A construção de um quasi-corpo como motivação ao estudo do q-cálculo

Caroline Mazini Rodrigues **Cristiane Nespoli**

E-mail: carolinemazinirodrigues@hotmail.com, nespoli.cristiane@gmail.com.

Detpo de Matemática e Computação, Universidade Estadual Paulista -UNESP, Presidente Prudente, SP

Amarísio da Silva Araújo

E-mail:amarisio5@gmail.com

Depto de Matemática, Universidade Federal de Viçosa - UFV, Viçosa, MG

RESUMO

Este trabalho teve como motivação o tópico inicial do minicurso intitulado *O q-Cálculo: Uma Introdução*, oferecido durante o V Programa de Verão do PosMAC/ UNESP. Neste tópico foi apresentado o seguinte problema motivador do curso: calcular a transformada de Fourier da seguinte função:

$$f_q(x) = \begin{cases} \alpha_q^-[1-\frac{1-q}{3-q}(\frac{x}{\sigma})^2]^{\frac{1}{q-1}}, -\infty < q < 1 \\ \alpha_q^+[1-\frac{1-q}{3-q}(\frac{x}{\sigma})^2]^{\frac{1}{1-q}}, 1 < q < 3 \end{cases} \quad (1)$$

onde q é um número real (parâmetro de extensividade) e α^- e α^+ são constantes (dependem de q).

A função acima é conhecida como distribuição de *Tsallis* (com média 0 e variância σ^2), e aparece na mecânica estatística não-extensiva. Sabe-se que, quando $q \to 1$, a distribuição de Tsallis converge para a distribuição Gaussiana com média 0 e variância σ^2.

Considerou-se o caso $1 < q < 3$. Para se calcular a transformada de Fourier da distribuição de Tsallis, deve-se resolver a seguinte integral imprópria:

$$\varphi_T(\omega) = \int_{-\infty}^{+\infty} e^{i\omega x}\alpha_q^+[1-(\frac{1-q}{3-q})(\frac{x}{\sigma})^2]^{\frac{1}{1-q}}dx \quad (2)$$

Esta é uma tarefa bastante árdua, ainda que seja fixado um valor para o parâmetro q. Assim, é interessante recorrermos ao cálculo da transformada de Fourier da distribuição Gaussiana mencionada anteriormente, para se ter uma ideia de como atacar o problema acima. Neste caso, temos:

$$\varphi_G(\omega) = \int_{-\infty}^{+\infty} e^{i\omega x}\frac{1}{\sqrt{2\pi\sigma^2}}e^{\frac{-\frac{x}{\sigma}^2}{2}}dx = e^{-\frac{\sigma^2\omega^2}{2}} \quad (3)$$

Considerando o limite fundamental $\lim_{x\to 0}(1+nx)^{\frac{1}{n}} = e^x$ e a convergência da distribuição de Tsallis para a Gaussiana, a expressão $(\frac{1-q}{3-q})(\frac{x}{\sigma})^2]^{\frac{1}{1-q}}$ em 2 sugere a definição de uma nova função exponencial, e_q^x, denominda *q-exponencial* dada por: $e_q^x = [1+(1-q)x]^{\frac{1}{1-q}}$. Daí, a integral em 2 se torna: $\varphi_T(\omega) = \int_{-\infty}^{+\infty} e^{i\omega x}\alpha_q^+ e_q^{[\frac{1}{q-3}(\frac{x}{\sigma})^2]}dx$.

Percebeu-se, para continuidade da resolução do problema, a necessidade da definição de novas operações que garantissem a preservação das propriedades básicas da função exponencial. Uma nova adição (*q-soma*), $\boxplus$, foi definida por $x\boxplus y = x+y+(1-q)xy$, garantindo a propriedade $e_q^x.e_q^y = e_q^{x\boxplus y}$. Para se definir uma nova operação de multiplicação (*q-multiplicação*), definiu-se, antes, uma *q- função logaritmo*, dada por $ln_q^x = \frac{x^{1-q}-1}{1-q}$, a partir da qual se chegou à *q-multiplicação*,$\boxtimes$, dada por $x\boxtimes y = [x^{1-q}+y^{1-q}-1]^{\frac{1}{1-q}}$, satisfazendo a propriedade $ln_q x + ln_q y = ln_q x\boxtimes y$.

Com estas duas operações, era natural querer investigar se a estrutura algébrica obtida, cf.[Borges (2004)] $R_q(\boxplus,\boxtimes)$ (o conjunto dos números reais com as duas *q-operações*) constituia um *Corpo*. Conclui-se que a distributividade não é satisfeita, sendo, então, o $R_q(\boxplus,\boxtimes)$ classificado como um *Quasi-corpo*.

Feita esta discussão algébrica, voltou-se ao problema da resolução da integral em 2 e introduziu-se o conceito de *q-Transformada de Fourier* baseado nas *q-operações* e na *q-exponencial*. Este trabalho pretende, portanto, apresentar todos os conceitos apresentados na caracterização do *Quasi-Corpo* $R_q(\boxplus,\boxtimes)$ e a ligação entre o problema de motivação do referido minicurso e a teoria do *q-Cálculo*.

Referências

[Borges (2004)] Borges, E. P., "A possible deformed algebra and calculus inspired in nonextensive thermostatistics ", in *Physica A: Statistical Mechanics and its Applications*, Vol. 340, 1, 95- 1011.

Álgebras de Lie de grupos algébricos

Adriana Rodrigues da Silva **Mateus Alves Melo***
Faculdade de Matemática, UFU
Av. João Naves de Ávila 2121
38408-100, Uberlândia, MG
E-mail: adriana@famat.ufu.br m2alvesmelo@hotmail.com

RESUMO

Seja S um subconjunto de $\mathbb{R}^k$. Um vetor v é dito ser **tangente** a S num ponto x se houver um caminho diferenciável $\varphi(t)$ inteiramente contido em S, tal que $\varphi(0) = x$ e $\varphi'(0) = v$.

Vamos introduzir um elemento infinitesimal ε. Trabalharemos com a regra $\varepsilon^2 = 0$ para definir o espaço vetorial $E = \{a + b\varepsilon \mid a, b \in \mathbb{R}\}$. Dado um ponto x de $\mathbb{R}^k$ e um vetor $v \in \mathbb{R}^k$, a soma $x + v\varepsilon$ é um vetor com entradas em E que interpretamos intuitivamente como uma mudança infinitesimal em x, na direção de v.

Seja $I = \{f_\alpha\}_\alpha \subseteq \mathbb{R}[x_1, \ldots, x_k]$ uma coleção de polinômios. Se S é o lugar geométrico de zeros de f_α, ou seja, $S = \mathcal{Z}(I) = \{x \in \mathbb{R}^k \mid f\alpha(x) = 0,\ \forall f_\alpha \in I\}$, ele é chamado um **conjunto algébrico real**.

No caso em que S é um conjunto algébrico real, definido por equações polinomiais $f_\alpha(x) = 0$, um vetor v é chamado uma **tangente infinitesimal** a S em $x \in S$ se $f_\alpha(x + v\varepsilon) = 0$.

O **grupo geral linear** $GL_n(\mathbb{R})$ é formado pelas matrizes reais de ordem n com determinante não nulo. Todo subgrupo de $GL_n(\mathbb{R})$ definido por um sistema de equações polinomiais é dito um **grupo algébrico linear**.

Considere G um grupo algébrico linear. O espaço de vetores tangentes à G na matriz identidade I, é chamado a **álgebra de Lie** do grupo G. Denotamos $\mathcal{G} = T_I G$.

Nosso objetivo é descrever as álgebras de Lie de alguns grupos algébricos lineares.

Seja $G = SL_n(\mathbb{R})$, o grupo algébrico linear das matrizes de determinante 1. Então, $\mathcal{G}$ é formada pelas matrizes de traço nulo.

Se $G = O_n(\mathbb{R})$, isto é, o grupo das matrizes $A \in GL_n(\mathbb{R})$ tais que $A^t A = I$, então $\mathcal{G}$ é o espaço vetorial das matrizes $n \times n$ antissimétricas.

