Corpos Numéricos e Aplicações em Reticulados

Eduardo Rogério Fávaro (eduardofavaro@yhaoo.com.br)

Orientador: **Antonio Aparecido de Andrade** (andrade@ibilce.unesp.br)

UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Campus de São José do Rio Preto

III Bienal da SBM - IME/UFG - 2006

1 Anéis Noetherianos e Domínios de Dedekeing

Sejam A um anel e M uma A-módulo. São equivalentes:

1. Todo família não vazia de submódulos de M coontém um elemento maximal;
2. Toda cadeia ascentente de submódulos de M é estacionária;
3. Todo submódulo de M é finitamentye gerado.

Se M satisfaz uma das três condições anteriores dizemos que M é um A-módulo Noetheriano. Dizemos que A é um anel Noetheriano se A, quando considerado como um A-módulo, for Noetheriano. Veja que todo anel principal, em particular $\mathbb{Z}$, é Noetheriano, pois seus ideais são gerados por um único elemento.

Um dominio A é um domínio de Dedekind, se A é Noetheriano, é integralmente fechado e se todo ideal primo não nulo é maximal.

Como todo dominio principal é integralmente fechado, e nele todo ideal primo não nulo é maximal, segue que um domínio de ideais principais é um domínio de Dedekind. Assim, $\mathbb{Z}$, $\mathbb{Z}[i]$ e $K[x]$, com K um corpo, são domínios de Dedekind.

Um resultado importante para mostrar que um dominio é de Dedekind é o seguinte:

Sejam A um anel de Dedekind, K seu corpo de frações e L uma extensão finita de K. Nestas condições, temos que o fecho inteiro de A de L é um domínio de Dedekind.

Disso, segue que o anel de inteiros de um corpo de números é um anel de Dedekind.

2 Corpos Quadrados e Ciclotômicos

Os corpos quadráticos e os corpos ciclotômicos são duas classes importantes de corpos de números.

Um corpo quadrático é um corpo numérico de grau 2, isto é, é uma extensão de grau 2 sobre $\mathbb{Q}$. Como consequência, os corpos quadráticos são da forma $K = Q(\sqrt{d})$, onde d é um inteiro livre de quadrados. Os monomorfismos de K em $\mathbb{C}$ são $\sigma_1(a+b\sqrt{d}) = a+b\sqrt{d}$ e $\sigma_2(a+b\sqrt{d}) = a-b\sqrt{d}$.

O anel de inteiros de um corpo quadrático K é dado por $\mathcal{O}_K = \mathbb{Z}[\alpha]$, onde $\alpha = \sqrt{d}$ se $d \equiv 2(mod\ 4)$ ou $d \equiv 3(mod\ 4)$, e $\alpha = \frac{1+\sqrt{d}}{2}$ se $d \equiv 1(mod\ 4)$. Para $d \equiv 2(mod\ 4)$ ou $d \equiv 3(mod\ 4)$, o discriminante de K é $D_K = 4d$, e para $d \equiv 1(mod\ 4)$, $D_K = d$.

Chamamos de n-éssimo corpo ciclotômico o corpo $Q(\xi_n)$, onde ξ_n é uma raiz n-éssima da unidade Neste caso, temos que $\xi_n = e^{2\pi i/n}$. O polinômio irredutível de ξ_n é $\Phi_n(x) = \prod_{\substack{i=1 \\ mdc(i,n)=1}}^{n} (x - \xi_n^i) \in \mathbb{Z}[x]$, e é chamado de n-éssimo polinômio ciclotômico. Um algoritmo para gerar os polinômios ciclotômiso é dado por

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Para $n = p$ primo, $x^p - 1 = \Phi_p(x)\Phi_1(x)$. Dai

$$\Phi_p(x) = \frac{x^p-1}{\Phi_1(x)} = \frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Para encontrarmos o anel de inteiros de $K = \mathbb{Q}(\xi_n)$, e o seu disciminante, são necessárias várias etapas. Deste modo, temos que o anel de inteiros é $\mathcal{O}_K = \mathbb{Z}[\xi_n]$, e o discriminante de K é dado por $D_K = \pm\frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}}$.

