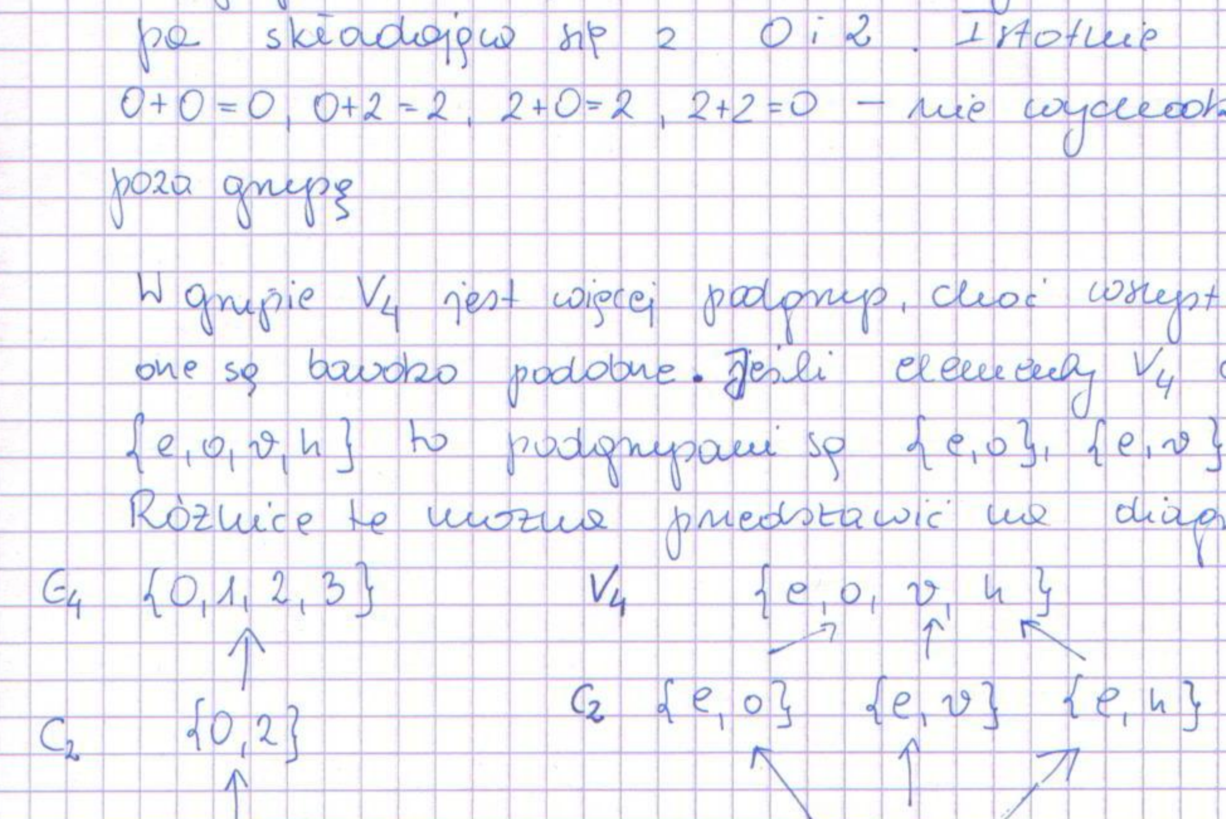
Do badania grup bardziej licznych niż 4 elementy przyda nam się trochę wiedzy teoretycznej. Pierwsze przydatne pojęcie to pojęcie podgrupy. Podgrupa jest to podzbiór w grupie, który zawiera element neutralny, jest zamknięty ze względu na mnożenie i branie odwrotności. Krótko mówiąc jest to podzbiór, który sam jest mniejszą grupą. Sprawdźmy, czy w znanych nam już grupach są jakieś podgrupy. Zacznijmy od grup czteroelementowych, bo w dużej grupie jest łatwo znaleźć podgrupę, tzn dokładniej mówiąc jest większa szansa, że jakaś podgrupa się znajdzie.

W grupie $\mathbb{Z}_4$ jest jedna nietrywialna podgrupa składająca się z 0 i 2. Istotnie $0+0=0$, $0+2=2$, $2+0=2$, $2+2=0$ – nie wychodzimy poza grupę

W grupie V_4 jest więcej podgrup, choć wszystkie one są bardzo podobne. Jeśli elementy V_4 oznaczymy $\{e, o, v, h\}$ to podgrupami są $\{e, o\}$, $\{e, v\}$ $\{e, h\}$
Różnice te można przedstawić na diagramie



Widzimy teraz jak różna jest struktura grupy C_4 i grupy V_4. Ciekawe dlaczego w żadnej z tych grup nie ma podgrupy mającej trzy elementy?

