

問3. 1

(1)

G の単位元を e, e' とすると,

$e = e \circ e' = e'$ ($\because$ 左のイコールは e' が単位元より, 右のイコールは e が単位元より.).

$\therefore$ 単位元は唯一である.

(2)

$a \in G$ の逆元を a^{-1}, a'^{-1} , 単位元を e とすると,

$$a^{-1} \circ a = e$$

$$\Rightarrow (a^{-1} \circ a) \circ a'^{-1} = e \circ a'^{-1}$$

$$\Rightarrow a^{-1} \circ (a \circ a'^{-1}) = a'^{-1}$$

$$\Rightarrow a^{-1} \circ e = a'^{-1}$$

$$\Rightarrow a^{-1} = a'^{-1}.$$

$\therefore$ 逆元は唯一である.

問3. 2

(1)

(G0) が成り立つのは明らか.

(G1) は両辺も abc を n で割った余りを考えているので, 成り立つ.

(G2) は $e = 1$ とすることで成り立つ.

(G3) を示す.

$$a \in \mathbb{Z}_n^* \Rightarrow \gcd(a, n) = 1 \Rightarrow \exists a^{-1} \in \mathbb{Z}_n^* (\because [2. 2. 1]).$$

$\therefore$ 群になる.

(2)

(G3) が成り立たないことを示す.

すなわち, $n = a, b$ ($1 < a, b \in \mathbb{N}$) のとき, $a^{-1} \notin \mathbb{Z}_n^*$ であることを示す.

もし, $c = a^{-1} \in \mathbb{Z}_n^*$ ならば, $ac = 1$ であるので,

$$b = (ac)b = cn \equiv 0 \pmod{n}.$$

よって, $b = 0$ であるが, これは矛盾.

$\therefore$ 群でない.

問3. 3

(1)

単位元は $e = 0$.

0 の逆元は 0, $a \in \mathbb{Z}_n^*$ の逆元は $n - a \in \mathbb{Z}_n^*$.

(2)

(G0) を示す.