Polinômios e Computação Algébrica

S. C. Coutinho
Universidade Federal do Rio de Janeiro

“What shall I learn of rings or rings of me? I cherish them, I study them, early and late I have an eye on them; and this is my day’s work”.

Para Martin Holland

Prefácio

Este livro originou-se em notas de aula escritas para um curso sobre demonstração automática de teoremas oferecido na Primeira Bienal de Sociedade Brasileira de Matemática, que realizou-se na Universidade Federal de Minas Gerais em 2002. Posteriormente, as mesmas notas foram utilizadas como texto para a disciplina eletiva de computação algébrica do curso de Ciência da Computação da Universidade Federal do Rio de Janeiro. Como os alunos da computação têm pouco conhecimento de álgebra, o curso deveria cobrir, além dos tópicos de computação algébrica, as noções básicas sobre anéis e ideais.

O resultado é um livro híbrido: uma introdução à álgebra no velho estilo dos séculos XVIII e XIX, em que a ênfase é sobre o que se pode calcular e como fazê-lo, ao invés de ser apenas uma discussão abstrata sobre estruturas. Mas há mais. A maior parte dos livros que adotam um caminho semelhante enxertam os tópicos tradicionais nas ementas usuais, em que a ênfase é sobre polinômios em *uma indeterminada* e extensões de corpos. Neste livro preferi adotar como coração do texto os polinômios em *várias indeterminadas* e o método das bases de Gröbner, que usamos para calcular com tais polinômios.

Há duas razões para esta escolha de um caminho alternativo. A primeira é que a principal aplicação destas técnicas é em geometria algébrica, uma da minhas áreas preferidas na matemática e que queria poder apresentar aos alunos de computação. A segunda é que isto abriria as portas para aplicações interessantes e fáceis de motivar, como programação inteira e técnicas automáticas para demonstração de teoremas de geometria plana e para o cálculo de integrais de funções elementares.

O livro se inicia com um capítulo em que defrontamos com o momento, no século XVII, em que álgebra e geometria se combinaram para dar origem à *Geometrie*, publicada por Descartes como adendo ao seu famoso *Discurso do Método*, do qual todos conhecemos a idéia crucial resumida no notório *penso, logo existo*. Esta introdução à geometria analítica, com forte sabor histórico, nos conduz a um método para demonstrar algebricamente teoremas da geometria elementar.

O problema é que, apesar de bastante geral, o método padece de sérios problemas na aplicação, porque frequentemente conduz a cáculos muito complicados. Daí a idéia de automatizar estes cálculos. Mas, para isto, precisamos primeiramente descobrir os algoritmos corretos que devem ser implementados no computador. Nos capítulos de 2 a 5 desenvolvemos a teoria necessária para

descrever e provar estes algoritmos. Desta forma, ao longo do caminho, introduzimos todas as noções necessárias sobre anéis e ideais. Contudo, ao contrário do curso tradicional, em que a ênfase é em resultados abstratos e que tem por principal exemplo os polinômios em uma variável e seus anéis quocientes, o principal exemplo neste livro são os polinômios em várias indeterminadas, sua tradução geométrica, e vários métodos explícitos para calculá-los. Assim, aos capítulos 2 e 3, de natureza mais conceitual, seguem-se dois capítulos cujo objetivo é descrever os principais algoritmos do livro: o algoritmo de divisão em várias indeterminadas e o algoritmo de bases de Gröbner devido a Bruno Buchberger.

A partir do capítulo 6 retornamos às aplicações. Mais precisamente, este capítulo formaliza o método de demonstração automática de teoremas de geometria plana esboçado no capítulo 1 e que remonta a Descartes. Para isto, usamos os algoritmos estudados dos capítulos 4 e 5. No capítulo 7 discutimos como as bases de Gröbner podem ser utilizadas para resolver problemas de computação inteira, uma área cujos algoritmos têm um custo notoriamente alto. Os capítulos 8 e 9 complementam alguns tópicos da teoria deixados de fora. Neles aplicamos as bases de Gröbner para estudar problemas de natureza aritmética (teoria de corpos) e geométrica (conjuntos algébricos). O último capítulo aplica quase tudo que aprendemos antes (e mais!) ao desenvolvimento de procedimentos para o cálculo exato das integrais de funções racionais: um dos exemplo mais importantes e menos estudados entre as integrais que aprendemos a determinar no curso de cálculo.

A quantidade de material apresentada neste livro é grande demais para que possa ser coberta com o devido cuidado em um semestre. Na disciplina eletiva a que me referi anteriormente, costumo apresentar em detalhes os capítulos 1 a 6 e deixar algumas das aplicações para os alunos implementarem em trabalhos de programação. Já um segundo curso de álgebra para alunos de matemática poderia consistir destes mesmos seis capítulos aos quais se acrescentaria o capítulo 8. Na verdade, muitas das aplicações de capítulos posteriores podem ser estudadas antes mesmo da introdução das bases de Gröbner. Este é o caso, por exemplo, do algoritmo de Hermite para o cálculo da parte racional da integral de uma função racional. Para descrever e provar este algoritmo precisamos apenas do algoritmo euclidiano estendido que já aparece no capítulo 2.

Todo livro de computação algébrica precisa confrontar-se com a questão do sistema no qual pressupõe-se que o leitor vá programar os vários algoritmos, se assim o desejar. Minha decisão foi tornar o livro independente de qualquer sistema, mas descrever os algoritmos em uma sintaxe próxima a de um dos meus sistemas favoritos, o `Axiom`. Este é um, dos dois sistemas de computação algébrica em domínio público, que costumo utilizar; sendo o outro o `Singular`, que contém algumas das melhores implementações atuais dos algoritmos aqui descritos. Escolhi adotar a sintaxe do `Axiom` porque se trata de um sistema menos especializado que o `Singular`, o que o torna mais atrativo para os estudantes. Além disso, este sistema merece ser mais conhecido e

divulgado no Brasil e esta é uma ótima oportunidade de fazer esta propaganda. Detalhes sobre como baixar e instalar estes sistemas, ambos amplamente documentados, podem ser encontrados no apêndice 2.

Gostaria de agradecer a todos os que, de uma forma ou de outra cooperaram para que este livro fosse escrito. Começo por todas aquelas pessoas que trabalharam no desenvolvimento dos programas de domínio público, listados adiante, que foram utilizados na confecção deste livro:

- `Axiom`;
- `Singular`;
- `MikTeX`;
- `TeXnicCenter`;
- `R. e C.`;
- `winplot`;

sem esquecer o MACTUTOR HISTORY OF MATHEMATICS ARCHIVE. Com Israel Vainsencher aprendi o que eram bases de Gröbner em um curso na XIII Escola de Álgebra de Campinas em julho de 1994, cujo texto pode ser obtido em [**13**].

Papel não menos importante foi desempenhado pelos alunos que assistiram às várias versões deste curso. Gostaria de agradecer especialmente a Bruno F. M. Ribeiro, Luiz Menaschè Schechter e Rodrigo Montenegro de Oliveira, com os quais aprendi mais do que lhes ensinei e a Alexandre Ferreira Sardinha de Mattos e Ana Alice Pacheco Monteiro pelas sugestões de correcões ao texto. Finalmente, agradeço a ???? que leram o texto e ofereceram sugestões e correções.

Rio de Janeiro, 30 de julho de 2009

Sumário

CAPíTULO 1

Introdução

Neste capítulo contamos um pouco da história por trás das ideias matemáticas que norteiam este livro, que são uma combinação de álgebra com geometria, tendo o computador como um tempero adicional. Ao longo do capítulo faremos usos de algumas noções básicas bem conhecidas sobre curvas, sobre as quais você deve ter aprendido em um curso de cálculo ou álgebra linear. De qualquer forma, uma primeira leitura impressionística deste capítulo é mais que suficiente para orientá-lo quanto ao conteúdo do livro. Quase tudo o que usamos aqui será tratado no corpo do texto de forma detalhada, de modo que você pode voltar e reler o capítulo mais adiante para poder saborear os detalhes que lhe tenham escapado em uma primeira leitura.

1. Descartes

No contexto da geometria plana, a palavra *demonstração* costuma suscitar lembranças de argumentos que utilizam construções geométricas simples e resultados relativos à congruência ou semelhança de triângulos. Na verdade, estas demonstrações remontam aos *Elementos*, um compêndio em 13 livros (ou capítulos) escrito por volta de 300 a.C. pelo matemático grego Euclides, que vivia na cidade de Alexandria. O estilo adotado por Euclides em sua obra tornou-se o método, por excelência, da matemática moderna. Tomando por base um pequeno conjunto de definições, axiomas e postulados, que supostamente descreveriam verdades fundamentais óbvias, Euclides explora as propriedades dos triângulos, quadriláteros, círculos e outras figuras geométricas. Cada resultado é enunciado e provado usando apenas os axiomas e postulados, além de outros resultados já demonstrados anteriormente (ou pelo menos é isso que Euclides nos quer fazer crer).

Apesar dos *Elementos* não serem o único, nem o mais importante, livro da matemática grega que chegou até nós, ele serve como uma espécie de referência para o que a matemática representava na antiga Grécia. Na verdade, pouco do que há nos *Elementos* é devido ao próprio Euclides, já que o livro foi escrito como uma espécie de repositório sistemático da matemática da época. O impacto deste livro pode ser sentido pelo fato de que, até meados do século XX, estudar geometria na escola secundária significava estudar os *Elementos* ou alguma obra didática claramente derivada dele. O escritor inglês E. M. Forster expressa isso muito bem em seu guia da cidade de Alexandria. Ao apresentar Euclides, ele comenta:

> Nada sabemos dele: para dizer a verdade, hoje o consideramos mais como um ramo do saber do que como um homem.

O estilo de geometria praticado por Euclides é conhecido hoje em dia como sintético. O termo é usado como contraponto ao método de coordenadas, ou analítico, inventado no século XVII. Apesar das importantes contribuições de Pierre de Fermat a este método, sua criação se acha indelevelmente ligado ao nome de René Descartes. Hoje em dia, Descartes é conhecido sobretudo como filósofo, o "Pai da Filosofia Moderna" e autor do *Discurso do Método*. Quem não ouviu falar do seu *penso, logo existo*? Entretanto, no século XVII, ainda havia pouca diferença entre a filosofia e o que hoje chamamos de ciência, e Descartes foi um dos mais importantes matemáticos e cientistas de sua época.

Descartes nasceu em 1596 na França, em uma cidade que então se chamava La Haye en Touraine, e que agora é conhecida como Descartes, em sua homenagem. Tendo perdido a mãe quando tinha apenas um ano de vida, Descartes foi criado pelo pai, que era juiz na Alta Corte de Justiça. Aos onze anos ingressou no Colégio Real Henry-Le-Grand que, segundo o próprio Descartes, era uma das mais famosas escolas européias da época. Tendo completado seus estudos no colégio, frequentou a Universidade de Poitiers, onde obteve o grau de bacharel em direito, como desejava seu pai. Entretanto, nunca exerceu esta profissão. Sua renda provinha de aplicações que fez com os recursos que obtivera da venda de uma propriedade em sua cidade natal e seu tempo era empregado estudando e escrevendo. Descartes morou boa parte da vida Holanda mas morreu na Suécia em 1650, para onde havia sido atraído pela rainha Cristina que o queria como seu preceptor.

Seus estudos de filosofia em Henry-Le-Grand não lhe deixaram uma impressão muito positiva. Contudo, como nos diz na primeira parte do famoso *Discurso do Método para Bem Conduzir a Razão*,

> sempre tive um enorme desejo de aprender a diferenciar o verdadeiro do falso, para ver claramente minhas ações e caminhar com segurança nesta vida.

Mas, continua,

> [a] verdade é que, ao limitar-me a observar os costumes dos outros homens, pouco encontrava que me satisfizesse, pois percebia neles quase tanta diversidade como a que notara anteriormente entre as opiniões dos filósofos. De forma que o maior proveito que daí tirei foi que, vendo uma quantidade de coisas que, apesar de nos parecerem muito extravagantes e ridículas, são comumente recebidas e aprovadas por outros grandes povos, aprendi a não acreditar com demasiada convicção em nada do que me havia sido inculcado só pelo exemplo e pelo hábito; e, dessa maneira, pouco a pouco, livrei-me de muitos enganos que

> ofuscam a nossa razão e nos tornar menos capazes de ouvir a razão.

Existem inúmeras traduções para o português do *Discurso*. A tradução usada aqui foi adaptada de [**22**].

O *método* ao qual se refere o título do discurso tinha quatro regras básicas:

Regra 1: nunca aceitar algo como verdadeiro algo que não conhecesse claramente como tal;

Regra 2: repartir cada dificuldade analisada em tantas partes quantas possíveis e necessárias para melhor resolvê-las;

Regra 3: ordenar os pensamentos de modo a começar pelos objetos mais simples e fáceis de conhecer e elevar-se, pouco a pouco, até os mais complexos;

Regra 4: em tudo fazer revisões gerais e cuidadosas de modo a certificar-se de nada omitir.

A inspiração para este método vinha da geometria:

> Essas longas séries de razões, todas simples e fáceis, que os geômetras costumam utilizar para chegar às suas mais difíceis demonstrações, tinham-me dado a oportunidade de imaginar que todas as coisas que pudessem ser conhecidas pelos homens seguem-se umas às outras do mesmo modo e que, uma vez que nos abstenhamos apenas de aceitar por verdadeira qualquer uma que não o seja, e que observemos sempre a ordem necessária para deduzi-las umas das outras, não pode existir nenhuma delas tão afastada a que não se chegue no final, nem tão escondida que não se descubra.

De fato, quando foi publicado em 1637 o *Discurso* veio acompanhado de três outros livros: os *Meteoros*, sobre fenômenos atmosféricos; a *Dióptrica*, sobre fenômenos ópticos; e a *Geometria*. Neles, Descartes aplicava seu método a cada uma destas áreas, ilustrando seu poder na solução de problemas que escapavam a seus contemporâneos. Na próxima seção analisaremos a *Geometria*, descrevendo, em linhas gerais, suas principais características.

2. A Geometria: livro primeiro

Talvez seja melhor começar dizendo o que a *Geometria* de Descartes não contém: nela não encontraremos nem a expressão *geometria analítica*, nem o desenvolvimento sistemático do método de coordenadas que costumamos associar a esta expressão; ambos só foram introduzidos no século XVIII. Na verdade a *Geometria* começa de um tanto bombástica:

> Todos os problemas de geometria se podem facilmente reduzir a tais termos que não há necessidade de conhecer mais que o comprimento de algumas linhas retas para os construir.

Facilmente? Bem, é Descartes falando. Note também que ele fala em *construir*, e não em *resolver* o problema. De fato, para Descartes, a meta da geometria é chegar a uma figura, uma imagem: uma curva é uma linha (ainda que ideal) traçada no papel. Assim, a equação é um meio de determinar as propriedades de uma figura e não um fim. Mas continuemos a ler:

> E, como toda a aritmética se compõe de apenas quatro ou cinco operações, que são a adição, a subtração, a multiplicação, a divisão e a extração de raízes, que podemos tomar por uma espécie de divisão: assim na geometria, nada há a fazer no que toca as linhas que procuramos senão somá-las ou subtraí-las; ou então, tomando uma que chamarei de unidade para relacioná-la mais diretamente aos números, e que em geral pode ser escolhida arbitrariamente, e tendo sido dadas duas outras linhas, encontrar uma quarta, que estará para uma das linhas dadas, como a outra está para a unidade, que é o mesmo que multiplicá-las.

Embora ele continue explicando quais são os equivalentes da divisão e da extração de raízes, vamos interrompê-lo aqui. O que exatamente Descartes está propondo como equivalente da multiplicação e qual a construção geométrica que a realiza?

Digamos que são dados dois segmentos de retas BD e BC que desejamos multiplicar. Estas são as *linhas* na terminologia da *Geometria*. Escolha um segmento AB de comprimento unitário e sejam ℓ_1 e ℓ_2 os comprimentos de BC e BD, respectivamente. A maneira como Descartes propõe-se a determinar o produto $\ell_1\ell_2$ consiste em calcular o número p que satisfaz a proporção

$$\frac{p}{\ell_1} = \frac{\ell_2}{1}. \tag{1}$$

Note que disto decorre, imediatamente, que $p = \ell_1\ell_2$. Para achar um segmento de comprimento p, Descartes propõe a construção ilustrada na figura 1.

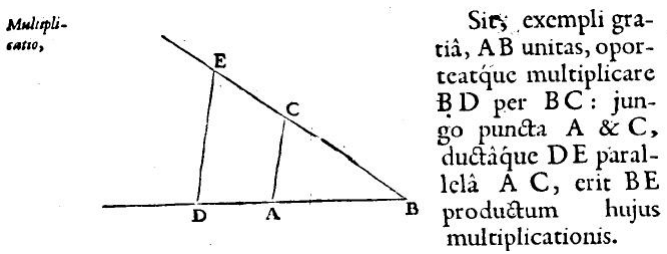


FIGURA 1. Multiplicando segmentos

O texto latino ao lado da figura nos diz como proceder. Depois de definir os segmentos BC e BD e a unidade AB exatamente como fizemos acima, Descartes explica que, para multiplicar BC por BD,

> devo apenas ligar os pontos A e C e desenhar DE paralela a AC; então BE é o produto de BC por BD.

A equação (1) é consequência direta da semelhança entre os triângulos BAC e BDE da figura 1.

Para entender a importância desta construção, devemos lembrar que, naquele momento do século XVII persistia uma distinção entre número e magnitude, herdada dos matemáticos da Grécia antiga. Assim, por *número* entendiam-se os nossos inteiros e frações; já uma *magnitude* era o comprimento de um segmento, uma área ou um volume. Na verdade, como o uso de Descartes no trecho acima sugere, a magnitude *era* um segmento, ou um espaço delimitado do plano ou do espaço. Em outras palavras, ainda não havia uma noção de número real, que permitisse representar um comprimento em pé de igualdade com uma fração.

A necessidade de pensar uma magnitude como um objeto geométrico cria vários problemas. Por exemplo, para construir uma figura plana cuja área é o dobro da de um quadrado dado basta construir um retângulo pela justaposição de dois quadrados iguais ao que foi dado. Note que podemos fazer isto sem jamais escolher uma unidade de medida! É exatamente nisto que Descartes rompe com a geometria dos antigos e mesmo com a de contemporâneos seus como Fermat. Tendo fixado uma unidade de medida, Descartes pode agora representar um produto, que até então era considerado um retângulo, como apenas mais um segmento de reta.

Na verdade a *Geometria* é o mais antigo livro de matemática que conseguimos ler sem ter maiores dificuldades com a notação ou a terminologia. Apesar disso, não se trata de uma leitura fácil. Mestre consumado da prosa clara, Descartes escreveu este livro de maneira deliberadamente obscura pois, como disse a um correspondente,

> eu havia previsto que certas pessoas, que se vangloriam tudo saber, não teriam deixado de dizer que eu nada havia escrito que eles já não conhecessem, se houvesse escrito de maneira suficientemente compreensível para eles.

A outro correspondente ele sugere

> acompanhar todos os cálculos, que podem a princípio parecer difíceis, com a pena [caneta] na mão

com o que deve acabar por acostumar-se a eles "depois de alguns dias". Ele também sugere passar do primeiro ao terceiro livro, pulando o segundo em uma primeira leitura.

Para enteder melhor o porquê deste último comentário de Descartes precisamos descrever em linhas gerais o conteúdo dos livros. O *Livro I* começa, como vimos, com uma explicação de como calcular com segmentos como se fossem números. Isto é seguido de uma explicação de como formular questões de geometria em termos de equações, que é ilustrada em um problema específico, que discutiremos na seção 4. O *Livro III* apresenta métodos para a resolução de equações polinomiais de uma variável pela interseção de curvas.

O *Livro II* que, conforme vimos, o próprio Descartes considera o mais difícil, trata de várias curvas e de sua classificação, questões que estudaremos na seção 5.

Lembrando que a *Geometria* foi escrita como propaganda do poder de seu método, e de sua intenção de torná-la deliberadamente obscura, não é de surpreender que os problemas lá resolvidos sejam já bastante complexos. Entretanto, seguindo o conselho do próprio Descartes em sua *Regra 4*, começaremos analisando alguns problemas bastante simples e fáceis e só então, pouco a pouco, passaremos a outros mais complexos.

3. Diagonais de um retângulo

Nesta seção examinaremos uma bem conhecida propriedade elementar das diagonais de um retângulo. Mais precisamente, provaremos o seguinte teorema da geometria elementar.

TEOREMA DAS DIAGONAIS. *As diagonais de um retângulo se intersectam no ponto médio das duas diagonais.*

Como desejamos resolver este problema usando métodos analíticos, começaremos por estabelecer o sistema de coordenadas. Na verdade Descartes nunca usa um sistema de coordenadas formado por dois eixos, essencialmente simétricos; esta novidade foi introduzida apenas no *Lieux géométriques*, publicado por Philippe de La Hire em 1679. Como desde então ela se tornou padrão, vamos adotá-las ao longo de todo este livro. Assim, todos os sistema de eixos que utilizarmos serão ortogonais. Como temos toda liberdade de pôr o sistema onde e como quisermos, faremos os eixos coincidirem com dois dos lados do retângulo, como ilustrado na figura 2.

Observe que posicionamos o ponto B nas coordenadas $(1, 0)$. À primeira vista pode parecer que com isto estaremos restringindo nossa demonstração aos retângulos cuja base tem comprimento 1. Na verdade, a demonstração será inteiramente geral porque, como o próprio Descartes já observara na primeira página da *Geometria*, a unidade "pode ser escolhida arbitrariamente". O que fizemos foi apenas escolher a escala das coordenadas de modo que o ponto B esteja a uma distância igual a 1 da origem. Mas, se é este o caso, por que chamamos de h a altura do retângulo? Por que não escolher a escala do eixo vertical de modo que a altura também seja 1? De fato podemos fazer isto, contudo com isto estaríamos escolhendo escalas diferentes para o eixo horizontal e vertical. Além desta não ser a convenção usual, tornaria mais difícil identificar com que tipo de retângulo estamos trabalhando: todos pareceriam quadrados, o que pode não ser uma boa ideia.

Nossa primeira meta é determinar as coordenadas do ponto P que está na interseção das diagonais do retângulo. Chamando de (x, y) as coordenadas deste ponto, queremos escrevê-las em função das coordenadas de A, B e C. Em primeiro lugar, temos que A, P e C estão alinhados. Isto significa que as retas por A e P, e por P e B têm a mesma inclinção. Mas a inclinação da reta

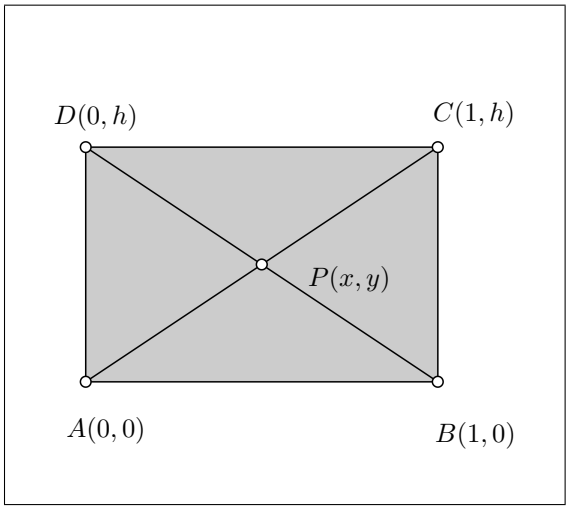


FIGURA 2. As diagonais de um retângulo

por A e P é igual a

$$\frac{y-0}{x-0}$$

e a da reta por P e B é igual a

$$\frac{h-y}{1-x}.$$

Igualando-as, obtemos

$$\frac{y-0}{x-0} = \frac{h-y}{1-x}.$$

De onde podemos concluir que

$$x(h-y) = y(1-x); \text{ isto é } x(h-y) - y(1-x) = 0.$$

Cancelando xy, resta

$$xh - y = 0.$$

Procedendo de maneira semelhante para a outra diagonal, temos que B, P e D estão alinhados. Igualando as inclinações das retas BP com PD, obtemos

$$\frac{y-0}{x-1} = \frac{h-y}{0-x};$$

donde concluímos que

$$xh + y - h = 0.$$

Começaremos analisando o caso em que o retângulo é um quadrado, que corresponde a $h = 1$. Neste caso, as duas equações são

$$x - y = x + y - 1 = 0.$$

Trata-se de um sistema linear e, ao resolvê-lo, verificamos que $x = 1/2$ e que $y = 1/2$. Desta forma, $P = (1/2, 1/2)$. Isto significa que as projeções

horizontais e verticais de P caem no meio dos lados do quadrado. Em outras palavras, P é o ponto médio das diagonais. Outra maneira de verificar isto consiste em calcular as distâncias entre A e P e entre P e C e mostrar que coincidem. Mas a distância entre A e P é

$$\sqrt{x^2+y^2} = \sqrt{\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2}$$

e a distância entre P e C é

$$\sqrt{(1-x)^2+(1-y)^2} = \sqrt{\left(1-\frac{1}{2}\right)^2 + \left(1-\frac{1}{2}\right)^2}$$

de modo que ambas são iguais a $\sqrt{1/2}$ e o ponto está mesmo no meio desta diagonal. O cálculo referente à outra diagonal é análogo e fica por sua conta.

Passando agora ao caso geral, as equações são

$$\begin{aligned} xh - y &= 0 \\ xh + y - h &= 0. \end{aligned}$$

Observe que, estritamente falando, estas não são mais equações lineares, uma vez que h agora também é uma variável. Contudo, podemos fazer de conta que escolhemos uma altura fixa para o retângulo que estamos considerando, de modo que h pode ser encarado como uma constante não nula. Isto nos permite resolver o sistema de equações lineares em x e y. Substituindo o valor de y obtido da primeira equação na segunda,

$$2xh - h = 0, \text{ donde } x = 1/2;$$

assim,

$$y = xh = h/2$$

e P tem coordenadas $(1/2, h/2)$, de modo que provamos que é mesmo o ponto médio das diagonais, mesmo quando o retângulo é completamente geral.

Nosso primeiro exemplo foi bastante simples, porque o objetivo era lhe dar uma idéia de como as coisas funcionam sem nos imiscuir em maiores complicações de natureza algábrica. O próximo exemplo já admite um tratamento algébrico mais elaborado.

4. O problema de Papus

A primeira pergunta que você deve estar se fazendo é quem ou o quê foi esse tal de Papus. A resposta é que foi um matemático de língua grega que viveu em Alexandria por volta de 300 d. C. e escreveu um tratado em oito livros conhecido como *A coleção*, no sétimo dos quais, nos diz Descartes,

> depois de devotar algum espaço a enumerar tudo que havia sido escrito em geometria por aqueles que o precederam, ele fala enfim de uma questão que, segundo ele, nem Euclides, nem Apolônio, nem mais ninguém conseguiu resolver completamente.

Segue-se o enunciado do problema proposto por Papus, não no original grego, mas em uma tradução latina para que, Descartes nos diz em um comentário na margem do texto,

> todos possam entendê-lo com mais facilidade.

Antes de enunciar o problema, precisamos relembrar o que significa a expressão *lugar geométrico*, muito usada para definir curvas em geometria. Em uma primeira aproximação, um lugar geométrico é apenas um conjunto de pontos com uma propriedade comum. Assim uma circunferência é o lugar geométrico dos pontos que guardam a mesma distância de um ponto fixo, chamado de centro. Outro lugar geométrico bem conhecido é formado pelos pontos cuja distância a uma reta fixa (a diretriz) é igual à sua distância de um ponto também fixo (ou foco). Neste caso, a curva é uma parábola. De fato, os lugares geométricos estudados pelos gregos eram quase todos cônicas o que, como veremos, explica a dificuldade que tiveram em resolver o problema de Papus para lá dos casos mais elementares. Com esta definição estamos prontos para enunciar o problema.

PROBLEMA DE PAPUS. *Dadas $2t$ retas em um plano, determinar o lugar de um ponto C que se move de modo que o produto das distâncias de C a t delas seja proporcional ao produto das distâncias às outras t, sendo as distâncias medidas em ângulos dados relativamente às retas.*

Enunciamos o problema no caso em que a quantidade de retas é par; no caso em que é ímpar apenas escolhemos metade mais uma das retas para um dos termos da razão. Este problema desempenhou um papel importante na história da *Geometria* porque Descartes ficou muito impressionado com a facilidade com que conseguiu resolvê-lo usando os métodos que havia desenvolvido. Segundo Papus, o problema só havia pelos gregos antigos nos casos em que havia apenas três ou quatro retas. E a solução viera de Apolônio, o maior dos geômetras da antiguidade. Logo veremos porque Apolônio conseguiu resolver este problema, mas não aqueles em que havia mais retas. No início da *Geometria* Descartes descreve o método a ser utilizado para resolver este e outros problemas da seguinte forma

> [a]ssim, desejando resolver algum problema, devemos portanto considerá-lo como já resolvido e dar nomes a todas as linhas, que parecem necessárias para construí-lo, tanto aquelas que já são conhecidas, quanto as demais. Então, sem considerar nenhuma diferença entre as linhas conecidas e desconhecidas, devemos percorrer a dificuldade, segundo a ordem que mostra mais naturalmente de que forma dependem mutuamente umas das outras, até que tenhamos encontrado um meio de exprimir uma mesma quantidade de duas maneiras: ao que se dá o nome de uma equação; porque os termos de uma destas expressões [tomados conjuntamente] são iguais aos da outra.

A este método de imaginar o problema já resolvido e usar isto para inventar relações que levem à sua eventual solução os gregos chamavam de *análise*. Aliás, é o próprio Papus quem explica no mesmo livro 7 de seu tratado que a palavra *análise* é usada porque quer dizer "solução de trás para a frente"; veja [**37**, vol. ii, p. 400]. Isto explica também de onde vem o adjetivo *analítco* que a partir do século XVIII começou a ser associado aos métodos geométricos inventados por Descartes.

A seguir, veremos uma versão modernizada da solução de Descartes do problema que se aplica a qualquer quantidade de retas. Na verdade, a solução consiste apenas em obter uma fórmula explícita para a distância de um ponto genérico a uma reta dada, sendo a distância medida ao longo de um ângulo também dado, e não necessariamente ao longo da perpendicular.

Em nossa terminologia, a primeira coisa que Descartes ao descrever sua solução é escolher duas das retas dadas que ele vai usar como eixos, supondo que se cruzem em algum ponto. O caso em que todas as retas são paralelas tem que ser tratado separadamente. O problema é que com isto obtemos um sistema de eixos que não são necessariamente ortogonais. Para manter a convenção usual de que os eixos são perpendiculares, adaptaremos um pouco o argumento de Descartes sem, contudo, alterar a sua essência.

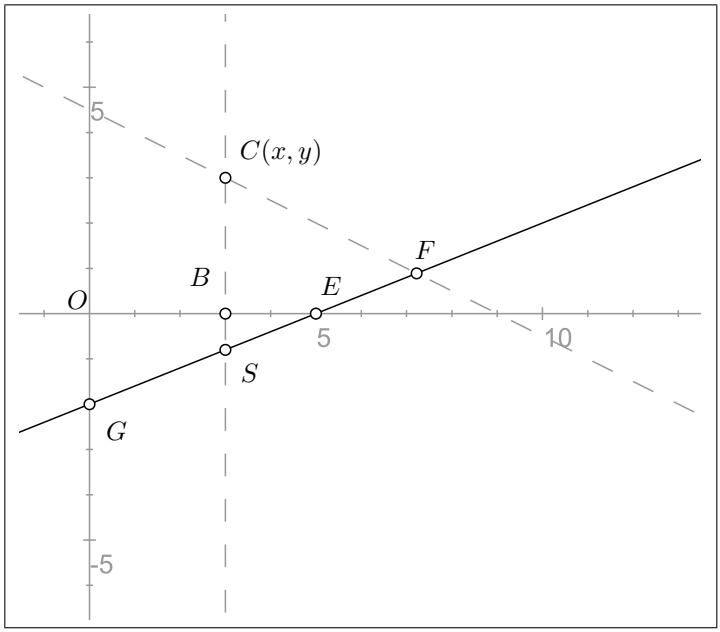


FIGURA 3. Uma das retas do problema de Papus

Tendo, então, fixado os eixos ortogonais em algum lugar do plano, e seguindo o método analítico de Descartes, devemos imaginar que $C = (x, y)$

é um ponto da curva que satisfaz as condições do problema. Seja EF uma das retas dadas. Por enquanto consideraremos apenas uma das retas, e suporemos que *não* é paralela ao eixo das abscissas, como na figura 3. O caso em que a reta é paralela a este eixo ficará por sua conta; veja exercício ???. Nosso objetivo é determinar a distância entre C e EF, medida segundo o ângulo α também dado, que na figura é representado por $\widehat{CFE}$.

Como o triângulo OGB fica completamente determinado pela reta EF, o número

$$k_1 = \frac{\overline{AE}}{\overline{AG}}$$

está completamente determinado pelos dados do problema. Mas os triângulos OGB e BSE são semelhantes, de modo que

$$\frac{\overline{AE}}{\overline{AG}} = \frac{\overline{BE}}{\overline{BS}}$$

e assim,

$$\overline{BS} = k_1 \overline{BE}.$$

Por outro lado,

$$\overline{BE} = \overline{OE} - \overline{OB} = \overline{OE} - y,$$

donde deduzimos que

$$\overline{BS} = k_1(\overline{OE} - x). \tag{2}$$

Passamos agora a analisar o triângulo CFS. Dois dos ângulos deste triângulo são conhecidos: $\widehat{CFE}$ porque é igual a α, que é um dos dados do problema, e $\widehat{BSE}$ porque é igual a $\widehat{AGE}$. Como quaisquer dois triângulos com dois ângulos iguais são semelhantes, isto significa que conhecemos a razão entre quaisquer dois lados de CFS. Com isto podemos supor

$$\frac{\overline{CS}}{\overline{CF}} = k_2,$$

em que k_2 é uma constante conhecida. Isto nos diz que a distância $\overline{CF}$ entre C e a reta EF segundo o ângulo $\widehat{CFE}$ dado é igual a

$$\overline{CF} = \frac{\overline{CS}}{k_2}.$$

Contudo,

$$\overline{CS} = \overline{CB} + \overline{BS} = y + \overline{BS}.$$

Combinando estas duas últimas equações com (2), obtemos

$$\overline{CF} = \frac{y + k_1(\overline{OE} - x)}{k_2}.$$

Como k_1, k_2 e $\overline{OE}$ são obtidos diretamente dos dados do problema, obtivemos uma fórmula para a distância desejada em termos das coordenadas de C. Resumindo, podemos dizer que provamos o seguinte:

dadas uma reta EF, um ponto C de coordenadas (x, y) e o ângulo $\alpha = \widehat{CFE}$, a distância de C a EF segundo o ângulo α é uma expressão linear em x e y cujos coeficientes dependem da reta e do ângulo dados.

Suponha, então que temos k retas $\ell_1, \ldots, \ell_k$ e k ângulos $\alpha_1, \ldots, \alpha_k$ e que distância à reta ℓ_j deve ser medida segundo o ângulo α_j.

Seja C um ponto da curva a ser determinada. Se C tem coordenadas (x, y), então a distância de C a ℓ_j ao longo de α_j é dada por

$$d_j = a_j x + b_j y + c_j,$$

em que a_j, b_j e c_j são constantes que dependem apenas de ℓ_j e de α_j. Portanto, o ponto C estará na curva definida pelo problema de Papus para k retas se, e somente se,

$$d_1 \cdots d_t = k_3 d_{t+1} \cdots d_k \tag{3}$$

em que k_3 é a constante de proporcionalidade entre os dois produtos de distâncias e $t = k/2$ ou $t = (k-1)/2$, dependendo se k é par ou ímpar.

Observe que o produto $d_1 \cdots d_t$ nos dá um polinômio de grau t nas variáveis x e y; já o polinômio $d_{t+1} \cdots d_k$ tem grau $k - t$. Em particular, tanto no caso em que há três retas, quanto no caso em que há quatro retas, a equação (3) tem grau dois e a curva correspondente é uma cônica, que pode ser identificada usando o método usual de diagonalização de matrizes que aprendemos no curso de álgebra linear; veja [**48**] por exemplo. Contudo, se a quantidade de retas é maior que quatro a curva solução do problema de Papus nunca dá uma cônica. Isto ajuda a entender porque Apolônio pôde resolver o problema "das três e quatro retas", ele era um especialista em cônicas e escreveu um tratado em oito livros sobre estas curvas.

5. A Geometria: livro segundo

Ao desenvolver seu método analítico, Descartes não desejava apenas obter uma técnica sistemática para resolver problemas ainda sem solução da geometria clássica. Ele esperava também estender a classe de problemas que poderiam ser abordados com estas técnicas. Por isso analisou de maneira bastante detalhada a forma como uma curva deveria ser definida para que continuasse sendo um objeto legítmimo de estudo pela geometria. De fato, embora os gregos houvessem estudado as cônicas em detalhes, como vimos na seção anterior, eles pouco sabiam sobre outras curvas mais complicadas. Entre as poucas que haviam considerado estavam a espiral e a quadratrix. A primeira foi tema de um livro de Arquimedes, a segunda foi usada para resolver o clássico problema da trisecção de um ângulo; isto é, construir um ângulo igual à terça parte de um ângulo dado. Na verdade, foi somente com a introdução de coordenadas por Descartes e Fermat, que a noção de lugar geométrico se expandiu para incluir uma variedade muito maior de curvas. Isto impediu os gregos de avançar na identificação das curvas que são solução do problema de Papus, porque não eram capazes de identificá-las como algo que já houvessem visto antes.

A discussão de novas variedades de curvas é um dos temas centrais da segunda parte da *Geometria*. Logo no início do Segundo Livro [**23**, p. 40 ff], Descartes observa que os gregos subdividiam as curvas em geométricas e mecânicas. Mas o critério usado para alocar curvas em uma ou outra classe não é claro. Certamente a razão não é que as segundas precisem de apetrechos mecânicos para produzi-las pois se fosse assim, então,

> para ser consistentes, deveríamos rejeitar pela mesma razão, círculos e retas; uma vez que para desenhá-las sobre o papel precisamos de um compasso e uma régua, que podemos também chamar de máquinas [**23**, p. 40-41].

Também não é verdade que outros instrumentos, ainda que mais complicados, sejam menos precisos que a régua e o compasso; afinal, precisão é ainda mais necessária em mecânica do que em geometria, como reconhece o próprio Descartes. O critério para acolher uma curva como parte da geometria, nos diz ele, é que sejamos capazes de raciocinar sobre elas de maneira exata. E isto, acrescenta, é possível mesmo em se tratando de curvas mais complicadas de descrever do que as cônicas tratadas na antiguidade. Descartes vai mais longe e propõe que, para tratar curvas mais complicadas, basta acrescentar às hipóteses usuais da geometria plana euclidiana a seguinte:

> duas ou mais linhas podem mover-se, uma sobre a outra, determinando outras curvas por sua interseção.

Um pouco adiante, depois de elaborar um pouco mais o mesmo argumento, ele conclui que

> não temos o direito de excluir as curvas mais complexas do que as simples, desde que possamos imaginar que sejam descritas por um movimento contínuo, ou por vários que sigam uns aos outros, desde que o último seja completamente determinado por aquelea que o precedem; pois, desta maneira, podemos sempre obter um conhecimento exato de sua magnitude [**23**, p. 42-43].

Como tudo isto ainda é um pouco vago, Descartes faz uma proposta concreta de uma maneira de desenhar tais curvas. A figura 4 representa a gravura original do instrumento que ele sugere utilizar para este fim.

A descrição que Descartes dá do instrumento é a seguinte:

> Considere as linhas AB, AD, AF, e assim por diante, que suporemos terem sido descritas com a ajuda de um instrumento YZ, que é composto de várias réguas conectadas de tal modo que quando a que está marcada com YZ for posta sobre a linha AN, podemos abrir e fechar o ângulo XYZ. Quando este ângulo estiver completamente fechado, os pontos B, C, D, F, G, H estarão todos juntos sobre o ponto A. À medida que o ângulo for sendo aberto, a régua BC, que é conectada em ângulo reto a YX no

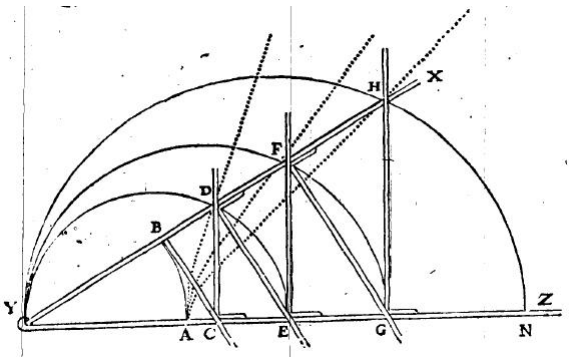


FIGURA 4. Esboçando curvas na Geometria de Descartes

> ponto B, empurra em direção a Z a régua CD que, por sua vez desliza sobre YZ sempre formando um ângulo reto. De maneira semelhante, CD empurra DE, que desliza ao longo de YX sempre paralela a BC; DE empurra EF; EF empurra FG; FG empurra GH, e assim por diante. Assim podemos imaginar uma infinidade de retas, cada uma das quais empurrando uma outra, metade das quais formam um ângulo reto com YX e a outra metade com YZ; [**23**, p. 46-47].

O ponto crítico desta parte do argumento surge na página seguinte:

> [...] mas para compreender em conjunto todas as curvas que existem na natureza e classificá-las por ordem em certos gêneros, não conheço nada melhor do que dizer que todo ponto daquelas [curvas] que chamamos de geométricas [...] têm necessariamente algum relação [bem definida] com os pontos de uma linha reta, e que esta relação pode ser expressa por meio de uma única equação. Se esta equação não contém termos superiores a um retângulo de duas quantidades desconhecidas [isto é, termos da forma xy] ou do quadrado de uma tal quantidade [isto é, termos da forma x^2 ou y^2] então a curva é do primeiro primeiro e mais simples dos gêneros, que contém apenas o círculo, a parábola, a hipérbole e a elipse; mas se a equação contém termos do terceiro ou quarto graus em uma ou ambas das quantidades indeterminadas (porque duas delas são necessárias para expressar a relação entre dois pontos), ela é do segundo; e se a equação contém um termo do quinto ou sexto grau em uma ou ambas as indeterminadas, a curva pertence ao terceiro gênero; e assim sucessivamente ao infinito, [**23**, p. 48-49].

Note que os *gêneros* de Descartes nada têm a ver com o uso moderno da palavra em geometria algébrica; eles nada mais são que classes de equações reunidas por terem graus semelhantes. Ao contrário do que acontecia nos outros trechos citados, no parágrafo anterior fica claro que Descartes está falando do algo que nós mesmos chamaríamos de *geometria analítica*—mas não ele, o termo foi usado pela primeira vez no século XVIII.

Vejamos como é possível obter equações para as curvas AB, AD e AF definidas pelo instrumento da figura 4. Situando a origem do sistema de coordenadas no ponto Y, com o eixo das abscissas ao longo de YZ, vemos que, ao aumentar o ângulo XYZ o ponto B descreve uma circunferência. Logo, $\overline{YA} = \overline{YB}$. Ajustando a escala ao longo de YZ podemos supor que o segmento $\overline{YA}$ tem comprimento unitário. Assim, AB corresponde a um arco da circunferência de equação $x^2 + y^2 = 1$. Passando agora à curva AD temos, pela semelhança dos triângulos retângulos YBC e YCD que

$$\frac{\overline{YD}}{\overline{YC}} = \frac{\overline{YC}}{\overline{YB}}. \tag{4}$$

Denotando $\overline{YC}$ por x e lembrando que $\overline{YB} = 1$,

$$\overline{YD} = x^2.$$

Contudo, pelo teorema de Pitágoras aplicado ao triângulo YCD,

$$\overline{YD}^2 = \overline{YC}^2 + \overline{CD}^2.$$

Se y for a ordenada de D, isto nos dá

$$x^4 = x^2 + y^2;$$

e temos a equação que descreve a curva AD.

Para achar a equação da curva AF começamos por renomear x e y como sendo as coordenadas de F. Procedendo como antes, a semelhança dos triângulos retângulos YEF e YDE nos dá

$$\frac{\overline{YF}}{\overline{YE}} = \frac{\overline{YE}}{\overline{YD}}.$$

donde

$$\overline{YD} = \frac{x^2}{\overline{YF}}, \tag{5}$$

pois $\overline{YE}$ é igual a abscissa x de F. Apelando, agora, para a semelhança entre YDE e YDC, obtemos

$$\frac{\overline{YE}}{\overline{YD}} = \frac{\overline{YD}}{\overline{YC}},$$

de forma que

$$\overline{YC} = \frac{\overline{YD}^2}{\overline{YE}}.$$

Contudo, (4) juntamente com $\overline{YF} = 1$ nos dá

$$\overline{YC}^2 = \overline{YD},$$

e combinando estas duas últimas fórmulas, concluímos que

$$\left(\frac{\overline{YD}^2}{\overline{YE}}\right)^2 = \overline{YD};$$

isto é,

$$\overline{YD}^3 = \overline{YE}^2.$$

Substituindo nesta fórmula o valor de $\overline{YD}$ obtido em (5) e lembrando que $\overline{YE} = x$,

$$\left(\frac{x^2}{\overline{YF}}\right)^3 = x^2.$$

que após os devidos cancelamentos nos dá

$$\overline{YF}^3 = x^4. \tag{6}$$

Resta apenas determinar $\overline{YF}$. Para oisto aplicamos o teorema de Pitágoras ao triângulo retângulo YEF, o que nos dá

$$\overline{YF} = \sqrt{x^2 + y^2}.$$

Com isto (6) torna-se

$$\sqrt{x^2 + y^2}^3 = x^4;$$

e, elevando ambos os membros ao quadrado chegamos a

$$(x^2 + y^2)^3 = x^8;$$

que é a equação desejada para a curva AF. Note que as equações obtidas nestes dois exemplos correspondem perfeitamente à descrição de Descartes no trecho da *Geometria* citado anteriormente. Isto é, são equações de grau superior a 2, expressas por uma única fórmula polinomial.

Na *Enciclopédia* de Diderot e D'Alembert, publicada nos anos 1780, lemos o seguinte resumo da opinião de Descartes no verbete *curvas mecânicas*:

> termo usado por Descartes para designar uma curva que não pode ser expressa por uma equação algébrica. Estas curvas são com isto postas em oposição às curvas geométricas ou algébricas.[...] M. Leibnitz & alguns outros as chamam de transcendentes em vez de mecânicas, e eles não concordam com a opinião de Descartes de que devemos excluí-las da geometria.

A terminologia de Leibniz continua sendo a que usamos atualmente. Assim, uma *curva algébrica* é aquela que pode ser descrita como o lugar dos pontos do plano que satisfazem uma dada equação polinomial. Em outras palavras, uma curva plana C é *algébrica* se existir um polinômio f nas variáveis x e y tal que

$$C = \mathcal{Z}(f) = \{p \in \mathbb{R}^2 | f(p) = 0\}.$$

Como veremos na seção 7 este é o primeiro exemplo de um *conjunto algébrico*, que é uma das noções chave deste livro. Contudo, existem curvas planas que

não podem ser escritas na forma acima; para um exemplo veja a seção 4 do capítulo 3.

É importante entender que, para Descartes, conhecer a equação de uma curva não era suficiente, deveríamos ser capazes de desenhá-la de maneira exata—pelo menos em princípio. Por isso, para ele os métodos algébricos eram, não um fim em si, mas um meio para entender melhor, e de maneira mais abrangente, a geometria das curvas planas. Daí a importância para Descartes de procedimentos mecânicos simples que tornassem possível esboçar a curva cuja equação havia obtido. Na verdade, Descartes acreditava que instrumentos como o da figura 4 seriam capazes de esboçar quaisquer curvas algébricas, fato que só viria a ser confirmado no século XIX por A. B. Kempe [**41**] que é mais conhecido hoje em dia por ter publicado em 1879 uma prova incorreta do *teorema das quatro cores* da teoria de grafos [**70**]. Como não é infrequente em matemática, foram as muitas e ricas idéias desta prova incorreta que levaram eventualmente à solução do problema em 1976 por Kenneth Appel e Wolfgang Haken—com a ajuda de um computador.

A menção de acoplamentos mecânicos pode parecer apenas uma curiosidade histórica, e assim o foi, por bastante tempo, mas não mais. Braços robóticos são exemplos de acoplamentos mecânicos e é importante saber qual a curva que a extremidade de um braço descreve ao movimentar-se. Este é um tema do qual não trataremos neste livro; veja [**51**] para mais detalhes.

6. As medianas de um triângulo

Nesta seção provaremos mais um teorema elementar da geometria plana usando o método de coordenadas. Entretanto, a natureza do problema nos leva a uma análise mais profunda do método analítico do que a que fizemos nos exemplos anteriores. O teorema é o seguinte.

TEOREMA DAS MEDIANAS. *As três medianas de um triângulo se encontram em um único ponto.*

Lembre-se que uma *mediana* de um triângulo é uma reta que une um vértice do triângulo à metade do lado oposto. É claro que duas medianas quaisquer de um triângulo se encontram em um ponto. O que é surpreendente é que a terceira mediana passe exatamente pelo mesmo ponto! Este ponto é conhecido como *baricentro*, ou centro de gravidade do triângulo.

Nossa estratégia para provar este teorema consiste em "determinar" o ponto onde duas medianas se encontram, e então provar que a terceira mediana passa pelo mesmo ponto. Na verdade, não temos como calcular exatamente as coordenadas do ponto de intersecção de duas medianas porque, afinal, não queremos mostrar que o resultado vale para um triângulo dado, mas sim para qualquer triângulo. Assim, "determinaremos" o ponto escrevendo as condições que tem que satisfazer para estar sobre estas duas medianas. Temos, então, que mostrar que a terceira mediana contém este mesmo ponto.

Como na seção anterior, escolheremos o sistema de coordenadas de modo que as equações que representam as hipóteses e a conclusão do teorema sejam

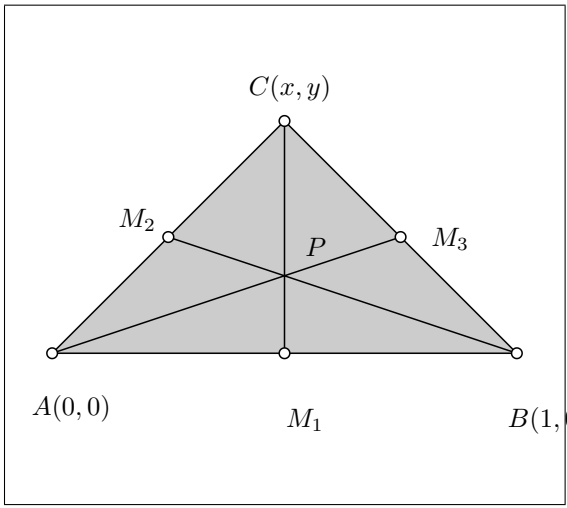


FIGURA 5. As medianas de um triângulo

as mais simples possíveis. Assim, fazemos a origem do sistema coincidir com um dos vértices do triângulo, de modo que um dos lados (a base) esteja sobre o eixo OX (do lado positivo do eixo). Além disso, podemos assumir que a escala foi escolhida de modo que a base do triângulo tenha comprimento 1. Vamos chamar os vértices do triângulo de A, B e C. De acordo com a figura 5 temos que

$$A = (0,0), \quad B = (1,0) \quad \text{e} \quad C = (x,y).$$

Assim, o ponto médio do lado AB tem coordenadas $M_1 = (1/2, 0)$, o ponto médio do lado AC tem coordenadas $M_2 = (x/2, y/2)$ e o ponto médio do lado BC tem coordenadas $M_3 = ((x+1)/2, y/2)$.

De posse destes dados podemos por em ação nossa estratégia. Seja P o ponto de intersecção das medianas que passam por A e por B; digamos que P tem coordenadas (u, v). Para determinar a equação que expressa o fato de P estar na mediana que passa por A basta igualar o coeficiente angular da reta por A e P com o coeficiente angular da reta por M_3 e A. Como ambas as retas têm o ponto A em comum, a igualdade dos coeficientes angulares garante que elas coincidem. Mas o coeficiente angular da reta por $A = (0,0)$ e $P = (u, v)$ é v/u, ao passo que o coeficiente angular da reta por A e M_3 é $y/(x+1)$. Igualando-os temos a condição para que P esteja na mediana que passa pelo vértice A, que é

$$\frac{v}{u} = \frac{y}{x+1}.$$

Eliminando os denominadores, podemos escrever esta mesma condição na forma

$$h_1 = 0, \quad \text{onde} \quad h_1 = vx + v - uy.$$

Procedendo de maneira análoga, expressamos a condição de que P pertença à mediana que passa pelo vértice B na forma

$$h_2 = 0, \quad \text{onde} \quad h_2 = vx - 2v - uy + y.$$

Portanto, se o ponto P pertence à intersecção das medianas pelos vértices A e B, então as equações $h_1 = h_2 = 0$ devem ser simultaneamente satisfeitas.

Por outro lado, o que queremos provar é que este ponto P também pertence à mediana que passa pelo vértice C. Mas esta última condição também se expressa como o anulamento de um polinômio

$$c = 2xv - v - 2uy + y,$$

que é obtido de modo análogo ao anterior. Precisamos mostrar que, se um ponto é zero comum de h_1 e h_2, então também é zero de c.

Uma maneira de fazer isto é supor que o vértice $C = (x, y)$ está fixo, de modo que x e y são constantes, cujos valores não conhecemos. A partir disso tentaremos calcular u e v. Sob estas hipóteses,

$$\begin{aligned} h_1 &= vx + v - uy = 0 \\ h_2 &= vx - 2v - uy + y \end{aligned}$$

é um sistema linear nas variáveis u e v. Como y é a altura do triângulo, certamente $y \neq 0$. Assim, podemos obter o valor de u a partir da primeira equação,

$$u = \frac{v(x+1)}{y}.$$

Substituindo isto na segunda equação

$$0 = vx - 2v - \frac{v(x+1)}{y}y + y = vx - 2v - v(x+1) + y,$$

donde $v = y/3$. Portanto,

$$P = \left(\frac{x+1}{3}, \frac{y}{3}\right).$$

Para saber se este ponto pertence à terceira mediana, basta substituí-lo na equação c. Isto nos dá,

$$(2x-1)\frac{y}{3} - 2\frac{x+1}{3}y + y = 0,$$

como desejávamos verificar.

Apesar deste procedimento ser inteiramente aceitável como uma demonstração geral, ele não é aplicável em teoremas mais complicados, que envolvam equações de grau maior que um. Por isso, apresentaremos uma solução alternativa, que envolve muito menos cálculos e pode ser generalizada para cobrir qualquer outro teorema. À primeira vista, este novo processo de demonstração pode parecer perfeito: mais geral e mais simples, o que podia ser melhor? Entretanto, o que é mais simples são os cálculos a serem realizados; este novo método faz demandas conceituais muito maiores em quem o utiliza.

Para aplicar este novo método, precisamos apenas verificar que

$$c = h_1 + h_2, \tag{7}$$

que é um cálculo quase imediato. Só que, desta vez, estamos considerando h_1, h_2 e c como polinômios nas quatro variáveis x y, u e v. Outra maneira de dizer isto é que estamos considerando os três polinômios como funções de $C = (x, y)$ e de $P = (u, v)$. Portanto, se P for um ponto na mediana de BC, então $h_1(C, P) = 0$, e se P for um ponto na mediana de AC, então $h_2(C, P) = 0$. Assim, o ponto P de interseção das medianas de AC e BC em um triângulo cujo vértice C tem coordenadas (x, y) fica completamente determinado pelas equações

$$h_1(C, P) = h_2(C, P) = 0. \tag{8}$$

Combinando isto com (7), verificamos que

$$c(C, P) = h_1(C, P) + h_2(C, P) = 0 + 0 = 0.$$

Isto nos diz que qualquer ponto P que

satisfaça (8), isto é, pertença às medianas AC e BC

também

satisfaz $c(C, P) = 0$, isto é, pertence à mediana por AB.

Como duas retas se intersectam em apenas um ponto, obtivemos uma demonstração do teorema das medianas.

7. O Método

Quando Descartes introduziu seus métodos analíticos em geometria, ele tinha uma intenção nada modesta. Os resultados dos matemáticos gregos não o impressionavam muito; "verdades pueris dedutivamente demonstradas com alguma ingenuidade" foi como se referiu a elas em certa ocasião. O que Descartes desejava era um método capaz de solucionar de maneira sistemática qualquer problema geométrico que encontrasse. É nesse espírito que analisaremos a segunda das duas soluções do problema das medianas. Nossa meta é generalizá-la para que possa ser aplicada para resolver de maneira sistemática muitos dos problemas da geometria euclidiana plana. Apesar de inspirada em Descartes, o tipo de estratégia que proporemos aqui só tornou-se possível depois que os espaços de dimensão maior que três foram introduzidos no século XIX. Só para que isto fique bem claro: muitas vezes precisaremos recorrer a espaços de dimensões *muito maior que três* embora o problema que queiramos resolver um problema *plana*.

Tanto no teorema das medianas, quanto no das diagonais, a primeira coisa que fizemos foi codificar as hipóteses e a conclusão do teorema como equações algébricas. Isto pode ser mais fácil ou mais difícil, dependendo das figuras geométricas a que se refere o teorema. Por enquanto admitiremos que sabemos efetuar esta codificação sem maior dificuldade, porque queremos tratar primeiro dos aspectos algébricos do problema, mas voltaremos à questão da codificação no capítulo 6.

É conveniente repassar o que fizemos na seção anterior. Começamos codificando o fato de P pertencer às medianas por A e por B como o anulamento simultâneo dos polinômios

$$h_1 = vx + v - uy \quad \text{e} \quad h_2 = vx - 2v - uy + y.$$

Entretanto, estes são polinômios em 4 variáveis, e o sistema $h_1 = h_2 = 0$ não determina um único ponto. O que eles fazem é estabelecer uma relação entre as coordenadas do ponto P, que pertence à interseção destas duas medianas, com as coordenadas do vértice C do triângulo. Isto ocorre porque *não estamos trabalhando com um triângulo específico*, pois queremos mostrar que o teorema vale *para qualquer triângulo*. Por isso, embora os vértices da base de nosso triângulo sejam $(0, 0)$ e $(1, 0)$, as coordenadas do terceiro vértice foram expressas na forma de variáveis (x, y) que podem assumir quaisquer valores que desejemos. Assim, dizer que o anulamento de h_1 e h_2 determina um ponto significa que, uma vez que tenham sido escolhidos valores x_0 e y_0 para x e y, o sistema

$$h_1(x_0, y_0, u, v) = h_2(x_0, y_0, u, v) = 0,$$

determina o ponto de intersecção das medianas por A e B no triângulo que tem vértice $C = (x_0, y_0)$.

Portanto, rigorosamente falando, o anulamento dos polinômios h_1 e h_2 não determina um ponto do plano, mas sim um conjunto $\mathcal{Z}(h_1, h_2)$ de pontos em um espaço de dimensão 4, cujas coordenadas são x, y, u e v. Por definição,

$$p_0 = (x_0, y_0, u_0, v_0) \in \mathcal{Z}(h_1, h_2)$$

se, e somente se

$$h_1(x_0, y_0, u_0, v_0) = h_2(x_0, y_0, u_0, v_0) = 0.$$

Portanto, levando em consideração a interpretação geométrica dos polinômios h_1 e h_2, podemos dizer que $p_0 \in \mathcal{Z}(h_1, h_2)$ significa que

> (u_0, v_0) são as coordenadas do ponto de intersecção das medianas por A e B do triângulo cujo vértice C tem coordenadas (x_0, y_0).

Contudo, o polinômio c que expressa a conclusão do teorema das medianas só se anula em p_0 se (u_0, v_0) pertence à mediana que passa por C. Portanto,

> provar que o teorema das medianas vale para todo triângulo significa mostrar que c se anula em todo ponto de $\mathcal{Z}(h_1, h_2)$.

Para sorte nossa, temos neste exemplo que $c = h_1 + h_2$. Deste modo

$$c(p_0) = h_1(p_0) + h_2(p_0) = 0,$$

pois

$$h_1(p_0) = h_2(p_0) = 0.$$

Filtrando tudo o que é contingente ao exemplo, verificamos que

> as hipóteses do teorema a ser demonstrado devem ser expressas sob a forma do anulamento de um conjunto (finito!) de polinômios $h_1, \ldots, h_t$ nas variáveis $x_1, \ldots, x_n$, ao passo que a conclusão do teorema corresponde ao anulamento de um outro polinômio em $x_1, \ldots, x_n$, que vamos chamar de c;

O teorema é verdadeiro se, e somente se,

c se anula em todo ponto em que cada um dos hs também se anula.

Para traduzir isto na linguagem de conjuntos, definimos o *conjunto algébrico*

$$\mathcal{Z}(h_1, \ldots, h_t) = \{p \in \mathbb{C}^n | h_j(p) = 0 \text{ para todo } 1 \leq j \leq t\}$$

dos pontos que se anulam para todos os hs. Assim, o teorema é verdadeiro se, e somente se,

$$c(p) = 0 \text{ para todo } p \in \mathcal{Z}(h_1, \ldots, h_t).$$

Contudo, para que isto seja verdadeiro, é *suficiente* que c possa ser escrito como

$$c = g_1 h_1 + \cdots + g_t h_t, \tag{9}$$

onde $g_1, \ldots, g_t$ também são polinômios nas variaáveis $x_1, \ldots, x_n$. Diremos que uma equação como (9) expressa c como uma *combinação linear com coeficientes polinomiais* de $h_1, \ldots, h_t$. Uma tal relação é *suficiente* para provar o que queremos porque se

$$p \in \mathcal{Z}(h_1, \ldots, h_t);$$

isto é, se p satisfaz

$$h_1(p) = \cdots = h_t(p) = 0,$$

então

$$c(p) = g_1(p)h_1(p) + \cdots + g_t(p)h_t(p) = 0.$$

Note porém o repetido e proposital uso de *suficiente* nas expressões acima. Embora uma relação como (9) seja suficiente, ela não é necessária. Isto é, pode acontecer que

$$c(p) = 0 \text{ para todo } p \in \mathcal{Z}(h_1, \ldots, h_t).$$

sem que c satisfaça uma relação de combinação linear do tipo especificado acima. Para um exemplo muito simples disto, considere o conjunto algébrico de $\mathbb{R}^2$ definido por $\mathcal{Z}(x^2, y^2)$ que é, evidentemente, igual a $\{(0, 0)\}$. Afinal, se x^2 e y^2 só se anulam se $x = y = 0$. Mas isto significa que o polinômio $c = x$ se anula em todos os pontos de $\mathcal{Z}(x^2, y^2)$; já que só há mesmo um, a origem. Entretanto não é possível escrever x como combinação dos polinômios x^2 e y^2; como é fácil ver se argumentarmos em termos dos graus dos vários polinômios envolvidos. Veremos como contornar este problema na seção 4 do capítulo 3.

8. Apolônio

Nesta seção usaremos o Método que acabamos de descrever para provar um um famoso teorema de Apolônio; o mesmo Apolônio que, segundo Papus, resolveu o problema das três e quatro retas.

TEOREMA DE APOLÔNIO. *O pé da altura sobre a hipotenusa e os pontos médios dos lados de um triângulo retângulo pertencem a uma mesma circunferência.*

Suponhamos que o triângulo tem vértices A, B e C, de modo que BAC é o ângulo reto. Então podemos escolher as coordenadas de forma que

$$A = (0,0),\ B = (1,0) \text{ e } C = (0,y).$$

Denotando por M_1 e M_2 os pontos médios dos catetos $\overline{AB}$ e $\overline{AC}$, e por M_3 o ponto médio da hipotenusa, temos que

$$M_1 = (1/2,0),\ M_2 = (0,y/2) \text{ e } M_3 = (1/2,y/2).$$

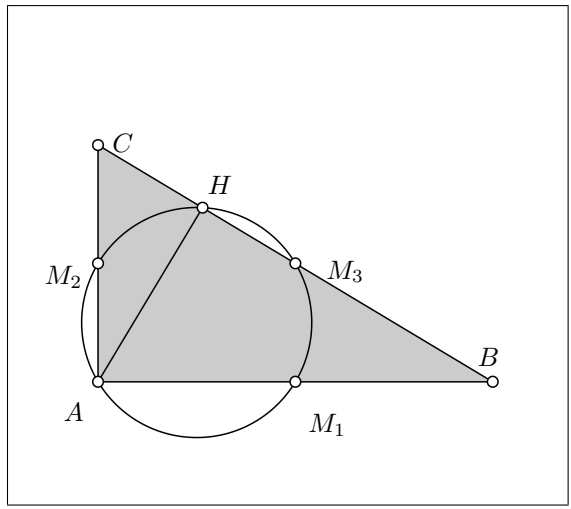


FIGURA 6. Teorema de Apolônio

Seja $P = (u,v)$ o centro da circunferência que passa por M_1, M_2 e M_3. Denotaremos por h_1 a equação que expressa o fato de M_2 pertencer à circunferência de centro P que passa por M_1 e por h_2 a equação segundo a qual M_3 está sobre a mesma circunferência. Em termos das coordenadas dos pontos, temos

$$h_1 = vy - y^2/4 - u + 1/4$$
$$h_2 = vy - y^2/4.$$

Por outro lado, se $H = (x, z)$ é o pé da altura sobre a hipotenusa, então o fato de AH ser perpendicular a BC corresponde à equação

$$h_3 = x - zy,$$

ao passo que a colinearidade entre H, C e B é dada por

$$h_4 = y(x - 1) + z.$$

Finalmente, a conclusão do teorema nos diz que H pertence à mesma circunferência de centro P que passa por M_1 discutida anteriormente, o que nos permite traduzi-la pelo anulamento do polinômio

$$c = -2ux + x^2 - 2vz + z^2 + u - 1/4.$$

Observe que neste exemplo já é muito mais difícil aplicar o método ingênuo adotado nos dois primeiros. Para isto teríamos que calcular as coordenadas de H e mostrar que satisfazem c. Mas não precisamos fazer isto, porque podemos usar o método da seção 7. Do ponto de vista algébrico, nossa meta é escrever c como combinação linear com coeficientes em $\mathbb{Q}[x, y, z, u, v]$, dos polinômios h_1, h_2, h_3 e h_4. Para isto, note que as duas últimas parcelas de c são $u - 1/4$, que é igual a $h_1 - h_2$. Assim,

$$c - (h_1 - h_2) = -2ux + x^2 - 2vz + z^2.$$

Nossa próxima meta é eliminar vz da expressão acima. Contudo, a variável z só aparece pura em h_4, e isto sugere que tomemos

$$vh_4 - xh_1 = -vy + vz + xy^2/4 + ux - x/4.$$

Portanto,

$$c - (h_1 - h_2) + 2(vh_4 - xh_1) = x^2 + z^2 - 2vy + xy^2/2 - x/2.$$

Para fazer desaparecer o vy basta somar $2h_2$ a esta última equação, o que nos dá

$$c - (h_1 - h_2) + 2(vh_4 - xh_1) + 2h_2 = x^2 + z^2 - x/2 + \frac{y}{2}y(x - 1).$$

A última parcela desta soma sugere somar $-yh_4/2$, donde

$$c - (h_1 - h_2) + 2(vh_4 - xh_1) + 2h_2 - yh_4/2 = x^2 + z^2 - x/2 - zy/2.$$

Contudo,

$$xh_3 - zh_4 = -x^2 - z^2 + zy,$$

de modo que

$$c - (h_1 - h_2) + 2(vh_4 - xh_1) + 2h_2 - yh_4/2 - xh_3 - zh_4 = -x/2 + zy/2.$$

Mas isto é igual a $h_3/2$. Concluímos, assim, que

$$c = (h_1 - h_2) - 2(vh_4 - xh_1) - 2h_2 + yh_4/2 + xh_3 + zh_4 - h_3/2.$$

Portanto, se (x, y, z, u, v) satisfazem

$$h_1 = h_2 = h_3 = h_4 = 0, \text{ então } c = 0.$$

Geometricamente,

$$h_1(y, u, v) = h_2(y, u, v) = 0$$

nos dizem que $P = (u, v)$ é o centro da cicunferência que passa por M_1, M_2 e M_3, ao passo que

$$h_3(x, y, z) = h_4(x, y, z) = 0$$

garantem que $H = (x, z)$ é o ponto de interseção da altura por A com a hipotenusa BC. Finalmente, o anulamento de c implica que H pertence à circunferência de centro P por M_1, M_2 e M_3, que é o resultado desejado.

Como você pode constatar, mesmo neste exemplo relativamente simples os cálculos necessários para escrever a conclusão como combinação polinomial das hipóteses foram bastante complicados. Isto nos leva a constatar que, para utilizar este método de modo prático precisamos certemente automatizar esta parte do procedimento, para que possa ser efetuado em um computador.

9. Comentários e complementos

A revolução promovida pela geometria analítica de Descartes acabou sofrendo uma reviravolta no século XIX quando alguns geometras declararam guerra ao uso das técnicas algébricas. Segundo Jakob Steiner, um dos maiores expoentes do método sintético naquela época, o cálculo substitui o pensamento, ao passo que a geometria deveria estimular o pensamento. Ele se opunha a qualquer "ajuda mecânica" em geometria, e listava o método analítico sob esta rubrica. Apesar de Steiner, o método de coordenadas foi intensamente explorado durante o século XIX, contando entre seus praticantes com grandes matemáticos como Julius Plücker e Arthur Cayley.

Este feudo do século XIX foi gradualmente esquecido, e deu lugar a uma atitude mais pragmática. Assim, a vasta maioria dos livros elementares de geometria escritos durante boa parte do século XX adotam o método sintético– muitos não passam, de fato, de paráfrases dos *Elementos*. Já os livros-textos universitários tendem a adotar o método analítico, em preparação para o uso das técnicas do cálculo. Assim, triângulos e quadriláteros sugerem Euclides, ao passo que cônicas remetem ao uso de coordenadas. Há razões de sobra para justificar esta escolha, afinal o método de coordenadas exige bastante destreza algébrica; contudo, a demonstração sintética de alguns resultados supostamente elementares são tão elaboradas, que uma prova analítica é certamente preferível.

Foi neste espírito que o desenvolvimento da computação algébrica a partir da década de 1960 acabou levando ao interesse pela sua utilização para dar demonstrações automáticas de teoremas de geometria. Ao contrário da computação numérica, sua irmã mais velha, a computação algébrica (ou simbólica) estuda algoritmos que possam ser executados de maneira exata. Para tornar isto viável, é necessário programar o computador para que seja capaz de calcular com inteiros sem limites fixos na quantidade de algarismos, com frações na forma de pares numéricos e com toda sorte de funções de maneira puramente simbólica. Por exemplo, enquanto em computação numérica a palavra integral sugere um numéro decimal calculado por um método de aproximação, um usuário da computação algébrica pensaria imediatamente na primitiva de

uma função elementar. Para mais detalhes, inclusive a definição do que é uma função elementar, consulte o capítulo 10.

Há vários enfoques possíveis na utilização da computação algébrica para demonstrar teoremas de geometria. A que adotaremos neste livro consiste em representar as hipóteses e a conclusão do teorema sob a forma de equações, seguindo de perto o método de Descartes. O computador é então utilizado para mostrar que a equação que representa a conclusão depende, da maneira esperada, das equações que codificam as hipóteses, provando assim o teorema. Portanto, a estratégia que usamos é inteiramente dependente do método analítico. Não nos resta escolha senão concluir que Steiner tinha razão na sua opinião de que o método analítico está profundamente ligado ao cálculo mecânico—pelo menos se incluirmos o computador como um artefato "mecânico", o que Steiner certamente faria.

O que tornou possível utilizar o computador para implementar esta estratégia foi o algoritmo descoberto por Bruno Buchberger em sua tese de doutorado defendida em 1965; veja [**6**] e [**7**]. O que Buchberger descobriu foi um algoritmo que estende o método usual de eliminação gaussiana para sistemas de equações polinomiais que não são lineares. Esta simples idéia abriu um novo mundo de aplicações, já que nos permite resolver inúmeros problemas de geometria de maneira totalmente automática. O equivalente de um sistema linear escalonado na teoria de Buchberger é a chamada *base de Gröbner reduzida*, assim chamada pelo próprio Buchberger em homenagem a Wolfgang Gröbner, seu orientador de doutorado. O algoritmo foi implementado, à época da tese, em código de máquina em um ZUSE Z 23, um computador eletrônico alemão da década de 1960, que continha cerca de 2700 transistores e mais de 600 diodos. Atualmente há versões deste algoritmo implementadas em quase todos os sistemas de computação algébrica mais populares, incluindo sistemas em domínio público como `Axiom`, `Maxima` e `Singular`.

No entanto, esta estratégia para demonstrar teoremas de geometria clássica é apenas uma das duas linhas mestras derivadas da *Geometria* de Descartes que exploraremos neste livro. A outra, que leva muito além do que um livro elementar pode chegar, origina-se na classificação das curvas contida no Livro Segundo da *Geometria*. O estudo das curvas algébricas (seção 5) lá iniciado, deu origem no século XIX à *geometria algébrica*. Combinando os métodos algébricos de Descartes aos espaços multidimensionais, os matemáticos do século XIX começaram a estudar toda sorte de objetos geométricos definidos por equações polinomiais. Hoje em dia, a *geometria algébrica* é considerada um tópico central da matemática e tem encontrado aplicações em áreas que vão desde a robótica e a computação gráfica até outras bem mais esotéricas como a teoria de cordas. As aplicações do algoritmo de Buchberger à geometria algébrica são ainda mais sensacionais e levaram à criação de uma área totalmente nova, a *geometria algébrica efetiva*, cujo objetivo é desenvolver algoritmos para o cálculo exato de diversos invariantes das curvas, superfícies e outros objetos estudados em geometria algébrica.

Como explicamos no início, nosso objetivo neste capítulo foi apenas o de mencionar algumas idéias básicas que serão desenvolvidas no curso do livro. Entre elas, estão:

- polinômios em uma e várias indeterminadas (variáveis);
- sistemas polinomiais e sua resolução;
- demonstração por computador de teoremas da geometria plana;
- estudo de curvas, superfícies e outros conjuntos algébricos.

Além destes tópicos, aplicaremos a maquinaria aqui estudada a duas outras áreas: a programação inteira e a integração de funções racionais. A primeira, como sua prima mais famosa, a programação linear, trata da determinação de soluções para sistemas de desigualdades lineares; mas, neste caso, estamos procurando soluções inteiras para os sistemas. A segunda aplicação é apenas a ponta do iceberg de uma área bastante interessante da computação algébrica: o desenvolvimento de algoritmos para calcular integrais e resolver equações diferenciais de maneira exata. Contudo, apesar de uma trajetória que leve diretamente a estes tópicos seja possível, há muitas outras aplicações interessantes que podem ver visitadas ao longo do caminho, alguns incorporados como seções de diversos capítulos, outros deixados como exercícios ou projetos; entre os quais, cálculos em corpos algébricos, coloração de grafos e ????.

10. Exercícios

1. Formule em termos de coordenadas as hipóteses e a conclusão do teorema de geometria elementar, segundo o qual *as três alturas de um triângulo sempre se cortam em um único ponto*. Este ponto é chamado de *ortocentro* do triângulo. Você consegue provar este teorema usando o método desenvolvido neste capítulo?

2. Formule em termos de coordenadas as hipóteses e a conclusão do teorema de geometria elementar, segundo o qual *as três bissetrizes de um triângulo sempre se cortam em um único ponto*.

3. Formule em termos de coordenadas as hipóteses e a conclusão da proposição 1 do *Livro dos Lemas* de Arquimedes:
   > se duas circunferências se tocam no ponto A, e se BD e EF são diâmetros paralelos nestas circunferências, então os pontos A, D e F são colineares.

4. Formule em termos de coordenadas as hipóteses e a conclusão do seguinte teorema de geometria plana elementar:
   > O baricentro, o ortocentro e o centro da circunferência circunscrita a um triângulo qualquer são colineares.

5. Formule o fato de uma reta r ser tangente a uma circunferência C, em termos das equações da reta e da circunferência.

6. Mostre que, na notação da Figura 3 da seção 4, temos que
$$\frac{\overline{CS}}{\overline{CF}} = \frac{\operatorname{sen}(\alpha)}{\operatorname{sen}(\beta)},$$
em que
$$\alpha = \widehat{CFS} \text{ e } \beta = \widehat{CSF}.$$

7. Mostre que ℓ é a reta paralela ao eixo das ordenadas de equação $x = d$ e se $C = (x, y)$ é um ponto fora de ℓ então a distância entre C e ℓ medida ao longo de um ângulo α é dada por
$$\frac{d - x}{\operatorname{sen}(\alpha)}.$$

8. Sejam a, b e c vetores no plano.
   (a) Prove que
   $$a \cdot (b - c) + b \cdot (c - a) + c \cdot (a - b) = 0;$$
   em que o ponto representa o produto escalar.
   (b) Interpretando os vetores a, b e c como na figura ???, quais são os vetores que correspondem a $a - b$, $b - c$ e $c - a$?
   (c) Use (a) e (b) para provar que as alturas de um triângulo não degenerado qualquer se cruzam em um único ponto.

CAPíTULO 2

Polinômios e ideais: uma indeterminada

Neste capítulo introduzimos os conceitos básicos da teoria de anéis e ideais e iniciamos nosso estudo dos polinômios, tratando do caso em que há apenas uma variável.

1. Anéis

Uma sistematização da álgebra semelhante à proposta por Euclides nos *Elementos* só foi desenvolvida a partir do século XIX. Não é surpreendente que os gregos não tenham feito pela álgebra o mesmo que fizeram pela geometria. De fato, eles só começaram a desenvolver um cálculo simbólico vários séculos depois de Euclides. Uma inspecção dos *Elementos* surpreende exatamente pela ausência quase absoluta de símbolos.

Já os árabes, herdeiros da matemática grega durante a Idade Média, tinham grande interesse na solução de equações, apesar do seu uso de símbolos ser ainda muito restrito. A própria palavra *álgebra* é derivada de "al-jabr w'al muqāballah", que é o nome de um tratado do famoso matemático árabe al-Khārizmī. Aliás, do nome al-Khārizmī são derivadas nossas palavras *algoritmo* e *algarismo*. Para mais detalhes sobre a contribuição de al-Khārizmī veja [**68**, p. 3–13]

É somente com o advento do século XVII que nos deparamos com cálculos algébricos expressos em uma forma que nos é familiar. A responsabilidade por esta novidade cabe a vários matemáticos, entre eles Descartes e Thomas Harriot. Como vimos a *Geometria* de Descartes é provavelmente o livro de matemática mais antigo que conseguimos ler sem ter grandes problemas com a notação.

Durante todo o século XVIII os matemáticos calcularam com suas expressões sem dar maior atenção às propriedades que os números e variáveis deveriam satisfazer. Entretanto, o final do século XVIII e início do século XIX foram marcados por sucessivas crises, sobretudo com relação ao conceito de limite, o que deflagrou um movimento por maior rigor em matemática.

No âmbito da álgebra o primeiro efeito deste movimento foi levar os matemáticos a sistematizarem as propriedades dos "números" no mesmo espírito em que Euclides e outros matemáticos gregos haviam procedido em geometria. Este movimento culminou no início do século XX com a chamada álgebra abstrata, onde o estudo das propriedades de objetos gerais substitui os exemplos concretos.

Apesar do nome, as estruturas algébricas não passam de definições de natureza classificatória. O objetivo primordial é semelhante ao das classes taxonômicas em biologia. A principal razão para definir a classe das aves, por exemplo, é tornar possível descrever com uma palavra uma série de animais com características comuns. Assim, é provável que você nunca tenha ouvido falar de um kakapo, mas se eu lhe disser que um kakapo é uma ave, você imediatamente vai imaginá-lo com duas patas, penas e bico [1].

Em álgebra acontece a mesma coisa. Da observação de exemplos com propriedades comuns surge a ideia de definir uma classe (ou estrutura) à qual pertencem estes vários exemplos. A diferença está no fato das estruturas em matemáticas serem muito mais simples e rígidas que as da biologia. Assim, uma definição satisfatória, em matemática, permite-nos deduzir uma cascata de novas propriedades que não estavam presentes na definição original. Por exemplo, das propriedades básicas dos números inteiros e da definição de número primo segue que existe uma infinidade de primos. No entanto, na definição de primo, não há nenhuma indicação quanto à sua quantidade.

Um dos primeiros matemáticos a oferecer uma sistematização das propriedades dos números (inteiros, racionais e reais) foi George Peacock, que se tornou conhecido como "o Euclides da álgebra". Em seu *Treatise on algebra*, ele explicitou claramente as diversas propriedades satisfeitas por estes números. Entretanto, foi só no início do século XX que estas propriedades foram sistematizadas na forma das definições gerais que usamos até hoje.

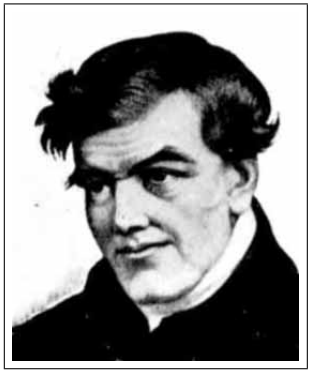


FIGURA 1. George Peacock (1791-1858)

Antes de mais nada, precisamos delimitar o âmbito da aplicação que faremos da noção de operação. Seja X um conjunto. Diremos que uma *operação* em X é uma regra que, a cada par de elementos de X associa um terceiro elemento, também em X. Por exemplo, se $X = \mathbb{N}$ é o conjunto dos números naturais (ou inteiros não negativos) então a soma e a multiplicação usuais são operações em $\mathbb{N}$. Entretanto, a subtração não é uma operação em $\mathbb{N}$ por que

[1] Um kakapo é um papagaio neozeolandês que não voa.

a diferença entre dois inteiros maiores ou iguais a zero pode não ser um inteiro maior ou igual a zero. Estamos, agora, prontos para uma das definições fundamentais deste livro.

Dizemos que um conjunto não vazio A é um *anel* se nele estão definidas duas operações, que chamaremos de adição (denotada por $+$) e multiplicação (denotada por $\cdot$ ou pela simples justaposição dos elementos que estão sendo multiplicados), que satisfazem as seguintes propriedades:

- quaisquer que sejam $a, b, c \in A$,

$$a + (b + c) = (a + b) + c \quad \text{e} \quad a(bc) = (ab)c$$
$$a + b = b + a \quad \text{e} \quad ab = ba$$

$$a(b + c) = ab + ac$$

- existem dois elementos especiais em A, denotados por 0 e 1, tais que, para todo $a \in A$,

$$a + 0 = a \quad \text{e} \quad a \cdot 1 = a$$

- para todo $a \in A$ existe um elemento $-a$ tal que

$$a + (-a) = 0.$$

Listamos algumas das propriedades da adição e da multiplicação lado a lado para chamar atenção sobre a sua semelhança. Observe que estamos exigindo que a operação de multiplicação de um anel seja comutativa; isto é, que $ab = ba$. Na maior parte dos livros de álgebra que você consultar o objeto que acabamos de definir será chamado um *anel comutativo*. Entretanto, não há razão para adotar esta nomenclatura aqui, já que *todos* os anéis que consideramos são comutativos.

Os elementos especiais 0 e 1 são conhecidos como *elementos neutros* da adição e multiplicação, respectivamente. O elemento $-a$ definido na última propriedade é chamado de *simétrico* de a. A terminologia é reminiscente do caso em que $A = \mathbb{Z}$. Neste caso, dispondo os inteiros ao longo de uma reta da maneira usual, temos que a e $-a$ são simétricos em relação à origem.

Os anéis são abundantes entre os objetos algébricos que nos são familiares. Os exemplos mais simples incluem os números inteiros, os racionais, os reais, os complexos e o conjunto $\mathbb{Z}_n$, das classes de inteiros módulo n. Outro exemplo familiar, que estudaremos com muito cuidado, é o conjunto dos polinômios em uma ou mais variáveis com as operações usuais de adição e multiplicação de polinômios, que será definido na seção 3.

Observe que

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C},$$

são todos anéis. Além disso, a soma de dois inteiros considerados como elementos de $\mathbb{Q}$ é igual à sua soma em $\mathbb{Z}$; e o mesmo acontece relativamente a todos os outros anéis na cadeia acima. Esta é uma situação tão comum que merece um nome especial. Se A for um anel e $S \subset A$ também for um anel relativamente às operações de A restritas a S, então dizemos que S é um subanel de A. Observe que a definição de subanel requer que

- o 0 e o 1 de A pertençam a S;
- se $s_1, s_2 \in S$, então $s_1 + s_2 \in S$;
- se $s_1, s_2 \in S$, então $s_1 \cdot s_2 \in S$;

em que $+$ e $\cdot$ denotam a soma e a multiplicação em A.

Entretanto, nem todo conjunto onde estão definidas uma soma e um produto constitue um anel. O exemplo mais natural é o conjunto $\mathbb{N}$ dos inteiros não negativos. Neste caso, todas as propriedades que definem um anel são satisfeitas exceto uma, a existência do simétrico. Falando em simétrico, com exceção da distributividade, que combina a soma e a multiplicação, a existência do simétrico é a única propriedade da adição que não tem correspondente na multiplicação. Vejamos o que deveria ser este correspondente. Por definição:

> o *simétrico* de $a \in A$ é o elemento que, *somado* a a, dá como resultado o *elemento neutro* da *soma*, que é *zero*.

Trocando as palavras em itálico por seus correspondentes multiplicativos, obtemos

> o *inverso* de $a \in A$ é o elemento que, *multiplicado* por a, dá como resultado o *elemento neutro* da *multiplicação*, que é *um*.

Em símbolos, o inverso de $a \in A$ é o elemento $a' \in A$ que satisfaz $aa' = 1$. Frequentemente denotaremos o inverso de a em A como a^{-1} ou $1/a$.

Ao contrário do que ocorre com o simétrico, nem todo elemento de um anel tem inverso. De fato, como $0 \cdot b = 0$, qualquer que seja $b \in A$, podemos concluir que 0 não pode ter inverso em nenhum anel. Se todos os elementos não nulos de um anel admitem um inverso, dizemos que este anel é um *corpo*. Exemplos de corpos incluem $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ além de $\mathbb{Z}_p$ quando $p > 0$ é primo. O enunciado de boa parte dos resultados deste livro começa com "seja K um corpo", o que significa que tais resultados são verdadeiros sobre, literalmente, qualquer corpo. Nestes casos você pode, se assim o desejar, tomar a frase "K é um corpo" como mera abreviação de

> K pode ser $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.

Entretanto, há um "conflito de interesses" entre alguns teoremas e todos os algoritmos deste livro que nos obriga a ter mais de um desses corpos sempre à nossa disposição. Isto se dá porque alguns dos teorema requerem que o corpo de base seja $\mathbb{C}$ pois dependem da existência de raízes de polinômios; veja o Apêndice I para mais detalhes. Já os algoritmos dependem de um corpo sobre o qual sejamos capazes de calcular no computador de maneira *exata*.

Acontece que isto não pode ser feito sobre os reais e os complexos, já que contêm números como π e a base e dos logaritmos naturais, que não podem ser representadas de maneira exata em um computador. Por isso, embora muitos algoritmos possam ser *enunciados* como se valessem para um corpo qualquer, só podem ser *executados* sobre um *corpo efetivo*: um corpo no qual as operações de adição, substração, multiplicação e divisão, além da comparação de dois elementos para determinar se são ou não iguais, podem ser executadas de maneira algorítmica e programadas em um computador. Por enquanto, os únicos corpos efetivos que conhecemos são $\mathbb{Q}$ e $\mathbb{Z}_p$ com p primo, mas outros exemplos serão estudados na seção 6 do capítulo 8.

2. Corpos e domínios

Observe que $\mathbb{Z}$ não é um corpo porque os únicos inteiros que têm inverso são 1 e -1. Apesar disso, $\mathbb{Z}$ se enquadra em uma outra classe importante de anéis, os domínios. Um anel A é um *domínio* se, sempre que $ab = 0$ para dois elementos $a, b \in A$, então $a = 0$ ou $b = 0$. Um exemplo de anel que *não* satisfaz esta propriedade é $\mathbb{Z}_6$. De fato, $\overline{2}$ e $\overline{3}$ são classes não nulas em $\mathbb{Z}_6$, mas $\overline{2} \cdot \overline{3} = \overline{0}$. Dizemos então que $\overline{2}$ e $\overline{3}$ são divisores de zero em $\mathbb{Z}_6$, já que seu produto dá zero. De maneira mais geral, um elemento a é um *divisor de zero* em um anel A se $a \neq 0$ e se existe outro elemento não nulo $b \in A$ tal que $ab = 0$.

Se K for um corpo, então um subanel S de K que também é um corpo, é chamado de *subcorpo* de K. Portanto, $\mathbb{Q}$ é subcorpo de $\mathbb{R}$ que é subcorpo de $\mathbb{C}$. Contudo, nem todo subanel de um corpo tem que ser um corpo; o exemplo mais óbvio é $\mathbb{Z}$, que não é corpo, mas é subanel dos racionais, reais e complexos. Por outro lado, todo subanel S de um corpo K tem que ser um domínio. Para provar isto suponha que existem $a, b \in S$ tais que $ab = 0$. Digamos que $a \neq 0$. Neste caso, a tem inverso $a^{-1} \in K$. Observe que não estamos afirmando que $a^{-1} \in S$; isto não precisa ocorrer para que o argumento a seguir funcione. Como S é um subanel de K, se $ab = 0$ em S então o mesmo vale em K. Mas se, por um lado,

$$a^{-1} \cdot (ab) = a^{-1} \cdot 0 = 0,$$

por outro,

$$a^{-1} \cdot (ab) = (a^{-1}a) \cdot b = 1 \cdot b = b;$$

donde concluímos que $b = 0$ em K. Contudo, usando novamente que S é subanel de K, temos que $b = 0$ em S. Portanto, sempre que $ab = 0$ em S podemos concluir que $a = 0$ ou $b = 0$; de modo que S é mesmo um domínio. Deparados com isto os matemáticos logo se perguntaram se a recíproca deste resultado seria verdadeira; isto é,

> dado um domínio D, é possível construir um corpo $Q(D)$ que contém D?

A resposta é sim: os elementos de $Q(D)$ são construídos na forma de "frações" cujo numerador e denominador pertencem a S. Como esta construção será muito usada neste livro, passamos a descrevê-la em detalhes. Contudo, você

deve ter em mente que o que faremos é essencialmente um exercício de plágio: tudo o que faremos é copiar num contexto mais geral a construção das frações a partir dos inteiros.

Seja, então, D um domínio e considere o conjunto dos pares

$$\mathcal{P} = \{(a, b) : a, b \in D \text{ e } b \neq 0\}.$$

Queremos pensar nestes pares como frações cujo numerador é A e cujo denominador é b. Entretanto, sabemos que duas frações podem ser iguais embora seus numeradores e denominadores sejam diferentes, como é o caso de $1/2$ e $2/4$. Entretanto, se n_1/q_1 e n_2/q_2 são frações, então

$$\frac{n_1}{q_1} = \frac{n_2}{q_2} \text{ se, e somente se, } n_1 q_2 = n_2 q_1,$$

que é a multiplicação cruzada usual. Usaremos isto como inspiração para definir a "igualdade" de pares $\mathcal{P}$. Na verdade, procedendo com um pouco mais de cuidado, começamos por definir uma relação $\sim$ em $\mathcal{P}$:

$$\text{se } (a_1, b_1), (a_2, b_2) \in \mathcal{P}, \text{ defina}$$

$$(a_1, b_1) \sim (a_2, b_2) \quad \text{se, e somente se,} \quad a_1 b_2 = a_2 b_1 \text{ em } D,$$

Precisamos verificar se $\sim$ se comporta como uma igualdade ou, na terminologia usual, se é uma relação de equivalência; veja [**15**, seção 1 do capítulo 4] para a definição. Para começar, $\sim$ é reflexiva, pois

$$(a, b) \sim (a, b),$$

qualquer que seja $(a, b) \in \mathcal{P}$, uma vez que $ab = ab$ evidentemente se verifica em D. Por outro lado, se dois elementos de $\mathcal{P}$ satisfazem

$$(a_1, b_1) \sim (a_2, b_2)$$

então, por definição,

$$a_1 b_2 = a_2 b_1 \text{ em } D$$

Mas esta última igualdade equivale a

$$a_2 b_1 = a_1 b_2,$$

que, por sua vez, implica que

$$(a_2, b_2) \sim (a_1, b_1).$$

Logo, de

$$\text{de } (a_1, b_1) \sim (a_2, b_2) \text{ podemos deduzir } (a_2, b_2) \sim (a_1, b_1),$$

o que prova que $\sim$ é simétrica. Note que, até aqui, não fizemos nenhum uso da restrição imposta à segunda coordenada dos pares em $\mathcal{P}$, que exigimos que fossem não nulas. Esta restrição só é necessária porque precisamos que $\sim$ também seja transitiva. Para ver isto, suponhamos que

$$(a_1, b_1) \sim (a_2, b_2) \text{ e que } (a_2, b_2) \sim (a_3, b_3)$$

em que

$$(a_1, b_1), (a_2, b_2), (a_3, b_3) \in \mathcal{P}.$$

Mas,

$$(a_1, b_1) \sim (a_2, b_2) \text{ equivale a dizer que } a_1 b_2 = a_2 b_1 \text{ em } D,$$

ao passo que

$$(a_2, b_2) \sim (a_3, b_3) \text{ equivale a } a_2 b_3 = a_3 b_2 \text{ em } D.$$

Multiplicando $a_2 b_3 = a_3 b_2$ por b_1, obtemos

$$b_1(a_2 b_3) = b_1(a_3 b_2). \tag{10}$$

Contudo, pela associatividade e comutatividade da multiplicação em D,

$$b_1(a_2 b_3) = b_3(a_2 b_1) = b_3(a_1 b_2), \tag{11}$$

em que a última igualdade segue de $a_1 b_2 = a_2 b_1$. Combinando (10) com (11), obtemos

$$b_3(a_1 b_2) = b_1(a_3 b_2).$$

Pondo b_2 em evidência dos dois lados,

$$b_2(a_1 b_3) = b_2(b_1 a_3);$$

que equivale a

$$b_2(a_1 b_3 - b_1 a_3) = 0.$$

É exatamente neste ponto do argumento que precisamos que D seja um domínio e que b_2 não seja nulo, porque sob estas hipóteses a última equação acima implica que

$$a_1 b_3 - b_1 a_3 = 0 \text{ isto é, que } a_1 b_3 = b_1 a_3.$$

Como esta última equação equivale a

$$(a_1, b_1) \sim (a_3, b_1),$$

provamos que $\sim$ é mesmo transitiva.

O conjunto $Q(D)$ subjacente ao corpo que queremos definir é o quociente de $\mathcal{P}$ por $\sim$, cujos elementos são as classes de equivalência desta relação. Dado $(a, b) \in \mathcal{P}$, denotaremos por

$$a/b \text{ ou } \frac{a}{b}$$

a classe de equivalência de (a, b) por $\sim$, para deixar claro os laços com as frações. Neste ponto o cuidado com que efetuamos esta construção nos ajuda a entender um pouco melhor o que igualdades tais como

$$\frac{1}{2} = \frac{2}{4} = \frac{6}{12}.$$

De fato, $\frac{1}{2}$ representa, não um par de números, mas sim uma classe de equivalência que, como tal, pode ser representada por quaisquer um de seus elementos, entre os quais se encontram os pares $(1, 2)$, $(2, 4)$ e $(6, 12)$.

Para tornar $Q(D)$ um corpo precisamos definir uma adição e uma multiplicação de classes de equivalência. Copiando mais uma vez as definições usadas para frações, defimos a adição de duas classes a_1/b_1 e a_2/b_2 de $Q(D)$ por

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2},$$

e sua multiplicação por

$$\frac{a_1}{b_1}\frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2}.$$

Observe que

$$\frac{a_1 b_2 + a_2 b_1}{b_1 b_2} \text{ e } \frac{a_1 a_2}{b_1 b_2}$$

são elementos legítimos de $Q(D)$, porque b_1 e b_2 são ambos diferentes de zero por definição e, portanto, seu produto tem que ser não nulo, já que D é um domínio.

Entretanto, como vimos acima, um elemento de $Q(D)$ é uma classe e pode ser representado por pares diferentes em $\mathcal{P}$. Como tanto a adição, quanto a multiplicação em $Q(D)$ são definidos a partir do representante escolhido para a classe, precisamos nos certificar de que a escolha de representantes diferentes para as classes que estamos somando não afeta o resultado final da operação. Mais precisamente, precisamos mostrar que se

$$\frac{a_1}{b_1} = \frac{a_1'}{b_1'}, \tag{12}$$

então,

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1'}{b_1'} + \frac{a_2}{b_2} \text{ e}$$
$$\frac{a_1}{b_1}\frac{a_2}{b_2} = \frac{a_1'}{b_1'}\frac{a_2}{b_2}.$$

Começando pela adição, temos que

$$\frac{a_1'}{b_1'} + \frac{a_2}{b_2} = \frac{a_1' b_2 + a_2 b_1'}{b_1' b_2},$$

de forma que a igualdade desejada equivale a

$$\frac{a_1 b_2 + a_2 b_1}{b_1 b_2} = \frac{a_1' b_2 + a_2 b_1'}{b_1' b_2},$$

que, pela definição de $\sim$, é verdadeira se, e somente se,

$$(a_1 b_2 + a_2 b_1) b_1' b_2 = (a_1' b_2 + a_2 b_1') b_1 b_2.$$

Contudo,

$$(a_1 b_2 + a_2 b_1) b_1' b_2 = (a_1 b_1') b_2 b_2 + a_2 b_1 b_1' b_2 = (a_1' b_1) b_2 b_2 + a_2 b_1 b_1' b_2,$$

em que a última igualdade segue de (12). Pondo $b_1' b_2$ nas duas parcelas desta última equação, chegamos a

$$(a_1 b_2 + a_2 b_1) b_1' b_2 = (a_1' b_2 + a_2 b_1') b_1 b_2,$$

que é a igualdade que queríamos provar. A demonstração de

$$\frac{a_1}{b_1}\frac{a_2}{b_2} = \frac{a_1'}{b_1'}\frac{a_2}{b_2}$$

é semelhante e fica aos seus cuidados.

Para completar nossa missão ainda nos falta provar que o conjunto $Q(D)$ assim construído é mesmo um corpo que contém D. Como,

$$\frac{a_1}{b_1} + \frac{0}{1} = \frac{a_1}{b_1}, \text{ e}$$
$$\frac{a_1}{b_1}\frac{1}{1} = \frac{a_1}{b_1},$$

concluímos que $Q(D)$ contém elementos neutros $0/1$ para adição e $1/1$ para a multiplicação, ao passo que se $a \neq 0$ o elemento $a/b \in Q(D)$ satisfaz,

$$\frac{a}{b}\frac{b}{a} = \frac{1}{1},$$

de modo que cada elemento não nulo de $Q(D)$ admite inverso. Ainda nos resta verificar que a adição e a multiplicação que definimos são associativas e comutativas, mas isto é fácil, embora monótono, e fica por sua conta. Dito isto, podemos tomar como provado que $Q(D)$ é mesmo um corpo, conhecido como o *corpo de frações ou de quocientes* de D.

Quanto à inclusão de D em $Q(D)$ precisamos encará-la com um alto grau de tolerância porque, francamente falando, os elementos de D não são da forma a/b, com $a, b \in D$ e $b \neq 0$ e, portanto, não estão contidos em D. Contudo, é fácil verificar que $Q(D)$ contém uma "cópia" de D, formada pelos elementos $a/1$, em que $a \in D$. O que isto quer dizer é que os cálculos com os elementos desta forma são tais e quais os cálculos com os elementos correspondentes de D. Isto nos permite identificar um elemento $a \in D$ com seu correspondente $a/1 \in Q(D)$, o que aliás estamos acostumados a fazer quando dizemos que $\mathbb{Q}$ contém $\mathbb{Z}$.

Por enquanto, o único exemplo que temos de corpo de frações é mesmo $\mathbb{Q}$, mas teremos novos exemplosa ssim que definirmos polinômios na próxima seção. Um outro exemplo de anel que temos à mão é $\mathbb{Z}_n$, mas neste caso não há porque aplicar esta construção uma vez que se n for composto, $\mathbb{Z}_n$ tem divisores de zero; ao passo que se n for primo, $\mathbb{Z}_n$ é um corpo. Isto não é característica apenas dos inteiros módulares, como mostra o exercício ???.

3. Anéis de polinômios

Ao longo de toda esta seção suporemos que A é um domínio. Nossa meta é construir, de maneira formal, o anel de polinômios em uma variável com coeficientes em A. A razão para fazer a construção neste grau de generalidade é que ela nos permite dar uma definição recursiva dos anéis de polinômios em mais de uma variável sem nenhum esforço extra. Se você preferir, pode imaginar, em uma primeira leitura, que A é $\mathbb{Z}$ ou outro anel que lhe seja familiar.

Seja x um símbolo, tradicionalmente conhecido como *variável* ou *indeterminada*. Um polinômio f na variável x, com coeficientes em A, é uma expressão da forma

$$f = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0, \tag{13}$$

em que n é um inteiro não negativo e $a_0, \ldots, a_n$ são elementos de A. Dizemos que a_j é o *coeficiente* de f em grau j. Se $a_n \neq 0$ e $a_j = 0$ para todo $j > 0$, então o inteiro n é o *grau* de f e a_n é o seu *coeficiente líder*; usaremos a notação $\mathrm{grau}(f)$ e $\mathrm{ld}(f)$ para denotá-los. A esta altura, um polinômio não passa de um encadeamento de símbolos, formando uma espécie de 'palavra'. Para dar vida a estes objetos precisamos explicar como interagem entre si.

O primeiro passo é definir a igualdade de polinômios. Seja

$$h = b_m x^m + \cdots + b_2 x^2 + b_1 x + b_0,$$

um outro polinômio. Dizemos que $f = h$ se $m = n$ e se $a_i = b_i$ para cada $0 \leq i \leq n$. Uma consequência imediata desta definição é que, se $m < n$, então os polinômios h e

$$0x^n + \cdots + 0x^{m+2} + 0x^{m+1} + b_m x^m + \cdots + b_2 x^2 + b_1 x + b_0$$

são iguais. Isto significa que sempre podemos supor que dois polinômios tenham o mesmo número de coeficientes, *desde que não estejamos fazendo nenhuma hipótese quanto a estes coeficientes serem ou não nulos!* Usaremos isto, de agora em diante, sem maior cerimônia.

Seja

$$g = b_n x^n + \cdots + b_2 x^2 + b_1 x + b_0,$$

um polinômio. Definimos a soma $f + g$ como sendo o polinômio

$$f + g = (a_n + b_n)x^n + \cdots + (a_1 + b_1)x + (a_0 + b_0). \tag{14}$$

De posse desta definição, podemos dizer que f é igual à soma dos polinômios $a_0, a_1 x, \ldots, a_n x^n$. Não esqueça que nossa convenção de permitir coeficientes nulos faz com que a fórmula da soma $f + g$ seja completamente geral. Por outro lado, se você assumir que $a_n \neq 0$ e $b_m \neq 0$ em (14), então o grau de f é, no máximo, o maior entre os inteiros m e n. Em outras palavras, temos a seguinte fórmula

$$\mathrm{grau}(f + g) \leq \max\{\mathrm{grau}(f), \mathrm{grau}(g)\}.$$

Se $m \neq n$ então teremos sempre uma igualdade na fórmula acima. Contudo, se $m = n$ os coeficientes líderes podem se cancelar, e a desigualdade na fórmula poderá ser estrita. Por exemplo,

$$(2x^3 + 5x + 4) + (-2x^3 + 7x^2) = -7x^2 + 5x + 4,$$

tem grau menor que 3, que é o grau das parcelas.

Passando à multiplicação, queremos descobrir como o produto fg deve ser definido. Como desejamos que o conjunto dos polinômios venha a ser um anel, podemos supor que a multiplicação de polinômios que pretendemos definir deva ser comutativa e distributiva. A primeira destas condições implica que

$$(a_i x^i)(b_j x^j) = a_i b_j x^{i+j},$$

em que o produto $a_i b_j$ é calculado no anel A. Observe que, subrepticiamente, estamos pensando no símbolo x^k, para um inteiro $k \geq 0$, como designando um produto; isto é,

$$x^k = \underbrace{x \cdots x}_{k \text{ vezes}},$$

em que, como usual, $x^0 = 1$. Levando isto em conta, temos que

$$fg = \sum_{i,j} a_i b_j x^{i+j}. \tag{15}$$

Mas esta fórmula não é muito satisfatória porque a expressão resultante não está na forma da equação (13). Por exemplo, aplicando a fórmula ao produto $(2x^2 + 3x)(x^3 + 3x^2 + 1)$, obtemos

$$2x^5 + 6x^4 + 2x^2 + 3x^4 + 9x^3 + 3x.$$

Para converter (15) para a forma padrão basta usar a distributividade para agrupar os termos de mesmo grau. Fazendo isto, no exemplo, obtemos

$$(2x^2 + 3x)(x^3 + 3x^2 + 1) = 2x^5 + 9x^4 + 9x^3 + 2x^2 + 3x.$$

Em geral, temos as seguintes expressões para os coeficientes de fg

coeficiente de x^0: $a_0 b_0$;
coeficiente de x^1: $a_0 b_1 + a_1 b_0$;
coeficiente de x^2: $a_0 b_2 + a_1 b_1 + a_2 b_0$.

Generalizando, obtemos a fórmula geral

$$\sum_{i=1}^{n} a_i b_{k-i} \tag{16}$$

para o coeficiente de x^k, que você pode facilmente provar por indução em k.

Ao escrever a fórmula (16), estamos subentendendo que alguns dos coeficientes podem ser nulos, mesmo se estão mais à esquerda do que o último coeficiente não nulo de f ou g. Entretanto, se f tem grau n e g tem grau m, então (16) implica que:

- os coeficientes de fg de grau maior que $n + m$ são todos nulos;
- o coeficiente de fg de grau $n + m$ é $a_n b_m$.

Como estamos supondo que f tem grau n e g tem grau m, os coeficientes a_n e b_m não podem ser nulos. Mas A é um domínio, portanto $a_n b_m \neq 0$; donde concluímos que

$$\text{grau}(fg) = \text{grau}(f) + \text{grau}(g).$$

Como consequência da equação acima, vemos que se $\text{grau}(f) \geq 1$, para algum polinômio $f \in A[x]$, então

$$\text{grau}(fg) = \text{grau}(f) + \text{grau}(g) \geq \text{grau}(g) + 1 \geq 1,$$

qualquer que seja $g \in A[x]$. Em particular, isto nos diz que se f tem grau maior ou igual a um, então não há nenhum polinômio g tal que $fg = 1$, pois fg tem grau pelo menos um. Em outras palavras, se um elemento de $A[x]$

for invertível, então tem que ter grau zero. Como, neste caso, o elemento pertencerá a A, podemos refinar esta afirmação, na forma

> os elementos invertíveis de $A[x]$ coincidem com os elementos invertíveis de A.

Já discutimos soma e produto de polinômios, falta-nos falar sobre a divisão de polinômios. Como no caso dos números inteiros, trataremos da divisão com resto. Em outras palavras, ao dividir um polinômio f por um polinômio g, esperamos encontrar dois novos polinômios, o quociente q e o resto r, de modo que $f = gq + r$. Além disto, queremos que o resto seja, de alguma forma, "menor" que o divisor. Faremos isto exigindo que r seja nulo, ou que tenha *grau* menor que o *grau* de g. Uma maneira de provar a existência de q e r é construir um algoritmo capaz de calculá-los. O algoritmo que apresentaremos será recursivo, e reduzirá o grau do dividendo f até que seja menor que o grau de g.

Digamos que

$$f = a_n x^n + \cdots + a_1 x + a_0 \quad \text{e} \quad g = b_m x^m + \cdots + b_1 x + b_0$$

com a_n e b_m não nulos. Se, por acaso, $n < m$, então o resto será o próprio f, e o quociente será zero. Assim, podemos supor que $n \geq m$. Neste caso, queremos subtrair de f um múltiplo de g de modo a anular o termo de maior grau de f. Para isto precisamos fazer duas coisas:

(1) compensar a diferença entre o grau de g e o de f multiplicando g por x^{n-m};

(2) compensar os coeficientes, multiplicando g por a_n/b_m.

É claro que (1) não oferece nenhuma dificuldade, mas para efetuar (2) precisamos poder dividir a_n por b_m em A, o que nem sempre é possível. Por exemplo, não é possível dividir $3x^2 + 1$ por $2x + 5$ em $\mathbb{Z}[x]$, porque 2 não divide 3 em $\mathbb{Z}$. Na prática este problema pode ser contornado admitindo que b_m tenha inverso multiplicativo em A. Ou seja, estamos admitindo que existe um elemento $b'_m \in A$ tal que $b_m b'_m = 1$. Isto significa que só vamos poder efetuar a divisão de polinômios em alguns caso especiais.

Supondo, então, que b_m tem inverso b'_m, efetuamos as operações (1) e (2), calculando $f - a_n b'_m x^{n-m} g$, cujo coeficiente de grau n é 0. Portanto, $f - a_n b'_m x^{n-m} g$ tem grau menor que o grau de f. O algoritmo consiste na repetição destes passos até que reste um polinômio de grau menor que g. Mais precisamente, temos o seguinte conjunto de instruções, nas quais usamos $\mathrm{ld}(f)$ para denotar o termo líder de um polinômio f como na página 38.

ALGORITMO 2.1 (Algoritmo de divisão para polinômios em uma variável). *Seja A um domínio. Dados polinômios $f, g \in A[x]$, de modo que o coeficiente de maior grau de g seja invertível em A, o algoritmo calcula polinômios $q, r \in A[x]$ tais que*

$$f = gq + r \text{ e } r = 0 \text{ ou } r \text{ tem grau menor que o grau de } g$$

Etapa 1: *Inicializa $F = f$ e $Q = 0$.*
Etapa 2: *Enquanto F tem grau maior ou igual que o grau de g, faça*

$$F = F - \frac{\mathrm{ld}(F)}{\mathrm{ld}(g)}x^{n-m}g \text{ e } Q = Q + \frac{\mathrm{ld}(F)}{\mathrm{ld}(g)}x^{n-m},$$

em que n é o grau de F e m o grau de g.
Etapa 2: *Imprima "o quociente é Q e o resto é F".*

Como no caso de inteiros, apresentamos a divisão de polinômios em uma tabela, como ilustra o exemplo a seguir.

$$\begin{array}{rl} 6x^6+7x^5+8x^4+1 & \big|\ x^4+x+1 \\ \cline{2-2} 7x^5+8x^4-6x^3-6x^2+1 & 6x^2+7x+8 \\ 8x^4-6x^3-13x^2-7x+1 & \\ -6x^3-13x^2-15x-7 & \end{array}$$

Portanto, neste exemplo, o quociente é $6x^2+7x+8$ e o resto é $-6x^3-13x^2-15x-7$.

