

# POLITECHNIKA KRAKOWSKA IM. TADEUSZA KOŚCIUSZKI

## KARTA PRZEDMIOTU

obowiązuje studentów rozpoczynających studia w roku akademickim 2020/2021

Wydział Informatyki i Telekomunikacji

Kierunek studiów: Informatyka

Profil: Ogólnoakademicki

Forma studiów: stacjonarne

Kod kierunku: I

Stopień studiów: II

Specjalności: Cyberbezpieczeństwo

### 1 INFORMACJE O PRZEDMIOCIE

|                                         |                            |
|-----------------------------------------|----------------------------|
| NAZWA PRZEDMIOTU                        | Algebra z teorią liczb     |
| NAZWA PRZEDMIOTU<br>W JĘZYKU ANGIELSKIM | Algebra and Number Theory  |
| KOD PRZEDMIOTU                          | WiT I oIIS D1 20/21        |
| KATEGORIA PRZEDMIOTU                    | Przedmioty specjalnościowe |
| LICZBA PUNKTÓW ECTS                     | 4.00                       |
| SEMESTRY                                | 1                          |

### 2 RODZAJ ZAJĘĆ, LICZBA GODZIN W PLANIE STUDIÓW

| SEMESTR | WYKŁAD | ĆWICZENIA | LABORATORIUM | LABORATORIUM<br>KOMPUTERO-<br>WE | SEMINARIUM | PROJEKT |
|---------|--------|-----------|--------------|----------------------------------|------------|---------|
| 1       | 30     | 30        | 0            | 0                                | 0          | 0       |

### 3 CELE PRZEDMIOTU

**Cel 1** Zapoznanie studentów z podstawowymi pojęciami i zagadnieniami współczesnej algebry abstrakcyjnej oraz teorii liczb w zakresie podstaw teorii grup, teorii pierścieni łącznych, teorii ciał i ich zastosowań, arytmetyki liczb całkowitych i arytmetyki modularnej umożliwiającym jak rozwiązywanie standardowych problemów tak i późniejsze wykorzystywanie ich w kodowaniu, kryptografii i kryptoanalizie

## 4 WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

1 Zaliczenie algebry z geometrią na pierwszym stopniu studiów informatycznych

## 5 EFEKTY KSZTAŁCENIA

**EK1 Wiedza** Student zna, rozumie i objaśnia podstawowe pojęcia i zagadnienia algebry i teorii liczb, potrafi rozwiązać standardowy problem stosujący się do podstawowych pojęć algebry abstrakcyjnej oraz teorii liczb i opierający się na podstawowych zagadnieniach algebry abstrakcyjnej

**EK2 Umiejętności** Student potrafi nie tylko prawidłowo sformułować podstawowe pojęcia i zagadnienia algebry i teorii liczb, lecz również zilustrować go umiejętnie podebranymi przykładami

**EK3 Wiedza** Student nie tylko zna podstawowe pojęcia i zagadnienia współczesnej algebry abstrakcyjnej oraz teorii liczb, lecz również może budować dowody twierdzeń opierających się na podstawowych faktach z teorii oraz przykłady zarówno ilustrujące pojęcia algebry abstrakcyjnej, jak i pozwalające obalić błędne hipotezy lub nieuprawnione rozumowania

**EK4 Kompetencje społeczne** Student potrafi formułować opinie na temat podstawowych zagadnień z algebry abstrakcyjnej oraz teorii liczb, potrafi samodzielnie wyszukiwać w literaturze, także w językach obcych

