代数学 I 第 8 回講義資料

担当：大矢 浩徳 (OYA Hironori)*

今回は大学で学ぶ数学において非常に重要な「同値関係による商集合」という概念を学ぶ．これまでは群と部分群の例を多数見てきたが，部分群を用いると，群自身に**同値関係**を入れることができる．これは，いわば群の元をいくつかの「クラス」に分けるというようなものである．実はこれが群の構造を調べる際に非常に手段となる．この考え方を導入すると，ほんの一例ではあるが例えば次のようなことがわかるようになる．

- 位数が $n(<\infty)$ の群 G の部分群の位数は必ず n の約数である (ラグランジュの定理)．特に，$\operatorname{ord} g$ は必ず n の約数であり，G の全ての元は $g^n = e$ を満たす．
- 位数が素数 p の群は “本質的に”(数学語で言うと『同型なものを同一視すると』)$\mathbb{Z}/p\mathbb{Z}$ しかない．

また，部分群による同値関係によって群の性質がわかるというだけではなく，そこから得られる**商集合**自体が重要な集合・空間となることもある (これは一般には群ではない)．群から作られる集合・空間ということで，この方法で良い対称性を持った集合・空間が得られるのである．例えば，円や球面といった空間は群の商集合として作ることができる．本講義の範囲を超えてしまうが，興味のある方は例えば「等質空間」というようなキーワードで調べてもらいたい．

6.1 同値関係

まず一旦群のことは忘れて単に集合とそこにおける同値関係について解説しよう．

定義 6.1

S を集合とする．任意の $x, y \in S$ に対し，

$$x \sim y \quad \text{または} \quad x \not\sim y$$

のいずれかか定まっているとする．このとき $\sim$ を S 上の**関係 (relation)** という[*1]．ここで，これが以下の 3 条件を満たすとき，$\sim$ を**同値関係 (equivalence relation)** という．

(i) (反射律) 任意の $x \in S$ に対して $x \sim x$.
(ii) (対称律) $x \sim y$ ならば $y \sim x$.
(iii) (推移律) $x \sim y$ かつ $y \sim z$ ならば $x \sim z$.

例 1. 集合 S において，イコール $=$ は同値関係である．

(i) (反射律) 任意の $x \in S$ に対して $x = x$.
(ii) (対称律) $x = y$ ならば $y = x$.
(iii) (推移律) $x = y$ かつ $y = z$ ならば $x = z$.

これが最も標準的な同値関係の例である．

* *e-mail* : hoya@shibaura-it.ac.jp

[*1] S 上の**関係**とは，より厳密には，$S \times S$ の部分集合 R のことである．$x, y \in S$ に対して，$(x, y) \in R$ のとき $x \sim y$，$(x, y) \notin R$ のとき $x \not\sim y$ と書くことにすれば，確かに任意の $x, y \in S$ に対して，$x \sim y$ または $x \not\sim y$ のいずれかが成立すると言える．

例 2. n を正の整数とする．整数のなす集合 $\mathbb{Z}$ において，

$$a \sim_n b \quad \Leftrightarrow \quad a-b \text{ が } n \text{ の倍数} \quad (\Leftrightarrow \quad [a]_n = [b]_n)$$

とすると，$\sim_n$ は $\mathbb{Z}$ 上の同値関係.

(i) (反射律) 任意の $x \in \mathbb{Z}$ に対して $x \sim_n x$.
(ii) (対称律) $x-y$ が n の倍数ならば $y-x=-(x-y)$ も n の倍数.
(iii) (推移律) $x-y$ が n の倍数，$y-z$ が n の倍数ならば $x-z=(x-y)+(y-z)$ も n の倍数.

例 3. 実数のなす集合 $\mathbb{R}$ において，不等号 $\leq$ は同値関係ではない．なぜなら，「$x \leq y$ ならば $y \leq x$」は一般に成り立たないからである．なお，反射律と推移律は満たされる．

例 4. 実数のなす集合 $\mathbb{R}$ において，

$$x \sim y \quad \Leftrightarrow \quad xy > 0$$

と定義すると，$\sim$ は同値関係ではない．なぜなら，$0 \times 0 = 0$ より，$0 \not\sim 0$ となって，反射律が満たされないためである．なお，対称律と推移律は満たされる．

例 5. $S = \{$ システム理工学部の学生 $\}$ において，

$$a \sim b \quad \Leftrightarrow \quad a \text{ さんは } b \text{ さんと同じ学科である}$$

とすると，$\sim$ は S 上の同値関係.

