Problema 38. Siguin n un nombre enter i d un divisor propi de n. Demostreu que el subgrup (ρ^d) de D_{2n} és un subgrup normal i que el grup quocient és isomorf a D_{2d}.

Nota 1: Un subgrup $H \subseteq G$ és normal quan se satisfà que $aHa^{-1} = H$, $\forall a \in G$.

Nota 2: $D_{2n} = \langle \rho, \sigma : \rho^n = \sigma^2 = Id, \sigma\rho\sigma = \rho^{-1} \rangle$.

Solució. Sabem que

$D_{2n} = \{Id, \rho, \rho^2, ..., \rho^{n-1}, \sigma, \sigma\rho, \sigma\rho^2, ..., \sigma\rho^{n-1}\}$ i $\langle \rho^d \rangle = \{Id, \rho^d, \rho^{2d}, ..., \rho^{(\frac{n}{d}-1)d}\}$, que té n/d elements.

Volem veure que $\langle \rho^d \rangle \triangleleft D_{2n}$.

Considerem $a \in D_{2n}$. Si demostrem que $a(\rho^d)a^{-1} = (\rho^d)^{k\prime}$, serà evident que $a(\rho^d)^k a^{-1} = (\rho^d)^{kk'}$, ja que $a(\rho^d)^k a^{-1} = a\rho^d \dots \rho^d a^{-1} = a\rho^d a^{-1} a\rho^d a^{-1} \dots a\rho^d a^{-1} = ((\rho^d)^{k\prime})^k = (\rho^d)^{kk'}$, i per tant $(\rho^d)^{kk'} \in \langle \rho^d \rangle$.

D_{2n} està format per dos tipus d'elements: ρ^k i $\sigma\rho^k$, per $k = 1, ..., n$.

Suposem que l'element a és del tipus ρ^k; llavors,

$$\rho^k \rho^d (\rho^k)^{-1} = \rho^k \rho^d \rho^{n-k} = \rho^d \in \langle \rho^d \rangle$$

.

Suposem que l'element a és del tipus $\sigma\rho^k$; llavors,

$$\sigma\rho^k \rho^d (\sigma\rho^k)^{-1} = \sigma\rho^k \rho^d \rho^{-k} \sigma = \sigma\rho^d\sigma = \sigma^2 \rho^{-d} = \rho^{-d} = (\rho^d)^{\frac{n}{d}-1} \in \langle \rho^d \rangle$$

.

Per tant, $\langle \rho^d \rangle$ és un subgrup normal de D_{2n}.

Ara veiem que el grup quocient és isomorf a D_{2d}.

Considerem

$$\begin{aligned} f : D_{2n} &\longrightarrow D_{2d} \\ \rho^k &\longmapsto \rho'^k \\ \sigma\rho^k &\longmapsto \sigma\rho'^k \end{aligned}$$

Hem de veure que f està ben definida:

$\rho^k = \rho^{k'} \Longleftrightarrow k - k' \equiv 0 (mod\ n)$

$f(\rho^k) = \rho'^k$

$f(\rho^{k'}) = \rho'^{k'}$

$k - k' \equiv 0 (mod\ n) \Longrightarrow \rho'^k = \rho'^{k'}$ a D_{2d}.

$\sigma\rho^k = \sigma\rho^{k'} \Longrightarrow \sigma\sigma\rho^k = \sigma\sigma\rho^{k'} \Longrightarrow \rho k = \rho^{k'} \Longrightarrow \rho'^k = \rho'^{k'}$.

$f(\sigma\rho^k) = \sigma\rho'^k = f(\sigma\rho^{k'}) = \sigma\rho'^{k'}$.

Ara hem de veure que f és un morfisme:

$f(\rho^k\rho^{k'}) = f(\rho^{k+k'}) = \rho'^{k+k'} = f(\rho^k)f(\rho^{k'})$.

$f(\sigma\rho^k\sigma\rho^{k'}) = f(\sigma\rho^k rho^{-k'}\sigma) = f(\sigma\rho^{k-k'}\sigma) = f(\sigma\sigma\rho^{k'-k}) = f(\rho^{k'-k}) = \rho'^{k'-k} = f(\sigma\rho^k)f(\sigma\rho^{k'})$.

$f(\sigma\rho\rho^{k'}) = f(\sigma\rho^{k+k'}) = \sigma'\rho'^{k+k'} = f(\sigma\rho^k)f(\rho^{k'})$.

$f(\rho^k\sigma\rho^{k'}) = f(\rho^k rho^{-k'}\sigma) = f(\rho^{k-k'}\sigma) = \rho^{k-k'}\sigma = f(\rho^k\sigma)f(\rho^{k'})$.

f és exhaustiu: D_{2d} té dos tipus d'elements: ρ'^k, que és imatge de ρ^k, i $\sigma\rho^k$, que és imatge de $\sigma\rho^k$. Per tant, $Imf = D_{2d}$.

$f(\rho^k) = \rho'^k = Id \Longrightarrow k$ és un múltiple de d. Per tant, el $Kerf = \rho^d, \rho^{2d}, ..., \rho^n = Id = < \rho^d >$.

Per tant, el grup quocient és isomorf a D_{2d}.