Teoria dos Corpos Comutativos

Textuniversitários 37

Jean A. Dieudonné

Teoria dos Corpos *Comutativos*

LF Editorial
São Paulo — 2025

1a. Edição

Editor: Victor Pereira Marinho / José Roberto Marinho
Projeto gráfico e diagramação: Thiago Augusto Silva Dourado
Capa: Fabrício Ribeiro

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Dieudonné, Jean A.
Teoria dos corpos comutativos / Jean A. Dieudonné. –– São Paulo : LF Editorial, 2025. –– (Textuniversitários ; 37)

ISBN 978-65-5563-684-0

1. Matemática I. Título. II. Série.

25-322952.0 CDD–510

Índices para catálogo sistemático:

1. Matemática 510

Eliane de Freitas Leite – Bibliotecária – CRB 8/8415

Impresso no Brasil
Printed in Brazil

LF EDITORIAL

www.lfeditorial.com.br
Visite nossa livraria no Instituto de Física da USP
www.livrariadafisica.com.br
Telefones:
(11) 39363413 - Editora
(11) 26486666 - Livraria

Nota do Editor

A ideia de editar esta obra não é nova. Tratando-se de um texto de primeira grandeza, escrito de forma esmiuçada e paulatina, visando ainda à autossuficiência, tanto quanto possível, e redigido em português por um dos grandes expoentes da Matemática do século XX, quando esteve no Brasil nos anos 1940, parecia inevitável que, em algum momento, eu me debruçasse sobre esta obra para produzir uma nova edição. Mas a tarefa sempre fora postergada em função de não poucos outros afazeres.

Em um encontro casual no meu primeiro ano de doutorado com o Prof. Odilon Luciano, em uma cafeteria da Universidade de São Paulo, compartilhando essa paixão comum por livros clássicos, contei sobre meu desejo e a dificuldade de tempo que enfrentaria, haja vista que teria de fazer uma edição do zero (digitação, confecção de figuras, diagramação, revisão, etc.). Mas então o Prof. Odilon me falou que um de seus colegas, José Augusto Abrantes, já havia digitado o livro inteiro. Nesse momento, percebi que a parte mais trabalhosa do processo já tinha sido feita, então não havia por que adiar mais. Reunimo-nos, então, Augusto, Odilon e eu, na sala de convivência do Instituto de Matemática e Estatística da Universidade de São Paulo (IME-USP), e demos início aos trabalhos. Após quatro anos, apresentamos ao público esta magnífica obra.

Inicialmente, a obra fora publicada pela Sociedade de Matemática de São Paulo em três volumes: 1946, 1947 e 1958, confeccionados em datilografia mecânica por Luiz Henrique Jacy Monteiro a partir dos apontamentos do curso do Prof. Jean Dieudonné, oferecido a então Faculdade de Filosofia, Ciências e Letras da Universidade de São Paulo, no ano de 1946. Resolvemos, por uma questão de pragmatismo, publicar a obra em um único volume, dividido em três partes, que correspondem aos volumes originais.

Thiago Augusto S. Dourado
São Paulo, dezembro de 2025

Sumário

Parte III.
Corpos Ordenados e Teoria das Valorizações

Introdução

A noção de corpo comutativo é, essencialmente, a de um sistema de elementos sobre os quais se podem efetuar duas operações fundamentais, a adição e a multiplicação, de tal modo que todas as regras formais do cálculo algébrico sobre os números racionais (com exceção das regras relativas às desigualdades) permaneçam válidas. Uma tal concepção só poderia surgir no dia em que se percebesse a necessidade de se considerar outros "números" além dos racionais; e é bem a esta época que é preciso fazer recuar a história da noção de corpo. Se se faz abstração, com efeito, das imperfeições da álgebra dos gregos (e principalmente do fato de que eles ignoravam os números negativos), é igualmente um fato que o movimento de ideias que acompanhou a descoberta dos números irracionais introduziu na ciência duas concepções fundamentais: de uma parte — com a teoria das "razões" edificada por Eudóxio, equivalente à teoria de Dedekind para números reais positivos — a noção de *extensão formal* de um sistema de "números", ligada à necessidade de *definir* para os novos "números" introduzidos a igualdade e as operações fundamentais, e daí *demonstrar* as propriedades, apoiando-se unicamente sobre as propriedades do sistema inicial; de outra parte, um primeiro germe de *classificação* dos irracionais, em relação estreita com os problemas clássicos de "construção por régua e compasso" que viriam ser a fonte de muitos progressos ulteriores.

