ALGEBRA LINIOWA 2

dr Joanna Jureczko

Politechnika Wrocławska
Wydział Elektroniki
Katedra Telekomunikacji i Teleinformatyki

Niniejsza prezentacja stanowi jedynie skrypt do wykładu. Wykład będzie wzbogacony o dodatkowe informacje, tj. dowody wybranych twierdzeń przykłady, wskazówki do zadań itp. Dodatkowe informacje dotyczące programu znajdują się w Karcie Przedmiotu.

WYKŁAD 2

Kongruencje
Grupa
Grupa Z_n Grupa S_n

KONGRUENCJA

Mówimy, że a **przystaje** do b modulo m i piszemy $a \equiv b \ (mod\ m)$ jesli m jest dzielnikiem $b - a$. Relację przystawania modulo m nazywamy relacją **kongruencji**.

Twierdzenie 2.1. Następujące warunki są równoważne:
1. $a \equiv b \ (mod\ m)$.
2. Istnieje liczba $k \in \mathbb{Z}$ taka, że $a = b + km$.
3. Liczby a i b dają tę samą resztę przy dzieleniu przez m.

Twierdzenie 2.2 Dla dowolnych $a, b, c, d \in \mathbb{Z}$

1) jeśli $a \equiv b \pmod{n}$, to $-a \equiv -b \pmod{n}$ oraz $ca \equiv cb \pmod{n}$ dla każdej liczby $c \in \mathbb{Z}$.

2) jeśli $a \equiv b \pmod{n}$ oraz $c \equiv d \pmod{n}$, to
$a + c \equiv b + d \pmod{n}$ oraz $ac \equiv bd \pmod{n}$

3) Dla każdej liczby $a \in \mathbb{Z}$ istnieje dokładnie jedna liczba r, że $a \equiv r \pmod{n}$ i $0 \leqslant r < n$. Taką liczbę nazywamy **resztą liczby** a **modulo** n i oznaczamy $(a)_n$.

Twierdzenie 2.3. Dla dowolnych $a, b \in \mathbb{Z}$ oraz $n \in \mathbb{N}$ zachodzą wzory

1) $((a)_n + (b)_n)_n = (a+b)_n$

2) $(-(a)_n)_n = (-a)_n$

3) $((a)_n \cdot (b)_n)_n = (a \cdot b)_n$

4) $(m \cdot (a)_n)_n = (m \cdot a)_n$

5) $(((a)_n)^m)_n = (a^m)_n$

Klasę $\{b\colon b \equiv a \ (mod\ m)\} = a + m\mathbb{Z}$ nazywamy **klasą reszt** liczby a modulo m.

Zbiór wszystkich klas reszt modulo m oznaczamy symbolem $\mathbb{Z}/m\mathbb{Z}$. Ma on m elementów, (czyli reszty z dzielenia przez m).

GRUPA
GRUPA Z_n GRUPA S_n

Dany jest niepusty zbiór A z działaniem dwuargumentowym $\circ$.
Niech $a, b, c \in A$. Działanie $\circ$ nazywamy **łącznym**, gdy

$$(a \circ b) \circ c = a \circ (b \circ c).$$

Działanie $\circ$ nazywamy **przemiennym**, gdy

$$a \circ b = b \circ a.$$

Mówimy, że działanie $\circ$ ma **element neutralny** $e \in A$, gdy

$$a \circ e = e \circ a = a.$$

Każdy element $a' \in A$ taki, że

$$a' \circ a = a \circ a' = e$$

nazywamy **elementem symetrycznym, (przeciwnym, odwrotnym)** do a.

Grupą nazywamy system $(G, \circ)$, w którym G jest zbiorem niepustym, $\circ$ jest działaniem łącznym oraz w G istnieje element neutralny tego działania i element symetryczny do każdego elementu z G.
Grupę $(G, \circ)$ nazywamy **abelową (przemienną)**, gdy dodatkowo działanie $\circ$ jest przemienne.

Moc zbioru G, (tzn. liczbę jego elementów) nazywamy **rzędem** grupy G i oznaczamy $|G|$.

