

離散数理工学 第7回  
離散代数：有限群の構造

岡本 吉央  
okamotoy@uec.ac.jp

電気通信大学

2019年11月19日

最終更新：2019年11月26日 13:51

## スケジュール 前半 (予定)

- |   |                      |         |
|---|----------------------|---------|
| 1 | 数え上げの基礎：二項係数と二項定理    | (10/1)  |
| 2 | 数え上げの基礎：漸化式の立て方      | (10/8)  |
| 3 | 数え上げの基礎：漸化式の解き方 (基礎) | (10/15) |
| ★ | 休み (祝日)              | (10/22) |
| 4 | 数え上げの基礎：漸化式の解き方 (発展) | (10/29) |
| 5 | 離散代数：図形とグラフの対称性      | (11/5)  |
| 6 | 離散代数：有限群             | (11/12) |
| 7 | 離散代数：有限群の構造          | (11/19) |
| 8 | 離散代数：グラフの対称性と有限群     | (11/26) |

注意：予定の変更もありうる

## スケジュール 後半 (予定)

- |    |                           |         |
|----|---------------------------|---------|
| 9  | 離散確率論：確率的離散システムの解析 (基礎)   | (12/3)  |
| ★  | 中間試験                      | (12/10) |
| 10 | 離散確率論：確率的離散システムの解析 (発展)   | (12/17) |
| 11 | 離散確率論：乱択データ構造とアルゴリズム (基礎) | (1/7)   |
| 12 | 離散確率論：乱択データ構造とアルゴリズム (発展) | (1/14)  |
| 13 | 離散確率論：マルコフ連鎖 (基礎)         | (1/21)  |
| 14 | 離散確率論：マルコフ連鎖 (発展)         | (1/28)  |
| ★  | 授業等調整日                    | (2/4)   |
| ★  | 期末試験                      | (2/18?) |

注意：予定の変更もありうる

### 今日の目標

部分群に関する概念を理解する

- ▶ 部分群, 正規部分群
- ▶ 剰余群

2つの群が同型でないことを証明する方法の1つを体得する

- ▶ 群同型定理

## 目次

- ① 部分群
- ② 剰余類と正規部分群
- ③ 群同型定理
- ④ 今日のまとめ

## 部分群

群  $(G, \circ)$ ,  $H \subseteq G$

定義：部分群とは？

$(H, \circ)$  が群であるとき,  $H$  を  $G$  の部分群と呼ぶ

注意：  $(G, \circ)$  と  $(H, \circ)$  における演算は同一

定義の言い換え：部分群とは？

$H$  が  $G$  の部分群であるとは,

- ▶  $x, y \in H \Rightarrow x \circ y \in H$  (演算の保存)
- ▶  $G$  の単位元  $e$  に対して,  $e \in H$  (単位元の保存)
- ▶  $x \in H \Rightarrow G$  における  $x$  の逆元  $x^{-1}$  に対して  $x^{-1} \in H$  (逆元の保存)

## 部分群：例

$$G = \{e, a, b, x, y, z\}$$

	$\circ$	$e$	$a$	$b$	$x$	$y$	$z$
	$e$	$e$	$a$	$b$	$x$	$y$	$z$
	$a$	$a$	$x$	$y$	$e$	$z$	$b$
群表	$b$	$b$	$z$	$e$	$y$	$x$	$a$
	$x$	$x$	$e$	$z$	$a$	$b$	$y$
	$y$	$y$	$b$	$a$	$z$	$e$	$x$
	$z$	$z$	$y$	$x$	$b$	$a$	$e$

次の部分集合  $H$  は  $G$  の部分群か？

▶  $H = \{e, a\}$

$$(a^{-1} = x \notin H)$$

▶  $H = \{e, a, x\}$

$$(e^{-1} = e, a^{-1} = x, x^{-1} = a)$$

▶  $H = \{e, b, y\}$

$$(b \circ y = x \notin H)$$

## 部分群であるための必要十分条件

群  $(G, \circ)$ , 部分集合  $H \subseteq G$ ,  $H \neq \emptyset$

性質：部分群であるための必要十分条件

$H$  が  $G$  の部分群である  $\Leftrightarrow$  任意の  $a, b \in H$  に対して,  $a^{-1}b \in H$