## 6 TREŚCI PROGRAMOWE

| WYKŁAD    |                                                                                                                                                                                                                                                                                                                             |                  |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| LP        | TEMATYKA ZAJĘĆ<br>OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH                                                                                                                                                                                                                                                                      | LICZBA<br>GODZIN |
| <b>W1</b> | Teoria grup: podgrupy, warstwy, indeks podgrupy, twierdzenie Lagrange'a dla grup skończonych, podgrupy normalne, grupy ilorazowe, homomorfizmy i izomorfizmy grup, grupy cykliczne i ich podgrupy, izomorficzna klasyfikacja grup cyklicznych, grupy przekształceń, produkty i sumy proste grup, działania grupy na zbiorze | 7                |
| <b>W2</b> | Podstawowe struktury algebraiczne: pierścienie, ciała, charakterystyka, dzielniki zera, elementy odwrotne                                                                                                                                                                                                                   | 2                |
| <b>W3</b> | Arytmetyka liczb całkowitych: dzielenie z resztą, rozszerzony algorytm Euklidesa, NWW, NWD, liczby pierwsze, zasadnicze twierdzenie arytmetyki, rozkład kanoniczny, twierdzenie Euklidesa o liczbach pierwszych, sito Eratostenesa, systemy liczbowe                                                                        | 3                |
| <b>W4</b> | Arytmetyka modularna: relacja przystawania modulo $n$ , pierścienie $\mathbb{Z}_n$ , funkcje arytmetyczne, twierdzenia Eulera i Fermata, logarytmy dyskretne – podstawowe własności, kongruencje liniowe, układy kongruencji liniowych, chińskie twierdzenie o resztach, reszty i niereszty kwadratowe                      | 10               |
| <b>W5</b> | Ułamki łańcuchowe i ich zastosowania, równania diofantyczne                                                                                                                                                                                                                                                                 | 2                |
| <b>W6</b> | Teoria ciał: rozszerzenie ciał (proste, skończone, algebraiczne), wielomian minimalny elementu algebraicznego nad ciałem, elementy transcendentne, struktura prostego rozszerzenia ciał, ciało rozkładu wielomianu                                                                                                          | 6                |

| ĆWICZENIA |                                                                                                                                                                                                                                                                                                                            |                  |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| LP        | TEMATYKA ZAJĘĆ<br>OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH                                                                                                                                                                                                                                                                     | LICZBA<br>GODZIN |
| C1        | Teoria grup: podgrupy, warstwy, indeks podgrupy, twierdzenie Lagrange'a dla grup skończonych, podgrupy normalne, grupy ilorazowe, homomorfizmy i izomorfizmy grup grupy cykliczne i ich podgrupy, izomorficzna klasyfikacja grup cyklicznych, grupy przekształceń, produkty i sumy proste grup, działania grupy na zbiorze | 7                |
| C2        | Podstawowe struktury algebraiczne: pierścienie, ciała, charakterystyka, dzielniki zera, elementy odwrotne                                                                                                                                                                                                                  | 2                |
| C3        | Arytmetyka liczb całkowitych: dzielenie z resztą, rozszerzony algorytm Euklidesa, NWW, NWD, liczby pierwsze, zasadnicze twierdzenie arytmetyki, rozkład kanoniczny, twierdzenie Euklidesa o liczbach pierwszych, sito Eratostenesa, systemy liczbowe                                                                       | 3                |
| C4        | Arytmetyka modularna: relacja przystawania modulo $n$ , pierścień $Z_n$ , funkcje arytmetyczne, twierdzenia Eulera i Fermata, logarytmy dyskretne – podstawowe własności, kongruencje liniowe, układy kongruencji liniowych, chińskie twierdzenie o resztach, reszty i niereszyt kwadratowe                                | 10               |
| C5        | Ułamki łańcuchowe i ich zastosowania, równania diofantyczne                                                                                                                                                                                                                                                                | 2                |
| C6        | Teoria ciał: rozszerzenie ciał (proste, skończone, algebraiczne), wielomian minimalny elementu algebraicznego nad ciałem, elementy transcendentne, struktura prostego rozszerzenia ciał, ciało rozkładu wielomianu                                                                                                         | 6                |

## 7 NARZĘDZIA DYDAKTYCZNE

N1 Wykłady

N2 Konsultacje

N3 Dyskusja

N4 Praca w grupach

## 8 OBCIĄŻENIE PRACĄ STUDENTA

| FORMA AKTYWNOŚCI                                                                                 | ŚREDNIA LICZBA GODZIN<br>NA ZREALIZOWANIE<br>AKTYWNOŚCI |
|--------------------------------------------------------------------------------------------------|---------------------------------------------------------|
| <b>Godziny kontaktowe z nauczycielem akademickim, w tym:</b>                                     |                                                         |
| Godziny wynikające z planu studiów                                                               | 60                                                      |
| Konsultacje przedmiotowe                                                                         | 21                                                      |
| Egzaminy i zaliczenia w sesji                                                                    | 0                                                       |
| <b>Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:</b> |                                                         |
| Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury                               | 39                                                      |
| Opracowanie wyników                                                                              | 0                                                       |
| Przygotowanie raportu, projektu, prezentacji, dyskusji                                           | 0                                                       |
| <b>SUMARYCZNA LICZBA GODZIN DLA PRZEDMIOTU WYNIKAJĄCA Z<br/>CAŁEGO NAKŁADU PRACY STUDENTA</b>    | <b>120</b>                                              |
| SUMARYCZNA LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU                                                    | 4.00                                                    |

