

離散数学及び演習  
講義12 2016. 7.14(木)

部分系, 準同型  
(教科書 pp.164-165, 170-173)

群(復習)

- 代数系  $(G, \cdot)$  は群(group)である
  - 次の(1)~(3)が成り立つ.
  - (1) 任意の  $x, y, z \in G$  に対して,  $x \cdot (y \cdot z) = (x \cdot y) \cdot z$   
(結合則 (associative law))
  - (2)  $e \in G$  が存在して, 任意の  $x \in G$  に対して,  $x \cdot e = e \cdot x = x$   
(単位元の存在)
    - $e$  ... 単位元 (unit element, identity element)
  - (3) 任意の  $x \in G$  に対して,  $y \in G$  が存在して,  $x \cdot y = y \cdot x = e$   
(逆元の存在)
    - $y = x^{-1}$  ...  $x$  の逆元 (inverse element)
- 条件(1)~(3) ... 群の公理 (axiom)

2

代数系間の関係

- 代数系
  - 組  $(X, f_1, f_2, \dots, f_n)$ 
    - $X$  は集合
    - $f_i: X^2 \rightarrow X$  ( $i=1, 2, \dots, n$ )
- 代数系  $(X, f_1, f_2, \dots, f_n), (Y, g_1, g_2, \dots, g_n)$  間の関係
  - 部分系
  - 準同型, 同型
  - 商系 (次回講義)

3

部分系(subsystem)

- 代数系  $(X, f_1, f_2, \dots, f_n)$  は代数系  $(Y, g_1, g_2, \dots, g_n)$  の部分系である
  - 次の(1), (2)が成り立つ.
  - (1)  $X \subseteq Y$
  - (2)  $(X, f_1, f_2, \dots, f_n)$  と  $(Y, g_1, g_2, \dots, g_n)$  は同じ公理を満たす.
- 代数系  $(H, \cdot)$  は群  $(G, \cdot)$  の部分群(subgroup) である
  - $H \subseteq G$ , かつ,  $(H, \cdot)$  は群である.
- 代数系  $(S, +, \cdot)$  は環  $(R, +, \cdot)$  の部分環(subring) である
  - $S \subseteq R$ , かつ,  $(S, +, \cdot)$  は環である.
- 代数系  $(K, +, \cdot)$  は体  $(F, +, \cdot)$  の部分体(subfield) である
  - $K \subseteq F$ , かつ,  $(K, +, \cdot)$  は体である.

4

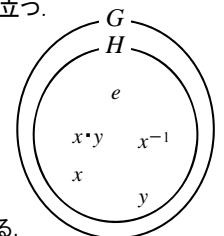
部分系(続き)

- 例:
- 整数環  $\mathbf{Z}$  は実数環  $\mathbf{R}$  の部分環
  - 実数体  $\mathbf{R}$  は複素数体  $\mathbf{C}$  の部分体
  - 自明な部分系
    - 群  $(G, \cdot, e)$  に対して,  
群  $(G, \cdot, e)$ , 群  $(\{e\}, \cdot, e)$  は部分群である  
... 自明な部分群
    - 環  $(R, +, \cdot, c, e)$  に対して,  
環  $(R, +, \cdot, c, e)$ , 環  $(\{c\}, +, \cdot, c, e)$  は部分環である  
... 自明な部分環

5

定理

- $(H, \cdot)$  が群  $(G, \cdot, e)$  の部分群であるとき,  
かつそのときに限り, 次の(1)~(4)が成り立つ.
- (1)  $H \subseteq G$ .
  - (2)  $e \in H$ .
  - (3) 任意の  $x \in H$  に対して,  $x^{-1} \in H$ .
  - (4) 任意の  $x, y \in H$  に対して,  $x \cdot y \in H$ .



- (2)  $G$  の単位元  $e$  は  $H$  の単位元でもある.
- (3)  $G$  における逆元は  $H$  における逆元でもある.

6

### 証明

- $(H, \cdot)$  が群  $(G, \cdot, e)$  の部分群であるとき、かつそのときに限り、次の(1)~(4)が成り立つ。
- (1)  $H \subseteq G$ . (2)  $e \in H$ . (3) 任意の  $x \in H$  に対して、 $x^{-1} \in H$ .
- (4) 任意の  $x, y \in H$  に対して、 $x \cdot y \in H$ .
- a) 「 $(H, \cdot)$  が  $(G, \cdot)$  の部分群ならば、(1)~(4)が成り立つ」を示す。
  - b) 「(1)~(4)が成り立つならば、 $(H, \cdot)$  は  $(G, \cdot)$  の部分群」を示す。
- 
- a)  $(H, \cdot)$  は  $(G, \cdot)$  の部分群であるとする。
- (1) 部分群の定義から明らかに、 $H \subseteq G$ .
- (2)  $H$  は群だから、単位元  $e' \in H$  が存在する。  
このとき、任意の  $x \in H$  に対して、 $x \cdot e' = e' \cdot x = x$ .  
ところが、 $x, e' \in H \subseteq G$  だから、 $e'$  は  $G$  の単位元でもある。  
群の単位元は唯一だから、 $e = e' \in H$ .
- (3)  $H$  は群だから、明らかに、任意の  $x \in H$  に対して、 $x^{-1} \in H$ .
- (4)  $H$  は群だから、明らかに、任意の  $x, y \in H$  に対して、 $x \cdot y \in H$ .

