Corpos e Equações Algébricas

Relatório de **Unidade curricular**

Jorge **Picado**

Coimbra 2008

ÍNDICE

I am searching for abstract ways of expressing reality, abstract forms that will enlighten my own mistery.

ERIC CANTONA[1]

(...) *in order for algebra courses to serve the needs of all students, there should be a greater emphasis on examples that illustrate the usefulness of algebra as a language for describing mathematical objects in pure and applied situations.*

DAVID A. COX[2]

1. Introdução

Este relatório refere-se ao programa, conteúdo e métodos de ensino e avaliação da disciplina de Corpos e Equações Algébricas (2º ano, 2º semestre) da Licenciatura em Matemática do Departamento de Matemática da Universidade de Coimbra (DMUC).

A disciplina de Corpos e Equações Algébricas, que funciona pela primeira vez no presente ano lectivo (2007/08), foi criada, no contexto da adaptação dos planos de estudo do DMUC ao processo de Bolonha, em substituição da disciplina de Álgebra II (3º ano, 1º semestre) da qual fui responsável nos três anos em que funcionou (2004/05, 2005/06 e 2006/07). A minha experiência na leccionação de disciplinas da área da álgebra abstracta inclui ainda o ano lectivo de 1997/98, ano em que regi um curso anual de Álgebra (2º ano)[3], além dos anos de 1987 a 1992 em que, como Assistente, dei aulas práticas de Álgebra (2º ano, anual).

A disciplina de Álgebra II tinha sido criada no contexto da revisão dos planos de estudo de Matemática implementada em 2003, após extensa e ampla discussão, tendo em mente a sua futura adequação, com rapidez e sem sobressaltos, ao novo paradigma de Bolonha, como veio a acontecer este ano.

[1] Futebolista, citado por Colva Roney-Dougal em [*The power of groups*, Plus magazine, Millennium Mathematics Project, Universidade de Cambridge, Junho de 2006].

[2] *What is the role of Algebra in Applied Mathematics*, Notices of the American Mathematical Society 52 (2005) 1193-1198.

[3] `www.mat.uc.pt/~picado/algebra`.

Uma das principais características dos novos planos de estudo é a adopção do chamado modelo 3+2, sendo o primeiro ciclo de estudos, a *Licenciatura*,

> «*uma formação de espectro largo, (...) rica em conhecimentos interessantes, motivadores e cuidadosamente seleccionados, e dirigida à aquisição de competências transversais, de competências de matemáticas de carácter genérico, diversificadas, solidamente aprendidas.*» [16]

> «*Serve como preparação de acesso aos 2os ciclos (Mestrados) em Matemática ou em Ensino da Matemática mas contempla também uma preparação que permite a entrada directa na vida activa em ocupações de carácter generalista nas quais sejam úteis o rigor e as capacidades que caracterizam um Matemático.*» [6]

A disciplina de Corpos e Equações Algébricas deverá ser uma continuação natural da disciplina de Grupos e Simetrias (1º semestre), e constituir com esta e com a disciplina de Álgebra Comutativa (3º ano, 1º semestre) a formação base em Álgebra, suas estruturas e aplicações. De acordo com o relatório do processo de adequação da Licenciatura em Matemática do DMUC ao processo de Bolonha [6],

> «*As álgebras têm como objectivo primordial o reforço da capacidade de abstracção, que será atingido mediante a apresentação de estruturas de base axiomática convenientemente ilustradas no concreto; a sua ligação à geometria ocupará parte importante dos dois primeiros semestres.*»

O carácter formativo da disciplina é evidente. O ponto de vista que enforma esta proposta de programa é o de que o ensino no 2º ano do curso de Matemática não deve ter um pendor muito abstracto e formalista[4], devendo ter-se a preocupação, na definição do seu conteúdo, de encontrar um ponto de equilíbrio entre abstracção e aplicações, aquilo que Rui Loja Fernandes e Manuel Ricou [14] apelidam de binómio abstracto-concreto:

[4]Nas palavras de 75 matemáticos famosos, numa tomada de posição contra o excesso formalista da matemática moderna, «*premature formalization may lead to sterility*» [L. V. Ahlfors *et al.*, *On the mathematics curriculum of the high school*, American Mathematical Monthly 69 (1962) 189-193].

«Antes de mais, deve observar-se que, hoje em dia, é aceite por toda a comunidade matemática a formulação conceptual, axiomática, da Álgebra. Mais do que isso, a metodologia algébrica é uma das ferramentas essenciais da Matemática. Por outro lado, depois de na segunda metade do século XX se ter assistido a uma abstracção sem paralelo na Matemática, mais recentemente, verificou-se um retorno a uma tradição nunca perdida: os desafios criados por problemas concretos, por vezes de natureza elementar, mas cuja solução requer métodos de extrema complexidade. O ensino da Álgebra deve, quanto a nós, reflectir este binómio abstracto-concreto. Como perguntava o grande matemático contemporâneo Vladimir Arnol'd, de que serve a um estudante saber o que é um anel local e as suas propriedades, se desconhecer o exemplo do anel das séries de potências?»

The point of these observations is not the reduction of the familiar to the unfamiliar (...) but the extension of the familiar to cover many more cases.

SAUNDERS MAC LANE[5]

Once, a mathematician was giving a talk and had just stated a complex theorem bristling with abstract concepts and symbols. Before he could begin to prove it, suddenly someone in the audience blurted out: "Wait! Is that really true?" The speaker paused and drew a small equilateral triangle on the board. He labelled its vertices A, B and C, as a schoolchild might. He stared at his triangle for a while, then erased it. "Yes, it is true. Let G be a group ...", going back to his theorem. Even someone comfortable with abstraction felt the need to think about a simple example before moving to the abstract statement.

PETER PESIC ([21], p. 111)

2. Programa

Enquadramento, temas e objectivos

Os alunos do 2º ano frequentaram já, no primeiro semestre, a disciplina de Grupos e Simetrias, onde foram iniciados na teoria dos grupos, tendo estudado, entre outros assuntos:

- Grupos (definição e exemplos).
- Subgrupos, classes laterais.
- Subgrupos normais, grupos quocientes.
- Homomorfismos, isomorfismos.

[5] *Categories for the Working Mathematician*, Graduate Texts in Mathematics 5, Springer Verlag, Nova Iorque, 1971.

- Grupos cíclicos.
- Classificação dos grupos abelianos finitos.
- Acções de grupos sobre conjuntos.
- Teoremas de Sylow.

Frequentaram, além disso, uma disciplina de Teoria dos Números no 1º ano do curso, onde foram introduzidos à teoria elementar dos números, dentro de um espírito matemático rigoroso, abordando, entre outros temas, as equações diofantinas.

