Introdução

Estas notas incluem com algum pormenor os principais conceitos e resultados apresentados nas aulas teóricas, completados aqui e acolá com alguns exemplos, observações e exercícios. Espera-se que sejam um auxiliar valioso para o curso, que permita 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, e que por outro lado sejam um estímulo à atenção e participação activa dos estudantes.

Devem ser encaradas como um mero guião das aulas, e portanto não são um substituto das mesmas nem sequer da bibliografia indicada.

Assumem-se alguns preliminares, nomeadamente:

- matéria dada na disciplina de Álgebra I.
- conhecimentos básicos de Teoria dos Números.
- conhecimentos gerais de Álgebra Linear.
- a "maturidade matemática" que se espera de estudantes do terceiro ano da licenciatura em Matemática.

No desenvolvimento do programa seguir-se-à a recomendação de fundo expressa no programa mínimo da disciplina:

"... que se faça uma abordagem com um grau de abstracção algo apurado, de acordo com o facto de se tratar de uma disciplina do terceiro ano da licenciatura, 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."

1. Anéis e Corpos

Uma das características da matemática do último século foi a sua tendência para a abstracção. Das áreas da chamada "álgebra moderna", só a teoria abstracta dos anéis e ideais é inteiramente um produto do século XX. De facto, praticamente toda a teoria de anéis estudada e ensinada hoje em dia é resultado do trabalho de matemáticos dos últimos 80 anos.

A teoria moderna dos anéis teve, no entanto, origem no século XIX, em duas fontes distintas: em Richard Dedekind (1831-1916), que introduziu em 1871 a noção de ideal, no seu trabalho de generalizar o Teorema Fundamental da Aritmética (da factorização única em primos) a contextos mais abstractos, e no trabalho de David Hilbert (1862-1945), Edmund Lasker (1868-1941) e F. S. Macaulay (1862-1927) em anéis de polinómios.

O pioneiro no tratamento abstracto da teoria dos anéis foi Adolf Fraenkel (1891-1965) com o artigo "On the divisors of zero and the decomposition of rings"[1]. Este artigo contém a primeira caracterização axiomática da noção de anel, embora não seja a utilizada hoje em dia. O seu objectivo era sair do estudo particular dos corpos, de modo a obter uma teoria suficientemente geral para poder ser aplicada aos inteiros módulo n, aos números p-ádicos e aos sistemas de "números hipercomplexos". A definição actualmente utilizada de anel (comutativo) parece ter aparecido pela primeira vez em 1917, num artigo do matemático japonês Masazo Sono intitulado "On congruences"[2].

O matemático que mais contribuiu para o avanço do ponto de vista abstracto na teoria dos anéis foi Emmy Noether (1882-1935). É costume apontar-se o seu artigo "Ideal theory in rings"[3] de 1921 como origem da teoria abstracta dos anéis. O seu tratamento axiomático, muito elegante, constituiu uma novidade ao tempo[4]. Neste artigo, Noether estende o trabalho de Hilbert, Lasker e Macaulay nos anéis de polinómios a anéis mais gerais. Num artigo subsequente [5], faz num anel abstracto o que Dedekind tinha feito para anéis de números algébricos.

A ideia revolucionária de trabalhar de modo abstracto com anéis e seus ideais —

[1] *Journal für die Reine und Angewandte Mathematik* 145 (1914) 139-176.

[2] *Memoirs of the College of Science of Kyoto* 2 (1917) 203-226.

[3] *Mathematische Annalen* 83 (1921) 24-66.

[4] Nas palavras de Kaplansky, "The importance of this paper is so great that it is surely not much of an exaggeration to call her the mother of modern algebra".

[5] Abstract study of ideal theory in algebraic number- and function-fields, *Mathematische Annalen* 96 (1927) 203-226.

devida a Fraenkel, Sono e Noether — conduziu ao contexto "certo" para o estudo da factorização prima e criou a área que hoje é chamada Álgebra Comutativa. Em 1931 o livro famoso de van der Waerden's[6] colocou todas estas ideias à disposição de uma nova geração de algebristas.

Porquê $(-1)(-1) = 1$? Mais geralmente, porquê $(-a)(-b) = ab$? E $a \cdot 0 = 0$? Estas são questões que fazem parte do problema geral de justificação lógica das leis de operação com os números negativos e que nos conduzem aos conceitos de anel (e domínio de integridade e estrutura ordenada).

ANEL

Um *anel* $(A, +, \cdot)$ é um conjunto A com duas operações binárias, que denotaremos por $+$ e $\cdot$, tais que:

(1) $(A, +)$ é um grupo abeliano.