Ainda precisamos provar que o algoritmo funciona. Isto significa, mostrar que sempre para e que calcula o que foi especificado na entrada. Para isso, denote por F_i e Q_i os valores das variáveis F e Q no i-ésimo passo da aplicação do algoritmo. Se escrevermos $F_0 = f$ para o valor de F no início da computação, teremos que

$$\text{grau}(F_0) > \text{grau}(F_1) > \text{grau}(F_2) > \cdots \geq 0,$$

pois

$$F_{i+1} = F_i - \frac{\mathrm{ld}(F)}{\mathrm{ld}(g)}x^{n-m}g$$

foi construído de modo que houvesse cancelamento do termo líder de F_i. Portanto, o algoritmo tem que parar. Por outro lado, o algoritmo só para no i-ésimo passo se

$$r = 0 \text{ ou } \text{grau}(F_i) < \text{grau}(g),$$

Mas temos, por indução em i, que $F_i = f - Q_i g$. Logo, tomando $r = F_i$ e $q = Q_i$ obtemos $f = qg + r$ e $r = 0$ ou r tem grau menor que o grau de g, como havia sido especificado na saída.

Há uma observação elementar, mas muito importante, sobre o algoritmo de divisão que precisamos fazer. Digamos que K é um corpo e que $f, g \in K[x]$. Ao longo de todos os passos do algoritmo de divisão estamos calculando apenas com elementos obtidos somando ou multiplicando os coeficientes de f e de g e seus inversos. Como estes coeficientes pertencem ao corpo K, em nenhum momento da execução do algoritmo obteremos polinômios que não pertençam a $K[x]$. Uma consequência disto é que se L é um corpo que contém K, então mesmo que consideremos f e g como elementos de $L[x]$, e não de

$K[x]$, isto *não* fará qualquer diferença no cálculo do quociente e do resto pelo algoritmo de divisão.

No futuro aplicaremos o algoritmo de divisão mais frequentemente quando o anel de coeficientes é um corpo K porque, neste caso, o polinômio divisor sempre tem coeficiente líder invertível, de modo que a divisão sempre é possível. Para falar a verdade, como $K[x]$ é um domínio, podemos ir além do que fizemos no que concerne à divisão: podemos construir um corpo que contém $K[x]$. Procedendo como na seção 2, obteremos um corpo cujos elementos são da forma

$$\frac{f}{g} \text{ em que } \quad f, g \in K[x] \text{ e } \quad g \neq 0.$$

Trata-se do *corpo das funções racionais*, que é usualmente denotado por $K(x)$. Como no caso geral, identificamos um polinômio $f \in K[x]$ com o elemento $f/1 \in K(x)$, o que nos permite tratar $K[x]$ como subanel de $K(x)$. Na seção 1 do capítulo 10, veremos como aplicar o algoritmo de divisão para escrever os elementos de $K(x)$ de forma a poder facilmente integrá-los: é a *decomposição em frações parciais*, que você aprendeu em cálculo 1 e que transformaremos em um algoritmo eficiente no capítulo 10.

A beleza da construção geral dos anéis de polinômios desta seção está em que ela nos permitirá definir anéis de polinômios em mais de uma variável sem nenhum custo adicional; coisa que faremos no próximo capítulo.

4. Ideais

A noção de ideal, de que trata esta seção, é uma generalização da noção de múltiplo. Por isso, convém relembrar as propriedades básicas dos múltiplos antes de embarcar na definição. Poderíamos fazer isto considerando apenas números inteiros, mas é conveniente tratar do caso mais geral de um anel qualquer A.

Se a e d são elementos de um anel A. Dizemos que d *divide* a se existe $c \in A$ tal que $a = dc$. Neste caso dizemos também que a é *múltiplo* de d. A partir desta definição podemos provar facilmente as seguintes propriedades:

(1) 0 é múltiplo de qualquer elemento de A;
(2) se a e b são múltiplos de d, então $a + b$ também é;
(3) se a é múltiplo de d e b é um elemento qualquer de A, então ab também é múltiplo de d.

Note que em (2) estamos exigindo que b seja múltiplo de d; mas não em (3).

A demonstração destas propriedades é muito simples. Para começo de conversa, (1) corresponde à bem conhecida propriedade $d \cdot 0 = 0$ para todo $d \in A$; veja exercício ???. Para provar (2), suponha que $a = dc$ e que $b = de$. Então,

$$a + b = dc + de = d(c + e),$$

de modo que $a + b$ é mútiplo de d, como esperado. Finalmente, se $a = dc$, e b é qualquer elemento de A (não necessariamente divisível por d), temos que

$$ba = b(dc) = (bc)d,$$

é múltiplo de d, o que prova (3).

O segundo passo para chegar à definição de ideal consiste em reformular a noção de múltiplo em termos de conjuntos. Aqui ajuda saber um pouco de história. O conceito de conjunto, embora anteriormente latente, tornou-se central em matemática a partir do século XIX, com o trabalho de matemáticos como Georg Cantor e Richard Dedekind. Ainda hoje somos herdeiros desta tradição, daí a preferência da álgebra moderna por definições em que as propriedades de uma relação se traduzem em termos de pertinência a um conjunto.

Para formular a divisibilidade por d neste contexto precisamos primeiro escolher um conjunto apropriado. Nossa escolha recairá sobre o conjunto M dos múltiplos de d, que denotaremos por $\langle d \rangle$; isto é

$$\langle d \rangle = \{xd : x \in A\}.$$

Mas já vimos que: (1) 0 é múltiplo de d, (2) a soma de dois múltiplos de d também é um múltiplo de d e (3) um múltiplo de d vezes qualquer coisa volta a ser um múltiplo de d. Reescrevendo estas propriedades em termos de pertinência a $\langle d \rangle$, temos

(1') $0 \in \langle d \rangle$;
(2') se $a, b \in \langle d \rangle$, então $a + b \in \langle d \rangle$;
(3') se $a \in \langle d \rangle$ e $b \in A$, então $ba \in \langle d \rangle$.

Estas três propriedades contêm o cerne do conceito de divisibilidade, conforme expresso em termos do conjunto dos múltiplos de um elemento. Isto levou os matemáticos do século XIX, sobretudo R. Dedekind e E. Kummer, a considerar qualquer subconjunto de A que satisfaça estas propriedades como sendo uma versão generalizada de um conjunto de múltiplos. Enunciando o conceito em todo o seu esplendor, temos a seguinte definição. Um subconjunto I de um anel A é um *ideal* se

- $0 \in I$;
- se $a, b \in I$, então $a + b \in I$;
- se $a \in I$ e $b \in A$, então $ba \in I$.

Observe que todo ideal contém 0, de modo que um ideal é sempre um conjunto não vazio. A razão para o nome ideal é curiosa e merece um comentário. Em sua tentativa de provar o Último Teorema de Fermat, Kummer havia se deparado com anéis onde havia uma fatoração, como a dos inteiros em primos. O problema é que esta fatoração *não* era única. Para contornar este problema, ele introduziu o que chamou de "números ideais", para os quais a unicidade da fatoração era recomposta. Mais tarde, baseando-se nos "números ideais" de Kummer, Dedekind introduziu a definição dada acima, que é a que ainda utilizamos atualmente. Na seção 6 discutiremos em detalhes em que consiste a fatoração em um anel e veremos exemplos em que a fatoração não é única.

Não é difícil produzir exemplos de ideais em um anel A. Os dois exemplos mais naturais correspondem às extremidades da escala; isto é, ao menor e ao maior ideal que um anel pode ter. Como já vimos que todo ideal tem que conter 0, o menor ideal possível de A é o conjunto unitário cujo único elemento é o

próprio zero. Já o maior ideal possível é o anel inteiro. Como é fácil constatar, os conjuntos $\{0\}$ e A satisfazem às condições (1), (2) e (3) acima, de modo que são realmente ideais de A.

Na verdade, A admite como gerador qualquer um de seus elementos invertíveis. De fato, se $u \in A$ tem inverso v, e a é um elemento qualquer de A, então

$$a = (av) \cdot u;$$

de forma que $A = \langle u \rangle$ segue da terceira condição na definição de ideal dada acima. O mesmo argumento mostra que, se um ideal I de A contém um elemento invertível, então $I = A$. Como consequência disto, podemos afirmar que os únicos ideais de um corpo são $\{0\}$ e o próprio corpo. A recíproca deste resultado também é verdadeira, como mostramos na proposição seguinte.

PROPOSIÇÃO 2.2. *Um anel A é um corpo se, e somente se, seus únicos ideais são $\{0\}$ e o próprio A.*

DEMONSTRAÇÃO. Como já provamos que a condição é suficiente, falta apenas mostrar que é necessária. Para isto suponha que A é um anel cujos únicos ideais são $\{0\}$ e A. Seja $a \neq 0$ um elemento de A. Mas $\langle a \rangle$ é um ideal de A. Além do mais, como

$$a = 1 \cdot a \in \langle a \rangle,$$

temos que $\langle a \rangle \neq \{0\}$. Com isso, devemos ter que

$$\langle a \rangle = A.$$

Mas isto significa que existe um elemento $b \in A$ tal que

$$1 = ab \in \langle a \rangle.$$

Portanto, a tem inverso b. Como este argumento se aplica a qualquer elemento não nulo de A, podemos concluir que A é um corpo. □

Antes de encerrar esta seção convém introduzir um exemplo menos elementar de ideal. Escolha um inteiro $n > 1$ e, no anel de polinômios $\mathbb{Z}[x]$, considere o subconjunto

$$I_n = \{f \in \mathbb{Z}[x] : f(0) \text{ é divisível por } n\}.$$

Vamos mostrar que I_n é um ideal de $\mathbb{Z}[x]$. Como 0 é divisível por n, é claro que $0 \in I_n$. Por outro lado, se $f, g \in I_n$, então

$$(f + g)(0) = f(0) + g(0).$$

Contudo, se $f, g \in I_n$, então $f(0)$ e $g(0)$ são múltiplos de n. Das propriedades dos múltiplos de n podemos concluir que $f(0) + g(0)$ também é múltiplo de n; logo $f + g \in I_n$. Finalmente, se $h \in \mathbb{Z}[x]$ e $f \in I_n$, então

$$(hf)(0) = h(0)f(0).$$

Como $f(0)$ é múltiplo de n, então $h(0)f(0)$ também é, de modo que $hf \in I_n$. Mostramos, assim, que I é mesmo um ideal de $\mathbb{Z}[x]$.

5. Polinômios em uma variável

Para explorar melhor as propriedades dos ideais de um anel, precisamos generalizar o procedimento usado para definir o ideal correspondente a um conjunto de múltiplos. Para isto, escolhemos um subconjunto S de elementos de A, que pode ser finito ou infinito. Definimos, então, um conjunto $\langle S\rangle$ cujos elementos são da forma

$$c_1 s_1 + \cdots + c_t s_t$$

em que $s_1, \ldots, s_t$ é uma escolha qualquer, de uma quantidade *finita* de elementos de S, e $c_1, \ldots, c_t \in A$. É fácil ver que $\langle S\rangle$ é um ideal de A. Para começar, podemos escrever 0 na forma $0 = 0s$ em que s é um elemento qualquer de S; logo $0 \in \langle S\rangle$. A propriedade aditiva requer um comentário preliminar. Para construir um elemento de $\langle S\rangle$ selecionamos primeiro uma quantidade *finita* dentre os (possivelmente infinitos) elementos de S e tomamos uma combinação linear com coeficientes em A. Portanto, ao tomar dois elementos $\alpha, \beta \in \langle S\rangle$, estamos fazendo duas escolhas, possivelmente diferentes, de subconjuntos finitos de S dos quais α e β serão combinações lineares. Entretanto, se $s_1, \ldots, s_t$ forem os elementos da *união* destes dois subconjuntos finitos, podemos escrever

$$\alpha = a_1 s_1 + \cdots + a_t s_t \text{ e } \beta = b_1 s_1 + \cdots + b_t s_t$$

desde que aceitemos que alguns dos coeficientes destas combinações possam ser nulos. Com isto, temos que

$$(\alpha + \beta) = (a_1 + b_1)s_1 + \cdots + (a_t + b_t)s_t$$

que também pertence a $\langle S\rangle$. Finalmente, se

$$\alpha = a_1 s_1 + \cdots + a_t s_t \in \langle S\rangle,$$

para uma escolha $s_1, \ldots, s_t \in S$ e b é um elemento qualquer de A, então

$$b\alpha = (ba_1)s_1 + \cdots + (ba_t)s_t \in \langle S\rangle,$$

concluindo a verificação de que $\langle S\rangle$ é um ideal de A. Diremos que este é o *ideal gerado por* S e que os elementos de S são seus geradores.

Se $S = \{s_1, \ldots, s_r\}$ for finito, então temos que

$$\langle S\rangle = \{c_1 s_1 + \cdots + c_r s_r : c_1, \ldots, c_r \in A\}.$$

Neste caso é costume escrever simplesmente $\langle s_1, \ldots, s_r\rangle$. Com isto voltamos ao ponto de partida, porque o conjunto dos múltiplos de um elemento d de A é igual a $\langle d\rangle$. Ideais gerados por um único elemento são chamados de *principais*. Em particular, os dois ideais mais simples de qualquer anel são sempre principais, pois

$$\{0\} = \langle 0\rangle \quad \text{e} \quad A = \langle 1\rangle.$$

Os ideais de um anel de polinômios *em uma variável* podem ser descritos de uma maneira surpreendentemente simples, como mostra o seguinte teorema. Em toda esta seção, K denotará um corpo.

TEOREMA 2.3. *Todo ideal de $K[x]$ é principal.*

DEMONSTRAÇÃO. Seja I um ideal de $K[x]$. Como tanto $\{0\}$ como $K[x]$ são obviamente gerados por um elemento, podemos supor que $\{0\} \subsetneq I \subsetneq K[x]$. A estratégia que adotaremos para mostrar que I tem um gerador pode ser dividida em duas partes:

(1) escolher um candidato g a gerador de I;
(2) mostrar que o resto da divisão de cada elemento de I por g é zero.

Note que (2) implica que $I \subseteq \langle g \rangle$. Como $g \in I$, por hipótese, teríamos neste caso a igualdade $I = \langle g \rangle$, como desejado.

O primeiro desafio consiste em escolher g de maneira adequada. Entretanto, como esperamos que g venha a dividir cada elemento de I, então deve ter o menor grau possível entre os elementos de I. Assim, escolheremos g como sendo um polinômio *não nulo* qualquer de I cujo grau é o menor possível. Note que, em princípio podem existir vários polinômios distintos satisfazendo esta propriedade.

Para provar que g divide cada elemento de I, tome $f \in I$ e divida-o por g, obtendo

$$f = gq + r \text{ em que } r = 0 \text{ ou } r \text{ tem grau menor que grau}(g).$$

Entretanto, como $f, g \in I$ então $f - qg \in I$, já que I é um ideal de $K[x]$. Assim, se $r \neq 0$ teríamos que

$$r \in I \text{ e } r \text{ tem grau menor que } g,$$

o que contradiz a escolha de g. Portanto, $r = 0$ e a demonstração está completa. □

Como consequência da demonstração vemos que, dois polinômios quaisquer de grau menor possível no ideal I têm que ser múltiplos um do outro. Entretanto, isto só é possível se estes polinômios forem associados ; isto é, se diferem apenas pelo produto por uma constante.

É importante frisar que este resultado só vale para polinômios de uma variável com coeficientes em um corpo. Por exemplo, o ideal I_n definido ao final da seção anterior não é principal. Isto é importante o suficiente para merecer uma demonstração. Lembre-se que se $n > 1$ for um inteiro, definimos

$$I_n = \{f \in \mathbb{Z}[x] : f(0) \text{ é divisível por } n\}.$$

e mostramos que é um ideal de $\mathbb{Z}[x]$. Provaremos, por contradição, que I_n não é principal. Se fosse, então deveria existir um polinômio $g \in I_n$ de modo que todo elemento de I_n fosse múltiplo de g. Contudo, x e n são elementos de I_n. Logo, devemos ter que

$$x = gh_1 \text{ e } n = gh_2,$$

para alguma escolha de $h_1, h_2 \in \mathbb{Z}[x]$. Contudo, como $\mathbb{Z}[x]$ é um domínio, temos da segunda equação que

$$0 = \text{grau}(n) = \text{grau}(g) + \text{grau}(h_2),$$

que implica que $\text{grau}(g) = 0$. Logo g tem que ser um número inteiro. Entretanto, como o coeficiente líder de x é igual a 1, a primeira das duas equações

implica que g tem que ser uma unidade; logo, $g = \pm 1$. Mas se ± 1 estivesse em I_n então I_n teria que ser igual a todo o anel $\mathbb{Z}[x]$. Isto não é verdade porque há elementos de $\mathbb{Z}[x]$ que não pertencem a I_n, um dos quais é $f(x) = x + 1$, uma vez que $f(0) = 1$ não é múltiplo de n. Portanto, I_n *não* pode ser principal, como havíamos afirmado. Apesar disso, dois elementos bastam para gerar I_n, a saber x e n; mas isso fica como exercício para você.

O exemplo anterior mostra que, se o anel de base de um anel de polinômios não for um corpo, então o anel de polinômios terá ideais que não são principais. Como veremos no próximo capítulo, um anel de polinômios em várias indeterminadas pode ser construído recursivamente, como um anel de polinômios cujo anel de base é um outro anel de polinômios. Estamos, assim, em uma situação semelhante a de $\mathbb{Z}[x]$, de modo que seria de esperar que, também neste caso, haja ideais que não são principais. Isto é, de fato, o que acontece, como veremos na seção 2 do capítulo 3.

A ideia de usar o algoritmo de divisão para provar que um determinado polinômio, ou polinômios, gera um dado ideal é o arquétipo de tudo o que está por vir neste livro. Por isso vamos explorar um pouco mais o papel do algoritmo de divisão no caso de uma variável.

Apesar do teorema 2.3 garantir que cada ideal de $K[x]$ pode ser gerado por apenas um elemento, nada nos impede de escolher vários polinômios $g_1, \ldots, g_s \in K[x]$ e considerar o ideal $\langle g_1, \ldots, g_s \rangle$, conforme definido na seção anterior. Entretanto, de acordo com o teorema, existe um polinômio h, tal que

$$\langle g_1, \ldots, g_s \rangle = \langle h \rangle.$$

É razoável perguntar quem é h, e como se deve proceder para calculá-lo a partir dos gs.

A primeira coisa a notar é que, como $g_i \in \langle h \rangle$, deve existir $a_i \in K[x]$ de modo que $g_i = a_i h$, para $1 \leq i \leq s$. Logo, h é um divisor de cada g_i. Por outro lado, $h \in \langle g_1, \ldots, g_s \rangle$, de forma que

$$h = g_1 b_1 + \cdots + g_s b_s, \tag{17}$$

para algum escolha de $b_1, \ldots, b_s \in K[x]$. Mas isto significa que, se d divide cada g_i, então d também divide h. Portanto, h deve ser o divisor comum de maior grau dos g_is; isto é, h é o máximo divisor comum de $g_1, \ldots, g_s$. Identificamos, portanto, h; resta-nos descobrir como calculá-lo a partir dos gs.

Nisto, a demonstração do teorema 2.3 em nada nos ajuda. O problema é que a escolha do gerador feita na demonstração requer um matemático capaz de conhecer todos os elementos do ideal, de modo a poder escolher o de menor grau. Mas só conhecemos um conjunto de geradores: nada mais. Aqui, mais uma vez, Euclides vem em nosso auxílio. O mesmo algoritmo euclidiano utilizado para calcular o máximo divisor comum de inteiros pode ser aplicado a polinômios em uma variável. Naturalmente, basta tratar do caso em que o ideal é gerado por dois elementos, já que podemos proceder por recorrência, usando

$$\langle g_1, g_2, \cdots, g_{s-1}, g_s \rangle = \langle q, g_s \rangle,$$

em que $\langle g_1, g_2 \cdots, g_{s-1}\rangle = \langle q\rangle$.

Sejam $f, g \in K[x]$, e digamos que f tem grau maior ou igual que o grau de g. Dividindo f por g, obtemos um quociente q_1 e um resto r_1, de modo que

$$f = gq_1 + r_1 \text{ em que } r_1 = 0 \text{ ou } r \text{ tem grau menor que o de } g.$$

Isto implica que

$$\langle f, g\rangle = \langle r_1, g\rangle.$$

Para provar a igualdade, escolha $h \in \langle f, g\rangle$. Então, existem $a, b \in K[x]$ tais que $h = af + bg$. Como $f = gq_1 + r_1$, temos que

$$h = af + bg = a(gq_1 + r_1) + bg = ar_1 + (aq_1 + b)g \in \langle r_1, g\rangle.$$

A demonstração da recíproca é análoga, bastando para isto escrever $r_1 = f - gq_1$. Os detalhes ficam por sua conta.

Prosseguindo como no algoritmo euclidiano para inteiros, precisamos dividir g por r_1, o que nos dá um quociente q_2 e um resto r_2. Como acima, obtemos

$$\langle f, g\rangle = \langle r_1, g\rangle = \langle r_1, r_2\rangle.$$

Contudo, se $\mathrm{i}(f, g) = \inf\{\mathrm{grau}(f), \mathrm{grau}(g)\}$ e nenhum dos restos for nulo, então

$$\mathrm{i}(f, g) > \mathrm{i}(r_1, r_2) \geq 0.$$

Mas isto significa que, se continuarmos o processo acima, dividindo cada resto r_i por r_{i+1}, sem que haja restos nulos, obteremos uma sequência decrescente

$$\mathrm{i}(f, g) > \mathrm{i}(r_1, r_2) > \mathrm{i}(r_3, r_4) > \cdots \geq 0.$$

Entretanto, esta sequuência de inteiros não negativos está limitada acima por $\mathrm{i}(f, g)$. Portanto, não pode ter mais que uma quantidade finita de elementos. Logo a sequência de restos tem que conter um resto nulo, digamos r_{n+1}. Mas, se $r_{n+1} = 0$, temos que

$$\langle f, g\rangle = \langle r_1, g\rangle = \cdots = \langle r_{n-1}, r_n\rangle = \langle r_{n+1}, r_n\rangle = \langle 0, r_n\rangle = \langle r_n\rangle.$$

Resumindo, concluímos que o último resto não nulo na sequência de divisões

$$\begin{aligned}
f &= gq_1 + r_1\\
g &= r_1q_2 + r_2\\
r_1 &= r_2q_3 + r_3\\
&\vdots\ \ \vdots \quad\ \ \vdots\\
r_{i-1} &= r_iq_{i+1} + r_{i+1}\\
&\vdots\ \ \vdots \quad\ \ \vdots\\
r_{n-2} &= r_nq_{n-1} + r_n\\
r_{n-1} &= r_nq_{n+1}
\end{aligned}$$

(18)

é o gerador de $\langle f, g\rangle$. Na sequência acima assumimos que este resto é $r_n \neq 0$.

Foi da equação (17) que deduzimos que o polinômio h era o máximo divisor comum os polinômios $g_1, \ldots, g_s \in K[x]$. Mas esta mesma equação expressa h como uma combinação linear polinomial dos gs. Em outras palavras,

> o máximo divisor comum entre dois ou mais polinômios pode ser escrito como uma combinação linear destes polinômios,

sem esquecer que os coeficientes desta combinação linear são, eles mesmos, polinômios. Para futuras aplicações precisamos conhecer os coeficintes polinomiais desta combinação linear. Como, mais uma vez, basta tratar o caso em que há dois geradores, formularemos e resolveremos o problema apenas neste caso.

Sejam, então, $f, g \in K[x]$, como antes. Desejamos determinar polinômios a e b tais que $r_n = af + bg$. Para calculá-los utilizaremos uma versão o *algoritmo euclidiano estendido*, originalmente desenvolvido por D. E. Knuth em [**29**].

A ideia do Knuth consiste em observar que cada resto r_i em (18) pode ser expresso em termos de f e g, com coeficientes que podem ser obtidos por uma recursão bastante simples. Digamos que

$$r_i = a_i f + b_i g. \tag{19}$$

Como $r_1 = f - gq_1$, temos que $a_1 = 1$ e $b_1 = -q_1$. Por outro lado,

$$r_2 = g - r_1 q_2 = g - (f - gq_1)q_2 = fq_2 + (1 + q_1 q_2)g,$$

de modo que $a_2 = q_2$ e $b_2 = 1 + q_1 q_2$. Supondo, agora, que já calculamos expressões para os restos até r_i, vejamos como achar a expressão para r_{i+1}. Por hipótese,

$$r_i = a_i f + b_i g \text{ e } r_{i-1} = a_{i-1} f + b_{i-1} g.$$

Substituindo a expressão para r_{i+1} em função dos restos anteriores, obtemos

$$r_{i+1} = r_{i-1} - r_i q_{i+1} = a_{i-1} f + b_{i-1} g - (a_i f + b_i g)q_{i+1}.$$

Pondo f e g em evidência, resta

$$r_{i+1} = (a_{i-1} - a_i q_{i+1})f + (b_{i-1} - b_i q_{i+1})g;$$

donde

$$a_{i+1} = a_{i-1} - a_i q_{i+1} \text{ e } b_{i+1} = b_{i-1} - b_i q_{i+1},$$

que nos dá a recursão desejada.

Embora a inicialização da recursão possa ser feita a partir dos valores de a_1, b_1 e a_2, b_2 calculados acima, há uma maneira mais prática de proceder. Basta interpretar f e g como se fossem restos, que podemos denotar por r_{-1} e r_0, e escrevê-los na forma da equação (19). Teremos, então

$$r_{-1} = f = fa_{-1} + gb_{-1} \quad \text{e} \quad r_0 = g = fa_0 + gb_0;$$

o que nos sugere escolher

$$a_{-1} = 1, b_{-1} = 0, a_0 = 0 \text{ e } b_0 = 1;$$

com o quê podemos dar início à recursão. Tendo executado o algoritmo, e descoberto que o máximo divisor comum corresponde ao resto r_{n-1}, obtemos

$$d = r_n = fa_n + gb_n.$$

Ou seja, $a = a_n$ e $b = b_n$.

Digamos que queremos calcular o máximo divisor comum d dos polinômios

$$f = x^4 + 5 \quad \text{e} \quad g = x^5 + x^3 + 2x + 1,$$

em $\mathbb{Q}[x]$, além de $a, b \in \mathbb{Q}[x]$ tais que

$$af + bg = d$$

A melhor maneira de aplicar o algoritmo estendido é organizar os dados em uma tabela. Os restos e quocientes das várias divisões aparecem nas primeiras duas colunas, já a terceira coluna contém os valores dos vários a_i.

resto	quociente	a
$x^4 + 5$	$**$	1
$x^5 + x^3 + 2x + 1$	$**$	0
$x^4 + 5$	0	1
$x^3 - 3x + 1$	x	$-x$
$3x^2 - x + 5$	x	$x^2 + 1$
$-\frac{41}{9}x + \frac{4}{9}$	$\frac{1}{3}x + \frac{1}{9}$	$-\frac{1}{3}x^3 - \frac{1}{9}x^2 - \frac{4}{3}x - \frac{1}{9}$

Observe que não há necessidade de calcular a coluna referente aos b_i, já que o valor final de b pode ser facilmente determinado como o quociente de $d - af$ por g, que neste exemplo dá

$$\frac{1}{3}x^2 + \frac{1}{9}x + 1$$

Encerramos observando que, como o algoritmo euclidiano efetua apenas divisões, então se $f, g \in K[x]$, tanto seu máximo divisor comum d como os polinômios a e b da relação $d = af + bg$ têm todos os seus coeficientes em K. Portanto, como na caso da divisão, se L for um corpo contendo K e se calcularmos d, a e b considerando f e g como elementos de L, obteremos exatamente os mesmos valores que teriam sido encontrados se tomados como elementos de K.

6. Fatoração de polinômios

Nesta seção discutiremos como fatorar polinômios, de maneira semelhante a dos inteiros em primos. Começaremos com algumas noções gerais, que se aplicam a qualquer anel, mas o único caso que trataremos em detalhe é o do anel de polinômios em uma variável sobre um corpo, denotado por K ao longo de toda a seção.

Seja A um anel e $a \in A$. Dizemos que um elemento não invertível $d \in A$ é um *fator próprio* de a, se existe outro elemento não invertível $c \in A$ tal que $a = dc$. O elemento c é conhecido como o *co-fator* de d em a. Note que precisamos supor que nem c, nem d, são invertíveis na definição acima porque, do contrário, a seria um fator próprio de si mesmo. Mas isto, evidentemente, não é o que queremos. Quando a e d diferem apenas pela multiplicação por um elemento invertível de A, dizemos que são *associados*. Um elemento $q \in A$ é *irredutível* se não é invertível, e não tem fatores próprios. Por exemplo, quando $A = \mathbb{Q}[x]$

$$(x-1)(x-2) \quad \text{e} \quad (x-2)(x-3)^2$$

são fatores próprios de

$$f = 5(x-1)^2(x-2)(x-3)^2,$$

ao passo que

$$(x-1)^2(x-2)(x-3)^2$$

é um associado de f.

O caso mais importante em que aplicaremos estas definições ocorre justamente quando $A = D[x]$ é um anel de polinômios sobre um domínio D. Digamos que $f \in A$, e que g é um fator de f com co-fator h. Aplicando a aditividade dos graus ao produto gh, vemos que

$$\text{grau}(f) = \text{grau}(g) + \text{grau}(h).$$

Como os únicos invertíveis em A são os elementos invertíveis de D, então $\text{grau}(h) > 0$. Logo, $\text{grau}(g) < \text{grau}(f)$. Por outro lado, os graus de g e h não podem ser ambos maiores que $\text{grau}(f)/2$, ou sua soma excederia $\text{grau}(f)$. Portanto, se f não for irredutível então:

- todos os seus fatores próprios têm grau menor que $\text{grau}(f)$;
- pelo menos um fator de f tem grau menor que a metade de $\text{grau}(f)$.

Como consequência das observaçõs acima, temos que qualquer polinômio de grau um em $D[x]$ é irredutível. Se D for o corpo dos números complexos, estes serão os únicos polinômios irredutíveis de $\mathbb{C}[x]$. Para entender isto precisamos relacionar os fatores lineares de um polinômio

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in D[x]$$

com suas raízes. Lembre-se que um elemento $\alpha \in D$ é uma *raiz* de $f(x)$ se

$$f(\alpha) = a_n \alpha^n + \cdots + a_1 \alpha + a_0 = 0.$$

LEMA 2.4. *Seja D um domínio e $f \in D[x]$. Então $\alpha \in D$ é uma raiz de f se, e somente se, $x - \alpha$ divide f.*

DEMONSTRAÇÃO. Suponhamos que $\alpha \in D$ é raiz de f. Dividindo f por $x - \alpha$ podemos escrever

$$f(x) = (x-\alpha)q(x) + r. \tag{20}$$

Mas $r = 0$, ou r tem grau menor que 1, que é o grau do divisor $x - \alpha$. Em qualquer dos dois casos, r é uma constante. Substituindo x por α em (20), e levando em conta que α é raiz de $f(x)$, temos

$$0 = f(\alpha) = (\alpha - \alpha)q(\alpha) + r = r,$$

já que r é uma constante e não depende de x. Logo, $f(x) = (x - \alpha)q(x)$; isto é, $x - \alpha$ divide de f. A recíproca é imediata. □

Disto fica fácil deduzir o que queremos, bastando para isto aplicar o teorema fundamental da álgebra, cujo enunciado relembramos abaixo. Uma demonstração deste teorema pode ser encontrada no apêndice A.

TEOREMA FUNDAMENAL DA ÁLGEBRA. *Todo polinômio não constante de $\mathbb{C}[x]$ admite uma raiz complexa.*

Usando o lemma 2.4, o enunciado deste teorema pode ser traduzido como

> todo polinômio não constante de $\mathbb{C}[x]$ admite um fator de grau um (ou fator linear).

Mas isto garante que nenhum polinômio de grau maior que um em $\mathbb{C}[x]$ seja irredutível, confirmando assim nossa afirmação anterior. Contudo, nada semelhante pode ser concluído se o corpo de base for real ou racional. Por exemplo, sobre $\mathbb{R}[x]$ também existem polinômios irredutíveis de grau 2. De fato, qualquer polinômio quadrático real cujo discriminante é negativo não tem raízes em $\mathbb{R}$. Utilizando o lema 2.4 novamente, podemos concluir que um tal polinômio não pode ter fatores lineares em $\mathbb{R}[x]$, de modo que tem que ser irredutível. Sobre $\mathbb{Q}[x]$ a situação é muito mais complicada: qualquer que seja o grau $k > 0$ escolhido, é possível construir um polinômio irredutível de grau k; veja exercício ???.

A maneira pela qual a fatoração de um polinômio depende do corpo ambiente deve ser contrastada às observações anteriores referentes ao resto e ao máximo divisor comum que, como vimos, são independentes do corpo. Precisamos chamar a atenção para a independência do resto e do máximo divisor comum porque utilizaremos isto adiante e, como mostra o exemplo da fatoração, eles poderiam não ser independentes do corpo de base.

Nosso próximo passo consiste em provar que todo polinômio em $K[x]$ admite uma fatoração em irredutíveis. Ao invés de dar uma demonstração direta, provaremos um resultado mais geral, do qual a fatoração dos polinômios pode ser facilmente deduzida. Faremos isto porque o resultado geral será aplicado em alguns outros exemplos importantes que discutiremos adiante.

Seja A um anel. Diremos que uma função $\nu : A \setminus \{0\} \to \mathbb{N}$ é *multiplicativa*, se satisfaz as duas seguintes condições:

(1) $\nu(ab) = \nu(a)\nu(b)$, quaisquer que sejam $a, b \in A$, e
(2) $\nu(a) = 1$ se, e somente se, a é invertível em A.

Há muitos exemplos de anéis para os quais uma tal função existe. Por exemplo, o módulo de um inteiro é uma função multiplicativa sobre $\mathbb{Z}$. Já no anel

de polinômios $K[x]$, podemos definir a função multiplicativa $2^{(}\mathrm{grau}(f))$. De fato, se $f, g \in K[x]$, a aditividade dos graus nos dá

$$2^{\mathrm{grau}(fg)} = 2^{(\mathrm{grau(f)}+\mathrm{grau}(g))} = 2^{\mathrm{grau}(f)}2^{\mathrm{grau}(g)}.$$

Outros exemplos podem ser encontrados no exercício ???.

A teoria de divisibilidade é bastante bem comportada sobre um anel A no qual está definida uma função multiplicativa. Suponha, por exemplo, que d é um fator próprio de $a \in A$ então $a = dc$, para algum co-fator $c \in A$. Aplicando ν vemos que $\nu(a) = \nu(d)\nu(c)$. Como c não é invertível em A, temos pela condição (2), que $\nu(c) > 1$. Mas isto implica que $\nu(a) > \nu(d)$. Portanto,

(21) se d é fator próprio de a, então $\nu(a) > \nu(d)$.

De posse deste resultado, podemos provar o seguinte teorema de fatoração.

TEOREMA 2.5. *Seja A um anel provido de uma função multiplicativa ν. Todo elemento não nulo de A pode ser escrito na forma*

$$up_1 \cdots p_t,$$

em que u é invertível em A e $p_1, \ldots, p_t$ são elementos irredutíveis de A.

DEMONSTRAÇÃO. Seja $a \in A$ um elemento não nulo. A demonstração será por indução em $\nu(a)$. Se $\nu(a) = 1$, então a é invertível. Neste caso, a fatoração não contém nenhum irredutível, e não há nada a fazer.

Seja $k > 1$ um inteiro, e suponhamos, por indução, que se $z \in A$ e $\nu(z) < k$, então z pode ser fatorado na forma do enunciado do teorema. Digamos que $\nu(a) = k$. Então temos duas possibilidades. A primeira é que a seja, ele próprio, irredutível, o que nos dá uma fatoração com $u = 1$ e $p_1 = a$. A segunda é que a possa ser escrito na forma $a = dc$, em que nem d, nem c, são invertíveis. Neste caso, tanto $\nu(d)$, quanto $\nu(c)$ são menores que $\nu(a) = k$. Portanto, pela hipótese de indução, podemos escrever

$$d = up_1 \cdots p_t, \text{ e } c = vq_1 \cdots q_s,$$

em que u e v são invertíveis e $p_1, \ldots, p_t, q_1, \ldots, q_s$ são irredutíveis em A. Contudo,

$$a = dc = (up_1 \cdots p_t)(vq_1 \cdots q_s) = (uv)p_1 \cdots p_t \cdot q_1 \cdots q_s,$$

é uma fatoração de a na forma do teorema, o que conclui a demonstração. □

Comparando este teorema ao da fatoração de inteiros, vemos que nada nos diz sobre a *unicidade* da fatoração. A razão para isto é muito simplesmente, mesmo em um anel provido de uma função multiplicativa a fatoração *não* precisa ser única. Por exemplo, o anel

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \,|\, a, b \in \mathbb{Z}\},$$

admite uma função multiplicativa dada por

$$N(a + b\sqrt{-5}) = a^2 + 5b^2,$$

como você é chamado a provar no exercício ???. Portanto, todo elemento de $\mathbb{Z}[\sqrt{-5}]$ admite uma fatoração em irredutíveis pelo teorema 2.5. De fato, não é difícil mostrar que 2, 3, $1+\sqrt{-5}$ e seu associado $1-\sqrt{-5}$ são todos quatro irredutíveis em $\mathbb{Z}[\sqrt{-5}]$, veja o exercício ??? para mais detalhes. Contudo,

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

de forma que 6 tem duas fatorações totalmente diferentes em $\mathbb{Z}[\sqrt{-5}]$. Esta igualdade também mostra que embora os irredutíveis 2 e 3 dividem o produto $(1+\sqrt{-5})(1-\sqrt{-5})$, nenhum dos dois divide $1+\sqrt{-5}$, nem $1-\sqrt{-5}$. Assim, uma outra importante propriedade dos primos é violada em $\mathbb{Z}[\sqrt{-5}]$; a saber,

> se um número inteiro primo divide o produto de dois inteiros então tem que dividir um dos fatores.

Não é surpreendente que esta propriedade seja falsa em $\mathbb{Z}[\sqrt{-5}]$ porque, na verdade, ela é equivalente à unicidade da fatoração em irredutíveis.

TEOREMA 2.6. *Seja A um anel no qual cada elemento pode ser fatorado como um produto de irredutíveis. As duas propriedades seguintes são equivalentes:*

(1) *se um irredutível de A divide o produto de dois elementos de A, então tem que dividir um destes dois fatores;*
(2) *a fatoração de um elemento de A em irredutíveis é única a menos de ordem e associados.*

Antes de poder provar o teorema precisamos discutir o que significa a estranha expressão *a menos de ordem e associados* aplicada à unicidade da fatoração em um anel, no enunciado acima. Lembre-se que, mesmo em $\mathbb{Z}$ precisamos tomar alguns cuidados antes de afirmar que a fatoração é única, como agrupar irredutíveis iguais em potências e arranjar os primos em ordem crescente. No caso de um anel qualquer, embora não haja problema em agrupar irredutíveis distintos em potências, arranjá-los em ordem crescente esta fora de cogitação. Nem mesmo um anel tão bem comportado e familiar como o dos polinômios sobre um corpo admite uma ordenação dos elementos. Por sorte este problema é fácil de contornar: basta não considerar a ordem dos fatores como característica relevante para distinguir duas fatorações.

Na verdade há outra hipótese feita sobre a fatoração dos inteiros que tende a passar despercebida: o teorema (quase sempre) só é enunciado para inteiros positivos. Mais precisamente, tanto o inteiro a ser fatorado quanto os primos devem ser números positivos. Se não fizermos isto teremos problemas. Por exemplo, $2 \cdot 3$ e $(-2)(-3)$ são fatorações distintas de 6? Se quisermos estender o teorema da fatoração única a todos os inteiros, positivos ou negativos, então precisaremos ser capazes de arranjar as definições de maneira que estas duas fatorações de 6 sejam indistinguíveis. Note, entretanto, que já temos os conceitos que precisamos para isto, porque 2 e -2 são irredutíveis associados, já que diferem apenas pela multiplicação por -1, que é invertível em $\mathbb{Z}$.

Portanto, mesmo quando tratamos dos inteiros, precisamos considerar como equivalentes primos que se distinguem apenas por serem associados.

Diante destas considerações estamos prontos para dizer o que significa a unicidade da fatoração em uma anel qualquer. Seja, então, A um anel e $a \in A$. Duas fatorações da forma

$$a = up_1 \cdots p_s \text{ e } a = vq_1 \cdots q_t$$

são *iguais a menos de ordem e associados* se $s = t$ e se, reordenando os qs se necessário, temos que p_i é associado de q_i para cada $1 \leq i \leq s$. Observe que as unidades que aparecem nas duas fatorações foram ignoradas nesta definição, simplesmente porque podem ser "absorvidas" em qualquer um dos irredutíveis; afinal, decidimos dizer que p_1 e up_1 são indistinguíveis, já que são associados. Com isto estamos prontos para provar o teorema 2.6.

DEMONSTRAÇÃO. Começamos mostranddo que (2) implica (1) porque é mais fácil. Como p divide o produto ab, então existe $c \in A$ tal que $ab = pc$. Multiplicando as fatorações de a, b em irredutíveis, obtemos uma fatoração de ab. Por outro lado, multiplicando a fatoração de c em irredutíveis por p, obtemos uma fatoração de pc. Como $ab = pc$ suas fatorações são iguais. Contudo, p é irredutível e aparece na fatoração de pc. Pela unicidade da fatoração, um associado de p deve ser um dos irredutíveis na fatoração de ab. Pela maneira como construímos esta fatoração, ele tem que ser fator de a ou de b. Portanto, p divide a ou b, o que conclui esta parte da demonstração.

Passando, agora, a outra parte, queremos mostrar que (1) implica (2). Há duas coisas que precisamos ter em mente. A primeira é que estamos supondo que todo elemento de A pode ser fatorado em irredutíveis; a segunda é que a definição de unicidade da fatoração que adotamos requer que a quantidade de fatores irredutíveis seja sempre a mesma para quaisquer duas fatorações de um mesmo elemento. Isto sugere proceder por indução na quantidade de fatores irredutíveis do elemento. Mais precisamente, queremos provar que a afirmação

> se um elemento de A tem uma fatoração com k fatores irredutíveis, então esta fatoração é única a menos de ordem e associados

é verdadeira para todo $k \geq 1$.

A base da indução é facilmente verificada. De fato, se $a \in A$ admite uma fatoração com um único irredutível, então a é associado a um irredutível e, portanto, é ele próprio irredutível. Em particular, só podemos escrever a como produto de dois fatores em A se um dos fatores for associado a a e o outro for um invertível. Mas isto significa que toda fatoração de a tem um único irredutível, confirmando a validade da base.

Suponha, então, que, para algum inteiro $k \geq 1$,

> a fatoração é única a menos de ordem e associados para todo elemento $a \in A$ que admite uma fatoração com k fatores irredutíveis.

Vamos provar que a unicidade se propaga para os elementos que admitem fatorações em $k+1$ irredutíveis. Seja a um tal inteiro e

$$a = p_1 \cdots p_{k+1}$$

sua fatoração em $k+1$ irredutíveis. Para mostrar a unicidade da fatoração, vamos imaginar que alguém descobriu uma outra fatoração de a, digamos

$$a = q_1 \cdots q_s$$

aparentemente diferente da anterior. Mostraremos que, de fato, têm que ser indistinguíveis a menos de ordem e associados.

Para começar, é claro que o irredutível p_1 divide

$$a = q_1 \cdots q_s = q_1(q_2 \cdots q_s)$$

de modo que, por (1), tem que dividir q_1 ou $q_2 \cdots q_s$. Se dividir q_1, então, como ambos são irredutíveis, têm que ser associados. Se não dividir q_1, então vai dividir

$$q_2 \cdots q_s = q_2(q_3 \cdots q_s)$$

e, novamente por (1), vai ter que dividir q_2 ou $q_3 \cdots q_s$. No primeiro caso, p_1 é associado a q_2; no segundo o argumento continua como antes. Como a quantidade de irredutíveis é finita, podemos concluir que p_1 tem que ser associado a um dos qs. Rearranjando a ordem dos qs, se for preciso, podemos supor que p_1 e q_1 são associados. Digamos que $q_1 = up_1$ para algum invertível u. Neste caso, podemos reescrever $q_1 \cdots q_s$ na forma

$$up_1q_2 \cdots q_s$$

Logo, Como temos duas fatorações do mesmo elemento $a \in A$, obtemos

$$p_1 \cdot p_2 \cdots p_{k+1} = up_1 \cdot q_2 \cdots q_s.$$

Dividindo tudo por p_1,

$$p_2 \cdots p_{k+1} = uq_2 \cdots q_s$$

que é um elemento de A, que chamaremos de b. Ocorre que a fatoração $p_2 \cdots p_{k+1}$ de b tem k irredutíveis. Assim, pela hipótese de indução, b tem uma única fatoração a menos de ordem e associados. Mas isto significa que $s = k+1$ e que, reordenando os qs se necessário for, temos que p_j e q_j são associados para todo $2 \leq j \leq k+1$. Contudo, como já sabemos que p_1 e q_1 também são associados, podemos concluir que a segunda fatoração obtida para a coincide com a primeira a menos de ordem e associados. Isto completa o passo de indução e confirma a unicidade para todos os elementos de A, como queríamos mostrar. □

O teorema de fatoração para polinômios em uma variável sobre um corpo é um corolário dos teoremas 2.5 e 2.6, com uma ajuda expressiva do algoritmo euclidiano estendido. Porém, antes de enunciá-lo e prová-lo, convém reescrever a fatoração de maneira que distinguir duas fatorações se torna quase tão simples quanto no caso dos inteiros. O ponto chave é que, como vimos na página 40, os únicos elementos invertíveis de um anel de polinômios são os

invertíveis do anel de base. Portanto, em nosso caso em que a base é um corpo K, todas as constantes não nulas são invertíveis. Isto significa que qualquer polinômio pode ser escrito como o produto de uma constante não nula com um polinômio cujo coeficiente líder é igual a 1. Mais precisamente, se

$$f = a_n x^n + \cdots + a_1 x + a_0, \text{ e } a_n \neq 0$$

então

$$f = a_n \left(x^n + \cdots + \frac{a_1}{a_n} x + \frac{a_0}{a_n} \right).$$

Um polinômio cujo termo líder é igual a um é chamado de *mônico*. Portanto, todo polinômio pode ser escrito como o produto do seu coeficiente líder por um polinômio mônico. A grande vantagem em trabalhar com polinômios mônicos está em que

> dois polinômios mônicos são associados se, e somente se, são iguais.

Afinal, multiplicar por uma constante não nula diferente de um altera o coeficiente líder e faz com que o polinômio deixe de ser mônico.

Seja, então, $f \in K[x]$ um polinômio que pode ser fatorado como

$$f = up_1 \cdots p_s,$$

em que os ps são polinômios irredutíveis e u é uma unidade. Escrevendo

$$p_i = c_i q_i \text{ com } c_i \in K \text{ e } q_i \text{ mônico}$$

para todo $1 \leq i \leq s$, temos que

$$f = (uc_1 \cdots c_s) q_1 \cdots q_s,$$

com $uc_1 \cdots c_s \in K \setminus \{0\}$. Como os qs são mônicos, podemos agrupar polinômios iguais em potências, como fazemos com inteiros, o que nos leva ao seguinte enunciado.

TEOREMA 2.7. *Seja K um corpo. Todo polinômio não nulo $f \in K[x]$ pode ser escrito na forma*

$$f = ap_1^{e_1} \cdots p_s^{e_s} \tag{22}$$

em que $a \in K$, $p_1, \ldots, p_s$ são polinômios irredutíveis mônicos distintos e os expoentes $e_1, \ldots, e_s$ são inteiros positivos. Além disto, esta maneira de escrever f é única, a menos da ordem dos fatores.

DEMONSTRAÇÃO. A existência da fatoração nesta forma é consequência imediata do Teorema 2.5 e dos comentários que precedem o enunciado, uma vez que $K[x]$ admite 2^{grau} como função multiplicativa. A unicidade será consequência do item (2) do teorema 2.6 se formos capazes de provar que (1) é verdadeiro em $K[x]$. Para isto usaremos o algoritmo euclidiano estendido. Seja p um polinômio irredutível e digamos que p divide o produto dos polinômios f e g em $K[x]$. Se p dividir f, nada há a fazer. Mostraremos que se p não divide f, mas divide fg, então tem que dividir g. Contudo, como p é

irredutível, o fato de não dividir f implica que $\mathrm{mdc}(p, f) = 1$. Assim, pelo algoritmo euclidiano estendido, existem polinômios q_1 e q_2 em $K[x]$ tais que

$$q_1 f + q_2 p = 1.$$

Multiplicando esta equação por g, vemos que

$$g = q_1 \cdot fg + q_2 g \cdot p.$$

Como p divide fg, concluímos que p divide ambas as parcelas à direita desta última equação. Portanto, p divide g, e a demonstração está completa. □

Não parece justo abandonar este tema neste ponto. Afinal de contas, este livro dá ênfase a métodos efetivos. Por isso descreveremos um algoritmo simples que permite fatorar polinômios. Contudo, não discutiremos os algoritmos de fatoração verdadeiramente eficientes: para isso precisaríamos de outro livro igual a este.

7. Fatoração à la Kronecker

A primeira pergunta que precisamos fazer é: qual será o corpo de base dos polinômios que pretendemos fatorar? Como já mencionamos acima, a fatoração depende da escolha do corpo de base. Por exemplo, a fatoração de

$$x^4 - x^2 - 2$$

sobre $\mathbb{Q}$ é

$$(x^2 - 2)(x^2 + 1),$$

já sobre $\mathbb{R}$ é

$$(x - \sqrt{2})(x + \sqrt{2})(x^2 + 1);$$

ao passo que sobre $\mathbb{C}$ é

$$(x - \sqrt{2})(x + \sqrt{2})(x + i)(x - i).$$

Já vimos que os únicos polinômios irredutíveis em uma variável com coeficientes complexos são os de grau 1. Mas isto significa que fatorar polinômios em $\mathbb{C}[x]$ é equivalente a encontrar suas raízes. De posse de uma fatoração sobre $\mathbb{C}$, obtemos facilmente uma fatoração sobre $\mathbb{R}$, bastando para isto agrupar os fatores que correspondem a raízes complexas conjugadas; veja exercício ???. Observe, entretanto, que para chegar a calcular estas fatorações de maneira exata, precisamos ser capazes de representar números reais e complexos (não necessariamente racionais) no computador. Voltaremos a discutir esta questão no capítulo 8, mas desde já você deve ter consciência de que não há uma solução geral realmente satisfatória se queremos efetuar apenas cálculos exatos.

Com isto, resta-nos apenas analisar a fatoração de polinômios sobre $\mathbb{Q}[x]$. Este tema foi estudado por vários matemáticos, desde o século XVII, entre eles Newton, Nicolau Bernoulli e L. Kronecker. Entretanto, métodos realmente eficientes só foram desenvolvidos a partir da introdução dos computadores na segunda metade do século XX. Para uma história do problema até o século XIX, consulte [**52**]. Uma resenha do estado atual da arte pode ser encontrada

em [????]. Descreveremos a seguir apenas o método de Kronecker que, apesar de pouco eficiente, é muito elementar. Este algoritmo encontra apenas um fator próprio (se existir) de um polinômio dado. Para obter a fatoração completa basta aplicar o algoritmo recursivamente; veja o exercício ???.

Seja $f \in \mathbb{Z}[x]$ o polinômio que desejamos fatorar. Vamos escrever o grau de f na forma $2n$, se for par, ou $2n+1$, se for ímpar. Já sabemos que, se não for irredutível, f deve ter um fator de grau menor ou igual a n. É este o fator que vamos procurar. Se ele não existir, então podemos estar certos de que f é irredutível.

Para começar, escolha inteiros distintos $r_0, \ldots, r_n$, e construa os polinômios

$$\ell_i(x) = \frac{(x-r_0)\cdots(x-r_{i-1})(x-r_{i+1})\cdots(x-r_n)}{(r_i-r_0)\cdots(r_i-r_{i-1})(r_i-r_{i+1})\cdots(r_i-r_n)},$$

para $i = 0, \ldots, n$. Observe que, no polinômio ℓ_i, o fator $x - r_i$ está ausente do numerador, e o fator $r_i - r_i$ do denominador—do contrário estaríamos encrencados. Estes polinômios foram escolhidos de forma que

$$\ell_i(r_j) = \begin{cases} 1 & \text{se } j = i \\ 0 & \text{se } j \neq i \end{cases} \tag{23}$$

como pode ser facilmente verificado. Note que isto nos dá $n+1$ polinômios de grau menor ou igual a n.

PROPOSIÇÃO 2.8. *Os polinômios $\ell_0, \ldots, \ell_n$ formam uma base do espaço vetorial dos polinômios de grau menor ou igual a n sobre $\mathbb{Q}$.*

DEMONSTRAÇÃO. A base mais conhecida deste espaço é

$$1, x, x^2, \ldots, x^n,$$

que tem $n+1$ elementos. Como o conjunto $\{\ell_0, \ldots, \ell_n\}$ também tem $n+1$ elementos, basta provar que é linearmente independente e podemos ter certeza de que se trata de uma base. Suponhamos que

$$c_0\ell_0 + \cdots + c_n\ell_n = 0,$$

em que $c_0, \ldots, c_n \in \mathbb{Q}$. Substituindo $x = r_j$ nesta expressão, obtemos da equação (23) que $c_j = 0$. Fazendo isto para cada $0 \leq j \leq n$, concluímos que cada um dos c_j é nulo, o que prova que o conjunto dos ℓs é linearmente independente. □

Suponhamos, agora, que g seja um fator próprio de f, de grau menor ou igual a n, com co-fator h. Pela proposição 2.8, podemos escrever g como combinação linear dos ℓs com coeficientes racionais, digamos

$$g = c_0\ell_0 + \cdots + c_n\ell_n.$$

Para achar g resta-nos apenas calcular os cs. Contudo, $g(r_j) = c_j$, para $0 \leq j \leq n$. Infelizmente, isto não parece nos levar a parte alguma, já que não conhecemos c_j nem g.

A saída consiste em assumir que o fator g tem coeficientes inteiros. Isto parece razoável, porque (subrepiticiamente) já havíamos introduzido a hipótese de que todos os coeficientes de f eram inteiros. Voltaremos a discutir este ponto com mais detalhes ao final da descrição do algoritmo de Kronecker. Assumindo, por enquanto, que g tem coeficientes inteiros, e lembrando que $f = gh$, concluímos que $c_j = h(r_j)$ é fator de

$$f(r_j) = g(r_j)h(r_j).$$

Como f é conhecido, podemos fatorar o inteiro $f(r_j)$ e testar todas as possibilidades de fatores como possíveis valores para c_j. Naturalmente isto tem que ser feito para cada $0 \leq j \leq n$.

A má notícia é que os fatores de $f(r_j)$ que precisamos considerar incluem todos os possíveis divisores deste número, tanto os positivos quanto os negativos, e não apenas os seus fatores primos. Precisamos até incluir ± 1 e $\pm f(r_j)$ entre este fatores. Isto significa que, em geral, teremos inúmeras possibilidades para considerar. Por exemplo, no melhor caso possível, $f(r_j)$ dá primo, de modo que tem apenas os 4 fatores ± 1 e $\pm f(r_j)$. Contudo, se isto ocorrer para cada um dos $0 \leq j \leq n$, teremos 4^n maneiras posssíveis de escolher a $n+1$-upla $(c_0, \ldots, c_n)$. Assim, se $n = 10$ isto já dá 1048576 possibilidades. Levando em conta que só raramente os $f(r_j)$ serão primos, é fácil entender porque o método é pouco eficiente.

Vejamos um exemplo de fatoração usando o método de Kronecker. Considere o polinômio

$$f = x^7 + 4x^6 + 7x^5 + 21x^4 + 21x^3 + 2x^2 + 35x + 7.$$

Como a parte inteira da metade do grau de f é 3, vamos procurar por fatores de grau 3. Escolhendo $r_i = i$ para $0 \leq i \leq 3$, teremos uma base fomada pelos seguintes polinômios

$$\begin{aligned}
\ell_0 &= -\frac{(x-1)(x-2)(x-3)}{6} \\
\ell_1 &= \frac{x(x-2)(x-3)}{2} \\
\ell_2 &= -\frac{x(x-1)(x-3)}{2} \\
\ell_3 &= \frac{x(x-1)(x-2)}{6}.
\end{aligned}$$

Em seguida, precisamos fatorar $f(i)$, para $0 \leq i \leq 3$. Reunimos os valores de $f(i)$ e seus divisores na tabela 1.

Denotando por D_i o conjunto dos divisores de $f(i)$, devemos agora, escolher $c_i \in D_i$ de todas as maneiras possíveis, construir os polinômios

$$c_0\ell_0 + c_1\ell_1 + c_2\ell_2 + c_3\ell_3$$

e verificar, um a um, se dividem f. Paramos ao encontrar o primeiro fator. Para termos certeza de que escolhemos os divisores em todas as combinações

i	$f(i)$	Divisores de $f(i)$
0	7	$\pm 1, \pm 7$
1	98	$\pm 1, \pm 2, \pm 7, \pm 14, \pm 49, \pm 98$
2	1197	$\pm 1, \pm 3, \pm 7, \pm 9, \pm 19, \pm 21, \pm 57, \pm 63,$ $\pm 133, \pm 171, \pm 399, \pm 1197$
3	9202	$\pm 1, \pm 2, \pm 43, \pm 86, \pm 107, \pm 214, \pm 4601, \pm 9202$

TABELA 1. Tabela de divisores dos $f(i)$

possíveis, ordenamos as 4-uplas de $S = D_0 \times D_1 \times D_2 \times D_3$ em ordem lexicográfica. Isto significa que

$$(d_0, d_1, d_2, d_3) < (d'_0, d'_1, d'_2, d'_3)$$

se, para algum $0 \leq k \leq 4$ temos que $d_i = d'_i$ para $0 \leq i \leq k$, porém $d_k < d'_k$. Em outras palavras, lendo as 4-uplas da esquerda para a direita, a primeira posição diferente entre as duas 4-uplas deve ser menor na 4-upla à esquerda do sinal $<$. Por exemplo, a menor das 4-uplas em S é $(-7, -98, -1197, -9202)$, a segunda menor é $(-7, -98, -1197, -4601)$, e assim por diante.

A expressão *ordem lexicográfica* tem sua origem no fato de que, se substituíssimos estas 4-uplas de números por sequências de letras, o que obteríamos seria a ordem em que as palavras são ordenadas em um dicionário. Em grego, *lexis* significa palavra; donde derivam *léxico*, o conjunto das palavras de uma língua, e lexicógrafo, que em seu famoso dicionário da língua inglesa publicado em 1755 Samuel Johnson descreveu como

> um escritor de dicionarios; um ??? inofensivo que se ocupa em descobrir a origem e detalhar o significado das palavras.

Como veremos nos próximos capítulos, a ordem lexicográfica desempenha um papel muito importante nos algoritmos que lidam com polinômios em várias indeterminadas.

Aplicando o algoritmo de Kronecker aos elementos de S listados em ordem lexicográfica, teremos que verificar 5877 elementos antes de encontrar a 4-upla $(-1, -7, -19, -43)$, que nos dá o fator

$$-\ell_0 - 7\ell_1 - 19\ell_2 - 43\ell_3 = x^3 + 5x + 1.$$

Voltando à questão da eficiência deste algoritmo, note que foi necessário testar mais de 5800 elementos de S para achar um fator de um polinômio cujo grau é apenas 7. Imagine o que aconteceria se f tivesse grau 20. Entretanto, usando métodos mais avançados é possível fatorar polinômios de grau 20 em apenas alguns milisegundos. Certamente este algoritmo não era viável em 1882, ano em que foi introduzido por Kronecker. Isto talvez tenha contribuído para que Kronecker dedicasse a ele apenas uma página, em um artigo de mais de 122 páginas, que trata da teoria dos números algébricos.

Antes de encerrar a seção precisamos justificar porque é suficiente buscar fatores com coeficientes inteiros, quando estamos na verdade interessados em fatorar polinômios em $\mathbb{Q}[x]$. Para justificar isto, basta mostrar que se $g \in \mathbb{Q}[x]$ é um fator próprio, não constante, de um polinômio com coeficients inteiros, então g também tem coeficientes inteiros. Este fato é consequência de um lema de Gauss que provaremos a seguir.

Para facilitar o enunciado do lema de Gauss é conveniente introduzir a seguinte definição. Se $f \in \mathbb{Z}[x]$, então o máximo divisor comum dos coeficientes de f é o *conteúdo* de f, denotado por $\mathrm{cont}(f)$. Um polinômio cujo conteúdo é igual a 1 é chamado de *primitivo*. Observe que todo polinômio mônico é primitivo.

LEMA DE GAUSS. *O produto de polinômios primitivos é primitivo.*

DEMONSTRAÇÃO. Sejam

$$f = a_n x^n + \cdots + a_1 x + a_0 \quad \text{e} \quad g = b_m x^m + \cdots + b_1 x + b_0$$

polinômios primitivos em $\mathbb{Z}[x]$. A demonstração do lema consiste em mostrar que $\mathrm{cont}(fg)$ não é divisível por nenhum primo. Assim, pelo Teorema da Fatoração Única para inteiros, deveremos ter que $\mathrm{cont}(fg) = 1$.

Seja $p > 0$ um número primo. Como $\mathrm{cont}(f) = 1$, o primo p não pode dividir todos os coeficientes de f. Seja r o menor inteiro não negativo para o qual a_r não é divisível por p. Da mesma forma, p não pode dividir todos os coeficientes de g, e s será o menor inteiro não negativo para o qual b_s não é divisível por p. Contudo, o coeficiente c_{r+s} de x^{r+s} em fg é

$$a_0 b_{r+s} + a_1 b_{r+s-1} + \cdots + a_{r-1} b_{s+1} + a_r b_s + a_{r+1} b_{s-1} + \cdots + a_{r+s} b_0.$$

Como p divide tanto $a_0, \ldots, a_{r-1}$ quanto $b_0, \ldots, b_{s-1}$, temos que

$$c_{r+s} \equiv a_r b_s \not\equiv 0 \pmod{p},$$

já que nem a_r, nem b_s são divisíveis por p. Portanto, p não pode dividir todos os coeficientes de fg. Como isto vale para qualquer primo p, podemos concluir que fg tem que ser primitivo. □

Como consequência imediata do lema de Gauss, temos a seguinte fórmula: se $f, g \in \mathbb{Z}[x]$, então

$$\mathrm{cont}(fg) = \mathrm{cont}(f)\mathrm{cont}(g).$$

O resultado que desejamos é um corolário desta fórmula. Para simplificar o enunciado, introduzimos a seguinte notação. Dado $g \in \mathbb{Q}[x]$, podemos escrevê-lo na forma,

$$g = \frac{a}{d}\hat{g},$$

em que $a, d \in \mathbb{Z}$ são primos entre si e $\hat{g} \in \mathbb{Z}[x]$ é um polinômio primitivo. Chamaremos $\hat{g}$ de *parte primitiva* de g.

COROLÁRIO 2.9. *Seja $f \in \mathbb{Z}[x]$ um polinômio primitivo. Se $g \in \mathbb{Q}[x]$ é fator de f, então sua parte primitiva também é.*

DEMONSTRAÇÃO. Suponhamos que o co-fator de g em f é um polinômio $h \in \mathbb{Q}[x]$, então $f = gh$. Podemos escrever

$$g = \frac{a_1}{d_1}\hat{g} \quad \text{e} \quad h = \frac{a_2}{d_2}\hat{h};$$

em que a_1/d_1 e a_2/d_2 são frações reduzidas e $\hat{g}, \hat{h} \in \mathbb{Z}[x]$ são as partes primitivas de g e h, respectivamente. Multiplicando tudo por $d_1 d_2$, obtemos

$$d_1 d_2 f = a_1 a_2 \hat{g}\hat{h}.$$

Calculando o conteúdo de ambos os membros e usando o lema de Gauss,

$$d_1 d_2 = a_1 a_2;$$

donde,

$$gh = \hat{g}\hat{h}.$$

Portanto,

$$f = \hat{g}\hat{h},$$

tem como fator o polinômio $\hat{g} \in \mathbb{Z}[x]$. □

Como um polinômio irredutível $f \in \mathbb{Z}[x]$ tem que ser primitivo, podemos concluir do lema que f tem que ser irredutível sobre $\mathbb{Q}[x]$. De fato, se tivesse algum fator em $\mathbb{Q}[x]$ a parte primitiva deste fator dividiria f, contradizendo sua irredutibilidade em $\mathbb{Z}[x]$.

8. Comentários e complementos

Este capítulo se distingue pela introdução de alguns dos conceitos fundamentais utilizados neste livro, principalmente

- anéis, domínios e corpos;
- ideais;
- anéis de polinômios em uma variável e suas operações básicas.

Dentre os resultados mais importantes que acabamos de discutir, destacamos:

- o algoritmo de divisão de polinômios;
- o algoritmo euclidiano estendido;
- a existência e unicidade da fatoração de polinômios com coeficientes em um corpo.

Na verdade, o principal algoritmo neste livro—conhecido como algoritmo de Buchberger e apresentado no capítulo 5—pode ser encarado como uma generalização do algoritmo euclidiano estendido. Já o algoritmo de divisão será estendido a polinômios em várias indeterminadas no capítulo 4 e, a partir daí, será componente essencial de nossos cálculos.

No próximo capítulo introduziremos os anéis de polinômios em várias indeterminadas e estudaremos algumas de suas propriedades básicas. Veremos que os ideais destes anéis estão intimamente ligados a figuras geométricas. Isto nos permitirá retomar a aproximação do porto seguro que vislumbramos com a introdução dos conjuntos algébricos na seção 7 do capítulo 1, e que perdemos de vista ao longo deste capítulo.

Um último comentário. Os anéis e ideais, dos quais trata este capítulo, constituem uma teoria importante e bastante vasta da álgebra, com aplicações na teoria de números, na geometria algébrica, na análise e em várias outras áreas da matemática. Como nossas aplicações neste livro são de natureza basicamente geométrica, o anel ao qual nos dedicaremos com maior afinco, a partir do próximo capítulo, será o dos polinômios em várias indeterminadas. Porém, há muitos outros exemplos importantes de anéis, em alguns dos quais a multiplicação não é comutativa; como ocorre com as matrizes quadradas de ordem $n \geq 2$ sobre um corpo. Na verdade, os anéis não comutativos desempenham um papel mais importante que os comutativos na física quântica. Por exemplo, o famoso *princípio da incerteza* de Heisenberg é consequência da não comutatividade dos operadores que descrevem a posição e o momento de uma partícula na álgebra da mecânica quântica. Veja, por exemplo, [**14**] para mais detalhes. Afinal, como alguém já disse, o mundo natural é intrinsecamente não comutativo: se não está convencido, experimente pôr as meias depois do sapato, em vez dos sapatos depois das meias.

9. Exercícios

1. Prove que $\mathbb{Z}_6$ não está contido em nenhum corpo.

2. Mostre que se A é um anel, então,
   (a) $0 \cdot a = 0$ para todo $a \in A$;
   (b) a adição não pode ter mais do que um elemento neutro;
   (c) a multiplicação não pode ter mais do que um elemento neutro;
   (d) cada elemento de A tem um único simétrico;
   (e) cada elemento invertível de A tem um único inverso.

3. Seja $\mathbb{Z}_n$ o conjunto das classes de equivalência de $\mathbb{Z}$ para a congruência módulo n. Denote por $\overline{a}$ a classe de um inteiro a em $\mathbb{Z}_n$.
   (a) Mostre que $\overline{a}$ é divisor de zero em $\mathbb{Z}_n$ se, e somente se, $\mathrm{mdc}(a, n) \neq 1$.
   (b) Mostre que se n é composto então $\mathbb{Z}_n$ não é um domínio.
   (c) Mostre que $\overline{a}$ tem inverso em $\mathbb{Z}_n$ se, e somente se, $\mathrm{mdc}(a, n) = 1$.
   (d) Mostre que $\mathbb{Z}_n$ é um corpo se, e somente se, n é primo.

4. Seja A um anel. Mostre que, para todo $a \in A$, temos que $(-1)a = -a$. Em outras palavras, o simétrico de a pode ser calculado multiplicando a pelo simétrico de 1.

5. Sejam A e B anéis. A *soma direta* $A \oplus B$ é definida como sendo o conjunto cujos elementos são os pares (a, b) com $a \in A$ e $b \in B$. Podemos definir operações de adição e multiplicação em $A \oplus B$ pela regras:
$$(a, b) + (a', b') = (a + a', b + b');$$
$$(a, b) \cdot (a', b') = (a \cdot a', b \cdot b');$$
   quaisquer que sejam $a, a' \in A$ e $b, b' \in B$. Prove que $A \oplus B$ é um anel. Identifique seu zero e sua unidade.

6. Mostre que a soma direta de dois domínios (até mesmo de dois corpos) sempre contém divisores de zero.

7. Seja A um anel e $\mathcal{F}(A)$ o conjunto de todas as funções de A em A. Definimos uma adição e uma multiplicação em $\mathcal{F}(A)$ por
$$(f+g)(a) = f(a) + g(a) \quad \text{e} \quad (fg)(a) = f(a)g(a)$$
quaisquer que sejam $f, g \in \mathcal{F}(A)$. Mostre que estas operações fazem de $\mathcal{F}(A)$ um anel. Identifique o zero e a identidade deste anel.

8. Prove todas as propriedades de $Q(D)$ que foram deixadas como exercício na seção 2.

9. Mostre que todo domínio com um número finito de elementos é um corpo.
SUGESTÃO: Aplique o princípio da casa do pombo, levando em conta que, se A é um domínio, finito, e $0 \neq a \in A$, então o conjunto das potências de a tem que ser finito.

10. Prove, por indução em n, a fórmula que dá o coeficiente do n-ésimo termo do produto de dois polinômios em uma variável.

11. Prove que a fórmula do binômio de Newton vale em qualquer anel comutativo. Mais precisamente, mostre que se A é um anel comutativo e $a, b \in A$, então
$$(a+b)^s = \sum_{i=1}^{s} \binom{s}{i} a^i b^{s-i},$$
para qualquer inteiro positivo s.

12. Explique porque, no algoritmo da divisão da seção 3 exigimos que o coeficiente líder do divisor fosse invertível, e não apenas que dividisse o coeficiente líder do dividendo.

13. Calcule os quocientes e restos das divisões dos seguintes polinômios de $\mathbb{C}[x]$:
(a) $x^4 + x + 2$ por $x^3 + 3x^2 + 1$;
(b) $2x^5 + 1$ por $\sqrt{2}x^2 + x$;
(c) $7x^8 - 3x^4 - 1$ por $ix^3 - 7x^2 - 2x - 1$;
(d) $x^n - 1$ por $x - 1$;
em que $n > 0$ é um inteiro.

14. Seja A um anel e I um subconjunto não vazio de A que satisfaz as condições (2) e (3) da definição de ideal. Mostre que $0 \in I$.
SUGESTÃO: Como I é não vazio, existe um $a \in I$. Calcule $a + (-1)a$ e explique porque pertence a I.

15. Quais dos seguintes conjuntos são ideais de $\mathbb{C}[x]$?
(a) $\{f \in \mathbb{C}[x] \mid f(0) = 1\}$;

(b) $\{f \in \mathbb{C}[x] \mid f(1) = 0\}$;
(c) $\{f \in \mathbb{C}[x] \mid f(1) = 1\}$;
(d) $\{f \in \mathbb{C}[x] \mid f(1) = f(2) = 0\}$;
(e) $\{f \in \mathbb{C}[x] \mid f^2$ é divisível por $x^2 + 1\}$;

16. Sejam I e J ideais de um anel A. Considere o conjunto

$$I + J = \{x + y : x \in I \text{ e } y \in J\}.$$

(a) Mostre que $I + J$ e $I \cap J$ também são ideais de A.
(b) Sob que circunstâncias $I \cup J$ é um ideal de A?

17. Determine um gerador para cada um dos subconjuntos do exercício anterior que sejam ideais de $\mathbb{C}[x]$.

18. Aplique o algoritmo euclidiano estendido a cada um dos dois polinômios dados no exercício ???.

19. Quais dos seguintes ideais de $\mathbb{Z}[x]$ são principais?
(a) $\{f \in \mathbb{Z}[x] \mid f(0) = 0\}$;
(b) $\{f \in \mathbb{C}[x] \mid f(1) = 0$ é divisível por $2\}$;
(c) $\{f \in \mathbb{C}[x] \mid f(3) = 0$ ou f é divisível por $5\}$;

20. Sejam $f = a_n x^n + \cdots + a_0$, $g = b_m x^m + \cdots + b_0$ e $h = c_k x^k + \cdots + c_0$, polinômios com coeficientes inteiros, tais que $f = gh$ e seja $p > 0$ um número primo. Mostre que se $i \geq 0$ é o menor inteiro tal que p não divide b_i e $j \geq 0$ o menor inteiro tal que p não divide c_j então p não divide $a_i b_j$.

21. Seja $f = a_n x^n + \cdots + a_0$, um polinômio com coeficientes inteiros e $p > 0$ um número primo. Use o exercício anterior para provar que se
- p divide a_i para $0 \leq i \leq n - 1$, mas
- p não divide a_n e p^2 não divide a_0;

então f tem que ser um polinômio irredutível sobre $\mathbb{Z}[x]$. Este resultado é conhecido como *Critério de Eisenstein*.

22. Prove que um polinômio de $\mathbb{Z}[x]$ que satisfaz as condições do Critério de Eisenstein é irredutível sobre $\mathbb{Q}[x]$ (e não apenas sobre $\mathbb{Z}[x]$).

23. Fatore os seguintes polinômios em $\mathbb{Q}[x]$ usando o algoritmo de Kronecker:
(a) $x^4 - x^3 + 2x^2 - x + 1$;
(b) $x^5 + x^4 + 1$.

24. Seja d um número inteiro (positivo ou negativo) e considere o conjunto

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\},$$

Note que se $d < 0$ e $b \neq 0$ então $a + b\sqrt{d}$ será um número complexo. Prove que $\mathbb{Z}[\sqrt{d}]$ é um domínio.

25. Nos exercícios ??? a ??? estudaremos as propriedades deste anel sob a condição extra de que d *não* é um quadrado perfeito. Explique porque o caso em que d é um quadrado perfeito não precisa ser estudada.

26. Se $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, então seu *conjugado* é definido como sendo o número
$$\widehat{\alpha} = a - b\sqrt{d}.$$
Sejam $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$.
    (a) Para que valores de d o conjugado definido acima coincide com o conjugado de um número complexo?
    (b) Mostre que
    $$\widehat{\alpha\beta} = \widehat{\alpha}\widehat{\beta}.$$
    (c) O que se pode dizer sobre um elemento de $\mathbb{Z}[\sqrt{d}]$ que é igual ao seu conjugado?

27. Se $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, então sua *norma* é definida por
$$N(\alpha) = \alpha \cdot \widehat{\alpha}.$$
    (a) Mostre que $N(\alpha)$ é sempre um número inteiro.
    (b) Mostre que se $d < 0$ então $N(\alpha)$ é sempre um inteiro não negativo.
    (c) Mostre que se $d < 0$ então $N(\alpha) = 0$ se, e somente se, $\alpha = 0$.
    (d) Quais os elementos de $\mathbb{Z}[\sqrt{2}]$ cuja norma é igual a zero?

28. Sejam $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$. Nesta questão dicutimos quando é possível dividir α por β.
    (a) Mostre que
    $$\frac{1}{\beta} = \frac{\widehat{\beta}}{N(\beta)}.$$
    (b) Calcule r e s tais que
    $$\frac{\alpha}{\beta} = r + s\sqrt{d}.$$
    e mostre que r e s pertencem a $\mathbb{Q}$, mas não necessariamente a $\mathbb{Z}$.
    (c) Mostre que se $N(\beta) = \pm 1$ então $\alpha/\beta \in \mathbb{Z}[\sqrt{d}]$.

29. Mostre que $2+\sqrt{3}$ é invertível unidade em $\mathbb{Z}[\sqrt{3}]$ e que $8+3\sqrt{7}$ é invertível em $\mathbb{Z}[\sqrt{7}]$.

30. Prove que α é invertível em $\mathbb{Z}[\sqrt{d}]$, se, e somente se, $N(\alpha) = 1$.

31. Nesta questão calculamos os invertíveis em $\mathbb{Z}[\sqrt{d}]$ para vários valores distintos de d. Para isto você deve usar o critério estabelecido no exercício acima.
    (a) Determine todos os invertíveis de $\mathbb{Z}[\sqrt{d}]$ quando $d < -1$.
    (b) Determine todos os invertíveis de $\mathbb{Z}[\sqrt{d}]$ quando $d = -1$.
    (c) Determine um elemento invertível diferente de ± 1 em $\mathbb{Z}[\sqrt{3}]$.

32. Mostre que se $\mathbb{Z}[\sqrt{d}]$ contém um elemento invertível $\omega \neq \pm 1$, então $\mathbb{Z}[\sqrt{d}]$ tem uma quantidade infinita de invertíveis.

33. Neste exercício você é chamado a provar os detalhes do argumento apresentado na página ????, referente à existência de mais de uma fatoração no anel $\mathbb{Z}[\sqrt{-5}]$. Seja d um inteiro *positivo* e considere o conjunto

$$\mathbb{Z}[\sqrt{-d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\},$$

    (a) Mostre que $\alpha \in \mathbb{Z}[\sqrt{d}]$ é *irredutível* se, e somente se, não pode ser escrito na forma $\alpha = \beta\gamma$ com $N(\beta) < N(\alpha)$ e $N(\gamma) < N(\alpha)$.
    (b) Mostre que se $\alpha \in \mathbb{Z}[\sqrt{d}]$ é irredutível e $\alpha = \beta\gamma$, então β ou γ é uma unidade em $\mathbb{Z}[\sqrt{d}]$.
    (c) Mostre que se $p < d$ e $q < d$ são números primos positivos (não necessariamente distintos), e $N(\alpha) = pq$, para algum $\alpha \in \mathbb{Z}[\sqrt{-5}]$, então α é irredutível em $\mathbb{Z}[\sqrt{d}]$.
    (d) Mostre que 2 e 3 são irredutíveis em $\mathbb{Z}[\sqrt{-5}]$.
    (e) Mostre que 6 tem duas fatorações distintas em irredutíveis em $\mathbb{Z}[\sqrt{-5}]$.

34. Vimos no exercício anterior que 3 e $1 + \sqrt{-5}$ são irredutíveis em $\mathbb{Z}[\sqrt{-5}]$. Prove que não existem α e β em $\mathbb{Z}[\sqrt{-5}]$ tais que

$$\alpha \cdot 3 + \beta(1 + \sqrt{-5}) = 1.$$

    Isto mostra que não existe nada semelhante a um algoritmo euclideano estendido em $\mathbb{Z}[\sqrt{-5}]$.

35. Verifique se o ideal de $\mathbb{Z}[\sqrt{-5}]$ gerado por 3 e por $1 + \sqrt{-5}$ é principal. Se for, determine o seu gerador.

CAPíTULO 3

Polinômios e ideais: várias indeterminadas

A partir deste capítulo veremos como estender o alcance dos métodos que introduzimos no capítulo 2, de modo a poder lidar também com polinômios em várias indeterminadas. Isto nos permitirá estudar de maneira mais precisa a relação entre problemas de geometria plana e sua tradução algébrica.

1. Polinômios em várias indeterminadas

Seja K um corpo e sejam $x_1, \ldots, x_n$ variáveis. Denotaremos o anel de polinômios nas variáveis $x_1, \ldots, x_n$ e coeficientes em K por $K[x_1, \ldots, x_n]$. Estes anéis são definidos, a partir da construção da seção 3 do capítulo 2, pela fórmula recursiva

$$K[x_1, \ldots, x_n] = K[x_1, \ldots, x_{n-1}][x_n].$$

Assim, um polinômio em $K[x_1, \ldots, x_n]$ deve ser entendido como um polinômio na variável x_n cujos coeficientes pertencem a $K[x_1, \ldots, x_{n-1}]$.

De acordo com esta definição, um polinômio $f \in K[x_1, \ldots, x_n]$ se escreve como uma soma de termos da forma $a_j x_n^j$, com $a_j \in K[x_1, \ldots, x_{n-1}]$. Entretanto, por sua vez,

$$a_j = b_{0,j} + b_{1,j}x_{n-1} + b_{2,j}x_{n-1}^2 + \cdots + b_{m,j}x_{n-1}^m,$$

em que $b_{0,j}, \ldots, b_{m,j} \in K[x_1, \ldots, x_{n-1}]$. Portanto,

$$a_j x_n^j = b_{0,j}x_n^j + b_{1,j}x_{n-1}x_n^j + b_{2,j}x_{n-1}^2x_n^j + \cdots + b_{m,j}x_{n-1}^m x_n^j.$$

Logo f é uma soma de parcelas da forma $b_{i,j}x_{n-1}^j x_n^i$, em que $b_{i,j}$ é um elemento de $K[x_1, \ldots, x_{n-2}]$. Prosseguindo desta maneira, verificamos que f pode ser escrito como uma soma de parcelas, ou *termos*, da forma

$$c_{\alpha_1,\ldots,\alpha_n} x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}, \tag{24}$$

em que $\alpha_1, \ldots, \alpha_n$ são números naturais. Antes de prosseguir com nossa discussão precisamos de uma notação que nos permita expressar (24) de uma maneira mais compacta. Fazemos isto usando *multi-índices*, que são vetores

$$\alpha = (\alpha_1, \ldots, \alpha_n),$$

cujas coordenadas são inteiros não negativos. Isto é, α é um elemento de $\mathbb{N}^n$. O *módulo* do multi-índice α é o inteiro

$$|\alpha| = \alpha_1 + \cdots + \alpha_n.$$

A cada multi-índice associamos o produto de potências das variáveis, ou *monômio*,

$$x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}.$$

Usando esta notação, podemos escrever (24) na forma

$$c_\alpha x^\alpha.$$

Portanto, um polinômio $f \in K[x_1, \ldots, x_n]$ se expressa como uma soma da forma

$$f = \sum_\alpha c_\alpha x^\alpha,$$

em que cada termo $c_\alpha x^\alpha$ é formado por uma constante $c_\alpha \in K$, o seu *coeficiente*, e um monômio x^α, o seu *suporte*. Já o *grau* de $c_\alpha x^\alpha$ é o módulo do multi-índice α.

Esta terminologia generaliza, de maneira natural, a que já vínhamos adotando para polinômios em uma variável. Contudo, ao contrário do que ocorria naquele caso, um polinômio em mais de uma variável pode ter vários monômios com o mesmo grau e os mesmos coeficientes, como é o caso de

$$x_1^3 + x_1^2 x_2 + x_1 x_2^2 + x_2^3.$$

Discutiremos esta questão em mais detalhes no capítulo 4.

O poder de compressão da notação de multi-índices nos permite escrever o produto dos polinômios

$$f = \sum_\alpha a_\alpha x^\alpha \text{ e } g = \sum_\beta b_\beta x^\beta,$$

como $fg = \sum_\gamma c_\gamma x^\gamma$, em que

$$c_\gamma = \sum_{\gamma=\alpha+\beta} a_\alpha b_\beta,$$

que é uma fórmula de aparência inteiramente análoga à que obtivemos para polinômios em uma variável sobre um anel.

Resta-nos definir uma noção apropriada de grau, e estabelecer fórmulas para o grau da soma e do produto de um polinômio em mais de uma variável. Para isso, introduzimos a noção de suporte. Seja $\mathbb{T}^n$ o conjunto de todos os monômios nas variáveis $x_1, \ldots, x_n$. O *suporte* de um polinômio $f \in K[x_1, \ldots, x_n]$ é o subconjunto de $\mathbb{T}^n$ definido por

$$\sup(f) = \{\mu \in \mathbb{T}^n : \text{ o termo em } \mu \text{ de } f \text{ tem coeficiente não nulo}\}.$$

Por exemplo,

$$\sup(x_1^3 + 8x_1x_2^2 + 9x_2^3 + x_1^2 + 10x_2 + 1) = \{x_1^3, x_1x_2^2, x_2^3, x_1^2, x_2, 1\}.$$

Segue da definição de suporte que se $f, g \in K[x_1, \ldots, x_n]$, então

$$\sup(f+g) \subseteq \sup(f) \cup \sup(g)$$

e que

$$\sup(fg) \subseteq \{\mu\nu : \mu \in \sup(f) \text{ e } \nu \in \sup(g)\}.$$

Uma definição simples no ajuda a escrever esta última fórmula de uma maneira mais compacta e mais fácil de lembrar. Sejam X e Y subconjuntos do anel A. Escrevemos $X \cdot Y$ para denotar o subconjunto de A cujos elementos são todos obtidos multiplicando um elemento de X por um elemento de Y. Em outras palavras,

$$X \cdot Y = \{ab : a \in X \text{ e } b \in Y\}.$$

Por exemplo, o produto dos subconjuntos

$$X = \{1, 2 + 3x, x^2\} \quad \text{e} \quad X = \{5x, 7x^3\}$$

de $\mathbb{Q}[x]$ é igual a

$$X \cdot Y = \{5x, 7x^3, 5(2 + 3x)x, 7(2 + 3x)x^3, 5x^3, 7x^5\}.$$

Usando esta notação, a fórmula para o suporte do produto de dois polinômios pode ser reescrita como

$$\sup(fg) \subseteq \sup(f) \cdot \sup(g). \tag{25}$$

O *grau total* de f é o grau máximo dentre os monômios que pertencem a $\sup(f)$. Por exemplo, $x_1^3 + 8x_1x_2^2 + 9x_2^3 + x_1^2 + 10x_2 + 1$ tem grau 3. Da fórmula para o suporte da soma segue imediatamente que

> o grau total de $f + g$ é menor ou igual ao máximo entre os graus totais de f e g.

Já a fórmula para o grau total do produto exige um esforço maior. Digamos que f tem grau total n e que g tem grau total m. Em primeiro lugar, (25) nos diz que os monômios de maior grau de $\sup(fg)$ resultam do produto de um monômio de grau n de $\sup(f)$ por um monômio de grau m de $\sup(g)$. Portanto, é claro que o grau total de fg não pode ser maior que $m + n$. Contudo, como pode haver vários monômios diferentes com estas propriedades, é concebível que pudesse haver cancelamento entre todos os monômios de grau $m + n$ de fg. Isto não acontece, e pode ser provado diretamente, como sugerido no exercício ???. Como teremos acesso à mesma fórmula por um aclive menos íngreme no capítulo 4, deixaremos a questão para ser resolvida lá.

Apesar de ainda não termos provado a aditividade do grau total do produto, vamos utilizá-la para provar que todo polinômio em várias indeterminadas sobre um corpo pode ser fatorado como um produto de polinômios irredutíveis. Como no caso de polinômios em uma variável, este resultado é consequência imediata do teorema 2.5, bastando para isto escolher uma função multiplicativa no anel $K[x_1, \ldots, x_n]$. Isto explica porque escolhemos expor a teoria de fatoração na forma mais geral do teorema 2.5. Se tivéssemos provado a fatoração em $K[x]$ diretamente teríamos que repetir essencialmente a mesma prova neste ponto—ou, mais provavelmente, deixá-la como exercício para você.

Copiando o caso de uma variável, escolhemos a função multiplicativa em $K[x_1, \ldots, x_n]$ como sendo $2^{\text{grautotal}}$. A multiplicatividade desta função segue da aditividade do grau total; veja exercício ???. Temos, portanto, o seguinte teorema.

TEOREMA 3.1. *Seja K um corpo. Todo polinômio não nulo f, pertencente ao anel $K[x_1, \ldots, x_n]$ pode ser escrito na forma*

$$f = ap_1^{e_1} \cdots p_s^{e_s} \tag{26}$$

em que $a \in K$, $p_1, \ldots, p_s$ são polinômios irredutíveis mônicos distintos e os expoentes $e_1, \ldots, e_s$ são inteiros positivos. Além disto, esta maneira de escrever f é única, a menos da ordem dos fatores.

A demonstração da unicidade da fatoração é feita por indução no número de variáveis. Antes de poder descrevê-la, precisamos aplicar a construção do anel de quocientes descrita na seção 2 do capítulo 2 ao anel de polinômios $K[x_1, \ldots, x_n]$, com coeficientes em um corpo K. Com isto obtemos um corpo $K(x_1, \ldots, x_n)$, cujos elementos são da forma

$$\frac{f}{g} \text{ em que } \quad f, g \in K[x_1, \ldots, x_n] \text{ e } \quad g \neq 0,$$

e que, como no caso de uma variável, é conhecido como *corpo das funções racionais*. Como sempre, identificamos um polinômio $f \in K[x_1, \ldots, x_n]$ com o elemento $f/1 \in K(x_1, \ldots, x_n)$, o que nos permite tratar $K[x_1, \ldots, x_n]$ como subanel de $K(x_1, \ldots, x_n)$.

Voltando à unicidade da fatoração, considere $K[x_1, \ldots, x_n]$ como um anel de polinômios na variável x_n com coeficientes em $K[x_1, \ldots, x_{n-1}]$. Como este último anel é subanel do corpo $K(x_1, \ldots, x_{n-1})$, temos que

$$K[x_1, \ldots, x_{n-1}][x_n] \text{ é subanel de } \quad K(x_1, \ldots, x_{n-1})[x_n].$$

Mas a fatoração neste último anel é única pelo teorema 2.7 da página 57, o que nos permite executar o passo de indução. Antes de dar os detalhes da demonstração, você deve saber que precisaremos de um dos corolários do *Lema de Gauss* para completar a prova da unicidade. Estritamente falando, só provamos o Lema de Gauss para $\mathbb{Z} \subset \mathbb{Q}$, entretanto, a mesma demonstração funciona também para

$$K[x_1, \ldots, x_n] \subset K(x_1, \ldots, x_n),$$

como você é chamado a mostrar no exercício ???.

DEMONSTRAÇÃO. Nosso objetivo é provar, por indução em n, que

> qualquer que seja o corpo K, a fatoração de um polinômio de $K[x_1, \ldots, x_n]$ em irredutíveis é única.

O significado da unicidade aqui é o mesmo já discutido na página 54. Quando $n = 1$ o resultado foi provado no teorema 2.7 da página 57. Suponhamos, então, que a fatoração em $K[x_1, \ldots, x_{n-1}]$ é única e vamos provar que o mesmo vale em $K[x_1, \ldots, x_n]$.

Suponhamos, por contradição, que existe $f \in K[x_1, \ldots, x_n]$ com duas fatorações distintas em irredutíveis; digamos,

$$f = c_1 p_1 \cdots p_s = c_2 q_1 \cdots q_v,$$

em que c_1 e c_2 são constantes não nulas de K e os ps e qs são irredutíveis em $K[x_1, \ldots, x_n]$. Observe que, pela hipótese de indução, $f \notin K[x_1, \ldots, x_{n-1}]$,

o que não impede que alguns dos ps e qs não contenham a variável x_n entre os seus monômios. Se isto ocorrer, rearrumamos os números de modo que estes polinômios apareceram ao final de cada fatoração. Mais precisamente, teremos que

$$f = c_1 p_1 \cdots p_r \cdots p_s = c_2 q_1 \cdots q_t \cdots q_v,$$

com

$$p_{r+1}, \ldots, p_s, q_{t+1}, \ldots, q_v \in K[x_1, \ldots, x_{n-1}].$$

Levando em conta que

$$K[x_1, \ldots, x_n] = K[x_1, \ldots, x_{n-1}][x_n] \subset K(x_1, \ldots, x_{n-1})[x_n],$$

consideraremos as fatorações

$$f = c_1 p_1 \cdots p_r \cdots p_s = c_2 q_1 \cdots q_t \cdots q_v,$$

em $K(x_1, \ldots, x_{n-1})[x_n]$. Neste caso,

$$u_1 = c_1 p_{r+1} \cdots p_s \text{ e } u_2 = q_{t+1} \cdots q_v$$

são invertíveis em $K(x_1, \ldots, x_{n-1})[x_n]$ e, pelo corolário 2.9 da página 62, $p_1, \ldots, p_r$ e $q_1, \ldots, q_t$ são irredutíveis em $K(x_1, \ldots, x_{n-1})[x_n]$. Entretanto, como $K(x_1, \ldots, x_{n-1})$ é um corpo, podemos aplicar o teorema 2.7 novamente para concluir que $r = s$, que $u_1 = u_2$ e que, rearrumando os qs se necessário for,

$$p_i \text{ é associado a } q_i \text{ para todo } 1 \leq i \leq r.$$

Isto implica que $p_i = \beta_i q_i$ para algum $\beta_i \in K(x_1, \ldots, x_{n-1})$. Mas,

$$\beta_i = \frac{h_i}{g_i}$$

em que $h_i, g_i \in K[x_1, \ldots, x_{n-1}]$ com $g_i \neq 0$; donde

$$g_i p_i = h_i q_i.$$

Como p_i e q_i são irredutíveis, e portanto primitivos, em $K[x_1, \ldots, x_{n-1}][x_n]$, teremos pelo Lema de Gauss que g_i = h_i, de forma que

$$p_i = q_i \text{ para todo } 1 \leq i \leq r.$$

Finalmente, de $u_1 = u_2$ obtemos

$$c_1 p_{r+1} \cdots p_s = q_{r+1} \cdots q_v.$$

Estes produtos descrevem um elemento de $K[x_1, \ldots, x_{n-1}]$ que, pela hipótese de indução, tem apenas uma fatoração. Assim, $s = v$ e, como os ps e qs são polinômios mônicos, $c_1 = c_2$ e

$$pj = q_j \text{ para todo } r \leq j \leq s,$$

a menos da possível necessidade de renumerar os qs. Reunindo tudo o que fizemos mostramos que

> $s = v$, $c_1 = c_2$ e que, a menos da necessidade de renumerar os qs, $p_i = q_i$ para $1 \leq i \leq r$,

o que prova o passo de indução. □

Finalmente, o que dizer sobre algoritmos que permitam calcular efetivamente a fatoração de um dado polinômio em várias indeterminadas? Ao contrário do caso de uma variável, mesmo quando o corpo é $\mathbb{C}$, a fatoração pode ser bastante difícil de obter. Desta vez chegamos à fronteira do que podemos tratar neste livro, de modo que vamos nos contentar em saber que é sempre possível obter uma fatoração, sem tentar calculá-la explicitamente. Uma discussão geral sobre algoritmos de fatoração para polinômios em várias indeterminadas com coeficientes racionais pode ser encontrada em [**20**]. Para a descrição detalhada de alguns algoritmos para fatoração sobre $\mathbb{C}$ consulte [**10**].

2. Ideais em várias indeterminadas

Como vimos na seção 4 do capítulo 2 um *ideal* I de um anel A é um subconjunto de A que satisfaz as propriedades usuais dos conjuntos de múltiplos; isto é,

- $0 \in I$;
- se $a, b \in I$ então $a + b \in I$;
- se $a \in A$ e $b \in I$ então $ab \in I$.

Também vimos naquela seção que todo ideal do anel de polinômios em uma variável sobre um corpo é gerado por um elemento e, portanto, é igual ao conjunto de múltiplos de algum polinômio. Entretanto este resultado é falso se o anel de base não for um corpo. Por exemplo, mostramos que se $n > 1$ é um inteiro, então o ideal $\langle n, x\rangle$ de $\mathbb{Z}[x]$ não pode ser gerado por um único elemento. Começaremos provando que um resultado semelhante vale em $K[x_1, \ldots, x_n]$ quando $n \geq 2$, mesmo se K for um corpo.

Por exemplo, quando $n \geq 2$, o ideal $\langle x_1, x_2\rangle$ de $K[x_1, \ldots, x_n]$ não pode ser gerado por apenas um elemento. É fácil provar isto por contradição, de maneira semelhante ao que fizemos para $\mathbb{Z}[x]$. Suponha que g fosse um gerador de $\langle x_1, x_2\rangle$. Neste caso, deveria existir um polinômio $h \in K[x_1, \ldots, x_n]$ tal que

$$x_2 = hg \tag{27}$$

Logo o grau de g como polinômio em x_2 com coeficientes em x_1 tem que ser no máximo 1. Mas o mesmo vale, se trocarmos os papéis de x_1 e x_2, de modo que g deve ser da forma $g = ax_1 + bx_2 + c$, em que $a, b, c \in K$. Contudo, se $a \neq 0$, a equação (27) implica que h tem grau zero, e que $b = c = 0$. Isto significa que $g = x_1$, contradizendo o fato de que g divide x_2. Por outro lado, se $a = 0$, então $g = bx_2 + c$, que não pode dividir x_1, a não ser que $b = 0$. Mas, neste caso, g teria que ser uma constante não nula, o que implicaria que

$$\langle x_1, x_2\rangle = K[x_1, \ldots, x_n],$$

que é evidentemente falso. Portanto, $\langle x_1, x_2\rangle$ não pode ser principal.

Utilizando indução em n, e um argumento semelhante ao usado acima, podemos mostrar que o ideal $\langle x_1, \ldots, x_n\rangle$ não pode ser gerado *por menos de* n elementos; veja exercício ???. Assim, temos que

- todo ideal de $K[x_1]$ pode ser gerado por um elemento;

- dado um inteiro positivo n qualquer, há ideais em $K[x_1, \ldots, x_n]$ que não podem ser gerados por menos de n elementos.

Considerando estas duas afirmações, talvez você esteja desconfiado que o que está por trás delas é que todo ideal de $K[x_1, \ldots, x_n]$ pode ser gerado por n elementos. Entretanto, nada poderia estar mais longe da verdade, como veremos em breve.

Continuando com o corpo K, diremos que um ideal I de $K[x_1, \ldots, x_n]$ é *monomial* se pode ser gerado apenas por monômios nas variáveis $x_1, \ldots, x_n$. Por exemplo, o ideal $\langle x_1 x_2^4, x_2^3 \rangle$ é monomial em $K[x_1, x_2]$, ao passo que $\langle x_1 + x_2 \rangle$ não é monomial. Um outro exemplo, menos imediato é o ideal $\langle x_1 x_2 + x_1^2, x_1 x_2 + 2x_1^2 \rangle$. Embora os geradores escolhidos acima não sejam monômios, este ideal é monomial porque

$$\langle x_1 x_2 + x_1^2, x_1 x_2 + 2x_1^2 \rangle = \langle x_1 x_2, x_1^2 \rangle,$$

como é fácil verificar. Por outro lado, nem todo ideal é monomial. Na verdade, qualquer ideal principal de $K[x_1, \ldots, x_n]$ cujo gerador não é monômio não pode ser um ideal monomial. A razão é que o produto de dois polinômios só poder dar um monômio se ambos os polinômios forem monômios; veja exercício ???. É possível caracterizar os ideais monomiais sem se referir aos geradores, como mostra a seguinte proposição.

PROPOSIÇÃO 3.2. *Um ideal I de $K[x_1, \ldots, x_n]$ é monomial se, e somente se,*

$$\sup(f) \subset I \quad \textit{para todo} \quad f \in I.$$

DEMONSTRAÇÃO. Seja μ um monômio e $f \in K[x_1, \ldots, x_n]$. Digamos que

$$f = c_s \nu_s + c_{s-1} \nu_{s-1} + \cdots + c_0 \nu_0,$$

em que $\nu_s, \ldots, \nu_0$ são monômios nas variáveis $x_1, \ldots, x_n$ e $c_s, \ldots, c_0 \in K$. Se $\mu \in I$, então,

$$\sup(f\mu) = \{\nu_1 \mu, \ldots, \nu_0 \mu\} \subseteq I. \tag{28}$$

Se I for gerado pelos monômios $\mu_1, \ldots, \mu_t$, então qualquer elemento de I pode ser escrito na forma

$$\sum_{i=1}^{t} f_i \mu_i \text{ para alguma escolha de } f_1, \ldots, f_t \in K[x_1, \ldots, x_n].$$

Expressando cada f_i como uma soma de monômios, temos pela equação (28) que

$$\sup(\sum_{i=1}^{t} f_i \mu_i) \subseteq \bigcup_{i=1}^{t} \sup(f_i \mu_i) \subseteq I,$$

como queríamos mostrar. A recíproca é imediata. □

Com isto estamos prontos para mostrar que $K[x_1, x_2]$ tem ideais monomiais com um número de elementos tão grande quanto desejarmos. Para isso,

defina I_k como sendo o ideal de $K[x_1, x_2]$ gerado por todos os monômios de grau k. Em outras palavras,

$$I_k = \langle x_1^k, x_1^{k-1}x_2, \ldots, x_1x_2^{k-1}, x_2^k \rangle.$$

Em particular,

$$I_1 = \langle x_1, x_2 \rangle \text{ e } I_2 = \langle x_1^2, x_1x_2, x_2^2 \rangle.$$

Um argumento combinatório elementar (veja exercício ???) mostra que existem $k+1$ monômios de grau k em duas variáveis.

PROPOSIÇÃO 3.3. *O ideal I_k não pode ser gerado por menos de $k+1$ polinômios.*

DEMONSTRAÇÃO. Suponha que I_k possa ser gerado por polinômios que denotaremos por $g_1, \ldots, g_s$, com $s < k+1$. Como I_k é gerado pelos monômios de grau k, o termo de menor grau de cada g_i tem que ter grau pelo menos k. Denote por t_i o termo de grau k de g_i. Note que não estamos excluindo a possibilidade de que t_i seja zero para alguns valores de i. De qualquer forma, temos que $g_i - t_i$ só tem termos de grau maior que k. Portanto,

$$g_i - t_i \in I_{k+1}.$$

Escrevendo o monômio $x_1^j x_2^{k-j}$ como combinação dos geradores $g_1, \ldots, g_s$, obtemos

$$x_1^j x_2^{k-j} = q_1g_1 + \cdots + q_sg_s.$$

Disto segue que,

$$x_1^j x_2^{k-j} - (c_1t_1 + \cdots + c_st_s) \in I_{k+1},$$

em que c_i é o termo constante de q_i. Como I_{k+1} só tem polinômios não nulos de grau maior ou igual a $k+1$, obtemos a igualdade

$$x_1^j x_2^{k-j} = c_1t_1 + \cdots + c_st_s.$$

Isto significa que os polinômios $t_1, \ldots, t_s$ geram o K-espaço vetorial V_k dos polinômios homogêneos de grau k. Obtivemos, assim, um conjunto de geradores para o espaço vetorial V_k com apenas s elementos.

Entretanto, os $k+1$ monômios de grau k formam uma base de V_k como espaço vetorial, de modo que $\dim_K(V_k) = k+1$. Como uma base é um conjunto mínimo de geradores para um espaço vetorial, temos uma contradição com a hipótese $s < k+1$. □

Acabamos de ver que o número mínimo de geradores de um ideal monomial de um anel de polinômios em mais de uma variável pode ser tão grande quanto desejarmos. Isto parece sugerir que, "passando ao limite" devemos poder construir ideais monomiais do anel de polinômios $K[x_1, \ldots, x_n]$ que não admitem um número finito de geradores. De certa maneira, isto é verdade. Por exemplo, no anel $K[x_1, x_2, \ldots]$ com uma infinidade de indeterminadas, o ideal I_∞ gerado por todas as variáveis é evidentemente monomial. O que acontece se supusermos que I_∞ tem uma quantidade finita de geradores, digamos $\{g_1, \ldots, g_s\}$? Como estes geradores são em número finito, podemos escrever

cada um dos gs usando apenas uma quantidade finita das variáveis do anel. Digamos que $x_1, \ldots, x_m$ são estas variáveis. Neste caso, não há como escrever x_{m+1} como combinação linear polinomial dos gs, o que contradiz nossa hipótese de que os gs seriam suficientes para gerar I_∞. Contudo, se aumentarmos a quantidade de variáveis o quanto quisermos, sem contudo admitir uma quantidade infinita delas, a resposta é bem diferente, como veremos no próximo teorema. Antes, porém, precisamos de um resultado técnico bastante geral. Para enunciá-lo com mais facilidade, diremos que um ideal J de um dado anel é *finitamente gerado* se pode ser gerado por uma quantidade finita de elementos de J.

PROPOSIÇÃO 3.4. *Seja I um ideal finitamente gerado de um anel A. Se S é um conjunto infinito de geradores de I, então existe um subconjunto finito de S que também gera I.*

Talvez seja conveniente elaborar um pouco mais sobre esta proposição, para que não fique a impressão de que seu contéudo é meramente tautológico. Dizer que I é finitamente gerado, é o mesmo que dizer que I admite *algum* conjunto *finito* de geradores. Mas a proposição nos diz que isto implica algo bem mais forte:

> dado um conjunto infinito de geradores, é possível escolher uma quantidade finita dos seus elementos para gerar todo o ideal.

Tendo esclarecido este ponto, vejamos como provar a proposição.

DEMONSTRAÇÃO. Como I é finitamente gerado, existem polinômios, digamos $g_1, \ldots, g_k \in I$, tais que

$$\langle g_1, \ldots, g_k \rangle = I.$$

Contudo S é um conjunto de geradores, de modo que cada g_j pode ser escrito como uma combinação linear *finita* dos elementos de S. Em outras palavras,

$$g_j \in \langle s_1, \ldots, s_{r(j)} \rangle,$$

para $1 \leq j \leq k$. Denotando por m o máximo entre os inteiros $r(1), \ldots, r(k)$, temos que

$$g_j \in \langle s_1, \ldots, s_m \rangle,$$

para todo $1 \leq j \leq k$. Contudo, $S \subseteq I$, de modo que

$$\langle g_1, \ldots, g_k \rangle \subseteq \langle s_1, \ldots, s_m \rangle \subseteq I.$$

Como os gs geram todo o I, concluímos que

$$\langle s_1, \ldots, s_m \rangle = I;$$

o que completa a demonstração. □

Estamos prontos para o teorema, que será de grande importância em muitas de nossas futuras aplicações.

TEOREMA 3.5. *Se K é um corpo, então todo ideal monomial do anel de polinômios $K[x_1, \ldots, x_n]$ é finitamente gerado.*

DEMONSTRAÇÃO. Vamos mostrar que se $K[x_1, \ldots, x_n]$ admite algum ideal monomial que não é finitamente gerado, então $K[x_1, \ldots, x_{n-1}]$ também admite um tal ideal. Continuando assim teríamos que $K[x_1]$ tem ideais monomiais que não são finitamente gerados, o que contradiz o teorema 2.3.

Suponha que I é um ideal monomial de $K[x_1, \ldots, x_n]$ que não é finitamente gerado. Escolha uma sequência de monômios em I da seguinte maneira:

$\mu_1 \in I$ e $\deg_{x_n}(\mu_1)$ é o menor possível;
$\mu_2 \in I \setminus \langle \mu_1 \rangle$ e $\deg_{x_n}(\mu_2)$ é o menor possível;
$\mu_3 \in I \setminus \langle \mu_1, \mu_2 \rangle$ e $\deg_{x_n}(\mu_3)$ é o menor possível;
e assim por diante.

Como I não é finitamente gerado, esta sequência é infinita. Entretanto, $\mu_i = \nu_i x_n^{k_i}$, em que ν_i é um monômio nas variáveis $x_1, \ldots, x_{n-1}$. Considere, então, o ideal J de $K[x_1, \ldots, x_{n-1}]$ gerado pelos νs. Vamos mostrar que J não pode ser finitamente gerado.

Se J fosse finitamente gerado, então pela proposição 3.4 poderia ser gerado pelos monômios $\nu_1, \ldots, \nu_m$, para algum inteiro $m > 0$. Isto implicaria que $\nu_{m+1} = \nu_\ell \eta$ para algum $1 \leq \ell \leq m$ e algum monômio $\eta \in K[x_1, \ldots, x_{n-1}]$. Por outro lado, a escolha dos μs implica que $k_{m+1} \geq k_\ell$. Temos, assim, que

$$\mu_{m+1} = \nu_{m+1} x_n^{k_m} = \eta x_n^{k_m - k_\ell} \mu_\ell.$$

Mas isto implica que $\mu_{m+1} \in \langle \mu_1, \ldots, \mu_m \rangle$, o que contradiz a escolha de μ_{m+1}. Portanto, J não pode ser finitamente gerado. □

Há duas consequências simples, mas muito úteis, deste teorema que convém explicitar para referência futura, a primeira das quais é mera combinação do teorema 3.5 com a proposição 3.4.

COROLÁRIO 3.6. *Seja K um corpo e seja S um conjunto infinito de monômios de $K[x_1, \ldots, x_n]$. Existe um subconjunto finito G de S que gera o mesmo ideal que S em $K[x_1, \ldots, x_n]$.*

COROLÁRIO 3.7. *Seja K um corpo e seja*

$$S_1 \subseteq S_2 \subseteq S_3 \subseteq \cdots .$$

uma sequência crescente de subconjuntos formados por monômios do anel de polinômios $K[x_1, \ldots, x_n]$. Então existe um inteiro $k > 0$ tal que $\langle S_t \rangle = \langle S_k \rangle$ para todo $t \geq k$.

DEMONSTRAÇÃO. Considere o conjunto S que é a união de todos os S_i, para $i \geq 1$. Pelo corolário 3.6 existe um subconjunto finito T de S que gera o ideal $\langle S \rangle$. Como T é finito, existe um inteiro $k > 0$ tal que $T \subseteq S_k$. Portanto, se $t \geq k$,

$$\langle T \rangle \subseteq \langle S_k \rangle \subseteq \langle S_t \rangle \subseteq \langle S \rangle \subseteq \langle T \rangle,$$

o que implica que

$$\langle S \rangle = \langle S_k \rangle = \langle S_t \rangle,$$

como queríamos mostrar. □

Há uma pergunta, não formulada, que a esta altura pode estar lhe assombrando. Vimos que todo ideal monomial é sempre finitamente gerado: o mesmo vale para qualquer ideal, mesmo que não seja monomial? Afinal, já vimos que tais ideais existem. A resposta a esta pergunta é sim.

TEOREMA DA BASE DE HILBERT. *Seja K um corpo. Todo ideal de $K[x_1, \ldots, x_n]$ admite um número finito de geradores.*

Apesar de utilizarmos este resultado na próxima seção, só veremos como demonstrá-lo na seção 1 do capítulo 5. A razão para adiar a demonstração até então é que somente lá desenvolveremos a maquinaria natural para reduzir o resultado do teorema ao caso monomial tratado no teorema 3.5.

3. Ideais e geometria

A geometria de uma reta é muito simples, por isso não consideramos aplicações geométricas do anel de polinômios em uma variável. Já a geometria dos espaços de dimensão dois ou mais é muito interessante e pode (deve!) ser utilizada na criação de exemplos bastante variados de ideais. Para isto, introduziremos a noção de ideal de um conjunto de pontos. Seja L um corpo e K um subcorpo de L. Se você preferir pode imaginar que K e L são corpos escolhidos entre os racionais, reais e complexos, que são os casos que realmente nos interessam. Seja $X \subseteq L^n$. O *ideal de* X em $K[x_1, \ldots, x_n]$ é definido por

$$\mathrm{I}_K(X) = \{f \in K[x_1, \ldots, x_n] : f(p) = 0 \text{ para todo } p \in X\}.$$

A razão pela qual escolhemos trabalhar com dois corpos $K \subseteq L$ é que, na prática teremos $K = \mathbb{Q}$ e $L = \mathbb{C}$. Isto se dá porque é sobre os racionais que melhor calculamos de maneira exata, ao passo que os complexos são necessários para podermos provar os teoremas geométricos de que precisamos. Contudo, teremos que esperar até o capítulo 9 para podermos dar uma resposta satisfatória a esta última afirmação; ainda que ao final desta seção venhamos a obter alguns indícios nesta direção. Naturalmente, é necessário verificar que o subconjunto $\mathrm{I}_K(X)$ definido acima satisfaz às propriedades requeridas para que seja um ideal de $K[x_1, \ldots, x_n]$. Como isto é muito fácil de fazer, vamos deixá-lo por sua conta; veja exercício ???. Como sempre, omitiremos o índice K sempre que não houver possibilidade de ambiguidade.