Co wspólnego mają ze sobą grupy C_n? Wszystkie one generowane są przez jeden element. Oznacza to, że wszystkie pozostałe elementy są ~~gen~~ potęgami tego jednego jedynego elementu np:

C_2 $\mathbb{Z}/_2$ jest generowana przez 1. $1+1=0$

C_3 $\mathbb{Z}/_3$ " 1 $1+1=2$ $1+1+1=0$

⋮

C_n $\mathbb{Z}/_n$ jest też generowana przez 1 $1+1=2$ $1+1+1=3 \dots$ $\underbrace{1+\cdots 1}_{n}=0.$

Potęgę do której należy podnieść dany element, żeby dostać element neutralny nazywamy rzędem elementu grupy. Mówiąc nowym językiem w grupie C_n jest zawsze przynajmniej jeden element rzędu n. Częściowo możemy więc odpowiedzieć na pytanie dlaczego żadna z czteroelementowych grup nie zawiera podgrupy mającej trzy elementy: Jest tylko jedna trójelementowa grupa: C_3. W C_3 jest element rzędu 3 a w żadnej z grup C_4 ani V_4 takiego elementu nie ma. W V_4 wszystkie pozostałe są rzędu 2 a w C_4 są dwa elementy rzędu 4, jeden rzędu 2 i element neutralny. Jest to odpowiedź tylko częściowa. No bo w końcu nigdy nie ma grupy rzędu 4 (a sprawdziliśmy że nie ma!)

która zawierałaby element rzędu 3? Żeby odpowiedzieć na to pytanie musimy dokładniej zająć się badaniem struktury grupy i jej podgrup. ~~Niech~~ Niech G będzie grupą a H podgrupą. W G wprowadzamy relację równoważności przy pomocy następującego warunku:

$$\boxed{\text{mówimy, że } g \sim h \text{ wtedy i tylko wtedy gdy } g^{-1}h \in H \quad (g, h \in G)}$$

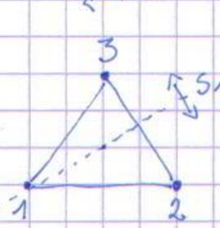
Sprawdźmy, że istotnie jest to relacja równoważności (1) sprawdzamy czy relacja jest zwrotna tzn. czy $\forall g \in G \ g \sim g$: oznaczałoby to, że $g^{-1}g \in H$ a tak jest, bo $g^{-1}g = e$, a każda podgrupa zawiera element neutralny;
(2) sprawdzamy czy relacja jest symetryczna tzn. czy jeśli $g \sim h$ to także $h \sim g$.
Niech więc $g^{-1}h \in H$. Skoro H jest podgrupą to także element $(g^{-1}h)^{-1}$ należy do H, ale

$$(g^{-1}h)^{-1} = h^{-1}(g^{-1})^{-1} = h^{-1}g$$

Otrzymaliśmy więc, że $h^{-1}g \in H$, czyli $h \sim g$.
(3) W końcu sprawdzamy, czy jeśli $g \sim h$ i $h \sim k$ to $g \sim k$ czyli czy relacja jest przechodnia. jeśli $g \sim h$ to $g^{-1}h \in H$, jeśli $h \sim k$ to $h^{-1}k \in H$, ale wtedy iloczyn $(g^{-1}h)(h^{-1}k)$ też jest elementem H. Korzystamy z łączności mnożenia:

$$(g^{-1}h)(h^{-1}k) = g^{-1}\underbrace{h \cdot h^{-1}}_{e}k = g^{-1}k \in H \quad \text{zatem } g \sim k$$

Relacja jest symetryczna, zwrotna i przechodnia, zatem jest relacją równoważności. Żeby przyjrzeć się dokładniej tej relacji zbadajmy nową grupę, tym razem mającą 6 elementów. Będzie to grupa symetrii trójkąta równobocznego. Grupę taką oznaczamy D_3.



