UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE CIÊNCIAS
PÓS-GRADUAÇÃO EM MATEMÁTICA

FAMÍLIAS INFINITAS DE CORPOS QUADRÁTICOS IMAGINÁRIOS

ALEXSANDRO BELÉM DA SILVA

Fortaleza
2010

UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE CIÊNCIAS
PÓS-GRADUAÇÃO EM MATEMÁTICA

FAMÍLIAS INFINITAS DE CORPOS QUADRÁTICOS IMAGINÁRIOS

ALEXSANDRO BELÉM DA SILVA

Orientador: Prof. Dr. José Othon Dantas Lopes

Dissertação apresentada ao curso de Mestrado em Matemática - UFC como pré-requisito parcial para obtenção do título de Mestre em Matemática.

Fortaleza
Julho – 2010

Silva, Alexsandro Belém da
S578f Famílias infinitas de corpos quadráticos imaginários/
Alexsandro Belém da Silva. 2010.
63 f.

Orientador: Prof. Dr. José Othon Dantas Lopes.
Área de concentração: Matemática.
Dissertacão (mestrado) - Universidade Federal do Ceará,
Depto de Matemática, 2010

1. Álgebra. 2. Teoria dos números.

CDD 512

À minha amada, minha companheira, meu porto seguro, minha paixão, minha emoção, minha vida: Eliziane Rose Belém.

AGRADECIMENTOS

Definitifamente este trabalho não é fruto somente do meu próprio esforço.

Primeiramente agradeço à Jesus Cristo, pelo dom da vida, pelas incontáveis bençãos a mim concedidas e também pelas batalhas pois elas me levam pra junto d'Ele. Sem Jesus nada disso seria possível.

Agradeço a minha esposa Eliziane Rose Belém, pessoa a quem amo incondicionalmente e que esteve comigo nos momentos felizes e, principalmente, nos não tão felizes assim, dessa caminhada. Sem ela tudo ficaria extremamente mais difícil.

Agradeço a minha mãe Maria Elizabete Belém, sem dúvida uma das pessoas mais importantes da minha vida, por ter acreditado em minha educação e pricipalmente por ter sempre me proporcionado um lar de paz, harmonia, carinho, e amor que foram fundamentais nessa trajetória. Sem ela tudo ficaria muito mais difícil.

.....

Agradeço à meu orientador prof. Dr. José Othon Dantas Lopes por ter desempenhado de forma brilhante este ofício de orientação (que não é nada trivial) com a enorme disposição e paciência que são necessárias a um iniciante em matemática. Sem ele tudo ficaria mais difícil.

Agradeço, em especial, ao meu professor e amigo Dr. Angelo Papa Neto do Instítuto Federal de Educação, Ciência e Tecnologia do Ceará (IFCE) com quem tive o prazer de "dar os primeiros pasos"em álgebra (e também em teoria algébrica de números - ainda que eu não tenha percebido naquele momento) e que sempre esteve disposto a me ajudar em termos matemáticos e também não-matemáticos com seu carisma, suas opiniões e seus conselhos preciosos que sempre me acompanharam nesses últimos anos. Sem ele tudo ficaria mais difícil.

As minhas duas famílias. A de sangue: meu irmão Orlando, meu sobrinho Bernardo, minha cunhada Virgínia, a todos os meus tios e tias, primos e primas e também a minha avó Dulcinéa (por permanecer entre nós durante todo esse tempo) que contribuiram direta ou indiretamente para eu chegar até aqui. A da fé: todos da Igreja Presbiteriana do Itapuã pelo amor, carinho, respeito e principalmente pela comunhão que há entre nós. Muito Obrigado a todos.

Agradeço a todos os professores do departamento de matemática da UFC, responsáveis pela minha excelente formação acadêmica. Em particular, aqueles com quem pude des-

frutar a satisfação de estar em sala de aula: José Robério, Fernanda Camargo, Luquésio Petrola, Silvano Menezes, Cleon Barroso, Aldir Chaves, Antônio Caminha e Marcos Melo. Sem eles tudo ficaria ralmente mais difícil.

Agradeço aos meus colegas da comunidade matemática da UFC: Rondinelle Marcolino, José Deibson, Antonio Wilson, Filipe Silva, Leon Denis, Tiago Veras (o buda), Ernani Junior, Kelton Silva, Ana Shirley, Antonia Jocivânia (Vânia), Priscila Rodrigues, Maria de Fátima (a gasguita), André Pinheiro, Joserlan Perote e tantos outros que por ventura tenha esquecido, pelo divertimento proporcionado durante esses dois anos e pela companhia nessa árdua (porém gratificante) estrada. Vocês foram muito importantes.

Agradeço ao professor Dr. Trajano Nóbrega pela participação na banca examinadora e por suas contribuições e sugestões valiosas. Sem ele este trabalho ainda estaria incompleto.

Agradeço a nossa secretária Andrea Dantas, pela simpatia e pela disposição em ajudar não só a mim mas a todos os alunos da pós-graduação.

Finalmente, porém não menos importante, agradeço a FUNCAP e a CAPES pelo apoio financeiro.

"Bem-aventurados os humildes de espírito, porque deles é o Reino dos Céus. Bem-aventurados os que choram, porque serão consolados. Bem-aventurados os mansos, porque herdarão a terra. Bem-aventurados os que tem fome e sede de justiça, porque serão fartos. Bem-aventurados os misericordiosos, porque alcançarão misericórdia. Bem-aventurados os limpos de coração, porque verão a Deus. Bem-aventurados os pacificadores, porque serão chamados filhos de Deus. Bem-aventurados os perseguidos por causa da justiça, porque deles é o Reino dos Ceus. Exultai e alegrai-vos sobremaneira, pois é explêndida a vossa recompensa nos céus."

Jesus Cristo

Resumo

Seja $\ell > 3$ um primo ímpar. Sejam S_0, S_+, S_- conjuntos finitos mutuamente disjuntos de primos racionais. Para qualquer número real suficientemente grande $\mathrm{X} > 0$, baseando-nos em [16], damos neste trabalho, um limite inferior do número de corpos quadráticos imaginários k que satisfazem as seguintes condições: o discriminante de k é maior que $-\mathrm{X}$ o número de classe de k é não divisível por ℓ, todo $q \in S_0$ se ramifica, todo $q \in S_+$ se decompõe e todo $q \in S_-$ é inerte em k, respectivamente.

Abstract

Let $\ell > 3$ be an odd prime. Let S_0, S_+, S_- be mutually disjoint finite sets of rational primes. For any suficiently large real number $\mathrm{X} > 0$, basing ourselves on [16], we give this paper a lower bound of the number of imaginary quadratic fields k which satisfy the following conditions: the discriminant of k is greater than $-\mathrm{X}$, the class number of k is not divisible by ℓ, every $q \in S_0$ ramifies, every $q \in S_+$ splits and every $q \in S_-$ is inert in k, respectively.

Sumário

Introdução

Seja $\mathbb{Z}$ o anel dos inteiros racionais, e $\mathbb{Q}$ o corpo dos números racionais. Para qualquer primo racional ℓ, denotamos por $\mathbb{Z}_\ell$ o anel dos inteiros ℓ-ádicos. Se k é um corpo numérico (veja início do capítulo 1) de grau finito sobre $\mathbb{Q}$, denotamos por $h(k)$ o número de classes de k e por $\mathrm{D}(k)$ o seu discriminante. $\sharp$ S denota a cardinalidade de um conjunto S.

Sejam $\mathcal{Q}^-$ e $\mathcal{Q}^+$ o conjunto de todos os corpos quadráticos imaginários e reais, respectivamente. Para qualquer número real $\mathrm{X} > 0$, ponhamos $\mathcal{Q}^-(\mathrm{X}) = \{k \in \mathcal{Q}^-;\ -\mathrm{X} < \mathrm{D}(k)\}$ e $\mathcal{Q}^+(\mathrm{X}) = \{k \in \mathcal{Q}^+;\ \mathrm{D}(k) < \mathrm{X}\}$. É claro que $\mathcal{Q}^-(X)$ e $\mathcal{Q}^+(X)$ são conjuntos finitos.

Em 1974, P. Hartung provou em [11] que $\{k \in \mathcal{Q}^-; 3 \nmid h(k)\}$ é um conjunto infinito, e observou que seu método (uma aplicação das relações do número de classe de Kronecker) pode ser aplicado à mesma afirmação no caso em que 3 é substituído por qualquer primo ímpar ℓ. O caso $\ell = 3$ está também implícito nas investigações de Davenport-Heilbronn [9, 8].

Kohnen e Ono em [18] obtêm, em 1999, um limite inferior de $\sharp\{k \in \mathcal{Q}^-(\mathrm{X});\ \ell \nmid h(k)\}$ onde $\ell \geq 5$ é qualquer primo. Isso é um refinamento quantitativo do resultado de Hartung. Ono [21] e Byeon [4], nesse mesmo ano, também obtiveram uma estimativa similar para o caso real.

Para qualquer corpo numérico k e qualquer primo racional ℓ, $\lambda_\ell(k)$ e $\mu_\ell(k)$ denotam as *invariantes de Iwasawa* da $\mathbb{Z}_\ell$-extansão básica sobre k (veja [15] para definições formais). Sabe-se, por Iwasawa [15], que se $\ell \nmid h(k)$ e ℓ não se decompõe absolutamente em k, então $\lambda_\ell(k) = \mu_\ell(k) = 0$.

Horie e Horie-Ônish [15, 16, 18] provaram que existem infinitos $k \in \mathcal{Q}^-$ que satizfazem $\ell \nmid h(k)$ e algumas condições de ramificação (por exemplo, $(\mathrm{D}(k)/\ell) \neq 1$) se ℓ é um primo suficientemente grande. Os métodos usados por eles envolvem uma representação

Galoisiana ℓ-ádica oriunda de certas curvas modulares Jacobianas e a fórmula do traço para operadores de Hecke agindo sobre certos espaços de formas parabólicas. Eles deduzem, utilizando o teorema de Iwasawa citado acima, que $\{k \in \mathcal{Q}^{-};\ \lambda_\ell(k) = \mu_\ell(k) = 0\}$ é um conjunto infinito.

Beladas e Fouvry [1] refinam, em um artigo publicado em 1999, as invetigações de Davenport e Heilbronn e estimam $\sharp\,\{k \in \mathcal{Q}^{+}(\mathrm{X});\ 3 \nmid h(k)$ e $\mathrm{D}(k)$ é um primo racional$\}$.

Byeon [5] extende a investigação de Kohnen-Ono de forma a abranger os casos tratados por Horie [14]. Ele obtém

$$\{k \in \mathcal{Q}^{-}(\mathrm{X});\ \lambda_\ell(k) = \mu_\ell(k) = 0\} \gg_{\ell,\varepsilon} \frac{\sqrt{\mathrm{X}}}{\log \mathrm{X}}$$

para qualquer primo $\ell \geq 5$ e qualquer número real $\varepsilon > 0$ (o sufixo de $\gg$ significa que a constante implícita depende dele). Ono [21] e Byeon [4, 3] também discutem o caso de corpos quadráticos reais e obtém limites inferiores similares. Seus métodos, baseiam-se no fato de que os coeficientes de $\theta^3(z)$, onde $\theta(z) = \sum_{n\in\mathbb{Z}} e^{2\pi i z n^2}$, estão intimamente relacionados com o número de classe de formas quadráticas, e o teorema de Sturm [30] sobre a congruência de formas modulares.

No presente trabalho, estudaremos uma versão quantitativa da investigação de Horie-Ônish [13] e Horie [12]. Mais precisamente, segundo o trabalho de I. Kimura [16], de 2003, daremos um limite inferior para o número de corpos $k \in \mathcal{Q}^{-}(\mathrm{X})$ que satisfazem $\ell \nmid h(k)$ e certas condições de ramificação a serem esclarecidas em momento oportuno.

A seguir descreveremos em linhas gerais o conteúdo de cada um dos capítulos dessa monografia. O capítulo 1 é elementar no sentido de que nele tratamos de fatos básicos da teoria dos números algébricos. Apresentamos o anel dos inteiros de um corpo numérico, provamos o teorema de Dirichlet sobre a decomposição de ideais primos e chegamos a um resultado, também devido a Dirichlet, sobre a finitude do grupo de classes de ideais.

No capítulo 2 discutiremos alguns aspectos elementares das relações entre a geometria não euclidina e a teoria dos números. Essa conexão começa por meio do grupo das matrizes $\mathrm{SL}_2(\mathbb{Z})$ e subgrupos de congruência (veja a seção 2.1 do capítulo 2). Em seguida apresentaremos uma classe de funções analíticas conhecidas como *formas modulares* e também as *formas automórficas*.

Para se ter uma ideia da importância e abrangência destes conceitos, a teoria das formas automórficas é uma generalização das formas modulares, na qual a teoria da representação de grupos topológicos tem um papel fundamental. Formas automórficas

constituem uma área da matemática cujos pilares são a *álgebra*, a *análise*, a *geometria* e a *topologia*. Alguns dos fundadores da teoria clássica são; C. F. Gaß (1777-1855), H. Poincaré (1854-1912), G. Eisenstein (1823-1852), H. Hecke (1887-1947), e C. L. Siegel (1896-1983). Por outro lado contribuíram para o avanço da teoria moderna de fomas automórficas muitos pesquisadores como I. M. Gelfond. Harish-Chandra, R. P. Langlands, G. Shimura e Andrew Wiles, esse último usa ideias de formas modulares para provar o famoso `Último Teorema de Fermat`, que esteve em aberto por mais de 350 anos (veja o artigo [31]).

No último e mais importante capítulo, analisaremos cuidadosamente os resultados obtidos por I. Kimura em 2003 no artigo [16]. Usamos séries de Eisenstein de valor metade de inteiros construídas por H. Cohen em [7] e o teorema de Sturm.

Embora o autor tenha feito um enorme esforço para que a maior parte do resultados no texto fossem provados, o trabalho não é auto-suficiente. Supomos que o leitor tenha um conhecimento prévio em álgebra abstrata e também em teoria elementar dos números. Mais precisamente as noções das principais estruturas álgebricas: *espaços vetorias, grupos, aneis, módulos* (dentre outras); e suas relações: *transformações lineares, homomorfismos, isomorfismos* são uilizados livremente e sem referências. Também não fazemos cerimônia em utilizar resultados clássicos da *teoria dos corpos* tais como o teorema da multiplicação dos graus em extensões finitas. As referências gerais são [24], [2] e [10]. No capítulo 2, utilizamos ainda alguns resultados de análise, principalmente de *variável complexa*.

Capítulo 1

Inteiros Algébricos

Um *corpo de números algébricos*, ou simplismente um *corpo numérico*, é uma extensão finita K de $\mathbb{Q}$. Os elementos de K são chamados *números algébricos*. Um número algébrico é chamado *inteiro*, ou um *inteiro algébrico* se ele é raiz de um polinômio mônico $f(x) \in \mathbb{Z}[x]$. Assim $\sqrt{2}$, $\sqrt{3}$, i, $e^{2\pi i/5}$ são inteiros algébricos. Não é imediatamente óbvio que somas ou produtos de números algébricos (respectivamente, inteiros algébricos) são ainda números algébricos (respectivamente, inteiros algébricos). Para superar esse problema, Dedekind utilizou a ideia de "linearização"do problema o que consiste na introdução da noção, bastante abstrada, de módulo. Essa noção de integralidade se aplica não somente a números algébricos mas ocorre em muitos outros contextos diferentes e portanto deve ser tratada em toda sua generalidade. Por um "anel"(respectivamente, "corpo"), a menos que se expecifique o contrário, entenderemos anel *comutativo* (respectivamente, corpo) *com elemento unidade*.

1.1 Integralidade

Definição 1.1 *Seja* R *um anel, e* A *um subanel de* R. *Dizemos que o elemento* $x \in$ R *é um* inteiro sobre A *quando existem elementos* $a_1, \ldots, a_n \in$ A *tais que* $x^n + a_{n-1}x^{n-1} + + \cdots + a_1x + a_0 = 0$.

Um dos resultados básicos da teoria é o seguinte:

Teorema 1.2 *Seja* R *um anel,* A *um subanel de* R *e* $x \in$ R. *Então as seguites afirmações são equivalentes:*

(a) x *é inteiro sobre* A.

(b) *O anel* $\mathrm{A}[x]$ *é um* A*-módulo do tipo finito.*

(c) *Existe um subanel* B *de* R *tal que* $\mathrm{A}[x] \subseteq \mathrm{B}$ *e* B *é um* A*-módulo do tipo finito.*

Prova. (a) $\Rightarrow$ (b) Assuma que $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$ com $a_0, \ldots, a_{n-1} \in$ $\in$ A. Mostraremos que $\{1, x, \ldots, x^{n-1}\}$ é um sistema de geradores do A-módulo $\mathrm{A}[x]$. De fato, $x^n = -(a_{n-1}x^{n-1} + \cdots + a_1x + a_0)$ segue-se que $x^{n+1}, x^{n+2}, \ldots$ são expressos como combinações lineares de $1, x, \ldots, x^{n-1}$ com coeficientes em A.
(b) $\Rightarrow$ (c) Basta tomar $\mathrm{B} = \mathrm{A}[x]$.
(c) $\Rightarrow$ (a) Seja $\mathrm{B} = \mathrm{A}y_1 + \cdots + \mathrm{A}y_n$ desde que $x, y_i \in \mathrm{B}$ então $xy_i \in \mathrm{B}$; assim existem elementos a_{ij} $(j = 1, \ldots, n)$ tais que $xy_i = \sum_{j=1}^{n} a_{ij}y_j$ (para todo $i = 1, \ldots, n$). Portanto, sendo $\delta_{ij} = 1$ quando $i = j$, $\delta_{ij} = 0$ quando $i \neq j$ podemos esrever $\sum_{j=1}^{n}(\delta_{ij}x - a_{ij})y_j = 0$ (para todo $1 \leq i \leq n$). Em outras palavras o sistema de equações lineares $\sum_{j=1}^{n}(\delta_{ij}x - a_{ij})\mathrm{Y}_j = 0$ (para todo $i = 1, \ldots, n$) possui a solução $(y_1, \ldots, y_n)$. Pela regra de Cramer, se d é determinante da matriz $(\delta_{ij}x - a_{ij})_{i,j}$, então $dy_j = 0$ (para todo $j = 1, \ldots, n$).

