2　群

定義 2.1 代数系 $(G\,;\varphi)$ が次の性質を持つとき**群** (*group*) という。
(1) φ は結合法則を満たす。
(2) φ に関する単位元 e が存在する。
(3) 任意の元 g に対しその逆元 g^{-1} が存在する。

群の演算は通常 $\varphi(g,h)=gh$ と書かれる。また演算を省略して '群 G' という言い方をする事もある。この記法で群の定義を述べると次になる。
(1) G の任意の元 a,b,c に対し $a(bc)=a(bc)$ が成立する。
(2) 単位元 (と呼ばれる元) e が存在して任意の元 $a\in G$ に対し $ae=ea=a$ が成立する。
(3) 任意の元 a に対しその逆元 (と呼ばれる元) a^{-1} が存在して $aa^{-1}=a^{-1}a=e$ が成立する。
　演算が交換法則を満たすときこの群を**可換群** (*commutative group*) または**アーベル群** (*Abel group, abelian group*) という。可換群の場合演算を和の記号「$+$」で書くことが多い。

命題 2.2 群 G に対し単位元は唯 1 つ存在する。任意の元 g に対しその逆元は唯 1 つ存在する。

証明　単位元の性質を持つものがもう 1 つあったとして，それを e' とする。このとき $e=ee'=e'$ である。また元 x に対し逆元の性質を持つ x' が存在したとする。$x^{-1}=x^{-1}e=x^{-1}(xx')=(x^{-1}x)x'=ex'=x'$ が成立する。

演習問題 2.1　次の例 1.1 の集合が群になるかどうか調べよ。

(1) $(\boldsymbol{B}\,;+)$	(2) $(\boldsymbol{B}\,;\cdot)$
(3) $(Y\,;+)$	(4) $(Y\,;\bigoplus)$
(5) $(Y\,;\cdot)$	(6) $(Y\,;\bigodot)$
(7) $(\boldsymbol{N}\,;\cdot)$	(8) $(\boldsymbol{Z}\,;+)$
(9) $(\boldsymbol{Z}\,;\cdot)$	(10) $(\boldsymbol{Q}\,;+)$
(11) $(\boldsymbol{Q}\,;\cdot)$	(12) $(\boldsymbol{R}\,;+)$
(13) $(\boldsymbol{R}\,;\cdot)$	

例 2.3
(1) 自然数 m に対し，$\boldsymbol{Z}_m=\{0,1,\ldots,m-1\}$ とする。$\boldsymbol{Z}_m$ 上に和を次の様に定義する。
　整数対し次の性質が成立する；『整数 n と自然数 m に対し，整数 q, r $(0\leqq r<m)$ が存在して $n=qm+r$ となる。この様な q,r は一意的である。』この r を $r=\mathrm{rem}(n,m)$ と書こう。このとき $\boldsymbol{Z}_m$ 上の演算 φ を $\varphi(a,b)=\mathrm{rem}(a+b,m)$ で定義する。通常この演算を和といい $a+b=\varphi(a,b)$ で表す。$(\boldsymbol{Z}_m\,;+)$ は群をなす。
(2) n を自然数とし，$N=\{1,\ldots,n\}$ と置く。N から N への全単射全体を S_n とするとき，S_n 上の演算を合成関数で定義する; 即ち S_n の元 (これを置換と呼ぶ)σ,τ に対し $(\sigma\cdot\tau)(i)=\sigma(\tau(i))$ で定義する。このとき $(S_n\,;\cdot)$ は群になる。この群を n **次対称群** (*symmetric group*) という。

S_n の元 σ に対し $\sigma = \begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix}$ という表現をする事がある。この表し方だと単位元 σ_0 は $\sigma_0 = \begin{pmatrix} 1\,2 & \cdots & n \\ 1\,2 & \cdots & n \end{pmatrix}$ と書かれる。

n 変数多項式 $f(X_1, \ldots, X_n)$ と S_n の元 σ に対し，
$(\sigma f)(X_1, \ldots, X_n) = f(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$ とおくと，$\sigma, \tau \in S_n$ に対し $\sigma_1(\sigma_2 f) = (\sigma_1\sigma_2)f$ が成立する。特に f として差積 $D = \prod_{i<j}(X_i - X_j)$ をとれば $\sigma D = \pm D$ となるので，$\sigma D = \varepsilon(\sigma) D$ と定義する。$\varepsilon(\sigma) = 1$ となる置換を**偶置換** (*even permutation*)，$\varepsilon(\sigma) = -1$ となる置換を**奇置換** (*odd permutation*) という。$A_n = \{\, \sigma \in S_n \mid$ σは偶置換$\,\}$ を n **次交代群** (*alternating group*) という。

(3) 正則な実 2 次行列全体を $GL(2, \boldsymbol{R})$ と書く。行列の積に関し群をなす。これを 2 次の**一般線型群** (*general linear group*) という。
$SL(2, \boldsymbol{R}) = \{\, A \in GL(2, \boldsymbol{R}) \mid \det(A) = 1 \,\}$ を 2 次の**特殊線型群** (*special linear group*)

(4) 平面 $\boldsymbol{R}^2$ 上にある幾何的図形 Δ があるとする。この図形を図形全体として固定する合同変換全体は群をなす。たとえば Δ として原点中心の半径 1 の円とすると，この群は 2 次**直交群** (*orthogonal group*) $O(2) = \{\, A \in GL(2, \boldsymbol{R}) \mid {}^tAA = E \,\}$ となる。