(i) (反射律) a さんは a さんと同じ学科である．
(ii) (対称律) a さんは b さんと同じ学科ならば，b さんは a さんと同じ学科である．
(iii) (推移律) a さんは b さんと同じ学科，b さんは c さんと同じ学科ならば，a さんは c さんと同じ学科である．

しかし，

$$a \sim' b \quad \Leftrightarrow \quad a \text{ さんは } b \text{ さんと一緒に遊んだことがある}$$

とすると，これは一般には同値関係ではない．なぜなら，「a さんは b さんと一緒に遊んだことがあって，b さんは c さんと一緒に遊んだことがあったとしても，a さんが c さんと一緒に遊んだことがない」ことがあるため[*2]，推移律が成り立たないためである．

[*2] 私の勝手な想像ですが，一般には良くあることだと思って書いています．

定義 6.2

集合 S 上に同値関係 $\sim$ が定まっているとする．このとき，$x \in S$ に対し，

$$C(x) \coloneqq \{y \in S \mid y \sim x\} (\subset S)$$

とし，これを x の**同値類 (equivalence class)** という．言葉で書くと，「$C(x)$ は x と同値関係で結ばれる元を全て集めてきてできる S の部分集合」である． $C(x)$ の各元 $y \in C(x)$ は $C(x)$ の**代表元 (representative)** と呼ばれる．さらに，

$$S/\sim \coloneqq \{C(x) \mid x \in S\}$$

とし，$S/\sim$ を S の $\sim$ による**商集合 (quotient set)** という．言葉で書くと，$S/\sim$ は「$\sim$ に関する同値類を集めてきてできる集合」である．写像

$$p\colon S \to S/\sim,\ x \mapsto C(x)$$

を**商写像 (quotient map)** という．商写像は定義から明らかに全射である．さらに，S の部分集合 R が $S/\sim$ の各元 (同値類) 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 (complete set of representatives)** という．

例 6. 例 5 の同値関係 $\sim$ の場合に，上で定義した諸概念を見てみよう．まず，$a \in S$ に対し，

$$C(a) \coloneqq \{b \in S \mid b \text{ さんは } a \text{ さんと同じ学科である }\}$$

となるので，a の同値類は a さんが所属する学科の全員からなる S の部分集合となる．このため，商集合は

$$\begin{aligned} S/\sim &\coloneqq \{C(a) \mid a \in S\} \\ &= \{\text{ 電子情報システム学科，機械制御システム学科，環境システム学科，生命科学科，数理科学科 }\} \end{aligned}$$

となる．商集合とはこのように，「$\sim$ によって定まるクラスの集まり」と考えれば良い．商写像

$$p\colon S \to S/\sim$$

は

$$a \mapsto (a \text{ さんの所属する学科})$$

という対応を与える写像である．完全代表系とは各学科からちょうど 1 人ずつの代表者を選んできてできる S の部分集合のことである．この例からも明らかなように完全代表系の選び方は沢山ある．

例 7. 例 2 の同値関係 $\sim_n$ の場合に，上で定義した諸概念を見てみよう．まず，同値類は

$$C(0) = \{nk \mid k \in \mathbb{Z}\},\ C(1) = \{nk+1 \mid k \in \mathbb{Z}\},\ C(2) = \{nk+2 \mid k \in \mathbb{Z}\}, \dots$$

となる．言葉で言うと，同値類は「n で割った余りが等しいものの集まり」である．この意味を考えれば明らかなように，任意の $k \in \mathbb{Z}$ に対し，$C(k) = C(k+n)$ が成立する．これより，

$$\mathbb{Z}/\sim_n \coloneqq \{C(a) \mid a \in \mathbb{Z}\} = \{C(0), C(1), \dots, C(n-1)\}$$