3 Fatoração

Para motivar a introdução da fatoração de ideais em ideais primos, que é feita de modo único em donínios de Dedekind, damos um exemplo de um anel de inteiros de um corpo de números que não é fatoriail, isto é, não vale a unicidade da fatoração de elementos em elementos irredutíveis. Como um exemplo deste fato, temos que $\mathbb{Z}[\sqrt{-5}]$ é o anel de inteiros de $\mathbb{Q}(\sqrt{-5})$ e não é fatorial pois $6 = 2 \times 3 = (1+\sqrt{-5})(1-\sqrt{-5})$, onde 2, 3, $1+\sqrt{-5}$ e $1+\sqrt{-5}$ são elementos irredutíveis em $\mathbb{Z}[\sqrt{-5}]$.

Agora, voltamos a fatoração de ideais. Para isso, seja $\mathcal{O}_K$ o anel de inteiros de um corpo de números K. Neste caso, temos que para um ideal $\mathfrak{a}$ de $\mathcal{O}_K$, existem ideais primos $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ de $\mathcal{O}_K$ tais que $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_n$ e tal fatoração é única. Assim, podemos supor que os ideais primos $\mathfrak{p}_i$ são distintos e podemos reescrever como $\mathfrak{a} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_n^{e_n}$, com $e_i \geqslant 1$ inteiros positivos.

Como um exemplo, tomando $K = \mathbb{Q}(\sqrt{-17})$ e $\mathcal{O}_K = \mathbb{Z}[\sqrt{-17}]$, temos que $18 = 2\times 3\times 3 = (1+\sqrt{-17})(1-\sqrt{-17})$. Deste modo, temos que o ideal 18 tem uma fatoração em elementos irredutíveis de dois modos. Assim, $< 18 >=< 2 >< 3 >< 3 >=< 1+\sqrt{-17} >< 1-\sqrt{-17} >$. Agora, tomando $\mathfrak{p} =< 2, 1+\sqrt{-17} >, \mathfrak{q} =< 3, 1+\sqrt{-17} >$ e $\mathfrak{r} =< 3, 1-\sqrt{-17} >$ ideais de $\mathcal{O}_K$, temos que $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}$ são ideais primos. Assim, $< 18 >= \mathfrak{p}^2\mathfrak{q}^2\mathfrak{r}^2$, e $< 2 >= \mathfrak{p}^2$, $< 3 >= \mathfrak{q}\mathfrak{r}$, $< 1+\sqrt{-17} >= \mathfrak{p}\mathfrak{q}^2$, $< 1-\sqrt{-17} >= \mathfrak{p}\mathfrak{r}^2$.

De um modo mais geral, tomando $K \subseteq L$ corpos de números, com $[L : K] = n$, $\mathfrak{p}$ um ideal primo não nulo de $\mathcal{O}_K$ e

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$$

a decomposição de $\mathfrak{p}\mathcal{O}_K$ em ideais primos de $\mathcal{O}_K$, temos que os ideais $\mathfrak{p}_i's$ são ideais primos $\mathfrak{q}$ de $\mathcal{O}_L$ acima de $\mathfrak{p}$, isto é, $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$. Os expoentes $e_i's$ são chamados de indice de ramificação de p e são denotados por $e(\mathfrak{q}|\mathfrak{p})$. Além do mais, temos que $\mathcal{O}_K/\mathfrak{p}$ e $\mathcal{O}_L/\mathfrak{q}$ são corpos finitos, chamados de corpos residuais associados a $\mathfrak{p}$ e $\mathfrak{q}$, respectivamente. Além disso, $\mathcal{O}_L/\mathfrak{q}$ é uma extensão de grau finito sobre $\mathcal{O}_K/\mathfrak{p}$. O grau dessa extensão é chamado de grau de inércia ou grau residual de $\mathfrak{q}$ sobre $\mathfrak{p}$, e é denotado por $f = f(\mathfrak{q}|\mathfrak{p})$.

