UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE CIÊNCIA
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

FLAVIANO FROTA DE SOUSA

ALGUNS RESULTADOS SOBRE O GRUPO DAS CLASSES DOS CORPOS QUADRÁTICOS

FORTALEZA
2017

FLAVIANO FROTA DE SOUSA

ALGUNS RESULTADOS SOBRE O GRUPO DAS CLASSES DOS CORPOS QUADRÁTICOS

Dissertação submetida à coordenação do curso de Pós-Graduação em Matemática da Universidade Federal do Ceará,para a obtenção do grau de mestre em Matemática. Área de concentração: Álgebra

Orientador: Prof. Dr. José Othon Dantas Lopes

FORTALEZA

2017

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

S696a Sousa, Flaviano Frota de.
Alguns resultados sobre o grupo das classes dos corpos quadráticos / Flaviano Frota de Sousa. – 2017.
74 f.

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Programa de Pós-Graduação em Matemática, Fortaleza, 2017.
Orientação: Prof. Dr. José Othon Dantas Lopes.

1. Discriminantes. 2. Corpos quadráticos reais e imaginários. 3. Grupos das classes. I. Título.
CDD 510

FLAVIANO FROTA DE SOUSA

ALGUNS RESULTADOS SOBRE O GRUPO DAS CLASSES DOS CORPOS QUADRÁTICOS

Dissertação apresentada ao programa de Pós-graduação em matemática do Departamento de matemática da Universidade Federal do Ceará, como parte dos requisitos necessário para obtenção do título de mestre em matemática
Área de concentração: Álgebra

Aprovoda em: 28 /07 / 2017.

BANCA EXAMINADORA

Prof. Dr. José Othon Dantas Lopes (Orientador)
Universidade Federal do Ceará (UFC)

Profª. Dr. José Valter Lopes Nunes
Universidade Federal do Ceará (UFC)

Prof. Dr. Ângelo Papa Neto
Instituto Federal de Educação de Ciência e Tecnologia do Ceará (IFCE)

Dedico este trabalho a minha mãe Assunção(in Memoriam) e a minha querida irmã Flaviana.

AGRADECIMENTOS

Em memória de minha mãe que sempre me deu todo apoio,e minha irmã a que sempre me incentivou e acreditou ao meu orientador, José Othon Dantas Lopes, pela paciência e dedicação e por depositar em mim sua confiança diante desse trabalho. aos meus professores de graduação, Alberto Maia, Francisco Pimentel, José de Anchieta Delgado, aos meus colegas do curso de pós-graduação, pela amizade agradável e convívio, e a coordenação da pós-graduação, á capes pelo suporte financeiro. E acima de tudo Deus, pois sem a permissão dele tudo isso não seria possível.

”Se Cheguei até aqui foi porque me apoiei no ombro dos gigantes...”(Isaac Newton)

RESUMO

Muitos são os resultados conhecidos envolvendo o grupo dos corpos de números e muitos são os problemas em aberto. Sabemos que o grupo das classes de um corpo de números é finito e abeliano. Neste trabalho apresentaremos alguns resultados sobre o grupo das classes dos corpos quadráticos. Sabe-se que para cada inteiro n maior que zero existem infinitos corpos quadráticos, tanto reais como imaginários, cujos os grupos das classes possuem um subgrupo cíclico de ordem n.
Para um grupo abeliano arbitrário G de ordem n, a existência ou não de infinitos corpos quadráticos com grupos das classes de ideais tendo um subgrupo isomorfo a G é um problema em aberto. Particularmente para grupos finitos abelianos não cíclicos G, Kwang-Seob Kim provou que, se $G = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, existem infinitos corpos quadráticos reais cujos os grupos das classes de ideais contêm um subgrupo isomorfo a G e que se $G = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, então existem infinitos copos quadráticos imaginários cujos os grupos das classes de ideais contêm um subgrupo isomorfo a G. O teorema de Kwang-Seob Kim é o principal resultado apresentado nesta dissertação.

Palavras-Chave: Discriminantes. Corpos quadráticos reais e imaginários. Grupos das classes.

ABSTRACT

Many are the known results involving the groups of numbers fields and many are the open problems. We know that the group of classes of a number fields is finite and abelian. In this paper we present some results about the group of the classes of the quadratic fields. It is known that for every intergers n greater than zero there are infinite quadratic fields, both real and imaginary, whose class groups have a cyclic subgroup of order n. For an arbitrary abelian group G of order n, the existence or not of infinite quadratic fields with groups of ideal classes having a subgroup isomorphic to G is an open problem. Particularly for non-cyclic finite abelian groups G, Kwang-Seob Kim has proved that there are infinite real quadratic bodies in $G = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Whose groups of ideal classes contains a subgroup isomorphic to G and that is $G = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ then there are infinite imaginary quadratic cups whose groups of ideal classes contain a subgroup isomorphic to G. The theorem of Kwang-Seob Kim is the main result presented in this dissertation.

Keywords: Discriminants. Fields reals and imaginary quadratics. Groups of classes

LISTA DE SÍMBOLOS

$\mathbb{N}$	Conjunto dos Números Naturais
$\mathbb{Z}$	Conjunto dos Números Inteiros
$\mathbb{Q}$	Conjunto dos Números Racionais
$\mathbb{R}$	Conjunto dos Números Reais
K, L	Corpos
$\mathfrak{a}$,$\mathfrak{b}$,$\mathfrak{p}$,$\mathfrak{q}$:	ideais
$F(X)$, $G(X)$, $P(X)$, $Q(X)$	POLINÔMIOS
$[\mathrm{L}/K : L]$	uma extensão de K
$A[x]$:	anel dos polinômios sobre A em x
$Ker(\sigma)$:	núcleo do homomorfismo
a/b:	a divide b
$\varphi(n)$:	φ-função de Euler para o inteiro n
$[L : K]$:	grau de L sobre K
$N_{L/K}$:	norma em relação à extensão L/K
$N(\mathfrak{p})$:	norma de um ideal $\mathfrak{p}$
$T_{rL/K}$:	traço em relação à extensão L/K
(A_{ij}):	matriz
$det(A_{ij})$:	determinante da matriz (A_{ij})
$D(x_1, ..., x_n)$	discriminante de uma n-upla
Σ:	somatório
Π:	produtorio
$K = \mathbb{Q}(\sqrt{d})$	Corpo quadrático onde d é livre de quadrado

SUMÁRIO

1 INTRODUÇÃO

No segundo capítulo introduzimos os conceitos de divisibilidade em anéis de ideais principais, módulos sobre anéis de ideais principais, raízes da unidade, corpos finitos, elementos inteiros sobre anéis e algébricos sobre um corpo, elementos conjugados, corpos conjugados, inteiros em corpos quadráticos, norma, traço, discriminante, corpos numéricos e módulos Noetherianos, anel de Dedekind, norma de um ideal e outros conceitos indispensáveis ao desenvolvimento dos demais capítulos.

Em seguida mostraremos que existem infinitos corpos quadrático reais com grupo das classes de ideais, tendo um subgrupo isomorfo $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ para cada número natural $n > 0$. Ao mesmo tempo, mostraremos que existem infinitos corpos quadráticos imaginário com o grupo das classes de ideais, tendo um subgrupo isomorfo a $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

2 PRELIMINARES

2.1 Classes residuais e grupos abelianos finitos

Definição 2.1 *Seja n um inteiro positivo. Dois número inteiros a e b são ditos congruente módulo n se as divisões euclidiana de a e b por n tiverem o mesmo resto. Neste caso, denotemos $a \equiv b\,(mod\, n)$.*

Equivalentemente, a e b são congruentes módulo n quando $n|(a-b)$. Como a relação de congruência módulo n é de equivalência, podemos considerar a classe residual de um inteiro a módulo n dado pelo conjunto $\bar{a} = \{x \in \mathbb{Z} : x \equiv a(mod\, n)\} = \{a + kn : k \in \mathbb{Z}\}$. Como em toda divisão euclidiana com divisor n os únicos restos possíveis são os valores inteiro, $0, 1, ..., n-1$, então o conjunto das classes residuais módulo n tem n elementos. Denotaremos esse conjunto por $\mathbb{Z}_n$ ou $\mathbb{Z}/n\mathbb{Z}$. Assim, $\mathbb{Z}_n = \{\bar{0}, \bar{1}, ..., \overline{n-1}\}$. Definimos duas operações sobre $\mathbb{Z}_n$: a soma de dois elementos $\bar{a}$ e $\bar{b}$ é dada por $\bar{a} + \bar{b} = \overline{a+b}$ e a multiplicação e dada por $\bar{a}\bar{b} = \overline{ab}$. Facilmente verifica que $(\mathbb{Z}_n, +)$ é um grupo cujo elemento neutro é $\bar{0}$. Por sua vez, $\mathbb{Z}_n$ com a operação de multiplicação, não é um grupo, pois nem todo elemento é invertível. Daí, vem a necessidade da proposição seguinte:

Proposição 2.1 *Um elemento $\overline{a} \in \mathbb{Z}_n$ é invertível (sobre a multiplicação) se, e somente se, $mdc(a, n) = 1$*

Demonstração: Seja $\overline{a} \in \mathbb{Z}_n$ um elemento invertível. Então, existe $\overline{b} \in \mathbb{Z}_n$ tal que $\overline{a}\overline{b} = \overline{ab} = \overline{1}$. Logo, $ab \equiv 1(mod\, n)$, donde segue que $n/(ab-1)$ e se existisse um primo p tal que dividisse n e a ao mesmo tempo, então p dividiria 1, o que é um absurdo. Logo, $mdc(n, a) = 1$. Reciprocamente, se $mdc(a, n) = 1$ então, a identidade de Bezout nos garante que existem b e q tais que $ab + qn = 1$. Logo, $n/(ab-1)$. Daí, $\overline{a}\overline{b} = \overline{ab} = \overline{1}$, ou seja, $\overline{a}$ é invertível

O conjunto dos elementos invertíveis (sobre a multiplicação) de $\mathbb{Z}_n$ será denotado por $\mathbb{Z}_n^*$ ou por $(\mathbb{Z}/n\mathbb{Z})^*$. Assim, a proposição nos mostra que que $\mathbb{Z}_n^* = \{\overline{a} \in \mathbb{Z}_n; mdc(a, n) = 1\}$. É fácil que ver $(\mathbb{Z}_n^*, \cdot)$ é um grupo. Claramente $\mathbb{Z}_n$ é um anel, porém nem sempre é um corpo. Exemplo, $\mathbb{Z}_4$ não é um corpo, já que $\overline{2}$ não tem inverso multiplicativo.

Proposição 2.2 *$\mathbb{Z}_p$ é um corpo se, e somente se, p é primo .*

Demonstração: Suponha que $\mathbb{Z}_p$ é um corpo, então $\mathbb{Z}_p - \{0\}$ é um grupo multiplicativo. Logo $mdc(a, p) = 1$ para todo $1 \leq a < p$. Logo, não existe $a < p$ e diferente de 1, que divide p. Portanto p é primo. Por outro lado, se p é primo, então o $mdc(a, p) = 1$ para todo $1 \leq a \leq p$. Daí, o conjunto dos elementos invertíveis de $\mathbb{Z}_p$ é $\{\bar{a} \in \mathbb{Z}_p : mdc(a, p) = 1\} = \mathbb{Z}_p - \{0\}$ e assim $\mathbb{Z}_p$ é um corpo.

Proposição 2.3 *Todo grupo cíclico com n elementos é isomorfo a $\mathbb{Z}_n$*

.

Demonstração: Seja G um grupo cíclico escrito aditivamente com n elementos cujo o gerador é g. Considere $\theta : \mathbb{Z} \longrightarrow G$ definida por $\theta(m) = mg$, para todo $m \in \mathbb{Z}$. Essa aplicação é um homomorfismo sobrejetor de grupos. Além disso, $\theta(m) = 0$ se, e só se $n|m$ (pois G tem ordem n). Logo, $ker(\theta) = n\mathbb{Z}$. Portanto, o teorema do Homomorfismo de grupo garante que $G \simeq \mathbb{Z}/n\mathbb{Z}$.

Proposição 2.4 *Se a é um inteiro positivo, então $\overline{a}$ é gerador de $\mathbb{Z}_n$ se, e só, se $mdc(a, n) = 1$.*

Demonstração: Suponha que $\overline{a}$ é um gerador de $\mathbb{Z}_n$ e $d = mdc(a, n)$ então $(n/d)a \equiv n(a/d) \equiv 0\,(mod\, n)$. Como a tem ordem n então $n|(n/d)$. Logo, $d = 1$. Por outro lado se, $mdc(a, n) = 1$ e h é a ordem de $\overline{a}$ então n/ha, pois $ha \equiv 0(mod\, n)$. Daí, n/h. Além disso, $n\overline{a} = \overline{0}$ implica que h/n. Portanto $n = h$.

Proposição 2.5 *Seja $n = \prod_{i=1}^{r} p_i^{e_i} > 1$, em que cada p_i é primo e $e_i > 0$ e $1 < i \leq r$. Então existe um isomorfismo de anéis $\phi : \mathbb{Z}_n \longmapsto \prod_{i=1}^{r} \mathbb{Z}_{p_i^{e_i}}$*

Demonstração: *Considere $\theta : \mathbb{Z} \longrightarrow \Pi_{i=1}^{n} \mathbb{Z}_{p_i^{e_i}}$ definida por $\theta(n) = (v_1, , , , v_r)$ para todo $n \in \mathbb{Z}$ em que v_i é a classe residual de n módulo $p_i^{e_i}$. Assim, θ é um homomorfismo de anéis com $K(\theta) = n\mathbb{Z}$, Pois m é múltiplo de n se, e somente se m é múltiplo de todo p_i^{ei}, $(1 \leq i \leq r)$. Logo, a aplicação induzida $\phi : \mathbb{Z}/n\mathbb{Z} \longmapsto \prod_{i=1}^{r} \mathbb{Z}_{p_i^{e_i}}$ é injetora. Como o número de elementos de $\prod_{i=1}^{r} \mathbb{Z}_{p_i^{e_i}}$ é igual a $\prod_{i=1}^{r} p_i^{e_i} = n$, segue-se ϕ é bijetora. Então segue o resultado.*

O seguinte corolário é conhecido como ***Teorema Chinês do Resto***

Corolário 2.1 *Se $p_1, p_2, ..., p_r$ são primos distintos, $e_1, e_2, ..., e_r$ são inteiros positivos e $a_1, a_2, ..., a_r$ inteiros quaisquer, então existe $n \in \mathbb{N}$ tal que $n \equiv a_i(mod\, p_i^{e_i})$, para todo $1 \leq i \leq r$. Além disso, n é único módulo $\Pi_{i=1}^{n} p_i^{e_i}$.*

Demostração: *Seja v_i a classe residual de a_i módulo $p_i^{e_i}$, devido ao isomorfismo estabelecido na proposição(2.5), existe um único $\overline{n} \in \mathbb{Z}_n$ tal que $\phi(\overline{n}) = (a_1, ..., a_r)$. Assim, n satisfaz as congruência $n \equiv a_i(mod\, p_i^{e_i})$. Portanto, segue o resultado.*

2.2 Divisibilidade em anéis de ideais principais e a função de φ Euler

Definição: Sejam A um domínio de integridade, $K = \{\frac{a}{b} \,|\, a, b \in A, b \neq 0\}$ seu corpo de frações e x, y elementos de K. Dizemos que x divide y se existe $a \in A$ tal que $y = ax$ Equivalentemente, dizemos que x é um divisor de y, ou ainda que y é um múltiplo de x.

Definição: Dado um $x \in k$, chamamos Ax o conjunto dos múltiplo de x. Assim podemos dizer que $y \in Ax$, em vez de $x|y$, ou ainda $Ay \subset Ax$.

Observação: O conjunto Ax é chamado um ideal fracionário principal de K, com respeito a A. Se $x \in A$, então Ax é o ideal principal (ordinário) de A gerado por x.

A relação de divisibilidade possui as seguintes propriedades:
(i) $x|x$
(ii) Se $x|y$ e $y|z$ então $x|z$
Em geral, não podemos concluir se $x|y$ e $y|x$ então $x = y$. Podemos apenas dizer que $Ax = Ay$, o que significa (se $y \neq 0$) que o quociente xy^{-1} é um elemento invertível de A. Neste caso, x e y são chamados associados.

Observação: Os elementos de K que são associados de 1, são os elementos invertíveis em A. Eles são chamados as unidades de A. Estes elementos formam um grupo com a multiplicação e denotamos por A^*.

Exemplo: Se A é um corpo, então $A^* = A - (0)$. Se $A = \mathbb{Z}$, então $A^* = \{1. - 1\}$

Definição: Um anel A é chamado de ideais principais, se o mesmo é um domínio de integridade e se todo ideal dele for principal.

Exemplo: $\mathbb{Z}$ é um anel de ideais principais

Exemplo: Se K é um corpo, o anel de polinômios em variável sobre K, $K[x]$, é um anel de ideais principais.

Vejamos algumas propriedades de divisibilidade em um corpo de frações K de um anel ideais principais A.

(i). Dois elementos arbitrários u e v de K possuem um máximo divisor comum (mdc), i.e, um elemento $d \in K$ tal que:

(1) d/u e d/v

(2) Se $x \in K$ $x|u$, $x|v$, então $(x|d)$

(ii). **(Identidade de Bezout):** Existem elementos $a, b \in A$ tal que o mdc de u e v pode ser inscrito da forma:

$$d = au + bv$$

(iii). Dois elementos abitrários u e v de K, possuem um mínimo múltiplo comum (mmc), isto é, existe um elemento $m \in K$, tal que.

(1) $u|m$ e $v|m$

(2) Se $y \in K$, $u|y$ e $v|y$, então $m|y$

(iv) Vale a seguinte relação entre o mdc e mmc:

$$mdc(u, v).mmc(u, v) = u.v$$

Definição: Dois elementos de a, b de A são chamados relativamente primos se $mdc(a, b) = 1$.

Lema 2.1 *(Euclides) Sejam a, b elementos inteiros de anéis de ideais principais A. Se a divide bc e a relativamente primo com b então, a divide c.*

Demonstração: Pela identidade de Bezout, existem $a', b' \in A$ tais que:

$$1 = a'a + b'b \Rightarrow c = a'ac + b'bc$$

Como a divide bc, então a divide $b'bc$. Por outro lado, a divide $a'ac$. Logo, a divide $a'ac + b'bc$ e daí a divide c.

O teorema a seguir mostra que existe uma única fatoração em produtos de primos.
Teorema 2.1 *Seja A um anel de ideais principais e K seu corpo de frações. Então existe um subconjunto $P \subset A$ tal que todo $x \in K$ pode ser expresso unicamente da forma*

$$x = u\Pi_{p \in P}\, p^{v_p(x)}$$

onde u é uma unidade em A e os expoentes $v_p(x)$ são elementos de $\mathbb{Z}$, todos nulos exceto para um subconjunto finito deles.

(Para uma demonstração desse teorema, veja em [Mollin, teorema 2.1 1999])

Definição: Seja $n \geq 1$, definimos $\varphi(n)$ como sendo o número de inteiros q, com $0 \leq q \leq n$, tal que q e n são relativamente primos. Como 0 e n são divisíveis por n, basta considerarmos $1 \leq q \leq n - 1$, $\forall n > 1$ e definimos $\varphi(1) = 1$. A função φ assim definida é chamada função φ de Euler.

Observação Se p é primo, então claramente temos:

$$\varphi(p) = p - 1$$

pois, como p é primo, todos elementos q, com $1 \leq q \leq p-1$, são relativamente primos com p.
Observação: Se $n = p^s$, uma potência de um primo, então os inteiros relativamente primos com n são todos os inteiros q, com $1 \leq q \leq n-1$, os quais não são múltiplos de p.

Proposição 2.6 *Seja $n \geq 1$ um número natural. O Valor $\varphi(n)$ da φ-função Euler é igual ao número de elementos de $\mathbb{Z}/n\mathbb{Z}$ que geram esse grupo. Também é igual ao número de unidades do anel $\mathbb{Z}/n\mathbb{Z}$.*

Demonstração: Sabemos que cada classe de congruência módulo $n\mathbb{Z}$, contém um único inteiro q tal que $0 \leq q \leq n-1$. Para cada inteiro q, denote $\overline{q}$ sua classe residual módulo n. Para demonstrar esta proposição vamos mostrar as seguintes implicações:
(i) Se q é relativamente primo com n, então $\overline{q}$ é uma unidade do anel $\mathbb{Z}/n\mathbb{Z}$

De fato, suponha que q seja relativamente primo com n. Assim, pela identidade de Bezout, existem inteiros x, y tais que $qx + ny = 1$. Daí, $\overline{qx+ny}=\overline{1} \Rightarrow \overline{qx}+\overline{ny} = \overline{1} \Rightarrow \overline{qx} = \overline{1}$ $\Rightarrow \overline{q}\,\overline{x} = \overline{1}$. Logo, $\overline{q}$ é uma unidade em $\mathbb{Z}/n\mathbb{Z}$.

(ii) Se $\overline{q}$ é uma unidade do anel $\mathbb{Z}/n\mathbb{Z}$, então $\overline{q}$ gera o grupo aditivo $\mathbb{Z}/n\mathbb{Z}$.
Se $\overline{q}$ uma unidade do anel $\mathbb{Z}/n\mathbb{Z}$ então existe um inteiro x tal que $\overline{q}\,\overline{x}=\overline{1}$. Daí, $\overline{a}\,\overline{q}\,\overline{x} = \overline{a}$ (no anel $\mathbb{Z}/n\mathbb{Z}$) onde $\overline{a}$ é um elemento arbitrário de $\mathbb{Z}/n\mathbb{Z}$, com $0 \leq a < n$. Segue-se $\overline{a} = \overline{a}\,\overline{x}\,\overline{q} = (ax)\overline{q}$ (no grupo aditivo $\mathbb{Z}/n\mathbb{Z}$). Logo $\overline{q}$ gera o grupo $\mathbb{Z}/n\mathbb{Z}$

(iii) Se $\overline{q}$ gera o grupo aditivo $\mathbb{Z}/n\mathbb{Z}$, então q é relativamente primo com n.

Se $\overline{q}$ gera o grupo aditivo $\mathbb{Z}/n\mathbb{Z}$, então existe um inteiro x tal que $x\overline{q}=\overline{1}$. Assim, $xq \equiv 1\,(mod\,n)$. Daí, existe um inteiro y tal que $xq-1 = yn \Rightarrow 1 = xq-yn$. Seja $d = mdc(q,n)$ então $d|q$ e $d|n$. Assim, $d|(xq-yn)$. Logo, $d|1$. Portanto, $mdc(q,n) = 1$.

Lema 2.2 *Sejam A um anel, $\mathfrak{a}$ e $\mathfrak{b}$ ideais de A tais que $\mathfrak{a}+\mathfrak{b} = A$. Então $\mathfrak{a}\cap\mathfrak{a} = \mathfrak{ab}$ e o homomorfismo canônico $\sigma : A \longrightarrow A/\mathfrak{a} \times A/\mathfrak{b}$ induz um isomorfismo $\theta : A/\mathfrak{ab} \longrightarrow A/\mathfrak{a} \times A/\mathfrak{b}$. Lembre-se que o homomorfismo σ leva cada $x \in A$ no par, constituído das classes de x módulo $\mathfrak{a}$ e das classes de x módulo $\mathfrak{b}$.*

Demonstração: Sabemos que, em geral $\mathfrak{ab} \subset \mathfrak{a}$ e $\mathfrak{ab} \subset \mathfrak{b}$, então $\mathfrak{ab} \subset \mathfrak{a}\cap\mathfrak{b}$. Seja

$x \in \mathfrak{a} \cap \mathfrak{b}$, como $\mathfrak{a} + \mathfrak{b} = A$, então existem elementos $x_1 \in \mathfrak{a}$ e $x_2 \in \mathfrak{b}$ tais que $x_1 + x_2 = 1_A$. Daí, $x = x_1x + x_2x = x_1x + xx_2$, pois A é comutativo. Como $x_1x \in \mathfrak{ab}$ e $xx_2 \in \mathfrak{ab}$ então $x_1x + xx_2 \in \mathfrak{ab}$. Logo, $x \in \mathfrak{ab}$ e assim, $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{ab}$. Portanto $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$.
Mostraremos agora que o homomorfismo σ induz o isomorfismo θ. De fato, $Ker\,\sigma = \{x \in A;\, \sigma(x) = 0_{A/\mathfrak{a}\times A/\mathfrak{b}}\}$. Se $x \in Ker(\sigma)$, temos $\sigma(x) = (x + \mathfrak{a}, x + \mathfrak{b}) = (0 + \mathfrak{a}, 0 + \mathfrak{b})$ o que implica isso, $x + \mathfrak{a} = 0 + \mathfrak{a}$ e $x + \mathfrak{b} = 0 + \mathfrak{b}$ e assim $x \in \mathfrak{a}$ e $x \in \mathfrak{b}$. Daí, $x \in \mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$. Logo, $Ker(\sigma) = \mathfrak{ab}$. Para provar que σ é sobrejetiva mostraremos que para todo par $(y + \mathfrak{a}, z + \mathfrak{b}) \in A/\mathfrak{a} \times A/\mathfrak{b}$ existe $x \in A$ tal que $(x + \mathfrak{a}, x + \mathfrak{b}) = (y + \mathfrak{a}, z + \mathfrak{b})$, ou seja, para cada par $(y, z) \in A$ existe um elemento $x \in A$ tal que $x + \mathfrak{a} = y + \mathfrak{a}$ e $x + \mathfrak{b} = z + \mathfrak{b}$. Considere $x_1 \in \mathfrak{a}$ e $x_2 \in \mathfrak{b}$ tal que $x_1 + x_2 = 1_A$ e tome $x = x_1z + x_2y$. Assim $x + \mathfrak{a} = (x_1z + x_2y) + \mathfrak{a} = x_2y + \mathfrak{a} = (1_A - x_1)y + \mathfrak{a}$, pois $x_1z \in \mathfrak{a}$ e $x_1 + x_2 = 1_A \Rightarrow x_2 = 1_A - x_1$. Logo, $x + \mathfrak{a} = (y - x_1y) + \mathfrak{a} = y + \mathfrak{a}$, isto,e $x \equiv y\,(mod\,\mathfrak{a})$. Temos também que $x + \mathfrak{b} = (x_1z + x_2y) + \mathfrak{b} = x_1z + \mathfrak{b} = (1_A - x_2)z + \mathfrak{b} = z - x_2z + \mathfrak{b} = z + \mathfrak{b}$, isto é $x \equiv z\,mod\,\mathfrak{b}$. Portanto, φ é sobrejetora. Logo pelo teorema dos isomorfismos de anéis temos que $A/Ker\sigma \cong A/\mathfrak{a} \times A/\mathfrak{b}$ ou seja, $A/\mathfrak{ab} \cong A/\mathfrak{a} \times A/\mathfrak{b}$. Portanto, σ induz o isomorfismo $\theta : A/\mathfrak{ab} \longrightarrow A/\mathfrak{a} \times A/\mathfrak{b}$

Lema 2.3 *Sejam A um anel e* $\{\mathfrak{a}_i\}_{1\leq i\leq r}$*, um conjunto finito de ideais de A tal que* $\mathfrak{a}_i + \mathfrak{a}_j = A$*,* $\forall i \neq j$*. Então existe um isomorfismo canônico de* $A/\mathfrak{a}_i...\mathfrak{a}_r$ *sobre* $\Pi_{i=1}^{r} A/\mathfrak{a}_i$*.*

Demonstração: Para o caso $r = 2$, fica provado pelo lema 2.2. Vamos usar indução em r. Ponha $\mathfrak{b} = \mathfrak{a}_2....\mathfrak{a}_r$. Mostraremos que $\mathfrak{a}_i + \mathfrak{b} = A$, para $i \geq 2$ temos $\mathfrak{a}_1 + \mathfrak{a}_i = A$, pois por hipótese de indução $\mathfrak{a}_i + \mathfrak{a}_j = A$, $\forall i \neq j$. Daí, existem elementos $x_i \in \mathfrak{a}_1$ e $y_i \in \mathfrak{a}_i$ tal que $x_i + y_i = 1_A$ e $1_A = \Pi_{i=2}^{r}(x_i + y_i) = c + y_2...y_r$, onde c é a soma dos termos, cada um dos quais contém ao menos x_i como fator. Temos que $c \in \mathfrak{a}_1$ e como $y_2...y_r \in \mathfrak{b}$ então $c + y_2...y_r \in \mathfrak{a}_1 + \mathfrak{b}$. Assim, $1_A \in \mathfrak{a}_i + \mathfrak{b}$ e daí $\mathfrak{a}_i + \mathfrak{b} = A$. Pelo lema 2.2, segue-se que $A/\mathfrak{a}_1\mathfrak{b}$ é isomorfo a $A/\mathfrak{a}_1 \times A/\mathfrak{b}$. Pela hipótese de indução, temos que $A/\mathfrak{b} = A/\mathfrak{a}_2.....\mathfrak{a}_r$ é isomorfo a $A/\mathfrak{a}_2 \times .... \times A/\mathfrak{a}_r$. Logo, $A/\mathfrak{a}_1.....\mathfrak{a}_r$ é isomorfo $A/\mathfrak{a}_1 \times .... \times A/\mathfrak{a}_r$.

