A RELAÇÃO DA RAMIFICAÇÃO COM OS CONCEITOS DE DISCRIMINANTE[1]

THE RELATION OF THE RAMIFICATION WITH THE CONCEPTS OF DISCRIMINANT

Ciléia Mazzei de OLIVEIRA[2]

***Resumo*:** Este artigo apresenta estudos sobre a Teoria Algébrica dos Números que tem sido bastante útil no desenvolvimento de códigos corretores de erros e reticulados. Corpos finitos foram a ferramenta chave para o desenvolvimento dos códigos binários, estruturas que despertaram gradativamente o interesse dos pesquisadores em teoria das comunicações. O objetivo deste trabalho foi relacionar a ramificação com os conceitos de discriminante.

***Palavras-chave*:** Discriminante. Ramificação.

***Abstract*:** This article introduces studies about Algebraic Number theory that has been enough availed in the development of error correction codes and lattices. Finite fields were the key for the development of binary codes, structures that aroused little by little the interest of researchers in communication theory. The aim of this work was to relate ramification with the concepts of discriminant.

***Keywords*:** Discriminant. Ramification.

[1] Este presente trabalho toma por base a dissertação de mestrado: Discriminante, Ramificação e Diferente, defendida por Ciléia Mazzei de Oliveira ao Departamento de Matemática - IBILCE – UNESP.

[2] Mestra em Matemática pela Universidade Estadual de São Paulo – UNESP/SP, área de Álgebra. Professora de Matemática da Faculdade da Fundação Educacional de Araçatuba/SP – FAC-FEA. cileia.mazzei@ig.com.br

Conceitos Básicos - Teoria dos Números Algébricos

Esta seção tem como objetivo o de introduzir conceitos importantes da Teoria Algébrica dos Números, os quais são utilizados posteriormente, tais como, elementos inteiros sobre um anel; sobre um corpo de números veremos os corpos quadráticos e, para finalizar, observaremos as principais propriedades dos anéis Noetherianos, dos anéis de Dedekind e dos anéis de frações.

Definição 1.1: Sejam A $\subseteq B$,A e B anéis. Dizemos que um elemento $\alpha \in$ B é inteiro sobre A, se α é uma raiz de um polinômio mônico com coeficientes em A, ou seja, se existem $a_0, a_1, ..., a_{n-1} \in$ A, não todos nulos, tal que $\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_0 = 0$. Essa equação é chamada de equação de dependência integral de α.

Teorema 1.1: Sejam A $\subseteq B$ e $\alpha \in$ B. São equivalentes as seguintes afirmações:

a) α é inteiro sobre A.

b) O anel A[α] é um A-módulo finitamente gerado.

c) Existe um subanel R do anel B tal que R é um A-módulo finitamente gerado que contém A e α.

Corolário 1.1: Sejam **A** $\subseteq B$ **e** $\alpha \in$ **B. Se** α, $\beta \in$ B são inteiros sobre A, então $\alpha \pm \beta, \alpha . \beta$ são inteiros sobre A.

Definição 1.2: Sejam **A** $\subseteq B$ anéis.

a) OB = { $\alpha \in$ B : α é inteiro sobre A} é chamado anel dos inteiros de A em B, ou fecho inteiro de A em B.

b) Se A é um domínio e B = K o corpo de frações de A, dizemos que OB é o anel dos inteiros de A em K. Além disso, se A = OB dizemos que A é um anel integralmente fechado.

c) Se $\mathbf{A} \subseteq B$ são anéis, então A $\subseteq$ OB $\subseteq$B.

Definição 1.3: Seja o endomorfismo θ_α: B −>B definido por θ_α (x) = αx, com $\alpha \in$ B. O traço de $\alpha \in$ B é definido por TrB|A(α) = TrB|A(θ_α), a norma de $\alpha \in$ B por NB|A(α) = det(θ_α) e o polinômio característico de α por mB|A(x) = det(xI − θ_α).

