

WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI					
<b>KARTA PRZEDMIOTU</b>					
<b>Nazwa przedmiotu w języku polskim</b>	: Wybrane Zagadnienia Algebry				
<b>Nazwa przedmiotu w języku angielskim</b>	: Selected Topics from Algebra				
<b>Kierunek studiów</b>	: Informatyka algorytmiczna				
<b>Specjalność (jeśli dotyczy)</b>	: —				
<b>Poziom i forma studiów</b>	: I stopień, stacjonarna				
<b>Rodzaj przedmiotu</b>	: wybieralny				
<b>Kod przedmiotu</b>	: INP002279Wcl				
<b>Grupa kursów</b>	: 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 punktów odpowiadająca zajęciom o charakterze praktycznym (P)		2	2		
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego udziału nauczycieli lub innych osób prowadzących zajęcia (BU)	2	1	1		
<b>WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I KOMPETENCJI SPOŁECZNYCH</b>					
Algebra z Geometrią Analityczną , Algebra Abstrakcyjna i Kodowanie.					
<b>CELE PRZEDMIOTU</b>					
<b>C1</b> Rozszerzenie i utrwalenie zdobytej wiedzy na temat algebry. Zapoznanie z zagadnieniami algebry mającymi związek z informatyką					
<b>C2</b> Lepsze zrozumienie materiału omawianego na wykładzie.					
<b>C3</b> Zapoznanie z algorytmami omawianymi na wykładzie.					

## PRZEDMIOTOWE EFEKTY KSZTAŁCENIA

Z zakresu wiedzy studenta:

**W1** Zna pojęcia i twierdzenia dotyczące przestrzeni unitarnej, twierdzenie spektralne. Rozumie metodę PCA.

**W2** Zna pojęcia przestrzeni rzutowej i grupy eliptycznej, oraz ich zastosowania.

**W3** Zna pojęcie bazy Gröbnera ideału, zna jej zastosowania.

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 - wykład

Wy1	Przestrzenie unitarne.	2h
Wy2	Przestrzeń probabilistyczna, zmienna losowa, kowariancja.	2h
Wy3	Analiza głównych składowych.	6h
Wy4	Grupy i ciała skończone	2h
Wy5	Przestrzenie rzutowe.	2h
Wy6	Grupy eliptyczne	6h
Wy7	Pierścienie.	2h
Wy8	Pierścień wielomianów, twierdzenie Hilberta.	2h
Wy9	Bazy Gröbnera.	6h
	Suma godzin	30h

### Forma zajęć - ćwiczenia

Ćw1	Wartości i wektory własne macierzy. Diagonalizacja.	1h
Ćw2	Rzut ortogonalny, ortogonalizacja. Macierze unitarne i hermitowskie	2h
Ćw3	Przestrzeń probabilistyczna, zmienna losowa, kowariancja.	1h
Ćw4	Analiza głównych składowych	2h
Ćw5	Grupy	1h
Ćw6	Przestrzenie rzutowe, współrzędne jednorodnie.	2h
Ćw7	Pierścienie, ideały, baza ideału.	2h
Ćw8	Pierścień wielomianów, twierdzenie Hilberta.	2h
Ćw9	Bazy Gröbnera.	2h
	Suma godzin	15h

### Forma zajęć - laboratorium

Lab1	Implementacja algorytmu PCA	5h
Lab2	Mnożenie na krzywych eliptycznych. Protokół Diffiego–Hellmana.	5h
Lab3	Bazy Gröbnera. Algorytm Buchbergera.	5h
	Suma godzin	15h

**STOSOWANE NARZĘDZIA DYDAKTYCZNE**

1. Wykład tradycyjny
2. Rozwiązywanie zadań i problemów
3. Rozwiązywanie zadań programistycznych
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-W3, K1-K1	Kolokwium
F2	U1-U2, K1-K1	Kartkówki, ocena aktywności.
F3	U1-U2, K1-K1	ocena programów oddanych przez studenta.

$$P=0.3\%*F1+0.4\%*F2+0.3\%*F3$$

**LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA**

1. A. Białyński-Birula, Algebra, PWN, 2021
2. A.I.Kostrikin, Wstęp do algebry. Algebra liniowa, PWN, 2012.
3. N. Koblitz, Algebraiczne aspekty kryptografii.
4. M. Dumnicki, T. Winiarski, Bazy Gröbnera, Wydawnictwo Naukowe Akademii Pedagogicznej- Kraków 2007
5. W. Adams, P.Loustaunau, An Introduction to Grobner Bases, AMS 1997.
6. J.S. Milne, Group Theory
7. Victor Shoup, A Computational Introduction to Number Theory and Algebra

**OPIEKUN PRZEDMIOTU**

dr Krzysztof Majcher

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

Przedmiotowy efekt uczenia się	Odniesienie przedmiotowego efektu do efektów uczenia się 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-Lab3	2 3 4
U2	K1_U13	C2 C3	Ćw1-Ćw9 Lab1-Lab3	2 3 4
K1	K1_K14	C1 C2 C3	Wy1-Wy9 Ćw1-Ćw9 Lab1-Lab3	1 2 3 4