$\Rightarrow$  の証明： $H$  が  $G$  の部分群であると仮定する

▶ 任意の  $a, b \in H$  を考える

▶

▶

$$a^{-1}b \in H$$

□

## 部分群であるための必要十分条件

群  $(G, \circ)$ , 部分集合  $H \subseteq G$ ,  $H \neq \emptyset$

性質：部分群であるための必要十分条件

$H$  が  $G$  の部分群である  $\Leftrightarrow$  任意の  $a, b \in H$  に対して,  $a^{-1}b \in H$

$\Rightarrow$  の証明： $H$  が  $G$  の部分群であると仮定する

- ▶ 任意の  $a, b \in H$  を考える
- ▶  $H$  は  $G$  の部分群なので,  $a^{-1} \in H$
- ▶

$$a^{-1}b \in H$$



## 部分群であるための必要十分条件

群  $(G, \circ)$ , 部分集合  $H \subseteq G$ ,  $H \neq \emptyset$

性質：部分群であるための必要十分条件

$H$  が  $G$  の部分群である  $\Leftrightarrow$  任意の  $a, b \in H$  に対して,  $a^{-1}b \in H$

$\Rightarrow$  の証明： $H$  が  $G$  の部分群であると仮定する

- ▶ 任意の  $a, b \in H$  を考える
- ▶  $H$  は  $G$  の部分群なので,  $a^{-1} \in H$
- ▶  $H$  は  $G$  の部分群で,  $a^{-1}, b \in H$  なので,  $a^{-1}b \in H$

□

## 部分群であるための必要十分条件 (続 1)

群  $(G, \circ)$ , 部分集合  $H \subseteq G$ ,  $H \neq \emptyset$

性質：部分群であるための必要十分条件

$H$  が  $G$  の部分群である  $\Leftrightarrow$  任意の  $a, b \in H$  に対して,  $a^{-1}b \in H$

$\Leftarrow$  の証明：任意の  $a, b \in H$  に対して  $a^{-1}b \in H$  であると仮定する

- ▶ このとき, 「演算の保存」, 「単位元の保存」, 「逆元の保存」を確認する

## 部分群であるための必要十分条件 (続 1)

群  $(G, \circ)$ , 部分集合  $H \subseteq G$ ,  $H \neq \emptyset$

性質：部分群であるための必要十分条件

$H$  が  $G$  の部分群である  $\Leftrightarrow$  任意の  $a, b \in H$  に対して,  $a^{-1}b \in H$

$\Leftarrow$  の証明：任意の  $a, b \in H$  に対して  $a^{-1}b \in H$  であると仮定する

▶ このとき, 「演算の保存」, 「単位元の保存」, 「逆元の保存」を確認する

単位元の保存

## 部分群であるための必要十分条件 (続 1)

群  $(G, \circ)$ , 部分集合  $H \subseteq G$ ,  $H \neq \emptyset$

性質：部分群であるための必要十分条件

$H$  が  $G$  の部分群である  $\Leftrightarrow$  任意の  $a, b \in H$  に対して,  $a^{-1}b \in H$

$\Leftarrow$  の証明：任意の  $a, b \in H$  に対して  $a^{-1}b \in H$  であると仮定する

- ▶ このとき, 「演算の保存」, 「単位元の保存」, 「逆元の保存」を確認する

単位元の保存

- ▶  $H \neq \emptyset$  なので, ある  $x \in G$  が存在して  $x \in H$

## 部分群であるための必要十分条件 (続 1)

群  $(G, \circ)$ , 部分集合  $H \subseteq G$ ,  $H \neq \emptyset$

性質：部分群であるための必要十分条件

$H$  が  $G$  の部分群である  $\Leftrightarrow$  任意の  $a, b \in H$  に対して,  $a^{-1}b \in H$

$\Leftarrow$  の証明：任意の  $a, b \in H$  に対して  $a^{-1}b \in H$  であると仮定する

- ▶ このとき, 「演算の保存」, 「単位元の保存」, 「逆元の保存」を確認する

単位元の保存

- ▶  $H \neq \emptyset$  なので, ある  $x \in G$  が存在して  $x \in H$
- ▶ 仮定において  $a = b = x$  とすると,  $x^{-1}x \in H$  が得られる

## 部分群であるための必要十分条件 (続 1)

群  $(G, \circ)$ , 部分集合  $H \subseteq G$ ,  $H \neq \emptyset$

性質：部分群であるための必要十分条件

$H$  が  $G$  の部分群である  $\Leftrightarrow$  任意の  $a, b \in H$  に対して,  $a^{-1}b \in H$