Nosso primeiro exemplo é a curva definida parametricamente por

$$X = \{(t^2, t^3) : t \in \mathbb{R}\} \subset \mathbb{R}^2,$$

cujo esboço aparece na figura 1.
Curvas como esta aparecem em muitos lugares na natureza, por exemplo, nas cáusticas formadas pela reflexão da luz em uma xícara de chá, como ilustrado na figura 2.

O ideal correspondente a esta curva é

$$\mathrm{I}(X) = \{f \in \mathbb{R}[x_1, x_2] : f(t^2, t^3) = 0, \text{ qualquer que seja } t \in \mathbb{R}\};$$

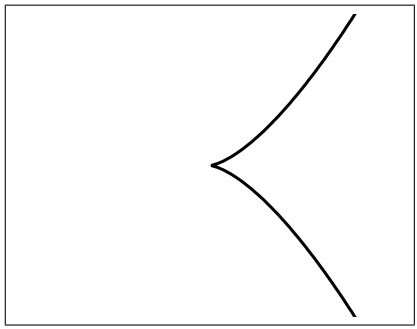


FIGURA 1. Cúspide

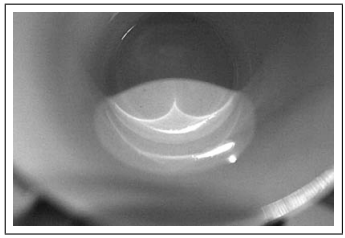


FIGURA 2. Cúspide em uma xícara de chá

e pretendemos identificar seus geradores. Uma simples substituição mostra que o polinômio $g = x_1^3 - x_2^2$ pertence a $\mathrm{I}(X)$: provaremos que $\mathrm{I}(X)$ é, de fato, gerado por g. Para isto tomaremos $f \in \mathrm{I}(X)$ e mostraremos que é múltiplo de g.

Como g é um polinômio mônico de grau apenas dois em x_2, é conveniente considerar $\mathbb{R}[x_1, x_2]$ como o anel dos polinômios na variável x_2 com coeficientes em $\mathbb{R}[x_1]$. Dividindo, então, f por g com o algoritmo da seção 3 do capítulo 2, obtemos

$$f = gq + r \text{ em que } r = 0 \text{ ou } r \text{ tem grau em } x_2 \text{ menor que } 2.$$

Para mostrar o que queremos, basta provar que r *não* pode ser diferente de 0. Mas, se $r \neq 0$, então, r tem grau menor que 2 em x_2, e podemos escrevê-lo na forma $r = a(x_1)x_2 + b(x_1)$, em que $a(x_1)$ e $b(x_1)$ são polinômios na variável x_1. Entretanto, $f, g \in \mathrm{I}(X)$, de modo que

$$0 = f(t^2, t^3) = g(t^2, t^3)q(t^2, t^3) + a(t^2) + b(t^2)t^3 = a(t^2) + b(t^2)t^3,$$

pois $g(t^2, t^3) = 0$. Contudo, o grau de cada termo de $a(t^2)$ é múltiplo de 2, ao passo que o grau de cada termo de $b(t^2)t^3$ é ímpar. Portanto, não pode haver cancelamento entre os termos de $a(t^2)$ e de $b(t^2)t^3$. Isto significa que todos os coeficientes de $a(t^2)$ e de $b(t^2)$ têm que ser nulos, de modo que

$$r(x_1, x_2) = a(x_1) + b(x_1)x_2 = 0.$$

Portanto,

$$\mathrm{I}(X) = \langle x_1^3 - x_2^2 \rangle,$$

como queríamos mostrar.

Na verdade, dado o gerador deste ideal, podemos reconstruir toda a curva X. Como X foi dada em forma paramétrica, tentaremos reconstruir sua parametrização partindo apenas da equação $x_1^3 - x_2^2 = 0$. Para isto consideramos a reta $x_2 = tx_1$. Esta reta intersecta a curva em apenas um ponto além da origem, como ilustrado na figura 3.

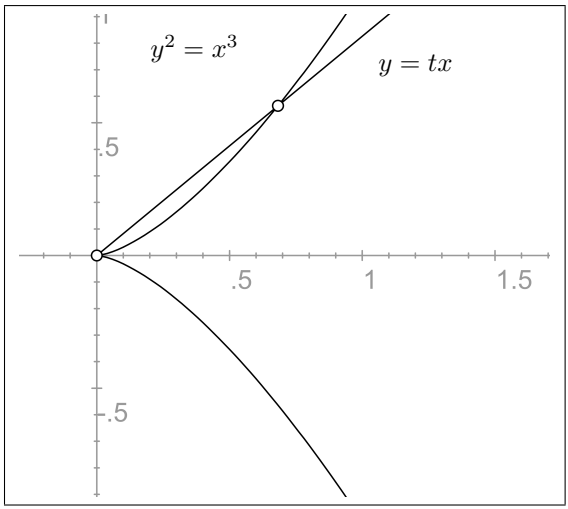


FIGURA 3. Parametrizando a cúspide

Isto significa que, cada valor de t define exatamente um ponto da curva. Para encontrar este ponto, substituímos $x_2 = tx_1$ na equação da curva, obtendo

$$0 = x_1^3 - (tx_1)^2 = x_1^2(x_1 - t^2).$$

Como estamos procurando o ponto de interseção *diferente da origem*, entre a reta e a curva , devemos ter $x_1 \neq 0$. Com isto, a equação acima nos dá

$$x_1 = t^2,$$

donde

$$x_2 = tx_1 = t^3.$$

Portanto, o ponto desejado é (t^2, t^3). Note que este ponto pertence à curva mesmo quando $t = 0$, que havia sido eliminado do argumento porque estávamos considerando apenas pontos diferentes da origem. Verificamos, assim, que os pontos (x_1, x_2) que satisfazem a equação $x_1^3 - x_2^2 = 0$ são exatamente os pontos da curva X dada originalmente.

Contudo, não são todas as curvas que podem ser recuperadas a partir do seu ideal. Um exemplo dramático é a curva que corresponde ao gráfico Γ da função seno; isto é, a curva

$$\Gamma = \{(t, \operatorname{sen}(t)) | t \in \mathbb{R}\}.$$

Vejamos o que acontece quando calculamos o ideal $\mathrm{I}(\Gamma)$. Por definição, se $f \in \mathrm{I}(\Gamma)$, então

$$f(t, \operatorname{sen}(t)) = 0,$$

para todo $t \in \mathbb{R}$. Considerando f como um polinômio em x_1, cujos coeficientes estão em $\mathbb{R}[x_2]$, podemos escrevê-lo na forma

$$f(x_1, x_2) = a_n(x_2)x_1^n + \cdots + a_1(x_2)x_1 + a_0(x_2).$$

Como o polinômio nulo evidentemente está $\mathrm{I}(\Gamma)$, podemos supor que $f \neq 0$ que, por sua vez, nos permite tomar $a_n(x_2) \neq 0$. Substituindo

$$x_1 = t \quad \text{e} \quad x_2 = \operatorname{sen}(t)$$

nesta expressão, obtemos

$$a_n(\operatorname{sen}(t))t^n + \cdots + a_1(\operatorname{sen}(t))t + a_0(\operatorname{sen}(t)) = 0. \tag{29}$$

Como $a_n(x_2)$ é não nulo, tem apenas uma quantidade finita de raízes. Seja $t_0 \in \mathbb{R}$ um número tal que $\operatorname{sen}(t_0)$ não é raiz de a_n. Por outro lado, a igualdade (29) vale para qualquer valor de t, de modo que, para todo inteiro k,

$$0 = f(t_0 + 2\pi k, \operatorname{sen}(t_0 + 2\pi k)) = f(t_0 + 2\pi k, \operatorname{sen}(t_0)),$$

já que o seno tem período 2π. Em outras palavras,

$$a_n(\operatorname{sen}(t_0))(t_0 + 2\pi k)^n + \cdots + a_1(\operatorname{sen}(t_0))(t_0 + 2\pi k) + a_0(\operatorname{sen}(t_0)) = 0.$$

Mas isto significa que todos os números da forma $t_0 + 2\pi k$ são raízes reais da equação polinomial

$$a_n(\operatorname{sen}(t_0))x_1^n + \cdots + a_1(\operatorname{sen}(t_0))x_1 + a_0(\operatorname{sen}(t_0)),$$

que só é possível se a equação for identicamente nula. Entretanto, este não é o caso da equação acima, já que tivemos o cuidado de escolher t_0 de modo que $a_n(\operatorname{sen}(t_0)) \neq 0$. Logo, o único polinômio que se anula em todos os pontos de Γ é o polinômio nulo. Em outras palavras,

$$\mathrm{I}(\Gamma) = \{0\}.$$

Desnecessário dizer que, deste ideal, nada se pode recuperar.

Os conjuntos de pontos que podem ser recuperados a partir dos seus ideais já cruzaram o nosso caminho anteriormente: são os conjuntos algébricos, cuja definição foi dada na seção 7 do capítulo 1: mas não custa relembrá-la. Dados corpos $K \subset L$ e um subconjunto $S \subset K[x_1, \ldots, x_n]$, o *conjunto algébrico* $\mathcal{Z}_L(S)$ é o conjunto dos pontos de L^n que se anulam em todos os polinômios de S; isto é,

$$\mathcal{Z}_L(S) = \{p \in L^n \mid f(p) = 0 \text{ para todo } \ f \in S\}$$

Quando $S = \{h_1, \ldots, h_t\}$ escreveremos também $\mathcal{Z}_L(h_1, \ldots, h_t)$ em lugar de $\mathcal{Z}_L(S)$.

Na verdade, esta definição é um pouco mais geral que a que havíamos apresentado no capítulo 1. Lá, o conjunto S tinha que ser finito, e todas as constantes, fossem coeficientes de polinômios ou coordenadas de pontos pertenciam a $\mathbb{C}$. Aqui, estamos admitindo que S seja infinito e escolhemos trabalhar com dois corpos, um contido no outro. A razão porque S não precisa ser finito será explicada ao final da seção; quanto aos dois corpos, são necessários para alertá-lo de que, na prática, nossos polinômios deverão ter coeficientes racionais (para que seja fácil calcular com eles de modo exato), mas definirão pontos com coordenadas reais (para que possamos desenhá-los) ou complexas (para que seja fácil provar teoremas sobre eles). Como este último caso é o que mais ocorre nas aplicações, não subescreveremos nada a $\mathcal{Z}$ quando o corpo em questão forem os complexos.

Além da cúspide, muitas das curvas e superfícies que aparecem nos cursos de cálculo, geometria analítica e álgebra linear são conjuntos algébricos, entre elas incluem-se todas as cônicas e quádricas, como o elipsóide

$$\mathcal{Z}_{\mathbb{R}}(2x_1^2 + 2x_2^2 + 4x_3^2 - 1) \subseteq \mathbb{R}^3$$

e o parabolóide hiperbólico

$$\mathcal{Z}_{\mathbb{R}}(x_1x_2 + x_3 - 1) \subseteq \mathbb{R}^3.$$

Já

$$\mathcal{Z}_{\mathbb{R}}(x_1 + x_2, x_1 + x_3) \subseteq \mathbb{R}^3$$

é uma reta no espaço tridimensional, enquanto

$$\mathcal{Z}_{\mathbb{R}}(x_2^5 - x_3^4, x_1x_3 - x_2^2, x_1x_2^3 - x_3^3, x_1^2x_2 - x_3^2 = x_1^3 - x_2x_3) \subseteq \mathbb{R}^3$$

é uma curva cujas propriedades serão consideradas em mais detalhe na seção 3 do capítulo 9.

Voltando à relação entre um conjunto algébrico e seu ideal, e conservando a notação utilizada na definição acima, gostaríamos de provar que $X = \mathcal{Z}_L(S)$ pode ser reconstruído a partir do seu ideal $\mathrm{I}_K(X)$. Começaremos com a seguinte afirmação, que é um pouco mais modesta.

PROPOSIÇÃO 3.8. *Se J é o ideal de $K[x_1, \ldots, x_n]$ gerado por um subconjunto $S \subset K[x_1, \ldots, x_n]$, então*

$$\mathcal{Z}_L(S) = \mathcal{Z}_L(J).$$

Qualificamos a proposição de *mais modesta* porque *não* sabemos se J coincide com $\mathrm{I}_K(X)$. De fato, como logo veremos, estes ideais não coincidem; ou não exatamente.

DEMONSTRAÇÃO. Para provar a proposição, tomamos $f \in J$. Então existem polinômios $q_1, \ldots, q_t$ em $K[x_1, \ldots, x_n]$ e $h_1, \ldots, h_t \in S$, tais que

$$f = q_1h_1 + \cdots + q_th_t.$$

Portanto, para todo $p \in \mathcal{Z}_L(S)$, temos que

$$f(p) = q_1(p)h_1(p) + \cdots + q_t(p)h_t(p) = 0.$$

Assim,

$$\mathcal{Z}_L(S) \subseteq \mathcal{Z}_L(J).$$

Contudo, a inclusão oposta é evidentemente verdadeira porque, se p é zero de todo polinômio de J então, em particular, p é zero de todo polinômio em $S \subseteq J$, o que completa a demonstração da proposição. □

Esta igualdade mostra que todos os conjuntos de geradores de um ideal definem um mesmo conjunto algébrico. Isto é, J provê uma espécie de 'referencial absoluto', independente do sistema de polinômios escolhido para representar o conjunto algébrico. Um importante resultado advém da combinação desta observação com o resultado, mencionado ao final da seção anterior, de que todo ideal de $K[x_1, \ldots, x_n]$ admite um conjunto finito de geradores. Aplicando isto a J, concluímos que existe um conjunto *finito* $G \subset J$ tal que

$$\mathcal{Z}_L(S) = \mathcal{Z}_L(J) = \mathcal{Z}_L(G).$$

Em particular,

> qualquer conjunto algébrico pode ser definido a partir de um subconjunto *finito* de polinômios,

o que explica porque não precisamos introduzir esta hipótese na definição de conjunto algébrico. Ainda que o conjunto S de polinômios escolhido originalmente para definir $\mathcal{Z}_L(S)$ seja infinito, existe algum conjunto finito que também define $\mathcal{Z}_L(S)$.

Outra aplicação importante da proposição ocorre na solução de sistemas de equações. Por exemplo, aplicando o método de Gauss à matriz do sistema linear

$$\begin{aligned} h_1 &= x + 2y + 2z = 0 \\ h_2 &= 3x + 8y + z = 0 \\ h_3 &= 4x + 10y + 3z = 0 \end{aligned}$$

verificamos que este sistema é equivalente a

$$\begin{aligned} r_1 &= x + 2y + 2z = 0 \\ r_2 &= 2y - 5z = 0. \end{aligned}$$

Mas equivalente aqui quer dizer que estes dois sistemas têm as mesmas soluções, isto é, que

$$\mathcal{Z}_{\mathbb{R}}(h_1, h_2, h_3) = \mathcal{Z}_{\mathbb{R}}(r_1, r_2).$$

Para ver isto basta mostrar que r_1 e r_2 geram o mesmo ideal de $\mathbb{Q}[x, y, z]$ que h_1, h_2 e h_3. De fato, como

$$r_1 = h_1 \text{ e } r_2 = h_2 - 3h_1$$

então $\langle r_1, r_2 \rangle \subseteq \langle h_1, h_2, h_3 \rangle$, ao passo que a inclusão oposta segue de

$$h_1 = r_1,\ h_2 = r_2 + 3r_1 \text{ e } h_3 = r_2 + 4r_1.$$

Como o sistema de duas equações $\mathcal{Z}(r_1, r_2)$ pode ser parametrizado na forma

$$\{(-3z, \frac{5}{2}z, z) \,|\, z \in \mathbb{R}\},$$

obtivemos assim uma representação para todas as soluções do sistema originalmente dado. No capítulo 5 veremos como o método de Gauss pode ser estendido a sistemas não lineares, o que tornará a proposição 3.8 a chave de todas as nossas futuras aplicações.

Tudo isto é muito interessante, e importante, mas não explica como é possível recuperar um conjunto algébrico a partir de seu ideal. Para isto precisamos primeiro identificar exatamente qual é este ideal. Esta é nossa meta para a próxima seção.

4. O radical

Convém começar relembrando precisamente o problema que nos foi legado da seção anterior. Dados corpos $K \subset L$ e um subconjunto S do anel de polinômios $K[x_1, \ldots, x_n]$, desejamos calcular o ideal $\mathrm{I}(X)$ corresponde ao conjunto algébrico

$$X = \mathcal{Z}_L(S)$$

e provar que é possível recuperar X a partir deste ideal.

Embora $\mathrm{I}(X)$ seja frequentemente igual ao ideal gerado por S, isto não é sempre verdadeiro como, aliás, já indicamos na seção anterior. Começamos com um exemplo, que ilustra as dificuldades que devemos esperar. Tome $S = \{x_1^2, x_2^2\}$ em $\mathbb{C}[x_1, x_2]$. Neste caso,

$$\mathcal{Z}_L(\langle x^2, y^2\rangle) = \{(0,0)\};$$

de modo que

$$\mathrm{I}(\{(0,0)\}) = \{f \in \mathbb{C}[x_1, x_2] : f(0,0) = 0\}.$$

Mas um polinômio f se anula na origem se, e somente se, seu termo constante é nulo; isto é, se pertence ao ideal gerado pelas variáveis. Em outras palavras,

$$\mathrm{I}(\{(0,0)\}) = \langle x_1, x_2\rangle,$$

que não é igual a

$$\langle S\rangle = \langle x_1^2, x_2^2\rangle.$$

De fato, o menor grau possível para um elemento deste último ideal é dois, ao passo que $\mathrm{I}(\{(0,0)\})$ contém elementos de grau um.

Na verdade, coisa semelhante ocorre em circunstâncias muito mais gerais. Voltando à notação do início do capítulo, suponha que, para algum polinômio f, temos $f^n \in \langle S\rangle$. Neste caso,

$$(f^n)(p) = 0 \text{ para todo } \; p \in \mathcal{Z}_L(S).$$

Mas

$$0 = (f^n)(p) = (f(p))^n$$

implica que $f(p) = 0$. Como isto vale para todo ponto de $\mathcal{Z}_L(S)$, temos por definição que

$$f \in \mathrm{I}(\mathcal{Z}_L(S))$$

mas f não pertence necessariamente ao ideal gerado por S, como foi o caso no exemplo acima. O surpreendente é que nada pior que isto pode acontecer, pelo menos se supusermos que $L = \mathbb{C}$, que é o que faremos de agora em diante.

Começamos introduzindo um novo conceito da teoria de ideais. Seja A um anel e I um ideal de A. O *radical* $\sqrt{I}$ de I é o conjunto dos $a \in A$ para os quais existe um $k \geq 0$ inteiro, tal que $a^k \in I$. Isto é, $\sqrt{I}$ é o conjunto dos elementos de A que têm alguma potência em I. Observe que a inclusão $I \subseteq \sqrt{I}$ é sempre verdadeira, mas pode ser própria. Por exemplo,

$$x, y \in \sqrt{\langle x^2, y^2 \rangle},$$

mas não pertencem a $\langle x^2, y^2 \rangle$. A principal propriedade do radical é que ele é um ideal.

PROPOSIÇÃO 3.9. *Se A é um anel e I é um ideal de A, então $\sqrt{I}$ também é um ideal de A.*

DEMONSTRAÇÃO. Como $0 \in I \subseteq \sqrt{I}$, basta mostrar que

- se $a, b \in \sqrt{I}$, então $a + b \in \sqrt{I}$, e que
- se $a \in A$ e $b \in \sqrt{I}$ então $ba \in \sqrt{I}$,

e teremos provado que o radical de I é um ideal. O segundo item é mais fácil que o primeiro, por isso vamos começar por ele.

Suponha, então, que $a \in A$ e $b \in \sqrt{I}$. Pela definição do radical, temos que $b^k \in I$, para algum $k \geq 0$. Como I é um ideal,

$$a^k b^k = (ab)^k \in I.$$

Logo, $ab \in \sqrt{I}$, e provamos que $\sqrt{I}$ é fechado para o produto por qualquer elemento de A.

Para mostrar que $\sqrt{I}$ é fechado para a soma, digamos que $a, b \in \sqrt{I}$. Neste caso, existem inteiros positivos k e m tais que $a^k \in I$ e $b^m \in I$. Na continuação deste argumento, lembre-se que se $s \geq k$ é um inteiro positivo, então

$$a^s = a^{s-k} a^k \in I.$$

Analogamente, $s \geq m$ implica que $b^s \in I$.

Uusaremos isto para mostrar que alguma potência de $a + b$ pertence a I. Pelo binômio de Newton (veja exercício ??? do capítulo 2), temos que

$$(a+b)^s = \sum_{i=1}^{s} \binom{s}{i} a^i b^{n-i}.$$

Pelo que vimos acima, se $i \geq k$, então $a^i b^j \in I$, uma vez que I é um ideal de A. Entretanto, i varia de zero a s, de modo que podemos ter $i < k$. Contudo, neste caso, a parcela do binômio contém b^{s-i}. Portanto, bastaria que $s - i \geq m$ e teríamos que $a^i b^{s-i} \in I$. Em outras palavras, se escolhermos s de modo

que $i \geq k$ ou $s - i \geq m$, cada uma das parcelas do binômio estará em I, e poderemos concluir que $(a+b)^s \in I$. Mas, para que $s - i \geq m$ quando $i < k$, devemos ter

$$s - k > s - i \geq m,$$

de modo que $s > m + k$. Assim, $(a + b)^{m+k+1} \in I$, de forma que $a + b \in \sqrt{I}$. □

Voltando ao exemplo anterior, vimos que

$$\langle x, y\rangle \subseteq \sqrt{\langle x^2, y^2\rangle}.$$

Contudo, esta inclusão não pode ser própria. Se fosse, $\sqrt{\langle x^2, y^2\rangle}$ conteria um polinômio h cujo termo constante c não é nulo. Mas, neste caso, $h - c$ seria um polinômio com termo constante nulo, de forma que

$$h - c \in \langle x, y\rangle \subseteq \sqrt{\langle x^2, y^2\rangle}.$$

Com isto h e $h - c$ pertenceriam ao radical e, como este é um ideal, teríamos que

$$c = h - (h - c) \in \sqrt{\langle x^2, y^2\rangle};$$

o que é evidentemente falso pois, sendo uma constante não nula, c não pode anular-se na origem. Logo,

$$\sqrt{\langle x^2, y^2\rangle} = \langle x, y\rangle,$$

e determinamos nosso primeiro radical. Em geral, calcular exatamente o radical não é uma tarefa fácil. Por isso os exemplos mais interessantes terão que esperar até o capítulo 9. Nossa meta imediata, contudo, é usar os radicais para calcular explicitamente o ideal de um conjunto algébrico. Antes, porém, precisamos de um teorema extremamente importante.

TEOREMA 3.10. *Sejam I um ideal e f um elemento do anel de polinômios $K[x_1, \ldots, x_n]$, então $f(p) = 0$ para todo $p \in \mathcal{Z}(I)$ se, e somente se, $f \in \sqrt{I}$.*

Este teorema é consequência do famoso *teorema dos zeros*, descoberto por D. Hilbert em 1893, e que provaremos no apêndice I. Nesta seção vamos nos contentar em enunciar o teorema dos zeros, e usá-lo para provar o teorema 3.10.

TEOREMA DOS ZEROS. *O conjunto algébrico $\mathcal{Z}(I)$ não é vazio se, e somente se, I é um ideal próprio de $K[x_1, \ldots, x_n]$.*

Em outras palavras, o *teorema dos zeros* nos diz que um ideal próprio é aquele que *tem zeros*. O argumento que leva à demonstração do teorema 3.10 a partir do teorema dos zeros é conhecido como *truque de Rabinowitch*. Como este argumento será utilizado nas aplicações que faremos no capítulo 6, convém enunciá-lo claramente. Para isso, formularemos uma proposição, um pouco mais técnica, da qual o teorema 3.10 segue como um corolário imediato. Começamos estabelecendo a seguinte notação.

Dados um polinômio f e um ideal I de $K[x_1, \ldots, x_n]$, seja

$$J(I, f) = \langle 1 - zf \rangle + K[x_1, \ldots, x_n, z]I.$$

Isto é, $J(I, f)$ é o ideal do anel de polinômios, nas antigas variáveis $x_1, \ldots, x_n$ e em uma nova variável z, gerado pelos polinômios de I e por $1-zf$. Assim, os zeros de $J(I, f)$ formam um conjunto algébrico em $\mathbb{C}^{n+1}$. A motivação para esta definição ficará clara no início da demonstração da próxima proposição.

PROPOSIÇÃO 3.11. *Sejam f um polinômio e I um ideal do anel de polinômios $K[x_1, \ldots, x_n]$. As seguintes afirmações são equivalentes:*

(1) *f se anula em todos os pontos de $\mathcal{Z}(I)$;*
(2) *$J(I, f) = K[x_1, \ldots, x_n, z]$;*
(3) *$f \in \sqrt{I}$.*

DEMONSTRAÇÃO. Mostraremos que (1) implica (2), que implica (3), que implica (1).

Suponha, então, que $f(p) = 0$ sempre que $p \in \mathcal{Z}(I)$. Neste caso, temos que

$$(1 - zf)(p) = 1 - zf(p) = 1,$$

de modo que o polinômio $1 - zf$ não pode se anular em nenhum ponto da forma $(p, z_0) \in \mathbb{C}^{n+1}$ para o qual $p \in \mathcal{Z}(I)$. Como,

$$\mathcal{Z}(J(I, f)) \subseteq \mathcal{Z}(I) \times \mathbb{C},$$

podemos concluir que $\mathcal{Z}(J(I, f)) = \emptyset$. Portanto, pelo *teorema dos zeros*, $J(I, f) = K[x_1, \ldots, x_n, z]$, e mostramos que (1) implica (2).

Passemos à dedução de (3) a partir de (2). Pelo *teorema da base de Hilbert* enunciado ao final da seção anterior, existem polinômios $g_1, \ldots, g_s$, contidos em $K[x_1, \ldots, x_n]$, que geram I. Em particular, os gs são polinômios apenas nas variáveis $x_1, \ldots, x_n$, com coeficientes em K. Assim, podemos escrever

$$J(I, f) = \langle g_1, \ldots, g_s, 1 - zf \rangle.$$

Como estamos supondo que $J(I, f) = K[x_1, \ldots, x_n, z]$, podemos concluir que existem $h_1, \ldots, h_{s+1} \in K[x_1, \ldots, x_n, z]$

$$1 = h_1 g_1 + \cdots + h_s g_s + h_{s+1}(1 - zf). \tag{30}$$

Aqui começa a parte mais surpreendente da demonstração. Como z é uma variável, podemos substituí-la pelo que quisermos, e a identidade (30) continuará sendo verdadeira. Nossa escolha será fazer $z = 1/f$. Mas lembre-se que os g_is não contêm z, de forma que a substituição de z por $1/f$ não irá afetá-los. Com isto, obtemos

$$1 = h_1(\underline{x}, \frac{1}{f})g_1(\underline{x}) + \cdots + h_s(\underline{x}, \frac{1}{f})g_s(\underline{x}) + h_{s+1}(\underline{x}, \frac{1}{f})\left(1 - \frac{1}{f} \cdot f\right), \tag{31}$$

em que $\underline{x}$ corresponde a $x_1, \ldots, x_n$.

Observe que a expressão em (31) não é polinomial, já que o polinômio $f \in K[x_1, \ldots, x_n]$ aparece no denominador da fração. O que temos, na verdade, é uma equação no anel de funções racionais $K(x_1, \ldots, x_n)$, que nem por isso

deixa de ser uma expressão idônea. Como o cancelamento entre 1 e $f \cdot 1/f$ faz com que a última parcela de (31) se anule, obtemos

$$1 = h_1(\underline{x}, \frac{1}{f})g_1(\underline{x}) + \cdots + h_s(\underline{x}, \frac{1}{f})g_s(\underline{x}).$$

Mas, se $k \geq 1$ é maior que os graus de todos os h_is, então $q_i f^k h_i(\underline{x}, \frac{1}{f})$ é um polinômio em $K[x_1, \ldots, x_n]$ para todo $1 \leq i \leq s$. Assim, multiplicando a equação anterior por f^k, concluímos que

$$f^k = q_1 g_1 + \cdots + q_s g_s \in \langle g_1, \ldots, g_s \rangle = I,$$

que equivale a dizer que $f \in \sqrt{I}$, como queríamos mostrar.

Finalmente, precisamos provar que (3) implica (1), que acaba sendo a parte mais fácil da demonstração. De fato, se $f \in \sqrt{I}$, então existe $k \geq 1$ tal que $f^k \in I$. Mas isto significa que $f^k(p) = 0$ para todo $p \in \mathcal{Z}(I)$, que só pode ocorrer se $f(p) = 0$. □

Do teorema 3.10 é fácil não apenas calcular o ideal de um conjunto algébrico X, como provar que dele se pode reconstruir todo o X.

TEOREMA 3.12. *Se I é um ideal $K[x_1, \ldots, x_n]$, então,*

$$\mathrm{I}(\mathcal{Z}(I)) = \sqrt{I}.$$

Reciprocamente, se $X \subseteq \mathbb{C}^n$ for um conjunto algébrico, então

$$\mathcal{Z}(\mathrm{I}(X)) = X.$$

DEMONSTRAÇÃO. A inclusão $\sqrt{I} \subseteq \mathrm{I}(\mathcal{Z}(I))$ é muito fácil, e fica por sua conta, provaremos apenas a inclusão oposta. Suponha que $f \in \mathrm{I}(\mathcal{Z}(I))$. Isto significa que $f(p) = 0$ para todo $p \in X = \mathcal{Z}(I)$. Assim, pelo teorema 3.10, $f \in \sqrt{I}$. Portanto, $\mathrm{I}(\mathcal{Z}(I)) \subseteq \sqrt{I}$.

Para provar a recíproca, suponha que X é um conjunto algébrico de $\mathbb{C}^n$. Por definição isto significa que existe um ideal J tal que $X = \mathcal{Z}(J)$. Pela primeira parte do teorema,

$$\mathrm{I}(X) = \sqrt{J},$$

de modo que

$$\mathcal{Z}(\mathrm{I}(X)) = \mathcal{Z}(\sqrt{J}) = \mathcal{Z}(J) = X,$$

que é a igualdade que desjávamos mostrar. □

Como consequência deste teorema podemos concluir que o conjunto

$$\Gamma = \{(t, \mathrm{sen}(t) | t \in \mathbb{C}\},$$

não pode ser algébrico. De fato, como $\mathrm{I}(\Gamma) = \{0\}$,

$$\mathcal{Z}(\mathrm{I}(\Gamma)) = \mathcal{Z}(\{0\}) = \mathbb{C}^2$$

que é, evidentemente diferente de Γ. Uma curva que não corresponde a nenhum conjunto algébrico é chamada de *transcendente*, na terminologia introduzida por Leibniz e que usamos até hoje. Veja, por exemplo, a citação da Enciclopédia de Diderot e D'Alembert na página 16.

Será que você notou o blefe no argumento acima? Este exemplo em muito se parece com o da página 82, que foi onde verificamos que o ideal de Γ é zero. Contudo, naquele exemplo o parâmetro era real e aqui foi escolhido como sendo complexo. Fizemos isto para obter uma curva em $\mathbb{C}^2$ à qual pudéssemos aplicar o teorema. Isto é necessário porque o teorema 3.12 é falso sobre os reais. Um contra-exemplo bem simples é obtido tomando-se $S = \{x_1^2 + x_2^2\}$. Neste caso,

$$\mathcal{Z}_{\mathbb{R}}(S) = \{(0,0)\}$$

de modo que,

$$\mathrm{I}_{\mathbb{R}}(\mathcal{Z}_{\mathbb{R}}(S)) = \langle x_1, x_2 \rangle$$

que não é igual a

$$\langle S \rangle = \langle x_1^2 + x_2^2 \rangle.$$

Encerraremos a seção com mais algumas propriedades básicas do radical. Antes, porém, precisamos de duas definições. A primeira você provavelmente conhece no contexto das matrizes. Um elemento a de um anel A é *nilpotente* se existe um inteiro $k > 0$ tal que $a^k = 0$. É claro que um domínio não pode ter nilpotentes não nulos, mas há anéis bem conhecidos nossos que admitem tais elementos. O exemplo mais simples é, provavelmente, $\mathbb{Z}_{p^n}$, quando p é primo e $n > 0$. Neste caso, $\overline{p} \neq \overline{0}$, porém $\overline{p}^n = \overline{p^n} = \overline{0}$. A segunda definição é mera questão de comodidade. Diremos que um ideal é *radical* se coincidir com o seu radical.

PROPOSIÇÃO 3.13. *Sejam A um anel, e I, J ideais de A.*

(1) $\sqrt{\sqrt{I}} = \sqrt{I}$.
(2) $\sqrt{I}$ *é o menor ideal radical que contém* I.
(3) $\sqrt{0}$ *é igual ao conjunto dos elementos nilpotentes de* A.
(4) *Toda interseção finita de ideais radicais é um ideal radical.*
(5) $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

DEMONSTRAÇÃO. Como todo ideal está contido em seu radical, temos que $\sqrt{I} \subseteq \sqrt{\sqrt{I}}$. Logo, para provar (1), basta verificar a inclusão oposta. Mas, se $a \in \sqrt{\sqrt{I}}$, então, pela definição do radical, existe algum inteiro $k > 0$ tal que $a^k \in \sqrt{I}$. Por sua vez, isto implica que existe algum $m > 0$ para o qual $(a^k)^m \in I$. Assim, $a^{km} \in I$ e, como $mk > 0$, isto implica que $a \in \sqrt{I}$, e temos (1).

Para provar (2) basta mostrar que, se J é um ideal radical que contém I, então J também contém $\sqrt{I}$. Como $\sqrt{I}$ é radical por (1), isto significa que tem que ser o menor de todos os ideais radicais que contêm I. Mas, se J é um ideal que contém I e $a^k \in I$, para algum $k > 0$, então $a^k \in J$. Assim, se J for radical, teremos que $a \in J$, sempre que $a^k \in I$. Isto significa que todo elemento do radical de I pertence a J, o que prova (2).

(3) é imediato, uma vez que $a \in \sqrt{0}$ se, e somente se, existe $k > 0$ tal que $a^k = 0$; que é a definição de nilpotente. Para provar (4), suponhamos que

$J_1, \ldots, J_s$ são ideais radicais de A. Se

$$a^k \in J_1 \cap \cdots \cap J_s,$$

então $a^k \in J_i$, para todo $1 \leq i \leq s$. Entretanto, J_i é um ideal radical, o que implica que $a \in J_i$ para cada $1 \leq i \leq s$. Mas isto equivale a dizer que

$$a \in J_1 \cap \cdots \cap J_s,$$

como afirmamos em (4).

Finalmente, sejam I e J ideais quaisquer de A. Como,

$$I \subseteq \sqrt{I} \quad \text{e} \quad J \subseteq \sqrt{J},$$

então,

$$I \cap J \subseteq \sqrt{I} \cap \sqrt{J}.$$

Contudo, $\sqrt{I} \cap \sqrt{J}$ é um ideal radical por (4). Portanto, segue de (1) que

$$\sqrt{I \cap J} \subseteq \sqrt{I} \cap \sqrt{J}.$$

Por outro lado, se $a \in \sqrt{I} \cap \sqrt{J}$ então, $a \in \sqrt{I}$ e $a \in \sqrt{J}$. Logo, existem inteiros positivos k e ℓ tais que

$$a^k \in I \quad \text{e} \quad a^\ell \in J.$$

Tomando, $m = \max\{k, \ell\}$, vemos que

$$a^m \in I \quad \text{e} \quad a^m \in J;$$

isto é, $a^m \in I \cap J$. Mas isto implica que $a \in \sqrt{I \cap J}$, e completa a demonstração de (5). □

5. Comentários e complementos

Neste capítulo introduzimos os principais entes algébricos do livro: os anéis de polinômios em várias indeterminadas, seus ideais e os conjuntos algébricos que eles representam. Desde o capítulo 1 sabemos que os problemas de geometria que queremos resolver por computador podem ser representados em termos de conjuntos algébricos. Neste capítulo, por sua vez, descobrimos que tais conjuntos podem ser definidos por seus ideais em um anel de polinômios. Resta-nos identificar com mais detalhes o que ainda está por fazer para que a estratégia esboçada nó capítulo 1 possa ser formalizada e completamente implementada.

Para começar, se pretendemos calcular com polinômios em um computador precisamos representá-los de alguma forma "dentro da máquina". Portanto o primeiro ponto de nossa agenda deve ser:

Item 1: Representar polinômios em mais de uma variável no computador.

Em segundo lugar, os exemplos estudados no capítulo 1 sugerem que, para implementar a demonstração automática de teoremas de geometria precisamos resolver o seguinte problema:

> Dados polinômios $h_1, \ldots, h_t, c$ no anel $\mathbb{C}[x_1, \ldots, x_n]$, determinar se c pode ser escrito como combinação linear polinomial dos hs.

Este problema pode ser facilmente reformulado em termos de ideais. Como se trata de um dos problemas mais importantes de que trata este livro, convém formulá-lo com precisão.

PROBLEMA DA PERTINÊNCIA. *Dados um polinômio c e um ideal $I = \langle h_1, \ldots, h_t \rangle$ do anel $\mathbb{C}[x_1, \ldots, x_n]$, determinar se c pertence a I.*

Se tivéssemos apenas dois polinômios h e c, em apenas uma variável, o problema seria fácil de resolver. Bastaria dividir c por h e verificar se o resto é nulo, com isto determinaríamos se c é ou não múltiplo de h. Uma solução ingênua para o problema geral consistiria em generalizar esta estratégia para várias indeterminadas. Para isto, precisaríamos de um algoritmo que nos permitisse dividir um polinômio por vários outros. De posse de um tal algoritmo, poderíamos dividir c por $h_1, \ldots, h_n$ e verificar se o resto é zero, exatamente como no caso de uma variável—ou pelo menos é isto que esperamos poder fazer. Copiando de perto o caso de uma variável, podemos formular nossa meta de maneira mais precisa:

> **Item 2:** Dados polinômios $h_1, \ldots, h_t, c$ no anel $\mathbb{C}[x_1, \ldots, x_n]$, dividir c por $h_1, \ldots, h_t$ de modo que
>
> $$c = q_1 h_1 + \cdots + q_t h_t + r,$$
>
> em que $q_1, \cdots, q_t$ e r são polinômios em $\mathbb{C}[x_1, \ldots, x_n]$. Além disso esperamos que $r = 0$ se, e somente se, c for combinação linear polinomial dos hs.

Estes dois itens de nossa agenda serão completamente resolvidos (com algumas surpresas) no próximo capítulo.

6. Exercícios

1. Sejam f e g polinômios no anel $K[x_1, \ldots, x_n]$. Mostre que $\langle f \rangle = \langle g \rangle$ se, e somente se existe uma constante não nula $c \in K$ tal que $f = cg$.

2. Seja $A = K[x_1, \ldots, x_n]$ o anel de polinômios sobre um corpo K nas indeterminadas $x_1, \ldots, x_n$ e $Q(A) = K(x_1, \ldots, x_n)$ o corpo de funções racionais correspondentes. Suponha que y é uma nova variável.
   (a) Defina o que significa um polinômio ser primitivo em $A[y]$.
   (b) Prove que o *Lema de Gauss* e todos os seus corolários continuam verdadeiros quando substituímos $\mathbb{Z}$ por A e $\mathbb{Q}$ pelo corpo $Q(A)$.

3. Um anel é *fatorial* se cada um de seus elementos pode ser escrito, de maneira única, como produto de elementos irredutíveis.
   (a) Dê uma definição formal de anel fatorial.
   (b) Dê exemplos de anéis fatoriais.

4. Mostre que o Lema de Gauss e seus corolários continuam verdadeiros se substituímos $\mathbb{Z}$ por um anel fatorial A e $\mathbb{Q}$ por seu corpo de frações $Q(A)$.

5. Prove que se A é um anel fatorial, então o anel de polinômios $A[x]$ também é.

6. Prove, por indução em n, que se A é um anel fatorial, então o anel de polinômios $A[x_1, \ldots, x_n]$ também é.

7. Seja I_n o ideal de $K[x_1, \ldots, x_n]$ gerado por $x_1, \ldots, x_n$. O objetivo deste exercício é mostrar, por indução em n, que o ideal I_n não pode ser gerado por menos de n elementos. Seja J_{n-1} o ideal de $K[x_1, \ldots, x_n]$ gerado por $x_1, \ldots, x_{n-1}$.
   (a) Mostre que se o ideal I_{n-1} de $K[x_1, \ldots, x_{n-1}]$ não pode ser gerado por menos de $n-1$ elementos, então o ideal J_{n-1} de $K[x_1, \ldots, x_n]$ também não pode ser gerado por menos de $n-1$ elementos. Observe que os geradores são iguais mas os ideais pertencem a anéis de poliômios diferentes.
   (b) Mostre que $x_n \notin J_{n-1}$.
   (c) Conclua o resultado desejado, por indução, a partir de (a) e (b).

8. Sejam I e J ideais de um anel A. O objetivo desta questão e da seguinte é definir o ideal produto IJ.
   (a) Mostre que se I e J são ideais principais, então o produto dos conjuntos $I \cdot J$, definido na página 71, é um ideal de A.
   (b) Seja K um corpo. Mostre que se $A = K[x_1, x_2, x_3]$ e
   $$I = \langle x_1, x_2 \rangle \quad \text{e} \quad J = \langle x_1, x_3 \rangle,$$
   então o produto dos conjuntos $I \cdot J$ *não* é um ideal de A.

9. Sejam I e J ideais de um anel A. Considere o conjunto IJ gerado pelo produto de conjuntos $I \cdot J$, definido na página 71. Isto é,
   $$IJ = \langle I \cdot J \rangle = \{a_1 b_1 + \cdots a_k b_k : a_i \in I, b_i \in J \text{ e } k \in \mathbb{N}\}.$$
   (a) Mostre que se I e J são ideais principais, então IJ também é.
   (b) Mostre que se I e J são ideais finitamente gerados, então IJ também é.

10. Dizemos que dois ideais I e J de um anel A são *co-máximos* se $I + J = A$.
   (a) Mostre que se I é um ideal máximo de A e $J \neq I$ um ideal não nulo qualquer de A, então I e J são co-máximos.
   (b) Seja K um corpo. Dê exemplo de dois ideais co-máximos I e J em $K[x_1, x_2]$, nenhum dos quais é máximo.
   (c) Mostre que se A é um anel no qual quaisquer dois ideais não nulos são co-máximos, então A é um corpo.

11. Sejam I_1, I_2 e J ideais de um anel A. O objetivo desta questão é investigar a igualdade
$$(I_1 + I_2)J = I_1J + I_2J.$$
(a) Mostre que esta igualdade vale sempre que o ideal J for principal.
(b) Seja K um corpo. Dê exemplos de ideais em $K[x_1, x_2]$ para os quais esta igualdade é falsa.
(c) Prove que, se I_1 e I_2 forem co-máximos, então a igualdade é verdadeira.

12. A *componente homogênea* de grau d de um polinômio em várias indeterminadas é a soma de todos os seus monômios de grau d. Seja K um corpo e $f, g \in K[x_1, \ldots, x_n]$. Observe que o grau total de f é igual ao grau de sua componente homogênea não nula de maior grau.
(a) Mostre que a componente homogênea não nula de maior grau de fg é igual ao produto das componentes homogêneas não nulas de maior grau de f e de g.
(b) Mostre que o produto de dois polinômios homogêneos não nulos também é não nulo.
(c) Mostre que o grau total de fg é igual a soma dos graus de f e g.

13. O objetivo deste exercício é obter uma fórmula para o número de monômios de grau k em n variáveis, em que k e n são inteiros positivos.
(a) Determine uma fórmula binomial para o número de soluções inteiras não negativas da equação
$$a_1 + a_2 + \cdots + a_n = k.$$
(b) Use (a) para mostrar que o número de monômios de grau k em n variáveis é igual a $\binom{n+k-1}{k-1}$.

14. Seja A um anel e $f, g \in A[x_1, \ldots, x_n]$.
(a) Prove que se A é um domínio então fg é um monômio se, e somente se, f e g são monômios.
(b) Dê exemplos de um anel A com divisores de zero e polinômios $f, g \in A[x]$ que não são monômios, tais que fg é um monômio.

15. Seja L um corpo, K um subcorpo de L e $X \subseteq L^n$. Prove que o conjunto definido por
$$\mathrm{I}_K(X) = \{f \in K[x_1, \ldots, x_n] : f(p) = 0 \text{ para todo } p \in X\}$$
é um ideal de $K[x_1, \ldots, x_n]$.

16. Prove que cada um dos conjuntos abaixo é algébrico:
(a) $\{(t^2 - t, t^3) \,|\, t \in \mathbb{R}\}$;
(b) $\{(t^n, t^m) \,|\, t \in \mathbb{R}\}$, em que $m, n \in \mathbb{N}$;
(c) $\{(t^{1/2}, t^{1/3}) \,|\, t \in \mathbb{R}\}$;
(d) $\{(t^{1/2}, t^{1/3}) \,|\, t \in \mathbb{R}\}$;

(e) $\{(a\cos(t), b\text{sen}(t) \mid t \in \mathbb{R}\}$, em que a, b são números reais não nulos;
(f) $\{(t, 1/t) \mid t \in \mathbb{R}\}$;
(g) $\{(a\cos^3(t), a\text{sin}^3(t) \mid t \in \mathbb{R}\}$;
(h) $\{(t, t^2, t^3) \mid t \in \mathbb{R}\}$.

17. Descrevemos abaixo as equações polares de várias curvas clássicas. Prove que cada uma delas é algébrica, determinando suas equações polinomiais:
(a) $r = m\text{sen}(n\theta)$, em que m e n são inteiros co-primos;
(b) $r = a\cos(\theta) \pm b$;
(c) $r = 2a(1 + \cos(\theta))$;
(d) $r = 4a\cos^3(\theta/3)$;
(e) $r = 2a\tan(\theta)\text{sen}(\theta)$;
(f) $r = a\cot(\theta)$;
(g) $r = b + 2a\cos(\theta)$;
em que $a, b \in \mathbb{R}$.

18. Prove que a curva de equação $x^{2/3} + y^{2/3} = 1$ é algébrica e sua equação polinomial tem grau seis. Esta curva é conhecida como *astróide*.

19. Seja C uma curva algébrica em $\mathbb{C}^2$ definida por uma equação polinomial de grau n. Prove que a interseção de C com qualquer reta não pode conter mais de n pontos.

20. Use o exercício anterior para dar uma outra demonstração de que a curva Γ definida como o gráfico da função seno não pode ser algébrica; cf. página 82.

21. Prove que nenhum dos conjuntos abaixo é algébrico:
(a) $\{(t, \cos(t)) \mid t \in \mathbb{R}\}$;
(b) $\{(\text{sen}(at), \cos(bt)) \mid t \in \mathbb{R}\}$ em que a e b são números reais cuja razão a/b é irracional.

22. Prove que se K é um corpo então
$$\sqrt{\langle x_1^{e_1}, \ldots, x_n^{e_n}\rangle} = \langle x_1, \ldots, x_n\rangle$$
em $K[x_1, \ldots, x_n]$, quaisquer que sejam os inteiros positivos $e_1, \ldots, e_n$.

23. Seja p um primo e n um inteiro positivo. Calcule o radical do ideal nulo em $\mathbb{Z}_{p^n}$.

24. Prove que se I é ideal radical de um anel A, então $\sqrt{I^n} = I$, qualquer que seja o inteiro positivo n.

25. Sejam I e J ideais de um anel A. Prove as seguintes propriedades do radical:
(a) $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$;
(b) $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$;

26. Sejam I e J ideais de um anel A. Prove que $I + J = A$ se, e somente se, $\sqrt{I} + \sqrt{J} = A$.

CAPíTULO 4

Ordens monomiais e divisão

Neste capítulo tratamos da representação de polinômios no computador e damos um grande passo na solução do problema da pertinência de um polinômio a um ideal dado. Ao longo de todo capítulo K denota um corpo, mas você pode pensar em K como sendo uma maneira abreviada de dizer que todos estes resultados valem para $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.

1. Motivação

O problema que desejamos abordar nesta seção é de caráter eminentemente prático: como representar um polinômio no computador? À primeira vista não parece haver nenhum problema, bastaria deixar que o computador representasse o polinômio como um vetor de coeficientes.

Entretanto, isso só é fácil de fazer se o polinômio tem apenas uma variável. Neste caso existe uma associação natural entre o polinômio

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

e o vetor

$$(a_n, a_{n-1}, \ldots, a_1, a_0).$$

Esta associação é possível porque temos uma ordenação dos termos deste polinômio de acordo com o grau.

Se o polinômio tem duas variáveis já não há uma associação tão natural. Para entender porque, escreva o polinômio como uma soma de termos que correspondem ao produto de um monômio em duas variáveis por uma constante. Por exemplo,

$$f = 3x_1^2 x_2 + 4x_1^3 + 5x_1^3 x_2^2 + 7x_1^2 + 8x_2^5 + 1.$$

Neste caso se tentarmos ordenar os termos do polinômio de acordo com o grau nos deparamos com o fato de f ter dois termos que correspondem a monômios diferentes, mas que têm o mesmo grau. Como decidir qual deles deveria vir primeiro na apresentação do polinômio como um vetor? Observe que a decisão não pode ser arbitrária, porque do contrário não teremos como reconstruir o polinômio a partir do vetor.

Uma saída possível consiste em utilizar a construção recursiva do anel $K[x_1, x_2]$. Para isto, começamos com $R = K[x_2]$ e, em seguida, fazemos $K[x_1, x_2] = R[x_1]$. Isto significa que estamos considerando um polinômio nas variáveis x_1 e x_2 como sendo um polinômio na variável x_1, cujos coeficientes

são polinômios na variável x_2. Por exemplo, o polinômio f do exemplo acima será escrito na forma

$$f = (5x_2^2 + 4)x_1^3 + (3x_2 + 7)x_1^2 + (8x_2^5 + 1) \tag{32}$$

No computador, esta representação corresponde a associar a um polinômio de $K[x_1, x_2]$ um vetor (o polinômio na variável x_1) cujas entradas também são vetores (os polinômios na variável x_2).

Contudo, do ponto de vista prático, esta representação tem vários incovenientes. O mais óbvio é que podemos querer manipular o polinômio na forma expandida; isto é, como uma soma de termos. Contudo, se temos o polinômio escrito na forma da equação (32), basta expandi-lo usando a propriedade distributiva para obter uma soma de monômios. Fazendo isto neste exemplo, teremos

$$f = 5x_2^2x_1^3 + 4x_1^3 + 3x_2x_1^2 + 7x_1^2 + 8x_2^5 + 1. \tag{33}$$

Note que, se escrevermos o polinômio tomando cuidado em preservar a ordem em que os termos apareciam antes da expansão, obtemos como resultado uma soma de termos que sempre estarão escritos na mesma ordem. Isto sugere que esta maneira de proceder induz uma ordenação natural dos termos de um polinômio. Entretanto, cada termo de um polinômio é composto de dois ingredientes: o *coeficiente*, que é uma constante, e o *suporte*, que é um monômio nas variáveis que formam o polinômio. Se o polinômio tem somente uma variável então o suporte é apenas uma potência desta variável. Portanto, quando arranjamos os termos de um polinômio em uma variável, da esquerda para a direita, em ordem descrescente dos graus, estamos de fato ordenando os suportes dos termos deste polinômio: os coeficientes de cada termo não desempenham nenhum papel nesta ordenação. Isto continuará sendo verdade para polinômios de duas variáveis, uma vez que estamos ordenando seus termos a partir da construção recursiva.

Desta discussão concluímos que o que desejamos aprender a ordenar são os monômios que entram na composição de um polinômio, e não exatamente os seus termos. Contudo, continuaremos a falar da ordenação dos termos, quando for conveniente, significando com isso a ordenação dos suportes destes termos. Por analogia com o caso de polinômios em uma variável, diremos que o procedimento recursivo exposto acima ordena os monômios de um polinômio do maior para o menor, quando o polinômio é lido da esquerda para a direita.

Precisamos, portanto, descobrir como a construção recursiva do anel de polinômios nos permite decidir qual o maior dentre dois monômios dados. Sejam $x_1^{\alpha_1}x_2^{\alpha_2}$ e $x_1^{\beta_1}x_2^{\beta_2}$ estes monômios. A maneira mais precisa de formular o que desejamos fazer consiste em dizer que queremos determinar as condições que α_1 e β_1, e α_2 e β_2, devem satisfazer para que, depois de expandida, a soma desses dois monômios tenha a forma

$$h = x_1^{\alpha_1}x_2^{\alpha_2} + x_1^{\beta_1}x_2^{\beta_2}. \tag{34}$$

É fácil ver que há duas situações diferentes em que isto pode acontecer. A primeira, e mais óbvia, ocorre quando $\alpha_1 > \beta_1$—sem que seja necessário impor nenhuma restrição sobre α_2 ou β_2. Neste caso, mesmo antes da expansão, h já tem a aparência da equação (34). A outra possibilidade ocorre quando $\alpha_1 = \beta_1$ e $\alpha_2 > \beta_2$, de forma que antes da expansão temos que

$$h = x_1^{\alpha_1}(x_2^{\alpha_2} + x_2^{\beta_2}).$$

A única outra possibilidade é que $\alpha_1 = \beta_1$ e $\alpha_2 = \beta_2$, mas neste caso os dois monômios são iguais.

Podemos enunciar isto de maneira formal observando que o que fizemos consistiu em definir uma *ordem total* no conjunto dos monômios nas variáveis x_1 e x_2. Uma tal ordem permite comparar quaisquer dois monômios dados e decidir—se forem diferentes—qual deles é o maior. Denotando esta ordem por $>$, podemos defini-la dizendo que

$$x_1^{\alpha_1}x_2^{\alpha_2} > x_1^{\beta_1}x_2^{\beta_2} \text{ se } \begin{cases} \alpha_1 > \beta_1 \\ \quad \text{ou} \\ \alpha_1 = \beta_1 \text{ e } \alpha_2 > \beta_2 \end{cases}$$

Observe que se interpretarmos os monômios em x_1 e x_2 como palavras em um dicionário, então eles estarão ordenados de acordo com a regra acima, desde que a letra x_1 preceda x_2. Por isso dizemos que esta é a *ordem lexicográfica* do conjunto dos monômios em x_1 e x_2. Neste ponto talvez você queira reler a página 61 e comparar a ordenação lexicográfica de n-uplas lá definida com a ordenação de monômios que acabamos de introduzir. Veja exercício ???.

O estudo que fizemos da ordenação dos termos (ou melhor, dos monômios) de um polinômio em duas variáveis suscita várias questões. As mais óbvias são as seguintes:

(1) De que forma a ordenação lexicográfica se estende a polinômios em mais de duas variáveis?
(2) Existem outras maneiras de ordenar polinômios em várias indeterminadas, além da ordem lexicográfica?

Na próxima seção vamos formalizar, sistematizar e generalizar tudo o que vimos aqui, e com isto responder completamente a estas duas perguntas.

2. Generalizando

Como estabelecemos na página 70, estamos denotando o conjunto (infinito) de todos os monômios nas variáveis $x_1, \ldots, x_n$ por $\mathbb{T}^n$. Um elemento típico de $\mathbb{T}^n$ é da forma x^α para algum multi-índice $\alpha \in \mathbb{N}^n$. Como $(0, \ldots, 0)$ é um elemento de $\mathbb{N}^n$, então $1 \in \mathbb{T}^n$.

Nesta notação, o que queremos fazer, em primeiro lugar, é determinar quais as propriedades que uma ordem $>$ no conjunto $\mathbb{T}^n$ deve satisfazer. Tomando por base nossa experiência da seção anterior, parece conveniente exigir que:

Propriedade 1: a ordem seja total;

Propriedade 2: $x^\alpha > 1$ sempre que o multi-índice α for diferente de zero.

A propriedade 1 significa que $>$ é uma relação transitiva no conjunto $\mathbb{T}^n$ tal que se μ e ν são dois monômios distintos em $\mathbb{T}^n$ então $\mu > \nu$ ou $\nu > \mu$, mas não ambos. Já a propriedade 2 não havia aparecido antes, mas estava subliminarmente presente: ela significa que o termo constante deve ser sempre o menor termo do polinômio.

Exigiremos que todas as ordens construídas nesta seção satisfaçam estas propriedades. Como teremos várias ordens diferentes em $\mathbb{T}^n$ ao longo deste livro, não podemos usar o símbolo $>$ indiscriminadamente para todas elas. Em vez de inventar um símbolo diferente para cada uma, vamos adicionar a $>$ um subscrito que indica qual a ordem com a qual estamos trabalhando. Este subscrito será sempre uma abreviação padrão da ordem. Por exemplo, no caso da ordem lexicográfica escreveremos $>_{\text{lex}}$. Como seria de esperar, a longa palavra 'lexicográfica' vai ser rapidamente encolhida para simplesmente 'lex'.

Devemos começar mostrando que a ordem lexicográfica se estende a monômios em qualquer número de variáveis. Usando a notação de multi-índices, podemos descrever a ordem lexicográfica em duas variáveis de maneira muito sucinta dizendo que $x^\alpha >_{\text{lex}} x^\beta$ ocorre se, e somente se, a primeira entrada de $\alpha - \beta$ é positiva ou, a primeira entrada de $\alpha - \beta$ é nula e a segunda é positiva. Esta definição pode ser facilmente adaptada ao caso de mais de duas variáveis: dizemos que $x^\alpha >_{\text{lex}} x^\beta$ na *ordem lexicográfica* de $\mathbb{T}^n$ se

$$\text{o coeficiente não-nulo mais à esquerda de } \alpha - \beta \text{ é positivo.}$$

Isto corresponde a aplicar à construção recursiva de $K[x_1, \ldots, x_n]$ o procedimento da seção anterior. Note que, ao considerar a entrada não-nula *mais à esquerda* do multi-índice, estamos indiretamente assumindo que

$$x_1 >_{\text{lex}} x_2 >_{\text{lex}} \cdots >_{\text{lex}} x_n.$$

Os matemáticos frequentemente avançam modificando conceitos já conhecidos de modo a ampliar seu campo de aplicabilidade. Ao construir a ordem lexicográfica procedemos desta maneira. Afinal, ela resultou da aplicação recursiva da ordenação usual de polinômios de uma variável pelo grau dos termos. Mas não é incomum que um mesmo conceito possa ser generalizado de várias maneiras diferentes. Assim, vamos buscar uma outra maneira de ordenar polinômios em várias indeterminadas que também seja uma generalização do que ocorre em uma variável.

Em primeiro lugar, lembre-se que o grau de um monômio x^α é o número $|\alpha| = \alpha_1 + \cdots + \alpha_n$. Já vimos que ao tentar ordenar os monômios em mais de uma variável pelo grau nos deparamos com uma ordem que não é total. Uma saída para torná-la total é, quando confrontados com dois monômios de um mesmo grau, decidir que o maior é aquele que tem precedência na ordem lexicográfica. Esta é a ordem *lexicográfica graduada* em $\mathbb{T}^n$, que será abreviada

como glex. Temos que

$$x^\alpha >_{\text{glex}} x^\beta \text{ se } \begin{cases} |\alpha| > |\beta| \\ \quad \text{ou} \\ |\alpha| = |\beta| \text{ e } x^\alpha >_{\text{lex}} x^\beta. \end{cases}$$

Isto produz uma ordem híbrida que é muito útil nas aplicações. Observe que lex e glex podem se comportar de maneira muito diferente quando confrontadas com o mesmo monômio. Por exemplo,

$$x_1^6 x_2 >_{\text{lex}} x_1^4 x_2^5 \text{ contudo } x_1^6 x_2 <_{\text{glex}} x_1^4 x_2^5.$$

Se você achou glex estranha, a próxima ordem vai lhe parecer uma verdadeira quimera. Com o nome de *ordem reversa lexicográfica graduada* (abreviação grlex) ela é definida da seguinte maneira

$$x^\alpha >_{\text{grlex}} x^\beta \text{ se } \begin{cases} |\alpha| > |\beta| \\ \quad \text{ou} \\ |\alpha| = |\beta| \text{ e o coeficiente não-nulo mais à direita} \\ \text{de } \alpha - \beta \text{ é } \textit{negativo}. \end{cases}$$

Mais uma vez surge uma lateralidade na definição da ordem. Note que, como nos casos anteriores esta construção implica que

$$x_1 >_{\text{grlex}} x_2 >_{\text{grlex}} \cdots >_{\text{grlex}} x_n.$$

Vejamos um exemplo. Temos que,

$$x_1^6 x_2^4 x_3^7 >_{\text{grlex}} x_1^7 x_2^2 x_3^8,$$

pois estes dois monômios têm o mesmo grau, mas a entrada não nula mais à direita de

$$(6, 4, 7) - (7, 2, 8) = (-1, 2, -1)$$

é -1, que é negativa. Note que esta ordem não coincide com glex, afinal

$$x_1^6 x_2^4 x_3^7 <_{\text{glex}} x_1^7 x_2^2 x_3^8,$$

pois a primeira entrada não nula à esquerda de

$$(7, 2, 8) - (6, 4, 7) = (1, -2, 1)$$

é positiva. Não é à toa que este exemplo usa polinômios em 3 variáveis: glex e grlex coincidem para polinômios em duas variáveis; veja exercício ???.

É claro que poderíamos ter alcançado grlex em duas etapas, construindo primeiro uma ordem que está para grlex como a ordem lexicográfica está para glex. Conhecida (obviamente!) como *ordem lexicográfica reversa*, e abreviada por rlex, esta ordem é definida por

> $x^\alpha >_{\text{rlex}} x^\beta$ se o coeficiente não-nulo mais à direita de $\alpha - \beta$ é negativo.

Assim,

$$x_1^6x_2^1x_3^7 >_{\text{rlex}} x_1^8x_2^2x_3^7, \text{ ao passo que } x_1^6x_2^1x_3^7 <_{\text{lex}} x_1^8x_2^2x_3^7.$$

É fácil constatar que rlex é uma ordem total em $\mathbb{T}^n$, entretanto $x^\alpha <_{\text{rlex}} 1$, sempre que $\alpha \neq 0$. Por isso, rlex não é uma ordem adequada para o que estamos fazendo. A importância da propriedade 2 e deste exemplo só ficarão completamente claras na seção 4.

Até aqui vimos tratando os polinômios apenas como um conjunto. Entretanto, não podemos esquecer que o que temos é, de fato, um anel. Além do mais, quase todos os problemas que propusemos no capítulo 2 estão relacionados à possibilidade de somar e multiplicar polinômios. Por isso, é necessário, antes de continuar, entender de que forma as ordens em $\mathbb{T}^n$ propostas aqui se comportam em relação às operações de soma e multiplicação de polinômios.

3. Ordens monomiais

Nossa investigação da interação entre ordens de $\mathbb{T}^n$ e operações com polinômios começa, como seria de esperar, com uma análise do caso em que $n = 1$. Neste caso, a ordenação fica completamente determinada pelo grau dos monômios. Com isso, as fórmulas básicas que relacionam as operações com polinômios com a ordenação dos monômios são geralmente expressas como propriedades do grau: dados $f, g \in K[x]$, temos que

$$\text{grau}(f+g) \leq \max\{\text{grau}(f), \text{grau}(g)\} \text{ e} \tag{35}$$

$$\text{grau}(fg) = \text{grau}(f)\text{grau}(g), \tag{36}$$

como vimos na seção 3 do capítulo 2. No caso dos polinômios em várias indeterminadas a situação é mais complicada porque, em vez de um número (como o grau), precisamos trabalhar com os termos que lideram os polinômios. Para isso devemos estabelecer uma nomenclatura apropriada.

Suponhamos que $>$ seja uma ordem de $\mathbb{T}^n$ que satisfaz as propriedades 1 e 2. O *termo inicial* de f com respeito a $>$ é o termo de f cujo suporte é o maior monômio de $\sup(f)$ (com respeito à ordem $>$ dada). Usaremos a notação $\text{in}_>(f)$ para o termo inicial mas, sempre que possível, substituiremos $>$ pela abreviação da ordem, ou a omitiremos completamente se o contexto tornar clara qual a ordem que estamos usando. Por exemplo, se f for o polinômio da equação (33), temos que

$$\text{in}_{\text{lex}}(f) = 5x_1^3x_2^2.$$

Começaremos discutindo o comportamente do termo inicial com relação à soma de polinômios. Suponhamos que $f, g \in K[x_1, \ldots, x_n]$. Como ordenar os termos de um polinômio equivale a ordenar os seus suportes, e como

$$\sup(f+g) \subseteq \sup(f) \cup \sup(g),$$

temos, então, que

$$\text{in}(f+g) \leq \max\{\text{in}(f), \text{in}(g)\}, \tag{37}$$

qualquer que seja a ordem total escolhida para $\mathbb{T}^n$. Note que esta é claramente uma generalização da fórmula (35) para o grau da soma de polinômios.

A discussão referente ao produto é bem mais delicada. Suponhamos que $>$ é uma ordem em $\mathbb{T}^n$, que satisfaz às propriedades 1 e 2, e que $f, g \in K[x_1, \ldots, x_n]$. Admitiremos, como é usual, que f e g estão escritos como somas de termos cujos suportes estão ordenados em ordem decrescente, da esquerda para à direita. Neste caso, a maneira mais fácil de calcular o produto fg é utilizar a propriedade distributiva da multiplicação de polinômios. Se tentamos ordenar os monômios do produto fg à medida que são calculados, nos deparamos, de imediato, com a necessidade de ordenar os monômios resultantes do produto de um termo de f por cada um dos termos de g.

Removendo tudo o que é circunstancial, o cerne da questão se reduz a perguntar se a seguinte propriedade é válida:

Propriedade 3: se $\mu > \mu'$ e ν são monômios de $\mathbb{T}^n$ então $\mu\nu > \mu'\nu$.

Note que nossa experiência com números inteiros positivos sugere imediatamente $\mu\nu > \mu'\nu$, e não $\mu\nu < \mu'\nu$ como sendo a desigualdade correta.

Podemos testar um exemplo para descobrir se isto é razoável. Consideremos $\mathbb{T}^n$ com a ordem lexicográfica. Sejam

$$\mu = x^\alpha, \mu' = x^{\alpha'} \text{ e } \nu = x^\beta.$$

Como estamos supondo que $\mu > \mu'$ e a ordem escolhida foi a lexicográfica, devemos ter que a entrada não nula, mais à esquerda, de $\alpha - \alpha'$ é positiva. Contudo,

$$\mu\nu = x^{\alpha+\beta} \text{ e } \mu'\nu = x^{\alpha'+\beta}.$$

ao passo que,

$$(\alpha + \beta) - (\alpha' + \beta) = \alpha - \alpha',$$

donde concluímos que $\mu\nu > \mu'\nu$. Portanto a propriedade 3 é válida para a ordem lexicográfica.

Um argumento semelhante, mas que deixaremos como exercício, mostra que o mesmo vale para glex e grlex; veja exercício ???. Isto nos leva a perguntar: será que uma ordem que satisfaz as propriedades 1 e 2 também satisfaz 3? A resposta, infelizmente, é não, mas como o exemplo é um pouco artificial, vamos deixá-lo para o exercício 4. Diante disto precisamos nos perguntar se queremos exigir que todas as ordens que vamos considerar satisfaçam a propriedade 3. Para ver que a resposta é sim, vamos continuar nossa análise da interação entre multiplicação e ordem, só que, de agora em diante, suporemos que a ordem $>$ que estamos adotando em $\mathbb{T}^n$ satisfaz as propriedades 1, 2 e 3.

A propriedade 3 nos permite comparar o produto de dois monômios distintos por um mesmo monômio. Resta-nos considerar a situação em que temos quatro monômios, $\mu > \mu'$ e $\nu > \nu'$, e precisamos escolher o maior entre $\mu\nu$ e $\mu'\nu'$. Entretanto, segue da propriedade 3 que

$$\mu'\nu' > \mu'\nu \text{ e que } \mu'\nu > \mu\nu.$$

Combinando as duas desigualdades, concluímos que $\mu'\nu' > \mu\nu$. Isto nos permite ordenar todos os monômios resultantes do produto dos termos de f pelos de g, e o que descobrimos é que o maior termo de fg é igual ao produto do maior termo de f pelo maior termo de g. Em outras palavras,

$$\text{in}(fg) = \text{in}(f)\text{in}(g). \tag{38}$$

Por exemplo, se

$$g = 6x_1^6x_2^4 + 8x_1^3x_2^7 + x_1^2x_2^8 + x_1x_2^6 + 1$$

e f é o polinômio definido na equação (33), então

$$\text{in}(fg) = \text{in}(f)\text{in}(g) = (5x_2^2x_1^3)(6x_1^6x_2^4) = 30x_1^9x_2^6,$$

com relação à ordem lexicográfica. Note que (38) é uma transcrição bastante satisfatória da fórmula do grau do produto para o caso de várias indeterminadas. Portanto, não resta dúvida que desejamos que todas as ordens que vamos considerar satisfaçam também a propriedade 3. Isto nos leva a definição chave desta seção. Uma ordem total de $\mathbb{T}^n$ é *monomial* quando

- $x^\alpha > 1$ sempre que $\alpha \neq 0$ e
- se $\mu > \mu'$ e ν são monômios de $\mathbb{T}^n$ então $\mu\nu > \mu'\nu$.

Há muitas outras ordens monomiais em $\mathbb{T}^n$ além de lex, glex e grlex; você encontrará algumas delas definidas nos exercícios ??? e ???. Várias dessas ordens serão utilizadas em aplicações que faremos posteriormente.

4. Divisão

Estamos prontos para considerar o segundo problema proposto na seção 5 do capítulo 3; isto é, como dividir polinômios de mais de uma variável? Começaremos recordando com cuidado o procedimento utilizado no caso de uma variável.

Suponhamos que temos dois polinômios

$$f = a_nx^n + \cdots + a_1x + a_0 \text{ e } g = b_mx^m + \cdots + b_1x + b_0,$$

em $K[x]$, com a_n e b_m não nulos. Desejamos dividir f por g de modo a obter um quociente q e um resto r. Lembre-se que f, g, q e r estão relacionados por

$$f = gq + r \text{ em que } r = 0 \text{ ou } r \text{ tem grau menor que o de } g. \tag{39}$$

Nesta divisão, f é o dividendo e g o divisor.

Começaremos por reformular o algoritmo de divisão de polinômios em uma variável usando a nomenclatura da seção anterior. A etapa crucial do algoritmo é a terceira. Nela cancelamos o termo líder de f usando um múltiplo de g. Mais precisamente, calculamos

$$f - \frac{a_n}{b_m}x^{n-m}g.$$

Entretanto, como

$$\text{in}(f) = a_nx^n \text{ e } \text{in}(g) = b_mx^m.$$

temos que $\mathrm{in}(f)/\mathrm{in}(g) = a_n x^{n-m}/b_m$. Denotando por $>$ a ordenação usual dos monômios em uma variável, podemos enunciar o algoritmo de divisão da seguinte maneira.

ALGORITMO 4.1 (Algoritmo de divisão em uma variável). *Dados polinômios f e g em $K[x]$, de graus n e m, respectivamente, o algoritmo tem como saída polinômios q e r tais que $f = gq + r$ e $r = 0$ ou $r < g$.*

Etapa 1: *Inicializa $F = f$ e $Q = 0$.*

Etapa 2: *Enquanto F tem grau maior ou igual que o grau de g, faça*

$$Q = Q + \frac{\mathrm{in}(f)}{\mathrm{in}(g)};$$

$$F = F - \frac{\mathrm{in}(f)}{\mathrm{in}(g)} g.$$

Etapa 2: *Imprima*

O RESTO É F E O QUOCIENTE É Q.

Uma vez que o algoritmo tenha sido formulado desta maneira, é difícil não se perguntar o que nos impede de aplicá-lo, como está, ao caso de mais de uma variável. Para isto bastaria escolher uma ordem monomial e interpretar a notação como se referindo a esta ordem. Para entender onde está o problema a melhor coisa a fazer é tentar um exemplo. Sejam $f = x_1$ e $g = x_2$. Assumindo a ordem lexicográfica, com $x_1 > x_2$, para $K[x_1, x_2]$ temos que $\mathrm{in}(f) > \mathrm{in}(g)$. Mas para dividir f por g usando o algoritmo anterior teremos que calcular

$$\frac{\mathrm{in}(f)}{\mathrm{in}(g)} = \frac{x_1}{x_2},$$

que não é um polinômio. Ou seja, quando o anel de polinômios tem mais de uma variável pode acontecer que um monômio maior não seja divisível por um monômio menor. Isto significa que será necessário alterar o algoritmo para poder aplicá-lo a mais de uma variável.

Antes de tomar uma decisão sobre o que devemos fazer, precisamos relembrar para que queremos este algoritmo de divisão. Nosso objetivo é achar um método sistemático que nos permita decidir se um dado polinômio f pode ser escrito como combinação (com coeficientes polinomiais) de polinômios $g_1, \ldots, g_s$ dados; veja página92. Como é claro que x_2 não divide x_1, então podemos tomar x_1 como sendo o resto da divisão entre $f = x_1$ e $g = x_2$, sem com isso comprometer nosso objetivo último. Isto sugere que, em geral, se o monômio $\mathrm{in}(g)$ não divide $\mathrm{in}(f)$, então devemos somá-lo ao resto, removê-lo do dividendo e continuar a divisão.

Por exemplo, digamos que queremos dividir

$$f = 6x_1^6 x_2^4 + 7x_1^5 + 8x_1^4 x_2^7 + 1$$

por

$$g = x_1^4 x_2^2 + 1$$

em $\mathbb{Q}[x_1, x_2]$ com a ordenação lexicográfica. Como

$$\frac{\text{in}(f)}{\text{in}(g)} = \frac{6x_1^6x_2^4}{x_1^4x_2^2} = 6x_1^2x_2^2$$

então podemos executar este passo do algoritmo exatamente como no caso de uma variável. Assim, ao final do primeiro passo temos que

$$\begin{aligned} Q &= 6x_1^2x_2^2 \\ F &= f - (6x_1^2x_2^2)g = 7x_1^5 + 8x_1^4x_2^7 - 6x_1^2x_2^2 + 1 \\ R &= 0. \end{aligned}$$

Observe que agora precisamos de três variáveis F, Q e R, para fazer o algoritmo funcionar. Em cada passo, F controla os termos do dividendo, Q os do quociente e R os do resto. No segundo passo, aplicaremos o mesmo procedimento a

$$F = 7x_1^5 + 8x_1^4x_2^7 - 6x_1^2x_2^2 + 1 \quad \text{e} \quad g = x_1^4x_2^2 + 1.$$

Só que desta vez $\text{in}(g) = x_1^4x_2^2$ não divide $\text{in}(f) = 7x_1^5$. Portanto, ao final da segunda passagem do algoritmo devemos ter

$$\begin{aligned} Q &= 6x_1^2x_2^2 \\ F &= F - 7x_1^5 = 8x_1^4x_2^7 - 6x_1^2x_2^2 + 1 \\ R &= 7x_1^5. \end{aligned}$$

Note que, desta vez, apenas removemos o termo inicial de F e o somamos ao resto. Ainda há alguns passos a executar antes do algoritmo parar. Ao invés de executá-los um a um como acima, vamos resumir toda a divisão em uma tabela seguindo o costume do caso em que os polinômios têm uma variável. Entretanto, ao contrário da tabela usual, nesta o resto aparece listado abaixo do quociente, como você pode ver na tabela 1.

$6x_1^6x_2^4 + 7x_1^5 + 8x_1^4x_2^7 + 1$	$x_1^4x_2^2 + 1$
$7x_1^5 + 8x_1^4x_2^7 - 6x_1^2x_2^2 + 1$	$Q = 6x_1^2x_2^2 + 8x_2^5$
$8x_1^4x_2^7 - 6x_1^2x_2^2 + 1$	$R = 7x_1^5 - 6x_1^2x_2^2 - 8x_2^5 + 1$
$-6x_1^2x_2^2 - 8x_2^5 + 1$	
$-8x_2^5 + 1$	
1	
0	

TABELA 1

No comentário que precede este exemplo relembramos que nossa meta consiste em verificar se f se escreve como combinação linear de polinômios $g_1, \ldots g_s$ dados. Pensando bem, o que obtivemos até agora (que não é pouco)

não atinge completamente nosso objetivo. O problema é que só conseguimos saber se um polinômio divide um outro; isto é, ainda não temos nenhum instrumento para saber se um polinômio é "divisível" por vários outros polinômios simultaneamente. Nisto o caso de uma variável não é de nenhuma ajuda, porque todo ideal de $K[x]$ é gerado por apenas um elemento, de modo que este problema nunca se põe neste caso. Como já sabemos que isto é falso em $K[x_1, \ldots, x_n]$, de modo que não há como escapar de um impasse.

A saída mais óbvia é efetuar a divisão um polinômio de cada vez. Digamos que estamos tentando dividir f por $g_1, \ldots, g_s$ em $K[x_1, \ldots, x_n]$, sob alguma ordem monomial $>$. Verificamos primeiro se $\mathrm{in}(g_1)$ divide $\mathrm{in}(f)$. Se dividir, sabemos como proceder; se não dividir, testamos se $\mathrm{in}(g_2)$ divide $\mathrm{in}(f)$. Mais uma vez, se dividir sabemos o que fazer; senão, passamos a g_3. Se $\mathrm{in}(f)$ não for divisível por nenhum $\mathrm{in}(g_1), \ldots, \mathrm{in}(g_s)$, não há outro remédio senão somá-lo ao resto. Se isto funcionar, nada poderia ser mais simples. Para eliminar qualquer dúvida formularemos o algoritmo que resulta desta estratégia com mais precisão.

ALGORITMO 4.2 (Algoritmo de divisão em mais de uma variável). *Dados polinômios f e $g_1, \ldots, g_s$ de $K[x_1, \ldots, x_n]$, ordenados sob uma ordem monomial $>$, o algoritmo tem como saída polinômios $q_1, \ldots, q_s$ e r tais que*

$$f = q_1 g_1 + \cdots + q_s g_s + r$$

e

- $r = 0$, *ou*
- *nenhum monômio de r é divisível pelos termos iniciais*

$$\mathrm{in}(g_1), \ldots, \mathrm{in}(g_s).$$

Etapa 1: *inicializa $F = f$, $Q_1 = \cdots = Q_s = 0$ e $R = 0$.*

Etapa 2: *Enquanto $F \neq 0$, verifique se existe algum inteiro i entre 1 e s para o qual $\mathrm{in}(g_i)$ divide $\mathrm{in}(f)$. Se existir escolha j como sendo o menor deles e faça*

$$Q_j = Q_j + \frac{\mathrm{in}(F)}{\mathrm{in}(g_j)};$$
$$F = F - \frac{\mathrm{in}(F)}{\mathrm{in}(g_j)} g_j;$$
$$R = R.$$

deixando as demais variáveis inalteradas; se tal i não existir, faça

$$F = F - \mathrm{in}(f);$$
$$R = R + \mathrm{in}(f).$$

deixando as demais variáveis inalteradas.

Etapa 3: *Imprima*

O RESTO É R E OS QUOCIENTES SÃO $Q_1, \ldots, Q_s$.

Vejamos como o algoritmo funciona quando tentamos dividir

$$f = 6x_1^6x_2^4 + 7x_1^5 + 8x_1^4x_2^7 + 1$$

por

$$g_1 = x_1^4x_2^2 + 1 \text{ e } g_2 = 2x_2^5 - x_2$$

sob a ordem lexicográfica. Como a tabela usual da divisão esconde muitos dos detalhes do funcionamente do algoritmo, vamos representar a divisão enumerando cada passo separadamente.

Primeiro passo: Neste passo apenas inicializamos as variáveis.

$F = f = 6x_1^6x_2^4 + 7x_1^5 + 8x_1^4x_2^7 + 1;$
$R = 0;$
$Q_1 = 0;$
$Q_2 = 0.$

Segundo passo: Como $\text{in}(g_1) = x_1^4x_2^2$ divide $\text{in}(F) = 6x_1^6x_2^4$, aplicamos a primeira parte da Etapa 2 com $j = 1$, obtendo:

$F = f - \frac{\text{in}(f)}{\text{in}(g_1)}g_1 = 7x_1^5 + 8x_1^4x_2^7 - 6x_1^2x_2^2 + 1;$
$R = 0;$
$Q_1 = \text{in}(f)/\text{in}(g_1) = 6x_1^2x_2^2;$
$Q_2 = 0.$

Terceiro passo: Como nem $\text{in}(g_1) = x_1^4x_2^2$, nem $\text{in}(g_2) = 2x_2^5$ dividem $\text{in}(F) = 7x_1^5$, aplicamos a segunda parte da Etapa 2, obtendo:

$F = F - \text{in}(F) = 8x_1^4x_2^7 - 6x_1^2x_2^2 + 1;$
$R = \text{in}(F) = 7x_1^5;$
$Q_1 = 6x_1^2x_2^2;$
$Q_2 = 0.$

Quarto passo: Como $\text{in}(g_1) = x_1^4x_2^2$ divide $\text{in}(F) = 8x_1^4x_2^7$, a primeira parte da Etapa 2 com $j = 1$, obtendo:

$F = F - \frac{\text{in}(F)}{\text{in}(g_1)}g_1 = -6x_1^2x_2^2 - 8x_2^5 + 1;$
$R = \text{in}(F) = 7x_1^5;$
$Q_1 = 6x_1^2x_2^2 + 8x_2^5;$
$Q_2 = 0.$

Quinto passo: Como nem $\text{in}(g_1) = x_1^4x_2^2$, nem $\text{in}(g_2) = 2x_2^5$ dividem o termo inicial $\text{in}(F) = -6x_1^2x_2^2$, aplicamos a segunda parte da Etapa 2, obtendo:

$F = F - \text{in}(F) = -8x_2^5 + 1;$
$R = R + \text{in}(F) = 7x_1^5 - 6x_1^2x_2^2;$
$Q_1 = 6x_1^2x_2^2;$
$Q_2 = 0.$

Sexto passo: Como $\text{in}(g_2) = 2x_2^5$ divide $\text{in}(F) = -8x_2^5$, aplicamos a primeira parte da Etapa 2 com $j = 2$, obtendo:

$F = F - \frac{\text{in}(F)}{\text{in}(g_2)}g_2 = 4x_2 + 1;$

$R = 7x_1^5 - 6x_1^2x_2^2;$
$Q_1 = 6x_1^2x_2^2 + 8x_2^5;$
$Q_2 = -4.$

Sétimo passo: Como nem $\mathrm{in}(g_1) = x_1^4x_2^2$, nem $\mathrm{in}(g_2) = 2x_2^5$ dividem $\mathrm{in}(F) = -4x_2$, aplicamos a segunda parte da Etapa 2, obtendo:

$F = F - \mathrm{in}(F) = 1;$
$R = R + \mathrm{in}(F) = 7x_1^5 - 6x_1^2x_2^2 - 4x_2;$
$Q_1 = 6x_1^2x_2^2 + 8x_2^5;$
$Q_2 = -4.$

Oitavo passo: Como nem $\mathrm{in}(g_1) = x_1^4x_2^2$, nem $\mathrm{in}(g_2) = 2x_2^5$ dividem $\mathrm{in}(F) = 1$, aplicamos a segunda parte da Etapa 2, obtendo:

$F = F - \mathrm{in}(F) = 0;$
$R = R + \mathrm{in}(F) = 7x_1^5 - 6x_1^2x_2^2 - 4x_2 + 1;$
$Q_1 = 6x_1^2x_2^2 + 8x_2^5;$
$Q_2 = -4.$

No próximo passo o algoritmo para. Resumimos tudo isto na tabela de divisão 2.

$6x_1^6x_2^4 + 7x_1^5 + 8x_1^4x_2^7 + 1$	$x_1^4x_2^2 + 1$
	$2x_2^5 - x_2$
$7x_1^5 + 8x_1^4x_2^7 - 6x_1^2x_2^2 + 1$	$Q_1 = 6x_1^2x_2^2 + 8x_2^5$
$8x_1^4x_2^7 - 6x_1^2x_2^2 + 1$	$Q_2 = -4$
$-6x_1^2x_2^2 - 8x_2^5 + 1$	$R = 7x_1^5 - 6x_1^2x_2^2 - 4x_2 + 1$
$-8x_2^5 + 1$	
$-4x_2 + 1$	
1	
0	

TABELA 2

Ainda precisamos provar que o algoritmo funciona, e estabelecer algumas de suas propriedades básicas, mas deixaremos isto para a próxima seção.

5. Análise do algoritmo de divisão

Começamos provando que o algoritmo funciona. Faremos isto em duas partes: mostraremos primeiramente que o algoritmo para, e depois que, de fato, calcula aquilo que foi explicitado como sendo sua saída. Para facilitar a discussão chamaremos de F^i, Q_j^i e R^i os valores das variáveis F, Q_j, e R, respectivamente, ao final do i-ésimo passo. Naturalmente estamos supondo que a entrada do algoritmo é formada por polinômios f e $g_1, \ldots, g_s$ do anel $K[x_1, \ldots, x_n]$ e por uma ordem monomial $>$.

Ao aplicar o algoritmo, temos que considerar, em cada passo, se está sendo aplicada a primeira ou segunda parte da Etapa 2; a primeira etapa serve apenas para inicializar as variáveis, ao passo que a terceira só é utilizada para retornar o resultado. Digamos que, no i-ésimo passo, esteja sendo aplicada a primeira parte da Etapa 2. Neste caso algum $\mathrm{in}(g_j)$ divide $\mathrm{in}(F_{i-1})$ e temos que

$$\begin{aligned} Q_j^i &= Q_j + \frac{\mathrm{in}(F^{i-1})}{\mathrm{in}(g_j)}; \\ F^i &= F^{i-1} - \frac{\mathrm{in}(F^{i-1})}{\mathrm{in}(g_j)} g_j; \\ R^i &= R^{i-1}. \end{aligned}$$

Como

$$\mathrm{in}(F^{i-1}) = \mathrm{in}\left(\frac{(\mathrm{in}(F^{i-1})}{\mathrm{in}(g_j))} g_j\right),$$

concluímos que $\mathrm{in}(F^{i-1}) > \mathrm{in}(F^i)$ e que $F^i - F^{i-1} \in \langle g_1, \ldots, g_s \rangle$.

Vejamos o que aconteceria se estivéssemos aplicando a segunda parte da Etapa 2, em vez da primeira, no i-ésimo passo. Neste caso, teríamos

$$\begin{aligned} F^i &= F^{i-1} - \mathrm{in}(F^i); \\ R^i &= R^{i-1} + \mathrm{in}(F^i). \end{aligned}$$

Mais uma vez, é claro que $\mathrm{in}(F^{i-1}) > \mathrm{in}(F^i)$. Contudo, desta vez, quem pertence a $\langle g_1, \ldots, g_s \rangle$ é $F^i - F^{i-1} + \mathrm{in}(F^i)$.

Desta análise segue que

$$\mathrm{in}(F^1) > \mathrm{in}(F^2) > \cdots > \mathrm{in}(F^i) > \mathrm{in}(F^{i-1});$$

é uma sequência estritamente decrescente de monômios na ordem monomial $>$. Se uma tal sequência não puder descrescer indefinidamente, então o algoritmo tem que parar. Uma ordem em relação à qual não existem sequências decrescentes infinitas em $\mathbb{T}^n$ é chamada de *boa ordem*. Será que toda ordem monomial de $\mathbb{T}^n$ é uma boa ordem?

Qualquer ordem que dependa do grau, como glex e grlex, é evidentemente uma boa ordem. A razão é que, em uma ordem deste tipo, se $|\alpha| > |\beta|$ então $x^\alpha > x^\beta$. Porém, dado um inteiro positivo k, o número de monômios de grau menor ou igual a k é finito. Logo, pelo menos neste caso, todas as sequências decrescentes de monômios são finitas. Entretanto, este argumento não funciona para a ordem lexicográfica, porque se $x_1 >_{\mathrm{lex}} x_2$, então qualquer potência de x_2 é menor que x_1. É possível provar diretamente que lex é uma boa ordem por indução no número de variáveis; veja exercício 5. Ao invés de fazer isto, passaremos ao resultado geral.

PROPOSIÇÃO 4.3. *Toda ordem monomial é uma boa ordem.*

DEMONSTRAÇÃO. Suponha, por contradição, que $>$ é uma ordem monomial de $\mathbb{T}^n$ que não é uma boa ordem. Então existe uma cadeia decrescente infinita de monômios em $\mathbb{T}^n$. Seja S o conjunto dos monômios que constituem

esta cadeia, e seja I o ideal de $K[x_1, \ldots, x_n]$ gerado pelos monômios de S. Pelo corolário 3.6, existe um subconjunto finito G de monômios de S que geram I. Como os elementos de S formam uma sequência decrescente, e como G é finito, existe um monômio $\mu \in S$ tal que todo monômio de G é maior que μ. Contudo, $\mu \in I$, de modo que deve existir $\nu \in G$ tal que $\mu = \sigma\nu$, para algum $\sigma \in \mathbb{T}^n$ que é diferente de 1. Isto implica que

$$\nu > \mu = \sigma\nu.$$

Entretanto, $>$ é uma ordem monomial, de modo que $\sigma > 1$ e, portanto, $\nu\sigma > \nu$; que é a contradição desejada. □

Você deve ter observado que uma propriedade das ordens monomiais que foi crucial na demonstração desta proposição foi o fato de que $\sigma \neq 1$ implica que $\sigma > 1$; isto é, se $\alpha \neq 0$ então $x^\alpha > 1$. Seria de esperar que uma ordem para a qual esta propriedade não vale não seja uma boa ordem; e este é, realmente, o caso. Um exemplo simples é rlex, sob a qual

$$x_1 >_{\text{rlex}} x_1^2 >_{\text{rlex}} x_1^3 >_{\text{rlex}} x_1^4 >_{\text{rlex}} \cdots$$

é uma sequência infinita descrescente de monômios. Isto mostra que nem toda ordem em $\mathbb{T}^n$ é uma boa ordem.

Segundo a proposição 4.3, não importa qual a ordem monomial utilizada na divisão de polinômios, podemos estar seguros de que o algoritmo que descrevemos sempre vai parar.

Tendo mostrado que o algoritmo sempre para, passamos a verificar que calcula o que especificamos na sua saída. Da análise precedente do que acontece em um passo, vemos que

$$F^i - F^{i-1} + \rho_i \in \langle g_1, \ldots, g_s \rangle,$$

onde

- $\rho_i = 0$, se neste passo executamos a primeira parte da Etapa 2, ou
- ρ_i não é divisível por nenhum $\text{in}(g_j)$, se neste passo executamos a segunda parte da Etapa 2.

Suponhamos que o algoritmo execute k passos. Somando todas estas equações, com i variando de 2 a k, e escrevendo $r = \rho_1 + \cdots + \rho_k$, concluímos que

$$F_k - F_1 + r = (F^2 - F^1 + \rho_1) + (F^3 - F^2 + \rho_2) + \cdots + (F^k - F^{k-1} + \rho_k)$$

pertence a $\langle g_1, \ldots, g_s \rangle$. Levando em conta que $F_1 = f$ e que $F_k = 0$, pois estamos supondo que o algoritmo para no k-ésimo passo, concluímos que $-f + r \in \langle g_1, \ldots, g_s \rangle$. Além disso, r é uma soma de monômios, nenhum dos quais pertence a $\langle \text{in}(g_1), \ldots, \text{in}(g_s) \rangle$, que é exatamente a prescrição da saída do algoritmo.

Há, ainda, uma propriedade da divisão que, apesar de não ter sido enunciada anteriormente, será de grande utilidade nas demonstrações que faremos

usando o algoritmo. Como, na saída do algoritmo, $f = q_1g_1 + \cdots + q_sg_s + r$, então

$$\text{in}(f) \leq \max\{\text{in}(q_1g_1), \ldots, \text{in}(q_sg_s), \text{in}(r)\}. \tag{40}$$

Isto não é novidade; é apenas consequência da aplicação repetida de (37). A propriedade que queremos provar diz que, neste caso, temos de fato uma igualdade. Mais uma vez basta utilizar a análise que já fizemos do comportamento passo a passo do algoritmo. Temos que

$$F^{i-1} = F^i + \nu_i,$$

onde ν_i é um monômio de algum q_jg_j ou de r, dependendo da etapa que foi aplicada neste passo. Em qualquer dos dois casos,

$$\text{in}(F^{i-1}) = \text{in}(\nu_i), \tag{41}$$

pois $\text{in}(F^{i-1}) > \text{in}(F^i)$. Mas esta última desigualdade, associada a (41), implica que

$$\text{in}(f) = \text{in}(F_1) = \text{in}(\nu_1),$$

que será o termo inicial de $q_1g_1 + \cdots + q_sg_s$ ou de r. De qualquer forma, isto implica que vale a igualdade em (40), que é o que queríamos mostrar.

Reuniremos tudo o que provamos em um teorema para referência futura.

TEOREMA 4.4. *Sejam $f, g_1, \ldots, g_s$ polinômios e $>$ uma ordem monomial do anel $K[x_1, \ldots, x_n]$. Então existem polinômios $q_1, \ldots, q_s$ tais que*

$$f = q_1g_1 + \cdots + q_sg_s + r,$$

onde

- *nenhum monômio de r pertence ao ideal $\langle \text{in}(g_1), \ldots, \text{in}(g_s)\rangle$, e*
- $\text{in}(f) = \max\{\text{in}(q_1g_1), \ldots, \text{in}(q_sg_s), \text{in}(r)\}$.

Escrevendo $G = \{g_1, \ldots, g_s\}$ para o conjunto dos divisores, denotaremos o polinômio r definido no teorema acima (o resto!) por $\text{R}_G(f)$. Diremos que um polinômio f é *reduzido* com relação a G se $\text{R}_G(f) = f$.

6. Comentários e complementos

Convém relembrar que, conforme a agenda estabelecida na seção 5 do capítulo 3, nosso objetivo ao definir um algoritmo de divisão para polinômios em várias indeterminadas era o de resolver o *problema da pertinência*, formulado na página 92. A aplicação deste problema aos métodos analíticos descritos no capítulo 1 é bastante clara. Por exemplo, na demonstração de que as medianas de um triângulo se encontram em um único ponto precisamos, verificar que o polinômio

$$f = 2xv - 2yu - v + y,$$

pertence ao ideal gerado por $g_1 = xv - uy + y - 2v$ e $g_2 = xv - yu + v$. Para isso podemos efetuar a divisão de f por $\{g_1, g_2\}$ e tomar o resto, que *deve* ser zero; afinal, já sabemos que $f \in \langle g_1, g_2\rangle$.

$$\begin{array}{r|l} 2xv - 2yu - v + y & xv - uy + y - 2v \\ & xv - yu + v \\ \hline 3v - y & Q_1 = 2 \\ & Q_2 = 0 \end{array}$$

Em princípio podemos efetuar este cálculo usando qualquer ordem monomial. Escolheremos glex com $x > y > u > v$. Calculando a divisão, temos

E, surpreendentemente, o resto não deu zero! Se você está achando que nada podia ser pior, está enganado. Digamos que efetuamos a divisão de novo, mas desta vez trocamos a ordem dos divisores: dividimos com g_1 antes de g_2.

$$\begin{array}{r|l} 2xv - 2yu - v + y & xv - yu + v \\ & xv - uy + y - 2v \\ \hline -x + u - 2v & Q_1 = 2 \\ & Q_2 = 0 \end{array}$$

Não só o resto deu diferente de zero de novo, mas deu diferente do anterior! Isto é realmente muito ruim, porque muitos resultados importantes referentes a polinômios em uma variável são provados usando a unicidade do resto.

Antes de prosseguir, vale a pena deixar claro o que queremos dizer ao afirmar que o resto não é único na divisão de polinômios em mais de uma variável. Digamos que temos um polinômio $f \in K[x_1, \ldots, x_n]$ e um conjunto de divisores $G = \{g_1, \ldots, g_s\}$. Não importa quantas vezes aplicarmos o algoritmo de divisão a f com respeito a $g_1, \ldots, g_s$ (nesta ordem!), obteremos sempre o mesmo resto. Isto ocorre porque o algoritmo é determinístico; quer dizer, as decisões que o algoritmo toma em cada etapa são *completamente determinadas* pela entrada. Neste sentido não é possível obter dois restos diferentes.

Entretanto, não é isto que entendemos quando falamos da unicidade do resto no caso de uma variável. Imagine que damos polinômios $f, g \in K[x]$ a duas pessoas diferentes, e que pedimos que calculem um polinômio r tal que exista $q \in K[x]$ com

$$f = qg + r \text{ e } r = 0 \text{ ou } r \text{ tem grau menor que } g.$$

Note que não estamos indicando nenhuma maneira pela qual estas pessoas devam calcular estes polinômios. Digamos que o resultado dos cálculos destas pessoas sejam os polinômios r_1 e r_2. Dizer que o resto é único significa que *sempre teremos* $r_1 = r_2$, não importando como o cálculo do resto foi feito.

O ponto crucial, naturalmente, é que estamos prescrevendo condições de natureza algébrica que o resto deve satisfazer; não estamos dizendo nada sobre como deveria ser calculado. Neste sentido, como mostra o exemplo acima, o resto da divisão de polinômios em mais de uma variável não é único. Dizendo

de outra maneira, as condições do teorema 4.4 não são suficientes para determinar o polinômio r de maneira única.

E agora? Todo este esforço foi em vão? Na verdade, o que acontece no caso dos polinômios terem mais de uma variável é que o resto só é único para certos conjuntos especiais de geradores dos ideais. Estes conjuntos, chamados de bases de Gröbner, serão o tema do próximo capítulo. Lá veremos que apesar dos polinômios g_1 e g_2 gerarem um ideal I, eles não formam uma base de Gröbner deste ideal. É precisamente aí que está o problema.

De nossa agenda original de trabalho, estabelecida na seção 5 do capítulo 3, solucionamos completamente os ítens 1 e 2, a saber:

Ítem 1: Representar polinômios em mais de uma variável no computador.

Ítem 2: Dividir polinômios em mais de uma variável de modo a obter quociente e resto.

Mesmo assim não conseguimos resolver de maneira satisfatória o *problema da pertinência*. Contudo, diante do que já aprendemos podemos reformular o que precisamos fazer de uma forma mais precisa como:

> determinar um conjunto de geradores para um ideal dado de modo que um polinômio pertença ao ideal se, e somente se, deixa resto zero na divisão por estes geradores.

A esta altura talvez você esteja pronto a protestar que nossa dicussão da representação de polinômios na seção 1 foi um mero pretexto para introduzir ordens monomiais—e você estará certo. Portanto, não é inteiramente verdade que resolvemos o ponto 1 da agenda original. Por isso encerraremos o capítulo com uma discussão um pouco mais detalhada de como os polinômios em várias variáveis são representados no computador.

Da discussão da seção 1 obtivemos uma representação em que cada polinômio corresponde a um vetor de números. Cada número, por sua vez, representa o coeficiente de um termo do polinômio. Finalmente, para evitar ambiguidade, pressupusemos sempre que os termos foram ordenados de acordo com alguma ordem monomial pré-determinada. Esta maneira de representar polinômios é conhecida como *cheia*.

Por exemplo, digamos que vamos trabalhar no anel $\mathbb{Q}[x, y]$ com a ordem glex, em que $x > y$. Sob estas hipóteses, o polinômio $xy^2 + 6y^2 + 8$ seria representado pelo vetor

$$(1, 0, 0, 0, 6, 0, 0, 8).$$

Cada entrada no vetor corresponde, da esquerda para a direita, aos coeficientes dos monômios menores que xy^2 sob glex, que são

$$xy^2 > y^3 > x^2 > xy > y^2 > x > y > 1.$$

Observe que, mesmo em um exemplo tão pequeno, a maior parte das entradas do vetor é zero. Isto é típico dos polinômios em mais de uma variável: um polinômio completo de um dado grau tem muitos coeficients, mas quase sempre os polinômios com os quais trabalhamos estão muito longe de

serem completos. Isto significa que, ao representar polinômios dessa forma, a maior parte da memória ocupada pelo vetor guarda zeros. Seria muito bom se pudéssemos evitar este desperdício. Fazemos isto com a chamada *representação esparsa*. Neste caso, cada entrada do vetor que representa o polinômio guarda o coeficiente e o monômio que o acompanha (ou melhor, os expoentes de cada variável). Assim, $x_1x_2^2 + 6x_2^2 + 8$ corresponde ao vetor

$$((1,(1,2)),(6,(0,2)),(8,(0,0)),$$

onde $(a,(i,j))$ representa o termo $ax_1^ix_2^j$.

Para dar um exemplo da economia que isto representa, considere o que acontece quando o polinômio é $x_1^{12}x_2$. Em representação cheia, teríamos um vetor com 92 entradas, ao passo que a representação esparsa é apenas $(1,(12,1))$. Para uma discussão mais detalhada deste problema consulte [**20**, p. 62].

7. Exercícios

1. Sejam $\alpha, \beta \in \mathbb{N}^k$ multi-índices. Mostre que $x^\alpha <_{\text{lex}} x^\beta$ se, e somente se, $\alpha < \beta$ segundo a ordenação lexigográfica definida à página 61.

2. Mostre que as ordens lexicográfica graduada e reversa lexicográfica graduada coincidem para polinômios em duas variáveis.

3. Prove que a única ordem monomial em $K[x]$ é a ordenação usual dos monômios pelos seus graus.

4. Calcule os quocientes e restos das seguintes divisões nas ordens prescritas (em cada caso $x < y$):
   (1) $x^2y + xy^2 + y^2$ por $y^2 - 1$ e $xy - 1$ em lex;
   (2) $x^7y^2 + x^3y^2 - y + 1$ por $xy^2 - x$ e $x - y^3$ em grlex.

5. Seja d um inteiro positivo. Calcule o resto da divisão de $x_1^dx_2^{d-1} - x_1$ por $x_2 - x_1^d$ sob a ordem lexicográfica com $x_2 > x_1$ e mostre que é igual a $x_1^{d^2} - x_1$.

6. Mostre, diretamente da definição, que as ordens lexicográfica graduada e reversa lexicográfica graduada são ordens monomiais.

7. Considere a ordem em $\mathbb{T}^1$ definida da seguinte maneira:

$$x^r > x^s \text{ se } \begin{cases} r \text{ e } s \text{ são ímpares e } r > s \\ r \text{ e } s \text{ são pares e } r > s \\ r \text{ é ímpar e } s \text{ é par} \end{cases}$$

   (1) Mostre que esta é uma ordem total que satisfaz $x^k > 1$ para todo $k > 0$.
   (2) Mostre que esta ordem não satisfaz a condição
   se $\mu > \mu'$ e ν são monômios de $\mathbb{T}^1$ então $\mu\nu > \mu'\nu$.

8. Mostre, diretamente da definição, que a ordem lexicográfica de $\mathbb{T}^n$ é uma boa ordem.

9. Seja K um corpo e $x_1, \ldots, x_n$ e $y_1, \ldots, y_m$ variáveis. Suponhamos que $<_x$ e $<_y$ são ordens monomiais nos anéis $K[x_1, \ldots, x_n]$ e $K[y_1, \ldots, y_m]$, respectivamente. Defina uma ordem no conjunto dos monômios nas variáveis $x_1, \ldots, x_n, y_1, \ldots, y_m$, da seguinte maneira:
   se μ_1, μ_2 são monômios nos xs e ν_1, ν_2 são monômios nos ys, então
   $$\mu_1\nu_1 < \mu_2\nu_2 \text{ se, e somente se, } \begin{cases} \mu_1 <_x \mu_2 \\ \quad \text{ou} \\ \mu_1 = \mu_2 \text{ e } \nu_1 <_y \nu_2. \end{cases}$$
   Prove que esta é uma ordem monomial. Trata-se de uma ordem muito importante em aplicações, conhecida como *ordem de eliminação*.

10. Seja u um vetor com n entradas, cujas coordenadas são inteiros positivos. Dados dois monômios x^α e x^β nas variáveis $x_1, \ldots, x_n$, defina uma ordem em $\mathbb{T}^n$ por
    $$x^\alpha < x^\beta \text{ se, e somente se, } \begin{cases} u \cdot \alpha < u \cdot \beta \\ \quad \text{ou} \\ u \cdot \alpha = u \cdot \beta \text{ e } x^\alpha <_{\text{lex}} x^\beta, \end{cases}$$
    onde $u \cdot \alpha$ denota o produto escalar de u e α considerados como vetores de $\mathbb{N}^n$. Mostre que esta é uma ordem monomial de $\mathbb{T}^n$.

11. Prove que, qualquer que seja a ordem monomial adotada, a divisão de um binômio por outro em qualquer anel de polinômios sempre tem por resto um binômio.

12. Sejam f e g polinômios e G um subconjunto de $K[x_1, \ldots, x_n]$. Mostre que:
    (a) se $f \in G$ então $\mathrm{R}_G(fg) = 0$;
    (b) se $\mu \in \mathbb{T}^n$ e $\mathrm{R}_G(f) = g$ então $\mathrm{R}_G(\mu f) = \mathrm{R}_G(\mu g)$.

13. Explique porque é impossível representar um polinômio na forma cheia usando a ordem lexicográfica.

14. Se $\mu = x^\alpha \in \mathbb{T}^n$ defina seu *multigrau* por $\mathrm{multigrau}(\mu) = \alpha \in \mathbb{N}^n$. Sejam $\mu_1, \mu_2 \in \mathbb{T}^n$.
    (a) Prove que
    $$\mathrm{multigrau}(\mu_1\mu_2) = \mathrm{multigrau}(\mu_1) + \mathrm{multigrau}(\mu_2).$$
    (b) Discuta sob que condições
    $$\mathrm{multigrau}(\mu_1 + \mu_2) = \max\{\mathrm{multigrau}(\mu_1), \mathrm{multigrau}(\mu_2)\}.$$

15. Se $f \in K[x_1, \ldots, x_n]$ e defina seu *multigrau* relativamente a uma ordem monomial fixada $>$ por
$$\text{multigrau}(f) = \text{multigrau}(\text{in}_>(f)) \in \mathbb{N}^n.$$
Sejam $f, g \in K[x_1, \ldots, x_n]$.
(a) Prove que
$$\text{multigrau}(fg) = \text{multigrau}(f) + \text{multigrau}(g).$$
(b) Discuta sob que condições
$$\text{multigrau}(f+g) = \max\{\text{multigrau}(f), \text{multigrau}(g)\}.$$

16. Um polinômio $f \in K[x_1, \ldots, x_n]$ é *simétrico* se não é alterado quando permutamos as variáveis de qualquer maneira que quisermos. Mostre que os polinômios
$$x_1 + x_2 + x_3,\ x_1x_2 + x_1x_3 + x_2x_3 \text{ e } x_1x_2x_3$$
são simétricos, mas que
$$x_1 + 2x_2 + 5x_3,\ x_1x_3 + x_2x_3 \text{ e } x_1x_2^2x_3$$
não são.

17. Mostre que o conjunto de todos os polinômios simétricos em $x_1, \ldots, x_n$, com coeficientes em K, é um subanel de $K[x_1, \ldots, x_n]$.

18. O polinômio $\sigma_k \in K[x_1, \ldots, x_n]$ é definido por
$$\sigma_k = \sum x_{j(1)} \cdots x_{j(k)},$$
em que a soma é tomada sobre todas as escolhas possíveis de índices
$$1 \leq j(1) < \cdots < j(k) \leq n.$$
Os polinômios σ_1, σ_2 e σ_3 de $K[x_1, x_2, x_3]$ são listados no exercício anterior. Prove que σ_k é um polinômio simétrico quaisquer que sejam os inteiros positivos k e n.

19. Seja $f \in K[x_1, \ldots, x_n]$ um polinômio qualquer. Prove que $f(\sigma_1, \ldots, \sigma_n)$ é um polinômio simétrico.

20. Seja $f \in K[x_1, \ldots, x_n]$ um polinômio simétrico e seja cx^α seu termo inicial relativamente à ordem lexicográfica com $x_1 > \cdots > x_n$, em que $c \in K$. Mostre que as coordenadas de α satisfazem
$$\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n.$$

21. Seja α um multi-índice cujas coordenadas satisfazem
$$\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n$$
e defina
$$g_\alpha = \sigma_1^{\alpha_1 - \alpha_2} \sigma_2^{\alpha_2 - \alpha_3} \cdots \sigma_{n-1}^{\alpha_{n-1} - \alpha_n} \sigma_n^{\alpha_n}$$

(a) Mostre que g_α é um polinômio simétrico.
(b) Calcule o termo inicial de relativamente à ordem lexicográfica com $x_1 > \cdots > x_n$.

22. Seja $f \in K[x_1, \ldots, x_n]$ um polinômio simétrico com $\mathrm{in}(f) = cx^\alpha$ relativamente à ordem lexicográfica com $x_1 > \cdots > x_n$.
(a) Mostre que $\mathrm{in}(f - cg_\alpha) < \mathrm{in}(f)$ em que g_α é o polinômio definido no exercício acima.
(b) Mostre que $f - cg_\alpha$ é um polinômio simétrico.
(c) Use (a), (b) e o fato de que toda ordem monomial é uma boa ordem para provar o seguinte teorema devido a I. Newton:

> todo polinômio simétrico em $K[x_1, \ldots, x_n]$ pode ser escrito na forma $h(\sigma_1, \ldots, \sigma_n)$, para algum polinômio h em $K[x_1, \ldots, x_n]$.

23. Mostre como converter o argumento do exercício anterior em um algoritmo que, tendo como entrada um polinômio simétrico $f \in K[x_1, \ldots, x_n]$, tem por saída um polinômio $h \in K[x_1, \ldots, x_n]$ tal que $f = h(\sigma_1, \ldots, \sigma_n)$.

24. Use o algoritmo do exercício anterior para determinar o polinômio h correspondente aos seguintes polinômios simétricos de $\mathbb{Q}[x_1, x_2]$:
(a) $x_1^2 + x_1x_2 + x_2^2$;
(b) $x_1^4 + x_2^4$;
(c) $x_1x_2^2 + x_2x_1^2$.

CAPíTULO 5

Bases de Gröbner

Neste capítulo resolveremos completamente o *problema da pertinência* formulado na página 92. Faremos isto implementando a estratégia proposta na seção 6 do capítulo 4. Mais precisamente, descreveremos um algoritmo que nos permitirá determinar um conjunto de geradores para um ideal dado de modo que um polinômio pertença ao ideal se, e somente se, deixa resto zero na divisão por estes geradores. Ao longo de todo o capítulo K denota um corpo.