である．例えば，

$$\mathbb{Z}/\sim_3 = \{C(0), C(1), C(2)\}$$

などである．この例では，0 は $C(0)$ の代表元，5 は $C(2)$ の代表元，-2 は $C(1)$ の代表元，$\dots$ となり，例えば，$\{0, 5, -2\}$ は $\sim_3$ の完全代表系である．

なお，$\sim_n$ に関して，$C(k)$ を $[k]_n$ と書くことにすると，$[k]_n = [k+n]_n$ 等も成立しており，$\mathbb{Z}/\sim_n$ は $\mathbb{Z}/n\mathbb{Z}$ と同一視できるものであるということに着目しておこう．実際，この見方が $\mathbb{Z}/n\mathbb{Z}$ の捉え方の 1 つであるということを今後説明する．

以下は同値類の基本性質である．

命題 6.3

集合 S 上に同値関係 $\sim$ が定まっているとする．このとき以下が成立する．

(1) 任意の $y, z \in C(x)$ に対して，$y \sim z$.

(2) 任意の $y \in C(x)$ に対して，$C(x) = C(y)$.

(3) $C(x) \cap C(y) \neq \emptyset$ ならば，$C(x) = C(y)$ である．

証明.

(1) 定義より，$y \sim x, z \sim x$ なので，推移律より，$y \sim z$ である (対称律より $x \sim z$ でもあることに注意).

(2) $y \sim x$ のとき，対称律より $x \sim y$ でもあるので，推移律から，

$$z \sim x \quad \Leftrightarrow \quad z \sim y.$$

よって，定義より $C(x) = \{z \in S \mid z \sim x\} = \{z \in S \mid z \sim y\} = C(y)$.

(3) $C(x) \cap C(y) \neq \emptyset$ のとき，$z \in C(x) \cap C(y)$ とすると，(2) より，$C(x) = C(z) = C(y)$. □

命題 6.3 より，同値関係 $\sim$ の定まった集合 S は同値類によって，交わりなく「クラス分け」がされているということがわかる (“交わりなく” というのは 2 つの異なる同値類に属しているような元が存在しないということである)．これは例 6，例 7 からも納得できるものであろう．

6.2 剰余類

さて，話を群論に戻そう．以下では G を群，$e \in G$ をその単位元とする．また，H を G の部分群とする．H を用いて，G に次のように同値関係を定めることができる．

定義 6.4

$g, g' \in G$ に対し，

$$g \overset{H}{\sim}_L g' \quad \Leftrightarrow \quad \text{ある } h \in H \text{ が存在して, } g = g'h,$$
$$g \overset{H}{\sim}_R g' \quad \Leftrightarrow \quad \text{ある } h \in H \text{ が存在して, } g = hg',$$

とする．$g \overset{H}{\sim}_L g'$ のとき，g は g' に (H に関して) **左合同 (left congruence)** といい，$g \overset{H}{\sim}_R g'$ のとき，g は g' に (H に関して) **右合同 (right congruence)** という[*3].

命題 6.5

$\overset{H}{\sim}_L$ と $\overset{H}{\sim}_R$ は G 上の同値関係である．

証明. $\overset{H}{\sim}_L$ の場合のみ示す．$\overset{H}{\sim}_R$ の証明は全く同様である．$\overset{H}{\sim}_L$ が反射率，対称律，推移律を満たすことを示せばよい．

(i) (反射律) 部分群 H は G の単位元 e を必ず含むので (第 1,2 回講義資料命題 1.4 (3))，任意の $g \in G$ に対して，$e \in H$ を取ると，$g = ge$. よって，$g \overset{H}{\sim}_L g$.

(ii) (対称律) $g \overset{H}{\sim}_L g'$ とすると，定義よりある $h \in H$ が存在して，$g = g'h$. この式の両辺に右から h^{-1} を掛けると，$g' = gh^{-1}$. ここで，H は部分群であることから，逆元を取る操作について閉じているので，$h^{-1} \in H$. よって，$g' \overset{H}{\sim}_L g$.

