部分系, 準同型
(教科書 pp.164-165, 170-173)

教科書…野崎昭弘: 離散系の数学, 近代科学社

部分系 (subsystem)
代数系 $(X, f_1, \ldots, f_n)$ は代数系 $(Y, g_1, \ldots, g_n)$ の
部分系である
次の(1), (2)が成り立つ.
(1) $X \subseteq Y$
(2) $(X, f_1, \ldots, f_n)$ と $(Y, g_1, \ldots, g_n)$ は同じ公理を満たす.

群 (group)
群 $(G, \cdot)$ 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 (continued)
例:
整数環 $\mathbb{Z}$ は実数環 $\mathbb{R}$ の部分環
実数体 $\mathbb{R}$ は複素数体 $\mathbb{C}$ 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

$(G, +, \cdot, c, e)$ に対して,
群 $(G, +, \cdot, c, e)$, $(c, +, \cdot, c, e)$ は部分群である ...
自明な部分群

群 (continued)
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)

定理
$(H, \cdot) \subseteq (G, \cdot, e)$ 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) $G$ の単位元は $H$ の単位元である．
(3) $G$ における逆元は $H$ における逆元でもある．
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) \( H \subseteq G \)。（H は G の部分群）
(2) \( e \in H \)。（H が単位元を含む）
(3) 任意の \( x, y \in H \) に対して，\( x^{-1} \in H \)。（逆元が存在する）
(4) 任意の \( x, y \in H \) に対して，\( x \cdot y \in H \)。（演算が閉じている）

a) \( (H, \cdot) \) は \((G, \cdot, e) \) の部分群であるとする。
(1) 部分群の定義からの明らかに，\( H \subseteq G \)。
(2) \( H \) は群だから，単位元 \( e \in H \) が存在する。
しかし，ある \( x \in H \) に対して，\( x \cdot x = e \) が成り立つことはない。
(3) 任意の \( x, y \in H \) 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) が成り立つと仮定する。
b-1) \( (1) \) から，\( H \subseteq G \)。
b-2) \( (2) \) から，\( e \in H \)。
b-3) \( (3) \) から，\( x^{-1} \in H \)。
b-4) \( (4) \) から，\( x \cdot y \in H \)。

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) \( H \subseteq G \)。（H は G の部分群）
(2) \( H \neq \emptyset \)。（H が空ではない）
(3) 任意の \( x, y \in H \) に対して，\( x \cdot y^{-1} \in H \)。（逆元が存在する）

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。

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) \( H \subseteq G \)。（H は G の部分群）
(2) \( e \in H \)。（H が単位元を含む）
(3) 任意の \( x, y \in H \) に対して，\( x \cdot y \in H \)。（演算が閉じている）
(4) 任意の \( x, y \in H \) に対して，\( x \cdot y \in H \)。

a) \( (1) \)～(4) が成り立つとする。
a-1) \( (1) \) から明らか。
a-2) \( (2) \) から，\( e \in H \)。
a-3) \( (3) \) から，\( y \in H \)。
a-4) \( (4) \) から，\( x \cdot y \in H \)。

b) \( (1) \)～(4) が成り立つと仮定する。
b-1) \( (1) \) から，\( H \subseteq G \)。
b-2) \( (2) \) から，\( e \in H \)。
b-3) \( (3) \) から，\( x \cdot y \in H \)。
b-4) \( (4) \) から，\( x \cdot y \in H \)。
定理
次の(i),(ii)が成り立つならば, \((H, \cdot)\)は群 \((G, \cdot)\)の部分群である。
(i) \(H\) は \(G\) の空でない有限部分集合である。
(ii) 任意の \(x, y \in H\) に対して, \(x \cdot y \in H\).

証明
次の(i),(ii)が成り立つならば, \((H, \cdot)\)は群 \((G, \cdot)\)の部分群である。
(i) \(H\) は \(G\) の空でない有限部分集合である。
(ii) 任意の \(x, y \in H\) に対して, \(x \cdot y \in H\).
定理

群準同型（続き2）

例：群（R, +）は群（R[x], +）に準同型である

準同型写像 φ: R[x] → R

任意の P(x) = a_n x^n + ... + a_1 x + a_0 ∈ R[x] に対して,
φ(P(x)) = a_n.

任意の P(x), Q(x) ∈ R[x] に対して,
φ(P(x) + Q(x)) = φ(P(x)) + φ(Q(x)).

群準同型（続き3）

例：乗法群（R, 0）は加法群（R, +）に準同型である

準同型写像 φ: R → R − [0]

任意の x ∈ R に対して, φ(x) = exp(x).

