

Fundação Getulio Vargas
Escola de Matemática Aplicada
Curso de Graduação em Matemática Aplicada

**ESTUDO SOBRE IDEAIS, BASES DE GRÖBNER E SUAS
APLICAÇÕES**

por Felipe Vieira Costa

Rio de Janeiro - Brasil

2020

FELIPE VIEIRA COSTA

ESTUDO SOBRE IDEAIS, BASES DE GRÖBNER E SUAS APLICAÇÕES

Trabalho de conclusão de curso apresentado à Escola de Matemática Aplicada, como parte dos requisitos para a obtenção do título de Bacharel em Matemática Aplicada.

Orientador: Luciano Guimarães Monteiro de Castro

Rio de Janeiro - Brasil
2020

FELIPE VIEIRA COSTA

ESTUDO SOBRE IDEAIS, BASES DE GRÖBNER E SUAS APLICAÇÕES

“Trabalho de Conclusão apresentado à Escola de Matemática Aplicada como requisito para a obtenção do grau de bacharel em Matemática Aplicada”

Aprovado em _____ de _____ de _____

Professor Orientador: Luciano Guimarães Monteiro de Castro
Escola de Matemática Aplicada
Fundação Getúlio Vargas



FELIPE VIEIRA COSTA

“ESTUDO SOBRE IDEAIS, BASES DE GRÖBNER E SUAS APLICAÇÕES”

Trabalho de Conclusão de Curso - TCC apresentado ao Curso de Graduação em Matemática Aplicada da Escola de Matemática Aplicada para obtenção do grau de Bacharel em Matemática Aplicada.

Data da Defesa: 08/12/2020

ASSINATURA DOS MEMBROS DA BANCA EXAMINADORA

Luciano Guimarães Monteiro de Castro
Orientador

Paulo Cezar Pinto Carvalho
Membro

DocuSigned by:

6812AE5B8AEA41A...
Alexandre Madureira
Membro

Nos termos da Lei nº 13.979 de 06/02/20 - DOU nº 27 de 07/02/20 e Portaria MEC nº 544 de 16/06/20 - DOU nº 114 de 17/06/20 que dispõem sobre a suspensão temporária das atividades acadêmicas presenciais e a utilização de recursos tecnológicos face ao COVID-19, as apresentações dos Trabalhos de Conclusão de Curso, de forma excepcional, serão realizadas de forma remota e síncrona, incluindo-se nessa modalidade membros da banca e discente.

Resumo

Neste trabalho, estudaremos o Teorema das Quatro Cores, problema que, apesar de simples de enunciar, ficou por mais de um século sem uma prova concreta. O resultado foi conjecturado em 1852, quando um matemático sul-africano chamado Francis Guthrie, ao tentar colorir o mapa de condados ingleses, notou que quatro cores bastavam para colorir cada região de modo que cada uma recebesse uma única cor e que condados vizinhos não fossem pintados com cores iguais. Daí, esta conjectura foi passando de boca em boca até chegar em Alfred Bray Kempe, que, em 1879, foi o primeiro a publicar uma tentativa de demonstração do Teorema, cujo método utilizado ficou conhecido como Método das Cadeias de Kempe. Porém, anos depois, em 1890, o matemático britânico Percy J. Heawood construiu um mapa no qual o processo de Kempe não funcionava, deixando a demonstração da até então Conjectura das Quatro Cores em aberto. Em 1976, 86 anos depois, foi publicado por Appel e Haken, finalmente, uma solução para o problema, com um detalhe curioso: eles tiveram o auxílio de um computador chamado IBM 360, que teve que realizar bilhões de cálculos por volta de 1200 horas. Em 1994, outro grupo de matemáticos conseguiu uma solução mais simples, também usando métodos computacionais, mas que ainda deixavam dúvidas pela dificuldade de ser analisada. Por fim, estas dúvidas foram saciadas por volta de 2005, graças ao trabalho de Georges Gonthier.

Nosso papel aqui será fazer uma abordagem diferente sobre o Problema das Quatro Cores sem usar, ao menos explicitamente, Teoria dos Grafos, que seria a abordagem mais usual para lidar com regiões e adjacências. Usaremos, no lugar, o conhecimento obtido estudando Álgebra, mais especificamente sobre Anéis, Ideais de Polinômios e Bases de Gröbner, chegando a um algoritmo que apesar de não poder ser usado em geral por sua complexidade e custo computacional, tem muito valor teórico e é capaz de colorir, usando apenas ferramentas algébricas, cálculos simples e um pouco de inteligência, um mapa plano com no máximo quatro cores, como demonstrado pela literatura.

PALAVRAS-CHAVE: Teorema das Quatro Cores, Álgebra, Polinômios, Ideais, Base de Gröbner

Abstract

In this work, we will study the Four Colors Theorem, a problem that, although simple to enunciate, was left for more than a century without concrete proof. The result was conjectured in 1852, when a South African mathematician named Francis Guthrie, while trying to color the map of English counties, noticed that four colors were enough to color each region so that each received a single color and that neighboring counties were not painted with the same colors. Hence, this conjecture passed from word of mouth to Alfred Bray Kempe, who, in 1879, was the first to publish an attempt to demonstrate the Theorem, whose method used was known as the Kempe Chain Method. However, years later, in 1890, the British mathematician Percy J. Heawood built a map in which the Kempe process did not work, leaving the demonstration of the hitherto Conjecture of the Four Colors open. In 1976, 86 years later, Appel and Haken finally published a solution to the problem, with a curious detail: they had the aid of a computer called IBM 360, which had to perform billions of calculations around 1200 hours. In 1994, another group of mathematicians achieved a simpler solution, also using computational methods, but which still left doubts due to the difficulty of being analyzed. Finally, these doubts were quenched around 2005, thanks to the work of Georges Gonthier. paragraph Our role here will be to take a different approach to the Four Color Problem without using, at least explicitly, Graph Theory, which would be the most usual approach to deal with regions and adjacencies. We will use, instead, the knowledge obtained by studying Algebra, more specifically on Rings, Polynomial Ideals and Gröbner Bases, arriving at an algorithm, which although it cannot be used in general due to its complexity and computational cost, has a lot of theoretical and is able to color, using only algebraic tools, simple calculations and a little intelligence, a flat map with a maximum of four colors, as demonstrated by the literature. **KEYWORDS: Four-Color Theorem, Algebra, Polynomials, Ideals, Gröbner Bases.**

Sumário

1	Introdução	7
1.1	O Problema	7
1.2	Primeiros Contatos	8
1.3	A “Prova” de Kempe	8
1.4	O contraexemplo de Heawood	12
1.5	Desfecho do Teorema	13
2	Teoria dos Ideais e Bases de Gröbner	14
2.1	Anéis, Corpos e Domínios	14
2.2	Ideais	15
2.3	Anéis de polinômios	16
2.4	Ideais de Polinômios	16
2.5	Ordem Monomial	16
2.6	Divisão de Polinômios Multivariados	17
2.7	Bases de Gröbner	19
2.7.1	Definição	19
2.7.2	Propriedades	19
2.7.3	O Algoritmo de Buchberger	20
3	O Algoritmo	22
3.1	Ideia Geral	22
3.1.1	Modelando o problema	22
3.1.2	Resolvendo o problema	23
3.2	O Algoritmo de Bases de Gröbner	23
3.3	Validade do Algoritmo	24
3.3.1	Sempre há solução	24
3.3.2	Sempre há como continuar	24
3.3.3	O algoritmo sempre termina	25
4	Exemplo: Colorindo o Mapa do Áustria	26
4.1	Modelagem	26
4.2	Resolvendo	28
4.3	Observações	31
5	Conclusão	33

1 Introdução

1.1 O Problema

O problema da Coloração de Mapa consiste num plano subdividido em regiões contínuas (chamado de **mapa**), em que objetivo é colorir essas regiões conforme a seguinte regra: *regiões que compartilham mais do que um ponto de fronteira devem ser coloridas de cores distintas*. Esse quebra-cabeça pode até ter um enunciado simples, mas há muitas questões interessantes que podem ser levantadas a partir de um mapa qualquer, como se ele pode ser pintado com um número dado de cores, de quantas formas ele pode ser colorido, qual a quantidade mínima de cores, etc. A última dessas deu origem ao que é chamado na literatura como o **Teorema das Quatro Cores**, que diz o problema da Coloração de Mapa pode ser resolvido usando não mais do que *quatro cores* para todo mapa definido como anteriormente.



