

# 代数学 1 群論入門 [1]

## 2.6 同値関係と剰余類

早稲田大学大学院 基幹理工学研究科  
情報理工・情報通信専攻 上田研究室  
5119F105 山田 悠之介

2019/6/12

# 目次

- ① 同値関係
- ② 同値類と商
- ③ 剰余類
- ④ ラグランジュの定理と応用
- ⑤ 演習

# 同値関係

## 定義 2.6.1

集合  $S$  上の関係  $\sim$  は次を満たすとき、同値関係という

任意の  $a, b, c \in S$  に対し

反射律  $a \sim a$

対称律  $a \sim b$  なら  $b \sim a$

推移律  $a \sim b, b \sim c$  なら  $a \sim c$

ある意味で等しいということ（普通は＝より荒い）

＝は最も基本的で最も細かい同値関係

# 同値関係の例

## 写像が定める同値関係 (例 2.6.4)

$f: A \rightarrow B$  を写像とする

$x, y \in A$  に対し,  $f(x) = f(y)$  であるとき,  $x \sim_f y$  と定めるとこれは同値関係である

## 合同関係 (例 2.6.5)

$n \in \mathbb{Z}_{>0}$  を固定する

$x - y$  が  $n$  で割り切れるとき  $x \equiv y \pmod{n}$  と定める

$x \equiv y \pmod{n}$  は同値関係である

## 無向グラフ

無向グラフ  $G$  のにおいて,  $x, y \in G$  に対し

$x$  から  $y$  へ道があるとき  $x \sim y$  と定めるとこれは同値関係である

# 部分群による同値関係

## 例 2.6.6

$G$  を群,  $H$  を  $G$  の部分群とする

$x, y \in G$  に対し,  $x \sim y \stackrel{\text{def}}{\iff} x^{-1}y \in H$  とする

$\sim$  は同値関係である

$\therefore$  任意の  $x, y, z \in G$  に対し

**反射律**  $x^{-1}x = 1 \in H$

**対称律**  $x^{-1}y \in H$  なら  $H$  は部分群だったので

$$(x^{-1}y)^{-1} = y^{-1}x \in H$$

**推移律**  $x^{-1}y, y^{-1}z \in H$  なら  $x^{-1}yy^{-1}z = x^{-1}z \in H$

$G$  として  $\mathbb{Z}$ ,  $H$  として  $n\mathbb{Z}$  をとると

$x \sim y \iff -x + y \in n\mathbb{Z}$  であるので  $\sim$  は  $\text{mod } n$  である

# 同値類

## 定義 2.6.7

$\sim$  を集合  $S$  上の同値関係とする

$x \in S$  に対し  $C(x) \stackrel{\text{def}}{=} \{y \in S \mid y \sim x\}$  を  $x$  の同値類という

## 命題 2.6.8

$\sim$  を集合  $S$  上の同値関係,  $x \in S$  とすると次が成り立つ

- ① 任意の  $y, z \in C(x)$  に対し,  $y \sim z$
- ②  $y \in C(x)$  なら  $C(x) = C(y)$
- ③  $x, y \in S, C(x) \cap C(y) \neq \emptyset$  なら  $C(x) = C(y)$

## 証明

- ①  $y \sim x, x \sim z$  なので  $y \sim z$

# 続き

## 命題 2.6.8

$\sim$  を集合  $S$  上の同値関係,  $x \in S$  とすると次が成り立つ

- ① 任意の  $y, z \in C(x)$  に対し,  $y \sim z$
- ②  $y \in C(x)$  なら  $C(x) = C(y)$
- ③  $x, y \in S, C(x) \cap C(y) \neq \emptyset$  なら  $C(x) = C(y)$

## 証明

- ②  $y \in C(x)$  とすると任意の  $z \in S$  に対して
$$z \in C(x) \iff y \sim z \stackrel{\text{def}}{\iff} z \in C(y)$$
- ③  $x, y \in S, \exists z \in C(x) \cap C(y)$  なら  
(2) より  $C(x) = C(y) = C(z)$

## 命題 2.6.8 の意味

$S$  上の同値関係  $\sim$  は  $S$  上の無向グラフとみなせる  
このとき  $C(x)$  は  $x$  の (属する) 連結成分である

命題 2.6.8 は

- ①  $x$  と  $y$  が同じ連結成分に属するなら道が存在
- ②  $y$  が  $x$  の連結成分に属するなら,  
 $x$  の連結成分と  $y$  の連結成分は同じ
- ③  $x$  の連結成分と  $y$  の連結成分は共通部分があるなら同じ  
となる



## 商

## 定義 2.6.9

$\sim$  を  $S$  上の同値関係とする

- ①  $S/\sim \stackrel{\text{def}}{=} \{C(x) \mid x \in S\}$  を同値関係の商という  
 $x \mapsto C(x)$  という対応の写像を  $S$  から  $S/\sim$  への  
自然な写像という
- ②  $C \in S/\sim$  に対し,  $x \in C$  となる  $x$  を  $C$  の代表元という
- ③  $R \subset S$  が  $S/\sim$  の各元の代表元をちょうど1つずつ含むとき  
 $R$  を  $\sim$  の完全代表系という

