FATORAÇÃO NO ANEL DE INTEIROS DE UM CORPO DE NÚMEROS ALGÉBRICOS

Simone Batista

DISSERTAÇÃO DEFENDIDA
NO
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
DA
UNIVERSIDADE DE SÃO PAULO
PARA
OBTENÇÃO DO GRAU DE MESTRE
EM
MATEMÁTICA

Área de Concentração: **Álgebra.**
Orientador: **Prof. Dr. Daniel Levcovitz.**

- São Paulo, fevereiro de 1995 -

FATORAÇÃO NO ANEL DE INTEIROS DE UM CORPO DE NÚMEROS ALGÉBRICOS

Este exemplar corresponde à redação final
da dissertação devidamente corrigida e
defendida por Simone Batista
e aprovada pela comissão julgadora.

São Paulo, 15 de fevereiro 1995.

Banca examinadora:

- Prof. Dr. Daniel Levcovitz (Orientador) - IME - USP
- Prof. Dr. Ricardo Bianconi - IME - USP
- Prof. Dr. Trajano Nóbrega - UNESP

Resumo

Seja K um corpo de números algébrico, $\mathcal{O}_K$ seu anel de inteiros, $\mathcal{H}_K$ o grupo de classes e h_K sua ordem. é conhecido que $h_K = 1$ se, e somente se, $\mathcal{O}_K$ é fatorial. Nesta dissertação nos estudamos a relação entre a estrutura do grupo abeliano finito $\mathcal{H}_K$ (e sua ordem h_K) e as propriedades aritméticas do anel de inteiros $\mathcal{O}_K$, concentrando nossa atenção na fatoração neste anel. O resultado principal (Teorema 3.9 , página 22) caracteriza os anéis $\mathcal{O}_K$ nos quais $\mathcal{H}_K$ é cíclico com ordem potência de um número primo.

Abstract

Let K be a Number field, $\mathcal{O}_K$ its ring of integers, $\mathcal{H}_K$ the class Group and h_K its order. We know that $h_K = 1$ if, and only if, $\mathcal{O}_K$ is factorial. In this dissertation we study the relathionship of h_K and the structure of the finite abelian group $\mathcal{H}_K$ and the arithmetical properties of the ring $\mathcal{O}_K$, concerning the factorization in it. The main result (Theorem 3.9. page 22) caracterizes the ring $\mathcal{O}_K$ for which $\mathcal{H}_K$ is cyclic with order a prime power.

À minha mãe
Neyde

Mini Dicionário:

- **Cafajeste:** Indivíduo infame, desprezível; biltre, canalha.

"Deus proteja meus amigos,

porque dos meus inimigos,

cuido eu."

Agradecimentos:

• Todos meus Professores e em particular ao Prof. Dr. Daciberg Lima Gonçalves, pelo incentivo.

• Funcionários da biblioteca e em particular a Marina, pelo carinho, a compreensão e pelos excelentes serviços prestados

• Minha família, pela dedicação em todos os momentos.

• Colegas do IME–USP, pelas dicas na digitação TEX e na elaboração do texto.

Índice:

Introdução

Nesta dissertação investigamos alguns aspectos da fatoração no anel de inteiros $\mathcal{O}_K$ de corpos de números algébricos K. Para isto, utilizaremos com freqüência dois resultados de teoria dos números. O primeiro é a fatoração única em ideais primos dos ideais de um domínio de Dedekind. O segundo é o que diz que cada classe do grupo de classes $\mathcal{H}_K$ de um corpo de números contém, pelo menos, um ideal primo. No primeiro capítulo apresentamos estes resultados, sem demonstrá-los, e aproveitamos para fixar a notação que será utilizada neste trabalho. Uma referência que traz uma abordagem mais abrangente e inclui as demostrações deste capítulo é [12].

Cabe observar que a maioria das conclusões a que chegaremos nesta dissertação pode ser estendida a domínios de Dedekind que tenham a propriedade de que cada classe de seu grupo de classes contém um ideal primo. Existem domínios de Dedekind que não satisfazem esta propriedade; temos um exemplo dado por Claborn em [6] de domínio de Dedekind com grupo de classes cíclico, de ordem $n \neq 1$, no qual todos os ideais primos estão concentrados em uma única classe.

No segundo capítulo apresentamos a primeira caracterização aritmética do anel de inteiros $\mathcal{O}_K$ com grupo de classes $\mathcal{H}_K$ não trivial. Esta caracterização, devida a Carlitz [3], nos assegura que o grupo de classes $\mathcal{H}_K$ tem ordem h_K menor ou igual a dois se, e somente se, quaisquer duas fatorações de um elemento de $\mathcal{O}_K$ em elementos irredutíveis

têm o mesmo número de fatores, ou seja, têm o mesmo comprimento. Somando-se esta caracterização ao resultado clássico, que diz que um corpo de números tem $\mathcal{H}_K$ trivial se, e somente se, seu anel de inteiros $\mathcal{O}_K$ tem fatoração única, obtemos a caracterização aritmética dos corpos de números com grupo de classes de ordem igual a dois.

No capítulo seguinte vamos expor os resultados obtidos por Krause [11], que estuda corpos de números cujo grupo de classes $\mathcal{H}_K$ é cíclico com ordem h_K potência de um primo. Utilizamos o conceito de elemento primário, um resultado combinatório envolvendo a ordem dos elementos de $\mathcal{H}_K$ e, como Carlitz, recorremos à unicidade de fatoração dos ideais de $\mathcal{O}_K$ em ideais primos. A caracterização obtida por Krause generaliza o resultado de Carlitz.

No quarto e último capítulo temos os resultados obtidos por Czogala, que caracteriza corpos de números que têm grupo de classe com ordem menor ou igual a quatro e também corpos que têm grupo de classes de ordem oito, quando este é isomorfo a soma direta de grupos cíclicos de ordem prima. Este trabalho caracteriza a fatoração em $\mathcal{O}_K$ através de duas propriedades: uma que limita o comprimento das possíveis fatorações de um elemento que tem, pelo menos, uma fatoração de comprimento dois; outra que determina que o quadrado de elementos irredutíveis têm todas as possíveis fatorações de comprimento dois. Usamos para isto, essencialmente, a técnica de Carlitz e propriedades aritméticas bastante específicas dos grupos de classes destes corpos.

Para finalizar observamos que o assunto abordado por esta dissertação, bem como, a generalização dos resultados apresentados continuam sendo estudados por diversos matemáticos. Podemos citar por exemplo: em [10] e [19] encontramos outras caracte-

rizações da fatoração no anel de inteiros $\mathcal{O}_K$ de corpos de números K, com grupo de classes $\mathcal{H}_K$ conhecidos; algumas desigualdades sobre o número de Cross de grupos abelianos finitos são estabelecidas em [9]; temos o interessante trabalho [4] que avalia o comprimento de fatorações no anel de inteiros de corpos de números através da constante de Davenport; e ainda [5], [21] e [22] onde são estudadas as propriedades aritméticas das fatorações em domínios que não são, em geral, anéis de inteiros de corpos de números.

Capítulo 1

Conceitos Gerais.

Neste capítulo, com o intuito de fixar a notação, apresentaremos alguns conceitos gerais que serão utilizados nos capítulos posteriores. Daremos ênfase aos aspectos que serão necessários neste trabalho.

Seja L uma extensão finita do corpo K. A dimensão de $L|K$ será denotada por n. Supondo $\alpha_1, \ldots \alpha_n$ uma base de $L|K$, se $\alpha \in L$ temos :

$$\alpha\alpha_i = \sum_{j=1}^{n} a_{ij}\alpha_j \quad \text{com} \quad a_{ij} \in K, \quad N(\alpha) := det(a_{ij}) \quad \text{e} \quad T(\alpha) := \sum_{i=1}^{n} a_{ii}$$

onde $N(\alpha)$ e $T(\alpha)$ são respectivamente a norma e o traço de α.

Verifica-se que a norma e o traço de um elemento independem da escolha da base e que :

$$N(\alpha\beta) = N(\alpha)N(\beta), \quad N(a\beta) = a^n N(\beta), \quad T(\alpha+\beta) = T(\alpha)+T(\beta), \quad \text{e} \quad T(a\beta) = aT(\beta).$$

onde $\alpha, \beta \in L$ e $a \in K$.

Se $L|K$ é separável e se $\sigma_1 \ldots \sigma_n$ são os K-isomorfismos distintos de L em um fecho algébrico fixado de K , então vale:

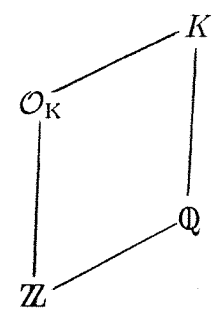
$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \quad \text{e} \quad T(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

Para $(\alpha_1, \ldots, \alpha_n)$ uma $n-$upla de elementos de L, definimos o discriminante de $(\alpha_1, \ldots, \alpha_n)$ por :

$$\Delta(\alpha_1, \ldots, \alpha_n) = det(T(\alpha_i \alpha_j)).$$

Um subcorpo K de $\mathbb{C}$ é chamado corpo de números algébricos, se K é uma extensão finita do corpo dos números racionais $\mathbb{Q}$ ou, equivalentemente, se $K = \mathbb{Q}(\alpha)$ com α um número algébrico.

Todo corpo de números algébricos K tem um anel distinguido $\mathcal{O}_K$ que é chamado anel de inteiros de K e é constituido pelos elementos de K que são inteiros sobre $\mathbb{Z}$. Ou seja, $\mathcal{O}_K$ é o conjunto dos $\alpha \in K$ tais que $F(\alpha) = 0$ com F polinômio mônico de $\mathbb{Z}[x]$.



Estamos interessados na fatoração em $\mathcal{O}_K$.

Um elemento $u \in \mathcal{O}_K$ é uma unidade se existe $v \in \mathcal{O}_K$ tal que $uv = 1$. Dois elementos a, b de $\mathcal{O}_K$ são associados se existe uma unidade $u \in \mathcal{O}_K$ tal que $a = ub$. Dizemos que $a \in \mathcal{O}_K$ é irredutível se não pode ser fatorado em $\mathcal{O}_K$, ou seja se $a = bc$ com $b, c \in \mathcal{O}_K$ então a ou c é unidade de $\mathcal{O}_K$.