Przykłady grup

$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$
$(\mathbb{Z}^*, \cdot)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ gdzie $A^* = A \setminus \{0\}$.

Powyższe grupy są grupami abelowymi.

Niels Henrik Abel (1802 – 1829) norweski matematyk, zajmował się różnymi gałęziami matematyki. Jego prace z algebry koncentrowały się wokół **rozwiązywania równań algebraicznych piątego stopnia**. Zastosował do tego celu tak zwaną teorię grup. Ponadto Abel zajmował się równaniami całkowymi i funkcjami eliptycznymi. W zakresie teorii liczb rozważał natomiast **zbieżność szeregów liczbowych i potęgowych**. Pozostawił po sobie dotyczące tego problemu tak zwane twierdzenia Abela. W wieku lat 16 **udowodnił wzór dwumianowy Newtona dla dowolnego wykładnika rzeczywistego**.

Grupy reszt (modulo n).

Niech n będzie liczbą naturalną większą od 0.
Zbiór

$$\mathbb{Z}_n = \{0, 1, ..., n-1\}$$

z określonym działaniem

$$a \oplus b = (a+b)_n,$$

jest grupą. Oznaczamy ją $(\mathbb{Z}_n, \oplus)$.

Zbiór

$$U(\mathbb{Z}_n) = \{k \in \mathbb{Z}_n \colon NWD(k,n) = 1\}$$

z działaniem

$$a \odot b = (a \cdot b)_n,$$

jest grupą. Oznaczamy ją $(U(\mathbb{Z}_n), \odot)$.

Grupy przekształceń

Niech X będzie zbiorem niepustym oraz

$$S(X) = \{f \colon f \colon X \to X \ f \text{ jest bijekcją}\}.$$

$(S(X), \circ)$ jest grupą z działaniem składanie funkcji $\circ$, którą nazywamy **grupą przekształceń** lub **grupą symetryczną** zbioru X.

Twierdzenie 2.4 (Cayleya). Każda grupa $(X, \circ)$ jest izomorficzna z podrupą grupy symetrycznej $(S(X), \circ)$.

Arthur Cayley (1821–1895) – angielski matematyk i prawnik. Zajmował się geometrią algebraiczną. Prowadził badania nad równaniami różniczkowymi i funkcjami eliptycznymi. Współtwórca teorii wyznaczników. Autor wielu pojęć z algebry liniowej. Autor **pierwszej aksjomatycznej definicji grupy** oraz **twierdzenia Cayleya**. Opracował metodę wyznaczania liczby izomerów związków organicznych. Zajmował się także astronomią i astrofizyką.

Grupa permutacji

Niech M będzie zbiorem skończonym. **Permutacją** zbioru M nazywamy odwozorowanie wzajemnie jednoznaczne g zbioru M na M.

Grupę wszystkich permutacji zbioru M nazywamy **grupą symetryczną** lub **grupą permutacji** zbioru M i oznaczamy symbolem $S(M)$.

Jeżeli $|M| = n$, to oznaczamy ją również krótko S_n. Oczywiście S_n jest izomorficzne z $S(N)$ dla każdego n-elementowego zbioru N oraz

$$|S_n| = n!.$$

Grupa S_n na ogół nie jest przemienna.

Permutację, która zachowuje każdy element nazywamy **identycznościową (tożsamościową)** i oznaczamy e.
Oczywiście mamy

$$e \circ g = g \circ e = g.$$

Dla każdej permutacji g zbioru M istnieje permutacja g' tego zbioru taka, że

$$g \circ g' = g' \circ g = e.$$

Nazywamy ją permutacją **odwrotną** do g i oznaczamy g^{-1}.

Zapis permutacji

Przykład Niech $M = \{a, b, c, d, e, f\}$. Wtedy zapisy

$$\begin{pmatrix} a & b & c & d & e & f \\ b & c & a & e & d & f \end{pmatrix},$$

$$\begin{pmatrix} a & c & f & e & d & b \\ b & a & f & d & e & c \end{pmatrix},$$

$$\begin{pmatrix} e & f & a & c & d & b \\ d & f & b & a & e & c \end{pmatrix},$$

przedstawiają tę samą permutację g zbioru M, która przeprowadza element a na b, b na c, itd.

