2010年7月6日

$GL(2,\mathbb{Z}/2\mathbb{Z})$ 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）。$A\in GL(2,\mathbb{Z}/2\mathbb{Z})$ に対し、$f(A)\in S_3$ を

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

で定めると、$f:GL(2,\mathbb{Z}/2\mathbb{Z})\to S_3$ 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、$f:GL(2,\mathbb{Z}/2\mathbb{Z})\to S_3$ 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。

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

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

$A,B\in GL(2,\mathbb{Z}/2\mathbb{Z})$ 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、

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

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。

$\mathbb{Z}$ から $\mathbb{Z}/m\mathbb{Z}$ 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、$G=\{a^n\mid n\in\mathbb{Z}\}$ 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 m 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。a は $0,\pm1$ と異なる実数なら何でもよいが、a が実数でなくても形式的な記号と解釈することもできる。

基本関係を用いた群の構成

$R \subset X \times X$ を X 上の関係とし、

$$\bar{R} = \{(a,a) \mid a \in X\} \cup \{(a,b) \mid (a,b) \in R \text{ or } (b,a) \in R\}$$

とおくと、反射律、対称律をみたす。$\tilde{R}$ を、$\bar{R}$ の推移閉包とする。すなわち

$$\tilde{R} = \{(a,b) \in X \times X \mid \exists n \in \mathbb{N},\ \exists a_1, a_2, \ldots, a_n \in X,\ (a,a_1),(a_1,a_2),\ldots,(a_n,b) \in \bar{R}\} \\ \cup \bar{R}.$$

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。

$$\begin{aligned} R = &\{(w_1w_2, w_1aaw_2) \mid w_1 \in X,\ w_2 \in X\} \\ &\cup \{(w_1w_2, w_1bbw_2) \mid w_1 \in X,\ w_2 \in X\} \\ &\cup \{(w_1w_2, w_1abababw_2) \mid w_1 \in X,\ w_2 \in X\} \end{aligned}$$

とおき、$\bar{R}$ の推移閉包 $\tilde{R}$ による商集合 $X/\tilde{R}$ 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、$X/\tilde{D}$ は群になり、しかも

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

である。

同様にして、無意味な記号の集合

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

に対し、A の元の有限列全体の集合 X を考えて、

$$X \supset T \supset \{a_ia_i^{-1} \mid i \in \{1,\ldots,n\}\} \cup \{a_i^{-1}a_i \mid i \in \{1,\ldots,n\}\}$$

を満たす T から

$$R = \{(w_1w_2, w_1tw_2) \mid w_1 \in X,\ w_2 \in X,\ t \in T\}$$

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

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

とすると、$X/\tilde{R} \cong S_4$ となる。