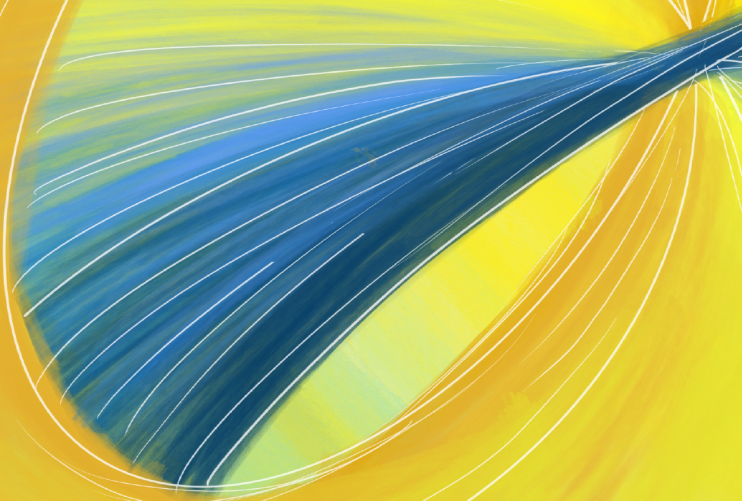
Códigos Geométricos

Uma introdução via corpos de funções algébricas



Gilberto Brito de Almeida Filho
Saeed Tafazolian

impa

33º Colóquio Brasileiro de Matemática

Códigos Geométricos

Uma introdução via corpos de funções algébricas

Códigos Geométricos
Primeira impressão, julho de 2021

Publicado no Brasil / Published in Brazil.

ISBN 978-65-89124-49-8
MSC (2020) Primary: 14H05, Secondary: 12F05, 11T71, 94B05

Coordenação Geral Carolina Araujo

Produção Books in Bytes **Capa** Izabella Freitas & Jack Salvador

Realização da Editora do IMPA
IMPA
Estrada Dona Castorina, 110
Jardim Botânico
22460-320 Rio de Janeiro RJ

www.impa.br
editora@impa.br

Sumário

1 Corpos de Funções Algébricas **1**
1.1 Propriedades de Curvas 1
1.2 Introdução à Corpos de Funções Algébricos 6
1.3 Divisores 23

2 Teorema de Riemann–Roch **31**
2.1 O Teorema de Riemann–Roch 31
2.2 Semigrupos Numéricos 40
2.3 Extensões Algébricas de Corpos de Funções 45
2.4 Extensões Especiais 50

3 Códigos Algébricos **56**
3.1 Códigos 56
3.2 Códigos Lineares 60
3.3 Codificando e Decodificando 66

4 Códigos Geométricos **74**
4.1 Códigos Geométricos e Resultados 74
4.2 Códigos Racionais e Hermitianos 80
4.3 AG Códigos, Semigrupos Numéricos e Curvas 84

Corpos Algébricos **100**

Álgebra Linear **103**

Bibliografia **106**

Lista de Símbolos **111**

Índice Remissivo **113**

1 Corpos de Funções Algébricas

1.1 Propriedades de Curvas

Neste capítulo abordaremos a teoria geral de Corpos de Funções Algébricas: Lugares, Divisores, anéis de valorização e Espaço de Riemann–Roch.

A menos de menção do contrário, neste capítulo sempre consideraremos K um corpo arbitrário.

Para um polinômio $f(x,y) \in K[x,y]$ a curva plana afim associada à f é o conjunto

$$\mathcal{X}_f := \left\{(a:b) \in \overline{K}^2 |\ f(a,b) = 0\right\}.$$

De forma análoga, dado polinômio homogêneo $F(X,Y,Z) \in K[X,Y,Z]$ a curva plana projetiva associada à F é o conjunto

$$\mathcal{X}_F := \left\{(a:b:c) \in \mathbb{P}^2(\overline{K}) |\ F(a,b,c) = 0\right\}.$$