Uma vez que a álgebra de Lie $\mathcal{G}$ é isomorfa à álgebra dos campos vetoriais sobre G que são invariantes por translação, a estrutura infinitesimal do grupo G no elemento identidade é quase o suficiente para estudarmos a estrutura do grupo G.

Referências

[1] ARTIN, M., *Algebra*, Prentice Hall, 1991.

[2] BOREL, A., *Linear Algebraic Groups*, W. A. Benjamin, Inc., 1969.

[3] GROVE, L.C., *Classical Groups and Geometric Algebra*, Graduate studies in mathematics, v.39, 2001.

*Bolsista PETMAT - SESu/MEC

APLICAÇÃO DO MÉTODO DE FUNÇÕES GERADORAS NA SOLUÇÃO DE RELAÇÕES DE RECORRÊNCIA

Andréia Cristina Ribeiro **Wállef Januário P. da Silva***
Universidade Federal do Mato Grosso do Sul - CPAR
Avenida Pedro Pedrossian, n.º725, Bairro Universitário
79.500-000, Paranaíba - MS
E-mail: andreiaribeiro.mat@gmail.com wallef.silva@gmail.com

RESUMO

As aplicações da Análise Combinatória no dia-a-dia são realmente fascinantes, pois, basta um problema que envolve contagem (ou escolhas) para vermos esta teoria na sua resolução. Por exemplo, nas formas de escolher opções de roupas para sair, ou opções de pizza para comer, assim como, nas formas de distribuir presentes no final de ano, ou até mesmo num jogo de lançar dados, como no problema estudado por Galileu Galilei, onde achava que no lançamento de três dados equilibrados, do tipo cúbico, com faces numeradas de 1 a 6, obtinha-se a soma 9 ou 10 com a mesma frequência, o que na verdade não acontece. Basta verificar isto, utilizando a técnica de funções geradoras na solução da equação linear $x_1 + x_2 + x_3 = r$ onde $1 \leq x_i \leq 6$ com $i = 1, 2, 3$. Neste trabalho pretendemos apresentar a aplicação do método de funções geradoras na solução do problema de permutações caóticas de n elementos que são a quantidade de permutações das n letras a, b, c, ..., nas quais nenhuma delas ocupa sua posição original, isto é, i-ésima posição, denotado por D_n e dado pela expressão a seguir:

$$D_n = n! \sum_{i=0}^{n} (-1)^n \left(\frac{1}{n!}\right), \forall n \geq 1$$

Referências

[1] SANTOS, J.P.O.; MELLO, M.P.; MURARI, I.T.C. *Introdução à Análise Combinatória*. Rio de Janeiro. Editora Ciência Moderna. 2007.

[2] NOLIBOS, D. A.. *Relações de Recorrências e Aplicações, Dissertação*. Campinas, UNICAMP. 2010.

*Bolsista de Iniciação Científica PIBIC/PROPP

Apresentações de Grupos

Orientador: Prof. Dr. Kisnney E. de Almeida **Saimon de S. Rocha***

Licenciatura em Matemática, UEFS
Av. Transnordestina, S/N, Novo Horizonte
(75) 3161-8000, Feira de Santana, BA
E-mail: kisnney@gmail.com saimonhp@gmail.com

RESUMO

Este trabalho é fruto de estudos realizados em um projeto de iniciação científica realizado no campus da Universidade Estadual de Feira de Santana, cujo objetivo é compreender os conceitos básicos da Teoria Combinatorial de Grupos. A Teoria Combinatorial de Grupos surgiu no final do século XIX (Chandler; Magnus, 1982), com o trabalho de Dyck (1882) e consiste em estudar grupos a partir de suas **apresentações**, isto é, de seus geradores e relações. Essa abordagem permitiu a aplicação mais eficiente de teoria de grupos a várias áreas da matemática e é especialmente útil no estudo de grupos infinitos. Enquanto o conceito de geradores de um grupo é em geral introduzido nas disciplinas de álgebra da graduação em matemática, o conceito de relações é visto apenas superficialmente, sem uma definição clara.

Uma **apresentação** de um grupo é dada por dois conjuntos: um conjunto de geradores e um conjunto de relações. Todo elemento do grupo pode ser obtido a partir de aplicações sucessivas da operação sobre os geradores, e as relações são propriedades que são satisfeitas por esses geradores e que são suficientes para determinar o grupo.

A notação é a seguinte:

$$G = \langle X \,|\, R \rangle ,$$

onde X é o conjunto de geradores e R é o conjunto de relações.

Por exemplo, o grupo $S_3 = \{1, a, a^2, b, ba, ba^2\}$ tem a seguinte apresentação:

$$S_3 = \langle a \,,\, b \,|\, a^3 = b^2 = 1 \,,\, ab = ba^{-1} \rangle,$$

que nos diz que o grupo pode ser descrito como tendo dois geradores, sendo um deles de ordem 3 e um de ordem 2, satisfazendo mais uma relação como descrita para de fato caracterizar o grupo S_3.

Em nossa apresentação, após uma rápida introdução sobre a teoria básica de grupos, definiremos e exibiremos brevemente a construção de grupos livres, pois para definirmos formalmente o que é uma apresentação de grupo, antes se faz necessário abordar o conceito de grupo livre (um grupo desprovido de relações, cujos elementos podem ser vistos como classes de equivalências de palavras formadas a partir de seus geradores e seus inversos). A seguir, exibiremos a definição de apresentação de um grupo e exemplos de apresentações de grupos importantes para a própria teoria de grupos e outras áreas da matemática.

Referências

[1] CHANDLER, B.; MAGNUS, W. *The History of Combinatorial Group Theory: a case study in the History of Ideas*. Springer-Verlag, 1982

[2] COHEN, D. E. *Combinatorial group theory: a topological approach*. Cambridge University Press, 1989.

[3] DYCK, W. von, "Gruppentheoretische Studien". In: *Math Annalen*, 20, 1882, p. 1-44.

[4] GONÇALVES, Adilson, *Introdução à álgebra*, 5. ed. Rio de Janeiro: IMPA, 2012.

*Bolsista de Iniciação Científica PIBIC/FAPESB

Bases de Groebner e Aplicações

Augusto Duarte Pena
aduarte@mat.ufu.br

Victor Gonzalo Lopez Neumann
gonzalo@famat.ufu.br

Faculdade de Matemática, UFU
Av. João Naves de Ávila 2121
38408-100, Uberlândia, MG

RESUMO

Uma base de Groebner é um conjunto de polinômios não lineares em várias variáveis que goza de certas propriedades que permitem soluções algorítmicas simples para vários problemas fundamentais em matemática.

Neste trabalho, apresentaremos o que é uma ordem monomial no conjunto de monómios do anel de polinômios em várias variáveis, o algoritmo de Euclides para polinômios em várias variáveis, a definição de ideais monomiais e o Lema de Dickson. Com isto, provamos o Teorema das Bases de Hilbert e a seguir estudamos o algoritmo de Buchberger, que permite construir, em um número finito de etapas, uma base de Groebner para um ideal polinomial qualquer, a partir de um conjunto finito de geradores.

Por fim, daremos algumas aplicações de Bases de Groebner: como determinar quando um polinômio pertence a um ideal gerado por vários polinômios e como resolver um sistema de equações polinomiais.

Referências

[1] ATIYAH, M. F.; MACDONALD, I. G. *Introduction to Commutative Algebra*. London: Westview Press, 1969.

[2] COX, D.; LITTLE, J.; DONAL, O. *Ideals, Varieties and Algorithms*. Massachussets: Springer, 2005.

Classificação de Corpos Finitos

Daniel Alves*
Faculdade de Matemática, UFU
Av. João Naves de Ávila 2121
38408-100, Uberlândia, MG
E-mail: danielalves@mat.ufu.br daniel_ptcino@hotmail.com

Cícero Carvalho
Faculdade de Matemática, UFU
Av. João Naves de Ávila 2121
38408-100, Uberlândia, MG
E-mail: cicero@ufu.br

RESUMO

Quando se trabalha com grupos finitos, sabe-se que existem grupos com uma quantidade arbitrária de elementos. De fato, dado um inteiro positivo n, um exemplo de grupo com n elementos é o grupo $\mathbb{Z}/n\mathbb{Z}$ de inteiros módulo n. Mais ainda, dentre os grupos com o mesmo número de elementos, podem haver dois que não são isomorfos entre si, isto é, com estruturas bem diferentes. Existem estudos voltados para a descrição das diferentes estruturas de grupo que podem ser definidas sobre um mesmo conjunto.