W skład grupy D_3 wchodzą

e - identyczność

O_1 - obrót wokół środka o $2\pi/3$ (120°)

O_2 - obrót wokół środka o $4\pi/3$ (240°)

S_1, S_2, S_3 - symetrie względem osi przechodzących przez wierzchołki 1, 2, 3 odpowiednio. Żeby dobrze zbadać tę grupę napiszmy jej tabelkę działania

	e	O_1	O_2	S_1	S_2	S_3
e	e	O_1	O_2	S_1	S_2	S_3
O_1	O_1	O_2	e	S_3	S_1	S_2
O_2	O_2	e	O_2	S_2	S_3	S_1
S_1	S_1	S_2	S_3	e	O_1	O_2
S_2	S_2	S_3	S_1	O_2	e	O_1
S_3	S_3	S_1	S_2	O_1	O_2	e

$O_1 \circ S_1 \binom{3}{1\;\;2} = O_1 \binom{2}{1\;\;3} = {}^{\;3}_{2\;\;1} = S_3 \binom{3}{1\;\;2}$

$O_1 S_1 = S_3$

$O_1 S_2 \binom{3}{1\;\;2} = O_1 \binom{1}{3\;\;2} = \cancel{\emptyset}\; {}^{\;2}_{1\;\;3} = S_1 \binom{3}{1\;\;2}$

$S_1 \circ O_1 \binom{3}{1\;\;2} = S_1 \binom{2}{3\;\;1} = {}^{\;1}_{3\;\;2} = S_2(\cdot\cdot)$

$S_1 S_2 \binom{3}{1\;\;2} = S_1 \binom{1}{3\;\;2} = \binom{2}{3\;\;1} = O_1$

Zauważmy przede wszystkim, że grupa ta nie jest przemienna! $O_1 S_1 = S_3 \neq S_1 O_1 = S_2$

elementy S_1, S_2, S_3 są rzędu 2, ponadto O_1, O_2 są rzędu 3

Oto struktura podgrup w D_3

$$
\begin{tikzcd}
 & & D_3 = \{e, o_1, o_2, s_1, s_2, s_3\} & \\
C_3 \simeq \{o_1, o_2, e\} \arrow[urr] & & & \\
C_2 \simeq \{e, s_1\} \arrow[uurr] & & \{e, s_2\} \arrow[uu] & \{e, s_3\} \arrow[uul] \\
 & \{e\} \arrow[ul] \arrow[uuul] \arrow[ur] \arrow[urr] & &
\end{tikzcd}
$$

Niech teraz $G = D_3$ a $H = \{e, s_1\}$. Sprawdźmy które elementy w D_3 są równoważne względem H

	e	o_1	o_2	s_1	s_2	s_3
e	X			X		
o_1		X				X
o_2			X		X	
s_1	X			X		
s_2			X		X	
s_3		X				X

co jest równoważne o_1?

$g \sim o_1 \iff o_1^{-1} g \in H$

$$o_1^{-1} g = \begin{cases} e \\ s_1 \end{cases}$$

$$\downarrow$$

$$o_2 g = \begin{cases} e \longrightarrow g = o_2^{-1} = o_1 \\ s_1 \longrightarrow g = s_3 \end{cases}$$

$$o_2^{-1} g = \begin{cases} e \\ s_1 \end{cases} \quad o_1 g = \begin{cases} e & o_2 \\ s_1 & s_2 \end{cases}$$

~~D_3 rozpada się,~~ D_3 rozpada się na sumę zbiorów wzajemnie równoważnych elementów:

$$D_3 = \underbrace{\{e_1, s_1\}}_{H} \cup \underset{\substack{\| \\ o_1 H \\ \| \\ s_3 H}}{\{o_1, s_3\}} \cup \underset{\substack{\| \\ o_2 H \\ \| \\ s_2 H}}{\{o_2, s_2\}}$$

każdy z tych zbiorów ma tyle samo elementów co podgrupa!

Tak jest zawsze! Nie tylko w tym przypadku.
Zobaczmy: $a, b \in G$ $a \sim b$ oznacza $a^{-1}b \in H$
czyli istnieje element $h \in H$ taki że $a^{-1}b = h$ czyli $\boxed{b = a \cdot h.}$
Z drugiej strony, jeśli $b = ah$ dla pewnego $h \in H$
to $a^{-1}b = h \in H$ więc $a \sim b$.
Wykazaliśmy właśnie że

$$a \sim b \iff \exists h: \; b = a \cdot h$$

Jeśli więc szukamy elementów równoważnych z a musimy wziąć zbiór $a \cdot H = \{ b : b = ah, \; h \in H \}$
dodatkowo wiemy, że mnożenie przez a w grupie G jest bijekcją, zatem nie może się zdarzyć, że $ah_1 = ah_2$ dla $h_1 \neq h_2$. Stąd wniosek, że zbiór elementów równoważnych z a ma tyle elementów ile grupa H. Stąd już prosty wniosek, że liczba elementów podgrupy jest dzielnikiem liczby elementów grupy. (Do uzasadnienia tego potrzeba jeszcze wiedzieć, że dwa zbiory elementów równoważnych (klasy równoważności) są albo równe albo mają puste przecięcie)
Liczbę elementów grupy nazywamy rzędem grupy.
Wykazaliśmy właśnie twierdzenie

LAGRANGE'A: Rząd podgrupy jest dzielnikiem rzędu grupy

Z tego twierdzenia wynika, że grupa rzędu 4 nie może mieć podgrupy rzędu 3.

