離散数学 講義資料 (9)

9.1　群

本節は，教科書 4.2.1 節の前半 (pp.168–170) に対応する．

定義 9.1 A を集合とし，f を $A \times A$ から A への関数，すなわち A 上の 2 変数関数とする．このとき，f を集合 A 上の **2 項演算** (binary operation) と呼ぶ．□

定義 9.2 f を集合 A 上の 2 項演算とし，A' を A の部分集合とする．もし，全ての $a_1, a_2 \in A'$ に対し $f(a_1, a_2) \in A'$ が成立するならば，A' は f に対して **閉じている** (closed) と言う．□

NOTE: 任意の $n, m \in \mathbb{Z}$ に対して，$n+m,\ n-m,\ n*m \in \mathbb{Z}$ が成立する．それゆえに，整数集合 $\mathbb{Z}$ は加法 $(+)$，減法 $(-)$，乗法 $(*)$ に対して閉じている．一方，$2, 3 \in \mathbb{N}$ であるが，$2-3 \notin \mathbb{N}$ である．それゆえに減法は自然数集合 $\mathbb{N}$ に対して閉じていない．

定義 9.3 群 (group) とは三つ組み $\langle G, \cdot, e\rangle$ の事である．ここで，G は集合であり，$\cdot$ は G 上の 2 項演算であり，$e \in G$ であり，さらに，以下の条件を満たすとする．

(G1) $\forall x, y, z.\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$

(G2) $\forall x.\ x \cdot e = e \cdot x = x$

(G3) $\forall x. \exists y.\ x \cdot y = y \cdot x = e$

ここで，e を $\cdot$ の **単位元** (unit element) と呼び，(G3) における x, y に対し，y を x の **逆元** (inverse element) と呼ぶ．特に，G が有限集合のとき群 $\langle G, \cdot, e\rangle$ を **有限群** (finite group) と呼ぶ．なお，2 項関係 $\cdot$ はしばしば省略される．また，群 $\langle G, \cdot, e\rangle$ を単に G で記すことも多い．□

定義 9.4 以下の条件を満たす群 $\langle G, \cdot, e\rangle$ を **可換群** (commutative group) または **アーベル群** (Abelian group) と呼ぶ．

(G4) $\forall x, y.\ x \cdot y = y \cdot x$　□

命題 9.5 群 $\langle G, \cdot, e\rangle$ において e は只一つの単位元である，すなわち，$\forall x.\ xe' = e'x = x$ ならば $e = e'$．

証明　e と異る単位元 e' が存在すると仮定する．e は単位元なので $ee' = e'$．e' も単位元なので $ee' = e$．よって，$e = e'$ となり矛盾．□

命題 9.6 $\langle G, \cdot, e\rangle$ を群とし，$x \in G$ とする．x の逆元は只一つ存在する．

証明 (G3) より少なくとも 1 つの逆元は存在する．ある x が 2 つの逆元 y, z を持つと仮定すると，

$$y = ye = y(xz) = (yx)z = ez = z$$

となり矛盾．よって，任意の $x \in G$ は只一つの逆元を持つ． □

定義 9.7 命題 9.6 より逆元が一意に存在することをふまえ，x の逆元を x^{-1} で記す．なお，アーベル群を取り扱うときには，しばしば群の演算を表す記号として $+$ を用いるが，このときは x の逆元を $-x$ と記す事が多い． □

命題 9.8 $\langle G, \cdot, e\rangle$ を群とする．このとき，以下が成立．

(1) $e^{-1} = e$　　(2) $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$　　(3) $(x^{-1})^{-1} = x$

証明 演習課題に残す． □

9.2 群の準同型写像

本節は，教科書 4.2.1 節の後半 (pp.170–171) に対応する．

定義 9.9 $\langle G, \cdot, e\rangle$ と $\langle G', *, e'\rangle$ を群とする．G から G' への写像 ϕ が**準同型写像** (homomorphism) であるとは以下の関係が成立することである．

$$\phi(x \cdot y) = \phi(x) * \phi(y) \qquad \text{for all } x, y \in G$$

特に，全単射な準同型写像を**同型写像** (isomorphism) と呼ぶ．
逆に，群 $\langle G, \cdot, e\rangle$ から群 $\langle G', *, e'\rangle$ へ準同型写像が存在するとき，群 $\langle G, \cdot, e\rangle$ と群 $\langle G', *, e'\rangle$ は**準同型** (homomorphism) であるという．また，同型写像が存在するとき**同型** (isomorphism) であるといい，$\langle G, \cdot, e\rangle \cong \langle G', *, e'\rangle$ で記す． □

