Algebra liniowa

Prof. PK Dr Marek Malinowski

Wykład kończy się oceną. **Na test należy przyjść z laptopem** (nie tablet, nie telefon), ponieważ test zostanie przeprowadzony na platformie MOODLE.
Pozytywna ocena z wykładu potwierdza uzyskanie przez studenta efektu uczenia się:

1. "EP-1 Zna i rozumie wybrane zagadnienia z zakresu algebry liniowej przydatne do formułowania i rozwiązywania zadań praktycznych związanych z informatyką. Zna podstawowe struktury algebraiczne, zna własności liczb zespolonych, zna własności przestrzeni liniowej, potrafi podać podstawowe własności macierzy."

   Wykład - skala ocen:

   - 51%-60% ocena 3.0,
   - 61%-70% ocena 3.5,
   - 71%-80% ocena 4.0,
   - 81%-90% ocena 4.5,
   - 91%-100% ocena 5.0

2. Drugi efekt uczenia się EP-2 (zgodny z sylabusem) zostanie oceniony w ramach Ćwiczeń.

Niech G oznacza niepusty zbiór, a $\circ$ dobrze określone działanie dwuargumentowe na tym zbiorze.

Definicja.

Parę uporządkowaną $(G, \circ)$ nazywamy **grupą**, jeśli

1. **Wewnętrzność**: dla dowolnych elementów $a, b \in G$ ich wynik $a \circ b$ również należy do zbioru G, mówi się wtedy, że zbiór G jest zamknięty ze względu na $\circ$.
2. **Łączność**: dla wszystkich $a, b, c \in G$ musi zachodzić $(a \circ b) \circ c = a \circ (b \circ c)$.
3. **Element neutralny**: istnieje element $e \in G$ spełniający dla dowolnego elementu $a \in G$ warunek $a \circ e = e \circ a = a$.
4. **Odwracalność**: dla każdego $a \in G$ musi istnieć $x \in G$, dla których $a \circ x = x \circ a = e$.

Uwaga.

Jeśli oprócz warunków z powyższej definicji spełniony jest również warunek:

- **Przemienność**: dla dowolnych elementów $a, b \in G$ spełniona jest równość $a \circ b = b \circ a$,

to $(G, \circ)$ nazywa się grupą przemienną (lub abelową).

Np. Rozważmy zbiór liczb całkowitych $\mathbf{Z}$ ze zwykłym działaniem dodawania $+$. Para $(\mathbf{Z}, +)$ jest grupą przemienną.

Np. Rozważmy zbiór liczb naturalnych z zerem $\mathbf{N_0}$ ze zwykłym działaniem dodawania $+$. Para $(\mathbf{N_0}, +)$ nie jest grupą. Nie jest spełniony warunek odwracalności.

Np. Rozważmy zbiór liczb rzeczywistych dodatnich $\mathbf{R}_+$ ze zwykłym działaniem mnożenia $\cdot$. Para $(\mathbf{R}_+, \cdot)$ jest grupą przemienną.

Np. Rozważmy zbiór liczb całkowitych $\mathbf{Z}$ z działaniem $\circ$ określonym jako $a \circ b = a + b + 2$. Para $(\mathbf{Z}, \circ)$ jest grupą przemienną.

Np. Rozważmy zbiór $\mathbf{Z_n} = \{0, 1, 2, \ldots, n-1\}$, gdzie n jest liczbą naturalną, z działaniem $+_n$ dodawania modulo n. Para $(\mathbf{Z_n}, +_n)$ jest grupą przemienną.

Arytmetykę modularną stosuje się tam, gdzie występuje cykliczność. Używa się jej w kryptografii, informatyce, przy tworzeniu sum kontrolnych. Zasada działania szyfru RSA oraz Test Millera-Rabina (czyli algorytm określający czy dana liczba jest pierwsza) opierają się na własnościach mnożenia w arytmetyce modularnej liczb całkowitych.

Ważnym przykładem grupy jest zbiór S_n bijekcji przekształcających $\{1, 2, \ldots, n\}$ na $\{1, 2, \ldots, n\}$ z działaniem $\circ$, które jest złożeniem. Takie bijekcje nazywamy też **permutacjami** zbioru $\{1, 2, \ldots, n\}$, a S_n - grupą permutacji. Permutacje należące do S_n możemy definiować podając tabelkę funkcji. Zwykle tabelka ma postać

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}.$$

Taka tabelka oznacza funkcję $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ zdefiniowaną wzorami $f(i) = a_i$ dla wszystkich $i = 1, 2, \ldots, n$. Grupa $(S_n, \circ)$ nie jest przemienna.

Definicja.

Strukturę algebraiczną $(G, \oplus, \odot)$ nazywamy **pierścieniem**, jeśli

1. $(G, \oplus)$ jest grupą przemienną.
2. Działanie $\odot$ jest wewnętrzne.
3. Działanie $\odot$ jest łączne.
4. Obustronna rozdzielność działania $\odot$ względem $\oplus$, tzn. dla wszystkich $a, b, c \in G$ zachodzi $a \odot (b \oplus c) = a \odot b \oplus a \odot c$ oraz $(b \oplus c) \odot a = b \odot a \oplus c \odot a$.