Wynik działania permutacji g na pewnym elemencie $a \in M$ (tzn. obraz wartości funkcji $g(a)$ elementu a przy działaniu g) oznaczamy a^g.

Gdy za M bierzemy zbiór początkowych liczb naturalnych, tzn. $M = \{1, 2, ..., n\}$, to umawiamy się raz na zawsze, że w pierwszym wierszu zapisu dowolnej permutacji piszemy liczby w naturalnym porządku.

Innym zapisem permutacji jest zapis w postaci grafów. (ciąg dalszy o grafach na Matematyce Dyskretnej lub Zaawansowanej Kombinatoryce).

Iloczynem (złożeniem, superpozycją) $g \circ h$, (krótko gh), permutacji g i h nazywamy permutację f zbioru M określoną za pomocą warunku

$$a^f = (a^g)^h, \quad a \in M.$$

Iloczyn dwóch permutacji jest permutacją.
Jeśli $(g_1 g_2 ... g_k)^{-1} = g_k^{-1} ... g_2^{-1} g_1^{-1}$.
Iloczyn permutacji na ogół nie jest przemienny.

Twierdzenie 2.6. Podzbiór niepusty $G \subseteq S_n$ jest grupą, gdy jest zamknięty ze względu na działanie $\circ$, tzn.

$$g_1 \circ g_2 \in G, \quad g_1, g_2, \in G.$$

Liczbę naturalną m nazywamy **rzędem** elementu g grupy G, jeżeli $g^m = e$ oraz $g^k \neq e$ dla każdego $k < m$.

Każdą permutację można przedstawić w postaci iloczynu cykli rozłącznych.

Cykl długości r w S_n ma rząd r.

Rząd permutacji g jest równy najmniejszej wspólnej wielokrotności (NWW) długości jego rozłącznych cykli.

Permutację g nazywamy **transpozycją** elementów a, b, jeżeli w jej rozkładzie na cykle występuje cykl ab długości 2, a pozostałe cykle mają długość 1.

W zapisie permutacji możemy opuszczać cykle długości 1.

Permutację g nazywamy **parzystą**, jeśli daje się ona przedstawić w postaci iloczynu parzystej liczby transpozycji. W przeciwnym przypadku permutację nazywamy nieparzystą.

Każda transpozycja jest nieparzysta.

Każdy cykl długości r jest iloczynem $r-1$ transpozycji (niekoniecznie rozłącznych). Dokładniej

$$(a_1 a_2 ... a_r) = (a_1 a_2) \circ (a_2 a_3) \circ ... \circ (a_{r-1} a_r).$$

Każda permutacja jest iloczynem transpozycji.

Cykl długości n jest permutacją parzystą, gdy n jest liczbą nieparzystą oraz permutacją nieparzystą, gdy n jest liczbą parzystą.

Grupa obrotów

Rozważmy figury Φ na płaszczyżnie $\mathbb{R}^2$ lub w przestrzeni $\mathbb{R}^3$, które można opisać za pomocą skończonego zbioru punktów $V(\Phi)$ i pewnych odcinków łączących te punkty. (Można taką figurę interpretować jako graf o wierzchołkach zawartych w płaszczyźnie lub w przestrzeni).

Izometrią figury płaskiej nazywamy taką izometrią płaszczyzny, która przeprowadza tę figurę w siebie. Podobnie określamy izometrie figur w przestrzeni. Zbiór wszystkich izometrii figury Φ oznaczamy przez $D(\phi)$.
$D(\Phi)$ jest grupą ze względu na składanie izometrii, którą będziemy nazywać **grupą izometrii** figury Φ.
W grupie $D(\Phi)$ wyróżniamy grupę $D^+(\Phi)$ wszystkich izometrii parzystych, (tzn. przesunięć i obrotów ale nie symetrii osiowych, przy których płaszczyzna zostaje "odwrócona").
$D^+(\Phi)$ będziemy nazywać **grupą obrotów** figury Φ.