＜定義 1 ＞群

G を空でない集合とする。G 上の演算が定義されていて、次の性質をも満たすとき、G を群という。

(1) 単位元と呼ばれる元 $e \in G$ があり、すべての $a \in G$ に対し $ae = ea = a$ となる。

(2) すべての $a \in G$ に対し、$b \in G$ が存在し、$ab = ba = e$ となる。この元 b は a の逆元とよばれ、a^{-1} と書く。

(3) 全ての $a, b, c \in G$ に対し、$(ab)c = a(bc)$ が成り立つ。

それぞれ、単位元の存在、逆元の存在、結合法則の成立を言っている。以降、集合 G の単位元を 1_G と書く。

＜定義 2 ＞可換群

a, b が群 G の元で $ab = ba$ なら、a, b は可換であるという。G の任意の元 a, b が可換なら、G を可換群、アーベル群、加法群、加群などという。

＜定義 3 ＞群の位数

g が群であるとき、その元の個数 $|G|$ を G の位数をいう。位数が有限である群を有限群、有限でない群を無限群とよぶ。

[例 4]$G = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ は加法によって可換群であり、$G = \mathbb{Q}\backslash\{0\}, \mathbb{R}\backslash\{0\}, \mathbb{C}\backslash\{0\}$ は乗法について可換群である。

[例 5]G が群で $a, b, c \in G$ なら、次の $(1), (2)$ が成り立つ。

(1)$ab = ac$ なら、$b = c$

(2)$ab = c$ なら、$b = a^{-1}c, a = cb^{-1}$

[例 6] 次のことが成り立つ。

(1) 群の単位元は 1 つしかない。

(2)$a \in G$ に対し、その逆元は一意的に定まる。

(3)$a, b \in G$ なら、$(ab)^{-1} = b^{-1}a^{-1}$.

(4)$a \in$ なら、$(a^{-1})^{-1} = a$

[例 7]X を集合とするとき、全単射写像 $\sigma : X \to X$ のことを X の置換という。この X の置換全体は群となり、X の置換群という。$X_n = \{1, 2, ..., n\}$ とする n 次の置換群全体の n 次対象群 $\mathfrak{S}_n$ の位数は $n!$ となる。

[例 8] 実数を成分に持つ $n \times n$ 正則行列全体の集合を $GL_n(\mathbb{R})$ と書く。同様に複素数せ成分に持つものを $GL_n(\mathbb{C})$ と書く。どちらも群となり、まとめて一般線形群という。

<定義 9 >環
集合 A に二つの演算が定義されているとする。次の性質を満たすとき、A を環とよぶ。
(1)A は $+$ に関して可換群になる。
(2) 全ての $a, b, c \in A$ に対し、$(ab)c = a(bc)$.
(3) 全ての $a, b, c \in A$ に対し、

$$a(b+c) = ab + ac, \qquad (a+b)c = ac + bc.$$

(4) 乗法について単位元が存在する。

環は一方の演算で可換性が保証され、もう一方の演算で結合法則と分配法則が成り立つものである。乗法について可換でなくてもよく、逆元は存在しなくてもよい。乗法について可換である環 A を可換環という。また、乗法について a が逆元を持つとき、a を可逆元あるいは単元とよぶ。A の単元全体の集合を $A^{\times}$ と書く。

[例 10]A を環とするとき、次の $(1), (2)$ が成り立つ。
(1) 任意の $a \in A$ に対し、$0a = a0 = 0$ である。
(2)$1 = 0$ ならば、A は自明な環である。

[例 11]$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ は通常の加法と乗法で可換環である。
[例 12] 成分が実数である $n \times n$ 行列の集合を $M_n(\mathbb{R})$ とする。これは積について環である。

<定義 13 >可除環
集合 K に二つの演算 $+$ と $\times$ が定義されていて、次の条件を満たすとき K を可除環という。
(1) 二つの演算により、K は環になる。
(2) 任意の 0 でない $a \in K$ が乗法に関して可逆元である。