7

### 証明(続き)

- $(H, \cdot)$  が群  $(G, \cdot, e)$  の部分群であるとき、かつそのときに限り、次の(1)~(4)が成り立つ。
- (1)  $H \subseteq G$ . (2)  $e \in H$ . (3) 任意の  $x \in H$  に対して、 $x^{-1} \in H$ .
- (4) 任意の  $x, y \in H$  に対して、 $x \cdot y \in H$ .
- b) 「(1)~(4)が成り立つならば、 $(H, \cdot)$  は  $(G, \cdot)$  の部分群」を示す。
    - b-1)  $H \subseteq G$  を示す。
    - b-2) 「 $H$  は演算  $\cdot$  に関して閉じている」を示す。
    - b-3) 「 $(H, \cdot)$  は群の公理を満たす」を示す。
- 
- b) (1)~(4)が成り立つと仮定する。
- b-1) (1)から、 $H \subseteq G$ .
- b-2) (4)から、 $H$  は演算  $\cdot$  について閉じている。

8

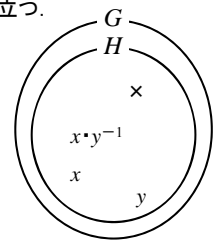
### 証明(続き2)

- $(H, \cdot)$  が群  $(G, \cdot, e)$  の部分群であるとき、かつそのときに限り、次の(1)~(4)が成り立つ。
- (1)  $H \subseteq G$ . (2)  $e \in H$ . (3) 任意の  $x \in H$  に対して、 $x^{-1} \in H$ .
- (4) 任意の  $x, y \in H$  に対して、 $x \cdot y \in H$ .
- b) 「(1)~(4)が成り立つならば、 $(H, \cdot)$  は  $(G, \cdot)$  の部分群」を示す。
    - b-3) 「 $(H, \cdot)$  は群の公理を満たす」を示す。
      - 1) 結合則, 2) 単位元の存在, 3) 逆元の存在
- 
- b) (1)~(4)が成り立つと仮定する。
- b-3-1) 任意の  $x, y, z \in H$  に対して、 $x, y, z \in G$  で、 $G$  は群だから、 $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ .
- b-3-2) 任意の  $x \in H$  に対して、 $x \in G$  で、 $G$  は群だから、 $x \cdot e = e \cdot x = x$ .  
ところが、(2)から、 $e \in H$ . ゆえに、 $H$  の単位元が存在する。
- b-3-3) 任意の  $x \in H$  に対して、 $x \in G$ .  
 $G$  は群だから、 $x^{-1} \in G$  が存在して、 $x \cdot x^{-1} = x^{-1} \cdot x = e$ .  
ところが、(3)から、 $x^{-1} \in H$ . ゆえに、 $H$  に  $x$  の逆元が存在する。  
以上から、 $(H, \cdot)$  は  $(G, \cdot)$  の部分群である。

9

### 系

- $(H, \cdot)$  が群  $(G, \cdot, e)$  の部分群であるとき、かつそのときに限り、次の(1)~(3)が成り立つ。
- (1)  $H \subseteq G$ .
- (2)  $H \neq \emptyset$ .
- (3) 任意の  $x, y \in H$  に対して、 $x \cdot y^{-1} \in H$ .



10

### 証明

- $(H, \cdot)$  が群  $(G, \cdot, e)$  の部分群であるとき、かつそのときに限り、次の(1)~(3)が成り立つ。
- (1)  $H \subseteq G$ . (2)  $H \neq \emptyset$ . (3) 任意の  $x, y \in H$  に対して、 $x \cdot y^{-1} \in H$ .
- 前の定理により、「次の i)~iv) が成り立つとき、かつそのときに限り、(1)~(3)が成り立つ」を示す。
    - i)  $H \subseteq G$ . ii)  $e \in H$ . iii) 任意の  $x \in H$  に対して、 $x^{-1} \in H$ .
    - iv) 任意の  $x, y \in H$  に対して、 $x \cdot y \in H$ .
  - a) 「i)~iv) が成り立つならば、(1)~(3)が成り立つ」を示す。
  - b) 「(1)~(3)が成り立つならば、i)~iv) が成り立つ」を示す。
- 
- a) i)~iv) が成り立つとする。
- (1) i)から明らか。
- (2) ii)から明らか。
- (3) iii)から、任意の  $y \in H$  に対して、 $y^{-1} \in H$ .  
ゆえに、iv)から、任意の  $x \in H$  とこの  $y^{-1} \in H$  に対して、 $x \cdot y^{-1} \in H$ .