Observamos que a partir de uma polinômio afim podemos obter um polinômio homogêneo e vise versa. Com efeito, seja $f(x,y) \in K[x,y]$ com $deg(f) = r$ então *homogenizando* f obtemos $F(X,Y,Z) = Z^r f(\frac{X}{Z}, \frac{Y}{Z})$. Reciprocamente, dado um polinômio homogêneo $F(X,Y,Z) \in K[X,Y,Z]$ obtemos um polinômio

em $K[x, y]$ *desomogenizando* com relação à uma das três variáveis $F(X, Y, 1)$, $F(X, 1, Z)$, $F(1, Y, Z)$. Estas operações de desomogenizar e homogenizar polinômios também cria uma relação entre os pontos das curvas, isto é, dado um ponto $(a, b) \in \overline{K}^2$ da curva afim $\mathcal{X}_f$ então temos que $(a : b : 1) \in \mathbb{P}^2(\overline{K})$ é um ponto da curva projetiva homogenizada $Z^r f(\frac{X}{Z}, \frac{Y}{Z})$. Por outro lado, se $(a : b : c) \in \mathbb{P}^2(\overline{K})$ com $Z \neq 0$ (resp. $X \neq 0$, ou $Y \neq 0$) é um ponto pertencente ao polinômio homogêneo $F(X, Y, Z)$ então $(a : b : 1)$ é um ponto da curva afim $F(x, y, 1)$ (resp. $F(1, y, z)$, $F(x, 1, z)$). O ponto $(a : b : 1)$ (com $Z \neq 0$) é chamados de *pontos afins* da curva $F(X, Y, Z)$, quando $Z = 0$ e dizemos que o ponto está no *infinito*.

Sejam $\mathcal{X}_F$ um curva e $p \in \mathcal{X}_F$ ponto. Dizemos que p é um *ponto singular* se

$$\begin{aligned} F_X(p) &= 0; \\ F_Y(p) &= 0; \\ F_Z(p) &= 0, \end{aligned}$$

onde F_X, F_Y, F_Z denotam as derivadas parciais em relação a cada variável. Caso contrário dizemos que p é um *ponto não singular*. Neste caso, a reta tangente em um ponto não singular é dada por

$$F_X(P)X + F_Y(P)Y + F_Z(P)Z = 0.$$

Curvas que não contém pontos singulares são chamadas de *curvas não singulares*.

A vantagem de utilizar curvas não singulares é que podemos obter o gênero destas curvas utilizando apenas o grau do polinômio. Mais precisamente, se $\mathcal{X}_F$ é uma curva não singular, então o gênero de $\mathcal{X}_F$ é

$$g = \frac{(deg(F) - 1)(deg(F) - 2)}{2}. \tag{1.1}$$

Ressaltamos que para curvas planas em geral o a formula para o calculo do gênero é um pouco diferente da formula acima.

Exemplo 1.1.1. *Seja K um corpo com* $\mathrm{Char}(K) \neq 2$. *Considere a curva dada pela equação*

$$F : Y^2T - (X - c_1T)(X - c_2T)(X - c_3T)$$

com $c_1, c_2, c_3 \in K$ distintos entre si. As derivadas parciais são:

$$\begin{aligned} F_X =& (X - c_2T)(X - c_3T) + (X - c_1T)(X - c_3T) + (x - c_1T)(X - c_2T); \\ F_Y =& 2YT; \\ F_T =& -c_1(X - c_2T)(X - c_3T) - c_2(X - c_1T)(X - c_3T) - c_3(X - c_1T)(X - c_2T), \end{aligned}$$

igualando as três derivadas a zero, obtemos que a única solução possível é $(0:0:0)$ *e desta forma* F *é não singular. Utilizando a formula do gênero, temos que* $g(F) = 1$.

Uma $\mathcal{X}_F$ curva definida sobre um corpo K é dita ser *geometricamente irredutível* sobre K se o polinômio F é irredutível sobre $\overline{K}$. Vamos sempre estar assumindo que uma curva é geometricamente irredutível.

Sobre as considerações acima podemos ver alguns exemplos:

Exemplo 1.1.2 (Curva Hermitiana)**.** *Seja q potência de um primo. Considere a equação* $X^{q+1} = Y^q Z + Y Z^q$. *Esta equação é chamada de* Curva Hermitiana $\mathcal{H}_q$ *definida sobre* $\mathbb{F}_{q^2}$. *Algumas propriedades de* $\mathcal{H}_q$

- *é geometricamente irredutível.*
- *As derivadas parciais de* $\mathcal{H}_q$ *são:*$F_X = X^q,\ F_Y = -Z^q,\ F_Z = Y^q$.