Como $1 \in \mathrm{B}$, podemos escrever $1 = \sum_{j=1}^{n} c_jy_j$ (com $c_j \in \mathrm{A}$), logo $d = d \cdot 1 =$ $= d \cdot \sum_{j=1}^{n} c_jy_j = \sum_{j=1}^{n} c_jdy_j = 0$. Calculando d explicitamente temos

$$d = \det \begin{pmatrix} x - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & x - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & x - a_{nn} \end{pmatrix},$$

deduzimos então que d é da forma $0 = d = x^n + b_{n-1}x^{n-1} + \cdots + b_0$ onde cada $b_i \in \mathrm{A}$. Isso prova que x é inteiro sobre A. ■

Exemplo. O elemento $x = \sqrt{2}$ de $\mathbb{R}$ é inteiro sobre $\mathbb{Z}$. $\Diamond$

Proposição 1.3 *Seja* R *um anel,* A *um subanel de* R*, e seja* $(x_i)_{1 \leq i \leq n}$ *um conjunto finito de elementos de* R*. Se, para todo* i*,* x_i *é inteiro sobre* $\mathrm{A}[x_1, \ldots, x_{i-1}]$ *(em particular se todos os* x_i*'s são inteiros sobre* A*), então* $\mathrm{A}[x_1, \ldots, x_n]$ *é um* A*-módulo do tipo finito.*

Prova. Arguiremos por indução sobre n. Para $n = 1$ temos a afirmação (b) do teorema 1.2. Assuma que $\mathrm{B} = \mathrm{A}[x_1, \ldots, x_{n-1}]$ é um A-módulo do tipo finito. Então $\mathrm{B} = \sum_{j=1}^{p} \mathrm{A}b_j$. O caso $n = 1$ implica que $\mathrm{B}[x_n] = \mathrm{A}[x_1, \ldots, x_{n-1}][x_n] = \mathrm{A}[x_1, \ldots, x_n]$ é um B-módulo do tipo finito. Escrevamos $\mathrm{B}[x_n] = \sum_{k=1}^{q} \mathrm{B}c_k$. Então

$$\mathrm{A}[x_1, \ldots, x_n] = \sum_{k=1}^{q} \mathrm{B}c_k = \sum_{k=1}^{q} \left(\sum_{j=1}^{p} \mathrm{A}b_j \right) c_k = \sum_{j,k} = \mathrm{A}b_j c_k.$$

Logo $(b_j c_k)_{\substack{1 \le j \le p \\ 1 \le k \le q}}$ é um conjunto finito de geradores para $A[x_1, \ldots, x_{n-1}]$ como um módulo sobre A. ■

Corolário 1.4 *Seja* R *um anel,* A *um subanel de* R*, x e y elementos de* R *que são inteiros sobre* A*. Então $x + y, x - y$ e xy são inteiors sobre* A*.*

Prova. Claramente $x + y, x - y$ e $xy \in A[x, y]$. Pela proposição 1.3, $A[x, y]$ é um A-módulo do tipo finito. Pela parte (c) do teorema 1.2, existe um subanel B de R que contém A, x e y. Em particular B contém A e $x + y$. Logo, $x + y$ é inteiro sobre A. O mesmo raciocínio vale para $x - y$ e xy. ■

Corolário 1.5 *Seja* R *um anel,* A *um subanel de* R*. O conjunto* A′ *dos elementos de* R *que são inteiros sobre* A *é um subanel de* R *que contém* A*.*

Prova. O corolário 1.4 implica A′ é um subanel de R. Temos $\mathrm{A} \subset \mathrm{A}'$, pois, se $a \in \mathrm{A}$, a é raiz do polinômio mônico $\mathrm{P}(x) = x - a$, o qual possui coeficientes em A. ■

Definição 1.6 *Seja* R *um anel,* A *um subanel de* R*. O anel* A′ *dos elementos de* R *que são inteiros sobre* A *é chamado* fecho inteiro *de* A *em* R*. Seja* R *um domínio de integridade e seja* K *seu corpo de frações. O fecho inteiro de* A *em* K *é chamado fecho inteiro 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 1.7 (Transitividade) *Seja* C *um anel,* B *um subanel de* C*, e* A *um subanel de* B*. Se* B *é inteiro sobre* A *e* C *é inteiro sobre* B*, então* C *é inteiro sobre* A*.*

Prova. Seja $x \in$ C. Como x é inteiro sobre B, existem elementos $b_i \in$ B, $i = 0, \ldots, n-1$, tais que $x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 = 0$. Ponha B$' =$ A$[b_0, \cdots, b_{n-1}]$. Então x é inteiro sobre B$'$. Como B é inteiro sobre A, os b_i são inteiros sobre A. Portanto a proposição 1.3 implica que B$'[x] =$ A$[b_0, \ldots, b_{n-1}, x]$ é um A-módulo do tipo finito. Pela parte (c) do teorema 1.2, x é inteiro sobre A. ■

Proposição 1.8 *Seja* 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.*

Prova. Suponha que A seja um corpo e seja $0 \neq b \in$ B. Então A$[b]$ é um espaço vetorial de dimensão finita sobre A (pela parte (b) do teorema 1.2). Por outro lado $y \mapsto by$ é uma A-transformação linear de A$[b]$. Ela é injetiva pois A$[b]$ é um domínio de integridade e $b \neq 0$ (logo seu núcleo é trivial). Segue-se do teorema do núcleo e da imagem que essa transformação é sobrejetiva. Assim, existe $b' \in$ B tal que $bb' = 1$. Isso significa que qualquer elemento não nulo de B é invertível, portanto B é um corpo.

Reciprocamente, suponha que B é um corpo. Seja $a \in$ A, $a \neq 0$. Então a possui um inverso $a^{-1} \in$ B o qual é inteiro sobre A, ou seja,

$$a^{-n} + a_{n-1}a^{-n+1} + \ldots + a_1 a^{-1} + a_0, \quad a_i \in \text{A}.$$

Multiplicando a igualdade acima por a^{n-1}, obtemos

$$a^{-1} = -(a_{n-1} + \ldots + a_1 a^{n-2} + a_0 a^{n-1}),$$

o que mostra que $a^{-1} \in$ A. Portanto A é um corpo. ■

1.2 Aneis Integralmente fechados

Definição 1.9 *Um anel* A *é chamado* integralmente fechado *se ele é um domínio de integridade e se ele é o seu próprio fecho inteiro.*

Em outras palavras, todo elemento x do corpo de frações K de A que é inteiro sobre A pertence a A.

Exemplos.

1. Seja A um domínio de integridade e K seu corpo de frações. Então o fecho inteiro A$'$ de A (isto é, o fecho inteiro de A em K) é integralmente fechado. ◊

2. *Todo anel de fatoração única é integralmente fechado.* De fato, por definição um anel de fatoração única é um domínio de integridade. Agora seja K o corpo de frações de um anel de fatoração única A. Seja $x \in \mathrm{K}$, $x \neq 0$, portanto $x = a/b$ com $a, b \in \mathrm{A}$, $a, b \neq 0$, e podemos assumir que m.d.c. $(a, b) = 1$.

   Se x é inteiro sobre A, existem $a_0, a_1, \ldots, a_{n-1} \in \mathrm{A}$ tais que $(a/b)^n + a_{n-1}(a/b)^{n-1} + \cdots + a_0 = 0$. Multiplicando por b^n obtemos $a^n + b(a_{n-1}a^{n-1} + \cdots + a_1 a b^{n-2} a_0 b^{n-1}) = 0$. Assim $b \mid a^n$, como m.d.c. $(a, b) = 1$ temos que $b \mid a$. Portanto, b é uma unidade em A e isso nos diz que $x \in \mathrm{A}$. Logo A é integralmete fechado. $\Diamond$

Em particular, desde que todo anel de ideais principais é um anel de fatoração única, segue-se que todo anel de ideais principais é também integralmete fechado.

1.3 Inteiros em corpos quadráticos

Qualquer extensão de grau 2 sobre o corpo dos números racionais é chamada um *corpo quadrático.*

Proposição 1.10 *Todo corpo quadrático é da forma $\mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrados (ou seja, d não é divisível por quadrados diferente de 1, mais precisamente $d = -1$ ou d é igual a mais ou menos um produto de primos distintos.)*

Prova. Se K é um corpo quadrático, qualquer elemento $x \in \mathrm{K} - \mathbb{Q}$ é de grau 2 sobre $\mathbb{Q}$, assim é um elemento primitivo de K (isto é, $\mathrm{K} = \mathbb{Q}[x]$ e $(1, x)$ é uma base de K sobre $\mathbb{Q}$). Seja $\mathrm{F(X)} = \mathrm{X}^2 + b\mathrm{X} + c$ $(b, c \in \mathbb{Q})$ o polinômio mínimo de um tal elemento $x \in \mathrm{K}$. Resolvendo a equação $x^2 + bx + c = 0$ temos $2x = -b \pm \sqrt{b^2 - 4ac}$, assim $\mathrm{K} = \mathbb{Q}(\sqrt{b^2 - 4ac})$. Agora $b^2 - 4ac$ é um número racional da forma $u/v = uv/v^2$ com $u, v \in \mathbb{Z}$. Vê-se que $\mathrm{K} = \mathbb{Q}(\sqrt{uv})$ com $u, v \in \mathbb{Z}$. Na verdade, percebe-se que é possivel escrever $\mathrm{K} = \mathbb{Q}(\sqrt{d})$ onde d é um inteiro livre de quadrados. ■

O elemento $\sqrt{d}$ é uma raiz do polinômio irredutível $\mathrm{X}^2 - d$. Esse elemento possui um *conjugado* em K, e o conjugado é $-\sqrt{d}$. Existe um automorfismo σ de K que leva $\sqrt{d}$ em $-\sqrt{d}$. Qualquer elemento de K é da forma $a + b\sqrt{d}$ com $a, b \in \mathbb{Q}$. Temos

$$\sigma(a + b\sqrt{d}) = a - b\sqrt{d}. \tag{1.1}$$

Teorema 1.11 *Seja $\mathrm{K} = \mathbb{Q}(\sqrt{d})$ um corpo quadrático com $d \in \mathbb{Z}$ livre de quadrados (portanto $\not\equiv 0 \pmod 4$) e seja* A *o anel dos inteiros de* K.

(a) *Se* $d \equiv 2 \pmod 4$ *ou* $d \equiv 3 \pmod 4$ *então* $\mathrm{A} = \{a + b\sqrt{d};\ a, b \in \mathbb{Z}\}$.

(b) *Se* $d \equiv 1 \pmod 4$ *então* $\mathrm{A} = \{\frac{u}{2} + \frac{v}{2}\sqrt{d};\ u, v \in \mathbb{Z}$ *ambos com a mesma paridade*$\}$.

Prova. Vimos anteriormente que existe um automorfismo de K que leva $\sqrt{d}$ em $-\sqrt{d}$. Se $x \in$ A, então claramente $\sigma(x) \in$ A ($x \in A \Rightarrow x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ com $a_i \in \mathbb{Z}$, $i = 0, \ldots, n-1$, portanto $\sigma(x^n + a_{n-1}x^{n-1} + \cdots + a_0) = 0 \Rightarrow \sigma(x)^n + a_{n-1}\sigma(x)^{n-1} + \cdots + a_0 = 0 \therefore \sigma(x) \in$ A). Como A é um anel $x + \sigma(x)$, $x \cdot \sigma(x) \in$ A. Mas se $x = a + b\sqrt{d}$ com $a, b \in \mathbb{Q}$ então por (1.1)

$$x + \sigma(x) = 2a \in \mathbb{Q} \quad \text{e} \quad x \cdot \sigma(x) = a^2 - db^2 \in \mathbb{Q}. \tag{1.2}$$

Desde que $\mathbb{Z}$ é um anel de ideais principais e portanto integralmente fechado (§ 1.2 exemplo 2), vemos que

$$2a \in \mathbb{Z}; \quad a^2 - db^2 \in \mathbb{Z}. \tag{1.3}$$

As condições (1.3) são necessárias para que $x = a + b\sqrt{d}$ seja inteiro sobre $\mathbb{Z}$. Elas são também suficientes, pois x é raiz de $\mathrm{X}^2 - 2a\mathrm{X} + a^2 - db^2 = 0$. Por (1.3), podemos observar que $\alpha = a^2 - db^2 \in \mathbb{Z}$ implica que $4\alpha = (2a)^2 - d(2b)^2$ também é um elemento de $\mathbb{Z}$ e como $2a \in \mathbb{Z}$ (consequentemente $(2a)^2 \in \mathbb{Z}$), temos que $d(2b)^2 \in \mathbb{Z}$ também. Por outro lado, d é livre de quadrados, assim, se $2b$ não fosse um inteiro, seu denominador teria um fator primo p. Esse fator primo teria de aparecer como p^2 no denominador de $(2b)^2$. Multiplicação por d não levaria $(2b)^2$ em $\mathbb{Z}$, pois p^2 não divide d. Podemos, então, concluir que $2b \in \mathbb{Z}$.

Resumindo, podemos tomar $a = u/2$, $b = v/2$ com $u, v \in \mathbb{Z}$. A condição (1.3) torna-se

$$u^2 - dv^2 \in 4\mathbb{Z}. \tag{1.4}$$

Assim, $u^2 - dv^2 = 4\alpha$, $\alpha \in \mathbb{Z}$. Se v é par, então $u^2 = 4\alpha + dv^2$ nos diz que u^2, e portanto u, também é par. Nesse caso, temos $a, b \in \mathbb{Z}$. Se v é impar então $v^2 \equiv 1 \pmod 4$. As possibilidades módulo 4 para u^2 são 0 e 1. Como d é livre de quadrados, ele não é múltiplo de 4. Necessariamente (por (1.4)) $u^2 \equiv 1 \pmod 4$ e $d \equiv 1 \pmod 4$ e, portanto, temos o caso (b). ■

No caso que $d \equiv 2$ ou $3 \pmod 4$, $(1, \sqrt{d})$ é uma base para A como um $\mathbb{Z}$-módulo. Se $d \equiv 1 \pmod 4$, $(1, \frac{1}{2}(1 + \sqrt{d}))$ é uma base para o $\mathbb{Z}$-módulo A. De fato, por (b), 1

e $\frac{1}{2}(1+\sqrt{d})$ pertencem a A. Reciprocamente, para mostrar que $\frac{1}{2}(u+v\sqrt{d})$ (com u, v como em (b)) é expresso como uma combinação $\mathbb{Z}$-linear de 1 e $\frac{1}{2}(1+\sqrt{d})$, podemos, por subtração de $\frac{1}{2}(1+\sqrt{d})$, reduzir o problema ao caso onde u e v são pares. Nesse caso

$$\frac{1}{2}(u+v\sqrt{d}) = \left(\frac{u}{2} - \frac{v}{2}\right)\cdot 1 + v\cdot\frac{1}{2}(1+\sqrt{d}).$$

Se $d > 0$, $\mathbb{Q}(\sqrt{d})$ é chamado *corpo quadrático real* (existe um subcorpo de $\mathbb{R}$ conjugado a $\mathbb{Q}(\sqrt{d})$ sobre $\mathbb{Q}$). Se $d < 0$, então $\mathbb{Q}(\sqrt{d})$ é chamado *corpo quadrático imaginário*.

1.4 O discriminante

No que se segue temos o objetivo de definir o *discriminante* de um corpo numérico, para tanto precisamos de alguns conceitos prévios acerca de traços e normas.

Seja A um anel, E um A-módulo livre de posto finito e seja u um endomorfismo de E. Em álgebra linear definimos o *traço*, o *determinante* e o *polinômio característico* de u. Se (e_i) é uma base de E e se (a_{ij}) é a matriz de u com respeito a essa base, então o traço, o determinante e o polinômio característico de u são respectivamente,

$$\mathrm{Tr}(u) = \sum_{i=1}^{n} a_{ii}, \quad \det(u) = \det(a_{ij}), \quad \text{e} \quad \det(\mathrm{X}\cdot \mathrm{I_E} - u) = \det(\mathrm{X}\,\delta ij - a_{ij}). \tag{1.5}$$

É claro que essas quantidades independem da escolha da base.

As fórmulas (1.5) implicam:

$$\mathrm{Tr}(u+u') = \mathrm{Tr}(u) + \mathrm{Tr}(u'), \tag{1.6}$$

$$\det(uu') = \det(u)\det(u'),$$

$$\det(\mathrm{X}\cdot \mathrm{I_E} - u) = \mathrm{X}^n - (\mathrm{Tr}(u))\mathrm{X}^{n-1} + \cdots + (-1)^n \det(u).$$

Agora seja B um anel e saja A um subanel de B tal que B é um A-módulo livre de posto finito n (por exemplo, A pode ser um corpo e B uma extensão finita de grau n de A). Para $x \in$ B, a multiplicação m_x por x (isto é, $y \mapsto xy$) é um endomorfismo do A-módulo B.

Definição 1.12 *Chamamos* traço *(respectivamente,* norma*,* polinômio característico*) de $x \in$ B, ralativo a* B *e* A*, o traço (respectivamente, determinante, polinômio característico) do endomorfismo m_x da multiplicação por x.*

O traço (respectivamente, a norma) de x é denotado por $\mathrm{Tr}_{\mathrm{B/A}}(x)$ (respectivamente, $\mathrm{N}_{\mathrm{B/A}}(x)$), ou simplismente $\mathrm{Tr}(x)$ (respectivamente, $\mathrm{N}(x)$) quando nenhuma confusão for possível. Eles são elementos de A. O polinômio característico é um polinômio mônico com coeficientes em A.

Para $x, x' \in \mathrm{B}$ e $a \in \mathrm{A}$ temos $m_x + m_{x'} = m_{x+x'}$, $m_x \circ m'_x = m_{xx'}$ e $m_{ax} = am_x$. Além disso, a matriz de m_a com respeito a qualquer base de B sobre A é toda matriz diagonal cujas entradas são a. Das fórmulas (1.5) e (1.6) obtemos:

$$\begin{gathered}\mathrm{Tr}(x+x') = \mathrm{Tr}(x) + \mathrm{Tr}(x'), \quad \mathrm{Tr}(ax) = a\mathrm{Tr}(x), \quad \mathrm{Tr}(a) = na \\ \mathrm{N}(xx') = \mathrm{N}(x)\mathrm{N}(x'), \quad \mathrm{N}(a) = a^n, \quad \text{e} \quad \mathrm{N}(ax) = a^n\mathrm{N}(x).\end{gathered} \tag{1.7}$$

Lembrando que se L e L′ são dois corpos que contém um corpo K, L e L′ são ditos K-isomorfos quando existe um isomorfismo $\varphi : \mathrm{L} \to \mathrm{L}'$ tal que $\varphi(a) = a$ para todo $a \in \mathrm{K}$; quando L e L′ são algebricamente fechados, dizemos ainda que eles são conjugados sobre K. Dadas duas extensões L e L′ de K, dizemos que dois elementos $x \in \mathrm{L}$ e $x' \in \mathrm{L}'$ são *conjugados* sobre K se existe um K-isomorfismo $\varphi : \mathrm{K}(x) \to \mathrm{K}(x')$ tal que $\varphi(x) = x'$.

Proposição 1.13 *Seja* K *um corpo de característica* 0 *ou um corpo finito, seja* L *uma extensão algébrica de* K *com* $[\mathrm{L} : \mathrm{K}] = n$*, seja* x *um elemento de* L*, e sejam* $x_1, \ldots, x_n$ *as raízes do polinômio mínimo* $\mathrm{F}(\mathrm{X}) \in \mathrm{K}[\mathrm{X}]$ *de* x *sobre* K *(em alguma extensão conveniente de* K*), cada uma repetida* $[\mathrm{L} : \mathrm{K}[x]]$ *vezes. Então* $\mathrm{Tr}_{\mathrm{L/K}}(x) = x_1 + \cdots + x_n$*,* $\mathrm{N}_{\mathrm{L/K}}(x) = x_1 \cdots x_n$*. O polinômio característico de* x*, relativo a* L *e* K *é* $(\mathrm{X} - x_1) \cdots (\mathrm{X} - x_n)$*.*

Prova. Vamos primeiro tratar o caso onde x é um elemento primitivo de L sobre K. Assim $\mathrm{K}[\mathrm{X}]/(\mathrm{F}(\mathrm{X}))$ é K-isomorfo a L, e $(x_1, \ldots, x_n)$ é uma base de L sobre K, onde $\mathrm{F}(\mathrm{X}) = \mathrm{X}^n + a_{n-1}\mathrm{X}^{n-1} + \cdots + a_0$ é o polinômio mínimo de x sobre K. A matriz do endomorfismo m_x com respeito a essa base é

$$\mathrm{M} = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & \vdots \\ \vdots & 0 & & \vdots & \vdots \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{bmatrix}.$$

O determinante de $\mathrm{X}\cdot\mathrm{I}_{\mathrm{L}} - m_x$ é portanto o determinante da matriz

$$\mathrm{X}\cdot\mathrm{I}_n - \mathrm{M} = \begin{bmatrix} \mathrm{X} & 0 & \cdots & 0 & a_0 \\ -1 & \mathrm{X} & \cdots & 0 & a_1 \\ 0 & -1 & \cdots & 0 & \vdots \\ \vdots & 0 & & \vdots & \vdots \\ \vdots & \vdots & & \mathrm{X} & a_{n-2} \\ 0 & 0 & \cdots & -1 & \mathrm{X}+a_{n-1} \end{bmatrix}.$$

Expandindo esse determinante como um polinômio em X, obtemos $\det(\mathrm{X}\cdot\mathrm{I}_n - \mathrm{M}) = \mathrm{X}^n + a_{n-1}\mathrm{X}^{n-1} + \cdots + a_0 = \mathrm{F}(\mathrm{X})$, ou seja, o polinômio característico de x é igual ao polinômio mínimo de x. Por (1.6), $\mathrm{Tr}(x) = -a_{n-1}$ e $\mathrm{N}(X) = (-1)^n a_0$. Como x é primitivo, $\mathrm{F}(\mathrm{X}) = (X - x_1)\cdots(X - x_n)$ (pois F possui exatamente n raízes); igualando os coeficientes, vemos que $\mathrm{Tr}(x) = x_1 + \cdots + x_n$ e $\mathrm{N}(x) = x_1 \cdots x_n$.