Proposição 1.1: Seja K um corpo de característica 0 ou um corpo finito. Sejam L uma extensão algébrica de grau n de K, α é um elemento de L e $\alpha_1,...,\alpha_n$ as raízes do polinômio minimal de α sobre K. Então TrL|K(α) = $\alpha_1 + ... + \alpha_n$, NL|K($\alpha$) = $\alpha_1 \cdot ... \cdot \alpha_n$ e o polinômio característico de α é mL|K(x) = (x − α_1)(x − α_2) · · · (x − α_n).

Proposição 1.2: Sejam A um domínio, K seu corpo de frações, K $\subseteq$ L uma extensão finita de grau n e $\alpha \in$ L um elemento inteiro sobre A. Então os coeficientes do polinômio característico de α são inteiros sobre A. Em particular, TrL|K(α) e NL|K(α) são inteiros sobre A.

Proposição 1.3: Sejam A um anel integralmente fechado, K seu corpo de frações, L uma extensão finita de K de grau n e OL o anel dos inteiros de A em L. Seja $\{\alpha_1,...,\alpha_n\}$ uma base de L sobre K onde det(TrL|K(α i α j)) ≠ 0. Seja $\alpha \in$ L. Se TrL|K(α . β) = 0 para todo $\beta \in$ L, então α = 0.

Definição 1.4: Um corpo de números é uma extensão finita de Q. Um corpo quadrático é uma extensão de grau 2 de Q.

Proposição 1.4: Um corpo quadrático é da forma Q($\sqrt{d}$), onde d é um inteiro livre de quadrados.

Observação 1.1: O elemento $\sqrt{d}$ é uma raiz do polinômio irredutível $x^2 - d$. O conjugado de $\sqrt{d}$ é $-\sqrt{d}$, ou seja, existe um automorfismo σ : Q($\sqrt{d}$) −> Q($\sqrt{d}$) tal que σ (a + b$\sqrt{d}$) = a − b $\sqrt{d}$.

Teorema 1.2 : Seja K = Q($\sqrt{d}$) um corpo quadrático, com d $\in$ Z livre de quadrados, ou seja, d não é côngruo a 0 mod 4.

a) Se d $\equiv$ 2 ou d $\equiv$ 3(modulo 4), então o anel dos inteiros OK, consiste de todos os elementos da forma a + b$\sqrt{d}$, com a, b $\in$ Z.

b) Se d $\equiv$ 1(modulo 4), então o anel dos inteiros OK, consiste de todos os elementos da forma $\frac{1}{2}$(a + b$\sqrt{d}$), com a, b $\in$ Z, e de mesma paridade.

Definição 1.5: Sejam A um anel e M um A-módulo. Dizemos que M é um A-módulo Noetheriano se satisfaz uma das seguintes condições:

a) Toda família não vazia de A-submódulos de M tem um elemento maximal.

b) Toda sequência crescente de A-submódulos de M é estacionária.

c) Todo A-submódulo de M é finitamente gerado. Dizemos que um anel A é Noetheriano se A considerado como um A-módulo for Noetheriano.

d) Todo anel principal A é Noetheriano.

e) Se A é um anel Noetheriano e M é um A-módulo finitamente gerado, então M é um A-módulo Noetheriano.

Proposição 1.5: Seja A um anel Noetheriano e integralmente

fechado. Sejam K o corpo de frações de A, $K \subseteq L$ uma extensão finita de grau n e OL o anel dos inteiros de A em L. Então OL é um A-módulo finitamente gerado e OL é um anel Noetheriano.

Definição 1.6: Dizemos que um domínio A é um anel de Dedekind se satisfaz as seguintes condições:

a) A é integralmente fechado.

b) A é Noetheriano

c) Todo ideal primo não nulo de A é maximal.

Teorema 1.3: Sejam A um anel de Dedekind, K seu corpo de frações, $K \subseteq L$ uma extensão finita de grau n e OL o anel dos inteiros de A em L. Então OL é um anel Dedekind.