任意の x, y ∈ R に対して,
φ(x + y) = exp(x + y) = exp(x) · exp(y) = φ(x) · φ(y).
環準同型

- 実数環 \( \mathbb{R} \) は多項式環 \( \mathbb{R}[x] \) に準同型である
  - 準同型写像 \( \phi : \mathbb{R}[x] \rightarrow \mathbb{R} \)
  - 任意の \( P(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{R}[x] \)に対して, \( \phi(P(x)) = a_0 \).
  - 任意の \( P(x), Q(x) \in \mathbb{R}[x] \)に対して, \( \phi(P(x) + Q(x)) = \phi(P(x)) + \phi(Q(x)) \)
  - \( \phi(P(x) \cdot Q(x)) = \phi(P(x)) \cdot \phi(Q(x)) \)

同型 (isomorphic)

- 代数系 \((X, f_1, \ldots, f_n)\) と代数系 \((Y, g_1, \ldots, g_n)\) は同型である
  - \((X, f_1, \ldots, f_n) \cong (Y, g_1, \ldots, g_n)\)
  - 準同型 \( \varphi : X \rightarrow Y \) が存在して, \( \varphi \) は全単射である
  - 関数 \( \varphi \) が \( X \rightarrow Y \) 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」

定理

- 群 \((G, \cdot, e)\), \((H, \ast, e')\) と準同型 \( \varphi : G \rightarrow H \) に対して,
  - 群の (1), (2) が成り立つ.
  - \((1)\) \( \varphi(e) = e' \)
  - \((2)\) 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
証明

群 (G, *, e) と準同型 φ : G → H に対して、
(1) φ(e) = e'
φは準同型だから、任意の x, y ∈ G に対して、
φ(x * y) = φ(x) * φ(y).
ここで、x * y = e とおくと、φ(e * e) = φ(e) * φ(e).
ゆえに、φ(e) = φ(e) * φ(e) だから、
φ(e) * φ(e) = (φ(e) * φ(e)) * φ(e) (結合法則)
= φ(e) * φ(e) * φ(e) (逆元)
= φ(e) * e' (単位元)
一方、φ(e) * φ(e) = e' だから、φ(e) = e'.

証明（続き）

群 (G, *, e) と準同型 φ : G → H に対して、
(2) 任意の x ∈ G に対して、φ(x⁻¹) = φ(x)⁻¹.
φは準同型だから、任意の x, y ∈ G に対して、
φ(x * y) = φ(x) * φ(y).
ここで、y = x⁻¹ とおくと、φ(x * x⁻¹) = φ(x) * φ(x⁻¹).
ゆえに、φ(x) = φ(x) * φ(x⁻¹) だから、
φ(x)⁻¹ * φ(x) = φ(x⁻¹) * φ(x) (結合則)
e * φ(x)⁻¹ = φ(x⁻¹) (逆元)
φ(x)⁻¹ = φ(x⁻¹) (単位元)
一方、(1) から、φ(e) = e' だから、
φ(x)⁻¹ * φ(x) = φ(x)⁻¹ * e' = φ(x⁻¹).
ゆえに、φ(x⁻¹) = φ(x⁻¹).
証明（続き）
群 \((G, \cdot, e), (H, \ast, e')\) と準同型 \(\varphi : G \to H\) に対して。
(2) \((\text{image}\varphi, \ast)\) 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、\(x'^{\large{-1}} \in \text{image}\varphi\).
  (d) 任意の \(x', y' \in \text{image}\varphi\) に対して、\(x' \ast y' \in \text{image}\varphi\).

(a) 明らかに、\(\text{image}\varphi \subseteq H\).
(b) 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、\(x'^{\large{-1}} = \varphi(x^{\large{-1}})\).
  ところで、準同型は逆元を保存するから、\(\varphi(x)^{\large{-1}} = \varphi(x^{\large{-1}})\).
  ゆえに、\(x'^{\large{-1}} \in \text{image}\varphi\).
  すなわち、\(x' \in G\) だから、\(\varphi(x)^{\large{-1}} \in \text{image}\varphi\).
  ゆえに、\(x'^{\large{-1}} \in \text{image}\varphi\).

まとめ
- 今日の講義
  - 部分系、準同型
- 次回の講義（2限）
  - 商系（教科書 pp.165-168）
- 今日の演習
  - なし

証明（続き2）
群 \((G, \cdot, e), (H, \ast, e')\) と準同型 \(\varphi : G \to H\) に対して。
(2) \((\text{image}\varphi, \ast)\) 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、\(x'^{\large{-1}} \in \text{image}\varphi\).
  (d) 任意の \(x', y' \in \text{image}\varphi\) に対して、\(x' \ast y' \in \text{image}\varphi\).

(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、\(x' \ast y' = \varphi(x) \ast \varphi(y) = \varphi(x \ast y)\).
  すなわち、\(x' \ast y' \in \text{image}\varphi\).
  以上から、\((\text{image}\varphi, \ast)\) は \(H\) の部分群である。