1. Bases de Gröbner

Vimos, no capítulo 4, que o algoritmo de divisão não pode ser usado para verificar se $f \in K[x_1, \ldots, x_n]$ pertence ao ideal gerado por um dado conjunto de polinômios $G = \{g_1, \ldots, g_s\}$. Isto se dá porque não basta que f seja combinação linear dos gs para que possamos garantir que deixará resto zero na divisão por G. Nesta seção resolvemos este impasse definindo um tipo especial de conjunto de geradores. Ao longo de toda esta seção suporemos fixada uma ordem monomial $>$ em $K[x_1, \ldots, x_n]$.

Seja I um ideal e $>$ uma ordem monomial de $K[x_1, \ldots, x_n]$. O *ideal inicial* $\mathrm{in}(I)$ de I é o ideal de $K[x_1, \ldots, x_n]$ gerado por $\mathrm{in}(f)$ para cada $f \in I$. Segundo esta definição $\mathrm{in}(I)$ é gerado pelo conjunto formado pelos monômios iniciais de cada um dos elementos de I. Mas este conjunto é infinito, o que parece tornar o cálculo explícito de $\mathrm{in}(I)$ praticamente inviável. Contudo, depois de pensar um pouco sobre a definição talvez você venha a concluir que estamos sendo desnecessariamente pessimistas. A saída parece estar na observação de que se os polinômios $g_1, \ldots, g_s$ geram I, então $\mathrm{in}(g_1), \ldots, \mathrm{in}(g_s)$ deveriam gerar $\mathrm{in}(I)$. Infelizmente, isto não é verdade, como mostra o seguinte exemplo. Considere o ideal I de $K[x_1, x_2]$ gerado por $g_1 = x_1^2$ e $g_2 = x_1x_2 + x_2^2$. Então,

$$\mathrm{in}_{\mathrm{lex}}(g_1) = x_1^2 \text{ e } \mathrm{in}_{\mathrm{lex}}(g_2) = x_1x_2, \text{ em que } x_1 > x_2.$$

Temos que,

$$f = x_2g_1 - x_1g_2 = -x_1x_2^2 \in I, \tag{42}$$

que não oferece nenhum problema porque $\mathrm{in}_{\mathrm{lex}}(f) = x_1x_2^2$ é divisível por $\mathrm{in}_{\mathrm{lex}}(g_2)$. Mas isto implica que

$$h = x_1x_2^2 - x_2g_2 = x_2^3 \in I. \tag{43}$$

Portanto,

$$x_2^3 = \mathrm{in}_{\mathrm{lex}}(h) \in \mathrm{in}_{\mathrm{lex}}(I).$$

Contudo, x_2^3 não pertence ao ideal gerado por $\mathrm{in}_{\mathrm{lex}}(g_1)$ e $\mathrm{in}_{\mathrm{lex}}(g_2)$.

Naturalmente, quando os termos iniciais dos geradores de I são geradores de $\mathrm{in}(I)$, temos uma situação muito satisfatória. A importância deste caso é tal que somos levados a estabelecê-lo sob a forma de uma definição, possivelmente a mais fundamental deste livro. Um subconjunto finito $G \subset I$ é uma *base de Gröbner* para I se $\mathrm{in}(I)$ for gerado por $\mathrm{in}(g)$ para cada $g \in G$. Neste caso, como G é finito por hipótese, estamos supondo que conhecemos um conjunto de geradores para $\mathrm{in}(I)$.

Se você leu a definição com muito cuidado deve ter percebido que não exigimos que G fosse um conjunto de geradores para I. Entretanto, se J é o ideal gerado pelos elementos de G, podemos concluir da definição de base de Gröbner que $J \subseteq I$ e que $\mathrm{in}(I) = \mathrm{in}(J)$. A próxima proposição implica que, sob estas circuntâncias, $I = J$, de modo que os elementos de G geram I. Na demonstração desta proposição usamos o fato de que toda ordem monomial é uma boa ordem.

PROPOSIÇÃO 5.1. *Sejam $J \subseteq I$ ideais de $K[x_1, \ldots, x_n]$. Se $\mathrm{in}(I) = \mathrm{in}(J)$, então $I = J$.*

DEMONSTRAÇÃO. Suponha, por contradição, que $J \neq I$. Como $>$ é uma boa ordem, então o conjunto $I \setminus J$ tem um elemento f cujo termo inicial é mínimo com respeito a $>$. Porém, como os ideais iniciais de I e J coincidem, temos que $\mathrm{in}(f) \in \mathrm{in}(J)$. Portanto, existe $g \in J$ tal que $\mathrm{in}(g) = \mathrm{in}(f)$. Mas isto implica que $\mathrm{in}(f) > \mathrm{in}(f - g)$. Portanto, pela minimalidade de f temos que $f - g \in J$. Como $g \in J$, isto implica que $f = (f - g) + g \in J$, que contradiz a hipótese feita sobre J e completa a demonstração. □

De agora em diante usaremos livremente o fato de que uma base de Gröbner de I gera I. Uma consequência importante desta proposição é o *teorema da base de Hilbert*, que já havíamos enunciado, e até aplicado, no capítulo 3.

TEOREMA DA BASE DE HILBERT. *Seja K um corpo. Todo ideal de $K[x_1, \ldots, x_n]$ admite um número finito de geradores.*

DEMONSTRAÇÃO. Seja I um ideal e $<$ uma ordem monomial do anel de polinômios $K[x_1, \ldots, x_n]$. Pelo teorema 3.5 da página 78 existe um conjunto finito de monômios $\{\mu_1, \ldots, \mu_s\}$ que gera $\mathrm{in}(I)$. Seja g_j um elemento de I cujo termo líder é μ_j, e considere o ideal J de $K[x_1, \ldots, x_n]$ gerado por $g_1, \ldots, g_s$. Então, $J \subseteq I$ e $\mathrm{in}(J) = \mathrm{in}(I)$. Portanto, pela proposição 5.1 temos que $J = I$. Em particular, I é gerado pelos elementos $g_1, \ldots, g_s$, e o teorema está provado. □

Antes mesmo de definir bases de Gröbner já tínhamos verificado que se $g_1 = x_1^2$ e $g_2 = x_1x_2 + x_2^2$ então $\{g_1, g_2\}$ *não* é uma base de Gröbner para o ideal $I = \langle g_1, g_2 \rangle$ sob a ordem lexicográfica. Resta-nos dar um exemplo de um conjunto de geradores que é uma base de Gröbner. Um dos exemplos não

triviais mais simples é o conjunto $G = \{g_1, g_2, h\}$, com $h = x_2^3$, conforme nossos cálculos anteriormente. Desta vez G é uma base de Gröbner para o ideal $I = \langle g_1, g_2 \rangle$ sob a ordem lexicográfica, como passamos a mostrar.

O que temos de provar é que $\mathrm{in}(g_1)$, $\mathrm{in}(g_2)$ e $\mathrm{in}(h)$ geram $\mathrm{in}(I)$. Para isso precisamos ser capazes de determinar os termos iniciais de todos os elementos de I. À primeira vista esta é uma tarefa sem esperança, já que I é infinito. Neste ponto a ordem lexicográfica vem em nosso socorro. Dado um polinômio qualquer $f \in K[x_1, x_2]$, podemos escrevê-lo na forma

$$f = x_1^2 f_1(x_1, x_2) + x_1 f_2(x_2) + f_3(x_2),$$

em que f_1 é um polinômio qualquer de $K[x_1, x_2]$, mas f_2 e f_3 são polinômios apenas na variável x_2. Como estamos operando sob a ordem lexicográfica com $x_1 >_{\mathrm{lex}} x_2$, temos que, se $f_1 \neq 0$, então

$$\mathrm{in}_{\mathrm{lex}}(f) = \mathrm{in}_{\mathrm{lex}}(x_1^2 f_1) = x_1^2 \mathrm{in}_{\mathrm{lex}}(f_1) \in \mathrm{in}_{\mathrm{lex}}(I).$$

Concluímos que todos os polinômios de I para os quais $f_1 \neq 0$ têm seu termo inicial em $\mathrm{in}_{\mathrm{lex}}(I)$. Como estes polinômios também pertencem a

$$\langle \mathrm{in}_{\mathrm{lex}}(g_1), \mathrm{in}_{\mathrm{lex}}(g_2), \mathrm{in}_{\mathrm{lex}}(h) \rangle = \langle x_1^2, x_1 x_2, x_2^3 \rangle,$$

podemos supor que estamos lidando com um elemento $f \in I$ para o qual $f_1 = 0$.

Supondo, desta vez, que $f_1 = 0$ mas que $f_2 \neq 0$, temos que

$$\mathrm{in}_{\mathrm{lex}}(f) = \mathrm{in}_{\mathrm{lex}}(x_1 f_2) = x_1 \mathrm{in}_{\mathrm{lex}}(f_2).$$

Aqui há duas possibilidades. Se f_2 não se reduzir ao termo constante, então $\mathrm{in}_{\mathrm{lex}}(f_2)$ é divisível por x_2. Mas, disto resulta que $\mathrm{in}_{\mathrm{lex}}(f)$ é divisível por $x_1 x_2 = \mathrm{in}(g_2)$. Caso f_2 se reduza ao termo constante, podemos escrever $f = ax_1 + f_3(x_2)$, em que a é uma constante não nula. Como estamos supondo que $f \in I$, devem existir $q_1, q_2 \in K[x_1, x_2]$ tais que

$$f = q_1 g_1 + q_2 g_2. \tag{44}$$

Fazendo $x_1 = 0$ na equação (44), obtemos

$$f(0, x_2) = f_3(x_2) = q_2(0, x_2) x_2^2$$

Logo $f = ax_1 + x_2^2 q_2(0, x_2)$. Porém, tomando agora $x_2 = 0$ em (44), temos que

$$f(x_1, 0) = ax_1 = q_1(x_1, 0) g_1(x_1, 0) = q_1(x_1, 0) x_1^2,$$

o que é uma contradição, pois $a \neq 0$. Logo não pode haver um polinômio em I para o qual $f_1 = 0$ e f_2 é uma constante não nula.

Falta apenas analisar o caso em que $f_1 = f_2 = 0$. Neste caso $f = f_3(x_2)$ é um polinômio apenas na variável x_2. Se f_3 for divisível por x_2^3, então $\mathrm{in}_{\mathrm{lex}}(f)$ também será divisível por $x_2^3 = \mathrm{in}_{\mathrm{lex}}(h)$. Portanto, podemos supor que $f_3 = ax_2^2 + bx_2 + c$, em que a, b e c são constantes. Como $f \in I$, podemos escrevê-lo na forma da equação (44). Contudo, fazendo $x_1 = 0$ nesta equação obtemos

$$f(0, x_2) = ax_2^2 + bx_2 + c = q_2(0, x_2) x_2^2.$$

Em particular, $b = c = 0$ e $f = ax_2^2$. Como $a \neq 0$, segue que

$$g_2 - \frac{1}{a} f = x_1 x_2.$$

Mas isto implica que

$$\langle x_1^2, x_1 x_2, x_2^2 \rangle \subseteq \langle x_1^2, x_1 x_2 + x_2^2 \rangle = I$$

Como o segundo ideal está contido no primeiro, temos uma igualdade. Entretanto, pela proposição 3.3 do capítulo 2, o ideal $\langle x_1^2, x_1 x_2, x_2^2 \rangle$ não pode ser gerado por apenas dois elementos , o que mostra que este caso não pode ocorrer e conclui nossa verificação de que $G = \{g_1, g_2, h\}$ é uma base de Gröbner para I.

A dificuldade de verificar, mesmo em um exemplo tão simples como este, que um dado conjunto de geradores é uma base de Gröbner põe em evidência a necessidade de obter um bom algoritmo para calcular estas bases. Antes, porém, precisamos mostrar que há alguma recompensa para todo este trabalho. Faremos isto enumerando algumas das propriedades mais importantes das bases de Gröbner.

2. Propriedades da base de Gröbner

Começamos mostrando que a divisão com respeito a uma base de Gröbner produz a tão cobiçada solução do problema da pertinência a um ideal. Lembre-se que se G é um subconjunto e f um elemento de $K[x_1, \ldots, x_n]$, então $\mathrm{R}_G(f)$ denota o resto da divisão de f por G.

PROPOSIÇÃO 5.2. *Seja I um ideal de $K[x_1, \ldots, x_n]$ e G uma base de Gröbner para I. Então, $f \in I$ se e somente se $\mathrm{R}_G(f) = 0$.*

DEMONSTRAÇÃO. Como G gera I, é claro que, se o resto da divisão de f por G for zero, então $f \in I$. Vamos provar a recíproca. Suponhamos, por contradição, que $f \in I$, mas que $\mathrm{R}_G(f) = r \neq 0$. Neste caso, como $f - r \in I$, temos que $r \in I$. Portanto, $\mathrm{in}(r) \in \mathrm{in}(I)$. Logo, pela definição de bases de Gröbner, $\mathrm{in}(r)$ é divisível por $\mathrm{in}(g)$ para algum $g \in G$. Mas isto contradiz o fato de que o resto, segundo o teorema 4.4 do capítulo 3, é sempre reduzido. Concluímos que $r = 0$, o que prova a proposição. □

Diremos que um subconjunto qualquer G de $K[x_1, \ldots, x_n]$ é uma *base de Gröbner* se G é uma base de Gröbner do ideal gerado por G. Uma consequência da proposição anterior é a unicidade do resto da divisão com respeito a uma base de Gröbner.

COROLÁRIO 5.3. *Seja $G = \{g_1, \ldots, g_s\}$ uma base de Gröbner e f um polinômio de $K[x_1, \ldots, x_n]$. Então existe um único polinômio r tal que*

$$f = q_1 g_1 + \cdots + q_s g_s + r,$$

em que $q_1, \ldots, q_s \in K[x_1, \ldots, x_n]$ e nenhum monômio de r pertence ao ideal gerado pelos termos iniciais dos gs.

DEMONSTRAÇÃO. Suponha, por contradição, que também podemos escrever f na forma

$$f = q'_1 g_1 + \cdots + q'_s g_s + r',$$

em que, como no enunciado do corolário, $q'_1, \ldots, q'_s \in K[x_1, \ldots, x_n]$ e nenhum monômio de r' pertence ao ideal gerado pelos termos iniciais dos gs. Subtraindo as expressões para f, obtemos

$$(q_1 g_1 + \cdots + q_s g_s + r) - (q'_1 g_1 + \cdots + q'_s g_s + r') = 0;$$

assim,

$$(q_1 - q'_1) g_1 + \cdots + (q_s - q'_s) g_s + (r - r') = 0,$$

donde concluímos que $r - r' \in \langle g_1, \ldots, g_s \rangle$. Logo, pela proposição 5.2, o resto da divisão de $r - r'$ por G tem que ser zero. Contudo, por hipótese, nenhum monômio de r ou r' é divisível pelo termo inicial de algum g. Mas isto implica que o resto de $r - r'$ por G é o próprio $r - r'$. Portanto, $r - r' = 0$, como queríamos mostrar. □

3. O algoritmo de Buchberger

Na seção 1 vimos que os polinômios $g_1 = x_1^2$ e $g_2 = x_1 x_2 + x_2^2$ não formam uma base de Gröbner em $K[x_1, x_2]$. O problema é que podemos obter polinômios no ideal $\langle g_1, g_2 \rangle$ cujo termo inicial é menor que os termos iniciais de g_1 e g_2. A maneira como obtivemos um tal monômio no exemplo acima foi através do "cancelamento dos termos iniciais" entre g_1 e g_2. O que queremos dizer com isso, é que devemos multiplicar g_1 por um monômio ν_1 e g_2 por um monômio ν_2, de modo que

$$\nu_1 \mathrm{in}(g_1) - \nu_2 \mathrm{in}(g_2) = 0.$$

Fazemos isto na esperança de que o polinômio $\nu_1 g_1 - \nu_2 g_2$ tenha um termo inicial que não seja divisível por $\mathrm{in}(g_1)$ nem por $\mathrm{in}(g_2)$ mas, infelizmente, isto nem sempre acontece. Voltando ao exemplo, o cancelamento dos termos iniciais entre g_1 e g_2 produziu o polinômio $f = x_1 x_2^2$. Contudo, este polinômio não oferece nenhuma dificuldade porque seu termo inicial (no caso o próprio f) é divisível por $\mathrm{in}(g_2)$. Por outro lado, não há porque parar ao primeiro percalço. Aplicando novamente este procedimento, desta vez a f e g_1, obtivemos o polinômio $h = x_2^3$, cujo termo inicial não é divisível por $\mathrm{in}(g_1)$ nem por $\mathrm{in}(g_2)$, exatamente como queríamos.

Observe que se continuássemos a fazer isto, não obteríamos nenhum novo polinômio cujo termo inicial já não fosse divisível por $\mathrm{in}(g_1)$, $\mathrm{in}(g_2)$ ou $\mathrm{in}(h)$. A razão é que, como mostramos na seção 1, o conjunto $G = \{g_1, g_2, h\}$ é uma base de Gröbner em $K[x_1, x_2]$.

Isto sugere que a estratégia de "cancelar termos iniciais" é uma boa maneira de descobrir polinômios que precisam ser acrescentados a um conjunto de geradores para formar uma base de Gröbner. Por isso passamos a analisar esta estratégia em mais detalhes. Para simplificar a notação, vamos nos referir a x^α como sendo o suporte do termo $c_\alpha x^\alpha$. Em outras palavras, identificaremos,

de agora em diante, o monômio x^α com o conjunto unitário $\{x^\alpha\}$, sempre que isto for conveniente.

Sejam g_1 e g_2 polinômios de $K[x_1, \ldots, x_n]$. A maneira mais fácil de "cancelar o termo inicial" entre g_1 e g_2 é tomar o polinômio

$$\mathrm{in}(g_2)g_1 - \mathrm{in}(g_1)g_2.$$

Contudo, esta não é a maneira mais econômica de proceder, porque $\mathrm{in}(g_1)$ e $\mathrm{in}(g_2)$ podem ter fatores comuns. Para evitar isto basta eliminar os fatores comuns, dividindo os termos iniciais pelo seu máximo divisor comum. Se x^α e x^β são os monômios que servem de suporte a $\mathrm{in}(g_1)$ e $\mathrm{in}(g_2)$, respectivamente, definimos o máximo divisor comum entre estes termos como sendo

$$\mathrm{mdc}(\mathrm{in}(g_1), \mathrm{in}(g_2)) = x^\gamma,$$

onde

$$\gamma_i = \min\{\alpha_i, \beta_i\},$$

para $i = 1, \ldots, n$. Como $\mathrm{in}(g_1)$ e $\mathrm{in}(g_2)$ são divisíveis por

$$\delta = \mathrm{mdc}(\mathrm{in}(g_1), \mathrm{in}(g_2)),$$

então

$$S(g_1, g_2) = \frac{\mathrm{in}(g_2)}{\delta} g_1 - \frac{\mathrm{in}(g_1)}{\delta} g_2$$

é um polinômio no qual também haverá cancelamento dos termos inicias. Dizemos que este é o *S-polinômio* de g_1 e g_2.

Por exemplo, se

$$g_1 = x_1^2 \quad \text{e} \quad g_2 = x_1x_2 + x_2^2,$$

então, sob a ordem lexicográfica com $x_1 > x_2$, temos $\mathrm{in}(g_1) = x_1^2$ e $\mathrm{in}(g_2) = x_1x_2$, de modo que

$$\delta = \mathrm{mdc}(x_1^2, x_1x_2) = x_1,$$

e, portanto, neste caso,

$$S(g_1, g_2) = \frac{x_1x_2}{x_1} g_1 - \frac{x_1^2}{x_1} g_2 = x_2g_1 - x_1g_2 = f,$$

exatamente como já havíamos feito, embora tateando, na equação (42). Quando calculamos este exemplo na seção 1, nosso passo seguinte foi verificar que $S(g_1, g_2)$ era divisível por $\mathrm{in}(g_2)$ e, portanto, podia ser descartado. Entretanto, podemos refinar este procedimento, considerando a relação entre $S(g_1, g_2)$ e os polinômios g_1 e g_2, ao invés de nos limitarmos aos termos iniciais como fizemos anteriormente. Para isto, dividimos $S(g_1, g_2)$ pelos polinômios g_1 e g_2, conforme ilustrado na tabela 1.

Portanto, o resto da divisão é o polinômio $-h$, que já havia sido calculado na equação (43). Obtivemos, assim, em apenas um passo, o novo candidato a gerador. Podemos, agora, repetir o mesmo procedimento com $G = \{g_1, g_2, h\}$,

$x_1x_2^2$	x_1^2
	$x_1x_2 + x_2^2$
$-x_2^3$	$Q_1 = 0$
	$Q_2 = x_2$
	$R = -x_2^3$.

TABELA 1. Divisão de $S(g_1, g_2)$ por g_1 e g_2.

calculando os S-polinômios e dividindo-os por G. Entretanto, se fizermos isto veremos que $S(g_1, h) = 0$ e que

$$S(g_2, h) = \frac{x_2^3}{x_2}g_2 - \frac{x_1x_2}{x_2}h = x_2^2(x_1x_2 + x_2^2) - x_1(x_2^3) = x_2^4,$$

que é divisível por G. Portanto, este procedimento acaba aqui. Isto sugere o seguinte algoritmo, originalmente proposto por Bruno Buchberger em sua tese de doutoramento [**6**].

ALGORITMO 5.4 (Algoritmo de Buchberger). *Seja $K[x_1, \ldots, x_n]$ um anel de polinômios munido de uma ordem monomial $>$. Dado um subconjunto finito $S \subset K[x_1, \ldots, x_n]$, o algoritmo tem como saída uma base de Gröbner do ideal gerado pelos polinômios de S no anel $K[x_1, \ldots, x_n]$.*

Etapa 1: *Inicializa $G = S$ e*

$$\mathcal{P} = \{(g, g') : g, g' \in G \text{ e } g \neq g'\}.$$

Etapa 2: *Enquanto $\mathcal{P} = \emptyset$, repita:*

- *escolha $(g, g') \in \mathcal{P}$:*
- *remova (g, g') de $\mathcal{P}$;*
- *calcule o resto r da divisão do S-polinômio $S(g, g')$ por G;*
- *se $r \neq 0$, então:*
  - *acrescente r a G;*
  - *acrescente a $\mathcal{P}$ os pares da forma (h, r) para cada $h \in G$;*

Etapa 3: *Páre e imprima os elementos de G.*

O que é realmente surpreendente é que um procedimento aparentemente tão ingênuo possa produzir uma base de Gröbner; o que provaremos na próxima seção. Observe que, como no caso do algoritmo de divisão, o de Buchberger sempre retorna polinômios com coeficientes que pertencem ao corpo de base dos polinômios dados como entrada. Antes de encerrar esta seção convém fazermos mais um exemplo da aplicação do algoritmo de Buchberger.

Retornando ao exemplo das medianas de um triângulo, lembre-se que tínhamos um ideal gerado pelos polinômios

$$h_1 = -yu + xv + y - 2v \text{ e } h_2 = -uy + xv + v,$$

no anel $\mathbb{C}[x, y, u, v]$. Desta vez vamos adotar a ordem grlex com $x > y > u > v$. Na verdade, já tomamos o cuidado de listar os monômios de h_1 e h_2 em ordem decrescente sob grlex. Aplicando o algoritmo de Buchberger, passo a passo, ao conjunto $\{h_1, h_2\}$, temos:

Primeiro passo: Neste passo apenas inicializamos as variáveis do algoritmo:

$$\mathcal{G} = \{h_1, h_2\},$$
$$\mathcal{P} = \{(h_1, h_2)\},$$

Segundo passo: Calculando o primeiro S-polinômio, temos

$$S(h_1, h_2) = h_1 - h_2 = y - 3v.$$

O termo inicial deste S-polinômio tem grau menor que os graus dos elementos de G, de modo que

$$\mathrm{R}_G(S(h_1, h_2)) = y - 3v.$$

Seja $h_3 = y - 3v$. Então, ao final deste passo teremos que

$$\mathcal{G} = \{h_1, h_2, h_3\},$$
$$\mathcal{P} = \{(h_1, h_3), (h_2, h_3)\},$$

Terceiro passo: Calculando o S-polinômio do par (h_1, h_3), obtemos

$$S(h_1, h_3) = 3h_1 - (-u)h_3 = -xv + 3uv - y + 2v$$

Dividindo $xv - 3uv + y - 2v$ por $G = \{h_1, h_2, h_3\}$, obtemos o resto $xv - 3uv + v$, como mostra a tabela 2.

$xv - 3uv + y - 2v$	$-yu + xv + y - 2v$
	$-uy + xv + v$
	$y - 2v$
$-3uv + y - 2v$	$Q_1 = 0$
$y - 2v$	$Q_2 = 0$
	$Q_3 = 1$
	$R = xv - 3uv$

TABELA 2. Cálculo do resto de $S(h_1, h_3)$

Escrevendo $h_4 = xv - 3uv + v$ temos, ao final deste passo:

$$\mathcal{G} = \{h_1, h_2, h_3, h_4\},$$
$$\mathcal{P} = \{(h_2, h_3), (h_1, h_4), (h_2, h_4), (h_3, h_4)\},$$

Quarto passo: Calculando o S-polinômio do par (h_2, h_3), obtemos

$$S(h_2, h_3) = 3h_1 - (-u)h_3 = -xv - v + 3uv = -h_4.$$

Portanto, este polinômio deixa resto zero na divisão por $G = \{h_1, h_2, h_3, h_4\}$. Ao final deste passo,

$$\mathcal{G} = \{h_1, h_2, h_3, h_4\},$$
$$\mathcal{P} = \{(h_1, h_4), (h_2, h_4), (h_3, h_4)\},$$

Quinto passo: Calculando o S-polinômio do par (h_1, h_4), obtemos

$$S(h_1, h_4) = xvh_1 - (-uy)h_4 = -x^2v^2 - xvy + 2xv^2 - uyv + 3u^2yv,$$

que deixa resto zero na divisão por G. Logo, ao final deste passo,

$$\mathcal{G} = \{h_1, h_2, h_3, h_4\},$$
$$\mathcal{P} = \{(h_2, h_4), (h_3, h_4)\},$$

Sexto passo: Calculando o S-polinômio do par (h_2, h_4), obtemos

$$S(h_2, h_4) = xvh_2 - (-uy)h_4 = -x^2v^2 - xv^2 - uyv + 3u^2yv,$$

que também deixa resto zero na divisão por G. Logo, ao final deste passo,

$$\mathcal{G} = \{h_1, h_2, h_3, h_4\},$$
$$\mathcal{P} = \{(h_3, h_4)\},$$

Sétimo passo: Calculando o S-polinômio do par (h_3, h_4), obtemos

$$S(h_3, h_4) = xvh_3 - yh_4 = -3xv^2 - vy + 3uyv,$$

que também deixa resto zero na divisão por G. Logo, ao final deste passo,

$$\mathcal{G} = \{h_1, h_2, h_3, h_4\},$$
$$\mathcal{P} = \emptyset,$$

Oitavo passo: Como $\mathcal{P} = \emptyset$ o algoritmo vai parar, tendo calculado a base de Gröbner

$$G = \{h_1, h_2, h_3, h_4\}.$$

4. Critério de Buchberger

Nesta seção provaremos que o algoritmo de Buchberger funciona. Há duas coisas a fazer: mostrar que o algoritmo para, e mostrar que tem sempre por saída uma base de Gröbner do ideal gerado pelo conjunto de polinômios especificado na entrada.

Começamos verificando que o algoritmo para. Seja $S \subset K[x_1, \ldots, x_n]$ o conjunto de polinômios dado como entrada ao algoritmo e seja I o ideal gerado por S. Ao final de cada passo, o algoritmo produz um novo conjunto de geradores de I. Digamos que $G_0 = S$ e que G_j é o conjunto de geradores resultante ao final do j-ésimo passo. Então,

$$G_{j+1} = G_j \cup \{r_{j+1}\},$$

onde r_{j+1} é o resto da divisão de algum S-polinômio por G_j relativamente à ordem monomial escolhida para a execução do algoritmo.

Em particular, os Gs formam uma sequência crescente

$$G_0 \subseteq G_1 \subseteq G_2 \subseteq \cdots$$

que, por sua vez, dá lugar a uma sequência crescente de ideais monomiais

$$\mathrm{in}(\langle G_0\rangle) \subseteq \mathrm{in}(\langle G_1\rangle) \subseteq \mathrm{in}(\langle G_2\rangle) \subseteq \cdots$$

Entretanto, pelo corolário 3.7 do capítulo 3, existe um inteiro $k > 0$ tal que

$$\mathrm{in}(\langle G_k\rangle) = \mathrm{in}(\langle G_t\rangle),$$

para todo $t \geq k$. Portanto,

$$\mathrm{in}(r_{t+1}) \in \mathrm{in}(\langle G_k\rangle), \tag{45}$$

para todo $t \geq k$, o que implica que $r_{t+1} = 0$. De fato, se r_{t+1} não se anulasse, então r_{t+1} seria reduzido com respeito a G_t. Mas isto significa que nenhum termo não nulo de r_{t+1} pertenceria a $\mathrm{in}(\langle G_t\rangle)$, o que contradiz (45).

Mostramos, então, que existe um inteiro $k > 0$ tal que o resto do S-polinômio correspondente a um par de elementos de G_k é sempre zero. Isto significa que o algoritmo tem que parar. Na prática, contudo, talvez ainda seja necessário executar mais alguns passos além do k-ésimo, porque o algorimo só para quando $\mathcal{P}$ se esvazia.

Por outro lado, para provar que o algoritmo funciona, basta mostrar que se todos os S-polinômios relativos a G_k são nulos, então G_k é uma base de Gröbner do ideal gerado pelo conjunto da entrada. Para não sobrecarregar a demonstração com detalhes circunstanciais, vamos isolar um dos resultados de que precisamos em um lema um tanto técnico, mas bastante simples. Ao ler o enunciado do lema, note cuidadosamente que os índices 1 e 2 se alternam entre u e ν!

LEMA 5.5. *Sejam g_1, g_2, u_1 e u_2 polinômios não nulos em $K[x_1, \ldots, x_n]$. Se $\mathrm{in}(u_1 g_1)$ é múltiplo constante de $\mathrm{in}(u_2 g_2)$ então existem constantes $c_1, c_2 \in K$ e um monômio $\theta \in \mathbb{T}^n$ tais que*

$$\mathrm{in}(u_1) = c_1\theta\nu_2 \quad e \quad \mathrm{in}(u_2) = c_2\theta\nu_1,$$

em que ν_i é o monômio obtido dividindo $\mathrm{in}(g_i)$ pelo máximo divisor comum entre $\mathrm{in}(g_1)$ e $\mathrm{in}(g_2)$.

DEMONSTRAÇÃO. Por hipótese temos que

$$\mathrm{in}(u_1)\mathrm{in}(g_1) = a\mathrm{in}(u_2)\mathrm{in}(g_2), \tag{46}$$

para algum $a \in K$. Por outro lado,

$$\mathrm{in}(g_i) = \delta\nu_i \text{ com } \nu_1, \nu_2 \in \mathbb{T}^n,$$

em que δ é o máximo divisor comum entre $\mathrm{in}(g_1)$ e $\mathrm{in}(g_2)$. Substituindo isto em (46) e cancelando δ, obtemos

$$\mathrm{in}(u_1)\nu_1 = a\mathrm{in}(u_2)\nu_2.$$

Como ν_1 e $\mathrm{in}(g_2)$ não têm monômio em comum, concluímos que

$$\mathrm{in}(u_2) = c_1\nu_1\theta \tag{47}$$

para algum monômio $\theta \in \mathbb{T}^n$ e alguma constante não nula $c_1 \in K$. Disto obtemos também que

$$\text{in}(u_1) = c_2\nu_2\theta. \tag{48}$$

em que $c_2 = ac_1$. □

CRITÉRIO DE BUCHBERGER. *Seja G um subconjunto finito do anel de polinômios $K[x_1, \ldots, x_n]$. Então G é uma base de Gröbner se, e somente se,*

$$\text{R}_G(S(g, g')) = 0,$$

para todo par $(g, g') \in G \times G$.

DEMONSTRAÇÃO. Suponhamos, primeiro, que G seja uma base de Gröbner no anel $K[x_1, \ldots, x_n]$. Se $g, g' \in G$, então $S(g, g')$ pertence ao ideal gerado por G. Portanto, segue da proposição 5.2 que $S(g, g')$ deixa resto zero na divisão por G.

Sem perda de generalidade, todos os elementos da base G podem ser escolhidos mônicos. Fazendo isto, seja

$$G = \{g_1, \ldots, g_t\}$$

e suponhamos que o resto da divisão por G dos S-polinômios

$$S_{ij} = S(g_i, g_j)$$

é zero quaisquer que sejam $1 \leq i, j \leq t$. Para provar a recíproca, devemos mostrar que

> se f pertence ao ideal I gerado por G em de $K[x_1, \ldots, x_n]$,
> então $\text{in}(f)$ é divisível por $\text{in}(g_i)$ para algum $1 \leq i \leq t$.

Como cada polinômio em I pode ser escrito como combinação dos elementos de G, existem $u_1, \ldots, u_t \in K[x_1, \ldots, x_n]$ tais que

$$f = u_1g_1 + \cdots + u_tg_t. \tag{49}$$

Neste caso, diremos que o vetor

$$\mathbf{u} = (u_1, \ldots, u_t) \in K[x_1, \ldots, x_n]^t$$

é uma *relação* de f em G e definiremos

$$\rho(\mathbf{u}) = \max\{\text{in}(u_ig_i) : 1 \leq i \leq t\}$$

que é um elemento de $\mathbb{T}^n$ e

$$\sigma(\mathbf{u}) = \#\{i : \text{in}(u_ig_i) \text{ divide } \rho(\mathbf{u})\}$$

que é um número entre 1 e t.

Suponhamos, para começar, que $\rho(\mathbf{u}) = \text{in}(f)$. Neste caso, existe algum $1 \leq k \leq t$ e alguma cosntante não nula $c \in K$, para os quais

$$\text{in}(f) = c\text{in}(u_kg_k) = c\text{in}(u_k)\text{in}(g_k).$$

Mas isto implica que $\text{in}(g_k)$ divide $\text{in}(f)$, que é o que precisávamos mostrar. Portanto, para concluir a demonstração do critério basta provar que todo f admite uma relação cujo ρ é múltiplo constante de $\text{in}(f)$. Nossa estratégia

consistirá em elaborar um algoritmo que transforma uma relação qualquer em outra que satisfaz a propriedade desejada.

Seja, então, $\mathbf{u}$ uma relação de f em G para a qual

$$\rho(\mathbf{u}) > \mathrm{in}(f).$$

Como os $\mathrm{in}(g_i)$ proporcionais a $\rho(\mathbf{u})$ são maiores que $\mathrm{in}(f)$, eles terão que se cancelar entre si, para que o lado direito de (49) possa ter termo inicial igual a $\mathrm{in}(f)$. Contudo, um tal cancelamento só é viável se houver mais de um $1 \leq i \leq t$ para o qual

$$\mathrm{in}(g_i) \text{ é múltiplo constante de } \rho(\mathbf{u}).$$

Portanto,

$$\text{se } \rho(\mathbf{u}) > \mathrm{in}(f) \text{ então } \sigma(\mathbf{u}) \geq 2.$$

Nossa estratégia consiste, então, em construir a partir de $\mathbf{u}$ uma nova relação $\mathbf{v}$ tal que

$$\rho(\mathbf{v}) < \rho(\mathbf{u}) \text{ ou } \sigma(\mathbf{v}) < \sigma(\mathbf{u}).$$

É nesta construção que intervém a hipótese de que os S-polinômios têm sempre resto zero relativo a G.

Relembrando, vimos que, como estamos supondo que $\rho(\mathbf{u}) > \mathrm{in}(f)$ devemos ter que $\sigma(\mathbf{u}) \geq 2$. Renumerando os gs, se necessário, podemos supor que $\mathrm{in}(u_1 g_1)$ e $\mathrm{in}(u_2 g_2)$ são ambos múltiplos constantes de $\rho(\mathbf{u})$. Em particular, estes dois termos têm $\mu(u)$ como suporte, de modo que seus termos iniciais são múltiplos constantes um do outro. Portanto, pelo lema 5.5 existem constantes $c_1, c_2 \in K$ e $\theta \in \mathbb{T}^n$ para os quais

$$\mathrm{in}(u_1) = c_1 \theta \nu_2 \quad \text{e} \quad \mathrm{in}(u_2) = c_2 \theta \nu_1,$$

em que δ é o máximo divisor comum entre $\mathrm{in}(g_1)$ e $\mathrm{in}(g_2)$ e ν_i é o cofator de δ em $\mathrm{in}(g_i)$.

Usando estas expressões para os termos iniciais de u_1 e u_2, podemos escrever

$$u_1 g_1 + u_2 g_2 = c_2 \nu_2 \theta g_1 + c_1 \nu_1 \theta g_2 + M \tag{50}$$

em que M representa uma soma de termos cujos suportes são monômios *menores* que

$$\rho(\mathbf{u}) = \mathrm{in}(u_1 g_1) = \mathrm{in}(u_2 g_2).$$

Pretendemos rearrumar (50) de modo a fazer aparecer S_{12}. Contudo,

$$c_2 \nu_2 \theta g_1 + c_1 \nu_1 \theta g_2 = (c_2 + c_1) \nu_2 \theta g_1 + c_1 \theta (\nu_1 g_2 - \mu_1 g_1).$$

ao passo que

$$S_{12} = \nu_1 g_2 - \nu_2 g_1.$$

Assim,

$$c_2 \nu_2 \theta g_1 + c_1 \nu_1 \theta g_2 = (c_2 + c_1) \nu_2 \theta g_1 + c_1 \theta S_{12}. \tag{51}$$

Contudo, a hipótese sobre os S-polinômios combinada ao teorema 4.4 da página 112, podemos escrever

$$S_{12} = q_1 g_1 + \cdots + q_t g_t,$$

com

$$\mathrm{in}(S_{12}) = \max\{\mathrm{in}(q_i g_i) : 1 \leq i \leq t\}.$$

Contudo, pela definição do S-polinômio,

$$\mathrm{in}(S_{12}) < \mathrm{in}(g_1 \nu_2) \leq \mathrm{in}(u_1 g_1),$$

de modo que

$$\mathrm{in}(q_i g_i) < \mathrm{in}(u_1 g_1) = \rho(\mathbf{u}),$$

para todo $1 \leq i \leq t$. Combinando isto com (51) podemos concluir que $u_1 g_1 + u_2 g_2$ pode ser escrito na forma

$$u_1 g_1 + u_2 g_2 = v_1 g_1 + \cdots + v_t g_t, \tag{52}$$

em que apenas $v_1 g_1$ pode ter termo inicial igual a $\rho(\mathbf{u})$, pois

$$\mathrm{in}(v_1 g_1) = (c_2 + c_1)\nu_2 \theta \mathrm{in}(g_1).$$

Note, contudo, que pode acontecer que

$$\mathrm{in}(v_i g_i) < \rho(\mathbf{u}),$$

bastando para isto que $c_2 + c_1 = 0$.

Substituindo (52) em (49), obtemos

$$f = v_1 g_1 + v_2 g_2 + (u_3 + v_3) g_3 + \cdots + (u_t + v_t) g_t$$

e as condições sobre os vs garantem que a relação $\mathbf{w}$ dada por

$$w_i = \begin{cases} v_i & \text{se } \ i = 1, 2 \\ v_i + u_i & \text{se } \ i \neq 1, 2 \end{cases}$$

satisfaz

$$\sigma(\mathbf{w}) < \sigma(\mathbf{u}).$$

Como a construção acima decresce σ, eventualmente obteríamos uma relação cujo σ é igual a um. Entretanto, como já observamos acima, isto não é possível. Portanto, ao final de uma quantidade finita de passos teremos algo ainda melhor: uma nova relação cujo ρ é menor que $\rho(\mathbf{u})$. Repetindo, este procedimento geraríamos uma sequência estritamente decrescente de monômios em $\mathbb{T}^n$. Contudo, tal sequência não pode ser infinita, porque toda ordem monomial é uma boa ordem. Portanto, após uma quantidade finita de etapas, esta construção dará lugar a uma relação cujo ρ é igual a $\mathrm{in}(f)$, o que conclui a demonstração. □

5. Bases de Gröbner reduzidas

Como sabemos resolver sistemas lineares pelo método de Gauss, é razoável perguntar o que acontece se aplicarmos o algoritmo de Buchberger a um ideal gerado por polinômios lineares. Digamos que I tem como geradores os polinômios

$$\begin{aligned} h_1 &= x + y + 2z \\ h_2 &= 2x + y + 3z \\ h_3 &= 5x + 4y + 9z, \end{aligned}$$

e que o anel é $\mathbb{C}[x, y, z]$, com a ordem lexicográfica e $x > y > z$.

Começamos inicializando as variáveis com

$$\mathcal{G} = \{h_1, h_2, h_3\} \text{ e } \mathcal{P} = \{(h_1, h_2), (h_1, h_3), (h_2, h_3)\}.$$

Calculando o primeiro S-polinômio temos que

$$S(h_1, h_2) = 2h_1 - h_2 = y + z,$$

que é seu próprio resto na divisão por $\mathcal{G}$. Portanto, ao final do primeiro passo teremos

$$\mathcal{G} = \{h_1, h_2, h_3, h_4\} \text{ e } \mathcal{P} = \{(h_1, h_3), (h_1, h_4), (h_2, h_3), (h_2, h_4), (h_3, h_4)\},$$

onde $h_4 = y + z$. Precisamos executar mais 5 passos, um para cada par em $\mathcal{P}$, mas um cálculo simples mostra que todos estes S-polinômios deixam resto zero na divisão por $\{h_1, h_2, h_3, h_4\}$. Portanto, o conjunto $\{h_1, h_2, h_3, h_4\}$ é uma base de Gröbner para o ideal I.

Entretanto, como estas equações são lineares, podemos aplicar o método de Gauss para simplicar o sistema linear $h_1 = h_2 = h_3 = 0$. Para isto, aplicamos eliminação por linhas à matriz

$$\begin{bmatrix} 1 & 1 & 2 \\ 2 & 1 & 3 \\ 5 & 4 & 9 \end{bmatrix};$$

obtendo

$$\begin{bmatrix} 1 & 1 & 2 \\ 0 & -1 & -1 \\ 0 & 0 & 0 \end{bmatrix};$$

Como aprendemos em álgebra linear, isto significa que o sistema linear $h_1 = h_2 = h_3 = 0$ é equivalente a

$$x + y + 2z = y + z = 0.$$

Contudo, como estes dois últimos polinômios foram obtidos como combinação linear de h_1, h_2, h_3 e h_4, temos também que

$$I = \langle h_1, h_2, h_3 \rangle = \langle x + y + 2z, y + z \rangle.$$

Por outro lado, segundo a base de Gröbner calculada acima, o ideal inicial de I é gerado por

$$\begin{aligned}\mathrm{in}(h_1) &= \mathrm{in}(x+y+2z) = x\\ \mathrm{in}(h_2) &= \mathrm{in}(2x+y+3z) = 2x\\ \mathrm{in}(h_3) &= \mathrm{in}(5x+4y+9z) = 5x\\ \mathrm{in}(h_4) &= \mathrm{in}(y+z) = y.\end{aligned}$$

Portanto,

$$\mathrm{in}(I) = \langle x, y\rangle.$$

Como

$$\mathrm{in}(x+y+2z) = x \quad \text{e} \quad \mathrm{in}(y+z) = y,$$

podemos concluir que $\{x+y+2z, y+z\}$ é uma outra base de Gröbner de I. Em particular, isto nos diz que um mesmo ideal pode ter mais de uma base de Gröbner, mesmo supondo que a ordem monomial esteja fixa.

Olhando para estas duas bases de Gröbner de I,

$$\{x+y+2z, 2x+y+3z, 5x+4y+9z, y+z\} \quad \text{e} \quad \{x+y+2z, y+z\}.$$

uma ao lado da outra, é impossível não notar que a segunda – que foi calculada pelo método de eliminação gaussiana – está contida na primeira. Em outras palavras, o algoritmo de Gauss foi capaz de eliminar polinômios desnessários para que o conjunto de geradores seja uma base de Gröbner, o que não ocorreu com o algoritmo de Buchberger. Uma análise mais cuidadosa do exemplo mostra que os polinômios descartados têm ambos termo inicial divisível por $\mathrm{in}(h_1)$. A justficativa para isto está na seguinte proposição.

PROPOSIÇÃO 5.6. *Seja G uma base de Gröbner no anel $K[x_1, \ldots, x_n]$, com respeito a alguma ordem monomial. Suponhamos que g e h são elementos de G e que $\mathrm{in}(g)$ divide $\mathrm{in}(h)$. Então*

$$H = G \setminus \{h\}$$

também é uma base de Gröbner de $\langle G\rangle$.

DEMONSTRAÇÃO. Para provar a proposição basta mostrar que, para cada $f \in \langle G\rangle$, o termo $\mathrm{in}(f)$ é divisível pelo termo inicial de algum polinômio de H.

Mas G é uma base de Gröbner e, portanto, $\mathrm{in}(f)$ é divisível pelo termo inicial de algum polinômio de G. Se este polinômio *não for* h, então pertence a H e nada há a fazer. Por outro lado, se o polinômio for h, então

$$\mathrm{in}(g) \text{ divide } \mathrm{in}(h) \text{ que divide } \mathrm{in}(f),$$

e em qualquer caso $\mathrm{in}(f)$ é divisível pelo termo inicial de um elemento de H como queríamos mostrar. Note que isto implica, pela proposição 5.1 que G e H geram o mesmo ideal. □

Vamos aplicar este resultado à base de Gröbner calculada na seção 3 para o ideal I gerado por

$$g_1 = -yu + xv + y - 2v \text{ e } g_2 = -uy + xv + v,$$

no anel $\mathbb{C}[x, y, u, v]$, sob a ordem grlex com $x < y < u < v$. A base que encontramos foi $G = \{g_1, g_2, g_3, g_4\}$, em que

$$g_3 = y - 3v \text{ e } g_4 = xv - 3uv + v$$

é uma base de Gröbner de I. Entretanto,

$$\mathrm{in}_{\mathrm{grlex}}(g_3) = y \text{ divide } \mathrm{in}_{\mathrm{grlex}}(g_1) = \mathrm{in}_{\mathrm{grlex}}(g_1) = -uy.$$

Como vimos na proposição 5.6, isto é suficiente para garantir que o conjunto $G' = \{g_3, g_4\}$ também é uma base de Gröbner de I.

Por conter menos elementos, G' é certamente preferível a G. Entretanto, além de menor, G' é menos redundante que G, já que o termo inicial de um elemento de G' não divide o termo inicial de nenhum outro elemento de G'; coisa que não ocorre em G. Isto sugere a seguinte definição. Seja K um corpo e $G = \{g_1, \ldots, g_t\}$ uma base de Gröbner em $K[x_1, \ldots, x_n]$ com respeito a uma ordem monomial $>$. Dizemos que G é *mínima* se

- $\mathrm{in}(g_i)$ tem coeficiente 1 para todo $i = 1, \ldots, t$, e
- se $i \neq j$ então $\mathrm{in}(g_i)$ não divide $\mathrm{in}(g_j)$.

Uma simples inspecção dos elementos mostra que $h_1 = x + y + 2z$ e $h_4 = y + z$ formam uma base de Gröbner mínima do ideal $\langle h_1, h_2, h_3 \rangle$ estudado no começo desta seção.

É fácil ver que o método de Gauss sempre produz uma base de Gröbner mínima de um sistema linear; veja exercício 3. Mesmo quando o sistema não é linear podemos construir uma base de Gröbner mínima a partir de uma base de Gröbner G qualquer. Para isto basta usar a proposição 5.6 várias vezes. O algoritmo resultante executa, para cada $g \in G$, o seguinte passo:

> se $\mathrm{in}(g)$ é divisível pelo termo inicial de algum elemento de G então faça $G = G \setminus \{g\}$.

Como $\langle G \rangle = \langle G \setminus \{g\} \rangle$, segue que a base obtida ao final da execução do algoritmo gera o mesmo ideal que a base da entrada.

As bases mínimas gozam de algumas excelentes propriedades, como mostra a proposição seguinte.

PROPOSIÇÃO 5.7. *Sejam $G = \{g_1, \ldots, g_s\}$ e $H = \{h_1, \ldots, h_t\}$ bases de Gröbner mínimas de um mesmo ideal. Então:*

(1) $s = t$;
(2) *é possível reordenar os elementos de H de modo que* $\mathrm{in}(h_i) = \mathrm{in}(g_i)$, *para* $i = 1, \ldots, s$.

DEMONSTRAÇÃO. Podemos supor, sem perda de generalidade, que $s \leq t$. Como H é uma base de Gröbner de $I = \langle G \rangle$, então o termo inicial de cada elemento de G será divisível pelo termo inicial de algum elemento de H. Para $i = 1, \ldots, t$ escolha h_i como sendo um elemento de H cujo termo inicial

divide $\mathrm{in}(g_i)$. Entretanto, como $h_i \in I$, então $\mathrm{in}(h_i)$ é divisível pelo termo inicial de algum elemento de G. Seja g_j este elemento. Mas

$$\mathrm{in}(g_j) \text{ divide } \mathrm{in}(h_i) \text{ que divide } \mathrm{in}(g_i).$$

Como G é uma base mínima, isto implica que

$$\mathrm{in}(g_j) = \mathrm{in}(h_i) = \mathrm{in}(g_i).$$

Finalmente, H não pode ter nenhum elemento além de $h_1, \ldots, h_s$. De fato, o termo inicial de um tal elemento seria divisível por $\mathrm{in}(g_i)$ para algum $1 \leq i \leq s$. Mas $\mathrm{in}(g_i) = \mathrm{in}(h_i)$ e obtemos uma contradição com o fato de H ser uma base mínima. □

Apesar de representarem um passo adiante, as bases mínimas ainda não são únicas. Por exemplo, tanto $\{x + y, y\}$ quanto $\{x, y\}$ são bases de Gröbner mínimas do ideal $\langle x, y\rangle$ no anel $\mathbb{C}[x, y]$ sob a ordem lexicográfica com $x > y$. Por isso, introduzimos uma definição ainda mais restritiva. Uma base de Gröbner G em $K[x_1, \ldots, x_n]$ é *reduzida* se:

- G é mínima;
- cada $g \in G$ é reduzido com relação a $G \setminus \{g\}$.

Voltando ao exemplo do início da seção, já vimos que os polinômios

$$g_3 = y - 3v \text{ e } g_4 = xv - 3uv + v$$

formam uma base mínima do ideal I que foi obtido a partir de nossa formulação do problema das medianas. Uma simples inspecção dos polinômios mostra que

$$\mathrm{R}_{\{g_4\}}(g_3) = g_3 \text{ e } \mathrm{R}_{\{g_3\}}(g_4) = g_4,$$

de modo que esta base também é reduzida.

Já conhecemos um algoritmo que, a partir de uma base de Gröbner qualquer, constrói uma base mínima. Portanto, precisamos apenas descrever um algoritmo que, a partir desta base mínima constrói uma base reduzida. Seja $G = \{g_1, \ldots, g_s\}$ uma base mínima de $K[x_1, \ldots, x_n]$, o algoritmo pode ser descrito compactamente da seguinte maneira:

> Inicialize $\mathcal{G}$ com G e então, começando de $i = 1$ e indo até $i = n$, troque g_i em $\mathcal{G}$ pelo seu resto na divisão por $\mathcal{G} \setminus \{g_i\}$.

Para entender porque o algoritmo funciona, vamos analisar sua execução. Seja $\mathcal{G}_i$ o valor da variável $\mathcal{G}$ ao final do i-ésimo laço e r_i o resto da divisão de g_i por $\mathcal{G}_{i-1} \setminus \{g_i\}$. Então $\mathcal{G}_0 = G$ e

$$\mathcal{G}_i = \{r_1, \ldots, r_i, g_{i+1}, \ldots, g_s\}.$$

Observe que

$$\langle \mathcal{G}_i \rangle = \langle \mathcal{G}_{i-1} \rangle,$$

pois $g_i - r_i$ é uma combinação linear de $r_1, \ldots, r_{i-1}$ e $g_{i+1}, \ldots, g_s$. Assim,

$$\langle \mathcal{G}_s \rangle = \langle \mathcal{G}_0 \rangle = G.$$

Logo a saída do algoritmo é um conjunto de geradores para o mesmo ideal do qual G é uma base de Gröbner.

Para concluir a demonstração de que o algoritmo funciona precisamos ainda verificar que $\mathcal{G}_s = \{r_1, \ldots, r_s\}$ é uma base reduzida. Como G é uma base de Gröbner mínima, o termo inicial de g_i não é divisível pelo termo inicial de nenhum g_j, quando $i \neq j$. Isto significa que, quando calculamos o resto da divisão de g_i por $\mathcal{G}_{i-1} \setminus \{g_i\}$, o termo inicial não é alterado. Em outras palavras, $\mathrm{in}(g_i) = \mathrm{in}(r_i)$. Em particular, $\mathcal{G}_s$ também é uma base mínima. Por outro lado, usando o teorema 4.4 do capítulo 3, podemos afirmar que o suporte de r_i não tem nenhum termo divisível por g_j, se $j \neq i$. Como $\mathrm{in}(g_j) = \mathrm{in}(r_j)$, a mesma afirmação vale se trocamos g_j por r_j. Mas isto significa que r_i é reduzido com respeito a $\mathcal{G}_s$. Portanto, $\mathcal{G}_s$ tem que ser, de fato, uma base de Gröbner reduzida.

Vejamos o que acontece quando aplicamos este algoritmo à base $\{h_1, h_4\}$, que já sabemos ser mínima. Inicializando

$$\mathcal{G} = \{h_1, h_4\} = \{x + y + 2z, y + z\},$$

devemos dividir h_1 por

$$\mathcal{G} \setminus \{h_1\} = \{h_2\}.$$

O resto desta divisão é $x + z$. Trocando h_1 por $x + z$ em $\mathcal{G}$, obtemos

$$\mathcal{G} = \{x + z, y + z\},$$

ao final do primeiro passo. No segundo passo devemos calcular o resto da divisão de $y + z$ por $x + z$. Mas neste caso o resto é igual a $y + z$ e não há nenhuma troca de elementos. Portanto, ao final da aplicação do algoritmo, obtemos a base reduzida $\{x + z, y + z\}$ para o ideal $\langle h_1, h_2, h_3 \rangle$. Observe que esta base é a mesma que resultaria da aplicação da redução da matriz do sistema formado pelos polinômios h_1, h_2 e h_3 à forma escalonada reduzida – aquela em que as posições acima dos pivôs não nulos de cada linha são todas zero.

Encerramos a seção mostrando que cada ideal tem apenas uma base de Gröbner reduzida para uma ordem monomial dada.

PROPOSIÇÃO 5.8. *Cada ideal de $K[x_1, \ldots, x_n]$ admite uma única base de Gröbner reduzida.*

DEMONSTRAÇÃO. Suponha que G e H são duas bases de Gröbner reduzidas de um ideal I de $K[x_1, \ldots, x_n]$ com respeito a uma mesma ordem monomial.

Em particular, G e H são bases mínimas. Portanto, têm o mesmo número de elementos. Além disso, se

$$G = \{g_1, \ldots, g_s\} \text{ e } H = \{h_1, \ldots, h_s\},$$

então, podemos assumir que $\mathrm{in}(g_i) = \mathrm{in}(h_i)$, para $i = 1, \ldots, s$. Segue desta igualdade que cada h_i é reduzido não apenas com respeito a $H \setminus \{h_i\}$, mas também com relação a $G \setminus \{g_i\}$. Para provar a proposição precisamos mostrar que $g_i = h_i$ para todo $1 \leq i \leq s$.

Suponha, então, por contradição, que $g_i \neq h_i$, para algum $1 \leq i \leq s$. Isto implica que o suporte de $g_i - h_i$ não é vazio. Mas $g_i - h_i \in I$, de modo que $\mathrm{R}_G(g_i - h_i) = 0$ pela proposição 5.2 . Isto significa que, dado um monômio do suporte de $g_i - h_i$, existirá um $\mathrm{in}(g_j)$ que o divide. Entretanto, como $\mathrm{in}(g_i) = \mathrm{in}(h_i)$, os monômios em $\mathrm{sup}(g_i - h_i)$ são menores que $\mathrm{in}(g_i)$. Portanto, $j \neq i$, o que contradiz o fato de g_i e h_i serem ambos reduzidos com respeito a $G \setminus \{g_i\}$, provando assim a proposição. □

6. O problema da pertinência

Como vimos na proposição 5.2 da página 122, é possível resolver completamente o problema da pertinência de um polinômio a um ideal usando bases de Gröbner e o algoritmo de divisão. Mais precisamente, suponha que queremos determinar se um polinômios f pertence ao ideal gerado por um subconjunto finito F de $K[x_1, \ldots, x_n]$. Para isto

- calculamos uma base de Gröbner G de $\langle F \rangle$;
- dividimos f por G;

então $f \in \langle F \rangle$ se, e somente se, o resto da divisão de f por G é zero. Começaremos aplicando esta estratégia aos problemas abordados nas seções 6 e 8 no capítulo 1.

Consideremos, primeiramente, o teorema das medianas de um triângulo. De acordo com o método esboçado na seção 7 do capítulo 1, precisamos apenas provar que o polinômio

$$c = 2xv - v - 2uy + y,$$

pertence ao ideal gerado pelos polinômios

$$h_1 = vx + v - uy \quad \text{e} \quad h_2 = vx - 2v - uy + y.$$

Em vez de usar a base de Gröbner deste ideal obtida na seção 3, vamos calcular uma nova base para este ideal, desta vez relativamente à ordem lexicográfica com $x > y > u > v$. Neste caso, temos

$$S(h_1, h_2) = -y + 3v,$$

que será denotado por h_3. Como os S-polinômios $S(h_1, h_3)$ e $S(h_2, h_3)$ deixam resto zero relativamente ao conjunto

$$\{h_1, h_2, h_3\},$$

podemos concluir do critério de Buchberger que este conjunto é uma base de Gröbner de $\langle h_1, h_2 \rangle$ relativamente à ordem lexicográfica com $x > y > u > v$. Contudo, h_1 e h_2 têm o mesmo termo inicial, de modo que esta base de Gröbner não é mínima. Para minimalizá-la removemos h_2, obtendo

$$\{h_1, h_3\}.$$

Esta nova é mínima mas não é reduzida, porque

$$\mathrm{R}(h_1)_{\{h_3\}} = xv - 3uv + v.$$

Como

$$\mathrm{R}(h_3)_{\{h_1\}} = h_3,$$

podemos concluir que

$$G = \{xv - 3uv + v, y - 3v\}$$

é uma base de Gröbner reduzida de $\langle h_1, h_2\rangle$.

Para finalizar a aplicação da estratégia delineada acima, resta-nos apenas calcular o resto da divisão de c por G, que nos dá

$$\begin{array}{rl|l} 2xv - v - 2uy + y & & xv - 3uv + v \\ & & y - 3v \\ \hline -2uy + y + 6uv - 3v & & Q_1 = 2 \\ y - 3v & & Q_2 = 2u + 1 \\ 0 & & R = 0 \end{array}$$

Isto comprova que c pertence mesmo ao ideal $\langle h_1, h_2\rangle$, completando assim a demonstração do teorema das medianas.

Passando ao teorema de Apolônio, lembre-se que, segundo a formulação algébrica descrita na seção 8 do capítulo 1, basta-nos mostrar que

$$c = -2ux + x^2 - 2vz + z^2 + u - 1/4.$$

pertence ao ideal de $\mathbb{Q}[x, y, u, v]$ gerado pelos polinômios

$$\begin{aligned} h_1 &= vy - y^2/4 - u + 1/4, \\ h_2 &= vy - y^2/4, \\ h_3 &= x - zy, \\ h_4 &= y(x - 1) + z. \end{aligned}$$

Neste caso o cálculo da base de Gröbner é mais complicado porque, de partida, temos que calcular S-polinômios correspondentes a

$$\binom{4}{2} = 6$$

pares de polinômios, o que é muito para fazer com lápis e papel. Com o auxílio de um computador, facilmente verificamos que a base de Gröbner reduzida de $\langle h_1, h_2, h_3, h_4\rangle$ relativamente à ordem lexicográfica com $x > y > u > v > z$ é

$$G = \{x - 4zv, y - 16zv^2 - z, u - \frac{1}{4}, z^2v^2 - \frac{zv}{4} + \frac{z^2}{16}\}.$$

Dividindo c por G verificamos que, de fato, o resto é zero, confirmando, assim, que

$$c \in \langle h_1, h_2, h_3, h_4\rangle;$$

que completa nossa demonstração do teorema de Apolônio.

Encerraremos a seção considerando um caso importante, e menos elementar, do problema da pertinência. Digamos que I seja um ideal de $K[x_1, \ldots, x_n]$ e que queremos determinar se um dado polinômio pertence, não a I, mas sim a seu radical $\sqrt{I}$. Tomando como ponto de partida a definição do radical, talvez lhe ocorra a ideia de testar se $c^k \in I$, enquanto incrementamos k de uma em uma unidade. Embora esta estratégia seja viável se $c \in \sqrt{I}$—ao menos em princípio—ela jamais será capaz de provar que $c \notin \sqrt{I}$, se for este o caso.

Contudo, aplicando a proposição 3.11 da página 88, podemos criar um algoritmo capaz de resolver completamente este problema. A parte da proposição 3.11 que nos interessa é a que diz que, sob a notação anterior,

> $f \in \sqrt{I}$ se, e somente se, o ideal
>
> $$J(I, f) = \langle 1 - zf \rangle + K[x_1, \ldots, x_n, z]I$$
>
> contém 1.

Usando o que aprendemos neste capítulo podemos reformular isto dizendo que

> $f \in \sqrt{I}$ se, e somente se, a base de Gröbner reduzida de $J(I, f)$ é igual a $\{1, \}$;

que sugere o seguinte algoritmo.

ALGORITMO 5.9 (Pertinência ao radical). *Dados um ideal I e um polinômio f do anel $\mathbb{Q}[x_1, \ldots, x_n]$, o algoritmo tem saída* `sim`*, se $f \in \sqrt{I}$; caso contrário, a saída é* `não`*.*

> **Etapa 1:** *O ideal I é dado em termos de um conjunto de geradores $g_1, \ldots, g_s$. Construa o ideal*
>
> $$J(I, f) = \langle g_1, \ldots, g_s, 1 - zf \rangle,$$
>
> *do anel $\mathbb{Q}[x_1, \ldots, x_s, z]$.*
> **Etapa 2:** *Calcule a base de Gröbner* reduzida G *de $J(I, f)$.*
> **Etapa 3:** *Se $G = \{1\}$ a saída é* `sim`*, caso contrário, a saída é* `não`*.*

Por exemplo, será que os polinômios

$$h_1 = y^4 + x^3 - x^2y + xy^2 + x^2 + x \quad \text{e} \quad h_2 = y^3 + x^2 + x - 3,$$

pertencem ao ideal I, gerado por

$$x^6 + 3x^4y^2 + 3x^2y^4 + y^6 + 3x^5 + 6x^3y^2 + 3xy^4 + 6x^4 + \\ + 9x^2y^2 + 3y^4 + 7x^3 + 6xy^2 + 6x^2 + 3y^2 + 3x + 1, \\ y^6 - 2x^2y^3 + x^4$$

no anel de polinômios $K[x, y]$? De acordo com o algoritmo acima, devemos calcular a base de Gröbner G_i correspondente ao ideal

$$J_i = I + \langle th_i - 1 \rangle,$$

para $1 \leq i \leq 2$. Fazendo isto, obtemos $G_1 = \{1\}$ e

$$\begin{aligned} G_2 = \{&x^6 + 3x^4y^2 + 3x^2y^4 + y^6 + 3x^5 + 6x^3y^2 + 3xy^4 + 6x^4 + \\ &+ 9x^2y^2 + 3y^4 + 7x^3 + 6xy^2 + 6x^2 + 3y^2 + 3x + 1, \\ &y^6 - 2x^2y^3 + x^4, \\ &y^4t + x^3t - x^2y^t + xy^2t + x^2t + xt - 1, \\ &y^3t + x^2t + x^t - 3t - 1\}. \end{aligned}$$

Portanto, h_1 pertence a $\sqrt{I}$, ao passo que h_2 não pertence.

O problema da pertinência de um polinômio ao radical de um dado ideal desempenhará papel fundamental no próximo capítulo, em que sistematizaremos alguns alguns algoritmos capazes de implementar de modo eficiciente o método do capítulo 1 para a demonstração automática de teoremas de geometria plana.

7. Complexidade

Nesta seção analisamos o custo do algoritmo de Buchberger, tendo como ponto de partida a relação entre o máximo dos graus de uma base de Gröbner mínima e do conjunto de geradores a partir do qual ela foi calculada. Dada a natureza um tanto intrincada das demonstrações, provaremos apenas alguns resultados elementares para o caso de duas variáveis. Também mencionaremos—sem demonstração—alguns resultados referentes ao tempo de execução e à quantidade de espaço de memória necessários para a execução do algoritmo de Buchberger. Estes últimos resultados requerem conhecimento básico de máquinas de Turing para o seu perfeito entendimento.

Seja, pois, K um corpo e S um subconjunto finito de $K[x_1, \ldots, x_n]$. Denotaremos por $\mathrm{grau}(S)$ o máximo entre os graus totais dos elementos de S. A primeira pergunta que desejamos fazer é a seguinte:

> se G é uma base de Gröbner de $\langle S \rangle$ relativamente a uma ordem monomial $<$ fixada, qual é a relação entre $\mathrm{grau}(S)$ e $\mathrm{grau}(G)$?

Como veremos, esta relação depende da ordem monomial escolhida. Nosso primeiro resultado refere-se à ordem glex aplicada ao caso em que o anel tem duas variáveis.

PROPOSIÇÃO 5.10. *Seja K um corpo. Dado um inteiro $d \geq 3$ existe um subconjunto finito S_d de $K[x_1, x_2]$ tal que*

$$\mathrm{grau}(G_d) \geq \mathrm{grau}(S_d)$$

em que G_d é a a base de Gröbner reduzida de $\langle S \rangle$ relativamente a glex com $x_2 > x_1$.

DEMONSTRAÇÃO. Dado d, considere o conjunto

$$S_d = \{x_1 x_2^{d-1} - x_1^d, x_2^d\}.$$

Para determinar a base de Gröbner correspondente, calculamos o S-polinômio entre os dois elementos de S_d; o que nos dá

$$S(x_2^d, x_1 x_2^{d-1} - x_1^d) = x_1^d x_2.$$

Como o S-polinômio entre quaisquer dois monômios é sempre nulo, na etapa seguinte basta calcular

$$S(x_1^d x_2, x_1 x_2^{d-1} - x_1^d) = x_1^{2d-1}.$$

Mais uma vez, obtivemos apenas um monômio, de modo que é suficiente calcular

$$S(x_1^{2d-1}, x_1 x_2^{d-1} - x_1^d) = x_1^{3d-2}.$$

Contudo, $3d - 2 \geq 2d - 1$ para todo $d \geq 3$, de forma que o resto da divisão deste último monômio pelo conjunto

$$G_d = \{x_1 x_2^{d-1} - x_1^d, x_2^d, x_1^d x_2, x_1^{2d-1}\}$$

tem que ser zero. Portanto, G_d é uma base de Gröbner do ideal gerado por S_d. Esta base é reduzida, como mostra uma simples inspecção dos seus elementos, o que prova o resultado desejado. □

A recíproca da proposição acima é verdadeira pelo seguinte teorema, devido a D. Lazard; veja [**8**, Theorem 1, p. 139].

TEOREMA 5.11. *Seja K um corpo, S um subconjunto finito de $K[x_1, x_2]$ e G uma base de Gröbner de $\langle S\rangle$ relativamente à ordem glex. Então,*

$$\text{grau}(G) \leq 2\text{grau}(S) - 1.$$

A demonstração consiste em mostrar que *todos* os polinômios que ocorrem no cálculo de uma base de Gröbner de $\langle S\rangle$ têm grau menor ou igual do que $2\text{grau}(2) - 1$. Em particular isto será verdadeiro para os elementos da base final. Passando, agora, à ordem lexicográfica, temos a seguinte proposição.

PROPOSIÇÃO 5.12. *Seja K um corpo. Dado um inteiro $d \geq 3$ existe um subconjunto finito S_d de $K[x_1, x_2]$ tal que*

$$\text{grau}(G_d) \geq \text{grau}(S_d)^2$$

em que G_d é a a base de Gröbner reduzida de $\langle S\rangle$ relativamente a lex com $x_2 > x_1$.

DEMONSTRAÇÃO. Dado d, considere o conjunto

$$S_d = \{x_2^d - x_1, x_2 - x_1^d\}.$$

Para determinar a base de Gröbner correspondente, calculamos o S-polinômio entre os dois elementos de S_d, que nos dá

$$S(x_2^d - x_1, x_2 - x_1^d) = x_1^d x_2^{d-1} - x_1,$$

e cujo resto relativamente a S_d é $x_1^{d^2} - x_1$; veja exercício ??? do capítulo 4. Um cálculo simples mostra que os S-polinômios entre os elementos de S_d e $x_1^{d^2} - x_1$ têm resto zero relativamente a

$$\{x_2^d - x_1, x_2 - x_1^d, x_1^{d^2} - x_1\}.$$

Portanto, esta é uma base de Gröbner do ideal gerado por S_d. Contudo, esta base não é sequer mínima, porque

$$\text{in}(x_2 - x_1^d) = x_2 \text{ divide } x_2^d = \text{in}(x_2^d - x_1).$$

Isto signfica que podemos descartar $x_2^d - x_1$, de modo que

$$\{x_2 - x_1^d, x_1^{d^2} - x_1\}$$

também é uma base de Gröbner do ideal gerado por S_d. Desta vez a base é reduzida, o que completa assim a demonstração da proposição. □

Observe a enorme variação no grau entre bases de Gröbner obtidas a partir de glex e a partir de lex. Isto ajuda a explicar porque o cálculo das bases de Gröbner relativas à ordem lexicográfica demora tanto relativamente ao custo do cálculo com ordens de grau. Este é um fenômeno bem conhecido e que levou ao desenvolvimento de algoritmos que, após calcular a base de Gröbner para uma ordem de grau, usa algum método rápido para disto derivar a base relativa a lex. Estudaremos um destes algoritmos na seção 8 do capítulo 8.

Existem resultados, semelhantes aos anteriores, que valem qualquer que seja a quantidade de variáveis presente no anel de polinômios. Um destes é o seguinte teorema cuja demonstração pode ser encontrada em [**24**].

TEOREMA 5.13. *Seja K um corpo, S um subconjunto finito de polinômios* homogêneos *de $K[x_1, \ldots, x_n]$ e G uma base de Gröbner de $\langle S \rangle$ relativamente a alguma ordem monomial. Se $d = \text{grau}(S)$, então,*

$$\text{grau}(G) \leq 2\left(\frac{d^2}{2} + d\right)^{2^{n-1}}.$$

Observe que se trata de uma cota *duplamente exponencial*; isto é, uma exponencial de exponencial de $\text{grau}(S)$. Quando $n = 2$, a cota que advém do teorema 5.13 é

$$\text{grau}(G) \leq 2\left(\frac{d^2}{2} + d\right)^{2};$$

em que o lado esquerdo é um polinômio em d de grau 4. Portanto, temos neste caso uma cota bem pior que a que foi dada no teorema 5.11. Entretanto, a cota do teorema 5.13 é verdadeira para *qualquer* ordem monomial, ao passo que a do teorema 5.11 está limitada a glex. Uma cota bem mais refinada que a do teorema 5.13 pode ser encontrada em [**53**, capítulo 38].

Quanto ao tempo de execução e ao uso de memória, pode-se provar que, dados um polinômio f e um ideal I de um anel de polinômios com coeficientes racionais, o problema de determinar se f pertence a I admite uma cota inferior *exponencial* para a quantidade de memória utilizada e uma cota inferior

duplamente exponencial para o tempo que uma máquina de Turing levaria para executá-lo. Porém, como vimos na proposição 5.2, este problema pode ser resolvido em duas etapas,

(1) calculando uma base de Gröbner G para I;
(2) verificando se f deixa resto zero na divisão por G.

Como a etapa (2) tem custo polinomial, o custo de resolver este problema recai inteiramente sobre o cálculo da base de Gröbner. Portanto, uma base de Gröbner não pode, em geral, ser calculada senão utilizando

- uma quantidade de memória que aumenta *exponencialmente*, e
- um tempo que aumenta de maneira *duplamente exponencial*

relativamente ao tamanho da entrada em bits. Neste contexto a quantidade de memória utilizada refere-se ao número de casas utilizadas no processamento do programa por uma máquina de Turing. Uma variedade de resultados semelhantes pode ser encontrado em [**31**, pp. 589–591]. Para mais detalhes sobre máquinas de Turing e sua importância no estudo da complexidade de algoritmos consulte [**62**, parte III].

8. Comentários e complementos

Há muito mais a dizer sobre bases de Gröbner e os algoritmos utilizados para calculá-las do que caberia neste capítulo ou, até mesmo, neste livro. Para começar o próprio Buchberger observou que há S-polinômios que não precisam ser calculados porque podemos prever que não darão lugar a nenhum novo polinômio que deva ser incluído na base. Este é o caso, por exemplo, de polinômios cujos termos iniciais são relativamente primos; veja ??? . Esta e outros melhoramentos simples ao algoritmo original de Buchberger podem ser encontrados em [**17**, seção 9 do capítulo 2]. Para um tratamento mais sistemático das bases de Gröbner que inclui inúmeras maneiras de otimizar o algoritmo consulte [**53**].

Todos os sistemas de computação algébrica de carácter geral, como o AXIOM e o MAXIMA, trazem implementações mais ou menos otimizadas do algoritmo de Buchberger. Além disso, há sistemas especializados dos quais este algoritmo constitui o próprio âmago, como o MACAULAY e o SINGULAR. Todos estes sistemas estão em domínio público e podem ser baixados e instalados diretamente da web.

9. Exercícios

1. Sejam f e g polinômios em $K[x]$. Mostre que aplicar o algoritmo de Buchberger a $\{f, g\}$ é essencilamente equivalente a aplicar o algoritmo euclidiano estendido a estes polinômios.

2. Seja K um corpo e $f, g \in K[x_1, \ldots, x_n]$. Mostre que:
   (a) se f e g são monômios então $S(f, g) = 0$;
   (b) se f e g são binômios então $S(f, g)$ é um binômio;
   (c) se f é um monômio e g um binômio então $S(f, g) = 0$.

3. Calcule bases de Gröbner para os seguintes ideais usando o algoritmo de Buchberger na ordem grlex:
   (a) $\langle x^2y - 1, xy^2 - x\rangle$;
   (b) $\langle x2 + y, x^4 + 2x^2y + y^2 + 3\rangle$;
   (c) $\langle x - z^4, y - z^5\rangle$.
   Confira o resultado que você obteve calculando estas mesmas bases em um sistema de computação algébrica.

4. Mostre que, se G é uma base de Gröbner e f um elemento de um anel de polinômios $K[x_1, \ldots, x_n]$ então qualquer escolha de i como primeiro caso no algoritmo de divisão produz o mesmo resto de f por G.

5. Mostre que o método de Gauss sempre produz bases de Gröbner mínimas, quando aplicado a um sistema linear. Essas bases são sempre reduzidas?

6. Ache bases de Gröbner reduzidas para os ideais do exercício 1.

7. Seja G uma base de Gröbner para a qual o coeficiente de $\mathrm{in}(g)$ é 1 para cada $g \in G$. Mostre que G é uma base de Gröbner mínima se, e somente se, nenhum subconjunto próprio de G é uma base de Gröbner.

8. Fixe uma ordem monomial e suponha que G e G' são bases de Gröbner mínimas, distintas, de um mesmo ideal. Mostre que $\mathrm{in}(G) = \mathrm{in}(G')$.

9. É verdade que uma base de Gröbner de um ideal monomial tem que ser formada por monômios?

10. Seja F um subconjunto finito de $K[x_1, \ldots, x_n]$. Mostre que, se cada elemento de F é uma diferença entre dois monômios, então o ideal $\langle F\rangle$ admite uma base de Gröbner que satisfaz esta mesma propriedade.

11. Seja G uma base de Gröbner reduzida de um ideal I do anel $K[x_1, \ldots, x_n]$. Mostre que $G = \{1\}$ se, e somente se, $I = K[x_1, \ldots, x_n]$.

12. Considere o ideal
$$I_k = \langle x_1^k, x_1^{k-1}x_2, \ldots, x_1x_2^{k-1}, x_2^k\rangle,$$
do anel de polinômios $\mathbb{Q}[x_1, x_2]$.
   (a) Determine uma base de Gröbner para o ideal I_k relativamente à ordem lexicográfica.
   (b) Determine uma base de Gröbner para o ideal I_k relativamente à ordem glex.
   (c) Determine uma base de Gröbner para o ideal I_k relativamente à ordem grlex.

13. Mostre que a base de Gröbner do ideal I_k definido no exercício anterior é a mesma, qualquer que seja a ordem monomial escolhida para $\mathbb{Q}[x_1, x_2]$.

14. Mostre que, dado um inteiro qualquer $d \geq 1$, existe um ideal de $k[x_1, x_2]$ cuja base de Gröbner tem, pelo menos, $d + 1$ elementos.

15. Explique detalhadamente porque o algoritmo de Buchberger se reduz ao algoritmo euclidiano quando utilizado em um anel de polinômios sobre um corpo que tem uma única indeterminada.

16. Seja $d \geq 3$ um inteiro positivo, e considere o ideal
$$I = \langle x_1 x_2^{d-1} - x_1^d, x_2^d \rangle$$
do anel de polinômios $K[x_1, x_2]$, munido da ordem glex, com $x_1 < x_2$.
    (a) Calcule uma base de Gröbner reduzida para I usando o algoritmo de Buchberger.
    (b) Use (a) para mostrar que, se G é uma base de Gröbner qualquer de I, relativa à ordem glex, então G admite um elemnto de grau total maior ou igual a $2d - 1$.

17. Seja $d \geq 3$ um inteiro positivo, e considere o ideal
$$I = \langle x_2^d - x_1, x_2 - x_1^d \rangle$$
do anel de polinômios $K[x_1, x_2]$, munido da ordem lexicográfica, com $x_1 < x_2$.
    (a) Calcule uma base de Gröbner reduzida para I usando o algoritmo de Buchberger.
    (b) Use (a) para mostrar que, se G é uma base de Gröbner qualquer de I, relativa à ordem lexicográfica, então G admite um elemento de grau total maior ou igual a d^2.

CAPíTULO 6

Geometria Euclidiana no Plano

Neste capítulo utilizaremos tudo o que foi feito anteriormente para elaborar em detalhes o método para a demonstração automática de teoremas de geometria euclidiana esboçado na seção 7 do capítulo 1. Começamos com um exemplo que nos ajudará a relembrar a maneira como os teoremas de geometria foram modelados em termos de equações algébricas no capítulo 1.

1. A reta de Newton-Gauss

Nosso ponto de partida é uma definição. Um *quadrilátero completo* é a figura determinada por quatro retas, das quais não há três concorrentes em um mesmo ponto, e seus seis pontos de interseção—chamados de *vértices*—como na ilustração abaixo.

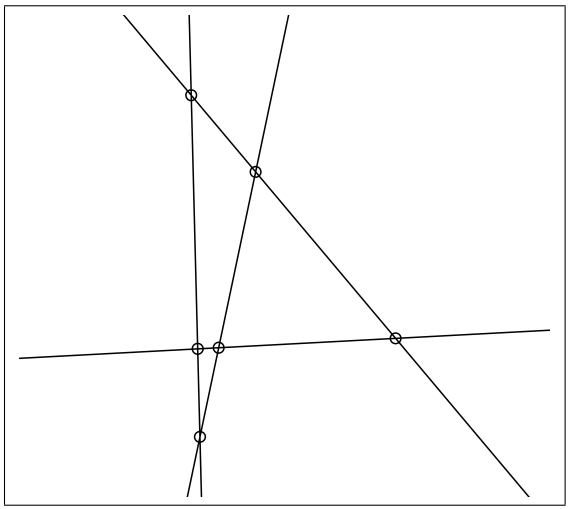


FIGURA 1. Um quadrilátero completo

Dizemos que dois vértices são *adjacentes* se não estão sobre uma mesma das quatro retas que constituem o quadrilátero. Como usual, uma *diagonal* de um quadrilátero completo é um segmento de une dois pontos que não são adjacentes. Usando esta terminologia, podemos enunciar o teorema que desejamos provar da seguinte maneira.

TEOREMA 6.1. *Os pontos médios das diagonais de um quadrilátero completo são colineares.*

A reta que contém estes pontos médios é conhecida como *reta de Newton-Gauss*. Newton mostrou que, se uma cônica é inscrita em um quadrilátero completo, então seu centro está contido na reta de Newton-Gauss. Na figura abaixo a reta de Newton-Gauss do quadrilátero completo da figura 1 aparece em negrito.

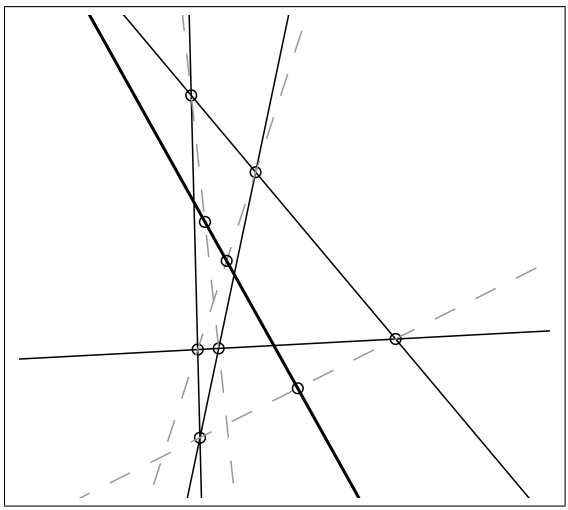


FIGURA 2. A reta de Newton-Gauss

Par modelar o teorema precisamos criar quatro retas que não são três a três coincidentes. Como cada dois pontos determinam uma reta, podemos pensar nas quatro retas como sendo A_1A_2, B_1B_2, A_2B_1 e A_1B_2. Onde A_1, A_2, B_1 e B_2 são quatro pontos distintos do plano. Resta-nos escolher as coordenadas destes pontos ou, o que dá no mesmo, escolher a melhor maneira de posicionar o sistema de coordenadas. A maneira mais natural seria posicionar o eixo x ao longo de uma das quatro retas. Mas não é isto que faremos. De fato, é preferível posicionar uma das diagonais, digamos A_1B_2, ao longo do eixo x. Escolhendo a escala de forma que $A_1 = (0, 0)$ e $B_2 = (1, 0)$, o ponto médio de A_1B_2 terá coordenadas $M_1 = (1/2, 0)$. Desta forma pudemos especificar os valores exatos de três dos nove pontos de que o problema trata. Se, ao invés disto, tivéssemos posicionado A_1B_1 ao longo de x, só teríamos podido fixar os valores das coordenadas de A_1 e B_1; isto é, de dois dos nove pontos.

Como A_2 e B_2 podem estar em qualquer posição relativamente aos pontos já escolhidos, escreveremos

$$A_2 = (x_1, y_1) \quad \text{e} \quad B_2 = (x_2, y_2).$$

Assim, o ponto médio M_2 da diagonal A_2B_2 tem coordenadas

$$M_2 = \left(\frac{x_1 + x_2}{2}, \frac{y_1 + y_2}{2} \right).$$

Até agora só consideramos quatro dos seis pontos que constituem o quadrilátero completo. Denotaremos por

$$Q_1 = (u, v) \quad \text{e} \quad Q_2 = (s, t),$$

os outros dois pontos. Se Q_1 pertence à interseção de A_1A_2 com B_1B_2 então, igualando coeficientes angulares, temos que

$$\frac{v}{u} = \frac{y_1}{u} \quad \text{e} \quad \frac{v}{u-1} = \frac{y_2}{x_2 - 1};$$

que nos dão duas hipóteses, representadas pelos polinômios

$$h_1 = vx_1 - y_1u \quad \text{e} \quad h_2 = v(x_2 - 1) - y_2(u - 1).$$

Procedendo de maneira análoga com respeito a Q_2, que é o ponto de interseção de A_1B_2 e A_2B_1, obtemos

$$\begin{aligned} h_3 &= tx_2 - sy_2 \quad \text{e} \\ h_4 &= t(x_1 - 1) - y_1(s - 1). \end{aligned}$$

O segmento Q_1Q_2 fornece a terceira diagonal do quadrilátero completo, cujo ponto médio é

$$M_3 = \left(\frac{u + s}{2}, \frac{v + t}{2} \right).$$

Finalmente, a conclusão corresponde a dizer que os pontos M_1, M_2 e M_3 são colineares, que é

$$c = (t + v)(x_1 + x_2 - 1) - (y_1 + y_2)(s + t - 1).$$

Reunindo, agora, as hipóteses no ideal

$$I = \langle h_1, h_2, h_3, h_4 \rangle,$$

calculamos a sua base de Gröbner reduzida G relativamente a glex. Além dos quatro geradores de I, esta base contém mais oito polinômios, a saber

$$\begin{aligned} &y_2x_1t - y_1x_2t + y_1y_2 - y_2t \\ &x_2vs - x_2ut - vs + x_2t \\ &x_1vs - x_1ut - x_1v + ut \\ &x_1x_2v + x_1x_2t - x_1ut - x_2ut - x_1v + ut \\ &y_1x_2v + y_1x_2t - x_1vt - x_2vt - y_1v + vt \\ &y_2x_1v + y_1x_2t - x_1vt - x_2vt - y_1y_2 + vt \\ &y_1y_2v + y_1y_2t - y_1vt - y_2vt \\ &x_1x_2ut + x_1x_2st - x_1ust - x_2ust - x_1x_2t + ust. \end{aligned}$$

Mas o resto de c relativamente a G é zero, o que confirma que $c \in I$, completando, assim, a demonstração do teorema.

Na próxima seção introduzimos algumas funções que tornarão mais simples a construção dos polinômios que representam as hipóteses e a conclusão dos teoremas que desejamos provar.

2. Modelando as hipóteses

Como a maior parte dos teoremas de geometria plana pode ser modelado a partir umas poucas relações padrão, precisamos apenas explicitar as equações utilizadas para modelar estas relações em termos de polinômios.

Sejam A_i pontos do plano de coordenadas (x_i, y_i), em que $1 \leq i \leq 6$. Começamos pela função para calcular o ponto médio do segmento $\overline{A_1A_2}$, que é

$$\texttt{medio}(\texttt{A}_1, \texttt{A}_2) = \left(\frac{x_1 + x_2}{2}, \frac{y_1 + y_2}{2} \right).$$

Note que esta função tem por entrada as coordenadas dos pontos extremos do segmento e por saída as coordenadas do próprio ponto médio do segmento. Ao contrário de `medio`, as demais funções *não retornam coordenadas de pontos*; elas apenas expressam relações entre vários pontos do plano que satisfazem a certas propriedades. Por exemplo, como já explicamos nas seções anteriores, os pontos A_1, A_2 e A_3 serão colineares se a inclinação das retas que passam por A_1 e A_2 e por A_1 e A_3 coincidem. Isto é, se

$$\frac{y_2 - y_1}{x_2 - x_1} = \frac{y_3 - y_1}{x_3 - x_1}.$$

Eliminando os denominadores, obtemos a identidade

$$(y_2 - y_1)(x_3 - x_1) = (y_3 - y_1)(x_2 - x_1).$$

Escrevendo

$$\texttt{colineares}(\texttt{A}_1, \texttt{A}_2, \texttt{A}_3) = (y_2 - y_1)(x_3 - x_1) - (y_3 - y_1)(x_2 - x_1),$$

podemos expressar a identidade acima na forma $\texttt{colineares}(\texttt{A}_1, \texttt{A}_2, \texttt{A}_3) = 0$. Em outras palavras,

A_1, A_2 e A_3 são colineares se, e somente se $\texttt{colineares}(\texttt{A}_1, \texttt{A}_2, \texttt{A}_3) = 0$.

A perpendicularidade entre dois segmentos pode ser expressa em termos do produto interno. Por exemplo, $\overline{A_1A_2}$ e $\overline{A_3A_4}$ são perpendiculares se, e somente se, o polinômio

$$\texttt{perp}(\texttt{A}_1, \texttt{A}_2 : \texttt{A}_3, \texttt{A}_4) = (x_1 - x_2)(x_3 - x_4) + (y_1 - y_2)(y_3 - y_4)$$

é igual a zero. Por outro lado, se o segmento $\overline{A_1A_2}$ tem k vezes o comprimento de $\overline{A_3A_4}$, então

$$\sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} = k\sqrt{(x_3 - x_4)^2 + (y_3 - y_4)^2}.$$

Elevando ambos os membros ao quadrado, verificamos que isto equivale a igualar a zero o polinômio

$$(x_1 - x_2)^2 + (y_1 - y_2)^2 - k^2((x_3 - x_4)^2 + (y_3 - y_4)^2),$$

que denotaremos por $\texttt{comprimento}(\texttt{k} : \texttt{A}_1, \texttt{A}_2 : \texttt{A}_3, \texttt{A}_4)$. Podemos usar esta relação, por exemplo, para determinar a condição para que um ponto A_3 pertença à circunferência de centro A_1 e raio $\overline{A_1A_2}$. Entretanto, como circunferências aparecem com frequência em problemas de geometria elementar, é conveniente definir uma relação especialmente para lidar com elas. Assim, usando a relação anterior, escrevemos

$$\texttt{circulo}(\texttt{A}_1, \texttt{A}_2 : \texttt{A}_3) = \texttt{comprimento}(\texttt{1} : \texttt{A}_1, \texttt{A}_2 : \texttt{A}_1, \texttt{A}_3) = 0,$$

para descrever a condição para que o ponto A_3 pertença à circunferência de centro A_1 e raio $\overline{A_1A_2}$.

Finalmente, resta-nos tratar das relações que lidam com ângulos. A primeira estabelece que o ângulo $A_1A_2A_3$ é igual ao ângulo $A_4A_5A_6$, desde que ambos sejam agudos. Para isso usamos, mais uma vez, o produto interno. Como estamos supondo que os dois ângulos são agudos, eles serão iguais se os seus cosenos forem iguais. Mas

$$\cos(A_1A_2A_3) = \frac{\overrightarrow{A_2A_1} \cdot \overrightarrow{A_2A_3}}{|\overrightarrow{A_2A_1}||\overrightarrow{A_2A_3}|},$$

em que o ponto denota a produto interno. Portanto, igualando $\cos(A_1A_2A_3)$ e $\cos(A_4A_5A_6)$, e eliminando os denominadores, obtemos

$$(\overrightarrow{A_2A_1} \cdot \overrightarrow{A_2A_3})|\overrightarrow{A_4A_5}||\overrightarrow{A_4A_6}|$$

que é igual a

$$(\overrightarrow{A_4A_5} \cdot \overrightarrow{A_4A_6})|\overrightarrow{A_2A_1}||\overrightarrow{A_2A_3}|.$$

A igualdade dos ângulos fica definida pelo anulamento da função

$$\texttt{ang}(\texttt{A}_1, \texttt{A}_2, \texttt{A}_3 : \texttt{A}_4, \texttt{A}_5, \texttt{A}_6),$$

que é o polinômio obtido substituindo as expressões analíticas para os produtos internos e módulos dos vetores em

$$(\overrightarrow{A_2A_1} \cdot \overrightarrow{A_2A_3})^2|\overrightarrow{A_4A_5}|^2|\overrightarrow{A_4A_6}|^2 - (\overrightarrow{A_4A_5} \cdot \overrightarrow{A_4A_6})^2|\overrightarrow{A_2A_1}|^2|\overrightarrow{A_2A_3}|^2.$$

Esta relação pode ser usada para definir uma reta como sendo a bissetriz de um ângulo. De fato, dizer que o ponto A_4 está na bissetriz do ângulo $A_1A_2A_3$ é o mesmo que dizer que os angulos $A_1A_2A_4$ e $A_4A_2A_3$ são iguais. Podemos expressar isto usando a relação

$$\texttt{bissetriz}(\texttt{A}_4 : \texttt{A}_1\texttt{A}_2\texttt{A}_3) = \texttt{ang}(\texttt{A}_1, \texttt{A}_2, \texttt{A}_4 : \texttt{A}_4, \texttt{A}_2, \texttt{A}_3).$$

Antes de enunciar o método de demonstração esboçado na seção 7 do capítulo 1 de maneira sistemática, precisamos considerar um exemplo que apontará para a necessidade de uma pequena generalização do método como originalmente proposto.

3. Diagonais de um paralelogramo

Nesta seção pretendemos utilizar a estratégia usual para provar o seguinte teorema.

TEOREMA DAS DIAGONAIS. *As diagonais de um paralelogramo se cruzam em seu ponto médio.*

Começamos escolhendo o sistema de eixos de modo que a origem seja um dos vértices do paralelogramo, cuja base deve estar sobre o eixo OX e ter comprimento 1. Denotando por A, B, C e D os vértices do paralelogramo em questão, temos que

$$A = (0, 0) \text{ e } B = (1, 0)$$

Além disso, se $D = (x, y)$, então x denota o afastamento horizontal de D com respeito à perpendicular; de modo que $C = (x + 1, y)$. Seja P o ponto de interseção das diagonais. Digamos que $P = (u, v)$.

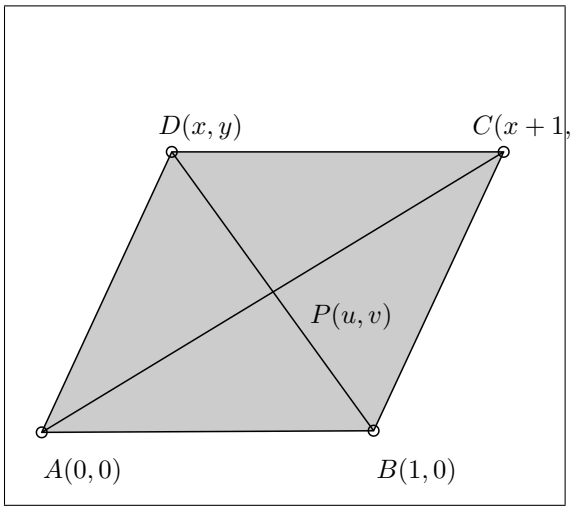


FIGURA 3. Diagonais do paralelogramo

A primeira hipótese é que P pertence à diagonal AC. Isto se traduz pela colinearidade de A, C e P que, usando a notação da seção 2, pode ser escrita como

$$h_1 = \texttt{colineares}(\texttt{A}, \texttt{P}, \texttt{C}) = v(x + 1) - uy.$$

Analogamente, o fato de P pertencer à diagonal BD se traduz por

$$h_2 = \texttt{colineares}(\texttt{B}, \texttt{D}, \texttt{P}) = v(x - 1) - y(u - 1).$$

Por outro lado, a conclusão a que queremos chegar é que P está a meio caminho entre A e C, e a meio caminho entre B e D. Em outras palavras, queremos mostrar as igualdades de segmentos $\overline{AP} = \overline{PC}$ e $\overline{BP} = \overline{PD}$.

Mas $\overline{AP}$ tem comprimento $\sqrt{u^2+v^2}$ ao passo que $\overline{PC}$ tem comprimento $\sqrt{(x+1-u)^2+(y-v)^2}$. Portanto, igualando os comprimentos de $\overline{AP}$ e $\overline{PC}$, e elevando ambos os membros da expressão resultante ao quadrado, obtemos

$$u^2+v^2=(x+1-u)^2+(y-v)^2.$$

Logo, a igualdade $\overline{AP}=\overline{PC}$ se expressa pelo anulamento do polinômio

$$c_1=(x+1-u)^2+(y-v)^2-u^2-v^2.$$

Na notação introduzida da seção 8, isto se escreve na forma

$$c_1=\texttt{comprimento}(\texttt{1}:\texttt{A},\texttt{P}:\texttt{P},\texttt{C}).$$

Analogamente, a igualdade $BP=PD$ é expressa pelo polinômio,

$$c_2=\texttt{comprimento}(\texttt{1}:\texttt{B},\texttt{P}:\texttt{P},\texttt{D})=(x-u)^2+(y-v)^2-(u-1)^2-v^2.$$

Finalmente, de acordo com nossa estratégia, construímos o ideal

$$I=\langle h_1,h_2\rangle,$$

formado pelas hipóteses do teorema e calculamos sua base de Gröbner reduzida relativamente à ordem lex, com

$$t>u>v>x>y,$$

que é

$$G=\{2v-y,2uy-xy-y\}.$$

Contudo,

$$\mathrm{R}_G(c_1)=2ux+2u-x2-2x-1,$$

que não é exatamente o que esperávamos, pois isto parece sugerir que o teorema é falso. O que poderia ter dado errado?

O primeiro pensamento que nos ocorre é que estamos testando a coisa errada. O que queremos mostrar, é que, toda vez que h_1 e h_2 se anulam em um ponto, então c também se anula. Na linguagem do capítulo 3, queremos mostrar que c_1 se anula em todos os pontos de $\mathcal{Z}(I)$. Contudo, isto não implica que $c_1\in I$, mas sim que $c_1\in\sqrt{I}$; cf. proposição 3.11 da página 88. Por sorte já sabemos como verificar isto: basta usar o algoritmo 5.9 da página 139.

Introduzindo uma nova variável t, maior que as demais, calcularemos uma base de Gröbner reduzida para o ideal

$$J=I+\langle ct-1\rangle.$$

O que esperamos obter é $\{1\}$, confirmando que alguma potência de c_1 pertence a I; mas, o que de fato acontece é que a base é igual a

$$\{y,v,2tux+2tu-tx2-2tx-t-1\}.$$

Será que o teorema é mesmo falso?

Para entender melhor o que possa estar causando o problema, tentaremos escrever alguma potência de c_1 como combinação dos elementos da base de Gröbner G de I. A esperança é que uma análise desta relação indique o que

pode estar errado em nosso argumento. Já que não sabemos que expoentes usar, digamos que

$$c_1^k \in \langle h_1, h_2 \rangle.$$

Portanto, devem existir polinômios $q_1, q_2 \in \mathbb{C}[x, y, u, v]$, com coeficientes complexos, tais que

$$c_1^k = q_1(2v - y) + q_2(2uy - xy - y).$$

Fatorando o y na segunda parcela,

$$c_1^k = q_1(2v - y) + q_2 \cdot y \cdot (2u - x - 1). \tag{53}$$

Mas uma igualdade de polinômios deve valer quaisquer que sejam os valores atribuídos às variáveis. Contudo, fazendo $y = 0$ de ambos os lados da equação (53), obtemos

$$(x - 1)^{2k} = q_1(x, 0, 0, 0) \cdot 2v,$$

que não pode ser verdade porque v não divide $x - 1$. Em particular, descobrimos que esta relação entre c_1 e a base G não pode ocorrer de forma alguma quando $y = 0$.

A próxima pergunta deve ser: que tipo de paralelogramo tem $y = 0$? A resposta é que se trata de um paralelogramo de altura zero; quer dizer, neste caso não temos paralelogramo nenhum. Se não há paralelogramo, não há diagonais bem definidas a se encontrarem em ponto algum. Portanto, não admira que a estratégia não tenha funcionado. Mas, qual a saída? A resposta é óbvia, devemos tentar impor a hipótese de que $y \neq 0$.

O problema é que, no nosso contexto, *hipótese* é o mesmo que anulamento de algum polinômio. Portanto, o que queremos é um polinômio que garanta que $y \neq 0$. Mas, se $y \neq 0$, então $1/y$ está bem definido. Tomando esta idéia por base, podemos pensar em acrescentar ao ideal I um polinômio da forma $yt - 1$, em que t é uma nova variável, que representa o inverso de y. Note que, se $yt - 1$ se anula em um ponto, então y não pode se anular neste ponto, do contrário obteríamos a contradição $0 = 1$.

Vamos tentar esta estratégia e ver o que acontece. O anel continuará sendo $\mathbb{C}[t, u, v, x, y]$, sob a ordem lexicográfica com $t > u > v > x > y$. O ideal será

$$J = \langle h_1, h_2, yt - 1 \rangle,$$

e contém $yt - 1$ apenas para impedir que y se anule. A base de Gröbner reduzida deste ideal é

$$\hat{G} = \{2v - y, 2u - x - 1, ty - 1\},$$

e desta vez $\mathrm{R}_G(c) = 0$, comprovando que o teorema é mesmo verdadeiro—desde que $y \neq 0$.

Do que foi feito podemos concluir que o problema estava na modelagem algébrica do que é, de fato, um problema geométrico. Nossa modelagem pressupôs que, para ter um paralelogramo basta dar quatro pontos, que serão os seus vértices. Mas isto *não* é verdade. Para que estes quatro pontos descrevam um paralelogramo é preciso que não sejam colineares; do contrário teremos

apenas uma reta. Dizendo de outra maneira, ao usar a palavra paralelograma estamos assumindo, implicitamente, que os vértices não podem ser colineares. Contudo esta hipótese não fazia parte da modelagem algébrica que originalmente fizemos deste problema.

Uma condição sob a qual um teorema é falso (como $y = 0$, no teorema das diagonais do paralelogramo) é chamada de *caso degenerado* do teorema. Pensando bem, é um pouco surpreendente que casos degenerados não tenham ocorrido em nenhum dos teoremas que provamos anteriormente. Afinal, já lidamos com triângulos que poderiam muito bem ter correspondido a três pontos colineares, e coisa semelhante podia ter acontecido na prova do teorema da reta de Newton-Gauss, na seção 1. A bem da verdade, só não tivemos casos degenerados naquele teorema por causa da maneira um tanto malandra com que modelamos o problema. Tente repeti-lo com um dos lados do quadrilátero ao longo do eixo x e você verá que imediatamente surgem casos degenerados.

Como veremos, casos degenerados representam a regra, e não a exceção, quando se trata de demonstrar teoremas geométricos por métodos algébricos. A vasta maioria dos teoremas de geometria elementar é falsa nestes casos, que incluem paralelogramos e triângulos de altura zero, círculos de raio zero, pontos que não podiam ser colineares, mas são, e também algumas outras situações mais insólitas, como veremos no teorema 6.7 da seção 6. Teremos muito mais a dizer sobre isto ao longo das próximas seções.

4. O método direto

O método direto, que foi discutido no capítulo 1 e utilizado nas seções anteriores, consiste em verificar que cada um dos polinômios que descrevem a conclusão do teorema pertence ao ideal gerado pelas hipóteses. Para poder enunciá-lo em mais detalhes, suponhamos que formulamos as hipóteses do teorema a ser provado na forma de equações polinomiais, obtendo o sistema

$$h_1 = \cdots = h_s = 0,$$

em que $h_1, \ldots, h_s \in \mathbb{C}[x_1, \ldots, x_n]$.

Não podemos nos esquecer que pode ser necessário eliminar casos degenerados, como vimos na seção 3. Seja como for, os valores para os quais as hipóteses são degeneradas podem ser descritos por um sistema de equações polinomiais. Digamos que, no caso que estamos considerando, este sistema seja

$$d_1 = \cdots = d_r = 0,$$

em que $d_1, \ldots, d_r$ são polinômios no anel $\mathbb{C}[x_1, \ldots, x_n]$. Finalmente, seja c o polinômio que descreve a conclusão do teorema.

Nestas circunstâncias, e usando as técnicas desenvolvidas nos capítulos anteriores e na seção 3 acima, queremos descobrir se c pertence ao ideal

$$\langle h_1, \ldots, h_s, d_1 t_1 - 1, \ldots, d_r t_r - 1 \rangle$$

do anel de polinômios $\mathbb{C}[x_1, \ldots, x_n, t_1, \ldots, t_r]$. Faremos isto usando bases de Gröbner, como descrito no seguinte algoritmo.

ALGORITMO 6.2 (Método direto). *Dados $h_1, \ldots, h_s$, $d_1, \ldots, d_r$ e c polinômios no anel $\mathbb{C}[x_1, \ldots, x_n]$, de modo que os h's determinam as hipóteses do resultado a ser provado, os d's determinam as condições de degeneração e c sua conclusão, o algoritmo retorna uma das duas afirmações seguintes: "o resultado é verdadeiro" ou "o resultado não pôde ser confirmado."*

Etapa 1: *Determine uma base de Gröbner reduzida G para o ideal gerado pelos polinômios*

$$h_1, \ldots, h_s, t_1d_1 - 1, \ldots, t_rd_r - 1$$

no anel $\mathbb{C}[x_1, \ldots, x_n, t_1, \ldots, t_r]$.

Etapa 2: *Calcule o resto $\mathrm{R}_G(c)$ da divisão de c por G. Se $\mathrm{R}_G(c) = 0$, então o resultado é verdadeiro, se $\mathrm{R}_G(c) \neq 0$, então o resultado não pôde ser confirmado.*

Na verdade, este algoritmo pode não funcionar corretamente ainda que o resultado seja verdadeiro. Isto não é nenhuma surpresa, porque provar o resultado equivale a dizer que c se anula sempre que as hipóteses se anulam (mas não as condições de não degeneração). Entretanto, como sabemos desde a seção 4 do capítulo 3, isto não quer dizer que c pertence ao ideal gerado pelas hipóteses e pela negação das condições de degeneração, mas sim que pertence ao radical deste ideal. Contudo, este algoritmo, além de muito simples, quase sempre funciona desde que sejamos capazes de detectar com precisão as condições de degeneração. Portanto, o verdadeiro problema está em identificar estas condições, que nem sempre são totalmente inocentes.

A seguir vamos aplicar o método direto para provar o teorema sobre as diagonais de um paralelogramo considerado na seção 3. Como já vimos, é necessário supor que o paralelogramo não tenha altura zero, do contrário o método não funcionará. Utilizando a estratégia delineada acima, podemos formular as hipóteses do teorema pelo anulamento dos polinômios

$$v(x+1) - uy \text{ e } v(x-1) - y(u-1).$$

Já a condição de não degeneração corresponde a dizer que $y \neq 0$. Portanto, o ideal que codifica as hipóteses do teorema, juntamente com a condição de não degeneração, é

$$\langle v(x+1) - uy, v(x-1) - y(u-1), yt - 1\rangle.$$

Calculando uma base de Gröbner reduzida para este ideal em relação à ordem lexicográfica com $t > u > v > x > y$, obtemos

$$G = \{2v - y, 2u - x - 1, yt - 1\}.$$

Finalmente, a conclusão do teorema se expressa pelos polinômios

$$c_1 = (x+1-u)^2+(y-v)^2-u^2-v^2 \text{ e } c_2 = (x-u)^2+(y-v)^2-(u-1)^2-v^2,$$

que deixam resto zero na divisão por G, confirmando assim a validade do teorema desde que o paralelogramo não tenha altura nula.

Antes de iniciar a discussão de um método mais geral, provaremos um outro teorema elementar sobre triângulos. Desta vez usaremos as funções da seção 2, para definir as hipóteses e a conclusão, e o algoritmo de Buchberger, para provar o teorema.

TEOREMA 6.3. *O produto dos dois lados de um triângulo é igual ao produto da altura sobre o terceiro lado pelo diâmetro do círculo circunscrito.*

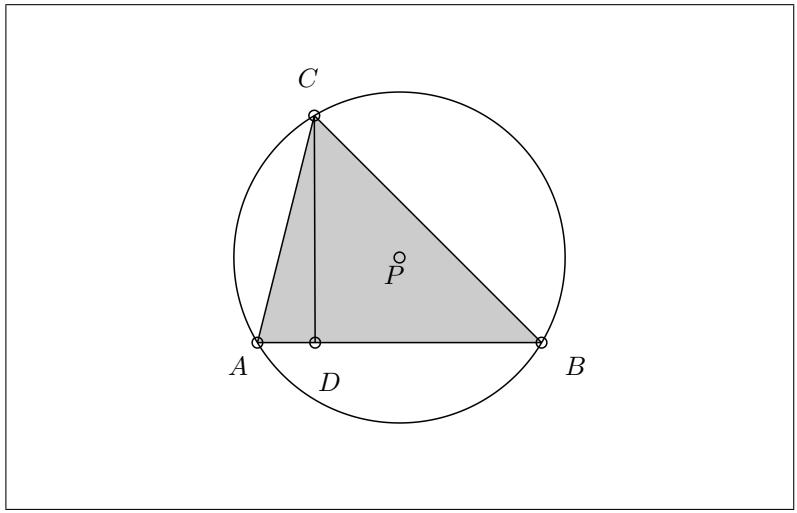


FIGURA 4. O triângulo e a circunferência

Como já fizemos anteriormente, suporemos que o triângulo tem vértices

$$A = (0,0),\ B = (1,0) \text{ e } C = (x,y).$$

As hipóteses correspondem a afirmar que o ponto $P = (u,v)$ é o centro da circunferência circunscrita, de modo que

$$h_1 = \texttt{circulo}(\texttt{A},\texttt{B}:\texttt{P})$$
$$h_2 = \texttt{circulo}(\texttt{A},\texttt{C}:\texttt{P}).$$

Efetuando os cálculos, obtemos

$$h_1 = (u-1)^2 + v^2 - (u^2+v^2);$$
$$h_2 = (u-x)^2 + (v-y)^2 - (u^2+v^2).$$

Como queremos mostrar que

$$\sqrt{x^2+y^2}\sqrt{(x-1)^2+y^2} = 2y\sqrt{u^2+v^2},$$

temos que a conclusão é dada pelo polinômio,

$$c = (x^2 + y^2)((x-1)^2 + y^2) - 4y^2(u^2 + v^2).$$

Aplicando o algoritmo de Buchberger a este ideal em relação à ordem lexicográfica com $x > y > u > v$, obtemos a base de Gröbner

$$G = \{x^2 - x + y^2 - 2yv, u - 1/2\}.$$

Um cálculo simples mostra que $\mathrm{R}_G(c) = 0$, de modo que o teorema vale sem nenhuma hipótese de não degeneração.

5. O método refutacional

É hora de enfrentar as dificuldades que surgem quando a conclusão não pertence ao ideal das hipóteses, mas mesmo assim o teorema é verdadeiro. Suporemos, como na seção 1, que as hipóteses do teorema são descritas por $h_1, \ldots, h_s \in \mathbb{C}[x_1, \ldots, x_n]$, ao passo que as condições de degeneração são dadas pelos polinômios $d_1, \ldots, d_r$ do mesmo anel.