Ramificação e Discriminante

Nesta seção introduzimos primeiramente o conceito de ramificação e apresentamos algumas propriedades, incluindo o Teorema da Igualdade Fundamental. Também apresentamos o conceito de ramificação em corpos quadráticos. Em seguida, apresentamos o conceito de discriminante e também a relação entre ramificação e discriminante. Na penúltima seção teremos o Teorema de Kummer, o qual nos apresenta um método de decomposição através de polinômios. Finalizando, apresentamos o conceito de reticulado como um subconjunto discreto do Rn e depois, através da Teoria dos Números Algébricos, apresentamos um método para gerarmos reticulados.

Conceitos de Ramificação

Sejam A um anel de Dedekind, K seu corpo de frações, L uma extensão finita de K de grau n e OL o anel do inteiro de A em L. Pelo Teorema 1.3, segue que OL é um anel de Dedekind. Apresentamos nesta seção a decomposição de ideais primos não nulos P de A na extensão L, ou seja, veremos que o ideal estendido POL de OL, é expresso de modo único na forma POL= $\prod_{i=1}^{g} Q_i^{e_i}$, onde os Qi são ideais primos de OL e os ei são elementos de Z, para i = 1, · · · , g.

Proposição 2.1: Os ideais primos Qi de OL são os únicos ideais primos de OL tais que Qi $\cap$ A = P, para i = 1, · · · , g.

Definição 2.1: O grau fi = f(Qi|P) da extensão OL/Qi sobre A/P é chamado de grau de inércia de OL sobre A, e o expoente ei = e(Qi|P) é chamado de índice de ramificação de Qi sobre A.

Definição 2.2: Dizemos que P é:

a) totalmente decomposto em L (ou em OL) quando e(Q|P) = f(Q|P) = 1, para todo ideal primo Q que esta acima de P.

b) inerte em L (ou em OL) quando e(Q|P) = 1 e f(Q|P) = n, para todo ideal primo Q que esta acima de P. ..

c) totalmente ramificado em L (ou em OL) quando e(Q|P) = n e f(Q|P) = 1, para todo ideal primo Q que esta acima de P.

d) ramificado em L (ou em OL) se existir um ideal primo Qi de OL que esta acima de P tal que ei > 1 para algum i.

Lema 2.1: Com as notações acima temos que:

a) POL $\cap$ A = P

b) OL/POL é um espaço vetorial de dimensão finita sobre A/P.

Lema 2.2: A sequência de ideais

OL $\supset Q_1 \supset Q_1^2 \supset \ldots \supset Q_1^{e_1} \supset Q_1^{e_1}Q_2 \supset Q_1^{e_1}Q_2^{e_2} \supset \ldots \supset Q_1^{e_1}Q_2^{e_2} \ldots Q_g^{e_g}$ =POL é maximal.

Teorema 2.1: (Teorema da Igualdade Fundamental) $\sum_{i=1}^{g} e_i f_i$ = [OL/POL : A/P] = n.

Lema 2.3: Se A1, A2 são ideais de um anel A e A1 + A2 = A então A1A2 = A1 $\cap$ A2.

Teorema 2.2: Sejam K $\subseteq$ L $\subseteq$ L1 corpos de números, com respectivos anéis de inteiros OK $\subseteq$ OL $\subseteq$ OL1 . Seja I um ideal primo de OL1 , Q = I $\cap$ OL e P = Q $\cap$ OK. Então e(I|Q)e(Q|P) = e(I|P) e f(I|Q)f(Q|P) = f(I|P).

Ramificação em Corpos Quadráticos

Apresentamos especificamente a ramificação nos corpos quadráticos. Deste modo, sejam d $\in$ Z livre de quadrados, L = Q($\sqrt{d}$),

OL o anel dos inteiros de L e p um número primo. Seja pOL = $\prod_{i-1}^{g} Q_i^{e_i}$ i a decomposição em L do ideal pOL como um produto de ideais primos de OL. Pelo Teorema 2.1, segue que $\sum_{i=1}^{g} e_i f_i$ =2. Assim, g $\leq$ 2 e temos os seguintes casos:

a) Se g = 2, e1 = e2 = 1, f1 = f2 = 1, então p se decompõe em L, ou seja,

pOL = Q1Q2, onde Q1,Q2 são ideais primos de OL acima de pZ.

b) Se g = 1, e1 = 1, f1 = 2, então p é inerte em L, ou seja, pOL = Q, onde Q é um ideal primo de OL acima de pZ.

c) Se g = 1, e1 = 2, f1 = 1, então p ramifica em L, ou seja, pOL = Q2, onde Q é um ideal

primo de OL acima de pZ.