Proposição 2.7 *Sejam n e n′ inteiros relativamente primos. Então o anel* $\mathbb{Z}/nn'\mathbb{Z}$ *é isomorfo ao anel produto* $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z}$

Demonstração: Como n e n' são inteiros relativamente primos, então existem inteiros x e y tais que $nx + n'x = 1$. Daí, como $nx + n'x \in n\mathbb{Z} + n'\mathbb{Z}$ temos que $1 \in n\mathbb{Z} + n'\mathbb{Z}$. Logo, $n\mathbb{Z} + n'\mathbb{Z} = \mathbb{Z}$ e portanto o resultado segue-se do lema 2.2

2.3 Módulos sobre anéis de ideais principais, raízes da unidade e corpos finitos

Definição: Um A-módulo M é um grupo (a operação é adição) provida da aplicação $A \times M \longrightarrow M$ tal que

$$a(x+y) = ax + ay$$

$$(a+b)x = ax + bx$$

$$a(bx) = (ab)x$$

$$1x = x$$

com $a, b \in A$ e $x, y \in M$

Definição: Sejam A uma anel comutativo e I um conjunto. Denotemos $A^{(I)}$ o conjuntos das sequência $(a_i)_{i\in I}$ indexada por I, de elementos de A tais que $a_i = 0$, exceto para um número finito de índices $i \in I$.

Definição: Um A-módulo M e dito ser A-módulo livre quando existe uma família $(a_i)_{i\in I}$ de elementos de M, satisfazendo as seguintes condições:
(a) A família $(a_i)_{i\in I}$ é linearmente independente:

(b) Todo elemento $a \in M$ é escrito como combinação linear de família $(a_i)_{i\in I}$

Observação: Uma família $(a_i)_{i\in I}$ satisfazendo as condições da definição acima é chamada uma base do A-módulo livre, onde o número de elementos da base é chamado de posto de M. Se I é um conjunto finito, dizemos que o A-módulo M é finitamente gerado ou do tipo finito.

Definição: Um A-módulo M é dito do tipo finito se contém um conjunto finito de geradores.

Teorema 2.2 *Sejam A um anel e M um A-módulo. As seguintes condições são equivalentes:*

(a) Toda família não vazia de submódulos de M contém um elemento um elemento maximal (com a relação de inclusão)
(b) Toda sequência crescente $(M_n)_{n\geq 0}$ (ainda com a relação de inclusão) de submódulo de M é estacionário, isto é, existe n_0 tal que que $M_n = M_{n_0}$, $\forall n \geq n_0$
(c) Todo submódulo de M do tipo finito.

Demonstração: Primeiro vamos mostrar que $(a) \Rightarrow (c)$. Seja E um submódulo de M e Φ a coleção consistindo de todos submódulos do tipo finito de E. Temos que Φ não é vazia, pois $0 \in \Phi$. Por (a), segue que Φ contém um elemento maximal F. Para $x \in E$, $F + Ax$ é um submódulo do tipo finito de E, pois Ax é um módulo gerado por x e F é um submódulo do tipo finito de E. Temos que $F + Ax$ é gerado pela união de $\{x\}$ e qualquer conjunto finito de geradores de F. Como $F \subset F + Ax$ e F é maximal, então $F = F + Ax$, $x \in F$, $E \subset F$ e assim $E = F$. Logo, E é do tipo finito.
Agora vamos mostrar que $(c) \Rightarrow (b)$. Seja $(M_n)_{n\geq 0}$ uma sequência de submódulos de M. Então $E = \cup_{n\geq 0} M_n$ é um submódulo de M. Por (c) este submódulo E contém um conjunto finito de geradores $\{x_1, ..., x_q\}$. Temos que, para todo i, existe um índice $n(i)$ tal que $x_i \in M_{n_i}$. Seja $n_0 = max(n_i)$. Então $x_i \in M_{n_0}$ $\forall\, i$ e assim $E \subset M_{n_0}$ e portanto $E = M_{n_0}$. Logo, a sequência $(M_n)_{n\geq 0}$ é estacionária a partir de n_0.
A equivalência de (a) em (b) é um caso particular do lema abaixo, para conjuntos parcialmente ordenados.

Lema 2.4 *Seja T um conjunto parcialmente ordenado. As seguintes afirmações são equivalentes:*
(a) Todo subconjunto não vazio de T contém um elemento maximal;

(b) Toda sequência crescente $(t_n)_{n\geq 0}$ de elementos de T é estacionária.

Demonstração: $(a) \Rightarrow (b)$ Por (a) temos que a sequência $(t_n)_{n\geq 0}$ contém um elemento maximal t_q. Como a sequência $(t_n)_{n\geq 0}$ é crescente, para $n \geq q$ temos $t_n \geq t_q$. Sendo t_q maximal, segue-se que $t_n = t_q$, $\forall n \geq q$. Logo, toda sequência $(t_n)_{n\geq 0}$ de elementos de T é estacionária.
$(b) \Rightarrow (a)$ Suponha que exista um subconjunto S de T que não contém um elemento maximal. Então para todo $x \in S$, o conjunto do elementos de S que são maiores do que x é não vazio. Daí, pelo axioma da escolha, existe uma aplicação $f : S \longrightarrow S$ tal que $f(x) > x$ $\forall x \in S$. Como S é não vazio, podemos escolher $t_0 \in S$ e definir por indução a sequência $(t_n)_{n\geq 0}$ da forma $t_{n+1} = f(t_n)$. Esta sequência é estritamente crescente e não estacionária, o que é uma contradição. Logo, todo subconjunto não vazio de T contém um elemento maximal.

Corolário 2.2 *Em um anel de ideais principais A toda família não vazia de ideais contém um elemento maximal.*

Demonstração: Se considerarmos A um módulo sobre si mesmo, seus submódulos são os seus ideais. Como todos os ideais são principais, eles são A-módulos gerados por único elemento e assim do tipo finito. Logo, o resultado segue-se pela implicação $(c) \Rightarrow (a)$ do Teorema 2.2.

Sejam A um domínio de integridade e K seu corpo de frações. Um A-módulo livre pode ser mergulhado em um espaço vetorial sobre K. Segue-se que o mesmo é verdade para qualquer submódulo M de um A-módulo livre.

Definição: A dimensão do subespaço gerado por M é chamado posto de M. Se M é livre e admite uma base possuindo n elementos, então o posto de M é n.

Teorema 2.3 *Seja A um anel de ideais principais, M um A-módulo livre de posto n, e M' um submódulo de M. Então:*
(a) M' é livre de posto q, com $0 \leq q \leq n$:

(b) Se $M' \neq 0$, então existem uma base $\{e_1, ..., e_n\}$ de M e elementos não nulos $a_1, ..., a_q \in A$, tal que $\{a_1e_1, ..., a_qe_q\}$ é uma base de M' e a_i/a_{i+1}, $1 \leq i \leq q-1$.

Veja a demonstração em [Pierre. S. 2008] Teorema 1 da pag.21

Observação: Os ideais Aa_i no Teorema 2.3 são chamados fatores invariantes de M' e M.

Corolário 2.3 *Sejam A um anel de ideais principais e E um A-módulo do tipo finito. Então, E é isomorfo ao produto $(A/\mathfrak{a}_1) \times .... \times (A/\mathfrak{a}_n)$ onde os $\mathfrak{a}_i's$ são ideais de A tais que $\mathfrak{a}_1 \supset ... \supset \mathfrak{a}_n$.*

Demonstração: Sendo E um A-módulo do tipo finito, considere $\{x_1, ..., x_n\}$ um conjunto finito de geradores de E. Sabemos que existe homomorfismo sobrejetivo $\sigma : A^n \longrightarrow E$ e então, $A^n/Ker\sigma$ é isomorfo a E. Temos, pelo Teorema 2.2, que existe uma base $\{e_1, ..., e_n\} \in A^n$, um inteiro $q \leq n$ e elementos não nulos tais $a_1, ...a_q \in A$ tais que $a_i|a_{i+1}$, $\forall i$, onde $1 \leq i \leq q-1$ e $\{a_1e_1, ..., a_qe_q\}$ é uma base de E. Ponhamos $\mathfrak{a}_\mathfrak{p} = 0$ para $q+1 \leq p \leq n$. Então, $A^n/Ker\sigma$ é isomorfo ao produto dos $Ae_i/A\mathfrak{a}_\mathfrak{i}e_i$, para $1 \leq i \leq n$. Temos ainda que $Ae_i|Aa_ie_i$ é isomorfo $A/A\mathfrak{a}_\mathfrak{i}$. Daí, $A^n/Ker\,\sigma$ é isomorfo ao produtos dos $A|Aa_i$. Pondo $\mathfrak{a}_\mathfrak{i} = Aa_i$, temos que $A^n/Ker\,\sigma$ é isomorfo ao produto dos $A/A\mathfrak{a}_\mathfrak{i}$. Logo, como $A^n/Ker\,\sigma$ é isomorfo a E, podemos concluir que E é isomorfo a $(A/\mathfrak{a}_1)\times....\times(A/\mathfrak{a}_n)$.

Definição: Dizemos que um módulo E sobre um domínio de integridade A é livre de torção se a relação $ax = 0$, com $a \in A$ e $x \in E$, implica $a = 0$ ou $x = 0$.

Corolário 2.4 *Sobre um anel de ideais principais A, todos módulo do tipo finito E, que é livre de torção, é livre.*

Demonstração: Temos pelo corolário 2.3, que E é isomorfo a $(A/\mathfrak{a}_1) \times .... \times (A/\mathfrak{a}_n)$.

Suprimindo os fatores que são nulos, podemos supor que $\mathfrak{a}_i \neq A\ \forall i$. Suponha que $\mathfrak{a}_1 \neq (0)$ e seja $a \in \mathfrak{a}_1$ diferente de zero e x_1 um elemento não nulo de $A|\mathfrak{a}_1$. Se $x = (x_1, 0, ..., 0) \in E$, então a $ax = 0$. Mas isto contraria a hipótese de E ser livre de torção. Logo, $\mathfrak{a}_1 = (0)$ e portanto $\mathfrak{a}_i = (0)$, $\forall i$, pois $\mathfrak{a}_i \subset \mathfrak{a}_1$. Daí, E é isomorfo a A^n e como A^n é livre, temos que E é livre.

Corolário 2.5 *Sobre um anel de ideais principais A, todo Módulo E do tipo finito é isomorfo a um produto finito de módulos $M_i's$, onde cada M_i é igual a A ou a um quociente A/A_{p^s}, com p primo.*

Demonstração: Usamos o corolário 2.3, decompomos cada fator A/Aa, onde $a \neq 0$. Pelo lema 2.3 temos que, se $a = up_1^{s_1}....p_n^{s_n}$ é fatoração de a como produto de potência de primos, então A/Aa, é isomorfo ao produto dos $Ap_i^{e_i}s$. Daí segue-se o resultado.

Corolário 2.6 *Seja G um grupo comutativo finito. Então existe $x \in G$, cuja ordem é o mínimo múltiplo comum das ordens dos elementos de G.*

Demonstração: Um grupo comutativo é um $\mathbb{Z}$-módulo (considerando a operação adição). Temos, pelo corolário 2.3 que G é isomorfo a $\mathbb{Z}/a_1\mathbb{Z} \times .... \times \mathbb{Z}/a_n\mathbb{Z}$, onde $a_1|a_2, ..., a_{n-1}|a_n$. Assim, temos $a_i \neq 0$, $\forall i$, caso contrario G seria infinito, Escrevemos y para a classe de resíduos de 1 em $\mathbb{Z}/a_n\mathbb{Z}$ e ponhamos $x = (0, ..., 0, y)$. Daí, a ordem de x é obviamente a_n. Assim, dado $z = (z_1, ..., z_n) \in G$, temos que $a_n z = 0$, pois a_i/a_n, $\forall i$. Logo, a_n é um múltiplo da ordem de z e portanto x é o elemento procurado.

Teorema 2.4 *Seja K um corpo.Todo subgrupo finito G do grupo multiplicativo K^* consiste de raízes da unidade e é cíclico.*

Demonstração: Temos pelo corolário 2.6, que existe um elemento $z \in G$, cuja ordem n é o mínimo múltiplo comum das ordens dos elementos de G. Logo, $y^n = 1$, $\forall y \in G$. Como um polinômio de grau n sobre um corpo tem no máximo n raízes no corpo, temos que G possui no máximo n elementos (estamos olhando o polinômio $y^n - 1$). Por outro lado, tendo z ordem n, temos que G contém os n elementos: $z, z^2, ..., z^n = 1$, os quais são todos distintos. Logo, G é constituído das n-ésimas da unidade e é cíclico gerado por z.

Observação: Seja K um corpo. Existe um homomorfismo de anéis $\sigma : \mathbb{Z} \longrightarrow K$ definido por $\sigma(n) = 1 + 1 + ... + 1$ n-vezes, para $n \geqslant 0$ e $\sigma(-n) = -\sigma(n)$. Se σ for injetiva, ela identifica $\mathbb{Z}$ com um subanel de K, então K também contém o corpo de frações $\mathbb{Q}$ de $\mathbb{Z}$. Neste caso dizemos que K tem característica zero. Se σ não é injetiva, o $Ker\,\sigma$ é um ideal de $\mathbb{Z}$, então $Ker\,\sigma = p\mathbb{Z}$, $p > 0$, pois todo ideal de $\mathbb{Z}$ é principal. Assim, $\mathbb{Z}/p\mathbb{Z}$ é identificado como subanel de K. Daí, $\mathbb{Z}/p\mathbb{Z}$ é um domínio de integridade (na verdade um corpo) e portanto p é número primo. Dizemos neste caso, que K é de característica p. Agora escrevemos F_p para designar $\mathbb{Z}/p\mathbb{Z}$. O subcorpo $\mathbb{Q}$ ou F_p, de K é o menor subcorpo de

K e é chamado o subcorpo primo de K. Temos que, para todo número primo p, existem corpos de característica p, ou seja F_p.

Proposição 2.8 *Se K é um corpo de característica $p \neq 0$, então $px = 0$, $\forall x \in K$ e $(x+y)^p = x^p + y^p$, $\forall x, y \in K$*

Demonstração: Como a característica de K é $p \neq 0$, então para todo $x \in K$, temos $px = (p1)x = 0x = 0$. Por outro lado, pela fórmula binominal, temos que:
$(x+y)^p = \Sigma_{j=0}^{n}\binom{p}{j}x^j y^{p-j} = \binom{p}{0}x^0 y^p + \Sigma_{j=1}^{p-j}\binom{p}{j}x^j y^{p-j} + \binom{p}{p}x^p y^0$,
isto é,

$$(x+y)^p = x^p + y^p + \Sigma_{j=1}^{p-j}\binom{p}{j}x^j y^{p-j}.$$

O coeficiente $\binom{p}{j}$ é um inteiro e o seu valor é $\dfrac{p!}{j!(p-j)!}$. Como o número primo p aparece no numerador, mas não no denominador, então $\binom{p}{j}$ é um múltiplo de p, $\forall\, 1 \leq j \leq p-1$. Logo $\binom{p}{j}x^j y^{p-j} = 0$, $\forall\, 1 \leq j \leq p-j$. Daí, $\Sigma_{j=1}^{p-1}\binom{p}{j}x^j y^{p-j} = 0$. Portanto $\forall x \in K$ $(x+y)^p = x^p + y^p$

Teorema 2.5 *Seja K um corpo finito. Se $q = card(K)$, então:*

(a) A característica de K é um primo p, K é um espaço vetorial de dimensão finita s sobre F_p e $q = p^s$;

(b) O grupo multiplicativo K^* é cíclico de ordem $q-1$;

(c) $x^{q-1} = 1$, $\forall\, x \in K^*$ e $x^q = x$, $\forall\, x \in K$

Demonstração: (a) Como $\mathbb{Z}$ é infinito e K é finito, então $\varphi : \mathbb{Z} \longrightarrow K$ não é injetiva. Daí, K não pode ter característica zero. Logo, K contém F_p, com p primo e sua característica é p. Temos que, K é um espaço vetorial sobre F_p, cuja dimensão s deve ser finita, pois caso contrário, K seria um corpo infinito. Seja $\{e_1, ..., e_s\}$ uma base de K sobre F_p. Assim, qualquer $x \in K$ pode ser escrito de maneira única como $x = x_1e_1 + ... + x_se_s$, onde $x_i \in F_p$, com $i = 1, ..., s$. Cada x_i na expressão pode ser escolhido de p maneiras, pois o número de elementos de F_p é igual a p. Logo, o número de elementos de K é p^s e daí teremos $q = p^s$ como queríamos.

(b) O resultado segue-se diretamente do Teorema 2.4.

(c) Como a ordem de K^* é $q-1$ pelo item (b), então temos $x^{q-1} = 1$, $\forall\, x \in K^*$ e $x^q = x$, $\forall\, x \in K$.

Observação: (a) e (c) implicam que um corpo finito K com q elementos é o conjunto de raízes do polinômio $P(x) = x^q - x$, que possui exatamente q raízes. Escrevemos F_q para um corpo com q elementos, pois dois corpos finitos com q elementos são isomorfos

Teorema 2.6 *(Chevalley) Sejam K um corpo finito e $F(X_1, ..., X_n)$ um polinômio homogêneo de grau d sobre K ("lembrando que, um polinômio é dito homogêneo de grau d, quando todos seus monômios tem grau d"). Suponha $d < n$, então existe um ponto $(x_1, ..., x_n) \in K^n$ diferente da origem tal que $F(x_1, ..., x_n) = 0$.*

Demonstração: Considere $q = card(K)$ e p a característica de K, então $q = p^s$, pelo Teorema 2.5. Seja $V \subset K^n$ o conjunto dos zeros de F, isto é, o conjunto dos pontos $(x_1, ..., x_n) \in K^n$ tais que $F(x_1, ..., x_n) = 0$ Temos, pelo Teorema 2.5, que $F(x)^{q-1} = 1$, $\forall x \in K^n - V$. Assim, o polinômio $G(x) = F(x)^{q-1} = 1$, $\forall x \in K^n - V$ com valores em F_p. O número módulo p de pontos de $K^n - V$ será então dado pela soma $\Sigma_{x \in K^n} G(x)$.

Vamos agora calcular esta soma e mostrar que ela vale zero módulo p, isto é, $\Sigma_{x \in K^n} G(x) \equiv 0 \, mod \, p$. Se isso ocorrer, então teremos que a $card(K^n - V)$ é um múltiplo de p. Como $card(K^n) = q^n = (p^s)^n = p^{ns}$ é também um múltiplo de p, então a $card(V)$ é também um múltiplo de p. Temos que V já contém a origem, então, necessariamente V contém outros pontos, pois $p \geq 2$. Para provar esse teorema é suficiente mostrar que $\Sigma_{x \in K^n} G(x) = 0 \in F_p$. Para calcular $\Sigma_{x \in K^n} G(x)$, observe que o polinômio G é uma combinação linear dos monômios $M_\alpha(x) = x_1^{\alpha_1} ... x_n^{\alpha_n}$. Para determinar $\Sigma_{x \in K^n} G(x)$ é suficiente calcular

$$\Sigma_{x \in K^n} M_\alpha(x) = \Sigma_{x \in K^n} x_1^{\alpha_1} ... x_n^{\alpha_n} = (\Sigma_{x_1 \in K^n} x_1^{\alpha_1}) ... (\Sigma_{x_n \in K^n} x_n^{\alpha_n})$$

Daí, o problema reduz-se ao cálculo de somas da forma $\Sigma_{y \in K} y^\beta$, com $\beta \in \mathbb{N}$

I) Para $\beta = 0$ temos $y^\beta = 1, \forall y \in K$, consequentemente, $\Sigma_{y \in K} y^\beta = \Sigma_{y \in K} 1 = q \equiv 0 \, mod \, p$.

II) Para $\beta > 0$, o termo 0^β é o zero, assim a soma reduz a $\Sigma_{y \in K^*} y^\beta$. Como K^* é um grupo cíclico de ordem $q - 1$, pelo item (b) teorema 2.5. Seja w gerador de K^*. Daí $\Sigma_{y \in K^*} y^\beta = \Sigma_{j=0}^{q-2} w^{\beta_j}$, que é a soma de uma progressão geométrica

Assim, consideremos dois casos:

III) Se $w^\beta \neq 1$, isto é, se β não é múltiplo de $q - 1$, então $\Sigma_{j=0}^{q-2} w^{\beta_j} = \dfrac{w^{\beta(q-1)} - 1}{w^\beta - 1} = 0$, pois $w^{q-1} = 1$

IV) Se $w^\beta = 1$, isto é, se β é um múltiplo de $q - 1$. Então,

$$\Sigma_{j=0}^{q-2} 1 = q - 1$$

Segue por I), III) e IV) que $\Sigma_{x \in K^n} x_1^{\alpha_1} ... x_n^{\alpha_n}$ se anula, a menos que todos os $\alpha_i's$ sejam não nulo e múltiplos de $q - 1$. Neste caso, o grau $\alpha_1 + ... + \alpha_n$ do monômio é no mínimo

$(q-1)n$. Mas, como $G = F^{q-1}$, G possui grau $(q-1)d$ e $(q-1)d < (q-1)n$, pois, por hipótese $d < n$. Portanto, $\Sigma_{x \in K^n} M_\alpha(x) = 0$, para todo monômio $M_\alpha(x)$ que aparece em G com coeficientes não nulos. Logo, $\Sigma_{x \in K^n} G(x) = 0$.

2.4 Elementos inteiros sobre anéis e algébricos sobre um corpo

Definição: Os números complexos x que satisfazem uma equação da forma $x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 = 0$, onde os coeficientes são racionais, são chamados números algébricos. Quando os coeficientes são inteiro o número algébrico x chama-se inteiro algébrico.

2.4.1 *Elementos inteiros sobre um anel*

Teorema 2.7 *Sejam R um anel, A um subanel de R e x um elemento de R. As seguintes condições são equivalentes:*
(a) Existem $a_0, ..., a_{n-1} \in A$ tal que $x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 = 0$, isto é, x é a raiz de um polinômio mônico com coeficientes em A;
(b) O anel $A[x]$ é um A-Módulo do tipo finito;
(c) Existe um subanel de B de R que contém A, e x o qual é um A-módulo do tipo finito.

Demonstração: Primeiro vamos mostrar que $(a) \Rightarrow (b)$. Temos por hipótese que existem $a_0, ..., a_{n-1} \in A$ tal que:

$$x^n + a_{n-1}x^{n-1} + ... + a_1 + a_0 = 0$$

Seja M o A-submódulo de R gerado por $1, x, ..., x^{n-1}$. Por (a) $x^n \in M$. Daí, multiplicando a equação acima por x^j, obtemos:

$$x^{n+j} = -a_{n-1}x^{n+j-1} - ... - a_1 x^{j+1} - a_0 x^j$$

fazendo indução sobre j, temos que $x^{n+j} \in M$, $\forall j \geqslant 0$. Como $A[x]$ é um A-módulo gerado por x^k, com $k \geqslant 0$, temos que $A[x] = M$. Sendo M um A-módulo do tipo finito temos $A[x]$ é um A-módulo do tipo finito.
$(b) \Rightarrow (c)$ Temos por hipótese que o anel $A[x]$ é um A-modulo do tipo finito. Daí, basta tomar $B = A[x]$. Logo existe um subanel de B de R que contém A e x, o qual é um A-módulo do tipo finito.
$(c) \Rightarrow (a)$ Temos por hipótese, que existe um subanel B de R que contém A e x, o qual é um A-módulo do tipo finito. Daí, B possui um conjunto de geradores. Seja $\{y_1, ...y_n\}$ um conjunto finito de geradores para B como um módulo sobre A, isto é,

$$B = Ay_1 + ... + Ay_n$$

Assim, como $x \in B$ e sendo B um subanel de R, segue-se que $xy_i \in B \; \forall i = 1, ..., n$. Logo, $xy_i = \Sigma_{j=1}^{n} a_{ij} y_j$, para qualquer $i = 1, ..., n$ e $a_{ij} \in A$, com $1 \leq i, \; j \leq n$. Isto significa que $\Sigma_{j=1}^{n} (\delta_{ij} x - a_{ij}) y_j = 0$, com $i = 1, ..., n$, onde $\delta_{ij} = 0$ se $i \neq j$ e $\delta_{ij} = 1$ se $i = j$. Considere o sistema de n equações em $\{y_1, ..., y_n\}$. Seja d o determinante $det(\delta_{ij} x - a_{ij})$. Fazendo o calculo e usando regra de Cramer, obtemos $dy_i = 0$, $\forall i = 1, ..., n$. Daí, $db = 0 \; \forall \, b \in B$ e, em particular $d.1 = d = 0$. Mas d é um polinômio mônico em x, pois o termo de ordem superior aparece na expansão do produto $\Pi_{i=1}^{n} (x - a_{ii})$, dos termos da diagonal principal. Daí, como $d = 0$, obtemos o que queríamos.

Definição: Sejam R um anel e A um subanel de R. Um elemento x de R é dito inteiro sobre A se satisfaz as condições de equivalente do Teorema 2.7. Seja $p \in A[X]$ um polinômio mônico tal que $p(x) = 0$, esta relação é chamada uma equação de dependência integral de x sobre A.

Exemplo O elemento $x = \sqrt{2}$ de R é um inteiro sobre $\mathbb{Z}$. A relação $x^2 - 2 = 0$ é uma equação de dependência inteira.