Como se aconselha no Relatório da Comissão de Reflexão sobre a Revisão dos Planos de Estudo de Matemática [16],

> «*Nas disciplinas de Álgebra o princípio da concretização deverá estar também presente, podendo começar-se com grupos de permutações e transformações, corpos e suas extensões, corpos finitos, polinómios numa e várias indeterminadas, polinómios simétricos, seguindo depois para as estruturas abstractas.*»

Não me restam assim muitas dúvidas quanto aos temas principais a abordar na disciplina de Corpos e Equações Algébricas:

- Anéis de polinómios (numa indeterminada).
- Anéis e corpos.
- Extensões de corpos e resolubilidade algébrica de equações.
- Corpos finitos.

O desenvolvimento do programa deverá ter em conta a seguinte observação referida em [16]:

> «*Mesmo as sínteses, que são operações internas da própria Matemática e que criaram as grandes estruturas que a dominam, têm como valor prático permitir expor quantidades cada vez maiores de conhecimentos num mesmo período de tempo. Este é um ponto que chama algo com interesse. As sínteses vão sempre no caminho da abstracção, sempre na ideia de que qualquer coisa é um caso particular de alguma coisa e que basta conhecer*

esta "alguma coisa" para se conhecerem todas as coisas a jusante. Porém, é preciso ter o cuidado de saber se os limites da capacidade de abstracção dos jovens estudiosos não foram já ultrapassados há muito. Se for o caso, os conhecimentos transmitidos não têm qualquer significado concreto parecendo como meros enunciados a que o estudante adere porque tem que passar no exame mas nos quais realmente não acredita.»

Seguiremos também o conselho de Emmy Noether[6]:

«In mathematics, as in knowledge of the world, both aspects are equally valuable: the accumulation of facts and concrete constructions and the establishment of general principles which overcome the isolation of each fact and bring the factual knowledge to a new stage of axiomatic understanding.»

Elejo como objectivos centrais do curso:

- Mostrar como as propriedades algébricas dos inteiros estudadas em Teoria dos Números e em Grupos e Simetrias se reproduzem, em perfeita analogia, nos anéis de polinómios sobre um corpo.
- Explicar como a teoria de Galois nasceu das tentativas de determinação de uma fórmula geral para o cálculo das raízes de uma equação polinomial em termos dos seus coeficientes, mostrando como este problema se traduz num problema sobre grupos, que pode então ser resolvido.
- Exposição dos aspectos teóricos e práticos fundamentais da teoria de Galois, bem como da teoria dos corpos finitos, incluindo demonstração de teoremas, resolução de problemas e ilustração da teoria através de exemplos concretos e de aplicações relevantes como:
    - a solução dos problemas geométricos clássicos relativos a construções com régua e compasso,
    - resolubilidade algébrica de equações através de radicais,

[6]Citada por Alexandrov em [*In memory of Emmy Noether*, 1935 (Trad. para inglês por N. & A. Koblitz, em *Emmy Noether: Gesammelte Abhandlungen*, Springer, 1983)].

- diversas aplicações modernas da teoria dos corpos finitos à teoria algébrica dos códigos.

Quanto às competências específicas que espero que os alunos atinjam no final do curso, realço:

- Dominar as propriedades fundamentais dos polinómios com coeficientes num corpo (e, mais geralmente, num anel).
- Saber traduzir em linguagem algébrica moderna problemas geométricos de construções com régua e compasso.
- Saber resolver equações de graus 3 e 4.
- Compreender as ideias básicas da teoria de Galois.
- Saber calcular grupos de Galois para extensões de corpos e polinómios muito simples.
- Perceber o conceito da solubilidade por radicais e porque falha para polinómios de grau superior a 4.
- Conhecer a classificação dos corpos finitos e saber construir corpos com um número finito de elementos (p^n elementos, p primo).
- Saber desenhar códigos correctores de erros duplos e triplos.

Há certamente muitos assuntos interessantes de anéis e corpos que não são contemplados neste programa por manifesta falta de tempo (exemplos mais relevantes: factorização em domínios gerais, elementos primos e irredutíveis em domínios gerais, domínios de factorização única, demonstração do Teorema Fundamental da Álgebra). Pensando nos estudantes mais interessados e motivados, propomos-lhes leituras avançadas opcionais sobre alguns desses temas (ao longo dos apontamentos [22], em observações breves ou, com mais pormenor, em apêndice).

Parece-nos, contudo, que a nossa opção programática cumpre o objectivo de fornecer ao estudante uma boa base de conhecimentos, permitindo o seu posterior desenvolvimento na disciplina de Álgebra Comutativa.

Já algumas dúvidas tenho se será esta a melhor maneira de organizar os dois primeiros semestres lectivos de disciplinas da área da álgebra abstracta.

Inclino-me mais para um esquema em que a disciplina do primeiro semestre seja uma continuação da Teoria dos Números, começando pelo estudo dos anéis de polinómios sobre um corpo, realçando a analogia com $\mathbb{Z}$ e como tudo se obtém como mera clonagem do encontrado em $\mathbb{Z}$, prosseguindo daí para um estudo mais geral dos domínios euclidianos (como extensão e formalização geral da divisibilidade em $\mathbb{Z}$ e nos polinómios sobre um corpo), domínios de ideias principais e domínios de factorização única (como extensão da teoria da factorização dos números inteiros e dos polinómios sobre um corpo[7]), chegando por fim à axiomática dos anéis, domínios e corpos (e, em particular, dos grupos); aqui cada noção (categorial) pode ser apresentada em simultâneo, de modo muito económico, nas diferentes categorias de álgebras (subgrupo, subanel; subgrupo normal, ideal; grupo quociente, anel quociente; homomorfismo de grupo, homomorfismo de anel; isomorfismo de grupo, isomorfismo de anel; etc.)[8]

A disciplina do segundo semestre contemplaria depois o estudo dos grupos e corpos finitos, a sua estrutura, as teorias das extensões de corpos e de Galois, e uma selecção das respectivas aplicações.

[7]Aqui, a descrição do caminho que a álgebra percorreu até à formalização do contexto "correcto" para o estudo da factorização providencia aos alunos um exemplo muito ilustrativo de como a matemática se desenvolveu ao longo dos últimos dois séculos [4].

[8]Os alunos já não teriam assim desculpa quando costumam responder "já não nos lembramos muito bem dessas definições em grupos ..." sempre que lhes são apresentadas essas noções em anéis, no segundo semestre, a partir das respectivas noções em grupos tratadas no primeiro semestre.

Pré-requisitos

Assumimos alguma familiaridade do aluno com:

- Conjuntos, funções e relações.
- Conhecimentos básicos de Teoria dos Números: números inteiros, divisibilidade, Teorema Fundamental da Aritmética.
- Números complexos, até à radiciação.
- Conhecimentos básicos de Álgebra Linear: espaços vectoriais e dimensão, sistemas de equações lineares.
- Análise de funções reais de uma variável real.
- Conceitos fundamentais de grupos estudados na disciplina de Grupos e Simetrias.