命題 9.10 ϕ を群 $\langle G, \cdot, e\rangle$ から群 $\langle G', *, e'\rangle$ への準同型写像とする．このとき，以下が成立．

(1) $\phi(e) = e'$　　(2) $\phi(x)^{-1} = \phi(x^{-1})$

証明

(1)
$$\begin{aligned}
\phi(e) &= e' * \phi(e) && (G2) \text{ より} \\
&= (\phi(e)^{-1} * \phi(e)) * \phi(e) && (G3) \text{ より} \\
&= \phi(e)^{-1} * (\phi(e) * \phi(e)) && (G1) \text{ より} \\
&= \phi(e)^{-1} * \phi(e \cdot e) && \phi \text{が準同型写像であることより} \\
&= \phi(e)^{-1} * \phi(e) && (G2) \text{ より} \\
&= e' && (G3) \text{ より}
\end{aligned}$$

$$
\begin{array}{lrll}
(2) & \phi(x)^{-1} & = & \phi(x)^{-1} * e' & (G2) \text{ より} \\
 & & = & \phi(x)^{-1} * \phi(e) & (1) \text{ より} \\
 & & = & \phi(x)^{-1} * \phi(x \cdot x^{-1}) & (G3) \text{ より} \\
 & & = & \phi(x)^{-1} * (\phi(x) * \phi(x^{-1})) & \phi \text{が準同型写像であることより} \\
 & & = & (\phi(x)^{-1} * \phi(x)) * \phi(x^{-1}) & (G1) \text{ より} \\
 & & = & e' * \phi(x^{-1}) & (G3) \text{ より} \\
 & & = & \phi(x^{-1}) & (G2) \text{ より}
\end{array}
$$
□

9.3 部分群

本節は，教科書 4.2.2 節の前半 (pp.171–173) に対応する．

定義 9.11 $\langle G, \cdot, e\rangle$ を群とする．ある G の部分集合 H にたいし，$\langle H, \cdot, e\rangle$ が群となるとき $\langle H, \cdot, e\rangle$ を $\langle G, \cdot, e\rangle$ の**部分群** (subgroup) であるという． □

命題 9.12 $\langle G, \cdot, e\rangle$ を群とし，H を G の空でない部分集合とする．このとき，$\langle H, \cdot, e\rangle$ が $\langle G, \cdot, e\rangle$ の部分群であることと以下の 2 条件が成立することとは必要十分である．

(S1) H が $\cdot$ で閉じている，すなわち任意の H の元 x, y に対し $x \cdot y \in H$ となる．

(S2) $x \in H$ ならば $x^{-1} \in H$．

証明 $\langle H, \cdot, e\rangle$ が $\langle G, \cdot, e\rangle$ の部分群であるときは，$\langle H, \cdot, e\rangle$ は群なので明らかに (S1),(S2) は成立する．
(S1),(S2) が成立するとして，$\langle H, \cdot, e\rangle$ が群であることを示す．性質 (S1) より，$\cdot$ は H 上の２項関係である．(G1),(G2) は明らかに成立し，性質 (S2) より (G3) が成立することも明らか．よって，$e \in H$ を示せば証明は完成する．
H は空でないので，ある $x \in H$ が存在．性質 (S2) より，$x^{-1} \in H$．性質 (S1) より，$e = x \cdot x^{-1} \in H$．よって，$e \in H$． □

命題 9.13 $\langle G, \cdot, e\rangle$ を群とし，H を G の空でない有限部分集合とする．このとき，$\langle H, \cdot, e\rangle$ が $\langle G, \cdot, e\rangle$ の部分群であることと以下の条件が成立することとは必要十分である．