Seja $a = a_1 \ldots . a_r$ uma fatoração de $a \in \mathcal{O}_K$ em elementos irredutíveis; r é chamado comprimento desta fatoração. Diremos que $\mathcal{O}_K$ tem fatoração única quando para todo $a \in \mathcal{O}_K$, a se escreve de maneira única, a menos de ordem, como $a = ua_1 \ldots . a_r$ com u unidade em $\mathcal{O}_K$ e $a_i \in \mathcal{O}_K$ irredutíveis.

Como veremos, em geral, não existe unicidade de fatoração em $\mathcal{O}_K$, ou seja, existem corpos cujos anéis de inteiros contêm elementos que podem ser fatorados de mais de uma maneira, inclusive com fatorações de comprimentos distintos.

Uma forma de contornar este problema, desenvolvida por Kummer e Dedekind, foi estudar a fatoração dos ideais de $\mathcal{O}_K$. A seguir,daremos um breve relato de como isto pode ser feito, pois os resultados obtidos serão uma ferramenta importante nos próximos capítulos.

Sabemos que $\mathcal{O}_K$ é anel Noetheriano, isto é, toda cadeia ascendente de ideais $I_1 \subset I_2 \subset \ldots$ é estacionária ou, em outras palavras, existe $N > 0$, tal que $I_m = I_{m+1}$ para todo $m > N$. Temos também que todo ideal primo, não nulo, de $\mathcal{O}_K$ é maximal, e que $\mathcal{O}_K$ é integralmente fechado, ou seja, se $\alpha \in K$ satisfaz um polinômio mônico com coeficientes em $\mathcal{O}_K$ então $\alpha \in \mathcal{O}_K$.

Um domínio de Dedekind é um domínio Noetheriano, integralmente fechado onde todo ideal primo, não nulo, é maximal. Pelas considerações anteriores, o anel $\mathcal{O}_K$ é um domínio de Dedekind.

Vamos estudar a fatoração de ideais em ideais primos nos domínios de Dedekind. Salvo menção explicita em contrário, todos os ideais considerados serão ideais não nulos.

Sejam D um domínio, K seu corpo de frações e vamos considerar os submódulos do D-módulo K com as operações de intersecção, soma e produto.

Um submódulo M de K será chamado um ideal fracionário de D se existir $d \in D|\{0\}$ tal que $dM \subseteq D$. Neste caso, dM é um ideal J de D e $M = d^{-1}J$. Os ideais de D

são exatamente os ideais fracionários que estão contidos em D.

É claro que todo submódulo finitamente gerado de K é um ideal fracionário e que, por outro lado num domínio noetheriano todo ideal fracionário é finitamente gerado. Verifica-se facilmente que a intersecção, a soma e o produto de dois ideais fracionários é um ideal fracionário

Um submódulo M de D é invertível se existir um submódulo N de D tal que $NM = D$. Neste caso, o inverso é univocamente determinado e será denotado por M^{-1}.

Denotaremos por $\mathcal{F}$ o conjunto dos ideais fracionários , por $\mathcal{G}$ os ideais , $\mathcal{P}_p$ os ideais principais e ainda por $\mathcal{P}$ os ideais primos de D.

Os submódulos invertíveis de K são necessariamente ideais fracionários, porém observemos ainda que o inverso de um ideal I não é, em geral, um ideal mas apenas um ideal fracionário.

Teorema 1.1 *Seja D um Domínio. São equivalentes:*

a) D é um domínio de Dedekind.

b) O conjunto $\mathcal{F}$ é um grupo, ou seja todo ideal fracionário de D é invertível.

c) Para todo ideal I de D existem ideais primos $P_1, \ldots, P_k$ em D tais que:

$$I = P_1 \ldots P_k.$$

e os ideais primos da fatoração acima são univocamente determinados (a menos de ordem).

Em D o conjunto dos ideais fracionários principais $\mathcal{P}_p$ formam um subgrupo do grupo $\mathcal{F}$. Chamamos o grupo quociente $\mathcal{H}_D = \mathcal{F}|\mathcal{P}_p$ de grupo de classes de ideais de D e sua ordem, que é denotada por h_K, de número de classes.

No caso do anel $\mathcal{O}_K$ de um corpo de números K, denotamos a ordem do grupo de classes por h_K ao invés de $h_{\mathcal{O}_K}$, e neste caso é verdade que h_K é finito. Assim para todo ideal A de $\mathcal{O}_K$, A^{h_K} é ideal principal.

Outro fato importante do grupo de classes $\mathcal{H}$, de corpos de números, que não ocorre em domínios de Dedekind em geral, é que todas classes possuem ideais primos. A demonstração deste fato é mais elaborada e utiliza métodos analíticos. Ela baseia-se no comportamento das L-séries:

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \quad Re(s) > 1.$$

onde χ é um caracter de Dirichlet e $Re(s)$ é a parte real de s.

Esta função também é útil na determinação do números de classes h_K de $\mathcal{H}$.

Para um estudo dos métodos analíticos e a demostração das propriedades dos corpos de números citadas acima podemos consultar [12] da bibliografia.

Capítulo 2

Carlitz e a Primeira Caracterização.

Iniciamos este capítulo com algumas considerações sobre certos subconjuntos de um grupo abeliano finito que denotaremos por G.

Definição 2.1 Um *sistema*, $S = \langle g_1, \ldots, g_n \rangle$, é uma seqüência finita não ordenada de elementos de G. Dado $g \in G$ e um sistema $S = \langle g_1, \ldots, g_n \rangle$ de G chamaremos de *grau de g no sistema S*, que indicaremos por $(g)_S$, o número de vezes que g aparece no sistema S. Adotaremos grau zero, $(g)_S = 0$, para os elementos de G que não aparecem no sistema. Um sistema S_1 será chamado de *sub-sistema* do sistema S se, para cada elemento $g \in G$, a ordem de g em S_1 for menor ou igual à ordem de g em S. Usaremos a notação: $S_1 \leq S$. Um sub-sistema S_1 será chamado *sub-sistema próprio* de S se existir um elemento $g \in G$, tal que sua ordem em S_1 seja estritamente menor que sua ordem em S, neste caso usaremos a notação: $S_1 < S$. Dado um sistema $S = \langle g_1, \ldots, g_n \rangle$ em G, n será chamado de *comprimento do sistema* S.

Definição 2.2 Um sistema S será chamado de *bloco* se o produto de todos seus elementos for unitário, isto é, $g_1 \cdots g_n = 1$. Para um bloco $B = \langle g_1, \ldots, g_n \rangle$ podemos falar em *sub-bloco, sub-bloco próprio, comprimento do bloco e grau de g no bloco B*, lembrando apenas que todo bloco é um sistema.

O comprimento de um sistema é igual a soma dos graus de seus elementos, ou seja, $n = \sum_{g \in G}(g)_S$. Denotaremos por $B(G)$ ao conjunto de todos blocos de G. Note que o conjunto dos blocos $B(G)$ tem estrutura natural de semi-grupo com a operação de justaposição.

Definição 2.3 Um bloco será chamado de *bloco minimal* se não puder ser escrito como produto de dois sub-blocos. Denotaremos por $M(B)$ o conjunto de todos blocos minimais de $B(G)$.

Um bloco é minimal se, e somente se, não admite sub-blocos próprios. Temos também que o elemento $g \in G$ tem ordem m se, e somente se, o bloco $B = \langle \underbrace{g, \ldots, g}_{m-\text{vezes}} \rangle$ é minimal.

Exemplo 2.4 No grupo $(\mathbb{Z}_6, +)$ temos:

$B_1 = \langle \overline{1}, \overline{1}, \overline{1}, \overline{1}, \overline{1}, \overline{2}, \overline{2}, \overline{3} \rangle$ é bloco pois: $\overline{1} + \overline{1} + \overline{1} + \overline{1} + \overline{1} + \overline{2} + \overline{2} + \overline{3} = \overline{0}$ e

B_1 não é minimal pois $B_1 = \langle \overline{1}, \overline{1}, \overline{1}, \overline{1}, \overline{1}, \overline{2}, \overline{2}, \overline{3} \rangle = \langle \overline{1}, \overline{1}, \overline{2}, \overline{2} \rangle \langle \overline{1}, \overline{1}, \overline{1}, \overline{3} \rangle$.

$B_2 = \langle \overline{1}, \overline{1}, \overline{1}, \overline{1}, \overline{1}, \overline{1} \rangle$ é bloco minimal, já que: $\text{ord}\,(\overline{1}) = 6$ em $(\mathbb{Z}_6, +)$.

A seguir relacionamos o conceito de elemento irredutível em um domínio de Dedekind e de bloco minimal no grupo de classes deste domínio.

Proposição 2.5 *Sejam D um domínio de Dedekind, $\mathcal{H}_D$ seu grupo de classes e $P_1, \ldots, P_n$ ideais primos em D. O bloco $B = \langle \overline{P}_1, \ldots, \overline{P}_n \rangle$ é minimal no grupo de classes $\mathcal{H}_D$ se, e somente se, existe um elemento $a \in D$, irredutível e não unidade, tal que $(a) = P_1 \cdots P_n$.*

Demonstração: Suponhamos que $B = \langle \overline{P}_1, \ldots, \overline{P}_n \rangle$ é bloco minimal em $\mathcal{H}_D$. Então $\overline{P}_1 \cdots \overline{P}_n = \overline{1}$ em $\mathcal{H}_D$, ou seja, o ideal $P_1 \ldots P_n$ é principal. Assim, existe $a \in D$, não unidade, tal que $(a) = P_1 \cdots P_n$.

Falta mostrar que a é irredutível. Para isto, sejam b e $c \in D$, tal que $a = bc$, então $b \backslash a$. Como $(a) = P_1 \cdots P_n$ temos que $(b) = P_{1_1} \cdots P_{1_m}$ com $B_1 = \langle \overline{P}_{1_1}, \ldots, \overline{P}_{1_m} \rangle$ sub-bloco de B. Mas B é minimal, assim $B_1 = B$. Portanto $(a) = P_1 \cdots P_n = P_{1_1} \cdots P_{1_m} = (b)$ Ou seja c é unidade e a é irredutível.