Proposição 2.9 *Sejam R um anel, A um subanel de R e $\{x_1, ..., x_n\}$ um conjunto finito de elementos de R. Se para todo i, x_i é um inteiro sobre $A[x_1, ..., x_{i-1}]$, em particular se todos os $x_i's$ são inteiros sobre A, então $A[x_1, ..., x_n]$ é um A-módulo do tipo finito.*

Demonstração: Usaremos indução sobre n. Para $n = 1$ temos pelo item (b) do Teorema 2.7, que $A[x_1]$ é um A-módulo do tipo finito. Assumiremos que $B = A[x_1, ..., x_{n-1}]$ é um A-módulo do tipo finito. Então, $B = \Sigma_{j=1}^{p} A b_j$. Temos que, o caso $n = 1$, implica que $A[x_1, ..., x_{n-1}] = B[x_n]$ é um B-módulo do tipo finito. Daí, escrevemos $B[x_n] = \Sigma_{k=1}^{q} B c_k$. Então $A[x_1, ..., x_n] = \Sigma_{k=1}^{q} (\Sigma_{j=1}^{p} A b_j) c_k = \Sigma_{k,j}^{q,p} A b_j c_k$. Assim $\{b_1 c_1, ..., b_p c_q\}$, é um conjunto finito de geradores para $A[x_1, ..., x_n]$, como um módulo sobre A. Logo, $A[x_1, ..., x_n]$ é um A-módulo do tipo finito.

Corolário 2.7 *Sejam R um anel, A um subanel de R, x e y elementos de R, os quais são inteiros sobre A, então $x + y$, $x - y$, xy são inteiros sobre A.*

Demonstração: Como $x + y$, $x - y$, xy pertence a $A[x, y]$, pela proposição 2.8, $A[x, y]$ é um A-módulo do tipo finito. Daí pelo item (c) do Teorema 2.4., temos que $x + y$, $x - y$, xy são inteiro sobre A.

Corolário 2.8 *Sejam R um anel e A um subanel de R. O conjunto A' de elementos de R os quais são inteiros sobre A é um subanel de R que contém A.*

Demonstração: Pelo corolário 2.4. A' é um subanel de R. Temos que $A \subset A'$, pois $a \in A$, é raiz do polinômio mônico $p(x) = x - a$ com coeficientes em A. Então a é inteiro

sobre A, isto é, $a \in A'$

Definição: Sejam R um anel, A um subanel de R, o anel A' de elementos de R os quais são inteiros sobre A é chamado o fecho inteiro de A em R. Seja A um domínio de integridade e K seu corpo de frações. O fecho integral de A em K é chamado fecho integral de A. Seja B um anel e A um subanel de B. Dizemos que B é inteiro sobre A, se todo elemento de B é inteiro sobre A, isto é, se o fecho inteiro de A em B é o próprio B.

Proposição 2.10 *Seja C um anel, B um subanel de C e A um subanel de B. Se B é inteiro sobre A e se C é inteiro sobre B. Então, C é inteiro sobre A.*

Demonstração Dado $x \in C$, como C é inteiro sobre B, temos que x é inteiro sobre B, daí existe uma equação dependência integral $x^n + b_{n-1}x^{n-1} + ... + b_0 = 0$. Com os $b_i \in B$, onde $i = 0, ..., n-1$. Ponha $B' = A[b_0, ..., b_{n-1}]$, então x é inteiro sobre B'. Como B é inteiro sobre A, os $b_i's$ são inteiro sobre A. Daí, pela proposição 2.9, temos que $B'[x] = A[b_0, ...b_{n-1}, x]$ é um A-módulo do tipo finito. Assim pelo item (c) teorema 2.7, x é um inteiro sobre A. Logo, C é inteiro sobre A.

Proposição 2.11 *Sejam B um domínio de integridade e A um subanel de B tal que B é inteiro sobre A. Para que B seja um corpo é necessário e suficiente que A seja um corpo.*

Demonstração: Suponha que A seja um corpo e considere $x \in B$ um elemento não nulo. Como x é um inteiro sobre A, então o anel $A[x]$ é um A-módulo finitamente gerado, o que acarreta que $A[x]$ é um espaço vetorial de dimensão finita sobre A. Considere $T : A[x] \longrightarrow A[x]$ a transformação linear dada por $T(y) = xy$, para todo $y \in A[x]$. Esta transformação é injetiva, pois, para quaisquer $y, z \in A[x]$

$$T(y) = T(x) \Rightarrow xy = xz \Rightarrow x(y-z) = 0 \Rightarrow y - z = 0 \Rightarrow y = z$$

já que B é um domínio de integridade e $x \neq 0$. Portanto, T é bijetora. Logo, existe $y \in A[x]$ tal que que $xy = 1$, ou seja, x é invertível. Portanto, B é um corpo.

Reciprocamente, suponha que B seja um corpo. Dado $a \in A - (0)$ temos que a possui um inverso multiplicativo $a^{-1} \in B$, como B é inteiro sobre A, então existem $b_0, b_1, ..., b_{n-1} \in A$ tais que $a^{-n} + b_{n-1}a^{-n+1} + ... + b_1a^{-1} + b_0 = 0$.
Multiplicando a equação anterior por a^{n-1}, temos $a^{-1} = -(b_{n-1} + ... + b_1a^{n-2} + b_0a^{n-1}) \in A$. Portanto, existe $a^{-1} \in A$ tal que $aa^{-1} = 1$ para todo $a \neq 0$ em A. Logo, A é um corpo.

Definição: Um anel A é dito integralmente fechado se for um domínio de integridade e se for seu próprio fecho integral. Em outras palavras, todo elemento x do corpo de frações K de A, que é inteiro sobre A, pertence a A.

Exemplo 1 Sejam A um domínio de integridade e K seu corpo de frações. Então o fecho integral A' de A, isto é, o fecho integral de A em K, é integralmente fechado. (Veja em Pierre Samuel, 2008)

Exemplo 2 Todo anel de ideais principais é integralmente fechado. De fato, por definição um anel de ideais principais é um domínio de integridade. Seja x um elemento do corpo de frações K de A, que é inteiro sobre A. Seja $x^n + a_{n-1}x^{-n+1} + ... + a_1x + a_0 = 0$, com $a_i \in A$, uma equação dependência integral sobre A. Escreva $x = \frac{a}{b}$, com $a, b \in A$ e o $mdc(a, b) = 1$. Substituindo $\frac{b}{a}$ na equação de dependência inteira e multiplicando por b^n, obtemos $a^n + b(a_{n-1}a^{n-1} + ... + a_1b^{n-2} + a_0b^{n-1}) = 0$. Assim, $b|a^n$ com $mdc(a, b) = 1$. Logo pelo o lema de Euclides temos que $b|a$. Portanto, b é uma unidade de A. Daí, $x = \frac{a}{b}$ é um elemento de A. Logo, A, é integralmente fechado.

Observação: Como usamos apenas as propriedades multiplicativas do anel de ideais principais, o mesmo argumento pode ser usado para mostrar que todo anel fatorial é integralmente fechado.

2.4.2 *Elementos algébricos sobre um corpo*

Definição: Sejam R um anel e K um subanel de R. Um elemento $x \in R$ é chamado algébrico sobre K se existirem $a_0, ..., a_n \in K$ nem todos nulos tal que

$$a_nx^n + ... + a_1x + a_0 = 0 \qquad (1).$$

Equivalentemente, os monômios $(x^j)_{j\in\mathbb{N}}$ são linearmente dependente sobre K. Um elemento de R que não é algébrico sobre K, é chamado transedental sobre K, isto é, x é transedental sobre K se e somente se, os monômios $(x^j)_{j\in\mathbb{N}}$, são linearmente independentes sobre K.

Observação Na definição anterior, podemos assumir $a_n \neq 0$. Neste caso, $a_n^{-1} \in K$ multiplicando a equação (1) por a_n^{-1}, obtemos uma equação de dependência integral. Portanto, sobre corpo, algébrico equivale a inteiro. Se $K \subset R$ e $x \in R$ temos que,pelo Teorema 2.7, x é algébrico sobre K se e somente se $[K[x] : K]$ é finito.

Definição: Dizemos que um anel R, contendo K, é algébrico sobre K, se todo elemento de R é algébrico sobre K. Se R é um corpo, então R é chamado uma extensão algébrico de K.

Definição: Dado um corpo L e um subcorpo K de L, chamamos a dimensão $[L : K]$, o grau de L sobre K. Toda extensão de grau finito de $\mathbb{Q}$ é chamado um corpo numérico algébrico (ou simplesmente um corpo numérico).

Observação: Pelo item (c) do Teorema 2.7. temos que, se o grau de L sobre K é finito, então L é uma extensão algébrica de L.

Proposição 2.12 *Sejam K um corpo, L uma extensão algébrica de K e M uma extensão algébrica de L. Então M é uma extensão algébrica de K. Além disso*

$$[M : K] = [M : L][L : K]$$

Demonstração: Pela proposição 2.10., segue-se que M é uma extensão de K. Resta mostrar que $[M : K] = [M : L][L : K]$. Seja $\{x_i\}_{i\in I}$ uma base de L sobre K e $\{y_j\}_{j\in J}$ uma base de M sobre L. Vamos mostrar que $\{x_iy_j\}_{(i,j)\in I\times J}$ é uma base de M sobre K. Da demonstração da preposição 2.9, vemos que $\{x_iy_j\}_{(i,j)\in I\times J}$ gera M sobre K. A relação $\Sigma a_{ij}x_iy_j = 0$ com $a_{ij} \in K$, implica $\Sigma(\Sigma a_{ij}x_j)y_j = 0$. Como $\{y_j\}_{j\in J}$ é $L.I$, pois $\{y_j\}_{j\in J}$ é uma base de L sobre K, $\Sigma(\Sigma a_{ij}x_j)y_j = 0$. Como $\{x_i\}_{i\in I}$ é $L.I$, pois $\{x_i\}_{i\in I}$ é uma base de L sobre K, temos que $a_{ij} = 0$. Assim $\{x_iy_j\}_{(i,j)\in I\times J}$ é $L.I$ sobre K. Portanto, $[M : K] = [M : L][L : K]$

Proposição 2.13 *Sejam R um anel e K um subanel de R. Então:*
(a) O conjunto K' de elementos de R, algébrico sobre K, é um subanel de R contendo K;
(b) Se R é um domínio de integridade, então K' é um subcorpo de R.

Demonstração: (a) Como K é um subcorpo de R, então os elementos de R que são algébrico sobre K são elementos inteiros sobre K. Logo, pelo corolário 2.8., o conjunto formados pelos elementos de R, que são inteiros sobre K, é um subanel de R que contém K.
(b) Como R é um domínio de integridade e $K' \subset R$, então K é um domínio de integridade. Além disso, K é um subanel de K' e K' é algébrico sobre K. Assim pela proposição 2.8 temos que K' é um corpo se e somente se K é um corpo. Como K é um subcorpo de R, então K' é um subcorpo de R.

Seja R um anel e K um subanel de R e x um elemento de R. Existe um único homomorfismo $\varphi : K[X] \longrightarrow R$ tal que $\varphi(X) = x$ e $\varphi(a) = a \ \forall\, a \in K$. A imagem de φ é $K[x]$.

Afirmamos que x é algébrico sobre K se, e somente se, $Ker(\varphi) \neq 0$.
De fato, se x é transcendente sobre K, temos $Ker(\varphi) = (0)$, se x é algébrico sobre K então existe $f(X) \in K[X]$, $f(X)$ não nulo, tal que $f(x) = 0$ e assim $\varphi(f(X)) = 0$, o que implica de $Ker\,\varphi \neq 0$.

Com as mesma notações anterior o $Ker\,\varphi$ é um ideal principal (desde que $K[X]$ é um anel principal) gerado por f, isto é, $Ker\,\varphi = (f(X))$. Nos podemos supor

que f é mônico, desde que K é um corpo. Assim f é unicamente determinado por K e x e é chamado de polinômio minimal de x sobre K.

Se $g(X) \in K[X]$ então $g(x) = 0$ se, e somente se, $f(X)$ divide $g(X)$ em $K[X]$.

Como $Ker\,\varphi = (f(X))$ e a imagem de φ é $K[x]$ temos $K[X]/\langle f(X)\rangle \simeq K[x]$.

Temos ainda que $K[x]$ é um subcorpo $\Leftrightarrow$ $K[x]$ é um domínio de integridade $\Leftrightarrow$ $f(X)$ é irredutível.

Proposição 2.14 *Sejam K um corpo e $P(X) \in K[X]$ um polinômio não constante. Então existe uma extensão algébrica K' de K de grau finito tal que $P(X)$ fatora $K'[X]$ em um produto de polinômio de grau 1 (polinômios lineares)*

Demostração: Usaremos indução sobre o grau d de $P(X)$. Se $d = 1$, o resultado segue, pois $P(X)$ é um polinômio de grau 1. Seja $F(X)$ um fator irredutível de $P(X)$. Temos que existe uma extensão K'' de grau finito sobre K (isto é, $K[x]$) contendo um elemento x tal que $X - x$ divide $F(X)$ em $K''[X]$. Portanto, $P(X) = (X - x)P_1(X)$ com $P_1(X) \in K''[X]$. Como $P(X)$ tem grau $d - 1$, então pela hipótese de indução sobre $P_1(X)$ fatora em produto de polinômio lineares em uma extensão de K' de grau finito K''. Pela proposição 2.9 K' e de grau finito sobre K. Logo, $P(X) = (X - x)P_2(X)$ onde $P_2(X)$ é a fatoração de $P_1(X)$ em produto de polinômio lineares em uma extensão K' de K.

Definição (Corpos algebricamente Fechados) Um corpo K é chamado algebricamente fechado se todo polinômio não constante $P(X) \in K[X]$ pode ser expresso como um produto de fatores lineares, todos em $K[X]$.

2.5 Elementos conjugados, corpos conjugados

Definição 2.2 *Dados dois corpos L e L' ambos contendo um corpo K, chamamos todo isomorfismo $\varphi : L \longmapsto L'$ tal que $\varphi(a) = a$ para todo $a \in K$ um K-isomorfismo de L em L'. Nesse caso, dizemos que L e L' são K-isomorfo e se são algébricos sobre K, dizemos que eles são conjugados sobre K.*

Definição 2.3 *Dados duas extensões L e L' de K, dizemos que dois elementos $x \in L$ e $x' \in L'$ são conjugados sobre K se existe um K-isomorfismo, $\varphi : K(x) \longmapsto K(x')$ tal que $\varphi(x) = x'$. Tal que φ é única*

Observação A Existência de φ significa que x e x' são ambos transcendentais sobre K ou são ambos algébricos sobre K, com o mesmo polinômio minimal.

Exemplo Sejam $F(X)$ um polinômio irredutível de grau n sobre K e $x_1, ..., x_n$ suas raízes

na extensão K' de K. Então os $x_i's$ são dois a dois conjugados sobre K.

Lema 2.5 *Sejam K um corpo de característica zero ou um corpo finito e $F(X) \in K[X]$ um polinômio mônico irredutível. Considere $F(X) = \prod_{I=1}^{n}(X - x_i)$ sua decomposição em produto de fatores lineares na extensão K' de K. Então as n raízes $x_1, ..., x_n$ de $F(X)$ são distintas.*

Demonstração: Suponha por absurdo, que as n raízes de $F(X)$ não são todas distintas, assim. $F(X)$ possui uma raiz múltipla. Daí, $F(X)$ possui uma raiz comum com a sua derivada $F'(X)$, pois, se a é uma raiz múltipla de $F(X)$ tem multiplicidade k então $F(X) = (X - a)^k G(X)$ e daí $F'(X) = K(X - a)^{k-1}G(X) + (x - a)^k G'(X)$. Logo, a é também raiz de $F'(X)$ de multiplicidade pelo menos $k - 1$ se $k > 1$. Logo $F(X)$ divide $F'(X)$. Como o grau de F' é menor e igual que o grau de F e F divide F' então $F'(x)$ é o polinômio zero. Daí, $F'(X) = nX^{n-1} + (n-1)a_{n-1}X^{n-2} + ... + a_1 = 0$. Isto significa que $n.1 = 0$ e $j.a_j = 0$ para todo $j = 1, ..., n - 1$. Mais isso não pode ocorrer em um corpo K de característica zero. Se K tem característica $p \neq 0$, então a relação $n.1 = 0$ e $j.a_i = 0$ para $j = 1, ..., n - 1$, significa que p divide n e que $a_j = 0$, $\forall j$ que não é múltiplo de p. Logo, F(X) é da forma:

$$F(X) = X^{qp} + b_{q-1}X^{(q-1)p} + ... + b_1X^p + b_0$$

com $b_i \in K$, pois os termos a_j que não são zero, são os termos que j é da forma: $qp - p$, $qp - 2p$,...,$qp - qp$. Se cada um dos $b_i's$ é uma p-ésima potência, isto é, $b_i = c_i^p$ com $c_i \in K$ então $F(X) = (X^q + C_{q-1}X^{q-1} + ... + C_0)^p$ pela proposição 2.13. Logo $F(X)$ não é irredutível o que é absurdo. Podemos supor sempre os b_is são p-ésima potência, pois se K é um corpo finito de característica $p \neq 0$, então a aplicação $f : K \longmapsto K$, dada por $f(x) = x^p$ é injetiva, pois $x^p = y^p \Rightarrow x^p - y^p = 0 \Rightarrow (x - y)^p = 0 \Rightarrow x - y = 0 \Rightarrow x = y$. Como K é finito e f e injetiva, então f é sobrejetora. Assim, para todo $y \in K$ existe um $x \in K$ tal que $f(x) = y$, ou seja, $x^p = y$. Portanto $F(X)$ não é irredutível, o que é uma contradição.

Observação: Os corpos K de característica $p \neq 0$ para os quais $x \longmapsto x^p$ é sobrejetiva (isto é, para os quais todo elemento de K é p-ésima potência) são chamada corpos perfeitos. Pelo que vimos anteriormente, os corpos finitos são perfeitos. Por convenção, corpos de característica zero são também considerados perfeitos. O lema 2.5 é verdadeiro para corpos perfeitos.

Teorema 2.8 *Seja K um corpo de característica zero ou um corpo finito. Considere K' uma extensão de K de grau finito n e B um corpo algebricamente fechado contendo K. Então existe n K-isomorfismo distintos de K' em B.*

Demonstração: Se o corpo K' é da forma $K' = K[x]$, com $x \in K'$, então o polinômio minimal $F(X)$ de x sobre K é de grau n. Ele possui n raízes $x_1, ..., x_n \in \mathbb{C}$ todas distintas, pelo lema 2.5. Pelo o exemplo acima os $x_i's$ são dois a dois conjugados sobre K e daí para cada $i = 1, ..., n$ temos um K-isomorfismo, $\sigma_i : K[X] \longmapsto B$ tal que $\sigma_i(x) = x_i$. Neste caso o teorema fica provado. Continuaremos por indução sobre o grau n de K'. Seja $x \in K'$ e considere os corpos $K \subset K[x] \subset K'$ e ponha $q = [K[x] : K]$. Podemos assumir $q > 1$, pois $K \neq K[x]$ pelo que vimos anteriormente, existem q K-isomorfismo distintos $\sigma_1, ..., \sigma_n$ de $K[x]$ em B. Como $K[x_i] = K[\sigma_i(x)]$ e $K[x]$ são isomorfos, pois x e x_i são conjugados e $K[x] \subset K'$, então é possível construir uma extensão K_i' de $K[\sigma_i(x)]$ e um isomorfismo $\tau : K' \longmapsto K_i'$ que estende σ_i (este resultado encontra-se em [Endler 2007]). Temos que $K[\sigma_i(x)]$ é um corpo de característica zero ou corpo finito, pois $K[\sigma_i(x)]$ é uma extensão finita de k e K é de característica zero ou corpo finito. Como $[K_i : K[\sigma_i(x)]] = [K' : K[x]] = \dfrac{n}{q} < n$, pois $K_i' \simeq K'$ e $K[\sigma_i(x)] \simeq K[x]$, então pela hipótese de indução temos que existem $\dfrac{n}{q}$ $K[\sigma_i(x)]$-isomorfismo distintos v_{ij} de K_i' em B (estamos supondo que teorema é válido para o caso em que $[K' : K] = h < n$), que é a hipótese de indução. Neste caso estamos considerando no teorema $K' = K_i'$ e $K = K[\sigma_i(x)]$. Logo, as n aplicações composta $v_{ij} \circ \tau_i$ resulta $q\dfrac{n}{q} = n$ K-isomorfismo de K' em B. Eles são distintos, pois $i \neq i'$ temos que $v_{ij} \circ \tau_i$ e $v_{i'j'}\tau_i'$ diferem em $K[x]$ e para $i = i'$, mas $j \neq j'$ temos que v_{ij} e $v_{ij'}$ diferem em K_i'. Portanto o teorema está provado.

Definição: Seja K um corpo e $L \supseteq K$ uma extensão de corpos. Dizemos que $x \in L$ é um elemento primitivo de L, se $L = K[x]$. Neste caso, dizemos que L é uma extensão simples.

Corolário 2.9 *(Teorema do elemento primitivo) Seja K corpo finito ou um corpo de característica zero. Seja K' uma extensão de grau finito n. Então, existe um elemento x de K' tal que $K' = K[x]$*

Demonstração: Se K é finito, então K' é finito, pois K' é uma extensão finita de K e seu grupo multiplicativo K'^* é formado de potência de um elemento x, pelo item (b) do Teorema 2.5. Logo, $K' = K[x]$. Suponha que K é de característica zero e assim K é um corpo infinito. Pelo Teorema 2.8 existem n K-isomorfismo distintos σ_i de K' em um corpo algebricamente fechado C, contendo K. Para $i \neq j$, a equação $\sigma_i(y) = \sigma_j(y)$, com $y \in K'$, define um subconjunto V_{ij} de K' que é um K-subespaço do espaço vetorial K'. De fato, sejam $y, y' \in V_{ij}$ e $k \in K$, então para $i \neq j$ temos que que $\sigma_i(y) = \sigma_j(y)$ e $\sigma_i(y') = \sigma_j(y')$. Daí, $\sigma_i(y + y') = \sigma_i(y) + \sigma_i(y') = \sigma_j(y) + \sigma_j(y') = \sigma_j(y + y')$ e ainda $\sigma_j(ky'') = \sigma_i(k)\sigma_i(y') = k\sigma_j(y') = \sigma_j(y') = \sigma_i(k)\sigma_j(y')$. Logo $y - y' \in V_{ij}$ e $ky' \in V_{ij}$ Assim, V_{ij} é um subespaço vetorial de K', diferente de K' quando $\sigma_i \neq \sigma_j$. Na verdade temos que a união dos v_{ij} está estritamente contido em K'. Tome x fora dessa união, então os $\sigma_i(x)$ são dois a dois distintos. Logo, o polinômio mínimo $P(X)$ de x sobre K possui

no mínimo n raízes que são os $\sigma_i(x)$ em C. Assim, $grau\, P \geqslant n$ ou seja, $[K[x] : K] \geqslant n$. Como $K[x] \subset K'$ e $[K' : K] = n$, portanto $[K[x] : K] = 1$. Logo, $K' = K[x]$.

Lema 2.6 *Seja A um domínio de integralmente fechado, K seu corpo de fração e L uma extensão algébrica de K. Se B é o fecho inteiro de A em L então $B \cap K = A$.*
Demonstração: Seja $x \in L$ um inteiro sobre A e seja $F(X) \in K[x]$ o polinômio minimal de x sobre K. Seja L' o corpo de raízes de F sobre K, isto é, o corpo gerado sobre K pelas raízes de F. Seja A' o fecho inteiro de A em L' então $A' \cap K = K$ pois $A' \cap K$ é inteiro sobre A . Daí, o lema segue do fato de A é integralmente fechado, isto é $B = A'$.

2.6 Norma, traço e discriminante

Seja A um anel, E um A-módulo livre de posto finito e seja u um endomorfismo de E, isto é, um homomorfismo $u : E \longrightarrow E$. Na álgebra linear definimos o traço, o determinante e o polinômio característico de u da seguinte forma: se $\{e_i\}$ é uma base de E e se (A_{ij}) é uma matriz de u com respeito a essa base, então o traço, o determinante e o polinômio característico de u são respectivamente:

$$Tr(u) = \Sigma_{i=1}^{n} a_{ii},\ detu = det(A_{ij})$$

$$det(XI_E - u) = det(X\delta_{ij} - A_{ij}),$$
onde $\delta_{ij} = 0$ se $j \neq i$ e $\delta_{ij} = 1$ se $i = j$

Observação: Esses valores independem da escolha da base. As fórmulas acima implicam:

$$Tr(u + u') = \Sigma_{i=1}^{n} a_{ii} + a'_{ii} = \Sigma_{i=1}^{n} a_{ii} + \Sigma_{i=1}^{n} a'_{ii} = Tr(u) + Tr(u')$$

$$det(uu') = det(A_{ij}A'_{ij}) = det(A_{ij})det(A'_{ij}) = det(u)det(u')$$

$$det(XI_E - u) = X^n - Tr(u)X^{n-1} + ... + (-1)^n det(u)$$

Seja B um anel e A um subanel de B tal que B é um A-módulo livre de posto n, por exemplo, A pode ser um corpo e B uma extensão finita de A com grau n. Para $x \in B$, a multiplicação m_x por x, isto é um homomorfismo de $y \longmapsto xy$ com y em B, é endomorfismo do A-módulo B, isto é, homomorfismo $m_x : B \longrightarrow B$

Definição: Chamaremos traço (resp. norma, o polinômio característico) de $x \in B$, relativo a B e A, o traço (resp. determinante, polinômio característico) do endomorfismo m_x da multiplicação por x.

Observação o traço (resp. a norma) de x é denotado por $T_{rB/A}(x)$ $(resp.\, N_{B/A}(x))$ ou $T_r(x)\,(resp.N(x))$ quando não houver confusão. Estes são elementos de A.

