は $U$ の要素の個数を保ちますね：

$$\#(g \cdot_{\lambda^{\mathcal{P}}} U) = \#U.$$

自然数 $m \geq 0$ にたいして、$X$ の部分集合 $U$ で要素の個数が $m$ なものの構成する $\mathcal{P}(X)$ の部分集合を $\mathcal{P}(X)_m$ とおきましょう：

$$\mathcal{P}(X)_m := \{U \in \mathcal{P}(X) \mid \#U = m\}.$$

うえのことから、写像 $\lambda^{\mathcal{P}}_g$ による $\mathcal{P}(X)_m$ の像は $\mathcal{P}(X)_m$ に一致します。

べき集合への作用 $\lambda^{\mathcal{P}} : G \curvearrowright \mathcal{P}(X)$ はこの部分集合 $\mathcal{P}(X)_m$ に制限できます。この制限された作用も $\lambda^{\mathcal{P}}$ であらわすことにします：

$$\lambda^{\mathcal{P}} : G \curvearrowright \mathcal{P}(X)_m.$$

### 15.1.2　証明

随伴作用 $\mathrm{ad} : G \curvearrowright G$ にたいして上の考察を適用すると、作用 $\mathrm{ad}^{\mathcal{P}} : G \curvearrowright \mathcal{P}(G)$ が得られます。

この作用による $H \in \mathcal{P}(G)$ の安定化部分群 $\mathrm{stab}\, H$ は正規化部分群 $N_G(H)$ と一致します：

$$\mathrm{stab}\, H = N_G(H).$$

また、軌道 $G \cdot_{\mathrm{ad}^{\mathcal{P}}} H$ は $H$ と共役な部分群の集合 $\mathcal{C}$ と一致します：

$$G \cdot_{\mathrm{ad}^{\mathcal{P}}} H = \{gHg^{-1} \mid g \in G\} = \mathcal{C}.$$

よって、命題 15.3 は軌道と安定化部分群の一般的な関係の特別な場合とわかりました：

$$G/\,\mathrm{stab}\, H \xrightarrow{\sim} G \cdot_{\mathrm{ad}^{\mathcal{P}}} H, \quad [g] \to g \cdot_{\mathrm{ad}^{\mathcal{P}}} H.$$

## 15.2　ついでに、

### 15.2.1　予備的な考察

群 $G$ の集合 $X$ への作用 $\lambda : G \curvearrowright X$ を考えましょう。

要素 $U \in \mathcal{P}(X)$ の安定化部分群 $\mathrm{stab}_{\lambda^{\mathcal{P}}}(U)$ を $H$ とおきましょう：

$$H := \mathrm{stab}_{\lambda^{\mathcal{P}}}(U) = \{g \in G \mid g \cdot U = U\}.$$

最右辺の記述から $h \in H$ にたいして定まる写像 $\lambda_h : X \to X$ は $U$ を保ちます。制限写像 $\lambda_h|_U : U \to U$ が得られ、これは全単射です。

これによって作用 $H \curvearrowright U$ が定まりました。

### 15.2.2　応用

ここでは、正則作用 $\lambda : G \curvearrowright G$ から誘導される作用 $\lambda^{\mathcal{P}} : G \curvearrowright \mathcal{P}(G)$ を考えます。

**補題 15.5.** $G$ を有限群とする。要素 $S \in \mathcal{P}(G)$ にたいして次が成り立つ：

$$\#\,\mathrm{stab}_{\lambda^{\mathcal{P}}} S | \#S.$$

*Proof.* 安定化部分群を $H := \mathrm{stab}_{\lambda^{\mathcal{P}}} S$ とおきましょう。証明の鍵は $H$ が集合 $S$ に作用するということです。

正則作用 $\lambda : G \curvearrowright G$ は自由だったので、誘導される作用 $H \curvearrowright S$ も自由です。よって、任意の軌道 $Hs$ の要素の個数は $H$ の要素の個数と一致します：$\#(Hs) = \#H$.

軌道分解 $S = \sqcup_{s \in R} Hs$ より主張が得られます。　□

# 16　シロー（Sylow）の定理

この節では $G$ は有限群を表す。

## 16.1　シローの定理

### 16.1.1　$p$ シロー部分群

**定義 16.1.** $p$ を素数とする。有限群 $G$ の位数は

$$\#G = n = p^a m \quad (m \text{ は } p \text{ と互いに素})$$

とあらわせるとする。

位数が $p^a$ である部分群 $H$ を $G$ の $p$ シロー部分群とよぶ。

$$\#H = p^a.$$

定義しただけでは $p$ シロー部分群が存在するかさえ定かではありません。シローの定理はその存在を保証するのみならず、それらがすべて互いに共役であることを等を主張します。

### 16.1.2　シローの定理

**定理 16.2.** $p$ を素数、$G$ を有限群とする。
次が成り立つ：

*(1)* $G$ は $p$ シロー部分群をもつ。

以下では $H$ は $p$ シロー部分群をあらわす。

*(2)* $G$ の部分群 $K < G$ で $p$ 群である（つまり、$\#K = p^b$ がなりたつ）ものは $H$ の部分群と共役である。

別の言い方をすると、ある $g \in G$ が存在して

$$gKg^{-1} \subset H$$

を満たす。

*(3)* 任意の $p$ シロー部分群は互いに共役である。

*(4)* $p$ シロー部分群の個数を $p$ で割ったときの余りは 1 である：($p$ シロー部分群 $H$ と共役な部分群の個数は $p$ で割ったときの余りが 1 である)

$$\#G/\#N_G(H) \equiv 1 \pmod{p}$$

### 16.1.3　証明

ボチボチ証明をしてきましょう。
有限群 $G$ の位数は

$$\#G = n = p^a m \quad (m \text{ は } p \text{ と互いに素})$$

とあらわせるとする。
要素の個数が $p^a$ である $G$ の部分集合 $S$ が構成する $\mathcal{P}(G)$ の部分集合を $X = \mathcal{P}(G)_{p^a}$ とおきます：

$$X := \mathcal{P}(G)_{p^a} = \{S \in \mathcal{P}(G) \mid \#S = p^a\}.$$

**補題 16.3.** $\#X$ は $p$ と互いに素である。

*Proof.* $X$ の要素の個数は

$$\#X = \binom{n}{p^a} = \prod_{k=0}^{p^a-1} \frac{n-k}{p^a-k}$$

ですね。

この積の各因子を調べます。$k$ $(0 \leq k \leq p^a - 1)$ を $k = p^b l$ ただし $l$ は $p$ と互いに素、とあらわします。すると、対応する因子は

$$\frac{n-k}{p^a-k} = \frac{p^{a-b}m - l}{p^{a-b} - l},$$

となります。ポイントは分子 $p^{a-b}m - l$ が $p$ と互いに素である、ということです。

問題の $\#X$ は分子 $\prod p^{a-b}m - l$ の約数なので、特に、$p$ と互いに素である。 □

シローの定理の証明. (1) 左正則作用 $\lambda : G \curvearrowright G$ の誘導する作用 $\lambda^{\mathcal{P}} : G \curvearrowright X$ を考えます。完全代表系 $R$ を選んで軌道分解から得られる等式を見ます：

$$\#X = \sum_{S \in R} \#(G \cdot_{\lambda^{\mathcal{P}}} S).$$

補題 16.3 から $\#(G \cdot_{\lambda^{\mathcal{P}}} S)$ が $p$ と互いに素である $S \in X$ が存在します。