11

### 証明(続き)

- $(H, \cdot)$  が群  $(G, \cdot, e)$  の部分群であるとき、かつそのときに限り、次の(1)~(3)が成り立つ。
- (1)  $H \subseteq G$ . (2)  $H \neq \emptyset$ . (3) 任意の  $x, y \in H$  に対して、 $x \cdot y^{-1} \in H$ .
- 前の定理により、「次の i)~iv) が成り立つとき、かつそのときに限り、(1)~(3)が成り立つ」を示す。
    - i)  $H \subseteq G$ . ii)  $e \in H$ . iii) 任意の  $x \in H$  に対して、 $x^{-1} \in H$ .
    - iv) 任意の  $x, y \in H$  に対して、 $x \cdot y \in H$ .
  - b) 「(1)~(3)が成り立つならば、i)~iv) が成り立つ」を示す。
- 
- b) (1)~(3)が成り立つとする。
- i) (1)から明らか。
- ii) (2)から、ある  $a \in H$  が存在する。このとき、(3)から、 $a \cdot a^{-1} = e \in H$ .
- iii)  $e \in H$  と任意の  $x \in H$  に対して、(3)から、 $e \cdot x^{-1} = x^{-1} \in H$ .
- iv) iii)から、任意の  $y \in H$  に対して、 $y^{-1} \in H$ .  
ゆえに、任意の  $x, y \in H$  に対して、(3)から、 $x \cdot (y^{-1})^{-1} = x \cdot y \in H$ .

12

## 定理

次の(1), (2)が成り立つならば,  $(H, \cdot)$ は群 $(G, \cdot)$ の部分群である.

- (1)  $H$ は $G$ の空でない有限部分集合である.
- (2) 任意の $x, y \in H$ に対して,  $x \cdot y \in H$ .

13

## 証明

次の(1), (2)が成り立つならば,  $(H, \cdot)$ は群 $(G, \cdot)$ の部分群である.

- (1)  $H$ は $G$ の空でない有限部分集合である.
- (2) 任意の $x, y \in H$ に対して,  $x \cdot y \in H$ .
  - 前の定理により, 次のi)~iv)が成り立つことを示す.
    - i)  $H \subseteq G$ , ii)  $e \in H$ , iii) 任意の $x \in H$ に対して,  $x^{-1} \in H$ .
    - iv) 任意の $x, y \in H$ に対して,  $x \cdot y \in H$ .

(1), (2)が成り立つとする.

- i) (1)から明らか.
- ii, iii) 任意の $x \in H$ に対して,  $x \cdot x = x^2 \in H, x \cdot x^2 = x^3 \in H, x \cdot x^3 = x^4 \in H, \dots$   
 $H$ は有限だから, すべての $x^i \in H$  ( $i > 0$ )が異なることはない.  
 すなわち, ある $m, n \in \mathbb{N}$  ( $m > n$ )が存在して,  $x^m = x^n$ .  
 ゆえに,  $x^m \cdot x^{-n} = x^m \cdot x^{-n} = e$ だから,  $e = x^{m-n} \in H$ .  
 さらに,  $e = x \cdot x^{m-n-1}$ だから,  $x^{-1} = x^{m-n-1} \in H$ .
- iv) (2)から明らか.

14

## 定理

$(S, +, \cdot)$ が環 $(R, +, \cdot, c, e)$ の部分環であるとき, かつそのときに限り, 次の(1)~(5)が成り立つ.

- (1)  $S \subseteq R$ .
- (2)  $c \in S$ .
- (3)  $e \in S$ .
- (4) 任意の $x, y \in S$ に対して,  $x + (-y) \in S$ .
- (5) 任意の $x, y \in S$ に対して,  $x \cdot y \in S$ .

- $(R, +)$ は群(加法群)である.
  - (2), (3)から,  $S \neq \emptyset$ .
  - (1), (2), (4) iff  $(S, +)$ は $(R, +)$ の部分群 (定理)

15

## 証明

$(S, +, \cdot)$ が環 $(R, +, \cdot, c, e)$ の部分環であるとき, かつそのときに限り, 次の(1)~(5)が成り立つ.

- (1)  $S \subseteq R$ . (2)  $c \in S$ . (3)  $e \in S$ .
- (4) 任意の $x, y \in S$ に対して,  $x + (-y) \in S$ .
- (5) 任意の $x, y \in S$ に対して,  $x \cdot y \in S$ .
  - a) 「 $(S, +, \cdot)$ が $(R, +, \cdot)$ の部分環ならば, (1)~(5)を示す.
  - b) 「(1)~(5)ならば,  $(S, +, \cdot)$ は $(R, +, \cdot)$ の部分環」を示す.

a)  $(S, +, \cdot)$ は $(R, +, \cdot)$ の部分環であるとする.