Vemos que $\mathcal{H}_q$ *é não singular. Vamos analisar um caso particular. Considerando* $q = 2$, *podemos facilmente calcular* $\mathbb{F}_{q^2} = \frac{\mathbb{Z}_2[x]}{(x^2+x+1)}$, *ie,* $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ *com* $\alpha^2 = 1 + \alpha$.

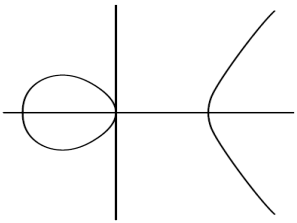
$\mathcal{H}_2$ *possui pontos no infinito? Resposta: O único ponto no infinito é o ponto* $P_\infty := (0:1:0)$, *pois* $\mathcal{H}_2 : (\frac{X}{Z})^{q+1} - (\frac{Y}{Z})^q - \frac{Y}{Z}$. *E esse é o único ponto em* $\mathcal{H}_2$ *quando* $Z = 0$.

De forma análoga podemos mostrar que $(0:1:0)$ *é o único ponto no infinito de* $\mathcal{H}_q$ *com* $Z = 0$.

Exemplo 1.1.3. *Seja* $K = \mathbb{Q}$. *Considere a equação* $G(X, Y, T) = Y^2T - X^3 + XT^2$. *então as derivadas parciais são:*

$$\begin{aligned} F_X &= 3X^2 - T^2; \\ F_Y &= 2YT; \\ F_T &= Y^2 - 2XT. \end{aligned}$$

Pela igualdade $F_Y = 0$ *temos que* $T = 0$ *ou* $Y = 0$. *Se* $T = 0$ *então por* $F_X = F_T = 0$ *temos* $X = Y = 0$. *Se* $Y = 0$ *então por* $F_X = F_T = 0$ *concluímos* $X = T = 0$. *Portanto, G é não singular e possui gênero um. Seja* $P = (T : X : Y)$ *um ponto na curva, quando* $T = 0$ *temos que* $Y = 0$ *e portanto* $P = P_\infty = (0:1:0)$ *é o único ponto no infinito. Abaixo podemos ver a figura do gráfico curva.*



Como podemos constatar no próximo exemplo, existem curvas que são singulares.

Exemplo 1.1.4. *Seja $K = \mathbb{F}_q$ um corpo com $q = l^3$ elementos. Considere a curva dada pela equação $F : Y^{l^2} - YT^{l^2-1} = X^{l^2-l+1}T^{l-1}$. Então temos que as derivadas parciais são:*

$$\begin{aligned} F_X =& (l^2 - l + 1)X^{l^2-l}T^{l-1}; \\ F_Y =& (l^2)Y^{l^2-1} - T^{l^2-1}; \\ F_T =& (l^2 - 1)YT^{l^2-2} - (l-1)X^{l^2-l+1}T^{l-2} \end{aligned} \quad ,$$

é uma curva singular, com um único ponto singular para $T = 0$. De fato, de $F_Y = 0$ temos que $Y = 0$ logo $(0 : 1 : 0)$ é o único ponto singular.

Exemplo 1.1.5. *Seja $K = \mathbb{R}$. Considere o polinômio $g(X, Y, Z) := Y^2Z^3 - X^5 - X^3Z^2$*

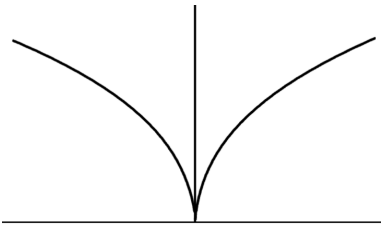
$$\begin{aligned} g_X =& -(5X^4 + 3X^2Z^2) \\ g_y =& 2YZ^3 \\ g_Z =& 3Z^2Y^2 - 2X^3Z, \end{aligned} \quad ;$$

Como as derivadas não si anulam simultaneamente, temos que g é não singular.

Abaixo podemos ver a figura do gráfico curva.

Como um dos nossos principais objetivos é o estudo sobre corpos finitos, convém mostrarmos que sobre um corpo finito sempre existem polinômio irredutíveis. Donde segue a motivação do próximo exemplo.

Exemplo 1.1.6. *Seja $\mathbb{F}_q$ um corpo com q elementos. Para cada natural n existe um polinômio irredutível em $\mathbb{F}_q$ de grau n.*



Vamos denotar por $N_q(n)$ o número de polinômios mônico irredutíveis de grau n em $\mathbb{F}_q$.

