

DALG LMO
Wstęp do algebry i teorii liczb
Semestr zimowy 2015/2016

Wykładowca: prof. dr hab. Wojciech Gajda
Miejsce pracy: Zakład Geometrii Algebraicznej
Collegium Mathematicum UAM,
Umultowska 87, B1-35
Dyżur: Wtorek 12-13, Czwartek 12-13
Telefon: (61)8295503

Literatura uzupełniająca do wykładu

A. Białynicki-Birula, *Algebra*, PWN 1980
T. Fryska, *Wstęp do algebry i teorii liczb*, UAM 1997
A. Iwaszkiewicz-Rudoszańska, *Wstęp do algebry i teorii liczb*, UAM 2009
A. Kostrykin, *Wstęp do algebry*, PWN 1984
A. Kostrykin, *Zbiór zadań z algebry*, PWN 1995
G. Banaszak, W. Gajda, *Elementy algebry liniowej I*, WNT 2002, zadania do rozdziału pierwszego.

Zaliczenie wykładu

Ocenę końcową z przedmiotu uzyskacie Państwo podczas egzaminu ustnego, który odbędzie się w sesji egzaminacyjnej w lutym 2016. Podczas dwugodzinnego egzaminu pisemnego będziecie rozwiązywać zadania zbliżone do zadań z kolokwiów oraz odpowiadać pisemnie na pytania dotyczące pojęć i twierdzeń omówionych na wykładzie. Ocenę z ćwiczeń uzyskacie na podstawie zebranych w ciągu semestru punktów według podanej poniżej skali. Pełną informację dotyczącą zaliczenia uzyskacie Państwo na ćwiczeniach. Podczas zajęć odbędą się dwa kolokwia: **4 grudnia i 22 stycznia**. Kolokwia składać się będą z 6-8 zadań.

Skala Ocen (orientacyjna)

dostateczny	powyżej 50 %
dobry	od 70 %
bardzo dobry	od 85 %

Program wykładu DALG LMO

Wstęp do algebry i teorii liczb,

wykładowca: prof. dr hab. Wojciech Gajda

Zima 2015/2016

Podstawowe struktury algebraiczne (dwa wykłady):

działanie w zbiorze, własności działań, grupa, pierścień, dziedzina całkowitości, ciało, **przykłady:** $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{Z}/n$, $\mathbf{F}_2$, grupy dihedralne: D_3 i D_4 , grupa permutacji Σ_3 , rząd elementu grupy, podgrupa, homomorfizm, izomorfizm struktur algebraicznych, np. $D_3 \cong \Sigma_3$

Permutacje i grupy symetrii (dwa wykłady):

składanie i rozkład permutacji na rozłączne cykle, grupa Σ_n , znak permutacji, grupa alternująca A_n

Pierścień liczb całkowitych $\mathbf{Z}$ (trzy wykłady):

zasada indukcji skończonej, podzielność w pierścieniu $\mathbf{Z}$, algorytm Euklidesa, NWD i NWW, zasadnicze twierdzenie arytmetyki, *istnieje ∞ wiele liczb pierwszych*, liczby Fermata i Mersenne'a, informacje o funkcji $\pi(x)$ i o podstawowych problemach o liczbach pierwszych, ciało liczb wymiernych $\mathbf{Q}$ jako ciało ułamków dziedziny całkowitości $\mathbf{Z}$

Kongruencje (dwa wykłady):

klasy i układy reszt modulo n , pierścień $\mathbf{Z}/n$, grupa jedności $(\mathbf{Z}/n)^\times$, ciało skończone $\mathbf{F}_p$, małe twierdzenie Fermata, twierdzenie Eulera, układy kongruencji i równań liniowych, twierdzenie chińskie o resztach dla $\mathbf{Z}/mn$, informacja o protokóle RSA, eliminacja Gaussa-Jordana nad ciałem $\mathbf{Q}$

Ciało liczb rzeczywistych $\mathbf{R}$ i ciało liczb zespolonych $\mathbf{C}$ (dwa wykłady):

konstrukcja ciała $\mathbf{R}^1$, ciało $\mathbf{C}$, postać trygonometryczna liczby zespolonej, wzory de Moivre'a, pierwiastki z liczb zespolonych i pierwiastki z jedynki, grupa okręgu i jej podgrupy cykliczne

Pierścień wielomianów jednej zmiennej o współczynnikach z podpierścienia ciała $\mathbf{C}$ (dwa wykłady):

konstrukcja pierścienia $K[x]$, ciało funkcji wymiernych, algorytm Euklidesa w $K[x]$ dla podciała $K \subset \mathbf{C}$ np. dla $K = \mathbf{Q}$, stopień i pierwiastki wielomianu, twierdzenie Bezoute'a, wzory Cardano/Tartaglii na pierwiastki wielomianów stopni 3 i 4.

¹Konstrukcję ciała liczb rzeczywistych omówię tylko wtedy na wykładzie DALG LMO, jeśli okaże się, że nie było jej jeszcze na wykładzie z analizy