雪江代数学 1(群論入門)：解答集

2021 年 7 月 27 日

目次

第 1 章の演習問題

1.1.1

▌ f が g, A が X, B が ${}^tXX$ にそれぞれ対応する.

1.1.2-(1)

▌ $f(S) = \{3, 4\}$

1.1.2-(2)

▌ $f^{-1}(S_1) = \varnothing$, $f^{-1}(S_2) = \{1, 3, 4, 5\}$

1.1.2-(3)

▌ $2 \in B$ であるが, $f(2) = \varnothing$ であるため, f は全射でない.

1.1.2-(4)

▌ $f(3) = f(5)$ であるが, $3 \neq 5$ であるため, f は単射でない.

第 2 章

2.3.3

Proof. H_1, H_2 は G の部分群ゆえ命題 2.3.2 より，$1_G \in H_1$ かつ $1_G \in H_2$．したがって，$1_G \in H_2 \cap H_2$．さらに，$a, b \in H_1 \cap H_2$ であるとき，$a, b \in H_1$ であるから，命題 2.3.2 より $ab \in H_1$．同様にして $ab \in H_2$．したがって，$ab \in H_1 \cap H_2$．$a \in H_1 \cap H_2$ とすると，$a \in H_1$ と命題 2.3.2 より $a^{-1} \in H_1$．同様に $a \in H_2$ より $a^{-1} \in H_2$．したがって，$a^{-1} \in H_1 \cap H_2$．以上より，命題 2.3.2 の (1)(2)(3) を $H_1 \cap H_2$ は満たすから，$H_1 \cap H_2$ は G の部分群. □

2.3.14

Proof. $S_1 \subset S_2$ ならば，S_1 のすべての元を S_2 が含むので，S_1 の元による語はすべて，S_2 の元から作れる．したがって，$\langle S_1 \rangle \subset \langle S_2 \rangle$ □

2.3.15

$\langle S \rangle = n\mathbb{Z}$ というのは，$\mathbb{Z}$ は演算を加法とする群であるから，$x^n = \underbrace{x + \cdots + x}_{n \text{ 個}} = nx$ ということになり，$\langle S \rangle = \{x^n \mid n \in \mathbb{Z}\} = \{nx \mid n \in \mathbb{Z}\}$ となる. [†1]

[†1] 冪 x^n の定義は定義 2.1.3 による.

2.3.20-(3)

$S = \{\sigma, \tau\}$ とすると，$\{\sigma\} \subset S$ かつ $\{\tau\} \subset S$ と命題 2.3.14 より，$\langle \sigma \rangle \subset \langle S \rangle$ かつ $\langle \tau \rangle \subset \langle S \rangle$．したがって $\langle \sigma \rangle \cup \langle \tau \rangle \subset \langle S \rangle$ となり，(1),(2) の結果と合わせて，回答のようになる.

2.3.22

$j = 1, \cdots, t$ に対し写像

$$i_j : G_j \ni g_j \mapsto (1_{G_1}, \cdots, 1_{G_{j-1}}, g_j, 1_{G_{j+1}}, \cdots, 1_{G_t}) \in G_1 \times \cdots \times G_t$$

を考えると，これは単射であるから，G_j を $G_1 \times \cdots \times G_t$ の部分集合とみなせるというのは，写像の終域 $G_1 \times \cdots \times G_t$ の部分集合の元に対して，G_j の元がただ一つ対応するということから，G_j を $G_1 \times \cdots \times G_t$ の部分集合と “みなす” ことができるということ.

2.4.4

Proof. $n \in \mathbb{Z}$ に対して $r(n)$ を以下で定義する. †1

$$r(n) = \begin{cases} (n \text{ を } m \text{ で割った余り}) & (n \notin m\mathbb{Z}) \\ m & (n \in m\mathbb{Z}) \end{cases}$$

$\sigma = (i_1 \cdots i_m)$ とすると，σ により i_j は $i_{r(j+1)}$ に移る．ある $n \in \mathbb{N}$ に対して σ^n によって i_j は $i_{r(j+n)}$ に移るとすると，σ^{n+1} によって i_j は $i_{r(j+n+1)}$ に移る．数学的帰納法により，σ^n によって i_j は $i_{r(j+n)}$ に移る．ここで，$j = r(j+n)$ を満たす最小の自然数 n は m である．これは，$1 \leq j \leq m$ の任意の j に対して成立する．したがって，σ の位数は m である. □

†1 $j = m$ だったりすると，i_{j+1} に移るわけではないので，そういったものを防ぐために r を導入した.