Figura 1: Mapa do Brasil colorido por quatro cores sem vizinhos de mesma cor

1.2 Primeiros Contatos

A conjectura do Teorema das Quatro Cores foi proposto pela primeira vez no dia 23 de Outubro de 1852, depois de Francis Guthrie, matemático e botanista sul-africano, enquanto tentava colorir o mapa de condados da Inglaterra, notar que quatro cores eram suficientes para pintar as regiões. Após esse resultado, ele contatou seu irmão, Frederick, também matemático, para contar sobre o que acabara de descobrir. Este, intrigado porém incapaz de provar naquele momento o que tinha acabado de ver, contatou Augustus De Morgan, do qual era estudante, e também não obteve uma solução. Anos depois, em 1878, Cayley, que soubera da conjectura também por De Morgan, fez uma pergunta à Sociedade Matemática de Londres questionando sobre se já haviam resolvido o problema de Guthrie. Pouco tempo depois, Cayley publicaria um artigo sobre as dificuldades de provar o Teorema.

1.3 A “Prova” de Kempe

O primeiro a publicar uma demonstração para o problema foi Alfred Bray Kempe, um advogado de Londres que estudou matemática com Cayley em Cambridge. Ele anunciou no dia 17 de Julho de 1879 que havia encontrado uma prova para a Conjectura das Quatro Cores. No mesmo ano, sob sugestão de Cayley, Kempe publicou sua demonstração no *American Journal of Mathematics*.

Mesmo que a frase “Indução Matemática” não apareça no paper de Kempe, o estilo de demonstração utilizado por ele foi basicamente indução no número de regiões. A base da indução era óbvia, como a maioria das bases de um processo indutivo: Qualquer mapa com 4 quatro ou menos regiões pode ser colorido com no máximo 4 cores. Para o passo indutivo, suponha que todo mapa com n regiões possa ser pintado com no máximo quatro cores e seja M um mapa com $n+1$ regiões. Kempe mostrou que M deve conter ao menos uma região com cinco ou menos vizinhos. Chame essa região de X e considere $M-X$, o mapa M “recortando” a região X pra fora. $M-X$ é um mapa de n regiões que, por hipótese, pode ser colorido por no máximo quatro cores. Feito isso, voltamos ao mapa original M que tem n regiões pintadas, por exemplo, de vermelho, amarelo, azul e verde, e a região X ainda descolorida. O objetivo de Kempe era reduzir (se necessário) o número de cores usadas nas regiões vizinhas a X , a fim de ter uma das quatro cores “livre” para a região ainda descolorida. Daí, ele dividiu o este problema em casos, dispensando rapidamente os mais simples. Primeiramente, se X tiver menos de três vizinhos, é muito claro que existirá uma cor livre para a região X . Agora, se X tiver quatro ou cinco regiões vizinhas, Kempe separou os casos em que as quatro cores são usadas nelas:

Caso 1: X adjacente a exatamente quatro regiões, todas de cores diferentes.

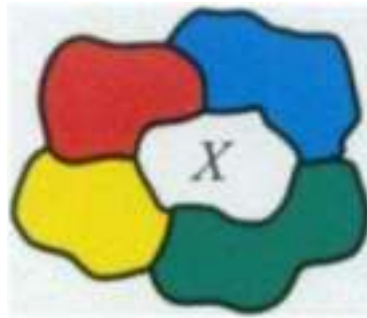


Figura 2: Exemplo de ocorrência do Caso 1

Caso 2: X adjacente a exatamente cinco regiões, coloridas de quatro cores diferentes.

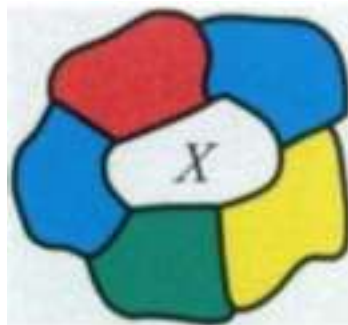


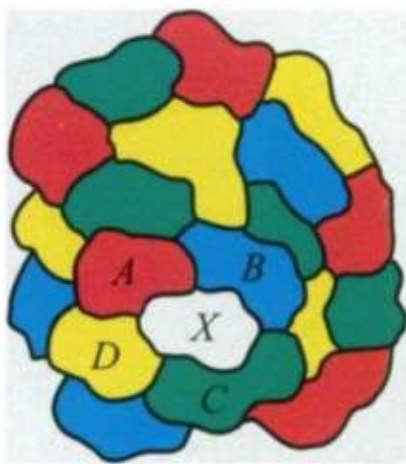
Figura 3: Exemplo de ocorrência do Caso 2

Para lidar com esse casos, Kempe usou o argumento que hoje é conhecido como o *Método das Cadeias de Kempe*. A noção de *cadeia* de Kempe era basicamente uma sequência de regiões adjacentes pintadas com duas cores específicas. O que ele notou foi que, ao mudar as cores das regiões de uma cadeia, a validade da coloração não é afetada. Agora mostraremos o argumento de Kempe para os dois casos.

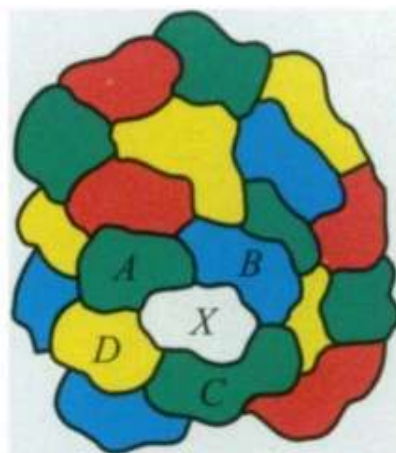
Para o primeiro caso, primeiro nós chamamos os 4 vizinhos de X de A , B , C e D . Então, Kempe considerou os seguintes subcasos:

Subcaso 1.1: As regiões A e C pertencem a cadeias verde-vermelha diferentes.

Neste caso, o que foi observado por Kempe foi que ele podia escolher umas das regiões, por exemplo A , e permutar as cores da cadeia verde-vermelha à qual A pertence (tornando as regiões vermelhas em verdes e vice-versa), tornando A verde e deixando a cor vermelha livre para X .



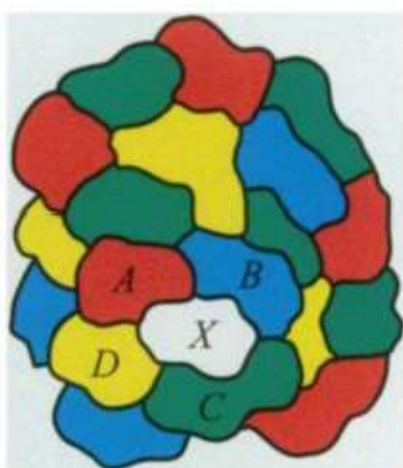
(a) Exemplo de mapa no Subcaso 1.1



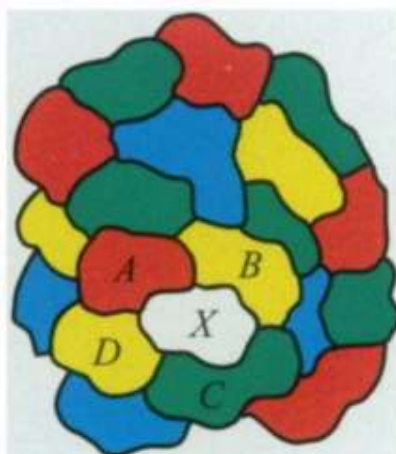
(b) Coloração depois da permutação de cores da cadeia de A

Figura 4: A troca de cores deixando uma cor livre para X

Subcaso 1.2: As regiões A e C pertencem à mesma cadeia verde-vermelha (ver Figura 5a). Kempe observou nesse caso que a cadeia verde-vermelha de A a C isolava B de D , impedindo que eles pertencessem à mesma cadeia amarela-azul. Assim, podemos alternar as cores da cadeia de B , por exemplo, e reduzir as cores em volta de X , como no Subcaso 1.1 (ver Figura 5b).