# Remark, 同値類の例

## Remark

- 命題 2.6.8(2) より  
 $x$  が  $C \in S/\sim$  の代表元なら  $C = C(x)$  である
- 選択公理より完全代表系は必ずとれる
- 命題 2.6.8(3) より同値類は  $S$  の分割であるので  
完全代表系  $R$  を用いて  $S = \coprod_{x \in R} C(x)$

## 自明な同値関係 (例 2.6.11)

$S$  上の同値関係  $=$  を考えると,  $C(x) = \{x\}$  なので  
自然な写像  $S \rightarrow S/ =$  は全単射

# 同値類の例

## 写像が定める同値関係（例 2.6.12）

$f : A \rightarrow B$  に対し，同値関係  $\sim_f$  が構成できた

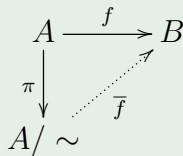
このとき  $\bar{f} : A / \sim_f \rightarrow B$  を

$C$  の代表元  $x$  を用いて  $\bar{f}(C) = f(x)$  と定めることができる

この写像  $\bar{f}$  は well-defined である

$\because x, y \in C \iff x \sim_f y \iff f(x) = f(y)$

$\pi : A \rightarrow A / \sim_f$  を自然な写像とすると， $f = \bar{f} \circ \pi$



# 集合の同型定理

$\bar{f}$  の定義より  $f(x) = f(y) \Rightarrow x \sim y$  なので  $\bar{f} : A/\sim \rightarrow B$  は単射  
よって  $\bar{f} : A/\sim \rightarrow f(A)$  は全単射

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \pi \downarrow & & \uparrow i \\ A/\sim & \xrightarrow{\bar{f}} & f(A) \end{array}$$

# 集合の群演算

## 定義

群  $G$  の部分集合  $S_1, S_2$  に対し

$S_1 S_2 \stackrel{\text{def}}{=} \{xy \mid x \in S_1, y \in S_2\}$  と定める

$S_1 = \{x\}$  のときには  $xS_2$  と書く

演算が加算のときには  $S_1 + S_2$  と書く

これは一般には群ではないことに注意!

## 合同関係 (例 2.6.15)

同値関係として合同関係を考える

$x \in \mathbb{Z}$  の同値類は  $y - x$  が  $n$  で割り切れるような整数全体である

これは  $y - x \in n\mathbb{Z}$  であることと同値である

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

この同値類を  $\bar{x}, x \bmod n$  などと書く

# 剰余類

## 定義 2.6.16

$H$  を群  $G$  の部分群,  $x, y \in G$  とする

- ①  $x \sim y \stackrel{\text{def}}{\iff} x^{-1}y \in H$  とすると同値関係であった  
 $x^{-1}y \in H \iff y \in xH$  なので  $x$  の同値類を  $xH$  と書き,  
 $x$  の  $H$  による左剰余類という  
この同値関係による商を  $G/H$  と書く
- ② 同様に  $yx^{-1}$  であるとき同値関係を  $x \sim y$  と定める  
 $x$  の同値類を  $Hx$  と書き,  
 $x$  の  $H$  による右剰余類という  
商を  $H \backslash G$  と書く

なぜ  $xH$  の集合が  $G/H$ ?

∴ 「 $h_1, h_2 \in H$  に対して  $xh_1, xh_2$  を同一視する」 もしくは  
「 $xH$  を  $x$  だと思う」 わけなので  $H$  で右から割ることになる

# Remark

- $G$  が可換群なら左剰余類と右剰余類は同じ
- 例 2.6.15 の同値関係は定義 2.6.16 の  $G, H$  として  $\mathbb{Z}, n\mathbb{Z}$  をとったものになる  
剰余類  $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$  は  
定義 2.2.9 で定義した  $\mathbb{Z}/n\mathbb{Z}$  と集合としては等しい  
 $H$  が正規部分群のとき  $G/H$  が群となること,  $\mathbb{Z}/n\mathbb{Z}$  が群として等しいことは 2.8 節で見る

# 剰余類と商の位数

## 命題 2.6.18

$H$  が群  $G$  の部分群なら次が成り立つ

- ①  $|G/H| = |H \backslash G|$
- ②  $\forall g \in G$  に対し  $|gH| = |Hg| = |H|$

## 証明

- ①  $\alpha : G/H \rightarrow H \backslash G$  を  $\alpha(gH) = Hg^{-1}$  と定める  
 $\alpha$  が well-def であることを確認する必要がある  
 $g \in G$  と同値なものは  $h \in H$  を用いて  $gh$  と書ける  
なので  $\alpha(ghH)$  が  $h$  の選び方によらず定まれば良い  
 $(gh)^{-1} = h^{-1}g^{-1}$  は  $g^{-1}$  と（右剰余類の意味で）同値  
よって  $Hh^{-1}g^{-1} = Hg^{-1}$  であり well-def である  
逆写像は  $Hg \mapsto g^{-1}H$  とすれば良い