Uma das coisas que torna a álgebra difícil é o grau de abstracção e sofisticação que nela encontramos. A abstracção e o ênfase nalgum formalismo poderá chocar o aluno matematicamente imaturo. Espera-se que estes aspectos[9], incluindo os pré-requisitos mencionados, tenham sido consolidados durante o primeiro semestre e o ano anterior, nas disciplinas de Teoria dos Números, Álgebra Linear e Grupos e Simetrias.

[9] É claro que a maturidade matemática só se ganha a frequentar cursos de matemática. Deverá haver sempre algum cuidado do professor, quer na aula quer no texto do curso, em ajudar os alunos menos preparados a fazer a contextualização e a ligação com as matérias anteriores.

Resumo

I - Anéis e corpos.

1. Anéis, domínios de integridade e corpos.

2. Subanéis e ideais. Ideais principais.

3. Anel quociente. Ideais primos e ideais maximais.

4. Homomorfismos de anéis.

II - Anéis de polinómios.

1. Polinómios. Anéis de polinómios.

2. Factorização: algoritmo da divisão, polinómios irredutíveis, Teorema de Gauss da factorização única.

III - Fundamentos da Teoria de Galois.

1. Extensões de corpos.

2. Aplicação: construções com régua e compasso, construção de polígonos regulares.

3. Teoria de Galois: extensões de decomposição, homomorfismos de extensões, grupo de Galois, Teorema Fundamental.

4. Aplicação: resolubilidade algébrica de equações por radicais.

IV - Corpos finitos.

1. Propriedades fundamentais. Classificação.

2. Aplicação: teoria algébrica dos códigos.

A proof is a complete explanation. Sometimes a partial explanation suffices.

REUBEN HERSH[10]

Andamento

Este programa refere-se a uma disciplina semestral, correspondente a cerca de 15 semanas de aulas, com 5 horas de carga lectiva semanal, repartidas por 2 aulas. A parte relativa aos anéis e corpos deve desenvolver-se de modo a não comprometer o fundamental dos dois últimos capítulos, sem muita insistência em situações muito gerais (como a não comutatividade) e nas demonstrações por via axiomática. A teoria de Galois deve desenvolver-se do modo mais económico possível, com redução ao caso mais significativo (do ponto de vista histórico): corpos de característica zero.

O plano das aulas pressupõe dedicar 2,5 semanas ao Capítulo I, 3 semanas ao Capítulo II, 6 semanas ao Capítulo III e 3,5 semanas ao Capítulo IV. Informação mais pormenorizada sobre o andamento que seguimos no ano lectivo 2006/07 (mas onde o modelo ainda era o de aulas teóricas e aulas práticas separadas) encontra-se disponível nos sumários das aulas em

`www.mat.uc.pt/~picado/algebraII/SumAlg06.html`

[10] *Proving is convincing and explaining*, Educational Studies in Mathematics 24 (1993) 389-399.

I am not quite so devoted to the idea that proof is the most essential thing in mathematics. What may be more important are the relationships of the main structures, the concepts, and the development of these concepts.

Stephen Smale[11]

Se estás a ouvir falar acerca de pessoas como Newton, Leibniz, Fourier e outros, isso quer dizer que o teu professor de cálculo do primeiro ano tem uma noção histórica da sua disciplina; e a tua pergunta "Como é que eles pensaram nestas coisas?" sugere que ele está a ensinar cálculo, não como um conjunto de revelações divinas (que é a forma como é frequentemente feito), mas como problemas reais que foram resolvidos por pessoas reais.

Ian Stewart[12]

Desenvolvimento

No desenvolvimento do programa segue-se a recomendação de fundo expressa no programa mínimo [18] da disciplina de Álgebra II do plano anterior:

> «(...) *que se faça uma abordagem com um grau de abstracção algo apurado, mas sem esquecer que a álgebra pode apresentar-se com um olhar nas aplicações, que os seus temas, "clássicos", ou "modernos", foram e vão sendo originados por problemas concretos, e que alguns dos seus tópicos mais interessantes têm origem em questões complexas da geometria e da análise. Nesta perspectiva, deverá incluir-se no programa a resolução de problemas clássicos sobre as construções com régua e compasso, a resolução de equações através de radicais e diversas aplicações modernas da teoria dos corpos finitos à teoria dos códigos.*»

[11] *Interview with Stephen Smale*, Notices of the AMS 54 (2007) 995-997 (Setembro de 2007).

[12] *Cartas a uma jovem matemática*, Relógio D'Água Editores, Lisboa, 2007.

O seguinte aviso, deixado pela Comissão de Bolonha do DMUC em [17], é também tido em conta:

> «*A sequência das álgebras foi puxada para o início do curso. A posição das álgebras no elenco actual justificou-se pela vantagem de adiar um semestre a introdução das estruturas abstractas. A posição agora proposta (que foi tradição no DMUC) deve, por isso, revestir-se de cuidados especiais de carácter metodológico na sua leccionação.*»

Introdução/Motivação

Após uma breve descrição das raízes históricas da álgebra, fazemos uma abordagem sucinta aos assuntos que trataremos de modo mais formal ao longo do curso, apresentando uma visão geral do tipo de problemas com que esta área da Matemática se preocupa. Apresentamos exemplos, incluindo alguns problemas famosos e respectiva história (dentro do espírito da excelente colecção de artigos [25], com destaque particular para os artigos [4] e [11], e do livro [3]), que servirão como motivação para os tópicos a estudar. Ao longo do curso iremos resolvendo esses problemas à medida que formos obtendo as ferramentas necessárias para tal.

(Textos de base: I. Bashmakova e G. Smirnova [3], D. M. Burton e D. H. Van Osdol [4], C. H. Hadlock [7], I. Kleiner [11], P. Pesic [21].)

I - Anéis e corpos

Neste primeiro capítulo sintetizamos as características comuns de alguns sistemas numéricos e algébricos (exemplos de anéis, domínios e corpos) que os alunos encontraram em disciplinas anteriores. Os estudantes têm a oportunidade de compreender mais profundamente conceitos como zero ou identidade (elemento neutro), simétrico ou inverso (elemento inverso) e divisor de zero. O que é comum à identidade para a multiplicação de números reais, à matriz identidade e à função identidade? Qual é a ideia comum por detrás da inversa de uma função, da inversa de uma matriz, e do inverso multiplicativo de um número real?