To proste twierdzenie ma też inne konsekwencje. Zauważmy na przykład, że każdy element grupy generuje pewną podgrupę składającą się ze wszystkich jego potęg. Ta podgrupa ~~jest~~ ma tyle elementów ile wynosi rząd tego elementu. Np. podgrupa $\{e, o_1, o_2\}$ jest generowana przez o_1, który jest rzędu 3: $o_1 \circ o_1 = o_2$ $o_1 \circ o_1 \circ o_1 = o_2 \circ o_1 = e$ (7)

Stąd wniosek, że rząd każdego elementu jest dzielnikiem rzędu grupy. Od razu możemy zatem stwierdzić ile jest grup rzędu p gdzie p jest liczbą pierwszą – tylko jedna! Na przykład gdy $p=5$ w grupie pięcioelementowej wszystkie elementy poza neutralnym muszą być rzędu 5. Weźmy jeden z nich: a; wtedy

$$G = \{a, a^2, a^3, a^4, a^5 = e\}$$

Grupa rzędu 5 jest więc identyczna z grupą C_5. Ogólnie rzecz biorąc grupa rzędu p to jedynie C_p jeśli p jest liczbą pierwszą. Poczyniliśmy więc spory postęp w kierunku opisania grup skończonych!

Wróćmy teraz na chwilę do relacji równoważności, której analiza doprowadziła nas do ~~po~~ twierdzenia Lagrange'a. Przypomnijmy tę relację:

$$\boxed{g \sim h \iff g^{-1}h \in H}$$

Jest jeszcze druga bardzo podobna relacja:

$$g \leftrightarrow h \iff gh^{-1} \in H$$

Porównajmy je:

$$g \sim h \iff g^{-1}h \in H \qquad g \leftrightarrow h \iff gh^{-1} \in H$$

Różnica polega na tym, którzy z czynników odwracamy: pierwszy czy drugi; Analizując pierwszą relację stwierdziliśmy że klasy równoważności, czyli zbiory elementów wzajemnie równoważnych to zbiory postaci gH tzn.

$$[g]_\sim = gH = \{g \cdot h : h \in H\}$$

klasa równoważności do której należy element g

Możemy podobne rozumowanie przeprowadzić dla drugiej relacji:

$a \leftrightarrow b \iff ab^{-1} \in H$ tzn. $\exists h \in H: ab^{-1} = h$ czyli $a = hb$. Z drugiej strony jeśli $a = h \cdot b$ to $ab^{-1} = h \in H$ czyli $a \leftrightarrow b$.

$$[a]_{\leftrightarrow} = H \cdot b = \{h \cdot b : h \in H\}$$

Klasy równoważności względem drugiej relacji są podobne. Różnica polega na mnożeniu z drugiej strony.

Sprawdźmy jak wyglądają klasy równoważności względem obu relacji dla dwóch różnych podgrup w D_3

Oznaczmy

$$H = \{e, s_1\} \qquad K = \{e, o_1, o_2\}$$

	$\sim$	$\longleftrightarrow$
H	$\{e, s_1\} \cup \{o_1, s_3\} \cup \{o_2, s_2\}$	$\{e, o_1, o_2\} \cup \{s_1, s_2, s_3\}$
K	$\{e, s_1\} \cup \{o_1, s_2\} \cup \{o_2, s_3\}$	$\{e, o_1, o_2\} \cup \{s_1, s_2, s_3\}$

$Ho_1 = \{o_1, s_1o_1\} = \{o_1\ s_2\}$

$Ho_2 = \{o_2\ \ s_1o_2\} = \{o_2\ s_3\}$

$s_1K = \{s_1, s_1o_1, s_1o_2\} =$
$= \{s_1, o_2, o_3\}$

$Ks_1 = \{s_1, o_1s_1, o_2s_1\} =$
$= \{s_1, s_3, s_2\}$

Rozkład na klasy względem obu relacji jest różny dla grupy H i taki sam dla K. Podgrupy mające tę własność, że klasy równoważności względem relacji $\sim$ i relacji $\longleftrightarrow$ ~~raz~~ są takie same nazywamy

PODGRUPAMI NORMALNYMI!