Reciprocamente, seja a irredutível e $(a) = P_1 \cdots P_n$. Temos: $\overline{1} = \overline{(a)} = \overline{P}_1 \cdots \overline{P}_n$ em $\mathcal{H}_D$, e portanto $B = \langle \overline{P}_1, \ldots, \overline{P}_n \rangle$ é bloco. Tomemos $B_1 = \langle \overline{P}_{1_1}, \ldots, \overline{P}_{1_m} \rangle$ sub-bloco de B. Como $\overline{P}_{1_1} \cdots \overline{P}_{1_m} = \overline{1}$, existe b (não unidade) com $(b) = P_{1_1} \cdots P_{1_m}$. Assim $b \backslash a$. Portanto, existe $c \in D$ tal que $a = bc$. Como a é irredutível, c é unidade, e $P_{1_1} \cdots P_{1_m} = (b) = (a) = P_1 \cdots P_n$ e pela unicidade de fatoração de um ideal em ideais primos, $\langle \overline{P}_{1_1}, \ldots, \overline{P}_{1_m} \rangle = \langle \overline{P}_1, \ldots, \overline{P}_n \rangle$, ou seja, B é minimal. ∎

Agora mostraremos o Teorema de Carlitz, que caracteriza os corpos de números algébricos K que têm o grupo de classes $\mathcal{H}_K$ com ordem igual a dois, como sendo os corpos que, apesar de não terem unicidade de fatoração em elementos irredutíveis nos seus anéis de inteiros, têm unicidade no comprimento de tais fatorações.

Teorema 2.6 (Teorema de Carlitz) *Seja K um corpo de números, $\mathcal{O}_K$ seu anel de inteiros e h_K a ordem do grupo de classes $\mathcal{H}_K$. Então $h_K \leq 2$ se, e somente se, todas as fatorações de qualquer elemento $a \in \mathcal{O}_K$ têm o mesmo comprimento.*

Demonstração: Como $h_K = 1$ se, e somente se, $\mathcal{O}_K$ é um domínio fatorial, o teorema é válido neste caso. Suponhamos $h_K = 2$. Seja $a = a_1 \cdots a_n$ uma fatoração em irredutíveis de a . Em termos de ideais temos:

$$(a) = (a_1) \cdots (a_n) \ . \tag{1}$$

Reordenando (1) de forma que os primeiros ideais da fatoração sejam os ideais primos que eventualmente apareçam nesta fatoração (digamos que apareçam s deles), temos:

$$(a) = \underbrace{(a_1)\cdots(a_s)}_{\text{ideais primos}}(a_{s_{+1}})\cdots(a_n) \tag{2}$$

onde (a_i) é não primo para i maior que s. Fatorando (a_i) em ideais primos obtemos: $(a_i) = P_{i_1}\cdots P_{i_m}$. Pela Proposição 2.5, $B = \langle \overline{P}_{i_1}, \ldots, \overline{P}_{i_m}\rangle$ é bloco minimal. Logo $\overline{(P_{i_j})} \neq \overline{1}$, $j = 1, \ldots m$. Como $h_K = 2$ devemos ter $\overline{P}_{i_1} = \overline{P}_{i_2} = \cdots = \overline{P}_{i_m}$ e ord $\left(\overline{(P_{i_1})}\right) = 2$. Assim $\overline{1} = (\overline{P}_{i_1})^2 = (\overline{P}_{i_1})(\overline{P}_{i_2})$ e portanto $m = 2$ e $(a_i) = P_{i_1}P_{i_2}$. Substituindo em (2) obtemos:

$$(a) = \overbrace{\underbrace{(a_1)\cdots(a_s)}_{\text{principais}}\underbrace{P_{s+1_1}P_{s+1_2}\cdots P_{n_1}P_{n_2}}_{\text{não principais}}}^{\text{ideais primos}} . \tag{3}$$

Em (3) temos o ideal (a) fatorado em ideais primos. Como esta fatoração em $\mathcal{O}_K$ é única, determinamos s e t; s é o número de ideais primos principais e $t = 2(n-s)$ é o número de ideais primos não principais. Logo $n = s + \frac{t}{2}$ independe da fatoração.

Reciprocamente vamos mostrar que para $h_K > 2$ existem fatorações com comprimentos distintos. Vamos dividir a prova em dois casos:

1º Caso: Existe pelo menos uma classe, que chamaremos de $\overline{A}$, em $\mathcal{H}_K$ com ordem maior que 2.

Digamos ord $(\overline{A}) = m$, $m > 2$ logo $\overline{A} \neq \overline{A}^{-1}$. Sejam P_1 e P_2 ideais primos de $\mathcal{O}_K$ com $P_1 \in \overline{A}$ e $P_2 \in \overline{A}^{-1}$. Como ord $(\overline{P}_1) =$ ord $(\overline{A}) = m =$ ord $(\overline{A}^{-1}) =$ ord $(\overline{P}_2)$, os blocos $B_1 = \langle \underbrace{\overline{P}_1, \ldots, \overline{P}_1}_{m-\text{vezes}}\rangle$ e $B_2 = \langle \underbrace{\overline{P}_2, \ldots, \overline{P}_2}_{m-\text{vezes}}\rangle$ são minimais. Sabemos que $\overline{P}_1\overline{P}_2 = \overline{A}\overline{A}^{-1} = \overline{1}$, $\overline{P}_1 \neq 1$, $\overline{P}_2 \neq 1$ e portanto o bloco $B_3 = \langle \overline{P}_1, \overline{P}_2\rangle$ é minimal. Assim existem a_1, a_2, a_3 irredutíveis tais que $(P_1)^m = (a_1)$, $(P_2)^m = (a_2)$, $P_1P_2 = (a_3)$. Como $(P_1P_2)^m = P_1^m P_2^m$

temos que $(a_3)^m = (a_1)(a_2)$. Assim, a menos de unidade temos $b = a_1a_2 = a_3^m$ (com $m \geq 3$). Logo b admite duas fatorações com comprimentos distintos.

2º Caso: Todas as classes de $\mathcal{H}_K$ têm ordem menor ou igual a 2.

Como $h_K > 2$ existem pelo menos duas classes distintas com ordem 2 em $\mathcal{H}_K$, digamos, $\overline{A}$ e $\overline{B}$. Temos $\overline{AB} \neq \overline{1}$, pois se $\overline{AB} = \overline{1}$ então $(\overline{A})^2\overline{B} = \overline{A}$ e portanto $\overline{B} = \overline{A}$. Sejam P_1, P_2, P_3 ideais primos em $\mathcal{O}_K$ com $P_1 \in \overline{A}$, $P_2 \in \overline{B}$ e $P_3 \in \overline{AB}$. Observamos que: $\text{ord}(\overline{A}) = \text{ord}(\overline{B}) = \text{ord}(\overline{AB}) = 2$. Portanto, os blocos $B_1 = \langle \overline{P}_1, \overline{P}_1 \rangle = \langle \overline{A}, \overline{A} \rangle$, $B_2 = \langle \overline{P}_2, \overline{P}_2 \rangle = \langle \overline{A}^{-1}, \overline{A}^{-1} \rangle$ e $B_3 = \langle \overline{P}_3, \overline{P}_3 \rangle = \langle \overline{AB}, \overline{AB} \rangle$ são minimais. Como $P_3 \in \overline{AB}$ e $P_1P_2 \in \overline{A}\,\overline{B}$, o bloco $B_4 = \langle \overline{P}_3, \overline{P}_1\overline{P}_2 \rangle = \langle \overline{AB}, \overline{AB} \rangle$ é minimal. Portanto existem a_1, a_2, a_3 e a_4 irredutíveis de $\mathcal{O}_K$ tais que $(a_1) = P_1P_1$, $(a_2) = P_2P_2$, $(a_3) = P_3P_3$ e $(a_4) = P_3P_1P_2$. Como $(P_1P_2P_3)^2 = P_1^2P_2^2P_3^2$, temos, $(a_4)^2 = (a_1)(a_2)(a_3)$. Assim, a menos de unidade temos $b = a_4^2 = a_1a_2a_3$. Logo b admite duas fatorações com comprimentos distintos. ∎

A seguir ilustramos o resultado anterior através de alguns exemplos.

Exemplos 2.7

2.7.1

Vamos observar o anel de inteiros $\mathbb{Z}(\sqrt{-5})$ do corpo $\mathbb{Q}(\sqrt{-5})$, onde podemos fatorar o número 6 de duas maneiras:

$$6 = 2.3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \tag{1}$$

Calculando a norma obtemos: $N(2) = 4$, $N(3) = 9$ e $N(1 + \sqrt{-5}) = 6$. O que nos mostra que eles são irredutíveis, pois um divisor próprio, não unidade de qualquer um

destes elementos deveria ter norma 2 ou 3, o que é impossível já que:

$$N(a + b\sqrt{-5}) = a^2 + 5b^2 \geq 5.$$

Assim, (1) nos dá duas fatorações em irredutíveis distintas e de mesmo comprimento.

2.7.2

Agora vamos observar o anel de inteiros $\mathbb{Z}\left(\frac{1}{2} + \frac{1}{2}\sqrt{-15}\right)$ do corpo $\mathbb{Q}(\sqrt{-15})$. Aqui podemos fatorar o número 4 de duas maneiras:

$$4 = 2.2 = \left(\frac{1}{2} + \frac{1}{2}\sqrt{-15}\right)\left(\frac{1}{2} - \frac{1}{2}\sqrt{-15}\right) \tag{2}$$

E, de forma análoga ao exemplo anterior, podemos concluir que (2) nos dá duas fatorações distintas em irredutíveis de mesmo comprimento.

Como nos dois exemplos acima temos $h_K = 2$, já poderíamos esperar que existissem elementos com fatorações distintas e de mesmo comprimento. A seguir apresentamos dois anéis onde ocorrem fatorações distintas de um elemento com comprimentos distintos.

2.7.3

Observemos o número 18 no anel de inteiros $\mathbb{Z}(\sqrt{-17})$ do corpo $\mathbb{Q}(\sqrt{-17})$:

$$18 = 2.3.3 = (1 + \sqrt{-17})(1 - \sqrt{-17}) \tag{3}$$

Novamente através do cálculo da norma dos elementos 2, 3 e $(1 \pm \sqrt{-17})$ concluimos que são irredutíveis. Assim, (3) nos dá duas fatorações em irredutíveis distintas de comprimentos distintos. Nesse caso $h_K = 4$.

