代数学１, 理解度チェック (余りの問題) の解答

担当：那須

1 (部分群) 次の群 G と部分集合 $H \subset G$ に対し, H が G の部分群になることを示せ.

(1) 対称群 $G = S_n$ において, 偶置換の全体の集合 $H = A_n$

(2) 乗法群 $G = GL(2, \mathbb{R})$ (実数を成分とする 2 次正則行列全体) と $H = SL(2, \mathbb{R})$ (実数を成分とする 2 次正方行列で行列式が 1 に等しいもの)

(3) 加法群 $G = \mathbb{R}^2$ (ベクトル空間 $\mathbb{R}^2$) と原点を通る傾き 2 の直線 $H = \left\{(x, y) \in \mathbb{R}^2 \,\middle|\, y = 2x\right\}$.

解答) 部分集合 H が G の部分群であることを示すには,

(i) H が G の演算で閉じていること,

(ii) H の任意の元の逆元が H に含まれること.

の 2 つを示せば良い.

(1) (i) $\sigma, \tau \in A_n$ とする. σ, τ はともに偶数個の互換の積として表されるので, 積 $\sigma\tau$ も偶数個の互換の積として表される. 従って $\sigma\tau \in A_n$.

(ii) $\sigma \in A_n$ とする. σ は偶数個の互換 $\tau_1, \ldots, \tau_{2n}$ の積として, $\sigma = \tau_1 \cdots \tau_{2n}$ と表される.

$$\sigma^{-1} = \tau_{2n}^{-1} \cdots \tau_1^{-1} = \tau_{2n} \cdots \tau_1$$

より, $\sigma^{-1} \in A_n$ となる.

(2) (i) $A, B \in SL(2, \mathbb{R})$ とする. 仮定より A, B の行列式の値は共に 1 に等しい. 従って, 積 AB の行列式の値は $|AB| = |A||B| = 1^2 = 1$ となり, $AB \in SL(2, \mathbb{R})$ となる.

(ii) $A \in SL(2, \mathbb{R})$ とする. A^{-1} を A の逆行列とする ($E = AA^{-1} = A^{-1}A$). このとき, $1 = |E| = |A||A^{-1}| = 1 \cdot |A^{-1}| = |A^{-1}|$ より, A^{-1} の行列式の値は 1 に等しい. 従って, $A^{-1} \in SL(2, R)$ となる.

(3) (i) 任意の H の元 (x, y) は実数 t を用いて, $(x, y) = (t, 2t)$ と表される. $(s, 2s), (t, 2t) \in H$ に対し, $(s, 2s) + (t, 2t) = (s + t, 2(s + t)) \in H$ より, $(s, 2s)$ と $(t, 2t)$ の和も H の元になる.

(ii) 任意の H の元 $(t, 2t)$ に対し, $-t \in \mathbb{R}$ より, G における逆元 $(-t, -2t) = (-t, 2(-t))$ も H の元である.

■

2 (置換, 対称群) 次の 4 次置換 $\sigma, \tau \in S_4$ に対し, (a)〜(d) の元を計算せよ.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$$

(a) $\sigma\tau$ (b) $\tau\sigma$ (c) σ^3 (d) τ^{-1}

解答) 答えのみ記す.

(a) $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ (b) $\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ (c) $\sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ (d) $\tau^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$

■

3 (1) 置換 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 6 & 3 & 1 & 8 & 5 & 7 & 9 & 2 \end{pmatrix} \in S_9$ をサイクルの分離積として表せ.

(2) σ を互換の積の形で表せ.

解答) (1) $\sigma = (1\ 4)(2\ 6\ 5\ 8\ 9)$ (2) $\sigma = (1\ 4)(2\ 6)(6\ 5)(5\ 8)(8\ 9)$ ■

4 次の置換の等式を示せ.

(1) 任意の i, j $(i, j \neq 1$ かつ $i \neq j)$ に対し, $(ij) = (1i)(1j)(1i)$

(2) 任意の i, j $(i, j \neq 1, 2$ かつ $i \neq j)$ に対し,

$$(1i)(12) = (12i), \quad (12)(1j) = (1j2) = (12j)^2, \quad (1i)(1j) = (12i)(12j)^2$$

解答) 2つの置換 σ, τ が等しい $(\sigma = \tau)$ という意味は, σ と τ が写像として等しい, すなわち任意の $k = 1, \ldots, n$ に対し, $\sigma(k) = \tau(k)$ が成り立つという意味である (問題 (1)). また $(a\ b\ c) = (a\ b)(b\ c)$ を用いて, 一方から他方へ式変形をして示しても良い (問題 (2)).