- (1), (2), (4) このとき,  $(S, +)$ は $(R, +)$ の部分群である.  
 ゆえに, 前の定理の系から, (1), (2), (4)が成り立つ.
- (3)  $S$ は環だから, 乗法の単位元 $e' \in S$ が存在する.  
 このとき, 任意の $x \in S$ に対して,  $x \cdot e' = e' \cdot x = x$ .  
 ところが,  $x, e' \in S \subseteq R$ だから,  $e'$ は $R$ における乗法の単位元でもある.  
 環における乗法の単位元は唯一だから,  $e = e' \in S$ .
- (5)  $(S, +, \cdot)$ は環だから, 明らかに, (5)が成り立つ.

16

## 証明(続き)

$(S, +, \cdot)$ が環 $(R, +, \cdot, c, e)$ の部分環であるとき, かつそのときに限り, 次の(1)~(5)が成り立つ.

- (1)  $S \subseteq R$ . (2)  $c \in S$ . (3)  $e \in S$ .
- (4) 任意の $x, y \in S$ に対して,  $x + (-y) \in S$ .
- (5) 任意の $x, y \in S$ に対して,  $x \cdot y \in S$ .
  - b) 「(1)~(5)ならば,  $(S, +, \cdot)$ は $(R, +, \cdot)$ の部分環」を示す.
    - b-1)  $S \subseteq R$ を示す.
    - b-2) 「 $S$ は乗法に関して閉じている」を示す.
    - b-3) 「 $S$ は加法に関して閉じている」と  
 「 $(S, +, \cdot)$ は環の公理を満たす」を示す.

b) (1)~(5)が成り立つと仮定する.

- b-1) (1)から,  $S \subseteq R$ .
- b-2) (5)から,  $S$ は乗法に関して閉じている.

17

## 証明(続き2)

$(S, +, \cdot)$ が環 $(R, +, \cdot, c, e)$ の部分環であるとき, かつそのときに限り, 次の(1)~(5)が成り立つ.

- (1)  $S \subseteq R$ . (2)  $c \in S$ . (3)  $e \in S$ .
- (4) 任意の $x, y \in S$ に対して,  $x + (-y) \in S$ .
- (5) 任意の $x, y \in S$ に対して,  $x \cdot y \in S$ .
  - b) 「(1)~(5)ならば,  $(S, +, \cdot)$ は $(R, +, \cdot)$ の部分環」を示す.
    - b-3) 「 $S$ は加法に関して閉じている」と  
 「 $(S, +, \cdot)$ は環の公理を満たす」を示す.

b) (1)~(5)が成り立つと仮定する.

- b-3-1) (1), (2), (4)から,  $(S, +)$ は $(R, +)$ の部分群である.
- b-3-2) (3)から,  $e \in S \subseteq R$ .  
 任意の $x \in S$ に対して,  $x \in R$ .  
 $e$ は $R$ における乗法の単位元だから,  $x \cdot e = e \cdot x = x$ .  
 ゆえに,  $e$ は $S$ における乗法の単位元でもある.
- b-3-3) 任意の $x, y, z \in S$ に対して,  $x, y, z \in R$ だから, 加法の交換則, 乗法の結合則, 分配則が成り立つ.

18

### 定理

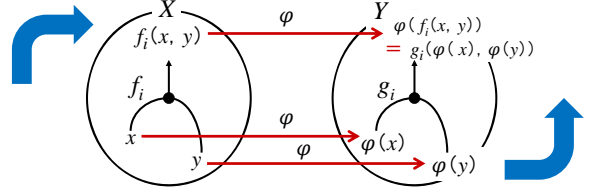
$(K, +, \cdot)$  が体  $(F, +, \cdot, c, e)$  の部分体であるとき、かつそのときに限り、次の (1) ~ (4) が成り立つ。

- (1)  $K \subseteq F$ .
  - (2)  $K \neq \emptyset$ .
  - (3) 任意の  $x, y \in K$  に対して、 $x + (-y) \in K$ .
  - (4) 任意の  $x, y \in K - \{c\}$  に対して、 $x \cdot y^{-1} \in K - \{c\}$ .
- (1), (2), (3) iff  $(K, +)$  は  $(F, +)$  の部分群
  - (1), (2), (4) iff  $(K - \{c\}, \cdot)$  は  $(F - \{c\}, \cdot)$  の部分群

19

### 準同型 (homomorphic)

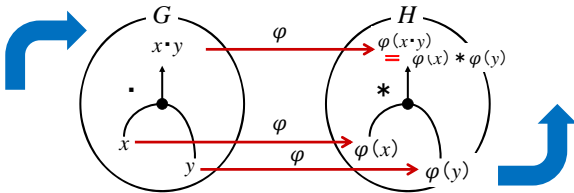
- 代数系  $(Y, g_1, g_2, \dots, g_n)$  は代数系  $(X, f_1, f_2, \dots, f_n)$  に準同型である
- 関数  $\varphi: X \rightarrow Y$  が存在して、次の性質が成り立つ。  
任意の  $x, y \in X$  と任意の  $i (i = 1, 2, \dots, n)$  に対して、  
$$\varphi(f_i(x, y)) = g_i(\varphi(x), \varphi(y))$$
- 関数  $\varphi: X$  から  $Y$  への準同型 (写像) (homomorphism)