(2) $\cdot$ é associativa; ou seja,

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \text{ para quaisquer } a, b, c \in A.$$

(3) $\cdot$ é distributiva relativamente a $+$; ou seja,

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

e

$$(b + c) \cdot a = b \cdot a + c \cdot a$$

para quaisquer $a, b, c \in A$.

Usaremos simplesmente a letra A para designar um anel arbitrário $(A, +, \cdot)$. Um anel A diz-se *comutativo* se $\cdot$ é comutativa e chama-se *anel com identidade* (ou *anel unitário*) se a operação $\cdot$ possui um elemento neutro (chamado *identidade*) — ou seja, se existe um elemento 1 em A tal que $a \cdot 1 = 1 \cdot a = a$ para qualquer $a \in A$.

[6] *Modern Algebra*, Springer-Verlag, Berlim, 1931.

Designação	Notação	O que representa
Zero do anel	0	neutro de $+$
Simétrico de $a \in A$	$-a$	inverso de a no grupo $(A, +)$
Múltiplo de $a \in A$	na	$a + a + \cdots + a$ ($n \in \mathbb{Z}$ parcelas)
Identidade do anel	1	neutro de $\cdot$, caso exista
Inverso de $a \in A$	a^{-1}	inverso de a em $(A, \cdot)$, caso exista
Potência de $a \in A$	a^n a^{-n}	$a \cdot a \cdot \cdots \cdot a$ ($n \in \mathbb{Z}^+$ factores) $a^{-1} \cdot a^{-1} \cdot \cdots \cdot a^{-1}$ ($n \in \mathbb{Z}^+$ factores)

Exercício. Verifique, por indução, que, para quaisquer $a_1, a_2, \cdots, a_n, b_1, b_2, \cdots, b_m$ em A, se tem:

(a) $a(b_1 + b_2 + \cdots + b_m) = ab_1 + ab_2 + \cdots ab_m$.

(b) $(a_1 + a_2 + \cdots + a_n)(b_1 + b_2 + \cdots + b_m) = a_1b_1 + a_1b_2 + \cdots + a_1b_m + a_2b_1 + a_2b_2 + \cdots + a_2b_m + \cdots + a_nb_1 + a_nb_2 + \cdots + a_nb_m$.

Exemplos de anéis:

(1) $(\mathbb{Z}, +, .)$, $(\mathbb{Q}, +, .)$, $(\mathbb{R}, +, .)$ e $(\mathbb{C}, +, .)$.

(2) $(n\mathbb{Z}, +, \cdot)$ $(n = 1, 2, \ldots)$. [para $n \geq 2$ não é unitário]

(3) $(\mathbb{Z}_n, \oplus_n, \otimes_n)$ $(n = 1, 2, \ldots)$. [$\mathbb{Z}_n = \{0\}$ para $n = 1$]

(4) O conjunto $M_n(\mathbb{Z})$ das matrizes quadradas de ordem n ($n \in \mathbb{N}$) com elementos inteiros, munido das operações de adição e multiplicação de matrizes.

[para $n \geq 2$ não é comutativo]

Mais geralmente, $M_n(A)$ para qualquer anel A.

(5) $(\mathcal{P}(X), \Delta, \cap)$ para qualquer conjunto $X \neq \emptyset$.

[recorde: $A \Delta B := (A \cup B) \setminus (A \cap B)$] [$0 = \emptyset$, $1 = X$]

[anel comutativo com identidade]

[observe: $A \Delta A = \emptyset$, $A \cap A = A$]

Proposição. *Seja A um anel. Para quaisquer $a, b \in A$ tem-se:*

(a) $a \cdot 0 = 0 \cdot a = 0$.

(b) $(-a)b = a(-b) = -(ab)$.

(c) $(-a)(-b) = ab$.

Demonstração. (a) $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$, o que implica, pela lei do cancelamento válida em qualquer grupo, $a \cdot 0 = 0$. Analogamente, $0 \cdot a = 0$.
(b) Usando a alínea (a), $ab + (-a)b = (a + (-a))b = 0 \cdot b = 0$, donde $(-a)b = -(ab)$. Analogamente, $a(-b) = -(ab)$.
(c) Pela alínea (b) tem-se $(-a)(-b) = -(a(-b)) = -(-(ab))$. Mas, em qualquer grupo, $-(-(ab)) = ab$. Logo $(-a)(-b) = ab$. ∎

Assumiremos sempre que num anel com identidade $1 \neq 0$. Com efeito, por 1(a), se $0 = 1$ então, para qualquer $a \in A$, $a = a \cdot 1 = a \cdot 0 = 0$ e o anel A reduz-se ao caso trivial $A = \{0\}$.