(1) $k \neq 1, i, j$ のとき, あきらかに $(ij)(k) = (1i)(1j)(1i)(k) = k$ が成り立つ. 一方, $i, j \neq 1$ より,

$$(1i)(1j)(1i)(1) = (1i)(1j)(i) = (1i)(i) = 1$$
$$(1i)(1j)(1i)(i) = (1i)(1j)(1) = (1i)(j) = j$$
$$(1i)(1j)(1i)(j) = (1i)(1j)(j) = (1i)(1) = i$$

が成り立つ. したがって任意の $k = 1, \ldots, n$ に対し, $(1i)(1j)(1i)(k) = (ij)(k)$ が成り立つ.

(2) 一般に互いに異なる $i_1, \ldots, i_k \in \{1, \ldots, n\}$ に対し, 長さ r のサイクル $(i_1 i_2 \ldots i_r)$ は,

$$(i_1\ i_2\ \cdots\ i_r) = (i_1\ i_2)(i_2\ i_3)\cdots(i_{r-1}\ i_r)$$

と隣接互換の積で表される (教科書 p.5 参照). 特に $(a\ b\ c) = (a\ b)(b\ c)$ が成り立つ.
したがって, 最初の等式については,

$$(1\ i)(1\ 2) = (i\ 1)(1\ 2) = (i\ 1\ 2) = (1\ 2\ i).$$

2つ目の等式については, $(1\ 2)(1\ j) = (2\ 1)(1\ j) = (2\ 1\ j) = (1\ j\ 2)$ と

$$(1\ 2\ j)^2 = (j\ 1\ 2)(1\ 2\ j) = (j\ 1)(1\ 2)(1\ 2)(2\ j) = (j\ 1)e(2\ j) = (1\ j\ 2)$$

から従う. 両者より

$$(1\ 2\ i)(1\ 2\ j)^2 = (1\ i)(1\ 2)(1\ 2)(1\ j) = (1\ i)(1\ 2)^2(1\ j) = (1\ i)e(1\ j) = (1\ i)(1\ j)$$

となり, 3つ目が従う.

■

5 (同型) 正三角形の対称群 $\mathrm{Sym}(\triangle)$ と3次対称群 S_3 が同型であること示せ. (両者の群表を書き, 一致することを示せばよい.)

解答) 3次対称群 S_3 の元を次のように定める.

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

$f : \mathrm{Sym}(\triangle) \to S_3$ を $f(I) = e$, $f(R_i) = \rho_i$ $(i = 1, 2)$, $f(T_j) = \tau_j$ $(j = 1, 2, 3)$ で定めると, 以下の表より, f は $\mathrm{Sym}(\triangle)$ から S_3 への準同型写像となる. 明らかに全単射であるため, f は同型である. ■

(a) S_3

a \ b	e	ρ_1	ρ_2	τ_1	τ_2	τ_3
e	e	ρ_1	ρ_2	τ_1	τ_2	τ_3
ρ_1	ρ_1	ρ_2	e	τ_3	τ_1	τ_2
ρ_2	ρ_2	e	ρ_1	τ_2	τ_3	τ_1
τ_1	τ_1	τ_2	τ_3	e	ρ_1	ρ_2
τ_2	τ_2	τ_3	τ_1	ρ_2	e	ρ_1
τ_3	τ_3	τ_1	τ_2	ρ_1	ρ_2	e

(b) Sym(△)

a \ b	I	R_1	R_2	T_1	T_2	T_3
I	I	R_1	R_2	T_1	T_2	T_3
R_1	R_1	R_2	I	T_3	T_1	T_2
R_2	R_2	I	R_1	T_2	T_3	T_1
T_1	T_1	T_2	T_3	I	R_1	R_2
T_2	T_2	T_3	T_1	R_2	I	R_1
T_3	T_3	T_1	T_2	R_1	R_2	I

6 同型

$$GL(2,\mathbb{R})/SL(2,\mathbb{R}) \simeq \mathbb{R}^\times$$

を示せ. ただし,

$$GL(2,\mathbb{R}) = \left\{ A \;\middle|\; A \text{ は } 2 \text{ 次正方行列で } \det(A) \neq 0 \right\},$$
$$SL(2,\mathbb{R}) = \left\{ A \;\middle|\; A \text{ は } 2 \text{ 次正方行列で } \det(A) = 1 \right\},$$
$$\mathbb{R}^\times = \mathbb{R} \setminus \{0\}.$$

とする.