2.7.4

Terminamos observando o anel $\mathbb{Z}\left(\frac{1}{2}+\frac{1}{2}\sqrt{-23}\right)$ do corpo $\mathbb{Q}(\sqrt{-23})$. Neste anel podemos fatorar o número 8 em elementos irredutíveis de duas maneiras:

$$8 = 2.2.2 = \left(\frac{3}{2}+\frac{1}{2}\sqrt{-23}\right)\left(\frac{3}{2}-\frac{1}{2}\sqrt{-23}\right) \tag{4}$$

Assim, (4) nos dá duas fatorações em irredutíveis de comprimentos distintos.

Ainda neste anel temos duas únicas fatorações do número 6 em elementos irredutíveis:

$$6 = 2.3 = \left(\frac{1}{2}+\frac{1}{2}\sqrt{-23}\right)\left(\frac{1}{2}-\frac{1}{2}\sqrt{-23}\right) \tag{5}$$

Neste caso $h_K = 3$ e (5) nos dá duas fatorações em irredutíveis distintas e de mesmo comprimento.

Ou seja, se um corpo K tem $h_K \geq 2$ isto significa que temos fatorações distintas de um mesmo elemento com comprimentos distintos em $\mathcal{O}_K$, mas não que todos elementos terão fatorações distintas com comprimentos distintos nem mesmo que todos elementos terão fatorações distintas.

Capítulo 3

Irredutíveis, Primos, Primários e o Teorema de Krause.

Em $\mathbb{Z}$ um número primo p tem duas propriedades básicas:

(1) $m|p \Rightarrow m = \pm p$ ou m é unidade

(2) $p|m.n \Rightarrow p|m$ ou $p|n$.

Podemos usar qualquer das duas propriedades como definição de número primo em $\mathbb{Z}$ pois uma decorre da outra. Em um domínio de Dedekind arbitrário, e em especial em anéis de inteiros, a propriedade (2), que é requerida para unicidade da fatoração, em geral, não decorre de (1).

A propriedade (1) é simplesmente a definição de número irredutível em D. A definição de número primo em D vem da propriedade (2) para um número p não nulo e não unidade. É fácil ver que um elemento primo é sempre irredutível, mas podemos ter elementos irredutíveis que não são primos como veremos no exemplo abaixo.

Exemplo 3.1 Em $\mathbb{Z}(\sqrt{-5})$, $6 = 2.3 = (1+\sqrt{-5})(1-\sqrt{-5})$ com 2, 3, $(1+\sqrt{-5})$ irredutíveis. Portanto 2 divide $(1+\sqrt{-5})(1-\sqrt{-5})$ e não divide $(1+\sqrt{-5})$ nem $(1-\sqrt{-5})$ pois: $N(2) = 4$ não divide $6 = N(1 \pm \sqrt{-5})$. Ou seja, 2 é irredutível e não é primo.

A seguir damos outra noção que se mostrou útil na fatoração em irredutíveis que é a de inteiro primário.

Definição 3.2 *Seja x um elemento irredutível, não nulo e não unidade, de um domínio D. Dizemos que x é primário se dados y e $z \in D$ temos:*

$$x|y.z \Rightarrow x|y \text{ ou } x|z^m \text{ , para algum } m \text{ natural.}$$

Voltando ao Exemplo 2.1 em $\mathbb{Z}(\sqrt{-5})$, $2|(1+\sqrt{-5})(1-\sqrt{-5})$ e $2\not|(1 \pm \sqrt{-5})$. Mas, $2|(1+\sqrt{-5})^2$ pois $(1+\sqrt{-5})^2 = (-4+2\sqrt{-5}) = 2(-2+\sqrt{-5})$. Assim neste anel, 2 não é primo, porém podemos ter 2 primário.

O próximo lema caracteriza números primários em corpos de números, e usaremos este para mostrar que 2 é primário em $\mathbb{Z}(\sqrt{-5})$.

Lema 3.3 *Seja I um ideal de um anel de inteiros $\mathcal{O}_K$, e $n(I)$ a ordem da classe $\overline{I}$ em $\mathcal{H}_K$. Então $x \in \mathcal{O}_K$ é primário se, e somente se, existe um ideal primo P em $\mathcal{O}_K$ tal que $(x) = P^{n(P)}$.*

Demonstração: Supondo que $x \in \mathcal{O}_K$ é primário. Vamos observar a fatoração em ideais primos do ideal gerado por x em $\mathcal{O}_K$, $(x) = P_1 \cdots P_r$. Como $n(P_i)$ divide o número de classes h temos que $m_i = \frac{h}{n(P_i)} \in \mathbb{N}$. Elevando-se x a h obtemos:

$$(x^h) = P_1^h \cdots P_r^h = = (x_1)^{m_1} \cdots (x_r)^{m_r} \text{ , onde } x_i \in \mathcal{O}_K \text{ e } (x_i) = P_i^{n(P_i)}.$$

Portanto $x|x_1^{m_1} \cdots x_r^{m_r}$, e como x é primário segue que $x|x_i^m$ para algum i e $m \in \mathbb{N}$. Mas, $(x_i) = P_i^{n(P_i)}$. Assim $(x) = P_i^k$ com $k \in \mathbb{N}$. Pela definição de $n(P_i)$, temos $k \geq n(P_i)$. Como x é irredutível, $k = n(P_i)$.

Inversamente, suponhamos que $(x) = P^{n(P)}$ para P um ideal primo em $\mathcal{O}_K$. Como $n(P)$ é mínimo, temos que x é irredutível. Sejam y e z em $\mathcal{O}_K$ tais que $x|y.z$ e suponhamos que $x \not| y$. Então a fatoração do ideal (z) contém o fator P^k, para algum $k \geq 1$. Como $n(P)$ divide h, a fatoração do ideal (z^h) contém o fator $P^{n(P).k} = (x)^k$. Assim, $x|z^h$, mostrando que x é primário. ∎

Finalmente, retornando ao Exemplo 2.1, como:

$(2) = (1+\sqrt{-5}, 1-\sqrt{-5})^2$ e $(1+\sqrt{-5}, 1-\sqrt{-5})$ é ideal primo,

podemos concluir que 2 não é primo em $\mathbb{Z}(\sqrt{-5})$, mas é primário.

A seguir vamos estudar outras propriedades interessantes de elementos primários.

Lema 3.4 *Se x é irredutível em um anel de inteiros $\mathcal{O}_K$, então:*

(I) x^{h_K} tem fatoração única, a menos de unidades e ordem dos fatores, em inteiros primários.

(II) Seja $(x) = P_1^{k_1} \cdots P_t^{k_t}$ com P_i ideais primos distintos e seja $m \in \mathbb{N}$ tal que x^m tem fatoração única em elementos primários. Então o número de fatores desta fatoração é deteminado por x e m e é dado por: $n = \left[\sum_{i=1}^{t} \left(\frac{k_i}{n(P_i)}\right) m\right]$.

Demonstração: Seja $(x) = P_1 \cdots P_r$ a fatoração em ideais primos do ideal (x). Sabemos pelo lema anterior que $P_i^{n(P_i)} = (x_i)$, $1 \leq i \leq r$, com x_i primário. Portanto, para $m_i = \frac{h}{n(P_i)}$ temos $x^h = (x_1)^{m_1} \cdots (x_r)^{m_r}$. Assim, x^{h_K} tem fatoração em primários. Seja $m \in \mathbb{N}$ tal que x^m tem fatoração em primários, e seja $x^m = u q_1^{l_1} \cdots q_s^{l_s}$ essa fatoração em primários não associados e u unidade. Pelo lema anterior $(q_i) = Q_i^{n(Q_i)}$ com Q_i ideal primo, para $1 \leq i \leq s$. Como, para $i \neq j$, q_i é não associado a q_j, temos $Q_i \neq Q_j$ se $i \neq j$. Assim,

$$(x)^m = Q_1^{n(Q_1)l_1} \cdots Q_s^{n(Q_s)l_s} . \qquad (1)$$

Por outro lado, olhando a fatoração em ideais primos do ideal gerado por x, temos: $(x) = P_1^{k_1} \cdots P_t^{k_t}$, com $P_i \neq P_j$ se $i \neq j$. Assim,

$$(x)^m = P_1^{k_1 m} \cdots P_t^{k_t m} \ . \tag{2}$$

Pela unicidade da fatoração em ideais primos em domínios de Dedekind, (1) e (2) nos leva a $s = t$ e reordenando os ideais, $Q_i = P_i$ e $n(Q_i)l_i = mk_i$, $1 \leq i \leq s$.

Como o número de fatores primários em x^m é $\sum_{i=1}^{s} l_i$ temos:

$$n = \sum_{i=1}^{s} l_i = \left(\sum_{i=1}^{s} \frac{k_i}{n(Q_i)} \right) m = \sum_{i=1}^{s} \frac{k_i}{n(P_i)} m \ .$$

■

Vamos agora dar a definição de número de Cross de um grupo G abeliano e finito.

Definição 3.5 *Seja G um grupo abeliano finito. O número:*

$$K(G) = \max \left\{ \sum_{i=1}^{r} \frac{1}{\text{ord}\,(g_i)} \ \textit{tal que} \ \langle g_1, \ldots, g_r \rangle \ \textit{é bloco minimal de} \ G \right\}$$

é chamado de número de Cross do grupo G.

Observe que o número de Cross de um grupo é um número racional, maior ou igual a um e menor que a ordem do grupo. (Ver exemplo 3.6.2).

A seguir vamos estudar como se comporta o número de Cross de alguns grupos.

Exemplos 3.6

3.6.1

Consideremos o grupo $\mathbb{Z}_6$. Temos que o bloco $B = \langle 1, 3, 4, 4, \rangle$ é minimal. Para este bloco: $\sum_{b \in B} \frac{1}{\text{ord}\,(b)} = \frac{4}{3} > 1$. Portanto, $K(\mathbb{Z}_6) > 1$. Na verdade, $K(\mathbb{Z}_6) = \frac{4}{3}$.

3.6.2

Seja G um grupo qualquer não trivial e $a \in G$, $a \neq 1$ e $n = ord(a)$, então $(\overbrace{a, \ldots, a}^{n-vezes})$ é bloco minimal, e $\sum_{i=1}^{n} \frac{1}{ord(a)} = \frac{n}{n} = 1$. Assim, para qualquer grupo G temos $K(G) \geq 1$.