Considere agora o caso geral. Sendo $r = [\mathrm{L} : \mathrm{K}[x]]$ é suficiente mostrar que o polinômio característico $\mathrm{P}(\mathrm{X})$ de x, com respeito a L e K, é igual a r-ésima potência do polinômio mínimo de x sobre K. Seja $(y_1, \ldots, y_q)$ uma base para $\mathrm{K}[x]$ sobre K e seja $(z_1, \ldots, z_r)$ uma base para L sobre $\mathrm{K}[x]$; então $(y_i z_j)$ é uma base para L sobre K e $n = qr$. Seja $\mathrm{M} = (a_{ih})$ a matriz para a multiplicação por x em $\mathrm{K}[x]$ com respeito a base (y_i): assim $xy_i = \sum_h a_{ih} y_h$, para todo $i = 1, \ldots, q$. Então

$$x(y_i z_j) = \Big(\sum_h a_{ih} y_h\Big) z_j = \sum_h a_{ih}(y_h z_j),$$

para $i = 1, \ldots, q$ e $j = 1, \ldots, r$. Logo, a matriz M_1 da multiplicação por x em L com respeito a essa base é uma matriz de blocos diagonais da forma

$$\mathrm{M}_1 = \begin{bmatrix} \mathrm{M} & 0 & \cdots & 0 \\ 0 & \mathrm{M} & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & \mathrm{M} \end{bmatrix}.$$

Como M_1 é $n \times n$ e M é $q \times q$ temos que M deve aparecer r vezes como blocos em M_1 (pois $n = qr$). Assim, a matriz $\mathrm{X}\cdot\mathrm{I}_n - \mathrm{M}_1$ consiste de r blocos diagonais, cada um da forma $\mathrm{X}\cdot\mathrm{I}_q - \mathrm{M}$. Consequentemente, $\det(\mathrm{X}\cdot\mathrm{I}_n - \mathrm{M}_1) = (\det(\mathrm{X}\cdot\mathrm{I}_q - \mathrm{M}))^r$. O lado esquerdo da equação anterior é $\mathrm{P}(\mathrm{X})$, enquanto $\det(\mathrm{X}\cdot\mathrm{I}_q - \mathrm{M})$ é o polinômio mínimo de x sobre K, de acordo com a primeira parte da prova. ■

Concluímos essa parte com um resultado sobre traços e normas de elementos inteiros.

Proposição 1.14 *Seja* A *um domínio de integridade* K *seu corpo de frações,* L *uma extensão de* K *com* $[\mathrm{L} : \mathrm{K}] < \infty$*, e* $x \in \mathrm{L}$ *inteiro sobre* A*. Suponha que* K *tem característica zero. Então os coeficientes do polinômio característico* $\mathrm{P}(\mathrm{X})$ *de* x *relativo a* L *e* K*, em particular, o traço e a norma de* x*, são inteiros sobre* A*.*

Prova. Pela proposição 1.13, $\mathrm{P}(\mathrm{X}) = (\mathrm{X} - x_1)\cdots(\mathrm{X} - x_n)$; assim os coeficientes de $\mathrm{P}(\mathrm{X})$ são, a menos de sinal, somas de produtos dos $x_i's$. É suficiente mostrar que $x_i's$ são inteiros sobre A. Mas cada x_i é um conjugado de x sobre K (pois os $x_i's$ são dois a dois conjugados e $\mathrm{K}[\mathrm{X}]/\mathrm{P}(\mathrm{X}) \simeq \mathrm{K}[x_i]$) e existe um K-isomorfismo $\sigma_i : \mathrm{K}[x] \to$ $\to \mathrm{K}[x_i]$ tal que $\sigma_i(x) = x_i$. Sendo x inteiro sobre A, existem $a_0, \ldots, a_{n-1} \in \mathrm{A}$ tais que $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$. Assim, $\sigma_i(x)^n + \cdots + \sigma_i(a_0) = 0$. Logo, $x_i^n + \cdots + a_0 = 0$ e isso prova que x_i é inteiro sobre A para todo i. ■

Adicionando as hipóteses da proposição anterior que A é integralmente fechado, então os coeficientes do polinômio característico de x, em particular, o traço e a norma de x, são elementos de A. De fato, eles são elementos de K, por definição, pela proposição 1.14 eles são inteiros sobre A, sendo A integralmente fechado, eles pertencem a A.

Definição 1.15 *Seja* B *um anel e seja* A *um subanel de* B *tal que* B *é um* A*-módulo livre de posto finito* n*. Para* $(x_1, \ldots, x_n) \in \mathrm{B}^n$ *chamamos o* discriminante *do conjunto* $(x_1, \ldots, x_n)$ *o elemento de* A *definido pela relação*

$$\mathrm{D}(x_1, \ldots, x_n) = \det(\mathrm{Tr}_{\mathrm{B/A}}(x_i x_j)), \tag{1.8}$$

isto é, o determinante da matriz cuja (i, j)*-ésima entrada é* $\mathrm{Tr}_{\mathrm{B/A}}(x_i x_j)$*.*

Proposição 1.16 *Se* $(y_1, \ldots, y_n) \in \mathrm{B}^n$ *é um outro conjunto de elementos de* B *tal que* $y_i = \sum_{j=1}^{n} a_{ij}x_j$ *para todo* $i = 1, \ldots, n$*, com* $a_{ij} \in \mathrm{A}$*, então*

$$\mathrm{D}(y_1, \ldots, y_n) = (\det(a_{ij}))^2 \mathrm{D}((x_1, \ldots, x_n)). \tag{1.9}$$

Prova. Primeiro notemos que

$$\mathrm{Tr}(y_p y_q) = \mathrm{Tr}\left[\left(\sum_{i=1}^{n} a_{pi}x_i\right)\left(\sum_{j=1}^{n} a_{qj}x_j\right)\right] = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{pi}a_{qj}\mathrm{Tr}(x_i x_j).$$

Isso nos dá a equação matricial

$$\mathrm{Tr}(y_p y_q) = \mathrm{M} \cdot \mathrm{Tr}(x_i x_j) \cdot \mathrm{M}'$$

(onde $\mathrm{M} = (a_{ij})$ e M' denota a matriz transposta de M). Assim

$$\begin{aligned} \mathrm{D}(y_1, \ldots, y_n) &= \det(\mathrm{Tr}(y_p y_q)) = \det(\mathrm{M} \cdot \mathrm{Tr}(x_i x_j) \cdot \mathrm{M}') \\ &= \det(\mathrm{M}) \cdot \det(\mathrm{Tr}(x_i x_j)) \cdot \det(\mathrm{M}') \\ &= (\det(a_{ij}))^2 \cdot \mathrm{D}(x_1, \ldots, x_n). \quad \blacksquare \end{aligned}$$

A proposição 1.16 implica que o discriminante de bases para B sobre A são *associados* em A; com efeito se $(x_1, \ldots, x_n)$, $(x'_1, \ldots, x'_n)$ são quaisquer duas bases do A-módulo B, então existem elementos $a_{ij} \in \mathrm{A}$ tais que

$$x'_j = \sum_{i=1}^{n} a_{ij} x_j,$$

para todo $j = 1, \ldots, n$. Assim, $\mathrm{D}(x'_1, \ldots, x'_n) = (\det(a_{ij}))^2 \cdot \mathrm{D}(x_1, \ldots, x_n)$. Isso significa que a matriz (a_{ij}) que expressa uma base em termos da outra possui uma inversa com entradas em A. Portanto, $(a_{ij}) \cdot (a_{ij})^{-1} = \mathrm{I}$ e daí, $\det(a_{ij}) \cdot \det(a_{ij})^{-1} = 1$, ou seja, $\det(a_{ij})$ e $\det(a_{ij})^{-1}$ são unidades em A. Podemos então formular a seguinte definição:

Definição 1.17 *Seja* B *um anel e seja* A *um subanel de* B *tal que* B *é um* A*-módulo livre de posto finito* n*. Se* $(x_1, \ldots, x_n)$ *é qualquer base de* B*, o ideal principal* $\mathrm{A} \cdot \mathrm{D}(x_1, \ldots, x_n)$ *é chamado o* discriminante de B sobre A *(ou relativo a* A*), e denotado por* $\mathcal{D}_{\mathrm{B/A}}$*.*

Na proposição a seguir, utilizaremos o seguinte lema, o qual não provaremos por se tratar de um fato bastante conhecido da teoria básica de grupos. A referida prova pode ser encontrada em qualquer livro introdutório de álgebra abstrata.

Lema 1.18 (Dedekind) *Seja* G *um grupo,* C *um corpo, e sejam* $\sigma_1, \ldots, \sigma_n$ *homomorfismos distintos de* G *no grupo multiplicativo* C^**. Então os* $\sigma'_i s$ *são linearmente independentes sobre* C *(i.e.* $\sum u_i \sigma_i(g) = 0$ *implica que todos os* $u'_i s$ *são zero).*

Sabemos que se K é um corpo finito ou de característica zero e L é uma extensão finita de K (com grau n) existem n K-isomorfismos $\sigma_1, \ldots, \sigma_n$ de L em um corpo algebricamente fechado C contendo K. Com isso temos a seguinte

Proposição 1.19 *Nas condições acima, se* $(x_1, \ldots, x_n)$ *é uma base de* L *sobre* K*,*

$$\mathrm{D}(x_1, \ldots, x_n) = \det(\sigma_i(x_j))^2 \neq 0. \tag{1.10}$$

Prova. A primeira igualdade segue do simples cálculo:

$$\begin{aligned} \mathrm{D}(x_1, \ldots, x_n) &= \det(\mathrm{Tr}(x_i x_j)) = \det\left(\sum_k \sigma_k(x_i x_j)\right) = \det\left(\sum_k \sigma_k(x_i)\sigma_k(x_j)\right) \\ &= \det(\sigma_k(x_i)) \cdot \det(\sigma_k(x_i)) = \det(\sigma_i(x_j))^2. \end{aligned}$$

Resta mostrar que $\det(\sigma_i(x_j)) \neq 0$. Se $\det(\sigma_i(x_j)) = 0$, existem $u_1, \ldots, u_n \in \mathrm{C}$, não todos nulos, tais que $\sum_{i=1}^{n} u_i \sigma_i(x_j) = 0$ para todo j. Por linearidade concluímos que $\sum_{i=1}^{n} u_i \sigma_i(x) = 0$ para todo $x \in \mathrm{L}$, contradizendo assim o lema de Dedekind. ■

Observação. Sob as condiões da proposição 1.19, a relação $\mathrm{D}(x_1, \ldots, x_n) \neq 0$ significa que a forma bilinear $(x, y) \mapsto \mathrm{Tr}_{\mathrm{L/K}}(xy)$ é não-degenerada, isto é, $\mathrm{Tr}_{\mathrm{L/K}}(xy) = 0$ para todo $y \in \mathrm{L}$ implica que $x = 0$. Assim a aplicação K-linear que associa a cada $x \in \mathrm{L}$ a forma K-linear $s_x : y \mapsto \mathrm{Tr}_{\mathrm{L/K}}(xy)$ é uma injeção de L em seu espaço dual $\mathrm{Hom}_{\mathrm{K}}(\mathrm{L}, \mathrm{K})$. Como L e $\mathrm{Hom}_{\mathrm{K}}(\mathrm{L}, \mathrm{K})$ são de mesma dimensão finita n sobre K, segue-se que $x \mapsto s_x$ é uma bijeção. A existência de "base dual"de um espaço vetorial e seu dual implica que, para qualquer base $(x_1, \ldots, x_n)$ de L sobre K, existe uma base $(y_1, \ldots, y_n)$ tal que

$$\mathrm{Tr}_{\mathrm{L/K}}(x_i y_j) = \delta_{ij} \quad (1 \leq i,\, j \leq n). \tag{1.11}$$

Essa observação será útil no seguinte teorema:

Teorema 1.20 *Seja* A *um anel integralmente fechado,* K *seu corpo de frações,* L *uma extensão de* K *com* $[\mathrm{L} : \mathrm{K}] = n$*, e* A′ *o fecho inteiro de* A *em* L*. Se* K *tem característica zero então* A′ *é um* A*-submódulo de um* A*-módulo livre de posto* n*.*

Prova. Seja $(x_1, \ldots, x_n)$ uma base de L sobre K. Cada x_i é algébrico sobre K, assim, para qualquer i, temos uma equação da forma $a_n x_i^n + a_{n-1} x_i^{n-1} + \cdots + a_0 = 0$, $a_j \in \mathrm{A}$ para todo j. Podemos assumir $a_n \neq 0$. Multiplicando ambos os lados por a_n^{n-1}, obtemos

$$(a_n x_i)^n + \underbrace{a_{n-1}}_{\in \mathrm{A}}(a_n x_i)^{n-1} + \underbrace{a_n a_{n-2}}_{\in \mathrm{A}}(a_n x_i)^{n-2} + \cdots + \underbrace{a_n^{n-1} a_0}_{\in \mathrm{A}} = 0,$$

ou seja, cada $a_n x_i$ é inteiro sobre A. Ponha $x'_i = a_n x_i$. Então $(x'_1, \ldots, x'_n)$ é uma base para L sobre K contida em A′.

Pela observação anterior, existe uma outra base $(y_1, \ldots, y_n)$ de L sobre K tal que $\mathrm{Tr}(x'_i y_j) = \delta_{ij}$. Seja $z \in \mathrm{A}'$. Como $(y_1, \ldots, y_n)$ é uma base de L sobre K, podemos escrever $z = \sum_{i=1}^{n} b_j y_j$ com $b_j \in \mathrm{K}$. Para qualquer i temos $x_i z \in \mathrm{A}'$ (pois $x_i \in \mathrm{A}'$). Portanto, pela observação feita após a proposição 1.14, $\mathrm{Tr}(x'_i z) \in \mathrm{A}$. Assim,

$$\mathrm{Tr}(x_i z) = \mathrm{Tr}\big(\sum_j b_j x'_i y_j\big) = \sum_j \mathrm{Tr}(x'_i y_j) = \sum_j b_j \delta_{ij} = b_i.$$

Concluímos então que A′ é um A-submódulo do A-módulo livre $\sum_{j=1}^{n} \mathrm{A} y_j$. ■

É conhecido o resultado: " 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 q, com $0 \leq q \leq n$. Além disso, se $\mathrm{M}' \neq (0)$, existe uma base $(e_1, \ldots, e_n)$ de M e elementos não-nulos $a_1, \ldots, a_q \in \mathrm{A}$ tais que $(a_1 e_1, \ldots, a_q e_q)$ é uma base de M′ e tais que a_i divide a_{i+1}, $1 \leq i \leq q-1$".

Uma demonstração pode ser encontrada em [22]. Com isso temos o seguinte

Corolário 1.21 *Adicionando as hipóteses do teorema* 1.20 *que* A *é um anel de ideais principais então* A′ *é um* A*-módulo livre de posto* n*.*

Prova. Sabemos que A′ é livre de posto $\leq n$. Por outro lado, vimos na prova do teorema 1.20 que A′ contém uma base de L sobre K (a qual possui n elementos). Logo, A′ é de posto n. ■

Para um corpo numérico K, o grau $[\mathrm{K} : \mathbb{Q}]$ é chamado o *grau* de K. Um corpo numérico de grau 2 (respec. 3) é chamado *corpo quadrático* (respec. *corpo cúbico*). Um corpo numérico sempre possui característica zero (pois seu corpo primo é $\mathbb{Q}$).

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 (corolário 1.5). Esse anel A é um $\mathbb{Z}$-módulo *livre* de posto $[\mathrm{K} : \mathbb{Q}]$ (corolário 1.21). O discriminante das bases do $\mathbb{Z}$-módulo A diferem por uma unidade em $\mathbb{Z}$ (definição 1.17), uma unidade que é exatamente um quadrado em $\mathbb{Z}$ (proposição 1.16). Essa unidade só pode ser $+1$, isto é, o discriminante do $\mathbb{Z}$-módulo A é um elemento bem definido de $\mathbb{Z}$. Ele é chamado o *discriminante* de K.

Frequentemente, por abuso de linguagem, atribuímos a K noções que são definidas relativas a A. Assim, quando falarmos por exemplo de ideais (ou unidades) de K, queremos dizer ideais (ou unidades) de A.

1.5 Aneis Noetherianos e aneis de Dedekind

Passaremos agora a estudar uma importante classe de aneis e módulos, a saber os Noetherianos e os de Dedekind. Os primeiros são mais gerais que os últimos. Veremos a seguir que o anel dos inteiros de um corpo numérico é um anel de Dedekind e, portanto, Noetheriano (mostraremos que ele é Noetheriano independentemente). Finalmente discutiremos o problema da fatoração única em aneis de Dedekind.

É bem conhecido o teorema

Teorema 1.22 *Seja* A *um anel e* E *um* A*-módulo. As seguintes afirmações são equivalentes.*

(a) *Toda família não-vazia de submódulos de* E *contém um elemento maximal (sob a relaçao de inclusão).*

(b) *Toda sequência crescente* $(\mathrm{E})_{n\geq 0}$ *(ainda pela relação de inclusão) de submódulos de* E *é estacionária* ($\exists\, n_0$ *tal que* $\mathrm{E}_n = \mathrm{E}_{n_0}$ *para todo* $n \geq n_0$).

(c) *Todo submódulo de* E *é do tipo finito.*

Decidimos pela omissão da prova desse teorema por se tratar de um resultado clássico e presente em qualquer livro introdutório em teoria algébrica de números e também em álgebra comutativa. Novamente em Ribenboin [22], capítulo 6, encontramos uma prova simples e clara.

Definição 1.23 *Um* A*-módulo* M *é chamado* Noetheriano *se ele satisfaz as condições equivalentes do teorema* 1.22*. Um anel* A *é Noetheriano se, considerado como um* A*-módulo, ele é Noetheriano.*

Sabemos que quando consideramos um anel como um módulo sobre se mesmo, seus submódulos são seus ideais; com isso, e em virtude da parte (c) do teorema 1.22, dizemos também que um *anel é Noetheriano quando seus ideais são gerados por um número finito de elementos.*

Como exemplo, observemos que todo anel de ideais principais é um anel Noetheriano. De fato, todos os ideais de um anel de ideais principais são gerados por um único elemento.

Outros exemplos são dados a seguir

Proposição 1.24 *Todo submódulo e todo módulo quociente de um módulo Noetheriano é um módulo Noetheriano.*

Prova. Seja A um anel, E um A-módulo Noetheriano e E' um submódulo de E. Todo submódulo de E' é também submódulo de E. Logo, pela parte (c) do teorema 1.22, esses são do tipo finito e a afirmação segue.