(S1) H が $\cdot$ で閉じている，すなわち任意の H の元 x, y に対し $x \cdot y \in H$ となる．

証明 命題 9.12 を考えて，性質 (S2) を成立することを示せば十分．以下では $x \in H$ とし $x^{-1} \in H$ を示す．
$x, x^2, x^3, \cdots$ を考える．性質 (S1) より $x, x^2, x^3, \cdots$ は全て H の元．また，H は有限集合なので，$x, x^2, x^3, \cdots$ の中には同じ元が含まれる，すなわち，ある整数 m, n が存在して $m < n$ かつ $x^m = x^n$．この両辺に x^{-1} を m 回掛けることにより $e = x^{n-m}$ を得る．$n - m = 1$ のときは $x = e$ なので，$x^{-1} = e$ が H に存在．$n - m > 1$ のときは $x^{-1} = x^{n-m-1}$ が H に存在する．よって，性質 (S2) が成立する． □

定義 9.14 ϕ を群 $\langle G, \cdot, e\rangle$ から群 $\langle G', *, e'\rangle$ への準同型写像とする．$Im(\phi) = \{\phi(a) \mid a \in G\}$ を ϕ の**像** (image) と呼び，$Ker(\phi) = \{a \in G \mid \phi(a) = e'\}$ を ϕ の**核** (kernel) と呼ぶ． □

命題 9.15 ϕ を群 $\langle G, \cdot, e\rangle$ から群 $\langle G', *, e'\rangle$ への準同型写像とする．このとき，$\langle Ker(\phi), \cdot, e\rangle$ は $\langle G, \cdot, e\rangle$ の部分群であり，$\langle Im(\phi), *, e'\rangle$ は $\langle G', *, e'\rangle$ の部分群である．

証明 命題 9.12 を用いて証明する．

- $\langle G, \cdot, e\rangle$ に対し $\langle Ker(\phi), \cdot, e\rangle$ が性質 (S1),(S2) を満たすことを示す．

  (S1) $x, y \in Ker(\phi)$ とする．Ker の定義より $\phi(x) = \phi(y) = e'$．ϕ は準同型写像なので，$\phi(x \cdot y) = \phi(x) * \phi(y) = e' * e' = e'$．よって，$x \cdot y \in Ker(\phi)$．

  (S2) $x \in Ker(\phi)$ とする．Ker の定義より $\phi(x) = e'$．命題 9.10(2) より，$\phi(x^{-1}) = \phi(x)^{-1} = e'^{-1} = e'$．よって，$x^{-1} \in Ker(\phi)$．

- $\langle G', *, e'\rangle$ に対し $\langle Im(\phi), *, e'\rangle$ が性質 (S1),(S2) を満たすことを示す．

  (S1) $x', y' \in Im(\phi)$ とする．Im の定義より，ある $x, y \in G$ が存在して $\phi(x) = x'$ かつ $\phi(y) = y'$．ϕ は準同型写像なので，$\phi(x \cdot y) = \phi(x) * \phi(y) = x' * y'$．よって，$x' * y' \in Im(\phi)$．

  (S2) $x' \in Im(\phi)$ とする．Im の定義より，ある $x \in G$ が存在して $\phi(x) = x'$．命題 9.10(2) より，$\phi(x^{-1}) = \phi(x)^{-1} = x'^{-1}$．よって，$x'^{-1} \in Im(\phi)$． □

9.4 位数とラグランジェの定理

本節は，教科書 4.2.2 節の後半 (pp.173–176) に対応する．

定義 9.16 $\langle G, \cdot, e\rangle$ を有限群とする．G の元の個数 $|G|$ をこの群の**位数** (order) と呼ぶ． □