Entretanto, quando se trata de corpos, a história é outra. O objetivo deste trabalho é enunciar alguns teoremas sobre a classificação de corpos finitos. Da Teoria dos Números, sabemos que $\mathbb{Z}/n\mathbb{Z}$ é um corpo (com a soma e produto usuais) se, e somente se, n é um número primo. Alguém poderia se perguntar se é possível definir uma estrutura de corpo em $\mathbb{Z}/n\mathbb{Z}$ quando n não é primo. Tomemos, por exemplo, um corpo $\mathbb{K}$ com 6 elementos. Sendo 1 o elemento neutro da multiplicação, definimos $2 := 1 + 1$ e $3 := 1 + 1 + 1$, e a distributividade nos garante que $2 \cdot 3 = 1 + 1 + 1 + 1 + 1 + 1 = 0$ (já que 6 é a ordem do grupo aditivo $\mathbb{K}$), donde $2 = 0$ ou $3 = 0$. Se $2 = 0$, então $\{0, 1\}$ é um subgrupo do grupo aditivo $\mathbb{K}$, e o quociente $\mathbb{K}/\{0, 1\} = \{\overline{0}, \overline{p}, \overline{q}\}$ é um grupo com 3 elementos, que sabemos ser cíclico, onde $\overline{p} + \overline{p} = \overline{p + p} = \overline{2 \cdot p} = \overline{0}$, o que é absurdo, já que $\overline{p}$ deve ter ordem 3. Analogamente, mostramos que $3 \neq 0$, ou seja, não pode haver um corpo com 6 elementos.

No presente trabalho mostramos que se $\mathbb{K}$ é um corpo com n elementos, então $n = p^r$ para algum primo p e um inteiro positivo r. Reciprocamente, dados um primo p e um inteiro positivo r sempre existem corpos com p^r elementos, e todos eles são isomorfos entre si. Além disso, se $\mathbb{K}$ é um corpo com p^r elementos e s divide r, então existe um único subcorpo de $\mathbb{K}$ com p^s elementos. E se s não divide r, $\mathbb{K}$ não possui tal subcorpo. Toda extensão finita de um corpo finito é uma extensão algébrica simples. Para todo corpo finito $\mathbb{K}$, e todo inteiro positivo n, existe um polinômio $p \in \mathbb{K}[X]$ de grau n irredutível. Finalmente, mostranos que se $\mathbb{K} \subseteq \mathbb{L}$ são corpos finitos, então o conjunto de automorfismos de $\mathbb{L}$ que fixam $\mathbb{K}$ é um grupo cíclico.

Os resultados sobre corpos finitos aqui apresentados são muito importantes no desenvolvimento da Teoria de Códigos, e têm sido muito utilizados nas Engenharias, na transmissão de dados, etc.

Referências

[1] Weintraub, Steven - Galois Theory, Springer-Verlag 2nd. ed. 2009.

[2] Hefez, Abramo e Vilela, Maria Lúcia T. - Códigos corretores de erros, IMPA 2008

*Bolsista de Iniciação Científica PICME/CNPq

Conexão: Álgebra - Geometria

Adriana Rodrigues da Silva **Camila Nogueira Gonçalves***
Faculdade de Matemática, UFU
Av. João Naves de Ávila 2121
38408-100, Uberlândia, MG
E-mail: adriana@famat.ufu.br camilanogon@yahoo.com.br

RESUMO

A Álgebra Comutativa é essencialmente o estudo de anéis comutativos e hoje em dia é uma das pedras fundamentais da geometria algébrica, além de fornecer ferramentas locais para o estudo da análise diferencial e da geometria diferencial. A relação entre álgebra comutativa e a geometria algébrica é dada pela correspondência entre ideais polinomiais e conjuntos algébricos.

Seja k um corpo algebricamente fechado, definimos um conjunto algébrico em k^n, como um subconjunto da forma

$$V(J) = \{P \in k^n \mid f(P) = 0, \text{para todo } f \in J\},$$

onde J é um ideal contido em $k[X_1, \cdots, X_n]$. Um conjunto algébrico irredutível é denominado variedade.

Seja $S \subset k^n$ subconjunto. O ideal de S é

$$I(S) = \{f \in k[X_1, \cdots, X_n] \mid f(P) = 0, \text{para todo } P \in S\}.$$

Temos assim, correspondência entre ideais de $k[X_1, \cdots, X_n]$ e pontos em k^n. Em particular,

$$\{\text{ideais primos}\} \overset{1-1}{\longleftrightarrow} \{\text{variedades}\}$$

$$\{\text{ideais maximais}\} \overset{1-1}{\longleftrightarrow} \{\text{ponto de } k^n\}.$$

A correspondência perfeita, entre ideais e conjuntos algébricos, é dada pelo Teorema dos Zeros (Nullstellensatz) que diz o seguinte:

a) Se $J \subset k[X_1, \cdots, X_n]$ ideal próprio, então $V(J) \neq \emptyset$.

b) $I(V(J)) = \text{rad } J$, em outras palavras, $f \in k[X_1, \cdots, X_n]$, com $f(P) = 0$ para todo $P \in V$ se, e somente se, $f^n \in J$ para algum n.

Definindo em k^n, um conjunto fechado sendo igual a um conjunto algébrico, obtêm-se uma topologia, chamada de Topologia de Zariski.

Referências

[1] Atiyah, M. F. and Macdonald, I. G., *Introduction to Commutative Algebra*, Addison Wesley, 1969.

[2] Fulton, W., *Algebraic Curves*, Benjamim, 1974. (disponível em www.math.lsa.umich.edu/∼wfulton/CurveBook.pdf, 2008.)

[3] Greuel, G-M, and Pfister G., *A Singular Introduction to Commutative Algebra*, Springer-Verlag, 2nd edition, 2008.

[4] Reid, M., *Undergraduate Commutative Algebra*, Cambridge University, 1995.

*Bolsista de Iniciação Científica PIBIC/CNPq

Conjectura de Zarrin

Alan Rodrigues dos Santos [1]
Unidade Acadêmica Especial - Instituto de Matemática e Tecnologia - IMTec, UFG
Rua 19 de novembro Nº366, Vila Erondina
75711-360, Catalão, GO
Email: alansantos2102@gmail.com

Igor dos Santos Lima
Unidade Acadêmica Especial - Instituto de Matemática e Tecnologia - IMTec, UFG
Av. Dr. Lamartine Pinto de Avelar 1120, St. Universitário
75704-020, Catalão - GO
Email: igor.matematico@gmail.com

RESUMO

Este trabalho é referente ao projeto em andamento Iniciação Científica (PIBIC 2014/2015), intitulado "Classificação de grupos com uma quantidade fixada de subgrupos solúveis e o programa GAP (Groups, Algorithms and Programming)", sob a orientação do Prof. Dr. Igor dos Santos Lima.

Aqui daremos uma abordagem sobre o que está sendo desenvolvido no projeto. Essencialmente o projeto visa testar (ou provar) via GAP uma Conjectura de Zarrin (2013) para grupos simples, que diz que dois grupos simples não-abelianos são isomorfos se, e somente se, eles possuem a mesma quantidade de subgrupos (próprios) solúveis.

Referências

[1] Zarrin, M. Groups With few solvable subgroups. *Journal of Algebra and Its Applications.* 2013..

[1]Bolsista de Iniciação Científica PIBIC/CNPq

III Colóquio de Matemática da Região Sudeste

Decomposição Primária

Caio Augusto Bulian Barcellos
Universidade Federal do Espírito Santo, UFES
Av. Fernando Ferrari, 514, Goiabeiras
29075-910, Vitória, ES
Email: caiobarcellos5@hotmail.com

Renato Fehlberg Júnior
Universidade Federal do Espírito Santo, UFES
Av. Fernando Ferrari, 514, Goiabeiras
29075-910, Vitória, ES
Email: renato.fehlberg@ufes.br

RESUMO

Dentro da Álgebra Comutativa a decomposição primária trata da decomposição de um ideal em uma interseção finita de ideais primários. Geometricamente, esse estudo tem relação com a decomposição de uma variedade algébrica em seus componentes irredutíveis.