(a) Exemplo no Subcaso 1.2



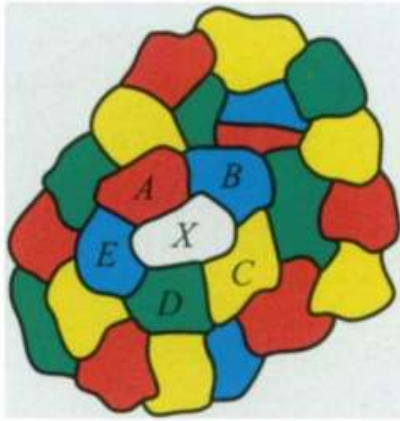
(b) Trocamos as cores da cadeia azul-amarela de B para deixar a cor azul livre para X

Figura 5: Resolução do Subcaso 1.2.

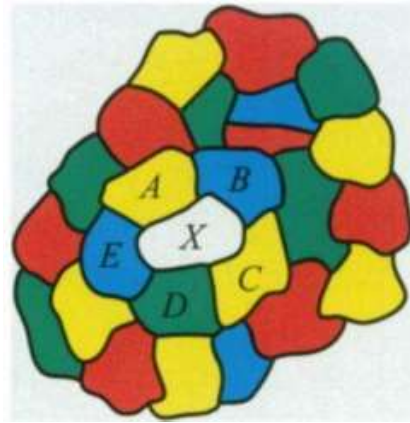
Para o Caso 2, vamos chamar as regiões que cercam X de A , B , C , D e E . Kempe dividiu a situação novamente em subcasos:

Subcaso 2.1: A e C pertencem a cadeias vermelha-amarela diferentes (ver Figura 6a) ou A e D pertencem a cadeias verde-vermelha diferentes.

No caso em que uma das duas coisas acima acontecem, podemos proceder como no Subcaso 1.1: Trocar as cores da cadeia vermelha-amarela de A deixando o vermelho livre para X (ver Figura 6b) ou trocar as cores da cadeia verde-vermelha de A , liberando também a cor vermelha.



(a) Exemplo no Subcaso 2.1

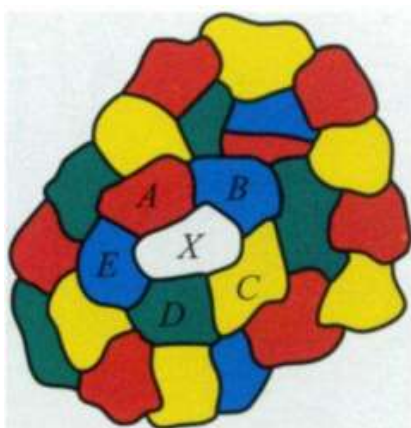


(b) Trocamos as cores da cadeia vermelha-amarela de A para deixar a cor vermelha livre para X .

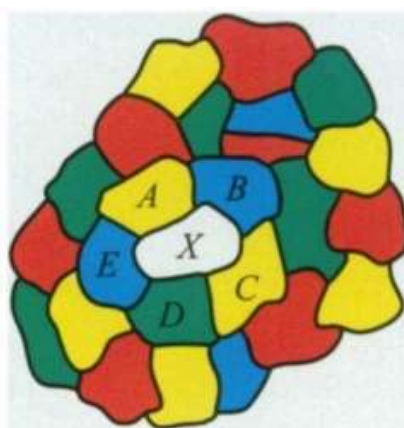
Figura 6: Resolução do Subcaso 2.1.

Subcaso 2.2: As regiões A e C pertencem à mesma cadeia vermelha-amarela e as regiões A e D pertencem à mesma região verde-vermelha (ver Figura 7a).

Neste último caso, o processo de Kempe para reduzir o número de cores em volta de X continha uma falha sutil. Para esta situação, Kempe observou corretamente que as duas regiões separavam B de E , o que significava que a região azul-verde de B era diferente da qual D e E pertenciam, e que a região azul-amarela de E era diferente da que B e C estavam contidas. Portanto, para reduzir o número de cores usadas nas regiões vizinhas de X , Kempe então trocou as cores da região verde-azul de B e da região azul-amarela de E , tornando B verde e E amarela, assim liberando a cor azul para X (ver Figura 7b).



(a) Exemplo no Subcaso 2.2



(b) Mapa depois de feitas as trocas de cores.

Figura 7: 'Resolução' do Subcaso 2.2.

1.4 O contraexemplo de Heawood

Infelizmente para Kempe, a solução dada por ele não funciona para qualquer mapa descrito como no Subcaso 2.2. Em 1890, Percy J. Heawood, matemático britânico, construiu um mapa onde o processo de Kempe falharia. O erro sutil era a possibilidade da região azul-verde de *B* tocar a região azul-amarela de *E*. O que Heawood notou foi que, quando isso acontece, uma troca de cores impede a outra de ser possível sem infringir a regra dos vizinhos terem cores diferentes. Note na Figura 8 que a cadeia verde-azul de *B* compartilha fronteira com a região

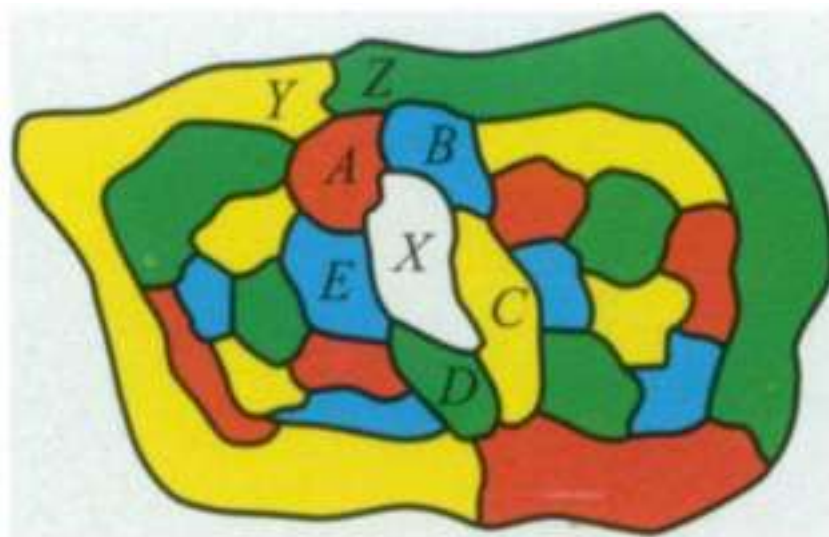


Figura 8: O mapa que impossibilita o processo de Kempe de funcionar.

azul-amarela de *E*. Quando tentamos fazer ambas as trocas de cores sugeridas por Kempe, as regiões vizinhas *Y* e *Z* recebem a mesma cor azul, tornando a coloração inviável.

Apesar de ter encontrado um contraexemplo para a solução de Kempe, Heawood não foi capaz de provar que quatro cores eram suficientes para colorir um mapa plano. Entretanto, ele provou o Teorema das Cinco Cores, ou seja, demonstrou que para colorir um mapa plano não é necessário mais do que cinco cores para ser possível cumprir a regra de que regiões que compartilhem uma fronteira maior que um ponto sejam coloridas de cores diferentes. Além disso, Heawood contribuiu para vários problemas semelhantes, como a quantidade mínima de cores para se pintar um mapa sobre alguns tipos de superfícies fechadas, como a esfera.