補題 9.17 $\langle G, \cdot, e\rangle$ を群とし，$\langle H, \cdot, e\rangle$ をその部分群とする．このとき，以下で定義される G 上の関係は同値関係になる．

$$x \sim_H y \iff^{\text{def}} x \cdot y^{-1} \in H$$

証明

(反射性) $x \cdot x^{-1} = e \in H$ より $x \sim_H x$．

(対称性) $x \sim_H y$ とする．$\sim_H$ の定義より $x \cdot y^{-1} \in H$．ここで，命題 9.8 と性質 (G3) より

$$y \cdot x^{-1} = (y^{-1})^{-1} \cdot x^{-1} = (x \cdot y^{-1})^{-1} \in H$$

よって，$y \sim_H x$．

(推移性) $x \sim_H y$ かつ $y \sim_H z$ とする．$\sim_H$ の定義より $x \cdot y^{-1} \in H$ かつ $y \cdot z^{-1} \in H$．性質 (G1) より $(x \cdot y^{-1}) \cdot (y \cdot z^{-1}) \in H$．また，$(x \cdot y^{-1}) \cdot (y \cdot z^{-1}) = x \cdot z^{-1}$．よって，$x \cdot z^{-1} \in H$，すなわち，$x \sim_H z$． □

定義 9.18 $\langle G,\cdot,e\rangle$ を群とし，$\langle H,\cdot,e\rangle$ をその部分群とする．同値関係 $\sim_H$ による同値類を $\langle G,\cdot,e\rangle$ の $\langle H,\cdot,e\rangle$ による**剰余類** (coset) と言う．また，商集合 $G/\sim_H$ を G/H で記す．□

定理 9.19 (ラグランジェ(Lagrange) の定理) $\langle G,\cdot,e\rangle$ を有限群とし，$\langle H,\cdot,e\rangle$ をその部分群とする．このとき，$\langle H,\cdot,e\rangle$ の位数は $\langle G,\cdot,e\rangle$ の位数の約数である，

証明 $\sim_H$ による任意の剰余類 C に対し $|C|=|H|$ となる事を示す．この事実が示されると，剰余類の全体は G の直和分解を与えるので $|H|$ が $|G|$ の約数となる事が導かれる．
最初に，$a\in C$ ならば $H\cdot a=C$ となる事を示す (ただし，$H\cdot a \stackrel{\text{def}}{=\!=} \{h\cdot a \mid h\in H\}$).

$$\begin{aligned} x\in C &\iff x\sim_H a \\ &\iff x\cdot a^{-1}\in H \\ &\iff \exists h\in H.\ x\cdot a^{-1}=h \\ &\iff \exists h\in H.\ x=h\cdot a \\ &\iff x\in H\cdot a \end{aligned}$$

また，任意の $a\in C$ と $h_1,h_2\in H$ に対し，$h_1=h_2 \iff h_1\cdot a=h_2\cdot a$ であるので $|H|=|H\cdot a|$ が成立．以上より $|C|=|H\cdot a|=|H|$ が得られる．□

定義 9.20 $\langle G,\cdot,e\rangle$ を有限群とし，$a\in G$ とする．$a^n=e$ となる最小の正整数 n を a の**位数** (order) と呼ぶ．□

定理 9.21 $\langle G,\cdot,e\rangle$ を有限群とし，$a\in G$ とする．このとき，a の位数は定義可能であり，さらに $\langle G,\cdot,e\rangle$ の位数の約数となる．

証明 $A=\{a^0,a^1,a^2,\ldots\}$ とする (ただし，$a^0=e$ と考える)．任意の $a^m,a^n\in A$ に対し $a^ma^n=a^{m+n}\in A$ であるので，命題 9.13 より $\langle A,\cdot,e\rangle$ は部分群．よって，定理 9.19 より $|A|$ は $|G|$ の約数．
また，G は有限なので A も有限．よって，ある整数 m,n が存在して $m<n$ かつ $a^m=a^n$．両辺に a^{-1} を m 回掛けることにより $e=a^{n-m}$ を得る．すなわち，a の位数は定義可能．ここで，a の位数を k とする．このとき明らかに $A=\{a^0,a^1,\ldots,a^{k-1}\}$．ある整数 m,n が存在して $0\le m<n<k$ かつ $a^m=a^n$ と仮定すると，$a^{n-m}=e$ かつ $0<n-m<k$ となるので，k の最小性に矛盾．よって，$|A|=k$．よって，k は $|G|$ の約数．□

9.5 いろいろな群

本節は，教科書 3.3 節の中程 (pp.136–137) を含む．
いろいろな群とは言っているが，本節では Z_n と $Z_p^\times$ で記される 2 つの重要な群のみを紹介するに留める．

