

ÁLGEBRA APLICADA (6 ECTS)

Mostrar algumas das aplicações da álgebra abstracta, nomeadamente da teoria de grupos, anéis e corpos, assim como de outras áreas mais recentes da álgebra.

Exemplos de tópicos que poderão ser abordados:

- Códigos correctores de erros: códigos lineares e majorantes básicos; códigos cíclicos, códigos BCH e códigos de Reed-Solomon.
- O uso de álgebra em criptografia, nomeadamente do corpo com 256 elementos no Advanced Encryption Standard (AES).
- Reticulados e circuitos.
- Autómatos, linguagens formais e semigrupos.

ANÁLISE E PROCESSAMENTO DIGITAL DE SINAL - ANÁLISE E PROCESSAMENTO DIGITAL DE SINAL (6 ECTS)

I. INTRODUÇÃO

- Introdução e Motivação para a disciplina.

II. SINAIS, SISTEMAS, TRANSFORMADAS E APLICAÇÕES

- Sinais e Sistemas: conceitos fundamentais numa perspectiva determinista.
- Série de Fourier. Transformada de Fourier, sinais periódicos / não periódicos, funções generalizadas
- Análise de sinais e sistemas nos domínios tempo e frequência.
- Amostragem de sinais em tempo contínuo
- Aplicações a dados de simulação e experimentais

III. PROCESSAMENTO DE SINAL EM TEMPO DISCRETO

- Transformada Z: propriedades e utilização na análise de sistemas.
- Filtragem FIR e IIR – implementação e análise.
- Introdução à análise espectral.

ANÁLISE LINEAR - ANÁLISE LINEAR (6 ECTS)

Espaços normados, espaços euclidianos. Completados. Séries de Fourier. Teorema da Representação de Riesz-Fisher. Transformadas de Fourier e de Laplace. Aplicações lineares contínuas. Espaço dual. Operadores adjuntos. Espectro de uma aplicação linear limitada. Aplicações compactas. Aplicações integrais. Teoria de Fredholm. Aplicações lineares em espaços de Hilbert. Aplicações elípticas. Equações diferenciais lineares ordinárias. Problemas de contorno.

GEOMETRIAS NÃO EUCLIDIANAS - COMPLEMENTOS DE GEOMETRIA (6 ECTS)

1) Geometria afim: coordenadas afins, transformações afins, estrutura abstracta de espaço afim, referenciais afins, razão de três pontos colineares, uso de métodos afins para obtenção de resultados geométricos elementares.

2) Circunferências no plano euclidiano (abordadas através das equações cartesianas): potência de um ponto relativamente a uma circunferência, circunferências ortogonais, feixes de circunferências, inversão.

3) Rectas projectivas reais e homografias: transformações de Möbius; razão dupla de quatro números reais; razão dupla de quatro pontos colineares e de quatro rectas concorrentes no plano; divisão harmónica de quatro pontos; homografia entre duas rectas; homografia de uma recta em si mesma. Coordenadas homogéneas e homografias no plano projectivo real. As homografias do plano projectivo que deixam invariante a recta de infinito são precisamente as transformações afins de \mathbb{R}^2 .

4) Estudo elementar das cónicas no plano euclidiano: definição por foco e recta directriz; equação cartesiana; definição bifocal (cónicas com centro); secções planas de um cone de revolução (teorema de Dandelin); intersecção de uma cónica com uma recta; tangentes a uma cónica; propriedades particulares (em especial propriedades ópticas) das parábolas, elipses e hipérbolas.

5) Cónicas no plano projectivo complexo: curvas algébricas de segundo grau; intersecção de uma cónica regular com uma recta; uma cónica não é regular (i.e., a matriz de uma sua equação tem determinante igual a zero) se e só se ela se decompuser em duas rectas (que podem ser coincidentes); pontos conjugados relativamente a uma cónica; recta polar de um ponto e pólo de uma recta; construção só com régua das tangentes a uma cónica (em particular, a uma circunferência) por um ponto dado. Cónica definida por cinco pontos. Teoremas de Pascal e Brianchon (sobre hexágonos inscritos ou circunscritos em cónicas).

SISTEMAS E CONTROLO LINEAR - CONTROLO AUTOMÁTICO (6 ECTS)

Modelos Matemáticos de sistemas: discreto, contínuo. Modelos não lineares; Descrição matemática de sistemas: Descrição matemática de sistemas por equações de estado. Linearização. Solução das equações de estado. Transformada de Laplace no estudo de sistemas lineares, matriz de transição, resposta impulsional e função de transferência, isomorfismos de espaço de estados;

Controlabilidade e observabilidade: definições, teste PHP; Forma canónica controlável e forma canónica observável. Realização de funções de transferência, realizações controláveis e observáveis.