Neste trabalho, apresentaremos as definições básicas para esse estudo e os teoremas de unicidade da decomposição primária, além de alguns exemplos.

Referências

[1] ATIYAH, M. F.; MACDONALD, I. G. Introduction to Commutative Algebra.
Addson-Weslwy Publishing Company 1969.

[2] MILNE, J. S. *A Primer of Commutative Algebra. Disponível em www.jmilne.org/math/, 2010.*

Dimensão de uma Variedade e a Funçao de Hilbert

Cicero F. de Carvalho cicero@ufu.br
Guilherme S. M. Dias* guimsd@gmail.com
Faculdade de Matemática, UFU
Av. João Naves de Ávila 2121
38408-100, Uberlândia, MG

RESUMO

Neste trabalho, queremos computar a dimensão da variedade afim definida por um ideal em $K[x_1, \cdots, x_n]$, onde K um corpo. Iniciaremos estudando a dimensão da variedade de um ideal monomial e depois generalizaremos para o caso de um ideal qualquer. Começamos o trabalho mostrando que a variedade de um ideal monomial em $K[x_1, \cdots, x_n]$ é uma união finita de subespaços coordenados de K^n. Em seguida definimos a dimensão desta variedade como sendo a dimensão do maior subespaço da união.

Iremos então fazer um estudo sobre monômios que não estão contidos em um ideal monomial $I \subset K[x_1, \ldots, x_n]$. Como pode haver infinitos destes monômios, nosso objetivo será encontrar uma fórmula para o número de monômios que não pertencem ao ideal e tenham grau menor que alguma cota. Os resultados obtidos a partir deste estudo são fundamentais para a definição de dimensão de uma variedade arbitrária.

Veremos que o conjunto $C(I) \subset \mathbb{Z}_{\geq 0}$ dos expoentes dos monômios que não se encontram em I pode ser escrito como uma união finita (mas não necessariamente disjunta) de translações de subespaços coordenados de $\mathbb{Z}_{\geq 0}$. E então verificaremos o número de elementos em cada uma destas translações que são menores que determinada cota.

Por fim, definiremos a função e o polinômio de Hilbert de um ideal, e concluiremos que a dimensão de $\mathbf{V}(I)$ é igual ao grau do polinômio de Hilbert de I.

Referências

[1] ATIYAH, M. F. and MACDONALD, I. G., *Introduction to Commutative Algebra*, Addison Wesley, 1969.

[2] COX, D.; LITTLE, J. e O'SHEA, D. *Ideals, Varieties, and Algorithms*, Springer-Verlag, 2010 (3a. ed.).

[3] HERSTEIN, I. N. *Tópicos de álgebra.* Ex. Polígono (Univ. de São Paulo), 1970.

*Parcialmente financiado pelaCAPES

Fatoração de Inteiros Usando Curvas Elípticas

Daniel Alves*
Faculdade de Matemática, UFU
Av. João Naves de Avila, 2121, Campus Santa Mônica
38.408-100, Uberlândia, MG
E-mail: danielalves@mat.ufu.br daniel_ ptcino@hotmail.com

Alonso S. Castellanos
Faculdade de Matemática, UFU
Av. João Naves de Avila, 2121, Campus Santa Mônica
38408-100, Uberlândia, MG
E-mail: alonso@famat.ufu.br

RESUMO

As curvas elípticas são curvas algébricas projetivas planas não singulares definidas por polinômios homogêneos de grau 3. É possível definir uma adição de pontos numa curva elíptica de modo que o conjunto de pontos da curva tenha uma estrutura de grupo abeliano. O objetivo deste trabalho é descrever um algoritmo para fatoração de inteiros que faz uso dessa estrutura de grupo. Tal algortimo é atribuído a H. W. Lenstra, Jr. ([1]), e é baseado no método $p-1$ de Pollard.

Começamos descrevendo a construção da reta projetiva, uma preparação para a introdução do plano projetivo. A seguir definimos polinômios homogêneos, e observamos uma propriedade que permite definir curvas algébricas projetivas. Só então definimos curvas elípticas sobre corpos, justificamos geometricamente a estrutura de grupo abeliano, e construímos as fórmulas a serem usadas para calcular a soma de pontos. Finalmente, explicamos o método $p-1$ de Pollard, e o algoritmo de Lenstra.

O método de curvas elípticas é muito bem sucedido em calcular um fator primo p de n quando $p < 10^{40}$. Valores de n usados em aplicações criptográficas são geralmente escolhidos como $n = pq$, onde p e q são primos grandes (pelo menos 75 algarismos). Para tais números, os métodos de fatoração *Quadratic Sieve* e *Number Field Sieve* - o campeão de todos os métodos de fatoração conhecidos ([4]) - superam o método de curvas elípticas em performance. Entretanto, o método de Lenstra é às vezes usado dentro desses métodos para procurar por fatores primos de tamanho médio que aparecem em passos intermediários.

Referências

[1] LENSTRA, H. W. Factoring Integer with Elliptic Curves. *Annals of Mathematics* v.126, p. 649-673, 1987.

[2] SILVERMAN, J. H.; TATE, J. *Rational Points on Elliptic Curves* New York: Springer-Verlag, 1992.

[3] WASHINGTON, L. C. *Elliptic Curves: Number Theory and Cryptography.* Boca Raton: Chapman & Hall/CRC, 2008.

[4] YAN, S. Y. *Number Theory for Computing* Springer, 2009.

*Bolsista de Iniciação Científica PICME/CNPq

.Anais do III Colóquio de Matemática da Região Sudeste
.Uberlândia - 13 a 17 de abril de 2015
Revista Matemática e Estatística em Foco – ISSN: 2318-0552

Grupos de Grothendieck e Categorificação Algébrica

Clayton C. Silva[1]
Departamento de Matemática, UFV
Av. P. H. Rolfs, s/n
36570-000, Viçosa, MG
Email: ccris22@gmail.com

Marinês Guerreiro
Departamento de Matemática, UFV
Av. P. H. Rolfs, s/n
36570-000, Viçosa, MG
Email: marinesguerreiro0208@gmail.com

RESUMO

O termo *categorificação*, introduzido por Louis Crane e Igor Frenkel refere-se ao processo de trocar noções da Teoria de Conjuntos por suas correspondentes análogas na Teoria de Categorias. Dessa forma, substituímos conjuntos por categorias, elementos por objetos, funções por funtores, relações entre elementos por morfismos entre objetos e relações entre funções por transformações naturais de funtores. A idéia por trás deste processo é obter informações extras que possam ser usadas para estudar o objeto original. Entretanto, o processo inverso, conhecido como *decategorificação*, onde objetos isomorfos são identificados como iguais, é um ponto de partida mais natural.

O método mais simples de esquecer informação em uma categoria é tomar o correspondente *grupo de Grothendieck*, que é um exemplo clássico do processo de decategorificação. Trata-se de um grupo abeliano sobre o conjunto das classes de isomorfismo de uma categoria essencialmente pequena munida de uma operação binária.

Certas categorias (*aditivas*, *abelianas* e *trianguladas*) fornecem a construção do grupo de Grothendieck de uma maneira natural. Neste trabalho, investigamos a estrutura dos grupos de Grothendieck desses vários tipos de categorias. Além disso, discutimos algumas propriedades que essas categorias podem ter que dão bases boas aos grupos de Grothendieck. No caso das categorias aditivas, isso nos dá a propriedade de Krull-Schmidt e para as categorias abelianas, o Teorema de Jordan-Hölder. Finalmente, no contexto de categorias trianguladas, fazemos uma breve discussão do exemplo da *categoria de homotopia* de uma categoria aditiva.

Referências

[1] LU, W.; MCBRIDE, A. K. Algebraic Structures on Grothendieck Groups. Department of Mathematics and Statistics, University of Ottawa, 2013.

[2] WEIBEL, C. A. An Introduction to Homological Algebra. Cambridge Studies in Advanced Mathematics, vol. 38, Cambridge University Press, 1994.