$\Leftarrow$  の証明：任意の  $a, b \in H$  に対して  $a^{-1}b \in H$  であると仮定する

- ▶ このとき, 「演算の保存」, 「単位元の保存」, 「逆元の保存」を確認する

単位元の保存

- ▶  $H \neq \emptyset$  なので, ある  $x \in G$  が存在して  $x \in H$
- ▶ 仮定において  $a = b = x$  とすると,  $x^{-1}x \in H$  が得られる
- ▶ 逆元の定義より,  $x^{-1}x = e$  なので,  $e \in H$  □

## 部分群であるための必要十分条件 (続 2)

群  $(G, \circ)$ , 部分集合  $H \subseteq G$ ,  $H \neq \emptyset$

性質 : 部分群であるための必要十分条件

$H$  が  $G$  の部分群である  $\Leftrightarrow$  任意の  $a, b \in H$  に対して,  $a^{-1}b \in H$

$\Leftarrow$  の証明 (続) :

## 部分群であるための必要十分条件 (続 2)

群  $(G, \circ)$ , 部分集合  $H \subseteq G$ ,  $H \neq \emptyset$

性質 : 部分群であるための必要十分条件

$H$  が  $G$  の部分群である  $\Leftrightarrow$  任意の  $a, b \in H$  に対して,  $a^{-1}b \in H$

$\Leftarrow$  の証明 (続) :

逆元の保存 :  $x \in H$  とする

演算の保存 :

これで3つの性質の成立が確かめられた



## 部分群であるための必要十分条件 (続 2)

群  $(G, \circ)$ , 部分集合  $H \subseteq G$ ,  $H \neq \emptyset$

性質 : 部分群であるための必要十分条件

$H$  が  $G$  の部分群である  $\Leftrightarrow$  任意の  $a, b \in H$  に対して,  $a^{-1}b \in H$

$\Leftarrow$  の証明 (続) :

**逆元の保存** :  $x \in H$  とする

▶ 仮定において  $a = x, b = e$  とすると,  $x^{-1}e \in H$  が得られる

**演算の保存** :

これで3つの性質の成立が確かめられた □

## 部分群であるための必要十分条件 (続 2)

群  $(G, \circ)$ , 部分集合  $H \subseteq G$ ,  $H \neq \emptyset$

性質 : 部分群であるための必要十分条件

$H$  が  $G$  の部分群である  $\Leftrightarrow$  任意の  $a, b \in H$  に対して,  $a^{-1}b \in H$

$\Leftarrow$  の証明 (続) :

逆元の保存 :  $x \in H$  とする

- ▶ 仮定において  $a = x, b = e$  とすると,  $x^{-1}e \in H$  が得られる
- ▶ 単位元の定義より,  $x^{-1}e = x^{-1}$  なので,  $x^{-1} \in H$  □

演算の保存 :

これで3つの性質の成立が確かめられた □

## 部分群であるための必要十分条件 (続 2)

群  $(G, \circ)$ , 部分集合  $H \subseteq G$ ,  $H \neq \emptyset$ 

性質 : 部分群であるための必要十分条件

 $H$  が  $G$  の部分群である  $\Leftrightarrow$  任意の  $a, b \in H$  に対して,  $a^{-1}b \in H$  $\Leftarrow$  の証明 (続) :逆元の保存 :  $x \in H$  とする

- ▶ 仮定において  $a = x, b = e$  とすると,  $x^{-1}e \in H$  が得られる
- ▶ 単位元の定義より,  $x^{-1}e = x^{-1}$  なので,  $x^{-1} \in H$  □

演算の保存 :  $x, y \in H$  とするこれで3つの性質の成立が確かめられた □

## 部分群であるための必要十分条件 (続 2)

群  $(G, \circ)$ , 部分集合  $H \subseteq G$ ,  $H \neq \emptyset$ 

性質 : 部分群であるための必要十分条件

 $H$  が  $G$  の部分群である  $\Leftrightarrow$  任意の  $a, b \in H$  に対して,  $a^{-1}b \in H$  $\Leftarrow$  の証明 (続) :逆元の保存 :  $x \in H$  とする