Estabilidade: estabilidade interna, definições, critérios; estabilidade externa: BIBO estabilidade, critérios.

Compensadores e Observadores de estado: realimentação de estado e estabilidade interna; Observadores assintóticos; Estabilização, síntese do compensador, princípio da separação. Descrição e análise de sistemas no domínio da frequência.

EQUAÇÕES ÀS DERIVADAS PARCIAIS E ANÁLISE DE FOURIER (6 ECTS)

Séries de Fourier e a sua convergência. Equação do Calor. Equação de onda. Transformada

de Fourier e aplicações. Equação de Laplace.

GEOMETRIA DIFERENCIAL - GEOMETRIA DIFERENCIAL (6 ECTS)

- 1) Curvas no espaço (revisões) e curvas no plano (curvatura com sinal).
- 2) Superfícies regulares em \mathbb{R}^3 : parametrizações; funções diferenciáveis em superfícies; espaço tangente; orientabilidade; a primeira forma fundamental (medição de áreas, comprimentos e ângulos em superfícies).
- 3) A geometria da aplicação de Gauss: a segunda forma fundamental; curvatura de uma superfície.
- 4) Geometria intrínseca das superfícies: aplicações conformes e isometrias; teorema egregio de Gauss; derivada covariante e transporte paralelo; curvatura geodésica; teorema de Gauss-Bonnet; geodésicas.
- 5) Distância intrínseca em superfícies conexas. Superfícies completas. Teorema de Hopf-Rinow.

INTRODUÇÃO À TOPOLOGIA - INTRODUÇÃO À TOPOLOGIA (6 ECTS)

Espaços métricos. Continuidade e convergência. Homeomorfismos. Conceitos métricos e topológicos: abertos, fechados; vizinhanças; aderência e interior; fronteira.

Topologias. Produto de espaços topológicos.

Espaços métricos conexos: Componentes conexas; produto de espaços conexos; conectividade e invariantes topológicos; conexos por caminhos; funções contínua em conexos e generalizações do teorema do valor intermédio de Bolzano.

Limites de sucessões: Convergência e topologia. Sucessões de funções. Limites de funções.

Espaços Métricos Completos: Sucessões de Cauchy. Completude. Teorema de Baire.

Espaços métricos compactos: definição e consequências.

LÓGICA E FUNDAMENTOS - LÓGICA E FUNDAMENTOS (6 ECTS)

1. CÁLCULO PROPOSICIONAL: semântica, sintaxe, completude e compacidade
2. LINGUAGENS DE PRIMEIRA ORDEM: símbolos funcionais e relacionais, constantes, linguagens com igualdade, termos e fórmulas
3. SEMÂNTICA: estruturas, interpretação das variáveis, consequência semântica, fórmulas válidas
4. SINTAXE: axiomas e inferência, consequência sintática, consistência, forma normal prenex

5. COMPLETUDE: teoremas da completude e da compacidade para a lógica de primeira ordem
6. LÓGICA DE SEGUNDA ORDEM: lógica de segunda ordem e lógica de segunda ordem monádica, teorema de Rabin
7. OS TEOREMAS DE INCOMPLETUDE DE GÖDEL: significado dos teoremas de incompletude, demonstração de uma versão simplificada do primeiro teorema
8. CONSTRUÇÃO DOS NÚMEROS NATURAIS: a axiomática de Peano, construção dos números inteiros, construção dos números racionais
9. CONSTRUÇÃO DOS NÚMEROS REAIS: cortes de Dedekind, referência à construção à base de sucessões de Cauchy
10. TEORIA AXIOMÁTICA DE CONJUNTOS: paradoxos resultantes da definição intuitiva de conjunto, axiomática de Zermelo-Fraenkel, construção dos números naturais nesta axiomática
11. ORDINAIS: conjuntos bem ordenados, indução transfinita, ordinais e suas propriedades
12. O AXIOMA DA ESCOLHA: axioma da escolha, diversas formulações equivalentes, um axioma não consensual
13. CARDINAIS: equipotência, conjuntos finitos e numeráveis, hipótese do contínuo, Teorema de Cantor-Schröder-Bernstein, Teorema de Cantor, cardinal de um conjunto

ÁLGEBRA COMPUTACIONAL - MATEMÁTICA COMPUTACIONAL (6 ECTS)

Métodos computacionais em pelo menos duas áreas distintas da matemática. Esta disciplina poderá ser dada em módulos, sugerindo-se os seguintes tópicos: Álgebra Computacional, Álgebra Linear Numérica, Teoria da Aproximação, Geometria Computacional, Métodos Numéricos Iterativos, Teoria dos Números Computacional.