Um relatório norte-americano recente[13] sobre a educação matemática dos futuros professores confirma que

> «*unfortunately, too many prospective high school teachers fail to understand connections between [abstract algebra and number theory] and the topics of school algebra.*» (p. 40)

Neste capítulo realça-se a ideia de que a álgebra abstracta é uma generalização da álgebra do ensino secundário, onde as variáveis deixam de ser só números e as equações deixam de ser formadas somente com as quatro operações aritméticas; agora as variáveis podem representar diversos objectos matemáticos como números, vectores, matrizes, funções, transformações geométricas, permutações, etc., e onde as expressões e equações são formadas por operações que façam sentido para esses objectos particulares: adição e multiplicação para matrizes, composição para funções, etc.

1. **Anéis, domínios de integridade e corpos.**

   Chega-se ao conceito de anel a partir da discussão da questão "Porquê $(-1)(-1) = 1$?"(como sugerido em [11]), ilustrando o facto de que, por vezes, considerações de ordem didáctica são o motor de desenvolvimento de nova matemática. Propriedades básicas dos anéis. Exemplos variados de anéis, incluindo anéis de funções. Divisores de zero. Domínios de integridade. Elementos invertíveis. Corpos. Característica de um anel.

2. **Subanéis e ideais. Ideais principais.**

   Subanéis e ideais. Construção dos ideais principais.

3. **Anel quociente. Ideais primos e ideais maximais.**

   Anel quociente: construção, exemplos. Quando é que um anel quociente é um domínio de integridade? E um corpo? Ideais primos e ideais maximais. Definição e exemplos. Determinação dos ideias primos e maximais no anel dos inteiros.

[13] Conference Board of the Mathematical Sciences, *The mathematical education of teachers*, American Mathematical Society, 2001.

4. Homomorfismos de anéis.

O papel dos morfismos não pode ser descurado no ensino das estruturas algébricas[14] (cf. Mac Lane [15]). Como C. McLarty explica em [20]:

> «*He [Mac Lane] urged his demand for morphisms because it expressed what is valuable in Mathematics far beyond solutions to equations: "Mathematics is in part a search for austere forms of beauty". His claim about structures and morphisms was a vision of vast order within and among all the branches of Mathematics, a vision of articulate global organization, of categorical Mathematics. It was a vision of Mathematical beauty.*»

Definição e exemplos. Comparação entre estruturas diferentes. Ilustração: critérios de divisibilidade (por 2, 3, 5, 6, 9, 11, etc.) nos inteiros; prova dos nove.

(Textos de base: R. Loja Fernandes e M. Ricou [14], Hungerford [9], R. Lidl e H. Niederreiter [13].)

II - Anéis de polinómios

1. Polinómios. Anéis de polinómios.

Definição algébrica de polinómio com coeficientes num anel A e relação com a definição analítica (função polinomial). A indeterminada x. Soma e produto (de convolução) de polinómios. O anel $A[x]$. O anel $A[x]$ é uma extensão de A. Grau de um polinómio. Propriedades.

[14] «*As you know, my honourable colleague Mac Lane maintains every notion of structure necessarily brings with it a notion of homomorphism, which consists of indicating, for each of the data that make up the structure, which ones behave covariantly and which contravariantly (...) what do you think we can gain from this kind of consideration ?*» (André Weil em carta a Claude Chevalley, 15 de Outubro de 1951, transcrita em [5], p. 380).

2. Factorização: algoritmo da divisão, polinómios irredutíveis, Teorema de Gauss da factorização única.

Algoritmo da divisão nos anéis de polinómios. Consequências do Algoritmo da divisão. Teorema do resto. Raízes de um polinómio. Exemplos. Conclusão de que os anéis de polinómios com coeficientes num corpo são domínios de ideais principais. Máximo divisor comum. Algoritmo de Euclides. Mínimo múltiplo comum. Polinómios irredutíveis. Exemplos. Critérios de irredutibilidade: critério da raiz, critério de Eisenstein e Lema de Gauss. Determinação dos polinómios irredutíveis sobre os complexos, os reais e os racionais. Propriedades dos polinómios irredutíveis. Factorização única nos domínios $C[x]$ (onde C é um corpo). Teorema da Factorização Única em $C[x]$.

(Textos de base: R. Loja Fernandes e M. Ricou [14], Hungerford [9], R. Lidl e H. Niederreiter [13].)

Leituras avançadas opcionais:

- Factorização única em anéis mais gerais: elementos primos e irredutíveis, domínios de factorização única [14, 22].
- Critérios de irredutibilidade [22, 23].
- Como encontrar números irracionais [23].
- Algoritmo da divisão: domínios euclidianos [14].

III - Fundamentos da teoria de Galois

Um dos problemas centrais da álgebra, que motivaram grandemente o seu desenvolvimento, foi o de procurar saber quando uma dada equação polinomial é resolúvel por radicais (isto é, quando as soluções são dadas a partir dos seus coeficientes por expressões envolvendo radicais — raízes quadradas, cúbicas e de ordem superior —, como a fórmula resolvente — quadrática — para equações do segundo grau). Galois descobriu uma teoria muito elegante que resolve completamente o problema e tem originado muitas ideias novas e fecundas em matemática:

Dada uma equação (ou um polinómio), associa-se a ela uma extensão de corpos, e a partir desta extensão, define-se um grupo (o chamado *grupo de Galois*). Este grupo, que pode ser visto como o grupo de simetrias das raízes do polinómio original, reflecte muitas das propriedades desse polinómio. Em particular, a teoria caracteriza completamente os polinómios resolúveis por radicais, e permite-nos facilmente apresentar exemplos de equações do quinto grau que não são resolúveis por radicais. Uma peculiaridade destes desenvolvimentos sobre resolução de equações é que os métodos usados para chegar à solução do problema mostraram ser muito mais interessantes para a álgebra que o próprio problema.

Este capítulo tem como objectivo explicar parcialmente os fundamentos desta teoria e convencer os alunos do acerto do uso, acima, do adjectivo "elegante". Como motivação, começa-se por descrever o problema da resolubilidade algébrica, apresentando as fórmulas resolventes para equações de grau 2, 3 e 4.

1. **Extensões de corpos.**

   Subcorpos. Subcorpos primos. Extensões de corpos. As extensões vistas como espaços vectoriais. Grau de uma extensão. Extensões finitas. Teorema da torre. Elementos algébricos e elementos transcendentes sobre um corpo. Referência aos teoremas de Lindemann (π *é transcendente sobre* $\mathbb{Q}$) e Hermite (e *é transcendente sobre* $\mathbb{Q}$). Extensões algébricas. Polinómio mínimo. Determinação do grau e de uma base de uma extensão algébrica simples. Extensões transcendentes.

