

問3. 7

(i) $a \equiv a$.

(ii) $a \equiv b \Rightarrow b \equiv a$.

(iii) $a \equiv b, b \equiv c \Rightarrow a \equiv c$.

の3つを示す.

(i) $H \leq G$ より, G の単位元を e とすると, $e \in H$.

よって, $a \circ e = a$.

$\therefore a \equiv a$.

(ii) $a \equiv b$ より, $\exists h \in H, a \circ h = b$①

$H \leq G$ より, $h^{-1} \in H$.

これを①の両辺に右から掛けると,

$$b \circ h^{-1} = (a \circ h) \circ h^{-1} = a \circ (h \circ h^{-1}) = a \circ e = a.$$

$\therefore b \equiv a$.

(iii) $a \equiv b$ より, $\exists h_1 \in H, a \circ h_1 = b$. $b \equiv c$ より, $\exists h_2 \in H, b \circ h_2 = c$.

$H \leq G$ より, $h_1 \circ h_2 \in H$.

よって, $c = b \circ h_2 = (a \circ h_1) \circ h_2 = a \circ (h_1 \circ h_2)$.

$\therefore a \equiv c$. Q.E.D.

問3. 8

(1)

$|1| = 1$.

$2^1 = 2, 2^2 = 4, 2^3 = 3, 2^4 = 1$ より, $|2| = 4$.

$3^1 = 3, 3^2 = 4, 3^3 = 2, 3^4 = 3^3 \times 3 = 6 = 1$ より, $|3| = 4$.

$4^1 = 4, 4^2 = 1$ より, $|4| = 2$.

よって, $Z_5^* = \langle a \rangle$ となる $a \in Z_5^*$ として, $a = 2, 3$ があるので, Z_5^* は巡回群である. Q.E.D.

(2)

部分群を H とする.

$H \leq Z_5^*$ より, $|H| \mid |Z_5^*| = 4$.

$\therefore |H| = 1, 2, 4$. また, 単位元は $1 \in H$.

$|H| = 1$ のとき, $H = \{1\}$.

$|H| = 2$ のとき, $H = \{1, a\}$.

(G3) より, $a^{-1} \in H$.