3. Warstwy grupy względem podgrupy, twierdzenie Lagrange'a

Stwierdzenie, że rząd podgrupy jest dzielnikiem rzędu grupy, które już udowodniliśmy dla grup cyklicznych, jest prawdziwe dla *wszystkich* grup skończonych i nosi nazwę twierdzenia Lagrange'a.

Niech G będzie dowolną (niekoniecznie skończoną) grupą, a $H \leqslant G$ jej podgrupą. Dla dowolnego $g \in G$ rozpatrzmy podzbiór $gH = \{gh;\, h \in H\} \subseteq G$. Łatwo zauważyć, że:

1) zbiór gH jest klasą abstrakcji zawierającą g następującej relacji równoważności w zbiorze elementów G: $x \sim y \iff x^{-1}y \in H$. Zbiór gH nazywamy **warstwą lewostronną elementu g względem podgrupy H**.
2) $1H = H$
3) Dowolne dwie warstwy lewostronne są równoliczne, w szczególności każda warstwa jest równoliczna ze zbiorem H (przyporządkowanie $h \mapsto gh$ ustala bijekcję zbioru H i warstwy gH).

Zbiór warstw lewostronnych oznaczamy symbolem G/H, a jego moc nazywamy **indeksem podgrupy H w grupie** G i oznaczamy $[G\colon H]$. (Uwaga: analogicznie można zdefiniować warstwy prawostronne grupy G względem podgrupy H — są to podzbiory postaci $Hg = \{hg :\, h \in H\} \subseteq G$).

Z faktu, że każda warstwa lewostronna ma tyle samo elementów, co podgrupa H wynika natychmiast następujące twierdzenie.

3.1. Twierdzenie Lagrange'a. *Jeżeli G jest grupą skończoną i $H \leqslant G$, to $|G| = |H| \cdot [G\colon H]$.*

To proste twierdzenie ma szereg oczywistych, ale ważnych, konsekwencji:

3.2. Wniosek. *Rząd elementu jest dzielnikiem rzędu grupy.*

3.3. Wniosek. *Każda grupa rzędu p, gdzie p jest liczbą pierwszą, jest izomorficzna z $\mathbb{Z}_p$.*

Dowód. Z twierdzenia Lagrange'a wynika, że podgrupa cykliczna generowana przez dowolny element różny od neutralnego musi być rzędu p, a więc musi być równa całej rozpatrywanej grupie. □

3.4. Stwierdzenie. *Grupa skończona G rzędu n jest cykliczna wtedy i tylko wtedy, gdy dla każdego $k \mid n$ zawiera co najwyżej jedną podgrupę rzędu k.*

Dowód. Wystarczy pokazać, że w grupie G istnieje element rzędu n. Niech $\nu(k)$ oznacza liczbę elementów rzędu k w grupie G. Z założenia wynika, że

$$\nu(k) \leq \varphi(k),$$

gdzie φ jest funkcją Eulera.Z twierdzenia Lagrange'a wnioskujemy że $\nu(k)$ ma szansę być niezerowe tylko wtedy, gdy $k \mid n$. Zatem

$$n = \sum_{k \mid n} \nu(k) \leq \sum_{k \mid n} \varphi(k) = n,$$

a więc dla każdego $k \mid n$ zachodzi równość $\nu(k) = \varphi(k)$. W szczególności $\nu(n) = \varphi(n) > 0$, co kończy dowód. □

W związku z twierdzeniem Lagrange'a nasuwa się pytanie o możliwość jego odwrócenia. Załóżmy, że k jest dzielnikiem $|G|$. Czy istnieje podgrupa rzędu k grupy G i ile jest takich podgrup? Częściową odpowiedzią na to pytanie będzie twierdzenie Cauchy'ego, które mówi, że jeżeli liczba pierwsza p jest dzielnikiem $|G|$, to w G istnieje element rzędu p, a więc i cykliczna podgrupa rzędu p. Udowodnimy je w następnym rozdziale.