MATEMÁTICA DISCRETA (6 ECTS)

MÉTODOS MATEMÁTICOS DA MECÂNICA ou MÉTODOS MATEMÁTICOS EM BIOLOGIA E MEDICINA - MODELOS MATEMÁTICOS NAS CIÊNCIAS (6 ECTS)

Desenvolvimento de métodos matemáticos para aplicação à modelação de fenómenos e resolução de problemas em, pelo menos, duas áreas científicas distintas. Esta UC poderá ser dada em módulos, sugerindo-se que sejam tratados modelos de duas das disciplinas Biologia, Economia e Física. Exemplificam-se possíveis temas a abordar:

- Desenvolvimento de métodos de sistemas dinâmicos, equações diferenciais, modelos com simetria e sistemas de células acopladas, para aplicação ao estudo de modelos em ecologia de populações, propagação de doenças infecciosas, propagação de impulsos nervosos ou formação de padrões e morfogênese.

- Desenvolvimento de princípios e métodos da Mecânica Newtoniana e Lagrangiana para aplicação ao estudo do movimento de sistemas de partículas sob ação de forças

conservativas.

- Desenvolvimento de tópicos de Probabilidades, Movimento Browniano e Processos Estocásticos para introduzir os conceitos básicos de Matemática Financeira e abordar o estudo de modelos de mercado.

OTIMIZAÇÃO E APLICAÇÕES (6 ECTS)

Modelos de Optimização (lineares e não lineares). Exemplos. Viabilidade e optimalidade. Estrutura geral dos algoritmos de optimização. Restrições. Convexidade. Convergência. Optimização sem restrições. Métodos de busca. Métodos gradiente. Método das direções conjugadas. Métodos Quasi-Newton. Aplicações. Optimização com restrições. Método de Lagrange. Introdução aos métodos heurísticos (opcional).

PROJETO MULTIDISCIPLINAR (6 ECTS)

Desenvolvimento de projetos de carácter multidisciplinar que devem integrar e aplicar, a outras áreas do saber, competências científicas desenvolvidas ao longo da formação curricular, nomeadamente a modelação, a identificação, a simulação, a previsão, a optimização e o controlo, e a utilização de ferramentas avançadas de computação.

SIMULAÇÃO - SIMULAÇÃO E PROCESSOS ESTOCÁSTICOS (6 ECTS)

I. Simulação e Método de Monte Carlo

Aspetos estatísticos da simulação. Simulação de dados (distribuições discretas e contínuas): métodos gerais, transformações e misturas; utilização crítica de geradores disponíveis correntes. Integração de Monte Carlo e estimação de valores esperados. Técnicas de redução de variância. Método de Monte Carlo em inferência estatística. Métodos de reamostragem.

II. Introdução aos Processos Estocásticos e sua Simulação

Classes de processos estocásticos. Introdução à análise estatística de sinais e séries temporais: caracterização, estacionariedade, autocorrelação. Processos AR e MA. Estimação e simulação. Modelação/simulação: cadeias de Markov, processo de Poisson, passeio aleatório; processos de nascimento e morte, filas de espera.

TEORIA DOS NÚMEROS E CRIPTOGRAFIA - TEORIA DE NÚMEROS E APLICAÇÕES (6 ECTS)

[0.] Introdução/motivação

Uma breve introdução ao GAP.

A cifra RSA (rudimentos).

[1.] Noções básicas.

Princípio da Boa Ordenação / Indução.

Algoritmo da divisão.

Números primos e números compostos.

Teorema Fundamental da Aritmética.

[II.] Congruências.

Introdução à aritmética modular; aplicações.

Teoremas de Fermat e de Euler.

Números de Fermat e números de Mersenne.

Exponenciação Modular.

Teorema Chinês dos Restos.

[III.] Rudimentos sobre testes de primalidade e algoritmos de factorização.

Considerações sobre a distribuição dos números primos.

Pseudo-primos de Fermat.

Números de Carmichael.

Pseudo-primos fortes e testemunhas.

Método de factorização de Fermat.

[IV.] Algoritmo de Euclides e aplicações.

Algoritmo de Euclides.

Algoritmo estendido de Euclides / Identidade de Bézout.

Inversos modulares.

[V.] Raízes primitivas.

Raízes primitivas módulo um inteiro.

Aplicação: Protocolo de troca de chaves de Diffie-Hellman.

[VI.] Resíduos quadráticos.

Símbolo de Legendre.

O carácter quadrático de 2.

Lei da reciprocidade quadrática.

Aplicações.

[VIII.] Criptografia.

Mais considerações sobre testes de primalidade e algoritmos de factorização.

O sistema criptográfico RSA.

Considerações sobre outros sistemas criptográficos.