2010年6月29日

環には $+$ と $\times$ の２つの演算が定義されていた。例えば $\mathbb{Z}/5\mathbb{Z}$ の $+$ と $\times$ の表は

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

ただし、$0, 1, 2, 3, 4$ はそれぞれ $[0], [1], [2], [3], [4] \in \mathbb{Z}/5\mathbb{Z}$ を表す。下に、$\mathbb{Z}/4\mathbb{Z}$ の $+$ の表と、上の右の表から 0 を除いて $3, 4$ の順序を入れ替えた表を示す。

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times$	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

これら２つの表は本質的に同じであることがわかる。

集合 G に演算 $* : G \times G \to G$ が定義されていて、次の性質を満たすとき、$(G, *)$ は群 (group) であるという。

(1) $\forall a, b, c \in G,\ (a * b) * c = a * (b * c)$ （結合法則）

(2) $\exists e \in G,\ \forall a \in G,\ a * e = e * a = a$ （単位元の存在）

(3) $\forall a \in G,\ \exists b \in G,\ a * b = b * a = e$ （逆元の存在）

もし $*$ を指定しなくても他の演算と混乱することがないときは、単に G は群であるという。e を 1 または 0 と書くこともある。上の b は a^{-1} または $-a$ と書くことがある。

任意の環は、その加法 $+$ に関して群になる。

二つの群 $(G_1, *_1)$, $(G_2, *_2)$ に対して、全単射 $f : G_1 \to G_2$ が存在して $\forall x, y \in G_1$, $f(x *_1 y) = f(x) *_2 f(y)$ が成り立つとき、$(G_1, *_1)$ と $(G_2, *_2)$ は同型 (isomorphic) であるといい、$(G_1, *_1) \cong (G_2, *_2)$ または $G_1 \cong G_2$ と書く。上の２つの本質的に同じ表は

$$(\mathbb{Z}/4\mathbb{Z}, +) \cong (\mathbb{Z}/5\mathbb{Z} - \{[0]\}, \times)$$

を意味している。その他にも $(\mathbb{R}_{>0}, \times) \cong (\mathbb{R}, +)$ という同型もある。

群 G の元 a と整数 n に対して、

$$a^n = \begin{cases} a * a * \cdots * a \quad (n\text{ 個}) & (n \in \mathbb{N}) \\ e & (n = 0) \\ a^{-1} * a^{-1} * \cdots * a^{-1} \quad (n\text{ 個}) & (-n \in \mathbb{N}) \end{cases}$$

と定義すると、指数法則 $a^{n+m} = a^n * a^m$ が成り立つ。

G を群とし、その単位元を 1 と書くことにする。$x \in G$ に対し、

$$o(x) = \min\{n \mid n \in \mathbb{N},\ x^n = 1\}$$

を、元 x の位数という。ただし $\{n \mid n \in \mathbb{N},\ x^n = 1\} = \emptyset$ のときは x の位数は無限であるという。

群 G が有限集合のとき有限群という。$x \in G$ の位数は $|G|$ の約数であることがわかる。

$n \in \mathbb{N}$ とし、n 個の元からなる集合（例えば $X = \{1, 2, \ldots, n\}$）からそれ自身への全単射全体のなす集合を n 次対称群 (symmetric group) といい、S_n で表す。S_n は写像の合成に関して群をなす。単位元は恒等写像、逆元は逆写像である。恒等写像というのは、

$$\mathrm{id}(1) = 1, \quad \mathrm{id}(2) = 2, \ldots, \mathrm{id}(n) = n$$

で定義される X から X への写像である。一般には $|S_n| = n!$ である。例えば、$n = 3$, $X = \{1, 2, 3\}$ とすると、

$$f(1) = 2, \quad f(2) = 3, \quad f(3) = 1,$$
$$g(1) = 2, \quad g(2) = 1, \quad g(3) = 3$$

などが S_3 の元である。これらは順列と考えても良く、省略してそれぞれ 231, 213 と書くこともできる。写像の合成 $f \circ g$ とは $f \circ g(x) = f(g(x))$ によって定義される写像である。上記の f, g に対しては

$$f \circ g(1) = 3, \quad f \circ g(2) = 2, \quad f \circ g(3) = 1$$

となる。一般に、f, g が全単射ならば、$f \circ g$ も全単射である。したがって $\circ$ は S_n における演算となり、この演算に関して S_n は群になる。

S_n は線形代数学で習ったはず：$A = (a_{ij})$ を n 次正方行列とすると

$$\det A = \sum_{f \in S_n} \mathrm{sgn}(f) \prod_{i=1}^{n} a_{i,f(i)}$$

と表される。ここで

$$\mathrm{sgn}(f) = (-1)^{|\{(i,j) | i \in X,\ j \in X,\ i < j,\ f(i) > f(j)\}|}.$$

A を環とすると、A の元を成分とする n 次正方行列に、通常の行列の積を定義することができる。A が環であることから、A の元を成分とする行列の積は結合法則をみたし、A の単位元、零元から単位行列を作ることができる。これにより A の元を成分とする n 次正方行列全体の集合 $M(n, A)$ は環になる。

A を可換環とし、A の元を成分とする逆行列をもつような、$M(n, A)$ の元全体の集合を $GL(n, A)$ と書く。すなわち、

$$GL(n, A) = \{X \in M(n, A) \mid \exists Y \in M(n, A),\ XY = I\},$$

ただし I は n 次の単位行列を表す。$GL(n, A)$ は行列の積に関して群になる。

例えば、$n = 2$, $A = \mathbb{Z}/2\mathbb{Z}$ とすると

$$GL(2, \mathbb{Z}/2\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\}.$$

S_3 も $GL(2, \mathbb{Z}/2\mathbb{Z})$ も位数 6 の元を持たないので、$\mathbb{Z}/6\mathbb{Z}$ とは同型でない。