Sob sua forma geométrica inicial, e mais ainda sob a forma algébrica mais geral do problema de resoluções de equações "por radicais", esses últimos problemas não deixaram de atrair a atenção dos matemáticos durante a Idade Média (quando a teoria abstrata de Eudóxio, muito acima da ciência da época, permanecia de lado). Mas foi somente no século XVI que apareceram os primeiros progressos importantes nessa via, com a descoberta das fórmulas de resolução por radicais das equações gerais de terceiro e quarto graus, devido à escola italiana; fato mais importante do que as próprias fórmulas, sua aplicação encontrou a necessidade de ampliar mais uma vez a noção de número, introduzindo as raízes quadradas de números negativos, isto é, os imaginários. Mais ainda que para os irracionais, aqui se trata de uma extensão "formal", pois decorreram dois séculos para que se tivesse uma representação geométrica desses números; mas, durante toda essa época (muito afastada, no conjunto, do espírito de rigor dos gregos), os números complexos foram manejados experimentalmente, sem a busca de se fazer repousar sua teoria sobre bases sólidas. Em fins do século XVII, e apesar de todas as tentativas infrutíferas de determinar a fórmula de resolução "por radicais" das equações de grau superior ao quarto, chegou-se à convicção de que toda equação algébrica tinha raízes complexas ("teorema de d'Alembert", cuja primeira demonstração rigorosa foi dada por Gauss), não parecia, então, necessário estender, novamente, a concepção de "número".

Foi neste momento que se abriu o período moderno da teoria, com as pesquisas de Lagrange: analisando as razões do sucesso dos métodos de resolução das equações de grau não superior à 4 e do insucesso das tentativas de extensão desses métodos, mostrou que elas estavam ligadas à existência de funções das raízes da equação que permaneciam invariantes por determinadas permutações dessas raízes. É esta ideia que conduziria, um pouco mais tarde, Ruffini e Abel à demonstração da impossibilidade da resolução por radicais das equações gerais de grau superior a 4; posteriormente, coube a Galois à teoria definitiva das resoluções das equações algébricas por meio de equações de grau inferior. Então, a noção de corpo de números algébricos era então conhecida em toda a sua generalidade e iria dominar a Teoria dos Números durante o século XIX.

Enfim, durante este último período, outros trabalhos levaram ainda a estender o conceito de corpo: de uma parte, a teoria dos corpos *finitos*, que decorre dos trabalhos de Galois; em segundo lugar, o método de Dedekind e Weber para o estudo de curvas algébricas, que repousa sobre a teoria dos corpos de *funções algébricas*; e, finalmente, a introdução de Hensel da fecunda noção de *números p-ádicos*. Restava somente reunir uma teoria geral das propriedades comuns a esses diversos corpos; esta foi a obra de Steinitz, que, numa memória fundamental publicada em 1910 (*Journal de Crelle*, vol. 137), deu a classificação completa de todas as estruturas possíveis de corpo comutativo.

Neste curso, desenvolveremos a teoria de Steinitz e alguns de seus prolongamentos mais interessantes. Após ter recordado, nos dois capítulos preliminares, as noções fundamentais da Álgebra Moderna que nos serão necessárias (grupos, anéis, espaços vetoriais, polinômios), estudaremos, no Capítulo III, a teoria geral das *extensões* de um corpo dado. O Capítulo IV será reservado para a teoria dos isomorfismos das extensões algébricas de um corpo, que conduz à importante distinção entre extensões separáveis e extensões inseparáveis, e tem sua aplicação na *teoria de Galois*, que forma o objeto dos Capítulos V e VI. No Capítulo VII, estudaremos um tipo bem peculiar de corpos: os *corpos ordenados*. Por fim, o último capítulo será consagrado ao estudo das *valorizações sobre um corpo* e suas extensões algébricas, bem como às aplicações dessa noção à teoria da divisibilidade nas extensões algébricas de um corpo.