2. **Aplicação: construções com régua e compasso, construção de polígonos regulares.**

   Aqui respondemos um pouco à pergunta proverbial "Para que é que isto serve?". Problemas da geometria da antiguidade. Regras para realizar tais construções. Exemplos de construções. Os quatro problemas famosos: a duplicação do cubo, a trissecção de um ângulo arbitrário, a quadratura do círculo e a inscrição de um heptágono regular numa circunferência. Tradução da questão em linguagem algébrica: pontos construtíveis. Prova de que, dado um conjunto de pontos do plano e sendo K_0 o corpo gerado pelas coordenadas desses pontos, se (x, y) é construtível a partir dos pontos dados então as dimensões $[K_0(x) : K_0]$

e $[K_0(y) : K_0]$ são potências de 2. Solução dos problemas famosos: impossibilidade da duplicação do cubo, impossibilidade da trissecção do ângulo de 60°, impossibilidade da quadratura do círculo, impossibilidade da construção de um heptágono regular. Construção de n-gonos regulares: notas históricas, análise da condição suficiente (de Gauss) e necessária (de Wantzel) de construtibilidade, números de Fermat.

3. **Teoria de Galois.**

   (Aqui restringimo-nos a corpos de característica zero.) Corpos algebricamente fechados. Caracterizações dos corpos algebricamente fechados. Extensões de decomposição: O teorema de existência e unicidade de Kronecker. Homomorfismos de extensões. Automorfismos de Galois. Grupo de Galois de uma extensão. Grupo de Galois de um polinómio. Sua representação em termos de permutações das raízes do polinómio. Extensões normais. Correspondência de Galois e Teorema Fundamental da Teoria de Galois.

4. **Aplicação: resolubilidade algébrica de equações por radicais.**

   Resolução de equações por radicais: descrição do problema. Definição exacta de resolubilidade por radicais de um polinómio sobre um corpo: extensões por radicais e polinómios resolúveis por radicais. Grupos resolúveis. Exemplos de grupos resolúveis. Critério de Galois sobre a resolubilidade de equações algébricas por radicais. Teorema de Abel-Ruffini sobre a não existência de fórmulas resolventes para a equação do quinto grau. Exemplos de polinómios do quinto grau não resolúveis por radicais. Exemplos de polinómios de grau arbitrário resolúveis por radicais.

(Textos de base: I. Stewart [24], R. Loja Fernandes e M. Ricou [14], Jones, Morris e Pearson [10].)

IV - Corpos finitos

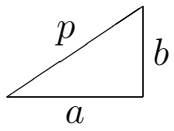
Neste capítulo final estudamos as propriedades fundamentais dos corpos finitos e descrevemos algumas das suas muitas aplicações, nomeadamente à teoria algébrica dos códigos, teoria dos números e jogos. Como motivação,

começamos por discutir um exemplo interessante de como a álgebra do corpo $\mathbb{F}_{2^2}$ permite analisar o *jogo do solitário* e tirar algumas conclusões interessantes[15].

1. **Propriedades fundamentais e classificação.**

   Possibilidades para a ordem de um corpo finito. Classificação dos corpos finitos: Teorema de Moore e Teorema de Galois. O corpo de Galois de ordem q. Classificação dos subcorpos de um corpo finito. Aplicações à Teoria dos Números; por exemplo, discussão do seguinte problema clássico:

   > *Seja $p \in \mathbb{N}$, primo. Quando é que p pode ser a hipotenusa de um triângulo rectângulo de catetos a e b inteiros?*

2. **Aplicação: teoria algébrica dos códigos.**

   Códigos sobre o corpo de Galois $\mathbb{F}_q$. Detecção e correcção de erros. Códigos t-correctores de erros. Distância de Hamming. Teorema de Hamming. Códigos lineares (n, k) sobre o corpo $\mathbb{F}_q$. Síndroma e peso de uma palavra. Classes de vectores de $\mathbb{F}_q^n$ e respectivos líderes. Algoritmo de correcção automática dos erros. Códigos polinomiais (n, k) sobre o corpo $\mathbb{F}_q$: códigos BCH. Algoritmo de correcção automática dos erros.

(Textos de base: R. Lidl e H. Niederreiter [13], A. Hefez e M. L. Villela [8], I. Stewart [24].)

Leituras avançadas opcionais:

- D. Dorninger e H. Kaiser, *Error correction and compact discs*, UMAP Journal 21 (2) (2000) 139-156.

[15] N. de Bruijn, *A solitaire game and its relation to a finite field*, J. Recreational Math. 5 (1972) 133-137.

Mathematical proof can convince, and it can explain. In mathematical research, its primary role is convincing. At the high-school or undergraduate level, its primary role is explaining.

Reuben Hersh[16]

Practice yourself, for heaven's sake, in little things; and thence proceed to greater.

Epictetus[17]

Material de apoio e bibliografia

Além do ensino directo (aulas e atendimento no gabinete) colocamos à disposição dos alunos o seguinte material pedagógico de apoio:

- manuscrito do curso [22].
- página na internet.
- bibliografia.

O manuscrito do curso é uma versão escrita da exposição dos assuntos nas aulas. Inclui, com algum pormenor, os principais conceitos e resultados apresentados nas aulas, completados aqui e acolá com exemplos, observações, aplicações e notas históricas. Contém ainda uma lista de exercícios, alguns deles resolvidos no final, suficiente para os estudantes se irem exercitando na aula e em casa.

Constitui um auxiliar valioso para o curso, permitindo uma maior liberdade nas aulas, na explicação teórica dos assuntos, substituindo uma exposição com grande pormenor formal por uma que realce a motivação e os aspectos intuitivos desses mesmos conceitos e respectivas inter-relações. Encaramo-lo como um mero guião das aulas, e não como um substituto das mesmas, e um estímulo à atenção e participação activa dos estudantes.

[16] *Proving is convincing and explaining*, Educational Studies in Mathematics 24 (1993) 389-399.
[17] Livro I, Cap. 18.

Foi escrito com o propósito de ser uma ferramenta útil para os alunos que são incapazes de tomar notas com cuidado e, simultaneamente, seguir a exposição. Permite-se assim que tais estudantes tenham a possibilidade de realmente participar na aula. Além disso torna a falta de comparência à aula menos inconveniente (só indo à aula quem nela esteja verdadeiramente interessado!). Na sua escrita tive quatro objectivos em mente:

- Oferecer uma diversidade de informações num só curso.
- Mostrar as relações entre os diferentes tópicos.
- Motivar os diferentes conceitos e estruturas com problemas clássicos e modernos relevantes, ilustrando o papel fundamental desses problemas no desenvolvimento da álgebra.
- Aplicar as técnicas e resultados obtidos à resolução dos problemas motivadores, mostrando como a álgebra abstracta também possui um carácter utilitário.

Em geral, tentámos caminhar sempre no sentido de motivar as estruturas mais abstractas a partir de exemplos e resultados mais concretos e simples. Tentámos também fazer com que, sempre que há uma demonstração simples para um determinado facto, o leitor não tenha que se envolver em abstracções desnecessárias para obter essa demonstração — à custa, evidentemente, de alguma repetição de demonstrações.

