

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI/KATEDRA PODSTAW INFORMATYKI					
KARTA PRZEDMIOTU					
Nazwa przedmiotu w języku polskim	: Algebra Abstrakcyjna i Kodowanie				
Nazwa przedmiotu w języku angielskim	: Abstract Algebra and Coding				
Kierunek studiów	: Informatyka algorytmiczna				
Specjalność (jeśli dotyczy)	: —				
Poziom i forma studiów	: I stopień, stacjonarna				
Rodzaj przedmiotu	: obowiązkowy				
Język wykładowy	: polski				
Cykl kształcenia od	: 2024/2025				
Kod przedmiotu	: W04INA-SI0031G				
Grupa zajęć	: TAK				
	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30	30			
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	50	75			
Forma zaliczenia	egzamin				
Dla grupy kursów zaznaczyć kurs końcowy	X				
Liczba punktów ECTS	2	3			
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)		3			
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	2,88				
WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH					
CELE PRZEDMIOTU					
C1 Poznanie podstawowych struktur algebry oraz ich własności. Zapoznanie z podstawami teorii kodowania.					
C2 Rozwiązywanie problemów dotyczących pojęć poznanych na wykładzie.					

PRZEDMIOTOWE EFEKTY UCZENIA SIĘ

Z zakresu wiedzy studenta:

- W1** Zna podstawowe pojęcia i twierdzenia teorii grup oraz zastosowania tej wiedzy w kryptografii.
- W2** Zna podstawowe pojęcia i twierdzenia teorii pierścieni oraz zastosowania tej wiedzy w kryptografii.
- W3** Zna proste zastosowanie teorii grup i pierścieni w teorii liczb.
- W4** Zna podstawy teorii ciał.
- W5** Zna podstawowe pojęcia i twierdzenia teorii kodowania.

Z zakresu umiejętności studenta:

- U1** Potrafi wykonywać obliczenia w zadanych grupach, pierścieniach i ciałach, sprawdzać rząd elementu, charakterystykę ciała.
- U2** Potrafi konstruować ciała skończone, produkty oraz ilorazy grup i pierścieni.
- U3** Potrafi wyznaczyć parametry kodu blokowego, macierze: generującą i parzystości kodu.

Z zakresu kompetencji społecznych studenta:

- K1** Rozumie znaczenie struktur algebraicznych w kryptografii.
- K2** Rozumie znaczenie algebry w konstrukcji kodów korekcyjnych.

TREŚCI PROGRAMOWE

Forma zajęć - wykład		
Wy1	Podstawy teorii grup.	4h
Wy2	Twierdzenie Eulera-Fermata. Protokół Diffiego-Hellmana.	2h
Wy3	Grupy ilorazowe i homomorfizmy.	4h
Wy4	Podstawy teorii pierścieni.	2h
Wy5	Pierścienie ilorazowe i homomorfizmy.	2h
Wy6	Funkcja Eulera. Chińskie Twierdzenie o resztach.	2h
Wy7	Protokół RSA.	2h
Wy8	Klasy pierścieni ID, UFD, PID, ED.	2h
Wy9	Ciała.	2h
Wy10	Kody blokowe.	2h
Wy11	Kody liniowe.	4h
Wy12	Kody cykliczne.	2h
	Suma godzin	30h

Forma zajęć - ćwiczenia		
Ćw1	Grupy, podgrupy, grafy Cayleya.	4h
Ćw2	Rząd elementu, grupa cykliczna.	2h
Ćw3	Warstwa w grupie. Grupa ilorazowa, dzielnik normalny.	2h
Ćw4	Homomorfizmy grup.	2h
Ćw5	Pierścienie oraz ich podpierścienie.	2h
Ćw6	Ideały, pierścienie ilorazowe.	4h
Ćw7	Elementy teorii liczb.	4h
Ćw8	Elementy kryptografii.	2h
Ćw9	Ciała.	2h
Ćw10	Blokowe kody liniowe, metryka i waga Hamminga.	2h
Ćw11	Kod Hamminga wykrywanie i korekcja błędów.	2h
Ćw12	Kolokwium.	2h
	Suma godzin	30h

STOSOWANE NARZĘDZIA DYDAKTYCZNE

1. Wykład tradycyjny
2. Rozwiązywanie zadań i problemów
3. Konsultacje
4. Praca własna studentów

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA SIĘ

Oceny (F - formatująca (w trakcie semestru), P - podsumowująca (na koniec semestru))	Numer efektu uczenia się	Sposób oceny osiągnięcia efektu uczenia się
F1	W1-W5, K1-K2	Egzamin
F2	U1-U3, K1-K2	Sprawdziany, odpowiedź ustna.
$P=50\%*F1+50\%*F2$		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

1. A. Białyński-Birula, Algebra, PWN, 2021
2. J. Rutkowski, Algebra abstrakcyjna w zadaniach, PWN, Warszawa 2005
3. W. Mochnacki, Kody korekcyjne i kryptografia, Oficyna Wyd. PWr, Wrocław 2000
4. R. Hill, A First Course in Coding Theory, Oxford Applied Mathematics and Computing Science Series., 1997
5. L. Gilbert, J. Gilbert, Elements of Modern Algebra, Brooks/Cole, Cengage Learning, 2009
6. J. Adamek, Foundations of coding. Theory and application of error-correcting codes, Wiley 1991
7. N. Koblitz, Algebraiczne aspekty kryptografii, WNT 2000

NAUCZYCIEL AKADEMICKI ODPOWIEDZIALNY ZA PRZEDMIOT

dr Krzysztof Majcher

MACIERZ POWIĄZANIA EFEKTÓW UCZENIA SIĘ DLA PRZEDMIOTU
Algebra Abstrakcyjna i Kodowanie
Z EFEKTAMI UCZENIA SIĘ NA KIERUNKU INFORMATYKA ALGORYTMICZNA

Przedmiotowy efekt uczenia się	Odniesienie przedmiotowego efektu do efektów uczenia się zdefiniowanych dla kierunku studiów	Cele przedmiotu**	Treści programowe**	Numer na- rzędzia dydaktycz- nego**
W1	K1_W01	C1	Wy1-Wy12	1 3 4
W2	K1_W01	C1	Wy1-Wy12	1 3 4
W3	K1_W01	C1	Wy1-Wy12	1 3 4
W4	K1_W01	C1	Wy1-Wy12	1 3 4
W5	K1_W01	C1	Wy1-Wy12	1 3 4
U1	K1_U07	C2	Ćw1-Ćw12	2 3 4
U2	K1_U07	C2	Ćw1-Ćw12	2 3 4
U3	K1_U07	C2	Ćw1-Ćw12	2 3 4
K1	K1_K01 K1_K02	C1 C2	Wy1-Wy12 Ćw1-Ćw12	1 2 3 4
K2	K1_K03 K1_K05	C1 C2	Wy1-Wy12 Ćw1-Ćw12	1 2 3 4