Definição 2.3: Dados um número primo ímpar p e um inteiro d relativamente primo com p, dizemos que d é um resíduo quadrático módulo p, se existir a 2 Z tal que

d $\equiv a^2$ (modulo p), isto é, se a classe de restos de d módulo p for um quadrado em Zp, caso contrário, d não é resíduo quadrático módulo p.

Exemplo 2.1: Se p = 5 então d = 19 é um resíduo quadrático módulo 5, pois existe a = 2 tal que 19 $\equiv 2^2$ (modulo 5). Se p = 7 então d = 19 não é resíduo quadrático módulo 7, pois não existe a tal que 19 $\equiv a^2$ (modulo 7).

Teorema 2.3 Seja L = Q($\sqrt{d}$) um corpo quadrático, onde d é um inteiro livre de quadrados.

a) Os primos ímpares p, onde d é um resíduo quadrático módulo p, decompõem em L.

b) Os primos ímpares p, onde d não é um resíduo quadrático módulo p, são inertes em L.

c) Os primos ímpares divisores de d ramificam em L.

Exemplo 2.2: Seja L = Q($\sqrt{10}$). Como 5 divide 10, temos pelo

Teorema 2.3, que 5

ramifica em L. Assim, e = 2 e f = 1. Agora, se p=3 então 10 é resíduo quadrático módulo 3, logo 3 decompõe. Assim, e = 1 e f = 1. Se p=7, temos que 10 não é resíduo quadrático módulo 7, então 7 é inerte.

Teorema 2.4 Seja L = Q($\sqrt{d}$), um corpo quadrático, onde d é um inteiro livre de quadrados. Então:

a) Se d $\equiv$ 1(modulo 8) então 2 se decompõe em L.

c) Se d $\equiv$ 5(modulo 8) então 2 é inerte em L.

d) Se d $\equiv$ 2(modulo 4) ou d $\equiv$ 3(modulo 4) então 2 ramifica em L.

Exemplo 2.3: Se L = Q($\sqrt{17}$), segue pelo Teorema 2.4 que 2 se decompõe em L. Se

L = Q($\sqrt{21}$), então 2 é inerte em L e se L = Q($\sqrt{6}$) então 2 ramifica em L.

Conceitos de Discriminante

Definição 2.4 Sejam A $\subseteq$ B anéis tal que B é um A - módulo livre de posto n. Seja $\{\alpha_1,...,\alpha_n\}$ $\subseteq$ B. Definimos o discriminante do conjunto $\{\alpha_1,...,\alpha_n\}$ por D($\alpha_1,...,\alpha_n$) = det(TrB|A($\alpha_i\alpha_j$)).

Exemplo 2.4: Sejam K = Q($\sqrt{1}$) um corpo de números e {1, $\sqrt{1}$ } $\subseteq$ K. Assim, D(1, $\sqrt{1}$) = $\begin{vmatrix} 2 & 0 \\ 0 & 22 \end{vmatrix}$ = 44.

Proposição 2.2: Sejam A $\subseteq$B anéis tal que B é um A - módulo livre de posto n. Se {y1, · · · , yn} é um conjunto de elementos de B, tais

que yi = $\sum_{j=1}^{n} a_{ij}\alpha_j$ com aij $\in$ A, para i = 1, · · · , n, então D(y1, · · · , yn)

= $\left(\det(\mathbf{aij})\right)^2$ D ($\alpha_1,...,\alpha_n$).