状況をまとめると、次のようになります：

$$\#(G \cdot_{\lambda^{\mathcal{P}}} S) \times \# \operatorname{stab} S = \#G = p^a m$$
$$\# \operatorname{stab} S | \#S = p^a$$

これらのことをまとめると $S$ の作用 $\lambda^{\mathcal{P}}$ による安定化部分群 $H := \operatorname{stab} S$ が $p$ シロー部分群であると結論できます。

(2) $p$ 部分群 $K$ の $G$ への左正則作用を考えます。この作用は商集合 $Y = G/H$ への作用を誘導します：

$$\lambda^K : K \curvearrowright Y, \quad k \cdot_{\lambda^Y} [g] := [kg].$$

$Y$ の要素の個数 $\#Y = m$ は $p$ と互いに素なので、(1) の冒頭と同様に軌道分解を考えることで、軌道の要素の個数 $\#(K \cdot_{\lambda^Y} [g])$ が $p$ と互いに素なものが存在するとわかります。

一方、軌道の要素の個数は作用する群の要素の個数 $\#K$ の約数でした。なので、 $\#(K \cdot_{\lambda^Y} [g]) = 1$ でなければいけません。

このことから、任意の $k \in K$ にたいして $kg \in gH$ が成り立つとわかります。つまり、$K \subset gHg^{-1}$ がわかります。

(3) は (2) の帰結です。

(4) $p$ シロー部分群の集合を $Z$ とおきます：

$$Z = \{H_1 = H, H_2, \cdots, H_s\}.$$

$H$ は $Z$ に随伴作用で作用しますね：

$$\mathrm{ad}^Z : H \curvearrowright Z, \quad h \cdot_{\mathrm{ad}^Z} H_i := hH_ih^{-1}.$$

等式 $\#(H \cdot_{\mathrm{ad}^Z} H) = 1$ は明らかですね。

**主張 16.4.** $\#(H \cdot_{\mathrm{ad}^Z} H_i) \neq 1$ *for all* $i \geq 2$.

*Proof.* 背理法を用います。

ある $i \geq 2$ にたいして $\#(H \cdot_{\mathrm{ad}^Z} H_i) = 1$ が成り立ったとします。これは $hH_ih^{-1} = H_i$ が任意の $h \in H$ にたいして成り立つということです。なので、$H < N_G(H_i)$ が成り立ちます。.

ポイントは $H$ と $H_i$ は $N_G(H_i)$ の $p$ シロー部分群であるということです。このことから、(3) により、ある $g \in N_G(H_i)$ が存在して $gH_ig^{-1} = H$ を満たすといことがわかります。

しかし、正規化部分群の定義より最後の等式は $H_i = H$ を意味するので、矛盾です。 □

この主張から、任意の $i \geq 2$ にたいして軌道の要素の個数 $\#(H \cdot_{\mathrm{ad}^Z} H_i)$ は 1 ではない $\#H = p^a$ の約数とわかります。作用 $\mathrm{ad}^Z : H \curvearrowright Z$ による $Z$ の軌道分解を考えることで $\#Z \equiv 1 (\mathrm{mod}\, p)$ が得られます。 □

## 16.2 例

### 16.2.1 有限巡回群の場合

位数が $n$ の有限巡回群 $\mathbb{Z}/n\mathbb{Z}$ を考えましょう。$n$ を素因数分解します：

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}.$$

すると、次の同型が存在します：

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{a_1} \times \mathbb{Z}/p_2^{a_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{a_r}\mathbb{Z}.$$

$\mathbb{Z}/n\mathbb{Z}$ の素数 $p_s$ に対応する $p_s$ シロー部分群は、上の同型の右辺でみると $s$ 番目の因子で与えられるものです。

巡回群は可換群なので任意の部分群は正規であり、特にシロー部分群は一意に定まります。

### 16.2.2 可換有限群の場合

有限アーベル群の構造定理により、巡回群の場合に帰着できますね。

### 16.2.3 3 次対称群 $S_3$

位数は $\#S_3 = 6 = 2 \times 3$ ですね。

- 2 シロー部分群を見つけましょう。

  位数 2 の群は巡回群なので、それを見つけるというのは位数 2 の要素を見つけることとほぼ同じですね。

  なので 2 シロー部分群は次のものです：

  $$\{e, (1,2)\},\ \{e, (2,3)\},\ \{e, (3,1)\}$$

- 3 シロー部分群を見つけましょう。

  位数 3 の群は巡回群なので、それを見つけるというのは位数 3 の要素を見つけることとほぼ同じですね。

  なので 3 シロー部分群は次のものです：

  $$\{e, (1,2,3), (1,3,2)\}.$$

  位数が 3 の $S_3$ の部分群の指数は $2 = 6/3$ なので、とくに正規です。よって、3 シロー部分群は一つしかありません。

### 16.2.4　4 次交代群 $A_4$

位数は $\#A_4 = 12 = 2^2 \times 3$ ですね。

- 3 シロー部分群を見つけましょう。

  位数 3 の群は巡回群なので、それを見つけるというのは位数 3 の要素を見つけることとほぼ同じですね。

  なので 3 シロー部分群は次のものです：

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

- 2 シロー部分群を見つけましょう。

  位数は $4 = 2^2$ ですね。

  具体例は既に講義に現れています。つぎの様な部分群を扱いました：

$$K := \{e,\ (1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3)\}.$$

  これは位数が 4 の $A_4$ の部分群なので 2 シロー部分群です。

  巡回置換の基本的な性質からこの部分群は $S_4$ の部分群として正規であると確認できます。なので、特に $A_4$ の部分群としても正規です。ゆえに、$A_4$ の 2 シロー部分群は $K$ のみとわかりました。

### 16.2.5　4 次対称群 $S_4$

位数は $\#S_4 = 24 = 2^3 \times 3$ ですね。

- 3 シロー部分群を見つけましょう。

  位数 3 の群は巡回群なので、それを見つけるというのは位数 3 の要素を見つけることとほぼ同じですね。

  なので 3 シロー部分群は次のものです：

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

- 2 シロー部分群を見つけましょう。

  位数は $8 = 2^3$ なので、直接求めるのは、なかなか、大変です。

  なので、上の部分群 $K$ を考えます：

$$K := \{e,\ (1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3)\}.$$

  巡回置換の基本的な性質からこの部分群は $S_4$ の部分群として正規であると確認できます。

  この部分群 $K$ の位数は 4 なのでシローの定理より、2 シロー部分群の部分群に共役です。しかし、正規（$gKg^{-1} = K$）なので、$K$ は任意の 2 シロー部分群に含まれるとわかりました。

  **主張 16.5.** 商群 $S_4/K$ は $S_3$ と同型である。さらには、同型写像 $f : S_4/K \to S_3$ で $(1,2), (2,3), (1,3) \in S_4$ の剰余類を $(1,2), (2,3), (1,3) \in S_3$ に移すものが存在する。