Se denotarmos por $e_1, e_2, \ldots, e_g$ e $f_1, f_2, \ldots, f_g$ os índices de ramificação e graus residuais de $\mathfrak{p}_i$ sobre $\mathfrak{p}$ na decomposição acima, temos que a seguinte igualdade fundamental:

$$n = \sum_{i=1}^{g} e_i f_i = [\mathcal{O}_L/\mathfrak{p} : \mathcal{O}_K/\mathfrak{q}] = [\mathcal{O}_L : \mathcal{O}_k].$$

4 Norma de um Ideal

Uma ferramenta para decidirmos se um ideal é primo, é a norma de um ideal, que de certo modo, é uma generalização da norma um elemento de $\mathcal{O}_K$.

Se K é um corpo de números de grau n, $\mathcal{O}_K$ é seu anel de inteiros e $\mathfrak{a}$ é um ideal não nulo de $\mathcal{O}_K$, definimos a norma $N(\mathfrak{a})$ de $\mathfrak{a}$ como sendo o número de elementos do anel quociente $\mathcal{O}_K/\mathfrak{a}$. Desse modo, temos que $N(\mathfrak{a})$ é um inteiro positivo.

Temos as seguinte propriedades relacionadas à norma de um ideal:

1. Todo ideal $\mathfrak{a}$ não nulo de $\mathcal{O}_K$ tem uma $\mathbb{Z}$-base $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, isto é, $\mathfrak{a}$ é um $\mathbb{Z}$, módulo livre de posto n.
2. Como no ítem anterior, se D_K é o discriminante de K, então
$$N(\mathfrak{a}) = \left|\frac{\Delta[\alpha_1, \alpha_2, \ldots, \alpha_n]}{D_K}\right|^{1/2};$$
3. Se $\mathfrak{a} =< a >$ é um ideal primo, $N(\mathfrak{a}) = |N(a)|$.
4. Se $\mathfrak{a}$ e $\mathfrak{b}$ são ideais não nulos, então $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$. Assim, se $N(\mathfrak{a})$ é um inteiro primo, então $\mathfrak{a}$ é um ideal primo.

Observamos que nem sempre a norma de um ideal primo é um número primo. Por exemplo, tomando $\mathcal{O}_K = \mathbb{Z}[\sqrt{-1}]$ e $\mathfrak{a} =< 11 >$, temos que 11 é irredutível, e $\mathbb{Z}[\sqrt{-1}]$ é fatorial. Deste modo, temos que 11 é um número primo, $< 11 >$ é um ideal primo, mas $N(< 11 >) = |N(11)| = 11^2$ não é um número primo.

5 Lema de Kummer

Dados um polinômio $f(x) = \sum_{i=1}^{m} a_i x^i \in \mathbb{Z}$ e p um primo, denotamos por $\overline{p}(x) = \sum_{i=1}^{m}(a_i + p\mathbb{Z})x^i \in \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$.

Sejam K um corpo de números de grau n, $\mathcal{O}_K$ seu anel de inteiros e $\theta \in \mathcal{O}_K$ tal que $K = \mathbb{Q}(\theta)$. Dado um primo p que não divide n, e f o polinômio irredutível de θ sobre $\mathbb{Q}$, então existem polinômios $p_1, p_2, \ldots, p_g \in \mathbb{Z}[x]$ com $\overline{p_i}$ irredutível em $\mathbb{Z}_p[x]$, $e_1, e_2, \ldots, e_g \in \mathbb{N}^*$, tal que

$$f \equiv p_i^{e_1}p_2^{e_2}\ldots p_g^{e_n}(mod\ p\mathbb{Z}) \quad e,$$

1. $\mathfrak{p}_\mathfrak{i} =< p, p_i(\theta) >= p\mathcal{O}_K + p_i(\theta)\mathcal{O}_K$ são ideais primos de $\mathcal{O}_K$ acima de $p\mathbb{Z}$;
2. $p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$;
3. $[\mathcal{O}_K/\mathfrak{p}_i : Z/p\mathbb{Z}] = \text{grau}(p_i) = f_i$.

