

4.7.1

H, K をそれぞれ G の  $2$ -Sylow 部分群S, t をそれぞれ  $2$ -Sylow 部分群の代表元とせよ。 $2$ -Sylow の定理よりS は  $P$  の約数  $63$ .  $S \equiv 1 \pmod{2}$ t は  $2$  の約数  $63$ .  $t \equiv 1 \pmod{P}$  $P$  は奇素数より $t \equiv 1 \pmod{P}$  より $k < G$  を意味するまた  $2$  は  $1$  より  $S = 1, P$  と  $2$  の積  $S = 1$  と  $2$  と  $H \triangleleft G$  となり位数より  $H \cap K = \{1\}$ ,  $HK = G$  であるが,  $P$  の定理 2.9.2 より

$$G \cong H \times K \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/P\mathbb{Z}$$

これは  $G$  が非可換であることに矛盾するので  $S = P$  となるよって  $P$  を  $2$  と  $63$  の積  $P$  は正規部分群,  $H$  は正規部分群であるということができる。また  $H \cong \mathbb{Z}/2\mathbb{Z}$ ,  $K \cong \mathbb{Z}/P\mathbb{Z}$  である。 $K$  は正規部分群なので  $HK$  は部分群  $HK \supset H, K$  より位数より  $HK = G$  となる。

$$K \cong \mathbb{Z}/P\mathbb{Z} \text{ より } \exists t \in K, K = \langle t \rangle$$

 $H$  の元  $h$  が  $t$  と可換であることより,  $H$  の元は  $K$  の元と可換になる。よって  $G = HK$  より  $g, g' \in G$  に対して  $g = hk, g' = h'k'$  となる。 $h, h' \in H, k, k' \in K$  が存在し

$$gg' = hk h' k'$$

$$= h h' k k'$$

(仮定より)

$$= h' h k' k$$

 $(H \cong \mathbb{Z}/2\mathbb{Z}, K \cong \mathbb{Z}/P\mathbb{Z} \text{ より})$ 

$$= k' k h k$$

(仮定より)

$$= g' g \text{ となり}$$

 $G$  は可換群となるので矛盾(1) から  $H$  の元  $h$  の  $2$  のべき乗  $h^2 = 1$  となる  $h$  は非可換である。これを  $r \in H$  とおくと

$$\text{明らかに } r \neq 1 \text{ であり } r^2 = 1$$

 $K \triangleleft G$  より  $r$  は  $K$  を非可換に作用する  $r t r^{-1} = t^i$  ( $i \in \mathbb{Z}, 2 \leq i \leq P-1$ ) が成り立つ。さらに  $r$  は  $K$  上の作用  $t \mapsto t^i$  とおくと

$$t = t^{i^2} \Leftrightarrow t^{i^2-1} = 1 \text{ となる}$$

$$i^2 - 1 \equiv 0 \pmod{P} \Leftrightarrow (i-1)(i+1) \equiv 0 \pmod{P}$$

 $\mathbb{Z}/P\mathbb{Z}$  は体の  $P$  の  $\mathbb{Z}$  上の剰余環であるから  $i-1 \neq 0$  より  $i+1 \equiv 0 \pmod{P}$ よって  $i \equiv -1 \pmod{P}$  となり  $r t r^{-1} = t^{-1}$  を意味するこの  $r$  の議論より  $r$  は関係式  $r^2 = 1, r t r^{-1} = t^{-1}$  を満たす。よって  $L = \langle x, y \mid x^P = y^2 = 1, y x y^{-1} = x^{-1} \rangle$  とおくと $L$  から  $G$  の全射準同型が存在する。さらに  $|L| \geq |G|$  であるが  $L$  の関係式より $L$  の元は  $y^j x^i$  ( $i = 0, 1, j = 0, \dots, P$ ) の形で表され  $2P = |G| \leq |L|$

いかにして

$G \cong L$ , 同様にして,  $L \cong D_p$  を示せばいい

$G \cong D_p$  となり 題意は示された.

(\*) の議論について

自分の解答では  $\mathbb{F}_p$  の体で  $\alpha$  を使ったが.

体論はまだ習っていない前提なので止めてかう.

その場合の別解を以下に示す.

$r$  の位数は  $2$  か  $p$  のどちらかである.

(1)  $r \neq 2$   $r \in H \cap K = \{1\}$  と矛盾,  $2p$  と  $2$  は非可換であるから.

$r$  の位数が  $p$  だとすると,  $K$  は唯一の  $(p-1)$ -部分群より

$r \in K$ . 故に  $rc = cr$  ( $c \in N$ ) が成り立つ.

しかし  $r \in H \cap K = \{1\}$  が示さるので矛盾.

ゆえに  $r$  の位数は  $2$  かつ  $(rc)^2 = 1$  が成り立つ

$rcrc = 1$  より

$rcr^{-1} = c^{-1}$  が示せる