1.5 Desfecho do Teorema

Após 124 anos de sua conjectura, em 1976, o Teorema das Quatro Cores finalmente teve uma solução. Kenneth Appel e Wolfgang Appel afirmaram ter conseguido provar o tão curioso teorema. Porém, tinha um detalhe sobre a prova que a difere das demonstrações padrões: ela contava com a ajuda de um computador, chamado IBM 360, que teve que fazer na ordem de bilhões de cálculos, trabalhando por 50 dias! Isso chamou bastante atenção da comunidade matemática na época, gerando bastante desconfiança, ainda mais pelo fato da prova ser longa demais para ser verificada por uma pessoa e sempre haver a possibilidade do computador ter cometido algum erro sutil. Porém, até hoje essa demonstração é aceita pela comunidade em geral, apesar de ainda ser polêmica, por ser baseada em uma quantidade enorme de cálculos feitos por um computador.

Motivados por essa dificuldade de analisar a demonstração de Haken e Appel, os matemáticos continuaram em busca de uma prova mais simples, que foi apresentada por Paul D. Seymour em 1994. Essa demonstração, que foi um trabalho conjunto de Seymour com Neil Robertson, Daniel P. Sanders e Robin Thomas, apesar de mais simples e exigir bem menos cálculos (qualquer pessoa com os programas e conhecimentos necessários conseguiria reproduzir a demonstração em um dia), também teve o auxílio de um computador. Outros trabalhos foram feitos nessa área, como o de Georges Gonthier, publicado em 2005. Porém, o problema de conseguir uma demonstração que não utilize um computador ainda está sem solução.

2 Teoria dos Ideais e Bases de Gröbner

Neste Capítulo, vamos reunir parte das definições e teoremas que dão base aos nossos estudos.

2.1 Anéis, Corpos e Domínios

Primeiramente, definiremos as estruturas algébricas que serão usadas aqui neste trabalho.

Definição 2.1 (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, também em X .*

Exemplos de operações podem ser facilmente encontrados, como a soma e multiplicação em \mathbb{N} . Um exemplo de uma regra que não é uma operação é a subtração em \mathbb{N} , pois o resultado da subtração de dois números naturais nem sempre é um número natural. Definido isso, vamos à primeira definição fundamental deste trabalho.

Definição 2.2 (Anel). *Um conjunto não vazio A é um **anel** quando estão definidas nele duas operações, chamadas de **adição** (representada por $+$) e **multiplicação** (representada por \cdot ou simples justaposição dos elementos multiplicados), que satisfazem as seguintes propriedades:*

- para todo $a, b, c \in A$,

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

$$a + b = b + a$$

$$a(bc) = (ab)c$$

$$ab = ba$$

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

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

$$a + 0 = a$$

$$a \cdot 1 = a$$

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

$$a + (-a) = 0 \tag{1}$$

Note que, entre as propriedades do primeiro ponto, estão a exigência de que as operações no anel sejam *comutativas*. Um anel em que as operações são comutativas é chamado de *anel comutativo*. Porém aqui neste texto, chamaremos apenas de anel.

Os elementos especiais 0 e 1 são conhecidos como *elementos neutros* da adição e multiplicação, respectivamente. Já o elemento $(-a)$ definido na última propriedade é chamado de *simétrico* de a . Existe uma definição parecida com a de simétrico relacionado à multiplicação, que chamamos de *inverso*. Semelhante à adição, a inverso a' de $a \in A$ é um elemento de A tal que $aa' = 1$.

Geralmente, não são todos os elementos de um Anel têm inversa. Por exemplo, em \mathbb{Z} os únicos elementos que têm inversa são o 1 e o -1 .

Definição 2.3 (Corpo). *Um anel A é um **corpo** quando todos os elementos não nulos de A admitem inverso.*

Apesar de o conjunto \mathbb{Z} não ser um corpo, ele se enquadra em uma outra classe importante dos anéis, que são os *domínios*.

Definição 2.4 (Domínio). *Um anel A é um domínio se, para todo $a, b \in A$:*

$$ab = 0 \iff a = 0 \vee b = 0$$

2.2 Ideais

A noção de ideal é uma generalização de múltiplo estendida para conjuntos.

Definição 2.5 (Ideal). *Um subconjunto I de um anel A é um **ideal** se satisfaz as seguintes propriedades:*

- $0 \in I$;
- $a, b \in I \implies a + b \in I$;
- $a \in I, b \in A \implies ab \in I$.

Essas propriedades lembram os fatos de que 0 é múltiplo de qualquer natural, a soma dos dois múltiplos de um número também é um múltiplo dele, e que um múltiplo de um múltiplo de um número também é divisível por ele.

2.3 Anéis de polinômios

Aqui vamos definir um tipo especial de anel que será muito usado no próximo capítulo.

Definição 2.6 (Anel de polinômios). *Um anel de polinômios $A[x]$ é um conjunto com elementos da forma*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \quad (2)$$

com a soma e produto usuais para polinômios.

Para polinômios multivariados a definição acima pode ser usada recursivamente, como feito a seguir:

$$A[x_1, \dots, x_n] = A[x_1, \dots, x_{n-1}][x_n]$$

ou seja, tratando os polinômios de n variáveis como um polinômio de uma variável com coeficientes dependendo das outras $n - 1$ variáveis. A partir da próxima seção, considere K um domínio.

2.4 Ideais de Polinômios

A definição de um ideal polinomial é bem simples de fazer dadas as definições 2.5 e 2.6. Basicamente, é um subconjunto de $A[x_1, \dots, x_n]$ que satisfaz as propriedades de um ideal.

Para um ideal, podemos definir o que seria um conjunto de geradores para ele.

Definição 2.7 (Gerador). *Um subconjunto S de um ideal I em A é um gerador desse ideal se, para todo $x \in I$ existem $c_1, \dots, c_n \in A$ tais que*

$$c_1 s_1 + c_2 s_2 + \cdots + c_n s_n = x, \quad s_i \in I \quad (3)$$

Usaremos neste trabalho alguns resultados importantes sobre geradores, como o Teorema de Bases de Hilbert, demonstrado na seção 5.1 do livro do S. C. Coutinho [3].

2.5 Ordem Monomial

Um problema importante de polinômios multivariados é como ordenar seus monômios. No caso univariado, isso é bem fácil de se fazer, bastando ordenar pelo grau. Já quando aumentamos a dimensão, pode ocorrer de monômios diferentes terem o mesmo grau. Nessa

seção, vamos apresentar algumas formas de ordenar monômios multivariados. Representaremos os monômios aqui como x^α , onde α é um vetor de expoentes para $x = x_1, \dots, x_n$ (por exemplo, $x^{(5,3,8)} = x_1^5 x_2^3 x_3^8$).

- **Ordem Lexicográfica:** Dizemos que $x^\alpha >_{lex} x^\beta$ quando a primeira entrada não nula de $\alpha - \beta$ é positiva. Por exemplo, $x^5 y >_{lex} x^4 y^3$, pois o grau de x é maior no primeiro monômio. Observe que o grau do segundo monômio é maior apesar da ordem.
- **Ordem Lexicográfica Graduada:** Dizemos que $x^\alpha >_{glex} x^\beta$ quando $|a| > |b|$ ou $|a| = |b|$ e a primeira entrada não nula de $\alpha - \beta$ é positiva. Por exemplo, $x^9 y^5 >_{glex} x^7 y^7$ e $x^4 y^3 >_{glex} x^5 y$, apesar da ordem ser contrária em $>_{lex}$ neste último.
- **Ordem Lexicográfica Graduada Reversa** Dizemos que $x^\alpha >_{grlex} x^\beta$ quando $|a| > |b|$ ou $|a| = |b|$ e a última entrada não nula de $\alpha - \beta$ é negativa. Por exemplo, $x^3 y^3 <_{grlex} x^5 y$, pois os graus são iguais e o último expoente (o de y) é menor no segundo monômio.