Exemplos

1. $K = \mathbb{Q}(\sqrt{-17})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-17}]$, $\theta = \sqrt{-11}$ e $p = 5$. Temos $f = x^2+17$, $\overline{f} = x^2 + (2 + 17\mathbb{Z}) \in \mathbb{Z}/5\mathbb{Z}$. Dai $\overline{f}$ é irredutível em $\mathbb{Z}/5\mathbb{Z}$. Assim, $g = 1$, $p_1 = x^2 + 2$, $e_1 = 1$. Logo
$$< 5 >= 5\mathbb{Z}[\sqrt{-17}] = 5\mathbb{Z}[\sqrt{-17}] + (-17+2)\mathbb{Z}[\sqrt{-17}] = 5\mathbb{Z}[\sqrt{-17}].$$
Portanto $5\mathbb{Z}[\sqrt{-17}]$ é um ideal primo em $\mathbb{Z}[\sqrt{-17}]$.
2. $K = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, $\theta = \sqrt{-5}$ e $p = 2$. Temos $f = x^2 + 5$, $\overline{f} = x^2 + \overline{5} = (x + \overline{1})^2 \in \mathbb{Z}/5\mathbb{Z}$, isto é $f \equiv (x+1)^2(mod\ 2\mathbb{Z})$. Assim, $g = 1$, $p_1 = x + 1$, $e_1 = 2$. Consequentemente
$$< 2 >= 2\mathcal{O}_K = \left(2\mathcal{O}_K + (\sqrt{-5}+1)\mathcal{O}_K\right)^2 =< 2, \sqrt{-5}+1 >^2,$$
com $< 2, \sqrt{-5}+1 >$ ideal primo em $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$.
3. $K = \mathbb{Q}(\xi_{15})$, $\mathcal{O}_K = \mathbb{Z}[\xi_{15}]$, $\theta = \xi_{15}$ e $p = 7$. Temos que $f = \Phi_{15} = x^8 - x^7 + x^5 - x^4 + x^2 + 2$. Veja que $p_1 = x^4 + 4x^3 + 2x^2 + x + 4$ e $p_2 = x^4+2x^3+4x^2+x+2$ satisfaz $f \equiv p_1p_2(mod\ 7\mathbb{Z})$. Desse modo, temos $g = 2$ $e_1 = 1$, $e_2 = 1$. E assim $\mathfrak{p}_i =< 7, p_i(\xi_{15}) >= 7\mathcal{O}_K + p_i(\xi_{15})\mathcal{O}_K$ são ideais primos de $\mathcal{O}_K$ tais que $7\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$.

6 Reticulados

De modo informal, um reticulado é um conjunto discreto de pontos de R^n. Um problema é encontrar um arranjo de esferas identicas com centro nesses pontos de modo que a proporção do espaço coberto por elas seja máximo. Muitos resultados mostram que o anel dos inteiros de um corpo ciclotômico é como um universo capaz de reproduzir ideais ordinários não nulos cuja representação geométrica coincidam com os reticulados mais densos conhecidos e até assumam novos recordes. Passamos as definições mais formais.