Estudaremos agora algumas propriedades do número de Cross de um grupo abeliano finito. Sabemos que todo grupo abeliano finito G é soma direta de grupos cíclicos com ordens potência de primos, $G = C_{n_1} \oplus \cdots \oplus C_{n_s}$ com $s \geq 1$ e $n_i \geq 2$, onde C_{n_i} é grupo cíclico de ordem n_i; n_i potência de um primo.

Lema 3.7 *Com a notação anterior, se G é um grupo abeliano finito então:*

$$K(G) \geq \left(\sum_{i=1}^{s} \frac{n_i - 1}{n_i} \right) + \frac{1}{\text{mmc}\{n_1, \ldots, n_s\}},$$

onde $\text{mmc}\{n_1, \ldots, n_s\}$ *é o mínimo múltiplo comum dos números* $n_1, \ldots, n_s$.

Demonstração: Seja g_i um gerador de C_{n_i}. Podemos escrever $1 = g_1^{n_1 - 1} \cdots g_s^{n_s - 1}.(g_1 \cdots g_s)$ com $\langle \underbrace{g_1, \ldots, g_1}_{(n_1-1)-vezes}, \ldots, \underbrace{g_s, \ldots, g_s}_{(n_s-1)-vezes}, g_1 \cdots g_s \rangle$ bloco minimal. Assim,

$$K(G) \geq \sum_{i=1}^{s} \frac{n_i - 1}{\text{ord}\,(g_i)} + \frac{1}{\text{ord}\,(g_1 \cdots g_s)}.$$

Como $\text{ord}\,(g_i) = n_i$ e $\text{ord}\,(g_1 \cdots g_s) = \text{mmc}\{n_1, \ldots, n_s\}$, temos:

$$K(G) \geq \sum_{i=1}^{s} \frac{n_i - 1}{n_i} + \frac{1}{\text{mmc}\{n_1, \ldots n_s\}}.$$

■

O teorema seguinte caracteriza os grupos com número de Cross igual a 1.

Teorema 3.8 *Um grupo abeliano finito tem número de Cross um se, e somente se, é cíclico e sua ordem é potência de um número primo.*

Demonstração: Seja $G = C_{n_1} \oplus \cdots \oplus C_{n_s}$, com $s \geq 1$ e $n_i \geq 2$. Se $K(G) = 1$, então $1 = K(G) \geq \sum_{i=1}^{s} \frac{n_i - 1}{n_i} + \frac{1}{\text{mmc}\{n_1,\ldots,n_s\}} > \sum_{i=1}^{s} \frac{n_i - 1}{n_i}$ e $1 > \sum_{i=1}^{s} \frac{n_i - 1}{n_i} \geq \frac{s}{2}$. Portanto, $s = 1$.

Reciprocamente, seja $G = C_{p^n}$, onde p é primo e $n \geq 1$. Mostraremos que $\sum_{i=1}^{k} \frac{1}{\text{ord}\,(g_i)} \leq 1$ para qualquer bloco minimal $\langle g_1, \ldots, g_k \rangle$ de G por indução em n e em k.

Para $n = 1$ e $k = 1$, o fato é trivial. Para $k > 1$, seja $\langle g_1, \ldots, g_k \rangle$ um bloco minimal e seja:

$$\begin{aligned} h_1 &= g_2 \cdots g_k \\ h_2 &= g_3 \cdots g_k \\ h_{k-1} &= g_k \ . \end{aligned}$$

Temos $h_i \neq h_j$ se $i \neq j$ e $h_i \neq 1$ para todos $1 \leq j, i \leq k-1$. Então, $k \leq p$ e temos: $\sum_{i=1}^{k} \frac{1}{\text{ord}\,(g_i)} = \frac{k}{p} \leq 1$. Assumindo agora que $\sum_{i=1}^{k} \frac{1}{\text{ord}\,(g_i)} \leq 1$ para $\langle g_1, \ldots, g_k \rangle$ bloco minimal em $C_{p^{n-1}}$. Provaremos que $\sum_{i=1}^{k} \frac{1}{\text{ord}\,(g_i)} \leq 1$ para $\langle g_1, \ldots, g_k \rangle$ bloco minimal em C_{p^n}.

Para $k = 1$ é trivial. Vamos assumir que a asserção é válida para todo $k' < k$. Seja $\langle g_1, \ldots, g_k \rangle$ um bloco minimal em C_{p^n}. Se $g_i \in C_{p^{n-1}}$ para todo i, $1 \leq i \leq k$, então $\langle g_1, \cdots, g_k \rangle$ é bloco minimal em $C_{p^{n-1}}$ e a asserção é válida pela hipótese de indução com respeito a n. Suponhamos então que: $J = \{i | g_i \notin C_{p^{n-1}}\} \neq \emptyset$. Como $1 = g_1 \cdots g_k$, temos:

$$\prod_{i \in J} g_i = \left(\prod_{i \notin J} g_i \right)^{-1} \in C_{p^{n-1}} \ .$$

Como $J \neq \emptyset$, seja I um subconjunto minimal de J tal que $\prod_{i \in I} g_i \in C_{p^{n-1}}$. Vamos estudar a cardinalidade de I: Primeiramente $|I| \geq 2$. Sejam $h_i = g_i^{p^{n-1}}$, $\forall i \in I$. Então $h_i \in C_{p^{n-1}}$, pois $h_i^p = 1$ e vale que $\prod_{i \in I} h_i = (\prod_{i \in I} g_i)^{p^{n-1}} = 1$.

Para qualquer subconjunto próprio I' de I, $\prod_{i \in I'} g_i \notin C_{p^{n-1}}$. Logo $\prod_{i \in I} h_i \neq 1$.

Pela hipótese de indução aplicada ao bloco minimal composto por h_i, $i \in I$, temos

que $\frac{|I|}{p} \leq 1$, pois $\text{ord}(h_i) = p$. Assim, $2 \leq |I| \leq p$ e temos

$$\sum_{i \in I} \frac{1}{\text{ord}(g_i)} = |I| \frac{1}{p^n} \leq \frac{1}{p^{n-1}} \leq \frac{1}{\text{ord}(g_0)} \ , \quad \text{onde } g_0 = \prod_{i \in I} g_i. \tag{1}$$

Por outro lado, considere o sistema $\langle g_i \rangle$, $i \in L$ onde $L = \{j | 1 \leq j \leq k, j \notin I\} \cup \{0\}$. Como $2 \leq |I|$, segue que $|L| = k - |I| + 1 < k$. Temos ainda que:

$$\prod_{i \in L} g_i = \prod_{i \notin I} g_i . g_0 = 1$$

Para qualquer subconjunto próprio L' de L, $\prod_{i \in L'} g_i \neq 1$. Portanto, o sistema $\langle g_i \rangle$, $i \in L$ é minimal e por indução:

$$\sum_{i \notin I} \frac{1}{\text{ord}(g_i)} + \frac{1}{\text{ord}(g_0)} \leq 1 \ . \tag{2}$$

Combinando (1) e (2), obtemos:

$$\sum_{i=1}^{k} \frac{1}{\text{ord}(g_i)} = \sum_{i \in I} \frac{1}{\text{ord}(g_i)} + \sum_{i \notin I} \frac{1}{\text{ord}(g_i)} \leq \frac{1}{\text{ord}(g_0)} + \sum_{i \notin I} \frac{1}{\text{ord}(g_i)} \leq 1 \ .$$

Assim, a asserção vale para k. ∎

Concluiremos este capítulo com o seguinte teorema devido a Krause, que caracteriza a fatoração em anéis de inteiros com número de Cross 1.

Teorema 3.9 (Teorema de Krause) *O grupo de classe de um corpo de números algébricos é cíclico com ordem potência de um primo se, e somente se, existe um número $m \in \mathbb{N}$ tal que a m-ésima potência de todo inteiro irredutível é produto de no máximo m inteiros primários. Neste caso o número de classes é o mínimo entre os m que satisfazem a condição anterior.*

Demonstração: Suponhamos que o grupo de classes $\mathcal{H}_K$ é cíclico e tem ordem potência de primo. Tomemos x um inteiro irredutível, e seja $(x) = P_1 \cdots P_r$ sua fatoração em

ideais primos. Como x é irredutível, o bloco $B = \langle \overline{P}_1, \ldots, \overline{P}_r \rangle$ é minimal em $\mathcal{H}_K$. Então, pela definição de número de Cross, e pelo Teorema 3.8, $\sum_{i=1}^{r} \frac{1}{n(P_i)} \leq K(\mathcal{H}_K) = 1$. Pelo Lema 3.4, x^h tem fatoração em, no máximo, $n = \left(\sum_{i=1}^{r} \frac{1}{n(P_i)} \right) h \leq h$ inteiros primários.

Reciprocamente, suponha que existe um número $m \in \mathbb{N}$, tal que, para todo x inteiro irredutível, x^m é produto de no máximo m inteiros primários e seja $B = \langle g_1, \ldots, g_r \rangle$, $r \geq 2$, um bloco minimal em $\mathcal{H}_K$. Tomemos ideais primos $P_i \in g_i$. Segue que existe x, inteiro irredutível, tal que $(x) = P_1 \cdots P_r$. Por hipótese x^m é produto de no máximo m inteiros primários. Do Lema 3.4 temos que o número de fatores é $n = \sum_{i=1}^{r} \left(\frac{1}{n(P_i)} \right) m$. Assim, $\sum_{i=1}^{r} \frac{1}{\mathrm{ord}(g_i)} = \sum_{i=1}^{r} \frac{1}{n(P_i)} \leq 1$. Logo $K(\mathcal{H}_K) = 1$. Pelo Teorema 3.8, $\mathcal{H}_K$ é cíclico de ordem potência de um primo.

Agora, supondo que existe m tal que, para todo x inteiro irredutível x^m é produto de no máximo m inteiros primários vamos observar que h é o mínimo entre estes m. Vamos chamar o mínimo de $\overline{m}$. Pelo início da demonstração temos que, $\overline{m} \leq h$. Como $\mathcal{H}_K$ é cíclico, existe um ideal primo P tal que $n(P) = h$.

