Zał. nr 5 do ZW 13/2019
Załącznik nr ..... do programu studiów

WYDZIAŁ PODSTAWOWYCH PROBLEMÓW TECHNIKI

KARTA PRZEDMIOTU

Nazwa w języku polskim	:	**Wybrane Zagadnienia Algebry**
Nazwa w języku angielskim	:	**Selected Topics from Algebra**
Kierunek studiów	:	Informatyka algorytmiczna
Specjalność (jeśli dotyczy)	:	
Stopień studiów i forma	:	inżynierskie, stacjonarne
Rodzaj przedmiotu	:	wybieralny
Kod przedmiotu	:	E1_W12
Grupa kursów	:	TAK

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30	15	15		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	60	60	60		
Forma zaliczenia	zaliczenie				
Dla grupy kursów zaznaczyć kurs końcowy	X				
Liczba punktów ECTS	2	2	2		
w tym liczba odpowiadająca zajęciom o charakterze praktycznym (P)		2	2		
w tym liczba punktów odpowiadająca zajęciom wymagającym bezpośredniego kontaktu (BK)	2	2	2		

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

Algebra z Geometrią Analityczną , Algebra Abstrakcyjna i Kodowanie.

CELE PRZEDMIOTU

C1 Rozszerzenie i utrwalenie zdobytej wiedzy na temat algebry. Zapoznanie z zagadnieniami algebry mającymi związek z informatyką

C2 Lepsze zrozumienie matriału omawianego na wykładzie.

C3 Zapoznanie z algorytmami omawianymi na wykładzie.

PRZEDMIOTOWE EFEKTY KSZTAŁCENIA

Z zakresu wiedzy studenta:

W1 Zna pojęcia grafu Cayleya grupy. Zna twierdzenia Cayleya i Sylowa. Zna działanie grupowe na krzywych eliptycznych.

W2 Zna pojęcia ideał, ideał główny, ideał maksymalny. Zna konstrukcje pierścienia ilorazowego, oraz zastosowanie konstrukcji do budowy ciał rozkładu wielomianów.

W3 Zna pojęcie rozszerzenia ciała i grupy Galois. Zna zastosowanie teorii Galois.

Z zakresu umiejętności studenta:

U1 Potrafi sprawdzać wybrane własności omawianych struktur algebraicznych.

U2 Potrafi implementować omawiane algorytmy.

Z zakresu kompetencji społecznych studenta:

K1 Rozumie znaczenie algebry w informatyce, w szczególności w kryptografii.

TREŚCI PROGRAMOWE

Forma zajęć - wykłady		
Wy1	Grupy.	4h
Wy2	Grupy abelowe, grupy cykliczne.	4h
Wy3	Twierdzenie Sylowa.	2h
Wy4	Zastosowanie grup w kryptografii.	2h
Wy5	Krzywe eliptyczne.	4h
Wy6	Pierścienie.	4h
Wy7	Elementy teorii liczb.	4h
Wy8	Ciała.	4h
Wy9	Teoria Galois.	4h

Forma zajęć - ćwiczenia		
Ćw1	Grupy.	2h
Ćw2	Grupy abelowe, grupy cykliczne.	2h
Ćw3	Twierdzenie Sylowa.	1h
Ćw4	Zastosowanie grup w kryptografii.	1h
Ćw5	Krzywe eliptyczne	1h
Ćw6	Pierścienie.	2h
Ćw7	Elementy teorii liczb.	2h
Ćw8	Ciała.	2h
Ćw9	Teoria Galois.	2h

Forma zajęć - laboratorium		
Lab1	Mnożenie i potęgowanie w wybranych grupach.	2h
Lab2	Mnożenie na krzywych eliptycznych.	4h
Lab3	Protokół Diffiego–Hellmana.	4h
Lab4	Algorytm Euklidesa	2h
Lab5	Rozkładanie wielomianów nad ciałami skończonymi.	3h

STOSOWANE NARZĘDZIA DYDAKTYCZNE

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

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW KSZTAŁCENIA

Oceny	Numer efektu kształcenia	Sposób oceny efektu kształcenia
F1	W1-W3, K1-K1	Kolokwium
F2	U1-U2, K1-K1	Kartkówki,ocena aktywnośic.
F3	U1-U2, K1-K1	ocena programów oddanych przez studenta.
P=30%*F1+40%*F2+30%*F3		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

1. Victor Shoup, A Computational Introduction to Number Theory and Algebra
2. J.S. Milne, Group Theory
3. S.Lang, Algebra

OPIEKUN PRZEDMIOTU

dr Krzysztof Majcher

MACIERZ POWIĄZANIA EFEKTÓW KSZTAŁCENIA DLA PRZEDMIOTU
Wybrane Zagadnienia Algebry
Z EFEKTAMI KSZTAŁCENIA NA KIERUNKU INFORMATYKA ALGORYTMICZNA

Przedmiotowy efekt kształcenia	Odniesienie przedmiotowego efektu do efektów kształcenia zdefiniowanych dla kierunku studiów i specjalności (o ile dotyczy)	Cele przedmiotu**	Treści programowe**	Numer narzędzia dydaktycznego**
W1	K1_W01	C1	Wy1-Wy9	1 4
W2	K1_W01	C1	Wy1-Wy9	1 4
W3	K1_W02	C1	Wy1-Wy9	1 4
U1	K1_U31	C2 C3	Ćw1-Ćw9 Lab1-Lab5	2 3 4
U2	K1_U13	C2 C3	Ćw1-Ćw9 Lab1-Lab5	2 3 4
K1	K1_K11	C1 C2 C3	Wy1-Wy9 Ćw1-Ćw9 Lab1-Lab5	1 2 3 4