つまり、0 で割る以外の加減乗除ができる集合が可除環である。また、K が可除環で、環として可換なら、K を体という。

[例 14]$GL_n(\mathbb{R})$ について体でない。
[例 15]$\mathbb{Z}/n\mathbb{Z}$ は可換環である。

<定義 16 >部分群
G を群、$H \subset G$ を部分集合とする。H が G の演算によって群になるとき、H を G の部分群という。

[例 17] 群 G の部分集合 H が G の部分群になるための必要十分条件は、次の 3 条件が満たされることである。
(1)$1_G \in H$
(2)$x, y \in H$ なら、$xy \in H$
(3)$x \in H$ なら、$x^{-1} \in H$

[例 18]G が群なら、$\{1\}$ と G は明らかに G の部分群である。これらを G の自明な部分群という。

[例 19]$G=\mathbb{R}^{\times}$ とすると、$H=\{\pm 1\}$ は、G の部分群である。

[例 20]$G=GL_n(\mathbb{R})$,$H=\{g\in G|\det g=1\}$ と置く。H は G の部分群である。H のことを $SL_n(\mathbb{R})$ と書き、特殊線形群をよぶ。

[例 21]$G=GL_n(\mathbb{R})$、$H=\{g\in G|{}^tgg=I_n\}$ とおく。H は G の部分群となる。この H のことを $O(n)$ と書き、直交群をよぶ。また、$SO(n)=O(n)\cap SL_n(\mathbb{R})$ を特殊直交群をよぶ。

[例 22]$H=GL_n(\mathbb{Z})$ を $G=GL_n(\mathbb{R})$ の部分集合で、成分が整数であり、行列式が ± 1 であるもの全体の集合とする。このとき、H は G の部分群となる。また、$SL_n(\mathbb{Z})=GL_n(\mathbb{Z})\cap SL_n(\mathbb{R})$ とするとこれも部分群となる。それぞれはモジュラー群と呼ばれる。

＜定義 23 ＞語 (word)
G を群、$S\subset G$ を部分集合とする。$x_1,\cdots,x_n\in S$ により、$x_1^{\pm 1}\cdots x_n^{\pm 1}$ という形をした G の元を S の元による語 (word) という。

[例 24]$\langle S\rangle$ を S の元による語全体の集合とするとき、次が成り立つ。

(1)$\langle S\rangle$ は G の部分群である。

(2)H が G の部分群で S を含めば、$\langle S\rangle\subset H$ である。

＜定義 25 ＞元の位数
G を群、$x\in G$ とする。もし、$x^n=1_G$ となる正の整数が存在すれば、その中で最小のものを x の位数という。なければ、x の位数は ∞ である。

[例 26] 群の単位元は位数が 1 のただ一つの元である。

[例 27]$G=\mathfrak{S}_3,\sigma=(123)$ のとき、σ の位数は 3 である。$\mathfrak{S}_n$ の巡回置換 $(i_1\cdots i_m)$ の位数は m である。

[例 28]G が有限群なら、G の任意の元の位数は有限である。

[例 29]G を群、$x\in G$ とし、x の位数は有限で d とする。このとき、$n\in\mathbb{Z}$ に対し次の 2 つは同値である。

(1)$x^n=1_G$

(2)n は d の倍数である。

＜定義 30 ＞準同型、同型、カーネル、イメージ
G_1,G_2 を群、$\phi:G_1\to G_2$ を写像とする。

・$\phi(xy)=\phi(x)\phi(y)$ がすべての $x,y\in G_1$ に対し成り立つとき、ϕ を準同型という。

・ϕ が準同型で逆写像を持ち、逆写像も準同型であるとき、ϕ は同型であるという。このとき、G_1,G_2 は同型であるといい、$G_1\cong G_2$ と書く。

・ϕ が準同型のとき、$Ker(\phi)=\{x\in G_1|\phi(x)=1_G\}$ を ϕ の核という。

・ϕ が準同型のとき、$Im(\phi)=\{\phi(x)|x\in G_1\}$ を ϕ の像という。

[例 31] 全単射写像 $\phi:G_1\to G_2$ が群の準同型なら、同型である。

[例 32]$\phi:G_1\to G_2$ を群の準同型とするとき、次が成り立つ。

(1)$\phi(1_{G_1})=1_{G_2}$ である。

(2) 任意の $x \in G_1$ に対し、$\phi(x^{-1}) = \phi(x)^{-1}$ である。

(3)$Ker(\phi), Im(\phi)$ はそれぞれ G_1, G_2 の部分群である。

[例 33]G を群、$x \in G$ とする。$\mathbb{Z}$ を加法により群とみなす。$\mathbb{Z}$ かた G への写像 ϕ を $\phi(n) = x^n$ と定義する。ϕ は準同型である。