Para $x, x' \in B$ e $a \in A$ temos $m_x + m'_x = m_{x+x'}$ e $m_x \circ m'_x = m_{xx}$ e $m_{ax} = am_x$. Obtemos então:

$$T_r(x + x') = T_r(m_{x+x'}) = T_r(m_x + m_{x'}) = T_r(m_x) + T_r(m_{x'}) = T_r(x) + T_r(x')$$

$$T_r(ax) = T_r(m_{ax}) = T_r(am_x) = aT_r(m_x) = aT_r(m_x) = aT_r(x)$$

$T_r(a) = T_r(m_a) = a + a.... + a = na$. De modo análogo mostra-se também que:

$$N(xx') = N(x)N(x')$$

$$N(a) = a^n$$

$$N(ax) = a^n N(x).$$

Proposição 2.15 *Seja K um corpo de característica zero ou finito, L uma extensão algébrica de K de grau n, x um elemento de L, e as raízes $x_1, ..., x_n$ do polinômio minimal $F(X) \in K[X]$ de x sobre K, cada uma repetida $[L : K[x]]$ vezes. Então $T_r(x) = x_1 + ... + x_n$, $N_{L/K}(x) = x_1...x_n$. O polinômio característico de x, relativo as extensões L e K é igual a $(X - x_1)...(X - x_n)$*

Demonstração: Vamos primeiro considerar o caso onde x é um elemento primitivo de L sobre K. Seja $F(X)$ o polinômio minimal de x sobre K. Então L é K-isomorfo a $K(X)/F(X)$ e $\{1, x, ..., x^{n-1}\}$ é uma base para L sobre K. Ponhamos $F(X) = X^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$. A matriz do endomorfismo m_x com respeito a esta base é:

$$M = \begin{vmatrix} 0 & 0 & ... & 0 & -a_0 \\ 1 & 0 & ... & 0 & -a_1 \\ 0 & 1 & ... & 0 & -a_2 \\ . & . & ... & . & . \\ . & . & ... & . & . \\ . & . & ... & . & . \\ 0 & 0 & ... & 1 & -a_{n-1} \end{vmatrix}$$

o determinante de $XI_L - m_x$ é portanto o determinante da matriz

$$XI_n - M = \det\left[\begin{pmatrix} x & 0 & ... & 0 \\ 0 & x & ... & 0 \\ . & . & ... & . \\ . & . & ... & . \\ . & . & ... & . \\ 0 & 0 & ... & x \end{pmatrix} - \begin{pmatrix} 0 & 0 & ... & 0 & -a_0 \\ 1 & 0 & ... & 0 & -a_1 \\ 0 & 1 & ... & 0 & -a_2 \\ . & . & ... & . & . \\ . & . & ... & . & . \\ 0 & 0 & .... & 1 & -a_{n-1} \end{pmatrix}\right] = det\begin{pmatrix} x & 0 & ... & 0 & a_0 \\ -1 & x & ... & 0 & a_1 \\ 0 & -1 & ... & 0 & a_2 \\ . & . & ... & . & . \\ . & . & ... & . & . \\ . & . & ... & . & . \\ 0 & 0 & ... & -1 & X - a_{n-1} \end{pmatrix}$$

Expandindo esse determinante como um polinômio em X, obtemos o polinômio característico de x, isto é, $det(XI_n - M) = X^n + a_{n-1}X^{n-1} + ... + a_1X + a_0 = F(X)$. Daí, pelas equações acima temos que $T_r(x) = -a_{n-1}$ e $N(x) = (-1)^n a_0$. Como x é um elemento primitivo de L sobre K, temos $F(X) = (X - x_1)....(X - x_n)$, pois F possui exatamente n raízes. Igualando os coeficientes vemos que $Tr(x) = x_1 + ... + x_n$ e $N(x) = x_1...x_n$.
Considere agora o caso geral. Ponha $r = [L : K[x]]$. É suficiente mostrar que o polinômio característico $P(X)$ de x, com respeito a L e K, é igual a r-ésima potência do polinômio minimal de x sobre $\mathbb{Z}$, isto é, $F(X)^n = P(X)$. Seja $\{y_i\}_{i=1,...,q}$ uma base para $K[x]$ e $\{z_i\}_{j=1,...,r}$ uma base para L sobre $K[x]$ e $\{y_i z_j\}_{i=1,..,q,j=1,..,r}$ uma base para L sobre K e $n = qr$ pela proposição 2.12. Seja $M = (A_{ih})$ a matriz para a multiplicação por x em $K]x]$, com respeito a base $\{y_i\}_{i=1,...,q}$. Assim, $xy_i = \Sigma_h a_{ih} y_h$. Daí, obtemos então $x(y_i z_j) = \Sigma_h (a_{ih} y_h) z_j = \Sigma_h a_{ih}(y_h z_j)$, para $i = 1, ..., q$ e $j = 1, ..., r$. Logo a matriz M_1 de $m_x : L \to L$, com respeito a base K-espaço vetorial, considerada acima, é a matriz de blocos diagonais da forma

$$M_1 = \begin{pmatrix} M & 0 & ... & 0 \\ 0 & M & ... & 0 \\ . & . & ... & . \\ . & . & ... & . \\ . & . & ... & . \\ 0 & 0 & ... & M \end{pmatrix}$$

.
Como M_1 é $n \times n$ e M é $q \times q$ temos que M deve aparecer r vezes em M_1, como blocos diagonais em M_1, já que $n = qr$. Daí, a matriz $XI_n - M_1$ consiste de r blocos diagonal cada um da forma $XI_q - M$. Consequentemente, $det(XI_n - M_1) = det(XI_n - M)^r$. O lado esquerdo da equação é $P(X)$, enquanto $det(XI_q - M)$ é o polinômio minimal de x sobre K, de acordo com a primeira parte da prova. Logo, o polinômio característico $P(X)$ de x, com respeito L e a K, é igual a r-ésima potência do polinômio minimal de x sobre K.

Proposição 2.16 *Seja A um domínio de integridade, K seu corpo de fração, L sua extensão de K com grau finito e x em L inteiro sobre A. Assuma que K tem característica*

zero. Então os coeficientes do polinômio característico $P(X)$ de x relativa a L e K, em particular $T_{rL/K}(x)$ e $N_{L/K}(x)$ são inteiros sobre A

Demonstração: Pela preposição 2.14, $P(X) = (X - x_1)....(X - x_n)$; assim os coeficientes de $P(X)$ são, a menos de sinal, soma de produtos dos $x_i's$. Daí, é suficiente mostrar que $x_i's$ que são inteiros sobre A pelo corolário 2.7. Como cada x_i é um conjugado de x sobre K, pois os $x_i^{'}s$ são dois a dois conjugados e $K[X]/P(X) \simeq K[x_i]$ e existe um K-isomorfismo $\sigma_i : K[x] \to K[x_i]$ tal que $\sigma_i(x) = x_i$. Sendo x inteiro sobre A existem $a_i \in A$, $i = 0, ..., n-1$ tais que $x^n + a_{n-1}x^{n-1} + ... + a_0 = 0$. Assim, $\sigma_i(x)^n + ... + \sigma_i(a_0) = 0$. Logo, $x_i^n + a_{n-1}x_i^{n-1} + ... + a_0 = 0$ e com isso prova que x_i é inteiro sobre A $\forall i$.

Corolário 2.10 *Suponha, além disso, que A é integralmente fechado. Então os coeficientes do polinômio característico de x, em particular $Tr_{L/K}(x)$ e $N_{L/K}(x)$, são elementos de A.*

Demonstração: Por definição os coeficientes são elementos de K. Pela proposição 2.17 eles são inteiros sobre A, sendo A integralmente fechado, eles pertence a A.

Definição 2.4 *Seja B um anel e A um subanel de B tal que B é um A-modulo livre de posto n. Para $\{x_1, ..., x_n\} \subset B^n$, chamamos o discriminante do conjunto $\{x_1, ..., x_n\}$ o elemento de A definido pela relação $D(x_1, ..., x_n) = det(Tr_{B/A}(x_i x_j)))$.*

Proposição 2.17 *Se $\{y_1, ..., y_n\} \subset B^n$ é o conjunto dos elementos de B tal que $y_i = \Sigma_{j=1}^n a_{ij}x_j$ com $a_{ij} \in A$. Então, $D(y_i, ..., y_n) = [det(a_{ij})]^2[D(x_1, ..., x_n)]$*

Demonstração: Veja que $Tr(y_p y_q) = Tr[(\Sigma_{i=1}^n a_{pi}x_i)(\Sigma_{j=1}^n a_{qj}x_j)] = Tr(\Sigma_{i,j} a_{pi}a_{qj}x_{ij}) = \Sigma_{i,j}\, a_{pi}a_{qj}(Tr(x_i x_j))$. Daí, temos a equação matricial
$Tr(y_p y_q) = (a_{pi})(Tr(x_i x_j)(a_{qj}^t)$ onde (a_{qj}^t) é a transposta de (a_{qj}). Calculando o determinante das matrizes acima, obtemos:

$$det(Tr(y_p y_q) = det(a_{pi})det(T_r(x_i x_j)det(a_{qj}^t)$$

$$D(y_1, ..., y_n) = det(a_{pi})det(Tr(x_i x_j))det(a_{qj}^t)$$

$$D(y_1, ..., y_n) = (det(a_{ij})^2 det(Tr(x_i x_j)))$$

$$D(y_1, ..., y_n) = (det(a_{ij})^2 D(x_1, ..., x_n)$$

Observação: A proposição 2.17 implica que o discriminante de bases para B sobre A são associados em A. Isto significa que a matriz (a_{ij}) que expressa uma base em termos da outra possui uma inversa com entradas em A. Assim, $(a_{ij})(a_{ij})^{-1} = I$ e daí

$det(a_{ij})det(a_{ij})^{-1} = 1$. Logo, $det(a_{ij})$ e $det(a_{ij})^{-1}$ são unidades em A.

Definição 2.5 *Seja B um anel e A um subanel de B tal que B é um A-modulo livre de posto n. Assim o ideal principal de A gerado pelo discriminante de qualquer base de B sobre A é chamado discriminante de B sobre A. Denotemos este ideal por $D_{B/A}$*

Proposição 2.18 *Suponha que $D_{B/A}$ contém um elemento que não é um divisor de zero. Então, para que o conjunto $\{x_1, ..., x_n\} \subset B^n$ seja uma base de B sobre A, é necessário e suficiente que $D(x_1, ..., x_n)$ gere $D_{B/A}$*

Demonstração:$\Rightarrow$ é imediato da definição
$\Leftarrow$ Suponha que $d = D(x_1, ..., x_n)$ gere $D_{B/A}$. Seja $\{e_1, ..., e_n\}$ uma base de B sobre A, ponha $d' = D(e_1, ..., e_n)$ e $x_i = \Sigma_{j=1}^n a_{ij}e_j$ com $a_{ij} \in A$, $1 \leq i \leq n$. Assim pela proposição 2.2 temos que $D(x_1, ..., x_n) = det(a_{ij})^2 D(e_1, ..., e_n)$ ou seja $d' = det(a_{ij})^2 d'$. Por hipótese, temos que $Ad = D_{B/A}$. Daí $Ad = D_{B/A} = Ad(a_{ij})^2 d' = Ad'$. Logo existe $b \in A$ tal que $d' = bd$ daí $d = det(a_{ij})^2 d' \Rightarrow d = det(a_{ij})^2 db \Rightarrow d - det(a_{ij})^2 db = 0 \Rightarrow d(1 - b\, det(a_{ij})^2) = 0$. Temos que d não é divisor pois caso contrário todo elemento de $D_{B/A}$ seria um divisor de zero (o que não pode ocorre, já que $D_{B/A}$ possui um elemento que não é divisor de zero). Logo $1 - bdet(a_{ij})^2 = 0$ isso significa que o $det(a_{ij}) \neq 0$. Assim a matriz (a_{ij}) é invertível. Portanto, $\{x_1, ..., x_n\}$ é uma base de B sobre A.

Proposição 2.19 *Seja K um corpo finito ou de característica zero e L uma extensão de K de grau finito n. Considere $\sigma_1, ..., \sigma_n$ os n K-isomorfismo distintos de L em um corpo algebricamente fechado C contendo K. Então, se $\{x_1, ..., x_n\}$ é uma base para L sobre K, temos que $D(x_1, ..., x_n) = det(\sigma_i(x_j))^2 \neq 0$*

Demonstração Mostraremos inicialmente que $D(x_1, ..., x_n) = det(\sigma_i(x_j))^2$. De fato, $D(x_1, ..., x_n) = det(T_r(x_i x_j)) = det(\sigma_1(x_j)) + ... + \sigma_n(x_i x_j)) = det(\Sigma\sigma_k(x_i x_j)) = det(\sigma_k(x_i)\sigma_k(x_j)) = det(\sigma_k(x_i))det(\sigma_k(x_j)) = det(\sigma_i x_j)^2$. Vamos mostrar que $det(\sigma_i(x_j)) \neq 0$. Suponha por contradição que $det(\sigma_i(x_j)) = 0$ então existem $\{u_1, ..., u_n\} \in C$ nem todos nulos, tais que $\Sigma_{i=1}^n u_i\sigma_i(x_j) = 0\ \forall j$, por linearidade concluímos que $\Sigma_{i=1}^n u_i\sigma_i(x)) = 0$ para todo $x \in L$, mais isso contradiz o lema abaixo.

Lema 2.7 ***Dedekind*** *Seja G um grupo. C um corpo e $\sigma_1, ..., \sigma_n$ homomorfismos distintos de G no grupo multiplicativo C^*. Então os $\sigma_i's$ são linearmente independentes sobre C, isto é, $\Sigma_{i=1}^n u_i\sigma_i(g) = 0$, $\forall g \in G$ implica que os $u_i's$ são zero. e*

Demonstração: Suponha por absurdo, que $\sigma_i's$ são linearmente dependente. Considere a relação não trivial $\Sigma_{i=1}^n u_i\sigma_i = 0$, com $u_i \in C$ tal que o número q de $u_I's$ que são não

nulo é mínimo. Após renumeração podemos supor que:

$$u_1\sigma_1(g) + ... + u_q\sigma_q(g)) = 0$$

$\forall g \in G$. Temos $q \geq 2$, pois os $\sigma_i's$ são não nulos. Para g e h arbitrários em G, temos que:

$$u_1\sigma_1(hg) + ... + u_q\sigma_q(hg) = u_1\sigma_1(h)\sigma_1(g) + ... + u_q\sigma_q(h)\sigma_q(g) = 0$$

pois, $hg \in G$ e como $u_1\sigma_1(g)+...+u_q\sigma_q(g) = 0$, $\forall g \in G$, então $u_1\sigma_1(hg)+...+u_q\sigma_q(hg) = 0$. Se multiplicar a equação $u_1\sigma_1(g) + ... + u_q\sigma_q(g)) = 0$ por $\sigma_1(h)$ temos:

$$u_1\sigma_1(h)\sigma_1(g) + ... + u_q\sigma_1(h)\sigma_q(g) = 0.$$

Daí obtemos,

$$u_1\sigma_1(h)\sigma_1(g) + ... + u_q\sigma_1(h)\sigma_q(g) - u_1\sigma_1(h)\sigma_1(g) - ... - u_q\sigma_q(h)\sigma_q(g) = 0$$

Assim,
$u_1(\sigma_1(h) - \sigma_2(h))\sigma_2(g) + ... + u_q(\sigma_1(h) - \sigma_q(h))\sigma_q(g) = 0$,
como esta igualdade é verdade $\forall g \in G$ e q foi escolhido tão pequeno quanto possível, segue-se que $u_2(\sigma_1(h) - \sigma_2(h)) = 0$. Daí, $\sigma_1(h) = \sigma_2(h)$, $\forall h \in G$, pois $u_2 \neq 0$, o que é absurdo, pois por hipótese os $\sigma_i's$ são distintos.

Teorema 2.9 *Seja A um anel integralmente fechado, K seu corpo de frações, L, uma extensão de K de grau finito n e A' o fecho inteiro sobre A em L. Suponha que K é de característica zero. Então A' é um A-submódulo de A-módulo livre de posto n.*

Demonstração: Seja $\{x_1, ..., x_n\}$ uma base de L sobre K. Cada x_i é algébrico sobre K e daí para todo i, temos uma equação da forma

$$a_n x_i^n + a_{n-1}x_i^{n-1} + ... + a_0 = 0$$

com $a_j \in A$, $\forall j = 0, ..., n$, pois L é uma extensão algébrica de K, já que $[L : K]$ é finito. Podemos assumir que $a_n \neq 0$. Multiplicando a equação acima a_n^{n-1}, obtemos

$$a_n^{n-1}a_n x_i^n + a_n^{n-1}a_{n-1}x_i^{n-1} + ... + a_n^{n-1}a_0 = 0$$

$$a_n^n x_i^n + a_n^{n-1}a_{n-1}x_i^{n-1} + ... + a_n^{n-1}a_0 = 0$$

$$(a_n x_i)^n + a_{n-1}(a_n x_i)^{n-1} + ... + a_n^{n-1} a_0 = 0$$

Logo, $a_n x_i$ é inteiro sobre A. Pondo $x'_i = a_n x_i$, então $\{x'_1, ...x'_n\}$ é uma base de L sobre K contido em A', pois $a_n x_i$ é inteiro sobre A. Sabemos que existe uma base $\{y_1, ..., y_n\}$ de L sobre K tal que $T_r(x'_i y_j) = \delta_{ij}$. Seja $z \in A'$. Como $\{y_1, ..., y_n\}$ é uma base de L sobre K, podemos escrever $z = \Sigma_{j=1}^n b_j y_j$, com $b_j \in K$, pois $z \in A' \Rightarrow z \in L$ ser um inteiro sobre A e como $\{y_1, , , y_n\}$ é uma base de L sobre K então de fato temos $z = \Sigma_{j=1}^n (b_j y_j)$. Para todo i, temos que $x'_i z \in A'$, pois $x'_i \in A'$ e $z \in A$. Logo, pelo corolário 4.1, $T_r(x'_i z) \in A$. Assim $T_r(x'_i z) = T_r(x'_i \Sigma_j^n b_j y_j) = T_r x'_i (\Sigma_j^n b_j y_j) = \Sigma_j^n T_r(x'_i y_j)$, pois $b_j \in K$.

$$Tr(x'_1 z) = \Sigma_{j=1}^n b_j \delta_{ij} = b_1 \delta_{i1} + ... + b_i \delta_{ij} = b_i$$

então podemos concluir que $b_i \in A$, $\forall i$, pois $Tr(x'_i z) \in A$. Isto implica que A' é um submódulo do A-módulo livre $\Sigma_{j=1}^n a_{yj}$, poi $x'z \in A'$, $\forall z \in \Sigma_{j=1}^n a_{yj}$ e $\forall\, x'_i \in A'$.

Corolário 2.11 *Com as hipóteses do teorema 2.9 e supondo que A é principal, temos que A' é um A-módulo livre de posto n.*

Demonstração: Como A' é um submódulo de A-módulo livre e A é principal, então temos pelo item (a) do Teorema 2.3, se A é um anel de ideais principais, M é um A-módulo livre de posto n e M' é um submódulo de M então M' é livre de *posto* $\leq n$. Daí, temos que A' é livre de *posto* $\leq n$. Por outro lado, temos pela prova do Teorema 2.10 que A' contém uma base de L sobre K. Assim, A' possui uma base com n elementos. Portanto, A' é de posto .

2.7 A terminologia dos corpos numéricos

Definição: Qualquer extensão finita (e portanto algébrica) de $\mathbb{Q}$ é chamada um corpo de números algébricos ou corpo numérico.

Definição: Um corpo numérico de grau 2 (resp. 3) é chamado corpo quadrático (rep. cúbico). Para um corpo numérico K, $[K : \mathbb{Q}]$ denota o grau de K.

Observação: Um corpo numérico sempre possui característica zero, pois contém $\mathbb{Q}$ e consequentemente $\mathbb{Z}$. Os elementos de um corpo numérico K que são inteiros sobre $\mathbb{Z}$ são chamados, os inteiros de K. Eles formam um subanel A de K pelo Corolário 2.7. Esse anel A é um $\mathbb{Z}$-módulo livre de posto $[K : \mathbb{Q}]$ pelo Corolário 2.11.

Definição: Os discriminantes das bases do $\mathbb{Z}$-módulo diferem pelo quadrado de uma unidade de $\mathbb{Z}$ e portanto são iguais. Este número é chamado discriminante de K

Definição: Seja K um corpo. Um elemento $\xi \in K$ tal que $\xi^n = 1$ é chamado uma raiz n-ésima da unidade. Dizemos que ξ é uma raiz n-ésima primitiva da unidade se $\xi^n = 1$ e $\xi^m \neq 1$ para $1 < m < n$.

Lema 2.8 *(Lema de Gauss) Seja A um anel de ideais principais, p um elemento primo de A e $F(X) = X^n + a_{n-1}X^{n-1} + ... + a_1X + a_0 \in A[X]$ tal que p/a_i $(0 \leq i \leq n-1)$ e $p \nmid a_0$. Então $F(X)$ é irredutível sobre K, o corpo de frações de A.*
Demonstração: Suponha que $F = GH$ com $G, H \in K[X]$ e ambos polinômios mônicos. As raízes de F são inteiras sobre A. Qualquer raiz de G ou H é uma raiz de F, portanto inteiro sobre A. Os coeficientes de G (resp. H) são somas de produtos de raízes de G (resp. H), eles são portanto inteiros sobre A, pelo Corolário 2.7. Como A é um anel de ideais principais, temos que A é integralmente fechado pelo Exemplo 2.7. Logo, $G, H \in A[X]$. Agora considere $\overline{F}$, $\overline{G}$ e $\overline{H}$ como sendo as imagens de F, G e H respectivamente em $(A/A_p)[x]$, então $\overline{F} = \overline{GH}$. Como por hipótese $p|a_i$, $0 \leq i \leq n-1$, temos que $\overline{F} = X^n$, pois $F[x] = \Sigma d_i x' \mapsto \overline{F(x)} = \Sigma \overline{d_i} x_i$. Como A/A_p é domínio de integridade, a fatoração $X^n = \overline{GH}$ é necessariamente da forma $X^n = X^q X^{n-q}$ (pois, G e H são mônicos), assim $\overline{G} = X^q$ e $\overline{H} = X^{n-q}$. Se G e H são ambos não constantes, então p divide os termos constantes de G e H. Logo, p^2 divide os termos constantes a_0 de F, mas isso contraria a hipótese. Logo, ou G ou H é constante e F é irredutível.
Exemplo O polinômio $X^3 - 2X + 6$ é irredutível sobre $\mathbb{Q}$. Basta tomar $p = 2$ e $A = \mathbb{Z}$ no Lema de Gauss.

2.8 Módulos Noetherianos e alguns preliminares sobre ideais

Definição: Um A-módulo M é chamado Noetheriano se o mesmo satisfaz as seguintes condições de equivalência:
(a) Toda coleção não vazia de submódulos de M contém um elemento maximal;
(b) Toda sequência crescente de submódulos de M é estacionária;
(c) Todo submódulo de M é do tipo finito.
Um anel A é Noetheriano se, considerado como um A-módulo, for um módulo Noetheriano.

Observação: Quando consideramos um anel como um A-módulo sobre si mesmo, seus submódulos são seus ideais, com isso e em virtude da condição (c), dizemos que um anel A é Noetheriano quando os seus ideais são gerados por um número finito de elementos

Exemplo: Todo anel de ideais principais é Noetheriano, pelo corolário 2.2

Proposição 2.20 *Seja A um anel, E um A-módulo e E' um submódulo de E. Para que E seja Noetheriano é necessário e suficiente que E' e E/E' sejam Noetherianos*
Demonstração: Suponha que E seja Noetheriano. Temos que toda sequência crescente de submódulos de E' é também uma sequência crescente de submódulos de E. Sendo E Noetheriano, toda sequência crescente de submódulos de E' é estacionária. Daí, toda sequência crescente de submódulos de E' é estacionária. Logo, E' é Noetheriano. Considerando o homomorfismo canônico $\sigma : E \longrightarrow E/E'$, o mesmo define uma correspondência biunívoca que preserva a inclusão entre os submódulos de E que contém E' e os submódulos de E/E'. Logo, toda sequência crescente de submódulos de E/E', corresponde através de σ a uma sequência crescente de submódulos de E. Como toda sequência crescente de submódulos de E é estacionária, temos que toda sequência crescente de submódulos de E/E' também é estacionária. Logo, E/E' é Noetheriano. Reciprocamente, suponha que E' e E/E' são Noetherianos. Seja $(F_n)_{n\geq 0}$ uma sequência crescente de submódulos de E. Como E' é Noetheriano, existe um inteiro n_0 tal que $F_n \cap E' = F_{n+1} \cap E'$ para todo $n \geq n_0$, pois $F_n \cap E'$ é uma sequência crescente de submódulos de E'. Como E/E' é Noetheriano, existe um inteiro n_1 tal que $(F_n + E')/E' = (F_{n+1} + E')/E'$ para todo $n \geq n_1$, pois é $(F_n + E')/E'$ uma sequência crescente de submódulos de E/E'. Logo, $F_n + E' = F_{n+1} + E'$ para todo $n \geq n_1$.Tome $n \geq sup(n_0, n_1)$. Mostraremos que $F_n = F_{n+1}$, para isto, é suficiente mostrar que $F_n \subset F_{n+1}$, pois $F_n \subset F_{n+1}$, já que $(F_n)_{n\geq 0}$ é crescente. De fato, seja $x \in F_{n+1}$ como $F_n + E' = F_{n+1} + E'$ temos que existem $y \in F_n$ e $y', y'' \in E'$ tais que $x + y' = y + y''$. Assim, $x - y = y'' - y' \in F_{n+1} \cap E' = F_n \cap E'$, pois $y'' - y' \in E'$ e como $x - y \in F_{n+1}$. Como $x - y$ e y pertencem a F_n temos que $(x - y) + y \in F_n$, isto é, $x \in F_n$. Logo, $F_{n+1} \subset F_n$. Portanto, $F_n = F_{n+1}$ para todo $n \geq sup(n_0, n_1)$. Logo, E é Noetheriano.

Corolário 2.12 *Seja A um anel e sejam $E_1, ..., E_n$ A-módulos Noetherianos. Então o A-módulo produto $\Pi_{i=1}^{n} E_i$ é Noetheriano.*
Demonstração: Faremos indução sobre n. Para $n = 1$ a afirmação é verdadeira, pois E_1 é Noetheriano. Suponha que a afirmação é verdadeira para $n - 1$, com $n \geq 2$. Temos que $(E_1 \times ... \times E_n)/E_n$ é isomorfo a $E_1 \times ... \times E_{n-1}$ que é Noetheriano por hipótese. Logo, pela Proposição 6.1 temos que $E_1 \times ... \times E_n$ é Noetheriano.

Corolário 2.13 *Seja A um anel Noetheriano e E um A-módulo do tipo finito. Então E é um módulo Noetheriano e portanto todos os seus submódulos são do tipo finito.*
Demonstração: Seja $E = Ax_1 + ... + Ax_n$ e $\varphi : A^n \longrightarrow E$ e um homomorfismo dado por $\varphi(a_1, ..., a_n) = \Sigma_{i=1}^{n} a_i x_i$. Assim, $A^n/Ker\,\varphi$ é isomorfo a E. Como A é Noetheriano, pelo corolário 6.1, temos que $A^n = A \times ... \times A$ é Noetheriano. Assim, pela proposição 6.1 temos que $A^n/Ker\,\varphi$ é Noetheriano. Logo, E é Noetheriano.

Proposição 2.21 *Seja A um anel Noetheriano integralmente fechado. Seja K seu corpo de frações, L a extensão finita de K, A' o fecho integral de A em L. Suponha que K tenha característica 0. Então A' é um A-módulo do tipo finito e é anel Noetheriano.*
Demonstração: Sabemos que A' é um submódulo de um A-modulo livre de posto n (Teorema 2.3). Então A' é um A-modulo do tipo finito (proposição 2.9), e, portanto, modulo Noetheriano. Por outro lado, os ideais de A' são um casos especiais de A-submódulo de A'. Eles satisfazem a condição maximalidade Teorema 2.2 (a), então A' é um anel Noetheriano.)

Exemplo: O anel dos inteiros de um corpo de números é Noetheriano ($A = \mathbb{Z}$ e $K = \mathbb{Q}$)

Definição: Um ideal $\mathfrak{p}$ de um anel A é chamado primo se o quociente $A/\mathfrak{p}$ for um domínio de integridade. Equivalentemente, se $x, y \in A - \mathfrak{p}$ então $xy \in A - \mathfrak{p}$ isto é, $A - \mathfrak{p}$ é fechado para a multiplicação.

Definição: Um ideal $\mathfrak{q}$ de um anel A é chamado maximal se o quociente $A/\mathfrak{q}$ for um corpo. Equivalentemente, se para todo ideal $\mathfrak{p}$ de A tal que $\mathfrak{q} \subseteq \mathfrak{p} \subseteq A$ implicar que $\mathfrak{p} = \mathfrak{q}$ ou $\mathfrak{p} = A$

Observação: Todo ideal maximal é primo. A recíproca é falsa, pois o ideal (0) de $\mathbb{Z}$ é primo, mas não é maximal.