Afirmamos que existe $x \in \mathcal{O}_K$ irredutível tal que

$(x) = P.P_1^{k_1} \cdots P_r^{k_r}$ com $P_i \neq P$, $1 \leq i \leq r$ e $P_i \neq P_j$ se $i \neq j$. De fato, como $P \supsetneq P^2$, existe $y \neq 0$ tal que $y \in P$, $y \notin P^2$. Fatorando $y = x_1 \cdots x_t$ em irredutíveis temos que existe x_j tal que $x_j \in P, x_j \notin P^2$.

Como a $\overline{m}$-ésima potência de qualquer elemento irredutível tem fatoração em no máximo $\overline{m}$ inteiros primários, temos: $x^{\overline{m}} = u q_1^{l_1} \cdots q_s^{l_s}$ com q_i primários e para $i \neq j$ q_i e q_j não associados, $l_i \in \mathbb{N}$ para $1 \leq i, j \leq s$ e u unidade. Pelo Lema 3.4,

$$(x^{\overline{m}}) = Q_1^{n(Q_1)l_1} \cdots Q_s^{n(Q_s)l_s} , \qquad (1)$$

com Q_i ideais primos distintos.

Por outro lado,

$$(x)^{\overline{m}} = P^{\overline{m}}.P_1^{k_1\overline{m}} \cdots P_r^{k_r\overline{m}} \ . \tag{2}$$

Pela unicidade de fatoração de ideais primos em domínios de Dedekind,

$$P = Q_i \quad \text{e} \quad \overline{m} = n(Q_i)l_i \ , \quad \text{para algum } i.$$

Assim, $h = n(P) = n(Q_i)$ divide $\overline{m}$. Em particular, $h \leq \overline{m}$. Portanto, $\overline{m} = h$. ■

Capítulo 4

O Teorema de Czogala.

Neste capítulo apresentaremos uma caracterização aritmética de corpos de números com número de classes h_k pequeno. Inicialmente vamos formular propriedades aritméticas de anéis de Dedekind que são importantes nos casos considerados.

Definição 4.1 *Dizemos que um anel de Dedekind D tem a propriedade V_n, $n \geq 2$, se para quaisquer elementos irredutíveis $a_1, a_2, b_1, \ldots, b_k \in D$, a igualdade:*

$$a_1.a_2 = b_1 \cdots b_k$$

implica que $k \leq n$.

Dizemos que um anel de Dedekind D tem a propriedade W_n, $n \geq 2$, se tem a propriedade V_n e se para quaisquer elementos irredutíveis $a, b_1, \ldots, b_k \in D$ a igualdade:

$$a^2 = b_1 \cdots b_k$$

implica que $k = 2$.

Assim V_n garante que em D o produto de dois irredutíveis não pode ser representado como o produto de mais que n irredutíveis, e W_n garante adicionalmente que o quadrado de qualquer elemento irredutível tem apenas decomposições de comprimento 2.

Observamos que temos algumas relações triviais entre as propriedades V e W, tais como: $V_n \Rightarrow V_{n+1}$, $W_n \Rightarrow W_{n+1}$ e $W_n \Rightarrow V_n$.

Proposição 4.2 *Seja D um anel de Dedekind com a propriedade que, para qualquer elemento irredutível $a \in D$ o ideal principal (a) é produto de no máximo n ideais primos, $n \geq 2$. Então D tem a propriedade V_n.*

Demonstração: Sejam $a_1, a_2, b_1, \ldots, b_k$ elementos irredutíveis de D tais que

$$a_1 a_2 = b_1 \ldots . b_k.$$

Vamos considerar dois casos:

1º Caso: Um dos ideais principais $(a_1), (a_2), (b_1), \ldots, (b_k)$ é ideal primo. Para fixar a notação podemos supor que (a_1) é ideal primo. O caso (b_1) é ideal primo é análogo a este. Então (a_1) divide um dos ideais (b_i), digamos que seja (b_1). Temos que a_1 divide b_1 em D. Como a_1 e b_1 são elementos irredutíveis em D, então $a_1 = b_1$ a menos de unidades e $a_2 = b_2 \cdots b_k$ e podemos concluir que $k = 2 \leq n$.

2º Caso: Agora vamos supor que nenhum dos ideais $(a_1), (a_2), (b_1), \ldots, (b_k)$ é um ideal primo. Assim, (a_i) é produto de n_i ideais primos, para $i = 1, 2$ e (b_j) é produto de m_j ideais primos, para $j = 1, \ldots, k$. Então $1 < n_i \leq n$ e $1 < m_j \leq n$ para $i = 1, 2$ e $j = 1, \ldots, k$. Assim:

$$2n \geq n_1 + n_2 = m_1 + \cdots + m_k \geq 2k \ .$$

Portanto, $k \leq n$ e vale V_n. ∎

A seguir chegaremos a conclusões quanto à ordem de $\mathcal{H}_K$, grupo de classes do anel de inteiros $\mathcal{O}_K$ de um corpo de números que satisfaz a propriedade V_n ou W_n.

Lema 4.3 *Se $\mathcal{O}_K$ é um anel de Inteiros que satisfaz a propriedade V_n, então a ordem de qualquer elemento do grupo de classes de ideais $\mathcal{H}_K$ é no máximo n.*

Demonstração: Suponhamos que $\mathcal{O}_K$ satisfaz V_n. Tomemos um elemento $X \in \mathcal{H}_K$ com ordem m. Logo a ordem de X^{-1} também é m. Sejam P e Q dois ideais primos tais que $P \in X$ e $Q \in X^{-1}$.Assim P^m e Q^m são ideais principais, digamos, $P^m = (a)$ e $Q^m = (b)$ e PQ também é ideal principal, digamos, $PQ = (c)$. Os elementos a, b, c são irredutíveis e a menos de unidades temos $ab = c^m$. A propriedade V_n implica que $m \leq n$. ∎

A caracterização de corpos de números com número de classe dois agora pode ser enunciada de forma diferente. Eles são exatamente aqueles cujo anel de inteiros $\mathcal{O}_K$ tem a propriedade V_2 e não tem unicidade de fatoração.

O teorema seguinte mostra que as propriedades V_3, V_4, W_3, W_4 são suficientes para caracterizar aritmeticamente corpos de números com número de classes igual a três, quatro e também alguns corpos com número de classe oito.

Teorema 4.4 (Teorema de Czogala) *Seja $\mathcal{O}_K$ um anel de inteiros de um corpo de números algébricos com grupo de classe de ideais $\mathcal{H}_K$ não trivial e C_n o grupo cíclico de ordem n. Então temos:*

(1) $\mathcal{O}_K$ tem a propriedade V_3 se, e somente se, $\mathcal{H}_K = C_2$ ou $\mathcal{H}_K = C_3$ ou $\mathcal{H}_K = C_2 \oplus C_2$;

(2) $\mathcal{O}_K$ tem a propriedade W_3 se, e somente se, $\mathcal{H}_K = C_2$ ou $\mathcal{H}_K = C_3$;

(3) $\mathcal{O}_K$ tem a propriedade W_4 se, e somente se, $\mathcal{H}_K = C_2$ ou $\mathcal{H}_K = C_3$ ou $\mathcal{H}_K = C_4$;

(4) $\mathcal{O}_K$ tem a propriedade V_4 se, e somente se, $\mathcal{H}_K = C_2$ ou $\mathcal{H}_K = C_3$ ou $\mathcal{H}_K = C_4$ ou $\mathcal{H}_K = C_2 \oplus C_2$ ou ainda $\mathcal{H}_K = C_2 \oplus C_2 \oplus C_2$.

Observe que se $\mathcal{H}_K = C_2$, pelo Teorema 2.6 $\mathcal{O}_K$ satisfaz W_2, logo satisfaz V_2, V_3, W_3, V_4 e W_4.

Para a prova deste teorema usaremos a proposição anterior e uma série de lemas que, vão estabelecer as propriedades aritméticas de anéis de Dedekind com grupo de classes de ideais $\mathcal{H}_K = C_3$ ou $\mathcal{H}_K = C_2 \oplus C_2$ ou $\mathcal{H}_K = C_4$ ou ainda $\mathcal{H}_K = C_2 \oplus C_2 \oplus C_2$.

Lema 4.5 *Se D é um anel de Dedekind com grupo de classes $\mathcal{H}_K = C_3$, então D satisfaz W_3.*

Demonstração: Inicialmente mostraremos a propriedade V_3. Tomemos um elemento irredutível $a \in D$ e considerando a fatoração do ideal (a) em produto de ideais primos, temos: $(a) = P_1 \cdots P_n$, com $\langle \overline{P}_1, \ldots, \overline{P}_n \rangle$ bloco minimal. Por outro lado, como $\mathcal{H}_K = C_3$, todo bloco minimal tem comprimento menor ou igual a três. Assim, $n \leq 3$ e pela Proposição 4.2 vale V_3.

Agora vamos ver que D satisfaz a propriedade W_3. Para isso, vamos considerar a igualdade

$$a^2 = b_1 \cdots b_k$$

com $a, b_1, \ldots, b_k$ irredutíveis. Se um dos ideais $(a), (b_1), \ldots, (b_k)$ é primo, analogamente ao primeiro caso da Proposição 4.2, podemos concluir que $k = 2$. Assim, podemos assumir que (a) é produto de $n > 1$ ideais primos e (b_i) é produto de $m_i > 1$ ideais primos, onde $2 \leq n \leq 3$ e $2 \leq m_i \leq 3$. Como $(a)^2 = (b_1) \cdots (b_k)$ temos:

$$6 \geq 2n = m_1 + \cdots + m_k \geq 2k \ .$$

Se $n = 2$, temos $k \leq 2$. Se $n = 3$, os três ideais na fatoração em ideais primos de (a) devem pertencer à mesma classe. Se $k = 3$ então $m_i = 2$, $i = 1, 2, 3$ e os fatores primos

na fatoração de (b_i) devem pertencer a classes distintas, mas isso é incompatível com a unicidade da decomposição em ideais primos. Assim, $k = 2$ e W_3 vale. ∎

Lema 4.6 *Se D é um anel de Dedekind com grupo de classes $\mathcal{H}_K = C_2 \oplus C_2$, então D satisfaz V_3.*

Demonstração: Seja $a \in D$, irredutível e $(a) = P_1 \cdots P_n$ sua fatoração em ideais primos. Então $B = \langle \overline{P}_1, \ldots, \overline{P}_n \rangle$ é bloco minimal. Se $n \geq 4$, deveremos ter dois ideais P_i e P_j na mesma classe de ideais e então $P_i P_j$ é principal, o que contradiz o bloco B ser minimal. Assim, $n \leq 3$ e vale V_3 para D. ∎

Lema 4.7 *Se D é um domínio de Dedekind com grupo de classes $\mathcal{H}_K = C_4$, então D satisfaz W_4.*

Demonstração: Tomemos a, um elemento irredutível de D, e sua fatoração em ideais primos: $(a) = P_1 \cdots P_n$. Então $B = \langle \overline{P}_1, \ldots, \overline{P}_n \rangle$ é bloco minimal. Chamando de X o gerador de $\mathcal{H}_K$ obtemos: $\mathcal{H}_K = \langle 1, X, X^2, X^3 \rangle$. Vamos supor $n \geq 5$. Então, $P_1, \ldots, P_n$ deve ter no máximo um ideal pertencente a X^2 e os outros devem estar distribuídos entre X e X^3, o que em qualquer caso levaria a um subproduto igual a identidade de $\mathcal{H}_K$, uma contradição com B ser minimal. Assim, $n \leq 4$ e D satisfaz V_4 pela Proposição 4.2.

