

定義 (同値関係)(教科書 p.112, 参考書 p.27). 集合 X の 2 つの元の間に定義された関係 $\sim$ が, 次の 3 つの条件を満たすとき, この関係 $\sim$ を**同値関係**という. ($\leftarrow$ 参考書では aRb という記号)

- (1) **反射律** $a \sim a \quad (\forall a \in X),$
- (2) **対称律** $a \sim b \implies b \sim a \quad (\forall a, b \in X),$
- (3) **推移律** $a \sim b \text{ かつ } b \sim c \implies a \sim c \quad (\forall a, b, c \in X).$

定義 (同値類). 同値関係 $\sim$ が定義された集合 X の各元 $a \in X$ に対して, $C(a) := \{x \in X \mid a \sim x\}$ を a を含む**同値類**といい, $\bar{a}$ または $[a]$ とも表す. 同値類 $C(a)$ の 1 つの元 $x \in C(a)$ をとって, x は $C(a)$ の**代表元**という. ($\leftarrow a$ は $C(a)$ の代表元の 1 つである)

定義 (類別; クラス分け). 集合 X に対し, 次の 3 条件を満たす X の部分集合 $C_i, (i \in I)$ の集まりを X の**類別**または**クラス分け**という:

- (1) $C_i \neq \emptyset,$
- (2) $X = \bigcup_{i \in I} C_i,$
- (3) $C_i \neq C_j \implies C_i \cap C_j = \emptyset.$

定理. 集合 X に同値関係 $\sim$ を定めると, 同値類 $C(a)$ によって X の類別が得られる. 逆に, X の類別が与えられると, 「 $a \sim b \iff a$ と b は同じ類」によって, X に同値関係が定義できる.

⊙ 反射律から $a \in C(a)$ であり, $C(a) \neq \emptyset$. $a \sim b$ を仮定すれば, 対称律から $b \sim a$ であり, $x \in X$ に対して, 推移律より $a \sim x \iff b \sim x$ が分かる. これは, $C(a) = C(b)$ を表わしている. また, $a \not\sim b$ を仮定して, $c \in C(a) \cap C(b)$ とすれば, $a \sim c$ かつ $b \sim c$ であり, 対称律, 推移律より $a \sim b$ となり仮定に反する. よって, $C(a) \cap C(b) = \emptyset$ であることが分かる.

定義 (商集合). X の同値類の集まりを, X の同値関係 $\sim$ による**商集合**といい,

$$X/\sim := \{C(a) \mid a \in X\} = \{\bar{a} \mid a \in X\} = \{[a] \mid a \in X\} \quad \text{と表す.}$$

- ここで, 法 m の世界のことを思い出す (p. 14 参照).

法 m に関して合同. $m \in \mathbb{N}$ とする. 整数 $a, b \in \mathbb{Z}$ が法 m に関して合同 (congruent) であるとは, $a - b$ が m で割り切れることと定義し, $a \equiv b \pmod{m}$ とかく. すなわち,

$$a \equiv b \pmod{m} \iff m \mid a - b.$$

命題 [1]. $\mathbb{Z}$ における, 法 m に関して合同という関係 ($\equiv$) は, 同値関係である.

例 (法 m に関する剰余類). $\mathbb{Z}$ の 2 つの元 $a, b \in \mathbb{Z}$ に定義された, 法 m に関して合同 $a \equiv b \pmod{m}$ という同値関係 $\equiv$ による $\mathbb{Z}$ の類別を考える. いま,

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

と書けば, $a + m\mathbb{Z} = \bar{a} = [a]$ であり, 合同 $\equiv$ による類別は

$$\begin{array}{lll} m = 2; & \mathbb{Z} = 2\mathbb{Z} \cup (1 + 2\mathbb{Z}), & \mathbb{Z} = \bar{0} \cup \bar{1}, \\ m = 3; & \mathbb{Z} = 3\mathbb{Z} \cup (1 + 3\mathbb{Z}) + (2 + 3\mathbb{Z}), & \mathbb{Z} = \bar{0} \cup \bar{1} \cup \bar{2}, \\ m = 4; & \mathbb{Z} = 4\mathbb{Z} \cup (1 + 4\mathbb{Z}) + (2 + 4\mathbb{Z}) + (3 + 4\mathbb{Z}), & \mathbb{Z} = \bar{0} \cup \bar{1} \cup \bar{2} \cup \bar{3} \end{array}$$

のように与えられる. この法 m に関して合同という同値関係 $\equiv$ による商集合 $\mathbb{Z}/\equiv$ ($\leftarrow \mathbb{Z}/\sim$ のこと) を $\mathbb{Z}/m\mathbb{Z}$ とかく. すなわち,

$$\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\} = \{[0], [1], \dots, [m-1]\}$$

である. この場合の各類は**法 m に関する剰余類**とも呼ばれる. また, 各剰余類から代表元を 1 つずつとって作った集合を**完全代表系**という. たとえば, $\{0, 1, \dots, m-1\}$ や $\{-2, -1, 0, \dots, m-3\}$ は完全代表系である. 特に, $\mathbb{Z}/m\mathbb{Z}$ と $\{0, 1, \dots, m-1\}$ は 1 対 1 に対応している.

