離散数学レポート

010119:大和谷 潔

平成 12 年 7 月 6 日

問題 1

$(Z, *)$ が群にならないことを示せ。

解答

$Z \ni 0$ に対して $0 \cdot a = a \cdot 0 = 1$ となる $a \in Z$ は存在しない。すなわち、0 は逆元を持たない。よって $(Z, *)$ は群ではない。

問題 2

S_n が群になることを示せ。

解答

S_n が・で閉じている $A = \{1, 2, 3, \cdots, n\}, S_n \in \sigma, \tau$ とすると、σ は A 上の 1 対 1 対応であるので $\sigma(A) = A$。同様に $\tau(A) = A$。よって $\sigma\tau(A) = A$ であるので、$\sigma\tau$ も A 上の 1 対 1 対応である。よって S_n は・で閉じている。

結合法則 $S_n \in \sigma, \tau, \upsilon$ とすると、

$$(\sigma\tau)\upsilon(n) = (\sigma(\tau(\upsilon(n)))) = \sigma(\tau\upsilon)(n)$$

であるので結合法則を満たす。

単位元の存在 以下のような置換 i が単位元となる。

$$i = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}$$

逆元の存在

$$f = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ f(1) & f(2) & f(3) & \cdots & f(n) \end{pmatrix}$$

に対して以下のような置換が f の逆元として存在する。

$$f^{-1} = \begin{pmatrix} f(1) & f(2) & f(3) & \cdots & f(n) \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}$$

問題 3

S_2 が可換群になることを示せ。

解答

S_2 の元は

$$f = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, g = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

の二つしかない。

$$ff = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, gg = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, fg = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, gf = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

であり、

$$ff, gg, fg, gf \in S_2$$

である。よって S_n は・で閉じている。

問題 4

S_3 は可換群ではないことを示せ。

解答

以下のように $f, g \in S_3$ を定義すると、

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

次のように、$fg \neq gf$ である。よって S_3 は可換群ではない。

$$fg = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$gf = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

問題 5

G を群とするとき、$G \ni b$ に対して

$$(b^{-1})^{-1} = b$$

を示せ。

解答

$$\begin{aligned} (b^{-1})^{-1} &= 1 \cdot (b^{-1})^{-1} \\ &= (b \cdot b^{-1}) \cdot (b^{-1})^{-1} \\ &= b \cdot (b^{-1} \cdot (b^{-1})^{-1}) \\ &= b \cdot 1 \\ &= b \end{aligned}$$

問題 6

群 G に対し $< a >$ が部分群になることを示せ。

解答

$< a >$ が・で閉じている $a^i a^j = a^{i+j} \in < a >$ であるので、$< a >$ は・で閉じている。

単位元の存在 $a^0 a^k = a^k a^0 = a^k$ より、$a^0 \in < a >$ が単位元である。

逆元の存在 a^k に対して、$a^k a^{-k} = a^{-k} a^k = a^0$ より、逆元 $a^{-k} \in < a >$ が存在する。

以上より、$< a >$ は部分群である。