Lista 4

Zad 4K

G: grupa, $g \in G$, $ord(g) = n \in \mathbb{N}_{>1}$, $k \in \mathbb{N}$, $r = r_n(k)$

(a) $g^k = g^r$

$r = r_n(k) \Rightarrow \exists t \in \mathbb{Z} \quad k = tn + r$

$$g^k = g^{tn+r} = (g^n)^t g^r \overset{n=ord(g)}{=\!=} e^t g^r = e g^r = g^r .$$

(b) $ord(g^k) = l$, gdzie $l := \min\{m > 0 : \underset{ord(g)}{n} \mid km\}$.

Lista 3 Zad 4(c) $\Rightarrow \forall t \in \mathbb{Z} \quad g^t = e \iff n \mid t$

$\Downarrow$ biorąc $t = km$

$g^{km} = e \iff n \mid km$

$\Rightarrow ord(g^k) = \min\{m > 0 : \underbrace{(g^k)^m}_{g^{km}} = e\} = \min\{m>0 : n \mid km\} = l$

(c) $ord(g^k) = \frac{n}{NWD(k,n)}$

Z (b) wystarczy pokazać: $\min\{m > 0 : n \mid km\} \overset{?}{=} \frac{n}{NWD(k,n)}$

Przygotowania

Niech $n = NWD(k,n) n'$ $\quad (n' = \frac{n}{NWD(k,n)})$

$k = NWD(k,n) k'$ $\quad k' \in \mathbb{N}_{>0}$

Wtedy $NWD(k', n') = 1$ (względnie pierwsze)

Teraz dowód. Weźmy $m > 0$.

$n \mid km \iff \underbrace{NWD(k,n)n'}_{n} \mid \underbrace{NWD(k,n)k'}_{k} m \iff n' \mid k'm$

Ale $NWD(k',n') = 1$, czyli $n' \mid k'm \iff n' \mid m$

Czyli $\underset{z\,(b)}{l} = \min\{m > 0 : n \mid km\} = \min\{m > 0 : n' \mid m\} = n' = \frac{n}{NWD(k,n)}$.

(d) $ord(g^k) = n \iff NWD(k,n) = 1$

(c) $\Rightarrow ord(g^k) = \frac{n}{NWD(k,n)} = n \iff NWD(k,n) = 1$ OK.

Mamy wniosek

$k \mid n \Rightarrow ord(g^k) = \frac{n}{k}$ i $ord(g^{\frac{n}{k}}) = k$.

$(ord(g) = n)$

ZAD 5K

Wyznaczyć wszystkie możliwe rzędy elementów D_n.

[$|G| = m \Rightarrow$ rzędy elementów G to dzielniki m. ! Ale nie wiemy, które dokładnie dzielniki.]

$|D_n| = 2n$

D_n — n symetrii osiowych] rząd $= 2$

D_n — n obrotów $\{id, O_{\frac{2\pi}{n}}, O_{\frac{4\pi}{n}}, \ldots, O_{\frac{2(n-1)\pi}{n}}\}$

$$= \{(O_{\frac{2\pi}{n}})^0, (O_{\frac{2\pi}{n}})^1, (O_{\frac{2\pi}{n}})^2, \ldots, (O_{\frac{2\pi}{n}})^{n-1}\} = \langle O_{\frac{2\pi}{n}} \rangle$$

$ord(O_{\frac{2\pi}{n}}) = n$

$\forall k \quad ord((O_{\frac{2\pi}{n}})^k) \mid n$

(też dlatego, że $(O_{\frac{2\pi}{n}})^k \in \langle O_{\frac{2\pi}{n}} \rangle$ i $|\langle O_{\frac{2\pi}{n}} \rangle| = n$.

Rzędy tych obrotów to dzielniki n i dla dowolnego $k \mid n$ wiemy, że $ord((O_{\frac{2\pi}{n}})^{\frac{n}{k}}) \underset{ZAD\ 4}{=} k$

$[(O_{\frac{2\pi}{n}})^{\frac{n}{k}} = O_{\frac{2\pi}{k}}]$ $\quad ord(O_{\frac{2\pi}{k}}) = k$.

Rzędy obrotów z D_n to wszystkie dzielniki n.

ODP Rzędy elementów D_n to 2 oraz wszystkie (dodatnie) dzielniki n.