2008年7月18日

$GL(2, \mathbf{Z}/2\mathbf{Z})$ と S_3 の同型写像の作り方

$$\left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\} = \{v_1, v_2, v_3\}$$

とする（v_1, v_2, v_3 の定め方は $3! = 6$ 通りある）。$A \in GL(2, \mathbf{Z}/2\mathbf{Z})$ に対し、$f(A) \in S_3$ を

$$Av_i = v_{f(A)(i)}$$

で定めると、$f : GL(2, \mathbf{Z}/2\mathbf{Z}) \to S_3$ は同型写像になる。このようにして、6個の同型写像が得られる。

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

とすれば、A, B の位数はともに 2 である。従って、$f : GL(2, \mathbf{Z}/2\mathbf{Z}) \to S_3$ が同型写像ならば、$f(A), f(B)$ も位数が 2 でなければならない。S_3 には位数 2 の元が3つ（213, 321, 132）存在するので、$(f(A), f(B))$ の取り得る値は高々 6通りしかない。

$$GL(2, \mathbf{Z}/2\mathbf{Z}) = \{I, A, B, AB, BA, ABA\}$$

が確かめられるので、同型写像 f は $f(A), f(B)$ のみで定まり、従って同型写像の個数は高々 6 個しかない。一方、実際に 6 個の同型写像があることはすでに示したので、答えは 6 個である。

記号的な群の構成法

$(\mathbf{Z}/6\mathbf{Z}, +) \cong ((\mathbf{Z}/7\mathbf{Z})^{\times}, \times) = \{[3]^n \mid n \in \mathbf{Z}\}$ である。

$\mathbf{Z}$ から $\mathbf{Z}/6\mathbf{Z}$ を構成するには、合同式で定義された同値関係を用いた。これを一般的、かつ乗法的に書くと、無限巡回群 $G = \{a^n \mid n \in \mathbf{Z}\}$ に同値関係

$$a^{n_1} \sim a^{n_2} \iff n_1 \equiv n_2 \pmod m$$

を定義して、商集合に演算を定義したものと考えることができる。これは、a または a^{-1} が n 個続けて並んだら単位元なのでそこを消して良い、という規則であると解釈できる。

$GL(2, \mathbf{Z}/2\mathbf{Z})$ は巡回群ではない（位数 6 の元を持たない）ので、$(\mathbf{Z}/7\mathbf{Z})^{\times}$ のように表すことはできない。しかし、$A, B \in GL(2, \mathbf{Z}/2\mathbf{Z})$ を上記のように定めると、他の全ての元は A, B で表すことができる。A, B, AB の位数はそれぞれ、$2, 2, 3$ であるから、

$$A^2 = B^2 = (AB)^3 = 1$$

が成り立つ。実はこの式だけから、$\{I, A, B, AB, BA, ABA\}$ が群になることが導かれるのである。

同値関係の作り方

X を集合、$D \subset X \times X$ とするとき、$\hat{D} \subset X \times X$ を次で定義する。

$$\begin{aligned}\hat{D} = &\{(x,x) \mid x \in X\} \\ &\cup \{(x,y) \mid x \in X,\ y \in X, \\ &\quad \exists x_0, x_1, \dots, x_n \in X,\ x_0 = x,\ x_n = y, \\ &\quad\quad \forall i \in \{1, \dots, n\},\ (x_{i-1}, x_i) \in D \text{ or } (x_i, x_{i-1}) \in D\}.\end{aligned}$$

このとき、$\hat{D}$ は同値関係になる。

基本関係を用いた群の構成

a, b を無意味な記号とし、X を a, b からなる有限列全体の集合とする。長さ 0 の列を 1 で表し、これも X の元とする。X には自明な演算が定義されている。

$$\begin{aligned}D = &\{(w_1 w_2, w_1 aa w_2) \mid w_1 \in X,\ w_2 \in X\} \\ &\cup \{(w_1 w_2, w_1 bb w_2) \mid w_1 \in X,\ w_2 \in X\} \\ &\cup \{(w_1 w_2, w_1 ababab w_2) \mid w_1 \in X,\ w_2 \in X\}\end{aligned}$$

とおき、D の推移閉包 $\hat{D}$ による商集合 $X/\hat{D}$ に演算 $[w][w'] = [ww']$ を定義することができる（well-defined になる）。この演算により、$X/\hat{D}$ は群になり、しかも

$$X/\hat{D} = \{[1], [a], [b], [ab], [ba], [aba]\}$$

である。

同様にして、無意味な記号の集合

$$A = \{a_1, a_2, \dots, a_n, a_1^{-1}, a_2^{-1}, \dots, a_n^{-1}\}$$

に対し、A の元の有限列全体の集合 X を考えて、

$$X \supset R \supset \{a_i a_i^{-1} \mid i \in \{1, \dots, n\}\} \cup \{a_i^{-1} a_i \mid i \in \{1, \dots, n\}\}$$

を満たす R から

$$D = \{(w_1 w_2, w_1 r w_2) \mid w_1 \in X,\ w_2 \in X\}$$

を作ると、$X/\hat{D}$ は群になる。例えば、$A = \{a, b, c, a^{-1}, b^{-1}, c^{-1}\}$,

$$R = \{a^2, b^2, c^2, (ab)^3, (bc)^3, aa^{-1}, a^{-1}a, bb^{-1}, b^{-1}b, cc^{-1}, c^{-1}c, \}$$

とすると、$X/\hat{D} \cong S_4$ となる。

第 2 学期火曜日 2 講時藤原教授による「情報基礎数理学 IVb」ではこのようにして得られた群に関してさらに進んだ内容を講義する予定。

前回までに講義済みの内容

群

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）

上の b は a^{-1} または $-a$ と書くことがある。

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 と G_2 は同型であるといい、$G_1 \cong G_2$ と書く。

$n \in \mathbf{N}$ 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。

K を体とし、K の元を成分とする n 次正則行列全体の集合を $GL(n, K)$ と書く。$GL(n, K)$ は行列の積に関して群になる。例えば、$n = 2,\ K = \mathbf{Z}/2\mathbf{Z}$ とすると

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

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