20

### 群準同型

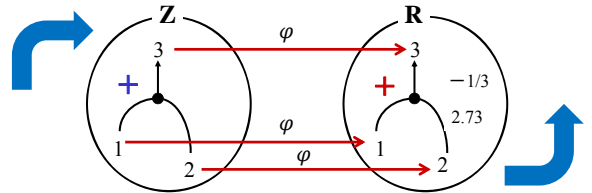
- 群  $(H, *)$  は群  $(G, \cdot)$  に (群) 準同型である
- 関数  $\varphi: G \rightarrow H$  が存在して、次の性質が成り立つ。  
任意の  $x, y \in G$  に対して、  
$$\varphi(x \cdot y) = \varphi(x) * \varphi(y)$$
- 関数  $\varphi: G$  から  $H$  への (群) 準同型写像



21

### 群準同型 (続き)

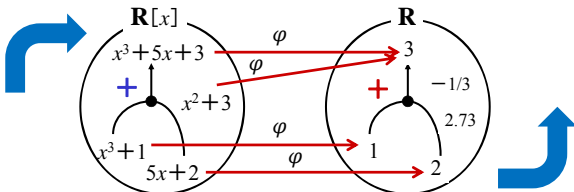
- 例: 群  $(\mathbf{R}, +)$  は群  $(\mathbf{Z}, +)$  に準同型である
- 準同型写像  $\varphi: \mathbf{Z} \rightarrow \mathbf{R}$   
任意の  $n \in \mathbf{Z}$  に対して、 $\varphi(n) = n$ .
  - 任意の  $x, y \in \mathbf{Z}$  に対して、  
$$\varphi(x + y) = x + y = \varphi(x) + \varphi(y)$$



22

### 群準同型 (続き2)

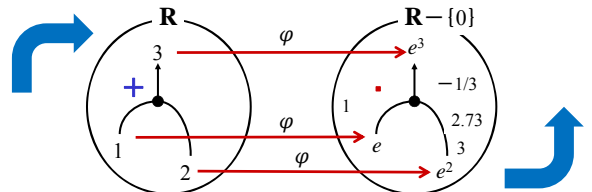
- 例: 群  $(\mathbf{R}, +)$  は群  $(\mathbf{R}[x], +)$  に準同型である
- 準同型写像  $\varphi: \mathbf{R}[x] \rightarrow \mathbf{R}$   
任意の  $P(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbf{R}[x]$  に対して、  
$$\varphi(P(x)) = a_0$$
  - 任意の  $P(x), Q(x) \in \mathbf{R}[x]$  に対して、  
$$\varphi(P(x) + Q(x)) = a_0 + b_0 = \varphi(P(x)) + \varphi(Q(x))$$



23

### 群準同型 (続き3)

- 例: 乗法群  $(\mathbf{R} - \{0\}, \cdot)$  は加法群  $(\mathbf{R}, +)$  に準同型である
- 準同型写像  $\varphi: \mathbf{R} \rightarrow \mathbf{R} - \{0\}$   
任意の  $x \in \mathbf{R}$  に対して、 $\varphi(x) = \exp(x)$
  - 任意の  $x, y \in \mathbf{R}$  に対して、  
$$\varphi(x + y) = \exp(x + y) = \exp(x) \cdot \exp(y) = \varphi(x) \cdot \varphi(y)$$



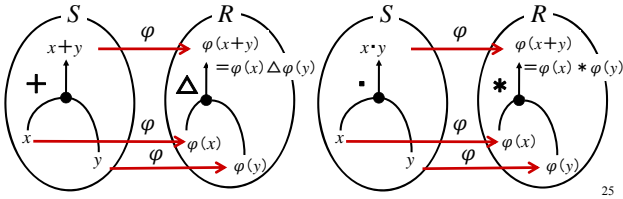
24

### 環準同型

- 環  $(R, \Delta, *)$  は環  $(S, +, \cdot)$  に(環)準同型である
- 関数  $\varphi : S \rightarrow R$  が存在して、次の性質が成り立つ。  
任意の  $x, y \in S$  に対して、  

$$\varphi(x+y) = \varphi(x) \Delta \varphi(y)$$

$$\varphi(x \cdot y) = \varphi(x) * \varphi(y)$$
- 関数  $\varphi \dots S$  から  $R$  への(環)準同型写像