[1] Bolsista de Iniciação Científica PICME/CNPq

Introdução ao estudo de anéis comutativos

Arthur F. Campos[*] **Fernando A. Freitas**[†]
Faculdade de Matemática, UFU
Av. João Naves de Ávila 2121
38408-100, Uberlândia, MG
E-mail: arthurfc10@hotmail.com fernandoaugusto.mat@gmail.com

Érika M. C. Lopes[‡]
Faculdade de Matemática, UFU
Av. João Naves de Ávila 2121
38408-100, Uberlândia, MG
E-mail: erika@famat.ufu.br

RESUMO

Este trabalho apresenta um resumo de alguns resultados sobre anéis comutativos, estudo que se encontra na fase inicial de um projeto de iniciação científica. Inicialmente estudamos os conceitos de grupo e morfismo de grupos, juntamente com algumas de suas propriedades. A seguir, chegamos à definição de anel como um grupo abeliano aditivo, no qual também está definida uma operação de multiplicação que satisfaz as propriedades associativa, comutativa, existência de elemento neutro e distributiva. Trabalhamos com algumas propriedades elementares dos anéis e o conceito de morfismo de anéis.

A partir do conceito de múltiplos em um anel qualquer, mostramos que existe um único morfismo do anel dos números inteiros em um anel qualquer R. Também estudamos a prova de que: i) se um anel possui característica 0, então tal morfismo de $\mathbb{Z}$ neste anel será injetor; ii) se a característica do anel R é m, pode-se definir um monomorfismo do anel $\mathbb{Z}_m$ dos inteiros módulo m neste anel R; iii) no anel R de característica finita, a ordem de cada elemento é um divisor de sua característica. Por fim verificamos que, dado uma função $f : \mathbb{N} \to R$ que preserva adição, multiplicação e unidades, existe um único morfismo de anéis $f' : \mathbb{Z} \to R$, com $f' \circ i = f$, onde $i : \mathbb{N} \to \mathbb{Z}$ é a inserção.

Referências

[1] MAC LANE, S.; BIRKHOFF, G. *Algebra*. Rhode Island: AMS Chelsea Publishing, 1999.

[2] HERSTEIN, I.N. *Topics in Algebra*. New York: John Wiley & Sons, 1975.

[*] Aluno do PET Matemática UFU-Santa Mônica
[†] Aluno do PET Matemática UFU-Santa Mônica
[‡] Professora orientadora

Lema de Dickson

Luciano da Silva Alves*
Faculdade de Matemática, UFU
Av. João Naves de Ávila 2121
38408-100, Uberlândia, MG
E-mail: lucianoalves@mat.ufu.br

Victor Gonzalo Lopez Neumann
Faculdade de Matemática, UFU
Av. João Naves de Ávila 2121
38408-100, Uberlândia, MG
E-mail: gonzalo@famat.ufu.br

RESUMO

Neste trabalho apresentaremos a demosntração do Lema de Dickson, elemento imprescindível na demosntração do Teorema da base de Hilbert.

Considere $\alpha = (\alpha_1, ..., \alpha_n)$. Em $k[x_1, ..., x_n]$ escrevemos $x^\alpha = x_1^{\alpha_1}...x_n^{\alpha_n}$.

Um ideal $I \subset k[x_1, ...x_n]$ é um **ideal monomial** se existe um subconjunto $A \subset \mathbb{Z}^n_{\geq 0}$(possivelmente infinito) segundo o qual I consiste de todos os polinômios que são somas finitas da forma $\sum_{\alpha \in A} h_\alpha x^\alpha$, onde $h_\alpha \in k[x_1, ..., x_n]$. Então escrevemos $I = \langle x^\alpha : \alpha \in A \rangle$.

Uma **ordem monomial** em $k[x_1, ..., x_n]$ é uma relação $>$ em $\mathbb{Z}^n_{\geq 0}$, ou equivalentemente, uma relação no conjunto dos monômios x^α, $\alpha \in \mathbb{Z}^n_{\geq 0}$, satisfazendo:

i. $>$ é uma relação de ordem total em $\mathbb{Z}^n_{\geq 0}$.

ii. Se $\alpha > \beta$ e $\gamma \in \mathbb{Z}^n_{\geq 0}$, então $\alpha + \gamma > \beta + \gamma$.

iii. $>$ é uma boa ordenação em $\mathbb{Z}^n_{\geq 0}$. Isto significa que todo subconjunto não vazio de $\mathbb{Z}^n_{\geq 0}$ tem um menor elemento segundo a ordem $>$.

Lema de Dickson: todo ideal monomial $I = \langle x^\alpha : \alpha \in A \rangle \subseteq k[x_1, ..., x_n]$ pode ser escrito na forma $I = \langle x^{\alpha(1)}, ..., x^{\alpha(s)} \rangle$, onde $\alpha(1), ..., \alpha(s) \in A$. Em particular, todo ideal monomial possui uma base finita.

Precisaremos de resultados preliminiares que nos ajudarão a distinguir quando um monômio pertence ao ideal monomial I, ou saber quando dois ideais monomiais são iguais. Concluíremos que um monômio pertence a um ideal se, e somente se, ele é múltiplo de algum monômio gerador do ideal e, ainda, que dois ideais monômiais são iguais se, e somente se, eles contêm os mesmo monômios.

Com estes resultados e uma ordem monomial em mãos, conseguimos demonstrar o Lema de Dickson construindo os ideais $J_k = \langle \{x^\alpha \mid x^\alpha y^k \in I\} \rangle$, com $k = 0, \ldots, m-1$, e mostrando que podemos escolher elementos de cada um dos ideais J_k de forma a obter um conjunto gerador para I. A partir desse conjunto de geradores encontramos uma base finita para I.

A partir do Lema de Dickson, pode-se provar que uma ordem $>$ em $\mathbb{Z}^n_{\geq 0}$ é monomial se ela satisfaz (i.) e (ii.), e se para todo $\alpha \in \mathbb{Z}^n_{\geq 0}$, tem-se $\alpha = 0$ ou $\alpha > 0$.

Referências

[1] COX, David; LITTLE, John; O'SHEA, Donal. *Ideals, Varieties, and Algorithms.* Springer, 2007.

*Bolsista de Iniciação Científica PICME/CNPq

O Teorema de Nullstellensatz e Aplicações

Alonso Sepúlveda Castellanos **Wagner Dias Alves de Souza***

Faculdade de Matemática, UFU
Av. João Naves de Ávila 2121
38408-100, Uberlândia, MG
E-mail: alonso@famat.ufu.br wagdias@hotmail.com

RESUMO

Neste trabalho demostraremos o Teorema dos zeros de Hilbert, também conhecido como Nullstellensatz. Para isso introduzimos os conceitos fundamentais da Geometria Algébrica tais como Conjuntos Algébricos e Variedades Afins.
Este é um teorema da Geometria Algébrica que relaciona conjuntos e ideais em anéis de polinômios sobre um corpo algebricamente fechado. Enunciamos o teorema:

Teorema 1 *(Zeros de Hilbert ou Nullstellensatz) Seja k um corpo algebricamente fechado.*

i) Todo ideal maximal no anel $A = k[X_1, \cdots, X_n]$ é da forma $\langle X_1 - a_1, \cdots, X_n - a_n \rangle$, onde $a_i \in k$.

ii) Seja J um ideal de A. Se $J \neq \langle 1 \rangle$, então $V(J)$ é não vazio.

iii) Para todo $J \subseteq A$, temos $I(V(J)) = \sqrt{J}$.

Depois de demonstado, faremos uma interessante aplicação do teorema.

Referências

[1] M.F ATIYAH & I.G MACDONALD, *Introduction to Commutative Algebra*, WESTVIEW PRESS, London, 1969.

[2] KUNZ, Ernst, *Introduction to Comutative Algebra an Algebric Geometry*, BIRKHAUSER, Boston, Basel, Stuttgart, 1985.