Similarmente, existe uma correspondência um-a-um, preservando inclusão, entre os submódulos do módulo quociente E/E' e os submódulos de E contendo E', a segunda afrmação segue também do teorema 1.22, parte (b). ■

Na verdade, vale também a recíproca do resultado anterior. Esse é o conteúdo da seguinte

Proposição 1.25 *Seja* A *um anel,* E *um* A*-módulo e* E' *um submódulo de* E *tal que* E' *e* E/E' *são módulos Noetherianos. Então o próprio* E *é um módulo Noetheriano.*

Prova. Seja $(\mathrm{F_n})_{\mathrm{n}\geq 0}$ uma sequência crescente de submódulos de E. Como E' é Noetheriano, existe um inteiro n_0 tal que $\mathrm{F_n}\cap\mathrm{E}' = \mathrm{F_{n+1}}\cap\mathrm{E}'$ para todo $n \geq n_0$. Analogamente, existe um inteiro n_1 tal que $(\mathrm{F_n}+\mathrm{E}')/\mathrm{E}' = (\mathrm{F_{n+1}}+\mathrm{E}')/\mathrm{E}'$ para todo $n \geq n_1$. Tome $n \geq \sup(n_0, n_1)$. Mostraremos que $\mathrm{F_n} = \mathrm{F_{n+1}}$. É suficiente mostrar que $\mathrm{F_n} \subset \mathrm{F_{n+1}}$. Dado $x \in \mathrm{F_{n+1}}$, como $\mathrm{F_{n+1}} + \mathrm{E}' = \mathrm{F_n} + \mathrm{E}'$, existem $y \in \mathrm{F_n}$ e $z', z'' \in \mathrm{E}'$ tais que $x + z' = y + z''$. Assim, $x - y = z'' - z' \in \mathrm{F_{n+1}} \cap \mathrm{E}' = \mathrm{F_n} \cap \mathrm{E}'$. Assim, $x - y$ e y pertencendo a $\mathrm{F_n}$ implica $x \in \mathrm{F_n}$ também. Concluímos que $\mathrm{F_n} = \mathrm{F_{n+1}}$ para todo $n \geq \sup(n_0, n_1)$. Logo, pela parte (b) do teorema 1.22, E é Noetheriano. ■

Corolário 1.26 *Seja* A *um anel,* $\mathrm{E}_1, \ldots, \mathrm{E}_n$ A*-módulos Noetherianos. Então* $\prod_{i=1}^{n} \mathrm{E}_i$ *é um* A*-módulo Noetheriano.*

Prova. É suficiente provar a afirmação para dois A-módulos $\mathrm{E}_1, \mathrm{E}_2$.

$\mathrm{E}_1 \times \mathrm{E}_2$ possui um submódulo Noetheriano E_1 tal que o módulo quociente $(\mathrm{E}_1 \times \mathrm{E}_2)/\mathrm{E}_1 \simeq \mathrm{E}_2$ é também Noetheriano. Logo, pela proposição 1.24 $\mathrm{E}_1 \times \mathrm{E}_2$ é um A-módulo Noetheriano. ■

Corolário 1.27 *Seja* A *um anel, Noetheriano e seja* E *um* A*-módulo do tipo finito. Então* E *é um módulo Noetheriano (e, portanto, todos os seus submódulos são do tipo finito).*

Prova. Seja $(x_1, \ldots, x_n)$ um sistema de geradores de E, $\mathrm{A}^n = \mathrm{A} \times \cdots \times \mathrm{A}$ o produto de n cópias do A-módulo A. Considere a aplicação

$$\begin{aligned} \varphi : \quad \mathrm{A}^n &\longrightarrow \mathrm{E} \\ a &\longmapsto \sum_{i=1}^{n} a_i x_i, \end{aligned}$$

onde $a = (a_1, \ldots, a_n)$ com $a_i \in \mathrm{A}$ para todo $i = 1, \ldots, n$. É fácil ver que φ é um homomorfismo entre módulos. Além disso, dado $x \in \mathrm{E}$ temos que $x = \sum_i a_i x_i$, $a_i \in \mathrm{A}$. Tomando $a = (a_1, \ldots, a_n) \in \mathrm{A}^n$ temos que $\varphi(a) = x$, ou seja, φ é sobre E. Segue do teorema do isomorfismo que $\mathrm{E} \simeq \mathrm{A}^n/\mathrm{Ker}\,\varphi$. Pelo corolário 1.26 A^n é Noetheriano, segue-se que $\mathrm{Ker}\,\varphi$ e $\mathrm{A}^n/\mathrm{Ker}\,\varphi$ são Noetherianos. Logo, E também o é. ■

Um importante e belíssimo resultado devido a Emilly Noether vem a seguir.

Teorema 1.28 *Seja* A *um anel Noetheriano integralmante fechado. Seja* K *o corpo de frações de* A*,* L *uma extensão finita de* K*, e* A′ *o fecho inteiro de* A *em* L*. Suponha que* K *é de característica zero. Então* A′ *é um* A*-módulo do tipo finito e um anel Noetheriano.*

Prova. Sabemos que A′ é um submódulo de um A-módulo livre de posto n (§ 1.4, teorema 1.20). Como A é Noetheriano e A′ é um A-submódulo segue-se que A′ é um A-módulo do tipo finito. Agora, pelo corolário 1.27 temos que A′ é um A-módulo Noetheriano. Por outro lado, os ideais de A′ são A-submódulos de A′, eles satizfazem a condição maximal (teorema 1.22, parte (a)), portanto A′ é um anel Noetheriano. ■

Escólio. *O anel dos inteiros de um corpo numérico é um anel Noetheriano.* (Tome $\mathrm{A} = \mathbb{Z}$ e $\mathrm{K} = \mathbb{Q}$ no teorema 1.28).

Para o Próximo teorema precisamos do seguinte

Lema 1.29 *Seja* A *um anel,* $\mathfrak{p}$ *um ideal primo de* A*, e seja* A′ *um subanel de* A*. Então* $\mathfrak{p} \cap \mathrm{A}'$ *é um ideal primo de* A′*.*

Prova. Sendo $\varphi : \mathrm{A}' \to \mathrm{A}$ a aplicação de inclusão e $\psi : \mathrm{A} \to \mathrm{A}/\mathfrak{p}$ o homomorfismo canônico. Então a composta $\phi = \psi \circ \varphi : \mathrm{A}' \to \mathrm{A}/\mathfrak{p}$ é um homomorfismo tal que $\mathrm{Ker}\,\phi = \{a' \in \mathrm{A};\ a' + \mathfrak{p} = 0 + \mathfrak{p}\} = \{a' \in \mathrm{A};\ a' \in \mathfrak{p}\}$; logo, $\mathrm{Ker}\,\phi = \mathrm{A}' \cap \mathfrak{p}$. Pelo teorema do isomorfismo $\mathrm{A}'/\mathrm{Ker}\,\phi = \mathrm{A}'/(\mathrm{A}' \cap \mathfrak{p})$ é um subanel de $\mathrm{A}/\mathfrak{p}$. Como um subanel de um domínio de integridade deve ser um domínio de integridade temos que $\mathrm{A}'/(\mathrm{A}' \cap \mathfrak{p})$ é um domínio de integridade e, portanto, o ideal $\mathrm{A}' \cap \mathfrak{p}$ é primo. ■

Definição 1.30 *Um domínio de integridade* A *é chamado um anel de* Dedekind *se ele é Noetheriano e integralmente fechado, e se todo ideal primo não-nulo de* A *é maximal.*

O anel $\mathbb{Z}$ e, mais geralmente, qualquer anel de ideais principais, é um anel de Dedekind.

Teorema 1.31 *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.*

Prova. O anel A′ é integralmente fechado por construção (exemplo 1, § 1.2). Ele é Noetheriano e um A-módulo do tipo finito pelo teorema 1.28. Resta mostrar que todo ideal $\mathfrak{p}' \neq (0)$, primo, de A′ é maximal. Para isso escolha um elemento $x \in \mathfrak{p}' - (0)$ e considere uma equação da forma

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \quad (a_i \in \mathrm{A}), \tag{1.12}$$

tal que n é o menor possivel. Então $a_0 \neq 0$. Por (1.12), temos $a_0 \in \mathrm{A}' \cap \mathrm{A} \subset \mathfrak{p}' \cap \mathrm{A}$ $(a_0 = -x(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1))$. Portanto, $\mathfrak{p}' \cap \mathrm{A} \neq (0)$. Pelo lema 1.29 $\mathfrak{p}' \cap \mathrm{A}$ é um ideal primo de A, dai $\mathfrak{p}' \cap \mathrm{A}$ é um ideal maximal de A e, portanto, $\mathrm{A}/(\mathfrak{p}' \cap \mathrm{A})$ é um corpo. Mas $\mathrm{A}/(\mathfrak{p}' \cap \mathrm{A})$ pode ser identificado com um subanel de $\mathrm{A}'/\mathfrak{p}'$ e $\mathrm{A}'/\mathfrak{p}'$ é inteiro sobre $\mathrm{A}/(\mathfrak{p}' \cap \mathrm{A})$. Assim pela proposição 1.8 do § 1.1, $\mathrm{A}'/\mathfrak{p}'$ é um corpo. Logo, $\mathfrak{p}'$ é maximal. ■

Escólio. *O anel dos inteiros de um corpo numérico é um anel de Dedekind.* (Tome $\mathrm{A} = \mathbb{Z}$ e $\mathrm{K} = \mathbb{Q}$ no teorema 1.31).

Nem sempre o anel dos inteiros de um corpo numérico é um anel de ideais principais. Por exemplo, considere o anel $\mathrm{A} = \mathbb{Z}[\sqrt{-5}]$ em $\mathbb{Q}[\sqrt{-5}]$. Observe que

$$(1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}) = 2 \cdot 3,$$

se A fosse principal o elemento primo $(1+\sqrt{-5})$ dividiria 2 ou 3, mas isso implicaria, tomando a norma, que 6 dividiria 4 ou 9, um absurdo.

A mais importante propriedade dos aneis de ideais peincipais é a fatoração única em produto de primos. Essa propriedade pode ser generalizada no caso de aneis de Dedekind. Em um anel desse tipo, ideais se fatoram de modo único em produto de ideais primos. É isso que passaremos a discutir com maior precisão agora. Antes alguns lemas acerca de ideais primos são necessários.

Lema 1.32 *Se um ideal primo* $\mathfrak{p}$ *de um anel* A *contém um produto* $\mathfrak{a}_1\mathfrak{a}_2\cdots\mathfrak{a}_n$ *de ideais, então* $\mathfrak{p}$ *contém pelo menos um dos ideais* $\mathfrak{a}_i$*.*

Prova. Se $\mathfrak{a}_i \not\subset \mathfrak{p}$ para todo i então existe $a_i \in \mathfrak{p}-\mathfrak{a}_i$ para todo i. Portanto $a_1\cdots a_n \notin \mathfrak{p}$, pois $\mathfrak{p}$ é primo. Mas $a_1\cdots a_n \in \mathfrak{a}_1\cdots\mathfrak{a}_n \subset \mathfrak{p}$ temos então uma contradição. ■

Lema 1.33 *Em um anel Noetheriano todo ideal contém um produto de ideais primos. Em um domínio de integridade Noetheriano, todo ideal não-nulo contém um produto de ideais primos não-nulos.*

Prova. Suponha por absudo 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 $\mathfrak{b}$. O ideal $\mathfrak{b}$ não pode ser primo, caso contrário $\mathfrak{b}$ não pertenceria a Φ. Assim, existem $x, y \in \mathrm{A}-\mathfrak{b}$ tais que $xy \in \mathfrak{b}$. Os ideais $\mathfrak{b}+\mathrm{A}x$ e $\mathfrak{b}+\mathrm{A}y$ contém $\mathfrak{b}$ como um subconjunto próprio, portanto eles não pertecem a Φ pois $\mathfrak{b}$ é maximal em Φ. Segue-se que esses ideais contém produtos de ideais primos não-nulos:

$$\mathfrak{p}_1\cdots\mathfrak{p}_n \subset \mathfrak{b}+\mathrm{A}x \quad \text{e} \quad \mathfrak{p}'_1\cdots\mathfrak{p}'_n \subset \mathfrak{b}+\mathrm{A}y.$$

Desde que $xy \in \mathfrak{b}$,

$$(\mathfrak{b}+\mathrm{A}x)(\mathfrak{b}+\mathrm{A}y) \subset \mathfrak{b},$$

consequentemente $\mathfrak{p}_1\cdots\mathfrak{p}_n\mathfrak{p}'_1\cdots\mathfrak{p}'_n \subset \mathfrak{b}$, o que gera o absurdo procurado. Isso prova a segunda afirmação. A primeira é completamente análoga, basta excluir a expressão "não-nulo"três vezes. ■

Agora seja A um domínio de integridade e K seu corpo de frações. Chamamos qualquer A-submódulo I de K para o qual existe $d \in \mathrm{A}-(0)$ tal que $d\cdot\mathrm{I} \subset \mathrm{A}$ um *ideal fracionário* de A (ou de K com respeito a A). Isso significa que os elementos de I tem um "denominador comum"$d \in \mathrm{A}$. Os ideais ordinários de A são fracionários (com

$d = 1$). As vezes os chamamos de *ideais inteiros* para distinguí-los dos ideais fracionários. Qualquer A-submódulo I do tipo finito contido em K é um ideal fracionário. Isso segue do fato que, se $(x_1, \ldots, x_n)$ é um conjunto finito de geradores para I, os $x_i's$ tem um denominador comum d (o produto dos denominadores d_i, onde $x_i = a_i \cdot d_i^{-1}$, 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 todos os submódulos de A são do tipo finito), isto é, I $\subset d^{-1}$A e d^{-1}A sendo um A-módulo isomorfo a A, é um módulo Noetheriano. Definindo o produto de ideais fracionários de maneira usual, os ideais fracionários não-nulos de A constituem um *monóide* comutativo sobre a multiplicação.

Teorema 1.34 *Seja* A *um anel de Dedekind que não é um corpo. Todo ideal maximal de* A *é invertível no monóide dos ideais fracionários de* A *(isto é, se* $\mathfrak{m}$ *é um ideal maximal de* A *existe um ideal fracionário* $\mathfrak{m}'$ *de* A *tal que* $\mathfrak{m}\mathfrak{m}' =$ A*).*

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

$$\mathfrak{m}' = \{x \in \mathrm{K};\ x\mathfrak{m} \subset \mathrm{A}\}. \tag{1.13}$$

Claramente, $\mathfrak{m}'$ é um A-submódulo de K; qualquer elemento não-nulo de M serve como um denominador comum para os elementos de $\mathfrak{m}'$. Assim $\mathfrak{m}'$ é um ideal fracionário de A. É suficiente mostrar que $\mathfrak{m}\mathfrak{m}' =$ A. Vemos que (1.13) implica que $\mathfrak{m}\mathfrak{m}' \subset$ A; por outro lado, A $\subset \mathfrak{m}'$ (pois $\mathfrak{m}$ é um ideal de A - $a \in$ A $\Rightarrow a\mathfrak{m} \subset \mathfrak{m} \subset$ A $\therefore a \in \mathfrak{m}'$), assim $\mathfrak{m} =$ A$\mathfrak{m} \subset \mathfrak{m}'\mathfrak{m}$. Como $\mathfrak{m}$ é maximal e $\mathfrak{m} \subset \mathfrak{m}'\mathfrak{m} \subset$ A então $\mathfrak{m} = \mathfrak{m}'\mathfrak{m}$ ou $\mathfrak{m}'\mathfrak{m} =$ A. Resta mostrar que $\mathfrak{m} = \mathfrak{m}'\mathfrak{m}$ não ocorre.

Agora se $\mathfrak{m} = \mathfrak{m}'\mathfrak{m}$ e se $x \in \mathfrak{m}'$, então $x\mathfrak{m} \subset \mathfrak{m}$, $x^2\mathfrak{m} \subset x\mathfrak{m} \subset \mathfrak{m}$, e $x^n\mathfrak{m} \subset \mathfrak{m}$ para qualquer n por indução. Assim qualquer elemento não-nulo $d \in \mathfrak{m}$ 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. Mas A é integralmente fechado; portanto, $x \in$ A; e consequentemente $\mathfrak{m}'\mathfrak{m} = \mathfrak{m}$ implica $\mathfrak{m}' =$ A. Resta mostrar que $\mathfrak{m}' =$ A é impossível.

Com esse propósito tome um elemento não-nulo $a \in \mathfrak{m}$. Pelo lema 1.33, o ideal Aa contém um produto de ideais primos não-nulos $\mathfrak{p}_1 \cdots \mathfrak{p}_n$. Podemos tomar n como o menor possível. Temos $\mathfrak{m} \supset$ A$a \supset \mathfrak{p}_1 \cdots \mathfrak{p}_n$, o que significa, pelo lema 1.32, que $\mathfrak{m} \supset \mathfrak{p}_i$ para algum i, digamos $i = 1$. Como $\mathfrak{p}_1$ é maximal por hipótese, $\mathfrak{m} = \mathfrak{p}_1$. Ponha $\mathfrak{b} = \mathfrak{p}_2 \cdots \mathfrak{p}_n$. Então A$a \supset \mathfrak{m}\mathfrak{b}$ e A$a \not\supset \mathfrak{b}$, pela escolha de n. Assim existe $b \in \mathfrak{b}$ tal que $b \notin$ Aa. Como $\mathfrak{m}\mathfrak{b} \subset$ Aa, $\mathfrak{m}b \subset$ Aa, consequentemente $\mathfrak{m}ba^{-1} \subset$ A. De acordo com a

definição de $\mathfrak{m}'$, isso significa que $ba^{-1} \in \mathfrak{m}'$. Mas, desde que $b \notin \mathrm{A}$, $ba^{-1} \notin \mathrm{A}$. Logo, $\mathfrak{m}' \neq \mathrm{A}$. ■

Chegamos agora a um dos principais resultados desse capítulo e também um dos principais da teoria dos números algébricos clássica.

Teorema 1.35 *Seja* A *um anel de Dedekind e seja* P *o conjunto dos ideais primos não-nulos de* A*. Então*

(a) *todo ideal fracionário não-nulo* $\mathfrak{b}$ *de* A *pode ser expresso de modo único na forma*

$$\mathfrak{b} = \prod_{\mathfrak{p} \in \mathrm{P}} \mathfrak{p}^{n_{\mathfrak{p}}(\mathfrak{b})}, \tag{1.14}$$

onde, para qualquer $\mathfrak{b} \in \mathrm{P}$*,* $n_{\mathfrak{p}}(\mathfrak{b}) \in \mathbb{Z}$ *e, para quase todo* $\mathfrak{p} \in \mathrm{P}$*,* $n_{\mathfrak{p}}(\mathfrak{b}) = 0$*.*

(b) *O monóide dos ideais fracionários não-nulos de* A *é um grupo.*

Prova. Primeiro provaremos a existência de (a), isto é, que qualquer ideal fracionário $\mathfrak{b}$ é um produto de potências (≥ 0 ou ≤ 0) de ideais primos. Existe $d \in \mathrm{A} - (0)$ tal que $d \cdot \mathfrak{b} \subset \mathrm{A}$, isto é, tal que $d \cdot \mathfrak{b}$ é um ideal inteiro de A, $\mathfrak{b} = (d\mathfrak{b}) \cdot (\mathrm{A}d)^{-1}$. Podemos, sem perda de generalidade, provar (a) para ideais inteiros. Como antes, considere a família Φ dos ideais não-nulos em A que não são produto de ideais primos. Suponha que Φ é não-vazia. Como A é Noetheriano, Φ possui um elemento maximal $\mathfrak{a}$. Então $\mathfrak{a} \neq \mathrm{A}$, pois A é o produto da coleção vazia de ideais primos. Portanto $\mathfrak{a}$ está contido em um ideal maximal $\mathfrak{p}$, o qual é um elemento maximal na família de ideais não-triviais de A que contém $\mathfrak{a}$. Seja $\mathfrak{p}'$ o ideal fracionário inverso de $\mathfrak{p}$. Como $\mathfrak{a} \subset \mathfrak{p}$, $\mathfrak{a}\mathfrak{p}' \subset \mathfrak{p}\mathfrak{p}' = \mathrm{A}$. Como $\mathfrak{p}' \supset \mathrm{A}$, $\mathfrak{a}\mathfrak{p}' \supset \mathfrak{a}$; de fato $\mathfrak{a}\mathfrak{p}' \neq \mathfrak{a}$ (se $\mathfrak{a}\mathfrak{p}' = \mathfrak{a}$ e se $x \in \mathfrak{p}'$, então $x\mathfrak{a} \subset \mathfrak{a}$, $x^n\mathfrak{a} \subset \mathfrak{a}$ para todo n, x é inteiro sobre A, e $x \in \mathrm{A}$ (como no teorema 1.34). Mas isso é impossível pois $\mathfrak{p}' \neq \mathrm{A}$ (caso contrário $\mathfrak{p}' = \mathrm{A}$ e $\mathfrak{p}\mathfrak{p}' = \mathfrak{p}'$).). Pela maximalidade de $\mathfrak{a}$ em Φ, temos $\mathfrak{a}\mathfrak{p}' \notin \Phi$, assim $\mathfrak{a}\mathfrak{p}' = \mathfrak{p}_1 \cdots \mathfrak{p}_n$. Multiplicando por $\mathfrak{p}$, vemos que $\mathfrak{a} = \mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_n$. Logo todo ideal inteiro de A é um produto de ideais primos.