解答) 群 $GL(2,\mathbb{R})$ から群 $\mathbb{R}^\times$ への写像 Φ を

$$\Phi : GL(2,\mathbb{R}) \longrightarrow \mathbb{R}^\times, \qquad A \longmapsto \det A$$

により定める. ただし $\det A$ は A の行列式を表す. 2 次正則行列 A, B に対し,

$$\Phi(AB) = \det(AB) = \det(A)\det(B) = \Phi(A)\Phi(B).$$

よって Φ は準同型写像となる. さらに Φ は全射である. 実際, 任意の $a \neq 0 \in \mathbb{R}$ に対し,

$$\Phi\left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}\right) = \det \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} = a.$$

である. 明らかに $\ker \Phi = \left\{ A \in GL(2,\mathbb{R}) \;\middle|\; \det A = 1 \right\} = SL(2,\mathbb{R})$. よって, 準同型定理より

$$GL(2,\mathbb{R})/SL(2,\mathbb{R}) \simeq \mathbb{R}^\times.$$

■

7 (1) 次の合同方程式を解け.

$$x^2 \equiv 1 \mod 35$$

(2) p, q を異なる 2 つの素数とする. 合同方程式

$$x^2 \equiv 1 \mod pq$$

の解を全て求めよ.

解答)

(1) $x^2 - 1 = (x-1)(x+1) = 0 \mod 5 \cdot 7$ は次の 4 つの連立合同方程式と同値である:

$$\begin{cases} x \equiv 1 \mod 5 \\ x \equiv 1 \mod 7 \end{cases} \quad \begin{cases} x \equiv 1 \mod 5 \\ x \equiv -1 \mod 7 \end{cases} \quad \begin{cases} x \equiv -1 \mod 5 \\ x \equiv 1 \mod 7 \end{cases} \quad \begin{cases} x \equiv -1 \mod 5 \\ x \equiv -1 \mod 7 \end{cases}$$

それぞれから, $x \equiv 1, x \equiv 6, x \equiv 29, x \equiv 34$ を得る.

(2) (1) と同様に, $x^2 \equiv 1 \mod pq$ は次の 4 つの合同方程式

$$\begin{cases} x \equiv 1 \mod p \\ x \equiv 1 \mod q \end{cases} \quad \begin{cases} x \equiv 1 \mod p \\ x \equiv -1 \mod q \end{cases} \quad \begin{cases} x \equiv -1 \mod p \\ x \equiv 1 \mod q \end{cases} \quad \begin{cases} x \equiv -1 \mod p \\ x \equiv -1 \mod q \end{cases}$$

と同値である. p と q は互いに素であるから, 拡張されたユークリッドの互除法により

$$pt_2 + qt_1 = 1$$

を満たす整数の組 (t_1, t_2) が存在する.

$$x = \pm 1 \cdot q \cdot t_1 \pm 1 \cdot p \cdot t_2 = \pm qt_1 \pm pt_2 \qquad \text{(複合任意)}$$

と置けば, $x \mod pq$ が求める解である.

■

8 (1) 合同方程式

$$19x^2 + 12x + 11 \equiv 0 \mod 21$$

を解け.

(2) 方程式 $7x^2 - 6y^2 = -1$ が整数解 (x, y) を持たない事を示せ. (ヒント：3 を法として $\mathbb{Z}/3\mathbb{Z}$ の世界で考えてみよう.)

解答)

(1) $21 = 3 \cdot 7$ より, 与えられた合同方程式は $19x^2+12x+11 \equiv 0 \mod 3$ または $19x^2+12x+11 \equiv 0 \mod 7$ と同値である. まず 3 を法として考えると, $(19 \equiv 1, 12 \equiv 0, 11 \equiv -1$ より$)$

$$19x^2 + 12x + 11 \equiv x^2 - 1 = (x+1)(x-1) \equiv (x-2)(x-1) = 0.$$

よって $x \equiv 1, 2 \mod 3$. 一方, 7 を法として考えると,

$$19x^2 + 12x + 11 \equiv 5x^2 - 2x - 3 = (5x+3)(x-1) \equiv 5(x+2)(x-1) \equiv 5(x-5)(x-1).$$

よって $x \equiv 1, 5 \mod 7$. 前問と同様に 4 つの連立合同方程式を解けば, $x \equiv 1, 5, 8, 19 \mod 21$ を得る.

(2) $7x^2 - 6y^2 \equiv x^2 \mod 3$ より, $7x^2 - 6y^2 = -1$ が整数解 (x, y) を持てば, 法 3 の下での還元

$$x^2 = 2 \mod 3$$

も $\mathbb{Z}/3\mathbb{Z}$ で解を持つ. しかし, 任意の $x \in \mathbb{Z}/3\mathbb{Z}$ に対し, $x^2 \equiv 0, 1 \mod 3$ であるから, これは矛盾.

■

[0]※この講義に関する情報はホームページを参照. https://fuji.ss.u-tokai.ac.jp/nasu/2024/alg1.html