Para mostrar que a conclusão do teorema é verdadeira sob as hipóteses dadas, *quando não estamos em um caso degenerado*, precisamos verificar que $c \in \mathbb{C}[x_1, \ldots, x_n]$ que descreve a conclusão do teorema, se anula em todo ponto $p \in \mathbb{C}^n$ para o qual

$$h_1(p) = 0, \ldots, h_s(p) = 0, \text{ mas } d_1(p) \neq 0, \ldots d_r(p) \neq 0.$$

Apelando para a proposição 3.11 da página 88, isto significa que devemos mostrar que alguma potência de c pertence ao ideal

$$\langle h_1, \ldots, h_s, d_1t_1 - 1, \ldots, d_rt_r - 1\rangle$$

do anel de polinômios $\mathbb{C}[x_1, \ldots, x_n, t_1, \ldots, t_r]$. Por sorte, o algoritmo 5.9 da página 139 nos dá uma maneira explícita de fazer isto. Utilizando este algoritmo, e continuando a usar a notação do começo da seção, vemos que

> o teorema é verdadeiro sob as hipóteses de degeneração dadas se, e somente se, a base de Gröbner reduzida do ideal
>
> $$I = \langle h_1, \ldots, h_s, d_1t_1 - 1, \ldots, d_rt_r - 1, cz - 1\rangle$$
>
> no anel $\mathbb{C}[x_1, \ldots, x_n, t_1, \ldots, t_r, z]$ é $\{1\}$.

Desta vez nosso resultado é inteiramente geral, ao contrário do que acontecia no método direto.

Convém parar um momento para entender o que acabamos de fazer de maneira mais heurística. Para começar, podemos pensar nos polinômios $d_jt_j - 1$ como sendo parte das hipóteses, se entendidas em sentido lato – isto é, como tudo aquilo que tem que ocorrer para que o teorema possa ser verdadeiro. Considerados sobre este ponto de vista, os polinômios do ideal I consistem nas hipóteses

$$h_1, \ldots, h_s, d_1t_1 - 1, \ldots, d_rt_r - 1$$

e na conclusão c. Entretanto, c aparece em I como parte do polinômio $cz - 1$, que é uma maneira algébrica de dizer que c não pode se anular nos pontos

onde as hipóteses se anulam. Em outras palavras, criamos um ideal que contém as hipóteses e a *negação da conclusão*. Esta é a técnica de demonstração conhecida como redução ao absurdo, ou demonstração por contradição. Portanto, o que esperamos obter ao final dos cálculos é uma contradição que, neste caso, consiste em dizer que o teorema nunca é verdadeiro; ou, de maneira mais algébrica, que o ideal I não tem zeros.

Infelizmente, ainda continuamos com um problema substancial: para aplicar esta estratégia precisamos determinar *a priori* as possíveis condições de degeneração do teorema. Como já observamos antes, estas condições nem sempre são de todo inocentes, e determiná-las pode ser mais que um problema de excluir círculos sem raio ou triângulos sem altura.

Entretanto, a análise heurística que fizemos acima sugere uma maneira sistemática que pode ser usada para determinar automaticamente as condições de degeneração. Voltando ao ideal I, digamos que seja gerado apenas pelas hipóteses e pela negação da conclusão. Imagine, agora, que $I \neq \{1\}$. Isto significa que *não* chegamos a uma contradição. Em outras palavras, há pontos nos quais as hipóteses valem, mas a conclusão é falsa – pontos de degeneração. Além disso, estes pontos são exatamente aqueles que estão em $\mathcal{Z}(I)$. Mas isto significa que, em geral, I representa as condições de degeneração: $I = \{1\}$ apenas nos diz que tais condições não existem.

Vejamos como sistematizar estas idéias. Utilizando, mais uma vez, a notação do começo da seção, vamos calcular uma base de Gröbner reduzida G para o ideal

$$I = \langle h_1, \ldots, h_s, cz - 1 \rangle,$$

deixando de fora as condições de degeneração. Segue da discussão acima que a base de Gröbner reduzida G de I deve conter os polinômios que descrevem as condições de degeneração. Contudo, há um detalhe do qual não podemos nos descuidar. As condições de degeneração devem corresponder a polinômios nas variáveis $x_1, \ldots, x_n$, que são as variáveis usadas para descrever as hipóteses e a conclusão do teorema. Dizendo de outra maneira, os polinômios que descrevem os casos degenerados não podem incluir a variável z, que é apenas uma variável auxiliar usada no cálculo da base de Gröbner. Portanto, as condições de degeneração serão apenas aqueles que pertencem ao ideal $I \cap \mathbb{C}[x_1, \ldots, x_n]$. Mas como calcular esta interseção? Por sorte já desenvolvemos toda a tecnologia necessária para isto, como mostra a proposição.

PROPOSIÇÃO 6.4. *Seja J um ideal do anel $K[x_1, \ldots, x_m, y_1, \ldots y_n]$. Se G é uma base de Gröbner de J com respeito à ordem lexicográfica com $y_1 < \cdots y_n < x_1 < \cdots < x_m$, então $G \cap K[y_1, \ldots, y_n]$ é uma base de Gröbner do ideal $J \cap K[y_1, \ldots, y_n]$.*

DEMONSTRAÇÃO. Seja $f \in J \cap K[y_1, \ldots, y_n]$. Pela definição de base de Gröbner, basta mostrar que $\mathrm{in}(f)$ é divisível por $\mathrm{in}(g)$ para algum $g \in G \cap K[x_1, \ldots, x_n]$. Entretanto, como G é uma base de Gröbner de J, existe $g \in G$ tal que $\mathrm{in}(g)$ divide $\mathrm{in}(f)$. Só precisamos mostrar que $g \in K[y_1, \ldots, y_n]$. Contudo, como $\mathrm{in}(f) \in K[y_1, \ldots, y_n]$, o mesmo vale para $\mathrm{in}(g)$. Mas se o

termo inicial de g não contém nenhum z, então nenhum termo de g contém x, porque estamos operando sob a ordem lexicográfica em que cada y é menor que todos os x. Logo, $g \in K[y_1, \ldots, y_n]$, e a demonstração está completa. □

Portanto, trata-se apenas de calcular uma base de Gröbner. O único problema é que é necessário que a ordem monomial escolhida seja a lexicográrfica. Como os cálculos com esta ordem podem ser muito lentos, implementá-los em alguns casos pode ser um sério problema.

Chamamos ao método de demonstração que resulta desta estratégia de *método refutacional*, porque busca as condições sob as quais o teorema é falso. Antes de enunciar o método refutacional sob a forma de um algoritmo, analisaremos os dois casos extremos. Em outras palavras, queremos determinar o que acontece quando o sistema

$$h_1 = \cdots = h_s = cz - 1 = 0,$$

não tem solução, e também quando todo ponto de $\mathbb{C}^{n+1}$ é solução deste sistema. Em primeiro lugar, se o sistema não tem solução, então a equação $c(p)z - 1 = 0$ não tem solução para nenhum ponto $p \in \mathcal{Z}(h_1, \ldots, h_s)$. Mas isto só acontece se c for zero em todo ponto de $\mathcal{Z}(h_1, \ldots, h_s)$. Portanto, a conclusão é universalmente válida neste caso. Por outro lado, se todo ponto de $\mathbb{C}^{n+1}$ é solução do sistema, então c nunca se anula em nenhum ponto de $\mathcal{Z}(h_1, \ldots, h_s)$. Mas isto significa que a conclusão do teorema nunca segue das hipóteses; isto é, o teorema é falso.

ALGORITMO 6.5 (Método refutacional). *Dados polinômios $h_1, \ldots, h_s$ e c em $\mathbb{Q}[x_1, \ldots, x_n]$, em que os hs descrevem as hipóteses, e c a conclusão, do resultado a ser provado, o algoritmo retorna uma das quatro afirmações seguintes:*

- *o resultado é universalmente verdadeiro; ou*
- *o resultado é falso, ou*
- *o resultado é verdadeiro desde que $d \neq 0$, em que $d \in \mathbb{Q}[x_1, \ldots, x_n]$; ou*
- *o resultado não pôde ser confirmado.*

Etapa 1: *Determine uma base de Gröbner reduzida G para o ideal gerado pelos polinômios*

$$h_1, \ldots, h_s, zc - 1,$$

no anel $\mathbb{Q}[x_1, \ldots, x_n, z]$ com respeito à ordem lexicográfica com $x_1 < \cdots < x_n < z$.

Etapa 2: *Se $G = \{1\}$ então o resultado é universalmente verdadeiro e se $G = \{0\}$ o resultado é falso.*

Etapa 3: *Se $G \neq \{0\}, \{1\}$, então para cada $d \in G \cap \mathbb{Q}[x_1, \ldots, x_n]$ que não coincide com um dos hs dados na hipótese:*

verifique se a base de Gröbner reduzida para o ideal

$$\langle h_1, \ldots, h_s, dt - 1 \rangle$$

(sob qualquer ordem monomial) é igual a 1. *Se isto não acontecer, então o resultado é verdadeiro desde que* $d \neq 0$*, e o algoritmo pára.*

Se a condição acima não for verificada para nenhum dos d*s, então o resultado não pôde ser confirmado, e o algoritmo pára.*

Você deve ter notado que a terceira etapa descreve uma parte do procedimento que não havia surgido na discussão anterior. Na verdade, esta etapa tem por função excluir polinômios da base que sejam apenas combinação de $h_1, \ldots, h_s$. Polinômios deste tipo podem surgir no cálculo da base de Gröbner, mas não correspondem a nenhum caso degenerado, já que as condições que impõem são meras consequências das hipóteses.

Vejamos o que acontece se aplicamos o método refutacional a um exemplo que já cohecemos bem, o teorema das diagonais de um paralelogramo. As hipóteses correspondem aos polinômios

$$h_1 = 2v - y \text{ e } \ h_2 = 2u - x - 1,$$

e a conclusão aos polinômios

$$c_1 = (x + 1 - u)^2 + (y - v)^2 - u^2 - v^2 \text{ e}$$
$$c_2 = (x - u)^2 + (y - v)^2 - (u - 1)^2 - v^2.$$

Aplicaremos o método refutacional a uma conclusão de cada vez. Para a conclusão c_1, calculamos a base de Gröbner reduzida do ideal $\langle h_1, h_2, c_1 z - 1\rangle$, obtendo

$$\{y, v, 2zxu + 2zu - zx^2 - 2zx - z + 1\}.$$

Os dois primeiros elementos desta base não contêm a variável z e, portanto, podem corresponder a casos degenerados. Mas tanto $y = 0$ quanto $v = 0$ implicam que o paralelogramo tem altura nula. Recobramos assim as condições que já conhecíamos.

Calculando agora a base de Gröbner reduzida para o ideal $\langle h_1, h_2, c_2 z - 1\rangle$, obtemos $\{y, v, 2zxu - 2zu - zx^2 + z + 1\}$, o que nos dá os mesmos casos degenerados já obtidos.

6. Mais exemplos

O primeiro teorema que queremos provar, nesta seção, usando o método refutacional, é o seguinte.

TEOREMA 6.6. *Sejam* A*,* B *e* C *três pontos do plano,* D *o ponto médio de* $\overline{AB}$ *e* E *o ponto médio de* $\overline{CD}$*. A reta* AE *interseta* BC *em um ponto* F *de modo que* $\overline{FB}$ *está para* $\overline{FC}$ *na razão de dois para um.*

Como sempre escolheremos A como sendo a origem do sistema de eixos e AB como estando ao longo do eixo OX, com a escala escolhida de modo que $B = (1, 0)$. Escrevendo $C = (x, y)$ temos que $D = (1/2, 0)$ é o ponto médio

de $\overline{AB}$. Portanto, o ponto médio de $\overline{CD}$ será

$$E = \left(\frac{2x+1}{4}, \frac{y}{2}\right).$$

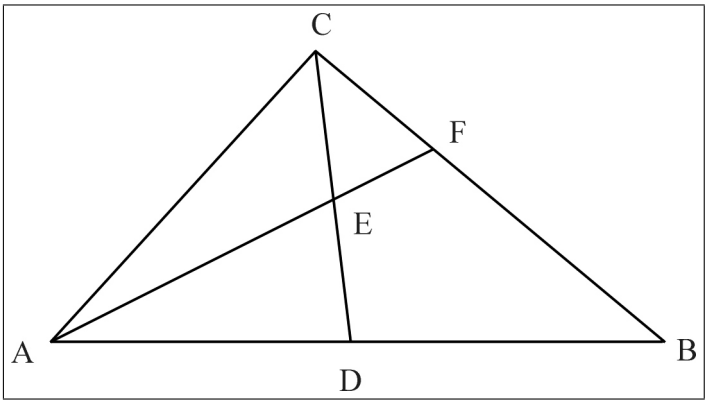


FIGURA 5. Teorema 3

Por outro lado, o ponto F pertence às retas AE e CB. Escrevendo $F = (u, v)$, estas condições se traduzem na forma

$$h_1 = \texttt{colinear}(\texttt{A}, \texttt{E}, \texttt{F}) = 0$$
$$h_2 = \texttt{colinear}(\texttt{C}, \texttt{F}, \texttt{B}) = 0.$$

Estas equações são dadas, explicitamente, por

$$h_1 = v(2x+1) - 2yu \text{ e}$$
$$h_2 = v(x-1) - y(u-1).$$

Já a conclusão pode ser escrita na forma

$$c = \texttt{comprimento}(\texttt{2} : \texttt{B}, \texttt{F} : \texttt{C}, \texttt{F}),$$

donde

$$c = (u-1)^2 + v^2 - 4((u-x)^2 + (v-y)^2)$$

Um cálculo rápido, usando bases de Gröbner, mostra que nenhuma potência de c pertence ao ideal $\langle h_1, h_2 \rangle$. Para aplicar o método refutacional, construímos o ideal $\langle h_1, h_2, c_1 z - 1 \rangle$ no anel $\mathbb{C}[x, y, u, v, z]$. Calculando sua base de Gröbner reduzida para a ordem lexicográfica com $x < y < u < v < z$, obtemos

$$G = \{y, 4zx^2 - 8zux + 3zu^2 + 2zu - z + 1, v\};$$

de modo que as condições de degeneração são

$$G \cap \mathbb{C}[x, y, u, v] = \{y, v\}.$$

Como v é uma das coordenadas do ponto F, ao qual se refere a conclusão do teorema, vamos considerar apenas a condição de degeneração $y = 0$. Calculando a base de Gröbner do ideal

$$\langle h_1, h_2, ty - 1\rangle$$

obtemos G mais uma vez. Portanto, $y = 0$ é uma condição de degeneração para este problema. Geometricamente, isto significa que o teorema é falso se o triângulo tiver altura zero.

Em todos os casos que vimos até agora, as condições de degeneração são bastante simples. Mas isto nem sempre ocorre, como mostra este segundo exemplo.

TEOREMA 6.7. *A reta que une os pontos médios das diagonais de um trapézio bissecta os lados que não são paralelos.*

Seja $ABCD$ o trapézio. Vamos escolher as coordenadas de modo que A seja a origem,

$$B = (1, 0), C = (x_2, y) \text{ e } D = (x_1, y).$$

Se E for o ponto médio da diagonal $\overline{AC}$ e F o ponto médio de $\overline{BD}$, então

$$E = (\frac{x_2}{2}, \frac{y}{2}) \text{ e } F = (\frac{x_1 + 1}{2}, \frac{y}{2}).$$

Queremos mostrar que a reta que passa por E e F corta o lado $\overline{AD}$ em $M = (x_1/2, y/2)$, que é o ponto médio de $\overline{AD}$.

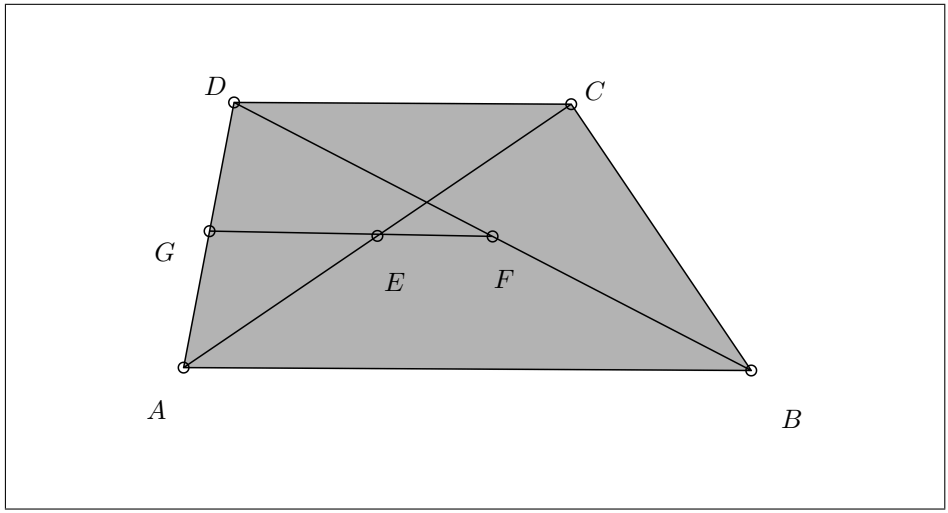


FIGURA 6. Teorema 4

Se você vem prestando atenção às coordenadas que calculamos para os pontos E, F e M, então deve ter notado que estes três ponto têm a mesma

ordenada. Mas isto é suficiente para provar o teorema, de modo que não foi preciso calcular nenhuma base de Gröbner! Apesar disso, vamos formular o problema na forma de equações e tentar resolvê-lo usando o método refutacional, porque esta resolução guarda uma surpresa interessante.

Chamando de $G = (u, v)$ o ponto em que a reta EF interseta o lado $\overline{AD}$, temos as seguintes equações

$$h_1 = \texttt{colinear}(\texttt{G}, \texttt{E}, \texttt{F}) = (2v - y)(2u - x_1 - 1) - (2v - y)(2u - x_2)$$
$$h_2 = \texttt{colinear}(\texttt{G}, \texttt{E}, \texttt{F}) = vx_1 - uy.$$

Queremos usá-las para mostrar que $G = M$. Portanto a conclusão é dada por

$$c_1 = u - x_1/2 \text{ e } \ c_2 = v - y/2.$$

Aplicaremos o método refutacional à conclusão c_1. Calculando uma base de Gröbner para o ideal

$$\langle h_1, h_2, c_1 z - 1 \rangle$$

do anel $\mathbb{C}[x_1, x_2, y, u, v, z]$, obtemos

$$H = \{y_1x_1 - y_1x_2 + y_1, vx_1 - vx_2 + v, y_1u - vx_2 + v,$$
$$- y_1 - 2zv + zy_1 + 2zvx_2 - zy_1x_2, 2zu - zx_1 - 1\}.$$

Os casos degenerados são dados pelos elementos de H que não contêm a variável z, que são

$$g_1 = y_1x_1 - y_1x_2 + y_1,$$
$$g_2 = vx_1 - vx_2 + v \text{ e}$$
$$g_3 = y_1u - vx_2 + v.$$

Em primeiro lugar é surpreendente que haja algum caso degenerado, afinal havíamos decidido que a conclusão do teorema seguia imediatamente da maneira como o formulamos. Isto pode nos levar a suspeitar que g_1, g_2 e g_3 sejam dependentes de h_1 e h_2, mas um cálculo com bases de Gröbner (a terceira etapa do método refutacional) mostra que esta suspeita não tem fundamento. Resta-nos, apenas, tentar descobrir o significado geométrico desses supostos casos degenerados. Por exemplo, se

$$g_1 = y_1(x_1 - x_2 + 1) = 0$$

então $y_1 = 0$, ou $x_1 - x_2 + 1$. Mas $y_1 = 0$ só acontece se o trapézio tem altura zero. Por outro lado, $x_2 = x_1 + 1$ significa que o trapézio é um paralelogramo. Neste caso as diagonais se encontram em seu ponto médio, o que significa que $E = F$. Portanto, a reta por E e F não está bem definida quando o trapézio é um paralelogramo. Vemos que, de fato, o teorema não se aplica neste caso. Assim, o enunciado deveria ter excluído o caso do trapézio ser um paralelogramo. Os outros dois casos degenerados são análogos a este, e deixaremos a análise detalhada por sua conta.

7. O teorema de Desargues

Nesta seção estudamos um teorema devido a Gérard Desargues (1591-1661), que foi um dos pais fundadores da geometria projetiva. Apesar de estar enunciado em termos de triângulos, este teorema trata da noção de perspectividade e, portanto, está relacionado à geometria projetiva. Teremos mais a dizer sobre isto quando tratarmos dos casos degenerados deste teorema.

TEOREMA DE DESARGUES. *Sejam ABC e $A'B'C'$ dois triângulos cujos lados correspondentes são paralelos, então as retas AA', BB' e CC' se cortam em um mesmo ponto.*

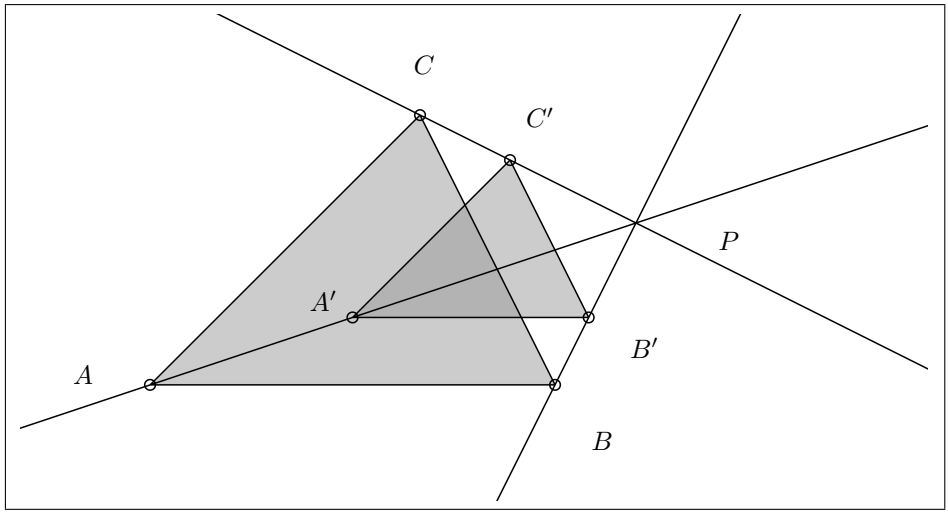


FIGURA 7. Teorema de Desargues

Como vimos no capítulo 1, sempre podemos supor que um dos triângulos tem um lado de comprimento um que está ao longo do eixo x. Suponhamos que este é o caso para o triângulo ABC. Isto significa que podemos escrever

$$A = (0,0) \quad \text{e} \quad B = (1,0)$$

e, como $A'B'$ é paralelo a AB,

$$A' = (u_1, v) \quad \text{e} \quad B' = (u_2, v).$$

Como nada sabemos a respeito de C e C', designaremos suas coordenadas utilizando novas variáveis,

$$C = (x_1, y_1) \quad \text{e} \quad C' = (x_2, y_2).$$

Por outro lado, para que AC seja paralelo a $A'C'$, devemos ter

$$\frac{y_2 - v}{x_2 - u_1} = \frac{y_1}{x_1};$$

que também pode ser expresso pelo anulamento do polinômio

$$h_1 = x_1(y_2 - v) - y_1(x_2 - u_1).$$

Analogamente, afirmar que BC é paralelo a $B'C'$ equivale ao anulamento do polinômio

$$h_2 = (x_1 - 1)(y_2 - v) - y_1(x_2 - u_2).$$

Em seguida precisamos determinar o ponto P que pertence à interseção das retas AA' e BB'. Se (w_1, w_2) são as coordenadas de P, então P está na reta AA' se

$$\frac{w_2}{w_1} = \frac{v}{u_1};$$

que corresponde ao anulamento do polinômio

$$h_3 = w_2u_1 - w_1v.$$

Analogamente, dizer que P pertence a BB' equivale ao anulamento do polinômio

$$h_4 = w_2(u_2 - 1) - v(w_1 - 1)$$

A conclusão desejada corresponde a afirmar que P pertence a CC', que corresponde ao anulamento do polinômio

$$c = (w_2 - y_1)(x_2 - x_1) - (w_1 - x_1)(y_2 - y_1).$$

Para aplicar o método refutacional, devemos considerar o ideal

$$I = \langle h_1, h_2, h_3, cz - 1\rangle;$$

cuja base de Gröbner reduzida, relativamente à ordem lexicográfica com

$$z_1 > w_1 > w_2 > x_1 > x_2 > y_1 > y_2 > u_1 > u_2 > v$$

tem 16 elementos. Destes, apenas quatro contêm somente as variáveis x_1, x_2, y_1, y_2, u_1, u_2 e v, e podem representar condições de degeneração. O primeiro dos quatro é

$$y_2v - v^2 = v(y_2 - v).$$

Isto sugere que precisamos supor que $v \neq 0$ e que $y_2 \neq v$. De fato, $y_2 = v$ implicaria que o triângulo $A'B'C'$ tem altura zero, o que não é aceitável. A condição $v = 0$ é mais sutil. Se ocorresse, teríamos os dois triângulos situados sobre uma mesma base. Isto faria com que as retas AA' e BB' coincidissem, e que CC' fosse paralela a $AA' = BB'$; de modo que o teorema seria falso neste caso.

O segundo candidato a condição de degeneração é o polinômio

$$y_1v,$$

segundo o qual y_1 também deve ser não nulo. Em outras palavras, o triângulo ABC também não pode ser degenerado. As outras duas condições de degeneração são dadas pelos polinômios

$$y_1u_1 - y_1u_2 + y_2 - v \quad \text{e} \quad x_1y_2 - x_1v - x_2y_1 + y_1u_2 - y_2 + v,$$

e parecem mais difíceis de analisar. Por isso, processaremos o ideal I mais uma vez, desta vez anexando as condições de degeneração já obtidas. Portanto, o novo ideal será

$$J = I + \langle y_1 t_1 - 1, y_2 t_2 - 1, v t_3 - 1 \rangle,$$

e as variáveis t serão declaradas como maiores que todas as outras que apareceram até aqui. Calculando a base de Gröbner reduzida de J relativamente à ordem lexicográfica, obtemos $\{1\}$. Portanto, as condições de não degeneração já obtidas bastam para garantir que o teorema é verdadeiro.

Observe que, das três condições de não degeneração que precisamos acrescentar, apenas duas significam que os triângulos não podem ser degenerados. Sobre estas nada há que falar, uma vez que este tipo de hipótese está sempre implícito quando se enuncia um teorema de geometria euclidiana. Já a outra condição é mais interessante. De fato, como vimos, se os dois triângulos têm, cada um, um lado situado sobre uma mesma reta, então o teorema é falso. Assim, seria mais correto enunciar o teorema da seguinte maneira:

> Sejam ABC e $A'B'C'$ dois triângulos cujos lados correspondentes são paralelos. Se estes triângulos não têm nenhum lado sob uma mesma reta suporte, então as retas AA', BB' e CC' se cortam em um mesmo ponto.

É justamente neste ponto que aparece a relação entre o Teorema de Desargues e a geometria projetiva. Podemos dizer que, heuristicamente, a geometria projetiva é aquela em que retas paralelas *de fato* se "cruzam no infinito". Para que isto ocorra é necessário acrescentar ao plano usual uma nova reta, formada por "pontos no infinito", onde as retas paralelas vão se cortar. Os detalhes de como isto é feito podem ser encontrados, por exemplo, em [**39**, capítulo 4, p. 44]. O fato é que, se $AA' = BB'$ nos triângulos ABC e $A'B'C'$, então CC' é paralelo à reta $AA' = BB'$ e, portanto, estas duas têm um ponto comum "no infinito". Com esta interpretação, o teorema vale mesmo neste suposto caso degenerado.

8. Descobrindo novos teoremas

Na seção 5, descobrimos como proceder para obter condições que precisavam ser excluídas, para que um dado teorema fosse verdadeiro. Nesta seção, faremos exatamente o oposto: procuraremos condições que devem ser acrescentadas para que uma dada afirmação se torne verdadeira e passe a constituir um teorema.

Começamos com um exemplo muito simples, para o qual não há necessidade de utilizar um sistema de computação algébrica na hora de fazer as contas.

PROBLEMA 6.8. *Quais os paralelogramos cujas diagonais se cortam em ângulo reto?*

Como de costume escolheremos o sistema de coordenadas de modo que o paralelogramo tenha um de seus vértices na origem e um dos lados com extremidade neste vértice se estenda ao longo do eixo x. Além disso, a escala dos

eixos pode ser ajustada de maneira que este lado tenha comprimento unitário. Com isto, as coordenadas dos vértices do paralelogramo serão

$$A = (0, 0), \quad B = (1, 0), \quad C = (x + 1, y) \quad \text{e} \quad D = (x, y).$$

Assim, as diagonais serão perpendiculares se, e somente se, os vetores $\overrightarrow{AC}$ e $\overrightarrow{BD}$ forem perpendiculares. Contudo,

$$\overrightarrow{AC} = (x + 1, y), \quad \text{ao passo que} \quad \overrightarrow{BD} = (x - 1, y).$$

Mas estes dois vetores serão perpendiculares se seu produto interno for nulo, o que nos dá

$$0 = \overrightarrow{AC} \cdot \overrightarrow{BD} = (x + 1)(x - 1) + y^2.$$

Disto concluímos que

$$x^2 + y^2 - 1 = 0;$$

isto é, o lado AD do paralelogramo também tem comprimento um. Naturalmente isto significa que os quatro lados do paralelogramo têm que ter o mesmo comprimento. Note que isto não significa que a figura tem que ser um quadrado! Disto concluímos o seguinte teorema.

TEOREMA 6.9. *Se os comprimentos dos quatro lados um paralelogramo são iguais então suas diagonais se cruzam em um ângulo reto.*

Este foi bastante fácil. Vejamos um outro problema, mais difícil de modelar, de resolver e, sobretudo, de interpretar geometricamente a condição obtida a partir da base de Gröbner.

PROBLEMA 6.10. *Seja ABC um triângulo e P um ponto do plano. Que condição P deve satisfazer para que os pés das perpendiculares de P aos lados de ABC (ou seus prolongamentos) sejam colineares?*

Como sempre modelamos o triângulo como tendo vértices

$$A = (0, 0), \quad B = (1, 0) \quad \text{e} \quad C = (x, y).$$

Seja $P = (u, v)$. Nesta caso, o pé da perpendicular sobre o lado AB é $Q_{AB} = (u, 0)$. Os pés das outras duas perpendiculares são mais difíceis de determinar. Por exemplo, se $Q_{AC} = (s, t)$ é o pé da perpendicular sobre AC, então Q_{AC} pertence à reta que é suporte de AC, de modo que

$$\frac{t}{s} = \frac{y}{x}.$$

Assim, nossa primeira hipótese corresponde ao anulamento do polinômio

$$h_1 = xt - sy.$$

Por outro lado, Q_{AC} também está sobre a perpendicular a AC por P. Isto é, os vetores $\overrightarrow{PQ_{AC}}$ e $\overrightarrow{AQ_{AC}}$ são perpendicular. Logo,

$$h_2 = (s - u, t - v) \cdot (x, y) = x(s - u) + y(t - v).$$

Procedendo de maneira análoga relativamente a $Q_{BC} = (w, z)$, obtemos duas novas hipóteses, definidas pelos polinômios

$$h_3 = z(x-1) - y(w-1) \quad \text{e} \quad h_4 = (x-1)(u-w) + y(v-z).$$

A conclusão que desejamos obter é que os pontos Q_{AB}, Q_{AC} e Q_{BC} estejam sobre uma mesma reta, que é equivalente ao anulamento de

$$c = z(s-u) - t(w-v).$$

Desta vez queremos descobrir as condições extra que devem ser atribuídas a $P = (u, v)$ para que $c = 0$ sempre que os hs se anulem. Por isso, construímos o ideal I que contém as hipóteses e também a conclusão – ao contrário do método refutacional, em que introduzimos a *negação da conclusão*. Assim,

$$I = \langle h_1, h_2, h_3, h_4, c\rangle.$$

Como as condições referem-se a P, as variávies u e v serão as menores, seguidas por x e y, uma vez que estas últimas determinam o triângulo ABC. As demais variáveis são secundárias e podem ser ordenadas de qualquer maneira. Digamos que escolhemos

$$u < v < x < y < s < t < w < z.$$

A base de Gröbner reduzida de I relativamente à ordem lexicográfica, com esta ordenação das variáveis, tem 21 elementos, dos quais somente

$$y^4v - y^3v^2 - y^3u^2 + y^3u + y^2x^2v - y^2xv$$

pertence a $\mathbb{C}[u, v, x, y]$. Desta forma, a única condição extra com a qual devemos lidar é

$$y^4v - y^3v^2 - y^3u^2 + y^3u + y^2x^2v - y^2xv = 0.$$

Como ABC não pode ter altura zero, podemos assumir que $y \neq 0$ e cancelá-lo da equação acima, obtendo

$$y^2v - yv^2 - yu^2 + yu + x^2v - xv = 0.$$

Completando, agora, os quadrados em u e v,

$$-y\left(u - \frac{1}{2}\right)^2 + \frac{y}{4} - y\left(v + \frac{(x - x^2 - y^2)}{2y}\right)^2 + \frac{(x - x^2 - y^2)^2}{4y} = 0;$$

donde

$$y\left(u - \frac{1}{2}\right)^2 + y\left(v + \frac{(x - x^2 - y^2)}{2y}\right)^2 = \frac{y}{4} + \frac{(x - x^2 - y^2)^2}{4y}.$$

Para descobrir o que esta equação representa, podemos considerar que se trata de um triângulo ABC especificado. Assim, os valores de x e y podem ser encarados como fixos. Sob este ponto de vista, temos uma equação nas variáveis u e v, com coeficientes em $\mathbb{C}(x, y)$. Mas, encarada desta maneira, esta última equação representa uma circunferência de raio

$$\sqrt{\frac{y}{4} + \frac{(x - x^2 - y^2)^2}{4y}}$$

e centro no ponto

$$S = \left(\frac{1}{2}, -\frac{(x - x^2 - y^2)}{2y}\right).$$

Logo, a colinearidade dos pés das perpendiculares ocorre sempre que P pertença a esta circunferência.

Podíamos parar aqui, mas é difícil evitar a impressão de que esta deveria ser alguma circunferência especial. Levando esta impressão a sério, notamos imediatamente que o centro S da circunferência pertence à perpendicular pelo meio do lado AB, já que tem abscissa $1/2$. Recordando a geometria básica, lembramos que o centro da circunferência circunscrita ao triângulo pertence à perpendicular pelo centro de cada lado. Para comprovar este palpite basta verificar se S também pertence à perpendicular pelo meio de AC. Como o ponto médio de AC é

$$M = \left(\frac{x}{2}, \frac{y}{2}\right),$$

precisamos verificar se $\overrightarrow{SM}$ é perpendicular a $\overrightarrow{AB} = (x, y)$. Contudo,

$$\overrightarrow{SM} = \left(\frac{1 - x}{2}, -\frac{(x - x^2)}{2y}\right),$$

de forma que

$$\overrightarrow{SM} \cdot \overrightarrow{AB} = 0,$$

como esperávamos comprovar. Com isto podemos enunciar o teorema que acabamos de descobrir.

TEOREMA 6.11. *Seja ABC um triângulo e P um ponto de sua circunferência circunscrita. Os pés das perpendiculares de P aos lados de ABC (ou seus prolongamentos) são colineares.*

Este resultado é conhecido como *teorema de Simson*, em homenagem do matemático Robert Simson (1687-1768), que foi professor de matemática na Universidade de Glasgow (Escócia). Curiosamente, o teorema não foi provado por Simson, mas sim por William Wallace (1768-1843), que foi professor de matemática na Universidade de Edinburgo entre 1819 e 1838. Wallace não foi sequer contemporâneo de Simson. O teorema, que foi publicado por Wallace em 1799, acabou levando o nome de Simson porque Poncelet em seu livro *Propriétés Projectives* diz que o teorema havia sido atribuído a Simson em um artigo publicado no *Annales de Gergonne*.

A esta altura, você pode estar se perguntando qual seria mesmo a diferença entre o que fizemos nesta seção e o método refutacional. Dar uma resposta formal é fácil. No método refutacional, acrescentamos ao ideal das hipóteses a negação da conclusão; aqui, foi a própria conclusão que foi acrescentada. Usando uma linguagem mais heurística, poderíamos dizer que, no método refutacional, procuramos as condições sob as quais o teorema é falso; aqui, buscamos aquelas sob as quais é verdadeiro. No primeiro caso as condições obtidas devem ser excluídas das hipóteses do teorema; no segundo caso, devem ser acrescentadas.

Dita, assim, a coisa pode parecer ainda mais estranha, afinal de contas, excluir uma condição não é o mesmo que incluir sua negação?

Para sair deste impasse devemos lembrar que a palavra condição tem, aqui, um significado muito restrito, já que é uma abreviação da expressão *condição de anulamento de um ou mais polinômios*. Portanto, o que incluímos ou excluímos é sempre a *possibilidade de um dado polinômio se anular*. A questão é que um polinômio se anula em muito poucos pontos, em comparação com os pontos onde não se anula. Portanto, ao excluir condições de degeneração, estamos excluindo apenas uns poucos pontos onde o teorema não vale. Por outro lado, ao incluir uma condição necessária para que o teorema seja verdadeiro, estamos restringindo drasticamente os objetos aos quais o teorema se aplica.

9. Engrenagens articuladas

Inspirados, mais uma vez, na *Geometria* de Descartes, onde desempenham importante papel, discutiremos nesta seção o comportamento de algumas engrenagens articuladas. Tais engrenagens já foram um objeto de estudo muito popular entre engenheiros e matemáticos, sobretudo durante a Revolução Industrial. Recentemente o tema voltou à moda por sua utilização em robôs, sobretudo autômatos paralelos como os que movem plataformas de simulação de voo e de simuladores em parques de diversão.

Um tema importante nos séculos XVIII e XIX era a construção de mecanismos capazes de converter movimento retilíneo em circular, ou vice-versa. A solução deste problema é menos simples do que possa parecer à primeira vista. Considere, por exemplo, o sistema proposto por James Watt em 1784, e que é ilustrada na figura 8.

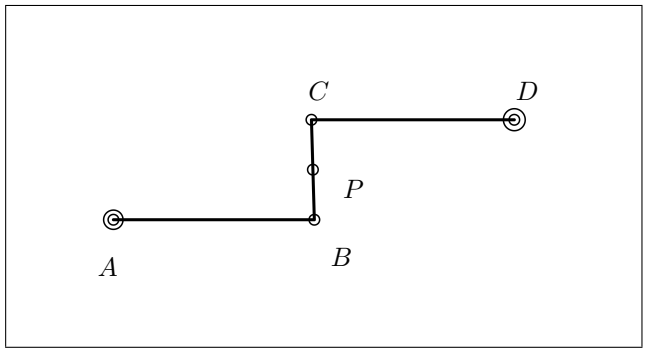


FIGURA 8. Engrenagem de Watt

Os pontos A e D são fixos e os segmentos $\overline{AB}$ e $\overline{CD}$ têm o mesmo comprimento. Além disso, o sistema é articulado nos pontos A, B, C e D. Ao movimentar esta engrenagem vemos o ponto médio P do segmento BC descrever uma curva que aproxima-se de uma reta vertical. Quanto mais longos forem $\overline{AB}$ e $\overline{CD}$ relativamente a $\overline{BC}$, melhor será a aproximação. Diz-se que

Watt orgulhava-se mais deste mecanismo que da invenção da máquina a vapor. Na verdade, tais engrenagens voltaram a ser usadas nos últimos anos na suspensão do eixo traseiro de alguns automóveis. Faremos uma análise detalhada de um caso particular da engrenagem de Watt na seção 2 do capítulo 9.

O primeiro mecanismo capaz de converter um movimento circular para uma linha reta foi proposto pelo matemático P. F. Sarrus em 1853, mas permaneceu pouco conhecido e não teve impacto significativo. Coube, assim, a Charles-Nicolas Peaucellier, um engenheiro que fez carreira como oficial do exército francês. O mecanismo de Peaucellier é ilustrado no diagrama da figura 9.

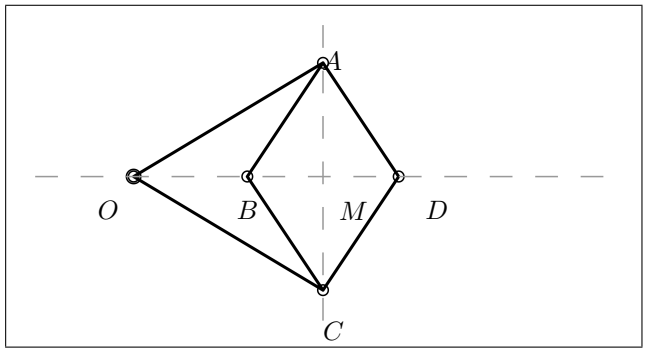


FIGURA 9. Engrenagem de Peaucellier

Neste caso apenas o ponto O está afixo. A engrenagem é articulada em O, A, B, C e D. Além disso, $ABCD$ forma um losango e os segmentos $\overline{OA}$ e $\overline{OC}$ têm o mesmo comprimento.

Um detalhe extremamente importante na análise do comportamento deste mecanismo é que, não importa como seja movido, os pontos O, B e D estarão sempre alinhados. Para entender porque, note que na figura 9 os triângulos OBA e BC são congruentes, de modo que BC é a bissetriz de AOB. Em particular, OB interseta AC em seu ponto médio M. Mas as diagonais de um losango se cortam em seus pontos médios. Portanto, os pontos B e M são comuns às retas OB e BD que, desta forma, têm que coincidir; o que basta para mostrar que O, B e D são realmente colineares.

Para entender o funcionamento da engrenagem adicionamos o braço PB à engrenagem, com o ponto P fixado. Peaucellier mostrou que, se deslocamos o ponto B ao longo da circunferência de centro P e raio $\overline{OP}$, então o ponto D descreve uma reta; como ilustrado na figura 10. É isto que desejamos provar, utilizando as técnicas de demonstração automática estudadas neste capítulo.

Para tornar o problema mais concreto suporemos que o mecanismo que estamos analisando tem dimensões

$$\overline{AB} = \overline{BC} = \overline{CD} = \overline{AD} = 2 \text{ e } \overline{OA} = \overline{OC} = 4.$$

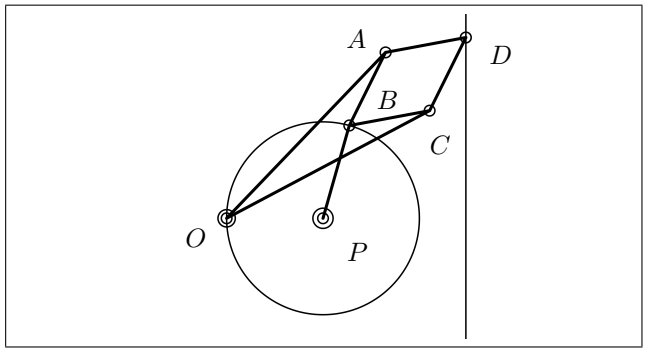


FIGURA 10. Círculos em retas

Além disso, suporemos que o ponto O está localizado na origem do sistema de eixos e que as coordenadas de cada um dos pontos são denotadas pela letra minúscula correspondente com índices um para a abscissa e dois para a ordenada. Desta forma

$$A = (a_1, a_2), \quad B = (b_1, b_2) \quad \text{e assim por diante.}$$

Com esta notação, as restrições sobre os comprimentos dos vários segmentos da engrenagem serão

$$\begin{aligned}
h_1 &= a_1^2 + a_2^2 - 16 \\
h_2 &= c_1^2 + c_2^2 - 16 \\
h_3 &= (b_1 - a_1)^2 + (b_2 - a_2)^2 - 4 \\
h_4 &= (b_1 - c_1)^2 + (b_2 - c_2)^2 - 4 \\
h_5 &= (d_1 - c_1)^2 + (d_2 - c_2)^2 - 4 \\
h_3 &= (d_1 - a_1)^2 + (d_2 - a_2)^2 - 4
\end{aligned}$$

A estas, acrescentamos a equação que estabelece a colinearidade dos pontos O, B e D, provada anteriormente, que é

$$h_7 = b_2 d_1 - b_1 d_2.$$

Finalmente, precisamos obrigar o ponto B a percorrer uma circunferência que, em nosso exemplo, terá centro em $(1, 0)$ e raio um, e que corresponde à equação

$$h_7 = (b_1 - 1)^2 + b_2^2 - 1.$$

A pergunta que queremos fazer é

sob estas hipóteses, qual a curva descrita pelo ponto D?

Algebricamente isto significa que queremos descobrir qual a equação que as coordenadas d_1 e d_2 de D satisfazem, *independentemente das coordenadas dos outros pontos*.

Para isto usaremos a proposição 6.4. Seja

$$I = \langle h_1, \ldots, h_7 \rangle.$$

Se G é uma base de Gröbner de I no anel

$$\mathbb{Q}[a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2]$$

relativamente à ordem lexicográfica com

$$a_1 > a_2 > b_1 > b_2 > c_1 > c_2 > d_1 > d_2$$

então $G \cap \mathbb{Q}[d_1, d_2]$ será constituída pelos geradores do ideal

$$I \cap \mathbb{Q}[d_1, d_2].$$

Procedendo aos cálculos, a base G obtida é formada por dez polinomios, apenas um dos quais contém somente as variáveis d_1 e d_2; a saber

$$d_2^2\, d_1 - 6\, d_2^2 + d_1^3 - 8\, d_1^2 + 12\, d_1.$$

Mas este polinômio pode ser fatorado como

$$(d_1 - 6)(d_2^2 + d_1^2 - 2\, d_1).$$

Para que este polinômio se anule é necessário que

$$d_1 - 6 = 0 \quad \text{ou} \quad d_2^2 + d_1^2 - 2\, d_1 = 0.$$

A primeira equação corresponde mesmo a uma reta, mas não a segunda. De fato, é fácil verificar completando quadrados que a segunda equação equivale a

$$(d - 1 - 1)^2 + d_2^2 = 1;$$

que é a circunferência de raio um e centro em P!

À primeira vista pode parecer que não obtivemos o que queríamos, mas não há nada de muito surpreendente neste resultado. O que aconteceu é que descobrimos um caso degenerado da construção, que ocorre quando os pontos D e C coincidem. Para comprovar a veracidade desta explicação basta introduzir uma nova variável t no anel e acrescentar em I a condição de não degeração

$$(b_1 - d_1)t - 1.$$

Efetuando o cálculo da base de Gröbner verificamos que, desta vez

$$I + \langle (b_1 - d_1)t - 1 \rangle \cap \mathbb{Q}[d_1, d_2] = \langle b_1 - 6 \rangle.$$

Portanto, se não permitirmos que os pontos B e D coincidam, o ponto D descreve a reta $d_1 = 6$, comprovando a afirmação feita por Peaucillier.

A engrenagem de Peaucillier está longe de ser a única que permite a conversão de um movimento circular em retilíneo. Um estudo detalhado destas engrenagens foi feito por A. B. Kempe, de quem já falamos no capítulo 1 (p. 17) em um contexto semelhante. Na verdade Kempe escreveu um livro inteiro sobre este assunto, apropriadamente chamado *Como desenhar uma linha reta*; [**42**]. Uma demonstração do funcionamento do mecanismo de Peaucellier por métodos geométricos tradicionais também pode ser encontrada em [**55**, p. 46].

10. Comentários e complementos

Muitos outros métodos, além das bases de Gröbner, podem ser aplicados na demonstração de teoremas da geometria plana. De fato, o que fizemos aqui é apenas uma pequena parte do que se conhece atualmente sobre este problema. Uma outra técnica muito utilizada é o *método do conjunto característico*, introduzido por Ritt no contexto da álgebra diferencial e aplicado por Wu aos anéis de polinômios. Como nos caso das bases de Gröbner, o método de Ritt-Wu descobre um novo conjunto de geradores para o ideal. Só que, neste caso, o conjunto de geradores é triangular: um dos geradores só depende de uma variável, o seguinte somente de duas, uma das quais é a do primeiro polinômio, e assim por diante. O resultado é um sistema que, se fosse linear, diríamos que está na forma escalonada. Podemos obter algo semelhante, no caso das bases de Gröbner sob a ordem lexicográfica, se o conjunto algébrico definido pelo ideal tiver apenas uma quantidade finita de soluções complexas.

Uma excelente referência para o método de Ritt-Wu é o livro [**72**] escrito pelo próprio Wu. Além de uma enorme quantidade de exemplos de teoremas da geometria euclidiana, este livro também ilustra como técnicas semelhantes podem ser usadas para provar resultados de geometria diferencial. Talvez mais surpreendente ainda seja o fato de que Wu foi capaz de provar automaticamente o teorema de Kepler, segundo o qual a órbita de um planeta sujeito apenas à força de gravidade do Sol deve ser elíptica; veja [**71**].

Finalmente, devemos observar que métodos algébricos como as bases de Gröbner e o método do conjunto característico de Ritt-Wu são apenas um dos enfoques possíveis para a demonstração automática de teoremas de geometria. Outra possibilidade que vem sendo bastante investigada consiste em explicitar os axiomas e as regras de inferência a serem utilizadas e utilizar técnicas de inteligência artificial para produzir novos teoremas a partir destes dados iniciais. Para uma introdução a tais métodos veja [???].

11. Exercícios

1. Determine uma expressão polinomial explícita para

   $$\mathtt{ang}(\mathtt{A}_1, \mathtt{A}_2, \mathtt{A}_3 : \mathtt{A}_4, \mathtt{A}_5, \mathtt{A}_6),$$

   em função das coordenadas x_i e y_i, dos pontos $A_i = (x_i, y_i)$, em que $1 \leq i \leq 6$.

   Todos os resultados abaixo devem ser provados usando o método direto ou o método refutacional.

2. Prove que as três alturas de um triângulo sempre se cortam em um único ponto.

3. Prove, que as três bissetrizes de um triângulo sempre se cortam em um único ponto.

4. Prove a proposição 1 do *Livro dos Lemas* de Arquimedes segundo a qual

Se duas circunferências se tocam no ponto A, e se BD e EF são diâmetros paralelos nestas circunferências, então os pontos A, D e F são colineares.

5. Prove que o baricentro, o ortocentro e o centro da circunferência circunscrita a um triângulo qualquer são colineares.

6. Prove que, se, sobre os três lados de um triângulo ABC, construímos triângulos equiláteros ABC', ACB' e BCA', então as retas AA', BB' e CC' são concorrentes.

7. Prove que duas secantes a uma circunferência C são traçadas a partir de um ponto P e cortam C em A e A', e B e B', respectivamente. Então,
$$|PA||PA'| = |PB||PB'|.$$

8. Prove que a circunferência determinada pelos pés das alturas de um triângulo também contém os pontos médios dos segmentos que unem o ortocentro do triângulo a seus três vértices. Lembre-se que o *ortocentro* de um triângulo é o ponto de interseção de suas três alturas.

9. Prove que os excírculos de um triângulo qualquer são tangentes à circunferência determinada pelos pés das alturas do triângulo. Lembre-se que um *excírculo* de um triângulo é a circunferência tangente (pelo lado de fora do triângulo), a um de seus lados e ao prolongamento dos outros dois lados.

10. Suponha que são dados oito pontos distintos $P_1, \ldots, P_8$ do plano, entre os quais podemos formar oito tríades da forma $P_iP_{i+1}P_{i+3}$, em que $1 \leq i \leq 8$ e a soma dos índices é tomada módulo 8. Prove que se estas oito tríades são colineares então os oito pontos têm que ser colineares.

11. Prove que o centro de qualquer circunferência tangente a duas retas dadas tem que estar sobre a bissetriz do ângulo formado por estas retas.

12. Prove o *teorma de Brianchon*, segundo o qual as retas que ligam vértices opostos de um hexágono inscrito em uma elipse se cortam em um único ponto.

13. Seja ABC um triângulo qualquer e construa, na parte exterior do triângulo, os quadrados $BCDE$, $ACFG$ e $BAHK$ cada um dos quais está sobre um dos lados do triângulo ABC. Então, construa os paralelogramos $FCDQ$ e $EBKP$. Prove que PAQ é um triângulo retângulo isósceles.

CAPíTULO 7

Programação inteira

Neste capítulo estudamos como aplicar o método das bases de Gröbner na resolução de problemas de programação inteira. A programação inteira, como a programação linear, trata de como otimizar uma função sob certas condições restritivas, geralmente apresentadas como desigualdades que precisam ser satisfeitas por equações lineares nas variáveis. Contudo, na programação inteira, as variáveis só podem assumir valores inteiros não negativos. Esta restrição extra torna o problema bem mais complicado, e todos os algoritmos conhecidos têm um custo bastante alto. Começaremos o capítulo descrevendo alguns problemas típicos de programação inteira, que serão resolvidos na seção 5 usando o método desenvolvido no resto do capítulo. O enfoque adotado aqui segue de perto a exposição de [**65**] e [**73**].

1. Alguns problemas

Suponhamos que uma indústria do Rio utiliza uma empresa de transportes de carga para entregar sua produção a revendedores em várias cidades. Os caminhões da empresa de transportes carregam uma carga máxima de $3,7$ toneladas, num volume que não pode exceder $20m^3$. A indústria tem revendedores em Angra dos Reis e em Paraty.

As cargas destes revendedores são fornecidas em paletas, quer dizer, estrados de madeira sobre os quais a carga é arrumada. Medindo o peso em quilogramas e o volume em metros cúbicos, as paletas enviadas a Angra e Paraty têm as seguintes especificações.

Cidade	Peso da paleta	Volume da paleta
Angra	400	2
Paraty	500	3

Como Paraty fica mais longe que Angra, a empresa de transportes cobra mais caro para levar os produtos até lá do que para enviá-los a Angra. Na verdade, o valor da entrega de uma paleta em Angra é de R$ $11,00$, ao passo que a entrega de uma paleta em Paraty custará R$ $15,00$. Cabe à empresa de transportes decidir quantas paletas devem ser postas em cada caminhão de modo que o lucro por caminhão seja maximizado.

Para modelar este problema matematicamente usaremos a para denotar o número de paletas que cada caminhão deve levar até Angra e p para denotar o número de paletas destinadas a Paraty. A modelagem tem que levar em conta o peso e o volume máximos transportados por caminhão, o que nos dá as equações

$$\begin{aligned} 4a + 5p &\leq 37 \\ 2a + 3b &\leq 20. \end{aligned} \tag{54}$$

Já o lucro será dado pela função

$$\ell(a, p) = 11a + 15p.$$

Observe que não podemos apelar para programação linear para resolver este problema porque cada caminhão transporta um número inteiro (não negativo) de paletas. Em outras palavras, $a \geq 0$ e $p \geq 0$.

Podemos reformular a maneira como modelamos este problema de forma mais compacta usando a linguagem de matrizes. Se

$$u = (u_1, \ldots, v_n) \text{ e } v = (v_1, \ldots, v_n)$$

forem dois vetores de $\mathbb{Z}^n$, diremos que $u \leq v$ se $u_j \leq v_j$ para todo $1 \leq j \leq n$. Escrevendo, então,

$$A = \begin{bmatrix} 4 & 5 \\ 2 & 3 \end{bmatrix}, u = \begin{bmatrix} a \\ p \end{bmatrix} \text{ e } b = \begin{bmatrix} 37 \\ 20 \end{bmatrix}$$

diremos que nosso problema consiste em

maximizar a função ℓ sob a condição $Au \leq b$.

Este é um problema típico de uma área da matemática conhecida como *programação inteira*. Naturalmente o adjetivo *inteira* é uma referência ao fato de que esperamos maximizar ℓ sob a restrição de que $u \in \mathbb{N}^2$. Problemas de programação inteira são comuns em engenharia, ciência da computação, pesquisa operacional e matemática. Nosso objetivo neste capítulo é descobrir de que forma o método das bases de Gröbner pode ser usado para resolver este problema. Na próxima seção formularemos o problema de uma maneira mais geral, e discutiremos alguns dos conceitos geométricos básicos utilizados na sua solução. Antes, porém, convém descrever mais alguns exemplos para que você possa formar uma ideia mais clara da gama de problemas abordados em programação inteira.

O segundo problema que desejamos descrever é conhecido como *problema da mochila* (em inglês "knapsack problem"). O problema pode ser descrito da seguinte maneira. Uma prova de uma gincana consiste em encher uma mochila que cabe no máximo $2000cm^3$ com vários objetos dispostos sobre uma mesa. Cada pessoa pode pôr na mochila no máximo um item de cada objeto. Ganha aquela pessoa que puser na mochila objetos que somem o maior valor total. Os objetos dispostos sobre a mesa, com seus respectivos volumes (em cm^3) e preços (em reais) são os seguintes:

Objeto	Volume	Preço
A	300	9
B	200	13
C	500	10
D	400	15
E	700	12
F	400	17

Para modelar o problema criamos uma variável para cada objeto. Para facilitar podemos chamar as variáveis de u_a, u_b, u_c, u_d, u_e e u_f. A condição sobre o volume que o problema deve satisfazer é

$$3u_a + 2u_b + 5u_c + 4u_d + 7u_e + 4u_f \leq 20.$$

Contudo, como só pode ser posto um item de cada objeto, devemos ter também que

$$0 \leq u_a, u_b, u_c, u_d, u_e, u_f \leq 1.$$

Por outro lado, a função preço, que avalia o custo total dos objetos postos na mochila é

$$\ell(u_a, u_b, u_c, u_d, u_e, u_f) = 9u_a + 13u_b + 10u_c + 15u_d + 12u_e + 17u_f.$$

Assim, o que desejamos fazer é maximizar o valor de p sob as condições impostas pelo problema.

Finalmente, o último exemplo que desejamos discutir está relacionado ao *problema do particionamento de conjuntos*. Digamos que uma loja de departamentos vende quatro produtos A, B, C e D. Como a loja oferece uma série de promoções, comprar um pacote com mais de um produto é mais econômico do que comprá-los separadamente. A tabela com os preços dos produtos e das várias promoções é dada a seguir. A pergunta é: qual a maneira mais econômica de adquirir exatamente um item de cada produto, levando em conta as promoções?

Promoção	Preço (em reais)	Promoção	Preço (em reais)
A	3	BC	7
B	4	BD	7
C	5	CD	10
D	6	ABC	9
AB	6	ABD	10
AC	6	ACD	12
AD	8	BCD	13

Desta vez a modelagem do problema é menos ingênua. Para cada produto, e cada promoção, criamos uma variável. Assim, à promoção BCD vai corresponder a variável r_{bcd}. Por outro lado, teremos uma equação para cada produto, e estas equações corresponderão a dizer que queremos exatamente um

item daquele produto em nossa compra. Por exemplo, o produto A aparece nos pacotes A, AB, AC, ABC, ABD, ACD. Assim, a equação correspondente a A é

$$r_a + r_{ab} + r_{ac} + r_{abc} + r_{abd} + r_{acd} = 1;$$

e teremos equações semelhantes para os produtos b, c e d. Naturalmente, o objetivo do problema é minimizar o custo, que é dado por

$$c = 3r_a + 4r_b + 5r_c + 6r_d + 6r_{ab} + 6r_{ac} + 8r_{ad} + 7r_{bc} + 7r_{bd} + 10r_{cd} + 9r_{abc} + 10r_{abd} + 12r_{acd} + 13r_{bcd}.$$

2. Padronizando os problemas

Em geral um problema de programação inteira pode ser um pouco mais complicado do que os que foram discutidos na seção anterior. Para começar, poderíamos ter muito mais variáveis, digamos $x_1, \ldots, x_n$. Por outro lado, embora as restrições sempre sejam formuladas como desigualdades envolvendo equações lineares, estas desigualdades tanto poderiam envolver $\leq$ quanto $\geq$. Este último ponto, entretanto, não oferece grande dificuldade, já que podemos converter um tipo de desigualdade no outro simplesmente multiplicando por -1. Em outras palavras, se $a_1, \ldots, a_n \in \mathbb{Z}$, então

$$a_1x_1 + \cdots + a_nx_n \geq b$$

é equivalente a

$$(-a_1)x_1 + \cdots + (-a_n)x_n \leq -b.$$

Isto significa que sempre podemos escrever as restrições de um problema de programação linear em forma matricial como

$$Au \leq b, \tag{55}$$

em que $A \in \mathrm{M}_{mn}(\mathbb{Z})$ e $b \in \mathbb{Z}^m$.

Uma observação mais sutil é que podemos converter as desigualdades de um problema em igualdades. Isto é possível porque estamos supondo que as variáveis presentes no problema sempre tomam valores não negativos. Assim,

$$a_1x_1 + \cdots + a_nx_n \leq b$$

pode ser reescrita na forma

$$a_1x_1 + \cdots + a_nx_n + y = b.$$

já que

$$y = b - (a_1x_1 + \cdots + a_nx_n) \geq 0.$$

Observe que, para converter $Au \leq b$ em uma igualdade, precisaremos de m variáveis novas, uma para cada linha da matriz.

Modificando cada problema conforme indicado acima, podemos supor que as restrições de todos os problemas de programação inteira que queremos resolver são da forma

$$Au = b, \text{ em que } A \in \mathrm{M}_{mn}(\mathbb{Z}) \text{ e } b \in \mathbb{Z}^m.$$

Mas, para que um ponto $u \in \mathbb{N}^n$ possa ser uma solução deste problema de programação inteira é preciso que pertença ao conjunto

$$P_A = \{u \in \mathbb{N}^n : Au = b\}.$$

Por isso, diremos que P_A é a *região de possibilidade* do problema $Au = b$.

Até aqui todas as considerações que fizemos referem-se às restrições do problema; é hora de passar a função a ser otimizada. Neste caso, para padronizar os problemas, suporemos sempre que desejamos *minimizar* a função dada. Isto levanta, imediatamente, uma questão, já que no exemplo da seção 1 a função lucro deve ser maximizada. Contudo, maximizar uma função linear ℓ é a mesma coisa que minimizar $-\ell$, de modo que não há realmente perda de generalidade se supusermos que todos os problemas tratam da minimização de uma função.

Sejam $v_0 \in \mathbb{Z}^n$, $A \in \mathrm{M}_{mn}(\mathbb{Z})$, $b \in \mathbb{Z}^m$, e denote por c a aplicação que leva $u \in \mathbb{N}^n$ em $v_0 \cdot u \in \mathbb{Z}$. Reunindo tudo o que dissemos anteriormente, fica claro que sempre podemos formular qualquer problema de programação linear na seguinte forma padrão:

> minimize a função linear c sob as restrições $Au = b$ e $u \geq 0$.

Como o problema requer a minimização de c, vamos chamá-la de *função custo* deste problema.

Vejamos como formular os problemas da seção 1 nesta forma. Para começar, o problema de particionamento de conjuntos, já está na forma requerida, uma vez que todas as restrições estão expressas como equações lineares e a função dada deve ser minimizada. Neste caso a matrix correspondente é

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Já no problema do transporte de cargas, precisamos introduzir duas novas variáveis, digamos y e z, a fim de converter as desigualdades dadas em igualdades. Neste caso, teremos as restrições (54) reescritas como

$$\begin{aligned} 4a + 5p + y &= 37 \\ 2a + 3b + z &= 20. \end{aligned}$$

Assim, se

$$\widehat{A} = \begin{bmatrix} 4 & 5 & 1 \\ 2 & 3 & 1 \end{bmatrix} \text{ e } \widehat{u} = \begin{bmatrix} a \\ p \\ y \\ z \end{bmatrix}$$

então as restrições são da forma

$$\widehat{A}\widehat{u} = b \text{ e } \widehat{u} \geq 0.$$

Note que as mudanças que fizemos na matriz não alteram o vetor b. Finalmente, maximizar a função lucro dada por $\ell(a, p, y, z) = 11a + 15p$ é o mesmo que minimizar a função $c : \mathbb{N}^4 \to \mathbb{Z}^4$ dada por

$$c(a, p, y, z) = -11a - 15p.$$

Portanto, neste exemplo $v_0 = (-11, -15, 0, 0)$. Como seria de esperar, as variáveis y e z em nada contribuem para a função a ser minimizada, já que não têm nenhum significado no problema original. Afinal estas variáveis são apenas um artefato usado para padronizar o problema.

A conversão do problema da mochila é semelhante ao anterior. À primeira vista pode parecer que temos apenas uma desigualdade, dada por

$$3u_a + 2u_b + 5u_c + 4u_d + 7u_e + 4u_f \leq 20.$$

Mas isto não é verdade, uma vez que cada variável só pode assumir um de dois valores: 0 ou 1. Por isso, precisaremos de 7 novas variáveis: uma para cada variável do problema original, e uma para a desigualdade acima. Chamaremos estas novas variáveis de v_a, v_b, v_c, v_d, v_e, v_f e w. As equações resultantes serão

$$3u_a + 2u_b + 5u_c + 4u_d + 7u_e + 4u_f + w = 20,$$

e também

$$\begin{aligned} u_a + v_a &= 1 & \qquad u_b + v_b &= 1 \\ u_c + v_c &= 1 & \qquad u_d + v_d &= 1 \\ u_e + v_e &= 1 & \qquad u_f + v_f &= 1 \end{aligned}$$

Portanto, a matriz A pode ser escrita como

$$\begin{bmatrix} 3 & 2 & 5 & 4 & 7 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Finalmente, a função a ser minimizada será

$$\begin{aligned} c(u_a, u_b, u_c, u_d, u_e, u_f) &= -\ell(u_a, u_b, u_c, u_d, u_e, u_f) \\ &= -(9u_a + 13u_b + 10u_c + 15u_d + 12u_e + 17u_f). \end{aligned}$$

Como já observado anteiormente, apenas as variáveis originais do problema aparecem na função custo.

3. Ideais e programação inteira

Nesta seção veremos como modelar um problema de programação inteira em termos de ideais. Já na próxima seção, discutiremos como resolvê-lo usando o método de bases de Gröbner. Suporemos que o problema que vamos considerar está na forma padrão estabelecida na seção 2. Portanto, dados

$$v_0 \in \mathbb{Z}^n, A \in \mathrm{M}_{mn}(\mathbb{Z}), \text{ e } b \in \mathbb{Z}^m,$$

considere a função $c : \mathbb{N}^n \to \mathbb{Z}^n$ definida por $c(w) = v_0 \cdot w$. Nesta notação o problema pode ser descrito na forma

> minimize a função linear c sob as restrições $Aw = b$ e $w \geq 0$.

Dois subconjuntos de $\mathbb{Z}^n$ desempenham um papel muito importante na descrição do procedimento. O primeiro é o conjunto dos vetores de coordenadas inteiras que pertencem ao núcleo da aplicação linear definida pela matriz A. Isto é, o conjunto

$$\mathrm{N}_{\mathbb{Z}}(A) = \{u \in \mathbb{Z}^n : Au = 0\}.$$

Note que $\mathrm{N}_{\mathbb{Z}}(A)$ independe tanto de b, quanto da função custo c. Já o outro conjunto que queremos definir depende de A e b, mas não de c. Mas, para poder descrevê-lo, precisamos de algumas definições preliminares.

Seja S um subconjunto de $\mathbb{R}^n$. Dizemos que S é um *conjunto convexo* se, dados dois pontos quaisquer u_1 e u_2 em S, temos que o segmento de reta que une u_1 a u_2 pertence a S. Quase todas as figuras tratadas pela geometria euclidiana usual são convexas, incluindo-se triângulos, paralelogramos e círculos. Já a figura 1 é plana, mas não é convexa. Se S não for um conjunto convexo, então o menor conjunto convexo $\widehat{S}$ que contém S é chamado de *fecho convexo* de S.

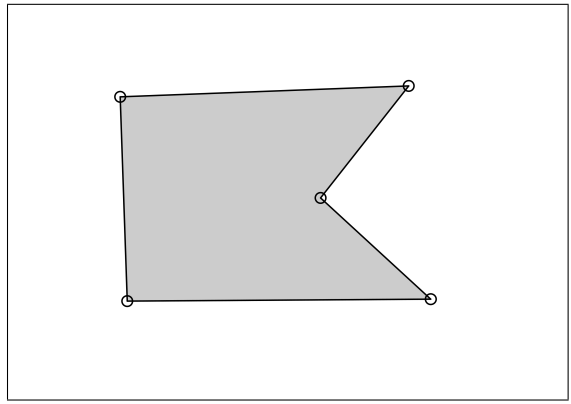


FIGURA 1. Um conjunto que não é convexo

Quando S é um subconjunto finito de pontos do plano, o fecho convexo pode ser descrito de uma maneira fácil de vizualizar. Basta fazer passar um

barbante por fora de todos os pontos e ir apertando até não poder mais. Neste caso o fecho conexo de S é formado pelos pontos que ficam dentro da região delimitada pelo barbante. Podemos proceder de maneira semelhante para descrever o fecho convexo de um conjunto finito de pontos no espaço. Só que desta vez devemos embrulhar os pontos com filme plástico da maneira mais apertada possível. Em ambos os casos o fecho convexo resultante é limitado; isto é, pode ser posto dentro de um quadrado de lado grande o suficiente. Entretanto, não é verdade que o fecho convexo de um conjunto qualquer é sempre limitado. Por exemplo, o fecho convexo do conjunto dos pontos do plano de coordenadas inteiras que pertencem aos semi-eixos positivos OX e OY é todo o primeiro quadrante.

O conjunto de que falamos anteriormente pode, agora, ser definido como o fecho convexo de

$$\{u \in \mathbb{N}^n : Au = b\}.$$

Vamos denotá-lo por $\mathrm{P}_A(b)$. Isto nos leva a nosso primeiro resultado.

PROPOSIÇÃO 7.1. *Seja A uma matriz de coeficientes não negativos. Se*

$$\mathrm{N}_{\mathbb{Z}}(A) \cap \mathbb{N} = \{0\},$$

então $\mathrm{P}_A(b)$ é um conjunto finito não vazio para todo b na região de possibilidades de um problema cujas restrições são dadas por $Au \leq b$ e $u \geq 0$.

DEMONSTRAÇÃO. $\mathrm{P}_A(b)$ não é vazio porque b pertence à região de possibilidades. Portanto, basta provar que $\mathrm{P}_A(b)$ é limitado. Mas um ponto $u \in \mathbb{R}^n$, cujas coordenadas não são negativas, satisfaz $Au \leq b$, se está na interseção das regiões do $\mathbb{R}^n$ delimitadas pelos hiperplanos

$$a_{i1}x_1 + \cdots + a_{in}x_n \leq b_i$$

em que $A = (a_{ij})$ e b_i é a i-ésima coordenada de b. Contudo, se $a_{ij} > 0$, então $x_j < b_i$. Além disso, dado $1 \leq j \leq n$ tem que existir pelo menos um i para o qual $a_{ij} > 0$, do contrário o vetor e_j seria anulado pela matriz A, e teríamos $e_j \in \mathrm{N}_{\mathbb{Z}}(A) \cap \mathbb{N}$ o que não é possível por hipótese. Portanto, cada ponto $u = (u_1, \ldots, u_n)$ para o qual $Au \leq 0$ satisfaz

$$0 \leq u_j \leq \max\{b_i : 1 \leq i \leq m\}.$$

Assim, todos os pontos $u \in \mathbb{N}^n$ para os quais $Au = b$ estão contidos em um quadrado. Como um quadrado é uma figura convexa, o fecho convexo destes pontos também estará contido no mesmo quadrado. Mas isto implica que $\mathrm{P}_A(b)$ é um conjunto limitado. □

Como o bom funcionamento do nosso algoritmo vai depender do fato $\mathrm{P}_A(b)$ ser limitado suporemos, de agora em diante, que A é uma matriz de coeficientes não negativos que satisfaz $\mathrm{N}_{\mathbb{Z}}(A) \cap \mathbb{N} = \{0\}$. É preciso deixar claro que o método desenvolvido a seguir também se aplica sem estas hipóteses. Entretanto, para tornar a exposição mais clara vamos nos limitar a este caso especial.

Com isto já temos todas as ferramentas necessárias para construir o ideal que vai modelar o problema de programação inteira que estamos considerando, e que consiste em minimizar c sob as restrições $Au = b$ e $u \geq 0$. Considere o conjunto $\mathcal{B}_A$ de binômios em $\mathbb{Q}[x_1, \ldots, x_n]$ da forma

$$x^\alpha - x^\beta,$$

em que $\alpha, \beta \in \mathbb{N}$ e $\alpha - \beta \in \mathrm{N}_\mathbb{Z}(A)$. Então, ao problema dado associamos o ideal I_A no anel de polinômios $\mathbb{Q}[x_1, \ldots, x_n]$ gerado pelos binômios de $\mathcal{B}_A$.

Para poder aplicar a teoria de bases de Gröbner a este ideal precisamos decidir qual a ordem monomial que será utilizada. É aqui que entra a função custo. Sejam $\alpha, \beta \in \mathbb{N}^n$. Diremos que uma ordem total $>$ em $\mathbb{T}^n$ que satisfaz a propriedade 3 da página 36 é *compatível com a função custo* c se

$$c(\alpha) > c(\beta) \text{ implica que } x^\alpha > x^\beta.$$

Uma maneira fácil de construir uma tal ordem é usar c para definir um vetor de pesos, e desempatar monômios iguais usando a ordem lexicográfica. Mais precisamente,

$$x^\alpha >_c x^\beta \text{ se, e somente se, } \begin{cases} c(\alpha) > c(\beta) & \text{ou} \\ c(\alpha) = c(\beta) & \text{e } \alpha >_{\text{lex}} \beta. \end{cases}$$

Esta é, claramente, uma ordem total. Vamos verificar se satisfaz as outras propriedades de uma ordem monomial. Suponha, primeiramente, que $x^\alpha >_c x^\beta$ e que x^γ é outro monômio qualquer. Como c é uma aplicação linear, temos que se $c(\alpha) > c(\beta)$, então

$$c(\alpha + \gamma) > c(\beta + \gamma);$$

que implica que $x^\gamma x^\alpha >_c x^\gamma x^\beta$. Da mesma forma se $c(\alpha) = c(\beta)$, então $c(\alpha + \gamma) = c(\beta + \gamma)$. Desta vez o resultado desejado segue do fato de que lex é uma ordem monomial. Resta-nos apenas verificar se $x^\alpha >_c 1$ para todo $\alpha \neq 0$. Infelizmente isto é falso em geral. De fato, se a i-ésima coordenada do vetor v que define c for negativa, então $c(e_i) < 0$, de modo que $1 >_c x^{e_i}$. Para evitar este problema basta supor que $v \geq 0$. Entretanto, esta hipótese tem a grande desvantagem de que o primeiro problema da seção 1 não satisfaz esta condição! Veremos na seção 5 como contornar este problema usando a proposição 7.1. Por enquanto, trabalharemos sob a hipótese de que $c \geq 0$.

Uma outra coisa que precisa ser observada é que, como a ordem $>$, compatível com c, tem sempre que ser total, acharemos apenas uma solução mínima para o problema. Entretanto, em geral pode haver vários valores de $\alpha \in \mathbb{N}^n$ que minimizam c e satisfazem $A\alpha = b$. Nosso método vai achar, entre todos estes, aquele α para o qual x^α é mínimo com respeito $>$. Por isso é conveniente reformular o problema levando em conta as várias hipóteses que fizemos ao longo da seção. Os dados do problema serão:

- uma matriz $n \times m$ A cujos coeficientes são inteiros não negativos, e que deve satisfazer

$$\mathrm{N}_\mathbb{Z}(A) \cap \mathbb{N} = \{0\};$$

- uma função custo $c \geq 0$;
- uma ordem monomial $>$ compatível com c.

Dado $b \in \mathbb{N}^m$, nosso objetivo é achar $\alpha \in \mathbb{N}^n$ tal que x^α é mínimo com respeito a $>$ entre os multi-índices que satisfazem $A\alpha = b$. Vamos nos referir a este problema como $\mathrm{PI}_{A,>}(b)$. Como a notação sugere, consideraremos A e $>$ como fixos e trataremos o problema como sendo uma função de b. Isto reflete o fato de que nosso enfoque consistirá em efetuar o preprocessamento do problema em função de A e $>$, de modo que poderemos calcular a solução mínima para cada b escolhido.

Encerraremos esta seção com um resultado que dá uma maneira de identificar as soluções mínimas do problema $\mathrm{P}_{A,c}(A\alpha)$ a partir do ideal I_A, preparando assim o terreno para a aplicação das bases de Gröbner a ser feita na próxima seção.

CRITÉRIO 7.2. *O ponto $\alpha \in \mathbb{N}^n$ é uma solução mínima do problema $\mathrm{P}_{A,c,>}(A\alpha)$ se, e somente se, $x^\alpha \notin \mathrm{in}(I_A)$.*

DEMONSTRAÇÃO. Para que $\alpha \in \mathbb{N}^n$ *não* seja uma solução mínima de $\mathrm{P}_{A,c}(A\alpha)$ é preciso que exista $\beta \in \mathbb{N}^n$ tal que $A\alpha = A\beta$ e $c(\alpha) > c(\beta)$. Mas isto implica que $x^\alpha - x^\beta$ não é nulo e pertence a I_A, já que

$$A(\alpha - \beta) = A(\alpha) - A(\beta) = 0.$$

Por outro lado, como $c(\alpha) > c(\beta)$, temos que

$$\mathrm{in}(x^\alpha - x^\beta) = x^\alpha.$$

A recíproca é imediata e fica por sua conta. □

4. Bases de Gröbner e programação inteira

Iniciamos a seção com um teorema que caracteriza a base de Gröbner do ideal I_A definido na seção anterior. Lembre-se que, ao problema $\mathrm{PI}_{A,>}(b)$ associamos o ideal I_A no anel de polinômios $\mathbb{Q}[x_1, \ldots, x_n]$ gerado pelos binômios do conjunto

$$\mathcal{B}_A = \{x^\alpha - x^\beta : \alpha, \beta \in \mathbb{N} \text{ e } \alpha - \beta \in \mathrm{N}_\mathbb{Z}(A)\}.$$

Antes de enunciar o teorema, precisamos da seguinte notação: se $u \in \mathrm{N}_\mathbb{Z}(A)$, então podemos decompô-lo na forma $u = u_+ - u_-$, em que u_+ e u_- não têm coordenadas negativas.

TEOREMA 7.3. *Seja G é um subconjunto finito de $\mathcal{B}_A$.*

(1) *Se $\mathrm{R}_G(x^\alpha) = x^\beta$, então $\alpha - \beta \in \mathrm{N}_\mathbb{Z}(A)$.*
(2) *Se $f \in \mathcal{B}_A$, então $\mathrm{R}_G(f) \in \mathcal{B}_A$.*
(3) *Se G é uma base de Gröbner de I_A então $G \subseteq \mathcal{B}_A$.*
(4) *Se G for uma base de Gröbner reduzida de I_A e $x^\alpha - x^\beta \in G$ então $\mathrm{mdc}(x^\alpha, x^\beta) = 1$.*

DEMONSTRAÇÃO. Para provar (1) observe que, como o algoritmo de divisão é recursivo e, em cada etapa, efetua apenas a divisão de um polinômio por outro, então basta considerar o caso em que estamos dividindo um monômio por um binômio de $\mathcal{B}_A$. Sejam x^α o monômio e $x^\eta - x^\theta$ o binômio, e digamos que $x^\eta > x^\theta$.

Ao dividir x^α por $x^\eta - x^\theta$ nos deparamos com duas possibilidades. A primeira é que x^α é divisível por x^η. Neste caso existe γ tal que $\alpha = \eta + \gamma$, de modo que o resto da divisão será

$$x^\alpha - x^\gamma(x^\eta - x^\theta) = x^{\gamma+\theta}.$$

Mas

$$b = A\alpha = A(\eta + \gamma) = A\eta + A\gamma.$$

Contudo, $A\eta = A\theta$, e portanto,

$$b = A\theta + A\gamma = A(\theta + \gamma),$$

que é o que queríamos mostrar. Por outro lado, se x^α não é divisível por x^η, então o resto da divisão será o próprio x^α e não há nada a fazer.

A demonstração de (2) é uma consequência imediata da demonstração de (1), e os detalhes ficam por sua conta.

Para provar (3) precisamos analisar o que acontece aos binômios quando aplicamos o algoritmo de Buchberger. Mas, em cada etapa deste algoritmo, calculamos apenas um S-polinômio e seu resto por elementos de $\mathcal{B}_A$. Como (1) e (2) já dão cabo do que acontece com os restos de divisões, resta-nos apenas mostrar que o S-polinômio de binômios em $\mathcal{B}_A$ ainda é um binômio em $\mathcal{B}_A$. Para isto suponha que

$$x^\alpha - x^\beta \text{ e } x^\eta - x^\theta$$

são binômios em $\mathcal{B}_A$ com $x^\alpha > x^\beta$ e $x^\eta > x^\theta$. Se

$$\mathrm{mdc}(x^\alpha, x^\eta) = x^\delta,$$

então

$$S(x^\alpha - x^\beta, x^\eta - x^\theta) = \left(\frac{x^\alpha}{x^\delta}\right) x^\theta - \left(\frac{x^\eta}{x^\delta}\right) x^\beta.$$

Assim,

$$S(x^\alpha - x^\beta, x^\eta - x^\theta) = x^{\alpha-\delta+\theta} - x^{\eta-\delta+\beta}.$$

Mas,

$$A(\alpha - \delta + \theta - (\eta - \delta + \beta)) = A(\alpha - \beta) + A(\theta - \eta) = 0,$$

de modo que o S-polinômio realmente pertence a $\mathcal{B}_A$, como afirmamos.

Finalmente, falta-nos provar (4). Para isto, suponha que $x^\alpha - x^\beta$ pertence a uma base de Gröbner reduzida e digamos que

$$\mathrm{mdc}(x^\alpha, x^\beta) = x^\delta.$$

Escrevendo

$$\alpha = \alpha_0 + \delta \text{ e } \beta = \beta_0 + \delta,$$

temos que

$$A(\alpha - \beta) = A(\alpha_0 - \beta_0) = 0.$$

Portanto, $x^{\alpha_0} - x^{\beta_0}$ pertence a I_A. Contudo, $x^\alpha > x^\beta$ implica que $x^{\alpha_0} > x^{\beta_0}$, de modo que

$$\text{in}(x^\alpha - x^\beta) = x^\alpha$$

é divisível por

$$\text{in}(x^{\alpha_0} - x^{\beta_0}) = x^{\alpha_0}.$$

Se $\delta \neq 0$, então $\alpha_0 \neq \alpha$. Como G é uma base de Gröbner reduzida, terá que existir um binômio $x^\eta - x^\theta \in G$ tal que $x^\eta > x^\theta$ e x^η divide x^{α_0}. Mas isto implica que

$$x^\eta \text{ divide } x^\alpha$$

e ao mesmo tempo é diferente de x^α, o que contradiz o fato da base ser reduzida. Portanto, $\delta = 0$ e

$$\text{mdc}(x^\alpha, x^\beta) = 1.$$

□

Com isto podemos enunciar e provar o algoritmo para solução do problema $\text{PI}_{A,>}(b)$. Como sempre estamos supondo que b pertence à região de possibilidade do problema.

ALGORITMO 7.4 (Resolvendo $\text{PI}_{A,>}(b)$.). *Dada a matriz A, a ordem $>$ e o vetor b, o algoritmo determina a solução mínima de* $\text{PI}_{A,>}(b)$.

Etapa 1: *Pré-processamento:*
- *Ache um conjunto de geradores para I_A.*
- *Calcule uma base de Gröbner reduzida G de I_A com respeito a $>$.*

Etapa 2: *Resolvendo* $\text{PI}_{A,>}(b)$
- *Ache uma solução qualquer α de* $\text{PI}_{A,>}(b)$.
- *Calcule* $\text{R}_G(x^\alpha) = x^\beta$.
- *Retorne β.*

DEMONSTRAÇÃO. Se $\text{R}_G(x^\alpha) = x^\beta$, então $\alpha - \beta \in \text{N}_\mathbb{Z}(A)$ pelo item (1) do teorema 7.3. Mas isto significa que $x^\alpha - x^\beta \in I_A$.

Suponha, agora, por contradição, que x^β não seja mínimo. Neste caso, existe η tal que $\alpha - \eta \in \text{N}_\mathbb{Z}(A)$ e $x^\beta > x^\eta$. Como isto implica que

$$x^\beta - x^\eta \in I_A, \text{ e que } x^\beta = \text{in}(x^\beta - x^\eta),$$

então

$$x^\beta \in \text{in}(I_A).$$

Mas isto contradiz o fato de x^β ser reduzido com respeito a G. Portanto, x^β é mínimo e o algoritmo funciona corretamente. □

Na prática existem dois obstáculos sérios à implementação do algoritmo, conforme descrito acima; a saber:

(1) precisamos encontrar um conjunto de geradores para I_A, e
(2) precisamos encontrar *alguma* solução de $\mathrm{PI}_{A,>}(b)$.

Para evitar estes problemas utilizamos uma ideia oriunda da programação linear, onde é conhecida como "the big-M method". A ideia, originalmente proposta por P. Conti e C. Traverso em 1991, consiste em estender o problema original de modo que seja fácil determinar tanto o conjunto de geradores, quanto uma solução especial.

Para fazer isto, criamos a matriz $n \times (n+m)$

$$B = [I_m, A]$$

em que I_m é a matriz identidade $m \times m$. Sejam agora $y_1, \ldots, y_m$ novas variáveis e consideremos o anel de polinômios $\mathbb{Q}[x_1, \ldots, x_n, y_1, \ldots, y_m]$. Seja $\succ_c$ a ordem de eliminação neste anel definida fazendo todos os ys maiores que todos os xs. Além disso, os ys podem ser ordenados entre si usando qualquer ordem monomial desejada, mas os xs são ordenados conforme $>_c$. O novo problema a ser resolvido será $\mathrm{PI}_{B,\succ_c}$.

A primeira vantagem do problema estendido sobre $\mathrm{PI}_{A,>_c}$ é que ele tem uma solução óbvia para cada b; basta tomar

$$u = \begin{bmatrix} b \\ 0 \end{bmatrix}$$

já que

$$[I_m, A]u = [I_m, A] \begin{bmatrix} b \\ 0 \end{bmatrix} = b.$$

Além disso, é fácil determinar geradores para o ideal I_B, como mostra nosso próximo resultado.

PROPOSIÇÃO 7.5. *O ideal I_B do anel $\mathbb{Q}[x_1, \ldots, x_n, y_1, \ldots, y_m]$ é gerado pelo conjunto de binômios*

$$\{y^{Ae_j} - x_j : 1 \leq j \leq n\}.$$

em que e_j é o multi-índice que tem 1 na posição j e zeros em todas as demais posições.

DEMONSTRAÇÃO. Sabemos, por definição, que o ideal I_B é gerado pelos binômios da forma

$$y^{\eta} x^{\alpha} - y^{\theta} x^{\beta},$$

em que

$$[I_m, A] \begin{bmatrix} \eta - \theta \\ \alpha - \beta \end{bmatrix} = 0.$$

Como

$$0 = I_m(\eta - \theta) = \eta - \theta,$$

verificamos que $\eta = \theta$ e o binômio pode ser escrito na forma

$$f_{\alpha,\beta,\eta} = y^{\eta} x^{\alpha} - y^{\eta} x^{\beta},$$

em que $A\alpha = A\beta$.

Considere, agora, o ideal J do anel $\mathbb{Q}[x_1, \ldots, x_n, y_1, \ldots, y_m]$ gerado pelo conjunto

$$G = \{y^{Ae_j} - x_j : 1 \leq j \leq n\}.$$

A proposição estará provada se mostrarmos que $f_{\alpha,\beta,\eta} \in J$, para cada gerador $f_{\alpha,\beta,\eta}$ de I_B.

Para isto vamos trabalhar no anel $\mathbb{Q}[x_1, \ldots, x_n, y_1, \ldots, y_m]$ com a ordem lexicográfica dada por

$$x_1 >_{\text{lex}} x_2 >_{\text{lex}} \cdots x_n >_{\text{lex}} y_1 >_{\text{lex}} \cdots >_{\text{lex}} y_m.$$

A razão para adotar $>_{\text{lex}}$ é que

$$\text{in}_{\text{lex}}(y^{Ae_j} - x_j) = x_j.$$

Assim, calculando o S-polinômio entre $y^{Ae_j} - x_j$ e $y^{Ae_i} - x_i$, obtemos

$$S(y^{Ae_j} - x_j, y^{Ae_i} - x_i) = x_i y^{Ae_j} - x_j y^{Ae_i}$$

que, dividido por G dá resto zero. Portanto, pelo critério de Buchberger, G é uma base de Gröbner de J com respeito a lex.

Como $J \subseteq I_B$ e G é uma base de Gröbner de J, então $f_{\alpha,\beta,\eta} \in J$ se e somente se $\text{R}_G(f_{\alpha,\beta,\eta}) = 0$. Portanto, basta calcularmos este resto e a proposição estará provada.

Suponhamos que x_j seja a maior variável dentre os xs a aparecer em $f_{\alpha,\beta,\eta}$. Então, a primeira etapa do processo de divisão nos dá

$$f_{\alpha,\beta,\eta} - (y^\eta x^{\alpha - Ae_j})(x_j - y^{Ae_j}) = y^{\eta + Ae_j} x^{\alpha - Ae_j} - y^\eta x^\beta.$$

As etapas seguintes da divisão serão análogas a esta, e o processo continuará até que não haja nenhum x_j no dividendo. O resto obtido ao final deste procedimento será

$$y^{\eta + \alpha_j Ae_j} x^{\alpha - \alpha_j Ae_j} - y^{\eta + \beta_j Ae_j} x^{\beta - \beta_j Ae_j},$$

em que α_j e β_j são as j-ésimas coordenadas de α e β respectivamente. Portanto, ao dividir f por G, obteremos um resto independente dos xs e igual a

$$\text{R}_G(f_{\alpha,\beta,\eta}) = y^{\eta + \sum_{j=1}^n \alpha_j Ae_j} - y^{\eta + \sum_{j=1}^n \beta_j Ae_j}.$$

Contudo,

$$\sum_{j=1}^n \alpha_j Ae_j = A(\sum_{j=1}^n \alpha_j e_j) = A\alpha, \text{ e, analogamente, } \sum_{j=1}^n \beta_j Ae_j = A\beta.$$

Assim,

$$\text{R}_G(f_{\alpha,\beta,\eta}) = y^{\eta + A\alpha} - y^{\eta + A\beta}.$$

Entretanto, $A\alpha = A\beta$ pela definição de I_B, de modo que $\text{R}_G(f_{\alpha,\beta,\eta}) = 0$, como queríamos mostrar. □

Com isto sabemos que, para o problema estendido $\mathrm{PI}_{B,\succ_c}(b)$ é fácil calcular uma solução na região de possibilidade, e também é fácil achar um conjunto de geradores para I_B. Resta-nos, apenas, mostrar que se b pertence à região de possibilidade do problema, então a solução mínima de $\mathrm{PI}_{B,\succ_c}(b)$ coincide com a solução mínima de $\mathrm{PI}_{A,>_c}(b)$.

Como os ys superam todos os xs em $\succ_c$, então, se α é a menor solução possível de $\mathrm{PI}_{A,>_c}(b)$, teremos que $(0,\alpha)$ será a menor solução possível de $\mathrm{PI}_{B,\succ_c}(b)$ Contudo, pelo algoritmo 7.4, a solução mínima de $\mathrm{PI}_{A,>_c}(b)$ é obtida calculando o resto da divisão de y^b por uma base de Gröbner reduzida G de I_B. Portanto, teremos que

$$\mathrm{R}_G(y^b) = x^\alpha.$$

Note que se, inadvertidamente, escolhermos b de maneira que $Au = b$ não tem solução então o resto acima *não* será independente de y. Encerramos esta seção reformulando o algoritmo na forma em que será utilizado nas aplicações das próximas seções.

ALGORITMO 7.6 (Resolvendo $\mathrm{PI}_{A,>}(b)$). *Dada a matriz A, a função custo c e o vetor b, o algoritmo encontra a solução mínima de $\mathrm{PI}_{A,>_c}(b)$ pelo método de Conti e Traverso.*

Etapa 1: *Pré-processamento:*

- *Contrua o ideal I_B gerado pelos binômios da forma $y^{Ae_j} - x_j$, para $1 \leq j \leq n$ no anel $\mathbb{Q}[x_1, \ldots, x_n, y_1, \ldots, y_m]$.*
- *Calcule uma base de Gröbner reduzida G de I_B com respeito a $\succ_c$.*

Etapa 2: *Resolvendo* $\mathrm{PI}_{A,>_c}(b)$

- *Calcule* $\mathrm{R}_G(y^b) = y^\eta x^\beta$.
- *Se $\eta \neq 0$ então o problema não tem solução.*
- *Se $\eta = 0$, retorne β.*

5. Resolvendo os exemplos

Dos três problemas apresentados na seção 1, o método descrito até aqui nos permite resolver apenas um, o problema das promoções em uma loja de departamentos. Neste caso precisamos criar 14 variáveis, uma para cada promoção. Vamos chamá-las de $x_1, \ldots, x_{14}$, supondo que correspondem às promoções na ordem em que aparecem na tabela. Para usar o algoritmo de Conti e Traverso precisamos de mais 4 variáveis, digamos $y_1, \ldots, y_4$, uma para cada

produto. Definindo I_B como na seção anterior, os polinômios em I_B serão

$$\begin{aligned}
y_1^1y_2^0y_3^0y_4^0 - x_1 &= y_1 - x_1\\
y_1^0y_2^1y_3^0y_4^0 - x_2 &= y_2 - x_2\\
y_1^0y_2^0y_3^1y_4^0 - x_3 &= y_3 - x_3\\
y_1^0y_2^0y_3^1y_4^0 - x_4 &= y_4 - x_4\\
y_1^1y_2^1y_3^0y_4^1 - x_5 &= y_1y_2 - x_5\\
y_1^1y_2^0y_3^1y_4^0 - x_6 &= y_1y_3 - x_6\\
y_1^1y_2^0y_3^0y_4^1 - x_7 &= y_1y_4 - x_7\\
y_1^0y_2^1y_3^1y_4^0 - x_8 &= y_2y_3 - x_8\\
y_1^0y_2^1y_3^0y_4^1 - x_9 &= y_2y_4 - x_9\\
y_1^0y_2^0y_3^1y_4^1 - x_{10} &= y_3y_4 - x_{10}\\
y_1^1y_2^1y_3^1y_4^0 - x_{11} &= y_1y_2y_3 - x_{11}\\
y_1^1y_2^1y_3^0y_4^1 - x_{12} &= y_1y_2y_4 - x_{12}\\
y_1^1y_2^0y_3^1y_4^1 - x_{13} &= y_1y_3y_4 - x_{13}\\
y_1^0y_2^1y_3^1y_4^1 - x_{14} &= y_2y_3y_4 - x_{14}
\end{aligned}$$

Já a função custo corresponde à ordenação dos monômios de forma que os ys sejam sempre maiores que os xs, sendo os xs ordenados por $>_c$. Uma boa maneira de fazer isto é escolher uma ordem de eliminação em que:

- os ys são maiores que os xs;
- os ys são ordenados por glex;
- os xs são ordenados por uma ordem de pesos definida pelo vetor de pesos

$$(3, 4, 5, 6, 6, 6, 8, 7, 7, 10, 9, 10, 12, 13).$$

Para executar o problema num sistema de computação algébrica, calculamos uma base de Gröbner G para o ideal acima e depois reduzimos o monômio $y_1y_2y_3y_4$ por esta base. O resultado será x_6x_9, que corresponde a comprar as promoções AC e BD.

Ainda há um obstáculo no nosso caminho antes de podermos resolver os outros dois exemplos. Em ambos, queremos maximizar uma função ℓ, mas fazemos isto minimizando $-\ell$, o que introduz coeficientes negativos. Como já vimos antes, a ordem de pesos definida com coeficientes negativos não é monomial, porque vão existir multi-índices α para os quais $x^\alpha < 1$. Infelizmente isto significa que o algoritmo de divisão pode vir a não parar sob uma ordem destas, o que poria o algoritmo de Buchberger em um laço infinito. Para nossa sorte isto não pode acontecer sob as hipóteses que adotamos.

PROPOSIÇÃO 7.7. *Suponha que $>$ é uma ordem compatível com c. Sejam $x^\alpha - x^\beta$ um binômio com $A\alpha = A\beta = b$ e $G \subseteq \mathcal{B}_A$. Se $\mathrm{P}_A(b)$ for finito, então o algoritmo de divisão aplicado a $x^\alpha - x^\beta$ e G vai parar sempre, depois de uma quantidade finita de etapas.*

DEMONSTRAÇÃO. Argumentando como na demonstração do teorema 7.3, vemos que, como o algoritmo de divisão é recursivo e, em cada etapa, efetua apenas a divisão de um polinômio por outro, então basta considerar o caso em que estamos dividindo $x^\alpha - x^\beta$ por um binômio qualquer de $x^\eta - x^\theta \in \mathcal{B}_A$. Digamos que $x^\alpha > x^\beta$ e que $x^\eta > x^\theta$.

Ao dividir $x^\alpha - x^\beta$ por $x^\eta - x^\theta$ basta considerar o caso em que x^α é divisível por x^η porque, caso contrário, não há nenhuma divisão a ser efetuada e o processo pára. Mas, isto significa que existe γ tal que $\alpha = \eta + \gamma$, de modo que ao final da primeira etapa da divisão teremos

$$x^\alpha - x^\gamma(x^\eta - x^\theta) = x^{\gamma+\theta}$$

como novo dividendo. Note que, como c é linear, então, $\alpha = \eta + \gamma$ e $x^\eta > x^\theta$ implicam que

$$x^{\gamma+\eta} > x^{\gamma+\theta}.$$

Portanto, tanto $x^{\gamma+\theta}$ quanto x^β são menores que x^α. Assim, os termos iniciais dos dividendos são progressivamente menores, ao longo do processo de divisão. Além disso,

$$b = A\alpha = A(\eta + \gamma) = A\eta + A\gamma.$$

Contudo, $A\eta = A\theta$, e portanto,

$$b = A\theta + A\gamma = A(\theta + \gamma).$$

Mostramos assim que, se $x^\alpha - x^\beta$ satisfaz $A\alpha = A\beta = b$ então ao longo de todo o processo de divisão, cada novo dividendo que surge tem que ser da forma $x^\rho - x^\phi$, em que $A\rho = A\phi = b$. Portanto, há uma quantidade finita de binômios que podem aparecer desta forma porque $\mathrm{P}_A(b)$ é finito. Entretanto, estes dividendos são sempre menores com respeito a $>$ e, portanto, não podem se repetir. Com isto o processo de divisão tem que parar, e a proposição está provada. □

Esta proposição significa que, sempre que $\mathrm{P}_A(b)$ for finito, podemos aplicar o algoritmo de Conti e Traverso, mesmo sabendo que a ordem que está sendo definida não é monomial. Além disso, pela proposição 7.1, isto acontece sempre que

$$\mathrm{N}_{\mathbb{Z}}(A) \cap \mathbb{N} = \{0\}$$

o que é relativamente fácil de verificar. Por exemplo, basta que *todos* os coeficientes de A sejam positivos para que esta última hipótese seja verificada. Isto põe a solução do primeiro problema da seção 1 imediatamente ao nosso alcance.

Neste caso a matriz do problema na forma padrão é dada por

$$A = \begin{bmatrix} 4 & 5 & 1 & 0 \\ 2 & 3 & 0 & 1 \end{bmatrix},$$

conforme vimos na seção 2, e a função custo por

$$c(a, p) = -\ell = -11a - 15p,$$

em que a e p são as variáveis do problema. Portanto, o ideal I_B será um ideal do anel $\mathbb{Q}[x_1, x_2, x_3, x_4, y_1, y_2]$ com geradores

$$y_1^4 y_2^2 - x_1,\ y_1^5 y_2^3 - x_2, y_1 - x_3 \text{ e } y_2 - x_4.$$

A ordem sob a qual faremos os cálculos da base de Gröbner será dada por

- $y_1 > y_2 > x_1 > x_2$;
- y_1 e y_2 são ordenados por glex;
- x_1 e x_2 são ordenados por uma ordem de pesos definida pelo vetor de pesos
$$(-11, -15).$$

Calculando a base de Gröbner usando um sistema de computação algébrica, obtemos os seguintes polinômios

$$y_1 - x_3,\ x_3^4 x_4^2 - x_1, x_1 x_3 x_4 - x_2,\ x_2 x_3^3 x_4 - x_1^2,$$
$$x_2 x_3^2 - x_1^3,\ x_1^4 x_4 - x_2^2 x_3 \text{ e } y_2 - x_4.$$

Para saber qual o valor mínimo precisamos calcular o resto de $y_1^{37} y_2^{20}$ por G, o que nos dá $x_1^4 x_2^4 x_3$. Portanto, uma solução mínima corresponde a levar 4 caixas para Paraty e 4 para Angra.

Finalmente, para converter o problema da mochila para a forma da entrada usada no algoritmo de Conti e Traverso precisamos de 13 variáveis: as 6 primeiras corresponderão às variáveis u do problema original, às seis seguintes às variáveis v e a última ao w. Por outro lado, precisamos introduzir 7 variáveis y, tantas quantas são as equações do problema original. Assim, o ideal I_B será gerado pelos binômios

$$\begin{array}{cccc} y_1^3 y_2 - x_1 & y_1^2 y_3 - x_2 & y_1^5 y_4 - x_3 & y_1^4 y_5 - x_4 \\ y_1^7 y_6 - x_5 & y_1^4 y_7 - x_6 & y_2 - x_7 & y_3 - x_8 \\ y_4 - x_9 & y_5 - x_{10} & y_6 - x_{11} & y_7 - x_{12} \\ y_1 - x_{13} & & & \end{array}$$

Já a ordem sob a qual faremos os cálculos da base de Gröbner será dada por

- os $y_1 > \cdots > y_7 > x_1 > \cdots > x_{13}$;
- os ys serão ordenados por glex;
- os xs serão ordenados por uma ordem definida pelo vetor de pesos
$$(-9, -13, -10, -15, -12, -17).$$

Utilizando um sistema de computação algébrica, verificamos que a base de Gröbner G de I_B com respeito a esta ordem tem 51 elementos. Determinando o resto de $y_1^{20}y_2y_3y_4y_5y_6$ por G, encontramos

$$x_2x_3x_4x_5x_7x_{13}^2,$$

que corresponde à solução

$$u_a = u_f = 0 \text{ e } u_b = u_c = u_d = u_e = 1.$$

6. Comentários e complementos

Como o algoritmo de Conti e Traverso depende do cálculo da base de Gröbner de um sistema bastante grande usando uma ordem de eliminação, é fácil imaginar que vai tornar-se bastante lento e ineficiente rapidamente. Levando em conta que os problemas de programação inteira que surgem no mundo real tendem a envolver uma quantidade enorme de variáveis, pode parecer que este método tem mais interesse teórico do que prático. Contudo, há ainda muita coisa que poderíamos fazer para tornar o algoritmo mais rápido.

Uma solução é evitar a introdução de novas variáveis (e consequentemente da ordem de eliminação) proposta pelo algoritmo de Conti e Traverso. Para isso, bastaria implementar o algoritmo 7.4. Contudo, vimos que, nesta formulação, o algoritmo incorre em dois problemas, já que antes de chegar a aplicar as bases de Gröbner precisamos encontrar um conjunto de geradores para o ideal I_A e alguma solução de $\mathrm{PI}_{A,>}(b)$. O primeiro destes problemas pode ser facilmente resolvido, e uma implementação que faz isto é apresentada em [**38**]. Escolhemos não discutir este enfoque aqui porque demanda um conhecimento de resultados mais sofisticados de álgebra, inclusive de algoritmos que não estão diretamente relacionados ao estudo de polinômios e bases de Gröbner, o que nos desviaria para muito além de nossa meta.

Outra maneira de acelerar estes procedimentos é implementando uma versão do algoritmo de Buchberger que calcula diretamente com os vetores de $\mathbb{N}^n$ (os multi-índices), em vez de tomar os polinômios a eles associados. Algoritmos que utilizam deste enfoque são discutidos em [**64**] e [**67**].

Finalmente, o método de bases de Gröbner é especialmente útil na solução de certas classes de problemas de programação inteira, um dos quais é discutido em [**54**].

7. Exercícios

1. Determine o máximo da função custo

$$c(x_1, x_2, x_3, x_4) = 1000x_1 + x_2 + x_3 + 100x_4,$$

sujeita às restrições

$$3x_1 - 2x_2 + x_3 - x_4 = -1 \text{ e } 4x_1 + x_2 - x_3 = 5.$$

2. Determine o máximo da função custo
$$c(x_1, x_2, x_3, x_4) = x_1 + 1000x_2 + x_3 + x_4,$$
sujeita às mesmas restrições do problema anterior.

3. Determine o máximo da função custo
$$c(x_1, x_2, x_3, x_4) = 2x_1 + 4x_2 + 3x_3 + x_4$$
sujeita às restrições
$$\begin{aligned} 3x_1 + x_2 + 4x_3 + x_4 &= 3 \\ x_1 - 3x_2 + 2x_3 + 3x_4 &= 3 \\ 2x_1 + x_2 + 3x_3 - x_4 &= 6. \end{aligned}$$

4. Modele e resolva o seguinte problema usando métodos de programação linear:

   Digamos que temos 14 mil reais para investir e que há quatro oportunidades de investimento que pretendemos considerar. A primeira requer 5 mil reais e vale atualmente 8 mil reais; a segunda requer 7 mil reais e vale 11 mil; a terceira requer 4 mil reais e vale 6 mil e a quarta requer 3 mil reais e vale 4 mil. Em quais destes investimentos devemos por nosso dinheiro de modo a maximizar nosso valor atual?

5. De que modo podemos formular as seguintes restrições no contexto do problema acima:
   (a) podemos fazer apenas um investimento;
   (b) se fizermos o investimento 2 então o investimento 4 também tem que ser feito;
   (c) se fizermos o investimento 1 então o investimento 3 não pode ser feito;

6. Sejam $x_1, \ldots, x_n$ variáveis binárias. Modele as seguintes afirmações em termos de equações ou inequações nestas variáveis:
   (a) ocorre, no máximo um dos eventos;
   (b) ou nenhum dos eventos ocorre, ou ocorrem ambos;
   (c) se o primeiro evento ocorre, então o segundo também ocorre.

7. Modele e resolva o seguinte problema usando métodos de programação linear:

   Uma mulher carregava uma cesta de ovos para o mercado quando um rapaz esbarrou nela, fazendo com que deixasse a cesta cair, quebrando todos os ovos. Consternado, o rapaz lhe pergunta quantos ovos havia na cesta para poder ressarcir o prejuízo. "Não sei exatamente, lhe responde a mulher. Mas lembro que sobrava sempre uma ovo quando eu os separava em grupos de 2,3,4,5 ou 6. Já quando tire-os da cesta de sete em sete, não sobrou nenhum ovo". Qual a quantidade mínima de ovos que havia na cesta?

8. Modele e resolva o seguinte problema usando métodos de programação linear:

   Uma livraria tem a seguinte política de descontos. Comprando r reais em livros, você tem um disconto de $r/10$ %. Portanto, se você comprar três livros ao custo de 10, 20 e 30 reais cada, será melhor negócio comprar o livro que custa 30 reais primeiro, no dia seguinte o que custa 20 e, em seguida, o que custa 10 reais, do que comprar primeiro o que custa 10, depois o que custa 20 e por fim o que custa 30. Suponha, então, que você precisa comprar cinco livros que custam, respectivamente 10, 20, 30, 40 e 50 reais. Qual a melhor maneira de distribuir as compras de modo a minimizar o custo total?

   SUGESTÃO: Sejam $1 \leq i, j \leq 5$. Chame de x_{ij} a variável que vale um se o livro que vale $10i$ reais foi comprado no dia j e, caso contrário, vale zero e de t_j a variável que corresponde ao valor total dos livros comprados no dia j. Se c_i representa o custo do i-ésimo livro, então queremos minimizar

$$\sum_{i=1}^{5} c_i - \sum_{k=2}^{5} t_{k-1} t_k$$

   sob as condições

$$t_j = \sum_{i=1}^{5} c_i x_{i,j} \text{ e } \sum_{i=1}^{5} x_{i,j} = 1, \text{ para } 1 \leq j \leq 5.$$

9. Modele o seguinte problema usando métodos de programação linear:

   Suponha que n computadores estão interligados entre si em um prédio térreo. Os cabos que interligam os computadores são subterrâneos e o custo de interligar o computador i ao computador j é conhecido e vale c_{ij}. De que maneira os computadores devem ser interligados, de maneira que o custo de estender os cabos seja mínimo e que nenhum computador fique fora da rede?

10. Resolva o problema acima no caso em que há cinco computadores e que o custo de interligá-los é dado na tabela abaixo

	1	2	3	4	5
1	*	1	4	6	2
2	1	*	3	*	2
3	4	3	*	5	2
4	6	*	5	*	4
5	2	2	2	4	*

   As casas marcadas com * correspondem a interligações que não são viáveis por causa da geografia do local onde os computadores foram instalados.

CAPíTULO 8

Anéis quocientes e homomorfismos

Neste capítulo descreveremos a construção dos anéis quocientes e veremos como aplicar bases de Gröbner para calcular nestes anéis. Esta construção será aplicada no próximo capítulo ao estudo dos sistemas com uma quantidade finita de soluções.

1. Inteiros módulares

Começamos relembrando a construção dos inteiros modulares, já que nossa meta consiste em generalizá-la a um anel qualquer. Em primeiro lugar, precisamos escolher um inteiro positivo n que será o módulo da construção. Em seguida, usamos n para definir uma relação de equivalência. Se $a, b \in \mathbb{Z}$, esta relação é dada pela regra

$$a \equiv b \pmod{n}, \text{ se e somente se, } a - b \text{ é múltiplo de } n.$$

Observe que podemos facilmente reescrever esta definição em termos de ideais de $\mathbb{Z}$, dizendo que

$$a \equiv b \pmod{n}, \text{ se e somente se, } a - b \in \langle n \rangle. \tag{56}$$

Como esta é uma relação de equivalência, o anel $\mathbb{Z}$ se decompõe em uma união disjunta de classes de equivalência, que neste caso serão

$$\overline{0}, \overline{1}, \ldots, \overline{n-1}.$$

O conjunto cujos elementos são estas classes de equivalência é conhecido por *conjunto quociente* de $\mathbb{Z}$ pela relação de congruência módulo n. Este é o conjunto usualmente denotado por $\mathbb{Z}_n$.

Na verdade, $\mathbb{Z}_n$ é mais que um mero conjunto, já que herda as operações de $\mathbb{Z}$, o que faz dele um anel. Mais precisamente, podemos somar e multiplicar classes de $\mathbb{Z}_n$ usando as fórmulas

$$\overline{a} + \overline{b} = \overline{a+b} \quad \text{e} \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b},$$

em que $\overline{a}, \overline{b} \in \mathbb{Z}_n$. Há várias coisas que precisamos verificar antes de nos dar por satisfeitos de que as operações assim definidas fazem de $\mathbb{Z}_n$ um anel. A mais óbvia é que as várias propriedades das operações de um anel têm que valer em $\mathbb{Z}_n$. Contudo, isto é fácil de fazer, uma vez que $\mathbb{Z}$ é um anel, e as propriedades das operações modulares seguem das propriedades correspondentes das operações com inteiros.

Menos óbvia é a necessidade de verificar que as regras acima estão bem definidas. Lembre-se que isto decorre do fato de que as operações com classes são definidas a partir de representantes das classes. Assim, precisamos provar que, ao escolher representantes diferentes, as classes resultantes da aplicação das operações não são alteradas. Logo voltaremos a esta questão, no âmbito mais geral dos anéis quocientes.