*Proof.* 3次対称群 $S_3$ は自然に $S_4$ の部分群とおもえるのでした。(集合 $\{1,2,3\}$ の自己全単射を文字4を動かさない集合 $\{1,2,3,4\}$ の自己全単射をとみなすのでした。) そう思ったときに $S_3 \cap K = \{e\}$ なので、合成写像

$$S_3 \to S_4 \xrightarrow{\pi} S_4/K$$

は単射です。さらに、位数を計算すると $\#S_4/K = (\#S_4)/(\#K) = 24/4 = 6$ なので、この写像は全射とわかり、主張が示せます。

□

$K$ を含む部分群 $H$ と $S_4/K$ の部分群 $L$ は一対一に対応するのでした。対応を復習すると

$$L \mapsto \pi^{-1}(L)$$

でした。また $\#L = \#\pi^{-1}(L)/\#K$ なので、

$$\#\pi^{-1}(L) = \#K \times \#L$$

が成り立ちます。

なので $S_4$ の 2 シロー部分群を求める問題は、$S_3$ の位数 2 の部分群を求める問題に帰着されます。そして、それは上で解決していました。

それを用いると、$S_4$ の 2 シロー部分群は以下の三つとわかります：

$$\langle K, (1,2)\rangle,\ \langle K, (2,3)\rangle,\ \langle K, (1,3)\rangle.$$

# 17　半直積群

## 17.1　半直積群の定義と基本性質

二つの群 $G, H$ から直積群 $G \times H$ を構成することができました。これ以外にも、二つの群から新たな群を構成する方法があります。

**定義 17.1.** $G, H$ を群、$\phi : G \to \mathrm{Aut}_{\mathrm{Gp}} H$ を群準同型写像とする。
この状況で、半直積群 $H \rtimes G = H \rtimes_\phi G$ を以下で定義する：

- 下部集合は直積集合 $H \times G$.
- 積は以下で定義する：

(17-9)　　$(h_1, g_1)(h_2, g_2) := (h_1 \phi_{g_1}(h_2), g_1 g_2) \quad (\forall h_1, h_2 \in H, \quad g_1, g_2 \in G).$

**練習問題 17.2.**（レポート問題　1月２６日講義開始時提出　$A4$ 片面、左上ホッチキス、表紙不要）
以下を確認し、上の定義により群 $H \rtimes G$ が定義されることを確かめよう。

*(1)* 積 (17-9) は結合法則をみたす。

*(2)* 積 (17-9) の単位元は $(e_H, e_G)$ である。

*(3)* 積 (17-9) に関する要素 $(h, g) \in H \times G$ の逆元は次で与えられる：

$$(h, g)^{-1} = (\phi_{g^{-1}}(h^{-1}), g^{-1}).$$

*(4)* 写像

$$j : G \to H \rtimes_\phi G, \ g \mapsto (e_H, g)$$

は単射群準同型写像である。

*(5)* 写像

$$i : H \to H \rtimes_\phi G, \ h \mapsto (h, e_G)$$

は単射群準同型写像である。

さらに、像 $\mathrm{Im}\, i$ は $H \rtimes_\phi G$ の正規部分群である。

- $i, j$ の像と定義域を同一視することで $H, G$ の下部集合を $H \rtimes_\phi G$ の下部集合の部分集合とみなします：

$$G = \{(e_H, g) \mid g \in G\}, \quad H = \{(h, e_G) \mid h \in H\}.$$

上の問題から、この同一視の下で、$G$ は $H \rtimes_\phi G$ の部分群であり、$H$ は $H \rtimes_\phi G$ の正規部分群であるとわかります。

以下、この同一視を継続します。

*(6)* 次の等式が成り立ちます：

$$(e, g)(h, e)(e, g)^{-1} = (\phi_g(h), e).$$

上の同一視のもとでは、この等式は次の様になります：

$$ghg^{-1} = \phi_g(h).$$

つまり、半直積群 $H \rtimes_\phi G$ の中での部分群 $G$ の正規部分群 $H$ への随伴作用として、最初に選んできている群準同型写像 $\phi : G \to \mathrm{Aut}_{\mathrm{Gp}}(H)$ が得られるのです。

*(7)*

$$HG = H \rtimes_\phi G, \quad H \cap G = \{e\}.$$

*(8)* $\phi$ が自明な群準同型写像なら $H \rtimes_\phi G = H \times G$.

### 17.1.1 基本的な性質

さて、直積集合 $H \times G$ から $H, G$ に成分を落とすことができ射影と呼ばれました。次は、射影を調べましょう：

**補題 17.3.** *(1)* 写像

$$q : H \rtimes_\phi G \to G, \quad (h, g) \mapsto g$$

は全射群準同型写像である。

*(2)* $\operatorname{Ker} q = H$.

*(3)* 群準同型写像 $q : H \rtimes_\phi G \to G$ は群同型写像

$$\overline{q} : (H \rtimes_\phi G)/H \xrightarrow{\cong} G$$

を誘導する。

*(4)* $q \circ j = \mathrm{id}_G$.

*(5)* （注意：一般には、写像

$$p : H \rtimes_\phi G \to H, \quad (h, g) \mapsto h$$

は群準同型写像ではない。特殊な設定では群準同型写像になることもある。）

**練習問題 17.4.** $\phi : G \to \mathrm{Aut}_{gp} H$ が自明な場合は $H \rtimes_\phi G$ は直積群である。

## 17.2 例：アフィン変換のなす群

自然な作用 $\nu : \mathrm{GL}_n(\mathbb{R}) \curvearrowright \mathbb{R}^n$ に対応する群準同型写像は $\mathbb{R}^n$ の群自己同型のなす群に値をもつので、群準同型写像

$$\nu : \mathrm{GL}_n(\mathbb{R}) \to \mathrm{Aut}_{\mathrm{Gp}}(\mathbb{R}^n)$$

をえる。

この群準同型写像による半直積群 $\mathbb{R}^n \rtimes_{nu} \mathrm{GL}_n(\mathbb{R})$ を $\mathbb{R}^n$ のアフィン変換群と呼び $\mathrm{Aff}(n; \mathbb{R})$ とかあらわす：

$$\mathrm{Aff}(n; \mathbb{R}) := \mathbb{R}^n \rtimes_\nu \mathrm{GL}_n(\mathbb{R}).$$

要素 $(v, A) \in \mathrm{Aff}(n; \mathbb{R})$ は $\mathbb{R}^n$ に次のように作用します：

$$(v, A) \cdot x := Ax + v \quad (\forall x \in \mathbb{R}^n).$$

正則行列 $A$ による線形変換のあとでベクトル $v$ に拠る平行移動をしています。

この様な変換のことをアフィン変換と呼びます。

より一般にアフィン写像という概念があり、線形写像と平行移動の合成のことを指します。

## 17.3 半直積群であると明らかにする方法

群 $K$ が半直積群 $H \rtimes_\phi G$ であると判断する方法があります。

**命題 17.5.** $G, H$ を群とする。

群 $K$ にたいして次は同値：

*(1)* ある群準同型写像 $\phi : G \to \mathrm{Aut}_{\mathrm{Gp}}(H)$ が存在して $K$ は半直積群 $H \rtimes_\phi G$ と同型である：

$$K \cong H \rtimes_\phi G.$$

*(2)* 群準同型写像

$$j : G \to K,\ q : K \to G$$

が存在して、次を満たす：

*(a)* $q \circ j = \mathrm{id}_G$.

*(b)* $\mathrm{Ker}\, q \cong H$.

*(3)* $K$ は $G$ と同型な部分群 $G'$ と $H$ と同型な正規部分群 $H'$ を持ち、これらは次を満たす：

*(a)* $H'G' = K$.

*(b)* $H' \cap G' = \{e\}$.