## 続き

## 命題 2.6.18

$H$  が群  $G$  の部分群なら次が成り立つ

- ①  $|G/H| = |H \backslash G|$
- ②  $\forall g \in G$  に対し  $|gH| = |Hg| = |H|$

## 証明

- ②  $\phi: H \rightarrow gH$  を  $h \mapsto gh$  とする  
 $h_1, h_2 \in H$  が  $gh_1 = gh_2$  なら  $h_1 = h_2$  である  
よって  $\phi$  は単射  
任意の  $x \in gH$  はある  $h \in H$  で  $x = gh$  なので全射  
よって  $\phi$  は全単射なので  $|H| = |gH|$   
 $|H| = |Hg|$  も同様

# 指数とラグランジュの定理

命題 2.6.18 より次が定義できる

## 定義 2.6.19

$G/H, H \setminus G$  の元の個数を  $(G : H)$  と書き,  
 $H$  の  $G$  における指数という

## 定理 2.6.20 (ラグランジュの定理)

$H$  が群  $G$  の部分群なら

$$|G| = (G : H)|H|$$

## 証明

$G/H$  の完全代表系  $\{x_i\}$  を取ると  $G = \coprod_i x_i H$   
任意の  $i$  に対し  $|x_i H| = |H|$  なので  $|G| = (G : H)|H|$

# ラグランジュの定理の系

## 系 2.6.21

$G$  を有限群とすると次が成り立つ

- ①  $H$  が  $G$  の部分群なら  $|H|$  は  $|G|$  の約数
- ②  $g \in G$  の位数は  $|G|$  の約数である

## 証明

- ① 明らか
- ②  $|\langle g \rangle|$  は  $g$  の位数（命題 2.4.19）であるので明らか

逆に有限群  $G$  の位数の任意の約数  $n$  に対し、  
位数  $n$  の  $G$  の部分群はあるだろうか？

一般には NO!

ただし十分条件は知られている（4 章のシローの定理）

# 位数が素数の群

系 2.6.21 は与えられた群を調べるための手がかりとなる

## 命題 2.6.22

$G$  を位数が素数  $p$  の群とする

このとき単位元でない  $x \in G$  に対し  $G = \langle x \rangle$  となる

よって  $G$  は巡回群である

## 証明

$|\langle x \rangle|$  は  $|G| = p$  の約数である

$x \neq 1_G$  であるので  $|\langle x \rangle| = p = |G|$

よって  $G = \langle x \rangle$  なので巡回群である

# フェルマーの小定理

## 定理 2.6.23

$p$  が素数で  $x \in \mathbb{Z}$  が  $p$  で割り切れなければ

$$x^{p-1} \equiv 1 \pmod{p}$$

## 証明

$(\mathbb{Z}/p\mathbb{Z})^\times$  は位数  $p-1$  の群なので

系 2.6.21 より  $k = 1, \dots, p-1$  の位数は  $p-1$  の約数である

従って  $\bar{k}^{p-1} = \bar{1}$  なので  $p \mid k^{p-1} - 1$  である

$x \in \mathbb{Z}$  を  $p$  で割った余りが  $k$  とすると

$x^{p-1}$  と  $k^{p-1}$  は  $p$  で割った余りが等しいので

$$x^{p-1} \equiv 1 \pmod{p}$$

# フェルマーの小定理の系

## 系 2.6.24

$p$  が素数なら任意の  $x \in \mathbb{Z}$  に対し

$$x^p \equiv x \pmod{p}$$

## 証明

$p|x$  なら  $x^p \equiv 0 \equiv x \pmod{p}$

そうでないなら定理 2.6.23 より  $p|x^{p-1} - 1$  なので  $p|x^p - x$

# 演習

## 問題 2.6.1

$R \stackrel{\text{def}}{=} \{(x, x) \mid x \in \mathbb{R}\} \cup \{(x, 2x) \mid x \in \mathbb{R}\} \cup \{(2x, x) \mid x \in \mathbb{R}\}$   
とすると  $R$  は  $\mathbb{R}$  上の同値関係になるか？

## 問題 2.6.2

$G$  を群とする

$a, b \in G$  が共役 ( $\exists g(a = gbg^{-1})$ ) であるとき  $a \sim b$  と定めると  
 $\sim$  は  $G$  上の同値関係となる

# 演習

## 問題 2.6.3

位数 3 の群は位数 5 の群の部分群にはならないことを証明せよ

## 問題 2.6.4

$G$  が群,  $H, K$  は  $G$  の有限部分群で  $|H|, |K|$  は互いに素とする  
このとき  $H \cap K = 1_G$  であることを証明せよ



## 参考文献

- [1] 雪江明彦.  
代数学 1 群論入門.  
日本評論社, 2010.