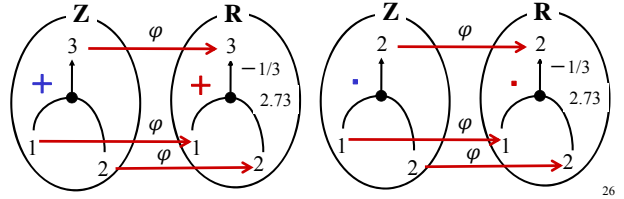
25

### 環準同型(続き)

- 例: 実数環  $(\mathbf{R}, +, \cdot)$  は整数環  $(\mathbf{Z}, +, \cdot)$  に準同型である
- 準同型写像  $\varphi : \mathbf{Z} \rightarrow \mathbf{R}$   
任意の  $n \in \mathbf{Z}$  に対して、 $\varphi(n) = n$ .
- 任意の  $x, y \in \mathbf{Z}$  に対して、  

$$\varphi(x+y) = \varphi(x) + \varphi(y),$$

$$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$$



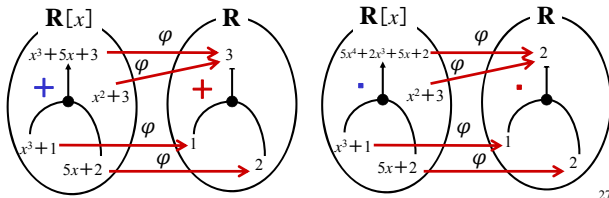
26

### 環準同型(続き2)

- 例: 実数環  $(\mathbf{R}, +, \cdot)$  は多項式環  $(\mathbf{R}[x], +, \cdot)$  に準同型である
- 準同型写像  $\varphi : \mathbf{R}[x] \rightarrow \mathbf{R}$   
任意の  $P(x) = a_n x^n + \dots + a_0 \in \mathbf{R}[x]$  に対して、 $\varphi(P(x)) = a_0$ .
- 任意の  $P(x), Q(x) \in \mathbf{R}[x]$  に対して、  

$$\varphi(P(x) + Q(x)) = \varphi(P(x)) + \varphi(Q(x)),$$

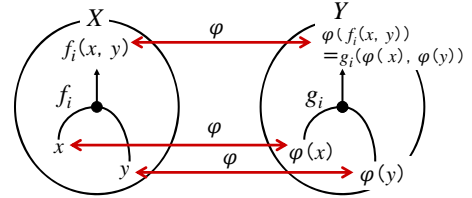
$$\varphi(P(x) \cdot Q(x)) = \varphi(P(x)) \cdot \varphi(Q(x))$$



27

### 同型(isomorphic)

- 代数系  $(X, f_1, f_2, \dots, f_n)$  と代数系  $(Y, g_1, g_2, \dots, g_n)$  は同型である  $\dots (X, f_1, f_2, \dots, f_n) \cong (Y, g_1, g_2, \dots, g_n)$
- 準同型  $\varphi : X \rightarrow Y$  が存在して、 $\varphi$  は全単射である
- 関数  $\varphi \dots X$  から  $Y$  への同型(写像)(isomorphism)
- $\varphi$  によって対応する要素を同一視すれば、 $X$  と  $Y$  は「同じもの」



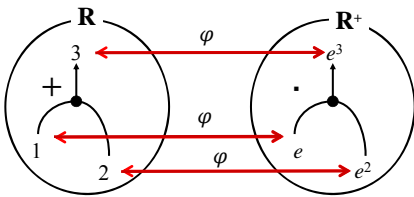
28

### 同型(続き)

- 例:  $\mathbf{R}^+ = \{x \in \mathbf{R} \mid x > 0\}$
- 乗法群  $(\mathbf{R}^+, \cdot)$  と加法群  $(\mathbf{R}, +)$  は同型
- 準同型写像  $\varphi : \mathbf{R} \rightarrow \mathbf{R}^+$   
任意の  $x \in \mathbf{R}$  に対して、 $\varphi(x) = \exp(x)$
- $\varphi$  は全単射
  - 任意の  $x_1, x_2 \in \mathbf{R}$  ( $x_1 \neq x_2$ ) に対して、 $\varphi(x_1) \neq \varphi(x_2)$ ,
  - 任意の  $y \in \mathbf{R}^+$  に対して、 $x = \log(y)$  とおくと、 $y = \varphi(x)$  ( $x \in \mathbf{R}$ )



計算尺



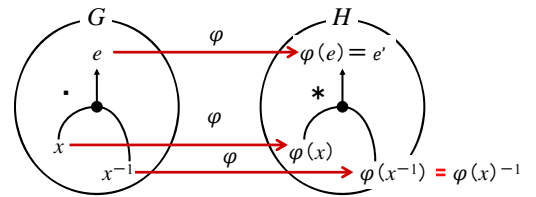
29

### 定理

群  $(G, \cdot, e)$ ,  $(H, *, e')$  と準同型  $\varphi : G \rightarrow H$  に対して、次の(1), (2)が成り立つ。

- $\varphi(e) = e'$
- 任意の  $x \in G$  に対して、 $\varphi(x^{-1}) = \varphi(x)^{-1}$

- 群準同型写像は単位元と逆元を保存する。



30

### 証明

群  $(G, \cdot, e)$ ,  $(H, *, e')$  と準同型  $\varphi: G \rightarrow H$  に対して,  
 (1)  $\varphi(e) = e'$