Vamos agora observar o quadrado de elementos irredutíveis de D. Sejam $a, b_1, \ldots, b_k$ irredutíveis de D tais que $a^2 = b_1 \cdots b_k$. Se algum dos ideais (a), $(b_1), \ldots, (b_k)$ é primo, como no primeiro caso da proposição 4.2, temos $k = 2$.

Vamos supor que (a) é produto de $n > 1$ ideais primos e (b_i) é produto de $m_i > 1$ ideais primos, então:

$$8 \geq 2n = m_i + \cdots + m_k \geq 2k \ .$$

Portanto $k \leq 4$ e devemos excluir os casos $k = 4$ e $k = 3$.

Se $k = 4$, temos necessariamente $n = 4$ e $m_i = 2$, $i = 1, 2, 3, 4$. Mas $n = 4$ significa que todos os ideais na fatoração em ideias primos de (a) pertencem a X ou todos pertencem a X^3, enquanto $m_i = 2$ significa que cada fator na fatoração em ideais primos de (b_i) pertence a X^2 ou um pertence a X e outro a X^3. Em qualquer caso, temos uma contradição em relação à unicidade de fatoração em ideais primos do ideal $(a)^2$.

Se $k = 3$ e $n = 4$, temos $m_1 + m_2 + m_3 = 8$ e ao menos um dos m_i's deve ser 2. Raciocinando analogamente ao caso $k = 4$ chegamos a uma contradição.

Se $k = 3$ e $n = 3$, então $m_1 = m_2 = m_3 = 2$ e $(a) = P_1P_2P_3$. Então, um dos ideais P_1, P_2 ou P_3 deve pertencer a X^2 e os outros dois devem estar na mesma classe que deve ser X ou X^3. Mas $(b_i) = P_iP_j$. Assim, ou temos P_i e P_j pertencentes a X^2 ou P_i pertencente a X e P_j pertencente a X^3. De qualquer maneira, temos novamente uma contradição quanto à unicidade de fatoração em ideais primos do ideal $(a)^2$.

Assim, podemos concluir que $k = 2$. ∎

Lema 4.8 *Se D é um domínio de Dedekind com grupo de classes $\mathcal{H}_K = C_2 \oplus C_2 \oplus C_2$, então D satisfaz V_4.*

Demonstração: Suponhamos $a \in D$, irredutível e $(a) = P_1 \cdots P_n$ sua fatoração em ideais primos. $B = \langle \overline{P}_1, \ldots, \overline{P}_n \rangle$ é bloco minimal. Vamos assumir que $n \geq 5$. Como todo elemento de $\mathcal{H}_K$ tem ordem 2 temos que $\overline{P}_1, \ldots, \overline{P}_5, \overline{P_1P_2}, \overline{P_1P_3}, \overline{P_1P_4}, \overline{P_1P_5}$ devem ser distintos dois a dois, o que é impossível já que $\mathcal{H}_K$ tem ordem 8. Assim, $n \leq 4$ e pela Proposição 4.3 temos que D satisfaz V_4. ∎

Proposição 4.9 *Se um anel de inteiros $\mathcal{O}_K$ de um corpo de números satisfaz a propriedade V_4 e seu grupo de classes $\mathcal{H}_K$ é não trivial, então $\mathcal{H}_K$ é um dos seguintes grupos: $C_2, C_3, C_4, C_2 \oplus C_2$ ou $C_2 \oplus C_2 \oplus C_2$.*

Demonstração: $\mathcal{H}_K$ é um grupo abeliano finito, então é soma direta de grupos cíclicos. Pelo Lema 4.3 os grupos cíclicos desta soma só podem ser C_2, C_3 e C_4. Como cada um dos grupos $C_2 \oplus C_3$ e $C_3 \oplus C_4$ tem um elemento de ordem maior que 4, então $\mathcal{H}_K$ não deve ter qualquer subgrupo deste tipo.

Sobram duas possibilidades, $\mathcal{H}_K = C_2^r \oplus C_4^s$ com $r \geq 0$ e $s \geq 0$ e $\mathcal{H}_K = C_3^t$, com $t \geq 0$. Vamos estudar cada uma das possibilidades.

Para a primeira possibilidade, $\mathcal{H}_K = C_2^r \oplus C_4^s$, tomemos $r > 0$ e $s > 0$, então $\mathcal{H}_K$ contém um subgrupo da forma $C_2 \oplus C_4$. Tomemos $X_1 = (0,1)$, $X_2 = (1,1)$, $X_3 = (1,0)$, $X_4 = (0,3)$, $X_5 = (1,3)$ em $C_2 \oplus C_4 \subset \mathcal{H}_K$, e ideais primos de $\mathcal{O}_K$ tais que $P_1 \in X_1$, $P_2 \in X_2, \ldots, P_5 \in X_5$. Então $P_1^3P_2P_3$, $P_3P_4^3P_5$, P_1P_4, P_2P_5, P_3^2 são ideais principais, digamos, $P_1^3P_2P_3 = (a_1)$, $P_3P_4^3P_5 = (a_2)$, $P_1P_4 = (b_1)$, $P_2P_5 = (b_2)$ e $P_3^2 = (b_3)$ e a_1, a_2, b_1, b_2 e b_3 são irredutíveis. Temos ainda $(a_1)(a_2) = P_1^3P_4^3P_2P_5P_3^2 = (b_1)^3(b_2)(b_3)$. Assim, a menos de unidades, temos $a_1a_2 = b_1^3b_2b_3$, o que contradiz V_4.

Assim, podemos ter apenas $\mathcal{H}_K = C_2^r$ ou $\mathcal{H}_K = C_4^s$.

Inicialmente vamos supor $\mathcal{H}_K = C_2^r$, com $r \geq 4$. Então $\mathcal{H}_K$ tem um subgrupo C_2^4 e sejam $X_1 = (1,0,0,0)$, $X_2 = (0,1,0,0)$, $X_3 = (0,0,1,0)$, $X_4 = (0,0,0,1)$ e $X_5 = (1,1,1,1) \in C_2^4 \subset \mathcal{H}_K$. Tomemos ideais primos $P_i \in X_i$ para $i = 1, \ldots, 5$. Sabemos que P_i^2 e $P_1P_2P_3P_4P_5$ são ideais principais, digamos, $(a) = P_1P_2P_3P_4P_5$ e $(b_i) = P_i^2$, para $i = 1, \ldots, 5$ e $a, b_1, \ldots, b_5$ irredutíveis. A menos de unidades temos $a^2 = b_1 \cdots b_5$ o que contradiz V_4. Podemos concluir que se $\mathcal{H}_K = C_2^r$, então $r \leq 3$.

Agora vamos estudar $\mathcal{H}_K = C_4^s$ com $s > 1$. Então $\mathcal{H}_K$ tem $C_4 \oplus C_4$ como subgrupo e portanto podemos escolher $X_1 = (0,1)$, $X_2 = (1,0)$, $X_3 = (2,2)$, $X_4 = (0,3)$

e $X_5 = (3,0) \in C_4 \oplus C_4 \oplus C_4 \subset \mathcal{H}_K$. Tomemos ideais primos P_i em X_i, $i = 1,\ldots,5$. Observemos que os ideais $P_1^2P_2^2P_3$, $P_3P_4^2P_5^2$, P_1P_4, P_2P_5, P_3^2 são todos principais, digamos, $(a_1) = P_1^2P_2^2P_3$, $(a_2) = P_3P_4^2P_5^2$, $(b_1) = P_1P_4$, $(b_2) = P_2P_3$ e $(b_3) = P_3^2$ com a_1, a_2, b_1, b_2 e b_3 irredutíveis. Como $(a_1)(a_2) = P_1^2P_2^2P_3^2P_4^2P_5^2 = (b_1)^2(b_2)^2(b_3)$, a menos de unidade $a_1a_2 = b_1^2b_2^2b_3$, o que contradiz V_4. Portanto, se $\mathcal{H}_K = C_4^s$, então $s = 1$.