Consideremos a gora a unicidade em (a). Suponha que

$$\prod_{\mathfrak{p} \in \mathrm{P}} \mathfrak{p}^{n(\mathfrak{p})} = \prod_{\mathfrak{p} \in \mathrm{P}} \mathfrak{p}^{m(\mathfrak{p})}, \quad \text{i.e.} \quad \prod_{\mathfrak{p} \in \mathrm{P}} \mathfrak{p}^{n(\mathfrak{p}) - m(\mathfrak{p})} = \mathrm{A}.$$

Se $n(\mathfrak{p}) - m(\mathfrak{p}) \neq 0$ para algum ideal primo $\mathfrak{p} \in \mathrm{P}$, podemos separar os expoentes positivos e negativos e escrever:

$$\mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_r^{\alpha_r} = \mathfrak{q}_1^{\beta_1} \cdots \mathfrak{q}_s^{\beta_s},$$

onde $\mathfrak{p}_i$, $\mathfrak{q}_j \in \mathrm{P}$, $\alpha_i > 0$, $\beta_j > 0$, $\mathfrak{p}_i \neq \mathfrak{q}_j$ para todo i e j. Assim $\mathfrak{p}_1$ contém $\mathfrak{q}_1^{\beta_1} \cdots \mathfrak{q}_s^{\beta_s}$; segue do lema 1.32, que $\mathfrak{p}_1 \supset \mathfrak{q}_j$ para algum j, digamos $\mathfrak{p}_1 \supset \mathfrak{q}_1$. Mas $\mathfrak{p}_1$ e $\mathfrak{q}_1$ são ambos maximais, o que implica $\mathfrak{p}_1 = \mathfrak{q}_1$, o que é um absurdo.

Finalmente (1.14) implica que $\prod_{\mathfrak{p}\in\mathrm{P}} \mathfrak{p}^{-n_\mathfrak{p}(\mathfrak{b})}$ é o inverso de $\mathfrak{b}$ e isso prova (b). ■

A parte (b) do teorema 1.35 nos dá exatamente que o monóide I(A) dos ideais fracionários não-nulos de um anel de Dedekind A é um grupo. Os ideais fracionários principais (isto é, aqueles da forma $\mathrm{A}x$, $x \in \mathrm{K}^*$) formam um subgrupo F(A) de I(A) (pois $(\mathrm{A}x) \cdot (\mathrm{A}y)^{-1} = \mathrm{A}xy^{-1}$). O grupo quociente $\mathrm{C(A)} = \mathrm{I(A)/F(A)}$ é chamado o **grupo de classes de ideais** de A (ou simplismente grupo de classes). A ordem de C(A) (não necessariamente finita) é chamada o **número de classes** de A e usualmente denotado por h_A. Para que A seja um anel de ideais principais é necessariamente e suficiente que C(A) consista de um único elemento, isto é, que $h_\mathrm{A} = 1$ (com efeito, se $h_\mathrm{A} = 1$ é porque I(A) = F(A), ou seja, todo ideal de A é principal. Reciprocamente, se todo ideal de A é principal é porque I(A) = F(A), logo C(A) é trivial, ou seja, $h_\mathrm{A} = 1$).

No caso geral, o número h_A, indicando o número (cardinal) de classes de ideais distintas, pode ser considerado como uma "medida"que indica o quanto o anel de Dedekind A difere de um anel principal. Veremos na próxima seção que no caso do anel dos inteiros A de um corpo numérico K, o número h_A é sempre finito.

1.6 Finitude do grupo de classes

Mostraremos a seguir que o grupo C(A) definido na seção anterior, no caso em que A é o anel dos inteiros de um corpo númerico, é finito. Isso nos permitirá definir o *número de classe* de um corpo numérico. Antes precisamos de algumas preliminares sobre a norma de um ideal.

Seja K um corpo numérico, n seu grau, e A o anel dos inteiros de K. ♯ S denota a cardinalidade de qualquer conjunto S.

Proposição 1.36 *Se x é um elemento não-nulo de* A*, então* $|\mathrm{N}(x)| = \sharp(\mathrm{A}/\mathrm{A}x)$.

> Note que se $x \in \mathrm{A}$, $\mathrm{N}(x) \in \mathbb{Z}$ (§ 1.4, proposição 1.14), assim essa fórmula faz sentido.

Prova. Sabemos que A é um $\mathbb{Z}$-módulo livre de posto n, e $\mathrm{A}x$ é um $\mathbb{Z}$-submódulo de A. Ele é também de posto n, pois a multiplicação por x aplica A em $\mathrm{A}x$ isomorficamente. Como já vimos existe uma base $(e_1, \ldots, e_n)$ do $\mathbb{Z}$-módulo A e elementos c_i de

$\mathbb{N}$ tais que $(c_1e_1, \ldots, c_ne_n)$ é uma base de Ax. Além disso, o grupo abeliano A/Ax é isomorfo ao grupo abeliano finito $\prod_{i=1}^{n} \mathbb{Z}/c_i\mathbb{Z}$, cuja ordem é $c_1c_2\cdots c_n$. Escreva u para a aplicação $\mathbb{Z}$-linear de A em Ax definida por $u(e_i) = c_ie_i$ para $i = 1, \ldots, n$. Temos que $\det(u) = c_1 \cdots c_n$. Por outro lado $(xe_1, \ldots, xe_n)$ 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 $v \cdot u$ é uma multiplicação por x e seu determinante é, por definição, N(x). Como $\det(v \cdot u) = \det(v) \cdot \det(u)$, podemos concluir que $\mathrm{N}(x) = \pm c_1 \cdots c_n = \pm\sharp(\mathrm{A}/\mathrm{A}x)$. ■

Definição 1.37 *Dado um ideal inteiro não-nulo* $\mathfrak{a}$ *de* A*, chamamos o número* $\sharp(\mathrm{A}/\mathrm{A}x)$ *a* norma *de* $\mathfrak{a}$ *e a denotamos por* $\mathrm{N}(\mathfrak{a})$*.*

Observemos que $\mathrm{N}(\mathfrak{a})$ é *finito*. De fato, se x é um elemento não-nulo de $\mathfrak{a}$, então A$x \subset \mathfrak{a}$, e A/$\mathfrak{a}$ pode ser identificado com um quociente de A/Ax. Assim $\sharp(\mathrm{A}/\mathfrak{a}) \leq \sharp(\mathrm{A}/\mathrm{A}x)$, e esse último é um número finito. Por outro lado, vemos que para um ideal principal Ay, $\mathrm{N}(\mathrm{A}y) = |\mathrm{N}(y)|$.

Proposição 1.38 *Se* $\mathfrak{a}$ *e* $\mathfrak{b}$ *são ideais inteiros não-nulos de* A*, então* $\mathrm{N}(\mathfrak{ab}) = \mathrm{N}(\mathfrak{a}) \cdot \mathrm{N}(\mathfrak{b})$*.*

Prova. O ideal $\mathfrak{b}$ se fatora em um produto de ideais maximais e é suficiente mostrar que $\mathrm{N}(\mathfrak{am}) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{m})$ para $\mathfrak{m}$ maximal. Como $\mathfrak{am} \subset \mathfrak{a}$, temos $\sharp(\mathrm{A}/\mathfrak{am}) = \sharp(\mathrm{A}/\mathfrak{a}) \cdot \sharp(\mathfrak{a}/\mathfrak{m})$. Resta mostrar que $\sharp(\mathfrak{a}/\mathfrak{am}) = \sharp(\mathrm{A}\mathfrak{a})$. Agora $\mathfrak{a}/\mathfrak{am}$ pode ser considerado como um espaço vetorial sobre A/$\mathfrak{m}$. Seus subespaços vetoriais 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 (1.17) da observação abaixo 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/$\mathfrak{m}$. Isso significa que $\sharp(\mathfrak{a}/\mathfrak{am}) = \sharp(\mathrm{A}/\mathfrak{m})$ ■

Observação. Nas fórmulas abaixo, $n_{\mathfrak{p}}(\mathfrak{b})$ denota o expoente de $\mathfrak{p}$ na fatoração de $\mathfrak{b}$ em um produto de ideais primos.

$$n_{\mathfrak{p}}(\mathfrak{ab}) = n_{\mathfrak{p}}(\mathfrak{a}) + n_{\mathfrak{p}}(\mathfrak{b}) \tag{1.15}$$

$$\mathfrak{b} \subset \mathrm{A} \Leftrightarrow n_{\mathfrak{p}}(\mathfrak{b}) \geq 0 \quad \forall\, \mathfrak{p} \in \mathrm{P}. \tag{1.16}$$

($\Rightarrow$ $\mathfrak{b}$ se decompõe em um produto de ideais primos; $\Leftarrow$ claro).

$$\mathfrak{a} \subset \mathfrak{b} \Leftrightarrow n_{\mathfrak{p}}(\mathfrak{a}) \geq n_{\mathfrak{p}}(\mathfrak{b}) \quad \forall\, \mathfrak{p} \in \mathrm{P}. \tag{1.17}$$

(basta observar que $\mathfrak{a} \subset \mathfrak{b}$ é o mesmo que $\mathfrak{a}\mathfrak{b}^{-1} \subset \mathrm{A}$. Agora aplicar (1.15) e (1.16)).

Seja K um corpo numérico, n seu grau. Sabemos que existem n isomorfismo distintos $\sigma_i : \mathrm{K} \to \mathbb{C}$. Seja $\alpha : \mathbb{C} \to \mathbb{C}$ a conjugação complexa. Então, para qualquer $i = 1, \ldots, n$ $\alpha \circ \sigma_i = \sigma_j$, $1 \leq j \leq n$, e $\sigma_i = \sigma_j$ se, e somente se, $\sigma_i(\mathrm{K}) \subset \mathbb{R}$. Escrevamos r_1 para o número de índices tais que $\sigma_i(\mathrm{K}) \subset \mathbb{R}$. Então $n - r_1$ é um número par, portanto podemos escrever

$$r_1 + 2r_2 = n. \tag{1.18}$$

Vamos reenumerar os $\sigma_i's$ de maneira que $\sigma_i(\mathrm{K}) \subset \mathbb{R}$ para $1 \leq i \leq r_1$ e também que $\sigma_{j+r_2}(x) = \overline{\sigma_j(x)}$ para $r_1 + 1 \leq j \leq r_1 + r_2$. Então os primeiros $r_1 + r_2$ isomorfismos determinam o último r_2. Para $x \in \mathrm{K}$ definimos

$$\sigma(x) = (\sigma_1(x), \ldots, \sigma_{r_1+r_2}(x)) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}. \tag{1.19}$$

Chamamos σ a *imersão canônica* de K em $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$; ela é um homomorfismo, injetivo, de aneis. Frequentemente identificaremos $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ com $\mathbb{R}^n$ (veja (1.18)). As notações σ, K, n, r_1, e r_2 serão usadas durante o restante dessa seção.

A prova da proposição a seguir utiliza noções de análise, como subgrupos discretos de $\mathbb{R}^n$ e medida de Lebesgue, (seria necessário desenvolver um vasto material preliminar) e por isso será omitida. O leitor poderá encontrá-la em [23].

Proposição 1.39 *Seja* K *um corpo numérico, n seu grau, r_1 e r_2 os inteiros definidos anteriormente, d o discriminante de* K*, e $\mathfrak{a}$ um ideal inteiro não-nulo de* K*. Então $\mathfrak{a}$ contém um elemento não-nulo x tal que*

$$|\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(x)| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d|^{1/2} \mathrm{N}(\mathfrak{a}). \tag{1.20}$$

Corolário 1.40 *Com as mesmas notações, toda classe de ideais de* K *contém um ideal inteiro $\mathfrak{b}$ tal que*

$$\mathrm{N}(\mathfrak{b}) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d|^{1/2}. \tag{1.21}$$

Prova. Seja $\mathfrak{a}'$ um ideal da classe dada. Multiplicando $\mathfrak{a}'$ por um ideal principal, podemos supor que $\mathfrak{a} = \mathfrak{a}'^{-1}$ é um ideal inteiro. Tome um elmento não-nulo $x \in \mathfrak{a}$ para o qual (1.20) é verdade. Então $\mathfrak{b} = x\mathfrak{a}^{-1}$ é um ideal inteiro na mesma classe que $\mathfrak{a}'$, e $\mathrm{N}(\mathfrak{b})$ satisfaz (1.21) em virtude da multiplicidade da norma, proposição 1.38. ■

Como existe sempre um ideal inteiro não-nulo $\mathfrak{b}$ em K e $\mathrm{N}(\mathfrak{b}) \geq 1$, obtemos, a partir de (1.21), $|d|^{1/2} \geq (\pi/4)^{r_2}(n^n/n!)$. Sendo $\pi/4 < 1$ e $2r_2 < n$ concluímos que $|d| \geq a_n$, onde $a_n = (\pi/4)^n[n^{2n}/(n!)^2]$. Pela fórmula do binômio, observamos que

$$a_2 = \frac{\pi^2}{4} \quad \text{e} \quad \frac{a_{n+1}}{a_n} = \frac{\pi}{4}\left(1 + \frac{1}{n}\right)^{2n} = \frac{\pi}{4} \quad (1 + 2 + \text{termos positivos}),$$

portanto $a_{n+1}/a_n \geq 3\pi/4$. Logo, para $n \geq 2$,

$$|d| \geq \frac{\pi^2}{4}\left(\frac{3\pi}{4}\right)^{n-2}.$$

Resumindo, temos a seguinte desigualdade

Corolário 1.41 *Seja* K *um corpo numérico, n seu grau, e seja d seu discriminante. Então, para* $n \geq 2$*,*

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

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

A majoração uniforme de $n/(\log|d|)$ segue tomando logarítimos.

Teorema 1.42 (Hermite-Minkowski) *Para qualquer corpo numérico* $\mathrm{K} \neq \mathbb{Q}$*, o discriminante de* K *é* $\neq \pm 1$*.*

Prova. Usando o corolário 1.41 vemos que $|d| \geq (\pi/3)(3\pi/4)^{n-1}$. Desde que $\pi/3 > 1$ e $3\pi/4 > 1$, temos que $|d| > 1$. ■

Estamos finalmente em condiçoes de provar o principal teorema dessa seção.

Teorema 1.43 (Dirichlet) *Para qualquer corpo numérico* K *o grupo de classe de ideais é finito.*

Prova. Pelo corolário 1.40 é suficiente mostrar que, para todo inteiro positivo q, o conjunto de todos os ideais inteiros $\mathfrak{b}$ de K que tem norma q é um conjunto finito. Para

um tal ideal $\mathfrak{b}$ temos $\sharp(\mathrm{A}/\mathfrak{b}) = q$. Segue que $q \in \mathfrak{b}$, pois para qualquer grupo a ordem de um elemento divide a ordem do grupo. Assim nossos ideais $\mathfrak{b}$ estão entre aqueles que contém Aq, e, pela fórmula (1.17) (ou pela finitude de A/Aq), só pode haver um número finito de tais ideais. ■

Definição 1.44 *O número de classes de ideais de um corpo numérico* A *é chamado o* número de classe *de* K.

Capítulo 2

Alguns conceitos elementares sobre formas modulares

Seja SL_2 o grupo das matrizes 2×2 com determinante igual a 1, mais precisamente $SL_2(R)$ denota os elementos de SL_2 que tem entradas em um anel R. Aqui estamos interessados no caso em que R é o anel $\mathbb{Z}$ dos inteiros racionais, isto é, $SL_2(\mathbb{Z})$, o qual é chamado *grupo modular*.

Neste capítulo, trataremos de algumas relações entre a geometria não euclidiana e a teoria dos números. O modelo da geometria não euclidiana considerado aqui é o da geometria hiperbólica do plano superior $\mathfrak{H}$, também conhecido como plano *Poincaré*. O conjunto $\mathfrak{H}$ consiste de números complexos com suas partes imaginárias positivas (veja definição 2.7). Essa conexão começa por meio do grupo $SL_2(\mathbb{R})$, seu subgrupo como $SL_2(\mathbb{Z})$ e subgrupos de congruência (veja seção 2.1).

O grupo $SL_2(\mathbb{R})$ e seus subgrupos agem sobre o conjunto $\mathfrak{H}$ e preservam a estrutura de geometria hiperbólica desse conjunto. Após um estudo básico dessa estrutura, apresentaremos o conjunto M_{2k} das formas modulares (veja definição 2.15). O fato de a matriz $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ser um elemento de $SL_2(\mathbb{Z})$ implica a evidência de as formas modulares serem periódicas de período 1. Portanto, elas tem expansões de Fourier, bem como uma conexão com a teoria dos números, pois os coeficientes dessas expansões são ricos em informações aritméticas.

Outro campo em que existem relações fundamentais entre formas modulares e teoria dos números é a área de estudos algébricos do espaço vetorial M_{2k}, pois esses são espaços vetorias complexos de dimensões finitas, onde estão definidos os operadores de Hecke,

que embora não tratados aqui, aparecem como uma ferramenta poderosa no estudo das formas modulares e das formas automorfas.

2.1 Subgrupos de congruência

Seja $M_2(\mathbb{Z})$ o anel das matrizes 2×2 com entradas em $\mathbb{Z}$, e N um inteiro positivo.

Definição 2.1 *Duas matrizes* $A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$, $B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \in M_2(\mathbb{Z})$ *são ditas* congruentes módulo N *quando* $a_i \equiv b_i \pmod{N}$, para todo $i = 1, \ldots, 4$.

Segue do fato de que a relação de congruência nos inteiros é uma relação de equivalência, que a relação de congruência entre matrizes também é uma relação de equivalencia.

Seja $\mathbb{Z}/N\mathbb{Z}$ o anel das classes de resíduos módulo N. Seja $\lambda : \mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$ o homomorfismo canônico. Podemos estender essa aplicação e definir

$$\begin{array}{rccc} \lambda_N : & SL_2(\mathbb{Z}) & \longrightarrow & SL_2(\mathbb{Z}/N\mathbb{Z}) \\ & \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \longmapsto & \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix}, \end{array}$$

onde $SL_2(\mathbb{Z}/N\mathbb{Z})$ são as matrizes 2×2 com entradas em $\mathbb{Z}/N\mathbb{Z}$ e determinante 1 ($\bar{1}$). Esse conjunto com a multiplicação de classes forma um grupo.

Lema 2.2 *λ_N é um homomorfismo de grupos.*

Prova. Sejam $A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$, $B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \in SL_2(\mathbb{Z})$. Então,

$$AB = \begin{pmatrix} a_1b_1 + a_2b_3 & a_1b_2 + a_2b_4 \\ a_3b_1 + a_4b_3 & a_3b_2 + a_4b_4 \end{pmatrix}.$$

A definição de λ_N nos mostra que

$$\begin{aligned} \lambda_N &= \begin{pmatrix} \overline{a_1b_1 + a_2b_3} & \overline{a_1b_2 + a_2b_4} \\ \overline{a_3b_1 + a_4b_3} & \overline{a_3b_2 + a_4b_4} \end{pmatrix} \\ &= \begin{pmatrix} \overline{a_1}\overline{b_1} + \overline{a_2}\overline{b_3} & \overline{a_1}\overline{b_2} + \overline{a_2}\overline{b_4} \\ \overline{a_3}\overline{b_1} + \overline{a_4}\overline{b_3} & \overline{a_3}\overline{b_2} + \overline{a_4}\overline{b_4} \end{pmatrix} \\ &= \lambda_N(A)\lambda_N(B). \qquad \blacksquare \end{aligned}$$

Definição 2.3 *O núcleo do homomorfismo* λ_{N} *é o* subgrupo de congruência principal de nível N *de* $\mathrm{SL}_2(\mathbb{Z})$.