- ▶ 仮定において  $a = x, b = e$  とすると,  $x^{-1}e \in H$  が得られる
- ▶ 単位元の定義より,  $x^{-1}e = x^{-1}$  なので,  $x^{-1} \in H$  □

演算の保存 :  $x, y \in H$  とする

- ▶ 仮定において,  $a = x^{-1}, b = y$  とすると,  $(x^{-1})^{-1}y \in H$  が得られる

これで3つの性質の成立が確かめられた □

## 部分群であるための必要十分条件 (続 2)

群  $(G, \circ)$ , 部分集合  $H \subseteq G$ ,  $H \neq \emptyset$ 

性質 : 部分群であるための必要十分条件

 $H$  が  $G$  の部分群である  $\Leftrightarrow$  任意の  $a, b \in H$  に対して,  $a^{-1}b \in H$  $\Leftarrow$  の証明 (続) :逆元の保存 :  $x \in H$  とする

- ▶ 仮定において  $a = x, b = e$  とすると,  $x^{-1}e \in H$  が得られる
- ▶ 単位元の定義より,  $x^{-1}e = x^{-1}$  なので,  $x^{-1} \in H$  □

演算の保存 :  $x, y \in H$  とする

- ▶ 仮定において,  $a = x^{-1}, b = y$  とすると,  $(x^{-1})^{-1}y \in H$  が得られる
- ▶ 演習問題 6.6 より,  $(x^{-1})^{-1} = x$  なので,  $xy \in H$  となる □

これで3つの性質の成立が確かめられた □

## 同型写像と部分群

群  $(G, \circ), (G', \circ')$ , 同型写像  $f: G \rightarrow G'$ , 部分群  $H \subseteq G$

## 性質：同型写像と部分群

$f(H)$  は  $G'$  の部分群

定義の確認： $f(H) = \{f(h) \mid h \in H\}$  ( $f$  による  $H$  の像)

証明：任意の  $a, b \in f(H)$  が  $a^{-1}b \in f(H)$  を満たすことを示す

- ▶  $f$  は同型写像なので, ある  $x, y \in H$  が存在して,  $f(x) = a, f(y) = b$
- ▶  $f$  は同型写像なので,

$$a^{-1}b = f(x)^{-1}f(y) \stackrel{(*)}{=} f(x^{-1})f(y) = f(x^{-1}y)$$

- ▶  $H$  は部分群なので,  $x^{-1}y \in H$
- ▶  $\therefore f(x^{-1}y) \in f(H)$  であり,  $a^{-1}b \in f(H)$

□

注：(\*) は演習問題

# 目次

- ① 部分群
- ② 剰余類と正規部分群
- ③ 群同型定理
- ④ 今日のまとめ

## 左剰余類

群  $(G, \circ)$ , 部分群  $H \subseteq G$ , 要素  $g \in G$

定義：左剰余類とは？

$g$  に関する  $H$  の左剰余類とは、次の集合のこと

$$gH = \{gh \mid h \in H\}$$

$G = \{e, a, b, x, y, z\}$ , 部分群  $H = \{e, a, x\}$

$\circ$	$e$	$a$	$b$	$x$	$y$	$z$
$e$	$e$	$a$	$b$	$x$	$y$	$z$
$a$	$a$	$x$	$y$	$e$	$z$	$b$
$b$	$b$	$z$	$e$	$y$	$x$	$a$
$x$	$x$	$e$	$z$	$a$	$b$	$y$
$y$	$y$	$b$	$a$	$z$	$e$	$x$
$z$	$z$	$y$	$x$	$b$	$a$	$e$

$$bH = \{be, ba, bx\} = \{b, z, y\}, \quad yH = \{ye, ya, yx\} = \{y, b, z\}$$

## 右剰余類

群  $(G, \circ)$ , 部分群  $H \subseteq G$ , 要素  $g \in G$

定義：右剰余類とは？

$g$  に関する  $H$  の右剰余類とは、次の集合のこと

$$Hg = \{hg \mid h \in H\}$$

$G = \{e, a, b, x, y, z\}$ , 部分群  $H = \{e, a, x\}$

$\circ$	$e$	$a$	$b$	$x$	$y$	$z$
$e$	$e$	$a$	$b$	$x$	$y$	$z$
$a$	$a$	$x$	$y$	$e$	$z$	$b$
$b$	$b$	$z$	$e$	$y$	$x$	$a$
$x$	$x$	$e$	$z$	$a$	$b$	$y$
$y$	$y$	$b$	$a$	$z$	$e$	$x$
$z$	$z$	$y$	$x$	$b$	$a$	$e$

