Matemática Universitária N. 7, Junho de 1988, 133 - 137.

Teoria dos Números Algébricos, por Otto Endler, Projeto Euclides, IMPA.

Fernando Quadros Gouvêa
Instituto de Matemática - USP
Caixa Postal 20.570 - Agência Iguatemi
01.498 - São Paulo, SP

A idéia de estudar a aritmética de domínios mais complicados do que os inteiros racionais surge naturalmente de vários problemas clássicos da teoria elementar dos números. O exemplo mais fácil são as equações diofantinas. Por exemplo, é fácil ver que a maneira certa de estudar o problema de encontrar inteiros x e y tais que $x^2 - y^2 = p$ (onde p é um primo) é escrever

$$x^2 - y^2 = (x + y)(x - y)$$

e interpretar a equação como um problema de fatoração em $\mathbb{Z}$. Da mesma forma, para determinar os inteiros x, y tais que $x^2+y^2 = p$, poderíamos escrever

$$(x + iy)(x - iy) = x^2 + y^2 = p$$

e interpretar a equação como um problema de fatoração em

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}.$$

A mesma idéia surge naturalmente para tratar equações como $x^2 \pm Dy^2 = p$, que sugerem a introdução de inteiros do tipo $a + \sqrt{\pm D}\, b$, $a, b \in \mathbb{Z}$, e até a equação de Fermat $x^n + y^n = z^n$, que sugere o estudo do anel $\mathbb{Z}[\varsigma]$, onde $\varsigma^n = 1$, para podermos escrever

$$x^n + y^n = (x + y)(x + \varsigma y)(x + \varsigma^2 y) \cdots (x + \varsigma^{n-1} y).$$

Além destes, outros problemas, como por exemplo a busca de generalizações do Teorema de Reciprocidade Quadrática, serviram de motivação inicial.

A dificuldade essencial na introdução destes "inteiros" mais gerais é determinar se as propriedades características dos inteiros racionais permanecem válidas. O exemplo mais marcante é o teorema de fatorização única, que diz que todo inteiro racional tem uma expressão única como produto de primos, (isto é, de números que não podem ser decompostos como produtos de outros números). A pressuposição inicial era de que o teorema análogo seria válido também no contexto mais geral; por exemplo, Lamé chegou a apresentar à Academia de Paris uma demonstração da conjetura de Fermat que pressupunha a unicidade de fatorização para os anéis $\mathbb{Z}[\zeta]$ de inteiros ciclotômicos. As dúvidas de Liouville em relação a essa pressuposição foram logo confirmadas por Kummer, que já havia notado a falta de fatorização única em certos anéis de inteiros ciclotômicos. (Por exemplo, em $\mathbb{Z}[\zeta]$ quando $\zeta^{23} = 1$.)

Foi o próprio Kummer quem primeiro propôs uma solução. Sua idéia foi definir *divisores primos ideais* para fazer as vezes dos primos: se p, q, r e s são irredutíveis (isto é, não podem ser decompostos como produto) e $p \cdot q = r \cdot s$, deve haver divisores p_1, p_2, q_1, q_2, tais que

$$p = p_1 \cdot p_2$$
$$q = q_1 \cdot q_2$$
$$r = p_1 \cdot q_2$$
$$s = p_2 \cdot q_1.$$

É claro que não há dois números p_1, p_2 cujo produto é p (porque p é irredutível!), mas Kummer construiu uma teoria completa para trabalhar com tais "divisores ideais". A observação fundamental é que basta descrever como saber *qual potência* de um "divisor ideal" divide um elemento do anel de inteiros em questão. Esta idéia é o germe do que hoje se chama *teoria das valorizações.*

A idéia dos "divisores primos ideais" causou dificuldade a muitos matemáticos, até que Dedekind mostrou que a teoria podia ser construída sem referência aos misteriosos "divisores ide-

ais". Em essência, ele observou que bastava substituir os "divisores ideais" de Kummer pelo conjunto dos seus *múltiplos*. Este conjunto é um *ideal* do anel de inteiros ($\mathcal{A} \subset R$ é um ideal se $x,\ y \in \mathcal{A} \Rightarrow x+y \in \mathcal{A}$ e $x \in \mathcal{A},\ y \in R \Rightarrow xy \in \mathcal{A}$), e a teoria de divisibilidade de Kummer pode ser completamente descrita em termos da *fatorização de ideais*. Esta versão da teoria é a mais "algébrica" (i.é, no espírito da álgebra abstrata) e a mais popular hoje, e é o que se estende por *teoria de números algébricos*.

A teoria trata de extensões finitas $K/\mathbb{Q}$ (chamadas *corpos de números algébricos*); o *anel de inteiros* de K é o anel $\mathcal{O}_K$ formado por elementos de K cujo polinômio mônico minimal sobre $\mathbb{Q}$ tem coeficientes em $\mathbb{Z}$. O problema fundamental da teoria é descrever como os primos $p \in \mathbb{Z}$ se decompõem em $\mathcal{O}_K$, isto é, descrever a decomposição do ideal $p \cdot \mathcal{O}_K$ como produto de ideais primos. Idealmente, esta descrição deveria ser feita em termos de congruências em $\mathbb{Z}$, mas este objetivo só foi conseguido, até agora, em casos muitos especiais (por exemplo, quando o grupo de Galois de $K/\mathbb{Q}$ é abeliano). Este permanece num objetivo central da teoria, não só no caso básico de extensões $K/\mathbb{Q}$ como também no caso de extensões mais gerais L/K.