Cada secção termina com uma lista de exercícios, alguns deles resolvidos no final dos apontamentos. Recomenda-se aos alunos que abordem os problemas individualmente, começando por compreender bem o enunciado e ensaiando casos particulares. Frequentemente, dessa análise surge a ideia para a solução completa do problema. Caso não sejam capazes de o resolver, antes de abandonar o problema, podem sempre dar uma vista de olhos às primeiras linhas das soluções, que poderão sugerir pistas para a sua resolução.

De modo a obterem uma compreensão plena dos temas, os alunos deverão tentar resolver com seriedade um grande número de problemas. É isso que lhes é exigido nas aulas e para trabalho de casa. Não conseguindo aplicar as ideias e os métodos não conseguirão progredir muito. Quando confrontado com uma solução, o aluno deverá levantar questões como "Como posso ter a

certeza?", "Há mais soluções?", "O que aconteceria se mudasse um aspecto particular do problema?".

A página da internet constitui um instrumento de comunicação muito importante entre o professor e os alunos. A par da informação relevante para o curso (programa, bibliografia, apontamentos, avaliação, horário de atendimento dos alunos e sumários, notas históricas e ligações a outras páginas com informação interessante sobre a matéria), contém um espaço de notícias e novidades onde se vai inserindo ao longo do curso informação actualizada e material novo para as aulas (como, por exemplo, enunciados de testes e exames e respectivas resoluções, e leituras suplementares para os alunos mais interessados). A comunicação por correio electrónico entre professor e alunos é também incentivada, nomeadamente para o esclarecimento de pequenas dúvidas.

Além dos apontamentos das aulas indico a seguinte bibliografia, recomendando especialmente os livros de R. Loja Fernandes e M. Ricou (que penso ser um texto excelente para servir as três disciplinas de álgebra ao longo da Licenciatura), I. Stewart (para o Capítulo III), e R. Lidl e H. Niederreiter (para o último capítulo).

- Textos genéricos sobre anéis e corpos [18]:

  - R. Loja Fernandes e M. Ricou, *Introdução à Álgebra*, IST Press, 2004.

    Livro excelente, em português, que abarca todos os tópicos habitualmente apresentados nos cursos de álgebra abstracta (grupos, anéis e corpos, teoria de Galois) e de álgebra comutativa (álgebras especiais, teoria dos módulos, Teorema da Base de Hilbert e Noether).

  - A. Gonçalves, *Introdução à Algebra*, IMPA, Rio de Janeiro, 1979.

    Anéis, corpos, polinómios, grupos e teoria de Galois elementar, esta num último capítulo onde é apresentada a demonstração do Teorema Fundamental de Galois para corpos de característica

zero e discutido o problema da resolubilidade de equações polinomiais através de radicais.

- C. H. Hadlock, *Field Theory and Its Classical Problems*, The Carus Mathematical Monographs 19, The Mathematical Association of America, 2000.

  Começa com as construções geométricas com régua e compasso e a sua algebrização, tratando os três problemas clássicos dos gregos e a construção de polígonos regulares, e segue até ao problema da resolução de equações por meio de radicais. A teoria das extensões de corpos e as ferramentas da análise, álgebra linear, teoria dos números e da geometria algébrica vão-se organizando naturalmente à medida que as questões levantadas pelos problemas a resolver o exigem. Assim, é frequente que, após a generalização de um conceito, se faça a pedagogia de revisitar o problema acabado de resolver com um olhar mais eficaz. São fornecidas soluções completas para todos os problemas.

- Textos sobre construções com régua e compasso e resolubilidade algébrica de equações:

  - A. Jones, S. Morris e K. Pearson, *Abstract Algebra and Famous Impossibilities*, Universitext, Springer Verlag, 1994.

    Trata com muito pormenor as construções geométricas com régua e compasso e a sua algebrização, e em particular os três problemas clássicos da antiguidade. São desenvolvidas a álgebra e a geometria necessárias para provar a impossibilidade das três construções geométricas clássicas com régua e compasso. Inclui provas da transcendência dos números e e π. Faz ainda uma digressão breve sobre outras impossibilidades e a sua relação com a álgebra: construção de polígonos regulares, resolução de equações por radicais, e o cálculo de primitivas por meio de uma soma finita de funções elementares.

  - J. Filipe Queiró, *Das equações à Álgebra moderna*, em: F. Estrada *et al.*, *História da Matemática*, Universidade Aberta, 2000.

Descreve a evolução do problema da resolubilidade algébrica de equações nos séculos XVII, XVIII e XIX, nomeadamente a história dos contributos de vários matemáticos para a dedução das fórmulas resolventes de grau dois, três e quatro e para a demonstração da não existência de uma fórmula resolvente geral para a equação de grau cinco.

• Textos sobre teoria de Galois:

- I. Stewart, *Galois Theory*, Chapman & Hall, 1973 ($3^{\underline{a}}$ edição, 2004).

  Exposição pormenorizada e completa, com forte motivação e muitos exemplos, dos resultados fundamentais da teoria de Galois no contexto das extensões arbitrárias de corpos, não apenas nos subcorpos do corpo dos complexos.

- E. Artin, *Galois Theory*, Dover, 1998.

  Hoje um clássico, constituiu a primeira exposição moderna da Teoria de Galois.

• Textos sobre corpos finitos e aplicações:

- R. Lidl e H. Niederreiter, *Introduction to Finite Fields and their Applications*, Cambridge University Press, 2000.

  Livro excelente sobre o assunto, com um capítulo de aplicações: códigos correctores de erros, geometrias finitas, combinatória, sistemas finitos de entrada-estado-saída.

- A. Hefez e M. L. Villela, *Códigos Correctores de Erros*, IMPA, Rio de Janeiro, 2002.

  Monografia sobre os principais tipos de códigos correctores de erros definidos sobre corpos finitos.

Teaching should not be subjected to sudden swings under the capricious blast of ephemeral fads.

Henri Poincaré

No domínio da ciência a questão é extremamente precisa: as pessoas ou sabem ou não sabem. É justamente por isso que em todos os outros domínios as pessoas se contentam em envolver tudo numa verborreia brumosa. É por isso que em França ficam tão contentes de fazer passar o fantástico antes do científico. Há tão poucos que sabem o que é a ciência. É tão mais cómodo ter palavras brumosas. Esse é exactamente o problema. Garanto-vos que é muito fácil, em matemática, saber se um tipo sabe alguma coisa ou não. Também é muito fácil sabê-lo em física, em química, e numa quantidade jeitosa de ciências muito mais exactas do que aquelas com que nos martelam os ouvidos debaixo do nome de ciências sociais e económicas.

