

Ficha de Unidade Curricular – (Versão A3ES 2018-2023)

1. Caracterização da Unidade Curricular.

- 1.1. **Designação da unidade curricular** (1.000 carateres).
Álgebra e Aplicações / Algebra and Applications
- 1.2. **Sigla da área científica em que se insere** (100 carateres).
MAT
- 1.3. **Duração**¹ (100 carateres).
Semestral
- 1.4. **Horas de trabalho**² (100 carateres).
162
- 1.5. **Horas de contacto**³ (100 carateres).
67.5TP; 5OT
- 1.6. **ECTS** (100 carateres).
6
- 1.7. **Observações**⁴ (1.000 carateres).
Optativa
- 1.7. **Remarks** (1.000 carateres).
Optional

2. Docente responsável e respetiva carga letiva na Unidade Curricular (preencher o nome completo) (1.000 carateres). Filipa Soares de Almeida (67.5h)

3. Outros docentes e respetivas cargas letivas na unidade curricular (1.000 carateres).

4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (1.000 carateres).

Dar aos alunos os conhecimentos necessários para compreender e trabalhar com as principais ferramentas algébricas a que recorrem as mais importantes aplicações da Álgebra em Análise de Dados/Aprendizagem Automática, Criptografia e Equações Diferenciais. Nomeadamente, pretende-se dar aos alunos conhecimentos sobre:

- fatorizações de matrizes e forma normal de Jordan, e sua aplicação à resolução de sistemas de equações lineares e de sistemas de equações diferenciais, ao método dos mínimos quadrados e à análise de componentes principais (PCA);

- teoria básica de grupos, e sua aplicação à criptografia.

Dominando tanto a fundamentação teórica como a aplicação prática dos tópicos abordados, o estudante deverá ser capaz de resolver problemas nestes domínios, não só por aplicação direta dos algoritmos e métodos estudados como por adaptação dos mesmos a novas situações.

Proporcionar um conhecimento mais sólido da Álgebra, para assim tirar melhor partido do poder desta disciplina na resolução de problemas.

4. Intended learning outcomes (knowledge, skills and competences to be developed by the students). (1.000 characters).

To give students the necessary knowledge to understand and work with the main algebraic tools used in some of the most important applications of Algebra to Cryptography, Data Science/Machine Learning, and Differential

Equations, namely:

- matrix factorizations and Jordan normal form, and its application to the solution of systems of linear equations and of systems of differential equations, the least squares method, and principal components analysis (PCA);
- basic group theory, and its applications to cryptography.

Mastering both the theoretical grounding and the practical applications of the topics studied, the student should be able to solve problems in these areas, not only by direct application of the algorithms and methods studied but also by their adaption to new scenarios.

To provide students a more thorough knowledge of Algebra, in order to enable them to effectively use the power of this discipline in problem solving.

5. Conteúdos programáticos (1.000 carateres).

1. Conceitos básicos sobre grupos: grupo, subgrupo, subgrupo invariante e homomorfismo.
2. Grupos finitos. Teorema de Lagrange. Permutações e grupo simétrico. Teorema de Cayley.
3. Grupos cíclicos. O problema do logaritmo discreto. Aplicações em criptografia.
4. Conceitos de anel e corpo. Anéis de matrizes. Fatorização LU. Aplicação: resolução de sistemas de equações lineares.
5. Polinómio característico e polinómio mínimo de uma matriz. Teorema de Cayley-Hamilton. Diagonalização e forma normal de Jordan. Aplicação: cálculo de potências de matrizes.
6. Exponencial de uma matriz. Aplicação: resolução de sistemas de equações diferenciais.
7. Matrizes ortogonais. Valores singulares e decomposição SVD. Aplicações: pseudo inverso de uma matriz; resolução de sistemas de equações lineares homogéneos e indeterminados; método dos mínimos quadrados e PCA.

5. Syllabus (1.000 characters).

1. Basic group theory: the notions of group, subgroup, invariant subgroup, and homomorphism.
2. Finite groups. Lagrange's Theorem. Permutations and the symmetric group. Cayley's Theorem.
3. Cyclic groups. The problem of the discrete logarithm. Applications in cryptography.
4. The notions of rings and fields. Matrix rings. LU decomposition. Application: systems of linear equations.
5. The characteristic polynomial and the minimal polynomial of a matrix. Cayley-Hamilton's Theorem. Eigendecomposition and Jordan normal form. Application: powers of a matrix.
6. Matrix exponential. Application: systems of differential equations.
7. Orthogonal matrices. Singular values and SVD decomposition. Applications: pseudoinverse of a matrix; homogeneous systems of linear equations and systems of linear equations with infinite solutions; least squares method and PCA.

6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular (1.000 carateres).

Os itens 1 a 3 desenvolvem a teoria básica de grupos, permitindo concretizar desde logo as aplicações destes à criptografia. As fatorizações LU (item 4) e SVD (item 7), pela importância que têm na resolução de sistemas de equações lineares, são primordiais em inúmeras aplicações provenientes de várias áreas. A diagonalização e a forma normal de Jordan são desenvolvidas e aplicadas às Equações Diferenciais, na resolução de sistemas de equações diferenciais, nos itens 5 e 6. A fatorização SVD é ainda aplicada à Análise de Dados/Aprendizagem Automática (método dos mínimos quadrados e PCA).