Por meio dessa definição podemos escrerver

$$\begin{aligned}\Gamma(\mathrm{N}) &= \mathrm{Ker}\,(\lambda_{\mathrm{N}}) = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \lambda_{\mathrm{N}}(\gamma) = \mathrm{I}\} \\ &= \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid a \equiv d \equiv 1 \,(\mod \mathrm{N}), c \equiv b \equiv 0 \,(\mod \mathrm{N})\},\end{aligned}$$

onde $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, e I é a matriz identidade em $\mathrm{SL}_2(\mathbb{Z}/\mathrm{N}\mathbb{Z})$.

Um *subgrupo de congruência* (de nível N) é um subgrupo de $\mathrm{SL}_2(\mathbb{Z})$ que contém o subgrupo de congruência principal de $\mathrm{SL}_2(\mathbb{Z})$.

Exemplos.

1. Seja $\Gamma_0(\mathrm{N})$ o *subgrupo de Hecke* definido por

$$\Gamma_0(\mathrm{N}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0 \,(\mod \mathrm{N}) \right\}.$$

   É claro que $\Gamma(\mathrm{N}) \subset \Gamma_0(\mathrm{N})$ qualquer que seja o inteiro N. Portanto, $\Gamma_0(\mathrm{N})$ é um subgrupo de congruência de $\mathrm{SL}_2(\mathbb{Z})$. $\Diamond$

2. $\Gamma_1(\mathrm{N}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid a \equiv d \equiv 1 \,(\mathrm{mod}\ \mathrm{N}), c \equiv 0 \,(\mathrm{mod}\ \mathrm{N}) \right\}$ é um subgrupo de congruência de $\mathrm{SL}_2(\mathbb{Z})$. $\Diamond$

2.1.1 O cálculo do índice

Vamos aqui calcular o índice $[\Gamma_0(\mathrm{N}) : \Gamma_1(\mathrm{N})]$ baseado nos lemas a seguir, os quais são bastantes simples e por isso provaremos apenas o primeiro.

Lema 2.4 $\Gamma_0(\mathrm{N})$ *e* $\Gamma_1(\mathrm{N})$ *são subgrupos de* $\mathrm{SL}_2(\mathbb{Z})$.

Prova. Sejam α e β dois elementos de $\Gamma_0(\mathrm{N})$. É claro que $\det(\alpha \cdot \beta) = \det(\alpha) \cdot \det(\beta) = 1 \cdot 1 = 1$, isto é, $\alpha\beta$ pertence a $\mathrm{SL}_2(\mathbb{Z})$. Agora sendo $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ e $\beta = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$ temos $\alpha \cdot \beta = \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix}$. Naturalmete, $c \equiv 0 \,(\mathrm{mod}\ \mathrm{N})$ e também $g \equiv 0 \,(\mathrm{mod}\ \mathrm{N})$ nos dá $(ce + cg) \equiv 0 \,(\mathrm{mod}\ \mathrm{N})$. Logo $\alpha\beta \in \Gamma_0(\mathrm{N})$. Finalmente, é claro que $\alpha^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in \Gamma_0(\mathrm{N})$. O caso $\Gamma_1(\mathrm{N})$ é análogo. ■

Lema 2.5 *$\Gamma_1(\mathrm{N})$ é um subgrupo normal de $\Gamma_0(\mathrm{N})$.*

Lema 2.6 *$\Gamma_0(\mathrm{N})/\Gamma_1(\mathrm{N})$ é isomorfo a $(\mathbb{Z}/\mathrm{N}\mathbb{Z})^*$.*

Daí podemos concluir que

$$[\Gamma_0(\mathrm{N}) : \Gamma_1(\mathrm{N})] = |\Gamma_0(\mathrm{N})/\Gamma_1(\mathrm{N})| = |(\mathbb{Z}/\mathrm{N}\mathbb{Z})^*| = \varphi(\mathrm{N}),$$

onde φ é a função de Euler. Logo,

$$[\Gamma_0(\mathrm{N}) : \Gamma_1(\mathrm{N})] = \mathrm{N}\prod_{p|\mathrm{N}}(1+p^{-1}),$$

onde o produtório é calculado sobre os primos p que dividem o inteiro N.

2.2 A ação de $\mathrm{SL}_2(\mathbb{Z})$ sobre $\mathfrak{H}$

Nesta seção, estudaremos o plano superior $\mathfrak{H}$ e a ação dos subgrupos de $\mathrm{SL}_2(\mathbb{Z})$ sobre ele. O plano superior é um modelo da geometria não euclidiana conhecida como *geometria hiperbólica*. O grupo $\mathrm{SL}_2(\mathbb{Z})$ age sobre $\mathfrak{H}$, e isso nos permite estudar (por meio da geometria de $\mathfrak{H}$) as formas modulares.

Teoricamente, uma maneira geral de estudar um grupo é por meio de suas ações e representações em um espaço. Reciprocamente, para estudar um espaço, podemos investigar seu grupo de automorfismo. Essa é uma parte da filosofia geral por detrás da teoria das formas modulares.

Definição 2.7 *O conjunto $\mathfrak{H} := \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ é chamado* plano superior.

O grupo $\mathrm{SL}_2(\mathbb{Z})$ e seus subgrupos agem sobre $\mathfrak{H}$ da seguinte forma:
se $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ e $z \in \mathfrak{H}$, definimos a ação de $\mathrm{SL}_2(\mathbb{Z})$ sobre $\mathfrak{H}$ por

$$g \cdot z := g(z) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d} \tag{2.1}$$

Lema 2.8 (a) *Para todo $g \in \mathrm{SL}_2(\mathbb{Z})$, $z \in \mathfrak{H}$, $cz + d \neq 0$.*

(b) *Para todo $g \in \mathrm{SL}_2(\mathbb{Z})$, $z \in \mathfrak{H}$, $g \cdot z \in \mathfrak{H}$.*

(c) *Para todo $z \in \mathfrak{H}$, $\mathrm{I} \cdot z = z$.*

(d) *Para todo* $g_1, g_2 \in \mathrm{SL}_2(\mathbb{Z})$, $z \in \mathfrak{H}$, $(g_1 g_2) \cdot z = g_1 \cdot (g_2 \cdot z)$.

Prova. seja $z = x + iy$. Suponha que $cz + d = 0$, então $cx + d = 0$, $cy = 0$. Se $c \neq 0$, então $y = 0$. Mas isso é um absurdo pois $y = \mathrm{Im}(z) > 0$. Assim $c = 0$ e, portanto, $d = 0$. Mas isso é novamente um absurdo, pois $\det(g) = ad - bc = 1 \neq 0$. Isso prova a parte (a). Para a parte (b) basta mostrar que $\mathrm{Im}(g \cdot z) > 0$. Mas

$$\begin{aligned} \mathrm{Im}(g \cdot z) &= \mathrm{Im}\left(\frac{az+b}{cz+d}\right) \\ &= \mathrm{Im}\left(\frac{ac(x^2+y^2) + adx + bcx + bd - (bc-ad)yi}{(cx+d)^2 + (cy)^2}\right) \\ &= \frac{y}{|cz+d|^2} > 0. \end{aligned}$$

Dessa forma, $g \cdot z \in \mathfrak{H}$. (c) é evidente e para (d) basta tomar $g_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$, $g_2 = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ e fazer $g_1 g_2 = \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix}$. Assim,

$$\begin{aligned} (g_1 g_2) \cdot z &= \frac{(a_1a_2 + b_1c_2)z + a_1b_2 + b_1d_2}{(c_1a_2 + d_1c_2)z + c_1b_2 + d_1d_2} = \frac{a_1a_2z + b_1c_2z + a_1b_2 + b_1d_2}{c_1a_2z + d_1c_2z + c_1b_2 + d_1d_2} \\ &= g_1 \cdot \frac{a_2z + b_2}{c_2z + d_2} = g_1 \cdot (g_2 \cdot z). \quad \blacksquare \end{aligned}$$

Segue imediatamente do lema anterior o seguinte

Corolário 2.9 *A fórmula* (2.1) *é bem definida e define a ação de* $\mathrm{SL}_2(\mathbb{Z})$ *sobre* $\mathfrak{H}$.

2.2.1 A compactação de $\mathfrak{H}$

O espaço $\mathfrak{H}$ é um espaço topológico com a topologia induzida de $\mathbb{C}$. Se $z \in \mathfrak{H}$ as vizinhanças de z são os discos abertos $\mathrm{D}(z, r)$ de centro z e raio r. O processo de compactação de $\mathfrak{H}$ é o mesmo de $\mathbb{C}$ nos cursos de variável complexa. Portanto, para a compactação de $\mathfrak{H}$, definimos o novo espaço $\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{R} \cup \{\infty\}$ formado pela união de $\mathfrak{H}$ e sua fronteira $\mathbb{R} \cup \{\infty\}$. No espaço $\mathfrak{H}^*$ definimos a seguinte topologia:

1. Se $z \in \mathfrak{H}$, as vizinhanças de z são discos abertos com centro z contidos em $\mathfrak{H}$.

2. Se $z \in \mathbb{R}$, as vizinhanças de z são as uniões de $\{z\}$ e os interiores de discos fechados contidos em $\mathfrak{H}$ e tangentes a z.

3. As vizinhanças de ∞ são conjuntos da forma

$$\mathrm{V}_\alpha = \{z \in \mathfrak{H} \mid \mathrm{Im}(z) > \alpha\}$$

e $\alpha \in \mathbb{R}$.

Uma das propriedades fundamentais de $\mathfrak{H}^*$ é que a ação de $\mathrm{SL}_2(\mathbb{Z})$ sobre $\mathfrak{H}$ pode ser estendida ao espaço compactado $\mathfrak{H}^*$. De fato, se $z \in \mathbb{R}$, a ação é a mesma da fórmula (2.1). Quando $z = \infty$, definimos a ação por

$$g \cdot \infty = \lim_{z \to \infty} \frac{az + b}{cz + d},$$

(onde $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ é um elemento de $\mathrm{SL}_2(\mathbb{Z})$) no sentido de variável complexa.

2.2.2 Pontos fixos

Por razões geométricas e algébricas, é fundamental conhecer os pontos fixos da ação de $\mathrm{SL}_2(\mathbb{Z})$. Para um estudo elementar dos pontos fixos, primeiro observemos que qualaquer subgrupo $\mathrm{G} \subseteq \mathrm{SL}_2(\mathbb{Z})$ age sobre $\mathfrak{H}$ (e repectivamente $\mathfrak{H}^*$) da mesma forma que $\mathrm{SL}_2(\mathbb{Z})$.

Definição 2.10 *Um* ponto fixo *de um subgrupo* $\mathrm{G} \subseteq \mathrm{SL}_2(\mathbb{Z})$ *é um ponto* $z \in \mathfrak{H}^*$ *(respectivamente* $\mathfrak{H}$*), tal que para algum* $g \in \mathrm{G}$, $g \neq \pm\mathrm{I}$ *(caso* $-\mathrm{I} \in \mathrm{G}$*) vale a igualdade*

$$g \cdot z = z.$$

Seja $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{G} \subseteq \mathrm{SL}_2(\mathbb{Z})$. Essa definição mostra-nos que os pontos fixos de G são raízes da equação

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = z.$$

E essa equação nos leva a uma equação do segundo grau

$$cz^2 + (d - a)z - b = 0. \tag{2.2}$$

O discriminante dessa equação é $\Delta = (d-a)^2 - 4bc$, que após o uso de $ad - bc = 1$ pode ser escrito como $\Delta = (a+d)^2 - 4$. Mas $a + d = \mathrm{tr}\,(g)$, então para estudar as raízes da equação (2.2), devemos considerar as seguintes possibilidades:

1. $\mathrm{tr}^2(g) - 4 > 0$,
2. $\mathrm{tr}^2(g) - 4 = 0$,
3. $\mathrm{tr}^2(g) - 4 < 0$.

E definimos:

Definição 2.11 *Seja $g \in \mathrm{G}$. Dizemos que:*

(1) *g é* hiperbólico $\Leftrightarrow |\mathrm{tr}(g)| > 2$,

(2) *g é* parabólico $\Leftrightarrow |\mathrm{tr}(g)| = 2$,

(3) *g é* elíptico $\Leftrightarrow |\mathrm{tr}(g)| < 2$.

Seja $\mathrm{G} \subseteq \mathrm{SL}_2(\mathbb{Z})$ um subgrupo. Um ponto $z \in \mathfrak{H}^*$ é *hiperbólico* para G (respec. *parabólico, elíptico*) quando existe um elemento $g \in \mathrm{G}$ e $g \neq \pm \mathrm{I}$ hiperbólico (respec. parabólico, elíptico), tal que z é seu ponto fixo.

Exemplos.

1. o elemento $\begin{pmatrix} \pi & -1 \\ 0 & \pi^{-1} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$ é hiperbólico.
2. $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ é um elemento parabólico de $\mathrm{SL}_2(\mathbb{Z})$.
3. Se $g \in \mathrm{SL}_2(\mathbb{Z})$ e $|\mathrm{tr}(g)| = 2$, então $|\mathrm{tr}(g^2)| = 2$. Suponha que $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ satisfaz a condição $\mathrm{tr}(g) = \pm 2$. Então $a + b = \pm 2$. Mas $\mathrm{tr}(g^2) = a^2 + b^2 + 2bc$. Usando o fato de que $ad - bc = 1$, temos que $\mathrm{tr}(g^2) = \mathrm{tr}^2(g) - 2$. E isso mostra que $|\mathrm{tr}(g^2)| = 2$. Como consequência, temos que as potências de um elemento parabólico são parabólicos.
4. Usando o exemplo acima, podemos imaginar que se g_1 e g_2 são parabólicos, então o produto deles também o é. Mas isso nem sempre é verdade, pois os elementos $g_1 = \begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix}$ e $g_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ são ambos parabólicos, e o produto tem traço 1, ou seja, é não parabólico.

Aqui o que mais nos interessa são os pontos fixos de subgrupos de congruência. Começando com o grupo $\mathrm{SL}_2(\mathbb{Z})$, temos a seguinte proposição.

Proposição 2.12 (a) *Qualquer ponto parabólico de* $\mathrm{SL}_2(\mathbb{Z})$ *é um número racional ou* ∞.

(b) *Se z é um ponto parabólico, para todo $g \in \mathrm{SL}_2(\mathbb{R})$, $g \cdot z$ também o é.*

(c) *Todos os números racionais são pontos parabólicos de* $\mathrm{SL}_2(\mathbb{Z})$.

Prova. (a) Seja $z \in \mathfrak{H}^*$ um ponto parabólico para $\mathrm{SL}_2(\mathbb{Z})$. Então, por definição, existe um elemento $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, com $\gamma \neq \mathrm{I}$, tal que $\gamma(z) = z$ (z é ponto fixo de $\mathrm{SL}_2(\mathbb{Z})$). Essa igualdade leva-nos à equação quadrática com coeficientes inteiros:

$$cz^2 + (d-a)z - b = 0.$$

Mas sendo γ um elemento parabólico, temos que $\mathrm{tr}\,(\gamma) = |a+d| = 2$. Daí, as raízes são racionais. O ∞ é o ponto fixo do elemento parabólico $\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Para provar a parte (b), basta achar um elemento parabólico $\delta \in \mathrm{SL}_2(\mathbb{Z})$, tal que $\delta(\gamma \cdot z) = \gamma \cdot z$. Para isso, seja α o elemento parabólico de $\mathrm{SL}_2(\mathbb{Z})$ que fixa z. Ponha $\delta := \gamma\alpha\gamma^{-1}$. É claro que δ é parabólico, pois $\mathrm{tr}\,(\delta) = \mathrm{tr}\,(\alpha)$. Mas também

$$\delta(\gamma \cdot z) = \gamma\alpha\gamma^{-1}(\gamma \cdot z) = \gamma\alpha \cdot z = \gamma \cdot z.$$

Isso completa a prova da parte (b). Para a parte (c), seja $r = \dfrac{m}{n} \in \mathbb{Q}$ com m.d.c. $(m,n) = 1$. Existem inteiros p e q tais que $\gamma = \begin{pmatrix} m & q \\ n & p \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ (de fato, m.d.c. $(m,n) = 1$ implica que existem $x, y \in \mathbb{Z}$ tais que $mx + ny = 1$. Daí, $mx - n(-y) = 1$. Basta tomar $p = x$ e $q = -y$). Agora,

$$\gamma \cdot \infty = \lim_{z \to \infty} \frac{mz+q}{nz+p} = \frac{m}{n}.$$

Mas ∞ é um ponto parabólico para $\mathrm{SL}_2(\mathbb{Z})$, segue então da parte (b) que $\gamma \cdot \infty = \dfrac{m}{n}$ é um ponto parabólico para $\mathrm{SL}_2(\mathbb{Z})$. ■

2.2.3 O modelo do disco unitário

Apesar de $\mathfrak{H}$ parecer uma região não limitada de $\mathbb{C}$, ele é uma região limitada! Mais precisamente, dizemos que um conjunto $\mathcal{R}$ em $\mathbb{C}$ é uma região limitada quando ele pode ser transformado num conjunto limitado. De forma exata definimos:

Definição 2.13 *Seja $\mathcal{R} \subseteq \mathbb{C}$ um conjunto aberto e conexo ($\mathcal{R}$ é uma região). Dizemos que $\mathcal{R}$ é* limitado *se existe um domínio limitado (contido num disco de raio finito) $\mathcal{D} \subseteq \mathbb{C}$ e uma função $\varphi : \mathcal{R} \to \mathcal{D}$, tal que*

(1) *φ é bijetora;*

(2) *φ é holomorfa;*

(3) *φ^{-1} é holomorfa.*

Lema 2.14 *$\mathfrak{H}$ é uma região limitada (domínio limitado) de $\mathbb{C}$.*

Prova. Seja $\mathrm{D} = \{w \in \mathbb{C} \mid |w| < 1\}$ o disco unitário aberto em $\mathbb{C}$. Seja $c : \mathfrak{H} \to \mathrm{D}$ a aplicação que associa a cada $z \in \mathfrak{H}$ o número complexo $w = \dfrac{z-i}{z+i}$. É claro que dado $z \in \mathfrak{H}$ o fato de $\mathrm{Im}(z) > 0$ implica $c(z) \in \mathrm{D}$. Fazendo $z = x + iy$, temos

$$\begin{aligned} c(z) &= \frac{x+iy-i}{x+iy+i} = \frac{x+(y-1)i}{x+(y+1)i} \\ &= \frac{x^2+y^2-1-2xi}{x^2+(y+1)^2} \\ &= \frac{x^2+y^2-1}{x^2+(y+1)^2} - \frac{2x}{x^2+(y+1)^2}i. \end{aligned}$$

Assim $c(x,y) = u(x,y)+v(x,y)i$, onde $u(x,y) = \dfrac{x^2+y^2-1}{x^2+(y+1)^2}$ e $v(x,y) = -\dfrac{2x}{x^2+(y+1)^2}$. Agora utilizando as equacões de *Cauchy-Riemman* podemos observar que c é uma função holomorfa em $\mathfrak{H}$. Observemos ainda que $c^{-1}(w) = \dfrac{(w+1)i}{1-w}$ é a inversa de c, a qual podemos mostrar ser também holomorfa de forma análoga ao que fizemos anteriormente. Portanto, $\mathfrak{H}$ é limitado. ■

2.3 Formas modulares

Nesta seção introduziremos o conceito preciso de formas modulares e estudaremos alguns de seus aspectos clássicos.