Noções Gerais sobre Teoria dos Conjuntos

1. Uma *aplicação* de um conjunto E em um conjunto F é uma operação que, a cada elemento x de E, faz corresponder *um e somente um elemento* y de F; se f designa uma aplicação de E em F, indica-se com $f(x)$ ou f_x (notação indicial) o elemento de F que corresponde a x pela aplicação f e que se chama a *imagem* de x por f, ou o *valor* de f para o elemento x. A aplicação f se escreve também $x \to f(x)$. As aplicações de um conjunto E em F são os elementos de um novo conjunto, o *conjunto das aplicações de* E *em* F, que se indica por F^E; para que duas aplicações f e g de E em F sejam iguais, é necessário e suficiente que $f(x) = g(x)$ para todo $x \in E$.

A aplicação $x \to x$ de E em E é denominada *aplicação identidade* de E. Se A for uma parte de E, a aplicação que, a todo $x \in A$, faz corresponder o mesmo elemento x, considerado como elemento de E, é chamada aplicação *canônica* de A em E.

Se f for uma aplicação de E em E, diz-se que $x \in E$ é *invariante por* f se $f(x) = x$.

Se f for uma aplicação de E em F, e A uma parte de E, a aplicação f_A que, a todo $x \in A$, faz corresponder $f(x)$, é denominada *restrição* de f ao conjunto A; inversamente, f é chamada *prolongamento à* E da aplicação f_A.

2. Diz-se que uma aplicação f de E em F é uma aplicação *sobre* F se, para todo $y \in F$, existe um $x \in E$ (pelo menos) tal que $f(x) = y$.

Diz-se que uma aplicação f de E em F é uma aplicação *unívoca* de E *em* F se da relação $f(x) = f(x')$ resultar $x = x'$.

Diz-se que uma aplicação f de E em F é uma aplicação *biunívoca* de E *sobre* F se, para todo $y \in F$, existe *um e somente um* $x \in E$ tal que $y = f(x)$; se indicarmos com $g(y)$ este elemento x, g é uma aplicação biunívoca de F sobre E, denominada *aplicação recíproca* de f.

Uma aplicação biunívoca de E sobre si mesmo é denominada *permutação* de E.

3. Seja f uma aplicação de E em F; para toda parte X de E, designa-se por $f(X)$ o conjunto dos $y \in F$ tais que exista um $x \in X$ tal que $y = f(x)$; diz-se que $f(X)$ é a *imagem de* X *por* f e a aplicação $X \to f(X)$ de $\mathscr{P}(E)$ (onde $\mathscr{P}(E)$ indica o conjunto formado pelos subconjuntos de E) em $\mathscr{P}(F)$ é denominada *extensão de* f *ao conjunto das partes*. A relação $X = \varnothing$ é equivalente a $f(X) = \varnothing$. Da relação $X \subset Y$ resulta $f(X) \subset f(Y)$.

Para toda parte Y de F, o conjunto dos $x \in E$ tais que $f(x) \in Y$ é indicado por $f^{-1}(Y)$ e denominado *imagem recíproca de Y por f*; da relação $X \subset Y$ resulta $f^{-1}(X) \subset f^{-1}(Y)$; tem-se $f^{-1}(\varnothing) = \varnothing$, mas se pode ter $f^{-1}(X) = \varnothing$ para uma parte não vazia X de F, salvo quando f é uma aplicação de E *sobre* F.

4. Se f é uma aplicação de E em F, g é uma aplicação de F em G, a aplicação $x \to g(f(x))$ de E em G é denominada *composta de g e de f*, e indicada por $g \circ f$; se $h = g \circ f$, tem-se $h(X) = g(f(X))$ para toda parte X de E e $h^{-1}(Z) = f^{-1}(g^{-1}(Z))$ para toda parte Z de G.

5. Quando se dá uma aplicação $\iota \to x_\iota$ de um conjunto I em um conjunto E, diz-se também que se deu uma *família de elementos* $(x_\iota)_{\iota \in I}$ tendo I para *conjunto de índices*. O *conjunto dos elementos* da família é a imagem de I pela aplicação $\iota \to x_\iota$; duas famílias distintas podem ter o mesmo conjunto de elementos. Uma *sequência* é um caso particular de uma família, correspondente ao caso em que I é o conjunto dos inteiros positivos; uma *sequência finita* corresponde ao caso em que I é um conjunto *finito* de inteiros.