Algumas propriedades podem ser destacadas, como:

- As ordens são totais;
- $x^\alpha > 1$ para todo $\alpha \neq 0$;
- Se $p > q$ e r são monômios, $pr > qr$ para todo $r \neq 0$.

As demonstrações e explicações dessas três propriedades estão bem detalhadas na Seção 4.2 do livro do S. C. Coutinho [3].

Definido o que é uma ordem monomial, podemos definir, agora no âmbito multivariado, o termo inicial de um polinômio.

Definição 2.8 (Termo Líder ou Termo Inicial). *O termo inicial do polinômio f em relação à ordem $>$ (denotado por $\text{in}(f)$) é o termo de f com maior suporte (parte restante do termo tirando o coeficiente) com respeito a $>$.*

Essa definição será útil para o algoritmo de divisão que será exibido a seguir.

2.6 Divisão de Polinômios Multivariados

Algoritmo 1 (Divisão de Polinômios Multivariados). *Dados polinômios f e g_1, \dots, g_s de $K[x_1, \dots, x_n]$, ordenados sob uma ordem monomial $>$, algoritmo tem como saída polinômios q_1, \dots, q_s e r tais que*

$$f = q_1 g_1 + q_2 g_2 + \dots + q_s g_s + r$$

e

- $r = 0$, ou
- nenhum monômio de r é divisível por nenhum dos termos iniciais $in(g_1), in(g_2), \dots, in(g_s)$.
- **Etapa 1:** Inicialize $F = f$, $Q_1 = Q_2 = \dots = Q_s = 0$ e $R = 0$
- **Etapa 2:** Enquanto $F \neq 0$, verifique se existe algum inteiro i entre 1 e s tal que $in(g_i)$ divida $in(f)$. Se existir, escolha j como o menor deles e faça

$$Q_j = Q_j + \frac{in(F)}{in(g_j)}$$

$$F = F - \frac{in(F)}{in(g_j)}$$

$$R = R + in(F)$$

deixando as demais variáveis inalteradas; se tal i não existir, faça

$$F = F - in(F);$$

$$R = R + in(F).$$

- **Etapa 3:** Retorne Q_1, \dots, Q_s como os quocientes e R como o resto.

Mais detalhes da construção do algoritmo estão disponíveis na seção 4.4 do livro do S. C. Coutinho [3].

Apesar do algoritmo funcionar para o objetivo dele, há algo curioso que pode acontecer: o resto dado pelo algoritmo pode ser diferente de zero mesmo se f for uma combinação polinomial dos divisores. Um exemplo simples de se observar esse caso é quando $f = 2xv + y - v$, $g_1 = xv - yu + v$ e $g_2 = xv + yu + y - 2v$. Veja que $f = g_1 + g_2$, porém no algoritmo de divisão, por $in(f) = 2 \cdot in(g_1)$, teremos já no primeiro passo, que $Q_1 = 2 > 1$, que seria o resultado esperado. Continuando por esperança, vemos que $f - 2g_1 = 2yu + y - 3v$ e que o termo inicial desse resto não divide nenhum dos termos iniciais dos g_i 's, o que fará o algoritmo alterar o resto para um polinômio diferente de zero. A consequência disso é de que para descobrir se um certo f pertence a um ideal gerado por g_1, \dots, g_s não é suficiente efetuar a divisão pelos geradores e esperar resto 0. Para resolver esse problema, vamos definir um conjunto de geradores especiais, como veremos a seguir.

2.7 Bases de Gröbner

2.7.1 Definição

Seja I um ideal e $>$ uma ordem monomial de $K[x_1, \dots, x_n]$. O *ideal inicial* $\text{in}(I)$ de I é o ideal de $K[x_1, \dots, x_n]$ gerado por $\text{in}(f)$ para cada $f \in I$. Uma coisa que pode ser questionada é se $\text{in}(g_1), \dots, \text{in}(g_n)$ geram $\text{in}(I)$ quando g_1, \dots, g_n geram I . A resposta é nem sempre, e quando acontece, damos um nome especial para esses geradores.

Definição 2.9 (Base de Gröbner). *Um subconjunto $G \subset I$ é uma **Base de Gröbner** de I se $\text{in}(I)$ é gerado por $\text{in}(g)$ para cada $g \in G$.*

Note que a definição acima não exige que G seja um conjunto de geradores de I . Porém, se J é o ideal gerado pelos elementos de G , podemos concluir a partir da definição de Bases de Gröbner que $J \subseteq I$ e $\text{in}(J) = \text{in}(I)$. A proposição a seguir implica que, sob essas circunstâncias, $I = J$, de modo que os elementos de G geram I . Vamos usar abaixo que toda ordem monomial é uma boa ordem.

Proposição 2.1. *Sejam $J \subseteq I$ ideais de $K[x_1, \dots, x_n]$. Se $\text{in}(I) = \text{in}(J)$, então $J = I$*

Demonstração. Suponha, por absurdo, que $J \neq I$. Como $>$ é uma boa ordem, então o conjunto I/J contém um elemento f tal que $\text{in}(f)$ é mínimo com respeito a $>$. Porém, como $\text{in}(I) = \text{in}(J)$, temos que $\text{in}(f) \in \text{in}(J)$. Portanto, existe $g \in J$ com $\text{in}(g) = \text{in}(f)$. Mas isso implica que $\text{in}(f) > \text{in}(f - g)$. Assim, pela minimalidade de f em I/J , devemos ter $f - g \in J$. Como $g \in J$, isto implica que $f = (f - g) + g \in J$, o que contradiz a hipótese feita sobre J e completa a demonstração. \square

Agora sabemos que uma Base de Gröbner de I gera I . Usaremos este fato importante na seção seguinte.

2.7.2 Propriedades

Proposição 2.2. *Seja I um ideal de $K[x_1, \dots, x_n]$ e G uma Base de Gröbner para I . Então, $f \in I$ se e somente se o resto da divisão de f por G é 0.*

Demonstração. Como G gera I , é claro que se $R_G(f) = 0$, então $f \in I$. Vamos provar a recíproca. Suponha, por contradição, que $f \in I$, mas que $R_G(f) \neq 0$. Neste caso, como $f - r \in I$, temos que $r \in I$. Portanto, $\text{in}(r) \in \text{in}(I)$. Logo, pela definição de Bases de Gröbner, $\text{in}(r)$ é divisível por $\text{in}(g)$ para algum $g \in G$. Mas isso contradiz o fato do resto ser sempre reduzido. Concluimos que $r = 0$, o que prova a proposição. \square

Corolário 2.1. *Seja $G = \{g_1, \dots, g_s\}$ uma base de Gröbner e f um polinômio de $K[x_1, \dots, x_n]$. Então existe um único polinômio r tal que*

$$f = q_1g_1 + \dots + q_sg_s + r,$$

em que $q_1, \dots, q_s \in K[x_1, \dots, x_n]$ e nenhum monômio de r pertence ao ideal formado pelos termos iniciais dos g 's.

