群論 (第5回) の解答

問題 5-1 の解答

S_4 の任意の元は互換の積で表せるので, $< S >= S_4$ を示すには各互換が S の元の積で表せることを言えばよい. 実際, S_4 の互換は $(1\ 2)$, $(1\ 3)$, $(1\ 4)$, $(2\ 3)$, $(2\ 4)$, $(3\ 4)$ の 6 つであり,

$$(2\ 3) = (1\ 2)(1\ 3)(1\ 2),\quad (2\ 4) = (1\ 2)(1\ 4)(1\ 2),\quad (3\ 4) = (1\ 3)(1\ 4)(1\ 3).$$

以上より S_4 の互換は $(1\ 2)$, $(1\ 3)$, $(1\ 4)$ の積でかける. よって $S_4 =< S >$.

問題 5-2 の解答

x の位数を n とすると, $n = 2m - 1$ $(m \in \mathbb{N})$ と表せる. $x^{2m-1} = 1_G$ より

$$x = x \cdot x^{2m-1} = (x^2)^m \in < x^2 > .$$

従って $< x > \subseteq < x^2 >$. 逆の包含は明らか.

問題 5-3 の解答

G は巡回群より, $G =< x >$ を満たす $x \in G$ が取れる. $y, z \in G$ を取り, $y = x^m$, $z = x^n$ $(m, n \in \mathbb{Z})$ で表す. このとき,

$$y \cdot z = x^m \cdot x^n = x^{m+n} = x^{n+m} = x^n \cdot x^m = z \cdot y.$$

従って G はアーベル群である.

問題 5-4 の解答

H を巡回群 G の部分群とする. G は巡回群より, $G =< x >$ を満たす $x \in G$ がある. $H = \{1_G\}$ なら問題ないので, $H \neq \{1_G\}$ の場合を考える. $x^n \in H$ を満たす最小の自然数 n を取ると, H は G の部分群より $< x^n > \subseteq H$. 逆に $y \in H$ を取ると, $y \in G$ より $y = x^m$ $(m \in \mathbb{Z})$ と表せる. ここで, $m = qn + r$ $(0 \leq r < n)$ を満たす整数 q, r を取ると,

$$x^r = x^m \cdot (x^n)^{-q} = y \cdot (x^n)^{-q} \in H.$$

n の最小性から $r = 0$ でなければならない. よって $y = x^m = (x^n)^q \in < x^n >$. これより $< x^n >= H$ を得る.