Resumindo:

- Para efetuar a construção de $\mathbb{Z}_n$ precisamos apenas de um inteiro positivo n; além do anel $\mathbb{Z}$, é claro!
- Utilizando a linguagem da teoria de anéis, podemos dizer que na definição da congruência, n é representado pelo ideal $\langle n \rangle$.
- A congruência deve dar lugar a uma relação de equivalência no anel $\mathbb{Z}$, para que possamos definir o conjunto quociente $\mathbb{Z}_n$.
- Precisamos de regras que nos permitam obter operações bem definidas no conjunto quociente $\mathbb{Z}_n$.
- Finalmente, precisamos verificar que as operações, como definidas, fazem do conjunto quociente um anel.

2. Anéis quocientes

Digamos que queremos generalizar a construção dos inteiros modulares a um anel comutativo qualquer A. A primeira coisa que o resumo do final da seção anterior sugere é que, para isso, precisamos de um ideal I de A. A próxima etapa, naturalmente, é a generalização da relação de congruência. Note que, se $a, b \in A$, faz sentido copiar a definição (56), substituindo apenas $\langle n \rangle$ por I. Fazendo isto, obtemos

$$a \equiv b \pmod{I}, \text{ se e somente se, } a - b \in I. \tag{57}$$

Chamaremos esta relação de *congruência módulo* I.

O surpreendente é que isto basta: esta é, de fato, uma relação de equivalência em I. Com efeito, as propriedades que fazem de I um ideal correspondem, uma a uma, àquelas que fazem da congruência uma relação de equivalência. Em primeiro lugar, $0 \in I$; o que significa que, qualquer que seja $a \in A$, a diferença $a - a = 0 \in I$. Reescrevendo em termos da congruência, isto nos dá que $a \equiv a \pmod{n}$; isto é, a congruência módulo I é reflexiva.

Para provar a simetria precisamos de dois elementos $a, b \in A$, que suporemos congruentes módulo n. Mas, $a \equiv b \pmod{I}$ nos diz que $a - b \in I$. Contudo,

$$b - a = (-1) \cdot (a - b) \in I,$$

já que o produto de qualquer elemento de I por algum elemento de A volta a estar em I. Mas isto é o mesmo que dizer que $b \equiv a \pmod{I}$. Finalmente, para a transitiva, tomamos

$$a \equiv b \pmod{I} \text{ e } b \equiv c \pmod{I},$$

com $a, b, c \in I$. Estas duas congruências correspondem, pela definição (57), às inclusões

$$a - b \in I \text{ e } b - c \in I.$$

Entretanto, a soma de elementos de I também pertence a I, de modo que

$$a - c = (a - b) + (b - c) \in I,$$

que é equivalente a $a \equiv c \pmod{I}$, completando, assim, nossa demonstração de que a congruência módulo I é uma relação de equivalência em A.

Talvez você esteja tentado a gritar "blefe!". Afinal, é meio exagerado dizer que a simetria da congruência "corresponde" ao fato de que dados $a \in A$ e $b \in I$, vale $ab \in I$. Na verdade, para provar a simetria usamos apenas que se $b \in I$ então $-b \in I$, o que é muito mais fraco. Se você está familiarizado com o jargão da álgebra moderna podemos reformular esta observação de maneira mais precisa dizendo que:

> para a definição (57) dar lugar a uma relação de equivalência, não é necessário que I seja um ideal, basta que seja um subgrupo aditivo de A.

Jargões à parte, logo usaremos com força total o fato de I ser ideal. Portanto, o blefe é só meio blefe.

Agora que temos a definição da congruência, podemos considerar o conjunto quociente de A pela congruência módulo I. Os elementos deste conjunto são as classes de equivalência. Mais precisamente, dado $a \in A$, definimos a classe de a por

$$\overline{a} = \{b \in A : a \equiv b \pmod{I}\}.$$

Como $b \equiv a \pmod{I}$ é equivalente a dizer que $b = a + x$, onde $x \in I$, podemos reescrever este conjunto na forma

$$\overline{a} = \{a + x : x \in I\}.$$

Por isso, a classe $\overline{a}$ também é denotada por $a + I$. Por sua vez, o conjunto quociente de A pela de congruência módulo I, que será denotado por A/I, tem por elementos as classes $\overline{a}$, com $a \in A$.

Para transformar A/I em um anel, precisamos definir operações de adição e multiplicação em A/I. Faremos isto usando exatamente as mesmas regras já utilizadas para o anel dos inteiros módulo n. Portanto, se $a, b \in A$, definimos

$$\overline{a} + \overline{b} = \overline{a + b} \quad \text{e} \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

Note que isto significa que, para somar a classe de a com a classe de b em A/I, somamos a com b e tomamos a classe correspondente. Em outras palavras, a classe correspondente à soma $\overline{a} + \overline{b}$ é obtida a partir da soma de elementos em A. Ocorre que podemos representar $\overline{a}$ por um elemento diferente, digamos a'. Isto é, podemos ter que $a \neq a'$, embora $\overline{a} = \overline{a'}$. Contudo, para que a soma de *classes* esteja bem definida é preciso que não faça diferença se usamos a ou a' como representante para a classe, já que ambos representam a mesma classe. Portanto, sempre que $\overline{a} = \overline{a'}$, devemos poder concluir que

$\overline{a+b} = \overline{a'+b}$. De maneira semelhante, é necessário que, se a e a' representem a mesma classe, então $\overline{ab} = \overline{a'b}$. Verificaremos a afirmação referente à multiplicação e deixaremos a que corresponde à adição para você fazer como exercício.

Em primeiro lugar, $\overline{a} = \overline{a'}$ significa que $a - a' \in I$. Como I é um ideal, qualquer elemento de A multiplicado por um elemento de I é absorvido por I. Assim,

$$ba - ba' = b(a - a') \in I.$$

Traduzindo isto em termos de classes, obtemos $\overline{ab} = \overline{a'b}$. Concluímos assim que,

$$\text{se } \ \overline{a} = \overline{a'} \ \text{ então } \ \overline{ab} = \overline{a'b};$$

de modo que a multiplicação não depende do representante escolhido para a classe. Note que, desta vez, usamos a propriedade do ideal absorver elementos por multiplicação com toda a sua força. Em outras palavras, se I não satisfizesse esta propriedade, a multiplicação acima não estaria bem definida.

Chegados a este ponto, temos um conjunto A/I, onde definimos uma adição e uma multiplicação. Para poder garantir que A/I é um anel ainda nos resta verificar que as propriedades listadas no capítulo 2 são satisfeitas. Identificar os elementos neutros é muito fácil, já que se $\overline{a} \in A/I$, então, pelas definições acima

$$\overline{a} + \overline{0} = \overline{a+0} = \overline{a} \quad \text{e} \quad \overline{a} \cdot \overline{1} = \overline{a \cdot 1} = \overline{a}.$$

Portanto, $\overline{0}$ é o elemento neutro da soma, e $\overline{1}$ o da multiplicação. Todas as demais propriedades das operações de A/I seguem das propriedades correspondentes para A. A verificação é fácil mas tediosa, por isto vamos omiti-la. Dito isto, podemos finalmente declarar que A/I, com as operações definidas acima, é um anel: o *anel quociente* de A pelo ideal I.

3. Exemplos

Para entender de maneira satisfatória a noção de anel quociente precisamos calcular alguns exemplos. O mais simples de todos é nosso velho conhecido, o anel dos inteiros módulo n. Como estamos nos concentrando neste livro no estudo dos anéis de polinômios, todos os nossos outros exemplos virão deste domínio.

Começamos com o caso mais simples, em que o anel de polinômios tem apenas uma variável x, e o anel de base é um corpo K. Neste caso, pelo teorema 2.3 basta considerar o caso em que o ideal é gerado por um polinômio $g \in K[x]$. Seja, portanto, $I = \langle g \rangle$, e vamos calcular a classe $\overline{f}$ de um polinômio $f \in K[x]$. Procederemos de maneira muito semelhante ao que se faz ao estudar as classes da congruência modular sobre $\mathbb{Z}$. Assim, dividimos f por g em $K[x]$, obtendo polinômios $q, r \in K[x]$ tais que

$$f = gq + r \ \text{ onde } \ r = 0 \ \text{ ou } \ \operatorname{grau}(r) < \operatorname{grau}(g).$$

Disto, obtemos

$$f - r = gq \in \langle g \rangle = I;$$

de modo que $\overline{f} = \overline{r}$. Logo, toda classe em $K[x]/I$ pode ser representada por um polinômio de grau menor que o grau de g. Para facilitar, digamos que g tem grau m.

Podemos ser ainda mais precisos em nossa caracterização. Digamos que r_1 e r_2 são dois polinômios em $K[x]$ de grau menor que m. Se $\overline{r_1} = \overline{r_2}$, então $r_1 - r_2$ tem que ser um múltiplo de g, que tem grau m. Mas isto só é possível se $r_1 - r_2 = 0$; donde $r_1 = r_2$. Desta forma, podemos refinar nossa afirmação anterior, dizendo que toda classe em $K[x]/I$ tem sempre um representante, *e apenas um*, entre os polinômios de grau menor que m.

Por enquanto vamos deixar o caso de uma variável neste pé. Na seção 5 identificaremos alguns destes anéis com objetos mais conhecidos. Antes de prosseguir com os exemplos, precisamos de algumas definições.

Seja A um anel qualquer. O maior ideal de A é o próprio A; assim como o menor é sempre 0. Naturalmente, ao dizer "maior" e "menor", estamos comparando estes ideais usando a relação de inclusão de conjuntos. Isto significa que o maior ideal de um anel não é muito interessante, porque pouco diz sobre este anel. Por isso, ao invés de olhar para o maior ideal, consideramos aqueles ideais que estão imediatamente abaixo de A. Mais precisamente, temos a seguinte definição.

Um ideal próprio $\mathfrak{m}$ de um anel A é máximo se não existe nenhum ideal próprio de A que contenha $\mathfrak{m}$. Isto é, entre $\mathfrak{m}$ e A não existe nenhum outro ideal. Um exemplo simples é o ideal $\mathfrak{m}$ gerado pelas variáveis no anel de polinômios $K[x_1, \ldots, x_n]$. Para provar que este ideal é máximo, tome

$$f \in K[x_1, \ldots, x_n] \setminus \mathfrak{m}$$

Mas os elementos de $\mathfrak{m}$ são aqueles polinômios cujo fator constante é nulo; como $f \notin \mathfrak{m}$, temos que

$$f(0) = a \neq 0, \text{ donde } (f - a)(0) = 0.$$

Assim, obtemos

$$f - a \in \mathfrak{m}. \tag{58}$$

Portanto, se houvesse um ideal I contendo f e $\langle x_1, \ldots, x_n \rangle$, teríamos que

$$a = f - (f - a) \in I.$$

Como a é uma constante não nula, concluímos que, sob estas hipóteses, $I = K[x_1, \ldots, x_n]$. Portanto, $\mathfrak{m}$ é mesmo um ideal máximo.

A equação (58) nos ajuda na descrição do quociente $K[x_1, \ldots, x_n]/\mathfrak{m}$. De fato, pela definição da congruência módulo um ideal, temos que

$$f - a \in \mathfrak{m} \text{ equivale a dizer que } f \equiv a \pmod{\mathfrak{m}}.$$

Desta forma, a classe de f tem $a = f(0)$ como representante. Em particular, cada classe é representada por uma, e apenas uma, constante de K. Além disso, como os elementos de K são invertíveis em $K[x_1, \ldots, x_n]$, também serão invertíveis em $K[x_1, \ldots, x_n]/\mathfrak{m}$. Portanto, este anel quociente é um

corpo. Afinal de contas, isto não parece muito surpreendente, já que os elementos do quociente são representados pelos elementos de K. Com efeito, nos sentimos tentados mesmo a dizer que $K[x_1, \ldots, x_n]/\mathfrak{m}$ é "igual" a K. O único problema é que os elementos de K e as classes que representam no quociente $K[x_1, \ldots, x_n]/\mathfrak{m}$ não são a mesma coisa. Mais uma vez será necessário esperar chegarmos à seção 5 para esclarecer este ponto de maneira satisfatória.

Continuando sob o mesmo tema, a próxima proposição provê uma caracterização completa dos ideais máximos do anel de polinômios em uma variável sobre um corpo.

PROPOSIÇÃO 8.1. *Seja $f \in K[x]$ um polinômio. O ideal principal gerado por f é máximo se, e somente se, f é irredutível.*

DEMONSTRAÇÃO. Suponhamos que I é um ideal de $K[x]$ tal que

$$\langle f \rangle \subsetneq I \subset K[x].$$

Como todo ideal de $K[x]$ é principal, temos que $I = \langle g \rangle$, para algum polinômio g. Mas isto implica que $f = gq$, para algum $q \in K[x]$. Como $\langle f \rangle$ está propriamente contido em I, o polinômio q não pode ser constante; do contrário I seria igual a $K[x]$. Logo, g é um fator próprio de f se, e somente se, gera um ideal próprio de $K[x]$ que contém $\langle f \rangle$. Portanto, $\langle f \rangle$ é máximo se, e somente se, f não tem fatores próprios. □

O resultado acima é falso se o anel de polinômios tiver várias indeterminadas. De fato, x_1 é irredutível em $K[x_1, x_2]$; contudo

$$\langle x_1 \rangle \subsetneq \langle x_1, x_2 \rangle \subsetneq K[x_1, x_2].$$

Entretanto, há uma propriedade que é compartilhada pelos ideais máximos e pelos ideais gerados por polinômios irredutíveis de $K[x_1, \ldots, x_n]$ e que, dada a sua importância, merece um nome especial. Um ideal P de um anel A é *primo* se, dados $a, b \in A$ tais que $ab \in P$, sempre temos que $a \in P$ ou $b \in P$.

Como veremos na proposição 8.2, todo ideal máximo é primo. Contudo, a recíproca é falsa. Por exemplo, o ideal gerado por x_1 em $K[x_1, x_2]$ é primo, mas não é máximo, já que está contido em $\langle x_1, x_2 \rangle$. Para provar a primalidade de $\langle x \rangle$, suponha que f e g são polinômios de $K[x_1, x_2]$ tais que

$$fg \in \langle x_1 \rangle,$$

então

$$f(0, x_2)g(0, x_2) = fg(0, x_2) = 0.$$

Mas isto implica que $f(0, x_2) = 0$ ou $g(0, x_2) = 0$; no primeiro caso $f \in \langle x_1 \rangle$, no segundo $g \in \langle x_1 \rangle$. Portanto, os conceitos de ideal máximo e ideal primo, apesar de estreitamente relacionados, não coincidem.

Você deve estar imaginando se *ideal primo* tem algo a ver com *número primo*. A resposta é sim. A estrutura de ideais do anel $\mathbb{Z}$ é muito semelhante ao de um anel de polinômios em uma variável sobre um corpo. Em particular, todo ideal de $\mathbb{Z}$ é principal; veja exercício ????. Um argumento semelhante ao

que utilizamos na proposição 8.1 mostra então que o ideal $\langle p\rangle \subseteq \mathbb{Z}$ é máximo se, e somente se, p é um número primo.

Ideais primos e ideais máximos podem ser igualmente bem definidos a partir das propriedades de seus anéis quocientes, como mostramos na próxima proposição.

PROPOSIÇÃO 8.2. *Seja A um anel e I um ideal de A.*

(1) $\sqrt{I} = I$ *se, e somente se, o quociente A/I não tem elementos nilpotentes.*
(2) I *é um ideal primo se, e somente se, o quociente A/I é um domínio.*
(3) I *é um ideal máximo se, e somente se, o quociente A/I é um corpo.*
(4) *Todo ideal máximo é primo.*

DEMONSTRAÇÃO. (1) e (2) seguem imediatamente das respectivas definições, e ficam como exercício. Provaremos apenas (3) e (4).

Suponhamos, primeiramente, que o ideal I é máximo. Se a for um elemento do anel A que não pertence a I, consideramos o ideal $\langle a, I\rangle$ gerado por a e por todos os elementos de I. Como a pertence a $\langle a\rangle + I$ mas não a I, temos que

$$I \subsetneq \langle a, I\rangle \subset A.$$

Contudo, I é máximo, de modo que devemos ter $\langle a, I\rangle = A$. Como $1 \in A$, esta igualdade implica que existem elementos $\alpha \in A$ e $i \in I$, tais que $\alpha a + i = 1$. Da igualdade destes elementos, segue a igualdade de suas classes, de modo que

$$\overline{1} = \overline{\alpha a + i} = \overline{\alpha a} + \overline{i} = \overline{\alpha a},$$

já que $\overline{i} = \overline{0}$. Concluímos que, se $\overline{a} \neq \overline{0}$ então tem inverso em A/I. Mas isto implica que este anel quociente é um corpo.

Para a recíproca, suponhamos que o quociente A/I é um corpo, e seja J um ideal de A que contém I propriamente. Mas isto implica que existe um elemento a em J que não pertence a I. Contudo, $a \notin I$ implica que $\overline{a} \neq \overline{0}$. Como A/I é um corpo, $\overline{a}$ deve ter um inverso $\overline{\alpha}$ em A/I. Isto é, $\overline{\alpha a} = \overline{1}$, que é equivalente a dizer que $\alpha a - 1 \in I$. Contudo $I \subsetneq J$ implica que $\alpha a - 1 \in J$. Porém, escolhemos $a \in J$, o que nos prmite concluir que $1 \in J$, ou $J = A$. Assim, o único ideal que contém I propriamente é A, o que é equivalente a dizer que I é máximo. Finalmente, como todo corpo é um domínio, (4) segue imediatamente de (2) e (3). □

Nosso último exemplo nesta seção é o quociente do anel $\mathbb{R}[x_1, x_2]$ pelo ideal principal gerado pelo polinômio $g = x_1^3 - x_2^2$. Considerado como polinômio em x_1 com coeficientes em $\mathbb{R}[x_2]$, este polinômio é mônico. Com isso, podemos facilmente dividir qualquer polinômio $f \in \mathbb{R}[x_1, x_2]$ por g, o que aliás já fizemos na página 80. Lá, vimos que

$$f = gq + r \text{ onde } \ r = 0 \text{ ou } \ r = ax_2 + b,$$

para alguma escolha de polinômios $a, b \in \mathbb{R}[x_1]$. Observe que a e b são polinômios que contêm apenas a variável x_1. Reescrevendo tudo isto em termos de $\mathbb{R}[x_1, x_2]/\langle g\rangle$, vemos que toda classe não nula deste quociente pode ser escrita

na forma $\overline{ax_2 + b}$, onde $a, b \in \mathbb{R}[x_1]$. Além disso, esta representação de uma dada classe é única, por um argumento que usa o grau, como no caso de uma variável discutido acima.

Esta maneira de representar as classes de $\mathbb{R}[x_1, x_2]/\langle x_1^3 - x_2^2\rangle$ nos permite efetuar cálculos explícitos com os seus elementos. Como a adição é imediata, trataremos apenas da multiplicação. Sejam, pois, $a_1, b_1, a_2, b_2 \in \mathbb{R}[x_1]$ e consideremos as classes $\overline{a_1x_2 + b_1}$ e $\overline{a_2x_2 + b_2}$ em $\mathbb{R}[x_1, x_2]/\langle x_1^3 - x_2^2\rangle$. Efetuando sua multiplicação, obtemos

$$(\overline{a_1x_2 + b_1}) \cdot (\overline{a_2x_2 + b_2}) = \overline{a_1a_2x_2^2 + (a_1 + a_2)x_2 + b_1b_2}. \tag{59}$$

Contudo, $\overline{x_1^3 - x_2^2} = \overline{0}$, já que este polinômio gera o ideal. Mas isto significa que

$$\overline{x_1}^3 - \overline{x_2^2} = \overline{0} \text{ donde } \overline{x_2^2} = -\overline{x_1}^3.$$

Substituindo em (59), obtemos

$$(\overline{a_1x_2 + b_1}) \cdot (\overline{a_2x_2 + b_2}) = \overline{(a_1b_2 + a_2b_1)x_2 + (b_1b_2 + a_1a_2\overline{x_1}^6)}. \tag{60}$$

Uma pergunta razoável é se este anel quociente é um domínio. A resposta é sim, como veremos ao final da próxima seção.

4. Homomorfismos

Nesta seção veremos como comparar dois anéis. Ignorando a natureza de que são feitos os elementos, diremos que dois anéis são equivalentes (ou isomorfos) se têm as mesmas propriedades algébricas. Para tornar isto mais preciso introduzimos aplicações entre anéis que preservam as suas operações.

Sejam A e B anéis. Uma aplicação $\phi : A \to B$ é um *homomorfismo* se, quaisquer que sejam $a, a' \in A$, temos que

- $\phi(a + a') = \phi(a) + \phi(a')$,
- $\phi(a \cdot a') = \phi(a) \cdot \phi(a')$,

e além disso $\phi(1) = 1$. Esta última propriedade nos diz que ϕ leva a identidade de A na identidade de B.

Na definição acima há uma assimetria curiosa entre soma e multiplicação. Afinal, da primeira propriedade temos que

$$\phi(a) = \phi(a + 0) = \phi(a) + \phi(0). \tag{61}$$

Assim, somando $-\phi(a)$ ao primeiro e ao último termos de (61), obtemos $\phi(0) = 0$. Entretanto, procedendo de maneira análoga para a multiplicação, não conseguimos deduzir, da segunda propriedade, que $\phi(1) = 1$. De fato, a aplicação que leva todos os elementos de A no $0 \in B$ satisfaz as duas primeiras propriedades, mas não a última. Isto explica porque fomos obrigados a incluir $\phi(1) = 1$ como parte da definição de homomorfismo. Para uma discussão mais detalhada veja o exercício ???.

Podemos imaginar um homomorfismo como uma correspondência entre os dois anéis que produz uma espécie de reflexo de A dentro de B. Este reflexo, naturalmente, é a imagem $\mathrm{Im}(\phi)$; uma palavra que, por si só, sugere

nosso símile. Naturalmente, a fidelidade do reflexo de um objeto em um espelho depende da qualidade do espelho. Um bom espelho, que reflete cada detalhe de um objeto, corresponde a um homomorfismo injetivo. Neste caso, cada elemento de A tem uma imagem diferente em B. Quando, além disso, cada elemento de B é imagem de um elemento de A, dizemos que se trata de um *isomorfismo*. Neste caso A e B são *isomorfos*, e escrevemos $A \cong B$. Dois anéis isomorfos têm exatamente as mesmas propriedades algébricas, muito embora seus elementos possam ser "manufaturados de materiais diferentes". Veremos vários exemplos disto na próxima seção.

À primeira vista pode parecer que estaremos apenas interessados em homomorfismos injetivos e isomorfismos, já que são os únicos a reproduzir fielmente o anel de partida. Contudo, às vezes um excesso de detalhes na imagem prejudica nossa capacidade de ver semelhanças. Assim, se usamos vidro vermelho na confecção de um espelho, faremos com que as cores azul e preta de uma figura refletida pelo espelho pareçam ambas pretas no reflexo. Isto pode ajudar a identificar padrões que, de outra forma seriam invisíveis. O mesmo acontece com os homomorfismos.

Nosso primeiro homomorfismo exemplifica o que foi explicado no parágrafo anterior. Seja n um inteiro e considere a aplicação $\pi : \mathbb{Z} \to \mathbb{Z}_n$ que leva cada inteiro a em sua classe módulo n. Ao passar por este homomorfismo estamos identificando uma infinidade de inteiros, agrupando-os em uma única classe. Temos, assim, um espelho extremamente infiel. No entanto, isto serve a um propósito importante, uma vez que, com isto, identificamos facilmente inteiros que deixam o mesmo resto na divisão por n. Como no nosso espelho fabricado com vidro vermelho, as propriedades comuns a dois inteiros são mais facilmente identificadas, porque parte da informação do original foi destruída na imagem.

Vejamos mais algumas aplicações bem conhecidas que são homomorfismos. Digamos que A é uma anel qualquer e x uma variável. Dado $a \in A$, considere a aplicação $\phi_a : A[x] \to A$ definida em um polinômio $f \in A[x]$ por $\phi_a(f) = f(a)$. É claro que ϕ aplica qualquer elemento de A sobre ele mesmo; portanto, $\phi_a(1) = 1$. Por outro lado se $f, g \in A[x]$, então

$$\begin{aligned} \phi_a(f+g) &= (f+g)(a) = f(a) + g(a) = \phi_a(f) + \phi_a(g) \text{ e} \\ \phi_a(f \cdot g) &= (f \cdot g)(a) = f(a) \cdot g(a) = \phi_a(f) \cdot \phi_a(g), \end{aligned}$$

confirmando que ϕ_a é mesmo um homomorfismo. Chamamos esta aplicação de *homomorfismo de especialização* de x em a.

Outro homomorfismo importante nos permite esclarecer a diferença entre um polinômio e uma função polinomial. Se $f \in A[x]$ é um polinômio, a *função polinomial* que lhe corresponde é $\widehat{f} : A \to A$, definida por $\widehat{f}(a) = f(a)$. Como já vimos no exercício ??? do capítulo 2, o conjunto $\mathcal{F}(A)$ das funções de A em A é um anel. Considere, agora, a aplicação $\psi : A[x] \to \mathcal{F}(A)$ que leva um polinômio f na função polinomial $\widehat{f}$. Como $\psi(1) = \widehat{1}$ é igual à função constante cujo único valor é 1, temos que a identidade de $A[x]$ é levada na

identidade de $\mathcal{F}(A)$. Por outro lado, se $f, g \in A[x]$, então $\psi(f+g) = \widehat{f+g}$. Mas, para qualquer $a \in A$,

$$\widehat{f+g}(a) = \widehat{f}(a) + \widehat{g}(a),$$

de modo que $\widehat{f+g} = \widehat{f} + \widehat{g}$, pela definição da adição em $\mathcal{F}(A)$. Portanto,

$$\psi(f+g) = \widehat{f+g} = \widehat{f} + \widehat{g} = \psi(f) + \psi(g).$$

A demonstração de que $\psi(f \cdot g) = \psi(f) \cdot \psi(g)$ é análoga, por isso deixamos os detalhes aos seus cuidados.

Vejamos agora o que acontece quando $A = \mathbb{Z}_p$, onde $p > 0$ é um número primo. Neste caso, apesar de

$$f = x^{p^p} + x^{p^{(p-1)}} + \cdots + x^{p^2} + x^p \in \mathbb{Z}_p[x]$$

ser um polinômio não nulo, a função polinomial correspondente é zero. De fato, qualquer que seja a classe $\overline{a} \in \mathbb{Z}_p$, temos pelo teorema de Fermat que $a^{p^k} \equiv a \pmod{p}$. Mas isto implica que

$$\widehat{f}(\overline{a}) = \overline{p} \cdot \overline{a} = \overline{0},$$

já que há p parcelas em f.

Podemos interpretar a observação do parágrafo anterior dizendo que há polinômios não nulos em $\mathbb{Z}_p[x]$ que são levados em zero por ψ. Pensando bem, um fenômeno similar ocorria com o homomorfismo de especialização. Por exemplo, ϕ_0 leva em zero todos os polinômios cujo termo constante é nulo. Nosso quarto exemplo de homomorfismo vai exibir este mesmo fenômeno de maneira ainda mais dramática. Com isto também voltamos ao início da seção, já que este exemplo é também uma generalização do primeiro.

Seja A um anel qualquer e I um ideal de A, e consideremos a aplicação $\pi : A \to A/I$ que leva a em sua classe módulo I, que denotaremos por $\overline{a}$. Como $\pi(1) = \overline{1}$, a identidade de A é levada na de A/I. As outras duas propriedades decorrem das definições de adição e multiplicação em A/I; assim,

$$\pi(a+b) = \overline{a+b} = \overline{a} + \overline{b} = \pi(a) + \pi(b) \text{ e}$$
$$\pi(a \cdot b) = \overline{a \cdot b} = \overline{a} \cdot \overline{b} = \pi(a) \cdot \pi(b),$$

quaisquer que sejam $a, b \in A$. Temos, portanto, um homomorfismo, conhecido como a *projeção canônica* de A no quociente A/I.

No caso específico da projeção, os elementos de A que são levados em $\overline{0} \in A/I$ são exatamente aqueles que pertencem a I. Portanto, os elementos que π leva em $\overline{0}$ formam um ideal de A. Na verdade, o mesmo acontece com nossos outros dois exemplos, o que sugere que isto não é mera coincidência.

PROPOSIÇÃO 8.3. *Sejam A e B anéis, e $\phi : A \to B$ um homomorfismo. O conjunto*

$$N(\phi) = \{a \in A : \phi(a) = 0\}$$

é um ideal de A.

DEMONSTRAÇÃO. Em primeiro lugar, é claro que $0 \in N(\phi)$, já que $\phi(0) = 0$. Como ϕ é um homomorfismo, temos que

$$\phi(a + a') = \phi(a) + \phi(a').$$

para todo $a, a' \in A$. No entanto, se $a, a' \in N(\phi)$ então

$$\phi(a) = \phi(a') = 0,$$

de modo que $\phi(a + a') = 0$. Concluímos, assim, que $a, a' \in N(\phi)$ implica que $a + a' \in N(\phi)$. Assumindo, agora, que $a' \in N(\phi)$, mas que a é qualquer elemento de A, temos que

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

Portanto, $aa' \in N(\phi)$ sempre que $a' \in N(\phi)$, não importando qual seja $a \in A$. Isto conclui a demonstração de que $N(\phi)$ é um ideal de A. □

O ideal $N(\phi)$, definido na proposição acima, é conhecido como o *núcleo* do homomorfismo ϕ. O núcleo nos dá uma maneira fácil de medir a fidelidade de nosso homomorfismo; isto é, o quanto ele se afasta de ser injetivo. Digamos que $\phi : A \to B$ é um homomorfismo de anéis e que $a, a' \in A$. Então, $\phi(a) = \phi(a')$ é equivalente a dizer que $\phi(a) - \phi(a') = 0$. Como ϕ é um homomorfismo, segue que $\phi(a - a') = 0$. Em outras palavras, $a - a' \in N(\phi)$. Mostramos, assim, que

$$\phi(a) = \phi(a') \text{ se, e somente se, } a - a' \in N(\phi).$$

Portanto, dizer que ϕ é injetivo é o mesmo que dizer que ϕ tem núcleo igual a zero. Por isso podemos afirmar que quanto menor o núcleo, mais "próximo" o homomorfismo está de ser injetivo.

Antes de encerrar, calcularemos o núcleo dos homomorfismos dos exemplos acima. Já vimos que, no caso da projeção, o núcleo é o ideal usado para construir o anel quociente. Mas o homomorfismo que leva $a \in \mathbb{Z}$ em sua classe de equivalência módulo n é um caso especial de projeção. Portanto, o núcleo deste isomorfismo é o ideal de $\mathbb{Z}$ gerado por n.

Pela definição do homomorfismo de especialização $\phi_a : A[x] \to A$ temos que

$$N(\phi_a) = \{f \in A[x] : f(a) = 0\}.$$

Em geral, este ideal poderá ter muitos geradores. Entretanto, se $A = K$, for um corpo, ele terá que ser principal. Na verdade, é fácil identificar o gerador neste caso especial, uma vez que o polinômio de menor grau que está contido em $N(\phi_a)$ é claramente $x - a$. Portanto, devemos ter que $N(\phi_a) = \langle x - a \rangle$. Como mostra o exercício ???, não é por coincidência que este ideal é máximo.

Vejamos o que podemos afirmar sobre o núcleo do homomorfismo

$$\psi : A[x] \to \mathcal{F}(A).$$

Neste caso, a definição de ψ nos diz que o núcleo é constituído pelos polinômios que são levados na função zero. Como no exemplo anterior, só é possível dar uma descrição satisfatória do núcleo deste homomorfismo fazendo algumas restrições. Por exemplo, supondo que A tem característica zero o núcleo é

muito fácil de descrever. De fato, se $f \in A[x]$ tem grau n podemos escrevê-lo na forma

$$f(x) = a_n x^n + \cdots + a_1 x + a_0,$$

onde $a_n, \ldots, a_0 \in A$. Mas, se $f \in N(\psi)$, então

$$\begin{aligned} f(1) &= a_n + \cdots + a_1 + a_0 = 0 \\ f(2) &= a_n 2^n + \cdots + a_1 2 + a_0 = 0 \\ f(3) &= a_n 3^n + \cdots + a_1 3 + a_0 = 0 \\ &\vdots \qquad\qquad\qquad \vdots \\ f(n) &= a_n n^n + \cdots + a_1 n + a_0 = 0. \end{aligned}$$

Consideraremos estas equações como descrevendo um sistema linear com os as como coeficientes. Este sistema tem como matriz

$$\begin{bmatrix} 1 & 1 & \cdots & 1 & 1 \\ 2^n & 2^{n-1} & \cdots & 2 & 1 \\ 3^n & 3^{n-1} & \cdots & 3 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ n^n & n^{n-1} & \cdots & n & 1 \end{bmatrix}.$$

Esta é uma matriz de Vandermonde, e seu determinante é igual

$$\pm(2-1)(3-1)(3-2)\cdot(n-1)(n-2)\cdot(n-(n-1)) \neq 0.$$

Logo, a única solução do sistema nos as é dada por

$$a_n = a_{n-1} = \cdots = a_1 = a_0 = 0.$$

Portanto, $N(\psi) = 0$, se A tem característica zero. Contudo, já vimos que, se a característica de A é positiva então $N(\psi) \neq 0$. Vale a pena você pensar um pouco porque é que o argumento anterior não funciona se a característica for positiva; veja o exercício ????.

Finalmente, voltamos a estudar o anel quociente $\mathbb{R}[x_1, x_2]/\langle x_1^3 - x_2^2\rangle$, na tentativa de determinar se é ou não um domínio. Lembre-se que cada classe deste anel pode ser escrita, de maneira única, na forma $\overline{ax_2 + b}$, para alguma escolha $a, b \in \mathbb{R}[x_1]$. Começamos por definir o homomorfismo

$$\rho : \mathbb{R}[x_1] \to \mathbb{R}[x_1, x_2]/\langle x_1^3 - x_2^2\rangle,$$

que a cada polinômio $a \in \mathbb{R}[x_1]$ associa a classe

$$\overline{b} = \overline{0 \cdot x_2 + b}.$$

Uma consequência imediata da unicidade da representação das classes nesta forma é que $\overline{b}$ só pode ser zero se o polinômio b for zero. Isto significa que o homomorfismo ρ é injetivo. Em particular, a imagem de ρ é isomorfa a $\mathbb{R}[x_1]$, de modo que podemos calcular com elementos da forma $\overline{b}$, quando $b \in \mathbb{R}[x_1]$, exatamente da mesma maneira que calculamos com os polinômios de $\mathbb{R}[x_1]$. Este é o ingrediente que faltava para podermos provar que $\mathbb{R}[x_1, x_2]/\langle x_1^3 - x_2^2\rangle$ é um domínio.

Da fórmula (60) para a multiplicação de duas classes neste anel temos que

$$(\overline{a_1x_2 + b_1}) \cdot (\overline{a_2x_2 + b_2}) = \overline{(a_1b_2 + a_2b_1)x_2 + (b_1b_2 + a_1a_2\overline{x_1}^6)}.$$

Mas cada classe no anel quociente $\mathbb{R}[x_1, x_2]/\langle x_1^3 - x_2^2\rangle$ tem apenas um representante com grau menor que 2 em x_2. Portanto, para que o produto $(\overline{a_1x_2 + b_1}) \cdot (\overline{a_2x_2 + b_2})$ seja igual a zero no anel quociente, devemos ter que

$$a_1b_2 + a_2b_1 = b_1b_2 + a_1a_2\overline{x_1}^6 = 0 \tag{62}$$

em $\mathbb{R}[x_1, x_2]$. Mas isto só é possível se $a_1b_2 = -a_2b_1$, donde

$$a_1(b_1b_2 + a_1a_2\overline{x_1}^6) = b_1a_1b_2 + a_1^2a_2\overline{x_1}^6 = -b_1^2a_2 + a_1^2a_2\overline{x_1}^6.$$

Pondo a_2 em evidência, temos

$$0 = a_1(b_1b_2 + a_1a_2\overline{x_1}^6) = a_2(-b_1^2 + a_1^2\overline{x_1}^6).$$

Supondo que $a_2 \neq 0$, e levando em conta que $\mathbb{R}[x_1]$ é um domínio, concluímos que

$$b_1^2 = (a_1\overline{x_1}^3)^2.$$

Entretanto, a unicidade da fatoração em $\mathbb{R}[x_1]$ implica que

$$b_1 = \pm x_1^3a_1. \tag{63}$$

Em particular, isto se $a_1 = 0$ então $b_1 = 0$; donde obtemos $a_1x_2 + b_1 = 0$. Assim, podemos supor que $a_1 \neq 0$. Substituindo, então, (63) em (62) e cancelando a_1, resta

$$\pm x_1^3a_2 + b_2 = \pm x_1^3b_2 + a_2 = 0,$$

de modo que $a_2 = b_2 = 0$, o que não é possível. Provamos, assim, que se $a_2 \neq 0$, então

$$(\overline{a_1x_2 + b_1}) \cdot (\overline{a_2x_2 + b_2}) = \overline{0}$$

implica que $\overline{a_1x_2 + b_1} = \overline{0}$. Para completar a demonstração de que o anel quociente $\mathbb{R}[x_1, x_2]/\langle x_1^3 - x_2^2\rangle$ é um domínio precisaríamos ainda mostrar que, se $a_1 = 0$ mas $b_1 \neq 0$, então $\overline{a_2x_2 + b_2} = \overline{0}$; mas esta parte da demonstração é fácil e fica por sua conta preencher os detalhes.

Diante do que fizemos no início da seção podemos nos perguntar se o domínio $\mathbb{R}[x_1, x_2]/\langle x_1^3 - x_2^2\rangle$ não é, na verdade, um corpo. Mas a resposta neste caso é não. Por exemplo, se $\overline{x_1}$ admitisse inverso neste anel quociente, teríamos que

$$\overline{x_1} \cdot \overline{ax_2 + b} = \overline{1},$$

para alguma escolha de $a, b \in \mathbb{R}[x_1]$. Só que isto equivale a

$$\overline{x_1ax_2 + x_1b} = \overline{1}.$$

Usando novamente a unicidade desta representação das classes no quociente, temos que $x_1ax_2 = 0$ e $x_1b = 1$, que não é possível para nenhum polinômio b no anel $\mathbb{R}[x_1]$.

5. Teorema do homomorfismo

O núcleo não serve apenas como critério para identificar se um dado homomorfismo é injetivo. Como mostra o próximo teorema, ele desempenha um papel crucial no estudo da relação entre homomorfismos e anéis quocientes.

TEOREMA DO HOMOMORFISMO. *Sejam A e B anéis, e $\phi : A \to B$ um homomorfismo sobrejetor. Então, $A/N(\phi)$ é isomorfo a B.*

DEMONSTRAÇÃO. É claro que precisamos usar ϕ para construir o isomorfismo entre $A/N(\phi)$ e B, que vamos chamar de $\overline{\phi}$. Na verdade, a primeira ideia que provavelmente vai lhe ocorrer é definir a imagem da classe de $\overline{a} \in A/N(\phi)$ como sendo $\phi(a)$; isto é $\overline{\phi}(\overline{a}) = \phi(a)$. O problema que imediatamente se põe é semelhante ao que já enfrentamos ao estabelecer as operações em um anel quociente. Afinal, estamos definindo a imagem de uma classe inteira pela imagem de um representante desta classe. Portanto, para mostrar que $\overline{\phi}$ está bem definida precisamos verificar que se $\overline{a} = \overline{a'}$, então $\phi(a) = \phi(a')$. Mas isto é fácil de fazer. Na verdade, dizer que $\overline{a} = \overline{a'}$ é o mesmo que dizer $a - a' \in N(\phi)$ que, por sua vez, é equivalente a

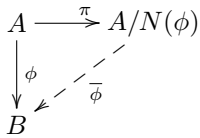
$$\phi(a) - \phi(a') = \phi(a - a') = 0.$$

Portanto, $\overline{a} = \overline{a'}$ ocorre, se e somente se, $\phi(a) = \phi(a')$. Isto é ótimo, porque resolve o problema que já formulamos, e ainda outro, que nem chegamos a enunciar. Com efeito, $\overline{a} = \overline{a'}$ nos garante que $\phi(a) = \phi(a')$, de modo que $\overline{\phi}$ está bem definida, como queríamos mostrar. Por outro lado, a recíproca nos dá que $\phi(a) = \phi(a')$ implica que $\overline{a} = \overline{a'}$. Mas isto equivale a dizer que $\overline{\phi}$ é injetiva. Portanto, a regra $\overline{\phi}(\overline{a}) = \phi(a)$ nos dá uma aplicação injetiva de $A/N(\phi)$ em B. Além disso, como ϕ é sobrejetiva, $\overline{\phi}$ tem que ser sobrejetiva. Concluímos, assim, que $\overline{\phi} : A/N(\phi) \to B$ é uma aplicação bijetiva. Só falta provar que $\overline{\phi}$ é um homomorfismo, mas esta é uma verificação de rotina, que deixaremos aos seus cuidados. □

Este teorema admite uma espécie de representação diagramática. De partida temos três anéis A, B e o quociente $A/N(\phi)$, que estão relacionados entre si por dois homomorfismos. Assim, ϕ aplica A em B e a projeção canônica π aplica A em $A/N(\phi)$. Podemos resumir isto no seguinte diagrama

$$\begin{array}{ccc} A & \xrightarrow{\pi} & A/N(\phi) \\ \big\downarrow{\scriptstyle \phi} & & \\ B & & \end{array}$$

O homomorfismo $\overline{\phi} : A/N(\phi) \to B$, que construímos como parte da demonstração do teorema se encaixa perfeitamente no diagrama, formando um triângulo, como segue



Representamos $\overline{\phi}$ com linhas tracejadas para chamar a atenção de que se trata de uma construção dada pelo teorema, que não é parte das hipóteses. Observe que, por construção, $\phi = \overline{\phi} \circ \pi$.

Este teorema era o ingrediente que faltava para podermos responder às questões que ficaram pendentes da seção 3. Em primeiro lugar, trataremos do caso em que K é um corpo e $\phi_a : K[x] \to K$ é a especialização em um elemento $a \in K$. Neste caso já sabemos que o núcleo da aplicação ϕ_a é o ideal máximo gerado por $\langle x - a \rangle$. O teorema do homomorfismo então nos diz que $K[x]/\langle x - a \rangle \cong K$. Em outras palavras, levando em consideração apenas as propriedades algébricas, não é possível distinguir estes dois anéis. Entretanto, os elementos de $K[x]/\langle x - a \rangle$ e K são manufaturados a partir de materiais diferentes. Com efeito, em $K[x]/\langle x - a \rangle$ temos classes de equivalência (que são subconjuntos de $K[x]$), em K temos apenas números.

Um exemplo bem mais interessante ocorre quando $K = \mathbb{Q}$ e $\alpha = \sqrt{2}$. Como $\sqrt{2}$ é raiz de $g = x^2 - 2$, segue que g pertence ao núcleo da especialização

$$\phi_{\sqrt{2}} : \mathbb{Q}[x] \to \mathbb{C}.$$

Dividindo $f \in \mathbb{Q}[x]$ por g, obtemos

$$f = qg + (ax + b),$$

onde $q \in \mathbb{Q}[x]$ e $a, b \in \mathbb{Q}$. Aplicando a especialização $\phi_{\sqrt{2}}$, e levando em conta que $g \in N(\phi_{\sqrt{2}})$, resta

$$\phi_{\sqrt{2}}(f) = a\sqrt{2} + b,$$

que é um número real. Portanto, nenhum número complexo cuja parte imaginária é não nula pertence à imagem de $\phi_{\sqrt{2}}$. Embora, à primeira vista, isto pareça um obstáculo à aplicação do teorema do homomorfismo, na prática é facilmente contornável. Afinal de contas, ϕ_α é sobrejetivo sobre sua imagem, que é necessariamente um anel; veja exercício ???. Na verdade os cálculos acima mostram que

$$\mathrm{Im}(\phi_{\sqrt{2}}) = \{a\sqrt{2} + b : a, b \in \mathbb{Q}\};$$

um subanel de $\mathbb{C}$ que é usualmente denotado por $\mathbb{Q}[\sqrt{2}]$. Aplicando, pois, o teorema do homomorfismo verificamos que

$$\mathbb{Q}[x]/\langle x^2 - 2 \rangle \cong \mathbb{Q}[\sqrt{2}] \subset \mathbb{C}.$$

Mas $x^2 - 2$ é irredutível sobre $\mathbb{Q}$, de modo que pela proposição 8.2, o anel quociente é um corpo. Como $\mathbb{Q}[\sqrt{2}]$ é isomorfo ao quociente, então é um subcorpo de $\mathbb{C}$. Trataremos um caso muito mais geral deste exemplo na seção 6.

No segundo exemplo da seção 3, o anel é o quociente de $K[x_1, x_2]$ pelo ideal máximo $\mathfrak{m} = \langle x_1, x_2 \rangle$, gerado pelas variáveis. Desta vez, consideraremos o homomorfismo de especialização $\phi_0 : K[x_1, x_2] \to K$, que leva $f \in K[x_1, x_2]$ em $f(0)$. É fácil ver que $N(\phi_0) = \mathfrak{m}$, de modo que o teorema do homomorfismo nos dá $K[x_1, x_2]/\mathfrak{m} \cong K$. Isto explica, de maneira rigorosa, a identificação entre $K[x_1, x_2]/\mathfrak{m}$ e K que os cálculos da seção 3 nos sugeriram.

Nosso último exemplo é o quociente de $\mathbb{R}[x_1, x_2]$ pelo ideal principal gerado por $g = x_1^3 - x_2^2$. Contudo, como vimos na página 79, a curva algébrica C, descrita por este ideal, pode ser parametrizada na forma

$$C = \{(t^2, t^3) : t \in \mathbb{R}\}.$$

Esta parametrização nos dá um homomorfismo $\alpha : \mathbb{R}[x_1, x_2] \to \mathbb{R}[t]$ que leva um polinômio $f \in \mathbb{R}[x_1, x_2]$ em $f(t^2, t^3)$. Traduzidos na linguagem deste capítulo, os cálculos que fizemos na página 80 mostram que o núcleo de α é g, como seria de esperar. No entanto, como já ocorreu em outro exemplo acima, o homomorfismo α não é sobrejetivo. De fato, se $f \in \mathbb{R}[x_1, x_2]$ não for constante, então $f(t^2, t^3) \in \mathrm{Im}(\alpha)$ é um polinômio de grau pelo menos 2 em t. Por isso, nenhum polinômio em $\mathbb{R}[t]$ de grau 1 pertence a $\mathrm{Im}(\alpha)$. Como acima, contornamos este problema escrevendo

$$\mathbb{R}[x_1, x_2]/\langle x_1^3 - x_2^2 \rangle \cong \mathrm{Im}(\alpha) \subsetneq \mathbb{R}[t].$$

Por sua vez, deste isomorfismo, concluímos que cada elemento da imagem de α pode ser escrito, de maneira única, na forma $f(t^2, t^3)$, onde $f \in \mathbb{R}[x_1, x_2]$ tem grau no máximo um na variável x_1.

Encerramos a seção com uma propriedade básica dos anéis quocientes de anéis de polinômios que será utilizada no próximo capítulo.

PROPOSIÇÃO 8.4. *Seja A um anel, I um ideal de A e x uma indeterminada. Denotando por $I[x]$ o conjunto dos elementos de $A[x]$ cujos coeficientes pertencem a I, temos que $I[x]$ é um ideal de $A[x]$ e que*

$$A[x]/I[x] \cong (A/I)[x].$$

DEMONSTRAÇÃO. Seja

$$\theta : A[x] \to (A/I)[x]$$

o homomorfismo que associa a cada

$$a_0 + a_1 x + \cdots + a_n x^n \in A[x],$$

o polinômio

$$\overline{a_0} + \overline{a_1} x + \cdots + \overline{a_n} x^n,$$

em $(A/I)[x]$. Como o núcleo de θ é claramente igual a $I[x]$, a proposição segue imediatamente do teorema do homomorfismo. □

6. Corpos efetivos

Nesta seção estudaremos alguns subcorpos efetivos de $\mathbb{C}$. Lembre-se que, segundo o que vimos na página 33, um corpo K é *efetivo* se as operações de adição, substração, multiplicação e divisão, além da comparação de dois elementos para determinar se são ou não iguais, pode ser feita de maneira algorítmica e programada em um computador. Já vimos que $\mathbb{Q}$ é efetivo, mas nem $\mathbb{R}$, nem $\mathbb{C}$ o são. A primeira impressão é que o obstáculo ao cálculo efetivo nestes dois últimos corpos está nos números irracionais. Entretanto, como veremos nesta seção, o problema é bem mais sutil.

Para entender onde está exatamente o problema, comecemos considerando os números irracionais mais simples que conhecemos; números como $\sqrt{2}$ ou $\sqrt[3]{5}$, isto é raízes n-ésimas dadas implicitamente. Não há nenhuma dificuldade em calcular com estes números de *maneira exata*, coisa que aprendemos a fazer ainda no ensino fundamental com as chamadas *expressões irracionais*. Para sistematizar e generalizar isto introduziremos algumas noções básicas da teoria de corpos.

Seja K um subcorpo de um corpo L. Quando queremos mudar a perspectiva e, partindo de K como base, chamar a atenção para L como um corpo que contém K, dizemos que L é uma *extensão* de K. Portanto, $\mathbb{R}$ é extensão de $\mathbb{Q}$ e $\mathbb{C}$ é extensão tanto de $\mathbb{Q}$ como de $\mathbb{R}$. Um elemento α de uma extensão L de K pode ser classificado em dois tipos diferentes, de acordo com o comportamento relativamente a K. Se α é raiz de um polinômio em $K[x]$, dizemos que é *algébrico sobre* K; caso contrário é *transcendente sobre* K. Por exemplo, quando $K = \mathbb{Q}$ e $L = \mathbb{C}$, os números $\sqrt{2}$, $\sqrt[3]{5}$ e

$$\sqrt[5]{1+\sqrt[3]{7}}$$

são algébricos, ao passo que π e a base e dos logaritmos naturais são transcendentes. O problema é que provar que um dado número é transcendente é bastante difícil e envolve o uso mais ou menos pesado de análise básica. Por isso, não provaremos que estes números são transcenedentes neste livro; veja [**27**, p. 170ss] para mais detalhes.

Números algébricos e transcendentes também podem ser caracterizados a partir de seu comportamento relativamente ao homomorfismo de especialização

$$\phi_\alpha : K[x] \to L.$$

Se α for *algébrico sobre* K então existe algum polinômio $g \in K[x]$ do qual α é raiz; mas isto significa que

$$\phi_\alpha(g) = g(\alpha) = 0;$$

e assim $\mathrm{N}(\phi_\alpha) \neq 0$ pois contém g. Por outro lado, se α for *transcendente sobre* K, então nenhum polinômio de $K[x]$ se anula em α; portanto, $\mathrm{N}(\phi_\alpha) = \{0\}$ neste caso. Resumindo:

$$\mathrm{N}(\phi_\alpha) \neq 0 \text{ se, e somente se, } \alpha \text{ é algébrico sobre } K.$$

Se α pertence a uma extensão L do corpo K, denotaremos por $K(\alpha)$ o menor subcorpo de L que contém K. Observe que os elementos de $K(\alpha)$ são da forma $f(\alpha)/q(\alpha)$, em que $f, q \in K[x]$ e $q(\alpha) \neq 0$. Se α for transcendente, então $q(\alpha) \neq 0$ sempre que o polinômio q for não nulo. Neste caso o corpo $K(\alpha)$ é isomorfo ao corpo das funções racionais, que estudaremos em mais detalhes na seção 1 do capítulo 10. Nossa primeira meta neste capítulo é caracterizar o corpo $K(\alpha)$ quando $\alpha \in \mathbb{C}$ é algébrico sobre K e

$$\mathbb{Q} \subset K \subset \mathbb{C}.$$

Seja, então, $\alpha \in \mathbb{C}$ um elemento algébrico sobre K. Entre todos os polinômios *mônicos* de $K[x]$ que têm α como raiz, digamos que g seja o de menor grau. Tome, agora, $f \in K[x]$ e divida-o por g; isto nos dá

$$f = gq + r \text{ onde } r = 0 \text{ ou } \operatorname{grau}(r) < \operatorname{grau}(g). \tag{64}$$

Se acontecer de α também ser raiz de f, então, da divisão,

$$0 = f(\alpha) = g(\alpha)q(\alpha) + r(\alpha) = r(\alpha),$$

porque $g(\alpha) = 0$ por hipótese. Entretanto, escolhemos g como o polinômio de *menor* grau satisfazendo esta hipótese, de forma que $r(\alpha) = 0$ é incompatível com

$$\operatorname{grau}(r) < \operatorname{grau}(g).$$

Concluímos, assim, que se $f(\alpha) = 0$ então $r = 0$; isto é, o polinômio r é identicamente nulo. Em particular, o polinômio mônico de grau menor do qual α é raiz tem que ser único; ele é conhecido como o *polinômio mínimo de α sobre K*. Usando esta terminologia, o que acabamos de provar pode ser enunciado na forma:

> o polinômio mínimo de α sobre K divide qualquer polinômio de $K[x]$ do qual α é raiz.

Disto podemos deduzir que o polinômio mínimo é irredutível sobre K. De fato, se $g = g_1 g_2$, então

$$0 = g(\alpha) = g_1(\alpha)g_2(\alpha).$$

Mas isto implica que $g_1(\alpha) = 0$ ou $g_2(\alpha) = 0$; donde podemos concluir que g divide g_1 ou g_2. Como estes polinômios são fatores de g, isto só pode ocorrer se g_1 ou g_2 é um múltiplo constante de g, o que garante a irredutibilidade do polinômio mínimo.

Combinando o que fizemos até aqui com o teorema do homomorfismo, verificamos que a especialização em α nos dá um homomorfismo

$$\phi_\alpha : K[x] \to \mathbb{C}$$

cujo núcleo é não nulo e contém o polinômio mínimo g de α sobre K. Mas este polinômio é irredutível, de modo que o ideal $\langle g \rangle$ é máximo em $K[x]$. Isto basta para garantir que

$$\mathrm{N}(\phi_\alpha) = \langle g \rangle$$

e que o quociente $K[x]/\langle g\rangle$ é um corpo. Assim, ϕ_α induz uma aplicação injetiva

$$\overline{\phi}_\alpha : K[x]/\langle g\rangle \to \mathbb{C}.$$

Mas, pelo teorema do homomorfismo,

$$\mathrm{Im}(\overline{\phi}_\alpha) \cong K[x]/\langle g\rangle,$$

que é um corpo. Assim, podemos concluir que

$$K(\alpha) = \mathrm{Im}(\overline{\phi}_\alpha),$$

e nosso problema estará resolvido se pudermos caracterizar de maneira simples a imagem da especialização em α.

Contudo, pela equação (64), se $f \in K[x]$ então

$$\overline{f} = \overline{r},$$

que é o resto da divisão de f por g. Por outro lado, dois elementos de $K[x]$ representam a mesma classe em $K[x]/\langle g\rangle$ se sua diferença for um múltiplo de g. Se, além disso, estes elementos tiverem ambos grau menor que o grau de g, então terão que ser iguais. Portanto, r é o único representante de $\overline{f}$ com grau menor que $\mathrm{grau}(g)$. Usando a linguagem da álgebra linear, podemos reformular isto dizendo que no K-espaço vetorial $K[x]/\langle g\rangle$, o conjunto

$$B = \{\overline{1}, \overline{x}, \ldots, \overline{x}^{\mathrm{grau}(g)-1}\}$$

é linearmente independente. Como estes elementos geram $K[x]/\langle g\rangle$, concluímos que B é uma base de $K[x]/\langle g\rangle$, de forma que este quociente tem dimensão igual a $\mathrm{grau}(g)$ como espaço vetorial sobre K. Como

$$K(\alpha) \cong K[x]/\langle g\rangle,$$

e a imagem de $\overline{x}^k$ por este isomorfismo é $\overline{\alpha}^k$, podemos concluir que

$$\{1, \alpha, \ldots, \alpha^{\mathrm{grau}(g)-1}\}$$

é uma base de $K(\alpha)$. Com isto obtemos a caracterização desejada para $K(\alpha)$.

PROPOSIÇÃO 8.5. *Seja K um subcorpo de $\mathbb{C}$ e $\alpha \in \mathbb{C}$ um número algébrico sobre K. Se $g \in K[x]$ de grau d for o polinômio mínimo de α sobre K então:*

(1) *g é irredutível;*
(2) *a especialização em α induz um isomorfismo*

$$K(\alpha) \cong K[x]/\langle g\rangle;$$

(3) *os elementos de $K(\alpha)$ podem ser escritos, de maneira única, na forma*

$$c_0 + c_1\alpha + \cdots + c_{d-1}\alpha^{d-1}$$

em que os cs pertencem a K;
(4) *$K(\alpha)$ tem dimensão d como espaço vetorial sobre K.*

Por exemplo, $\sqrt[3]{2}$ tem como polinômio mínimo $x^3 - 2$ sobre $\mathbb{Q}$, de modo que

$$\mathbb{Q}(\sqrt[3]{2}) = \{a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{2} \,|\, a_0, a_1, a_2 \in \mathbb{Q}\};$$

já

$$\alpha = \sqrt[5]{1 + \sqrt[3]{7}}$$

tem polinômio mínimo igual a

$$x^{15} - 3x^{10} + 3x^5 - 8$$

como é fácil de verificar; de modo que $K(\alpha)$ tem dimensão 15.

O isomorfismo $\overline{\phi}_\alpha$ nos permite calcular facilmente com os elementos de $K(\alpha)$. Digamos que sejam dados dois elementos não nulos $f_1(\alpha)$ e $f_2(\alpha)$ deste corpo. Já vimos que f_1 e f_2 sempre podem ser escolhidos como sendo polinômios de grau menor que $\text{grau}(g)$ em $K[x]$. Para multiplicar estes elementos, procedemos da segunte maneira. Em primeiro lugar, dividimos o produto dos polinômios $f_1 f_2$ por g, o que nos dá

$$f_1 f_2 = gq + r \text{ onde } \text{grau}(r) < \text{grau}(g).$$

Observe que o resto não pode ser zero porque supusemos os elementos não nulos e o quociente é um corpo. Assim,

$$\overline{f_1 f_2} = \overline{r}$$

em $K[x]/\langle g\rangle$, de modo que

$$f_1(\alpha) f_2(\alpha) = \overline{\phi_\alpha}(f_1 f_2) = \overline{\phi_\alpha}(r) = r(\alpha),$$

uma vez que $\overline{\phi_\alpha}$ é um isomorfismo de corpos. Vejamos como isto funciona se o que queremos é multiplicar

$$(1 + 2\sqrt[3]{2} + 7\sqrt[3]{2}^2)(3 + 5\sqrt[3]{2}^2)$$

na extensão $\mathbb{Q}(\sqrt[3]{2})$ de $\mathbb{Q}$. Primeiramente multiplicamos os polinômios correspondentes, obtendo

$$(1 + 2x + 7x^2)(3 + 5x^2) = 35x^4 + 10x^3 + 26x^2 + 6x + 3;$$

que dividimos pelo polinômio mínimo $g = x^3 - 2$ de $\sqrt[3]{2}$ sobre $\mathbb{Q}$. Como o resto da divisão é $26x^2 + 76x + 23$, podemos concluir que

$$(1 + 2\sqrt[3]{2} + 7\sqrt[3]{2}^2)(3 + 5\sqrt[3]{2}^2) = 26\sqrt[3]{2}^2 + 76\sqrt[3]{2} + 23.$$

É claro que este procedimento pode ser facilmente automatizado.

Diremos que uma extensão de $L \subset \mathbb{C}$ de um subcorpo K de $\mathbb{C}$ é *simples* se existe um número $\alpha \in L$ tal que $L = K(\alpha)$. Neste caso dizemos também que L é obtido de K por *adjunção* de α. O que fizemos até aqui mostra que uma extensão simples de $\mathbb{Q}$ por adjunção de um número algébrico é um corpo efetivo. Para ser honesto, mesmo se L for obtido de $\mathbb{Q}$ por adjunção de um número transcendente, continua sendo verdade que L é efetivo, como veremos na seção 1 do capítulo 10. O problema surge quando estamos adjuntando vários números, e pode ser formulado de maneira precisa como segue:

> dados $\alpha, \beta \in \mathbb{C}$ e K um subcorpo de $\mathbb{C}$, descrever os elementos do menor subcorpo $K(\alpha, \beta)$ de $\mathbb{C}$ que contém α, β e todos os elementos de K de maneira que os cálculos neste corpo possam ser efetuados de maneira algorítmica.

Veremos que se α e β são algébricos, então $K(\alpha, \beta)$ é extensão simples por adjunção de um número da forma $\alpha + c\beta$, para um $c \in K$ escolhido de maneira apropriada. No caso transcendente não existe um resultado semelhante o que torna o problema muito mais difícil.

TEOREMA DO ELEMENTO PRIMITIVO. *Sejam K um subcorpo e α e β elementos de $\mathbb{C}$. Existe $c \in K$ tal que*

$$K(\alpha, \beta) = K(\alpha + c\beta).$$

DEMONSTRAÇÃO. A demonstração consiste em descobrir que condições a constante $c \in K$ deve satisfazer para que

$$\beta \in K(\gamma_c), \text{ com } \gamma_c = \alpha + c\beta.$$

Com efeito, isto garante que

$$\alpha = \gamma_c - c\beta \in K(\gamma_c).$$

Mas se $\alpha, \beta \in K(\gamma_c)$, então

$$K(\alpha, \beta) \subseteq K(\gamma_c) = K(\alpha + c\beta).$$

Como a outra inclusão é óbvia, obtemos a igualdade desejada.

Para mostrar que $\beta \in K(\gamma_c)$ começamos tomando o polinômio mínimo f de α. Então, supondo $c \in K \setminus \{0\}$ fixo, temos que

$$h(x) = f(\gamma_c - cx),$$

é um polinômio na variável x com coeficientes em $K(\gamma_c)$ que se anula em β. Seja g o polinômio mínimo de β e

$$\beta_1 = \beta, \beta_2, \ldots, \beta_s$$

suas raízes. Então,

$$h(\beta_i) = f(\gamma - c\beta_i) = 0$$

se, e somente se $\gamma - c\beta_i$ é uma raiz de f. Mas, se

$$\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_t$$

forem todas as raízes de f, então isto significa que

$$\gamma - c\beta_i = \alpha_j$$

para algum $1 \leq j \leq t$. Neste caso,

$$\gamma = \alpha_j + c\beta_i.$$

É claro que isto ocorre quando $i = j = 1$; digamos que não ocorra para nenhuma outra escolha de valores de i e j. Em outras palavras, suponhamos que

$$h(\beta_i) = 0 \text{ se e somente se, } i = 1. \tag{65}$$

Portanto, h e f só têm uma raiz comum, que é o próprio $\beta_1 = \beta$. Em particular,

$$\mathrm{mdc}(h, f) = x - \beta.$$

Como h e f são polinômios de uma variável com coeficients em $K(\gamma_c)$, então o mesmo vale para seu máximo divisor comum. Mas isto só é possível se $\beta \in K(\gamma_c)$, como queríamos provar.

Para que a demonstração esteja completa só nos falta mostrar que é mesmo possível escolher $c \in K \setminus \{0\}$ de forma que (65) seja satisfeita. Contudo, se isto for falso e

$$\alpha_1 + c\beta_1 = \alpha_j + c\beta_i,$$

para alguma escolha de i e j ambos diferentes de 1, então a igualdade acima nos dá

$$c = \frac{\alpha_1 - \alpha_j}{\beta_i - \beta_1}.$$

Portanto, qualquer c que esteja fora do conjunto finito

$$\left\{ \frac{\alpha_1 - \alpha_j}{\beta_i - \beta_1} \,|\, 2 \leq j \leq s \text{ e } \ 2 \leq i \leq t \right\}$$

satisfaz (65). Em outras palavras, quase todo número em $K \setminus \{0\}$ satisfará a condição desejada! □

Um exemplo simples ilustra o funcionamento do teorema. Digamos que queremos encontrar um número racional c tal que

$$\mathbb{Q}(\sqrt{5}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt{5} + c\sqrt[3]{2}).$$

O polinômio mínimo de $\sqrt{5}$ sobre $\mathbb{Q}$ é $x^2 - 5$ e o de $\sqrt[3]{2}$ é $x^3 - 2$; o primeiro polinômio tem raízes $\pm\sqrt{5}$ e o segundo

$$\sqrt[3]{2}, \sqrt[3]{2}\zeta \text{ e } \ \sqrt[3]{2}\zeta^2 \text{ com } \ \zeta = \frac{-1 + i\sqrt{3}}{2}.$$

Portanto, os valores de $c \neq 0$ que devemos excluir são os números racionais que pertencem ao conjunto

$$\left\{ \frac{2\sqrt{5}}{\sqrt[3]{2}(\zeta^r - 1)} \,|\, 1 \leq r \leq 3 \right\}.$$

Como não há racionais neste conjunto, qualquer número racional não nulo pode ser escolhido para fazer o papel de c; o que nos permite escolher $c = 1$. Portanto,

$$\mathbb{Q}(\sqrt{5}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt{5} + \sqrt[3]{2}).$$

Embora isto tenha ficado implícito do que dissemos anteriormente, nada no teorema do elemento primitivo nos garante que o número $\alpha + c\beta$ é necessariamente algébrico. Entretanto, precisamos que isto seja verdadeiro para poder continuar adjuntando números a esta extensão, caso precisemos calcular simultaneamente com vários números algébricos diferentes. Isto, contudo, é fácil de provar e é o que faremos antes de encerrar esta seção.

A primeira ferramenta que precisamos para o que estamos por fazer é a noção de grau de uma extensão. Na verdade, este é só um nome tradicional para algo que já usamos anteriormente. Se K é um subcorpo de L, então o *grau* $[L : K]$ da extensão $K \subset L$ é a dimensão de L como espaço vetorial sobre K. Portanto, podemos reformular o item (4) da proposição 8.5 dizendo que se $\alpha \in \mathbb{C}$ é algébrico sobre um subcorpo $K \subset \mathbb{C}$ então

$$[K(\alpha) : K] = \text{ grau do polinômio mínimo de } \alpha \text{ sobre } K.$$

Em particular, se α é algébrico a extensão simples tem dimensão finita sobre K. Isto é falso se α for transcendente porque, neste caso, o morfismo de especialização em α é injetivo, de modo que $K[x]$ é um subanel de $K(\alpha)$. Como $K[x]$ tem dimensão infinita sobre K, o mesmo terá que valer para $K(\alpha)$. A próxima proposição é uma meia recíproca desta propriedade dos números algébricos.

PROPOSIÇÃO 8.6. *Sejam $K \subset L$ subcorpos de $\mathbb{C}$. Se $[L : K]$ for finito, então todos os elementos de L são algébricos sobre K.*

DEMONSTRAÇÃO. A demonstração usa apenas a definição do que significa ter dimensão finita. Seja $\alpha \in L$ e considere o conjunto (infinito) P das potências de α. Como L é um espaço vetorial de dimensão finita sobre K, o conjunto P tem que ser linearmente dependente. Logo, existem números $c_0, \ldots, c_k \in K$ tais que

$$c_0 + c_1\alpha + \cdots + c_k\alpha^k = 0.$$

Portanto, α é raiz do polinômio

$$g(x) = c_0 + c_1x + \cdots + c_kx^k \in K[x],$$

o que faz dele um número algébrico sobre K. □

De posse deste resultado, fica fácil mostrar que se α e β são algébricos, então $\alpha + c\beta$ também é, não importa qual seja $c \in K$, desde que sejamos capazes de provar que $K(\alpha, \beta)$ é um extensão de dimensão finita de K. Afinal, $\alpha + c\beta \in K(\alpha, \beta)$, qualquer que seja c. Para isto, construiremos $K(\alpha, \beta)$ a partir de K em duas etapas. Adjuntando primeiro α e depois β, temos duas extensões consecutivas,

$$K \subset K(\alpha) \subset K(\alpha)(\beta) = K(\alpha, \beta),$$

ambas algébricas, já que estamos supondo que tanto α quanto β são algébricos sobre K. Observe que sendo algébrico sobre K, o número β é necessariamente algébrico sobre qualquer corpo que contém K; em nosso caso, $K(\alpha)$. O que torna a solução do problema viável é a seguinte fórmula para calcular o grau de uma extensão construída em duas etapas.

PROPOSIÇÃO 8.7. *Se $K \subset L \subset M$ são corpos, então,*

$$[M : K] = [M : L][L : K].$$

DEMONSTRAÇÃO. Como a dimensão de um espaço vetorial é a quantidade de elementos de uma base, precisamos apenas mostrar como construir uma base com $[M : L][L : K]$ elementos para M como espaço vetorial sobre K, a partir das bases B de M sobre L e B' de L sobre K. Mas estas bases têm $[M : L]$ e $[L : K]$ elementos respectivamente. Isto sugere que a base que desejamos deve ser obtida multiplicando os elementos de B pelos de B'. Sejam, então,

$$B = \{v_1, \ldots, v_k\} \quad \text{e} \quad B' = \{u_1, \ldots, u_r\},$$

em que $k = [M : L]$ e $r = [L : K]$. Queremos mostrar que o conjunto

$$BB' = \{u_j v_i \,|\, 1 \leq j \leq k \quad \text{e} \quad 1 \leq i \leq r\},$$

é uma base de M sobre K. Como BB' tem $rs = [M : L][L : K]$, isto basta para provar a proposição.

Seja $w \in M$. Como B é uma base de M sobre L, existem números $c_1, \ldots, c_k \in L$, tais que

$$w = c_1 v_1 + \cdots + c_k v_k. \tag{66}$$

Entretanto, cada $c_i \in L$ pode ser escrito na forma

$$c_i = a_{i1} u_1 + \cdots + a_{ir} u_r, \tag{67}$$

com os as em K. Substituindo (67) em (66),

$$w = (\sum_{j=1}^{r} a_{1j} u_j) v_1 + \cdots + (\sum_{j=1}^{r} a_{1j} u_j) v_k.$$

Efetuando os produtos obtemos w expresso como combinação linear dos elementos de BB' com coeficientes em K. Logo, BB' gera M sobre K. Resta, apenas, provar que BB' é linearmente independente.

Para isto, reproduzimos o argumento acima do fim para o início. Mais precisamente, suponhamos que

$$\sum_{i,j} a_{ij} v_i u_j = 0.$$

Pondo os v_i em evidência, obtemos uma expressão da forma

$$\sum_{j=1}^{k} (\sum_{i=1}^{r} a_{ij} u_j) v_i = 0.$$

Como os as pertencem a K, temos que

$$\sum_{i=1}^{r} a_{ij} u_j \in L \text{ para todo } 1 \leq j \leq k.$$

Como os vs formam a base B de M sobre L, podemos concluir que

$$\sum_{i=1}^{r} a_{ij} u_j = 0 \text{ para todo } 1 \leq j \leq k.$$

Mas, por sua vez, os us formam a base B' de L sobre K, de modo que estas últimas equações implicam que

$$a_{ij} = 0 \text{ para todo } 1 \leq j \leq k \text{ e todo } 1 \leq i \leq r,$$

o que mostra que BB' é um conjunto linearmente independente. □

Podemos, agora, completar o argumento para mostrar que se dois números complexos α e β são algébricos sobre um subcorpo $K \subset \mathbb{C}$, então $\alpha + c\beta$ também é, qualquer que seja $c \in K$. Como, as duas extensões consecutivas,

$$K \subset K(\alpha) \subset K(\alpha)(\beta) = K(\alpha, \beta),$$

são ambas algébricas, temos que

$$[K(\alpha, \beta) : K(\alpha)] \quad \text{e} \quad [K(\alpha) : K]$$

são ambas finitas. Logo,

$$[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\alpha)][K(\alpha) : K]$$

também é finita. Portanto, pela proposição 8.6, todos os elementos de $K(\alpha, \beta)$ são algébricos sobre K. Em particular, isto vale para todo $\alpha + c\beta$, com $c \in K$. Combinando este argumento com uma indução simples, temos o seguinte corolário.

COROLÁRIO 8.8. *Se $\alpha_1, \ldots, \alpha_s \in \mathbb{C}$ são números algébricos e K é um subcorpo de $\mathbb{C}$, então existem números $c_2, \ldots, c_s \in K$ tais que*

$$K(\alpha_1, \ldots, \alpha_s) = K(\alpha_1 + c_2\alpha_2 + \cdots + c_s\alpha_s),$$

é uma extensão simples e de dimensão finita sobre K, cujos elementos são todos algébricos sobre K.

Portanto, se $\alpha_1, \ldots, \alpha_s \in \mathbb{C}$ são números algébricos, então $\mathbb{Q}(\alpha_1, \ldots, \alpha_s)$ é um corpo efetivo. Na próxima seção veremos como utilizar bases de Gröbner para calcular de maneira efetiva em anéis quocientes de anéis de polinômios sobre corpos efetivos. Aproveitaremos a oportunidade para explicar como o polinômio mínimo de um número algébrico dado pode ser calculado.

7. Bases de Gröbner e cálculos efetivos

Tendo calculado vários exemplos, estamos suficientemente familiarizamos com os anéis quocientes, para que possamos discutir o papel das bases de Gröbner nesta construção. Para falar a verdade, bases de Gröbner já apareceram mais de uma vez, disfarçadas sob a forma do único gerador de um ideal principal. Nestes exemplos, procedemos sempre da mesma maneira: dado um representante f de uma classe, e o gerador g do ideal, dividimos f por g e obtivemos r como resto. Em seguida, mostramos que a classe de f admitia um representante único de grau menor que o grau de g: o resto r da divisão. Veremos nesta seção que, usando bases de Gröbner, podemos proceder essencialmente da mesma maneira para qualquer quociente de um anel de polinômios.

Seja K um corpo efetivo e I um ideal do anel de polinômios $K[x_1, \ldots, x_n]$. Suporemos, ao longo da seção, que $<$ é uma ordem monomial deste anel. Se G

for uma base de Gröbner de I e $f \in K[x_1, \ldots, x_n]$, podemos efetuar a divisão de f por G, obtendo o resto $\mathrm{R}_G(f)$. Portanto,

$$f - \mathrm{R}_G(f) \in I,$$

o que nos dá a igualdade das classes $\overline{f} = \overline{\mathrm{R}_G(f)}$ no anel quociente $K[x_1, \ldots, x_n]/I$.

Por outro lado, sabemos pelo teorema 4.4 da página 112, que o resto se caracteriza pelo fato de nenhum monômio em seu suporte ser divisível pelo termo inicial de um elemento de G. Isto nos leva à seguinte definição. Seja $h \in K[x_1, \ldots, x_n]$ e G uma base de Gröbner de I. A classe $\overline{h}$ de h em $K[x_1, \ldots, x_n]/I$ está em *forma normal* se

$$\sup(h) \cap \langle \mathrm{in}(G) \rangle = \sup(h) \cap \mathrm{in}(I) = \emptyset.$$

Portanto, para reduzir uma classe $\overline{f}$ qualquer à sua forma normal basta dividir f por G. Isto é, $\overline{\mathrm{R}_G(f)}$ é a forma normal de $\overline{f}$.

Pelo corolário 5.3 da página 122, a forma normal de uma classe relativa a uma base de Gröbner é única. Em particular, duas classes $\overline{f}$ e $\overline{h}$ em forma normal são iguais se e somente se $f = g$. Isto facilita enormemente a comparação e o cálculo com classes, e explica porque preferiremos sempre trabalhar com as classes expressas em forma normal.

Como conseqüência da discussão anterior, podemos descrever uma base de $K[x_1, \ldots, x_n]/I$ como K-espaço vetorial.

TEOREMA 8.9. *Seja I um ideal de $K[x_1, \ldots, x_n]$ e G uma base de Gröbner de I relativamente a alguma ordem monomial. O conjunto*

$$\mathbb{T}^n \setminus \mathrm{in}(I)$$

é uma base de $K[x_1, \ldots, x_n]/I$ como K-espaço vetorial. Além disso, um monômio de $\mathbb{T}^n$ pertence a esta base se, e somente se, não for divisível por $\mathrm{in}(g)$, para algum $g \in G$.

DEMONSTRAÇÃO. Em primeiro lugar, já vimos que cada elemento de $K[x_1, \ldots, x_n]/I$ pode ser escrito como combinação linear de classes de monômios de $\mathbb{T} \setminus \mathrm{in}(I)$. Logo, estas classes formam um conjunto de geradores para o anel quociente. Falta-nos, apenas, mostrar que são linearmente independentes sobre K. Sejam $\mu_1 < \cdots < \mu_t$ monômios em $\mathbb{T} \setminus \mathrm{in}(I)$, e suponhamos que

$$a_1\overline{\mu_1} + \cdots a_t\overline{\mu_t} = \overline{0},$$

em que $a_1, \ldots, a_t \in K \setminus \{0\}$. Como esta igualdade só ocorre se

$$a_1\mu_1 + \cdots a_t\mu_t \in I,$$

temos que

$$\mathrm{in}(a_1\mu_1 + \cdots a_t\mu_t) = a_t\mu_t \in \mathrm{in}(I),$$

o que contradiz a hipótese de que $\mu_1, \ldots, \mu_t$ não pertencem ao ideal inicial de I. Como G é uma base de Gröbner de I, então

$$\mathrm{in}(I) = \langle \mathrm{in}(G) \rangle.$$

A afirmação final do enunciado do lema segue imediatamente desta igualdade. □

Como exemplo da aplicação do teorema, considere o ideal

$$I = \langle x_1 + 5x_2 + x_3, x_1^3 + x_2, x_1x_2 - x_3^2 \rangle$$

do anel $\mathbb{Q}[x_1, x_2, x_3]$. Calculando a base de Gröbner de I relativamente a lex com $x_3 < x_2 < x_1$, obtemos

$$\{625x_3^6 + 31x_3^4 + x_3^2, 9x_2 - 2500x_3^5 + x_3^3, x_1 + 5x_2 + x_3\},$$

de modo que $\mathrm{in}(I)$ contém x_1 e x_2. Portanto,

$$\mathbb{T}^n \setminus \mathrm{in}(I)$$

contém apenas potências de x_3. Como a menor potência de x_3 em $\mathrm{in}(I)$ é x_3^6, concluímos que

$$\mathbb{T}^n \setminus \mathrm{in}(I) = \{1, x_3, \ldots, x_3^5\}$$

de forma que $\mathbb{Q}[x_1, x_2, x_3]/I$ tem dimensão igual a 6 como espaço vetorial sobre $\mathbb{Q}$. Voltaremos a este exemplo em mais detalhes no próximo capítulo; veja página 267.

Observe que podemos usar este teorema para determinar *se* um dado anel quociente tem ou não dimensão finita.

COROLÁRIO 8.10. *Seja I um ideal de $K[x_1, \ldots, x_n]$ e G uma base de Gröbner de I relativamente a alguma ordem monomial. O anel quociente $K[x_1, \ldots, x_n]/I$ tem dimensão finita como K-espaço vetorial se e somente se o conjunto $\mathbb{T}^n \setminus \mathrm{in}(I)$ é finito.*

As formas normais são muito convenientes quando precisamos efetuar cálculos no anel quociente. Se I é um ideal de $K[x_1, \ldots, x_n]$ e G uma base de Gröbner de I relativamente a alguma ordem monomial, consideremos dois elementos do quociente $K[x_1, \ldots, x_n]/I$ em forma normal $\overline{f_1}$ e $\overline{f_1}$. A forma normal da sua soma e produto serão

$$\overline{f_1} + \overline{f_2} = \overline{\mathrm{R}_G(f_1 + f_2)}$$
$$\overline{f_1} \cdot \overline{f_2} = \overline{\mathrm{R}_G(f_1 \cdot f_2)}.$$

Aplicando estas regras ao anel acima teremos, por exemplo,

$$\overline{x_1^4} + \overline{x_1^3} = \overline{-\frac{125}{9}x_3^5 - \frac{4}{9}x_3^3}.$$

Cálculos como estes podem ser realizados mesmo que o quociente não tenha dimensão finita. Digamos, por exemplo que

$$J = \langle x_1x_2^2 - x_3^2, x_1^2x_3 - x_2^2 \rangle$$

no anel $\mathbb{Q}[x_1, x_2, x_3]$, que tem base de Gröbner reduzida igual a

$$\{x_1x_2^2 - x_3^2, x_1^2x_3 - x_2^2, x_1x_3^3 - x_2^4, x_2^6 - x_3^5\}.$$

Neste caso, $\mathrm{in}(J)$ é gerado por

$$\{x_1x_2^2, x_1^2x_3, x_1x_3^3, x_2^6\}.$$

de modo que

$$\mathbb{T} \setminus \mathrm{in}(J)$$

contém todas as potências de x_3, independentemente de qual seja o expoente. Em particular, o anel quociente $\mathbb{Q}[x_1, x_2, x_3]/J$ tem dimensão infinita como $\mathbb{Q}$-espaço vetorial. Mas a soma ou produto podem ser facilmente calculados pela mesma regra; por exemplo, para determinar a forma normal de

$$(\overline{x_1^3 x_2 + x_3}) \cdot (\overline{x_3^3 + 3x_2^2})$$

multiplicamos os dois polinômios, obtendo

$$x_1^3 x_2 x_3^3 + 3x_1^3 x_2^3 + x_3^4 + 3x_2^2 x_3$$

cuja divisão por G deixa resto

$$x_2 x_3^4 + 3x_2^3 x_3 + x_3^4 + 3x_2^2 x_3;$$

donde

$$(\overline{x_1^3 x_2 + x_3}) \cdot (\overline{x_3^3 + 3x_2^2}) = \overline{x_2 x_3^4 + 3x_2^3 x_3 + x_3^4 + 3x_2^2 x_3}.$$

Podemos utilizar este procedimento para calcular diretamente no corpo $\mathbb{Q}(\alpha, \beta)$, quando os números complexos α e β são algébricos, sem precisar achar um elemento primitivo para o corpo. Por exemplo, $\alpha = \sqrt[3]{2}$ e $\beta = \sqrt{5}$ têm polinômios mínimos $x^3 - 2$ e $x^2 - 5$ sobre $\mathbb{Q}$. Utilizando o teorema do homomorfismo é fácil mostrar que

$$\mathbb{Q}(\sqrt[3]{2}, \sqrt{5}) \cong \mathbb{Q}[x, y]/\langle x^3 - 2, y^2 - 5\rangle. \tag{68}$$

Como os dois polinômios têm variáveis distintas, seu S-polinômio é nulo, de forma que $\{x^3 - 2, y^2 - 5\}$ é uma base de Gröbner de $\langle x^3 - 2, y^2 - 5\rangle$, o que torna os cálculos no quociente extremamente simples. Como vimos na página 220,

$$\mathbb{Q}(\sqrt[3]{2}, \sqrt{5}) = \mathbb{Q}(\sqrt[3]{2} + \sqrt{5})$$

de modo que é possível escrever $\sqrt[3]{2}$ a partir de $\sqrt[3]{2} + \sqrt{5}$. Faremos isto usando a representação da extensão $\mathbb{Q}(\sqrt[3]{2}, \sqrt{5})$ que foi descrita acima e efetuando os cálculos através da base de Gröbner. Denotando $\overline{(x + y)}$ por u para simplificar a notação, temos, no quociente $\mathbb{Q}[x, y]/\langle x^3 - 2, y^2 - 5\rangle$ que

$$u^2 = \overline{x^2 + 2xy + 5};$$
$$u^4 = \overline{30x^2 + 20xy + 2x + 8y + 25}.$$

Portanto,

$$u^4 - 10u^2 - 8u = \overline{20x^2 - 6x - 25};$$

ao passo que,

$$3u^5 - 50u^3 - 15u^2 + 175u = \overline{-9x^2 - 200x + 125};$$

e, assim,

$$\frac{u^4 - 10u^2 - 8u}{20} + \frac{3u^5 - 50u^3 - 15u^2 + 175u}{9} - \frac{455}{36} = -\frac{2027}{90}\overline{x}.$$

Finalmente, levando em conta que u corresponde a γ e $\overline{x}$ a $\sqrt[3]{2}$ sob o isomorfismo (68), podemos concluir que

$$\sqrt[3]{2} = -\frac{90}{2027}\left(\frac{\gamma^4 - 10\gamma^2 - 8\gamma}{20} + \frac{3\gamma^5 - 50\gamma^3 - 15\gamma^2 + 175\gamma}{9} - \frac{455}{36}\right).$$

É claro que este procedimento pode ser generalizado para extensões com qualquer quantidade finita de números algébricos.

Já que estamos tratando de bases de Gröbner, vejamos como usá-las para obter o polinômio mínimo de um elemento em uma extensão algébrica. Novamente, apenas ilustraremos o procedimento no exemplo acima. Digamos que queremos determinar o polinômio mínimo de $\sqrt[3]{2} + \sqrt{5}$ sobre $\mathbb{Q}$. Para isto calcularemos na extensão $\mathbb{Q}(\sqrt[3]{2}, \sqrt{5})$. Usando a descrição em termos do anel quociente, seja t uma nova variável que fará o papel de $x + y$ e consideremos o ideal

$$J = \langle x^3 - 2, y^2 - 5, t - (x + y)\rangle$$

de $\mathbb{Q}[x, y, t]$. Isto significa que a imagem $\overline{t}$ de t em $\mathbb{Q}[x, y, t]/J$ representa o elemento $\overline{x + y}$. Como este elemento corresponde à soma $\sqrt[3]{2} + \sqrt{5}$ sob o isomorfismo

$$\mathbb{Q}[x, y]/\langle x^3 - 2, y^2 - 5\rangle \cong \mathbb{Q}(\sqrt[3]{2}, \sqrt{5}),$$

podemos concluir que é é algébrico sobre o anel quociente. Logo existe algum polinômio $f(t)$ cuja imagem em $\mathbb{Q}[x, y, t]/J$ é nula. Mas isto significa que

$$f(t) \in J \text{ donde } \ f(t) \in J \cap \mathbb{Q}[t].$$

Contudo, já sabemos determinar a interseção $J \cap \mathbb{Q}[t]$ desde que estudamos a proposição 6.4 na página 159. Para isto basta calcular a base de Gröbner G de J relativamente a lex com $t < x < y$; o polinômio puro em t contido em G será o gerador da interseção. Fazendo isto neste exemplo, obtemos uma base com os polinômios,

$$\begin{aligned} &t^6 - 15t^4 - 4t^3 + 75t^2 - 60t - 121, \\ &4054y - 60t^5 - 9t^4 + 1000t^3 - 748t + 2275, \\ &x + y - t. \end{aligned}$$

Portanto o polinômio mínimo de $\sqrt[3]{2} + \sqrt{5}$ sobre $\mathbb{Q}$ é

$$t^6 - 15t^4 - 4t^3 + 75t^2 - 60t - 121,$$

o que completa o ciclo de ideias relativo aos corpos efetivos cujo estudo iniciamos na seção anterior.

8. Comentários e complementos

Embora nosso estudo dos homomorfismos e anéis quocientes tenha sido bastante completo, o mesmo não se pode dizer do tratamento que fizemos da teoria de corpos. Desta teoria, tocamos apenas ponta do iceberg. Em particular, nada dissemos sobre teoria de Galois, a partir da qual se pode prever, de maneira algorítmica, se as raízes de uma dada equação polinomial (em

uma variável com coeficientes racionais) pode ser descrita a partir das quatro operações fundamentais (adição, subtração, multiplicação e divisão) e da extração de raízes de qualquer ordem. Desde o trabalho de N. H. Abel no século XIX, sabemos que tal tipo de fórmula para as raízes só é viável em geral para equações de grau menor que cinco. Entretanto, E. Galois foi mais longe e, utilizando teoria de grupos, inventou um algoritmo capaz de determinar se uma fórmula deste tipo existe ou não para uma dada equação. Além disso, quando a fórmula existe, os métodos de Galois nos permitem determiná-la.

A teoria de Galois é uma área muito rica da matemática, que tem uma forte componente computacional. Entretanto, a interseção da teoria de Galois com os métodos elementares da álgebra comutativa aqui discutidos é muito pequena. De fato, esta teoria está lastreada em cálculos com grupos, uma área que não exploramos neste livro. Para mais detalhes consulte o artigo [**61**] ou o livro [**28**].

9. Exercícios

1. Sejam A e B anéis e $\phi : A \to B$ uma aplicação que satisfaz $\phi(a + a') = \phi(a) + \phi(a')$ e $\phi(a \cdot a') = \phi(a) \cdot \phi(a')$ para todo $a, a' \in A$. Mostre que cada uma das seguintes condições é suficiente para garantir que $\phi(1) = 1$:
   (a) A e B são corpos,
   (b) A e B contêm um corpo K e $\phi(K) \subset K$,
   (c) $\phi \neq 0$ e B é um domínio.

2. Mostre que a imagem de um homomorfismo de anéis $\phi : A \to B$ é um subanel de B.

3. Dizemos que uma propriedade P é *estável por isomorfismo* se, dados dois anéis isomorfos $A \cong B$ quaisquer, podemos sempre afirmar que A satisfaz P se, e somente se, B satisfaz P. Prove que as seguintes propriedades são estáveis por isomorfismo:
   (a) ter divisores de zero;
   (b) ser domínio;
   (c) ser corpo.

4. Mostre que I é um ideal de A se, e somente se, existe um homomorfismo ϕ, em algum anel B, do qual I é o núcleo.

5. Sejam A um anel e K um corpo. Mostre que se $\phi : A \to K$ é um homomorfismo sobrejetor, então $N(\phi)$ é um ideal máximo.

6. Sejam A um anel e K um corpo. Mostre que se $\phi : K \to A$ é um homomorfismo, então $N(\phi) = 0$.

7. Seja D um domínio e F um corpo. Suponha que existe um homomorfismo injetivo $\psi : D \to F$.

(a) Mostre que ψ pode ser estendido a um homomorfismo injetivo $\overline{\psi} : Q(D) \to F$.

Dizer que $\overline{\psi}$ *estende* ψ significa que $\overline{\psi}(a/1) = \psi(a)$.

(b) Use (a) para mostrar que $Q(A)$ é o menor corpo (com respeito à inclusão), que contém D.

8. Seja I um ideal de um anel A. Prove que todo ideal do anel quociente A/I é imagem pela projeção canônica $\pi : A \to A/I$ de um ideal J de A que contém I.

9. Sejam $I \subset J$ ideais de um anel A e $\pi : A \to A/I$ a projeção canônica. Prove que:
   (a) $\pi(J)$ é ideal primo de A/I se, e somente se, J é um ideal primo de A;
   (b) $\pi(J)$ é ideal máximo de A/I se, e somente se, J é um ideal máximo de A.

10. Sejam $I \subset J$ ideais de um anel A e $\pi : A \to A/I$ a projeção canônica. Use o teorema do homomorfismo para provar que
$$(A/I)/\pi(J) \cong A/J.$$

11. Seja $K \subset L$ uma extensão de corpos e t uma variável. Dado um elemento $r \in L$ transcendente sobre K, considere a aplicação
$$\phi : K(t) \to L$$
definida por $\phi(f(t)) = f(r)$ para cada função racional $f \in K(t)$. Prove que ϕ é um homomorfismo injetivo de corpos.

12. Calcule um elemento primitivo para cada uma das seguintes extensões de $\mathbb{Q}$:
   (a) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$;
   (b) $\mathbb{Q}(\sqrt[3]{2}, \sqrt[5]{3})$;
   (c) $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

13. Calcule o grau de cada uma das extensões do exercício anterior.

14. Use bases de Gröbner para determinar o polinômio mínimo do elemento primitivo encontrado para cada uma das extensões do exercício ???.

15. O objetivo deste exercício é estudar os ideais do anel $\mathbb{Z}[x]$, dos polinômios em uma variável com coeficientes inteiros. Seja p um número primo positivo.
   (a) Mostre que o ideal $\langle p, x\rangle$ é máximo mas não é principal.
   (b) Mostre que o ideal principal $\langle p\rangle$ é primo mas não é máximo.
   (c) Mostre que
$$\mathbb{Z}[x]/\langle p, x\rangle \cong \mathbb{Z}_p[x].$$

CAPíTULO 9

Geometria algébrica

Neste capítulo estudaremos de maneira mais sistemática os objetos geométricos definidos por conjuntos algébricos. Começaremos por relembrar as definições básicas. Como sempre K denotará um corpo efetivo contido em $\mathbb{C}$.

1. Conjuntos algébricos

Seja S um subconjunto de $K[x_1, \ldots, x_n]$. O *conjunto algébrico* definido por S é

$$\mathcal{Z}(S) = \{p \in \mathbb{C}^n : f(p) = 0 \quad \text{para todo} \quad f \in S\}.$$

Apesar dos pontos de $\mathcal{Z}(S)$ terem coordenadas complexas, quaisquer eventuais esboços que fizermos destas figuras corresponderão aos pontos cujas coordenadas são reais, que são os únicos que podemos desenhar. Já os polinômios de S terão coeficientes em K, um subcorpo efetivo de $\mathbb{C}$ que será quase sempre $\mathbb{Q}$.

Na seção 3 do capítulo 3 verificamos que

$$\mathcal{Z}(S) = \mathcal{Z}(\langle S \rangle),$$

em que temos o conjunto S do lado esquerdo e o ideal de $K[x_1, \ldots, x_n]$ gerado por S do lado direito. Esta igualdade tem a consequência imediata de sempre nos permitir definir conjuntos algébricos a partir de ideais, quando isto for conveniente. Entretanto, combinando-a com o teorema da base de Hilbert podemos também concluir que, como qualquer ideal de $K[x_1, \ldots, x_n]$ admite um conjunto finito de geradores, sempre é possível escolher o conjunto S como sendo finito ao definir um conjunto algébrico. Usaremos estes fatos livremente no que segue.

Já encontramos muitos exemplos de conjuntos algébricos neste livro e também estudamos algumas de suas propriedades, a mais importante das quais está contida no teorema 3.12 cujo enunciado reproduzimos abaixo.

TEOREMA 9.1. *Se I é um ideal $K[x_1, \ldots, x_n]$, então,*

$$\mathrm{I}(\mathcal{Z}(I)) = \sqrt{I}.$$

Reciprocamente, se $X \subseteq \mathbb{C}^n$ for um conjunto algébrico, então

$$\mathcal{Z}(\mathrm{I}(X)) = X.$$

Lembre-se que o radical $\sqrt{I}$ de um ideal I em um anel A é definido como sendo o conjunto

$$\sqrt{I} = \{a \in A | a^k \in I \text{ para algum inteiro } k > 0\}$$

que, como vimos na proposição 3.9 também é um ideal de A. Como calcular o radical é uma das questões que analisaremos mais adiante neste capítulo.

Tendo expresso os conjuntos algébricos em termos de ideais, é razoável perguntar de que forma a geometria destes conjuntos se reflete em propriedades algébricas dos ideais. Começaremos com algumas propriedades bastante elementares. Por exemplo:

> se I e J são ideais de $K[x_1, \ldots, x_n]$ e $I \subseteq J$, então qual a relação entre $\mathcal{Z}(I)$ e $\mathcal{Z}(J)$?

Isto é fácil de determinar. De fato se $p \in \mathcal{Z}(J)$, então $f(p) = 0$ para todo $f \in J$. Como $I \subseteq J$, também será verdade que $h(p) = 0$ para todo $h \in I$. Logo $p \in \mathcal{Z}(I)$. Portanto,

$$\text{se } I \subseteq J \text{ então } \mathcal{Z}(I) \supseteq \mathcal{Z}(J).$$

Observe a inversão da inclusão: quando passamos dos ideais para os conjuntos algébricos, $\subseteq$ torna-se $\supseteq$. Como consequência do que acabamos de mostrar, temos que

$$\text{se } I = J \text{ em } K[x_1, \ldots, x_n] \text{ então } \mathcal{Z}(J) = \mathcal{Z}(I).$$

E a recíproca? Isto é, se I e J são ideais de $K[x_1, \ldots, x_n]$ e $\mathcal{Z}(J) = \mathcal{Z}(I)$, o que podemos afirmar sobre $I \subseteq J$? A resposta é dada na proposição seguinte.

COROLÁRIO 9.2. *Sejam I e J ideais de $K[x_1, \ldots, x_n]$. Então, $\mathcal{Z}(I) = \mathcal{Z}(J)$ se, e somente se, $\sqrt{I} = \sqrt{J}$.*

DEMONSTRAÇÃO. Já vimos que a igualdade dos ideais garante a igualdade dos conjuntos algébricos correspondentes. Falta-nos mostrar que, se $\mathcal{Z}(I) = \mathcal{Z}(J)$, então $\sqrt{I} = \sqrt{J}$. Mas, para isto, basta provar que se $\mathcal{Z}(I) \subseteq \mathcal{Z}(J)$, então $\sqrt{I} \supseteq \sqrt{J}$; lembre-se que a inclusão é invertida na passagem entre ideais e seus conjuntos algébricos. A outra inclusão é análoga.

Suponha, então, que $f \in \sqrt{J}$. Isto implica que $f^k \in J$ para algum inteiro $k > 0$. Mas, pela definição de conjunto algébrico,

$$f^k(p) = 0 \text{ para todo } p \in \mathcal{Z}(J).$$

Como $\mathcal{Z}(I) \subseteq \mathcal{Z}(J)$ temos, em particular, que $f^k(p) = 0$ para todo $p \in \mathcal{Z}(I)$. Assim, pelo teorema 9.1, $f \in \sqrt{I}$, como queríamos mostrar. □

Vejamos, agora, o que ocorre aos ideais quando conjuntos algébricos são submetidos às operações de união e interseção. Sejam $g_1, \ldots, g_s$ e $h_1, \ldots, h_t$ polinômios em $K[x_1, \ldots, x_n]$ e denotemos por

$$X = \mathcal{Z}(g_1, \ldots, g_s) \text{ e } Y = \mathcal{Z}(h_1, \ldots, h_t)$$

os respectivos conjuntos algébricos. Então $X \cap Y$ é o conjunto dos pontos que satisfazem simultaneamente as equações que definem X e as que definem Y. Em outras palavras,

$$X \cap Y = \mathcal{Z}(g_1, \ldots, g_s, h_1, \ldots, h_t).$$

Em particular, $X \cap Y$ fica definido pelo ideal

$$M = \langle g_1, \ldots, g_s, h_1, \ldots, h_t \rangle$$

de $K[x_1, \ldots, x_n]$. Precisamos entender qual a relação deste ideal com os ideais

$$I = \langle g_1, \ldots, g_s \rangle \text{ e } J = \langle h_1, \ldots, h_t \rangle, \tag{69}$$

que definem, respectivamente, X e Y. Por definição, um elemento $f \in M$ pode ser escrito na forma

$$q_1 g_1 + \cdots + q_s g_s + p_1 h_1 + \cdots + p_t h_t$$

para uma escolha adequada de polinômios qs e ps em $K[x_1, \ldots, x_n]$. Entretanto,

$$q_1 g_1 + \cdots + q_s g_s \in I \text{ e } p_1 h_1 + \cdots + p_t h_t \in J.$$

De modo que f pertence ao conjunto

$$I + J = \{g + h : g \in I \text{ e } h \in J\}.$$

É fácil verificar que $I + J$ também é um ideal de $K[x_1, \ldots, x_n]$; veja exercício ???. Assim, provamos que $\mathcal{Z}(I) \cap \mathcal{Z}(J) \subseteq \mathcal{Z}(I + J)$. A inclusão oposta é provada de maneira semelhante, de modo que obtemos a igualdade

$$\mathcal{Z}(I) \cap \mathcal{Z}(J) = \mathcal{Z}(I + J).$$

Tendo resolvido o problema da interseção, passamos a considerar a união. Digamos que I e J são os ideais de $K[x_1, \ldots, x_n]$ definidos na equação (69), e que $p \in \mathcal{Z}(I) \cup \mathcal{Z}(J)$. Então $p \in \mathcal{Z}(I)$ ou $p \in \mathcal{Z}(J)$. Portanto, ou $g(p) = 0$ para todo $g \in I$, ou $h(p) = 0$ para todo $h \in J$. Para expressar esta afirmação em uma única equação, basta lembrar que o produto de dois números dá zero se, e somente se, um dos dois é zero. Assim, $g(p) = 0$ ou $h(p) = 0$ é equivalente a

$$(gh)(p) = g(p)h(p) = 0.$$

Contudo, ao contrário do que ocorreu na soma, o conjunto

$$S = \{gh : g \in I \text{ e } h \in J\}$$

não é um ideal de $K[x_1, \ldots, x_n]$. Por exemplo, se tomarmos

$$I = \langle x, y \rangle \text{ e } J = \langle x, z \rangle$$

ideais de $\mathbb{Q}[x, y, z]$, vemos que x^2 e yz são produtos de elementos de I por J. Contudo, $x^2 + yz$ não pode ser escrito como o produto de um elemento de I por um elemento de J. Portanto, o conjunto dos produtos não é um ideal neste caso. A saída é tomar, não o conjunto dos produtos, mas sim o ideal que ele gera. Isto nos leva a seguinte definição

$$IJ = \langle gh : g \in I \text{ e } h \in J \rangle.$$

Portanto,

$$\mathcal{Z}(I) \cup \mathcal{Z}(J) = \mathcal{Z}(IJ).$$

Podemos usar esta última igualdade para identificar o conjunto algébrico definido por um ideal monomial. Considere, por exemplo, $\mathcal{Z}(x^2z, xyz, y^2z)$. Pondo z em evidência em cada gerador, vemos que

$$I = \langle x^2z, xyz, y^2z\rangle = \langle x^2, xy, y^2\rangle\langle z\rangle.$$

Por sua vez, $\langle x^2, xy, y^2\rangle$ contém todos os monômios de grau 2 nas variáveis x e y, de modo que

$$\langle x^2, xy, y^2\rangle = \langle x, y\rangle^2.$$

Portanto,

$$I = \langle x, y\rangle^2\langle z\rangle,$$

como ideal de $K[x_1, \ldots, x_n]$. Segue, assim, da discussão anterior que

$$\mathcal{Z}(I) = \mathcal{Z}(x, y) \cup \mathcal{Z}(z) = (\mathcal{Z}(x) \cap \mathcal{Z}(y)) \cup \mathcal{Z}(z),$$

pois

$$\mathcal{Z}(J^2) = \mathcal{Z}(J),$$

qualquer que seja o ideal J. Logo, $\mathcal{Z}(x^2yz, xy^2z, y^3z) = \mathcal{Z}(I)$ corresponde à união da reta $x = y = 0$ com o plano $z = 0$. O próximo teorema resume o que aprendemos nesta seção.

TEOREMA 9.3. *Sejam I e J ideais de $K[x_1, \ldots, x_n]$.*

(1) *Se $I \subseteq J$ então $\mathcal{Z}(J) \subseteq \mathcal{Z}(I)$.*
(2) *$I = J$ se, e somente se, $\mathcal{Z}(J) = \mathcal{Z}(I)$.*
(3) *$\mathcal{Z}(I) \cap \mathcal{Z}(J) = \mathcal{Z}(I + J)$, em que $I + J = \{g + h : g \in I \text{ e } h \in J\}$.*
(4) *$\mathcal{Z}(I) \cup \mathcal{Z}(J) = \mathcal{Z}(IJ)$ em que $IJ = \langle gh : g \in I \text{ e } h \in J\rangle$.*

Há um resultado particular referente à decomposição de conjuntos algébricos que precisaremos utilizar na próxima seção e que pode ser visto como uma consequência do teorema acima e da seguinte proposição.

PROPOSIÇÃO 9.4. *Seja I um ideal do anel $K[x_1, \ldots, x_n]$ e suponha que $I \cap K[x_1]$ é gerado por um polinômio não nulo g. Se $g = p_1 \cdots p_s$, em que os ps são polinômios irredutíveis sobre K* distintos*, então*

(1) $I = (I + \langle p_1\rangle) \cap \cdots \cap (I + \langle p_s\rangle)$
(2) $\sqrt{I} = \sqrt{I + \langle p_1\rangle} \cap \cdots \cap \sqrt{I + \langle p_s\rangle}$.

DEMONSTRAÇÃO. É claro que

$$I \subseteq (I + \langle p_1\rangle) \cap \cdots \cap (I + \langle p_s\rangle),$$

em que $\langle p_1\rangle$ denota o ideal gerado por p_j em $K[x_1, \ldots, x_n]$. Para provar a inclusão oposta observe que, dado

$$f \in (I + \langle p_1\rangle) \cap \cdots \cap (I + \langle p_s\rangle),$$

existem polinômios $r_j \in I$ e $q_j \in K[x_1, \ldots, x_n]$, tais que

$$f = r_j + q_j p_j$$

para $1 \leq j \leq s$. Assim, se

$$P_j = p_1 \cdots p_{j-1} p_{j+1} \cdots p_s,$$

denota o produto dos ps cujo índice é diferente de j, temos que

$$f \cdot P_j = r_j P_j + q_j p_j P_j = r_j P_j + q_j g_1 \in J, \tag{70}$$

já que tanto r_j, quanto g_1 pertencem ao ideal J. Contudo, os P_j são elementos do anel de polinômios em uma variável $K[x_1]$. Além disso, p_j divide todos os P_i para $i \neq j$, mas não P_j; de modo que

$$\operatorname{mdc}(P_1, \ldots, P_s) = 1.$$

Portanto, pelo algoritmo euclidiano estendido, existem $h_j \in K[x_1]$, tais que

$$1 = h_1 P_1 + \cdots + h_s P_s.$$

Multiplicando esta equação por f, concluímos por (70) que

$$f = h_1 \cdot fP_1 + \cdots + h_s \cdot fP_s \in I.$$

Com isto, provamos a igualdade em (1). A igualdade dos radicais segue de (1) e da proposição 3.13 da página 90. □

Temos, então o seguinte resultado, que é consequência imediata da parte (1) da proposição e da parte (4) do teorema 9.3.

COROLÁRIO 9.5. *Se I é um ideal e f e g são polinômios em $K[x_1, \ldots, x_n]$, então*

$$\mathcal{Z}(I + \langle fg \rangle) = \mathcal{Z}(I + \langle f \rangle) \cup \mathcal{Z}(I + \langle g \rangle).$$

2. A lemniscata de Bernoulli

A justa apreciação dos resultados introduzidos na seção anterior requer um exemplo razoavelmente substancial. Para isto, exploraremos, utilizando as ferramentas de bases de Gröbner e as propriedades dos conjuntos algébricos, o comportamento de um caso especial do sistema de alavancas de Watt; cf. página 171. Começaremos relembrando em que o sistema consiste, no caso que desejamos tratar.

Na figura 1 os pontos A e D são fixos e a distância entre eles é igual a $\sqrt{2}$ unidades. Já os segmentos $\overline{AB}$ e $\overline{CD}$ têm ambos comprimento igual a uma unidade, ao passo que $\overline{BC}$ também tem comprimento $\sqrt{2}$ unidades.
O sistema é articulado nos pontos A, B, C e D e, ao ser movimentada, o ponto médio P do segmento BC descreve uma curva cuja equação queremos determinar. Como veremos, trata-se de uma curva definida pelo anulamento de um polinômio em duas variáveis e, portanto, de uma curva que é um conjunto algébrico. Tais curvas são conhecidas como *curvas algébricas*.

Para preservar a simetria da construção, escolheremos

$$A = (-\sqrt{2}/2, 0) \text{ e } D = (\sqrt{2}, 0).$$

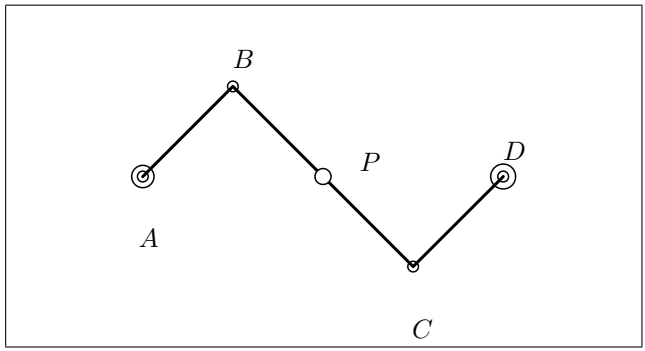


FIGURA 1. Engrenagem de Watt

Como $\overline{BC}$ tem comprimento igual a $\sqrt{2}$ e $\overline{AC} = \overline{CD} = 1$, as equações equivalentes que descrevem as restrições sobre os pontos B e C são

$$h_1 = (b_1 - \sqrt{2}/2)^2 + b_2^2 - 1 = 0$$
$$h_2 = (c_1 + \sqrt{2}/2)^2 + c_2^2 - 1 = 0$$
$$h_3 = (b_1 - c_1)^2 + (b_2 - c_2)^2 - 2 = 0.$$

Como P é o ponto médio do segmento BC, temos ainda que

$$h_4 = 2x_1 - (b_1 + c_1)$$
$$h_5 = 2x_2 - (b_2 + c_2).$$

Obter a equação da curva descrita pelo ponto P equivale a encontrar uma equação que só envolva as coordenadas x_1 e x_2 deste ponto. Para isto usaremos a estratégia já aplicada na seção 9 do capítulo 6. Isto é, calculamos uma base de Gröbner G de

$$I = \langle h_1, \ldots, h_5 \rangle$$

relativamente a uma ordenação lexicográfica para a qual x_1 e x_2 são as duas menores variáveis. Em seguida, usamos a proposição 6.4, segundo a qual $G \cap \mathbb{Q}[x_1, x_2]$ será constituída pelos geradores do ideal

$$I \cap \mathbb{Q}[x_1, x_2].$$

Estes geradores determinam o lugar dos pontos médios de $\overline{BC}$ à medida que o mecanismo se move.

Para implementar esta estratégia, calcularemos a base de Gröbner G de I relativamente à ordem lexicográfica com

$$x_1 < x_2 < b_1 < b_2 < c_1 < c_2.$$

Esta base tem 7 elementos, dos quais apenas

$$x_1^6 + 3\,x_1^4\,x_2^2 - 2\,x_1^4 + 3\,x_1^2\,x_2^4 - 2\,x_1^2\,x_2^2 + x_1^2 + x_2^6 - x_2^2$$

pertence a $\mathbb{Q}[x_1, x_2]$. Mas este polinômio pode ser fatorado como

$$\left(x_1^2 + x_2^2 - 1\right)\left(x_1^4 + 2\,x_1^2\,x_2^2 - x_1^2 + x_2^4 + x_2^2\right)$$

de modo que, pela proposição 9.3, a curva algébrica que desejamos pode ser escrita como a união da circunferência

$$x_1^2 + x_2^2 = 1 \tag{71}$$

com a curva

$$x_1^4 + 2\,x_1^2\,x_2^2 - x_1^2 + x_2^4 + x_2^2 = 0.$$

Por sua vez, esta última equação é igual a

$$(x_1^2 + x_2^2)^2 - (x_1^2 - x_2^2) = 0. \tag{72}$$

Uma busca entre as equações de curvas clássicas mostra que se trata da *lemniscata de Bernoulli*. O nome lemniscata foi escolhido por Jakob Bernoulli porque, segundo ele

> sua forma lembra a de um número oito deitado ∞, ou uma faixa ou fita [leminisci] dobrada em um nó, *d'un noeud de ruban Gallis* [um nó de fita Galês, em francês no original];

veja [**3**, p. 609]. Bernoulli acreditava haver sido o primeiro a estudar esta curva em seu artigo *Construtio Curvæ Accessus et Recessus aequabilis* [**3**, pp. 608–612], publicado na *Acta Eruditorum* em 1694. Entretanto, sem que soubesse, a curva já havia sido estudada por Giovanni Domenico Cassini, como um exemplo das curvas hoje conhecidas como *ovais de Cassini*. Na figura 2 temos a lemniscata de equação (72) em torno da qual está a circunferência (71).