定義 9.22 集合 Z_n を $\{0,1,\ldots,n-1\}$ で，集合 $Z_n^\times$ を $\{1,\ldots,n-1\}$ で定義する．集合 Z_n 上の 2 項演算 $\oplus_n$ と $\otimes_n$ を以下で定義する．

$$\begin{aligned} x\oplus_n y &\stackrel{\text{def}}{=\!=} (x+y) \bmod n \\ x\otimes_n y &\stackrel{\text{def}}{=\!=} xy \bmod n \end{aligned}$$

□

命題 9.23 任意の正整数 n に対し，$\langle Z_n, \oplus_n, 0\rangle$ は群になる．

証明 性質 (G1) と (G2) が成立することは明らか．よって，性質 (G3)，すなわち逆元の存在を示せば十分．$x \in Z_n$ とする．このとき，$n - x \in Z_n$ かつ $x \oplus_n (n-x) = (x + (n-x)) \bmod n = n \bmod n = 0$．よって，$n - x$ は x の逆元． □

命題 9.24 任意の正整数 p に対し以下が成立．

$$p\text{が素数} \iff \langle Z_p^\times, \otimes_p, 1\rangle \text{が群}$$

証明

- p を合成数とする．このとき，ある整数 m, n が存在して $1 < m, n < p$ かつ $p = mn$．一方，$m, n \in Z_p^\times$ かつ $m \otimes_p n = mn \bmod p = 0 \notin Z_p^\times$ であるので，$\otimes_p$ は $Z_p^\times$ に閉じてない．すなわち，$\langle Z_p^\times, \otimes_p, 1\rangle$ は群でない．

- p を素数とする．

  最初に，$\otimes_p$ が $Z_p^\times$ に閉じていることを示す．$m, n \in Z_p^\times$ とする．p は素数なので $(m, p) = (n, p) = 1$．よって，$(mn, p) = 1$．よって，$m \otimes_p n = mn \bmod p \neq 0$．すなわち，$m \otimes_p n \in Z_p^\times$．

  性質 (G1),(G2) が成立することは明らか．よって，性質 (G3)，すなわち逆元の存在を示せば十分．$x \in Z_p^\times$ とする．補題 8.1 で定義した関数 $f_x : Z_p^\times \to Z_p^\times$ を考える．f_x は全射であったので，ある $i \in Z_p^\times$ が存在して $f_x(i) = 1$．よって，$x \otimes_p i = xi \bmod p = f_x(i) = 1$．よって，$x^{-1} = i$． □

定理 9.25 (フェルマーの小定理) p を 2 以上の整数とし，a を $a \not\equiv 0 \pmod p$ となる任意の整数とする．

$$p \text{ が素数} \implies a^{p-1} \equiv 1 \pmod p$$

証明 p が素数であるので命題 9.24 より $\langle Z_p^\times, \otimes_p, 1\rangle$ は群．定理 9.21 より $a \bmod p$ の群 $\langle Z_p^\times, \otimes_p, 1\rangle$ における位数 k は $|Z_p^\times| = p - 1$ の約数．よって，$a^k \equiv 1 \pmod p$ なので，$a^{p-1} \equiv 1 \pmod p$． □

演習課題

問 9.1 命題 9.8 を示せ．すなわち，$\langle G, \cdot, e\rangle$ を群としたとき，以下が成立することを示せ．

(1) $e^{-1} = e$　　(2) $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$　　(3) $(x^{-1})^{-1} = x$

問 9.2 ϕ を群 $\langle G, \cdot, e\rangle$ から群 $\langle G', *, e'\rangle$ への準同型写像とする．このとき，次の関係が成立することを証明せよ．

$$\phi\text{が単射} \iff Ker(\phi) = \{e\}$$

問 9.3 群 $\langle G, \cdot, e\rangle$ が，ある $a \in G$ によって $G = \{a^0, a^1, \ldots\}$ と表されるとき，**巡回群** (cyclic group) と呼ばれる．位数が素数になる群は全て巡回群であることを証明せよ．