(5) (前項の続き) 平面図形として正 n 角形 Δ をとる。正 n 角形は原点中心で 1 つの頂点が $(1, 0)$ にあるとする。この図形を固定する合同変換全体を n 次の **2 面体群** (*dyhedral group*) といい，D_n と書く。

演習問題 2.2　例 2.3 で取り上げた群が実際に群になる事を示せ。

演習問題 2.3　例 2.3(1) と同様に積を定義する。$\boldsymbol{Z}_m^* = \boldsymbol{Z}_m - \{0\}$ 上で積が群をなすかどうか調べよ。

演算のところで定義した同型・準同型を群に関しもう一度述べておく。

定義 2.4 群 G_1 から群 G_2 への写像 f が次を満たすとき写像 f を準同型写像という; G_1 の任意の元 g, h に対し $f(gh) = f(g)f(h)$。この f が全単射のとき f を同型写像といい，G_1 と G_2 は同型であるといい，$G_1 \cong G_2$ と書く。

例 2.3 でもあった様に，群の部分集合がまた群になる事があった。その場合について次の定義を与えておこう。

定義 2.5 群 G の部分集合 H がこの演算に関して群になるときこの H を G の**部分群** (*subgroup*) といい，$H < G$ とかく。

命題 2.6 群 G の空でない部分集合 H が次の条件を満たすとき部分群になる;
(1) 任意の $g, h \in H$ に対し $gh \in H$
(2) 任意の元 $g \in H$ に対し $g^{-1} \in H$

命題 2.7 群 G の空でない部分集合 H が次の条件を満たすとき部分群になる; 任意の $g, h \in H$ に対し $g^{-1}h \in H$

演習問題 2.4　群 G の 2 つの部分群 H_1, H_2 に対し $H_1 \cap H_2$ は G の部分群である事を示せ。

定義 2.8 群 G の元 g を 1 つ固定する。$\{\, g^n \mid n \in \boldsymbol{Z} \,\}$ は G の部分群になるが，これを $\langle\, g \,\rangle$ と書き，g が生成する**巡回群** (*cyclic group*) という。またこのとき g を**生成元** (*generator*) という。

演習問題 2.5　$\langle g \rangle$ が部分群になる事を示せ。

演習問題 2.6　巡回群 $\langle g \rangle$ は $(\boldsymbol{Z}; +)$ または $(\boldsymbol{Z}_m; +)$ と同型である事を示せ。$\boldsymbol{Z}$ を**無限巡回群** (*infinite cyclic group*)，$\boldsymbol{Z}_m$ を位数 m の **(有限) 巡回群** (*(finite) cyclic group*) という。

定義 2.9 2 つの群 $(G_1; \varphi_1)$, $(G_2; \varphi_2)$ に対し $G_1 \times G_2$ 上の演算 φ を $\varphi((g_1, g_2), (h_1, h_2)) = (\varphi_1(g_1, h_1), \varphi_2(g_2, h_2))$ で定義すると $(G_1 \times G_2; \varphi)$ は群になる。これを G_1 と G_2 の**直和** (*direct sum*) といい，$G_1 \bigoplus G_2$ と書く。

演習問題 2.7　m と n が互いに素であれば $\boldsymbol{Z}_m \bigoplus \boldsymbol{Z}_n \cong \boldsymbol{Z}_{mn}$ である事を示せ。

以下この節では群は**有限群** (*finite group*)，つまり集合として見たときに有限集合であると仮定する。群 G の元の個数を $|G|$ と書き, これを群の**位数** (*order*) という。また G の元 g に対し $\langle g \rangle$ の位数を元 g の位数という。位数の小さい場合にどんな群があるか，すべてをリストアップする事を目標として考えていく。

演算表:　群 G を $G = \{g_1, g_2, \ldots, g_n\}$ とするとき，次の様な表を**演算表** (**乗積表**) という。

	g_1	$\cdots$	g_j	$\cdots$	g_n
g_1	g_1g_1	$\cdots$	g_1g_j	$\cdots$	g_1g_n
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
g_i	g_ig_1	$\cdots$	g_ig_j	$\cdots$	g_ig_n
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
g_n	g_ng_1	$\cdots$	g_ng_j	$\cdots$	g_ng_n

例えば $G = \boldsymbol{Z}_4$ のとき g を生成元とすると，G の各元 g_i は $g_i = g^i$ $(i = 0, 1, 2, 3)$ と書けるので演算表は次の様になる。

	g^0	g	g^2	g^3
g^0	g^0	g	g^2	g^3
g	g	g^2	g^3	g^0
g^2	g^2	g^3	g^0	g
g^3	g^3	g^0	g	g^2

$G = \boldsymbol{Z}_2 \bigoplus \boldsymbol{Z}_2$ のとき，それぞれの生成元を h_1, h_2 とする。G の元 g_1, g_2 を $g_1 = (h_1, h_2^0)$,$g_2 = (h_1^0, h_2)$ と置く。G の残りの元は単位元 e と g_1g_2 なので演算表は次の様になる。

	e	g_1	g_2	g_1g_2
e	e	g_1	g_2	g_1g_2
g_1	g_1	e	g_1g_2	g_2
g_2	g_2	g_1g_2	e	g_1
g_1g_2	g_1g_2	g_2	g_1	e

上の演算表からも分かるように，群の演算表には特徴がある。各行にすべての元が出てきている。また各列に関しても同様である。

また群の同型については次が分かる。2 つの群 G と G' とが対応 $a_i \longleftrightarrow a_i'$ によって同型のとき，G' の演算表は G の演算表の a_i を a_i' に置き換えて得られる。