## 9 SPOSOBY OCENY

### OCENA FORMUJĄCA

F1 Kolokwia

### OCENA PODSUMOWUJĄCA

P1 Zaliczenie pisemne

P4 Średnia ważona ocen formujących

### WARUNKI ZALICZENIA PRZEDMIOTU

W3 Ocena końcowa jest średnią ocen P1, P2, P3 i P4

### OCENA AKTYWNOŚCI BEZ UDZIAŁU NAUCZYCIELA

B1 Test

### KRYTERIA OCENY

| EFEKT KSZTAŁCENIA 1 |                                                                                          |
|---------------------|------------------------------------------------------------------------------------------|
| NA OCENĘ 2.0        | Student nie zna podstawowych pojęć algebry abstrakcyjnej (teorii grup) oraz teorii liczb |

|                     |                                                                                                                                                                                                                                                                                                                                                                |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NA OCENĘ 3.0        | Student zna podstawowe pojęcia algebry abstrakcyjnej (teorii grup)                                                                                                                                                                                                                                                                                             |
| NA OCENĘ 3.5        | Student potrafi nie tylko prawidłowo sformułować podstawowe pojęcia algebry abstrakcyjnej (teorii grup) oraz teorii liczb, lecz również zilustrować ich pewnymi przykładami                                                                                                                                                                                    |
| NA OCENĘ 4.0        | Student objaśnia podstawowe pojęcia algebry abstrakcyjnej (teorii grup) oraz teorii liczb, formułuje i udowadnia podstawowe twierdzenia oraz rozwiązuje standardowe zadania                                                                                                                                                                                    |
| NA OCENĘ 4.5        | Student potrafi nie tylko wyjaśnić podstawowe pojęcia algebry abstrakcyjnej (teorii grup) oraz teorii liczb, sformułować i udowodnić podstawowe twierdzenia, lecz stosować ich do rozwiązywania zadań teoretycznego i praktycznego charakteru                                                                                                                  |
| NA OCENĘ 5.0        | Student potrafi nie tylko wyjaśnić podstawowe pojęcia algebry abstrakcyjnej (teorii grup) oraz teorii liczb, sformułować i udowodnić podstawowe twierdzenia, lecz stosować ich do rozwiązywania praktycznych i teoretycznych zadań niestandardowego charakteru                                                                                                 |
| EFEKT KSZTAŁCENIA 2 |                                                                                                                                                                                                                                                                                                                                                                |
| NA OCENĘ 2.0        | Student nie potrafi w sposób zrozumiały, w mowie i pisemnie, przedstawić poprawne rozumowania z algebry abstrakcyjnej (teorii grup) oraz teorii liczb, formułując definicje i twierdzenia                                                                                                                                                                      |
| NA OCENĘ 3.0        | Student zna podstawowe pojęcia i potrafi w sposób zrozumiały, w mowie i pisemnie, przedstawić poprawne rozumowania z algebry abstrakcyjnej (teorii grup) oraz teorii liczb, formułując definicje i twierdzenia                                                                                                                                                 |
| NA OCENĘ 3.5        | Student potrafi nie tylko podstawowe pojęcia i potrafi w sposób zrozumiały, w mowie i pisemnie, przedstawić poprawne rozumowania z algebry abstrakcyjnej (teorii grup) oraz teorii liczb, formułując definicje i twierdzenia, lecz również prowadzi łatwe i średnio trudne dowody z algebry abstrakcyjnej oraz teorii liczb, ilustruje ich pewnymi przykładami |
| NA OCENĘ 4.0        | Student objaśnia podstawowe pojęcia algebry abstrakcyjnej (teorii grup) oraz teorii liczb i potrafi ich zastosować, formułuje i udowadnia podstawowe twierdzenia oraz rozwiązuje standardowe ćwiczenia                                                                                                                                                         |
| NA OCENĘ 4.5        | Student potrafi nie tylko wyjaśnić podstawowe pojęcia abstrakcyjnej (teorii grup) oraz teorii liczb, sformułować i udowodnić podstawowe twierdzenia, lecz stosować ich do rozwiązywania ćwiczeń                                                                                                                                                                |
| NA OCENĘ 5.0        | Student potrafi nie tylko wyjaśnić podstawowe pojęcia abstrakcyjnej (teorii grup) oraz teorii liczb, sformułować i udowodnić podstawowe twierdzenia, lecz stosować ich do rozwiązywania praktycznych                                                                                                                                                           |
| EFEKT KSZTAŁCENIA 3 |                                                                                                                                                                                                                                                                                                                                                                |
| NA OCENĘ 2.0        | Student nie zna podstawowych pojęć algebry abstrakcyjnej (teorii pierścieni, teorii podzielności w dziedzinach całkowitości, teorii ciał) oraz teorii liczb                                                                                                                                                                                                    |
| NA OCENĘ 3.0        | Student zna podstawowe pojęcia algebry abstrakcyjnej (teorii pierścieni, teorii podzielności w dziedzinach całkowitości, teorii ciał) oraz teorii liczb                                                                                                                                                                                                        |