*Proof.* (1) ⇒ (2) は既に示した。

(2) ⇒ (3). $G' = \mathrm{Im}\, j,\ H' := \mathrm{Ker}\, q$ と置けばよい。

(3) ⇒ (1) $H'$ は $K$ の正規部分群なので、随伴作用を定める群準同型写像 $\mathrm{ad} : K \to \mathrm{Aut}_{\mathrm{Gp}}(H')$ があるが、定義域を $G'$ に制限することで群準同型写像 $\phi' : G' \to \mathrm{Aut}_{\mathrm{Gp}}(H')$ が得られる。つまり、

$$\phi'_g(h) := ghg^{-1}$$

写像

$$f : H' \rtimes_{\phi'} G' \to K,\quad (h, g) \mapsto hg$$

と定義する。

**主張 17.6.** この写像 $f$ は群同型写像である。

*Proof.* $f$ が群準同型写像であること：
$x_1 = (h_1, g_1),\ x_2 = (h_2, g_2) \in H' \rtimes_{\phi'} G'$ をとってくる。
（$f(x_1x_2) = f(x_1)f(x_2)$ を示す。）
まず、

$$x_1x_2 = (h_1, g_1)(h_2, g_2) = (h_1\phi_{g_1}(h_2),\ g_1g_2) = (h_1g_1h_2g_1^{-1},\ g_1g_2).$$

なので、

$$f(x_1x_2) = (h_1g_1h_2g_1^{-1})(g_1g_2) = h_1g_1h_2g_2 = f(x_1)f(x_2).$$

$f$ が全射であること。
$f$ の定義より $\mathrm{Im}\, f = H'G'$ である。仮定より、$\mathrm{Im}\, f = K$ となり、$f$ は全射である。

$f$ が単射であること。
$\mathrm{Ker}\, f = \{e\}$ を示す。
$x = (h, g) \in \mathrm{Ker}\, f$ をとってくる。$f$ の定義より $hg = e$ が成り立つ。この等式に、右から $g^{-1}$ を掛けて等式 $g^{-1} = h$ が得られる。
よって、$h \in H' \cap G'$ とわかり、仮定より $h = e$ である。さらに、上の等式より $g = e$ を得る。
（半直積群の単位元は $(e_{H'}, e_{G'})$ だったので）これで $x = e$ がわかった。

□

あとは、同型 $G \cong G',\ H \cong H'$ を使って半直積群 $H' \rtimes_{\phi'} G'$ と $H \rtimes_\phi G$ の同型を構成すればよい。

□

## 17.4 例

### 17.4.1 対称群

例 **17.7.** 2 次巡回群 $C_2 = \langle g \rangle$ を $\{\pm 1\}$ と同一視する。すると群準同型 $\operatorname{sgn} : S_n \to C_2$ が得られる。
核が交代群なのであった $\ker \operatorname{sgn} = A_n$.
一方、$s_1$ の位数は 2 なので群準同型 $\rho : C_2 \to S_n,\ \rho(g) := s_1$ が存在する。
等式 $\operatorname{sgn} \circ \rho = \mathrm{id}_{C_2}$ がなりたつ。
よって、$S_n \cong A_n \rtimes C_2$ である。

**注意 17.8.** この同型は位数 2 の要素の選び方に依存している。

### 17.4.2 二面体群

二面体群の導入の仕方はいろいろありますが、ここでは巡回群から半直積により構成します。

例 **17.9.** 自然数 $n \geq 2$ を選ぶ。
$n$ 次巡回群 $\mathbb{Z}/n\mathbb{Z}$ の自己群同型写像

$$\sigma : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad \sigma([a]_{\mathbb{Z}/n\mathbb{Z}}) = [-a]_{\mathbb{Z}/n\mathbb{Z}}$$

を考える。
これは

$$\sigma \circ \sigma = \mathrm{id}_{\mathbb{Z}/n\mathbb{Z}}$$

を満たす。
$n = 2$ の場合、$\sigma = \mathrm{id}$ である。$n \geq 3$ の場合は $\sigma \neq \mathrm{id}$ である。
つまり、自己群同型群 $\mathrm{Aut}_{\mathrm{Gp}}(\mathbb{Z}/n\mathbb{Z})$ の要素として $\sigma$ の位数は次のようになる：

$$\mathrm{ord}_{\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})}\, \sigma = \begin{cases} 1 & (n = 2) \\ 2 & (n \geq 3) \end{cases}.$$

この観察から、群準同型写像

$$\phi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}_{gp}(\mathbb{Z}/n\mathbb{Z}), \quad 1 \to \sigma$$

が得られる。
半直積群 $\mathbb{Z}/n\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z}$ のことを $n$ 次二面体群とよび $D_n$ とあらわす：

$$D_n = \mathbb{Z}/n\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z}.$$

二つの要素

$$r := ([1]_{\mathbb{Z}/n\mathbb{Z}}, 0), \quad s := (0, [1]_{\mathbb{Z}/2\mathbb{Z}}) \in D_n$$

が $D_n$ の生成元である。これらは関係式

$$r^n = e_{D_n},\ s^2 = e_{D_n},\ srs^{-1} = r^{-1}$$

を満たす。
最後の式の導出：

$$srs^{-1} = (\sigma([1]_{\mathbb{Z}/n\mathbb{Z}}), 0) = ([-1]_{\mathbb{Z}/n\mathbb{Z}}, 0) = r^{-1}.$$

二面体群を平面の変換群として実現することが出来ます。そして、その方が普通の定義です。

**練習問題 17.10.** 実数 $\theta$ にたいして行列 $R(\theta), S(\theta)$ を次で定める：

$$R(\theta) := \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, S(\theta) := \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}.$$

自然数 $n \geq 1$ にたいして以下で $\mathrm{GL}(2;\mathbb{R})$ の部分集合 $C'_n, D'_n$ を定義する。

$$C'_n := \left\{ R\left(\frac{2k\pi}{n}\right) \middle| \ k \in \mathbb{Z} \right\}.$$
$$D'_n := \left\{ R\left(\frac{2k\pi}{n}\right), S\left(\frac{2k\pi}{n}\right) \middle| \ k \in \mathbb{Z} \right\}.$$

*(i)* $C'_n$ は $n$ 次巡回群であることを示せ。

*(ii)* $D'_n$ は $n$ 次二面体群と同型であることを示せ。

**練習問題 17.11.** 3 次二面体群は 3 次対称群と同型である：

$$D_3 \cong S_3.$$

# 18　位数 6 の群の分類

**命題 18.1.** 位数 6 の群 $G$ は次のいずれかに同型である：

$$\mathbb{Z}/6\mathbb{Z}, \quad S_3.$$

*Proof.* $H$ を $G$ の 2 シロー部分群、$K$ を $G$ の 3 シロー部分群とする。

次のことは簡単に分かる：

$$H \cap K = \{e\}, \ KH = G.$$

**主張 18.2.** $K$ は正規部分群である。

よって、$G$ はある群準同型写像 $\phi : H \to \mathrm{Aut}_{\mathrm{Gp}}(K)$ による半直積群 $K \rtimes_\phi H$ に同型である。

$$G \cong K \rtimes_\phi H.$$

*Proof.* （$K$ の指数 $[G : K] = 2$ から従うことですが、ここでは別の証明を与えます。）

正規性をいう方法の一つは正規化部分群 $N_G(K)$ が全体に一致することを示すことでした。包含関係 $K < N_G(K) < G$ から、

$$3 = \#K \mid \#N_G(K) \mid \#G = 6$$

が従います。なので、$\#N_G(K) = 3$ or 6 です。一方、シローの定理より、3 シロー部分群の個数は 3 で割ると 1 余るのでした：

$$\#G/\#N_G(K) \equiv 1 \pmod 3.$$

これが成り立つためには $\#N_G(K) = 6$ でなければいけません。

よって、$N_G(K) = G$ が示せて、主張の証明が完了しました。 □

$K$ は位数 3 の群なので巡回群です。同型 $K \cong \mathbb{Z}/3\mathbb{Z}$ を通じて

$$\mathrm{Aut}_{\mathrm{Gp}}(K) = \{e, \sigma\}$$

がわかります。ここで $\sigma$ は $[a]_{\mathbb{Z}/3\mathbb{Z}} \mapsto [-a]_{\mathbb{Z}/3\mathbb{Z}}$ に対応する $K$ の群自己同型としています。