2.3.1 Formas modulares de valor par

As formas modulares aparecem de maneira natural em varios contextos da matemática, tais como variável complexa e teoria dos números.

Definição 2.15 *Seja k um inteiro positivo. Uma* forma modular *de valor $2k$ para $\mathrm{SL}_2(\mathbb{Z})$ é uma função holomorfa $f : \mathfrak{H} \cup \{\infty\} \to \mathbb{C}$ satisfazendo a condição:*

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^{2k} f(z),\ z \in \mathfrak{H} \quad e \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \tag{2.3}$$

O número $2k$ é chamado *valor* da forma f. Quando $f\left(\frac{az+b}{cz+d}\right) = f(z)$, dizemos que f é uma *forma modular de valor zero* ou uma *forma automorfa*.

Exemplo 2.16 Seja $z \in \mathfrak{H}$ e k um inteiro maior ou igual a 1. Considere a soma infinita

$$\mathrm{G}_{2k} = \frac{1}{2} \sum_{(m,n)\neq(0,0)} (mz+n)^{-2k},$$

onde a soma percorre os inteiros m, n que não são zero ao mesmo tempo.

Vejamos algumas propriedades dessa série.

(1) $\mathrm{G}_{2k}\left(\frac{az+b}{cz+d}\right) = (cz+d)^{2k}\mathrm{G}_{2k}(z)$ para todo $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.

Para verificar isso, fazemos os seguintes cálculos:

$$\begin{aligned}
\mathrm{G}_{2k}\left(\frac{az+b}{cz+d}\right) &= \frac{1}{2} \sum_{(m,n)\neq(0,0)} \left(m\frac{az+b}{cz+d} + n\right)^{-2k} \\
&= \frac{1}{2} \sum_{(m,n)\neq(0,0)} \left(\frac{maz+mb+ncz+nd}{cz+d}\right)^{-2k} \\
&= \frac{1}{2} \sum_{(m,n)\neq(0,0)} \frac{1}{(cz+d)^{-2k}} ((ma+nc)z + (mb+nd))^{-2k} \\
&= \frac{1}{2}(cz+d)^{2k} \sum_{(m,n)\neq(0,0)} ((ma+nc)z + (mb+nd))^{-2k}.
\end{aligned}$$

Vamos mostrar que $(ma+nc, mb+nd) \neq (0,0)$. Suponha o contrário, que essa desigualdade não é verdadeira. Então temos o seguinte sistema de equações

$$\begin{cases} ma+nc &= 0 \\ mb+nd &= 0. \end{cases}$$

Mas $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0$, portanto o sistema tem as soluções $m = 0$, $n = 0$. Isso é uma contradição a nossa suposição.

(2) $G_{2k}(z)$ é uma função analítica em $\mathfrak{H}$.

Para provar isso, vamos provar que G_{2k} é uma função analítica no plano $\mathbb{C}$. Provaremos que G_{2k} é absoluta e uniformemente convergente em todos os conjuntos compactos do plano (inclusive no ∞)[1]. Agora, seja $z \in \mathbb{C}$ e

$$L_z := \{mz + n \mid m, n \in \mathbb{Z}\}.$$

É claro que L_z é um reticulado em $\mathbb{C}$ gerado por $\{1, z\}$. Seja r um inteiro positivo e π_r o paralelogramo

$$\pi_r := \{\pm rz + n; nz \pm r \mid -r \leq n \leq r\}.$$

Esse paralelogramo tem 8 vértices (ou seja, π_r tem 8 pontos de reticulados em seu perímetro). Suponha que h é a distância mínima de π_1 até a origem. Portanto, rh é distância mínima de π_r até a origem. Logo podemos concluir que

$$|mz + n| \geq rh, \quad \text{se} \quad mz + n \in \pi_r.$$

Implicando

$$\sum_{(m,n)\in\pi_r} \frac{1}{|mz+n|^{2k}} \leq \frac{8r}{(hr)^{2k}} = 8h^{-2k}\frac{1}{r^{2k-1}}$$

e

$$\begin{aligned}\sum_{r=1}^{\infty}\sum_{(m,n)\in\pi_r} \frac{1}{|mz+n|^{2k}} &= \sum_{r=1}^{\infty}\sum_{(m,n)\in\pi_r} \frac{1}{|mz+n|^{2k}} \\ &\leq 8h^{-2k}\sum_{r=1}^{\infty}\frac{1}{r^{2k-1}} < \infty.\end{aligned}$$

Esse é o resultado desejado. $\Diamond$

Definição 2.17 *Seja $z \in \mathfrak{H}$. A série $G_{2k}(z)$ é chamada* série de Eisenstein generalizada.

Portanto a série de Eisenstein generalizada é uma forma modular de valor $2k$ para $SL_2(\mathbb{Z})$.

Denotamos por M_{2k} o conjunto ds formas modulares de valor $2k$ e por M_0 o conjunto das formas modulares de valor zero para o grupo $SL_2(\mathbb{Z})$.

[1]Veja, por exemplo, [29] para verificar por que isso implica que a função G_{2k} é analítica em $\mathfrak{H}$ e em $\mathfrak{H} \cup \{\infty\}$

Teorema 2.18 M_{2k} *é um espaço vetorial complexo.*

Prova. Sejam f e g duas formas modulares de valor $2k$ para $\mathrm{SL}_2(\mathbb{Z})$. É claro que $(f+g)(z) := f(z) + g(z)$ é uma função holomorfa que satisfaz (2.3). Assim, $f+g$ é uma forma modular de valor $2k$. Também é fácil ver que a função $(\alpha f)(z) := \alpha f(z)$ para todo $\alpha \in \mathbb{C}$ é uma forma modular de valor $2k$. Portanto, M_{2k} é um espaço vetorial sobre o corpo dos números complexos. ■

Usando $g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ em (2.3), temos que $f(z+1) = f(z)$. Isso nos diz que f é periódica de período 1. Assim tal função pode ser escrita como uma soma infinita que envolve as funções trigonométricas sen e cos . Mais precisamente, f pode ser escrita como a série infinita (expansão de Laurent)

$$f(z) = \sum_{n=-\infty}^{+\infty} a(n) e^{2\pi i n z}$$

com coeficientes $a(n)$.

Como podemos ver, o teorema 2.18 não mostra se a dimensão do espaço vetorial M_{2k} é finita ou infinita, o que é importante para entender esse espaço o melhor possível. Um dos objetivos fundamentais da teoria das formas modulares é investigar e descobrir as propriedades do espaço vetorial M_{2k}. O exemplo 2.16 é importante no seguinte sentido: usando um pouco de variável complexa, pode-se estudar aspectos algébricos e aritméticos do espaço M_{2k} e classificar esse espaço por meio das séries generalizadas de Eisenstein.

A título de informação temos que o espaço vetorial M_{2k} é de dimensão finita. Mais precisamente temos o seguinte

Teorema 2.19 *São verdadeiras as expressões:*

(1) $\mathrm{M}_0 = \mathbb{C}$*;*

(2) $\mathrm{M}_2 = \{0\}$*;*

(3) $\mathrm{M}_{2k} = \mathbb{C} \cdot \mathrm{G}_{2k}$*, para* $k = 2, 3, 4, 5$*;*

(4) $\mathrm{M}_{2k+12} = \mathbb{C} \oplus \mathrm{M}_{2k}$*,* $k \geq 6$*;*

(5) *A dimensão do espaço vetorial complexo* M_{2k} *é:*

$$\dim_{\mathbb{C}}(\mathrm{M}_{2k}) = \begin{cases} [k/6], & se \quad k \equiv 1 \ (\mod 6), \\ [k/6]+1, & se \quad k \not\equiv 1 \ (\mod 6). \end{cases}$$

Lembrando que $[x]$ denota a parte inteira de x, isto é, o maior inteiro n tal que $n \leq x$.

A prova desse teorema foge do escopo do nosso trabalho. O leitor interessado pode encontrá-la em Serre [25], Shimura [26] ou ainda Shokranian [28]. Um pouco mais adiante, os autores apresentam ainda uma base para o espaço M_{2k} fazendo novamente uso das séries generalizadas de Eisenstein.

2.3.2 A expansão de Fourier

Uma boa maneira de estudar as funções complexas e, naturalmente, as formas modulares é por meio de seus coeficientes na expansão de Laurent. Para formas modulares, existe uma expansão mais usada nos estudos de teoria de formas modulares e, em geral, na teoria de formas automórficas, conhecida como a expansão de Fourier. Essa expansão é baseada no fato de que as formas modulares são periódicas. Por exemplo, ja sabemos que se $f \in \mathrm{M}_{2k}$ tem-se que

$$f(u \cdot z) = f(z+1) = f(z),$$

onde $u = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. É claro que essa igualdade mostra que f é periódica de período 1. E esse fato é consequência direta da exsitência do elemento u no grupo $\mathrm{SL}_2(\mathbb{Z})$. A expansão Laurent de f no ponto parabólico ∞ (como representante de todos os pontos parabólicos de $\mathrm{SL}_2(\mathbb{Z})$) é a expansão de Fourier (ou a q-expansão) de f. Para obter essa expansão no ∞, definimos uma função adequada no disco unitário (o modelo limitado de $\mathfrak{H}$) e identificamos o ∞ com o ponto $(0,0)$ do disco. Mais precisamente, considere a função $\tilde{f}$ definida no disco sem centro $\mathrm{D} - \{(0,0)\}$ por

$$f(z) = \tilde{f}(e^{2\pi iz}).$$

Observe que quando $z \to \infty$, $e^{2\pi iz} \to 0$, pois $|e^{2\pi iz}| \to 0$ ficará óbvio que a função $\tilde{f}(e^{2\pi iz})$ também será periódica com período 1, e então, no ponto 0, ela terá a seguinte expansão de Laurent

$$\tilde{f}(e^{2\pi iz}) = \sum_{n=0}^{\infty} c(n) e^{2\pi inz}. \tag{2.4}$$

Geralmente, colocamos $q = e^{2\pi iz}$, e a expansão acima também pode ser escrita como:

$$f(z) = \tilde{f}(q) = \sum_{n=0}^{\infty} c(n) q^n. \tag{2.5}$$

Uma fórmula modular de valor $2k$ é, portanto dada, por uma série

$$f(z) = \sum_{n=0}^{\infty} c(n)q^n = \sum_{n=0}^{\infty} c(n)e^{2\pi inz},$$

a qual converge para $|q| < 1$, isto é, para $\mathrm{Im}\,(z) > 0$. Mais precisamente temos a seguinte

Definição 2.20 *A expansão* (2.4) (*respec.* (2.5)) *de* $\tilde{f}$ *no ponto* 0 *é chamada de* série de Fourier *(respec.* q-expansão*) de* f *no ponto parabólico* ∞*.*

2.3.3 Formas modulares com carácter - o espaço $\mathrm{M}_k(\Gamma, \chi)$

Para definir e estudar formas modulares para subgrupos de congruência, é necessário saber um pouco sobre os caracteres de grupos abelianos.

Considere o grupo finito abeliano $(\mathbb{Z}/r\mathbb{Z})^*$, onde r é um inteiro positivo.

Definição 2.21 *Um* carácter *do grupo abeliano finito* $(\mathbb{Z}/r\mathbb{Z})^*$ *é um homomorfismo* $\chi : (\mathbb{Z}/r\mathbb{Z})^* \to \mathbb{C}^*$.

Definição 2.22 *Um carácter* χ *é chamado* primitivo módulo r *se não existirem outros caracteres* χ' *do grupo* $(\mathbb{Z}/s\mathbb{Z})^*$*, onde* $s \mid r$*, tal que* $\chi'(x) = \chi(x)$ *para todo* x *tal que* $\mathrm{m.d.c}\,(x, r) = 1$.

Quando essa condição é satisfeita, r é chamado *condutor* de χ.

Agora queremos estender essa noção de carácter de um grupo abeliano finito para o grupo infinito dos inteiros.

Definição 2.23 *O* carácter de dirichlet *de* $\mathbb{Z}$ *é definido por*

$$\chi(c) = \begin{cases} \chi(\bar{c}), & se \quad \mathrm{m.d.c.}(c, r) = 1, \\ 0, & se \quad \mathrm{m.d.c.}(c, r) \neq 1 \end{cases}$$

onde a barra significa a congruência módulo r*.*

Em outras palavras, o carácter de Dirichilet de $\mathbb{Z}$ para todos os inteiros relativamente primos com r assume o valor do carácter $(\mathbb{Z}/r\mathbb{Z})^*$, e se um número não é relativamente primo com r, o valor do carácter de Dirichlet será zero para esse número.

Para termos uma ideia de como deveria ser a definição de formas modulares para subgrupos de congruência, consideremos a função **theta de Jacobi**, que tem a seguinte expansão de Fourier:

$$\Theta_J(z) = \sum_{n\in\mathbb{Z}} e^{\pi i z n^2}.$$

Essa função não é de período 1, pois $\Theta_J(z+1) \neq \Theta_J(z)$. Em outras palavras, essa função não é invariante pela ação do grupo $\mathrm{SL}_2(\mathbb{Z})$, pois não é invariante pela matriz $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ de $\mathrm{SL}_2(\mathbb{Z})$. Portanto, a função *theta* de Jacobi não pode ser uma forma modular para o grupo $\mathrm{SL}_2(\mathbb{Z})$. Mas uma observação cuidadosa leva-nos a deduzir que

$$\Theta_J(z+2) = \Theta_J(z).$$

Então, é possível que $\Theta_J(z)$ seja uma forma modular para o grupo de congruência $\Gamma(2)$ (que na verdade é). Como outro exemplo considere a função *theta*

$$\Theta(z) = \sum_{n\in\mathbb{Z}} q^{n^2} = \sum_{n\in\mathbb{Z}} e^{2\pi i z n^2}.$$

Nesse caso, $\Theta(z+1) = \Theta(z)$, mas $\Theta\left(-\dfrac{1}{z}\right) \neq z^{2k}\Theta(z)$. Então, função *theta* não obedece à equação funcional das formas modulares para o elemento $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ de $\mathrm{SL}_2(\mathbb{Z})$. Mas

$$\Theta\left(-\frac{1}{4z}\right) = \left(\frac{2z}{i}\right)^{\frac{1}{2}} \Theta(z).$$

É possível provar que essa igualdade é a equação funcional para o grupo $\Gamma_0(4)$.

Apresentamos a seguir a definição de formas modulares para grupos de congruência.

Para um inteiro positivo k e um subgrupo de congruência Γ de $\mathrm{SL}_2(\mathbb{Z})$, definiremos o espaço $\mathrm{M}_k(\Gamma, \chi)$ das funções holomorfas sobre $\mathfrak{H}$. O espaço $\mathrm{M}_k(\Gamma, \chi)$ consiste de funções holomorfas sobre $\mathfrak{H}$, que satisfazem as seguintes condições:

(1) f é holomorfa no ∞ e em todos os pontos parabólicos de Γ,

(2) para um elemento $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, f tem de satisfazer a equação funcional

$$f\left(\frac{az+b}{cz+d}\right) = \chi(d)(cz+d)^k f(z),$$

onde $\chi : (\mathbb{Z}/r\mathbb{Z})^* \to \mathbb{C}^*$ é um carácter de Dirichlet de certo condutor r, a ser determinado dependendo do grupo γ.

Por exemplo, se $\Gamma = \Gamma_0(\mathrm{N})$, então $r = \mathrm{N}$, pois m.d.c. $(d, \mathrm{N}) = 1$. Em particular, observe que $\chi(d)$ é realmente um carácter de $(\mathbb{Z}/\mathrm{N}\mathbb{Z})^*$.

Definição 2.24 *O espaço* $\mathrm{M}_k(\Gamma, \chi)$ *é chamado de* espaço das formas modulares com carácter de Dirichlet χ relativo ao grupo Γ.

As formas modulares e principalmente as formas automórficas tratam-se de uma parte bastante extensa, complicada e frutífera da matemática. Muitos e conceituados matemáticos vem publicando constantemente um arsenal enorme de artigos de pesquisa em revistas e periódicos de renome internacional.

Nos limitaremos aqui a essas breves noções, porém indicamos aos leitores interessados no assunto que consultem as obras clássicas de Serre [25] e Shimura [26].

Capítulo 3

Famílias de corpos quadráticos

Chegamos agora ao ápice desta monografia. Trataremos neste capítulo dos resultados obtidos por Iwao Kimura em 2003 publicados em [16]. As formas modulares discutidas no capítulo anterior são de fundamental importância aqui e é através delas que chegamos ao teorema de Sturm, teorema 3.1, na seção 3.1. Após rápidas preliminares, na seção 3.2 demostramos os resultados principais desse trabalho.

3.1 Preliminares

Seja $k = \mathbb{Q}(\sqrt{d})$ um corpo quadrático de discriminante d. Denotamos por (d/p), $p \in \mathbb{Z}$ um primo racional, o *símbolo de Legendre-Kronecker* definido por

$$\left(\frac{d}{p}\right) = \begin{cases} +1, & \text{se } p \text{ se decompõe em } k; \\ 0, & \text{se } p \text{ se ramifica em } k; \\ -1, & \text{se } p \text{ é inerte em } k. \end{cases}$$

A seguir z denotará um número complexo cuja parte imaginária é positiva. Agora, para qualquer inteiro metade $k \in \frac{1}{2}\mathbb{Z}$ e um número natural N (se $k \notin \mathbb{Z}$ assumimos que $4 \mid \mathrm{N}$), denotemos por $\mathrm{M}_k(\mathrm{N}, \chi)$ o espaço das formas modulares de valor k e carácter de Dirichlet χ, com respeito a um subgrupo de congruência $\Gamma_0(\mathrm{N})$ do grupo linear especial $\mathrm{SL}_2(\mathbb{Z})$.

Seja $g(z) = \sum_{n=0}^{\infty} a(n)q^n$, $q = e^{2\pi iz}$, a q-expansão no infinito de $g(z) \in \mathrm{M}_k(\mathrm{N}, \chi)$. Escrevemos $g(z) \in \mathrm{M}_k(\mathrm{N}, \chi) \cap \mathbb{Q}[[q]]$ (respec. $g(z) \in \mathrm{M}_k(\mathrm{N}, \chi) \cap \mathbb{Z}[[q]]$) se os coeficientes $a(n)$ de $g(z)$ são números racionais (respec. inteiros racionais).

Para formas modulares $g(z) = \sum_{n=0}^{\infty} a(n)q^n$, $h(z) = \sum_{n=0}^{\infty} b(n)q^n \in \mathrm{M}_k(\mathrm{N}, \chi) \cap \mathbb{Z}[[q]]$ e qualquer inteiro racional m definimos $g(z) \equiv h(z) \pmod{m}$ se, e somente se, $a(n) \equiv b(n) \pmod{\mathrm{m}}$ para todo $n \geq 0$.

Seja $g = \sum_{n=0}^{\infty} a(n)q^n \in \mathbb{Z}[[q]]$ uma série de potências formais com coeficientes inteiros racionais para uma indeterminada q. Definimos a ordem $\mathrm{ord}_\ell(g)$ de g em um primo racional ℓ por

$$\mathrm{ord}_\ell(g) := \min\{n \geq 0; a(n) \not\equiv 0 \pmod{\ell}\}$$

com a convenção de $\mathrm{ord}_\ell(g) = \infty$, se $\ell \mid a(n)$ para todo n.

Precisamos do teorema de Sturm ([30]) sobre a congruência de formas modulares.

Teorema 3.1 (Sturm) *Se $g(z) \in \mathrm{M}_k(\mathrm{N}, \chi)$ possui coeficientes inteiros racionais e*

$$\mathrm{ord}_\ell(g) > \kappa(\mathrm{N}, k) = \frac{k}{12}\,[\Gamma_0(1) : \Gamma_0(\mathrm{N})] = \frac{k}{12}\mathrm{N}\prod_{q \mid \mathrm{N}}(1 + q^{-1}),$$

então $g(z) \equiv 0 \pmod{\ell}$, onde ℓ é um primo racional.