Demonstração. Suponha, por contradição, que também podemos escrever f da forma

$$f = q'_1g_1 + \dots + q'_sg_s + r'$$

em que, assim como no enunciado do corolário, $q'_1, \dots, q'_s \in K[x_1, \dots, x_n]$ e nenhum monômio de r' pertence ao ideal gerado pelos termos iniciais dos g 's. Subtraindo as expressões para f , temos

$$(q_1g_1 + \dots + q_sg_s + r) - (f = q'_1g_1 + \dots + q'_sg_s + r') = 0;$$

assim,

$$(q_1 - q'_1)g_1 + \dots + (q_s - q'_s)g_s + (r - r') = 0,$$

de onde concluímos que $(r - r') \in G$ e, pela Proposição 2.2, que o resto de $r - r'$ por G deve ser zero. Entretanto, por hipótese, nenhum monômio de r ou r' é divisível pelo termo inicial de algum $g \in G$, o que implica que o resto da divisão de $r - r'$ por G é o próprio $r - r'$. Portanto, $r - r' = 0$, como queríamos demonstrar. \square

2.7.3 O Algoritmo de Buchberger

Agora vamos mostrar o Algoritmo de Buchberger, método usado para calcular Bases de Gröbner a partir de um conjunto finito de geradores de um ideal. No algoritmo, usaremos o que chamamos de *S-polinômio*, que dados dois polinômios g_1 e g_2 , retorna

$$S(g_1, g_2) = \frac{\text{in}(g_2)}{\delta} g_1 - \frac{\text{in}(g_1)}{\delta} g_2,$$

onde $\delta = \text{mdc}(\text{in}(g_1), \text{in}(g_2))$. Esse polinômio tem como função produzir um polinômio cujo termo inicial não divida $\text{in}(g_1)$ e nem $\text{in}(g_2)$.

Algoritmo 2 (Algoritmo de Buchberger). *Seja $K[x_1, \dots, x_n]$ um anel de polinômios munido de uma ordem monomial $>$. Dado um subconjunto finito $S \subset K[x_1, \dots, x_n]$, algoritmo tem como saída uma Base de Gröbner do ideal gerado pelos polinômios de S no anel $K[x_1, \dots, x_n]$.*

- **Etapa 1:** Inicia $G = S$ e

$$P = \{(g, g') : g, g' \in G, g \neq g'\}.$$

- **Etapa 2:** Enquanto P não for vazio, repita:

- Escolha $(g, g') \in P$;
- Remova $(g, g') \in P$;
- Calcule o resto r do S -polinômio $S(g, g')$ por G ;
- Se $r \neq 0$, adicione r em G e acrescente a P todos os pares (h, r) com $h \in G$

- Pare e dê como saída os elementos de G .

Mostraremos abaixo um exemplo do Algoritmo de Buchberger em ação.

Exemplo 2.1. Calcular uma base de Gröbner para o ideal gerado pelos polinômios $g_1 = x_1^2$ e $g_2 = x_1x_2 + x_2^2$:

- Inicializamos $G = \{g_1, g_2\}$ e $P = \{(g_1, g_2)\}$;
- Escolhemos e removemos (g_1, g_2) de P ;
- Calculamos $S(g_1, g_2) = \frac{x_1x_2}{x_1}x_1^2 + \frac{x_1^2}{x_1}(x_1x_2 + x_2^2) = -x_2^2$;
- Calculamos o resto de $S(g_1, g_2)$ por G , que dá $g_3 = -x_2^3$, e adicionamos em G , além de adicionar (g_1, g_3) e (g_2, g_3) em P ;
- Escolhemos e removemos (g_1, g_3) de P calculamos $S(g_1, g_3) = 0$;
- Passamos para (g_2, g_3) e calculamos $S(g_2, g_3) = -x_2^4$, que é divisível por G .
- Devolvemos $G = \{g_1, g_2, g_3\}$ como a base de Gröbner do ideal gerado por g_1 e g_2 .

Para mais detalhes sobre a construção e validade do algoritmo acima, veja a Seção 5.4 do livro do S.C. Coutinho [3].

3 O Algoritmo

Neste capítulo, vamos usar os conceitos exibidos na seção anterior, providas do livro do S. C. Coutinho [3] que servirão de base para boa parte dos argumentos feitos sobre o algoritmo a ser introduzido.

3.1 Ideia Geral

O conceito geral do nosso algoritmo é basicamente trazer o problema de escolher cores para regiões com certas restrições para a o campo da Álgebra. O objetivo principal dele é receber um mapa e entregar, para cada região, uma cor da qual ele deve ser colorida para a pintura ser válida. Vamos fazer isso trazendo as cores como valores possíveis para incógnitas, e produzir um sistema de equações polinomiais que restringirão esse espaço de possibilidades, formando nosso conjunto viável. Vale lembrar que a solução não é única e, portanto, nosso algoritmo vai retornar apenas uma delas.

3.1.1 Modelando o problema

Para modelar nosso problema, iremos usar um corpo específico: o \mathbb{Z}_5 , que é o anel dos inteiros módulo 5. Usar este corpo será essencial para nosso algoritmo por ter algumas propriedades, por exemplo:

- É um corpo muito simples de entender;
- Ele contém exatamente exatamente quatro elementos não nulos, que vamos usar para representar nossas cores;
- Todos os elementos não-nulos têm uma propriedade em comum: $x^4 = 1 \forall x \in \mathbb{Z}_5^*$.

Para construir o sistema de equações, vamos proceder da seguinte forma (vamos, a partir daqui, chamar o conjunto de regiões de V e o de adjacências de E):

- Primeiramente, nosso sistema terá uma incógnita para cada região, portanto $|V|$ incógnitas, e terá $|V| + |E|$ equações, como veremos posteriormente;
- Nós queremos que cada incógnita receba um valor não nulo. Para isso, usando a 3ª propriedade de \mathbb{Z}_5 citada acima, colocaremos, para cada incógnita x_i , a restrição de que

$$x_i^4 - 1 = 0 \tag{4}$$

- Para as restrições de adjacências, usaremos que, além de, em \mathbb{Z}_5 ,

$$x^4 - y^4 = 0 \quad \forall x, y \neq 0$$

também valer, por fatoração

$$x^4 - y^4 = (x - y)(x^3 + x^2y + xy^2 + y^3)$$

. Assim, para ter $x \neq y$, deve ser satisfeito que

$$x^3 + x^2y + xy^2 + y^3 = 0 \tag{5}$$

para todo x, y adjacente no mapa.

Assim, temos o nosso sistema de equações completo e podemos pensar na resolução dele.

3.1.2 Resolvendo o problema

Agora, com o problema modelado, vamos tratar da solução dele. O que temos é um sistema de equações polinomiais não-lineares com várias incógnitas. A primeira vista, isso pode parecer bem assustador, mas felizmente temos uma boa ferramenta para resolver sistemas de equações de nosso interesse: as Bases de Gröbner.

O nosso método de resolução vai ser criar um ideal que será gerado por todas as equações do sistema, calcular sua base de Gröbner e anular essa base, substituindo as variáveis por valores de maneira específica.

3.2 O Algoritmo de Bases de Gröbner

Por fim, chegamos ao algoritmo abaixo:

Algoritmo 3 (Algoritmo de Coloração de Mapas via Bases de Gröbner). *Seja M um mapa em que V é seu conjunto de regiões e $E = \{(i, j), i, j \in V, i \sim j\}$ seu conjunto de adjacências. O algoritmo retorna, para cada $i \in V$, um $x_i \in \{1, 2, 3, 4\}$ tal que $i \sim j \implies x_i \neq x_j$.*

1. Definimos o anel de polinômios $A = \mathbb{Z}[x_1, \dots, x_{|V|}]$.
2. Para cada $i \in V$, definimos o polinômio $p_i = x_i^4 - 1$;
3. Definimos, para cada $(i, j) \in E$, os polinômios $q_{ij} = x_i^3 + x_i^2x_j + x_ix_j^2 + x_j^3$;

4. Definimos $I \subset A$ como o ideal gerado por todos os p_i 's e q_{ij} 's;
5. Calculamos a base de Gröbner de I usando o Algoritmo de Buchberger e o armazenamos em gI ;
6. Identificamos, em $gI = \{b_1, \dots, b_n\}$, um polinômio univariado b_{k_1} ;
7. Anulamos ele substituindo x_{k_1} (sua única variável) por $x_1^* \in \{1, 2, 3, 4\}$ em ordem crescente (como é um número finito e pequeno de opções, não é custoso testar);
8. Substituímos x_{k_1} por seu novo valor em todo $b_i \in gI$;
9. Identificamos um próximo b_{k_2} univariado;
10. Repetimos os passos 9 e 10 para esse b_k ;
11. Fazemos os passos 11 e 12 até anular gI , o que acontecerá quando o $|V|$ -ésimo b_k for anulado.
12. A saída serão os valores de x_i , que representam as cores das quais as regiões correspondentes serão coloridas.