[例 34]$\mathbb{R}_> = \{r \in \mathbb{R} | r > 0\}$ とおく。$\mathbb{R}_>$ を乗法により、また $\mathbb{R}$ を加法により群とみなす。写像 $\phi : \mathbb{R} \to \mathbb{R}_>$ を $\phi(x) = e^x$ と定義する。このとき ϕ は同型である。

[例 35]$\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times$ を行列式とする。det は準同型である。

[例 36]$\mathbb{R}$ から $GL_2(\mathbb{R})$ への写像 ϕ を $\phi(u) = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$ と定義する。ϕ は準同型である。

[例 37]G_1, G_2 を群、$\phi_1, \phi_2 : G_1 \to G_2$ を準同型とする。もし G_1 が部分集合 S で生成されていて、$\phi_1(x) = \phi_2(x)$ がすべての $x \in S$ に対して成り立てば、$\phi_1 = \phi_2$ である。

[例 38]$\phi : G_1 \to G_2$ が準同型なら、次は同値である。

(1)ϕ は単射である。

(2)$\mathrm{Ker}(\phi) = \{1_{G_1}\}$

G_1, G_2 が群で $\phi : G_1 \to G_2$ が同型写像なら、G_1 に関する群論的性質は G_2 でも成り立つ。例えば G_1, G_2 の群、元の位数は一致する。

＜定義 39 ＞自己同型群

G を群とする。G から G への同型を自己同型という。G の自己同型全体を $\mathrm{Aut}G$ とかく。$\mathrm{Aut}G$ は群となる。この $\mathrm{Aut}G$ を G の自己同型群という。

[例 40]G を群、$g \in G$ とする。このとき、写像 $i_g : G \to G$ を $i_g(h) = ghg^{-1}$ と定義する。i_g は同型である。

＜定義 41 ＞内部自己同型

G を群とする。

・i_g という形をした群 G の自己同型のことを内部自己同型という。内部自己同型でない自己同型を外部自己同型という。

・$h_1, h_2 \in G$ とする。$g \in G$ があり $h_1 = gh_2g^{-1} = i_g(h_2)$ となるとき、h_1, h_2 は共役であるという。

G が可換群なら、すべての内部自己同型は恒等写像である。また、元 g と共役な元は g のみである。

[例 42]$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \begin{pmatrix} 4 & 3 \\ 2 & 1 \end{pmatrix}$ は共役である。

[例 43]G を群とするとき、写像 $\phi : G \to \mathrm{Aut}(G)$ を $\phi(g) = i_g$ と定義する。このとき、ϕ は準同型である。

＜定義 44 ＞同値関係

集合 S 上の関係 $\sim$ が次の関係を満たすとき、同値関係という。以下 a, b, c は S の任意の元を表す。

(1)$a \sim a$.

(2)$a \sim b$ なら $b \sim a$.
(3)$a \sim b$,$b \sim c$ なら $a \sim c$.

[例 45]" $=$ " は同値関係であるが " $\geq$ " は同値関係でない。

[例 46]$f : A \to B$ を集合 A から集合 B への写像とする。$x, y \in A$ に対し、$f(x) = f(y)$ であるとき $x \sim y$ と定義する。これは集合 A 上の同値関係となる。

[例 47] 正の整数 n を固定する。$x, y \in \mathbb{Z}$ に対し、$x - y$ が n で割り切れるとき $x \equiv y \mod n$ と定義する。このとき $x \equiv y \mod n$ は同値関係になる。

[例 48]G を群、$H \subset G$ を部分群とする。$x, y \in G$ に対し、$x^{-1}y \in H$ であるとき $x \sim y$ と定義する。このとき $x \sim y$ は同値関係である。

＜定義 49 ＞同値類
$\sim$ を集合 S 上の同値関係とする。$x \in S$ に対し、

$$C(x) = \{y \in S | y \sim x\}$$

を x の同値類という。つまり、上の定義で同値類とは x と同値関係にあるものすべてからなる集合である。