Ile wynosi dwa plus dwa,
czyli w grupie można więcej!

Jeżeli spytamy kogoś ile wynosi dwa plus dwa, to spotkamy się prawdopodobnie z uśmiechem politowania. Wiadomo, cztery. Podobnie jak dwa razy dwa. Istnieje też powiedzenie: to proste jak dwa razy dwa. Czy rzeczywiście w matematyce nie ma możliwości, aby było inaczej? Pewnie wiele osób nie wyobraża sobie w ogóle takiej możliwości. Jeśli Ty też tak uważasz, a masz trochę czasu i cierpliwości, to ten artykuł jest dla Ciebie.

Najpierw definicja. Jedną z najprostszych struktur w matematyce jest pojęcie grupy. Co to jest grupa?
Grupa to zbiór elementów $\boldsymbol{G}$, wraz z określonym na nich działaniem $\bigcirc$ (nazwijmy je mnożeniem, ale może to być dodawanie, złożenie funkcji itd.), które spełniają następujące warunki:

1. wynik "mnożenia" dwóch elementów jest elementem grupy $a \bigcirc b = c \in \boldsymbol{G}$ (działanie jest wewnętrzne).
2. działanie jest łączne, tzn. $(a \bigcirc b) \bigcirc c = a \bigcirc (b \bigcirc c)$
3. istnieje element neutralny e ("jedynka") o właściwości: $e \bigcirc a = a \bigcirc e = a$, dla każdego $a \in \boldsymbol{G}$
4. dla każdego $a \in \boldsymbol{G}$ istnieje element odwrotny $a^{-1} \in \boldsymbol{G}$, taki że $a \bigcirc a^{-1} = e$.

Rolę elementów mogą pełnić liczby, ale również wielomiany, wektory, macierze, operacje symetrii itp. itd. Tak więc jest to bardzo ogólna definicja, obejmująca bardzo różne twory i struktury. Poniżej podam stosunkowo proste przykłady grup:

Przykład 1. Zbiór liczb całkowitych z działaniem dodawania jako "mnożeniem" stanowi grupę.
To dosyć łatwe do sprawdzenia, że aksjomaty grupy są spełnione. Wynik dodawania dwóch liczb całkowitych jest liczbą całkowitą. Elementem neutralnym jest zero. Dodawanie jest łączne, a dla każdej liczby a możemy podać element odwrotny $-a$. Mamy oczywiście $a + -a = 0$, co odpowiada zapisowi ogólnemu dla grup $a \bigcirc a^{-1} = e$.
Zbiór dodatnich liczb całkowitych (zbiór liczb naturalnych) z dodawaniem nie stanowi grupy, gdyż nie zawiera elementów odwrotnych.

Przykład 2. Zbiór niezerowych liczb całkowitych z działaniem mnożenia nie stanowi grupy. Co prawda iloczyn dwóch liczb całkowitych jest liczbą całkowitą, mnożenie jest działaniem łącznym, możemy wyodrębnić element neutralny (liczbą tą jest jeden), ale odwrotności liczb całkowitych nie należą do zbioru liczb całkowitych. Być może była to jedna z przyczyn, dla których wymyślono ułamki i liczby wymierne.

Przykład 3. Zbiór liczb wymiernych z działaniem zwyczajnego mnożenia jest grupą pod warunkiem wykluczenia liczby zero, która nie ma elementu odwrotnego. Oczywiście wynik mnożenia dwóch liczb wymiernych jest liczbą wymierną. Elementem neutralnym jest liczba jeden.

Przykład 4.
Podobnie grupę stanowią: zbiór liczb rzeczywistych różnych od zera z działaniem mnożenia oraz cały zbiór liczb wymiernych ze zwykłym dodawaniem.

Powyżej podane przykłady są ciekawe z punktu widzenia powstawania matematyki i ewolucji pojęć od liczb naturalnych i dodawania poprzez wprowadzanie liczb ujemnych, ułamkowych i rzeczywistych na drodze wprowadzania dodatkowych działań i poszukiwania elementów odwrotnych.
Zbiór elementów grupy może być nieskończony, jak w dotychczasowych przykładach, lub skończony. Dla chemików w nauce o symetrii ciekawsze są grupy oparte o skończony zbiór elementów.