3.3 Validade do Algoritmo

3.3.1 Sempre há solução

Bom, como dito pelo Teorema das Quatro Cores, todo mapa plano dividido em regiões admite uma 4-coloração em que regiões vizinhas têm cores diferentes. Isso garante que existem x_1, \dots, x_n tais que o Ideal gerado pelos polinômios de nossa restrição se anule. Como gI representa o mesmo ideal, apenas trocando sua base, devemos ter que o núcleo de gI é igual ao núcleo de I , garantindo então uma solução não nula para o nosso sistema de equações após o cálculo da base de Gröbner.

3.3.2 Sempre há como continuar

Primeiro passo O cálculo da base de Gröbner utilizado pelo nosso algoritmo funciona de tal forma que sempre tenha um polinômio univariado no começo. A justificativa disso acontecer é que, no sistema original, os polinômios de maior grau são justamente as expressões da forma $x^4 - 1$, portanto eles são sempre escolhidos para fazerem parte da base de Gröbner do Ideal.

Passos consequentes Para os passos consequentes, o argumento também é simples. Quando colorimos uma região, eliminamos uma variável. Após isso, todos os polinômios bivariados do sistema que dependiam dela, mais especificamente as equações que modelam os vizinhos dessa região colorida que ainda não foram pintados (existe ao menos um, a não ser que o mapa esteja totalmente pintado, pois o mapa é conexo) se tornam univariados, tornando possível a continuidade do algoritmo selecionando uma dessas variáveis para o próximo passo.

3.3.3 O algoritmo sempre termina

Dado que o problema sempre tem uma solução e que, a cada passo do algoritmo, é colorida uma região, podemos afirmar com certeza que o algoritmo para, dada a finitude de regiões.

4 Exemplo: Colorindo o Mapa do Áustria

Para ilustrar e entender como nosso algoritmo funciona, vamos colorir o mapa dos estados austríacos, em referência à nacionalidade de Wolfgang Gröbner, cujos estudos dão base e nome a este trabalho. Este exemplo foi implementado usando o Singular [5], um sistema de álgebra computacional para cálculos polinomiais com ênfase em álgebra comutativa e não comutativa. O tempo de rodagem foi de alguns segundos, tornando viável a reprodução deste.

4.1 Modelagem

Para começarmos, precisamos entender como é o mapa. O primeiro passo é nomear os



Figura 9: Mapa dos estados da Áustria

estados e identificar os vizinhos. Com um pouco de trabalho e numerando os estados como 1 = Vorarlberg, 2 = Tirol, 3 = Salzburgo, 4 = Caríntia, 5 = Alta Áustria, 6 = Estíria, 7 = Baixa Áustria, 8 = Bungenland e 9 = Viena, temos que os pares de vizinhos são:

$$(1,2), (2,3), (2,4), (3,4), (3,5), (3,6), (4,6), (5,6), (5,7), (6,7), (6,8), (7,8), (7,9)$$

Depois disso, trabalhando no corpo \mathbb{Z}_5 temos que montar nosso sistema de equações que dará origem ao ideal. Como vimos no capítulo anterior, cada região i terá que ter um polinômio $x_i^4 - 1$ representando que esta região receberá uma 'cor' de 1 a 4 (que representaremos, respectivamente, por vermelho, verde, azul e amarelo), e cada adjacência (i, j) será modelada

como $x_i^3 + x_i^2 x_j + x_i x_j^2 + x_j^3$. Assim, nosso conjunto de equações a serem resolvidas é:

$$\begin{array}{ll}
x_1^4 - 1 = 0 & x_2^3 + x_2^2 x_4 + x_2 x_4^2 + x_4^3 = 0 \\
x_2^4 - 1 = 0 & x_3^3 + x_3^2 x_4 + x_3 x_4^2 + x_4^3 = 0 \\
x_3^4 - 1 = 0 & x_3^3 + x_3^2 x_5 + x_3 x_5^2 + x_5^3 = 0 \\
x_4^4 - 1 = 0 & x_3^3 + x_3^2 x_6 + x_3 x_6^2 + x_6^3 = 0 \\
x_5^4 - 1 = 0 & x_4^3 + x_4^2 x_6 + x_4 x_6^2 + x_6^3 = 0 \\
x_6^4 - 1 = 0 & x_5^3 + x_5^2 x_6 + x_5 x_6^2 + x_6^3 = 0 \\
x_7^4 - 1 = 0 & x_5^3 + x_5^2 x_7 + x_5 x_7^2 + x_7^3 = 0 \\
x_8^4 - 1 = 0 & x_6^3 + x_6^2 x_7 + x_6 x_7^2 + x_7^3 = 0 \\
x_9^4 - 1 = 0 & x_6^3 + x_6^2 x_8 + x_6 x_8^2 + x_8^3 = 0 \\
x_1^3 + x_1^2 x_2 + x_1 x_2^2 + x_2^3 = 0 & x_7^3 + x_7^2 x_8 + x_7 x_8^2 + x_8^3 = 0 \\
x_2^3 + x_2^2 x_3 + x_2 x_3^2 + x_3^3 = 0 & x_7^3 + x_7^2 x_9 + x_7 x_9^2 + x_9^3 = 0
\end{array}$$

Para finalizar o processo de modelagem e finalmente começar a coloração, nós definiremos I como o ideal gerado pelos 22 polinômios acima e calculamos sua base de Gröbner (nós usamos a função *std* do Singular [5] para isso), que é a seguinte:

$$\begin{array}{l}
gI[1] = x_6^2 + x_6 x_7 + x_7^2 + x_6 x_8 + x_7 x_8 + x_8^2 \\
gI[2] = x_5^2 + x_5 x_6 + x_5 x_7 + 4x_6 x_8 + 4x_7 x_8 + 4x_8^2 \\
gI[3] = x_3 x_4 + x_4^2 + 4x_3 x_5 + x_4 x_6 + x_5 x_7 + 4x_6 x_8 + 4x_7 x_8 + 4x_8^2 \\
gI[4] = x_3^2 + x_3 x_5 + x_3 x_6 + 4x_5 x_7 + 4x_6 x_7 + 4x_7^2 \\
gI[5] = x_2^2 + x_2 x_3 + x_2 x_4 + 4x_3 x_6 + 4x_4 x_6 + x_6 x_7 + x_7^2 + x_6 x_8 + x_7 x_8 + x_8^2 \\
gI[6] = x_7^2 x_8 + x_7 x_8^2 + x_8^3 + 4x_7^2 x_9 + 4x_7 x_9^2 + 4x_9^3 \\
gI[7] = x_7^3 + x_7^2 x_8 + x_7 x_8^2 + x_8^3 \\
gI[8] = x_4^3 + x_4^2 x_6 + x_4 x_6^2 + 4x_6^2 x_8 + 4x_6 x_8^2 + 4x_8^3 \\
gI[9] = x_1^3 + x_1^2 x_2 + x_1 x_2^2 + 4x_2^2 x_4 + 4x_2 x_4^2 + x_4^2 x_6 + x_4 x_6^2 + 4x_6^2 x_8 + 4x_6 x_8^2 + 4x_8^3 \\
gI[10] = x_9^4 + 4 \\
gI[11] = x_8^4 + 4
\end{array}$$

4.2 Resolvendo

Nosso objetivo aqui é encontrar $x_1, \dots, x_9 \in \mathbb{Z}_5/\{0\}$ em que o ideal gI (consequentemente o ideal I), se anula. Para isso, faremos o caminho descrito pelo algoritmo da Seção 2.2, começando pelos polinômios de uma variável.