Lema 2.9 *Seja A um anel, $\mathfrak{p}$ um ideal primo de A e A' um subanel de A. Então $\mathfrak{p} \cap A'$ é um ideal primo de A'.*
Demonstração Seja $\varphi : A' \longrightarrow A$ a aplicação de inclusão e $\sigma : A \longrightarrow A - \mathfrak{p}$ o homomorfismo canônico. Assim, a composta $\phi = \sigma \circ \varphi : A' \longrightarrow A - \mathfrak{p}$ um homomorfismo tal que $Ker\,\phi = \{a' \in A' |\, \phi(a') = 0\} = \{a' \in A' |\, a' + \mathfrak{p} = 0 + \mathfrak{p}\} = \{a' \in A' |\, a' \in \mathfrak{p}\}$. Assim, $ker\,\phi = A' \cap \mathfrak{p}$. Pelo teorema dos homomorfismos de anéis temos que $A'/A' \cap \mathfrak{p} \simeq im\,\phi$. Logo, $A'/A' \cap \mathfrak{p}$ é um subanel de $A/\mathfrak{p}$. Como $\mathfrak{p}$ é um ideal primo então $A/\mathfrak{p}$ é um $D.I.$ Como um subanel de um $D.I.$ é também um $D.I.$ temos que $A'/A' \cap \mathfrak{p}$ é um $D.I.$ E daí $A' \cap \mathfrak{p}$ é um ideal primo.

Definição: Dados dois ideais $\mathfrak{a}$ e $\mathfrak{b}$ de um anel A, definimos o produto de $\mathfrak{a}$ e $\mathfrak{b}$ como o conjunto de todas as somas finitas $\Sigma_{i=1}^{n} a_i b_i$ de produtos de elementos de $\mathfrak{a}$ por elementos de $\mathfrak{b}$, isto é:

$$\mathfrak{ab} = \{\Sigma_{i=1}^{n} a_i b_i |\, n \in \mathbb{Z}; n > 0, a_i \in \mathfrak{a}\, e\, b_i \in \mathfrak{b}\}$$

É claro que $\mathfrak{ab}$ é um ideal de A. Além disso, $\mathfrak{ab} \subset \mathfrak{a}$ e $\mathfrak{ab} \subset \mathfrak{b}$ e daí $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$, mas nem sempre ocorre $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$. Se $\mathfrak{a} + \mathfrak{b} = A$ então $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$.

É fácil ver que multiplicação de ideais é associativa e comutativa. A atua como o elemento identidade no monoide.

Lema 2.10 *Se um ideal primo* $\mathfrak{p}$ *de um anel* A *contém um produto* $\mathfrak{a}_1...\mathfrak{a}_n$ *de ideais, então* $\mathfrak{p}$ *contém pelo menos um dos ideais* $\mathfrak{a}_i$*.*
Demonstração: Suponha por absurdo que $\mathfrak{a}_i \nsubseteq \mathfrak{p}$ para todo i. Assim, existe $x_i \in \mathfrak{a}_i - \mathfrak{p}$ para todo i. Logo, $x_1x_2...x_n \notin \mathfrak{p}$, pois $\mathfrak{p}$ é primo Mas, $x_1x_2...x_n \in \mathfrak{a}_1\mathfrak{a}_2...\mathfrak{a}_n \subset \mathfrak{p}$ que é absurdo. Portanto, $\mathfrak{p}$ contém pelo menos um dos ideais $\mathfrak{a}_i$.

Lema 2.11 *Em um anel Noetheriano todo ideal contém um produto de ideais primos. Em um domínio de integridade Noetheriano* A*, todo ideal não nulo contém um produto de ideais primos não nulos.*
Demostração: Suponha por absurdo que a família ϕ dos ideais não nulos de A que não contém um produto de ideais primos não nulos é não vazia. Como A é Noetheriano, ϕ contém um elemento maximal $\mathfrak{q}$. O ideal $\mathfrak{q}$ não pode ser primo, pois caso contrário $\mathfrak{q}$ não pertenceria a ϕ . Assim, existem $x, y \in A - \mathfrak{q}$ tais que $xy \in \mathfrak{q}$. Os ideais $\mathfrak{q} + Ax$ e $\mathfrak{q} + Ay$ contém $\mathfrak{q}$ como um subconjunto próprio, pois $x \in \mathfrak{q} + Ax$ e $x \notin \mathfrak{q}$, $y \in \mathfrak{q} + Ay$ e $y \notin \mathfrak{q}$. Como $\mathfrak{q}$ é um elemento maximal da família ϕ , temos que os ideais $\mathfrak{q} + Ax$ e $\mathfrak{q} + Ay$ não pertencem a ϕ . Logo, estes ideais contém produto de ideais primos não nulos $\mathfrak{p}_1...\mathfrak{p}_n \subset \mathfrak{q} + Ax$ e $\mathfrak{p'}_1...\mathfrak{p'}_n \subset \mathfrak{q} + Ay$ como $xy \in \mathfrak{q}$ então $(\mathfrak{q} + Ax)(\mathfrak{q} + Ay) \subset \mathfrak{q}$. Logo, $\mathfrak{p}_1...\mathfrak{p}_n\mathfrak{p'}_1...\mathfrak{p'}_n \subset \mathfrak{q}$ o que é absurdo, pois $\mathfrak{q} \in \phi$. Portanto, ϕ é vazia.

Agora seja A um domínio de integridade e K seu corpo de frações. Chamamos qualquer A-submódulo I de K para o qual existe $d \in A - (0)$ tal que $dI \subset A$ um ideal fracionário de A ou de K com respeito a A. Isso significa que os elementos de I tem um denominador comum $d \in A$. Os ideais ordinários de A são ideais fracionários com $(d = 1)$. As vezes os chamamos de ideais inteiros para distingui-los entre os ideais fracionários. Qualquer A-submódulo I do tipo finito contido em K é um ideal fracionário. Isto segue do fato que se $\{x_1, ..., x_n\}$ é um conjunto de geradores de I, os x'_is tem um denominador comum d (o produto dos denominadores d'_is onde $x_i = a_id_i^{-1}$ com $a_i, d_i \in A$) e d é um denominador comum para I. Reciprocamente, se A é Noetheriano, todo ideal fracionário I é um A-módulo do tipo finito, pois $I \subset d^{-1}A$ e $d^{-1}A$ é um A-módulo isomorfo a A. Como A é Noetheriano, todo submódulo de A é do tipo finito. Logo, I é do tipo finito.

Definição: Definimos o produto II' de dois ideais fracionários I e I' como o conjunto das somas finitas Σx_iy_i onde $x_i \in I$ e $y_i \in I'$.

Observação: Se I e I' são ideais fracionários com denominadores comum d e d' respectivamente, então os conjuntos $I \cap I'$, $I + I'$ e II' são todos ideais fracionários. Eles são claramente A-submódulos de K e tem como denominador comum d ou d', $d + d'$ e dd' respectivamente. Os ideai fracionários não nulos de A constituem um monoide comutativo sobre a multiplicação, isto é, um semigrupo comutativo com unidade.

2.9 Anéis de Dedekind e norma de um ideal

Definição: Um domínio de integridade A é chamado um anel de Dedekind se o mesmo é Noetheriano e integralmente fechado, e se todo ideal primo não nulo de A for maximal.

Exemplo: Qualquer anel de ideais principais é um anel de Dedekind, pois o mesmo é Noetheriano, integralmente fechado e todos ideal primo não nulo seu é maximal.

Teorema 2.10 *Seja A um anel de Dedekind, K seu corpo de frações, L uma extensão finita de K, e A' o fecho inteiro de A em L. Assuma que K tem característica zero. Então A' é um anel de Dedekind e um A-módulo do tipo finito*

Demonstração: O anel A é integralmente fechado por construção, é Notheriano e um A-módulo do tipo finito pela Proposição 4.1. Resta mostrar que todo ideal primo $\mathfrak{p}' \neq 0$ de A' é maximal. Para isso escolha um elemento $x \in \mathfrak{p}' - (0)$ e considere uma equação de dependência inteira de x sobre A, que possui menor grau possível

$$x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = 0 \qquad (1)$$

, com $a_i \in A$. Assim, $a_0 \neq 0$, caso contrário x satisfaz uma equação de dependência inteira de grau menor que n. Pela equação (1) temos que $a_0 \in A'x \cap A \subset \mathfrak{p}' \cap A$, pois $a_0 = -x(x^{n-1} + a_{n-1}x^{n-1} + ... + a_1)$. Portanto, $\mathfrak{p}' \cap A \neq (0)$ Como $\mathfrak{p}' \cap A$ é um ideal primo de A pelo Lema 4.1, temos que $\mathfrak{p}' \cap A$ é um ideal maximal de A, pois A é de Dedekind. Portanto, $A/\mathfrak{p}' \cap A$ é um corpo. Mas, $A/\mathfrak{p}' \cap A$ pode ser identificado como um subanel de $A'/\mathfrak{p}'$ e este é inteiro sobre $A/\mathfrak{p}' \cap A$, pois A' é inteiro sobre A. Assim, $A'/\mathfrak{p}'$ é um corpo pela Proposição 4.1. Logo, $\mathfrak{p}'$ é maximal.

Teorema 2.11 *Seja A um anel de Dedekind que não é um corpo. Todo ideal maximal de A é invertível no monoide de ideais fracionários de A, isto é, se $\mathfrak{a}$ é um ideal maximal de A existe um ideal fracionário $\mathfrak{a}'$ de A tal que $\mathfrak{a}\mathfrak{a}' = A$*

Demonstração: Seja $\mathfrak{a}$ um ideal maximal de A. Então $\mathfrak{a} \neq (0)$, pois A não é um corpo. Ponha

$$\mathfrak{a}' = \{x \in K \,|\, x\mathfrak{a} \subset A\} \qquad (2)$$

Claramente, $\mathfrak{a}'$ é um A-submódulo de K, qualquer elemento não nulo de $\mathfrak{a}$ serve como um denominador comum para os elementos de M'. Assim, $\mathfrak{a}'$ é um ideal fracionário de A. É suficiente mostrar que $\mathfrak{a}\mathfrak{a}' = A$. Pela equação (2) temos que $\mathfrak{a}'\mathfrak{a} \subset A$, por outro lado, $A \subset \mathfrak{a}'$, pois sendo $\mathfrak{a}$ um ideal maximal de A, dado $a \in A$, $a\mathfrak{a} \subset \mathfrak{a} \subset A \Rightarrow a \in \mathfrak{a}'$. Assim, $\mathfrak{a} = A\mathfrak{a} \subset \mathfrak{a}'\mathfrak{a}$. Como $\mathfrak{a}$ é maximal e $\mathfrak{a} \subset \mathfrak{a}'\mathfrak{a} \subset A$ então $\mathfrak{a} = \mathfrak{a}'\mathfrak{a}$ ou $\mathfrak{a}'\mathfrak{a} = A$. Daí, resta mostrar que $\mathfrak{a} = \mathfrak{a}'\mathfrak{a}$ não pode ocorrer. Se $\mathfrak{a}'\mathfrak{a} = \mathfrak{a}$ e $x \in \mathfrak{a}'$ então $x\mathfrak{a} \subset \mathfrak{a}$, $x^2\mathfrak{a} \subset x\mathfrak{a} \subset \mathfrak{a}$ e $x^n\mathfrak{a} \subset \mathfrak{a}$ para qualquer $n \in \mathbb{N}$, por indução. Assim, qualquer elemento não nulo $d \in \mathfrak{a}$ é um denominador comum para todas as potências x^n de x, $n \in \mathbb{N}$. Segue-se que $A[x]$ é um ideal fracionário de A. Como A é Noetheriano, $A[x]$ é um A-módulo do tipo finito, assim x é inteiro sobre A pelo Teorema 2.5. Mas, A é integralmente fechado, portanto $x \in A$ e consequentemente $\mathfrak{a}'\mathfrak{a} = \mathfrak{a}$ implica $\mathfrak{a}' = A$. Daí, resta mostrar que $\mathfrak{a}' = A$ não pode ocorrer, para isso, tome um elemento não nulo $a \in \mathfrak{a}$. O ideal A contém um produto de ideais primos não nulos $\mathfrak{p}_1...\mathfrak{p}_n$ pelo Lema 4.3. Podemos tomar n como o menor possível. Daí, temos $\mathfrak{a} \supset A\mathfrak{a} \supset \mathfrak{p}_1...\mathfrak{p}_n$ isto significa que $\mathfrak{a} \supset \mathfrak{p}_1$ para algum i pelo Lema 4.2, digamos $1 = i$. Como $\mathfrak{p}_1$ é maximal, pois A é de Dedekind, temos que $\mathfrak{a} = \mathfrak{p}_1$. Ponha $\mathfrak{q} = \mathfrak{p}_2...\mathfrak{p}_n$, daí $Aa \supset \mathfrak{a}\mathfrak{q}$ e $Aa \not\supseteq \mathfrak{q}$ pois n é o menor possível. Assim, existe $b \in \mathfrak{q}$ tal que $b \notin Aa$. Como $\mathfrak{a}\mathfrak{q} \subset Aa$ temos que $\mathfrak{a}b \subset Aa$ e consequentemente $aba^{-1} \subset A$. De acordo com a definição de $\mathfrak{a}'$, isso significa que $ba^{-1} \in \mathfrak{a}'$. Mas, como $b \notin Aa$ temos que $ba^{-1} \notin A$ Assim, $\mathfrak{a}' \neq A$ e consequentemente $\mathfrak{a}'\mathfrak{a} \neq \mathfrak{a}$. Logo, $\mathfrak{a}'\mathfrak{a} = A$ como queríamos provar.

Teorema 2.12 *Seja A um anel de Dedekind, K seu corpo de frações, L uma extensão finita de K, e A' o fecho inteiro de A em L. Assuma que K tem característica zero. Então A' é um anel de Dedekind e um A-módulo do tipo finito*

Demonstração: O anel A é integralmente fechado por construção, é Notheriano e um A-módulo do tipo finito pela Proposição 4.1. Resta mostrar que todo ideal primo $\mathfrak{p}' \neq 0$ de A' é maximal. Para isso escolha um elemento $x \in \mathfrak{p}' - (0)$ e considere uma equação de dependência inteira de x sobre A, que possui menor grau possível

$$x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = 0 \qquad (1)$$

, com $a_i \in A$. Assim, $a_0 \neq 0$, caso contrário x satisfaz uma equação de dependência inteira de grau menor que n. Pela equação (1) temos que $a_0 \in A'x \cap A \subset \mathfrak{p}' \cap A$, pois $a_0 = -x(x^{n-1} + a_{n-1}x^{n-1} + ... + a_1)$. Portanto, $\mathfrak{p}' \cap A \neq (0)$ Como $\mathfrak{p}' \cap A$ é um ideal primo de A pelo Lema 4.1, temos que $\mathfrak{p}' \cap A$ é um ideal maximal de A, pois A é de Dedekind.

Portanto, $A/\mathfrak{p}' \cap A$ é um corpo. Mas, $A/\mathfrak{p}' \cap A$ pode ser identificado como um subanel de $A'/\mathfrak{p}'$ e este é inteiro sobre $A/\mathfrak{p}' \cap A$, pois A' é inteiro sobre A. Assim, $A'/\mathfrak{p}'$ é um corpo pela Proposição 4.1. Logo, $\mathfrak{p}'$ é maximal.

Teorema 2.13 *Seja A um anel de Dedekind que não é um corpo. Todo ideal maximal de A é invertível no monoide de ideais fracionários de A, isto é, se $\mathfrak{a}$ é um ideal maximal de A existe um ideal fracionário $\mathfrak{a}'$ de A tal que $\mathfrak{a}\mathfrak{a}' = A$*
Demonstração: Seja $\mathfrak{a}$ um ideal maximal de A. Então $\mathfrak{a} \neq (0)$, pois A não é um corpo. Ponha

$$\mathfrak{a}' = \{x \in K \mid x\mathfrak{a} \subset A\} \qquad (2)$$

Claramente, $\mathfrak{a}'$ é um A-submódulo de K, qualquer elemento não nulo de $\mathfrak{a}$ serve como um denominador comum para os elementos de M'. Assim, $\mathfrak{a}'$ é um ideal fracionário de A. É suficiente mostrar que $\mathfrak{a}\mathfrak{a}' = A$. Pela equação (2) temos que $\mathfrak{a}'\mathfrak{a} \subset A$, por outro lado, $A \subset \mathfrak{a}'$, pois sendo $\mathfrak{a}$ um ideal maximal de A, dado $a \in A$, $a\mathfrak{a} \subset \mathfrak{a} \subset A \Rightarrow a \in \mathfrak{a}'$. Assim, $\mathfrak{a} = A\mathfrak{a} \subset \mathfrak{a}'\mathfrak{a}$. Como $\mathfrak{a}$ é maximal e $\mathfrak{a} \subset \mathfrak{a}'\mathfrak{a} \subset A$ então $\mathfrak{a} = \mathfrak{a}'\mathfrak{a}$ ou $\mathfrak{a}'\mathfrak{a} = A$. Daí, resta mostrar que $\mathfrak{a} = \mathfrak{a}'\mathfrak{a}$ não pode ocorrer. Se $\mathfrak{a}'\mathfrak{a} = \mathfrak{a}$ e $x \in \mathfrak{a}'$ então $x\mathfrak{a} \subset \mathfrak{a}$, $x^2\mathfrak{a} \subset x\mathfrak{a} \subset \mathfrak{a}$ e $x^n\mathfrak{a} \subset \mathfrak{a}$ para qualquer $n \in \mathbb{N}$, por indução. Assim, qualquer elemento não nulo $d \in \mathfrak{a}$ é um denominador comum para todas as potências x^n de x, $n \in \mathbb{N}$. Segue-se que $A[x]$ é um ideal fracionário de A. Como A é Noetheriano, $A[x]$ é um A-módulo do tipo finito, assim x é inteiro sobre A pelo Teorema 2.5. Mas, A é integralmente fechado, portanto $x \in A$ e consequentemente $\mathfrak{a}'\mathfrak{a} = \mathfrak{a}$ implica $\mathfrak{a}' = A$. Daí, resta mostrar que $\mathfrak{a}' = A$ não pode ocorrer, para isso, tome um elemento não nulo $a \in \mathfrak{a}$. O ideal A contém um produto de ideais primos não nulos $\mathfrak{p}_1...\mathfrak{p}_n$ pelo Lema 4.3. Podemos tomar n como o menor possível. Daí, temos $\mathfrak{a} \supset A\mathfrak{a} \supset \mathfrak{p}_1...\mathfrak{p}_n$ isto significa que $\mathfrak{a} \supset \mathfrak{p}_1$ para algum i pelo Lema 4.2, digamos $1 = i$. Como $\mathfrak{p}_1$ é maximal, pois A é de Dedekind, temos que $\mathfrak{a} = \mathfrak{p}_1$. Ponha $\mathfrak{q} = \mathfrak{p}_2...\mathfrak{p}_n$, daí $Aa \supset \mathfrak{a}\mathfrak{q}$ e $Aa \not\supseteq \mathfrak{q}$ pois n é o menor possível. Assim, existe $b \in \mathfrak{q}$ tal que $b \notin Aa$. Como $\mathfrak{a}\mathfrak{q} \subset Aa$ temos que $\mathfrak{a}b \subset Aa$ e consequentemente $aba^{-1} \subset A$. De acordo com a definição de $\mathfrak{a}'$, isso significa que $ba^{-1} \in \mathfrak{a}'$. Mas, como $b \notin Aa$ temos que $ba^{-1} \notin A$ Assim, $\mathfrak{a}' \neq A$ e consequentemente $\mathfrak{a}'\mathfrak{a} \neq \mathfrak{a}$. Logo, $\mathfrak{a}'\mathfrak{a} = A$ como queríamos provar.

Teorema 2.14 *Seja A um anel de Dedekind e P um conjunto de ideais primos não nulos de A. Então*
(a) Todo ideal fracionário não nulo $\mathfrak{q}$ de A, pode ser unicamente expresso na forma:

$$\mathfrak{q} = \Pi_{\mathfrak{a} \in P} \mathfrak{a}^{n_{\mathfrak{p}(\mathfrak{q})}} \qquad (3)$$

onde, para qualquer $\mathfrak{a} \in P$, $n_{\mathfrak{p}}(\mathfrak{q}) \in \mathbb{Z}$ e para quase todo $\mathfrak{a} \in P$, $n_{\mathfrak{p}}(\mathfrak{q}) = 0$

(b) O monoide dos ideais fracionários não nulos de A é um grupo.

Demonstração: Primeiro provaremos a existência do item (a), isto é, que qualquer ideal fracionário $\mathfrak{q}$ é um produto de potências ($\leq 0\, ou\, \geq 0$) de ideais primos. Existe $d \in A-(0)$ tal que $d\mathfrak{q} \subset A$, isto é, tal que $\mathfrak{q}$ é um ideal inteiro de A, $\mathfrak{q} = (d\mathfrak{q})(Ad)^{-1}$. Sem perda de generalidade, podemos provar (a) para ideais inteiros. Prosseguindo como no Lema 4.3, considere a coleção ϕ dos ideais não nulos em A que não são produto de ideais primos. Suponha que ϕ não é vazia. Como A é Noetheriano, ϕ possui um elemento maximal $\mathfrak{p}$. Então $\mathfrak{p} \neq A$, pois A é produto da coleção vazia de ideais primos. Assim, $\mathfrak{p}$ está contido em um ideal maximal $\mathfrak{a}$, que é um elemento maximal na coleção de ideais não triviais de A que contém $\mathfrak{p}$. Seja $\mathfrak{a}'$ o ideal fracionário inverso de $\mathfrak{a}$. Como $\mathfrak{p} \subset \mathfrak{a}$ temos que $\mathfrak{p}a' \subset \mathfrak{a}\mathfrak{a}' = A$. Como $\mathfrak{a} \supset A$ temos que $\mathfrak{p}\mathfrak{a}' \supset \mathfrak{a}'$. De fato, $\mathfrak{p}\mathfrak{a}' \neq \mathfrak{p}$, pois se $\mathfrak{p}\mathfrak{a}' = \mathfrak{p}$ e $x \in \mathfrak{a}'$ então $x\mathfrak{p} \subset \mathfrak{p}$, $x^n \subset \mathfrak{p}$ para todo n, x é inteiro sobre A e $x \in A$. Mas, isso é impossível, pois $\mathfrak{a}' \neq A$, caso contrário teríamos $\mathfrak{a}' = A$ e $\mathfrak{a}\mathfrak{a}' = \mathfrak{a}$. Pela maximalidade de $\mathfrak{p}$ em ϕ , temos que $\mathfrak{p}\mathfrak{a}' \notin \phi$, assim $\mathfrak{p}\mathfrak{a}' = \mathfrak{a}_1 ... \mathfrak{a}_n$. Multiplicando por $\mathfrak{a}$ temos que $\mathfrak{p} = \mathfrak{a}\mathfrak{a}_1 ... \mathfrak{a}_n$ o que é absurdo, pois $\mathfrak{p} \in \phi$. Logo, todo ideal inteiro de A é produto de ideais primos. Provaremos agora a unicidade em (a). Suponha que $\Pi_{\mathfrak{a}\in P}\mathfrak{a}^{n(\mathfrak{p})} = \Pi_{\mathfrak{a}\in P}\mathfrak{a}^{m(\mathfrak{p})}$, isto é, $\Pi_{\mathfrak{a}\in P}\mathfrak{a}^{n(\mathfrak{p})-m(\mathfrak{p})} = A$. Se $n(\mathfrak{p}) - m(\mathfrak{p}) \neq 0$ para algum ideal primo $\mathfrak{a} \in P$, podemos separar os expoentes positivos e negativos escrever

$$\mathfrak{a}_1^{\alpha_1} ... \mathfrak{a}_r^{\alpha_r} = \mathfrak{a'}_1^{s_1} ... \mathfrak{a'}_s^{s_k} \qquad (4)$$

onde $\mathfrak{a}_i, \mathfrak{a'}_j \in P$, $\alpha_i > 0$ e $\beta_j > 0$, $\mathfrak{a}_i \neq \mathfrak{a'}_j$ para todo i e j. Assim, $\mathfrak{a}_1$ contém $\mathfrak{a'}_1^{\beta_1} ... \mathfrak{a'}_s^{\beta_k}$ pelo Lema 4.3, daí $\mathfrak{a}_1 \supset \mathfrak{a'}_j$, digamos $\mathfrak{a}_1 \supset \mathfrak{a'}_1$ Mas, $\mathfrak{a}_1$ e $\mathfrak{a'}_1$ são ambos maximais, o que implica $\mathfrak{a}_1 = \mathfrak{a}'_1$, o que é uma contradição, pois $\mathfrak{a}_i \neq \mathfrak{a}'_j$ para todo $i\, e\, j$. Finalmente, temos que $\Pi_{\mathfrak{a}\in P}\mathfrak{a}^{-n_p(\mathfrak{q})}$ é o inverso de $\Pi_{\mathfrak{a}\in P}\mathfrak{a}^{n_p(\mathfrak{q})}$, e isto prova (b).

Observação: Temos abaixo algumas fórmulas as quais $n_\mathfrak{p}(\mathfrak{b})$ denota o expoente de $\mathfrak{p}$ na fatoração de $\mathfrak{b}$ em um produto de ideais primos. Veja:

$$(5) \quad n_\mathfrak{p}(\mathfrak{a}\mathfrak{b}) = n_\mathfrak{p}(\mathfrak{a}) + n_\mathfrak{p}(\mathfrak{b})$$
$$(6) \quad \mathfrak{b} \subset A \Leftrightarrow n_\mathfrak{p}(\mathfrak{b}) \geq 0,\ \forall \mathfrak{p} \in P$$
$$(7) \quad \mathfrak{a} \subset \mathfrak{b} \Leftrightarrow n_\mathfrak{p}(\mathfrak{a}) \geq n_\mathfrak{p}(\mathfrak{b}),\ \forall \mathfrak{p} \in P$$
$$(8) \quad n_\mathfrak{p}(\mathfrak{a} + \mathfrak{b}) = min\{n_\mathfrak{p}(\mathfrak{a}), n_p(\mathfrak{b})\}$$
$$(9) \quad n_\mathfrak{p}(\mathfrak{a} \cap \mathfrak{b}) = max\{n_p(\mathfrak{a}), n_p(\mathfrak{b})\}$$

Seja K é um corpo de números, n o seu grau, e A o anel dos inteiros de K. Para simplificar a notação escreveremos $N(x)$ no lugar de $N_{K/\mathbb{Q}}(x)$.