2.4.17

ここでの群は，加法による群である．$d \in H$ ならば $d + d \in H$ である．これを繰り返せば $d^q = qd \in H$ である．H は $\mathbb{Z}$ の部分群であるから，$(d^q)^{-1} = -qd \in H$ である．よって，$n \in H$ ならば $r = n + (-qd) = n - qd \in H$ である．ところで，r は $0 \leq r < d$ を満たすものであるので，$r \neq 0$ とすると d 未満の正整数が H の元としてあることになって，d の取り方に矛盾する．よって，$r = 0$ であるから，$n = qd \in d\mathbb{Z}$ となり，$n \in H$ ならば $n \in d\mathbb{Z}$ である．したがって，$H \subset d\mathbb{Z}$. †1

Proof. ($H \supset d\mathbb{Z}$ の証明) $n \in d\mathbb{Z}$ とすると，$d\mathbb{Z} = \langle \{d\} \rangle$ であり，$d \in H$ ゆえ，$\{d\} \subset H$ である．また，命題 2.3.13 より $\{d\} \subset H$ ならば $\langle \{d\} \rangle \subset H$ である．したがって，$d\mathbb{Z} \subset H$ である. □

$H \subset d\mathbb{Z}$ かつ $H \supset d\mathbb{Z}$ より $H = d\mathbb{Z}$

†1 $H \supset d\mathbb{Z}$ は明らかなのか，証明が省かれている.

第 2 章の演習問題

2.1.1

1 が単位元である．0 に逆元がないことがわかる．したがって，G は演算 $\cdot$ により群とならない.

2.1.2

0 が単位元である．$a + b + ba = 0$ とすると，$a \neq -1$ のときは $b = -\frac{a}{1+a}$ となるが，$a = -1$ のときは任意の $b \in \mathbb{R}$ に対して $a + b + ab = -1$ となるため，-1 の逆元が存在しない．したがって，$\mathbb{R}$ は演算 $\circ$ により群とならない. †1

†1 結合法則は成立している.

2.1.4

$((ab)c)d = (a(bc))d = a((bc)d)$

2.2.2

(3)　39 を法とする合同式を使うと

$$\begin{aligned}
16^8 &= (13+3)^8 \\
&\equiv 13^8 + 3^8 && (\text{これら以外の項は } 13 \text{ と } 3 \text{ の両方を因数に持つ}) \\
&\equiv 13(12+1)^7 + 3^2 \cdot 27 \cdot 27 \\
&\equiv 13 + 3^2(13\cdot 2+1)(13\cdot 2+1) && ((12+1)^7 \text{を展開すると，} 1 \text{ 以外の項は全て } 3 \text{ を因数に持つ}) \\
&\equiv 13 + 3^2 \cdot 1 = 22
\end{aligned}$$

となる．ここから答えがわかる．

(4)　(3) と同様に計算を行うと

$$\begin{aligned}
16^{34} &= (13+3)^{34} \\
&\equiv 13^{34} + 3^{34} \\
&\equiv 13(12+1)^{33} + 3(13\cdot 2+1)^{11} \\
&\equiv 13 + 3 = 16
\end{aligned}$$

となる．ここから答えがわかる．

2.3.1

Proof. H が G の部分群であることと同値な条件は命題 2.3.2 から，

$$\begin{cases} ① & 1_G \in H \\ ② & \forall x, \forall y \in H\,,\, xy \in H \\ ③ & \forall x\,,\, x^{-1} \in H \end{cases}$$

である．これを用いて証明する．

$\Longrightarrow$ の証明：② と③ より H が G の部分群であれば，任意の $x, y \in H$ に対して $x^{-1}y \in H$

$\Longleftarrow$ の証明：任意の $x \in H$ に対して $x^{-1}x = 1_G \in H$ である (①)．$1_G \in H$ より，任意の $x \in H$ に対して $x^{-1}1_G = x^{-1} \in H$ である (③)．任意の $x \in H$ に対して $x^{-1} \in H$ であるから，任意の $x, y \in H$ に対して $(x^{-1})^{-1}y = xy \in H$ である (②)．　□