Sejam V um $\mathbb{R}$-espaço vetorial e $\beta = \{v_1, v_2, \ldots, v_n\}$ uma base para V. O reticulado com base β é o subconjunto de V,

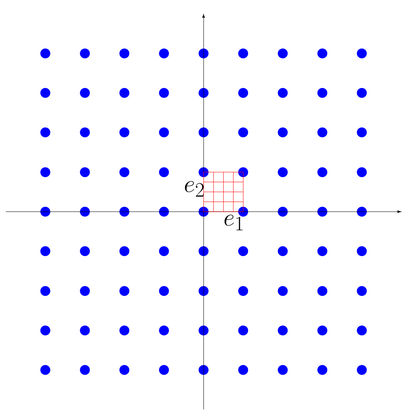
$$\mathcal{H}_\beta = \left\{ x = \sum_{i=1}^{n} a_i v_i; a_i \in \mathbb{R} \right\}.$$

E ao conjuto

$$\mathcal{P}_\beta = \left\{ x \in \mathbb{R}^n; x = \sum_{i=1}^{n} \lambda_i v_i, 0 \leq \lambda_i < 1 \right\},$$

definimos como a região fundamental de $\mathcal{H}_\beta$, com relação a base β.

Exemplo $\mathcal{H}_\beta = \mathbb{Z}^2$ é um reticulado gerado pelos vetores $e_1 = (1, 0)$ e $e_2 = (0, 1)$ com região fundamental descrita na figura abaixo.



Para o reticulado $\mathcal{H}_\beta$, com base base $\beta = \{v_1, v_2, \ldots, v_n\}$. Se $v_i = (v_{i1}, \ldots, v_{in})$, para $i = 1, 2, \ldots, n$, definimos o volume do reticulado $\mathcal{H}_\beta$ como o módulo do determinante da matriz

$$\begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n1} & v_{n2} & \cdots & v_{nn} \end{pmatrix},$$

que é indepentdente da base β, e denotamos por $\text{Vol}(\mathcal{H}_\beta)$.

Um empacotamento reticulado, é uma distribuição de esferas de mesmo raio no $\mathbb{R}^n$, em que o conjunto dos centros das esferas formem um reticulado $\mathcal{H}$ do $\mathbb{R}^n$, de forma que a interseção de quaisquer duas esferas tenha no máximo um ponto. Pode-se descrever um empacotamento indicando apenas o conjunto dos centros das esferas e o raio. A densidade de empacotamento é a proporção do espaço $\mathbb{R}^n$ coberto pela união das esferas.

Temos que $(\mathcal{H}_{\beta_{min}})^2$ é chamado de norma mínima de $\mathcal{H}_\beta$, onde $\mathcal{H}_{\beta_{min}} = \min\{|\lambda|; \lambda \in \mathcal{H}_\beta, \lambda \neq 0\}$, e que $\rho = \frac{\mathcal{H}_{\beta_{min}}}{2}$ é o maior raio para o qual é possível distribuir esferas centradas nos pontos de $\mathcal{H}_\beta$ e obter um empacotamento. Dessa forma, estudar os empacotamentos reticulados equivale ao estudo dos reticulados. Neste caso, o que importa é a densidade de centro, dada por

$$\delta(\mathcal{H}_\beta) = \frac{\rho^n}{\text{Vol}(\mathcal{H}_\beta)}.$$

Para o reticulado $\mathcal{H}_\beta = \mathbb{Z}^n$ com base $e_1, e_1, \ldots, e_n$, temos que $\rho = 1/2$. Dai a densidade de centro é $\delta(\mathcal{H}_\beta) = 1/2^n$.

7 Homomorfismo Canônico

Existem vários métodos para obter um reticulado a partir de ideais do anel de corpos de números. Utilizaremos o método de Minkowisk.

Sejam K um corpo de números de grau n e $\sigma_j : K \longrightarrow \mathbb{C}$, os monomorfismos distintos de K em $\mathbb{C}$. Se $\sigma_j(K) \subseteq \mathbb{R}$, diz-se que σ_j é real, caso contrário, σ_j é dito imaginário. Quando todos os monomorfismos são reais diz-se que K é um corpo totalmente real e quando os monomorfismos são todos imaginários diz-se que K é um corpo totalmente complexo.