|                     |                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NA OCENĘ 3.5        | Student potrafi nie tylko prawidłowo sformułować podstawowe pojęcia algebry abstrakcyjnej (teorii pierścieni, teorii podzielności w dziedzinach całkowitości, teorii ciał) oraz teorii liczb, lecz również zilustrować ich pewnymi przykładami                                                                                                                           |
| NA OCENĘ 4.0        | Student objaśnia podstawowe pojęcia algebry abstrakcyjnej (teorii pierścieni, teorii podzielności w dziedzinach całkowitości, teorii ciał) oraz teorii liczb, formułuje i udowadnia podstawowe twierdzenia oraz rozwiązuje standardowe zadania teoretycznego i praktycznego charakteru                                                                                   |
| NA OCENĘ 4.5        | Student potrafi nie tylko wyjaśnić podstawowe pojęcia algebry abstrakcyjnej (teorii pierścieni, teorii podzielności w dziedzinach całkowitości, teorii ciał) oraz teorii liczb, sformułować i udowodnić podstawowe twierdzenia, lecz stosować ich do rozwiązywania różnych zadań                                                                                         |
| NA OCENĘ 5.0        | Student potrafi nie tylko wyjaśnić podstawowe pojęcia algebry abstrakcyjnej (teorii pierścieni, teorii podzielności w dziedzinach całkowitości, teorii ciał) oraz teorii liczb, sformułować i udowodnić podstawowe twierdzenia, lecz stosować ich do rozwiązywania praktycznych i teoretycznych zadań standardowego i niestandardowego charakteru                        |
| EFEKT KSZTAŁCENIA 4 |                                                                                                                                                                                                                                                                                                                                                                          |
| NA OCENĘ 2.0        | Student nie zna podstawowych pojęć algebry abstrakcyjnej oraz teorii liczb, nie potrafi ich zastosować, nie potrafi samodzielnie wyszukać informacji w literaturze, w językach obcych i nie potrafi formułować opinii na temat podstawowych zagadnień algebry abstrakcyjnej                                                                                              |
| NA OCENĘ 3.0        | Student zna podstawowe pojęcia algebry abstrakcyjnej oraz teorii liczb, potrafi ich zastosować, potrafi samodzielnie wyszukać informacje w literaturze, w językach obcych i potrafi formułować opinie na temat podstawowych zagadnień algebry abstrakcyjnej                                                                                                              |
| NA OCENĘ 3.5        | Student potrafi nie tylko prawidłowo sformułować podstawowe pojęcia algebry abstrakcyjnej oraz teorii liczb, lecz również zilustrować ich pewnymi przykładami, potrafi samodzielnie wyszukać informacje w literaturze, w językach obcych i potrafi formułować opinie na temat podstawowych zagadnień algebry abstrakcyjnej                                               |
| NA OCENĘ 4.0        | Student objaśnia podstawowe pojęcia algebry abstrakcyjnej oraz teorii liczb, potrafi ich zastosować, formułuje i udowadnia podstawowe twierdzenia oraz rozwiązuje standardowe ćwiczenia, potrafi samodzielnie wyszukać informacje w literaturze, w językach obcych i potrafi formułować opinie na temat podstawowych zagadnień algebry abstrakcyjnej                     |
| NA OCENĘ 4.5        | Student potrafi nie tylko wyjaśnić podstawowe pojęcia algebry abstrakcyjnej oraz teorii liczb, sformułować i udowodnić podstawowe twierdzenia, lecz stosować ich do rozwiązywania ćwiczeń, potrafi samodzielnie wyszukać informacje w literaturze, w językach obcych i potrafi formułować opinie na temat podstawowych zagadnień algebry abstrakcyjnej oraz teorii liczb |