[*3] h が右にあるとき左合同，h が左にあるとき右合同という名前がついていてややこしいが，これは誤植ではない．

(iii) (推移律) $g \overset{H}{\sim}_L g', g' \overset{H}{\sim}_L g''$ とすると，定義より，ある $h, h' \in H$ が存在して，$g = g'h, g' = g''h'$．このとき，$g = g''h'h$ となるが，いま H は部分群であることから，二項演算で閉じているので，$h'h \in H$．よって，$g \overset{H}{\sim}_L g''$．

以上より示すべきことは全て示された． □

命題 6.5 の証明内では，H が部分群であること，すなわち，空集合ではなく (=単位元を含み)，二項演算と逆元を取る操作について閉じているという事実を本質的に使っていることに注意しよう．H が部分群であることが，定義 6.4 の方法で同値関係を定義できることを保証しているのである．

定義 6.6

群 G 上の同値関係 $\overset{H}{\sim}_L$，$\overset{H}{\sim}_R$ による商集合はそれぞれ，

$$G/H \coloneqq G/\overset{H}{\sim}_L \qquad\qquad H\backslash G \coloneqq G/\overset{H}{\sim}_R$$

と書かれる．また，各 $g \in G$ に対し，$\overset{H}{\sim}_L$，$\overset{H}{\sim}_R$ に関する g の同値類は，それぞれ

$$\{g' \in G \mid g' \overset{H}{\sim}_L g\} = \{gh \mid h \in H\} =: gH$$
$$\{g' \in G \mid g' \overset{H}{\sim}_R g\} = \{hg \mid h \in H\} =: Hg$$

と書かれる．これらの記号を用いると，

$$G/H = \{gH \mid g \in G\} \qquad H\backslash G = \{Hg \mid g \in G\}$$

である．gH を g の H による**左剰余類 (left coset)** といい，Hg を g の H による**右剰余類 (right coset)** という．G/H の元の個数 $|G/H|$ を H の G における**指数 (index)** といい，$(G : H)$ と書く．また，$\overset{H}{\sim}_L$ の完全代表系を**左完全代表系 (complete set of left coset representatives)**，$\overset{H}{\sim}_R$ の完全代表系を**右完全代表系 (complete set of right coset representatives)** という．

例 8. $n \in \mathbb{Z}_{>0}$ とする．加法群 $\mathbb{Z}$ と n の倍数全体からなる $\mathbb{Z}$ の部分群

$$n\mathbb{Z} \coloneqq \langle n \rangle = \{nk \mid k \in \mathbb{Z}\}$$

に関して，定義 6.6 で定義された諸概念を見てみよう．各 $a \in \mathbb{Z}$ に対して，a の $n\mathbb{Z}$ による左剰余類は (加法群の二項演算は $+$ であったことに注意すると),

$$a + n\mathbb{Z} = \{a + nk \mid k \in \mathbb{Z}\}$$

であり，右剰余類は,

$$n\mathbb{Z} + a = \{nk + a \mid k \in \mathbb{Z}\} = a + n\mathbb{Z}$$

である．よって，このときには左剰余類と右剰余類の違いはない．一般に可換群においては，左剰余類と右剰余類の違いはないことが定義からすぐにわかるであろう．商集合は,

$$\mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} \mid a \in \mathbb{Z}\} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$$

である．よって，$n\mathbb{Z}$ の $\mathbb{Z}$ における指数は

$$(\mathbb{Z} : n\mathbb{Z}) = |\mathbb{Z}/n\mathbb{Z}| = n$$

である．例えば，$\{0, 1, 2, \ldots, n-1\}$ が (左) 完全代表系である．

また，同値関係 $\overset{n\mathbb{Z}}{\sim}_L$ は以下のように考えると，例 2 の同値関係と同じであることがわかる．

$$\begin{aligned} a \overset{n\mathbb{Z}}{\sim}_L a' &\Leftrightarrow \text{ある } nk \in n\mathbb{Z} \text{ が存在して, } a = a' + nk \\ &\Leftrightarrow a - a' \text{が } n \text{ の倍数} \\ &\Leftrightarrow a \sim_n a' (\Leftrightarrow [a]_n = [a']_n). \end{aligned}$$