Proposição 2.22 *Seja K um corpo numérico, n seu grau e A o anel dos inteiros de K.*

Se x é um elemento não nulo de A, então $|N(x)| = card(A/Ax)$.
Demonstração: Sabemos que A é um $\mathbb{Z}$-módulo livre de posto n e Ax é um $\mathbb{Z}$-submódulo de A, também de posto n, pois a multiplicação por x implica A em Ax isomorficamente. Pelo Teorema 2.3 existe uma base $\{e_1, ..., e_n\}$ do $\mathbb{Z}$-módulo A e elementos c_i de $\mathbb{N}$ tais que $\{c_1e_1...c_ne_n\}$ é uma base de Ax. Além disso, o grupo abeliano A/Ax é isomorfo ao grupo abeliano finito $\Pi_{i=1}^{n}\mathbb{Z}/c_i\mathbb{Z}$, cuja a ordem é, $c_1...c_n$. Escreva u para a aplicação $\mathbb{Z}$-linear de A em Ax definida por $u(e_i) = c_ie_i$, para $i = 1, ..., n$. Temos que $det(u) = c_1...c_n$, por outro lado, $\{xe_1...xe_n\}$ é também uma base para Ax. Existe assim um automorfismo v do $\mathbb{Z}$-módulo Ax tal que $v(c_ie_i) = xe_i$. Então $det(v)$ é invertível em $\mathbb{Z}$, portanto $det(v) = \pm 1$. Mas, vu é uma multiplicação por x, e seu determinante é, por definição, $N(x)$. Como $det(vu) = det(v)det(u)$ podemos concluir que $N(x) = \pm c_1...c_n = \pm card(A/Ax)$.

Definição: Dado um ideal inteiro não nulo $\mathfrak{a}$ de A, chamamos o número $card(A/a)$ a norma de $\mathfrak{a}$ é denotada por $N(\mathfrak{a})$.

Observação: Note que $N(\mathfrak{a})$ é finita. De fato, se x é um elemento não nulo de $\mathfrak{a}$ então $Ax \subset \mathfrak{a}$ e $A/\mathfrak{a}$ pode ser identificado com um quociente de A/Ax. Assim, $card(A/\mathfrak{a}) \leq card(A/Ax)$, que é finita pela Proposição 5.1. Por outro lado, vemos que para um ideal principal Ay temos $N(Ay) = |N(y)|$.

Proposição 2.23 *Seja K um corpo numérico, n seu grau e A o anel dos inteiros de K. Se $\mathfrak{a}$ e $\mathfrak{b}$ são ideais inteiros não nulos de A, então $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.*
Demonstração: O ideal $\mathfrak{b}$ se fatora em um produto de ideais maximais pelo Teorema 5.3, daí é suficiente mostrar que $N(\mathfrak{am}) = N(\mathfrak{a})N(\mathfrak{m})$ para $\mathfrak{m}$ maximal. Como $\mathfrak{am} \subset \mathfrak{a}$ temos $card(A/\mathfrak{am}) = card(A/\mathfrak{a})card(\mathfrak{a}/\mathfrak{am})$. Assim é suficiente mostrar que $card(\mathfrak{a}/\mathfrak{am}) = card(A/\mathfrak{m})$. Agora $\mathfrak{a}/\mathfrak{am}$ é um A-modulo anulado por $\mathfrak{m}$, o qual pode ser considerado como um espaço vetorial sobre $A/\mathfrak{m}$. Seus subespaços são seus A-submódulos, eles são da forma $\mathfrak{q}/\mathfrak{am}$ onde $\mathfrak{q}$ é um ideal tal que $\mathfrak{am} \subset \mathfrak{q} \subset \mathfrak{a}$. Mas, a fórmula (iii) acima, implica que não existem ideais entre $\mathfrak{am}$ e $\mathfrak{a}$. Portanto, o espaço vetorial $\mathfrak{a}/\mathfrak{am}$ é de dimensão 1 sobre $A/\mathfrak{m}$. Logo, temos que $card(\mathfrak{a}/\mathfrak{am}) = card(A/\mathfrak{m})$.

2.10 Grupo das classes de um ideal.

Vimos que o monoide $I(A)$ dos ideais fracionários não nulo de um anel de Dedekind é um grupo. Os ideais fracionários principais (i.e. aqueles da forma Ax, $x \in K^*$) forma um subgrupo $F(A)$ de $I(A)$ (já que $(Ax)(Ay)^{-1} = Axy^{-1}$). O grupo quociente $C(A) = I(A)/F(A)$ é chamado o grupo das classe de ideais de A. Para que A seja um anel de ideais principais é necessário e suficiente que $C(A)$ consista de único elemento.

2.11 Imersão canônica em corpos de números

Seja K um corpo de números e n o seu grau. Vimos que existem exatamente K-isomorfismo distintos $\sigma_i : K \longrightarrow \mathbb{C}$. Seja $\alpha : \mathbb{C} \longrightarrow \mathbb{C}$ a conjugação complexa. Então, para todo $i = 1, ..., n$, $\alpha \circ \sigma_i = \sigma_j$, $1 \leq j \leq n$, $\sigma_i = \sigma_j$ se e somente $\sigma_i(K) \subset \mathbb{R}$. Seja r_1 o número de índices tais que $\sigma_i(K) \subset \mathbb{R}$. Então $n - r_1$ é um número par, que representaremos por $2r_2$. Podemos escrever

$$r_1 + 2r_2 = n$$

.
Vamos renumerar os $\sigma_i's$ de modo que $\sigma_i(K) \subset \mathbb{R}$ para $1 \leq i \leq r_1$ e $\sigma_{j+r_2}(x) = \overline{\sigma_j(x)}$ para $r_1 + 1 \leq j \leq r_1 + r_2$. Para $x \in K$ definimos

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

Chamaremos σ de imersão canônica de K com $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ e observamos que é um homomorfismo injetivo de anéis. Identificaremos frequentemente $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ com $\mathbb{R}^n$.

Proposição 2.24 *Se M é um $\mathbb{Z}$-submódulo livre de K de posto n e se $(x_i)_{1 \leq i \leq n}$ é uma $\mathbb{Z}$-base de M, então $\sigma(M)$ é um reticulado em $\mathbb{R}^n$, cujo volume é:*

$$v(\sigma(M)) = 2^{-r_2}|det(\sigma_i(x_j))|, 1 \leq i \text{ e } j \leq n$$

Veja a demonstração em [Samuel, P. 2008] proposição 1 da pag. 56

Proposição 2.25 *Seja d o discriminante absoluto de K, Seja A o anel dos inteiros em K, e seja $\mathfrak{a}$ o ideal inteiro nao nulo de A. Então $\sigma(A)$ e $\sigma(\mathfrak{a})$ são reticulados. além disso $v(\sigma(A)) = 2^{-r_2}|d|^{1/2}$ e $v(\sigma(\mathfrak{a})) = 2^{-r_2}|d|^{1/2}N(\mathfrak{a})$*
Veja a demonstração em [Samuel, P. 2008] proposição 2 da pag. 57

2.12 Finitude das classes de ideais de um grupo

Proposição 2.26 *Seja K um corpo de números, n o seu grau, r_1 e r_2, os inteiros definidos acima, d o discriminante de K, e $\mathfrak{a}$ o ideal inteiro não nulo de K. Então $\mathfrak{a}$ contém um elemento não nulo x tal que.*

$$|N_{K/\mathbb{Q}}(x)| \leq (\frac{4}{\pi})^{r_2}\frac{n!}{n^n}|d|^{1/2}N(\mathfrak{a})$$

Veja a demonstração em [Samuel, P. 2008] proposição 1 da pag. 57

Corolário 2.14 *Com as mesma notações, cada classes de ideais de K contem um ideal*

inteiro $\mathfrak{b}$ *tal que.*

$$|N(\mathfrak{b})| \leq (\frac{4}{\pi})^{r_2}\frac{n!}{n^n}|d|^{1/2}$$

Veja a demonstração em [Samuel, P. 2008] corolário 1 da pag. 58

Corolário 2.15 *Seja K um corpo de números, seja n o seu grau, e seja d o discriminante absoluto. Então, para $n \geq 2$*

$$|d| \geq \frac{\pi}{3}(\frac{3\pi}{4})^{n-1}$$

e $n|(log|d|)$ é majorado por uma constante independente de K

Veja a demonstração em [Samuel, P. 2008] corolário 2 da pag. 58

Teorema 2.15 *(Hemite-Minkowski) Para todo corpo numérico $K \neq \mathbb{Q}$, o discriminante absoluto d de K é $\neq \pm 1$.*
Demonstração: Usando o corolário 10.1 da preposição 10.1 nos vemos que $|d| \geq (\pi/3)(3\pi/4)^{n-1}$. Desde $\pi/3 > 1$ e $3\pi/4 > 1$, nós temos $|d| > 1$.

Teorema 2.16 *(Dirichet). Para qualquer corpo de números K, o grupo das classes de ideais é finito.*
Demonstração: Pelo corolário 2.14 da proposição 2.26 , basta mostrar, para cada inteiro positivo q, o conjunto de todos os ideais $\mathfrak{b}$ de K que têm q como sua norma é um conjunto finito. Para tais ideais $\mathfrak{b}$ temos $\text{card}(A/\mathfrak{b}) = q$. Como a ordem de qualquer elemento de um grupo é um divisor da ordem do grupo, temos que para toda classe $a + \mathfrak{b}$ pertencente a $A/\mathfrak{b}$, $q(a + \mathfrak{b}) = 0 + \mathfrak{b} = \mathfrak{b}$. Tomando $a = 1$, temos $q(1 + \mathfrak{b}) = \mathfrak{b}$, isto é, $q + \mathfrak{b} = \mathfrak{b}$ e assim $q \in B$. Assim, os ideais $\mathfrak{b}$ estão entre os que contêm Aq, e portanto so pode existir um número finitos de tais ideais.
Teorema 2.17 *(Hermite) Em $\mathbb{C}$ há apenas um número finito de corpos numéricos com discriminante d.*
Veja a demonstração em [Samuel, P. 2008] teorema 3 da pag. 59.

2.13 O Teorema das unidades

Seja K um corpo de números e seja A o anel dos inteiros em K. Por abuso de linguagem, usamos a expressão "unidades em K"para referir as unidades do anel A. Lembremos que as unidades A formam um grupo sob a multiplicação. Representaremos este grupo por A^*.
Proposição 2.27 *Seja K um corpo de números e seja $x \in K$. Para que x seja uma unidade de K é necessário e suficiente que seja um inteiro de K de norma ± 1*
Demonstração: Se x é unidade em K, então $N(x)$ e $N(x^{-1})$ pertencem a $\mathbb{Z}$. Temos

$N(x)N(x^{-1}) = N(x.x^{-1})$ e assim $N(x) = \pm 1$. Por outro lado, seja x um inteiro de K com norma ± 1. Sua equação característica tem a forma

$$x^n + a_{n-1}x^{n-1} + ... + a_1 x \pm 1 = 0$$

com $a_i \in \mathbb{Z}$. Portanto, $\pm(x^{n-1} + a_{n-1}x^{n-2} + ... + a_1) = x^{-1}$ e, já que x^{-1} é inteiro de K, x é uma unidade de K.

Teorema 2.18 *(Dirichet) Seja K um corpo de números, n o se grau, seja r_1 e r_2 os inteiros já definido acima. Tome $r = r_1 + r_2 - 1$. O grupo A^* é isomorfo a $\mathbb{Z}^r \times G$, onde G é um grupo cíclico finito composto pelas raízes da unidade contidas em K.*

Veja a demonstração em [Samuel, P. 2008] Teorema 1 da pag. 60.

2.14 A decomposição de ideais primos em uma extensão

Nesta seção A denota um anel Dedekind de característica zero, K seus corpo de fração, L uma extensão finita de K de grau n e B o fecho integral de A em L. Lembramos que B também é um anel Dedekind (Teorema 2.2)

Seja $\mathfrak{p}$ um ideal primo não nulo de A. Então $B\mathfrak{p}$ é um ideal de B e é expresso da forma

$$B\mathfrak{p} = \Pi_{i=1}^{q} \mathfrak{B}_i^{e_i} \qquad (1)$$

onde o $\mathfrak{B}_i's$ são os ideais primos distintos de B, os $e_i's$ são inteiros positivos.

Proposição 2.28 *Os $\mathfrak{B}i's$ são precisamente aqueles ideais primos $\mathfrak{D}$ de B tais que $\mathfrak{D} \cap A = \mathfrak{p}$.*

Veja a demonstração em [Samuel, P. 2008] preposição 1 da pag. 71.

A aplicação $f : A/\mathfrak{p} \longrightarrow B/\mathfrak{B}_i$ dada por $f(a+\mathfrak{p}) = a+\mathfrak{B}_i$ é claramente injetiva e portanto $A/\mathfrak{p}$ pode ser identificado como um subanel de $B/\mathfrak{B}_i$ para todo $i = 1, ..., q$. $A/\mathfrak{p}$ e $B/\mathfrak{B}_i$ são corpos, desde que B é um A-modulo do tipo finito (Teor. 7.1), $B/\mathfrak{B}_i$ é um espaço vetorial de dimensão finita sobre $A/\mathfrak{p}$. Denotamos por f_i a dimensão de $B/\mathfrak{B}_i$ sobre $A/\mathfrak{p}$ e chamamos f_i de grau residual de $\mathfrak{B}_i$ sobre A. O expoente e_i em (1) é chamado de índice de ramificação de $\mathfrak{B}_i$ sobre A. Observamos finalmente que $B\mathfrak{p} \cap A = \mathfrak{p}$ e assim $B/B\mathfrak{p}$ é um espaço vetorial de dimensão finita sobre $A/\mathfrak{p}$.

Teorema 2.19 *Com as notações anteriores*

$$\Sigma_{i=1}^{q} e_i f_i = [B/B\mathfrak{p} : A/\mathfrak{p}] = n \qquad (2)$$

Veja a demonstração em [Samuel, P. 2008] Teorema 1 da pag. 71.

Proposição 2.29 *Com as notações anteriores, o anel $B/B\mathfrak{p}$ é isomorfo ao anel $\Pi_{i=1}^{q} B/\mathfrak{B}_i^{e_i}$.*

Demonstração: $\mathfrak{B}_i$ é o único ideal máximo de B que contém $\mathfrak{B}_i^{e_i}$, então $\mathfrak{B}_i^{e_i} + \mathfrak{B}_j^{e_j} = B$ para $i \neq j$
A proposição agora segue de (1) e do Lema 2.2

2.15 O discriminante e ramificação

Com as mesmas notações do paragrafo anterior dizemos que um ideal primo $\mathfrak{p}$ de A se ramifica em (B ou em L) se algum dos seus índices de ramificação e_i é maior que 1. Usando a teoria do discriminante, vamos caracterizar aqueles ideais primos de A que se ramificam em B. Em particular, mostraremos que apenas número finito de ideais primo de A se ramifica em B.

Lema 2.12 *Seja A um anel, seja $B_1, \ldots, B_q$ anéis contendo A que são A-modulo livre do tipo finito, e seja $B = \Pi_{i=1}^{q} B_i$ o produto de anéis. Então $\mathfrak{D}_{B/A} = \Pi_{i=1}^{q} \mathfrak{D}_{B_i/A}$*
Veja a demonstração em [Samuel, P. 2008] lema 1 da pag. 73

Lema 2.13 *Seja B um anel, A um subanel de B e $\mathfrak{a}$ um ideal de A. Suponha que B é um módulo livre sobre A com a base $(x_1, ..., x_n)$. Para $x \in B$ seja $\overline{x}$ a classe residual de x em $B/\mathfrak{a}B$. Então $(\overline{x}_1, ..., \overline{x}_n)$ é a base de $B/\mathfrak{a}B$ sobre $A/\mathfrak{a}$ e*

$$D(\overline{x}_1, ..., \overline{x}_n) = D(\overline{x_1, ..., x_n}) \qquad (1)$$

Demonstração: Seja $x \in B$. Se a matriz da multiplicação por x, com respeito à base $(x_1, ..., x_n)$ é a_{ij} ($a_{ij} \in A$), então para a matriz da multiplicação por $\overline{x}$ em relação à base $(\overline{x}_1, ..., \overline{x}_n)$ é $\overline{a}_{ij}$. Então, $Tr(\overline{x}) = \overline{Tr(x)}$. Tomando $x = x_i x_j$, obtemos $Tr(\overline{x_i x_j}) = \overline{Tr(x_i x_j)}$, e (1) segue tomando determinantes.

Lema 2.14 *Seja K um corpo finito ou de característica zero. Seja L uma K-algébra (comutativa) de dimensão finita. Para que L seja reduzido, é necessário e suficiente $\mathfrak{D}_{L/K} \neq (0)$*
Veja a demonstração em [Samuel, P. 2008] lema 3 pagina 73

Definição: Seja K e L corpos de números com $K \subset L$. Seja A e B os anéis de inteiros de K e L respectivamente. O discriminante (ideal) de B sobre A (ou de L sobre K) é o ideal de A gerado pelos discriminantes de base de L sobre K que estão contidas em B. Notação $\mathfrak{D}_{B/A}$ ou $\mathfrak{D}_{L/K}$.

Observação: Se $(x_1, ..., x_n)$ é uma base de L sobre K contida em B, então $Tr_{L/K}(x_i x_j) \in$

A assim $D(x_1, ..., x_n) \in A$. Portanto $\mathfrak{D}_{B/A}$ é um ideal inteiro de A

Observação: Quando B é um A-modulo livre (ex. se A for principal) nos já definimos o $\mathfrak{D}_{B/A}$ como o ideal gerado por $D(e_1, ..., e_n)$ onde $(e_1, ..., e_n)$ é uma base do A-modulo B. Nossa antiga definição coincide com a dada acima, uma vez para qualquer base (x_i) de L sobre K contida B vemos que $x_i = \Sigma_j a_{ij} e_j$ com $a_{ij} \in A$. Portanto

$$D(x_1, ..., x_n) = det(a_{ij})^2 D(e_1, ..., e_n)$$

Teorema 2.20 *Com as mesma notações anteriores, para que um ideal primo* $\mathfrak{p}$ *de* A *se ramifique em* B*, é necessário e suficiente que contenha o discriminante* $\mathfrak{D}_{B/A}$*. Existem apenas finitos ideais principais de* A *que ramificam em* B
Veja a demonstração em [Samuel, P. 2008] Teorema 1 pagina 74

2.16 Lei da reciprocidade quadrática

Dado um número primo p e um inteiro d relativamente primo com p como já introduzido que $''d$ é um resíduo quadrático mod p'' (resp. $''d$ não é um resíduo mod p'') como significando que a classe de resíduos de d mod p é um quadrado (resp. não é um quadrado) em F_p^*. Agora definimos o símbolo Legendre da seguinte forma:

$$\begin{cases} (\frac{d}{p}) = +1, \text{se } d \text{ é um resíduo quadrático mod } p \\ (\frac{d}{p}) = -1, \text{se } d \text{ não é um resíduo quadrático mod } p. \end{cases}$$

Entende-se que $(\frac{d}{p})$ é definido apenas para inteiros d que são relativamente primos para p, i.e, $d \in \mathbb{Z} - p\mathbb{Z}$.

Proposição 2.30 *O grupo multiplicativo* F_p^* *sendo cíclico da mesma ordem* $p-1$*, os quadrados em* F_p^* *formam um subgrupo* $(F_p^*)^2$ *de índice 2, e* $F_p^*/(F_p^*)^2$ *é isomorfo a* $\{+1, -1\}$
Demonstração: Claramente, o símbolo Legendre representa a composição dos seguintes homomorfismos:

$$\mathbb{Z} - p\mathbb{Z} \longrightarrow F_p^* \longrightarrow F_p^*/(F_p^*)^2 \backsimeq \{+1, -1\}$$

Como consequência, existe a fórmula:

$$(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p}), \qquad a, b \in \mathbb{Z} - p\mathbb{Z}$$

.

Proposição 2.31 *(Critério de Euler) Se p é um primo impar e se* $a \in \mathbb{Z} - p\mathbb{Z}$*, então*

$$(\frac{a}{p}) \equiv a^{(p-1)/2} \, (mod \, p)$$

Demonstração: Escreva w para a raiz primitiva mod p. Então $a \equiv w^j \, (mod \, p)$, com $0 \leq j \leq p-1$, uma vez que a classe de resíduos $\overline{w}$ de w gera F_p^*. Claramente, a é um resíduo quadrático se e somente se j for o mesmo. Portanto, $(\frac{a}{p}) = (-1)^j$. Por outro lado, F_p^* contém apenas um elemento de ordem 2; este elemento pode ser escrito como $\overline{w}^{(p-1)/2}$ ou -1. Em $\mathbb{Z}$, nos temos $-1 \equiv w^{(p-1)/2} \, (mod \, p)$. Assim,

$$(\frac{a}{p}) = (-1)^j \equiv w^{j(p-1)/2} \equiv a^{(p-1)/2} (mod \, p)$$

.

Teorema 2.21 *("Lei de reciprocidade quadrática de Legendre-Gauss") Se p e q são números distintos primos impares, então*

$$(\frac{p}{q})(\frac{q}{p}) = (-1)^{(p-1)(q-1)/4}$$

Veja a demonstração em [Samuel, P. 2008] teorema 1 pagina 78

Proposição 2.32 *("O complemento da formula") Se p é um primo impar, então*
(a) $(\frac{-1}{p}) = (-1)^{(p-1)/2}$ *e*

(b) $(\frac{2}{p}) = (-1)^{(p^2-1)/8}$

Veja a demonstração em [Samuel, P. 2008] preposição 2 pagina 80

3 CORPOS QUADRÁTICOS

Definição 3.1 *Qualquer extensão de grau dois sobre o corpo $\mathbb{Q}$ dos números racionais é chamado um corpo quadrático.*

Proposição 3.1 *Todo corpo quadrático é da forma $\mathbb{Q}(\sqrt{d})$ onde d é um inteiro livre de quadrado, ou seja d não é divisível por quadrados diferentes de 1, mais precisamente $d = -1$ ou d é igual a mais ou menos o produto de primos distintos*

Demonstração: Seja K um corpo quadrático, qualquer elemento $x \in K - \mathbb{Q}$ é de grau 2 sobre $\mathbb{Q}$, assim é um elemento primitivo de K, isto é $K = \mathbb{Q}[x]$ e $(1, x)$ é uma base de K sobre $\mathbb{Q}$. Seja $F(X) = X^2 + bX + c$ onde $b, c \in \mathbb{Q}$ o polinômio minimal de tal elemento $x \in K$. Resolvendo a equação quadrática $x^2 + bx + c = 0$ obtemos $x = \frac{-b}{2} \pm \frac{1}{2}\sqrt{b^2 - 4c}$, como $\frac{-b}{2}$ e $\frac{1}{2}$ ja pertence a $\mathbb{Q}$, temos que $K = \mathbb{Q}(\sqrt{b^2 - 4c})$. Agora $b^2 - 4c$ é um número racional $\frac{u}{v} = \frac{uv}{v^2}$ com u e $v \in \mathbb{Z}$. Daí, como $\frac{1}{v^2}$ está em $\mathbb{Q}$ temos que $K = \mathbb{Q}(\sqrt{uv})$. Com efeito é possível escrever $K = \mathbb{Q}(\sqrt{d})$ onde d é um inteiro livre de quadrado, isto é, d é mais ou menos o produto de primos distintos.

Observação: O elemento $\sqrt{d}$ é a raiz do polinômio irredutível $X^2 - d$. Esse elemento $\sqrt{d}$ possui um conjugado em K e este será denotado por $-\sqrt{d}$

Observação: Existe um automorfismo σ de K que leva $\sqrt{d}$ em $-\sqrt{d}$. Daí, para qualquer elemento de K da forma $a + b\sqrt{d}$ com a,$b \in \mathbb{Q}$ temos

$$\sigma(a + b\sqrt{d}) = a - b\sqrt{d}.$$

Teorema 3.1 *Seja $K = \mathbb{Q}(\sqrt{d})$ um corpo quadrático com $d \in \mathbb{Z}$ livre de quadrado, portanto não congruente a zero modulo 4.*
(a) Seja $d \equiv 2 \, mod \, 4$ ou $d \equiv 3 \, mod \, 4$, o anel A dos inteiros de K consiste de todos elementos da forma $a + b\sqrt{d}$ com $a, b \in \mathbb{Z}$
(b) Se $d \equiv 1 \, mod \, 4$, A consiste de todos elementos da forma $\frac{1}{2}(u + v\sqrt{d})$ com $u, v \in \mathbb{Z}$ de mesma paridade.

Demonstração: Vimos anteriormente que um automorfismo σ de K que leva $\sqrt{d}$ em $\sqrt{-d}$. Se $x \in A$ então existe $a_i \in \mathbb{Z}$, $i = 0, 1, ..., n-1$ tais que $x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = 0$, portanto $\sigma(x)^n + a_{n-1}\sigma(x)^{n-1} + ... + a_0 = 0$, isto é, $\sigma(x) \in A$. Como A é um anel $x + \sigma(x) \in A$ e $x\sigma(x) \in A$. Mas, se $x = a + b\sqrt{d}$, com $a, b \in \mathbb{Q}$ então o pelo observação acima $\sigma(a + b\sqrt{d}) = (a - b\sqrt{d})$ temos:

$$x + \sigma(x) = a + b\sqrt{d} + \sigma(a + b\sqrt{d}) = a + b\sqrt{d} + a - b\sqrt{d} = 2a$$

$$x\sigma(x) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2 \in \mathbb{Q}.$$

Como $\mathbb{Z}$ é um domínio de integralmente fechado, segue-se do lema 2.6 que

$$2a \in A \cap \mathbb{Q} = \mathbb{Z}$$

e

$$a^2 - db^2 \in A \cap \mathbb{Q} = \mathbb{Z}$$

. As condições acima são necessária para que $x = a + b\sqrt{d}$ seja um inteiro sobre $\mathbb{Z}$. E são suficiente, pois x é raiz de $x^2 - 2ax + a^2 - db^2 = 0$ que pertence a $\mathbb{Z}[x]$. Ainda pela estas condições podemos escrever que $4(a^2 - db^2) \in \mathbb{Z}$ isto é, $(2a)^2 - d(2b)^2 \in \mathbb{Z}$. Como $2a \in \mathbb{Z}$ temos que $(2a)^2 \in \mathbb{Z}$ e então concluímos que $d(2b)^2 \in \mathbb{Z}$). Por outro lado, d é livre de quadrado. Assim se $2b$ não fosse inteiro, o denominador não teria um fator primo p. Esse fator primo teria que aparecer p^2 no denominador de $(2b)^2$. Multiplicando por d não valeria $(2b)^2$ em $\mathbb{Z}$, pois $p^2 \nmid d$. Logo, podemos concluir que $2b$ é um número inteiro. Resumindo podemos tomar $a = \dfrac{u}{2}$ e $b = \dfrac{v}{2}$ com $u, v \in \mathbb{Z}$. Daí pelas condições ja vistas acima temos que:

$$u^2 - dv^2 \in 4\mathbb{Z}.$$

Se v é par então u é par pois, $v = 2k$ implica $u^2 = 4t - 4dk^2 = 4(t - dk^2)$ e daí $u^2 \equiv 0\, mod\, 4$ e assim u é par. Se v é impar então u também é impar, pois $v = 2k + 1$ implica $u^2 = 4t + 4(2k + 1)^2 = 4t + 4k^2 + 4k + 1$ e daí $u^2 \equiv 1\, mod\, 4$ e assim u é impar. Portanto concluímos que u e v tem a mesma paridade.

Como $u^2 - dv^2 \in 4\mathbb{Z}$, temos que $u^2 - dv^2 \equiv\, mod\, 4$, isto é, $u^2 \equiv\, dv^2\, mod\, 4$.

Se $d \equiv 2\, mod\, 4$, temos que $u^2 \equiv 2v^2\, mod\, 4$. Então, devemos ter u e v pares.

Se $d \equiv 3\, mod\, 4$ temos $u^2 \equiv 3v^2\, mod\, 4$. Então, neste caso devemos ter também u e v pares. Portanto se $d \equiv 2\, mod\, 4$ ou $d \equiv 3\, mod\, 4$, o anel A dos inteiros de K consiste de todos elementos da forma $a + b\sqrt{d}$ com $a, b \in \mathbb{Z}$.