Podgrupy normalne odgrywają bardzo ważną rolę w teorii grup. W szczególności w zbiorze

klas równoważności względem podgrupy normalnej można wprowadzić działanie, które powoduje, że zbiór klas równoważności sam staje się grupą. Działanie to można zadać na reprezentantach pamiętając, że, jako zbiory, $aH = Ha$
(co oznacza, że $\forall h \in H \ \exists h' \in H: \ ah = h'a$)

$$[a]\cdot[b] = [a\cdot b] \quad \left((a\cdot H)\cdot(b\cdot H) = ab\cdot H \right)$$

czy to jest dobrze określone? Tak! jeśli weźmiemy dwóch innych reprezentantów np $a' = a\cdot h$ i $b' = b\cdot k$ to

$$[a']\cdot[b'] \underset{\substack{\uparrow \\ \text{z definicji}}}{=} [a'b'] = a'b'\cdot H = ahb\underbrace{k\cdot H}_{H} = ah\,bH = ah\underbrace{H}_{H}b = abH = [ab]$$

Wynik nie zależy od wyboru reprezentantów. Tak nie jest dla grupy, która nie jest normalna. Weźmy np klasy względem $\sim$ dla grupy $\{e, s_1\}$ i sprawdźmy, czy da się pomnożyć dwie takie klasy np:

$$[s_3]_\sim \cdot [s_2]_\sim \overset{?}{=} [s_3\cdot s_2]_\sim = [O_2]$$

↓ zmieniamy reprezentantów

różne wyniki!!

$$\left.\begin{array}{l}[s_3]_\sim = [O_1]_\sim \\ [s_2]_\sim = [O_2]_\sim\end{array}\right\} \Rightarrow [O_1]_\sim \cdot [O_2]_\sim \overset{?}{=} [O_1 O_2]_\sim = [e]_\sim \neq [O_2]_\sim$$

Jeśli podgrupa nie jest normalna mnożenie w zbiorze klas jest źle określone!

Grupę, która powstaje poprzez wprowadzenie w zbiorze klas równoważności mnożenia nazywamy GRUPĄ ILORAZOWĄ

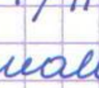
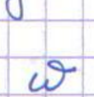
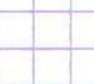
Klasy równoważności względem $\sim$ to LEWE WARSTWY względem podgrupy, a klasy względem relacji $\leftrightarrow$ to PRAWE WARSTWY.

Podgrupa jest normalna jeżeli lewe i prawe warstwy są jednakowe. Oznacza to, że

$$\forall a \quad aH = Ha \quad \text{albo} \quad \forall a \quad aHa^{-1} = H$$

Zastanówmy się jaką grupę otrzymamy dzieląc D_3 przez podgrupę obrotów $K = \{O_1, O_2, e\}$?

$D_3/K = ?$ Jest to grupa dwuelementowa, więc musi być koniecznie identyczna z $\mathbb{Z}_2$ (C_2) pod względem struktury.

Zadanie na ćwiczenia: Weźć grupę D_4 symetrii kwadratu składającą się z e - elementu neutralnego, O_1, O_2, O_3 obrotów o $\pi/4$, $\pi/2$, $3\pi/4$ i czterech symetrii v:  h:  r  l 
Zrobić tabelkę działania, znaleźć podgrupy, które z tych podgrup są normalne, sprawdzić jaką grupę czteroelementową jest D_4/H gdzie H jest dwuelementową podgrupą normalną w D_4

Zadanie domowe:

Zrobić to samo dla grupy ośmioelementowej Q_8 nazywanej grupą kwaternionową. Grupa ta składa się z następujących elementów:

$Q_8=\{1,-1,i,j,k,-i,-j,-k\}$ o następujących własnościach

$$i^2=j^2=k^2=-1 \qquad ij=k$$

mnożenie przez (-1) jest zwyczajne, tzn zmienia znak: $(-1)\cdot k=-k$, ponadto (-1) jest przemienne ze wszystkim $(-1)\cdot k=k\cdot(-1)$. Ogólnie grupa jest nieprzemienna. Z powyższych własności da się już wydedukować wszystkie wyniki mnożenia, na przykład

$$ik \underset{k=ij}{=} iij \underset{i^2=-1}{=} (-1)\cdot j=-j \quad \text{itd...}$$