2.3.2

Proof. まずは，命題 2.3.2 を使って考えてみる．$G = \mathrm{GL}_{2n}(\mathbb{R})$ とする．[†1] 単位行列 $I_{2n} = 1_G \in G$ は ${}^tI_{2n}J_nI_{2n} = J_n$ を満たすから，$1_G \in \mathrm{Sp}(2n)$ である．また，$A, B \in \mathrm{Sp}(2n)$ とすると，

$$ {}^t(AB)J_n(AB) = {}^tB{}^tAJ_nAB = {}^tBJ_nB = J_n $$

となるから，$AB \in \mathrm{Sp}(2n)$ である．また，$A \in \mathrm{Sp}(2n)$ とすると

$$ {}^t(A^{-1})J_nA^{-1} = ({}^tA)^{-1}J_nA^{-1} = ({}^tA)^{-1}{}^tAJ_nAA^{-1} = J_n $$

となるから，$A^{-1} \in \mathrm{Sp}(2n)$ である． □

Proof. 次に，演習問題 2.3.1 の必要十分条件を使って考えてみる．$1_G \in \mathrm{Sp}(2n)$ より，$\mathrm{Sp}(2n)$ は空でない G の部分集合である．$A, B \in \mathrm{Sp}(2n)$ とすると

$$ {}^t(A^{-1}B)J_n(A^{-1}B) = {}^tB{}^t(A^{-1}){}^tAJ_nAA^{-1}B = {}^tB({}^tA)^{-1}{}^tAJ_nB = {}^tBJ_nB = J_n $$

となるから，$A^{-1}B \in \mathrm{Sp}(2n)$ である． □

[†1] P31 例 2.3.9 によると，$\mathrm{Sp}(2n) = \mathrm{Sp}(4n, \mathbb{R})$ となるはずだが，$\mathrm{GL}_{2n}(\mathbb{R})$ の部分群になるためにはそんな訳ないので，ここでは $\mathrm{Sp}(2n) = \mathrm{Sp}(2n, \mathbb{R})$ と考える．

2.3.3

Proof. 命題 2.3.2 を使って考える．$G = \mathrm{GL}_n(\mathbb{C})$ とする．単位行列 $I_n = 1_G \in G$ は ${}^t\bar{I}_nI_n = {}^tI_nI_n = I_n$ を満たすから，$1_G \in \mathrm{U}(n)$ である．また，$A, B \in \mathrm{U}(n)$ とすると，

$$ {}^t(\bar{A}\bar{B})(AB) = {}^t\bar{B}{}^t\bar{A}AB = {}^t\bar{B}B = I_n $$

となるから，$AB \in \mathrm{U}(n)$ である．また，$A \in \mathrm{U}(n)$ とすると，

$$ {}^t\overline{A^{-1}}A^{-1} = {}^t\overline{A^{-1}}I_nA^{-1} = \overline{{}^tA}^{-1}{}^t\bar{A}AA^{-1} = I_n $$

となるから，$A^{-1} \in \mathrm{U}(n)$ である． □

Proof. 演習問題 2.3.1 の必要十分条件を使って考える．$1_G \in \mathrm{U}(n)$ より，$\mathrm{U}(n)$ は空でない G の部分集合である．$A, B \in \mathrm{U}(n)$ とすると

$$ {}^t(\overline{A^{-1}B})(A^{-1}B) = {}^t\bar{B}{}^t(\overline{A^{-1}})I_nA^{-1}B = {}^t\bar{B}\,({}^t\bar{A})^{-1}{}^t\bar{A}AA^{-1}B = {}^t\bar{B}B = I_n $$

となるので，$A^{-1}B \in \mathrm{U}(n)$．ただし，共役を取ってから逆行列を求めても，逆行列を求めてから共役を取っても変わらず[†1]，共役を取ってから転置を取っても，転置をとってから共役を取っても変わらないことを用いた． □

[†1] 行列式の計算は和と積のみで，余因子を求めるときにも和と積の計算しかしない．任意の複素数 z, w に対して $\overline{zw} = \bar{z}\bar{w}$ で，$\overline{z + w} = \bar{z} + \bar{w}$ であることからこれがわかる．