Przykład 5. Zbiór liczb {0, 1, 2} z działaniem $\oplus$: dodawania modulo 3 (reszta z podzielenia sumy liczb przez 3) stanowi grupę. Przykładowo: $2 \oplus 2 =$ (reszta z dzielenia sumy 2+2 przez 3) 4 podzielone przez 3 wynosi 1 reszta 1. Jako wynik bierzemy tylko resztę z tego dzielenia. Ponieważ wynik jest resztą z dzielenia przez 3, więc może przyjmować tylko wartości należące do grupy, tzn. 0, 1 lub 2.
Elementem neutralnym jest ponownie zero. Co z elementami odwrotnymi? Odwrotnością jedynki jest dwa i vice versa odwrotnością 1 jest 2. Mamy bowiem $2 \oplus 1 =$ reszta z dzielenia $(2+1)/3 = 0$. Zero jest odwrotnością samego siebie: $0 \oplus 0 =$ reszta z dzielenia $(0+0)/3 = 0$.
Najciekawsze jest to, że ta grupa jest ściśle związana (jest izomorficzna) z grupą obrotów figury o 120º. Działaniem w grupie obrotów jest złożenie dwóch obrotów. Złożenie trzech obrotów o 120º jest równoważne obrotowi o 0º. Podobnie $1 \oplus 1 \oplus 1 = 0$. Mamy przyporządkowanie: obrót o 0º odpowiada elementowi **0** grupy, obrót o 120º odpowiada elementowi **1** grupy, natomiast obrót o 240º odpowiada elementowi **2** grupy.

Mamy już ilustrację tytułu: 2⊕2 = reszta z dzielenia (4/3) = 1. W tej grupie nie ma innej możliwości, liczba 4 nie występuje, podobnie jak 4 obroty o 120º dają po prostu jeden obrót o 120º.
Łatwo się zorientować, że analogicznie każda grupa skończona typu {0, 1, ... ***k***–1} z działaniem dodawania modulo ***k*** stanowi model obrotów figury o całkowite wielokrotności kąta 360º/***k***. Zaiste zdumiewające zastosowanie dzielenia z resztą - tak niedocenianego przeze mnie w szkole podstawowej...

Przykład 6. Zbiór dwóch liczb {1, –1} z działaniem mnożenia tworzy grupę. Jeżeli szukać analogii geometrycznych to grupa ta może modelować operację odbicia w płaszczyźnie (symetrię zwierciadlaną) bądź operację odbicia w środku symetrii. element 1 odpowiada przekształceniu identycznościowemu (brak zmian, element neutralny) a element –1 odbiciu w płaszczyźnie, bądź odbiciu przez środek symetrii. Mnożenie liczb w grupie geometrycznej zastępuje złożenie dwóch operacji symetrii. Grupa trochę prymitywna i okrojona do dwóch elementów, no ale aksjomaty spełnia.

Przykład 7. Ważny dla chemików w nauce o symetrii. Zbiór operacji symetrii własnej cząsteczki z działaniem grupowym będącym złożeniem dwóch operacji symetrii stanowi grupę. Jest tak, ponieważ złożenie dwóch operacji symetrii jest też jakąś operacją symetrii, czyli elementem należącym do grupy. Zawsze też daje się znaleźć operację symetrii odwrotną, która sprowadza cząsteczkę do stanu początkowego.
Przykładowo dla cząsteczki wody mamy operacje: identyczności, obrotu o 180º, odbicia w płaszczyźnie zawierającej wszystkie trzy atomy oraz w płaszczyźnie do niej prostopadłej, przechodzącej przez atom tlenu.

Czy zatem nauki o symetrii nie da się sprowadzić i wymodelować za pomocą jakiejś kombinacji grup skończonych z odpowiednimi definicjami dodawania i mnożenia? W dużej mierze tak, może napiszę o tym w kolejnym artykule.

Inne matematyki, "matematyka małżeńska"

Przykład 8. Można zdefiniować grupę składającą się z liczb całkowitych z działaniem grupowym (nazwijmy je dodawaniem) określonym jako $a \oplus b = a + b + 1$. Elementem neutralnym e jest wówczas –1.
Mamy $a \oplus (-1) = a - 1 + 1 = a$ dla każdego $a \in G$. Wyznaczmy element odwrotny do a w tej grupie.
Z warunku $a \oplus a^{-1} = e$ mamy $a + a^{-1} + 1 = -1$, czyli $a^{-1} = -a - 2$.
W grupie tej można rozwiązywać tradycyjne równania zawierające dodawanie. Na przykład równanie x⊕2=1 ma w tej grupie rozwiązanie inne od tradycyjnego: x⊕2 = x+2+1 = 1, czyli x = –2. Jak łatwo zauważyć dowolne równanie będzie można rozwiązać, znajdując rozwiązanie w obrębie elementów grupy.
Pokuśmy się o dywagacje całkiem nieścisłe, choć chyba warte uwagi. W grupie tej mamy zakłócony intuicyjny, odruchowy wynik charakterystyczny dla naturalnej sumy 2+2=4. W wyniku dodawania mamy przecież 2⊕2=5! Można nazwać tę grupę "grupą sprzedawcy", który zawsze dolicza do rachunku. Jeżeli działanie grupowe nazwiemy "dodawaniem" to mamy 1⊕1= 3, co pewnie ze zrozumieniem i radością przyjmą pary małżeńskie spodziewające się potomka ;-). Jakie zastosowanie może mieć taka grupa? Może w szyfrowaniu informacji?