Boris Vian[18]

3. Métodos de ensino e avaliação

Aulas de carácter misto (exposição de matéria, discussão de exemplos e aplicações, resolução de problemas), onde se ensinam as ideias e estruturas fundamentais praticando sobre casos concretos, ilustradas com os aspectos históricos motivadores da sua génese e com aplicações relevantes. Dedica-se um espaço substancial à resolução de problemas por parte dos alunos, onde se encoraja o trabalho individual e a discussão em grupo. Aí tentamos dirigir o aluno na procura das soluções, combatendo as atitudes passivas. Os alunos «*só podem aprender a fazer Matemática através da imitação e prática.*»[19]

[18] *Boris Vian por Boris Vian* , Fenda, Lisboa, 2006.

[19] G. Polya, *Dez mandamentos para Professores*, Revista do Professor de Matemática, São Paulo, Sociedade Brasileira de Matemática, n.º 10: 2-10, 1987.

Concordo com Polya quando afirma qual é o objectivo principal do ensino da Matemática: «*ensinar os alunos a pensar.*»[20] Mas isso não significa que releguemos para segundo plano o aspecto informativo. O aluno só terá capacidade para pensar num problema se dominar uma parte substancial da matéria no qual ele se insere.

A minha abordagem às diversas matérias tenta ser genética. A intenção, como Otto Toeplitz descreve em [26] (ver, também, [11]), é olhar para as origens históricas de uma ideia de modo a encontrar a melhor maneira de a motivar: considerar o contexto no qual o "criador" da ideia estava a trabalhar de modo a determinar o "*burning problem*" que ele tentava resolver.

Como neste tema de ensino e pedagogia a minha opinião coincide, em muitos aspectos, com a perspectiva pessoal de S. Krantz [12] (um dos autores que mais têm influenciado a minha docência[21]), e não encontro melhores palavras que as dele, prefiro citá-lo nalguns pontos essenciais:

- «*Go from the simple to the complex — not the other way. It's an obvious point, but it works.*» (p. 17)
- «*Only wimps do the general case. Real teachers tackle examples.*» (citando B. Parlett na página 18)
- «*Many students read their texts with little or no understanding. They see the words but they do not understand the concepts. They need someone to tell them what is important, to give priority to the ideas, to demonstrate the techniques, to respond to their questions. This is something that a computer, or even a book, will never be able to do.*» (p. 21)
- «*Professor of Economic History Jonathan Hughes was wise to observe that "There is no substitute for knowing what you are talking about".*» (p. 16)
- «(...) *Let me assure you that I have discussed this point with the presidents of large high tech corporations and they agree with me absolutely.*

[20] G. Polya, *On learning, teaching, and learning teaching*, American Mathematical Monthly 70 (1963) 605-619.

[21] A par de [S. Zucker, *Teaching at the University Level*, Notices of the American Mathematical Society 43 (1996) 863-865].

Use of the new technology should be layered atop a traditional foundation. That is what works in the classroom and that is what works in the real world.» (p. 26)

- «*We must believe that being a good teacher is something worth achieving. We must provide some peer support to each other to bring about this necessary positive attitude towards teaching. The last thing I want is for mathematicians to spend all day in the coffee room debating the latest pedagogical techniques being promulgated by some Ivy League school of education. I want to see mathematicians learning and creating mathematics and sharing it with others. But these others should include undergraduates. That is what teaching is about.*» (p. 70)

Quanto à metodologia de avaliação, penso que deve reunir vários ingredientes que, em conjunto, promovam o envolvimento dos alunos nas aulas e na aprendizagem:

- Avaliação com diversas componentes, que em conjunto devem resultar na classificação final.

- Avaliação frequente: os alunos devem ser sujeitos a pequenas provas de avaliação frequentes, todas com peso na classificação final; terão assim tendência para estudar também de forma regular. O exame final deve ter particular ênfase na visão integradora da matéria da disciplina, evitando a sua atomização; a avaliação das várias partes da matéria já terá sido feita nos testes.

- As provas de avaliação devem ser devolvidas aos estudantes num prazo curto após a avaliação, para que estes possam ver o que fizeram bem e mal, e aprender corrigindo os erros.

- Promoção do trabalho autónomo. Só se aprende matemática fazendo matemática, e não sentado a olhar enquanto alguém a faz. Se o aluno se limita a observar o que professor faz, mesmo que entenda porque é que as coisas que ele faz estão correctas, poderá ter grandes dificuldades em fazer a mesma coisa mais tarde.

- Ser capaz de resolver um problema é só uma parte da aprendizagem matemática. É também importante que o aluno seja capaz de explicar o seu trabalho e os seus argumentos aos outros.

Concordo pois com as Metodologias de Avaliação propostas pela Comissão de Bolonha do DMUC em [19]:

> «*De forma recorrente surgem, nos vários documentos sobre estudos no âmbito de Bolonha, objectivos conducentes a um ensino mais personalizado, uma aprendizagem mais acompanhada e uma maior componente de avaliação contínua. Estes são objectivos que o Departamento também reconhece como importantes para uma melhoria da qualidade do estudo e da aprendizagem dos estudantes. Atingir tais objectivos exige não só uma eventual mudança na forma de ensino e avaliação, mas também uma alteração significativa de comportamento por parte da maioria dos estudantes. Há assim que encontrar mecanismos que permitam criar nos alunos hábitos de trabalho regular, maior autonomia e capacidade de iniciativa. O acompanhamento com sucesso de cada aluno deve ser um objectivo principal das metodologias a pôr em prática. (...) Apresenta-se de seguida uma proposta de avaliação que pretende ir ao encontro de uma valorização real do sistema de avaliação contínua e, assim, promover um estudo e uma aprendizagem de qualidade:*
>
> *(...) Para cada disciplina estaria prevista uma avaliação contínua e uma avaliação meramente final.*
>
> *Avaliação contínua: a realizar ao longo do período de leccionação da disciplina através da resolução de problemas, da elaboração de trabalhos individuais ou de grupo e/ou de pequenos testes, com pesos a definir para cada componente. A opção por este tipo de avaliação implicaria a presença, por exemplo, a 75% das aulas. Este tipo de avaliação deverá incluir uma componente de avaliação individual obrigatória, com um peso mínimo de 50%, que permita testar a compreensão global das matérias da disciplina. Uma classificação de 10 valores, pelo menos, neste*

processo garantiria a aprovação na disciplina. Para os alunos que, não tendo atingido os 10 valores, fossem considerados admitidos nesta avaliação (tendo atingido, por exemplo, um mínimo de 6,5 valores) haveria um exame final, que poderia ser apenas oral. Este exame seria aberto (quer para obter aprovação, quer para melhoria de classificação) apenas aos alunos que se tivessem submetido à avaliação contínua.