（自己同型群 $\mathrm{Aut}_{\mathrm{Gp}}(K)$ は 2 次の巡回群なのです。）

$H$ は位数 2 の群なので、2 次の巡回群です。生成系を $h$ としましょう。

$$H = \{e, h\}.$$

半直積群 $K \rtimes_\phi H$ を分類するには群準同型写像 $\phi : H \to \mathrm{Aut}_{\mathrm{Gp}}(K)$ を分類すればいいのですが、今の場合は、値域定義域ともに 2 次の巡回群なので話はとても簡単です：

つまり、群準同型写像

$$\phi : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$$

をすべて見つけましょう、ということになります。これは生成元 $[1]_{\mathbb{Z}/2\mathbb{Z}}$ の像 $\phi([1]_{\mathbb{Z}/2\mathbb{Z}})$ ですべて決まってしまいます。結果をいうと二つしかありません。

それを元の問題にもどすと、次をえます：

$$\mathrm{Hom}_{\mathrm{Gp}}(H, \mathrm{Aut}_{\mathrm{Gp}}(K)) = \{\phi_0,\ \phi_1\}.$$

ただし、

(0) $\phi_0$ は自明な群準同型写像

(1) $\phi_1$ は $h$ を $\sigma$ に移す群準同型写像

それぞれに対応する半直積群 $K \rtimes_{\phi_i} H$ は

(0) 自明な群準同型に対応する半直積群は直積群だったので、

$$K \rtimes_{\phi_0} H \cong K \times H \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$$

である。

(1) これは $S_3$ の半直積群としての表示に現れたものと同型 $K \cong A_3,\ H \cong C_2$ で一致するので、群準同型 $\phi_1$ による半直積群 $K \rtimes_{\phi_1} H$ は 3 次対称群と同型である：

$$K \rtimes_{\phi_1} H \cong S_3.$$

□

# 19　単純群

## 19.1　単純群

**定義 19.1.** 非自明な正規部分群をもたない群を単純群とよぶ。

つまり、群 $G$ が単純とは正規部分群 $H \lhd G$ が $H = \{e\}$ または $H = G$ に限る群と定義する。

**命題 19.2.** 群 $G$ が単純であるための必要十分条件は次がなりたつことである：

群準同型写像 $f : G \to H$ は単射であるか、あるいは自明なものである。

さきに行った部分群の分類から次が容易に従います。

**命題 19.3.** 巡回群が単純であるための必要十分条件は位数が素数あるいは 1 であることである。

次は Galois 理論において重要な意味を持つ結果です。

**定理 19.4.** $n \geq 5$ にたいして $n$ 次交代群 $A_n$ は単純である。

**注意 19.5.** *(1)* $A_1 = \{e\}$ は単純群。

*(2)* $A_2 = \{e\}$ は単純群。

*(3)* $A_3$ は 3 次巡回群であり、よって特に単純群。

*(4)* $A_4$ は単純群ではない。

# 20　交換子、交換子部分群

**定義 20.1.** 群 $G$ の要素 $g, h \in G$ にたいして

$$[g, h] := ghg^{-1}h^{-1}$$

と定め、$g, h$ の交換子と呼ぶ。

次の補題は直接計算で容易に確かめられる。

**補題 20.2.** 群 $G$ の要素 $g, h, k \in G$ にたいして次がなりたつ：

*(1)* $k[g, h]k^{-1} = [kgk^{-1}, khk^{-1}]$.

*(2)* $[g, h]^{-1} = [h, g]$

*(3)* $[g, h] = e \quad \Leftrightarrow \quad gh = hg$.
（雰囲気：このことから $[g, h]$ は $g$ と $h$ が非可換な度合いを測ってるようにも見える。）

*(4)* 群準同型写像 $f : G \to H$ にたいして次がなりたつ：

$$f([g, h]) = [f(g), f(h)]$$

後半二つの主張から次が導かれますね。

**系 20.3.** 群準同型写像 $f : G \to A$ の値域 $A$ は可換群とする。このとき、任意の $g, h \in G$ にたいして

$$f([g, h]) = e$$

がなりたつ。

**定義 20.4.** $G$ を群とする。

*(1)* 部分群 $H, K < G$ にたいして部分群 $[H, K]$ を以下で定義する：

$$[H, K] := \langle \{[h, k] \mid h \in H, k \in K\} \rangle$$

*(2)* $[G, G]$ を $G$ の交換子部分群とよぶ。

**補題 20.5.** *(1)* 交換子部分群 $[G, G]$ は正規である。

*(2)* 商群 $G/[G, G]$ は可換群である。

*(3)* 群準同型写像 $f : G \to A$ で値域 $A$ が可換群であるものにたいしては $[G, G] \subset \mathrm{Ker}\, f$ がなりたつ。よって、群準同型写像 $\tilde{f} : G/[G, G] \to A$ が一意的に存在して $f = \tilde{f} \circ \pi$ を満たす。ただし、$\pi : G \to G/[G, G]$ は商写像を表す。

**練習問題 20.6.** 群 $G$ にたいして次が成り立つ：

*(1)* 可換群 $A$ にたいして商写像 $\pi : G \to G/[G, G]$ が誘導する写像

$$\mathrm{Hom}_{\mathrm{gp}}(G/[G, G], A) \to \mathrm{Hom}_{\mathrm{gp}}(G, A), \ f \mapsto f \circ \pi$$