Se $d \equiv 1\, mod\, 4$ temos que $u^2 \equiv 1\, (mod\, 4)$. Então, neste caso devemos ter u e v ambos pares. Portanto se $d \equiv 1\, mod\, 4$, A consiste de todos elementos da forma $\dfrac{1}{2}(u + v\sqrt{d})$ com $u, v \in \mathbb{Z}$ de mesma paridade.

observação 3: No caso que $d \equiv 2\, mod\, 4$ ou $d \equiv 3\, mod\, 4$, $(1, \sqrt{d})$ é uma base para A como $\mathbb{Z}$-modulo. Se $d \equiv 1\, mod\, 4$ temos que $(1, \dfrac{1}{2}(1 + \sqrt{d}))$ é uma base para $\mathbb{Z}$-modulo A. De fato por (b) 1, $\dfrac{1}{2}(1 + \sqrt{d}) \in A$. Para mostra, que $\dfrac{1}{2}(u + v\sqrt{d})$ (com $u, v \in \mathbb{Z}$ de

mesma paridade) é expresso como combinação $\mathbb{Z}$-linear de 1 e $\frac{1}{2}(1+\sqrt{d})$, basta ver que $\frac{1}{2}(u+v\sqrt{d}) = \frac{u}{2}+\frac{v}{2}\sqrt{d}+\frac{v}{2}-\frac{v}{2} = (\frac{u}{2}-\frac{v}{2})1+v\frac{1}{2}(1+\sqrt{d})$. Logo $\frac{1}{2}(u+v\sqrt{d})$ é inscrito como combinação linear de 1 e $\frac{1}{2}(1+\sqrt{d})$.

Observação: Se $d>0$, $\mathbb{Q}(\sqrt{d})$ é chamado corpo quadrático real. Se $d<0$, então $\mathbb{Q}(\sqrt{d})$ é chamado corpo quadrático imaginário.

3.1 Unidades em corpos quadráticos imaginários

Seja K um corpo quadrático imaginário. Então $r_1 = 0$, $2r_2 = 2$, $r_2 = 1$, $r_1 + r_2 - 1 = 0$. Assim, as únicas unidades em K são as raízes da unidade contidas em K, que é um grupo cíclico finito (Teorema 10.1).

Seja $K = \mathbb{Q}[\sqrt{-m}]$, onde m é um inteiro positivo livre de quadrado. Lembrando que as unidades de K são números inteiros de norma ± 1 (proposição 10.1).

(1) Se $m \equiv 1(mod\,4)$ ou $m \equiv 2(mod\,4)$, o anel dos inteiros de K e da forma $\mathbb{Z}+\mathbb{Z}\sqrt{-m}$ (Teorema 3.1). Para $x = a+b\sqrt{-m}$ com $a, b \in \mathbb{Z}$, temos $N(x) = a^2+mb^2 \geq 0$. Para que x seja uma unidade, devemos ter $a^2+mb^2 = 1$. Se $m \geq 2$, Isso implica que $b = 0$ e $a = \pm 1$, assim $x = \pm 1$. Se $m = 1$, além da solução $x = \pm 1$, há a solução $a = 0$, $b = \pm 1$, i.e. $x = \pm i$ (com $i^2 = -1$).

(2) Se $m \equiv 3\,(mod\,4)$ o anel dos inteiros de K é da forma $\mathbb{Z}+\mathbb{Z}[(1+\sqrt{-m})/2]$ (Teorema 3.1). Para $x = a+(b/2)(1+\sqrt{-m})$ com $(a,\, b \in \mathbb{Z})$, temos $N(x) = (a+b/2)^2 + mb^2/4$. Para que x seja uma unidade devemos ter $(2a+b)^2 + mb^2 = 4$. Se $m \geq 7$, Isso implica que $b = 0$, assim $4a^2 = 4$, $a = \pm 1$, $x = \pm 1$. Se $m = 3$, então $b = \pm 1$ e $(2a \pm 1) = \pm 1$ o que implicam as soluções adicionais $x = \frac{1}{2}(\pm 1 \pm \sqrt{-3})$ (Os sinais são independentes).

Resumindo, provamos os seguintes resultados:

Proposição 3.2 *Se K é um corpo quadrático imaginário, o grupo G das unidades em K é composto das raízes quadradas das unidades $+1$ e -1, exceto nos dois casos seguintes:*
(1) Se $K = \mathbb{Q}[i]\,(i^2 = 1)$, G é composto de quatro raízes da unidade i, -1, -1,1
(2) Se $K = \mathbb{Q}[\sqrt{-3}]$, G é composto de seis raízes da unidade: $[(1+\sqrt{-3})/2]^j$, $j = 0, 1, \ldots, 5$

3.2 Unidades em corpos quadráticos reais

Esta seção será consideravelmente mais interessante do que a anterior.

Seja K quadrático real. Com as notações usuais, temos $r_1 = 2$ e $r_2 = 0$, assim $r = r_1 + r_2 - 1 = 1$. O teorema 10.1 implica que o grupo de unidades de K é isomórfico ao produto de $\mathbb{Z}$ com o grupo de raízes da unidade contida em K. Como K admite uma

imersão em $\mathbb{R}$, as únicas raízes da unidade em K são ± 1. Assim, temos:

Proposição 3.3 *As unidades positivas de um corpo quadrático real $K \subset \mathbb{R}$ formam um grupo isomorfo a $\mathbb{Z}$.*

Este grupo contém um e único gerador maior do que um, o qual chamamos de unidade fundamental de K

Seja $K = \mathbb{Q}[\sqrt{d}]$, onde $d \geq 2$ é um inteiro livre de quadrado, e seja $x = a + b\sqrt{d}$, com a, $b \in \mathbb{Q}$ uma unidade de K. Os números x, x^{-1}, $-x$ e $-x^{-1}$ são unidades de K e como $N(x) = (a+b\sqrt{d})(a-b\sqrt{d}) = \pm 1$ (proposição 11.1), estes quatro números são $\pm a \pm b\sqrt{d}$. Para $x \neq \pm 1$ apenas um dos quatro números x, x^{-1}, $-x$ e $-x^{-1}$ é maior do que um, e é o maior dos quatro. Assim, as unidades maiores do que um de K são as da forma $a + b\sqrt{d}$, $a, b \in \mathbb{Z}$ com $a > 0$, $b > 0$.

(a) Suponha primeiro que $d \equiv 2\,(mod\,4)$ ou $d \equiv 3\,(mod\,4)$. Neste caso, anel de inteiros de K é da forma $\mathbb{Z} + \mathbb{Z}\sqrt{d}$ (Teorema 3.1). Como as unidades de K são inteiros de norma ± 1 (proposição 11.1), as unidades maiores que um de K são os números da forma $a + b\sqrt{d}$ com $a, b \in \mathbb{Z}$ e $a > 0$, $b > 0$ tal que

$$a^2 - db^2 = \pm 1 \qquad (1)$$

Observamos que as soluções "em números naturais" (a, b) da equação (1) (chamada equação de Pell-Fermat) São obtidos da seguinte forma: tome a unidade fundamental $a_1 + b_1\sqrt{d}$ de K e coloque

$$a_n + b_n\sqrt{d} = (a_1 + b_1\sqrt{d})^n\,, n \geq 1 \qquad (2)$$

A lista de sequência (a_n, b_n) de todas as soluções da equação (1)

Observações:(1) Segue-se (2) que $b_{n+1} = a_1 b_n + b_1 a_n$. Já que, a_1, b_1, a_n e b_n são todos são positivos, a sequência (b_n) é estritamente crescente. Assim, para calcular explicitamente a unidade fundamental $a_1 + b_1\sqrt{d}$ basta escrever a sequencia (db^2) para $b \in \mathbb{N}$, $b \geq 1$ e para parar no primeiro números db_1^2 desta sequência que difere por um quadrado a_1^2 de ± 1. Então $a_1 + b_1\sqrt{d}$ é a unidade fundamental de K. Por exemplo, se $d = 7$, a sequencia db^2 é 7, 28, $63 = 64 - 1 = 8^2 - 1$, então, tomando $b_1 = 3$ e $a_1 = 8$, nós vemos que $8 + 3\sqrt{7}$ é a unidade fundamental de $\mathbb{Q}[\sqrt{7}]$. Vemos de forma semelhante que as unidades fundamentais de $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$ e $\mathbb{Q}[\sqrt{6}]$ são $1 + \sqrt{2}$, $2 + \sqrt{3}$ e $5 + 2\sqrt{6}$.

Observação:(2) Se a unidade fundamental for de norma um, a sequência (a_n, b_n) de soluções apenas para a equação $(I')\,a^2 - db^2 = 1$; neste caso, a equação $(I'')\,a^2 - db^2 = -1$ não tem solução em números naturais. Se a unidade fundamental tem norma -1, a solução

de (I') compreende a sequência (a_{2n}, b_{2n}) e as de (I'') a sequência (a_{2n+1}, b_{2n+1})
O primeiro caso ocorre quando $d = 3$, 6 ou 7, o segundo quando $d = 2$ ou $3 + \sqrt{10}$ é a unidade fundamental em $\mathbb{Q}[\sqrt{10}]$.
(b) suponha agora que $d \equiv 1\,(mod\,4)$. Os inteiros de $K = \mathbb{Q}[\sqrt{d}]$ são os números $\frac{1}{2}(a + b\sqrt{d})$ com $a, b \in \mathbb{Z}$ da mesma paridade (Teorema 3.1). Consequentemente, se $\frac{1}{2}(a + b\sqrt{d})$ é uma unidade de K, devemos ter

$$a^2 - db^2 = \pm 4 \qquad (3)$$

Reciprocamente, se (a, b) é uma solução inteira de (3), então $\frac{1}{2}(a + b\sqrt{d})$ é um número inteiro de K (Seu traço é uma e sua norma, por (3), é ± 1) e, portanto, uma unidade de K. Como em (a), escrevendo $a_1 + b_2\sqrt{d}$ para a unidade fundamental de K, vemos que as soluções em pares de números naturais (a, b) de (3) compreender os valores da sequência (a_n, b_n) com $(n \geq 1)$ definidos pela configuração

$$a_n + b_n\sqrt{d} = 2^{1-n}(a_1 + b_1\sqrt{d})^n \qquad (4)$$

O cálculo de $a_1 + b_1\sqrt{d}$ pode ser realizado como em (a). Por exemplo, a unidade fundamental de $\mathbb{Q}[\sqrt{5}]$, $\mathbb{Q}[\sqrt{13}]$ e $\mathbb{Q}[\sqrt{17}]$ são $\frac{1}{2}(1 + \sqrt{5})$, $\frac{1}{2}(3 + \sqrt{13})$ e $4 + \sqrt{17}$; estas três unidades têm norma -1. Para a escolha do sinal ± 1 em (3), temos resultados semelhantes aos obtidos em (a)
Observação: No caso $d \equiv 1\,(mod\,4)$ a solução da equação de Pell-Fermat

$$a^2 - db^2 = \pm 1 \qquad (5)$$

Correspondem a unidades $a + b\sqrt{d}$ $(com\, a, b > 0)$ que pertencem ao anel $B = \mathbb{Z}[\sqrt{d}]$. Este anel B é um subanel do anel A dos inteiros de K e as unidades positivas de B formam um subgrupo G do grupo das unidades positivas de A. Seja $u = \frac{1}{2}(a + b\sqrt{d})$ a unidade fundamental de K. Se a e b são ambos pares, então $u \in B$, de modo que G consiste das potência de u (Este é o caso, por exemplo, quando $d = 17$). Se a e b são ambos ímpares, então $u^3 \in B$. (Para ver esta nota que $8u^3 = a(a^2 + 3b^2d) + b(3a^2 + b^2d)\sqrt{d}$). Já que $a^3 - b^2d = \pm 4$, $a^2 + 3b^2d = 4(b^2d \pm 1)$, que é um múltiplo de 8, uma vez que b e d são ímpares. Similarmente $3a^2 + b^2d = 4(a^2 \pm 1)$, que é novamente, porque a é impar, um múltiplo de 8. Nesse caso, G é composto por potência de u^3 $(u^2 \notin B$, de outra forma $u = u^3/u^2 \in B)$. Isso acontece, por exemplo, quando $d = 5$ (resp. $d = 13$), nesse caso $u^3 = 2 + \sqrt{5}$ (resp. $u^3 = 18 + 5\sqrt{13}$).

3.3 A decomposição de números primos em corpos quadrático

Seja $d \in \mathbb{Z}$ livre de quadrado, seja L o corpo quadrático $\mathbb{Q}[\sqrt{d}]$. Seja B o anel do inteiros de L, e seja p um número primo. Vamos estudar a fatoração do ideal pB em um produto de ideais primos de B
A formula $\Sigma_{i=1}^{q} e_i f_i = 2$ (Teorema 13.1) implica $q \leq 2$ e as seguintes possibilidades:
(a) $q = 2$, $e_1 = e_2 = 1$, $f_1 = f_2 = 1$, neste caso dizemos que p se decompõe em L
(b) $q = 1$, $e_1 = 1$, $f_1 = 2$; Neste caso, dizemos que p permanece primo em L
(c) $q = 1$, $e_1 = 2$, $f_1 = 1$; Neste caso dizemos que p se ramifica em L

Vamos primeiro considerar o caso em que p é impar. Nós sabemos que $B = \mathbb{Z} + \mathbb{Z}\sqrt{d}$ ou $B = \mathbb{Z} + \mathbb{Z}[(1+\sqrt{d})/2]$, dependendo de d. Mas, se passamos para as classes resíduo de B modulo Bp, vemos no segundo caso que $a + b[(1+\sqrt{d})/2]$ com b impar é congruente com $a + (b+p)[1+\sqrt{d}/2]$, que pertence a $B = \mathbb{Z} + \mathbb{Z}\sqrt{d}$. Portanto, para qualquer d, temos $B/Bp \cong (\mathbb{Z} + \mathbb{Z}\sqrt{d})/(p)$. Também vemos isso

$$\mathbb{Z} + \mathbb{Z}\sqrt{d} \cong \mathbb{Z}[X]/(X^2 - d)$$

assim

$$B/Bp \cong \mathbb{Z}[X]/(p, X^2 - d) \cong (\mathbb{Z}[X]/(p)/(X^2 - d)) \cong F_p[X]/(X^2 - \overline{d})$$

onde $\overline{d}$ denota a classe resíduo do d módulo p. Agora a afirmação de que p se decompõe (respectivamente, permanece primo, ramifica) na interpretação: B/Bp é o produto de dois corpos (respectivamente, é um corpo, contém elementos nilpotentes). Em outras palavras, o polinômio $X^2 - \overline{d} \in F_p$ é produtos de dois polinômios lineares (respectivamente, é irredutível, é um quadrado). Isso acontece se $\overline{d}$ é um quadrado não-nulo em F_p (respectivamente não é um quadrado em F_p, é zero em F_p). Quando d é quadrado não nulo em F_p (respectivamente não é um quadrado em F_p), nós dizemos que d é um resíduo quadrático (respectivamente, não resíduo) modulo p.

Agora considere o caso $p = 2$. Se $d \equiv 2\,(mod\,4)$ ou $d \equiv 3\,(mod\,4)$, então $B = \mathbb{Z} + \mathbb{Z}\sqrt{d}$, e assim, como acima, temos $B/2B \cong F_2[X]/(X^2+1)$. Nesse caso X^2 é igual a X^2 ou a $X^2 + 1 = (X+1)^2$, sendo assim, em qualquer caso, um quadrado. Portanto 2 se ramifica em B. Se $d \equiv 1\,(mod\,4)$, $(1+\sqrt{d})/2$ tem $X^2 - X - (d-1)/4$ como seu polinômio minimal, e então, como acima, $B/2B \cong [F_2[X]/X^2 - X - \delta]$, onde δ é a classe resíduo modulo 2 de $(d-1)/4$. Para $d \equiv 1\,(mod\,8)$, $\delta = 0$ e $X^2 - X - \delta = X(X-1)$, de modo que 2 se decompõe. Para $d \equiv 1\,(mod\,8)$, $\delta = 1$ e $X^2 - X - \delta = X^2 + X + 1$, que é irredutível em $F_2[X]$, então 2 permanecem primo.
Em resumo, provamos o seguinte:

Proposição 3.4 *Seja $L = \mathbb{Q}[\sqrt{d}]$, o corpo quadrático associado ao inteiro livre quadrado d.*
(a) Os primos impares p para os quais d é resíduo quadrado mod p se decompõe em L. O mesmo acontece com o primo 2, se $d \equiv 1\,(mod\,8)$.
(b) Os primos impares p para os quais d não é um resíduo quadrado mod p permanecem primos em L, o mesmo acontece com o primo 2, se $d \equiv 5\,(mod\,8)$
(c) Os divisores primos impares de d se ramifica em L. O mesmo acontece com o primo 2 se $d \equiv 2\,(mod\,4)$ ou $d \equiv 3(mod\,4)$

4 ALGUNS RESULTADOS SOBRE O GRUPO DAS CLASSES DOS CORPOS QUADRÁTICOS

Neste capítulo, vamos provar o resultado principal contido no artigo, e que foi utilizado como referência das técnicas na sua demonstração. Primeiramente, veremos alguns resultados importantes para o entendimento.

Teorema 4.1 *Para cada inteiro $n \geq 1$, existem infinitos corpos quadráticos imaginários com grupo de classes de ideais contendo um subgrupo isomorfo a $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.*

Esse artigo é do YOSHIHIKO YAMAMOTO (Received September 8, 1969). Agora estenderemos o resultado, mostraremos que existem infinitos corpos quadráticos imaginários com o grupo das classes de ideias contendo um subgrupo isomorfo a $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, e além disso existem infinitos corpos quadráticos reais contendo um subgrupo isomorfo a $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Seja K um corpo de números quadrático com o discriminante D, assuma $D \neq -3$ e $D \neq -4$ para simplificar nosso argumento a seguir. Então, seja σ um automorfismo não trivial de K sobre $\mathbb{Q}$. Defina ϵ por $\epsilon = \begin{cases} a \text{ unidade fundamental de K se } D > 0 \\ 1 \text{ se } D < -4 \end{cases}$.

Enunciaremos alguns lemas necessários nessa demonstração. A demonstração pode ser encontrada em YAMAMOTO (1970) . Para uma melhor compreensão apresentamos a prova de cada um deles abaixo.

Lema 4.1 *Sejam x, y, z as soluções em $\mathbb{Z}$ da equação Diofantina*

$$X^2 - Y^2 D = 4Z^n \tag{1}$$

satisfazendo $(x, z) = 1$. Então existe um ideal (ideal inteiro) $\mathfrak{a}$ de K tal que:
(a) $\left(\frac{x + y\sqrt{D}}{2}\right) = \mathfrak{a}^n$
(b) $\mathfrak{a}$ e $\mathfrak{a}^\sigma$ são relativamente primos, onde (α) denota o ideal principal em K gerado por um elemento α de K.

Demonstração: Seja $\alpha = \frac{x + y\sqrt{D}}{2}$ então α é um inteiro em K pois, de (1), temos que $\alpha + \alpha^\sigma = x$ e $\alpha.\alpha^\sigma = z^n$. Temos assim $(\alpha)(\alpha^\sigma) = (z)^n$. Por outro lado temos que $(\alpha, \alpha^\sigma) = 1$, já que $x, z^n \in (\alpha, \alpha^\sigma)$ e $(x, z) = 1$. Decompondo o ideal (z) num produto de ideais primos em K, obtemos $(\alpha) = \mathfrak{a}^n$ para algum ideal inteiro $\mathfrak{a}$.
A condição (b) segue de $(\alpha, \alpha^\sigma) = 1$

Seja p um fator primo de n. Tome outro número l primo tal que

$$l \equiv 1(mod\, 2p) \tag{2}$$

de modo que -1 é uma p-ésima potência $mod\, l$ (i.e $-1 \equiv x^p mod\, l$)
Suponha que temos uma solução x, y, z da equação (1) satisfazendo
(i) $(x, z) = 1$
(ii) l/z
(iii) x não é a p-ésima potência $mod\, l$.
Como x, y, z é solução da equação (1), temos que $z^n = \dfrac{x^2 - y^2 D}{4}$, mais l/z, então l/z^n, daí $\dfrac{x^2 - y^2 D}{4} \equiv 0\,(mod\, l)$, isso implica que $x^2 \equiv y^2 D\,(mod\, l)$, além disso temos que $(y, l) = 1$, pois caso não fosse primos entre si, l seria um múltiplo de y, i.e, $y = lk$ isso implica $y \equiv 0(mod\, l)$ e consequentemente $x^2 \equiv y^2 D \equiv D(mod\, l)$, então $x^2 \equiv 0(mod\, l)$, assim l/x^2, como l é primo, temos que l/x, mas por hipótese l/z, portanto $l/(x, z) = 1$, absurdo. Conclusão, $x^2.(y^2)^{-1} \equiv D(mod\, l)$ e portanto D é um resíduo quadrático mod l.

$$\left(\frac{D}{l}\right) = 1 \tag{3}$$

Onde o lado esquerdo é o símbolo de Legendre. Pela lei de decomposição dos primos temos $(l) = \tau\tau^\sigma$ onde τ e τ^σ são ideais primos conjugados distintos em A, onde A é o anel dos inteiros de K.
Seja $\alpha = \dfrac{x + y\sqrt{D}}{2}$, temos $\alpha^\sigma = \dfrac{x - y\sqrt{D}}{2}$ e daí $\alpha.\alpha^\sigma = \dfrac{x + y\sqrt{D}}{2}.\dfrac{x - y\sqrt{D}}{2} = \dfrac{x^2 - Dy^2}{4} = z^n$. Logo $(\alpha)(\alpha^\sigma) = (z)^n$, como l/z e $(l) = \tau\tau^\sigma$ temos que $\tau\tau^\alpha/(\alpha)(\alpha^\sigma)$.
Portanto, podemos supor que $\tau/(\alpha^\sigma)$. Porem, $\tau \nmid (\alpha)$ pois, pelo lema acima, (α) e (α^σ) são relativamente primos. Então temos o seguinte:
Lema 4.2 *Se ϵ é a p-ésima potência resíduo modτ, então o ideal (α) não é a p-ésima potência de qualquer ideal principal em K.*
Demonstração: Como $\alpha^\sigma \in \tau$, obtemos que $x \equiv y\sqrt{D}\,(mod\, \tau)$ e consequentemente $\alpha \equiv x\,(mod\, \tau)$. Portanto α é a p-ésima potência não resíduo mod τ, pois o corpo das classe de resíduo mod τ é canonicamente isomorfo ao corpo principal $\mathbb{Z}/l\mathbb{Z}$. Assuma $(\alpha) = (\beta)^p$ com o ideal principal β em K. Como α é um inteiro em K, β é um inteiro em K. Temos

$$\alpha = \pm\epsilon^k \beta^p \tag{4}$$

para algum $k \in \mathbb{Z}$. Assim segue de $\alpha = \pm\epsilon^k\beta^p$ e da suposição do lema que α é a p-ésima potência de resíduo mod τ. Isto é uma contradição e daí segue-se o lema.

Seja

$$n = p_1^{e_1} p_2^{e_2} ... p_s^{e_s}$$

a decomposição de fatores primo de n. Para cada i $(1 \leq i \leq s)$, fixamos um número primo l_i satisfazendo

$$l_i \equiv 1 (mod\, 2p_i) \tag{5}$$

Suponha que temos uma solução x, y, z da equação (1), satisfazendo as condições:
(i)' $(x, z) = 1$
(ii)' l_i/z, para $i = 1, 2, ..., s$
(iii)' x não é a p-ésima potência resíduo $mod\, l_i$ para $i = 1, ..., s$

Então, tome

$$\alpha = \frac{x + y\sqrt{D}}{2}$$

do lema (4.1) temos $(\alpha) = \mathfrak{a}^n$ com $\mathfrak{a}$ ideal em K, e cada l_i é decomposto em K como $l_i = \tau_i \tau_i^\sigma$ em K. Assuma que $\tau_i/(\alpha^\sigma)$. Denotemos por $[\mathfrak{a}]$ a classe de ideais contendo α. Então nós temos que $[\mathfrak{a}]^n = [(\alpha)] = 1$

Proposição 4.1 *Considere as mesmas notações e suposições acima. Se ϵ é a p_i-ésima potência resíduo mod τ_i para cada i $(1 \leq i \leq s)$, então a ordem de $[\mathfrak{a}]$ é igual a n*
Demonstração: Assuma que $[\mathfrak{a}]^m = 1$ para algum m $(1 \leq m \leq n)$. É óbvio que m é um divisor de n e portanto existe pelo menos um divisor primo p_i de n tal que mp_i/n. Então, $[\mathfrak{a}]^{n/p_i} = 1$. Portanto existe um inteiro β em K tal que $\mathfrak{a}^{n/p_i} = \beta$. Então, $(\alpha) = \mathfrak{a}^n = (\beta)^{p_i}$. No entanto isso é impossível pelo lema (4.2). Portanto, temos $[\mathfrak{a}]^m \neq 1$ para $m = 1, 2, ..., n-1$. Segue-se que a ordem $[\mathfrak{a}]$ é igual a n.
Observação: No caso em que $D < -4$, não exigimos a condição sobre ϵ do Lema 4.2 e a Proposição 4.1, uma vez que $\epsilon = 1$.
Tomaremos três sistemas de números primos $\{l_i\}$, $\{l_i'\}$ e $\{l_i''\}$, cada um satisfazendo a condição (5). Além disso assuma l_i, l_i' e l_i'' são dois a dois distintos para cada i $(1 \leq i \leq s)$
Proposição 4.2 *Sejam x, z, x', z', x'' e z'' uma solução não-trivial da equação Diophantine*

$$X^2 - 4Z^n = X'^2 - 4Z'^n = X''^2 - 4Z''^n \tag{6}$$

satisfazendo as condições:
(i) $(x, z) = (x', z') = (x'', z'') = 1$
(ii) l_i/z, l_i'/z' *e* l_i''/z''
(iii) x *(resp.* x',x''*) são* p_i*-ésima potência não resíduo mod* l_i *(resp.* l_i',l_i''*)*
(iv) $(x + x')/2$ *e* $(x + x'')/2$ *são* p_i*-ésima potência resíduo mod* l_i

(v) $(x+x')/2$ *e* $(x+x'')/2$ *são* p_i*-ésima potência resíduo mod* l_i'
(vi) $(x'+x'')/2$ *e* $(x+x'')/2$ *são* p_i*-ésima potência resíduo mod* l_i'',
para cada i $(1 \leq i \leq s)$. *Então, o grupo das classes de ideais do corpo*

$$K = \mathbb{Q}(\sqrt{x^2 - 4z^n})$$

tem um subgrupo N, *tal que*

$$N \simeq \left\{ \begin{array}{ll} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & se\ D < -4 \\ \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & se\ D > 0 \end{array} \right\}$$

onde D *é o discriminante de* K.