Agora estudemos a segunda possibilidade, $\mathcal{H}_K = C_3^t$. Tomemos $t > 1$. Então $\mathcal{H}_K$ contém um subgrupo $C_3 \oplus C_3$. Sejam $X_1 = (0,1)$, $X_2(1,0)$, $X_3 = (1,1)$, $X_4 = (0,2)$, $X_5 = (2,0)$ e $X_6 = (2,2) \in C_3 \oplus C_3 \subset \mathcal{H}_K$ e podemos escolher P_i ideais primos tais que $P_i \in X_i$, $i = 1,\ldots,6$. Os ideais $P_1^2P_2^2P_3$, $P_4^2P_5^2P_6$, P_1P_4, P_2P_5, P_3P_6 são principais, digamos, $(a_1) = P_1^2P_2^2P_3$, $(a_2) = P_4^2P_5^2P_6$, $(b_1) = P_1P_4$, $(b_2) = P_2P_5$, $(b_3) = P_3P_6$ com a_1, a_2, b_1, b_2 e b_3 irredutíveis. Como $(a_1)(a_2) = P_1^2P_2^2P_3P_4^2P_5^2P_6 = (b_1)^2(b_2)^2(b_3)$, a menos de unidades temos $a_1a_2 = b_1^2b_2^2b_3$, o que contradiz V_4. Portanto, se $\mathcal{H}_K = C_3^t$, então $t = 1$. ∎

Lema 4.10 *Se $\mathcal{O}_K$ é anel de inteiros de um corpo de números que satisfaz W_4 e seu grupo de classes $\mathcal{H}_K$ é não trivial, então $\mathcal{H}_K = C_2$, $\mathcal{H}_K = C_3$ ou $\mathcal{H}_K = C_4$.*

Demonstração: Sabemos que se $\mathcal{O}_K$ satisfaz W_4, então $\mathcal{O}_K$ satisfaz V_4 e pela proposição anterior $\mathcal{H}_K = C_2$, $\mathcal{H}_K = C_3$, $\mathcal{H}_K = C_4$, $\mathcal{H}_K = C_2 \oplus C_2$ ou ainda $\mathcal{H}_K = C_2 \oplus C_2 \oplus C_2$. Basta mostrar que se $\mathcal{O}_K$ satisfaz W_4, então $\mathcal{H}_K$ não pode ter $C_2 \oplus C_2$ como subgrupo. Caso contrário, sejam $X_1 = (0,1)$, $X_2 = (1,0)$ e $X_3 = (1,1) \in C_2 \oplus C_2 \subset \mathcal{H}_K$ e tomemos ideias primos $P_1 \in X_1$, $P_2 \in X_2$ e $P_3 \in X_3$. Os ideais $P_1P_2P_3$, P_1^2, P_2^2 e P_3^2 são principais, digamos, $(a) = P_1P_2P_3$, $(b_1) = P_1^2$, $(b_2) = P_2^2$ e $(b_3) = P_3^3$, com a, b_1, b_2 e b_3 irredutíveis. Como $(a)^2 = P_1^2P_2^2P_3^2 = (b_1)(b_2)(b_3)$, a menos de unidades temos: $a^2 = b_1b_2b_3$, o que contradiz W_4. ∎

Lema 4.11 *Se $\mathcal{O}_K$ é anel de inteiros de um corpo de números que satisfaz V_3 e seu grupo de classes $\mathcal{H}_K$ é não trivial, então $\mathcal{H}_K = C_2$, $\mathcal{H}_K = C_3$ ou $\mathcal{H}_K = C_2 \oplus C_2$.*

Demonstração: Como $\mathcal{O}_K$ satisfaz V_3, então $\mathcal{H}_K$ satisfaz V_4 e, usando a Prop 4.9, precisamos apenas descartar as possibilidades $\mathcal{H}_K = C_4$ e $\mathcal{H}_K = C_2 \oplus C_2 \oplus C_2$.

Inicialmente vamos supor que $\mathcal{H}_K = C_4$. Seja X um gerador de $\mathcal{H}_K$ e tomemos P_1, P_2 ideais primos tais que $P_1 \in X$ e $P_2 \in X^{-1}$. Então, P_1P_2, P_1^4, P_2^4 são ideais principais, digamos, $P_1P_2 = (a)$, $P_1^4 = (b_1)$ e $P_2^4 = (b_2)$, com a, b_1 e b_2 irredutíveis. Como $(a)^4 = P_1^4P_2^4 = (b_1)(b_2)$, temos, a menos de unidades, $a^4 = b_1b_2$, o que contradiz V_3.

Agora vamos assumir que $\mathcal{H}_K = C_2 \oplus C_2 \oplus C_2$. Tomemos os seguintes elementos de H, $X_1 = (0,0,1)$, $X_2 = (0,1,0)$, $X_3 = (1,0,0)$ e $X_4 = (1,1,1)$ e sejam os ideais primos $P_i \in X_i$, para $i = 1,\ldots,4$. Todos os ideais $P_1P_2P_3P_4$, P_1^2, P_2^2, P_3^2, P_4^2 são principais, digamos, $(a) = P_1P_2P_3P_4$, $(b_1) = P_1^2$, $(b_2) = P_2^2$, $(b_3) = P_3^2$ e $(b_4) = P_4^2$, com a, b_1, b_2, b_3 e b_4 irredutíveis. Como $(a)^2 = P_1^2P_2^2P_3^2P_4^2 = (b_1)(b_2)(b_3)(b_4)$, a menos de unidades, temos $a^2 = b_1b_2b_3b_4$, o que contradiz V_3. ∎

Lema 4.12 *Se $\mathcal{O}_K$ é anel de inteiros de um corpo de números que satisfaz W_3 e um grupo de classes $\mathcal{H}_K$ não trivial, então $\mathcal{H}_K = C_2$ ou $\mathcal{H}_K = C_3$.*

Demonstração: Como $\mathcal{O}_K$ satisfaz W_3, então satisfaz V_3. Pelo lema anterior , $\mathcal{H}_K = C_2$, $\mathcal{H}_K = C_3$ ou $\mathcal{H}_K = C_2 \oplus C_2$. Como $\mathcal{O}_K$ satisfaz W_3, então satisfaz W_4 e, pelo Lema 4.10, $H = C_2$, $\mathcal{H}_K = C_3$ ou $\mathcal{H}_K = C_4$. Portanto, $\mathcal{H}_K = C_3$ ou $\mathcal{H}_K = C_2$. ∎

Através do Teorema 4.4 podemos caracterizar os corpos, cuja ordem do grupo de classe é menor que 4 pelo corolário que segue, lembrando apenas das caracterizações já estudadas nos casos $h_k = 1$ e $h_k = 2$.

Corolário 4.13 *Seja $\mathcal{O}_K$ o anel de inteiros de um corpo de números K com grupo de classe $\mathcal{H}_K$ não trivial. Então*

(1) $\mathcal{H}_K = C_3$ se, e somente se, $\mathcal{O}_K$ satisfaz W_3 e não satisfazV_2;

(2) $\mathcal{H}_K = C_2 \oplus C_2$ se, e somente se, $\mathcal{O}_K$ satisfaz V_3 e não satisfaz W_3;

(3) $\mathcal{H}_K = C_4$ se, e somente se, $\mathcal{O}_K$ satisfaz W_4 e não satisfaz W_3;

(4) $\mathcal{H}_K = C_2 \oplus C_2 \oplus C_2$ se, e somente se, $\mathcal{O}_K$ satisfaz V_4 e não satisfaz W_4 nem V_3. □

Bibliografia:

[1] ATIYAH, M.F.; MACDONALD I.G. *Introduction to Commutative Algebra.* Reading, Addison–Wesley, 1969. 128p.

[2] BOREVICH, Z.I.; SHAFAREVICH, I.R. *Number Theory.* New York, Academic Press, 1966. 435p. (Pure and Applied Mathematics, 20). New York.

[3] CARLITZ, L. A Characterization of Algebraic Number Field with Class Number Two. *Proceedings of the American Mathematical Society,* v.11, n.3, part.I, p.391–392, 1960.

[4] CHAPMAN, S.T.; On the Lengths of Factorizations of Elements in an Algebraic Number Ring. *Journal of Number Theory,* v.43, n.1, p.24 – 30, 1993.

[5] CHAPMAN, S.T.; SMITH, W.W.; Factorizations on Dedekind Domains with Finite Class Group. *Israel Journal of Mathematics,* v.71, n.1, p.65 – 95, 1990.

[6] CLABORN, L. Specified Relations in the Ideal Group. *Michigan Mathematical Journal,* v.15, n.2, p.249 – 255, 1966.

[7] CZOGALA, A. Arithmetic Characterization of Algebraic Number Fields with Small Class Numbers. *Mathematische Zeitschrift*, v.176, n.2, p.247–253, 1981.

[8] ENDLER, O. *Teoria dos Números Algébricos.* Rio de Janeiro, IMPA–CNPq, 1986. 199p. (Projeto Euclides).

[9] GEROLDINGER, A.; The Cross Number of Finite Abelian Groups. *Journal of Number Theory*, v.48, n.2, p.219 –223, 1994.

[10] KACZOROWSKI. J.; A Pure Arithmetical Characterization for Certain Fields with a given Class Group. *Colloquium Mathematicum*, v.45, n.2, p.327 –330, 1981.

[11] KRAUSE, U. A characterization of Algebraic Number Fields with Cyclic Class Group of Prime Power Order. *Mathematische Zeitschrift*, v.186, n.2, p.143–148, 1984.

[12] MARCUS, D.A. *Number Fields.* New York, Springer–Verlag, 1977. 279p. (Universitext)

[13] NARKEWICZ, W. *Elementary and Analytic Theory of Algebraic Numbers.* Warszawa, Polish Scientific Publishers, 1974.

[14] NARKEWICZ, W. ; ŚLIWA, J. Finite Abelian Groups and Factorization Problems II. *Colloquium Mathematicum*, v.15, n.1, p.49–58, 1966.

[15] NARKEWICZ, W. Finite Abelian Groups and Factorization Problems. *Colloquium Mathematicum,* v.42, n.2, p.319–330, 1979.

[16] NARKEWICZ, W. Some Insolved Problems. *Bulletin de La Societè mathematique de France,* memoire 25, p.159–164, 1971. (Supplement au Numero de Mars, 1971).

[17] OLSON, J.E. A Combinatorial Problem on Finite Abelian Groups I. *Journal of Number Theory,* v.1, n.1, p.8 – 10, 1969.

[18] OLSON, J.E. A Combinatorial Problem on Finite Abelian Groups II. *Journal of Number Theory,* v.1, n.2, p.195–199, 1969.

[19] RUSH, D.E.; An Arithmetic Characterization of Algebraic Number Fields with a given Class Group. *Mathematical Proceedings of the Cambridge Philosophical Society,* v.94, n.1, p. 23 – 28, 1983.

[20] STWART, I.N. and TALL, D.O. *Algebraic Number Theory.* London, Chapman and Hall, 1979. 257p. (Chapman and Hall Mathematics Series).

[21] ZAKS, A. Half–Factorial Domains. *Bulletin of American Society,* v.82, n.5, p.721–724, 1976.

[22] ZAKS, A. Half–Factorial Domains. *Israel Journal of Mathematics,* v.37,n.4, p.281–302, 1980.