は全単射である。

*(2)* 次が成り立つ：

$$[G, G] = \bigcap_{\phi : G \to A} \ker \phi$$

ただし、共通部分は任意の可換群 $A$ への任意の群準同型写像 $f : G \to A$ に渡ってとっている。

**定義 20.7.** $G$ を群とする。$n \geq 0$ にたいして帰納的に $D_n(G)$ を以下で定義し、これを第 $n$ 次交換子部分群とよぶ：

$$D_0(G) := G, \quad D_n(G) = [D_{n-1}(G), D_{n-1}(G)]$$

定義より、部分群の減少列ができている：

$$\cdots < D_{n+1}(G) < D_n(G) < \cdots < D_1(G) < D_0(G) = G.$$

これを $G$ の交換子列とよぶ。それぞれの部分群は先行するものの正規部分群であることに注意しておく：

$$D_{n+1}(G) \lhd D_n(G).$$

**定義 20.8.** 群 $G$ が可解とはある自然数 $n$ が存在して $D_n(G) = \{e\}$ を満たすことをいう。

**例 20.9.** 群 $G$ が可換であるための必要十分条件は $D_1(G) = \{e\}$ である。
よって、特に可換群は可解である。

**命題 20.10.** 群 $G$ にたいして次の命題は同値：

*(1)* $G$ は可解群。

*(2)* $G$ は次の条件をみたす部分群の有限な減少列をもつ：

$$\{e\} = G_n < G_{n-1} < \cdots < G_1 < G_0 = G$$

各 $G_i$ が $G_{i-1}$ の正規部分群であり商群 $G_{i-1}/G_i$ が可換群である。

*Proof.* (1) $\Rightarrow$ (2) は明らか。

(2) $\Rightarrow$ (1).
各 $i$ にたいして $G_{i-1}/G_i$ は可換群なので

$$[G_{i-1}, G_{i-1}] < G_i$$

が成り立つ。
とくに $G_0 = G$ なので $D_1(G) < G_1$ である。いか下で示すように帰納的に $D_i(G) < G_i$ をえる：

$$D_i(G) = [D_{i-1}(G).D_{i-1}(G)] < [G_{i-1}.G_{i-1}] < G_i$$

よって特に $D_n(G) < G_n = \{e\}$ であり、$D_n(G) = \{e\}$ を結論する。 □

### 20.0.1 例

**例 20.11.** $N \geq 2$ を 2 以上の自然数とします。$N$ 次二面体群 $D_N := \mathbb{Z}/N\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ は可換ではない可解群です。
復習しておくと積は

$$([m]_N, [a]_2)([n]_N, [b]_2) := ([m + (-1)^a n]_N, [a + b]_2)$$

と定義されているのでした。逆元は $([m]_N, [a]_2)^{-1} = ([(-1)^{-a+1}m]_N, [-a]_2) = ([(-1)^{a+1}m]_N, [a]_2)$ ですね。
可換子を計算しましょう。

$$\begin{aligned}
[([m]_N, [a]_2), ([n]_N, [b]_2)] &= ([m]_N, [a]_2)([n]_N, [b]_2)([m]_N, [a]_2)^{-1}([n]_N, [b]_2)^{-1} \\
&= ([m]_N, [a]_2)([n]_N, [b]_2)([(-1)^{a+1}m]_N, [a]_2)([(-1)^{b+1}n]_N, [b]_2) \\
&= ([m + (-1)^a n + (-1)^{b+1}m - n]_N, [0]_2) \\
&= ([(1 - (-1)^b)m + ((-1)^a - 1)n]_N, [0]_2).
\end{aligned}$$

この計算から可換子部分群 $D_1(D_N) = [D_N, D_N]$ は次のようになることが分かります：

$$D_1(D_N) = [D_N, D_N] = \begin{cases} \{([m]_N, [0]_2) \mid m \in \mathbb{Z}\} \cong \mathbb{Z}/N\mathbb{Z} & (N \text{ 奇数}) \\ \{([m]_N, [0]_2) \mid m \in 2\mathbb{Z}\} \cong \mathbb{Z}/(N/2)\mathbb{Z} & (N \text{ 偶数}) \end{cases}$$

$N$ の偶奇により表示式は異なりますが、どちらの場合でも巡回群、とくに可換群です。このことから、第二交換子群 $D_2(D_N)$ は単位群になることが分かります：

$$D_2(D_N) = \{e\}.$$

ゆえに $N$ 次二面体群は可解群と分かりました。

**例 20.12.** 自然数 $n$ と可換環 $R$ にたいして群 $G$ を上半三角行列のなす $\mathrm{GL}_n(R)$ の部分群として定める。

$$G := \{A = (a_{ij}) \in \mathrm{GL}_n(R) \mid a_{ij} = 0 \ (i > j)\}$$

$G$ は可換群ではないが可解ではある。

## 20.1 対称群の可解性

ガロア理論との関係で次の定理は重要です。5 次以上の代数方程式が冪根による解の公式をもたないという事実を証明する鍵なのです。

**定理 20.13.** $n$ 次対称群 $S_n$ が可解であるための必要十分条件は $n \leq 4$ である。

**命題 20.14.** 任意の自然数 $n \geq 1$ にたいして次がなりたつ：

$$[S_n, S_n] = A_n$$

*Proof.* 包含関係 $[S_n, S_n] \subset A_n$ は明らか。

逆向きの包含関係を示す。$A_n$ の要素というのは偶数個の Coxeter 元の積だったので、二つの Coxeter 元の積 $s_i s_j$ が $[S_n, S_n]$ に属することを示せばよい。

$j = i$ の場合は $s_i s_i = e$ なので目的の性質は示された。
$j = i + 1$ の場合は、直接計算で次をえる $s_i s_{i+1} = [s_{i+1}, s_i]$：

$$(\text{RHS}) \ = s_{i+1} s_i s_{i+1} s_i = s_i s_{i+1} s_i s_i = (\text{LHS})$$

$i + 1 < j$ の場合は

$$s_i s_j = s_i s_{i+1} s_{i+1} s_{i+2} \cdots s_{j-1} s_j = [s_{i+1}, s_i] \cdots [s_j, s_{j-1}]$$

$j < i$ の場合は $s_i s_j = (s_j s_i)^{-1}$ なので、$i$ と $j$ を入れ替えて上の考察を適用すればよい。 □

**補題 20.15.** $n \leq 4$ にたいして $S_n$ は可解である。

*Proof.* $n = 1$ の場合。$S_1 = \{e\}$ なので可解。

$n = 2$ の場合。$S_2$ は 2 次の巡回群なので特に可換であり、可解である。

$n = 3$ の場合。$D_1(S_3) = A_3$ は 3 次の巡回群である。よって、$D_2(S_3) = D_1(A_3) = \{e\}$ がなりたつ。

$n = 4$ の場合。$A_4$ の要素 $\sigma_1, \sigma_2, \sigma_3$ を以下で定める：

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \ \sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

（注意:講義で詳しく解説していない巡回置換を用いると、これらの要素はそれぞれ$\sigma_1 = (1,2)(3,4), \sigma_2 = (1,3)(2,4), \sigma_3 = (1,4)(2,3)$ とあらわされる。）
次の部分集合 $H$ は $S_4$ の部分群であり、$A_4$ の正規部分群である：

$$H = \{e, \sigma_1, \sigma_2, \sigma_3\}.$$

$H \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ であり、とくに可換群である。
さらに次が確かめられる：

$$D_2(S_4) = D_1(A_4) = H, \quad D_3(S_3) = D_1(H) = \{e\}$$

よって $S_4$ は可解である。 □

定理 *20.13* の証明. $n \leq 4$ にたいして $S_n$ が可解であることは個別の分析で示している。

$n \geq 5$ とする。
上の補題より $D_1(S_n) = A_n$ である。$n$ 次交代群 $A_n$ は単純群だったので $D_2(S_n) = D_1(A_n)$ は $A_n$ もしくは $\{e\}$ のどちらかである。しかし、$A_n$ は非可換群なので $D_1(A_n) \neq \{e\}$ である。よって、$D_2(S_n) = A_n$ である。帰納的に任意の自然数 $m$ にたいして $D_m(S_n) = A_n \neq \{e\}$ が分かる。
よって、$S_n$ は可解ではない。 □

# 21　対称群の共役類

2 以上の自然数 $n \geq 2$ にたいする対称群 $S_n$ の共役類を調べます。
　そのために、巡回置換表示をおもいだしましょう。

## 21.1　巡回置換表示と対称群の要素の型

**定義 21.1** (巡回置換). *(1)* $r$ を 2 以上の自然数とする。$r$ 個の要素からなる部分集合 $\{i_1, \cdots, i_r\} \subset \{1, \cdots, n\}$ にたいして要素 $(i_1 i_2 \cdots i_r) \in S_n$ をつぎの式で定義します：