Proposição 2.3: Seja K = Q($\sqrt{d}$), onde d $\in$ Z é livre de quadrados. Se d $\equiv$ 2(módulo 4) ou d $\equiv$ 3(modulo 4) então o discriminante de OK, onde OK é o anel dos inteiros de K sobre Z, é 4d.

Proposição 2.4: Seja K = Q($\sqrt{d}$), onde d $\in$ Z é livre de quadrados. Se d $\equiv$ 1 (módulo 4) então o discriminante de OK, onde OK é o anel dos inteiros de K sobre Z, é d.

As Relações entre Ramificação e Discriminante

Sejam A um anel de Dedekind, K seu corpo de frações, L uma extensão finita de K de grau n e OL o anel do inteiro de A em L. Esta seção tem como objetivo relacionar os conceitos de ramificação e discriminante, onde provamos que os ideais primos de A ramificam se, e somente se, esses ideais contêm o discriminante.

Teorema 2.5 Sejam K $\subseteq$ L corpos de números. Sejam OK e OL os anéis dos inteiros de K e L, respectivamente, e P um ideal primo de OK. Então P ramifica se, e somente se, P$\supset$ DOL|OK.

Exemplo 2.5: Sejam K = Q e L = Q($\sqrt{d}$), onde d é um inteiro livre de quadrados.

a) Se d $\equiv$ 2 ou 3(modulo 4) então Z[$\sqrt{d}$] é o anel dos inteiros de K e D(1, $\sqrt{d}$) = 4d. Assim, os primos que se ramificam em K é o 2 e os divisores de d.

b) Se d $\equiv$ 1(modulo 4) então Z$\left[\frac{1+\sqrt{d}}{2}\right]$ é o anel dos inteiros de K e D (1, $\frac{1+\sqrt{d}}{2}$)=d. Assim, os primos que ramificam em K são os divisores de d.

Teorema de Kummer: Sejam OL = A[α], onde $\alpha \in$ OL, e mα |K(x) o polinômio minimal de α sobre K. Sejam m1(x), ...,mg(x) polinômios mônicos em A[x] tal que m(x) = m1(x)$^{e_1}\cdots$mg(x)^{e_g} é a fatoração de m(x) em polinômios irredutíveis distintos em (A/P)[x]. Então existem ideais primos distintos Q1, · · · ,Qg de OL acima de P tal que OL/Qi = A/P(α_i), onde α_i é uma raiz de mi(x), e assim f(Qi|P) = gr(mi), para i = 1, · · · , g.

Corolário 2.1. Com as hipóteses do Teorema de Kummer temos que:

a) P decompõe em L se, e somente se, m(x) fatora em (A/P)[x] em fatores lineares distintos x − (ai + P), para i = 1, · · · , n. Neste caso, POL = Q1 · · ·Qn, onde Qj = POL + (α − ai)OL são ideais primos distintos de OL, para i = 1, · · · , n.

b) P é inerte em L se, e somente se, m(x) é irredutível em (A/P)[x]. Neste caso, POL é um ideal primo de OL.

c) P é totalmente ramificado em L se, e somente se, m(x) é uma potência n-ésima em (A/P)[x], isto é, $m(x) = (x - (a + P))^n$, para algum $a \in A$. Neste caso, POL = Qn, onde Q =POL + (α − a)OL é um ideal de OL.

Exemplo 2.6: Seja K = Q($\sqrt{-1}$) = Q(α). Pelo Teorema 1.2 temos que o anel dos inteiros de K é OK = Z[$\sqrt{-1}$]. Para P = <3>, temos que x^2 + 1 = m_|Q(x) é irredutível módulo 3Z[x]. Assim, pelo Corolário 2.1, temos que <3> é totalmente inerte, ou seja, 3OK = Q, onde Q é um ideal primo de OK, com e(Q|P) = 1, e pelo Teorema Kummer, temos que f(Q|P) = 2.