- Observe que há dois polinômios em gI que são univariados: $gI[10]$ e $gI[11]$. Isso indica que o algoritmo selecionou as variáveis x_8 e x_9 para serem preenchidas primeiro e independentemente. É fácil ver também que não há restrição de cor para estas duas regiões, o que é de se esperar. Como o algoritmo testa as cores em ordem crescente, ele escolherá $x_8 = 1$ e $x_9 = 1$.



Figura 10: Primeiro passo do algoritmo: ele pinta as regiões 8 e 9 de vermelho.

- Substituindo os valores de x_8 e x_9 nos polinômios de gI , podemos notar que $gI[6]$ se anula (que sorte!) e que $gI[7]$ fica univariado em x_7 . De fato, agora temos $gI[7] = x_7^3 + x_7^2 + x_7 + 1$. É bem tranquilo verificar que $gI[7] = 0$ para $x_7 \in \{2, 3, 4\}$. Escolhemos então $x_7 = 2$. O curioso aqui é que, mesmo sem olhar o mapa de fato, o algoritmo nos deu como opções para coloração da região 7 as mesmas alternativas que a gente teria se estivéssemos pintando no olho (ver Figura 11).
- Com x_7 definido, vamos agora para o próximo passo. Identificamos que o polinômio $gI[1] = x_6^2 + 3x_6 + 2$ só depende de x_6 . Novamente, é bem fácil testar, para os valores possíveis de x_6 , quais dele anulam $gI[6]$: são eles o 3 e o 4. O algoritmo então escolherá $x_6 = 3$, pintando o estado de Estíria de azul (ver Figura 12). Novamente, podemos ver as contas batendo: 3 e 4 (azul e amarela) eram justamente as cores disponíveis para a Estíria, dado que ela compartilha fronteira com Bungenland, que havia sido pintada de vermelho, e com a Baixa Áustria, que foi colorida de verde.



Figura 11: Segundo passo do algoritmo: ele pinta a Baixa Áustria de verde.



Figura 12: Terceiro passo do algoritmo: pintamos a Estíria de azul.

- Neste passo, ao fazer as contas, vemos que, com a escolha de x_6 , temos dois polinômios que agora dependem de uma só variável: $gI[2] = x_5^2 + 4$ e $gI[8] = x_4^3 + 3x_4^2 + 4x_4 + 2$. Para $gI[2]$, temos que as raízes são 1 e 4. Já para $gI[8]$, as raízes são 1, 2 e 4. Escolhemos, então, $x_4 = 1$ e $x_5 = 1$. Novamente, podemos ver pela Figura 13 que as regiões da Alta Áustria e Caríntia não são vizinhas e, condizendo com a realidade, o algoritmo pintou essas regiões independentemente.
- Nesse momento, temos $gI[4] = x_3^2 + 4x_3 + 3$ como o polinômio univariado, que tem como raízes os valores 2 e 4. Então, escolhemos $x_3 = 2$, pintando Salzburgo de verde.
- Finalmente, temos mais duas regiões a pintar, 1 e 2, e mais dois polinômios não nulos: $gI[5] = x_2^2 + 3x_2 + 2$ e $gI[9] = x_1^3 + x_1^2x_2 + x_1x_2^2 + 4x_2^2 + 4x_2 + 4$. Podemos anular $gI[5]$ com $x_2 = 3$, ficando com $gI[9] = x_1^3 + 3x_1^2 + 4x_1 + 2$. Por fim, $gI[9]$ tem como



Figura 13: Quarto passo: pintamos a Alta Áustria e a Caríntia de vermelho.



Figura 14: Quinto passo: pintamos Salzburgo de verde.

raízes 1, 2 e 4, onde ficamos com o 1, anulando todos os polinômios e encerrando o algoritmo com todas as regiões pintadas.



Figura 15: Sexto passo do algoritmo: colorimos Tirol de azul.



Figura 16: Último passo: colorimos Vorarlberg de vermelho.

4.3 Observações

Há coisas bem interessantes a se destacar sobre o exemplo acima:

- Os passos do algoritmo seguiram uma ordem plausível com a forma que uma pessoa pintaria o mapa na mão: escolheu uma região para ser pintada primeiro, de preferência nas extremidades do mapa, e foi colorindo os vizinhos dele com as cores disponíveis. A ordem de pintura varia com a ordem monomial escolhida para o nosso anel de polinômios.
- Novamente destacamos que, em nenhum momento da pintura, houve a possibilidade de ocorrer de estados vizinhos obterem a mesma cor, graças à boa modelação do problema.
- Excetuando o cálculo da base de Gröbner do conjunto de polinômios, que será citado

posteriormente, as operações e passos são bem simples de fazer, podendo, em casos pequenos como esse, ser feitos a papel e caneta.

- O algoritmo encontrou, para o mapa escolhido, uma coloração com três cores. Não são todos os mapas que podem ser coloridos assim, mas este era e foi assim pintado. Analisando o processo de escolha das cores, vemos que o algoritmo é bem econômico quanto à quantidade de cores utilizada, pois ele só iria utilizar uma quarta cor se somente ela estivesse disponível em algum passo.
- O único ponto negativo deste algoritmo, que é suficiente para ele não poder ser usado na prática para mapas grandes, é justamente o cálculo da base do Gröbner do ideal gerado pois, como foi mostrado no livro S. C. Coutinho [3], o limitante superior do grau da base de Gröbner é exponencial em função do número de regiões.

5 Conclusão

O que podemos tirar desse trabalho é que a Álgebra é um lugar rico em recursos teóricos que pode ser ainda bastante explorado para aplicações, mesmo que pareça mais ser um tema de Matemática Pura, cheio de definições e teoremas. Aqui, apesar do nosso algoritmo não ser algo que será tão útil para resolver problemas reais, pode ser um início de uma investigação maior, como foi a tentativa de Kempe para a solução do Teorema das Quatro Cores que temos hoje, para formas diferentes de se colorir um mapa plano usando ferramentas simples e fáceis de entender. E mesmo que a teoria de Bases de Gröbner seja da área de Geometria Algébrica e Álgebra Computacional, ela pode ter sido usada para tratar de assuntos distantes de seu foco, como visto com o desenvolvimento do nosso algoritmo.

Novamente, vale ressaltar que o objetivo final deste trabalho não foi encontrar algo mirabolante ou inovador, mas sim se enriquecer, ao menos um pouco mais, intelectualmente sobre as possibilidades de alcance de um tema sobre outras áreas, mesmo que não de forma tão impactante e, além disso, explorar muito mais desse ramo chamado Álgebra, área tão antiga e importante da Matemática que particularmente gosto muito e que teve a contribuição de tantos matemáticos importantes.

6 Referências

- [1] SIPKA, Timothy. Alfred Bray Kempe's "Proof" of the Four-Color Theorem. **www.maa.org**, 2002. Disponível em <<https://www.math.wisc.edu/svs/475/kempe.pdf>>. Acesso em: 25/11/2020
- [2] GONTHIER, Georges. Formal Proof - The Four-Color Theorem. **www.ams.org**, 2008. Disponível em <<http://www.ams.org/notices/200811/tx081101382p.pdf>>. Acesso em: 25/11/2020.
- [3] COUTINHO, S. C. **Polinômios e Computação Algébrica**. 1ª Ed. Rio de Janeiro: IMPA, 2012.
- [4] FRITSCH, Rudolf; FRISTCH, Gerda, **The four color theorem**: history, topological foundations, and the idea of proof, Springer-Verlag New York, Inc., 1998.
- [5] Decker, W.; Greuel, G.-M.; Pfister, G.; Schönemann, H.: SINGULAR 4-1-2 — A computer algebra system for polynomial computations. <http://www.singular.uni-kl.de> (2019).