Avaliação só final: aprovação em exame final.»

Assim, proponho o seguinte método de avaliação:

(1) 3 testes,

(2) prova de frequência,

(3) exame final,

(4) prova complementar.

Os testes poderão consistir em pequenas provas escritas, realizadas durante a aula, ou na apresentação oral ou escrita, durante a aula ou no horário de gabinete, da solução de um problema escolhido de uma lista previamente distribuída aos alunos para trabalho de casa.

Sendo a cotação de cada teste igual a 1,5 valores, a da prova de frequência igual a 15,5 e a do exame igual a 20 valores, a nota final por frequência é igual à soma das notas dos testes com a nota da frequência, enquanto a nota final por exame é calculada pela fórmula

$$\boxed{\mathsf{Nota\ final} = \max\left\{\tfrac{15{,}5}{20} \times\ \mathsf{nota\ exame}\ +\ \mathsf{nota\ testes}\ ,\ \mathsf{nota\ exame}\right\}}$$

No futuro, o número e peso dos testes poderão ser aumentados caso esta experiência de avaliação revele melhorias na aprendizagem dos alunos.

Aos alunos exijo-lhes apenas o que lhes ensino. Em troca não faço concessões à sua falta de preparação. Nos exames não evito totalmente as chamadas "perguntas teóricas directas" pois penso que o aluno não pode descurar o exercício da sua memória, tão importante na sua vida futura. No entanto, essa componente, onde habitualmente peço aos alunos que formalizem um determinado conceito importante e apresentem uma demonstração de um

determinado resultado que envolva tal conceito (evidentemente, contido na lista dos resultados fundamentais apresentados no curso), nunca ultrapassa $\frac{1}{4}$ da cotação total da prova. No resto da prova tento avaliar principalmente a capacidade do aluno em usar os conhecimentos adquiridos ao longo do curso na resolução de problemas novos.

Aos alunos com classificação superior a 16 exijo, para confirmação da nota, a prestação de uma prova complementar com questões de dificuldade acima da média.

Referências bibliográficas

[1] E. Artin, *Galois Theory*, Dover, 1998.

[2] M. Atiyah, A. Borel, G. Chaitin, D. Friedan, Glimm, J. Gray, M. W. Hirsch, S. Mac Lane, B. Mandelbrot, D. Rulle, A. Schwarz, K. Uhlenbeck, R. Thom, E. Witten, C. Zeeman, *Responses to: A. Jaffe and F. Quinn, "Theoretical mathematics: toward a cultural synthesis of mathematics and theoretical physics"*, Bulletin of the American Mathematical Society 30 (1996) 178–207.

[3] I. Bashmakova e G. Smirnova, *The Beginnings and Evolution of Algebra*, Dolciani Mathematical Expositions 23, The Mathematical Association of America, 2000.

[4] D. M. Burton e D. H. Van Osdol, *Toward the definition of abstract ring*, em: *Learn from the Masters*, editado por F. Swetz, J. Farel, O. Bekken, B. Johansson e V. Katz, Mathematical Association of America, 1995, pgs. 241–251.

[5] L. Corry, *Modern Algebra and the Rise of Mathematical Structures*, Birkhäuser, 1996.

[6] Faculdade de Ciências e Tecnologia da Universidade de Coimbra, *Processo de Adequação de Ciclo de Estudos, Licenciatura em Matemática*, Outubro de 2006.

[7] C. H. Hadlock, *Field Theory and Its Classical Problems*, The Carus Mathematical Monographs 19, The Mathematical Association of America, 2000.

[8] A. Hefez e M. L. Villela, *Códigos Correctores de Erros*, IMPA, Rio de Janeiro, 2002.

[9] T. W. Hungerford, *Algebra*, Springer Verlag, 1980.

[10] A. Jones, S. Morris e K. Pearson, *Abstract Algebra and Famous Impossibilities*, Universitext, Springer Verlag, 1994.

[11] I. Kleiner, *The teaching of Abstract Algebra: an historical perspective*, em: *Learn from the Masters*, editado por F. Swetz, J. Farel, O. Bekken, B. Johansson e V. Katz, Mathematical Association of America, 1995, pgs. 225-239.

[12] S. Krantz, *How to Teach Mathematics, a personal perspective*, American Mathematical Society, 1993.

[13] R. Lidl e H. Niederreiter, *Introduction to Finite Fields and their Applications*, Cambridge University Press, 2000.

[14] R. Loja Fernandes e M. Ricou, *Introdução à Álgebra*, IST Press, 2004.

[15] S. Mac Lane, *Abstract Algebra uses homomorphisms*, American Mathematical Monthly 103 (1996) 330-331.

[16] E. Marques de Sá, J. Nunes da Costa, P. de Oliveira, P. Oliveira, J. F. Queiró, J. M. Urbano, *Relatório da Comissão de Reflexão sobre a Revisão dos Planos de Estudo de Matemática*, DMUC, 23/10/2001 (`www.mat.uc.pt/~reflecte/Relatorio.doc`).

[17] E. Marques de Sá, M. N. Mendes Lopes, J. F. Queiró, J. C. Petronilho e R. Kahle, *Estruturação do curso de Matemática no âmbito do processo de Bolonha: Propostas*, Comissão de Bolonha do DMUC, 19/05/2006.

[18] E. Marques de Sá, M. Sobral e O. Azenhas, *Álgebra I e Álgebra II: programas mínimos*, DMUC, 2003.

[19] E. Marques de Sá, M. N. Mendes Lopes, J. F. Queiró, J. C. Petronilho e R. Kahle, *O Processo de Bolonha no DMUC: algumas linhas de acção*, Comissão de Bolonha do DMUC, 11/01/2007.

[20] C. McLarty, *The last mathematician from Hilbert's Göttingen: Saunders Mac Lane as philosopher of mathematics*, British J. Philos. Sci. 58 (2007) 77-112.

[21] P. Pesic, *Abel's Proof, An Essay on the Sources and Meaning of Mathematical Unsolvability*, MIT Press, 2003.

[22] J. Picado, *Corpos e Equações Algébricas*, Notas de curso, Universidade de Coimbra, 2007 (`www.mat.uc.pt/~picado/corpos/apontamentos.html`, Primeira versão: Aulas de Álgebra II, 2005).

[23] J. Picado e M. Sobral, *Textos de Apoio de Álgebra*, Universidade de Coimbra, 2000.

[24] I. Stewart, *Galois Theory*, Chapman & Hall, 1973 (3ª edição, 2004).

[25] F. Swetz, J. Farel, O. Bekken, B. Johansson e V. Katz, *Learn from the Masters*, Mathematical Association of America, 1995.

[26] O. Toeplitz, *Calculus: A Genetic Approach*, The University of Chicago Press, 1963.