Em tempos mais recentes, muitas outras idéias frutíferas foram introduzidas na teoria: métodos analíticos, a idéia de considerar os vários completamentos dos corpos de números algébricos, métodos cohomológicos, e até mesmo a analogia entre a teoria de números algébricos e a teoria de curvas algébricas notada por Weil e desenvolvida recentemente por Arakelov e outros. Todos estes métodos trouxeram contribuições importantes, e são parte essencial da "caixa de ferramentas" do teorista de números.

Para um livro introdutório, esta multiplicidade de métodos e idéias representa uma dificuldade grande. Basicamente, é preciso optar entre uma exposição eclética e uma exposição seguindo uma linha consistentemente; no segundo caso, ainda resta a questão de definir qual a linha a seguir. A linha eclética é mais difícil, e poucos autores a adotam (Lang é o melhor exemplo). Entre os livros de tendência definida, há os que usam a teoria de valorizações (Hasse, Weiss), os que usam o método local-global (Cassells e Fröhlich) e os que usam método algébrico, da teoria de ideais. É este último

método que Otto Endler usa em seu livro *Teoria dos Números Algébricos*.

O livro de Endler contém uma exposição da teoria básica sob um enfoque estritamente algébrico. Em certos momentos, o livro assume mesmo o aspecto de um livro de álgebra comutativa, já que muitos dos teoremas são tratados sob hipóteses mais gerais do que seria necessário. Por exemplo, as propriedades básicas dos anéis de inteiros algébricos são discutidas em um capítulo sobre *Anéis Noetherianos e Domínios de Dedekind*. O principal risco que se corre ao escolher este modo de tratar o tema é o de tornar a exposição muito lenta (já que o caso geral é freqüentemente mais difícil). Este perigo é habilmente evitado no livro de Endler, em que a generalidade é procurada apenas até o ponto em que não prejudica a exposição. Desta forma, em cerca de duzentas páginas o autor apresenta todos os resultados básicos sobre a decomposição de primos em anéis de números algébricos (incluindo alguma coisa sobre extensões galoisianas e grupos de ramificação), e os dois teoremas mais importantes sobre a estrutura desses anéis: a finitude do número de classes e o teorema das unidades de Dirichlet (que o autor chama de *teorema dos invertíveis*). Para este último, a autor inclui as idéias básicas de geometria de números.

Como aplicação, o autor estuda a aritmética dos corpos quadráticos e dos corpos ciclotômicos, obtendo descrições da decomposição de primos em cada caso. No caso dos corpos quadráticos, trata-se do *teorema de reciprocidade quadrática*; a demonstração dada é a que se encontra na maioria dos livros elementares, apesar do autor ter à mão os elementos para uma demonstração mais elegante. O tratamento dos corpos quadráticos inclui a consideração de ordens não-maximais, e o teorema das unidades é provado em suficiente generalidade para incluir esse caso.

Ficam de fora, entretanto, vários temas básicos, principalmente os que requerem métodos analíticos. As somas de Gauss não são discutidas, o que evita a inclusão do teorema de Stickelberger sobre corpos ciclotômicos. As funções L e zeta não são mencionadas, nem os completamentos p-ádicos. Estes são temas que o aluno interessado em teoria de números terá que aprender para poder continuar na teoria (por exemplo, em direção à teoria

de corpos de classe); os livros de Lang e de Cassells e Fröhlich parecem as fontes naturais para esta continuação do estudo.

Dentro daquilo a que o autor se propõe, o livro faz um trabalho exemplar, dando ao interessado um ponto de partida sólido na teoria algébrica dos corpos de números. Os muitos exercícios incluídos completam o trabalho, que deverá ser útil à próxima geração de teoristas de números brasileiros.

Deve-se, finalmente, fazer alguns comentários sobre a produção do livro. A capa é bastante bem feita, atraente e significativa. A tipografia é funcional, apesar de certas esquisitices quanto ao uso de pontos para indicar multiplicação: o livro usa $\alpha \cdot R$ sistematicamente onde se esperaria αR, produzindo expressões como $\mathbb{Z}/p \cdot \mathbb{Z}$ para $\mathbb{Z}/p\mathbb{Z}$ e $R + \alpha \cdot R$ para $R + \alpha R$. O uso de I e J no mesmo contexto (veja, por exemplo, na página 96: "denotaremos... por I (respectivamente J)...") também não ajuda muito o leitor. A revisão é bem feita, deixando poucos erros de impressão.

No todo, o livro representa uma ótima contribuição à literatura matemática no Brasil, e pode ser recomendado a estudantes interessados em teoria de números.