$\varphi$  は準同型だから, 任意の  $x, y \in G$  に対して,  
 $\varphi(x \cdot y) = \varphi(x) * \varphi(y)$ .  
 ここで,  $x = y = e$  とおくと,  $\varphi(e \cdot e) = \varphi(e) * \varphi(e)$ .  
 ゆえに,  $\varphi(e) = \varphi(e) * \varphi(e)$  だから,  
 $\varphi(e) * \varphi(e)^{-1} = (\varphi(e) * \varphi(e)) * \varphi(e)^{-1}$   
 $= \varphi(e) * (\varphi(e) * \varphi(e)^{-1})$  (結合則)  
 $= \varphi(e) * e'$  (逆元)  
 $= \varphi(e)$  (単位元)  
 一方,  $\varphi(e) * \varphi(e)^{-1} = e'$  だから,  $\varphi(e) = e'$ .

31

### 証明(続き)

群  $(G, \cdot, e)$ ,  $(H, *, e')$  と準同型  $\varphi: G \rightarrow H$  に対して,  
 (2) 任意の  $x \in G$  に対して,  $\varphi(x^{-1}) = \varphi(x)^{-1}$

$\varphi$  は準同型だから, 任意の  $x, y \in G$  に対して,  
 $\varphi(x \cdot y) = \varphi(x) * \varphi(y)$ .  
 ここで,  $y = x^{-1}$  とおくと,  $\varphi(x \cdot x^{-1}) = \varphi(x) * \varphi(x^{-1})$ .  
 ゆえに,  $\varphi(e) = \varphi(x) * \varphi(x^{-1})$  だから,  
 $\varphi(x)^{-1} * \varphi(e) = \varphi(x)^{-1} * (\varphi(x) * \varphi(x^{-1}))$   
 $= (\varphi(x)^{-1} * \varphi(x)) * \varphi(x^{-1})$  (結合則)  
 $= e' * \varphi(x^{-1})$  (逆元)  
 $= \varphi(x^{-1})$  (単位元)  
 一方, (1) から,  $\varphi(e) = e'$  だから,  
 $\varphi(x)^{-1} * \varphi(e) = \varphi(x)^{-1} * e' = \varphi(x)^{-1}$ .  
 ゆえに,  $\varphi(x^{-1}) = \varphi(x)^{-1}$ .

32

### 系

環  $(S, +, \cdot, c, e)$ ,  $(R, +, \cdot, c', e')$  と準同型  $\varphi: S \rightarrow R$  に対して,  
 次の (1), (2) が成り立つ.

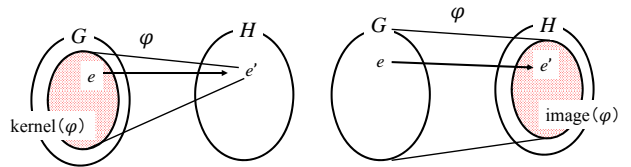
- (1)  $\varphi(c) = c'$
- (2) 任意の  $x \in S$  に対して,  $\varphi(-x) = -\varphi(x)$
- $(S, +, c)$ ,  $(R, +, c')$  は加法群だから, 明らか.
- 環準同型写像は加法の単位元と逆元を保存する.
  - 乗法の単位元を保存するとは限らない.

33

### 群準同型写像の核, 像

群  $(G, \cdot, e)$ ,  $(H, *, e')$  と準同型  $\varphi: G \rightarrow H$  に対して,

- $\varphi$  の核 (kernel)
  - $\text{kernel}(\varphi) = \{x \in G \mid \varphi(x) = e'\}$  (Ker  $\varphi$ )
- $\varphi$  の像 (image)
  - $\text{image}(\varphi) = \{\varphi(x) \mid x \in G\}$  (Im  $\varphi$ )

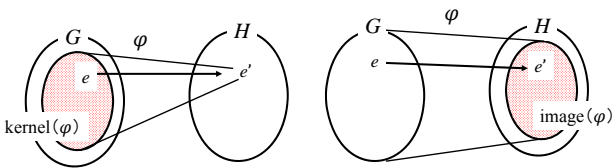


34

### 定理

群  $(G, \cdot, e)$ ,  $(H, *, e')$  と準同型  $\varphi: G \rightarrow H$  に対して,  
 次の (1), (2) が成り立つ.

- (1)  $(\text{kernel}(\varphi), \cdot)$  は  $G$  の部分群である.
- (2)  $(\text{image}(\varphi), *)$  は  $H$  の部分群である.