6. Se $(X_\iota)_{\iota \in I}$ é uma família de partes de E, a *união* dessa família é o conjunto dos $x \in E$ tais que existe pelo menos um X_ι tal que $x \in X_\iota$; indica-se este conjunto por $\bigcup_{\iota \in I} X_\iota$; a união de uma sequência finita $(X_i)_{1 \le i \le n}$ indica-se por $X_1 \cup X_2 \cup \cdots \cup X_n$.

A *interseção* da família $(X_\iota)_{\iota \in I}$ é o conjunto dos $x \in E$ tais que $x \in X_\iota$ para *todo* $\iota \in I$; indica-se esse conjunto por $\bigcap_{\iota \in I} X_\iota$; a interseção de uma sequência finita $(X_i)_{1 \le i \le n}$ indica-se por $X_1 \cap X_2 \cap \cdots \cap X_n$.

Para toda aplicação f de E em F e toda família $(X_\iota)_{\iota \in I}$ de partes de E, tem-se

$$f\left(\bigcup_{\iota \in I} X_\iota\right) = \bigcup_{\iota \in I} f(X_\iota);$$

e para toda família $(Y_\lambda)_{\lambda \in L}$ de partes de F, tem-se

$$f^{-1}\left(\bigcup_{\lambda \in I} Y_\lambda\right) = \bigcup_{\lambda \in L} f^{-1}(Y_\lambda) \quad \text{e} \quad f^{-1}\left(\bigcap_{\lambda \in I} Y_\lambda\right) = \bigcap_{\lambda \in L} f^{-1}(Y_\lambda).$$

7. Chama-se *produto* de dois conjuntos E e F e se indica por $E \times F$ o conjunto dos pares (x, y) tais que $x \in E$ e $y \in F$. Define-se do mesmo modo o produto de mais de dois conjuntos.

A toda relação R entre um elemento $x \in E$ e um elemento $y \in F$ corresponde o conjunto de pares (x, y) de $E \times F$ tais que x e y estejam ligados pela relação R. Este conjunto é denominado *conjunto representativo* da relação R.

Em particular, se f é uma aplicação de uma parte A de E em F, o conjunto dos pares (x, y) de $E \times F$ tais que $x \in A$ e $y = f(x)$ é o *conjunto representativo* ou o *gráfico* da aplicação f. Para que uma aplicação g de uma parte de E em F seja um prolongamento de f, é necessário e suficiente que o gráfico de f esteja contido no gráfico de g.

Sejam f uma aplicação de E em E' e g uma aplicação de F em F': a aplicação $(x, y) \to (f(x), g(y))$ de $E \times F$ em $E' \times F'$ é denominada *extensão ao produto* das aplicações f e g.

8. Diz-se que uma relação R entre dois elementos (variáveis) de um conjunto E é uma *relação de equivalência* se ela verificar as seguintes condições:

1º) Tem-se $R(x, x)$ para todo $X \in E$ (*reflexividade*);

2º) Se se tem $R(x, y)$, tem-se também $R(y, x)$ (*simetria*);

3º) Se se tem $R(x, y)$ e $R(y, z)$, tem-se também $R(x, z)$ (*transitividade*).

Para todo $x \in E$, o conjunto dos $y \in E$ tais que $R(x, y)$ é um conjunto K_x denominado *classe de equivalência de* x; os elementos de K_x são ditos *equivalentes a* x (pela relação R); se $y \in K_x$, tem-se $K_y = K_x$; se $y \notin K_x$, tem-se $K_x \cap K_y = \varnothing$.

O conjunto das classes de equivalência K_x (parte de $\mathscr{P}(E)$) é denominado *conjunto quociente* de E pela relação R e indicado por E/R

em geral; a aplicação $x \to K_x$ de E sobre E/R é denominada *aplicação canônica*.

9. Diz-se que uma relação ω entre dois elementos (variáveis) de um conjunto E é uma *relação de ordem* se verificar as seguintes condições:

1º) Se se tem $\omega(x,y)$ e $\omega(y,z)$, tem-se também $\omega(x,z)$ (*transitividade*);

2º) Se se tem $\omega(x,y)$ e $\omega(y,x)$, tem-se necessariamente $x = y$.