Afirmação 1:

Seja $f \in \mathbb{F}_q[x]$ mônico, irredutível de grau d. $f|x^{q^n} - x \iff d|n$. De fato, se $d|n$ então $\mathbb{F}_q \subset \mathbb{F}_{q^d} \subset \mathbb{F}_{q^n}$. Seja α uma raiz qualquer de f em alguma extensão de $\mathbb{F}_q$, logo $d = [\mathbb{F}_q(\alpha) : \mathbb{F}_q]$ e portanto $\mathbb{F}_{q^d} = \mathbb{F}_q(\alpha)$. Assim, $\alpha \in \mathbb{F}_{q^n}$ e $\alpha^{q^n} - \alpha = 0$ então $f|x^{q^n} - x$. Reciprocamente, se $f|x^{q^n} - x$ considere α uma raiz qualquer de f em alguma extensão de $\mathbb{F}_q$, logo $\alpha^{q^n} - \alpha = 0$ e assim $\alpha \in \mathbb{F}_{q^n}$ e portanto $\mathbb{F}_{q^d} \subset \mathbb{F}_{q^n}$, isto é, $d|n$.

Afirmação 2:*Para cada natural n, $x^{q^n} - x$ é igual ao produto de todos os polinômios irredutíveis sobre $\mathbb{F}_q$ com grau dividindo n.*

Com efeito, pela afirmação 1 temos que cada polinômio mônico irredutível com grau dividindo n aparece pelo menos uma vez na fatoração de $x^{q^n} - x$. Como $x^{q^n} - x$ é separável, então cada irredutível aparece exatamente uma única vez na fatoração de $x^{q^n} - x$.

Afirmação 3: $q^n = \sum_{d|n} d N_q(d)$. *para cada natural n.*

De fato, segue da afirmação 2 comparando o grau de cada lado da igualdade.

Fato: ***[Formula de inversão de Möbius]*** *Seja $f(n)$ uma função sobre os naturais e $F(n) = \sum_{d|n} f(d)$. Então, para cada natural n temos que*

$$f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d}).$$

Então obtemos que

$$N_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{\frac{n}{d}}.$$

E portanto $N_q(n) > 0$ para cada natural n. Para mais detalhes sobre a Formula de inversão de Möbius veja (Martinez et al. 2018).

Ao longo deste livro iremos estudar mais aspectos destas e de outras curvas, nos apropriando da linguagem de curvas e corpos de funções.

1.2 Introdução à Corpos de Funções Algébricos

Começamos esta seção relembrando a definição de base de transcendência. Considere F/K uma extensão qualquer de corpos. Dizemos que um conjunto T de F é *algebricamente dependente* se existe um número natural n, um polinômio não nulo $p(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ e ainda elementos distintos $t_1, \ldots, t_n \in T$ satisfazendo $f(t_1, \ldots, t_n) = 0$. No caso contrário dizemos que T é *algebricamente independente* sobre K.

Usando a inclusão de conjuntos algebricamente independentes podemos aplicar o Lema de Zorn para obter um conjunto maximal algebricamente independente. Este conjunto maximal chamaremos de *base de transcendência* de F/K.

Exemplo 1.2.1. *Considere $p(x, y) \in \mathbb{Q}[x, y]$ dado por $p(x, y) = x^3 + y - 1$. Definindo o corpo quociente $F = \frac{\mathbb{Q}[x,y]}{p(x,y)}$ temos que as variáveis $z = \frac{x}{p(x,y)}$ e $w = \frac{y}{p(x,y)}$ são uma base de transcendência de F sobre $\mathbb{Q}$.*

Da definição de base de transcendência, vemos que uma mesma extensão não temos unicidade com relação a base. Porém, como veremos no próximo resultado, a cardinalidade é invariante.

Teorema 1.2.1. *Qualquer duas bases de transcendência possuem mesma cardinalidade.*

A partir da seguinte definição concentraremos nosso estudo em extensões com base de transcendência de tamanho 1.

Definição 1.2.1. *Um* corpo de funções algébricas *F/K de uma variável sobre K é uma extensão de corpos $K \subset F$ tal que F é uma extensão algébrica finita de $K(x)$ para algum elemento $x \in F$ que é transcendente sobre K.*

Para facilitar referências futuras, iremos abreviar Corpos de Funções Algébricos para Corpos de Funções.