[3] LANG, SERGE, *Graduete Texts in Mathematics*, SPRINGER, New Haven, 2002

*Graduando em Matemática

O Uso de Imagens Digitais Obtidas por Sensoriamento Remoto como Recurso Didático no Ensino de Matrizes

Antônio A. de S. Costa Neuma T. dos Santos Geraldo S. de Melo

Campus de Capanema, UFRA.
Rua João Pessoa, 121. 68700-030, Capanema, PA
Email: adryanufr@gmail.com neuma.santos@ufra.edu.br geraldo.melo@ufra.edu.br

Dandara B. Resque[1] **João A. C. Soares**

Instituto Ciberespacial, UFRA.
Av. Tancredo Neves, s/n, Caixa Postal 917. 66077-530, Belém, PA
Email: dandararesque@hotmail.com joao.almiro@ufra.edu.br

RESUMO

Este trabalho tem como objetivo explanar algumas atividades pautada em modelagem matemática [1], utilizando a aprendizagem de matrizes e o uso de suas operações adição, subtração e multiplicação como importantes ferramentas para o processo de aquisições de Imagens Digitais, além de proporcionar um novo viés para o ensino/aprendizagem de Álgebra Linear aplicado à engenharia [4].

Abordaremos o tema a partir de quatro aspectos principais: Importância de Álgebra Linear na Engenharia; Modelagem Matemática como viés de Ensino; Sensoriamento Remoto: Conceito, Contexto, Aplicações usando Álgebra Linear e Imagem Digital Aplicado ao Ensino de Matrizes (Adição, Subtração e Multiplicação) [2].

Esses aspectos auxiliam o ensino/aprendizagem de alunos do ensino médio que desejam não só ingressar em engenharia, mas também molda-los para a compreensão da estrutura algébrica e seu significado/código, buscando enfatizar condições para retratar os problemas decorrentes no ensino/aprendizagem de matrizes, onde muitas vezes a falta de compressão do conteúdo no ensino médio, prejudica a aprendizagem do aluno no ensino superior quando necessário.

Sendo assim, as atividades propostas estão intimamente relacionadas à Matrizes/Álgebra Linear e o quanto é fundamental entender o código matemático provindo de estudos anteriores, que uma vez aproveitados com clareza, tornam-se imprescindíveis para a vida acadêmica e profissional.

Tabela 1 ï Relação entre Operações Aritméticas Matriciais e Imagem Digital [3].

OPERAÇÕES MATRICIAIS	IMAGEM DIGITAL
ADIÇÃO	Usado em conjunto de imagens para criar uma nova imagem composta pelo mesmo conjunto.
SUBTRAÇÃO	Encontra diferenças entre duas imagens, realçando os detalhes da imagem e removendo as características que não mudaram.
MULTIPLICAÇÃO	Qualifica os sistemas oferecidos pelas outras operações aritméticas auxiliando na sobreposição de uma imagem em outra.

Referências

[1] FLEMMING, D.; LUZ, E.; MELLO, A. Tendências em Educação Matemática. 2. ed. Santa Catarina (SC), 2005.

[2] JENSEN, John R. *Sensoriamento Remoto do Ambiente*: Uma perspectiva em recursos terrestres. 2° edição. Arêntese. São José dos Campos. SP, Brasil. 2009.

[3] MÜLLER, D. N.; DARONCO, E. L. Operações Aritméticas em Imagens. Universidade Federal do Rio Grande do Sul. Programa de Pós-Graduação em Computação. Porto Alegre (RS), Abril de 2000.

[4] PESCADOR, A. POSSAMAI, J. P. POSSAMAI, C. R. Aplicação de Álgebra Linear na Engenharia. In: CONGRESSO BRASILEIRO DE EDUCAÇÃO EM ENGENHARIA 39. 211, Blumenau. Anais... Santa Catarina, 2011.

[1]Bolsista de Iniciação Científica CNPq. Chamada Nº 18/2013 MCTI/CNPq/SPM-PR/Petrobras - Meninas e Jovens Fazendo Ciências Exatas, Engenharias e Computação.

Parâmetros de um Código de Avaliação

Cirilo Gonçalves Júnior
Centro Federal de Educação Tecnológica de Minas Gerais
Rua Santa Rita, 900
35790-000, Curvelo, MG
E-mail: cirilo@curvelo.cefetmg.br

Cícero Carvalho*
Faculdade de Matemática, UFU
Av. João Naves de Ávila, 2121
38408-100, Uberlândia, MG
E-mail: cicero@ufu.br

RESUMO

Este trabalho estuda os parâmetros de um código de avaliação definido sobre uma interseção completa. Sejam $A = K[x_0, x_1, \ldots, x_n] = \oplus_{j\geq 0} A_j$, $\mathcal{Y} = \{P_1, \ldots, P_m\}$ um subconjunto do espaço projetivo $\mathbb{P}^n(K)$ e $I_{\mathcal{Y}} := \{f \in A \mid f(P) = 0, \forall P \in \mathcal{Y}\}$ (ver [1]). O código avaliação de ordem d, denotado por $C_{\mathcal{Y}}(d)$, é a imagem do homomorfismo

$$\begin{aligned} ev_d : A_d &\longrightarrow K^m \\ f &\longmapsto (f(P_1), \ldots, f(P_m)). \end{aligned}$$

Considere o conjunto

$$\mathcal{X} = \{[1, t_1^{m_1}, t_2^{m_2}, \ldots, t_n^{m_n}] \mid t_i \in K^* \text{ para todo } i = 1, \ldots, n\} \subseteq \mathbb{P}^n(K).$$

Temos que $\mathcal{X}$ é uma interseção completa, pois, $I_{\mathcal{X}} = \langle f_1, \ldots, f_n \rangle$, onde $f_i = x_i^{s_i} - x_0^{s_i}$ e $s_i = \frac{q-1}{\gcd(q-1, m_i)}$ para todo $i = 1, \ldots, n$, além disso, f_i não é divisor de zero em $A/\langle f_1, \ldots, f_{i-1} \rangle$ para todo $i = 1, \ldots, n$ (ver [2]). Então o código $C_{\mathcal{X}}(d)$ tem dimensão

$$\dim C_{\mathcal{X}}(d) = \binom{n+d}{d} - \sum_{i=1}^{n} \binom{n+d-s_i}{d-s_i} + \sum_{1\leq i_1 < i_2 \leq n} \binom{n+d-(s_{i_1}+s_{i_2})}{d-(s_{i_1}+s_{i_2})} -$$

$$- \sum_{1\leq i_1 < i_2 < i_3 \leq n} \binom{n+d-(s_{i_1}+s_{i_2}+s_{i_3})}{d-(s_{i_1}+s_{i_2}+s_{i_3})} + \ldots + (-1)^n \binom{n+d-(s_1+\ldots+s_n)}{d-(s_1+\ldots+s_n)}$$

e comprimento $|\mathcal{X}| = s_1 \cdot \ldots \cdot s_n = \prod_{i=1}^n s_i$. Temos ainda que $\{f_1, \ldots, f_n\}$ é uma base de Groebner para $I_{\mathcal{X}}$ (ver [1]). Seja $\delta_d = \min\{w(ev_d(f)) \mid f \in A_d\}$ a distância mínima do código $C_{\mathcal{X}}(d)$ (ver [3]), dado $e \geq |\mathcal{X}| - 1$ e $d < \sum_{i=1}^n (s_i - 1)$ temos que $(s_{k+1} - l)\prod_{i=k+2}^n s_i \leq \delta_d \leq w(ev_d(f))$, para todo $f \in A_d \backslash I_{\mathcal{X},d}$, onde k e l são unicamente determinados por $d = \sum_{i=1}^n (s_1 - 1) + l$ com $0 \leq l \leq s_{k+1} - 1$. Se $k + 1 = n$ então entenderemos que $\prod_{i=k+2}^n s_i = 1$, e se $d < s_1 - 1$ então temos $k = 0$ e $l = d$. Além disso, existe $f \in A_d \backslash I_{\mathcal{X},d}$ tal que $w(ev_d(f)) = (s_{k+1} - l)\prod_{i=k+2}^n s_i$. Portanto, a distância mínima do código $C_{\mathcal{X}}(d)$ é $\delta_d = (s_{k+1} - l)\prod_{i=k+2}^n s_i$.

Referências

[1] COX, D.; LITTLE, J.; O'SHEA D. *Ideals, Varieties, e Algorithms*, second ed; Springer; Berlim, 1997.