Demonstração: Da equação (5) temos que

$$x^2 - 4z^n = x'^2 - 4z'^n = x''^2 - 4z''^n = y^2 D \tag{7}$$

Para algum $y \in \mathbb{Z}$. Assim, temos

$$x^2 - y^2 D = 4z^n \tag{8}$$

$$x'^2 - y^2 D = 4z'^n \tag{9}$$

$$x''^2 - y^2 D = 4z''^n. \tag{10}$$

Portanto, obtemos três soluções (x, y, z), (x', y', z') e (x'', y'', z'') da Diofantina (5). Resulta do Lema 4.1 que existem ideais $\mathfrak{a}$, $\mathfrak{a}'$ e $\mathfrak{a}''$ em K, tal que $(\alpha) = \mathfrak{a}^{\mathfrak{n}}$, $(\alpha') = \mathfrak{a}'^{\mathfrak{n}}$ e $(\alpha'') = \mathfrak{a}''^{\mathfrak{n}}$, onde

$$\alpha = \frac{x + y\sqrt{D}}{2},$$

$$\alpha' = \frac{x' + y\sqrt{D}}{2},$$

$$\alpha' = \frac{x'' + y\sqrt{D}}{2}$$

Sejam τ_i, τ_i' e τ_i'' $(1 \leq i \leq s)$ ideais primos em A, tal que

$$(l_i) = \tau_i \tau_i^{\sigma}, \tau_i/(\alpha^{\sigma}),$$

$$(l_i') = \tau_i' \tau_i'^{\sigma}, \tau_i'/(\alpha'^{\sigma}),$$

$$(l_i'') = \tau_i'' \tau_i''^{\sigma}, \tau_i''/(\alpha''^{\sigma}).$$

Sejam R_i (respe. R_i' e R_i'') os conjuntos de todos inteiros em A que são p_i-ésima potência de resíduos $mod\,\tau_i$ (resp. τ_i' e τ_i''). Uma vez que

$$\alpha \equiv x(mod\,\tau_i),\ \alpha \equiv \frac{x+x'}{2}(mod\,\tau_i'),\ \alpha \equiv \frac{x+x''}{2}(mod\,\tau_i'')$$

$$\alpha' \equiv \frac{x+x'}{2}(mod\,\tau_i),\ \alpha' \equiv x'(mod\,\tau_i'),\ \alpha' \equiv \frac{x'+x''}{2}(mod\,\tau_i'') \text{ e}$$

$$\alpha'' \equiv \frac{x+x''}{2}(mod\,\tau_i),\ \alpha' \equiv \frac{x'+x''}{2}(mod\,\tau_i''),\ \alpha'' \equiv x''(mod\,\tau_i'')$$

Segue das condições (iii) - (vi) da Proposição 4.2 que

$$\alpha \notin R_i,\ \alpha \in R_i',\ \alpha \in R_i'',$$

$$\alpha' \in R_i,\ \alpha' \notin R_i',\ \alpha' \in R_i'',$$

$$\alpha'' \in R_i,\ \alpha'' \in R_i',\ \alpha'' \notin R_i''$$

para cada i $(1 \leq i \leq s)$

O caso em que $D < -4$.

Decorre da preposição (4.1) que as classe de ideais $[\mathfrak{a}]$,$[\mathfrak{a}']$, $[\mathfrak{a}'']$ tem a mesma ordem. Suponhamos que a seguinte equação seja válida para $m, m', m'' > 0$:

$$[\mathfrak{a}]^m[\mathfrak{a}']^{m'}[\mathfrak{a}'']^{m''} = 1. \tag{11}$$

Então, existe número $\beta \in A$ tal que

$$\mathfrak{a}^m\mathfrak{a}'^{m'}\mathfrak{a}''^{m''} = \beta \tag{12}$$

Tomando o n-ésima potência em ambos os lados, obtemos

$$\alpha^m\alpha'^{m'}\alpha''^{m''} = \pm\beta^n \tag{13}$$

Defina d_i por $p_i^{d_i} \parallel (m, m'm'')$, e e_i por $p_i^{e_i} \parallel n$, $(1 \leq i \leq s)$. Afirmamos que $d_i \geq e_i$ para todo i. Suponha que $d_i < e_i$ para alguns i, e tome

$$m = p_i^d m_0, m' = p_i^d m_0', m'' = p_i^d m_0'', n = p_i^d n_0 \tag{14}$$

onde p_i/n_0. Decorre da equação (14)

$$\alpha^{m_0}\alpha'^{m_0'}\alpha''^{m_0''} = \pm\beta^{n_0}, \tag{15}$$

desde que K não contem raiz da unidade diferente de ± 1. Uma vez que $\alpha'^{(m'_0)} \in R_i$, $\alpha''^{(m''_0)} \in R_i$ e $\pm\beta^{n_0} \in R_i$. Nos temos, $\alpha^{m_0} \in R_i$. Porém, $\alpha \notin R_i$, então temos que $p_i | m_0$. Da mesma forma, também temos que $p_i | m'_0$ e $p_i | m''_0$. Consequentemente, de (14), temos que $p_i^{d_i+1} | (m, m', m'')$. Isso contradiz a definição de d_i e portanto, temos que $d_i \geq e_i$ para cada i. Temos portanto, $n|m$, $n|m'$, e $n|m''$. Seja N o subgrupo do grupo das classes de ideais gerado por $[\mathfrak{a}]$, $[\mathfrak{a}']$ e $[\mathfrak{a}'']$. Então N é isomorfo a $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
O caso em que $D > 0$.
Seja

$$n = p_1^{e_i} p_2^{e_i} ... p_s^{e_s}$$

decomposição em fatores primo de n. Vamos mostrar que o grupos das classes de ideais de K tem um subgrupo isomorfo ao $\mathbb{Z}/p^{e_i}\mathbb{Z} \times \mathbb{Z}/p^{e_i}\mathbb{Z}$ $(1 \leq i \leq s)$. Seja ϵ uma unidade fundamental fixada de K
Defina

$$I : \{i | \, \epsilon \in R_i, 1 \leq i \leq s\}$$

$$I' : \{i | \, \epsilon \in R'_i, 1 \leq i \leq s\}$$

$$I'' : \{i | \, \epsilon \in R''_i, 1 \leq i \leq s\}$$

Então, sejam m, m' e m'' as ordens das classes de ideais $[\mathfrak{a}]$, $[\mathfrak{a}']$ e $[\mathfrak{a}'']$, respectivamente $(m/n, m'/n' e\, m''/n'')$. Segue-se do lema (4.2) que m é um múltiplo de $\Pi_{i \in I} p_i^{e_i}$. Afirmamos que m' e m'' são múltiplos de $\Pi_{i \notin I} p_i^{e_i}$. Assuma que $p_i m'/n$, para algum $i \notin I$. Portanto, existe um número $\beta \in A$ tal que

$$\mathfrak{a}'^{(n)} = (\alpha') = (\beta)^{p_i}$$

Portanto, temos

$$\alpha' = \pm\epsilon^k \beta^{p_i}, \quad \text{para algum} \quad k \in \mathbb{Z}.$$

Uma vez que $\alpha' \in R_i$, $\beta^{p_i} \in R_i$ e $\epsilon \notin R_i$, obtemos que p_i/k. Segue-se que $\pm\epsilon^k \beta^{p_i} \in R'_i$. Portanto, temos que $\alpha \in R'_i$. Isto é uma contradição. Segue-se que $p_i m' \nmid n$, $\forall i \notin I$. Portanto, m' é um múltiplo de $\Pi_{i \notin I} p_i^{e_i}$. Similarmente, m'' é múltiplo de $\Pi_{i \notin I} p_i^{e_i}$. Pelo mesmo raciocínio temos que

$(\Pi_{i \notin I'} p_i^{e_i}) | m$, $(\Pi_{i \in I'} p_i^{e_i}) | m'$ e $(\Pi_{i \notin I'} p_i^{e_i}) | m''$.

Além disso, temos

$(\Pi_{i \notin I''} p_i^{e_i}) | m$, $(\Pi_{i \notin I''} p_i^{e_i}) | m'$ e $(\Pi_{i \in I''} p_i^{e_i}) | m''$.

Afirmamos que $p_j^{e_j}$ divide pelo menos dois dos m, m' e m'', para cada j.

Caso 1-$p_j^{e_j} \nmid m$. Sem perda de generalidade suponha que $p_j^{e_j} \nmid m$ para algum j. Nós

sabemos que m é um múltiplo de $(\Pi_{i\notin I'} p_i^{e_i})$ e também é múltiplo de $(\Pi_{i\notin I''} p_i^{e_i})$. Portanto,

$$p_j^{e_j} \nmid (\Pi_{i\notin I'} p_i^{e_i}) \text{ e } p_j^{e_j} \nmid (\Pi_{i\notin I''} p_i^{e_i})$$

.

então,

$$p_j^{e_j} | (\Pi_{i\in I'} p_i^{e_i}) \text{ e } p_j^{e_j} | (\Pi_{i\in I''} p_i^{e_i}).$$

Isso implica que $p_j^{e_j}$ divide m' (respectivamente m''), e que j esta contido em I (respectivamente em I'').
Considere $\tilde{n} := n/p_j^{e_j}$. Então, a classe de ideal $[\mathfrak{a}'^{(\tilde{n})}]$ e $[\mathfrak{a}''^{(\tilde{n})}]$ têm a mesma ordem, $p_j^{e_j}$.
Suponha que a seguinte equação é válida para $m' > 0$ e $m'' > 0$:

$$[\mathfrak{a}'^{(\tilde{n})}]^{m'} [\mathfrak{a}''^{(\tilde{n})}]^{m''} = 1 \tag{16}$$

Sabemos que uma unidade fundamental ϵ de K é um p_j-ésima potência resíduo módulo τ_j' e τ_j''.
Então, podemos mostrar que o subgrupo gerado por $[\mathfrak{a}'^{(\tilde{n})}]$ e $[\mathfrak{a}''^{(\tilde{n})}]$ é isomorfo a $\mathbb{Z}/p_j^{e_j}\mathbb{Z} \times \mathbb{Z}/p_j^{e_j}\mathbb{Z}$, da mesma forma que no caso em que $D < -4$.

Caso 2-$p_j^{e_j}$ divide m,m' e m''.
Assumiremos que $p_j^{e_j}$ divide m, m' e m''. Considere $\tilde{n} := n/p_j^{e_j}$. Por conveniência usaremos as seguintes notações:

$$\tilde{\mathfrak{a}} := \mathfrak{a}^{(\tilde{n})}, \tilde{\mathfrak{a}'} := \mathfrak{a}'^{(\tilde{n})} \text{ e } \tilde{\mathfrak{a}''} := \mathfrak{a}''^{(\tilde{n})}.$$

Então, a classes de ideais $[\tilde{\mathfrak{a}}]$, $[\tilde{\mathfrak{a}'}]$ e $[\tilde{\mathfrak{a}''}]$ tem a mesma ordem, $p_j^{e_j}$.

Sem perda de generalidade, suponha que $\langle[\tilde{\mathfrak{a}}]\rangle \cap \langle[\tilde{\mathfrak{a}'}]\rangle = 1$. Então, o subgrupo gerado por $[\tilde{\mathfrak{a}}]$ e $[\tilde{\mathfrak{a}'}]$ é isomorfo a $\mathbb{Z}/p_j^{e_j}\mathbb{Z} \times \mathbb{Z}/p_j^{e_j}\mathbb{Z}$.

Suponha que $\langle[\tilde{\mathfrak{a}}]\rangle \cap \langle[\tilde{\mathfrak{a}'}]\rangle \neq 1$, i.e., $\langle[\tilde{\mathfrak{a}}]^{p_j^r}\rangle = \langle[\tilde{\mathfrak{a}'}]^{p_j^r}\rangle$, para algum r $(1 \leq r < e_j)$. Isso significa que

$$[\tilde{\mathfrak{a}}]^{p_j^r p_j^s} [\tilde{\mathfrak{a}'}]^{p_j^r} = 1 \tag{17}$$

para algum inteiro s qualquer $(s, p_j) = 1$. Então, existe um número $\beta \in A$ tal que

$$\tilde{\mathfrak{a}}^{p_j^r s}\,\tilde{\mathfrak{a}'}^{p_j^r} = (\beta). \tag{18}$$

Tomando a $p_j^{(e_j - r)}$ é-sima potência em ambos os lados, obtemos

$$\pm\,\epsilon^k \alpha^s \alpha' = \beta^{p_j^{(e_j - r)}} \tag{19}$$

Como $e_j > r$, temos que $\pm\epsilon^k\alpha^s \in R_j$ e $\pm\epsilon^k\alpha' \in R'_j$. No entanto, $\alpha \notin R_j$ e $\alpha' \notin R'_j$, e então temos que $p_j \nmid k$. Como $\alpha^s \in R''_j$, $\alpha' \in R''_j$ e $\beta^{p_j^{e_j - r}} \in R''_j$, nós temos que $\epsilon^k \in R''_j$. Uma vez que k é relativamente primo para p_j, temos que $\epsilon \in R''_j$. Suponha que $\langle[\tilde{\mathfrak{a}}]\rangle \cap \langle[\tilde{\mathfrak{a}''}]\rangle \neq 1$, i.e., $\langle[\tilde{\mathfrak{a}}]^{p_j^q}\rangle = \langle[\tilde{\mathfrak{a}''}]^{p_j^q}\rangle$, para algum q $(1 \leq q \leq e_q)$. Isso implica que

$$[\tilde{\mathfrak{a}}]^{p_{j^t}^q}[\tilde{\mathfrak{a}''}]^{p_j^q} = 1, \tag{20}$$

para algum t relativamente primo com p_j. Então, existe um número $\gamma \in A$ tal que

$$\tilde{\mathfrak{a}}^{p_{j^t}^q}\,\tilde{\mathfrak{a}''}^{p_j^q} = (\gamma). \tag{21}$$

Elevando em ambos os lados a $p_j^{e_j - r}$ p-ésima potência em (21), obtemos

$$\pm\,\epsilon^l \alpha^t \alpha'' = \gamma^{p_j^{e_j - r}} \tag{22}$$

visto que $e_j > q$, temos que $\pm\epsilon^l\alpha^t \in R''_j$ e $\pm\epsilon^l\alpha'' \in R''_j$. Sabemos que $\epsilon \in R''_j$. Portanto, obtemos que $\alpha'' \in R''_j$. Então temos uma contradição. Logo $\langle[\tilde{\mathfrak{a}}]\rangle \cap \langle[\tilde{\mathfrak{a}'}]\rangle = 1$. Segue-se que o subgrupo gerado por $[\tilde{\mathfrak{a}}]$ e $[\tilde{\mathfrak{a}''}]$ é isomorfo ao $\mathbb{Z}/p_j^{e_j}\mathbb{Z} \times \mathbb{Z}/p_j^{e_j}\mathbb{Z}$.

Em conclusão, K tem um subgrupo isomorfo a $\mathbb{Z}/p_j^{e_j}\mathbb{Z} \times \mathbb{Z}/p_j^{e_j}\mathbb{Z}$, para todo j, ou seja, K tem um subgrupo isomorfo a $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Seja

$$n = p_1^{e_1} p_2^{e_s} ... p_s^{e_s}$$

a decomposição de fatores primo de n.
Precisamos de mais um lema antes de provarmos o teorema principal.

Lema 4.3 *Para cada número primo $p_i \neq 2$, existem infinitos números primo l, tal que*
(a) $l \equiv 1 (mod\, 2p_i)$

(b) -1 é n-ésima potência resíduo módulo l
(c) 2 não é a p_i potência resíduo módulo l

Demonstração: Defina $F := \mathbb{Q}(2^{1/p_i}, \xi_{2n})$. Então, F é Galois sobre $\mathbb{Q}$. Decorre do teorema da densidade de Chebotarev que existem infinitos números primos l, cuja os corpos de decomposição são iguais em $\mathbb{Q}(\xi_{2n})$. Podemos deduzir que tais primos l satisfazem as condições do lema.
O lema abaixo é para o caso onde $p_i = 2$, para alguns i.
Lema 4.4 *Existem infinitos números primos l tais que*
(a) $l \equiv 1 (mod\, 4)$
(b) o $p_i^2 s$ e o -1 são n-ésima potência resíduos módulo l
(c) $p_1^2 p_2^2 ... p_s^2 + 1$ não é um quadrado módulo l

Demonstração: Defina $F := \mathbb{Q}(p_1^{2/n}, p_2^{2/n}, ..., p_s^{2/n}, \xi_{2n})$ e $\tilde{F} := F(\sqrt{(p_1^2 p_2^2 ... p_s^2 + 1)})$. Então, $\tilde{F}$ é Galois sobre $\mathbb{Q}$ visto que $p_1^2 p_2^2 ... p_s^2 + 1$ não é um quadrado módulo l e é relativamente primo para n, $\sqrt{p_1^2 p_2^2 ... p_s^2 + 1} \in F$. Resulta do teorema de densidade de Chebotarev que existem infinitos número primos l cujo os corpos de decomposição são iguais a F.

Teorema 4.2 *Para cada inteiro $n \geq 1$, existem infinitos corpos quadráticos real (resp. imaginário) com grupo de classes de ideais contendo um subgrupo isomorfo a $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ (resp. $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$).*

Demonstração: Para cada p_i, fixe o números primos l_i, l_i' e l_i'' satisfazendo as condições do lema(4.3) e o lema(4.4). Vamos supor que todos os l_i, l_i' e l_i'' são distintos. Portanto, podemos encontrar um inteiro c_i $(resp. a_i, b_i)$ tal que $c_i^n \equiv -1 mod\, l_i$ $(resp. a_i^n \equiv -1 mod\, l_i', b_i^n \equiv -1 mod\, l_i'')$ quando $p_i \neq 2$. Se $p_i = 2$ para alguns i, Podemos encontrar um inteiro c_i $(resp. a_i, b_i)$ tal que $c_i^n \equiv -(p_1 p_2 ... p_s)^2 \, mod\, l_i$ (respectivamente $a_i^n \equiv -(p_1 p_2 ... p_s)^2 \, mod\, l_i'$ e $b_i^n \equiv -(p_1 p_2 ... p_s)^2 \, mod\, l_i''$). Pelo teorema chines do resto podemos encontrar inteiros A, B e C satisfazendo

$$\begin{cases} A \equiv 0, B \equiv 1, C \equiv c_i & (mod\, l_i) \quad \forall i, \\ A \equiv a_i, B \equiv 0, C \equiv 1 & (mod\, l_i') \quad \forall i, \\ A \equiv 1, B \equiv b_i, C \equiv 0 & (mod\, l_i'') \quad \forall i, \end{cases} \tag{23}$$

e

$$\begin{cases} B \equiv 1, C \equiv 0 & (mod\, q) \quad \forall q \in \mathfrak{D}_A \backslash \{l_i\}, \\ C \equiv 0 & (mod\, q) \quad \forall q \in \mathfrak{D}_B \backslash \{l_i'\}, \\ C \equiv 1 & (mod\, q) \quad \forall q \in \mathfrak{D}_{(B^n - A^n)}, \end{cases} \tag{24}$$

Onde $\mathfrak{D}_m$ denota o conjunto de fatores primos de um inteiro m. (pode se verificar que $(A, B) = 1$ e $\{l_i\}$,$\{l_i'\}$,$\{l_i''\}$, $\mathfrak{D}_A \backslash \{l_i\}$, $\mathfrak{D}_B \backslash \{l_i'\}$ e $\mathfrak{D}_{(A^n - B^n)}$ são conjuntos disjuntos.)

Sempre que $(A, B) = 1$ e $(C, B_n - A_n) = 1$, temos

$$(A, B^n - C^n) = 1 \text{ e } (B, C^n - A^n) = 1 \tag{25}$$

Caso 1 - Corpos quadráticos de números reais.
Então nós temos

$$\begin{cases} x = A^n + B^n - C^n,\ z = AB, \\ x' = -A^n + B^n + C^n,\ z' = BC, \\ x'' = A^n - B^n + C^n,\ z'' = CA. \end{cases} \tag{26}$$

Então, obtemos

$$\begin{aligned} A^{2n} + B^{2n} + C^{2n} - 2(AB)^n - 2(BC)^n - 2(CA)^n &= x^2 - 4z^n \\ &= x'^2 - 4z'^n \\ &= x''^2 - 4z''^n \end{aligned} \tag{27}$$

e

$$x \equiv \begin{cases} 2 & (mod\, l_i)\, se\, p_i \neq 2, \\ p_1^2 p_2^2 ... p_s^2 + 1 & (mod\, l_i)\ se\ p_i = 2, \end{cases} \qquad z \equiv 0\ (mod\, l_i),$$

$$x' \equiv \begin{cases} 2 & (mod\, l_i')\, se\, p_i \neq 2, \\ p_1^2 p_2^2 ... p_s^2 + 1 & (mod\, l_i')\ se\ p_i = 2, \end{cases} \qquad z' \equiv 0\ (mod\, l_i'),$$

$$x'' \equiv \begin{cases} 2 & (mod\, l_i'')\, se\, p_i \neq 2, \\ p_1^2 p_2^2 ... p_s^2 + 1 & (mod\, l_i'')\ se\ p_i = 2, \end{cases} \qquad z'' \equiv 0\ (mod\, l_i''),$$

para todo i $(1 \leq i \leq s)$. Além disso, temos

$$\frac{x + x'}{2} = B^n,\ \frac{x' + x''}{2} = C^n,\ \frac{x + x''}{2} = A^n.$$

De (25), temos também $(x, z) = (x', z') = (x'', z'') = 1$. Daqui decorre que x, z, x', z', x'' e z'' é uma solução da equação Diofantine

$$X^2 - 4Z^n = X'^2 - 4Z'^n = X''^2 - 4Z''^n$$

Satisfazendo todas as condições da proposição 4.2 (note que $p_i | n$, para todo $1 \leq i \leq s$). Sempre que

$$\begin{aligned} x^2 - 4z^n &= A^{2n} + B^{2n} + C^{2n} - 2(AB)^n - 2(BC)^n - 2(CA)^n \\ &= C^{2n} - 2C^n(A^n + B^n) + (A^n - B^n)^2, \end{aligned} \tag{28}$$

e C é determinado por uma condição de congruência, Podemos deixar o valor $x^2 - 4z^n$ ser positivo, escolhendo um C adequado. Agora estabelecendo $K = \mathbb{Q}(\sqrt{x^2 - 4z^n})$. Segue-se da Proposição 4.2, que o grupo das classes de ideais de um corpo um quadrático real K tem $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ como um subgrupo. A propriedade infinita segue-se diretamente da existência, do seguinte modo. Suponha que exista apenas um número finito de tais $K's$ e denote o conjunto deles por $\mathfrak{R}$. Seja k o valor máximo do número de classe de tais $K's$. Então, podemos obter $(nt)^2 > k$, escolhendo um t adequado. Seja K' um corpo quadrático real cujo o grupo das classes tem um subgrupo isomorfo a $\mathbb{Z}/nt\mathbb{Z} \times \mathbb{Z}/nt\mathbb{Z}$. Então, K' também está contido em $\mathfrak{R}$. Isso contradiz o Maximalidade de k. Portanto temos o que queríamos.

Caso 2 - Corpos de números quadráticos imaginários

Seja t um múltiplo do produto de todos os números primos em:

$\{l_i\}$, $\{l_i'\}$, $\{l_i''\}$, $\mathfrak{D}_{[(B-A)^n-(C-A)^n]}$, $\mathfrak{D}_{[(B-A)^n-(B-A)^n]}$ e $\mathfrak{D}_{[(C-A)^n-(C-B)^n]}$

De $(A, B^n - C^n) = 1$ e $(B, C^n - A^n) = 1$, podemos verificar que:

$$\begin{aligned} 1 &= (t - A, (B-A)^n - (C-A)^n) \\ &= (t - B, (B-A)^n - (B-C)^n) \\ &= (t - C, (C-A)^n - (C-B)^n) \end{aligned} \tag{29}$$

Agora nós tomamos

$$\begin{cases} x = (A-t)^n + (B-t)^n - (C-t)^n,\ z = (A-t)(B-t), \\ x' = (A-t)^n + (B-t)^n - (C-t)^n,\ z = (B-t)(C-t), \\ x'' = (A-t)^n + (B-t)^n - (C-t)^n,\ z = (A-t)(C-t), \end{cases} \tag{30}$$

Então, também temos

$$x^2 - 4z^n = x'^2 - 4z'^n = x''^2 - 4z''^n \tag{31}$$

e

$$x \equiv \begin{cases} 2 & (mod\, l_i)\, se\, p_i \neq 2, \\ p_1^2 p_2^2 ... p_s^2 + 1 & (mod\, l_i)\ se\ p_i = 2, \end{cases} \qquad z \equiv 0\ (mod\, l_i),$$

$$x' \equiv \begin{cases} 2 & (mod\, l_i')\, se\, p_i \neq 2, \\ p_1^2 p_2^2 ... p_s^2 + 1 & (mod\, l_i')\ se\ p_i = 2, \end{cases} \qquad z' \equiv 0\ (mod\, l_i'),$$

$$x'' \equiv \begin{cases} 2 & (mod\, l_i'')\, se\, p_i \neq 2, \\ p_1^2 p_2^2 ... p_s^2 + 1 & (mod\, l_i'')\ se\ p_i = 2, \end{cases} \qquad z'' \equiv 0\ (mod\, l_i''),$$

para todo i $(1 \leq i \leq s)$. Além disso, temos

$$\frac{x + x'}{2} = (B - t)^n,\ \frac{x' + x''}{2} = (C - t)^n,\ \frac{x + x''}{2} = (A - t)^n.$$

De (29), temos que $(x, z) = (x', z') = (x'', z'') = 1$. Resulta disto que x, z, x', z', x'', z'' é uma solução da equação Diophantine (6), satisfazendo as condições da preposição 4.2 (note que $p_i | n$, para todo $1 \leq i \leq s$). Uma vez que

$$x^2 - 4z^n = -3t^{2n} + (Termos\, de\, menor\, grau\, em\, t) \tag{32}$$

Podemos tornar o valor $x^2 - 4z^n$ negativo tomando t suficientemente grande. Agora defina, $K = \mathbb{Q}(\sqrt{x^2 - 4z^n})$. Segue-se da Proposição 4.2 que o grupo das classes ideais de um corpo quadrático imaginário K tem $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ como um subgrupo. A propriedade infinita pode ser mostrada de maneira análoga ao caso anterior. Portanto temos o resultado desejado.

5 CONCLUSÃO

Portanto, concluímos que para um grupo finito abeliano não cíclico $G = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, existem infinitos corpos quadráticos reais cujos os grupos das classes de ideais contêm um subgrupo isomorfo a G.

Sendo $G = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, então existem infinitos copos quadráticos imaginários cujos os grupos das classes de ideais contêm um subgrupo isomorfo a G.

REFERÊNCIAS

ENDLER, O. **Teoria dos números algébricos**. Rio de Janeiro: IMPA, 1986.

ENDLER, O. **Teoria dos Corpos**. Rio de Janeiro: IMPA, 2007.

G.YU. A Note on the divisibility of class numbers of real quadratic fields,. **J.Number Teory**, , n. 97, p. 35–44, 2002.

K.SOUNDARARAJAN. Divisibility of Class Numbers of Imaginary Quadratic Fields. **J.Lodon Math**, , n. 7, p. 681–690, 2000.

MOLLIN, R. A. **Algebraic number theory**. Boca Raton: Chapman & Hall, 1999.

N.BOURBAKI. **Elementos of Mathematics,Commutative**. Berlin Heidelberg New York, 1985.

SAMUEL, P. **Algebraic theory of numbers**. New York: Dover, 2008.

WEINBERGER, P. Real quadratics fields with class numbers divisible by n. **J. Numbers Theory** , , n. 5, p. 237–241, 1973.

YAMAMOTO, Y. On unramified Galois extensions of quadratic number fields. **Osaka J. Math.**, , n. 7, p. 57–76, 1970.