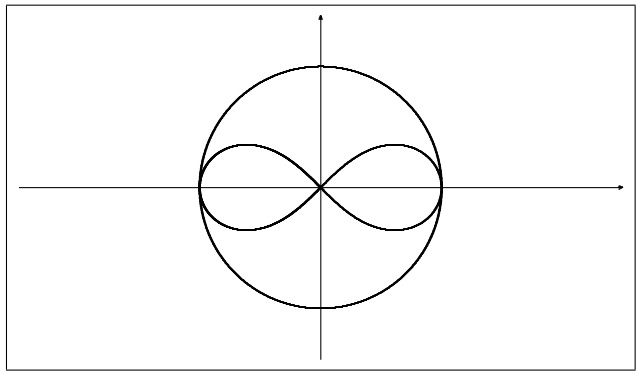


FIGURA 2. A lemniscata e a circunferência

No caso específico do mecanismo que gera a lemniscata, queremos ser mais ousados. Em vez de obter apenas a equação dos pontos P da curva, gostaríamos também de ter equações capazes de descrever a posição dos pontos B e C correspondentes a cada posição de P. Para isto, começaremos por recalcular a base de Gröbner, adicionando ao ideal I o polinômio

$$h_6 = x_1^4 + 2\,x_1^2\,x_2^2 - x_1^2 + x_2^4 + x_2^2.$$

Fazemos isto porque estamos interessados apenas nos pontos que pertencem à lemniscata e, por isso, queremos descartar aqueles que estão sobre a circunferência. Calculando a base de Gröbner de

$$\langle h_1, \ldots, h_5, h_6 \rangle$$

relativamente à mesma ordenação lexicográfica utilizada anteriormente, obtemos a base que chamaremos de H, e que consiste dos polinômios

$$\begin{aligned}
g_1 &= c_1 - \frac{1}{2}\, x_1^2\, \sqrt{2} - x_1 - \frac{1}{2}\, x_2^2\, \sqrt{2},\\
g_2 &= c_2 + b_2 - 2\, x_2,\\
g_3 &= b_1 + \frac{1}{2}\, x_1^2\, \sqrt{2} - x_1 + \frac{1}{2}\, x_2^2\, \sqrt{2},\\
g_4 &= b_2^2 - x_1^3\, \sqrt{2} + \frac{1}{2}\, x_1^2 - x_1\, x_2^2\, \sqrt{2} + x_1\, \sqrt{2} - \frac{3}{2}\, x_2^2 - \frac{1}{2},\\
g_5 &= b_2\, x_2 - \frac{1}{2}\, x_1^3\, \sqrt{2} - \frac{1}{2}\, x_1\, x_2^2\, \sqrt{2} + \frac{1}{2}\, x_1\, \sqrt{2} - x_2^2,\\
g_6 &= x_1^4 + 2\, x_1^2\, x_2^2 - x_1^2 + x_2^4 + x_2^2,
\end{aligned}$$

além de

$$\begin{aligned}
g_7 = b_2\, x_1^3 - b_2\, x_1 - x_1^3\, x_2 - \frac{1}{2}\, x_1^2\, x_2^3\, \sqrt{2} + \frac{1}{2}\, x_1^2\, x_2\, \sqrt{2} + x_1\, x_2 - \\
\frac{1}{2}\, x_2^5\, \sqrt{2} - x_2^3\, \sqrt{2} - \frac{1}{2}\, x_2\, \sqrt{2},
\end{aligned}$$

Observe que se $x_2 \neq 0$ então as coordenadas dos pontos B e C são facilmente calculadas a partir dos demais elementos de H. De fato, c_1 e b_1 são obtidas diretamente a partir de g_1 e g_3 como função das coordenadas x_1 e x_2 de P. Além disso, como estamos supondo que $x_2 \neq 0$, a coordenada b_2 também é obtida a partir das coordenadas de P, dessa vez usando g_5. Finalmente, c_2 é calculada a partir de g_2. Sobraram dois polinômios, que não utilizamos nestes cálculos; a saber, g_4 e g_7. O fato de termos podido calcular P, B e C sem utilizá-los sugere que se $x_2 \neq 0$ então estes polinômios são redundantes. Para testar esta hipótese calcularemos a base de Gröbner de

$$\langle g_1, \ldots, g_7, x_2 t - 1 \rangle,$$

cujos polinômios são

$$\begin{aligned}
&c_1 - \frac{1}{2}\, x_1^2\, \sqrt{2} - x_1 - \frac{1}{2}\, x_2^2\, \sqrt{2},\\
&c_2 + \frac{1}{2}\, x_1^3\, \sqrt{2}\, u + \frac{1}{2}\, x_1\, x_2\, \sqrt{2} - \frac{1}{2}\, x_1\, \sqrt{2}\, u - x_2,\\
&b_1 + \frac{1}{2}\, x_1^2\, \sqrt{2} - x_1 + \frac{1}{2}\, x_2^2\, \sqrt{2},\\
&b_2 - \frac{1}{2}\, x_1^3\, r\, u - \frac{1}{2}\, x_1\, x_2\, \sqrt{2} + \frac{1}{2}\, x_1\, \sqrt{2}\, u - x_2,\\
&x_1^4 + 2\, x_1^2\, x_2^2 - x_1^2 + x_2^4 + x_2^2,\\
&x_2\, u - 1;
\end{aligned}$$

confirmando, assim, nossa suspeita de que aqueles dois polinômios são mesmos desnecessários, *desde que* $x_2 \neq 0$.

Mas o que acontece se $x_2 = 0$? Substituindo x_2 por zero em H e recalculando a base de Gröbner neste caso, obtemos

$$c_1 - \frac{1}{2}\, x_1^2\, \sqrt{2} - x_1, \quad c_2 + b_2, \quad b_1 + \frac{1}{2}\, x_1^2\, \sqrt{2} - x_1, \quad b_2^2 + \frac{1}{2}\, x_1^2 - \frac{1}{2}, \quad x_1^3 - x_1.$$

Vemos, de imediato, que há polinômios nesta base que podem ser fatorados, como é o caso de $x_1^3 - x_1$. Na esperança de poder simplificar ainda mais a base, vamos utilizar a estratégia de fatorar os polinômios que lá aparecem e recalcular bases separadas nas quais inserimos um fator de cada vez. Além disso, repetiremos isto recursivamente para cada um dos polinômios que vier a ser acrescentado às bases pelo algoritmo de Buchberger. O resultado final é a seguinte lista de bases

$$\begin{aligned}
H_1 &= \left\{ x_1,\ b_2 + c_2,\ b_1,\ c_2^2 - \frac{1}{2},\ c_1 \right\},\\
H_2 &= \left\{ x_1 - 1,\ \sqrt{2} - 2\, c_1 + 2,\ b_2,\ b_1 + c_1 - 2,\ c_2,\ c_1^2 - 2\, c_1 + \frac{1}{2} \right\},\\
H_3 &= \left\{ x_1 + 1,\ \sqrt{2} - 2\, c_1 - 2,\ b_2,\ b_1 + c_1 + 2,\ c_2,\ c_1^2 + 2\, c_1 + \frac{1}{2} \right\}.
\end{aligned}$$

Mas, pelo corolário 9.5, isto significa que

$$\mathcal{Z}(H \cup \{x_2\}) = \mathcal{Z}(H_1) \cup \mathcal{Z}(H_2) \cup \mathcal{Z}(H_3). \tag{73}$$

Resta-nos entender o que esta decomposição nos diz a respeito do comportamento do sistema.

Como $\mathcal{Z}(H \cup \{x_2\})$ é o conjunto dos pontos em que P está sobre o eixo OX, temos pela equação (73) que isto corresponde a apenas três configurações possíveis do sistema. Resolvendo o sistema de equações obtido igualando a

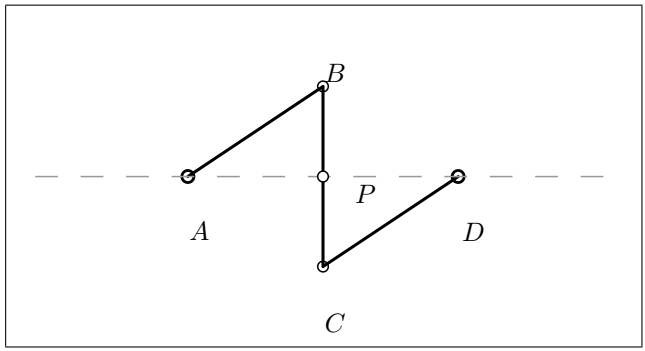


FIGURA 3. O caso $P = (0, 0)$

zero os polinômios de H_1, obtemos os pontos

$$P = (0, 0), \quad B = \left(0, \pm\frac{1}{\sqrt{2}}\right) \quad \text{e} \quad C = \left(0, \mp\frac{1}{\sqrt{2}}\right)$$

de modo que o sistema assume a posição da figura 3 neste caso. Como a distância entre A e B é igual a $\sqrt{2}$, temos neste caso que

$$\overline{AP} = \overline{PD} = \frac{\sqrt{2}}{2}.$$

Por outro lado, $\overline{AB} = \overline{DB} = 1$, de modo que

$$\overline{AP}^2 + \overline{PB}^2 = \overline{AB}^2 \quad \text{e} \quad \overline{DP}^2 + \overline{PC}^2 = \overline{BC}^2$$

de forma que os triângulos ABP e CDP são ambos retângulos pela recíproca do *teorema de Pitágoras*; proposição 48 do Livro I dos *Elementos* de Euclides.

As outras duas configurações são simétricas e basta analisar uma delas. Por exemplo, resolvendo o sistema obtido igualando a zero os polinômios de H_2, obtemos

$$P = (1, 0), \quad B = \left(\frac{2-\sqrt{2}}{2}, 0\right) \quad \text{e} \quad C = \left(\frac{2+\sqrt{2}}{2}, 0\right)$$

que corresponde à posição do sistema em que os braços estão todos alinhados, como ilustrado na figura 4.

Você pode estar se perguntando: e daí? Acontece que estas configurações são extremamente especiais do ponto de vista do comportamento mecânico da engrenagem. Imagine, por exemplo, que o sistema é movido por um motor cujo eixo de rotação é perpendicular ao plano do sistema e se liga a ela no ponto A. Para fixar as idéias, diremos que o eixo do motor roda em sentido horário.

Neste caso é a rotação do braço AB em torno de A que movimenta todo o resto da engrenagem. Quando a configuração dos braços coincide com aquela

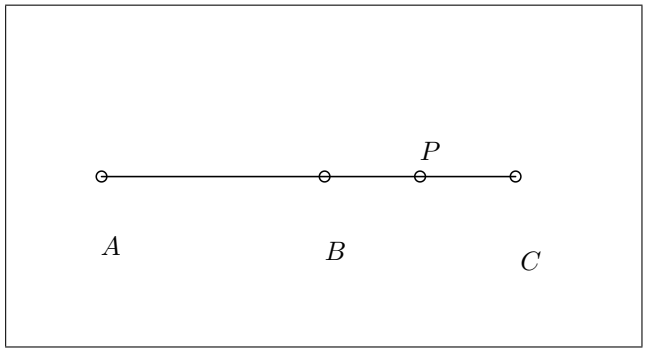


FIGURA 4. O caso $P = (1, 0)$

ilustrada na figura 1, o braço AB funciona como uma alavanca que atua sobre BC. Entretanto, quando AB e BC estão alinhados, como na figura 4, o efeito de alavanca deixa de existir e o braço AB fica momentaneamente parado. Temos, assim, o que é conhecido como um *ponto morto* desta engrenagem.

Entretanto, este não é o único papel que os pontos $(-1, 0)$ e $(1, 0)$ desempenham no funcionamento desta engrenagem. Para entender o que mais pode acontecer note que, na figura 2 estes pontos pertencem tanto à lemniscata quanto à circunferência, e que *ambas podem ser geradas pelo mecanismo*. Por isso, estes também são pontos em que pode haver mudança no comportamento do sistema de alavancas, que deixa de mover-se ao longo da lemniscata e passa a mover-se em uma circunferência, ou vice-versa. Algo semelhante ocorre no ponto $(0, 0)$. Ao atingir este ponto, o sistema de Watt pode mover-se de duas maneiras diferentes: pode avançar da parte superior da alça esquerda da lemniscata para a alça direita, ou pode continuar movendo-se sobre a alça esquerda, de cima para baixo. Portanto, todos estes são pontos em que o comportamente deste sistema mecânico fica essencialmente indeterminado, a não ser que sejam tomadas precauções adicionais.

Embora a análise que fizemos esteja restrita a um sistema de alavancas bastante simples, fenômenos semelhantes ocorrem em sistemas mecânicos mais complexos, como os que movimentam braços robóticos em fábricas ou plataformas paralelas em simuladores de voo. No entanto, em ambos os casos, um mecanismo que tenha comportamento não totalmente predizível pode levar a efeitos catastróficos. Daí a importância de analisar cuidadosamente o movimento destes sistemas no intuito de descobrir tais pontos especiais. Isto pode ser feito usando bases de Gröbner e uma estratégia semelhante a que adotamos aqui—ainda que recursos matemáticos e computacionais mais poderosos sejam necessários. Para mais detalhes consulte [**17**, capítulo 6] e [**51**].

3. Conjuntos construtivos e parametrizações

Há uma operação cujo efeito sobre conjuntos algébricos não fez parte de nossa discussão na seção 1: a diferença. Lembre-se que, se X e Y são subconjuntos de um conjunto $\mathcal{C}$, então $X \setminus Y$ é o conjunto dos elementos de X que não pertencem a Y. Um caso particular desta operação é o complementar de X em $\mathcal{C}$, que é $\overline{X} = \mathcal{C} \setminus X$. Reciprocamente, podemos definir a diferença a partir do complementar pela equação

$$X \setminus Y = X \cap \overline{Y}.$$

A razão pela qual não tratamos ainda da diferença é simples: a diferença entre dois conjuntos algébricos *não é* um conjunto algébrico. Vejamos um exemplo bastante simples. No espaço complexo de dimensão um, os conjuntos algébricos correspondem aos zeros de uma equação polinomial em uma variável. Contudo, estas equações têm sempre uma quantidade finita de zeros, que não pode exceder o grau da equação. Portanto, todo conjunto algébrico de $\mathbb{C}$ é finito. Reciprocamente, um conjunto finito

$$X = \{\alpha_1, \ldots, \alpha_s\} \subset \mathbb{C},$$

é algébrico sobre $\mathbb{C}$, porque corresponde aos zeros da equação

$$(x - \alpha_1) \cdots (x - \alpha_s).$$

Entretanto, se X for um conjunto finito, $\mathbb{C} \setminus X$ é infinito, de modo que não pode ser um conjunto algébrico.

Outro contexto em que conjuntos algébricos dão lugar a outros que não são algébricos ocorre quando consideramos suas imagens por aplicações polinomiais. Uma aplicação

$$\phi : \mathbb{C}^m \to \mathbb{C}^n$$

pode ser definida em termos de coordenadas como

$$\phi(p) = (\phi_1(p), \ldots, \phi_n(p)),$$

em que $p \in \mathbb{C}^m$ e ϕ_j é uma função de $\mathbb{C}^m$ em $\mathbb{C}$ para $1 \leq j \leq n$. Dizemos que ϕ é *polinomial* se ϕ_j é um polinômio em $\mathbb{C}[x_1, \ldots, x_m]$, para cada $1 \leq j \leq n$.

Suponhamos que $Y \subset \mathbb{C}^n$ é um conjunto algébrico e que a aplicação ϕ definida acima é polinomial. Como Y está contido no conjunto de chegada de ϕ, podemos considerar a imagem inversa de Y por ϕ,

$$\phi^{-1}(Y) = \{p \in \mathbb{C}^m : \phi(p) \in Y\}.$$

É fácil ver que este conjunto é algébrico. Sejam $g_1, \ldots, g_t \in \mathbb{C}[y_1, \ldots, y_m]$ polinômios tais que

$$Y = \mathcal{Z}(g_1, \ldots, g_t).$$

Note que estamos usando y para as coordenadas do conjunto de chegada $\mathbb{C}^n$, assim como usaremos x para as coordenadas do domínio $\mathbb{C}^m$.

Seja $p \in \phi^{-1}(Y)$. Como $\phi(p) \in Y$, temos que

$$g_j(\phi(p)) = 0 \text{ para todo } 1 \leq j \leq t.$$

Considere,

$$h_j(x_1,\ldots,x_m) = g_j(\phi(x_1,\ldots,x_m));$$

isto é,

$$h_j(x_1,\ldots,x_m) = g_j(\phi_1(x_1,\ldots,x_m),\ldots,\phi_n(x_1,\ldots,x_m)),$$

que é o polinômio obtido substituindo ϕ_i no lugar da variável y_i em g_j. Mas o resultado destas substituições é um polinômio em $\mathbb{C}[x_1,\ldots,x_m]$. Portanto,

$$h_j \in \mathbb{C}[x_1,\ldots,x_m] \text{ satisfaz } h_j(p) = 0, \text{ para todo } 1 \leq j \leq t.$$

Em outras palavras, todo ponto da imagem inversa $\phi^{-1}(Y)$ é zero de cada um dos hs; donde

$$\phi^{-1}(Y) \subset \mathcal{Z}(h_1,\ldots,h_t).$$

A inclusão oposta segue imediatamente da definição dos hs, de modo que

$$\phi^{-1}(Y) = \mathcal{Z}(h_1,\ldots,h_t).$$

Em particular, mostramos que:

> a imagem inversa de um conjunto algébrico por uma aplicação polinomial também é um conjunto algébrico.

Diante disto pareceria razoável supor que a imagem de um conjunto algébrico $X \subset \mathbb{C}^m$ por uma aplicação polinomial ϕ deveria ser um conjunto algébrico. Isto, entretando, é falso. Suponhamos, por exemplo, que a aplicação

$$\phi : \mathbb{C}^2 \to \mathbb{C},$$

seja dada por $\phi(x_1,x_2) = (x_1, x_1x_2)$. Calcularemos a imagem de ϕ. Se $(y_1,y_2) \in \mathrm{Im}(\phi)$, então existe $(x_1,x_2) \in \mathbb{C}^2$ tal que

$$\phi(x_1,x_2) = (x_1, x_1x_2) = (y_1,y_2).$$

Assim,

$$x_1 = y_1 \text{ e } x_1x_2 = y_2.$$

Mas, supondo que $y_1 \neq 0$, obtemos destas equações que $x_2 = y_2/y_1$. Portanto, os pontos da forma (y_1,y_2) com $y_1 \neq 0$ pertencem à imagem. Falta verificar o que ocorre quando $y_1 = 0$. Neste caso $x_1 = 0$, de modo que $y_2 = 0$. Então, o único ponto de $\mathbb{C}^2$, com abscissa zero, que pertence à imagem de ϕ é $(0,0)$. Concluímos, assim, que

$$\mathrm{Im}(\phi) = \{(0,0)\} \cup \{(y_1,y_2) : y_1 \neq 0\}.$$

Contudo, este não é um conjunto algébrico. Para entender o porquê disto intersetamos $\mathrm{Im}(\phi)$ com a reta L de equação $y_2 = 1$, o que nos dá

$$\mathrm{Im}(\phi) \cap L = \{(y_1,1) : y_1 \neq 0\}. \tag{74}$$

Mas L é um conjunto algébrico. Portanto, se $\mathrm{Im}(\phi)$ também fosse algébrico, o mesmo aconteceria com $\mathrm{Im}(\phi) \cap L$, pelo teorema 9.3. Entretanto, pela equação (74), $\mathrm{Im}(\phi) \cap L$ é igual a uma reta menos um ponto; que, como vimos acima, não pode ser algébrico.

Na verdade, embora $\mathrm{Im}(\phi) \cap L$ não seja um conjunto algébrico, podemos escrevê-lo a partir de conjuntos algébricos desde que adotemos a diferença de

conjuntos como uma operação permitida. De fato, se L_0 é a reta de equação $y_1 = 0$, então

$$\mathrm{Im}(\phi) \cap L = \{(0,0)\} \cup (\mathbb{C}^2 \setminus L_0),$$

é a união do conjunto algébrico $\{(0,0)\}$ com uma diferença entre dois outros conjuntos algébricos. Tais conjuntos são chamados de construtíveis. Dada a sua importância, vale a pena defini-los de maneira formal.

Um conjunto $X \subseteq \mathbb{C}^n$ é *construtível* se existirem conjuntos algébricos $Y_1, \ldots, Y_s$ e $Y_1', \ldots, Y_s'$ tais que $Y_i' \subset Y_i$ para todo $1 \leq i \leq s$ e

$$X = (Y_1 \setminus Y_1') \cup \cdots \cup (Y_s \setminus Y_s').$$

Observe que todo conjunto algébrico Z é construtível, já que

$$Z = Z \setminus \emptyset,$$

e $\emptyset = \mathcal{Z}(1)$ é um conjunto algébrico.

O exemplo do efeito de uma função polinomial sobre um conjunto algébrico dado acima é típico, no sentido de que nada pior que um conjunto construtível pode aparecer como imagem de um conjunto algébrico. Isto é uma consequência imediata do seguinte teorema.

TEOREMA 9.6. *A imagem de um conjunto construtível por uma aplicação polinomial sempre é um conjunto construtível.*

Não provaremos este teorema aqui porque não vamos utilizá-lo em nossas aplicações futuras. A demonstração pode ser encontrada em [**35**, Teorema 3.16, p.39]. Concluímos a seção aplicando o que aprendemos acima ao estudo das curvas parametrizadas.

Um conjunto $X \subset \mathbb{C}^n$ é dado em *forma paramétrica*, se os pontos de X são os elementos da imagem de uma aplicação $\phi : \mathbb{C}^m \to \mathbb{C}^n$. Em outras palavras, para cada $p_0 \in X$ existe $u_0 \in \mathbb{C}^m$ tal que $p_0 = \phi(u_0)$. Neste caso dizemos que ϕ é uma *parametrização* de X.

Vejamos um exemplo bastante simples. Seja $\phi : \mathbb{C} \to \mathbb{C}^2$ definida por $\phi(t) = (t^2, t^3)$. Queremos identificar, através de uma equação em x e y, os pontos da imagem de ϕ. Na verdade já fizemos isto, usando um argumento geométrico, na página 80, mas desta vez faremos uma demonstração puramente algébrica. Se $(x, y) \in \mathrm{Im}(\phi)$, então existe $t \in \mathbb{C}$ tal que

$$x = t^2 \text{ e } y = t^3;$$

donde,

$$x^3 = t^6 = y^2.$$

Logo, cada ponto de $\mathrm{Im}(\phi)$ satisfaz a equação $y^2 = x^3$, de modo que $\mathrm{Im}(\phi) \subseteq \mathcal{Z}(y^2 - x^3)$. Por outro lado, se x_0 e y_0 são números complexos para os quais $y_0^2 = x_0^3$, então

$$\phi(\sqrt{x_0}) = (x_0, (\sqrt{x_0})^3) = (x_0, \sqrt{x_0^3}) = (x_0, \sqrt{y_0^2}) = (x_0, y_0).$$

Portanto, $\mathrm{Im}(\phi) = \mathcal{Z}(y^2 - x^3)$.

Já sabemos, de nossa discussão anterior, que um conjunto X definido parametricamente será sempre construtível, mas não tem que ser algébrico. Apesar disto, nada nos impede de procurar o *menor* conjunto algébrico que contém X. Isto é conhecido como *implicitizar* a parametrização de X; isto é, achar suas equações implícitas: aquelas que dependem apenas das coordenadas do conjunto de chegada. Vejamos como fazer isto.

Suponhamos que X é a imagem da aplicação $\phi : \mathbb{C}^m \to \mathbb{C}^n$, em que $\phi_j \in K[x_1, \ldots, x_m]$, para $1 \leq j \leq n$, e K é um subcorpo efetivo dos complexos. Se $p_0 \in X$, então a k-ésima coordenada de p_0 vai ser dada por $\phi_k(u_0)$, para algum $u_0 \in \mathbb{C}^m$. Portanto, se as coordenadas do conjunto de chegada forem $y_1, \ldots, y_n$, temos que (p_0, u_0) é um zero do ideal

$$I = \langle y_1 - \phi_1, \ldots, y_n - \phi_n \rangle$$

no anel $K[x_1, \ldots, x_m, y_1, \ldots, y_n]$.

Para entender o ponto chave do argumento, observe que

$$\mathcal{Z}(I) \subset X \times \mathbb{C}^m \subset \mathbb{C}^{n+m}.$$

Portanto, as m primeiras coordenadas de qualquer ponto de $\mathcal{Z}(I)$ descrevem um ponto da imagem X de ϕ. Logo, $h \in K[y_1, \ldots, y_n] \cap \sqrt{I}$ se, e somente se,

$$0 = h(p_0, u_0) = h(p_0),$$

para todo $p_0 = \phi(u_0) \in X$, já que h não contém as variaveis $x_1, \ldots, x_m$. Desta forma,

$$K[y_1, \ldots, y_n] \cap \sqrt{I} = \mathrm{I}(X).$$

Mas,

$$\sqrt{K[y_1, \ldots, y_n] \cap I} = K[y_1, \ldots, y_n] \cap \sqrt{I}.$$

Portanto, para obter um sistema de polinômios que defina X basta calcular os geradores de $K[y_1, \ldots, y_n] \cap I$, coisa que aprendemos a fazer na proposição 6.4 da página 159, que relembramos abaixo.

PROPOSIÇÃO 9.7. *Seja I um ideal do anel $K[x_1, \ldots, x_m, y_1, \ldots y_n]$. Se G é uma base de Gröbner de I com respeito à ordem lexicográfica com $y_1 < \cdots y_n < x_1 < \cdots < x_m$, então $G \cap K[y_1, \ldots, y_n]$ é uma base de Gröbner do ideal $I \cap K[y_1, \ldots, y_n]$.*

Considere, por exemplo, a curva C definida parametricamente como sendo a imagem da aplicação $\phi : \mathbb{C} \to \mathbb{C}^3$ dada por

$$\phi(t) = (t^3, t^4, t^5).$$

Esta curva tem uma propriedade bastante interessante, por isso escolhemos usá-la como exemplo. Para calcular o sistema que define C construímos o ideal

$$\langle x_1 - t^3, x_2 - t^4, x_3 - t^5 \rangle,$$

cuja base de Gröbner reduzida, com respeito à ordem lexicográfica para a qual $t > x_1 > x_2 > x_3$, é

$$\{x_2^5 - x_3^4, x_1x_3 - x_2^2, x_1x_2^3 - x_3^3, x_1^2x_2 - x_3^2, x_1^3 - x_2x_3, \\ tx_3 - x_1^2, tx_2 - x_3, tx_1 - x_2, t^3 - x_1\}.$$

Pela proposição 6.4 podemos concluir que C fica definida pelo sistema

$$\begin{aligned} x_2^5 - x_3^4 &= 0 \\ x_1x_3 - x_2^2 &= 0 \\ x_1x_2^3 - x_3^3 &= 0 \\ x_1^2x_2 - x_3^2 &= 0 \\ x_1^3 - x_2x_3 &= 0. \end{aligned}$$

Seja $I(C)$ o ideal gerado por estes polinômios. Isto significa que podemos definir C como solução de um sistema de cinco equações. Mas, precisamos realmente de tantas equações?

A resposta seria mais fácil de dar se a curva estivesse contida em um subespaço de dimensão dois de $\mathbb{C}^3$. Neste caso, o famoso *teorema de Bézout* nos diz que o conjunto algébrico de $\mathbb{C}^2$ definido por dois polinômios co-primos é finito; veja [**39**, p. 62] para uma demonstração. Portanto, o ideal de qualquer curva algébrica em $\mathbb{C}^2$ sempre pode ser gerado por apenas um elemento.

Contudo, é fácil ver que C não está contida em nenhum plano de $\mathbb{C}^3$. Para entender porque, suponha que $ax + by + c = 0$ fosse a equação de um plano que contém C. Neste caso, os pontos de C, definidos parametricamente, teriam que satisfazer a equação do plano. Portanto, deveríamos ter que

$$at^3 + bt^4 + ct^5 = 0 \text{ para todo } t \in \mathbb{C},$$

que é equivalente a dizer que

$$a + bt + ct^2 = 0 \text{ para todo } t \in \mathbb{C} \setminus \{0\}.$$

Contudo, isto é impossível, já que uma equação do segundo grau não pode ter mais de duas raízes complexas. Uma curva de $\mathbb{C}^3$ que não está contida em nenhum plano, como é o caso de C, é chamada de *reversa*.

Como C é reversa não podemos considerá-la como estando em nenhum espaço de dimensão menor que três. Começando com as superfícies de $\mathbb{C}^3$, vemos que o ideal de qualquer uma delas é principal. Porém, a demonstração deste fato é bem mais difícil que a do teorema de Bézout; veja [**36**, Proposition 1.13] para mais detalhes. E o ideal de uma curva de $\mathbb{C}^3$? Lembrando do que sabemos da álgebra linear poderíamos pensar assim:

> Sabemos que planos de $\mathbb{C}^3$ são definidos por uma equação, e retas por duas. Mas acabamos de ver que superfícies de $\mathbb{C}^3$ também são definidas por uma equação. Logo, por analogia, curvas deveriam ser definidas por duas equações.

Chegados neste ponto precisamos tomar muito cuidado com o que isto quer dizer. Por exemplo, não é verdade que o ideal de uma curva em $\mathbb{C}^3$ *sempre* pode ser gerado por dois elementos. E não precisamos ir muito longe para encontrar um exemplo. O ideal da curva C, que foi definida acima, não pode ser gerado por dois elementos. Para provar isto, procedemos por contradição, usando a demonstração da proposição 3.3, da página 76, como inspiração.

Digamos que $\mathrm{I}(C)$ pudesse ser gerado pelos polinômios f e g do anel $\mathbb{Q}[x_1, x_2, x_3]$. Nenhum monômio no suporte dos geradores de $\mathrm{I}(C)$ tem grau menor que 2. Portanto, o mesmo tem que ser verdade para todo os elementos não nulos de $\mathrm{I}(C)$. Em particular, as componentes homogêneas de menor grau de f e g têm grau maior ou igual a 2 (para a definição de componente homogênea veja página 94). Além disso, teriam que existir polinômios $\alpha_1, \alpha_2, \alpha_3$ e $\beta_1, \beta_2, \beta_3$ em $\mathbb{Q}[x_1, x_2, x_3]$ tais que

$$\begin{aligned} x_1x_3 - x_2^2 &= \alpha_1 f + \beta_1 g \\ x_1^2x_2 - x_3^2 &= \alpha_2 f + \beta_2 g \\ x_1^3 - x_2x_3 &= \alpha_3 f + \beta_3 g. \end{aligned}$$

Fazendo $x_1 = 0$ nestas equações, obtemos

$$\begin{aligned} -x_2^2 &= \widehat{\alpha_1}\widehat{f} + \widehat{\beta_1}\widehat{g} \\ -x_3^2 &= \widehat{\alpha_2}\widehat{f} + \widehat{\beta_2}\widehat{g} \\ -x_2x_3 &= \widehat{\alpha_3}\widehat{f} + \widehat{\beta_3}\widehat{g}; \end{aligned}$$

em que o circunflexo indica que substituímos x_1 por zero no respectivo polinômio. Disto podemos concluir que o espaço vetorial formado pelos polinômios homogêneos de grau 2 de $\mathbb{Q}[x_2, x_3]$ pode ser gerado pelas componentes homogêneas de grau 2 de $\hat{f}$ e $\hat{g}$. Mas isto contradiz o fato de que este espaço tem dimensão três, e conclui a demonstração de que $\mathrm{I}(C)$ não pode ser gerado por dois elementos.

No entanto, dizer que uma curva de $\mathbb{C}^3$ pode ser definida por apenas duas equações é mais fraco do que exigir que seu ideal seja gerado por dois elementos. De fato, se

$$C = \{p \in \mathbb{C}^3 : f(p) = g(p) = 0\},$$

então sabemos apenas que $\mathrm{I}(C) = \sqrt{\langle f, g\rangle}$. Portanto, o problema deveria ser reformulado da seguinte maneira.

PROBLEMA 9.8. *Dada uma curva algébrica (irredutível) de $\mathbb{C}^3$, existem polinômios f e g em $\mathbb{C}[x_1, x_2, x_3]$ tais que o ideal da curva é igual a $\sqrt{\langle f, g\rangle}$?*

O adjetivo irredutível no enunciado do problema significa que o ideal da curva é primo. Esta hipótese é verificada para a curva C acima, como passamos a mostrar. Para começar, a parametrização de C nos permite definir um homomorfismo

$$\psi : \mathbb{C}[x_1, x_2, x_3] \to \mathbb{C}[t]$$

por

$$\psi(f) = f(t^3, t^4, t^5) \text{ para todo } \ f \in \mathbb{C}[x_1, x_2, x_3].$$

Pelo teorema do homomorfismo da página 212,

$$\frac{\mathbb{C}[x_1, x_2, x_3]}{N(\psi)} \cong \mathrm{Im}(\psi).$$

Entretanto, o núcleo $N(\psi)$ é igual, por definição de ψ, ao conjunto dos polinômios que se anulam em C; isto é, ao ideal de C. Portanto,

$$\frac{\mathbb{C}[x_1, x_2, x_3]}{\mathrm{I}(C)} \cong \mathrm{Im}(\psi).$$

Como $\mathrm{Im}(\psi)$ é subanel de $\mathbb{C}[t]$, que é um domínio, podemos concluir que $\mathrm{Im}(\psi)$ e, portanto,

$$\frac{\mathbb{C}[x_1, x_2, x_3]}{\mathrm{I}(C)}$$

também é um domínio. Logo, pela proposição 8.2, o ideal $\mathrm{I}(C)$ é primo.

Ao longo da história deste problema, a distinção entre (1) o número de geradores de um ideal da curva, e (2) o número de equações necessárias para definir a curva no sentido usado no problema 9.8, nem sempre foi feita claramente. Por um longo tempo isto foi uma dramática fonte de confusão. O problema foi inicialmente posto por L. Kröencker em 1880, quando ele mostrou que quatro equações são sempre suficientes para determinar qualquer curva em três dimensões. Como uma equação não basta, a questão se resumia a verificar se o número correto de equações seria 2, 3, ou 4. Em 1891, K. Th. Vahlen deu uma demonstração de que três equações não bastariam para qualquer curva, sem contudo esclarecer em qual sentido isto deveria ser entendido. Em 1941, O. Perron descobriu que existem três curvas que determinam o exemplo de Vahlen no sentido (2). Contudo, em um artigo posterior, ele afirmou—sem citar nomes—que alguns 'leitores' o haviam acusado de não ter entendido nem a formulação original de Krönecker, nem o exemplo de Vahlen. Algum tempo depois F. Severi publicou um artigo em que revelava ter sido ele um dos 'leitores' que haviam criticado o artigo de Perron. Neste artigo, Severi afirma que o exemplo de Vahlen deveria ser interpretado no que é, essencialmente, o sentido (1). Segundo ele, teria sido esta a intenção do próprio Krönecker ao formular o problema. Perron respondeu com uma análise detalhada deste artigo, em que acaba sugerindo que Severi não entendia completamente sua própria interpretação do significado do problema! Apesar de ter degenerado em uma polêmica sobre o uso correto da palavra 'curva', esta disputa acabou levando outros matemáticos a se interessarem pelo problema, e a explicitar os vários sentidos em que pode ser entendido. Para mais detalhes veja [**56**].

Talvez lhe tenha ocorrido perguntar se implicitizar uma curva ou superfície tem algum valor prático. À primeira vista pode parecer que não. Por exemplo, é muito mais fácil usar o computador para desenhar uma curva descrita parametricamente, do que uma que está definida por equações implícitas. Entretanto, há circunstâncias em que é preferível ter as equações implícitas. Isto acontece,

por exemplo, quando desejamos achar os pontos de interseção de duas curvas. Se ambas forem dadas em forma implícita, basta reunir as equações das duas em um só sistema e resolvê-lo. Mas se forem dadas parametricamente, o problema é muito mais complicado, porque precisamos achar os pontos em que as duas parametrizações coincidem.

Para ter um exemplo concreto, vejamos como intersectar a curva C definida acima, com a parábola

$$x_2 - x_1 = x_3 + x_1^2 - 1 = 0.$$

Para isto basta reunir as equações destas duas curvas em um só sistema e determinar sua base de Gröbner, que será dada por

$$x_3^2 - x_3, \quad x_2x_3 - x_3, \quad x_2^2 - x_2x_3, \quad \text{e} \quad x_1 - x_2,$$

se utilizarmos a ordem lexicográfica com as variáveis ordenadas na forma $x_1 > x_2 > x_3$. Observe que este sistema é muito fácil de resolver. Da primeira equação, temos

$$0 = x_3^2 - x_3 = x_3(x_3 - 1);$$

donde

$$x_3 = 0 \quad \text{ou} \quad x_3 = 1.$$

Por outro lado, a terceira equação pode ser reescrita na forma

$$0 = x_2(x_2 - x_3);$$

logo $x_2 = 0$ ou $x_2 = x_3$. Finalmente, levando em conta, também, a quarta equação, concluímos que os pontos de interseção são

$$(1, 1, 1) \quad \text{e} \quad (0, 0, 0).$$

Como veremos na seção 4 qualquer sistema com uma quantidade finita de soluções pode ser resolvido usando-se um procedimento semelhante ao que foi empregado acima, o que aliás já havia sido sugerido por Descartes em sua *Geometria*! Lá, veremos também, que a utilização da ordem lexicográfica é essencial para o funcionamento correto deste método.

4. Sistemas de dimensão zero

O segredo da solução de um sistema linear nas variáveis $x_1, \ldots, x_n$ por eliminação gaussiana está na redução da matriz do sistema à forma escada. Se o sistema for determinado, isto nos permite resolvê-lo calculando o valor de x_n da última equação, substituindo-o na equação anterior para achar o valor de x_{n-1}, e continuando assim até calcular x_1. Se o sistema não for determinado, o procedimento é um pouco mais complicado, já que teremos de expressar uma variável em função de outras. Por isso vamos nos concentrar em resolver, usando bases de Gröbner, o análogo não linear de um sistema determinado. Mas a diferença entre um sistema que é determinado, e um que não é, está na quantidade de soluções: um sistema linear determinado tem apenas uma solução, ao passo que um sistema linear indeterminado tem infinitas soluções.

Isto sugere que a generalização não linear de um sistema lineare determinado é um sistema com um número finito de soluções.

Na terminologia usual, um conjunto algébrico X tem *dimensão zero* quando contém apenas um número finito de pontos. Neste caso diremos também que o ideal de X e o sistema de equações coorespondente têm dimensão zero. Naturalmente esta terminologia sugere que há aqui uma definição de dimensão implícita, e é realmente este o caso, mas não vamos discuti-la neste livro. Para mais detalhes, consulte [**17**, capítulo 9] e [**33**, capítulo 5] para um tratamento ao estilo computacional, ou [**46**, capítulo II] para uma abordagem mais teórica.

De posse desta definição, podemos enunciar o objetivo desta seção como sendo o de obter, para um sistema de dimensão zero, uma base de Gröbner "em forma escada", que nos permita resolver este sistema *não linear* de maneira tão simples quanto o método de Gauss nos permite resolver um sistema *linear*. Contudo, para que o procedimento funcione de maneira satisfatória, precisamos escolher uma ordem adequada. Começamos calculando um exemplo.

Seja J o ideal de $K[x, y, z]$ gerado pelos elementos do conjunto

$$G = \{x^2 - 4, y^2 - x^3 - 1, z - xy^2 + 4\}.$$

É fácil verificar, diretamente da definição, que G é uma base de Gröbner de J relativamente à ordem lexicográfica com $x < y < z$. Este sistema é muito fácil de resolver. Para achar os valores de x que o satisfazem, basta calcular as raízes de $x^2 - 4$, que é uma equação em apenas uma variável. Fazendo isto, obtemos $x = \pm 2$. Substituindo estes valores de x na equação $y^2 - x^3 - 1$, obtemos duas equações na variável y, a saber $y^2 - 9 = 0$ e $y^2 + 7 = 0$. Portanto, $x = 2$ e $y = \pm 3$, ou $x = -2$ e $y = \pm\sqrt{7}$. Finalmente, substituindo estes valores na equação $z = xy^2 + 4$, obtemos os pontos

$$(2, 3, 22), (2, -3, 22), (-2, \sqrt{7}, 10) \text{ e } (-2, -\sqrt{7}, 10),$$

como sendo as soluções do sistema dado por G. Observe que foi fácil resolver este sistema porque ele estava em "forma escada", isto é, havia uma equação apenas na variável x, uma equação em x e y cujo termo inicial era uma potência pura de y, e uma equação em x, y e z cujo termo inicial era uma potência pura de z. O surpreendente é que todo sistema de dimensão zero admite uma base de Gröbner em forma escada: isto segue da proposição 6.4 da página 159. Para proceder à análise de um sistema de dimensão zero à luz daquela proposição, é mais conveniente denotar todas as variáveis por um mesmo símbolo, em vez de agrupá-las com nomes diferentes, como no enunciado original da proposição. Fazendo isto, o resultado de que precisamos corresponde à seguinte afirmação:

Se J é um ideal de dimensão zero em $K[x_1, \ldots, x_n]$, então

$$J \cap K[x_1, \ldots, x_k] \neq \{0\} \text{ para todo } 1 \leq k \leq n.$$

Combinando esta afirmação com a proposição 6.4, temos que se G é uma base de Gröbner de J relativa à ordem lexicográfica com $x_1 < \cdots < x_n$, então

$$G \cap K[x_1, \ldots, x_k] \neq \emptyset$$

é uma base de Gröbner de $J \cap K[x_1, \ldots, x_k]$. É este o resultado que iremos provar a seguir, ainda que de uma forma mais refinada.

PROPOSIÇÃO 9.9. *Seja J um ideal de dimensão zero de $K[x_1, \ldots, x_n]$ e G uma base de Gröbner reduzida de J relativa à ordem lexicográfica com $x_1 < \cdots < x_n$. Então, para cada $1 \leq k \leq n$ temos que G contém um elemento h_k da forma*

$$x_k^{d_k} + a_{d_k-1}x_k^{d_k-1} + \cdots + a_1x_k + a_0 \in G \cap \mathbb{C}[x_1, \ldots, x_k], \tag{75}$$

em que $a_{d_k-1}, \ldots, a_1, a_0 \in K[x_1, \ldots, x_{k-1}]$.

DEMONSTRAÇÃO. Suponhamos, para começar, que $K = \mathbb{C}$ e digamos que

$$\mathcal{Z}(J) = \{p_1, \ldots, p_s\}.$$

Escolha $1 \leq k \leq n$, e sejam $\alpha_1, \ldots, \alpha_s$ as k-ésimas coordenadas dos pontos $p_1, \ldots, p_s$. Considere, agora, o polinômio

$$g_k = (x_k - \alpha_1) \cdots (x_k - \alpha_s) \in \mathbb{C}[x_1, \ldots, x_n].$$

Apesar de estarmos pensando em g_k como um polinômio em $\mathbb{C}[x_1, \ldots, x_n]$, seu suporte contém apenas a variável x_k. Contudo,

$$g_k(p_j) = (\alpha_j - \alpha_1) \cdots (\alpha_j - \alpha_s) = 0,$$

já que o j-ésimo termo deste produto é $\alpha_j - \alpha_j$. Portanto, pelo teorema 9.1,

$$g_k \in \mathrm{I}(X) = \sqrt{J}.$$

Logo, $\sqrt{J} \cap \mathbb{C}[x_1, \ldots, x_k]$ contém g_k.

Mas, se $g_k \in \sqrt{J}$, então existe algum $t \geq 1$, para o qual $g_k^t \in J$. Assim, $\mathrm{in}(g_k) = x_k^{ts}$. Entretanto, como G é uma base de Gröbner de J e $g_k^t \in J$, tem que haver um elemento em G cujo termo inicial divide $\mathrm{in}(g_k^t)$. Portanto, G tem um elemento, digamos h_k, cujo termo inicial é uma potência pura de x_k, de grau d_k. Contudo, estamos trabalhando sob a ordem lexicográfica, de modo que os demais monômios de h_k conterão apenas as variáveis $x_1, \ldots, x_k$. Além disso, o grau de x_k em cada um destes outros monômios terá que ser inferior a d_k. Sistematizando tudo o que descobrimos, temos que a base de Gröbner reduzida G contém elementos

$$h_k = x_k^{d_k} + a_{d_k-1}x_k^{d_k-1} + \cdots + a_1x_k + a_0, \tag{76}$$

em que $a_{d_k-1}, \ldots, a_1, a_0 \in \mathbb{C}[x_1, \ldots, x_{k-1}]$.

Falta-nos considerar o que acontece se $K \subsetneq \mathbb{C}$. Contudo, neste caso a única diferença é que os coeficientes dos polinômios que geram J pertencem a K. Como o cálculo dos S-polinômios e das divisões só envolve estes polinômios (direta ou indiretamente) o resultado será uma base de Gröbner que só contém polinômios com coeficientes em K. □

Pela forma dos h_k, vemos que o sistema

$$h_1 = \cdots = h_n = 0,$$

está em forma escada, no sentido discutido no início da seção. Antes de prosseguir, é importante você notar que não estamos afirmando que G é formada apenas pelos polinômios $h_1, \ldots, h_n$: isto não é verdade em geral, como veremos, mais adiante, em um exemplo.

Segue imediatamente desta proposição que

$$J \cap \mathbb{C}[x_1] \neq \{0\}.$$

Contudo, não há nada de especial em x_1 neste contexto, além do fato de ter sido escolhido como a menor variável relativamente à ordem lex. Isto nos conduz ao seguinte resultado, que será muito útil na seção 7.

COROLÁRIO 9.10. *J é um ideal de dimensão zero em $\mathbb{C}[x_1, \ldots, x_n]$ se, e somente se,*

$$J \cap \mathbb{C}[x_k] \neq \{0\} \text{ para todo } 1 \leq k \leq n.$$

DEMONSTRAÇÃO. Se J tem dimensão zero então, escolhendo a variável x_k como sendo a menor variável relativamente à ordem lexicográfica, podemos concluir da proposição 9.9 que

$$J \cap \mathbb{C}[x_k] \neq \{0\}$$

como desejado.

Passando à recíproca, suponhamos que

$$J \cap \mathbb{C}[x_k] \neq \{0\} \text{ para todo } 1 \leq k \leq n.$$

Mas, pelo teorema 2.3 da página 45, o ideal $J \cap \mathbb{C}[x_k]$ tem que ser principal. Digamos que seu gerador seja g_k. Como

$$\langle g_k \rangle J \cap \mathbb{C}[x_k] \subseteq J,$$

temos que

$$\mathcal{Z}(J) \subseteq \mathcal{Z}(g_k);$$

segundo a qual a k-ésima coordenada de qualquer ponto de $\mathcal{Z}(J)$ satisfaz é raiz do polinômio g_k. Como g_k tem apenas uma variável, o conjunto R_k das suas raízes não pode ter mais do que $\mathrm{grau}(g_k)$ elementos. Em particular, trata-se de um conjunto finito. Contudo,

$$\mathcal{Z}(J) \subseteq R_1 \times \cdots \times R_k,$$

de modo que também $\mathcal{Z}(J)$ tem que ser um conjunto finito. Um detalhe importante para o qual vale a pena chamar a sua atenção é que $\mathcal{Z}(g_1)$ *não é um conjunto finito*. Por exemplo,

$$\mathcal{Z}(g_1) = R_1 \times \mathbb{C}^{n-1},$$

uma vez que apenas as primeiras coordenadas dos seus pontos estão sujeitas a alguma restrição. □

Este corolário nos dá um critério que podemos usar para decidir se um dado ideal tem ou não dimensão finita. Isto é muito importante, porque os algoritmos das próximas seções requerem que o ideal dado na entrada tenha dimensão finita para poderem funcionar corretamente.

Finalmente, estamos prontos para delinear a estratégia que usaremos para resolver um sistema de dimensão zero. Suponha que

$$f_1 = \cdots = f_m = 0,$$

é um tal sistema, em que $f_1, \ldots, f_m \in \mathbb{C}[x_1, \ldots, x_n]$. Considere o ideal J de $\mathbb{C}[x_1, \ldots, x_n]$ gerado pelos fs, e calcule uma base de Gröbner reduzida G de J com respeito à ordem lexicográfica com $x_1 < \cdots < x_n$. Podemos resolver este sistema recursivamente, usando os polinômios h_k definidos acima, da seguinte maneira. Em primeiro lugar, h_1 contém apenas a variável x_1. Assim, podemos calcular as suas raízes, que nos darão as coordenadas x_1 dos pontos de $\mathcal{Z}(J)$.

Passando ao passo recursivo, digamos que S_{k-1} é o conjunto formado pelos pontos de $\mathbb{C}^{k-1}$ que correspondem às soluções do sistema

$$h_1 = \cdots = h_{k-1} = 0.$$

A razão pela qual S_{k-1} está contido em um espaço de dimensão $k-1$, e não de dimensão n, é que os $k-1$ primeiros hs só contêm as $k-1$ primeiras variáveis. Substituindo um dos pontos $q \in S_{k-1}$ na expressão para h_k obtida em (75), teremos uma equação polinomial

$$h_k(q, x_k) = x_k^{d_k} + a_{d_k-1}(q)x_k^{d_k-1} + \cdots + a_1(q)x_k + a_0(q),$$

em apenas uma variável, a saber x_k. As possíveis coordendas x_k dos pontos de $\mathcal{Z}(J)$ estão entre as raízes complexas de $h_k(q, x_k)$, cujo conjunto denotaremos por $\mathcal{R}_q$. Em seguida, coletamos em S_k os pontos da forma (q, α), em que $\alpha \in \mathcal{R}_q$, para cada $q \in S_{k-1}$, e repetimos o passo recursivo. Faremos isto até que $k = n$. Tendo usado todos os h_k (mas não necessariamente todos os elementos de G) o procedimento para.

Como consequência deste procedimento temos uma cota superior para o número de pontos em $\mathcal{Z}(J)$, baseada na inclusão

$$\mathcal{Z}(J) \subseteq S_n.$$

O ponto chave, é que é fácil estimar a quantidade de pontos de S_n. Usando a definição recursiva descrita acima, temos que

$$S_k \leq \sharp S_{k-1} \cdot d_k,$$

em que d_k é o grau de h_k. Como S_1 é o conjunto das raízes de h_1, temos também que $\sharp S_1 \leq d_1$. Portanto,

$$\sharp\mathcal{Z}(J) \leq \sharp S_n \leq d_1 \cdots d_n. \tag{77}$$

Não podemos substituir nenhuma das duas desigualdades por igualdades nesta fórmula. Em primeiro lugar, a desigualdade da direita será própria sempre que um dos h_k tiver raízes cuja multiplicidade é maior que um. Em segundo lugar, os pontos de S_n que não satisfizerem os elementos de $G \setminus \{h_1, \ldots, h_k\}$ não pertencerão a $\mathcal{Z}(J)$. Esta última situação ocorre no próximo exemplo.

No anel $\mathbb{C}[x, y]$, considere o ideal

$$J = \langle (x^2 + y + 1)^2(x + y^3 + 1)^3, (x^2 + 2y)^3(x + 3y^3)^2 \rangle,$$

e seja G sua base de Gröbner reduzida com respeito à ordem lexicográfica para a qual $x < y$. Ordenando os elementos de G segundo seus termos iniciais, temos sete elementos, dos quais o primeiro é um polinômio de grau 64 apenas na variável x, ao passo que o quinto elemento tem termo líder y^4. Portanto, pelo argumento anterior, o número de soluções do sistema definido por J não pode exceder $64 \cdot 4 = 256$ quando, na verdade, o sistema tem apenas 108 soluções. A maneira pela qual a quantidade correta de soluções foi obtida será discutida na seção 5. Como o que está por trás da solução deste problema é o radical do ideal dos pontos, precisaremos antes descobrir como calcular este radical; coisa que faremos, em etapas, a partir da próxima seção.

O algoritmo resultante da análise anterior pode ser enunciado da seguinte maneira.

ALGORITMO 9.11 (Resolução de sistemas de dimensão zero). *Dado um ideal J de $\mathbb{C}[x_1, \ldots, x_n]$ de dimensão zero, o algoritmo tem como saída os pontos de $\mathcal{Z}(J)$.*

Primeira etapa: *Calcule uma base de Gröbner G para J relativamente à ordem lexicográfica com $x_1 < \cdots < x_n$.*

Segunda etapa: *Para $1 \leq k \leq n$, repita:*

- *Inicialize $S_k = \emptyset$.*
- *Escolha*

$$h_k = x_k^{d_k} + a_{d_k-1}x_k^{d_k-1} + \cdots + a_1 x_k + a_0$$

em $G \cap \mathbb{C}[x_1, \ldots, x_k]$, para o qual

$$a_{d_k-1}, \ldots, a_1, a_0 \in \mathbb{C}[x_1, \ldots, x_{k-1}]$$

- *Para cada $p \in \mathcal{S}_{k-1}$ e para cada raiz α de $h_k(p, x_k)$ acrescente (p, α) a S_k.*

Terceira etapa: *Inicialize $R = \emptyset$*

Quarta etapa: *Para $p \in S_n$, repita*

- *Verifique se p é zero dos polinômios em $G \setminus \{h_1, \ldots, h_n\}$.*
- *Se a resposta for sim, exclua p de S_n e acrescente-o em R; se a resposta for não, apenas exclua p de S_n.*

Quinta etapa: *Retorne R.*

Honestamente falando, este algoritmo deixa muito a desejar do ponto de vista da computação algébrica. A razão reside na segunda etapa, em que precisamos calcular raízes de polinômios. Embora isto possa ser feito usando, por exemplo, o método de Newton, o resultado é um valor aproximado, e não um valor exato, que é o que estamos sempre esperando obter com nossos algoritmos. Há várias maneiras de contornar este problema. A mais óbvia é aceitar que às vezes teremos apenas resultados aproximados, e seguir adiante. Outra saída consiste em inventar maneiras indiretas de representar as raízes de um polinômio em uma indeterminada. Por exemplo, se $f \in \mathbb{R}[x]$, podemos isolar uma raiz real de f encontrando números racionais $q_1 < q_2$, de modo que f tem apenas uma raiz no intervalo (q_1, q_2). Em outras palavras, o par formado

por f e pelo intervalo (q_1, q_2) com extremos racionais, determina um único número real, que é raiz da equação f. Para mais detalhes sobre este tipo de representação veja [**26**].

5. Contando pontos

Nesta seção mostraremos que é possível contar os pontos de um conjunto algébrico X de *dimensão zero* a partir dos ideais máximos que contêm o ideal $\mathrm{I}(X)$. Começaremos tratando do caso em que X contém apenas um ponto. Antes, porém, precisamos de uma propriedade básica dos ideais máximos. Como esta mesma propriedade vale, mais geralmente, para ideais primos, é neste caso que vamos demonstrá-la. As definições de ideais primos e máximos se encontram na página 204.

Digamos, por exemplo, que P seja um ideal primo de um anel A. Se $a \in \sqrt{P}$, então existe $k \geq 1$ tal que $a^k \in P$. Porém, como P é primo, isto implica que $a \in P$. Logo, $\sqrt{P} \subseteq P$. Como a inclusão oposta é verdadeira para qualquer ideal, temos que $\sqrt{P} = P$. Um ideal I de A, que satisfaz $\sqrt{I} = I$ é chamado de *radical*. Temos, assim, o seguinte resultado, cuja segunda afirmação decorre do fato de que todo ideal máximo é primo, provada na proposição 8.2.

PROPOSIÇÃO 9.12. *Todo ideal primo é radical. Em particular, todo ideal máximo é radical.*

Contudo, a recíproca desta proposição é falsa. Por exemplo, é claro que o ideal I gerado por xy em $\mathbb{Q}[x, y]$ não é primo, mas não é difícil verificar que se trata de um ideal radical. De fato, se $f \in \sqrt{I}$, então $f^k \in I$, para algum inteiro $k \geq 0$. Pela definição de I, isto implica que

$$f^k(0, y) = 0 \text{ donde } \ f(0, y) = 0.$$

Entretanto, $f(0, y) = 0$ significa que $f(x, y)$ é múltiplo de x; digamos $f(x, y) = xg(x, y)$. Assim,

$$0 = f(x, 0) = xg(x, 0), \text{ donde } \ g(x, 0) = 0.$$

Por sua vez, $g(x, 0) = 0$ significa que $g(x, y) = yh(x, y)$, para algum polinômio $h \in \mathbb{Q}[x, y]$. Portanto,

$$f = xg(x, y) = xyh(x, y) \in I.$$

Concluímos que I é radical, apesar de não ser primo. Encerraremos esta seção utilizando a proposição 9.12 para caracterizar os ideais máximos de um anel de polinômios sobre *os números complexos*.

A primeira parte do argumento generaliza um exemplo da página 203. A um ponto $p = (\alpha_1, \ldots, \alpha_n)$ de $\mathbb{C}^n$, podemos associar o ideal

$$\mathfrak{m}_p = \langle x_1 - \alpha_1, \ldots, x_n - \alpha_n \rangle.$$

Como a notação sugere, queremos provar que este é um ideal máximo do anel $\mathbb{C}[x_1, \ldots, x_n]$. Mas, $\mathfrak{m}_p$ é o núcleo do homomorfismo de especialização

$$\phi_p : \mathbb{C}[x_1, \ldots, x_n] \to \mathbb{C}$$

que leva um polinômio $f \in \mathbb{C}[x_1, \ldots, x_n]$ em $f(p)$. Como a imagem de ϕ_p é um corpo—neste caso o próprio $\mathbb{C}$—temos, pela proposição 8.2 que

$$N(\phi_p) = \mathfrak{m}_p$$

é máximo como ideal de $\mathbb{C}[x_1, \ldots, x_n]$. Tudo isto já era um tanto predizível diante do que fizemos anteriormente; o surpreendentemente é que vale a recíproca:

> todo ideal máximo de $\mathbb{C}[x_1, \ldots, x_n]$ é da forma $\mathfrak{m}_p$ para algum ponto $p \in \mathbb{C}^n$.

Para provar isto, suponha que M é um ideal máximo de $\mathbb{C}[x_1, \ldots, x_n]$. Como M é próprio temos, pelo teorema dos zeros, que $\mathcal{Z}(M) \neq \emptyset$. Seja $p \in \mathcal{Z}(M)$ e considere o ideal $\mathfrak{m}_p$ correspondente. Como

$$\mathcal{Z}(\mathfrak{m}_p) = \{p\} \subseteq \mathcal{Z}(M),$$

segue do corolário 9.2 que

$$M \subseteq \sqrt{M} \subseteq \sqrt{\mathfrak{m}_p}.$$

Como M é máximo $M = \sqrt{\mathfrak{m}_p}$. Contudo, todo ideal máximo é radical pela proposição 9.12. Portanto, $M = \mathfrak{m}_p$. Este resultado é suficientemente importante para merecer o status de teorema.

TEOREMA 9.13. *Todo ideal máximo de* $\mathbb{C}[x_1, \ldots, x_n]$ *é da forma* $\mathfrak{m}_p$ *para algum ponto* $p \in \mathbb{C}^n$ *e*

$$\mathbb{C}[x_1, \ldots, x_n]/\mathfrak{m}_p \cong \mathbb{C}.$$

É importante observar que este teorema é falso sobre $\mathbb{Q}$ e também sobre $\mathbb{R}$. Para falar a verdade, isto não é muito surpreendente, já que o mesmo ocorre com o teorema dos zeros, do qual sua demonstração depende. Um exemplo simples é o ideal M de $\mathbb{R}[x, y]$ gerado por $x^2 + 1$ e $y + 1$. Seja f um polinômio de $\mathbb{R}[x, y]$ que não está contido em M. Dividindo f por $G = \{x^2 + 1, y + 1\}$ obtemos como resto um polinômio r que não contém y, nem nenhum monômio em x de grau maior que 1. Logo, $r = ax + b$, em que $a, b \in \mathbb{R}$. Como $f \notin M$, então

$$r \in (M + \langle f \rangle) \cap \mathbb{R}[x] \supsetneq M \cap \mathbb{R}[x].$$

Contudo, $x^2 + 1$ é irredutível sobre $\mathbb{R}[x]$, de modo que, pela proposição 8.1 da página 204, o ideal de $\mathbb{R}[x]$ gerado por $x^2 + 1$ é máximo. Portanto,

$$\langle 1 \rangle = \langle x^2 + 1, r \rangle \subseteq M + \langle f \rangle,$$

o que mostra que M é máximo, embora não tenha a forma prescrita no teorema 9.13.

Com isto estamos prontos para considerar conjuntos de dimensão zero que contêm mais de um ponto. O resultado que pretendemos provar é o conteúdo do seguinte teorema.

TEOREMA 9.14. *Seja I um ideal de dimensão zero de $\mathbb{C}[x_1, \ldots, x_n]$. Então,*

$$\sharp\mathcal{Z}(I) = \dim_{\mathbb{C}}(\mathbb{C}[x_1, \ldots, x_n]/\sqrt{I}).$$

Para provar o teorema precisamos relacionar os pontos de $\mathcal{Z}(I)$ com objetos do anel quociente $\mathbb{C}[x_1, \ldots, x_n]/\sqrt{I}$. Faremos isto recorrendo ao teorema 9.13. Simplificando um pouco a notação utilizada na acima, se

$$\mathcal{Z}(I) = \{p_1, \ldots, p_s\},$$

denotaremos por $\mathfrak{m}_i$ o ideal máximo associado ao ponto p_i, para $1 \leq i \leq s$. O resultado de que precisamos é o seguinte.

PROPOSIÇÃO 9.15. *Se I é um ideal de $\mathbb{C}[x_1, \ldots, x_n]$ tal que*

$$\mathcal{Z}(I) = \{p_1, \ldots, p_s\},$$

então

$$\sqrt{I} = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_s.$$

DEMONSTRAÇÃO. Para facilitar a notação, digamos que

$$J = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_s,$$

de forma que precisamos provar que $\sqrt{I_c} = J$. Pelo teorema 9.3 temos que se

$$\{p_i\} = \mathcal{Z}(\mathfrak{m}_i) \subseteq \mathcal{Z}(I),$$

então

$$\sqrt{I_c} \subseteq \mathfrak{m}_i \text{ para todo } 1 \leq i \leq s.$$

Mas isto implica que $\sqrt{I_c} \subseteq J$, donde

$$\mathcal{Z}(J) \subseteq \mathcal{Z}(\sqrt{I_c}). \tag{78}$$

Contudo, este dois conjuntos algébricos são iguais a $\mathcal{Z}(I)$. Assim, a inclusão em (78) é, na verdade, uma igualdade; o que significa que $\sqrt{J} = \sqrt{I_c}$ pelo corolário 9.2. Contudo, pela proposição 3.13, $\sqrt{J} = J$, o que completa a demonstração. □

A proposição acima mostra que os pontos de $\mathcal{Z}(I)$ estão em correspondência biunívoca com os ideais máximos de $\mathbb{C}[x_1, \ldots, x_n]$ que contêm $\sqrt{I}$. Portanto, o próximo passo deve ser descobrir a relação entre a quantidade de ideais máximos que contêm $\sqrt{I}$ e a dimensão do anel quociente. Para isso precisamos de uma versão do teorema chinês do resto. Antes, porém, uma definição. Se A e B são anéis, então a *soma direta* $A \oplus B$ é definida como sendo o anel cujos elementos são os pares (a, b) em que $a \in A$ e $b \in B$, com a adição e multiplicação definidas coordenada a coordenada. Em outras palavras,

$$(a, b) + (a', b') = (a + a', b + b');$$
$$(a, b) \cdot (a', b') = (a \cdot a', b \cdot b');$$

quaisquer que sejam $a, a' \in A$ e $b, b' \in B$. Veja também o exercício ??? do capítulo 2.

TEOREMA CHINÊS DO RESTO. *Seja A um anel e I_1 e I_2 ideais de A. Se $I_1 + I_2 = A$, então*

$$\frac{A}{I_1 \cap I_2} \cong \frac{A}{I_1} \oplus \frac{A}{I_2}.$$

Quando dois ideais I_1 e I_2 de um anel A satisfazem a condição $I_1+I_2 = A$ do teorema chinês do resto, dizemos que são *co-máximos*. Por exemplo, dois ideais máximos distintos de A são sempre co-máximos.

DEMONSTRAÇÃO. Seja π_j a projeção canônica de A sobre o anel quociente A/I_j, e considere a aplicação

$$\phi : A \to A/I_1 \oplus A/I_2,$$

definida por

$$\phi(a) = (\pi_1(a), \pi_2(a)).$$

É fácil verificar que esta aplicação é um homomorfismo de anéis, e deixaremos os detalhes por sua conta. Como desejamos usar o teorema do homomorfismo, precisamos mostrar que ϕ é sobrejetiva e depois calcular seu núcleo.

Escolha um par qualquer

$$(\overline{b_1}, \overline{b_2}) \in A/I_1 \oplus A/I_2.$$

Queremos achar um único $a \in A$ tal que

$$\pi_1(a) = \overline{b_1} \text{ e } \pi_2(a) = \overline{b_2}. \tag{79}$$

Para isto suporemos que um tal a existe e tentaremos ver o que conseguimos descobrir a seu respeito. Porém, se $\pi_1(a) = \overline{b_1}$, então $a - b_1 = x_1 \in I_1$. Assim, $a = b_1 + x_1$. Mas, devemos ter também que

$$(b_1 + x_1) - b_2 = a - b_2 \in I_2,$$

já que $\pi_2(a) = \overline{b_2}$. Desta forma,

$$b_1 - b_2 + x_1 = x_2 \in I_2$$

donde

$$b_1 - b_2 = x_2 - x_1. \tag{80}$$

Com isto,

$$a = b_1 + x_1 = b_2 + x_2 \text{ em que } x_1 \in I_1 \text{ e } x_2 \in I_2,$$

satisfaz (79). Como esta definição de a segue imediatamente de (80), basta achar x_1 e x_2 que satisfaçam (80) e teremos o desejado. É neste ponto que precisamos da condição $I_1 + I_2 = A$.

Organizando tudo isto na ordem direta, temos a seguinte prova da sobrejetividade de ϕ. Como $I_1+I_2 = A$, existem $y_1 \in I$ e $y_2 \in J$ tais que $y_1+y_2 = 1$. Portanto, se

$$x_1 = (b_1 - b_2)y_1 \text{ e } x_2 = -(b_1 - b_2)y_2,$$

temos que

$$b_1 - b_2 = x_1 - x_2.$$

Tomando

$$a = b_1 + x_1 = b_2 + x_2.$$

concluímos que, como $x_j \in I_j$, então

$$\pi_j(a) = \overline{b_j + x_j} = \overline{b_j}$$

para $1 \leq j \leq 2$; o que completa a prova da sobrejetividade.

Ainda falta calcular o núcleo de ϕ. Mas,

$$\phi(a) = (\overline{a}, \overline{a}) = (\overline{0}, \overline{0})$$

ocorre se, e somente se, $a \in I_1$ e $a \in I_2$. Portanto,

$$\mathrm{N}(\phi) = I_1 \cap I_2,$$

e o isomorfismo segue imediatamente do teorema do homomorfismo. □

Como quaisquer dois ideais máximos distintos são co-máximos, temos por indução o seguinte corolário.

COROLÁRIO 9.16. *Seja A um anel e sejam $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ ideais máximos distintos de A. Se $J = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_s$, então,*

$$A/J \cong A/\mathfrak{m}_1 \oplus \cdots \oplus A/\mathfrak{m}_s.$$

DEMONSTRAÇÃO. Supondo fixado o anel A, o resultado a ser provado por indução é o seguinte,

se $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ são ideais máximos *distintos* de A, então:

(1) $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_{s-1}$ é $\mathfrak{m}_s$ são co-máximos;

(2) existe um isomorfismo

$$A/(\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_{s-1}) \cong A/\mathfrak{m}_1 \oplus \cdots \oplus A/\mathfrak{m}_s.$$

Observe que (1) é necessário apenas para que a indução possa ser aplicada juntamente com o teorema chinês do resto.

Se $s = 2$, o resultado é consequência da co-maximalidade de ideais máximos distintos e do teorema chinês do resto. Suponhamos que o resultado é verdadeiro para qualquer escolha de $s - 1$ ideais máximos e digamos que dispomos de s destes ideais, todos distintos. Como $\mathfrak{m}_i \neq \mathfrak{m}_s$ para todo $i \neq s$, existe um elemento

$$m_i \in \mathfrak{m}_i \setminus \mathfrak{m}_s,$$

donde

$$m_1 \cdots m_{s-1} \in \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_{s-1}.$$

Contudo,

$$m = m_1 \cdots m_{s-1} \notin \mathfrak{m}_s$$

pois, do contrário, algum m_i teria que pertencer a $\mathfrak{m}_s$, já que ideais máximos são primos; veja proposição 8.2 da página 205. Entretanto, como $\mathfrak{m}_s$ é máximo e não contém m, concluímos que

$$\langle m \rangle + \mathfrak{m}_s = A.$$

Contudo,

$$\langle m \rangle + \mathfrak{m}_s \subseteq (\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_{s-1}) + \mathfrak{m}_s,$$

de modo que

$$\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_{s-1} \text{ e } \mathfrak{m}_s,$$

são ideais co-máximos. Mas isto nos permite aplicar o teorema chinês do resto a estes dois ideais, o que nos dá

$$A/(\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_s) \cong A/(\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_{s-1}) \oplus A/\mathfrak{m}_s,$$

o resultado desejado segue agora da hipótese de indução, segundo a qual

$$A/(\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_{s-1}) \cong A/\mathfrak{m}_1 \oplus \cdots \oplus A/\mathfrak{m}_{s-1}.$$

□

É hora de ver o que já sabemos até este ponto. Em primeiro lugar, pela proposição 9.15, temos que

$$\frac{\mathbb{C}[x_1, \ldots, x_n]}{\sqrt{I}} \cong \frac{\mathbb{C}[x_1, \ldots, x_n]}{\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_s}.$$

Mas, pelo teorema chinês do resto, este último anel é isomorfo a

$$\frac{\mathbb{C}[x_1, \ldots, x_n]}{\mathfrak{m}_1} \oplus \cdots \oplus \frac{\mathbb{C}[x_1, \ldots, x_n]}{\mathfrak{m}_s}.$$

Como cada um destes ideais é máximo, temos pelo teorema 9.13 que

$$\frac{\mathbb{C}[x_1, \ldots, x_n]}{\mathfrak{m}_j} \cong \mathbb{C} \text{ para todo } 1 \leq j \leq s.$$

Reunindo tudo isto,

$$\frac{\mathbb{C}[x_1, \ldots, x_n]}{\sqrt{I}} \cong \mathbb{C}^s,$$

de modo que

$$\dim_{\mathbb{C}} \left(\frac{\mathbb{C}[x_1, \ldots, x_n]}{\sqrt{I}} \right) = s,$$

que é o número de pontos de $\mathcal{Z}(I)$. Temos, assim, uma demonstração completa do teorema 9.14.

Em princípio este teorema poderia ser utilizado para calcular o número de pontos de um conjunto finito. Afinal de contas, pelo teorema 8.9, o conjunto dos monômios de $\mathbb{T} \backslash \mathrm{in}(\sqrt{I})$ forma uma base do anel quociente $\mathbb{C}[x_1, \ldots, x_n]/\sqrt{I}$. Como estes monômios são facilmente determinados a partir de uma base de Gröbner de $\sqrt{I}$, bastaria contá-los para obter a dimensão de $\mathbb{C}[x_1, \ldots, x_n]/\sqrt{I}$ como K-espaço vetorial.

Na prática, porém, a utilidade do teorema 9.14, na formulação dada acima, é limitada por dois problemas. O primeiro é que, dado o ideal I, precisamos ser capazes de calcular seu radical para que o teorema possa ser aplicado. O segundo, é que estamos supondo que o corpo de base é $\mathbb{C}$, que *não é* um corpo efetivo. Veremos como resolver estes problemas na seção 7, e com isto seremos capazes de obter um procedimento verdadeiramente efetivo para a contagem de pontos em conjuntos de dimensão zero. Nosso primeiro passo nesta direção consiste em estudar o caso mais simples possível do cálculo do radical em um anel de polinômios.

6. O radical em uma indeterminada

É chegada a hora de enfrentar a questão de como calcular efetivamente o radical de um dado ideal. Começaremos com o caso de um anel de polinômios com apenas uma variável sobre um corpo. Seja, pois, K um corpo e I um ideal do anel $K[x]$. Sabemos pelo teorema 2.3 do capítulo 3 que I é um ideal principal. Portanto, existe um polinômio g que gera I. Fatorando g, obtemos

$$g = cp_1^{e_1} \cdots p_s^{e_s}, \tag{81}$$

em que $c \in K \setminus \{0\}$, $p_1, \ldots, p_s$ são polinômios irredutíveis, e os expoentes $e_1, \ldots, e_s$ são todos positivos. Contudo, se

$$e = \max\{e_1, \ldots, e_s\},$$

então

$$(p_1 \cdots p_s)^e = \left(\frac{1}{c} p_1^{e-e_1} \cdots p_s^{e-e_s}\right) g \in I. \tag{82}$$

Isto implica que $p_1 \cdots p_s \in \sqrt{I}$. Entretanto, $\sqrt{I}$ também é um ideal principal, gerado, digamos, por um polinômio $q \in K[x]$. Mas isto só pode acontecer se q divide o produto $p_1 \cdots p_s$. Portanto, os fatores irredutíveis de q estarão entre os ps. Mais precisamente, a fatoração de q terá a forma

$$q = p_1^{\beta_1} \cdots p_s^{\beta_s},$$

em que $\beta_i = 1$ se p_i ocorre na fatoração de q; do contrário, $\beta_i = 0$. Mas, para algum $r > 0$,

$$q^r = p_1^{r\beta_1} \cdots p_s^{r\beta_s} \in I.$$

Portanto, o gerador g de I deve dividir q^r. Contudo, a multiplicidade de cada um dos ps na fatoração de g é positiva. Assim, g só pode dividir q^r se nenhum β é nulo. Logo, $q = p_1 \cdots p_s$.

A próxima proposição resume o que provamos até aqui. Antes, porém, convém introduzir a seguinte terminologia. Dado um polinômio $g \in K[x]$, escreva-o na forma da equação (81). Então, a *parte livre de quadrados* de g é igual a

$$\mathrm{lq}(g) = p_1 \cdots p_s.$$

Em outras palavras, a parte livre de quadrados é igual ao produto dos fatores irredutíveis de g tomados com multiplicidade um.

PROPOSIÇÃO 9.17. *Seja I um ideal em $K[x]$. O radical de I é gerado pela parte livre de quadrados do gerador de I.*

Para poder aplicar esta proposição precisamos de um procedimento para calcular a parte livre de quadrados de um polinômio sem precisar fatorá-lo. Tal procedimento existe, e se baseia na seguinte fórmula. Suponha que g se fatora como na equação (81). Então,

$$g' = \frac{dg}{dx} = \sum_{j=1}^{s} e_j c p_1^{e_1} \cdots p_j^{e_j - 1} \cdots p_s^{e_s}$$

donde

$$g' = cp_1^{e_1-1}\cdots p_s^{e_s-1}\sum_{j=1}^{s} e_j p_1\cdots p_{j-1}p_{j+1}\cdots p_s.$$

Note que a j-ésima parcela do somatório não inclui o fator p_j; de modo que

$$\operatorname{mdc}\left(g, \sum_{j=1}^{s} e_j p_1\cdots p_{j-1}p_{j+1}\cdots p_s\right) = 1.$$

Portanto,

$$\operatorname{mdc}(g, g') = p_1^{e_1-1}\cdots p_s^{e_s-1}.$$

Logo,

$$f = \frac{g}{\operatorname{mdc}(g, g')} = cp_1\cdots p_s;$$

isto é,

$$\operatorname{lq}(g) = \frac{f}{\operatorname{ld}(f)}.$$

Lembre-se que $\operatorname{ld}(f)$ representa o coeficiente líder do polinômio f; veja página 38. Mas o máximo divisor comum, para polinômios em uma variável, pode ser calculado sem a necessidade de fatorar os polinômios. Para isto basta usar o algoritmo euclidiano descrito na seção 5 do capítulo 3. Para referência futura, formalizaremos estas ideias em um algoritmo.

ALGORITMO 9.18 (Radical para polinômios em uma variável). *Dado o gerador g de um ideal I de $K[x]$, o algoritmo tem como saída o radical $\sqrt{I}$.*

Etapa 1: *Use o algoritmo euclidiano para calcular $d = \operatorname{mdc}(g, g')$.*
Etapa 2: *Calcule $f = g/d$.*
Etapa 3: *Retorne $\operatorname{lq}(g) = f/\operatorname{ld}(f)$.*

Por exemplo, se

$$g = x^9 + 7x^8 + 21x^7 + 39x^6 + 55x^5 + 61x^4 + 51x^3 + 33x^2 + 16x + 4,$$

então,

$$g' = 9x^8 + 56x^7 + 147x^6 + 234x^5 + 275x^4 + 244x^3 + 153x^2 + 66x + 16.$$

Aplicando o algoritmo euclidiano, obtemos

$$\operatorname{mdc}(g, g') = x^5 + 4x^4 + 6x^3 + 6x^2 + 5x + 2.$$

Efetuando a divisão de g pelo máximo divisor comum, obtemos

$$x^4 + 3x^3 + 3x^2 + 3x + 2.$$

Como este polinômio já é mônico, não precisamos dividi-lo por seu coeficiente líder. Assim,

$$\operatorname{lq}(g) = x^4 + 3x^3 + 3x^2 + 3x + 2.$$

Além de achar o radical, o algoritmo anterior também pode ser usado para calcular uma espécie de fatoração parcial de um polinômio $g \in K[x]$. Digamos que

$$g = p_1^{e_1}\cdots p_s^{e_s}$$

é a fatoração completa de g em $K[x]$. A *fatoração livre de quadrados* de f é

$$g = g_1 g_2^2 \cdots g_m^m,$$

em que g_i é o produto dos fatores irredutíveis de g cuja multiplicidade é i e

$$m = \mu(g) = \max\{e_1, \ldots, e_s\}$$

é a *multiplicidade máxima* de g. Além de poder ser obtida a um custo muito baixo, esta fatoração tem a vantagem de agrupar os fatores de f de acordo com sua multiplicidade.

Como vimos anteriormente, se

$$g = p_1^{e_1} \cdots p_s^{e_s}$$

então,

$$\mathrm{mdc}(g, g') = p_1^{e_1 - 1} \cdots p_s^{e_s - 1}.$$

Assim, um fator irredutível que tem multiplicidade k em f, terá multiplicidade $k-1$ em $\mathrm{mdc}(g, g')$. Desta forma, para determinar o produto dos polinômios irredutíveis que aparecem com multiplicidade k na fatoração de g basta calcular os que aparecem com multiplicidade $k-1$ na fatoração de $\mathrm{mdc}(g, g')$. Em particular, na notação usada na página 263,

$$\mu(\mathrm{mdc}(g, g')) = \mu(f) - 1 = m - 1.$$

Temos, então, um procedimento que nos permite reduzir o problema a um polinômio cuja multiplicidade máxima é menor que a de g.

Para converter este procedimento em um algoritmo, basta-nos encontrar uma maneira de calcular o produto g_1 dos fatores de multiplicidade 1. Porém, a parte livre de quadrados de $\mathrm{mdc}(g, g')$ contém apenas aqueles fatores irredutíveis cuja multiplicidade em g é maior ou igual a um. Desta forma,

$$g_1 = \frac{\mathrm{lq}(g)}{\mathrm{lq}(\mathrm{mdc}(g, g'))}.$$

Podemos sistematizar este algoritmo da seguinte forma.

ALGORITMO 9.19. *Dado um polinômio $g \in K[x]$, o algoritmo calcula sua fatoração livre de quadrados*

$$g = \mathrm{ld}(g) \cdot g_1 g_2^2 \cdots g_m^m,$$

sendo g_i o produto dos fatores irredutíveis de g cuja multiplicidade é i.

Inicialização: *Inicialize a lista $\mathcal{L}$ com $\mathrm{lc}(g)$ e as variáveis G e D com g.*

Laço principal: *Enquanto $D \neq 1$ repita:*

- *calcule $D = \mathrm{mdc}(G, G')$;*
- *acrescente $\mathrm{lq}(G)/\mathrm{lq}(D)$ ao final da lista $\mathcal{L}$;*
- *faça $G = D$.*

Etapa final: *Acrescente G ao final de $\mathcal{L}$, retorne $\mathcal{L}$ e páre.*

Note que a saída do algoritmo é a lista

$$\mathfrak{L} = [\mathrm{lc}(g), g_1, g_2, \ldots, g_m].$$

Portanto, o $i+1$-ésimo elemento da lista corresponde ao produto g_i dos fatores que aparecem em g com multiplicidade i. Assim, podemos determinar a multiplicidade do fator pela sua posição na lista. Por exemplo, seja

$$g = x^9 + 7x^8 + 21x^7 + 39x^6 + 55x^5 + 61x^4 + 51x^3 + 33x^2 + 16x + 4.$$

o mesmo polinômio utilizado no exemplo anterior. Neste caso a lista $\mathfrak{L}$ é inicializada como

$$\mathfrak{L} = [1],$$

já que $G = g$ é mônico. Aplicando o algoritmo a g, temos os seguintes passos:

Primeiro passo: Já vimos, anteriormente, que

$$D = \mathrm{mdc}(G, G') = x^5 + 4x^4 + 6x^3 + 6x^2 + 5x + 2;$$

e que

$$\mathrm{lq}(G) = x^4 + 3x^3 + 3x^2 + 3x + 2.$$

Utilizando o algoritmo 9.18, obtemos

$$\mathrm{lq}(D) = x^4 + 3x^3 + 3x^2 + 3x + 2;$$

donde

$$g_1 = 1.$$

Portanto g não tem fatores irredutíveis com multiplicidade um. Ao final deste passo

$$G = x^5 + 4x^4 + 6x^3 + 6x^2 + 5x + 2,$$
$$\mathfrak{L} = [1, 1].$$

Segundo passo: Desta vez, temos que

$$D = \mathrm{mdc}(G, G') = x + 1,$$

ao passo que

$$\mathrm{lq}(G) = x^4 + 3x^3 + 3x^2 + 3x + 2$$

e

$$\mathrm{lq}(D) = x + 1.$$

Efetuando a divisão, obtemos

$$g_2 = x^3 + 2x^2 + x + 2.$$

Ao final do segundo passo

$$G = x + 1,$$
$$\mathfrak{L} = [1, 1, x^3 + 2x^2 + x + 2].$$

Terceiro passo: Como $G' = 1$,

$$D = \mathrm{mdc}(G, G') = 1,$$

e resta-nos apenas acrescentar $G = x + 1$ ao final da lista, obtendo

$$\mathcal{L} = [1, 1, x^3 + 2x^2 + x + 2, x + 1].$$

O resultado obtido pelo algoritmo significa que

$$g = (x^3 + 2x^2 + x + 2)^2(x + 1)^3,$$

como é fácil comprovar, efetuando a multiplicação.

7. Radicais em dimensão zero

Seja K um corpo e I um ideal do anel $K[x_1, \ldots, x_n]$. Digamos que I é um ideal *radical* que tem *dimensão zero*, e vejamos o que podemos deduzir disto. Pelo corolário 9.10, da página 252, temos que

$$J \cap K[x_k] \neq \{0\},$$

para cada $1 \leq k \leq n$. Mas $J \cap K[x_k]$ é um ideal do anel de polinômios em uma indeterminada $K[x_k]$. Portanto, pelo teorema 2.3 da página 45, o ideal $J \cap K[x_k]$ é principal, gerado por um polinômio não nulo que vamos chamar de f_k. Fatorando f_k, temos que

$$f_k = cp_1^{e_1} \cdots p_s^{e_s},$$

em que c é uma constante não nula, os ps são polinômios irredutíveis mônicos de $K[x_k]$, e os es são inteiros positivos. Mas, se

$$e = \max\{e_1, \ldots, e_n\},$$

obtemos

$$(p_1 \cdots p_s)^e = (\frac{1}{c} p_1^{e-e_1} \cdots p_s^{e-e_s}) f_k \in J.$$

Como J é radical, podemos concluir que $p_1 \cdots p_s \in J$. Mostramos, assim, que se J é radical e de dimensão zero, então $J \cap K[x_k]$ contém um polinômio livre de quadrados. Surpreendentemente, a recíproca deste resultado é verdadeira. Isto foi provado por A. Seidenberg [**60**] e é o principal ingrediente do nosso algoritmo para cálculo do radical. A demonstração se apóia em uma passagem ao quociente. Lembre-se que é fácil reconhecer se um ideal I, de um anel A, é ou não radical, pelas propriedades do quociente A/I; veja proposição 8.2 da página 205.

LEMA DE SEIDENBERG. *Seja I um ideal de dimensão zero do anel de polinômios $K[x_1, \ldots, x_n]$. O ideal I é radical se, e somente se, para cada $1 \leq j \leq n$, existe um polinômio livre de quadrados em $I \cap K[x_j]$.*

DEMONSTRAÇÃO. Já provamos que a condição é necessária, resta apenas provar que é suficiente. Em outras palavras, precisamos mostrar que se, para cada $1 \leq j \leq n$, existe um polinômio livre de quadrados em $I \cap K[x_j]$, então I é radical.

A demonstração será por indução no número n de variáveis. Se $n = 1$, o resultado segue da proposição 9.17. Suponha, então, que o resultado vale

para todo anel de polinômios com $n-1$ indeterminadas, e vamos provar que também vale quando há n indeterminadas.

Começamos mostrando que é possível simplificar este passo, antes de abordá-lo. Pela hipótese de indução, $J \cap K[x_1]$ contém um polinômio livre de quadrados $g_1 \neq 0$. Fatorando g_1, podemos escrevê-lo na forma $g_1 = p_1 \cdots p_s$, em que os ps são polinômios irredutíveis sobre K. Como g_1 é livre de quadrados, a multiplicidade de cada p na fatoração de g_1 é igual a um. Lembrando do conteúdo da proposição 9.4, provaremos no passo indutivo apenas que

$$I + \langle p_j \rangle = \sqrt{I + \langle p_j \rangle}, \quad \text{para todo} \quad 1 \leq j \leq s. \tag{83}$$

Para provar (83), fixe um inteiro j entre 1 e s, e considere o quociente

$$A = K[x_1, \ldots, x_n]/(I + \langle p_j \rangle).$$

Como

$$(I + \langle p_j \rangle) \cap K[x_1] = \langle p_j \rangle,$$

temos, pelo teorema 8.4 da página 214, que

$$A \cong L[x_2, \ldots, x_n]/\overline{I}, \tag{84}$$

em que $L = K[x_1]/\langle p_j \rangle$. Como p_j é um polinômio irredutível de $K[x_1]$ temos, pela proposição 8.2 da página 205, que L é um corpo. O ideal $\overline{I}$ corresponde à imagem de I em $L[x_2, \ldots, x_n]$. Mas, se

$$I \cap K[x_j] = \langle g_j \rangle,$$

então

$$\overline{I} \cap L[x_j] = \langle \overline{g_j} \rangle.$$

Como, por hipótese, g_j é um polinômio livre de quadrados, isto também será verdade para a imagem $\overline{g_j}$ de g_j em $L[x_j]$. Com isso, $\overline{I}$ é um ideal do anel $L[x_2, \ldots, x_n]$, que satisfaz as condições da proposição 9.4. Portanto, pela hipótese de indução $\overline{I}$ é um ideal radical de $L[x_2, \ldots, x_n]$. Segue, assim, da equação (84) e da proposição 8.2 que A não tem elementos nilpotentes. Contudo,

$$A = K[x_1, \ldots, x_n]/(I + \langle p_j \rangle).$$

Assim, aplicando novamente a proposição 8.2, concluímos que $I + \langle p_j \rangle$ é um ideal radical. Finalmente, segue da proposição 9.4 que se $I + \langle p_j \rangle$ é radical para cada $1 \leq j \leq s$, então I também é radical. □

De acordo com o lema de Seidenberg, há apenas duas coisas que precisamos fazer para calcular o radical de um ideal I de dimensão zero em $K[x_1, \ldots, x_n]$. A primeira é calcular as bases de Gröbner das interseções de I com os subanéis $K[x_j]$, para cada $1 \leq j \leq n$. Como cada interseção nos dá um ideal em um anel de polinômios em uma variável, estas bases de Gröbner conterão apenas um elemento. Digamos que

$$I \cap K[x_j] = \langle g_j \rangle \text{ para } 1 \leq j \leq n.$$

A segunda etapa consiste em calcular a representação livre de quadrados q_j de cada um dos g_j. O ideal J gerado por I e pelos qs é um ideal radical pelo

lema de Seidenberg. Mas, pela proposição 3.13, $\sqrt{I}$ é o menor ideal radical que contém I. Como

$$I \subseteq J \subseteq \sqrt{I},$$

podemos concluir que J e $\sqrt{I}$ são iguais. Podemos formular este algoritmo detalhadamente da seguinte forma.

ALGORITMO 9.20 (Radical de ideais de dimensão zero). *Dado um ideal I de dimensão zero em $K[x_1, \ldots, x_n]$, o algoritmo calcula $\sqrt{I}$.*

Primeira etapa: *Para $1 \leq j \leq n$ repita:*

- *calcule a base de Gröbner reduzida G_j de I com respeito à ordem lexicográfica para a qual*

$$x_j < x_1 < \cdots < x_{j-1} < x_{j+1} < \cdots < x_n;$$

- *tome g_j tal que $G \cap K[x_j] = \{g_j\}$.*
- *calcule a representação livre de quadrados q_j de g_j usando o algoritmo 9.18.*

Segunda etapa: *Retorne*

$$J = I + \langle q_1, \ldots, q_n \rangle.$$

Como exemplo da aplicação do algoritmo, considere o ideal de dimensão zero

$$I = \langle x_1 + 5x_2 + x_3, x_1^3 + x_2, x_1x_2 - x_3^2 \rangle$$

do anel $\mathbb{Q}[x_1, x_2, x_3]$. Calculando a base de Gröbner de I relativamente a lex com $x_3 < x_2 < x_1$, obtemos

$$\{625x_3^6 + 31x_3^4 + x_3^2, 9x_2 - 2500x_3^5 + x_3^3, x_1 + 5x_2 + x_3\}.$$

Portanto,

$$I \cap \mathbb{Q}[x_3] = \langle 625x_3^6 + 31x_3^4 + x_3^2 \rangle,$$

e a parte livre de quadrados do gerador deste último ideal é

$$\mathrm{lq}(625x_3^6 + 31x_3^4 + x_3^2) = 625x_3^5 + 31x_3^3 + x_3$$

Repetindo os cálculos para lex com $x_1 < x_2 < x_3$, obtemos a base

$$\{25x_1^6 - 9x_1^4 + x_1^2, x_2 + x_1^3, x_3 + 5x_2 + x_1\}$$

e a parte livre de quadrados do gerador de $I \cap \mathbb{Q}[x_1]$ é

$$\mathrm{lq}(25x_1^6 - 9x_1^4 + x_1^2) = 25x_1^5 - 9x_1^3 + x_1;$$

ao passo que se $x_2 < x_1 < x_3$, a base é

$$\{15625x_2^5 - 54x_2^3 + x_2, 56x_1x_2 - 15625x_2^4 + 279x_2^2, \\ x_1^2 + 9x_1x_2 + 25x_2^2, x_3 + x_1 + 5x_2\}$$

e a parte livre de quadrados do gerador de $I \cap \mathbb{Q}[x_2]$ é

$$\mathrm{lq}(15625x_2^5 - 54x_2^3 + x_2) = 15625x_2^5 - 54x_2^3 + x_2.$$

De acordo com o algoritmo, isto significa que o radical de I é o ideal gerado pelos polinômios

$$x_1 + 5x_2 + x_3, x_1^3 + x_2, x_1x_2 - x_3^2, 625x_3^5 + 31x_3^3 + x_3,$$
$$25x_1^5 - 9x_1^3 + x_1, 15625x_2^5 - 54x_2^3 + x_2,$$

cuja base de Gröbner relativa a lex com $x_3 < x_2 < x_1$ é igual a

$$\{625x_3^5 + 31x_3^3 + x_3, 9x_2 - 2500x_3^5 + x_3^3, x_1 + 5x_2 + x_3\}.$$

O algoritmo de Seidenberg requer que calculemos os geradores dos ideais $I \cap K[x_j]$ para cada uma das variáveis x_j do anel de polinômios. Ao formular o algoritmo acima, utilizamos a ordem lexicográfica para fazer isto, o que não é bom, porque já sabemos da seção 7 do capítulo 5 que esta é a ordem para a qual o algoritmo de Buchberger é mais lento. Para piorar, este passo precisa ser repetido tantas vezes quantas são as variáveis do anel de polinômios. Para nossa sorte há uma outra maneira de abordar o mesmo problema, que consiste em obter o polinômio a partir de uma base de Gröbner relativa a uma ordem (rápida) qualquer, que pode ser escolhida de acordo com o ideal que está sendo utilizado.

A ideia é a seguinte. Digamos que queremos calcular o gerador de $I \cap K[x_j]$. Como estamos supondo que $K[x_1, \ldots, x_n]/I$ tem dimensão finita sobre K, as imagens das potências de x_j no anel quociente não podem ser todas linearmente independentes. Suponhamos que m é o menor inteiro positivo tal que x^m é linearmente dependente das potências anteriores em $K[x_1, \ldots, x_n]/I$. Neste caso, existem coeficientes $a_{m-1}, \ldots, a_0 \in K$ tais que

$$\overline{x_j}^m = a_{m-1}\overline{x_j}^{m-1} + \cdots + a_1\overline{x_j} + a_0$$

em que a barra denota classes em $K[x_1, \ldots, x_n]/I$. Mas isto significa que

$$x_j^m - a_{m-1}x_j^{m-1} - \cdots - a_1x_j - a_0 \in I. \tag{85}$$

Além disso, como m é o menor inteiro positivo que satisfaz esta propriedade, então o polinômio (85) gera $I \cap K[x_j]$; veja a demonstração do teorema 2.3. Portanto, para obter o polinômio desejado, basta calcular m e os coeficientes da combinação linear. A questão, agora, é como fazer isto de maneira eficiente.

A ideia mais ingênua para encontrar os coeficientes da decomposição acima é utilizar o método dos coeficientes a determinar, incrementando as potências de $\overline{x_j}$, de um em um, até achar uma que seja combinação linear das anteriores. Por sorte esta ideia funciona muito bem. Vejamos como utilizar esta estratégia para determinar se $\overline{x_j}^k$ é combinação linear de $1, \ldots, \overline{x_j}^{k-1}$, em que $k \geq 0$ é um inteiro fixado. Como o algoritmo vai incrementando o expoente de $\overline{x_j}$ de um em um, podemos supor que $1, \ldots, \overline{x_j}^{k-1}$ são linearmente independentes, do contrário o algoritmo já teria parado em um passo anterior.

Como a suposta combinação linear terá $k+1$ coeficientes, introduzimos novas variáveis $y_0, \ldots, y_k$. A combinação linear desejada terá a forma

$$y_k\overline{x_j}^k + \cdots + y_1\overline{x_j} + y_0,$$

em que a barra denota classes em $K[x_1, \ldots, x_n]/I$. A esta altura precisamos introduzir uma base de Gröbner G de I, que pode ser calculada relativamente a qualquer ordem monomial desejada. Como $\mathrm{R}_G(x_j^k)$ é um representante de $\overline{x_j^k}$ no anel quociente, o problema se resume a achar valores para os ys de modo que

$$y_k \mathrm{R}_G(x_j^k) + \cdots + y_1 \mathrm{R}_G(x_j) + y_0 = 0, \tag{86}$$

A expressão da esquerda pode ser reescrita como uma combinação linear de $1, \ldots, \overline{x_j}^{k-1}$ com coeficientes $\alpha_0, \ldots, \alpha_{k-1} \in K[y_0, \ldots, y_k]$. Mas, a independência linear de $1, \ldots, \overline{x_j}^{k-1}$ implica que (86) é equivalente a

$$\alpha_0 = \cdots = \alpha_{k-1} = 0. \tag{87}$$

Portanto, $\overline{x_j}^k$ é combinação linear de $1, \ldots, \overline{x_j}^{k-1}$ se, e somente se, o sistema acima tem solução não trivial. Por sorte os y aparecem com grau um em (86), o que faz de (87) um sistema linear. Isto simplifica enormemente os cálculos.

Vejamos o que acontece quando encontramos o menor k para o qual (87) tem solução, aquele que chamamos de m na discussão acima. Neste caso, o sistema homogêneo (87) é indeterminado, e seu espaço solução é infinito. Contudo, a cada solução

$$(u_0, \ldots, u_m) \in K^m$$

de (87) corresponde um polinômio não nulo

$$u_0 + u_1 x_j + \cdots + u_m x_j^m$$

que é gerador de $K[x_j] \cap I$. Mas, quaisquer dois geradores deste ideal são múltiplos constantes um do outro. Portanto, o espaço solução do sistema (87) não pode ter dimensão maior que 1. Assim, quando m for alcançado e (87) for indeterminado, resolvemos o sistema usando y_m como parâmetro e calculamos o valor dos demais ys fazendo $y_m = 1$. Desta forma garantimos que o gerador escolhido para $K[x_j] \cap I$ é mônico. Relatando esta estratégia passo a passo, obtemos o seguinte algoritmo.

ALGORITMO 9.21. *Dados um inteiro j entre 1 e n, um ideal de dimensão zero I de $K[x_1, \ldots, x_n]$ e uma ordem monomial deste anel, o algoritmo calcula um gerador mônico para $K[x_j] \cap I$.*

Etapa 1: *Calcule uma base de Gröbner G para I, relativamente à ordem monomial dada.*

Etapa 2: *Inicialize $k = 1$ e $I = \langle y_0 \rangle$.*

Etapa 3: *Enquanto o sistema linear S só tiver solução nula, repita*

- *calcule*

$$y_k \mathrm{R}_G(x_j^k) + \cdots + y_1 \mathrm{R}_G(x_j) + y_0,$$

  e determine o ideal I de $K[y_0, \ldots, y_m]$ gerado pelos coeficientes de $1, \ldots, x_j^{k-1}$;
- *incremente k de uma unidade;*

Etapa 4: *Quando o sistema linear correspondente a I tiver solução não nula, resolva-o relativamente à variável y_k e calcule a solução*

$$y_k = 1, y_{k-1} = u_{k-1}, \ldots, y_0 = u_0.$$

Etapa 5: *Imprima* $x_j^k + u_{k-1}x_j^{k-1} + \cdots u_1 x_j + u_0$.

Aplicaremos este algoritmo para calcular $I \cap \mathbb{Q}[x_3]$, em que

$$I = \langle x_1 + 5x_2 + x_3, x_1^3 + x_2, x_1x_2 - x_3^2 \rangle$$

é o mesmo ideal do anel $\mathbb{Q}[x_1, x_2, x_3]$ utilizado no exemplo anterior. A base de Gröbner G de I relativamente a glex com $x_3 < x_2 < x_1$, é

$$\{x_1 + 5x_2 + x_3, 5x_2^2 + x_2x_3 + x_3^2, 20x_2x_3^2 + 9x_3^3 + x_2, 125x_3^4 + 9x_2x_3 + 4x_3^2\}.$$

Os restos das primeiras quatro potências de x_3 relativamente a esta base são iguais às próprias potências e, portanto, linearmente independentes. Por outro lado,

$$\mathrm{R}_G(x_3^4) = \frac{-9}{125}x_2x_3 - \frac{-4}{125}x_3^2,$$

que contém x_2 e, por isso, ainda é linearmente independente dos restos anteriores. De modo semelhante,

$$\mathrm{R}_G(x_3^5) = \frac{1}{2500}x_3^3 + \frac{9}{2500}x_2,$$

continua linearmente independente. Entretanto,

$$\mathrm{R}_G(x_3^6) = \frac{279}{78125}x_2x_3 - \frac{1}{78125}x_2,$$

é linearmente *dependende* dos demais pois

$$\frac{78125}{279}\mathrm{R}_G(x_3^6) + \frac{125}{9}\mathrm{R}_G(x_3^4) = -\frac{125}{279}x_3^2$$

que é igual a

$$-\frac{125}{279}\mathrm{R}_G(x_3^2).$$

Logo,

$$\frac{78125}{279}\mathrm{R}_G(x_3^6) + \frac{125}{9}\mathrm{R}_G(x_3^4) + \frac{125}{279}\mathrm{R}_G(x_3^2) \in I;$$

de modo que o polinômio desejado é

$$\frac{78125}{279}x_3^6 + \frac{125}{9}x_3^4 + \frac{125}{279}x_3^2 \in I.$$

Multiplicando este polinômio por $279/125$ obtemos

$$625x_3^6 + 31x_3^4 + x_3^2 \in I;$$

o mesmo polinômio que já havíamos encontrado anteriormente usando a ordem lexicográfica.

Para encerrar usaremos o Lema de Seidenberg para estabelecer um critério efetivo que nos permita contar a quantidade de pontos de um conjunto algébrico

finito. Lembre-se que, em princípio, já sabemos fazer isto. De fato, se I for um ideal de $\mathbb{C}[x_1, \ldots, x_n]$, então, pelo teorema 9.14, $\mathcal{Z}(I)$ tem

$$\dim_{\mathbb{C}} \mathbb{C}[x_1, \ldots, x_n]/I \quad \text{pontos.}$$

Mas, pelo teorema 8.9 da página 224, esta dimensão é igual à quantidade de monômios de $\mathbb{T}^n$ que *não* são divisíveis por $\mathrm{in}(g)$, para nenhum g em uma *base de Gröbner* de I. Se o corpo dos complexos fosse efetivo, nosso problema estaria resolvido: bastaria calcular esta base de Gröbner. Como não é este o caso, precisaremos refinar a teoria um pouco mais.

PROPOSIÇÃO 9.22. *Se I é um ideal de dimensão zero de $K[x_1, \ldots, x_n]$, então $\sqrt{I_c}$ é igual ao ideal de $\mathbb{C}[x_1, \ldots, x_n]$ gerado por $\sqrt{I}$.*

DEMONSTRAÇÃO. Como I tem dimensão zero por hipótese,

$$\mathcal{Z}(I) = \mathcal{Z}(\sqrt{I}) = \mathcal{Z}(I_c) = \mathcal{Z}(\sqrt{I_c}), \tag{88}$$

pelo ????. Contudo, $\sqrt{I} \subseteq \sqrt{I_c}$, de modo que

$$\sqrt{I} \cap K[x_j] \subseteq \sqrt{I} \cap \mathbb{C}[x_j] \subseteq \sqrt{I_c} \cap \mathbb{C}[x_j],$$

para todo $1 \leq j \leq n$. Como estes ideais são principais,

$$\langle p_j \rangle = \sqrt{I} \cap K[x_j] \subseteq \sqrt{I_c} \cap \mathbb{C}[x_j] = \langle q_j \rangle,$$

em que $p_j \in K[x_j]$ e $q_j \in \mathbb{C}[x_j]$. Assim, q_j divide p_j. Entretanto, pelo lema de Seidenberg, p_j e q_j são polinômios livres de quadrados. Portanto, se os radicais de I e I_c fossem distintos, então existiria um fator linear de q_j que não divide p_j. Mas, as raízes de p_j correspondem às coordenadas x_j dos pontos de $\mathcal{Z}(\sqrt{I})$. Isto significa que há pontos de $\mathcal{Z}(\sqrt{I_c})$ cuja coordenada x_j não corresponde a nenhum ponto de $\mathcal{Z}(\sqrt{I})$, o que contradiz as igualdades 88 e prova a proposição. □

Observe que estamos incluindo, entre as hipóteses da proposição, que o ideal tenha dimensão zero. Esta hipótese é realmente necessária, já que a igualdade da proposição não vale para um ideal qualquer em um anel de polinômios. Para mais detalhes veja o exercício ???.

COROLÁRIO 9.23. *Se I é um ideal de dimensão zero de $K[x_1, \ldots, x_n]$, então*

$$\dim_{\mathbb{C}} \left(\frac{\mathbb{C}[x_1, \ldots, x_n]}{\sqrt{I_c}} \right) = \dim_K \left(\frac{K[x_1, \ldots, x_n]}{\sqrt{I}} \right).$$

DEMONSTRAÇÃO. Seja G uma base de Gröbner para $\sqrt{I}$. Pelo Critério de Buchberger, esta também é uma base de Gröbner para o ideal do anel $\mathbb{C}[x_1, \ldots, x_n]$ gerado por $\sqrt{I}$, que é igual a $\sqrt{I_c}$, pela proposição 9.22. Portanto, pelo teorema 8.9, as dimensões de

$$\frac{\mathbb{C}[x_1, \ldots, x_n]}{\sqrt{I_c}} \text{ e de } \frac{K[x_1, \ldots, x_n]}{\sqrt{I}},$$

são ambas iguais ao número de monômios de $\mathbb{T}^n$ que não são divisíveis por $\mathrm{in}(g)$, para algum $g \in G$, o que prova o corolário. □

Resta-nos aplicar este resultado a um exemplo. Digamos que desejamos contar a quantidade de pontos do conjunto algébrico determinado em $\mathbb{C}^3$ pelo ideal

$$I = \langle x_1 + 5x_2 + x_3, x_1^3 + x_2, x_1x_2 - x_3^2 \rangle$$

do anel $\mathbb{Q}[x_1, x_2, x_3]$; o mesmo que consideramos no exemplo da página 267. Naquela ocasião já havíamos determinado que o radical deste ideal tinha base de Gröbner

$$\{625x_3^5 + 31x_3^3 + x_3, 9x_2 - 2500x_3^5 + x_3^3, x_1 + 5x_2 + x_3\}.$$

relativamente à ordem lexicográfica com $x_3 < x_2 < x_1$. Como a equação que define x_2 em termos das variáveis menores é linear em x_2 e o mesmo acontece com a equação que define x_1, podemos concluir que,

$$\mathbb{Q}[x_1, x_2, x_3]/I \cong \mathbb{Q}[x_3]/\langle 625x_3^5 + 31x_3^3 + x_3 \rangle,$$

que tem dimensão cinco. Portanto, $\mathcal{Z}(I)$ tem exatamente cinco pontos.

8. FGLM

Como vimos na seção 7 do capítulo 5, o tempo de execução do algoritmo de Buchberger sob a ordem lexicográfica tende a ser muito maior do que quando utilizamos uma ordem que começa selecionando os polinômios pelo grau. Isto é muito frustrante porque várias das aplicações que fizemos requerem o uso da ordem lexicográfica. Uma maneira de contornar este problema seria inventar uma forma de construir uma base de Gröbner sob lex a partir de uma base cujo cálculo seja mais rápido. Naturalmente, para que isto valha a pena, o processo que converte a ordem rápida em lex tem que ser, ele próprio, muito eficiente. Nesta seção veremos um algoritmo que, no caso especial em que o ideal tem dimensão zero, converte uma base qualquer para lex utilizando apenas a solução de sistemas lineares. Publicado em 1993 por J. C. Faugère, P. Gianni, D. Lazard e T. Mora, o algoritmo tornou-se conhecido como FGLM, a partir das iniciais dos sobrenomes dos autores; veja [**25**].

ALGORITMO 9.24 (O algoritmo FGLM). *Seja $I \neq 0$ um ideal de dimensão zero de $K[x_1, \ldots, x_n]$. Dada uma base de Gröbner G de I relativamente a uma ordem monomial qualquer $>$, o algoritmo tem como saída uma base de Gröbner G_{lex} de I para a ordem lexicográfica com $x_1 < \cdots < x_n$ e uma base B do K-espaço vetorial $K[x_1, \ldots, x_n]/I$.*

Inicialização: $G_{\text{lex}} = B = \emptyset$, $g = 0$ *e* $\mu = 1$.

Laço principal: *Enquanto* $\text{in}_>(g) \neq x_n^k$, *para algum* $k > 0$ *inteiro, repita:*

- *se μ for linearmente* ***dependente*** *das imagens de B no quociente $K[x_1, \ldots, x_n]/I$, escolha constantes c_ν tais que*

$$\text{R}_G(\mu) = \sum_{\nu \in B} c_\nu \text{R}_G(\nu), \tag{89}$$

e acrescente o polinômio

$$g = \mu - \sum_{\nu \in B} c_\nu \nu \in I$$

a G_{lex}*;*

- *se* μ *for linearmente* ***independente*** *das imagens de* B *no quociente* $K[x_1, \ldots, x_n]/I$*, apenas acrescente* μ *a* B*;*
- *substitua* μ *pelo elemento seguinte sob lex que não é divisível pelo termo inicial de nenhum elemento em* G_{lex}.

Neste enunciado, formulamos a condição sob a qual o laço principal opera em termos de monômios serem linearmente dependentes ou não de outros monômios. Apesar disto tornar o conteúdo conceitual da encruzilhada mais claro, não é desta forma que o algoritmo opera. Na verdade, o algoritmo calcula diretamente com os restos dos monômios por G, já que estes representam as mesmas classes de equivalência módulo I que os próprios monômios. Naturalmente a vantagem de calcular com os restos é que duas classes coincidem se, e somente se, os restos que as representam são iguais *como polinômios*. Em outras palavras, basta descobrir se existem constantes c_ν que satisfaçam (89). Isto pode ser feito facilmente resolvendo um sistema linear.

Antes de explicar porque este algoritmo para e porque funciona corretamente, convém calcular um exemplo em todos os seus detalhes. Seja I o ideal gerado pelos polinômios

$$x_1^2 x_2 - 1 \text{ e } x_1^3 - x_2^2$$

no anel $\mathbb{Q}[x_1, x_2]$. Aplicando o algoritmo de Buchberger sob a ordem glex com $x_2 > x_1$, encontramos a seguinte base de Gröbner para I,

$$G = \{x_1^3 - x_2^2, x_1^2 x_2 - 1, x_2^3 - x_1\},$$

na qual os polinômios foram escritos com seus termos iniciais mais à esquerda. Usaremos agora o algoritmo FGLM para determinar uma base de Gröbner relativa a lex para este mesmo ideal.