Ele prova esse fato quando k é um inteiro (uma prova detalhada pode ser encontrada em Murty [20]), mas Kohnen-Ono [18] observam que é possível verificar que o mesmo também ocorre quando k é um inteiro metade.

Seja p um primo racional qualquer. Definimos duas aplicações lineares U_p e V_p de $\mathrm{M}_k(\mathrm{N}, \chi)$ em $\mathrm{M}_k(p\mathrm{N}, \chi(p/\cdot))$ de modo usual. Para qualquer $g(z) = \sum_{n=0}^{\infty} a(n)q^n \in \mathrm{M}_k(\mathrm{N}, \chi)$, ponha

$$(U_p g)(z) = \sum_{n=0}^{\infty} a(pn)q^n, \quad (V_p g)(z) = \sum_{n=0}^{\infty} a(n)q^{pn}.$$

Uma *forma quadrática binária* f é uma função $f(x, y) = ax^2 + bxy + cy^2$ onde os coeficientes a, b e c são inteiros racionais, a qual é denotada mais abreviadamente por (a, b, c). Dizemos que a forma f é *primitiva* se m.d.c.$(a, b, c) = 1$. Dizemos ainda que f é *positiva definida* se $a > 0$. Se f e g são duas formas quadráticas, dizemos que f e g são *equivalentes* se existir uma matriz $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, tal que $g(x, y) = f(\alpha x + \beta y, \gamma x + \delta y)$.

Definição 3.2 *Seja n um inteiro não negativo. O* número de classe se Hurwitz $H(n)$ *é definido como segue.*

1. $H(n) = 0$ *se* $n \equiv 1$ *ou* $2 \pmod 4$.

2. $H(n) = -1/12$ *se* $n = 0$.

3. *caso contrário (isto é,* $n \equiv 0$ *ou* $3 \pmod 4$ *e* $n > 0$*) definimos* $H(n)$ *como o número de classes de formas quadráticas de discriminante* $-n$ *(positivas definidas) não necessariamente primitivas, exceto que formas equivalentes a* $a(x^2+y^2)$ *serão contadas com coeficiente* $1/2$*, e aquelas equivalentes a* $a(x^2+xy+y^2)$ *com coeficiente* $1/3$.

Consultando a seção 3 do capítulo 5 de Cohen [6] chegamos a seguinte relação entre o número de classe usual e o número de classe de Hurwitz que definimos anteriormente.

Teorema 3.3 *Se* $-n = \mathrm{D}f^2$ *onde* D *é um discriminante fundamental negativo, então*

$$H(n) = \frac{h(\mathrm{D})}{\omega(\mathrm{D})} \sum_{d \mid f} \mu(d) \left(\frac{\mathrm{D}}{d}\right) \sigma_1\left(\frac{f}{d}\right). \tag{3.1}$$

Aqui $h(\mathrm{D})$ é o número de classes de $\mathbb{Q}(\sqrt{\mathrm{D}})$, $\omega(D)$ é a metade do número de raizes da unidade em $\mathbb{Q}(\sqrt{\mathrm{D}})$, $\mu(\cdot)$ é a *função de Möbius* definida por $\mu(d) = (-1)^s$ se d é o produto de s primos distintos (incluindo $s = 0$), e $\mu(d) = 0$ caso contrário, $(\cdot/\cdot)$ é o símbolo de Legendre-Kronecker, e $\sigma_1(\cdot)$ é a soma dos divisores positivos.

Sejam $c, d \in \mathbb{Z}$ com $d \geq 1$. Suponha que $-c$ é um não-resíduo quadrático módulo d (isto é, que a equação $x^2 \equiv -c \pmod d$ não possui solução). Então definimos a função $\mathcal{H}^{c,d}(z)$ por

$$\mathcal{H}^{c,d}(z) = \sum_{n \equiv c \pmod d} H(n) q^n \qquad (q = e^{2\pi i z}).$$

De acordo com o corolário 3.4 de Cohen [7] sabemos que $\mathcal{H}^{c,d}(z) \in \mathrm{M}_{3/2}(\mathrm{A})$ onde $\mathrm{A} = 4d^2$. Ademais, A pode ser tomado como d^2, se d é par.

3.2 Resultados e provas

Estamos agora em condições de demonstrar nosso teorema principal, juntamente com seu corolário que, na verdade, é o resultado central desse trabalho.

Teorema 3.4 *Seja* $\ell > 3$ *um primo ímpar. Sejam* S_0, S_+, S_- *conjuntos finitos mutuamente disjuntos de primos racionais. Tome um inteiro* $b > 0$ *que satisfaz as seguintes condições:*

(a) $-b$ *é um discriminante fundamental;*

(b) $\ell \nmid h(\mathbb{Q}(\sqrt{-b}))$*;*

(c) $(-b/q) = 0, 1, -1$ *de acordo com* $q \in S_0$, S_+, S_- *respectivamente (onde* $(\cdot/\cdot)$ *é o símbolo de Legendre-Kronecker);*

Ponha $\mathrm{P} = 4\prod_{q\in S} q$*, onde* $S = S_0 \cup S_+ \cup S_-$*. Para qualquer primo* p *que satisfaz* $p^2 \equiv 1 \pmod{\mathrm{P}}$ *e* $(-b/p) \not\equiv p \pmod{\ell}$*, seja* $\kappa = \frac{1}{2}p\mathrm{P}^2 \prod_{q\,|\,p\mathrm{P}} (1 + q^{-1})$*. Existe um número natural* $m_p < \kappa$ *que satisfaz as seguintes condições:*

(i) *O número de classe do corpo quadrático imaginário* $\mathbb{Q}(\sqrt{-m_p})$ *é não divisível por* ℓ*;*

(ii) *todo primo* $q \in S_0$, S_+, S_- *se ramifica, se decompõe, é inerte, em* $\mathbb{Q}(\sqrt{-m_p})$*, respectivamente.*

K. Honrie [12] mostra a existência de um tal discriminante fundamental para um primo ℓ suficientemente grande. Podemos, dados ℓ, S_0, S_+, S_-, determminar um discriminante fundamental $-b$ que satisfaz as condições afirmadas no teorema por um cálculo numérico em muitos casos. Por exemplo, no caso $\ell = 5$, $S_0 = \{11\}$; $-b = -11$ satisfaz. Antes da demonstração desse resultado, precisamos do lema a seguir.

Definimos $f(z) = 6\mathcal{H}^{b,\mathrm{P}}(z)$. Claramente os coeficientes de $f(z)$ são inteiros raionais pois $0 \not\equiv c \pmod{d}$, ou seja, $H(0) = -1/12$ não aparece em $f(z)$.

Lema 3.5 *Seja* p *um primo racional satisfazendo* $p^2 \equiv 1 \pmod{\mathrm{P}}$*,* $p \not\equiv (-b/p) \pmod{\ell}$*. Então* $(U_p f)(z) \not\equiv (V_p f)(z) \pmod{\ell}$*.*

Prova. Já sabemos que $\mathcal{H}^{b,\mathrm{P}}(z) \in \mathrm{M}_{3/2}(4\mathrm{P}^2)$. Desde que $\mathrm{M}_{3/2}(4\mathrm{P}^2)$ é um espaço vetorial complexo temos que $f(z) = 6\mathcal{H}^{b,\mathrm{P}}(z) \in \mathrm{M}_{3/2}(4\mathrm{P}^2)$. Agora segue da definição de U_p e V_p que

$$\begin{aligned}(U_p f)(z) &= 6 \sum_{pn\equiv b \pmod{\mathrm{P}}} H(pn)q^n \in \mathrm{M}_{3/2}(4\mathrm{P}^2 p),\\ (V_p f)(z) &= 6 \sum_{n\equiv b \pmod{\mathrm{P}}} H(n)q^{pn} \in \mathrm{M}_{3/2}(4\mathrm{P}^2 p).\end{aligned}$$

Pois nesse caso, χ é o carácter trivial. Os bp-ésimos coeficientes de $(U_p f)(z)$ e $(V_p f)(z)$ são respectivamente $H(bp^2) = (1 + p - (-b/p))H(b)$ e $H(\frac{bp}{p}) = H(b)$. Note que $H(bp^2)$

aparece em $(U_p f)(z)$ pois $bp^2 \equiv b \pmod{P}$. Por hipótese $p \not\equiv (-b/p) \pmod{\ell}$, ou seja, $p - (-b/p) \not\equiv 0 \pmod{\ell}$, logo os dois coeficientes acima não podem ser congruentes módulo ℓ. ■

Prova do teorema 3.4. Pelo lema acima e pelo teorema de Sturm, existe um número natural n_p com

$$\begin{aligned} n_p < \kappa(4\mathrm{P}^2 p, 3/2) &= \frac{3}{2} \cdot \frac{1}{12} \cdot 4\mathrm{P}^2 p \prod_{q \,|\, 4\mathrm{P}^2 p} (1 + q^{-1}) \\ &= \frac{1}{2}\mathrm{P}^2 p \prod_{q \,|\, p\mathrm{P}} (1 + q^{-1}); \end{aligned}$$

(note que $q \,|\, 4\mathrm{P}^2 p = 4\mathrm{PP}p$ implica que $q \,|\, p\mathrm{P}$ já que $q \,|\, 4\mathrm{P}$ implicaria 4P múltiplo de q e daí P múltiplo de $1/4$, o que certamente não ocorre) tal que o n_p-ésimo coeficiente de $(U_p f)(z) - (V_p f)(z)$ é não congruente a 0 módulo ℓ, isto é,

$$H(pn_p) \not\equiv H\left(\frac{n_p}{p}\right) \pmod{\ell}.$$

Se $p \nmid n_p$, interpretamos que o n_p-ésimo coeficiente $H(n_p/p)$ de $(V_p f)(z)$ é 0 (pois nesse caso $H(n_p/p)$ não está definido). Assim

$$H(pn_p) \not\equiv 0 \pmod{\ell}.$$

Desde que $pn_p \equiv b \pmod{\mathrm{P}}$, vemos também que

$$\left(\frac{-pn_p}{q}\right) = \left(\frac{-b}{q}\right) = 0, 1, -1 \quad \text{se} \quad q \in S_0, S_+, S_-$$

respectivamente.

Por outro lado, se $p \mid n_p$, isto é, $n_p = pn'_p$ para algum número natural n'_p, então

$$H(pn_p) = H(p^2 n'_p) = \left(1 + p - \left(\frac{-n'_p}{p}\right)\right) H(n'_p) \not\equiv H(n'_p) \pmod{\ell}.$$

Como $H(pn_p)$ é múltiplo de $H(n'_p)$ temos necessariamente que $H(n'_p) \not\equiv 0 \pmod{\ell}$, caso contrário $H(pn_p)$ seria múltiplo de ℓ e, consequentemente, a diferença $H(pn_p) - H(n'_p)$ também seria múltiplo de ℓ e chegaríamos a um absurdo. Além disso, temos $n'_p = pn_p/p^2 \equiv pn_p \pmod{\mathrm{P}}$ pois $p^2 \equiv 1 \pmod{\mathrm{P}}$. Isso nos diz que

$$\left(\frac{-n'_p}{q}\right) = \left(\frac{-pn_p}{q}\right) = \left(\frac{-b}{q}\right) = 0, 1, -1 \quad \text{se} \quad q \in S_0, S_+, S_-$$

respectivamente. Tomando $m_p = pn_p$ ou n'_p conforme $p \nmid n_p$ ou $p \mid n_p$ e usando a fórmula (3.1), temos o resultado. ■

Corolário 3.6 (do teorema 3.4) *Com as mesmas hipóteses do teorema* 3.4*, sejam* ℓ *um primo suficientemente grande e* $\varepsilon > 0$ *um número real arbitrário. Então, para* $\mathrm{X} > 0$ *suficientemente grande, temos*

$$\sharp\{k \in \mathcal{Q}^{-}(\mathrm{X}); \ell \nmid h(k) \text{ e (ii) vale em } k \} \gg_{\ell,\varepsilon,\mathrm{P}} \frac{\sqrt{\mathrm{X}}}{\log \mathrm{X}}$$

(a constante depende das variáveis no subscrito).

Prova. Primeiramente observemos que as condições sobre p indicadas no teorema são equivalentes a condição que p pertence a alguma progressão aritmética módulo P. Com efeito, podemos considerar a progressão $1 + s\mathrm{P}$, $s \in \mathbb{Z}$. Dado $p_1 = 1 + s_1\mathrm{P}$ temos que

$$\mathrm{P} \mid p_1 - 1 \Rightarrow \mathrm{P} \mid (p_1 - 1)(p_1 + 1) \Rightarrow \mathrm{P} \mid ({p_1}^2 - 1) \Rightarrow p_1^2 \equiv 1 \ (\mod \mathrm{P}).$$

Sejam $p_1 < p_2 < p_3 \cdots$ os primos contidos em uma dessas progressões, tomados em ordem crescente. Pelo teorema 3.4, podemos concluir que de cada três primos $p_i < p_j < p_k$, pelo menos dois dos discriminantes $\mathrm{D}_i, \mathrm{D}_j, \mathrm{D}_k$ dos corpos quadráticos imaginários $\mathbb{Q}(\sqrt{-m_{p_i}}), \mathbb{Q}(\sqrt{-m_{p_j}}), \mathbb{Q}(\sqrt{-m_{p_k}})$ são distintos.

Agora seja t a quantidades de primos em S. Defina $\mathrm{X} = 2^{t-1}\mathrm{P}^2{p_i}^2$ e denote por $\mathbf{\Pi}_{\mathrm{P}}(\mathrm{X})$ a cardinalidade do conjunto

$$\{p \in \mathbb{Z} \text{ primo} \mid p < \mathrm{X} \text{ e } p \text{ está em P.A. módulo P}\}.$$

Sabemos que

$$\mathbf{\Pi}_{\mathrm{P}}(\mathrm{X}) = \frac{1}{\varphi(\mathrm{P})} \cdot \frac{\mathrm{X}}{\log \mathrm{X}}.$$

Assim,

$$\begin{aligned}
\frac{\mathbf{\Pi}_{\mathrm{P}}(\mathrm{X})}{2} = \frac{1}{2} \cdot \frac{1}{\varphi(\mathrm{P})} \cdot \frac{\mathrm{X}}{\log \mathrm{X}} \Rightarrow \frac{\mathbf{\Pi}_{\mathrm{P}}(\mathrm{X})}{2} &= \frac{1}{2} \cdot \frac{1}{\varphi(4q_1 \cdots q_t)} \cdot \frac{2^{t-1}\mathrm{P}^2{p_i}^2}{\log \mathrm{X}} \\
&= \frac{1}{2} \cdot \frac{1}{2(q_1 - 1) \cdots (q_t - 1)} \cdot \frac{2^{t-1}4^2{q_1}^2 \cdots {q_t}^2{p_i}^2}{\log \mathrm{X}} \\
&> \frac{2^{t-1}4^2{q_1}^2 \cdots {q_t}^2{p_i}^2}{\log \mathrm{X}} > \frac{\sqrt{2^{t-1}4^2{q_1}^2 \cdots {q_t}^2{p_i}^2}}{\log \mathrm{X}} \\
&= \frac{\sqrt{2^{t-1}}4q_1 \cdots q_t p_i}{\log \mathrm{X}} = \frac{\sqrt{\mathrm{X}}}{\log \mathrm{X}}.
\end{aligned}$$

Por outro lado, sabemos também que para cada um desses primos p_i, temos

$$\mathrm{D}_i \geq -p_i\kappa(4\mathrm{P}^2p_i, \frac{3}{2}) = -p_i \cdot \frac{1}{2} \cdot \mathrm{P}^2p_i \prod_{q \mid p_i\mathrm{P}} (1 + q^{-1}) > -\frac{1}{2}\mathrm{P}^2p_i^2 2^t = -2^{t-1}\mathrm{P}^2p_i^2 = -\mathrm{X}$$

e, portanto, o corolário está provado. ■

Referências Bibliográficas

[1] K. Belabas and E. Fouvry, *Sur le 3-rang des corps quadratiques de discriminant premier ou presque premier*, Duke Math. J. (2) 98 (1999), 217-268.

[2] P.B. Bhattacharya, S.K. Jain and S.R. Nagpaul, *Basic abstract algebra*, Cambridge University Press 2ed., New York, 1995.

[3] D. Byeon, *Indivisibility of class numbers and Iwasawa λ-invariants of real quadratic fields*, Compositio Math. (3) 126 (2001), 249-256.

[4] D. Byeon, *Class numbers and Iwasawa invariants of certain totally real number fields*, J. Number Theory, (2) 79 (1999), 249-257.

[5] D. Byeon, *A note on basic Iwasawa λ-invariants of imaginary quadratic fields and congruence of modular forms*, Acta Arith. (3) 89 (1999), 295-299.

[6] H. Cohen, *A course in computational algebraic number theory*, Springer-Verlag, Berlin, 1993.

[7] H. Cohen, *Sums involving the values at negative integers of L-functions of quadratic characters*, Math. Ann. 217 (1975), 271-285.

[8] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields. II*, Proc. Roy. Soc. London Ser. A 322 (1971), 405-420.

[9] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields*, Bull. London Math. Soc. 1 (1969), 345-348.

[10] D.S. Dumit and R.M. Foote, *Basic abstract algebra*, John Wiley and Sons, Inc. 3ed., New Jersey, 2004.

[11] P. Hartung, *Proof of the existence of infinitely many imaginary quadratic fields whose class number is not divisible by 3*, J. Number Theory 6 (1974), 276-278.

[12] K. Horie, *Trace formulae and imaginary quadratic fields*, Math. Ann. (4) 288 (1990), 605-612.

[13] K. Horie and Y. Ônishi. *The existence of certain infinite families of imaginary quadratic fields*, J. Reine Angew. Math. 390 (1988), 97-113.

[14] K. Horie, *A note on basic Iwasawa λ-invariants of imaginary quadratic fields*, Invent. Math. (1) 88 (1987), 31-38.

[15] K. Iwasawa, *A note on class numbers of algebraic number fields*, Abh. Math. Sem. Univ. Hamburg, 20 (1956), 257-258.

[16] I. Kimura, *A note on the existence of certain infinite families of imaginary quadratic fields*, Acta Arithmetica 110.1 (2003), 37-43.

[17] I. Kimura, *Indivisibility of special values of zeta functions associated to real quadratic fields*, submitted, 2007.

[18] W. Kohnen and K. Ono, *Indivibility of class numbers of imaginary quadratic fields and orders of Tate-Shafarevich groups of elliptic curves with complex multiplication*, Invent. Math. 135 (1999), 387-398.

[19] F. Lemmermeyer, *Reciprocity laws: From Euler to Eisensteins*, Springer, 2000.

[20] M. R. Murty, *Congruence between modular forms* in: Analitic Number Theory (Kioto, 1996), London Mayh. Soc. Japan 43 (1991), 185-194.

[21] K. Ono, *Indivisibility of class numbers of real quadratic fields*, Compositio Math. (1) 119 (1999), 1-11.

[22] P. Ribenboin *Algebraic numbers*, John Wiley and Sons, Inc., Toronto, 1972.

[23] P. Samuel, *Algebraic theory of numbers*, Dover ed., Paris, 1970.

[24] J. P. O. Santos, *Intodução à teoria dos números*, IMPA 2ed., Rio de Janeiro, 2005.

[25] J. P. Serre, *A course in arithmetic*, Springer-Verlag, New York, 1973.

[26] G. Shimura, *Introduction to the arithmetic theory of automorphic functios*, Princiton University Press, Princiton, 1971.

[27] G. Shimura, *On modular forms of half integral weight*, Ann. of Math. (2) 97 (1973), 440-481.

[28] S. Shokranian, *Geometria hiperbólica e teoria dos números*, Editora UnB, Brasília, 2004.

[29] S. Shokranian, *Variável complexa 1*, Editora UnB, Brasília, 2002.

[30] J. Sturm, *On the congruence of modular forms*, in: Number theory (New York, 1984-1985), Lecture Notes in Math. 1240, Springer, Berlin, 1987, 275-280.

[31] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. 142 (1995), 443-551.