Veja que para cada σ_j imaginário, existe $k \neq j$ tal que σ_k é o conjugado complexo de σ_j. Dai os monomorfismos imaginários aparrecem ao pares. Denotando por r_1 o número homomorfismos reais, podemos reordenar os monomorfismos $\sigma_1, \ldots, \sigma_n$ de modo que $\sigma_1, \ldots, \sigma_{r_1}$ sejam os monomorfismos reais e que $\sigma_{r_1+1}, \ldots, \sigma_{r_2}$ sejam os pares de monomorfismos imaginários. Assim, $n = r_1 + 2r_2$ e para cada $x \in K$, temos que o homomorfismo $\sigma_K : K \longrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ definido por

$$\sigma_K(x) = (\sigma_1(x), \ldots, \sigma_{r_1+r_2(x)}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2},$$

é um homomorfismo injetivo de anéis, chamado de homomorfismo canônico ou homomorfismo de Minkowisk, de K em $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$.

Geralmente identificamos $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ com $\mathbb{R}^n$, e este homomorfismo também pode ser visto como

$$\sigma_K(x) = (\sigma_1(x), \ldots, \sigma_{r_1}(x), \text{Re}\sigma_{r_1+1}(x), \text{Im}\sigma_{r_1+1}(x), \ldots, \text{Re}\sigma_{r_1+r_2}(x), \text{Im}\sigma_{r_1+r_2}(x)),$$

onde Re representa a parte real e Im representa a parte imaginária do número complexo.

Se K é um corpo de números de grau n e $\mathfrak{a}$ um ideal não nulo de $\mathcal{O}_K$, a densidade de centro de $\sigma_K(\mathfrak{a}) = \{\sigma_K(x); x \in \mathfrak{a}\}$ é dada por

$$\frac{\left(\frac{t_\mathfrak{a}}{4}\right)^{\frac{n}{2}}}{|D_K|^{\frac{1}{2}}\, N(\mathfrak{a})},$$

onde $t_\mathfrak{a} = min\{Tr(x\overline{x}),\ x \in \mathfrak{a},\ x \neq 0\}$.

Exemplos

1. Se $K = \mathbb{Q}(\sqrt{7})$ então $\mathcal{O}_K = \mathbb{Z}[\sqrt{7}]$ e $D_K = 28$. Se $\alpha = a + b\sqrt{7} \in \mathcal{O}_K$, temos $Tr(\alpha\overline{\alpha}) = 2(a^2 + 7b^2)$, e assim $t_{\mathcal{O}_k} = min\{Tr(\alpha\overline{\alpha}); \alpha \neq 0,\ \alpha \in \mathcal{O}_K\} = 2$, para $a = 1$ e $b = 0$. Assim,
$$\delta(\sigma_K(\mathcal{O}_K)) = \frac{1}{2\sqrt{28}} \simeq 0,09449.$$
2. Sejam $K = \mathbb{Q}(\sqrt{5})$, $O_K = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ e $\dashv$ o ideal principal de $\mathcal{O}_K$ gerado por $\gamma = 3 - 2\sqrt{5}$. A densidade de centro é dada por
$$\delta(\sigma_K(\mathfrak{a})) = \frac{27}{44\sqrt{5}} \simeq 0,2744.$$
3. Para o corpo ciclotômico $\mathbb{Q}(\xi_3)$, temos que $\mathcal{O}_K = \mathbb{Z}[\xi_3]$. A densidade de centro de ideal principal $\mathfrak{p}$ gerado por $1 - \xi_3$ é $\frac{1}{2\sqrt{3}} \simeq 0,288675$, que é a maior densidade de centro em dimensão 2 conhecida na literatura.

8 Referências

1. **Endler, O.** "*Teoria dos números algébricos.*" Rio de Janeiro, IMPA, 1986.
2. **Samuel, P.** "*Algebraic theory of numbers.*" Paris, Hermana 1967.
3. **Stewart, I., Tall, D.** "*Algebric number theory.*" Chapman & New York, Hall 1987.

9 Agradecimentos

FAPESP