例 [2](共役類)．群 G の元 $a, b \in G$ に対して,

$$a \sim b \iff b = \tau a \tau^{-1} \quad (\exists \tau \in G)$$

とすれば, $\sim$ は同値関係となる．このとき, $\sim$ による同値類を**共役類**といい, a と b は**共役**という．

定義 (不変量)． X, Y を集合, $\sim$ を X 上の同値関係とする．このとき, 写像 $\pi: X \rightarrow Y$ が, 任意の $x, y \in X$ に対して, $x \sim y \Rightarrow \pi(x) = \pi(y)$ をみたすとき, π を $\sim$ に関する**不変量**と呼ぶ．

補題．巡回置換 $\sigma = (i_1 \cdots i_k) \in S_n$ と $\tau = \begin{pmatrix} i_1 & i_2 & \cdots & i_k \\ j_1 & j_2 & \cdots & j_k \end{pmatrix} \in S_n$ に対して,

$$\tau \sigma \tau^{-1} = (\tau(i_1) \tau(i_2) \cdots \tau(i_k)) = (j_1 j_2 \cdots j_k). \quad (\leftarrow \sigma \text{ の中身を } \tau \text{ で動かしたもの})$$

定理 (S_n の共役な元)． $\sigma, \sigma' \in S_n$ に対して,

σ と σ' は共役 $\iff \sigma$ と σ' のサイクル分解は同じ形． $(\leftarrow \text{サイクル分解は p.4 参照})$

$\odot \sigma = (i_1 \cdots i_k) \cdots (l_1 \cdots l_s)$ とする．

$(\implies) \sigma' = \tau \sigma \tau^{-1}$ のとき, $\sigma' = (\tau(i_1) \cdots \tau(i_k)) \cdots (\tau(l_1) \cdots \tau(l_s))$ は σ と同じ形のサイクル分解．

$(\impliedby) \sigma' = (i'_1 \cdots i'_k) \cdots (l'_1 \cdots l'_s)$ と $\tau = \begin{pmatrix} i_1 & \cdots & i_k & \cdots & l_1 & \cdots & l_s \\ i'_1 & \cdots & i'_k & \cdots & l'_1 & \cdots & l'_s \end{pmatrix}$ に対して, $\sigma' = \tau \sigma \tau^{-1}$ ．

$(\leftarrow \text{サイクル分解の形 (型という) が不変量の役割を果たしている (!)})$

例 (S_3, S_4 の共役類)． $\bullet S_3$ の共役類による類別は,

$$S_3 = \{1\} \cup \{(12), (13), (23)\} \cup \{(123), (132)\} = \{1\} \cup [(12)] \cup [(123)].$$

それぞれの共役類の位数を等式で表わしてみると (**類等式**という), $6 = 1 + 3 + 2$ となる．

$\bullet S_4$ の共役類による類別は,

$$S_4 = \{1\} \cup [(12)] \cup [(123)] \cup [(12)(34)] \cup [(1234)]$$

であり, 類等式は $24 = 1 + 6 + 8 + 3 + 6$. $(\leftarrow 1$ つの類に多くの元が入っている事と群の非可換性の強さには関係がある事を群論で学ぶ, 定義から可換群の各共役類には1つの元しか入っていない)

例 ($GL_n(\mathbb{R})$ の共役類)．群 $G = GL_n(\mathbb{R})$ での共役を考える．

例えば, $A = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}$ と $B = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \in G$ は共役である．実際, $P = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ に対して, $P^{-1}AP = B$ を満たしている． $(\leftarrow Q := P^{-1}$ が存在して $Q A Q^{-1} = B$ でもある)

補題 [3]．行列 $A, B \in M_n(\mathbb{R})$ に対して, (1) $\det(AB) = \det(A) \det(B)$, (2) $\text{tr}(AB) = \text{tr}(BA)$ ．

命題 [4]．以下は相似 ($\sim$) に関する不変量である:

(1) $\det: GL_n(\mathbb{R}) \rightarrow \mathbb{R}, A \mapsto \det(A)$, (2) $\text{tr}: GL_n(\mathbb{R}) \rightarrow \mathbb{R}, A \mapsto \text{tr}(A)$ ．

$\odot$ 補題 [3] より, $\det(P^{-1}AP) = \det(P^{-1}) \det(A) \det(P) = \frac{1}{\det(P)} \det(A) \det(P) = \det(A)$,

$\text{tr}(P^{-1}AP) = \text{tr}((P^{-1}A)P) = \text{tr}(P(P^{-1}A)) = \text{tr}((PP^{-1})A) = \text{tr}(A)$. $(\leftarrow \text{補題 [3] と結合法則})$

例．次の行列 A, B は相似ではない．すなわち, $P^{-1}AP = B$ なる正則行列 P は存在しない:

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}. \quad (\leftarrow \det A = 1 \neq \det B = 2, \text{あるいは } \text{tr} A = 2 \neq \text{tr} B = 3 \text{ より})$$

$A \sim B$ のとき, 行列 A と B は**相似**ともいい, A が対角行列と相似のとき**対角化可能**という．
 $(\leftarrow \text{対角化可能 (共役類に対角行列が入っている) か, 対角化できない場合の代表元としてどのような (対角行列に近い) ものが取れるか (ジョルダン標準形) は, (基底変換に関連する) 線形代数の主題の1つである. しかし, 不変量 } \det \text{ と } \text{tr} \text{ だけでは判定できない (不十分である)})$