Chcemy rozpoznawać kiedy dwie warstwy są równe.
Służy temu:

TW. 2 Załóżmy, że $a, b \in G$. Wtedy:
(1) $aH = bH \iff a^{-1}b \in H \iff b^{-1}a \in H$.
(2) $Ha = Hb \iff ab^{-1} \in H \iff ba^{-1} \in H$.

Dowód (tylko (1))
Z TW. 1 mamy ($bo\ b \in bH$):
$aH = bH \iff b \in aH \iff \exists h \in H\ b = ah \iff a^{-1}b \in H$

Mamy: $\forall g \in H \quad g \in H \iff g^{-1} \in H$.
Biorąc $g = a^{-1}b$ mamy: $a^{-1}b \in H \iff \underbrace{(a^{-1}b)^{-1}}_{b^{-1}a} \in H$ ∎

Przykład
- $1+3\mathbb{Z} = 4+3\mathbb{Z}$, bo $4-1 = 3 \in 3\mathbb{Z}$
- $1+3\mathbb{Z} \neq 2+3\mathbb{Z}$, bo $2-1 = 1 \notin 3\mathbb{Z}$.

Kiedy dalej w abstrakcji...

Def
- G/H oznacza zbiór wszystkich warstw lewostronnych H w G
$G/H := \{gH \mid g \in G\}$ (czyli G/H to pewien zbiór podzbiorów G)
- $H\backslash G := \{Hg \mid g \in G\}$ ← zbiór wszystkich warstw prawostronnych H w G.

Zwykle rozważamy G/H.

Przykłady
(1) $\mathbb{Z}/3\mathbb{Z} = \{\underbrace{0+3\mathbb{Z}}_{3\mathbb{Z}}, 1+3\mathbb{Z}, 2+3\mathbb{Z}\}$ ← 3 warstwy
(2) $\mathbb{Z}_8/\{0,2,4,6\} = \{\{0,2,4,6,8\}, \{1,3,5,7,9\}\}$ ← 2 —"—
(3) $S_3/\{id,(12)\} = \{\{id,(12)\}, \{(13),(123)\}, \{(23),(132)\}\}$ ← 3 —"—

Czemu rozważamy G/H?
Idea: Chcemy wydzielić G przez podgrupę H i znowu dostać grupę. Podobnie jak mając dwie liczby n, m chcemy podzielić i dostać $\frac{n}{m}$.

TW. 3
$|G/H| = |H\backslash G|$, czyli zbiór warstw lewostronnych H w G jest równoliczny z ——"— prawo ——"— .

Dowód (szkic)
Dla dowolnego $A \subseteq G$ definiujemy $A^{-1} := \{a^{-1} \mid a \in A\}$.
Wtedy dla $gH \in G/H$ mamy $(gH)^{-1} = Hg^{-1} \in H\backslash G$.
Dostajemy funkcję $\begin{array}{ccc} G/H & \longrightarrow & H\backslash G \\ gH & \longmapsto & (gH)^{-1} \end{array}$ która jest bijekcją. ∎

Def.
Indeks H w G, oznaczany $[G:H]$, to jest moc zbioru G/H (równoważnie moc zbioru $H\backslash G$) warstw lewostronnych H w G

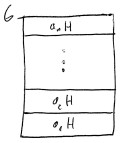
Zmieniamy do powtórzenia: $|H|, |G|, [G:H]$.

TW. 4
$\forall g \in G \quad |gH| = |H| = |Hg|$, czyli wszystkie warstwy są równoliczne.

Dowód (szkic)
Mamy $\begin{array}{ccc} H & \longrightarrow & gH \\ h & \longmapsto & gh \end{array}$ i to jest bijekcja. ∎

TW. Lagrange'a
Niech G będzie grupą skończoną i $H \leq G$. Wtedy mamy:
$|G| = [G:H] \cdot |H|$. W szczególności dostajemy:
$|H| \mid |G|$ oraz $[G:H] \mid |G|$. Czyli:
- rząd podgrupy dzieli rząd grupy
- indeks ——"—— .

Dowód
Wiemy, że G jest rozłączną sumą warstw H.
Oznaczmy $n := [G:H]$ (indeks, tzn. ilość warstw).
Mamy:



$|G| \overset{\text{rozłączność warstw}}{=\!=} |a_1H| + \ldots + |a_nH| = \overset{\text{równoliczność warstw}}{=\!=} n \cdot |H| = [G:H] \cdot |H|$ ∎

Wniosek
Niech G będzie grupą skończoną rzędu k i $a \in G$. Wtedy mamy: $ord(a) \mid k$ oraz $a^k = e$. Czyli:
rząd elementu dzieli rząd grupy.

Dowód
Wiemy, że $ord(a) = |\langle a \rangle|$. Czyli biorąc $H := \langle a \rangle$ z tw. Lagrange'a dostajemy:
$ord(a) \mid |G| = k$.
Stąd $k = L \cdot ord(a)$ dla $L = [G : \langle a \rangle]$.
Czyli $a^k = a^{L \cdot ord(a)} = (a^{ord(a)})^L = e^L = e$. ∎

Def (przyda się do przykładów)
Dla $n \in \mathbb{N}_{>0}$ definiujemy: $A_n := \{\sigma \in S_n \mid \sigma \text{ jest parzysta}\}$.
ĆW: $A_n \leq S_n$ (podgrupa alternująca)
Zauważmy: $|A_n| = \frac{n!}{2}$ $\quad |A_3| = 3,\ |A_4| = 12,\ |A_5| = 60, \ldots$

Uwaga
(1) Z Wniosku rząd elementu dzieli rząd grupy czyli np. nie ma elementu rzędu 4 w S_3, bo $4 \nmid 6 = |S_3|$.
Ale implikacja odwrotna NIE jest prawdziwa, bo np. $4 \mid 4 = |K_4|$ ale w K_4 nie ma elementu rzędu 4.
2. Z tw. Lagrange'a nie ma tej podgrupy rzędu 4 w S_3.
Implikacja odwrotna nie jest prawdziwa, bo np. $6 \mid 12 = |A_4|$, ale w A_4 nie ma podgrupy rzędu 6.