Se P =<5>, temos que x^2 + 1 = m α |Q(x) = (x + 2)(x + 3) módulo 5Z[x]. Assim, pelo Corolário 2.1, temos que <5> é totalmente decomposto, ou seja, 5OK = Q1Q2, onde
Q1 = <5, α + 2>, Q2 = <5, α + 3> são ideais primos de OL com e(Q1|P)e(Q2|P) = 1 e f(Q1|P)f(Q2|P) = 1.

Exemplo 2.6: Seja K = Q($\sqrt{10}$). Pelo Teorema 1.2, temos que o anel dos inteiros de Q($\sqrt{10}$) é OK = Z ($\sqrt{10}$). Para P = <2>, temos que x^2 − 10 = m$\sqrt{10}$|Q(x) = x^2 módulo 2Z[x]. Então <2>OL =P^2, onde P = <2, 10>. Assim, e(P|<2>) = 2. Portanto, P = <2> é totalmente ramificado em Q($\sqrt{10}$). Para P = <3> um ideal primo de Z temos que x^2 − 10 = m $\sqrt{10}$|Q(x) = (x + 1)(x − 1) módulo 3Z[x], e então <3>OL = <3, 1 +$\sqrt{10}$ > <3, 1 −$\sqrt{10}$ > = PP' . Assim, e(P|<3>) = e(P'|<3>) = 1 e f(P|<3>) = f(P'|<3>) = 1. Portanto, P = <3> é totalmente decomposto em Q($\sqrt{10}$).

OLIVEIRA, Ciléia Mazzei de. A relação da ramificação com os conceitos de discriminante. **Economia & Pesquisa**, Araçatuba, v.12, n.12, p. 102 - 115, nov. 2010.

Referências

BAYER, E. F. Lattices and number fields. **Contemporary Mathematics**, v.241, 1999.

BAYER, E. F.; OGGIER, F.; Viterbo, E. New algebraic constructions of rotated Znlattice. Constellations for the rayleigh fading channel. **IEEE Trans. Inform. Theory,** v. 50, n. 4, April 2004.

BOUTROS, J.; Viterbo, E.; Rastello, C.; Belfiori, J. C. Good lattice constellations forboth rayleigh fading and gaussian channels. **IEEE Trans. Inform. Theory**, v. 42, n.2, p. 502-517, March 1996.

CONWAY, J. H.; SLOANE, N. J. A. **Sphere packing, lattices and groups**. Springer-Verlag,1988.

CRAIG, M. A cyclotomic construction of Leech's lattice. **Mathematika**, v.25, p. 236-241, 1978.

CRAIG, M. Extreme forms and cyclotomy. **Mathematika**, v. 25, p. 44-56, 1978.

DAMEN, M.O.; TEWFIK, A.; BELFIORE, J. C. A constructions of a space-time code based on number theory. **IEEE Trans. Inform. Theory**, v. 49, n.5, p. 1037-1113, May 2003.
ENDLER, O. **Teoria dos números algébricos**. Rio de Janeiro, IMPA, 1986.

FORNEY JR.; G. D. Part I: Introduction and geometrical classification. **IEEE Trans. Inform. Theory**, v. l, 34, n. 5, September 1988.

MOLLIN, R. A. **Algebraic number theory.** Canada: University of Calgary, 2003.

RIBEIRO, A. C. **Reticulados sobre corpos de números.** 2003. 84 f. Dissertação (Mestrado em Matemática) - Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, 2003.

RIBENBOIM, P. **Algebraic numbers**. Wiley - Interscience, 1972.

RODRIGUES, T. M. Cúbicas galoisianas. 2003. 80 f. Dissertação (Mestrado em Matemática) - Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, 2003.

SAMUEL, P. **Algebraic theory of numbers**. Paris, Hermana 1967.

SIMONATO, A. L. Reticulados em corpos ciclotômicos. 2000. 82 f. Dissertação (Mestrado em Matemática) - Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, 2000.

STEWART, I.; TALL, D. **Algebric number theory**. Chapman & New York: Hall, 1987.

VITERBO, E. **Algebraic number theory and its application to code design for Rayleigh fading channels.** Notas, August 2004.