[2] SARABIA M. G.; RENTERÍA, C.; HERNÁNDEZ, A. J. S. *Evaluation Codes Over a Particular Complete Intersection*, Int. J. Contemp. Math. Sciences, Vol. 6, 2011, no. 30, 1497-1504.

[3] SARABIA M. G.; RENTERÍA, C.; HERNÁNDEZ, A. J. S. *Minimum distance of some evaluation codes*, AAECC, Springer, (2013) 24:95-106.

*Parcialmente financiado pelo CNPq proc. 480477/2013-2

Pesos Generalizados dos Códigos de Hamming e Simplex

Leandro Cruvinel Lemes **Ghais Júnio Della Noce Wehbe***
Faculdade de Matemática, UFTM
Av. Dr. Randolfo Borges Júnior 1250
38064-200, Uberaba, MG
E-mail: leandro@icte.uftm.edu.br ghaisdellanoce@hotmail.com

RESUMO

Este trabalho tem por finalidade a análise e o cálculo dos pesos generalizados do $[7,4]_2$-código de Hamming e de seu dual, o $[7,3]_2$-código Simplex. Um $[n,k]_q$-código linear q-ário C é um $\mathbb{F}_q$-subespaço vetorial k-dimensional de $\mathbb{F}_q^n$, com $\mathbb{F}_q$ sendo um corpo finito com q elementos. Os elementos de C são chamados de palavras. Um $\mathbb{F}_q$-subspaço vetorial D de C é chamado de subcódigo de C. O dual de um código C, denotado por $C^{\perp}$, é o complemento ortogonal de C relativo ao produto interno canônico formal em $\mathbb{F}_q^n$. Exemplos de $[7,4]_2$-códigos lineares são o de Hamming e o Simplex. O código de Hamming é gerado por $A = \{1000110, 0100101, 0010011, 0001111\}$ e o Simplex é seu dual.

Em 1950, Hamming [2] apresentou o conceito de distância mínima de um código C como sendo o número mínimo de coordenadas não nulas que uma palavra de C pode ter. Em [4], Wei generalizou esse conceito introduzindo os pesos generalizados de Hamming (GHW). O suporte de um subcódigo D, denotado por $\text{supp}(D)$, é definido por $\text{supp} = \{i : \exists (x_1, ..., x_n) \in C; x_i \neq 0\}$. Os r-ésimo peso generalizado de Hamming é definido por $d_r(C) = \min\{|\text{supp}(D)| : D \subseteq C \text{ com } dim(D) = r\}$. Se um $[n,k]_q$-código C satisfaz $d_1(C) = n - k$, então C é dito AMDS (almost MDS). Além disso, se $d_2(C) = n - k + 2$, então C é dito NMDS (near MDS).

Códigos lineares são usados para inserir redundâncias em mensagens e assim detectar possíveis erros de transmissão. Encontrar códigos que minimizem a probabilidade de ocorrências de erros de decodificação é o principal problema em teoria de informação. Relações entre estas probabilidades e os GHW são encontradas na literatura [1] ilustrando a importância destes parâmetros. Kløve et al. [3], mostrou que todos os $[n,k]_2$-códigos NMDS são próprios para correção de erros.

Seja C código de Hamming, pelos Teoremas da Monotonicidade e da Dualidade [4] temos que $d_1(C) = 7 - 4 = 3$, $d_2(C) = 7 - 4 + 2 = 5$, $d_3(C) = 6$, $d_4(C) = 7$, $d_1(C^{\perp}) = 7 - 3 = 4$, $d_2(C^{\perp}) = 7 - 3 + 2 = 6$ e $d_3(C^{\perp}) = 7$. Logo, verifica-se que os códigos de Hamming e Simplex são NMDS. Fato este é consequência da dualidade entre estes dois códigos como demonstrado em [3].

Referências

[1] DIDIER, F. *A New Upper Bound on the Block Error Probability After Decoding Over the Erasure Channel*. IEEE Trans. Inform. Theory., vol. 52, no. 10, pp. 4496-4503, 2006.

[2] HAMMING, R. W. *Error Detecting and Error Correcting Codes*. Bell System Technical Journal, vol. 29, pp. 147-160, 1950.

[3] DODUNEKOVA, R.; DODUNEKOV, M. S.; KLØVE, T. *Almost-MDS and Near- MDS Code for Error Detection*. IEEE Trans. Inform. Theory., vol. 43, no. 1, pp. 286, 1997.

[4] WEI, K. V. *Generalized Hamming Weights for Linear Codes*. IEEE Trans. Inform. Theory., vol. 37, pp. 1412-1413, 1987.

*Bolsista de Iniciação Científica PIBITI/Funttel

Pontos Racionais em Curvas Elípticas e os Números Congruentes

Alexandre Silva dos Reis
Curso de Mestrado em Matemática – PPGMAT - UFES
Avenida Fernando Ferrari, 514, Goiabeiras
29075-910, Vitória, ES
Email: alexandre.silva.reis@gmail.com

José Gilvan de Oliveira
Departamento de Matemática – DMAT - UFES
Avenida Fernando Ferrari, 514, Goiabeiras
29075-910, Vitória, ES
Email: jgilvanol@gmail.com

RESUMO

Neste trabalho apresentamos brevemente o conceito de curva elíptica e algumas de suas propriedades como, por exemplo, a importante estrutura de grupo. Destacamos ainda, de maneira alternativa, como uma tal curva pode ser obtida por meio de uma função meromorfa específica. Nosso objetivo é relacionar tais curvas elípticas com o clássico problema dos números congruentes. Um número inteiro positivo n é congruente se existe um triângulo retângulo de área n cujas medidas de seus lados são números racionais. Apresentamos duas caracterizações dos números congruentes. A primeira demonstra a relação desses números com certas progressões aritméticas de três termos que são quadrados de números inteiros. A segunda caracterização mostra a estrita relação entre os números congruentes e certas curvas elípticas. Mais ainda, ela mostra também como a já citada estrutura de grupo dessa curva permite descrever, por meio de pontos racionais da curva, a existência ou não de solução para o problema dos números congruentes.

Referências

[1] CONRAD, K. The Congruent Number Problem. Disponível em (http://www.math.uconn.edu/ kconrad/blurbs/ugradnumthy/congnumber.pdf)

[2] HENNIART, G. Congruent Numbers, Elliptic Curves and Modular Forms. Disponível em (http://www.fen.bilkent.edu.tr/ franz/publ/guy.pdf)

[3] KOBLITZ, N. Introduction to Elliptic Curves and Modular Forms, Springer-Verlag, New York, 1984.

Resolução de sistemas de equações polinomiais usando Teorema da eliminação

Hugo Leonardo Lopes Costa hugoleo1905@hotmail.com

Victor Gonzalo Lopez Neumann gonzalo@famat.ufu.br

Faculdade de Matemática, UFU
Av. João Naves de Ávila, 2121
38408-100, Uberlândia, MG

RESUMO

A teoria das bases de Groebner juntamente com o algoritmo de Buchberger é muito importante na Geometria Algébrica e em outras áreas do conhecimento científico, uma vez que fornece ferramentas computacionais que podem ser aplicadas na solução de problemas nas áreas de Matemática, Engenharias, Ciências da Computação, dentre outras.

Este trabalho apresenta uma revisão teórica de monômios, ordenação monomial, algoritmo da divisão, ideais polinomiais, Bases de Groebner, algoritmo de Buchberger e teoria da eliminação.

O objetivo principal é realizar um estudo sobre as propriedades das Bases de Groebner e utilizando o algoritmo de Buchberger, com a ordem lexicográfica, podemos resolver sistemas de equações polinomiais.

Referências

[1] GONC¸ ALVES, A. Introdução à álgebra. Projeto Euclides. 5 ed. Rio de Janeiro: SBM, 2009.

[2] COX, D.; LITTLE, J.; O'SHEA, D. Ideals, Varieties, and Algorithms. 2. ed. New York: SpringerVerlag, 1997.

[3] ABREU, K. K, Uma introdução às bases de Groebner / Karina de Kassia Abreu, 2011. disponível em: < http : //www.unif al−mg.edu.br/matematica/f iles/f ile/T CC/T CC−KARINA.pdf >. Acesso em: 02 de agosto de 2014.