No caso em que F/K é uma extensão com base de transcendência de tamanho $s \geqslant 2$ dizemos que F é um corpo de funções algébrico de n variáveis.

Exercício 1.2.1. *Considere o conjunto* $\mathcal{K} := \{u \in F \mid u \text{ é algebrico sobre } K\}$. *Mostre que com as as operações de usuais de* F, $\mathcal{K}$ *é um subcorpo de* F.

O corpo $\mathcal{K}$ é chamado *corpo de constantes* de F/K.

Seja F/K uma extensão de corpos. Um subconjunto finito $\{x_1, \ldots, x_r\} \subset F$ é algebricamente independente sobre K se não existe $F(t_1, \ldots, t_r)$ em $K[t_1, \ldots, t_r]$ satisfazendo $F(x_1, \ldots, x_r) = 0$. Um subconjunto arbitrário $S \subset F$ é algebricamente independente sobre K se todos os subconjuntos finitos de S são algebricamente independentes sobre K.

Uma base de transcendência da extensão F/K é um subconjunto $\mathcal{A}$ de F que satisfaz:

- $\mathcal{A}$ é algebricamente independente.
- $\mathcal{A} \subset \mathcal{A}'$ e $\mathcal{A}'$ é um subconjunto algebricamente independente de F, então $\mathcal{A} = \mathcal{A}'$.

Um resultado sobre a cardinalidade é o seguinte:

Quaisquer duas bases de transcendncia da extenso F/K *possuem a mesma cardinalidade.*

Portanto chamamos de *grau de transcendência*, e denotamos por $trdeg(F/K)$, a cardinalidade da base transcendência de F/K.

Sobre o grau de transcendência de F/K temos dois resultados importantes: *F/K é uma extensão algébrica se, e somente se,* $trdeg(F/K) = 0$.

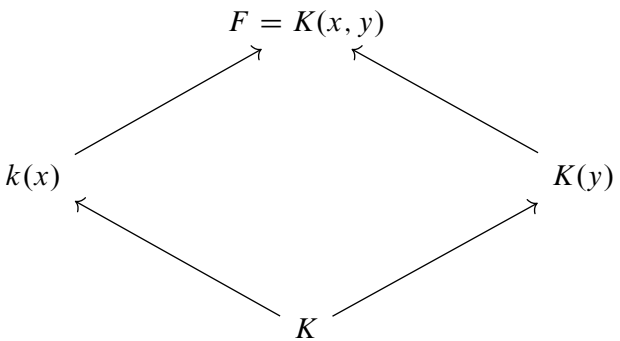
Se F é algébrico sobre $K(A)$, para algum subconjunto A de F, então A contém uma base de transcendência de F/K.

Exemplo 1.2.2. *O* corpo de funções racionais F/K *é chamado racional se* $F = K(x)$, *para algum* $x \in F$ *que é transcendente sobre* K. *Mais adiante iremos explorar esse exemplo de forma mais profunda.*

Exemplo 1.2.3. *Seja* $K = \mathbb{Q}$ *e considere* $p(X, Y) = X^3 - Y^2 + Y + 1 \in K[X, Y]$. *Considere o quociente* $F = \frac{K[X,Y]}{p(X,Y)}$. *Fazendo* $x := X \ mod \ p(X, Y)$ *e* $y := Y \ mod \ p(X, Y)$ *temos que* $F = K(x, y)$ *com* $x^3 = y^2 - y - 1$ *é um corpo de funções algébricas de uma variável.*

Segue da Teoria de Extensões de Corpos uma representação F/K através de uma equação polinomial. Uma vez que x é transcendente sobre K temos que

$F/K(x)$ é uma extensão finita. Se tomarmos qualquer outro elemento transcendente y sobre K então x e y terão uma relação de dependência sobre K uma vez que o grau de transcendência é um. Em outras palavras, existe um polinômio $p(t_1, t_2) \in K[z, w]$ tal que $p(x, y) = 0$. Desta forma, concluímos que x é algébrico sobre $K(y)$ (via $p(t_1, y) \in K(y)[t_1]$) e y algébrico sobre $K(x)$ (via $p(x, t_2) \in K(x)[t_2]$). Vendo o corpo de funções F/K como $F = K(x, y)$ podemos escolher estudar a extensão mais conveniente pois podemos ver como duas extensões, isto é, podemos ver F como extensão de $k(x)$ ou de $K(y)$. Conforme diagrama abaixo.