Vimos que μ é inicializado como 1 que, evidentemente, é linearmente independente módulo I. Com o monômio seguinte a 1 em lex é x_1, temos ao final da primeira execução do laço principal que

$$\begin{aligned} \mu &= x_1 \\ G_{\text{lex}} &= \emptyset \\ B &= \{1\}. \end{aligned}$$

Mas x_1 é independente de $\{1\}$ módulo I e, para falar a verdade, x_1^2 também é independente de $\{1, x_1\}$ módulo I. Com isto, ao final das primeiras três execuções do laço principal teremos:

$$\begin{aligned} \mu &= x_1^3 \\ G_{\text{lex}} &= \emptyset \\ B &= \{1, x_1, x_1^2\}. \end{aligned}$$

Desta vez

$$\mathrm{R}_G(x_1^3) = x_2^2,$$

que ainda é linearmente independente de $B = \{1, x_1, x_1^2\}$; donde

$$\begin{aligned} \mu &= x_1^4 \\ G_{\mathrm{lex}} &= \emptyset \\ B &= \{1, x_1, x_1^2, x_1^3\}. \end{aligned}$$

De fato, continuaremos obtendo restos independentes até chegarmos a x_1^6. Ao final da execução deste laço, teremos

$$\begin{aligned} \mu &= x_1^7 \\ G_{\mathrm{lex}} &= \emptyset \\ B &= \{1, x_1, x_1^2, x_1^3, x_1^4, x_1^5, x_1^6\}. \end{aligned}$$

Mas,

$$\mathrm{R}_G(x_1^7) = 1$$

que é linearmente dependente de B. Desta vez, o polinômio $x_1^7 - 1$ deve ser anexado a G_{lex}. Como $\mathrm{in}_{\mathrm{lex}}(x_1^7 - 1) = x_1^7$, todas as potências de x_1 maiores que x_1^7 serão divisíveis pelo termo inicial de $x_1^7 - 1$. Logo, o próximo monômio a ser considerado será x_2, e ao final deste laço temos

$$\begin{aligned} \mu &= x_2 \\ G_{\mathrm{lex}} &= \{x_1^7 - 1\} \\ B &= \{1, x_1, x_1^2, x_1^3, x_1^4, x_1^5, x_1^6\}. \end{aligned}$$

Contudo, os restos dos elementos de B por G são

$$\{1, x_1, x_1^2, x_2^2, x_1x_2^2, x_2, x_1x_2\}$$

de modo que x_2 já apareceu no conjunto como o resto de x_1^5. Por isso devemos acrescentar $x_2 - x_1^5$ a G_{lex}. Como, além disso, o termo inicial deste elemento é uma potência de x_2, o algoritmo encerra sua execução nesta etapa. Portanto, podemos afirmar que I tem base de Gröbner

$$G_{\mathrm{lex}} = \{x_1^7 - 1, x_2 - x_1^5\},$$

relativamente a lex e que o quociente $\mathbb{Q}[x_1, x_2]/I$ tem base

$$B = \{1, x, x^2, x^3, x^4, x^5, x^6\};$$

de modo que

$$\dim_{\mathbb{Q}}(\mathbb{Q}[x_1, x_2]/I) = 8.$$

Em particular, o conjunto algébrico

$$\mathcal{Z}(x_1^3 - x_2^2, x_1^2x_2 - 1, x_2^3 - x_1)$$

tem oito elementos distintos.

Resta-nos explicar porque o algoritmo o funciona corretamente. Para isto usaremos algumas consequências, mais ou menos imediatas, das escolhas de

elementos que são feitas ao longo de sua execução. Em todas as afirmações abaixo o termo inicial é tomado relativamente à ordem lexicográfica:

(1) as imagens dos elementos de B são linearmente independentes em $K[x_1, \ldots, x_n]/I$;
(2) o termo inicial de $g \in G_{\text{lex}}$ não é divisível pelo termo inicial de nenhum elemento de G_{lex} que preceda g;
(3) se $g \in G_{\text{lex}}$ e μ é um monômio menor que $\text{in}_{\text{lex}}(g)$ então μ é divisível pelo termo inicial de algum elemento de G_{lex} anterior a g ou $\mu \in B$.

O ALGORITMO FGLM PARA: Suponhamos, por contradição, que o algoritmo *não* para. Para que isto fosse possível, uma das duas opações no laço principal precisaria ser executada infinitas vezes, sem que nunca chegássemos a um elemento cujo termo inicial, relativamente a lex, fosse uma potência de x_1. Entretanto, como o quociente $K[x_1, \ldots, x_n]/I$ tem dimensão finita como espaço vetorial sobre K, o conjunto B tem que ser finito pelo teorema 8.9. Isto forçaria o conjunto G_{lex} a ser infinito. Contudo, se

$$G_{\text{lex}} = \{g_1, g_2, \ldots\},$$

então, por (2), $\text{in}_{\text{lex}}(g_j)$ não poderia dividir $\text{in}_{\text{lex}}(g_i)$ quando $i < j$. Isto implicaria que dois termos da cadeia crecente

$$\langle \text{in}_{\text{lex}}(g_1) \rangle \subset \langle \text{in}_{\text{lex}}(g_1), \text{in}_{\text{lex}}(g_2) \rangle \subset \cdots$$

nunca poderiam coincidir, o que contradiz o teorema 3.5 da página 78 (ou, se você preferir, o teorema da base de Hilbert).

Tendo provado que o algoritmo para, mostraremos que o conjunto finito G_{lex} por ele gerado é uma base de Gröbner relativamente à ordem lexicográfica com $x_1 < \cdots < x_n$.

O ALGORITMO FGLM FUNCIONA: Seja, pois, $\mu \in \text{in}_{\text{lex}}(I)$. Devemos mostrar que μ é divisível pelo termo inicial de algum elemento de G_{lex}. Mas, se g foi o último elemento acrescentado a G_{lex} então, pela condição de parada do laço principal, temos que

$$\text{in}_{\text{lex}}(g) = x_n^k \quad \text{para algum inteiro } k > 0.$$

Como x_n é a maior das variáveis sob a ordem monomial que adotamos, temos que se $\mu \geq x_n^k$ então μ tem que conter uma potência de x_n com expoente maior que k. Logo,

$$\text{in}_{\text{lex}}(g) = x_n^k \text{ divide } \mu,$$

e obtemos o resultado desejado. Portanto, podemos supor que

$$\mu < \text{in}_{\text{lex}}(g).$$

Neste caso o resultado segue das observações (1) e (3) listadas acima, provando, assim, que G_{lex} é uma base de Gröbner de I.

9. Comentários e complementos

De todos os capítulos, este é provavelmente o que cobre menos material relativamente ao tema proposto, que é nada menos que uma área inteira da matemática, a *geometria algébrica*. E que área? Considerada anos atrás como uma das áreas mais abstratas da matemática, nos dias de hoje métodos e estruturas da geometria algébrica penetraram não apenas outras áreas da matemática, como também a física, a computação gráfica e a análise numérica.

Para fazer justiça à importância e à profundidade desta área, este capítulo não deve ser considerado como mais do que um tira-gosto. Tratamos apenas de tópicos muito elementares, e sequer avançamos para além dos conjuntos algébricos afins. Mas é na geometria algébrica projetiva que a área mostra seu real sabor e revela toda a sua elegância. Para falar a verdade, mesmo nosso tratamento das variedades afins é extremamente incompleto e inadequado, porque deixa de fora tópicos básicos como a definição e o cálculo da dimensão de conjuntos algébricos; veja [**17**, capítulo 9].

Um tratamento mais completo da geometria algébrica e da álgebra comutativa que lhe serve de linguagem, ao estilo computacional, pode ser encontrado nos livros [**17**] e [**33**].

10. Exercícios

1. Prove que se I e J são ideais de um anel A então
$$I + J = \{i + j \mid i \in I \text{ e } \ j \in J\}$$
também é.

2. Seja A um subanel de um anel B. Mostre que se J é um ideal radical de B então $J \cap A$ é um ideal *radical* de A.

3. Calcule a interseção dos conjuntos algébricos definidos pelos seguintes ideais de $\mathbb{Q}[x, y, z]$
$$I_1 = \langle x^2y - y - 1, xy + x^2\rangle \quad \text{e} \quad I_2 = \langle x^2 - 1, -x^2y + xy + y + x^3 + x^2 - x\rangle.$$

4. Dados ideais I_1 e I_2 de $K[x - 1, \ldots, x_n]$, e uma nova variável y, defina o ideal J de $K[x - 1, \ldots, x_n, y]$ por
$$J = \langle yI_1, (1 - y)I_2\rangle.$$
Prove que
$$I_1 \cap I_2 = J \cap K[x_1, \ldots, x_n].$$

5. Sejam I_1 e I_2 os ideais de $\mathbb{Q}[x, y, z]$ definidos na questão ???. Calcule $I_1 \cap I_2$ usando o método do exercício anterior.

6. No mecanismo ilustrado na figura 5, os pontos A e B estão fixos e as juntas em A, B, C e D são articuladas. Prove que, se $\overline{AB} = \sqrt{2\overline{BC}}$ então o ponto P descreve uma lemniscata.

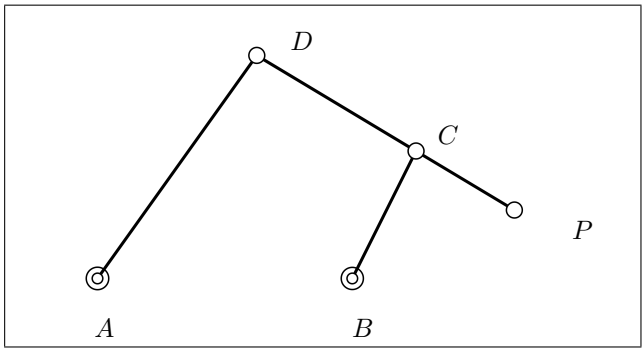


FIGURA 5. Mecanismo para desenhar a lemniscata

7. Dizemos que um ideal de dimensão finita I do anel $K[x_1, \ldots, x_n]$ está em *posição geral* relativamente à variável x_j se quaisquer dois pontos de $\mathcal{Z}(I)$ têm j-ésimas coordenadas distintas.

8. Calcule a fatoração livre de quadrados dos seguintes polinômio de $\mathbb{Q}[x]$:
   (a) $x^8 - 5x^6 + 6x^4 + 4x^2 - 8$;
   (b) $x^6 + 11x^4 + 39x^2 + 45$;
   (c) $x^4 + 12x^3 + 6x^2 - 52x + 33$.

CAPíTULO 10

Integração de funções racionais

As funções racionais estão aquelas que primeiro aprendemos a integrar em um curso básico de cálculo. O método ensinado ainda hoje foi descrito originalmente por Johan Bernoulli no século XVIII e consiste em decompor a função racional em frações parciais e integrá-las uma a uma. O resultado contém dois tipos de parcelas: uma função racional e uma soma de logaritmos. Apesar de sua descrição simples, este método não é usado na prática, já que requer que o denominador da função racional seja fatorado sobre os reais. Entretanto, já no século XIX eram conhecidos métodos mais eficientes para calcular a parte racional da integral. O desenvolvimento da computação algébrica nas últimas décadas do século XX deu novo ímpeto a esta área, levando a vários algoritmos completos para a integração eficiente de funções racionais. Neste capítulo descrevemos um destes métodos, baseado no uso de bases de Gröbner. Contudo, iniciamos o capítulo revisando o método de Bernoulli, já que é conceitualmente mais simples, além de sugerir os passos que devemos seguir na construção de um algoritmo melhor.

1. Funções racionais

Como vimos na seção 2 do capítulo 2, dado qualquer domínio D, podemos construir um corpo $Q(D)$, que contém D e cujos elementos são frações que têm numerador e denominador em D. Aplicando esta construção ao anel de polinômios $K[x]$, sobre um corpo K, obtemos o corpo das funções racionais sobre K; veja página 42. Portanto, os elementos de $K(x)$ são expressões da forma

$$f/g \quad \text{em que} \quad f, g \in K[x] \quad \text{e} \quad g \neq 0.$$

Duas expressões deste tipo f_1/g_1 e f_2/g_2 são iguais se

$$f_1 g_2 = f_2 g_1.$$

Já a adição e multiplicação de dois elementos de $f_1/g_1, f_2/g_2 \in K(x)$ são definidas por

$$\frac{f_1}{g_1} + \frac{f_2}{g_2} = \frac{f_1 g_2 + f_2 g_1}{g_1 g_2} \quad \text{e por} \quad \frac{f_1}{g_1} \cdot \frac{f_2}{g_2} = \frac{f_1 f_2}{g_1 g_2}$$

respectivamente.

Nosso objetivo nesta seção é mostrar que é possível decompor funções racionais de uma variável como somas de outras mais simples. Começamos

com um exemplo, para relembrar a técnica de frações parciais que todos aprendemos no primeiro curso de cálculo. Dada a função racional

$$\frac{x^2+2}{x^4+4x^3+5x^2+4x+4} \tag{90}$$

fatoramos o denominador em $\mathbb{R}[x]$ e obtemos

$$x^4+4x^3+5x^2+4x+4 = (x^2+1)(x+2)^2.$$

Tentamos, então, escrever (90) na forma

$$\frac{a_1x+a_2}{x^2+1} + \frac{b}{x+2} + \frac{c}{(x+2)^2}. \tag{91}$$

Expressando esta soma como um quociente de polinômios, vemos que seu numerador é igual a

$$a_1x^3+4a_1x^2+4a_1x+a_2x^2+4a_2x+4a_2+bx^3+2bx^2+bx+2b+cx^2+c$$

Para que (90) e (91) tenham o mesmo numerador, este último polinômio deve ser igual a x^2+2. Igualando os coeficientes, obtemos o sistema linear

$$\begin{aligned} a_1+b &= 0\\ 4a_1+a_2+2b+c &= 1\\ 4a_1+4a_2+b &= 0\\ 4a_2+2b+c &= 2; \end{aligned}$$

que, ao ser resolvido, nos dá

$$\begin{aligned} a_1 &= 4/25\\ a_2 &= 3/25\\ b &= 4/25\\ c &= 6/5. \end{aligned}$$

Logo, a função racional (90) pode ser escrita na forma

$$\frac{1}{25}\left(\frac{4x+3}{x^2+1}\right) + \frac{4}{25}\left(\frac{1}{x+2}\right) + \frac{6}{5}\left(\frac{1}{(x+2)^2}\right). \tag{92}$$

Nossa meta consiste em (1) mostrar que uma decomposição deste tipo existe para toda função racional e (2) utilizar os algoritmos já estabelcidos para polinômios, a fim de dar um procedimento melhor para o cálculo desta decomposição. Trataremos (1) e (2) simultaneamente, subdividindo o processo de decomposição em várias etapas.

Sejam f e $g \neq 0$ polinômios em $K[x]$, e consideremos a função racional f/g. Dividindo f por g, obtemos

$$f = gq + r \quad \text{em que} \quad r = 0 \quad \text{ou} \quad \operatorname{grau}(r) < \operatorname{grau}(g).$$

Assim,

$$\frac{f}{g} = \frac{gq+r}{g} = q + \frac{r}{g}.$$

Com isto, podemos restringir a aplicação do processo de decomposição a uma função racional cujo numerador tem grau menor que seu denominador.

Reciclando a notação anterior, suporemos agora que f e g são polinômios em $K[x]$ tais que $\mathrm{grau}(f) < \mathrm{grau}(g)$. O próximo passo consiste em fatorar g de modo a obter

$$g = p_1^{e_1} \cdots p_k^{e_k},$$

em que os ps são polinômios irredutíveis de $K[x]$ e os es são inteiros positivos. Defina

$$c_j = \frac{g}{p_j^{e_j}}.$$

Como $p_j^{e_j}$ divide g, a função racional c_j é igual ao polinômio

$$p_1^{e_1} \cdots p_{j-1}^{e_{j-1}} \cdot p_{j+1}^{e_{j+1}} \cdots p_k^{e_k}.$$

Em outras palavras, c_j é o produto de todos os $p_i^{e_i}$ para os quais $i \neq j$. Como p_j não divide c_j, temos que

$$\mathrm{mdc}(c_1, \ldots, c_k) = 1.$$

Aplicando o algoritmo euclidiano estendido aos cs, determinamos polinômios $h_1, \ldots, h_k \in K[x]$ tais que

$$h_1 c_1 + \cdots + h_k c_k = 1.$$

Portanto,

$$\frac{1}{g} = \frac{h_1 c_1 + \cdots + h_k c_k}{p_1^{e_1} \cdots p_k^{e_k}}.$$

Levando em conta a definição dos cs e efetuando os devidos cancelamentos

$$\frac{1}{g} = h_1 \frac{1}{p_1^{e_1}} + \cdots + h_k \frac{1}{p_k^{e_k}}.$$

Multiplicando tudo isto por f,

$$\frac{f}{g} = \frac{f h_1}{p_1^{e_1}} + \cdots + \frac{f h_k}{p_k^{e_k}}.$$

Vejamos o que ocorre se aplicarmos esta estratégia à função racional (90), que podemos reescrever como

$$\frac{x^2 + 2}{(x^2 + 1)(x + 2)^2}.$$

Neste caso,

$$p_1 = x^2 + 1 \quad \text{e} \quad p_2 = x + 2,$$

ao passo que $e_1 = 1$ e $e_2 = 2$. Logo,

$$c_1 = p_2^2 \quad \text{e} \quad c_2 = p_1.$$

Aplicando o algoritmo euclidiano estendido, obtemos

$$h_1 = \frac{4}{25}x + \frac{13}{25} \quad \text{e} \quad h_2 = -\frac{4}{25}x + \frac{3}{25}.$$

Portanto,

$$\frac{x^2+2}{(x^2+1)(x+2)^2} = \frac{1}{25}\left(\frac{(x^2+2)(-4x+3)}{x^2+1}\right)+\frac{1}{25}\left(\frac{(x^2+2)(4x+13)}{(x+2)^2}\right).$$

Observe que o numerador de ambas as frações são maiores que 2, que é o grau do numerador em ambos os casos. Isto significa que podemos efetuar uma divisão e reduzir cada uma das frações parciais obtidas um pouco mais. Fazendo isto, obtemos

$$\frac{(x^2+2)(4x+13)}{x^2+1} = -4x+3+\frac{-4x+3}{x^2+1}$$

ao passo que

$$\frac{(x^2+2)(4x+3)}{(x+2)^2} = 4x-3+\frac{4x+38}{(x+2)^2}.$$

Somando os dois, e multiplicando tudo pela constante $1/25$,

$$\frac{x^2+2}{(x^2+1)(x+2)^2} = \frac{1}{25}\left(\frac{-4x+3}{x^2+1}+\frac{4x+38}{(x+2)^2}\right); \tag{93}$$

já que as parcelas que são polinômios se cancelam mutuamente. Observe que esta decomposição não é igual à que foi obtida em (92). Isto significa que deve ser possível decompor a segunda parcela do lado direito um pouco mais. Antes de prosseguir, convém enunciar o algoritmo obtido até aqui.

ALGORITMO 10.1. *Dados polinômios f e g em $K[x]$, o algoritmo calcula uma decomposição em frações parciais de f/g.*

Etapa 1: *Fatore g em $K[x]$ para obter*

$$g = p_1^{e_1}\cdots p_k^{e_k}.$$

Etapa 2: *Para $1 \leq j \leq k$, faça*

$$c_j = \frac{g}{p_j^{e_j}}.$$

Etapa 3: *Use o algoritmo euclidiano estendido para determinar polinômios $h_1, \ldots, h_k$ tais que*

$$h_1c_1 + \cdots + h_kc_k = 1.$$

Etapa 4: *Para cada $1 \leq j \leq k$, calcule o resto r_i e o quociente q_i da divisão de fh_i por $p_i^{e_i}$.*

Etapa 5: *Retorne a soma*

$$q_1 + \cdots + q_k,$$

que corresponde à parcela polinomial da decomposição, e a lista

$$[r_1, \ldots, r_k]$$

que corresponde aos numeradores das parcelas cujos denominadores são, respectivamente $p_1^{e_1}, \ldots, p_k^{e_k}$.

Reciclando uma última vez a notação, precisamos considerar apenas o caso em que f e g são polinômios em $K[x]$ tais que $g \neq 0$ é irredutível e $\mathrm{grau}(f) < \mathrm{grau}(g^e)$, para algum inteiro positivo e. Inspirados pelo que aprendemos em cálculo esperamos poder escrever f/g^e na forma

$$\frac{f}{g^e} = \sum_{i=0}^{e} \frac{a_i}{g^i}. \tag{94}$$

Note, contudo, que se $\mathrm{grau}(g) > 1$, os a_i poderão ser polinômios não constantes. De fato, em geral $a_i \in K[x]$ satisfaz apenas a condição

$$\mathrm{grau}(a_i) < \mathrm{grau}(g) \quad \text{para todo} \quad 1 \leq i \leq k.$$

Contudo (94) representa uma espécie de expansão de f/g^e em potências negativas de g. Como os expoentes são todos maiores que $-e$, podemos tentar expandir f em potências de g e dividir tudo por g^e. Tomando como ponto de partida o algoritmo usado para converter inteiros para uma base dada, dividimos f por g, obtendo

$$f = q_0 g + r_0, \quad \text{em que} \quad \mathrm{grau}(r_0) < \mathrm{grau}(g).$$

Repetindo o processo com q_0 e g,

$$q_0 = q_1 g + r_1, \quad \text{em que} \quad \mathrm{grau}(r_1) < \mathrm{grau}(g).$$

Substituindo a segunda igualdade na primeira

$$f = (q_1 g + r_1)g + r_0 = q_1 g^2 + r_1 g + r_0.$$

Continuando o processo,

$$f = r_e g^e + \cdots + r_1 g + r_0.$$

Dividindo esta última expressão por g^e,

$$\frac{f}{g^e} = r_e + \cdots + \frac{r_1}{g^{e-1}} + \frac{r_0}{g^e};$$

de modo que $a_i = r_{e-i}$ em (94). Esta maneira de escrever f/g^e é conhecida como sua *decomposição g-ádica*.

Para calcular a decomposição g-ádica de

$$\frac{4x + 38}{(x+2)^2}$$

basta efetuar a divisão de $4x + 38$ por $x + 2$, o que nos dá resto 30 e quociente 4. Assim,

$$\frac{4x + 38}{(x+2)^2} = \frac{4(x+2) + 30}{(x+2)^2};$$

e, após o cancelamento,

$$\frac{4x + 38}{(x+2)^2} = \frac{4}{(x+2)} + \frac{30}{(x+2)^2}.$$

Substituindo em (93),

$$\frac{x^2+2}{(x^2+1)(x+2)^2} = \frac{1}{25}\left(\frac{-4x+3}{x^2+1} + \frac{4}{(x+2)} + \frac{30}{(x+2)^2}\right);$$

que é igual a (92), como esperávamos. O algoritmo para a decomposição g-ádica pode ser descrito da seguinte maneira.

ALGORITMO 10.2. *Dados polinômios $f, g \in K[x]$ e um inteiro positivo e, tais que $g \neq 0$ é irredutível em $K[x]$ e*

$$\text{grau}(f) < \text{grau}(g^e),$$

o algoritmo calcula a decomposição g-ádica de f/g^e.

Etapa 1: *Inicialize $\mathcal{L}$ como a lista vazia e Q com f.*

Etapa 2: *Se $\text{grau}(Q) < \text{grau}(g)$, acrescente Q ao fim da lista, páre e retorne $\mathcal{L}$. Observe que o i-ésimo elemento da lista é o quociente de g^i na decomposição g-ádica de f/g.*

Etapa 3: *Calcule o resto r e o quociente q da divisão de Q por g.*

Etapa 4: *Acrescente r ao fim da lista, faça $Q = q$ e volte à Etapa 2.*

Encerramos esta seção enunciando um teorema que resume tudo o que aprendemos sobre a decomposição de uma função racional em frações parciais.

TEOREMA 10.3. *Sejam f e $g \neq 0$ polinômios em $K[x]$. Se*

$$g = p_1^{e_1} \cdots p_k^{e_k}.$$

é a fatoração de g em irredutíveis, então podemos escrever

$$\frac{f}{g} = q + \sum_{j=1}^{k} \frac{h_j}{p_j^{e_j}},$$

em que $q \in K[x]$ e cada $h_j \in K[x]$ tem grau menor que $p_j^{e_j}$. Além disso, existem polinômios r_{ij} de grau menor que p_j tais que

$$\frac{h_j}{p_j^{e_j}} = \sum_{i=1}^{e_j} \frac{r_{ij}}{p_j^i}.$$

2. Bernoulli

Antes de mais nada, uma observação sobre notação. Ao longo de todo o capítulo, usaremos tanto df/dx, quanto f', para denotar a derivada de uma função f, na variável x.

Podemos escrever uma função racional $f \in \mathbb{R}(x)$ na forma $f = N/D$, em que $N, D \in \mathbb{R}[x]$ e $D \neq 0$. Se N tem grau maior do que D, podemos dividi-los obtendo

$$N = DQ + R, \text{ em que } R = 0 \text{ ou } \text{grau}(R) < \text{grau}(D).$$

Assim,

$$f = \frac{N}{D} = \frac{DQ+R}{D} = Q + \frac{R}{D},$$

de forma que

$$\int f dx = \int Q dx + \int \frac{R}{D} dx.$$

Como Q é um polinômio, não há dificuldade em integrá-lo. Portanto, para obter a integral de f basta integrar R/D quando R tem grau menor que D.

Para isto, começamos fatorando D. Como estamos trabalhando com funções reais, a fatoração terá que ser sobre $\mathbb{R}[x]$. Portanto, esperamos encontrar entre os fatores de D polinômios de grau um ou dois, já que estas são as únicas possibilidades quando o polinômio é irredutível sobre $\mathbb{R}$. Digamos que

$$D = (x-\alpha_1)^{r_1} \cdots (x-\alpha_m)^{r_m} (x^2 + a_1 x + b_1)^{s_1} \cdots (x^2 + a_n x + b_n)^{s_n}.$$

A partir desta fatoração podemos escrever a decomposição em frações parciais de R/D. As parcelas nesta decomposição são de dois tipos, dependendo do seu denominador. Para os fatores de grau um temos parcelas da forma

$$\frac{c_{ik}}{(x-\alpha_i)^k} \text{ em que } 1 \leq k \leq r_i \text{ e } c_{ik}, \alpha_i \in \mathbb{R}.$$

Já os fatores de grau dois dão origem a parcelas do tipo

$$\frac{d_{ik}x + c_{i\ell}}{(x^2 + a_i x + b_i)^\ell} \text{ em que } 1 \leq \ell \leq s_i \text{ e } d_{ik}, c_{ik}, a_i, b_i \in \mathbb{R}.$$

Antes de prosseguir, vejamos um exemplo. Seja

$$f = \frac{x^2+3}{x^6 - 3x^2 - 2}. \tag{95}$$

Como o numerador de f já tem grau menor que o seu denominador, não precisamos efetuar nenhuma divisão. Passamos, assim, diretamente à fatoração do denominador, que é

$$x^6 - 3x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})(x^2+1)^2.$$

A decomposição em frações parciais correspondente será

$$\frac{5\sqrt{2}}{36}\left(\frac{1}{x-\sqrt{2}} - \frac{1}{x+\sqrt{2}}\right) - \frac{5}{9}\left(\frac{1}{x^2+1}\right) - \frac{2}{3}\left(\frac{1}{(x^2+1)^2}\right).$$

Voltemos ao caso geral, analisado acima. Tendo em mãos a decomposição em frações parciais de R/Q basta integrá-la termo a termo. Portanto, reduzimos o problema à integração das funções racionais dos seguintes tipos

$$\frac{1}{(x-\alpha)^k} \text{ e } \frac{ax+b}{(x^2+\alpha x+\beta)^2},$$

em que a, b, α e β são números reais, e $k \geq 2$ é um inteiro positivo. Trataremos cada um destes casos separadamente. Em primeiro lugar, uma simples integração por substituição nos dá

$$\int \frac{dx}{(x-\alpha)^k} = \begin{cases} -\frac{(x-\alpha)^{1-k}}{k-1} & \text{se } k > 1 \\ \log(x-\alpha) & \text{se } k = 1. \end{cases} \tag{96}$$

Passando ao segundo caso, precisamos integrar

$$\int \frac{ax+b}{(x^2+\alpha x+\beta)^k}dx,$$

para $k \geq 1$. Para simplificar a notação, denotaremos o numerador por f e o denominador por g. Então, $g' = 2x + \alpha$, de modo que

$$f = ax + b = \frac{a}{2}g' + b - \frac{a}{2}.$$

Portanto,

$$\int \frac{f}{g^k}dx = \frac{a}{2}\int \frac{g'}{g^k}dx + \left(b - \frac{a}{2}\right)\int \frac{1}{g^k}dx.$$

Contudo,

$$\int \frac{g'}{g^k}dx = \begin{cases} \log g & \text{se } \ k = 1 \\ \frac{1}{(1-k)}g^{1-k} & \text{se } \ k \geq 2. \end{cases}$$

Assim, basta calcular

$$\int \frac{1}{g^k}dx$$

para encerrar o problema. Mas, completando quadrados em g, obtemos

$$g = \left(x + \frac{\alpha}{2}\right)^2 + \beta - \frac{\alpha^2}{4}.$$

Fazendo, agora, a mudança de variáveis

$$x = \left(\frac{4\beta - \alpha^2}{4}\right)^{-1/2}(y - \alpha/2),$$

a integral se reescreve como

$$\int \frac{1}{g^k}dx = \left(\frac{4}{4\beta - \alpha^2}\right)^{k/2}\int \frac{1}{(y^2+1)^k}dy,$$

o que reduz o problema à integração de $1/(y^2+1)^k$.

Fazemos esta integração em duas etapas: reduzimos, recursivamente, ao caso $k = 1$ e, então, calculamos este caso explicitamente. Porém,

$$\frac{d}{dy}(\arctan y) = \frac{1}{1+y^2}, \tag{97}$$

de forma que

$$\int \frac{1}{y^2+1}dy = \arctan y, \tag{98}$$

resolvendo assim o caso $k = 1$. Para obter a fórmula de redução, integramos $1/(y^2+1)^{k-1}$ por partes, o que nos dá

$$\int \frac{1}{(y^2+1)^{k-1}}dy = \frac{y}{(y^2+1)^{k-1}} + 2(k-1)\int \frac{y^2}{(y^2+1)^k}dy. \tag{99}$$

Somando e subtraindo 1 do numerador y^2, e efetuando os cancelamentos necessários, temos que

$$\int \frac{y^2 dy}{(y^2+1)^k} = \int \frac{dy}{(y^2+1)^{k-1}} - \int \frac{dy}{(y^2+1)^k} dy.$$

Substituindo em (99),

$$\int \frac{dy}{(y^2+1)^{k-1}} = \frac{y}{(y^2+1)^{k-1}} + \int \frac{2(k-1)dy}{(y^2+1)^{k-1}} - \int \frac{2(k-1)dy}{(y^2+1)^k}.$$

Resolvendo para a integral de $1/(y^2+1)^k$, obtemos a fórmula de redução desejada

$$\int \frac{dy}{(y^2+1)^k} = \frac{y}{2(k-1)(y^2+1)^{k-1}} + \frac{2k-3}{2(k-1)} \int \frac{dy}{(y^2+1)^{k-1}}.$$

Ao invés de substituir estas equações umas nas outras para obter uma fórmula recursiva geral de redução, é preferível efetuar as substituições uma a uma à medida que o processo vai sendo realizado. Desta forma é mais fácil acompanhar a mecânica do procedimento. Vamos aplicar este método à integral da função f definida em (95). Usando a decomposição em frações parciais, vemos que f tem como primitiva

$$\frac{5\sqrt{2}}{36}\left(\int \frac{dx}{x-\sqrt{2}} - \int \frac{dx}{x+\sqrt{2}}\right) - \frac{5}{9}\int \frac{dx}{x^2+1} - \frac{2}{3}\int \frac{dx}{(x^2+1)^2}. \tag{100}$$

Cada uma destas integrais será calculada separadamente, usando o algoritmo de Bernoulli, como o descrevemos acima. Em primeiro lugar,

$$\int \frac{1}{x-\sqrt{2}} dx = \log(x-\sqrt{2}) \text{ e } \int \frac{1}{x+\sqrt{2}} dx = \log(x+\sqrt{2}), \tag{101}$$

não oferecem nenhuma dificuldade. Já a terceira integral é calculada usando (98),

$$\int \frac{1}{x^2+1} dx = \arctan(x).$$

Usando a fórmula de redução na última integral da equação (100),

$$\int \frac{dx}{(x^2+1)^2} = \frac{1}{2}\int \frac{dx}{(x^2+1)} + \frac{x}{2(x^2+1)} = \frac{1}{2}\left(\arctan x + \frac{x}{(x^2+1)}\right).$$

Substituindo tudo de volta na integral original e efetuando as reduções necessárias, obtemos a seguinte primitiva para f,

$$\frac{5\sqrt{2}}{36}\left(\log(x-\sqrt{2}) - \log(x+\sqrt{2})\right) - \frac{8}{9}\arctan(x) - \frac{1}{3}\frac{x}{(x^2+1)}.$$

Finalmente, as propriedades dos logaritmos, nos permitem escrever esta função na forma

$$\int \frac{x^2+3}{x^6-3x^2-2} dx = \frac{5\sqrt{2}}{36}\log\left(\frac{x-\sqrt{2}}{x+\sqrt{2}}\right) - \frac{8}{9}\arctan(x) - \frac{1}{3}\frac{x}{(x^2+1)}.$$

Uma maneira de evitar a fórmula de redução é admitir funções de variável complexa. Se fizermos isto, a primeira coisa a ser simplificada é a decomposição de f em frações parciais, que passa a ser

$$\frac{5\sqrt{2}}{36}\left(\frac{1}{x-\sqrt{2}}-\frac{1}{x+\sqrt{2}}\right)+\frac{4}{9}\left(\frac{i}{x-i}-\frac{i}{x+i}\right)+\frac{1}{6}\left(\frac{1}{(x-i)^2}+\frac{1}{(x+i)^2}\right).$$

Neste caso podemos usar o equivalente da fórmula (96) para cada uma das parcelas. Fazendo isto, e agrupando os logaritmos, obtemos a seguinte primitiva para f,

$$\frac{5\sqrt{2}}{36}\log\left(\frac{x-\sqrt{2}}{x+\sqrt{2}}\right)+\frac{4}{9}i\log\left(\frac{x-i}{x+i}\right)-\frac{1}{6}\left(\frac{1}{(x-i)}+\frac{1}{(x+i)}\right).$$

Como você vê, não há nenhum arco tangente à vista! Contudo, a integral de uma função real acabou dando uma função complexa, o que não é muito agradável. Contudo, se as duas fórmulas que obtivemos para a primitiva de f estão corretas, então devem diferir apenas por uma constante; e é isto que mostraremos a seguir.

Para tal precisamos apenas considerar o que ocorre com as três últimas parcelas, já que a primeira coincide nas duas fórmulas. Contudo,

$$\frac{1}{(x-i)}+\frac{1}{(x+i)}=\frac{2x}{(x^2+1)},$$

de forma que o problema se reduz a expressar

$$\log\left(\frac{x-i}{x+i}\right)$$

em termos de arcos tangentes. Para isto, podemos usar o seguinte lema.

LEMA 10.4. *Se $g\in\mathbb{R}(x)$ e $g^2\neq -1$, então*

$$i\frac{d}{dx}\log\left(\frac{g+i}{g-i}\right)=2\frac{d}{dx}\arctan(g).$$

DEMONSTRAÇÃO. Derivando $\log(g-i/g+i)$ em relação a x, obtemos

$$\frac{g-i}{g+i}\cdot\frac{g'(g-i)-g'(g+i)}{(g-i)^2}=2i\frac{g'}{g^2+1}.$$

Portanto,

$$i\frac{d}{dx}\log\left(\frac{g+i}{g-i}\right)=\frac{2g'}{g^2+1},$$

que, por sua vez, é igual à derivada de $2\arctan(g)$, pela regra da cadeia. □

Aplicando o lema, vemos que, a menos de uma constante, a função

$$i \log(x - i/x + i)$$

é igual a $2 \arctan(x)$. Juntando tudo o que fizemos, concluímos que

$$\int f dx = \frac{5\sqrt{2}}{36} \log\left(\frac{x - \sqrt{2}}{x + \sqrt{2}}\right) - \frac{8}{9} \arctan(x) - \frac{1}{6} \frac{2x}{(x^2 + 1)},$$

que é igual ao resultado obtido pelo método de Bernoulli. Na prática, é desta última maneira que vamos proceder. Isto é, faremos a integração em termos de logaritmos, admitindo argumentos e coeficientes complexos, se necessário. Ao final, converteremos o resultado em uma função real usando o lema 10.4. Como veremos, isto pode causar alguns problemas; mas tudo a seu tempo.

Encerramos esta seção enunciando o teorema que resulta de nossa excursão pelos números complexos. Para prová-lo, basta calcular, termo a termo, as primitivas da decomposição em frações parciais sobre $\mathbb{C}$ do integrando.

TEOREMA 10.5. *Sejam N e D polinômios com coeficientes reais e tais que $\operatorname{grau}(N) < \operatorname{grau}(D)$ e seja*

$$D = (x - \alpha_1)^{e_1} \cdots (x - \alpha_d)^{e_d},$$

em que $\alpha_1, \ldots, \alpha_d$ são complexos distintos, e $e_1, \ldots, e_d$ são inteiros positivos. Então

$$\int \frac{N}{D} dx = g + \sum_{i=1}^{d} c_i \log(x - \alpha_i),$$

em que $g \in \mathbb{R}(x)$ e $c_i \in \mathbb{C}$, para $1 \leq i \leq d$. Além disso, $g = 0$ caso $e_i = 1$ para todo $1 \leq i \leq d$.

DEMONSTRAÇÃO. A decomposição em frações parciais de N/D será uma soma de termos da forma

$$\frac{c}{(x - \alpha)^k},$$

em que $c, \alpha \in \mathbb{C}$ e $k > 0$ é um número inteiro. Pela fórmula (96), a integral desta função racional será outra função racional se $k > 1$. Caso contrário, a integral será um logaritmo. Como a fórmula geral segue da integração de cada parcela da decomposição em frações parciais, o teorema esta provado. □

3. Funções elementares

Como consequência do algoritmo de Bernoulli, temos que a integral de qualquer função racional com coeficientes reais pode ser escrita como a soma de funções racionais, logaritmos e arcos tangentes. Estas três são típicas representantes das funções tradicionalmente estudadas nos cursos de cálculo, e que chamamos de funções elementares. Como vamos usar este conceito de maneira sistemática, é conveniente defini-lo de maneira mais precisa.

Uma função de uma variável é *elementar* se pode ser escrita a partir das funções

- racionais;
- algébricas;
- trigonométricas diretas e inversas;
- exponenciais e logaritmos;

pela aplicação recursiva das operações de adição, subtração, multiplicação, divisão e composição de funções.

Das quatro categorias básicas de funções, apenas a segunda precisa de esclarecimentos adicionais. Dizemos que uma função f na variável (real) x é *algébrica* se existe um polinômio irredutível $G(x, y) \in \mathbb{R}[x, y]$ tal que

$$G(x, f(x)) = 0,$$

para todo x no domínio de f. Por exemplo, $\sqrt{x}$ é algébrica, já que satisfaz o polinômio irredutível $F(x, y) = y^2 - x$. As funções racionais também são algébricas. De fato, se $p, q \in \mathbb{R}[x]$ e $q \neq 0$, então a função racional p/q satisfaz o polinômio $p - qy$. Em particular, vemos que as classes de funções básicas que aparecem na definição de funções elementares não são mutuamente exclusivas. Com um pouco de esforço (que não faremos aqui) pode-se mostrar que:

> toda função construída a partir das quatro operações aritméticas elementares, da extração de raízes e da composição de funções, é algébrica.

Contudo, a recíproca desta afirmação é falsa.

Por outro lado, nem todas as funções são algébricas, um fato que já havia sido notado por I. Newton. O que Newton observou é que toda função algébrica satisfaz a seguinte propriedade.

PROPOSIÇÃO 10.6. *Se o gráfico de uma função algébrica corta uma reta do plano em uma quantidade infinita de pontos, então o gráfico é a própria reta.*

DEMONSTRAÇÃO. Seja f uma função algébrica e $G \in \mathbb{R}[x, y]$ um polinômio irredutível tal que $G(x, f(x)) = 0$ para todo ponto do domínio de f. Digamos que r é uma reta do plano que intersecta o gráfico de f em uma infinidade de pontos. Note que r não pode ser uma reta vertical porque o gráfico de uma função não corta nenhuma reta vertical em mais de um ponto. Assim, podemos supor que r tem equação $y = ax + b$, em que $a, b \in \mathbb{R}$.

Considere, agora, um ponto de abscissa x_0 que esteja na interseção do gráfico de f com a reta r. Para que isto ocorra, devemos ter que $f(x_0) = ax_0 + b$, donde

$$G(x_0, ax_0 + b) = 0.$$

Em outras palavras, x_0 é raiz do polinômio de uma variável $q(t) = G(t, at+b)$. Se há infinitos pontos de interseção, então q tem infinitas raízes. Mas isto só pode ocorrer se q for identicamente nulo. Neste caso, dividindo G por $y - ax - b$, obtemos

$$G = Q \cdot (y - ax - b) + R, \text{ em que } Q, R \in \mathbb{R}[x, y].$$

Note que esta divisão é possível porque $y - ax - b$ é mônico como polinômio em y.

Contudo, como o resto R é um polinômio cujo grau em y é menor que o de $y - ax - b$, concluímos que R contém apenas a variável x. Substituindo $y = ax + b$ na equação acima, e levando em conta que $G(x, ax + b) = 0$, verificamos que $R = 0$. Portanto,

$$G = Q \cdot (y - ax - b),$$

o que contradiz o fato de G ser irredutível, a não ser que $G = y - ax - b$. Mas, neste último caso, a função f é a prórpria reta como pretendíamos provar. □

Usando esta proposição, verificamos que uma função periódica, como o seno ou o cosseno, não pode ser algébrica, já que seu gráfico corta alguma reta horizontal em uma infinidade de pontos. Uma função que não é algébrica é conhecida como *transcendente*. As funções exponencial e logaritmo também são transcendentes. Contudo, como não são periódicas, não podemos provar isto usando a proposição 10.6. Para uma demonstração da transcendência da exponencial, do logaritmo, e de outras funções correlatas, veja [**34**, p. 44, §16]. Observe as funções transcendentes estão para as funções algébricas assim como os números transcendentes estão para os números algébricos!

Voltando ao que dizíamos no início da seção, segue do algoritmo de Bernoulli que a primitiva de uma função racional pode ser escrita como soma de uma função racional (e, portanto, algébrica) com arcos tangentes e logaritmos (que são transcendentes). Isto sugere a pergunta

> é possível reformular a parte transcendente da integral, total ou parcialmente, usando funções racionais?

A resposta é não, mas prová-la requer técnicas que estão além dos limites deste livro. Por isso vamos nos contentar em mostrar que a parte transcendente não pode ser *igual* a nenhuma função racional. Um tratamento completo desta questão pode ser encontrado em [REF].

PROPOSIÇÃO 10.7. *Sejam α_i e c_i números complexos, $1 \leq i \leq d$. Se os α_i são todos distintos e $\sum_{i=1}^{d} c_i \log(x - \alpha_i)$ é uma função racional, então $c_i = 0$ para todo $1 \leq i \leq d$.*

DEMONSTRAÇÃO. Suponhamos, por contradição, que

$$\sum_{i=1}^{d} c_i \log(x - \alpha_i) = p/q,$$

em que $p, q \in \mathbb{C}[x]$ e $\mathrm{mdc}(p, q) = 1$. Derivando ambos os lados, temos que

$$\sum_{i=1}^{d} \frac{c_i}{x - \alpha_i} = \frac{p'q - pq'}{q^2}. \tag{102}$$

Digamos que $(x-\beta)$ é um fator cuja multiplicidade na fatoração de q é r. Logo a multiplicidade de $x - \beta$ na fatoração de q' é $r - 1$. Portanto, como p e q são primos entre si, a maior potência de $x - \beta$ que divide $p'q - pq'$ é $(x - \beta)^{r-1}$.

Assim, expressando o lado direito da equação (102) em forma reduzida, vemos que seu denominador contém um fator $(x-\beta)^{r+1}$, obtido do cancelamento do $(x-\beta)^{r-1}$ do numerador, com o $(x-\beta)^{2r}$ do denominador. Contudo, expressando o lado esquerdo de (102) em forma reduzida, não encontramos nenhum fator com multiplicadade superior a um. Portanto, $r+1=1$, donde $r=0$. Mas isto significa que q é constante e podemos absorvê-lo no p. Fazendo isto (102) se reduz a

$$\sum_{i=1}^{d} \frac{c_i}{x-\alpha_i} = p'.$$

Multiplicando ambos os lados desta equaÇão por $(x-\alpha_k)$, para algum $1 \leq k \leq d$,

$$c_k + \sum_{i \neq k} \frac{c_i(x-\alpha_k)}{x-\alpha_i} = p'(x-\alpha_k).$$

Mas, fazendo $x=\alpha_k$ nesta expressão, obtemos $c_k=0$. Como isto vale para todo $1 \leq k \leq d$, a demonstração está completa. □

Com o que vimos até agora, o resultado do algoritmo de Bernoulli pode ser reformulado como a afirmação de que a integral de uma função racional consiste de duas partes. A parte algébrica, que é uma função racional, e a parte transcendente, que é uma soma de logaritmos e arcos tangentes. Nas próximas três seções estudaremos algoritmos eficientes que nos permitirão calcular cada uma destas partes.

4. Hermite

Embora o procedimento de Bernoulli nos dê um algoritmo, ele é pouco eficiente, já que demanda uma fatoração completa do denominador sobre $\mathbb{R}$. Entretanto, como C. Hermite observou em 1872, é possível obter a parte racional da integral de $f \in \mathbb{R}(x)$, e o integrando da parte transcendente, sem que seja necessário fatorar o denominador de f em termos de seus fatores *irredutíveis*. O procedimento originalmente proposto por Hermite começa por calcular a decomposição em frações parciais que resulta da fatoração livre de quadrados do denominador; veja página 261.

Seja K um subcorpo efetivo de $\mathbb{C}$. Na prática estaremos interessados no caso em que $K=\mathbb{Q}$. Retomando a notação do início da seção, digamos que

$$f = N/D, \text{ com } N, D \in K[x] \text{ e } \operatorname{grau}(N) < \operatorname{grau}(D).$$

Observe que, desta vez, estamos assumindo que tanto o numerador quanto o denominador de f têm coeficientes no corpo K. Ao invés de fatorar D completamente, calcularemos apenas sua fatoração livre de quadrados, definida na seção 6 do capítulo 9. Seja

$$D = D_1 D_2^2 \cdots D_m^m$$

esta decomposição. Lembre-se que isto significa que D_i é o produto de todos os fatores irredutíveis, de multiplicidade i, na fatoração de D. Além disso,

sabemos do algoritmo 9.19 da página 263, que esta fatoração pode ser obtida calculando apenas com elementos do corpo K.

Se $m = 1$, então D tem apenas fatores com multiplicidade um e, pelo teorema 10.5, sua integral é uma soma de logaritmos. Nossa meta é reduzir, passo a passo, a integral de N/D ao cálculo da primitiva de uma função racional cujo denominador é livre de quadrados. A cada passo a integral é reescrita como uma soma de duas parcelas. A primeira é uma função racional, ao passo que a segunda é a primitiva de uma outra função racional. Entretanto, esta nova função da qual ainda precisaremos achar a primitiva terá um denominador cuja multiplidade máxima, como definida na página 263, é *menor* que a do passo anterior. O processo termina quando a função racional que ainda falta integrar tem denominador livre de quadrados. Neste estágio teremos obtido

$$\int \frac{N}{D} dx = Q + \int \frac{\hat{N}}{\hat{D}},$$

em que $Q \in K(x)$ e $\hat{D}$ é livre de quadrados. A primitiva de $\hat{N}/\hat{D}$ corresponde à parte transcendente da integral de N/D, ao passo que Q nos dá sua parte racional. Portanto, o algoritmo que estamos prestes a descrever nos dará

- a parte racional da integral de N/D;
- a função racional cuja integral corresponde à parte transcendente da integral de N/D.

Continuando a assumir que a função a ser integrada é N/D e que

$$D = D_1 D_2^2 \cdots D_m^m$$

é a decomposição livre de quadrados do seu denominador. Seja

$$U = \frac{D}{D_m^m} = D_1 D_2^2 \cdots D_{m-1}^{m-1}.$$

Como $\mathrm{mdc}(D_i, D_m) = 1$, para todo $1 \leq i \leq m-1$, e como D_m não tem quadrados, podemos concluir que D_m e

$$U(D_m)' = D_1 D_2^2 \cdots D_{m-1}^{m-1} D_m'$$

têm que ser primos entre si. Portanto, pelo algoritmo euclidiano estendido, podemos calcular polinômios α_0 e β_0, tais que

$$\alpha_0 U D_m' + \beta_0 D_m = 1.$$

Multiplicando ambos os membros desta equação por N,

$$(N\alpha_0) U D_m' + (N\beta_0) D_m = N.$$

Entretanto, precisamos de cuidados extra para garantir que, ao final de um passo da redução, o numerador do integrando tenha grau menor que seu denominador. Para isso, dividimos $N\alpha_0$ por D_m, obtendo r como resto e q como divisor. Desta forma,

$$N = (N\alpha_0) U D_m' + (N\beta_0) D_m = r U D_m' + (N\beta_0 + q U D_m') D_m.$$

Portanto, fazendo

$$\alpha = r \quad \text{e} \quad \beta = N\beta_0 + qUD'_m$$

temos que

$$\alpha UD'_m + \beta D_m = N \text{ com } \operatorname{grau}(\alpha) < \operatorname{grau}(D_m), \tag{103}$$

já que α é o resto (não nulo) de uma divisão por D_m. Com isto,

$$(m-1)\frac{N}{D} = (m-1)\left(\frac{\alpha UD'_m + \beta D_m}{UD_m^m}\right);$$

donde,

$$(m-1)\frac{N}{D} = \frac{(m-1)\alpha D'_m}{D_m^m} + \frac{(m-1)\beta}{UD_m^{m-1}}.$$

Substituindo, agora,

$$\frac{d}{dx}\left(\frac{\alpha}{D_m^{m-1}}\right) = \frac{\alpha'}{D_m^{m-1}} - \frac{(m-1)\alpha D'_m}{D_m^m}.$$

na equação anterior, obtemos

$$(m-1)\frac{N}{D} = \left(\frac{\alpha'}{D_m^{m-1}} - \frac{d}{dx}\left(\frac{\alpha}{D_m^{m-1}}\right)\right) + \frac{(m-1)\beta}{UD_m^{m-1}}.$$

Desta forma,

$$(m-1)\frac{N}{D} = \frac{\alpha' U + (m-1)\beta}{UD_m^{m-1}} - \frac{d}{dx}\left(\frac{\alpha}{D_m^{m-1}}\right).$$

Assim,

$$\int \frac{N}{D}dx = \frac{1}{m-1}\left(\int \frac{\alpha' U + (m-1)\beta}{UD_m^{m-1}}dx\right) - \frac{\alpha}{D_m^{m-1}}.$$

Como,

$$UD_m^{m-1} = D_1 D_2^2 \cdots (D_{m-1}D_m)^{m-1},$$

sua multiplicidade máxima é

$$\mu(UD_m^{m-1}) = m-1,$$

como queríamos.

Ainda precisamos nos certificar de que o numerador $\alpha' U + (m-1)\beta$ tem grau menor que o denominador UD_m^{m-1}. Contudo, de (103), temos que

$$\operatorname{grau}(\beta D_m) \leq \max\{\operatorname{grau}(\alpha UD'_m), \operatorname{grau}(N)\}.$$

Mas,

$$\operatorname{grau}(\alpha UD'_m) = \operatorname{grau}(\alpha) + \operatorname{grau}(U) + \operatorname{grau}(D'_m)$$

Porém, $\operatorname{grau}(\alpha) < \operatorname{grau}(D_m)$ e $m \geq 2$, de forma que

$$\operatorname{grau}(\alpha UD'_m) < \operatorname{grau}(UD_m^2) - 1 < \operatorname{grau}(UD_m^m).$$

Como N também tem grau menor que $D = UD_m^m$,

$$\operatorname{grau}(\beta D_m) \leq \operatorname{grau}(D).$$

Portanto,

$$\text{grau}(\beta) \leq \text{grau}(D) - \text{grau}(D_m) < \text{grau}(UD_m^{m-1}),$$

Finalmente,

$$\text{grau}(\alpha' U + (m-1)\beta) \leq \max\{\text{grau}(\alpha') + \text{grau}(U), \text{grau}(\beta)\},$$

e levando em conta a desigualdade para o grau de α mais uma vez, obtemos

$$\text{grau}(\alpha' U + (m-1)\beta) < \max\{\text{grau}(UD_m), \text{grau}(UD_m^{m-1})\};$$

donde

$$\text{grau}(\alpha' U + (m-1)\beta) < \text{grau}(UD_m^{m-1}),$$

como precisávamos mostrar.

O algoritmo que resulta do processo de redução descrito acima pode ser formulado da seguinte maneira.

ALGORITMO 10.8 (Algoritmo de Hermite). *Dada uma função racional $f = N/D$, com $N, D \in K[x]$ e $\text{grau}(N) < \text{grau}(D)$ o algoritmo calcula a parte racional da primitiva de N/D, juntamente com o integrando da parte transcendente.*

Etapa 1: *Inicialize $R = 0$ e $j = m$.*

Etapa 2: *Calcule a fatoração livre de quadrados de $D_1 D_2^2 \cdots D_m^m$ de D e seja $\mathcal{L}$ a lista $[D_1, \ldots, D_m]$.*

Etapa 3: *Enquanto $j > 1$ repita:*

- *se* $\text{grau}(D_j) > 0$,
  - *faça*
    $$V = D_j \text{ e } U = D/V^j.$$
  - *aplique o algoritmo euclidiano estendido a UV' e V, calcule polinômios A e B tais que*
    $$AUV' + BV = 1.$$
  - *calcule o quociente Q da divisão de NA por V e faça*
    $$\alpha = NA - QV$$
    $$\beta = NB + QUV'$$
    $$R = R - \frac{\alpha}{V^{j-1}}$$
    $$N = \alpha' U + (j-1)\beta$$
    $$D = UV^{j-1} \text{ e}$$
- *faça $j = j - 1$;*

Etapa 4: *Imprima R e N/D.*

Resta-nos descrever um exemplo para que você possa ver este algoritmo em ação. Digamos que $N = 1$ e que D corresponde ao polinômio cuja fatoração livre de quadrados é

$$D = (x+1)(x^2+2)^2(x^3+3)^3.$$

Desta forma, no primeiro laço,

$$j = 3,\ V = x^3 + 3 \text{ e } U = (x+1)(x^2+2)^2.$$

Assim, $UV' = 3x^2(x+1)(x^2+2)^2$ e, pelo algoritmo euclidiano estendido

$$A = \frac{5}{5202}x^2 + \frac{67}{5202}x - \frac{3}{578}$$
$$B = -\frac{5}{1734}x^6 - \frac{12}{289}x^5 - \frac{10}{289}x^4 - \frac{41}{289}x^3 + \frac{6}{289}x^2 + \frac{1}{3}$$

Multiplicando por $N = 1$ e dividindo o coeficiente de UV' por V, obtemos

$$\alpha = A \text{ e } \beta = B,$$

donde

$$R = \left(-\frac{5}{10404}x^2 - \frac{67}{10404}x + \frac{3}{1156}\right)/(x^6 + 6x^3 + 9)$$
$$N = -\frac{5}{2601}x^6 - \frac{355}{10404}x^5 - \frac{253}{10404}x^4 - \frac{292}{2601}x^3 + \frac{131}{2601}x^2 + \frac{77}{2601}x + \frac{934}{2601}$$
$$D = (x+1)((x^2+2)(x^3+3))^2.$$

Para o segundo laço, repetimos o processo anterior com os valores de N e D obtidos ao final do primeiro laço. Temos,

$$j = 2,\ V = (x^2+2)(x^3+3) \text{ e } U = (x+1).$$

Assim, $UV' = (5x^4+6x^2+6x)(x+1)$ e, pelo algoritmo euclidiano estendido

$$A = -\frac{65}{10404}x^4 + \frac{50}{2601}x^3 - \frac{1}{306}x^2 + \frac{43}{10404}x + \frac{5}{578}$$
$$B = \frac{325}{10404}x^4 - \frac{75}{1156}x^3 - \frac{545}{5202}x^2 - \frac{5}{578}x + \frac{1}{6}$$

de modo que

$$\alpha = \frac{521}{795906}x^4 + \frac{8423}{795906}x^3 - \frac{689}{93636}x^2 + \frac{22217}{1591812}x - \frac{54}{4913}$$
$$\beta = -\frac{2605}{795906}x^4 - \frac{22360}{397953}x^3 - \frac{21497}{1591812}x^2 + \frac{4225}{265302}x - \frac{467}{7803},$$

donde R tem por numerador

$$-\frac{521}{795906}x^7 - \frac{8423}{795906}x^6 + \frac{689}{93636}x^5 - \frac{6527}{795906}x^4 + \\ - \frac{14431}{530604}x^3 + \frac{185}{7803}x^2 - \frac{29051}{530604}x + \frac{375}{9826}$$

e por denominador $x^8 + 2x^6 + 6x^5 + 12x^3 + 9x^2 + 18$, ao passo que

$$N = -\frac{521}{795906}x^4 - \frac{5789}{265302}x^3 + \frac{5615}{1591812}x^2 + \frac{8047}{530604}x + \frac{117485}{1591812}$$
$$D = (x+1)(x^2+2)(x^3+3).$$

No próximo laço já temos $j = 1$, de forma que a parte racional da integral é dada pelo valor de R acima, e o integrando da parte transcendente é

$$\frac{-\frac{521}{795906}x^4 - \frac{5789}{265302}x^3 + \frac{5615}{1591812}x^2 + \frac{8047}{530604}x + \frac{117485}{1591812}}{(x+1)(x^2+2)(x^3+3)}.$$

5. Rothstein e Trager

Como dissemos ao final da seção 2, determinaremos a parte transcendente da integral de uma função racional em termos de logaritmos. Para isto, precisamos fatorar completamente o denominador da função racional. Contudo, tendo aplicado primeiro o algoritmo de Hermite, podemos assumir que o denominador a ser fatorado é livre de quadrados. Em outras palavras, o denominador se escreve como um produto de termos lineares *distintos*. Entretanto, chegados a este ponto, nos vemos forçados a lidar com números irracionais em nossos procedimentos. Note que isto ocorre mesmo se estivermos supondo que a função racional a ser integrada tem coeficientes em $\mathbb{Q}$.

Infelizmente não há uma maneira geral (e exata) de representar um número irracional no computador. Por outro lado, todos os números irracionais que aparecem nestes algoritmos são algébricos; veja página 215. Isto nos permite chegar a uma solução intermediária, que consiste em não explicitar estes números, mas apenas dizer qual a equação polinomial em $\mathbb{Q}[x]$ que eles satisfazem.

Para poder tornar mais preciso o que precisa ser feito, devemos relembrar o que já sabemos sobre a parte transcendente da integral. Suponha que N e D são polinômios em $K[x]$ que satisfazem

- $\mathrm{grau}(N) < \mathrm{grau}(D)$ e
- D é livre de quadrados.

Neste caso, pelo teorema 10.5,

$$\int \frac{N}{D}dx = \sum_{i=1}^{d} c_i \log(x - \alpha_i),$$

em que os cs e αs são números complexos, e $\alpha_i \neq \alpha_j$ se $i \neq j$. Agrupando os logaritmos que correspondem a um mesmo valor de c, podemos escrever esta soma na forma

$$\int \frac{N}{D}dx = \sum_{i=1}^{s} c_i \log(v_i), \tag{104}$$

em que $s \leq d$, os vs são dois a dois coprimos e os cs são todos distintos.

Note que há s pares da forma (c_i, v_i) que precisamos determinar. A estratégia consistirá em achar um polinômio de $\mathbb{Q}[x]$ cujas raízes são exatamente os cs, e em seguida descrever um procedimento que nos permite calcular o polinômio v correspondente a um dado valor de c. Este é o conteúdo do próximo teorema, que foi provado, independentemente, por M. Rothstein e B. Trager em 1976. Antes, porém, precisamos de um lema auxiliar. Mantendo a notação do início da seção, seja $I(N, D)$ o ideal de $K[x, y]$ gerado por D e por

$N - yD'$. Este lema foi originalmente provado por G. Czichowski em 1995 [**19**, lemma 2.1, p. 164], como parte do trabalho que exporemos na próxima seção. Contudo, antes de poder enunciar o lema precisamos de uma definição. Um ideal de dimensão finita I do anel $K[x_1, \ldots, x_n]$ está em *posição geral* relativamente à variável x_j se quaisquer dois pontos de $\mathcal{Z}(I)$ têm j-ésimas coordenadas distintas.

LEMA 10.9. *Suponha que N e D não são nulos e que satisfazem*

- $\operatorname{grau}(N) < \operatorname{grau}(D)$ *e*
- D *é livre de quadrados.*

Então $I(N, D)$ é um ideal radical de dimensão zero, que está em posição geral com respeito a x.

DEMONSTRAÇÃO. Como estamos supondo que N e D estão fixos, escreveremos I, em lugar de $I(N, D)$, para facilitar a notação. Seja (x_0, y_0) um ponto de $\mathcal{Z}(I)$. Então x_0 é raiz de D e y_0 é raiz de $N(x_0) - y_0 D'(x_0)$. Como D é livre de quadrados, temos que $D'(x_0) \neq 0$. Portanto, para uma dada raiz x_0 de D existe apenas um y_0 que satisfaz $N(x_0) - y_0 D'(x_0) = 0$. Em particular, $\mathcal{Z}_{\mathbb{C}}(I)$ tem exatamente $\operatorname{grau}(D)$ pontos. Mas isto implica que I tem dimensão finita e está em posição geral com respeito a x.

Resta-nos provar que I é radical. Como $\operatorname{mdc}(D, D') = 1$, segue do algoritmo euclidiano estendido que podemos calcular polinômios $\alpha, \beta \in K[x]$ tais que

$$\alpha D + \beta D' = 1.$$

Portanto, substituindo $\beta D'$ por $1 - \alpha D$ em $\beta(N - yD')$, obtemos

$$\beta N - y - y\alpha D = \beta N - y(1 - \alpha D) = \beta(N - yD') \in I.$$

Como $D \in I$, podemos concluir que $\beta N - y \in I$. Mas, o conjunto $G = \{D, \beta N - y\}$ é uma base de Gröbner de I com respeito à ordem lexicográfica para a qual $y > x$.

Seja, agora, $f \in \sqrt{I}$. Dividindo f por G, temos que

$$f - R_G(f) \in \langle G \rangle = I. \tag{105}$$

Além disso, como $\beta N - y \in G$, então $R_G(f) \in K[x]$. Mas f pertence ao radical de I, de modo que se anula em todo ponto de $\mathcal{Z}_{\mathbb{C}}(I)$. Assim, por (105), $R_G(F) \in K[x]$ também se anula em todo ponto de $\mathcal{Z}_{\mathbb{C}}(I)$. Contudo, as abscissas dos pontos de $\mathcal{Z}_{\mathbb{C}}(I)$ são as raízes de D. Como D é livre de quadrados isto nos permite concluir que D divide $R_G(F)$. Logo, $R_G(F) \in I$, e de (105), $f \in I$. Portanto,

$$I \subseteq \sqrt{I} \subseteq I,$$

provando assim que I é radical. □

Seja $r_{N,D}$ o gerador do ideal $I(N, D) \cap K[y]$. Pelo lema 10.9, $I(N, D)$ é um ideal radical de dimensão zero. Logo, $r_{N,D} \neq 0$ pelo corolário 9.10 da página 252.

TEOREMA 10.10. *Sejam N e D polinômios em $K[x]$ que satisfazem*

- $\text{grau}(N) < \text{grau}(D)$ *e*
- D *é livre de quadrados.*

Então,

$$\int \frac{N}{D}dx = \sum_{i=1}^{s} c_i \log(v_i),$$

em que, c_i é raiz de $r_{N,D}$, e $v_i = \text{mdc}(D, N - yD')$ para todo $1 \leq i \leq d$.

DEMONSTRAÇÃO. Como suporemos N e D fixos ao longo de toda a demonstração, escreveremos simplesmente I e r, em lugar de $I(N, D)$ e $r_{N,D}$.

Derivando

$$\int \frac{N}{D}dx = \sum_{i=1}^{s} c_i \log(v_i),$$

obtemos

$$\frac{N}{D} = \sum_{i=1}^{s} c_i \frac{v_i'}{v_i}.$$

Multiplicando esta última equação por $Dv_1 \cdots v_s$, de maneira a eliminar os denominadores,

$$Nv_1 \cdots v_s = D \sum_{i=1}^{s} c_i v_i' u_i, \tag{106}$$

em que

$$u_i = \frac{v_1 \cdots v_s}{v_i},$$

é igual ao produto de todos os vs, exceto v_i. Em particular,

$$\text{mdc}(v_i, u_i) = 1 \text{ para todo } 1 \leq i \leq s.$$

Da maneira como a fórmula (104) foi obtida do teorema 10.5 no início da seção, temos que $D = v_1 \cdots v_s$. Cancelando os termos comuns na equação (106), obtemos

$$N = \sum_{i=1}^{s} c_i v_i' u_i.$$

Assim,

$$N - c_j v_j' u_j = \sum_{i \neq j}^{s} c_i v_i' u_i \in \langle v_j \rangle \tag{107}$$

já que u_i é divisível por v_j, quando $i \neq j$. Como

$$D' = \sum_{i=1}^{s} v_i' u_i$$

podemos concluir que

$$N - c_j D' = (N - c_j v_j' u_j) - c_j \sum_{i \neq j}^{s} v_i' u_i \in \langle v_j \rangle.$$

Portanto,

$$\mathrm{mdc}(N - c_j D', v_j) = v_j. \tag{108}$$

Por outro lado, se $k \neq j$, então da equação (107), temos que

$$N - c_k D' = \sum_{i \neq k}^{s} (c_i - c_k) v_i' u_i = (c_j - c_k) v_j' u_j + \sum_{i \neq j,k}^{s} (c_i - c_k) v_i' u_i.$$

Porém, como o somatório é divisível por v_j,

$$\mathrm{mdc}(N - c_k D', v_j) = \mathrm{mdc}((c_j - c_k) v_j' u_j, v_j) = 1, \tag{109}$$

já que, tanto u_j, como v_j', são primos com v_j.

Como $D = v_1 \cdots v_s$, as equações (108) e (109) nos permitem concluir que

$$\mathrm{mdc}(N - c_j D', D) = v_j,$$

como desejado.

Resta-nos, apenas, mostrar que os cs correspondem às raízes de r. Mas a equação acima é equivalente à igualdade

$$\langle N - c_j D', D \rangle = \langle v_j \rangle,$$

entre ideais de $K[x]$. Portanto, $\alpha \in \mathbb{C}$ é raiz de v_j se, e somente se, $(\alpha, c_j) \in \mathcal{Z}_{\mathbb{C}}(I)$. Desta forma, os c_j são exatamente as ordenadas dos pontos de $\mathcal{Z}_{\mathbb{C}}(I)$; isto é, são as raízes de r. □

Obtemos com isto uma versão do algoritmo de Rothstein-Trager. A versão padrão, implementada em sistemas de computação algébrica como o AXIOM utiliza resultantes, em vez de bases de Gröbner. Veja os exercícios ??? para mais detalhes.

ALGORITMO 10.11 (Algoritmo de Rothstein-Trager). *Dados polinômios N e D em $K[x]$ que satisfazem*

- $\mathrm{grau}(N) < \mathrm{grau}(D)$ *e*
- D *é livre de quadrados.*

o algoritmo calcula pares $(c_j, v_j) \in \mathbb{C} \times \mathbb{C}[x]$, tais que

$$\int \frac{N}{D} dx = \sum_{i=1}^{s} c_i \log(v_i).$$

Etapa 1: *Construa o ideal $I(N, D)$ de $K[x, y]$ gerado por D e $N - yD'$.*

Etapa 2: *Calcule a base de Gröbner de I para a ordem lexicográfica na qual $y < x$ e obtenha o gerador $r = r(y)$ da interseção $I \cap K[y]$.*

Etapa 3: *Para cada raiz c de r, calcule*

$$v_c = \mathrm{mdc}(N - cD', D).$$

Etapa 4: *Imprima cada c com seu respectivo v_c.*

Aplicaremos este algoritmo à integral

$$\int \frac{-\frac{13385}{1591812}x^4 - \frac{38497}{530604}x^3 + \frac{92473}{397953}x^2 + \frac{60551}{530604}x - \frac{59363}{1591812}}{(x+1)(x^2+2)(x^3+3)}\,dx,$$

obtida ao final da seção 4. Neste exemplo, o numerador da função a ser integrada é

$$N = -\frac{13385}{1591812}x^4 - \frac{38497}{530604}x^3 + \frac{92473}{397953}x^2 + \frac{60551}{530604}x - \frac{59363}{1591812}$$

e o denominador é

$$D = (x+1)(x^2+2)(x^3+3).$$

Calculando uma base de Gröbner de $I(N, D)$ com respeito à ordem lexicográfica na qual $y < x$, obtemos o seguinte resultado, um tanto ou quanto espetacular, no qual o primeiro polinômio é $P_1 = x + g(y)$, com g é igual a

$$\frac{7975266246120947698311001756643789581601028217446760337623710360966795264}{307669602885302796876661733242884272282421379398014137541427725}y^5+$$

$$\frac{765395305313612886648476363139179838116753774019139085156479289539706 88}{307669602885302796876661733242884272282421379398014137541427725}y^4+$$

$$\frac{297963599700173653715896025123596983374721482326573080357910654870944}{615339205770605593753323466485768544564842758796028275082855 45}y^3+$$

$$\frac{139400839009874365891929524396968201402788062997238959381494983322 88}{307669602885302796876661733242884272282421379398014137541427725}y^2+$$

$$\frac{954481514113592801113916470127661436889061555945781075091027084 79}{615339205770605593753323466485768544564842758796028275082855450}y+$$

$$-\frac{3263842180464016340216348324695178024080068526626013572883344 62}{307669602885302796876661733242884272282421379398014137541427725},$$

ao passo que o segundo polinômio é

$$P_2 = y^6 - \frac{8917240841513}{52724672145101952}y^4 - \frac{21633427966541}{57654428990668984512}y^3+$$

$$\frac{1699777407653}{819974101200625557504}y^2 - \frac{3306713087191}{298880559887628015710208}y-$$

$$\frac{7211969}{57454932696583624704}$$

O polinômio P_2 pode ser fatorado como

$$\left(y - \frac{1}{72}\right)\left(y^2 - \frac{5122}{751689}y + \frac{1}{36992}\right)$$
$$\left(y^3 + \frac{13833}{668168}y^2 + \frac{2718605}{19727326116}y + \frac{7211969}{21571831107846}\right)$$

Portanto, $c_1 = 1/72$; de modo que

$$v_1 = \mathrm{mdc}(N - \frac{1}{72}D', D) = x + 1.$$

Com isto, uma das parcelas da parte transcendente será igual a

$$\frac{1}{72}\log(x+1).$$

Ao usar o mesmo método para obter as demais parcelas, precisamos calcular máximos divisores comuns de polinômios sobre extensões do tipo $\mathbb{Q}[\alpha]$, em que α é a raiz de um dos outros fatores irredutíveis de r. Isto é possível, como vimos nas seções 6 e 7 do capítulo 8, mas, felizmente, não é necessário. No final da década de 1980, D. Lazard e R. Rioboo [**47**], descobriram um algoritmo capaz de determinar a parte transcendente, sem efetuar cálculos em extensões do corpo de base. Pouco depois, descobriram que B. Trager havia implementado o mesmo algoritmo no sistema de computação algébrica SCRATCHPAD, precursor do atual AXIOM. O algoritmo de Lazard-Rioboo-Trager utiliza resultantes. Entretanto, como veremos na próxima seção, é possível obter resultados semelhantes utilizando bases de Gröbner.

6. Czichowski

O algoritmo que exporemos nesta seção foi originalmente proposto por G. Czichowski em 1995, veja [**19**]. Seu objetivo é utilizar bases de Gröbner para determinar a parte transcendente da integral de uma função racional sem a necessidade de efetuar cálculos sobre extensões do corpo de base. É importante notar que este algoritmo não é mais prático, nem mais rápido, que o algoritmo de Lazard-Rioboo-Trager, mencionado ao final da seção anterior. Contudo, do nosso ponto de vista, tem a vantagem de utilizar os métodos da teoria de bases de Gröbner que estudamos nos capítulos anteriores.

Começamos recordando a notação do início da seção 5, que continuaremos a usar nesta seção: N e D são polinômios em $K[x]$ que satisfazem

- $\mathrm{grau}(N) < \mathrm{grau}(D)$ e
- D é livre de quadrados.

Supondo que N e D estão fixos, denotaremos por I o ideal de $K[x, y]$ gerado por $N - yD'$ e D. Seja G a base de Gröbner reduzida de I relativa à ordem lexicográfica para a qual $x > y$.

Usando o lema 10.9, estabeleceremos algumas propriedades de G. Antes, porém, há um detalhe para o qual convém chamar logo sua atenção. Embora o lema nos diga que I é radical e zero dimensional, não sabemos se está em

posição geral relativamente à y. Se por acaso ele estiver, então podemos deduzir pelo exercício ??? que G tem apenas dois elementos. Embora isto possa, e vá ocorrer em alguns casos, não é verdadeiro em geral. Por isso, devemos escrever G na forma

$$G = \{P_1, \ldots, P_m\},$$

em que os $P_i \in K[x, y]$ estão enumerados em ordem crescente de seus termos iniciais relativamente a `lex` com $x > y$. Escrevendo P_i como polinômio em x, com coeficientes em $K[y]$, seu termo líder será da forma

$$r_i x^{n_i}, \text{ em que } r_i \text{ é um polinômio mônico de } K[y].$$

A ordenação dos termos iniciais relativamente a `lex` com $x > y$ implica que $n_{i+1} \geq n_i$. Levando em conta a minimalidade de G, isto força que $\text{grau}(r_{i+1}) < \text{grau}(r_i)$. Contudo, sob esta última condição, dois Ps consecutivos não podem ter o mesmo grau em x, porque se isto ocorresse

$$\text{in}(P_{i+1}) \quad \text{dividiria} \quad \text{in}(P_i)$$

contradizendo a minimalidade de G. Portanto, a ordenação imposta aos Ps nos garante que

- $n_{i+1} > n_i$;
- $\text{grau}(r_{i+1}) < \text{grau}(r_i)$.

Começamos por investigar a relação entre os coeficientes líderes de x de dois Ps consecutivos.

PROPRIEDADE 10.12. *Para cada* $1 \leq i \leq m-1$ *existe um polinômio* $b_i \in K[x]$ *tal que* $r_i = b_i r_{i+1}$.

DEMONSTRAÇÃO. Já sabemos que r_i tem grau menor que r_{i+1}, de modo que o máximo divisor comum d destes dois polinômios tem que ter grau menor ou igual que o grau de r_{i+1}. Pelo algoritmo euclidiano estendido, existem polinômios α e β em $K[y]$ tais que

$$\alpha r_i + \beta r_{i+1} = d.$$

Considere, agora, o polinômio

$$Q = \alpha P_i + \beta P_{i+1}.$$

Trata-se de um polinômio de I cujo coeficiente líder é igual a $dx^{n_{i+1}}$. Contudo, como d tem grau menor ou igual ao de r_{i+1}, o termo inicial $\text{in}(P_j)$ não divide $\text{in}(Q)$ para $j \leq i$. Por outro lado, como

$$\text{grau}(P_j) = n_j > n_{i+1} = \text{grau}(Q), \text{ quando } j > i+1,$$

então $\text{in}(P_j)$ também não pode dividir $\text{in}(Q)$ quando $j > i+1$. Portanto, $\text{in}(Q)$ tem que ser divisível por $\text{in}(P_{i+1})$. Em particular, devemos ter que d e r_{i+1} têm o mesmo grau, o que só pode acontecer se $d = r_{i+1}$. Mas isto implica que r_{i+1} divide r_i, como afirma a proposição. □

Passando à segunda propriedade, temos o seguinte um resultado técnico.

PROPRIEDADE 10.13. *Para $1 \leq i \leq m-1$, existem polinômios $v_i \in K[x,y]$, mônicos com respeito à variável x, tais que $P_i = r_i v_i$. Como consequência disto,*

$$b_k P_k \in \langle P_1, \ldots, P_{k-1} \rangle.$$

DEMONSTRAÇÃO. Procederemos por indução em i. Como o ideal I tem dimensão zero, então pelo corolário 9.10 da página 252, P_1 é um polinômio que só contém a variável y. Portanto, a propriedade vale para $i = 1$, desde que tomemos $r_1 = P_1$ e $v_1 = 1$. Isto estabelece a base da indução.

Suponhamos que esta propriedade vale para todo $i \leq k-1$. Temos, da propriedade 10.12 que r_k divide r_j, para $1 \leq j \leq k$. Em particular, $r_{k-1} = b_k r_k$ para algum $b_k \in K[y]$. Apelando, novamente, para a propriedade 10.12, podemos concluir que $b_k r_k$ divide r_j, para $1 \leq j \leq k-1$. Entretanto, pela hipótese de indução, r_j divide P_j para $1 \leq j \leq k-1$. Portanto, $b_k r_k$ divide P_j para $1 \leq j \leq k-1$.

Considere, agora, o polinômio

$$b_k P_k - x^{n_k - n_{k-1}} P_{k-1} \in I.$$

Como G é uma base de Gröbner, este polinômio terá resto zero na divisão por G. Em outras palavras,

$$b_k P_k - x^{n_k - n_{k-1}} P_{k-1} = Q_1 P_1 + \cdots + Q_m P_m$$

em que

$$\operatorname{grau}(b_k P_k - x^{n_k - n_{k-1}} P_{k-1}) = \max\{\operatorname{grau}(Q_i P_i) : 1 \leq i \leq m\}.$$

Contudo, $b_k P_k - x^{n_k - n_{k-1}} P_{k-1}$ tem grau menor que n_k, de modo que a condição nos graus das parcelas das somas acima implica que

$$Q_k = \cdots = Q_m = 0.$$

Assim,

$$b_k P_k - x^{n_k - n_{k-1}} P_{k-1} = Q_1 P_1 + \cdots + Q_{k-1} P_{k-1},$$

donde

$$b_k P_k = Q_1 P_1 + \cdots + (Q_{k-1} + x^{n_k - n_{k-1}}) P_{k-1}.$$

Entretanto, como vimos acima, $b_k r_k$ divide $P_1, \ldots, P_{k-1}$, de forma que

$$Q_1 P_1 + \cdots + (Q_{k-1} + x^{n_k - n_{k-1}}) P_{k-1} = b_k r_k v_k,$$

para algum polinômio $v_k \in K[x,y]$. Assim,

$$b_k P_k = b_k r_k v_k,$$

e cancelando b_k em ambos os lados desta equação, obtemos

$$P_k = r_k v_k,$$

o que completa a demonstração do passo de indução. Portanto, pelo princípio de indução finita, a propriedade vale para todo $1 \leq i \leq m$. □

Antes de enunciar a próxima propriedade, há algumas considerações preliminares que precisamos fazer. Em primeiro lugar, segue imediatamente da propriedade 10.13 que

$$r_1 = b_1 r_2 = b_1 b_2 r_3 = \cdots = b_1 \cdots b_{m-1} r_m.$$

Mas, pelas propriedades 10.12 e 10.13, r_m divide todos os Ps. Como o ideal é zero dimensional isto implica que r_m é uma constante. Assim, se c for uma raiz de r_1, existe um único inteiro $\kappa(c)$ tal que

$$b_{\kappa(c)}(c) = 0, \text{ mas } b_{\kappa(c)+1}(c) \neq 0.$$

PROPRIEDADE 10.14. *Se c é uma raiz de $r = r_1$, então*

$$\mathrm{mdc}(P_1(x,c), \ldots, P_m(x,c)) = P_{\kappa(c)+1}(x,c).$$

DEMONSTRAÇÃO. Seja $\kappa = \kappa(c)$. Como $r_\kappa = b_\kappa r_{\kappa+1}$ divide P_j para todo $1 \leq j \leq \kappa$, temos que

$$P_1(x,c) = \cdots = P_\kappa(x,c) = 0; \tag{110}$$

Logo, a propriedade estará provada se mostrarmos que

$$P_{\kappa+1}(x,c) \text{ divide } P_j(x,c) \text{ para todo } \kappa + 1 \leq j \leq \kappa.$$

Faremos isto por indução em j. Como isto é óbvio se $j = \kappa + 1$, não há nada a fazer para estabelecer a base da indução. Suponha, agora, que $P_{\kappa+1}(x,c)$ divide $P_j(x,c)$ para todo ℓ que satisfaz,

$$\kappa + 1 \leq j \leq \ell \leq m.$$

Pela propriedade 10.13, temos que

$$b_\ell P_{\ell+1} = \sum_{i=1}^{\ell} Q_i P_i.$$

De modo que pela equação (110),

$$b_\ell(c) P_{\ell+1}(x,c) = \sum_{i=\kappa+1}^{\ell} Q_i(x,c) P_i(x,c).$$

Como $b_\ell(c) \neq 0$ pela escolha de κ e ℓ,

$$P_{\ell+1}(x,c) = \sum_{i=\kappa+1}^{\ell} \frac{Q_i(x,c)}{b_\ell(c)} P_i(x,c).$$

Mas, pela hipótese de indução, $P_{\kappa+1}(x,c)$ divide cada parcela da soma; logo divide $P_{\ell+1}(x,c)$, como queríamos mostrar. O resultado desejado segue pelo princípio de indução finita, completando assim a demonstração da propriedade. □

Finalmente, a quarta propriedade nos diz que os polinômios vs definidos na propriedade 10.13 são os mesmos que apareceram no teorema 10.10.

PROPRIEDADE 10.15. *Se c é uma raiz de $r = r_1$, então*

$$\mathrm{mdc}(N - cD', D) = v_{\kappa(c)+1}.$$

DEMONSTRAÇÃO. Da igualdade

$$\langle N - yD', D\rangle = \langle P_1, \ldots, P_m\rangle$$

entre ideais de $K[x, y]$, obtemos

$$\langle N - cD', D\rangle = \langle P_1(x, c), \ldots, P_m(x, c)\rangle$$

em $K[x]$. Temos, assim, um ideal de $K[x]$ representado por dois conjuntos diferentes de geradores. Usando o conjunto da esquerda, concluímos que

$$\mathrm{mdc}(N - cD', D),$$

gera o ideal. Já o conjunto da direita a dá lugar ao gerador

$$\mathrm{mdc}(P_1(x, c), \ldots, P_m(x, c)).$$

Mas o máximo divisor comum é sempre mônico, e dois geradores não podem diferir por mais que uma constante. Assim,

$$\mathrm{mdc}(N - cD', D) = \mathrm{mdc}(P_1(x, c), \ldots, P_m(x, c)),$$

que, pela propriedade 10.15, é igual a $P_{\kappa+1}(x, c)$, a menos de uma constante. Entretanto,

$$P_{\kappa+1}(x, c) = r_{\kappa+1}(c)v_{\kappa+1}(x, c).$$

Como $r_{\kappa+1}(c) \neq 0$ pela escolha de κ, e $v_{\kappa+1}(x, c)$ é mônico, podemos concluir que

$$\mathrm{mdc}(N - cD', D) = v_{\kappa+1}(x, c),$$

como no enunciado da proposição. □

A propriedade 10.15 nos permite identificar, em termos da base de Gröbner G, os polinômios utilizados na integração de N/D pelo algoritmo de Rothstein-Trager. Podemos, assim, enunciar o algoritmo de Czichowski.

ALGORITMO 10.16 (Algoritmo de Czichowski). *Dados polinômios N e D em $K[x]$ que satisfazem*

- $\mathrm{grau}(N) < \mathrm{grau}(D)$ *e*
- D *é livre de quadrados.*

o algoritmo calcula pares $(c_j, v_j) \in \mathbb{C} \times \mathbb{C}[x]$, tais que

$$\int \frac{N}{D}dx = \sum_{i=1}^{s} c_i \log(v_i).$$

Etapa 1: *Construa o ideal $I(N, D)$ de $K[x, y]$ gerado por D e $N - yD'$.*

Etapa 2: *Calcule a base de Gröbner*

$$G = \{P_1, \ldots, P_m\},$$

de I para a ordem lexicográfica na qual $y < x$ e faça $\rho = P_1$.

Etapa 3: *Inicialize L como uma lista vazia, $j = m - 1$ e $b = 1$.*

Etapa 4: *Enquanto $j > 1$, repita:*
- *calcule o conteúdo* $\mathrm{cont}(P_j)$ *como polinômio na variável* x *com coeficientes em* $K[y]$*;*
- *calcule* $b = \mathrm{cont}(P_j)/b$ *e* $v = P_j/\mathrm{cont}(P_j)$.
- *acrescente o par* (b, v) *'a lista* L*;*
- *faça* $j = j - 1$.

Etapa 5: *Imprima* L *e pare.*

Resta-nos aplicar este algoritmo ao exemplo que tentamos calcular ao final da seção anterior. A integral é

$$\int \frac{-\frac{13385}{1591812}x^4 - \frac{38497}{530604}x^3 + \frac{92473}{397953}x^2 + \frac{60551}{530604}x - \frac{59363}{1591812}}{(x+1)(x^2+2)(x^3+3)}$$

e a base de Gröbner do ideal $\langle N - yD', D\rangle$ para a ordem lexicográfica com $x > y$ é igual a $G = \{P_1, P_2\}$, em que $P_1 = x + g$ e g e P_2 são polinômios apenas em y; veja página 301. Assim, pelo algoritmo de Czichowski, a integral deve ser igual a

$$\sum_{c|P_2(c)=0} \log(x+g).$$

A princípio isto parece incompatível com o que obtivemos na seção 5; afinal, onde está a parcela $\log(x+1)/72$? Entretanto, podemos usar a fatoração de P_2 da página 302 para reescrever a primitiva de uma maneira mais palatável. Como os fatores de P_2 são

$$\begin{aligned} f_1 &= y - \frac{1}{72} \\ f_2 &= y^2 - \frac{5122}{751689}y + \frac{1}{36992} \\ f_3 &= y^3 + \frac{13833}{668168}y^2 + \frac{2718605}{19727326116}y + \frac{7211969}{21571831107846}, \end{aligned}$$

então a integral pode ser escrita na forma

$$\frac{1}{72}\log(x + g(1/72)) + \sum_{c|f_2(c)=0} \log(x+g) + \sum_{c|f_3(c)=0} \log(x+g).$$

Calculando g em $1/72$ descobrimos que o resultado é 1, o que nos dá a parcela que já havíamos calculado. As duas outras parcelas também podem ser simplificadas, ainda que não tanto. Por exemplo, dividindo g por f_2, obtemos

$$g = f_2 q + \frac{12027024}{33401}y + \frac{40976}{33401}.$$

Logo, se c for raiz de f_2, então

$$x + g(c) = x + f_2(c)q(c) + \frac{12027024}{33401}c + \frac{40976}{33401} = x + \frac{12027024}{33401}c + \frac{40976}{33401}.$$

De maneira semelhante, se c for raiz de f_3, então $x + g(c)$ é igual a

$$x - \frac{20425417005266892}{1163563480223}y^2 - \frac{1544168715066315}{2327126960446} - \frac{4286488033626}{1163563480223}.$$

Com isso, podemos reescrever a primitiva desejada na forma

$$\frac{1}{72}\log(x+1)+ \sum_{c|f_2(c)=0} \log(x+\frac{12027024}{33401}c+\frac{40976}{33401})+ \sum_{c|f_3(c)=0} \log(x-\frac{20425417005266892}{1163563480223}y^2- \frac{1544168715066315}{2327126960446}-\frac{4286488033626}{1163563480223}).$$

7. Integrais: definidas e indefinidas

Como vimos nas seções anteriores, uma combinação dos algoritmos de Hermite e Czichowski, nos permitem integrar automaticamente qualquer função racional. Mas há mais. No século XIX, K. Weierstrass observou que é possível reduzir qualquer integral construída a partir das funções trigonométricas diretas, usando as quatro operações aritméticas básicas, à integração de uma função racional. Mais precisamente, uma *integral trigonométrica* é aquela cujo integrando é da forma

$$f(\operatorname{sen}(x), \cos(x))$$

em que f é uma função racional com coeficientes em um corpo $K \subseteq \mathbb{C}$. Como todas as funções trigonométricas diretas (de um mesmo argumento) podem ser escritas em função de senos e co-senos, qualquer integral que envolva apenas estas funções e as operações aritméticas básicas pode ser reduzida à forma acima.

A ideia de Weierstrass consiste em substituir senos e co-senos pelas suas expressões em função da tangente da metade do ângulo. As fórmulas são,

$$\operatorname{sen}(x) = \frac{2u}{1+u^2} \text{ e } \cos(x) = \frac{1-u^2}{1+u^2} \text{ em que } u = \tan(\frac{x}{2}).$$

Como $x = 2\arctan(u)$, temos que

$$\frac{dx}{du} = \frac{2}{u^2+1},$$

de forma que

$$\int f(\operatorname{sen}(x), \cos(x))dx = \int f\left(\frac{2u}{1+u^2}, \frac{1-u^2}{1+u^2}\right)\frac{2}{1+u^2}du.$$

Para obter a primitiva desejada, basta calcular esta integral e substituir u por $\tan(x/2)$.

Por exemplo, digamos que queremos calcular a integral

$$\int \operatorname{sen}^2(x)dx.$$

Usando a substituição acima, obtemos

$$\int \operatorname{sen}^2(x)dx = \int \left(\frac{2u}{1+u^2}\right)^2 \frac{2}{1+u^2}du = \int \frac{8u^2du}{(1+u^2)^3}.$$

Como o numerador tem grau menor que o denominador, não há necessidade de efetuar nenhuma divisão de polinômios. Contudo, o denominador tem fatores mútiplos, de forma que precisamos começar aplicando o algoritmo Hermite. Como a multiplicidade máxima dos fatores no denominador é três, o algoritmo de Hermite executará dois laços, dando como resultado

$$\frac{u^3-u}{u^4+2u^2+1} + \int \frac{du}{u^2+1}.$$

Portanto, por (97), temos que

$$\int \frac{8u^2du}{(1+u^2)^3} = \frac{u^3-u}{u^4+2u^2+1} + \arctan(u).$$

Substituindo $u = \tan(x/2)$, a integral final é

$$\frac{\tan(x/2)^3 - \tan(x/2)}{\tan(x/2)^4 + 2\tan(x/2)^2 + 1} + \arctan(\tan(x/2)).$$

Chegados a este ponto, talvez lhe venha o impulso de escrever $x/2$, em lugar de $\arctan(\tan(x/2))$. Contudo, isto só é verdadeiro se sabemos que $-\pi < x < \pi$. De fato, a tangente está definida em qualquer intervalo da forma $(-k\pi/2, k\pi/2)$, com k ímpar; ao passo que a imagem do arcotangente está toda contida em $(-\pi/2, \pi/2)$. Este detalhe torna-se particularmente relevante quando usamos primitivas para calcular integrais definidas.

Para analisar a relação entre integrais definidas e indefinidas, precisamos do chamado *teorema fundamental do cálculo*, que aprendemos em cálculo I. O teorema, que foi descoberto independentemente por Newton e Leibniz, pode ser enunciado da seguinte forma.

TEOREMA FUNDAMENAL DO CÁLCULO. *Sejam $I \subseteq \mathbb{R}$ um intervalo aberto e $f : I \to \mathbb{R}$ uma função contínua. Se $F : I \to \mathbb{R}$ é uma primitiva de f e $a, b \in I$, então*

$$\int_a^b f dx = F(b) - F(a).$$

Na prática, integrais definidas normalmente são calculadas usando métodos numéricos, e não o teorema fundamental do cálculo, veja ???? por exemplo. Contudo, como temos algoritmos que nos permitem determinar algumas primitivas de forma exata, parece razoável utilizá-las. O uso de primitivas é especialmente atrativo se precisamos calcular a integral da mesma função com vários limites de integração diferentes.

Apesar de parecer uma boa ideia, este método conduz a uma série de problemas. Por exemplo, vamos determinar

$$\int_1^2 \frac{x^4-3x^2+6}{x^6-5x^4+5x^2+4}dx.$$

Como o denominador do integrando é livre de quadrados, podemos utilizar diretamente o algoritmo de Czichowski. Calculando uma base de Gröbner para o ideal

$$\langle x^4 - 3x^2 + 6 - y(6x^5 - 20x^3 + 10x^2), x^6 - 5x^4 + 5x^2 + 4\rangle,$$

obtemos

$$G = \{x^3 + 2yx^2 - 3x - 4y, y^2 + \frac{1}{4}\}.$$

Assim, a primitiva desejada é

$$i\frac{1}{2}\log(x^3 + ix^2 - 3x - 2i) - i\frac{1}{2}\log(x^3 - ix^2 - 3x + 2i),$$

que é igual a

$$\frac{1}{2}i\log(\frac{g+i}{g-i}), \text{ em que } g = \frac{x^3 - 3x}{x^2 - 2}.$$

Aplicando, agora, o lema 10.4 concluímos que a primitiva é igual a

$$\arctan(\frac{x^3 - 3x}{x^2 - 2}).$$

Portanto, a integral desejada é

$$\arctan(\frac{x^3 - 3x}{x^2 - 2})|_1^2 = \arctan(1) - \arctan(2);$$

que é aproximadamente igual a $-0,32175$. Contudo, se aplicarmos um método numérico no cálculo desta integral, descobrimos que o resultado dá ????. A pergunta, naturalmente, é: onde está o erro?

Na verdade o erro está na escolha da primitiva usada na aplicação do teorema fundamental do cálculo. No exemplo acima, a função

$$\arctan(\frac{x^3 - 3x}{x^2 - 2})$$

tem uma singularidade em $\sqrt{2}$, que fica entre os limites de integração. Portanto, a primitiva não é contínua neste intervalo e, consequentemente, não podemos usá-la para calcular a integral definida no *intervalo dado*. Note, porém, que esta singularidade é um artefato do processo de integração em si. De fato, o denominador do integrando não tem nenhuma raiz real, de modo que a primitiva deveria estar definida em qualquer intervalo desejado. Chamaremos de *espúria* uma singularidade da primitiva que não é singularidade do integrando.

O exemplo apareceu originalmente na tese de doutorado de R. Rioboo. Nela, Rioboo descreve um algoritmo que permite representar a integral de qualquer função racional com *coeficientes reais* sem nenhuma singularidade espúria. Aplicado ao exemplo acima, o algoritmo de Rioboo nos dá a primitiva

$$\arctan\left(\frac{x^5 - 3x^3 + x}{2}\right) + \arctan(x^3) + \arctan(x),$$

que não tem nenhuma singularidade. A princípio isto pode parecer muito estranho. Afinal, duas primitivas diferem apenas por uma constante, e as constantes se cancelam quando fazemos a diferença dos seus valores nos limites de integração, não se cancelam? Entretanto, uma mera constante pode ser suficiente para remover uma singularidade de uma integral indefinida, ou introduzi-la. Este é, infelizmente, um fato raramente apresentado em um curso elementar de cáculo, apesar de sua importância nas aplicações. Como se trata de um algoritmo cuja descrição é bastante técnica, ainda que elementar, não apresentaremos o algoritmo de Rioboo aqui. Para uma descrição detalhada veja [**4**, capítulo 2, seção 2.8, p. 59].

Este mesmo problema torna-se muito mais agudo quando consideramos funções mais complicadas. Um tratamento detalhado do que acontece com as funções trigonométricas consideradas no início da seção, pode ser encontrado em [**40**]. Para o caso geral veja [**21**].

8. Comentários e complementos

O cálculo de integrais de funções elementares em termos de funções elementares foi estudado por vários matemáticos do século XIX, mas teve sua formulação mais precisa no trabalho de J. Liouville. Em uma série de artigos publicados nas décadas de 1830 e 1840 Liouville mostrou, entre outras coisas, que há funções elementares, como $\exp(x)/x$ cuja primitiva não é uma funcção elementar; veja [**49**, rodapé à página 192] ou [**50**].

No início do século XX, G. H. Hardy fez um sumário dos vários resultados conhecidos desta área em sua monografia *Integration of functions of a single variable*, [**34**]. Entre outras coisas, ele esboçou um algoritmo de integração para funções elementares transcendentes. O problema foi retomado, em um contexto mais algébrico, por Ritt, Kolchin e Rosenlicht. Em 1969 Risch, um estudante de Rosenlicht, apresentou um algoritmo capaz de integrar qualquer função elementar cuja primitiva também é elementar; [**57**]. Este algoritmo foi posteriormente aperfeiçoado por vários matemáticos, entre eles R. Trager e M. Bronstein, e parcialmente implementados em vários sistemas de computação algébrica, como o AXIOM e o MAXIMA. Até o momento nenhuma implementação completa de tais algoritmos existe em qualquer dos sistemas de computação algébrica atualmente disponíveis. O principal problema está nos algoritmos que tratam de funções algébricas, que utilizam métodos muito mais sofisticados do que aqueles que tratam de funções transcendentes; veja [**66**], por exemplo.

A principal referência para o assunto é *Symbolic integration I* de Manuel Bronstein; veja [**4**]. Entretanto, este livro aborda apenas a integração de funções transcendentes. Infelizmente Bronstein faleceu em 2005, sem ter completado o volume que trataria das funções algébricas. Um apanhado geral do problema de integração pode ser encontrado em seu *Symbolic integration tutorial* [**5**], onde há um esboço detalhado do enfoque a ser adotado na integração de funções algébricas.

9. Exercícios

1. Seja I um ideal de dimensão zero de $K[x_1, \ldots, x_n]$. Mostre que se I é radical e está em posição geral relativamente à variável x_1, então a inclusão de $K[x_1]$ em $K[x_1, \ldots, x_n]$ induz um isomorfismo
$$\frac{K[x_1]}{g} \cong \frac{K[x_1, \ldots, x_n]}{I}$$
em que g é o gerador de $I \cap K[x_1]$.

2. Seja I um ideal de dimensão zero de $K[x_1, \ldots, x_n]$. Mostre que se I é radical e está em posição geral relativamente à variável x_1, então admite uma base de Gröbner da forma
$$\{g_1, x_2 - g_2, \ldots, x_n - g_n\}$$
em que g_1 é o gerador de $I \cap K[x_1]$ e $g_2, \ldots, g_n \in K[x_1]$. Na literatura de língua inglesa este resultado é conhecido como o *shape lema*.

3. Seja I um ideal de dimensão zero de $K[x_1, \ldots, x_n]$. Mostre que se I é radical e está em posição geral relativamente à variável x_1, então é possível usar o resultado do exercício anterior para dar uma descrição completa de $\mathcal{Z}(I)$ a partir das raízes do gerador de $I \cap K[x_1]$.

4. Calcule
$$\int \frac{x^2 - 7}{x^4 + 12x^3 + 6x^2 - 52x + 33} dx$$

5. Calcule
$$\int \frac{x^3 + x + 1}{x^6 + 11x^4 + 39x^2 + 45} dx$$

6. Calcule
$$\int \frac{dx}{x^6 - 2x^5 + 3x^4 - 4x^3 + 3x^2 - 2x + 1}$$

7. Calcule
$$\int \frac{x}{x^3 + 1} dx.$$

8. Calcule
$$\int \frac{dx}{x^4 + 1} dx \quad \text{e} \quad \int \frac{x^2 dx}{x^4 + 1} dx.$$

9. Prove que
$$\operatorname{sen}(2t) = \frac{2\tan(t)}{1 + \tan^2(t)} \quad \text{e que} \quad \cos(2t) = \frac{1 - \tan^2(t)}{1 + \tan^2(t)}.$$

10. Seja $R \in \mathbb{Q}(x, y)$ uma função racional em duas variáveis. Use as fórmulas da questão anterior para reduzir

$$\int R(\mathrm{sen}(t), \cos(t))dt,$$

à integral de uma função racional em uma única variável $u = t/2$.

11. Seja $R \in \mathbb{Q}(x, y)$ uma função racional em duas variáveis. Use os algoritmos descritos neste capítulo e a redução do exercício anterior para calcular as primitivas das seguintes funções:
    (a) $\mathrm{sen}(2t)^3 + + \cos(2t)^3$;
    (b) $3\mathrm{sen}(2t)/(2 + \mathrm{sen}(t))^2$;
    (c) $\mathrm{sen}(2t)^3 + \mathrm{sen}(t)^2\cos(t) + \cos(t)^5$;
    (d) $(3\mathrm{sen}(t) + 7\cos(t))/(1 + \mathrm{sen}(t)^5)$.

Referências Bibliográficas

[1] Adams, W. W. e Loustaunau, P., *An introduction to Gröbner bases*, American Mathematical Society, Providence (1994).

[2] M. Artin, M., *Algebra*, Prentice Hall, New Jersey, (1991).

[3] Jacobi Bernoulli, *Opera*, vol. 1, editado por G. Cramer, Basiléia (1744).

[4] M. Bronstein, *Symbolic integration I: transcendental functions*, segunda edição, Springer (2005).

[5] M. Bronstein, *Symbolic integration tutorial*, ISSAC'98, Rostock (August 1998)and Differential Algebra Workshop, Rutgers (2000).

[6] Buchberger, B., *Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungsystems*, Aeq. Math., (1970) 374–383.

[7] B. Buchberger, *An algorithmic criterium for the solvability of a system of algebraic equations*, Gröbner bases and applications, ed. B. Buchberger e F. Winkler, Cambridge University Press, Cambridge (1998), 535–545.

[8] B. Buchberger, *A note on the complexity of constructing Gröbner-bases*. Computer algebra (London, 1983), Lect. Notes in Comput. Sci., **162**, Springer, (1983), 137–145.

[9] Buchberger, B. e Winkler, F., eds. *Gröbner bases and applications*, ed. B. Buchberger e F. Winkler, Cambridge University Press, Cambridge (1998).

[10] G. Chèze e A. Galligo, *Four lectures on polynomial absolute factorization*, em *Solving polynomial equations*, Editado por Alicia Dickenstein and Ioannis Z. Emiris. Algorithms Comput. Math., **14**, Springer, Berlin (2005), 339–392.

[11] F. Chyzak, Gröbner bases, symbolic summation and symbolic integration, *Gröbner bases and applications*, ed. B. Buchberger e F. Winkler, Cambridge University Press, Cambridge (1998), 32–60.

[12] P. Conti e C. Traverso, Buchberger algorithm and integer programming, *Applied algebra, algebraic algorithms, and error-correcting codes AAECC'9*, H. F. Mattson, T. Mora e T. R. N. Rao, eds, Lecture Notes in Computer Science, **539**, Springer, Berlin and New York (1991), 130–139.

[13] A. V. Costa e I. Vainsencher, *Bases de Gröbner: Resolvendo Equações Polinomiais*, Atas da XIII Escola de Álgebra, Campinas, julho 1994, (1995), 111–184; disponível em `http://www.mat.ufmg.br/~israel/Ensino/imeccfin.ps.gz`.

[14] S. C. Coutinho, *The many avatars of a simple algebra*, Amer. Math. Monthly 104 (1997), 593–604.

[15] S. C. Coutinho, *Números inteiros e criptografia RSA*, segunda edição, Instituto de Matemática Pura e Aplicada e Sociedade Brasileira de Matemática (2000).

[16] S. C. Coutinho e B. F. M. Ribeiro, On holomorphic foliations without algebraic solutions, *Experimental Mathematics*, **10** (2001), 529–536.

[17] D. Cox, J. Little, e D. O'Shea, *Ideals, varieties and algorithms*, Springer, New York (1992).

[18] D. Cox, e B. Sturmfelds, eds., *Applications of computational algebraic geometry*, American Mathematical Society, Providence (1998).

[19] G. Czichowski, A note on Gröbner bases and integration of rational functions, J. Symbolic Computation **20** (1995), 163–167.

[20] J. H. Davenport, Y. Siret, e E. Tournier, *Computer algebra*, Academic Press, Suffolk (1988).

[21] J. H. Davenport, *The difficulties of definite integration*, web????

[22] R. Descartes, *Discurso do método*, Edição IntraText CT, (2007)

[23] R. Descartes, *The Geometry of Rene Descartes, with a facsimile of the first edition*, translated from the French and Latin by D. E. Smith and M. L. Latham, Dover (1954).

[24] Dubé, Thomas W., *The structure of polynomial ideals and Gröbner bases*, SIAM J. Comput. **19** (1990), 750–775.

[25] J. C. Faugère, P. Gianni, D. Lazard e T. Mora, *Efficient computation of zero-dimensional Gröbner bases by change of ordering*, J. Symbolic Comput. **16** (1993), 329–344.

[26] B. Hayes, *A lucid interval*, American Scientist, **91** (2003), 484–488.

[27] G. H. Hardy e E. M. Wright, *An introduction to the theory of numbers*, quinta edição, Oxford University Press (1994).

[28] D. F. Holt, B. Eick, Bettina, E. A. O'Brien, *Handbook of computational group theory*, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, (2005).

[29] D. E. Knuth, *The art of computer programming: seminumerical algorithms*, volume 2, segunda edição, Addison-Wesley, Reading (1981).

[30] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Springer, Berlin-New York (1995).

[31] J. von zur Gathen e J. Gerhard, *Modern computer algebra*, Cambridge University Press (1999).

[32] G.-M. Greuel, Computer algebra and algebraic geometry—achievements and perspectives, *J. Symbolic Computation* **30** (2000), 253–289.

[33] G.-M. Greuel e G. Pfister, *A Singular introduction to commutative algebra*, Springer (2002).

[34] G. H. Hardy, *Integration of functions of a single variable*, segunda edição, Cambridge University Press (1928).

[35] J. Harris, *Algebraic geometry*, Graduate Texts in Mathematics 133, Springer-Verlag (1993).

[36] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics 52, Springer-Verlag, (1977).

[37] T. Heath, *A history of Greek mathematics*, Dover (1981).

[38] S. Hoşten e B. Sturmfels, *GRIN: an implementation of Gröbner bases for integer programming*, LNCS 920, Springer (1995), 267–276.

[39] I. Vainsencher, *Introdução às curvas algébricas planas*, Segunda Edição, Coleção Matemática Universitária, Instituto Nacional de Matemática Pura e Aplicada (2005).

[40] D. J. Jeffrey e A. D. Rich, *The evaluation of trigonometric integrals avoiding spurious discontinuities*, ACM Trans. Math. Software, **20** (1994), 124–135.

[41] A. B. Kempe, *On a general method of describing plane curves of the nth degree by linkwork*, Proc. London Math. Soc. (1876), 213–216.

[42] A. B. Kempe, *How to draw a straight line: a lecture on linkages*, MacMillan and Co. (1877).

[43] D. E. Knuth, *The art of computer programming: seminumerical algorithms*, vol. 2, segunda edição, Addison-Wesley (1981).

[44] M. Kreuzer e L. Robbiano, *Computational commutative algebra 1*, Springer (2000).

[45] M. Kreuzer e L. Robbiano, *Computational commutative algebra 2*, Springer (2005).

[46] E. Kunz, *Introduction to commutative algebra and algebraic geometry*, Birkhäuser (1985).

[47] D. Lazard e R. Rioboo, *Integration of rational functions: rational computation of the logarithmic part*, **9** (1990), 113–115.

[48] E. L. Lima, *Geometria analítica e álgebra linear*, Coleção Matemática Universitária, Segunda Edição, IMPA, (2005).

[49] J. Liouville, *Second Mémeoire sur la détermination des intégrales dont la valeur est algébrique*, Journal de L'Ecole Polytechnique, **14** (1833), 149–193.

[50] J. Liouville, *Mémeoire sur l'integration d'un classe de fonctions transcendentes*, Journal für die reine und angewandte Mathematik, **13** (1835), 93–118.

[51] J.P. Merlet, *Parallel Robots*, Solid Mechanics and Its Applications, 2nd ed. edition, Springer (2005).

[52] M. Mignotte e D. Ştefanescu, *La première méthode générale de factorisation des polynômes. Autour d'un mémoire de F.T. Schubert*, Revue d'histoire des mathématiques **7** (2001), 67-89.

[53] T. Mora, *Solving polynomial equation systems. II. Macaulay's paradigm and Gröbner technology*, Encyclopedia of Mathematics and its Applications **99**, Cambridge University Press, Cambridge (2005).

[54] N. R. Natraj, S. R. Tayur e R. R. Thomas, *An algebraic geometry algorithm for scheduling in the presence of setups and correlated demands*, Mathematical Programming **69** (1995), 369–401.

[55] C. S. Ogilvy, *Excursions in geometry*, Dover (1990).

[56] J. Ohm, *Space curves as ideal-theoretic complete intersections*, Studies in algebraic geometry, MAA Stud. Math., 20, Math. Assoc. America, Washington, D.C. (1980), pp. 47–115.

[57] R. H. Risch, *The problem of integration in finite terms*, Trans. Amer. Math. Soc. **139** (1969), 167–189.

[58] L. Robbiano, *Gröbner bases and statistics*, ed. B. Buchberger e F. Winkler, Cambridge University Press, Cambridge (1998), 179–204.

[59] M. Saito, B. Sturmfels e N. Takayama, *Gröbner deformations of hypergeometric differential equations*, Springer, Berlin-Heidelberg-New York (2000).

[60] A. Seidenberg, *Constructions in algebra*, Trans. Am. Math. Soc., **197** (1974), 273–313.

[61] A. Seress, *An introduction to computational group theory*, Notices of the American Mathematical Society **44** (1997), 671–679.

[62] M. Sipser, *Introduction to the theory of computation*, PWS Publishing (1997).

[63] D. Struppa, Gröbner bases in partial differential equations, *Gröbner bases and applications*, ed. B. Buchberger e F. Winkler, Cambridge University Press, Cambridge (1998), 235–245.

[64] R. Thomas, A geometric Buchberger algorithm for integer programming, *Math. Op. Research* **20** (1995), 864–884

[65] R. R. Thomas, *Algebraic methods in integer programming*, Encyclopedia of Optimization (eds: C. Floudas and P. Pardalos), Kluwer Academic Publishers, Dordrecht, (2001).

[66] B. M. Trager, *Integration of algebraic functions*, PhD Thesis, Massachussets Institute of Technology (1984).

[67] R. Urbaniak, R. Weismantel e G. M. Ziegler, *A variant of Buchberger's algorithm for integer programming*, SIAM J. Discrete Math. **10** (1997), 96–108.

[68] B. L. van der Waerden, *A history of algebra: from al-Khārizmī to Emmy Noether*, Springer (1985).

[69] D. Wang, Gröbner bases applied to geometric theorem proving and discovering, *Gröbner bases and applications*, ed. B. Buchberger e F. Winkler, Cambridge University Press, Cambridge (1998), 281–301.

[70] R. J. Wilson, *Four Colours Suffice: How the Map Problem Was Solved*, Penguin Books (2003).

[71] Wen-Tsun Wu, *Mechanical theorem proving of differential geometries and some of its applications in mechanics*, J. Automat. Reason. **7** (1991), 171–191.

[72] Wen-Tsun Wu, *Mathematics mechanization*, Science Press/Kluwer Academic Publishers (2000).

[73] G. M. Ziegler, *Gröbner bases and integer programming*, em *Some Tapas of Computer Algebra*, A. M. Cohen, H. Cuypers e H. Sterk, editores, Springer (1999), 168–183.