Przykład 9 (nie tylko grupy). Jeżeli jako zbiór elementów przyjmiemy zbiór liczb rzeczywistych z dodawaniem zdefiniowanym jak w przykładzie 8: $a \oplus b = a + b + 1$, to przyjmując definicję mnożenia jako $a \otimes b = ab + a + b$ otrzymamy spójny zbiór (tzw. ciało liczbowe), w którym obowiązuje prawo łączności mnożenia $(a \otimes b) \otimes c = a \otimes (b \otimes c)$ oraz rozdzielność mnożenia względem dodawania $(a \oplus b) \otimes c = a \otimes c \oplus b \otimes c$.
Sprawdźmy łączność:
$(a \otimes b) \otimes c = (ab + a + b) \otimes c = abc + ac + bc + ab + a + b + c$
$a \otimes (b \otimes c) = a \otimes (bc + b + c) = abc + ab + ac + a + bc + b + c$
a teraz rozdzielność:
$(a \oplus b) \otimes c = (a + b + 1) \otimes c = ac + bc + c + a + b + 1 + c$
$a \otimes c \oplus b \otimes c = (ac + a + c) \oplus (bc + b + c) = ac + a + c + bc + b + c + 1$

W tym ciele liczbowym mamy 2⊗2= 2*2+2+2= 8. Zbiór niezerowych liczb wymiernych z operacją mnożenia zdefiniowaną powyżej stanowi grupę. Elementem neutralnym tego mnożenia jest zero: a⊗0=a.
Ciekawe jest, że np. dowolne równanie liniowe czy kwadratowe można rozwiązywać w tym ciele zamiast w tradycyjnym ciele z normalnymi działaniami i będziemy otrzymywać równie jednoznaczne pierwiastki tych równań. Oczywiście jedno rozwiązanie dla równania liniowego a dwa, bądź jedno, bądź żadnego rozwiązania dla równania kwadratowego (w zależności od delty).

P.S. Jeśli Cię to zaciekawiło, to sprawdź, że biorąc definicje działań a⊕b=a+b–1 i $a \otimes b = -ab + a + b$ możemy otrzymać "ciało liczbowe kupującego", który zawsze od sumy do zapłacenia odejmuje jedynkę ;-). Łączność

mnożenia i rozdzielność mnożenia względem dodawania są spełnione. W tym ciele mamy matematykę dla oblubieńców na noc poślubną $1 \oplus 1 = 1$. Dwie jednostki po dodaniu zaczynają tworzyć jedność. Niestety, teraz wynik mnożenia też ulega zmianie: $2 \otimes 2 = 0$. Nie wiem czy odnosi się to finansów - to już byłaby chyba nadinterpretacja ;-).
Może powinienem jeszcze wspomnieć także o "naturalnych" odstępstwach od równania 2+2=4 wynikających ze zastosowania innych niż dziesiątkowy systemów liczenia. Na przykład w trójkowym systemie liczenia (trzy jednostki rzędu niższego stanowią jedną jednostkę rzędu wyższego) 2+2 = 11, a w czwórkowym 2+2 = 10.

Uwagi końcowe:

1. Nie ma pełnej dowolności w tworzeniu grup. Nie każde działanie musi być łączne i nie każdy zestaw (zbiór liczb + działanie) tworzy grupę: np. działanie $a \bigcirc b = 2a + b$ nie jest łączne, gdyż

$$(a \bigcirc b) \bigcirc c = (2a + b) \bigcirc c = 4a + 2b + c$$
$$a \bigcirc (b \bigcirc c) = a \bigcirc (2b + c) = 2a + 2b + c.$$

Podobnie działanie $a \bigcirc b = a^2 + b^2$ nie jest łączne, gdyż mamy

$$(a \bigcirc b) \bigcirc c = (a^2 + b^2) \bigcirc c = a^4 + 2a^2b^2 + b^4 + c^2$$
$$a \bigcirc (b \bigcirc c) = a \bigcirc (b^2 + c^2) = a^2 + b^4 + 2b^2c^2 + c^4$$

2. Celowo nie omówiłem grup opartych o permutacje, wielomiany, liczby zespolone, macierze (tutaj działanie mnożenia jest nieprzemienne), kwaterniony i inne obiekty matematyczne, aby nie zacierać prostoty powyższych przykładów i skupić się na filozoficznych aspektach podejścia do zagadnienia grupy i aby uzasadnić możliwości istnienia wyników mnożenia dwa razy dwa różnych od czterech.

Dr inż. Jarosław Chojnacki