Np. Liczby całkowite z działaniami arytmetycznymi zwykłego dodawania i zwykłego mnożenia $(\mathbf{Z}, +, \cdot)$ tworzą pierścień.

Np. Zbiór rzeczywistych funkcji liniowych $f(x) = ax + b$, gdzie $a, b \in \mathbf{R}$ z dodawaniem i składaniem funkcji nie tworzy pierścienia. Należy zauważyć, że $f_1 \circ (f_2 + f_3) \neq f_1 \circ f_2 + f_1 \circ f_3$.

Definicja.

Strukturę algebraiczną $(K, \oplus, \odot)$ nazywamy **ciałem**, jeśli

1. $(K, \oplus)$ jest grupą przemienną.
2. $(K \setminus \{0\}, \odot)$ jest grupą przemienną, gdzie 0 oznacza element neutralny w grupie $(K, \oplus)$.
3. Działanie $\odot$ jest jednostronnie rozdzielne względem $\oplus$, tzn. dla wszystkich $a, b, c \in K$ zachodzi $a \odot (b \oplus c) = a \odot b \oplus a \odot c$ (przemienność $\odot$ zapewnia drugą rozdzielność).

Np. Zbiór liczb wymiernych $\mathbf{Q}$ ze zwykłymi działaniami $+, \cdot$ tworzy ciało.

Np. Zbiór liczb rzeczywistych $\mathbf{R}$ ze zwykłymi działaniami $+, \cdot$ tworzy ciało.

Np. Zbiór $\mathbf{Z_6} = \{0, 1, \ldots, 5\}$ z dodawaniem i mnożeniem modulo 6 nie jest ciałem. Należy zauważyć, że np. $2 \cdot_6 3 = 0$, a to oznacza, że mnożenie $\cdot_6$ nie jest działaniem wewnętrznym w $\mathbf{Z_6} \setminus \{0\}$.

Uwaga.

Zbiór $\mathbf{Z}_p = \{0, 1, \ldots, p-1\}$ z dodawaniem i mnożeniem modulo p jest ciałem wtedy i tylko wtedy, gdy p jest liczbą pierwszą.

Liczby pierwsze: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$ itd.

Uwaga.

Rozważmy zbiór $\mathbf{R}^2$ z działaniami $\oplus, \odot$ określonymi jako

$$(x, y) \oplus (z, t) = (x + z, y + t), \quad (x, y) \odot (z, t) = (xz - yt, yz + xt),$$

gdzie $(x, y), (z, t) \in \mathbf{R}^2$. Struktura $(\mathbf{R}^2, \oplus, \odot)$ jest ciałem.

Jako ćwiczenie uzasadnić powyższą Uwagę.

Uwaga.

Każde ciało jest pierścieniem.

Zastosowania grup, pierścieni i ciał w informatyce

Struktury algebraiczne takie jak grupy, pierścienie i ciała mają wiele zastosowań w informatyce – często w miejscach, gdzie ich obecność może nie być od razu oczywista. Oto jak każda z nich się przydaje.

Grupy abelowe to struktury, które opisują symetrie i operacje odwracalne. Ich zastosowania obejmują:

- **Kryptografia**: Grupy cykliczne są podstawą algorytmów takich jak Diffie-Hellman czy ElGamal.
- **Kompresja danych**: Permutacje (np. grupa S_n) są używane w algorytmach kodowania.
- **Grafika komputerowa**: Grupy transformacji są używane do manipulacji obiektami w przestrzeni 2D/3D.
- **Teoria automatów**: Grupy mogą opisywać symetrie w automatach i językach formalnych.

Pierścienie łączą dodawanie i mnożenie w jednej strukturze. Ich zastosowania to:

- **Arytmetyka modularna**: Wykorzystywana w kryptografii (np. RSA).
- **Kodowanie informacji**: Pierścienie są używane w teorii kodów (np. kody cykliczne).
- **Algebra komputerowa**: Systemy CAS operują na pierścieniach wielomianów.
- **Bazy danych**: Algebra relacyjna korzysta z podobnych zasad.

Ciała to pierścienie, w których każdy niezerowy element ma odwrotność. Są szczególnie ważne w:

- **Kryptografii**: Ciała skończone (np. $\mathrm{GF}(p)$, $\mathrm{GF}(2^n)$) są podstawą szyfrów symetrycznych.
- **Teorii kodów**: Kody liniowe (np. Hamminga, Reed-Solomon) działają nad ciałami skończonymi.
- **Grafice komputerowej**: Operacje na kolorach i pikselach mogą być modelowane jako działania w ciałach.
- **Algorytmach numerycznych**: Ciała liczb rzeczywistych i zespolonych są podstawą obliczeń.

Zadanie

Rozważmy zbiór $G = \{1, -1\}$ z działaniem mnożenia. Jest to bardzo mała, ale nietrywialna grupa, zwana grupą znaków.

- Zbuduj tabelę dla mnożenia w zbiorze $\{1, -1\}$.
- Sprawdź wszystkie warunki grupy.
- Uzasadnij, że jest to grupa abelowa.
- Po kolejnym wykładzie, zastanów się, czy $\{1, -1, i, -i\}$ z mnożeniem w liczbach zespolonych tworzy grupę.