Um conjunto munido de uma relação de ordem é denominado conjunto *ordenado* (por esta relação). A relação de inclusão $X \subset Y$ entre partes de um conjunto E é uma relação de ordem em $\mathscr{P}(E)$; a relação "g é um prolongamento de f" entre aplicações f e g de partes de E num conjunto F é uma relação de ordem no conjunto de todas as aplicações. Uma relação de ordem sobre um conjunto E é indicada, em geral, por $x \leq y$; a relação $x < y$ significa então que $x \leq y$ e $x \neq y$.

Um conjunto E é denominado *totalmente ordenado* por uma relação de ordem $x \leq y$ se para dois elementos quaisquer x, y de E tem-se sempre, seja $x \leq y$, seja $y \leq x$.

10. Diz-se que uma parte A de um conjunto ordenado E admite um *menor elemento* (respectivamente, *maior elemento*) $a \in A$, se para todo $x \in A$, tem-se $a \leq x$ (respectivamente, $x \leq a$); se este elemento existir, ele é único. Se A é um conjunto de partes de E, o menor elemento (respectivamente, maior elemento) pela relação de inclusão é a interseção (respectivamente, a união) dos conjuntos pertencentes a A, desde que esta interseção (respectivamente, união) pertença a A; no caso contrário, A não tem menor elemento (respectivamente, maior).

Diz-se que um elemento a de uma parte A de E é *minimal* (respectivamente, *maximal*) se não existir nenhum elemento x de A tal que $x < a$ (respectivamente, $a < x$); se A tiver um menor elemento (respectivamente, maior elemento), este é o único elemento minimal (respectivamente, maximal), mas um conjunto pode ter uma infinidade de elementos minimais (respectivamente, maximais), ou não ter nenhum.

Diz-se que um conjunto $A \subset E$ possui um *extremo superior* (respectivamente, *extremo inferior*) se o conjunto B dos elementos y de E que são tais que $y \geq x$ (respectivamente, $y \leq x$) para todo $x \in A$, possui um menor elemento (respectivamente, um maior elemento); este elemento é, então, por definição, o extremo superior (respectivamente, extremo inferior) de A.

11. Diz-se que um conjunto ordenado é *indutivo* se toda parte G de E, *totalmente ordenada* (nº 9) possui um *extremo superior* (nº 10).

Teorema de Zorn. *Todo conjunto ordenado indutivo possui pelo menos um elemento maximal.*

Em particular, um conjunto $\mathfrak{A}$ de partes de E é indutivo (pela relação de inclusão) se, para toda parte $\mathfrak{B}$ de $\mathfrak{A}$ totalmente ordenada, a *união* dos conjuntos de $\mathfrak{B}$ pertence a $\mathfrak{A}$.

12. Seja E um conjunto considerado como fundamental, $A, B, \ldots$ um certo número de conjuntos considerados como auxiliares. Diz-se que um conjunto pertence à *escala de conjuntos* construída sobre $E, A, B, \ldots,$ se ele se obtém repetindo um certo número de vezes a partir destes conjuntos as operações que consistem em formar o *produto* de dois conjuntos ou o *conjunto das partes* de um conjunto; por exemplo, $E \times A$, $\mathscr{P}(E \times E)$, $\mathscr{P}(\mathscr{P}(E))$ e $\mathscr{P}(A \times \mathscr{P}(E))$ são conjuntos da escala.

Por definição, uma *estrutura* sobre E é um elemento σ de um dos conjuntos da escala precedentes. Por exemplo, uma relação de ordem ω sobre E define uma parte de $E \times E$, seu conjunto representativo (nº 7) é um elemento σ de $\mathscr{P}(E \times E)$; σ é a *estrutura de conjunto ordenado* definida sobre E pela relação ω. Do mesmo modo, uma aplicação f de $A \times E$ em E define uma parte de $(A \times E) \times E$, seu gráfico (nº 7) é então um elemento σ de $\mathscr{P}((A \times E) \times E)$; esta aplicação (dita *lei de composição externa* sobre E) define então uma estrutura σ sobre E.

Seja E' um segundo conjunto fundamental. A todo conjunto M da escala construída sobre $E, A, B, \ldots,$ corresponde um conjunto M' da escala construída sobre $E', A, B, \ldots,$ obtido efetuando sobre