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NA OCENĘ 5.0 | Student potrafi nie tylko objaśnić podstawowe pojęcia algebry abstrakcyjnej oraz teorii liczb, sformułować i udowodnić podstawowe twierdzenia, lecz stosować ich do rozwiązywania praktycznych, potrafi samodzielnie wyszukiwać informacje w literaturze, w językach obcych i nie potrafi formułować opinii na temat podstawowych zagadnień algebry abstrakcyjnej oraz teorii liczb, potrafi samodzielnie wyszukiwać informacje w literaturze, w językach obcych i potrafi formułować opinie na temat podstawowych zagadnień algebry abstrakcyjnej oraz teorii liczb |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## 10 MACIERZ REALIZACJI PRZEDMIOTU

| EFEKT KSZTAŁCENIA | ODNIESIENIE DANEGO EFEKTU DO SZCZEGÓŁOWYCH EFEKTÓW ZDEFINIOWANYCH DLA PROGRAMU | CELE PRZEDMIOTU | TREŚCI PROGRAMOWE | NARZĘDZIA DYDAKTYCZNE | SPOSOBY OCENY |
|-------------------|--------------------------------------------------------------------------------|-----------------|-------------------|-----------------------|---------------|
| EK1               | I2_W01<br>I2_W05                                                               | Cel 1           | W1 W2 C1 C2       | N1 N2 N3 N4           | F1 P1 P4      |
| EK2               | I2_U01b<br>I2_U04b                                                             | Cel 1           | W3 C3             | N1 N2 N3 N4           | F1 P1 P4      |
| EK3               | I2_W01<br>I2_W05                                                               | Cel 1           | W4 C4             | N1 N2 N3 N4           | F1 P1 P4      |
| EK4               | I2_K01 I2_K02                                                                  | Cel 1           | W5 C5             | N1 N2 N3 N4           | F1 P1 P4      |

## 11 WYKAZ LITERATURY

### LITERATURA PODSTAWOWA

- [1] | A.I. Kostrikin — *Algebra (cz 1, 3)*, Warszawa, 2005, PWN
- [2] | O. Artemowicz, A. Piękosz — *Algebra*, Kraków, 2010, PK
- [3] | J. Rutkowski — *Algebra abstrakcyjna w zadaniach*, Warszawa, 2001, PWN
- [4] | W. Więśław — *Grupy, pierścienie, ciała*, Wrocław, 1979, UW
- [5] | M. Bryński, J. Jurkiewicz — *Zbiór zadań z algebry*, Warszawa, 1975, PWN

### LITERATURA UZUPEŁNIAJĄCA

- [1] | A. Białynicki-Birula — *Algebra*, Warszawa, 1971, PWN
- [2] | Cz. Bagiński — *Wstęp do teorii grup*, Warszawa, 2001, Skrypt

[3] | J. Gancarzewicz — *Arytmetyka*, Kraków, 2002, UJ

[4] | J. Browkin — *Teoria ciał*, Warszawa, 1978, PWN

[5] | W.J. Gilbert, W.K. Nicolson — *Algebra współczesna z zastosowaniami*, Warszawa, 2008, PWN

## 12 INFORMACJE O NAUCZYCIELACH AKADEMICKICH

### OSOBA ODPOWIEDZIALNA ZA KARTĘ

prof. dr hab. Orest Artemowych (kontakt: [artemo@pk.edu.pl](mailto:artemo@pk.edu.pl))

### OSOBY PROWADZĄCE PRZEDMIOT

1 Prof. dr hab. Orest Artemowych (kontakt: [artemo@usk.pk.edu.pl](mailto:artemo@usk.pk.edu.pl))

2 Dr Maciej Zakarczemny (kontakt: [mzakarczemny@pk.edu.pl](mailto:mzakarczemny@pk.edu.pl))

## 13 ZATWIERDZENIE KARTY PRZEDMIOTU DO REALIZACJI

---

(miejscowość, data)

(odpowiedzialny za przedmiot)

(dziekan)

PRZYJMUJĘ DO REALIZACJI (data i podpisy osób prowadzących przedmiot)

.....

.....