$$Hb = \{eb, ab, xb\} = \{b, y, z\} = bH$$

## 剰余類と同値関係

群  $G$ , 部分群  $H \subseteq G$  $G$  の上の二項関係  $\sim$  を次で定義任意の  $a, b \in G$  に対して

$$a \sim b \iff aH = bH$$

先ほどの例 :  $b \sim y$ 

性質 : この二項関係は同値関係

上で定義した  $\sim$  は  $G$  上の同値関係, つまり, 次の3つを満たす

- ▶ 任意の  $a \in G$  に対して,  $aH = aH$  (反射性)
- ▶ 任意の  $a, b \in G$  に対して,  $aH = bH$  ならば  $bH = aH$  (対称性)
- ▶ 任意の  $a, b, c \in G$  に対して,  $aH = bH$  かつ  $bH = cH$  ならば  
 $aH = cH$  (推移性)

これが成り立つことはすぐ分かる (演習問題)

## 剰余類と同値分割

群  $G$ , 部分群  $H \subseteq G$  $G$  上の二項関係  $\sim$  を次で定義任意の  $a, b \in G$  に対して

$$a \sim b \iff aH = bH$$

これは  $G$  上の同値関係なので,  $G$  の同値分割を与える

つまり,

 $G / \sim = \{gH \mid g \in G\}$  は  $G$  の分割この同値分割を  $G/H$  と書く (注:  $\frac{G}{H}$  とは書かない)先ほどの例:  $G = \{e, a, b, x, y, z\}$ ,  $H = \{e, a, x\}$  $eH = aH = xH = \{e, a, x\}$ ,  $bH = yH = zH = \{b, y, z\}$  なので,

$$G/H = \{\{e, a, x\}, \{b, y, z\}\}$$

## 正規部分群

群  $(G, \circ)$ , 部分群  $H \subseteq G$

定義：正規部分群とは？

$H$  が  $G$  の正規部分群であるとは、次の条件を満たすこと

任意の要素  $g \in G$  に対して、 $gH = Hg$

$\circ$	$e$	$a$	$b$	$x$	$y$	$z$
$e$	$e$	$a$	$b$	$x$	$y$	$z$
$a$	$a$	$x$	$y$	$e$	$z$	$b$
$b$	$b$	$z$	$e$	$y$	$x$	$a$
$x$	$x$	$e$	$z$	$a$	$b$	$y$
$y$	$y$	$b$	$a$	$z$	$e$	$x$
$z$	$z$	$y$	$x$	$b$	$a$	$e$

- ▶  $H = \{e, a, x\}$  は  $G$  の正規部分群
- ▶  $H = \{e, b\}$  は  $G$  の部分群であるが、正規部分群ではない
  - ▶  $aH = \{ae, ab\} = \{a, y\}$
  - ▶  $Ha = \{ea, ba\} = \{a, z\}$

## 正規部分群と同値分割：例

群  $G$ 

定義：部分集合の積

 $G$  の2つの部分集合  $H_1, H_2$  に対して,  $H_1 H_2$  を次のように定義

$$H_1 H_2 = \{h_1 h_2 \mid h_1 \in H_1, h_2 \in H_2\}$$

先ほどの例で,  $H = \{e, a, x\}$  のとき,

	$\{e, a, x\}$	$\{b, y, z\}$
$\{e, a, x\}$	$\{e, a, x\}$	$\{b, y, z\}$
$\{b, y, z\}$	$\{b, y, z\}$	$\{e, a, x\}$

 $\rightsquigarrow$   $H$  が正規部分群であるとき,  $G/H$  はこの演算に関して群になる

## 正規部分群と同値分割 (1)

群  $G$ , 部分群  $H \subseteq G$

性質：正規部分群と同値分割

$H$  が  $G$  の正規部分群  $\Rightarrow G/H$  は前のページの演算で群になる

証明：4つのことを確認する

- ▶ 演算で閉じていること
- ▶ 単位元を持つこと
- ▶ 逆元を持つこと
- ▶ 結合性を持つこと

## 部分集合の積の性質

群  $G$ 

## 性質：部分集合の積の性質

- 1  $H$  が  $G$  の部分群  $\Rightarrow HH = H$
- 2  $H_1, H_2, H_3 \subseteq G \Rightarrow (H_1 H_2) H_3 = H_1 (H_2 H_3)$