　記号を簡単にするために $\sigma = (i_1 i_2 \cdots i_r)$ とかくことにします：

$$\sigma(j) = \begin{cases} i_{s+1} & (j = i_s \text{ for } s = 1, 2, \cdots, r-1) \\ i_1 & (j = i_r) \\ j & (j \notin \{i_1, \cdots, i_r\}) \end{cases}$$

*(2)* 便宜上、一点からなる部分集合 $\{i\} \subset \{1, 2, \cdots, n\}$ に付随する巡回置換 $(i)$ を単位元として定義します。

　巡回置換に関して次の二つの命題が基本的です。

**補題 21.2.** 二つの部分集合 $\{i_1, \cdots, i_p\}$, $\{j_1, \cdots, j_q\} \subset \{1, 2, \cdots, n\}$ が共通部分を持たなければ、巡回置換 $(i_1, i_2, \cdots, i_p)$, $(j_1, j_2, \cdots, j_q)$ は可換である。

**補題 21.3.** 要素 $\sigma \in S_n$ と巡回置換 $(i_1, i_2, \cdots, i_p)$ にたいして次の等式がなりたつ：

$$\sigma(i_1, i_2, \cdots, i_p)\sigma^{-1} = (\sigma(i_1), \sigma(i_2), \cdots, \sigma(i_p)).$$

**命題 21.4** (教科書 p97, 命題 4.2.1). $n \geq 2$ とする。
　要素 $\sigma \in S_n$ をとってくる。
　$\sigma$ は巡回置換の積で表され、

$$\sigma = (i_1^{(1)} \cdots i_{\lambda_1}^{(1)})(i_1^{(2)} \cdots i_{\lambda_2}^{(2)}) \cdots (i_1^{(p)}, \cdots, i_{\lambda_p}^{(p)}) \tag{21-10}$$

しかも、巡回置換に現れる部分集合は $\{1, 2, \cdots, n\}$ の非交和分解

$$\{1, 2, \cdots, n\} = \{i_1^{(1)}, \cdots, i_{\lambda_1}^{(1)}\} \sqcup \{i_1^{(2)}, \cdots, i_{\lambda_2}^{(2)}\} \sqcup \cdots \sqcup \{i_1^{(p)}, \cdots, i_{\lambda_p}^{(p)}\} \tag{21-11}$$

をあたえる。

　注意：

1. 補題 *21.2* より、等式 (21-10) において $\sigma$ の因子に現れている巡回置換は可換である。
　なので、積の順を並び替えて
$$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_p$$
　がなりたつとしてよい。

2. この命題では長さが 1 の巡回置換（つまり $\lambda_r = 1$ の場合）も考えに入れている。
   そうしないと、非交和分解 (21-11) は得られない。
   しかし、巡回置換の積に要素を表示する場合通常は長さ 1 の巡回置換は書かない。
   単位元なので計算結果はどちらの場合でも変わらない。

3. 非交和分解 (21-11) は $\sigma$ から一意的に定まる。
   また、巡回置換の積による表示 (21-10) も並び替えを除いて一意的である。

略証. 自然な作用 $S_n \curvearrowright \{1, 2, \cdots, n\}$ が誘導する作用 $\langle\sigma\rangle \curvearrowright \{1, 2, \cdots, n\}$ による軌道分解を考える：

$$\{1, 2, \cdots, n\} = \bigsqcup_{r=1}^{p} \langle\sigma\rangle i^{(r)}.$$

ただし、完全代表系を $R = \{i^{(1)}, i^{(2)}, \cdots, i^{(p)}\}$ とあらわした。
各 $r = 1, 2, \cdots, p$ にたいして

$$i_1^{(r)} := i^{(r)},\ i_2^{(r)} := \sigma(i^{(r)}), i_3^{(r)} := \sigma^2(i^{(r)}), \cdots, i_a^{(r)} := \sigma^{a-1}(i^{(r)}), \cdots (a \geq 1)$$

と定めればよい。 □

**定義 21.5.** 要素 $\sigma \in S_n$ の型 $\{\lambda_r\}_{r\geq 1}^{p}$ を $\sigma$ を巡回置換の積に表した時に得られる自然数の減少列

$$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_p$$

と定める。

**命題 21.6.** 二つの要素 $\sigma, \tau \in S_n$ が互いに共役であるための必要十分条件は型が一致することである。

*Proof.* 十分条件：二つの要素 $\sigma, \tau \in S_n$ の型が等しいとする。その型を $\{\lambda_r\}_{r=1}^{p}$ とする。

$$\sigma = (i_1^{(1)} \cdots i_{\lambda_1}^{(1)})(i_1^{(2)} \cdots i_{\lambda_2}^{(2)}) \cdots (i_1^{(p)}, \cdots, i_{\lambda_p}^{(p)}),$$
$$\tau = (j_1^{(1)} \cdots j_{\lambda_1}^{(1)})(j_1^{(2)} \cdots j_{\lambda_2}^{(2)}) \cdots (j_1^{(p)}, \cdots, j_{\lambda_p}^{(p)})$$

写像 $\eta : \{1, 2, \cdots, n\} \to \{1, 2, \cdots, n\}$ を

$$\eta(i_a^{(r)}) := j_a^{(r)} \quad (1 \leq r \leq p,\ a = 1, 2, \cdots, \lambda_r)$$

と定めると、これは全単射である。よって、$\eta$ は $S_n$ の要素である。

**主張 21.7.** 等式 $\eta\sigma\eta^{-1} = \tau$ がなりたつ。

この主張から $\sigma$ と $\tau$ は互いに共役である。

主張の証明. 任意の $k \in \{1, 2, \cdots, n\}$ にたいして $\eta\sigma\eta^{-1}(k) = \tau(k)$ を示せばよい。
これは補題 21.3 から従う。

□

必要条件であることは各自証明してみてください。 □

**命題 21.8.** 要素 $\sigma \in S_n$ は型 $\{\lambda_r\}_{r=1}^p$ を持つとする。

各自然数 $m \geq 1$ にたいして、$\lambda_r = m$ をみたす $r$ の個数を $L_m$ とおく：

$$L_m := \#\{r \mid \lambda_r = m\}.$$

このとき、$\sigma$ の共役類の個数 $\#C(\sigma)$ は次で与えられる：

$$\#C(\sigma) = \frac{n!}{\lambda_1\lambda_2\cdots\lambda_p L_1!L_2!\cdots L_{\lambda_1}!}. \tag{21-12}$$

*Proof.* 随伴作用 $\mathrm{ad} : S_n \curvearrowright S_n$ による安定化部分群 $\mathrm{stab}_{\mathrm{ad}}\,\sigma$ の位数は

$$\#\,\mathrm{stab}_{\mathrm{ad}}\,\sigma = \lambda_1\lambda_2\cdots\lambda_p L_1!L_2!\cdots L_{\lambda_1}!$$

である。

よって、

$$\#C(\sigma) = \frac{\#S_n}{\#\,\mathrm{stab}_{\mathrm{ad}}\,\sigma} = \frac{n!}{\lambda_1\lambda_2\cdots\lambda_p L_1!L_2!\cdots L_{\lambda_1}!}.$$