確かに例 7 の同値類とここでの剰余類を比べてみると，$C(a) = a + n\mathbb{Z}$ となっていることがわかる．特に，

$$\mathbb{Z}/\sim_n = \mathbb{Z}/n\mathbb{Z}$$

である．剰余類 $a + n\mathbb{Z}$ を $[a]_n$ と書くと，これは今まで学んできた $\mathbb{Z}/n\mathbb{Z}$ と整合している．実際，$a + n\mathbb{Z} = (a + nk) + n\mathbb{Z}$ $(k \in \mathbb{Z})$ も成立している (これは命題 6.3 (2) であると言っても良い)．$\mathbb{Z}/n\mathbb{Z}$ という記号を使っていたのはこの考え方によるものだったのである．

例 9. $D_3 = \{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ を 3 次二面体群とする $(\sigma^3 = e, \tau^2 = e, \sigma^k\tau = \tau\sigma^{-k}\ (k \in \mathbb{Z}))$．$D_3$ の部分群 $H = \langle\tau\rangle = \{e, \tau\}$ に関して，定義 6.6 で定義された諸概念を見てみよう．$e \in D_3$ の H による左剰余類は，

$$eH = \{eh \mid h \in H\} = \{ee, e\tau\} = \{e, \tau\}(= H)$$

である (一般の群 G とその部分群 H に対して，同様に $eH = H$ であることはすぐにわかるであろう)．$\sigma \in D_3$ の H による左剰余類は，

$$\sigma H = \{\sigma h \mid h \in H\} = \{\sigma e, \sigma\tau\} = \{\sigma, \sigma\tau\}$$

である．$\sigma^2 \in D_3$ の H による左剰余類は，

$$\sigma^2 H = \{\sigma^2 h \mid h \in H\} = \{\sigma^2 e, \sigma^2\tau\} = \{\sigma^2, \sigma^2\tau\}$$

である．以上より $D_3 = eH \cup \sigma H \cup \sigma^2 H$ であるので，結局

$$D_3/H = \{gH \mid g \in D_3\} = \{H, \sigma H, \sigma^2 H\}$$

である (命題 6.3 (2) より，$eH = \tau H, \sigma H = \sigma\tau H, \sigma^2 H = \sigma^2\tau H$ である)．これより H の D_3 における指数は，

$$(D_3 : H) = |D_3/H| = 3$$

である．例えば，$\{e, \sigma, \sigma^2\}, \{\tau, \sigma, \sigma^2\tau\}$ 等は左完全代表系である．

なお，上の例で各剰余類に含まれる元の個数は $2(= |H|)$ 個だったので，指数は

$$(D_3 : H) = 6/2 = |D_3|/|H|$$

と計算できる．実はこのような計算は常に行うことができ，これが次回説明するラグランジュの定理である．

最後に右剰余類を見ておこう．$e \in D_3$ の H による右剰余類は，

$$He = \{he \mid h \in H\} = \{ee, \tau e\} = \{e, \tau\}(= H)$$

である (一般の群 G とその部分群 H に対して，同様に $He = H$ であることはすぐにわかるであろう)．$\sigma \in D_3$ の H による右剰余類は，

$$H\sigma = \{h\sigma \mid h \in H\} = \{e\sigma, \tau\sigma\} = \{\sigma, \sigma^{-1}\tau\} = \{\sigma, \sigma^2\tau\} \neq \sigma H$$

である．非可換群であるので，このように同じ元の同じ部分群による左剰余類と右剰余類が異なるということがある．$\sigma^2 \in D_3$ の H による右剰余類は，

$$H\sigma^2 = \{h\sigma^2 \mid h \in H\} = \{e\sigma^2, \tau\sigma^2\} = \{\sigma^2, \sigma^{-2}\tau\} = \{\sigma^2, \sigma\tau\} \neq \sigma^2 H$$

である．以上より $D_3 = H \cup H\sigma \cup H\sigma^2$ であるので，結局

$$H\backslash D_3 = \{Hg \mid g \in D_3\} = \{H, H\sigma, H\sigma^2\}$$

である．例えば，$\{e, \sigma, \sigma^2\}, \{\tau, \sigma, \sigma\tau\}$ 等は右完全代表系である．