

Problem: Udowodnić, że nie istnieje grupa, w której elementów rzędu 7 jest dokładnie 18.

Uwaga 1.: Niech G, H będą grupami. Jeśli $NWD(|G|, |H|)=1$, to każdy homomorfizm tych grup jest trywialny.

Dowód: Niech $f: G \rightarrow H$ będzie homomorfizmem. $|f(G)| \mid |H|$, ponieważ $f(G) \leq H$. Ponadto $|f(G)| \mid |G|$, a więc z faktu, że $NWD(|G|, |H|)=1$ wynika $|f(G)|=1$, czyli $f(G)=\{1\}$.

Uwaga 2.: $xy = yx \wedge \langle x \rangle \cap \langle y \rangle = \{1\} \Rightarrow \langle x, y \rangle \cong \langle x \rangle \times \langle y \rangle$

Przypuśćmy, że istnieje grupa G zawierająca dokładnie 18 elementów rzędu 7. Oznaczmy przez H_1, H_2, H_3 3 cykliczne podgrupy rzędu 7. Ponieważ wartość funkcji Eulera dla liczby 7 wynosi 6, dowolny nie-neutralny element z grupy H_i jest jej generatorem; W szczególności w każdej z nich jest 6 elementów rzędu 7. Ponadto podgrupy te nie mają elementów wspólnych poza elementem neutralnym, a więc jest w nich łącznie 18 różnych elementów rzędu 7. Wybierając dowolne elementy h_1, h_2, h_3 należące do grup H_1, H_2, H_3 odpowiednio, oznaczmy:

$$H_1 = \langle h_1 \rangle = \{1, h_1, h_1^2, \dots, h_1^6\}$$

$$H_2 = \langle h_2 \rangle$$

$$H_3 = \langle h_3 \rangle$$

Rozpatrzmy działanie H_1 na G poprzez automorfizmy wewnętrzne:

$$\varphi: H_1 \rightarrow \text{Aut}(G), \quad \varphi(x) = \varphi_x, \quad \varphi_x(g) = x \cdot g \cdot x^{-1} \quad \text{dla } x \in H_1, g \in G.$$

Działanie to zachowuje 3-elementowy zbiór grup cyklicznych rzędu 7. Poprzez obcięcie automorfizmów własnych do H_1 otrzymujemy homomorfizm $\psi: H_1 \rightarrow \sum_3$, który na mocy Uwagi 1. jest trywialny, gdyż $|\sum_3| = 6$. Wynika z tego, że automorfizmy wewnętrzne wyznaczone przez H_1 zachowują podgrupę H_2 .

Otrzymujemy zatem homomorfizm $\bar{\varphi}: H_1 \rightarrow \text{Aut}(H_2)$. $|\text{Aut}(H_2)|=6$, więc z Uwagi 1.

$$\forall_{x \in H_1, y \in H_2} \quad \bar{\varphi}_x(y) = xyx^{-1} = y$$

a więc w szczególności $h_1 h_2 = h_2 h_1$. Na mocy Uwagi 2. $\langle h_1, h_2 \rangle \cong \langle h_1 \rangle \times \langle h_2 \rangle \cong \mathbb{Z}_7 \times \mathbb{Z}_7$, $|\langle h_1, h_2 \rangle| = |\mathbb{Z}_7 \times \mathbb{Z}_7| = 48$. Ponieważ $\langle h_1, h_2 \rangle \leq G$, oznacza to, że w grupie G istnieje co najmniej 48 elementów rzędu 7, wbrew założeniu.