が成り立つ。 □

## 21.2 自然数の分割

**定義 21.9.** 1 以上の自然数 $n$ の分割 $\lambda = \{\lambda_r\}_{r=1}^p$ とは、1 以上の自然数の減少列

$$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_p$$

で

$$\lambda_1 + \lambda_2 + \cdots + \lambda_p = n$$

をみたすものをいう。減少列 $\lambda$ が $n$ の分割であることを

$$\lambda \vdash n$$

とあらわす。

**補題 21.10.** 任意の $n$ の分割 $\lambda$ にたいして、これを型とする要素 $\sigma$ が存在する。

$n$ の分割 $\lambda$ を型とする $S_n$ の要素の集合を $C_\lambda$ とあらわします。共役類による分解と類等式は次のように書けます：

$$S_n = \bigsqcup_{\lambda\vdash n} C_\lambda, \quad n! = \sum_{\lambda\vdash n} \#C_\lambda.$$

命題 21.8 を使うと対称群 $S_n$ の類等式は以下のことを主張します：

**命題 21.11.** $n$ を 1 以上の自然数とする。このとき、次の等式がなりたつ：

$$n! = \sum_{\lambda\vdash n} \frac{n!}{\lambda_1\lambda_2\cdots\lambda_p L_1^\lambda!L_2^\lambda!\cdots L_{\lambda_1}^\lambda!}. \tag{21-13}$$

ただし、ここで $n$ の分割 $\lambda$ と自然数 $m$ にたいして

$$L_m^\lambda := \#\{r \mid \lambda_r = m\}.$$

と定めた。

等式 (21-13) は $n!$ で割ることで、次と同値ですね：

$$1 = \sum_{\lambda\vdash n} \frac{1}{\lambda_1\lambda_2\cdots\lambda_p L_1^\lambda!L_2^\lambda!\cdots L_{\lambda_1}^\lambda!}. \tag{21-14}$$

こんな分数の和が 1 に一致するなんてビックリですね。（群論を使わずに証明をする方法はあるんでしょうか？）

### 21.2.1 例：$n = 3$

3 の分割は次の三つあります：

$$(1,1,1),\ (2,1),\ (3)$$

これに対応する共役類というのはそれぞれ次のようになります。

- $(1,1,1)$. 対応する共役類の要素は長さ 1 の巡回置換（＝単位元）の 3 個の積なので、単位元しかありません。

$$C_{(1,1,1)} = \{e\}.$$

分割 $(1,1,1)$ にたいしては $L_1 = 1$ であり、それ以外の $\lambda_p$ や $L_m$ は 1 になるので、共役類の個数を与える公式 (21-12) を計算すると

$$\frac{n!}{\lambda_1\lambda_2\cdots\lambda_p L_1!L_2!\cdots L_{\lambda_1}!} = \frac{3!}{3!} = 1$$

となり、もちろん、$\#C_{(1,1,1)} = 1$ と一致します。

- $(2,1)$. 対応する共役類の要素はは長さ 2 の巡回置換（と長さ 1 の巡回置換の積）です。なので、共役類は次です：

$$C_{(2,1)} = \{(12),(2,3),(1,3)\}.$$

共役類を与える公式 (21-12) を計算してみると、$L_m = 1, 0$ が任意の自然数 $m$ にたいして成り立つので

$$\frac{n!}{\lambda_1\lambda_2\cdots\lambda_p L_1!L_2!\cdots L_{\lambda_1}!} = \frac{3!}{2\times 1} = \frac{6}{2} = 3.$$

です。もちろん $\#C_{(2,1)} = 3$ と一致します。

- $(3)$. 対応する共役類は長さ 3 の巡回置換なので

$$C_{(3)} = \{(1,2,3),\ (1,3,2)\}.$$

共役類を与える公式 (21-12) を計算してみると、

$$\frac{n!}{\lambda_1\lambda_2\cdots\lambda_p L_1!L_2!\cdots L_{\lambda_1}!} = \frac{3!}{3} = \frac{6}{3} = 2.$$

もちろん、$\#C_{(3)} = 2$ と一致します。

### 21.2.2 例:$n = 4$

4 の分割は以下の五つです：

$$(1,1,1,1),\ (2,1,1),\ (2,2),\ (3,1),\ (4).$$

それぞれに対応する共役類をすべて書きならべるのは大変なので、個数だけを書きます。

- 

$$C_{(1,1,1,1)} = \frac{4!}{1\times 1\times 1\times 1\times 4!} = 1.$$

これは単位元の共役類の個数なので 1 です。

- $$C_{(2,1,1)} = \frac{4!}{2 \times 1 \times 1 \times 2!} = 6.$$
- $$C_{(2,2)} = \frac{4!}{2 \times 2 \times 2!} = 3.$$
- $$C_{(3,1)} = \frac{4!}{3 \times 1} = 8.$$
- $$C_{(4)} = \frac{4!}{4} = 6.$$

# 22

**命題 22.1.** 群 $G$ と真の部分群 $H$ にたいして、群準同型写像 $\phi, \psi : G \to K$ でつぎを満たすものが存在する：

*(1)* $\phi \neq \psi$.

*(2)* $\phi|_H = \psi|_H$.

*Proof.* 指数による場合分けを行う。

$[G : H] = 2$ の場合。この場合は $H$ は正規部分群である。商群 $G/H$ への商写像 $\pi : G \to G/H$ と自明な群準同型写像 $\epsilon : G \to G/H$ が条件をみたすものである。

$[G : H] \geq 3$ の場合。$G$ の $H$ に関する右剰余類による分解を考える。$R$ を $e$ を含む完全代表系とする。相異なる要素 $r_1, r_2 \in R$ を選ぶ。全単射 $\sigma : G \to G$ を

$$\sigma(g) := \begin{cases} g & (g \in G \setminus (Hr_1 \sqcup H_{r_2})) \\ gr_1^{-1}r_2 & (g \in Hr_1) \\ gr_2^{-1}r_1 & (g \in Hr_2) \end{cases}$$

$\sigma^2 = \mathrm{id}$ に注意しておく。

写像 $\phi : G \to \mathrm{Aut}_{\mathrm{Set}}(G)$ を $\phi_g(x) := gx$ で定義する。さらに、写像 $\psi : G \to \mathrm{Aut}_{\mathrm{Set}}(G)$ を $\psi(g) := \sigma\phi_g\sigma$ で定義する。こうすれば、この $\phi, \psi$ が条件を満たす。

(1) 定義から、次を得る：$\phi_{r_1}(e) = r_1$. 一方、

$$\psi_{r_1}(e) = \sigma\phi_{r_1}(e) = \sigma(r_1) = r_2.$$

ゆえに $\phi \neq \psi$ である。

(2) $h \in H$ をとって来る。$\phi_h = \psi_h$ を確かめる。
(2-i) $g \in G \setminus (Hr_1 \sqcup H_{r_2})$ の場合：

$$\psi_h(g) = \sigma\phi_h(g) = \sigma(hg) = hg = \phi_h(g).$$

(2-ii) $g \in Hr_1$ の場合：

$$\psi_h(g) = \sigma\phi_h(gr_1^{-1}r_2) = \sigma(hgr_1^{-1}r_2) = hg = \phi_h(g).$$

(2-iii) $g \in Hr_2$ の場合：

$$\psi_h(g) = \sigma\phi_h(gr_2^{-1}r_1) = \sigma(hgr_2^{-1}r_1) = hg = \phi_h(g).$$

□

**系 22.2.** 群準同型 $f : G \to H$ が群の圏のエピ射であるための必要十分条件は下部集合の写像として全射であることである。