Teorema de Bézout

Adriana Rodrigues da Silva **Paulo Victor Machado Prado***
Faculdade de Matemática, UFU
Av. João Naves de Ávila 2121
38408-100, Uberlândia, MG
E-mail: adriana@famat.ufu.br paulovictor_prado@hotmail.com

RESUMO

Uma *curva algébrica* é uma variedade algébrica de dimensão um. A teoria destas curvas em geral foi completamente desenvolvida no século dezenove e uma parte desta teoria se dedica à interseção de curvas planas projetivas.

Uma das perguntas a ser respondida é qual o número de pontos na interseção de duas curvas projetivas F, G de graus arbitrários. Se temos duas curvas planas projetivas F, G, então $F \cap G$ é finita se e só se F, G não admitem componente em comum. Nesse caso, nos resta saber agora como calcular o número de pontos na interseção.

Sejam $P_i = (x_i : y_i : z_i)$, $i = 1, ..., r$ os pontos distintos de $F \cap G$. Dizemos que F, G estão *bem posicionadas* se $P_0 = (0 : 1 : 0) \notin F \cap G$. Dizemos também que F, G estão *muito bem posicionadas* se $P_0 \notin F \cap G$ e se para cada par $P_j \neq P_i \in F \cap G$ tivermos que P_0, P_j, P_i não são colineares.

Se F, G estão muito bem posicionadas, a resultante $R = R(X, Z)$ de F, G com respeito a Y se escreve na forma

$$R = c \prod_{i=1}^{r} (z_i X - x_i Z)^{mi}$$

com $\sum m_i = d^\circ R = (d^\circ F) \cdot (d^\circ G)$. Por outro lado, para cada $(x : z) \in \mathbb{P}^1$ temos que $R(x, z) = 0$ se e somente se existe y tal que $(x : y : z) \in F \cap G$.

Supondo então que F, G não têm componente em comum e que F, G são muito bem posicionadas, definimos a *multiplicidade de interseção* de F, G no ponto P como segue

$$(F, G)_P := \begin{cases} 0 & \text{se } \mathrm{P} \notin \mathrm{F} \cap \mathrm{G} \\ m_i & \text{se } \mathrm{P} = \mathrm{P_i} \text{ nas condições acima.} \end{cases}$$

Uma vez que a multiplicidade de interseção é invariante por mudança de coordenadas, podemos estender a definição da multiplicidade de interseção de duas curvas F, G sem componentes em comum no ponto $P \in \mathbb{P}^2$, mesmo que F, G não estejam muito bem posicionadas, como segue

$$(F, G)_P := (T_\bullet F, T_\bullet G)_{TP}$$

onde T denota uma projetividade tal que $T_\bullet F, T_\bullet G$ estejam muito bem posicionadas.

Desse modo, concluímos nosso trabalho com o importante:

Teorema de Bézout: Se F, G são curvas planas sem componente em comum, então o número de pontos na interseção $F \cap G$, contados com multiplicidades, é igual a $(d^\circ F) \cdot (d^\circ G)$.

Referências

[1] CARVALHO, C. F., *Introdução às curvas algébricas planas*, notas de aula - UFU, 2003.

[2] FULTON, W., *Algebraic curves*, Benjamim, 1974. (disponível em www.math.lsa.umich.edu/ wfulton/CurveBook.pdf, 2008.)

[3] VAINSENCHER, I., *Introdução às curvas algébricas planas*, Matemática Universitária - SBM, 1996.

*Bolsista PETMAT-SESu/MEC

Uma correspondência entre conceitos de álgebra e de geometria

Fernando dos Reis Naves*
Faculdade de Matemática, UFU
Av. João Naves de Ávila 2121
38408-100, Uberlândia, MG
E-mail: fernando.r.naves@gmail.com
Cicero Carvalho †
Faculdade de Matemática, UFU
Av. João Naves de Ávila 2121
38408-100, Uberlândia, MG
E-mail: cicero@ufu.br

RESUMO

Seja K um corpo e sejam $f_1, ..., f_s \in K[x_1, ..., x_n]$. A esse conjunto finito de polinômio associamos o seguinte objeto geométrico:

$$\boldsymbol{V}(f_1, ..., f_s) = \{(a_1, ..., a_n) \in K^n : f_i(a_1, ..., a_n) = 0, \forall\ 1 \leq i \leq s\}.$$

Chamaremos $V(f_1, ..., f_s)$ a variedade afim definida por $f_1, ..., f_s$. Por outro lado, dada uma variedade $V \subseteq K^n$ podemos associar a ela um objeto algébrico, a saber, o ideal

$$\boldsymbol{I}(V) = \{f \in K[x_1, ..., x_n] : f(\boldsymbol{x}) = 0, \forall \boldsymbol{x} \in V\}$$

formado pelos polinômios que se anulam em todos os pontos de V. Isso nos dá um mapa

$$\begin{array}{rccc} \varphi: & \text{variedades afins} & \longrightarrow & \text{ideais} \\ & V & & \boldsymbol{I}(V) \end{array}$$

O teorema da base de Hilbert nos diz que dado um ideal $I \subset K[x_1, ..., x_n]$ existe um conjunto finito de polinômios $f_1, ..., f_s \in I$ tais que $\langle f_1, ..., f_s \rangle = I$. Se definirmos $\boldsymbol{V}(I)$ como o conjunto dos zeros (em K^n) comuns a todos os polinômios de I, temos que $\boldsymbol{V}(I)$ é uma variedade afim, pois como mostrado no presente trabalho temos que $\boldsymbol{V}(I) = \boldsymbol{V}(f_1, ..., f_s)$.

Assim temos um outro mapa

$$\begin{array}{rccc} \psi: & \text{ideais} & \longrightarrow & \text{variedades afins} \\ & I & & \boldsymbol{V}(I) \end{array}$$

Neste trabalho também exploramos a natureza dessas correspondências, utilizando principalmente o assim chamado Teorema dos Zeros de Hilbert, e com isto poderemos construir uma espécie de dicionário entre a álgebra e a geometria, onde uma afirmação sobre ideais em $K[x_1, ..., x_n]$ pode ser traduzida em uma afirmação sobre variedades afins em K^n e vice-versa. Damos especial atenção à corresponência entre variedades irredutíveis e ideais primos.

Referências

[1] Cox, D., Little, J. e O'Shea, D., *Ideals, Varieties, and Algorithms*, Springer..

*Bolsista CNPq - proc. 480477/2013-2
†Parcialmente financiado pelo CNPq proc. 480477/2013-2

Uma introdução ao estudo dos espaços homogêneos

Luciana Aparecida Alves **Ruy César de Oliveira**[1]

Faculdade de Matemática, UFU
Av. João Naves de Ávila, 2121
38408-100, Uberlândia, MG
Email: lualves@.famat.ufu.br ruycesar11@gmail.com

,

RESUMO

A principal motivação desse trabalho é introduzir o estudo dos espaços homogêneos. Para isto, apresentamos certas estruturas algébricas sob um ponto de vista geométrico de modo a facilitar a sua aplicação em Geometria e Topologia. Apresentamos, como exemplos de grupos, a circunferência unitária, o toro e alguns grupos de matrizes, como o grupo linear geral, o grupo das matrizes de determinante 1 e o grupo ortogonal. Posteriormente, exploramos a teoria algébrica de ações de grupos em conjuntos e definimos os conceitos de subgrupo de isotropia e, por fim, espaços homogêneos.

.

Referências

[1] BARROS, C.J.B; SANTANA, A.J. Estruturas Algébricas: com ênfase em elemento da teoria de Lie. Maringá: EDUEM, 2011.

[2] COELHO, F. U; LOURENÇO, M.L. Um Curso de Álgebra Linear. São Paulo: Edusp, 2007.

[3] LIMA, E.L. Álgebra Linear. Rio de Janeiro: Coleção de Matemática Universitária. IMPA, 2000.

[4] TAPP, K. Matrix Groups for Undergraduates. Student Mathematical Library, v.29, American Mathematical Society, 2005.

[1]Bolsista de Iniciação Científica Sisu/CAPES