証明 1 :  $H$  が  $G$  の部分群であるとする

- ▶  $H$  は演算で閉じているので、任意の  $h, h' \in H$  に対して、 $hh' \in H$
- ▶  $\therefore HH \subseteq H$
- ▶ 一方で、任意の  $h \in H$  に対して、 $h = eh \in HH$
- ▶  $\therefore H \subseteq HH$  □

証明 2 :  $H_1, H_2, H_3 \subseteq G$  とし、 $h_1 \in H_1, h_2 \in H_2, h_3 \in H_3$  とする

- ▶  $G$  が結合性を持つので、 $(h_1 h_2) h_3 = h_1 (h_2 h_3)$
- ▶  $\therefore (H_1 H_2) H_3 = H_1 (H_2 H_3)$  □

## 正規部分群と同値分割 (2)

## 演算で閉じていること

- ▶  $H_1, H_2 \in G/H$  とすると,  
ある  $g_1, g_2 \in G$  を使って,  $H_1 = g_1H, H_2 = g_2H = Hg_2$  と書ける
- ▶ このとき, 「部分集合の積の性質」から

$$\begin{aligned} H_1 H_2 &= (g_1H)(g_2H) \stackrel{2}{=} g_1(Hg_2)H \\ &= g_1(g_2H)H \stackrel{2}{=} g_1g_2(HH) \stackrel{1}{=} g_1g_2H \end{aligned}$$

- ▶  $g_1g_2H \in G/H$  なので, 確かに  $G/H$  はこの演算で閉じている

## 結合性を持つこと :

- ▶ 「部分集合の積の性質 2」から正しいと分かる

## 正規部分群と同値分割 (3)

**単位元を持つこと** :  $eH \in G/H$  が単位元であることを示す

- ▶  $gH \in G/H$  とすると (ただし,  $g \in G$  は任意の要素)

$$(gH)(eH) = g(He)H = g(eH)H = (ge)(HH) = gH$$

$$(eH)(gH) = e(Hg)H = e(gH)H = (eg)(HH) = gH$$

- ▶ したがって,  $eH$  は  $G/H$  の単位元である

**逆元を持つこと** :  $gH \in G/H$  の逆元が  $g^{-1}H \in G/H$  であることを示す

- ▶  $eH$  が  $G/H$  の単位元なので, 次の計算から それが分かる

$$(gH)(g^{-1}H) = g(Hg^{-1})H = g(g^{-1}H)H = (gg^{-1})(HH) = eH$$

$$(g^{-1}H)(gH) = g^{-1}(Hg)H = g^{-1}(gH)H = (g^{-1}g)(HH) = eH$$

□

## 目次

- ① 部分群
- ② 剰余類と正規部分群
- ③ 群同型定理**
- ④ 今日のまとめ

## 群同型定理

群  $G, G'$ , 同型写像  $f: G \rightarrow G'$ , 部分群  $H \subseteq G$

## 群同型定理 (第一群同型定理)

$H$  が  $G$  の正規部分群  $\Rightarrow G/H$  と  $G'/f(H)$  は同型

注:

- ▶  $f(H)$  は  $G'$  の正規部分群 (まず, これを確認する)
- ▶ 通常「第一群同型定理」と呼ばれるものは, これと内容が違う  
ここでの「第一群同型定理」は通常「第一群同型定理」から分かる

## 群同型定理：補題

群  $G, G'$ , 群同型写像  $f: G \rightarrow G'$ , 部分群  $H \subseteq G$

## 補題

$H$  が  $G$  の正規部分群  $\Rightarrow f(H)$  が  $G'$  の正規部分群

証明：任意の  $g' \in G'$  に対して  $g'f(H) \subseteq f(H)g'$  となることを示す  
 $(g'f(H) \supseteq f(H)g')$  の証明も同様)

- ▶  $g'f(x) \in g'f(H)$  とする (ただし,  $x \in H$ )
- ▶  $f$  は同型写像なので, ある  $g \in G$  に対して,  $g' = f(g)$
- ▶  $gH = Hg$  より, ある  $y \in H$  が存在して,  $gx = yg$
- ▶  $\therefore g'f(x) = f(g)f(x) = f(gx) = f(yg) = f(y)f(g) = f(y)g'$
- ▶  $f(y) \in f(H)$  なので,  $g'f(x) = f(y)g' \in f(H)g'$  □