35

### 証明

群  $(G, \cdot, e)$ ,  $(H, *, e')$  と準同型  $\varphi: G \rightarrow H$  に対して,

- (1)  $(\text{kernel}(\varphi), \cdot)$  は  $G$  の部分群である.
  - 前の定理により, 次の (a) ~ (d) を示す.
    - (a)  $\text{kernel}(\varphi) \subseteq G$ . (b)  $e \in \text{kernel}(\varphi)$ .
    - (c) 任意の  $x \in \text{kernel}(\varphi)$  に対して,  $x^{-1} \in \text{kernel}(\varphi)$ .
    - (d) 任意の  $x, y \in \text{kernel}(\varphi)$  に対して,  $x \cdot y \in \text{kernel}(\varphi)$ .
- (a)  $\text{kernel}(\varphi)$  の定義から明らかに,  $\text{kernel}(\varphi) \subseteq G$ .
- (b) 群準同型は単位元を保存するから,  $\varphi(e) = e'$ . ゆえに,  $e \in \text{kernel}(\varphi)$ .
- (c) 任意の  $x \in \text{kernel}(\varphi)$  に対して,  $\varphi(x) = e'$  だから,  
 $\varphi(x^{-1}) = e' * \varphi(x^{-1}) = \varphi(x) * \varphi(x^{-1})$ .  
 $\varphi$  は準同型だから,  $\varphi(x) * \varphi(x^{-1}) = \varphi(x \cdot x^{-1}) = \varphi(e) = e'$ .  
 ゆえに,  $\varphi(x^{-1}) = e'$  だから,  $x^{-1} \in \text{kernel}(\varphi)$ .
- (d) 任意の  $x, y \in \text{kernel}(\varphi)$  に対して,  $\varphi$  は準同型だから,  
 $\varphi(x \cdot y) = \varphi(x) * \varphi(y) = e' * e' = e'$ . ゆえに,  $x \cdot y \in \text{kernel}(\varphi)$ .  
 以上から,  $(\text{kernel}(\varphi), \cdot)$  は  $G$  の部分群である.

36

## 証明(続き)

群  $(G, \cdot, e)$ ,  $(H, *, e')$  と準同型  $\varphi : G \rightarrow H$  に対して,

(2)  $(\text{image}(\varphi), *)$  は  $H$  の部分群である.

- 前の定理により, 次の (a) ~ (d) を示す.
  - (a)  $\text{image}(\varphi) \subseteq H$ .      (b)  $e' \in \text{image}(\varphi)$ .
  - (c) 任意の  $x' \in \text{image}(\varphi)$  に対して,  $x'^{-1} \in \text{image}(\varphi)$ .
  - (d) 任意の  $x', y' \in \text{image}(\varphi)$  に対して,  $x' * y' \in \text{image}(\varphi)$ .

- (a) 明らかに,  $\text{image}(\varphi) \subseteq H$ .
- (b) 群準同型は単位元を保存するから,  $\varphi(e) = e'$ . ゆえに,  $e' \in \text{image}(\varphi)$ .
- (c) 任意の  $x' \in \text{image}(\varphi)$  に対して,  $x \in G$  が存在して,  $x' = \varphi(x)$ .  
ゆえに,  $x'^{-1} = \varphi(x)^{-1}$ .  
ところで, 群準同型は逆元を保存するから,  $\varphi(x)^{-1} = \varphi(x^{-1})$ .  
ゆえに,  $x'^{-1} = \varphi(x^{-1})$ .  
 $x^{-1} \in G$  だから,  $\varphi(x^{-1}) \in \text{image}(\varphi)$ .  
ゆえに,  $x'^{-1} \in \text{image}(\varphi)$ .

37

## 証明(続き2)

群  $(G, \cdot, e)$ ,  $(H, *, e')$  と準同型  $\varphi : G \rightarrow H$  に対して,

(2)  $(\text{image}(\varphi), *)$  は  $H$  の部分群である.

- 前の定理により, 次の (a) ~ (d) を示す.
  - (a)  $\text{image}(\varphi) \subseteq H$ .      (b)  $e' \in \text{image}(\varphi)$ .
  - (c) 任意の  $x' \in \text{image}(\varphi)$  に対して,  $(x')^{-1} \in \text{image}(\varphi)$ .
  - (d) 任意の  $x', y' \in \text{image}(\varphi)$  に対して,  $x' * y' \in \text{image}(\varphi)$ .

- (d) 任意の  $x', y' \in \text{image}(\varphi)$  に対して,  $x, y \in G$  が存在して,  
 $x' = \varphi(x)$ ,  $y' = \varphi(y)$ .  
 $\varphi$  は準同型だから,  $x' * y' = \varphi(x) * \varphi(y) = \varphi(x \cdot y)$ .  
 $x \cdot y \in G$  だから,  $\varphi(x \cdot y) \in \text{image}(\varphi)$ .  
すなわち,  $x' * y' \in \text{image}(\varphi)$ .  
以上から,  $(\text{image}(\varphi), *)$  は  $H$  の部分群である.

38

## まとめ

- 今日の講義
  - 部分系, 準同型
- 次回の講義
  - 商系(教科書 pp.165-168)
- 今日の演習
  - 部分系, 準同型

39