Ao estender os conceitos e ferramentas básicos adquiridos em Álgebra Linear (itens 4, 5, 6 e 7), introduzir os rudimentos da Álgebra Abstrata (itens 1, 2, 3 e 4) e exemplificar como uma e outra se unificam (itens 4 e 7), o estudante fica detentor de um conhecimento mais abrangente, fiel e sólido da Álgebra e do seu contributo nas aplicações da Matemática.

6. Evidence of the syllabus coherence with the curricular unit's intended learning outcomes (1.000 characters).

Items 1 to 3 develop the basic group theory that will, in particular, allow for the applications in cryptography. The LU decomposition (item 4) and SVD decomposition (item 7), in view of their importance in the solution of systems of linear equations, are unavoidable in a wide range of applications from various fields. Eigen decomposition and Jordan normal form are developed and applied to Differential Equations, namely in the solution of systems of differential equations, in items 5 and 6. Applications to Data Science/Machine Learning are illustrated in item 7 (least squares method and PCA)-

By extending the basic notions and tools acquired in the introductory Linear Algebra course (items 4, 5, 6 e 7), introducing the basics of Abstract Algebra (items 1, 2, 3 e 4), and illustrating how one and the other come together in a unified manner (items 4 and 7), the student deepens and widens her/his view of Algebra and of its contributions to the applications of Mathematics.

7. Metodologias de ensino (avaliação incluída) (1.000 carateres).

Com recurso ao método teórico-prático, as ferramentas teóricas, devidamente fundamentadas, são motivadas e concretizadas nas aplicações descritas para cada tópico. Listas de exercícios selecionados para as aulas e para trabalho autónomo proporcionam o necessário consolidar dos conhecimentos.

Os objetivos de aprendizagem são avaliados individualmente através de exame (NE), de trabalhos realizados ao longo do semestre (NT), num máximo de 7, e de um projeto (NP). Para obter aprovação é preciso ter nota mínima de 9.5 valores em NE e na nota final NF, onde $NF=0.6*NE+0.15*NT+0.25*NP$.

7. Teaching methodologies (including assessment) (1.000 characters).

Classes combine the theoretical exposition of the syllabus with the application/applications of each topic, both as a source of motivation and to lay out its use in problem solving. Sheets of selected exercises, including class and individual work, provide the required consolidation of the knowledge.

The learning outcomes are evaluated by means of a global exam (NE), practice tasks during the course of the semester (NT) in a maximum of 7, and a project (NP). The final grade (NF) is given by $NF=0.6*NE+0.15*NT+0.25*NP$. In order to pass the unit, a minimum of 9.5 is required for both NE and NF.

8. Demonstração da coerência das metodologias de ensino com os objetivos de aprendizagem da unidade curricular (3.000 carateres).

O desenvolvimento da teoria em conjunto com a sua concretização em aplicações práticas, nas aulas, e a realização dos trabalhos ao longo do semestre e do desenvolvimento projeto, por parte do aluno, asseguram que o estudante amplie os seus conhecimentos nos tópicos descritos com ênfase na resolução de problemas.

8. Evidence of the teaching methodologies coherence with the curricular unit's intended learning outcomes (3.000 characters).

The development of the theory in parallel with its application, in class, along with the solution of the practice tasks and of the development of the project, ensure that students learn the intended topics with an emphasis in problem solving.

9. Bibliografia de consulta/existência obrigatória (1.000 carateres).

1. Anton, H., Rorres, C., "Álgebra Linear com Aplicações", Bookman, 10th edition, 2012.
2. Byrne, C., "Applied and Computational Linear Algebra: A First Course", 2016. Disponível em <http://faculty.uml.edu/cbyrne/aclafctext.pdf>.
3. I. Goodfellow, Y. Bengio, A. Courville, "Deep Learning", MIT Press, 2016.

4. M. W. Hirsh, S. Smale, "Differential Equations, Dynamical Systems, and Linear Algebra", Academic Press, 1974.
5. Olver, P. J., Shakiban, C., "Applied Linear Algebra", Pearson Prentice Hall, 2006.
6. Judson, T. W., "Abstract Algebra: Theory and Applications", 2016. Disponível em <https://open.umn.edu/opentextbooks/textbooks/abstract-algebra-theory-and-applications>.
7. Strang, G., "Linear Algebra and its Applications", Brooks/Cole, 4th edition, 2005.

¹ Anual, semestral, trimestral, ...

² Número total de horas de trabalho.

³ Discriminadas por tipo de metodologia adotado (T - Ensino teórico; TP - Ensino teórico-prático; PL - Ensino prático e laboratorial; TC - Trabalho de campo; S - Seminário; E - Estágio; OT - Orientação tutorial; O - Outro).

⁴ Assinalar sempre que a unidade curricular seja optativa.