## 群同型定理：証明 (1)

写像  $f': G/H \rightarrow G'/f(H)$  を次のように定義

$$\text{任意の } gH \in G/H \text{ に対して } f'(gH) = f(g)f(H)$$

この  $f'$  が同型写像であることを証明する  
つまり、次の3つを証明する

1  $f'$  が全射であること

$$\forall g'f(H) \in G'/f(H) \exists gH \in G/H : f'(gH) = g'f(H)$$

2  $f'$  が単射であること

$$f'(g_1H) = f'(g_2H) \Rightarrow g_1H = g_2H$$

3  $f'$  が次を満たすこと

$$\forall g_1H, g_2H \in G/H : f'(g_1Hg_2H) = f'(g_1H)f'(g_2H)$$

## 群同型定理：証明 (2)

証明 1：任意の  $g'f(H) \in G'/f(H)$  を考える

- ▶  $f$  は全射なので、ある  $g \in G$  が存在して、 $f(g) = g'$
- ▶ このとき、 $gH \in G/H$  を考えると

$$f'(gH) = f(g)f(H) = g'f(H) \in G'/f(H)$$

証明 2：  $g_1H, g_2H \in G/H$  が  $f'(g_1H) = f'(g_2H)$  を満たすとする

- ▶ このとき、 $f(g_1)f(H) = f'(g_1H) = f'(g_2H) = f(g_2)f(H)$
- ▶ まず、 $g_1H \subseteq g_2H$ であることを示す ( $g_1H \supseteq g_2H$ の証明も同様)
- ▶  $g_1h_1 \in g_1H$  とすると、

$$f(g_1h_1) = f(g_1)f(h_1) \in f(g_1)f(H) = f(g_2)f(H)$$

- ▶ よって、ある  $h_2 \in H$  が存在して、 $f(g_1h_1) = f(g_2)f(h_2) = f(g_2h_2)$
- ▶  $f$  は全単射なので、 $g_1h_1 = g_2h_2$  (つまり、 $g_1h_2 \in g_2H$ )

## 群同型定理：証明 (3)

証明 3 :  $g_1H, g_2H \in G/H$  とする

▶ このとき

$$\begin{aligned}
 f'(g_1Hg_2H) &= f'(g_1g_2HH) && (H \text{ が } G \text{ の正規部分群}) \\
 &= f'(g_1g_2H) && (H \text{ は } G \text{ の部分群}) \\
 &= f(g_1g_2)f(H) && (f' \text{ の定義}) \\
 &= f(g_1)f(g_2)f(H) && (f \text{ は同型写像}) \\
 &= f(g_1)f(g_2)f(H)f(H) && (f(H) \text{ は } G' \text{ の部分群}) \\
 &= f(g_1)f(H)f(g_2)f(H) && (f(H) \text{ は } G' \text{ の正規部分群}) \\
 &= f'(g_1H)f'(g_2H) && (f' \text{ の定義})
 \end{aligned}$$

これで、証明が完了した

□

## 群同型定理：再掲

群  $G, G'$ , 同型写像  $f: G \rightarrow G'$ , 部分群  $H \subseteq G$

## 群同型定理 (第一群同型定理)

$H$  が  $G$  の正規部分群  $\Rightarrow G/H$  と  $G'/f(H)$  は同型

## 目次

- ① 部分群
- ② 剰余類と正規部分群
- ③ 群同型定理
- ④ 今日のまとめ

## 今日のまとめ

## 今日の目標

部分群に関する概念を理解する

- ▶ 部分群, 正規部分群
- ▶ 剰余群

2つの群が同型でないことを証明する方法の1つを体得する

- ▶ 群同型定理

## 残った時間の使い方

- ▶ 演習問題をやる
  - ▶ 相談推奨 (ひとりでやらない)
- ▶ 質問をする
  - ▶ 教員と TA は巡回
- ▶ 退室時, 小さな紙に感想など書いて提出する ← 重要
  - ▶ 内容は何でも OK
  - ▶ 匿名で OK

## 目次

- ① 部分群
- ② 剰余類と正規部分群
- ③ 群同型定理
- ④ 今日のまとめ