Observamos que a definição acima pode ser resgatada se partimos de uma curva plana projetiva (ou afim). Seja $\mathcal{X}_F$ um curva plana algébrica, projetiva, irredutível sobre um corpo K associada ao polinômio homogêneo $F \in K[X, Y, Z]$.

Desta forma consideramos o seguinte conjunto

$$\frac{K(X,Y,Z)}{(F)} := \left\{\overline{G}(X,Y,Z) |\ G(X,Y,Z) \in K(X,Y,Z)\ G \text{ homogêneo}\right\},$$

onde $\overline{G}(X, Y, Z)$ denota a classe do polinômio G. Tal conjunto é um domínio de integridade, pois F é irredutível. Dizemos que dois polinômios são equivalentes se sua diferença é múltipla de F. Isto nos permite construir o corpo de frações $\mathcal{Q}_F$. Para avaliar uma tal fração em um ponto projetivo, queremos o resultado não dependa do representante do representante escolhido. Portanto, exigimos que o numerador e o denominador tenham um representantes ambos com o mesmo grau. O corpo de funções de $\mathcal{X}_F$, denotado por $K(\mathcal{X}_F)$, é o conjunto de elementos de $\mathcal{Q}_F$ admitindo uma tal representação (O caso afim é obtido de forma similar). Esses elementos recebem o nome de *funções racionais* de $\mathcal{X}_F$. Um elemento $z \in K(\mathcal{X}_F)$ é chamado de *função regular* em um ponto p se $z = \frac{G(X,Y,Z)}{Q(X,Y,Z)}$ com $Q(p) \neq 0$.

Títulos Publicados — 33º Colóquio Brasileiro de Matemática

Geometria Lipschitz das singularidades – *Lev Birbrair e Edvalter Sena*

Combinatória – *Fábio Botler, Maurício Collares, Taísa Martins, Walner Mendonça, Rob Morris e Guilherme Mota*

Códigos Geométricos – *Gilberto Brito de Almeida Filho e Saeed Tafazolian*

Topologia e geometria de 3-variedades – *André Salles de Carvalho e Rafał Marian Siejakowski*

Ciência de Dados: Algoritmos e Aplicações – *Luerbio Faria, Fabiano de Souza Oliveira, Paulo Eustáquio Duarte Pinto e Jayme Luiz Szwarcfiter*

Discovering Euclidean Phenomena in Poncelet Families – *Ronaldo A. Garcia e Dan S. Reznik*

Introdução à geometria e topologia dos sistemas dinâmicos em superfícies e além – *Víctor León e Bruno Scárdua*

Equações diferenciais e modelos epidemiológicos – *Marlon M. López-Flores, Dan Marchesin, Vítor Matos e Stephen Schecter*

Differential Equation Models in Epidemiology – *Marlon M. López-Flores, Dan Marchesin, Vítor Matos e Stephen Schecter*

A friendly invitation to Fourier analysis on polytopes – *Sinai Robins*

PI-álgebras: uma introdução à PI-teoria – *Rafael Bezerra dos Santos e Ana Cristina Vieira*

First steps into Model Order Reduction – *Alessandro Alla*

The Einstein Constraint Equations – *Rodrigo Avalos e Jorge H. Lira*

Dynamics of Circle Mappings – *Edson de Faria e Pablo Guarino*

Statistical model selection for stochastic systems – *Antonio Galves, Florencia Leonardi e Guilherme Ost*

Transfer Operators in Hyperbolic Dynamics – *Mark F. Demers, Niloofar Kiamari e Carlangelo Liverani*

A Course in Hodge Theory Periods of Algebraic Cycles – *Hossein Movasati e Roberto Villaflor Loyola*

A dynamical system approach for Lane–Emden type problems – *Liliane Maia, Gabrielle Nornberg e Filomena Pacella*

Visualizing Thurston's Geometries – *Tiago Novello, Vinícius da Silva e Luiz Velho*

Scaling Problems, Algorithms and Applications to Computer Science and Statistics – *Rafael Oliveira e Akshay Ramachandran*

An Introduction to Characteristic Classes – *Jean-Paul Brasselet*

impa

Instituto de
Matemática
Pura e Aplicada

ISBN 978-65-89124-49-8

9 786589 124498